Contents

Formaliz. Math. 27 (**2**)

FORMALIZED MATHEMATICS
Vol. 27, No. 2, Pages 93–100, 2019
DOI: 10.2478/forma-2019-0010

https://www.sciendo.com/

On Roots of Polynomials over $F[X]/\langle p\rangle$

Christoph Schwarzweller
Institute of Informatics
University of Gdańsk
Poland

Summary. This is the first part of a four-article series containing a Mizar [3], [1], [2] formalization of Kronecker's construction about roots of polynomials in field extensions, i.e. that for every field F and every polynomial $p \in F[X]\backslash F$ there exists a field extension E of F such that p has a root over E. The formalization follows Kronecker's classical proof using $F[X]/{<}p{>}$ as the desired field extension E [9], [4], [6].

In this first part we show that an irreducible polynomial $p \in F[X]\backslash F$ has a root over $F[X]/{<}p{>}$. Note, however, that this statement cannot be true in a rigid formal sense: We do not have $F \subseteq F[X]/ < p >$ as sets, so F is not a subfield of $F[X]/{<}p{>}$, and hence formally p is not even a polynomial over $F[X]/ < p >$. Consequently, we translate p along the canonical monomorphism $\phi : F \longrightarrow F[X]/{<}p{>}$ and show that the translated polynomial $\phi(p)$ has a root over $F[X]/{<}p{>}$.

Because F is not a subfield of $F[X]/{<}p{>}$ we construct in the second part the field $(E \setminus \phi F) \cup F$ for a given monomorphism $\phi : F \longrightarrow E$ and show that this field both is isomorphic to F and includes F as a subfield. In the literature this part of the proof usually consists of saying that "one can identify F with its image ϕF in $F[X]/{<}p{>}$ and therefore consider F as a subfield of $F[X]/{<}p{>}$". Interestingly, to do so we need to assume that $F \cap E = \emptyset$, in particular Kronecker's construction can be formalized for fields F with $F \cap F[X] = \emptyset$.

Surprisingly, as we show in the third part, this condition is not automatically true for arbitray fields F: With the exception of $\mathbb{Z}_2$ we construct for every field F an isomorphic copy F' of F with $F' \cap F'[X] \neq \emptyset$. We also prove that for Mizar's representations of $\mathbb{Z}_n$, $\mathbb{Q}$ and $\mathbb{R}$ we have $\mathbb{Z}_n \cap \mathbb{Z}_n[X] = \emptyset$, $\mathbb{Q} \cap \mathbb{Q}[X] = \emptyset$ and $\mathbb{R} \cap \mathbb{R}[X] = \emptyset$, respectively.

In the fourth part we finally define field extensions: E is a field extension of F iff F is a subfield of E. Note, that in this case we have $F \subseteq E$ as sets, and thus a polynomial p over F is also a polynomial over E. We then apply the construction of the second part to $F[X]/{<}p{>}$ with the canonical monomorphism

ISSN 1426–2630(Print), 1898-9934(Online)

$\phi : F \longrightarrow F[X]/{<}p{>}$. Together with the first part this gives - for fields F with $F \cap F[X] = \emptyset$ - a field extension E of F in which $p \in F[X] \backslash F$ has a root.

MSC: 12E05 12F05 68T99 03B35

Keywords: roots of polynomials; field extensions; Kronecker's construction

MML identifier: FIELD_1, version: 8.1.09 5.57.1355

1. Preliminaries

From now on n denotes a natural number.

Let L be a non empty zero structure and p be a polynomial over L. We introduce the notation $\mathrm{LM}(p)$ as a synonym of Leading-Monomial p.

Now we state the proposition:

(1) Let us consider a non empty zero structure L, and a polynomial p over L. Then $\deg p$ is an element of $\mathbb{N}$ if and only if $p \neq \mathbf{0}.L$.

Let R be a non degenerated ring and p be a non zero polynomial over R. Note that the functor $\deg p$ yields an element of $\mathbb{N}$. Let R be an add-associative, right zeroed, right complementable, right distributive, non empty double loop structure and f be an additive function from R into R. One can check that $f(0_R)$ reduces to 0_R.

Now we state the proposition:

(2) Let us consider a ring R, an ideal I of R, an element x of ${}^{R}\!/_{I}$, and an element a of R. Suppose $x = [a]_{\mathrm{EqRel}(R,I)}$. Let us consider a natural number n. Then $x^n = [a^n]_{\mathrm{EqRel}(R,I)}$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv x^{\$_1} = [a^{\$_1}]_{\mathrm{EqRel}(R,I)}$. For every natural number i, $\mathcal{P}[i]$. □

Let R be a ring and a, b be elements of R. We say that b is an irreducible factor of a if and only if

(Def. 1) $b \mid a$ and b is irreducible.

Observe that there exists an integral domain which is non almost left invertible and factorial.

Now we state the proposition:

(3) Let us consider a non almost left invertible, factorial integral domain R, and a non zero non-unit a of R. Then there exists an element b of R such that b is an irreducible factor of a.

2. THE POLYNOMIALS $a \cdot x^n$

Let R be a ring, a be an element of R, and n be a natural number. We introduce the notation $\mathrm{anpoly}(a,n)$ as a synonym of $\mathrm{seq}(n,a)$.

Let R be a non degenerated ring and a be a non zero element of R. One can check that $\mathrm{anpoly}(a,n)$ is non zero.

Let R be a ring and a be a zero element of R. Observe that $\mathrm{anpoly}(a,n)$ is zero.

Now we state the propositions:

(4) Let us consider a non degenerated ring R, and a non zero element a of R. Then $\deg \mathrm{anpoly}(a,n) = n$.

(5) Let us consider a non degenerated ring R, and an element a of R. Then $\mathrm{LC}\, \mathrm{anpoly}(a,n) = a$.

(6) Let us consider a non degenerated ring R, a non zero natural number n, and elements a, x of R. Then $\mathrm{eval}(\mathrm{anpoly}(a,n),x) = a \cdot (x^n)$.

(7) Let us consider a non degenerated ring R, and an element a of R. Then $\mathrm{anpoly}(a,0) = a \restriction R$.

(8) Let us consider a non degenerated ring R, and a non zero element n of $\mathbb{N}$. Then $\mathrm{anpoly}(1_R,n) = \mathrm{rpoly}(n,0_R)$.

(9) Let us consider a non degenerated commutative ring R, and non zero elements a, b of R. Then $b \cdot (\mathrm{anpoly}(a,n)) = \mathrm{anpoly}(a \cdot b,n)$.

(10) Let us consider a non degenerated commutative ring R, non zero elements a, b of R, and natural numbers n, m. Then $\mathrm{anpoly}(a,n) * \mathrm{anpoly}(b,m) = \mathrm{anpoly}(a \cdot b, n+m)$. The theorem is a consequence of (9).

(11) Let us consider a non degenerated ring R, and a non zero polynomial p over R. Then $\mathrm{LM}(p) = \mathrm{anpoly}(p(\deg p), \deg p)$.

(12) Let us consider a non degenerated commutative ring R. Then $\langle 0_R, 1_R\rangle^n = \mathrm{anpoly}(1_R,n)$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv \langle 0_R, 1_R\rangle^{\$_1} = \mathrm{anpoly}(1_R, \$_1)$. $\mathcal{P}[0]$ by [8, (15)]. For every natural number k, $\mathcal{P}[k]$. □

3. MORE ON HOMOMORPHISMS

Now we state the propositions:

(13) Let us consider a ring R, an R-homomorphic ring S, a homomorphism h from R to S, an element a of R, and a natural number n. Then $h(a^n) = h(a)^n$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv h(a^{\$_1}) = h(a)^{\$_1}$. $\mathcal{P}[0]$ by [10, (8)]. For every natural number n, $\mathcal{P}[n]$. □

(14) Let us consider a ring R, an R-homomorphic ring S, and a homomorphism h from R to S. Then $h(\sum \varepsilon_{\alpha}) = 0_S$, where α is the carrier of R.

Let us consider a ring R, an R-homomorphic ring S, a homomorphism h from R to S, a finite sequence F of elements of R, and an element a of R. Now we state the propositions:

(15) $h(\sum(\langle a\rangle \frown F)) = h(a) + h(\sum F)$.

(16) $h(\sum(F \frown \langle a\rangle)) = h(\sum F) + h(a)$.

(17) Let us consider a ring R, an R-homomorphic ring S, a homomorphism h from R to S, and finite sequences F, G of elements of R. Then $h(\sum(F \frown G)) = h(\sum F) + h(\sum G)$.

(18) Let us consider a ring R, an R-homomorphic ring S, and a homomorphism h from R to S. Then $h(\prod \varepsilon_{\alpha}) = 1_S$, where α is the carrier of R.

Let us consider a ring R, an R-homomorphic ring S, a homomorphism h from R to S, a finite sequence F of elements of R, and an element a of R. Now we state the propositions:

(19) $h(\prod(\langle a\rangle \frown F)) = h(a) \cdot h(\prod F)$.

(20) $h(\prod(F \frown \langle a\rangle)) = h(\prod F) \cdot h(a)$.

(21) Let us consider a ring R, an R-homomorphic ring S, a homomorphism h from R to S, and finite sequences F, G of elements of R. Then $h(\prod(F \frown G)) = h(\prod F) \cdot h(\prod G)$.

4. Lifting Homomorphisms from R to $R[X]$

Let R, S be rings, f be a function from PolyRing(R) into PolyRing(S), and p be an element of the carrier of PolyRing(R). Observe that the functor $f(p)$ yields an element of the carrier of PolyRing(S). Let R be a ring, S be an R-homomorphic ring, and h be an additive function from R into S. The functor PolyHom(h) yielding a function from PolyRing(R) into PolyRing(S) is defined by

(Def. 2) for every element f of the carrier of PolyRing(R) and for every natural number i, $(it(f))(i) = h(f(i))$.

Let h be a homomorphism from R to S. Observe that PolyHom(h) is additive, multiplicative, and unity-preserving.

Let us consider a ring R, an R-homomorphic ring S, and a homomorphism h from R to S. Now we state the propositions:

(22) $(\mathrm{PolyHom}(h))(\mathbf{0}.R) = \mathbf{0}.S$.

(23) $(\mathrm{PolyHom}(h))(\mathbf{1}.R) = \mathbf{1}.S$.

Let us consider a ring R, an R-homomorphic ring S, a homomorphism h from R to S, and elements p, q of the carrier of PolyRing(R). Now we state the propositions:

(24) $(\mathrm{PolyHom}(h))(p+q) = (\mathrm{PolyHom}(h))(p) + (\mathrm{PolyHom}(h))(q)$.

(25) $(\mathrm{PolyHom}(h))(p \cdot q) = (\mathrm{PolyHom}(h))(p) \cdot (\mathrm{PolyHom}(h))(q)$.

(26) Let us consider a ring R, an R-homomorphic ring S, a homomorphism h from R to S, an element p of the carrier of PolyRing(R), and an element b of R. Then $(\mathrm{PolyHom}(h))(b \cdot p) = h(b) \cdot (\mathrm{PolyHom}(h))(p)$.

(27) Let us consider a ring R, an R-homomorphic ring S, a homomorphism h from R to S, an element p of the carrier of PolyRing(R), and an element a of R. Then $h(\mathrm{eval}(p, a)) = \mathrm{eval}((\mathrm{PolyHom}(h))(p), h(a))$.

Proof: Define $\mathcal{P}$[natural number] $\equiv$ for every element p of the carrier of PolyRing(R) for every element a of R such that $\mathrm{len}\, p = \$_1$ holds $h(\mathrm{eval}(p, a)) = \mathrm{eval}((\mathrm{PolyHom}(h))(p), h(a))$. $\mathcal{P}[0]$ by [7, (5), (17)], [5, (6)], (22). For every natural number k, $\mathcal{P}[k]$. □

(28) Let us consider an integral domain R, an R-homomorphic integral domain S, a homomorphism h from R to S, an element p of the carrier of PolyRing(R), and elements b, x of R. Then $h(\mathrm{eval}(b \cdot p, x)) = h(b) \cdot (\mathrm{eval}((\mathrm{PolyHom}(h))(p), h(x)))$. The theorem is a consequence of (27) and (26).

Let R be a ring. One can check that there exists a ring which is R-homomorphic and R-monomorphic and there exists a ring which is R-homomorphic and R-isomorphic and every ring which is R-monomorphic is also R-homomorphic.

Let S be an R-homomorphic, R-monomorphic ring and h be a monomorphism of R and S. Note that PolyHom(h) is monomorphic.

Let S be an R-isomorphic, R-homomorphic ring and h be an isomorphism between R and S. Let us note that PolyHom(h) is isomorphism.

Now we state the propositions:

(29) Let us consider a ring R, an R-homomorphic ring S, a homomorphism h from R to S, and an element p of the carrier of PolyRing(R). Then $\deg(\mathrm{PolyHom}(h))(p) \leqslant \deg p$.

(30) Let us consider a non degenerated ring R, an R-homomorphic ring S, a homomorphism h from R to S, and a non zero element p of the carrier of PolyRing(R). Then $\deg(\mathrm{PolyHom}(h))(p) = \deg p$ if and only if $h(\mathrm{LC}\, p) \neq 0_S$.

Let us consider a ring R, an R-monomorphic, R-homomorphic ring S, a monomorphism h of R and S, and an element p of the carrier of PolyRing(R). Now we state the propositions:

(31) $\deg(\mathrm{PolyHom}(h))(p) = \deg p$.

(32) LM((PolyHom(h))(p)) = (PolyHom(h))(LM(p)). The theorem is a consequence of (31).

(33) Let us consider a ring R, an R-homomorphic ring S, a homomorphism h from R to S, an element p of the carrier of PolyRing(R), and an element a of R. If a is a root of p, then $h(a)$ is a root of (PolyHom(h))(p). The theorem is a consequence of (27).

(34) Let us consider a ring R, an R-monomorphic, R-homomorphic ring S, a monomorphism h of R and S, an element p of the carrier of PolyRing(R), and an element a of R. Then a is a root of p if and only if $h(a)$ is a root of (PolyHom(h))(p). The theorem is a consequence of (27) and (33).

(35) Let us consider a ring R, an R-isomorphic, R-homomorphic ring S, an isomorphism h between R and S, an element p of the carrier of PolyRing (R), and an element b of S. Then b is a root of (PolyHom(h))(p) if and only if there exists an element a of R such that a is a root of p and $h(a) = b$. The theorem is a consequence of (27).

(36) Let us consider a ring R, an R-homomorphic ring S, a homomorphism h from R to S, and an element p of the carrier of PolyRing(R). Then Roots(p) $\subseteq$ $\{a$, where a is an element of $R : h(a) \in$ Roots((PolyHom(h)) (p))$\}$. The theorem is a consequence of (33).

(37) Let us consider a ring R, an R-monomorphic, R-homomorphic ring S, a monomorphism h of R and S, and an element p of the carrier of PolyRing(R). Then Roots(p) $=$ $\{a$, where a is an element of $R : h(a) \in$ Roots((PolyHom(h))(p))$\}$. The theorem is a consequence of (36) and (34).

(38) Let us consider a ring R, an R-isomorphic, R-homomorphic ring S, an isomorphism h between R and S, and an element p of the carrier of PolyRing(R). Then Roots((PolyHom(h))(p)) $=$ $\{h(a)$, where a is an element of $R : a \in$ Roots(p)$\}$. The theorem is a consequence of (35).

5. Kronecker's Construction

In the sequel F denotes a field, p denotes an irreducible element of the carrier of PolyRing(F), f denotes an element of the carrier of PolyRing(F), and a denotes an element of F.

Let us consider F and p. The functor KroneckerField(F, p) yielding a field is defined by the term

(Def. 3) $\text{PolyRing}(F)/_{\{p\}\text{-ideal}}$.

The functor embedding(p) yielding a function from F into KroneckerField (F, p) is defined by the term

(Def. 4) (the canonical homomorphism of $\{p\}$–ideal into quotient field) $\cdot$ (the canonical homomorphism of F into quotient field).

Let us observe that embedding(p) is additive, multiplicative, and unity-preserving and embedding(p) is monomorphic and KroneckerField(F, p) is F-homomorphic and F-monomorphic.

Let us consider f. The functor f_p yielding an element of the carrier of PolyRing(KroneckerField(F, p)) is defined by the term

(Def. 5) (PolyHom(embedding(p)))(f).

The functor KrRoot(p) yielding an element of KroneckerField(F, p) is defined by the term

(Def. 6) $[\langle 0_F, 1_F\rangle]_{\mathrm{EqRel(PolyRing}(F),\{p\}\text{–ideal})}$.

Now we state the propositions:

(39) (embedding(p))$(a) = [a{\restriction}F]_{\mathrm{EqRel(PolyRing}(F),\{p\}\text{–ideal})}$.

(40) $(f_p)(n) = [f(n){\restriction}F]_{\mathrm{EqRel(PolyRing}(F),\{p\}\text{–ideal})}$. The theorem is a consequence of (39).

(41) eval$(f_p$, KrRoot$(p)) = [f]_{\mathrm{EqRel(PolyRing}(F),\{p\}\text{–ideal})}$.

PROOF: Set $z =$ KrRoot(p). Define $\mathcal{P}$[natural number] $\equiv$ for every f such that len $f = \$_1$ holds eval$(f_p, z) = [f]_{\mathrm{EqRel(PolyRing}(F),\{p\}\text{–ideal})}$. For every natural number k, $\mathcal{P}[k]$. □

(42) KrRoot(p) is a root of p_p. The theorem is a consequence of (41).

(43) If f is not constant, then there exists an irreducible element p of the carrier of PolyRing(F) such that f_p has roots. The theorem is a consequence of (3) and (42).

(44) If embedding(p) is isomorphism, then p has roots. The theorem is a consequence of (38) and (42).

(45) If p has no roots, then embedding(p) is not isomorphism.

REFERENCES

[1] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, Karol Pąk, and Josef Urban. Mizar: State-of-the-art and beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8_17.

[2] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pąk. The role of the Mizar Mathematical Library for interactive proof development in Mizar. *Journal of Automated Reasoning*, 61(1):9–32, 2018. doi:10.1007/s10817-017-9440-6.

[3] Adam Grabowski, Artur Korniłowicz, and Christoph Schwarzweller. On algebraic hierarchies in mathematical repository of Mizar. In M. Ganzha, L. Maciaszek, and M. Paprzycki, editors, *Proceedings of the 2016 Federated Conference on Computer Science and Infor-*

mation Systems (FedCSIS), volume 8 of *Annals of Computer Science and Information Systems*, pages 363–371, 2016. doi:10.15439/2016F520.

[4] Nathan Jacobson. *Basic Algebra I.* Dover Books on Mathematics, 1985.

[5] Artur Korniłowicz and Christoph Schwarzweller. The first isomorphism theorem and other properties of rings. *Formalized Mathematics*, 22(**4**):291–301, 2014. doi:10.2478/forma-2014-0029.

[6] Heinz Lüneburg. *Gruppen, Ringe, Körper: Die grundlegenden Strukturen der Algebra.* Oldenbourg Verlag, 1999.

[7] Robert Milewski. The evaluation of polynomials. *Formalized Mathematics*, 9(**2**):391–395, 2001.

[8] Robert Milewski. Fundamental theorem of algebra. *Formalized Mathematics*, 9(**3**):461–470, 2001.

[9] Knut Radbruch. *Algebra I.* Lecture Notes, University of Kaiserslautern, Germany, 1991.

[10] Christoph Schwarzweller. The binomial theorem for algebraic structures. *Formalized Mathematics*, 9(**3**):559–564, 2001.

Accepted March 28, 2019

FORMALIZED MATHEMATICS
Vol. 27, No. 2, Pages 101–106, 2019
DOI: 10.2478/forma-2019-0011

sciendo
https://www.sciendo.com/

Isomorphisms from the Space of Multilinear Operators

Kazuhisa Nakasho
Yamaguchi University
Yamaguchi, Japan

Summary. In this article, using the Mizar system [5], [2], the isomorphisms from the space of multilinear operators are discussed. In the first chapter, two isomorphisms are formalized. The former isomorphism shows the correspondence between the space of multilinear operators and the space of bilinear operators.

The latter shows the correspondence between the space of multilinear operators and the space of the composition of linear operators. In the last chapter, the above isomorphisms are extended to isometric mappings between the normed spaces. We referred to [6], [11], [9], [3], [10] in this formalization.

MSC: 46-00 47A07 47A30 68T99 03B35

Keywords: linear operators; bilinear operators; multilinear operators; isomorphism of linear operator spaces

MML identifier: `LOPBAN12`, version: `8.1.09 5.57.1355`

1. Plain Isomorphisms from the Space of Multilinear Operators

From now on X, Y, Z, E, F, G, S, T denote real linear spaces.

Let G be a real linear space sequence. Note that $\prod G$ is constituted finite sequences. Now we state the propositions:

(1) Let us consider an element s of $\prod\langle E, F\rangle$, an element i of $\operatorname{dom}\langle E, F\rangle$, and an object x_1. Then $\operatorname{len}(s +\cdot (i, x_1)) = 2$.

(2) Let us consider a real linear space sequence G, an element i of $\operatorname{dom} G$, an element x of $\prod G$, and an element r of $G(i)$. Then $(\operatorname{reproj}(i, x))(r) = x +\cdot (i, r)$.

Let X, Y be real linear spaces. The functor IsoCPRLSP(X, Y) yielding a linear operator from $X \times Y$ into $\prod\langle X, Y\rangle$ is defined by

(Def. 1) for every point x of X and for every point y of Y, $it(x, y) = \langle x, y\rangle$.

Now we state the proposition:

(3) Let us consider real linear spaces X, Y. Then $0_{\prod\langle X,Y\rangle} =$ (IsoCPRLSP$(X, Y))(0_{X\times Y})$.

Let X, Y be real linear spaces. One can check that IsoCPRLSP(X, Y) is bijective and there exists a linear operator from $X \times Y$ into $\prod\langle X, Y\rangle$ which is bijective. Now we state the proposition:

(4) Let us consider a linear operator I from S into T. Suppose I is bijective. Then there exists a linear operator J from T into S such that

(i) $J = I^{-1}$, and

(ii) J is bijective.

Proof: Reconsider $J = I^{-1}$ as a function from T into S. For every points v, w of T, $J(v + w) = J(v) + J(w)$. For every point v of T and for every real number r, $J(r \cdot v) = r \cdot J(v)$. □

Let X, Y be real linear spaces and f be a bijective linear operator from $X \times Y$ into $\prod\langle X, Y\rangle$. One can verify that the functor f^{-1} yields a linear operator from $\prod\langle X, Y\rangle$ into $X \times Y$. One can check that f^{-1} is bijective as a linear operator from $\prod\langle X, Y\rangle$ into $X \times Y$ and there exists a linear operator from $\prod\langle X, Y\rangle$ into $X \times Y$ which is bijective. Now we state the propositions:

(5) Let us consider real linear spaces X, Y, a point x of X, and a point y of Y. Then $((\text{IsoCPRLSP}(X, Y))^{-1})(\langle x, y\rangle) = \langle x,\, y\rangle$.

(6) Let us consider real linear spaces X, Y. Then $((\text{IsoCPRLSP}(X, Y))^{-1})$ $(0_{\prod\langle X,Y\rangle}) = 0_{X\times Y}$. The theorem is a consequence of (3).

(7) Let us consider a multilinear operator u from $\langle E, F\rangle$ into G. Then $u \cdot$ (IsoCPRLSP$(E, F))$ is a bilinear operator from $E \times F$ into G.
Proof: Reconsider $L = u \cdot$ (IsoCPRLSP$(E, F))$ as a function from $E \times F$ into G. For every points x_1, x_2 of E and for every point y of F, $L(x_1 + x_2, y) = L(x_1, y) + L(x_2, y)$. For every point x of E and for every point y of F and for every real number a, $L(a \cdot x, y) = a \cdot L(x, y)$. For every point x of E and for every points y_1, y_2 of F, $L(x, y_1 + y_2) = L(x, y_1) + L(x, y_2)$. For every point x of E and for every point y of F and for every real number a, $L(x, a \cdot y) = a \cdot L(x, y)$ by [1, (31)]. □

(8) Let us consider a bilinear operator u from $E \times F$ into G. Then $u \cdot ((\text{IsoCPRLSP}(E, F))^{-1})$ is a multilinear operator from $\langle E, F\rangle$ into G.
Proof: Reconsider $M = u \cdot ((\text{IsoCPRLSP}(E, F))^{-1})$ as a function from $\prod\langle E, F\rangle$ into G. For every element i of dom$\langle E, F\rangle$ and for every element

s of $\prod\langle E, F\rangle$, $M \cdot (\mathrm{reproj}(i, s))$ is a linear operator from $\langle E, F\rangle(i)$ into G. □

(9) There exists a linear operator I from VectorSpaceOfBilinOpers$_{\mathbb{R}}(X, Y, Z)$ into VectorSpaceOfMultOpers$_{\mathbb{R}}(\langle X, Y\rangle, Z)$ such that

(i) I is bijective, and

(ii) for every point u of VectorSpaceOfBilinOpers$_{\mathbb{R}}(X, Y, Z)$, $I(u) = u \cdot ((\mathrm{IsoCPRLSP}(X, Y))^{-1})$.

Proof: Set F_1 = the carrier of VectorSpaceOfBilinOpers$_{\mathbb{R}}(X, Y, Z)$. Set F_2 = the carrier of VectorSpaceOfMultOpers$_{\mathbb{R}}(\langle X, Y\rangle, Z)$. Define $\mathcal{P}[\text{function}, \text{function}] \equiv \$_2 = \$_1 \cdot ((\mathrm{IsoCPRLSP}(X, Y))^{-1})$. For every element x of F_1, there exists an element y of F_2 such that $\mathcal{P}[x, y]$. Consider I being a function from F_1 into F_2 such that for every element x of F_1, $\mathcal{P}[x, I(x)]$. For every objects x_1, x_2 such that x_1, $x_2 \in F_1$ and $I(x_1) = I(x_2)$ holds $x_1 = x_2$. For every object y such that $y \in F_2$ there exists an object x such that $x \in F_1$ and $y = I(x)$. For every points x, y of VectorSpaceOfBilinOpers$_{\mathbb{R}}(X, Y, Z)$, $I(x + y) = I(x) + I(y)$. For every point x of VectorSpaceOfBilinOpers$_{\mathbb{R}}(X, Y, Z)$ and for every real number a, $I(a \cdot x) = a \cdot I(x)$. □

(10) There exists a linear operator I from VectorSpaceOfLinearOpers$_{\mathbb{R}}(X,$ VectorSpaceOfLinearOpers$_{\mathbb{R}}(Y, Z))$ into VectorSpaceOfMultOpers$_{\mathbb{R}}(\langle X, Y\rangle,$ $Z)$ such that

(i) I is bijective, and

(ii) for every point u of VectorSpaceOfLinearOpers$_{\mathbb{R}}(X,$ VectorSpaceOfLinearOpers$_{\mathbb{R}}(Y, Z))$ and for every point x of X and for every point y of Y, $I(u)(\langle x, y\rangle) = u(x)(y)$.

The theorem is a consequence of (9) and (5).

2. Extensions to Isometric Isomorphism from the Normed Space of Multilinear Operators

In the sequel X, Y, Z, E, F, G denote real normed spaces and S, T denote real norm space sequences. Now we state the propositions:

(11) Let us consider a point s of $\prod\langle E, F\rangle$, an element i of $\mathrm{dom}\langle E, F\rangle$, and an object x_1. Then $\mathrm{len}(s +\cdot (i, x_1)) = 2$.

(12) Let us consider a Lipschitzian multilinear operator u from $\langle E, F\rangle$ into G. Then $u \cdot (\mathrm{IsoCPNrSP}(E, F))$ is a Lipschitzian bilinear operator from E $\times$ F into G.

Proof: Reconsider $L = u \cdot (\mathrm{IsoCPNrSP}(E, F))$ as a function from $E \times F$ into G. For every points x_1, x_2 of E and for every point y of F, $L(x_1 + x_2, y) = L(x_1, y) + L(x_2, y)$. For every point x of E and for every point y of F and for every real number a, $L(a \cdot x, y) = a \cdot L(x, y)$. For every point x of E and for every points y_1, y_2 of F, $L(x, y_1 + y_2) = L(x, y_1) + L(x, y_2)$. For every point x of E and for every point y of F and for every real number a, $L(x, a \cdot y) = a \cdot L(x, y)$. There exists a real number K such that $0 \leqslant K$ and for every vector x of E and for every vector y of F, $\|L(x, y)\| \leqslant K \cdot \|x\| \cdot \|y\|$. □

(13) Let us consider a Lipschitzian bilinear operator u from $E \times F$ into G. Then $u \cdot ((\mathrm{IsoCPNrSP}(E, F))^{-1})$ is a Lipschitzian multilinear operator from $\langle E, F \rangle$ into G.

Proof: Reconsider $M = u \cdot ((\mathrm{IsoCPNrSP}(E, F))^{-1})$ as a function from $\prod\langle E, F \rangle$ into G. For every element i of $\mathrm{dom}\langle E, F \rangle$ and for every element s of $\prod\langle E, F \rangle$, $M \cdot (\mathrm{reproj}(i, s))$ is a linear operator from $\langle E, F \rangle(i)$ into G. There exists a real number K such that $0 \leqslant K$ and for every point s of $\prod\langle E, F \rangle$, $\|M(s)\| \leqslant K \cdot (\mathrm{NrProduct}\, s)$. □

(14) There exists a linear operator I from $\mathrm{NormSpaceOfBoundedBilinOpers}_{\mathbb{R}}(X, Y, Z)$ into $\mathrm{NormSpaceOfBoundedMultOpers}_{\mathbb{R}}(\langle X, Y \rangle, Z)$ such that

(i) I is bijective and isometric, and

(ii) for every point u of $\mathrm{NormSpaceOfBoundedBilinOpers}_{\mathbb{R}}(X, Y, Z)$, $I(u) = u \cdot ((\mathrm{IsoCPNrSP}(X, Y))^{-1})$.

Proof: Set $F_1 =$ the carrier of $\mathrm{NormSpaceOfBoundedBilinOpers}_{\mathbb{R}}(X, Y, Z)$. Set $F_2 =$ the carrier of $\mathrm{NormSpaceOfBoundedMultOpers}_{\mathbb{R}}(\langle X, Y \rangle, Z)$. Define $\mathcal{P}[\text{function}, \text{function}] \equiv \$_2 = \$_1 \cdot ((\mathrm{IsoCPNrSP}(X, Y))^{-1})$. For every element x of F_1, there exists an element y of F_2 such that $\mathcal{P}[x, y]$. Consider I being a function from F_1 into F_2 such that for every element x of F_1, $\mathcal{P}[x, I(x)]$. For every objects x_1, x_2 such that x_1, $x_2 \in F_1$ and $I(x_1) = I(x_2)$ holds $x_1 = x_2$. For every object y such that $y \in F_2$ there exists an object x such that $x \in F_1$ and $y = I(x)$. For every points x, y of $\mathrm{NormSpaceOfBoundedBilinOpers}_{\mathbb{R}}(X, Y, Z)$, $I(x + y) = I(x) + I(y)$. For every point x of $\mathrm{NormSpaceOfBoundedBilinOpers}_{\mathbb{R}}(X, Y, Z)$ and for every real number a, $I(a \cdot x) = a \cdot I(x)$ by [8, (19)], [4, (18)], [7, (20)]. For every element u of $\mathrm{NormSpaceOfBoundedBilinOpers}_{\mathbb{R}}(X, Y, Z)$, $\|I(u)\| = \|u\|$. □

(15) There exists a linear operator I from the real norm space of bounded linear operators from X into the real norm space of bounded linear operators from Y into Z into $\mathrm{NormSpaceOfBoundedMultOpers}_{\mathbb{R}}(\langle X, Y \rangle, Z)$ such that

(i) I is bijective and isometric, and

(ii) for every point u of the real norm space of bounded linear operators from X into the real norm space of bounded linear operators from Y into Z, $\|u\| = \|I(u)\|$ and for every point x of X and for every point y of Y, $I(u)(\langle x, y\rangle) = u(x)(y)$.

Proof: Consider I being a linear operator from the real norm space of bounded linear operators from X into the real norm space of bounded linear operators from Y into Z into $\mathrm{NormSpaceOfBoundedBilinOpers}_{\mathbb{R}}(X, Y, Z)$ such that I is bijective and for every point u of the real norm space of bounded linear operators from X into the real norm space of bounded linear operators from Y into Z, $\|u\| = \|I(u)\|$ and for every point x of X and for every point y of Y, $I(u)(x, y) = u(x)(y)$. Consider J being a linear operator from $\mathrm{NormSpaceOfBoundedBilinOpers}_{\mathbb{R}}(X, Y, Z)$ into $\mathrm{NormSpaceOfBoundedMultOpers}_{\mathbb{R}}(\langle X, Y\rangle, Z)$ such that J is bijective and isometric and for every point u of $\mathrm{NormSpaceOfBoundedBilinOpers}_{\mathbb{R}}(X, Y, Z)$, $J(u) = u \cdot ((\mathrm{IsoCPNrSP}(X, Y))^{-1})$.

Reconsider $K = J \cdot I$ as a linear operator from the real norm space of bounded linear operators from X into the real norm space of bounded linear operators from Y into Z into $\mathrm{NormSpaceOfBoundedMultOpers}_{\mathbb{R}}(\langle X, Y\rangle, Z)$. For every element x of the real norm space of bounded linear operators from X into the real norm space of bounded linear operators from Y into Z, $\|K(x)\| = \|x\|$. □

(16) Let us consider real norm space sequences X, Y, and a real normed space Z. Then there exists a linear operator I from the real norm space of bounded linear operators from $\prod X$ into the real norm space of bounded linear operators from $\prod Y$ into Z into $\mathrm{NormSpaceOfBoundedMultOpers}_{\mathbb{R}}(\langle \prod X, \prod Y\rangle, Z)$ such that

(i) I is bijective and isometric, and

(ii) for every point u of the real norm space of bounded linear operators from $\prod X$ into the real norm space of bounded linear operators from $\prod Y$ into Z, $\|u\| = \|I(u)\|$ and for every point x of $\prod X$ and for every point y of $\prod Y$, $I(u)(\langle x, y\rangle) = u(x)(y)$.

Acknowledgement: I would like to express my gratitude to Professor Yasunari Shidama for his helpful advice.

References

[1] Grzegorz Bancerek and Andrzej Trybulec. Miscellaneous facts about functions. *Formalized Mathematics*, 5(**4**):485–492, 1996.

[2] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pąk. The role of the Mizar Mathematical Library for interactive proof development in Mizar. *Journal of Automated Reasoning*, 61(1):9–32, 2018. doi:10.1007/s10817-017-9440-6.

[3] Nelson Dunford and Jacob T. Schwartz. *Linear operators I.* Interscience Publ., 1958.

[4] Yuichi Futa, Noboru Endou, and Yasunari Shidama. Isometric differentiable functions on real normed space. *Formalized Mathematics*, 21(**4**):249–260, 2013. doi:10.2478/forma-2013-0027.

[5] Adam Grabowski, Artur Korniłowicz, and Adam Naumowicz. Four decades of Mizar. *Journal of Automated Reasoning*, 55(3):191–198, 2015. doi:10.1007/s10817-015-9345-1.

[6] Miyadera Isao. *Functional Analysis.* Riko-Gaku-Sya, 1972.

[7] Kazuhisa Nakasho. Bilinear operators on normed linear spaces. *Formalized Mathematics*, 27(**1**):15–23, 2019. doi:10.2478/forma-2019-0002.

[8] Hiroyuki Okazaki, Noboru Endou, and Yasunari Shidama. Cartesian products of family of real linear spaces. *Formalized Mathematics*, 19(**1**):51–59, 2011. doi:10.2478/v10037-011-0009-2.

[9] Laurent Schwartz. *Théorie des ensembles et topologie, tome 1. Analyse.* Hermann, 1997.

[10] Laurent Schwartz. *Calcul différentiel, tome 2. Analyse.* Hermann, 1997.

[11] Kosaku Yoshida. *Functional Analysis.* Springer, 1980.

Accepted May 27, 2019

FORMALIZED MATHEMATICS
Vol. 27, No. 2, Pages 107–115, 2019
DOI: 10.2478/forma-2019-0012

sciendo
https://www.sciendo.com/

Invertible Operators on Banach Spaces

Kazuhisa Nakasho
Yamaguchi University
Yamaguchi, Japan

Summary. In this article, using the Mizar system [2], [1], we discuss invertible operators on Banach spaces. In the first chapter, we formalized the theorem that denotes any operators that are close enough to an invertible operator are also invertible by using the property of Neumann series.

In the second chapter, we formalized the continuity of an isomorphism that maps an invertible operator on Banach spaces to its inverse. These results are used in the proof of the implicit function theorem. We referred to [3], [10], [6], [7] in this formalization.

MSC: 47A05 47J07 68T99 03B35

Keywords: Banach space; invertible operator; Neumann series; isomorphism of linear operator spaces

MML identifier: `LOPBAN13`, version: `8.1.09 5.57.1355`

1. Neumann Series and Invertible Operator

From now on X, Y, Z denote non trivial real Banach spaces.

Let X, Y be real normed spaces and u be a point of the real norm space of bounded linear operators from X into Y. We say that u is invertible if and only if

(Def. 1) u is one-to-one and $\operatorname{rng} u =$ the carrier of Y and u^{-1} is a point of the real norm space of bounded linear operators from Y into X.

Assume u is invertible. The functor $\operatorname{Inv} u$ yielding a point of the real norm space of bounded linear operators from Y into X is defined by the term

(Def. 2) u^{-1}.

Now we state the propositions:

(1) Let us consider a real normed space X, a sequence s_6 of X, and a natural number k. Then $\|((\sum_{\alpha=0}^{\kappa} s_6(\alpha))_{\kappa\in\mathbb{N}})(k)\| \leqslant ((\sum_{\alpha=0}^{\kappa}\|s_6\|(\alpha))_{\kappa\in\mathbb{N}})(k)$.
PROOF: Define $\mathcal{P}[\text{natural number}] \equiv \|((\sum_{\alpha=0}^{\kappa} s_6(\alpha))_{\kappa\in\mathbb{N}})(\$_1)\| \leqslant ((\sum_{\alpha=0}^{\kappa}\|s_6\|(\alpha))_{\kappa\in\mathbb{N}})(\$_1)$. For every natural number k, $\mathcal{P}[k]$. □

(2) Let us consider a real Banach space X, and a sequence s of X. Suppose s is norm-summable. Then $\|\sum s\| \leqslant \sum\|s\|$. The theorem is a consequence of (1).

(3) Let us consider a Banach algebra, and a point z of X. Suppose $\|z\| < 1$. Then

(i) $(z^{\kappa})_{\kappa\in\mathbb{N}}$ is norm-summable, and

(ii) $\|\sum(z^{\kappa})_{\kappa\in\mathbb{N}}\| \leqslant \frac{1}{1-\|z\|}$.

PROOF: For every natural number n, $0 \leqslant \|(z^{\kappa})_{\kappa\in\mathbb{N}}\|(n) \leqslant ((\|z\|^{\kappa})_{\kappa\in\mathbb{N}})(n)$. $\|\sum(z^{\kappa})_{\kappa\in\mathbb{N}}\| \leqslant \sum\|(z^{\kappa})_{\kappa\in\mathbb{N}}\|$. □

(4) Let us consider a Banach algebra, and a point w of S. Suppose $\|w\| < 1$. Then

(i) $1_S + w$ is invertible, and

(ii) $((-w)^{\kappa})_{\kappa\in\mathbb{N}}$ is norm-summable, and

(iii) $(1_S + w)^{-1} = \sum((-w)^{\kappa})_{\kappa\in\mathbb{N}}$, and

(iv) $\|(1_S + w)^{-1}\| \leqslant \frac{1}{1-\|w\|}$.

The theorem is a consequence of (3).

(5) Let us consider a non trivial real Banach space X, Lipschitzian linear operators v_1, v_2 from X into X, points w_1, w_2 of NormedAlgebraOfBoundedLinearOpers$_{\mathbb{R}}(X)$, and a real number a. Suppose $v_1 = w_1$ and $v_2 = w_2$. Then

(i) $v_1 \cdot v_2 = w_1 \cdot w_2$, and

(ii) $v_1 + v_2 = w_1 + w_2$, and

(iii) $a \cdot v_1 = a \cdot w_1$.

PROOF: Reconsider $z_1 = w_1$, $z_3 = w_2$ as a point of the real norm space of bounded linear operators from X into X. Reconsider $z_2 = z_1 + z_3$ as a point of the real norm space of bounded linear operators from X into X. For every object s such that $s \in \operatorname{dom}(v_1 + v_2)$ holds $(v_1 + v_2)(s) = z_2(s)$. Reconsider $z_2 = a \cdot z_1$ as a point of the real norm space of bounded linear operators from X into X. For every object s such that $s \in \operatorname{dom}(a \cdot v_1)$ holds $(a \cdot v_1)(s) = z_2(s)$. □

(6) Let us consider a non trivial real Banach space X, points v_1, v_2 of the real norm space of bounded linear operators from X into X, points w_1, w_2 of NormedAlgebraOfBoundedLinearOpers$_{\mathbb{R}}(X)$, and a real number a. Suppose $v_1 = w_1$ and $v_2 = w_2$. Then

(i) $v_1 + v_2 = w_1 + w_2$, and

(ii) $a \cdot v_1 = a \cdot w_1$.

(7) Let us consider a non trivial real Banach space X, points v_1, v_2 of the real norm space of bounded linear operators from X into X, and points w_1, w_2 of NormedAlgebraOfBoundedLinearOpers$_{\mathbb{R}}(X)$. If $v_1 = w_1$ and $v_2 = w_2$, then $v_1 \cdot v_2 = w_1 \cdot w_2$.

(8) Let us consider a non trivial real Banach space X, a point v of the real norm space of bounded linear operators from X into X, and a point w of NormedAlgebraOfBoundedLinearOpers$_{\mathbb{R}}(X)$. Suppose $v = w$. Then

(i) v is invertible iff w is invertible, and

(ii) if w is invertible, then $v^{-1} = w^{-1}$.

Proof: If v is invertible, then w is invertible. If w is invertible, then v is invertible and $v^{-1} = w^{-1}$. □

(9) Let us consider points v, I of the real norm space of bounded linear operators from X into X. Suppose $I = \mathrm{id}_X$ and $\|v\| < 1$. Then

(i) $I + v$ is invertible, and

(ii) $\|\mathrm{Inv}\, I + v\| \leqslant \frac{1}{1-\|v\|}$, and

(iii) there exists a point w of NormedAlgebraOfBoundedLinearOpers$_{\mathbb{R}}(X)$ such that $w = v$ and $((-w)^{\kappa})_{\kappa \in \mathbb{N}}$ is norm-summable and $\mathrm{Inv}\, I + v = \sum((-w)^{\kappa})_{\kappa \in \mathbb{N}}$.

The theorem is a consequence of (4) and (8).

(10) Let us consider real normed spaces X, Y, Z, W, a point f of the real norm space of bounded linear operators from X into Y, a point g of the real norm space of bounded linear operators from Y into Z, and a point h of the real norm space of bounded linear operators from Z into W. Then $h \cdot (g \cdot f) = (h \cdot g) \cdot f$.

(11) Let us consider real normed spaces X, Y, and a point f of the real norm space of bounded linear operators from X into Y. Suppose f is one-to-one and $\mathrm{rng}\, f =$ the carrier of Y. Then

(i) $f^{-1} \cdot f = \mathrm{id}_X$, and

(ii) $f \cdot (f^{-1}) = \mathrm{id}_Y$.

(12) Let us consider a point u of the real norm space of bounded linear operators from X into Y. Suppose u is invertible. Then

(i) $0 < \|u\|$, and

(ii) $0 < \|\mathrm{Inv}\, u\|$.

(13) Let us consider points u, v of the real norm space of bounded linear operators from X into Y. Suppose u is invertible and $\|v\| < \frac{1}{\|\mathrm{Inv}\, u\|}$. Then

(i) $u + v$ is invertible, and

(ii) $\|\mathrm{Inv}\, u + v\| \leqslant \frac{1}{\frac{1}{\|\mathrm{Inv}\, u\|} - \|v\|}$, and

(iii) there exists a point w of NormedAlgebraOfBoundedLinearOpers$_{\mathbb{R}}(X)$ and there exist points s, I of the real norm space of bounded linear operators from X into X such that $w = (\mathrm{Inv}\, u) \cdot v$ and $s = w$ and $I = \mathrm{id}_X$ and $\|s\| < 1$ and $((-w)^{\kappa})_{\kappa \in \mathbb{N}}$ is norm-summable and $I + s$ is invertible and $\|\mathrm{Inv}\, I + s\| \leqslant \frac{1}{1 - \|s\|}$ and $\mathrm{Inv}\, I + s = \sum((-w)^{\kappa})_{\kappa \in \mathbb{N}}$ and $\mathrm{Inv}\, u + v = (\mathrm{Inv}\, I + s) \cdot (\mathrm{Inv}\, u)$.

PROOF: Reconsider $I = \mathrm{id}_X$ as a point of the real norm space of bounded linear operators from X into X. Reconsider $u_1 = (\mathrm{Inv}\, u) \cdot v$ as a point of the real norm space of bounded linear operators from X into X. $\|\mathrm{Inv}\, u\| \neq 0$ by [9, (2)]. $I + u_1$ is invertible and $\|\mathrm{Inv}\, I + u_1\| \leqslant \frac{1}{1 - \|u_1\|}$ and there exists a point w of NormedAlgebraOfBoundedLinearOpers$_{\mathbb{R}}(X)$ such that $w = u_1$ and $((-w)^{\kappa})_{\kappa \in \mathbb{N}}$ is norm-summable and $\mathrm{Inv}\, I + u_1 = \sum((-w)^{\kappa})_{\kappa \in \mathbb{N}}$. For every element x of the carrier of X, $(u + v)(x) = (u \cdot (I + u_1))(x)$. $\mathrm{PartFuncs}((I + u_1)^{-1}, X, X) = \mathrm{PartFuncs}(\mathrm{Inv}\, I + u_1, X, X)$. Consider w being a point of NormedAlgebraOfBoundedLinearOpers$_{\mathbb{R}}(X)$ such that $w = u_1$ and $((-w)^{\kappa})_{\kappa \in \mathbb{N}}$ is norm-summable and $\mathrm{Inv}\, I + u_1 = \sum((-w)^{\kappa})_{\kappa \in \mathbb{N}}$. □

(14) Let us consider a subset S of the real norm space of bounded linear operators from X into Y. Suppose $S = \{v$, where v is a point of the real norm space of bounded linear operators from X into $Y : v$ is invertible$\}$. Then S is open.

PROOF: Set $P =$ the real norm space of bounded linear operators from X into Y. For every point u of P such that $u \in S$ there exists a real number r such that $r > 0$ and $\mathrm{Ball}(u, r) \subseteq S$ by (12), [4, (17)], (13). □

Let us consider X and Y. The functor InvertOpers(X, Y) yielding an open subset of the real norm space of bounded linear operators from X into Y is defined by the term

(Def. 3) $\{v$, where v is a point of the real norm space of bounded linear operators from X into $Y : v$ is invertible$\}$.

Now we state the propositions:

(15) Let us consider a point u of the real norm space of bounded linear operators from X into Y. Suppose u is invertible. Then

(i) $\operatorname{Inv} u$ is invertible, and

(ii) $\operatorname{Inv} \operatorname{Inv} u = u$.

(16) There exists a function I from $\mathrm{InvertOpers}(X, Y)$ into $\mathrm{InvertOpers}(Y, X)$ such that

(i) I is one-to-one and onto, and

(ii) for every point u of the real norm space of bounded linear operators from X into Y such that $u \in \mathrm{InvertOpers}(X, Y)$ holds $I(u) = \operatorname{Inv} u$.

Proof: Set $S =$ the real norm space of bounded linear operators from X into Y. Define $\mathcal{Q}[\text{object}, \text{object}] \equiv$ there exists a point u of S such that $\$_1 = u$ and $\$_2 = \operatorname{Inv} u$. For every object x such that $x \in \mathrm{InvertOpers}(X, Y)$ there exists an object y such that $y \in \mathrm{InvertOpers}(Y, X)$ and $\mathcal{Q}[x, y]$. Consider I being a function from $\mathrm{InvertOpers}(X, Y)$ into $\mathrm{InvertOpers}(Y, X)$ such that for every object x such that $x \in \mathrm{InvertOpers}(X, Y)$ holds $\mathcal{Q}[x, I(x)]$. For every point u of S such that $u \in \mathrm{InvertOpers}(X, Y)$ holds $I(u) = \operatorname{Inv} u$. If $\mathrm{InvertOpers}(X, Y) \neq \emptyset$, then $\mathrm{InvertOpers}(Y, X) \neq \emptyset$. For every objects x_1, x_2 such that x_1, $x_2 \in \mathrm{InvertOpers}(X, Y)$ and $I(x_1) = I(x_2)$ holds $x_1 = x_2$. □

(17) Let us consider points u, v of the real norm space of bounded linear operators from X into Y. Suppose u is invertible and $\|v - u\| < \frac{1}{\|\operatorname{Inv} u\|}$. Then

(i) v is invertible, and

(ii) $\|\operatorname{Inv} v\| \leqslant \frac{1}{\frac{1}{\|\operatorname{Inv} u\|} - \|v-u\|}$, and

(iii) there exists a point w of $\mathrm{NormedAlgebraOfBoundedLinearOpers}_{\mathbb{R}}(X)$ and there exist points s, I of the real norm space of bounded linear operators from X into X such that $w = (\operatorname{Inv} u) \cdot (v - u)$ and $s = w$ and $I = \mathrm{id}_X$ and $\|s\| < 1$ and $((-w)^{\kappa})_{\kappa \in \mathbb{N}}$ is norm-summable and $I + s$ is invertible and $\|\operatorname{Inv} I + s\| \leqslant \frac{1}{1 - \|s\|}$ and $\operatorname{Inv} I + s = \sum((-w)^{\kappa})_{\kappa \in \mathbb{N}}$ and $\operatorname{Inv} v = (\operatorname{Inv} I + s) \cdot (\operatorname{Inv} u)$.

The theorem is a consequence of (13).

2. Isomorphic Mapping to Inverse Operators

Now we state the propositions:

(18) Let us consider real normed spaces X, Y, Z, a point u of the real norm space of bounded linear operators from X into Y, a point v of the real norm space of bounded linear operators from Y into Z, and a point w of the real norm space of bounded linear operators from X into Z. Suppose $w = v \cdot u$. Then $\|w\| \leqslant \|v\| \cdot \|u\|$.

(19) Let us consider real normed spaces X, Y, Z, points u, v of the real norm space of bounded linear operators from X into Y, and a point w of the real norm space of bounded linear operators from Y into Z. Then

(i) $w \cdot (u - v) = w \cdot u - w \cdot v$, and

(ii) $w \cdot (u + v) = w \cdot u + w \cdot v$.

Proof: For every point x of X, $(w \cdot (u - v))(x) = (w \cdot u)(x) - (w \cdot v)(x)$. For every point x of X, $(w \cdot (u + v))(x) = (w \cdot u)(x) + (w \cdot v)(x)$. □

(20) Let us consider real normed spaces X, Y, Z, a point w of the real norm space of bounded linear operators from X into Y, and points u, v of the real norm space of bounded linear operators from Y into Z. Then

(i) $(u - v) \cdot w = u \cdot w - v \cdot w$, and

(ii) $(u + v) \cdot w = u \cdot w + v \cdot w$.

Proof: For every point x of X, $((u - v) \cdot w)(x) = (u \cdot w)(x) - (v \cdot w)(x)$. For every point x of X, $((u + v) \cdot w)(x) = (u \cdot w)(x) + (v \cdot w)(x)$. □

(21) Let us consider real normed spaces X, Y, and points u, v of the real norm space of bounded linear operators from X into Y. Then $u - (u + v) = -v$.

(22) Let us consider real normed spaces X, Y, and a point u of the real norm space of bounded linear operators from X into Y. Suppose u is invertible. Then

(i) $(\operatorname{Inv} u) \cdot u = \mathrm{id}_X$, and

(ii) $u \cdot (\operatorname{Inv} u) = \mathrm{id}_Y$.

(23) Let us consider a point u of the real norm space of bounded linear operators from X into Y. Suppose u is invertible. Let us consider a real number r. Suppose $0 < r$. Then there exists a real number s such that

(i) $0 < s$, and

(ii) for every point v of the real norm space of bounded linear operators from X into Y such that $\|v - u\| < s$ holds $\|\operatorname{Inv} v - \operatorname{Inv} u\| < r$.

The theorem is a consequence of (12), (17), (20), (18), (22), (19), and (21).

(24) Let us consider a partial function I from the real norm space of bounded linear operators from X into Y to the real norm space of bounded linear operators from Y into X.

Suppose $\operatorname{dom} I = \operatorname{InvertOpers}(X, Y)$ and for every point u of the real norm space of bounded linear operators from X into Y such that $u \in \operatorname{InvertOpers}(X, Y)$ holds $I(u) = \operatorname{Inv} u$. Then I is continuous on $\operatorname{InvertOpers}(X, Y)$. The theorem is a consequence of (23).

(25) There exists a partial function I from the real norm space of bounded linear operators from X into Y to the real norm space of bounded linear operators from Y into X such that

(i) $\operatorname{dom} I = \operatorname{InvertOpers}(X, Y)$, and

(ii) $\operatorname{rng} I = \operatorname{InvertOpers}(Y, X)$, and

(iii) I is one-to-one and continuous on $\operatorname{InvertOpers}(X, Y)$, and

(iv) there exists a partial function J from the real norm space of bounded linear operators from Y into X to the real norm space of bounded linear operators from X into Y such that $J = I^{-1}$ and J is one-to-one and $\operatorname{dom} J = \operatorname{InvertOpers}(Y, X)$ and $\operatorname{rng} J = \operatorname{InvertOpers}(X, Y)$ and J is continuous on $\operatorname{InvertOpers}(Y, X)$, and

(v) for every point u of the real norm space of bounded linear operators from X into Y such that $u \in \operatorname{InvertOpers}(X, Y)$ holds $I(u) = \operatorname{Inv} u$.

Proof: Consider J being a function from $\operatorname{InvertOpers}(X, Y)$ into $\operatorname{InvertOpers}(Y, X)$ such that J is one-to-one and onto and for every point u of the real norm space of bounded linear operators from X into Y such that $u \in \operatorname{InvertOpers}(X, Y)$ holds $J(u) = \operatorname{Inv} u$. If $\operatorname{InvertOpers}(X, Y) \neq \emptyset$, then $\operatorname{InvertOpers}(Y, X) \neq \emptyset$. Reconsider $L = J^{-1}$ as a function from $\operatorname{InvertOpers}(Y, X)$ into $\operatorname{InvertOpers}(X, Y)$. For every point v of the real norm space of bounded linear operators from Y into X such that $v \in \operatorname{InvertOpers}(Y, X)$ holds $L(v) = \operatorname{Inv} v$. □

Let us consider real normed spaces X, Y, Z, a point u of the real norm space of bounded linear operators from X into Y, and a point w of the real norm space of bounded linear operators from Y into Z. Now we state the propositions:

(26) (i) $w \cdot (-u) = -w \cdot u$, and

(ii) $(-w) \cdot u = -w \cdot u$.

Proof: For every point x of X, $(w \cdot (-u))(x) = (-1) \cdot (w \cdot u)(x)$. For every point x of X, $((-w) \cdot u)(x) = (-1) \cdot (w \cdot u)(x)$. □

(27) $(-w) \cdot (-u) = w \cdot u$. The theorem is a consequence of (26).

(28) Let us consider real normed spaces X, Y, Z, a point u of the real norm space of bounded linear operators from X into Y, a point w of the real

norm space of bounded linear operators from Y into Z, and a real number r. Then

(i) $w \cdot (r \cdot u) = (r \cdot w) \cdot u$, and

(ii) $r \cdot w \cdot u = r \cdot w \cdot u$, and

(iii) $(r \cdot w) \cdot u = r \cdot (w \cdot u)$.

PROOF: For every point x of X, $(w \cdot (r \cdot u))(x) = r \cdot (w \cdot u)(x)$. For every point x of X, $(r \cdot w \cdot u)(x) = r \cdot (w \cdot u)(x)$. □

(29) Let us consider real normed spaces X, Y, Z. Then there exists a bilinear operator I from the real norm space of bounded linear operators from X into Y × the real norm space of bounded linear operators from Y into Z into the real norm space of bounded linear operators from X into Z such that

(i) I is continuous on the carrier of (the real norm space of bounded linear operators from X into Y) × (the real norm space of bounded linear operators from Y into Z), and

(ii) for every point u of the real norm space of bounded linear operators from X into Y and for every point v of the real norm space of bounded linear operators from Y into Z, $I(u, v) = v \cdot u$.

PROOF: Set $E =$ the real norm space of bounded linear operators from X into Y. Set $F =$ the real norm space of bounded linear operators from Y into Z. Set $G =$ the real norm space of bounded linear operators from X into Z. Define $\mathcal{Q}[\text{object}, \text{object}] \equiv$ there exists a point u of E and there exists a point v of F such that $\$_1 = \langle u, v\rangle$ and $\$_2 = v \cdot u$. For every object x such that $x \in$ the carrier of $E \times F$ there exists an object y such that $y \in$ the carrier of G and $\mathcal{Q}[x, y]$ by [5, (18)]. Consider L being a function from the carrier of $E \times F$ into the carrier of G such that for every object x such that $x \in$ the carrier of $E \times F$ holds $\mathcal{Q}[x, L(x)]$.

For every point u of the real norm space of bounded linear operators from X into Y and for every point v of the real norm space of bounded linear operators from Y into Z, $L(u, v) = v \cdot u$. For every points x_1, x_2 of E and for every point y of F, $L(x_1 + x_2, y) = L(x_1, y) + L(x_2, y)$. For every point x of E and for every point y of F and for every real number a, $L(a \cdot x, y) = a \cdot L(x, y)$. For every point x of E and for every points y_1, y_2 of F, $L(x, y_1 + y_2) = L(x, y_1) + L(x, y_2)$. For every point x of E and for every point y of F and for every real number a, $L(x, a \cdot y) = a \cdot L(x, y)$. Set $K = 1$. For every point x of E and for every point y of F, $\|L(x, y)\| \leqslant K \cdot \|x\| \cdot \|y\|$. □

Let us consider real normed spaces X, Y, a Lipschitzian linear operator v from X into Y, a point w of the real norm space of bounded linear operators from X into Y, and a real number a. Now we state the propositions:

(30) If $v = w$, then $a \cdot w = a \cdot v$.

Proof: For every object s such that $s \in \mathrm{dom}(a \cdot v)$ holds $(a \cdot v)(s) = (a \cdot w)(s)$ by [8, (36)]. □

(31) If $v = w$, then $-w = -v$. The theorem is a consequence of (30).

Acknowledgement: I would like to express my gratitude to Professor Yasunari Shidama for his helpful advice.

References

[1] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pąk. The role of the Mizar Mathematical Library for interactive proof development in Mizar. *Journal of Automated Reasoning*, 61(1):9–32, 2018. doi:10.1007/s10817-017-9440-6.

[2] Adam Grabowski, Artur Korniłowicz, and Adam Naumowicz. Four decades of Mizar. *Journal of Automated Reasoning*, 55(3):191–198, 2015. doi:10.1007/s10817-015-9345-1.

[3] Miyadera Isao. *Functional Analysis.* Riko-Gaku-Sya, 1972.

[4] Kazuhisa Nakasho, Yuichi Futa, and Yasunari Shidama. Implicit function theorem. Part I. *Formalized Mathematics*, 25(**4**):269–281, 2017. doi:10.1515/forma-2017-0026.

[5] Hiroyuki Okazaki, Noboru Endou, and Yasunari Shidama. Cartesian products of family of real linear spaces. *Formalized Mathematics*, 19(**1**):51–59, 2011. doi:10.2478/v10037-011-0009-2.

[6] Laurent Schwartz. *Théorie des ensembles et topologie, tome 1. Analyse.* Hermann, 1997.

[7] Laurent Schwartz. *Calcul différentiel, tome 2. Analyse.* Hermann, 1997.

[8] Yasunari Shidama. Banach space of bounded linear operators. *Formalized Mathematics*, 12(**1**):39–48, 2004.

[9] Yasunari Shidama. The Banach algebra of bounded linear operators. *Formalized Mathematics*, 12(**2**):103–108, 2004.

[10] Kosaku Yoshida. *Functional Analysis.* Springer, 1980.

Accepted May 27, 2019

FORMALIZED MATHEMATICS
Vol. 27, No. 2, Pages 117–131, 2019
DOI: 10.2478/forma-2019-0013

https://www.sciendo.com/

Implicit Function Theorem. Part II

Kazuhisa Nakasho
Yamaguchi University
Yamaguchi, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. In this article, we formalize differentiability of implicit function theorem in the Mizar system [3], [1]. In the first half section, properties of Lipschitz continuous linear operators are discussed. Some norm properties of a direct sum decomposition of Lipschitz continuous linear operator are mentioned here.

In the last half section, differentiability of implicit function in implicit function theorem is formalized. The existence and uniqueness of implicit function in [6] is cited. We referred to [10], [11], and [2] in the formalization.

MSC: 26B10 47A05 47J07 53A07 03B35

Keywords: implicit function theorem; Lipschitz continuity; differentiability; implicit function

MML identifier: NDIFF_9, version: 8.1.09 5.57.1355

1. Properties of Lipschitz Continuous Linear Operators

From now on S, T, W, Y denote real normed spaces, f, f_1, f_2 denote partial functions from S to T, Z denotes a subset of S, and i, n denote natural numbers.

Now we state the propositions:

(1) Let us consider real normed spaces E, F, a partial function f from E to F, a subset Z of E, and a point z of E. Suppose Z is open and $z \in Z$ and $Z \subseteq \operatorname{dom} f$ and f is differentiable in z. Then

(i) $f \restriction Z$ is differentiable in z, and

(ii) $f'(z) = (f \restriction Z)'(z)$.

PROOF: Consider N being a neighbourhood of z such that $N \subseteq \mathrm{dom}\, f$ and there exists a rest R of E, F such that for every point x of E such that $x \in N$ holds $f_{/x} - f_{/z} = (f'(z))(x - z) + R_{/x-z}$. Consider r being a real number such that $r > 0$ and $\mathrm{Ball}(z, r) \subseteq Z$. Reconsider $N_4 = N \cap Z$ as a neighbourhood of z. Consider R being a rest of E, F such that for every point x of E such that $x \in N$ holds $f_{/x} - f_{/z} = (f'(z))(x - z) + R_{/x-z}$. For every point x of E such that $x \in N_4$ holds $(f\restriction Z)_{/x} - (f\restriction Z)_{/z} = (f'(z))(x - z) + R_{/x-z}$. □

(2) Let us consider real normed spaces E, F, G, a partial function f from $E \times F$ to G, a subset Z of $E \times F$, and a point z of $E \times F$. Suppose Z is open and $z \in Z$ and $Z \subseteq \mathrm{dom}\, f$. Then

(i) if f is partially differentiable in z w.r.t. 1, then $f\restriction Z$ is partially differentiable in z w.r.t. 1 and $\mathrm{partdiff}(f, z)\,\text{w.r.t.}\,1 =$ $\mathrm{partdiff}(f\restriction Z, z)\,\text{w.r.t.}\,1$, and

(ii) if f is partially differentiable in z w.r.t. 2, then $f\restriction Z$ is partially differentiable in z w.r.t. 2 and $\mathrm{partdiff}(f, z)\,\text{w.r.t.}\,2 =$ $\mathrm{partdiff}(f\restriction Z, z)\,\text{w.r.t.}\,2$.

PROOF: If f is partially differentiable in z w.r.t. 1, then $f\restriction Z$ is partially differentiable in z w.r.t. 1 and $\mathrm{partdiff}(f, z)\,\text{w.r.t.}\,1 = \mathrm{partdiff}(f\restriction Z, z)\,\text{w.r.t.}\,1$. Set $g = f \cdot (\mathrm{reproj2}(z))$. Consider N being a neighbourhood of $(z)_{\mathbf{2}}$ such that $N \subseteq \mathrm{dom}\, g$ and there exists a rest R of F, G such that for every point x of F such that $x \in N$ holds $g_{/x} - g_{/(z)_{\mathbf{2}}} = (\mathrm{partdiff}(f, z)\,\text{w.r.t.}\,2)(x - (z)_{\mathbf{2}}) + R_{/x-(z)_{\mathbf{2}}}$. Consider R being a rest of F, G such that for every point x of F such that $x \in N$ holds $g_{/x} - g_{/(z)_{\mathbf{2}}} = (\mathrm{partdiff}(f, z)\,\text{w.r.t.}\,2)(x - (z)_{\mathbf{2}}) + R_{/x-(z)_{\mathbf{2}}}$.

Set $h = (f\restriction Z) \cdot (\mathrm{reproj2}(z))$. Consider r_1 being a real number such that $r_1 > 0$ and $\mathrm{Ball}(z, r_1) \subseteq Z$. Consider r_2 being a real number such that $r_2 > 0$ and $\{y$, where y is a point of $F : \|y - (z)_{\mathbf{2}}\| < r_2\} \subseteq N$. Set $r = \min(r_1, r_2)$. Set $M = \mathrm{Ball}((z)_{\mathbf{2}}, r)$. $M \subseteq N$ and for every point x of F such that $x \in M$ holds $(\mathrm{reproj2}(z))(x) \in Z$. $M \subseteq \mathrm{dom}\, h$. For every point x of F such that $x \in M$ holds $h_{/x} - h_{/(z)_{\mathbf{2}}} = (\mathrm{partdiff}(f, z)\,\text{w.r.t.}\,2)(x - (z)_{\mathbf{2}}) + R_{/x-(z)_{\mathbf{2}}}$. □

(3) Let us consider real normed spaces X, E, G, F, a bilinear operator B from $E \times F$ into G, a partial function f from X to E, a partial function g from X to F, and a subset S of X. Suppose B is continuous on the carrier of $E \times F$ and $S \subseteq \mathrm{dom}\, f$ and $S \subseteq \mathrm{dom}\, g$ and for every point s of X such that $s \in S$ holds f is continuous in s and for every point s of X such that $s \in S$ holds g is continuous in s. Then there exists a partial function H from X to G such that

(i) $\operatorname{dom} H = S$, and

(ii) for every point s of X such that $s \in S$ holds $H(s) = B(f(s), g(s))$, and

(iii) H is continuous on S.

Proof: Define $\mathcal{P}[\text{object}, \text{object}] \equiv$ there exists a point t of X such that $t = \$_1$ and $\$_2 = B(f(t), g(t))$. For every object x such that $x \in S$ there exists an object y such that $y \in$ the carrier of G and $\mathcal{P}[x, y]$. Consider H being a function from S into G such that for every object z such that $z \in S$ holds $\mathcal{P}[z, H(z)]$. For every point s of X such that $s \in S$ holds $H(s) = B(f(s), g(s))$. For every point x_0 of X and for every real number r such that $x_0 \in S$ and $0 < r$ there exists a real number p_2 such that $0 < p_2$ and for every point x_1 of X such that $x_1 \in S$ and $\|x_1 - x_0\| < p_2$ holds $\|H_{/x_1} - H_{/x_0}\| < r$. □

(4) Let us consider real normed spaces E, F, a partial function g from E to F, and a subset A of E. Suppose g is continuous on A and $\operatorname{dom} g = A$. Then there exists a partial function x_2 from E to $E \times F$ such that

(i) $\operatorname{dom} x_2 = A$, and

(ii) for every point x of E such that $x \in A$ holds $x_2(x) = \langle x, g(x) \rangle$, and

(iii) x_2 is continuous on A.

Proof: Define $\mathcal{P}[\text{object}, \text{object}] \equiv$ there exists a point t of E such that $t = \$_1$ and $\$_2 = \langle t, g(t) \rangle$. For every object x such that $x \in S$ there exists an object y such that $y \in$ the carrier of $E \times F$ and $\mathcal{P}[x, y]$. Consider H being a function from S into $E \times F$ such that for every object z such that $z \in S$ holds $\mathcal{P}[z, H(z)]$. For every point s of E such that $s \in S$ holds $H(s) = \langle s, g(s) \rangle$. For every point x_0 of E and for every real number r such that $x_0 \in S$ and $0 < r$ there exists a real number p_2 such that $0 < p_2$ and for every point x_1 of E such that $x_1 \in S$ and $\|x_1 - x_0\| < p_2$ holds $\|H_{/x_1} - H_{/x_0}\| < r$. □

(5) Let us consider real normed spaces S, T, V, a point x_0 of V, a partial function f_1 from the carrier of V to the carrier of S, and a partial function f_2 from the carrier of S to the carrier of T. Suppose $x_0 \in \operatorname{dom}(f_2 \cdot f_1)$ and f_1 is continuous in x_0 and f_2 is continuous in f_{1/x_0}. Then $f_2 \cdot f_1$ is continuous in x_0.

Proof: $\operatorname{rng}(f_{1*}s_1) \subseteq \operatorname{dom} f_2$. □

(6) Let us consider real normed spaces E, F, a point z of $E \times F$, a point x of E, and a point y of F. Suppose $z = \langle x, y \rangle$. Then $\|z\| \leqslant \|x\| + \|y\|$.

(7) Let us consider real normed spaces E, F, G, and a linear operator L from $E \times F$ into G. Then there exists a linear operator L_1 from E into G

and there exists a linear operator L_2 from F into G such that for every point x of E and for every point y of F, $L(\langle x, y\rangle) = L_1(x) + L_2(y)$ and for every point x of E, $L_1(x) = L_{/\langle x, 0_F\rangle}$ and for every point y of F, $L_2(y) = L_{/\langle 0_E, y\rangle}$.

Proof: Define $\mathcal{C}(\text{point of } E) = L_{/\langle \$_1, 0_F\rangle}$. Consider L_1 being a function from the carrier of E into the carrier of G such that for every point x of E, $L_1(x) = \mathcal{C}(x)$. For every elements s, t of E, $L_1(s+t) = L_1(s) + L_1(t)$. For every element s of E and for every real number r, $L_1(r \cdot s) = r \cdot L_1(s)$. Define $\mathcal{D}(\text{point of } F) = L_{/\langle 0_E, \$_1\rangle}$. Consider L_2 being a function from the carrier of F into the carrier of G such that for every point x of F, $L_2(x) = \mathcal{D}(x)$. For every elements s, t of F, $L_2(s+t) = L_2(s) + L_2(t)$. For every element s of F and for every real number r, $L_2(r \cdot s) = r \cdot L_2(s)$. For every point x of E and for every point y of F, $L(\langle x, y\rangle) = L_1(x) + L_2(y)$. □

(8) Let us consider real normed spaces E, F, G, a linear operator L from $E \times F$ into G, a linear operator L_{11} from E into G, a linear operator L_{12} from F into G, a linear operator L_{21} from E into G, and a linear operator L_{22} from F into G. Suppose for every point x of E and for every point y of F, $L(\langle x, y\rangle) = L_{11}(x) + L_{12}(y)$ and for every point x of E and for every point y of F, $L(\langle x, y\rangle) = L_{21}(x) + L_{22}(y)$. Then

(i) $L_{11} = L_{21}$, and

(ii) $L_{12} = L_{22}$.

(9) Let us consider real normed spaces E, F, G, a linear operator L_1 from E into G, and a linear operator L_2 from F into G. Then there exists a linear operator L from $E \times F$ into G such that

(i) for every point x of E and for every point y of F, $L(\langle x, y\rangle) = L_1(x) + L_2(y)$, and

(ii) for every point x of E, $L_1(x) = L_{/\langle x, 0_F\rangle}$, and

(iii) for every point y of F, $L_2(y) = L_{/\langle 0_E, y\rangle}$.

Proof: Define $\mathcal{P}[\text{object}, \text{object}] \equiv$ there exists a point x of E and there exists a point y of F such that $\$_1 = \langle x, y\rangle$ and $\$_2 = L_1(x) + L_2(y)$. For every element z of $E \times F$, there exists an element y of G such that $\mathcal{P}[z, y]$. Consider L being a function from $E \times F$ into G such that for every element z of $E \times F$, $\mathcal{P}[z, L(z)]$. For every points z, w of $E \times F$, $L(z + w) = L(z) + L(w)$. For every element z of $E \times F$ and for every real number r, $L(r \cdot z) = r \cdot L(z)$. For every point x of E and for every point y

of F, $L(\langle x, y\rangle) = L_1(x)+L_2(y)$. For every point x of E, $L_1(x) = L_{/\langle x, 0_F\rangle}$. For every point y of F, $L_2(y) = L_{/\langle 0_E, y\rangle}$ by [9, (3)]. □

(10) Let us consider real normed spaces E, F, G, and a Lipschitzian linear operator L from $E \times F$ into G. Then there exists a Lipschitzian linear operator L_1 from E into G and there exists a Lipschitzian linear operator L_2 from F into G such that for every point x of E and for every point y of F, $L(\langle x, y\rangle) = L_1(x)+L_2(y)$ and for every point x of E, $L_1(x) = L_{/\langle x, 0_F\rangle}$ and for every point y of F, $L_2(y) = L_{/\langle 0_E, y\rangle}$. The theorem is a consequence of (7).

(11) Let us consider real normed spaces E, F, G, a Lipschitzian linear operator L_1 from E into G, and a Lipschitzian linear operator L_2 from F into G. Then there exists a Lipschitzian linear operator L from $E \times F$ into G such that

(i) for every point x of E and for every point y of F, $L(\langle x, y\rangle) = L_1(x)+L_2(y)$, and

(ii) for every point x of E, $L_1(x) = L_{/\langle x, 0_F\rangle}$, and

(iii) for every point y of F, $L_2(y) = L_{/\langle 0_E, y\rangle}$.

The theorem is a consequence of (9).

(12) Let us consider real normed spaces E, F, G, and a point L of the real norm space of bounded linear operators from $E \times F$ into G. Then there exists a point L_1 of the real norm space of bounded linear operators from E into G and there exists a point L_2 of the real norm space of bounded linear operators from F into G such that for every point x of E and for every point y of F, $L(\langle x, y\rangle) = L_1(x) + L_2(y)$ and for every point x of E, $L_1(x) = L(\langle x, 0_F\rangle)$ and for every point y of F, $L_2(y) = L(\langle 0_E, y\rangle)$ and $\|L\| \leqslant \|L_1\| + \|L_2\|$ and $\|L_1\| \leqslant \|L\|$ and $\|L_2\| \leqslant \|L\|$.

Proof: Reconsider $L = L_4$ as a Lipschitzian linear operator from $E \times F$ into G. Consider L_1 being a Lipschitzian linear operator from E into G, L_2 being a Lipschitzian linear operator from F into G such that for every point x of E and for every point y of F, $L(\langle x, y\rangle) = L_1(x) + L_2(y)$ and for every point x of E, $L_1(x) = L_{/\langle x, 0_F\rangle}$ and for every point y of F, $L_2(y) = L_{/\langle 0_E, y\rangle}$.

Reconsider $L_5 = L_1$ as a point of the real norm space of bounded linear operators from E into G. Reconsider $L_3 = L_2$ as a point of the real norm space of bounded linear operators from F into G. For every point x of E, $L_5(x) = L_4(\langle x, 0_F\rangle)$. For every point y of F, $L_3(y) = L_4(\langle 0_E, y\rangle)$. For every real number t such that $t \in \mathrm{PreNorms}(L)$ holds $t \leqslant \|L_5\|+\|L_3\|$.

For every real number t such that $t \in \mathrm{PreNorms}(L_1)$ holds $t \leqslant \|L_4\|$. For every real number t such that $t \in \mathrm{PreNorms}(L_2)$ holds $t \leqslant \|L_4\|$. □

(13) Let us consider real normed spaces E, F, G, a point L of the real norm space of bounded linear operators from $E \times F$ into G, points L_{11}, L_{12} of the real norm space of bounded linear operators from E into G, and points L_{21}, L_{22} of the real norm space of bounded linear operators from F into G. Suppose for every point x of E and for every point y of F, $L(\langle x, y\rangle) = L_{11}(x) + L_{21}(y)$ and for every point x of E and for every point y of F, $L(\langle x, y\rangle) = L_{12}(x) + L_{22}(y)$. Then

(i) $L_{11} = L_{12}$, and

(ii) $L_{21} = L_{22}$.

The theorem is a consequence of (8).

2. Differentiability of Implicit Function

Now we state the propositions:

(14) Let us consider real normed spaces E, G, F, a subset Z of $E \times F$, a partial function f from $E \times F$ to G, and a point z of $E \times F$. Suppose f is differentiable in z. Then

(i) f is partially differentiable in z w.r.t. 1, and

(ii) f is partially differentiable in z w.r.t. 2, and

(iii) for every point d_7 of E and for every point d_8 of F, $(f'(z))(\langle d_7, d_8\rangle) = (\mathrm{partdiff}(f, z)\,\mathrm{w.r.t.}\,1)(d_7) + (\mathrm{partdiff}(f, z)\,\mathrm{w.r.t.}\,2)(d_8)$.

Proof: Reconsider $y = (\mathrm{IsoCPNrSP}(E, F))(z)$ as a point of $\prod\langle E, F\rangle$. Consider N being a neighbourhood of z such that $N \subseteq \operatorname{dom} f$ and there exists a rest R of $E \times F$, G such that for every point w of $E \times F$ such that $w \in N$ holds $f_{/w} - f_{/z} = (f'(z))(w - z) + R_{/w-z}$. Consider R being a rest of $E \times F$, G such that for every point w of $E \times F$ such that $w \in N$ holds $f_{/w} - f_{/z} = (f'(z))(w - z) + R_{/w-z}$. Reconsider $L = f'(z)$ as a Lipschitzian linear operator from $E \times F$ into G. Consider L_1 being a Lipschitzian linear operator from E into G, L_2 being a Lipschitzian linear operator from F into G such that for every point d_7 of E and for every point d_8 of F, $L(\langle d_7, d_8\rangle) = L_1(d_7) + L_2(d_8)$ and for every point d_7 of E, $L_1(d_7) = L_{/\langle d_7, 0_F\rangle}$ and for every point d_8 of F, $L_2(d_8) = L_{/\langle 0_E, d_8\rangle}$.

Reconsider $L_3 = L_1$ as a point of the real norm space of bounded linear operators from E into G. Reconsider $L_4 = L_2$ as a point of the real norm space of bounded linear operators from F into G. Set $g_1 = f \cdot (\mathrm{reproj1}(z))$.

Set $g_2 = f \cdot (\text{reproj2}(z))$. Reconsider $x = (z)_{\mathbf{1}}$ as a point of E. Reconsider $y = (z)_{\mathbf{2}}$ as a point of F. Consider r_0 being a real number such that $0 < r_0$ and $\{y$, where y is a point of $E \times F : \|y - z\| < r_0\} \subseteq N$. Consider r being a real number such that $0 < r < r_0$ and $\text{Ball}(x, r) \times \text{Ball}(y, r) \subseteq \text{Ball}(z, r_0)$. Define $\mathcal{C}(\text{point of } E) = R_{/\langle \$_1, 0_F \rangle}$. Consider R_1 being a function from the carrier of E into the carrier of G such that for every point p of E, $R_1(p) = \mathcal{C}(p)$. Define $\mathcal{D}(\text{point of } F) = R_{/\langle 0_E, \$_1 \rangle}$. Consider R_2 being a function from the carrier of F into the carrier of G such that for every point p of F, $R_2(p) = \mathcal{D}(p)$.

For every real number r such that $r > 0$ there exists a real number d such that $d > 0$ and for every point z of E such that $z \neq 0_E$ and $\|z\| < d$ holds $\|z\|^{-1} \cdot \|R_{1/z}\| < r$. For every real number r such that $r > 0$ there exists a real number d such that $d > 0$ and for every point z of F such that $z \neq 0_F$ and $\|z\| < d$ holds $\|z\|^{-1} \cdot \|R_{2/z}\| < r$. Reconsider $N_1 = \text{Ball}(x, r)$ as a neighbourhood of x. Reconsider $N_2 = \text{Ball}(y, r)$ as a neighbourhood of y. $N_1 \subseteq \operatorname{dom} g_1$. $N_2 \subseteq \operatorname{dom} g_2$. For every point x_1 of E such that $x_1 \in N_1$ holds $g_{1/x_1} - g_{1/x} = L_3(x_1 - x) + R_{1/x_1 - x}$. For every point y_1 of F such that $y_1 \in N_2$ holds $g_{2/y_1} - g_{2/y} = L_4(y_1 - y) + R_{2/y_1 - y}$. □

(15) Let us consider real normed spaces E, G, F, a subset Z of $E \times F$, a partial function f from $E \times F$ to G, a point a of E, a point b of F, a point c of G, a point z of $E \times F$, real numbers r_1, r_2, a partial function g from E to F, a Lipschitzian linear operator P from E into G, and a Lipschitzian linear operator Q from G into F.

Suppose Z is open and $\operatorname{dom} f = Z$ and $z = \langle a, b \rangle$ and $z \in Z$ and $f(a, b) = c$ and f is differentiable in z and $0 < r_1$ and $0 < r_2$ and $\operatorname{dom} g = \text{Ball}(a, r_1)$ and $\operatorname{rng} g \subseteq \text{Ball}(b, r_2)$ and $g(a) = b$ and g is continuous in a and for every point x of E such that $x \in \text{Ball}(a, r_1)$ holds $f(x, g(x)) = c$ and $\text{partdiff}(f, z)$ w.r.t. 2 is one-to-one and $Q = (\text{partdiff}(f, z) \text{ w.r.t. } 2)^{-1}$ and $P = \text{partdiff}(f, z)$ w.r.t. 1. Then

(i) g is differentiable in a, and

(ii) $g'(a) = -Q \cdot P$.

Proof: Reconsider $L = Q \cdot P$ as a point of the real norm space of bounded linear operators from E into F. Consider N_0 being a neighbourhood of z such that $N_0 \subseteq \operatorname{dom} f$ and there exists a rest R of $E \times F$, G such that for every point w of $E \times F$ such that $w \in N_0$ holds $f_{/w} - f_{/z} = (f'(z))(w - z) + R_{/w - z}$. Consider R being a rest of $E \times F$, G such that for every point w of $E \times F$ such that $w \in N_0$ holds $f_{/w} - f_{/z} = (f'(z))(w - z) + R_{/w - z}$. Consider r_0 being a real number such that $0 < r_0$ and $\{y$, where y is a point of $E \times F : \|y - z\| < r_0\} \subseteq N_0$. Consider r_3 being a real number such that $0 < r_3 < r_0$ and $\mathrm{Ball}(a, r_3) \times \mathrm{Ball}(b, r_3) \subseteq \mathrm{Ball}(z, r_0)$. Reconsider $r_4 = \min(r_1, r_3)$ as a real number.

Consider r_5 being a real number such that $0 < r_5$ and for every point x_1 of E such that $x_1 \in \mathrm{dom}\, g$ and $\|x_1 - a\| < r_5$ holds $\|g_{/x_1} - g_{/a}\| < r_3$. Reconsider $r_6 = \min(r_4, r_5)$ as a real number. Reconsider $N = \mathrm{Ball}(a, r_6)$ as a neighbourhood of a. Define $\mathcal{C}(\text{point of } E) = -Q(R_{/\langle \$_1, g_{/a+\$_1} - g_{/a} \rangle})$. Consider R_1 being a function from the carrier of E into the carrier of F such that for every point p of E, $R_1(p) = \mathcal{C}(p)$. For every point x of E such that $x \in N$ holds $g_{/x} - g_{/a} = (-L)(x - a) + R_{1/x-a}$. Define $\mathcal{D}[\text{point of } E, \text{object}] \equiv \$_2 = \langle \$_1,\, g_{/a+\$_1} - g_{/a} \rangle$. For every element d_7 of the carrier of E, there exists an element d_8 of the carrier of $E \times F$ such that $\mathcal{D}[d_7, d_8]$.

Consider V being a function from the carrier of E into the carrier of $E \times F$ such that for every element d_7 of the carrier of E, $\mathcal{D}[d_7, V(d_7)]$. Reconsider $Q_1 = Q$ as a point of the real norm space of bounded linear operators from G into F. Set $Q_2 = \|Q_1\|$. Consider d_0 being a real number such that $d_0 > 0$ and for every point d_9 of $E \times F$ such that $d_9 \neq 0_{E \times F}$ and $\|d_9\| < d_0$ holds $\|d_9\|^{-1} \cdot \|R_{/d_9}\| < \frac{1}{2 \cdot (Q_2 + 1)}$. Consider d_1 being a real number such that $0 < d_1 < d_0$ and $\mathrm{Ball}(a, d_1) \times \mathrm{Ball}(g_{/a}, d_1) \subseteq \mathrm{Ball}(z, d_0)$. Consider d_2 being a real number such that $0 < d_2$ and for every point x_1 of E such that $x_1 \in \mathrm{dom}\, g$ and $\|x_1 - a\| < d_2$ holds $\|g_{/x_1} - g_{/a}\| < d_1$. Reconsider $d_3 = \min(d_1, d_2)$ as a real number. Reconsider $d_4 = \min(d_3, r_1)$ as a real number.

For every point d_7 of E such that $d_7 \neq 0_E$ and $\|d_7\| < d_4$ holds $\|R_{/V(d_7)}\| \leqslant \frac{1}{2 \cdot (Q_2 + 1)} \cdot (\|d_7\| + \|g_{/a+d_7} - g_{/a}\|)$. For every point d_7 of E such that $d_7 \neq 0_E$ and $\|d_7\| < d_4$ holds $\|R_{1/d_7}\| \leqslant \frac{1}{2} \cdot (\|d_7\| + \|g_{/a+d_7} - g_{/a}\|)$. Set $Q_3 = \|L\|$. Reconsider $d_5 = \min(r_6, d_4)$ as a real number. For every point d_7 of E such that $d_7 \neq 0_E$ and $\|d_7\| < d_5$ holds $\|g_{/a+d_7} - g_{/a}\| \leqslant (2 \cdot Q_3 + 1) \cdot \|d_7\|$. For every real number r such that $r > 0$ there exists a real number d such that $d > 0$ and for every point d_7 of E such that $d_7 \neq 0_E$ and $\|d_7\| < d$ holds $\|d_7\|^{-1} \cdot \|R_{1/d_7}\| < r$ by [4, (23)], [7, (7)], [8, (18)]. □

From now on X, Y, Z denote non trivial real Banach spaces.

Now we state the propositions:

(16) Let us consider a point u of the real norm space of bounded linear operators from X into Y. Suppose u is invertible. Then there exist real numbers K, s such that

(i) $0 \leqslant K$, and

(ii) $0 < s$, and

(iii) for every point d_6 of the real norm space of bounded linear operators from X into Y such that $\|d_6\| < s$ holds $u + d_6$ is invertible and $\|\mathrm{Inv}\, u + d_6 - \mathrm{Inv}\, u - -(\mathrm{Inv}\, u) \cdot d_6 \cdot (\mathrm{Inv}\, u)\| \leqslant K \cdot (\|d_6\| \cdot \|d_6\|)$.

(17) Let us consider a partial function I from the real norm space of bounded linear operators from X into Y to the real norm space of bounded linear operators from Y into X. Suppose $\mathrm{dom}\, I = \mathrm{InvertOpers}(X, Y)$ and for every point u of the real norm space of bounded linear operators from X into Y such that $u \in \mathrm{InvertOpers}(X, Y)$ holds $I(u) = \mathrm{Inv}\, u$. Let us consider a point u of the real norm space of bounded linear operators from X into Y. Suppose $u \in \mathrm{InvertOpers}(X, Y)$. Then

(i) I is differentiable in u, and

(ii) for every point d_6 of the real norm space of bounded linear operators from X into Y, $(I'(u))(d_6) = -(\mathrm{Inv}\, u) \cdot d_6 \cdot (\mathrm{Inv}\, u)$.

Proof: Set $S =$ the real norm space of bounded linear operators from X into Y. Set $W =$ the real norm space of bounded linear operators from Y into X. Set $N = \mathrm{InvertOpers}(X, Y)$. Define $\mathcal{C}(\text{point of } S) = -(\mathrm{Inv}\, u) \cdot \$_1 \cdot (\mathrm{Inv}\, u)$. Consider L being a function from the carrier of S into the carrier of W such that for every point x of S, $L(x) = \mathcal{C}(x)$. For every elements s, t of S, $L(s + t) = L(s) + L(t)$. For every element s of S and for every real number r, $L(r \cdot s) = r \cdot L(s)$. Define $\mathcal{D}(\text{point of } S) = \mathrm{Inv}\, u + \$_1 - \mathrm{Inv}\, u - L(\$_1)$.

Consider R being a function from the carrier of S into the carrier of W such that for every point x of S, $R(x) = \mathcal{D}(x)$. For every point x of S, $R(x) = \mathrm{Inv}\, u + x - \mathrm{Inv}\, u - -(\mathrm{Inv}\, u) \cdot x \cdot (\mathrm{Inv}\, u)$. Reconsider $L_0 = L$ as a point of the real norm space of bounded linear operators from S into W. For every real number r such that $r > 0$ there exists a real number d such that $d > 0$ and for every point z of S such that $z \neq 0_S$ and $\|z\| < d$ holds $\|z\|^{-1} \cdot \|R_{/z}\| < r$. Reconsider $R_0 = R$ as a rest of S, W. For every point v of S such that $v \in N$ holds $I_{/v} - I_{/u} = L_0(v - u) + R_{0/v-u}$. □

(18) There exists a partial function I from the real norm space of bounded linear operators from X into Y to the real norm space of bounded linear operators from Y into X such that

(i) $\mathrm{dom}\, I = \mathrm{InvertOpers}(X, Y)$, and

(ii) $\mathrm{rng}\, I = \mathrm{InvertOpers}(Y, X)$, and

(iii) I is one-to-one and differentiable on $\mathrm{InvertOpers}(X, Y)$, and

(iv) there exists a partial function J from the real norm space of bounded linear operators from Y into X to the real norm space of bounded linear operators from X into Y such that $J = I^{-1}$ and J is one-to-one and $\operatorname{dom} J = \text{InvertOpers}(Y, X)$ and $\operatorname{rng} J = \text{InvertOpers}(X, Y)$ and J is differentiable on $\text{InvertOpers}(Y, X)$, and

(v) for every point u of the real norm space of bounded linear operators from X into Y such that $u \in \text{InvertOpers}(X, Y)$ holds $I(u) = \operatorname{Inv} u$, and

(vi) for every points u, d_6 of the real norm space of bounded linear operators from X into Y such that $u \in \text{InvertOpers}(X, Y)$ holds $(I'(u))(d_6) = -(\operatorname{Inv} u) \cdot d_6 \cdot (\operatorname{Inv} u)$.

Proof: Consider I being a partial function from the real norm space of bounded linear operators from X into Y to the real norm space of bounded linear operators from Y into X such that $\operatorname{dom} I = \text{InvertOpers}(X, Y)$ and $\operatorname{rng} I = \text{InvertOpers}(Y, X)$ and I is one-to-one and continuous on $\text{InvertOpers}(X, Y)$ and there exists a partial function J from the real norm space of bounded linear operators from Y into X to the real norm space of bounded linear operators from X into Y such that $J = I^{-1}$ and J is one-to-one and $\operatorname{dom} J = \text{InvertOpers}(Y, X)$ and $\operatorname{rng} J = \text{InvertOpers}(X, Y)$ and J is continuous on $\text{InvertOpers}(Y, X)$ and for every point u of the real norm space of bounded linear operators from X into Y such that $u \in \text{InvertOpers}(X, Y)$ holds $I(u) = \operatorname{Inv} u$.

Consider J being a partial function from the real norm space of bounded linear operators from Y into X to the real norm space of bounded linear operators from X into Y such that $J = I^{-1}$ and J is one-to-one and $\operatorname{dom} J = \text{InvertOpers}(Y, X)$ and $\operatorname{rng} J = \text{InvertOpers}(X, Y)$ and J is continuous on $\text{InvertOpers}(Y, X)$. For every point u of the real norm space of bounded linear operators from X into Y such that $u \in \text{InvertOpers}(X, Y)$ holds I is differentiable in u. For every point v of the real norm space of bounded linear operators from Y into X such that $v \in \text{InvertOpers}(Y, X)$ holds $J(v) = \operatorname{Inv} v$ by [5, (15)]. For every point v of the real norm space of bounded linear operators from Y into X such that $v \in \text{InvertOpers}(Y, X)$ holds J is differentiable in v. □

(19) Let us consider real normed spaces E, G, F, a subset Z of $E \times F$, a partial function f from $E \times F$ to G, a point a of E, a point b of F, a point c of G, a point z of $E \times F$, a subset A of E, a subset B of F, and a partial function g from E to F. Suppose Z is open and $\operatorname{dom} f = Z$ and A is open and B is open and $A \times B \subseteq Z$ and $z = \langle a, b \rangle$ and $f(a, b) = c$ and f is differentiable in z and $\operatorname{dom} g = A$ and $\operatorname{rng} g \subseteq B$ and $a \in A$ and $g(a) = b$ and g is continuous in a and for every point x of E such that $x \in A$ holds $f(x, g(x)) = c$ and $\operatorname{partdiff}(f, z)$ w.r.t. 2 is invertible. Then

(i) g is differentiable in a, and

(ii) $g'(a) = -(\mathrm{Inv\,partdiff}(f,z)\text{ w.r.t. }2) \cdot (\mathrm{partdiff}(f,z)\text{ w.r.t. }1)$.

Proof: Consider r_2 being a real number such that $0 < r_2$ and $\mathrm{Ball}(b, r_2) \subseteq B$. Consider r_3 being a real number such that $0 < r_3$ and for every point x_1 of E such that $x_1 \in \mathrm{dom}\, g$ and $\|x_1 - a\| < r_3$ holds $\|g_{/x_1} - g_{/a}\| < r_2$. Consider r_4 being a real number such that $0 < r_4$ and $\mathrm{Ball}(a, r_4) \subseteq A$. Set $r_1 = \min(r_3, r_4)$. Set $g_1 = g \restriction \mathrm{Ball}(a, r_1)$. For every real number r such that $0 < r$ there exists a real number s such that $0 < s$ and for every point x_1 of E such that $x_1 \in \mathrm{dom}\, g_1$ and $\|x_1 - a\| < s$ holds $\|{g_1}_{/x_1} - {g_1}_{/a}\| < r$. For every point x of E such that $x \in \mathrm{Ball}(a, r_1)$ holds $f(x, g_1(x)) = c$.

Reconsider $Q = (\mathrm{partdiff}(f,z)\text{ w.r.t. }2)^{-1}$ as a Lipschitzian linear operator from G into F. Reconsider $P = \mathrm{partdiff}(f,z)\text{ w.r.t. }1$ as a Lipschitzian linear operator from E into G. g_1 is differentiable in a and ${g_1}'(a) = -Q \cdot P$. Consider N being a neighbourhood of a such that $N \subseteq \mathrm{dom}\, g_1$ and there exists a rest R of E, F such that for every point x of E such that $x \in N$ holds ${g_1}_{/x} - {g_1}_{/a} = ({g_1}'(a))(x - a) + R_{/x-a}$. Consider R being a rest of E, F such that for every point x of E such that $x \in N$ holds ${g_1}_{/x} - {g_1}_{/a} = ({g_1}'(a))(x - a) + R_{/x-a}$. For every point x of E such that $x \in N$ holds $g_{/x} - g_{/a} = ({g_1}'(a))(x - a) + R_{/x-a}$. □

(20) Let us consider a real normed space E, non trivial real Banach spaces G, F, a subset Z of $E \times F$, a partial function f from $E \times F$ to G, a point c of G, a subset A of E, a subset B of F, and a partial function g from E to F. Suppose Z is open and $\mathrm{dom}\, f = Z$ and A is open and B is open and $A \times B \subseteq Z$ and f is differentiable on Z and $f'_{\restriction Z}$ is continuous on Z and $\mathrm{dom}\, g = A$ and $\mathrm{rng}\, g \subseteq B$ and g is continuous on A and for every point x of E such that $x \in A$ holds $f(x, g(x)) = c$ and for every point x of E and for every point z of $E \times F$ such that $x \in A$ and $z = \langle x, g(x) \rangle$ holds $\mathrm{partdiff}(f,z)\text{ w.r.t. }2$ is invertible. Then

(i) g is differentiable on A, and

(ii) $g'_{\restriction A}$ is continuous on A, and

(iii) for every point x of E and for every point z of $E \times F$ such that $x \in A$ and $z = \langle x, g(x) \rangle$ holds $g'(x) = -(\mathrm{Inv\,partdiff}(f,z)\text{ w.r.t. }2) \cdot (\mathrm{partdiff}(f,z)\text{ w.r.t. }1)$.

Proof: For every point x of E and for every point z of $E \times F$ such that $x \in A$ and $z = \langle x, g(x) \rangle$ holds g is differentiable in x and $g'(x) = -(\mathrm{Inv\,partdiff}(f,z)\text{ w.r.t. }2) \cdot (\mathrm{partdiff}(f,z)\text{ w.r.t. }1)$. For every point x of E such that $x \in A$ holds g is differentiable in x. Consider x_2 being a partial function from E to $E \times F$ such that $\mathrm{dom}\, x_2 = A$ and for every point x of E such that $x \in A$ holds $x_2(x) = \langle x, g(x) \rangle$ and x_2 is continuous on A. Consider B being a bilinear operator from the real norm space of bounded linear operators from E into G × the real norm space of bounded linear operators from G into F into the real norm space of bounded linear operators from E into F such that B is continuous on the carrier of (the real norm space of bounded linear operators from E into G) × (the real norm space of bounded linear operators from G into F) and for every point u of the real norm space of bounded linear operators from E into G and for every point v of the real norm space of bounded linear operators from G into F, $B(u, v) = v \cdot u$.

Consider I being a partial function from the real norm space of bounded linear operators from F into G to the real norm space of bounded linear operators from G into F such that $\operatorname{dom} I = \text{InvertOpers}(F, G)$ and $\operatorname{rng} I = \text{InvertOpers}(G, F)$ and I is one-to-one and continuous on $\text{InvertOpers}(F, G)$ and there exists a partial function J from the real norm space of bounded linear operators from G into F to the real norm space of bounded linear operators from F into G such that $J = I^{-1}$ and J is one-to-one and $\operatorname{dom} J = \text{InvertOpers}(G, F)$ and $\operatorname{rng} J = \text{InvertOpers}(F, G)$ and J is continuous on $\text{InvertOpers}(G, F)$ and for every point u of the real norm space of bounded linear operators from F into G such that $u \in \text{InvertOpers}(F, G)$ holds $I(u) = \operatorname{Inv} u$. For every point x of E such that $x \in A$ holds $(g'_{\restriction A})_{/x} = -B_{/\langle ((f \restriction^1 Z) \cdot x_2)(x),\, (I \cdot (f \restriction^2 Z) \cdot x_2)(x) \rangle}$.

For every point x of E such that $x \in A$ holds $x \in \operatorname{dom}((f \restriction^1 Z) \cdot x_2)$ and $(f \restriction^1 Z) \cdot x_2$ is continuous in x. For every point x of E such that $x \in A$ holds $x \in \operatorname{dom}(I \cdot (f \restriction^2 Z) \cdot x_2)$ and $I \cdot (f \restriction^2 Z) \cdot x_2$ is continuous in x. Consider H being a partial function from E to the real norm space of bounded linear operators from E into F such that $\operatorname{dom} H = A$ and for every point x of E such that $x \in A$ holds $H(x) = B(((f \restriction^1 Z) \cdot x_2)(x), (I \cdot (f \restriction^2 Z) \cdot x_2)(x))$ and H is continuous on A. For every point x_0 of E such that $x_0 \in A$ holds $B(\langle ((f \restriction^1 Z) \cdot x_2)(x_0),\, (I \cdot (f \restriction^2 Z) \cdot x_2)(x_0) \rangle) = B_{/\langle ((f \restriction^1 Z) \cdot x_2)(x_0),\, (I \cdot (f \restriction^2 Z) \cdot x_2)(x_0) \rangle}$. For every point x_0 of E such that $x_0 \in A$ holds $g'_{\restriction A} \restriction A$ is continuous in x_0. □

(21) Let us consider a real normed space E, non trivial real Banach spaces G, F, a subset Z of $E \times F$, a partial function f from $E \times F$ to G, a point a of E, a point b of F, a point c of G, and a point z of $E \times F$. Suppose Z is open and $\operatorname{dom} f = Z$ and f is differentiable on Z and $f'_{\restriction Z}$ is continuous on Z and $\langle a, b \rangle \in Z$ and $f(a, b) = c$ and $z = \langle a, b \rangle$ and $\text{partdiff}(f, z)$ w.r.t. 2 is invertible. Then there exist real numbers r_1, r_2 such that

(i) $0 < r_1$, and

(ii) $0 < r_2$, and

(iii) $\text{Ball}(a, r_1) \times \overline{\text{Ball}}(b, r_2) \subseteq Z$, and

(iv) for every point x of E such that $x \in \operatorname{Ball}(a, r_1)$ there exists a point y of F such that $y \in \operatorname{Ball}(b, r_2)$ and $f(x, y) = c$, and

(v) for every point x of E such that $x \in \operatorname{Ball}(a, r_1)$ for every points y_1, y_2 of F such that y_1, $y_2 \in \operatorname{Ball}(b, r_2)$ and $f(x, y_1) = c$ and $f(x, y_2) = c$ holds $y_1 = y_2$, and

(vi) there exists a partial function g from E to F such that $\operatorname{dom} g = \operatorname{Ball}(a, r_1)$ and $\operatorname{rng} g \subseteq \operatorname{Ball}(b, r_2)$ and g is continuous on $\operatorname{Ball}(a, r_1)$ and $g(a) = b$ and for every point x of E such that $x \in \operatorname{Ball}(a, r_1)$ holds $f(x, g(x)) = c$ and g is differentiable on $\operatorname{Ball}(a, r_1)$ and $g'_{\restriction \operatorname{Ball}(a, r_1)}$ is continuous on $\operatorname{Ball}(a, r_1)$ and for every point x of E and for every point z of $E \times F$ such that $x \in \operatorname{Ball}(a, r_1)$ and $z = \langle x, g(x) \rangle$ holds $g'(x) = -(\operatorname{Inv} \operatorname{partdiff}(f, z) \text{ w.r.t. } 2) \cdot (\operatorname{partdiff}(f, z) \text{ w.r.t. } 1)$ and for every point x of E and for every point z of $E \times F$ such that $x \in \operatorname{Ball}(a, r_1)$ and $z = \langle x, g(x) \rangle$ holds $\operatorname{partdiff}(f, z)$ w.r.t. 2 is invertible, and

(vii) for every partial functions g_1, g_2 from E to F such that $\operatorname{dom} g_1 = \operatorname{Ball}(a, r_1)$ and $\operatorname{rng} g_1 \subseteq \operatorname{Ball}(b, r_2)$ and for every point x of E such that $x \in \operatorname{Ball}(a, r_1)$ holds $f(x, g_1(x)) = c$ and $\operatorname{dom} g_2 = \operatorname{Ball}(a, r_1)$ and $\operatorname{rng} g_2 \subseteq \operatorname{Ball}(b, r_2)$ and for every point x of E such that $x \in \operatorname{Ball}(a, r_1)$ holds $f(x, g_2(x)) = c$ holds $g_1 = g_2$.

Proof: Set $P = f_0 \restriction^2 Z_0$. Consider p_1 being a real number such that $0 < p_1$ and $\operatorname{Ball}(P_{/z}, p_1) \subseteq \operatorname{InvertOpers}(F, G)$. Consider s_1 being a real number such that $0 < s_1$ and for every point z_1 of $E \times F$ such that $z_1 \in Z_0$ and $\|z_1 - z\| < s_1$ holds $\|P_{/z_1} - P_{/z}\| < p_1$. Consider s_2 being a real number such that $0 < s_2$ and $\operatorname{Ball}(z, s_2) \subseteq Z_0$. Set $s = \min(s_1, s_2)$. Set $Z = \operatorname{Ball}(z, s)$. Set $f = f_0 \restriction Z$. Set $D = f'_{\restriction Z}$. For every point z of $E \times F$ such that $z \in Z$ holds ${f_0}'(z) = f'(z)$. For every point x_0 of $E \times F$ and for every real number r such that $x_0 \in Z$ and $0 < r$ there exists a real number s such that $0 < s$ and for every point x_1 of $E \times F$ such that $x_1 \in Z$ and $\|x_1 - x_0\| < s$ holds $\|D_{/x_1} - D_{/x_0}\| < r$. For every point z of $E \times F$ such that $z \in Z$ holds $\operatorname{partdiff}(f_0, z)$ w.r.t. 1 $=$ $\operatorname{partdiff}(f, z)$ w.r.t. 1 and $\operatorname{partdiff}(f_0, z)$ w.r.t. 2 $=$ $\operatorname{partdiff}(f, z)$ w.r.t. 2.

Consider r_1, r_2 being real numbers such that $0 < r_1$ and $0 < r_2$ and $\operatorname{Ball}(a, r_1) \times \overline{\operatorname{Ball}}(b, r_2) \subseteq Z$ and for every point x of E such that $x \in \operatorname{Ball}(a, r_1)$ there exists a point y of F such that $y \in \operatorname{Ball}(b, r_2)$ and $f(x, y) = c$ and for every point x of E such that $x \in \operatorname{Ball}(a, r_1)$ for every points y_1, y_2 of F such that y_1, $y_2 \in \operatorname{Ball}(b, r_2)$ and $f(x, y_1) = c$ and $f(x, y_2) = c$ holds $y_1 = y_2$ and there exists a partial function g from E to F such that g is continuous on $\operatorname{Ball}(a, r_1)$ and $\operatorname{dom} g = \operatorname{Ball}(a, r_1)$ and

$\operatorname{rng} g \subseteq \operatorname{Ball}(b, r_2)$ and $g(a) = b$ and for every point x of E such that $x \in \operatorname{Ball}(a, r_1)$ holds $f(x, g(x)) = c$ and for every partial functions g_1, g_2 from E to F such that $\operatorname{dom} g_1 = \operatorname{Ball}(a, r_1)$ and $\operatorname{rng} g_1 \subseteq \operatorname{Ball}(b, r_2)$ and for every point x of E such that $x \in \operatorname{Ball}(a, r_1)$ holds $f(x, g_1(x)) = c$ and $\operatorname{dom} g_2 = \operatorname{Ball}(a, r_1)$ and $\operatorname{rng} g_2 \subseteq \operatorname{Ball}(b, r_2)$ and for every point x of E such that $x \in \operatorname{Ball}(a, r_1)$ holds $f(x, g_2(x)) = c$ holds $g_1 = g_2$.

For every point x of E and for every point y of F such that $x \in \operatorname{Ball}(a, r_1)$ and $y \in \operatorname{Ball}(b, r_2)$ holds $f_0(x, y) = f(x, y)$. For every point x of E such that $x \in \operatorname{Ball}(a, r_1)$ there exists a point y of F such that $y \in \operatorname{Ball}(b, r_2)$ and $f_0(x, y) = c$. For every point x of E such that $x \in \operatorname{Ball}(a, r_1)$ for every points y_1, y_2 of F such that y_1, $y_2 \in \operatorname{Ball}(b, r_2)$ and $f_0(x, y_1) = c$ and $f_0(x, y_2) = c$ holds $y_1 = y_2$. Consider g being a partial function from E to F such that g is continuous on $\operatorname{Ball}(a, r_1)$ and $\operatorname{dom} g = \operatorname{Ball}(a, r_1)$ and $\operatorname{rng} g \subseteq \operatorname{Ball}(b, r_2)$ and $g(a) = b$ and for every point x of E such that $x \in \operatorname{Ball}(a, r_1)$ holds $f(x, g(x)) = c$. For every point x of E and for every point w of $E \times F$ such that $x \in \operatorname{Ball}(a, r_1)$ and $w = \langle x, g(x) \rangle$ holds $\operatorname{partdiff}(f_0, w)$ w.r.t. 2 is invertible. For every point x of E and for every point w of $E \times F$ such that $x \in \operatorname{Ball}(a, r_1)$ and $w = \langle x, g(x) \rangle$ holds $\operatorname{partdiff}(f, w)$ w.r.t. 2 is invertible.

For every point x of E such that $x \in \operatorname{Ball}(a, r_1)$ holds $f_0(x, g(x)) = c$. g is differentiable on $\operatorname{Ball}(a, r_1)$ and $g'_{\restriction \operatorname{Ball}(a, r_1)}$ is continuous on $\operatorname{Ball}(a, r_1)$ and for every point x of E and for every point z of $E \times F$ such that $x \in \operatorname{Ball}(a, r_1)$ and $z = \langle x, g(x) \rangle$ holds $g'(x) = -(\operatorname{Inv} \operatorname{partdiff}(f_0, z)$ w.r.t. $2) \cdot$ $(\operatorname{partdiff}(f_0, z)$ w.r.t. $1)$. For every partial functions g_1, g_2 from E to F such that $\operatorname{dom} g_1 = \operatorname{Ball}(a, r_1)$ and $\operatorname{rng} g_1 \subseteq \operatorname{Ball}(b, r_2)$ and for every point x of E such that $x \in \operatorname{Ball}(a, r_1)$ holds $f_0(x, g_1(x)) = c$ and $\operatorname{dom} g_2 = \operatorname{Ball}(a, r_1)$ and $\operatorname{rng} g_2 \subseteq \operatorname{Ball}(b, r_2)$ and for every point x of E such that $x \in \operatorname{Ball}(a, r_1)$ holds $f_0(x, g_2(x)) = c$ holds $g_1 = g_2$. □

References

[1] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pąk. The role of the Mizar Mathematical Library for interactive proof development in Mizar. *Journal of Automated Reasoning*, 61(1):9–32, 2018. doi:10.1007/s10817-017-9440-6.

[2] Bruce K. Driver. *Analysis Tools with Applications*. Springer, Berlin, 2003.

[3] Adam Grabowski, Artur Korniłowicz, and Adam Naumowicz. Four decades of Mizar. *Journal of Automated Reasoning*, 55(3):191–198, 2015. doi:10.1007/s10817-015-9345-1.

[4] Hiroshi Imura, Morishige Kimura, and Yasunari Shidama. The differentiable functions on normed linear spaces. *Formalized Mathematics*, 12(**3**):321–327, 2004.

[5] Kazuhisa Nakasho. Invertible operators on Banach spaces. *Formalized Mathematics*, 27 (**2**):107–115, 2019. doi:10.2478/forma-2019-0012.

[6] Kazuhisa Nakasho, Yuichi Futa, and Yasunari Shidama. Implicit function theorem. Part I. *Formalized Mathematics*, 25(**4**):269–281, 2017. doi:10.1515/forma-2017-0026.

[7] Takaya Nishiyama, Keiji Ohkubo, and Yasunari Shidama. The continuous functions on normed linear spaces. *Formalized Mathematics*, 12(**3**):269–275, 2004.

[8] Hiroyuki Okazaki, Noboru Endou, and Yasunari Shidama. Cartesian products of family of real linear spaces. *Formalized Mathematics*, 19(**1**):51–59, 2011. doi:10.2478/v10037-011-0009-2.

[9] Hideki Sakurai, Hiroyuki Okazaki, and Yasunari Shidama. Banach's continuous inverse theorem and closed graph theorem. *Formalized Mathematics*, 20(**4**):271–274, 2012. doi:10.2478/v10037-012-0032-y.

[10] Laurent Schwartz. *Théorie des ensembles et topologie, tome 1. Analyse.* Hermann, 1997.

[11] Laurent Schwartz. *Calcul différentiel, tome 2. Analyse.* Hermann, 1997.

Accepted May 27, 2019

FORMALIZED MATHEMATICS
Vol. 27, No. 2, Pages 133–137, 2019
DOI: 10.2478/forma-2019-0014

sciendo
https://www.sciendo.com/

On Monomorphisms and Subfields

Christoph Schwarzweller
Institute of Informatics
University of Gdańsk
Poland

Summary. This is the second part of a four-article series containing a Mizar [2], [1] formalization of Kronecker's construction about roots of polynomials in field extensions, i.e. that for every field F and every polynomial $p \in F[X]\backslash F$ there exists a field extension E of F such that p has a root over E. The formalization follows Kronecker's classical proof using $F[X]/{<}p{>}$ as the desired field extension E [5], [3], [4].

In the first part we show that an irreducible polynomial $p \in F[X]\backslash F$ has a root over $F[X]/{<}p{>}$. Note, however, that this statement cannot be true in a rigid formal sense: We do not have $F \subseteq F[X]/<p>$ as sets, so F is not a subfield of $F[X]/{<}p{>}$, and hence formally p is not even a polynomial over $F[X]/<p>$. Consequently, we translate p along the canonical monomorphism $\phi : F \longrightarrow F[X]/{<}p{>}$ and show that the translated polynomial $\phi(p)$ has a root over $F[X]/{<}p{>}$.

Because F is not a subfield of $F[X]/{<}p{>}$ we construct in this second part the field $(E \setminus \phi F) \cup F$ for a given monomorphism $\phi : F \longrightarrow E$ and show that this field both is isomorphic to F and includes F as a subfield. In the literature this part of the proof usually consists of saying that "one can identify F with its image ϕF in $F[X]/{<}p{>}$ and therefore consider F as a subfield of $F[X]/{<}p{>}$". Interestingly, to do so we need to assume that $F \cap E = \emptyset$, in particular Kronecker's construction can be formalized for fields F with $F \cap F[X] = \emptyset$.

Surprisingly, as we show in the third part, this condition is not automatically true for arbitray fields F: With the exception of $\mathbb{Z}_2$ we construct for every field F an isomorphic copy F' of F with $F' \cap F'[X] \neq \emptyset$. We also prove that for Mizar's representations of $\mathbb{Z}_n$, $\mathbb{Q}$ and $\mathbb{R}$ we have $\mathbb{Z}_n \cap \mathbb{Z}_n[X] = \emptyset$, $\mathbb{Q} \cap \mathbb{Q}[X] = \emptyset$ and $\mathbb{R} \cap \mathbb{R}[X] = \emptyset$, respectively.

In the fourth part we finally define field extensions: E is a field extension of F iff F is a subfield of E. Note, that in this case we have $F \subseteq E$ as sets, and thus a polynomial p over F is also a polynomial over E. We then apply the construction of the second part to $F[X]/{<}p{>}$ with the canonical monomorphism

ISSN 1426–2630(Print), 1898-9934(Online)

$\phi : F \longrightarrow F[X]/{<}p{>}$. Together with the first part this gives - for fields F with $F \cap F[X] = \emptyset$ - a field extension E of F in which $p \in F[X] \backslash F$ has a root.

MSC: 12E05 12F05 68T99 03B35

Keywords: roots of polynomials; field extensions; Kronecker's construction

MML identifier: `FIELD_2`, version: `8.1.09 5.57.1355`

From now on R denotes a ring, S denotes an R-monomorphic ring, K denotes a field, F denotes a K-monomorphic field, and T denotes a K-monomorphic commutative ring.

Let us consider R and S. Let f be a monomorphism of R and S. Let us observe that the functor f^{-1} yields a function from $\operatorname{rng} f$ into R. Now we state the propositions:

(1) Let us consider a monomorphism f of R and S, and elements a, b of $\operatorname{rng} f$. Then

(i) $(f^{-1})(a+b) = (f^{-1})(a) + (f^{-1})(b)$, and

(ii) $(f^{-1})(a \cdot b) = (f^{-1})(a) \cdot (f^{-1})(b)$.

(2) Let us consider a monomorphism f of R and S, and an element a of $\operatorname{rng} f$. Then $(f^{-1})(a) = 0_R$ if and only if $a = 0_S$.

Let us consider a monomorphism f of R and S. Now we state the propositions:

(3) (i) $(f^{-1})(1_S) = 1_R$, and

(ii) $(f^{-1})(0_S) = 0_R$.

The theorem is a consequence of (1).

(4) f^{-1} is one-to-one and onto.

(5) Let us consider a monomorphism f of R and S, and an element a of R. Then $f(a) = 0_S$ if and only if $a = 0_R$.

(6) Let us consider a monomorphism f of K and F, and an element a of K. If $a \neq 0_K$, then $f(a^{-1}) = f(a)^{-1}$. The theorem is a consequence of (5).

Let R, S be rings. We introduce the notation R and S are disjoint as a synonym of R misses S.

One can check that R and S are disjoint if and only if the condition (Def. 1) is satisfied.

(Def. 1) $\Omega_R \cap \Omega_S = \emptyset$.

Let us consider R and S. Let f be a monomorphism of R and S. The functor $\overline{f}$ yielding a non empty set is defined by the term

(Def. 2) $(\Omega_S \setminus \operatorname{rng} f) \cup \Omega_R$.

Let R be a ring, S be an R-monomorphic ring, and a, b be elements of $\overline{f}$. The functor $\operatorname{addemb}(f,a,b)$ yielding an element of $\overline{f}$ is defined by the term

$$\text{(Def. 3)}\quad \begin{cases} (\text{the addition of } R)(a,b), & \textbf{if } a,b \in \Omega_R, \\ (\text{the addition of } S)(f(a),b), & \textbf{if } a \in \Omega_R \text{ and } b \notin \Omega_R, \\ (\text{the addition of } S)(a,f(b)), & \textbf{if } b \in \Omega_R \text{ and } a \notin \Omega_R, \\ (f^{-1})((\text{the addition of } S)(a,b)), & \textbf{if } a \notin \Omega_R \text{ and } b \notin \Omega_R \text{ and} \\ & \quad (\text{the addition of } S)(a,b) \in \operatorname{rng} f, \\ (\text{the addition of } S)(a,b), & \textbf{otherwise}. \end{cases}$$

The functor $\operatorname{addemb}(f)$ yielding a binary operation on $\overline{f}$ is defined by

(Def. 4) for every elements a, b of $\overline{f}$, $\mathit{it}(a,b) = \operatorname{addemb}(f,a,b)$.

Let K be a field, T be a K-monomorphic commutative ring, f be a monomorphism of K and T, and a, b be elements of $\overline{f}$. The functor $\operatorname{multemb}(f,a,b)$ yielding an element of $\overline{f}$ is defined by the term

$$\text{(Def. 5)}\quad \begin{cases} (\text{the multiplication of } K)(a,b), & \textbf{if } a,b \in \Omega_K, \\ 0_K, & \textbf{if } a = 0_K \text{ or } b = 0_K, \\ (\text{the multiplication of } T)(f(a),b), & \textbf{if } a \in \Omega_K \text{ and } a \neq 0_K \text{ and} \\ & \quad b \notin \Omega_K, \\ (\text{the multiplication of } T)(a,f(b)), & \textbf{if } b \in \Omega_K \text{ and } b \neq 0_K \text{ and} \\ & \quad a \notin \Omega_K, \\ (f^{-1})((\text{the multiplication of } T)(a,b)), & \textbf{if } a \notin \Omega_K \text{ and } b \notin \Omega_K \text{ and} \\ & \quad (\text{the multiplication of } T) \\ & \quad (a,b) \in \operatorname{rng} f, \\ (\text{the multiplication of } T)(a,b), & \textbf{otherwise}. \end{cases}$$

The functor $\operatorname{multemb}(f)$ yielding a binary operation on $\overline{f}$ is defined by

(Def. 6) for every elements a, b of $\overline{f}$, $\mathit{it}(a,b) = \operatorname{multemb}(f,a,b)$.

The functor $\operatorname{embField}(f)$ yielding a strict double loop structure is defined by

(Def. 7) the carrier of $\mathit{it} = \overline{f}$ and the addition of $\mathit{it} = \operatorname{addemb}(f)$ and the multiplication of $\mathit{it} = \operatorname{multemb}(f)$ and the one of $\mathit{it} = 1_K$ and the zero of $\mathit{it} = 0_K$.

One can verify that $\operatorname{embField}(f)$ is non degenerated and $\operatorname{embField}(f)$ is Abelian and right zeroed.

Let us consider a monomorphism f of K and T. Now we state the propositions:

(7) If K and T are disjoint, then $\operatorname{embField}(f)$ is add-associative. The theorem is a consequence of (1).

(8) If K and T are disjoint, then $\operatorname{embField}(f)$ is right complementable.

Let K be a field, T be a K-monomorphic commutative ring, and f be a monomorphism of K and T. Note that $\operatorname{embField}(f)$ is commutative and well unital.

(9) Let us consider a monomorphism f of K and F. If K and F are disjoint, then embField(f) is associative. The theorem is a consequence of (1), (2), and (6).

(10) Let us consider a monomorphism f of K and T. If K and T are disjoint, then embField(f) is distributive. The theorem is a consequence of (3), (2), and (1).

Let us consider a monomorphism f of K and F. Now we state the propositions:

(11) If K and F are disjoint, then embField(f) is almost left invertible. The theorem is a consequence of (3).

(12) If K and F are disjoint, then embField(f) is a field.

Let K be a field, F be a K-monomorphic field, and f be a monomorphism of K and F. The functor emb-iso(f) yielding a function from embField(f) into F is defined by

(Def. 8) for every element a of embField(f) such that $a \notin K$ holds $it(a) = a$ and for every element a of embField(f) such that $a \in K$ holds $it(a) = f(a)$.

One can verify that emb-iso(f) is unity-preserving.

Let us consider a monomorphism f of K and F. Now we state the propositions:

(13) If K and F are disjoint, then emb-iso(f) is additive.

(14) If K and F are disjoint, then emb-iso(f) is multiplicative.

Let K be a field, F be a K-monomorphic field, and f be a monomorphism of K and F. Note that emb-iso(f) is one-to-one.

Let us consider a monomorphism f of K and F. Now we state the propositions:

(15) If K and F are disjoint, then emb-iso(f) is onto.

(16) If K and F are disjoint, then F and embField(f) are isomorphic. The theorem is a consequence of (13), (14), and (15).

(17) Let us consider a monomorphism f of K and F, and a field E. If $E =$ embField(f), then K is a subfield of E.

(18) If K and F are disjoint, then there exists a field E such that E and F are isomorphic and K is a subfield of E. The theorem is a consequence of (7), (9), (10), (8), (11), (16), and (17).

(19) Let us consider fields K, F. Suppose K and F are disjoint. Then F is K-monomorphic if and only if there exists a field E such that E and F are isomorphic and K is a subfield of E. The theorem is a consequence of (18).

References

[1] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pąk. The role of the Mizar Mathematical Library for interactive proof development in Mizar. *Journal of Automated Reasoning*, 61(1):9–32, 2018. doi:10.1007/s10817-017-9440-6.

[2] Adam Grabowski, Artur Korniłowicz, and Adam Naumowicz. Four decades of Mizar. *Journal of Automated Reasoning*, 55(3):191–198, 2015. doi:10.1007/s10817-015-9345-1.

[3] Nathan Jacobson. *Basic Algebra I.* Dover Books on Mathematics, 1985.

[4] Heinz Lüneburg. *Gruppen, Ringe, Körper: Die grundlegenden Strukturen der Algebra.* Oldenbourg Verlag, 1999.

[5] Knut Radbruch. *Algebra I.* Lecture Notes, University of Kaiserslautern, Germany, 1991.

Accepted May 27, 2019

FORMALIZED MATHEMATICS
Vol. **27**, No. **2**, Pages 139–152, **2019**
DOI: 10.2478/forma-2019-0015

sciendo
https://www.sciendo.com/

Natural Addition of Ordinals

Sebastian Koch
Johannes Gutenberg University
Mainz, Germany[1]

Summary. In [3] the existence of the Cantor normal form of ordinals was proven in the Mizar system [6]. In this article its uniqueness is proven and then used to formalize the natural sum of ordinals.

MSC: 03E10 68T99 03B35

Keywords: ordinal numbers; Cantor normal form; Hessenberg sum; natural sum

MML identifier: `ORDINAL7`, version: `8.1.09 5.57.1355`

0. Introduction

It is well known that any ordinal number α can be uniquely written as

$$\alpha = \sum_{i=1}^{k} n_i \omega^{\beta_i},$$

where k is a natural number, $n_1, \ldots, n_k$ are positive integers and $\beta_1 > \ldots > \beta_k$ are ordinal numbers. This representation, usually called the Cantor Normal Form, has been formalized as the tuple $\langle n_1\omega^{\beta_1}, \ldots, n_k\omega^{\beta_k}\rangle$ in [3] and the existence of such a sequence that sums up to a given ordinal α has been proven in the same, but the uniqueness was omitted.

The basic proof idea for the uniqueness is well known (cf. [1], [2], [4], [5], [8]). This article provides a variant which utilizes the additional closure of ordinals, i.e. that any ordinals α, β, γ with $\alpha, \beta \in \omega^\gamma$ also satisfy $\alpha + \beta \in \omega^\gamma$. Usually the

[1] The author is enrolled in the Johannes Gutenberg University in Mayence, Germany, mailto: `skoch02@students.uni-mainz.de`

additional closure is proven using the uniqueness in the literature, but here the additional closure is proven first by using theorems from [3]. Other theorems of this article include:

- For ordinals α, β with $1 \in \alpha \in \beta$ holds $\beta + \alpha \in \alpha\beta \in \beta^\alpha \in \beta \uparrow\uparrow \alpha$.
- Decreasing ordinal sequences with the same range are equal.

In the last section of the article the natural sum or Hessenberg sum (cf. [2], [5]) of two ordinals α, β, denoted by $\alpha \oplus \beta$, is formalized using the Cantor Normal Form. The concept of bags, as used to formalize polynomials in Mizar (cf. [7]), couldn't easily be applied in this case since there is no set of all ordinals, so it wasn't used here. The chosen definition of the natural sum turned out to be slightly sophisticated, leading to a rather long proof of its monotonicity property, while the proofs of the other shown properties are straightforward.

1. Preliminaries

Now we state the proposition:

(1) Let us consider a set X. Then $X \cap \operatorname{succ} X = X$.

Let A be an increasing sequence of ordinal numbers and a be an ordinal number. Let us observe that $A \restriction a$ is increasing.

Now we state the propositions:

(2) Let us consider an ordinal number a. Then $a + a = 2 \cdot a$.

(3) Let us consider ordinal numbers a, b. If $1 \in a$ and $a \in b$, then $b + a \in a \cdot b$. The theorem is a consequence of (2).

(4) Let us consider an ordinal number a. Then $a \cdot a = a^2$.

Let us consider ordinal numbers a, b. Now we state the propositions:

(5) If $1 \in a$ and $a \in b$, then $a \cdot b \in b^a$. The theorem is a consequence of (4).

(6) If $1 \in a$ and $a \in b$, then $b^a \in b \uparrow\uparrow a$.

Let us observe that there exists a sequence of ordinal numbers which is infinite.

Now we state the propositions:

(7) Let us consider transfinite sequences A, B. Suppose $A \frown B$ is ordinal yielding. Then

(i) A is ordinal yielding, and

(ii) B is ordinal yielding.

(8) Let us consider ordinal numbers a, b. If $a \in b$, then b-exponent$(a) = 0$.

Let us consider ordinal numbers a, b, c. Now we state the propositions:

(9) If $a \subseteq c$, then b-exponent$(a) \subseteq b$-exponent(c).

(10) If $0 \in a$ and $1 \in b$ and $a \in b^c$, then b-exponent$(a) \in c$.
Proof: b-exponent$(a) \subseteq c$. b-exponent$(a) \neq c$. □

Let us note that every sequence of ordinal numbers which is decreasing is also one-to-one. Let A be a decreasing transfinite sequence and a be an ordinal number. One can verify that $A{\restriction}a$ is decreasing.

Let A be a non-decreasing transfinite sequence. One can verify that $A{\restriction}a$ is non-decreasing. Let A be a non-increasing transfinite sequence. One can verify that $A{\restriction}a$ is non-increasing.

Now we state the propositions:

(11) Let us consider finite sequences A, B of ordinal numbers. Then $\sum A^\frown B = \sum A + \sum B$.
Proof: Define $\mathcal{P}$[natural number] $\equiv$ for every finite sequences A, B of ordinal numbers such that $\operatorname{dom} B = \$_1$ holds $\sum A \frown B = \sum A + \sum B$. $\mathcal{P}[0]$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every natural number n, $\mathcal{P}[n]$. □

(12) Let us consider ordinal numbers a, b. Then $\sum \langle a, b\rangle = a+b$. The theorem is a consequence of (11).

Let A be a non empty, non-empty, finite sequence of ordinal numbers. Let us observe that $\sum A$ is non empty.

Let B be a finite sequence of ordinal numbers. Note that $\sum A \frown B$ is non empty and $\sum B \frown A$ is non empty.

Now we state the propositions:

(13) Let us consider an ordinal number a, and a natural number n. Then $\sum n \longmapsto a = n \cdot a$.

(14) Let us consider a finite sequence A of ordinal numbers, and an ordinal number a. Then $\sum A{\restriction}a \subseteq \sum A$.

(15) Let us consider finite sequences A, B of ordinal numbers. Suppose $\operatorname{dom} A \subseteq \operatorname{dom} B$ and for every object a such that $a \in \operatorname{dom} A$ holds $A(a) \subseteq B(a)$. Then $\sum A \subseteq \sum B$.
Proof: Set $a = \operatorname{dom} A$. Consider f_1 being a sequence of ordinal numbers such that $\sum A = \operatorname{last} f_1$ and $\operatorname{dom} f_1 = \operatorname{succ} \operatorname{dom} A$ and $f_1(0) = 0$ and for every natural number n such that $n \in \operatorname{dom} A$ holds $f_1(n+1) = f_1(n) + A(n)$. Consider f_2 being a sequence of ordinal numbers such that $\sum B{\restriction}a = \operatorname{last} f_2$ and $\operatorname{dom} f_2 = \operatorname{succ} \operatorname{dom}(B{\restriction}a)$ and $f_2(0) = 0$ and for every natural number n such that $n \in \operatorname{dom}(B{\restriction}a)$ holds $f_2(n+1) = f_2(n) + (B{\restriction}a)(n)$. Define $\mathcal{P}$[natural number] $\equiv$ if $\$_1 \in \operatorname{succ} a$, then $f_1(\$_1) \subseteq f_2(\$_1)$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every natural number n, $\mathcal{P}[n]$. $\sum B{\restriction}a \subseteq \sum B$. □

(16) Let us consider a Cantor normal form sequence A of ordinal numbers. Suppose $A \neq \emptyset$. Then there exists a Cantor normal form sequence B of ordinal numbers and there exists a Cantor component ordinal number a such that $A = B \frown \langle a \rangle$. The theorem is a consequence of (7).

Let A be a Cantor normal form sequence of ordinal numbers and n be a natural number. Let us observe that $A \restriction n$ is Cantor normal form and $A_{\lfloor n}$ is Cantor normal form and every transfinite sequence which is natural-valued is also ordinal yielding and every natural number which is limit ordinal is also zero and there exists an ordinal number which is non limit ordinal.

Let n, m be natural numbers. We identify $\max(n, m)$ with $n \cup m$. We identify $\min(n, m)$ with $n \cap m$.

2. About the Cantor Normal Form

Now we state the proposition:

(17) Let us consider ordinal numbers a, b. Then $a + b = b$ if and only if $\omega \cdot a \subseteq b$. The theorem is a consequence of (2).

Let us consider a non empty, Cantor normal form sequence A of ordinal numbers and an object a. Now we state the propositions:

(18) If $a \in \operatorname{dom} A$, then ω-exponent(last A) $\subseteq$ ω-exponent($A(a)$). The theorem is a consequence of (16).

(19) If $a \in \operatorname{dom} A$, then ω-exponent($A(a)$) $\subseteq$ ω-exponent($A(0)$).

(20) Let us consider non empty, Cantor normal form sequences A, B of ordinal numbers. Suppose ω-exponent($B(0)$) $\in$ ω-exponent(last A). Then $A \frown B$ is Cantor normal form.

Proof: For every ordinal numbers a, b such that $a \in b$ and $b \in \operatorname{dom}(A \frown B)$ holds ω-exponent($(A \frown B)(b)$) $\in$ ω-exponent($(A \frown B)(a)$) by [9, (20)]. □

(21) Let us consider decreasing sequences A, B of ordinal numbers. If $\operatorname{rng} A = \operatorname{rng} B$, then $A = B$.

Proof: Define $\mathcal{P}$[natural number] $\equiv$ for every decreasing sequences A, B of ordinal numbers such that $\operatorname{len} A = \$_1$ and $\operatorname{rng} A = \operatorname{rng} B$ holds $A = B$. $\mathcal{P}[0]$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every natural number n, $\mathcal{P}[n]$. □

Let a be an ordinal number. Let us observe that ω^a is Cantor component.

Let n be a non zero natural number. Let us note that $n \cdot \omega^a$ is Cantor component and every natural number which is non zero is also Cantor component.

Let c be a Cantor component ordinal number. Let us observe that $\langle c \rangle$ is Cantor normal form.

Now we state the proposition:

(22) Let us consider Cantor component ordinal numbers c, d.
Suppose ω-exponent$(d) \in \omega$-exponent(c). Then $\langle c, d\rangle$ is Cantor normal form. The theorem is a consequence of (20).

Let a be a non empty ordinal number and m be a non zero natural number. Note that $\langle \omega^a, m\rangle$ is Cantor normal form.

Let n be a non zero natural number. Observe that $\langle n \cdot \omega^a, m\rangle$ is Cantor normal form.

Now we state the proposition:

(23) Let us consider Cantor component ordinal numbers c, d, e. Suppose ω-exponent$(d) \in \omega$-exponent(c) and ω-exponent$(e) \in \omega$-exponent(d). Then $\langle c, d, e\rangle$ is Cantor normal form. The theorem is a consequence of (22) and (20).

Let us consider a non empty, Cantor normal form sequence A of ordinal numbers, an ordinal number b, and a non zero natural number n. Now we state the propositions:

(24) If $b \in \omega$-exponent(last A), then $A \frown \langle n \cdot \omega^b\rangle$ is Cantor normal form. The theorem is a consequence of (20).

(25) If ω-exponent(last A) $\neq 0$, then $A \frown \langle n\rangle$ is Cantor normal form. The theorem is a consequence of (24).

(26) If ω-exponent$(A(0)) \in b$, then $\langle n \cdot \omega^b\rangle \frown A$ is Cantor normal form. The theorem is a consequence of (20).

(27) Let us consider ordinal numbers a_1, a_2, b. If $a_1, a_2 \in \omega^b$, then $a_1 + a_2 \in \omega^b$.

(28) Let us consider a finite sequence A of ordinal numbers, and an ordinal number b. Suppose for every ordinal number a such that $a \in \operatorname{dom} A$ holds $A(a) \in \omega^b$. Then $\sum A \in \omega^b$. The theorem can be shown by natural induction and (27).

(29) Let us consider ordinal numbers a, b, and a natural number n. If $a \in \omega^b$, then $n \cdot a \in \omega^b$. The theorem is a consequence of (28) and (13).

(30) Let us consider a finite sequence A of ordinal numbers, and an ordinal number a. Suppose $\langle a\rangle \frown A$ is Cantor normal form. Then $\sum A \in \omega^{\omega\text{-exponent}(a)}$. The theorem is a consequence of (29) and (28).

(31) Let us consider a Cantor normal form sequence A of ordinal numbers. Then ω-exponent$(\sum A) = \omega$-exponent$(A(0))$.
Proof: Define $\mathcal{P}$[natural number] $\equiv$ for every Cantor normal form sequence A of ordinal numbers such that len $A = \$_1$ holds ω-exponent$(\sum A) = \omega$-exponent$(A(0))$. $\mathcal{P}[0]$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every natural number n, $\mathcal{P}[n]$. □

(32) Let us consider Cantor normal form sequences A, B of ordinal numbers.

If $\sum A = \sum B$, then $A = B$.

Proof: Define $\mathcal{P}$[natural number] $\equiv$ for every Cantor normal form sequences A, B of ordinal numbers such that $\operatorname{dom} A \cup \operatorname{dom} B = \$_1$ and $\sum A = \sum B$ holds $A = B$. $\mathcal{P}[0]$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every natural number n, $\mathcal{P}[n]$. □

Let A be a sequence of ordinal numbers and b be an ordinal number. The functor b-exponent(A) yielding a sequence of ordinal numbers is defined by

(Def. 1) $\operatorname{dom} it = \operatorname{dom} A$ and for every object a such that $a \in \operatorname{dom} A$ holds $it(a) = b$-exponent$(A(a))$.

Let A be an empty sequence of ordinal numbers.

One can check that b-exponent(A) is empty.

Let A be a non empty sequence of ordinal numbers. One can verify that b-exponent(A) is non empty. Let A be a finite sequence of ordinal numbers. Let us observe that b-exponent(A) is finite.

Let A be an infinite sequence of ordinal numbers. Let us observe that b-exponent(A) is infinite.

Now we state the propositions:

(33) Let us consider ordinal numbers a, b. Then b-exponent$(\langle a \rangle) = \langle b$-exponent$(a)\rangle$.

(34) Let us consider sequences A, B of ordinal numbers, and an ordinal number b. Then b-exponent$(A \frown B) = (b$-exponent$(A)) \frown (b$-exponent$(B))$.

(35) Let us consider a sequence A of ordinal numbers, and ordinal numbers b, c. Then b-exponent$(A{\restriction}c) = (b$-exponent$(A)){\restriction}c$.

(36) Let us consider a finite sequence A of ordinal numbers, an ordinal number b, and a natural number n. Then b-exponent$(A_{\lfloor n}) = (b$-exponent$(A))_{\lfloor n}$.

Let A be a Cantor normal form sequence of ordinal numbers. Let us note that ω-exponent(A) is decreasing.

Now we state the propositions:

(37) Let us consider sequences A, B of ordinal numbers. Suppose $A \frown B$ is Cantor normal form. Then rng$(\omega$-exponent$(A))$ misses rng$(\omega$-exponent$(B))$.

Proof: rng$(\omega$-exponent$(A)) \cap$ rng$(\omega$-exponent$(B)) = \emptyset$. □

(38) Let us consider a Cantor normal form sequence A of ordinal numbers. Then $0 \in$ rng$(\omega$-exponent$(A))$ if and only if $A \neq \emptyset$ and ω-exponent(last A) $= 0$. The theorem is a consequence of (18) and (16).

Let a, b be ordinal numbers. The functor b-LC(a) yielding an ordinal number is defined by the term

(Def. 2) $a \operatorname{div} b^{b\text{-exponent}(a)}$.

Let us consider an ordinal number a. Now we state the propositions:

(39) $0\text{-LC}(a) = a$.

(40) $1\text{-LC}(a) = a$.

(41) Let us consider an ordinal number b. Then $b\text{-LC}(0) = 0$.

(42) Let us consider ordinal numbers a, b. If $a \in b$, then $b\text{-LC}(a) = a$. The theorem is a consequence of (8).

(43) Let us consider an ordinal number b. Then $b\text{-LC}(1) = 1$. The theorem is a consequence of (42), (40), and (39).

(44) Let us consider ordinal numbers a, b, c. If $c \in b$, then $b\text{-LC}(c \cdot b^a) = c$.

(45) Let us consider ordinal numbers a, b. If $1 \in b$, then $b\text{-LC}(b^a) = 1$. The theorem is a consequence of (44).

Let c be a Cantor component ordinal number. Observe that $\omega\text{-LC}(c)$ is natural and non empty.

Now we state the proposition:

(46) Let us consider a Cantor component ordinal number c. Then $c = (\omega\text{-LC}(c)) \cdot \omega^{\omega\text{-exponent}(c)}$. The theorem is a consequence of (44).

Let A be a sequence of ordinal numbers and b be an ordinal number. The functor $b\text{-LC}(A)$ yielding a sequence of ordinal numbers is defined by

(Def. 3) $\operatorname{dom} it = \operatorname{dom} A$ and for every object a such that $a \in \operatorname{dom} A$ holds $it(a) = b\text{-LC}(A(a))$.

Let A be an empty sequence of ordinal numbers. Let us observe that $b\text{-LC}(A)$ is empty. Let A be a non empty sequence of ordinal numbers. Observe that $b\text{-LC}(A)$ is non empty.

Let A be a finite sequence of ordinal numbers. Let us note that $b\text{-LC}(A)$ is finite. Let A be an infinite sequence of ordinal numbers. Let us note that $b\text{-LC}(A)$ is infinite. Now we state the propositions:

(47) Let us consider ordinal numbers a, b. Then $b\text{-LC}(\langle a \rangle) = \langle b\text{-LC}(a) \rangle$.

(48) Let us consider sequences A, B of ordinal numbers, and an ordinal number b. Then $b\text{-LC}(A \frown B) = (b\text{-LC}(A)) \frown (b\text{-LC}(B))$.

(49) Let us consider a sequence A of ordinal numbers, and ordinal numbers b, c. Then $b\text{-LC}(A \restriction c) = (b\text{-LC}(A)) \restriction c$.

(50) Let us consider a finite sequence A of ordinal numbers, an ordinal number b, and a natural number n. Then $b\text{-LC}(A_{\downharpoonright n}) = (b\text{-LC}(A))_{\downharpoonright n}$.

Let A be a Cantor normal form sequence of ordinal numbers and a be an object. Note that $(\omega\text{-LC}(A))(a)$ is natural and $\omega\text{-LC}(A)$ is natural-valued and non-empty.

Let us consider a Cantor normal form sequence A of ordinal numbers and an object a. Now we state the propositions:

(51) If $a \in \operatorname{dom} A$, then $A(a) = (\omega\text{-LC}(A(a))) \cdot \omega^{\omega\text{-exponent}(A(a))}$. The theorem is a consequence of (46).

(52) If $a \in \operatorname{dom} A$, then $A(a) = (\omega\text{-LC}(A))(a) \cdot \omega^{(\omega\text{-exponent}(A))(a)}$. The theorem is a consequence of (51).

(53) Let us consider a decreasing sequence A of ordinal numbers, and a natural-valued, non-empty sequence B of ordinal numbers. Suppose $\operatorname{dom} A = \operatorname{dom} B$. Then there exists a Cantor normal form sequence C of ordinal numbers such that

(i) ω-exponent$(C) = A$, and

(ii) $\omega\text{-LC}(C) = B$.

Proof: Define $\mathcal{F}(\text{ordinal number}) = B(\$_1) \cdot \omega^{A(\$_1)}$. Consider C being a sequence of ordinal numbers such that $\operatorname{dom} C = \operatorname{dom} A$ and for every ordinal number a such that $a \in \operatorname{dom} A$ holds $C(a) = \mathcal{F}(a)$. □

(54) Let us consider Cantor normal form sequences A, B of ordinal numbers. Suppose ω-exponent$(A) = \omega$-exponent(B) and $\omega\text{-LC}(A) = \omega\text{-LC}(B)$. Then $A = B$. The theorem is a consequence of (52).

Let a be an ordinal number. The functor CNF(a) yielding a Cantor normal form sequence of ordinal numbers is defined by

(Def. 4) $\sum it = a$.

Note that $\sum \text{CNF}(a)$ reduces to a. Let A be a Cantor normal form sequence of ordinal numbers. One can check that $\text{CNF}(\sum A)$ reduces to A.

Now we state the proposition:

(55) $\text{CNF}(\emptyset) = \emptyset$.

Let a be an empty ordinal number. Note that CNF(a) is empty.

Let a be a non empty ordinal number. Note that CNF(a) is non empty.

Now we state the propositions:

(56) Let us consider an ordinal number a, and a non zero natural number n. Then $\text{CNF}(n \cdot \omega^a) = \langle n \cdot \omega^a \rangle$.

(57) Let us consider a Cantor component ordinal number a. Then $\text{CNF}(a) = \langle a \rangle$.

(58) Let us consider a non zero natural number n. Then $\text{CNF}(n) = \langle n \rangle$.

(59) Let us consider a non empty ordinal number a, and non zero natural numbers n, m. Then $\text{CNF}(n \cdot \omega^a + m) = \langle n \cdot \omega^a, m \rangle$. The theorem is a consequence of (12).

(60) Let us consider a non empty ordinal number a, an ordinal number b, and a non zero natural number n. Suppose $b \in \omega$-exponent(last CNF(a)). Then $\text{CNF}(a + n \cdot \omega^b) = \text{CNF}(a) \frown \langle n \cdot \omega^b \rangle$. The theorem is a consequence of (24).

(61) Let us consider a non empty ordinal number a, and a non zero natural number n. Suppose ω-exponent(last CNF(a)) $\neq 0$. Then CNF$(a + n) =$ CNF$(a) \frown \langle n \rangle$. The theorem is a consequence of (60).

(62) Let us consider a non empty ordinal number a, an ordinal number b, and a non zero natural number n. Suppose ω-exponent((CNF(a))(0)) $\in b$. Then CNF$(n \cdot \omega^b + a) = \langle n \cdot \omega^b \rangle \frown$ CNF(a). The theorem is a consequence of (26).

3. Natural Addition of Ordinals

Let a, b be ordinal numbers. The functor $a \oplus b$ yielding an ordinal number is defined by

(Def. 5) there exists a Cantor normal form sequence C of ordinal numbers such that *it* $= \sum C$ and rng(ω-exponent(C)) $=$ rng(ω-exponent(CNF(a))) $\cup$ rng(ω-exponent(CNF(b))) and for every object d such that $d \in \operatorname{dom} C$ holds:

if ω-exponent($C(d)$) $\in$ rng(ω-exponent(CNF(a)))$\setminus$rng(ω-exponent(CNF (b))), then ω-LC($C(d)$) $=$ (ω-LC(CNF(a)))(((ω-exponent(CNF(a)))$^{-1}$) (ω-exponent($C(d)$))) and

if ω-exponent($C(d)$) $\in$ rng(ω-exponent(CNF(b)))$\setminus$rng(ω-exponent(CNF (a))), then ω-LC($C(d)$) $=$ (ω-LC(CNF(b)))(((ω-exponent(CNF(b)))$^{-1}$) (ω-exponent($C(d)$))) and

if ω-exponent($C(d)$) $\in$ rng(ω-exponent(CNF(a)))$\cap$rng(ω-exponent(CNF (b))), then ω-LC($C(d)$) $=$ (ω-LC(CNF(a)))(((ω-exponent(CNF(a)))$^{-1}$) (ω-exponent($C(d)$))) $+$ (ω-LC(CNF(b)))(((ω-exponent(CNF(b)))$^{-1}$) (ω-exponent($C(d)$))).

One can verify that the functor is commutative.

Let us consider ordinal numbers a, b. Now we state the propositions:

(63) rng(ω-exponent(CNF$(a \oplus b)$)) $=$
rng(ω-exponent(CNF(a))) $\cup$ rng(ω-exponent(CNF(b))).

(64) dom(CNF(a)) $\subseteq$ dom(CNF$(a \oplus b)$). The theorem is a consequence of (63).

Let us consider ordinal numbers a, b and an object d. Now we state the propositions:

(65) Suppose $d \in$ dom(CNF$(a \oplus b)$) and ω-exponent((CNF$(a \oplus b)$)(d)) $\in$ rng(ω-exponent(CNF(a))) $\setminus$ rng(ω-exponent(CNF(b))). Then ω-LC((CNF $(a \oplus b)$)(d)) $=$ (ω-LC(CNF(a)))(((ω-exponent(CNF(a)))$^{-1}$)(ω-exponent ((CNF$(a \oplus b)$)(d)))).

(66) Suppose $d \in \operatorname{dom}(\mathrm{CNF}(a \oplus b))$ and ω-exponent$((\mathrm{CNF}(a \oplus b))(d)) \in \operatorname{rng}(\omega\text{-exponent}(\mathrm{CNF}(b))) \setminus \operatorname{rng}(\omega\text{-exponent}(\mathrm{CNF}(a)))$. Then ω-LC$((\mathrm{CNF}(a \oplus b))(d)) = (\omega\text{-LC}(\mathrm{CNF}(b)))(((\omega\text{-exponent}(\mathrm{CNF}(b)))^{-1})(\omega\text{-exponent}((\mathrm{CNF}(a \oplus b))(d))))$.

(67) Suppose $d \in \operatorname{dom}(\mathrm{CNF}(a \oplus b))$ and ω-exponent$((\mathrm{CNF}(a \oplus b))(d)) \in \operatorname{rng}(\omega\text{-exponent}(\mathrm{CNF}(a))) \cap \operatorname{rng}(\omega\text{-exponent}(\mathrm{CNF}(b)))$. Then ω-LC$((\mathrm{CNF}(a \oplus b))(d)) = (\omega\text{-LC}(\mathrm{CNF}(a)))(((\omega\text{-exponent}(\mathrm{CNF}(a)))^{-1})(\omega\text{-exponent}((\mathrm{CNF}(a \oplus b))(d)))) + (\omega\text{-LC}(\mathrm{CNF}(b)))(((\omega\text{-exponent}(\mathrm{CNF}(b)))^{-1})(\omega\text{-exponent}((\mathrm{CNF}(a \oplus b))(d))))$.

(68) Let us consider ordinal numbers a, b, c. Then $(a \oplus b) \oplus c = a \oplus (b \oplus c)$.

(69) Let us consider an ordinal number a. Then $a \oplus 0 = a$.

(70) Let us consider ordinal numbers a, b, and a natural number n. Suppose ω-exponent$(a) \subseteq b$. Then $n \cdot \omega^b \oplus a = n \cdot \omega^b + a$. The theorem is a consequence of (31), (69), (56), (33), (21), (47), (44), (51), and (52).

(71) Let us consider finite sequences A, B of ordinal numbers. Suppose $A \frown B$ is Cantor normal form. Then $\sum A \oplus \sum B = \sum A + \sum B$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every finite sequences A, B of ordinal numbers such that $\operatorname{len} A = \$_1$ and $A \frown B$ is Cantor normal form holds $\sum A \oplus \sum B = \sum A + \sum B$. $\mathcal{P}[0]$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every natural number n, $\mathcal{P}[n]$. □

(72) Let us consider ordinal numbers a, b. Suppose if $a \neq 0$, then ω-exponent$(b) \in \omega$-exponent(last CNF(a)). Then $a \oplus b = a + b$. The theorem is a consequence of (69), (31), (20), and (71).

(73) Let us consider ordinal numbers a, b, and a natural number n. Suppose if $a \neq 0$, then $b \subseteq \omega$-exponent(last CNF(a)). Then $a \oplus n \cdot \omega^b = a + n \cdot \omega^b$. The theorem is a consequence of (69), (16), (70), (11), (71), (68), and (12).

(74) Let us consider an ordinal number a, and natural numbers n, m. Then $n \cdot \omega^a \oplus m \cdot \omega^a = (n + m) \cdot \omega^a$. The theorem is a consequence of (69), (56), and (73).

(75) Let us consider an ordinal number a, and a natural number n. Then $a \oplus n = a + n$. The theorem is a consequence of (73).

(76) Let us consider natural numbers n, m. Then $n \oplus m = n + m$. The theorem is a consequence of (75).

Let n, m be natural numbers. We identify $n + m$ with $n \oplus m$. Now we state the propositions:

(77) Let us consider an ordinal number a. Then $a \oplus 1 = \operatorname{succ} a$. The theorem is a consequence of (75).

(78) Let us consider ordinal numbers a, b. Then $a \oplus \operatorname{succ} b = \operatorname{succ}(a \oplus b)$. The theorem is a consequence of (77) and (68).

Let a be an empty ordinal number. Let us note that $a \oplus a$ is empty.

Let a be a non empty ordinal number and b be an ordinal number. Let us note that $a \oplus b$ is non empty. Now we state the proposition:

(79) Let us consider an ordinal number a. Then a is limit ordinal if and only if $0 \notin \operatorname{rng}(\omega\text{-exponent}(\mathrm{CNF}(a)))$. The theorem is a consequence of (16), (46), (38), (77), (58), (33), and (8).

Let a, b be limit ordinal ordinal numbers. Let us note that $a \oplus b$ is limit ordinal. Let a be an ordinal number and b be a non limit ordinal ordinal number. One can check that $a \oplus b$ is non limit ordinal.

Now we state the propositions:

(80) Let us consider ordinal numbers a, b, and a non zero natural number n. Suppose $n \cdot \omega^b \subseteq a$ and $a \in (n+1) \cdot \omega^b$. Then $(\mathrm{CNF}(a))(0) = n \cdot \omega^b$.
Proof: Consider a_0 being a Cantor component ordinal number, A_0 being a Cantor normal form sequence of ordinal numbers such that $\mathrm{CNF}(a) = \langle a_0 \rangle \mathbin{^\frown} A_0$. $b \subseteq \omega\text{-exponent}(a) \subseteq b$. Reconsider $m = \omega\text{-LC}((\mathrm{CNF}(a))(0))$ as a natural number. $(\mathrm{CNF}(a))(0) = m \cdot \omega^b$. $m = n$. □

(81) Let us consider ordinal numbers a, b. Suppose $\operatorname{rng}(\omega\text{-exponent}(\mathrm{CNF}(a))) = \operatorname{rng}(\omega\text{-exponent}(\mathrm{CNF}(b)))$. Let us consider an ordinal number c. Suppose $c \in \operatorname{dom}(\mathrm{CNF}(a))$. Then $(\omega\text{-LC}(\mathrm{CNF}(a \oplus b)))(c) = (\omega\text{-LC}(\mathrm{CNF}(a)))(c) + (\omega\text{-LC}(\mathrm{CNF}(b)))(c)$. The theorem is a consequence of (21).

Let us consider ordinal numbers a, b. Now we state the propositions:

(82) (i) if $\omega\text{-exponent}((\mathrm{CNF}(a \oplus b))(0)) \in \operatorname{rng}(\omega\text{-exponent}(\mathrm{CNF}(a)))$, then $\omega\text{-exponent}((\mathrm{CNF}(a \oplus b))(0)) = (\omega\text{-exponent}(\mathrm{CNF}(a)))(0)$, and

(ii) if $\omega\text{-exponent}((\mathrm{CNF}(a \oplus b))(0)) \in \operatorname{rng}(\omega\text{-exponent}(\mathrm{CNF}(b)))$, then $\omega\text{-exponent}((\mathrm{CNF}(a \oplus b))(0)) = (\omega\text{-exponent}(\mathrm{CNF}(b)))(0)$.

Proof: Set $E_1 = \omega\text{-exponent}(\mathrm{CNF}(a))$. Set $E_2 = \omega\text{-exponent}(\mathrm{CNF}(b))$. Set $C_0 = \mathrm{CNF}(a \oplus b)$. $\operatorname{rng}(\omega\text{-exponent}(C_0)) = \operatorname{rng} E_1 \cup \operatorname{rng} E_2$. Consider x being an object such that $x \in \operatorname{dom} E_2$ and $E_2(x) = \omega\text{-exponent}(C_0(0))$. $x = 0$. □

(83) (i) if $\omega\text{-exponent}((\mathrm{CNF}(a \oplus b))(0)) \in \operatorname{rng}(\omega\text{-exponent}(\mathrm{CNF}(a))) \setminus \operatorname{rng}(\omega\text{-exponent}(\mathrm{CNF}(b)))$, then $(\mathrm{CNF}(a \oplus b))(0) = (\mathrm{CNF}(a))(0)$, and

(ii) if $\omega\text{-exponent}((\mathrm{CNF}(a \oplus b))(0)) \in \operatorname{rng}(\omega\text{-exponent}(\mathrm{CNF}(b))) \setminus \operatorname{rng}(\omega\text{-exponent}(\mathrm{CNF}(a)))$, then $(\mathrm{CNF}(a \oplus b))(0) = (\mathrm{CNF}(b))(0)$, and

(iii) if $\omega\text{-exponent}((\mathrm{CNF}(a \oplus b))(0)) \in \operatorname{rng}(\omega\text{-exponent}(\mathrm{CNF}(a))) \cap \operatorname{rng}(\omega\text{-exponent}(\mathrm{CNF}(b)))$, then $(\mathrm{CNF}(a \oplus b))(0) = (\mathrm{CNF}(a))(0) + (\mathrm{CNF}(b))(0)$.

The theorem is a consequence of (82), (51), and (52).

Let us consider ordinal numbers a, b and an object x. Now we state the propositions:

(84) $(\omega\text{-exponent}(\mathrm{CNF}(a)))(x) \subseteq (\omega\text{-exponent}(\mathrm{CNF}(a \oplus b)))(x)$.
PROOF: Set $E_1 = \omega\text{-exponent}(\mathrm{CNF}(a))$. Set $E_2 = \omega\text{-exponent}(\mathrm{CNF}(b))$. Set $C_0 = \mathrm{CNF}(a \oplus b)$. Define $\mathcal{P}[\text{ordinal number}] \equiv (\omega\text{-exponent}(C_0))(\$_1) \in E_1(\$_1)$. There exists an ordinal number z such that $\mathcal{P}[z]$. Consider y being an ordinal number such that $\mathcal{P}[y]$ and for every ordinal number z such that $\mathcal{P}[z]$ holds $y \subseteq z$. $\mathrm{rng}(\omega\text{-exponent}(C_0)) = \mathrm{rng}\, E_1 \cup \mathrm{rng}\, E_2$. Consider z being an object such that $z \in \mathrm{dom}(\omega\text{-exponent}(C_0))$ and $(\omega\text{-exponent}(C_0))(z) = E_1(y)$. $z \in y$. □

(85) $(\mathrm{CNF}(a))(x) \subseteq (\mathrm{CNF}(a \oplus b))(x)$.
PROOF: Set $E_1 = \omega\text{-exponent}(\mathrm{CNF}(a))$. Set $E_2 = \omega\text{-exponent}(\mathrm{CNF}(b))$. Set $L_1 = \omega\text{-LC}(\mathrm{CNF}(a))$. Set $L_2 = \omega\text{-LC}(\mathrm{CNF}(b))$. Set $C_0 = \mathrm{CNF}(a \oplus b)$.

Consider C being a Cantor normal form sequence of ordinal numbers such that $a \oplus b = \sum C$ and $\mathrm{rng}(\omega\text{-exponent}(C)) = \mathrm{rng}\, E_1 \cup \mathrm{rng}\, E_2$ and for every object d such that $d \in \mathrm{dom}\, C$ holds if $\omega\text{-exponent}(C(d)) \in \mathrm{rng}\, E_1 \setminus \mathrm{rng}\, E_2$, then $\omega\text{-LC}(C(d)) = L_1(({E_1}^{-1})(\omega\text{-exponent}(C(d))))$ and if $\omega\text{-exponent}(C(d)) \in \mathrm{rng}\, E_2 \setminus \mathrm{rng}\, E_1$, then $\omega\text{-LC}(C(d)) = L_2(({E_2}^{-1})(\omega\text{-exponent}(C(d))))$ and if $\omega\text{-exponent}(C(d)) \in \mathrm{rng}\, E_1 \cap \mathrm{rng}\, E_2$, then $\omega\text{-LC}(C(d)) = L_1(({E_1}^{-1})(\omega\text{-exponent}(C(d)))) + L_2(({E_2}^{-1})(\omega\text{-exponent}(C(d))))$.

$\mathrm{dom}(\mathrm{CNF}(a)) \subseteq \mathrm{dom}(\mathrm{CNF}(a \oplus b))$. $C_0(x) = (\omega\text{-LC}(C_0))(x) \cdot \omega^{(\omega\text{-exponent}(C_0))(x)}$. $(\mathrm{CNF}(a))(x) = L_1(x) \cdot \omega^{E_1(x)}$. $E_1(x) = (\omega\text{-exponent}(C_0))(x)$. □

Let us consider ordinal numbers a, b. Now we state the propositions:

(86) $a \subseteq a \oplus b$. The theorem is a consequence of (64), (85), and (15).

(87) $\omega\text{-exponent}(a \oplus b) = (\omega\text{-exponent}(a)) \cup (\omega\text{-exponent}(b))$. The theorem is a consequence of (9), (86), (63), (82), and (31).

(88) Let us consider ordinal numbers a, b, c. If $a, b \in \omega^c$, then $a \oplus b \in \omega^c$. The theorem is a consequence of (69), (10), and (87).

The scheme *OrdinalCNFIndA* deals with a unary predicate $\mathcal{P}$ and states that

(Sch. 1) For every non empty ordinal number a, $\mathcal{P}[a]$

provided

- for every ordinal number a and for every non zero natural number n, $\mathcal{P}[n \cdot \omega^a]$ and

- for every ordinal number a and for every non empty ordinal number b and for every non zero natural number n such that $\mathcal{P}[b]$ and $a \notin \operatorname{rng}(\omega\text{-exponent}(\mathrm{CNF}(b)))$ holds $\mathcal{P}[b \oplus n \cdot \omega^a]$.

The scheme *OrdinalCNFIndB* deals with a unary predicate $\mathcal{P}$ and states that

(Sch. 2) For every non empty ordinal number a, $\mathcal{P}[a]$

provided

- for every ordinal number a, $\mathcal{P}[\omega^a]$ and

- for every ordinal number a and for every non zero natural number n such that $\mathcal{P}[n \cdot \omega^a]$ holds $\mathcal{P}[(n+1) \cdot \omega^a]$ and

- for every ordinal number a and for every non empty ordinal number b and for every non zero natural number n such that $\mathcal{P}[b]$ and $a \notin \operatorname{rng}(\omega\text{-exponent}(\mathrm{CNF}(b)))$ holds $\mathcal{P}[b \oplus n \cdot \omega^a]$.

The scheme *OrdinalCNFIndC* deals with a unary predicate $\mathcal{P}$ and states that

(Sch. 3) For every non empty ordinal number a, $\mathcal{P}[a]$

provided

- for every ordinal number a, $\mathcal{P}[\omega^a]$ and

- for every ordinal number a and for every non empty ordinal number b such that $\mathcal{P}[b]$ holds $\mathcal{P}[b \oplus \omega^a]$.

Now we state the propositions:

(89) Let us consider ordinal numbers a, b.
Suppose $\omega\text{-exponent}(a) \in \omega\text{-exponent}(b)$. Then $a \in \omega^{\omega\text{-exponent}(b)}$.
Proof: Define $\mathcal{P}$[non empty ordinal number] $\equiv$ for every ordinal number b such that $\omega\text{-exponent}(\$_1) \in \omega\text{-exponent}(b)$ holds $\$_1 \in \omega^{\omega\text{-exponent}(b)}$. For every ordinal number c and for every non zero natural number n, $\mathcal{P}[n \cdot \omega^c]$. For every ordinal number c and for every non empty ordinal number d and for every non zero natural number n such that $\mathcal{P}[d]$ and $c \notin \operatorname{rng}(\omega\text{-exponent}(\mathrm{CNF}(d)))$ holds $\mathcal{P}[d \oplus n \cdot \omega^c]$. For every non empty ordinal number a, $\mathcal{P}[a]$. □

(90) Let us consider non empty ordinal numbers a, b. Then $\omega \cdot a \subseteq b$ if and only if $\omega\text{-exponent}(a) \in \omega\text{-exponent}(b)$. The theorem is a consequence of (89) and (29).

Let us consider ordinal numbers a, b. Now we state the propositions:

(91) If ω-exponent$(a) \in \omega$-exponent(b), then $b - a = b$. The theorem is a consequence of (90), (17), and (89).

(92) $a + b \subseteq a \oplus b$.

Proof: Define $\mathcal{P}$[natural number] $\equiv$ for every non empty ordinal numbers a, b such that $\operatorname{len} \mathrm{CNF}(a) = \$_1$ holds $a + b \subseteq a \oplus b$. $\mathcal{P}[1]$. For every non zero natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every non zero natural number n, $\mathcal{P}[n]$. □

Let us consider ordinal numbers a, b, c. Now we state the propositions:

(93) If $a \oplus b = a \oplus c$, then $b = c$.

Proof: Set $E_2 = \omega$-exponent$(\mathrm{CNF}(b))$. Set $E_3 = \omega$-exponent$(\mathrm{CNF}(c))$. Set $L_2 = \omega$-LC$(\mathrm{CNF}(b))$. Set $L_3 = \omega$-LC$(\mathrm{CNF}(c))$. $\operatorname{rng} E_2 = \operatorname{rng} E_3$. $E_2 = E_3$. For every object x such that $x \in \operatorname{dom} L_2$ holds $L_2(x) = L_3(x)$. $\sum \mathrm{CNF}(b) = \sum \mathrm{CNF}(c)$. □

(94) If $b \in c$, then $a \oplus b \in a \oplus c$. The theorem is a consequence of (69), (11), (71), and (68).

(95) If $b \subseteq c$, then $a \oplus b \subseteq a \oplus c$. The theorem is a consequence of (94).

References

[1] Alexander Abian. *The theory of sets and transfinite arithmetic.* Saunders mathematics books. Saunders, Philadelphia [u.a.], 1965.

[2] Heinz Bachmann. *Transfinite Zahlen.* Ergebnisse der Mathematik und ihrer Grenzgebiete, (1). Springer, Berlin [u.a.], 2., neubearb. aufl. edition, 1967.

[3] Grzegorz Bancerek. Epsilon numbers and Cantor normal form. *Formalized Mathematics*, 17(**4**):249–256, 2009. doi:10.2478/v10037-009-0032-8.

[4] Georg Cantor. Beiträge zur begründung der transfiniten mengenlehre. *Mathematische Annalen*, 49(2):207–246, 1897.

[5] Oliver Deiser. *Einführung in die Mengenlehre: die Mengenlehre Georg Cantors und ihre Axiomatisierung durch Ernst Zermelo.* Springer, Berlin [u.a.], 2., verb. und erw. aufl. edition, 2004. ISBN 3-540-20401-6.

[6] Adam Grabowski, Artur Korniłowicz, and Adam Naumowicz. Four decades of Mizar. *Journal of Automated Reasoning*, 55(3):191–198, 2015. doi:10.1007/s10817-015-9345-1.

[7] Piotr Rudnicki and Andrzej Trybulec. Multivariate polynomials with arbitrary number of variables. *Formalized Mathematics*, 9(**1**):95–110, 2001.

[8] Wacław Sierpiński. *Cardinal and ordinal numbers.* Polska Akademia Nauk. Monografie matematyczne, (34) (in Polish). PWN, Warszawa, 2. ed., rev edition, 1965.

[9] Tetsuya Tsunetou, Grzegorz Bancerek, and Yatsuka Nakamura. Zero-based finite sequences. *Formalized Mathematics*, 9(**4**):825–829, 2001.

Accepted May 27, 2019

FORMALIZED MATHEMATICS
Vol. 27, No. 2, Pages 153–179, 2019
DOI: 10.2478/forma-2019-0016

sciendo
https://www.sciendo.com/

About Supergraphs. Part III

Sebastian Koch
Johannes Gutenberg University
Mainz, Germany[1]

Summary. The previous articles [5] and [6] introduced formalizations of the step-by-step operations we use to construct finite graphs by hand. That implicitly showed that any finite graph can be constructed from the trivial edgeless graph K_1 by applying a finite sequence of these basic operations. In this article that claim is proven explicitly with Mizar[4].

MSC: 05C76 68T99 03B35

Keywords: supergraph; graph operations; construction of finite graphs

MML identifier: GLIB_008, version: 8.1.09 5.57.1355

0. Introduction

In the literature a mutual understanding how the graphical representation of graphs is to be translated into a description fitting the set-theoretic definition is usually assumed (cf. [9], [3], [8], [2]), but in Mizar we need explicit operations, which were provided in [5] and [6].

The rather extensive preliminaries contain many theorems that would fit well into earlier articles of the GLIB series, for example:

- In a simple graph, the degree of a vertex equals the cardinality of its neighbors.
- The operations of removing a vertex or an edge in a graph commute.
- Every finite connected graph has a spanning tree.

[1] The author is enrolled in the Johannes Gutenberg University in Mayence, Germany, mailto: skoch02@students.uni-mainz.de

- Endvertices are no cut vertices.

Graphs without edges are rigorously introduced in the following section. Wilson calls those *null graphs* ([9]). Bondy and Murty call them *empty graphs* ([3]), while naming the graph without vertices *the null graph.* Both notations are common in the literature. To avoid confusion those graphs are simply introduced as `edgeless` here.

To describe the construction of finite graphs starting from the trivial edgeless K_1, finite sequences yielding graphs are needed, which are introduced in the next section expanding the notation from [7], [1].

The last section contains the formalizations of the main results:

- Adding n vertices to a graph can be done by adding one vertex after another.
- Any finite edgeless graph can be constructed from K_1 by adding one vertex at a time.
- Any finite (connected) graph can be reconstructed from a spanning (connected) subgraph by adding one edge at a time.
- Any finite graph can be constructed from K_1 by adding one vertex or one edge at a time.
- Any finite tree can be constructed from K_1 by adding one vertex and an edge incident with that vertex at a time.
- Any finite connected graph can be constructed from K_1 by adding one edge or one vertex and an edge incident with that vertex at a time.
- Adding a vertex to a graph and connecting it to a (possibly empty) subset of the vertices of said graph can be done by first adding the new vertex and then adding one edge at a time.
- Any finite simple graph can be constructed from K_1 by adding one vertex connecting it to a (possibly empty) subset of the vertices of the previous contruction step at a time.
- If the finite simple graph is also connected, the subset of adjacent vertices can be guarantied to be non empty.

The number of operations needed is given for each process in terms of order and size of the involved graphs. Some proof schemes are presented to make use of these constructions.

1. Preliminaries

Let G be a graph and v be a vertex of G. Let us observe that every subgraph of G induced by $\{v\}$ is trivial.

Let us consider a graph G, a set X, and a vertex v of G. Now we state the propositions:

(1) G.edgesBetween$(X \setminus \{v\}) = G$.edgesBetween$(X) \setminus v$.edgesInOut().

(2) If v is isolated, then G.edgesBetween$(X \setminus \{v\}) = G$.edgesBetween(X).
The theorem is a consequence of (1).

Let us consider a non-directed-multi graph G and a vertex v of G. Now we state the propositions:

(3) v.inDegree() $= \overline{\overline{v\text{.inNeighbors()}}}$.
Proof: Define $\mathcal{P}[\text{object}, \text{object}] \equiv \$_2$ joins $\$_1$ to v in G. Consider f being a function such that $\operatorname{dom} f = v$.inNeighbors() and for every object x such that $x \in v$.inNeighbors() holds $\mathcal{P}[x, f(x)]$. f is a bijection between v.inNeighbors() and v.edgesIn(). □

(4) v.outDegree() $= \overline{\overline{v\text{.outNeighbors()}}}$.
Proof: Define $\mathcal{P}[\text{object}, \text{object}] \equiv \$_2$ joins v to $\$_1$ in G. Consider f being a function such that $\operatorname{dom} f = v$.outNeighbors() and for every object x such that $x \in v$.outNeighbors() holds $\mathcal{P}[x, f(x)]$. f is a bijection between v.outNeighbors() and v.edgesOut(). □

(5) Let us consider a simple graph G, and a vertex v of G. Then v.degree() $= \overline{\overline{v\text{.allNeighbors()}}}$.
Proof: v.inNeighbors() $\cap\, v$.outNeighbors() $= \emptyset$. □

(6) Let us consider a graph G. Then G is loopless if and only if for every vertex v of G, $v \notin v$.allNeighbors().
Proof: For every object v, there exists no object e such that e joins v and v in G. □

(7) Let us consider a graph G, and a vertex v of G. Then v is isolated if and only if v.allNeighbors() $= \emptyset$.

(8) Let us consider a graph G_1, a set v, and a subgraph G_2 of G_1 with vertex v removed. Suppose G_1 is trivial or $v \notin$ the vertices of G_1. Then $G_1 \approx G_2$.

(9) Let us consider graphs G_1, G_2, and a set v. Suppose $G_1 \approx G_2$ and (G_1 is trivial or $v \notin$ the vertices of G_1). Then G_2 is a subgraph of G_1 with vertex v removed.

(10) Let us consider a graph G. Suppose there exist vertices v_1, v_2 of G such that $v_1 \neq v_2$. Then G is not trivial.
Proof: $\overline{\overline{\alpha}} \neq 1$, where α is the vertices of G. □

Let G be a non trivial graph and X be a set. Let us note that every subgraph of G with edges X removed is non trivial. Now we state the propositions:

(11) Let us consider a finite graph G_1, and a subgraph G_2 of G_1. Then G_2 is spanning if and only if G_1.order() $= G_2$.order().

(12) Let us consider a graph G_1, and a spanning subgraph G_2 of G_1. Suppose the edges of $G_1 =$ the edges of G_2. Then $G_1 \approx G_2$.

(13) Let us consider a finite graph G_1, and a spanning subgraph G_2 of G_1. If G_1.size() $= G_2$.size(), then $G_1 \approx G_2$. The theorem is a consequence of (12).

(14) Let us consider a graph G_1, a set V, and a subgraph G_2 of G_1 induced by V. If G_2 is spanning, then $G_1 \approx G_2$.

Let us consider a graph G. Now we state the propositions:

(15) G is not trivial if and only if there exists a subgraph H of G such that H is not spanning.

(16) If there exists a vertex v of G such that v is endvertex, then G is not trivial.

Proof: Consider e being an object such that v.edgesInOut() $= \{e\}$ and e does not join v and v in G. For every vertex u of G, the vertices of $G \neq \{u\}$. □

(17) Let us consider a graph G_1, sets v, e, a subgraph G_2 of G_1 with vertex v removed, and a subgraph G_3 of G_1 with edge e removed. Then every subgraph of G_2 with edge e removed is a subgraph of G_3 with vertex v removed. The theorem is a consequence of (1), (8), and (9).

(18) Let us consider a graph G_1, sets v, e, a subgraph G_2 of G_1 with edge e removed, and a subgraph G_3 of G_1 with vertex v removed. Then every subgraph of G_2 with vertex v removed is a subgraph of G_3 with edge e removed. The theorem is a consequence of (1) and (8).

Let G be a finite, connected graph. Note that there exists a subgraph of G which is spanning, tree-like, connected, and acyclic.

Now we state the propositions:

(19) Let us consider a connected graph G_1, and a subgraph G_2 of G_1. Suppose the edges of $G_1 \subseteq$ the edges of G_2. Then $G_1 \approx G_2$.

Proof: The vertices of $G_1 =$ the vertices of G_2. □

(20) Let us consider a finite, connected graph G_1, and a subgraph G_2 of G_1. If G_1.size() $= G_2$.size(), then $G_1 \approx G_2$. The theorem is a consequence of (19).

(21) Let us consider a finite, tree-like graph G_1, and a spanning, tree-like subgraph G_2 of G_1. Then $G_1 \approx G_2$. The theorem is a consequence of (11)

and (13).

Let G be a non trivial graph. Observe that there exists a subgraph of G which is non spanning, trivial, and connected.

Now we state the propositions:

(22) Let us consider a graph G, and vertices v_1, v_2 of G. Suppose $v_1 \notin G.\mathrm{reachableFrom}(v_2)$.
Then $G.\mathrm{reachableFrom}(v_1)$ misses $G.\mathrm{reachableFrom}(v_2)$.

(23) Let us consider a graph G. Then $G.\mathrm{componentSet}()$ is a partition of the vertices of G.
Proof: Set $V =$ the vertices of G. For every subset A of V such that $A \in G.\mathrm{componentSet}()$ holds $A \neq \emptyset$ and for every subset B of V such that $B \in G.\mathrm{componentSet}()$ holds $A = B$ or A misses B. □

(24) Let us consider a graph G, a partition C of the vertices of G, and a vertex v of G. If $C = G.\mathrm{componentSet}()$,
then $\mathrm{EqClass}(v, C) = G.\mathrm{reachableFrom}(v)$.

(25) Let us consider a graph G_1, vertices v_0, v_1 of G_1, a subgraph G_2 of G_1 with vertex v_0 removed, and a vertex v_2 of G_2. Suppose v_0 is endvertex and $v_1 = v_2$ and $v_1 \in G_1.\mathrm{reachableFrom}(v_0)$. Then $G_2.\mathrm{reachableFrom}(v_2) = (G_1.\mathrm{reachableFrom}(v_1)) \setminus \{v_0\}$.
Proof: G_1 is not trivial. For every object w, $w \in G_2.\mathrm{reachableFrom}(v_2)$ iff $w \in G_1.\mathrm{reachableFrom}(v_1)$ and $w \notin \{v_0\}$. □

(26) Let us consider a non trivial graph G_1, vertices v_0, v_1 of G_1, a subgraph G_2 of G_1 with vertex v_0 removed, and a vertex v_2 of G_2. Suppose $v_1 = v_2$ and $v_1 \notin G_1.\mathrm{reachableFrom}(v_0)$. Then $G_2.\mathrm{reachableFrom}(v_2) = G_1.\mathrm{reachableFrom}(v_1)$.
Proof: For every object w such that $w \in G_1.\mathrm{reachableFrom}(v_1)$ holds $w \in G_2.\mathrm{reachableFrom}(v_2)$. □

(27) Let us consider a non trivial, finite, tree-like graph G, and a vertex v of G. If $G.\mathrm{order}() = 2$, then v is endvertex.

Let G be a non trivial, connected graph and v be a vertex of G. Observe that $v.\mathrm{allNeighbors}()$ is non empty.

Now we state the propositions:

(28) Let us consider a tree T, and a vertex a of T. Then $T.\mathrm{pathBetween}(a, a) = T.\mathrm{walkOf}(a)$.

(29) Let us consider a tree T, vertices a, b of T, and an object e. If e joins a and b in T, then $T.\mathrm{pathBetween}(a, b) = T.\mathrm{walkOf}(a, e, b)$.

(30) Let us consider a non trivial, finite tree T, and a vertex v of T. Then there exist vertices v_1, v_2 of T such that

(i) $v_1 \neq v_2$, and

(ii) v_1 is endvertex, and

(iii) v_2 is endvertex, and

(iv) $v \in (T.\text{pathBetween}(v_1, v_2)).\text{vertices}()$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv$ for every non trivial, finite tree T for every vertex v of T such that $T.\text{order}() = \$_1 + 2$ there exist vertices v_1, v_2 of T such that $v_1 \neq v_2$ and v_1 is endvertex and v_2 is endvertex and $v \in (T.\text{pathBetween}(v_1, v_2)).\text{vertices}()$. $\mathcal{P}[0]$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every natural number k, $\mathcal{P}[k]$. Consider k being a natural number such that $T.\text{order}() = 2 + k$. □

(31) Let us consider a non trivial, finite, tree-like graph G_1, and a non spanning, connected subgraph G_2 of G_1. Then there exists a vertex v of G_1 such that

(i) v is endvertex, and

(ii) $v \notin$ the vertices of G_2.

The theorem is a consequence of (30).

(32) Let us consider graphs G_2, G_3, a set V, and a supergraph G_1 of G_2 extended by the vertices from V. Suppose $G_2 \approx G_3$. Then G_1 is a supergraph of G_3 extended by the vertices from V.

(33) Let us consider a graph G_2, and a supergraph G_1 of G_2. Suppose the edges of $G_1 =$ the edges of G_2. Then G_1 is a supergraph of G_2 extended by the vertices from (the vertices of G_1) $\setminus$ (the vertices of G_2).

(34) Let us consider a finite graph G_1, and a subgraph G_2 of G_1. Suppose $G_1.\text{size}() = G_2.\text{size}()$. Then G_1 is a supergraph of G_2 extended by the vertices from (the vertices of G_1) $\setminus$ (the vertices of G_2). The theorem is a consequence of (33).

(35) Let us consider a non trivial graph G_1, a vertex v of G_1, and a subgraph G_2 of G_1 with vertex v removed. If v is isolated, then G_1 is a supergraph of G_2 extended by v. The theorem is a consequence of (2).

(36) Let us consider graphs G_2, G_3, objects v_1, e, v_2, and a supergraph G_1 of G_2 extended by e between vertices v_1 and v_2. Suppose $G_2 \approx G_3$. Then G_1 is a supergraph of G_3 extended by e between vertices v_1 and v_2.

(37) Let us consider a graph G_1, a set e, and a subgraph G_2 of G_1 with edge e removed. Suppose $e \in$ the edges of G_1. Then G_1 is a supergraph of G_2 extended by e between vertices (the source of G_1)(e) and (the target of G_1)(e).

Proof: Set $u =$ (the source of G_1)(e). Set $w =$ (the target of G_1)(e). For every object e_0 such that $e_0 \in \text{dom}$(the source of G_1) holds (the source of

$G_1)(e_0) = (($the source of $G_2)+\cdot(e \dot{\longmapsto} u))(e_0)$. For every object e_0 such that $e_0 \in \operatorname{dom}($the target of $G_1)$ holds (the target of $G_1)(e_0) = (($the target of $G_2)+\cdot(e \dot{\longmapsto} w))(e_0)$. □

(38) Let us consider a non trivial graph G_1, a vertex v of G_1, an object e, and a subgraph G_2 of G_1 with vertex v removed. Suppose $\{e\} = v.\mathrm{edgesInOut}()$ and e does not join v and v in G_1. Then G_1 is supergraph of G_2 extended by $v.\mathrm{adj}(e)$, v and e between them or supergraph of G_2 extended by v, $v.\mathrm{adj}(e)$ and e between them. The theorem is a consequence of (1).

(39) Let us consider a graph G_2, vertices v_1, v_2 of G_2, an object e, a supergraph G_1 of G_2 extended by e between vertices v_1 and v_2, a vertex w of G_1, and a vertex v of G_2. Suppose $v_2 \in G_2.\mathrm{reachableFrom}(v_1)$ and $v = w$. Then $G_1.\mathrm{reachableFrom}(w) = G_2.\mathrm{reachableFrom}(v)$.

(40) Let us consider a graph G_2, vertices v_1, v_2 of G_2, an object e, and a supergraph G_1 of G_2 extended by e between vertices v_1 and v_2. Suppose $v_2 \in G_2.\mathrm{reachableFrom}(v_1)$. Then $G_1.\mathrm{componentSet}() = G_2.\mathrm{componentSet}()$. The theorem is a consequence of (39).

(41) Let us consider a graph G_2, vertices v_1, v_2 of G_2, an object e, a supergraph G_1 of G_2 extended by e between vertices v_1 and v_2, and vertices w_1, w_2 of G_1. Suppose $e \notin$ the edges of G_2 and $w_1 = v_1$ and $w_2 = v_2$. Then $w_2 \in G_1.\mathrm{reachableFrom}(w_1)$.

(42) Let us consider a graph G_2, vertices v_1, v_2 of G_2, an object e, a supergraph G_1 of G_2 extended by e between vertices v_1 and v_2, and a vertex w_1 of G_1. Suppose $e \notin$ the edges of G_2 and $w_1 = v_1$. Then $G_1.\mathrm{reachableFrom}(w_1) = (G_2.\mathrm{reachableFrom}(v_1)) \cup (G_2.\mathrm{reachableFrom}(v_2))$.

Proof: For every object x such that $x \in G_1.\mathrm{reachableFrom}(w_1)$ holds $x \in (G_2.\mathrm{reachableFrom}(v_1)) \cup (G_2.\mathrm{reachableFrom}(v_2))$. $G_2.\mathrm{reachableFrom}(v_2) \subseteq G_1.\mathrm{reachableFrom}(w_1)$. □

(43) Let us consider a graph G_2, vertices v_1, v_2 of G_2, an object e, a supergraph G_1 of G_2 extended by e between vertices v_1 and v_2, a vertex w of G_1, and a vertex v of G_2. Suppose $e \notin$ the edges of G_2 and $v = w$ and $v \notin G_2.\mathrm{reachableFrom}(v_1)$ and $v \notin G_2.\mathrm{reachableFrom}(v_2)$. Then $G_1.\mathrm{reachableFrom}(w) = G_2.\mathrm{reachableFrom}(v)$.

Proof: For every object x such that $x \in G_1.\mathrm{reachableFrom}(w)$ holds $x \in G_2.\mathrm{reachableFrom}(v)$. □

(44) Let us consider a graph G_2, vertices v_1, v_2 of G_2, an object e, and a supergraph G_1 of G_2 extended by e between vertices v_1 and v_2. Suppose $e \notin$ the edges of G_2. Then $G_1.\mathrm{componentSet}() = (G_2.\mathrm{componentSet}() \setminus \{G_2.\mathrm{reachableFrom}(v_1), G_2.\mathrm{reachableFrom}(v_2)\}) \cup \{(G_2.\mathrm{reachableFrom}(v_1)) \cup (G_2.\mathrm{reachableFrom}(v_2))\}$.

(45) Let us consider a graph G_1, a vertex v of G_1, and a subgraph G_2 of G_1 with vertex v removed. If v is endvertex, then G_1.numComponents() $=$ G_2.numComponents().

PROOF: G_1 is not trivial. There exists a function f such that f is one-to-one and $\operatorname{dom} f = G_1$.componentSet() and $\operatorname{rng} f = G_2$.componentSet(). □

Let G be a graph. One can check that every vertex of G which is endvertex is also non cut-vertex. Now we state the propositions:

(46) Let us consider a non trivial, finite, connected graph G_1, and a non spanning, connected subgraph G_2 of G_1. Then there exists a vertex v of G_1 such that

(i) v is not cut-vertex, and

(ii) $v \notin$ the vertices of G_2.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every non trivial, finite, connected graph G_1 for every non spanning, connected subgraph G_2 of G_1 such that G_1.order() $+ \$_1 = G_1$.size() $+ 1$ there exists a vertex v of G_1 such that v is not cut-vertex and $v \notin$ the vertices of G_2. $\mathcal{P}[0]$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every natural number k, $\mathcal{P}[k]$. □

(47) Let us consider a non trivial, simple graph G_1, a vertex v of G_1, and a subgraph G_2 of G_1 with vertex v removed. Then G_1 is a supergraph of G_2 extended by vertex v and edges between v and v.allNeighbors() of G_2.

2. Edgeless and Non Edgeless Graphs

Let G be a graph. We say that G is edgeless if and only if

(Def. 1) the edges of $G = \emptyset$.

Let us consider a graph G. Now we state the propositions:

(48) G is edgeless if and only if $\overline{\overline{\alpha}} = 0$, where α is the edges of G.

(49) G is edgeless if and only if G.size() $= 0$.

Let G be a graph. Observe that every subgraph of G with edges the edges of G removed is edgeless and there exists a graph which is edgeless and there exists a subgraph of G which is edgeless and spanning and there exists a subgraph of G which is edgeless and trivial.

Let G be an edgeless graph. One can check that the edges of G is empty and every graph which is edgeless is also non-multi, non-directed-multi, loopless, simple, and directed-simple and every graph which is trivial and loopless is also edgeless.

Let V be a non empty set and S, T be functions from $\emptyset$ into V. One can check that createGraph$(V, \emptyset, S, T)$ is edgeless.

Now we state the propositions:

(50) Let us consider an edgeless graph G, and objects e, v_1, v_2. Then

(i) e does not join v_1 and v_2 in G, and

(ii) e does not join v_1 to v_2 in G.

(51) Let us consider an edgeless graph G, an object e, and sets X, Y. Then

(i) e does not join a vertex from X and a vertex from Y in G, and

(ii) e does not join a vertex from X to a vertex from Y in G.

(52) Let us consider graphs G_1, G_2. If $G_1 \approx G_2$, then if G_1 is edgeless, then G_2 is edgeless.

Let G be an edgeless graph. Let us observe that every walk of G is trivial and every subgraph of G is edgeless.

Let X be a set. Note that G.edgesInto(X) is empty and G.edgesOutOf(X) is empty and G.edgesInOut(X) is empty and G.edgesBetween(X) is empty and G.set(WeightSelector, X) is edgeless and G.set(ELabelSelector, X) is edgeless and G.set(VLabelSelector, X) is edgeless and every supergraph of G extended by the vertices from X is edgeless and every graph given by reversing directions of the edges X of G is edgeless.

Let Y be a set. Let us note that G.edgesBetween(X, Y) is empty and

G.edgesDBetween(X, Y) is empty and every graph which is edgeless is also acyclic and chordal and every graph which is trivial and edgeless is also tree-like and every graph which is non trivial and edgeless is also non connected, non tree-like, and non complete and every graph which is connected and edgeless is also trivial.

Now we state the propositions:

(53) Let us consider an edgeless graph G_1, and a subgraph G_2 of G_1. Then G_1 is a supergraph of G_2 extended by the vertices from (the vertices of G_1) $\setminus$ (the vertices of G_2). The theorem is a consequence of (33).

(54) Let us consider a graph G_2, vertices v_1, v_2 of G_2, an object e, and a supergraph G_1 of G_2 extended by e between vertices v_1 and v_2. Suppose $e \notin$ the edges of G_2. Then G_1 is not edgeless.

(55) Let us consider a graph G_2, a vertex v_1 of G_2, objects e, v_2, and a supergraph G_1 of G_2 extended by v_1, v_2 and e between them. Suppose $v_2 \notin$ the vertices of G_2 and $e \notin$ the edges of G_2. Then G_1 is not edgeless.

(56) Let us consider a graph G_2, objects v_1, e, a vertex v_2 of G_2, and a supergraph G_1 of G_2 extended by v_1, v_2 and e between them. Suppose

$v_1 \notin$ the vertices of G_2 and $e \notin$ the edges of G_2. Then G_1 is not edgeless.

(57) Let us consider a graph G_2, an object v, a non empty subset V of the vertices of G_2, and a supergraph G_1 of G_2 extended by vertex v and edges between v and V of G_2. Suppose $v \notin$ the vertices of G_2. Then G_1 is not edgeless.

Let G be a graph. Let us observe that every supergraph of G extended by vertex the vertices of G and edges from the vertices of G to the vertices of G is non edgeless and every supergraph of G extended by vertex the vertices of G and edges from the vertices of G to the vertices of G is non edgeless and every supergraph of G extended by vertex the vertices of G and edges between the vertices of G and the vertices of G is non edgeless.

Let v be a vertex of G. Let us note that every supergraph of G extended by v, the vertices of G and the edges of G between them is non edgeless and every supergraph of G extended by the vertices of G, v and the edges of G between them is non edgeless.

Let w be a vertex of G. Let us note that every supergraph of G extended by the edges of G between vertices v and w is non edgeless.

Let G be an edgeless graph. Note that every component of G is trivial and v.edgesIn() is empty and v.edgesOut() is empty and v.edgesInOut() is empty and every vertex of G is isolated, non cut-vertex, and non endvertex and v.inDegree() is empty and v.outDegree() is empty and v.inNeighbors() is empty and v.outNeighbors() is empty and v.degree() is empty and v.allNeighbors() is empty and there exists a graph which is trivial, finite, and edgeless and there exists a graph which is non trivial, finite, and edgeless and there exists a graph which is trivial, finite, and non edgeless and there exists a graph which is non trivial, finite, and non edgeless.

Let G be a non edgeless graph. One can check that the edges of G is non empty and every supergraph of G is non edgeless.

Let X be a set. One can verify that every graph given by reversing directions of the edges X of G is non edgeless and $G.\mathrm{set}(\mathrm{WeightSelector}, X)$ is non edgeless and $G.\mathrm{set}(\mathrm{ELabelSelector}, X)$ is non edgeless and $G.\mathrm{set}(\mathrm{VLabelSelector}, X)$ is non edgeless.

An edge of G is an element of the edges of G. Now we state the proposition:

(58) Let us consider a finite, edgeless graph G_1, and a subgraph G_2 of G_1. If G_1.order() $= G_2$.order(), then $G_1 \approx G_2$.

Let F be a graph-yielding function. We say that F is edgeless if and only if

(Def. 2) for every object x such that $x \in \operatorname{dom} F$ there exists a graph G such that $F(x) = G$ and G is edgeless.

Let F be a non empty, graph-yielding function. Note that F is edgeless if and only if the condition (Def. 3) is satisfied.

(Def. 3) for every element x of $\operatorname{dom} F$, $F(x)$ is edgeless.

Let S be a graph sequence. Let us note that S is edgeless if and only if the condition (Def. 4) is satisfied.

(Def. 4) for every natural number n, $S(n)$ is edgeless.

Let us observe that every graph-yielding function which is trivial and loopless is also edgeless and every graph-yielding function which is edgeless is also non-multi, non-directed-multi, loopless, simple, directed-simple, and acyclic.

Let F be an edgeless, non empty, graph-yielding function and x be an element of $\operatorname{dom} F$. Observe that $F(x)$ is edgeless.

Let S be an edgeless graph sequence and x be a natural number. Observe that $S(x)$ is edgeless.

3. Finite Graph Sequences

Let G be a graph. Note that $\langle G\rangle$ is graph-yielding.

Let G be a finite graph. Let us note that $\langle G\rangle$ is finite.

Let G be a loopless graph. Observe that $\langle G\rangle$ is loopless.

Let G be a trivial graph. Let us observe that $\langle G\rangle$ is trivial.

Let G be a non trivial graph. Let us observe that $\langle G\rangle$ is nontrivial.

Let G be a non-multi graph. One can verify that $\langle G\rangle$ is non-multi.

Let G be a non-directed-multi graph. One can check that $\langle G\rangle$ is non-directed-multi.

Let G be a simple graph. Note that $\langle G\rangle$ is simple.

Let G be a directed-simple graph. Let us note that $\langle G\rangle$ is directed-simple.

Let G be a connected graph. Observe that $\langle G\rangle$ is connected.

Let G be an acyclic graph. Let us observe that $\langle G\rangle$ is acyclic.

Let G be a tree-like graph. One can verify that $\langle G\rangle$ is tree-like.

Let G be an edgeless graph. One can check that $\langle G\rangle$ is edgeless and there exists a finite sequence which is empty and graph-yielding and there exists a finite sequence which is non empty and graph-yielding.

Let p be a non empty, graph-yielding finite sequence. Note that $p(1)$ is function-like and relation-like and $p(\operatorname{len} p)$ is function-like and relation-like and $p(1)$ is finite and $\mathbb{N}$-defined and $p(\operatorname{len} p)$ is finite and $\mathbb{N}$-defined and $p(1)$ is graph-like and $p(\operatorname{len} p)$ is graph-like and there exists a graph-yielding finite sequence which is non empty, finite, loopless, trivial, non-multi, non-directed-multi, simple, directed-simple, connected, acyclic, tree-like, and edgeless and there exists a graph-yielding finite sequence which is non empty, finite, loopless, nontrivial, non-multi, non-directed-multi, simple, directed-simple, connected, acyclic, and tree-like.

Let p be a graph-yielding finite sequence and n be a natural number. Let us observe that $p{\restriction}n$ is graph-yielding and $p_{\lfloor n}$ is graph-yielding.

Let m be a natural number. Note that $\mathrm{smid}(p, m, n)$ is graph-yielding and $\langle p(m), \ldots, p(n)\rangle$ is graph-yielding.

Let p be a finite, graph-yielding finite sequence. One can verify that $p{\restriction}n$ is finite and $p_{\lfloor n}$ is finite and $\mathrm{smid}(p, m, n)$ is finite and $\langle p(m), \ldots, p(n)\rangle$ is finite.

Let p be a loopless, graph-yielding finite sequence. One can verify that $p{\restriction}n$ is loopless and $p_{\lfloor n}$ is loopless and $\mathrm{smid}(p, m, n)$ is loopless and $\langle p(m), \ldots, p(n)\rangle$ is loopless.

Let p be a trivial, graph-yielding finite sequence. One can verify that $p{\restriction}n$ is trivial and $p_{\lfloor n}$ is trivial and $\mathrm{smid}(p, m, n)$ is trivial and $\langle p(m), \ldots, p(n)\rangle$ is trivial.

Let p be a nontrivial, graph-yielding finite sequence. One can verify that $p{\restriction}n$ is nontrivial and $p_{\lfloor n}$ is nontrivial and $\mathrm{smid}(p, m, n)$ is nontrivial and $\langle p(m), \ldots, p(n)\rangle$ is nontrivial.

Let p be a non-multi, graph-yielding finite sequence. One can verify that $p{\restriction}n$ is non-multi and $p_{\lfloor n}$ is non-multi and $\mathrm{smid}(p, m, n)$ is non-multi and $\langle p(m), \ldots, p(n)\rangle$ is non-multi.

Let p be a non-directed-multi, graph-yielding finite sequence. One can verify that $p{\restriction}n$ is non-directed-multi and $p_{\lfloor n}$ is non-directed-multi and $\mathrm{smid}(p, m, n)$ is non-directed-multi and $\langle p(m), \ldots, p(n)\rangle$ is non-directed-multi.

Let p be a simple, graph-yielding finite sequence. One can verify that $p{\restriction}n$ is simple and $p_{\lfloor n}$ is simple and $\mathrm{smid}(p, m, n)$ is simple and $\langle p(m), \ldots, p(n)\rangle$ is simple.

Let p be a directed-simple, graph-yielding finite sequence. One can verify that $p{\restriction}n$ is directed-simple and $p_{\lfloor n}$ is directed-simple and $\mathrm{smid}(p, m, n)$ is directed-simple and $\langle p(m), \ldots, p(n)\rangle$ is directed-simple.

Let p be a connected, graph-yielding finite sequence. One can verify that $p{\restriction}n$ is connected and $p_{\lfloor n}$ is connected and $\mathrm{smid}(p, m, n)$ is connected and $\langle p(m), \ldots, p(n)\rangle$ is connected.

Let p be an acyclic, graph-yielding finite sequence. One can verify that $p{\restriction}n$ is acyclic and $p_{\lfloor n}$ is acyclic and $\mathrm{smid}(p, m, n)$ is acyclic and $\langle p(m), \ldots, p(n)\rangle$ is acyclic.

Let p be a tree-like, graph-yielding finite sequence. One can verify that $p{\restriction}n$ is tree-like and $p_{\lfloor n}$ is tree-like and $\mathrm{smid}(p, m, n)$ is tree-like and $\langle p(m), \ldots, p(n)\rangle$ is tree-like.

Let p be an edgeless, graph-yielding finite sequence. One can verify that $p{\restriction}n$ is edgeless and $p_{\lfloor n}$ is edgeless and $\mathrm{smid}(p, m, n)$ is edgeless and $\langle p(m), \ldots, p(n)\rangle$

is edgeless.

Let p, q be graph-yielding finite sequences. Let us note that $p \mathbin{^\frown} q$ is graph-yielding and $p \smallfrown\!\!\smallfrown q$ is graph-yielding.

Let p, q be finite, graph-yielding finite sequences. Let us observe that $p \mathbin{^\frown} q$ is finite and $p \smallfrown\!\!\smallfrown q$ is finite.

Let p, q be loopless, graph-yielding finite sequences. Let us observe that $p \mathbin{^\frown} q$ is loopless and $p \smallfrown\!\!\smallfrown q$ is loopless.

Let p, q be trivial, graph-yielding finite sequences. Let us observe that $p \mathbin{^\frown} q$ is trivial and $p \smallfrown\!\!\smallfrown q$ is trivial.

Let p, q be nontrivial, graph-yielding finite sequences. Let us observe that $p \mathbin{^\frown} q$ is nontrivial and $p \smallfrown\!\!\smallfrown q$ is nontrivial.

Let p, q be non-multi, graph-yielding finite sequences. Observe that $p \mathbin{^\frown} q$ is non-multi and $p \smallfrown\!\!\smallfrown q$ is non-multi.

Let p, q be non-directed-multi, graph-yielding finite sequences. Observe that $p \mathbin{^\frown} q$ is non-directed-multi and $p \smallfrown\!\!\smallfrown q$ is non-directed-multi.

Let p, q be simple, graph-yielding finite sequences. Observe that $p \mathbin{^\frown} q$ is simple and $p \smallfrown\!\!\smallfrown q$ is simple.

Let p, q be directed-simple, graph-yielding finite sequences. One can verify that $p \mathbin{^\frown} q$ is directed-simple and $p \smallfrown\!\!\smallfrown q$ is directed-simple.

Let p, q be connected, graph-yielding finite sequences. Note that $p \mathbin{^\frown} q$ is connected and $p \smallfrown\!\!\smallfrown q$ is connected.

Let p, q be acyclic, graph-yielding finite sequences. Note that $p \mathbin{^\frown} q$ is acyclic and $p \smallfrown\!\!\smallfrown q$ is acyclic.

Let p, q be tree-like, graph-yielding finite sequences. Note that $p \mathbin{^\frown} q$ is tree-like and $p \smallfrown\!\!\smallfrown q$ is tree-like.

Let p, q be edgeless, graph-yielding finite sequences. Observe that $p \mathbin{^\frown} q$ is edgeless and $p \smallfrown\!\!\smallfrown q$ is edgeless.

Let G_1, G_2 be graphs. Note that $\langle G_1, G_2 \rangle$ is graph-yielding.

Let G_3 be a graph. Let us note that $\langle G_1, G_2, G_3 \rangle$ is graph-yielding.

Let G_1, G_2 be finite graphs. Let us observe that $\langle G_1, G_2 \rangle$ is finite.

Let G_3 be a finite graph. One can verify that $\langle G_1, G_2, G_3 \rangle$ is finite.

Let G_1, G_2 be loopless graphs. Note that $\langle G_1, G_2 \rangle$ is loopless.

Let G_3 be a loopless graph. Let us note that $\langle G_1, G_2, G_3 \rangle$ is loopless.

Let G_1, G_2 be trivial graphs. Let us observe that $\langle G_1, G_2 \rangle$ is trivial.

Let G_3 be a trivial graph. One can verify that $\langle G_1, G_2, G_3 \rangle$ is trivial.

Let G_1, G_2 be non trivial graphs. One can check that $\langle G_1, G_2 \rangle$ is nontrivial.

Let G_3 be a non trivial graph. One can check that $\langle G_1, G_2, G_3 \rangle$ is nontrivial.

Let G_1, G_2 be non-multi graphs. Let us note that $\langle G_1, G_2 \rangle$ is non-multi.

Let G_3 be a non-multi graph. Observe that $\langle G_1, G_2, G_3 \rangle$ is non-multi.

Let G_1, G_2 be non-directed-multi graphs. One can verify that $\langle G_1, G_2\rangle$ is non-directed-multi.

Let G_3 be a non-directed-multi graph. One can check that $\langle G_1, G_2, G_3\rangle$ is non-directed-multi.

Let G_1, G_2 be simple graphs. Let us note that $\langle G_1, G_2\rangle$ is simple.

Let G_3 be a simple graph. Observe that $\langle G_1, G_2, G_3\rangle$ is simple.

Let G_1, G_2 be directed-simple graphs. One can verify that $\langle G_1, G_2\rangle$ is directed-simple.

Let G_3 be a directed-simple graph. One can check that $\langle G_1, G_2, G_3\rangle$ is directed-simple.

Let G_1, G_2 be connected graphs. Let us note that $\langle G_1, G_2\rangle$ is connected.

Let G_3 be a connected graph. Observe that $\langle G_1, G_2, G_3\rangle$ is connected.

Let G_1, G_2 be acyclic graphs. One can verify that $\langle G_1, G_2\rangle$ is acyclic.

Let G_3 be an acyclic graph. One can check that $\langle G_1, G_2, G_3\rangle$ is acyclic.

Let G_1, G_2 be tree-like graphs. Let us note that $\langle G_1, G_2\rangle$ is tree-like.

Let G_3 be a tree-like graph. Observe that $\langle G_1, G_2, G_3\rangle$ is tree-like.

Let G_1, G_2 be edgeless graphs. One can verify that $\langle G_1, G_2\rangle$ is edgeless.

Let G_3 be an edgeless graph. One can check that $\langle G_1, G_2, G_3\rangle$ is edgeless.

4. Construction of Finite Graphs

Now we state the propositions:

(59) Let us consider a graph G_2, a finite set V, and a supergraph G_1 of G_2 extended by the vertices from V. Then there exists a non empty, graph-yielding finite sequence p such that

(i) $p(1) \approx G_2$, and

(ii) $p(\operatorname{len} p) = G_1$, and

(iii) $\operatorname{len} p = \overline{\overline{V \setminus \alpha}} + 1$, and

(iv) for every element n of $\operatorname{dom} p$ such that $n \leqslant \operatorname{len} p - 1$ there exists a vertex v of G_1 such that $p(n+1)$ is a supergraph of $p(n)$ extended by v and $v \notin$ the vertices of $p(n)$,

where α is the vertices of G_2.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv$ for every finite set V for every supergraph G_1 of G_2 extended by the vertices from V such that $\overline{\overline{V \setminus (\text{the vertices of } G_2)}} = \$_1$ there exists a non empty, graph-yielding finite sequence p such that $p(1) \approx G_2$ and $p(\operatorname{len} p) = G_1$ and $\operatorname{len} p = \overline{\overline{V \setminus (\text{the vertices of } G_2)}} + 1$ and for every element n of $\operatorname{dom} p$ such that

$n \leqslant \operatorname{len} p - 1$ there exists a vertex v of G_1 such that $p(n+1)$ is a supergraph of $p(n)$ extended by v and $v \notin$ the vertices of $p(n)$.

$\mathcal{P}[0]$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every natural number k, $\mathcal{P}[k]$. □

(60) Let us consider a finite graph G, and a subgraph H of G. Suppose G.size() $=$ H.size(). Then there exists a non empty, finite, graph-yielding finite sequence p such that

(i) $p(1) \approx H$, and

(ii) $p(\operatorname{len} p) = G$, and

(iii) $\operatorname{len} p = G$.order() $-$ H.order() $+ 1$, and

(iv) for every element n of $\operatorname{dom} p$ such that $n \leqslant \operatorname{len} p - 1$ there exists a vertex v of G such that $p(n+1)$ is a supergraph of $p(n)$ extended by v and $v \notin$ the vertices of $p(n)$.

Proof: Set $V =$ (the vertices of G)$\setminus$(the vertices of H). G is a supergraph of H extended by the vertices from V. Consider p being a non empty, graph-yielding finite sequence such that $p(1) \approx H$ and $p(\operatorname{len} p) = G$ and $\operatorname{len} p = \overline{\overline{V \setminus \alpha}} + 1$, where α is the vertices of H and for every element n of $\operatorname{dom} p$ such that $n \leqslant \operatorname{len} p - 1$ there exists a vertex v of G such that $p(n+1)$ is a supergraph of $p(n)$ extended by v and $v \notin$ the vertices of $p(n)$.

Define $\mathcal{P}[\text{natural number}] \equiv$ for every element n of $\operatorname{dom} p$ such that $\$_1 = n$ holds $p(n)$ is finite. For every non zero natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every non zero natural number k, $\mathcal{P}[k]$. For every element x of $\operatorname{dom} p$, $p(x)$ is finite. □

(61) Let us consider a finite, edgeless graph G, and a subgraph H of G. Then there exists a non empty, finite, edgeless, graph-yielding finite sequence p such that

(i) $p(1) \approx H$, and

(ii) $p(\operatorname{len} p) = G$, and

(iii) $\operatorname{len} p = G$.order() $-$ H.order() $+ 1$, and

(iv) for every element n of $\operatorname{dom} p$ such that $n \leqslant \operatorname{len} p - 1$ there exists a vertex v of G such that $p(n+1)$ is a supergraph of $p(n)$ extended by v and $v \notin$ the vertices of $p(n)$.

Proof: G.size() $= 0$. Consider p being a non empty, finite, graph-yielding finite sequence such that $p(1) \approx H$ and $p(\operatorname{len} p) = G$ and $\operatorname{len} p =$ G.order() $-$ H.order() $+ 1$ and for every element n of $\operatorname{dom} p$ such that

$n \leqslant \operatorname{len} p - 1$ there exists a vertex v of G such that $p(n+1)$ is a supergraph of $p(n)$ extended by v and $v \notin$ the vertices of $p(n)$. Define $\mathcal{P}[\text{natural number}] \equiv$ for every element n of $\operatorname{dom} p$ such that $\$_1 = n$ holds $p(n)$ is edgeless.

$\mathcal{P}[1]$. For every non zero natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every non zero natural number k, $\mathcal{P}[k]$. For every element x of $\operatorname{dom} p$, $p(x)$ is edgeless. □

(62) Let us consider a finite, edgeless graph G. Then there exists a non empty, finite, edgeless, graph-yielding finite sequence p such that

(i) $p(1)$ is trivial and edgeless, and

(ii) $p(\operatorname{len} p) = G$, and

(iii) $\operatorname{len} p = G.\text{order}()$, and

(iv) for every element n of $\operatorname{dom} p$ such that $n \leqslant \operatorname{len} p - 1$ there exists a vertex v of G such that $p(n+1)$ is a supergraph of $p(n)$ extended by v and $v \notin$ the vertices of $p(n)$.

The theorem is a consequence of (61) and (52).

The scheme *FinEdgelessGraphs* deals with a unary predicate $\mathcal{P}$ and states that

(Sch. 1) For every finite, edgeless graph G, $\mathcal{P}[G]$

provided

- for every trivial, edgeless graph G, $\mathcal{P}[G]$ and
- for every finite, edgeless graph G_2 and for every object v and for every supergraph G_1 of G_2 extended by v such that $v \notin$ the vertices of G_2 and $\mathcal{P}[G_2]$ holds $\mathcal{P}[G_1]$.

Now we state the propositions:

(63) Let us consider a non empty, graph-yielding finite sequence p. Suppose $p(1)$ is edgeless and for every element n of $\operatorname{dom} p$ such that $n \leqslant \operatorname{len} p - 1$ there exists an object v such that $p(n+1)$ is a supergraph of $p(n)$ extended by v. Then $p(\operatorname{len} p)$ is edgeless.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv$ for every non empty, graph-yielding finite sequence p such that $\operatorname{len} p = \$_1$ and $p(1)$ is edgeless and for every element n of $\operatorname{dom} p$ such that $n \leqslant \operatorname{len} p - 1$ there exists an object v such that $p(n+1)$ is a supergraph of $p(n)$ extended by v holds $p(\operatorname{len} p)$ is edgeless.

For every non zero natural number m such that $\mathcal{P}[m]$ holds $\mathcal{P}[m+1]$. For every non zero natural number m, $\mathcal{P}[m]$. □

(64) Let us consider a finite graph G, and a spanning subgraph H of G. Then there exists a non empty, finite, graph-yielding finite sequence p such that

(i) $p(1) \approx H$, and

(ii) $p(\operatorname{len} p) = G$, and

(iii) $\operatorname{len} p = G.\mathrm{size}() - H.\mathrm{size}() + 1$, and

(iv) for every element n of $\operatorname{dom} p$ such that $n \leqslant \operatorname{len} p - 1$ there exist vertices v_1, v_2 of G and there exists an object e such that $p(n+1)$ is a supergraph of $p(n)$ extended by e between vertices v_1 and v_2 and $e \in$ (the edges of G) $\setminus$ (the edges of $p(n)$) and v_1, $v_2 \in$ the vertices of $p(n)$.

Proof: Define $\mathcal{P}$[natural number] $\equiv$ for every spanning subgraph H of G such that $G.\mathrm{size}() - H.\mathrm{size}() = \$_1$ there exists a non empty, finite, graph-yielding finite sequence p such that $p(1) \approx H$ and $p(\operatorname{len} p) = G$ and $\operatorname{len} p = G.\mathrm{size}() - H.\mathrm{size}() + 1$ and for every element n of $\operatorname{dom} p$ such that $n \leqslant \operatorname{len} p - 1$ there exist vertices v_1, v_2 of G and there exists an object e such that $p(n+1)$ is a supergraph of $p(n)$ extended by e between vertices v_1 and v_2 and $e \in$ (the edges of G) $\setminus$ (the edges of $p(n)$) and v_1, $v_2 \in$ the vertices of $p(n)$.

$\mathcal{P}[0]$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every natural number k, $\mathcal{P}[k]$. □

(65) Let us consider a finite graph G. Then there exists a non empty, finite, graph-yielding finite sequence p such that

(i) $p(1)$ is edgeless, and

(ii) $p(\operatorname{len} p) = G$, and

(iii) $\operatorname{len} p = G.\mathrm{size}() + 1$, and

(iv) for every element n of $\operatorname{dom} p$ such that $n \leqslant \operatorname{len} p - 1$ there exist vertices v_1, v_2 of G and there exists an object e such that $p(n+1)$ is a supergraph of $p(n)$ extended by e between vertices v_1 and v_2 and $e \in$ (the edges of G) $\setminus$ (the edges of $p(n)$) and v_1, $v_2 \in$ the vertices of $p(n)$.

The theorem is a consequence of (64), (52), and (49).

(66) Let us consider a finite, connected graph G, and a spanning, connected subgraph H of G. Then there exists a non empty, finite, connected, graph-yielding finite sequence p such that

(i) $p(1) \approx H$, and

(ii) $p(\operatorname{len} p) = G$, and

(iii) $\operatorname{len} p = G.\mathrm{size}() - H.\mathrm{size}() + 1$, and

(iv) for every element n of $\operatorname{dom} p$ such that $n \leqslant \operatorname{len} p - 1$ there exist vertices v_1, v_2 of G and there exists an object e such that $p(n+1)$ is a supergraph of $p(n)$ extended by e between vertices v_1 and v_2 and $e \in$ (the edges of G) $\setminus$ (the edges of $p(n)$) and v_1, $v_2 \in$ the vertices of $p(n)$.

Proof: Consider p being a non empty, finite, graph-yielding finite sequence such that $p(1) \approx H$ and $p(\operatorname{len} p) = G$ and $\operatorname{len} p = G.\mathrm{size}() - H.\mathrm{size}() + 1$ and for every element n of $\operatorname{dom} p$ such that $n \leqslant \operatorname{len} p - 1$ there exist vertices v_1, v_2 of G and there exists an object e such that $p(n+1)$ is a supergraph of $p(n)$ extended by e between vertices v_1 and v_2 and $e \in$ (the edges of G) $\setminus$ (the edges of $p(n)$) and v_1, $v_2 \in$ the vertices of $p(n)$.

Define $\mathcal{P}[\text{natural number}] \equiv$ for every element n of $\operatorname{dom} p$ such that $\$_1 = n$ holds $p(n)$ is connected. For every non zero natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every non zero natural number k, $\mathcal{P}[k]$. For every element x of $\operatorname{dom} p$, $p(x)$ is connected. □

(67) Let us consider a finite graph G_1, and a subgraph H of G_1. Then there exists a spanning subgraph G_2 of G_1 and there exists a non empty, finite, graph-yielding finite sequence p such that $H.\mathrm{size}() = G_2.\mathrm{size}()$ and $p(1) \approx H$ and $p(\operatorname{len} p) = G_2$ and $\operatorname{len} p = G_1.\mathrm{order}() - H.\mathrm{order}() + 1$ and for every element n of $\operatorname{dom} p$ such that $n \leqslant \operatorname{len} p - 1$ there exists a vertex v of G_1 such that $p(n+1)$ is a supergraph of $p(n)$ extended by v and $v \notin$ the vertices of $p(n)$.

Proof: Set $V =$ (the vertices of G_1) $\setminus$ (the vertices of H). Set $G_2 =$ the supergraph of H extended by the vertices from V. Consider p being a non empty, graph-yielding finite sequence such that $p(1) \approx H$ and $p(\operatorname{len} p) = G_2$ and $\operatorname{len} p = \overline{\overline{V \setminus \alpha}} + 1$, where α is the vertices of H and for every element n of $\operatorname{dom} p$ such that $n \leqslant \operatorname{len} p - 1$ there exists a vertex v of G_2 such that $p(n+1)$ is a supergraph of $p(n)$ extended by v and $v \notin$ the vertices of $p(n)$.

Define $\mathcal{P}[\text{natural number}] \equiv$ for every element n of $\operatorname{dom} p$ such that $\$_1 = n$ holds $p(n)$ is finite. For every non zero natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every non zero natural number k, $\mathcal{P}[k]$. For every element x of $\operatorname{dom} p$, $p(x)$ is finite. G_2 is a subgraph of G_1. Consider v being a vertex of G_2 such that $p(n+1)$ is a supergraph of $p(n)$ extended by v and $v \notin$ the vertices of $p(n)$. □

(68) Let us consider a finite graph G, and a subgraph H of G. Then there exists a non empty, finite, graph-yielding finite sequence p such that

(i) $p(1) \approx H$, and

(ii) $p(\operatorname{len} p) = G$, and

(iii) $\operatorname{len} p = G.\mathrm{order}() + G.\mathrm{size}() - (H.\mathrm{order}() + H.\mathrm{size}()) + 1$, and

(iv) for every element n of $\operatorname{dom} p$ such that $n \leqslant \operatorname{len} p - 1$ holds there exist vertices v_1, v_2 of G and there exists an object e such that $p(n+1)$ is a supergraph of $p(n)$ extended by e between vertices v_1 and v_2 and $e \in$ (the edges of G) $\setminus$ (the edges of $p(n)$) and v_1, $v_2 \in$ the vertices of $p(n)$ or there exists a vertex v of G such that $p(n+1)$ is a supergraph of $p(n)$ extended by v and $v \notin$ the vertices of $p(n)$.

The theorem is a consequence of (67), (64), (36), and (60).

(69) Let us consider a finite graph G. Then there exists a non empty, finite, graph-yielding finite sequence p such that

(i) $p(1)$ is trivial and edgeless, and

(ii) $p(\operatorname{len} p) = G$, and

(iii) $\operatorname{len} p = G.\mathrm{order}() + G.\mathrm{size}()$, and

(iv) for every element n of $\operatorname{dom} p$ such that $n \leqslant \operatorname{len} p - 1$ holds there exist vertices v_1, v_2 of G and there exists an object e such that $p(n+1)$ is a supergraph of $p(n)$ extended by e between vertices v_1 and v_2 and $e \in$ (the edges of G) $\setminus$ (the edges of $p(n)$) and v_1, $v_2 \in$ the vertices of $p(n)$ or there exists a vertex v of G such that $p(n+1)$ is a supergraph of $p(n)$ extended by v and $v \notin$ the vertices of $p(n)$.

The theorem is a consequence of (68), (52), and (49).

The scheme *FinGraphs* deals with a unary predicate $\mathcal{P}$ and states that

(Sch. 2) For every finite graph G, $\mathcal{P}[G]$

provided

- for every trivial, edgeless graph G, $\mathcal{P}[G]$ and

- for every finite graph G_2 and for every object v and for every supergraph G_1 of G_2 extended by v such that $v \notin$ the vertices of G_2 and $\mathcal{P}[G_2]$ holds $\mathcal{P}[G_1]$ and

- for every finite graph G_2 and for every vertices v_1, v_2 of G_2 and for every object e and for every supergraph G_1 of G_2 extended by e between vertices v_1 and v_2 such that $e \notin$ the edges of G_2 and $\mathcal{P}[G_2]$ holds $\mathcal{P}[G_1]$.

Now we state the propositions:

(70) Let us consider a non empty, graph-yielding finite sequence p. Suppose $p(1)$ is finite and for every element n of $\operatorname{dom} p$ such that $n \leqslant \operatorname{len} p - 1$ holds there exists an object v such that $p(n+1)$ is a supergraph of $p(n)$ extended by v or there exist objects v_1, e, v_2 such that $p(n+1)$ is a supergraph of $p(n)$ extended by e between vertices v_1 and v_2. Then $p(\operatorname{len} p)$ is finite.

Proof: Define $\mathcal{Q}$[natural number] $\equiv$ if $\$_1 \leqslant \operatorname{len} p$, then there exists an element k of $\operatorname{dom} p$ such that $\$_1 = k$ and $p(k)$ is finite. $\mathcal{Q}[1]$. For every non zero natural number m such that $\mathcal{Q}[m]$ holds $\mathcal{Q}[m+1]$.

For every non zero natural number m, $\mathcal{Q}[m]$. Consider k being an element of $\operatorname{dom} p$ such that $\operatorname{len} p = k$ and $p(k)$ is finite. □

(71) Let us consider a finite, tree-like graph G, and a connected subgraph H of G. Then there exists a non empty, finite, tree-like, graph-yielding finite sequence p such that

(i) $p(1) \approx H$, and

(ii) $p(\operatorname{len} p) = G$, and

(iii) $\operatorname{len} p = G.\text{order}() - H.\text{order}() + 1$, and

(iv) for every element n of $\operatorname{dom} p$ such that $n \leqslant \operatorname{len} p - 1$ there exist vertices v_1, v_2 of G and there exists an object e such that $p(n+1)$ is a supergraph of $p(n)$ extended by v_1, v_2 and e between them and $e \in$ (the edges of G) $\setminus$ (the edges of $p(n)$) and ($v_1 \in$ the vertices of $p(n)$ and $v_2 \notin$ the vertices of $p(n)$ or $v_1 \notin$ the vertices of $p(n)$ and $v_2 \in$ the vertices of $p(n)$).

Proof: Define $\mathcal{P}$[natural number] $\equiv$ for every finite, tree-like graph G for every connected subgraph H of G such that $\$_1 = G.\text{order}() - H.\text{order}()$ there exists a non empty, finite, tree-like, graph-yielding finite sequence p such that $p(1) \approx H$ and $p(\operatorname{len} p) = G$ and $\operatorname{len} p = G.\text{order}() - H.\text{order}() + 1$ and for every element n of $\operatorname{dom} p$ such that $n \leqslant \operatorname{len} p - 1$ there exist vertices v_1, v_2 of G and there exists an object e such that $p(n+1)$ is a supergraph of $p(n)$ extended by v_1, v_2 and e between them and $e \in$ (the edges of G)$\setminus$(the edges of $p(n)$) and ($v_1 \in$ the vertices of $p(n)$ and $v_2 \notin$ the vertices of $p(n)$ or $v_1 \notin$ the vertices of $p(n)$ and $v_2 \in$ the vertices of $p(n)$).

$\mathcal{P}[0]$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every natural number k, $\mathcal{P}[k]$. □

(72) Let us consider a finite, tree-like graph G. Then there exists a non empty, finite, tree-like, graph-yielding finite sequence p such that

(i) $p(1)$ is trivial and edgeless, and

(ii) $p(\operatorname{len} p) = G$, and

(iii) $\operatorname{len} p = G.\text{order}()$, and

(iv) for every element n of $\operatorname{dom} p$ such that $n \leqslant \operatorname{len} p - 1$ there exist vertices v_1, v_2 of G and there exists an object e such that $p(n+1)$ is a supergraph of $p(n)$ extended by v_1, v_2 and e between them and $e \in$ (the edges of G) $\setminus$ (the edges of $p(n)$) and ($v_1 \in$ the vertices of

$p(n)$ and $v_2 \notin$ the vertices of $p(n)$ or $v_1 \notin$ the vertices of $p(n)$ and $v_2 \in$ the vertices of $p(n)$).

The theorem is a consequence of (71) and (52).

The scheme *FinTrees* deals with a unary predicate $\mathcal{P}$ and states that

(Sch. 3) For every finite, tree-like graph G, $\mathcal{P}[G]$

provided

- for every trivial, edgeless graph G, $\mathcal{P}[G]$ and
- for every finite, tree-like graph G_2 and for every vertex v of G_2 and for every objects e, w such that $e \notin$ the edges of G_2 and $w \notin$ the vertices of G_2 and $\mathcal{P}[G_2]$ holds for every supergraph G_1 of G_2 extended by v, w and e between them, $\mathcal{P}[G_1]$ and for every supergraph G_1 of G_2 extended by w, v and e between them, $\mathcal{P}[G_1]$.

Now we state the propositions:

(73) Let us consider a non empty, graph-yielding finite sequence p. Suppose $p(1)$ is tree-like and for every element n of $\operatorname{dom} p$ such that $n \leqslant \operatorname{len} p - 1$ there exist objects v_1, e, v_2 such that $p(n+1)$ is a supergraph of $p(n)$ extended by v_1, v_2 and e between them. Then $p(\operatorname{len} p)$ is tree-like.
Proof: Define $\mathcal{Q}$[natural number] $\equiv$ if $\$_1 \leqslant \operatorname{len} p$, then there exists an element k of $\operatorname{dom} p$ such that $\$_1 = k$ and $p(k)$ is tree-like. $\mathcal{Q}[1]$.

For every non zero natural number m such that $\mathcal{Q}[m]$ holds $\mathcal{Q}[m+1]$. For every non zero natural number m, $\mathcal{Q}[m]$. Consider k being an element of $\operatorname{dom} p$ such that $\operatorname{len} p = k$ and $p(k)$ is tree-like. □

(74) Let us consider a finite, connected graph G. Then there exists a non empty, finite, connected, graph-yielding finite sequence p such that

(i) $p(1)$ is trivial and edgeless, and

(ii) $p(\operatorname{len} p) = G$, and

(iii) $\operatorname{len} p = G.\mathrm{size}() + 1$, and

(iv) for every element n of $\operatorname{dom} p$ such that $n \leqslant \operatorname{len} p - 1$ holds there exist vertices v_1, v_2 of G and there exists an object e such that $p(n+1)$ is a supergraph of $p(n)$ extended by v_1, v_2 and e between them and $e \in$ (the edges of G) $\setminus$ (the edges of $p(n)$) and ($v_1 \in$ the vertices of $p(n)$ and $v_2 \notin$ the vertices of $p(n)$ or $v_1 \notin$ the vertices of $p(n)$ and $v_2 \in$ the vertices of $p(n)$) or there exist vertices v_1, v_2 of G and there exists an object e such that $p(n+1)$ is a supergraph of $p(n)$ extended by e between vertices v_1 and v_2 and $e \in$ (the edges of G) $\setminus$ (the edges of $p(n)$) and v_1, $v_2 \in$ the vertices of $p(n)$.

The theorem is a consequence of (72), (66), and (36).

The scheme *FinConnectedGraphs* deals with a unary predicate $\mathcal{P}$ and states that

(Sch. 4) For every finite, connected graph G, $\mathcal{P}[G]$

provided

- for every trivial, edgeless graph G, $\mathcal{P}[G]$ and
- for every finite, connected graph G_2 and for every vertex v of G_2 and for every objects e, w such that $e \notin$ the edges of G_2 and $w \notin$ the vertices of G_2 and $\mathcal{P}[G_2]$ holds for every supergraph G_1 of G_2 extended by v, w and e between them, $\mathcal{P}[G_1]$ and for every supergraph G_1 of G_2 extended by w, v and e between them, $\mathcal{P}[G_1]$ and
- for every finite, connected graph G_2 and for every vertices v_1, v_2 of G_2 and for every object e and for every supergraph G_1 of G_2 extended by e between vertices v_1 and v_2 such that $e \notin$ the edges of G_2 and $\mathcal{P}[G_2]$ holds $\mathcal{P}[G_1]$.

Now we state the propositions:

(75) Let us consider a non empty, graph-yielding finite sequence p. Suppose $p(1)$ is connected and for every element n of $\mathrm{dom}\, p$ such that $n \leqslant \mathrm{len}\, p - 1$ there exist objects v_1, e, v_2 such that $p(n+1)$ is supergraph of $p(n)$ extended by v_1, v_2 and e between them or supergraph of $p(n)$ extended by e between vertices v_1 and v_2. Then $p(\mathrm{len}\, p)$ is connected.

Proof: Define $\mathcal{Q}$[natural number] $\equiv$ if $\$_1 \leqslant \mathrm{len}\, p$, then there exists an element k of $\mathrm{dom}\, p$ such that $\$_1 = k$ and $p(k)$ is connected. $\mathcal{Q}[1]$. For every non zero natural number m such that $\mathcal{Q}[m]$ holds $\mathcal{Q}[m+1]$. For every non zero natural number m, $\mathcal{Q}[m]$. □

(76) Let us consider a graph G_2, an object v, a set V_1, a finite set V_2, and a supergraph G_1 of G_2 extended by vertex v and edges between v and $V_1 \cup V_2$ of G_2. Suppose $V_1 \cup V_2 \subseteq$ the vertices of G_2 and $v \notin$ the vertices of G_2 and V_1 misses V_2. Then there exists a non empty, graph-yielding finite sequence p such that

(i) $p(1) = G_2$, and

(ii) $p(\mathrm{len}\, p) = G_1$, and

(iii) $\mathrm{len}\, p = \overline{\overline{V_2}} + 2$, and

(iv) $p(2)$ is a supergraph of G_2 extended by vertex v and edges between v and V_1 of G_2, and

(v) for every element n of $\operatorname{dom} p$ such that $2 \leqslant n \leqslant \operatorname{len} p - 1$ there exists a vertex w of G_2 and there exists an object e such that $e \in$ (the edges of G_1)$\setminus$(the edges of $p(n)$) and $p(n+1)$ is supergraph of $p(n)$ extended by e between vertices v and w or supergraph of $p(n)$ extended by e between vertices w and v.

Proof: Define $\mathcal{P}$[natural number] $\equiv$ for every finite set V_2 for every supergraph G_1 of G_2 extended by vertex v and edges between v and $V_1 \cup V_2$ of G_2 such that $V_1 \cup V_2 \subseteq$ the vertices of G_2 and $v \notin$ the vertices of G_2 and V_1 misses V_2 and $\overline{\overline{V_2}} = \$_1$ there exists a non empty, graph-yielding finite sequence p such that $p(1) = G_2$ and $p(\operatorname{len} p) = G_1$ and $\operatorname{len} p = \overline{\overline{V_2}} + 2$ and $p(2)$ is a supergraph of G_2 extended by vertex v and edges between v and V_1 of G_2 and for every element n of $\operatorname{dom} p$ such that $2 \leqslant n \leqslant \operatorname{len} p - 1$.

There exists a vertex w of G_2 and there exists an object e such that $e \in$ (the edges of G_1) $\setminus$ (the edges of $p(n)$) and $p(n+1)$ is supergraph of $p(n)$ extended by e between vertices v and w or supergraph of $p(n)$ extended by e between vertices w and v. $\mathcal{P}[0]$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every natural number k, $\mathcal{P}[k]$. □

(77) Let us consider a graph G_2, an object v, a finite set V, and a supergraph G_1 of G_2 extended by vertex v and edges between v and V of G_2. Suppose $V \subseteq$ the vertices of G_2 and $v \notin$ the vertices of G_2. Then there exists a non empty, graph-yielding finite sequence p such that

(i) $p(1) = G_2$, and

(ii) $p(\operatorname{len} p) = G_1$, and

(iii) $\operatorname{len} p = \overline{\overline{V}} + 2$, and

(iv) $p(2)$ is a supergraph of G_2 extended by v, and

(v) for every element n of $\operatorname{dom} p$ such that $2 \leqslant n \leqslant \operatorname{len} p - 1$ there exists a vertex w of G_2 and there exists an object e such that $e \in$ (the edges of G_1)$\setminus$(the edges of $p(n)$) and $p(n+1)$ is supergraph of $p(n)$ extended by e between vertices v and w or supergraph of $p(n)$ extended by e between vertices w and v.

The theorem is a consequence of (76).

(78) Let us consider a graph G_2, an object v, a non empty, finite set V, and a supergraph G_1 of G_2 extended by vertex v and edges between v and V of G_2. Suppose $V \subseteq$ the vertices of G_2 and $v \notin$ the vertices of G_2. Then there exists a non empty, graph-yielding finite sequence p such that

(i) $p(1) = G_2$, and

(ii) $p(\operatorname{len} p) = G_1$, and

(iii) $\operatorname{len} p = \overline{\overline{V}} + 1$, and

(iv) there exists a vertex w of G_2 and there exists an object e such that $e \in$ (the edges of G_1) $\setminus$ (the edges of G_2) and $p(2)$ is supergraph of G_2 extended by v, w and e between them or supergraph of G_2 extended by w, v and e between them, and

(v) for every element n of $\operatorname{dom} p$ such that $2 \leqslant n \leqslant \operatorname{len} p - 1$ there exists a vertex w of G_2 and there exists an object e such that $e \in$ (the edges of G_1) $\setminus$ (the edges of $p(n)$) and $p(n+1)$ is supergraph of $p(n)$ extended by e between vertices v and w or supergraph of $p(n)$ extended by e between vertices w and v.

The theorem is a consequence of (76).

(79) Let us consider a finite, simple graph G, a set W, and a subgraph H of G induced by W. Then there exists a non empty, finite, simple, graph-yielding finite sequence p such that

(i) $p(1) \approx H$, and

(ii) $p(\operatorname{len} p) = G$, and

(iii) $\operatorname{len} p = G.\mathrm{order}() - H.\mathrm{order}() + 1$, and

(iv) for every element n of $\operatorname{dom} p$ such that $n \leqslant \operatorname{len} p - 1$ there exists an object v and there exists a finite set V such that $v \in$ (the vertices of G) $\setminus$ (the vertices of $p(n)$) and $V \subseteq$ the vertices of $p(n)$ and $p(n+1)$ is a supergraph of $p(n)$ extended by vertex v and edges between v and V of $p(n)$.

Proof: Define $\mathcal{P}$[natural number] $\equiv$ for every finite, simple graph G for every set W for every subgraph H of G induced by W such that $G.\mathrm{order}() - H.\mathrm{order}() = \$_1$ there exists a non empty, finite, simple, graph-yielding finite sequence p such that $p(1) \approx H$ and $p(\operatorname{len} p) = G$ and $\operatorname{len} p = G.\mathrm{order}() - H.\mathrm{order}() + 1$ and for every element n of $\operatorname{dom} p$ such that $n \leqslant \operatorname{len} p - 1$ there exists an object v and there exists a finite set V such that $v \in$ (the vertices of G) $\setminus$ (the vertices of $p(n)$) and $V \subseteq$ the vertices of $p(n)$ and $p(n+1)$ is a supergraph of $p(n)$ extended by vertex v and edges between v and V of $p(n)$.

$\mathcal{P}[0]$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every natural number k, $\mathcal{P}[k]$. □

(80) Let us consider a finite, simple graph G. Then there exists a non empty, finite, simple, graph-yielding finite sequence p such that

(i) $p(1)$ is trivial and edgeless, and

(ii) $p(\operatorname{len} p) = G$, and

(iii) $\operatorname{len} p = G$.order(), and

(iv) for every element n of $\operatorname{dom} p$ such that $n \leqslant \operatorname{len} p - 1$ there exists an object v and there exists a finite set V such that $v \in$ (the vertices of G) $\setminus$ (the vertices of $p(n)$) and $V \subseteq$ the vertices of $p(n)$ and $p(n+1)$ is a supergraph of $p(n)$ extended by vertex v and edges between v and V of $p(n)$.

The theorem is a consequence of (79) and (52).

The scheme *FinSimpleGraphs* deals with a unary predicate $\mathcal{P}$ and states that

(Sch. 5) For every finite, simple graph G, $\mathcal{P}[G]$

provided

- for every trivial, edgeless graph G, $\mathcal{P}[G]$ and
- for every finite, simple graph G_2 and for every object v and for every finite set V and for every supergraph G_1 of G_2 extended by vertex v and edges between v and V of G_2 such that $v \notin$ the vertices of G_2 and $V \subseteq$ the vertices of G_2 and $\mathcal{P}[G_2]$ holds $\mathcal{P}[G_1]$.

Now we state the propositions:

(81) Let us consider a non empty, graph-yielding finite sequence p. Suppose $p(1)$ is simple and for every element n of $\operatorname{dom} p$ such that $n \leqslant \operatorname{len} p - 1$ there exists an object v and there exists a set V such that $p(n+1)$ is a supergraph of $p(n)$ extended by vertex v and edges between v and V of $p(n)$. Then $p(\operatorname{len} p)$ is simple.

Proof: Define $\mathcal{Q}$[natural number] $\equiv$ if $\$_1 \leqslant \operatorname{len} p$, then there exists an element k of $\operatorname{dom} p$ such that $\$_1 = k$ and $p(k)$ is simple. $\mathcal{Q}[1]$. For every non zero natural number m such that $\mathcal{Q}[m]$ holds $\mathcal{Q}[m+1]$. For every non zero natural number m, $\mathcal{Q}[m]$. □

(82) Let us consider a finite, simple, connected graph G. Then there exists a non empty, finite, simple, connected, graph-yielding finite sequence p such that

(i) $p(1)$ is trivial and edgeless, and

(ii) $p(\operatorname{len} p) = G$, and

(iii) $\operatorname{len} p = G$.order(), and

(iv) for every element n of $\operatorname{dom} p$ such that $n \leqslant \operatorname{len} p - 1$ there exists an object v and there exists a non empty, finite set V such that $v \in$ (the vertices of G) $\setminus$ (the vertices of $p(n)$) and $V \subseteq$ the vertices of $p(n)$ and $p(n+1)$ is a supergraph of $p(n)$ extended by vertex v and edges between v and V of $p(n)$.

Proof: Define $\mathcal{P}$[natural number] $\equiv$ for every finite, simple, connected graph G such that G.order() $= \$_1$ there exists a non empty, finite, simple, connected, graph-yielding finite sequence p such that $p(1)$ is trivial and edgeless and $p(\operatorname{len} p) = G$ and $\operatorname{len} p = G$.order() and for every element n of $\operatorname{dom} p$ such that $n \leqslant \operatorname{len} p - 1$ there exists an object v and there exists a non empty, finite set V such that $v \in$ (the vertices of G) $\setminus$ (the vertices of $p(n)$) and $V \subseteq$ the vertices of $p(n)$ and $p(n+1)$ is a supergraph of $p(n)$ extended by vertex v and edges between v and V of $p(n)$.

$\mathcal{P}[1]$. For every non zero natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every non zero natural number k, $\mathcal{P}[k]$. □

The scheme *FinSimpleConnectedGraphs* deals with a unary predicate $\mathcal{P}$ and states that

(Sch. 6) For every finite, simple, connected graph G, $\mathcal{P}[G]$

provided

- for every trivial, edgeless graph G, $\mathcal{P}[G]$ and
- for every finite, simple, connected graph G_2 and for every object v and for every non empty, finite set V and for every supergraph G_1 of G_2 extended by vertex v and edges between v and V of G_2 such that $v \notin$ the vertices of G_2 and $V \subseteq$ the vertices of G_2 and $\mathcal{P}[G_2]$ holds $\mathcal{P}[G_1]$.

Now we state the proposition:

(83) Let us consider a non empty, graph-yielding finite sequence p. Suppose $p(1)$ is simple and connected and for every element n of $\operatorname{dom} p$ such that $n \leqslant \operatorname{len} p - 1$ there exists an object v and there exists a non empty set V such that $p(n+1)$ is a supergraph of $p(n)$ extended by vertex v and edges between v and V of $p(n)$. Then $p(\operatorname{len} p)$ is simple and connected.

Proof: Define $\mathcal{Q}$[natural number] $\equiv$ if $\$_1 \leqslant \operatorname{len} p$, then there exists an element k of $\operatorname{dom} p$ such that $\$_1 = k$ and $p(k)$ is simple and connected. $\mathcal{Q}[1]$.

For every non zero natural number m such that $\mathcal{Q}[m]$ holds $\mathcal{Q}[m+1]$. For every non zero natural number m, $\mathcal{Q}[m]$. □

References

[1] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.

[2] Lowell W. Beineke and Robin J. Wilson, editors. *Selected Topics in Graph Theory.* Academic Press, London, 1978. ISBN 0-12-086250-6.

[3] John Adrian Bondy and U. S. R. Murty. *Graph Theory.* Graduate Texts in Mathematics, 244. Springer, New York, 2008. ISBN 978-1-84628-969-9.

[4] Adam Grabowski, Artur Korniłowicz, and Adam Naumowicz. Four decades of Mizar. *Journal of Automated Reasoning*, 55(3):191–198, 2015. doi:10.1007/s10817-015-9345-1.

[5] Sebastian Koch. About supergraphs. Part I. *Formalized Mathematics*, 26(**2**):101–124, 2018. doi:10.2478/forma-2018-0009.

[6] Sebastian Koch. About supergraphs. Part II. *Formalized Mathematics*, 26(**2**):125–140, 2018. doi:10.2478/forma-2018-0010.

[7] Gilbert Lee and Piotr Rudnicki. Alternative graph structures. *Formalized Mathematics*, 13(**2**):235–252, 2005.

[8] Klaus Wagner. *Graphentheorie*. B.I-Hochschultaschenbücher; 248. Bibliograph. Inst., Mannheim, 1970. ISBN 3-411-00248-4.

[9] Robin James Wilson. *Introduction to Graph Theory.* Oliver & Boyd, Edinburgh, 1972. ISBN 0-05-002534-1.

Accepted May 27, 2019

FORMALIZED MATHEMATICS
Vol. 27, No. 2, Pages 181–187, 2019
DOI: 10.2478/forma-2019-0017

https://www.sciendo.com/

Partial Correctness of a Factorial Algorithm

Adrian Jaszczak
Institute of Informatics
University of Białystok
Poland

Artur Korniłowicz
Institute of Informatics
University of Białystok
Poland

Summary. In this paper we present a formalization in the Mizar system [3],[1] of the partial correctness of the algorithm:

```
i := val.1
j := val.2
n := val.3
s := val.4
while (i <> n)
   i := i + j
   s := s * i
return s
```

computing the factorial of given natural number `n`, where variables `i, n, s` are located as values of a `V-valued Function`, `loc`, as: `loc/.1 = i`, `loc/.3 = n` and `loc/.4 = s`, and the constant `1` is located in the location `loc/.2 = j` (set `V` represents simple names of considered nominative data [16]).

This work continues a formal verification of algorithms written in terms of simple-named complex-valued nominative data [6],[8],[14],[10],[11],[12]. The validity of the algorithm is presented in terms of semantic Floyd-Hoare triples over such data [9]. Proofs of the correctness are based on an inference system for an extended Floyd-Hoare logic [2],[4] with partial pre- and post-conditions [13],[15],[7],[5].

MSC: 68Q60 68T37 03B70 03B35

Keywords: factorial; nominative data; program verification

MML identifier: `NOMIN_5`, version: `8.1.09 5.57.1355`

Let D be a set and f_1, f_2, f_3 be binominative functions of D. The functor PP-composition(f_1, f_2, f_3) yielding a binominative function of D is defined by the term

(Def. 1) $f_1 \bullet f_2 \bullet f_3$.

Let f_1, f_2, f_3, f_4 be binominative functions of D. The functor PP-composition (f_1, f_2, f_3, f_4) yielding a binominative function of D is defined by the term

(Def. 2) PP-composition$(f_1, f_2, f_3) \bullet f_4$.

From now on D denotes a non empty set, f_1, f_2, f_3, f_4 denote binominative functions of D, and p, q, r, t, w denote partial predicates of D.

Now we state the proposition:

(1) UNCONDITIONAL COMPOSITION RULE FOR 3 PROGRAMS: Suppose $\langle p, f_1, q\rangle$ is an SFHT of D and $\langle q, f_2, r\rangle$ is an SFHT of D and $\langle r, f_3, w\rangle$ is an SFHT of D and $\langle \sim q, f_2, r\rangle$ is an SFHT of D and $\langle \sim r, f_3, w\rangle$ is an SFHT of D. Then $\langle p, \text{PP-composition}(f_1, f_2, f_3), w\rangle$ is an SFHT of D.

(2) UNCONDITIONAL COMPOSITION RULE FOR 4 PROGRAMS: Suppose $\langle p, f_1, q\rangle$ is an SFHT of D and $\langle q, f_2, r\rangle$ is an SFHT of D and $\langle r, f_3, w\rangle$ is an SFHT of D and $\langle w, f_4, t\rangle$ is an SFHT of D and $\langle \sim q, f_2, r\rangle$ is an SFHT of D and $\langle \sim r, f_3, w\rangle$ is an SFHT of D and $\langle \sim w, f_4, t\rangle$ is an SFHT of D. Then $\langle p, \text{PP-composition}(f_1, f_2, f_3, f_4), t\rangle$ is an SFHT of D.

In the sequel d, v, v_1 denote objects, V, A denote sets, z denotes an element of V, d_1 denotes a non-atomic nominative data of V and A, f denotes a binominative function over simple-named complex-valued nominative data of V and A, and T denotes a nominative data with simple names from V and complex values from A.

Now we state the proposition:

(3) If V is without nonatomic nominative data w.r.t. A and $v \in V$ and $v \neq v_1$ and $v_1 \in \operatorname{dom} d_1$, then $(d_1 \nabla_a^v T)(v_1) = d_1(v_1)$.

Let x, y be objects. Assume x is a complex number and y is a complex number. The functors: $x + y$ and $x * y$ yielding complex numbers are defined by conditions

(Def. 3) there exist complex numbers x_1, y_1 such that $x_1 = x$ and $y_1 = y$ and $x + y = x_1 + y_1$,

(Def. 4) there exist complex numbers x_1, y_1 such that $x_1 = x$ and $y_1 = y$ and $x * y = x_1 \cdot y_1$,

respectively. Let us consider A. Assume A is complex containing. The functors: addition(A) and multiplication(A) yielding functions from $A \times A$ into A are defined by conditions

(Def. 5) for every objects x, y such that $x, y \in A$ holds addition$(A)(x, y) = x + y$,

(Def. 6) for every objects x, y such that $x, y \in A$ holds multiplication$(A)(x, y) = x * y$,

respectively. Let us consider V. Let x, y be elements of V. The functors: addition

(A, x, y) and multiplication(A, x, y) yielding binominative functions over simple-named complex-valued nominative date of V and A are defined by terms

(Def. 7) lift-binary-op(addition$(A), x, y)$,

(Def. 8) lift-binary-op(multiplication$(A), x, y)$,

respectively.

Let us consider elements i, j of V and complex numbers x, y. Now we state the propositions:

(4) Suppose A is complex containing and $i, j \in \operatorname{dom} d_1$ and $d_1 \in$ dom(addition $(A, i, j))$. Then if $x = d_1(i)$ and $y = d_1(j)$, then (addition$(A, i, j))(d_1) = x + y$.

(5) Suppose A is complex containing and i, $j \in \operatorname{dom} d_1$ and $d_1 \in$ dom(multiplication$(A, i, j))$. Then if $x = d_1(i)$ and $y = d_1(j)$, then (multiplication$(A, i, j))(d_1) = x \cdot y$.

In the sequel *loc* denotes a V-valued function and *val* denotes a function.

Let us consider V, A, and *loc*. The functor factorial-loop-body(A, loc) yielding a binominative function over simple-named complex-valued nominative data of V and A is defined by the term

(Def. 9) $\mathrm{Asg}^{(loc_{/1})}$(addition$(A, loc_{/1}, loc_{/2})) \bullet (\mathrm{Asg}^{(loc_{/4})}$(multiplication$(A, loc_{/4}, loc_{/1})))$.

The functor factorial-main-loop(A, loc) yielding a binominative function over simple-named complex-valued nominative data of V and A is defined by the term

(Def. 10) WH($\neg$ Equality$(A, loc_{/1}, loc_{/3})$, factorial-loop-body(A, loc)).

Let us consider *val*. The functor factorial-var-init(A, loc, val) yielding a binominative function over simple-named complex-valued nominative data of V and A is defined by the term

(Def. 11) PP-composition($\mathrm{Asg}^{(loc_{/1})}(val(1) \Rightarrow_a), \mathrm{Asg}^{(loc_{/2})}(val(2) \Rightarrow_a), \mathrm{Asg}^{(loc_{/3})}(val(3) \Rightarrow_a), \mathrm{Asg}^{(loc_{/4})}(val(4) \Rightarrow_a)$).

The functor factorial-main-part(A, loc, val) yielding a binominative function over simple-named complex-valued nominative data of V and A is defined by the term

(Def. 12) factorial-var-init$(A, loc, val) \bullet$ (factorial-main-loop(A, loc)).

Let us consider z. The functor factorial-program(A, loc, val, z) yielding a binominative function over simple-named complex-valued nominative data of V and A is defined by the term

(Def. 13) factorial-main-part$(A, loc, val) \bullet (\mathrm{Asg}^{z}((loc_{/4}) \Rightarrow_a))$.

In the sequel n_0 denotes a natural number.

Let us consider V, A, *val*, n_0, and d. We say that n_0 and d constitute a valid input for the factorial w.r.t. V, A and *val* if and only if

(Def. 14) there exists a non-atomic nominative data d_1 of V and A such that $d = d_1$ and $\{val(1), val(2), val(3), val(4)\} \subseteq \operatorname{dom} d_1$ and $d_1(val(1)) = 0$ and $d_1(val(2)) = 1$ and $d_1(val(3)) = n_0$ and $d_1(val(4)) = 1$.

The functor valid-factorial-input(V, A, val, n_0) yielding a partial predicate over simple-named complex-valued nominative data of V and A is defined by

(Def. 15) $\operatorname{dom} it = \mathrm{ND}_{\mathrm{SC}}(V, A)$ and for every object d such that $d \in \operatorname{dom} it$ holds if n_0 and d constitute a valid input for the factorial w.r.t. V, A and val, then $it(d) = true$ and if n_0 and d do not constitute a valid input for the factorial w.r.t. V, A and val, then $it(d) = false$.

Note that valid-factorial-input(V, A, val, n_0) is total.

Let us consider z and d. We say that n_0 and d constitute a valid output for the factorial w.r.t. A and z if and only if

(Def. 16) there exists a non-atomic nominative data d_1 of V and A such that $d = d_1$ and $z \in \operatorname{dom} d_1$ and $d_1(z) = n_0!$.

The functor valid-factorial-output(A, z, n_0) yielding a partial predicate over simple-named complex-valued nominative data of V and A is defined by

(Def. 17) $\operatorname{dom} it = \{d$, where d is a nominative data with simple names from V and complex values from $A : d \in \operatorname{dom}(z \Rightarrow_a)\}$ and for every object d such that $d \in \operatorname{dom} it$ holds if n_0 and d constitute a valid output for the factorial w.r.t. A and z, then $it(d) = true$ and if n_0 and d do not constitute a valid output for the factorial w.r.t. A and z, then $it(d) = false$.

Let us consider loc and d. We say that n_0 and d constitute a valid invariant for the factorial w.r.t. A and loc if and only if

(Def. 18) there exists a non-atomic nominative data d_1 of V and A such that $d = d_1$ and $\{loc_{/1}, loc_{/2}, loc_{/3}, loc_{/4}\} \subseteq \operatorname{dom} d_1$ and $d_1(loc_{/2}) = 1$ and $d_1(loc_{/3}) = n_0$ and there exist natural numbers I, S such that $I = d_1(loc_{/1})$ and $S = d_1(loc_{/4})$ and $S = I!$.

The functor factorial-inv(A, loc, n_0) yielding a partial predicate over simple-named complex-valued nominative data of V and A is defined by

(Def. 19) $\operatorname{dom} it = \mathrm{ND}_{\mathrm{SC}}(V, A)$ and for every object d such that $d \in \operatorname{dom} it$ holds if n_0 and d constitute a valid invariant for the factorial w.r.t. A and loc, then $it(d) = true$ and if n_0 and d do not constitute a valid invariant for the factorial w.r.t. A and loc, then $it(d) = false$.

One can check that factorial-inv(A, loc, n_0) is total.

Let us consider val. We say that loc and val are compatible w.r.t. 4 locations if and only if

(Def. 20) $val(4) \neq loc_{/3}$ and $val(4) \neq loc_{/2}$ and $val(4) \neq loc_{/1}$ and $val(3) \neq loc_{/2}$ and $val(3) \neq loc_{/1}$ and $val(2) \neq loc_{/1}$.

Now we state the propositions:

(6) Suppose V is not empty and V is without nonatomic nominative data w.r.t. A and $loc_{/1}$, $loc_{/2}$, $loc_{/3}$, $loc_{/4}$ are mutually different and loc and val are compatible w.r.t. 4 locations. Then $\langle$valid-factorial-input(V, A, val, n_0), factorial-var-init(A, loc, val), factorial-inv$(A, loc, n_0)\rangle$ is an SFHT of $\mathrm{ND}_{\mathrm{SC}}$ (V, A).

Proof: Set $i = loc_{/1}$. Set $j = loc_{/2}$. Set $n = loc_{/3}$. Set $s = loc_{/4}$. Set $i_1 = val(1)$. Set $j_1 = val(2)$. Set $n_1 = val(3)$. Set $s_1 = val(4)$. Set $I =$ valid-factorial-input(V, A, val, n_0). Set $i_2 =$ factorial-inv(A, loc, n_0). Set $D_1 = i_1 \Rightarrow_a$. Set $D_2 = j_1 \Rightarrow_a$. Set $D_3 = n_1 \Rightarrow_a$. Set $D_4 = s_1 \Rightarrow_a$. Set $S_1 = \mathrm{S_P}(i_2, D_4, s)$. Set $R_1 = \mathrm{S_P}(S_1, D_3, n)$. Set $Q_1 = \mathrm{S_P}(R_1, D_2, j)$. Set $P_1 = \mathrm{S_P}(Q_1, D_1, i)$. $I \models P_1$. □

(7) Suppose V is not empty and A is complex containing and V is without nonatomic nominative data w.r.t. A and $loc_{/1}$, $loc_{/2}$, $loc_{/3}$, $loc_{/4}$ are mutually different. Then $\langle$factorial-inv(A, loc, n_0), factorial-loop-body(A, loc), factorial-inv$(A, loc, n_0)\rangle$ is an SFHT of $\mathrm{ND}_{\mathrm{SC}}(V, A)$. The theorem is a consequence of (3), (4), and (5).

(8) $\langle\sim$ factorial-inv(A, loc, n_0), factorial-loop-body(A, loc), factorial-inv$(A, loc, n_0)\rangle$ is an SFHT of $\mathrm{ND}_{\mathrm{SC}}(V, A)$.

(9) Suppose V is not empty and A is complex containing and V is without nonatomic nominative data w.r.t. A and $loc_{/1}$, $loc_{/2}$, $loc_{/3}$, $loc_{/4}$ are mutually different. Then $\langle$factorial-inv(A, loc, n_0), factorial-main-loop(A, loc), Equality$(A, loc_{/1}, loc_{/3})\wedge$factorial-inv$(A, loc, n_0)\rangle$ is an SFHT of $\mathrm{ND}_{\mathrm{SC}}(V, A)$. The theorem is a consequence of (7) and (8).

(10) Suppose V is not empty and A is complex containing and V is without nonatomic nominative data w.r.t. A and $loc_{/1}$, $loc_{/2}$, $loc_{/3}$, $loc_{/4}$ are mutually different and loc and val are compatible w.r.t. 4 locations. Then $\langle$valid-factorial-input(V, A, val, n_0), factorial-main-part(A, loc, val), Equality$(A, loc_{/1}, loc_{/3})\wedge$factorial-inv$(A, loc, n_0)\rangle$ is an SFHT of $\mathrm{ND}_{\mathrm{SC}}(V, A)$. The theorem is a consequence of (6) and (9).

(11) Suppose V is not empty and V is without nonatomic nominative data w.r.t. A and for every T, T is a value on $loc_{/1}$ and T is a value on $loc_{/3}$. Then Equality$(A, loc_{/1}, loc_{/3}) \wedge$ factorial-inv$(A, loc, n_0) \models$ $\mathrm{S_P}($valid-factorial-output$(A, z, n_0), (loc_{/4}) \Rightarrow_a, z)$.

Proof: Set $i = loc_{/1}$. Set $j = loc_{/2}$. Set $n = loc_{/3}$. Set $s = loc_{/4}$. Set $D_4 = s \Rightarrow_a$. Consider d_1 being a non-atomic nominative data of V and A such that $d = d_1$ and $\{i, j, n, s\} \subseteq \operatorname{dom} d_1$ and $d_1(j) = 1$ and $d_1(n) = n_0$ and there exist natural numbers I, S such that $I = d_1(i)$ and $S = d_1(s)$ and $S = I!$. Reconsider $d_2 = d$ as a nominative data with simple names from

V and complex values from A. Set $L = d_2 \nabla_a^z D_4(d_2)$. n_0 and L constitute a valid output for the factorial w.r.t. A and z. □

(12) Suppose V is not empty and V is without nonatomic nominative data w.r.t. A and for every T, T is a value on $loc_{/1}$ and T is a value on $loc_{/3}$. Then $\langle \text{Equality}(A, loc_{/1}, loc_{/3}) \wedge \text{factorial-inv}(A, loc, n_0), \text{Asg}^z((loc_{/4}) \Rightarrow_a),$ $\text{valid-factorial-output}(A, z, n_0)\rangle$ is an SFHT of $\text{ND}_{\text{SC}}(V, A)$. The theorem is a consequence of (11).

(13) Suppose for every T, T is a value on $loc_{/1}$ and T is a value on $loc_{/3}$. Then $\langle \sim (\text{Equality}(A, loc_{/1}, loc_{/3}) \wedge \text{factorial-inv}(A, loc, n_0)), \text{Asg}^z((loc_{/4}) \Rightarrow_a),$ $\text{valid-factorial-output}(A, z, n_0)\rangle$ is an SFHT of $\text{ND}_{\text{SC}}(V, A)$.

(14) Partial correctness of a FACTORIAL algorithm:
Suppose V is not empty and A is complex containing and V is without nonatomic nominative data w.r.t. A and $loc_{/1}$, $loc_{/2}$, $loc_{/3}$, $loc_{/4}$ are mutually different and loc and val are compatible w.r.t. 4 locations and for every T, T is a value on $loc_{/1}$ and T is a value on $loc_{/3}$. Then $\langle \text{valid-factorial-input}(V,$ $A, val, n_0), \text{factorial-program}(A, loc, val, z), \text{valid-factorial-output}(A, z, n_0)\rangle$ is an SFHT of $\text{ND}_{\text{SC}}(V, A)$. The theorem is a consequence of (10), (12), and (13).

References

[1] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pąk. The role of the Mizar Mathematical Library for interactive proof development in Mizar. *Journal of Automated Reasoning*, 61(1):9–32, 2018. doi:10.1007/s10817-017-9440-6.

[2] R.W. Floyd. Assigning meanings to programs. *Mathematical aspects of computer science*, 19(19–32), 1967.

[3] Adam Grabowski, Artur Korniłowicz, and Adam Naumowicz. Four decades of Mizar. *Journal of Automated Reasoning*, 55(3):191–198, 2015. doi:10.1007/s10817-015-9345-1.

[4] C.A.R. Hoare. An axiomatic basis for computer programming. *Commun. ACM*, 12(10): 576–580, 1969.

[5] Ievgen Ivanov and Mykola Nikitchenko. On the sequence rule for the Floyd-Hoare logic with partial pre- and post-conditions. In *Proceedings of the 14th International Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer. Volume II: Workshops, Kyiv, Ukraine, May 14–17, 2018*, volume 2104 of *CEUR Workshop Proceedings*, pages 716–724, 2018.

[6] Ievgen Ivanov, Mykola Nikitchenko, Andrii Kryvolap, and Artur Korniłowicz. Simple-named complex-valued nominative data – definition and basic operations. *Formalized Mathematics*, 25(**3**):205–216, 2017. doi:10.1515/forma-2017-0020.

[7] Ievgen Ivanov, Artur Korniłowicz, and Mykola Nikitchenko. Implementation of the composition-nominative approach to program formalization in Mizar. *The Computer Science Journal of Moldova*, 26(1):59–76, 2018.

[8] Ievgen Ivanov, Artur Korniłowicz, and Mykola Nikitchenko. On an algorithmic algebra over simple-named complex-valued nominative data. *Formalized Mathematics*, 26(**2**):149–158, 2018. doi:10.2478/forma-2018-0012.

[9] Ievgen Ivanov, Artur Korniłowicz, and Mykola Nikitchenko. An inference system of an extension of Floyd-Hoare logic for partial predicates. *Formalized Mathematics*, 26(**2**): 159–164, 2018. doi:10.2478/forma-2018-0013.

[10] Ievgen Ivanov, Artur Korniłowicz, and Mykola Nikitchenko. On algebras of algorithms and specifications over uninterpreted data. *Formalized Mathematics*, 26(**2**):141–147, 2018. doi:10.2478/forma-2018-0011.

[11] Artur Kornilowicz, Andrii Kryvolap, Mykola Nikitchenko, and Ievgen Ivanov. Formalization of the algebra of nominative data in Mizar. In Maria Ganzha, Leszek A. Maciaszek, and Marcin Paprzycki, editors, *Proceedings of the 2017 Federated Conference on Computer Science and Information Systems, FedCSIS 2017, Prague, Czech Republic, September 3–6, 2017.*, pages 237–244, 2017. ISBN 978-83-946253-7-5. doi:10.15439/2017F301.

[12] Artur Kornilowicz, Andrii Kryvolap, Mykola Nikitchenko, and Ievgen Ivanov. Formalization of the nominative algorithmic algebra in Mizar. In Leszek Borzemski, Jerzy Świątek, and Zofia Wilimowska, editors, *Information Systems Architecture and Technology: Proceedings of 38th International Conference on Information Systems Architecture and Technology – ISAT 2017 – Part II, Szklarska Poręba, Poland, September 17–19, 2017*, volume 656 of *Advances in Intelligent Systems and Computing*, pages 176–186. Springer, 2017. ISBN 978-3-319-67228-1. doi:10.1007/978-3-319-67229-8_16.

[13] Artur Korniłowicz, Andrii Kryvolap, Mykola Nikitchenko, and Ievgen Ivanov. An approach to formalization of an extension of Floyd-Hoare logic. In Vadim Ermolayev, Nick Bassiliades, Hans-Georg Fill, Vitaliy Yakovyna, Heinrich C. Mayr, Vyacheslav Kharchenko, Vladimir Peschanenko, Mariya Shyshkina, Mykola Nikitchenko, and Aleksander Spivakovsky, editors, *Proceedings of the 13th International Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer, Kyiv, Ukraine, May 15–18, 2017*, volume 1844 of *CEUR Workshop Proceedings*, pages 504–523. CEUR-WS.org, 2017.

[14] Artur Korniłowicz, Ievgen Ivanov, and Mykola Nikitchenko. Kleene algebra of partial predicates. *Formalized Mathematics*, 26(**1**):11–20, 2018. doi:10.2478/forma-2018-0002.

[15] Andrii Kryvolap, Mykola Nikitchenko, and Wolfgang Schreiner. Extending Floyd-Hoare logic for partial pre- and postconditions. In Vadim Ermolayev, Heinrich C. Mayr, Mykola Nikitchenko, Aleksander Spivakovsky, and Grygoriy Zholtkevych, editors, *Information and Communication Technologies in Education, Research, and Industrial Applications: 9th International Conference, ICTERI 2013, Kherson, Ukraine, June 19–22, 2013, Revised Selected Papers*, pages 355–378. Springer International Publishing, 2013. ISBN 978-3-319-03998-5. doi:10.1007/978-3-319-03998-5_18.

[16] Volodymyr G. Skobelev, Mykola Nikitchenko, and Ievgen Ivanov. On algebraic properties of nominative data and functions. In Vadim Ermolayev, Heinrich C. Mayr, Mykola Nikitchenko, Aleksander Spivakovsky, and Grygoriy Zholtkevych, editors, *Information and Communication Technologies in Education, Research, and Industrial Applications – 10th International Conference, ICTERI 2014, Kherson, Ukraine, June 9–12, 2014, Revised Selected Papers*, volume 469 of *Communications in Computer and Information Science*, pages 117–138. Springer, 2014. ISBN 978-3-319-13205-1. doi:10.1007/978-3-319-13206-8_6.

Accepted May 27, 2019

FORMALIZED MATHEMATICS
Vol. 27, No. 2, Pages 189–195, 2019
DOI: 10.2478/forma-2019-0018

sciendo
https://www.sciendo.com/

Partial Correctness of a Power Algorithm

Adrian Jaszczak
Institute of Informatics
University of Białystok
Poland

Summary. This work continues a formal verification of algorithms written in terms of simple-named complex-valued nominative data [6],[8],[15],[11],[12],[13]. In this paper we present a formalization in the Mizar system [3],[1] of the partial correctness of the algorithm:

```
i := val.1
j := val.2
b := val.3
n := val.4
s := val.5
while (i <> n)
   i := i + j
   s := s * b
return s
```

computing the natural `n` power of given complex number `b`, where variables `i, b, n, s` are located as values of a `V-valued Function`, `loc`, as: `loc/.1 = i`, `loc/.3 = b`, `loc/.4 = n` and `loc/.5 = s`, and the constant `1` is located in the location `loc/.2 = j` (set `V` represents simple names of considered nominative data [17]).

The validity of the algorithm is presented in terms of semantic Floyd-Hoare triples over such data [9]. Proofs of the correctness are based on an inference system for an extended Floyd-Hoare logic [2],[4] with partial pre- and post-conditions [14],[16],[7],[5].

MSC: 68Q60 68T37 03B70 03B35

Keywords: power; nominative data; program verification

MML identifier: NOMIN_6, version: 8.1.09 5.57.1355

Let D be a set and f_1, f_2, f_3, f_4, f_5 be binominative functions of D. The functor PP-composition$(f_1, f_2, f_3, f_4, f_5)$ yielding a binominative function of D is defined by the term

(Def. 1) PP-composition$(f_1, f_2, f_3, f_4) \bullet f_5$.

From now on D denotes a non empty set, f_1, f_2, f_3, f_4, f_5 denote binominative functions of D, and p, q, r, t, w, u denote partial predicates of D.

Now we state the proposition:

(1) Unconditional composition rule for 5 programs: Suppose $\langle p, f_1, q\rangle$ is an SFHT of D and $\langle q, f_2, r\rangle$ is an SFHT of D and $\langle r, f_3, w\rangle$ is an SFHT of D and $\langle w, f_4, t\rangle$ is an SFHT of D and $\langle t, f_5, u\rangle$ is an SFHT of D and $\langle\sim q, f_2, r\rangle$ is an SFHT of D and $\langle\sim r, f_3, w\rangle$ is an SFHT of D and $\langle\sim w, f_4, t\rangle$ is an SFHT of D and $\langle\sim t, f_5, u\rangle$ is an SFHT of D. Then $\langle p, \text{PP-composition}(f_1, f_2, f_3, f_4, f_5), u\rangle$ is an SFHT of D.

In the sequel d, v, v_1 denote objects, V, A denote sets, i, j, b, n, s, z denote elements of V, i_1, j_1, b_1, n_1, s_1 denote objects, d_1, L_2, L_3, L_1, L_4, L_5 denote non-atomic nominative data of V and A, and D_2, D_3, D_1, D_4, D_5 denote binominative functions over simple-named complex-valued nominative date of V and A.

Now we state the propositions:

(2) Suppose V is not empty and V is without nonatomic nominative data w.r.t. A and $D_2 = i_1 \Rightarrow_a$ and $D_3 = j_1 \Rightarrow_a$ and $D_1 = b_1 \Rightarrow_a$ and $D_4 = n_1 \Rightarrow_a$ and $D_5 = s_1 \Rightarrow_a$ and $L_2 = d_1 \nabla^i_a D_2(d_1)$ and $L_3 = L_2 \nabla^j_a D_3(L_2)$ and $L_1 = L_3 \nabla^b_a D_1(L_3)$ and $L_4 = L_1 \nabla^n_a D_4(L_1)$ and $L_5 = L_4 \nabla^s_a D_5(L_4)$ and j_1, b_1, n_1, $s_1 \in \operatorname{dom} d_1$ and $d_1 \in \operatorname{dom} D_2$ and $s \neq n$. Then $L_5(n) = L_4(n)$.

(3) Suppose V is not empty and V is without nonatomic nominative data w.r.t. A and $D_2 = i_1 \Rightarrow_a$ and $D_3 = j_1 \Rightarrow_a$ and $D_1 = b_1 \Rightarrow_a$ and $D_4 = n_1 \Rightarrow_a$ and $D_5 = s_1 \Rightarrow_a$ and $L_2 = d_1 \nabla^i_a D_2(d_1)$ and $L_3 = L_2 \nabla^j_a D_3(L_2)$ and $L_1 = L_3 \nabla^b_a D_1(L_3)$ and $L_4 = L_1 \nabla^n_a D_4(L_1)$ and $L_5 = L_4 \nabla^s_a D_5(L_4)$ and j_1, b_1, n_1, $s_1 \in \operatorname{dom} d_1$ and $d_1 \in \operatorname{dom} D_2$ and $s \neq i$. Then $L_5(i) = L_4(i)$.

In the sequel f denotes a binominative function over simple-named complex-valued nominative data of V and A, T denotes a nominative data with simple names from V and complex values from A, loc denotes a V-valued function, and val denotes a function.

Let us consider V, A, and loc. The functor power-loop-body(A, loc) yielding a binominative function over simple-named complex-valued nominative data of V and A is defined by the term

(Def. 2) $\text{Asg}^{(loc_{/1})}(\text{addition}(A, loc_{/1}, loc_{/2})) \bullet (\text{Asg}^{(loc_{/5})}(\text{multiplication}(A, loc_{/5}, loc_{/3})))$.

The functor power-main-loop(A, loc) yielding a binominative function over simple-named complex-valued nominative data of V and A is defined by the term

(Def. 3) $\mathrm{WH}(\neg\,\mathrm{Equality}(A, loc_{/1}, loc_{/4}), \text{power-loop-body}(A, loc))$.

Let us consider *val*. The functor power-var-init(A, loc, val) yielding a binominative function over simple-named complex-valued nominative data of V and A is defined by the term

(Def. 4) $\text{PP-composition}(\mathrm{Asg}^{(loc_{/1})}(val(1) \Rightarrow_a), \mathrm{Asg}^{(loc_{/2})}(val(2) \Rightarrow_a),$ $\mathrm{Asg}^{(loc_{/3})}(val(3) \Rightarrow_a), \mathrm{Asg}^{(loc_{/4})}(val(4) \Rightarrow_a), \mathrm{Asg}^{(loc_{/5})}(val(5) \Rightarrow_a))$.

The functor power-main-part(A, loc, val) yielding a binominative function over simple-named complex-valued nominative data of V and A is defined by the term

(Def. 5) $\text{power-var-init}(A, loc, val) \bullet (\text{power-main-loop}(A, loc))$.

Let us consider z. The functor power-program(A, loc, val, z) yielding a binominative function over simple-named complex-valued nominative data of V and A is defined by the term

(Def. 6) $\text{power-main-part}(A, loc, val) \bullet (\mathrm{Asg}^{z}((loc_{/5}) \Rightarrow_a))$.

In the sequel n_0 denotes a natural number and b_0 denotes a complex number.

Let us consider V, A, *val*, b_0, n_0, and d. We say that b_0, n_0 and d constitute a valid input for the power w.r.t. V, A and *val* if and only if

(Def. 7) there exists a non-atomic nominative data d_1 of V and A such that $d = d_1$ and $\{val(1), val(2), val(3), val(4), val(5)\} \subseteq \operatorname{dom} d_1$ and $d_1(val(1)) = 0$ and $d_1(val(2)) = 1$ and $d_1(val(3)) = b_0$ and $d_1(val(4)) = n_0$ and $d_1(val(5)) = 1$.

The functor valid-power-input(V, A, val, b_0, n_0) yielding a partial predicate over simple-named complex-valued nominative data of V and A is defined by

(Def. 8) $\operatorname{dom} it = \mathrm{ND}_{\mathrm{SC}}(V, A)$ and for every object d such that $d \in \operatorname{dom} it$ holds if b_0, n_0 and d constitute a valid input for the power w.r.t. V, A and *val*, then $it(d) = \mathit{true}$ and if b_0, n_0 and d do not constitute a valid input for the power w.r.t. V, A and *val*, then $it(d) = \mathit{false}$.

Let us observe that valid-power-input(V, A, val, b_0, n_0) is total.

Let us consider z and d. We say that b_0, n_0 and d constitute a valid output for the power w.r.t. A and z if and only if

(Def. 9) there exists a non-atomic nominative data d_1 of V and A such that $d = d_1$ and $z \in \operatorname{dom} d_1$ and $d_1(z) = {b_0}^{n_0}$.

The functor valid-power-output(A, z, b_0, n_0) yielding a partial predicate over simple-named complex-valued nominative data of V and A is defined by

(Def. 10) $\operatorname{dom} it = \{d$, where d is a nominative data with simple names from V and complex values from $A : d \in \operatorname{dom}(z \Rightarrow_a)\}$ and for every object d such that $d \in \operatorname{dom} it$ holds if b_0, n_0 and d constitute a valid output for the power w.r.t. A and z, then $it(d) = \mathit{true}$ and if b_0, n_0 and d do not constitute a valid output for the power w.r.t. A and z, then $it(d) = \mathit{false}$.

Let us consider loc and d. We say that b_0, n_0 and d constitute a valid invariant for the power w.r.t. A and loc if and only if

(Def. 11) there exists a non-atomic nominative data d_1 of V and A such that $d = d_1$ and $\{loc_{/1}, loc_{/2}, loc_{/3}, loc_{/4}, loc_{/5}\} \subseteq \operatorname{dom} d_1$ and $d_1(loc_{/2}) = 1$ and $d_1(loc_{/3}) = b_0$ and $d_1(loc_{/4}) = n_0$ and there exists a complex number S and there exists a natural number I such that $I = d_1(loc_{/1})$ and $S = d_1(loc_{/5})$ and $S = {b_0}^{I}$.

The functor PP-composition(A, loc, b_0, n_0) yielding a partial predicate over simple-named complex-valued nominative data of V and A is defined by

(Def. 12) $\operatorname{dom} it = \mathrm{ND}_{\mathrm{SC}}(V, A)$ and for every object d such that $d \in \operatorname{dom} it$ holds if b_0, n_0 and d constitute a valid invariant for the power w.r.t. A and loc, then $it(d) = \mathit{true}$ and if b_0, n_0 and d do not constitute a valid invariant for the power w.r.t. A and loc, then $it(d) = \mathit{false}$.

Observe that PP-composition(A, loc, b_0, n_0) is total.

Let us consider val. We say that loc and val are compatible w.r.t. 5 locations if and only if

(Def. 13) $val(5) \neq loc_{/4}$ and $val(5) \neq loc_{/3}$ and $val(5) \neq loc_{/2}$ and $val(5) \neq loc_{/1}$ and $val(4) \neq loc_{/3}$ and $val(4) \neq loc_{/2}$ and $val(4) \neq loc_{/1}$ and $val(3) \neq loc_{/2}$ and $val(3) \neq loc_{/1}$ and $val(2) \neq loc_{/1}$.

Now we state the propositions:

(4) Suppose V is not empty and V is without nonatomic nominative data w.r.t. A and $loc_{/1}$,$loc_{/2}$,$loc_{/3}$,$loc_{/4}$,$loc_{/5}$ are mutually different and loc and val are compatible w.r.t. 5 locations. Then $\langle$valid-power-input(V, A, val, b_0, n_0), power-var-init(A, loc, val), PP-composition$(A, loc, b_0, n_0)\rangle$ is an SFHT of $\mathrm{ND}_{\mathrm{SC}}(V, A)$.

Proof: Set $i = loc_{/1}$. Set $j = loc_{/2}$. Set $b = loc_{/3}$. Set $n = loc_{/4}$. Set $s = loc_{/5}$. Set $i_1 = val(1)$. Set $j_1 = val(2)$. Set $b_1 = val(3)$. Set $n_1 = val(4)$. Set $s_1 = val(5)$. Set $I =$ valid-power-input(V, A, val, b_0, n_0). Set $i_2 =$ PP-composition(A, loc, b_0, n_0). Set $D_2 = i_1 \Rightarrow_a$. Set $D_3 = j_1 \Rightarrow_a$. Set $D_1 = b_1 \Rightarrow_a$. Set $D_4 = n_1 \Rightarrow_a$. Set $D_5 = s_1 \Rightarrow_a$. Set $T_1 = \mathrm{S}_{\mathrm{P}}(i_2, D_5, s)$. Set $S_1 = \mathrm{S}_{\mathrm{P}}(T_1, D_4, n)$. Set $R_1 = \mathrm{S}_{\mathrm{P}}(S_1, D_1, b)$. Set $Q_1 = \mathrm{S}_{\mathrm{P}}(R_1, D_3, j)$. Set $P_1 = \mathrm{S}_{\mathrm{P}}(Q_1, D_2, i)$. $I \models P_1$ by [6, (39)], [8, (9)], [10, (4)]. □

(5) Suppose V is not empty and A is complex containing and V is without nonatomic nominative data w.r.t. A and $loc_{/1}$,$loc_{/2}$,$loc_{/3}$,$loc_{/4}$,$loc_{/5}$ are

mutually different. Then $\langle$PP-composition(A, loc, b_0, n_0), power-loop-body (A, loc), PP-composition$(A, loc, b_0, n_0)\rangle$ is an SFHT of $\mathrm{ND}_{\mathrm{SC}}(V, A)$.

(6) $\langle\sim$ PP-composition(A, loc, b_0, n_0), power-loop-body(A, loc), PP-composition$(A, loc, b_0, n_0)\rangle$ is an SFHT of $\mathrm{ND}_{\mathrm{SC}}(V, A)$.

(7) Suppose V is not empty and A is complex containing and V is without nonatomic nominative data w.r.t. A and $loc_{/1}$,$loc_{/2}$,$loc_{/3}$,$loc_{/4}$,$loc_{/5}$ are mutually different. Then $\langle$PP-composition(A, loc, b_0, n_0), power-main-loop (A, loc), Equality$(A, loc_{/1}, loc_{/4})\wedge$PP-composition$(A, loc, b_0, n_0)\rangle$ is an SFHT of $\mathrm{ND}_{\mathrm{SC}}(V, A)$. The theorem is a consequence of (5) and (6).

(8) Suppose V is not empty and A is complex containing and V is without nonatomic nominative data w.r.t. A and $loc_{/1}$,$loc_{/2}$,$loc_{/3}$,$loc_{/4}$,$loc_{/5}$ are mutually different and loc and val are compatible w.r.t. 5 locations. Then $\langle$valid-power-input(V, A, val, b_0, n_0), power-main-part(A, loc, val), Equality $(A, loc_{/1}, loc_{/4})\wedge$PP-composition$(A, loc, b_0, n_0)\rangle$ is an SFHT of $\mathrm{ND}_{\mathrm{SC}}(V, A)$. The theorem is a consequence of (4) and (7).

(9) Suppose V is not empty and V is without nonatomic nominative data w.r.t. A and for every T, T is a value on $loc_{/1}$ and for every T, T is a value on $loc_{/4}$. Then Equality$(A, loc_{/1}, loc_{/4}) \wedge$ PP-composition$(A, loc, b_0, n_0) \models$ S_{P}(valid-power-output(A, z, b_0, n_0), $(loc_{/5}) \Rightarrow_a, z)$.

Proof: Set $i = loc_{/1}$. Set $j = loc_{/2}$. Set $b = loc_{/3}$. Set $n = loc_{/4}$. Set $s = loc_{/5}$. Set $D_5 = s \Rightarrow_a$. Consider d_1 being a non-atomic nominative data of V and A such that $d = d_1$ and $\{i, j, b, n, s\} \subseteq \operatorname{dom} d_1$ and $d_1(n) = n_0$ and $d_1(b) = b_0$ and there exists a complex number S and there exists a natural number I such that $I = d_1(i)$ and $S = d_1(s)$ and $S = {b_0}^I$. Reconsider $d_2 = d$ as a nominative data with simple names from V and complex values from A. Set $L = d_2 \nabla_a^z D_5(d_2)$. b_0, n_0 and L constitute a valid output for the power w.r.t. A and z. □

(10) Suppose V is not empty and V is without nonatomic nominative data w.r.t. A and for every T, T is a value on $loc_{/1}$ and for every T, T is a value on $loc_{/4}$. Then $\langle$Equality$(A, loc_{/1}, loc_{/4}) \wedge$ PP-composition(A, loc, b_0, n_0), $\mathrm{Asg}^z((loc_{/5}) \Rightarrow_a)$, valid-power-output$(A, z, b_0, n_0)\rangle$ is an SFHT of $\mathrm{ND}_{\mathrm{SC}}(V, A)$. The theorem is a consequence of (9).

(11) Suppose for every T, T is a value on $loc_{/1}$ and for every T, T is a value on $loc_{/4}$. Then $\langle\sim$ (Equality$(A, loc_{/1}, loc_{/4}) \wedge$ PP-composition(A, loc, b_0, n_0)), $\mathrm{Asg}^z((loc_{/5}) \Rightarrow_a)$, valid-power-output$(A, z, b_0, n_0)\rangle$
is an SFHT of $\mathrm{ND}_{\mathrm{SC}}(V, A)$.

(12) Partial correctness of a POWER algorithm:
Suppose V is not empty and A is complex containing and V is without nonatomic nominative data w.r.t. A and $loc_{/1}$,$loc_{/2}$,$loc_{/3}$,$loc_{/4}$,$loc_{/5}$ are

mutually different and loc and val are compatible w.r.t. 5 locations and for every T, T is a value on $loc_{/1}$ and for every T, T is a value on $loc_{/4}$. Then $\langle$valid-power-input(V, A, val, b_0, n_0), power-program(A, loc, val, z), valid-power-output$(A, z, b_0, n_0)\rangle$ is an SFHT of $\mathrm{ND}_{\mathrm{SC}}(V, A)$. The theorem is a consequence of (8), (10), and (11).

References

[1] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pąk. The role of the Mizar Mathematical Library for interactive proof development in Mizar. *Journal of Automated Reasoning*, 61(1):9–32, 2018. doi:10.1007/s10817-017-9440-6.

[2] R.W. Floyd. Assigning meanings to programs. *Mathematical aspects of computer science*, 19(19–32), 1967.

[3] Adam Grabowski, Artur Korniłowicz, and Adam Naumowicz. Four decades of Mizar. *Journal of Automated Reasoning*, 55(3):191–198, 2015. doi:10.1007/s10817-015-9345-1.

[4] C.A.R. Hoare. An axiomatic basis for computer programming. *Commun. ACM*, 12(10): 576–580, 1969.

[5] Ievgen Ivanov and Mykola Nikitchenko. On the sequence rule for the Floyd-Hoare logic with partial pre- and post-conditions. In *Proceedings of the 14th International Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer. Volume II: Workshops, Kyiv, Ukraine, May 14–17, 2018*, volume 2104 of *CEUR Workshop Proceedings*, pages 716–724, 2018.

[6] Ievgen Ivanov, Mykola Nikitchenko, Andrii Kryvolap, and Artur Korniłowicz. Simple-named complex-valued nominative data – definition and basic operations. *Formalized Mathematics*, 25(**3**):205–216, 2017. doi:10.1515/forma-2017-0020.

[7] Ievgen Ivanov, Artur Korniłowicz, and Mykola Nikitchenko. Implementation of the composition-nominative approach to program formalization in Mizar. *The Computer Science Journal of Moldova*, 26(1):59–76, 2018.

[8] Ievgen Ivanov, Artur Korniłowicz, and Mykola Nikitchenko. On an algorithmic algebra over simple-named complex-valued nominative data. *Formalized Mathematics*, 26(**2**):149–158, 2018. doi:10.2478/forma-2018-0012.

[9] Ievgen Ivanov, Artur Korniłowicz, and Mykola Nikitchenko. An inference system of an extension of Floyd-Hoare logic for partial predicates. *Formalized Mathematics*, 26(**2**): 159–164, 2018. doi:10.2478/forma-2018-0013.

[10] Ievgen Ivanov, Artur Korniłowicz, and Mykola Nikitchenko. Partial correctness of GCD algorithm. *Formalized Mathematics*, 26(**2**):165–173, 2018. doi:10.2478/forma-2018-0014.

[11] Ievgen Ivanov, Artur Korniłowicz, and Mykola Nikitchenko. On algebras of algorithms and specifications over uninterpreted data. *Formalized Mathematics*, 26(**2**):141–147, 2018. doi:10.2478/forma-2018-0011.

[12] Artur Kornilowicz, Andrii Kryvolap, Mykola Nikitchenko, and Ievgen Ivanov. Formalization of the algebra of nominative data in Mizar. In Maria Ganzha, Leszek A. Maciaszek, and Marcin Paprzycki, editors, *Proceedings of the 2017 Federated Conference on Computer Science and Information Systems, FedCSIS 2017, Prague, Czech Republic, September 3–6, 2017.*, pages 237–244, 2017. ISBN 978-83-946253-7-5. doi:10.15439/2017F301.

[13] Artur Kornilowicz, Andrii Kryvolap, Mykola Nikitchenko, and Ievgen Ivanov. Formalization of the nominative algorithmic algebra in Mizar. In Leszek Borzemski, Jerzy Świątek, and Zofia Wilimowska, editors, *Information Systems Architecture and Technology: Proceedings of 38th International Conference on Information Systems Architecture and Technology – ISAT 2017 – Part II, Szklarska Poręba, Poland, September 17–19, 2017*, volume 656 of *Advances in Intelligent Systems and Computing*, pages 176–186. Springer, 2017. ISBN 978-3-319-67228-1. doi:10.1007/978-3-319-67229-8_16.

[14] Artur Korniłowicz, Andrii Kryvolap, Mykola Nikitchenko, and Ievgen Ivanov. An approach to formalization of an extension of Floyd-Hoare logic. In Vadim Ermolayev, Nick Bassiliades, Hans-Georg Fill, Vitaliy Yakovyna, Heinrich C. Mayr, Vyacheslav Kharchen-

ko, Vladimir Peschanenko, Mariya Shyshkina, Mykola Nikitchenko, and Aleksander Spivakovsky, editors, *Proceedings of the 13th International Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer, Kyiv, Ukraine, May 15–18, 2017*, volume 1844 of *CEUR Workshop Proceedings*, pages 504–523. CEUR-WS.org, 2017.

[15] Artur Korniłowicz, Ievgen Ivanov, and Mykola Nikitchenko. Kleene algebra of partial predicates. *Formalized Mathematics*, 26(**1**):11–20, 2018. doi:10.2478/forma-2018-0002.

[16] Andrii Kryvolap, Mykola Nikitchenko, and Wolfgang Schreiner. Extending Floyd-Hoare logic for partial pre- and postconditions. In Vadim Ermolayev, Heinrich C. Mayr, Mykola Nikitchenko, Aleksander Spivakovsky, and Grygoriy Zholtkevych, editors, *Information and Communication Technologies in Education, Research, and Industrial Applications: 9th International Conference, ICTERI 2013, Kherson, Ukraine, June 19–22, 2013, Revised Selected Papers*, pages 355–378. Springer International Publishing, 2013. ISBN 978-3-319-03998-5. doi:10.1007/978-3-319-03998-5_18.

[17] Volodymyr G. Skobelev, Mykola Nikitchenko, and Ievgen Ivanov. On algebraic properties of nominative data and functions. In Vadim Ermolayev, Heinrich C. Mayr, Mykola Nikitchenko, Aleksander Spivakovsky, and Grygoriy Zholtkevych, editors, *Information and Communication Technologies in Education, Research, and Industrial Applications – 10th International Conference, ICTERI 2014, Kherson, Ukraine, June 9–12, 2014, Revised Selected Papers*, volume 469 of *Communications in Computer and Information Science*, pages 117–138. Springer, 2014. ISBN 978-3-319-13205-1. doi:10.1007/978-3-319-13206-8_6.

Accepted May 27, 2019

FORMALIZED MATHEMATICS
Vol. **27**, No. **2**, Pages 197–208, **2019**
DOI: 10.2478/forma-2019-0019

sciendo
https://www.sciendo.com/

Diophantine Sets. Part II

Karol Pąk
Institute of Informatics
University of Białystok
Poland

Summary. The article is the next in a series aiming to formalize the MDPR-theorem using the Mizar proof assistant [3], [6], [4]. We analyze four equations from the Diophantine standpoint that are crucial in the bounded quantifier theorem, that is used in one of the approaches to solve the problem.

Based on our previous work [1], we prove that the value of a given binomial coefficient and factorial can be determined by its arguments in a Diophantine way. Then we prove that two products

$$z=\prod_{i=1}^{x}(1+i\cdot y),\qquad z=\prod_{i=1}^{x}(y+1-j),\tag{0.1}$$

where $y > x$ are Diophantine.

The formalization follows [10], Z. Adamowicz, P. Zbierski [2] as well as M. Davis [5].

MSC: 11D45 68T99 03B35

Keywords: Hilbert's 10th problem; Diophantine relations

MML identifier: HILB10_4, version: 8.1.09 5.57.1355

1. Product of Zero Based Finite Sequences

From now on i, j, n, n_1, n_2, m, k, l, u denote natural numbers, r, r_1, r_2 denote real numbers, x, y denote integers, a, b denote non trivial natural numbers, F denotes a finite 0-sequence, $\mathcal{F}$, $\mathcal{F}_1$, $\mathcal{F}_2$ denote complex-valued finite 0-sequences, and c, c_1, c_2 denote complex numbers.

Let us consider c_1 and c_2. Let us note that $\langle c_1, c_2\rangle$ is complex-valued.

Let $\mathcal{F}$ be a finite 0-sequence. The functor $\prod \mathcal{F}$ yielding an element of $\mathbb{C}$ is defined by the term

(Def. 1) $\cdot_{\mathbb{C}} \odot \mathcal{F}$.

Now we state the propositions:

(1) If $\mathcal{F}$ is real-valued, then $\prod \mathcal{F} = \cdot_{\mathbb{R}} \odot \mathcal{F}$.

(2) If $\mathcal{F}$ is $\mathbb{Z}$-valued, then $\prod \mathcal{F} = \cdot_{\mathbb{Z}} \odot \mathcal{F}$.

(3) If $\mathcal{F}$ is natural-valued, then $\prod \mathcal{F} = \cdot_{\mathbb{N}} \odot \mathcal{F}$.

Let F be a real-valued finite 0-sequence. One can check that $\prod F$ is real.

Let F be a natural-valued finite 0-sequence. One can verify that $\prod F$ is natural.

Now we state the propositions:

(4) If $\mathcal{F} = \emptyset$, then $\prod \mathcal{F} = 1$.

(5) $\prod \langle c \rangle = c$.

(6) $\prod \langle c_1, c_2 \rangle = c_1 \cdot c_2$.

(7) $\prod (\mathcal{F}_1 \frown \mathcal{F}_2) = (\prod \mathcal{F}_1) \cdot (\prod \mathcal{F}_2)$.

(8) $c + \mathcal{F}_1 \frown \mathcal{F}_2 = (c + \mathcal{F}_1) \frown (c + \mathcal{F}_2)$.

PROOF: For every object x such that $x \in \operatorname{dom}(c + \mathcal{F}_1 \frown \mathcal{F}_2)$ holds $(c + \mathcal{F}_1 \frown \mathcal{F}_2)(x) = ((c + \mathcal{F}_1) \frown (c + \mathcal{F}_2))(x)$. □

(9) $c_1 + \langle c_2 \rangle = \langle c_1 + c_2 \rangle$.

(10) Let us consider finite 0-sequences f_1, f_2, and n. Suppose $n \leqslant \operatorname{len} f_1$. Then $(f_1 \frown f_2)_{\lfloor n} = f_{1 \lfloor n} \frown f_2$.

Let us consider n. One can verify that there exists a finite 0-sequence which is n-element and natural-valued and there exists a finite 0-sequence which is natural-valued and positive yielding.

Let R be a positive yielding binary relation and X be a set. Observe that $R \restriction X$ is positive yielding.

Let X be a positive yielding, real-valued finite 0-sequence. One can verify that $\prod X$ is positive.

Now we state the proposition:

(11) Let us consider a natural-valued, positive yielding finite 0-sequence X. If $i \in \operatorname{dom} X$, then $X(i) \leqslant \prod X$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every natural-valued, positive yielding finite 0-sequence X for every natural number i such that $\operatorname{len} X = \$_1$ and $i \in \operatorname{dom} X$ holds $X(i) \leqslant \prod X$. If $\mathcal{P}[n]$, then $\mathcal{P}[n+1]$. $\mathcal{P}[n]$. □

Let X be a natural-valued finite 0-sequence and n be a positive natural number. Let us observe that $n + X$ is positive yielding.

Now we state the proposition:

(12) Let us consider natural-valued finite 0-sequences X_1, X_2. Suppose $\operatorname{len} X_1 = \operatorname{len} X_2$ and for every n such that $n \in \operatorname{dom} X_1$ holds $X_1(n) \leqslant X_2(n)$. Then $\prod X_1 \leqslant \prod X_2$.

Proof: Define $\mathcal{P}$[natural number] $\equiv$ for every natural-valued finite 0-sequences X_1, X_2 such that $\operatorname{len} X_1 = \$_1 = \operatorname{len} X_2$ and for every n such that $n \in \operatorname{dom} X_1$ holds $X_1(n) \leqslant X_2(n)$ holds $\prod X_1 \leqslant \prod X_2$. $\mathcal{P}[0]$. If $\mathcal{P}[n]$, then $\mathcal{P}[n+1]$. $\mathcal{P}[n]$. □

2. Binomial is Diophantine

Now we state the propositions:

(13) If $k \leqslant n$, then $\binom{n}{k} \leqslant n^k$.

Proof: Define $\mathcal{P}$[natural number] $\equiv$ if $\$_1 \leqslant n$, then $\binom{n}{\$_1} \leqslant n^{\$_1}$. If $\mathcal{P}[m]$, then $\mathcal{P}[m+1]$. $\mathcal{P}[m]$. □

(14) If $u > n^k$ and $n \geqslant k > i$, then $\binom{n}{i} \cdot (u^i) < \frac{u^k}{n}$. The theorem is a consequence of (13).

(15) If $u > n^k$ and $n \geqslant k$, then $\lfloor \frac{(u+1)^n}{u^k} \rfloor \bmod u = \binom{n}{k}$.

Proof: Set $I = \langle \binom{n}{0} 1^0 u^n, \ldots, \binom{n}{n} 1^n u^0 \rangle$. Set $k_1 = k + 1$. Consider q being a finite sequence such that $I = (I \restriction k_1) \frown q$. Reconsider $I_1 = I$ as a finite sequence of elements of $\mathbb{N}$. Set $k_2 = k \mapsto \frac{u^k}{n}$. For every natural number i such that $i \in \operatorname{Seg} k$ holds $(I_1 \restriction k)(i) < k_2(i)$. Define $\mathcal{P}$[natural number, object] $\equiv \$_2 \in \mathbb{N}$ and for every natural number i such that $i = \$_2$ holds $q(\$_1) = u^k \cdot u \cdot i$. For every natural number j such that $j \in \operatorname{Seg} \operatorname{len} q$ there exists an object x such that $\mathcal{P}[j, x]$. Consider Q being a finite sequence such that $\operatorname{dom} Q = \operatorname{Seg} \operatorname{len} q$ and for every natural number j such that $j \in \operatorname{Seg} \operatorname{len} q$ holds $\mathcal{P}[j, Q(j)]$. $\operatorname{rng} Q \subseteq \mathbb{N}$. For every natural number i such that $1 \leqslant i \leqslant \operatorname{len} q$ holds $q(i) = (u^k \cdot u \cdot Q)(i)$. $\lfloor \frac{\sum I_1}{u^k} \rfloor = \binom{n}{k} + u \cdot (\sum Q)$. $\binom{n}{k} \leqslant n^k$. □

(16) Let us consider natural numbers x, y, z. Then $x \geqslant z$ and $y = \binom{x}{z}$ if and only if there exist natural numbers u, v, y_1, y_2, y_3 such that $y_1 = x^z$ and $y_2 = (u+1)^x$ and $y_3 = u^z$ and $u > y_1$ and $v = \lfloor \frac{y_2}{y_3} \rfloor$ and $y \equiv v \pmod{u}$ and $y < u$ and $x \geqslant z$.

Proof: If $x \geqslant z$ and $y = \binom{x}{z}$, then there exist natural numbers u, v, y_1, y_2, y_3 such that $y_1 = x^z$ and $y_2 = (u+1)^x$ and $y_3 = u^z$ and $u > y_1$ and $v = \lfloor \frac{y_2}{y_3} \rfloor$ and $y \equiv v \pmod{u}$ and $y < u$ and $x \geqslant z$. $y \bmod u = \binom{x}{z}$. □

3. Factorial is Diophantine

Now we state the propositions:

(17) If $k > 0$ and $n > 2 \cdot k^{k+1}$, then $k! = \lfloor \frac{n^k}{\binom{n}{k}} \rfloor$.

(18) Let us consider natural numbers x, y. Then $y = x!$ if and only if there exist natural numbers n, y_1, y_2, y_3 such that $y_1 = 2 \cdot x^{x+1}$ and $y_2 = n^x$ and $y_3 = \binom{n}{x}$ and $n > y_1$ and $y = \lfloor \frac{y_2}{y_3} \rfloor$.
Proof: If $y = x!$, then there exist natural numbers n, y_1, y_2, y_3 such that $y_1 = 2 \cdot x^{x+1}$ and $y_2 = n^x$ and $y_3 = \binom{n}{x}$ and $n > y_1$ and $y = \lfloor \frac{y_2}{y_3} \rfloor$. □

4. Diophanticity of Selected Products

In the sequel x, y, x_1, u, w denote natural numbers.

Now we state the propositions:

(19) Let us consider natural numbers x_1, w, u. Suppose $x_1 \cdot w \equiv 1 \pmod{u}$. Let us consider a natural number x. Then $\prod(1 + x_1 \cdot (\mathrm{idseq}(x))) \equiv {x_1}^x \cdot (x!) \cdot \binom{w+x}{x} \pmod{u}$.
Proof: Consider b being an integer such that $u \cdot b = x_1 \cdot w - 1$. Define $\mathcal{P}[\text{natural number}] \equiv \prod(1 + x_1 \cdot (\mathrm{idseq}(\$_1))) \equiv {x_1}^{\$_1} \cdot (\$_1!) \cdot \binom{w+\$_1}{\$_1} \pmod{u}$. If $\mathcal{P}[n]$, then $\mathcal{P}[n+1]$ by [12, (43)]. $\mathcal{P}[n]$. □

(20) Let us consider natural numbers x, y, x_1. Suppose $x_1 \geqslant 1$. Then $y = \prod(1 + x_1 \cdot (\mathrm{idseq}(x)))$ if and only if there exist natural numbers u, w, y_1, y_2, y_3, y_4, y_5 such that $u > y$ and $x_1 \cdot w \equiv 1 \pmod{u}$ and $y_1 = {x_1}^x$ and $y_2 = x!$ and $y_3 = \binom{w+x}{x}$ and $y_1 \cdot y_2 \cdot y_3 \equiv y \pmod{u}$ and $y_4 = 1 + x_1 \cdot x$ and $y_5 = {y_4}^x$ and $u > y_5$.
Proof: Define $\mathcal{P}[\text{natural number}] \equiv (1 + x_1 \cdot \$_1)^{\$_1} \geqslant \prod(1+x_1 \cdot (\mathrm{idseq}(\$_1)))$. If $\mathcal{P}[n]$, then $\mathcal{P}[n+1]$. $\mathcal{P}[n]$. If $y = \prod(1+x_1 \cdot (\mathrm{idseq}(x)))$, then there exist natural numbers u, w, y_1, y_2, y_3, y_4, y_5 such that $u > y$ and $x_1 \cdot w \equiv 1 \pmod{u}$ and $y_1 = {x_1}^x$ and $y_2 = x!$ and $y_3 = \binom{w+x}{x}$ and $y_1 \cdot y_2 \cdot y_3 \equiv y \pmod{u}$ and $y_4 = 1+x_1 \cdot x$ and $y_5 = {y_4}^x$ and $u > y_5$ by [8, (16)]. Set $U = {x_1}^x \cdot (x!) \cdot \binom{w+x}{x}$. $\prod(1 + x_1 \cdot (\mathrm{idseq}(x))) \equiv U \pmod{u}$. □

(21) $c_1 + n \mapsto c_2 = n \mapsto (c_1 + c_2)$.

(22) Let us consider natural numbers x, y, x_1. If $x_1 = 0$, then $y = \prod(1 + x_1 \cdot (\mathrm{idseq}(x)))$ iff $y = 1$. The theorem is a consequence of (21).

(23) If $n \geqslant k$, then $\prod(n + 1 + -\mathrm{idseq}(k)) = k! \cdot \binom{n}{k}$.
Proof: Define $\mathcal{P}[\text{natural number}] \equiv$ if $\$_1 \leqslant n$, then $\prod(n+1+-\mathrm{idseq}(\$_1)) = \$_1! \cdot \binom{n}{\$_1}$. If $\mathcal{P}[i]$, then $\mathcal{P}[i+1]$ by [7, (3), (2)]. $\mathcal{P}[i]$. □

(24) Let us consider natural numbers y, x_1, x_2. Then $y = \prod(x_2 + 1 + -\mathrm{idseq}(x_1))$ and $x_2 > x_1$ if and only if $y = x_1! \cdot \binom{x_2}{x_1}$ and $x_2 > x_1$.

5. Selected Subsets of Zero Based Finite Sequences of $\mathbb{N}$ as Diophantine Sets

From now on n, m, k denote natural numbers, p, q denote n-element finite 0-sequences of $\mathbb{N}$, i_1, i_2, i_3, i_4, i_5, i_6 denote elements of n, and a, b, d, f denote integers.

Now we state the propositions:

(25) Let us consider natural numbers a, b, i_1, i_2, and i_3. Then $\{p : p(i_1) = (a \cdot p(i_2) + b) \cdot p(i_3)\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$.
Proof: Define $\mathcal{R}(\text{natural number}, \text{natural number}, \text{natural number}) = a \cdot \$_1 + b$. Define $\mathcal{P}_1[\text{natural number}, \text{natural number}, \text{natural object}, \text{natural number}, \text{natural number}, \text{natural number}] \equiv 1 \cdot \$_1 = 1 \cdot \$_3 \cdot \$_2$. For every n, i_1, i_2, i_3, i_4, and i_5, $\{p : \mathcal{P}_1[p(i_1), p(i_2), \mathcal{R}(p(i_3), p(i_4), p(i_5)), p(i_3), p(i_4), p(i_5)]\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$. Define $\mathcal{Q}_1[\text{finite 0-sequence of } \mathbb{N}] \equiv \mathcal{P}_1[\$_1(i_1), \$_1(i_3), a \cdot \$_1(i_2) + b, \$_1(i_3), \$_1(i_3), \$_1(i_3)]$. Define $\mathcal{Q}_2[\text{finite 0-sequence of } \mathbb{N}] \equiv \$_1(i_1) = (a \cdot \$_1(i_2) + b) \cdot \$_1(i_3)$. $\{p : \mathcal{Q}_1[p]\} = \{q : \mathcal{Q}_2[q]\}$. □

(26) $\{p : p(i_1) = a \cdot p(i_2) \cdot p(i_3)\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$.
Proof: Define $\mathcal{Q}_1[\text{finite 0-sequence of } \mathbb{N}] \equiv 1 \cdot \$_1(i_1) = a \cdot \$_1(i_2) \cdot \$_1(i_3)$. Define $\mathcal{Q}_2[\text{finite 0-sequence of } \mathbb{N}] \equiv \$_1(i_1) = a \cdot \$_1(i_2) \cdot \$_1(i_3)$. $\{p : \mathcal{Q}_1[p]\} = \{q : \mathcal{Q}_2[q]\}$. □

(27) Let us consider a Diophantine subset A of the n-xtuples of $\mathbb{N}$, and natural numbers k, n_4. Suppose $k + n_4 = n$. Then $\{p_{\lfloor n_4} : p \in A\}$ is a Diophantine subset of the k-xtuples of $\mathbb{N}$.
Proof: Consider n_3 being a natural number, p_1 being a $\mathbb{Z}$-valued polynomial of $n + n_3$,$\mathbb{R}_{\mathrm{F}}$ such that for every object s, $s \in A$ iff there exists an n-element finite 0-sequence x of $\mathbb{N}$ and there exists an n_3-element finite 0-sequence y of $\mathbb{N}$ such that $s = x$ and $\mathrm{eval}(p_1, {}^{@}(x \frown y)) = 0$. Reconsider $I = \mathrm{id}_{n+n_3}$ as a finite 0-sequence. Set $I_1 = I \upharpoonright n_4$. Set $I_2 = (I \upharpoonright n)_{\lfloor n_4}$. Set $I_3 = I_{\lfloor n}$. Reconsider $J = (I_2 \frown I_1) \frown I_3$ as a function from $n + n_3$ into $n + n_3$. Set $h =$ the p_1 permuted by J^{-1}. Reconsider $H = h$ as a polynomial of $k + (n_4 + n_3)$,$\mathbb{R}_{\mathrm{F}}$. Set $Y = \{p_{\lfloor n_4} : p \in A\}$. $Y \subseteq$ the k-xtuples of $\mathbb{N}$. For every object s, $s \in Y$ iff there exists a k-element finite 0-sequence x of $\mathbb{N}$ and there exists an $(n_4 + n_3)$-element finite 0-sequence y of $\mathbb{N}$ such that $s = x$ and $\mathrm{eval}(H, {}^{@}(x \frown y)) = 0$ by [9, (25)], [11, (27)]. □

(28) Let us consider integers a, b, a natural number c, i_1, i_2, and i_3. Then $\{p : a\cdot p(i_1) = \lfloor\frac{b\cdot p(i_2)}{c\cdot p(i_3)}\rfloor$ and $c\cdot p(i_3)\neq 0\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$.

Proof: Define $\mathcal{F}_2$(natural number, natural number, natural number) $= c\cdot\$_3+a\cdot c\cdot\$_1\cdot\$_3$. For every n, i_1, i_2, i_3, i_4, and d, $\{p : \mathcal{F}_2(p(i_1), p(i_2), p(i_3)) = d\cdot p(i_4)\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$. Define $\mathcal{P}_2$[natural number, natural number, integer] $\equiv b\cdot\$_1+0<\$_3$. For every n, i_1, i_2, i_3, i_4, and i_5, $\{p : \mathcal{P}_2[p(i_1), p(i_2), \mathcal{F}_2(p(i_3), p(i_4), p(i_5))]\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$. Define $\mathcal{P}_3$[natural number, natural number, integer] $\equiv b\cdot\$_1\geqslant\$_3+0$. Define $\mathcal{F}_3$(natural number, natural number, natural number) $= a\cdot c\cdot\$_1\cdot\$_3$. For every n, i_1, i_2, i_3, i_4, and i_5, $\{p : \mathcal{P}_3[p(i_1), p(i_2), \mathcal{F}_3(p(i_3), p(i_4), p(i_5))]\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$.

Define $\mathcal{Q}_1$[finite 0-sequence of $\mathbb{N}$] $\equiv \mathcal{P}_2[\$_1(i_2), \$_1(i_2), \mathcal{F}_2(\$_1(i_1), \$_1(i_1), \$_1(i_3))]$. Define $\mathcal{Q}_2$[finite 0-sequence of $\mathbb{N}$] $\equiv \mathcal{P}_3[\$_1(i_2), \$_1(i_2), \mathcal{F}_3(\$_1(i_1), \$_1(i_1), \$_1(i_3))]$. Define $\mathcal{Q}_{12}$[finite 0-sequence of $\mathbb{N}$] $\equiv \mathcal{Q}_1[\$_1]$ and $\mathcal{Q}_2[\$_1]$. Define $\mathcal{Q}_3$[finite 0-sequence of $\mathbb{N}$] $\equiv c\cdot\$_1(i_3)\neq 0\cdot\$_1(i_3)+0$. Define $\mathcal{Q}_{123}$[finite 0-sequence of $\mathbb{N}$] $\equiv \mathcal{Q}_{12}[\$_1]$ and $\mathcal{Q}_3[\$_1]$. Define $\mathcal{T}$[finite 0-sequence of $\mathbb{N}$] $\equiv a\cdot\$_1(i_1) = \lfloor\frac{b\cdot\$_1(i_2)}{c\cdot\$_1(i_3)}\rfloor$ and $c\cdot\$_1(i_3)\neq 0$. $\{p : \mathcal{Q}_1[p]$ and $\mathcal{Q}_2[p]\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$. $\{p : \mathcal{Q}_{12}[p]$ and $\mathcal{Q}_3[p]\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$. For every p, $\mathcal{T}[p]$ iff $\mathcal{Q}_{123}[p]$. $\{p : \mathcal{T}[p]\} = \{q : \mathcal{Q}_{123}[q]\}$. □

Let us consider i_1, i_2, and i_3. Now we state the propositions:

(29) If $n\neq 0$, then $\{p : p(i_1)\geqslant p(i_3)$ and $p(i_2) = \binom{p(i_1)}{p(i_3)}\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$.

Proof: Set $n_6 = n+6$. Define $\mathcal{R}$[finite 0-sequence of $\mathbb{N}$] $\equiv \$_1(i_1)\geqslant\$_1(i_3)$ and $\$_1(i_2) = \binom{\$_1(i_1)}{\$_1(i_3)}$. Set $RR = \{p : \mathcal{R}[p]\}$. Reconsider $X = i_1$, $Y = i_2$, $Z = i_3$, $U = n$, $V = n+1$, $Y_1 = n+2$, $Y_2 = n+3$, $Y_3 = n+4$, $U_1 = n+5$ as an element of $n+6$. Define $\mathcal{P}_1$[finite 0-sequence of $\mathbb{N}$] $\equiv \$_1(Y_1) = \$_1(X)^{\$_1(Z)}$. Define $\mathcal{P}_2$[finite 0-sequence of $\mathbb{N}$] $\equiv \$_1(Y_2) = \$_1(U_1)^{\$_1(X)}$. Define $\mathcal{P}_3$[finite 0-sequence of $\mathbb{N}$] $\equiv \$_1(Y_3) = \$_1(U)^{\$_1(Z)}$. Define $\mathcal{P}_4$[finite 0-sequence of $\mathbb{N}$] $\equiv 1\cdot\$_1(U) > 1\cdot\$_1(Y_1)+0$. Define $\mathcal{P}_5$[finite 0-sequence of $\mathbb{N}$] $\equiv 1\cdot\$_1(V) = \lfloor\frac{1\cdot\$_1(Y_2)}{1\cdot\$_1(Y_3)}\rfloor$ and $1\cdot\$_1(Y_3)\neq 0$. $\{p$, where p is an n_6-element finite 0-sequence of $\mathbb{N} : \mathcal{P}_5[p]\}$ is a Diophantine subset of the n_6-xtuples of $\mathbb{N}$.

Define $\mathcal{P}_6$[finite 0-sequence of $\mathbb{N}$] $\equiv 1\cdot\$_1(Y)\equiv 1\cdot\$_1(V) \pmod{1\cdot\$_1(U)}$. Define $\mathcal{P}_7$[finite 0-sequence of $\mathbb{N}$] $\equiv 1\cdot\$_1(U) > 1\cdot\$_1(Y)+0$. Define $\mathcal{P}_8$[finite 0-sequence of $\mathbb{N}$] $\equiv 1\cdot\$_1(X)\geqslant 1\cdot\$_1(Z)+0$. Define $\mathcal{P}_9$[finite 0-sequence of $\mathbb{N}$] $\equiv 1\cdot\$_1(U_1) = 1\cdot\$_1(U)+1$. Define $\mathcal{P}_{12}$[finite 0-sequence of $\mathbb{N}$] $\equiv$

$\mathcal{P}_1[\$_1]$ and $\mathcal{P}_2[\$_1]$. $\{p$, where p is an n_6-element finite 0-sequence of $\mathbb{N}$: $\mathcal{P}_{12}[p]\}$ is a Diophantine subset of the n_6-xtuples of $\mathbb{N}$. Define $\mathcal{P}_{123}$[finite 0-sequence of $\mathbb{N}$] $\equiv \mathcal{P}_{12}[\$_1]$ and $\mathcal{P}_3[\$_1]$. $\{p$, where p is an n_6-element finite 0-sequence of $\mathbb{N}$: $\mathcal{P}_{123}[p]\}$ is a Diophantine subset of the n_6-xtuples of $\mathbb{N}$. Define $\mathcal{P}_{1234}$[finite 0-sequence of $\mathbb{N}$] $\equiv \mathcal{P}_{123}[\$_1]$ and $\mathcal{P}_4[\$_1]$. $\{p$, where p is an n_6-element finite 0-sequence of $\mathbb{N}$: $\mathcal{P}_{1234}[p]\}$ is a Diophantine subset of the n_6-xtuples of $\mathbb{N}$. Define $\mathcal{P}_{12345}$[finite 0-sequence of $\mathbb{N}$] $\equiv \mathcal{P}_{1234}[\$_1]$ and $\mathcal{P}_5[\$_1]$. $\{p$, where p is an n_6-element finite 0-sequence of $\mathbb{N}$: $\mathcal{P}_{12345}[p]\}$ is a Diophantine subset of the n_6-xtuples of $\mathbb{N}$.

Define $\mathcal{P}_{123456}$[finite 0-sequence of $\mathbb{N}$] $\equiv \mathcal{P}_{12345}[\$_1]$ and $\mathcal{P}_6[\$_1]$. $\{p$, where p is an n_6-element finite 0-sequence of $\mathbb{N}$: $\mathcal{P}_{123456}[p]\}$ is a Diophantine subset of the n_6-xtuples of $\mathbb{N}$. Define $\mathcal{P}_{1234567}$[finite 0-sequence of $\mathbb{N}$] $\equiv \mathcal{P}_{123456}[\$_1]$ and $\mathcal{P}_7[\$_1]$. $\{p$, where p is an n_6-element finite 0-sequence of $\mathbb{N}$: $\mathcal{P}_{1234567}[p]\}$ is a Diophantine subset of the n_6-xtuples of $\mathbb{N}$. Define $\mathcal{P}_{12345678}$[finite 0-sequence of $\mathbb{N}$] $\equiv \mathcal{P}_{1234567}[\$_1]$ and $\mathcal{P}_8[\$_1]$. $\{p$, where p is an n_6-element finite 0-sequence of $\mathbb{N}$: $\mathcal{P}_{12345678}[p]\}$ is a Diophantine subset of the n_6-xtuples of $\mathbb{N}$. Define $\mathcal{P}_{123456789}$[finite 0-sequence of $\mathbb{N}$] $\equiv \mathcal{P}_{12345678}[\$_1]$ and $\mathcal{P}_9[\$_1]$. Set $PP = \{p$, where p is an n_6-element finite 0-sequence of $\mathbb{N}$: $\mathcal{P}_{123456789}[p]\}$. PP is a Diophantine subset of the n_6-xtuples of $\mathbb{N}$. Reconsider $PP_n = \{p{\restriction}n$, where p is an n_6-element finite 0-sequence of $\mathbb{N}$: $p \in PP\}$ as a Diophantine subset of the n-xtuples of $\mathbb{N}$. $PP_n \subseteq RR$. $RR \subseteq PP_n$. □

(30) $\{p : p(i_1) \geqslant p(i_3)$ and $p(i_2) = \binom{p(i_1)}{p(i_3)}\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$. The theorem is a consequence of (29).

Let us consider i_1 and i_2. Now we state the propositions:

(31) If $n \neq 0$, then $\{p : p(i_1) = p(i_2)!\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$.

Proof: Set $n_6 = n+6$. Define $\mathcal{R}$[finite 0-sequence of $\mathbb{N}$] $\equiv \$_1(i_1) = \$_1(i_2)!$. Set $RR = \{p : \mathcal{R}[p]\}$. Reconsider $Y = i_1$, $X = i_2$, $N = n$, $Y_1 = n+1$, $Y_2 = n+2$, $Y_3 = n+3$, $X_1 = n+4$, $X_2 = n+5$ as an element of $n+6$. Define $\mathcal{P}_1$[finite 0-sequence of $\mathbb{N}$] $\equiv \$_1(Y_1) = \$_1(X_2)^{\$_1(X_1)}$. Define $\mathcal{P}_2$[finite 0-sequence of $\mathbb{N}$] $\equiv \$_1(Y_2) = \$_1(N)^{\$_1(X)}$. Define $\mathcal{P}_3$[finite 0-sequence of $\mathbb{N}$] $\equiv \$_1(N) \geqslant \$_1(X)$ and $\$_1(Y_3) = \binom{\$_1(N)}{\$_1(X)}$. $\{p$, where p is an n_6-element finite 0-sequence of $\mathbb{N}$: $\mathcal{P}_3[p]\}$ is a Diophantine subset of the n_6-xtuples of $\mathbb{N}$. Define $\mathcal{P}_4$[finite 0-sequence of $\mathbb{N}$] $\equiv 1 \cdot \$_1(Y) = \lfloor \frac{1 \cdot \$_1(Y_2)}{1 \cdot \$_1(Y_3)} \rfloor$ and $1 \cdot \$_1(Y_3) \neq 0$. $\{p$, where p is an n_6-element finite 0-sequence of $\mathbb{N}$: $\mathcal{P}_4[p]\}$ is a Diophantine subset of the n_6-xtuples of $\mathbb{N}$. Define $\mathcal{P}_5$[finite 0-sequence of $\mathbb{N}$] $\equiv 1 \cdot \$_1(X_2) = 2 \cdot \$_1(X) + 0$. Define $\mathcal{P}_6$[finite 0-sequence of $\mathbb{N}$] $\equiv 1 \cdot \$_1(X_1) = 1 \cdot \$_1(X) + 1$. Define $\mathcal{P}_7$[finite 0-sequence of $\mathbb{N}$] $\equiv 1 \cdot \$_1(N) >$

$1 \cdot \$_1(Y_1) + 0$. Define $\mathcal{P}_{12}$[finite 0-sequence of $\mathbb{N}$] $\equiv \mathcal{P}_1[\$_1]$ and $\mathcal{P}_2[\$_1]$. $\{p$, where p is an n_6-element finite 0-sequence of $\mathbb{N} : \mathcal{P}_{12}[p]\}$ is a Diophantine subset of the n_6-xtuples of $\mathbb{N}$.

Define $\mathcal{P}_{123}$[finite 0-sequence of $\mathbb{N}$] $\equiv \mathcal{P}_{12}[\$_1]$ and $\mathcal{P}_3[\$_1]$. $\{p$, where p is an n_6-element finite 0-sequence of $\mathbb{N} : \mathcal{P}_{123}[p]\}$ is a Diophantine subset of the n_6-xtuples of $\mathbb{N}$. Define $\mathcal{P}_{1234}$[finite 0-sequence of $\mathbb{N}$] $\equiv \mathcal{P}_{123}[\$_1]$ and $\mathcal{P}_4[\$_1]$. $\{p$, where p is an n_6-element finite 0-sequence of $\mathbb{N} : \mathcal{P}_{1234}[p]\}$ is a Diophantine subset of the n_6-xtuples of $\mathbb{N}$. Define $\mathcal{P}_{12345}$[finite 0-sequence of $\mathbb{N}$] $\equiv \mathcal{P}_{1234}[\$_1]$ and $\mathcal{P}_5[\$_1]$. $\{p$, where p is an n_6-element finite 0-sequence of $\mathbb{N} : \mathcal{P}_{12345}[p]\}$ is a Diophantine subset of the n_6-xtuples of $\mathbb{N}$. Define $\mathcal{P}_{123456}$[finite 0-sequence of $\mathbb{N}$] $\equiv \mathcal{P}_{12345}[\$_1]$ and $\mathcal{P}_6[\$_1]$. $\{p$, where p is an n_6-element finite 0-sequence of $\mathbb{N} : \mathcal{P}_{123456}[p]\}$ is a Diophantine subset of the n_6-xtuples of $\mathbb{N}$. Define $\mathcal{P}_{1234567}$[finite 0-sequence of $\mathbb{N}$] $\equiv \mathcal{P}_{123456}[\$_1]$ and $\mathcal{P}_7[\$_1]$. Set $PP = \{p$, where p is an n_6-element finite 0-sequence of $\mathbb{N} : \mathcal{P}_{1234567}[p]\}$. PP is a Diophantine subset of the n_6-xtuples of $\mathbb{N}$. Reconsider $PP_n = \{p{\restriction}n$, where p is an n_6-element finite 0-sequence of $\mathbb{N} : p \in PP\}$ as a Diophantine subset of the n-xtuples of $\mathbb{N}$. $PP_n \subseteq RR$. $RR \subseteq PP_n$. □

(32) $\{p : p(i_1) = p(i_2)!\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$. The theorem is a consequence of (31).

(33) $\{p : 1 + (p(i_1) + 1) \cdot (p(i_2)!) = p(i_3)\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$.

PROOF: Define $\mathcal{R}$(natural number, natural number, natural number) $= 1 \cdot \$_1 + -1$. Define $\mathcal{P}_1$[natural number, natural number, integer] $\equiv 1 \cdot \$_1 \cdot \$_2 = \$_3$. For every i_1, i_2, i_3, i_4, and i_5, $\{p : \mathcal{P}_1[p(i_1), p(i_2), \mathcal{R}(p(i_3), p(i_4), p(i_5))]\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$. Define $\mathcal{F}_2$(natural number, natural number, natural number) $= \$_1!$. For every i_1, i_2, i_3, and i_4, $\{p : \mathcal{F}_2(p(i_1), p(i_2), p(i_3)) = p(i_4)\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$. Define $\mathcal{P}_2$[natural number, natural number, natural object, natural number, natural number, natural number] $\equiv 1 \cdot \$_1 \cdot \$_3 = 1 \cdot \$_2 - 1$.

For every i_1, i_2, i_3, i_4, and i_5, $\{p : \mathcal{P}_2[p(i_1), p(i_2), \mathcal{F}_2(p(i_3), p(i_4), p(i_5)), p(i_3), p(i_4), p(i_5)]\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$. Define $\mathcal{P}_3$[natural number, natural number, natural object, natural number, natural number, natural number] $\equiv 1 \cdot \$_3 \cdot (\$_1!) = 1 \cdot \$_2 - 1$. Define $\mathcal{F}_3$(natural number, natural number, natural number) $= 1 \cdot \$_1 + 1$. For every n, i_1, i_2, i_3, i_4, and i_5, $\{p : \mathcal{P}_3[p(i_1), p(i_2), \mathcal{F}_3(p(i_3), p(i_4), p(i_5)), p(i_3), p(i_4), p(i_5)]\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$. Define $\mathcal{Q}_1$[finite 0-sequence of $\mathbb{N}$] $\equiv \mathcal{P}_3[\$_1(i_2), \$_1(i_3), 1 \cdot \$_1(i_1) + 1, \$_1(i_3), \$_1(i_3), \$_1(i_3)]$. Define $\mathcal{Q}_2$[finite 0-sequence of $\mathbb{N}$] $\equiv 1 + (\$_1(i_1) + 1) \cdot (\$_1(i_2)!) = \$_1(i_3)$. $\{p : \mathcal{Q}_1[p]\} = \{q : \mathcal{Q}_2[q]\}$. □

Let us consider i_1, i_2, and i_3. Now we state the propositions:

(34) If $n \neq 0$, then $\{p : p(i_3) = \prod(1 + p(i_1) \cdot (\mathrm{idseq}(p(i_2)))) \text{ and } p(i_1) \geqslant 1\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$.

Proof: Set $n_{12} = n+13$. Define $\mathcal{R}$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $\$_1(i_3) = \prod(1+ \$_1(i_1) \cdot (\mathrm{idseq}(\$_1(i_2))))$ and $\$_1(i_1) \geqslant 1$. Set $RR = \{p : \mathcal{R}[p]\}$. Reconsider $X_1 = i_1$, $X = i_2$, $Y = i_3$, $U = n$, $W = n+1$, $Y_1 = n+2$, $Y_2 = n+3$, $Y_3 = n+4$, $Y_4 = n+5$, $Y_5 = n+6$, $X_3 = n+7$, $W_1 = n+8$, $Y_6 = n+9$, $Y_7 = n+10$, $X_4 = n+11$, $O = n+12$ as an element of n_{12}. Define $\mathcal{Q}$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $1 \cdot \$_1(X_1) \geqslant 0 \cdot \$_1(Y) + 1$. Define $\mathcal{P}_1$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $1 \cdot \$_1(U) > 1 \cdot \$_1(Y) + 0$. Define $\mathcal{P}_2$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $1 \cdot \$_1(X_3) = 1 \cdot \$_1(X_1) \cdot \$_1(W)$.

Define $\mathcal{P}_3$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $\$_1(O) = 1$. Define $\mathcal{P}_4$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $1 \cdot \$_1(X_3) \equiv 1 \cdot \$_1(O) \pmod{1 \cdot \$_1(U)}$. Define $\mathcal{P}_5$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $\$_1(Y_1) = \$_1(X_1)^{\$_1(X)}$. Define $\mathcal{P}_6$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $\$_1(Y_2) = \$_1(X)!$. $\{p$, where p is an n_{12}-element finite 0-sequence of $\mathbb{N}$: $\mathcal{P}_6[p]\}$ is a Diophantine subset of the n_{12}-xtuples of $\mathbb{N}$. Define $\mathcal{P}_7$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $1 \cdot \$_1(W_1) = 1 \cdot \$_1(W) + 1 \cdot \$_1(X) + 0$. Define $\mathcal{P}_8$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $\$_1(W_1) \geqslant \$_1(X)$ and $\$_1(Y_3) = \binom{\$_1(W_1)}{\$_1(X)}$. $\{p$, where p is an n_{12}-element finite 0-sequence of $\mathbb{N}$: $\mathcal{P}_8[p]\}$ is a Diophantine subset of the n_{12}-xtuples of $\mathbb{N}$. Define $\mathcal{P}_9$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $1 \cdot \$_1(Y_6) = 1 \cdot \$_1(Y_1) \cdot \$_1(Y_2)$. Define $\mathcal{PA}$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $1 \cdot \$_1(Y_7) = 1 \cdot \$_1(Y_6) \cdot \$_1(Y_3)$. Define $\mathcal{PB}$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $1 \cdot \$_1(Y_7) \equiv 1 \cdot \$_1(Y) \pmod{1 \cdot \$_1(U)}$. Define $\mathcal{PC}$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $1 \cdot \$_1(X_4) = 1 \cdot \$_1(X_1) \cdot \$_1(X)$. Define $\mathcal{PD}$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $1 \cdot \$_1(Y_4) = 1 \cdot \$_1(X_4) + 1$. Define $\mathcal{PE}$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $\$_1(Y_5) = \$_1(Y_4)^{\$_1(X)}$. Define $\mathcal{PF}$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $1 \cdot \$_1(U) > 1 \cdot \$_1(Y_5) + 0$.

Define $\mathcal{C}_1$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $\mathcal{Q}[\$_1]$ and $\mathcal{P}_1[\$_1]$. $\{p$, where p is an n_{12}-element finite 0-sequence of $\mathbb{N}$: $\mathcal{C}_1[p]\}$ is a Diophantine subset of the n_{12}-xtuples of $\mathbb{N}$. Define $\mathcal{C}_2$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $\mathcal{C}_1[\$_1]$ and $\mathcal{P}_2[\$_1]$. $\{p$, where p is an n_{12}-element finite 0-sequence of $\mathbb{N}$: $\mathcal{C}_2[p]\}$ is a Diophantine subset of the n_{12}-xtuples of $\mathbb{N}$. Define $\mathcal{C}_3$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $\mathcal{C}_2[\$_1]$ and $\mathcal{P}_3[\$_1]$. $\{p$, where p is an n_{12}-element finite 0-sequence of $\mathbb{N}$: $\mathcal{C}_3[p]\}$ is a Diophantine subset of the n_{12}-xtuples of $\mathbb{N}$. Define $\mathcal{C}_4$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $\mathcal{C}_3[\$_1]$ and $\mathcal{P}_4[\$_1]$. $\{p$, where p is an n_{12}-element finite 0-sequence of $\mathbb{N}$: $\mathcal{C}_4[p]\}$ is a Diophantine subset of the n_{12}-xtuples of $\mathbb{N}$. Define $\mathcal{C}_5$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $\mathcal{C}_4[\$_1]$ and $\mathcal{P}_5[\$_1]$. $\{p$, where p is an n_{12}-element finite 0-sequence of $\mathbb{N}$: $\mathcal{C}_5[p]\}$ is a Diophantine subset of the n_{12}-xtuples of $\mathbb{N}$. Define $\mathcal{C}_6$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $\mathcal{C}_5[\$_1]$ and $\mathcal{P}_6[\$_1]$. $\{p$, where p is an n_{12}-element finite 0-sequence of $\mathbb{N}$: $\mathcal{C}_6[p]\}$ is a Diophantine subset of the n_{12}-xtuples of $\mathbb{N}$. Define $\mathcal{C}_7$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $\mathcal{C}_6[\$_1]$ and $\mathcal{P}_7[\$_1]$. $\{p$, where p is an n_{12}-element finite 0-sequence of $\mathbb{N}$: $\mathcal{C}_7[p]\}$ is a Diophantine subset of the n_{12}-xtuples of $\mathbb{N}$. Define $\mathcal{C}_8$[finite 0-sequence of $\mathbb{N}$] $\equiv \mathcal{C}_7[\$_1]$ and $\mathcal{P}_8[\$_1]$. $\{p$, where p is an n_{12}-element finite 0-sequence of $\mathbb{N}$: $\mathcal{C}_8[p]\}$ is a Diophantine subset of the n_{12}-xtuples of $\mathbb{N}$. Define $\mathcal{C}_9$[finite 0-sequence of $\mathbb{N}$] $\equiv \mathcal{C}_8[\$_1]$ and $\mathcal{P}_9[\$_1]$. $\{p$, where p is an n_{12}-element finite 0-sequence of $\mathbb{N}$: $\mathcal{C}_9[p]\}$ is a Diophantine subset of the n_{12}-xtuples of $\mathbb{N}$.

Define $\mathcal{CA}$[finite 0-sequence of $\mathbb{N}$] $\equiv \mathcal{C}_9[\$_1]$ and $\mathcal{PA}[\$_1]$. $\{p$, where p is an n_{12}-element finite 0-sequence of $\mathbb{N}$: $\mathcal{CA}[p]\}$ is a Diophantine subset of the n_{12}-xtuples of $\mathbb{N}$. Define $\mathcal{CB}$[finite 0-sequence of $\mathbb{N}$] $\equiv \mathcal{CA}[\$_1]$ and $\mathcal{PB}[\$_1]$. $\{p$, where p is an n_{12}-element finite 0-sequence of $\mathbb{N}$: $\mathcal{CB}[p]\}$ is a Diophantine subset of the n_{12}-xtuples of $\mathbb{N}$. Define $\mathcal{CC}$[finite 0-sequence of $\mathbb{N}$] $\equiv \mathcal{CB}[\$_1]$ and $\mathcal{PC}[\$_1]$. $\{p$, where p is an n_{12}-element finite 0-sequence of $\mathbb{N}$: $\mathcal{CC}[p]\}$ is a Diophantine subset of the n_{12}-xtuples of $\mathbb{N}$. Define $\mathcal{CD}$[finite 0-sequence of $\mathbb{N}$] $\equiv \mathcal{CC}[\$_1]$ and $\mathcal{PD}[\$_1]$. $\{p$, where p is an n_{12}-element finite 0-sequence of $\mathbb{N}$: $\mathcal{CD}[p]\}$ is a Diophantine subset of the n_{12}-xtuples of $\mathbb{N}$. Define $\mathcal{CE}$[finite 0-sequence of $\mathbb{N}$] $\equiv \mathcal{CD}[\$_1]$ and $\mathcal{PE}[\$_1]$. $\{p$, where p is an n_{12}-element finite 0-sequence of $\mathbb{N}$: $\mathcal{CE}[p]\}$ is a Diophantine subset of the n_{12}-xtuples of $\mathbb{N}$. Define $\mathcal{CF}$[finite 0-sequence of $\mathbb{N}$] $\equiv \mathcal{CE}[\$_1]$ and $\mathcal{PF}[\$_1]$. Set $PP = \{p$, where p is an n_{12}-element finite 0-sequence of $\mathbb{N}$: $\mathcal{CF}[p]\}$. PP is a Diophantine subset of the n_{12}-xtuples of $\mathbb{N}$. Reconsider $PP_n = \{p{\restriction}n$, where p is an n_{12}-element finite 0-sequence of $\mathbb{N}$: $p \in PP\}$ as a Diophantine subset of the n-xtuples of $\mathbb{N}$. $PP_n \subseteq RR$. $RR \subseteq PP_n$. □

(35) $\{p : p(i_3) = \prod(1 + p(i_1) \cdot (\mathrm{idseq}(p(i_2))))$ and $p(i_1) \geqslant 1\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$. The theorem is a consequence of (34).

(36) $\{p : p(i_3) = \prod(1 + p(i_1)! \cdot (\mathrm{idseq}(1 + p(i_2))))\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$.

Proof: Define $\mathcal{R}$(natural number, natural number, natural number) $= \$_1!$. For every i_1, i_2, i_3, and i_4, $\{p : \mathcal{R}(p(i_1), p(i_2), p(i_3)) = p(i_4)\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$. Define $\mathcal{P}_1$[natural number, natural number, natural object, natural number, natural number, natural number] $\equiv \$_1 = \prod(1 + \$_3 \cdot (\mathrm{idseq}(\$_2)))$ and $\$_3 \geqslant 1$. For every i_1, i_2, i_3, i_4, i_5, and i_6, $\{p : \mathcal{P}_1[p(i_1), p(i_2), p(i_3), p(i_4), p(i_5), p(i_6)]\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$.

For every i_1, i_2, i_3, i_4, and i_5, $\{p : \mathcal{P}_1[p(i_1), p(i_2), \mathcal{R}(p(i_3), p(i_4), p(i_5)), p(i_3), p(i_4), p(i_5)]\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$. Define $\mathcal{F}_2$(natural number, natural number, natural number) $= 1 \cdot \$_1 + 1$. Define $\mathcal{P}_2$[natural number, natural number, natural object, natural number, natural number, natural number] $\equiv \$_1 = \prod(1 + \$_2! \cdot (\mathrm{idseq}(\$_3)))$ and $\$_2! \geqslant 1$. For every i_1, i_2, i_3, i_4, and i_5, $\{p : \mathcal{P}_2[p(i_1), p(i_2), \mathcal{F}_2(p(i_3), p(i_4), p(i_5)), p(i_3), p(i_4), p(i_5)]\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$. Define $\mathcal{Q}_1$[finite

0-sequence of $\mathbb{N}] \equiv \mathcal{P}_2[\$_1(i_3), \$_1(i_1), 1 \cdot \$_1(i_2) + 1, 1 \cdot \$_1(i_3), \$_1(i_3), \$_1(i_3)]$. Define $\mathcal{Q}_2$[finite 0-sequence of $\mathbb{N}] \equiv \$_1(i_3) = \prod(1 + \$_1(i_1)! \cdot (\mathrm{idseq}(1 + \$_1(i_2))))$. $\{p : \mathcal{Q}_1[p]\} = \{q : \mathcal{Q}_2[q]\}$. □

Let us consider i_1, i_2, and i_3. Now we state the propositions:

(37) If $n \neq 0$, then $\{p : p(i_3) = \prod(p(i_2) + 1 + -\mathrm{idseq}(p(i_1)))$ and $p(i_2) > p(i_1)\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$.

PROOF: Set $n_2 = n + 2$. Define $\mathcal{R}$[finite 0-sequence of $\mathbb{N}] \equiv \$_1(i_3) = \prod(\$_1(i_2) + 1 + -\mathrm{idseq}(\$_1(i_1)))$ and $\$_1(i_2) > \$_1(i_1)$. Set $RR = \{p : \mathcal{R}[p]\}$. Reconsider $Y = i_3$, $X_2 = i_2$, $X_1 = i_1$, $C = n$, $F = n + 1$ as an element of n_2. Define $\mathcal{P}_1$[finite 0-sequence of $\mathbb{N}] \equiv \$_1(X_2) \geqslant \$_1(X_1)$ and $\$_1(C) = \binom{\$_1(X_2)}{\$_1(X_1)}$. $\{p$, where p is an n_2-element finite 0-sequence of $\mathbb{N} : \mathcal{P}_1[p]\}$ is a Diophantine subset of the n_2-xtuples of $\mathbb{N}$. Define $\mathcal{P}_2$[finite 0-sequence of $\mathbb{N}] \equiv \$_1(F) = \$_1(X_1)!$. $\{p$, where p is an n_2-element finite 0-sequence of $\mathbb{N} : \mathcal{P}_2[p]\}$ is a Diophantine subset of the n_2-xtuples of $\mathbb{N}$. Define $\mathcal{P}_3$[finite 0-sequence of $\mathbb{N}] \equiv 1 \cdot \$_1(X_2) > 1 \cdot \$_1(X_1) + 0$. Define $\mathcal{P}_4$[finite 0-sequence of $\mathbb{N}] \equiv 1 \cdot \$_1(Y) = 1 \cdot \$_1(F) \cdot \$_1(C)$.

Define $\mathcal{P}_{12}$[finite 0-sequence of $\mathbb{N}] \equiv \mathcal{P}_1[\$_1]$ and $\mathcal{P}_2[\$_1]$. $\{p$, where p is an n_2-element finite 0-sequence of $\mathbb{N} : \mathcal{P}_{12}[p]\}$ is a Diophantine subset of the n_2-xtuples of $\mathbb{N}$. Define $\mathcal{P}_{123}$[finite 0-sequence of $\mathbb{N}] \equiv \mathcal{P}_{12}[\$_1]$ and $\mathcal{P}_3[\$_1]$. $\{p$, where p is an n_2-element finite 0-sequence of $\mathbb{N} : \mathcal{P}_{123}[p]\}$ is a Diophantine subset of the n_2-xtuples of $\mathbb{N}$. Define $\mathcal{P}_{1234}$[finite 0-sequence of $\mathbb{N}] \equiv \mathcal{P}_{123}[\$_1]$ and $\mathcal{P}_4[\$_1]$. Set $PP = \{p$, where p is an n_2-element finite 0-sequence of $\mathbb{N} : \mathcal{P}_{1234}[p]\}$. PP is a Diophantine subset of the n_2-xtuples of $\mathbb{N}$. Reconsider $PP_n = \{p \upharpoonright n$, where p is an n_2-element finite 0-sequence of $\mathbb{N} : p \in PP\}$ as a Diophantine subset of the n-xtuples of $\mathbb{N}$. $PP_n \subseteq RR$. $RR \subseteq PP_n$. □

(38) $\{p : p(i_3) = \prod(p(i_2) + 1 + -\mathrm{idseq}(p(i_1)))$ and $p(i_2) > p(i_1)\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$. The theorem is a consequence of (37).

(39) $\{p : p(i_1) = \prod(i + p_{\lfloor n_1} \upharpoonright n_2)\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every n such that $\$_1 + n_1 \leqslant n$ for every i_1, $\{p : p(i_1) = \prod(i + p_{\lfloor n_1} \upharpoonright \$_1)\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$. $\mathcal{P}[0]$. If $\mathcal{P}[m]$, then $\mathcal{P}[m + 1]$. $\mathcal{P}[m]$. □

References

[1] Marcin Acewicz and Karol Pąk. Basic Diophantine relations. *Formalized Mathematics*, 26(**2**):175–181, 2018. doi:10.2478/forma-2018-0015.

[2] Zofia Adamowicz and Paweł Zbierski. *Logic of Mathematics: A Modern Course of Classical*

Logic. Pure and Applied Mathematics: A Wiley Series of Texts, Monographs and Tracts. Wiley-Interscience, 1997.

[3] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, Karol Pąk, and Josef Urban. Mizar: State-of-the-art and beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8_17.

[4] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pąk. The role of the Mizar Mathematical Library for interactive proof development in Mizar. *Journal of Automated Reasoning*, 61(1):9–32, 2018. doi:10.1007/s10817-017-9440-6.

[5] Martin Davis. Hilbert's tenth problem is unsolvable. *The American Mathematical Monthly, Mathematical Association of America*, 80(3):233–269, 1973. doi:10.2307/2318447.

[6] Adam Grabowski, Artur Korniłowicz, and Adam Naumowicz. Four decades of Mizar. *Journal of Automated Reasoning*, 55(3):191–198, 2015. doi:10.1007/s10817-015-9345-1.

[7] Artur Korniłowicz and Karol Pąk. Basel problem – preliminaries. *Formalized Mathematics*, 25(**2**):141–147, 2017. doi:10.1515/forma-2017-0013.

[8] Xiquan Liang, Li Yan, and Junjie Zhao. Linear congruence relation and complete residue systems. *Formalized Mathematics*, 15(**4**):181–187, 2007. doi:10.2478/v10037-007-0022-7.

[9] Karol Pąk. Diophantine sets. Preliminaries. *Formalized Mathematics*, 26(**1**):81–90, 2018. doi:10.2478/forma-2018-0007.

[10] Craig Alan Smorynski. *Logical Number Theory I, An Introduction*. Universitext. Springer-Verlag Berlin Heidelberg, 1991. ISBN 978-3-642-75462-3.

[11] Tetsuya Tsunetou, Grzegorz Bancerek, and Yatsuka Nakamura. Zero-based finite sequences. *Formalized Mathematics*, 9(**4**):825–829, 2001.

[12] Rafał Ziobro. On subnomials. *Formalized Mathematics*, 24(**4**):261–273, 2016. doi:10.1515/forma-2016-0022.

Accepted May 27, 2019

FORMALIZED MATHEMATICS
Vol. 27, No. 2, Pages 209–221, 2019
DOI: 10.2478/forma-2019-0020

sciendo
https://www.sciendo.com/

Formalization of the MRDP Theorem in the Mizar System[1]

Karol Pąk
Institute of Informatics
University of Białystok
Poland

Summary. This article is the final step of our attempts to formalize the negative solution of Hilbert's tenth problem.

In our approach, we work with the Pell's Equation defined in [2]. We analyzed this equation in the general case to show its solvability as well as the cardinality and shape of all possible solutions. Then we focus on a special case of the equation, which has the form $x^2 - (a^2 - 1)y^2 = 1$ [8] and its solutions considered as two sequences $\{x_i(a)\}_{i=0}^{\infty}$, $\{y_i(a)\}_{i=0}^{\infty}$. We showed in [1] that the n-th element of these sequences can be obtained from lists of several basic Diophantine relations as linear equations, finite products, congruences and inequalities, or more precisely that the equation $x = y_i(a)$ is Diophantine. Following the post-Matiyasevich results we show that the equality determined by the value of the power function $y = x^z$ is Diophantine, and analogously property in cases of the binomial coefficient, factorial and several product [9].

In this article, we combine analyzed so far Diophantine relation using conjunctions, alternatives as well as substitution to prove the bounded quantifier theorem. Based on this theorem we prove MDPR-theorem that *every recursively enumerable set is Diophantine,* where recursively enumerable sets have been defined by the Martin Davis normal form.

The formalization by means of Mizar system [5], [7], [4] follows [10], Z. Adamowicz, P. Zbierski [3] as well as M. Davis [6].

MSC: 11D45 68T99 03B35

Keywords: Hilbert's 10th problem; Diophantine relations

MML identifier: HILB10_5, version: 8.1.09 5.57.1355

[1] This work has been financed by the resources of the Polish National Science Centre granted by decision no. DEC-2015/19/D/ST6/01473.

1. Preliminaries

From now on i, j, n, n_1, n_2, m, k, l, u denote natural numbers, i_1, i_2, i_3, i_4, i_5, i_6 denote elements of n, p, q denote n-element finite 0-sequences of $\mathbb{N}$, and a, b, c, d, e, f denote integers.

Let n be a natural number. Let us note that idseq(n) is $\mathbb{Z}$-valued.

Let x be an n-element, natural-valued finite 0-sequence and p be a $\mathbb{Z}$-valued polynomial of n,$\mathbb{R}_{\rm F}$. One can check that eval(p, ${}^{@}x$) is integer.

Now we state the proposition:

(1) Let us consider a $\mathbb{Z}$-valued polynomial p of n,$\mathbb{R}_{\rm F}$, and n-element finite 0-sequences x, y of $\mathbb{N}$. Suppose $k \neq 0$ and for every i such that $i \in n$ holds $k \mid x(i) - y(i)$. Then $k \mid$ (eval(p, ${}^{@}x$) **qua** integer)$-$(eval(p, ${}^{@}y$) **qua** integer).
Proof: Reconsider $f_1 = \mathbb{R}_{\rm F}$ as a field. Reconsider $p_1 = p$ as a polynomial of n,f_1. Reconsider $x_2 = {}^{@}x$, $y_2 = {}^{@}y$ as a function from n into the carrier of f_1. Set $s_3 = \mathrm{SgmX}(\mathrm{BagOrder}\, n, \mathrm{Support}\, p_1)$. Consider X being a finite sequence of elements of the carrier of f_1 such that $\mathrm{len}\, X = \mathrm{len}\, s_3$ and $\mathrm{eval}(p_1, x_2) = \sum X$ and for every element i of $\mathbb{N}$ such that $1 \leqslant i \leqslant \mathrm{len}\, X$ holds $X_{/i} = p_1 \cdot s_{3/i} \cdot (\mathrm{eval}(s_{3/i}, x_2))$.

Consider Y being a finite sequence of elements of the carrier of f_1 such that $\mathrm{len}\, Y = \mathrm{len}\, s_3$ and $\mathrm{eval}(p_1, y_2) = \sum Y$ and for every element i of $\mathbb{N}$ such that $1 \leqslant i \leqslant \mathrm{len}\, Y$ holds $Y_{/i} = p_1 \cdot s_{3/i} \cdot (\mathrm{eval}(s_{3/i}, y_2))$. Reconsider $Y_2 = Y$, $X_4 = X$ as a finite sequence of elements of $\mathbb{R}$. Define $\mathcal{P}$[natural number] $\equiv$ if $\$_1 \leqslant \mathrm{len}\, X$, then $\sum(X_4 {\restriction} \$_1) - \sum(Y_2 {\restriction} \$_1)$ is an integer and for every integer d such that $d = \sum(X_4 {\restriction} \$_1) - \sum(Y_2 {\restriction} \$_1)$ holds $k \mid d$. For every natural number i such that $\mathcal{P}[i]$ holds $\mathcal{P}[i+1]$. $\mathcal{P}[i]$. □

Let f be a $\mathbb{Z}$-valued function. Let us note that $-f$ is $\mathbb{Z}$-valued.

The scheme *SCH1* deals with a binary predicate $\mathcal{P}$ and a finite-0-sequence-yielding finite 0-sequence f and states that

(Sch. 1) $\{f(i)(j)$, where i, j are natural numbers : $\mathcal{P}[i,j]\}$ is finite.

Now we state the propositions:

(2) If $m \geqslant n > 0$, then $1 + m! \cdot (\mathrm{idseq}(n))$ is a CR-sequence.
Proof: Set $h = 1 + m! \cdot (\mathrm{idseq}(n))$. Define $\mathcal{F}$(natural number) $= m! \cdot \$_1 + 1$. For every i such that $i \in \mathrm{dom}\, h$ holds $h(i) = \mathcal{F}(i)$. h is positive yielding. For every natural numbers i, j such that $i, j \in \mathrm{dom}\, h$ and $i < j$ holds $h(i)$ and $h(j)$ are relatively prime. h is Chinese remainder. □

(3) Let us consider a prime number p, and a finite sequence f of elements of $\mathbb{N}$. Suppose f is positive yielding and $p \mid \prod f$. Then there exists i such that

(i) $i \in \mathrm{dom}\, f$, and

(ii) $p \mid f(i)$.

Proof: Define $\mathcal{P}$[natural number] $\equiv$ for every finite sequence f of elements of $\mathbb{N}$ such that $\operatorname{len} f = \$_1$ and f is positive yielding and $p \mid \prod f$ there exists i such that $i \in \operatorname{dom} f$ and $p \mid f(i)$. $\mathcal{P}[0]$. If $\mathcal{P}[n]$, then $\mathcal{P}[n+1]$. $\mathcal{P}[n]$. □

2. Selected Operations on Polynomials

Let n be a set and p be a series of n, $\mathbb{R}_{\mathrm{F}}$. The functor $|p|$ yielding a series of n, $\mathbb{R}_{\mathrm{F}}$ is defined by

(Def. 1) for every bag b of n, $it(b) = |p(b)|$.

Now we state the proposition:

(4) Let us consider a set n, and a series p of n, $\mathbb{R}_{\mathrm{F}}$. Then $\operatorname{Support} p = \operatorname{Support} |p|$.

Let n be an ordinal number and p be a polynomial of n,$\mathbb{R}_{\mathrm{F}}$. Let us note that $|p|$ is finite-Support.

Let n be a set, S be a non empty zero structure, and p be a finite-Support series of n, S. One can check that $\operatorname{Support} p$ is finite.

Let n be an ordinal number, L be an add-associative, right zeroed, right complementable, non empty additive loop structure, and p be a polynomial of n,L. The functor $\sum \texttt{coeff}(p)$ yielding an element of L is defined by the term

(Def. 2) $\sum p \cdot (\operatorname{SgmX}(\operatorname{BagOrder} n, \operatorname{Support} p))$.

The functor $\operatorname{degree}(p)$ yielding a natural number is defined by

(Def. 3) (i) there exists a bag s of n such that $s \in \operatorname{Support} p$ and $it = \operatorname{degree}(s)$ and for every bag s_1 of n such that $s_1 \in \operatorname{Support} p$ holds $\operatorname{degree}(s_1) \leqslant it$, **if** $p \neq 0_n L$,

(ii) $it = 0$, **otherwise**.

Now we state the propositions:

(5) Let us consider an ordinal number n, and a bag b of n. Then $\operatorname{degree}(b) = \sum b \cdot (\operatorname{SgmX}(\subseteq_n, \operatorname{support} b))$.

(6) Let us consider an ordinal number n, an add-associative, right zeroed, right complementable, non empty additive loop structure L, and a polynomial p of n,L. Then $\operatorname{degree}(p) = 0$ if and only if $\operatorname{Support} p \subseteq \{\operatorname{EmptyBag} n\}$.

Proof: If $\operatorname{degree}(p) = 0$, then $\operatorname{Support} p \subseteq \{\operatorname{EmptyBag} n\}$. Consider s being a bag of n such that $s \in \operatorname{Support} p$ and $\operatorname{degree}(p) = \operatorname{degree}(s)$. □

(7) Let us consider an ordinal number n, an add-associative, right zeroed, right complementable, non empty additive loop structure L, a polynomial p of n,L, and a bag b of n. If $b \in \operatorname{Support} p$, then $\operatorname{degree}(p) \geqslant \operatorname{degree}(b)$.

(8) Let us consider an ordinal number n, and a polynomial p of n,$\mathbb{R}_{\mathrm{F}}$. If $|p| = 0_n(\mathbb{R}_{\mathrm{F}})$, then $p = 0_n(\mathbb{R}_{\mathrm{F}})$.

Let n be a set. One can verify that $|0_n(\mathbb{R}_{\mathrm{F}})|$ reduces to $0_n(\mathbb{R}_{\mathrm{F}})$. Now we state the propositions:

(9) Let us consider an ordinal number n, and a polynomial p of n,$\mathbb{R}_{\mathrm{F}}$. Then $\mathrm{degree}(p) = \mathrm{degree}(|p|)$. The theorem is a consequence of (8) and (4).

(10) Let us consider an ordinal number n, a bag b of n, and a real number r. Suppose $r \geqslant 1$. Let us consider a function x from n into the carrier of $\mathbb{R}_{\mathrm{F}}$. Suppose for every object i such that $i \in \mathrm{dom}\, x$ holds $|x(i)| \leqslant r$. Then $|\,\mathrm{eval}(b, x)| \leqslant r^{\mathrm{degree}(b)}$.

Proof: Reconsider $f_1 = \mathbb{R}_{\mathrm{F}}$ as a field. Set $s_2 = \mathrm{SgmX}(\subseteq_n, \mathrm{support}\, b)$. Set $B = b \cdot s_2$. Consider y being a finite sequence of elements of f_1 such that $\mathrm{len}\, y = \mathrm{len}\, s_2$ and $\mathrm{eval}(b, x) = \prod y$ and for every element i of $\mathbb{N}$ such that $1 \leqslant i \leqslant \mathrm{len}\, y$ holds $y_{/i} = \mathrm{power}_{\mathbb{R}_{\mathrm{F}}}(x \cdot s_{2/i}, B_{/i})$.

Define $\mathcal{P}[\text{natural number}] \equiv$ if $\$_1 \leqslant \mathrm{len}\, y$, then $\prod(y \restriction \$_1)$ is a real number and for every real number P such that $P = \prod(y \restriction \$_1)$ holds $|P| \leqslant r^{\sum(B \restriction \$_1)}$. For every i such that $\mathcal{P}[i]$ holds $\mathcal{P}[i+1]$. For every i, $\mathcal{P}[i]$. □

(11) Let us consider an ordinal number n, a polynomial p of n,$\mathbb{R}_{\mathrm{F}}$, and a real number r. Suppose $r \geqslant 1$. Let us consider a function x from n into the carrier of $\mathbb{R}_{\mathrm{F}}$. Suppose for every object i such that $i \in \mathrm{dom}\, x$ holds $|x(i)| \leqslant r$. Then $|\,\mathrm{eval}(p, x)| \leqslant (\sum \mathtt{coeff}(|p|)) \cdot (r^{\mathrm{degree}(p)})$.

Proof: Reconsider $f_1 = \mathbb{R}_{\mathrm{F}}$ as a field. Reconsider $p_1 = p$, $A_1 = |p|$ as a polynomial of n,f_1. Reconsider $x_2 = x$ as a function from n into the carrier of f_1. Set $S_1 = \mathrm{SgmX}(\mathrm{BagOrder}\, n, \mathrm{Support}\, p_1)$. Reconsider $H = A_1 \cdot S_1$ as a finite sequence of elements of the carrier of $\mathbb{R}_{\mathrm{F}}$. $\sum \mathtt{coeff}(|p|) = \sum A_1 \cdot S_1$.

Consider y being a finite sequence of elements of the carrier of f_1 such that $\mathrm{len}\, y = \mathrm{len}\, S_1$ and $\mathrm{eval}(p, x) = \sum y$ and for every element i of $\mathbb{N}$ such that $1 \leqslant i \leqslant \mathrm{len}\, y$ holds $y_{/i} = p_1 \cdot S_{1/i} \cdot (\mathrm{eval}(S_{1/i}, x_2))$. Reconsider $Y = y$ as a finite sequence of elements of $\mathbb{R}$. Define $\mathcal{P}[\text{natural number}] \equiv$ if $\$_1 \leqslant \mathrm{len}\, y$, then $|\sum(Y \restriction \$_1)| \leqslant (\sum(H \restriction \$_1)) \cdot (r^{\mathrm{degree}(p)})$. For every natural number i such that $\mathcal{P}[i]$ holds $\mathcal{P}[i+1]$. For every natural number i, $\mathcal{P}[i]$. □

Let n be an ordinal number and p be a $\mathbb{Z}$-valued polynomial of n,$\mathbb{R}_{\mathrm{F}}$. Let us note that $|p|$ is natural-valued and there exists a polynomial of n,$\mathbb{R}_{\mathrm{F}}$ which is natural-valued.

Let O be an ordinal number and p be a natural-valued polynomial of O,$\mathbb{R}_{\mathrm{F}}$. Let us observe that $\sum \mathtt{coeff}(p)$ is natural.

3. Selected Subsets of Zero Based Finite Sequences of $\mathbb{N}$ as Diophantine Sets

The scheme *SubsetDioph* deals with a natural number n and a 4-ary predicate $\mathcal{P}$ and a set $\mathcal{S}$ and states that

(Sch. 2) For every elements i_2, i_3, i_4 of n, $\{p$, where p is an n-element finite 0-sequence of $\mathbb{N}$: for every natural number i such that $i \in \mathcal{S}$ holds $\mathcal{P}[p(i), p(i_2), p(i_3), p(i_4)]\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$

provided

- for every elements i_1, i_2, i_3, i_4 of n, $\{p$, where p is an n-element finite 0-sequence of $\mathbb{N}$: $\mathcal{P}[p(i_1), p(i_2), p(i_3), p(i_4)]\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$ and
- $\mathcal{S} \subseteq \mathbb{Z}_n$.

Now we state the propositions:

(12) Suppose $n_1 + n_2 \leqslant n$.
Then $\{p : p(i_1) \geqslant k\cdot((p(i_2)^{\mathbf{2}} + 1) \cdot (\prod(1 + p_{\lfloor n_1} \restriction n_2)) \cdot (l \cdot p(i_3) + m)^{i \cdot p(i_4)+j})\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$.
Proof: Define $\mathcal{F}_0$(natural number, natural number, natural number) $=$ ${\$_1}^{\$_2}$. Define $\mathcal{P}_0$[natural number, natural number, natural object, natural number, natural number, natural number] $\equiv 1 \cdot \$_1 \geqslant k \cdot \$_3 + 0$. For every i_1, i_2, i_3, i_4, and i_5, $\{p : \mathcal{P}_0[p(i_1), p(i_2), \mathcal{F}_0(p(i_3), p(i_4), p(i_5)), p(i_3), p(i_4), p(i_5)]\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$. Define $\mathcal{F}_1$(natural number, natural number, natural number) $= i\cdot\$_1 + j$. Define $\mathcal{P}_1$[natural number, natural number, natural object, natural number, natural number, natural number] $\equiv \$_1 \geqslant k\cdot({\$_2}^{\$_3})$. For every i_1, i_2, i_3, i_4, and i_5, $\{p : \mathcal{P}_1[p(i_1), p(i_2), \mathcal{F}_1(p(i_3), p(i_4), p(i_5)), p(i_3), p(i_4), p(i_5)]\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$. Define $\mathcal{F}_2$(natural number, natural number, natural number) $= 1 \cdot \$_1 \cdot \$_2$.

Define $\mathcal{P}_2$[natural number, natural number, natural object, natural number, natural number, natural number] $\equiv \$_1 \geqslant k\cdot({\$_3}^{i\cdot\$_2+j})$. For every i_1, i_2, i_3, i_4, and i_5, $\{p : \mathcal{P}_2[p(i_1), p(i_2), \mathcal{F}_2(p(i_3), p(i_4), p(i_5)), p(i_3), p(i_4), p(i_5)]\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$. Define $\mathcal{P}_3$[natural number, natural number, natural object, natural number, natural number, natural number] $\equiv \$_1 \geqslant k \cdot (\$_6 \cdot {\$_3}^{i\cdot\$_2+j})$. For every i_1, i_2, i_3, i_4, and i_5, $\{p : \mathcal{P}_3[p(i_1), p(i_2), \mathcal{F}_2(p(i_3), p(i_4), p(i_5)), p(i_3), p(i_4), p(i_5)]\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$. Define $\mathcal{F}_5$(natural number, natural number, natural number) $= 1\cdot\$_1 + 1$. Define $\mathcal{P}_5$[natural number, natural number, natural object, natural number, natural number, natural number] $\equiv \$_1 \geqslant k \cdot (\$_3 \cdot \$_5 \cdot {\$_6}^{i\cdot\$_2+j})$. For every i_1, i_2, i_3, i_4, and i_5, $\{p : \mathcal{P}_5[p(i_1), p(i_2), \mathcal{F}_5(p(i_3),$

$p(i_4), p(i_5)), p(i_3), p(i_4), p(i_5)]\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$. Define $\mathcal{G}$(natural number, natural number, natural number) $= l \cdot \$_1 + m$. Define $\mathcal{R}_1$[natural number, natural number, natural object, natural number, natural number, natural number] $\equiv \$_1 \geqslant k \cdot (\$_3 \cdot \$_5 \cdot (\$_6 + 1)^{i \cdot \$_2 + j})$. For every i_1, i_2, i_3, i_4, and i_5, $\{p : \mathcal{R}_1[p(i_1), p(i_2), \mathcal{G}(p(i_3), p(i_4), p(i_5)), p(i_3), p(i_4), p(i_5)]\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$.

Define $\mathcal{P}_6$[natural number, natural number, natural object, natural number, natural number, natural number] $\equiv \$_1 \geqslant k \cdot ((\$_3 + 1) \cdot \$_5 \cdot (l \cdot \$_6 + m)^{i \cdot \$_2 + j})$. Define $\mathcal{F}_6$(natural number, natural number, natural number) $= 1 \cdot \$_1 \cdot \$_1$. For every n, i_1, i_2, i_3, i_4, and i_5, $\{p : \mathcal{P}_6[p(i_1), p(i_2), \mathcal{F}_6(p(i_3), p(i_4), p(i_5)), p(i_3), p(i_4), p(i_5)]\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$. Set $X = n + 1$. Reconsider $N = n$, $I_1 = i_1$, $I_2 = i_2$, $I_3 = i_3$, $I_4 = i_4$ as an element of X. Define $\mathcal{P}_7$[finite 0-sequence of $\mathbb{N}$] $\equiv \$_1(I_1) \geqslant k \cdot ((1 \cdot \$_1(I_2) \cdot \$_1(I_2) + 1) \cdot \$_1(N) \cdot (l \cdot \$_1(I_3) + m)^{i \cdot \$_1(I_4) + j})$. Define $\mathcal{Q}_7$[finite 0-sequence of $\mathbb{N}$] $\equiv \$_1(N) = \prod(1 + \$_{1\lfloor n_1} \upharpoonright n_2)$. Set $P_1 = \{p$, where p is an X-element finite 0-sequence of $\mathbb{N}$: $\mathcal{P}_7[p]$ and $\mathcal{Q}_7[p]\}$. P_1 is a Diophantine subset of the X-xtuples of $\mathbb{N}$. Define $\mathcal{S}$[finite 0-sequence of $\mathbb{N}$] $\equiv \$_1(i_1) \geqslant k \cdot ((\$_1(i_2)^{\mathbf{2}} + 1) \cdot (\prod(1 + \$_{1\lfloor n_1} \upharpoonright n_2)) \cdot (l \cdot \$_1(i_3) + m)^{i \cdot \$_1(i_4) + j})$. Set $S = \{p : \mathcal{S}[p]\}$. $S \subseteq$ the n-xtuples of $\mathbb{N}$. □

(13) Let us consider a $\mathbb{Z}$-valued polynomial P of k,$\mathbb{R}_{\mathrm{F}}$, an integer a, a permutation p_2 of n, and i_1. Suppose $k \leqslant n$. Then $\{p :$ for every k-element finite 0-sequence q of $\mathbb{N}$ such that $q = p \cdot p_2 \upharpoonright k$ holds $a \cdot p(i_1) = \mathrm{eval}(P, {}^{@}q)\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$.

(14) Let us consider a $\mathbb{Z}$-valued polynomial P of $k+1$,$\mathbb{R}_{\mathrm{F}}$, an integer a, n, i_1, and i_2. Suppose $k + 1 \leqslant n$ and $k \in i_2$. Then $\{p :$ for every $(k+1)$-element finite 0-sequence q of $\mathbb{N}$ such that $q = \langle p(i_2) \rangle \frown (p \upharpoonright k)$ holds $a \cdot p(i_1) = \mathrm{eval}(P, {}^{@}q)\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$.

Proof: Set $k_1 = k + 1$. Reconsider $I_5 = \mathrm{id}_k$ as a finite 0-sequence. Set $f = \langle i_2 \rangle \frown I_5$. Set $R = \mathrm{rng}\, f$. Consider g being a function such that g is one-to-one and $\mathrm{dom}\, g = n \setminus k_1$ and $\mathrm{rng}\, g = n \setminus R$. Reconsider $f_1 = f {+\cdot} g$ as a function from n into n. Define $\mathcal{Q}$[finite 0-sequence of $\mathbb{N}$] $\equiv$ for every k_1-element finite 0-sequence q of $\mathbb{N}$ such that $q = \$_1 \cdot f_1 \upharpoonright k_1$ holds $a \cdot \$_1(i_1) = \mathrm{eval}(P, {}^{@}q)$. Define $\mathcal{R}$[finite 0-sequence of $\mathbb{N}$] $\equiv$ for every $(k+1)$-element finite 0-sequence q of $\mathbb{N}$ such that $q = \langle \$_1(i_2) \rangle \frown (\$_1 \upharpoonright k)$ holds $a \cdot \$_1(i_1) = \mathrm{eval}(P, {}^{@}q)$. For every n-element finite 0-sequence p of $\mathbb{N}$, $\mathcal{Q}[p]$ iff $\mathcal{R}[p]$. $\{p : \mathcal{Q}[p]\} = \{q : \mathcal{R}[q]\}$. □

(15) Let us consider a $\mathbb{Z}$-valued polynomial P of $k+1$,$\mathbb{R}_{\mathrm{F}}$, n, i_1, and i_2. Suppose $k + 1 \leqslant n$ and $k \in i_1$. Then $\{p :$ for every $(k+1)$-element finite 0-sequence q of $\mathbb{N}$ such that $q = \langle p(i_1) \rangle \frown (p \upharpoonright k)$ holds $\mathrm{eval}(P, {}^{@}q) \equiv 0 \pmod{p(i_2)}\}$ is

a Diophantine subset of the n-xtuples of $\mathbb{N}$.

Proof: Set $k_1 = k + 1$. Set $X = n + 1$. Reconsider $N = n$, $I_1 = i_1$, $I_2 = i_2$ as an element of X. Define $\mathcal{P}$[finite 0-sequence of $\mathbb{N}$] $\equiv 1 \cdot \$_1(N) \equiv 0 \cdot \$_1(I_1) \pmod{1 \cdot \$_1(I_2)}$. Define $\mathcal{O}$[finite 0-sequence of $\mathbb{N}$] $\equiv$ for every k_1-element finite 0-sequence q of $\mathbb{N}$ such that $q = \langle \$_1(I_1) \rangle \frown (\$_1 \restriction k)$ holds $1 \cdot \$_1(N) = \mathrm{eval}(P, {}^{@}q)$. Define $\mathcal{M}$[finite 0-sequence of $\mathbb{N}$] $\equiv$ for every k_1-element finite 0-sequence q of $\mathbb{N}$ such that $q = \langle \$_1(I_1) \rangle \frown (\$_1 \restriction k)$ holds $(-1) \cdot \$_1(N) = \mathrm{eval}(P, {}^{@}q)$. Define $\mathcal{Q}$[finite 0-sequence of $\mathbb{N}$] $\equiv \mathcal{O}[\$_1]$ or $\mathcal{M}[\$_1]$. $\{p$, where p is an X-element finite 0-sequence of $\mathbb{N} : \mathcal{O}[p]\}$ is a Diophantine subset of the X-xtuples of $\mathbb{N}$. $\{p$, where p is an X-element finite 0-sequence of $\mathbb{N} : \mathcal{M}[p]\}$ is a Diophantine subset of the X-xtuples of $\mathbb{N}$. $\{p$, where p is an X-element finite 0-sequence of $\mathbb{N} : \mathcal{O}[p]$ or $\mathcal{M}[p]\}$ is a Diophantine subset of the X-xtuples of $\mathbb{N}$. Set $P_1 = \{p$, where p is an X-element finite 0-sequence of $\mathbb{N} : \mathcal{P}[p]$ and $\mathcal{Q}[p]\}$. P_1 is a Diophantine subset of the X-xtuples of $\mathbb{N}$.

Set $P_2 = \{p \restriction n$, where p is an X-element finite 0-sequence of $\mathbb{N} : p \in P_1\}$. Define $\mathcal{S}$[finite 0-sequence of $\mathbb{N}$] $\equiv$ for every k_1-element finite 0-sequence q of $\mathbb{N}$ such that $q = \langle \$_1(i_1) \rangle \frown (\$_1 \restriction k)$ holds $\mathrm{eval}(P, {}^{@}q) \equiv 0 \pmod{\$_1 (i_2)}$. Set $S = \{p : \mathcal{S}[p]\}$. $S \subseteq P_2$. $P_2 \subseteq S$. □

4. Bounded Quantifier Theorem and its Variant

Let us consider a $\mathbb{Z}$-valued polynomial p of $2 + n + k$,$\mathbb{R}_{\mathrm{F}}$, an n-element finite 0-sequence X of $\mathbb{N}$, and an element x of $\mathbb{N}$. Now we state the propositions:

(16) For every element z of $\mathbb{N}$ such that $z \leqslant x$ there exists a k-element finite 0-sequence y of $\mathbb{N}$ such that $\mathrm{eval}(p, {}^{@}((\langle z, x \rangle \frown X) \frown y)) = 0$ if and only if there exists a k-element finite 0-sequence Y of $\mathbb{N}$ and there exist elements Z, e, K of $\mathbb{N}$ such that $K > x$ and $K \geqslant (\sum \mathtt{coeff}(|p|)) \cdot ((x^{\mathbf{2}} + 1) \cdot (\prod(1 + X)) \cdot e^{\mathrm{degree}(p)})$ and for every natural number i such that $i \in k$ holds $Y(i) > e$ and $e > x$ and $1 + (Z + 1) \cdot (K!) = \prod(1 + K! \cdot (\mathrm{idseq}(x + 1)))$ and $\mathrm{eval}(p, {}^{@}((\langle Z, x \rangle \frown X) \frown Y)) \equiv 0 \pmod{1 + (Z + 1) \cdot (K!)}$ and for every natural number i such that $i \in k$ holds $\prod(Y(i) + 1 + -\mathrm{idseq}(e)) \equiv 0 \pmod{1 + (Z + 1) \cdot (K!)}$.

Proof: If for every element z of $\mathbb{N}$ such that $z \leqslant x$ there exists a k-element finite 0-sequence y of $\mathbb{N}$ such that $\mathrm{eval}(p, {}^{@}((\langle z, x \rangle \frown X) \frown y)) = 0$, then there exists a k-element finite 0-sequence Y of $\mathbb{N}$ and there exist elements Z, e, K of $\mathbb{N}$ such that $K > x$ and $K \geqslant (\sum \mathtt{coeff}(|p|)) \cdot ((x^{\mathbf{2}} + 1) \cdot (\prod(1 + X)) \cdot e^{\mathrm{degree}(p)})$ and for every natural number i such that $i \in k$ holds $Y(i) > e$ and $e > x$ and $1 + (Z + 1) \cdot (K!) = \prod(1 + K! \cdot (\mathrm{idseq}(x +$

1))) and $\operatorname{eval}(p, {}^{@}(((\langle Z, x\rangle \frown X) \frown Y)) \equiv 0 \pmod{1 + (Z + 1) \cdot (K!)}$ and for every natural number i such that $i \in k$ holds $\prod(Y(i) + 1 + -\operatorname{idseq}(e)) \equiv 0 \pmod{1 + (Z + 1) \cdot (K!)}$. Set $K_1 = K!$. Set $z_1 = 1 + (z + 1) \cdot K_1$. Consider p_3 being an element of $\mathbb{N}$ such that $p_3 \mid z_1$ and $p_3 \leqslant z_1$ and p_3 is prime. Define $\mathcal{P}(\text{object}) = Y(\$_1) \bmod p_3$.

Consider Y_3 being a finite 0-sequence such that $\operatorname{len} Y_3 = k$ and for every natural number i such that $i \in k$ holds $Y_3(i) = \mathcal{P}(i)$. $\operatorname{rng} Y_3 \subseteq \mathbb{N}$. Reconsider $E_1 = \operatorname{eval}(p, {}^{@}(((\langle Z, x\rangle \frown X) \frown Y))$ as an integer. $K < p_3$. For every i such that $i \in 2 + k + n$ holds $p_3 \mid (((\langle Z, x\rangle \frown X) \frown Y)(i) - (((\langle z, x\rangle \frown X) \frown Y_3)(i)$. $p_3 \mid E_1 - \operatorname{eval}(p, {}^{@}(((\langle z, x\rangle \frown X) \frown Y_3))$. Consider m being a natural number such that $|\operatorname{eval}(p, {}^{@}(((\langle z, x\rangle \frown X) \frown Y_3))| = p_3 \cdot m$. For every object i such that $i \in \operatorname{dom}({}^{@}(((\langle z, x\rangle \frown X) \frown Y_3))$ holds $|({}^{@}(((\langle z, x\rangle \frown X) \frown Y_3))(i)| \leqslant (x^{\mathbf{2}} + 1) \cdot (\prod(1 + X)) \cdot e$. $|\operatorname{eval}(p, {}^{@}(((\langle z, x\rangle \frown X) \frown Y_3))| \leqslant (\sum \mathtt{coeff}(|p|)) \cdot ((x^{\mathbf{2}} + 1) \cdot (\prod(1 + X)) \cdot e^{\operatorname{degree}(p)})$. □

(17) For every element z of $\mathbb{N}$ such that $z \leqslant x$ there exists a k-element finite 0-sequence y of $\mathbb{N}$ such that for every i such that $i \in k$ holds $y(i) \leqslant x$ and $\operatorname{eval}(p, {}^{@}(((\langle z, x\rangle \frown X) \frown y)) = 0$ if and only if there exists a k-element finite 0-sequence Y of $\mathbb{N}$ and there exist elements Z, K of $\mathbb{N}$ such that $K > x$ and $K \geqslant (\sum \mathtt{coeff}(|p|)) \cdot ((x^{\mathbf{2}} + 1) \cdot (\prod(1 + X))^{\operatorname{degree}(p)})$ and for every natural number i such that $i \in k$ holds $Y(i) > x + 1$ and $1 + (Z + 1) \cdot (K!) = \prod(1 + K! \cdot (\operatorname{idseq}(x + 1)))$ and $\operatorname{eval}(p, {}^{@}(((\langle Z, x\rangle \frown X) \frown Y)) \equiv 0 \pmod{1 + (Z + 1) \cdot (K!)}$ and for every natural number i such that $i \in k$ holds $\prod(Y(i) + 1 + -\operatorname{idseq}(x + 1)) \equiv 0 \pmod{1 + (Z + 1) \cdot (K!)}$.

Proof: Set $x_1 = x + 1$. If for every element z of $\mathbb{N}$ such that $z \leqslant x$ there exists a k-element finite 0-sequence y of $\mathbb{N}$ such that for every i such that $i \in k$ holds $y(i) \leqslant x$ and $\operatorname{eval}(p, {}^{@}(((\langle z, x\rangle \frown X) \frown y)) = 0$, then there exists a k-element finite 0-sequence Y of $\mathbb{N}$ and there exist elements Z, K of $\mathbb{N}$ such that $K > x$ and $K \geqslant (\sum \mathtt{coeff}(|p|)) \cdot ((x^{\mathbf{2}} + 1) \cdot (\prod(1 + X))^{\operatorname{degree}(p)})$ and for every natural number i such that $i \in k$ holds $Y(i) > x_1$ and $1 + (Z + 1) \cdot (K!) = \prod(1 + K! \cdot (\operatorname{idseq}(x + 1)))$ and $\operatorname{eval}(p, {}^{@}(((\langle Z, x\rangle \frown X) \frown Y)) \equiv 0 \pmod{1 + (Z + 1) \cdot (K!)}$ and for every natural number i such that $i \in k$ holds $\prod(Y(i) + 1 + -\operatorname{idseq}(x_1)) \equiv 0 \pmod{1 + (Z + 1) \cdot (K!)}$. Set $K_1 = K!$. Set $z_1 = 1 + (z + 1) \cdot K_1$.

Consider p_3 being an element of $\mathbb{N}$ such that $p_3 \mid z_1$ and $p_3 \leqslant z_1$ and p_3 is prime. Define $\mathcal{P}(\text{object}) = Y(\$_1) \bmod p_3$. Consider Y_3 being a finite 0-sequence such that $\operatorname{len} Y_3 = k$ and for every natural number i such that $i \in k$ holds $Y_3(i) = \mathcal{P}(i)$. $\operatorname{rng} Y_3 \subseteq \mathbb{N}$. Reconsider $E_1 = \operatorname{eval}(p, {}^{@}(((\langle Z, x\rangle \frown X) \frown Y))$ as an integer. $K < p_3$. For every natural number i such that $i \in k$ holds $Y_3(i) \leqslant x$. For every i such that $i \in 2 + k + n$ holds $p_3 \mid (((\langle Z, x\rangle \frown X) \frown Y)(i) - (((\langle z, x\rangle \frown X) \frown Y_3)(i)$. $p_3 \mid E_1 - \operatorname{eval}(p, {}^{@}(((\langle z, x\rangle \frown X) \frown Y_3))$. Consider

m being a natural number such that $|\mathrm{eval}(p, {}^{@}((\langle z, x\rangle ^\frown X)^\frown Y_3))| = p_3 \cdot m$. For every object i such that $i \in \mathrm{dom}({}^{@}((\langle z, x\rangle ^\frown X)^\frown Y_3))$ holds $|({}^{@}((\langle z, x\rangle ^\frown X) ^\frown Y_3))(i)| \leqslant (x^{\mathbf{2}} + 1) \cdot (\prod(1 + X))$. $|\mathrm{eval}(p, {}^{@}((\langle z, x\rangle ^\frown X) ^\frown Y_3))| \leqslant (\sum \texttt{coeff}(|p|)) \cdot ((x^{\mathbf{2}} + 1) \cdot (\prod(1 + X))^{\mathrm{degree}(p)})$. □

Let us consider a $\mathbb{Z}$-valued polynomial p of $2 + n + k$,$\mathbb{R}_{\mathrm{F}}$. Now we state the propositions:

(18) $\{X$, where X is an n-element finite 0-sequence of $\mathbb{N}$: there exists an element x of $\mathbb{N}$ such that for every element z of $\mathbb{N}$ such that $z \leqslant x$ there exists a k-element finite 0-sequence y of $\mathbb{N}$ such that $\mathrm{eval}(p, {}^{@}((\langle z, x\rangle ^\frown X)^\frown y)) = 0\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$.

Proof: Set $X_0 = \{X$, where X is an n-element finite 0-sequence of $\mathbb{N}$: there exists an element x of $\mathbb{N}$ such that for every element z of $\mathbb{N}$ such that $z \leqslant x$ there exists a k-element finite 0-sequence y of $\mathbb{N}$ such that $\mathrm{eval}(p, {}^{@}((\langle z, x\rangle ^\frown X)^\frown y)) = 0\}$. Set $n_1 = 1 + n + k$. Set $s_4 = \sum \texttt{coeff}(|p|)$. Set $D = \mathrm{degree}(p)$. Reconsider $Z_0 = 0$, $i_0 = n_1$, $i_1 = n_1 + 1$, $i_2 = n_1 + 2$, $i_3 = n_1 + 3$ as an element of $n_1 + 4$. Define $\mathcal{P}_2$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $1 \cdot \$_1(i_1) > 1 \cdot \$_1(Z_0) + 0$. Define $\mathcal{P}_3$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $\$_1(i_1) \geqslant s_4 \cdot ((\$_1(Z_0)^{\mathbf{2}} + 1) \cdot (\prod(1 + \$_{1\lfloor 1}\restriction n)) \cdot (1 \cdot \$_1(i_0) + 0)^{0 \cdot \$_1(i_0) + D})$. $\{q$, where q is an $(n_1 + 4)$-element finite 0-sequence of $\mathbb{N}$: $\mathcal{P}_3[q]\}$ is a Diophantine subset of the $n_1 + 4$-xtuples of $\mathbb{N}$.

Define $\mathcal{P}_4$[finite 0-sequence of $\mathbb{N}$] $\equiv$ for every natural number i such that $i \in k$ holds $\$_1(1+n+i) > \$_1(i_0)$ and $\prod(\$_1(1+n+i)+1+-\mathrm{idseq}(\$_1(i_0))) \equiv 0 \pmod{\$_1(i_2)}$. $\{q$, where q is an $(n_1 + 4)$-element finite 0-sequence of $\mathbb{N}$: $\mathcal{P}_4[q]\}$ is a Diophantine subset of the $n_1 + 4$-xtuples of $\mathbb{N}$. Define $\mathcal{P}_5$[finite 0-sequence of $\mathbb{N}$] $\equiv 1 \cdot \$_1(i_0) > 1 \cdot \$_1(Z_0) + 0$. Define $\mathcal{P}_6$[finite 0-sequence of $\mathbb{N}$] $\equiv 1 + (\$_1(i_3) + 1) \cdot (\$_1(i_1)!) = \$_1(i_2)$. Define $\mathcal{P}_7$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $\$_1(i_2) = \prod(1 + \$_1(i_1)! \cdot (\mathrm{idseq}(1 + \$_1(Z_0))))$. Reconsider $R = p$ as a $\mathbb{Z}$-valued polynomial of $1 + n_1$,$\mathbb{R}_{\mathrm{F}}$. Define $\mathcal{P}_8$[finite 0-sequence of $\mathbb{N}$] $\equiv$ for every $(1 + n_1)$-element finite 0-sequence Y of $\mathbb{N}$ such that $Y = \langle \$_1(i_3)\rangle ^\frown (\$_1 \restriction n_1)$ holds $\mathrm{eval}(R, {}^{@}Y) \equiv 0 \pmod{\$_1(i_2)}$. $\{q$, where q is an (n_1+4)-element finite 0-sequence of $\mathbb{N}$: $\mathcal{P}_8[q]\}$ is a Diophantine subset of the $n_1 + 4$-xtuples of $\mathbb{N}$.

Define $\mathcal{P}_{123}$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $\mathcal{P}_2[\$_1]$ and $\mathcal{P}_3[\$_1]$. $\{q$, where q is an $(n_1 + 4)$-element finite 0-sequence of $\mathbb{N}$: $\mathcal{P}_{123}[q]\}$ is a Diophantine subset of the $n_1 + 4$-xtuples of $\mathbb{N}$. Define $\mathcal{P}_{1234}$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $\mathcal{P}_{123}[\$_1]$ and $\mathcal{P}_4[\$_1]$. $\{q$, where q is an $(n_1 + 4)$-element finite 0-sequence of $\mathbb{N}$: $\mathcal{P}_{1234}[q]\}$ is a Diophantine subset of the $n_1 + 4$-xtuples of $\mathbb{N}$. Define $\mathcal{P}_{12345}$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $\mathcal{P}_{1234}[\$_1]$ and $\mathcal{P}_5[\$_1]$. $\{q$, where q is an (n_1+4)-element finite 0-sequence of $\mathbb{N}$: $\mathcal{P}_{12345}[q]\}$ is a Diophantine subset of the n_1+4-xtuples of $\mathbb{N}$. Define $\mathcal{P}_{123456}$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $\mathcal{P}_{12345}[\$_1]$ and $\mathcal{P}_6[\$_1]$. $\{q$, where q is an (n_1+4)-element finite 0-sequence of $\mathbb{N}$: $\mathcal{P}_{123456}[q]\}$ is a Diophantine subset of the n_1+4-xtuples of $\mathbb{N}$. Define $\mathcal{P}_{1234567}$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $\mathcal{P}_{123456}[\$_1]$ and $\mathcal{P}_7[\$_1]$. $\{q$, where q is an (n_1+4)-element finite 0-sequence of $\mathbb{N}$: $\mathcal{P}_{1234567}[q]\}$ is a Diophantine subset of the n_1+4-xtuples of $\mathbb{N}$.

Define $\mathcal{P}_{12345678}$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $\mathcal{P}_{1234567}[\$_1]$ and $\mathcal{P}_8[\$_1]$. Set $X_3=\{q$, where q is an (n_1+4)-element finite 0-sequence of $\mathbb{N}$: $\mathcal{P}_{12345678}[q]\}$. X_3 is a Diophantine subset of the n_1+4-xtuples of $\mathbb{N}$. Set $X_2=\{X\upharpoonright(n+1)$, where X is an (n_1+4)-element finite 0-sequence of $\mathbb{N}$: $X\in X_3\}$. Define $\mathcal{S}$[finite 0-sequence of $\mathbb{N}$] $\equiv$ for every element z of $\mathbb{N}$ such that $z\leqslant\$_1(0)$ there exists a k-element finite 0-sequence y of $\mathbb{N}$ such that for every n-element finite 0-sequence X_1 of $\mathbb{N}$ such that $X_1=\$_{1\lfloor 1}$ holds eval$(p,{}^{@}((\langle z,\$_1(0)\rangle\frown X_1)\frown y))=0$. Set $X_1=\{X$, where X is an $(n+1)$-element finite 0-sequence of $\mathbb{N}$: $\mathcal{S}[X]\}$. For every object s, $s\in X_1$ iff $s\in X_2$. Set $Y_1=\{X_{\lfloor 1}$, where X is an $(n+1)$-element finite 0-sequence of $\mathbb{N}$: $X\in X_1\}$. For every object s, $s\in Y_1$ iff $s\in X_0$. □

(19) $\{X$, where X is an n-element finite 0-sequence of $\mathbb{N}$: there exists an element x of $\mathbb{N}$ such that for every element z of $\mathbb{N}$ such that $z\leqslant x$ there exists a k-element finite 0-sequence y of $\mathbb{N}$ such that for every natural number i such that $i\in k$ holds $y(i)\leqslant x$ and eval$(p,{}^{@}((\langle z,x\rangle\frown X)\frown y))=0\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$.

Proof: Set $X_0=\{X$, where X is an n-element finite 0-sequence of $\mathbb{N}$: there exists an element x of $\mathbb{N}$ such that for every element z of $\mathbb{N}$ such that $z\leqslant x$ there exists a k-element finite 0-sequence y of $\mathbb{N}$ such that for every natural number i such that $i\in k$ holds $y(i)\leqslant x$ and eval$(p,$ ${}^{@}((\langle z,x\rangle\frown X)\frown y))=0\}$. Set $n_1=1+n+k$. Set $s_4=\sum\texttt{coeff}(|p|)$. Set $D=\text{degree}(p)$. Reconsider $Z_0=0$, $i_0=n_1$, $i_1=n_1+1$, $i_2=n_1+2$, $i_3=n_1+3$ as an element of n_1+4. Define $\mathcal{P}_2$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $1\cdot\$_1(i_1)>1\cdot\$_1(Z_0)+0$. Define $\mathcal{P}_3$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $\$_1(i_1)\geqslant s_4\cdot((\$_1(Z_0)^{\mathbf{2}}+1)\cdot(\prod(1+\$_{1\lfloor 1}\upharpoonright n))\cdot(0\cdot\$_1(i_0)+1)^{0\cdot\$_1(i_0)+D})$. $\{q$, where q is an (n_1+4)-element finite 0-sequence of $\mathbb{N}$: $\mathcal{P}_3[q]\}$ is a Diophantine subset of the n_1+4-xtuples of $\mathbb{N}$.

Define $\mathcal{P}_4$[finite 0-sequence of $\mathbb{N}$] $\equiv$ for every natural number i such that $i\in k$ holds $\$_1(1+n+i)>\$_1(i_0)$ and $\prod(\$_1(1+n+i)+1+-\text{idseq}(\$_1(i_0)))\equiv 0\ (\operatorname{mod}\$_1(i_2))$. $\{q$, where q is an (n_1+4)-element finite 0-sequence of $\mathbb{N}$: $\mathcal{P}_4[q]\}$ is a Diophantine subset of the n_1+4-xtuples of $\mathbb{N}$. Define $\mathcal{P}_5$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $\$_1(i_0)=1\cdot\$_1(Z_0)+1$. Define $\mathcal{P}_6$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $1+(\$_1(i_3)+1)\cdot(\$_1(i_1)!)=\$_1(i_2)$. Define $\mathcal{P}_7$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $\$_1(i_2)=\prod(1+\$_1(i_1)!\cdot(\text{idseq}(1+\$_1(Z_0))))$. Reconsider $R=p$ as a $\mathbb{Z}$-valued polynomial of $1 + n_1$,$\mathbb{R}_\mathrm{F}$. Define $\mathcal{P}_8$[finite 0-sequence of $\mathbb{N}$] $\equiv$ for every $(1+n_1)$-element finite 0-sequence Y of $\mathbb{N}$ such that $Y = \langle \$_1(i_3) \rangle \frown (\$_1 {\restriction} n_1)$ holds $\mathrm{eval}(R, {}^{@}Y) \equiv 0 \pmod{\$_1(i_2)}$. $\{q$, where q is an (n_1+4)-element finite 0-sequence of $\mathbb{N}$: $\mathcal{P}_8[q]\}$ is a Diophantine subset of the $n_1 + 4$-xtuples of $\mathbb{N}$.

Define $\mathcal{P}_{123}$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $\mathcal{P}_2[\$_1]$ and $\mathcal{P}_3[\$_1]$. $\{q$, where q is an $(n_1 + 4)$-element finite 0-sequence of $\mathbb{N}$: $\mathcal{P}_{123}[q]\}$ is a Diophantine subset of the $n_1 + 4$-xtuples of $\mathbb{N}$. Define $\mathcal{P}_{1234}$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $\mathcal{P}_{123}[\$_1]$ and $\mathcal{P}_4[\$_1]$. $\{q$, where q is an $(n_1 + 4)$-element finite 0-sequence of $\mathbb{N}$: $\mathcal{P}_{1234}[q]\}$ is a Diophantine subset of the $n_1 + 4$-xtuples of $\mathbb{N}$. Define $\mathcal{P}_{12345}$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $\mathcal{P}_{1234}[\$_1]$ and $\mathcal{P}_5[\$_1]$. $\{q$, where q is an (n_1+4)-element finite 0-sequence of $\mathbb{N}$: $\mathcal{P}_{12345}[q]\}$ is a Diophantine subset of the $n_1 + 4$-xtuples of $\mathbb{N}$. Define $\mathcal{P}_{123456}$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $\mathcal{P}_{12345}[\$_1]$ and $\mathcal{P}_6[\$_1]$. $\{q$, where q is an $(n_1 + 4)$-element finite 0-sequence of $\mathbb{N}$: $\mathcal{P}_{123456}[q]\}$ is a Diophantine subset of the $n_1 + 4$-xtuples of $\mathbb{N}$. Define $\mathcal{P}_{1234567}$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $\mathcal{P}_{123456}[\$_1]$ and $\mathcal{P}_7[\$_1]$. $\{q$, where q is an $(n_1 + 4)$-element finite 0-sequence of $\mathbb{N}$: $\mathcal{P}_{1234567}[q]\}$ is a Diophantine subset of the $n_1 + 4$-xtuples of $\mathbb{N}$. Define $\mathcal{P}_{12345678}$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $\mathcal{P}_{1234567}[\$_1]$ and $\mathcal{P}_8[\$_1]$. Set $X_3 = \{q$, where q is an (n_1+4)-element finite 0-sequence of $\mathbb{N}$: $\mathcal{P}_{12345678}[q]\}$. X_3 is a Diophantine subset of the $n_1 + 4$-xtuples of $\mathbb{N}$. Set $X_2 = \{X {\restriction} (n+1)$, where X is an (n_1+4)-element finite 0-sequence of $\mathbb{N}$: $X \in X_3\}$.

Define $\mathcal{S}$[finite 0-sequence of $\mathbb{N}$] $\equiv$ for every element z of $\mathbb{N}$ such that $z \leqslant \$_1(0)$ there exists a k-element finite 0-sequence y of $\mathbb{N}$ such that for every n-element finite 0-sequence X_1 of $\mathbb{N}$ such that $X_1 = \$_{1\lfloor 1}$ holds for every i such that $i \in k$ holds $y(i) \leqslant \$_1(0)$ and $\mathrm{eval}(p, {}^{@}((\langle z, \$_1(0) \rangle \frown X_1) \frown y)) = 0$. Set $X_1 = \{X$, where X is an $(n + 1)$-element finite 0-sequence of $\mathbb{N}$: $\mathcal{S}[X]\}$. For every object s, $s \in X_1$ iff $s \in X_2$. Set $Y_1 = \{X_{\lfloor 1}$, where X is an $(n+1)$-element finite 0-sequence of $\mathbb{N}$: $X \in X_1\}$. For every object s, $s \in Y_1$ iff $s \in X_0$. □

Let n be a natural number and A be a subset of the n-xtuples of $\mathbb{N}$. We say that A is recursively enumerable if and only if

(Def. 4) there exists a natural number m and there exists a $\mathbb{Z}$-valued polynomial P of $2 + n + m$,$\mathbb{R}_\mathrm{F}$ such that for every n-element finite 0-sequence X of $\mathbb{N}$, $X \in A$ iff there exists an element x of $\mathbb{N}$ such that for every element z of $\mathbb{N}$ such that $z \leqslant x$ there exists an m-element finite 0-sequence Y of $\mathbb{N}$ such that for every object i such that $i \in \mathrm{dom}\, Y$ holds $Y(i) \leqslant x$ and $\mathrm{eval}(P, {}^{@}((\langle z, x \rangle \frown X) \frown Y)) = 0$.

Now we state the proposition:

(20) Let us consider a natural number n, and a subset A of the n-xtuples of $\mathbb{N}$. If A is Diophantine, then A is recursively enumerable.

PROOF: Consider m being a natural number, P being a $\mathbb{Z}$-valued polynomial of $n + m$,$\mathbb{R}_{\mathrm{F}}$ such that for every object s, $s \in A$ iff there exists an n-element finite 0-sequence x of $\mathbb{N}$ and there exists an m-element finite 0-sequence y of $\mathbb{N}$ such that $s = x$ and $\mathrm{eval}(P, {}^{@}(x ^\frown y)) = 0$. Set $n_4 = n+m$. Reconsider $\mathrm{P}_0 = P$ as a $\mathbb{Z}$-valued polynomial of $0 + n_4$,$\mathbb{R}_{\mathrm{F}}$. Consider q being a polynomial of $0 + 2 + n_4$,$\mathbb{R}_{\mathrm{F}}$ such that $\mathrm{rng}\, q \subseteq \mathrm{rng}\, \mathrm{P}_0 \cup \{0_{\mathbb{R}_{\mathrm{F}}}\}$ and for every function x_1 from $0 + n_4$ into $\mathbb{R}_{\mathrm{F}}$ and for every function X_1 from $0 + 2 + n_4$ into $\mathbb{R}_{\mathrm{F}}$ such that $x_1 {\restriction} 0 = X_1 {\restriction} 0$ and $({}^{@}x_1)_{\lfloor 0} = ({}^{@}X_1)_{\lfloor 0+2}$ holds $\mathrm{eval}(\mathrm{P}_0, x_1) = \mathrm{eval}(q, X_1)$.

Reconsider $Q = q$ as a $\mathbb{Z}$-valued polynomial of $2+n+m$,$\mathbb{R}_{\mathrm{F}}$. If $X \in A$, then there exists an element x of $\mathbb{N}$ such that for every element z of $\mathbb{N}$ such that $z \leqslant x$ there exists an m-element finite 0-sequence Y of $\mathbb{N}$ such that for every object i such that $i \in \mathrm{dom}\, Y$ holds $Y(i) \leqslant x$ and $\mathrm{eval}(Q, {}^{@}((\langle z, x \rangle ^\frown X) ^\frown Y)) = 0$. Consider y being an m-element finite 0-sequence of $\mathbb{N}$ such that for every object i such that $i \in \mathrm{dom}\, y$ holds $y(i) \leqslant a$ and $\mathrm{eval}(Q, {}^{@}((\langle a, a \rangle ^\frown X) ^\frown y)) = 0$. □

5. MRDP Theorem

Now we state the proposition:

(21) YURI MATIYASEVICH, JULIA ROBINSON, MARTIN DAVIS, HILARY PUTNAM THEOREM:

Let us consider a natural number n, and a subset A of the n-xtuples of $\mathbb{N}$. If A is recursively enumerable, then A is Diophantine. The theorem is a consequence of (19).

References

[1] Marcin Acewicz and Karol Pąk. Basic Diophantine relations. *Formalized Mathematics*, 26(**2**):175–181, 2018. doi:10.2478/forma-2018-0015.

[2] Marcin Acewicz and Karol Pąk. Pell's equation. *Formalized Mathematics*, 25(**3**):197–204, 2017. doi:10.1515/forma-2017-0019.

[3] Zofia Adamowicz and Paweł Zbierski. *Logic of Mathematics: A Modern Course of Classical Logic*. Pure and Applied Mathematics: A Wiley Series of Texts, Monographs and Tracts. Wiley-Interscience, 1997.

[4] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, Karol Pąk, and Josef Urban. Mizar: State-of-the-art and beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8_17.

[5] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pąk. The role of the Mizar Mathematical Library for interactive proof development in Mizar. *Journal of Automated Reasoning*, 61(1):9–32, 2018. doi:10.1007/s10817-017-9440-6.

[6] Martin Davis. Hilbert's tenth problem is unsolvable. *The American Mathematical Monthly, Mathematical Association of America*, 80(3):233–269, 1973. doi:10.2307/2318447.

[7] Adam Grabowski, Artur Korniłowicz, and Adam Naumowicz. Four decades of Mizar. *Journal of Automated Reasoning*, 55(3):191–198, 2015. doi:10.1007/s10817-015-9345-1.

[8] Karol Pąk. The Matiyasevich theorem. Preliminaries. *Formalized Mathematics*, 25(**4**): 315–322, 2017. doi:10.1515/forma-2017-0029.

[9] Karol Pąk. Diophantine sets. Part II. *Formalized Mathematics*, 27(**2**):197–208, 2019. doi:10.2478/forma-2019-0019.

[10] Craig Alan Smorynski. *Logical Number Theory I, An Introduction.* Universitext. Springer-Verlag Berlin Heidelberg, 1991. ISBN 978-3-642-75462-3.

Accepted May 27, 2019