FORMALIZED MATHEMATICS
Vol. 21, No. 1, Pages 1–23, 2013
DOI: 10.2478/forma-2013-0001

VERSITA
degruyter.com/view/j/forma

Analysis of Algorithms: An Example of a Sort Algorithm

Grzegorz Bancerek
Association of Mizar Users
Białystok, Poland

Summary. We analyse three algorithms: exponentiation by squaring, calculation of maximum, and sorting by exchanging in terms of program algebra over an algebra.

MML identifier: AOFA_A01, version: 8.0.01 5.5.1167

The notation and terminology used in this paper have been introduced in the following articles: [37], [1], [2], [17], [3], [4], [13], [18], [34], [23], [29], [19], [20], [15], [5], [33], [6], [27], [38], [28], [30], [14], [7], [8], [31], [16], [24], [26], [35], [9], [21], [32], [39], [36], [10], [11], [25], [12], and [22].

1. Exponentiation by Squaring Revisited

Now we state the propositions:

(1) (i) $1 \bmod 2 = 1$, and

(ii) $2 \bmod 2 = 0$.

(2) Let us consider a non empty non void many sorted signature Σ, an algebra $\mathfrak{A}$ over Σ, a subalgebra $\mathfrak{B}$ of $\mathfrak{A}$, a sort symbol s of Σ, and a set a. Suppose $a \in$ (the sorts of $\mathfrak{B}$)(s). Then $a \in$ (the sorts of $\mathfrak{A}$)(s).

(3) Let us consider a non empty set I, sets a, b, c, and an element i of I. Then $c \in (i\text{-singleton}\, a)(b)$ if and only if $b = i$ and $c = a$.

(4) Let us consider a non empty set I, sets a, b, c, d, and elements i, j of I. Then $c \in (i\text{-singleton}\, a \cup j\text{-singleton}\, d)(b)$ if and only if $b = i$ and $c = a$ or $b = j$ and $c = d$. The theorem is a consequence of (3).

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

Let Σ be a boolean correct non empty non void boolean signature with integers with connectives from 4 and the sort at 1 and $\mathfrak{A}$ be a non-empty algebra over Σ. We say that $\mathfrak{A}$ is integer if and only if

(Def. 1) There exists an image $\mathfrak{C}$ of $\mathfrak{A}$ such that $\mathfrak{C}$ is a boolean correct algebra over Σ with integers with connectives from 4 and the sort at 1.

Now we state the propositions:

(5) Let us consider a non empty non void many sorted signature Σ and a non-empty algebra $\mathfrak{A}$ over Σ. Then $\operatorname{Im} \mathrm{id}_\alpha =$ the algebra of $\mathfrak{A}$, where α is the sorts of $\mathfrak{A}$.

(6) Let us consider a non empty non void many sorted signature Σ. Then every non-empty algebra over Σ is an image of $\mathfrak{A}$. The theorem is a consequence of (5). Proof: $\mathfrak{A}$ is $\mathfrak{A}$-image. □

Let Σ be a boolean correct non empty non void boolean signature with integers with connectives from 4 and the sort at 1. One can verify that there exists a non-empty algebra over Σ which is integer.

Let $\mathfrak{A}$ be an integer non-empty algebra over Σ. Note that there exists an image of $\mathfrak{A}$ which is boolean correct.

Let us note that there exists a boolean correct image of $\mathfrak{A}$ which has integers with connectives from 4 and the sort at 1.

Now we state the proposition:

(7) Let us consider a non empty non void many sorted signature Σ, a non-empty algebra $\mathfrak{A}$ over Σ, an operation symbol o of Σ, a set a, and a sort symbol r of Σ. Suppose o is of type $a \to r$. Then

(i) $\mathrm{Den}(o, \mathfrak{A})$ is a function from (the sorts of $\mathfrak{A})^{\#}(a)$ into (the sorts of $\mathfrak{A})(r)$, and

(ii) $\mathrm{Args}(o, \mathfrak{A}) =$ (the sorts of $\mathfrak{A})^{\#}(a)$, and

(iii) $\mathrm{Result}(o, \mathfrak{A}) =$ (the sorts of $\mathfrak{A})(r)$.

Let Σ be a boolean correct non empty non void boolean signature and $\mathfrak{A}$ be a boolean correct non-empty algebra over Σ. Observe that every non-empty subalgebra of $\mathfrak{A}$ is boolean correct.

Let Σ be a boolean correct non empty non void boolean signature with integers with connectives from 4 and the sort at 1 and $\mathfrak{A}$ be a boolean correct non-empty algebra over Σ with integers with connectives from 4 and the sort at 1. Note that every non-empty subalgebra of $\mathfrak{A}$ has integers with connectives from 4 and the sort at 1.

Let X be a non-empty many sorted set indexed by the carrier of Σ. Let us observe that $\mathfrak{F}_\Sigma(X)$ is integer as a non-empty algebra over Σ.

Now we state the proposition:

(8) Let us consider a non empty non void many sorted signature Σ, algebras $\mathfrak{A}_1$, $\mathfrak{A}_2$, $\mathfrak{B}_1$ over Σ, and a non-empty algebra $\mathfrak{B}_2$ over Σ. Suppose

(i) the algebra of $\mathfrak{A}_1$ = the algebra of $\mathfrak{A}_2$, and

(ii) the algebra of $\mathfrak{B}_1$ = the algebra of $\mathfrak{B}_2$.

Let us consider a many sorted function h_1 from $\mathfrak{A}_1$ into $\mathfrak{B}_1$ and a many sorted function h_2 from $\mathfrak{A}_2$ into $\mathfrak{B}_2$. Suppose

(iii) $h_1 = h_2$, and

(iv) h_1 is an epimorphism of $\mathfrak{A}_1$ onto $\mathfrak{B}_1$.

Then h_2 is an epimorphism of $\mathfrak{A}_2$ onto $\mathfrak{B}_2$.

Let Σ be a boolean correct non empty non void boolean signature with integers with connectives from 4 and the sort at 1 and X be a non-empty many sorted set indexed by the carrier of Σ. Let us note that there exists an including Σ-terms over X non-empty free variable algebra over Σ which is vf-free and integer.

Let Σ be a non empty non void many sorted signature. Let $\mathfrak{T}$ be an including Σ-terms over X non-empty algebra over Σ. The functor FreeGenerator($\mathfrak{T}$) yielding a non-empty generator set of $\mathfrak{T}$ is defined by the term

(Def. 2) FreeGenerator(X).

Let X_0 be a countable non-empty many sorted set indexed by the carrier of Σ and $\mathfrak{T}$ be an including Σ-terms over X_0 non-empty algebra over Σ. Let us observe that FreeGenerator($\mathfrak{T}$) is Equations($\Sigma, \mathfrak{T}$)-free and non-empty.

Let X be a non-empty many sorted set indexed by the carrier of Σ, $\mathfrak{T}$ be an including Σ-terms over X algebra over Σ, and G be a generator set of $\mathfrak{T}$. We say that G is basic if and only if

(Def. 3) FreeGenerator($\mathfrak{T}$) $\subseteq G$.

Let s be a sort symbol of Σ and x be an element of $G(s)$. We say that x is pure if and only if

(Def. 4) $x \in$ (FreeGenerator($\mathfrak{T}$))(s).

Observe that FreeGenerator($\mathfrak{T}$) is basic.

Note that there exists a non-empty generator set of $\mathfrak{T}$ which is basic.

Let G be a basic generator set of $\mathfrak{T}$ and s be a sort symbol of Σ. One can check that there exists an element of $G(s)$ which is pure.

Now we state the proposition:

(9) Let us consider a non empty non void many sorted signature Σ, a non-empty many sorted set X indexed by the carrier of Σ, an including Σ-terms over X algebra $\mathfrak{T}$ over Σ, a basic generator set G of $\mathfrak{T}$, a sort symbol s of Σ, and a set a. Then a is a pure element of $G(s)$ if and only if $a \in$ (FreeGenerator($\mathfrak{T}$))(s).

Let Σ be a non empty non void many sorted signature, X be a non-empty many sorted set indexed by the carrier of Σ, $\mathfrak{T}$ be an including Σ-terms over X algebra over Σ, and G be a generator system over Σ, X, and $\mathfrak{T}$. We say that G is basic if and only if

(Def. 5) The generators of G are basic.

Observe that there exists a generator system over Σ, X, and $\mathfrak{T}$ which is basic.

Let G be a basic generator system over Σ, X, and $\mathfrak{T}$. Note that the generators of G are basic.

In this paper Σ denotes a boolean correct non empty non void boolean signature with integers with connectives from 4 and the sort at 1, X denotes a non-empty many sorted set indexed by the carrier of Σ, $\mathfrak{T}$ denotes a vf-free including Σ-terms over X integer non-empty free variable algebra over Σ, $\mathfrak{C}$ denotes a boolean correct non-empty image of $\mathfrak{T}$ with integers with connectives from 4 and the sort at 1, G denotes a basic generator system over Σ, X, and $\mathfrak{T}$, $\mathfrak{A}$ denotes a if-while algebra over the generators of G, I denotes an integer sort symbol of Σ, x, y, z, m denote pure elements of (the generators of G)(I), b denotes a pure element of (the generators of G)((the boolean sort of Σ)), τ, τ_1, τ_2 denote elements of $\mathfrak{T}$ from I, P denotes an algorithm of $\mathfrak{A}$, and s, s_1, s_2 denote elements of $\mathfrak{C}$-States(the generators of G).

Let Σ be a boolean correct non empty non void boolean signature and $\mathfrak{A}$ be a non-empty algebra over Σ. The functor $\mathrm{false}_{\mathfrak{A}}$ yielding an element of $\mathfrak{A}$ from the boolean sort of Σ is defined by the term

(Def. 6) $\neg\,\mathrm{true}_{\mathfrak{A}}$.

In this paper f denotes an execution function of $\mathfrak{A}$ over $\mathfrak{C}$-States(the generators of G) and $\mathrm{States}_{b\nrightarrow\mathrm{false}_{\mathfrak{C}}}$(the generators of G).

Now we state the proposition:

(10) $\mathrm{false}_{\mathfrak{C}} = \mathit{false}$.

Let Σ be a boolean correct non empty non void boolean signature, X be a non-empty many sorted set indexed by the carrier of Σ, $\mathfrak{T}$ be an including Σ-terms over X algebra over Σ, G be a generator system over Σ, X, and $\mathfrak{T}$, b be an element of (the generators of G)((the boolean sort of Σ)), $\mathfrak{C}$ be an image of $\mathfrak{T}$, $\mathfrak{A}$ be a pre-if-while algebra, f be an execution function of $\mathfrak{A}$ over $\mathfrak{C}$-States(the generators of G) and $\mathrm{States}_{b\nrightarrow\mathrm{false}_{\mathfrak{C}}}$(the generators of G), s be an element of $\mathfrak{C}$-States(the generators of G), and P be an algorithm of $\mathfrak{A}$. Note that the functor $f(s, P)$ yields an element of $\mathfrak{C}$-States(the generators of G). Let Σ be a non empty non void many sorted signature, $\mathfrak{T}$ be a non-empty algebra over Σ, G be a non-empty generator set of $\mathfrak{T}$, s be a sort symbol of Σ, and x be an element of $G(s)$. The functor ${}^{@}x$ yielding an element of $\mathfrak{T}$ from s is defined by the term

(Def. 7) x.

Let us consider Σ, X, $\mathfrak{T}$, G, $\mathfrak{A}$, b, I, τ_1, and τ_2. The functors $b\,\mathrm{leq}(\tau_1, \tau_2, \mathfrak{A})$ and $b\,\mathrm{gt}(\tau_1, \tau_2, \mathfrak{A})$ yielding algorithms of $\mathfrak{A}$ are defined by the terms, respectively.

(Def. 8) $b{:=}_{\mathfrak{A}}(\mathrm{leq}(\tau_1, \tau_2))$.

(Def. 9) $b{:=}_{\mathfrak{A}}(\neg \operatorname{leq}(\tau_1, \tau_2))$.

The functor $2^I_{\mathfrak{T}}$ yielding an element of $\mathfrak{T}$ from I is defined by the term

(Def. 10) $1^I_{\mathfrak{T}} + 1^I_{\mathfrak{T}}$.

Let us consider G, $\mathfrak{A}$, and b. Let us consider τ. The functors τ is $\operatorname{odd}(b, \mathfrak{A})$ and τ is $\operatorname{even}(b, \mathfrak{A})$ yielding algorithms of $\mathfrak{A}$ are defined by the terms, respectively.

(Def. 11) $b\,\operatorname{gt}(\tau \bmod 2^I_{\mathfrak{T}}, 0^I_{\mathfrak{T}}, \mathfrak{A})$.

(Def. 12) $b\,\operatorname{leq}(\tau \bmod 2^I_{\mathfrak{T}}, 0^I_{\mathfrak{T}}, \mathfrak{A})$.

Let us consider $\mathfrak{C}$. Let us consider s. Let x be an element of (the generators of G)(I). Let us note that $s(I)(x)$ is integer.

Let us consider τ. Let us note that τ value at$(\mathfrak{C}, s)$ is integer.

In the sequel u denotes a many sorted function from FreeGenerator$(\mathfrak{T})$ into the sorts of $\mathfrak{C}$.

Let us consider Σ, X, $\mathfrak{T}$, $\mathfrak{C}$, I, u, and τ. One can verify that τ value at$(\mathfrak{C}, u)$ is integer.

Let us consider G. Let us consider s. Let τ be an element of $\mathfrak{T}$ from the boolean sort of Σ. One can verify that τ value at$(\mathfrak{C}, s)$ is boolean.

Let us consider u. One can check that τ value at$(\mathfrak{C}, u)$ is boolean.

Let us consider an operation symbol o of Σ. Now we state the propositions:

(11) Suppose $o =$ (the connectives of Σ)$(1)(\in$ (the carrier' of $\Sigma))$. Then
  (i) $o =$ (the connectives of Σ)(1), and
  (ii) $\operatorname{Arity}(o) = \emptyset$, and
  (iii) the result sort of $o =$ the boolean sort of Σ.

(12) Suppose $o =$ (the connectives of Σ)$(2)(\in$ (the carrier' of $\Sigma))$. Then
  (i) $o =$ (the connectives of Σ)(2), and
  (ii) $\operatorname{Arity}(o) = \langle$the boolean sort of $\Sigma\rangle$, and
  (iii) the result sort of $o =$ the boolean sort of Σ.

(13) Suppose $o =$ (the connectives of Σ)$(3)(\in$ (the carrier' of $\Sigma))$. Then
  (i) $o =$ (the connectives of Σ)(3), and
  (ii) $\operatorname{Arity}(o) = \langle$the boolean sort of Σ, the boolean sort of $\Sigma\rangle$, and
  (iii) the result sort of $o =$ the boolean sort of Σ.

(14) Suppose $o =$ (the connectives of Σ)$(4)(\in$ (the carrier' of $\Sigma))$. Then
  (i) $\operatorname{Arity}(o) = \emptyset$, and
  (ii) the result sort of $o = I$.

(15) Suppose $o =$ (the connectives of Σ)$(5)(\in$ (the carrier' of $\Sigma))$. Then
  (i) $\operatorname{Arity}(o) = \emptyset$, and
  (ii) the result sort of $o = I$.

(16) Suppose $o =$ (the connectives of Σ)(6)($\in$ (the carrier' of Σ)). Then

(i) Arity$(o) = \langle I \rangle$, and

(ii) the result sort of $o = I$.

(17) Suppose $o =$ (the connectives of Σ)(7)($\in$ (the carrier' of Σ)). Then

(i) Arity$(o) = \langle I, I \rangle$, and

(ii) the result sort of $o = I$.

(18) Suppose $o =$ (the connectives of Σ)(8)($\in$ (the carrier' of Σ)). Then

(i) Arity$(o) = \langle I, I \rangle$, and

(ii) the result sort of $o = I$.

(19) Suppose $o =$ (the connectives of Σ)(9)($\in$ (the carrier' of Σ)). Then

(i) Arity$(o) = \langle I, I \rangle$, and

(ii) the result sort of $o = I$.

(20) Suppose $o =$ (the connectives of Σ)(10)($\in$ (the carrier' of Σ)). Then

(i) Arity$(o) = \langle I, I \rangle$, and

(ii) the result sort of $o =$ the boolean sort of Σ.

(21) Let us consider a non empty non void many sorted signature Σ and an operation symbol o of Σ. Suppose Arity$(o) = \emptyset$. Let us consider an algebra $\mathfrak{A}$ over Σ. Then Args$(o, \mathfrak{A}) = \{\emptyset\}$.

(22) Let us consider a non empty non void many sorted signature Σ, a sort symbol a of Σ, and an operation symbol o of Σ. Suppose Arity$(o) = \langle a \rangle$. Let us consider an algebra $\mathfrak{A}$ over Σ. Then Args$(o, \mathfrak{A}) = \prod \langle$(the sorts of $\mathfrak{A})(a) \rangle$.

(23) Let us consider a non empty non void many sorted signature Σ, sort symbols a, b of Σ, and an operation symbol o of Σ. Suppose Arity$(o) = \langle a, b \rangle$. Let us consider an algebra $\mathfrak{A}$ over Σ. Then Args$(o, \mathfrak{A}) = \prod \langle$(the sorts of $\mathfrak{A})(a)$, (the sorts of $\mathfrak{A})(b) \rangle$.

(24) Let us consider a non empty non void many sorted signature Σ, sort symbols a, b, c of Σ, and an operation symbol o of Σ. Suppose Arity$(o) = \langle a, b, c \rangle$. Let us consider an algebra $\mathfrak{A}$ over Σ. Then Args$(o, \mathfrak{A}) = \prod \langle$(the sorts of $\mathfrak{A})(a)$, (the sorts of $\mathfrak{A})(b)$, (the sorts of $\mathfrak{A})(c) \rangle$.

(25) Let us consider a non empty non void many sorted signature Σ, non-empty algebras $\mathfrak{A}$, $\mathfrak{B}$ over Σ, a sort symbol s of Σ, an element a of $\mathfrak{A}$ from s, a many sorted function h from $\mathfrak{A}$ into $\mathfrak{B}$, and an operation symbol o of Σ. Suppose Arity$(o) = \langle s \rangle$. Let us consider an element p of Args$(o, \mathfrak{A})$. If $p = \langle a \rangle$, then $h \# p = \langle h(s)(a) \rangle$.

(26) Let us consider a non empty non void many sorted signature Σ, non-empty algebras $\mathfrak{A}$, $\mathfrak{B}$ over Σ, sort symbols s_1, s_2 of Σ, an element a of $\mathfrak{A}$ from s_1, an element b of $\mathfrak{A}$ from s_2, a many sorted function h from $\mathfrak{A}$ into $\mathfrak{B}$, and an operation symbol o of Σ. Suppose $\mathrm{Arity}(o) = \langle s_1, s_2 \rangle$. Let us consider an element p of $\mathrm{Args}(o, \mathfrak{A})$. Suppose $p = \langle a, b \rangle$. Then $h\#p = \langle h(s_1)(a), h(s_2)(b) \rangle$.

(27) Let us consider a non empty non void many sorted signature Σ, non-empty algebras $\mathfrak{A}$, $\mathfrak{B}$ over Σ, sort symbols s_1, s_2, s_3 of Σ, an element a of $\mathfrak{A}$ from s_1, an element b of $\mathfrak{A}$ from s_2, an element c of $\mathfrak{A}$ from s_3, a many sorted function h from $\mathfrak{A}$ into $\mathfrak{B}$, and an operation symbol o of Σ. Suppose $\mathrm{Arity}(o) = \langle s_1, s_2, s_3 \rangle$. Let us consider an element p of $\mathrm{Args}(o, \mathfrak{A})$. Suppose $p = \langle a, b, c \rangle$. Then $h\#p = \langle h(s_1)(a), h(s_2)(b), h(s_3)(c) \rangle$.

Let us consider a many sorted function h from $\mathfrak{T}$ into $\mathfrak{C}$, a sort symbol a of Σ, and an element τ of $\mathfrak{T}$ from a. Now we state the propositions:

(28) If h is a homomorphism of $\mathfrak{T}$ into $\mathfrak{C}$,
then τ value at$(\mathfrak{C}, h \restriction \mathrm{FreeGenerator}(\mathfrak{T})) = h(a)(\tau)$.

(29) Suppose h is a homomorphism of $\mathfrak{T}$ into $\mathfrak{C}$ and $s = h \restriction$ the generators of G. Then τ value at$(\mathfrak{C}, s) = h(a)(\tau)$.

(30) $\mathrm{true}_{\mathfrak{T}}$ value at$(\mathfrak{C}, s) = \mathit{true}$. The theorem is a consequence of (11) and (21).

(31) Let us consider an element τ of $\mathfrak{T}$ from the boolean sort of Σ. Then $\neg\tau$ value at$(\mathfrak{C}, s) = \neg(\tau$ value at$(\mathfrak{C}, s))$. The theorem is a consequence of (29), (12), (22), and (25).

(32) Let us consider a boolean set a and an element τ of $\mathfrak{T}$ from the boolean sort of Σ. Then $\neg\tau$ value at$(\mathfrak{C}, s) = \neg a$ if and only if τ value at$(\mathfrak{C}, s) = a$. The theorem is a consequence of (31).

(33) Let us consider an element a of $\mathfrak{C}$ from the boolean sort of Σ and a boolean set x. Then $\neg a = \neg x$ if and only if $a = x$.

(34) $\mathrm{false}_{\mathfrak{T}}$ value at$(\mathfrak{C}, s) = \mathit{false}$. The theorem is a consequence of (31) and (30).

(35) Let us consider elements τ_1, τ_2 of $\mathfrak{T}$ from the boolean sort of Σ. Then $(\tau_1 \wedge \tau_2)$ value at$(\mathfrak{C}, s) = (\tau_1$ value at$(\mathfrak{C}, s)) \wedge (\tau_2$ value at$(\mathfrak{C}, s))$. The theorem is a consequence of (29), (13), (23), and (26).

(36) $0^I_{\mathfrak{T}}$ value at$(\mathfrak{C}, s) = 0$. The theorem is a consequence of (14) and (21).

(37) $1^I_{\mathfrak{T}}$ value at$(\mathfrak{C}, s) = 1$. The theorem is a consequence of (15) and (21).

(38) $(-\tau)$ value at$(\mathfrak{C}, s) = -\tau$ value at$(\mathfrak{C}, s)$. The theorem is a consequence of (16), (22), and (25).

(39) $(\tau_1 + \tau_2)$ value at$(\mathfrak{C}, s) = \tau_1$ value at$(\mathfrak{C}, s) + \tau_2$ value at$(\mathfrak{C}, s)$. The theorem is a consequence of (17), (23), and (26).

(40) $2^I_{\mathfrak{T}}$ value at$(\mathfrak{C}, s) = 2$. The theorem is a consequence of (37) and (39).

(41) $(\tau_1 - \tau_2)$ value at$(\mathfrak{C}, s) = \tau_1$ value at$(\mathfrak{C}, s) - \tau_2$ value at$(\mathfrak{C}, s)$. The theorem is a consequence of (39) and (38).

(42) $(\tau_1 \cdot \tau_2)$ value at$(\mathfrak{C}, s) = (\tau_1$ value at$(\mathfrak{C}, s)) \cdot (\tau_2$ value at$(\mathfrak{C}, s))$. The theorem is a consequence of (29), (18), (23), and (26).

(43) $(\tau_1 \operatorname{div} \tau_2)$ value at$(\mathfrak{C}, s) = \tau_1$ value at$(\mathfrak{C}, s) \operatorname{div} \tau_2$ value at$(\mathfrak{C}, s)$. The theorem is a consequence of (19), (23), and (26).

(44) $(\tau_1 \bmod \tau_2)$ value at$(\mathfrak{C}, s) = \tau_1$ value at$(\mathfrak{C}, s) \bmod \tau_2$ value at$(\mathfrak{C}, s)$. The theorem is a consequence of (41), (42), and (43).

(45) $\mathrm{leq}(\tau_1, \tau_2)$ value at$(\mathfrak{C}, s) = \mathrm{leq}(\tau_1$ value at$(\mathfrak{C}, s), \tau_2$ value at$(\mathfrak{C}, s))$. The theorem is a consequence of (20), (23), and (26).

(46) true$_{\mathfrak{T}}$ value at$(\mathfrak{C}, u) = \mathit{true}$. The theorem is a consequence of (11) and (21).

(47) Let us consider an element τ of $\mathfrak{T}$ from the boolean sort of Σ. Then $\neg\tau$ value at$(\mathfrak{C}, u) = \neg(\tau$ value at$(\mathfrak{C}, u))$. The theorem is a consequence of (28), (12), (22), and (25).

(48) Let us consider a boolean set a and an element τ of $\mathfrak{T}$ from the boolean sort of Σ. Then $\neg\tau$ value at$(\mathfrak{C}, u) = \neg a$ if and only if τ value at$(\mathfrak{C}, u) = a$. The theorem is a consequence of (47).

(49) false$_{\mathfrak{T}}$ value at$(\mathfrak{C}, u) = \mathit{false}$. The theorem is a consequence of (47) and (46).

(50) Let us consider elements τ_1, τ_2 of $\mathfrak{T}$ from the boolean sort of Σ. Then $(\tau_1 \wedge \tau_2)$ value at$(\mathfrak{C}, u) = (\tau_1$ value at$(\mathfrak{C}, u)) \wedge (\tau_2$ value at$(\mathfrak{C}, u))$. The theorem is a consequence of (28), (13), (23), and (26).

(51) $0^I_{\mathfrak{T}}$ value at$(\mathfrak{C}, u) = 0$. The theorem is a consequence of (14) and (21).

(52) $1^I_{\mathfrak{T}}$ value at$(\mathfrak{C}, u) = 1$. The theorem is a consequence of (15) and (21).

(53) $(-\tau)$ value at$(\mathfrak{C}, u) = -\tau$ value at$(\mathfrak{C}, u)$. The theorem is a consequence of (16), (22), and (25).

(54) $(\tau_1 + \tau_2)$ value at$(\mathfrak{C}, u) = \tau_1$ value at$(\mathfrak{C}, u) + \tau_2$ value at$(\mathfrak{C}, u)$. The theorem is a consequence of (17), (23), and (26).

(55) $2^I_{\mathfrak{T}}$ value at$(\mathfrak{C}, u) = 2$. The theorem is a consequence of (52) and (54).

(56) $(\tau_1 - \tau_2)$ value at$(\mathfrak{C}, u) = \tau_1$ value at$(\mathfrak{C}, u) - \tau_2$ value at$(\mathfrak{C}, u)$. The theorem is a consequence of (54) and (53).

(57) $(\tau_1 \cdot \tau_2)$ value at$(\mathfrak{C}, u) = (\tau_1$ value at$(\mathfrak{C}, u)) \cdot (\tau_2$ value at$(\mathfrak{C}, u))$. The theorem is a consequence of (28), (18), (23), and (26).

(58) $(\tau_1 \operatorname{div} \tau_2)$ value at$(\mathfrak{C}, u) = \tau_1$ value at$(\mathfrak{C}, u) \operatorname{div} \tau_2$ value at$(\mathfrak{C}, u)$. The theorem is a consequence of (19), (23), and (26).

(59) $(\tau_1 \bmod \tau_2)$ value at$(\mathfrak{C}, u) = \tau_1$ value at$(\mathfrak{C}, u) \bmod \tau_2$ value at$(\mathfrak{C}, u)$. The theorem is a consequence of (56), (57), and (58).

(60) $\mathrm{leq}(\tau_1, \tau_2)$ value $\mathrm{at}(\mathfrak{C}, u) = \mathrm{leq}(\tau_1$ value $\mathrm{at}(\mathfrak{C}, u), \tau_2$ value $\mathrm{at}(\mathfrak{C}, u))$.
The theorem is a consequence of (20), (23), and (26).

(61) Let us consider a sort symbol a of Σ and an element x of (the generators of $G)(a)$. Then ${}^{@}x$ value $\mathrm{at}(\mathfrak{C}, s) = s(a)(x)$. The theorem is a consequence of (29).

(62) Let us consider a sort symbol a of Σ, a pure element x of (the generators of $G)(a)$, and a many sorted function u from FreeGenerator($\mathfrak{T}$) into the sorts of $\mathfrak{C}$. Then ${}^{@}x$ value $\mathrm{at}(\mathfrak{C}, u) = u(a)(x)$.

Let us consider integers i, j and elements a, b of $\mathfrak{C}$ from I. Now we state the propositions:

(63) If $a = i$ and $b = j$, then $a - b = i - j$.

(64) If $a = i$ and $b = j$ and $j \neq 0$, then $a \bmod b = i \bmod j$.

(65) Suppose G is $\mathfrak{C}$-supported and $f \in \mathfrak{C}$-$\mathrm{Execution}_{b \nrightarrow \mathrm{false}_{\mathfrak{C}}}(\mathfrak{A})$. Then let us consider a sort symbol a of Σ, a pure element x of (the generators of $G)(a)$, and an element τ of $\mathfrak{T}$ from a. Then

(i) $f(s, x{:=}_{\mathfrak{A}}\tau)(a)(x) = \tau$ value $\mathrm{at}(\mathfrak{C}, s)$, and

(ii) for every pure element z of (the generators of $G)(a)$ such that $z \neq x$ holds $f(s, x{:=}_{\mathfrak{A}}\tau)(a)(z) = s(a)(z)$, and

(iii) for every sort symbol b of Σ such that $a \neq b$ for every pure element z of (the generators of $G)(b)$, $f(s, x{:=}_{\mathfrak{A}}\tau)(b)(z) = s(b)(z)$.

(66) Suppose G is $\mathfrak{C}$-supported and $f \in \mathfrak{C}$-$\mathrm{Execution}_{b \nrightarrow \mathrm{false}_{\mathfrak{C}}}(\mathfrak{A})$. Then

(i) τ_1 value $\mathrm{at}(\mathfrak{C}, s) < \tau_2$ value $\mathrm{at}(\mathfrak{C}, s)$ iff $f(s, b\,\mathrm{gt}(\tau_2, \tau_1, \mathfrak{A})) \in \mathrm{States}_{b \nrightarrow \mathrm{false}_{\mathfrak{C}}}$(the generators of G), and

(ii) τ_1 value $\mathrm{at}(\mathfrak{C}, s) \leqslant \tau_2$ value $\mathrm{at}(\mathfrak{C}, s)$ iff $f(s, b\,\mathrm{leq}(\tau_1, \tau_2, \mathfrak{A})) \in \mathrm{States}_{b \nrightarrow \mathrm{false}_{\mathfrak{C}}}$(the generators of G), and

(iii) for every x, $f(s, b\,\mathrm{gt}(\tau_1, \tau_2, \mathfrak{A}))(I)(x) = s(I)(x)$ and $f(s, b\,\mathrm{leq}(\tau_1, \tau_2, \mathfrak{A}))(I)(x) = s(I)(x)$, and

(iv) for every pure element c of (the generators of $G)$((the boolean sort of Σ)) such that $c \neq b$ holds $f(s, b\,\mathrm{gt}(\tau_1, \tau_2, \mathfrak{A}))$((the boolean sort of Σ))$(c) = s$((the boolean sort of Σ))(c) and $f(s, b\,\mathrm{leq}(\tau_1, \tau_2, \mathfrak{A}))$ ((the boolean sort of Σ))$(c) = s$((the boolean sort of Σ))(c).

The theorem is a consequence of (31), (45), and (33).

Let i, j be real numbers and a, b be boolean sets. One can verify that $(i > j \to a, b)$ is boolean.

Now we state the proposition:

(67) Suppose G is $\mathfrak{C}$-supported and $f \in \mathfrak{C}$-$\mathrm{Execution}_{b \nrightarrow \mathrm{false}_{\mathfrak{C}}}(\mathfrak{A})$. Then

(i) $f(s, \tau\,\mathrm{is\ odd}(b, \mathfrak{A}))$((the boolean sort of Σ))$(b) = \tau$ value $\mathrm{at}(\mathfrak{C}, s) \bmod 2$, and

(ii) $f(s, \tau \text{ is even}(b, \mathfrak{A}))((\text{the boolean sort of } \Sigma))(b) = (\tau \text{ value at}(\mathfrak{C}, s) + 1) \bmod 2$, and

(iii) for every z, $f(s, \tau \text{ is odd}(b, \mathfrak{A}))(I)(z) = s(I)(z)$ and $f(s, \tau \text{ is even}(b, \mathfrak{A}))(I)(z) = s(I)(z)$.

The theorem is a consequence of (36), (40), (64), (31), (45), (44), and (1).

Let us consider Σ, X, $\mathfrak{T}$, G, and $\mathfrak{A}$. We say that $\mathfrak{A}$ is elementary if and only if

(Def. 13) rng the assignments of $\mathfrak{A} \subseteq \text{ElementaryInstructions}_{\mathfrak{A}}$.

Now we state the proposition:

(68) Suppose $\mathfrak{A}$ is elementary. Then let us consider a sort symbol a of Σ, an element x of (the generators of $G)(a)$, and an element τ of $\mathfrak{T}$ from a. Then $x{:=}_{\mathfrak{A}}\tau \in \text{ElementaryInstructions}_{\mathfrak{A}}$.

Let us consider Σ, X, $\mathfrak{T}$, and G. One can verify that there exists a strict if-while algebra over the generators of G which is elementary.

Let $\mathfrak{A}$ be an elementary if-while algebra over the generators of G, a be a sort symbol of Σ, x be an element of (the generators of $G)(a)$, and τ be an element of $\mathfrak{T}$ from a. Let us observe that $x{:=}_{\mathfrak{A}}\tau$ is absolutely-terminating.

Now let Γ denotes the program

```
y :=_𝔄 1^I_𝔗;
while b gt(@m, 0^I_𝔗, 𝔄) do
  if @m is odd(b, 𝔄) then
    y :=_𝔄 @y · @x
  fi;
  m :=_𝔄 @m div 2^I_𝔗;
  x :=_𝔄 @x · @x
done
```

Then we state the propositions:

(69) Let us consider an elementary if-while algebra $\mathfrak{A}$ over the generators of G and an execution function f of $\mathfrak{A}$ over $\mathfrak{C}$-States(the generators of G) and $\text{States}_{b \nrightarrow \text{false}_{\mathfrak{C}}}$(the generators of G). Suppose

(i) G is $\mathfrak{C}$-supported, and

(ii) $f \in \mathfrak{C}\text{-Execution}_{b \nrightarrow \text{false}_{\mathfrak{C}}}(\mathfrak{A})$, and

(iii) there exists a function d such that $d(x) = 1$ and $d(y) = 2$ and $d(m) = 3$.

Then Γ is terminating w.r.t. f and $\{s : s(I)(m) \geqslant 0\}$. The theorem is a consequence of (66), (36), (61), (65), (40), and (43). Proof: Set $ST = \mathfrak{C}$-States(the generators of G). Set $TV = \text{States}_{b \nrightarrow \text{false}_{\mathfrak{C}}}$(the generators of G). Set $P = \{s : s(I)(m) \geqslant 0\}$. Set $W = b\,\text{gt}(@m, 0^I_{\mathfrak{T}}, \mathfrak{A})$. Define $\mathcal{F}(\text{element of } ST) = \$_1(I)(m)(\in \mathbb{N})$. Define $\mathcal{R}[\text{element of } ST] \equiv \$_1(I)(m) >$

0. Set $K =$ if ${}^{@}m$ is odd$(b, \mathfrak{A})$ then$(y{:=}_{\mathfrak{A}}({}^{@}y \cdot {}^{@}x))$.
Set $J = (K; m{:=}_{\mathfrak{A}}({}^{@}m \operatorname{div} 2^{I}_{\mathfrak{T}})); x{:=}_{\mathfrak{A}}({}^{@}x \cdot {}^{@}x)$. P is invariant w.r.t. W and f. For every element s of ST such that $s \in P$ and $f(f(s, J), W) \in TV$ holds $f(s, J) \in P$. P is invariant w.r.t. $y{:=}_{\mathfrak{A}}(1^{I}_{\mathfrak{T}})$ and f. For every s such that $f(s, W) \in P$ holds iteration of f started in $J; W$ terminates w.r.t. $f(s, W)$. □

(70) Suppose G is $\mathfrak{C}$-supported and there exists a function d such that $d(b) = 0$ and $d(x) = 1$ and $d(y) = 2$ and $d(m) = 3$. Then let us consider an element s of $\mathfrak{C}$-States(the generators of G) and a natural number n. Suppose $n = s(I)(m)$. If $f \in \mathfrak{C}$-Execution$_{b \nrightarrow \text{false}_{\mathfrak{C}}}(\mathfrak{A})$, then $f(s, \Gamma)(I)(y) = s(I)(x)^n$. The theorem is a consequence of (65), (66), (36), (61), (37), (40), (43), (67), (10), and (42). PROOF: Set $\Sigma = \mathfrak{C}$-States(the generators of G). Set $W = \mathfrak{T}$. Set $g = f$. Set $\mathfrak{T} =$ States$_{b \nrightarrow \text{false}_{\mathfrak{C}}}$(the generators of G). Set $s0 = f(s, y{:=}_{\mathfrak{A}}(1^{I}_{W}))$. Define $\mathcal{R}$[element of Σ] $\equiv \$_1(I)(m) > 0$. Set $\mathfrak{C} = b\,\mathrm{gt}({}^{@}m, 0^{I}_{W}, \mathfrak{A})$. Define $\mathcal{P}$[element of Σ] $\equiv s(I)(x)^n = \$_1(I)(y) \cdot \$_1(I)(x)^{\$_1(I)(m)}$ and $\$_1(I)(m) \geqslant 0$. Define $\mathcal{F}$(element of Σ) $= \$_1(I)(m) (\in \mathbb{N})$. Set $I =$ if ${}^{@}m$ is odd$(b, \mathfrak{A})$ then$(y{:=}_{\mathfrak{A}}({}^{@}y \cdot {}^{@}x))$.
Set $J = (I; m{:=}_{\mathfrak{A}}({}^{@}m \operatorname{div} 2^{Y}_{W})); x{:=}_{\mathfrak{A}}({}^{@}x \cdot {}^{@}x)$. For every element s of Σ such that $\mathcal{P}[s]$ holds $\mathcal{P}[(g(s, \mathfrak{C})$ **qua** element of $\Sigma)]$ and $g(s, \mathfrak{C}) \in \mathfrak{T}$ iff $\mathcal{R}[(g(s, \mathfrak{C})$ **qua** element of $\Sigma)]$. Set $s_1 = g(s0, \mathfrak{C})$. For every element s of Σ such that $\mathcal{R}[s]$ holds $\mathcal{R}[(g(s, J; \mathfrak{C})$ **qua** element of $\Sigma)]$ iff $g(s, J; \mathfrak{C}) \in \mathfrak{T}$ and $\mathcal{F}((g(s, J; \mathfrak{C})$ **qua** element of $\Sigma)) < \mathcal{F}(s)$. Set $q = s$. For every element s of Σ such that $\mathcal{P}[s]$ and $s \in \mathfrak{T}$ and $\mathcal{R}[s]$ holds $\mathcal{P}[(g(s, J)$ **qua** element of $\Sigma)]$. □

2. CALCULATION OF MAXIMUM

Let X be a non empty set, f be a finite sequence of elements of X^ω, and x be a natural number. Let us observe that $f(x)$ is transfinite sequence-like finite function-like and relation-like.

Let us note that every finite sequence of elements of X^ω is function yielding.

Let i be a natural number, f be an i-based finite array, and a, x be sets. Note that $f +\cdot (a, x)$ is i-based finite and segmental.

Let X be a non empty set, f be an X-valued function, a be a set, and x be an element of X. Let us observe that $f +\cdot (a, x)$ is X-valued.

The scheme *Sch1* deals with a non empty set $\mathcal{X}$ and a natural number j and a set $\mathfrak{B}$ and a ternary functor $\mathcal{F}$ yielding a set and a unary functor $\mathfrak{A}$ yielding a set and states that

(Sch. 1) There exists a finite sequence f of elements of $\mathcal{X}^\omega$ such that $\operatorname{len} f = j$ and $f(1) = \mathfrak{B}$ or $j = 0$ and for every natural number i such that $1 \leqslant i < j$ holds $f(i + 1) = \mathcal{F}(f(i), i, \mathfrak{A}(i))$

provided

- for every 0-based finite array a of $\mathcal{X}$ and for every natural number i such that $1 \leqslant i < j$ for every element x of $\mathcal{X}$, $\mathcal{F}(a, i, x)$ is a 0-based finite array of $\mathcal{X}$ and
- $\mathfrak{B}$ is a 0-based finite array of $\mathcal{X}$ and
- for every natural number i such that $i < j$ holds $\mathfrak{A}(i) \in \mathcal{X}$.

Now we state the propositions:

(71) Let us consider a non empty non void boolean signature Σ with arrays of type 1 with connectives from 11 and integers at 1, sets J, L, and a sort symbol K of Σ. Suppose (the connectives of Σ)(11) is of type $\langle J, L\rangle \to K$. Then

(i) $J =$ the array sort of Σ, and

(ii) for every integer sort symbol I of Σ, the array sort of $\Sigma \neq I$.

(72) Let us consider a 1-1-connectives 11-array correct boolean correct non empty non void boolean signature Σ with integers with connectives from 4 and the sort at 1 and arrays of type 1 with connectives from 11 and integers at 1, an integer sort symbol I of Σ, a boolean correct non-empty algebra $\mathfrak{A}$ over Σ with integers with connectives from 4 and the sort at 1 and arrays of type 1 with connectives from 11 and integers at 1, and elements a, b of $\mathfrak{A}$ from I. If $a = 0$, then init.array$(a, b) = \emptyset$.

(73) Let us consider an 11-array correct boolean correct non empty non void boolean signature Σ with arrays of type 1 with connectives from 11 and integers at 1 and an integer sort symbol I of Σ. Then

(i) the array sort of $\Sigma \neq I$, and

(ii) (the connectives of Σ)(11) is of type $\langle$the array sort of $\Sigma, I\rangle \to I$, and

(iii) (the connectives of Σ)$(11 + 1)$ is of type $\langle$the array sort of $\Sigma, I, I\rangle \to$ the array sort of Σ, and

(iv) (the connectives of Σ)$(11 + 2)$ is of type $\langle$the array sort of $\Sigma\rangle \to I$, and

(v) (the connectives of Σ)$(11 + 3)$ is of type $\langle I, I\rangle \to$ the array sort of Σ.

(74) Let us consider a 1-1-connectives 11-array correct boolean correct non empty non void boolean signature Σ with arrays of type 1 with connectives from 11 and integers at 1 and integers with connectives from 4 and the sort at 1, an integer sort symbol I of Σ, and a boolean correct non-empty algebra $\mathfrak{A}$ over Σ with arrays of type 1 with connectives from 11 and integers at 1 and integers with connectives from 4 and the sort at 1. Then

(i) (the sorts of $\mathfrak{A}$)(the array sort of Σ) $= \mathbb{Z}^{\omega}$, and

(ii) for every elements i, j of $\mathfrak{A}$ from I such that i is a non negative integer holds $\mathrm{init.array}(i, j) = i \longmapsto j$, and

(iii) for every element a of (the sorts of $\mathfrak{A}$)(the array sort of Σ), $\mathrm{length}_I\, a = \overline{\overline{a}}$ and for every element i of $\mathfrak{A}$ from I and for every function f such that $f = a$ and $i \in \mathrm{dom}\, f$ holds $a(i) = f(i)$ and for every element x of $\mathfrak{A}$ from I, $a_{i \leftarrow x} = f +\cdot (i, x)$.

The theorem is a consequence of (71).

Let a be a 0-based finite array. Observe that $\mathrm{length}\, a$ is finite.

Let Σ be a 1-1-connectives 11-array correct boolean correct non empty non void boolean signature with integers with connectives from 4 and the sort at 1 and arrays of type 1 with connectives from 11 and integers at 1 and $\mathfrak{A}$ be a boolean correct non-empty algebra over Σ with arrays of type 1 with connectives from 11 and integers at 1 and integers with connectives from 4 and the sort at 1. Observe that every non-empty subalgebra of $\mathfrak{A}$ has arrays of type 1 with connectives from 11 and integers at 1.

Let $\mathfrak{A}$ be a non-empty algebra over Σ. We say that $\mathfrak{A}$ is integer array if and only if

(Def. 14) There exists an image $\mathfrak{C}$ of $\mathfrak{A}$ such that $\mathfrak{C}$ is a boolean correct algebra over Σ with integers with connectives from 4 and the sort at 1 and arrays of type 1 with connectives from 11 and integers at 1.

Let X be a non-empty many sorted set indexed by the carrier of Σ. One can verify that $\mathfrak{F}_\Sigma(X)$ is integer array as a non-empty algebra over Σ.

Note that every non-empty algebra over Σ which is integer array is also integer.

One can check that there exists an including Σ-terms over X non-empty strict free variable algebra over Σ which is vf-free and integer array.

One can check that there exists a non-empty algebra over Σ which is integer array.

Let $\mathfrak{A}$ be an integer array non-empty algebra over Σ. Observe that there exists a boolean correct image of $\mathfrak{A}$ which has integers with connectives from 4 and the sort at 1 and arrays of type 1 with connectives from 11 and integers at 1.

In this paper Σ denotes a 1-1-connectives 11-array correct boolean correct non empty non void boolean signature with integers with connectives from 4 and the sort at 1 and arrays of type 1 with connectives from 11 and integers at 1, X denotes a non-empty many sorted set indexed by the carrier of Σ, $\mathfrak{T}$ denotes a vf-free including Σ-terms over X integer array non-empty free variable algebra over Σ, $\mathfrak{C}$ denotes a boolean correct non-empty image of $\mathfrak{T}$ with arrays of type 1 with connectives from 11 and integers at 1 and integers with connectives from 4 and the sort at 1, G denotes a basic generator system over Σ, X, and $\mathfrak{T}$, $\mathfrak{A}$ denotes a if-while algebra over the generators of G, I denotes an integer sort symbol of Σ, x, y, m, i denote pure elements of (the generators of G)(I), M, N

denote pure elements of (the generators of G)(the array sort of Σ), b denotes a pure element of (the generators of G)((the boolean sort of Σ)), and s, s_1 denote elements of $\mathfrak{C}$-States(the generators of G).

Let us consider Σ. Let $\mathfrak{A}$ be a boolean correct non-empty algebra over Σ with arrays of type 1 with connectives from 11 and integers at 1. Observe that every element of (the sorts of $\mathfrak{A}$)(the array sort of Σ) is relation-like and function-like.

Note that every element of (the sorts of $\mathfrak{A}$)(the array sort of Σ) is finite and transfinite sequence-like.

Let us consider an operation symbol o of Σ. Now we state the propositions:

(75) Suppose $o =$ (the connectives of Σ)(11)($\in$ (the carrier' of Σ)). Then
  (i) Arity$(o) = \langle$the array sort of $\Sigma, I\rangle$, and
  (ii) the result sort of $o = I$.

(76) Suppose $o =$ (the connectives of Σ)(12)($\in$ (the carrier' of Σ)). Then
  (i) Arity$(o) = \langle$the array sort of $\Sigma, I, I\rangle$, and
  (ii) the result sort of $o =$ the array sort of Σ.

(77) Suppose $o =$ (the connectives of Σ)(13)($\in$ (the carrier' of Σ)). Then
  (i) Arity$(o) = \langle$the array sort of $\Sigma\rangle$, and
  (ii) the result sort of $o = I$.

(78) Suppose $o =$ (the connectives of Σ)(14)($\in$ (the carrier' of Σ)). Then
  (i) Arity$(o) = \langle I, I\rangle$, and
  (ii) the result sort of $o =$ the array sort of Σ.

(79) Let us consider an element τ of $\mathfrak{T}$ from the array sort of Σ and an element τ_1 of $\mathfrak{T}$ from I.
Then $\tau(\tau_1)$ value at$(\mathfrak{C}, s) = (\tau$ value at$(\mathfrak{C}, s))(\tau_1$ value at$(\mathfrak{C}, s))$. The theorem is a consequence of (29), (75), (23), and (26).

(80) Let us consider an element τ of $\mathfrak{T}$ from the array sort of Σ and elements τ_1, τ_2 of $\mathfrak{T}$ from I. Then $\tau_{\tau_1 \leftarrow \tau_2}$ value at$(\mathfrak{C}, s) =$
$(\tau$ value at$(\mathfrak{C}, s))_{\tau_1 \text{ value at}(\mathfrak{C},s) \leftarrow \tau_2 \text{ value at}(\mathfrak{C},s)}$. The theorem is a consequence of (29), (76), (24), and (27).

(81) Let us consider an element τ of $\mathfrak{T}$ from the array sort of Σ. Then length$_I\,\tau$ value at$(\mathfrak{C}, s) =$ length$_I(\tau$ value at$(\mathfrak{C}, s))$. The theorem is a consequence of (29), (77), (22), and (25).

(82) Let us consider elements τ_1, τ_2 of $\mathfrak{T}$ from I. Then init.array(τ_1, τ_2) value at$(\mathfrak{C}, s) =$ init.array$(\tau_1$ value at$(\mathfrak{C}, s), \tau_2$ value at$(\mathfrak{C}, s))$. The theorem is a consequence of (29), (78), (23), and (26).

In the sequel u denotes a many sorted function from FreeGenerator$(\mathfrak{T})$ into the sorts of $\mathfrak{C}$.

Now we state the propositions:

(83) Let us consider an element τ of $\mathfrak{T}$ from the array sort of Σ and an element τ_1 of $\mathfrak{T}$ from I.
Then $\tau(\tau_1)$ value at$(\mathfrak{C}, u) = (\tau$ value at$(\mathfrak{C}, u))(\tau_1$ value at$(\mathfrak{C}, u))$. The theorem is a consequence of (28), (75), (23), and (26).

(84) Let us consider an element τ of $\mathfrak{T}$ from the array sort of Σ and elements τ_1, τ_2 of $\mathfrak{T}$ from I.
Then $\tau_{\tau_1 \leftarrow \tau_2}$ value at$(\mathfrak{C}, u) = (\tau$ value at$(\mathfrak{C}, u))_{\tau_1 \text{ value at}(\mathfrak{C},u) \leftarrow \tau_2 \text{ value at}(\mathfrak{C},u)}$. The theorem is a consequence of (28), (76), (24), and (27).

(85) Let us consider an element τ of $\mathfrak{T}$ from the array sort of Σ. Then length$_I \tau$ value at$(\mathfrak{C}, u) =$ length$_I(\tau$ value at$(\mathfrak{C}, u))$. The theorem is a consequence of (28), (77), (22), and (25).

(86) Let us consider elements τ_1, τ_2 of $\mathfrak{T}$ from I. Then init.array(τ_1, τ_2) value at$(\mathfrak{C}, u) =$ init.array$(\tau_1$ value at$(\mathfrak{C}, u), \tau_2$ value at$(\mathfrak{C}, u))$. The theorem is a consequence of (28), (78), (23), and (26).

Let us consider Σ, X, $\mathfrak{T}$, and I. Let i be an integer. The functor $i^I_{\mathfrak{T}}$ yielding an element of $\mathfrak{T}$ from I is defined by

(Def. 15) There exists a function f from $\mathbb{Z}$ into (the sorts of $\mathfrak{T})(I)$ such that

(i) $it = f(i)$, and

(ii) $f(0) = 0^I_{\mathfrak{T}}$, and

(iii) for every natural number j and for every element τ of $\mathfrak{T}$ from I such that $f(j) = \tau$ holds $f(j+1) = \tau + 1^I_{\mathfrak{T}}$ and $f(-(j+1)) = -(\tau + 1^I_{\mathfrak{T}})$.

Now we state the propositions:

(87) $0^I_{\mathfrak{T}} = 0^I_{\mathfrak{T}}$.

(88) Let us consider a natural number n. Then

(i) $(n+1)^I_{\mathfrak{T}} = n^I_{\mathfrak{T}} + 1^I_{\mathfrak{T}}$, and

(ii) $-(n+1)^I_{\mathfrak{T}} = -(n+1)^I_{\mathfrak{T}}$.

(89) $1^I_{\mathfrak{T}} = 0^I_{\mathfrak{T}} + 1^I_{\mathfrak{T}}$. The theorem is a consequence of (88) and (87).

(90) Let us consider an integer i. Then $i^I_{\mathfrak{T}}$ value at$(\mathfrak{C}, s) = i$. The theorem is a consequence of (87), (36), (37), (88), (39), and (38).

Let us consider Σ, X, $\mathfrak{T}$, G, I, and M. Let i be an integer. The functor $M(i, I)$ yielding an element of $\mathfrak{T}$ from I is defined by the term

(Def. 16) $({}^{@}M)(i^I_{\mathfrak{T}})$.

Let us consider $\mathfrak{C}$ and s. Note that s(the array sort of $\Sigma)(M)$ is function-like and relation-like.

Note that s(the array sort of $\Sigma)(M)$ is finite transfinite sequence-like and $\mathbb{Z}$-valued.

Observe that rng(s(the array sort of $\Sigma)(M)$) is finite and integer-membered.

Let us consider an integer j. Now we state the propositions:

(91) Suppose $j \in \mathrm{dom}(s(\text{the array sort of } \Sigma)(M))$ and $M(j, I) \in (\text{the generators of } G)(I)$. Then $s(\text{the array sort of } \Sigma)(M)(j) = s(I)(M(j, I))$.

(92) Suppose $j \in \mathrm{dom}(s(\text{the array sort of } \Sigma)(M))$ and $({}^{@}M)({}^{@}i) \in (\text{the generators of } G)(I)$ and $j = {}^{@}i \text{ value at}(\mathfrak{C}, s)$. Then $(s(\text{the array sort of } \Sigma)(M))({}^{@}i \text{ value at}(\mathfrak{C}, s)) = s(I)(((({}^{@}M)({}^{@}i)))$.

Let X be a non empty set. One can verify that X^ω is infinite.

Now we state the propositions:

(93) Now let Γ denotes the program

```
m :=_𝔄 0^I_𝔛;
for i :=_𝔄 1^I_𝔛 until b gt(length_I @M, @i, 𝔄) step i :=_𝔄 @i + 1^I_𝔛
do
  if b gt((@M)(@i), (@M)(@m), 𝔄) then
    m :=_𝔄 @i
  fi
done
```

Let us consider an execution function f of $\mathfrak{A}$ over $\mathfrak{C}$-States(the generators of G) and $\mathrm{States}_{b \nrightarrow \mathrm{false}_{\mathfrak{C}}}(\text{the generators of } G)$. Suppose

(i) $f \in \mathfrak{C}\text{-Execution}_{b \nrightarrow \mathrm{false}_{\mathfrak{C}}}(\mathfrak{A})$, and

(ii) G is $\mathfrak{C}$-supported, and

(iii) $i \neq m$, and

(iv) $s(\text{the array sort of } \Sigma)(M) \neq \emptyset$.

Let us consider a natural number n. Suppose $f(s, \Gamma)(I)(m) = n$. Let us consider a non empty finite integer-membered set X. Suppose $X = \mathrm{rng}(s(\text{the array sort of } \Sigma)(M))$. Then $M(n, I) \text{ value at}(\mathfrak{C}, s) = \max X$. The theorem is a consequence of (65), (36), (37), (74), (71), (66), (81), (61), (39), (79), and (90). Proof: Set $ST = \mathfrak{C}$-States(the generators of G). Define $\mathcal{R}[\text{element of } ST] \equiv s(\text{the array sort of } \Sigma)(M) = \$_1(\text{the array sort of } \Sigma)(M)$. Reconsider $sm = s$ as a many sorted function from the generators of G into the sorts of $\mathfrak{C}$. Reconsider $z = sm(\text{the array sort of } \Sigma)(M)$ as a 0-based finite array of $\mathbb{Z}$. Define $\mathcal{P}[\text{element of } ST] \equiv \mathcal{R}[\$_1]$ and $\$_1(I)(i), \$_1(I)(m) \in \mathbb{N}$ and $\$_1(I)(i) \leqslant \mathrm{len}\, z$ and $\$_1(I)(m) < \$_1(I)(i)$ and $\$_1(I)(m) < \mathrm{len}\, z$ and for every integer mx such that $mx = \$_1(I)(m)$ for every natural number j such that $j < \$_1(I)(i)$ holds $z(j) \leqslant z(mx)$. Define $\mathcal{Q}[\text{element of } ST] \equiv \mathcal{R}[\$_1]$ and $\$_1(I)(i) < \mathrm{length}_I {}^{@}M \text{ value at}(\mathfrak{C}, s)$. Set $s0 = s$. Set $s_1 = f(s, m{:=}_{\mathfrak{A}}(0^I_{\mathfrak{T}}))$. Set $s_2 = f(s_1, i{:=}_{\mathfrak{A}}(1^I_{\mathfrak{T}}))$. Consider $J1$, $K1$, $L1$ being elements of Σ such that $L1 = 1$ and $K1 = 1$ and $J1 \neq L1$ and $J1 \neq K1$ and (the connectives of Σ)(11) is of type $\langle J1, K1\rangle \to L1$ and (the connectives of Σ)$(11 + 1)$ is of type $\langle J1, K1, L1\rangle \to J1$ and (the connectives of Σ)$(11 + 2)$ is of type $\langle J1\rangle \to K1$ and

(the connectives of Σ)$(11 + 3)$ is of type $\langle K1, L1\rangle \to J1$. $\mathcal{P}[s_2]$. Define $\mathcal{F}$(element of ST) = (len($s0$(the array sort of Σ)(M)) − $\$_1(I)(i)$)$(\in \mathbb{N})$. $f(s_2, W) \in TV$ iff $\mathcal{Q}[f(s_2, W)]$. Now let Γ denotes the program

J;
K;
W

For every element s of ST such that $\mathcal{Q}[s]$ holds $\mathcal{Q}[f(s, \Gamma)]$ iff $f(s, \Gamma) \in TV$ and $\mathcal{F}(f(s, \Gamma)) < \mathcal{F}(s)$. For every element s of ST such that $\mathcal{P}[s]$ and $s \in TV$ and $\mathcal{Q}[s]$ holds $\mathcal{P}[f(s, J; K)]$. For every element s of ST such that $\mathcal{P}[s]$ holds $\mathcal{P}[f(s, W)]$ and $f(s, W) \in TV$ iff $\mathcal{Q}[f(s, W)]$. $M(n, I)$ value at$(\mathfrak{C}, s)$ is a upper bound of X. For every upper bound x of X, $M(n, I)$ value at$(\mathfrak{C}, s) \leqslant x$. □

(94) Now let Γ denotes the program

J;
$i :=_{\mathfrak{A}}{}^{@}i + 1^I_{\mathfrak{T}}$

Now let Δ denotes the program

`for` $i :=_{\mathfrak{A}} \tau_0$ `until` $b\,\mathrm{gt}(\tau_1, {}^{@}i, \mathfrak{A})$ `step` $i :=_{\mathfrak{A}}{}^{@}i + 1^I_{\mathfrak{T}}$ `do`
J
`done`

Let us consider an elementary if-while algebra $\mathfrak{A}$ over the generators of G and an execution function f of $\mathfrak{A}$ over $\mathfrak{C}$-States(the generators of G) and States$_{b \nrightarrow \mathrm{false}_{\mathfrak{C}}}$(the generators of G). Suppose

(i) $f \in \mathfrak{C}$-Execution$_{b \nrightarrow \mathrm{false}_{\mathfrak{C}}}(\mathfrak{A})$, and

(ii) G is $\mathfrak{C}$-supported.

Let us consider elements τ_0, τ_1 of $\mathfrak{T}$ from I, an algorithm J of $\mathfrak{A}$, and a set P. Suppose

(iii) P is invariant w.r.t. $i :=_{\mathfrak{A}} \tau_0$ and f, invariant w.r.t. $b\,\mathrm{gt}(\tau_1, {}^{@}i, \mathfrak{A})$ and f, invariant w.r.t. $i :=_{\mathfrak{A}} ({}^{@}i + 1^I_{\mathfrak{T}})$ and f, and invariant w.r.t. J and f, and

(iv) J is terminating w.r.t. f and P, and

(v) for every s, $f(s, J)(I)(i) = s(I)(i)$ and $f(s, b\,\mathrm{gt}(\tau_1, {}^{@}i, \mathfrak{A}))(I)(i) = s(I)(i)$ and τ_1 value at$(\mathfrak{C}, f(s, b\,\mathrm{gt}(\tau_1, {}^{@}i, \mathfrak{A}))) = \tau_1$ value at$(\mathfrak{C}, s)$ and τ_1 value at$(\mathfrak{C}, f(s, \Gamma)) = \tau_1$ value at$(\mathfrak{C}, s)$.

Then Δ is terminating w.r.t. f and P. The theorem is a consequence of (61), (66), (65), (39), and (37). PROOF: Set $W = b\,\mathrm{gt}(\tau_1, {}^{@}i, \mathfrak{A})$. Set $L = i :=_{\mathfrak{A}} ({}^{@}i + 1^I_{\mathfrak{T}})$. Set $K = i :=_{\mathfrak{A}} \tau_0$. Set $ST = \mathfrak{C}$-States(the generators of G). Set TV = States$_{b \nrightarrow \mathrm{false}_{\mathfrak{C}}}$(the generators of G). Now let Γ denotes the program

J;
L;
W

For every s such that $f(s, W) \in P$ holds iteration of f started in Γ terminates w.r.t. $f(s, W)$. □

(95) Now let Γ denotes the program

m :=$_{\mathfrak{A}}0^I_{\mathfrak{T}}$;
for i :=$_{\mathfrak{A}}1^I_{\mathfrak{T}}$ until $b\,\mathrm{gt}(\mathrm{length}_I\,{}^{@}M, {}^{@}i, \mathfrak{A})$ step i :=$_{\mathfrak{A}}{}^{@}i + 1^I_{\mathfrak{T}}$
do
  if $b\,\mathrm{gt}(({}^{@}M)({}^{@}i), ({}^{@}M)({}^{@}m), \mathfrak{A})$ then
    m :=$_{\mathfrak{A}}{}^{@}i$
  fi
done

Let us consider an elementary if-while algebra $\mathfrak{A}$ over the generators of G and an execution function f of $\mathfrak{A}$ over $\mathfrak{C}$-States(the generators of G) and $\mathrm{States}_{b \nrightarrow \mathrm{false}_{\mathfrak{C}}}$(the generators of G). Suppose

(i) $f \in \mathfrak{C}\text{-Execution}_{b \nrightarrow \mathrm{false}_{\mathfrak{C}}}(\mathfrak{A})$, and

(ii) G is $\mathfrak{C}$-supported, and

(iii) $i \neq m$.

Then Γ is terminating w.r.t. f and $\{s : s(\text{the array sort of } \Sigma)(M) \neq \emptyset\}$. The theorem is a consequence of (74), (73), (65), (61), (81), and (94). Proof: Set $J = m{:=}_{\mathfrak{A}}(0^I_{\mathfrak{T}})$. Set $K = i{:=}_{\mathfrak{A}}(1^I_{\mathfrak{T}})$. Set $W = b\,\mathrm{gt}(\mathrm{length}_I\,{}^{@}M, {}^{@}i, \mathfrak{A})$. Set $L = i{:=}_{\mathfrak{A}}({}^{@}i + 1^I_{\mathfrak{T}})$. Set $N = b\,\mathrm{gt}(({}^{@}M)({}^{@}i), ({}^{@}M)({}^{@}m), \mathfrak{A})$. Set $O = m{:=}_{\mathfrak{A}}({}^{@}i)$. Set $a =$ the array sort of Σ. Set $P = \{s : s(a)(M) \neq \emptyset\}$. P is invariant w.r.t. J and f. P is invariant w.r.t. K and f. P is invariant w.r.t. W and f. P is invariant w.r.t. L and f. P is invariant w.r.t. N and f. P is invariant w.r.t. O and f. Set $ST = \mathfrak{C}$-States(the generators of G). Set $TV = \mathrm{States}_{b \nrightarrow \mathrm{false}_{\mathfrak{C}}}$(the generators of G). P is invariant w.r.t. if N then O and f. Now let Γ denotes the program

if N then
  O
fi;
L

For every s, $f(s, \text{if } N \text{ then } O)(I)(i) = s(I)(i)$ and $f(s, W)(I)(i) = s(I)(i)$ and $\mathrm{length}_I\,{}^{@}M$ value at$(\mathfrak{C}, f(s, W)) = \mathrm{length}_I\,{}^{@}M$ value at$(\mathfrak{C}, s)$ and $\mathrm{length}_I\,{}^{@}M$ value at$(\mathfrak{C}, f(s, \Gamma)) = \mathrm{length}_I\,{}^{@}M$ value at$(\mathfrak{C}, s)$. □

3. SORTING BY EXCHANGING

In this paper i_1, i_2 denote pure elements of (the generators of G)(I).

Let us consider Σ, X, $\mathfrak{T}$, and G. We say that G is integer array if and only if

(Def. 17) (i) $\{({}^{@}M)(\tau)$ where τ is an element of $\mathfrak{T}$ from I : not contradiction$\} \subseteq$ (the generators of G)(I), and

(ii) for every M and for every element τ of $\mathfrak{T}$ from I and for every element g of G from I such that $g = ({}^{@}M)(\tau)$ there exists x such that $x \notin (\mathrm{vf}\,\tau)(I)$ and supp-var $g = x$ and (supp-term g)(the array sort of Σ)$(M) = ({}^{@}M)_{\tau \leftarrow {}^{@}x}$ and for every sort symbol s of Σ and for every y such that $y \in (\mathrm{vf}\,g)(s)$ and if $s =$ the array sort of Σ, then $y \neq M$ holds (supp-term g)$(s)(y) = y$.

Now we state the proposition:

(96) If G is integer array, then for every element τ of $\mathfrak{T}$ from I, $({}^{@}M)(\tau) \in$ (the generators of G)(I).

The functor $\langle \mathbb{Z}, \leqslant \rangle$ yielding a strict real non empty poset is defined by the term

(Def. 18) RealPoset $\mathbb{Z}$.

Let us consider Σ, X, $\mathfrak{T}$, and G. Let $\mathfrak{A}$ be an elementary if-while algebra over the generators of G, a be a sort symbol of Σ, and τ_1, τ_2 be elements of $\mathfrak{T}$ from a. Assume $\tau_1 \in$ (the generators of G)(a). The functor $\tau_1 :=_{\mathfrak{A}} \tau_2$ yielding an absolutely-terminating algorithm of $\mathfrak{A}$ is defined by the term

(Def. 19) (The assignments of $\mathfrak{A}$)$(\langle \tau_1, \tau_2 \rangle)$.

Now we state the proposition:

(97) Let us consider a countable non-empty many sorted set X indexed by the carrier of Σ, a vf-free including Σ-terms over X integer array non-empty free variable algebra $\mathfrak{T}$ over Σ, a basic generator system G over Σ, X, and $\mathfrak{T}$, a pure element M of (the generators of G)(the array sort of Σ), and pure elements i, x of (the generators of G)(I). Then $({}^{@}M)({}^{@}i) \neq x$. The theorem is a consequence of (73), (79), (61), and (74).

Let Σ be a non empty non void many sorted signature and $\mathfrak{A}$ be a disjoint valued algebra over Σ. Note that the sorts of $\mathfrak{A}$ is disjoint valued.

Let us consider Σ and X. Let $\mathfrak{T}$ be an including Σ-terms over X algebra over Σ. We say that $\mathfrak{T}$ is array degenerated if and only if

(Def. 20) There exists I and there exists an element M of (FreeGenerator($\mathfrak{T}$))(the array sort of Σ) and there exists an element τ of $\mathfrak{T}$ from I such that $({}^{@}M)(\tau) \neq \mathrm{Sym}((\text{the connectives of } \Sigma)(11)(\in (\text{the carrier' of } \Sigma)), X)\text{-tree}(\langle M, \tau \rangle)$.

Observe that $\mathfrak{F}_\Sigma(X)$ is non array degenerated.

Observe that there exists an including Σ-terms over X algebra over Σ which is non array degenerated.

Now we state the propositions:

(98) Suppose $\mathfrak{T}$ is non array degenerated. Then $\mathrm{vf}((^{@}M)(^{@}i)) = I$-singleton $i \cup$ (the array sort of Σ)-singleton M. The theorem is a consequence of (73). Proof: Set $\tau = (^{@}M)(^{@}i)$. Reconsider $N = M$ as an element of (FreeGenerator($\mathfrak{T}$))(the array sort of Σ). Consider m being a set such that $m \in X$(the array sort of Σ) and $M =$ the root tree of $\langle m$, the array sort of $\Sigma\rangle$. Consider j being a set such that $j \in X(I)$ and $i =$ the root tree of $\langle j, I\rangle$. $\{M\} = (\mathrm{vf}\,\tau)$(the array sort of Σ). $\{i\} = (\mathrm{vf}\,\tau)(I)$. For every sort symbol s of Σ such that $s \neq$ the array sort of Σ and $s \neq I$ holds $\emptyset = (\mathrm{vf}\,\tau)(s)$. $\square$

(99) Let us consider an elementary if-while algebra $\mathfrak{A}$ over the generators of G and an execution function f of $\mathfrak{A}$ over $\mathfrak{C}$-States(the generators of G) and $\mathrm{States}_{b \not\to \mathrm{false}_{\mathfrak{C}}}$(the generators of G). Suppose

(i) G is integer array and $\mathfrak{C}$-supported, and

(ii) $f \in \mathfrak{C}$-$\mathrm{Execution}_{b \not\to \mathrm{false}_{\mathfrak{C}}}(\mathfrak{A})$, and

(iii) X is countable, and

(iv) $\mathfrak{T}$ is non array degenerated.

Let us consider an element τ of $\mathfrak{T}$ from I. Then $f(s, (^{@}M)(^{@}i) :=_{\mathfrak{A}} \tau) = f(s, M :=_{\mathfrak{A}} ((^{@}M)_{@i \leftarrow \tau}))$. The theorem is a consequence of (96), (98), (97), (4), (3), (62), (73), (61), (84), (65), and (80). Proof: Reconsider $H =$ FreeGenerator($\mathfrak{T}$) as a many sorted subset of the generators of G. Set $v = \tau$ value at$(\mathfrak{C}, s)$. Reconsider $p = (^{@}M)(^{@}i)$ as an element of G from I. Reconsider $g = s$ as a many sorted function from the generators of G into the sorts of $\mathfrak{C}$. Reconsider $g1 = f(s, (^{@}M)(^{@}i) :=_{\mathfrak{A}} \tau)$, $g2 = f(s, M :=_{\mathfrak{A}} ((^{@}M)_{@i \leftarrow \tau}))$ as a many sorted function from the generators of G into the sorts of $\mathfrak{C}$. Reconsider $Mi = (^{@}M)(^{@}i)$ as an element of (the generators of G)(I). Reconsider $m = M$ as an element of G from the array sort of Σ. Consider x such that $x \notin (\mathrm{vf}\,{}^{@}i)(I)$ and supp-var $p = x$ and (supp-term p)(the array sort of Σ)$(M) = (^{@}M)_{@i \leftarrow @x}$ and for every sort symbol s of Σ and for every y such that $y \in (\mathrm{vf}\,p)(s)$ and if $s =$ the array sort of Σ, then $y \neq M$ holds (supp-term p)$(s)(y) = y$. $g1 = g2$. $\square$

Let us consider Σ, X, $\mathfrak{T}$, G, $\mathfrak{C}$, s, and b. Let us observe that s((the boolean sort of Σ))(b) is boolean.

Now we state the proposition:

(100) Now let Γ denotes the program

```
while J do
  y :=𝔄(@M)(@i1);
  (@M)(@i1) :=𝔄(@M)(@i2);
  (@M)(@i2) :=𝔄@y
done
```

Let us consider an elementary if-while algebra $\mathfrak{A}$ over the generators of G and an execution function f of $\mathfrak{A}$ over $\mathfrak{C}$-States(the generators of G) and $\mathrm{States}_{b \nrightarrow \mathrm{false}_{\mathfrak{C}}}$(the generators of G). Suppose

(i) G is integer array and $\mathfrak{C}$-supported, and

(ii) $f \in \mathfrak{C}\text{-}\mathrm{Execution}_{b \nrightarrow \mathrm{false}_{\mathfrak{C}}}(\mathfrak{A})$, and

(iii) $\mathfrak{T}$ is non array degenerated, and

(iv) X is countable.

Let us consider an algorithm J of $\mathfrak{A}$. Suppose

(v) $f(s, J)$(the array sort of Σ)$(M) = s$(the array sort of Σ)(M), and

(vi) for every array D of $\langle \mathbb{Z}, \leqslant \rangle$ such that $D = s$(the array sort of Σ)(M) holds if $D \neq \emptyset$, then $f(s, J)(I)(i_1)$, $f(s, J)(I)(i_2) \in \operatorname{dom} D$ and if inversions $D \neq \emptyset$, then $\langle f(s, J)(I)(i_1), f(s, J)(I)(i_2) \rangle \in$ inversions D and $f(s, J)$((the boolean sort of Σ))$(b) = \mathit{true}$ iff inversions $D \neq \emptyset$.

Let us consider a 0-based finite array D of $\langle \mathbb{Z}, \leqslant \rangle$. Suppose

(vii) $D = s$(the array sort of Σ)(M), and

(viii) $y \neq i_1$, and

(ix) $y \neq i_2$.

Then

(x) $f(s, \Gamma)$(the array sort of Σ)(M) is an ascending permutation of D, and

(xi) if J is absolutely-terminating, then Γ is terminating w.r.t. f and $\{s_1 : s_1$(the array sort of Σ)$(M) \neq \emptyset\}$.

The theorem is a consequence of (73), (10), (61), (65), (99), (80), (74), and (79). PROOF: Define $\mathcal{F}$(natural number, element of $\mathfrak{C}$-States(the generators of G)) $= f(\$_2, ((J; y{:=}\mathfrak{A}((@M)(@i_1))); (@M)(@i_1){:=}\mathfrak{A}((@M)(@i_2))); (@M)(@i_2){:=}\mathfrak{A}(@y))$. Set $ST = \mathfrak{C}$-States(the generators of G). Consider g being a function from $\mathbb{N}$ into ST such that $g(0) = s$ and for every natural number i, $g(i+1) = \mathcal{F}(i, (g(i)$ **qua** element of $ST))$. Define $\mathcal{G}$(element) $= g(\$_1(\in \mathbb{N}))$(the array sort of Σ)(M). Consider h being a function from $\mathbb{N}$ into $\mathbb{Z}^\omega$ such that for every element i such that $i \in \mathbb{N}$ holds $h(i) = \mathcal{G}(i)$. For every ordinal number a such that $a \in \operatorname{dom} g$ holds $h(a)$ is an array of $\langle \mathbb{Z}, \leqslant \rangle$. Set $TV = \mathrm{States}_{b \nrightarrow \mathrm{false}_{\mathfrak{C}}}$(the generators of G). Consider s_1 such that $s = s_1$ and s_1(the array sort of Σ)$(M) \neq \emptyset$. Reconsider

$D = s(\text{the array sort of } \Sigma)(M)$ as a 0-based finite non empty array of $\langle \mathbb{Z}, \leqslant \rangle$. Consider g being a function from $\mathbb{N}$ into ST such that $g(0) = s$ and for every natural number i, $g(i+1) = \mathcal{F}(i, (g(i)$ **qua** element of $ST))$. Define $\mathcal{G}(\text{element}) = g(\$_1(\in \mathbb{N}))(\text{the array sort of } \Sigma)(M)$. Consider h being a function from $\mathbb{N}$ into $\mathbb{Z}^\omega$ such that for every element i such that $i \in \mathbb{N}$ holds $h(i) = \mathcal{G}(i)$. For every ordinal number a such that $a \in \operatorname{dom} g$ holds $h(a)$ is an array of $\langle \mathbb{Z}, \leqslant \rangle$. Define $\mathfrak{T}[\text{natural number}] \equiv h(\$_1) \neq \emptyset$. For every natural number i such that $\mathfrak{T}[i]$ holds $\mathfrak{T}[i+1]$. For every natural number a and for every array R of $\langle \mathbb{Z}, \leqslant \rangle$ such that $R = h(a)$ for every s such that $g(a) = s$ there exist sets x, y such that $x = f(s, J)(I)(i_1)$ and $y = f(s, J)(I)(i_2)$ and x, $y \in \operatorname{dom} R$ and $h(a+1) = \operatorname{Swap}(R, x, y)$. Define $\mathcal{Q}[\text{natural number}] \equiv h(\$_1)$ is a permutation of D. Define $\mathcal{P}[\text{natural number}] \equiv g(\$_1)(\text{the array sort of } \Sigma)(M)$ is an ascending permutation of D. There exists a natural number i such that $\mathcal{P}[i]$. Consider $\mathfrak{B}$ being a natural number such that $\mathcal{P}[\mathfrak{B}]$ and for every natural number i such that $\mathcal{P}[i]$ holds $\mathfrak{B} \leqslant i$. Reconsider $c = h\restriction \operatorname{succ} \mathfrak{B}$ as an array of $\mathbb{Z}^\omega$. Set $TV = \text{States}_{b \nrightarrow \text{false}_{\mathfrak{C}}}(\text{the generators of } G)$. Define $\mathcal{H}(\text{natural number}) = f(g(\$_1 - 1), J)$. Consider r being a finite sequence such that $\operatorname{len} r = \mathfrak{B} + 1$ and for every natural number i such that $i \in \operatorname{dom} r$ holds $r(i) = \mathcal{H}(i)$. $\operatorname{rng} r \subseteq ST$. Reconsider $R = g(\mathfrak{B})(\text{the array sort of } \Sigma)(M)$ as an ascending permutation of D. Now let Γ denotes the program

$y :=_{\mathfrak{A}} ({}^{@}M)({}^{@}i_1)$;
$({}^{@}M)({}^{@}i_1) :=_{\mathfrak{A}} ({}^{@}M)({}^{@}i_2)$;
$({}^{@}M)({}^{@}i_2) :=_{\mathfrak{A}} {}^{@}y$;
J

For every natural number i such that $1 \leqslant i < \operatorname{len} r$ holds $r(i) \in TV$ and $r(i+1) = f(r(i), \Gamma)$. □

References

[1] Grzegorz Bancerek. Mizar analysis of algorithms: Preliminaries. *Formalized Mathematics*, 15(**3**):87–110, 2007. doi:10.2478/v10037-007-0011-x.

[2] Grzegorz Bancerek. Program algebra over an algebra. *Formalized Mathematics*, 20(**4**): 309–341, 2012. doi:10.2478/v10037-012-0037-6.

[3] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.

[4] Grzegorz Bancerek. Sorting by exchanging. *Formalized Mathematics*, 19(**2**):93–102, 2011. doi:10.2478/v10037-011-0015-4.

[5] Grzegorz Bancerek. Institution of many sorted algebras. Part I: Signature reduct of an algebra. *Formalized Mathematics*, 6(**2**):279–287, 1997.

[6] Grzegorz Bancerek. Complete lattices. *Formalized Mathematics*, 2(**5**):719–725, 1991.

[7] Grzegorz Bancerek. Free term algebras. *Formalized Mathematics*, 20(**3**):239–256, 2012. doi:10.2478/v10037-012-0029-6.

[8] Grzegorz Bancerek. Terms over many sorted universal algebra. *Formalized Mathematics*, 5(**2**):191–198, 1996.

[9] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.

[10] Grzegorz Bancerek. König's lemma. *Formalized Mathematics*, 2(**3**):397–402, 1991.

[11] Grzegorz Bancerek. Joining of decorated trees. *Formalized Mathematics*, 4(**1**):77–82, 1993.

[12] Grzegorz Bancerek. Directed sets, nets, ideals, filters, and maps. *Formalized Mathematics*, 6(**1**):93–107, 1997.

[13] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.

[14] Grzegorz Bancerek and Artur Korniłowicz. Yet another construction of free algebra. *Formalized Mathematics*, 9(**4**):779–785, 2001.

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

[16] Ewa Burakowska. Subalgebras of many sorted algebra. Lattice of subalgebras. *Formalized Mathematics*, 5(**1**):47–54, 1996.

[17] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.

[18] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.

[19] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**): 55–65, 1990.

[20] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.

[21] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.

[22] Czesław Byliński. Galois connections. *Formalized Mathematics*, 6(**1**):131–143, 1997.

[23] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.

[24] Małgorzata Korolkiewicz. Homomorphisms of many sorted algebras. *Formalized Mathematics*, 5(**1**):61–65, 1996.

[25] Jarosław Kotowicz, Beata Madras, and Małgorzata Korolkiewicz. Basic notation of universal algebra. *Formalized Mathematics*, 3(**2**):251–253, 1992.

[26] Rafał Kwiatek. Factorial and Newton coefficients. *Formalized Mathematics*, 1(**5**):887–890, 1990.

[27] Takashi Mitsuishi and Grzegorz Bancerek. Lattice of fuzzy sets. *Formalized Mathematics*, 11(**4**):393–398, 2003.

[28] Beata Perkowska. Free many sorted universal algebra. *Formalized Mathematics*, 5(**1**): 67–74, 1996.

[29] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1 (**2**):329–334, 1990.

[30] Andrzej Trybulec. A scheme for extensions of homomorphisms of many sorted algebras. *Formalized Mathematics*, 5(**2**):205–209, 1996.

[31] Andrzej Trybulec. Many sorted algebras. *Formalized Mathematics*, 5(**1**):37–42, 1996.

[32] Andrzej Trybulec. Many sorted sets. *Formalized Mathematics*, 4(**1**):15–22, 1993.

[33] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.

[34] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(**3**):575–579, 1990.

[35] Wojciech A. Trybulec and Grzegorz Bancerek. Kuratowski – Zorn lemma. *Formalized Mathematics*, 1(**2**):387–393, 1990.

[36] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

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

[38] Edmund Woronowicz. Many argument relations. *Formalized Mathematics*, 1(**4**):733–737, 1990.

[39] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1 (**1**):73–83, 1990.

Received November 9, 2012

FORMALIZED MATHEMATICS
Vol. 21, No. 1, Pages 25–31, 2013
DOI: 10.2478/forma-2013-0002

VERSITA
degruyter.com/view/j/forma

The C^k Space[1]

Katuhiko Kanazashi
Shizuoka City, Japan

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. In this article, we formalize continuous differentiability of real-valued functions on n-dimensional real normed linear spaces. Next, we give a definition of the C^k space according to [23].

MML identifier: CKSPACE1, version: 8.0.01 5.5.1167

The notation and terminology used in this paper have been introduced in the following articles: [1], [4], [10], [3], [5], [11], [17], [6], [7], [19], [18], [2], [8], [14], [12], [15], [13], [21], [22], [16], [20], and [9].

1. Definition of Continuously Differentiable Functions and Some Properties

Let m be a non zero element of $\mathbb{N}$, f be a partial function from $\mathcal{R}^m$ to $\mathbb{R}$, k be an element of $\mathbb{N}$, and Z be a set. We say that f is continuously differentiable up to order of k and Z if and only if

(Def. 1) (i) $Z \subseteq \operatorname{dom} f$, and

(ii) f is partial differentiable up to order k and Z, and

(iii) for every non empty finite sequence I of elements of $\mathbb{N}$ such that $\operatorname{len} I \leqslant k$ and $\operatorname{rng} I \subseteq \operatorname{Seg} m$ holds $f\restriction^I Z$ is continuous on Z.

Now we state the propositions:

(1) Let us consider a non zero element m of $\mathbb{N}$, a set Z, a non empty finite sequence I of elements of $\mathbb{N}$, and a partial function f from $\mathcal{R}^m$ to $\mathbb{R}$. Suppose f is partially differentiable on Z w.r.t. I. Then $\operatorname{dom}(f\restriction^I Z) = Z$.

[1] This work was supported by JSPS KAKENHI 22300285.

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

(2) Let us consider a non zero element m of $\mathbb{N}$, an element k of $\mathbb{N}$, a non empty subset X of $\mathcal{R}^m$, and a partial function f from $\mathcal{R}^m$ to $\mathbb{R}$. Suppose

(i) X is open, and

(ii) $X \subseteq \operatorname{dom} f$.

Then f is continuously differentiable up to order of 1 and X if and only if f is differentiable on X and for every element x_0 of $\mathcal{R}^m$ and for every real number r such that $x_0 \in X$ and $0 < r$ there exists a real number s such that $0 < s$ and for every element x_1 of $\mathcal{R}^m$ such that $x_1 \in X$ and $|x_1 - x_0| < s$ for every element v of $\mathcal{R}^m$, $|f'(x_1)(v) - f'(x_0)(v)| \leqslant r \cdot |v|$.

(3) Let us consider a non zero element m of $\mathbb{N}$, a non empty subset X of $\mathcal{R}^m$, and a partial function f from $\mathcal{R}^m$ to $\mathbb{R}$. Suppose

(i) X is open, and

(ii) $X \subseteq \operatorname{dom} f$, and

(iii) f is continuously differentiable up to order of 1 and X.

Then f is continuous on X. The theorem is a consequence of (2).

(4) Let us consider a non zero element m of $\mathbb{N}$, an element k of $\mathbb{N}$, a non empty subset X of $\mathcal{R}^m$, and partial functions f, g from $\mathcal{R}^m$ to $\mathbb{R}$. Suppose

(i) f is continuously differentiable up to order of k and X, and

(ii) g is continuously differentiable up to order of k and X, and

(iii) X is open.

Then $f + g$ is continuously differentiable up to order of k and X. The theorem is a consequence of (1). PROOF: For every non empty finite sequence I of elements of $\mathbb{N}$ such that $\operatorname{len} I \leqslant k$ and $\operatorname{rng} I \subseteq \operatorname{Seg} m$ holds $(f+g)\restriction^I X$ is continuous on X. □

(5) Let us consider a non zero element m of $\mathbb{N}$, an element k of $\mathbb{N}$, a non empty subset X of $\mathcal{R}^m$, a real number r, and a partial function f from $\mathcal{R}^m$ to $\mathbb{R}$. Suppose

(i) f is continuously differentiable up to order of k and X, and

(ii) X is open.

Then $r \cdot f$ is continuously differentiable up to order of k and X. The theorem is a consequence of (1). PROOF: For every non empty finite sequence I of elements of $\mathbb{N}$ such that $\operatorname{len} I \leqslant k$ and $\operatorname{rng} I \subseteq \operatorname{Seg} m$ holds $r \cdot f\restriction^I X$ is continuous on X. □

(6) Let us consider a non zero element m of $\mathbb{N}$, an element k of $\mathbb{N}$, a non empty subset X of $\mathcal{R}^m$, and partial functions f, g from $\mathcal{R}^m$ to $\mathbb{R}$. Suppose

(i) f is continuously differentiable up to order of k and X, and

(ii) g is continuously differentiable up to order of k and X, and

(iii) X is open.

Then $f - g$ is continuously differentiable up to order of k and X. The theorem is a consequence of (1). PROOF: For every non empty finite sequence I of elements of $\mathbb{N}$ such that $\operatorname{len} I \leqslant k$ and $\operatorname{rng} I \subseteq \operatorname{Seg} m$ holds $(f-g)\restriction^I X$ is continuous on X. □

Let us consider a non zero element m of $\mathbb{N}$, a non empty subset Z of $\mathcal{R}^m$, a partial function f from $\mathcal{R}^m$ to $\mathbb{R}$, and non empty finite sequences I, G of elements of $\mathbb{N}$. Now we state the propositions:

(7) $f\restriction^{G^\frown I} Z = (f\restriction^G Z)\restriction^I Z$.

(8) $f\restriction^{G^\frown I} Z$ is continuous on Z if and only if $(f\restriction^G Z)\restriction^I Z$ is continuous on Z.

Now we state the propositions:

(9) Let us consider a non zero element m of $\mathbb{N}$, a non empty subset Z of $\mathcal{R}^m$, a partial function f from $\mathcal{R}^m$ to $\mathbb{R}$, elements i, j of $\mathbb{N}$, and a non empty finite sequence I of elements of $\mathbb{N}$. Suppose

(i) f is continuously differentiable up to order of $i + j$ and Z, and

(ii) $\operatorname{rng} I \subseteq \operatorname{Seg} m$, and

(iii) $\operatorname{len} I = j$.

Then $f\restriction^I Z$ is continuously differentiable up to order of i and Z. The theorem is a consequence of (1) and (7).

(10) Let us consider a non zero element m of $\mathbb{N}$, a non empty subset Z of $\mathcal{R}^m$, a partial function f from $\mathcal{R}^m$ to $\mathbb{R}$, and elements i, j of $\mathbb{N}$. Suppose

(i) f is continuously differentiable up to order of i and Z, and

(ii) $j \leqslant i$.

Then f is continuously differentiable up to order of j and Z.

(11) Let us consider a non zero element m of $\mathbb{N}$ and a non empty subset Z of $\mathcal{R}^m$. Suppose Z is open. Let us consider an element k of $\mathbb{N}$ and partial functions f, g from $\mathcal{R}^m$ to $\mathbb{R}$. Suppose

(i) f is continuously differentiable up to order of k and Z, and

(ii) g is continuously differentiable up to order of k and Z.

Then $f \cdot g$ is continuously differentiable up to order of k and Z. The theorem is a consequence of (10), (1), (3), (9), and (7). PROOF: Define $\mathcal{P}[\text{element of } \mathbb{N}] \equiv$ for every partial functions f, g from $\mathcal{R}^m$ to $\mathbb{R}$ such that f is continuously differentiable up to order of $\$_1$ and Z and g is continuously differentiable up to order of $\$_1$ and Z holds $f \cdot g$ is continuously differentiable up to order of $\$_1$ and Z. Set $Z0 = (0$ **qua** natural number). $\mathcal{P}[0]$. For every element k of $\mathbb{N}$ such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. □

(12) Let us consider a non zero element m of $\mathbb{N}$, a partial function f from $\mathcal{R}^m$ to $\mathbb{R}$, a non empty subset X of $\mathcal{R}^m$, and a real number d. Suppose

(i) X is open, and

(ii) $f = X \longmapsto d$.

Let us consider an element x of $\mathcal{R}^m$. If $x \in X$, then f is differentiable in x and $f'(x) = \mathcal{R}^m \longmapsto 0$.

(13) Let us consider a non zero element m of $\mathbb{N}$, a partial function f from $\mathcal{R}^m$ to $\mathbb{R}$, a non empty subset X of $\mathcal{R}^m$, and a real number d. Suppose

(i) X is open, and

(ii) $f = X \longmapsto d$.

Let us consider an element x_0 of $\mathcal{R}^m$ and a real number r. Suppose

(iii) $x_0 \in X$, and

(iv) $0 < r$.

Then there exists a real number s such that

(v) $0 < s$, and

(vi) for every element x_1 of $\mathcal{R}^m$ such that $x_1 \in X$ and $|x_1 - x_0| < s$ for every element v of $\mathcal{R}^m$, $|f'(x_1)(v) - f'(x_0)(v)| \leqslant r \cdot |v|$.

The theorem is a consequence of (12).

(14) Let us consider a non zero element m of $\mathbb{N}$, a partial function f from $\mathcal{R}^m$ to $\mathbb{R}$, a non empty subset X of $\mathcal{R}^m$, and a real number d. Suppose

(i) X is open, and

(ii) $f = X \longmapsto d$.

Then

(iii) f is differentiable on X, and

(iv) $\operatorname{dom} f'_{\restriction X} = X$, and

(v) for every element x of $\mathcal{R}^m$ such that $x \in X$ holds $(f'_{\restriction X})_x = \mathcal{R}^m \longmapsto 0$.

The theorem is a consequence of (12).

(15) Let us consider a non zero element m of $\mathbb{N}$, a partial function f from $\mathcal{R}^m$ to $\mathbb{R}$, a non empty subset X of $\mathcal{R}^m$, a real number d, and an element i of $\mathbb{N}$. Suppose

(i) X is open, and

(ii) $f = X \longmapsto d$, and

(iii) $1 \leqslant i \leqslant m$.

Then

(iv) f is partially differentiable on X w.r.t. i, and

(v) $f\restriction^i X$ is continuous on X.

The theorem is a consequence of (14) and (13).

(16) Let us consider a non zero element m of $\mathbb{N}$, an element i of $\mathbb{N}$, a partial function f from $\mathcal{R}^m$ to $\mathbb{R}$, a non empty subset X of $\mathcal{R}^m$, and a real number d. Suppose

(i) X is open, and

(ii) $f = X \longmapsto d$, and

(iii) $1 \leqslant i \leqslant m$.

Then $f\restriction^i X = X \longmapsto 0$. The theorem is a consequence of (15) and (12).

Let us consider a non zero element m of $\mathbb{N}$, a non empty finite sequence I of elements of $\mathbb{N}$, a non empty subset X of $\mathcal{R}^m$, a partial function f from $\mathcal{R}^m$ to $\mathbb{R}$, and a real number d. Now we state the propositions:

(17) Suppose X is open and $f = X \longmapsto d$ and $\operatorname{rng} I \subseteq \operatorname{Seg} m$. Then

(i) $(\text{PartDiffSeq}(f, X, I))(0) = X \longmapsto d$, and

(ii) for every element i of $\mathbb{N}$ such that $1 \leqslant i \leqslant \operatorname{len} I$ holds $(\text{PartDiffSeq}(f, X, I))(i) = X \longmapsto 0$.

(18) Suppose X is open and $f = X \longmapsto d$ and $\operatorname{rng} I \subseteq \operatorname{Seg} m$. Then

(i) f is partially differentiable on X w.r.t. I, and

(ii) $f\restriction^I X$ is continuous on X.

Now we state the proposition:

(19) Let us consider a non zero element m of $\mathbb{N}$, an element k of $\mathbb{N}$, a non empty subset X of $\mathcal{R}^m$, a partial function f from $\mathcal{R}^m$ to $\mathbb{R}$, and a real number d. Suppose

(i) X is open, and

(ii) $f = X \longmapsto d$.

Then f is continuously differentiable up to order of k and X. The theorem is a consequence of (18).

Let m be a non zero element of $\mathbb{N}$. Observe that there exists a non empty subset of $\mathcal{R}^m$ which is open.

2. Definition of the C^k Space

Let m be a non zero element of $\mathbb{N}$, k be an element of $\mathbb{N}$, and X be a non empty open subset of $\mathcal{R}^m$. The functor the $\mathbb{C}^k$ functions of k and X yielding a non empty subset of $\operatorname{RAlgebra} X$ is defined by the term

(Def. 2) $\{f$ where f is a partial function from $\mathcal{R}^m$ to $\mathbb{R} : f$ is continuously differentiable up to order of k and X and $\operatorname{dom} f = X\}$.

Let us note that the $\mathbb{C}^k$ functions of k and X is additively linearly closed and multiplicatively closed.

The functor the $\mathbb{R}$ algebra of $\mathbb{C}^k$ functions of k and X yielding a subalgebra of RAlgebra X is defined by the term

(Def. 3) $\langle$the $\mathbb{C}^k$ functions of k and X, mult(the $\mathbb{C}^k$ functions of k and X, RAlgebra X), Add(the $\mathbb{C}^k$ functions of k and X, RAlgebra X), Mult(the $\mathbb{C}^k$ functions of k and X, RAlgebra X), One(the $\mathbb{C}^k$ functions of k and X, RAlgebra X), Zero(the $\mathbb{C}^k$ functions of k and X, RAlgebra X)$\rangle$.

Let us note that the $\mathbb{R}$ algebra of $\mathbb{C}^k$ functions of k and X is Abelian add-associative right zeroed right complementable vector distributive scalar distributive scalar associative scalar unital commutative associative right unital right distributive and vector associative.

Now we state the propositions:

(20) Let us consider a non zero element m of $\mathbb{N}$, an element k of $\mathbb{N}$, a non empty open subset X of $\mathcal{R}^m$, vectors F, G, H of the $\mathbb{R}$ algebra of $\mathbb{C}^k$ functions of k and X, and partial functions f, g, h from $\mathcal{R}^m$ to $\mathbb{R}$. Suppose

(i) $f = F$, and

(ii) $g = G$, and

(iii) $h = H$.

Then $H = F+G$ if and only if for every element x of X, $h(x) = f(x)+g(x)$.

(21) Let us consider a non zero element m of $\mathbb{N}$, an element k of $\mathbb{N}$, a non empty open subset X of $\mathcal{R}^m$, vectors F, G, H of the $\mathbb{R}$ algebra of $\mathbb{C}^k$ functions of k and X, partial functions f, g, h from $\mathcal{R}^m$ to $\mathbb{R}$, and a real number a. Suppose

(i) $f = F$, and

(ii) $g = G$.

Then $G = a \cdot F$ if and only if for every element x of X, $g(x) = a \cdot f(x)$.

(22) Let us consider a non zero element m of $\mathbb{N}$, an element k of $\mathbb{N}$, a non empty open subset X of $\mathcal{R}^m$, vectors F, G, H of the $\mathbb{R}$ algebra of $\mathbb{C}^k$ functions of k and X, and partial functions f, g, h from $\mathcal{R}^m$ to $\mathbb{R}$. Suppose

(i) $f = F$, and

(ii) $g = G$, and

(iii) $h = H$.

Then $H = F \cdot G$ if and only if for every element x of X, $h(x) = f(x) \cdot g(x)$.

Let us consider a non zero element m of $\mathbb{N}$, an element k of $\mathbb{N}$, and a non empty open subset X of $\mathcal{R}^m$. Now we state the propositions:

(23) $0_\alpha = X \longmapsto 0$, where α is the $\mathbb{R}$ algebra of $\mathbb{C}^k$ functions of k and X.

(24) $\mathbf{1}_\alpha = X \longmapsto 1$, where α is the $\mathbb{R}$ algebra of $\mathbb{C}^k$ functions of k and X.

REFERENCES

[1] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.

[2] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.

[3] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.

[4] Czesław Byliński. The complex numbers. *Formalized Mathematics*, 1(**3**):507–513, 1990.

[5] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.

[6] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**): 55–65, 1990.

[7] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.

[8] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.

[9] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.

[10] Agata Darmochwał. The Euclidean space. *Formalized Mathematics*, 2(**4**):599–603, 1991.

[11] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.

[12] Noboru Endou, Hiroyuki Okazaki, and Yasunari Shidama. Higher-order partial differentiation. *Formalized Mathematics*, 20(**2**):113–124, 2012. doi:10.2478/v10037-012-0015-z.

[13] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**): 35–40, 1990.

[14] Takao Inoué, Adam Naumowicz, Noboru Endou, and Yasunari Shidama. Partial differentiation of vector-valued functions on n-dimensional real normed linear spaces. *Formalized Mathematics*, 19(**1**):1–9, 2011. doi:10.2478/v10037-011-0001-x.

[15] Andrzej Kondracki. Basic properties of rational numbers. *Formalized Mathematics*, 1(**5**): 841–845, 1990.

[16] Beata Perkowska. Functional sequence from a domain to a domain. *Formalized Mathematics*, 3(**1**):17–21, 1992.

[17] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1 (**2**):329–334, 1990.

[18] Andrzej Trybulec. On the sets inhabited by numbers. *Formalized Mathematics*, 11(**4**): 341–347, 2003.

[19] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.

[20] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

[21] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1 (**1**):73–83, 1990.

[22] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

[23] Kosaku Yosida. *Functional Analysis*. Springer Classics in Mathematics, 1996.

Received November 9, 2012

FORMALIZED MATHEMATICS
Vol. 21, No. 1, Pages 33–39, 2013
DOI: 10.2478/forma-2013-0003

VERSITA
degruyter.com/view/j/forma

Random Variables and Product of Probability Spaces[1]

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. We have been working on the formalization of the probability and the randomness. In [15] and [16], we formalized some theorems concerning the real-valued random variables and the product of two probability spaces. In this article, we present the generalized formalization of [15] and [16]. First, we formalize the random variables of arbitrary set and prove the equivalence between random variable on Σ, Borel sets and a real-valued random variable on Σ. Next, we formalize the product of countably infinite probability spaces.

MML identifier: RANDOM_3, version: 8.1.01 5.7.1169

The notation and terminology used in this paper have been introduced in the following articles: [1], [14], [12], [4], [11], [18], [7], [8], [5], [2], [3], [9], [13], [22], [15], [16], [20], [21], [17], [19], [6], and [10].

1. Random Variables

In this paper Ω, Ω_1, Ω_2 denote non empty sets, Σ denotes a σ-field of subsets of Ω, S_1 denotes a σ-field of subsets of Ω_1, and S_2 denotes a σ-field of subsets of Ω_2.

Now we state the proposition:

(1) Let us consider a non empty set B and a function f. Then $f^{-1}(\bigcup B) = \bigcup\{f^{-1}(Y)$ where Y is an element of B : not contradiction$\}$.

Let us consider a function f from Ω_1 into Ω_2, a sequence B of subsets of Ω_2, and a sequence D of subsets of Ω_1. Now we state the propositions:

[1]The 1st author was supported by JSPS KAKENHI 21240001, and the 2nd author was supported by JSPS KAKENHI 22300285.

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

(2) If for every element n of $\mathbb{N}$, $D(n) = f^{-1}(B(n))$, then $f^{-1}(\bigcup B) = \bigcup D$.

(3) If for every element n of $\mathbb{N}$, $D(n) = f^{-1}(B(n))$, then $f^{-1}(\text{Intersection } B) = \text{Intersection } D$.

Now we state the propositions:

(4) Let us consider a function F from Ω into $\mathbb{R}$ and a real number r. Suppose F is a real-valued random variable on Σ. Then $F^{-1}(]-\infty, r[) \in \Sigma$. PROOF: Consider X being an element of Σ such that $X = \Omega$ and F is measurable on X. For every element z, $z \in F^{-1}(]-\infty, r[)$ iff $z \in \Omega_\Sigma \cap \text{LE-dom}(F, r)$. □

(5) Let us consider a function F from Ω into $\mathbb{R}$. Suppose F is a real-valued random variable on Σ. Then $\{x$ where x is an element of the Borel sets : $F^{-1}(x)$ is element of $\Sigma\}$ is a σ-field of subsets of $\mathbb{R}$. The theorem is a consequence of (4) and (3). PROOF: Set $S = \{x$ where x is an element of the Borel sets : $F^{-1}(x)$ is an element of $\Sigma\}$. For every element x such that $x \in S$ holds $x \in$ the Borel sets. Set $r_0 =$ the element of $\mathbb{R}$. Reconsider $y_0 = \text{halfline}(r_0)$ as an element of the Borel sets. For every subset A of $\mathbb{R}$ such that $A \in S$ holds $A^{\text{c}} \in S$. For every sequence A_1 of subsets of $\mathbb{R}$ such that $\text{rng } A_1 \subseteq S$ holds Intersection $A_1 \in S$. □

Let us consider a function f from Ω into $\mathbb{R}$. Now we state the propositions:

(6) Suppose f is a real-valued random variable on Σ. Then $\{x$ where x is an element of the Borel sets : $f^{-1}(x)$ is an element of $\Sigma\}$ = the Borel sets.

(7) f is random variable on Σ and the Borel sets if and only if f is a real-valued random variable on Σ.

(8) The set of random variables on Σ and the Borel sets = the real-valued random variables set on Σ.

Let us consider Ω_1, Ω_2, S_1, and S_2. Let F be a function from Ω_1 into Ω_2. We say that F is (S_1, S_2)-random variable-like if and only if

(Def. 1) F is random variable on S_1 and S_2.

Observe that there exists a function from Ω_1 into Ω_2 which is (S_1, S_2)-random variable-like.

A random variable of S_1 and S_2 is an (S_1, S_2)-random variable-like function from Ω_1 into Ω_2. Now we state the proposition:

(9) Let us consider a function f from Ω into $\mathbb{R}$. Then f is a random variable of Σ and the Borel sets if and only if f is a real-valued random variable on Σ.

Let F be a function. We say that F is random variable family-like if and only if

(Def. 2) Let us consider a set x. Suppose $x \in \text{dom } F$. Then there exist non empty sets Ω_1, Ω_2 and there exists a σ-field S_1 of subsets of Ω_1 and there exists

a σ-field S_2 of subsets of Ω_2 and there exists a random variable f of S_1 and S_2 such that $F(x) = f$.

One can verify that there exists a function which is random variable family-like.

A random variable family is a random variable family-like function. In this paper F denotes a random variable of S_1 and S_2.

Let Y be a non empty set, S be a σ-field of subsets of Y, and F be a function. We say that F is S-measure valued if and only if

(Def. 3) Let us consider a set x. If $x \in \operatorname{dom} F$, then there exists a σ-measure M on S such that $F(x) = M$.

Note that there exists a function which is S-measure valued.

Let F be a function. We say that F is S-probability valued if and only if

(Def. 4) Let us consider a set x. If $x \in \operatorname{dom} F$, then there exists a probability P on S such that $F(x) = P$.

Let us note that there exists a function which is S-probability valued.

Let X, Y be non empty sets. One can verify that there exists an S-probability valued function which is X-defined.

One can verify that there exists an X-defined S-probability valued function which is total.

Let Y be a non empty set. Let us note that every function which is S-probability valued is also S-measure valued.

Let F be a function. We say that F is S-random variable family if and only if

(Def. 5) Let us consider a set x. Suppose $x \in \operatorname{dom} F$. Then there exists a real-valued random variable Z on S such that $F(x) = Z$.

Observe that there exists a function which is S-random variable family.

Now we state the propositions:

(10) Let us consider an element y of S_2. Suppose $y \neq \emptyset$. Then $\{z$ where z is an element of $\Omega_1 : F(z)$ is an element of $y\} = F^{-1}(y)$. PROOF: Set $D = \{z$ where z is an element of $\Omega_1 : F(z)$ is an element of $y\}$. For every element x, $x \in D$ iff $x \in F^{-1}(y)$. $\square$

(11) Let us consider a random variable F of S_1 and S_2. Then

(i) $\{x$ where x is a subset of $\Omega_1 :$ there exists an element y of S_2 such that $x = F^{-1}(y)\} \subseteq S_1$, and

(ii) $\{x$ where x is a subset of $\Omega_1 :$ there exists an element y of S_2 such that $x = F^{-1}(y)\}$ is a σ-field of subsets of Ω_1.

The theorem is a consequence of (3). PROOF: Set $S = \{x$ where x is a subset of $\Omega_1 :$ there exists an element y of S_2 such that $x = F^{-1}(y)\}$. For every element x such that $x \in S$ holds $x \in S_1$. For every subset A of

Ω_1 such that $A \in S$ holds $A^{\mathrm{c}} \in S$. For every sequence A_1 of subsets of Ω_1 such that $\operatorname{rng} A_1 \subseteq S$ holds Intersection $A_1 \in S$. $\square$

Let us consider Ω_1, Ω_2, S_1, and S_2. Let M be a measure on S_1 and F be a random variable of S_1 and S_2. The functor the image measure of F and M yielding a measure on S_2 is defined by

(Def. 6) Let us consider an element y of S_2. Then $it(y) = M(F^{-1}(y))$.

Let M be a σ-measure on S_1. Note that the image measure of F and M is σ-additive.

Now we state the proposition:

(12) Let us consider a probability P on S_1 and a random variable F of S_1 and S_2. Then (the image measure of F and $\operatorname{P2M} P)(\Omega_2) = 1$.

Let us consider Ω_1, Ω_2, S_1, and S_2. Let P be a probability on S_1 and F be a random variable of S_1 and S_2. The functor probability(F, P) yielding a probability on S_2 is defined by the term

(Def. 7) $\operatorname{M2P}$ the image measure of F and $\operatorname{P2M} P$.

Now we state the propositions:

(13) Let us consider a probability P on S_1 and a random variable F of S_1 and S_2. Then probability$(F, P) =$ the image measure of F and $\operatorname{P2M} P$. The theorem is a consequence of (12).

(14) Let us consider a probability P on S_1, a random variable F of S_1 and S_2, and a set y. If $y \in S_2$, then (probability$(F, P))(y) = P(F^{-1}(y))$. The theorem is a consequence of (13).

(15) Every function from Ω_1 into Ω_2 is a random variable of the trivial σ-field of Ω_1 and the trivial σ-field of Ω_2.

(16) Let us consider a non empty set S. Then every non empty finite sequence of elements of S is a random variable of the trivial σ-field of $\operatorname{Seg} \operatorname{len} F$ and the trivial σ-field of S. The theorem is a consequence of (15).

(17) Let us consider finite non empty sets V, S, a random variable G of the trivial σ-field of V and the trivial σ-field of S, and a set y. Suppose $y \in$ the trivial σ-field of S. Then (probability$(G,$ the trivial probability of $V))(y) = \frac{\overline{\overline{G^{-1}(y)}}}{\overline{\overline{V}}}$. The theorem is a consequence of (14).

(18) Let us consider a finite non empty set S, a non empty finite sequence s of elements of S, and a set x. Suppose $x \in S$. Then there exists a random variable G of the trivial σ-field of $\operatorname{Seg} \operatorname{len} s$ and the trivial σ-field of S such that

(i) $G = s$, and

(ii) (probability$(G,$ the trivial probability of $\operatorname{Seg} \operatorname{len} s))(\{x\}) = \operatorname{Prob}_{\mathrm{D}}(x, s)$.

The theorem is a consequence of (16) and (17).

2. Product of Probability Spaces

Let D be a non-empty many sorted set indexed by $\mathbb{N}$ and n be a natural number. One can check that $D(n)$ is non empty.

Let S, F be many sorted sets indexed by $\mathbb{N}$. We say that F is σ-field S-sequence-like if and only if

(Def. 8) Let us consider a natural number n. Then $F(n)$ is a σ-field of subsets of $S(n)$.

Let S be a many sorted set indexed by $\mathbb{N}$. Let us observe that there exists a many sorted set indexed by $\mathbb{N}$ which is σ-field S-sequence-like.

Let D be a many sorted set indexed by $\mathbb{N}$. A σ-field sequence of D is a σ-field D-sequence-like many sorted set indexed by $\mathbb{N}$. Let S be a σ-field sequence of D and n be a natural number. Note that the functor $S(n)$ yields a σ-field of subsets of $D(n)$. Let D be a non-empty many sorted set indexed by $\mathbb{N}$. Let M be a many sorted set indexed by $\mathbb{N}$. We say that M is S-probability sequence-like if and only if

(Def. 9) Let us consider a natural number n. Then $M(n)$ is a probability on $S(n)$.

Observe that there exists a many sorted set indexed by $\mathbb{N}$ which is S-probability sequence-like.

A probability sequence of S is an S-probability sequence-like many sorted set indexed by $\mathbb{N}$. Let P be a probability sequence of S and n be a natural number. One can verify that the functor $P(n)$ yields a probability on $S(n)$. Let D be a many sorted set indexed by $\mathbb{N}$. The functor the product domain D yielding a many sorted set indexed by $\mathbb{N}$ is defined by

(Def. 10) (i) $it(0) = D(0)$, and

(ii) for every natural number i, $it(i+1) = it(i) \times D(i+1)$.

Now we state the proposition:

(19) Let us consider a many sorted set D indexed by $\mathbb{N}$. Then

(i) (the product domain D)$(0) = D(0)$, and

(ii) (the product domain D)$(1) = D(0) \times D(1)$, and

(iii) (the product domain D)$(2) = D(0) \times D(1) \times D(2)$, and

(iv) (the product domain D)$(3) = D(0) \times D(1) \times D(2) \times D(3)$.

Let D be a non-empty many sorted set indexed by $\mathbb{N}$. Let us note that the product domain D is non-empty.

Let D be a finite-yielding many sorted set indexed by $\mathbb{N}$. One can check that the product domain D is finite-yielding.

Let us consider Ω and Σ. Let P be a set. Assume P is a probability on Σ. The functor modetrans(P, Σ) yielding a probability on Σ is defined by the term

(Def. 11) P.

Let D be a finite-yielding non-empty many sorted set indexed by $\mathbb{N}$. The functor the trivial σ-field sequence D yielding a σ-field sequence of D is defined by

(Def. 12) Let us consider a natural number n. Then $it(n) =$ the trivial σ-field of $D(n)$.

Let P be a probability sequence of the trivial σ-field sequence D and n be a natural number. One can check that the functor $P(n)$ yields a probability on the trivial σ-field of $D(n)$. The functor ProductProbability(P, D) yielding a many sorted set indexed by $\mathbb{N}$ is defined by

(Def. 13) (i) $it(0) = P(0)$, and

(ii) for every natural number i, $it(i+1) =$ Product-Probability((the product domain $D)(i), D(i+1),$ modetrans $(it(i),$ the trivial σ-field of (the product domain $D)(i)), P(i+1))$.

Let us consider a finite-yielding non-empty many sorted set D indexed by $\mathbb{N}$, a probability sequence P of the trivial σ-field sequence D, and a natural number n. Now we state the propositions:

(20) (ProductProbability$(P, D))(n)$ is a probability on the trivial σ-field of (the product domain $D)(n)$.

(21) There exists a probability P_4 on the trivial σ-field of (the product domain $D)(n)$ such that

(i) $P_4 =$ (ProductProbability$(P, D))(n)$, and

(ii) (ProductProbability$(P, D))(n+1) =$ Product-Probability((the product domain $D)(n), D(n+1), P_4, P(n+1))$.

Now we state the proposition:

(22) Let us consider a finite-yielding non-empty many sorted set D indexed by $\mathbb{N}$ and a probability sequence P of the trivial σ-field sequence D. Then

(i) (ProductProbability$(P, D))(0) = P(0)$, and

(ii) (ProductProbability$(P, D))(1) =$ Product-Probability$(D(0), D(1), P(0), P(1))$, and

(iii) there exists a probability P_1 on the trivial σ-field of $D(0) \times D(1)$ such that $P_1 =$ (ProductProbability$(P, D))(1)$ and (ProductProbability$(P, D))(2) =$ Product-Probability$(D(0) \times D(1), D(2), P_1, P(2))$, and

(iv) there exists a probability P_2 on the trivial σ-field of $D(0) \times D(1) \times D(2)$ such that $P_2 =$ (ProductProbability$(P, D))(2)$ and (ProductProbability$(P, D))(3) =$ Product-Probability$(D(0) \times D(1) \times D(2), D(3), P_2, P(3))$, and

(v) there exists a probability P_3 on the trivial σ-field of $D(0) \times D(1) \times D(2) \times D(3)$ such that $P_3 =$ (ProductProbability$(P, D))(3)$ and

(ProductProbability(P, D))(4) = Product-Probability$(D(0) \times D(1) \times D(2) \times D(3), D(4), P_3, P(4))$.

The theorem is a consequence of (19) and (21).

REFERENCES

[1] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.

[2] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.

[3] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.

[4] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.

[5] Józef Białas. The σ-additive measure theory. *Formalized Mathematics*, 2(**2**):263–270, 1991.

[6] Józef Białas. Series of positive real numbers. Measure theory. *Formalized Mathematics*, 2(**1**):173–183, 1991.

[7] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**): 55–65, 1990.

[8] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.

[9] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.

[10] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.

[11] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.

[12] Peter Jaeger. Elementary introduction to stochastic finance in discrete time. *Formalized Mathematics*, 20(**1**):1–5, 2012. doi:10.2478/v10037-012-0001-5.

[13] Andrzej Nędzusiak. σ-fields and probability. *Formalized Mathematics*, 1(**2**):401–407, 1990.

[14] Hiroyuki Okazaki. Probability on finite and discrete set and uniform distribution. *Formalized Mathematics*, 17(**2**):173–178, 2009. doi:10.2478/v10037-009-0020-z.

[15] Hiroyuki Okazaki and Yasunari Shidama. Probability on finite set and real-valued random variables. *Formalized Mathematics*, 17(**2**):129–136, 2009. doi:10.2478/v10037-009-0014-x.

[16] Hiroyuki Okazaki and Yasunari Shidama. Probability measure on discrete spaces and algebra of real-valued random variables. *Formalized Mathematics*, 18(**4**):213–217, 2010. doi:10.2478/v10037-010-0026-6.

[17] Beata Padlewska. Families of sets. *Formalized Mathematics*, 1(**1**):147–152, 1990.

[18] Andrzej Trybulec and Agata Darmochwał. Boolean domains. *Formalized Mathematics*, 1 (**1**):187–190, 1990.

[19] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

[20] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1 (**1**):73–83, 1990.

[21] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

[22] Bo Zhang, Hiroshi Yamazaki, and Yatsuka Nakamura. The relevance of measure and probability, and definition of completeness of probability. *Formalized Mathematics*, 14 (**4**):225–229, 2006. doi:10.2478/v10037-006-0026-8.

Received December 1, 2012

FORMALIZED MATHEMATICS
Vol. 21, No. 1, Pages 41–46, 2013
DOI: 10.2478/forma-2013-0004

VERSITA
degruyter.com/view/j/forma

Semantics of MML Query - Ordering

Grzegorz Bancerek
Association of Mizar Users
Białystok, Poland

Summary. Semantics of order directives of MML Query is presented. The formalization is done according to [1].

MML identifier: MMLQUER2, version: 8.1.01 5.7.1169

The notation and terminology used in this paper have been introduced in the following articles: [2], [7], [13], [9], [10], [8], [3], [4], [5], [11], [17], [19], [18], [6], [15], [16], [14], and [12].

1. Preliminaries

In this paper X denotes a set, R, R_1, R_2 denote binary relations, x, y, z denote sets, and n, m, k denote natural numbers.

Let us consider a binary relation R on X. Now we state the propositions:

(1) $\operatorname{field} R \subseteq X$.

(2) If $x, y \in R$, then $x, y \in X$.

Now we state the propositions:

(3) Let us consider sets X, Y. Then $(\mathrm{id}_X)^{\circ}Y = X \cap Y$.

(4) $\langle x, y\rangle \in R \,|^2\, X$ if and only if $x, y \in X$ and $\langle x, y\rangle \in R$.

(5) $\operatorname{dom}(X \restriction R) \subseteq \operatorname{dom} R$.

(6) Let us consider a total reflexive binary relation R on X and a subset S of X. Then $R \,|^2\, S$ is a total reflexive binary relation on S. The theorem is a consequence of (4). Proof: Set $Q = R \,|^2\, S$. $\operatorname{dom} Q = S$. □

(7) Let us consider transfinite sequences f, g. Then $\operatorname{rng}(f^\frown g) = \operatorname{rng} f \cup \operatorname{rng} g$.

Let us consider R. Let us note that R is transitive if and only if the condition (Def. 1) is satisfied.

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

(Def. 1) If $x, y \in R$ and $y, z \in R$, then $x, z \in R$.

One can verify that R is antisymmetric if and only if the condition (Def. 2) is satisfied.

(Def. 2) If $x, y \in R$ and $y, x \in R$, then $x = y$.

Now we state the proposition:

(8) Let us consider a non empty set X, a total connected binary relation R on X, and elements x, y of X. If $x \neq y$, then $x, y \in R$ or $y, x \in R$.

2. Composition of Orders

Let R_1, R_2 be binary relations. The functor R_1, R_2 yielding a binary relation is defined by the term

(Def. 3) $R_1 \cup (R_2 \setminus R_1^{\smile})$.

Now we state the propositions:

(9) $x, y \in R_1$, R_2 if and only if $x, y \in R_1$ or $y, x \notin R_1$ and $x, y \in R_2$.

(10) $\operatorname{field}(R_1, R_2) = \operatorname{field} R_1 \cup \operatorname{field} R_2$. The theorem is a consequence of (9).

(11) R_1, $R_2 \subseteq R_1 \cup R_2$. The theorem is a consequence of (9).

Let X be a set and R_1, R_2 be binary relations on X. Note that the functor R_1, R_2 yields a binary relation on X. Let R_1, R_2 be reflexive binary relations. One can verify that R_1, R_2 is reflexive.

Let R_1, R_2 be antisymmetric binary relations. Note that R_1, R_2 is antisymmetric.

Let X be a set and R be a binary relation on X. We say that R is β-transitive if and only if

(Def. 4) Let us consider elements x, y of X. If $x, y \notin R$, then for every element z of X such that $x, z \in R$ holds $y, z \in R$.

Observe that every binary relation on X which is connected total and transitive is also β-transitive.

Let us observe that there exists an order in X which is connected.

Let R_1 be a β-transitive transitive binary relation on X and R_2 be a transitive binary relation on X. Observe that R_1, R_2 is transitive.

Let R_1 be a binary relation on X and R_2 be a total reflexive binary relation on X. Let us note that R_1, R_2 is total and reflexive as a binary relation on X.

Let R_2 be a total connected reflexive binary relation on X. One can verify that R_1, R_2 is connected.

Now we state the propositions:

(12) $(R, R_1), R_2 = R, (R_1, R_2)$. The theorem is a consequence of (9).

(13) Let us consider a connected reflexive total binary relation R on X and a binary relation R_2 on X. Then $R, R_2 = R$. The theorem is a consequence of (9) and (2).

3. number of ORDERING

Let X be a set and f be a function from X into $\mathbb{N}$. The functor number of f yielding a binary relation on X is defined by

(Def. 5) $x, y \in it$ if and only if x, $y \in X$ and $f(x) < f(y)$.

Let us note that number of f is antisymmetric transitive and β-transitive.

Let X be a finite set and O be an operation of X. The functor value of O yielding a function from X into $\mathbb{N}$ is defined by

(Def. 6) Let us consider an element x of X. Then $it(x) = \overline{\overline{x(O)}}$.

Now we state the proposition:

(14) Let us consider a finite set X, an operation O of X, and elements x, y of X. Then $x, y \in$ number of value of O if and only if $\overline{\overline{x(O)}} < \overline{\overline{y(O)}}$.

Let us consider X. Let O be an operation of X. The functor first O yielding a binary relation on X is defined by

(Def. 7) Let us consider elements x, y of X. Then $x, y \in it$ if and only if $x(O) \neq \emptyset$ and $y(O) = \emptyset$.

Let us observe that first O is antisymmetric transitive and β-transitive.

4. ORDERING BY RESOURCES

Let A be a finite sequence and x be an element. The functor $A \leftarrow x$ yielding a set is defined by the term

(Def. 8) $\bigcap(A^{-1}(\{x\}))$.

Let us consider x. Note that $A \leftarrow x$ is natural.

Let us consider a finite sequence A. Now we state the propositions:

(15) If $x \notin \operatorname{rng} A$, then $A \leftarrow x = 0$.

(16) If $x \in \operatorname{rng} A$, then $A \leftarrow x \in \operatorname{dom} A$ and $x = A(A \leftarrow x)$.

(17) If $A \leftarrow x = 0$, then $x \notin \operatorname{rng} A$.

Let us consider X. Let A be a finite sequence and f be a function. The functor resource(X, A, f) yielding a binary relation on X is defined by

(Def. 9) $x, y \in it$ if and only if x, $y \in X$ and $A \leftarrow (f(x)) \neq 0$ and $A \leftarrow (f(x)) < A \leftarrow (f(y))$ or $A \leftarrow (f(y)) = 0$.

Let us observe that resource(X, A, f) is antisymmetric transitive and β-transitive.

5. Ordering by Number of Iteration

Let us consider X. Let R be a binary relation on X and n be a natural number. One can check that the functor R^n yields a binary relation on X. Now we state the propositions:

(18) If $(R^n)^\circ X = \emptyset$ and $m \geqslant n$, then $(R^m)^\circ X = \emptyset$.

(19) If for every n, $(R^n)^\circ X \neq \emptyset$ and X is finite, then there exists x such that $x \in X$ and for every n, $(R^n)^\circ x \neq \emptyset$. The theorem is a consequence of (18). PROOF: Define $\mathcal{P}$[element, element] $\equiv$ there exists n such that $\$_2 = n$ and $(R^n)^\circ \$_1 = \emptyset$. For every element x such that $x \in X$ there exists an element y such that $y \in \mathbb{N}$ and $\mathcal{P}[x, y]$. Consider f being a function such that $\operatorname{dom} f = X$ and $\operatorname{rng} f \subseteq \mathbb{N}$ and for every element x such that $x \in X$ holds $\mathcal{P}[x, f(x)]$. Consider n such that $\operatorname{rng} f \subseteq \mathbb{Z}_n$. $\{\{x\}$ where x is an element of $X : x \in X\} \subseteq 2^X$. Reconsider $Y = \{\{x\}$ where x is an element of $X : x \in X\}$ as a family of subsets of X. $X = \bigcup Y$. $\{(R^n)^\circ y$ where y is a subset of $X : y \in Y\} \subseteq \{\emptyset\}$. $\square$

(20) If R is reversely well founded and irreflexive and X is finite and R is finite, then there exists n such that $(R^n)^\circ X = \emptyset$. The theorem is a consequence of (19). PROOF: Define $\mathcal{Q}$[element] $\equiv$ for every n, $(R^n)^\circ \$_1 \neq \emptyset$. Consider $x0$ being a set such that $x0 \in X$ and $\mathcal{Q}[x0]$. Define $\mathcal{P}$[element, element, element] $\equiv$ if $\mathcal{Q}[\$_2]$, then $\$_3 \in R^\circ \$_2$ and $\mathcal{Q}[\$_3]$. For every natural number n and for every set x, there exists a set y such that $\mathcal{P}[n, x, y]$. Consider f being a function such that $\operatorname{dom} f = \mathbb{N}$ and $f(0) = x0$ and for every natural number n, $\mathcal{P}[n, f(n), f(n+1)]$. Define $\mathcal{R}$[natural number] $\equiv$ $\mathcal{Q}[f(\$_1)]$. $\operatorname{rng} f \subseteq \operatorname{field} R$. Consider z being an element such that $z \in \operatorname{rng} f$ and for every element x such that $x \in \operatorname{rng} f$ and $z \neq x$ holds $\langle z, x\rangle \notin R$. Consider y being an element such that $y \in \mathbb{N}$ and $z = f(y)$. $\square$

Let us consider X. Let O be an operation of X. Assume O is reversely well founded, irreflexive, and finite. The functor `iteration of` O yielding a binary relation on X is defined by

(Def. 10) There exists a function f from X into $\mathbb{N}$ such that

(i) $it =$ `number of` f, and

(ii) for every element x of X such that $x \in X$ there exists n such that $f(x) = n$ and $x(O^n) \neq \emptyset$ or $n = 0$ and $x(O^n) = \emptyset$ and $x(O^{n+1}) = \emptyset$.

Let us note that every binary relation which is empty is also irreflexive and reversely well founded.

Let us consider X. Let us note that there exists an operation of X which is empty.

Let O be a reversely well founded irreflexive finite operation of X. One can check that `iteration of` O is antisymmetric transitive and β-transitive.

6. `value of` ORDERING

Let X be a finite set. Let us observe that every order in X is well founded.

Note that every connected order in X is well-ordering.

Let us consider X. Let R be a connected order in X and S be a finite subset of X. The functor order(S, R) yielding a finite 0-sequence of X is defined by

(Def. 11) (i) $\operatorname{rng} it = S$, and

(ii) it is one-to-one, and

(iii) for every natural numbers i, j such that i, $j \in \operatorname{dom} it$ holds $i \leqslant j$ iff $it(i), it(j) \in R$.

Now we state the proposition:

(21) Let us consider finite subsets S_1, S_2 of X and a connected order R in X. Then $\operatorname{order}(S_1 \cup S_2, R) = \operatorname{order}(S_1, R) \frown \operatorname{order}(S_2, R)$ if and only if for every x and y such that $x \in S_1$ and $y \in S_2$ holds $x \neq y$ and $x, y \in R$. The theorem is a consequence of (7). PROOF: Set $o1 = \operatorname{order}(S_1, R)$. Set $o2 = \operatorname{order}(S_2, R)$. $\operatorname{order}(S_1, R) \frown \operatorname{order}(S_2, R)$ is one-to-one. □

Let X be a finite set, O be an operation of X, and R be a connected order in X. The functor `value of`(O, R) yielding a binary relation on X is defined by

(Def. 12) Let us consider elements x, y of X. Then $x, y \in it$ if and only if $x(O) \neq \emptyset$ and $y(O) = \emptyset$ or $y(O) \neq \emptyset$ and $(\operatorname{order}(x(O), R))_0, (\operatorname{order}(y(O), R))_0 \in R$ and $(\operatorname{order}(x(O), R))_0 \neq (\operatorname{order}(y(O), R))_0$.

Let R_1 be a connected order in X. One can check that `value of`(O, R_1) is antisymmetric transitive and β-transitive.

REFERENCES

[1] Grzegorz Bancerek. Information retrieval and rendering with MML query. *LNCS*, 4108: 266–279, 2006.

[2] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.

[3] Grzegorz Bancerek. Semantics of MML query. *Formalized Mathematics*, 20(**2**):147–155, 2012. doi:10.2478/v10037-012-0017-x.

[4] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.

[5] Grzegorz Bancerek. Increasing and continuous ordinal sequences. *Formalized Mathematics*, 1(**4**):711–714, 1990.

[6] Grzegorz Bancerek. Reduction relations. *Formalized Mathematics*, 5(**4**):469–478, 1996.

[7] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.

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

[9] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**): 55–65, 1990.

[10] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.

[11] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.

[12] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.

[13] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[14] Krzysztof Hryniewiecki. Relations of tolerance. *Formalized Mathematics*, 2(**1**):105–109, 1991.
[15] Beata Padlewska. Families of sets. *Formalized Mathematics*, 1(**1**):147–152, 1990.
[16] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[17] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1 (**1**):73–83, 1990.
[18] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.
[19] Edmund Woronowicz and Anna Zalewska. Properties of binary relations. *Formalized Mathematics*, 1(**1**):85–89, 1990.

Received December 1, 2012

FORMALIZED MATHEMATICS
Vol. 21, No. 1, Pages 47–53, 2013
DOI: 10.2478/forma-2013-0005

VERSITA
degruyter.com/view/j/forma

A Test for the Stability of Networks

Agnieszka Rowińska-Schwarzweller
Chair of Display Technology
University of Stuttgart
Allmandring 3b, 70596 Stuttgart, Germany

Christoph Schwarzweller
Institute of Computer Science
University of Gdansk
Wita Stwosza 57, 80-952 Gdansk, Poland

Summary. A complex polynomial is called a Hurwitz polynomial, if all its roots have a real part smaller than zero. This kind of polynomial plays an all-dominant role in stability checks of electrical (analog or digital) networks. In this article we prove that a polynomial p can be shown to be Hurwitz by checking whether the rational function $e(p)/o(p)$ can be realized as a reactance of one port, that is as an electrical impedance or admittance consisting of inductors and capacitors. Here $e(p)$ and $o(p)$ denote the even and the odd part of p [25].

MML identifier: `HURWITZ2`, version: `8.1.01 5.8.1171`

The notation and terminology used in this paper have been introduced in the following articles: [16], [14], [2], [3], [10], [4], [5], [22], [19], [21], [15], [1], [6], [17], [11], [12], [13], [18], [8], [26], [23], [20], [24], [9], [27], and [7].

1. Preliminaries

Now we state the propositions:

(1) Let us consider complex numbers x, y. If $\Im(x) = 0$ and $\Re(y) = 0$, then $\Re(\frac{x}{y}) = 0$.

(2) Let us consider a complex number a. Then $a \cdot \overline{a} = |a|^{\mathbf{2}}$.

One can check that there exists a polynomial of $\mathbb{C}_{\mathrm{F}}$ which is Hurwitz and 0 is even.

Now we state the propositions:

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

(3) Let us consider an add-associative right zeroed right complementable associative distributive non empty double loop structure L, an even element k of $\mathbb{N}$, and an element x of L. Then $\mathrm{power}_L(-x,k) = \mathrm{power}_L(x,k)$.

(4) Let us consider an add-associative right zeroed right complementable associative distributive non empty double loop structure L, an odd element k of $\mathbb{N}$, and an element x of L. Then $\mathrm{power}_L(-x,k) = -\mathrm{power}_L(x,k)$. The theorem is a consequence of (3).

(5) Let us consider an even element k of $\mathbb{N}$ and an element x of $\mathbb{C}_{\mathrm{F}}$. If $\Re(x) = 0$, then $\Im(\mathrm{power}_{\mathbb{C}_{\mathrm{F}}}(x,k)) = 0$.

(6) Let us consider an odd element k of $\mathbb{N}$ and an element x of $\mathbb{C}_{\mathrm{F}}$. If $\Re(x) = 0$, then $\Re(\mathrm{power}_{\mathbb{C}_{\mathrm{F}}}(x,k)) = 0$.

2. Even and Odd Part of Polynomials

Let L be a non empty zero structure and p be a sequence of L. The functors the even part of p and the odd part of p yielding sequences of L are defined by the conditions, respectively.

(Def. 1) Let us consider an even natural number i. Then

(i) (the even part of p)$(i) = p(i)$, and

(ii) for every odd natural number i, (the even part of p)$(i) = 0_L$.

(Def. 2) Let us consider an even natural number i. Then

(i) (the odd part of p)$(i) = 0_L$, and

(ii) for every odd natural number i, (the odd part of p)$(i) = p(i)$.

Let p be a polynomial of L. Observe that the even part of p is finite-Support and the odd part of p is finite-Support. Now we state the propositions:

(7) Let us consider a non empty zero structure L. Then

(i) the even part of $\mathbf{0}.L = \mathbf{0}.L$, and

(ii) the odd part of $\mathbf{0}.L = \mathbf{0}.L$.

(8) Let us consider a non empty multiplicative loop with zero structure L. Then

(i) the even part of $\mathbf{1}.L = \mathbf{1}.L$, and

(ii) the odd part of $\mathbf{1}.L = \mathbf{0}.L$.

Let us consider a left zeroed right zeroed non empty additive loop structure L and a polynomial p of L. Now we state the propositions:

(9) (The even part of p) + (the odd part of p) $= p$.

(10) (The odd part of p) + (the even part of p) $= p$.

Let us consider an add-associative right zeroed right complementable non empty additive loop structure L and a polynomial p of L. Now we state the propositions:

(11) $p -$ the odd part of $p =$ the even part of p.

(12) $p -$ the even part of $p =$ the odd part of p.

Let us consider an add-associative right zeroed right complementable Abelian non empty additive loop structure L and a polynomial p of L. Now we state the propositions:

(13) (The even part of p) $- p = -$the odd part of p.

(14) (The odd part of p) $- p = -$the even part of p.

Let us consider an add-associative right zeroed right complementable Abelian non empty additive loop structure L and polynomials p, q of L. Now we state the propositions:

(15) The even part of $p + q =$ (the even part of p) + (the even part of q).

(16) The odd part of $p + q =$ (the odd part of p) + (the odd part of q).

Let us consider a well unital non empty double loop structure L and a polynomial p of L. Now we state the propositions:

(17) Suppose $\deg p$ is even. Then the even part of Leading-Monomial $p =$ Leading-Monomial p.

(18) If $\deg p$ is odd, then the even part of Leading-Monomial $p = \mathbf{0}.L$.

(19) If $\deg p$ is even, then the odd part of Leading-Monomial $p = \mathbf{0}.L$.

(20) Suppose $\deg p$ is odd. Then the odd part of Leading-Monomial $p =$ Leading-Monomial p.

Now we state the proposition:

(21) Let us consider a well unital add-associative right zeroed right complementable Abelian associative distributive non degenerated double loop structure L and a non zero polynomial p of L. Then $\deg$ the even part of $p \neq \deg$ the odd part of p. The theorem is a consequence of (9).

Let us consider a well unital add-associative right zeroed right complementable associative Abelian distributive non degenerated double loop structure L and a polynomial p of L. Now we state the propositions:

(22) (i) $\deg$ the even part of $p \leqslant \deg p$, and

(ii) $\deg$ the odd part of $p \leqslant \deg p$.

(23) $\deg p = \max(\deg$ the even part of $p, \deg$ the odd part of $p)$.

3. Even and Odd Polynomials and Rational Functions

Let L be a non empty additive loop structure and f be a function from L into L. We say that f is even if and only if

(Def. 3) Let us consider an element x of L. Then $f(-x) = f(x)$.

We say that f is odd if and only if

(Def. 4) Let us consider an element x of L. Then $f(-x) = -f(x)$.

Let L be a well unital non empty double loop structure and p be a polynomial of L. We say that p is even if and only if

(Def. 5) Polynomial-Function(L, p) is even.

We say that p is odd if and only if

(Def. 6) Polynomial-Function(L, p) is odd.

Let Z be a rational function of L. We say that Z is odd if and only if

(Def. 7) (i) $Z_{\mathbf{1}}$ is even and $Z_{\mathbf{2}}$ is odd, or

(ii) $Z_{\mathbf{1}}$ is odd and $Z_{\mathbf{2}}$ is even.

We introduce Z is even as an antonym for Z is odd.

Observe that there exists a polynomial of L which is even.

Let L be an add-associative right zeroed right complementable well unital non empty double loop structure. Let us note that there exists a polynomial of L which is odd.

Let L be a well unital add-associative right zeroed right complementable associative non degenerated double loop structure. Observe that there exists a polynomial of L which is non zero and even.

Let L be an add-associative right zeroed right complementable Abelian well unital non degenerated double loop structure. One can verify that there exists a polynomial of L which is non zero and odd.

Now we state the propositions:

(24) Let us consider a well unital non empty double loop structure L, an even polynomial p of L, and an element x of L. Then $\mathrm{eval}(p, -x) = \mathrm{eval}(p, x)$.

(25) Let us consider an add-associative right zeroed right complementable Abelian well unital non degenerated double loop structure L, an odd polynomial p of L, and an element x of L. Then $\mathrm{eval}(p, -x) = -\mathrm{eval}(p, x)$.

Let L be a well unital non empty double loop structure. One can verify that $\mathbf{0}.L$ is even.

Let L be an add-associative right zeroed right complementable well unital non empty double loop structure. One can verify that $\mathbf{0}.L$ is odd.

Let L be a well unital add-associative right zeroed right complementable associative non degenerated double loop structure. Note that $\mathbf{1}.L$ is even.

Let L be an Abelian add-associative right zeroed right complementable well unital left distributive non empty double loop structure and p, q be even polynomials of L. Let us note that $p + q$ is even.

Let p, q be odd polynomials of L. Let us note that $p + q$ is odd.

Let L be an Abelian add-associative right zeroed right complementable associative well unital distributive non degenerated double loop structure and p

be a polynomial of L. One can check that the even part of p is even and the odd part of p is odd.

Now we state the propositions:

(26) Let us consider an Abelian add-associative right zeroed right complementable well unital distributive non degenerated double loop structure L, an even polynomial p of L, an odd polynomial q of L, and an element x of L. If x is a common root of p and q, then $-x$ is a root of $p+q$. The theorem is a consequence of (24) and (25).

(27) Let us consider a Hurwitz polynomial p of $\mathbb{C}_{\mathrm{F}}$. Then the even part of p and the odd part of p have no common roots. The theorem is a consequence of (9) and (26).

4. Real Positive Polynomials and Rational Functions

Let p be a polynomial of $\mathbb{C}_{\mathrm{F}}$. We say that p is real if and only if

(Def. 8) Let us consider a natural number i. Then $p(i)$ is a real number.

We say that p is positive if and only if

(Def. 9) Let us consider an element x of $\mathbb{C}_{\mathrm{F}}$. If $\Re(x) > 0$, then $\Re(\mathrm{eval}(p, x)) > 0$.

Let us note that $\mathbf{0}.\mathbb{C}_{\mathrm{F}}$ is real and non positive and $\mathbf{1}.\mathbb{C}_{\mathrm{F}}$ is real and positive and there exists a polynomial of $\mathbb{C}_{\mathrm{F}}$ which is non zero, real, and positive and every polynomial of $\mathbb{C}_{\mathrm{F}}$ which is real is also real-valued.

Let p be a real polynomial of $\mathbb{C}_{\mathrm{F}}$. One can verify that the even part of p is real and the odd part of p is real.

Let L be a non empty additive loop structure and p be a polynomial of L. We say that p has all coefficients if and only if

(Def. 10) Let us consider a natural number i. If $i \leqslant \deg p$, then $p(i) \neq 0$.

Let p be a real polynomial of $\mathbb{C}_{\mathrm{F}}$. We say that p has positive coefficients if and only if

(Def. 11) Let us consider a natural number i. If $i \leqslant \deg p$, then $p(i) > 0$.

We say that p is negative coefficients if and only if

(Def. 12) Let us consider a natural number i. If $i \leqslant \deg p$, then $p(i) < 0$.

One can check that every real polynomial of $\mathbb{C}_{\mathrm{F}}$ which has positive coefficients has also all coefficients and every real polynomial of $\mathbb{C}_{\mathrm{F}}$ which is negative coefficients has also all coefficients and there exists a real polynomial of $\mathbb{C}_{\mathrm{F}}$ which is non constant and has positive coefficients.

Let p be a non zero real polynomial of $\mathbb{C}_{\mathrm{F}}$ with all coefficients. Let us note that the even part of p is non zero. Note that the odd part of p is non zero.

Let Z be a rational function of $\mathbb{C}_{\mathrm{F}}$. We say that Z is real if and only if

(Def. 13) Let us consider a natural number i. Then

(i) $Z_{\mathbf{1}}(i)$ is a real number, and

(ii) $Z_{\mathbf{2}}(i)$ is a real number.

We say that Z is positive if and only if

(Def. 14) Let us consider an element x of $\mathbb{C}_{\mathrm{F}}$. Suppose

(i) $\Re(x) > 0$, and

(ii) $\mathrm{eval}(Z_{\mathbf{2}}, x) \neq 0$.

Then $\Re(\mathrm{eval}(Z, x)) > 0$.

One can check that there exists a rational function of $\mathbb{C}_{\mathrm{F}}$ which is non zero, odd, real, and positive.

Let p_1 be a real polynomial of $\mathbb{C}_{\mathrm{F}}$ and p_2 be a non zero real polynomial of $\mathbb{C}_{\mathrm{F}}$. Let us note that $\langle p_1, p_2 \rangle$ is real as a rational function of $\mathbb{C}_{\mathrm{F}}$.

5. The Routh-Schur Stability Criterion

A one port function is a real positive rational function of $\mathbb{C}_{\mathrm{F}}$. A reactance one port function is an odd real positive rational function of $\mathbb{C}_{\mathrm{F}}$.

Let us consider a real polynomial p of $\mathbb{C}_{\mathrm{F}}$ and an element x of $\mathbb{C}_{\mathrm{F}}$. Now we state the propositions:

(28) If $\Re(x) = 0$, then $\Im(\mathrm{eval}(\text{the even part of } p, x)) = 0$.

(29) If $\Re(x) = 0$, then $\Re(\mathrm{eval}(\text{the odd part of } p, x)) = 0$.

Now we state the proposition:

(30) Let us consider a non constant real polynomial p of $\mathbb{C}_{\mathrm{F}}$ with positive coefficients. Suppose

(i) $\langle$the even part of p, the odd part of $p\rangle$ is positive, and

(ii) the even part of p and the odd part of p have no common roots.

Then

(iii) for every element x of $\mathbb{C}_{\mathrm{F}}$ such that $\Re(x) = 0$ and $\mathrm{eval}(\text{the odd part of } p, x) \neq 0$ holds $\Re(\mathrm{eval}(\langle\text{the even part of } p, \text{the odd part of } p\rangle, x)) \geqslant 0$, and

(iv) (the even part of p) + (the odd part of p) is Hurwitz.

The theorem is a consequence of (28), (29), and (1).

Now we state the proposition:

(31) Routh-Schur stability criterion (for a single-input, single-output (SISO), linear time invariant (LTI) control system): Let us consider a non constant real polynomial p of $\mathbb{C}_{\mathrm{F}}$ with positive coefficients. Suppose

(i) $\langle$the even part of p, the odd part of $p\rangle$ is a one port function, and

(ii) degree($\langle$the even part of p, the odd part of $p\rangle$) = degree(p).

Then p is Hurwitz. The theorem is a consequence of (23), (30), and (9).

References

[1] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.

[2] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.

[3] Czesław Byliński. The complex numbers. *Formalized Mathematics*, 1(**3**):507–513, 1990.

[4] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**): 55–65, 1990.

[5] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.

[6] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.

[7] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.

[8] Andrzej Kondracki. Basic properties of rational numbers. *Formalized Mathematics*, 1(**5**): 841–845, 1990.

[9] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.

[10] Anna Justyna Milewska. The field of complex numbers. *Formalized Mathematics*, 9(**2**): 265–269, 2001.

[11] Robert Milewski. The ring of polynomials. *Formalized Mathematics*, 9(**2**):339–346, 2001.

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

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

[14] Michał Muzalewski and Wojciech Skaba. From loops to abelian multiplicative groups with zero. *Formalized Mathematics*, 1(**5**):833–840, 1990.

[15] Jan Popiołek. Real normed space. *Formalized Mathematics*, 2(**1**):111–115, 1991.

[16] Piotr Rudnicki and Andrzej Trybulec. Abian's fixed point theorem. *Formalized Mathematics*, 6(**3**):335–338, 1997.

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

[18] Christoph Schwarzweller. Introduction to rational functions. *Formalized Mathematics*, 20 (**2**):181–191, 2012. doi:10.2478/v10037-012-0021-1.

[19] Christoph Schwarzweller and Agnieszka Rowińska-Schwarzweller. Schur's theorem on the stability of networks. *Formalized Mathematics*, 14(**4**):135–142, 2006. doi:10.2478/v10037-006-0017-9.

[20] Andrzej Trybulec and Czesław Byliński. Some properties of real numbers. *Formalized Mathematics*, 1(**3**):445–449, 1990.

[21] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.

[22] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.

[23] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.

[24] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

[25] Rolf Unbehauen. *Netzwerk- und Filtersynthese: Grundlagen und Anwendungen.* Oldenbourg-Verlag, fourth edition, 1993.

[26] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1 (**1**):73–83, 1990.

[27] Hiroshi Yamazaki and Yasunari Shidama. Algebra of vector functions. *Formalized Mathematics*, 3(**2**):171–175, 1992.

Received January 17, 2013

FORMALIZED MATHEMATICS
Vol. 21, No. 1, Pages 55–64, 2013
DOI: 10.2478/forma-2013-0006

VERSITA
degruyter.com/view/j/forma

Relational Formal Characterization of Rough Sets

Adam Grabowski
Institute of Informatics
University of Białystok
Akademicka 2, 15-267 Białystok, Poland

Summary. The notion of a rough set, developed by Pawlak [10], is an important tool to describe situation of incomplete or partially unknown information. In this article, which is essentially the continuation of [6], we try to give the characterization of approximation operators in terms of ordinary properties of underlying relations (some of them, as serial and mediate relations, were not available in the Mizar Mathematical Library). Here we drop the classical equivalence- and tolerance-based models of rough sets [12] trying to formalize some parts of [19] following also [18] in some sense (Propositions 1–8, Corr. 1 and 2; the complete description is available in the Mizar script). Our main problem was that informally, there is a direct correspondence between relations and underlying properties, in our approach however [7], which uses relational structures rather than relations, we had to switch between classical (based on pure set theory) and abstract (using the notion of a structure) parts of the Mizar Mathematical Library. Our next step will be translation of these properties into the pure language of Mizar attributes.

MML identifier: `ROUGHS_2`, version: `8.1.01 5.8.1171`

The notation and terminology used in this paper have been introduced in the following articles: [13], [11], [5], [1], [2], [14], [3], [9], [16], [6], [15], [17], [8], and [4].

1. Preliminaries

One can verify that there exists a relational structure which is non empty and void.

Now we state the propositions:

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

(1) Let us consider a total non empty relational structure R and an element x of R. Then $x \in$ field the internal relation of R.

(2) Let us consider a non empty 1-sorted structure R and a subset X of R. Then $\{x$ where x is an element of $R : \emptyset \subseteq X\} = \Omega_R$. PROOF: $y \in \{x$ where x is an element of $R : \emptyset \subseteq X\}$. $\square$

(3) Let us consider a 1-sorted structure R and a subset X of R. Then $\{x$ where x is an element of $R : \emptyset$ meets $X\} = \emptyset_R$.

2. Missing Ordinary Properties of Binary Relations

Let R be a binary relation and X be a set. We say that R is serial in X if and only if

(Def. 1) Let us consider an element x. Suppose $x \in X$. Then there exists an element y such that

(i) $y \in X$, and

(ii) $\langle x, y\rangle \in R$.

We say that R is serial if and only if

(Def. 2) R is serial in field R.

Let R be a relational structure. We say that R is serial if and only if

(Def. 3) the internal relation of R is serial in the carrier of R.

One can check that every relational structure which is reflexive is also serial.

Let R be a non empty relational structure. One can verify that R is serial if and only if the condition (Def. 4) is satisfied.

(Def. 4) Let us consider an element x of R. Then there exists an element y of R such that $x \leqslant y$.

Let us observe that every relational structure which is total is also serial and every relational structure which is serial is also total.

Let R be a non empty serial relational structure and x be an element of R. Let us note that $[x]_{\text{the internal relation of } R}$ is non empty.

Now we state the proposition:

(4) Let us consider a non empty reflexive relational structure R and an element x of R. Then $x \in [x]_\alpha$, where α is the internal relation of R. The theorem is a consequence of (1).

Let R be a non empty reflexive relational structure and x be an element of R. Note that $[x]_{\text{the internal relation of } R}$ is non empty.

Let R be a binary relation and X be a set. We say that R is mediate in X if and only if

(Def. 5) Let us consider elements x, y. Suppose x, $y \in X$. If $\langle x, y\rangle \in R$, then there exists an element z such that $z \in X$ and $\langle x, z\rangle$, $\langle z, y\rangle \in R$.

We say that R is mediate if and only if

(Def. 6) R is mediate in field R.

Let R be a relational structure. We say that R is mediate if and only if

(Def. 7) the internal relation of R is mediate in the carrier of R.

Let us note that every relational structure which is reflexive is also mediate.

3. Approximations Revisited

Now we state the proposition:

(5) Let us consider a non empty relational structure R and elements a, b of R. Suppose $a \in \mathrm{UAp}(\{b\})$. Then $\langle a, b \rangle \in$ the internal relation of R.

Let R be a non empty relational structure and X be a subset of R. The functor $\mathrm{Uap}\, X$ yielding a subset of R is defined by the term

(Def. 8) $(\mathrm{LAp}(X^{\mathrm{c}}))^{\mathrm{c}}$.

The functor $\mathrm{Lap}\, X$ yielding a subset of R is defined by the term

(Def. 9) $(\mathrm{UAp}(X^{\mathrm{c}}))^{\mathrm{c}}$.

Now we state the propositions:

(6) Let us consider a non empty relational structure R, a subset X of R, and an element x. If $x \in \mathrm{LAp}(X)$, then $[x]_\alpha \subseteq X$, where α is the internal relation of R.

(7) Let us consider a non empty relational structure R, a subset X of R, and a set x. If $x \in \mathrm{UAp}(X)$, then $[x]_\alpha$ meets X, where α is the internal relation of R.

Let us consider a non empty relational structure R and a subset X of R. Now we state the propositions:

(8) $\mathrm{Uap}\, X = \mathrm{UAp}(X)$.

(9) $\mathrm{Lap}\, X = \mathrm{LAp}(X)$.

Let us consider a non empty void relational structure R and a subset X of R. Now we state the propositions:

(10) $\mathrm{LAp}(X) = \Omega_R$.

(11) $\mathrm{UAp}(X) = \emptyset_R$.

4. General Properties of Approximations

Let R be a non empty relational structure. Observe that $\mathrm{LAp}(\Omega_R)$ reduces to Ω_R.

Let R be a non empty serial relational structure. One can check that $\mathrm{UAp}(\Omega_R)$ reduces to Ω_R.

One can check that $\mathrm{LAp}(\emptyset_R)$ reduces to $\emptyset_R$.

Let R be a non empty relational structure. Note that $\mathrm{UAp}(\emptyset_R)$ reduces to $\emptyset_R$.

Let us consider a non empty relational structure R and subsets X, Y of R. Now we state the propositions:

(12) $\mathrm{LAp}(X \cap Y) = \mathrm{LAp}(X) \cap \mathrm{LAp}(Y)$.

(13) $\mathrm{UAp}(X \cup Y) = \mathrm{UAp}(X) \cup \mathrm{UAp}(Y)$.

(14) If $X \subseteq Y$, then $\mathrm{LAp}(X) \subseteq \mathrm{LAp}(Y)$.

(15) If $X \subseteq Y$, then $\mathrm{UAp}(X) \subseteq \mathrm{UAp}(Y)$.

Now we state the propositions:

(16) Let us consider a non empty relational structure R and a subset X of R. Then $\mathrm{LAp}(X^{\mathrm{c}}) = (\mathrm{UAp}(X))^{\mathrm{c}}$.

(17) Let us consider a non empty serial relational structure R and a subset X of R. Then $\mathrm{LAp}(X) \subseteq \mathrm{UAp}(X)$.

5. Auxiliary Operations on Approximation Operators

Let R be a non empty relational structure. The functors $\mathrm{LAp}(R)$ and $\mathrm{UAp}(R)$ yielding functions from $2^{\text{the carrier of } R}$ into $2^{\text{the carrier of } R}$ are defined by the conditions, respectively.

(Def. 10) Let us consider a subset X of R. Then $(\mathrm{LAp}(R))(X) = \mathrm{LAp}(X)$.

(Def. 11) Let us consider a subset X of R. Then $(\mathrm{UAp}(R))(X) = \mathrm{UAp}(X)$.

Let A be a non empty set and U be a function from 2^A into 2^A. We say that U preserves empty set if and only if

(Def. 12) $U(\emptyset) = \emptyset$.

We say that U preserves universe if and only if

(Def. 13) $U(A) = A$.

Observe that id_{2^A} preserves empty set and universe as a function from 2^A into 2^A.

One can verify that there exists a function from 2^A into 2^A which preserves empty set and universe.

Let X be a set and f be a function from 2^X into 2^X. The functor $\mathrm{Flip}\, f$ yielding a function from 2^X into 2^X is defined by

(Def. 14) Let us consider a subset x of X. Then $it(x) = f(x^{\mathrm{c}})^{\mathrm{c}}$.

Let us consider a set X and a function f from 2^X into 2^X. Now we state the propositions:

(18) If $f(\emptyset) = \emptyset$, then $(\mathrm{Flip}\, f)(X) = X$.

(19) If $f(X) = X$, then $(\mathrm{Flip}\, f)(\emptyset) = \emptyset$.

(20) If $f = \mathrm{id}_{2^X}$, then $\mathrm{Flip}\, f = f$.

Let us consider a set X, a function f from 2^X into 2^X, and subsets A, B of X. Now we state the propositions:

(21) If for every subsets A, B of X, $f(A \cup B) = f(A) \cup f(B)$, then $(\mathrm{Flip}\, f)(A \cap B) = (\mathrm{Flip}\, f)(A) \cap (\mathrm{Flip}\, f)(B)$.

(22) If for every subsets A, B of X, $f(A \cap B) = f(A) \cap f(B)$, then $(\mathrm{Flip}\, f)(A \cup B) = (\mathrm{Flip}\, f)(A) \cup (\mathrm{Flip}\, f)(B)$.

Now we state the proposition:

(23) Let us consider a set X and a function f from 2^X into 2^X. Then $\mathrm{Flip}\,\mathrm{Flip}\, f = f$. PROOF: Set $g = \mathrm{Flip}\,\mathrm{Flip}\, f$. For every subset x of X, $g(x) = f(x)$. □

Let A be a non empty set and f be a function from 2^A into 2^A. Observe that $\mathrm{Flip}\, f$ preserves empty set.

Let f be a function from 2^A into 2^A. One can verify that $\mathrm{Flip}\, f$ preserves universe.

Now we state the proposition:

(24) Let us consider a non empty set A and functions L, U from 2^A into 2^A. Suppose

(i) $U = \mathrm{Flip}\, L$, and

(ii) for every subset X of A, $L(L(X)) \subseteq L(X)$.

Let us consider a subset X of A. Then $U(X) \subseteq U(U(X))$.

6. Towards Topological Models of Rough Sets

Let T be a topological space. The functors $\mathrm{ClMap}\, T$ and $\mathrm{IntMap}\, T$ yielding functions from $2^{\text{the carrier of } T}$ into $2^{\text{the carrier of } T}$ are defined by the conditions, respectively.

(Def. 15) Let us consider a subset X of T. Then $(\mathrm{ClMap}\, T)(X) = \overline{X}$.

(Def. 16) Let us consider a subset X of T. Then $(\mathrm{IntMap}\, T)(X) = \mathrm{Int}\, X$.

Let f be a function from $2^{\text{the carrier of } T}$ into $2^{\text{the carrier of } T}$. We say that f is closed-valued if and only if

(Def. 17) Let us consider a subset X of T. Then $f(X)$ is closed.

We say that f is open-valued if and only if

(Def. 18) Let us consider a subset X of T. Then $f(X)$ is open.

Note that $\mathrm{ClMap}\, T$ is closed-valued and $\mathrm{IntMap}\, T$ is open-valued.

Let us observe that there exists a function from $2^{\text{the carrier of } T}$ into $2^{\text{the carrier of } T}$ which is closed-valued and there exists a function from $2^{\text{the carrier of } T}$ into $2^{\text{the carrier of } T}$ which is open-valued.

Let us consider a topological space T. Now we state the propositions:

(25) $\mathrm{Flip}\,\mathrm{ClMap}\, T = \mathrm{IntMap}\, T$.

(26) $\operatorname{Flip}\operatorname{IntMap} T = \operatorname{ClMap} T$.

Let T be a non empty topological space. One can verify that $\operatorname{ClMap} T$ preserves empty set and universe and $\operatorname{IntMap} T$ preserves empty set and universe.

7. Formalization of Zhu's Paper [19]

Let us consider a non empty relational structure R. Now we state the propositions:

(27) $\operatorname{Flip}\operatorname{UAp}(R) = \operatorname{LAp}(R)$.

(28) $\operatorname{Flip}\operatorname{LAp}(R) = \operatorname{UAp}(R)$.

Now we state the proposition:

(29) Let us consider a non empty finite set A and a function U from 2^A into 2^A. Suppose

(i) $U(\emptyset) = \emptyset$, and

(ii) for every subsets X, Y of A, $U(X \cup Y) = U(X) \cup U(Y)$.

Then there exists a non empty finite relational structure R such that

(iii) the carrier of $R = A$, and

(iv) $U = \operatorname{UAp}(R)$.

The theorem is a consequence of (13). Proof: Define $\mathcal{P}[\mathrm{set}, \mathrm{set}] \equiv \$_1 \in L(\{\$_2\})$. Consider R being a binary relation on A such that for every elements x, y of A, $\langle x, y\rangle \in R$ iff $\mathcal{P}[x, y]$. Reconsider $RR = \langle A, R\rangle$ as a non empty finite relational structure. For every element y of RR and for every subset Y of RR such that $Y = \{y\}$ holds $\operatorname{UAp}(Y) = L(Y)$. For every element x such that $x \in \operatorname{dom}\operatorname{UAp}(RR)$ holds $(\operatorname{UAp}(RR))(x) = L(x)$. □

Let us consider a non empty finite set A and a function L from 2^A into 2^A. Now we state the propositions:

(30) Suppose $L(A) = A$ and for every subsets X, Y of A, $L(X \cap Y) = L(X) \cap L(Y)$. Then there exists a non empty finite relational structure R such that

(i) the carrier of $R = A$, and

(ii) $L = \operatorname{LAp}(R)$.

(31) Suppose $L(A) = A$ and $L(\emptyset) = \emptyset$ and for every subsets X, Y of A, $L(X \cap Y) = L(X) \cap L(Y)$. Then there exists a non empty serial relational structure R such that

(i) the carrier of $R = A$, and

(ii) $L = \operatorname{LAp}(R)$.

Now we state the propositions:

(32) Let us consider a non empty finite set A and a function U from 2^A into 2^A. Suppose

(i) $U(A) = A$, and

(ii) $U(\emptyset) = \emptyset$, and

(iii) for every subsets X, Y of A, $U(X \cup Y) = U(X) \cup U(Y)$.

Then there exists a non empty finite serial relational structure R such that

(iv) the carrier of $R = A$, and

(v) $U = \mathrm{UAp}(R)$.

The theorem is a consequence of (29). PROOF: Consider R being a non empty finite relational structure such that the carrier of $R = A$ and $U = \mathrm{UAp}(R)$. For every element x such that $x \in$ the carrier of R there exists an element y such that $y \in$ the carrier of R and $\langle x, y \rangle \in$ the internal relation of R. □

(33) Let us consider a non empty finite set A and a function L from 2^A into 2^A. Suppose

(i) $L(A) = A$, and

(ii) for every subset X of A, $L(X) \subseteq L(X^{\mathrm{c}})^{\mathrm{c}}$, and

(iii) for every subsets X, Y of A, $L(X \cap Y) = L(X) \cap L(Y)$.

Then there exists a non empty finite serial relational structure R such that

(iv) the carrier of $R = A$, and

(v) $L = \mathrm{LAp}(R)$.

The theorem is a consequence of (30). PROOF: Consider R being a non empty finite relational structure such that the carrier of $R = A$ and $L = \mathrm{LAp}(R)$. For every element x such that $x \in$ the carrier of R there exists an element y such that $y \in$ the carrier of R and $\langle x, y \rangle \in$ the internal relation of R. □

(34) Let us consider a non empty finite set A and a function U from 2^A into 2^A. Suppose

(i) $U(\emptyset) = \emptyset$, and

(ii) for every subset X of A, $U(X^{\mathrm{c}})^{\mathrm{c}} \subseteq U(X)$, and

(iii) for every subsets X, Y of A, $U(X \cup Y) = U(X) \cup U(Y)$.

Then there exists a non empty serial relational structure R such that

(iv) the carrier of $R = A$, and

(v) $U = \mathrm{UAp}(R)$.

The theorem is a consequence of (29), (19), and (27). PROOF: Consider R being a non empty finite relational structure such that the carrier of $R = A$ and $U = \mathrm{UAp}(R)$. For every element x such that $x \in$ the carrier of R there exists an element y such that $y \in$ the carrier of R and $\langle x, y \rangle \in$ the internal relation of R. □

Let us consider a non empty reflexive relational structure R and a subset X of R. Now we state the propositions:

(35) $\mathrm{LAp}(X) \subseteq X$.

(36) $X \subseteq \mathrm{UAp}(X)$.

Now we state the propositions:

(37) Let us consider a non empty finite set A and a function U from 2^A into 2^A. Suppose

(i) $U(\emptyset) = \emptyset$, and

(ii) for every subset X of A, $X \subseteq U(X)$, and

(iii) for every subsets X, Y of A, $U(X \cup Y) = U(X) \cup U(Y)$.

Then there exists a non empty finite reflexive relational structure R such that

(iv) the carrier of $R = A$, and

(v) $U = \mathrm{UAp}(R)$.

The theorem is a consequence of (32). PROOF: Consider R being a non empty finite serial relational structure such that the carrier of $R = A$ and $U = \mathrm{UAp}(R)$. For every element x such that $x \in$ the carrier of R holds $\langle x, x \rangle \in$ the internal relation of R. □

(38) Let us consider a non empty finite set A and a function L from 2^A into 2^A. Suppose

(i) $L(A) = A$, and

(ii) for every subset X of A, $L(X) \subseteq X$, and

(iii) for every subsets X, Y of A, $L(X \cap Y) = L(X) \cap L(Y)$.

Then there exists a non empty finite reflexive relational structure R such that

(iv) the carrier of $R = A$, and

(v) $L = \mathrm{LAp}(R)$.

The theorem is a consequence of (19), (22), (37), (23), and (27). PROOF: Set $U = \mathrm{Flip}\, L$. For every subset X of A, $X \subseteq U(X)$. Consider R being a non empty finite reflexive relational structure such that the carrier of $R = A$ and $U = \mathrm{UAp}(R)$. □

Let us consider a non empty mediate relational structure R and a subset X of R. Now we state the propositions:

(39) $\mathrm{UAp}(X) \subseteq \mathrm{UAp}(\mathrm{UAp}(X))$.

(40) $\mathrm{LAp}(\mathrm{LAp}(X)) \subseteq \mathrm{LAp}(X)$.

Now we state the proposition:

(41) Let us consider a non empty finite set A and a function U from 2^A into 2^A. Suppose

(i) $U(\emptyset) = \emptyset$, and

(ii) for every subset X of A, $U(X) \subseteq U(U(X))$, and

(iii) for every subsets X, Y of A, $U(X \cup Y) = U(X) \cup U(Y)$.

Then there exists a non empty mediate finite relational structure R such that

(iv) the carrier of $R = A$, and

(v) $U = \mathrm{UAp}(R)$.

The theorem is a consequence of (29) and (5). PROOF: Consider R being a non empty finite relational structure such that the carrier of $R = A$ and $U = \mathrm{UAp}(R)$. For every elements x, y such that x, $y \in$ the carrier of R holds if $\langle x, y \rangle \in$ the internal relation of R, then there exists an element z such that $z \in$ the carrier of R and $\langle x, z \rangle$, $\langle z, y \rangle \in$ the internal relation of R. □

Let us consider a non empty finite set A and a function L from 2^A into 2^A. Now we state the propositions:

(42) Suppose $L(A) = A$ and for every subset X of A, $L(L(X)) \subseteq L(X)$ and for every subsets X, Y of A, $L(X \cap Y) = L(X) \cap L(Y)$. Then there exists a non empty mediate finite relational structure R such that

(i) the carrier of $R = A$, and

(ii) $L = \mathrm{LAp}(R)$.

(43) Suppose $L(A) = A$ and for every subsets X, Y of A, $L(X \cap Y) = L(X) \cap L(Y)$. Then for every subset X of A, $L(X) \subseteq L(X^{\mathrm{c}})^{\mathrm{c}}$ if and only if $L(\emptyset) = \emptyset$.

Now we state the proposition:

(44) Let us consider a non empty finite set A and a function U from 2^A into 2^A. Suppose

(i) $U(\emptyset) = \emptyset$, and

(ii) for every subsets X, Y of A, $U(X \cup Y) = U(X) \cup U(Y)$.

Then for every subset X of A, $U(X^{\mathrm{c}})^{\mathrm{c}} \subseteq U(X)$ if and only if $U(A) = A$. The theorem is a consequence of (34), (32), (27), and (17).

References

[1] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**): 55–65, 1990.

[2] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.

[3] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.

[4] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.

[5] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.

[6] Adam Grabowski. Basic properties of rough sets and rough membership function. *Formalized Mathematics*, 12(**1**):21–28, 2004.

[7] Adam Grabowski and Magdalena Jastrzębska. A note on a formal approach to rough operators. In Marcin S. Szczuka and Marzena Kryszkiewicz et al., editors, *Rough Sets and Current Trends in Computing – 7th International Conference, RSCTC 2010, Warsaw, Poland, June 28-30, 2010. Proceedings*, volume 6086 of *Lecture Notes in Computer Science*, pages 307–316. Springer, 2010. doi:10.1007/978-3-642-13529-3_33.

[8] Artur Korniłowicz. Cartesian products of relations and relational structures. *Formalized Mathematics*, 6(**1**):145–152, 1997.

[9] Beata Padlewska and Agata Darmochwał. Topological spaces and continuous functions. *Formalized Mathematics*, 1(**1**):223–230, 1990.

[10] Z. Pawlak. Rough sets. *International Journal of Parallel Programming*, 11:341–356, 1982. doi:10.1007/BF01001956.

[11] Konrad Raczkowski and Paweł Sadowski. Equivalence relations and classes of abstraction. *Formalized Mathematics*, 1(**3**):441–444, 1990.

[12] Andrzej Skowron and Jarosław Stepaniuk. Tolerance approximation spaces. *Fundamenta Informaticae*, 27(2/3):245–253, 1996. doi:10.3233/FI-1996-272311.

[13] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**): 115–122, 1990.

[14] Wojciech A. Trybulec and Grzegorz Bancerek. Kuratowski – Zorn lemma. *Formalized Mathematics*, 1(**2**):387–393, 1990.

[15] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

[16] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1 (**1**):73–83, 1990.

[17] Mirosław Wysocki and Agata Darmochwał. Subsets of topological spaces. *Formalized Mathematics*, 1(**1**):231–237, 1990.

[18] Y.Y. Yao. Two views of the theory of rough sets in finite universes. *International Journal of Approximate Reasoning*, 15(4):291–317, 1996. doi:10.1016/S0888-613X(96)00071-0.

[19] William Zhu. Generalized rough sets based on relations. *Information Sciences*, 177: 4997–5011, 2007.

Received January 17, 2013

FORMALIZED MATHEMATICS
Vol. 21, No. 1, Pages 65–74, 2013
DOI: 10.2478/forma-2013-0007

VERSITA
degruyter.com/view/j/forma

Isomorphisms of Direct Products of Finite Commutative Groups[1]

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Hiroshi Yamazaki
Shinshu University
Nagano, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. We have been working on the formalization of groups. In [1], we encoded some theorems concerning the product of cyclic groups. In this article, we present the generalized formalization of [1]. First, we show that every finite commutative group which order is composite number is isomorphic to a direct product of finite commutative groups which orders are relatively prime. Next, we describe finite direct products of finite commutative groups.

MML identifier: GROUP_17, version: 8.1.01 5.9.1172

The notation and terminology used in this paper have been introduced in the following articles: [2], [3], [19], [7], [13], [20], [8], [9], [10], [23], [24], [25], [26], [27], [14], [22], [17], [4], [5], [15], [16], [6], [11], [21], [18], [29], [28], and [12].

1. Preliminaries

Now we state the propositions:

(1) Let us consider sets A, B, A_1, B_1. Suppose

(i) A misses B, and

(ii) $A_1 \subseteq A$, and

(iii) $B_1 \subseteq B$, and

(iv) $A_1 \cup B_1 = A \cup B$.

Then

[1]The 1st author was supported by JSPS KAKENHI 21240001, and the 3rd author was supported by JSPS KAKENHI 22300285.

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

(v) $A_1 = A$, and

(vi) $B_1 = B$.

PROOF: $A \subseteq A_1$. $B \subseteq B_1$. □

(2) Let us consider non empty finite sets H, K. Then $\overline{\overline{\prod \langle H, K \rangle}} = \overline{\overline{H}} \cdot \overline{\overline{K}}$.

Let us consider bags p_2, p_1, f of Prime and a natural number q. Now we state the propositions:

(3) If $\operatorname{support} p_2$ misses $\operatorname{support} p_1$ and $f = p_2 + p_1$ and $q \in \operatorname{support} p_2$, then $p_2(q) = f(q)$.

(4) If $\operatorname{support} p_2$ misses $\operatorname{support} p_1$ and $f = p_2 + p_1$ and $q \in \operatorname{support} p_1$, then $p_1(q) = f(q)$.

Now we state the propositions:

(5) Let us consider a non zero natural number h and a prime number q. If q and h are not relatively prime, then $q \mid h$.

(6) Let us consider non zero natural numbers h, s. Suppose a prime number q. Suppose $q \in \operatorname{support} \operatorname{PrimeFactorization}(s)$. Then q and h are not relatively prime. Then $\operatorname{support} \operatorname{PrimeFactorization}(s) \subseteq \operatorname{support} \operatorname{PrimeFactorization}(h)$. The theorem is a consequence of (5).

(7) Let us consider non zero natural numbers h, k, s, t. Suppose

(i) h and k are relatively prime, and

(ii) $s \cdot t = h \cdot k$, and

(iii) for every prime number q such that $q \in \operatorname{support} \operatorname{PrimeFactorization}(s)$ holds q and h are not relatively prime, and

(iv) for every prime number q such that $q \in \operatorname{support} \operatorname{PrimeFactorization}(t)$ holds q and k are not relatively prime.

Then

(v) $s = h$, and

(vi) $t = k$.

The theorem is a consequence of (6), (1), (3), and (4). PROOF: Set $p_2 = \operatorname{PrimeFactorization}(s)$. Set $p_1 = \operatorname{PrimeFactorization}(t)$. For every natural number p such that $p \in \operatorname{support} \operatorname{PFExp}(h)$ holds $p_2(p) = p^{p\text{-}\operatorname{count}(h)}$. For every natural number p such that $p \in \operatorname{support} \operatorname{PFExp}(k)$ holds $p_1(p) = p^{p\text{-}\operatorname{count}(k)}$. □

Let G be a non empty multiplicative magma, I be a finite set, and b be a (the carrier of G)-valued total I-defined function. The functor $\prod b$ yielding an element of G is defined by

(Def. 1) There exists a finite sequence f of elements of G such that

(i) $it = \prod f$, and

(ii) $f = b \cdot \mathrm{CFS}(I)$.

Now we state the propositions:

(8) Let us consider a commutative group G, non empty finite sets A, B, a (the carrier of G)-valued total A-defined function F_3, a (the carrier of G)-valued total B-defined function F_2, and a (the carrier of G)-valued total $A \cup B$-defined function F_1. Suppose

(i) A misses B, and

(ii) $F_1 = F_3 + \cdot F_2$.

Then $\prod F_1 = \prod F_3 \cdot \prod F_2$.

(9) Let us consider a non empty multiplicative magma G, a set q, an element z of G, and a (the carrier of G)-valued total $\{q\}$-defined function f. If $f = q \longmapsto z$, then $\prod f = z$.

2. Direct Product of Finite Commutative Groups

Now we state the propositions:

(10) Let us consider non empty multiplicative magmas X, Y. Then the carrier of $\prod\langle X, Y\rangle = \prod\langle$the carrier of X, the carrier of $Y\rangle$. PROOF: Set $CarrX =$ the carrier of X. Set $CarrY =$ the carrier of Y. For every element a such that $a \in$ dom the support of $\langle X, Y\rangle$ holds (the support of $\langle X, Y\rangle)(a) = \langle$the carrier of X, the carrier of $Y\rangle(a)$. □

(11) Let us consider a group G and normal subgroups A, B of G. Suppose (the carrier of A) $\cap$ (the carrier of B) $= \{\mathbf{1}_G\}$. Let us consider elements a, b of G. If $a \in A$ and $b \in B$, then $a \cdot b = b \cdot a$.

(12) Let us consider a group G and normal subgroups A, B of G. Suppose

(i) for every element x of G, there exist elements a, b of G such that $a \in A$ and $b \in B$ and $x = a \cdot b$, and

(ii) (the carrier of A) $\cap$ (the carrier of B) $= \{\mathbf{1}_G\}$.

Then there exists a homomorphism h from $\prod\langle A, B\rangle$ to G such that

(iii) h is bijective, and

(iv) for every elements a, b of G such that $a \in A$ and $b \in B$ holds $h(\langle a, b\rangle) = a \cdot b$.

The theorem is a consequence of (11). PROOF: Define $\mathcal{P}[\mathrm{set}, \mathrm{set}] \equiv$ there exists an element x of G and there exists an element y of G such that $x \in A$ and $y \in B$ and $\$_1 = \langle x, y\rangle$ and $\$_2 = x \cdot y$. For every element z of $\prod\langle A, B\rangle$, there exists an element w of G such that $\mathcal{P}[z, w]$. Consider h being a function from $\prod\langle A, B\rangle$ into G such that for every element z of $\prod\langle A, B\rangle$, $\mathcal{P}[z, h(z)]$. For every elements a, b of G such that $a \in A$ and $b \in B$ holds

$h(\langle a, b\rangle) = a \cdot b$. For every elements z, w of $\prod\langle A, B\rangle$, $h(z \cdot w) = h(z) \cdot h(w)$. □

Let us consider a finite commutative group G, a natural number m, and a subset A of G. Now we state the propositions:

(13) Suppose $A = \{x$ where x is an element of $G : x^m = \mathbf{1}_G\}$. Then

(i) $A \neq \emptyset$, and

(ii) for every elements g_1, g_2 of G such that g_1, $g_2 \in A$ holds $g_1 \cdot g_2 \in A$, and

(iii) for every element g of G such that $g \in A$ holds $g^{-1} \in A$.

(14) Suppose $A = \{x$ where x is an element of $G : x^m = \mathbf{1}_G\}$. Then there exists a strict finite subgroup H of G such that

(i) the carrier of $H = A$, and

(ii) H is commutative and normal.

Now we state the propositions:

(15) Let us consider a finite commutative group G, a natural number m, and a finite subgroup H of G. Suppose the carrier of $H = \{x$ where x is an element of $G : x^m = \mathbf{1}_G\}$. Let us consider a prime number q. Suppose $q \in$ support PrimeFactorization$(\overline{\overline{H}})$. Then q and m are not relatively prime.

(16) Let us consider a finite commutative group G and natural numbers h, k. Suppose

(i) $\overline{\overline{G}} = h \cdot k$, and

(ii) h and k are relatively prime.

Then there exist strict finite subgroups H, K of G such that

(iii) the carrier of $H = \{x$ where x is an element of $G : x^h = \mathbf{1}_G\}$, and

(iv) the carrier of $K = \{x$ where x is an element of $G : x^k = \mathbf{1}_G\}$, and

(v) H is normal, and

(vi) K is normal, and

(vii) for every element x of G, there exist elements a, b of G such that $a \in H$ and $b \in K$ and $x = a \cdot b$, and

(viii) (the carrier of H) $\cap$ (the carrier of K) $= \{\mathbf{1}_G\}$.

The theorem is a consequence of (14). PROOF: Set $A = \{x$ where x is an element of $G : x^h = \mathbf{1}_G\}$. Set $B = \{x$ where x is an element of $G : x^k = \mathbf{1}_G\}$. $A \subseteq$ the carrier of G. $B \subseteq$ the carrier of G. Consider H being a strict finite subgroup of G such that the carrier of $H = A$ and H is commutative and H is normal. Consider K being a strict finite subgroup of G such that the carrier of $K = B$ and K is

normal. Consider a, b being integers such that $a \cdot h + b \cdot k = 1$. (The carrier of H) $\cap$ (the carrier of K) $\subseteq \{\mathbf{1}_G\}$. For every element x of G, there exist elements s, t of G such that $s \in H$ and $t \in K$ and $x = s \cdot t$. $\square$

(17) Let us consider finite groups H, K. Then $\overline{\overline{\prod \langle H, K \rangle}} = \overline{\overline{H}} \cdot \overline{\overline{K}}$. The theorem is a consequence of (10) and (2).

(18) Let us consider a finite commutative group G and non zero natural numbers h, k. Suppose

(i) $\overline{\overline{G}} = h \cdot k$, and

(ii) h and k are relatively prime.

Then there exist strict finite subgroups H, K of G such that

(iii) $\overline{\overline{H}} = h$, and

(iv) $\overline{\overline{K}} = k$, and

(v) (the carrier of H) $\cap$ (the carrier of K) $= \{\mathbf{1}_G\}$, and

(vi) there exists a homomorphism F from $\prod \langle H, K \rangle$ to G such that F is bijective and for every elements a, b of G such that $a \in H$ and $b \in K$ holds $F(\langle a, b \rangle) = a \cdot b$.

The theorem is a consequence of (16), (12), (17), (15), and (7).

3. Finite Direct Products of Finite Commutative Groups

Let us consider a group G, a set q, an associative group-like multiplicative magma family F of $\{q\}$, and a function f from G into $\prod F$. Now we state the propositions:

(19) If $F = q \mapsto G$ and for every element x of G, $f(x) = q \mapsto x$, then f is a homomorphism from G to $\prod F$.

(20) If $F = q \mapsto G$ and for every element x of G, $f(x) = q \mapsto x$, then f is bijective.

Now we state the propositions:

(21) Let us consider a set q, an associative group-like multiplicative magma family F of $\{q\}$, and a group G. Suppose $F = q \mapsto G$. Then there exists a homomorphism I from G to $\prod F$ such that

(i) I is bijective, and

(ii) for every element x of G, $I(x) = q \mapsto x$.

The theorem is a consequence of (19) and (20). PROOF: Define $\mathcal{P}[\text{set}, \text{set}] \equiv \$_2 = q \mapsto \$_1$. For every element z of G, there exists an element w of $\prod F$ such that $\mathcal{P}[z, w]$. Consider I being a function from G into $\prod F$ such that for every element x of G, $\mathcal{P}[x, I(x)]$. $\square$

(22) Let us consider non empty finite sets I_0, I, an associative group-like multiplicative magma family F_0 of I_0, an associative group-like multiplicative magma family F of I, groups H, K, an element q of I, an element k of K, and a function g. Suppose

(i) $g \in$ the carrier of $\prod F_0$, and

(ii) $q \notin I_0$, and

(iii) $I = I_0 \cup \{q\}$, and

(iv) $F = F_0 +\cdot (q \mapsto K)$.

Then $g +\cdot (q \mapsto k) \in$ the carrier of $\prod F$. PROOF: Set $HK = \langle H, K \rangle$. Set $w = g +\cdot (q \mapsto k)$. For every element x such that $x \in \operatorname{dom}$ the support of F holds $w(x) \in$ (the support of F)(x). □

Let us consider non empty finite sets I_0, I, an associative group-like multiplicative magma family F_0 of I_0, an associative group-like multiplicative magma family F of I, groups H, K, an element q of I, a function G_0 from H into $\prod F_0$, and a function G from $\prod \langle H, K \rangle$ into $\prod F$. Now we state the propositions:

(23) Suppose G_0 is a homomorphism from H to $\prod F_0$ and G_0 is bijective and $q \notin I_0$ and $I = I_0 \cup \{q\}$ and $F = F_0 +\cdot (q \mapsto K)$. Then suppose for every element h of H and for every element k of K, there exists a function g such that $g = G_0(h)$ and $G(\langle h, k \rangle) = g +\cdot (q \mapsto k)$. Then G is a homomorphism from $\prod \langle H, K \rangle$ to $\prod F$.

(24) Suppose G_0 is a homomorphism from H to $\prod F_0$ and G_0 is bijective and $q \notin I_0$ and $I = I_0 \cup \{q\}$ and $F = F_0 +\cdot (q \mapsto K)$. Then suppose for every element h of H and for every element k of K, there exists a function g such that $g = G_0(h)$ and $G(\langle h, k \rangle) = g +\cdot (q \mapsto k)$. Then G is bijective.

Now we state the propositions:

(25) Let us consider a set q, a multiplicative magma family F of $\{q\}$, and a non empty multiplicative magma G. Suppose $F = q \mapsto G$. Let us consider a (the carrier of G)-valued total $\{q\}$-defined function y. Then

(i) $y \in$ the carrier of $\prod F$, and

(ii) $y(q) \in$ the carrier of G, and

(iii) $y = q \mapsto y(q)$.

(26) Let us consider a set q, an associative group-like multiplicative magma family F of $\{q\}$, and a group G. Suppose $F = q \mapsto G$. Then there exists a homomorphism H_0 from $\prod F$ to G such that

(i) H_0 is bijective, and

(ii) for every (the carrier of G)-valued total $\{q\}$-defined function x, $H_0(x) = \prod x$.

The theorem is a consequence of (21), (25), and (9). PROOF: Consider I being a homomorphism from G to $\prod F$ such that I is bijective and for every element x of G, $I(x) = q\mapsto x$. Set $H_0 = I^{-1}$. For every (the carrier of G)-valued total $\{q\}$-defined function y, $H_0(y) = \prod y$. $\square$

(27) Let us consider non empty finite sets I_0, I, an associative group-like multiplicative magma family F_0 of I_0, an associative group-like multiplicative magma family F of I, groups H, K, an element q of I, and a homomorphism G_0 from H to $\prod F_0$. Suppose

(i) $q \notin I_0$, and

(ii) $I = I_0 \cup \{q\}$, and

(iii) $F = F_0 +\cdot (q\mapsto K)$, and

(iv) G_0 is bijective.

Then there exists a homomorphism G from $\prod\langle H, K\rangle$ to $\prod F$ such that

(v) G is bijective, and

(vi) for every element h of H and for every element k of K, there exists a function g such that $g = G_0(h)$ and $G(\langle h, k\rangle) = g +\cdot (q\mapsto k)$.

The theorem is a consequence of (22), (23), and (24). PROOF: Set $HK = \langle H, K\rangle$. Define $\mathcal{P}[\mathrm{set}, \mathrm{set}] \equiv$ there exists an element h of H and there exists an element k of K and there exists a function g such that $\$_1 = \langle h, k\rangle$ and $g = G_0(h)$ and $\$_2 = g +\cdot (q\mapsto k)$. For every element z of $\prod\langle H, K\rangle$, there exists an element w of the carrier of $\prod F$ such that $\mathcal{P}[z, w]$. Consider G being a function from $\prod\langle H, K\rangle$ into $\prod F$ such that for every element x of $\prod\langle H, K\rangle$, $\mathcal{P}[x, G(x)]$. For every element h of H and for every element k of K, there exists a function g such that $g = G_0(h)$ and $G(\langle h, k\rangle) = g +\cdot (q\mapsto k)$. $\square$

(28) Let us consider non empty finite sets I_0, I, an associative group-like multiplicative magma family F_0 of I_0, an associative group-like multiplicative magma family F of I, groups H, K, an element q of I, and a homomorphism G_0 from $\prod F_0$ to H. Suppose

(i) $q \notin I_0$, and

(ii) $I = I_0 \cup \{q\}$, and

(iii) $F = F_0 +\cdot (q\mapsto K)$, and

(iv) G_0 is bijective.

Then there exists a homomorphism G from $\prod F$ to $\prod\langle H, K\rangle$ such that

(v) G is bijective, and

(vi) for every function x_0 and for every element k of K and for every element h of H such that $h = G_0(x_0)$ and $x_0 \in \prod F_0$ holds $G(x_0 +\cdot (q\mapsto k)) = \langle h, k\rangle$.

The theorem is a consequence of (27). PROOF: Set $L0 = {G_0}^{-1}$. Consider L being a homomorphism from $\prod\langle H, K\rangle$ to $\prod F$ such that L is bijective and for every element h of H and for every element k of K, there exists a function g such that $g = L0(h)$ and $L(\langle h, k\rangle) = g{+}\cdot(q \mapsto k)$. Set $G = L^{-1}$. For every function x_0 and for every element k of K and for every element h of H such that $h = G_0(x_0)$ and $x_0 \in \prod F_0$ holds $G(x_0{+}\cdot(q \mapsto k)) = \langle h, k\rangle$. $\square$

(29) Let us consider a non empty finite set I, an associative group-like multiplicative magma family F of I, and a total I-defined function x. Suppose an element p of I. Then $x(p) \in F(p)$. Then $x \in$ the carrier of $\prod F$.

(30) Let us consider non empty finite sets I_0, I, an associative group-like multiplicative magma family F_0 of I_0, an associative group-like multiplicative magma family F of I, a group K, an element q of I, and an element x of $\prod F$. Suppose

(i) $q \notin I_0$, and

(ii) $I = I_0 \cup \{q\}$, and

(iii) $F = F_0{+}\cdot(q \mapsto K)$.

Then there exists a total I_0-defined function x_0 and there exists an element k of K such that $x_0 \in \prod F_0$ and $x = x_0{+}\cdot(q \mapsto k)$ and for every element p of I_0, $x_0(p) \in F_0(p)$. PROOF: Reconsider $y = x$ as a total I-defined function. Reconsider $k = y(q)$ as an element of K. Reconsider $y0 = y{\restriction}I_0$ as an I_0-defined function. For every element i of I_0, $y0(i) \in$ (the support of F_0)(i) and $y0(i) \in F_0(i)$. $\square$

(31) Let us consider a group G, a subgroup H of G, a finite sequence f of elements of G, and a finite sequence g of elements of H. If $f = g$, then $\prod f = \prod g$. PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every finite sequence f of elements of G for every finite sequence g of elements of H such that $\$_1 = \operatorname{len} f$ and $f = g$ holds $\prod f = \prod g$. $\mathcal{P}[0]$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. $\square$

(32) Let us consider a non empty finite set I, a group G, a subgroup H of G, a (the carrier of G)-valued total I-defined function x, and a (the carrier of H)-valued total I-defined function x_0. If $x = x_0$, then $\prod x = \prod x_0$. The theorem is a consequence of (31).

(33) Let us consider a commutative group G, non empty finite sets I_0, I, an element q of I, a (the carrier of G)-valued total I-defined function x, a (the carrier of G)-valued total I_0-defined function x_0, and an element k of G. Suppose

(i) $q \notin I_0$, and

(ii) $I = I_0 \cup \{q\}$, and

(iii) $x = x_0 + \cdot (q \mapsto k)$.

Then $\prod x = \prod x_0 \cdot k$. The theorem is a consequence of (8) and (9). PROOF: Reconsider $y = q \mapsto k$ as a (the carrier of G)-valued total $\{q\}$-defined function. I_0 misses $\{q\}$. □

Let us consider a finite commutative group G. Now we state the propositions:

(34) Suppose $\overline{\overline{G}} > 1$. Then there exists a non empty finite set I and there exists an associative group-like commutative multiplicative magma family F of I and there exists a homomorphism H_0 from $\prod F$ to G such that $I = \operatorname{support} \operatorname{PrimeFactorization}(\overline{\overline{G}})$ and for every element p of I, $F(p)$ is a subgroup of G and $\overline{\overline{F(p)}} = (\operatorname{PrimeFactorization}(\overline{\overline{G}}))(p)$ and for every elements p, q of I such that $p \neq q$ holds (the carrier of $F(p)) \cap$ (the carrier of $F(q)) = \{\mathbf{1}_G\}$ and H_0 is bijective and for every (the carrier of G)-valued total I-defined function x such that for every element p of I, $x(p) \in F(p)$ holds $x \in \prod F$ and $H_0(x) = \prod x$.

(35) Suppose $\overline{\overline{G}} > 1$. Then there exists a non empty finite set I and there exists an associative group-like commutative multiplicative magma family F of I such that $I = \operatorname{support} \operatorname{PrimeFactorization}(\overline{\overline{G}})$ and for every element p of I, $F(p)$ is a subgroup of G and $\overline{\overline{F(p)}} = (\operatorname{PrimeFactorization}(\overline{\overline{G}}))(p)$ and for every elements p, q of I such that $p \neq q$ holds (the carrier of $F(p)) \cap$ (the carrier of $F(q)) = \{\mathbf{1}_G\}$ and for every element y of G, there exists a (the carrier of G)-valued total I-defined function x such that for every element p of I, $x(p) \in F(p)$ and $y = \prod x$ and for every (the carrier of G)-valued total I-defined functions x_1, x_2 such that for every element p of I, $x_1(p) \in F(p)$ and for every element p of I, $x_2(p) \in F(p)$ and $\prod x_1 = \prod x_2$ holds $x_1 = x_2$.

REFERENCES

[1] Kenichi Arai, Hiroyuki Okazaki, and Yasunari Shidama. Isomorphisms of direct products of finite cyclic groups. *Formalized Mathematics*, 20(**4**):343–347, 2012. doi:10.2478/v10037-012-0038-5.

[2] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.

[3] Grzegorz Bancerek. König's theorem. *Formalized Mathematics*, 1(**3**):589–593, 1990.

[4] Grzegorz Bancerek. Monoids. *Formalized Mathematics*, 3(**2**):213–225, 1992.

[5] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.

[6] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.

[7] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.

[8] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**): 55–65, 1990.

[9] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.

[10] Czesław Byliński. The modification of a function by a function and the iteration of the composition of a function. *Formalized Mathematics*, 1(**3**):521–527, 1990.

[11] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.

[12] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[13] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[14] Artur Korniłowicz. The product of the families of the groups. *Formalized Mathematics*, 7(**1**):127–134, 1998.
[15] Artur Korniłowicz and Piotr Rudnicki. Fundamental Theorem of Arithmetic. *Formalized Mathematics*, 12(**2**):179–186, 2004.
[16] Rafał Kwiatek. Factorial and Newton coefficients. *Formalized Mathematics*, 1(**5**):887–890, 1990.
[17] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relatively primes. *Formalized Mathematics*, 1(**5**):829–832, 1990.
[18] Beata Madras. Product of family of universal algebras. *Formalized Mathematics*, 4(**1**): 103–108, 1993.
[19] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**): 115–122, 1990.
[20] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1 (**2**):329–334, 1990.
[21] Andrzej Trybulec. Many sorted sets. *Formalized Mathematics*, 4(**1**):15–22, 1993.
[22] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[23] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.
[24] Wojciech A. Trybulec. Subgroup and cosets of subgroups. *Formalized Mathematics*, 1(**5**): 855–864, 1990.
[25] Wojciech A. Trybulec. Classes of conjugation. Normal subgroups. *Formalized Mathematics*, 1(**5**):955–962, 1990.
[26] Wojciech A. Trybulec. Lattice of subgroups of a group. Frattini subgroup. *Formalized Mathematics*, 2(**1**):41–47, 1991.
[27] Wojciech A. Trybulec and Michał J. Trybulec. Homomorphisms and isomorphisms of groups. Quotient group. *Formalized Mathematics*, 2(**4**):573–578, 1991.
[28] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[29] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1 (**1**):73–83, 1990.

Received January 31, 2013