FORMALIZED MATHEMATICS
Vol.1, No.**4**, September–October 1990
Université Catholique de Louvain

Binary Operations Applied to Finite Sequences

Czesław Byliński[1]
Warsaw University
Białystok

Summary. The article contains some propositions and theorems related to [7] and [4]. The notions introduced in [7] are extended to finite sequences. A number additional propositions related to this notions are proved. There are also proved some properties of distributive operations and unary operations. The notation and propositions for inverses are introduced.

MML Identifier: `FINSEQOP`.

The notation and terminology used in this paper are introduced in the following articles: [9], [1], [5], [3], [2], [6], [7], [4], and [8]. For simplicity we adopt the following convention: x, y will be arbitrary, C, C', D, D', E will be non-empty sets, c will be an element of C, c' will be an element of C', d, d_1, d_2, d_3, d_4, e will be elements of D, and d' will be an element of D'. Next we state several propositions:

(1) For every function f holds $\langle \Box, f \rangle = \Box$ and $\langle f, \Box \rangle = \Box$.

(2) For every function f holds $[\!:\Box, f:\!] = \Box$ and $[\!: f, \Box :\!] = \Box$.

(3) $(C \longmapsto d)(c) = d$.

(4) For all functions F, f holds $F^{\circ}(\Box, f) = \Box$ and $F^{\circ}(f, \Box) = \Box$.

(5) For every function F holds $F^{\circ}(\Box, x) = \Box$.

(6) For every function F holds $F^{\circ}(x, \Box) = \Box$.

(7) For every set X and for arbitrary x_1, x_2 holds $\langle X \longmapsto x_1, X \longmapsto x_2 \rangle = X \longmapsto \langle\!\langle x_1, x_2 \rangle\!\rangle$.

(8) For every function F and for every set X and for arbitrary x_1, x_2 such that $\langle\!\langle x_1, x_2 \rangle\!\rangle \in \mathrm{dom}\, F$ holds $F^{\circ}(X \longmapsto x_1, X \longmapsto x_2) = X \longmapsto F(\langle\!\langle x_1, x_2 \rangle\!\rangle)$.

[1] Supported by RPBP.III-24.C1.

ISSN 0777–4028

For simplicity we adopt the following rules: i, j will denote natural numbers, F will denote a function from $[: D, D' :]$ into E, p, q will denote finite sequences of elements of D, and p', q' will denote finite sequences of elements of D'. Let us consider D, D', E, F, p, p'. Then $F^\circ(p, p')$ is a finite sequence of elements of E.

Let us consider D, D', E, F, p, d'. Then $F^\circ(p, d')$ is a finite sequence of elements of E.

Let us consider D, D', E, F, d, p'. Then $F^\circ(d, p')$ is a finite sequence of elements of E.

Let us consider D, i, d. Then $i \longmapsto d$ is an element of D^i.

In the sequel f, f' are functions from C into D and h is a function from D into E. Let us consider D, E, p, h. Then $h \cdot p$ is a finite sequence of elements of E.

Next we state two propositions:

(9) $h \cdot (p \frown \langle d \rangle) = (h \cdot p) \frown \langle h(d) \rangle$.

(10) $h \cdot (p \frown q) = (h \cdot p) \frown (h \cdot q)$.

For simplicity we follow a convention: T, T_1, T_2, T_3 denote elements of D^i, T' denotes an element of D'^i, S denotes an element of D^j, and S' denotes an element of D'^j. Next we state a number of propositions:

(11) $F^\circ(T \frown \langle d \rangle, T' \frown \langle d' \rangle) = F^\circ(T, T') \frown \langle F(d, d') \rangle$.

(12) $F^\circ(T \frown S, T' \frown S') = F^\circ(T, T') \frown F^\circ(S, S')$.

(13) $F^\circ(d, p' \frown \langle d' \rangle) = F^\circ(d, p') \frown \langle F(d, d') \rangle$.

(14) $F^\circ(d, p' \frown q') = F^\circ(d, p') \frown F^\circ(d, q')$.

(15) $F^\circ(p \frown \langle d \rangle, d') = F^\circ(p, d') \frown \langle F(d, d') \rangle$.

(16) $F^\circ(p \frown q, d') = F^\circ(p, d') \frown F^\circ(q, d')$.

(17) For every function h from D into E holds $h \cdot (i \longmapsto d) = i \longmapsto h(d)$.

(18) $F^\circ(i \longmapsto d, i \longmapsto d') = i \longmapsto F(d, d')$.

(19) $F^\circ(d, i \longmapsto d') = i \longmapsto F(d, d')$.

(20) $F^\circ(i \longmapsto d, d') = i \longmapsto F(d, d')$.

(21) $F^\circ(i \longmapsto d, T') = F^\circ(d, T')$.

(22) $F^\circ(T, i \longmapsto d) = F^\circ(T, d)$.

(23) $F^\circ(d, T') = F^\circ(d, \mathrm{id}_{D'}) \cdot T'$.

(24) $F^\circ(T, d) = F^\circ(\mathrm{id}_D, d) \cdot T$.

In the sequel F, G are binary operations on D, u is a unary operation on D, and H is a binary operation on E. One can prove the following propositions:

(25) If F is associative, then $F^\circ(d, \mathrm{id}_D) \cdot F^\circ(f, f') = F^\circ(F^\circ(d, \mathrm{id}_D) \cdot f, f')$.

(26) If F is associative, then $F^\circ(\mathrm{id}_D, d) \cdot F^\circ(f, f') = F^\circ(f, F^\circ(\mathrm{id}_D, d) \cdot f')$.

(27) If F is associative, then $F^\circ(d, \mathrm{id}_D) \cdot F^\circ(T_1, T_2) = F^\circ(F^\circ(d, \mathrm{id}_D) \cdot T_1, T_2)$.

(28) If F is associative, then $F^\circ(\mathrm{id}_D, d) \cdot F^\circ(T_1, T_2) = F^\circ(T_1, F^\circ(\mathrm{id}_D, d) \cdot T_2)$.

(29) If F is associative, then $F^\circ(F^\circ(T_1, T_2), T_3) = F^\circ(T_1, F^\circ(T_2, T_3))$.

(30) If F is associative, then $F^\circ(F^\circ(d_1, T), d_2) = F^\circ(d_1, F^\circ(T, d_2))$.

(31) If F is associative, then $F^\circ(F^\circ(T_1, d), T_2) = F^\circ(T_1, F^\circ(d, T_2))$.

(32) If F is associative, then $F^\circ(F(d_1, d_2), T) = F^\circ(d_1, F^\circ(d_2, T))$.

(33) If F is associative, then $F^\circ(T, F(d_1, d_2)) = F^\circ(F^\circ(T, d_1), d_2)$.

(34) If F is commutative, then $F^\circ(T_1, T_2) = F^\circ(T_2, T_1)$.

(35) If F is commutative, then $F^\circ(d, T) = F^\circ(T, d)$.

(36) If F is distributive w.r.t. G, then $F^\circ(G(d_1, d_2), f) = G^\circ(F^\circ(d_1, f), F^\circ(d_2, f))$.

(37) If F is distributive w.r.t. G, then $F^\circ(f, G(d_1, d_2)) = G^\circ(F^\circ(f, d_1), F^\circ(f, d_2))$.

(38) If for all d_1, d_2 holds $h(F(d_1, d_2)) = H(h(d_1), h(d_2))$, then $h \cdot F^\circ(f, f') = H^\circ(h \cdot f, h \cdot f')$.

(39) If for all d_1, d_2 holds $h(F(d_1, d_2)) = H(h(d_1), h(d_2))$, then $h \cdot F^\circ(d, f) = H^\circ(h(d), h \cdot f)$.

(40) If for all d_1, d_2 holds $h(F(d_1, d_2)) = H(h(d_1), h(d_2))$, then $h \cdot F^\circ(f, d) = H^\circ(h \cdot f, h(d))$.

(41) If u is distributive w.r.t. F, then $u \cdot F^\circ(f, f') = F^\circ(u \cdot f, u \cdot f')$.

(42) If u is distributive w.r.t. F, then $u \cdot F^\circ(d, f) = F^\circ(u(d), u \cdot f)$.

(43) If u is distributive w.r.t. F, then $u \cdot F^\circ(f, d) = F^\circ(u \cdot f, u(d))$.

(44) If F has a unity, then $F^\circ(C \longmapsto \mathbf{1}_F, f) = f$ and $F^\circ(f, C \longmapsto \mathbf{1}_F) = f$.

(45) If F has a unity, then $F^\circ(\mathbf{1}_F, f) = f$.

(46) If F has a unity, then $F^\circ(f, \mathbf{1}_F) = f$.

(47) If F is distributive w.r.t. G, then $F^\circ(G(d_1, d_2), T) = G^\circ(F^\circ(d_1, T), F^\circ(d_2, T))$.

(48) If F is distributive w.r.t. G, then $F^\circ(T, G(d_1, d_2)) = G^\circ(F^\circ(T, d_1), F^\circ(T, d_2))$.

(49) If for all d_1, d_2 holds $h(F(d_1, d_2)) = H(h(d_1), h(d_2))$, then $h \cdot F^\circ(T_1, T_2) = H^\circ(h \cdot T_1, h \cdot T_2)$.

(50) If for all d_1, d_2 holds $h(F(d_1, d_2)) = H(h(d_1), h(d_2))$, then $h \cdot F^\circ(d, T) = H^\circ(h(d), h \cdot T)$.

(51) If for all d_1, d_2 holds $h(F(d_1, d_2)) = H(h(d_1), h(d_2))$, then $h \cdot F^\circ(T, d) = H^\circ(h \cdot T, h(d))$.

(52) If u is distributive w.r.t. F, then $u \cdot F^\circ(T_1, T_2) = F^\circ(u \cdot T_1, u \cdot T_2)$.

(53) If u is distributive w.r.t. F, then $u \cdot F^\circ(d, T) = F^\circ(u(d), u \cdot T)$.

(54) If u is distributive w.r.t. F, then $u \cdot F^\circ(T, d) = F^\circ(u \cdot T, u(d))$.

(55) If G is distributive w.r.t. F and $u = G^\circ(d, \mathrm{id}_D)$, then u is distributive w.r.t. F.

(56) If G is distributive w.r.t. F and $u = G^\circ(\mathrm{id}_D, d)$, then u is distributive w.r.t. F.

(57) If F has a unity, then $F^\circ(i \longmapsto \mathbf{1}_F, T) = T$ and $F^\circ(T, i \longmapsto \mathbf{1}_F) = T$.

(58) If F has a unity, then $F^\circ(\mathbf{1}_F, T) = T$.

(59) If F has a unity, then $F^\circ(T, \mathbf{1}_F) = T$.

Let us consider D, u, F. We say that u is an inverse operation w.r.t. F if and only if:

for every d holds $F(d, u(d)) = \mathbf{1}_F$ and $F(u(d), d) = \mathbf{1}_F$.

One can prove the following proposition

(60) u is an inverse operation w.r.t. F if and only if for every d holds $F(d, u(d)) = \mathbf{1}_F$ and $F(u(d), d) = \mathbf{1}_F$.

Let us consider D, F. We say that F has an inverse operation if and only if: there exists u such that u is an inverse operation w.r.t. F.

Next we state the proposition

(61) F has an inverse operation if and only if there exists u such that u is an inverse operation w.r.t. F.

Let us consider D, F. Let us assume that F has a unity and F is associative and F has an inverse operation. The inverse operation w.r.t.F yields a unary operation on D and is defined as follows:

the inverse operation w.r.t.F is an inverse operation w.r.t. F.

We now state a number of propositions:

(62) If F has a unity and F is associative and F has an inverse operation, then for every u holds $u =$ the inverse operation w.r.t.F if and only if u is an inverse operation w.r.t. F.

(63) If F has a unity and F is associative and F has an inverse operation, then F((the inverse operation w.r.t.F)(d), d) $= \mathbf{1}_\mathrm{F}$ and $F(d,$ (the inverse operation w.r.t.F)(d)) $= \mathbf{1}_\mathrm{F}$.

(64) If F has a unity and F is associative and F has an inverse operation and $F(d_1, d_2) = \mathbf{1}_F$, then $d_1 =$ (the inverse operation w.r.t.F)(d_2) and (the inverse operation w.r.t.F)(d_1) $= \mathrm{d}_2$.

(65) If F has a unity and F is associative and F has an inverse operation, then (the inverse operation w.r.t.F)($\mathbf{1}_\mathrm{F}$) $= \mathbf{1}_\mathrm{F}$.

(66) If F has a unity and F is associative and F has an inverse operation, then (the inverse operation w.r.t.F)((the inverse operation w.r.t.F)(d)) = d.

(67) If F has a unity and F is associative and F is commutative and F has an inverse operation, then the inverse operation w.r.t.F is distributive w.r.t. F.

(68) If F has a unity and F is associative and F has an inverse operation but $F(d, d_1) = F(d, d_2)$ or $F(d_1, d) = F(d_2, d)$, then $d_1 = d_2$.

(69) If F has a unity and F is associative and F has an inverse operation but $F(d_1, d_2) = d_2$ or $F(d_2, d_1) = d_2$, then $d_1 = \mathbf{1}_F$.

(70) If F is associative and F has a unity and F has an inverse operation and G is distributive w.r.t. F and $e = \mathbf{1}_F$, then for every d holds $G(e, d) = e$ and $G(d, e) = e$.

(71) If F has a unity and F is associative and F has an inverse operation and $u =$ the inverse operation w.r.t.F and G is distributive w.r.t. F, then $u(G(d_1, d_2)) = G(u(d_1), d_2)$ and $u(G(d_1, d_2)) = G(d_1, u(d_2))$.

(72) If F has a unity and F is associative and F has an inverse operation and $u =$ the inverse operation w.r.t.F and G is distributive w.r.t. F and G has a unity, then $G^\circ(u(\mathbf{1}_G), \mathrm{id}_D) = u$.

(73) If F is associative and F has a unity and F has an inverse operation and G is distributive w.r.t. F, then $(G^\circ(d, \mathrm{id}_D))(\mathbf{1}_F) = \mathbf{1}_F$.

(74) If F is associative and F has a unity and F has an inverse operation and G is distributive w.r.t. F, then $(G^\circ(\mathrm{id}_D, d))(\mathbf{1}_F) = \mathbf{1}_F$.

(75) If F has a unity and F is associative and F has an inverse operation, then $F^\circ(f,$ (the inverse operation w.r.t.F) $\cdot$ f) $=$ C $\longmapsto \mathbf{1}_{\rm F}$ and $F^\circ($(the inverse operation w.r.t.F) $\cdot$ f, f) $=$ C $\longmapsto \mathbf{1}_{\rm F}$.

(76) If F is associative and F has an inverse operation and F has a unity and $F^\circ(f, f') = C \longmapsto \mathbf{1}_F$, then $f =$ (the inverse operation w.r.t.F) $\cdot$ f′ and (the inverse operation w.r.t.F) $\cdot$ f $=$ f′.

(77) If F has a unity and F is associative and F has an inverse operation, then $F^\circ(T,$ (the inverse operation w.r.t.F) $\cdot$ T) $=$ i $\longmapsto \mathbf{1}_{\rm F}$ and $F^\circ($(the inverse operation w.r.t.F) $\cdot$ T, T) $=$ i $\longmapsto \mathbf{1}_{\rm F}$.

(78) If F is associative and F has an inverse operation and F has a unity and $F^\circ(T_1, T_2) = i \longmapsto \mathbf{1}_F$, then $T_1 =$ (the inverse operation w.r.t.F) $\cdot$ T_2 and (the inverse operation w.r.t.F) $\cdot$ $\mathrm{T}_1 = \mathrm{T}_2$.

(79) If F is associative and F has a unity and $e = \mathbf{1}_F$ and F has an inverse operation and G is distributive w.r.t. F, then $G^\circ(e, f) = C \longmapsto e$.

(80) If F is associative and F has a unity and $e = \mathbf{1}_F$ and F has an inverse operation and G is distributive w.r.t. F, then $G^\circ(e, T) = i \longmapsto e$.

Let F, f, g be functions. The functor $F \circ (f, g)$ yielding a function is defined by:

$F \circ (f, g) = F \cdot [\!: f, g :\!]$.

Next we state several propositions:

(81) For all functions F, f, g holds $F \circ (f, g) = F \cdot [\!: f, g :\!]$.

(82) For all functions F, f, g such that $\langle x, y \rangle \in \mathrm{dom}(F \circ (f, g))$ holds $(F \circ (f, g))(\langle x, y \rangle) = F(\langle f(x), g(y) \rangle)$.

(83) For all functions F, f, g such that $\langle x, y \rangle \in \mathrm{dom}(F \circ (f, g))$ holds $(F \circ (f, g))(x, y) = F(f(x), g(y))$.

(84) For every function F from $[\!: D, D' :\!]$ into E and for every function f from C into D and for every function g from C' into D' holds $F \circ (f, g)$ is a function from $[\!: C, C' :\!]$ into E.

(85) For all functions u, u' from D into D holds $F \circ (u, u')$ is a binary operation on D.

Let us consider D, F, and let f, f' be functions from D into D. Then $F \circ (f, f')$ is a binary operation on D.

The following propositions are true:

(86) For every function F from $[: D, D' :]$ into E and for every function f from C into D and for every function g from C' into D' holds $(F \circ (f, g))(c, c') = F(f(c), g(c'))$.

(87) For every function u from D into D holds $(F \circ (\mathrm{id}_D, u))(d_1, d_2) = F(d_1, u(d_2))$ and $(F \circ (u, \mathrm{id}_D))(d_1, d_2) = F(u(d_1), d_2)$.

(88) $(F \circ (\mathrm{id}_D, u))^\circ(f, f') = F^\circ(f, u \cdot f')$.

(89) $(F \circ (\mathrm{id}_D, u))^\circ(T_1, T_2) = F^\circ(T_1, u \cdot T_2)$.

(90) Suppose F is associative and F has a unity and F is commutative and F has an inverse operation and $u = \mathrm{the\,inverse\,operation\,w.r.t.F}$. Then $u((F \circ (\mathrm{id}_D, u))(d_1, d_2)) = (F \circ (u, \mathrm{id}_D))(d_1, d_2)$ and $(F \circ (\mathrm{id}_D, u))(d_1, d_2) = u((F \circ (u, \mathrm{id}_D))(d_1, d_2))$.

(91) If F is associative and F has a unity and F has an inverse operation, then $(F \circ (\mathrm{id}_D, \mathrm{the\,inverse\,operation\,w.r.t.F}))(\mathrm{d}, \mathrm{d}) = \mathbf{1}_{\mathrm{F}}$.

(92) If F is associative and F has a unity and F has an inverse operation, then $(F \circ (\mathrm{id}_D, \mathrm{the\,inverse\,operation\,w.r.t.F}))(\mathrm{d}, \mathbf{1}_{\mathrm{F}}) = \mathrm{d}$.

(93) If F is associative and F has a unity and F has an inverse operation and $u = \mathrm{the\,inverse\,operation\,w.r.t.F}$, then $(F \circ (\mathrm{id}_D, u))(\mathbf{1}_F, d) = u(d)$.

(94) If F is commutative and F is associative and F has a unity and F has an inverse operation and $G = F \circ (\mathrm{id}_D, \mathrm{the\,inverse\,operation\,w.r.t.F})$, then for all d_1, d_2, d_3, d_4 holds $F(G(d_1, d_2), G(d_3, d_4)) = G(F(d_1, d_3), F(d_2, d_4))$.

References

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

[2] Czesław Byliński. Basic functions and operations on functions. *Formalized Mathematics*, 1(**1**):245–254, 1990.

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

[4] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 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] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.

[8] Andrzej Trybulec. Semilattice operations on finite subsets. *Formalized Mathematics*, 1(**2**):369–376, 1990.

[9] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.

Received May 4, 1990