JOURNAL OF FORMALIZED MATHEMATICS
Volume 2, Released 1990, Published 2003
Inst. of Computer Science, Univ. of Białystok

Binary Operations Applied to Finite Sequences

Czesław Byliński
Warsaw University
Białystok

Summary. The article contains some propositions and theorems related to [9] and [8]. The notions introduced in [9] are extended to finite sequences. A number of 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.

WWW: http://mizar.org/JFM/Vol2/finseqop.html

The articles [11], [7], [12], [13], [4], [1], [6], [5], [3], [2], [9], [8], and [10] provide the notation and terminology for this paper.

For simplicity, we follow the rules: x, y denote sets, C, C', D, D', E denote non empty sets, c denotes an element of C, c' denotes an element of C', d, d_1, d_2, d_3, d_4, e denote elements of D, and d' denotes an element of D'.

We now state several propositions:

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

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

(4)[1] For all functions F, f holds $F^\circ(\emptyset, f) = \emptyset$ and $F^\circ(f, \emptyset) = \emptyset$.

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

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

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

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

For simplicity, we follow the rules: i, j denote natural numbers, F denotes a function from $[: D, D' :]$ into E, p, q denote finite sequences of elements of D, and p', q' 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 $i \mapsto d$ is an element of D^i.

In the sequel f, f' denote functions from C into D and h denotes a function from D into E.

[1] The proposition (3) has been removed.

Let D, E be sets, let p be a finite sequence of elements of D, and let h be a function from D into E. Then $h \cdot p$ is a finite sequence of elements of E.

One can prove the following 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 adopt the following convention: T, T_1, T_2, T_3 are elements of D^i, T' is an element of D'^i, S is an element of D^j, and S' is an element of D'^j.

We now 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 $h \cdot (i \mapsto d) = i \mapsto h(d)$.

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

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

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

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

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

(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.

Next we state a number of 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 $F^{\circ}(i \mapsto \mathbf{1}_F, T) = T$ and $F^{\circ}(T, i \mapsto \mathbf{1}_F) = T$.

(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:

(Def. 1) 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 if and only if:

(Def. 2) There exists u which is an inverse operation w.r.t. F.

We introduce F has an inverse operation as a synonym of F
let us consider D, F. Let us assume that F has a unity 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 by:

(Def. 3) The inverse operation w.r.t. F is an inverse operation w.r.t. F.

One can prove the following propositions:

(63)[2] Suppose F is associative and has a unity and an inverse operation. Then $F(($the inverse operation w.r.t. $F)(d), d) = \mathbf{1}_F$ and $F(d, ($the inverse operation w.r.t. $F)(d)) = \mathbf{1}_F$.

[2] The propositions (60)–(62) have been removed.

(64) Suppose F is associative and has a unity and 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. $F)(d_1) = d_2$.

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

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

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

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

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

(70) Suppose F is associative and has a unity and an inverse operation and G is distributive w.r.t. F and $e = \mathbf{1}_F$. Let given d. Then $G(e, d) = e$ and $G(d, e) = e$.

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

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

(76) Suppose F is associative and has an inverse operation and 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) Suppose F is associative and has a unity and an inverse operation. Then $F^\circ(T,$ (the inverse operation w.r.t. $F) \cdot T) = i \mapsto \mathbf{1}_F$ and $F^\circ(($the inverse operation w.r.t. $F) \cdot T, T) = i \mapsto \mathbf{1}_F$.

(78) Suppose F is associative and has an inverse operation and a unity and $F^\circ(T_1, T_2) = i \mapsto \mathbf{1}_F$. Then $T_1 =$ (the inverse operation w.r.t. $F) \cdot T_2$ and (the inverse operation w.r.t. $F) \cdot T_1 = T_2$.

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

Let F, f, g be functions. The functor $F \circ (f, g)$ yields a function and is defined as follows:

(Def. 4) $F \circ (f, g) = F \cdot [: f, g :]$.

The following four propositions are true:

(82)[3] For all functions F, f, g such that $\langle x, y \rangle \in \mathrm{dom}(F \circ (f, g))$ holds $(F \circ (f, g))(\langle x, y \rangle) = F(\langle f(x), g(y) \rangle)$.

[3] The proposition (81) has been removed.

(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) Let F be a function from $[:D, D':]$ into E, f be a function from C into D, and g be a function from C' into D'. Then $F\circ(f,g)$ 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.

We now state several propositions:

(86) Let F be a function from $[:D, D':]$ into E, f be a function from C into D, and g be a function from C' into D'. Then $(F\circ(f,g))(c, c') = F(f(c), g(c'))$.

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

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

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

(94) Suppose F is commutative and associative and has a unity and an inverse operation and $G = F\circ(\mathrm{id}_D,$the inverse operation w.r.t. $F)$. Let given d_1, d_2, d_3, d_4. Then $F(G(d_1, d_2), G(d_3, d_4)) = G(F(d_1, d_3), F(d_2, d_4))$.

REFERENCES

[1] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/finseq_1.html.

[2] Czesław Byliński. Basic functions and operations on functions. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/funct_3.html.

[3] Czesław Byliński. Binary operations. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/binop_1.html.

[4] Czesław Byliński. Functions and their basic properties. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/funct_1.html.

[5] Czesław Byliński. Functions from a set to a set. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/funct_2.html.

[6] Czesław Byliński. Partial functions. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/partfun1.html.

[7] Czesław Byliński. Some basic properties of sets. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/zfmisc_1.html.

[8] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/finseq_2.html.

[9] Andrzej Trybulec. Binary operations applied to functions. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/funcop_1.html.

[10] Andrzej Trybulec. Semilattice operations on finite subsets. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/setwiseo.html.

[11] Andrzej Trybulec. Tarski Grothendieck set theory. *Journal of Formalized Mathematics*, Axiomatics, 1989. http://mizar.org/JFM/Axiomatics/tarski.html.

[12] Zinaida Trybulec. Properties of subsets. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/subset_1.html.

[13] Edmund Woronowicz. Relations and their basic properties. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/relat_1.html.

Received May 4, 1990

Published January 2, 2004