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

Semigroup Operations on Finite Subsets

Czesław Byliński
Warsaw University
Białystok

Summary. A continuation of [10]. The propositions and theorems proved in [10] are extended to finite sequences. Several additional theorems related to semigroup operations of functions not included in [10] are proved. The special notation for operations on finite sequences is introduced.

MML Identifier: `SETWOP_2`.

WWW: `http://mizar.org/JFM/Vol2/setwop_2.html`

The articles [11], [15], [12], [1], [16], [17], [4], [2], [13], [6], [5], [3], [9], [10], [8], [7], and [14] provide the notation and terminology for this paper.

For simplicity, we adopt the following rules: C, C', D, E are non empty sets, c, c_1, c_2, c_3 are elements of C, B, B_1, B_2 are elements of $\mathrm{Fin}\,C$, A is an element of $\mathrm{Fin}\,C'$, d, d_1, d_2, d_3, d_4, e are elements of D, F, G are binary operations on D, u is a unary operation on D, f, f' are functions from C into D, g is a function from C' into D, H is a binary operation on E, h is a function from D into E, i, j are natural numbers, s is a function, p, q are finite sequences of elements of D, and T_1, T_2 are elements of D^i.

We now state a number of propositions:

(3)[1] If F is commutative and associative and $c_1 \neq c_2$, then $F\text{-}\sum_{\{c_1,c_2\}} f = F(f(c_1), f(c_2))$.

(4) If F is commutative and associative and if $B \neq \emptyset$ or F has a unity and if $c \notin B$, then $F\text{-}\sum_{B \cup \{c\}} f = F(F\text{-}\sum_B f, f(c))$.

(5) If F is commutative and associative and $c_1 \neq c_2$ and $c_1 \neq c_3$ and $c_2 \neq c_3$, then $F\text{-}\sum_{\{c_1,c_2,c_3\}} f = F(F(f(c_1), f(c_2)), f(c_3))$.

(6) If F is commutative and associative and if $B_1 \neq \emptyset$ and $B_2 \neq \emptyset$ or F has a unity and if B_1 misses B_2, then $F\text{-}\sum_{B_1 \cup B_2} f = F(F\text{-}\sum_{B_1} f, F\text{-}\sum_{B_2} f)$.

(7) Suppose that

(i) F is commutative and associative,

(ii) $A \neq \emptyset$ or F has a unity, and

(iii) there exists s such that $\mathrm{dom}\, s = A$ and $\mathrm{rng}\, s = B$ and s is one-to-one and $g{\restriction}A = f \cdot s$.

Then $F\text{-}\sum_A g = F\text{-}\sum_B f$.

(8) If H is commutative and associative and if $B \neq \emptyset$ or H has a unity and if f is one-to-one, then $H\text{-}\sum_{f^\circ B} h = H\text{-}\sum_B h \cdot f$.

[1] The propositions (1) and (2) have been removed.

(9) If F is commutative and associative and if $B \neq \emptyset$ or F has a unity and if $f \restriction B = f' \restriction B$, then $F\text{-}\sum_B f = F\text{-}\sum_B f'$.

(10) If F is commutative and associative and has a unity and $e = \mathbf{1}_F$ and $f^\circ B = \{e\}$, then $F\text{-}\sum_B f = e$.

(11) Suppose F is commutative and associative and has a unity and $e = \mathbf{1}_F$ and $G(e, e) = e$ and for all d_1, d_2, d_3, d_4 holds $F(G(d_1, d_2), G(d_3, d_4)) = G(F(d_1, d_3), F(d_2, d_4))$. Then $G(F\text{-}\sum_B f, F\text{-}\sum_B f') = F\text{-}\sum_B G^\circ(f, f')$.

(12) If F is commutative and associative and has a unity, then $F(F\text{-}\sum_B f, F\text{-}\sum_B f') = F\text{-}\sum_B F^\circ(f, f')$.

(13) Suppose F is commutative and associative and has a unity and an inverse operation and $G = F \circ (\mathrm{id}_D, \text{the inverse operation w.r.t.} F)$. Then $G(F\text{-}\sum_B f, F\text{-}\sum_B f') = F\text{-}\sum_B G^\circ(f, f')$.

(14) Suppose F is commutative and associative and has a unity and $e = \mathbf{1}_F$ and G is distributive w.r.t. F and $G(d, e) = e$. Then $G(d, F\text{-}\sum_B f) = F\text{-}\sum_B G^\circ(d, f)$.

(15) Suppose F is commutative and associative and has a unity and $e = \mathbf{1}_F$ and G is distributive w.r.t. F and $G(e, d) = e$. Then $G(F\text{-}\sum_B f, d) = F\text{-}\sum_B G^\circ(f, d)$.

(16) Suppose F is commutative and associative and has a unity and an inverse operation and G is distributive w.r.t. F. Then $G(d, F\text{-}\sum_B f) = F\text{-}\sum_B G^\circ(d, f)$.

(17) Suppose F is commutative and associative and has a unity and an inverse operation and G is distributive w.r.t. F. Then $G(F\text{-}\sum_B f, d) = F\text{-}\sum_B G^\circ(f, d)$.

(18) Suppose that

(i) F is commutative and associative and has a unity,

(ii) H is commutative and associative and has a unity,

(iii) $h(\mathbf{1}_F) = \mathbf{1}_H$, and

(iv) for all d_1, d_2 holds $h(F(d_1, d_2)) = H(h(d_1), h(d_2))$.

Then $h(F\text{-}\sum_B f) = H\text{-}\sum_B h \cdot f$.

(19) If F is commutative and associative and has a unity and $u(\mathbf{1}_F) = \mathbf{1}_F$ and u is distributive w.r.t. F, then $u(F\text{-}\sum_B f) = F\text{-}\sum_B u \cdot f$.

(20) Suppose F is commutative and associative and has a unity and an inverse operation and G is distributive w.r.t. F. Then $(G^\circ(d, \mathrm{id}_D))(F\text{-}\sum_B f) = F\text{-}\sum_B G^\circ(d, \mathrm{id}_D) \cdot f$.

(21) Suppose F is commutative and associative and has a unity and an inverse operation. Then $(\text{the inverse operation w.r.t.} F)(F\text{-}\sum_B f) = F\text{-}\sum_B (\text{the inverse operation w.r.t.} F) \cdot f$.

Let us consider D, p, d. The functor $\Omega_d(p)$ yields a function from $\mathbb{N}$ into D and is defined by:

(Def. 1) $\Omega_d(p) = (\mathbb{N} \longmapsto d) {+\cdot} p$.

Next we state several propositions:

(22) If $i \in \operatorname{dom} p$, then $(\Omega_d(p))(i) = p(i)$ and if $i \notin \operatorname{dom} p$, then $(\Omega_d(p))(i) = d$.

(23) $\Omega_d(p) \restriction \operatorname{dom} p = p$.

(24) $\Omega_d((p \frown q)) \restriction \operatorname{dom} p = p$.

(25) $\operatorname{rng} \Omega_d(p) = \operatorname{rng} p \cup \{d\}$.

(26) $h \cdot \Omega_d(p) = \Omega_{h(d)}((h \cdot p))$.

Let us consider i. Then $\mathrm{Seg}\,i$ is an element of $\mathrm{Fin}\,\mathbb{N}$.

Let f be a finite sequence. Then $\mathrm{dom} f$ is an element of $\mathrm{Fin}\,\mathbb{N}$.

Let us consider D, p, F. Let us assume that F has a unity or $\mathrm{len}\,p \geq 1$ but F is associative and commutative. Then $F \odot p$ can be characterized by the condition:

(Def. 2) $F \odot p = F\text{-}\sum_{\mathrm{dom}\,p} \Omega_{\mathbf{1}_F}(p)$.

We introduce $F \circledast p$ as a synonym of $F \odot p$.

The following propositions are true:

(35)[2] If F has a unity, then $F \odot i \mapsto \mathbf{1}_F = \mathbf{1}_F$.

(37)[3] If F is associative and if $i \geq 1$ and $j \geq 1$ or F has a unity, then $F \odot (i+j) \mapsto d = F(F \odot i \mapsto d, F \odot j \mapsto d)$.

(38) If F is commutative and associative and if $i \geq 1$ and $j \geq 1$ or F has a unity, then $F \odot (i \cdot j) \mapsto d = F \odot j \mapsto (F \odot i \mapsto d)$.

(39) If F has a unity and H has a unity and $h(\mathbf{1}_F) = \mathbf{1}_H$ and for all d_1, d_2 holds $h(F(d_1, d_2)) = H(h(d_1), h(d_2))$, then $h(F \odot p) = H \odot h \cdot p$.

(40) If F has a unity and $u(\mathbf{1}_F) = \mathbf{1}_F$ and u is distributive w.r.t. F, then $u(F \odot p) = F \odot u \cdot p$.

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

(42) Suppose F is commutative and associative and has a unity and an inverse operation. Then (the inverse operation w.r.t. F)$(F \odot p) = F \odot$(the inverse operation w.r.t. $F) \cdot p$.

(43) Suppose that

(i) F is commutative and associative and has a unity,

(ii) $e = \mathbf{1}_F$,

(iii) $G(e, e) = e$,

(iv) for all d_1, d_2, d_3, d_4 holds $F(G(d_1, d_2), G(d_3, d_4)) = G(F(d_1, d_3), F(d_2, d_4))$, and

(v) $\mathrm{len}\,p = \mathrm{len}\,q$.

Then $G(F \odot p, F \odot q) = F \odot G^{\circ}(p, q)$.

(44) Suppose F is commutative and associative and has a unity and $e = \mathbf{1}_F$ and $G(e, e) = e$ and for all d_1, d_2, d_3, d_4 holds $F(G(d_1, d_2), G(d_3, d_4)) = G(F(d_1, d_3), F(d_2, d_4))$. Then $G(F \odot T_1, F \odot T_2) = F \odot G^{\circ}(T_1, T_2)$.

(45) If F is commutative and associative and has a unity and $\mathrm{len}\,p = \mathrm{len}\,q$, then $F(F \odot p, F \odot q) = F \odot F^{\circ}(p, q)$.

(46) If F is commutative and associative and has a unity, then $F(F \odot T_1, F \odot T_2) = F \odot F^{\circ}(T_1, T_2)$.

(47) If F is commutative and associative and has a unity, then $F \odot i \mapsto F(d_1, d_2) = F(F \odot i \mapsto d_1, F \odot i \mapsto d_2)$.

(48) 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. $F)$. Then $G(F \odot T_1, F \odot T_2) = F \odot G^{\circ}(T_1, T_2)$.

(49) Suppose F is commutative and associative and has a unity and $e = \mathbf{1}_F$ and G is distributive w.r.t. F and $G(d, e) = e$. Then $G(d, F \odot p) = F \odot G^{\circ}(d, p)$.

(50) Suppose F is commutative and associative and has a unity and $e = \mathbf{1}_F$ and G is distributive w.r.t. F and $G(e, d) = e$. Then $G(F \odot p, d) = F \odot G^{\circ}(p, d)$.

[2] The propositions (27)–(34) have been removed.

[3] The proposition (36) has been removed.

(51) Suppose F is commutative and associative and has a unity and an inverse operation and G is distributive w.r.t. F. Then $G(d, F \odot p) = F \odot G^{\circ}(d, p)$.

(52) Suppose F is commutative and associative and has a unity and an inverse operation and G is distributive w.r.t. F. Then $G(F \odot p, d) = F \odot G^{\circ}(p, d)$.

REFERENCES

[1] Grzegorz Bancerek. The fundamental properties of natural numbers. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/nat_1.html`.

[2] 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`.

[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. Binary operations applied to finite sequences. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/finseqop.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] Andrzej Trybulec. Subsets of real numbers. *Journal of Formalized Mathematics*, Addenda, 2003. `http://mizar.org/JFM/Addenda/numbers.html`.

[13] Andrzej Trybulec and Agata Darmochwał. Boolean domains. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/finsub_1.html`.

[14] Wojciech A. Trybulec. Binary operations on finite sequences. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/finsop_1.html`.

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

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

[17] Edmund Woronowicz. Relations defined on sets. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/relset_1.html`.

Received May 4, 1990

Published January 2, 2004