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

Semigroup operations on finite subsets

Czesław Byliński[1]
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.

The articles [11], [1], [9], [6], [2], [12], [7], [3], [13], [8], [10], [5], and [4] provide the terminology and notation for this paper. For simplicity we adopt the following rules: x will be arbitrary, C, C', D, E will denote non-empty sets, c, c_1, c_2, c_3 will denote elements of C, B, B_1, B_2 will denote elements of $\mathrm{Fin}\,C$, A will denote an element of $\mathrm{Fin}\,C'$, d, d_1, d_2, d_3, d_4, e will denote elements of D, F, G will denote binary operations on D, u will denote a unary operation on D, f, f' will denote functions from C into D, g will denote a function from C' into D, H will denote a binary operation on E, h will denote a function from D into E, i, j will denote natural numbers, s will denote a function, p, p_1, p_2, q will denote finite sequences of elements of D, and T_1, T_2 will denote elements of D^i. We now state a number of propositions:

(1) $\mathrm{Seg}\,i$ is an element of $\mathrm{Fin}\,\mathbb{N}$.

(2) $i + j \longmapsto x = (i \longmapsto x) \frown (j \longmapsto x)$.

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

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

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

ISSN 0777–4028

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

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

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

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

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

(14) If F is commutative and F is associative and F 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) If F is commutative and F is associative and F 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) If F is commutative and F is associative and F has a unity and F has 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) If F is commutative and F is associative and F has a unity and F has 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 F is commutative and F is associative and F has a unity and H is commutative and H is associative 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 $h(F\text{-}\sum_B f) = H\text{-}\sum_B (h \cdot f)$.

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

(21) If F is commutative and F is associative and F has a unity and F

has an inverse operation, then (the inverse operation w.r.t.F)(F- $\sum_{\rm B}$ f) = F- $\sum_{\rm B}$((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:

if $i \in \mathrm{Seg}(\mathrm{len}\, p)$, then $(\Omega_d(p))(i) = p(i)$ but if $i \notin \mathrm{Seg}(\mathrm{len}\, p)$, then $(\Omega_d(p))(i) = d$.

Next we state several propositions:

(22) For every function h from $\mathbb{N}$ into D holds $h = \Omega_d(p)$ if and only if for every i holds if $i \in \mathrm{Seg}(\mathrm{len}\, p)$, then $h(i) = p(i)$ but if $i \notin \mathrm{Seg}(\mathrm{len}\, p)$, then $h(i) = d$.

(23) $\Omega_d(p) \restriction \mathrm{Seg}(\mathrm{len}\, p) = p$.

(24) $\Omega_d((p \frown q)) \restriction \mathrm{Seg}(\mathrm{len}\, p) = p$.

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

(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 X be a non-empty subset of $\mathbb{R}$, and let x be an element of X. Then $\{x\}$ is an element of $\mathrm{Fin}\, X$. Let y be an element of X. Then $\{x, y\}$ is an element of $\mathrm{Fin}\, X$. Let z be an element of X. Then $\{x, y, z\}$ is an element of $\mathrm{Fin}\, X$.

Let us consider D, F, p. The functor $F \circledast p$ yielding an element of D is defined by:

$F \circledast p = F\text{-}\sum_{\mathrm{Seg}(\mathrm{len}\, p)} \Omega_{\mathbf{1}_F}(p)$.

Next we state several propositions:

(27) $F \circledast p = F\text{-}\sum_{\mathrm{Seg}(\mathrm{len}\, p)} \Omega_{\mathbf{1}_F}(p)$.

(28) If F is commutative and F is associative and F has a unity, then $F \circledast \varepsilon_D = \mathbf{1}_F$.

(29) If F is commutative and F is associative, then $F \circledast \langle d \rangle = d$.

(30) If F is commutative and F is associative but $\mathrm{len}\, p \neq 0$ or F has a unity, then $F \circledast (p \frown \langle d \rangle) = F(F \circledast p,\, d)$.

(31) If F is commutative and F is associative but $\mathrm{len}\, p_1 \neq 0$ and $\mathrm{len}\, p_2 \neq 0$ or F has a unity, then $F \circledast (p_1 \frown p_2) = F(F \circledast p_1,\, F \circledast p_2)$.

(32) If F is commutative and F is associative but $\mathrm{len}\, p \neq 0$ or F has a unity, then $F \circledast (\langle d \rangle \frown p) = F(d,\, F \circledast p)$.

Let us consider D, d_1, d_2. Then $\langle d_1, d_2 \rangle$ is a finite sequence of elements of D.

One can prove the following proposition

(33) If F is commutative and F is associative, then $F \circledast \langle d_1, d_2 \rangle = F(d_1,\, d_2)$.

Let us consider D, d_1, d_2, d_3. Then $\langle d_1, d_2, d_3 \rangle$ is a finite sequence of elements of D.

We now state a number of propositions:

(34) If F is commutative and F is associative, then $F \circledast \langle d_1, d_2, d_3 \rangle = F(F(d_1,\, d_2),\, d_3)$.

(35) If F is commutative and F is associative and F has a unity and $e = \mathbf{1}_F$, then $F \circledast (i \longmapsto e) = e$.

(36) If F is commutative and F is associative, then $F \circledast (1 \longmapsto d) = d$.

(37) If F is commutative and F is associative but $i \neq 0$ and $j \neq 0$ or F has a unity, then $F \circledast (i + j \longmapsto d) = F(F \circledast (i \longmapsto d), F \circledast (j \longmapsto d))$.

(38) If F is commutative and F is associative but $i \neq 0$ and $j \neq 0$ or F has a unity, then $F \circledast (i \cdot j \longmapsto d) = F \circledast (j \longmapsto F \circledast (i \longmapsto d))$.

(39) Suppose F is commutative and F is associative and F has a unity and H is commutative and H is associative 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 $h(F \circledast p) = H \circledast (h \cdot p)$.

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

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

(42) If F is commutative and F is associative and F has a unity and F has an inverse operation, then (the inverse operation w.r.t.F)(F⊛p) = F⊛((the inverse operation w.r.t.F) · p).

(43) Suppose that

(i) F is commutative,

(ii) F is associative,

(iii) F has a unity,

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

(v) $G(e, e) = e$,

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

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

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

(44) Suppose F is commutative and F is associative and F 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 $G(F \circledast T_1, F \circledast T_2) = F \circledast G^{\circ}(T_1, T_2)$.

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

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

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

(48) If F is commutative and F is associative and F has a unity and F has an inverse operation and $G = F \circ (\mathrm{id}_D$, the inverse operation w.r.t.F), then $G(F \circledast T_1, F \circledast T_2) = F \circledast G^{\circ}(T_1, T_2)$.

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

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

(51) If F is commutative and F is associative and F has a unity and F has an inverse operation and G is distributive w.r.t. F, then $G(d, F \circledast p) = F \circledast (G^\circ(d,p))$.

(52) If F is commutative and F is associative and F has a unity and F has an inverse operation and G is distributive w.r.t. F, then $G(F \circledast p, d) = F \circledast (G^\circ(p,d))$.

References

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

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

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

[4] Czesław Byliński. Binary operations applied to finite sequences. *Formalized Mathematics*, 1(**4**):643–649, 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] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.

[9] Andrzej Trybulec. Enumerated sets. *Formalized Mathematics*, 1(**1**):25–34, 1990.

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

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

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

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

Received May 4, 1990