PUBLICATIONS DE L'INSTITUT MATHÉMATIQUE
Nouvelle série, tome 82(96) (2007), 155–163 DOI 102298/PIM0796155P

FIN-SET: A SYNTACTICAL DEFINITION OF FINITE SETS

Slaviša B. Prešić

Abstract. We state Fin-set, by which one founds the notion of finite sets in a syntactical way. Any finite set $\{a_1, a_2, \dots, a_n\}$ is defined as a well formed term of the form $S(a_1 + (a_2 + (\cdots + (a_{n-1} + a_n)\cdots)))$, where $+$ is a binary and S a unary operational symbol. Related to the operational symbol $+$ the term-substitutions (1) are introduced. Definition of finite sets is called syntactical because by two algorithms Set-alg and Calc one can effectively establish whether any given set-terms are equal or not equal.

All other notions related to finite sets, like $\in$, ordered pair, Cartesian product, relation, function, cardinal number are defined as terms as well. Each of these definitions is recursive. For instance, $\in$ is defined by

$$x \in S(a_1) \quad \text{iff} \quad x = a_1$$
$$x \in S(a_1 + \cdots + a_n) \quad \text{iff} \quad x = a_1 \text{ or } x \in S(a_2 + \cdots + a_n)$$
$$x \notin \emptyset \quad (\emptyset \text{ denotes the empty set})$$

1. The key idea

Finite sets are usually expressed by some set-terms like $\{a\}$, $\{a, \{b, c\}\}$, $\{a_1, \dots, a_n\}$. Related to such terms there are infinite number of 'algebraic laws' like

$$(*) \qquad \{x, x\} = \{x\}, \quad \{x, y\} = \{y, x\}, \quad \{x, y, z\} = \{z, x, y\}$$

which express various properties of finite sets. In order to state all such algebraic laws we use the following idea: We 'divide' the notion of finite set into two 'parts'. The first one is the *preset*, formalized by means of a binary operational symbol $+$. The second one is the *set-maker*, formalized by an unary operational symbol S.

For instance, using S and $+$ the ordinary set-terms $\{a\}$, $\{\{a, b\}, c\}$, $\{a_1, \dots, a_n\}$ are represented by the following $(S, +)$-terms

$$S(a), \quad S(S(a + b) + c), \quad S(a_1 + (a_2 + \cdots + (a_{n-1} + a_n) + \cdots))$$

respectively. Having in mind $(*)$ for $+$ we put term-substitutions (1) (below).

2000 *Mathematics Subject Classification*: 03E30.
Key words and phrases: finite set, algorithm, syntactical definition.

2. $(+, S)-$terms

Denote by Γ a collection of constant symbols, called *initial elements.* Symbol $\emptyset$ is also an element of Γ. Let L be a language whose elements are all elements of Γ and also the operational symbols $+$ and S ($+$ is a binary, S a unary operational symbol). The symbols $x, y, z, u, x', y', z', u', \dots$ are used as variables. We define *terms* by the generalized inductive definition:

(i) Any element of Γ is a term.
(ii) A variable is a term.
(iii) If A, B are terms, then the words $(A + B)$, $S(A)$ are terms.

Next we introduce the following term-substitutions

$$(1)\qquad \begin{array}{rr} (i) & (\tau_1 + \tau_1) \to \tau_1 \\ (i') & \tau_1 \to (\tau_1 + \tau_1) \\ (ii) & (\tau_1 + \tau_2) \to (\tau_2 + \tau_1) \\ (iii) & ((\tau_1 + \tau_2) + \tau_3) \to (\tau_1 + (\tau_2 + \tau_3)) \\ (iii') & (\tau_1 + (\tau_2 + \tau_3)) \to ((\tau_1 + \tau_2) + \tau_3) \\ (iv) & \tau_1 \to \tau_1 \end{array}$$

where τ_1, τ_2, τ_3 are any terms.

Let $\sigma_1 \to \sigma_2$ be a substitution. Suppose that t_1 is a term which contains, at some place[1] a subterm of the form σ_1. Replacing σ_1 with σ_2 at such a place from t_1 we obtain a new term denoted by t_2. We shall say that t_2 *is neighbouring to* t_1. For the sentence: t_2 *is neighbouring to* t_1 we shall use the following notation: $t_1 \to t_2$. For instance, let t_1 be a term

$$S(S(x + S(a + (b + c))) + S(a + (b + c)))$$

and let the substitution $\sigma_1 \to \sigma_2$ be of the form $(\tau_1 + \tau_2) \to (\tau_2 + \tau_1)$. In the given term t_1 there are six subterms of the form $(\tau_1 + \tau_2)$, since the symbol $+$ appears in t_1 just six times. Let us consider the subterm $(a + (b + c))$, at its first occurrence. Then τ_1 is a, and τ_2 is $(b + c)$. By applying the substitution $(\tau_1 + \tau_2) \to (\tau_2 + \tau_1)$ from term t_1 we obtain the term t_2

$$S(S(x + S((b + c) + a)) + S(a + (b + c)))$$

which is neighbouring to t_1. Due to (1)(iv) any term t is neighbouring to t, i.e., $t \to t$. Next, we shall define a relation $=$ ('equality') between two terms t_1, t_2. Namely:

(2) We shall say that $t_1 = t_2$ holds iff *either* the word t_1 is literally equal to the word t_2 *or* there are terms $\tau_1, \tau_2, \dots, \tau_k$ such that τ_1 is t_1, τ_k is t_2, and each τ_i $(1 < i \leqslant k)$ is neighbouring to τ_{i-1}

In other words, $t_1 = t_2$ holds iff we have the following 'substitutional chain'

$$(3')\qquad \tau_1 \to \tau_2 \to \tau_3 \to \cdots \to \tau_k \quad (\tau_1 \text{ is } t_1,\ \tau_k \text{ is } t_2)$$

---

[1]Starting, say, with certain i-th letter of the word t_1

If the relation $t_1 = t_2$ holds we shall say that t_1 *is equal to* t_2. Obviously relation $=$ has the following properties

$$\begin{array}{ll} & \tau_1 = \tau_1 \\ & \text{If } \tau_1 = \tau_2, \text{ then } \tau_2 = \tau_1 \\ (3) & \text{If } \tau_1 = \tau_2 \text{ and } \tau_2 = \tau_3, \text{ then } \tau_1 = \tau_3 \\ & \text{If } \tau_1 = \tau_2, \text{ then } S(\tau_1) = S(\tau_2) \\ & \text{If } \tau_1 = \tau_2 \text{ and } \tau_3 = \tau_4, \text{ then } (\tau_1 + \tau_3) = (\tau_2 + \tau_4) \end{array}$$

REMARK 1. Relation $=$ can be defined by equational axioms $x+x=x$, $x+y=y+x$, $(x+y)+z=x+(y+z)$. Namely, it can be easily proved that relation $t_1 = t_2$ holds *iff* formula $t_1 = t_2$ is an equational consequence of the axioms, where x, y, z can be any $(S,+)$-terms.

Now we consider terms of the form

$$A_1, \quad (A_1 + A_2), \quad ((A_1 + A_2) + A_3), \quad (((A_1 + A_2) + A_3) + A_4), \dots$$

For them we shall use the notation

$$A_1, \quad A_1 + A_2, \quad A_1 + A_2 + A_3, \quad A_1 + A_2 + A_3 + A_4, \dots$$

respectively and call them *sum-terms*. Suppose that by $\mathrm{term}(+, A_1, \dots, A_k)$ any term is denoted which is built up from its subterms $A_1, \dots, A_k$ by use of the operational symbol $+$ only. The order of these A_i is not important. Then the following equality holds:

$$(*_1) \qquad \mathrm{term}(+, A_1, \dots, A_k) = A_1 + \cdots + A_k$$

This equality holds in virtue of substitutions (1) of the form (*ii*), (*iii*), (*iii′*). For instance, the equality $((A + (C + B)) + (E + D)) = A + B + C + D + E$ is true.

Let $A_1 + \cdots + A_k$, $B_1 + \cdots + B_q$ be any sum-terms. We define relation $=_S$ between them:

(4) $A_1 + \cdots + A_p =_S B_1 + \cdots + B_q$ holds iff each A_i is equal to some B_j and each B_k is equal to some A_l

The relation $=_S$ has the following properties

(5) (*i*) $A_1 + \cdots + A_p =_S A_{f(1)} + \cdots + A_{f(p)}$, where f is any permutation of indexes $1, \dots, p$.

(*ii*) $A_1 + \cdots + A_i + \cdots + A_p =_S A_1 + \cdots + A_i + A_i + \cdots + A_p$, where the right hand side is obtained from the left hand side by replacing A_i by $A_i + A_i$

(*ii′*) $A_1 + \cdots + A_i + A_i + \cdots + A_p =_S A_1 + \cdots + A_i + \cdots + A_p$, where the left hand side is obtained from the right hand side by replacing A_i by $A_i + A_i$

(*iii*) If $A_1 + \cdots + A_p =_S B_1 + \cdots + B_q$, then $B_1 + \cdots + B_q =_S A_1 + \cdots + A_p$

(*iv*) If $A_1 + \cdots + A_p =_S B_1 + \cdots + B_q$ and $B_1 + \cdots + B_q =_S C_1 + \cdots + C_r$, then $A_1 + \cdots + A_p =_S C_1 + \cdots + C_r$

(*v*) $A_1 + \cdots + A_i + \cdots + A_p =_S A_1 + \cdots + B + \cdots + A_p$ assuming that A_i is replaced by B and $A_i = B$

Assertion (5) is an immediate consequence of definition (4). Relation $=_S$ has also this property

$(*_2)$ If $A_1 + \cdots + A_p =_S B_1 + \cdots + B_q$, then $A_1 + \cdots + A_p = B_1 + \cdots + B_q$

which is an immediate consequence of (4) and definition of $=$, i.e., of (2). For instance, $A + B + C =_S B + C + A + C$ holds. Also $A + B + C = B + C + A + C$ holds, which can be proved easily by substitutions (1).

Related to implication $(*_2)$ it is important to know when the opposite implication is true too. In connection with it we introduce the notion of *full sum-term*. Namely, we shall say that $A_1 + \cdots + A_k$ is a *full sum-term* if none of A_i is of the form $(P + Q)$ for some P, Q. Obviously, any sum-term is equal to certain full sum-term.

Now we shall prove

$(*_3)$ If $B_1 + \cdots + B_q$ is a full sum-term, which is neighbouring to a full sum-term $A_1 + \cdots + A_p$, then $A_1 + \cdots + A_p =_S B_1 + \cdots + B_q$ holds.

Indeed, denote by σ a substitution of type (1) by which from $A_1 + \cdots + A_p$ we obtain $B_1 + \cdots + B_q$. We distinguish two cases:

1° σ is related to some subterm of $A_1 \cdots + A_p$ whose $+$ is inside one A_i.

2° σ is related to one of $p-1$ symbols $+$ occuring in the sum-term $A_1+A_2+\cdots+A_p$

In the first case applying σ to A_i we obtain some B, such that $A_i = B$. Then in virtue of (5)(v) we conclude that

$$A_1 + \cdots + A_{i-1} + A_i + \cdots + A_p =_S A_1 + \cdots + A_{i-1} + B + \cdots + A_p$$

and proof is complete in the first case.

In the second case, having in mind (5)(i), (ii), (ii') the proof completes.

Now we shall prove a generalization of $(*_3)$

$(*_4)$ If $A_1 + \cdots + A_p = B_1 + \cdots + B_q$ holds, where $A_1 + \cdots + A_p$, $B_1 + \cdots + B_q$ are full sum-terms, then also $A_1 + \cdots + A_p =_S B_1 + \cdots + B_q$ holds.

Indeed, let $A_1 + \cdots + A_p = B_1 + \cdots + B_q$. Then, like (3′), there is certain substitutional chain

$$\tau_1 \to \tau_2 \to \cdots \to \tau_k \quad (\tau_1 \text{ is } A_1 + \cdots + A_p,\ \tau_k \text{ is } B_1 + \cdots + B_q)$$

In virtue of $(*_3)$ we have $\tau_1 =_S \tau_2$, $\tau_2 =_S \tau_3, \ldots, \tau_{k-1} =_S \tau_k$. Having in mind (5)($iv$) we conclude $\tau_1 =_S \tau_k$ and the proof completes.

LEMMA 1. *Suppose that $A_1 + \cdots + A_p$, $B_1 + \cdots + B_q$ are full sum-terms. Then the following equivalence is true*

$$A_1 + \cdots + A_p = B_1 + \cdots + B_q \text{ holds iff each } A_i \text{ is equal to some } B_j \text{ and each } B_k \text{ is equal to some } A_l$$

PROOF. Proof follows immediately from $(*_3)$ and (4). For instance, if $p = 2$, $q = 2$ then we have the following equivalence

$(*_5)$ $A_1 + A_2 = B_1 + B_2$ iff $(A_1 = B_1 \wedge A_2 = B_2) \vee (A_1 = B_2 \wedge A_2 = B_1)$ □

LEMMA 2. *$S(A) = S(B)$ iff $A = B$.*

Proof follows directly from the definition (1).

Now we define the notion of *monomial*. This is a term t which is not of the form $(P+Q)$ for some P, Q. Let t be any term. It is a monomial just in three cases: t is an initial element or t is a variable or t has the form $S(P)$ for some P. Term of the form $S(P)$ will be called *S-monomial*. An equality of the form $m_1 = m_2$, where m_1, m_2 are monomials will be called *a monomial equality*. Such an equality will be called *a reduced monomial equality* if at least one of m_1, m_2 is not an S-monomial.

LEMMA 3. *Let $m_1 = m_2$ be a reduced monomial equality. This equality holds iff m_1, m_2 are equal as words.*

As a matter of fact, Lemma 1, Lemma 2 and Lemma 3 describe an algorithm, called Set-alg, by which one can decide whether any given terms t_1, t_2 are equal or not. Namely, to given equality $t_1 = t_2$ we apply Lemma 1 or Lemma 2 as many times as possible. At the end we obtain some logical expression Expr, built from certain reduced monomial equations $m_i = m_j$ using logical connectives $\wedge$ and $\vee$. Having in mind Lemma 3 we can calculate logical value of Expr. If the obtained value is $\top$, then the equality $t_1 = t_2$ holds. If the value is $\perp$, then the equality $t_1 = t_2$ does not hold. We shall illustrate this algorithm by some examples.

EXAMPLE 1. Let a, b, c, d be some initial elements. Calculate the logical value of a given equality:

$$1^\circ\ S(a+b) = S(b+a), \quad 2^\circ\ S(a+b) = S(b+\emptyset)$$
$$3^\circ\ S(a+S(b+c+d)+b) = S(b+a+S(d+c+b))$$

Solution. 1° We have the following equivalence-chain

$S(a+b) = S(b+a)$
iff $a+b = b+a$ (By Lemma 2)
iff $(a = b \wedge b = a) \ \vee\ (a = a \wedge b = b)$ (By $(*_5)$, i.e. by Lemma 1)

The answer is *yes* since by Lemma 3 the equalities $a = a$ and $b = b$ are true.

2° We have the following equivalence-chain

$S(a+b) = S(b+\emptyset)$
iff $a+b = b+\emptyset$ (By Lemma 2)
iff $(a = b \wedge b = \emptyset) \ \vee\ (a = \emptyset \wedge b = b)$ (By $(*)$, i.e. by Lemma 1)

The answer is *no* since by Lemma 3 equalities $a = b$, $a = \emptyset$ and $b = \emptyset$ are false.

3° By Lemma 2 we see that the given equality reduces to

$$a + S(b+c+d) + b = b + a + S(d+c+b)$$

Applying Lemma 1 this equality reduces to $S(b+c+d) = S(d+c+b)$. Applying Lemma 2 this equality reduces to $b+c+d = d+c+b$. Finally applying Lemma 1 and Lemma 3 we conclude that the answer is *yes*.

REMARK 2. Here, in brief, we describe an algorithm, called Calc, which is simpler than Set-alg. Let a term S_1 have the form $S(p_1 + p_2 + \cdots + p_m)$, where p_i are some initial elements. We shall say that such a term is *countable*. Term S_1 can be equal to certain other countable term, say $S(q_1 + q_2 + \cdots + q_n)$, where q_j are some initial elements. In such case each element p_i must be the same as some q_j and also each q_k must be the same as some p_r. For instance, if a, b, c are initial elements we have equality

$$S(a + b + a + b + c) = S(c + b + a + a)$$

Suppose now that a term t_1 has certain countable subterm S_1, and that a 'list' $S_1, S_2, \dots S_p$ contains all countable subterms of t, which are equal to S_1. Suppose that t_1 equals t_2. Then like $(3')$ we have the following substitutional chain

$$(\sigma_1) \qquad \tau_1 \to \tau_2 \to \tau_3 \to \cdots \to \tau_s \qquad (\tau_1 \text{ is } t_1,\ \tau_s \text{ is } t_2)$$

In the first step $\tau_1 \to \tau_2$ of this chain, any S_i remains unchanged or transforms to some countable term S_i', which is equal to S_i. The same holds for other steps. Denote by $S_1, \dots S_p, \dots S_P$ all terms occurring in (σ_1) which are equal to S_1.

Let C be an initial element not occurring in the chain (σ_1). In this chain replace all $S_1, \dots S_p, \dots S_P$ by C. If t is any term, by $t\langle C\rangle$ we denote the term obtained by that replacement. In such a way from (σ_1) we obtain the following 'formal chain'

$$(\sigma_2) \qquad \tau_1\langle C\rangle \to \tau_2\langle C\rangle \to \tau_3\langle C\rangle \to \cdots \to \tau_s\langle C\rangle$$

Obviously $\tau_1\langle C\rangle, \dots \tau_s\langle C\rangle$ are well-formed $(S,+)$-terms and in addition to that (σ_2) is a valid substitutional chain. So we conclude the following

$$\text{If } t_1 = t_2, \text{ then } t_1\langle C\rangle = t_2\langle C\rangle.$$

Now suppose that in (σ_2) every C is replaced by any terms $S_1, \dots S_p, \dots S_P$. Then from (σ_2) we shall obtain a chain which can be easily extended to a valid substitutional chain[2]. So, we conclude also

$$\text{If } t_1\langle C\rangle = t_2\langle C\rangle, \text{ then } t_1 = t_2.$$

The mentioned algorithm *Calc* is based on the equivalence

$$(\text{Cal}) \qquad t_1 = t_2 \quad \text{iff} \quad t_1\langle C\rangle = t_2\langle C\rangle$$

We illustrate Calc by two examples. First one is: prove or disprove the equality

$$S(a + S(S(a) + b) + S(b + S(a)) + c) = S(a + c + S(b + S(a)))$$

Using (Cal) we have the following equivalence-chain

$S(a + S(S(a) + b) + S(b + S(a)) + c) = S(a + c + S(b + S(a)))$

iff $S(a + S(p + b) + S(b + p) + c) = S(a + c + S(b + p))$ $\quad$ ($S(a)$ is replaced by p)

iff $S(a + q + q + c) = S(a + c + q)$ $\quad$ ($S(p + b)$, $S(b + p)$ are replaced by q)

iff $r = r$ $\quad$ ($S(a + q + q + c)$, $S(a + c + q)$ are replaced by r)

---

[2]For instance, if in the chain $S(a + C) \to S(C + a)$ we replace the first C by $S(p + q)$ and the second by $S(q + p)$ we obtain $S(a + S(p + q)) \to S(S(q + p) + a)$, which can be extended to this valid substitutional chain $S(a + S(p + q)) \to S(S(p + q) + a) \to S(S(q + p) + a)$.

So, the given equality is proven. Here p, q, r are initial elements.

The second example is: prove or disprove the equality

$$S(a + S(S(b)) + c) = S(c + a + S(S(b) + d))$$

Using (Cal) we have the following equivalence-chain

$$S(a + S(S(b)) + c) = S(c + a + S(S(b) + d))$$
iff $S(a + S(p) + c) = S(c + a + S(p + d))$ ($S(b)$ is replaced by p)
iff $S(a + q + c) = S(c + a + S(p + d))$ ($S(p)$ is replaced by q.)

As a matter of fact, because $S(p)$ does not appear on the right hand side we conclude that the last equality is false. Consequently the given equality is false.

Notice that the name Calc is related to the fact that this algorithm in some sense 'calculates' the given terms. Terms of the form $S(p_1 + p_2 + \cdots + p_m)$, where p_i are some initial elements, are called *countable*, since the algorithm *Calc* is 'able to calculate just them'.

3. Definition of finite sets

A *ground* term is a term not containing variables. Now we define the notion of a finite set:

(6) A finite set is either $\emptyset$ (called the empty set) or a ground term of the form $S(A)$ (called a non-empty set).

According to Lemma 1 any set A can be expressed in one of the forms

$$(*_6) \qquad 1^\circ:\ \emptyset, \qquad 2^\circ:\ S(A_1 + \cdots + A_n)$$

where $n = 1, 2, \ldots$ and $A_1 + \cdots + A_n$ is a full sum-term. One may suppose that A_i are pairwise different terms. These forms are called *the canonical forms* for set A. By virtue of Lemma 1 the form $(*_6)$ 2° is unique up to the order of $A_1, A_2, \ldots, A_n$. In the sequel we always assume that finite sets are given in a canonical form.

EXAMPLE 2. Let $1, 2, 3$ be initial elements. Then the ground term $S((1+3)+(2+3))$ is a finite set. One of its canonical forms is $S(1+2+3)$. Besides this there are also 5 others canonical forms

$$S(1+3+2),\ S(2+1+3),\ S(2+3+1),\ S(3+1+2),\ S(3+2+1)$$

which differ only in the order of $1, 2, 3$.

Concerning the given definition (6) of a finite set we point out that a finite set is defined as *a well defined term*. Consequently, we can produce various recursive definitions for them.

First, we define the relation $\in$:

(7) $x \in S(A)$ iff $x = A$
$x \in S(A_1 + A_2 + \cdots + A_n)$ iff $x = A_1$ or $x \in S(A_2 + \cdots + A_n)$ $(n > 1)$
$x \notin \emptyset$

For instance, $2 \in S(1+2+3)$. Indeed:

$$\begin{aligned} 2 \in S(1+2+3) \ &\text{iff} \ \ 2 = 1 \text{ or } 2 \in S(2+3) \\ &\text{iff} \ \ 2 \in S(2+3) \qquad \text{(Since } 2 = 1 \text{ is false)} \\ &\text{iff} \ \ 2 = 2 \text{ or } 2 \in S(3) \\ &\text{iff} \ \ 2 = 2 \qquad \text{(Since } 2 = 2 \text{ is true)} \end{aligned}$$

So, it is true that $2 \in S(1+2+3)$. But, for instance $2 \notin S(1+3)$. Indeed:

$$\begin{aligned} 2 \in S(1+3) \ &\text{iff} \ \ 2 = 1 \text{ or } 2 \in S(3) \\ &\text{iff} \ \ 2 \in S(3) \qquad \text{(Since } 2 = 1 \text{ is false)} \\ &\text{iff} \ \ 2 = 3 \end{aligned}$$

Since the equality $2 = 3$ is false we conclude that $2 \in S(1+3)$ is false too.

Notice that in general if $A_1, \dots, A_n$ are some given ground terms then $S(A_1 + \cdots + A_n)$ is the set whose all elements are $A_1, \dots, A_n$.

Bearing in mind Lemma 1 and the definition (7) one can easily prove the following well known equivalence (*Extensionality axiom in ZF set theory*)

$$A = B \ \leftrightarrow \ (\forall x)(x \in A \leftrightarrow x \in B)$$

where A, B are any finite sets and the variable x ranges over ground terms only.

The next step is to define $|A|$–the cardinal number of the set A. By use of the 'ordinary' notion of natural number we have the inductive definition

$$|\emptyset| = 0, \quad |S(A)| = 1, \quad |S(A_1 + A_2 + \cdots + A_n)| = 1 + |S(A_2 + \cdots + A_n)|.$$

Now we give several definitions, and each of them will be syntactical; in other words for each of them we can make a corresponding *decision algorithm*.

(Relation $\subseteq$) $\quad A \subseteq B$ iff $(\forall x)(x \in A \Rightarrow x \in B)$
(Operation $\cup$) $\quad \emptyset \cup x = x \quad$ (x is any finite set)
$S(A_1) \cup S(B_1 + \cdots + B_m)$ is $S(A_1 + B_1 + \cdots + B_m)$
$S(A_1 + \cdots + A_n) \cup S(B_1 + \cdots + B_m)$ is $S(A_2 + \cdots + A_n) \cup S(B_1 + \cdots + B_m)$ if $A_1 \in S(B_1 + \cdots + B_m)$,
otherwise it is $S(A_1) \cup (S(A_2 + \cdots + A_n) \cup S(B_1 + \cdots + B_m))$
(Operation $\cap$) $\quad \emptyset \cap x = \emptyset \quad$ (x is any finite set)
$S(A_1 + \cdots + A_n) \cap S(B_1 + \cdots + B_m)$ is $S(A_2 + \cdots + A_n) \cap S(B_1 + \cdots + B_m)$ if $A_1 \notin S(B_1 + \cdots + B_m)$,
otherwise it is $S(A_1) \cup \big(S(A_2 + \cdots + A_n) \cap S(B_1 + \cdots + B_m)\big)$
(Operation $\smallsetminus$) $\quad \emptyset \smallsetminus x = \emptyset \quad$ (x is any finite set)
$S(A_1 + \cdots + A_n) \smallsetminus S(B_1 + \cdots + B_m)$ is $S(A_2 + \cdots + A_n) \smallsetminus S(B_1 + \cdots + B_m)$ if $A_1 \in S(B_1 + \cdots + B_m)$,
otherwise it is $S(A_1) \cup \big(S(A_2 + \cdots + A_n) \smallsetminus S(B_1 + \cdots + B_m)\big)$

Now we shall define the ordered pair of two member terms x, y, in symbols $\Pi(x, y)$. There are two ways to do this: one is to extend Ω by a new binary operational symbol Π and to add no new axiom concerning Π, and to regard term

$\Pi(x,y)$ as the ordered pair of x and y. The alternative way is to adopt Wiener–Kuratowski idea, i.e., to introduce the following definition

$$\Pi(x,y) = S(S(x) + S(x+y))$$

Further, we can in the usual way define cartesian product $X \times Y$ of two sets, of more sets, a binary, ternary,... relation, a function $f : X \to Y$, etc. Again and again each of such notions is determined by some ground term.

EXAMPLE 3. Let $A = S(1+2+3)$, $B = S(a+b)$. Then

$$A \times B = S(\Pi(1,a) + \Pi(1,b) + \Pi(2,a) + \Pi(2,b) + \Pi(3,a) + \Pi(3,b))$$

The term $S(\Pi(1,a) + \Pi(2,b) + \Pi(3,a))$ determines a function $f : A \to B$ such that $f(1) = a$, $f(2) = b$, $f(3) = a$.

We have already mentioned that the finite sets defined by (6) satisfy Extensionality axiom of ZF set theory. It is not difficult to see that, in Fin-set, except *Axiom of infinity*, all other axioms of ZF theory can be proved in a simple way. Moreover, if some axioms say that there exist some sets $x, y, \dots$, then one can make 'algorithmic proof', which effectively construct such sets $x, y, \dots$

We illustrate this idea by considering *Subset axioms*. So, let $t = S(a_1 + \cdots + a_n)$ be a given set and $\phi(x)$ any given formula, condition containing x as a free variable. Suppose that for each a_i we can determine whether $\phi(a_i)$ is true or false. We should prove that there exists a set T such that: $x \in T$ iff $x \in t \wedge \phi(x)$.

Denote by $b_1, \dots, b_k$ all of those a_i for which $\phi(a_i)$ is true. If $k = 0$, then $T = \emptyset$, otherwise $T = S(b_1 + \cdots + b_k)$. The proof is complete.

EXAMPLE 4. Let $t = S(1+2+3+4+5)$ and let $\phi(x)$ be the following condition $x \in S(1+4+8+9)$. Then $T = S(1+4)$. However, suppose that we extend the language Ω by a relation symbol ev ('to be even') and also add the following new axioms ev(2), ev(4), ev(6). Let $\phi(x)$ be the formula ev(x). Then the corresponding T is $S(2+4)$.

Matematički fakultet
11000 Beograd
Serbia
spresic@matf.bg.ac.yu