A finite axiomatization of flowchart schemes

M. Bartha

1. Introduction

An equational axiomatization of flowchart schemes and their behaviours, being the syntax and semantics of flowchart algorithms, was given by Bloom and Ésik in [B—Es]. This paper is another approach toward the same goal, characterizing the algebra of schemes with a different set of operations. We use separated sum and a constant ε instead of the pairing operation, and replace iteration by an operation called the feedback. The advantage of using this operation is that vector iteration can be done simply by a repeated application of the feedback. This advantage comes out apparently in the form of the axioms that are much simpler than those listed in [B—Es].

Since the algebra of flowchart schemes is sorted by the infinite set $N \times N$ (N denotes the set of all nonnegative integers), to describe our system of axioms we use a scheme of axioms rather than a set of ordinary equational axioms where both sides of the equations are terms built up from constants and variable symbols of fixed sort with the given operations. In our sense such a scheme consists of equation patterns of the following form. The terms on the left and right side are built up from variables of variable sort and subterms denoting algebraic constants. These subterms, however, are allowed to depend on the sort of the variables so that they are uniquely determined by a fixed choice of the sorts of the variables occuring in the whole term. A scheme of axioms is called finite if the number of equation patterns is finite. In this sense the scheme of axioms developed in [B—Es] is infinite. It turns out, however, that a more careful treatment of algebraic constants yields a finite scheme.

As the scheme algebra operations of Bloom and Ésik are easy to derive from our ones (and vice versa), it is possible to approve our scheme of axioms by proving the equivalence of the two axiom systems remaining strictly within the framework of equational logic. This, however, would require a tremendous amount of computation. Instead, we follow the way of constructing suitable normal forms of terms (as it was done also in [B—Es]), which is easy to illustrate by schematic proof-diagrams.

2. The axiomatization of flowchart schemes

We shall consider three classes of $(N\times N)$-sorted algebras, called P, M and S-algebras, respectively. If A is such an algebra, then $A(p, q)$ denotes the underlying set of A corresponding to sort (p, q). The notation $f\colon p\to q$ is introduced with the meaning $f\in A(p, q)$ if A is understood.

A P-algebra is an $(N\times N)$-sorted algebra equipped with the following operations and constants.

Composition: a binary operation which maps $A(p, q)\times A(q, r)$ into $A(p, r)$ for each triple $p, q, r\in N$. Composition is usually denoted by juxtaposition or $\cdot$ if it is intended to be emphasized. Composition is in fact a collection of binary operations $\cdot_{(p,q,r)}$, but the subscript (p, q, r) is omitted for simplicity.

Separated sum: also a binary operation mapping $A(p_1, q_1)\times A(p_2, q_2)$ into $A(p_1+p_2, q_1+q_2)$ for each choice p_1, q_1, p_2, q_2 of nonnegative integers. Separated sum is denoted by $+$.

There are three constants: $1\in A(1, 1)$, $0\in A(0, 0)$ and $x\in A(2, 2)$.

Terms constructed from these constants with the above operations are called base P-terms. Clearly, every base P-term is of sort (p, p) for some $p\in N$. For each $n\in N$ let $t(n)$ denote the base P-term defined recursively as follows.

(i) if $n=0$ or $n=1$, then $t(n)=n$,

(ii) $t(n+1)=t(n)+1$ if $n\geqq 1$.

However, we shall write n instead of $t(n)$ if there is no danger of confusion.

Definition 1. A permutation algebra is a P-algebra satisfying the following equational axioms:

$P1$: $f\cdot(g\cdot h)=(f\cdot g)\cdot h$ for all $f\colon p\to q$, $g\colon q\to r$, $h\colon r\to s$;

$P2$: $f+(g+h)=(f+g)+h$ for all $f\colon p_1\to q_1$, $g\colon p_2\to q_2$, $h\colon p_3\to q_3$;

$P3$: $p\cdot f=f$ and $f\cdot q=f$ for all $f\colon p\to q$;

$P4$: $f+0=f$ and $0+f=f$ for all $f\colon p\to q$;

$P5$: $(f_1\cdot g_1)+(f_2\cdot g_2)=(f_1+f_2)\cdot(g_1+g_2)$ for all $f_i\colon p_i\to q_i$, $g_i\colon q_i\to r_i$, $i=1,2$;

$P6^*$: $x\cdot x=2$;

$P7^*$: $(1+x)(x+1)(1+x)=(x+1)(1+x)(x+1)$.[1]

For each pair $(p, q)\in N\times N$ let $\Pi(p, q)$ denote the set of all p-ary permutations if $p=q$, else let $\Pi(p, q)=\varnothing$. Define composition and separated sum over the sets $\Pi(p, q)$ in the usual way, and let 1 and 0 be the unique elements of $\Pi(1, 1)$ and $\Pi(0, 0)$, respectively. Interpreting x as the transposition $2\to 2$ we get a P-algebra Π, which is clearly a permutation algebra.

[1] $P6^*$ and $P7^*$ will be replaced by a single axiom called the block permutation axiom. In fact $P6^*$ and $P7^*$ are the weakest special cases of this axiom that are enough to prove that the P-algebra of all permutations is the initial permutation algebra.

A base P-term is called simple if it is equal to k for some $k \in N$, or it is of the form $(i-1)+x+(n-i)$ for some $n \geqq 1$, $i \in [n]=\{1, 2, \ldots, n\}$. (In the latter case if $(i-1)$ or $(n-i)$ is 0, then it is omitted according to $P4$.) The term $(i-1)+x+(n-i)$ will be denoted by $x_n(i)$. Let P denote the collection of axioms $P1, \ldots, P7$. The following remark can be easily proved using only the "magmoid identities" (cf. [AD]) $P1, \ldots, P5$.

Remark. For every base P-term t there exists a base P-term t' which is the composite of a number of simple base P-terms (called the factors of t') and $P \vdash t=t'$, i.e. the identity $t=t'$ is provable from P. t' is said to be in split normal form (s.n.f. for short).

Lemma 1. Let $n \geqq 1$ and $i \in [n-1]$ ($[0]=\emptyset$). Then

$$x_n(1)x_n(2)\cdot \ldots \cdot x_n(n)x_n(i) = x_n(i+1)x_n(1)x_n(2)\cdot \ldots \cdot x_n(n)$$

is provable from P.

Proof. (See also Fig. 1 for the case $n=3$, $i=1$.)

$$x_n(1)x_n(2)\cdot \ldots \cdot x_n(n)x_n(i) = x_n(1)\cdot \ldots \cdot x_n(i)x_n(i+1)x_n(i)x_n(i+2)\cdot \ldots \cdot x_n(n) =$$
$$= (\text{by } P7) = x_n(1)\cdot \ldots \cdot x_n(i-1)x_n(i+1)x_n(i)x_n(i+1)\cdot \ldots \cdot x_n(n) =$$
$$= x_n(i+1)x_n(1)\cdot \ldots \cdot x_n(n).$$

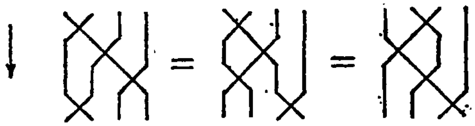

Fig. 1. Proof of Lemma 1 on an example

In two steps of the above derivation we used the obvious identity $x_n(k)x_n(l)= =x_n(l)x_n(k)$, where $1 \leqq k < l-1 < n$.

For a base P-term t let $|t|$ denote the value of t in Π. (In other words $|\ |$ is the unique homomorphism of the initial P-algebra into Π.) Since every permutation is expressible as a composite of permutations of the form $|x_n(i)|$, the following proposition says that the initial permutation algebra is Π.

Proposition 1. Let t and t' be base P-terms. If $|t|=|t'|$, then $P \vdash t=t'$.

Proof. By the Remark we can assume that t and t' are both in s.n.f. Listing the factors of t in reverse order we get a term t^{-1} such that $P \vdash t^{-1}t=n$ for appropriate $n \in N$. If we can prove $t't^{-1}=n$, then we get the required proof: $t'= =t'(t^{-1}t)=(t't^{-1})t=t$. Hence it is enough to show that if $|t|=|n|$ for some base P-term t in s.n.f., then $P \vdash t=n$. We follow an induction on n. If $n \leqq 1$, then the statement is trivial. Let $n \geqq 2$. If none of the factors of t is equal to $x_{n-1}(1)$, then $t=1+t'$, and the induction hypothesis works for t'. If $x_{n-1}(1)$ occurs in t, then assume indirectly that $P \nvdash t=n$, and the length of t (i.e. the number of the factors of t) is minimal. Split $t=\alpha x_{n-1}(1)\beta$ so that $x_{n-1}(1)$ should not occur in α. By

Lemma 1 and the assumption that the length of t is minimal we get that $P\vdash x_{n-1}(1)\beta=\gamma x_{n-1}(1)x_{n-1}(2)\cdot\ldots\cdot x_{n-1}(j)$ for some $j\in[n-1]$, where $x_{n-1}(1)$ does not occur even in γ. We conclude that $P\vdash t=\alpha\gamma x_{n-1}(1)\ldots x_{n-1}(j)$ which is a contradiction, since in this case $|t|(1)=j+1>1$.

Corollary 1. The initial permutation algebra is Π.

In the light of Proposition 1, when working in permutation algebras we identify a base P-term t with the permutation $|t|$.

The following definition is adopted from [B—Es]. Let s be a finite sequence $(n_1, \ldots, n_r)$ of nonnegative integers and suppose that $\alpha\colon r\to r$ is a permutation. Let n be the sum of the numbers n_i.

Definition 2. $\alpha\# s\colon n\to n$ is the permutation which takes a number in $[n]$ of the form

$$n_1+\ldots+n_k+j,$$

where $j\in[n_{k+1}]$, to the number $y+j$, where y is the sum of all numbers n_i such that $\alpha(i)<\alpha(k+1)$.

From now on we drop the axioms $P6^*$ and $P7^*$, replacing them by the stronger block permutation axiom of [ES]:

$$P6;\, f_1+f_2 = x \# (p_1,p_2)\cdot(f_2+f_1)\cdot x \# (q_2,q_1) \quad \text{for all}$$

$$f_i\colon p_i \to q_i, \quad i=1,2.$$

Assume that $x\#(p_1,p_2)$ and $x\#(q_2,q_1)$ are represented in $P6$ by base P-terms in a minimal length s.n.f. Then we see that $P6^*$ and $P7^*$ are indeed consequences of $P6$. (Take $f_1=f_2=1$ in the case of $P6$, and $f_1=x$, $f_2=1$ for $P7$.) Since $P6$ is also valid in Π, Π remains initial. Now the following lemma is true in every permutation algebra.

Lemma 2. Let $\alpha\colon r\to r$ be a permutation and $f_i\colon p_i\to q_i$ for each $i\in[r]$. Then

$$\sum_{i=1}^{r} f_i = (\alpha^{-1}\# s_1)\cdot\Big(\sum_{i=1}^{r}\cdot f_{\alpha(i)}\Big)\cdot(\alpha\# s_2),$$

where $s_1=(p_1,\ldots,p_r)$ and $s_2=(q_{\alpha(1)},\ldots,q_{\alpha(r)})$.

Proof. Easy induction on the length of a base P-term in s.n.f. representing α.

An M-algebra is an $(N\times N)$-sorted algebra having all the operations and constants of P-algebras and two further constats: ε of sort $(2,1)$ and 0_1 of sort $(0,1)$. As in the case of P-algebras, base M-terms are those built up from the constants using the given operations. Define base M-terms ε_n and 0_n for each $n\in N$ as follows.

(i) $\varepsilon_0=0_1,\quad \varepsilon_1=1,\quad \varepsilon_2=\varepsilon,\quad 0_0=0,\quad 0_2=0_1+0_1;$

(ii) if $n\geqq 2$ then $\varepsilon_{n+1}=(\varepsilon_n+1)\cdot\varepsilon,\quad 0_{n+1}=0_n+0_1.$

Definition 3. A mapping algebra is an M-algebra satisfying the identities belonging to P and the following ones.

$M1$: $(\varepsilon+1)\cdot\varepsilon=(1+\varepsilon)\cdot\varepsilon$;

$M2$: $x\cdot\varepsilon=\varepsilon$;

$M3$: $(1+0_1)\cdot\varepsilon=1$.

For $(p,q)\in N\times N$ let $\theta(p,q)$ be the set of all mappings of $[p]$ into $[q]$. Let 0_1 and ε be the unique elements of $\theta(0,1)$ and $\theta(2,1)$, respectively, and interpret the P-algebra operations and constants over the sets $\theta(p,q)$ as an obvious extension of their interpretation in Π. In this way we get the M-algebra θ, which is clearly a mapping algebra as well.

A base M-term is called simple if it is a simple base P-term, or it is one of the forms

(i) $(i-1)+0_1+(n-i)$, or

(ii) $(i-1)+\varepsilon+(n-i)$

for some $n\geqq 1$, $i\in[n]$. Let M denote the collection of axioms $M1$, $M2$, $M3$. As in the case of base P-terms, for every base M-term t these exists a base M-term t' such that t' is the composite of simple base M-terms and $P\vdash t=t'$. Moreover, by $P6$ it is possible to rearrange the factors of t' in such a way that $P\cup M\vdash t'=\alpha\beta$, where α is a base P-term in s.n.f., but none of the factors of β is a simple base P-term (exept when $\beta=k$ for some $k\in N$). But then $P\cup M\vdash\beta=\varepsilon_{j_1}+\ldots+\varepsilon_{j_m}$ for some non-negative integers m, $j_1,\ldots,j_m$.

For a base M-term t let $|t|$ denote the value of t in θ. The above reasoning together with Proposition 1 yields the following result.

Proposition 2. Let t and t' be base M-terms. If $|t|=|t'|$, then $P\cup M\vdash t=t'$. Equivalently, the initial mapping algebra is θ.

As in the case of permutation algebras, when working in mapping algebras we identify a base M-term t with the mapping $|t|$.

Let $\alpha\colon p\to q$ be a mapping and $B\subseteq[q]$. We say that α is onto B if $\alpha^{-1}(j)\neq\emptyset$ for any $j\in B$. If $\alpha_i\colon p_i\to q$, $i=1,2$ are mappings, then define their pairing $\langle\alpha_1,\alpha_2\rangle\colon p_1+p_2\to q$ as

$$\langle\alpha_1,\alpha_2\rangle(i)=\begin{cases}\alpha_1(i) & \text{if } i\in[p_1]\\ \alpha_2(i-p_1) & \text{if } i\in[p_1+p_2]-[p_1].\end{cases}$$

An S-algebra has one further unary operation beyond the M-algebra operations and constants. This operation will be called the feedback and denoted by $\uparrow$. In an S-algebra the feedback maps $A(1+p,1+q)$ into $A(p,q)$ for each pair $(p,q)\in N\times N$.

Let Σ be a doubly ranked set. (Recall from [B—Es] that

$$\Sigma=\{\Sigma(p,q)|(p,q)\in N\times N\},$$

where the sets $\Sigma(p, q)$ are pairwise disjoint.) A Σ-flowchart scheme with p begins and q exist consists of:

(i) A finite nonempty set V of labelled vertices, where the labels belong to the union of four, pairwise disjoint sets:

$$(\cup\Sigma)\cup\{b_i|i\in[p]\}\cup\{\mathrm{ex}_j|j\in[q]\}\cup\{\perp\}.$$

For each $i\in[p]$ and $j\in[q]$ there exists exactly one vertex labelled by b_i, called the i-th begin vertex, and exactly one vertex labelled by ex_j, the j-th exit vertex. Moreover, exactly one vertex, the loop vertex is labelled by $\perp$. For each $v\in V$ denote v_{in} and v_{out} the following sets of so called "signed vertices". Let α be the label of v. If $\alpha\in\Sigma(r, s)$, then

$$v_{\mathrm{in}} = \{(v, i)|i\in[r]\} \quad \text{and} \quad v_{\mathrm{out}} = \{(v, j)|j\in[s]\}.$$

If $\alpha=\mathrm{ex}_j$ or $\alpha=\perp$, then $v_{\mathrm{in}}=\{(v, 1)\}$ and $v_{\mathrm{out}}=\emptyset$, else (i.e. if $\alpha=b_i$) $v_{\mathrm{in}}=\emptyset$ and $v_{\mathrm{out}}=\{(v, 1)\}$. Signed vertices belonging to begin, exit and loop vertices will be identified with their label.

(ii) A mapping E of $V_{\mathrm{out}}=\cup(v_{\mathrm{out}}|v\in V)$ into $V_{\mathrm{in}}=\cup(v_{\mathrm{in}}|v\in V)$. E represents the edges of the scheme, and in this sense we consider Σ-flowchart schemes as directed graphs.

Define the S-algebra operations on Σ-schemes as follows.

— The composition of schemes $F\colon p\to q$ and $G\colon q\to r$ is constructed in three steps.

1) Take the disjoint union of the graphs of F and G.

2) Direct each edge of F ending in any exit vertex of F, say ex_j to the signed vertex pointed by $E(b_j)$ in G.

3) Identify the lopp vertices of F and G, and delete the exists of F as well as the begins of G (together with all the incoming and outgoing edges, of course).

— The sum of schemes $F_1\colon p_1\to q_1$ and $F_2\colon p_2\to q_2$ is taken as follows.

1) Take the disjoint union of F_1 and F_2.

2) Relabel each begin vertex of F_2 from b_i to b_{p_1+i} and each exit vertex of F_2 from ex_j to ex_{q_1+j} $(i\in[p_2], j\in[q_2])$.

3) Identify their loop vertices.

— If F is a scheme $1+p\to 1+q$, then $\uparrow F$ is constructed as follows.

1) Direct each edge of F ending in ex_1 to $E(b_1)$ if $E(b_1)\neq\mathrm{ex}_1$, else to $\perp$.

2) Delete vertices b_1 and ex_1, and relabel b_{i+1} and ex_{j+1} as b_i (resp. ex_j) for $i\in[p]$, $j\in[q]$.

— The interpretation of the constants is shown by Fig. 2.

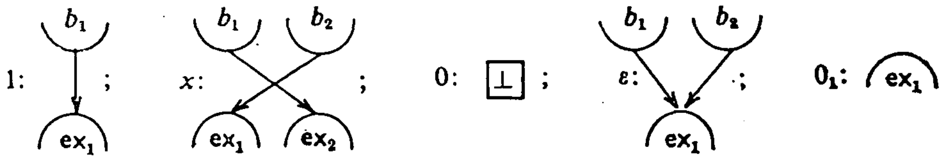

Fig. 2. Interpretation of the constants as schemes

The loop vertex is omitted on the figure (exept for 0).

Definition 4. A scheme algebra is an S-algebra satisfying the identities $P\cup M$ and the following ones (the collection of these identities will be denoted by PMS).

$S1$: $\uparrow(f_1+f_2)=\uparrow f_1+f_2$ for $f_1\colon 1+p_1\to 1+q_1$, $f_2\colon p_2\to q_2$;

$S2$: $\uparrow\uparrow((x+p)f)=\uparrow\uparrow(f(x+q))$ for $f\colon 2+p\to 2+q$;

$S3$: $\uparrow(f(1+g))=(\uparrow f)g$ for $f\colon 1+p\to 1+q$, $g\colon q\to r$;

$S4$: $\uparrow((1+g)f)=g\cdot\uparrow f$ for $f\colon 1+q\to 1+r$, $g\colon p\to q$;

$S5$: $\uparrow 1=0$ and $\varepsilon\cdot\bot=\bot+\bot$, where $\bot=\uparrow\varepsilon$;

$S6$: $\uparrow x=1$.

It is easy to see that Σ-schemes together with the operations and constants defined above form a scheme algebra, which will be denoted by $\mathrm{Sch}\,(\Sigma)$.

Lemma 3. If $\alpha\colon 1+p\to 1+q$ is a mapping with $\alpha(1)\neq 1$, then there exists a mapping $\beta\colon p\to q$ such that $PMS\vdash\uparrow\alpha=\beta$.

Proof. Split α into the form

$$(1+\beta_1)(x+r)(1+\beta_2),$$

where $\beta_1\colon p\to 1+r$ and $\beta_2\colon 1+r\to q$ are appropriate mappings. Then

$$\uparrow\alpha=(\text{by } S3 \text{ and } S4)=\beta_1\cdot\uparrow(x+r)\beta_2=(\text{by } S1 \text{ and } S6)=\beta_1\beta_2.$$

Claim. The following identities are valid in every scheme algebra.

$S1^*$: $\uparrow^l(f_1+f_2)=\uparrow^l f_1+f_2$ for $f_1\colon l+p_1\to l+q_1$, $f_2\colon p_2\to q_2$.

($\uparrow^l$ denotes the l-fold application of $\uparrow$.)

$S3^*$: $\uparrow^l(f(l+g))=(\uparrow^l f)\cdot g$ for $f\colon l+p\to l+q$, $g\colon q\to r$.

$S4^*$: $\uparrow^l((l+g)f)=g\cdot\uparrow^l f$ for $f\colon l+q\to l+r$, $g\colon p\to q$.

Proof. Trivial.

$X1$: $\uparrow^l((\alpha+p)f(\alpha^{-1}+q))=\uparrow^l f$ for $f\colon l+p\to l+q$ and permutation α.

Proof. Put α into s.n.f., and apply $S2$ with $S3^*$ and $S4^*$ repeatedly.

$X2$: $\uparrow^{l_1+l_2}((l_1+x\,\#(l_2,p_1)+p_2)(f_1+f_2)(l_1+x\,\#(q_1,l_2)+q_2))=$

$=\uparrow^{l_1}f_1+\uparrow^{l_2}f_2$ for $f_i\colon l_i+p_i\to l_i+q_i$, $i=1,2$.

Proof. A schematic derivation is shown by Fig. 3.

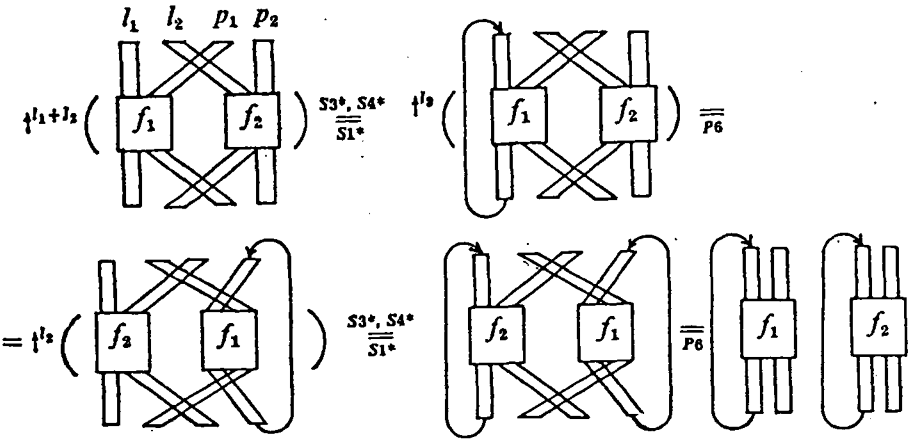

Fig. 3. Schematic proof of X2

The same proof formally:

$$\uparrow^{l_1+l_2}((l_1+x\,\#(l_2,p_1)+p_2)(f_1+f_2)(l_1+x\,\#(q_1,l_2)+q_2)) =$$

$$= \uparrow^{l_2}(\uparrow^{l_1}((l_1+x\,\#(l_2,p_1)+p_2)((f_1+f_2)(l_1+x\,\#(q_1,l_2)+q_2)))) = (S4^*)$$

$$= \uparrow^{l_2}((x\,\#(l_2,p_1)+p_2)\cdot\uparrow^{l_1}((f_1+f_2)(l_1+x\,\#(q_1,l_2)+q_2))) = (S3^*)$$

$$= \uparrow^{l_2}((x\,\#(l_2,p_1)+p_2)\cdot\uparrow^{l_1}(f_1+f_2)(x\,\#(q_1,l_2)+q_2)) = (S1^*)$$

$$= \uparrow^{l_2}((x\,\#(l_2,p_1)+p_2)(\uparrow^{l_1}f_1+f_2)(x\,\#(q_1,l_2)+q_2)) = (P6)$$

$$= \uparrow^{l_2}((l_2+x\,\#(p_1,p_2))(f_2+\uparrow^{l_1}f_1)(l_2+x\,\#(q_2,q_1))) = (S4^*,\ S3^*,\ S1^*)$$

$$= (x\,\#(p_1,p_2))(\uparrow^{l_2}f_2+\uparrow^{l_1}f_1)(x\,\#(q_2,q_1)) = (P6) = \uparrow^{l_1}f_1+\uparrow^{l_2}f_2.$$

In the sequel we shall omit the tedious formal proofs restricting ourselves to the corresponding schematic ones.

$X3a$: $\uparrow^{q}(x\,\#(p,q)+l)(f+g)) = (f+l)g$ for

$f\colon p \to q$, $g\colon q+l \to r$,

$X3b$: $\uparrow^{q}((g+f)(x\,\#(r,q)+l)) = f(g+l)$ for

$f\colon p \to q+l$, $g\colon q \to r$.

Proof. Both cases a and b can be proved in a similar way, so we only prove $X3a$. (Dotted lines indicate composition in Fig. 4.)

$X4$: $\uparrow(f(\varepsilon+q)) = \uparrow^{2}((\varepsilon+p)f)$ for $f\colon 1+p \to 2+q$.

Proof. See Fig. 5.

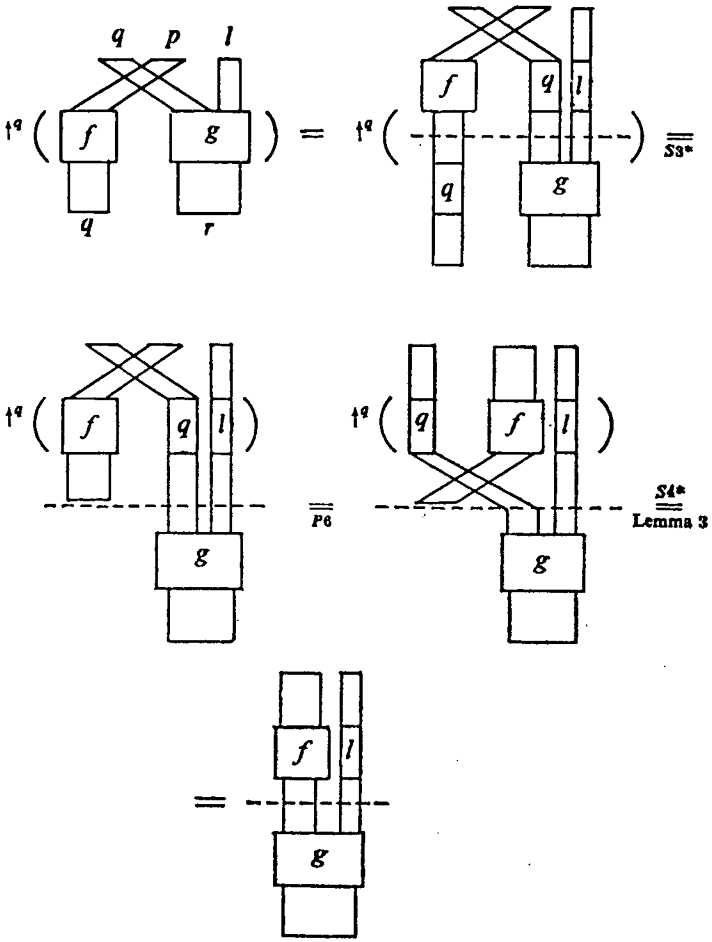

Fig. 4. Proof of X3a

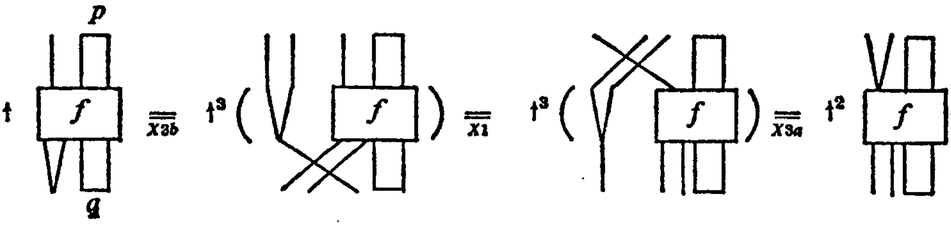

Fig. 5. Proof of X4

Lemma 4. Let $\alpha\colon r\to 1+p$ and $\beta\colon 1+q\to s$ be mappings, $f\colon p\to q$. In every scheme algebra we have

a) if $\alpha(1)=1$ and $\beta(1)\neq 1$, then

$$\uparrow(\alpha(1+f)\beta)=\alpha'(1+f)\beta';$$

b) if $\beta(1)=1$ and $\alpha(1)\neq 1$, then

$$\uparrow(\alpha(1+f)\beta)=\uparrow(\alpha''f\beta'');$$

c) if $\alpha(1)=\beta(1)=1$, then

$$\uparrow(\alpha(1+f)\beta)=\uparrow(\alpha'''(\perp+f)\beta''')$$

for appropriate mappings $\alpha', \alpha'', \alpha''', \beta', \beta'', \beta'''$; moreover $\alpha'''(1)=1$.

Proof.

Case a: By assumption α can be written in the form $\alpha=(1+\alpha')(\varepsilon+p)$. Then

$$\alpha(1+f)\beta=(1+\alpha')(\varepsilon+p)(1+f)\beta=(1+\alpha')(2+f)(\varepsilon+q)\beta=$$
$$=(1+\alpha'(1+f))(\varepsilon+q)\beta.$$

Hence by $S4$:

$$\uparrow(\alpha(1+f)\beta)=\alpha'(1+f)\cdot\uparrow((\varepsilon+q)\beta).$$

Since $\beta(1)\neq 1$, Lemma 3 says that $\uparrow((\varepsilon+q)\beta)=\beta'$ for some mapping β'.

Case b: In this case β can be written in the form

$$\beta=(1+\beta'')(\varepsilon+s-1),$$

so

$$\uparrow(\alpha(1+f)\beta)=\uparrow((\alpha(1+f)\beta''(\varepsilon+s-1))=(\text{by } X4)$$
$$=\uparrow^2((\varepsilon+r-1)\alpha(1+f)(1+\beta''))=\uparrow(\uparrow((\varepsilon+r-1)\alpha(1+f\beta'')))=(\text{by } S3)$$
$$=\uparrow(\uparrow((\varepsilon+r-1)\alpha)f\beta'')=(\text{by Lemma 3})=\uparrow(\alpha''f\beta'').$$

Case c: As in the previous case we have

$$\uparrow(\alpha(1+f)\beta)=\uparrow(\uparrow((\varepsilon+r-1)\alpha)f\beta'')$$

but now

$$(\varepsilon+r-1)\alpha=(\varepsilon+r-1)(1+\alpha')(\varepsilon+p)=(1+r)(2+\alpha')(\varepsilon_3+p);$$
$$\uparrow((\varepsilon+r-1)\alpha)=(\text{by } S4)=(1+\alpha')\uparrow(\varepsilon_3+p)=(1+\alpha')(\varepsilon\cdot\perp+p)=$$
$$=(1+\alpha')(\varepsilon+p)(\perp+p).$$

Putting $\alpha'''=(1+\alpha')(\varepsilon+p)$ and $\beta'''=\beta''$ we get:

$$\uparrow(\alpha(1+f)\beta)=\uparrow(\alpha'''(\perp+p)f\beta''')=\uparrow(\alpha'''(\perp+f)\beta''').$$

We call Σ-terms those S-terms that are built up from the elements of Σ considered as atomic terms (recall that Σ is a doubly ranked alphabet) and from the constants, using the given operations. Since the S-algebra of Σ-terms is freely generated by Σ, each homomorphism of it into the algebra $\mathrm{Sch}(\Sigma)$ is uniquely determined by its restristion to Σ. Let $|\ |$ be the homomorphism determined by the mapping shown by Fig. 6.

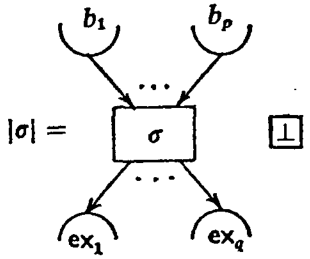

Fig. 6. $\sigma \in \Sigma(p, q)$ *as an atomic scheme*

A Σ-term t is said to be in weak normal form (w.n.f.) if

$$t = \uparrow^l(\alpha(a_1 + \ldots + a_n)\beta),$$

where

(i) $a_i \in \Sigma$ or $a_i = 1$ or $a_i = \perp$ for each $i \in [n]$,

and there exists at least one $j \in [n]$ such that $a_j = \perp$.

(ii) α and β are mappings of appropriate sort.

Lemma 5. For each Σ-term t there exists a Σ-term t' in w.n.f. such that $t = t'$ is provable from *PMS*.

Proof. Induction on the structure of t. If t is a constant, then its simplest w.n.f. is one of the following: $1 = (1 + 0_1)(1 + \perp)$, $0 = 0_1 \cdot \perp$, $x = (x + 0_1)(2 + \perp)$, $0_1 = 0_1 \cdot \perp \cdot 0_1$, $\varepsilon = (\varepsilon + 0_1)(1 + \perp)$. These identities are easy to prove. If $t = \sigma \in \Sigma(p, q)$, then its w.n.f. is $(p + 0_1)(\sigma + \perp)$. Let $t = t_1 \text{ op } t_2$, where op$= +$or$\cdot$, and let t_1' and t_2' be some w.n.f.-s of t_1 and t_2, respectively. If op$= +$, then we get a w.n.f. of t by applying $X2$ for $f_1 = t_1'$ and $f_2 = t_2'$. If op$= \cdot$, then apply $X3$ with $l = 0$ (both cases a and b are appropriate), and then $X2$ together with $S3^*$ or $S4^*$ to get the required w.n.f. of t. For $t = \uparrow t'$ the induction step is trivial.

Definition 5. A Σ-term $t\colon p \to q$ is said to be in normal form (n.f.) if

$$t = \uparrow^l(\langle \alpha_1 + 0_{k+1}, \alpha_2 \rangle \cdot (\sum_{i-1}^{n} \sigma_i + \perp + k) \cdot \langle \beta_2, 0_l + \beta_1 \rangle),$$

where

(i) $n \geqq 0, \sigma_i \in \Sigma(r_i, s_i)$ for each $i \in [n]$,

$$\sum_{i=1}^{n} r_i = r, \quad \sum_{i=1}^{n} s_i = s;$$

(ii) $\alpha_1, \alpha_2, \beta_1$ and β_2 are mappings such that

$\alpha_1\colon l \to r+1$ and $\beta_1\colon k \to q$ are injective and monotonic,

$\alpha_2\colon p \to r+1+k$ is onto $[r+1+k] - [r+1]$;

$\beta_2\colon s \to l+q$ is onto $[l]$.

Lemma 6. For each Σ-term $t\colon p \to q$ there exists a Σ-term t' in n.f. such that $t = t'$ is provable from *PMS*.

Proof. By Lemma 5 we can assume that t is in w.n.f., i.e. $t=\uparrow^l(\alpha(a_1+\ldots+a_m)\beta)$. Moreover, by $P6$ and $S5$ we can assume that for some $n<m$ we have: $a_i\in\Sigma$ if $i\in[n]$, $a_{n+1}=\perp$ and $a_j=1$ for each $n+1\leqq j\leqq m$. Let $k=m-n-1$. We prove by induction on the number $k+l$. If $k+l=0$, then we have nothing to prove. For $k+l>0$ we distinguish two cases. By assumption, α: $l+p\to r+1+k$ and β:$s+k\to\to l+q$ for some $r,s\in N$.

Case a: $l>0$ and one of conditions $(*)$, $(**)$ or $(***)$ below is satisfied. Suppose that for some $j\in[k]$

$$(\alpha^{-1}(r+1+j)\cup\beta(s+j))\cap[l]\neq\emptyset. \qquad (*)$$

By $P6$ and $X1$

$$t=\uparrow^l(\alpha'(1+a_1+\ldots+a_{j-1}+a_{j+1}+\ldots+a_m)\beta')$$

is provable for some α' and β' such that $\alpha'(1)=1$ or $\beta'(1)=1$. Using Lemma 4 we obtain a simpler w.n.f. of t by decreasing the number k or l, which makes the induction hypothesis applicable. If this type of reduction cannot be applied, i.e. condition $(*)$ does not holds for any $n+1<j\leqq m$, then α and β can be written in the form

$$\alpha=\langle\alpha_1+0_{k+1},\alpha_2\rangle \quad\text{and}\quad \beta=\langle\beta_2,0_l+\beta_1\rangle,$$

where α_1: $l\to r+1$, α_2: $p\to r+1+k$, β_1: $k\to q$ and β_2: $s\to l+q$ are appropriate mappings. Now suppose that there are distinct integers

$$1\leqq i_1<i_2\leqq l \quad\text{such that}\quad \alpha_1(i_1)=\alpha_1(i_2). \qquad (**)$$

By $X1$ we can assume that $i_1=1$ and $i_2=2$. Using $X4$ we can decrease l making the induction hypothesis applicable. In this way α_1 can be made injective. It is also easy to see that if

$$\beta_2 \text{ is not onto } [l], \qquad (***)$$

then the feedback counter l can be decreased again.

Case b: $l=0$ or none of $(*)$, $(**)$ and $(***)$ is satisfied.

In this case if α_2 were not onto $[r+1+k]-[r+1]$, then k could be decreased trivially, moreover any duplication of β_1 could be "lifted" to α_2 causing again the number k to be decreased.

Thus, we have seen that in any case when the induction hypothesis cannot be applied we have all the conditions of the n.f. satisfied, except monotonicity of α_1 and β_1. However, this can also be adjusted by the application of $X1$ and $P6$, so the proof is complete.

Theorem 1. Let t and t' be Σ-terms. If $|t|=|t'|$, then $t=t'$ is provable from *PMS*.

Proof. By Lemma 6 we can assume that t and t' are in n.f. Normal form of Σ-terms was defined in such a way that if t and t' were not identical, then the only difference between them should appear in the order of the atomic terms occuring in the sum $\sum_{i=1}^{n}\sigma_i$. In this case, however, an application of Lemma 2 with an appropriate permutation α will make them identical.

This theorem and the following corollary are the main results of the paper.

Corollary 2. $\mathrm{Sch}(\Sigma)$ is the free scheme algebra generated by Σ.

3. Connections to the same result of [B—Es]

In [B—Es] schemes are axiomatized as algebras equipped with the following operations and constants.

Composition, $\cdot$: $A(n,p)\times A(p,q)\to A(n,q)$;

Pairing, $\langle , \rangle$: $A(n,q)\times A(p,q)\to A(n+p,q)$;

Iteration, †: $A(n,n+p)\to A(n,p)$;

$\pi_p^i\in A(1,p)$ for each $p\in N$, $i\in[p]$;

$0_p\in A(0,p)$ for each $p\in N$.

Let us call algebras of hist type BS-algebras, and to make a temporary distinction call the BS-type scheme algebras of [B—Es] B-scheme algebras.

In an arbitrary scheme algebra A we can introduce the BS-algebra operations as derived ones in the following way.

Composition: adopted as a basic operation;

Pairing: for $f\colon n\to q$ and $g\colon p\to q$ let

$$\langle f,g\rangle=(f+g)\cdot w_2(q),$$

where $w_k(q)\colon kq\to q$ is the mapping which takes $(j-1)q+i$ to i for each $j\in[k]$, $i\in[q]$;

Iteration: for $f\colon n\to n+p$ let

$$f^\dagger=\uparrow^n(w_2(n)f);$$

$$\pi_p^i=0_{i-1}+1+0_{p-i} \quad \text{and} \quad 0_p \text{ is adopted.}$$

It is straightforward to check that if A is a free scheme algebra, then the above derived interpretation of the BS-algebra operations coincides with their original interpretation considering A as a free B-scheme algebra. From well-known results of universal algebra it follows that every scheme algebra equipped with these BS-algebra operations becomes a B-scheme algebra.

Now let A be a B-scheme algebra. We can derive the S-algebra operations in A as follows.

$1=\pi_1^1$; $x=\langle\pi_2^2,\pi_2^1\rangle$; $\varepsilon=\langle\pi_1^1,\pi_1^1\rangle$; 0_1: adopted;

Composition: adopted;

Sum: for $f_1\colon p_1\to q_1$, $f_2\colon p_2\to q_2$ let

$$f_1+f_2=\left\langle f_1\langle\pi_{q_1+q_2}^1,\dots,\pi_{q_1+q_2}^{q_1}\rangle, f_2\langle\pi_{q_1+q_2}^{q_1+1},\dots,\pi_{q_1+q_2}^{q_1+q_2}\rangle\right\rangle;$$

Feedback: for $f\colon 1+p\to 1+q$ let

$$\uparrow f=(0_1+p)\big(f(1+0_p+q)\big)^\dagger.$$

Repeating the previous argument for free algebras we can see that A equipped with the above defined S-algebra operations becomes a scheme algebra. Thus, we can state

Theorem 2. The equational class of all scheme algebras is equivalent to that of all B-scheme algebras.

4. Algebraic and iteration theories

Roughly speaking an algebraic theory (theory for short) is a BS-algebra without iteration satisfying the following equational axioms.

$TH1$: $f\cdot(g\cdot h)=(f\cdot g)\cdot h$ for all $f\colon n\to p$, $g\colon p\to q$, $h\colon q\to r$,

$TH2$: $\underline{p}\cdot f=f=f\cdot\underline{q}$ for all $f\colon p\to q$ ($\underline{p}$ denotes the term $\langle\pi_p^1,\ldots,\pi_p^p\rangle$),

$TH3$: $\langle\langle f,g\rangle,h\rangle=\langle f,\langle g,h\rangle\rangle$ for all $f\colon m\to q$, $g\colon n\to q$, $h\colon p\to q$,

$TH4$: $\langle f,0_q\rangle=f=\langle 0_q,f\rangle$ for all $f\colon p\to q$,

$TH5$: $\pi_p^i\langle f_1,\ldots,f_p\rangle=f_i$ for all $f_1,\ldots,f_p\colon 1\to q$, $i\in[p]$,

$TH6$: $\langle\pi_p^1 f,\ldots,\pi_p^p f\rangle=f$ for all $f\colon p\to q$.

We would like to extend our system of axioms PMS in such a way that in the corresponding smaller equational class each algebra should derive a B-scheme algebra which is a theory. We claim that the following two axioms are sufficient.

$Th1$: $0_1\cdot f=0_q$ for all $f\colon 1\to q$,

$Th2$: $w_p(p)\cdot f=\left(\sum\limits_{i=1}^{p}f\right)\cdot w_p(q)$ for all $f\colon p\to q$

(recall that $w_p(q)\colon pq\to q$ takes $(j-1)q+i$ to i for each $j\in[p]$, $i\in[q]$). Indeed, the derived correspondents of $TH1$—$TH4$ follows already from $P\cup M$, so we only have to prove $TH5$ and $TH6$. The derived form of $TH5$ in S-algebras in the following:

$$(0_{i-1}+1+0_{p-i})(f_1+\ldots+f_p)w_p(q)=f_i.$$

By $Th1$ the left-hand side reduces to

$$(0_{(i-1)q}+f_i+0_{(p-i)q})w_p(q),$$

which is clearly equal to f_i.

Concerning $TH6$ we have to prove that

$$((1+0_{p-1})f+\ldots+(0_{p-1}+1)f)w_p(q)=f.$$

Manipulating the left-hand side using *Th*2 we obtain:

$$(\sum_{i=1}^{p}((0_{i-1}+1+0_{p-i})f))w_p(q) = (\sum_{i=1}^{p}(0_{i-1}+1+0_{p-i}))(\sum_{i=1}^{p} f)w_p(q) =$$

$$= (\sum_{i=1}^{p}(0_{i-1}+1+0_{p-i}))w_p(p)f = f.$$

Unfortunately I did not succeed in an essential simplification of Ésik's "commutativity" axioms (cf. [Es]) for iteration theories:

$$IT\colon \langle \pi_m^1 \varrho f(\varrho_1+p), \dots, \pi_n^n \varrho f(\varrho_n+p)\rangle^\dagger = \varrho\big(f(\varrho+p)\big)^\dagger,$$

where $f\colon n \to m+p$, $\varrho\colon m \to n$ is a surjective mapping and $\varrho_i\colon m \to m$ are also mappings satisfying $\varrho_i \varrho = \varrho$. In our sense *IT* is an infinite scheme of axioms, moreover, Ésik has proved that it cannot be replaced by any finite scheme, see [Es1].

BOLYAI INSTITUTE
A. JÓZSEF UNIVERSITY
ARADI VÉRTANÚK TERE 1
SZEGED, HUNGARY
H—6720

References

[B—Es] Bloom, S. L., Z. Ésik, Axiomatizing schemes and their behaviours, J. Comp. System Sci., 31/3 (1985), 375—393.

[ES] Elgot, C. C., J. Shepherdson, An equational axiomatization of reducible flowchart schemes, in Calvin C. Elgot, Selected papers, S. L. Bloom, ed., Springer-Verlag, 1982.

[Es] Ésik, Z. Identities in iterative and rational theories, Comput. Languages 14 (1980), 183—207.

[Es1] Ésik, Z., Independence of the equational axioms of iteration theories, to appear.

[AD] Arnold, A., M. Dauchet, Theorie des magmoïdes, RAIRO Inform. Theor. 12 (1978) 235—257 and 13 (1979) 135—154.

(Received Oct. 8, 1986)