Intern. J. Computer Math. 1981, Vol. 9, pp. 305–320
0020-7160/81/0904-0305 $06.50/0

Printed in Great Britain

Small Specifications for Large Finite Data Structures

J. A. BERGSTRA AND J.-J. Ch. MEYER

Department of Mathematics, University of Leiden, Wassenaarseweg 80, Leiden, The Netherlands

(*Received June 1980*)

Having concerned ourselves with boundedness properties of algebraic data structure specifications in the sense of the ADJ Group (see [4, 6, 7]) before now—see [1], which is in a sense a follow-up of [3] of Bergstra and Tucker—we show in this paper that data structures of cardinality $>n$ can be specified by means of a bounded number of equations, not depending on n, which are each of length $\mathcal{O}(n)$ only.

KEY WORDS: algebraic data structures; equational and conditional specifications; boundedness properties.

INTRODUCTION

In [3] has been shown that a particular data structure A_n with $|A_n| = ack(n,n)+1$ which is $\gg n$ if n is large, can be specified (in the sense of the *ADJ* Group see [4,6,7]) using only a bounded number N of equations, not depending on n, which are each of length $\mathcal{O}(n)$. Now the question arises whether or not such a specification can also be given for a data stricture $\mathscr{V}=\langle D_{\mathscr{V}},\Sigma\rangle$ with $|D_{\mathscr{V}}|\geqq f(n)$ where f is an arbitrary recursive function $\omega\to\omega$.

We shall prove that this can be done: first, in section two, we shall show that it can be done easily when using conditional equations, resulting in the following

THEOREM *If f is a recursive function $\omega\to\omega$ then there exists for each n a finite algebraic data structure $\mathscr{V}_n$ such that $\mathscr{V}_n$ can be specified by means of a conditional specification $\langle\Sigma,E_n\rangle$ with $|E_n|<N$, $\|e\|\leqq c\cdot n$ for each $e\in E_n$, and $|\mathscr{V}_n|>f(n)$, where N and c are certain fixed natural numbers not depending on n;*

next, in section three, we shall show that it can also be done by means of (ordinary) equations, resulting in the

THEOREM *If f is a recursive function $\omega \to \omega$ then there exists for each n a finite algebraic data structure $\mathscr{W}_n$ such that $\mathscr{W}_n$ can be specified by means of an ordinary equational specification $\langle \Sigma', E'_n \rangle$ with $|E'_n| < N$, $\|e\| \leqq c \cdot n$ for each $e \in E'_n$, and $|\mathscr{W}_n| > f(n)$, where N and c are certain fixed natural numbers not depending on n.*

But before all this we shall recapitulate the main definitions and notions for specification of data structures in general.

1. SEMANTICS AND SPECIFICATIONS OF DATA STRUCTURES

An *algebra* $\mathscr{V}$ of signature Σ is a structure $\langle D_{\mathscr{V}}, \Sigma \rangle$, in which $D_{\mathscr{V}}$ is a set of elements called the *domain* of $\mathscr{V}$ and Σ is a set of names of functions defined on $D_{\mathscr{V}}$ and names of special elements of $D_{\mathscr{V}}$ (the *individual constants* of $\mathscr{V}$). It is said that Σ names the *constants* of $\mathscr{V}$.

An algebra $\mathscr{V}$ is called *finite*, if it has a finite domain.

The following facts are easy to establish:

Let $\mathscr{V}$ and $\mathscr{W}$ be algebras of signature Σ both finitely generated by their constants.

Then:

1) any Σ-homomorphism $\varphi\colon \mathscr{V} \to \mathscr{W}$ is surjective.
2) if $\varphi, \psi\colon \mathscr{V} \to \mathscr{W}$ are Σ-homomorphisms then $\varphi = \psi$.
3) if there are Σ-homomorphisms $\varphi\colon \mathscr{V} \to \mathscr{W}$ and $\psi\colon \mathscr{W} \to \mathscr{V}$ then $\mathscr{V} \cong \mathscr{W}$ (by either φ or ψ).

Let Σ be a signature. Then $T(\Sigma)$ denotes the Σ-algebra of all terms over Σ and $T_\Sigma[X_1, \ldots, X_n]$ denotes the algebra of polynomials in the indeterminates $X_1, \ldots, X_n$.

If $\mathscr{V}$ is a Σ-algebra then we mean by *term evaluation in* $\mathscr{V}$ a map $\mathrm{val}_{\mathscr{V}}$: $T(\Sigma) \to \mathscr{V}$ which evaluates each term $t \in T(\Sigma)$ by substituting the constants of $\mathscr{V}$ for their names in t.

$\mathrm{val}_{\mathscr{V}}$ can be uniquely defined as an epimorphism $T(\Sigma) \to \mathscr{V}$.

Clearly, the following holds: if $\varphi\colon \mathscr{V} \to \mathscr{W}$ is a homomorphism between Σ-algebras, then the following diagram commutes:

$$
\begin{tikzcd}
 & T(\Sigma) \arrow[dl, "\mathrm{val}_{\mathscr{V}}"'] \arrow[dr, "\mathrm{val}_{\mathscr{W}}"] & \\
\mathscr{V} \arrow[rr, "\varphi"] & & \mathscr{W}
\end{tikzcd}
$$

We define *polynomial evaluation* in $\mathscr{V}$ as the substitution of some *a*

$=(a_1,\ldots,a_n)\in D^n_{\mathscr{V}}$ for indeterminates $X=(X_1,\ldots,X_n)$ and of the constants of $\mathscr{V}$ for their names into polynomial $t(X)\in T_\Sigma[X_1,\ldots,X_n]$, followed by the evaluation of $t(a)$ in $\mathscr{V}$.

An *(ordinary) equation* is a pair $(t(X),t'(X))$ of polynomials from some $T_\Sigma[X_1,\ldots,X_n]$, written as $t(X)=t'(X)$, whereat it must be noted that $t(X)$ and $t'(X)$ need not have any indeterminate in common.

A *conditional equation* is a formula of the form

$$t_1(X)=t_1'(X)\wedge\ldots\wedge t_k(X)=t_k'(X)\rightarrow t(X)=t'(X).$$

The *length* of an equation e, notated as $\|e\|$, is the length of e thought of as a string over signature Σ and the alphabet

$$(\quad),=\wedge\rightarrow 0\,1$$

where $\{0,1\}$ is used to represent indeterminates by means of the binary representations of their natural number indices.

If E is a set of formulae over Σ and A is a Σ-algebra such that $A\models E$, we say that A is an *E-algebra.*

We define $ALG(\Sigma,E)$ as the class of all E-algebras and $T(\Sigma,E)$ as the *initial algebra* for $ALG(\Sigma,E)$, constructed from $T(\Sigma)$; $T(\Sigma,E)=T(\Sigma)/\equiv_E$ where $\equiv_E$ denotes the smallest congruence on $T(\Sigma)$ that identifies terms of $T(\Sigma)$ by means of the equations of E.

Finally we define: an algebra $\mathscr{V}=\langle D_{\mathscr{V}},\Sigma_{\mathscr{V}}\rangle$ has a *finite (ordinary or conditional) equational specification* (Σ,E) if $\Sigma_{\mathscr{V}}=\Sigma$, E is a finite set of (ordinary or conditional respectively) equations over Σ, and $T(\Sigma,E)\cong\mathscr{V}$.

We shall leave it at that as far as basic concepts are concerned; more details can be obtained from [2, 4, 6, 7].

2. SMALL SPECIFICATIONS OF LARGE FINITE DATA STRUCTURES BY MEANS OF CONDITIONAL EQUATIONS

If S is a set we shall use the notation $|S|$ for the cardinality of S (i.e. the number of elements in S); if $\mathscr{V}$ is an algebra we shall mean by $|\mathscr{V}|$ the cardinality of the domain of $\mathscr{V}$. Now we can state our

THEOREM 2.1 *Let f be a recursive function $\omega\rightarrow\omega$. Then there exists for each n a finite algebraic data structure $\mathscr{V}_n$ such that $\mathscr{V}_n$ can be specified by means of a conditional specification (Σ,E_n) with $|E_n|=5$, $\|e\|\leqq c\cdot n$ for each $e\in E_n$, and $|\mathscr{V}_n|>f(n)$, where c is a certain fixed natural number not depending on n.*

Proof To prove our theorem we shall make use of the Diophantine Theorem of Y. Matijacevič which we shall state explicitly first: let P_m stand for the set of polynomials in m indeterminates over $\mathbb{Z}$, constructed from the usual addition $+$, subtraction $-$ and multiplication $\cdot$ on $\mathbb{Z}$.

A set $\Omega \subset \omega^k$ is said to be *diophantine* if there exists a polynomial $r \in P_{k+l}$ such that

$$(x_1, \ldots, x_k) \in \Omega \quad \text{iff}$$

$$\exists y_1, \ldots, y_l \in \omega \text{ s.t. } \quad r(x_1, \ldots, x_k, y_1, \ldots, y_l) = 0.$$

Obviously, the condition for a set to be diophantine is equivalent to the condition that there exists polynomials p, $q \in P_{k+l}$ constructed from $+$ and $\cdot$ only, such that $(x_1, \ldots, x_k) \in \Omega$ iff

$$\exists y_1, \ldots, y_l \in \omega \text{ s.t. } p(x_1, \ldots, x_k, y_1, \ldots, y_l) = q(x_1, \ldots, x_k, y_1, \ldots, y_l).$$

In this form we shall use the concept of diophantine.

Now the *Diophantine Theorem* states that every recursively enumerable set is diophantine. (See [5] for a proof of this.)

As f is a recursive function, graph $(f) = \{(x, y) \mid y = f(x)\} \subset \omega^2$ is a recursively enumerable set, and thus by the Diophantine Theorem to be written as

$$\{(x, y) \in \omega^2 \mid \exists z_1, \ldots, z_l \in \omega \text{ s.t.}$$

$p(x, y, z_1, \ldots, z_l) = q(x, y, z_1, \ldots, z_l)\}$ for some polynomials $p, q \in P_{l+2}$ constructed using $+$ and $\cdot$ only.

For notational convenience sake we shall abbreviate $z_1, \ldots, z_l$ as $\mathbf{z}$ in future.

So now we have that

$$\forall x, y \in \omega : y = f(x) \quad \text{iff} \quad \exists \mathbf{z} \text{ s.t.}$$

$$p(x, y, \mathbf{z}) = q(x, y, \mathbf{z}). \tag{*}$$

or equivalently:

$$\forall x \in \omega : \exists \mathbf{z} \text{ s.t. } p(x, f(x), \mathbf{z}) = q(x, f(x), \mathbf{z}) \tag{**}$$

Let $t_n = \mu u \in \omega[\exists \mathbf{z}$ s.t.

$$u = p(n, f(n), \mathbf{z}) = q(n, f(n), \mathbf{z})],$$

in which $\mu u[\Phi u]$ stands for the least number u such that Φu holds.

Notice that $t_n < \infty$, for by (**) such a u exists.
We shall need the following

LEMMA 2.2 $t_n \geqq f(n)$.

Proof Take a u such that $u = p(n, f(n), \mathbf{z}_0) = q(n, f(n), \mathbf{z}_0)$ for some $\mathbf{z}_0$. Suppose that both polynomials $p(n, f(n), \mathbf{z}_0)$ and $q(n, f(n), \mathbf{z}_0)$ contain no terms with $f(n)$. Then it holds: $u = p(n, y, \mathbf{z}_0) = q(n, y, \mathbf{z}_0)$ for any $y \in \omega$, which implies that $\forall y \in \omega : y = f(n)$. But this contradicts the functionality of f.

So either $p(n, f(n), \mathbf{z}_0)$ or $q(n, f(n), \mathbf{z}_0)$ contains a term with $f(n)$, suppose $p(n, f(n), \mathbf{z}_0)$. But $p(n, f(n), \mathbf{z}_0)$ is a composition of only $+$ and $\cdot$, so $u = p(n, f(n), \mathbf{z}_0)$ must be $\geqq f(n)$.

This argumentation holds for every $u = p(n, f(n), \mathbf{z}_0) = q(n, f(n), \mathbf{z}_0)$ for some $\mathbf{z}_0$.

So also $t_n = \mu u[u = p(n, f(n), \mathbf{z}_0) = q(n, f(n), \mathbf{z}_0)] \geqq f(n)$. $\square$

Now we define Σ as the signature $\{S, \underline{+}, \underline{\cdot}, \underline{0}\}$ and E_n as the set equations over Σ:

$$\left.\begin{aligned} &X \underline{+} \underline{0} = X \\ &X \underline{+} S(Y) = S(X \underline{+} Y) \\ &X \underline{\cdot} \underline{0} = \underline{0} \\ &X \underline{\cdot} S(Y) = (X \underline{\cdot} Y) \underline{+} X \end{aligned}\right\} \text{forming together } E^*, \text{ and the equation:}$$

$$\underline{p}(S^n(\underline{0}), Y, \mathbf{Z}) = \underline{q}(S^n(\underline{0}), Y, \mathbf{Z}) \to \underline{p}(S^n(\underline{0}), Y, \mathbf{Z}) = S(\underline{p}(S^n(\underline{0}), Y, \mathbf{Z}))$$

in which $\underline{p}$ and $\underline{q}$ are built like p and q respectively but with $\underline{+}$ and $\underline{\cdot}$ instead of $+$ and $\cdot$ respectively.

Notice that $\forall n : |E_n| = 5$, and that $\forall n\ \forall e \in E_n : \|e\| \leqq c \cdot n$ for some fixed c.

Now we shall consider $T(\Sigma, E_n)$. First we prove the following

LEMMA 2.3 *Let* $p \in P_k$ *be constructed using* $+$ *and* $\cdot$ *only and let* $p(a_1, \ldots, a_k) = a$.

Then it holds that

$$T(\Sigma, E_n) \models \underline{p}(S^{a_1}(\underline{0}), \ldots, S^{a_k}(\underline{0})) = S^a(\underline{0}).$$

Proof Suppose $p(a_1,\ldots,a_k)=a$. Then also $\langle\omega, S, \underline{+}, \underline{\cdot}, \underline{0}\rangle \models \underline{p}(S^{a_1}(\underline{0}),\ldots, S^{a_k}(\underline{0}))=S^a(\underline{0})$ in which S names $s(x)=x+1$

$\underline{+}$ names addition on ω, and

$\underline{\cdot}$ names multiplication on ω.

But it is easy to see that

$$\langle\omega, S, \underline{+}, \underline{\cdot}, \underline{0}\rangle \cong T(\Sigma, E^*).$$

So also $T(\Sigma, E^*)\models \underline{p}(S^{a_1}(\underline{0}),\ldots, S^{a_k}(\underline{0}))=S^a(\underline{0})$, and as $T(\Sigma, E_n)$ is a homomorphic image of $T(\Sigma, E^*)$, it also holds that $T(\Sigma, E_n)\models \underline{p}(S^{a_1}(\underline{0}),\ldots, S^{a_k}(\underline{0}))=S^a(\underline{0})$. □

Let $\mathscr{T}_n$ now be the algebra $\langle\{0,1,\ldots,t_n\},\Sigma\rangle$ in which

Σ names $s_{t_n}(x)=\min(x+1,t_n)$ by S,

$f(x,y)=\min(x+y,t_n)$ by $\underline{+}$,

$g(x,y)=\min(x\cdot y,t_n)$ by $\underline{\cdot}$,

and $0\in\omega$ by $\underline{0}$.

($+$ and $\cdot$ are the usual addition and multiplication on ω again). Then we can state the

PROPOSITION 2.4

$$T(\Sigma, E_n)\cong\mathscr{T}_n.$$

Proof First we notice that $\mathscr{T}_n\models E_n$, because it is clear that $\mathscr{T}_n\models E^*$ and furthermore it holds that

$$p(s^n_{t_n}(0),y,\mathbf{z})=q(s^n_{t_n}(0),y,\mathbf{z})\to p(s^n_{t_n}(0),y,\mathbf{z})=s_{t_n}(p(s^n_{t_n}(0),y,\mathbf{z})),$$

for if $p(s^n_{t_n}(0),y,\mathbf{z})=q(s^n_{t_n}(0),y,\mathbf{z})$ for some y and $\mathbf{z}$, then $p(n',y,\mathbf{z})=q(n',y,\mathbf{z})$ with $n'=\min(t_n,n)$ and so by (*) $y=f(n')$. Now there are two possibilities:

i) $n'=t_n$ and then, as p and q are constructed by means of $+$ and $\cdot$ only, $p(n',y,\mathbf{z})=q(n',y,\mathbf{z})=t_n$, if either p or q has a term with n'. If neither p nor q has a term with n', then we can infer analogously to the proof of lemma 2.2 that f is a constant function. So in that case we have $y=f(n')=f(n)$, and thus $p(n,f(n),\mathbf{z})=p(n',y,\mathbf{z})=q(n',y,\mathbf{z})=q(n,f(n),\mathbf{z})$.

ii) $n'=n$, and then we also have $p(n,f(n),\mathbf{z})=q(n,f(n),\mathbf{z})$. So we always have that either $p(n',y,\mathbf{z})=q(n',y,\mathbf{z})=t_n$ which implies that $s_{t_n}(p(s^n_{t_n}(0),y,\mathbf{z}))=s_{t_n}(p(n',y,\mathbf{z}))=s_{t_n}(t_n)=t_n=p(n',y,\mathbf{z})=p(s^n_{t_n}(0),y,\mathbf{z})$, or $p(n,f(n),\mathbf{z})=q(n,f(n),\mathbf{z})\leq t_n$.

But this last formula implies $p(n,f(n),\mathbf{z})=q(n,f(n),\mathbf{z})=t_n$ too, because if $p=q$ were $<t_n$, then there would be a $u<t_n$ such that $u=p=q$, and this contradicts the minimality of t_n.

So in any case we have that $s_{t_n}(p(s^n_{t_n}(0), y, \mathbf{z})) = p(s^n_{t_n}(0), y, \mathbf{z})$. From the fact that $\mathscr{T}_n \models E_n$, we can infer that $\forall i,j \in \{0,\ldots,t_n\}$ $S^i(\underline{0}) \equiv_{E_n} S^j(\underline{0}) \Leftrightarrow i = j$, for $S^i(\underline{0}) \equiv_{E_n} S^j(\underline{0})$ implies that $E_n \vdash S^i(\underline{0}) = S^j(\underline{0})$ and thus $\mathscr{T}_n \models S^i(\underline{0}) = S^j(\underline{0})$, i.e. $\mathrm{val}_{\mathscr{T}_n}(S^i(\underline{0})) = \mathrm{val}_{\mathscr{T}_n}(S^j(\underline{0}))$, i.e. $i=j$, (and the converse is trivial). Next it is not difficult to prove that $\forall t \in T(\Sigma)$ holds that $t \equiv_{E_n} S^u(\underline{0})$ for some $0 \leqq u \leqq t_n$.

The proof is given by induction on the complexity of terms in $T(\Sigma)$: the basis is obvious and the induction step follows from the

LEMMA 2.5 *If* $d_i \equiv_{E_n} S^{u_i}(\underline{0})$ *for some* $0 \leqq u_i \leqq t_n$ *and* $\underline{\lambda} \in \Sigma$, *then* $\underline{\lambda}(\mathbf{d}) \equiv_{E_n} S^{\lambda(\mathbf{u})}(\underline{0})$ *where* λ *is the m-ary function named by* $\underline{\lambda}$ *in* Σ *and* $\mathbf{d} = (d_1, \ldots, d_m)$ *and* $\mathbf{u} = (u_1, \ldots, u_m)$.

Proof

i) $\underline{\lambda} = S; \lambda = s_{t_n}$.

First, as $t_n = p(n, f(n), \mathbf{z}_0) = q(n, f(n), \mathbf{z}_0)$ for some $\mathbf{z}_0$, we know by lemma 2.3 that

$$T(\Sigma, E_n) \models S^{t_n}(\underline{0}) = \underline{p}(S^n(\underline{0}), S^{f(n)}(\underline{0}), S^{\mathbf{z}_0}(\underline{0})) = \underline{q}(S^n(\underline{0}), S^{f(n)}(\underline{0}), S^{\mathbf{z}_0}(\underline{0})),$$

in which

$$S^{\mathbf{z}_0}(\underline{0}) = (S^{(\mathbf{z}_0)_1}(\underline{0}), \ldots, S^{(\mathbf{z}_0)_k}(\underline{0})).$$

Thus

$$E_n \vdash S^{t_n}(\underline{0}) = \underline{p}(S^n(\underline{0}) \cdot S^{f(n)}(\underline{0}),\ S^{\mathbf{z}_0}(\underline{0})) = \underline{q}(S^n(\underline{0}), S^{f(n)}(\underline{0}), S^{\mathbf{z}_0}(\underline{0})$$

and so also

$$E_n \vdash S^{t_n}(\underline{0}) = \underline{p}(S^n(\underline{0}), S^{f(n)}(\underline{0}), S^{\mathbf{z}_0}(\underline{0})) = S(p(S^n(\underline{0}), S^{f(n)}(\underline{0}), S^{\mathbf{z}_0}(\underline{0})$$

$$= SS^{t_n}(\underline{0}) = S^{t_n+1}(\underline{0}). \qquad (***).$$

Therefore

$$E_n \vdash S(S^u(\underline{0})) = S^{u+1}(\underline{0}) = \begin{cases} S^{t_n+1}(\underline{0}) \overset{(***)}{=} S^{t_n}(\underline{0}) = S^{S_{t_n}(u)}(\underline{0}) & \text{if} \quad u = t_n \\ S^{S_{t_n}(u)}(\underline{0}) \quad \text{if} \quad u < t_n \end{cases}$$

ii) $\underline{\lambda} = \underline{+}; \lambda = f$.

$$E_n \vdash S^{u_1}(\underline{0}) \underline{+} S^{u_2}(\underline{0}) = S^{u_1}(\underline{0}) \underline{+} S(S^{u_2-1}(\underline{0}))$$

$$= S(S^{u_1}(\underline{0}) \underline{+} S^{u_2-1}(\underline{0})) = S^2(S^{u_1}(\underline{0}) \underline{+} S^{u_2-2}(\underline{0}))$$

$$= \dots = S^{u_2}(S^{u_1}(\underline{0}) \underline{+} S^0(\underline{0})) = S^{u_2}(S^{u_1}(\underline{0}) \underline{+} \underline{0}) = S^{u_2}(S^{u_1}(\underline{0}))$$

$$= S^{u_1+u_2}(\underline{0}) = \begin{cases} S^{t_n}(\underline{0}) \text{ (by } ^{(***)}) = S^{f(u_1,u_2)}(\underline{0}) & \text{if } \; u_1+u_2 > t_n \\ S^{f(u_1,u_2)}(\underline{0}) \; \text{ if } \; u_1+u_2 \leqq t_n \end{cases}$$

iii) $\underline{\lambda} = \underline{\cdot}; \lambda = g$.

$$E_n \vdash S^{u_1}(\underline{0}) \underline{\cdot} S^{u_2}(\underline{0}) = S^{u_1}(\underline{0}) \underline{\cdot} S(S^{u_2-1}(\underline{0})) = (S^{u_1}(\underline{0}) \underline{\cdot} S^{u_2-1}(\underline{0})) \underline{+} S^{u_1}(\underline{0}) = \dots$$

$$= (S^{u_1}(\underline{0}) \underline{\cdot} S^0(\underline{0})) \underline{+} \underbrace{S^{u_1}(\underline{0}) \underline{+} \dots \underline{+} S^{u_1}(\underline{0})}_{u_2 \text{ times}}$$

$$= \underline{0} \underline{+} S^{2u_1}(\underline{0}) \underline{+} \underbrace{S^{u_1}(\underline{0}) \underline{+} \dots \underline{+} S^{u_1}(\underline{0})}_{u_2 - 1 \text{ times}}$$

$$= S^{u_1 u_2}(\underline{0}) = \begin{cases} S^{t_n}(\underline{0})(by\ (***)) = S^{g(u_1,u_2)}(\underline{0}) & \text{if } \; u_1 u_2 > t_n \\ S^{g(u_1,u_2)}(\underline{0}) \; \text{ if } \; u_1 u_2 \leqq t_n. \end{cases} \qquad \square$$

From the preceding we can easily conclude that the function φ defined by $\varphi(i) = \mathscr{C}_{E_m}(S^i(\underline{0}))$, the $\equiv_E$ -equivalence class of $S^i(\underline{0})$ is a bijective homomorphism $\mathscr{T}_n \to T(\Sigma, E_n)$. Therefore $T(\Sigma, E_n) \cong \mathscr{T}_n$.
(A more extensive treatment of an argumentation of this kind can be found in [1, 2, 3].)

With this our theorem has been proved. Q.E.D.

3. SMALL SPECIFICATIONS OF LARGE FINITE DATA STRUCTURES BY MEANS OF ORDINARY EQUATIONS.

THEOREM 3.1 *Let f be a recursive function $\omega \to \omega$. Then there exists for each n a finite algebraic structure $\mathscr{W}_n$ such that $\mathscr{W}_n$ can be specified by means of an ordinary equational specification (Σ', E'_n) with $|E'_n| = 18$, $\|e\| \leqq c \cdot n$ for each $e \in E'_n$, and $|\mathscr{W}_n| > f(n)$, where c is a certain fixed natural number not depending on n.*

Proof By the Diophantine Theorem again we have that

$$\forall x, y \in \omega : y = f(x) \quad \text{iff} \quad \exists \mathbf{z} \text{ s.t.}$$

$$p(x, y, \mathbf{z}) = q(x, y, \mathbf{z}) \, (*)$$

and

$$\forall x \in \omega : \exists \mathbf{z} \text{ s.t.}$$

$$p(x, f(x), \mathbf{z}) = q(x, f(x), \mathbf{z}) \ (**)$$

for some $p, q \in P_{l+2}$ constructed by means of $+$ and $\cdot$ only.

Again, let $t_n = \mu u \in \omega[\exists \mathbf{z} \text{ s.t. } u = p(n, f(n), \mathbf{z}) = q(n, f(n), \mathbf{z})]$. Then again it holds that

$$f(n) \leqq t_n < \infty \cdot \text{(by lemma 2.2).}$$

Now we define Σ' as the signature $\{S, \underline{+}, \underline{\cdot}, H, \mathrm{MAX}, \underline{0}\}$ and E'_n as $E_* \cup \{e_n\}$ where E_* is the set of equations:

$$\left.\begin{array}{l} X \underline{+} \underline{0} = X \\ X \underline{+} S(Y) = S(X \underline{+} Y) \\ X \underline{\cdot} \underline{0} = \underline{0} \\ X \underline{\cdot} S(Y) = (X \underline{\cdot} Y) \underline{+} X \end{array}\right\} \text{which was the } E^* \text{ of section 2.}$$

$$\mathrm{MAX}(X, \underline{0}) = X$$

$$\mathrm{MAX}(S(X), S(Y)) = S(\mathrm{MAX}(X, Y))$$

$$\mathrm{MAX}(X, Y) = \mathrm{MAX}(Y, X)$$

$$H(\underline{0}, \underline{0}, X) = X$$

$$H(S(X), S(X), Y) = H(X, X, Y)$$

$$H(X, Y, Z) = H(Y, X, Z)$$

$$H(X, Y, H(U, V, W)) = H(U, V, H(X, Y, W))$$

$$H(X, Y, H(X, Y, Z) = H(X, Y, Z)$$

$$H(H(X, Y, Z), U, V) = H(Z, U, H(X, Y, V))$$

$$S(H(X, Y, Z)) = H(X, Y, S(Z))$$

$$H(X, Y, Z) \underline{+} U = H(X, Y, Z \underline{+} U)$$

$H(X, Y, Z) \underline{\cdot} U = H(X, Y, Z \underline{\cdot} U)$

$\mathrm{MAX}(H(X, Y, Z), U) = H(X, Y, \mathrm{MAX}(Z, U))$

and e_n is the equation

$$H(\underline{p}(S^n(\underline{0}), Y, \mathbf{Z}), \underline{q}(S^n(\underline{0}), Y, \mathbf{Z}), \underline{p}(S^n(\underline{0}), Y, \mathbf{Z}))$$

$$= H(p(S^n(\underline{0}), Y, \mathbf{Z}), \underline{q}(S^n(\underline{0}), Y, \mathbf{Z}), S(\underline{p}(S^n(\underline{0}), Y, \mathbf{Z})))$$

in which $\underline{p}$ and $\underline{q}$ are built like p and q respectively but with $\underline{+}$ and $\underline{\cdot}$ instead of $+$ and $\cdot$ respectively.

Notice that $\forall n: |E_n| = 18$, and $\forall n \forall e \in E_n: \|e\| \leq c \cdot n$ for some fixed n.

Before looking closer at $T(\Sigma', E_n')$ we shall first prove the

LEMMA 3.2 *If $p \in P_k$ is constructed by means of $+$ and $\cdot$ only and* $p(a_1, \ldots, a_k) = a$, then $T(\Sigma', E_n') \models \underline{p}(S^{a_1}(\underline{0}), \ldots, S^{a_k}(\underline{0})) = S^a(\underline{0})$.

Proof If $p(a_1, \ldots, a_k) = a$ we can prove analogously to the proof of Lemma 2.3 that $T(\Sigma', E^*) \models \underline{p}(S^{a_1}(\underline{0}), \ldots, S^{a_k}(\underline{0})) = S^a(\underline{0})$ and as $T(\Sigma', E_n')$ is a homomorphic image of $T(\Sigma', E^*)$ we also have $T(\Sigma', E_n') \models \underline{p}(S^{a_1}(\underline{0}), \ldots, S^{a_k}(\underline{0}) = S^a(\underline{0})$. $\square$

Let τ_n be the set $\{0.1, \ldots, t_n\}$ and σ_n be the set of two element subsets of τ_n. Now consider the following algebraic structures of signature Σ':
$\mathscr{A}_n = \langle V, S, \underline{+}, \underline{\cdot}, H, \mathrm{MAX}, \underline{0} \rangle$ in which

$V = \Pi(\sigma_n) \times \tau_n$, where

$\Pi(\sigma)$ stands for the power set of σ,

S names the operation

$s(A, i) = (A, \min(t_n, i+1))$

$\underline{+}$ names the operation $\oplus$ on V

defined by $(A, i) \oplus (B, j) = (A \cup B, \min(t_n, i+j))$

$\underline{\cdot}$ names the operation $\odot$ on V

defined by $(A, i) \odot (B, j) = (A \cup B, \min(t_n, i \cdot j))$

H names the operation

$h((A, i), (B, j), C, k))$

$= (A \cup B \cup C \cup \{i, j\}, k)$ if $i \neq j$

$(A \cup B \cup C, k)$ otherwise

MAX names the operation

$$m((A,i),(B,j))=(A\cup B,\ \max(i,j))$$

and $\underline{0}$ names $(\emptyset,0)\in V$.

(min, max, $+,\cdot$ have their usual meaning as operations on ω).

and $\mathscr{B}_n$ is the homomorphic image of $\mathscr{A}_n$ in which all elements $(A,i)\in V$ with $A\neq\emptyset$ have been identified.

We can now prove the following

PROPOSITION 3.3

i) *There exists an epimorphism* $\varphi:\mathscr{A}_n\to T(\Sigma',E_n')$.

ii) *There exists an epimorphism* $\psi:\ T(\Sigma',E_n')\to\mathscr{B}_n$.

Proof (i) Just as in section 2 we can say that

$$E_n'\vdash S^{t_n}(\underline{0})=\underline{p}(S^n(\underline{0}),S^{f(n)}(\underline{0}),S^{z_0}(\underline{0}))=\underline{q}(S^n(\underline{0})\cdot S^{f(n)}(\underline{0}),S^{z_0}(\underline{0}))$$

for certain $\mathbf{z}_0$. and so

$$\begin{aligned}E_n'\vdash S^{t_n}(\underline{0})&=H(\underline{0},\underline{0},S^{t_n}(\underline{0}))\\&=H(S(\underline{0}),S(\underline{0}),S^{t_n}(\underline{0}))\\&=\ldots=H(S^{t_n}(\underline{0}),S^{t_n}(\underline{0}),S^{t_n}(\underline{0}))\\&=H(\underline{p}(S^n(\underline{0}),S^{f(n)}(\underline{0}),S^{z_0}(\underline{0})),\\&\quad\underline{q}(S^n(\underline{0}),S^{f(n)}(\underline{0}),S^{z_0}(\underline{0})),\underline{p}(S^n(\underline{0}),S^{f(n)}(\underline{0}),S^{z_0}(\underline{0})))\\&=H(\underline{p}(S^n(\underline{0}),S^{f(n)}(\underline{0}),S^{z_0}(\underline{0})),\\&\quad\underline{q}(S^n(\underline{0}),S^{f(n)}(\underline{0}),S^{z_0}(\underline{0})),S\underline{p}(S^n(\underline{0}),S^{f(n)}(\underline{0}),S^{z_0}(\underline{0})),\\&=H(S^{t_n}(\underline{0}),S^{t_n}(\underline{0}),S^{t_n+1}(\underline{0}))\\&=\ldots=H(S(\underline{0}),S(\underline{0}),S^{t_n+1}(\underline{0}))\\&=H(\underline{0},\underline{0},S^{t_n+1}(\underline{0}))=S^{t_n+1}(\underline{0}).\end{aligned}$$

As thus $E_n'\vdash S^{t_n}(\underline{0})=S^{t_n+1}(\underline{0})$, it holds that $T(\Sigma',E_n')\models E_*\cup\{S^{t_n}(\underline{0})=S^{t_n+1}(\underline{0})\}$, so that $T(\Sigma',E_n')$ is the homomorphic image of $T(\Sigma',E_*\cup\{S^{t_n}(\underline{0})=S^{t_n+1}(\underline{0})\})$, which is $\cong\mathscr{A}_n$ as we shall see now:

LEMMA 3.4 $T(\Sigma', E_* \cup \{S^{t_n}(\underline{0}) = S^{t_n+1}(\underline{0})\} \cong \mathscr{A}_n$.

Proof For convenience we shall name the equation $S^{t_n}(\underline{0}) = S^{t_n+1}(\underline{0})$ by ε_n. Notice first that $\mathscr{A}_n \models E_* \cup \{\varepsilon_n\}$.

Now define χ: $\mathscr{A}_n \to T(\Sigma', E_n')$ by

$$\chi(A, i) = \begin{cases} \mathscr{C}_{E_* \cup \{\varepsilon_n\}}(S^i(\underline{0})) \quad \text{if} \quad A = \emptyset. \\ \mathscr{C}_{E_* \cup \{\varepsilon_n\}}(H(S^{a_1}(\underline{0}), S^{b_1}(\underline{0}), H(S^{a_2}(\underline{0}), S^{b_2}(\underline{0}), \\ H(\ldots S^{a_m}(\underline{0}), S^{b_m}(\underline{0}), S^i(\underline{0}))\ldots), \quad \text{if} \quad A = \{\{a_1, b_1\}, \ldots, \{a_m, b_m\}\}. \end{cases}$$

For convenience we shall omit the index $E_* \cup \{\varepsilon_n\}$ of $\mathscr{C}$ and write

$$H(S^{a_1}(\underline{0}), S^{b_1}(\underline{0}), H(S^{a_2}(\underline{0}), \ldots, S^{b_m}(\underline{0}), S^i(\underline{0}))\ldots)$$

as

$$H({}^{a_1}, {}^{b_1}, H({}^{a_2}, {}^{b_2}, H(\ldots {}^{a_m}, {}^{b_m}, {}^{i})\ldots).$$

Then

a) χ is a function, because $(A, i) = (A, j) \Rightarrow (A = B) \wedge (i = j) \Rightarrow \chi(A, i) = \chi(B, j)$.

b) χ is injective, because $\chi(A, i) = \chi(B, j) \Rightarrow (A = B = \emptyset \vee (A \neq \emptyset \wedge B \neq \emptyset))$ because of the fact that something of the form $S^i(\underline{0})$ can never be $\equiv E_* \cup \{\varepsilon_n\}$ something of the form

$$H({}^{a_1}, {}^{b_1} H(\ldots {}^{a_m}, {}^{b_m}, {}^{i})\ldots) \quad \text{where} \quad a_k \neq b_k,$$

and

$$A = B = \emptyset \Rightarrow \mathscr{C}(S^i(\underline{0})) = \mathscr{C}(S^j(\underline{0})) \Rightarrow S^i(\underline{0}) \equiv S^j(\underline{0}) \Rightarrow E_* \cup \{\varepsilon_n\} \vdash S^i(\underline{0})$$

$$= S^j(\underline{0}) = \mathscr{A}_n \models S^i(\underline{0}) = S^j(\underline{0}) \Rightarrow \mathrm{val}_{\mathscr{A}_n}(S^i(\underline{0})) = \mathrm{val}_{\mathscr{A}_n}(S^j(\underline{0})) \Rightarrow (\emptyset, i)$$

$$= (\emptyset, j) \Rightarrow (A, i) = (B, j)$$

and

$$(A \neq \emptyset \wedge B \neq \emptyset) \Rightarrow A = \{\{a_1, b_1\}, \ldots, \{a_m, b_m\}\}$$

for some $a_k \neq b_k$ and $B = \{\{a'_1, b'_1\}, \ldots, \{a'_r, b'_r\}\}$ for some $a'_k \neq b'_k$

$$\Rightarrow \mathscr{C}(H(^{a_1}, {}^{b_1}, H(^{a_2}, {}^{b_2}, H(\ldots {}^{a_m}, {}^{b_m}, {}^{i}) \ldots), = \mathscr{C}(H(^{a'_1}, {}^{b'_1}, \ldots {}^{b'_r}, {}^{j}) \ldots))$$

$$E_* \cup \{\varepsilon_n\} \vdash H(^{a_1}, {}^{b_1} \ldots {}^{i}) \ldots) = H(^{a'_1}, {}^{b'_1} \ldots {}^{j}) \ldots)$$

$$\Rightarrow \mathscr{A}_n \models H(^{a_1} \ldots {}^{i}) = H(^{a_1} \ldots {}^{j}) \Rightarrow \mathrm{val}_{\mathscr{A}_n}(H(^{a_1} \ldots {}^{i})) = \mathrm{val}_{\mathscr{A}_n}(H(^{a_1} \ldots {}^{j}))$$

$$= h((\emptyset, a_1), (\emptyset, b_1), h((\emptyset, a_2) \ldots (\emptyset, b_n), (\emptyset, i) \ldots)$$

$$= h((\emptyset, a'_1), (\emptyset, b'_1), \ldots, (\emptyset, j) \ldots) \Rightarrow$$

$$\left(\bigcup_{k=1}^{m} \{\{a_k, b_k\}\}, i\right) = \left(\bigcup_{k=1}^{r} \{\{a'_k, b'_k\}\}, j\right), \quad \text{i.e.} \quad (A, i) = (B, j).$$

Thus anyhow $\chi(A, i) = \chi(B, j) \Rightarrow (A, i) = (B, j)$

c) χ is surjective, because for every $t \in T(\Sigma)$ it holds that $t \equiv_{E_* \cup \{\varepsilon_n\}} S^i(\underline{0})$ for some i or $t \equiv_{E_* \cup \{\varepsilon_n\}} H(^{a_1}, {}^{b_1}, H(\ldots {}^{a_m}, {}^{b_m}, {}^{i}) \ldots)$ for some $a_k \neq b_k$. This is proved by induction on term complexity: the basis is clear ($\underline{0} = S^0(\underline{0})$), and the induction step follows from the following

LEMMA 3.5 *If* $d_k \equiv S^{u_k}(\underline{0})$ *or* $d_k \equiv H(^{a_{k1}}, {}^{b_{k1}}, H(^{a_{k2}}, {}^{b_{k2}}, H(\ldots {}^{b_{km}}, {}^{u_k}) \ldots)$ *for some* $u_k \in \tau_n$ *and* $a_{kr} \neq b_{kr} (\forall r)$, $\{a_{kr}, b_{kr}\} \neq \{a_{kr'}, b_{kr'}\} (\forall r, r')$ *and* $\underline{\lambda} \in \Sigma'$ *names M-ary operation* λ, *then* $\underline{\lambda}(\mathbf{d})$ *is* $\equiv$ *with a formula of one of the two forms too.* $(\mathbf{d} = d_1, \ldots, d_M)$.

Proof We shall only consider the following possibilities for $\underline{\lambda}$ (and leave the rest to the reader):

α) $\underline{\lambda} = S; \lambda = s$. As we know that $E'_n \vdash \varepsilon_n$

$$E'_n \vdash S\, S^u(\underline{0}) = S^{u+1}(\underline{0}) = \begin{cases} S^{t_n}(\underline{0}) & \text{if} \quad u = t_n n \\ S^v(\underline{0}) & \text{with} \quad v \leqq t_n \quad \text{otherwise} \end{cases}$$

and

$$E'_n \vdash S(H(^{a_1}, {}^{b_1}, H(\ldots {}^{a_m}, {}^{b_m}, {}^{u}) \ldots) = H(^{a_1}, {}^{b_1}, SH(\ldots {}^{u}) \ldots) = \ldots$$
$$= H(^{a_1}, {}^{b_1}, H(\ldots {}^{u+1}) \ldots) = H(^{a_1}, {}^{b_1}, H(\ldots {}^{v}) \ldots) \quad \text{with} \quad v \leqq t_n.$$

β) $\underline{\lambda} = H; \lambda = h$. For convenience we take as an example $d_1 \equiv S^u(\underline{0})$,

$$d_2 \equiv H(S^a(\underline{0}), S^b(\underline{0}), S^a(\underline{0}))$$

and

$$d_3 \equiv H(S^u(\underline{0}), S^b(\underline{0}), S^c(\underline{0})).$$

Then

$$E'_n \vdash H(S^u(\underline{0}), H(S^a(\underline{0}), S^b(\underline{0}), S^a(\underline{0})), H(S^u(\underline{0}), S^b(\underline{0}), H^c(\underline{0})))$$

$$= H(H(^a,^b,^a),^u, H(^u,^b,^c)) = H(^a,^u, H(^a,^b, H(^u,^b,^c))).$$

In general we can always get a form with $a_r \neq b_r (\forall r)$, $\{a_r, b_r\} \neq \{a_{r'}, b_{r'}\} (\forall r, r')$ and $u \in \tau_n$.

d) χ is a homomorphism: $\underline{\lambda}\chi(A, i) = \chi(\lambda(A, i))$. This can be seen by looking more precisely at the formula$\equiv \underline{\lambda}(\mathbf{d})$ in lemma 3.5: for example: for $\underline{\lambda} = S$ and $A = \{\{a_1, \ldots, b_m\}\}$ then $S\chi(A, i) = SH(^{a_1}, \ldots, ^{b_m}, ^i) \ldots)$

$$= \begin{cases} H(^{a_1}, \ldots, ^{b_m}, ^{t_n}) & \text{if} \quad i = t_n \\ H(^{a_1}, \ldots, ^{b_m}, ^{i+1}) & \text{if} \quad i < t_n \end{cases} = \chi s(A, i).$$

By a), b), c) and d) we know that $T(\Sigma', E_* \cup \{\varepsilon_n\}) \cong \mathscr{A}_n$, so lemma 3.4 has been proved. □

Therefore it is also clear that $T(\Sigma', E'_n)$ is the homomorphic image of $\mathscr{A}_n$: the proof of proposition 3.3 i) is complete. □

In order to prove ii) we consider the following. It is a routine matter to check that $\mathscr{B}_n \models E_*$, but also it holds that $\mathscr{B}_n \models e_n$, i.e.

$$\mathrm{val}_{\mathscr{B}_n}(H(\underline{p}(\quad), \underline{q}(\quad), \underline{p}(\quad)))$$

$$= \mathrm{val}_{\mathscr{B}_n}(H(p(\quad), q(\quad), Sp(\quad))), \text{i.e.}$$

$$h(p_{\mathscr{B}}(\quad), q_{\mathscr{B}}(\quad), p_{\mathscr{B}}(\quad)) = h(p_{\mathscr{B}}(\quad), q_{\mathscr{B}}(\quad), sp_{\mathscr{B}}(\quad))),$$

where $p_{\mathscr{B}}$ and $q_{\mathscr{B}}$ are the operations on $\mathscr{B}_n$ corresponding to $\underline{p}$ and $\underline{q}$ respectively, constructed from $\oplus$ and $\odot$ instead of $\dot{+}$ and $\dot{\cdot}$.

This is so because

1) If $p_{\mathscr{B}}(\quad)$ and $q_{\mathscr{B}}(\quad)$ are both $(\emptyset, i)$ for some $i \in \tau_n$, then i must be $= p(\quad) = q(\quad)$ and so $i = t_n$. (Otherwise the minimality of t_n is contradicted.)

   So

$$h(p_{\mathscr{B}}(\quad), q_{\mathscr{B}}(\quad), p_{\mathscr{B}}(\quad))$$

$$= h((\emptyset, t_n), (\emptyset, t_n), (\emptyset, t_n)) = (\emptyset, t_n) \quad \text{and} \quad h(p_{\mathscr{B}}(\quad), q_{\mathscr{B}}(\quad), sp_{\mathscr{B}}(\quad))$$

$$= h((\emptyset, t_n), (\emptyset, t_n), (\emptyset, \min(t_n, t_n + 1))) = (\emptyset, t_n) \quad \text{too.}$$

2) If $p_{\mathscr{B}}(\ )$ and $q_{\mathscr{B}}(\ )$ are not both $(\emptyset, i)$ for certain $i \in \tau_n$, then $h(p_{\mathscr{B}}(\ ), q_{\mathscr{B}}(\ ), p_{\mathscr{B}}(\ )) = (A, j)$ for certain $A \neq \emptyset$ and $j \in \tau_n$, and $h(p_{\mathscr{B}}(\ ), q_{\mathscr{B}}(\ ), sp_{\mathscr{B}}(\ )) = (A, \min(t_n, j+1))$ and thus they are identical in $\mathscr{B}_n$ by definition.

So we know that $\mathscr{B}_n \models E'_n$, which implies that $\exists$ epimorphism ψ: $T(\Sigma', E'_n) \to \mathscr{B}_n$, which had to be proved. $\square$

COROLLARY 3.6

$$f(n) < |T(\Sigma', E'_n)| < \infty.$$

Proof By Proposition 3.3 i):

$$T(\Sigma', E'_n) = \varphi(\mathscr{A}_n) \text{ for a certain homomorphism } \varphi.$$

So

$$|T(\Sigma', E'_n)| \leqq |\mathscr{A}_n| = |V|$$

$$= |\Pi(\sigma_n)| \cdot |\tau_n| = 2^{|\sigma_n|} \cdot (t_n + 1)$$

$$= 2^{\frac{1}{2}t_n(t_n - 1)} \cdot (t_n + 1) < \infty$$

because $t_n < \infty$, and on the other hand by Proposition 3.3 ii):
$\mathscr{B}_n = \psi(T(\Sigma', E'_n))$ for a certain homomorphism ψ. So $|T(\Sigma', E'_n)| \geqq |\mathscr{B}_n|$

As $\mathscr{B}_n \cong \left\langle \bigcup_{i \in \tau_n} \{(\emptyset, i)\} \cup \{(\{0,1\}, 0)\}, \Sigma' \right\rangle$

if $t_n \geqq 1$ and $\mathscr{B}_n \cong \left\langle \bigcup_{i \in \tau_n} \{(\emptyset, i)\}, \Sigma' \right\rangle$

if $t_n = 0$, where Σ' names the same functions as in $\mathscr{A}_n$, is

$$|T(\Sigma', E'_n)| \geqq |\mathscr{B}_n| \geqq t_n + 1 \geqq f(n) + 1 > f(n). \quad \square$$

Hence $T(\Sigma', E'_n)$ satisfies all the requirements to be $\mathscr{W}_n$ in Proposition 3.1. So take $\mathscr{W}_n = T(\Sigma', E'_n)$. Q.E.D.

References

[1] J. A. Bergstra and J.-J. Ch. Meyer, On bounds for the specification of finite minimal monoids by means of equations using only unary hidden functions, Institute of Applied Mathematics and Computer Science, University of Leiden, Report 80–11, Leiden, 1980.

[2] J. A. Bergstra, and J. V. Tucker, Equational specifications for computable data types: six hidden functions suffice and other sufficiency bounds, Mathematical Centre, Department of Computer Science Research Report IW 128, Amsterdam, 1980.

[3] J. A. Bergstra and J. V. Tucker, On bounds for the specification of finite data types by means of equations and conditional equations, Mathematical Centre, Department of Computer Science Research Report IW 131, Amsterdam, 1980.

[4] J. A. Goguen, J. W. Thatcher and E. G. Wagner, An initial algebra approach to the specification, correctness and implementation of abstract data types, in R. T. YEH (ed.) Current trends in programming methodology IV, Data structuring, Prentice-Hall, Englewood Cliffs, New Jersey, 1978, 80–149.

[5] Y. Manin, A course in mathematical logic, Springer-Verlag, New York, 1977.

[6] J. W. Thatcher, E. G. Wagner and J. B. Wright, Specification of abstract data types using conditional axioms, IBM—T. J. Watson Research Center Report RC-6214, Yorktown Heights, 1976.

[7] J. W. Thatcher, E. G. Wagner and J. B. Wright, Data type specification: parameterization and the power of specification techniques, IBM—T. J. Watson Research Center Report RC-7757, Yorktown Heights 1979. (Revision of paper with same title in Proceedings, SIGACT 10th Annual Symposium on Theory of Computing, ACM 1978, 119–132).