ANNALES SOCIETATIS MATHEMATICAE POLONAE
Series IV: FUNDAMENTA INFORMATICAE IV.4 (1981)

ALGORITHMIC DEGREES OF ALGEBRAIC STRUCTURES

Jan B e r g s t r a

Leiden University

Jerzy T i u r y n

RWTH Aachen

Received January 26, 1980

AMS Categories: 68B10, 68B05

A b s t r a c t. We define a reducibility relation $\leqslant$ between algebraic structures. $\mathcal{A} \leqslant \mathcal{B}$ means that $\mathcal{A}$ can be embeddet in an enrichment of $\mathcal{B}$ with partial computable operations. This notion is a generalized version of implementability as known in the theory of algebraic data types.

K e y w o r d s: algorithmic degrees, program schemes, programmability in algebraic structures.

1. Introduction

We will define a reducibility relation $\leqslant$ between algebraic structures. $\mathcal{A} \leqslant \mathcal{B}$ means that $\mathcal{A}$ can be embedded in an enrichment of $\mathcal{B}$ with partially computable operations. This notion is a generalized version of implementability as known in the theory of

algebraic data types. For this work we have no specific applications in mind. We feel that this reducibility, which is closely connected to the notion of existential recursiveness [4], deserves study in its own right. Apart from the previously mentioned connections with data types we would like to mention some places in the literature where similar notions occur.

Throughout the paper $\langle \omega, s, 0 \rangle$ denotes the structure over natural numbers with successor function s and constant 0. Moreover, for structures $\mathcal{A}, \mathcal{B}, \ldots$ the corresponding carries are denoted by A, B, ... respectively.

1.1.

In [3] it is proved that if $\langle \omega, s, 0 \rangle \leq \mathcal{A}$ then for every functional effective definitional scheme S (in the sense of H.Friedman [2]) there is a recursive procedure P with $\mathcal{A} \models P \sim S$, i.e. P and S are equivalent in $\mathcal{A}$.

1.2.

In [5] the notion of a privacy homomorphism between two algebraic structures is introduced. The existence of such a homomorphism between and $\mathcal{B}$ implies $\mathcal{A} \leq \mathcal{B}$, of course some restrictions are imposed on the embeddings in this case.

1.3.

In [2] the phrase "$\mathcal{A}$ is ω-rich" is used to express $\langle \omega, s, 0 \rangle \leq \mathcal{A}$. After the introduction of $\leq$ we will present a characterization of the existentially recursive structures as those infinite structures $\mathcal{A}$ for which $\mathcal{A} \leq \langle \omega, s, 0 \rangle$ holds. Then we characterize the structures which are equivalent to $\langle \omega, s, 0 \rangle$ under the equivalence $\equiv$ generated by $\leq$.

In section 3 we show that above each structure of the form $\langle A \rangle$, for an infinite set A, there is no minimal degree, but there

is a structure of the form $\langle A, r\rangle$, where r is a binary relation, which has a minimal cover.

2.

We refer to [1], [2] for such notions as functional and relational effective definitional scheme (feds and reds, respectively), and for the semantics of the logic of effective deffinitions.

If $\mathcal{A}$ is an algebraic structure then $\sigma_{\mathcal{A}}$ denotes the signature of $\mathcal{A}$, we always assume that σ contains only a finite number of finitary functions, relations and constants. If $\mathcal{A}$ and $\mathcal{B}$ are algebraic structures and h: $A \to B$ is an injective map then by $h(\sigma_{\mathcal{A}})$ we denote the image of $\sigma_{\mathcal{A}}$ in B under h, i.e. if $f \in \sigma_{\mathcal{A}}$ is an n-ary operation then corresponding $\tilde{f} \in h(\sigma_{\mathcal{A}})$ is defined as follows:
$\mathrm{dom}(\tilde{f}) = h(A)^n$; if $\vec{b} = (h(a_1), \ldots, h(a_n)) \in h(A)^n$ then $\tilde{f}(\vec{b}) =$
$= h(f(a_1, \ldots, a_n)$ relations from $\sigma_{\mathcal{A}}$ are transformed componentwise.

Let $\mathcal{A}$ be an algebraic system, and let $n \in \omega$. A relation $r \subseteq A^n$ is said to be semi-recursive (s.r.) in $\mathcal{A}$ iff there is a n-ary reds R over $\sigma_{\mathcal{A}}$ such that for all $\vec{a} \in A^n$, $\vec{a} \in r$ if $\models R[\vec{a}]$.

A partial function f: $A^n \to A$ is said to be partially recursive (computable) in $\mathcal{A}$ iff there is a n-ary feds S over $\sigma_{\mathcal{A}}$ such that for all $\vec{a} \in A^n$, $b \in A$: $f(\vec{a}) = b$ if $\mathcal{A} \models S[\vec{a}] = b$.

For algebraic structures $\mathcal{A}$, $\mathcal{B}$ we say that $\mathcal{A}$ is reducible to $\mathcal{B}$ ($\mathcal{A} < \mathcal{B}$) if there is an injective map h: $A \to B$ such that:

(2.1) h(A) is s.r. in $\mathcal{B}$

(2.2) For every constant c in $\sigma_{\mathcal{A}}$ there is a closed term t over $\sigma_{\mathcal{A}}$ such that $h(c) = t_{\mathcal{B}}$.

(2.3) The functions and relations in $h(\sigma_{\mathcal{A}})$ are partial recursive and semi-recursive in $\mathcal{B}$, respectively.

$\mathcal{A} \leq_h \mathcal{B}$ indicates that $\mathcal{A}$ is reducible to $\mathcal{B}$ by the map h.

2.1. Lemma. If $\mathfrak{A} \leqslant_h \mathfrak{B}$ then for every n-ary reds R over $\sigma_{\mathfrak{A}}$ there is a n-ary reds $\tilde{R}$ over $\sigma_{\mathfrak{A}}$ such that for all $\vec{a} \in A^n$,

$$\mathfrak{A} \models R[\vec{a}] \quad \text{iff} \quad \mathfrak{B} \models \tilde{R}[h(\vec{a})].$$

In other words, the property of being a s.r. relation is preserved by h.

P r o o f. By the definition of reducibility it follows that for any formula α of the form: $P(x_1,\ldots,x_n)$, or $x_n = f(x_1,\ldots,x_{n-1})$, where P is a predicate symbol and f is a function symbol in $\sigma_{\mathfrak{A}}$, there is a n-ary reds $\tilde{R}$ over $\sigma_{\mathfrak{B}}$ such that for all $\vec{a} \in A^n$:

(2.4) $$\mathfrak{A} \models \alpha[\vec{a}] \quad \text{if} \quad \mathfrak{B} = \tilde{R}[h(\vec{a})].$$

From the fact that red's are closed under boolean combinations and fed's are closed under composition (c.f. [6] it follows that (2.4) holds for arbitrary first order open formulas α.

Now if $R = \{(\Phi_n, \alpha_n)\}$ is an arbitrary n-ary reds over $\sigma_{\mathfrak{A}}$ then we first transform it to $R' = \{(\Phi_n \wedge \alpha_n,\ x_1 = x_1) : n \in \omega\}$. R' obviously has the property that for every $\vec{a} \in A^n$, $\mathfrak{A} \models R[\vec{a}]$ if $\mathfrak{A} \models R'[\vec{a}]$. So we may assume that R is already in the form $R = \{(\Phi_n,\ x_1 = x_1) : n \in \omega\}$. Let $Q_n = \{(\xi_k^n, \beta_k^n) : k \in \omega\}$ be a reds over $\sigma_{\mathfrak{B}}$ corresponding to the formula Φ_n for $n \in \omega$. Define $\tilde{R}$ as follows:

$$\tilde{R} = \{(\xi_0^0, \beta_0^0),\ (\xi_1^0, \beta_1^0),\ (\xi_0^1, \beta_0^1), \ldots\}.$$

Pairs (ξ_k^n, β_k^n) for $n, k \in \omega$ appear in $\tilde{R}$ in the order corresponding to the numbering along the "short diagonal" i.e. the standard enumeration of pairs of integers.

It is easy to check that $\tilde{R}$ has the required properties.

As an immediate consequence of lemma 2.1 one obtains the transitivity of $\leqslant$.

2.2. Proposition. If $\mathfrak{A} \leqslant_h \mathfrak{B}$ and $\mathfrak{B} \leqslant_g \mathfrak{C}$ then $\mathfrak{A} \leqslant_{gh} \mathfrak{C}$.

Let $\underline{\omega} = \langle \omega, s, 0 \rangle$, where $s(x) = x + 1$ is the successor function and 0 is the constant zero. Moreover, let $\omega = \langle \omega \rangle$, i.e. the algebraic system with empty signature over the set ω.

An algebraic system $\mathfrak{A}$ is said to be $\exists$-recursive is there is a bijection $g: A \to \omega$ such that $g(\sigma_{\mathfrak{A}})$ is recursive in $\underline{\omega}$.

2.3. Proposition. An algebraic structure $\mathfrak{A}$ is $\exists$-recursive if and only if $\omega \leqslant \mathfrak{A} \leqslant \underline{\omega}$.

P r o o f. "$\longrightarrow$" is obvious. Suppose that $\omega \leqslant \mathfrak{A} \leqslant_h \underline{\omega}$. Then $h(A)$ must be an infinite and recursively enumerable set. Hence there is a recursive injection $\xi : \omega \to \omega$ such that $\xi(\omega) = h(A)$. Then it is easy to check that $\xi^{-1}(h(\sigma_{\mathfrak{A}}))$ is a collection of recursive functions and relations and consequently $\xi^{-1}h : A \to \omega$ establishes that $\mathfrak{A}$ is $\exists$-recursive.

2.4. Lemma. Let $\mathfrak{A}$ be an algebraic system, then $\underline{\omega} \leqslant \mathfrak{A}$ if and only if $\sigma_{\mathfrak{A}}$ has at least one constant and $\mathfrak{A}$ has no finite subalgebras.

P r o o f. "$\longrightarrow$" suppose that $\omega \leqslant_h \mathfrak{A}$. By the definition of reducibility it follows that $\sigma_{\mathfrak{A}}$ must contain at least one constant. Moreover the infinite set $h(\omega)$ is contained in every subalgebra of $\mathfrak{A}$

"$\longleftarrow$" Suppose that $\mathfrak{A}$ has the mentioned properties. Let c be a constant of $\sigma_{\mathfrak{A}}$. Let $\{t_n : n \in \omega\}$ be an effective enumeration of all closed terms over $\sigma_{\mathfrak{A}}$ such that t_0 is c. Moreover, let $\Phi_{n,k}$ for $n, k \in \omega$ be the following formula: $x_1 \neq t_0 \wedge \ldots \wedge x_1 \neq t_{n-1} \wedge x_1 \neq t_n \wedge x_1 = t_{n+k+1}$.

For $n \in \omega$ let k_n be the least $k > n$ such that $t_{k,\mathfrak{A}} \notin \{t_{0,\mathfrak{A}}, \ldots, t_{n-1,\mathfrak{A}}\}$. Define $h : \omega \to A$ by $h(n) = t_{k_n,\mathfrak{A}}$. It is easy to check that:

(i) $h(0) = c$,

(ii) $h(\omega)$ is semi-recursive in $\mathcal{A}$. Take for example the following reds $\{(x_1 = t_n,\ x_1 = x_1) : n \in \omega\}$,

(iii) Let $S = \{(\phi_{n,k},\ t_{n+k+1}) : n, k \in \omega\}$. Then s computes the translation under h of s into $\mathcal{A}$, i.e. $\mathcal{A} \models S[t_{k_n}] = t_{k_{n+1}}$ for all $n \in \omega$.

Algebraic structures $\mathcal{A}$ and $\mathcal{B}$ are said to be of the same algorithmic degree if both $\mathcal{A} \leqslant \mathcal{B}$ and $\mathcal{B} \leqslant \mathcal{A}$ hold ($\mathcal{A} \equiv \mathcal{B}$).

2.5. Theorem. For an algebraic structure $\mathcal{A}$ the following conditions are equivalent:

(i) $\mathcal{A} \equiv \underline{\omega}$;

(ii) $\sigma_{\mathcal{A}}$ contains at least one constant and $\mathcal{A}$ is an $\exists$-recursive structure without finite subalgebras.

P r o o f. Immediate using proposition 2.3 and lemma 2.4.

3.

Let $\mathcal{A}$ and $\mathcal{B}$ be algebraic structures. We abbreviate $\mathcal{A} \leqslant \mathcal{B}$ and $\mathcal{B} \not\leqslant \mathcal{A}$ to $\mathcal{A} < \mathcal{B}$.

3.1. Theorem.

For an arbitrary infinite structure $\mathcal{A}$, if $A < \mathcal{A}$ then there is a structure $\hat{\mathcal{A}}$ such that $A < \hat{\mathcal{A}} < \mathcal{A}$, i.e. there is no minimal algorithmic degree above a pure infinite set.

P r o o f. Without loss of generality we may assume that the signature $\sigma_{\mathcal{A}}$ contains relations only, as we can replace all functions by their graphs without increasing the degree of the structure. So we assume that $\mathcal{A} = \langle A, r_1, r_2, \ldots, r_k \rangle$. As $A < \mathcal{A}$ there is no first order definition in the language of pure identity of at least one of the relations of $\mathcal{A}$, say r. Let $n \geqslant 1$ be the arity of r.

Let F be a maximal binary relation over $\{1,\ldots,n\}$ such that $(\bigwedge_{(i,j)\in F} x_i = x_j) \wedge \upsilon$ is not definable in the language of pure identity $\mathcal{L}_=$. It is easy to see that F is an equivalence relation.

Let m be the number of equivalence classes of F and let integers i, $1 \leqslant i \leqslant m$, denote all these classes.

Define a m-ary relation $\hat{r}$ by the formula:

$\hat{r}(x_1,\ldots,x_m) \leftrightarrow r^*(x_1(x_{i_1},\ldots,x_n)x_{i_n})$, where $1 \leqslant i_j \leqslant m$ for $1 \leqslant j \leqslant n$, and i_j is the name of the equivalence class of F containing j.

Let $\bar{r}$ be a m+1-ary relation defined by the formula:

$\bar{r}(x_1,\ldots,x_{m+1}) \leftrightarrow \bigwedge_{1\leqslant i\leqslant m} (x_i \neq y_{m+1}) \wedge \hat{r}$.

These are some properties of $\hat{r}$ and $\bar{r}$ which follow immediately from our definitions

(3.1) $\hat{r}$ and $\bar{r}$ are not first order definable in $\mathcal{L}_=$.

(3.2) $\langle A,\bar{r}\rangle \leqslant \langle A,\hat{r}\rangle \leqslant \langle A,r\rangle$

(3.3) for all $1 \leqslant i < j \leqslant m+1$ the formula $(y_i=y_j) \wedge \bar{r}$ is first order definable in $\mathcal{L}_=$.

From (3.3) it follows that $\langle A,\hat{r}\rangle \not\leqslant \langle A,\bar{r}\rangle$ because in $\langle A,\bar{r}\rangle$ all k-ary s.r. relations, for $1 \leqslant k \leqslant m$, are trivial, i.e. first order definable in $\mathcal{L}_=$. In particular ϕ and A are the only s.r. subsets in $\langle A,\bar{r}\rangle$, so the possible reduction from $\langle A,\hat{r}\rangle$ to $\langle A,\bar{r}\rangle$ is a bijection. Then the image of $\hat{r}$ under this reduction will be first order definable in $\mathcal{L}_=$. But this is impossible because then $\hat{r}$ itself would have been first order definable in $\mathcal{L}_=$.

So we have shown that $\langle A\rangle < \langle A,\bar{r}\rangle < \langle A,\hat{r}\rangle$ which completes the proof of the theorem.

The last part of the above proof leads to the following result.

3.2. Corollary. For an arbitrary infinite set A and for every $n > 1$ there is an algebraic structure $\mathcal{A}_n = \langle A, r \rangle$ with $r \subseteq A^n$ such that

(i) $A < \mathcal{A}_n$,

(ii) If $A < \mathcal{B} < \mathcal{A}_n$ is an algebraic structure with $\sigma_{\mathcal{B}}$ containing only relations of arity less than n, then $\mathcal{B} \equiv \mathcal{A}_n$, i.e. there is no nontrivial structure between A and $\mathcal{A}_n$ with relations of arity less than n.

We will now prove that the algorithmic degrees of infinite structures are not dense.

3.3. Theorem. There are infinite structures $\mathcal{A}$ and $\mathcal{A}'$ such that

(i) $\mathcal{A}' < \mathcal{A}$ and

(ii) $\mathcal{A}' \leq \mathcal{B} \leq \mathcal{A}$ implies $\mathcal{A}' \equiv \mathcal{B}$ or $\mathcal{A} \equiv \mathcal{B}$.

P r o o f. Let A be an infinite set and $a \in A$, we define r_a and r_a^1 as follows on A:

$$r_a(x) \Leftrightarrow x = a: \quad r_a^1(x,y) \Leftrightarrow x = a \wedge x \neq y.$$

We take $\mathcal{A}' = \langle A, r_a^1 \rangle$ and $\mathcal{A} = \langle A, r_a \rangle$

$\mathcal{A}' \leq \mathcal{A}$ is immediate, take $\phi(x) = x : A \to A$, to see $\mathcal{A} \not\equiv \mathcal{A}'$ assume that $\Psi : A \to A$ is an imbedding of $\mathcal{A}$ in $\mathcal{A}'$; as $\{\bar{a}\}$ is a recursive subset of $|\mathcal{A}|$, $\Psi(a)$ must be a semirecursive subset of $|\mathcal{A}'|$. However, it is easily seen that the semirecursive subsets of $|\mathcal{A}'|$ are either $\emptyset$ or A (because a computation with a single cannot involve any use of r_a^1).

Let us now assume $\mathcal{A}' \leq \mathcal{B} \leq \mathcal{A}$ and $\mathcal{B} = \langle B, f_1, \ldots, f_k, r_1, \ldots, r_l \rangle$ $\mathcal{B}$ cannot contain any constants of course. Let Φ be an embedding: $\mathcal{A} \to \mathcal{B}$ and Ψ an embedding $\mathcal{B} \to \mathcal{A}$.

Replacing $\mathcal{B}$ by an isomorphic structure we can assume that $|\mathcal{B}| \subseteq A$ and that Ψ is the identity function. It follows that $|\mathcal{B}|$

is semirecursive in $\mathcal{A}$ and thus $|\mathfrak{B}| = A$ because the semirecursive subsets of A in $\mathcal{A}$ are $\emptyset$, $\{a\}$, A, $A - \{a\}$, and $|B| = A - \{a\}$ would imply that B has no nontrivial structure at all (all functions and relations are recursive in the equality relation). Let $f: A^n \to A$ ($r: A^n \to \{T, F\}$) be a function (relation) of $\mathfrak{B}$. If $V \subseteq A - \{a\}$ then $f(r)$ must be constant on V^n. Suppose $\phi(a) \neq a$; take x such that $x \neq a$ and $\phi(x) \neq a$, which is possible because A is infinite. Then take $V = \{\phi(a), \phi(x)\}$. It follows that the operations and relations of $\mathfrak{B}$ are constant on V^n. As $\mathcal{A}' \leq \mathfrak{B}$ the operations and relations of $\mathcal{A}'$ must therefore be constant on $\{a, x\}^2$ but this is not the case. It follows that $\phi(a) = a$. As $\phi(A)$ is semi-recursive in $\mathfrak{B}$, it is so in $\mathcal{A}$, therefore $\phi(A) = A$. ϕ is injective and bijective and as such an automorphism of $\mathcal{A}'$. It follows that we may replace $\mathcal{A}'$ by an isomorphic copy of itself and take ϕ to be the identity as well.

We must now show that either r_a is computable in $\mathfrak{B}$ or the relations and operations of $\mathfrak{B}$ are computable from r_a^1.

The first step is to reduce $\mathfrak{B}$ to a relational structure by proving that for every function $f(x_1, \ldots, x_n)$ of $\mathfrak{B}$ there can be found a relation $h(y_1, \ldots, y_n, y_{n+1})$ such that f is computable from h and h from f.

Take $h(y_1, \ldots, y_n, y_{n+1}) \Leftrightarrow f(y_1, \ldots, y_n) = y_{n+1}$.

Obviously h is computable from f. Now suppose that h is given. To compute f from h note that as $\mathcal{A}$ contains no functions, the image of each function f in $\mathfrak{B}$ on an input list must be one of the inputs itself.

So we assume that $\mathfrak{B}$ contains relations only.

Finally consider an n-ary relation r of $\mathfrak{B}$. We will show that either r_a is computable from r or r is computable from r_a^1. This proves the required result immediately. We distinguish two cases:

(i) There are x an y such that $r(x,\ldots,x) \not\Leftrightarrow r(y,\ldots,y)$.
Then either x or y is a and therefore either $r_a(x) \Leftrightarrow r(x,\ldots,x)$ or $r_a(x) \Leftrightarrow \neg r(x,\ldots,x)$ holds for all x.
So in this case r_a is computable from r.

(ii) For all x,y $r(x,\ldots,x) \Leftrightarrow r(y,\ldots,y)$.
Then to compute r from r_a^1 one works as follows:
Let $r(x,\ldots,x) = T$ for all x for instance. Then given $x_1,\ldots,x_n$ decide if for some $i \neq j, x_i \neq x_j$, if not then $r(x_1,\ldots,x_n) = r(x_1,\ldots,x_1) = T$.
If so then r_a can be computed from r_a^1, x and y. As r can be computed from r_a we find that in this case r is computable from r_a^1.

References

[1] B e r g s t r a, J. A., T i u r y n, J., Implicit definability of algebraic systems by means of program properties. In: Proceedings of FC T'79. Ed. L. Budach, Akademie Verlag, Berlin 1979.

[2] F r i e d m a n, H., Algorithmic procedures, generalized Turing algorithms and elementary recursion theory, in: Logic colloquium '69, ed. R.O. Gandy and C.M.E. Yates, North Holland, 1971.

[3] K f o u r y, A. J., Translatability of schemas over restricted Interpretations. J.C.S.S. vol. 8, 1974.

[4] L a c o m b e, D., Recursion theoretic structure for relational systems, in the same volume as (2).

[5] R i v e s t, R. L., A d l e m a n, L. and D e r t o u z o s, M. L., Data Banks and Privacy Homomorphisms, in: Foundations of secure computation Ed. R.A. Demillo et. al, Academic Press 1978.

[6] T i u r y n, J., Logic of effective definitions. Schriften zur Informatik und Angewandten Mathematik, Bericht Nr. 55, RWTH Aachen, 1979. To appear in Fundamenta Informaticae.