Commentationes Mathematicae Universitatis Carolinae

Marie Demlová; Jiří Demel; Václav Koubek

Simplicity of algebras requires to investigate almost all operations

Commentationes Mathematicae Universitatis Carolinae, Vol. 23 (1982), No. 2, 325--335

Persistent URL: http://dml.cz/dmlcz/106155

COMMENTATIONES MATHEMATICAE UNIVERSITATIS CAROLINAE
23,2 (1982)

SIMPLICITY OF ALGEBRAS REQUIRES TO INVESTIGATE ALMOST ALL OPERATIONS

M. DEMLOVÁ, J. DEMEL, V. KOUBEK

Abstract: It is shown: If we want to prove that an algebra is simple or subdirectly irreducible then we must investigate almost all results of all operations. Analogously, if we want to prove that an automaton is simple or subdirectly irreducible then we must investigate almost its whole next state function. The consequences concerning the computation theory are given.

Key words: Simple algebra, subdirectly irreducible algebra, automaton, algorithm, time complexity.

Classification: 03D15, 08A30, 08A99

This paper continues the papers [3,4] in which an algorithm for finding minimal congruences of an algebra has been given and some consequences of it have been stated. Particularly, upper bounds for time complexity of a decision whether a given algebra is simple or subdirectly irreducible have been proved. Here, we give lower bounds of time complexity of these problems.

By an algebra we mean a couple $\mathcal{A} = (A,F)$, where A is an underlying finite set and $F = \{f_i \mid i \in I\}$ is a finite family of operations, i.e. mappings $f_i\ A^{m_i} \longrightarrow A$ where m_i is a natural number called arity of the operation f_i and will be denoted by $ar(f_i)$.

The algebra is assumed to be given by lists of elements, operations and results of these operations.

Denote by $|A|$ the cardinality of A. In [4] there is proved that the upper bounds of time complexity of a decision whether a given algebra is simple or subdirectly irreducible are $\mathcal{O}(\sum_{f \in F} |A|^{ar(f)+1})$. Moreover, there is an algorithm deciding whether an abelian group is simple (or subdirectly irreducible) requiring $\mathcal{O}(\sqrt[7]{|A|})$ (or $\mathcal{O}(|A|)$, resp.) time. This leads to the question how effective algorithms, in general, exist for these problems. Here is proved that lower bounds are "linear", precisely $\mathcal{O}(\sum_{f \in F} |A|^{ar(f)})$.

As a consequence of these results we obtain that these problems belong to the following class of problems:
If we consider a model of computation which allows to access every element of the input data set in time at most "logarithmic" to the size of the input data set then these problems are in NP but not in P. The same property has e.g. the problem whether a sequence of 0 and 1 contains at most one 1.

Recall some basic notions concerning algebras. Denote by Δ , ∇ , resp. the least (identical), greatest, resp. congruences.

An algebra is simple if it has no proper congruences (i.e. the only congruences are Δ and ∇).

An algebra is subdirectly irreducible if every separating system of congruences (i.e. for every pair (a,b) of distinct elements there is a congruence not containing (a,b)) contains Δ . For finite algebras it is equivalent to that there is only one minimal non-identical congruence.

For more details concerning algebras see e.g. [5].

To prove lower bounds of time complexity of deterministic algorithms we shall use the following classical method:

Suppose a class $\mathcal{L}$ of algebras (not necessarily of the same type) and a subclass $\mathcal{S} \subseteq \mathcal{L}$ are given. Let us consider the decision problem whether a given algebra $\mathcal{A} \in \mathcal{L}$ belongs to $\mathcal{S}$.

Let t be a positive integer. For each integer $n \geq t$ and each finite sequence of positive integers $r_1,\dots,r_k$ we shall construct an algebra $\mathcal{A}(n,r_1,\dots,r_k) \notin \mathcal{S}$ and a set of algebras $\mathcal{D}(n,r_1,\dots,r_k) = \{\mathcal{A}_j \mid j \in I\} \subseteq \mathcal{S}$ such that:

1) They have the same underlying set having cardinality n and k operationswith arities $r_1,\dots,r_k$.

2) Each $\mathcal{A}_j$ differs from $\mathcal{A}(n,r_1,\dots,r_k)$ in exactly one result of exactly one operation and distinct algebras $\mathcal{A}_i$, $\mathcal{A}_j \in$ $\in \mathcal{D}(n,r_1,\dots,r_k)$ differ from $\mathcal{A}(n,r_1,\dots,r_k)$ in results of distinct operations or in results of the same m-ary operation but on two distinct m-tuples.

Then every deterministic algorithm deciding whether a given algebra, having n elements and arities of operations $r_1,\dots,r_k$ is in $\mathcal{S}$, has to examine at least card $\mathcal{D}(n,r_1,\dots$ $\dots,r_k)$ results of operations, hence card $\mathcal{D}(n,r_1,\dots,r_k)$ is a lower bound of time complexity.

We shall now show that for a decision whether an algebra is simple (subdirectly irreducible) it is necessary to use in the computation results of all operations on nearly all ar(f)-tuples of the underlying set.

<u>Theorem 1</u>. Let $\mathcal{L}$ be a class of algebras $\mathcal{A} = (A,F) \in \mathcal{L}$ with $\sum_{f \in F} ar(f) \geq 2$ and $|A| \geq 3$.

Then every deterministic algorithm deciding whether a given algebra from $\mathcal{L}$ is simple requires time at least $\mathcal{O}(\sum_{f \in F} |A|^{ar(f)})$.

Proof: We shall use the method described above. First, let us construct algebras $\mathcal{A}(n,r_1,\dots,r_k) = (A,F)$, which are "almost simple" for $|A| \geq 3$.

We can suppose that $r_i > 0$ for $i = 1,\dots,k$, since nullary operations have no influence to congruences. Put $A = \{0,1,\dots \dots,n-1\}$. Choose $a,b \in \{1,\dots,k\}$ and (r_a-1)-tuple α and (r_b-1)-tuple β of elements of A such that either $a \neq b$ or $\alpha \neq \beta$.

$$\text{Put:}\quad \begin{aligned} &f_a(0,\alpha) = f_b(0,\beta) = 0, \\ &f_a(1,\alpha) = 1, \\ &f_a(i,\alpha) = i-1 \text{ for } 2 \leq i \leq n-1, \\ &f_b(1,\beta) = n-2, \\ &f_b(2,\beta) = n-1, \end{aligned} \qquad (*)$$

otherwise, results of all operations are put to be

equal to 1 . (**)

Notice that $(*)$ ensures that whenever distinct $i,j \in A \setminus \{0\}$ are congruent, so are all elements of $A \setminus \{0\}$. Therefore $\mathcal{A}(n,r_1,\dots,r_k)$ has exactly one non-trivial congruence given by $i \sim j$ iff either $i = j$ or $i \neq 0 \neq j$.

Moreover, for every f_i and r_i-tuple γ , such that γ contains at least one non-zero element and $f_i(\gamma)$ is defined by $(**)$, one can obtain a simple algebra by the single change putting $f_i(\gamma) = 0$.

Let $\mathcal{D}(n,r_1,\dots,r_k)$ be the set of all such "locally changed" algebras. The number of all such changes, i.e.

card $\mathcal{D}(n,r\ ,\dots,r\ )$ is at least $\sum_{i=1}^{k} n^{r_i} - k - n - 3$ which is $\mathcal{O}(\sum_{i=1}^{k} n^{r_i})$.

__Theorem 2.__ Let $\mathcal{L}$ be a class of algebras $\mathcal{A} = (A,F) \in \mathcal{L}$ with $|A| \geq 4$.

Then every deterministic algorithm deciding whether a given algebra from $\mathcal{L}$ is subdirectly irreducible requires time at least $\mathcal{O}(\sum_{f \in F} |A|^{ar(f)})$.

Proof: We shall construct algebras $\mathcal{A}(n,r_1,\dots,r_k) = (A,F)$ for $|A| \geq 4$.

First, consider the case $\sum r_i \geq 2$.

Put $A = \{0,1,\dots,n-1\}$. Choose $a,b \in \{1,\dots,k\}$ and (r_a-1)-tuple α and (r_b-1)-tuple β of elements of A such that either $a \neq b$ or $\alpha \neq \beta$.

Put: $f_a(i,\alpha) = i$ for $i = 1,n-1$,

$f_a(i,\alpha) = i+1$ for $i \neq 1$, $i \neq n-1$,

$f_b(n-1,\beta) = 2$, $f_b(n-2,\beta) = 3$, $\quad (*)$

$f_b(1,\beta) = f_b(0,\beta) = 0$,

otherwise, results of all operations are put to be

the first projection. $\quad (**)$

So, $\mathcal{A}(n,r_1,\dots,r_k)$ is defined.

Notice that $(*)$ ensures that:

1) Whenever distinct $i,j \in A \setminus \{0,1\}$ are congruent, so all elements of $A \setminus \{0,1\}$.

2) Whenever $i \in A \setminus \{0,1\}$, $j \in \{0,1\}$ are congruent, so are all elements of A.

Therefore $\mathcal{A}(n,r_1,\dots,r_k)$ has exactly two minimal non-identical congruences:

1) $i \sim j$ iff either $i,j \in A \setminus \{0,1\}$ or $i =$,

2) $i \approx j$ iff either $i,j \in \{0,1\}$ or $i = k$.

Thus $\mathcal{A}(n,r_1,\dots,r_k)$ is not subdirectly irreducible.

On the other hand, for every f_i and r_i-tuple γ such that $f_i(\gamma)$ is defined by (**) we can obtain a subdirectly irreducible algebra by a single change of $f_i(\gamma)$ in the following way: if $f_i(\gamma) \in \{0,1\}$ then put $f_i(\gamma) = 2$, otherwise put $f_i(\gamma) = 0$. Indeed, one of two minimal non-trivial congruences of $\mathcal{A}(n,r_1,\dots,r_k)$ is not a congruence in the changed algebra and no other non-trivial congruence has occurred due to (*).

The number of all such changes is at least $\sum_{i=1}^{k} n^{r_i} - n - 2$ which is $\mathcal{O}(\sum_{i=1}^{k} n^{r_i})$.

Now, consider the case $\sum_{i=1}^{k} r_i = 1$. We can assume that $k = 1$ and $r_1 = 1$. Define $\mathcal{A}(n,r_1) = (A,F)$ by $A = \{0,\dots,n-1\}$ and $f_1(0) = 0$, $f_1(i) = i-1$ for $i \neq 0$. Then $\mathcal{A}(n,r_1)$ is subdirectly irreducible since it has only one minimal non-identical congruence given by $i \sim j$ iff either $\{i,j\} = \{0,1\}$ or $i = j$.

For every $i \in A$ one can obtain a subdirectly reducible algebra by a single change

$f_1(i) = i$ if $i \neq 0$, or $f_1(i) = i+1$ if $i = 0$.

The resulting algebra has at least two minimal non-identical congruences, thus it is not subdirectly irreducible.

The number of all such changes is n.

<u>Corollary 1</u>. Considering algebras of the same fixed ty- (i.e. with the same arities of operations) one obtains in above theorems the lower bounds $\mathcal{O}(|A|^{\max(ar(f))})$.

Corollary 2. Consider the class $\mathcal{L}$ of all algebras (A,F) with $\sum_{f\in F} ar(f) \leq |A|$. Then every deterministic algorithm deciding whether a given algebra from $\mathcal{L}$ is simple (subdirectly irreducible) has time complexity at least $\mathcal{O}(n^n)$, where $n = |A|$.

Note. The exponential time limit is due to the fact that the complexity is considered with respect to n only and due to the definition of the class $\mathcal{L}$.

Now, let us deal with automata. Recall that $\mathfrak{M} = (X,Q,Y,\delta,\mu)$ is a Mealy, Moore resp. automaton if X,Y,Q are sets and $\delta : X \times Q \longrightarrow Q$, $\mu : X \times Q \longrightarrow Y$, $\mu : Q \longrightarrow Y$ resp. are mappings. Further $\mathfrak{M} = (X,Q,\delta)$ is a Medvedev automaton if X, Q are sets and $\delta : X \times Q \longrightarrow Q$ is a mapping. A congruence on a Mealy, Moore, Medvedev automaton is an equivalence on X,Q,Y which is "preserved" by mappings δ, μ. (If we consider automata as heterogeneous algebras then these mappings correspond with operations.) Hence we can define subdirectly irreducible automata and simple automata as above.

Corollary 3. Every deterministic algorithm deciding whether a Mealy, Moore, Medvedev resp. automaton is subdirectly irreducible (or simple) requires time at least $\mathcal{O}(\min\{|X|.|Q|,|Q^Q|\})$.

Proof: By results in [2] we have that: if there is a deterministic algorithm deciding whether a Mealy (or Moore) automaton is subdirectly irreducible (simple) requiring $\mathcal{O}(t)$ time then there is a deterministic algorithm deciding whether a Medvedev automaton is subdirectly irreducible (simple) with the same time bound. This allows us to deal only Medvedev automata.

Clearly, every Medvedev automaton $\mathcal{M} = (X,Q,\sigma)$ corresponds with an algebra $\mathcal{A}(\mathcal{M}) = (Q, \{\sigma(x,-) \mid x \in X\})$ and $\mathcal{M}$ is subdirectly irreducible (simple) iff $\mathcal{A}(\mathcal{M})$ is so and

$\sigma(x_1,-) \neq \sigma(x_2,-)$ whenever $x_1 \neq x_2$ $(*\!*\!*)$

Hence to get Corollary 3 it suffices to modify the definitions of $\mathcal{A}(n,1,\dots,1)$ and $\mathcal{D}(n,1,\dots,1)$ in the proofs of Theorems 1,2 so that also $(*\!*\!*)$ will hold.

Theorem 1. It suffices to change values of $f(q)$ for some couples f, q, defined by $(**)$ so that $f(q) \neq 0$. Congruences on the new $\mathcal{A}(n,1,\dots,1)$ and algebras of $\mathcal{D}(n,1,\dots,1)$ do not change. Such different operations we have $(n-1)^n$ and therefore card $\mathcal{D}(n,1,\dots,1) \geq (n-1)^n$.

Theorem 2. It suffices to change values of $f(q)$ for some couples f, q, defined by $(**)$ so that $f(q) \in \{0,1\}$ iff $q \in \in \{0,1\}$. Such different operations we have $4.(n-2)^{n-2}$ and therefore card $\mathcal{D}(n,1,\dots,1) \geq 4.(n-2)^{n-2}$.

Theorem 3. There exists a non-deterministic algorithm deciding whether a given algebra is simple with time complexity $\mathcal{O}(n^3.(t+m))$ where:

n is the number of elements of the underlying set,

m is the maximal arity of operations and

t is the worst time needed for obtaining the result of any given r-ary operation on the given r-tuple of elements of the underlying set.

Note: The time bound in the above theorem is not the best possible. One can construct an algorithm with time complexity $\mathcal{O}(n^2.(t + m))$, but the proof is more complicated and later we use only the fact that time complexity is polynomial with respect to n.

Proof: An algebra $\mathcal{A} = (A,F)$ is simple iff for every pair of distinct elements $a,b \in A$ the implication

(1) whenever a, b are congruent, all elements of A are so

holds.

First, consider a fixed pair of elements $a,b \in A$. We shall describe a non-deterministic procedures verifying implication (1) with time complexity $\mathcal{O}(n.(t + m))$. Then the use of this procedure for all pairs of distinct elements will do.

To verify implication (1) it suffices to construct a sequence of pairs of distinct elements of A, $\{a_1,b_1\}$, $\{a_2,b_2\}$, $\dots,\{a_s,b_s\}$ such that:

(2) $\{a_1b_1\} = \{a,b\}$.

(3) For every pair $\{a_i,b_i\}$, $i > 1$ there exists $j < i$ such that there exist $f \in F$, two ar(f)-tuples $x_1,\dots,x_{ar(f)}$, $y_1,\dots$ $\dots,y_{ar(f)}$ and $k \leq ar(f)$ such that

(i) $\{x_k,y_k\} = \{a_j,b_j\}$,

(ii) $x_t = y_t$ for all $t = 1,\dots,ar(f)$ except for $t = k$,

(iii) $\{a_i,b_i\} = \{f(x_1,\dots,x_{ar(f)}),\ f(y_1,\dots,y_{ar(f)})\}$.

(4) The set $\{\{a_i,b_i\} \mid i = 1,\dots,s\}$ forms a set of edges of a tree on the set A.

If such a sequence exists then, clearly, implication (1) holds. Moreover, in such a case $s = n-1$ due to (4). Therefore the time needed for random choice of a_i,b_i,f,x_z,y_t,k is $\mathcal{O}(n.m)$ and the time needed for checking correctness of this choice is $\mathcal{O}(n.t)$.

It remains to show that if the algebra is simple then for every pair of distinct elements $a,b \in A$ there exists a sequence fulfilling (2) - (4). Indeed, there exists a sequence fulfilling (2),(3) and such that the set $\{\{a_i,b_i\} \mid i = 1,\ldots ,s\}$ forms a set of edges of a graph without cycles (i.e. only the condition of connectedness of the graph is omitted). Consider a maximal (with respect to inclusion) such sequence S and take the least equivalence relation $\sim$ with $a_i \sim b_i$ for $i = 1,\ldots,s$. Then $\sim$ is the minimal congruence containing (a,b). To show this, it suffices to verify the substitution property: if $c \sim d$ then $f(x_1,\ldots,x_{k-1},c,x_{k+1},\ldots,x_{ar(f)}) \sim$ $\sim f(x_1,\ldots,x_{k-1},d,x_{k+1},\ldots,x_{ar(f)})$ for all $f \in F$, $1 \leq k \leq ar(f)$, $x_t \in A$. For pairs $\{c,d\} \in S$ it follows from (3) and from maximality of S. Let $\{c,d\} \in S$ and $c \sim d$. Then there exists a path, in the graph induced by S, connecting c and d, that consists of pairs belonging to S. For these pairs the substitution property holds, so, using transitivity of $\sim$, we obtain that it holds for $\{c,d\}$,too.

Now, the simplicity of the algebra yields (4).

Note. An analogous theorem also holds for existence of a non-deterministic algorithm deciding whether an algebra is subdirectly irreducible. In this case, first we guess a minimal congruence $\sim$ and then for each couple $\{a,b\}$ of points we generate a forest by (2) and (3) the weakly connected components of which are unions of classes of $\sim$.

Consider the following computational model:

(a) there is a natural number K, such that an arbitrary element of an input data set can be accessed in time

$\mathcal{O}((\log m)^K)$ (where m is the size of the input data set).

This holds e.g. if the time needed for reading input data is not included in time complexity, or if the input data set is not arranged on an input tape but in a tree and a reading head moves along its edges.

Then Corollary 2 and Theorem 3 imply that the problems whether an algebra in $\mathcal{L}$ is simple, or subdirectly irreducible belong to NP (in this computational model) but not to P. Thus for this computational model NP$\neq$P.

References

[1] A.V. AHO, J.E. HOPCROFT, J.D. ULLMAN: The design and analysis of computer algorithms, Addison-Wesley, 1974.

[2] M. DEMLOVÁ, J. DEMEL, V. KOUBEK: On subdirectly irreducible automata, to appear in RAIRO.

[3] M. DEMLOVÁ, J. DEMEL, V. KOUBEK: Several algorithms for finite algebras, Fundamentals of Computer Theory, FCT´79, 1979, 99-104.

[4] M. DEMLOVÁ, J. DEMEL, V. KOUBEK: Algorithms deciding subdirect irreducibility of algebras, to appear.

[5] G. GRÄTZER: Universal algebra, Princeton, Van Nostrand and co., Inc., 1968.

Electro-engineering Faculty, Technical University of Prague,
Suchbátarova 2, 16627 Praha 6, Czechoslovakia

Faculty of Civil Engineering, Technical University of Prague,
Thákurova 7, 16629 Praha 6, Czechoslovakia

Faculty of Mathematics and Physics, Charles University, Malostranské nám. 25, 11800 Praha 1, Czechoslovakia

(Oblatum 30.11. 1981)