REPORTS ON MATHEMATICAL LOGIC
31 (1997), 75–92

Tomasz A. GORAZD

THE ISOMORPHISM TESTING FOR DIRECTLY REPRESENTABLE VARIETES

A b s t r a c t Let $\mathcal{V}$ be a variety of algebras with a finite list of finite directly indecomposable members. We show that there is a polynomial time algorithm that tests the isomorphism between any two finite algebras from $\mathcal{V}$. This includes the following classical structures in algebra:

- Abelian groups with $nx = 0$, $n > 0$,
- Boolean algebras,
- Rings with $x^m = x$, $m > 1$,
- Modules over a finite semisimple ring.

An isomorphism testing problem for a class $\mathcal{K}$ of structures ($\mathcal{K}$–**Iso**) is to determine the exact computational complexity of the following problem:

INSTANCE: Two finite structures from $\mathcal{K}$.

QUESTION: Is there an isomorphism between them ?

Received May 14, 1997
Research supported by the KBN grant no. 2P03A 031 09.

We say that a problem can be **solved in polynomial time** if there is a polynomial p and an algorithm $\mathcal{A}$ such that $\mathcal{A}$ solves the problem for all possible input data and the computation always stops after at most $p(n)$ steps where n is the size of input data.

One of the most famous and fascinating problems in isomorphism testing and the complexity theory is the isomorphism problem for graphs : **Graph–Iso**. This is because the problem belongs to the class NP but is one of the few known problems (see [5]) for which neither its NP–completeness has been shown nor any polynomial time algorithm has been found. We refer the reader to [9] for a discussion of the influence the possible solutions to the problem would have for the computational hierarchy.

A lot of problems have already been proved to be polynomially equivalent to **Graph–Iso**. Such classes are to be called isomorphism complete. Among them we have: regular graphs [2], semigroups [2], algebras with two unary operations [8], lattices. All the above results were established by polynomial time coding of graphs into considered structures.

On the other hand for many classes polynomial time algorithms for isomorphism testing are known. Such results are usually established by a deep look into the structure of members of the investigated class. Sometimes nice representation can help a lot. Thus the research on the isomorphism problem can be also considered as building a nice structure theory and/or representation theory.

This paper is a contribution to the following problem:

Characterize (quasi)varieties of algebras that have the isomorphism testing problem solvable in polynomial time.

In this paper we assume that a variety $\mathcal{V}$ is presented by a finite set of finite algebras $\mathcal{K}$ which generates $\mathcal{V}$, i.e. $\mathcal{V} = HSP(\mathcal{K})$.

Although there are a lot of results dealing with the problem, almost all of them describe particular examples of varieties that are either isomorphism complete or have polynomial time isomorphism testing. Only a few of them are general enough to be considered to give algebraic conditions for a (quasi)variety in order to have polynomial time isomorphism testing.

One should mention among them: varieties of multi–unary algebras [11], strongly Abelian varieties [14], varieties of semigroups and monoids [6], finitely generated varieties of lattices [15] and (quasi)varieties generated by a single two element algebra [7].

In this paper we deal with the isomorphism testing problem for directly representable varieties. We will show that it has a polynomial time solution. A variety $\mathcal{V}$ is said to be a *directly representable* if it is finitely generated and has (up to isomorphism) only finitely many finite directly indecomposable members. From now on by $\mathcal{V}_{DI}$ we mean the set $\{\mathbf{K}_1 \dots \mathbf{K}_s\}$ of all (up to isomorphism) finite directly indecomposable algebras from $\mathcal{V}$.

Every finite algebra from $\mathcal{V}$ is isomorphic to an algebra from the class $P_{fin}(\mathcal{V}_{DI})$ of all finite products of $\mathcal{V}_{DI}$. Unfortunately the representation of an algebra from $\mathcal{V}$ by a product of elements from $\mathcal{V}_{DI}$ is not unique. Therefore we can not get the answer about an isomorphism only by simple decomposition into elements from $\mathcal{V}_{DI}$. Additionally, if we want to use the decomposition into $\mathcal{V}_{DI}$, we have to get it in polynomial time.

In this paper we use the concepts of commutator and center in an algebra from a congruence modular variety. For definitions and more information we refer to [4]. For any algebra $\mathbf{A}$ the commutator of two congruences ϕ and θ is denoted by $[\phi, \theta]$. The center of $\mathbf{A}$ is denoted by $\xi_{\mathbf{A}}$. The least and largest elements of the congruence lattice of $\mathbf{A}$ are $0_{\mathbf{A}}$ and $1_{\mathbf{A}}$ (sometimes 0 and 1, if the algebra $\mathbf{A}$ is known from the context).

We will often use the following properties of a directly representable variety $\mathcal{V}$ (see R.McKenzie [12] for proofs).

1. $\mathcal{V}$ is congruence permutable ([12] Th. 5.11(1)),
2. each element of $\mathcal{V}_{DI}$ is either abelian or simple ([12] Cor. 5.10),
3. for each finite algebra $\mathbf{A}$ in $\mathcal{V}$ the congruences $[1_{\mathbf{A}}, 1_{\mathbf{A}}]$ and $\xi_{\mathbf{A}}$ form a complement pair in $\mathbf{ConA}$ ([12] Th. 5.9), i.e. $\mathbf{A}$ is isomorphic to $\mathbf{A}/[1_{\mathbf{A}}, 1_{\mathbf{A}}] \times \mathbf{A}/\xi_{\mathbf{A}}$,

4. for every algebra $\mathbf{A}$ in $\mathcal{V}$ the congruence $[1_{\mathbf{A}}, 1_{\mathbf{A}}]$ is a neutral element, which means that for all congruences $\phi, \psi \in Con\mathbf{A}$ the sublattice generated by $[1_{\mathbf{A}}, 1_{\mathbf{A}}], \phi$ and ψ is distributive ([12] Lemma 5.8),
5. for every congruence ϕ of an algebra $\mathbf{A} \in \mathcal{V}$ we have $[1_{\mathbf{A}}, 1_{\mathbf{A}}] \wedge \phi = [1_{\mathbf{A}}, \phi]$ ([12] Lemma 5.8).

For a finite algebra $\mathbf{A}$ from $\mathcal{V}$, any product of algebras from $\mathcal{V}_{DI}$ which is isomorphic to $\mathbf{A}$ will be called a $\mathcal{V}_{DI}$-factorization of $\mathbf{A}$. For any two $\mathcal{V}_{DI}$-factorizations of a finite algebra $\mathbf{A}$ from $\mathcal{V}$ the products of all abelian factors occurring in each factorization are isomorphic, while nonabelian simple factors are the same ([12] Th. 5.9).

For a finite algebra $\mathbf{A}$ from $\mathcal{V}$ and a $\mathcal{V}_{DI}$-factorization of $\mathbf{A}$ the quotient $\mathbf{A}/[1_{\mathbf{A}}, 1_{\mathbf{A}}]$ is isomorphic to the product of all abelian factors of $\mathbf{A}$, and $\mathbf{A}/\xi_{\mathbf{A}}$ is isomorphic to the product of all nonabelian simple factors of $\mathbf{A}$ ([12] Th. 5.9).

Because for any algebra from $\mathcal{V}$ the congruences ξ and $[1, 1]$ are complementary, two finite algebras $\mathbf{A}$ and $\mathbf{B}$ are isomorphic iff $\mathbf{A}/\xi_{\mathbf{A}} \cong \mathbf{B}/\xi_{\mathbf{B}}$ and $\mathbf{A}/[1_{\mathbf{A}}, 1_{\mathbf{A}}] \cong \mathbf{B}/[1_{\mathbf{B}}, 1_{\mathbf{B}}]$. The quotients $\mathbf{A}/\xi_{\mathbf{A}}$ and $\mathbf{A}/[1_{\mathbf{A}}, 1_{\mathbf{A}}]$ will be called the **nonabelian** and **abelian** part (respectively) of $\mathbf{A}$.

To check the existence of an isomorphism between two algebras we will check the isomorphism between their nonabelian parts and abelian parts.

1. Preprocessing

For testing the existence of an isomorphism between two finite algebras from $\mathcal{V}$ we define several invariants of $\mathcal{V}$ that do not depend on a particular member $\mathbf{A} \in \mathcal{V}$, and therefore can be computed in constant time.

- Free algebras $\mathbf{F}_{\mathcal{V}}(2)$ and $\mathbf{F}_{\mathcal{V}}(3)$.

Because the variety $\mathcal{V}$ is congruence permutable it is possible to find out

- the Mal'cev term $p(x, y, z)$
  by simple checking of all elements of $\mathbf{F}_{\mathcal{V}}(3)$.

We also need the following constant values for the variety $\mathcal{V}$:

- s = the number of elements of $\mathcal{V}_{DI}$,
- $k = \max(|\mathbf{K}| \ , \ \mathbf{K} \in \mathcal{V}_{DI})$,
- T is the maximal arity of basic operations in the language of $\mathcal{V}$,
- $z = |\mathbf{F}_{\mathcal{V}}(2)|$.

2. Polynomial time decomposition

Given a finite algebra $\mathbf{A}$ from $\mathcal{V}$, in the first step we decompose $\mathbf{A}$ into $\mathbf{A}/[1_{\mathbf{A}}, 1_{\mathbf{A}}] \times \mathbf{A}/\xi_{\mathbf{A}}$. To do this in polynomial time, all we need to know is the following.

Proposition 1. *There exists a polynomial time algorithm which for any algebra* $\mathbf{A}$ *from* $\mathcal{V}_{fin}$ *computes* $\xi_{\mathbf{A}}$ *and* $[1_{\mathbf{A}}, 1_{\mathbf{A}}]$.

Proof. Let $|A| = n$. From ([4] Th. 14.1) we have that for any algebra $\mathbf{A}$ of $\mathcal{V}$ two elements a, b from $\mathbf{A}$ are congruent modulo the center of $\mathbf{A}$ iff for any basic operations f, all $c = (c_1, \ldots, c_l) \in A^l$ (l is the arity of f) and all binary term operations $r_i (i = 1, \ldots, l)$

$$f(p(r_1(a,b), r_1(b,b), c_1), \ldots, p(r_l(a,b), r_l(b,b), c_l)) =$$

$$p(f(r_1(a,b), \ldots, r_l(a,b)), f(r_1(b,b), \ldots, r_l(b,b)), f(c)).$$

To get the list of all binary term operations we use the free algebra $\mathbf{F}_{\mathcal{V}}(2)$. For every basic operation with the arity l there are n^l possible c's in A^l. For every c we have to consider z^l tuples $(r_1, \ldots, r_l)$. There are n^2 pairs of elements of $\mathbf{A}$. Therefore it is possible to compute $\xi_{\mathbf{A}}$ in $O(n^{T+2})$ steps.

To compute $[1,1]_{\mathbf{A}}$ let us define $\Theta = \{\theta(a,b) : \theta(a,b) \wedge \xi_{\mathbf{A}} = 0_{\mathbf{A}}, a, b \in \mathbf{A}\}$ and $\Phi = \bigvee_{\theta \in \Theta} \theta$. Now we will show that $[1,1]_{\mathbf{A}} = \Phi$. We make use of following properties of $[1,1]_{\mathbf{A}}$: (see [12])

- the congruence $[1_{\mathbf{A}}, 1_{\mathbf{A}}]$ is a neutral element,
- for every congruence ϕ we have $[1_{\mathbf{A}}, 1_{\mathbf{A}}] \wedge \phi = [1, \phi]_{\mathbf{A}}$.

Because $[1_{\mathbf{A}}, 1_{\mathbf{A}}]$ and $\xi_{\mathbf{A}}$ are complementary, by the definition of Φ we have that $[1_{\mathbf{A}}, 1_{\mathbf{A}}] \leq \Phi$. To prove that $\Phi \leq [1_{\mathbf{A}}, 1_{\mathbf{A}}]$ it is enough to show that $\theta \leq [1_{\mathbf{A}}, 1_{\mathbf{A}}]$ for every $\theta \in \Theta$. Suppose that there is a congruence $\theta = \theta(a, b), a \neq b$ such that $\xi_{\mathbf{A}} \wedge \theta = 0_{\mathbf{A}}$ and $\theta \not\leq [1_{\mathbf{A}}, 1_{\mathbf{A}}]$. We have that $[1_{\mathbf{A}}, 1_{\mathbf{A}}] \wedge \theta < \theta$. Then $[1_{\mathbf{A}}, 1_{\mathbf{A}}] \wedge \theta = [1_{\mathbf{A}}, \theta]$ which gives $[1_{\mathbf{A}}, 1_{\mathbf{A}}] \wedge \theta \neq 0_{\mathbf{A}}$ because $\xi_{\mathbf{A}}$ is the largest congruence ϕ satisfying $[1_{\mathbf{A}}, \phi] = 0_{\mathbf{A}}$ and $\xi_{\mathbf{A}} \wedge \theta = 0_{\mathbf{A}}$. Since $[1_{\mathbf{A}}, 1_{\mathbf{A}}]$ is neutral, $([1_{\mathbf{A}}, 1_{\mathbf{A}}] \wedge \theta) \vee \xi_{\mathbf{A}} = \theta \vee \xi_{\mathbf{A}}$. The sublattice consisting of $0_{\mathbf{A}}, \xi_{\mathbf{A}}, \theta, [1_{\mathbf{A}}, 1_{\mathbf{A}}] \wedge \theta$ and $\theta \vee \xi_{\mathbf{A}}$ is isomorphic to $\mathbf{N}_5$ which contradicts the modularity of **ConA**.

Now to compute $[1_{\mathbf{A}}, 1_{\mathbf{A}}] = \bigvee_{\theta \in \Theta} \theta$ note that there are at most n^2 elements in Θ. A principal congruence can be obtained in polynomial time (see [10]), the intersection of two congruences is computable in $O(n^4)$. Therefore in polynomial time we get a list of all elements of Θ. Since $[1_{\mathbf{A}}, 1_{\mathbf{A}}] \wedge \xi_{\mathbf{A}} = 0_{\mathbf{A}}$, we have that $[1_{\mathbf{A}}, 1_{\mathbf{A}}] = \bigvee_{\theta \in \Theta} \theta = \bigcup_{\theta \in \Theta} \theta$. Therefore $[1_{\mathbf{A}}, 1_{\mathbf{A}}]$ can be computed in polynomial time. ∎

Our next step is to describe how in polynomial time we can test the isomorphism between the nonabelian parts of two algebras from $\mathcal{V}_{fin}$. For $\mathbf{A} \in \mathcal{V}_{fin}$ we know that $\mathbf{A}/\xi_{\mathbf{A}}$ is isomorphic to a product of some simple nonabelian members of $\mathcal{V}_{DI}$. The decomposition of $\mathbf{A}/\xi_{\mathbf{A}}$ into a product of members of $\mathcal{V}_{DI}$ is unique (up to permutation of factors) [12]. The only problem to be solved here is to get this decomposition in polynomial time.

Without loss of generality we can assume that $\mathbf{K}_1, \ldots, \mathbf{K}_l$ is a list of all simple nonabelian algebras from $\mathcal{V}_{DI}$. Therefore for any finite algebra $\mathbf{A}$ from $\mathcal{V}$ there exists a unique l-tuple $(\alpha_1^{\mathbf{A}}, \ldots, \alpha_l^{\mathbf{A}})$ of integers such that $\mathbf{A}/\xi_{\mathbf{A}} \cong \mathbf{K}_1^{\alpha_1^{\mathbf{A}}} \times \mathbf{K}_2^{\alpha_2^{\mathbf{A}}} \times \ldots \times \mathbf{K}_l^{\alpha_l^{\mathbf{A}}}$. Therefore for two finite algebras $\mathbf{A}$ and $\mathbf{B}$ from $\mathcal{V}$ to check the isomorphism of $\mathbf{A}/\xi_{\mathbf{A}}$ and $\mathbf{B}/\xi_{\mathbf{B}}$ it is enough to compute and compare the corresponding l-tuples $(\alpha_1^{\mathbf{A}}, \ldots, \alpha_l^{\mathbf{A}})$ and $(\alpha_1^{\mathbf{B}}, \ldots, \alpha_l^{\mathbf{B}})$. The next proposition shows that this can be done in polynomial time.

Proposition 2. *There exists a polynomial time algorithm which for any finite algebra* $\mathbf{A}$ *from* $\mathcal{V}$ *computes an* l*-tuple* $(\alpha_1, \ldots, \alpha_l)$ *such that* $\mathbf{A}/\xi_{\mathbf{A}} \cong \mathbf{K}_1^{\alpha_1} \times \mathbf{K}_2^{\alpha_2} \times \ldots \times \mathbf{K}_l^{\alpha_l}$.

Proof. Let $|A| = n$ and $\mathbf{C} = \mathbf{A}/\xi_{\mathbf{A}}$. It is possible to compute $\mathbf{C}$ in polynomial time. Moreover $|C| \leq n$.

Suppose $\mathbf{C} \cong \mathbf{K}_1^{\alpha_1} \times \mathbf{K}_2^{\alpha_2} \times \ldots \times \mathbf{K}_l^{\alpha_l}$. This decomposition is unique. Since $\mathbf{K}_1, \ldots, \mathbf{K}_l$ are simple, $\mathbf{ConA} \cong \mathbf{2}^m$ and $\mathbf{A}$ is congruence permutable then for each $i = 1, \ldots, l$ there exist exactly α_i maximal (in $\mathbf{ConC} \setminus 1_{\mathbf{C}}$) congruences $\phi_i^1, \ldots, \phi_i^{\alpha_i}$ of $\mathbf{C}$ such that $\mathbf{C}/\phi_i^s \cong \mathbf{K}_i$. Moreover $M = \{\phi_1^1, \ldots, \phi_1^{\alpha_1}, \ldots, \phi_l^1, \ldots, \phi_l^{\alpha_l}\}$ is the set of all maximal congruences of $\mathbf{C}$. For any maximal congruence ψ from M it is possible to compute $\mathbf{C}/\psi$ in polynomial time. In constant time we can find such $\mathbf{K}_i$ that $\mathbf{C}/\psi \cong \mathbf{K}_i$ because $|\mathbf{K}_i| \leq k$. Therefore to compute in polynomial time $(\alpha_1, \ldots, \alpha_l)$ it is enough to compute in polynomial time all maximal congruences of $\mathbf{C}$.

The lattice of congruences of $\mathbf{C}$ is isomorphic to the power $\mathbf{2}^m$ of the two element chain $\mathbf{2}$ (for some m) [12]. Therefore there is one-to-one correspondence between all maximal and atomic congruences. For maximal congruence ϕ there exists exactly one atom θ with $\phi \wedge \theta = 0$ and $\phi \vee \theta = 1$.

To compute all maximal congruences we first create the list L of all nontrivial principal congruences. Because for $a, b \in C$ we can compute in polynomial time the principal congruence $\theta(a, b)$ (see [10] for such an algorithm) we get L in polynomial time. There are at most n^2 elements of L. Next we mark out all the atom congruences. Every congruence is a set containing at most n^2 elements. To compare two such sets we need at most $O(n^4)$ steps. Therefore in time $O(n^6)$ we create the list L' of all minimal elements of L which are also all the atom congruences of $\mathbf{C}$.

For each congruence θ from L' we compute the corresponding maximal congruence ϕ satisfying $\phi \wedge \theta = 0$ and $\phi \vee \theta = 1$. One can see that for $x, y \in \mathbf{C}$, $(x, y) \in \phi$ iff $\theta(x, y) \wedge \theta = 0$. For every x, y we take the congruence $\theta(x, y)$ from the list L. The intersection $\theta(x, y) \wedge \theta$ is obtained in polynomial time. If this is equal to 0, the pair (x, y) belongs to ϕ. There are at most n^2 principal congruences and therefore we get the maximal congruence in polynomial time. Thus we obtain (in polynomial time) the list M of all maximal congruences of $\mathbf{C}$. ∎

Now we show that there exists a polynomial time algorithm which tests the existence of an isomorphism between the abelian parts of two algebras from $\mathcal{V}_{fin}$. For an algebra $\mathbf{A}$ from $\mathcal{V}_{fin}$ the quotient $\mathbf{A}/[1_{\mathbf{A}}, 1_{\mathbf{A}}]$ is isomorphic to a product of abelian members of $\mathcal{V}_{DI}$. Unfortunately the decomposition of $\mathbf{A}/[1_{\mathbf{A}}, 1_{\mathbf{A}}]$ into a product of abelian members of $\mathcal{V}_{DI}$ is not unique. Therefore the testing of existence of the isomorphism cannot be done only by simple decomposition and comparison of factors. In the following we will show how one can manage this situation.

The abelian parts of algebras of $\mathcal{V}_{fin}$ belong to the variety $\mathcal{V}_{ab}$ generated by all abelian members of $\mathcal{V}_{DI}$. The variety $\mathcal{V}_{ab}$ is finitely generated, abelian ([4], Proposition 4.4 and 4.5) and congruence permutable. We will show that the isomorphism testing problem for such a variety is solvable in polynomial time.

Definition 3. Let $\mathbf{R}$ be a finite ring.
An algebra $(M, +, -, 0, (m_r)_{r\in R}, c_1, \ldots, c_v)$ is called an *expanded R-module* if $(M, +, -, 0, (m_r)_{r\in R})$ is an $\mathbf{R}$-module and $c_1, \ldots, c_v$ are constant operations over M.
An expanded $\mathbf{R}$-module with $c_1 = \ldots = c_v = 0$ will be identified with the module $(M, +, -, 0, (m_r)_{r\in R})$.

Proposition 4. *Let $\mathcal{W}$ be a finitely generated congruence permutable abelian variety of algebras of finite type $\mathcal{F}$. There exists a finite ring with unit $\mathbf{R}$ such that for any algebra $\mathbf{A} \in \mathcal{W}$ and $e \in A$ there exists a unitary expanded $\mathbf{R}$-module*

$$\mathbf{M}(\mathbf{A}, e) = (A, +, -, 0^{\mathbf{M}(\mathbf{A},e)}, (m_r^{\mathbf{M}(\mathbf{A},e)})_{r\in R}, (c_g^{\mathbf{M}(\mathbf{A},e)})_{g\in\mathcal{F}})$$

such that $0^{\mathbf{M}(\mathbf{A},e)} = e$ and $\mathbf{M}(\mathbf{A}, e)$ is polynomially equivalent to $\mathbf{A}$. Additionally for any l-ary function symbol $g \in \mathcal{F}$ there exist $r_1^g, \ldots, r_l^g \in R$ such that for any algebra $\mathbf{A}$ in $\mathcal{W}$ we have

$$g^{\mathbf{A}}(x_1, \ldots, x_l) = (\sum_{i=1}^{l} m_{r_i^g}^{\mathbf{M}(\mathbf{A},e)}(x_i)) + c_g^{\mathbf{M}(\mathbf{A},e)}.$$

For an algebra $\mathbf{A}$ *from* $\mathcal{W}_{fin}$ *and* $e \in A$ *the corresponding expanded* $\mathbf{R}$*-module* $\mathbf{M}(\mathbf{A}, e)$ *can be computed in polynomial time.*

Proof. By ([4], pp.108–110) we know that there exists a finite ring with unit $\mathbf{R}$ such that every algebra from $\mathcal{W}$ it is polynomially equivalent to a module over $\mathbf{R}$. The ring $\mathbf{R} = (R, +, *, -, 0, 1)$ is given by $R = \{r \in \mathbf{F}_{\mathcal{V}}(x, y) : \mathcal{V} \models r(x, x) = x\}$ and

$$\begin{aligned} r(x,y) + s(x,y) &= p(r(x,y), y, s(x,y)) \\ r(x,y) * s(x,y) &= r(s(x,y), y) \\ -r(x,y) &= p(y, r(x,y), y) \\ 0 &= y \\ 1 &= x. \end{aligned}$$

Next for an algebra $\mathbf{A} \in \mathcal{W}$ and an element $e \in A$ the operations $+, -, 0^{\mathbf{M}(\mathbf{A},e)}, (m_r^{\mathbf{M}(\mathbf{A},e)})_{r \in R}$ are defined by

$$\begin{aligned} a + b &= p(a, e, b) \\ -a &= p(e, a, e) \\ 0^{\mathbf{M}(\mathbf{A},e)} &= e \\ m_r^{\mathbf{M}(\mathbf{A},e)}(a) &= r(a, e). \end{aligned}$$

The elements r_i^g of $\mathbf{R}$ are defined by

$$\begin{aligned} r_1^g(x,y) &= p(g(x,y,y,\ldots,y), g(y,\ldots,y), y) \\ r_2^g(x,y) &= p(g(y,x,y,\ldots,y), g(y,\ldots,y), y) \\ &\vdots \\ r_l^g(x,y) &= p(g(y,y,\ldots,y,x), g(y,\ldots,y), y). \end{aligned}$$

For an algebra $\mathbf{A}$ from [4] (p. 109) we have

$$g^{\mathbf{A}}(x_1, \ldots, x_l) = (\sum_{i=1}^{l} m_{r_i^g}^{\mathbf{M}(\mathbf{A},e)}(x_i)) + g^{\mathbf{A}}(0^{\mathbf{M}(\mathbf{A},e)}, \ldots, 0^{\mathbf{M}(\mathbf{A},e)}).$$

The ring can by computed in preprocessing. For every finite algebra $\mathbf{A}$ the corresponding module is computable in time $O(|\mathbf{A}|^2)$.

We define the constants by putting

$$c_g^{\mathbf{M}(\mathbf{A},e)} = g^{\mathbf{A}}(0^{\mathbf{M}(\mathbf{A},e)}, \dots, 0^{\mathbf{M}(\mathbf{A},e)})$$

for every basic operation symbol $g \in \mathcal{F}$. They are computable in constant time. One can see that we can compute the expanded $\mathbf{R}$- module $M(\mathbf{A}, e)$ in polynomial time. ∎

From now on for any expanded $\mathbf{R}$-module

$$\mathbf{M} = (M, +, -, 0, (m_r)_{r\in R}, c_1, \dots, c_v)$$

we will use the notation rx for $m_r^{\mathbf{M}}(x)$ if it is clear from context.

For a finitely generated, congruence permutable abelian variety $\mathcal{W}$ of finite type $\mathcal{F}$ we form a ring $\mathbf{R}$ like in Proposition 4 and define the concept of $\mathcal{W}$-expanded $\mathbf{R}$-module to be the algebra of the form $\mathbf{M}(\mathbf{A}, e)$ for $\mathbf{A} \in \mathcal{W}$ and $e \in A$.

Corollary 5. *Let $\mathcal{W}$ be a finitely generated congruence permutable abelian variety and $\mathbf{R}$ be the corresponding ring as described in Proposition 4. Then two algebras $\mathbf{A}$ and $\mathbf{B}$ from $\mathcal{W}$ are isomorphic iff there exist elements $a \in A$ and $b \in B$ such that the $\mathcal{W}$-expanded $\mathbf{R}$-modules $\mathbf{M}(\mathbf{A}, a)$ and $\mathbf{M}(\mathbf{B}, b)$ are isomorphic.* ∎

Given a directly representable variety $\mathcal{V}$ we compute its subvariety $\mathcal{V}_{ab}$ and a sublist $\mathbf{A}_1, \dots, \mathbf{A}_q$ of all abelian members of $\mathcal{V}_{DI}$. Next we compute the free algebra $\mathbf{F}_{\mathcal{V}_{ab}}(2)$ ($\cong \mathbf{F}_{\mathcal{V}}(2)/[1,1]$) and the ring $\mathbf{R}$ for $\mathcal{V}_{ab}$. Then for each $\mathbf{A}_i$ $(i = 1, \dots q)$ and every $a \in A_i$ we compute the $\mathcal{V}_{ab}$-expanded $\mathbf{R}$-module $\mathbf{M}_i^a = \mathbf{M}(\mathbf{A}_i, a)$ as described in Proposition 4. All of the above computation can be done in constant time.

One can prove that the class $\mathcal{W}$ of all $\mathcal{V}_{ab}$-expanded $\mathbf{R}$-modules is a variety generated by the set $\{\mathbf{M}_i^a \,:\, i = 1, \dots, q, \text{ and } a \in A_i\}$. Additionally

$\mathcal{W}$ is directly representable and $\{\mathbf{M}_i^a \ : \ i = 1, \ldots, q, \text{ and } a \in A_i\}$ is a set of all (up to isomorphism) finite directly indecomposable members of $\mathcal{W}$.

Since for every finite algebra $\mathbf{A}$ from $\mathcal{V}_{ab}$ and $a \in A$ the corresponding $\mathcal{V}_{ab}$-expanded $\mathbf{R}$-module $\mathbf{M}(\mathbf{A}, a)$ can be computed in polynomial time (Proposition 4) it remains to show that the isomorphism testing problem for directly representable variety of unitary expanded modules over a fixed finite ring with unit $\mathbf{R}$ is solvable in polynomial time.

From now on let $\mathcal{M}$ be a directly representable variety of unitary expanded modules over a fixed finite ring with unit $\mathbf{R}$. Let $\mathcal{M}_{DI} = \{\mathbf{M}_1, \ldots, \mathbf{M}_r\}$ denote a fixed list of all (up to isomorphism) finite directly indecomposable members of $\mathcal{M}$.

We will use the following Lovasz's cancellation theorem:

Theorem 6. *For finite algebras $\mathbf{P}, \mathbf{Q}, \mathbf{C}$ with $\mathbf{P} \times \mathbf{C} \cong \mathbf{Q} \times \mathbf{C}$ one has $\mathbf{P} \cong \mathbf{Q}$ if $\mathbf{C}$ has a one-element subalgebra (see e.g. [13] Theorem 5.23 and Cor. 3).* ∎

Definition 7. A module $\mathbf{N}$ is a *retract* of a module $\mathbf{M}$ iff there are two homomorphisms $h : \mathbf{N} \longrightarrow \mathbf{M}$ and $f : \mathbf{M} \longrightarrow \mathbf{N}$ such that $f \circ h = id_{\mathbf{N}}$. In this case f will be called a *retraction*.

Proposition 8. *A module $\mathbf{N}$ is a retract of a module $\mathbf{M}$ iff there is a submodule $\mathbf{J}$ of $\mathbf{M}$ with $\mathbf{J} \cong \mathbf{N}$ and $\mathbf{M} \cong \mathbf{J} \times \mathbf{M}/\mathbf{J}$.*

Proof. First let $\mathbf{J}$ be a submodule of $\mathbf{M}$ with $\mathbf{M} \cong \mathbf{J} \times \mathbf{M}/\mathbf{J}$ and $g : \mathbf{J} \longrightarrow \mathbf{N}$ be an isomorphism. Define $h : \mathbf{N} \longrightarrow \mathbf{J} \times \mathbf{M}/\mathbf{J}$ by $h(x) = (g^{-1}(x), 0)$. Then for $f = g \circ \pi_{\mathbf{J}} : \mathbf{J} \times \mathbf{M}/\mathbf{J} \longrightarrow \mathbf{N}$ we have $f \circ h = id_{\mathbf{N}}$. This means that $\mathbf{N}$ is a retract of $\mathbf{M}$.

Conversely, if $f : \mathbf{M} \longrightarrow \mathbf{N}$ is a retraction and $h : \mathbf{N} \longrightarrow \mathbf{M}$ is the corresponding homomorphism from Definition 7 then by putting $\mathbf{J} = h(\mathbf{N})$ we have $\mathbf{J} \cong \mathbf{N}$. Moreover h and $f|_{\mathbf{J}}$ are isomorphisms between $\mathbf{N}$ and $\mathbf{J}$, $h \circ f|_{\mathbf{J}} = id|_{\mathbf{J}}$. We define $g : \mathbf{M} \longrightarrow \mathbf{J} \times \mathbf{M}/\mathbf{J}$:

$$g(d) = \langle (h \circ f)(d), d/\mathbf{J} \rangle.$$

which is a required isomorphism. Indeed, if $(h \circ f)(d_1) = (h \circ f)(d_2)$ and $d_1/\mathbf{J} = d_2/\mathbf{J}$ then $d_1 - d_2 \in \mathbf{J}$ and $0 = (h \circ f)(d_1 - d_2) = d_1 - d_2$, so $d_1 = d_2$, i.e. we get injectivity.

Now, for surjectivity, take $\langle a, d/\mathbf{J}\rangle \in \mathbf{J} \times \mathbf{M}/\mathbf{J}$. Then $a + d - (h \circ f)(d)$ is mapped onto $\langle (h \circ f)(a + d - (h \circ f)(d)), (a + d - (h \circ f)(d))/\mathbf{J}\rangle = \langle a, d/\mathbf{J}\rangle$ since $h \circ f|_{\mathbf{J}} = id|_{\mathbf{J}}$ and $a, (h \circ f)(d) \in \mathbf{J}$. ∎

For an expanded $\mathbf{R}$-module $\mathbf{M}$ define $\mathbf{M}_\nabla$, the linearization on $\mathbf{M}$, by putting $\mathbf{M}_\nabla = \mathbf{M}^2/\triangle_{1,1}$ where $\triangle_{1,1}$ is the congruence of $\mathbf{M}^2$ generated by the set $\{(\ (a, a), (b, b)\ ) :\ a, b \in M\}$.

By $\mathbf{M}_0$ we mean an expanded $\mathbf{R}$-module built from the expanded $\mathbf{R}$-module $\mathbf{M}$ by replacing of all constant operations by $0^{\mathbf{M}}$.

Fact 9. *For an expanded* $\mathbf{R}$*-module* $\mathbf{M}$ *we have* $\mathbf{M}_\nabla \cong \mathbf{M}_0$.

Proof. For the proof notice that the function $h : \mathbf{M}^2 \longrightarrow \mathbf{M}_0$ given by $h(a, b) = a - b$ is an epimorphism with $ker(h) = \nabla$. ∎

Proposition 10. *For an expanded* $\mathbf{R}$*-module* $\mathbf{M}$ *we have*

(a) *If* $\mathbf{M}$ *belongs to a variety* $\mathcal{V}$ *then* $\mathbf{M}_0$ *belongs to* $\mathcal{V}$.

(b) *if* $\mathbf{M}$ *is directly indecomposable so is* $\mathbf{M}_0$,

(c) $\mathbf{M} \times \mathbf{M}_0 \cong \mathbf{M} \times \mathbf{M}$.

Proof. **(a)** follows from Fact 9. For **(b)**, notice that $\mathbf{M}_0$ is an expanded $\mathbf{R}$-module obtained from $\mathbf{M}$ by replacing all the additional constant operations by $0^{\mathbf{M}}$ and therefore $\mathbf{ConM}_0 = \mathbf{ConM}$. **(c)** is Prop. 9.18(ii) of [4]. ∎

Lemma 11. *Let* $\mathbf{M}$ *and* $\mathbf{J}$ *be expanded* $\mathbf{R}$*-modules. Then* $\mathbf{J}$ *is a factor of* $\mathbf{M}$ *iff there exists a retraction* $f : \mathbf{M}_0 \longrightarrow \mathbf{J}_0$ *that preserves all additional constant operations, i.e.* $f(c_i^{\mathbf{M}}) = c_i^{\mathbf{J}},\ i = 1, \ldots, v$.

Proof. Let $g : \mathbf{M} \longrightarrow \mathbf{N} \times \mathbf{J}$ be an isomorphism. Then obviously $\mathbf{M}_0 \cong \mathbf{N}_0 \times \mathbf{J}_0$. Take $f = \pi_{\mathbf{J}_0} \circ g\ : \mathbf{M}_0 \longrightarrow \mathbf{J}_0$. Now define $h\ :\ \mathbf{J}_0 \longrightarrow \mathbf{M}_0$

by $h(a) = g^{-1}(0, a)$. We have $f \circ h = id_J$ and therefore f is a retraction. One can see that f preserves all additional constant operations.
Conversely, let $f : \mathbf{M}_0 \longrightarrow \mathbf{J}_0$ be a retraction that preserves all additional constant operations. By Proposition 8, and by proof of Proposition 8, there is a submodule $\mathbf{I}$ of $\mathbf{M}_0$ such that $f|_{\mathbf{I}} : \mathbf{I} \longrightarrow \mathbf{J}_0$ is an isomorphism and $\mathbf{M}_0 \cong \mathbf{I} \times \mathbf{M}_0/\mathbf{I}$. Take $\overline{\mathbf{N}} = \mathbf{M}_0/\mathbf{I}$ then $\mathbf{M}_0 \cong \overline{\mathbf{N}} \times \mathbf{J}_0$. Similarly as in the proof of Proposition 8 one can see that $h : \mathbf{M}_0 \longrightarrow \overline{\mathbf{N}} \times \mathbf{J}_0$ defined by $h(d) = (d/\mathbf{I}, f(d))$ is an isomorphism. For $c_i^{\mathbf{M}} \in M$, $i = 1, \ldots, v$, $h(c_i^{\mathbf{M}}) = (c_i^{\mathbf{M}}/\mathbf{I}, c_i^{\mathbf{J}})$. Now, put $\mathbf{N} = (\overline{N}, +, -, 0^{\overline{\mathbf{N}}}, (m_r^{\overline{\mathbf{N}}})_{r \in R}, c_1^{\mathbf{N}}, \ldots, c_v^{\mathbf{N}})$ with $c_i^{\mathbf{N}} = c_i^{\mathbf{M}}/\mathbf{I}$. It is clear that $\mathbf{M} \cong \mathbf{N} \times \mathbf{J}$. ∎

Proposition 12. *Let* $\mathbf{D}$ *be a finite unitary module over a finite ring with unit* $\mathbf{R}$ *and* $|D| = n \geq 2$. *It is possible to produce, in* $pol(n)$*-time, a set* G *of generators of* $\mathbf{D}$ *with* $|G| \leq \log_2(n)$.

Proof. First note that for $x \in D$ we can get, in constant time, the submodule $\langle x \rangle$ of $\mathbf{D}$ generated by x, $\langle x \rangle = \{rx \ : \ r \in R\}$. For two submodules $\mathbf{X}, \mathbf{Y}$ of $\mathbf{D}$ the least module containing $\mathbf{X}$ and $\mathbf{Y}$ is the module $\mathbf{X} \vee \mathbf{Y} = \{x + y, \ x \in X, \ y \in Y\}$. Thus we can compute $\mathbf{X} \vee \mathbf{Y}$ in $pol(n)$-time.
It is easy to check that for a submodule $\mathbf{Z}$ of $\mathbf{D}$ and $x \notin Z$

$$|\mathbf{Z} \vee \langle x \rangle| \geq 2|\mathbf{Z}|. \quad (1)$$

The following algorithm produces the required set of generators G.

$Z := \{0\}$ $\quad G := \emptyset$
`while` $D \setminus Z \neq \emptyset$ `do`
`begin`
`pick` $x \in D \setminus Z$
$G := G \cup \{x\}$
$\mathbf{Z} := \mathbf{Z} \vee \langle x \rangle$
`end`

From (1) we have that the loop in the above algorithm will be executed at most $\log_2(n)$ times, and therefore $|G| \leq \log_2(n)$. All sets in the algorithm can be obtained in $pol(n)$-time, so that the whole algorithm will run in $pol(n)$-time. ∎

Lemma 13. *For any fixed expanded* $\mathbf{R}$*-module* $\mathbf{J}$ *there is an algorithm that checks, in* $pol(|M|)$*-time, whether* $\mathbf{J}$ *is a direct factor of an expanded* $\mathbf{R}$*-module* $\mathbf{M}$ *and, if it is so, the algorithm produces an expanded* $\mathbf{R}$*-module* $\mathbf{N}$ *with* $\mathbf{M} \cong \mathbf{N} \times \mathbf{J}$.

Proof. Let $|M| = n$, $|J| = c$ and $|R| = r$. In constant time we compute $\mathbf{M}_0$ and $\mathbf{J}_0$. By Proposition 12, we can find a set G of generators of $\mathbf{M}_0$ with $|G| \leq \log_2(n)$ in $pol(n)$-time.

There are $c^{\log_2(n)} = n^{\log_2(c)}$ possible functions $f : G \longrightarrow J_0$. Note that a function $f : G \longrightarrow J_0$ can be extended to a homomorphism $\bar{f} : \mathbf{M}_0 \longrightarrow \mathbf{J}_0$ iff

$$\forall\, r_1, \ldots, r_k \in R \quad \sum_{i=1}^{k} r_i g_i = 0 \Rightarrow \sum_{i=1}^{k} r_i f(g_i) = 0. \quad (2)$$

where $G = \{g_1, \ldots, g_k\}$.

Thus to check if a function $f : G \longrightarrow \mathbf{J}_0$ can be extended to a homomorphism we have to consider $r^{|G|} \leq r^{\log_2(n)} = n^{\log_2(r)}$ sequences $\langle r_1, \ldots, r_{|G|} \rangle \in R^{|G|}$ while checking (2).

The elements of $\mathbf{M}_0$ are of the form $\sum_{i=1}^{k} r_i g_i$, for some $r_1, \ldots, r_k \in R$. Therefore after checking that f is extendable, we produce the homomorphim $\bar{f}$ in time in time $O(n^{\log_2(r)})$ ($r^{|G|} \leq r^{\log_2(n)} = n^{\log_2(r)}$). Next, we check whether the extension is a retraction which fulfills the condition from Lemma 11. In constant time we test whether $\bar{f}(c_i^{\mathbf{M}}) = c_i^{\mathbf{J}}$, $i = 1, \ldots, v$. There are at most n^c functions of the form $h : J_0 \longrightarrow M_0$. In constant time $(r \cdot c)^2$, we can check if h is a homomorphism. For all such homomorphisms h we test in constant time if $\bar{f} \circ h = id_{\mathbf{J}_0}$.
We do this for all mappings $f : G \longrightarrow J_0$. Thus in $pol(n)$-time we can check, with the use of Lemma 11, whether $\mathbf{J}$ is a factor of $\mathbf{M}$. If $\mathbf{M} \cong \mathbf{N} \times \mathbf{J}$ we compute $\mathbf{N}$ like in the proof of Lemma 11 in $pol(n)$-time. ∎

Lemma 14. *Let $\mathcal{M}$ be a directly representable variety of expanded modules, $\mathcal{M}_{DI} = \{\mathbf{M}_1, \ldots, \mathbf{M}_r\}$ is the set of all (up to isomorphism) finite directly indecomposable members of $\mathcal{M}$. The isomorphism problem for $\mathcal{M}$ is solvable in polynomial time.*

Proof. Let $\mathbf{M}_1, \ldots, \mathbf{M}_m$ be all the expanded nontrivial modules from $\mathcal{M}_{DI}$ with one element expanded $\mathbf{R}$-submodule, i.e. $\mathbf{M}_i \cong (\mathbf{M}_i)_0$. Note that for every expanded module $\mathbf{M}_j$ with $m+1 \leq j \leq r$ there exists $i \in \{1, \ldots, m\}$ such that $(\mathbf{M}_j)_0 \cong \mathbf{M}_i$ (Proposition 10 (**a**),(**b**)). For an expanded module $\mathbf{M}$ from $\mathcal{M}$, with $|M| = n$, we build a sequence of integers $a_1^{\mathbf{M}}, \ldots, a_m^{\mathbf{M}}$ and an expanded module $\mathbf{D}(\mathbf{M})$ such that $\mathbf{M} \cong \mathbf{M}_1^{a_1^{\mathbf{M}}} \times \ldots \times \mathbf{M}_m^{a_m^{\mathbf{M}}} \times \mathbf{D}(\mathbf{M})$ and $|D(\mathbf{M})| \leq \prod_{i=m+1}^{r} |M_i|$.

```
For all i = 1...m     a_i^M := 0
for i := 1 to m
    while M_i is a factor of M
          begin
          a_i^M := a_i^M + 1
          M := N  for N such that M ≅ N × M_i  (Lemma 13)
          end
D(M) := M
```

The `while` loop is executed at most n times. From Lemma 13 we know that this loop is executed in $pol(n)$-time. Thus the sequence $a_1^{\mathbf{M}}, \ldots, a_m^{\mathbf{M}}$ and the module $\mathbf{D}(\mathbf{M})$ can be computed in $pol(n)$-time.

By Proposition 10(c) we know that $\mathbf{D}(\mathbf{M}) \cong \mathbf{M}_{m+1}^{b_{m+1}} \times \ldots \times \mathbf{M}_r^{b_r}$ with $b_i \leq 1$ (the b_i's we can compute in constant time). Thus $|D(\mathbf{M})| \leq |M_{m+1}| \cdot |M_{m+2}| \cdot \ldots \cdot |M_r|$.

From Lovasz's cancellation theorem we have that two expanded modules $\mathbf{M}$ and $\mathbf{N}$ are isomorphic iff $(a_1^{\mathbf{M}}, \ldots, a_m^{\mathbf{M}}) = (a_1^{\mathbf{N}}, \ldots, a_m^{\mathbf{N}})$ and $\mathbf{D}(\mathbf{M}) \cong \mathbf{D}(\mathbf{N})$. The existence of an isomorphism between $\mathbf{D}(\mathbf{M})$ and $\mathbf{D}(\mathbf{N})$ can be

checked in constant time. Thus the isomorphism problem for $\mathcal{M}$ is solvable in polynomial time. ∎

3. Main theorem

Now we are able to prove

Theorem 15. *The isomorphism testing problem for a directly representable variety $\mathcal{V}$ is solvable in polynomial time.*

Proof. First for the variety $\mathcal{V}$ in the preprocessing stage we compute free algebras $\mathbf{F}_{\mathcal{V}}(2)$, $\mathbf{F}_{\mathcal{V}}(3)$ and $\mathbf{F}_{\mathcal{V}_{ab}}(2)$ ($\cong \mathbf{F}_{\mathcal{V}}(2)/[1,1]$). Next we produce the Mal'cev term $p(x,y,z)$ simply by checking all elements of $\mathbf{F}_{\mathcal{V}}(3)$. Then we compute the ring $\mathbf{R}$ as described in Proposition 4.

We divide the list $\mathcal{V}_{DI}$ into two parts:

1. $\mathcal{K} = \{\mathbf{K}_1 \dots \mathbf{K}_l\}$ of all nonabelian simple members of $\mathcal{V}_{DI}$,
2. $\mathcal{A} = \{\mathbf{A}_1, \dots, \mathbf{A}_q\}$ of all abelian members of $\mathcal{V}_{DI}$.

Next, for all algebras $\mathbf{A}$ from $\mathcal{A}$ and for all $a \in A$ we compute the list $\mathcal{M}_{DI} = \{\mathbf{M}_1, \dots, \mathbf{M}_r\}$ of corresponding $\mathcal{V}_{ab}$-expanded $\mathbf{R}$-modules of the form $\mathbf{M}(\mathbf{A}, a)$ (Proposition 4). We can assume that $\{\mathbf{M}_1, \dots, \mathbf{M}_m\}$ is the list of all nontrivial members of $\mathcal{M}_{DI}$ with one element expanded $\mathbf{R}$-submodule.

All the above described objects we can compute in constant time.

For a given algebra $\mathbf{A} \in \mathcal{V}_{fin}$ we compute in polynomial time $\xi_{\mathbf{A}}, [1_{\mathbf{A}}, 1_{\mathbf{A}}]$, (Proposition 1) and the corresponding quotient algebras. Next, we compute in polynomial time the numbers $\alpha_1^{\mathbf{A}}, \dots, \alpha_l^{\mathbf{A}}$ such that $\mathbf{A}/\xi_{\mathbf{A}} \cong \mathbf{K}_1^{\alpha_1^{\mathbf{A}}} \times \ldots \times \mathbf{K}_l^{\alpha_l^{\mathbf{A}}}$ (Proposition 2).

For $\mathbf{A}' = \mathbf{A}/[1_{\mathbf{A}}, 1_{\mathbf{A}}]$ and all $a \in A'$ we compute in polynomial time of $|A|$ the corresponding $\mathcal{V}_{ab}$-expanded $\mathbf{R}$-modules $\mathbf{M}(\mathbf{A}', a)$. Then we compute (like in Lemma 14) the list of numbers $\beta_1^{\mathbf{A},a}, \dots, \beta_r^{\mathbf{A},a}$ such that $\mathbf{M}(\mathbf{A}', a) \cong \mathbf{M}_1^{\beta_1^{\mathbf{A},a}} \times \ldots \times \mathbf{M}_r^{\beta_r^{\mathbf{A},a}}$ and for $i = m+1, \dots, r$, $\beta_i^{\mathbf{A},a} \leq 1$.

Let $\mathbf{A}, \mathbf{B} \in \mathcal{V}_{fin}$. If we test the existence of an isomorphism between $\mathbf{A}$ and $\mathbf{B}$ we can assume that $|A| = |B|$. As above we compute in polynomial time two lists

$$\alpha_1^{\mathbf{A}}, \ldots, \alpha_l^{\mathbf{A}}, \langle \beta_1^{\mathbf{A},a}, \ldots, \beta_r^{\mathbf{A},a} \rangle_{a \in A}$$

and

$$\alpha_1^{\mathbf{B}}, \ldots, \alpha_l^{\mathbf{B}}, \langle \beta_1^{\mathbf{B},b}, \ldots, \beta_r^{\mathbf{B},b} \rangle_{b \in B}.$$

The algebras $\mathbf{A}$ and $\mathbf{B}$ are isomorphic iff $\alpha_i^{\mathbf{A}} = \alpha_i^{\mathbf{B}}$ for $i = 1, \ldots, l$ and if there exist $a \in A$ and $b \in B$ such that $\beta_j^{\mathbf{A},\mathbf{a}} = \beta_j^{\mathbf{B},\mathbf{b}}$ for $j = 1, \ldots, m$ and $\mathbf{M}_{m+1}^{\beta_{m+1}^{\mathbf{A},a}} \times \ldots \times \mathbf{M}_r^{\beta_r^{\mathbf{A},a}} \cong \mathbf{M}_{m+1}^{\beta_{m+1}^{\mathbf{B},b}} \times \ldots \times \mathbf{M}_r^{\beta_r^{\mathbf{B},b}}$ (Lemma 14). Since the size of $\mathbf{M}_{m+1}^{\beta_{m+1}^{\mathbf{A},a}} \times \ldots \times \mathbf{M}_r^{\beta_r^{\mathbf{A},a}}$ is bounded by $k \cdot s$ (i.e. independently of $\mathbf{A}$) we can check the existence of an isomorphism between $\mathbf{A}$ and $\mathbf{B}$ in polynomial time. ■

We started with an additional assumption that together with a directly representable variety $\mathcal{V}$ a list $\mathcal{V}_{DI}$ is given, or in other words that $\mathcal{V}$ is presented by listing all its (up to isomorphism) directly indecomposable algebras. In general $\mathcal{V}$ can be presented by arbitrary finite set $\mathcal{K}$ of finite algebras that generate $\mathcal{V}$. The problem whether it is possible to pass from $\mathcal{K}$ to $\mathcal{V}_{DI}$ is equivalent to the following.

Problem 16. *Let* $\mathbf{A}$ *be a finite algebra generating a directly representable variety* $\mathcal{V}$. *Is the function* $f(|\mathbf{A}|) = max\{|\mathbf{D}| : \mathbf{D} \in \mathcal{V}_{DI}(\mathbf{A})\}$ *recursive?*

References

[1] Babai L., Kantor W.M. and Luks E.M., *Computational complexity and the classification of finite simple groups,* 24th IEEE Symposium on Foundations of Comp.Sci., (1983), 162–171.

[2] Booth K.S., *Isomorphism testing for graphs, semigroups, and finite automata are polynomially equivalent problems,* SIAM J. of Computing, **7**(1978), 273–279.

[3] Burris S. and Sankappanavar H.P., *A Course in Universal Algebra*, Springer Verlag 1981.

[4] Freese R. and McKenzie R., *Commutator Theory for Congruence Modular Varieties.* London Math. Soc. LNS ♯ 125, Cambridge University Press, 1987.

[5] Garey M.R. and Johnson D.S., *Computers and Intractability. A Guide to the Theory of NP–Completeness*, W.H.Freeman & Co., 1979.

[6] Goralčíková A., Goralčík P. and Koubek V., *A boundary of isomorphism completeness in the lattice of semigroup pseudovarieties,* Proc. ICALP'82, Lect.Notes in Comp.Sci., 140, Springer Verlag 1982, pp.292–299.

[7] Gorazd T., Idziak P.M., *The isomorphism problem for varieties generated by a two-element algebra*, Algebra Universalis, **34** (1995) 430-439.

[8] Hedrlin Z. and Pultr A., *On full embeddings of categories of algebras,* Illinois J. of Math., **10**(1966), 392–406.

[9] Kőbler J., Schőning U. and Torán J., *The Graph Isomorphism Problem: Its Structural Complexity*, Progress in Theoretical Computer Science, Birkhauser 1993.

[10] Kozen D., *Complexity of finitely presented algebras*, Proc. 9^{th} Symposium STOC (1977), 164-177.

[11] Kučera L. and Trnková V., *Isomorphism testing of unary algebras*, SIAM J. of Computing, **17**(1988), 673-686.

[12] McKenzie R.N., *Narrowness implies uniformity*, Algebra Universalis, **15** (1982) 67-87.

[13] McKenzie R.N., McNulty G.F., and Taylor W.F., *Algebras, Lattices, and Varieties.* Vol. I. Wadsworth and Brooks/Cole, Mathematics Series, 1987.

[14] Valeriote M. and Willard R., unpublished.

[15] Willard R., unpublished.

Computer Science Department
Jagiellonian University
Krakow
Poland

e-mail: uigorazd@cyf-kr.edu.pl