2) $t_1^- = (\lambda x^B \mathfrak{s}^-, v^-), t_2^- = \mathfrak{s}_{x^B}^- [v^-]$, then either $x^B \mathfrak{s}, v) \underset{BC}{\equiv} \mathfrak{s}_{x^B}[v] = t_2$, or $t_1 = |\mu x^B \mathfrak{s}, v| \underset{BC}{\equiv} \mathfrak{s}_{x^B}[v] =$

ecision algorithm is given in [3] for $\underset{\mathfrak{s}MC}{\equiv}$. We obtain from it and Theorem 4.2 a decision algorithm for $\underset{BC}{\equiv}$. Moreover, from Theorem 4.2 and the coherence theorem for c morphisms in $\mathfrak{s}MC$ categories, we deduce the coherence theorem for canonical morphisms categories.

THEOREM 4.3. (Coherence). If f, f': A → B are canonical morphisms and the sequence A → B is I-balanced, then f = f'.

LITERATURE CITED

1. J. Lambek, "Deductive systems and categories. II," Lect. Notes Math., 86, 76-122 (1969).
2. A. A. Babaev, "Equality of canonical morphisms in closed categories. I," Izv. Akad. Nauk Az. SSR, Ser. Fiz.-Tekh. Mat., 6 (1980).
3. A. A. Babaev, "Equality of morphisms in closed categories. II," Izv. Akad. Nauk Az. SSR, Ser. Fiz.-Tekh. Mat., 6 (1980).
4. G. E. Mintz, "Closed categories and proof theory," Zap. Nauchn. Sem. Leningr. Otd. Mat. Inst. Akad. Nauk SSSR, 68, 88-114 (1977).
5. G. E. Mintz, "Category theory and proof theory," in: Contemporary Questions of Logic and Scientific Methodology [in Russian], Kiev (1980), pp. 252-278.
6. C. Mann, "The connection between equivalence of proofs and Cartesian closed categories," Proc. London Math. Soc., 31, No. 3, 289-310 (1975).
7. A. A. Babaev, S. V. Solov'ev, "A coherence theorem for canonical morphisms in Cartesian closed categories," Zap. Nauchn. Sem. Leningr. Otd. Mat. Inst. Akad. Nauk SSSR, 88, 3-29 (1979).
8. G. Kelly and S. MacLane, "Coherence in closed categories," J. Pure Appl. Algebra, 1, No. 1, 97-140 (1971).

COMPLEXITY OF "WILD" MATRIX PROBLEMS AND OF ISOMORPHISM OF ALGEBRAS AND GRAPHS

D. Yu. Grigor'ev

UDC 519.5+512.46

It is shown that isomorphism of semisimple algebras over an algebraically closed field is recognized in polynomial time. The polynomial equivalence of isomorphism of graphs and isomorphism of algebras (over an algebraically closed field) with zero square of the radical and commutative quotient modulo the radical is proved. A series of problems about the complexity of matrix problems and isomorphism of algebras are posed.

In the present article, we pose a series of complexity problems of algebraic origin and indicate their interrelations with the complexity of recognition of isomorphism of graphs. In addition, we elucidate the complexity of recognition of isomorphism for two classes of algebras (see the proposition and the theorem).

1. It has been shown by the efforts of many Soviet mathematicians that, in the first place, many problems about the classification of modules (over a given algebra) are reduced to the so-called matrix problems, and these, in their turn, are classified into three types of problems: finite, tame, and wild, such that all the problems of one type are equivalent to each other in a definite sense (one of the first articles on this theme was [1]; further, see the series of articles in [2] and the recent articles of L. A. Nazarova, A. V. Roiter, Yu. A. Drozd, A. V. Yakovlev, and others). We can take the following problems as the model

Translated from Zapiski Nauchnykh Seminarov Leningradskogo Otdeleniya Matematicheskogo Instituta im. V. A. Steklova AN SSSR, Vol. 105, pp. 10-16, 1981. Original article submitted September 16, 1980.

problems of each type: classification of the matrices up to left and right multiplication by nonsingular matrices (finite type), classification of matrices over an algebraically closed field up to similarity (tame type), and classification of pairs of matrices up to similarity (wild type).

Let us turn to the algorithmic formulations of the matrix problems. In this connection, we consider matrices with rational elements, although we can take the elements from other "well-defined" fields. The algorithmic formulation of the model finite problem lies in P, since it is sufficient to compute the rank to determine the equivalence of matrices in this case, which can be done in polynomial time, using, e.g., [3] or [4]. Let us at once observe that the reductions of matrix problems to the above-mentioned models, known to the author, for all the three types are, in particular, P-equivalences. The algorithmic formulation of the tame problem also lies in P, since coincidence of the Jordan forms of two matrices can be verified in polynomial time (see [4], [5], Appendix A] and also [6], in which it has actually been shown that another tame problem — a problem about a matrix bundle, is solvable in polynomial time).

The above-formulated wild problem about the classification of pairs of matrices is regarded as a standard of difficulty in linear algebra. It is interesting to elucidate whether it is complex in the algorithmic sense. The algorithmic formulation of the standard wild problem is as follows: to elucidate whether two pairs of matrices (A, B) and (C, D) are equivalent, i.e., does there exist an invertible matrix X such that $AX = XC$ and $BX = XD$? The last two equations can be considered as a linear system in the coefficients $\{x_{ij}\}$ of the matrix X, its solution in the matrix form is found, and then we arrive at the following algorithmic problem: Does there exist a nonsingular matrix in the given linear variety of matrices? It is clear that this problem lies in NP, since the last problem is equivalent to the problem of nonidentity of the determinant of the parametric matrix. Does this problem lie in P?

2. Side by side with the problem about isomorphism of modules over a given algebra, which, as observed above, reduces to a matrix problem, there also arises the problem of isomorphism of associative algebras.

We assume the algebras to be given by their integral structure tensors. For simplicity, we consider finite-dimensional algebras with identity over an algebraically closed field F (in order not to be occupied by the problems of representation of elements and of carrying out the operations in the field, we set $F = \mathbb{C}$ in the proofs). In this case, the quotient A/R of an algebra A modulo its Jacobson radial R is a direct sum $\oplus_i Fk_i$ of the algebras of the $k_i \times k_i$-matrices over F by the Wedderburn theorem (see [7, 8]). If R = 0, then the algebra A is said to be semisimple.

Proposition 1. Isomorphism of semisimple algebras (over an algebraically closed field) is recognized in polynomial time.

Proof. It is sufficient to find a set $\{K_i\}$ in polynomial time such that the semisimple algebra $A = \oplus_i Fk_i$. We carry out the proof by induction on $\dim_F A$.

At first, we find the center C(A) of the algebra A by solving the system of the linear equations, each of which means commutation with an element of the basis of A over F. Let $\dim C(A) > 1$ and $\mu \cdot 1 \neq a \in C(A)$ for any $\mu \in F$. Let us consider a as a linear operator (by means of left multiplication) on A and find a root λ of the characteristic (integral) polynomial $\chi_a = \det(a - \lambda \cdot 1)$. The coefficients of the characteristic polynomial are computed in polynomial time on the basis of [4, 9].

The algebraic number λ takes part in the computations as a symbol that satisfies the equation $\chi_a(\lambda) = 0$. Getting a few steps ahead, let us observe that here, as in other situations where algebraic numbers occur in computations, it is convenient to use the following device. We temporarily assume χ_a to be irreducible (as a preliminary, having gotten rid of the multiple factors by means of the derivative). If a certain number λ_1 — a root of the polynomial f — also occurs in the computations and if the greatest common divisor (χ_a, f) is nontrivial, then we assume λ to be a root of the (temporarily irreducible) polynomial $\chi_a/(\chi_a, f)$ and start the procedure afresh. It is obvious that the number of steps of the algorithm here remain polynomial, since the degrees of the considered polynomials are lowered. But if $\deg \times (\chi_a, f)$, then, e.g., the set $deg(\chi_a, f)$ where $0 \leqslant i < \deg \chi_a$ and $0 \leqslant j < \deg f$, is a generating system of the field $\mathbb{Q}(\lambda, \lambda_1) = \mathbb{Q}[x, y]/(\chi_a(x), f(y))$ (reasoning as above, we temporarily assume that this ring is a field) over $\mathbb{Q}$, and the computations can be carried out in this system.

In particular, if it is required to elucidate the problem of equality to zero of the element $g(\lambda_1)$, where the polynomial $g \in (\lambda)[x]$, then we find the common divisor (f, g), and if $\deg(f, g) = 0$, then $g(\lambda_1) \neq 0$, but if $\deg(f, g) = \deg f$, then $g(\lambda_1) = 0$, and in the contrary case we indicate arbitrarily whether λ_1 is a root of the polynomial (f, g) or a root of the polynomial $f/(f, g)$, we memorize this for the future and, depending on this, we regard $g(\lambda_1)$ as equal to or not equal to zero, respectively. We act analogously on the appearance of other algebraic numbers in computations.

We return to the element $a - \lambda \cdot 1$ and consider the two-sided ideal $I = (a - \lambda \cdot 1)A$. Let us set the two-sided ideal $\mathcal{J} = \{b \in A : b \cdot I = 0\}$. Then $I \oplus \mathcal{J} = A$ (a direct sum of algebras) and $I = \oplus_{i \in S} F_{ki}$ and $\mathcal{J} = \oplus_{j \in T} F_{kj}$ for certain nonempty index sets S and T. We define the decompositions of the algebras I and J by the induction hypothesis. The proposition is proved.

The class of the algebras with the condition $R^2 = 0$ (the modules over these algebras have been studied in connection with matrix problems in Kruglyak's article in [2], pp. 60-68) is next to the class of semisimple algebras in difficulty. But even for algebras of this class, the isomorphism problem is quite difficult from the complexity point of view, which is obvious from the following well-known reduction of isomorphism of graphs to isomorphism of algebras of this class (a similar structure is constructed in the theory of incidence algebras — see, e.g., [10]). With respect to an oriented graph G on n vertices and with m edges, we construct an $(n + m)$-dimensional algebra A with a basis $e_1, \ldots, e_n, \{e_{ij}\}$, where (i, j) is an edge of the graph G, and with the relations $e_i e_j = \delta_{ij} e_i$, $e_i e_{kj} = \delta_{ik} e_{kj}$, $e_{kj} e_i = \delta_{ij} e_{kj}$, $e_{ij} e_{kl} = 0$, where δ_{ij} is the Kronecker symbol. Then $e_1 + \ldots + e_n$ is the identity of the algebra A, $\{e_{ij}\}$ is a basis of its radical R whose square is equal to zero, and $A/R = \oplus F$ is the direct sum of n copies of the field F. Isomorphism of oriented graphs is equivalent to isomorphism of the corresponding algebras. The fact that isomorphism of graphs implies isomorphism of algebras is obvious; the converse will follow from the proof of Theorem 1. This theorem asserts that the problem of isomorphism of graphs is equivalent to the problem of isomorphism of a certain class of algebras. See, e.g., [11] for other algebraic approaches to isomorphism of graphs.

THEOREM 1. Isomorphism of algebras with identity (over an algebraically closed field) with the condition $R^2 = 0$ and commutative quotient A/R modulo the radical R is P-equivalent to isomorphism of graphs.

Remark. Actually, we will construct an epimorphic functor (i.e., a functor that is an onto mapping for objects as well as for morphisms) from the category of algebras, having the properties stated in Theorem 1, where isomorphisms are taken as morphisms, onto the category of graphs with natural weights on the edges. Moreover, we will show that this functor can be constructed in polynomial time.

Proof. By the condition, $A/R = \oplus F$ (the direct sum of n copies of the field F); let $f_1, \ldots, f_n$ be pairwise orthogonal idempotents (see [8]) in A/R and $e_1, \ldots, e_n$ be any of their preimages under the epimorphism $A \to A/R$. Let us construct an n-vertex oriented graph $G = G_A$ with weights on the edges by taking the weight on the edge (i, j) equal to $\dim_F e_i R e_j$. Since $R^2 = 0$, it follows that $e_i R e_j$ does not depend on the choice of the preimages $\{e_i\}$.

LEMMA 1. Isomorphism of the algebras A and B is equivalent to isomorphism of the corresponding graphs G_A and G_B.

Proof of the Lemma. Let $A \xrightarrow{\varphi} B$ be a certain isomorphism of algebras (here and below in the proof of Theorem 1 we assume that the algebras are taken from the class under consideration). Then $\varphi(R_A) = R_B$ (R_A is the radical of the algebra A) and $\varphi(e_1), \ldots, \varphi(e_n)$ are the preimages of the pairwise orthogonal idempotents of the quotient under the epimorphism $B \to B/R_B$. Consequently, $\varphi(e_i R_A e_j) = \varphi(e_i) R_B \varphi(e_j)$ and $\dim e_i R_A e_j = \dim \varphi(e_i) R_B \varphi(e_i)$, which shows that the graphs G_A and G_B are isomorphic.

Before proving the converse, we show that $R = \oplus_{1 \leq i, j \leq n} e_i R e_j$, where the direct sum is understood as a direct sum of F-linear spaces. Let, on the contrary, $\sum_{1 \leq i, j \leq n} e_i r_{ij} e_j = 0$ for certain $r_{ij} \in R$. Multiplying both of the sides of this equation, on the left by e_{i_0} and on the right by

e_{j_0}, for certain i_0 and j_0 such that $1 \leqslant i_0, j_0 \leqslant n$, we get $e_{i_0} r_{i_0 j_0} e_{j_0} = 0$ (since $R^2 = 0$), i.e., the sum $\sum_{1 \leqslant i,j \leqslant n} e_i R e_j$ is direct.

Let us decompose the identity: $1 = \sum_{1 \leqslant i \leqslant n} \lambda_i e_i + r_1$, where $\lambda_i \in F$ and $r_1 \in R$ (it is easily seen by squaring both sides of the equation that actually $\lambda_1 = \ldots = \lambda_n = 1$). The relation $r = 1 \cdot r \cdot 1 = \sum_{1 \leqslant i,j \leqslant n} \lambda_i \lambda_j e_i r e_j$ holds for each $r \in R$, which proves the equality $R = \bigoplus_{1 \leqslant i,j \leqslant n} e_i R e_j$.

Further, we use a theorem of Wedderburn (see [7]) by which the algebra A has a subalgebra $C_A \simeq A/R_A$ such that $C_A \cap R_A = \{0\}$. Now, let us suppose that the n-vertex graphs G_A and G_B are isomorphic and $e_1^{(A)}, \ldots, e_n^{(A)}$ and $e_1^{(B)}, \ldots e_n^{(B)}$ are pairwise orthogonal idempotents in the algebras C_A and C_B, respectively, indexed such that $\dim e_i^{(A)} R_A e_j^{(A)} = \dim e_i^{(B)} R_B e_j^{(B)}$ for all $1 \leqslant i, j \leqslant n$. Let us define a mapping $\psi: A \to B$ by setting $\psi(e_i^{(A)}) = e_i^{(B)}$ for $1 \leqslant i \leqslant n$ and by setting ψ equal to a certain ψ_{ij} on $e_i^{(A)} R_A e_j^{(A)}$ $(1 \leqslant i, j \leqslant n)$, where ψ_{ij} is an arbitrary nonsingular F-linear mapping such that $e_i^{(A)} R_A e_j^{(A)} \xrightarrow{\psi_{ij}} e_i^{(B)} R_B e_j^{(B)}$ (an F-linear isomorphism). Since $R = \bigoplus_{1 \leqslant i,j \leqslant n} \times e_i R e_j$, as proved above, ψ is defined properly and is an F-linear isomorphism of additive subgroups of the algebras A and B.

It remains to verify that $\psi(a_1 a_2) = \psi(a_1)\psi(a_2)$ for $a_1, a_2 \in A$. Let $a_1 = \sum_{1 \leqslant i \leqslant n} \eta_i e_i^{(A)} + \sum_{1 \leqslant i,j \leqslant n} \times e_i^{(A)} \rho_{ij} e_j^{(A)}$ and $a_2 = \sum_{1 \leqslant i \leqslant n} \mu_i e_i^{(A)} + \sum_{1 \leqslant i,j \leqslant n} e_i^{(A)} q_{ij} e_j^{(A)}$, where $\eta_i, \mu_i \in F$ and $\rho_{ij}, q_{ij} \in R_A$. Then $a_1 a_2 = \sum_{1 \leqslant i \leqslant n} \eta_i \mu_i e_i^{(A)} + \sum_{1 \leqslant i,j \leqslant n} \eta_i e_i^{(A)} q_{ij} e_j^{(A)} + \sum_{1 \leqslant i,j \leqslant n} \mu_j e_i^{(A)} \rho_{ij} e_j^{(A)}$; whence $\psi(a_1 a_2) = \sum_{1 \leqslant i \leqslant n} \eta_i \mu_i e_i^{(B)} + \sum_{1 \leqslant i,j \leqslant n} \eta_i \psi_{ij} \times (e_i^{(A)} q_{ij} e_j^{(A)}) + \sum_{1 \leqslant i,j \leqslant n} \mu_j \psi_{ij} (e_i^{(A)} \rho_{ij} e_j^{(A)})$. On the other hand,

$$\psi(a_1)\psi(a_2) = \Big(\sum_{1 \leqslant i \leqslant n} \eta_i e_i^{(B)} + \sum_{1 \leqslant i,j \leqslant n} \psi_{ij}(e_i^{(A)} \rho_{ij} e_j^{(A)})\Big)\Big(\sum_{1 \leqslant i \leqslant n} \mu_i e_i^{(B)} + \sum_{1 \leqslant i,j \leqslant n} \psi_{ij}(e_i^{(A)} q_{ij} e_j^{(A)})\Big)$$

$$= \sum_{1 \leqslant i \leqslant n} \eta_i \mu_i e_i^{(B)} + \sum_{1 \leqslant i,j \leqslant n} \eta_i \psi_{ij}(e_i^{(A)} q_{ij} e_j^{(A)}) + \sum_{1 \leqslant i,j \leqslant n} \mu_j \psi_{ij}(e_i^{(A)} \rho_{ij} e_j^{(A)}),$$

which completes the proof of the lemma.

In order to complete the proof of Theorem 1, it should be shown that the graph G_A can be constructed with respect to A in polynomial time (the converse, i.e., the construction of a certain algebra B with respect to a graph G such that $G_B = G$ had actually been carried out before the formulation of Theorem 1). To this end, it is sufficient to find R in polynomial time (pairwise orthogonal idempotents in the commutative semisimple algebra A/R can be found in polynomial time with the help of the procedure set forth earlier in the proof of Proposition 1).

At first, let us construct the commutant Com (A), which is the F-linear hull of the elements $\{a_i a_j - a_j a_i\}$ for an arbitrary basis $\{a_i\}$ of the algebra A. It can be verified that $\mathrm{com}(A) = \bigoplus_{1 \leqslant i,j \leqslant n, i \neq j} e_i R e_j$. Therefore, to find R it is sufficient to find the radical R_1 of the commutative algebra $A_1 = A/\mathrm{Com}\ (A)$. Obviously, $R_1 = \bigoplus_{1 \leqslant i \leqslant n} e_i R_1 e_i$.

As in the proof of Proposition 1, we find R_1 by induction on $\dim A_1$. Remembering the remark about computation with algebraic numbers, we find a $\lambda_1 \in F$ such that $\det(a_1 - \lambda_1 \cdot 1) = 0$

(we find the identity of the algebra in polynomial time from the linear system $\left(\sum_{1\leqslant i\leqslant n} x_i a_i\right) a_j = a_j$ for $1 \leqslant j \leqslant n$) if a_1 is considered as an F-linear operator on A_1 (we suppose that $a_1 \neq \mu \cdot 1$ for any $\mu \in F$). This means that a certain $\theta_i = 0$ in the decomposition $a_1 - \lambda_1 \cdot 1 = \sum_{1\leqslant i\leqslant n} \theta_i e_i + r$, where $r \in R_1$. Let us suppose that $(a_1 - \lambda_1 \cdot 1)^2 \neq 0$. Then we consider the ideals $I = \{a \in A_1 : a(a_1 - \lambda_1 \cdot 1)^2 = 0\}$ and $J = \{a \in A_1 : aI = 0\}$ (the ideals I and J are constructed in polynomial time, starting from obvious linear systems). In this case, $I \oplus J = A_1$ (a nontrivial direct sum of algebras), and we use the induction hypothesis. Now, let $(a_1 - \lambda_1 \cdot 1)^2 = 0$. Then we find an i for which $(a_i - \lambda_i \cdot 1)^2 \neq 0$, where $\lambda_i \in F$, such that $\det (a_i - \lambda_i \cdot 1)^2 = 0$, and act as above (if such an i does not exist, then $a_i - \lambda_i \cdot 1 \in R_1$ for each i and $\{a_i - \lambda_i \cdot 1\}$ is a basis of R_1; in this case, $A_1/R_1 = F$).

Thus, R_A and, by the same token, G_A are constructed in polynomial time, which completes the proof of the theorem.

In conclusion, we pose a series of problems: What can be said about the complexity of re recognition of isomorphism for classes of algebras more general than the ones considered? It would also be interesting to study hierarchy of classes of algebras, whose k-th member consists of algebras for which $R^k = 0$, from the point of view of complexity. Also, it is not known whether the radical of each algebra can be found in polynomial time.

LITERATURE CITED

1. I. M. Gel'fand and V. A. Ponomarev, "Remarks on the classification of pairs of commuting linear transformations in a finite-dimensional space," Funkts. Anal. Prilozhen., 3, No. 4, 81-82 (1969).
2. Zap. Nauchn. Sem. Leningr. Otd. Mat. Inst. Akad. Nauk SSSR, 28 (1972).
3. I. Borosh and A. S. Fraenkel, "Exact solutions of linear equations with rational coefficients by congruence techniques," Math. Comput., 20, No. 93, 107-117 (1966).
4. M. T. McClellan, "The exact solution of system of linear equations with polynomial coefficients," J. Assoc. Comput. Mach., 20, No. 4, 563-588 (1973).
5. T. C. Hu, Integer Programming and Network Flows, Addison-Wesley, New York (1970).
6. D. Yu. Grigor'ev (D. Yu. Grigoryev), "Some new bounds on tensor rank," LOMI Preprint E-2-78, Leningrad (1978).
7. N. Jacobson, Theory of Rings, Amer. Math. Soc., Providence (1943).
8. I. Herstein, Noncommutative Rings, Math. Assoc. Amer., Philadelphia (1968).
9. E. Horowitz and S. Sahni, "On computing the exact determinant of matrices with polynomial entries," J. Assoc. Comput. Mach., 22, No. 1, 38-50 (1975).
10. N. A. Nachev, "On incidence rings," Vestn. Mosk. Gos. Univ., Ser. I, No. 1, 36-42 (1977).
11. D. Yu. Grigor'ev, "Two reductions of isomorphism of graphs to problems about polynomials," Zap. Nauchn. Sem. Leningr. Otd. Mat. Inst. Akad. Nauk SSSR, 88, 56-61 (1979).