TWO REDUCTIONS OF GRAPH ISOMORPHISM TO PROBLEMS ON POLYNOMIALS

D. Yu. Grigor'ev

UDC 510.52+519.17

It is proved that for isomorphism of n-vertex graphs with weights on the edges there exists a complete system of $n^2 + 1$ polynomial invariants. It is also shown that isomorphism of graphs reduces in polynomial time to the factorization of a polynomial in one variable into factors irreducible over some field.

In the present note two reductions are given of the problem of isomorphism of graphs (in connection with the literature, cf. [1-4]). It is proved that for n-vertex graphs with weights on the edges, there exists a complete system of invariants, consisting of $(n^2 + 1)$ polynomials, the degree of each of which does not exceed n^2. The second result consists of the reduction in polynomial time of the problem of isomorphism of graphs to the factorization of a polynomial into irreducible factors over some field. There appears to be great interest in estimating the complexity of the factorization of a polynomial into irreducible factors (especially over the field of rational numbers, cf., e.g., [5, 4.6.2]). In some sense both the reductions indicated are realizations of the "functorial" approach (the term is borrowed by the author from [4]).

To get the reductions indicated, one uses concepts and results, well known in the theory of invariants and Galois theory (references are given to the corresponding literature). We shall consider the problem, formally more general than the problem of isomorphism of graphs, of the isomorphism of hypergraphs with weights on the edges – for this problem there is a clearer connection evident with the algebraic concepts used. The last problem reduces in polynomial time to the problem of isomorphism of graphs with weights 0, 1 on the edges – we shall call them simply graphs (the indicated reduction is in [2] and is based on considerations already known to Birkhoff).

In order to precisely formulate the problem of isomorphism of hypergraphs, we fix a field F of characteristic q. By a (k, n)-hypergraph we shall mean a k-dimensional tensor $T = (T_{i_1 \ldots i_k})$, where $1 \le i_1, \ldots, i_k \le n$, i.e., a k-dimensional cube with side n, in whose cells stand $T_{i_1 \ldots i_k}$, elements of the field F; the class of all (k, n)-hypergraphs we denote by $G_{k,n}$. We shall call a (k, n)-hypergraph T symmetric if $T_{i_1 \ldots i_k} = T_{i_{\pi(1)} \ldots i_{\pi(k)}}$ for any π, an element of the group S_k of all permutations of a set of k elements. In the case when k = 2 and all elements T_{ij} assume values 0, 1, we get the contiguity matrix of an ordinary graph (if T is symmetric, then the corresponding graph is unoriented). Two (k, n)-hypergraphs T and T' are called isomorphic (and we write $T \sim T'$), if there exists a permutation $\tau \in S_n$, such that $T = \tau T'$, i.e., $T_{i_1 \ldots i_k} = T'_{\tau(i_1) \ldots \tau(i_k)}$ for all $1 \le i_1, \ldots, i_k \le n$. If $\tau T = T$, then τ is called an automorphism of the hypergraph T, and the group of all automorphisms we denote by aut T.

The algorithmic formulation of the isomorphism problem consists in estimating the complexity of the recognition problem: Are two given graphs isomorphic or not (cf., e.g., [1]? This problem is considered difficult (a fairly detailed bibliography on attempts to solve it is given in [3]) – it remains an open question whether it belongs to the class of problems recognizable in polynomial time or not.

For the first reduction of the isomorphism problem of (k, n)-hypergraphs one constructs a complete system of $n^k + 1$ invariant polynomials. n^k of them have simple form and their values can be calculated rapidly, while the remaining $(n^k + 1)$-th polynomial takes a long time to calculate with the help of the known schemes of calculation (furthermore, there is no evident effective method of defining it). If one succeeded in giving a calculation of the values of this polynomial in polynomial time, then it would be established that the isomorphism of graphs belongs to the class of problems recognizable in polynomial time.

1. We denote by F_q the primitive field of characteristic q (q is a prime or zero). We call a polynomial $P(\langle x_{i_1 \ldots i_k} \rangle)$ in n^k variables with coefficients in the field F_q an invariant q-polynomial, or simply an invariant

Translated from Zapiski Nauchnykh Seminarov Leningradskogo Otdeleniya Matematicheskogo Instituta im. V. A. Steklova AN SSSR, Vol. 88, pp. 56-61, 1979. Original article submitted May 19, 1977; revision submitted December 12, 1978.

 0090-4104/82/2004-2296$07.50

for $G_{k,n}$, if for any $T \in G_{k,n}$ and any permutation $\tau \in S_n$ one has $P(\langle T_{i_1\ldots i_k}\rangle) = P(\langle T_{\tau(i_1)\ldots\tau(i_k)}\rangle)$. A system (finite or infinite) of invariants $\{P_j\}$ is called complete if for any T, $T' \in G_{k,n}$, from the fact that $P_j(\langle T_{i_1\ldots i_k}\rangle) = P_j(\langle T'_{i_1\ldots i_k}\rangle)$ for all j, it follows that $T \sim T'$. We denote by $R = R(q, k, n)$ the ring of invariant q-polynomials for $G_{k,n}$, by $F(q, k, n)$ its field of fractions.

We give examples of the simplest invariants. Let $M \in G_{k,n}$ and the elements of M be zero and one (we shall use this notation below also). We set

$$f_M = \prod_{1 \le i_1,\ldots,i_k \le n} x_{i_1\ldots i_k},$$

where the product is taken over all $x_{i_1\ldots i_k}$ for which $M_{i_1\ldots i_k} = 1$. Then $P_M = \sum_{\tau \in S_n} f_{\tau(M)}$ is an invariant.

THEOREM 1. For any q, k, n, there exists a complete system of invariants for $G_{k,n}$, containing $n^k + 1$ elements, each of which is an F_q-linear combination of invariants $\{P_M\}$.

LEMMA 1. The ring R is finitely generated over F_q (its generating system is, e.g., the set of all $\{P_M\}$).

The assertion about the finite generation of the ring R follows from the theorem of Hilbert–Nagata ([6, p. 368] – in the present case $\mathcal{G} = S_n$, $A^{\mathcal{G}} = R$). The proof of the fact that for any q, as generating system one can take $\{P_M\}$, completely follows the proof of the fundamental theorem on symmetric polynomials [7, p. 124].

LEMMA 2. The ring R(q, k, n) is a complete system of invariants for $G_{k,n}$.

For each $T \in G_{k,n}$ we define in the following way a polynomial $f_T(\Gamma, \langle\gamma_{i_1\ldots i_k}\rangle)$ of $n^k + 1$ variables:

$$f_T(\Gamma,\langle\gamma_{i_1\ldots i_k}\rangle) = \prod_{\tau \in S_n}\Big(\Gamma - \prod_{1 \le i_1,\ldots i_k \le n}(\gamma_{i_1\ldots i_k} - T_{\tau(i_1)\ldots\tau(i_k)})\Big).$$

If $T \sim T'$, then $f_T = f_{T'}$ as polynomials, i.e., their corresponding coefficients coincide. Conversely, let $f_T = f_{T'}$. We consider f_T and $f_{T'}$ as polynomials in one variable Γ with coefficients in the ring $R = F[\langle\gamma_{i_1\ldots i_k}\rangle]$. Since the roots of the polynomials f_T and $f_{T'}$ coincide, for some $\tau \in S_n$ in the ring R_1 one has

$$\prod_{1 \le i_1,\ldots i_k \le n}(\gamma_{i_1\ldots i_k} - T_{i_1\ldots i_k}) = \prod_{1 \le i_1,\ldots i_k \le n}(\gamma_{i_1\ldots i_k} - T'_{\tau(i_1)\ldots\tau(i_k)}).$$

By virtue of the factoriality of the ring R_1 [7, p. 115], $T_{i_1\ldots i_k} = T'_{\tau(i_1)\ldots\tau(i_k)}$ for all $1 \le i_1, \ldots, i_k \le n$. Hence $T \sim T'$ is equivalent with the fact that $f_T = f_{T'}$, which means the coincidence of the corresponding coefficients of the polynomials f_T and $f_{T'}$, all of which are elements of R(q, k, n).

LEMMA 3. The field F(q, k, n) is generated over F_q by (n^k+1) by elements which can be chosen as F_q-linear combinations of the invariants $\{P_M\}$.

This lemma is a special case of Theorem 6 of [8, p. 48], which follows from the primitive element theorem (cf. [7, p. 168]). In the present case, the transcendence degree of the field F(q, k, n) over F_q is equal to n^k, and that the field F(q, k, n) is finitely generated over F_q follows from Lemma 1.

The theorem follows from Lemmas 2 and 3.

Remark. From what is mentioned on p. 417 of [9] it follows that Lemma 3 can be improved: even the ring R(q, k, n) is generated over F_q by $(n^k + 1)$ elements.

2. The isomorphism problem for hypergraphs reduces to the isomorphism problem for symmetric hypergraphs, even graphs – cf., e.g., [2] (here and later the reducibility means reducibility in polynomial time). In this section, without saying this each time specially, we consider symmetric hypergraphs.

Let $T \in G_{k,n}$. We divide the set of numbers $\{1, \ldots, n\}$ into domains of transitivity with respect to T, putting i, j $(1 \le i, j \le n)$ into one domain if and only if one can find a $\tau \in \operatorname{aut} T$ such that $\tau i = j$.

It is well known that the problem of isomorphism of graphs reduces to the problem of partitioning into domains of transitivity with respect to a given hypergraph. Namely, for T', $T'' \in G_{k,n}$ we construct $T \in G_{k,2n}$, setting

$$T_{i_1\ldots i_k} = T'_{i_1\ldots i_k}, \quad \text{if } 1 \le i_1,\ldots i_k \le n,$$
$$T_{i_1\ldots i_k} = T''_{i_1-n\ldots i_k-n}, \quad \text{if } n+1 \le i_1,\ldots,i_k \le 2n,$$

and otherwise setting $T_{i_1 \ldots i_k}$ equal to an element of the field F, not occurring among the elements $\{T'_{j_1 \ldots j_k}\}$ and $\{T''_{j_1 \ldots j_k}\}$ (if the field F is finite and this cannot be done, then we pass temporarily to a larger field, and then with the help of the method already mentioned, recounted in [2], we pass to graphs). Hypergraphs T' and T" are isomorphic if and only if one can find natural numbers i, j satisfying $1 \le i \le n < j \le 2n$, and lying in one domain of transitivity with respect to T.

Now let $T \in G_{k,n}$ and let $y_1, \ldots, y_n$ be algebraically independent over F. Let, further, $\sigma_1 = y_1 + \ldots + y_n, \ldots, \sigma_n = y_1 \ldots y_n$ be elementary symmetric polynomials in $y_1, \ldots, y_n$. We consider the finite Galois extension of fields $F_\sigma = F(\sigma_1, \ldots, \sigma_n) \subset F(y_1, \ldots, y_n) = F_y$. The degree of this extension is equal to n! and its Galois group is S_n (cf. [7, p. 222]). We denote by $f \in F_\sigma[z]$ the polynomial $z^n - \sigma_1 z^{n-1} + \ldots + (-1)^n \sigma_n$. Its roots are $y_1, \ldots, y_n$. We denote further by $\theta_T \in F_y$ the element $\sum_{1 \le i_1, \ldots, i_k \le n} T_{i_1 \ldots i_k} y_{i_1} \cdots y_{i_k}$ and by F_T the field $F_\sigma(\theta_T)$.

THEOREM 2. The problem of partition into domains of transitivity with respect to T reduces to the problem of factoring the polynomial f into irreducible factors over the field F_T.

Let $f = f_1 \ldots f_l$ be the factorization of f into factors, irreducible over F_T. Substituting successively $y_1, \ldots, y_n$ into $f_1, \ldots, f_l$, we clarify which are the roots of the polynomials $f_1, \ldots, f_l$. By I_j we denote the set of indices of roots of the polynomial f_j $(1 \le j \le l)$, i.e., $i \in I_j \Longleftrightarrow f_j(y_i) = 0$.

The Galois group $G \subset S_n$ of the extension $F_T \subset F_y$ coincides (as permutation group) with the group of automorphisms aut T. In fact, let $g \in G$, then $g\theta_T = \theta_T$ and $gT = T$ (from the symmetry of T). Conversely, let $g \in \operatorname{aut} T$, then $g\theta_T = \theta_T$ and $g \in G$.

The elements of the group G act transitively on the roots of the polynomials f_j $(1 \le j \le l)$, and a root of the polynomial f_i cannot be translated into some root of a polynomial f_j $(j \ne i)$. This assertion is well known in Galois theory, but below we give a short proof of it, based on the fundamental theorem of Galois theory (cf. [7, p. 202]). The second part of the assertion is proved thus. Let $g \in G$ and $gy_u = y_v$, where $f_i(y_u) = 0$ and $f_j(y_v) = 0$ $(i \ne j)$. But $gf_i = f_i$, so $f_i(y_v) = 0$ and the polynomials f_i and f_j have common roots – contradiction. Now we prove the first part. Let $f_j = h_1 \ldots h_m$, where the group G now acts transitively on the roots of each of the polynomials $h_1, \ldots, h_m$ (we use the already proved second part of the assertion). Then G acts invariantly on all the polynomials $h_1, \ldots, h_m$, hence according to the fundamental theorem of Galois theory the coefficients of the polynomials $h_1, \ldots, h_m$ lie in the field F_T, but f_j is irreducible over F_T, i.e., $m = 1$, so G acts on the roots of each of the polynomials f_j $(1 \le j \le l)$ transitively.

It follows from the two assertions proved above that $I_1, \ldots, I_l$ is a partition into domains of transitivity with respect to T. The theorem is proved.

The author thanks B. S. Stechkin for helpful conversations on isomorphism of graphs.

LITERATURE CITED

1. S. A. Cook, "The complexity of theorem-proving procedure," in: Proc. 3rd Ann. ACM Symp. Theory Comput., Shaker Heights, Ohio (1971), pp. 151-159
2. G. L. Miller, "Graph isomorphism, general remarks," Tech. Report 18, University of Rochester (1977).
3. R. C. Read and D. G. Corneil, "Graph isomorphism disease," J. Graph Theory, 1, 339-363 (1977).
4. L. Babai, "On the isomorphism problem," in: Proc. 1977 Comput. Theory Conf., Poznan-Kornik, Poland (1977).
5. D. Knuth, The Art of Computer Programming, Vol. 2, Mass. (1969).
6. N. Bourbaki, Algebre Commutative, Paris (1965).
7. B. L. van der Waerden, Algebra I, New York (1971).
8. I. R. Shafarevich, Foundations of Algebraic Geometry [in Russian], Moscow (1972).
9. A. I. Kostrikin, Introduction to Algebra [in Russian], Moscow (1977).