JOURNAL OF COMPUTER AND SYSTEM SCIENCES 42, 237–248 (1991)

On Isomorphism Testing of a Class of 2-Nilpotent Groups*

MAX GARZON AND YECHEZKEL ZALCSTEIN†

Department of Mathematical Sciences, Memphis State University, Memphis, Tennessee 38152

Received September 25, 1987; revised September 20, 1989

A polynomial time isomorphism test for a class of groups, properly containing the class of abelian groups, given either by multiplication tables or by generators and relators, is described. It is also shown that graph isomorphism testing is uniformly reducible to a word problem of a finitely presented group.

1. INTRODUCTION

In contrast to graph isomorphism, very little is known about the complexity of group isomorphism testing. For groups given by multiplication tables, Tarjan [15] has produced an $O(n^{\log n})$-time isomorphism test (for groups of order n given by multiplication tables) which was discovered independently in [9] as a sharper $O(\log^2 n)$-space algorithm. Since two finite presentations of a finitely generated abelian group are isomorphic if and only if their associated matrices over the integers have the same invariant factors (which can be computed in time polynomial in the size of the presentations [5], even under the logarithmic cost criterion [8]), isomorphism of finitely generated abelian groups given by generators and relators can be tested in polynomial time. On the other hand, testing isomorphism of arbitrary *finite* groups given by generators and relations is, to the best of our knowledge, an open problem.

A natural hierarchy of finite groups, whose first layer is the class of abelian groups, has been recently introduced in the literature. The groups in the second layer are defined by a permutational property for products of any three elements and are herein referred to as P_3 groups. This paper provides a polynomial time isomorphism test for P_3 groups given succinctly by means of generators and relations, and a fortiori, a test for multiplication tables. The algorithm follows from a structure theorem established in Section 3. In Section 5 it is shown that graph

* This research was partially supported by NSF Grant DCR-8602319.

† Current address: Division of Computer and Computation Research, National Science Foundation, Washington, DC 20550.

0022-0000/91 $3.00

571/42/2-8

isomorphism testing is polynomial-time reducible to the word problem of a certain finitely presented group.

A preliminary version of this paper presented in [2] contained an incorrect version of the structure theorem. It was then erroneously claimed as a consequence that isomorphism testing of P_3 groups was graph-isomorphism complete. We are grateful to the anonymous referee for pointing out these errors in the original manuscript.

2. Permutation Properties

Permutation properties (here denoted P) were apparently first introduced by Restivo and Reutenauer [12], who show that the strong Burnside Problem for semigroups (viz., is every finitely generated torsion semigroup finite?) has a positive solution for semigroups with the permutation property (for a survey, see [13]).

Definition 2.1. Let $n \geq 2$ be a positive integer and S a semigroup. An n-tuple $(x_1, x_2, ..., x_n)$ of elements of S satisfies P_n—the permutation property of degree n—if there exists a nontrivial permutation σ of its components such that

$$x_1 x_2 \cdots x_n = x_{\sigma(1)} x_{\sigma(2)} \cdots x_{\sigma(n)}. \tag{1}$$

S satisfies P_n if every n-tuple of elements of S satisfies P_n.

Standard notation and results from classical group theory, necessary in the discussion below, are introduced next. As usual, $[x, y]$ (x^y, resp.) will denote the *commutator* $xyx^{-1}y^{-1}$ (*conjugation* yxy^{-1}) of two group elements x, y. The *commutator* (or *derived*) *subgroup* G' of a group G is the subgroup consisting of all possible products of commutators of G (e.g., the trivial subgroup in an abelian group). The *center* of $Z(G)$ of G is a subgroup consisting of those elements that commute with every other element. An abelian group is *elementary abelian* if it is isomorphic to a direct product of copies of Z_2. Further, a group G is *nilpotent of class at most* 2 if it is abelian (class 1) or every commutator is a central element (i.e., commutes with all other elements) of G.

Now let $X(X^{-1})$ be a (finite) alphabet of symbols (in one–one correspondence with X, respectively) and R a subset of $(X \cup X^{-1})^*$. Recall that $\langle X | R \rangle$ is a *presentation* of a group G if G is the largest group which contains generators $x_1, ..., x_n$, in one-to-one correspondence with the symbols in X, in which the following property is satisfied:

> all words $w \in R$ become the identity elements of G when generators $x_1, ..., x_n$ are substituted for the respective elements of X and concatenation and inversion are interpreted as the operations in the group G, respectively. (†)

In other words, any other group in which this property holds is a homomorphic image of $\langle X | R \rangle$.

THEOREM 2.1 (Von Dyck). *If H is any group generated by X and all words in R satisfy property (†) in H, then there exists a homomorphism of $\langle X | R \rangle$ onto H.*

A *finite presentation* $\langle X | R \rangle$ in which both sets X and R are finite. The reader is referred to [5,10,11] for further discussion of presentations and related notions.

The following result has been proved in [1] (see also [3]).

THEOREM 2.2. *A group G is a P_3 group if and only if $|G'| \leqslant 2$.*

In particular, the nontrivial commutators of a P_3 group are central involutions. For example, the quaternion and dihedral groups Q, D_4 are easily seen to satisfy P_3, as is the infinite group F_2 given by

$$F_2 = \langle x, y | u^2, [u, x], [u, y] \rangle,$$

since the defining relators imply that $u := [x, y]$ is a central involution and the following is a commutator identity

$$[x, yz] = [x, y][x, z]^y.$$

However, it will be clear that, in general, P_3 groups are *not* extraspecial (where $G' = Z(G)$) since their centers can have an arbitrarily large order while the order of the derived subgroup is 2 (see Theorem 2.2). Many examples can be constructed as quotients of F_2 by imposing relators of the type x^{2^n}.

Here, and throughout this paper, u denotes the (only) commutator of a P_3 group, e.g., $[x, y]$ in F_2. Also, a relator in R of type wv^{-1} is sometimes written in the form $w = v$. For all other undefined algebraic terminology and notation see [7, 10, 11] and/or [14].

3. A STRUCTURE THEOREM

The purpose of this section is to establish a structure theorem for the class of finite P_3 groups. Since a P_3 group is nilpotent of class $\leqslant 2$, a finite P_3 group is a direct product of a finite abelian group of odd order and a finite P_3 2-group (see [3, Corollary 1]). Thus in the remainder of this section G is a nonabelian P_3 2-group.

The discussion requires the next two lemmas, the first of which is an elementary fact.

LEMMA 3.1. *A group G is (isomorphic to) the direct product of two normal subgroups H and K if and only if $H \cap K = 1$ and every element in G is of the form hk for some $h \in H$, $k \in K$.*

Next, observe that if the cosets of elements $x_1, ..., x_n$ are a basis of the *abelianization* $G_{ab} := G/G'$ of an indecomposable P_3 group G, then $x_1, ..., x_n$ generate G. Thus, by a *basis* of G we denote generators

$$x_1, ..., x_n, \tag{2}$$

whose cosets modulo G' form a basis of the abelian group G_{ab} in the usual sense. On the other hand, it is well known that if the central quotient G/Z of a 2-group G is elementary abelian (i.e., a vector space over the field $GF(p)$ of p elements), one can define a regular alternating bilinear $[\cdot, \cdot]$ form on G/Z so that $u^{[xZ, yZ]} = [x, y]$ (see [7, Sect. II.9]). Such an alternating vector space has a *symplectic basis*, which are orthonormal vectors, cosets of

$$x_1, y_1, ..., x_s, y_s, \tag{3}$$

where $[x_i, y_j] = \delta_{ij}$ (the Kronecker delta δ_{ij} is equal to 1 if $i = j$ and 0 otherwise). For the purposes of Section 4 it is necessary to describe a polynomial time algorithm for obtaining such a basis from a basis (2) of a nonabelian group G. Ignoring central elements and rearranging the basis (2) in ascending order $|x_1| \leqslant |x_2| \leqslant \cdots$, assume that $x_k Z$ is the first coset satisfying $[x_1, x_k] \neq 1$ (such a k exists for x_1 is not central) and let $y_1 := x_k$. Replace each of the remaining elements x_i $(1 \neq i \neq k)$ by

$$X_i = x_i x_1^{\epsilon_k} x_k^{\epsilon_1}, \qquad [x_i, x_j] = u^{\epsilon_j}, \qquad j = 1, k,$$

so that $|X_i| = |x_i|$ and the new elements $X_3, ..., X_n$ all commute with x_1, y_1. Recursively, find elements of the desired type (2) for the remaining generators. A generating set

$$z_1, ..., z_r, x_1, y_1, ..., x_s, y_s, \tag{4}$$

consisting of elements of type (3) plus central generators $z_1, ..., z_r$ of G, which is also a basis of G, as previously defined, will be called a *symplectic basis* of G. Since it is easy to check that the set obtained by performing all the required substitutions of the X_i is still a basis of G/G', and their cosets are now a symplectic basis of G/Z, it follows that

LEMMA 3.2. *Every P_3 group has a symplectic basis.*

The foregoing is a standard argument when dealing with symplectic forms. A further nonlinear argument is necessary to establish a structure theorem for P_3 groups. The class of P_3 groups is closed under subgroups and homomorphic images but not under direct products. Nonetheless, it is closed under a slight variation of the direct product operation, which will be used as a basic construction for obtaining arbitrary P_3 groups.

DEFINITION 3.1. Let u (v, resp.) be a nontrivial central involution in a P_3 group $G(H)$, the nontrivial commutator if $G(H)$ is not abelian. The amalgamated direct product of G and H, with u and v amalgamated, is the quotient of the cartesian product $G \times H$ by the normal subgroup $\{(1, 1), (u, v)\}$.

Informally, the amalgamated product is obtained from the ordinary direct product by identifying the two involutions u and v. The definition can be obviously extended to any number of factors. Note that if the involutions are both nontrivial then the amalgamated product is a particular case of the ordinary central product (see [7, I.9.10]) and it enjoys similar properties like associativity and commutativity of the factors (up to isomorphism), and the cyclic group of order 2 acts as an identity element, as can be easily checked. Therefore, from now on in all amalgamated products with an abelian group it will be assumed that the abelian group has order at least 4. In this notation Lemma 3.2 yields

LEMMA 3.3. *Every finite P_3 group G is (isomorphic to) the direct product of an abelian group A, the amalgamated product of two-generator P_3 2-groups, and possibly a cyclic group of order at least* 4.

Proof. The claim is true if G is abelian or generated by two elements, so assume that G is a nonabelian 2-group, so that $s \geqslant 1$ in a fixed symplectic basis (4) of G. Every element of G can be written uniquely in the form

$$x_1^{k_1} \cdots x_n^{k_n} u^{\varepsilon}, \qquad 0 \leqslant k_i < |x_i|'; \qquad \varepsilon = 0, 1, \tag{5}$$

where the primed orders are the orders of the cosets $x_i G'$ in G/G', by first expressing its coset modulo G' as a product of the cosets of x_i's and then multiplying by the central commutator u if necessary.

Recall that in a class 2 nilpotent group the identity

$$(xy)^n = x^n y^n [x, y]^{n(n-1)/2}$$

holds. Therefore, squaring an element of G squares the generators in (5) and possibly produces an extra power of the commutator u. Thus, since squares are central elements in G, raising the element in (5) to a power $2^k \geqslant 4$ only raises every factor to the same power. Therefore, the order of an element equals the order of the largest generator in the symplectic basis occurring in its expression (5), hence the largest order of an element in G occurs among the basis elements.

If a central generator z has largest order in (4) and u is not a power of z then its coset zG' has largest order in G_{ab}. An element of largest order in an abelian group generates a direct factor of G, i.e., $G/G' = \langle zG' \rangle \times K/G'$ for some subgroup K such that $\langle z \rangle \cap K \subseteq G'$, whence $G = \langle z \rangle \times K$ by Lemma 3.1. Thus every central generator of G of maximum order in a symplectic basis generates a direct factor. Furthermore, if z is a central generator with the largest n such that $z^n = u$ (whence $n = |z|/2$) and $z_i^m = u$, replace each z_i with $z_i^m = u$ by the product $Z_i := z^{n/m} z_i$. Note that Z_i has a coset Z_i/G' of the same order as z_i (so that the resulting elements are

still a symplectic basis of G) but which does not have u as a power, for $Z_i^m = z^n z_i^m = u^2 = 1$. Repeating this process, one arrives at a symplectic basis (5) all of whose central generators, except possibly one, do not have u as a power. The same argument shows that if $n \geqslant m$ for some noncentral generator x_i (or y_i) such that u is not a power of x_i but $x_i^m = 1$, then substitution of $X_i := z^{n/m} x_i$ for x_i will yield a symplectic basis in which $X_i^m = u$. Finally, let A be the subgroup generated by all central generators in the resulting basis which do not have u as a power and K the subgroup generated by the remaining generators. Thus, by Lemma 3.1, A and K are both direct factors of G. Since (4) is a basis of G, K is the amalgamated product of possibly the remaining central generator which has u as a power, and of the two-generator P_3 2-groups generated by the symplectic pairs x_i, y_i. ∎

Thus, nonabelian two-generator groups turn out to be basic building blocks of arbitrary P_3 groups. The next lemma elucidates the structure of these groups.

LEMMA 3.4. *A two-generator nonabelian P_3 2-group is (isomorphic to) exactly one of the following three types of groups*:

(F) *a group $F(n, m)$ of order 2^{n+m+1} presented by*

$$\langle x, y \mid x^{2^n}, y^{2^m}, [x, y]^2, [[x, y], x], [[x, y], y] \rangle \qquad (n \geqslant m \geqslant 1);$$

(D) *a dihedral type group $D(n, m)$ of order 2^{n+m} presented by*

$$\langle x, y \mid x^{2^n}, y^{2^m}, y^x = y^{2^{m-1}}, [[x, y], x], [[x, y], y] \rangle \qquad (n \geqslant m \geqslant 2);$$

(Q) *a quaternion type group $Q(n, m)$ of order 2^{n+m-1} presented by*

$$\langle x, y \mid x^{2^n}, y^{2^m}, x^{2^{n-1}} = y^{2^{m-1}}, x^y = x^{2^{m-1}+1} \rangle \qquad (n \geqslant m \geqslant 2).$$

Moreover, any two of these presentations $X(n, m)$ and $X(n', m')$ of the same type $X = F$, D, or Q are isomorphic if and only if $n = n'$ and $m = m'$.

Proof. Groups of the given types are finite quotients of the (infinite) group F_2, by Von Dyck's theorem, so they are P_3 groups.

To establish that every two-generator P_3 2-group G has a presentation of the above type, assume, without loss of generality, that x, y is a symplectic basis of G with $2^n := |x| \geqslant |y| := 2^m$. Since G is nonabelian, x, y do *not* commute. Since $F(1, 1)$ and $Q(2, 2)$ are isomorphic to the only two nonabelian groups of order 8, the dihedral and quaternion groups, assume that the order of G is at least 16, i.e., $n \geqslant 2$.

First assume that the decomposition in (5), now with

$$x_i y_j u^\varepsilon, \qquad 0 \leqslant i < |x|, 0 \leqslant j < |y|, \varepsilon = 0, 1, \tag{6}$$

is unique for all elements of G, i.e., that an element (6) is trivial only in case $i = j = \varepsilon = 0$. In particular, u cannot be a power of either generator of G and hence the orders of x, y are equal to the orders of their cosets in G_{ab}. Since only the

relators in the given presentation are necessary to reduce a product of x, y and their inverses to an expression of the form (6) it follows that, in this case, G is defined by a presentation of type (F).

Now assume that there is a nontrivial relator of type (6) in G. The relation also holds in G_{ab}. It follows that

$$x^i = u, \qquad y^j = 1, \qquad \varepsilon = 1$$

or

$$x^i = 1, \qquad y^j = u, \qquad \varepsilon = 1$$

or

$$x^i = u, \qquad y^j = u, \qquad \varepsilon = 0.$$

In all cases either nonzero $i = |x|/2 = 2^{n-1}$ or $j = |y|/2 = 2^{m-1}$. In the first case, if $n = m$, G is of type $D(m, n)$; if $n > m$, the elements $X := x$ and $Y := yx^{2^{n-m-1}}$ are still a basis of G and $Y^{2^{m-1}} = u$, so consider only the last two cases. In the second case the group is isomorphic to $D(n, m)$ and in the third case G is isomorphic to $Q(n, m)$. It only remains to show that no two of the given presentations give rise to isomorphic groups.

Since squaring an element of type (6) squares each factor and possibly gives rise to a commutator factor, no element other than u itself has u as a power in $F(n, m)$, unless $n = m = 1$. Therefore no F group is isomorphic to any D or Q group. The largest order of an element in a D group is 2^n, and the order of $D(n, m)$ is 2^{n+m}, so two D groups are isomorphic if and only if their defining parameters n, m are identical. Likewise for Q groups. Finally, one knows that $F(1, 1) \equiv D_4$ and $Q(2, 2) \equiv Q$ are not isomorphic so assume $n \geqslant 2$. Again, squaring the element (6) shows that one only obtains seven nontrivial involutions in D-type groups, while there are nine involutions in $Q(n, m)$. Thus no Q-type group can be isomorphic to a D-type group. ∎

The groups $Q(n, m)$ are metacyclic since they are extensions of a cyclic group $\langle x \rangle$ of order 2^n by a cyclic group of order 2^{m-1} with its generator acting as $x^y = x^{2^{n-1}+1}$. Likewise for $D(n, m)$ and $\langle y \rangle$.

There only remains to determine under which conditions the parameters involved in the decomposition of G provided by Lemmas 3.3 and 3.4 define isomorphic groups. The following theorem provides an answer to this question. It is easy to check that a group may admit more than one decomposition of this type, since, for instance, the central and amalgamated product of two quaternion groups coincides with the same product of two dihedral groups (see Satze I.9.10, III.13.7, and III.13.8 in [7]). Moreover, the amalgamated direct product M of a cyclic group C generated by an element c of order at least 4 and of the group D_4 generated by x, y coincides with the central product of C and D_4 and is isomorphic to the amalgamated (central) product of the two subgroups $\langle c \rangle$ and $\langle x, c^{|c|/4} y \rangle$, the

latter being generated by two elements of order 4, as can be easily checked. Therefore M is isomorphic to the amalgamated direct product of C and $Q = Q(2, 2)$.

By the remark at the beginning of this section, it suffices to establish the following theorem in case G is a P_3 2-group.

THEOREM 3.1. *A finite P_3 group G determines four lists of integers (c^ε, δ), $(a_1, ..., a_r)$, $(n_1, ..., n_s)$, and $(m_1, ..., m_s)$, r and/or s possibly equal to 0, satisfying the following conditions*:

1. *$(a_1, ..., a_r)$ are the invariants of an abelian direct factor of G of largest order.*
2. *$n_i \leqslant n_j$ and $m_i \leqslant n_i$, for all $1 \leqslant i \leqslant j \leqslant s$.*
3. *If $T := \max\{n_p, m_j \mid j \leqslant q\}$, then for some p and q, $1 \leqslant p < q \leqslant s$:*
   - *if $\varepsilon = 1$, $c^\varepsilon \geqslant T$; otherwise $c = 1$;*
   - *$n_{p+1} > T + 1$ and $m_j > T + 1$ for all $p < j \leqslant q$.*
4. *G is (isomorphic to) the direct product of an abelian group with invariants $a_1, ..., a_r$, and the amalgamated product of the Q groups $Q(n_i, m_i)$ $(1 \leqslant i \leqslant p)$, the D groups $D(n_j, m_j)$ $(p < j \leqslant q)$, the F groups $F(n_k, m_k)$ $(q < k \leqslant s)$, and possibly a cyclic group of order c^ε and/or $\delta = 0$ or 1 copy of a dihedral group of order 8.*

Moreover, these four lists, thus specified, are a complete set of invariants of the isomorphism class of G.

These invariants will be referred to as the *canonical invariants* of the P_3 group G.

Proof. The existence and uniqueness of the invariants hold in case G is abelian (with $\varepsilon = \delta = p = q = s = 0$) by the basis theorem for abelian groups, or G has exponent four (see Satz III.13.8 in [7]). Thus assume that some generator of G has order larger than 4. By the remarks preceding the theorem assume also without loss of generality that G is a 2-group.

Call an element of G *hard* if u is a power of x, $x^n = u$ (necessarily $n = |x|/2$). Let (4) be any symplectic basis of G in which only at most one central generator of order c is hard, and if there is one such generator, all noncentral generators of order less than c are hard, as in the proof of Lemma 3.3. Let $2n = 2^t$ be the largest order of a hard generator x in (4), say $x^n = u$. For a nonhard generator x_i with $x_i^m = 1$ consider the element $X_i := x^{n/m} x_i$. If $x^{n/m}$ is a central element, the same substitution as in the proof of Lemma 3.3 of X_i for x_i, so that X_i has a coset $X_i G'$ of the same order as x_i and the resulting elements are still a symplectic basis of G, makes X_i a hard generator since $X_i^m = x^n x_i^m = u$. Note that $x^{n/m}$ is a central element if and only if x is central or $n > m$. Likewise, one can substitute the hard central generator by a nonhard generator if x is noncentral and its order $c < 2^t$. Repeating this process, one arrives at a symplectic basis (5) with the following properties:

(a) all central generators are nonhard (and $\varepsilon = 0$), except possibly one of order $c \geqslant 4$ (and so $\varepsilon = 1$); in this case $c = 2^t :=$ largest order of a hard generator;

(b) every generator of order at most $2^{t-2+\varepsilon}$ is hard, which will be called a *canonical basis* of G. The corresponding orders of the cyclic and the various types of two-generator amalgamated factors showed that G can be expressed as described in condition 4 of the theorem. The occurrence of two factors $F(1, 1)$ can be replaced by the amalgamated product of two copies of $Q(2, 2)$, as pointed out after Lemma 3.4.

In order to prove the uniqueness of these invariants, let P be the set of elements of G that can be written as a product of hard elements of G. Clearly P is a normal subgroup of G and it is the largest subgroup of G consisting of hard elements. By the uniqueness of the decomposition of an element in the form (5) and the observations in the second paragraph in the proof of Lemma 3.3, P is generated by the hard elements in any canonical basis, no elements outside P has u as a power, and 2^t is the exponent of P. Now, given any two canonical bases of G, the quotient G/P is an abelian group whose invariants are the orders of the remaining generators in any canonical basis of G, and are therefore uniquely determined invariants of G independently of the canonical basis. Thus to complete the proof of Theorem 3.1 it suffices to show it in case all generators in a canonical basis of G are hard. But in this case, the order of the noncentral canonical generators is twice the order of their cosets in G_{ab}, which are determined up to isomorphism. Hence, the F-, D-, and Q-type amalgamated factors generated by two elements in a canonical basis, and therefore G, are unique up to isomorphism. ∎

4. Complexity of P_3 Group Isomorphism Testing

The structure Theorem 3.1 naturally raises the question of the complexity of testing isomorphism of P_3 groups. In a preliminary version of this paper [2] it was erroneously stated that isomorphism testing of P_3 groups given by presentations is isomorphism complete, but it is P-time if given as multiplication tables. The following result proves that, in fact, both problems are solvable in polynomial time.

THEOREM 4.1. *The canonical invariants of a finite P_3 group given by a presentation can be computed in polynomial time. Thus the isomorphism problem for P_3 group presentations and multiplication tables is solvable in polynomial time.*

It suffices to prove that isomorphism of finite P_3 groups given by presentations can be tested in polynomial time since every multiplication table can be readily translated into a presentation of the same group. All of the constructions that have been used in Section 3 to arrive at the canonical invariants of G can be performed in polynomial time if one has an algorithm to check if two elements of a given P_3 group commute. The following observation settles this question.

LEMMA 4.1. *There is a polynomial time algorithm to check if an arbitrary presentation of a P_3 group is abelian. Therefore there is a polynomial time algorithm to*

check if two elements of any P_3 group commute if given by words on the generators of a presentation.

Proof. Let the presentation $\pi := \langle X | R \rangle$ define a finite P_3 group G on a generating set X given by Eq. (2). Assume without loss of efficiency that X is a basis of G. Find the order n_i of the coset of each generator x_i in the abelianized presentation obtained by adding the relators $[x_i, x_j] = 1$ for $1 \leqslant i \leqslant n$ to π. For each i, find the order of the cyclic group G_i obtained by adding the $n-1$ relators $x_j = x_i^{n_i}$ $(j \neq i)$ to π. It can be easily checked that $|G_i| = |x_i|$ in G, since in the presentation of G_i all x_j have been collapsed to 1 or u. Thus, if G is abelian, the order of F_{ab} equals the product of the orders of the groups G_i. Conversely, if u is a power of at least one of the x_i,

$$|G_{ab}| = \prod_i |x_i G'| < \prod_i |x_i| = \prod_i |G_i|.$$

Therefore if the order of G_{ab} equals the product of the order of the G_i, then G is either abelian or nonabelian but u is not a power of any element in G. Thus G is abelian if and only if the order of H_{ab} equals the product of the orders of the groups H_i as H runs over G and each of the groups H_{ijk} presented by $\langle X | R, [x_i, x_j] = x_k^{n_k} \rangle$.

Finally, two arbitrary elements x, y of G commute if and only if either the given presentation defines an abelian group or the one obtained by adding the relator $[x, y] = 1$ defines a nonabelian group. ∎

Proof of Theorem 4.1. The proofs of Lemmas 3.2–4.1 allow the construction of a symplectic basis and the proof of Theorem 3.1 leads to the canonical invariants of G in polynomial time. The algorithm is as follows.

BEGIN

A. For each presentation,

1. find a basis of the abelianized group G_{ab} (see the algorithm in appendix to chapter VII.2 in [5] or in [8].)
2. use the algorithm of Lemma 4.1 to determine the central generators and the noncentral generators;
3. find a canonical symplectic basis of G by the polynomial time algorithm in the proof of Lemmas 3.2, 4.1, and 3.4.
4. Perform the basis changes indicated in the proof of Theorem 3.1 and thereby find the canonical invariants of G;

B. The two groups are isomorphic if and only if the two sets of invariants are the same.

END

The correctness of the algorithm follows from Theorem 3.1 and the results in Section 3. ∎

It is natural to ask how close Theorem 3 is to being an optimal result. While a complete answer to this question is difficult to give, it has been pointed out by the referee that results in [6] provide a class of 2-nilpotent p-groups testing isomorphism of which is graph isomorphism complete.

5. Further Results

It has been proved in [4, Corollary 2] that most time and space complexity classes contain complete word problems of groups of transformations of the infinite complete binary tree with respect to *logspace*- and *linear*-time reductions. It is not known if a similar result holds for lower complexity classes such as NP. A classical construction by G. Higman can be used to establish the following extension of this result to graph isomorphism. One can associate with an arbitrary graph Γ with adjacency matrix $[a_{ij}]$ a finite P_3 group $\pi(\Gamma)$ with a generating set X in one–one correspondence, with the vertices of Γ defined by the presentation

$$\langle x_1, \ldots, x_n \mid x_i^2 = 1,\ [x_i, x_j] = u(a_{ij} = 1),\ [x_i, x_j, x_k] = 1\ (a_{ij} = 0,\ 1 \leqslant k \leqslant n) \rangle. \quad (7)$$

This group will be referred to as the P_3 *group associated* with G.

Definition 5.1. A finite presentation of a group is (graph) *isomorphism universal* if there exists a function computable in polynomial time which associates to every (finite) graph a word on the generators of the presentation and/or their inverses in such a way that two graphs are isomorphic if and only if their corresponding words represent the same group element, i.e., if the corresponding presentation has a (graph) isomorphism complete word problem. ∎

Theorem 5.1. *There exists an isomorphism universal group presentation.*

Proof. Without loss of generality assume that *labelled* graphs are represented by their adjacency matrices and thus graphs of the same number of vertices can be ordered lexicographically. Enumerate all (finite) labelled graphs $\Gamma_1, \Gamma_2, \Gamma_3, \ldots$ by increasing order and lexicographically for graphs of the same order. Let $\pi(\Gamma_1), \pi(\Gamma_2), \pi(\Gamma_3), \ldots$ be the associated P_3 groups on successive disjoint generating subsets of the countably infinite set $x_1, x_2, \ldots$. Let π'' be the free product with amalgamation (see of [10, Chap. IV]) of this sequence of elementary P_3 groups amalgamating any two isomorphic groups, and let $f(\Gamma_i)$ be the product of the generators of the presentation $\pi(\Gamma_i)$. Embed the group thus recursively presented by π'' into a recursively presented group π' generated by two elements a, t by the encodings

$$b = t^{-1}at, \qquad x_i = t^{-1}b^{-i}ab^{i}ta^{-i}b^{-1}a^{i}. \quad (8)$$

Such a group exists by the classical HNN embedding Theorem 3.1 in [10] due to

Higman–Neumann–Neumann. Because there are at most 2^n labeled graphs of order at most n, $f(\Gamma_i)$ can be encoded in polynomial time as a word on a, t, using the defining words (8) and a binary representation for the subindices involved. Now, since π' is a recursively presented group, the Higman–Valiev embedding theorem (cf. [10, 16]) can be applied to embed π' as a subgroup of a finitely presented group π with a polynomially equivalent word problem. Thus it suffices to show that two graphs are isomorphic if and only if the corresponding words on a, t represent the same group element. But this is clear from the construction of π, the normal form for words in a free product with amalgamation (see in [10, Sect. IV.2]), and the above encoding. ∎

ACKNOWLEDGMENTS

The authors thank G. Higman, L. Babai, and the anonymous referee for pointing out errors in a preliminary version of Theorem 3.1 and for suggestions that improved the presentation of the paper. Thanks also to I. D. Macdonald for a careful reading of an earlier version of the corrected manuscript.

REFERENCES

1. M. CURZIO, P. LONGOBARDI, AND M. MAJ, Su di un problema combinatorio in teoria dei gruppi, *Atti Lincei VIII* **74** (1983), 136–142.
2. M. GARZON AND Y. ZALCSTEIN, Complexity of isomorphism testing, *in* "27th FOCS, Toronto, 1986," pp. 313–321.
3. M. GARZON AND Y. ZALCSTEIN, On permutation properties in groups and semigroups, *Semigroup Forum* **35** (1987), 337–351.
4. M. GARZON AND Y. ZALCSTEIN, The complexity of Grigorchuk groups with application to cryptography, *Theoret. Comput. Sci.* **91** (1992) to appear.
5. T. HUNGERFORD, "Algebra," Springer-Verlag, Berlin/New York, 1980.
6. H. HEINEKEN AND H. LIEBECK, The occurrence of finite groups in the automorphism group of nilpotent groups of class 2, *Arch. Math.* **25** (1974), 8–16.
7. B. HUPPERT, "Endliche Gruppen, I," Springer-Verlag, Berlin, 1967.
8. R. KANNAN AND A. BACHEM, Polynomial algorithms for computing the Smith and Hermite normal forms of an integer matrix, *SIAM J. Comput.* **8**, No. 4 (1979), 499–507.
9. R. J. LIPTON, L. SNYDER, AND Y. ZALCSTEIN, Complexity of the word and isomorphism problems for finite groups, *in* "Proceedings, Conf. on Inform. Sci. and Systems," pp. 33–35, Johns Hopkins University, 1976.
10. R. LYNDON AND P. E. SCHUPP, "Combinatorial Group Theory," Springer-Verlag, Berlin/New York, 1977.
11. W. MAGNUS, A. KARRASS, AND D. SOLITAR, "Combinatorial Group Theory," Dover, New York, 1965.
12. A. RESTIVO AND C. REUTENAUER, On the Burnside Problem for semigroups, *J. Algebra* **89** (1984), 102–104.
13. A. RESTIVO AND C. REUTENAUER, Rational languages and the Burnside Problem, *Theoret. Comput. Sci.* **40**, No. 1 (1985), 13–30.
14. D. J. S. ROBINSON, "A Course in the Theory of Groups," Springer-Verlag, Berlin/New York, 1982.
15. R. E. TARJAN, unpublished.
16. M. VALIEV, "On Polynomial Reducibility of Word Problems under Embedding of Recursively Presented Groups in Finitely Presented Groups," Springer-Verlag LNCS 32, pp. 432–438.