CALIBRATING WORD PROBLEMS OF GROUPS VIA THE COMPLEXITY OF EQUIVALENCE RELATIONS

ANDRÉ NIES AND ANDREA SORBI

ABSTRACT. (1) There is a finitely presented group with a word problem which is a uniformly effectively inseparable equivalence relation. (2) There is a finitely generated group of computable permutations with a word problem which is a universal co-computably enumerable equivalence relation. (3) Each c.e. truth-table degree contains the word problem of a finitely generated group of computable permutations.

1. INTRODUCTION

Given two equivalence relations R, S on the set ω of natural numbers, we say that R is *computably* reducible to S (or, simply, R is reducible to S; notation: $R \leq S$) if there exists a computable function f such that, for every $x, y \in \omega$,

$$x \ R \ y \Leftrightarrow f(x) \ S \ f(y)$$

The first systematic study of this reducibility on equivalence relations is implicit in Ershov [13, 14]. Recently this reducibility has been successfully applied to classify natural problems arising in mathematics and computability theory: see for instance in [11, 15, 16].

In classifying objects according to their relative complexity, an important role is played by objects that are universal, or complete, with respect to some given class. We are interested in this notion for the case of equivalence relations on ω .

Definition 1.1. Let \mathcal{A} be a class of equivalence relations. An equivalence relation $R \in \mathcal{A}$ is called \mathcal{A} -universal, (also sometimes called \mathcal{A} -complete) if $S \leq R$ for every $S \in \mathcal{A}$.

For instance, by Fokina et al. [16] the isomorphism relation for various familiar classes of computable structures is Σ_1^1 -universal, and by Fokina, Friedman and Nies [15] the relation of computable isomorphism of c.e. sets is Σ_3^0 -universal. Ianovski et al. [20, Theorem 3.5] provide a natural example of a Π_1^0 -universal equivalence relation, namely equality of unary quadratic time computable functions. In contrast, they show [20, Corollary 3.8] that there is no Π_n^0 -universal equivalence relation for n > 1.

In this paper we are interested in Σ_1^0 -universal and in Π_1^0 -universal equivalence relations arising from group theory. They arise naturally via word problems, if we view the word problem of a group as the equivalence relation that holds for two terms if they denote the same group element.

In Theorem 3.2 we will build a finitely presented group with a word problem as follows: each pair of distinct equivalence classes is effectively inseparable in a uniform way. Since this property for ceers implies Σ_1^0 -universality (see [1]), it follows that the word problem is Σ_1^0 -universal.

¹⁹⁹¹ Mathematics Subject Classification. 03D45.

Key words and phrases. Word problem of groups, equivalence relations, computable reducibility.

Nies is partially supported by the Marsden fund of New Zealand. Sorbi is a member of INDAM-GNSAGA; he was partially supported by Grant 3952/GF4 of the Science Committee of the Republic of Kazakhstan, and by PRIN 2012 "Logica Modelli e Insiemi ".

Finitely generated (f.g.) groups of computable permutations are special cases of f.g. groups with a co-c.e. set of relators. The word problem of any finitely generated (f.g.) group of computable permutations is Π_1^0 . Using the theory of numberings, Morozov [26] built an example of a f.g. group with Π_1^0 word problem that is not isomorphic to a f.g. group of computable permutations. (We conjecture that future research might provide a natural example of such a group, generated for instance by finitely many computable isometries of the Urysohn space.) As our second main result, in Theorem 5.1 we will build a f.g. group of computable permutations with a Π_1^0 -universal word problem. Thus, within the groups that have a Π_1^0 word problem, the maximum complexity of the word problem is already assumed within the restricted class of f.g. groups of computable permutations. By varying the methods, in Theorem 5.2 we show that every c.e. truth-table degree contains the word problem of a 3-generated group of computable permutations.

We include a number of open questions. Is the computably enumerable equivalence relation of isomorphism among finitely presented groups recursively isomorphic to equivalence of sentences under Peano arithmetic? What is the complexity of embedding and isomorphism among f.g. groups of (primitive) recursive permutations? A natural guess would be Σ_3^0 -universality.

2. Background and preliminaries

Group theory. Group theoretic terminology and notations are standard, and can be found for instance in [21]. Throughout let F(X) be the free group on X, consisting of all reduced words of letters from $X \cup X^{-1}$, with binary operation induced by concatenation and cancellation of x with x^{-1} , and the empty string as identity; see [21, p.89] for notations and details. It is customary to write $F(x_1, \ldots, x_k)$ if $X = \{x_1, \ldots, x_k\}$ is finite. The symbol \cong denotes isomorphism of groups, and, for a group H and a set $S \subseteq H$, by $\operatorname{Ncl}_H(S)$ one denotes the normal closure of S in H; if H is clear from the context one writes $\operatorname{Ncl}(S)$. A presentation of a group G is a pair $\langle X; R \rangle$ with $R \subseteq F(X)$ such that $G \cong F(X)/\operatorname{Ncl}_{F(X)}(R)$. It is legitimate to write $G = \langle X; R \rangle$ since the presentation identifies G up to group isomorphism. The congruence corresponding to the normal subgroup $\operatorname{Ncl}_{F(X)}(R)$ will be written as $=_G$; the relation $=_G$ is clearly an equivalence relation on F(X), which we will call the *word problem* of $G = \langle X; R \rangle$. If X is a finite set then we can encode the elements of F(X) by natural numbers, and multiplication becomes a binary computable function. A group $G = \langle X; R \rangle$ is finitely presented (f.p.) if both X and R are finite. It is easy to see (under coding) that in this case, $=_G$ is a computably enumerable equivalence relation on ω .

Our terminology is slightly nonstandard because by the word problem of a f.p. group $G = \langle X; R \rangle$, one usually means the equivalence class $[1]_G$, and the problem of deciding, for a given word $w \in F(X)$, whether $w \in [1]_G$. The difference is minor, though, since $=_G$ and the set $[1]_G$ are *m*-equivalent. The 1-reduction $x \mapsto \langle x, 1 \rangle$ shows that $[1]_G \leq_1 =_G$ (where the symbol \leq_1 denotes 1-reducibility), and the *m*-reduction $\langle x, y \rangle \mapsto xy^{-1}$ shows that $=_G \leq_m [1]_G$ (where the symbol \leq_m denotes *m*-reducibility).

Effective inseparability. The reader is referred to [28] for any unexplained notation and terminology from computability theory. A partial computable function which is total is simply called a computable function. If $A, B \subseteq \omega$, one writes $A \equiv B$ if there exists a computable permutation f of ω such that f(A) = B; if (A, B) and (C, D) are disjoint pairs of subsets of ω , one writes $(A, B) \equiv (C, D)$, if there exists a computable permutation f of ω such that f(A) = C and f(B) = D. We recall that a disjoint pair of sets (A, B) is called *recursively inseparable* if there is no recursive set X such that $A \subseteq X$ and $B \subseteq X^c$, where X^c denotes the complement of X. The following property is stronger: (A, B) is *effectively inseparable* (e.i.) if there is *productive* function, that is, a partial computable function $\psi(u, v)$ such that

$$(\forall u, v) [A \subseteq W_u \& B \subseteq W_v \& W_u \cap W_v = \emptyset \Rightarrow \psi(u, v) \downarrow \notin W_u \cup W_v].$$

Remark 2.1. It is well known (see e.g. [28, II.4.13]) that if (A, B) and (C, D) are disjoint pairs of c.e. sets then:

- (C, D) e.i. implies $(A, B) \leq_1 (C, D)$;
- if both pairs are e.i. then $(A, B) \equiv (C, D)$;
- if $(A, B) \leq_m (C, D)$ and (A, B) is e.i. then (C, D) is e.i. as well;
- if $A \subseteq C$, $B \subseteq D$ and (A, B) is e.i. then (C, D) is e.i. as well.

The following fact about e.i. pairs of c.e. sets will be used in the proof of Theorem 3.2.

Lemma 2.2. If (A, B) and (C, D) are e.i. pairs of c.e. sets, then so is the pair $(A \times C, B \times D)$. Moreover, a productive function for $(A \times C, B \times D)$ can be found uniformly from productive functions for (A, B) and (C, D).

Proof. We prove in fact that if (A, B) is a disjoint pair of c.e. sets, and (C, D) is e.i., then $(A, B) \leq_1 (A \times C, B \times D)$: hence, if (A, B) is e.i., then $(A \times C, B \times D)$ is e.i. as well. Let g be a computable function such that $g(A) \subseteq C$ and $g(B) \subseteq D$; such a function exists because $(A, B) \leq_1 (C, D)$. Clearly the 1-1 computable function

$$f(x) = \langle x, g(x) \rangle$$

provides a 1-reduction showing that $(A, B) \leq_1 (A \times C, B \times D)$.

The claim about uniformity is straightforward.

Although not used in this paper, it is worth noting that a statement analogous to the lemma above holds when we replace "effectively inseparable" by the weaker notion of being recursively inseparable.

Proposition 2.3. If (A, B) and (C, D) are recursively inseparable pairs of c.e. sets, then so is $(A \times C, B \times D)$.

Proof. Assume that R is a computable set such that $A \times C \subseteq R$ and $B \times D \subseteq R^c$. For every v, let

$$R_v = \{ x : \langle x, v \rangle \in R \}.$$

We observe that for every v there exists $x \in A$ such that $\langle x, v \rangle \in R^c$, or there exists $x \in B$ such that $\langle x, v \rangle \in R$; otherwise $A \subseteq R_v$ and $B \subseteq R_v^c$, which would contradict the inseparability of (A, B). Let R_A and R_B be computable binary relations such that

$$(\exists x)[x \in A \& \langle x, v \rangle \in R^c] \Leftrightarrow (\exists s)R_A(v, s), (\exists x)[x \in B \& \langle x, v \rangle \in R] \Leftrightarrow (\exists s)R_B(v, s),$$

and define

$$U = \{v : (\exists s) [R_A(v, s)] \& (\forall t \le s) \neg R_B(v, t)] \}.$$

The set U is decidable, as we have seen that for every v, there exists $x \in A$ such that $\langle x, v \rangle \in R^c$, or there exists $x \in B$ such that $\langle x, v \rangle \in R$. Now $v \in C \cap U$ implies $(\exists x)[x \in A \& \langle x, v \rangle \in R^c]$ contrary to $A \times C \subseteq R$. Similarly, $v \in D \setminus U$ implies $(\exists x)[x \in B \& \langle x, v \rangle \in R]$, contrary to $B \times D \subseteq R^c$. We conclude that $C \subseteq U^c$ and $D \subseteq U$, which is the final contradiction.

C.e. equivalence relations and word problems. Computably enumerable equivalence relations have been studied extensively; see for instance [5, 12, 18]. While they are called *positive* in the Russian literature, we call such an equivalence relation a *ceer* following Andrews et al. [1]. Σ_1^0 -universal ceers arising naturally in formal logic have been pointed out in papers by Montagna and others [4, 25, 29].

Definition 2.4 ([3]). A cere *E* is called *uniformly effectively inseparable* (*u.e.i.*) if there is a computable binary function *p* such that, whenever $a \not E b$, the partial computable function $\psi(u, v) = \varphi_{p(a,b)}(u, v)$ witnesses that the pair of equivalence classes $([a]_E, [b]_E)$ is e.i.

As already observed in the introduction, it is shown in [1] that every u.e.i. ceer is Σ_1^0 -universal. It is worth recalling that uniformity plays a crucial role in yielding universality, as there are nonuniversal ceers yielding a partition of ω into effectively inseparable pairs of distinct classes [1].

Surprisingly, f.p. groups with a Σ_1^0 -universal word problem appeared in the literature prior to any explicit study of computable reducibility among equivalence relations. Charles F. Miller III [24] proved that there exists a f.p. group with Σ_1^0 -universal word problem. He shows that another interesting equivalence relation is Σ_1^0 -universal: the isomorphism relation between finite presentations of groups, which (via encoding of finite presentations by numbers) can be seen as a ceer. Not knowing of this much earlier result, Ianovski, Miller, Ng, and Nies [20, Question 6.1] had recently posed this as an open question.

Theorem 2.5 ([24]).

(1) Given a cere E one can effectively build a f.p. group $G_E = \langle X; R \rangle$, and a computable sequence of words $(w_i)_{i \in \omega}$ in F(X) such that, for every i, j,

$$i E j \Leftrightarrow w_i =_{G_E} w_j.$$

(2) Given a finite presentation $\langle X; R \rangle$ of a group G one can effectively find a computable family $(H_w^G)_{w \in F(X)}$ of f.p. groups such that, for all $v, w \in F(X)$,

$$v =_G w \Leftrightarrow H_v^G \cong H_w^G$$

Proof. The first item is obtained in [24, p 90f], used as a preliminary step to prove Theorem V.2. The second item is [24, Theorem V.1]. \Box

Corollary 2.6.

- (1) There exists a f.p. group G such that $=_G$ is a Σ_1^0 -universal ceer.
- (2) The isomorphism problem $\cong_{f.p.}$ between finite presentations of groups is a Σ_1^0 -universal ceer.

Proof. Let E be a Σ_1^0 -universal ceer. Then

- (1) by Theorem 2.5(1), $E \leq =_{G_E}$, and thus $=_{G_E}$ is Σ_1^0 -universal;
- (2) by Theorem 2.5(2),

$$i E j \Leftrightarrow H_v^{G_E} \cong H_w^{G_E}.$$

This shows that $E \leq \cong_{f.p.}$, whence $\cong_{f.p.}$ is Σ_1^0 -universal.

We observe that Σ_1^0 -universality of the word problem does not necessarily imply being u.e.i.

Theorem 2.7. There exists a f.p. group G such that $=_G$ is Σ_1^0 -universal, but not u.e.i.

Proof. We build a f.p. group G such that $=_G$ is Σ_1^0 -universal, but it does not even yield a partition into recursively inseparable pairs of disjoint equivalence classes. To see this, let $H = \langle X; R \rangle$ be a f.p. group such that $=_H$ is Σ_1^0 -universal. Let $v \notin X$ be a new letter. The free product G = H * F(v)(where F(v) is the free group on v) has the finite presentation $\langle X, v; R \rangle$. Since H can be seen as a subgroup of G and the embedding is computable, the group G has Σ_1^0 -universal word problem. Any word $w \in F(X \cup \{v\})$ can be uniquely written as $w = h_1 v^{n_1} h_2 \cdots v^{n_r} h_{r+1}$, with $h_j \in F(X)$ and $n_j \neq 0$, for all j. Let

$$n_v(w) = n_1 + \dots + n_r$$

be the exponent sum of v in w, and let $S = \{w \in F(X \cup \{v\}) : n_v(w) = 0\}$. It is immediate that $[1]_G \subseteq S$ and $[v]_G \subseteq S^c$, so the recursive set S separates the pair $([1]_G, [v]_G)$.

The proof of the previous theorem suggests an additional comment. We observe that if in a group G the operations are computable, then all $=_G$ -equivalence classes are uniformly computably isomorphic: the function $w \mapsto wu^{-1}v$ is a computable permutation of the group (uniformly depending on u, v) which maps $[u]_G$ onto $[v]_G$. Thus if an equivalence class $[u]_G$ is creative, so is any other equivalence class $[v]_G$, and creativeness holds uniformly, i.e. there is a computable function p such that, for every v, $\varphi_{p(v)}$ is productive for the complement of $[v]_G$. Nothing like this holds for effective inseparability, or for computable inseparability. Indeed, one can take the group H considered in the proof of Theorem 2.7 to be such that its word problem yields at least a pair of effectively inseparable classes (for instance take H = D, where D is the group built in Theorem 3.2 in which all distinct pairs of equivalence classes are effectively inseparable). Thus the word problem of the group G of Theorem 2.7 does have effectively inseparable classes, but not all pairs are so, since there are pairs which can be computably separated.

3. A FINITELY PRESENTED GROUP WITH U.E.I. WORD PROBLEM

We now build a f.p. group with a word problem that is a u.e.i. ceer. We first provide Lemma 3.1 that if G is a f.p. group containing a word w such that $([1]_G, [w]_G)$ is e.i., then all disjoint pairs $([s]_G, [t]_G)$ with $s, t \in \operatorname{Ncl}_G(w)$ are e.i. in a uniform way. For the main construction, using a result of Miller III, we take a computably presented group A containing a word w such that the pair $([1]_A, [w]_A)$ is e.i. By the Higman Embedding Theorem combined with a construction due to Rabin, we embed A into a f.p. group D so that if N is a non-trivial normal subgroup of D, with $w \in N$, then N = D. Taking $N = \operatorname{Ncl}_D(w)$ and observing that the pair $([1]_D, [w]_D)$ is also e.i., the lemma shows that $=_D$ is u.e.i.

Lemma 3.1. Let $G = \langle X; R \rangle$ be a given f.p. group, and let w be an element of F(X) such that $([1]_G, [w]_G)$ is e.i. Let $N = \text{Ncl}_G(w)$. For $s, t \in N$ such that $s \neq_G t$, the pair of sets $([s]_G, [t]_G)$ is e.i. uniformly in s, t.

Proof. Since $([s]_G, [t]_G) \equiv ([1]_G, [s^{-1}t]_G)$, it suffices to show that $([1]_G, [r]_G)$ is uniformly e.i. for any $r \in N \setminus [1]_G$. Note that N consists of the products of conjugates of w and of w^{-1} , so it is enough to show:

- (1) if $([1]_G, [u]_G)$ is e.i., then so is $([1]_G, [u^{-1}]_G)$: this follows from the fact that $([1]_G, [u]_G) \equiv ([u^{-1}]_G, [1]_G)$, via the computable permutation $x \mapsto u^{-1}x$;
- (2) if $([1]_G, [u]_G)$ is e.i., then so is $([1]_G, [g^{-1}ug]_G)$ for every $g \in G$: the computable permutation $x \mapsto g^{-1}xg$ provides an isomorphism $([1]_G, [u]_G) \equiv ([1]_G, [g^{-1}ug]_G)$;

(3) if $uv \neq_G 1$ and the pairs $([1]_G, [u]_G)$ and $([1]_G, [v]_G)$ are e.i., then $([1]_G, [uv]_G)$ is e.i.: By Lemma 2.2 the pair $([1]_G \times [1]_G, [u]_G \times [v]_G)$ is e.i. On the other hand, let

$$X = \{ \langle w, z \rangle : wz \in [1]_G \}, Y = \{ \langle w, z \rangle : wz \in [uv]_G \}.$$

Then $[1]_G \times [1]_G \subseteq X$ and $[u]_G \times [v]_G \subseteq Y$, and thus, by Remark 2.1, (X, Y) is e.i. Since $(X, Y) \leq_m ([1]_G, [uv]_G)$ via the mapping $\langle w, z \rangle \mapsto wz$, it follows that $([1]_G, [uv]_G)$ is e.i., as desired.

Each step provides being e.i. in a uniform fashion. If $r \in N$ we can obtain its representation as a product of conjugates of w and of w^{-1} effectively. Since $[1]_G$ and N are c.e., there is a partial computable function p such that $\varphi_{p(a,r)}$ is productive for $([a]_G, [r]_G)$, when $a \in [1]_G$ and $r \in N \setminus [1]_G$. So $([1]_G, [r]_G)$ is e.i. uniformly in r, whence $([s]_G, [t]_G)$ is e.i. uniformly in s, t as required. \Box

Theorem 3.2. There exists a f.p. group D such that $=_D$ is u.e.i.

Proof. For elements u, t of a group, we write $Cj(u, t) = t^{-1}ut$. Following [23], take an e.i. pair (Y_0, Y_1) of c.e. sets. Let F = F(c, d) be the free group on two generators c, d; for every i > 0, let

$$b_{i-1} = \operatorname{Cj}(\operatorname{Cj}(c, d^{-1}), c^i) \cdot \operatorname{Cj}(\operatorname{Cj}(\operatorname{Cj}(c^{-1}, d), c^i), d^{-2})$$

Next let

$$R = \operatorname{Ncl}_F(\{b_0 b_i^{-1} : i \in Y_0\} \cup \{b_1 b_j^{-1} : j \in Y_1\}),$$

and let $A = \langle c, d; R \rangle$. Note that A is a *computably presented* group, namely A has a presentation $\langle Z; T \rangle$ where Z is finite and T is c.e. It can be shown [23] that the computable mapping $i \mapsto b_i$ provides a reduction

$$(Y_0, Y_1) \leq_1 ([b_0]_A, [b_1]_A)$$

Hence, by the third item in Remark 2.1, the pair $([b_0]_A, [b_1]_A)$ is e.i. We now follow a line of argument as in the proof of Theorem IV.3.5 of [22], to which the reader is referred to fill in the details of the present proof; the only difference between our proof and that in [22] is that we first embed A into a f.p. group L, aiming at a final f.p. group D, whereas in the proof of Theorem IV.3.5 of [22] the starting group C is first embedded into a countable simple group S, as the goal in that case is to end up with a finitely generated simple group. (The construction provided by Theorem IV.3.5 of [22] is due to Rabin [27]; the version presented in [22] is modelled on Miller III [24].)

By the Higman Embedding Theorem ([19]; see also [22, Theorem IV.7.1]) the computably presented group A can be embedded into a f.p. group L; next embed, using [22, Theorem IV.3.1], the free product L * F(x) (with x a new generator) in a f.p. group U, generated by u_1 and u_2 both of infinite order.

In order to build the desired f.p. group D, we are now going to introduce additional groups, using two well known combinatorial group theoretic constructions, namely HNN-extension (where HNN stands for Higman-Neumann-Neumann), and free product with amalgamation. We briefly recall these two constructions. If $G = \langle T; Z \rangle$ is a group presentation, and $\varphi : H \to K$ is an isomorphism between subgroups of G, then the HNN-extension of G, relative to H, K and φ , is the group $\langle T, p; Z \cup \{p^{-1}hp = \varphi(h) : h \in H\}\rangle$, of which G is a subgroup, and p (with $p \notin G$) realizes by conjugation the given isomorphism; p is called the stable letter. It is clear that one can limit oneself to let the added relations vary on a set of generators of H, instead of adding one relation for each $h \in H$. Moreover, if $G_1 = \langle T_1; Z_1 \rangle$, $G_2 = \langle T_2; Z_2 \rangle$ are group presentations of disjoint groups, with two isomorphic subgroups H_1, H_2 , via isomorphism $\varphi : H_1 \to H_2$, then their free product amalgamating H_1 and H_2 by φ is the group $\langle T_1 \cup T_2; Z_1 \cup Z_2 \cup \{h = \varphi(h : h \in H\}\rangle$, which is intuitively the "freest" overgroup of both G_1 and G_2 in which their subgroups are identified. Again, it is clear that one can limit oneself to let the added relations vary on a set of generators of H_1 , instead of adding one relation for each $h \in H_1$. For more on these constructions, see [22].

Consider the groups

$$\begin{split} J &= \langle U, y_1, y_2; y_1^{-1} u_1 y_1 = u_1^2, y_2^{-1} u_2 y_2 = u_2^2 \rangle, \\ K &= \langle J, z; z^{-1} y_1 z = y_1^2, z^{-1} y_2 z = y_2^2 \rangle, \\ P &= \langle r, s; s^{-1} r s = r^2 \rangle, \\ Q &= \langle r, s, t; s^{-1} r s = r^2, t^{-1} s t = s^2 \rangle. \end{split}$$

The group J is the (double) HNN-extension of U with stable letters y_1, y_2 , where for each $i \in \{1, 2\}$, y_i realizes by conjugation the isomorphism induced by $u_i \mapsto u_i^2$, between the subgroups generated by u_i , and by u_i^2 , respectively; K is the HNN-extension of J, with stable letter z, realizing by conjugation the isomorphism induced by $y_1 \mapsto y_1^2$ and $y_2 \mapsto y_2^2$, between the subgroups generated by y_1, y_2 , and by y_1^2, y_2^2 , respectively; P is the HNN-extension of F(r), with stable letter s, realizing by conjugation the isomorphism induced by $r \mapsto r^2$, between the subgroups generated by r, and by r^2 , respectively; Q is the HNN-extension of P, with stable letter t, realizing by conjugation the isomorphism induced by $r \mapsto r^2$, between the subgroups generated by r, and by r^2 , respectively; Q is the HNN-extension of P, with stable letter t, realizing by conjugation the isomorphism induced by $r \mapsto r^2$, between the subgroups generated by r, and by r^2 , respectively; Q is the HNN-extension of P, with stable letter t, realizing by conjugation the isomorphism induced by $r \mapsto r^2$, between the subgroups generated by r, and by r^2 , respectively; Q is the HNN-extension of P, with stable letter t, realizing by conjugation the isomorphism induced by $s \mapsto s^2$, between the subgroups generated by s, and by s^2 , respectively. It is shown in the proof of [22, Theorem IV.3.4] that r, t freely generate a subgroup of Q. Let $w \in L$, with $w \neq_L 1$: since the commutator [w, x] has infinite order in U, an argument similar to the one used for r, t, and Q (see again [22]) shows that [w, x] and z freely generate a subgroup of K. Thus, one can form the free product with amalgamation

$$D = \langle K * Q; r = z, t = [w, x] \rangle.$$

All groups mentioned are finitely presented except for A. We summarize the chains of embeddings provided by the constructions:

As pointed out in the proof of [22, Theorem IV.3.4], if $N \triangleleft D$ and $w \in N$, then w = 1 in the quotient D/N. Then [w, x] = 1 in this quotient. Using the relators, we conclude that t = 1, s = 1, r = 1, z = 1, $y_1 = 1$, $y_2 = 1$, $u_1 = 1$ and $u_2 = 1$. Therefore the quotient is trivial, and hence N = D.

Keeping track of the images of the generators c, d of A into D, under the chain of embeddings leading from A to D, one sees that there is a computable function k from F(c, d) into F(X), where X is the set of generators of D in the exhibited presentation of D. Let us identify k(a) with a, for all $a \in F(c, d)$. Since, under this identification, $[b_0]_A \subseteq [b_0]_D, [b_1]_A \subseteq [b_1]_D$, and $([b_0]_A, [b_1]_A)$ is e.i., it follows that $([b_0]_D, [b_1]_D)$ is e.i. by the last item in Remark 2.1. Let $w = b_1^{-1}b_0$. Via embeddings, the word w can be thought of as lying in L, with $w \neq_L 1$, and hence in D. The pair $([1]_D, [w]_D)$ is e.i., and by Lemma 3.1, the normal closure $N = \text{Ncl}_D(w)$ satisfies the property that all pairs $([s]_D, [t]_D)$ of disjoint equivalence classes of N are e.i., uniformly in s, t. Since $w \in N$, it follows that N = D. Therefore D is a f.p. group with u.e.i. word problem. \Box

4. DIAGONAL FUNCTIONS

A diagonal function for an equivalence relation E is a computable function δ such that $a \not E \delta(a)$, for all a. In this section we apply diagonal functions to ceers arising from group theory, and pose some related open questions. Following [25], a ceer E is uniformly finitely precomplete if there exists a computable function f(D, e, x) such that for all D, e, x, with D a finite set. (Here, and in the following, when given as an input to a computable function, a finite set will be always identified with its canonical index.)

$$\varphi_e(x) \downarrow \in [D]_E \Rightarrow f(D, e, x) \mathrel{E} \varphi_e(x),$$

where $[D]_E$ is the *E*-closure of *D*. An important example of a uniformly finitely precomplete ceer is provable equivalence in Peano Arithmetic, i.e. the ceer \sim_{PA} defined by $\lceil \sigma \rceil \sim_{PA} \lceil \tau \rceil$ if and only if $\vdash_{PA} \sigma \leftrightarrow \tau$. Here σ, τ are sentences of *PA*, and we refer to some computable bijection $\lceil \rceil$ of the set of sentences with ω . A diagonal function is given by $\delta(\sigma) = \neg \sigma$.

Ceers E and F are called *computably isomorphic* if there exists a computable permutation p of ω such that p(E) = F. The notions of a diagonal function and a uniformly finitely precomplete ceer play an important role in the study and classification of Σ_1^0 -universal ceers.

Proposition 4.1 ([25]). (i) Every uniformly finitely precomplete ceer is u.e.i.

(ii) A ceer E is computably isomorphic to \sim_{PA} if and only if E is uniformly finitely precomplete and E has a diagonal function.

A strong diagonal function for an equivalence relation E is a computable function δ such that $\delta(D) \notin [D]_E$, for every finite set D. And rews and Sorbi [2] have shown that every u.e.i. ceer with a strong diagonal function is uniformly finitely precomplete, and therefore computably isomorphic to \sim_{PA} .

Suppose a f.p. group $G = \langle X; R \rangle$ is nontrivial, say $w \neq_G 1$ for some $w \in F(X)$. Then $=_G$ has a diagonal function, namely the map $\delta(r) = rw$ $(r \in F(x))$. It would be interesting to prove that there exists a f.p. group G such that $=_G$ is uniformly finitely precomplete, for this would yield an example of a word problem of a f.p. group which is computably isomorphic to \sim_{PA} . To show this, one can try to strengthen Theorem 3.2 to provide a f.p. group G such that $=_G$ is u.f.p., or, equivalently, to extend its proof in order to provide a f.p. group G such that $=_G$ is u.e.i. and G has a strong diagonal function. Thereafter one can use the above-mentioned result of Andrews and Sorbi [2]. We do not know at present how to do carry out this plan.

Proposition 4.2. The isomorphism problem $\cong_{f.p.}$ between finite presentations of groups has a strong diagonal function.

Proof. Uniformly in a finite presentation $G = \langle x_1, \ldots, x_n; r_1, \ldots, r_k \rangle$, the abelianization G_{ab} has the finite presentation

$$G_{ab} = \langle x_1, \dots, x_n; r_1, \dots, r_k, |x_i, x_j| : 1 \le i < j \le n \rangle,$$

where $[u, v] = u^{-1}v^{-1}uv$ is the usual commutator of u, v. Given a finite set $S = \{G_1, \ldots, G_r\}$ of finite presentations, let $\delta(S)$ be the canonical finite presentation of the abelian group $H = \mathbb{Z} \times \prod_{1 \leq u \leq r} (G_u)_{ab}$. Then $H \not\cong G_u$ for each u. For, if G_u is abelian, then the torsion free rank of H exceeds that of G_u .

We note that, via a less elementary method involving the Grushko-Neumann Theorem (see [22, p. 178]), one could also simply let H be the amalgam of \mathbb{Z} and all the G_u .

We conjecture that $\cong_{f.p.}$ is uniformly finitely precomplete, and hence computably isomorphic to \sim_{PA} . In view of the foregoing proposition it would suffice to show that the ceer $\cong_{f.p.}$ is u.e.i. By a result of Rabin, every equivalence class of $\cong_{f.p.}$ is creative; see [22, p. 193].

5. Π_1^0 -universality and groups of computable permutations

We use the following notation: the product $\alpha\beta$ of two permutations on some set S is the permutation $\alpha\beta(s) = \beta(\alpha(s))$ where $s \in S$.

Theorem 5.1. There is a f.g. group of computable permutations with a Π_1^0 -universal word problem.

Proof. Given a Π_1^0 equivalence relation E, by [20, Prop. 3.1] there is a computable binary function f such that

$$x E y \Leftrightarrow (\forall n)[f(x, n) = f(y, n)]$$

The construction of f shows that $f(x, n) \leq x$ for each x, n.

Via a computable bijection we identify $\mathbb{Z} \times \omega$ with ω . We think of the domain of our computable permutations as a disjoint union of pairs of "columns"

$$C_x^i = \{2x+i\} \times \omega,$$

where $i = 0, 1, x \in \mathbb{Z}$ for the rest of this proof.

The first two of the three computable permutations σ, τ, α we are about to define do not depend at all on f. The permutation σ shifts C_x^i to C_{x+1}^i :

$$\sigma(\langle 2x+i,n\rangle) = \langle 2x+2+i,n\rangle.$$

The permutation τ exchanges C_0^i with C_0^{1-i} and is the identity elsewhere:

$$\tau(\langle i, n \rangle) = \langle 1 - i, n \rangle$$

We now define a computable permutation α coding f in the sense that there exists a fixed computable sequence $(t_x(\alpha, \sigma, \tau))_{x \in \omega}$ in the free group generated by symbols α, σ, τ , such that for each $x, y \in \omega$,

(5.1)
$$\forall n f(x, n) = f(y, n) \Leftrightarrow t_x = t_y,$$

where equality $t_x = t_y$ is in the group generated by the three permutations. For each n, the permutation α has a cycle of length f(x, n) in the interval $n(x+1), \ldots, (n+1)(x+1) - 1$ of C_x^0 . Thus, for each $x, n \in \omega$ and $k \leq x$,

$$\alpha(\langle 2x, n(x+1)+k\rangle) = \begin{cases} \langle 2x, n(x+1)+k+1\rangle & \text{if } k < f(x,n) \\ \langle 2x, n(x+1)\rangle & \text{if } k = f(x,n) \\ \langle 2x, n(x+1)+k\rangle & \text{otherwise,} \end{cases}$$

and α is the identity on the remaining columns. We now define the terms t_x for $x \in \omega$. The permutation $t_x(\alpha, \sigma, \tau)$ will only retain the encoding of the values f(x, n), and erase all other information. It also moves this information to the pair of columns C_0^0, C_0^1 . In this way we can compare the values f(x, n) and f(y, n) applying t_x and t_y to α, σ, τ .

Recall that for elements u, t of a group we write $Cj(u, t) = t^{-1}ut$. We let

$$t_x = \operatorname{Cj}(\alpha, \sigma^{-x})\tau\operatorname{Cj}(\alpha^{-1}, \sigma^{-x}).$$

Let α_x be the permutation given by $\alpha(\langle 2x, y \rangle) = \langle 2x, \alpha_x(y) \rangle$. Using that everything cancels except what α codes on the column C_x^0 , we obtain

$$t_x(\langle u, y \rangle) = \begin{cases} \langle u, y \rangle, & \text{if } u \neq 0, 1, \\ \langle 1, \alpha_x(y) \rangle, & \text{if } u = 0, \\ \langle 0, (\alpha_x)^{-1}(y) \rangle, & \text{if } u = 1. \end{cases}$$

By the definition of α it is now clear that (5.1) is satisfied.

In the area of computational complexity, one writes input numbers in binary and considers time bounds compared to their length. A quadratic time variant G of the function f encoding the equivalence relation E is obtained in [20, Theorem 3.5]. Some modifications to the proof above yield three permutations that are polynomial time computable, as are their inverses, and they still generate a group with Π_1^0 -universal word problem.

Independently Fridman [17], Clapham [9] and Boone [6, 7, 8] proved that each c.e. Turing degree contains the word problem of a f.p. group. (Here and throughout next theorem and its proof, "word problem" is meant classically as the equivalence class of the identity element). Later Collins [10] extended this to c.e. truth table degrees. In contrast, Ziegler [30] constructed a bounded truth-table degree that does not contain the word problem of a f.p. group. For f.g. groups with Π_1^0 word problem, Morozov [26] has shown that there is a two-generator group which is not embeddable into the group of computable permutations of ω .

Using the methods of the foregoing result, here we obtain an analog of the results by Fridman, Clapham, Boone and Collins for f.g. groups of computable permutations. In fact we can choose the permutations of a special kind.

Let us call a permutation σ fully primitive recursive if both σ and σ^{-1} are primitive recursive. Note that the fully primitive recursive permutations form a group.

Theorem 5.2. Given a Π_1^0 set S we can effectively build fully primitive recursive permutations β, σ, τ such that the group G generated by them has word problem in the same truth-table degree as S.

Proof. In this proof we work with an array of columns indexed by integers. Let $\sigma(\langle x, n \rangle) = \langle x+1, n \rangle$ $(x \in \mathbb{Z}, n \in \omega)$ be the shift to the next column. Let τ consist of the 2-cycles $(\langle 0, 3t+1 \rangle, \langle 0, 3t+2 \rangle)$ for each t: in other words, $\tau(\langle 0, 3t+1 \rangle) = \langle 0, 3t+2 \rangle, \tau(\langle 0, 3t+2 \rangle) = \langle 0, 3t+1 \rangle$ for all t, and τ is the identity elsewhere.

Let S be a given Π_1^0 set, and let $S^c = \omega \setminus S$ be the complement of S. First we show we may assume that, up to *m*-equivalence, S^c is the range of a 1-1 function with graph effectively given by an index for a primitive recursive relation. We can uniformly replace S^c by $\{2n: n \in S^c\} \cup \{2n+1: n \in \omega\}$, so we may assume that S^c is infinite. From a c.e. index for S^c we may effectively obtain an index e of a Turing machine that computes a 1-1 function f with range S^c . Thus, for all x we have $f(x) = U(\mu y, T(e, x, y))$, where U and T are respectively a primitive recursive function and a primitive recursive predicate as in the Kleene Normal Form Theorem. Consider the primitive recursive predicate P(e, x, y), which holds if and only if $T(e, x, y) \& \forall z < y [\neg T(e, x, z)]$. Using the standard primitive recursive pairing function $\langle ., . \rangle$, let $g(\langle x, y \rangle) = 2U(y)$ if P(e, x, y) holds, and $g(\langle x, y \rangle) = 2\langle x, y \rangle + 1$ otherwise. Clearly g is a 1-1 function with primitive recursive graph. The range of g is $\{2n: n \in S^c\} \cup \{2\langle x, y \rangle + 1: \neg P(e, x, y)\}$, which is *m*-equivalent to S^c .

Next we code the graph of g into a fully primitive recursive permutation β as follows: if g(t) = x, then β has a 2-cycle $(\langle x, 3t \rangle, \langle x, 3t + 1 \rangle)$. Thus, among the three permutations only β depends on S. Clearly β is fully primitive recursive uniformly in a c.e. index for S^c .

Let G be the group of permutations generated by σ, τ, β . For $x \in \omega$, we can picture $Cj(\beta, \sigma^{-x})$ as the "shift" of β by x columns to the left. The set S is many-one below the word problem of G because

$$x \in S \Leftrightarrow [Cj(\beta, \sigma^{-x}), \tau] = 1,$$

where $[u, v] = u^{-1}v^{-1}uv$ is the usual commutator of u, v. To see this, first note that if $y \neq 0$, then $Cj(\beta, \sigma^{-x})(\langle y, t \rangle)$ still lies in the y-th column, and thus $Cj(\beta, \sigma^{-x})\tau(\langle y, t \rangle) = \tau Cj(\beta, \sigma^{-x})(\langle y, t \rangle)$, as τ is the identity on the y-th column. Now, if $x \in S$, then β is the identity on the x-th column

and thus $Cj(\beta, \sigma^{-x})$ is the identity on the 0-th column, giving $[Cj(\beta, \sigma^{-x}), \tau] = 1$; if $x \notin S$, and t is such that g(t) = x, then $Cj(\beta, \sigma^{-x})\tau(\langle 0, i \rangle) \neq \tau Cj(\beta, \sigma^{-x})(\langle 0, i \rangle)$, for every $i \in \{3t, 3t+1, 3t+2\}$.

It remains to show that the word problem of G is truth-table below S. We note that τ and β are involutions. For any $x \in \mathbb{Z}$ we write $\beta_x = Cj(\beta, \sigma^{-x})$ and $\tau_x = Cj(\tau, \sigma^{-x})$. It is easy to see that $[\beta_x, \beta_y] = 1$ and $[\tau_x, \tau_y] = 1$, for all x, y. Suppose now that a word $w \in F(\beta, \sigma, \tau)$ (the free group on $\{\beta, \sigma, \tau\}$) is given; we have to decide whether w = 1 in G by accessing the oracle S in a truth-table fashion. If the exponent sum of σ in w (i.e. the sum of all exponents of occurrences of σ in w) is nonzero then $w \neq 1$ in G. Otherwise, using the observations above, we can effectively replace w by an equivalent word

(5.2)
$$(\prod_{x \in L_1} \beta_x) (\prod_{u \in M_1} \tau_u) (\prod_{x \in L_2} \beta_x) (\prod_{u \in M_2} \tau_u) \dots (\prod_{x \in L_k} \beta_x) (\prod_{u \in M_k} \tau_u)$$

where the L_i and M_i are effectively given finite sets of distinct integers, which are nonempty except for possibly L_1 or M_k . Let $L = \bigcup_i L_i$ and $M = \bigcup_i M_i$.

Notice that a product $\beta_x \tau_u$ produces a 3-cycle in column -u precisely when $x - u \in S^c$, otherwise $\beta_x \tau_u$ coincides on C_{-u} with τ_u . For every x, u let w(x, u) be the word obtained from (5.2) by deleting all elements different from β_x, τ_u , and cancelling all occurrences of subwords $\beta_x \beta_x$ and $\tau_u \tau_u$. Since g is 1-1, we have that the cycles of β_x and β_y are disjoint for any $x \neq y$: therefore the permutations corresponding to w(x, u) and w coincide in the interval $\{\langle -u, 3t \rangle, \langle -u, 3t + 1 \rangle, \langle -u, 3t + 2 \rangle\}$ of the column C_{-u} , where g(t) = x.

To decide whether the word in (5.2) is equal to 1 in G, we give a procedure to decide whether the permutation corresponding to w is the identity on each column C_{-u} . First notice that w fixes all columns C_{-u} with $u \notin M$ if and only, for all $x \in L$, the number of occurrences of β_x in (5.2) is even. Indeed, if $u \notin M$ and $x \in L$, then w(x, u) is a word consisting of only occurrences of β_x ; which by cancellation is either empty (if the number of occurrences is even) or equal to β_x : if the former case happens for every $x \in L$, then every column C_{-u} with $u \notin M$ remains fixed; if $x \in L$ satisfies the latter case, and $u \notin M$ is such that $x - u \in S^c$, then w does not fix C_{-u} , in which case we output $w \neq 1$ in G.

If we have already ascertained that all columns C_{-u} remain fixed for all $u \notin M$, then take any $u \in M$, and for every $x \in L$, perform the following check querying the oracle:

- (1) if $x u \notin S^c$ then on the column C_{-u} , the permutation corresponding to w(x, u) coincides the one corresponding to the word obtained from it by cancelling all occurrences of β_x ; in this case, say that C_{-u} is *x*-fixed if and only if the length of the resulting word is even;
- (2) if $x u \in S^c$ and the number of occurrences in w(x, u) of the subword $\beta_x \tau_u$ is a not a multiple of 3, then the 3-cycles produced by β_x and τ_u do not cancel each other: say in this case that C_{-u} is not x-fixed; otherwise, cancel from w(x, u) all occurrences of $\beta_x \tau_u$, and say that C_{-u} is x-fixed if and only if the resulting word is empty.

If for all $x \in L$ we have stated that C_{-u} is x-fixed, then we conclude that C_{-u} is fixed under the permutation corresponding to w.

If for all $u \in M$, we have concluded that C_{-u} is fixed, then we output that w = 1 in G; otherwise we output $w \neq 1$ in G. An output will be achieved no matter what the oracle is, so the reduction is truth-table.

It would be interesting to determine the complexity of isomorphism and embedding for f.g. groups of recursive permutations. Totality of a function described by a recursive index is already Π_2^0 complete, so it might be more natural to restrict oneself to fully primitive recursive permutations as defined above. It is a Π_1^0 condition of an index consisting of a pair of indices (e, i) for primitive

recursive functions (one for the potential permutation, one for its potential inverse) whether it describes such a permutation.

In both settings, isomorphism and embedding are Σ_3^0 relations between finitely generated groups given by finite sets of indices for the generators. For an example where the isomorphism relation has an intermediate complexity, suppose the domain is \mathbb{Z} , and consider the subgroup G of the group of computable permutations generated by the shift. The problem whether a group generated by finitely many fully primitive recursive permutations is isomorphic to G is Π_2^0 -hard. To see this, note that infinity of a c.e. set W_e is Π_2^0 -complete. Build a fully primitive recursive permutation p_e by adding a cycle of length n involving large numbers when n enters W_e . Then the subgroup generated by p_e is isomorphic to G if and only if p_e has infinite order if and only if W_e is infinite.

References

- U. Andrews, S. Lempp, J. S. Miller, K. M. Ng, L. San Mauro, and A. Sorbi. Universal computably enumerable equivalence relations. J. Symbolic Logic, 79(1):60–88, March 2014.
- [2] U. Andrews and A. Sorbi. Jumps of computably enumerable equivalence relations. in preparation, 2015.
- [3] C. Bernardi. On the relation provable equivalence and on partitions in effectively inseparable sets. Studia Logica, 40:29–37, 1981.
- [4] C. Bernardi and F. Montagna. Equivalence relations induced by extensional formulae: Classifications by means of a new fixed point property. *Fund. Math.*, 124:221–232, 1984.
- [5] C. Bernardi and A. Sorbi. Classifying positive equivalence relations. J. Symbolic Logic, 48(3):529–538, 1983.
- [6] W. W. Boone. Word problems and recursively enumerable degrees of unsolvability. A first paper on Thue systems. Ann. of Math., 83:520–571, 1966.
- [7] W. W. Boone. Word problems and recursively enumerable degrees of unsolvability. A sequel on finitely presented groups. Ann. of Math., 84:49–84, 1966.
- [8] W. W. Boone. Word problems and recursively enumerable degrees of unsolvability. An emendation. Ann. of Math., 94:389–391, 1971.
- C. R. J. Clapham. Finitely presented groups with word problems of arbitrary degrees of insolubility. Proceedings of the London Mathematical Society, 3(4):633–676, 1964.
- [10] D. J. Collins. Truth-table degrees and the Boone groups. Ann. of Math., 94(3):392–396, 1971.
- [11] S. Coskey, J. D. Hamkins, and R. Miller. The hierarchy of equivalence relations on the natural numbers. Computability, 1:15–38, 2012.
- [12] Yu. L. Ershov. Positive equivalences. Algebra and Logic, 10(6):378-394, 1973.
- [13] Yu. L. Ershov. Theorie der Numerierungen I. Z. Math. Logik Grundlag. Math., 19:289–388, 1973.
- [14] Yu. L. Ershov. Theorie der Numerierungen II. Z. Math. Logik Grundlag. Math., 19:473–584, 1975.
- [15] E. B. Fokina, S. D. Friedman, and A. Nies. Equivalence relations that are Σ_3^0 complete for computable reducibility (Extended Abstract). In *WoLLIC*, pages 26–33, 2012.
- [16] E.B. Fokina, S.D. Friedman, V. Harizanov, J.F. Knight, C. Mc Coy, and A. Montalbán. Isomorphism relations on computable structures. J. Symbolic Logic, 77(1):122–132, 2012.
- [17] A. A. Fridman. Degrees of unsolvability of the problem of identity in finitely presented groups. Soviet. Math., 3(Part 2):1733–1737, 1962.
- [18] S. Gao and P. Gerdes. Computably enumerable equivalence relations. Studia Logica, 67:27–59, 2001.
- [19] G. Higman. Subgroups of finitely presented groups. Proc. Royal Soc. London Ser A, 262:455–475, 1961.
- [20] E. Ianovski, R. Miller, K. M. Ng, and A. Nies. Complexity of equivalence relations and preorders from computability theory. J. Symbolic Logic, 79(3):859–881, 2014.
- [21] M. I. Kargapolov and Ju. I Merzljakov. Fundamentals of the Theory of Groups. Graduate Texts in Mathematics. Springer-Verlag, New York, Heidelberg, Berlin, second edition, 1979.
- [22] R. C. Lyndon and P. E. Schupp. Combinatorial Group Theory. Springer-Verlag, Berlin Heidelberg, 1977.
- [23] C. F. Miller III. The word problem in quotients of a group. http://www.ms.unimelb.edu.au/~cfm/papers/ paperpdfs/wpqg.pdf. 2002.
- [24] C. F. Miller III. Group-Theoretic Decision Problems and their Classification. Number 68 in Annals of Mathematical Studies. Princeton University Press, Princeton, New Jersey, 1971.
- [25] F. Montagna. Relative precomplete numerations and arithmetic. J. Philosphical Logic, 11:419–430, 1982.
- [26] A. S. Morozov. Once again on the Higman question. Algebra i logika, 39(2):134-144, 2000.

CALIBRATING WORD PROBLEMS OF GROUPS VIA THE COMPLEXITY OF EQUIVALENCE RELATIONS 13

- [27] M. O. Rabin. Recursive unsolvability of group theoretic problems. Ann. of Math., 67:172–174, 1958.
- [28] R. I. Soare. *Recursively Enumerable Sets and Degrees*. Perspectives in Mathematical Logic, Omega Series. Springer-Verlag, Heidelberg, 1987.
- [29] A. Visser. Numerations, λ-calculus & arithmetic. In J. P. Seldin and J. R. Hindley, editors, To H. B. Curry: Essays on Combinatory Logic, Lambda Calculus and Formalism, pages 259–284. Academic Press, London, 1980.
- [30] M. Ziegler. Ein rekursiv aufzählbarer btt-Grad, der nicht zum Wortproblem einer Gruppe gehört. Z. Math. Logik Grundlag. Math., 22:165–168, 1976.

Department of Computer Science, University of Auckland, Private Bag 92019, Auckland, New Zealand

E-mail address: andre@cs.auckland.ac.nz

Dipartimento di Ingegneria dell'Informazione e Scienze Matematiche, Università di Siena, 53100 Siena, Italy

 $E\text{-}mail\ address:$ and rea. sorbi@unisi.it