Conjugacy equivalence relation on subgroups

by

Alessandro Andretta (Torino), Riccardo Camerlo (Torino) and Greg Hjorth (Los Angeles, CA)

Abstract. If G is a countable group containing a copy of $\mathbf{F}_2$ then the conjugacy equivalence relation on subgroups of G attains the maximal possible complexity.

1. Introduction. This paper is primarily directed towards the study of subgroups of countable groups and the complexity of the conjugacy equivalence relation, $E_c(G, \mathrm{Sgr}(G))$, on the space $\mathrm{Sgr}(G)$ of these subgroups.

It had previously been shown that:

LEMMA 1.1 (Stuck, Zimmer, see [8], 3.9). *The conjugacy equivalence relation on subgroups of $\mathbf{F}_2$, the free group on two generators, is not smooth.*

We give the precise definition of smooth below in §2. Roughly speaking, 1.1 states that there is no Borel function assigning elements of $\mathbb{R}$ as complete invariants to the equivalence classes of $E_c(\mathbf{F}_2, \mathrm{Sgr}(\mathbf{F}_2))$.

This was recently strengthened in [9]:

THEOREM 1.2 (Thomas, Veličković). $E_c(\mathbf{F}_2, \mathrm{Sgr}(\mathbf{F}_2))$ *is a universal countable Borel equivalence relation.*

Again the exact definitions can be found in §2. In essence, 1.2 states that $E_c(\mathbf{F}_2, \mathrm{Sgr}(\mathbf{F}_2))$ attains the maximal possible complexity. In [3] Su Gao showed $E_c(G, \mathrm{Sgr}(G))$ to be universal for a variety of finitely generated groups, including $\mathbf{F}_2$, all of which contained $\mathbf{F}_2$ as a subgroup.

In this present paper we obtain a completely general result:

THEOREM 1.3. *For G a countable group containing $\mathbf{F}_2$ as a subgroup, $E_{\mathrm{c}}(G, \mathrm{Sgr}(G))$ is universal.*

For instance, Theorem 1.3 implies that the conjugacy equivalence relation on $\mathrm{SL}_2(\mathbb{Z})$ is universal since, as noted in [10], $\mathrm{SL}_2(\mathbb{Z})$ contains a copy of $\mathbf{F}_2$. The universality of this specific conjugacy relation does not seem to follow from the arguments of Gao or Thomas and Veličković.

The proof of 1.3 came about as a result of thinking about the following still open and seemingly difficult problem.

QUESTION 1.4. Must any countable Borel equivalence relation including a universal countable Borel equivalence relation itself be universal?

It is easily seen that $E_{\mathrm{c}}(\mathbf{F}_2, \mathrm{Sgr}(\mathbf{F}_2))$ includes a universal countable Borel equivalence relation, and hence so too does $E_{\mathrm{c}}(G, \mathrm{Sgr}(G))$ whenever $\mathbf{F}_2 \subseteq G$. The proof of 1.3 below demonstrates universality of $E_{\mathrm{c}}(G, \mathrm{Sgr}(G))$ by going to a subspace of $\mathrm{Sgr}(G)$ on which the universal equivalence relation included in $E_{\mathrm{c}}(G, \mathrm{Sgr}(G))$ exactly equals $E_{\mathrm{c}}(G, \mathrm{Sgr}(G))$; in other words, we restrict to a subspace on which the extra parts of $E_{\mathrm{c}}(G, \mathrm{Sgr}(G))$ are killed off and only the universal countable equivalence relation remains. In some sense the proof can be thought of as a kind of trial effort to affirmatively answer the above open question, but using all the extra information given by the specific context.

The proof of 1.3 also uses the following improvement of a theorem by Dougherty and Kechris:

THEOREM 1.5. *For G a countable group of permutations including the recursive permutations, $\cong_G^5$ is universal.*

Here $\cong_G^5$ is the equivalence relation on $5^{\mathbb{N}}$ arising from the natural shift action on this space.

Previously it was shown:

THEOREM 1.6 (Dougherty, Kechris, see [2]). *For G a countable group of permutations including the recursive permutations, $\cong_G^{\mathbb{N}}$ is universal.*

These results came as an attempt to settle the following open problem.

QUESTION 1.7. Is $\equiv_{\mathrm{T}}$, the relation of Turing equivalence on $\mathbb{N}^{\mathbb{N}}$ (or equivalently $2^{\mathbb{N}}$), universal among countable Borel equivalence relations?

An affirmative answer to 1.4 together with 1.6 would yield an affirmative answer to 1.7, which in turn would refute in a very strong way a conjecture of Martin's in recursion theory—see the Appendix in [6].

2. Notation and definitions. We give a stick figure sketch of the most of the definitions and notation. The reader is referred to [5] for basic facts

on descriptive set theory, while more extensive introductions to the theory of Borel equivalence relations can be found in [1] or [4].

A topological space X is said to be *Polish* if it is separable and completely metrizable. For example, $k^{\mathbb{N}}$ and $\mathbb{N}^{\mathbb{N}}$ are both Polish with the topology of pointwise convergence. (Here and below we adopt the usual convention of identifying an integer k with the set $\{0, \ldots, k-1\}$ of all of its predecessors and A^B with the set of all functions from B to A.) We say that $B \subseteq X$ is *Borel* if it appears in the smallest σ-algebra containing the open sets. A function $f : X \to Y$ between Polish spaces is *Borel* if $f^{-1}[U]$ is Borel for any open $U \subseteq Y$.

An equivalence relation E on X is *Borel* if is Borel as a subset of $X \times X$. For E and F Borel equivalence relations on Polish spaces X and Y we say that E is *Borel reducible* to F, written $E \leq_{\mathrm{B}} F$, if there is a Borel function $f : X \to Y$ which embeds E in F, in the sense that for all $x_1, x_2 \in X$,

$$x_1 \, E \, x_2 \ \Leftrightarrow \ f(x_1) \, F \, f(x_2).$$

We say that E on X is *smooth* if $E \leq_{\mathrm{B}} \Delta(\mathbb{R})$, the equality equivalence relation on $\mathbb{R}$. We say that E on X is *countable* if all of its equivalence classes are countable. A countable Borel equivalence relation E is said to be *universal* if for any other countable Borel equivalence relation F we have $F \leq_{\mathrm{B}} E$.

It is a somewhat non-trivial fact that there is a universal countable Borel equivalence relation. We work towards giving an example due to Dougherty, Jackson, and Kechris.

Let G be an infinite countable group. Then G acts on 2^G by *left* shift, namely we define $G \times 2^G \to 2^G$, $(g, x) \mapsto g.x$, to be

$$\forall h \in G \ ((g.x)(h) = x(g^{-1}h)).$$

We then denote the resulting orbit equivalence relation on 2^G by $E(G, 2)$. Note that 2^G is Polish, being homeomorphic to $2^{\mathbb{N}}$, and that $E(G, 2)$ is countable Borel.

THEOREM 2.1 (Dougherty, Jackson, Kechris, see [1]). *$E(\mathbf{F}_2, 2)$ is universal.*

For G a countable group, we let $\mathrm{Sgr}(G)$ be the collection of all subgroups of G. Under the natural identification of $\mathcal{P}(G)$ with 2^G we find that $\mathrm{Sgr}(G)$ is a closed subset of 2^G, and hence a Polish space in its own right. We then let G act on $\mathrm{Sgr}(G)$ by conjugation and define $E_{\mathrm{c}}(G, \mathrm{Sgr}(G))$ to be the resulting orbit equivalence relation. Thus for $H_1, H_2 \subseteq G$ we have

$$H_1 \, E_{\mathrm{c}}(G, \mathrm{Sgr}(G)) \, H_2 \ \Leftrightarrow \ \exists g \in G \ (gH_1g^{-1} = H_2).$$

If X is a set then $\mathrm{Sym}(X)$ is the group of all permutations of X. Usually, $\mathrm{Sym}(\mathbb{N})$ is denoted by S_{∞}. We let S_{∞} act on the *right* on $k^{\mathbb{N}}$, by $k^{\mathbb{N}} \times$

$S_\infty \to k^\mathbb{N}$, $(x, g) \mapsto x \circ g$. We then obtain for any subgroup $G \subseteq S_\infty$ the corresponding equivalence relation $\cong_G^k$:

$$x \cong_G^k y \iff \exists g \in G \ (x \circ g = y).$$

Similarly we define $\cong_G^\mathbb{N}$ on $\mathbb{N}^\mathbb{N}$.

3. Groups of permutations. We now prove Theorem 1.5. In fact, we will prove a slightly stronger assertion.

THEOREM 3.1. *There is a countable group $G_0 \subseteq S_\infty$ of recursive permutations such that $G_0 \cong \mathbf{F}_2$, and for every countable group G with $G_0 \subseteq G \subseteq S_\infty$, the equivalence relation $\cong_G^5$ on $5^\mathbb{N}$ is universal among countable Borel equivalence relations. In particular, this holds when $G = \mathrm{Rec}$, the group of recursive bijections.*

Proof. Rather than working with subgroups of S_∞ we will look at subgroups G of $\mathrm{Sym}(M)$, where $M = \mathbf{F}_2 \times \mathbb{N}^2$. The set M is best visualized as $\mathbf{F}_2$-many copies of the square $\mathbb{N} \times \mathbb{N}$:
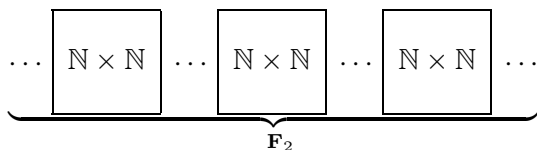
A generic element of M is denoted by (w, n, k) with n ranging on the x-axis and k ranging on the y-axis of the wth square. Thus a set of the form $\{(w, n, k) \in M \mid k_0 \leq k \leq k_1\}$ is called a *horizontal strip* of M.

For every $w \in \mathbf{F}_2$ let $\widehat{w} \in \mathrm{Sym}(M)$ be defined by

$$\widehat{w}(v, n, k) = (vw, n, k)$$

and let $G_0 = \{\widehat{w} \mid w \in \mathbf{F}_2\}$. (Note that the map $\mathbf{F}_2 \to G_0$, $w \mapsto \widehat{w^{-1}}$, is an isomorphism.) An element of the form $\widehat{w}$ acts by right multiplication on the $\mathbf{F}_2$-coordinate, leaving the other two coordinates unchanged. Let G be a countable group with $G_0 \subseteq G \subseteq \mathrm{Sym}(M)$. If G were equal to G_0 then we would be done by 2.1 and $E(G_0, 2) \leq_B \cong_{G_0}^5$. So we try to analyze how different from an element of G_0 can an element of G be. Fix an enumeration $(g_i)_{i>0}$ of G. (For notational reasons it is more convenient to avoid 0 as an index here.) An element $g \in G$ is called a *quasi-shift above l* iff

$\forall (w, n, k) \in M$

$\quad [k > l \Rightarrow g(w, n, k) = (\varphi(w, n, k), n, k) \ \& \ g^{-1}(w, n, k) = (\psi(w, n, k), n, k)]$

for some functions $\varphi, \psi : M \to \mathbf{F}_2$. In other words, a quasi-shift respects pointwise the second and third coordinates of M. If the functions φ, ψ above depend on $\mathbf{F}_2$ only, i.e., $g(w, n, k) = (\varphi(w), n, k)$ and $g^{-1}(w, n, k) = (\psi(w), n, k)$, then g is a *shift*. Elements of G_0 are particular types of shifts.

An increasing sequence $(l_i)_{i \in \mathbb{N}}$ of integers is defined inductively.

Set $l_0 = -1$ and suppose l_{i-1} has been defined for some $i \geq 1$. We now distinguish two cases:

• g_i is not a quasi-shift above l_{i-1}, i.e., there is a $w_0 \in \mathbf{F}_2$ and there are $(n_0, k_0) \in \mathbb{N}^2$ such that $g_i(w_0, n_0, k_0) = (w_0', n_0', k_0')$ and $(n_0, k_0) \neq (n_0', k_0')$, with $k_0 > l_{i-1}$ or $k_0' > l_{i-1}$. Then we have the following possibilities:

   (i) $g_i(w_0, n_0, k_0) = (w_0', n_0', k_0')$ for some $(w_0, n_0, k_0), (w_0', n_0', k_0') \in M$ with $k_0 > l_{i-1}$ and $k_0 > k_0'$;
   (ii) $g_i^{-1}(w_0, n_0, k_0) = (w_0', n_0', k_0')$ for some $(w_0, n_0, k_0), (w_0', n_0', k_0') \in M$ with $k_0 > l_{i-1}$ and $k_0 > k_0'$, and (i) fails;
   (iii) $g_i(w_0, n_0, k_0) = (w_0', n_0', k_0)$ for some $(w_0, n_0, k_0), (w_0', n_0', k_0) \in M$ with $k_0 > l_{i-1}$ and $n_0 \neq n_0'$, and both (i) and (ii) fail.

Then set $l_i = k_0$, for the least possible k_0 as above.

• Otherwise, that is: g_i is a quasi-shift above l_{i-1}. Then set $l_i = l_{i-1} + 1$.

Suppose g_i is a quasi-shift above l_{i-1}. Then g_i shuffles the l_ith rows among the various squares, and, in particular, $\forall n \in \mathbb{N} \, \exists w \in \mathbf{F}_2 \, (g_i(1_{\mathbf{F}_2}, n, l_i) = (w, n, l_i))$.

We say that g_i is *good* if there is an increasing sequence $(n_m)_m$ of natural numbers and a fixed $w_\infty \in \mathbf{F}_2$ such that

$$\forall m \in \mathbb{N} \, (g_i(1_{\mathbf{F}_2}, n_m, l_i) = (w_\infty, n_m, l_i)).$$

If g_i is not good then it is called *bad*. In this case we can find an increasing sequence $(n_m)_m$ of natural numbers and a sequence $(w_m)_m$ of distinct elements in $\mathbf{F}_2$ such that

$$\forall m \in \mathbb{N} \, (g_i(1_{\mathbf{F}_2}, n_m, l_i) = (w_m, n_m, l_i)).$$

Let also $z_{m+1} = w_{m+1} w_m^{-1}$ and define $\mu : 2^{\mathbf{F}_2} \to \{1, 2, \ldots, \infty\}$ by

$$\mu(x) = \begin{cases} \text{the least } m \geq 1 \text{ such that } z_m.x \neq x, \\ \infty \quad \text{if } \forall m \geq 1 \, (z_m.x = x). \end{cases}$$

We record a few simple facts about μ whose proof is left to the reader.

CLAIM 3.2. *$\forall j < \mu(w_0.x) \, (w_j.x = w_0.x)$, and if $\mu(w_0.x) < \infty$ then $\mu(w_{\mu(w_0.x)}.x) \leq \mu(w_0.x)$.*

Obviously all of the above (n_m's, w_m's, z_m's, μ) depend on i so we should really write $n_m^{(i)}$, $w_m^{(i)}$, etc.

We shall define a Borel map $2^{\mathbf{F}_2} \to 5^M$, $x \mapsto x^*$, witnessing the reduction $E(\mathbf{F}_2, 2) \leq_{\mathrm{B}} \cong_G^5$. The map $x^* : M \to 5$ assigns to each element of M a *colour*, i.e., an integer between 0 and 4. The colouring of x^* will encode x in a sufficiently "rigid" way so that for all $x, y \in 2^{\mathbf{F}_2}$,

   1. $\forall w \in \mathbf{F}_2 \, (w.x = y \Rightarrow x^* \circ \widehat{w} = y^*)$, hence $x \, E(\mathbf{F}_2, 2) \, y \Rightarrow x^* \cong_G^5 y^*$,

2. $\forall g \in G \, \exists w \in \mathbf{F}_2 \, (x^* \circ g = y^* \Rightarrow w.x = y)$, and hence $x^* \cong_G^5 y^* \Rightarrow x \, E(\mathbf{F}_2, 2) \, y$.

The function $x^* : M \to 5$ will be defined on the horizontal strips

$$\{(w, n, k) \in M \mid l_{i-1} < k \leq l_i\}$$

by induction on $i \geq 1$ in such a way that if g_i is not a quasi-shift then the value of x^* is independent of x, i.e.,

g_i not a quasi-shift

$$\Rightarrow \; \forall x, y \in 2^{\mathbf{F}_2} \, \forall (w, n, k) \, (l_{i-1} < k \leq l_i \Rightarrow x^*(w, n, k) = y^*(w, n, k)).$$

The horizontal strip $\{(w, n, k) \in M \mid l_{i-1} < k \leq l_i\}$ is used to "kill" the g_i's which are not quasi-shifts, i.e., it is used to make sure that $\forall x, y \in 2^{\mathbf{F}_2} \, (x^* \circ g_i \neq y^*)$. If instead g_i is a quasi-shift, then $l_{i-1} + 1 = l_i$ and the set $\{(w, n, l_i) \mid n \in \mathbb{N}\}$ is used either to kill g_i or else to encode $w.x$. Also, the map $x \mapsto \{(w, n, k) \mid x^*(w, n, k) = 4\}$ will be constant, that is, whether or not $x^*(w, n, k) = 4$ will not depend on x but on (w, n, k) only.

Now the details. We will consider two cases depending on whether or not g_i is a quasi-shift.

$\boxed{g_i \text{ is a quasi-shift above } l_{i-1}.}$

Then $l_{i-1} + 1 = l_i$ and we only have to define $x^*(w, n, l_i)$ for $w \in \mathbf{F}_2$ and $n \in \mathbb{N}$. Let $(n_m)_m$ be as in the definition of good/bad quasi-shift. Fix an enumeration without repetitions $(u_m)_m$ of $\mathbf{F}_2$.

(0) For $n \notin \{n_m \mid m \in \mathbb{N}\}$ set $x^*(w, n, l_i) = 0$.
(1) If g_i is good then set for every $w \in \mathbf{F}_2$ and $m \in \mathbb{N}$

$$x^*(w, n_m, l_i) = (w.x)(u_m) \in \{0, 1\}.$$

In other words, we are encoding $w.x$ on the sequence $(n_m)_m$ in the wth square. Therefore for all $(w, m) \in \mathbf{F}_2 \times \mathbb{N}$,

$$x^*(w, n_m, l_i) = (w.x)(u_m) = (w.x)^*(1_{\mathbf{F}_2}, n_m, l_i)$$

and thus $\forall w \in \mathbf{F}_2 \, \forall n \in \mathbb{N} \, (x^*(w, n, l_i) = (w.x)^*(1_{\mathbf{F}_2}, n, l_i))$ by (0).

(2) If g_i is bad and $\mu(w.x) = \infty$ then set, for every $m \in \mathbb{N}$,

$$x^*(w, n_0, l_i) = 0, \quad x^*(w, n_1, l_i) = 3, \quad x^*(w, n_{m+2}, l_i) = (w.x)(u_m).$$

Also in this case $w.x$ is encoded on $(n_m)_m$ in the wth square, but a "flag" 03 is attached at the very beginning. Again it is easy to check that $\forall w \in \mathbf{F}_2 \, \forall n \in \mathbb{N} \, (x^*(w, n, l_i) = (w.x)^*(1_{\mathbf{F}_2}, n, l_i))$.

So we may assume g_i is bad and $0 < \mu(w.x) < \infty$. We will need the following result which is an immediate consequence of Proposition 4.6 of [7].

LEMMA 3.3. *Let* $T : X \to X$ *be a Borel transformation on a standard Borel space* X. *There are pairwise disjoint Borel sets* $X^{(0)}$, $X^{(1)}$, $X^{(2)}$ *such that* $X^{(0)} \cup X^{(1)} \cup X^{(2)} = X$ *and such that for all* $x \in X$ *and* $j \in \{0, 1, 2\}$,

$$(x \neq T(x) \ \& \ x \in X^{(j)}) \ \Rightarrow \ T(x) \notin X^{(j)}.$$

That is to say: *if* x *is not a fixed point of* T *then* x *and* $T(x)$ *belong to different pieces of the partition* $\{X^{(0)}, X^{(1)}, X^{(2)}\}$.

For every $m \in \mathbb{N}$ the map $T_m : 2^{\mathbf{F}_2} \to 2^{\mathbf{F}_2}$, $x \mapsto z_m.x$, is a Borel transformation, where $(z_m)_m$ is as in the definition of bad quasi-shift. Let $X_m^{(0)}$, $X_m^{(1)}$, and $X_m^{(2)}$ be as in the lemma, with $T = T_m$. Then set

$$J_m(x) = \text{the unique } j \in \{0, 1, 2\} \text{ such that } x \in X_m^{(j)}.$$

(Note that the definition of J_m depends on z_m and hence on the index i.)

(3) If g_i is bad and $0 < \mu(w.x) < \infty$ then

$$x^*(w, n_m, l_i) = \begin{cases} 3 & \text{if } m < \mu(w.x) - 1, \\ J_{\mu(w.x)}(w.x) & \text{if } m = \mu(w.x) - 1 \text{ or } m = \mu(w.x), \\ 3 & \text{if } m > \mu(w.x). \end{cases}$$

In this case x^* is *not* encoding $w.x$ on $\{(w, n_m, l_i) \mid m \in \mathbb{N}\}$: the particular definition of $x^*(w, n_m, l_i)$ will be used to show that $x^* \circ g_i \neq y^*$, for any $y \in 2^{\mathbf{F}_2}$.

We now want to check that the behaviour of x^* on the set $\{(1_{\mathbf{F}_2}, n_m, l_i) \mid m \in \mathbb{N}\}$ determines whether we are in case (1), (2), or (3) above.

CLAIM 3.4. *Let* $i \geq 1$ *be such that* g_i *is a quasi-shift above* l_{i-1} *and let* $x, y \in 2^{\mathbf{F}_2}$ *be such that* $\forall m \ (x^*(1_{\mathbf{F}_2}, n_m, l_i) = y^*(1_{\mathbf{F}_2}, n_m, l_i))$.

Suppose the definition of x^* *on the set* $\{(1_{\mathbf{F}_2}, n_m, l_i) \mid m \in \mathbb{N}\}$ *is as in case* (1), (2), *or* (3). *Then also the definition of* y^* *on* $\{(1_{\mathbf{F}_2}, n_m, l_i) \mid m \in \mathbb{N}\}$ *is as in case* (1), (2), *or* (3), *respectively*.

Moreover, the sequence $(x^*(1_{\mathbf{F}_2}, n_m, l_i))_m$ *is of the form*:

- *an element of* $2^{\mathbb{N}}$ *if* x^* *is defined as in* (1),
- 03 *followed by an element of* $2^{\mathbb{N}}$ *if* x^* *is defined as in* (2),
- $(3, \ldots, 3, n, n, 3, 3, \ldots)$ *starting with a possibly empty sequence of* 3*'s, then two consecutive* n*'s with* $n \in \{0, 1, 2\}$, *at position* $\mu(x) - 1$ *and* $\mu(x)$, *and then* 3 *from now on. This happens when* x^* *is defined as in* (3).

Proof. If x^* on $\{(1_{\mathbf{F}_2}, n_m, l_i) \mid m \in \mathbb{N}\}$ is defined as in (1) then g_i must be good, hence also y^* is defined as in (1).

For the other cases notice that if $x^*(1_{\mathbf{F}_2}, n_0, l_i) \in \{1, 2, 3\}$ then x^* (and hence y^*) is defined as in (3), while if $x^*(1_{\mathbf{F}_2}, n_0, l_i) = 0$ then either $x^*(1_{\mathbf{F}_2}, n_1, l_i) = 0$ and we are in case (3) with $\mu = 1$ or else $x^*(1_{\mathbf{F}_2}, n_1, l_i) = 3$ and we are in case (2). ∎

REMARK 3.5. The only reason for using the flag 03 before the sequence coding $w.x$ in (2) is to be able to distinguish, assuming g_i is bad, whether $(x^*(1_{\mathbf{F}_2}, n_m, l_i))_m$ is defined as in (2) or (3) only by looking at its first 2 elements. Had we been less stingy with the number of colours and used, say, 5 and 6 instead of 0 and 1 in (2) then we could have avoided using the flag 03.

We now consider the other case, namely

g_i **is not a quasi-shift above** l_{i-1}.

Let w_0, n_0, k_0, w_0', n_0', k_0' be as in cases (i)–(iii). We must define $x^*(w, n, k)$ for all $w \in \mathbf{F}_2$, $n \in \mathbb{N}$ and $l_{i-1} < k \le l_i$.

Suppose case (i) holds.

If $k_0' \le l_{i-1}$ then set

$$x^*(w, n, k) = \begin{cases} 0 & \text{if } x^*(w_0', n_0', k_0') = 4, \\ 4 & \text{if } x^*(w_0', n_0', k_0') \le 3. \end{cases}$$

(This is the only way for x^* to achieve value 4.)

If $l_{i-1} < k_0'$ then set

$$x^*(w, n, k) = \begin{cases} 1 & \text{if } k = k_0', \\ 0 & \text{if } k \ne k_0'. \end{cases}$$

If case (ii) holds then proceed as in case (i).

If case (iii) holds then set

$$x^*(w, n, k) = \begin{cases} 1 & \text{if } n = n_0', \\ 0 & \text{if } n \ne n_0'. \end{cases}$$

This concludes the definition of x^*.

We must check that $x \mapsto x^*$ is indeed a reduction.

As the value of $x^*(w, n, k)$ is independent of x and w, when $l_{i-1} < k \le l_i$ and g_i is not a quasi-shift, or else depends on $w.x$ only (when g_i is a quasi-shift), it is straightforward to check that

$$\forall v \in \mathbf{F}_2 \ \forall (w, n, k) \in M \ ((v.x)^*(w, n, k) = x^* \circ \widehat{v}(w, n, k)).$$

We will now show that

$$\exists i \ (y^* = x^* \circ g_i) \ \Rightarrow \ \exists v \in \mathbf{F}_2 \ (y = v.x)$$

and hence $x \mapsto x^*$ is a reduction. The reader may find useful to refer to Figure 1 while checking the details.

Suppose $y^* = x^* \circ g_i$.

CLAIM 3.6. *g_i is a quasi-shift above l_{i-1}.*

Proof. Deny. Let w_0, n_0, k_0, w_0', n_0', and k_0' be as in (i)–(iii) above. Notice that their choice as well as the decision as to which of (i)–(iii) we fall into
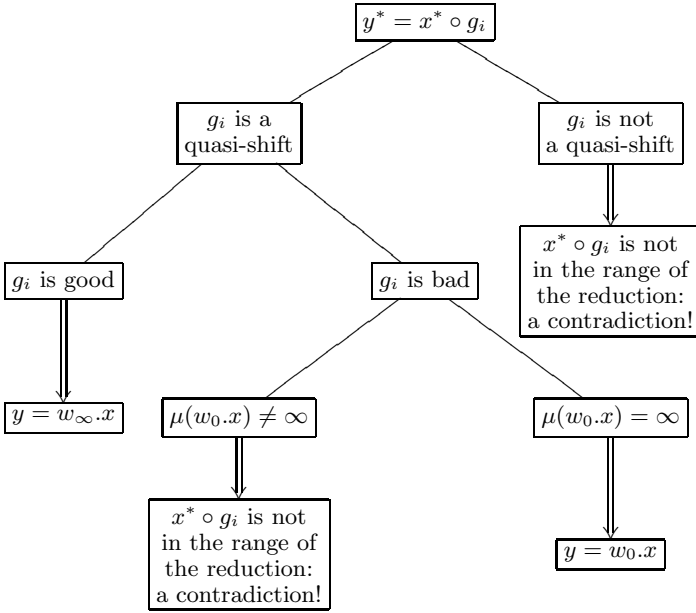
Fig. 1. Plan of the proof of Theorem 3.1

as well as the definition of $x^*(w, n, k)$ for $l_{i-1} < k \leq k_0$ are independent of x. In particular, x^* and y^* agree on (w_0, n_0, k_0). If we are in case (i) then

$$y^*(w_0, n_0, k_0) = x^*(w'_0, n'_0, k'_0) \neq x^*(w_0, n_0, k_0),$$

and if we are in case (ii) then

$$x^*(w_0, n_0, k_0) = y^*(w'_0, n'_0, k'_0) \neq y^*(w_0, n_0, k_0),$$

in both cases reaching a contradiction. If we are in case (iii) then

$$0 = y^*(w_0, n_0, l_i) = x^*(w'_0, n'_0, l_i) = 1,$$

a contradiction again. ∎

Therefore we may assume that

$$\boxed{g_i \text{ is a quasi-shift.}}$$

Again we take cases. Suppose $w_\infty \in \mathbf{F}_2$ and $(n_m)_m \subseteq \mathbb{N}$ witness that g_i is good. Then

$$y^*(1_{\mathbf{F}_2}, n_m, l_i) = x^* \circ g_i(1_{\mathbf{F}_2}, n_m, l_i) = x^*(w_\infty, n_m, l_i)$$
$$= (w_\infty.x)^*(1_{\mathbf{F}_2}, n_m, l_i).$$

As g_i is good, both $(w_\infty.x)^*$ and y^* are defined on $\{(1_{\mathbf{F}_2}, n_m, l_i) \mid m \in \mathbb{N}\}$

as in (1), hence $\forall m \; (y(u_m) = (w_\infty.x)(u_m))$. Therefore

$$\boxed{g_i \text{ is good } \Rightarrow \; y = w_\infty.x.}$$

So we may assume that g_i is bad and let $(w_m)_m \subseteq \mathbf{F}_2$ and $(n_m)_m \subseteq \mathbb{N}$ witness this so that

$$\forall m \in \mathbb{N} \; (y^*(1_{\mathbf{F}_2}, n_m, l_i) = x^* \circ g_i(1_{\mathbf{F}_2}, n_m, l_i) = x^*(w_m, n_m, l_i)).$$

Suppose first $\mu(w_0.x) = \infty$. Then by Claim 3.2, $\forall m \; ((w_m.x)^* = (w_0.x)^*)$ hence

$$x^*(w_m, n_m, l_i) = (w_m.x)^*(1_{\mathbf{F}_2}, n_m, l_i) = (w_0.x)^*(1_{\mathbf{F}_2}, n_m, l_i).$$

Since $(w_0.x)^*$ is defined on $\{(1_{\mathbf{F}_2}, n_m, l_i) \mid m \in \mathbb{N}\}$ as in (2) we see that y^* is defined on $\{(1_{\mathbf{F}_2}, n_m, l_i) \mid m \in \mathbb{N}\}$ as in (2) and hence $\forall m \; (y(u_m) = w_0.x(u_m))$. Therefore

$$\boxed{\mu(w_0.x) = \infty \; \Rightarrow \; y = w_0.x.}$$

Suppose now $1 \leq \mu(w_0.x) = m < \infty$. Then by Claim 3.2,

$$\forall j < m \; (\mu(w_j.x) = m \;\&\; J_m(w_j.x) = J_m(w_0.x)) \quad \text{and} \quad \mu(w_m.x) \leq m.$$

By (3), the first m elements of the sequence $(x^* \circ g_i(1_{\mathbf{F}_2}, n_j, l_i))_j$ are $(3, \ldots, 3, J_m(w_0.x))$. If $m > 1$ (so that the sequence starts with 3) or if $J_m(w_0.x) \neq 0$ then by Claim 3.4 the next element must be

$$x^*(w_m, n_m, l_i) = J_m(w_0.x) \in \{0, 1, 2\}.$$

If $m = 1$ and $J_m(w_0.x) = 0$ then the sequence starts with 0, hence the next element can only be 0 or 3, i.e.,

$$x^*(w_m, n_m, l_i) \in \{0, 3\}.$$

In order to compute this value and eventually reach a contradiction we must consider two cases.

Suppose $\mu(w_m.x) = m$. Since $w_0.x = w_{m-1}.x$ and $z_m.w_0.x = w_m.x$ are distinct, they belong to different $X_m^{(j)}$'s and therefore, by (3),

$$x^*(w_m, n_m, l_i) = J_m(w_m.x) \notin \{J_m(w_0.x), 3\},$$

a contradiction.

Suppose $0 < \mu(w_m.x) < m$. Then $m > 1$ and by (3) again,

$$x^*(w_m, n_m, l_i) = 3 \neq J_m(w_0.x),$$

a contradiction.

Therefore we have shown that

$$\boxed{1 \leq \mu(w_0.x) < \infty \; \Rightarrow \; x^* \circ g_i \text{ is not in the range of the reduction.}}$$

This concludes the proof. ∎

Notice that for $k \geq 5$ or $k = \mathbb{N}$ and G as in the theorem, the inclusion map $5^{\mathbb{N}} \hookrightarrow k^{\mathbb{N}}$ witnesses $\cong_G^k$ is universal. Focusing on Rec, the group of recursive permutations, one can show that

$$\cong_{\mathrm{Rec}}^{\mathbb{N}} \!\restriction\! \{x \in \mathbb{N}^{\mathbb{N}} \mid x : \mathbb{N} \twoheadrightarrow \mathbb{N} \text{ is onto}\}$$

is universal. To see this assign to each non-empty subset $S \subseteq 5 = \{0, \ldots, 4\}$ an integer $\varrho(S) > 0$, and consider the map $5^{\mathbb{N}} \to \{x \in \mathbb{N}^{\mathbb{N}} \mid x : \mathbb{N} \twoheadrightarrow \mathbb{N}$ is onto$\}$, $x \mapsto x^*$, defined as follows: on the even integers we copy x, i.e. $\forall n \ (x^*(2n) = x(n))$, and on the odd integers we start with $\varrho(\mathrm{range}(x))$ consecutive 5's followed by the increasing enumeration of $\mathbb{N} \backslash (\mathrm{range}(x) \cup \{5\})$. It is easy to check that x^* is indeed onto and that $x \mapsto x^*$ is Borel. If $x \circ f = y$ for some recursive f then letting $g(2n + 1) = 2n + 1$ and $g(2n) = 2f(n)$ we find that $x^* \circ g = y^*$. Suppose instead $x^* \circ f = y^*$ for some recursive bijection f. Since the numbers of 5's in x^* and in $x^* \circ f = y^*$ are the same, $\mathrm{range}(x) = \mathrm{range}(y)$ and hence f restricted to the even numbers must be a bijection. Letting $h(n) = \frac{1}{2}f(2n)$ we see that $x \circ h = y$. Therefore $x \mapsto x^*$ is a reduction of $\cong_{\mathrm{Rec}}^5$ to $\cong_{\mathrm{Rec}}^{\mathbb{N}} \!\restriction\! \{x \in \mathbb{N}^{\mathbb{N}} \mid x : \mathbb{N} \twoheadrightarrow \mathbb{N} \text{ is onto}\}$.

By extracting the salient features of Rec used above we get

COROLLARY 3.7. *Let $G_0 \subseteq G \subseteq S_\infty$ be as in the theorem. Suppose G has the following closure property*:

- *if $f \in G$ then $g \in G$ where $g(2n + 1) = 2n + 1$ and $g(2n) = 2f(n)$,*
- *if $f \in G$ and f is a bijection when restricted to the set of even numbers (i.e., $\forall n \ \exists m \ (f(2m) = 2n)$ and $\forall n \ \exists m \ (f(2n) = 2m))$ then $h \in G$ where $h(n) = \frac{1}{2}f(2n)$.*

Then $\cong_G^{\mathbb{N}} \!\restriction\! \{x \in \mathbb{N}^{\mathbb{N}} \mid x : \mathbb{N} \twoheadrightarrow \mathbb{N}$ is onto$\}$ is universal.

Let $\mathcal{L}$ be a language consisting of one binary relation symbol and let $X_{\mathcal{L}} = 2^{\mathbb{N}^2}$ be the space of all $\mathcal{L}$-structures with universe $\mathbb{N}$. Let $\mathrm{Eq}(k) \subseteq X_{\mathcal{L}}$ be the set of all structures which are models for equivalence relations whose equivalence classes are of size at most k, that is, $x \in \mathrm{Eq}(k)$ iff the relation E^x on $\mathbb{N}$ defined by

$$nE^x m \ \Leftrightarrow \ x(n, m) = 1$$

is an equivalence relation on $\mathbb{N}$ and $\forall n \in \mathbb{N} \ (|[n]_{E^x}| \leq k)$. For $x, y \in X_{\mathcal{L}}$ set $x \cong_G^{\mathcal{L}} y$ just in case the models $\langle \mathbb{N}, E^x \rangle$ and $\langle \mathbb{N}, E^y \rangle$ are isomorphic via a bijection in G.

For $G \subseteq S_\infty$ let $\sim_G$ denote the conjugation relation on S_∞ via elements in G

$$x \sim_G y \ \Leftrightarrow \ \exists g \in G \ (g^{-1} \circ x \circ g = y).$$

Let also $\sim_G^k = \sim_G \!\restriction\! \{x \in S_\infty \mid x \text{ is a product of cycles of length } \leq k\}$.

A group $G \subseteq S_\infty$ is *closed under pairing* if there is a pairing function, i.e., a bijection $j : \mathbb{N}^2 \to \mathbb{N}$ with inverses $(j(n,m))_0 = n$ and $(j(n,m))_1 = m$ such that:

For every $g \in G$ the bijection $h \in S_\infty$ defined by

$$h(j(n,m)) = j(g(n), m)$$

is in G, and if

$$f(n) = (g(j(n,0)))_0$$

is a bijection, then f is also in G. For example, Rec is closed under pairing.

PROPOSITION 3.8. *Let* $G \subseteq S_\infty$ *be a countable group closed under pairing. Then*

$$\cong_G^k \ \sqsubseteq_c \ \cong_G^{\mathcal{L}} \upharpoonright \mathrm{Eq}(k+1),$$

that is to say: *the equivalence relation given by the right action of* G *on* $k^{\mathbb{N}}$ *is continuously embeddable into the* G-*isomorphism relation between equivalence relations on* $\mathbb{N}$ *with equivalence classes of size* $\leq k+1$.

Similarly, $\cong_G^k$ *continuously embeds into conjugacy on* S_∞ *via elements of* G *restricted to products of cycles of size* $\leq k+1$:

$$\cong_G^k \ \sqsubseteq_c \ \sim_G^{k+1}.$$

In particular, for all $G_0 \subseteq G \subseteq S_\infty$ *as in the theorem,* $\cong_G^{\mathcal{L}} \upharpoonright \mathrm{Eq}(6)$ *and* $\sim_G^6$ *are both universal.*

Proof. Let $\vartheta : k^{\mathbb{N}} \to \mathrm{Eq}(k+1)$ be defined by

$$j(n,m)\, E^{\vartheta(x)}\, j(n',m') \ \Leftrightarrow \ n = n' \ \& \ (m = m' \ \lor \ m, m' \leq x(n) + 1)$$

where j is the pairing function for G. (It is most convenient to visualize $E^{\vartheta(x)}$ as the equivalence relation on $\mathbb{N}^2$ obtained by connecting on each vertical line $\{(n,m) \mid m \in \mathbb{N}\}$ all the points $\leq x(n) + 1$.) It is immediate to check that $\vartheta(x) \in \mathrm{Eq}(k+1)$ and that ϑ is continuous and injective.

Suppose first $x, y \in k^{\mathbb{N}}$ and $x \circ g = y$ for some $g \in G$. Let $h \in G$ be defined by $h(j(n,m)) = j(g(n), m)$. Then

$$h(j(n,m))\, E^{\vartheta(x)}\, h(j(n',m')) \ \Leftrightarrow \ j(g(n),m)\, E^{\vartheta(x)}\, j(g(n'),m')$$

$$\Leftrightarrow \ j(n,m)\, E^{\vartheta(y)}\, j(n',m'),$$

that is, $\vartheta(y) \cong_G^{\mathcal{L}} \vartheta(x)$ via h.

Conversely, suppose $\vartheta(y) \cong_G^{\mathcal{L}} \vartheta(x)$ via some $g \in G$. Let $f \in G$ be defined by $f(n) = (g(j(n,0)))_0$. We must show that $x \circ f = y$. Fix $n \in \mathbb{N}$. Since $[j(n,0)]_{E^{\vartheta(y)}}$ has $y(n) + 1$ elements and g is an isomorphism between $E^{\vartheta(y)}$ and $E^{\vartheta(x)}$, we see that $[g(j(n,0))]_{E^{\vartheta(x)}}$ also has $y(n)+1$ elements. In particular, $[g(j(n,0))]_{E^{\vartheta(x)}}$ is not a singleton. But $g(j(n,0)) = j(f(n), l)$ for some l, so $[j(f(n),l)]_{E^{\vartheta(x)}} = [j(f(n),0)]_{E^{\vartheta(x)}}$ has $x(f(n)) + 1$ elements. Therefore $y(n) = x(f(n))$, which is what we had to prove.

For $\sim_G^{k+1}$ we use essentially the same reduction: for $x \in k^{\mathbb{N}}$ let $\varphi(x) \in S_\infty$ be defined by $\varphi(x) = \prod_n c_n(x)$ where $c_n(x)$ is the cycle

$$j(n,0) \longmapsto j(n,1) \longmapsto \cdots \longmapsto j(n,x(n)+1) \ .$$

It is immediate to check that $x \cong_G^k y \Leftrightarrow \varphi(x) \sim_G^{k+1} \varphi(y)$. ∎

Even if the theorem holds for $k = 2$ (as we conjecture) the proposition above does not yield any information about the universality of $\cong_G^{\mathcal{L}} \!\restriction \mathrm{Eq}(2)$. We can still though relate this equivalence relation to $\sim_G$.

For $x \in \mathrm{Eq}(2)$ let $x^* \in S_\infty$ be defined by

$$x^*(n) = \begin{cases} m & \text{if } [n]_{E^x} = \{n,m\} \text{ and } n \neq m, \\ n & \text{if } [n]_{E^x} = \{n\}. \end{cases}$$

Then $x^* \in I := \{f \in S_\infty \mid f \circ f = \mathrm{id}\}$, the set of all involutions, and the map $\mathrm{Eq}(2) \to I$, $x \mapsto x^*$, is clearly a Borel bijection. Moreover, if $G \subseteq S_\infty$ is a subgroup, $g \in G$, and $x, y \in \mathrm{Eq}(2)$ then $g : \langle \mathbb{N}, E^x \rangle \to \langle \mathbb{N}, E^y \rangle$ is an isomorphism iff $g \circ x^* \circ g^{-1} = y^*$. Therefore we have proved

PROPOSITION 3.9. *Let $G \subseteq S_\infty$ be a subgroup. The logic action of G on* $\mathrm{Eq}(2)$ *is isomorphic to the conjugacy of G on elements of I. In particular*,

$$\cong_G^{\mathcal{L}} \!\restriction \mathrm{Eq}(2) \ \cong_{\mathrm{B}} \sim_G \!\restriction I.$$

4. Conjugacy of subgroups. We will now prove Theorem 1.3. The proof will use a combination of the techniques used in proving 3.1 together with a few facts about free groups.

Let $\mathbf{F}(X)$ be the free group on the set $X \neq \emptyset$, let $x \in X$ and let $w \in \mathbf{F}(X)$. Let $x_1^{k_1} \ldots x_n^{k_n}$ be the unique reduced word for w. Then we say that w *starts* with x_1 and *ends* with x_n. Whenever we write "*vw* is a reduced word" we mean that both v and w are already written as reduced words, and for no $x \in X$, v ends with x and w starts with x. We say that x^k *occurs in* w ($k \in \mathbb{Z} \setminus \{0\}$) if $w = v_0 x^k v_1$ and $v_0 x^k v_1$ is a reduced word, i.e., v_0 and v_1 are reduced and neither v_0 ends with x nor v_1 begins with x. If x^k occurs in w then we say that x is a *generator* in w. It is easy to see that if x is a generator in w, then it is a generator in every w^n, for $n \neq 0$. A word w is *symmetric* if it can be written in reduced form as $w = v_0 x^k v_0^{-1}$; otherwise it is *asymmetric*.

LEMMA 4.1. *If $w \in \mathbf{F}(X)$ is asymmetric then there is a fixed bound M depending on w such that if x^k occurs in any w^n then $|k| \leq M$, i.e.*,

$$\exists M > 0 \ \forall x \in X \ \forall k \in \mathbb{Z} \setminus \{0\} \ \forall n \ (x^k \text{ occurs in } w^n \Rightarrow |k| \leq M).$$

Proof. It is enough to show that for any $x \in X$ which is a generator of w there is an M_x such that if x^h occurs in w^n, then $|h| \leq M_x$, so that we

can set

$$M = \sup\{M_x \mid x \text{ is a generator in } w\}.$$

Let x be a generator in w so that $w = v_0 x^k v_1$ is a reduced word and $v_1 \neq v_0^{-1}$. Then the reduced form of $v_1 v_0$ cannot start and end with x since otherwise either v_1 would have to start with x or v_0 would have to end with x, hence $v_0 x^k v_1$ would not be reduced. Consider the product

$$w^n = v_0 \boxed{x^k} v_1 \cdot v_0 \boxed{x^k} v_1 \ldots v_0 \boxed{x^k} v_1.$$

After the reduction:

• if $v_1 \cdot v_0$ in reduced form does not start or end with x, then the boxed occurrences of x^k remain unchanged, so let

$$M_x = \max(|k|, \sup\{|h| \mid x^h \text{ occurs in } v_0, \text{ or in } v_1, \text{ or in } v_1 v_0\}),$$

• if $v_1 \cdot v_0$ in reduced form is ux^h or $x^h u$, then the first (respectively: the last) boxed occurrence of x^k remains unchanged, so let

$$M_x = \max(|k|, |k+h|, \sup\{|j| \mid x^j \text{ occurs in } v_0, \text{ or in } v_1, \text{ or in } u\}). \ \blacksquare$$

Proof of Theorem 1.3. Since inside every free group on two generators there is a copy of the free group on three generators, pick independent elements $a, b, c \in G$ so that $\langle a, b, c \rangle$ is a free group on 3 generators. Let $\mathbf{F}_3 = \langle a, b, c \rangle$ be this particular realization of the free group on 3 generators and let $\mathbf{F}_2 = \langle a, b \rangle \subset \mathbf{F}_3$. We want to construct a copy of $\mathbf{F}_\omega$, the free group of rank $\aleph_0$, inside $\mathbf{F}_3$. We need the following lemma.

LEMMA 4.2. *Let* $w_1, \ldots, w_n \in \mathbf{F}_2$ *be distinct. Then* $\langle w_1 c w_1^{-1}, \ldots, w_n c w_n^{-1} \rangle$ *is a free group on n generators. In particular, if* $(w_n)_n \subseteq \mathbf{F}_2$ *are all distinct then* $\langle w_1 c w_1^{-1}, w_2 c w_2^{-1}, \ldots \rangle$ *is a free group of rank $\aleph_0$.*

Proof. Choose new letters $\sigma_1, \ldots, \sigma_n$, and let $\langle \sigma_1, \ldots, \sigma_n \rangle$ be the free group of rank n generated by them. It is enough to show that $\ker(\varphi)$ is null, where $\varphi : \langle \sigma_1, \ldots, \sigma_n \rangle \twoheadrightarrow \langle w_1 c w_1^{-1}, \ldots, w_n c w_n^{-1} \rangle$ is the epimorphism induced by the map $\sigma_i \mapsto w_i c w_i^{-1}$. Let $v = \sigma_{i_1}^{k_1} \sigma_{i_2}^{k_2} \ldots \sigma_{i_m}^{k_m}$ be a reduced word of $\langle \sigma_1, \ldots, \sigma_n \rangle$. If

$$\varphi(v) = w_{i_1} c^{k_1} w_{i_1}^{-1} \cdot w_{i_2} c^{k_2} w_{i_2}^{-1} \ldots w_{i_m} c^{k_m} w_{i_m}^{-1} = 1_{\mathbf{F}_2}$$

and $m > 1$, then $w_{i_j} = w_{i_{j+1}}$ for all $1 \leq j < m$, hence $\sigma_{i_j} = \sigma_{i_{j+1}}$. Therefore $m = 1$, $v = \sigma_{i_1}^{k_1}$ and hence $\varphi(v) = w_{i_1} c^{k_1} w_{i_1}^{-1} = 1_{\mathbf{F}_2}$ implies $k_1 = 0$. This contradicts the assumption that v is reduced. $\blacksquare$

Define also the free group on two generators $\widetilde{\mathbf{F}}_2 = \langle a^2, b^2 \rangle \subset \mathbf{F}_2$, and let $w \mapsto \widetilde{w}$ be the isomorphism $\mathbf{F}_2 \to \widetilde{\mathbf{F}}_2$ given by $a \mapsto a^2$ and $b \mapsto b^2$. For any $w \in \mathbf{F}_2$ and $n \in \mathbb{Z}$ let

$$\gamma(w, n) = \widetilde{w}^{-1} b a^{2n} c a^{-2n} b^{-1} \widetilde{w} \in \mathbf{F}_3.$$

Let $\Gamma = \bigcup_{w \in \mathbf{F}_2} \Gamma_w \subset \mathbf{F}_3$, where $\Gamma_w = \{\gamma(w,n) \mid n \in \mathbb{Z}\}$. Suppose $\gamma(w,n) = \gamma(z,m)$. Then

$$\widetilde{w}^{-1} ba^{2n} ca^{-2n} b^{-1} \widetilde{w} = \widetilde{z}^{-1} ba^{2m} ca^{-2m} b^{-1} \widetilde{z}.$$

As there is only one occurrence of c on both sides of the equation, we have

$$\widetilde{w}^{-1} ba^{2n} = \widetilde{z}^{-1} ba^{2m}.$$

As $\widetilde{w}, \widetilde{z} \in \widetilde{\mathbf{F}}_2$, it is easy to see that $w = z$ and $n = m$. Therefore

$$\forall w, z \in \mathbf{F}_2 \ (w \neq z \Rightarrow \Gamma_z \cap \Gamma_w = \emptyset).$$

Since $\gamma(w,n) = (\widetilde{w}^{-1} ba^{2n}) c (\widetilde{w}^{-1} ba^{2n})^{-1}$ and $\widetilde{w}^{-1} ba^{2n} \in \mathbf{F}_2$, Lemma 4.2 implies that Γ is a countable set of independent elements and

$$\mathbf{F}_\omega = \langle \Gamma \rangle \subset \mathbf{F}_3 \subseteq G$$

is a free group on $\aleph_0$ generators. We now concentrate on subgroups of $\mathbf{F}_\omega$ and from now on *words* will mean *words built from elements in Γ*. Notice that in our set-up $\mathbf{F}_2 \not\subseteq \mathbf{F}_\omega$.

The plan is to associate, in a Borel way, with each $x \in 2^{\mathbf{F}_2}$ a group $H(x) \subseteq \mathbf{F}_\omega$ such that $H(x) \cong \mathbf{F}_\omega$ and

$$\forall w \in \mathbf{F}_2 \ \forall x \in 2^{\mathbf{F}_2} \ (H(w.x) = \widetilde{w} H(x) \widetilde{w}^{-1}),$$
$$\forall g \in G \ \forall x, y \in 2^{\mathbf{F}_2} \ (H(y) = g H(x) g^{-1} \Rightarrow \exists w \in \mathbf{F}_2 \ (w.x = y)).$$

This implies that the shift action of $\mathbf{F}_2$ on $2^{\mathbf{F}_2}$ is reducible to $E_c(G, \mathrm{Sgr}(G))$, proving the universality of the latter.

The group $H(x)$ will be given via an infinite set $\mathcal{G}(x)$ of generators so that

(1) $\mathcal{G}(x)$ is an independent set of elements of $\mathbf{F}_\omega$ and $\langle \mathcal{G}(x) \rangle = H(x) \cong \mathbf{F}_\omega$.

In order to define the $\mathcal{G}(x)$'s we need to re-arrange the enumeration of Γ a bit: fix a bijection $j : \mathbb{N}^2 \to \mathbb{Z}$ and set

$$\alpha(w,n,m) = \gamma(w, j(n,m)).$$

The third component of the indexing gives the *level* of the elements of Γ, so we say that $\alpha(w,n,m)$ is of level m. Fix for every $i > 0$ an infinite set $S_i \subseteq \mathbb{P}$ (= the set of all primes) such that $i \neq j \Rightarrow S_i \cap S_j = \emptyset$. As in the proof of 3.1 an increasing sequence of integers $(l_i)_{i \in \mathbb{N}}$ with $l_0 = -1$ will be defined inductively. At stage i the only elements added to $\mathcal{G}(x)$ will be of the form γ^p, where $\gamma \in \Gamma$ is of level between l_{i-1} and l_i and p is some unique element of S_i; moreover, some such element should be added at this stage:

(2) $\forall z \in \mathcal{G}(x) \ \exists \alpha(w,n,m) \in \Gamma \ \exists p \ (\alpha(w,n,m)^p = z \ \& \ (l_{i-1} < m \leq l_i \Rightarrow p \in S_i)) \ \& \ \forall \gamma \in \Gamma \ \forall p, q \in \mathbb{P} \ (\gamma^p, \gamma^q \in \mathcal{G}(x) \Rightarrow p = q)$.

(3) $\exists \alpha(w,n,m) \in \Gamma \ \exists p \in S_i \ (l_{i-1} < m \leq l_i \ \& \ \alpha(w,n,m)^p \in \mathcal{G}(x))$.

(4) $\forall w \in \mathbf{F}_2 \ (\widetilde{w}\mathcal{G}(x)\widetilde{w}^{-1} = \mathcal{G}(w.x))$.

(5)   If $w \in H(x)$ and $\alpha(w, n, m)^k$ occurs in w and $l_{i-1} < m \le l_i$ then

$$\exists p \in S_i \ (p \mid k \ \& \ \alpha(w, n, m)^p \in \mathcal{G}(x)).$$

In particular, $\Gamma \cap \mathcal{G}(x) = \emptyset$. By (2) the prime p is unique.

(6)   If vw is a reduced word then $vw \in H(x) \Rightarrow v, w \in H(x)$.

Notice that properties (2) and (3) imply properties (1) and (5), property (6) follows from property (5), and as $\widetilde{z}^{-1}\gamma(w, n)^k \widetilde{z} = \gamma(wz, n)^k$ for any $z, w \in \mathbf{F}_2$ and $n, k \in \mathbb{Z}$, property (4) will hold.

We now start the construction.

In analogy with the proof of 3.1, we say that an element $g \in G$ is a *quasi-shift above l* if

$\forall w, n \ (g^{-1} \cdot \alpha(w, n, l+1) \cdot g \in \mathbf{F}_\omega$

& every generator from Γ in $g^{-1} \cdot \alpha(w, n, l+1) \cdot g$

is either of the form $\alpha(z, m, k)$ with $k \le l$

or else of the form $\alpha(z, n, l+1)$

& $\exists z \ \alpha(z, n, l+1)$ is a generator in $g^{-1} \cdot \alpha(w, n, l+1) \cdot g)$.

Fix an enumeration $(g_i)_{i \ge 1}$ of G.

Set $l_0 = -1$ and suppose l_{i-1} has been defined for some $i \ge 1$. We now distinguish two cases:

• g_i is not a quasi-shift above l_{i-1}. Then letting $k_0 = l_{i-1} + 1$, we have the following possibilities:

(i) $\exists w_0, n_0 \ (g_i^{-1} \cdot \alpha(w_0, n_0, k_0) \cdot g_i \notin \mathbf{F}_\omega)$.

(ii) Case (i) fails and

$\exists w_0, n_0, w_0', n_0', k_0' \ (k_0' > k_0$

$\& \ \alpha(w_0', n_0', k_0')$ is a generator in $g_i^{-1} \cdot \alpha(w_0, n_0, k_0) \cdot g_i)$.

(iii) Cases (i) and (ii) fail and

$\exists w_0, n_0, w_0', n_0' \ (n_0 \ne n_0'$

$\& \ \alpha(w_0', n_0', k_0)$ is a generator in $g_i^{-1} \cdot \alpha(w_0, n_0, k_0) \cdot g_i)$.

(iv) Cases (i)–(iii) fail and

$\exists w_0, n_0 \ \forall w_0', n_0', k_0' \ (\alpha(w_0', n_0', k_0')$ is a generator in $g_i^{-1} \cdot \alpha(w_0, n_0, k_0) \cdot g_i$

$$\Rightarrow k_0' < k_0).$$

Then set $l_i = \max(k_0, k_0')$. (Notice that if g_i is not a quasi-shift above l_{i-1} because of (iv) then all of the generators of $g_i^{-1} \cdot \alpha(w_0, n_0, k_0) \cdot g_i$ are of level $< k_0$.)

• Otherwise, that is: g_i is a quasi-shift above l_{i-1}. In this case set $l_i = l_{i-1} + 1$.

Suppose g_i is a quasi-shift above l_{i-1}. We say that g_i is *good* if there is an increasing sequence $(n_m)_m$ of natural numbers and a $w_\infty \in \mathbf{F}_2$ such that

$$\alpha(w_\infty, n_m, l_i) \text{ is a generator in } g_i^{-1} \cdot \alpha(1_{\mathbf{F}_2}, n_m, l_i) \cdot g_i.$$

If g_i is not good then it is called *bad*. In this case there is an increasing sequence $(n_m)_m$ of natural numbers and a sequence $(w_m)_m$ of distinct elements in $\mathbf{F}_2$ such that

$$\forall m \in \mathbb{N} \ (\alpha(w_m, n_m, l_i) \text{ is a generator in } g_i^{-1} \cdot \alpha(1_{\mathbf{F}_2}, n_m, l_i) \cdot g_i).$$

Let also $(z_m)_{m \geq 1}$, μ and J_m be defined as in the proof of 3.1.

Finally, we define the map $x \mapsto \mathcal{G}(x)$, and hence the reduction $H : 2^{\mathbf{F}_2} \to \mathrm{Sgr}(G)$, $x \mapsto H(x)$, so that properties (1)–(6) hold.

> **g_i is not a quasi-shift above l_{i-1}.**

Let w_0, n_0, k_0, w_0', n_0', k_0' be as in cases (i)–(iv).

Suppose case (i) holds. Then $l_i = k_0$. Let r be the least positive integer such that $g_i^{-1} \cdot \alpha(w_0, n_0, k_0)^r \cdot g_i \in \mathbf{F}_\omega$ if such an integer exists, or $r = 0$ otherwise. Let $p = \min(S_i \setminus \{r\})$ be the least element of S_i different from r. We now require in our construction that

$$\forall x \in 2^{\mathbf{F}_2} \ \forall w \in \mathbf{F}_2 \ (\alpha(w, n_0, l_i)^p \in \mathcal{G}(x)).$$

Suppose case (ii) holds. Then $k_0 = l_{i-1} + 1 < l_i$. Let $p = \min(S_i)$ and set

$$\forall x \in 2^{\mathbf{F}_2} \ \forall w \in \mathbf{F}_2 \ (\alpha(w, n_0, k_0)^p \in \mathcal{G}(x)).$$

Suppose case (iii) or (iv) holds. Let $p = \min(S_i)$ and set

$$\forall x \in 2^{\mathbf{F}_2} \ \forall w \in \mathbf{F}_2 \ (\alpha(w, n_0, l_i)^p \in \mathcal{G}(x)).$$

For $k \in (l_{i-1}, l_i]$ and $n \in \mathbb{N}$, $p \in \mathbb{P}$ place $\alpha(w, n, k)^p$ in $\mathcal{G}(x)$ only if required by the cases above.

We now consider the other case, namely

> **g_i is a quasi-shift above l_{i-1}.**

There are two possibilities.

• For some $\alpha(w_0, n_0, l_i) \in \Gamma$, the reduced word v obtained from $g_i^{-1} \cdot \alpha(w_0, n_0, l_i) \cdot g_i$ is *either* asymmetric *or else* it is symmetric of the form $v_1 \cdot \alpha(w_0', n_0', k)^m \cdot v_1^{-1}$ with $k < l_i$ and $m \neq 0$. In either case, by Lemma 4.1 or by inspection, there is M such that

$$\forall r \ (\alpha(z, n_0, l_i)^k \text{ occurs in } v^r \Rightarrow |k| \leq M).$$

When this happens g_i is said to be *bounded*. Let p be the least element in S_i larger than M and set

$$\forall x \in 2^{\mathbf{F}_2} \ \forall w \in \mathbf{F}_2 \ (\alpha(w, n_0, l_i)^p \in \mathcal{G}(x)).$$

• Otherwise $\forall w \in \mathbf{F}_2 \ \forall n \in \mathbb{N} \ \exists z \in \mathbf{F}_2 \ \exists u \in \mathbf{F}_\omega$ such that

$$g_i^{-1} \cdot \alpha(w, n, l_i) \cdot g_i = u \cdot \alpha(z, n, l_i)^{r(w,n)} \cdot u^{-1}$$

where $r(w, n) \in \mathbb{Z} \setminus \{0\}$. In this case g_i is said to be *unbounded*.

CASE 1: $\exists w_0, n_0 \ (|r(w_0, n_0)| > 1)$, that is, for some w_0, n_0, z, u,

$$g_i^{-1} \cdot \alpha(w_0, n_0, l_i) \cdot g_i = u \cdot \alpha(z, n_0, l_i)^r \cdot u^{-1}$$

with $r = r(w_0, n_0)$ and $|r| > 1$. Then let $p = \min(S_i)$ and set

$$\forall x \in 2^{\mathbf{F}_2} \ \forall w \in \mathbf{F}_2 \ (\alpha(w, n_0, l_i)^p \in \mathcal{G}(x)).$$

CASE 2: $\forall w \in \mathbf{F}_2 \ \forall n \in \mathbb{N} \ (|r(w, n)| = 1)$, that is,

$\forall w \in \mathbf{F}_2 \ \forall n \in \mathbb{N} \ \exists z \in \mathbf{F}_2 \ \exists u \in \mathbf{F}_\omega \ (g_i^{-1} \cdot \alpha(w, n, l_i) \cdot g_i = u \cdot \alpha(z, n, l_i)^{\pm 1} \cdot u^{-1}).$

Then we can mimic the construction of 3.1. Fix an enumeration $(u_m)_m$ of $\mathbf{F}_2$ without repetitions. Let $p_0, \ldots, p_5$ be the first six elements of S_i. We distinguish three possibilities.

• g_i is good. Then $\exists w_\infty \ \exists (n_m)_m \ \exists (v_m)_m$ such that $(n_m)_m$ is increasing and $g_i^{-1} \cdot \alpha(1_{\mathbf{F}_2}, n_m, l_i) \cdot g_i = v_m \cdot \alpha(w_\infty, n_m, l_i)^{\pm 1} \cdot v_m^{-1}$. By thinning down the sequence we may assume that the exponent is constant, say 1. Set

$$\alpha(w, n_m, l_i)^{p_1} \in \mathcal{G}(x) \ \Leftrightarrow \ w.x(u_m) = 1,$$
$$\alpha(w, n, l_i)^{p_0} \in \mathcal{G}(x) \ \Leftrightarrow \ (n = n_m \ \& \ w.x(u_m) = 0) \lor n \notin \{n_m \mid m \in \mathbb{N}\}.$$

So we may assume that g_i is bad hence $\exists (w_m)_m \ \exists (n_m)_m \ \exists (v_m)_m$ such that the n_m's are increasing, the w_m's are distinct, and $g_i^{-1} \cdot \alpha(1_{\mathbf{F}_2}, n_m, l_i) \cdot g_i = v_m \cdot \alpha(w_m, n_m, l_i)^{\pm 1} \cdot v_m^{-1}$. Again by thinning down we may assume that the exponent is 1.

• g_i is bad and $\mu(w.x) = \infty$. Set

$$\alpha(w, n_m, l_i)^{p_1} \in \mathcal{G}(x) \ \Leftrightarrow \ w.x(u_n) = 1,$$
$$\alpha(w, n, l_i)^{p_0} \in \mathcal{G}(x) \ \Leftrightarrow \ (n = n_m \ \& \ w.x(u_n) = 0) \lor n \notin \{n_m \mid m \in \mathbb{N}\}.$$

• g_i is bad and $\mu(w.x) < \infty$. Then set

$$\alpha(w, n, l_i)^{p_j} \in \mathcal{G}(x),$$

where

$$j = \begin{cases} 0 & \text{if } n \notin \{n_m \mid m \in \mathbb{N}\}, \\ 2 & \text{if } n = n_m \text{ and } m < \mu(w.x) - 1 \text{ or } m > \mu(w.x), \\ J_{\mu(w.x)}(w.x) + 3 & \text{if } n = n_m \text{ and } m \in \{\mu(w.x), \mu(w.x) - 1\}. \end{cases}$$

Finally, no γ^p not mentioned in the above is allowed in $\mathcal{G}(x)$.

This concludes the definition of $x \mapsto \mathcal{G}(x)$.

It is straightforward to check that Properties (1)–(6) hold and therefore

$$\forall x \in 2^{\mathbf{F}_2} \ \forall w \in \mathbf{F}_2 \ (H(w.x) = \widetilde{w} H(x) \widetilde{w}^{-1}).$$

The following claim, whose proof is left to the reader, is the analogue of 3.4.

CLAIM 4.3. *Suppose g_i is an unbounded quasi-shift satisfying Case 2, i.e.,*

$$\forall w \in \mathbf{F}_2 \ \forall n \in \mathbb{N} \ \exists z \in \mathbf{F}_2 \ \exists u \in \mathbf{F}_\omega \ (g_i^{-1} \cdot \alpha(w, n, l_i) \cdot g_i = u \cdot \alpha(z, n, l_i)^{\pm 1} \cdot u^{-1}).$$

Suppose also $(w_m)_m$, $(n_m)_m$, and $(v_m)_m$ witness that g_i is bad. Then for all $x \in 2^{\mathbf{F}_2}$,

$$\mu(x) = \infty \ \Leftrightarrow \ \forall m \ (\alpha(1_{\mathbf{F}_2}, n_m, l_i)^{p_0} \in \mathcal{G}(x) \vee \alpha(1_{\mathbf{F}_2}, n_m, l_i)^{p_1} \in \mathcal{G}(x))$$

and if $\mu(x) < \infty$ and $\alpha(1_{\mathbf{F}_2}, n_m, l_i)^p \in \mathcal{G}(x)$ then

$$p = \begin{cases} p_2 & \text{if } m \notin \{\mu(x) - 1, \mu(x)\}, \\ p_j & \text{if } m \in \{\mu(x) - 1, \mu(x)\} \text{ and } j = J_{\mu(x)}(x) + 3. \end{cases}$$

We will now show that

$$\exists i \ (g_i H(x) g_i^{-1} = H(y) \Rightarrow \exists w \in \mathbf{F}_2 \ (y = w.x)).$$

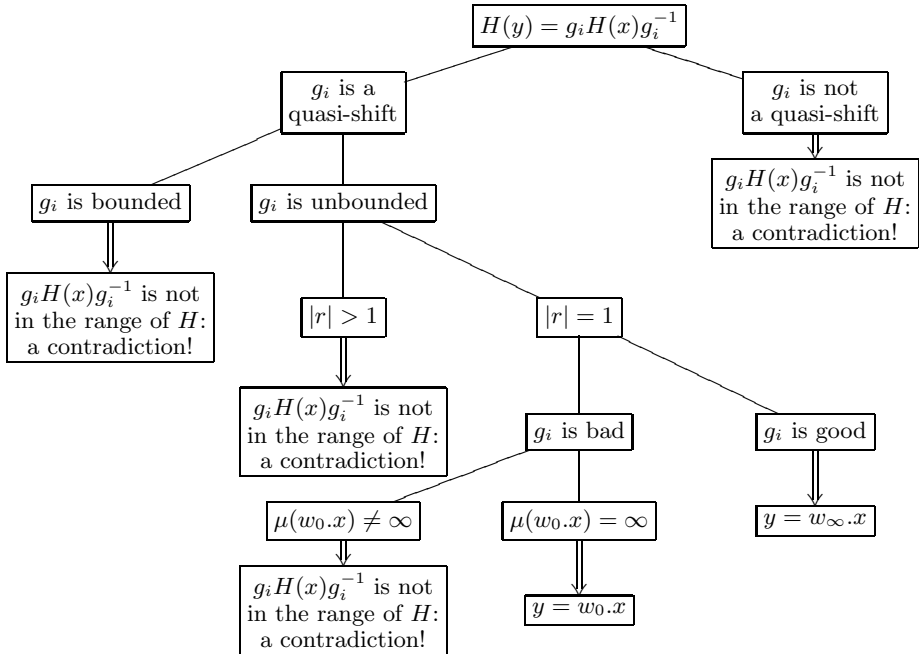The reader may find it useful to refer to Figure 2 while checking the details.

Fig. 2. Plan of the proof of Theorem 1.3

Assume that
$$H(y) = g_i H(x) g_i^{-1}.$$

Suppose g_i is not a quasi-shift, and let $w_0, n_0, k_0, w_0', n_0', k_0'$ be as in (i)–(iv).

If (i) holds then we have $k_0 = l_i$ and $\alpha(w_0, n_0, k_0)^p \in \mathcal{G}(y)$, where $p = \min(S_i \setminus \{r\})$ and $r > 0$ is least such that $g_i^{-1} \cdot \alpha(w_0, n_0, k_0)^r \cdot g_i \in \mathbf{F}_\omega$ if such an r exists, or $r = 0$ otherwise. Since $\alpha(w_0, n_0, k_0)^p \in H(y)$ we have

$$g_i^{-1} \cdot \alpha(w_0, n_0, k_0)^p \cdot g_i \in H(x) \subseteq \mathbf{F}_\omega,$$

hence $r > 0$. As r and p are relatively prime let $\lambda, \nu \in \mathbb{Z}$ be such that $\lambda r + \nu p = 1$ so that

$$g_i^{-1} \cdot \alpha(w_0, n_0, k_0) \cdot g_i = (g_i^{-1} \cdot \alpha(w_0, n_0, k_0)^r \cdot g_i)^\lambda \cdot (g_i^{-1} \cdot \alpha(w_0, n_0, k_0)^p \cdot g_i)^\nu \in \mathbf{F}_\omega$$

contradicting our assumption case.

If (ii) holds then $l_{i-1} + 1 = k_0 < l_i = k_0'$, $\alpha(w_0, n_0, k_0)^p \in \mathcal{G}(y)$, where $p = \min(S_i)$, and

$$\forall w, n, r \ (\alpha(w, n, k_0')^r \notin \mathcal{G}(x)).$$

By case hypothesis $\alpha(w_0', n_0', k_0')$ is a generator in $g_i^{-1} \cdot \alpha(w_0, n_0, k_0)^p \cdot g_i \in H(x)$, hence by (5) above, $\alpha(w_0', n_0', k_0')^q \in \mathcal{G}(x)$ for some $q \in S_i$ such that $q \mid p$. A contradiction.

If (iii) holds then $k_0 = l_i$, $\alpha(w_0, n_0, l_i)^{\min(S_i)} \in \mathcal{G}(y)$, and $\alpha(w_0', n_0', l_i)^r \notin \mathcal{G}(x)$, for any r. But $g_i^{-1} \cdot \alpha(w_0, n_0, l_i)^{\min(S_i)} \cdot g_i \in H(x)$ implies by (5) that $\alpha(w_0', n_0', l_i)^q \in \mathcal{G}(x)$ for some appropriate $q \in S_i$. A contradiction.

So suppose (iv) holds. Then $k_0 = l_i$, $\alpha(w_0, n_0, l_i)^p \in \mathcal{G}(y) \subseteq H(y)$, where $p = \min(S_i)$, and all generators of $g_i^{-1} \cdot \alpha(w_0, n_0, l_i) \cdot g_i$ are of level $< l_i$. For notational ease let $v = g_i^{-1} \cdot \alpha(w_0, n_0, l_i) \cdot g_i$ so that $v^p \in H(x)$. If we show that $v \in H(x)$ then we will reach the desired contradiction, since this would imply that $\alpha(w_0, n_0, l_i) = g_i \cdot v \cdot g_i^{-1} \in H(y)$, against (5).

If v were a generator then, by case assumption, its level would be between l_{j-1} and l_j, with $j < i$, so by $v^p \in H(x)$ and by (5), there should be a $q \in S_j$ such that $q \mid p$, which is absurd. Therefore we may assume that $v \notin \Gamma$. If $v \ldots v$ is in reduced form (in other words: if v starts and ends with different generators) then we are done by (6), so we may assume otherwise. Let v_0 be the longest initial segment of the word $v \in \mathbf{F}_\omega$ such that v ends with v_0^{-1}, and let $v = v_0 \cdot v_1 \cdot v_0^{-1}$. Suppose first v_0 is non-empty. Then either

(a) $v_0 \cdot v_1 \cdot v_0^{-1}$ is a reduced word, or else

(b) v_0 ends with the same generator that v_1 starts with, or else

(c) v_1 ends with the same generator that v_0^{-1} starts with, and (b) fails.

If v_0 is empty, then

(d) $v = \gamma^h \cdot u \cdot \gamma^k$ with $\gamma \in \Gamma$, $h, k \in \mathbb{Z} \setminus \{0\}$, $h + k \neq 0$, and u does not start or end with γ.

Note that cases (a), (b), (c), and (d) are mutually exclusive.

Let us deal with case (d) first. Then

$$v^p = \gamma^h \cdot u \cdot \gamma^{h+k} \cdot u \ldots u \cdot \gamma^{h+k} \cdot u \cdot \gamma^k$$

is a reduced word, so by (6), $\gamma^h, u, \gamma^k \in H(x)$ and therefore $v = \gamma^h \cdot u \cdot \gamma^k \in H(x)$.

If case (a) holds then we have two subcases. Either $v_1 \ldots v_1$ is in reduced form so that v^p can be written in reduced form as

$$v^p = v_0 \cdot \underbrace{v_1 \ldots v_1}_{p} \cdot v_0^{-1},$$

and hence by (6), $v_0, v_1 \in H(x)$, and thus $v \in H(x)$, or else v_1 starts and ends with the same generator, so by (6) and case (d) applied to v_1,

$$v_0 \cdot v_1^p \cdot v_0^{-1} \in H(x) \;\Rightarrow\; v_0, v_1^p \in H(x) \;\Rightarrow\; v_0, v_1 \in H(x),$$

hence $v \in H(x)$.

If case (b) holds, let $\gamma \in \Gamma$ be such that $v_0 = z \cdot \gamma^h$ and $v_1 = \gamma^k \cdot u$ are both reduced words. By case assumption, z does not end with γ, and $h, k \in \mathbb{Z} \setminus \{0\}$ have the same sign. Then

$$v^p = z \cdot \gamma^{h+k} \cdot u \cdot \gamma^k \cdot u \ldots \gamma^k \cdot u \cdot \gamma^{-h} \cdot z^{-1}$$

is in reduced form, so by (6), $z, u, \gamma^k, \gamma^{-h} \in H(x)$ and therefore

$$v = (z \cdot \gamma^h) \cdot (\gamma^k \cdot u) \cdot (z \cdot \gamma^h)^{-1} \in H(x).$$

Case (c) is similar and left to the reader.

Therefore in all cases $v \in H(x)$, reaching a contradiction. Thus

$$\boxed{g_i \text{ is not a quasi-shift above } l_{i-1} \;\Rightarrow\; g_i H(x) g_i^{-1} \text{ is not in the range of } H.}$$

So we may assume from this point on that g_i is a quasi-shift above l_{i-1}.

Suppose g_i is bounded and let $\alpha(w_0, n_0, l_i)$ witness this. Let also $\alpha(z, n_0, l_i)$ be a generator in $v = g_i^{-1} \cdot \alpha(w_0, n_0, l_i) \cdot g_i$. Since $\alpha(w_0, n_0, l_i)^p \in H(y)$, we have $g_i^{-1} \cdot \alpha(w_0, n_0, l_i)^p \cdot g_i = v^p \in H(x)$, hence its generators to some appropriate prime powers must be in $\mathcal{G}(x)$. In particular, this must be true of $\alpha(z, n_0, l_i)$: by properties (1) and (5) there are $q \in S_i$ and k such that $\alpha(z, n_0, l_i)^k$ occurs in v^p, $q \mid k$ and $\alpha(z, n_0, l_i)^q \in \mathcal{G}(x)$. But by definition of $\mathcal{G}$, if g_i is bounded then $q = p > |k|$, a contradiction.

Thus

$$\boxed{g_i \text{ is bounded } \;\Rightarrow\; g_i H(x) g_i^{-1} \text{ is not in the range of } H.}$$

So we may assume that g_i is unbounded.

Suppose Case 1 holds: let $g_i^{-1} \cdot \alpha(w_0, n_0, l_i) \cdot g_i = v = v_0 \cdot \alpha(z, n_0, l_i)^r \cdot v_0^{-1}$ and $r = r(w_0, n_0)$, $|r| > 1$. Since $\alpha(w_0, n_0, l_i)^p \in H(y)$ and $v^p =$

$v_0 \cdot \alpha(z, n_0, l_i)^{rp} \cdot v_0^{-1} \in H(x)$ is reduced, we have $v_0, \alpha(z, n_0, l_i)^p \in H(x)$ by properties (5) and (6). Therefore $v_0 \cdot \alpha(z, n_0, l_i)^p \cdot v_0^{-1} \in H(x)$ and computing in $H(y)$, we get

$$
\begin{aligned}
(g_i \cdot v_0 \cdot \alpha(z, n_0, l_i)^p \cdot v_0^{-1} \cdot g_i^{-1})^r &= g_i \cdot v_0 \cdot \alpha(z, n_0, l_i)^{pr} \cdot v_0^{-1} \cdot g_i^{-1} \\
&= g_i \cdot v^p \cdot g_i^{-1} = \alpha(w_0, n_0, l_i)^p,
\end{aligned}
$$

a contradiction, since $\alpha(w_0, n_0, l_i)^p \in \mathcal{G}(y)$ is a generator of $H(y)$ and hence it is not the rth power of any element.

Thus

$$
\boxed{g_i \text{ is unbounded } \& \ |r| > 1 \ \Rightarrow \ g_i H(x) g_i^{-1} \text{ is not in the range of } H.}
$$

Therefore we may assume we are in Case 2, that is, $\forall w \in \mathbf{F}_2 \ \forall n \ (|r(w, n)| = 1)$.

Suppose g_i is good, so that

$$
g_i^{-1} \cdot \alpha(1_{\mathbf{F}_2}, n_m, l_i) \cdot g_i = v_m \cdot \alpha(w_\infty, n_m, l_i)^{r(1_{\mathbf{F}_2}, n_m)} \cdot v_m^{-1}.
$$

Then, by property (6), for $e = 0, 1$,

$$
\begin{aligned}
y(u_m) = e \ &\Leftrightarrow \ \alpha(1_{\mathbf{F}_2}, n_m, l_i)^{pe} \in H(y) \\
&\Leftrightarrow \ v_m \cdot \alpha(w_\infty, n_m, l_i)^{pe \cdot r(1_{\mathbf{F}_2}, n_m)} \cdot v_m^{-1} \in H(x) \\
&\Rightarrow \ \alpha(w_\infty, n_m, l_i)^{pe} \in H(x) \\
&\Leftrightarrow \ w_\infty . x(u_m) = e,
\end{aligned}
$$

that is, $w_\infty . x = y$. Thus

$$
\boxed{g_i \text{ is good } \Rightarrow \ y = w_\infty . x.}
$$

Therefore we may assume g_i is bad, hence $g_i^{-1} \cdot \alpha(1_{\mathbf{F}_2}, n_m, l_i) \cdot g_i = v_m \cdot \alpha(w_m, n_m, l_i)^{r(1_{\mathbf{F}_2}, n_m)} \cdot v_m^{-1}$. Suppose $\mu(w_0 . x) = \infty$. Then by Claim 3.2 in the proof of 3.1, $\forall m \ (w_m . x = w_0 . x)$ hence

$$
\forall m \ (\mu(w_m . x) = \infty \text{ and } H(w_m . x) = H(w_0 . x)).
$$

For $p \in S_i$, using property (6) and the fact that $r(1_{\mathbf{F}_2}, n_m) = \pm 1$ we get

$$
\begin{aligned}
\alpha(1_{\mathbf{F}_2}, n_m, l_i)^p \in H(y) \ &\Leftrightarrow \ v_m \cdot \alpha(w_m, n_m, l_i)^{p \cdot r(1_{\mathbf{F}_2}, n_m)} \cdot v_m^{-1} \in H(x) \\
&\Rightarrow \ \alpha(w_m, n_m, l_i)^p \in H(x) \\
&\Leftrightarrow \ \alpha(1_{\mathbf{F}_2}, n_m, l_i)^p \in H(w_m . x) = H(w_0 . x) \\
&\Rightarrow \ p = p_0 \lor p = p_1.
\end{aligned}
$$

By Claim 4.3, $\mu(y) = \infty$ and hence, for $e = 0, 1$,

$$
\begin{aligned}
y(u_m) = e \;&\Leftrightarrow\; \alpha(1_{\mathbf{F}_2}, n_m, l_i)^{p^e} \in H(y) \\
&\Rightarrow\; \alpha(1_{\mathbf{F}_2}, n_m, l_i)^{p^e} \in H(w_0.x) \\
&\Leftrightarrow\; w_0.x(u_m) = e,
\end{aligned}
$$

that is, $w_0.x = y$. Thus

$$
\boxed{g_i \text{ is bad } \& \; \mu(w_0.x) = \infty \;\Rightarrow\; w_0.x = y.}
$$

Suppose $\mu(w_0.x) = m < \infty$. Then by 3.2,

$$
\forall j < m \; (\mu(w_j.x) = m \; \& \; J_m(w_j.x) = J_m(w_0.x)) \text{ and } \mu(w_m.x) \le m.
$$

Let $e_j \in \{0, \ldots, 5\}$ be the unique value such that

$$
\alpha(w_j, n_j, l_i)^{p^{e_j}} \in \mathcal{G}(x).
$$

Then the first m elements of $(e_j)_j$ are $(2, \ldots, 2, J_m(w_0.x) + 3)$ and by Claim 4.3 the next element must be $J_m(w_0.x) + 3$.

Suppose $\mu(w_m.x) = m$. Since $w_0.x = w_{m-1}.x$ and $z_m.w_0.x = w_m.x$ are distinct, $J_m(w_0.x) \ne J_m(w_m.x)$, a contradiction.

Suppose $\mu(w_m.x) < m$. Then $e_m = 2 \ne J_m(w_0.x) + 3$, a contradiction again.

Thus

$$
\boxed{g_i \text{ is bad } \& \; \mu(w_0.x) < \infty \;\Rightarrow\; g_i H(x) g_i^{-1} \text{ is not in the range of } H.}
$$

This concludes the proof. ∎

References

[1]   R. Dougherty, S. Jackson and A. S. Kechris, *The structure of hyperfinite Borel equivalence relations*, Trans. Amer. Math. Soc. 341 (1994), 193–225.

[2]   R. Dougherty and A. S. Kechris, *How many Turing degrees are there?*, in: Computability Theory and its Applications (Boulder, CO, 1999), Contemp. Math. 257, Amer. Math. Soc., 2000, 83–94.

[3]   S. Gao, *Coding subset shift by subgroup conjugacy*, Bull. London Math. Soc. 32 (2000), 653–657.

[4]   G. Hjorth and A. S. Kechris, *Borel equivalence relations and classifications of countable models*, Ann. Pure Appl. Logic 82 (1996), 221–272.

[5]   A. S. Kechris, *Classical Descriptive Set Theory*, Grad. Texts in Math. 156, Springer, 1995.

[6]   A. S. Kechris and Y. N. Moschovakis (eds.), *Cabal Seminar 76–77*, Lecture Notes in Math. 689, Springer, 1978.

[7]   A. S. Kechris, S. Solecki and S. Todorčević, *Borel chromatic numbers*, Adv. Math. 141 (1999), 1–44.

[8]   G. Stuck and R. J. Zimmer, *Stabilizers for ergodic actions of higher rank semisimple groups*, Ann. of Math. 139 (1994), 723–747.

[9]   S. Thomas and B. Veličković, *On the complexity of the isomorphism relation for finitely generated groups*, J. Algebra 217 (1999), 352–373.

[10]   S. Wagon, *The Banach–Tarski Paradox*, Encyclopedia Math. Appl. 24, Cambridge Univ. Press, 1985.

Dipartimento di Matematica   Department of Mathematics
Università di Torino   University of California at Los Angeles
via Carlo Alberto 10   Los Angeles, CA 900095-1555, U.S.A.
10123 Torino, Italy   E-mail: greg@math.ucla.edu
E-mail: andretta@dm.unito.it
        camerlo@dm.unito.it