THE CONJUGACY PROBLEM AND RELATED PROBLEMS IN LATTICE-ORDERED GROUPS

W. CHARLES HOLLAND AND BOAZ TSABAN

Abstract. We study, from a constructive computational point of view, the techniques used to solve the conjugacy problem in the "generic" lattice-ordered group $\mathrm{Aut}(\mathbb{R})$. We use these techniques in order to show that for all $f, g \in \mathrm{Aut}(\mathbb{R})$, the equation $xfx = g$ is effectively solvable in $\mathrm{Aut}(\mathbb{R})$.

1. Introduction

The conjugacy problem. Elements g_1 and g_2 in a group G are *conjugate* if there exists $h \in G$ such that $g_1 = h^{-1}g_2h$. The *conjugacy problem* for a given group G is the question whether there exists an effective procedure to determine whether g_1 and g_2 are conjugate, given arbitrary $g_1, g_2 \in G$.

This problem is of significant theoretical interest, but recently it became extremely important from a practical point of view. In [2] and [8], a family of cryptosystems was suggested, whose strength heavily depends on the intractability of variants of the conjugacy problem in the underlying group. It seemed that for $G = B_n$, the *Braid group* with n strands, the goal of achieving a secure cryptosystem was reached, but recent results [3, 5] suggest that B_n is not a good candidate and the search for a better group has revived.

Lattice-ordered groups. A *partially ordered group* is a group G endowed with a partial ordering $\leq$ which is respected by the group operations, that is, for each $g_1, g_2 \in G$ such that $g_1 \leq g_2$, $xg_1 \leq xg_2$ and $g_1x \leq g_2x$ for all $x \in G$. If the underlying partial order $\leq$ on G is a lattice (that is, for each $g_1, g_2 \in G$ there exists a least upper bound $g_1 \vee g_2 \in G$ and a greatest lower bound $g_1 \wedge g_2 \in G$), then we say that G is a *lattice-ordered group*.

If G is a lattice-ordered group, then the lattice operations distribute over each other, and the group operation distributes over the lattice

1991 *Mathematics Subject Classification.* 06F15, 20F10 .

Key words and phrases. conjugacy problem, lattice-ordered groups, parametric equations.

operations, too. Consequently, any element in a lattice-ordered group generated by $\{x_1, \ldots, x_n\}$ can be written in the form

$$w(x_1, \ldots, x_n) = \bigwedge_i \bigvee_j u_{ij}(x_1, \ldots, x_n)$$

where each expression $u_{ij}(x_1, \ldots, x_n)$ is an element of the free group on $\{x_1, \ldots, x_n\}$. The form above for $w(x_1, \ldots, x_n)$ is not unique. In [7], an algorithm was given to determine whether two given expressions of this form represent the same element of the *free lattice-ordered group* $\mathbb{F}_n$ (and, therefore, the same element in *every* lattice-ordered group G).

Let $\mathrm{Aut}(\mathbb{R})$ denote the collection of all order preserving bijections $f : \mathbb{R} \to \mathbb{R}$, that is, order automorphisms of $\mathbb{R}$. Observe that each $f \in \mathrm{Aut}(\mathbb{R})$ is continuous. $\mathrm{Aut}(\mathbb{R})$, with the operation of composition, is a group which is lattice-ordered by:

$$f \le g \quad \text{if} \qquad f(x) \le g(x) \text{ for all } x \in \mathbb{R}.$$

The lattice operations are defined by

$$\begin{aligned}(f \vee g)(x) &= \max\{f(x), g(x)\}\\ (f \wedge g)(x) &= \min\{f(x), g(x)\}\end{aligned}$$

for each $x \in \mathbb{R}$. In 1963, Holland proved that every lattice-ordered group can be embedded in the lattice-ordered group $\mathrm{Aut}(\Omega, \le)$ of automorphisms of a totally ordered set $(\Omega, \le)$. This is discussed in detail in section 7.1 of [4]. A particular case of this theorem is, that the free lattice-ordered group $\mathbb{F}_n$ can be embedded in $\mathrm{Aut}(\mathbb{R})$. Consequently, $\mathrm{Aut}(\mathbb{R})$ satisfies a given equation $w(x_1, \ldots, x_n) = u(x_1, \ldots, x_n)$ if, and only if, every lattice-ordered group satisfies this equation.

Parametric equations. Because of the generic nature of the lattice-ordered group $\mathrm{Aut}(\mathbb{R})$, it would be interesting to know which elements of this group are conjugate. A simple conjugacy criterion was given in [6]. In Section 2 we analyze this treatment of the *conjugacy problem in* $\mathrm{Aut}(\mathbb{R})$ from a computational point of view, and show that in fact, there exists an effective definition of the conjugator when the given elements are conjugate. The conjugacy problem in $\mathrm{Aut}(\mathbb{R})$ is a specific case of an *equation with parameters* from $\mathrm{Aut}(\mathbb{R})$. Thus, a natural extension of the conjugacy problem in this group is, which equations with parameters in $\mathrm{Aut}(\mathbb{R})$ have solutions in $\mathrm{Aut}(\mathbb{R})$. We solve several problems of this type in Section 3. In particular, we show that every element of $\mathrm{Aut}(\mathbb{R})$ is a commutator (that is, for each $g \in \mathrm{Aut}(\mathbb{R})$ there exist $x, y \in \mathrm{Aut}(\mathbb{R})$ such that $x^{-1}y^{-1}xy = g$), and that the equation $xfx = g$ is effectively solvable in $\mathrm{Aut}(\mathbb{R})$.

Effectiveness. When dealing with parametric equations in $\mathrm{Aut}(\mathbb{R})$, we use the following natural model of computation: The parameters appearing in the equation are treated as "black box" functions, that is, the allowed operations in our model are evaluation of any of the parameters at any desired point in $\mathbb{R}$, as well as the basic arithmetic operations (addition, subtraction, multiplication and division), and any (finite) composition of these.

Moreover, we consider the basic arithmetic operations as computationally negligible. Thus, in this model, a solution to a given parametric equation (that is, well defined elements of $\mathrm{Aut}(\mathbb{R})$ which satisfy the equation when substituted for the variables) is *effective* if its evaluation at each given point requires only finitely many evaluations of the functions appearing as parameters in the equations.

Notational convention. For the rest of this paper, we use the convention that the functions are evaluated from left to right, that is, the value of g at α is αg and the value of gf at α is $\alpha gf = (\alpha g)f$.

2. The conjugacy problem

For $g \in \mathrm{Aut}(\mathbb{R})$, let

$$\begin{aligned}\mathrm{Supp}(g) &= \{\alpha \in \mathbb{R} \ : \ \alpha \neq \alpha g\}\\ \mathrm{Supp}^+(g) &= \{\alpha \in \mathbb{R} \ : \ \alpha < \alpha g\}\\ \mathrm{Supp}^-(g) &= \{\alpha \in \mathbb{R} \ : \ \alpha g < \alpha\}\end{aligned}$$

Then $\mathrm{Supp}^+(g)$ and $\mathrm{Supp}^-(g)$ are disjoint open subsets of $\mathbb{R}$, and $\mathrm{Supp}(g) = \mathrm{Supp}^+(g) \cup \mathrm{Supp}^-(g)$. Consequently, $\mathrm{Supp}(g)$ is a disjoint union of open intervals (the *components* of $\mathrm{Supp}(g)$), where each interval is a component of either $\mathrm{Supp}^+(g)$ (a *positive component*) or of $\mathrm{Supp}^-(g)$ (a *negative component*).

We now describe a useful method to obtain a partition of a component of $\mathrm{Supp}(g)$ into a sequence of half-open intervals. Suppose I is a positive component of $\mathrm{Supp}(g)$ and $\alpha \in I$. Then $\alpha < \alpha g$. As g is order preserving, we have that for all $i \in \mathbb{Z}$, $\alpha g^i < \alpha g^{i+1}$. Let I' be the *convex hull* of $\{\alpha g^i \ : \ i \in \mathbb{Z}\}$, that is,

$$I' = \bigcup_{i\in\mathbb{Z}} [\alpha g^i, \alpha g^{i+1}).$$

Then $I' \subseteq I$. Moreover, $I'g = I'$. If I' has an upper bound, then it has a least upper bound γ, and $\lim_{n\to\infty} \alpha g^n = \gamma$. As g is continuous, $\gamma g = \gamma$, and so $\gamma \notin I$. A similar result holds if I' has a lower bound.

Therefore, $I' = I$. Similarly, for each negative component I of $\mathrm{Supp}(g)$ and each $\alpha \in I$,

$$I = \bigcup_{i \in \mathbb{Z}} [\alpha g^{i+1}, \alpha g^i).$$

The following lemma is an extension of the corresponding lemma from [6]. Recall that if α lies in a positive component of a function g, then $\alpha < \alpha g$, and the function ψ in the following lemma is well defined.

Lemma 2.1. *Let $f, g \in \mathrm{Aut}(\mathbb{R})$, let I be a positive component of $\mathrm{Supp}(f)$ and J be a positive component of $\mathrm{Supp}(g)$. Fix elements $\alpha \in I$ and $\beta \in J$. Define the usual affine order preserving bijection $\psi : [\alpha, \alpha g) \to [\beta, \beta f)$ by*

$$\gamma\psi = \frac{\beta f - \beta}{\alpha g - \alpha}(\gamma - \alpha) + \beta.$$

The following procedure defines an order preserving bijection $x : I \to J$ such that on J, $f = x^{-1}gx$, by defining its evaluation on a given $\gamma \in I$:

1. *If $\gamma > \alpha$, compute $\alpha g, \alpha g^2, \dots$ until the first positive integer i such that $\alpha g^i \leq \gamma < \alpha g^{i+1}$ is found.*
2. *If $\gamma < \alpha$, compute $\alpha g^{-1}, \alpha g^{-2}, \dots$ until the first negative integer i such that $\alpha g^i \leq \gamma < \alpha g^{i+1}$ is found.*
3. *Compute $\gamma x := \gamma g^{-i}\psi f^i$ by making i evaluations of g^{-1}, one evaluation of ψ, and i evaluations of f.*

A similar result holds in the case that I and J are negative components.

Proof. Let $\alpha \in I$, $\beta \in J$. We may assume $\alpha < \alpha g$ and $\beta < \beta f$.

$$I = \bigcup_{i \in \mathbb{Z}} [\alpha g^i, \alpha g^{i+1})$$

and

$$J = \bigcup_{i \in \mathbb{Z}} [\beta f^i, \beta f^{i+1}).$$

Let $\psi : [\alpha, \alpha g] \to [\beta, \beta g]$ be the order preserving bijection defined above. For each $i \in \mathbb{Z}$ define an order preserving bijection $x_i : [\alpha g^i, \alpha g^{i+1}) \to [\beta f^i, \beta f^{i+1})$ by

$$x_i = g^{-i}\psi f^i,$$

and take $x = \bigcup_{i \in \mathbb{Z}} x_i$. Then $x : I \to J$ is an order preserving bijection, and if $\beta f^i \leq \delta < \beta f^{i+1}$, then $\alpha g^i \leq \delta x^{-1} < \alpha g^{i+1}$. Therefore,

$$\begin{aligned} \delta x^{-1} g x &= \delta x^{-1} g g^{-(i+1)} \psi f^{i+1} = \\ &= \delta x^{-1} g^{-i} \psi f^{i+1} = \delta x^{-1} x f = \delta f. \end{aligned}$$

□

The following is obvious.

Lemma 2.2. *Let I and J be nontrivial maximal intervals of fixed points of f and g, respectively.*

(1) *If $I = [\alpha_1, \alpha_2]$ and $J = [\beta_1, \beta_2]$, define*
$$\psi : [\alpha_1, \alpha_2] \to [\beta_1, \beta_2]$$
as in Lemma 2.1;

(2) *If $I = (-\infty, \alpha_2]$ and $J = (-\infty, \beta_2]$, define*
$$\psi : (-\infty, \alpha_2] \to (-\infty, \beta_2]$$
by $\gamma\psi = \gamma - \alpha_2 + \beta_2$;

(3) *If $I = [\alpha_1, \infty)$ and $J = [\beta_1, \infty)$, define*
$$\psi : [\alpha_1, \infty) \to [\beta_1, \infty)$$
by $\gamma\psi = \gamma - \alpha_1 + \beta_1$;

(4) *If $I = \mathbb{R} = J$, define*
$$\psi : \mathbb{R} \to \mathbb{R}$$
by $\gamma\psi = \gamma$.

Let $x = \psi$. Then $x : I \to J$ is an order preserving bijection such that on J, $f = x^{-1}gx$.

The computational complexity in Lemmas 2.1 and 2.2 is unbounded, but the procedure requires only finitely many steps. For each given γ, the computational complexity of the evaluation of γx can be reduced from i (as defined there) to the order of $\log_2 i$ if we work in the *fast forward model*, where the computational complexity of evaluating g^i and f^i is independent of i (this model was studied in another context in [9, 10]). In this model, step 3 of the procedure requires a negligible amount of time, and step 1 can be accelerated by first finding the first n such that $\alpha g^{2^n} < \gamma < \alpha g^{2^{n+1}}$ and continuing this binary search in the interval $[\alpha g^{2^n}, \alpha g^{2^{n+1}})$ in a nested manner.

Definition 2.3. For an element $g \in \mathrm{Aut}(\mathbb{R})$, let $F(g)$ be the set of nontrivial maximal intervals of fixed points of g, let $P(g)$ be the set of positive components of $\mathrm{Supp}(g)$, and let $N(g)$ be the set of negative components of $\mathrm{Supp}(g)$. The set $T(g) = P(g) \cup N(g) \cup F(g)$ inherits a total order from $\mathbb{R}$. We call $T(g)$ the *terrain* of g.

Following is a simple characterization of terrains.

Lemma 2.4. *Assume that $g \in \mathrm{Aut}(\mathbb{R})$. Give the elements of $F(g)$ the color 0, the elements of $P(g)$ the color $+$, and the elements of $N(g)$ the* *color* $-$. *Then the terrain* $T(g)$ *is a countable* $\{0,+,-\}$*-colored totally ordered set such that no two adjacent points are both colored* 0.

Conversely, any countable $\{0,+,-\}$*-colored totally ordered set such that no two adjacent points are both colored* 0 *is the terrain of some element* $g \in \mathrm{Aut}(\mathbb{R})$.

Proof. $T(g)$ is countable because the component intervals and the maximal nontrivial fixed point intervals are all disjoint, and each contains a rational number. No two adjacent intervals are both fixed point intervals, as this would contradict the maximality.

Conversely, if T is a countable $\{0,+,-\}$-colored ordered set, let $\mathbb{Q}$ be the set of rational numbers with the usual order and let $S = T \times \mathbb{Q}$ be the lexicographically ordered product. Then S is a countable ordered set without end points, and so S is isomorphic $\mathbb{Q}$, and hence the Dedekind completion of S is isomorphic to the real line $\mathbb{R}$. Under the isomorphism, for each $t \in T$, the Dedekind completion of the interval $\{t\} \times \mathbb{Q}$ is isomorphic to an interval of the form $\{t\} \times \mathbb{R}$, and we can define $g \in \mathrm{Aut}(\mathbb{R})$ so that if t has color $+$, then $(t,x)g = (t,x+1)$, and if t has color $-$, then $(t,x)g = (t,x-1)$, and g fixes all other points of the Dedekind completion of S. Then the terrain of g is isomorphic to T. $\square$

Definition 2.5. An *isomorphism* of terrains T_1 and T_2 is a color- and order-preserving bijection from T_1 to T_2. If there exists such an isomorphism then we say that T_1 and T_2 are isomorphic.

Theorem 2.6. *Two elements* $g, f \in \mathrm{Aut}(\mathbb{R})$ *are conjugate if, and only if,* $T(f)$ *is isomorphic to* $T(g)$. *Moreover, if an isomorphism of* $T(f)$ *and* $T(g)$ *is given (as a "black-box" function), then there exists an effective procedure defining an element* $h \in \mathrm{Aut}(\mathbb{R})$ *such that* $f = h^{-1}gh$.

Proof. It is clear that if $C \in T(f)$ is a component of f, and $h \in \mathrm{Aut}(\mathbb{R})$, then $Ch \in T(h^{-1}fh)$ is a component of $h^{-1}fh$ of the same "color". Hence, conjugation by h induces an isomorphism of the terrains $T(f) \cong T(h^{-1}fh)$. Conversely, if we are given an isomorphism $\tau : T(f) \cong T(g)$ of terrains, then for every component $I = C \in T(f)$, and $J = C\tau \in T(g)$, we have that I and J satisfy the conditions of Lemmas 2.1 or 2.2. Since the union of all of the components of any element of $\mathrm{Aut}(\mathbb{R})$ is a dense subset of $\mathbb{R}$, if x is defined on each of the intervals as in Lemmas 2.1 and 2.2, there is a unique extension to an element $h \in \mathrm{Aut}(\mathbb{R})$, and the theorem is proved. $\square$

Of course, $T(f)$ may typically be infinite, but for a large class of elements, it is finite. For example, there are exactly three (isomorphism classes of) one-element terrains, and thus three conjugacy classes of the corresponding members of Aut($\mathbb{R}$). There are exactly 8 two-element terrains, and so 8 conjugacy classes of corresponding elements of Aut(R). And there are exactly 22 three-element terrains, etc.

3. Other parametric equations

The conjugacy problem in Section 2 can be expressed in the following way: Given parameters g_1, g_2, does there exist a $g_3 \in \mathrm{Aut}(\mathbb{R})$ such that $g_1^{-1} g_3^{-1} g_2 g_3 = e$? The general problem is this: given a lattice-ordered group G and an element

$$w(x_1, \ldots, x_n) = \bigwedge_i \bigvee_j u_{ij}(x_1, \ldots, x_n)$$

of the free lattice-ordered group on $\{x_1, \ldots, x_k, \ldots, x_n\}$, $1 \leq k \leq n$, and elements $g_1, \ldots, g_{k-1} \in G$, do there exist elements $g_k, \ldots, g_n \in G$ such that $w(g_1, \ldots, g_{k-1}, g_k, \ldots, g_n) = e$?

Another special case of this is when there is only one parameter, and it occurs only once. This was solved (modulo the effectiveness assertion) in the following theorem and corollaries in [1].

Theorem 3.1. *Let $w(x_2, ..., x_n)$ be a group word (not involving the lattice operations, and let $g \in \mathrm{Aut}(\mathbb{R})$. Then there exists an effective proceedure defining $g_2, ..., g_n \in \mathrm{Aut}(\mathbb{R})$ such that $g = w(g_2, ..., g_n)$.*

Proof. We define the functions g_i $(i = 2, \ldots, n)$ on each component I of Supp(g), and then patch the results together. Let I be a component of Supp(g), say, a positive component. Choose any $\alpha \in I$. Then, as shown in the previous section, $\alpha < \alpha g$ and $\{\alpha g^i\}$ is unbounded above and below in I.

We may write the equation $w(x_2, \ldots, x_n) = g$ in the form

$$w(x_2, \ldots, x_n) = x_{\sigma(1)}^{\epsilon(1)} x_{\sigma(2)}^{\epsilon(2)} \cdots x_{\sigma(m)}^{\epsilon(m)} = g,$$

where $\sigma : \{1, \ldots, m\} \to \{2, \ldots, n\}$, and $\epsilon(i) = \pm 1$, and we may assume that the left-hand side is in reduced form, that is, $x_{\sigma(i+1)}^{\epsilon(i+1)} \neq x_{\sigma(i)}^{-\epsilon(i)}$.

Let $\cdots < \beta_i < \beta_{i+1} < \cdots$ be any sequence of points of I which has no upper or lower bound in I. In each interval $[\beta_i, \beta_{i+1})$, choose points $\beta_i = \gamma_{i,0} < \gamma_{i,1} < \cdots < \gamma_{i,m} = \beta_{i+1}$.

For each $\sigma(j)$ with $0 < j \leq m$ we can define an order preserving bijection $g_{\sigma(j)} \in \mathrm{Aut}(\mathbb{R})$ such that for each $i \in \mathbb{Z}$ and each j, $\gamma_{i,j-1} g_{\sigma(j)}^{\epsilon(j)} = \gamma_{i,j}$, and $\gamma_{\sigma(j)}$ is affine on each of the intervals $[\gamma_{i,k-1}, \gamma_{i,k}]$.

We have that $\beta_i w(g_2, \ldots, g_n) = \beta_{i+1}$ for each i. We do not necessarily have that $w(g_2, \ldots, g_n) = g$, but we do have that I is a positive component of $w(g_2, \dots, g_n)$. Therefore, by Theorem 2.6, there is (an effectively computable) $y \in \mathrm{Aut}(\mathbb{R})$ such that on I

$$w(y^{-1}g_2y, \dots, y^{-1}g_ny) = y^{-1}w(g_2, \dots, g_n)y = g.$$

We do this on each component, letting all x's be e on each fixed point of g, and patch the results together, and the theorem is proved. $\square$

Corollary 3.2. *Every element $g \in \mathrm{Aut}(\mathbb{R})$ is a commutator.*

Proof. Take $g = x^{-1}y^{-1}xy$. $\square$

Corollary 3.3. *Every element $g \in \mathrm{Aut}(\mathbb{R})$ has an nth root for each positive integer n.*

Proof. Take $g = x^n$. $\square$

Let us now consider the case of two parameters, but only one variable. Two special cases of this are considered in the next theorem.

Theorem 3.4. *Let $\epsilon(i) = \pm 1$, and consider the equation $x^{\epsilon(1)}gx^{\epsilon(2)}f^{-1} = e$ in $\mathrm{Aut}(\mathbb{R})$. Then:*

1. *If $\epsilon(1) = -\epsilon(2)$, then the equation has a solution if and only if $T(f) \cong T(g)$.*
2. *If $\epsilon(1) = \epsilon(2)$, then the equation has a solution for all f, g.*

Moreover, when these equations have solutions, they have effectively defined solutions.

Proof. (1) This is Theorem 2.6.

(2) We write the equation in the form $xgx = f$. Since $f^{-1}(fg)f = gf$, by Theorem 2.6, $T(fg) \cong T(gf)$. In particular, if I is a component of $\mathrm{Supp}(fg)$, then If is the corresponding component of $\mathrm{Supp}(gf)$. Suppose, for example that fg is positive on I. Then gf is positive on If. Choose $\alpha \in I$. Then

$$\cdots < \alpha < \alpha fg < \alpha(fg)^2 < \cdots$$

is unbounded in I. It follows that

$$\cdots < \alpha f(gf)^{-1} = \alpha g^{-1} < \alpha f < \alpha f(gf) < \cdots$$

is unbounded in If. Choose $\beta \in If$ so that $\alpha g^{-1} < \beta < \alpha f$. Then

$$\cdots < \alpha < \beta g < \alpha(fg) < \beta g(fg) < \alpha(fg)^2 < \beta g(fg)^2 < \cdots$$

and

$$\cdots < \beta < \alpha f < \beta(gf) < \alpha f(gf) < \beta(gf)^2 < \alpha f(gf)^2 < \cdots,$$

and each of these sequences is unbounded in the corresponding component.

Let $\psi : [\alpha, \beta g) \to [\beta, \alpha f)$ be any order preserving bijection between the real intervals, for example the affine one. We now define an order preserving bijection $x : I \to If$ by extending ψ in the following way. For $\gamma \in I$:

$$\gamma x = \begin{cases} \gamma(fg)^{-i}\psi(gf)^i, & \text{if } \alpha(fg)^i \le \gamma < \beta g(fg)^i \\ \gamma(fg)^{-i}g^{-1}\psi^{-1}f(gf)^i, & \text{if } \beta g(fg)^i \le \gamma < \alpha(fg)^{i+1}. \end{cases}$$

Then x is, indeed, an order preserving bijection of I onto If. And on I, $xgx = f$ because: if $\alpha(fg)^i \le \gamma < \beta g(fg)^i$ then $\gamma x = \gamma(fg)^{-i}\psi(gf)^i$, and so

$$\beta(gf)^i = \alpha(fg)^i(fg)^{-i}\psi(gf)^i \le \gamma x < \beta g(fg)^i(fg)^{-i}\psi(gf)^i = \alpha f(gf)^i$$

and so

$$\beta g(fg)^i = \beta(gf)^i g \le \gamma xg < \alpha f(gf)^i g = \alpha(fg)^{i+1}$$

which implies

$$\begin{aligned} \gamma xgx &= (\gamma x)g(fg)^{-i}g^{-1}\psi^{-1}f(gf)^i \\ &= (\gamma(fg)^{-i}\psi(gf)^i)g(fg)^{-i}g^{-1}\psi^{-1}f(gf)^i \\ &= \gamma(fg)^{-i}(fg)^i f \\ &= \gamma f; \end{aligned}$$

and in the other case, $\beta g(fg)^i \le \gamma < \alpha(fg)^{i+1}$, so $\gamma x = \gamma(fg)^{-i}g^{-1}\psi^{-1}f(gf)^i$, whence

$$\begin{aligned} \alpha f(gf)^i &= \beta g(fg)^i(fg)^{-i}g^{-1}\psi^{-1}f(gf)^i \\ &\le \gamma x \\ &< \alpha(fg)^{i+1}(fg)^{-i}g^{-1}\psi^{-1}f(gf)^i \\ &= \beta(gf)^{i+1}, \end{aligned}$$

from which follows $\alpha(fg)^{i+1} \le \gamma xg < \beta g(fg)^{i+1}$, and hence

$$\begin{aligned} \gamma xgx &= (\gamma x)g(fg)^{-(i+1)}\psi(gf)^{i+1} \\ &= (\gamma(fg)^{-i}g^{-1}\psi^{-1}f(gf)^i)g(fg)^{-(i+1)}\psi(gf)^{i+1} \\ &= \gamma(fg)^{-i}g^{-1}(gf)^{i+1} \\ &= \gamma f. \end{aligned}$$

Repeating this process on each of the components of $\mathrm{Supp}(fg)$ (and defining $x = f$ on the fixed points of fg), produces an $x \in \mathrm{Aut}(\mathbb{R})$ such that $xgx = f$. $\square$

References

[1] Samson Adeleke and W. C. Holland, *Representation of order automorphisms by words*, Forum Mathematicum **6** (1994), 315–321.

[2] I. Anshel, M. Anshel, and D. Goldfeld, *An algebraic method for Public-Key Cryptography*, Mathematical Research Letters **6** (1999), 287–291.

[3] D. Garber, S. Kaplan, M. Teicher, B. Tsaban, and U. Vishne, Length-based conjugacy search in the Braid group, preprint available at `http://arxiv.org/abs/math.GR/0209267`

[4] A. M. W. Glass, *Partially Ordered Groups*, World Scientific, 1999.

[5] D. Hofheinz and R. Steinwandt, *A practical attack on some Braid group based cryptographic primitives*, International Workshop on Practice and Theory in Public Key Cryptography, PKC 2003 Proceedings, LNCS **2567** (2002), 187–198.

[6] W. C. Holland, *The lattice-ordered group of automorphisms of an ordered set*, Michigan Math. J. **10** (1963), 399–408.

[7] W. C. Holland and S. H. McCleary, *The word problem for free lattice-ordered groups*, Houston J. Math. **5** (1979), 99–105.

[8] K. H. Ko, S. J. Lee, J. H. Cheon, J. W. Han, J. Kang, and C. Park, *New Public-Key Cryptosystem using Braid groups*, Advances in Cryptology – Crypto 2000 Proceedings, LNCS **1880**, 166–183.

[9] M. Naor and O. Reingold, *Constructing Pseudo-Random Permutations with a Prescribed Structure*, Journal of Cryptology **15** (2002), 97–102.

[10] B. Tsaban, *Permutation graphs, fast forward permutations, and sampling the cycle structure of a permutation*, Journal of Algorithms **47** (2003), 104–121.

Department of Mathematics, Bowling Green State University, Bowling Green, Ohio, USA

E-mail address: `chollan@bgnet.bgsu.edu`

Department of Applied Mathematics and Computer Science, The Weizmann Institute of Science, Rehovot 76100, Israel

E-mail address: `boaz.tsaban@weizmann.ac.il`

URL: `http://www.cs.biu.ac.il/~tsaban`