Garside groups have the falsification by fellow-traveller property

Derek F. Holt

Abstract. A group *G* is said to have the *falsification by fellow-traveller property* (FFTP) with respect to a specified finite generating set *X* if, for some constant *K*, all non-geodesic words over $X \cup X^{-1}$ *K*-fellow-travel with *G*-equivalent shorter words. This implies, in particular, that the set of all geodesic words over $X \cup X^{-1}$ is regular. We show that Garside groups with appropriate generating set satisfy FFTP.

Mathematics Subject Classification (2010). 20F36, 20F10, 20F65.

Keywords. Garside groups, braid groups, Artin groups, geodesics, regular sets, fellow-traveller property.

1. Introduction

Throughout this article we let G be a group generated by a finite set X and set $A := X \cup X^{-1}$. So elements of G are represented by words $w \in A^*$. We denote the length of the word w and the length of a shortest word w' with $w' =_G w$ by |w| and $|w|_G$, respectively. Then w is *geodesic* if $|w| = |w|_G$.

For a non-negative integer *i* and $w \in A^*$, w(i) will denote the prefix of *w* of length *i* if $i \leq |w|$, or *w* if i > |w|. For $K \geq 0$, we say that words *w* and *v* (synchronously) *K*-fellow-travel if $|w(i)^{-1}v(i)|_G \leq K$ for all $i \geq 0$.

Definition 1.1. The group *G* has the *falsification by fellow traveller property* (FFTP) with respect to *X* or *A* if there is a constant $K \ge 0$ such that, for any non-geodesic word $v \in A^*$, there exists a word $w \in A^*$ with $v =_G w$ and |w| < |v| such that v and w *K*-fellow travel.

This property was introduced by Neumann and Shapiro in [6]. They prove in Proposition 4.1 of that paper that, when this property holds, the set $\mathscr{G}(G, A)$ of geodesic words is a regular set, and they use it to prove that virtually abelian groups and geometrically finite hyperbolic groups have regular sets of geodesics with respect to suitable generating sets.

In fact the definition given in [6] stipulates the apparently weaker condition that v and w asynchronously K-fellow travel, but it is straightforward to prove (exercise,

or see [4], Lemma 1) that the two definitions are equivalent. It is also proved in [4] that groups with FFTP are almost convex, satisfy a quadratic isoperimetric function, and have the property F_3 . Furthermore, their word problem is solvable in quadratic time.

It is not true that the regularity of $\mathscr{G}(G, A)$ implies that *G* has FFTP with respect to *X*. This is demonstrated by an example presented in [5], namely the wreath product of an infinite cyclic group with a group of order 2 defined by the presentation $\langle t, a \mid t^2, [a, tat] \rangle$, with $X = \{a, t\}$. Note, however, that this group does have FFTP with respect to $X = \{a, b, t\}$, where b = tat.

It is proved in [2] that *Garside groups*, which include the braid groups, have regular geodesics with respect to suitable X, and the purpose of this note is to show that they also satisfy FFTP with respect to the same X. Our proof is self-contained, but many of our arguments are adaptations of those in [2]. See also [3] for a general treatment of Garside groups, including the proof of their biautomaticity.

2. Garside groups

The definition of a Garside group depends on the concept of an *atomic monoid*. An element *m* of a monoid *M* is called *indivisible* if $m \neq 1$ and m = ab implies a = 1 or b = 1. Then *M* is called *atomic* if it is generated by its indivisible elements and, for each $m \in M$, the supremum of the lengths of words $a_1a_2...a_r$ equal to *m* in *M* and with each a_i indivisible is finite. We can define a partial order with respect to left divisibility on any atomic monoid by $a \leq b$ if ac = b for some $c \in M$. The finiteness of the supremum of lengths of words for elements in *M* implies that we cannot have a = acd for $a, c, d \in M$ unless c = d = 1. Hence $a \leq b$ and $b \leq a$ if and only if a = b. We can do the same for right divisibility, but we shall assume throughout that the partial order \leq on atomic monoids represents left divisibility.

A *Garside group* G is defined to be a group having a submonoid G^+ which is atomic, and which has the following additional properties:

- (1) Any two elements of G^+ have a least common multiple and a greatest common divisor on both the left and the right;
- (2) there exists an element Δ of G^+ with the property that the sets of left and right divisors of Δ are the same, and they form a finite generating set for G^+ as a monoid and G as a group.

Let G be a Garside group, let \tilde{X} be the set of left and right divisors of the specified element Δ , and set $X = \tilde{X} \setminus \{1\}$. We shall prove that G has FFTP with respect to the generating set $A := X \cup X^{-1}$. In the course of the proof we shall need to consider words over $\tilde{A} := A \cup \{1\}$. Since no word in \tilde{A}^* that contains 1 can be a geodesic, we have $\mathscr{G}(G, \tilde{A}) = \mathscr{G}(G, A)$.

The Garside groups include the braid groups and, more generally, the Artin groups of finite type. The simplest example is the braid group on three strings generated by *a*

and b, for which $\Delta = aba = bab$ and $X = \{a, b, ab, ba, aba\}$. Notice that the set X of divisors of Δ is generally much larger than the natural minimal generating set of the group. For the braid group B_n on n strings generated by n - 1 simple crossings, we have |X| = n! - 1. The n - 1 simple crossings are of course the atomic elements.

For $g, h \in G^+$, we write $g \wedge h$ for the greatest common left divisor of g and h. Then we have:

Lemma 2.1. For $g \in X$ and $h \in G^+$, $\Delta \wedge (gh) = \Delta \wedge (g(\Delta \wedge h))$.

Proof. Clearly any common divisor of Δ and $g(\Delta \wedge h)$ is a common divisor of Δ and gh. Conversely, let $\Delta \wedge (gh) = k$, so gh = kl for some $l \in G^+$. Since $g \in X$, $g \leq \Delta$ and hence $g \leq \Delta \wedge (gh) = k$, so k = gm for some $m \in G^+$. Hence gh = gml and, by the cancellation law, h = ml. Now m is a right divisor of k which is itself a left and hence right divisor of Δ , so $m \in \tilde{X}$, and hence $m \leq \Delta \wedge h$. So $k = gm \leq g(\Delta \wedge h)$, which completes the proof.

(By expressing an arbitrary $g \in G^+$ as a word in X^* , we can use a straightforward induction argument on the length of the word to prove that the above result holds for all $g \in G^+$, but we shall not need that result.)

Let $g \in G^+$ be represented by the word $w = \mu_1 \mu_2 \dots \mu_n \in X^*$. Then we define $\eta_i \in X$ for $1 \le i \le n$ by $\eta_n = \mu_n$ and $\eta_i = \Delta \land (\mu_i \eta_{i+1})$ for $1 \le i < n$. By repeated application of Lemma 2.1, we see that $\eta_i = \Delta \land (\mu_i \dots \mu_n)$ for $1 \le i \le n$.

Now for each i < n we have $\mu_i \eta_{i+1} = \eta_i \nu_{i+1}$ for some $\nu_{i+1} \in G^+$. But since $\mu_i \leq \Delta$ and $\eta_i = \Delta \land (\mu_i \eta_{i+1})$, we have $\mu_i \leq \eta_i$ so ν_{i+1} is a right divisor of η_{i+1} , which implies that $\nu_{i+1} \in \tilde{X}$.

We have now derived an alternative word $\eta_1 \nu_2 \dots \nu_n \in \widetilde{X}^*$ that represents g, and we shall refer to this process as *rewriting* the word w.

Lemma 2.2. If $g \in G^+$ is represented by $w \in X^*$ and $\Delta \leq g$, then $g =_G \Delta v$ for some $v \in X^*$ with |v| < |w|.

Proof. Let $w = \mu_1 \mu_2 \dots \mu_n \in X^*$. In the notation just introduced, we have $g = \eta_1 \nu_2 \dots \nu_n$ with $\eta_1 = \Delta \wedge w = \Delta \wedge g$. But $\Delta \leq g$ implies that $\Delta \wedge g = \Delta$, so $\eta_1 = \Delta$ and the result follows.

(By repeating the rewriting process starting with the element $\nu_2 \dots \nu_n$, we can find a word $\eta'_1 \eta'_2 \dots \eta'_k$ for g with $k \leq n$, where each $\eta'_i = \Delta \wedge (\eta'_i \dots \eta'_k)$. This is the known as the *left greedy normal form* for g, and plays an important role in the automatic structure for G, but we shall not pursue that further here.)

For $\mu \in \tilde{X}$, we have $\Delta =_G \mu \mu^*$ where, since \tilde{X} is the set of right divisors of Δ , $\mu^* \in \tilde{X}$. Similarly, there exists $*\mu \in \tilde{X}$ with $\Delta =_G *\mu\mu$.

It follows from the cancellation laws in G that the maps $\mu \mapsto \mu^*$ and $\mu \mapsto *\mu$ are permutations of \tilde{X} . Note also that $\Delta \mu^* =_G *\mu \mu \mu^* =_G *\mu \Delta$, so there is a permutation σ of \tilde{X} (which restricts to a permutation of X) for which $\Delta \mu =_G \sigma(\mu)\Delta$

D.F. Holt

for all $\mu \in \widetilde{X}$, and $*\mu =_G \sigma(\mu^*)$. We have $\Delta^r \in Z(G^+)$ and hence $\Delta^r \in Z(G)$, where *r* is the order of the permutation σ . In the braid groups, for example, we have r = 2.

Henceforth g will denote an arbitrary element of G, which is represented by the word $w = \mu_1^{\epsilon_1} \mu_2^{\epsilon_2} \dots \mu_n^{\epsilon_n} \in \tilde{A}^*$, where each $\mu_i \in \tilde{X}$ and $\epsilon_i \in \{1, -1\}$. (We assume that $\epsilon_i = 1$ if $\mu_i = 1$.) Let p := p(w) and m := m(w) be the total number of ϵ_i equal to 1 and -1, respectively; so p + m = n.

Suppose that $m \ge 1$ and k is maximal with $\epsilon_k = -1$. Then, using the relations $\Delta \mu =_G \sigma(\mu) \Delta$ and $\mu^{-1} \Delta =_G \mu^*$ for $\mu \in \widetilde{X}$, we have

$$w\Delta =_G \mu_1^{\epsilon_1} \dots \mu_{k-1}^{\epsilon_{k-1}} \mu_k^* \sigma^{-1}(\mu_{k+1}) \dots \sigma^{-1}(\mu_n),$$

and we shall denote this word of length *n* in \tilde{A}^* by $\rho(w\Delta)$. If $m \ge 2$, then we can define $\rho(w\Delta^2)$ as $\rho(\rho(w\Delta)\Delta)$ and hence by recursion we can define $\rho(w\Delta^r)$ for any $0 \le r \le m$. We define $\rho(\Delta^r w)$ in a similar manner for $0 \le r \le m$, and we have $\rho(w\Delta^m), \rho(\Delta^m w) \in \tilde{X}^*$.

Analogously, if $p \ge 1$ and k is maximal with $\epsilon_k = 1$, then

$$w\Delta^{-1} =_G \mu_1^{\epsilon_1} \dots \mu_{k-1}^{\epsilon_{k-1}} * \mu_k^{-1} \sigma(\mu_{k+1})^{-1} \dots \sigma(\mu_n)^{-1},$$

and we denote this word by $\rho(w\Delta^{-1})$. We can thus define $\rho(w\Delta^{-r})$ and (similarly) $\rho(\Delta^{-r}w)$ for $0 \le r \le p$, and it is straightforward to verify that $\rho(w\Delta^{-r}) = \rho(\Delta^r w^{-1})^{-1}$ and $\rho(\Delta^{-r}w) = \rho(w^{-1}\Delta^r)^{-1}$. These words all have length n = |w|.

For $g \in G^+$, it is conceivable that the length $|g|_{G^+}$ of the shortest word in X^* that represents g could be longer than the length $|g|_G$ of the shortest word in A^* that represents g. Our next aim is to prove that this does not happen, and so $|g|_{G^+} = |g|_G$.

Lemma 2.3. Let $g \in G^+$ with $|g|_{G^+} = n$. Then $|\Delta^r g|_{G^+} = n + r$ for any $r \ge 0$.

Proof. It is clearly sufficient to prove this for r = 1. Let $v_1 \dots v_k$ be a shortest word in X^* that represents Δg . Then, by Lemma 2.2, we can assume that $v_1 = \Delta$, but then cancelling Δ gives $g =_G v_2 \dots v_k$, so $k - 1 \ge n$. But clearly $k \le n + 1$, so k = n + 1 as claimed.

Proposition 2.4. Let $g \in G^+$ with $|g|_{G^+} = n$, and suppose that $g =_G w$ with $w \in A^*$. Then $|w| - m(w) \ge n$. In particular, $|w| \ge n$ and so $|g|_G = n$.

Proof. Let m = m(w). Since $\rho(\Delta^m w)$ is a word in \tilde{X}^* of length |w| with $\rho(\Delta^m w) =_G \Delta^m g$, Lemma 2.3 implies that $|w| \ge m + n$.

The next two results are parts of Lemma 3.2 and Proposition 3.3 of [2].

Lemma 2.5. Let $g \in G^+$ with $|g|_G = n$ and let $k \in \mathbb{N}$ with $1 \le k \le n$. Then $|g\Delta^{-k}|_G = |\Delta^{-k}g|_G \le n$ with equality if and only if $\Delta \nleq g$.

780

Proof. We have $g\Delta^{-k} = \Delta^k (\Delta^{-k}g)\Delta^{-k}$, and X is closed under conjugation by Δ , so $|g\Delta^{-k}|_G = |\Delta^{-k}g|_G$.

Let $w \in X^*$ represent g with |w| = n. Since $|\rho(\Delta^{-k}w)| = n$, we have $|\Delta^{-k}g|_G \leq n$. Clearly $\Delta \leq g$ implies that $|\Delta^{-k}g|_G < n$ when k > 0. Conversely, suppose that $\Delta^{-k}g =_G v$ with $v \in A^*$ and |v| < n. So $g =_G \Delta^k v$. By Proposition 2.4, we have $n = |g|_G \leq k + |v| - m$ where m = m(v), so m < k. Hence $g =_G \Delta^{k-m}\rho(\Delta^m v) \in \tilde{X}^*$, so $\Delta < g$.

Lemma 2.6. Let $g \in G^+$ and let $w \in \tilde{X}^*$ with $w =_G g$ and |w| = n. Then $w \in \mathscr{G}(G, A)$ (that is, $|g|_G = n$) if and only if $\Delta \not\leq \Delta^n w^{-1}$.

Proof. If $|g|_G < n$ and $g =_G v$ with $v = v_1 \dots v_k \in X^*$ and k < n, then $\Delta^n w^{-1} =_G \Delta^{n-k} \rho(\Delta^k v^{-1})$, so $\Delta < \Delta^n w^{-1}$. Conversely, if $\Delta < \Delta^n w^{-1}$ then, by Lemma 2.2, we can write $\Delta^n w^{-1} =_G \Delta v$, for some $v \in X^*$ with $|v| < |\rho(\Delta^n w^{-1})| = n$, so $g =_G w =_G v^{-1} \Delta^{n-1} =_G \rho(v^{-1} \Delta^{|v|}) \Delta^{n-1-|v|}$, which is a word of length at most n-1. Hence $|g|_G < n$.

As before, let $w = \mu_1^{\epsilon_1} \mu_2^{\epsilon_2} \dots \mu_n^{\epsilon_n} \in \tilde{A}^*$ represent $g \in G$, where each $\mu_i \in \tilde{X}$ and $\epsilon_i \in \{1, -1\}$, and let p := p(w) and m := m(w). Define $\overline{w} = \rho(g\Delta^m)$ and $\underline{w} = \rho(g^{-1}\Delta^p)$. So \overline{w} and \underline{w} are both words in \tilde{X}^* of length n.

Proposition 2.7. For $w \in \tilde{A}^*$, we have

- (i) $\overline{w} \in \mathscr{G}(G, \widetilde{A}) \iff \Delta \nleq \Delta^p g^{-1};$
- (ii) $\underline{w} \in \mathscr{G}(G, \tilde{A}) \iff \Delta \nleq g \Delta^m \iff \Delta \nleq \Delta^m g.$

Proof. (i) follows from Lemma 2.6 and the fact that $\Delta^n \overline{w}^{-1} =_G \Delta^p g^{-1}$. Lemma 2.6 tells us that $\underline{w} \in \mathscr{G}(G, \widetilde{A})$ if and only if $\Delta \not\leq \Delta^n \underline{w}^{-1} =_G \Delta^m g$. But since $g\Delta^m =_G \Delta^{-m} (\Delta^m g) \Delta^m$, this is the case if and only if $\Delta \not\leq g\Delta^m$.

The following result, which is Lemma 3.6 of [2], characterizes the words in $\mathscr{G}(G, A) = \mathscr{G}(G, \tilde{A})$.

Proposition 2.8. Let $w \in A^*$ represent $g \in G$, with |w| = n and m = m(w). Then $w \in \mathcal{G}(G, A)$ if and only if one of the following holds:

- (1) m = 0 and $w = \overline{w} \in \mathscr{G}(G, A)$;
- (2) m = n and $w^{-1} = \underline{w} \in \mathscr{G}(G, A)$;
- (3) 0 < m < n and both \overline{w} and w lie in $\mathcal{G}(G, A)$.

Proof. The cases m = 0 and m = n are obvious, so suppose that 0 < m < n. Let $k = |\overline{w}|_G$, so $k \le |\overline{w}| = n$. First note that, if k < m, then $g =_G \overline{w}\Delta^{-m} =_G \rho(v\Delta^{-k})\Delta^{-m+k}$, where v is a word in X* of length k representing \overline{w} . So $|g|_G \le m$ and, since m < n, neither w nor \overline{w} is geodesic.

Hence we may assume that $k \ge m$ and by Lemma 2.5 applied with \overline{w} in place of g and m in place of k, we have $|g|_G \le k$, with equality if and only if $\Delta \not\le \overline{w}$. Now w is geodesic if and only if $|g|_G = n$, which is the case if and only if k = n and $\Delta \not\le \overline{w}$. Clearly k = n is equivalent to $\overline{w} \in \mathcal{G}(G, A)$. By Lemma 2.7, $\underline{w} \in \mathcal{G}(G, A)$ if and only if $\Delta \not\le g\Delta^m =_G \overline{w}$.

We are now ready to prove our main result.

Theorem 2.9. If $w \in A^*$ with $w \notin \mathscr{G}(G, A)$, then w 3-fellow travels with an equivalent shorter word. So G has FFTP with respect to A.

Proof. Let $w = \mu_1^{\epsilon_1} \mu_2^{\epsilon_2} \dots \mu_n^{\epsilon_n}$ with each $\mu_i \in X$, $\epsilon_i \in \{1, -1\}$, and set p := p(w) and m := m(w). We may assume that the maximal proper prefix w(n-1) of w is geodesic.

By Propositions 2.8 and 2.7 either p > 0 and $\Delta \leq \Delta^p g^{-1}$ or m > 0 and $\Delta \leq \Delta^m g$. These two conditions are clearly symmetrical, so we shall assume that the first one holds.

For $0 \le i \le n$, let $p(i) := p(w(i)) = |\{j \mid 1 \le j \le i, \epsilon_j = 1\}|$. Recalling the conditions $\Delta \mu =_G \sigma(\mu) \Delta$ and $\Delta \mu^{-1} =_G *\mu = \sigma(\mu^*)$, we find that $\rho(\Delta^p g^{-1}) = \lambda_n \lambda_{n-1} \dots \lambda_1$ where each $\lambda_i \in \widetilde{X}$ and, for $1 \le i \le n$, $\lambda_i = \sigma^{p(i)}(\mu_i^*)$ when $\epsilon_i = 1$ and $\lambda_i = \sigma^{p(i)}(\mu_i)$ when $\epsilon_i = -1$.

We now rewrite the word $\lambda_n \lambda_{n-1} \dots \lambda_1$ as described in the comments preceding Lemma 2.2. So we define elements η_i for $1 \le i \le n$ and ν_i for $1 \le i < n$ of \widetilde{X} which satisfy $\eta_1 = \lambda_1$ and $\lambda_{i+1}\eta_i = \eta_{i+1}\nu_i$ for $1 \le i < n$, where $\eta_{i+1} = \Delta \wedge (\lambda_{i+1}\eta_i)$. Then $\lambda_n \dots \lambda_1 =_G \eta_n \nu_{n-1} \dots \nu_1$ and $\eta_i = \Delta \wedge (\lambda_i \dots \lambda_1)$ for $1 \le i \le n$. So, since we are assuming that $\Delta \le \Delta^p g^{-1} =_G \lambda_n \lambda_{n-1} \dots \lambda_1$, we have $\eta_n = \Delta$.

We shall now proceed to define a word $v = \kappa_1 \dots \kappa_{n-1} \in A^*$, which is equal in *G* to *w*. We shall then go on to show that *v* 2-fellow travels with *w*.

Let k be maximal such that $k \le n$ and $\epsilon_k = 1$. (We are assuming p > 0, so such a k exists.) Define q(i) := p(i) for $0 \le i < k$ and q(i) := p(i) - 1 = p - 1for $k \le i < n$. Then, for $1 \le i < n$, since q(i) = q(i - 1) or q(i - 1) + 1, we have $\Delta^{-q(i-1)}v_i^{-1}\Delta^{q(i)} \in \tilde{A}$, and we define κ_i to be this element. Since $\eta_n = \Delta$ and q(n-1) = p - 1, we have

$$v := \kappa_1 \dots \kappa_{n-1} =_G v_1^{-1} v_2^{-1} \dots v_{n-1}^{-1} \Delta^{p-1} =_G \lambda_1^{-1} \dots \lambda_n^{-1} \Delta^p =_G w$$

The configuration is illustrated in Figure 1 for a word $w = \mu_1 \mu_2 \mu_3^{-1} \mu_4 \mu_5 \mu_6^{-1} \mu_7^{-1}$ in which p = 4, m = 3 and k = 5.

To show that v 2-fellow travels with w, observe that, for $1 \le i < n$,

$$w(i)\Delta^{-p(i)} =_{G} \lambda_{1}^{-1} \dots \lambda_{i}^{-1}$$

= $_{G} v_{1}^{-1} v_{2}^{-1} \dots v_{i-1}^{-1} \eta_{i}^{-1}$
= $_{G} v_{1}^{-1} v_{2}^{-1} \dots v_{i}^{-1} \Delta^{q(i)} \Delta^{-q(i)} v_{i} \eta_{i}^{-1}$
= $_{G} \kappa_{1} \dots \kappa_{i} \Delta^{-q(i)} v_{i} \eta_{i}^{-1} = v(i) \Delta^{-q(i)} v_{i} \eta_{i}^{-1}.$



Figure 1. w and v fellow travel.

Thus $v(i)^{-1}w(i) =_G \Delta^{-q(i)}v_i\eta_i^{-1}\Delta^{p(i)}$. Since p(i) = q(i) or q(i) + 1 for all i, we have $\eta_i^{-1}\Delta \in \tilde{A}$, and \tilde{A} is closed under conjugation by Δ . This proves that $|v(i)^{-1}w(i)|_G \leq 2$.

Since the word v is in \tilde{A}^* , it could conceivably include occurrences of 1. However, from our assumption that $w(n-1) \in \mathcal{G}(G, A)$, we have $|w|_G \ge n-2$, so in fact $\kappa_i = 1$ for at most one value of i. By removing such an element κ_i from v if it exists, we obtain a word equivalent to w in A^* which 3-fellow travels with w. This completes the proof.

References

- R. Charney, Geodesic automation and growth functions for Artin groups of finite type. *Math. Ann.* 301 (1995), 307–324. Zbl 0813.20042 MR 1314589
- [2] R. Charney and J. Meier, The language of geodesics for Garside groups. *Math. Z.* 248 (2004), 495–509. Zbl 1062.57002 MR 2097371
- [3] P. Dehornoy and L. Paris, Gaussian groups and Garside groups, two generalisations of Artin groups. *Proc. London Math. Soc.* (3) 79 (1999), 569–604. Zbl 1030.20021 MR 1710165
- [4] M. J. Elder, Finiteness and the falsification by fellow traveler property. *Geom. Dedicata* 95 (2002), 103–113. Zbl 1045.20033 MR 1950887
- [5] M. Elder, Regular geodesic languages and the falsification by fellow traveler property. *Algebr. Geom. Topol.* 5 (2005), 129–134. Zbl 1076.20030 MR 2135549
- [6] W. D. Neumann and M. Shapiro, Automatic structures, rational growth, and geometrically finite hyperbolic groups. *Invent. Math.* **120** (1995), 259–287. Zbl 0831.20041 MR 1329042

Received June 16, 2009; revised January 7, 2010

D. F. Holt, Mathematics Institute, University of Warwick, Zeeman Building, Coventry CV4 7AL, UK

E-mail: D.F.Holt@warwick.ac.uk

784