

DEEP POCKETS IN LATTICES AND OTHER GROUPS

ANDREW D. WARSHALL

ABSTRACT. We show the nonexistence of deep pockets in a large class of groups, extending a result of Bogopol'skii. We then give examples of important groups (namely lattices in Nil and Sol) which have deep pockets.

1. INTRODUCTION

Let G be an infinite group and A a finite generating set for G . We define the *depth* (or more verbosely the *dead-end depth*) of an element $g \in G$ with respect to A to be the distance (in the word metric with respect to A) from g to the complement of the radius- $d_A(1, g)$ closed ball about the identity in G . In fact this definition makes sense if G is replaced with an arbitrary pointed metric space; this will be used in Section 4. Depth must be finite for all $g \in G$ since G is infinite and finitely generated. If the depth of g is > 1 , then g is called a *dead end*. (The idea is that a geodesic word representing g cannot be extended further if it is to remain a geodesic.) We define the depth of G with respect to A to be the supremum of the depths of all elements of G .

A natural question to ask is whether the depth of G for some given generating set A is finite; if it is not, G is said to have *deep pockets* (or alternatively *infinite depth*) with respect to A . One result in this direction has been proven by Bogopol'skii (see [1]), who showed that all hyperbolic groups have finite depth with respect to all generating sets. We extend this result to a broader class of groups, namely those with a regular language of geodesics. To be precise, we prove the following

Theorem 1.1. *Let G be an infinite group with a regular language L of geodesics with respect to a finite generating set A for G . Then there exists a uniform bound for the depth of elements of G with respect to A .*

Definition 1.2. A group is said to be *weakly geodesically automatic* if it admits an automatic structure made up entirely of geodesics.

Corollary 1.3. *Any group G weakly geodesically automatic with respect to a generating set A has a uniform bound on depth with respect to A .*

Two cases of this corollary are hyperbolic groups and finitely generated abelian groups, each with respect to any set of generators; for details see [5]. The first of these coincides with Bogopol'skii's result, while the second is extended by Lehnert

Received by the editors March 30, 2007.

2000 *Mathematics Subject Classification.* Primary 20F65.

The author thanks his advisor, Andrew Casson, as well as John Mackay and Joshua Zelinsky for their helpful comments and the anonymous referee for two careful readings.

in [6], where he shows that finitely generated abelian groups in fact have finitely many dead ends (of any depth).

The next result provides a slight extension of the finitely generated abelian case. By a euclidean group is meant a group acting discretely by isometries on \mathbb{E}^n for some nonnegative integer n . It is well known that any such group has a finite-index subgroup isomorphic to \mathbb{Z}^n for some nonnegative integer n .

Theorem 1.4. *Any euclidean group has a uniform bound on depth with respect to any set of generators.*

These theorems seem unsurprising, since previous constructions of groups with deep pockets tended to involve wreath products or the like; see [4], [3]¹ and [7]². However, here we give two examples of comparatively well-known and well-behaved groups whose depth is infinite with respect to reasonably standard generating sets.

Theorem 1.5. *Let $H = \langle a, b \mid [a, [a, b]], [b, [a, b]] \rangle$ be the discrete Heisenberg group. Then H has infinite depth with respect to its two-element generating set $\{a, b\}$.*

Theorem 1.6. *Let R be a hyperbolic automorphism of \mathbb{Z}^2 and let $G_R = \mathbb{Z}^2 \rtimes_R \mathbb{Z}$. Let $\{a, b\}$ be the standard generating set for \mathbb{Z}^2 and let $\{c\}$ be that for \mathbb{Z} . Then G_R has infinite depth with respect to $\{a, b, c\}$.*

It is interesting that H and G_R are lattices in two of Thurston's eight three-dimensional model geometries (see [8]), namely Nil and Sol respectively. In contrast, it follows from Theorem 1.1 (or [1]) and Theorem 1.4 that no lattice in \mathbb{H}^3 , $S^2 \times \mathbb{R}$, $\widehat{SL}_2(\mathbb{R})$ or \mathbb{E}^3 can have deep pockets. Since the question of admitting a lattice with deep pockets is meaningless for S^3 as it is compact (so that any lattice must be finite), there remains one model geometry for which it is (to the best of this author's knowledge) open, namely $\mathbb{H}^2 \times \mathbb{R}$.

The paper is organized as follows. In the short Section 2, we prove Theorem 1.1. Then, in Section 3, we prove some preliminary results, which will be used in Sections 1.4 and 1.6. Sections 4, 5 and 6 contain the proofs of Theorems 1.4, 1.5 and 1.6 respectively, except that the proof of Theorem 1.6 in Section 6 assumes three auxiliary results about $\mathbb{Z}[t, t^{-1}]$ -module structures on \mathbb{Z}^2 , namely Proposition 6.6 and Lemmas 7.10 and 7.11. These are somewhat technical and are proven in Section 7.

2. GROUPS WITH A REGULAR LANGUAGE OF GEODESICS

Proof of Theorem 1.1. Since G is infinite, every individual element has finite depth. Let n be the number of states of a (deterministic) finite-state automaton F accepting L . Then it will suffice to prove the existence of a uniform bound on depth for elements at distance at least n from the identity in G with respect to A . Let g be such an element and consider the sequence of states assumed by F as it reads the element w of A representing g . This sequence has length at least $n + 1$, so, by the pigeonhole principle, the last $n + 1$ terms of this sequence must contain at least one

¹The published version of this paper contains an error, pointed out by Lehnert; a corrected version is available from the [arXiv](https://arxiv.org/).

²The published version of this paper contains an analogous error, as became clear when the error in [3] was pointed out. This does not, however, affect the proof of Theorem 3, contained in Sections 2 and 3.

repetition. We thus express w as abc , where $|bc| \leq n$, $|b| > 0$ and F is in the same state after reading ab as after reading a . Then F will also accept abc , since after reading abb it will be in the same state as after reading ab , so that reading c will get it into an accept state. Since all words accepted by F are geodesic, abc is a geodesic word of length greater than that of $w = abc$ (since $|b| > 0$) and representing a group element within $|c| + |bc| \leq 2|bc| \leq 2n$ of g . Thus the depth of g is $\leq 2n$, so we are done. \square

3. PRELIMINARIES ON METRIC GEOMETRY

We need the following auxiliary result, which will be used in Sections 4 and 6.

Lemma 3.1 (Fuzz Lemma). *Let f be a function from a metric space A to \mathbb{Z} and let $n \in \mathbb{Z}$. Suppose there exists $a \in A$ and $r \in \mathbb{Z}$ such that, for all $a' \in B_r(a)$, $f(a') \leq f(a) + n$. Then there exists some $a_0 \in A$ such that f attains a maximum on $B_{r/n}(a_0)$ at a_0 .*

Proof. Define $g(x)$ to be $\max_{b \in B_a(x)} f(b)$ for $x > 0$ and $f(a)$ for $x = 0$. Clearly, g is nondecreasing and, by hypothesis, $g(r) \leq f(a) + n = g(0) + n$. Thus there must exist some x such that g is constant on the interval $(x, x + r/n]$, where $x + r/n \leq r$. Then we may just set a_0 to be an element of A at distance $\leq x$ from a such that $f(a_0) = g(x)$. By the triangle inequality and the definition of g , f is bounded on $B_{r/n}(a_0)$ by $g(x + r/n) = g(x) = f(a_0)$. \square

From this we deduce

Proposition 3.2. *Suppose a pointed metric space (A, a_0, d) has deep pockets. Then, if C is a real number and d' is a integer-valued metric on A such that*

$$(3.1) \quad |d'(a_1, a_2) - d(a_1, a_2)| < C$$

for all $a_1, a_2 \in A$, the resulting pointed metric space (A, a_0, d') will still have deep pockets.

Proof. Let $f: A \rightarrow \mathbb{Z}$ be distance from the origin with respect to the new metric, and let a have depth at least $r + C$ with respect to (A, a_0, d) . Then Lemma 3.1 gives a dead end with respect to (A, a_0, d') of depth at least r/C . Since r was arbitrary, we are done. \square

We should also point out that the concept of deep pockets can be applied to functions on metric spaces. If (A, d) is a metric space and $f: A \rightarrow \mathbb{R}$, then we say f has deep pockets (with respect to d) if for every $n \in \mathbb{N}$ there is $a \in A$ such that f attains its maximum on $B_n(a)$ at a . Lemma 3.1 thus implies

Proposition 3.3. *Let (A, a_0, d) be a pointed metric space. Let $R \in \mathbb{R}$ and let $f: A \rightarrow \mathbb{Z}$ be such that $|f(a) - d(a, a_0)| \leq R$ for every $a \in A$. Then f has deep pockets (with respect to d) iff (A, a_0, d) has deep pockets (in the usual sense).*

4. EUCLIDEAN GROUPS

In this section, we prove Theorem 1.4. Although our treatment is self-contained, it should be noted that it is along the same lines as Cannon's proof of Theorem 2.5

in [2]. In particular, our proof of Proposition 4.6 uses in effect Benson's so-called (by Cannon) Factorization Lemma, cited in [2]. We start with the following

Definition 4.1. We define a *weighted* subset of \mathbb{Z}^n to be an ordered pair (A, μ) , where A is a subset of \mathbb{Z}^n and $\mu: A \rightarrow \mathbb{N}$ is called the *weight* function. If A is a generating set for \mathbb{Z}^n , then we call (A, μ) a weighted generating set. We say that the *length* of the word $a_1 a_2 \dots a_m$ with respect to the weight function μ is $\sum_{i=1}^m \mu(a_i)$.

It is clear that a weighted generating set defines a word metric just as does an ordinary generating set. The idea of the proof will be that a generating set for a euclidean group gives rise to a weighted generating set for a finite-index abelian subgroup which has (roughly) the same depth properties. We will then be done by the following

Proposition 4.2. *Every finite weighted generating set for \mathbb{Z}^n has depth bounded for all group elements.*

Let (A, μ) be a generating set for \mathbb{Z}^n . Let M be the least common multiple of the elements of the image of μ and let A' be the set consisting of $aM/\mu(a)$ for every $a \in A$. If we regard \mathbb{Z}^n as being embedded in the obvious way as a lattice in \mathbb{R}^n and let B be the convex hull of $A' \cup A'^{-1}$ in \mathbb{R}^n , then B will clearly be a convex polytope. In fact, its dimension will be n , since otherwise A would be contained in an $(n-1)$ -dimensional subspace and hence could not generate. We have the following

Proposition 4.3. *If $a_1, a_2, \dots, a_m \in A' \cup A'^{-1}$ are the vertices of a facet of B and i_1, i_2, \dots, i_m are nonnegative integers, then $w = a_1^{i_1} a_2^{i_2} \dots a_m^{i_m}$ is a geodesic word. In fact, w lies on a geodesic ray.*

For the proof, we remind the reader that by a facet of an n -dimensional polytope is meant an $(n-1)$ -dimensional face.

Proof. The facet of B of which a_1, a_2, \dots, a_m are vertices must lie in some hyperplane H in \mathbb{R}^n , say $\mathbf{a} \cdot \mathbf{x} = b$. Since B is symmetric about the origin and lies in one of the closed half-spaces bounded by H , if the origin lay in H , then B would lie entirely in H . But then so would $A' \cup A'^{-1}$, and hence $A \cup A^{-1}$ would as well, which is a contradiction since A generates \mathbb{Z}^n . Thus $b \neq 0$ and we may choose \mathbf{a} so that $b = 1$; so H is given by the equation $\mathbf{a} \cdot \mathbf{x} = 1$ and B lies in the closed half-space given by $\mathbf{a} \cdot \mathbf{x} \leq 1$. In particular, so does $A' \cup A'^{-1}$; therefore, if $g \in \mathbb{Z}^n$ is given by a word of length l with respect to (A, μ) , then $\mathbf{a} \cdot g \leq l/M$. Setting $g = a_1^{i_1} a_2^{i_2} \dots a_m^{i_m}$, we have $\mathbf{a} \cdot g = \sum_{j=1}^m i_j$, so the minimal length for a word representing g is $M \sum_{j=1}^m i_j$. But this is the length of w since each a_i has length M , proving the first sentence. The second sentence follows clearly. \square

Proposition 4.4. *Every element of \mathbb{Z}^n is within uniformly bounded distance (with respect to (A, μ)) of a geodesic ray.*

Proof. By choosing a finite triangulation of each facet f_i of B , we can assume without loss of generality that the facets are all $(n-1)$ -simplices and hence have n vertices. As in the proof of Proposition 4.3, no facet may be confined to any hyperplane through the origin, so the vertices of each facet (since they clearly cannot lie in one $(n-2)$ -plane) must be linearly independent and hence generate a maximal-rank lattice. If we regard this lattice as a based lattice embedded in

\mathbb{R}^n with the usual norm, it will partition \mathbb{R}^n , hence \mathbb{Z}^n , into closed parallelepipeds. Clearly there exists some bound d_i on the A -distance between any element of \mathbb{Z}^n contained in the closed unit parallelepiped generated by the facet f_i and the origin. By translation, we find that every element of \mathbb{Z}^n is within d_i of some corner of every parallelepiped in which it lies. Since B has finitely many facets, we may set d to be the greatest of the d_i .

We claim that every element of $\mathbb{Z}^n - B$ is within d of a geodesic ray. So let $g \in \mathbb{Z}^n - B$ and consider the line segment s (in \mathbb{R}^n) between g and the origin. Since the origin is in B , $g \notin B$ and B is convex, s intersects the boundary of B exactly once. We call this point of intersection t and let a_1, a_2, \dots, a_n be the vertices of a (closed) facet containing t . By the previous paragraph, g is within distance d of some corner of every parallelepiped of the $a_1 a_2 \dots a_n$ -lattice to which it belongs. But the coordinates of g with respect to a_1, a_2, \dots, a_n as an element of \mathbb{R}^n must be nonnegative since they are obtained by multiplying a positive number by the coordinates of t , which is (as a vector) a weighted average of a_1, a_2, \dots, a_n . Hence g belongs to a parallelepiped, all of whose corners have all their coordinates nonnegative and hence (by Proposition 4.3) lie on a geodesic ray, proving our claim.

Since B is bounded, the case $g \in B$ is trivial. □

We will now finish the proof that depth is bounded for abelian groups with respect to finite weighted generating sets.

Proof of Proposition 4.2. Let d be the bounded distance whose existence was proven in the preceding proposition. Let $g \in \mathbb{Z}^n$ with word length l . Then g is at distance at most d from an element on a geodesic ray whose (A, μ) -distance from the origin is, by the triangle inequality, at least $l - d$. Then there exists a group element g' at distance at least $d + 1$ but at most $d + M + 1$ further out along this ray, since every length- M segment of a geodesic ray contains at least one group element. The distance of g' from the origin must be at least $l + 1$ and, by the triangle inequality again, its distance from g is at most $2d + M + 1$. Thus g has depth at most $2d + M + 1$, as claimed. □

Let A be a generating set for a euclidean group E and let $\mathbb{Z}^n \triangleleft E$. We will construct a finite weighted generating set for \mathbb{Z}^n with roughly the same depth properties that A has as a generating set for E . Let $\phi: F_A \rightarrow E$ be the projection map. We denote the length of a word $w \in F_A$ by $l(w)$. Let A' be the set of words w in $A \cup A^{-1}$ such that $\phi(w) \in \mathbb{Z}^n$ but, for any proper subword w' of w , $\phi(w') \notin \mathbb{Z}^n$. Let (B, μ) be the finite weighted subset of \mathbb{Z}^n where $B = \{a^g \mid a \in A', g \in E\} = \bigcup_{h \in E/\mathbb{Z}^n} A'^h$ and μ is defined so that $\mu(a^g)$ is the length of a (as a word in A) for $a \in A'$ and $g \in E$. It will follow from Proposition 4.5 that this is in fact a weighted generating set. In any event, let $\pi: \mathbb{Z}^B \rightarrow \mathbb{Z}^n$ be the projection and let $l_\mu(v)$ denote the length of the word $v \in \mathbb{Z}^B$ with respect to μ . We denote the distance of $x \in \mathbb{Z}^n$ from the origin (at the moment, possibly infinite) with respect to this generating set by $\|x\|$.

Proposition 4.5. *Suppose $w \in F_A$ with $\phi(w) = x \in \mathbb{Z}^n$. Then $\|x\| \leq l(w)$. In particular, B is a generating set for \mathbb{Z}^n .*

Proof. Since $\phi(w) \in \mathbb{Z}^n$, w must contain some minimal subword under inclusion in $\phi^{-1}(\mathbb{Z}^n)$, say w_1 . By definition, $w_1 \in A'$. Then $w = w_l w_1 w_r$ may be replaced with

$w_1^{w_i^{-1}} w_l w_r$, where $w_1^{w_i^{-1}} \in B$ and

$$(4.1) \quad \mu(w_1^{w_i^{-1}}) = \mu(w_1) = l(w_1) = l(w) - l(w_l) - l(w_r) \leq l(w) - l(w_l w_r)$$

by definition and the triangle inequality. The first claim is now proven by induction. The second claim follows easily. \square

Proposition 4.6. *There exists a D such that for any $x \in \mathbb{Z}^n$ there is a word $w \in F_A$ with $\phi(w) = x$ and $l(w) \leq \|x\| + D$.*

Proof. Let $m = [E : \mathbb{Z}^n]$ and pick a set of words w_1, \dots, w_m in F_A representing each of the finitely many cosets of \mathbb{Z}^n in E . Consider a word $v \in \mathbb{Z}^B$ with $\pi(v) = x$ and $l_\mu(v) = \|x\|$. Since \mathbb{Z}^n is abelian, we can assume that v is ordered to separate out the letters in each A^h . The word v is thus divided into m pieces, $v_1 v_2 \dots v_m$, where each $v_i \in \mathbb{Z}^{A^h}$ for some specific $h \in E/\mathbb{Z}^n$. Thus each v_i can be replaced with $w_i^{-1} v'_i w_i$ for some $v'_i \in \mathbb{Z}^{A'}$ with $l_\mu(v'_i) = l_\mu(v_i)$. But then each v'_i can be replaced with a $v''_i \in F_A$ with $l(v''_i) \leq l_\mu(v'_i) = l_\mu(v_i)$ by the construction of A' and μ . We thus have

$$(4.2) \quad l(w_i^{-1} v''_i w_i) \leq 2l(w_i) + l(v''_i) \leq 2l(w_i) + l_\mu(v_i).$$

Concatenating these yields $w = w_1^{-1} v''_1 w_1 w_2^{-1} v''_2 w_2 \dots w_m^{-1} v''_m w_m \in F_A$ with $\phi(w) = x$ and

$$(4.3) \quad \begin{aligned} l(w) &\leq \sum_{i=1}^m l(w_i^{-1} v''_i w_i) \leq \sum_{i=1}^m (2l(w_i) + l_\mu(v_i)) \\ &= 2 \sum_{i=1}^m l(w_i) + l_\mu(v) = 2 \sum_{i=1}^m l(w_i) + \|x\|, \end{aligned}$$

so we are done if we set $D = 2 \sum_{i=1}^m l(w_i)$. \square

Proof of Theorem 1.4. It follows from Propositions 4.2, 4.5, 4.6 and 3.2 that \mathbb{Z}^n cannot have deep pockets with respect to the subspace metric induced from the metric with respect to A on E . But since $[E : \mathbb{Z}^n] < \infty$, every element of E lies within bounded distance b of \mathbb{Z}^n . Thus, if E had a dead end of depth d , then \mathbb{Z}^n would have (with respect to the subspace metric) a dead end of depth at least $d/b + 1$, by Lemma 3.1. Thus E cannot have deep pockets, as claimed. \square

5. THE HEISENBERG GROUP

In this section, we prove Theorem 1.5. We consider the Heisenberg group H with respect to its standard two-generator presentation $\langle a, b \mid [a, [a, b]], [b, [a, b]] \rangle$. (We use $[x, y]$ to denote $x^{-1}y^{-1}xy$.) It is well known that every element of H is expressible uniquely as a word of the form $a^i b^j [a, b]^k$, with $a, b, c \in \mathbb{Z}$. In general, of course, these words are not of minimal length; for example, ba is expressed as $ab[a, b]^{-1}$. However, we give the following way of visualizing elements of H , from which insight can be gained as to minimal-length words.

Consider i and j as coordinates in the standard integer lattice \mathbb{Z}^2 . Then we can represent a word in a and b as a path in \mathbb{Z}^2 starting at the origin. Multiplication on the right by $a^{\pm 1}$ corresponds to appending to the path a segment one unit to the right or left, while multiplication by $b^{\pm 1}$ corresponds to appending a segment one unit up or down. It is clear that this gives a one-to-one correspondence between words and paths and that a word representing $a^i b^j [a, b]^k$ corresponds to a path

from the origin to (i, j) . If to this path we append a vertical segment leading from (i, j) to $(i, 0)$ and a horizontal segment from $(i, 0)$ to the origin, we get a loop based at the origin. This loop will correspond to a word representing $a^i b^j [a, b]^k b^{-j} a^{-i} = a^i b^j b^{-j} a^{-i} [a, b]^k = [a, b]^k$. We have thus reduced the study of the correspondence between paths starting at the origin and elements of H to that of the correspondence between loops based at the origin and powers of $[a, b]$.

Proposition 5.1. *If two loops based at the origin correspond to the same power of $[a, b]$, then they enclose the same oriented area.*

Proof. Consider two loops based at the origin that correspond to the same power of $[a, b]$. Then one can be transformed into the other by appending loops conjugate to $a^{-1}a$, aa^{-1} , $b^{-1}b$, bb^{-1} , $[a, [a, b]]$, $[b, [a, b]]$, $[[a, b], a]$ and $[[a, b], b]$. But the area enclosed by the concatenation of two loops is the sum of the areas enclosed by each loop, so it suffices to show that any loop conjugate to one of the eight listed above encloses zero area. Since conjugation does not affect the area enclosed by a loop, it in fact suffices to show that the eight loops listed above enclose zero area. But this can be checked trivially. \square

Proposition 5.2. *Any loop based at the origin corresponds to $[a, b]^k$, where k is the oriented area it encloses.*

Proof. By Proposition 5.1 and the discussion preceding it, it suffices to show that the path corresponding to the word $[a, b]$ encloses an oriented area of 1. But this is clear. \square

Proposition 5.3. *Any path P from the origin to (i, j) corresponds to $a^i b^j [a, b]^k$, where k is the oriented area enclosed by the concatenation of P and the path corresponding to $b^{-j} a^{-i}$.*

Proof. This is just the combination of Proposition 5.2 and the discussion preceding Proposition 5.1. \square

Proposition 5.4. *The element $[a, b]^{n^2+1}$ is at distance $4n + 2$ from the identity.*

Proof. Clearly, $[a, b]^{n^2+1}$ is within $4n + 2$ of the identity, since it equals

$$(5.1) \quad [a, b][a, b]^{n^2} = [a, b][a^n, b^n] = a^{-n}[a, b]b^{-n}a^n b^n = a^{-n-1}b^{-1}ab^{-n+1}a^n b^n.$$

So consider a word w representing $[a, b]^{n^2+1}$. By Proposition 5.3, we know that w corresponds to a loop based at the origin enclosing oriented area $n^2 + 1$. The word w must contain the same number of letters a as a^{-1} and the same number of letters b as b^{-1} . Let x be the number of letters a , and let y be the number of letters b . Then $xy > n^2$, so, by the arithmetic mean–geometric mean inequality, $x + y > 2n$. Thus $x + y \geq 2n + 1$, so the length of w is at least $4n + 2$. \square

Proposition 5.5. *The element $a^i b^j [a, b]^k$ with $|i| < n$, $|j| < n$ and $|k| < n(n + 1)$ is within $4n + 2$ of the identity.*

Proof. Since, by Proposition 5.3, rotations of the plane by $\pi/2$ about the origin and reflections about the line $j = 0$ do not affect distance from the identity, we may assume without loss of generality that $i \geq |j|$ and $k \geq 0$. Let $k = q(n + 1) + r$, $0 \leq r \leq n$, and $0 \leq q \leq n - 1$. Then clearly $b^{-q-1}a^r b a^{n+1-r} b^q a^{-n-1}$ is a loop based at the origin of length $2q + 2n + 4 \leq 4n + 2$, bounding oriented area $q(n + 1) + r =$

k. Thus $b^{-q-1}a^rba^{n+1-r}b^qa^{i-n-1}b^j$ represents $a^ib^j[a, b]^k$, and it will have length $2q + 2n + 4 - i + |j| \leq 2q + 2n + 4 \leq 4n + 2$ since $|j| \leq i \leq n + 1$. \square

Proposition 5.6. *Every element within distance m of $[a, b]^{n^2+1}$ is of the form*

$$(5.2) \quad a^ib^j[a, b]^k$$

with $|i| \leq m, |j| \leq m$ and $|k| \leq n^2 + 1 + m(m - 1)/2$.

Proof. We proceed by induction. The statement is clear for $m = 0$. So consider $w = a^ib^j[a, b]^k$ with $|i| \leq m, |j| \leq m$ and $|k| < n^2 + 1 + m(m - 1)/2$. Then $wb = a^ib^{j+1}[a, b]^k, wb^{-1} = a^ib^{j-1}[a, b]^k, wa = a^ib^ja[a, b]^k = a^{i+1}b^j[a, b]^{-j}[a, b]^k = a^{i+1}b^j[a, b]^{k-j}$ and $wa^{-1} = a^ib^ja^{-1}[a, b]^k = a^{i-1}b^j[a, b]^j[a, b]^k = a^{i-1}b^j[a, b]^{k+j}$. By the triangle inequality, these four new words can all be expressed as $a^{i'}b^{j'}[a, b]^{k'}$ with

$$(5.3) \quad |i'| \leq m + 1, \quad |j'| \leq m + 1$$

and

$$(5.4) \quad |k'| \leq n^2 + 1 + \frac{m(m - 1)}{2} + |j| \leq n^2 + 1 + \frac{m(m - 1)}{2} + m = n^2 + 1 + \frac{m(m + 1)}{2},$$

as claimed. \square

The last sentence of the following proposition is just Theorem 1.5.

Proposition 5.7. *If $n > 2$, the element $g_n = [a, b]^{n^2+1}$ is a dead end of depth at least $\sqrt{2n - 4} + 1$. In particular, H has arbitrarily deep dead ends with respect to the generating set $\{a, b\}$.*

Proof. By Proposition 5.4, g_n is at distance $4n + 2$ from the identity. But, by Proposition 5.6, any group element within $\sqrt{2n - 4}$ of g_n is of the form $a^ib^j[a, b]^k$, with

$$(5.5) \quad |i| \leq \sqrt{2n - 4} < n, \quad |j| \leq \sqrt{2n - 4} < n$$

and

$$(5.6) \quad |k| \leq n^2 + n - 1 - \frac{\sqrt{2n - 4}}{2} < n^2 + n = n(n + 1).$$

By Proposition 5.5, any such element is within $4n + 2$ of the identity. The second sentence then follows clearly. \square

6. LATTICES IN SOL

In this section, we begin the proof of Theorem 1.6.

Let R be a hyperbolic automorphism of \mathbb{Z}^2 . We turn our attention to the group

$$(6.1) \quad G_R = \mathbb{Z}^2 \rtimes_R \mathbb{Z}.$$

We denote the standard generators of \mathbb{Z}^2 by a and b and the generator of \mathbb{Z} by c . This group is soluble, as its commutator is contained in (in fact identical to) the span of a and b , which commute with each other. Thus $G'_R = \langle a, b \rangle \cong \mathbb{Z}^2$ is a normal subgroup and $G_R/G'_R = \langle G'_R c \rangle$. The powers of c are thus a complete set of coset representatives, so every element of G_R can be expressed uniquely in the form $a^ib^jc^k$, where i, j and $k \in \mathbb{Z}$. We will use a, b and c to denote these three elements of G_R throughout, and write $S = \{a, b, c\}$. If $g \in G_R$, then $|g|$ will mean the word length of g with respect to S .

Let F_S be the free group on the set S and let N be the normal closure of a and b in F_S . We know N is freely generated by $\{a^{c^i}, b^{c^i} \mid i \in \mathbb{Z}\}$. Any element $g \in F_S$ can be expressed uniquely as a product uc^i , where $u \in N$ and $i \in \mathbb{Z}$. Define $\phi: F_S \rightarrow N_{ab}$ to send g to the image of u under the abelianization map. (We denote by N_{ab} the abelianization of the group N .) Note that N_{ab} is freely generated as an abelian group by $\{a^{c^i}, b^{c^i} \mid i \in \mathbb{Z}\}$.

Define $\pi: N_{ab} \rightarrow G'_R$ to send $v \in N_{ab}$ to the element of G'_R represented by v . Similarly, define $\sigma_R: F_S \rightarrow G_R$ to send $w \in F_S$ to the element of G_R represented by w . Then we have the following commutative diagram:

$$(6.2) \quad \begin{array}{ccc} F_S & \xrightarrow{\phi} & N_{ab} \\ \sigma_R \downarrow & & \downarrow \pi \\ G_R & \xrightarrow{uc^z \mapsto u} & G'_R \end{array}$$

where the bottom arrow represents a map taking uc^z to u for $u \in G_R$ and $z \in \mathbb{Z}$. (Note that neither horizontal arrow represents a group homomorphism.)

Notation. For $w \in F_S$ or N_{ab} , let $l(w)$ denote its length in the given set of generators.

Definition 6.1. Let $g = uc^z \in G_R$ with $u \in G'_R$ and $z \in \mathbb{Z}$. Let $s(g)$ represent the minimal length of any element w of $\sigma_R^{-1}(g)$ such that $\phi(w)$ is of minimal length in $\pi^{-1}(u)$.

Remark 6.2. Any element $w \in \sigma_R^{-1}(g)$ must satisfy $\pi(\phi(w)) = u$.

We can now state the following proposition, which is the first ingredient of the proof of Theorem 1.6 and whose proof we postpone. It gives a coarse equality between the two concepts of “distance from the identity” ($|\cdot|$ and s) on G_R . By Proposition 3.2, this means that one has deep pockets if and only if the other does.

Proposition 6.3. *Let $G_R = \mathbb{Z}^2 \rtimes_R \langle c \rangle$, where R is a hyperbolic automorphism of \mathbb{Z}^2 , and let $S = \{a, b, c\}$, where a and b are the standard generators of \mathbb{Z}^2 . Let $|g|$ denote the word length of g with respect to S . Then there exists D such that, for any $g \in G_R$, $s(g) - D \leq |g| \leq s(g)$.*

The second ingredient, an adaptation of Cleary and Taback’s result on word length in wreath products, is used both in proving and in applying Proposition 6.3. In the notation of the definition of s , it gives us a formula for the minimal length of an element w of $\sigma_R^{-1}(g)$ such that $\phi(w)$ is some specified element of N_{ab} . This will give us control over the behavior of s away from G'_R and hence, by Proposition 6.3, over the $|\cdot|$ norm as well, given information about the geometry of G'_R .

Notation. Let u_1 denote a and u_2 denote b . If $i \in \mathbb{Z}$, let $u_1^{c^i}$ denote $c^{-i}ac^i$ and $u_2^{c^i}$ denote $c^{-i}bc^i$.

Lemma 6.4 (Lamplighter Lemma). *Let $g = uc^z \in G_R = \mathbb{Z}^2 \rtimes_R \langle c \rangle$, where R is a hyperbolic automorphism of \mathbb{Z}^2 , $u \in G'_R$ and $z \in \mathbb{Z}$. Let $v = \sum_{j=1}^n u_{k_j}^{c^{i_j}} \in N_{ab}$ (where all the k_j are 1 or 2) such that $\pi(v) = u$, and let $S = \{a, b, c\}$ where a and*

b are the standard generators of \mathbb{Z}^2 . Then the minimal length of all words $w \in F_S$ such that $\sigma_R(w) = g$, $\phi(w) = v$ is

$$(6.3) \quad 2(\max(i_j, 0) - \min(i_j, 0)) + \min(|z - \max(i_j, 0)| - \max(i_j, 0), |z - \min(i_j, 0)| + \min(i_j, 0)) + n.$$

Proof. Consider the natural maps π_S and π_T mapping F_S and \mathbb{Z}^T , respectively, to

$$(6.4) \quad \mathbb{Z}^2 \wr \mathbb{Z} = \left\langle a, b, c \mid [a^{c^i}, b^{c^j}], [a^{c^i}, a^{c^j}], [b^{c^i}, b^{c^j}] \forall i, j \in \mathbb{Z} \right\rangle.$$

A word $w \in F_S$ satisfies $\sigma_R(w) = g$ and $\phi(w) = v$ if and only if $\pi_S(w) = \pi_T(v)c^z$ in $\mathbb{Z}^2 \wr \mathbb{Z}$. (This is because $\phi(w) = v$ if and only if $\pi_S(w) = \pi_T(v)c^k$ for some k , and then we have $\sigma_R(w) = \pi(v)c^k$.) Thus the minimal length for w is simply the minimal length of a word in F_S representing $\pi_T(v)c^z$ in $\mathbb{Z}^2 \wr \mathbb{Z}$. The result now follows from Cleary and Taback’s length formula in [4] for lamplighter groups. These are essentially wreath products $G \wr \mathbb{Z}$, G some group, with respect to a generating set consisting of generators of G and a standard generator for \mathbb{Z} . \square

The final main ingredient in the proof of Theorem 1.6 is the following proposition, which tells us what we need to know about the geometry of G'_R and whose proof we likewise postpone. It gives us, in particular, large regions of G'_R where distance from the identity with respect to the $|\cdot|$ norm (hence, by Proposition 6.3, also s) is maximized well away from the boundary of the region.

For any group G with generating set A , d_A denotes distance with respect to the word metric on G induced by A . If $v \in N_{ab}$, by $M(v)$ (respectively $m(v)$) we mean the maximal (resp. minimal) exponent i such that v contains a letter a^{c^i} or b^{c^i} .

Proposition 6.5. *Let $G_R = \mathbb{Z}^2 \rtimes \langle c \rangle$, where R is a hyperbolic automorphism of \mathbb{Z}^2 , and let $\{a, b\}$ be a \mathbb{Z} -basis for G'_R . Then there is $T \geq 3$ with the following property. Let n be a positive integer; then for any sufficiently large positive integer m there exists $B_{m,n} \subset G'_R$ such that every $u \in B_{m,n}$ has the following properties:*

- If u is expressed as $ia + jb$, $i, j \in \mathbb{Z}$, then $|i|, |j| < T^m$.
- If $v \in N_{ab}$ is a minimal-length element of $\pi^{-1}(u)$, then $M(v) > n$ and $m(v) < -n$.

Furthermore, there exist $p = p(R, m, n) \in \mathbb{Z}$ and $u \in B_{m,n}$ such that for all u' with $d_{\{a,b\}}(u, u') \leq p$ the following conditions hold:

- $u' \in B_{m,n}$; and
- $|u'| \leq |u|$, where, as usual, $|u|$ refers to the length of u with respect to $\{a, b, c\}$.

Finally, $\lim_{m \rightarrow \infty} p(R, m, n) = \infty$ for every R and n .

With these ingredients, we give the proof of Theorem 1.6, which asserts the existence of deep pockets in G_R with respect to $S = \{a, b, c\}$. Note that R , being hyperbolic, has two real eigenvalues. One of these has absolute value greater than 1; denote this eigenvalue by τ .

Proof of Theorem 1.6. By Proposition 6.3, there exists D such that, for any $g \in G_R$, $s(g) - D \leq |g| \leq s(g)$. Thus, by Proposition 3.3, to prove that G_R has deep pockets with respect to the word metric in S it suffices to prove that for any $n \in \mathbb{N}$ there is $g \in G_R$ such that $s(g) \geq s(g')$ for any g' with $|g^{-1}g'| < n$. (We remind the reader that by $|g^{-1}g'|$ we mean the length of $g^{-1}g'$ with respect to $\{a, b, c\}$.)

To that end, we let τ be the eigenvalue of R of greater absolute value. Then we choose m so that $n|\tau|^n \leq p(R, m, n)$, where p is given by Proposition 6.5; this choice of m is possible since $\lim_{m \rightarrow \infty} p(R, m, n) = \infty$. Define $u \in G'_R$ and $B_{m,n} \subset G'_R$ to be the element and subset given by this same application of Proposition 6.5. Then let $g \in G_R$ be any element of G_R within distance n of u with respect to $S = \{a, b, c\}$. Express g as $u'c^i$, with $u' \in G'_R$ and $i \in \mathbb{Z}$. If $s \in G'_R$ and $i' \in \mathbb{Z}$, then $sc^{i'}a^{\pm 1} = sR^{-i'}(a^{\pm 1})c^{i'}$ and similarly $sc^{i'}b^{\pm 1} = sR^{-i'}(b^{\pm 1})c^{i'}$. It follows that right multiplication of any $sc^{i'}$ with $s \in G'_R$ and $|i'| \leq n$ by any letter of S or its inverse gives $s'c^{i''}$, with $s' \in G'_R$, $i'' \in \mathbb{Z}$, $|i'' - i'| \leq 1$ and $d_{\{a,b\}}(s, s') \leq |\tau|^n$. Thus $|i| \leq |g| \leq n$ and $d_{\{a,b\}}(u, u') < n|\tau|^n \leq p(R, m, n)$, so, by Proposition 6.5, $u' \in B_{m,n}$.

Now let $v \in N_{ab}$ be a minimal-length element of $\pi^{-1}(u')$; then we have $M(v) > n$ and $m(v) < -n$. Since $|i| \leq n$, this implies by Lemma 6.4 that $s(g) = s(u'c^i) \leq s(u')$. But Proposition 6.3 tells us that $s(u') \leq |u'| + D$ and $|u| \leq s(u)$ and Proposition 6.5 tells us that $|u'| \leq |u|$, so we have $s(g) \leq s(u') \leq |u'| + D \leq |u| + D \leq s(u) + D$ and we are done by Lemma 3.1. \square

It remains to prove Propositions 6.3 and 6.5. Let p_R be the characteristic polynomial of R . We denote the greater (in absolute value) of the two eigenvalues of R by τ . Let $\mathbb{Z}[t, t^{-1}]$ denote the ring of Laurent polynomials in one variable over \mathbb{Z} . Any $p \in \mathbb{Z}[t, t^{-1}]$ can be expressed uniquely in the form $\sum_{i=m}^M p_i t^i$ where m, M and all the $p_i \in \mathbb{Z}$ and neither p_m nor p_M is 0. Denote by $m(p)$ and $M(p)$ the values of m and M in this expression and define the *length* of p to be $\|p\| = \sum_{i=m}^M |p_i|$.

The action by R gives rise to the structure of a $\mathbb{Z}[t, t^{-1}]$ -module on $\langle a, b \rangle \cong \mathbb{Z}^2$, where t acts by R . Let M_R refer to \mathbb{Z}^2 with this $\mathbb{Z}[t, t^{-1}]$ -action. We denote the elements of M_R corresponding to a and b by x and y .

The map R , being hyperbolic, has two real eigenvalues, τ and $\pm 1/\tau$, where we take τ to be the eigenvalue of greater absolute value.

We will want some more definitions. If $p, q \in \mathbb{Z}[t, t^{-1}]$, define the *length* of (p, q) to be $\|p\| + \|q\|$. We denote by $M(p, q)$ the greater of $M(p)$ and $M(q)$ and by $m(p, q)$ the lesser of $m(p)$ and $m(q)$.

Observe that conjugation by c sends $a^i b^j$ to $a^{i'} b^{j'}$, where $(i', j') = R(i, j)$. Let $\beta: G'_R \leftrightarrow M_R$ send a to x and b to y . Then $\beta(a^c) = R(\beta(a))$ and $\beta(b^c) = R(\beta(b))$, so this diagram commutes:

$$(6.5) \quad \begin{array}{ccc} G'_R & \xrightarrow{c} & G'_R \\ \beta \downarrow & & \downarrow \beta \\ M_R & \xrightarrow{R} & M_R \end{array}$$

Furthermore, β induces an obvious one-to-one length-preserving correspondence θ between N_{ab} and $\mathbb{Z}[t, t^{-1}]^2$ such that this diagram commutes:

$$(6.6) \quad \begin{array}{ccc} N_{ab} & \xrightarrow{\theta} & \mathbb{Z}[t, t^{-1}]^2 \\ \pi \downarrow & & \downarrow (p,q) \mapsto px+qy \\ G'_R & \xrightarrow{\beta} & M_R \end{array}$$

Proposition 6.3 will then follow from Lemma 6.4 and from

Proposition 6.6. *Let R be a hyperbolic automorphism of \mathbb{Z}^2 , and let A denote \mathbb{Z}^2 equipped with an action by $\mathbb{Z}[t, t^{-1}]$, where t acts by R . Let $\{x, y\}$ be a \mathbb{Z} -basis of A . Let τ be the eigenvalue of R of greater absolute value. Then there are $D_2 > 1$ and $D_1 > D_2 \ln |\tau|/8$ with the following property. Let $z \in A$ and let p, q, p' and $q' \in \mathbb{Z}[t, t^{-1}]$ be such that $px + qy = p'x + q'y = z$, with $\|p\| + \|q\|$ minimal subject to this condition and p' and q' not both 0. Then*

$$(6.7) \quad |\tau|^{M(p,q)-M(p',q')} < D_1(\|p'\| + \|q'\| - \|p\| - \|q\|) + D_2$$

and

$$(6.8) \quad |\tau|^{m(p,q)-m(p',q')} < D_1(\|p'\| + \|q'\| - \|p\| - \|q\|) + D_2.$$

Since the proof of this result is technical, it is deferred to Section 7. We can now combine Proposition 6.6 with Lemma 6.4 to prove Proposition 6.3 and establish the desired coarse equality between $|\cdot|$ and s .

Proof of Proposition 6.3. The bound $|g| \leq s(g)$ is obvious, so we need only prove $s(g) - D \leq |g|$. Write $g = uc^z$, where $u \in G'_R$ and $z \in \mathbb{Z}$, and let v be a minimal-length element of $\pi^{-1}(u)$. Let $w \in F_S$ be a minimal-length element of $\phi^{-1}(v) \cap \sigma_R^{-1}(g)$ and let $w' \in F_S$ be a minimal-length element of $\sigma_R^{-1}(g)$. By definition, $|g| = l(w')$ and $s(g) \leq l(w)$. It will thus be enough to prove that $l(w) - D \leq l(w')$.

Let $v' = \phi(w')$. We note that $\pi(v') = u = \pi(v)$. It is clear from the definition of M and m that $M(v) \geq m(v)$, so we cannot have both $M(v)$ negative and $m(v)$ positive, and similarly for $M(v')$ and $m(v')$. We may thus assume without loss of generality that $m(v)$ and $m(v')$ are both nonpositive. We will further assume that $M(v)$ and $M(v')$ are both nonnegative; the other cases are easier and are left to the reader.

We want an upper bound on $l(w) - l(w')$. Since w is of minimal length in $\phi^{-1}(v) \cap \sigma_R^{-1}(g)$, we have by Lemma 6.4 that

$$(6.9) \quad l(w) - l(v) = 2[M(v) - m(v)] + \min(|z - M(v)| - M(v), |z - m(v)| + m(v))$$

(since n in the statement of Lemma 6.4 corresponds to $l(v)$ here), and similarly for w' and v' . Thus

$$(6.10) \quad \begin{aligned} [l(w) - l(w')] - [l(v) - l(v')] &= 2[M(v) - M(v')] + 2[m(v') - m(v)] \\ &\quad + \min(|z - M(v)| - M(v), |z - m(v)| + m(v)) \\ &\quad - \min(|z - M(v')| - M(v'), |z - m(v')| + m(v')). \end{aligned}$$

Noting that

$$(6.11) \quad |z - M(v)| - M(v) \geq |z - m(v)| + m(v)$$

iff

$$(6.12) \quad |z - M(v')| - M(v') \geq |z - m(v')| + m(v')$$

iff $z \geq 0$, we find by using the triangle inequality that

$$\begin{aligned}
 (6.13) \quad [l(w) - l(w')] - [l(v) - l(v')] - 2[M(v) - M(v')] - 2[m(v') - m(v)] \\
 \leq \max(|z - M(v)| - |z - M(v')| + M(v') - M(v), \\
 |z - m(v)| - |z - m(v')| + m(v) - m(v')) \\
 \leq \max(2|M(v') - M(v)|, 2|m(v) - m(v')|) \\
 \leq 2|M(v') - M(v)| + 2|m(v) - m(v')|.
 \end{aligned}$$

It follows that

$$\begin{aligned}
 (6.14) \quad [l(w) - l(w')] - [l(v) - l(v')] \\
 \leq 2[M(v) - M(v')] + 2|M(v') - M(v)| + 2[m(v') - m(v)] + 2|m(v) - m(v')| \\
 = 4 \max(M(v) - M(v'), 0) + 4 \max(m(v') - m(v), 0).
 \end{aligned}$$

If $v' = 0$, then $v' = v$, so $w' = w$ and there is nothing to prove. Otherwise, we apply Proposition 6.6 to $z = \beta(u)$, $(p_1, p_2) = \theta(v)$ and $(p'_1, p'_2) = \theta(v')$. We thus get

$$\begin{aligned}
 (6.15) \quad [l(w) - l(w')] - [l(v) - l(v')] \\
 \leq 4 \max(M(v) - M(v'), 0) + 4 \max(m(v') - m(v), 0) \\
 < 4 \max(\log_{|\tau|}[D_1(l(v') - l(v)) + D_2], 0) + 4 \max(\log_{|\tau|}[D_1(l(v') - l(v)) + D_2], 0) \\
 = 8 \log_{|\tau|}[D_1(l(v') - l(v)) + D_2].
 \end{aligned}$$

Rearranging yields that $l(w) - l(w') \leq 8 \log_{|\tau|}[D_1(l(v') - l(v)) + D_2] - (l(v') - l(v))$.

It thus remains to show that the right-hand side of the above inequality is bounded from above. Since v is given to be of minimal length in $\pi^{-1}(u)$, we have $l(v') \geq l(v)$. We thus want to show that $f(x) = 8 \log_{|\tau|}(D_1 x + D_2) - x$ attains an absolute maximum value on the domain $[0, \infty)$. This can be shown by differential calculus. (The absolute maximum value will depend only on R since τ , D_1 and D_2 depend only on R .) We compute $f'(x) = 8D_1/[(D_1 x + D_2) \ln |\tau|] - 1$ and observe that it is a strictly decreasing function on the domain of interest, so (by the first derivative test for absolute maxima), if it has a zero, the absolute maximum of f is attained there. We find that $\lim_{x \rightarrow \infty} f'(x) = -1$ while $f'(0) = 8D_1/(D_2 \ln |\tau|) - 1 > 0$ since we took $D_1 > D_2 \ln |\tau|/8$. Since f' is continuous on $[0, \infty)$, we are done. \square

This concludes the proof of Proposition 6.3. We now need only prove Proposition 6.5, which deals with the geometry of the $|\cdot|$ norm. We want, as mentioned above, to show the existence of a large region of G'_R on which this norm has a coarse maximum well away from the boundary. To do this, we prove the following proposition, which asserts that the geometry of G'_R with respect to S is highly distorted with respect to the geometry induced from \mathbb{Z}^2 . This proof again requires a technical lemma, which will be proven in Section 7.

Proposition 6.7. *Let $G_R = \mathbb{Z}^2 \rtimes_R \langle c \rangle$, where R is a hyperbolic automorphism of \mathbb{Z}^2 . Let T be $|\text{tr } R|$ unless the latter is 1 or 2, in which case let T be 3 or 6, respectively. Let $m \in \mathbb{N}$ and let $z_1, z_2 \in \mathbb{Z}$ be such that $|z_1|, |z_2| < T^m$. Let $\{a, b\}$ be a \mathbb{Z} -basis of G'_R , and let σ_R be the surjection from F_S onto G_R sending the free generators a, b and c of F_S to their namesakes. Thus $z_1 a + z_2 b = z \in G'_R$. Let*

$M = m$ unless $|\text{tr } R|$ is 1 or 2, in which case let $M = 2m$. Then there exists a word $w \in \sigma_R^{-1}(z)$ such that $l(w) \leq T(2^{m+1} - 1) + 4M$.

Proof. It follows from Lemma 7.10 (or Lemma 7.11 if $|\text{tr } R|$ is 1 or 2) that there are $z'_{1i}, z'_{2i} \in \mathbb{Z}$ (where i ranges over the elements of \mathbb{Z}) with $\sum_{i=-\infty}^{\infty} (z'_{1i} + z'_{2i}) \leq T(2^{m+1} - 1)$ such that

$$(6.16) \quad z = \left(\sum_{k=-m}^m z'_{1k} R^k \right) a + \left(\sum_{k=-m}^m z'_{2k} R^k \right) b.$$

Thus there exists $v = \sum_{j=1}^n u_{k_j}^{i_j} \in N_{ab}$ with $\pi(v) = z$ and all $k_j = 1$ or 2 such that all i_j satisfy $-M \leq i_j \leq M$ and $n \leq T(2^{m+1} - 1)$. (Recall that u_1 and u_2 are alternate names for a and b , respectively.) By Lemma 6.4, this gives a $w \in \sigma_R^{-1}(z)$ such that $l(w) \leq T(2^{m+1} - 1) + 4M$, as claimed. \square

We will need some more notation. The eigenvalues of R , τ and $\pm 1/\tau$, correspond to two eigenvectors $\mathbf{v}_e(R)$ and $\mathbf{v}_c(R)$. Since $|\tau| > 1$, these eigenvectors are expanding and contracting respectively. (Clearly, each of them is defined only up to a multiplicative constant.) The line spanned by $\mathbf{v}_e(R)$ will be called the *expanding line* and the line spanned by $\mathbf{v}_c(R)$ the *contracting line*. For any $z \in M_R$, let $d_c(z)$ (respectively $d_e(x)$) be the (Euclidean) distance of z from the contracting (resp. expanding) line.

We can now state

Proposition 6.8. *Let R be a hyperbolic automorphism of \mathbb{Z}^2 , and let A denote \mathbb{Z}^2 equipped with an action by $\mathbb{Z}[t, t^{-1}]$, where t acts by R . Let $\{x, y\}$ be a \mathbb{Z} -basis for A . Then there is $C > 0$ with the following property. Let $z \in A$ and let $p, q \in \mathbb{Z}[t, t^{-1}]$ such that $px + qy = z$ and $\|p\| + \|q\|$ is minimal subject to this condition. Then $d_c(z) < C|\tau|^{M(p,q)}$ and $d_e(z) < C|\tau|^{-m(p,q)}$.*

This follows trivially from Proposition 7.1.

Proof of Proposition 6.5. Note that $\text{tr } R \neq 0$, since R is hyperbolic. Let $T = |\text{tr } R|$ unless the latter is 1 or 2, in which case let T be 3 or 6, respectively. Then $T \geq 3$. Let $M = m$ unless $|\text{tr } R|$ is 1 or 2, in which case let $M = 2m$.

We first construct $B_{m,n}$ for $m, n \in \mathbb{N}$ with m sufficiently large. Recall that β is the correspondence between G'_R and M_R and θ is that between N_{ab} and $\mathbb{Z}[t, t^{-1}]^2$. Let $u \in G'_R$ and set $v \in N_{ab}$ to be a minimal-length element of $\pi^{-1}(u)$. Then, by Proposition 6.8 (setting $(p, q) = \theta(v)$, $x = a$ and $y = b$),

$$(6.17) \quad d_c(\beta(u)) = d_c(pa + qb) < C|\tau|^{M(\theta(v))}$$

and

$$(6.18) \quad d_e(\beta(u)) < C|\tau|^{-m(\theta(v))}$$

where C depends only on R . Then, if we assume

$$(6.19) \quad d_c(\beta(u)) > C|\tau|^n \quad \text{and} \quad d_e(\beta(u)) > C|\tau|^n,$$

this implies that $M(\theta(v)) > n$ and $m(\theta(v)) < -n$, so that $M(v) > n$ and $m(v) < -n$. We let $B_{m,n}$ be the set of $u = ia + jb \in G'_R$ such that $i, j \in \mathbb{Z}$ with $|i|, |j| < T^m$,

$$(6.20) \quad d_c(\beta(u)) > C|\tau|^n \quad \text{and} \quad d_e(\beta(u)) > C|\tau|^n.$$

We proceed with the proof of the rest of the proposition.

Let K and L be positive integers such that

$$(6.21) \quad \frac{L \max(d_c(a), d_c(b), d_e(a), d_e(b)) + C|\tau|^n}{\min(d_c(a), d_e(a))} < K < T^m - L;$$

such K and L clearly exist for sufficiently large m and we can arrange for L to grow proportionally to T^m for R and n fixed. Let $z = Ka$. Addition or subtraction of a or b does not change $d_c(z)$ by more than $\max(d_c(a), d_c(b))$ or $d_e(z)$ by more than $\max(d_e(a), d_e(b))$. Thus any element $z' = z'_1 a + z'_2 b \in G'_R$ at $\{a, b\}$ -distance less than L from z satisfies

$$(6.22) \quad d_c(z') > Kd_c(a) - L \max(d_c(a), d_c(b)) > C|\tau|^n$$

and $d_e(z') > C|\tau|^n$. But z'_1 and z'_2 must then also satisfy $|z'_1|, |z'_2| < K + L < T^m$; so $z' \in B_{m,n}$. But it also follows from Proposition 6.7 that there is $w \in \sigma_R^{-1}(z')$ with $l(w) \leq T(2^{m+1} - 1) + 4M$. Since $|z'| \leq l(w)$, this is the same as saying that $|z'| \leq T(2^{m+1} - 1) + 4M$. (We remind the reader that, for $g \in G$, $|g|$ means the length of g with respect to $S = \{a, b, c\}$.) Letting

$$(6.23) \quad p = p(R, m, n) = \left\lfloor \frac{L}{T(2^{m+1} - 1) + 4M} \right\rfloor - 1,$$

the result now follows from Lemma 3.1 if we take $f(z') = |z'|$. It is straightforward to check that $\lim_{m \rightarrow \infty} p(R, m, n) = \infty$, since $T > 2$. \square

7. SOME RESULTS ABOUT $\mathbb{Z}[t, t^{-1}]$ -MODULES

We first fix some notation. Let $p \in \mathbb{Z}[t, t^{-1}]$. Then either $p = 0$ or p can be expressed uniquely as $\sum_{i=m}^M p_i t^i$, with m, M and all $p_i \in \mathbb{Z}$ and $p_m, p_M \neq 0$. Define $M(p)$ and $m(p)$ to be the M and m in this expression. Thus $M(p)$ and $m(p)$ are the degrees of the highest- and lowest-order nonzero terms of p , respectively. If $p = 0$, then we say $M(p) = -\infty$ (the supremum of the empty set) and $m(p) = \infty$ (the infimum of the empty set). If both p and $q \in \mathbb{Z}[t, t^{-1}]$, then $M(p, q)$ and $m(p, q)$ should be the degrees of the highest- and lowest-order nonzero terms occurring in p or q . Thus, $M(p, q)$ refers to the greater of $M(p)$ and $M(q)$ and $m(p, q)$ to the lesser of $m(p)$ and $m(q)$. Let $\|p\| = \sum_{i=m}^M |p_i|$, the sum of the absolute values of the coefficients.

Now let R be a hyperbolic automorphism of \mathbb{Z}^2 . This induces a $\mathbb{Z}[t, t^{-1}]$ -action on \mathbb{Z}^2 , where t acts by R . We denote \mathbb{Z}^2 with this $\mathbb{Z}[t, t^{-1}]$ -module structure by A . Considered as an automorphism of \mathbb{R}^2 , R has two (distinct) eigenvalues. One of these (which we call τ) has absolute value > 1 , and the other has absolute value < 1 . Thus R determines two 1-dimensional \mathbb{R} -eigenspaces of $A \otimes \mathbb{R}$, corresponding to these two eigenvalues. We call these the *expanding line* and the *contracting line*, respectively.

Let $\{x, y\}$ be a \mathbb{Z} -basis for A . Define functions $d_c, d_e: A \rightarrow [0, \infty)$ taking each point of A to its distance from the contracting and expanding line, respectively. For this purpose, “distance” means distance in the Euclidean norm with respect to the basis $\{x, y\}$.

The following diagrams commute by construction:

$$\begin{array}{ccc} A & \xrightarrow{t \cdot} & A \\ d_c \downarrow & & \downarrow d_c \\ \mathbb{R}_{\geq 0} & \xrightarrow{\cdot|\tau|} & \mathbb{R}_{\geq 0} \end{array}$$

and

$$\begin{array}{ccc} A & \xrightarrow{t^{-1} \cdot} & A \\ d_e \downarrow & & \downarrow d_e \\ R_{\geq 0} & \xrightarrow{\cdot|\tau|} & \mathbb{R}_{\geq 0} \end{array}$$

Many of the results of this section share many hypotheses in common. For the sake of brevity, we state these hypotheses once and for all:

Usual Assumptions. Let R be a hyperbolic automorphism of \mathbb{Z}^2 and p_R its characteristic polynomial. Let $\alpha_R: \mathbb{Z}[t, t^{-1}] \rightarrow \mathbb{Z}[t]/p_R(t)$ be the projection map. Let A denote \mathbb{Z}^2 equipped with an action by $\mathbb{Z}[t, t^{-1}]$, where t acts by R . Let $\{x, y\}$ be a \mathbb{Z} -basis for A . Let τ denote the eigenvalue of R of greater absolute value, and let d_c and d_e refer to distance with respect to $\{x, y\}$ from the contracting and expanding lines for R .

7.1. Beginning of the proof of Proposition 6.6. The principal goal of Section 7 is to prove Proposition 6.6. For the convenience of the reader, we repeat it here.

Proposition 6.6. *Under the usual assumptions, there are $D_2 > 1$ and $D_1 > D_2 \ln |\tau|/8$ with the following property. Let $z \in A$ and let p, q, p' and $q' \in \mathbb{Z}[t, t^{-1}]$ be such that $px + qy = p'x + q'y = z$, with $\|p\| + \|q\|$ minimal subject to this condition and p' and q' not both 0. Then*

$$(7.1) \quad |\tau|^{M(p,q) - M(p',q')} < D_1(\|p'\| + \|q'\| - \|p\| - \|q\|) + D_2$$

and

$$(7.2) \quad |\tau|^{m(p,q) - m(p',q')} < D_1(\|p'\| + \|q'\| - \|p\| - \|q\|) + D_2.$$

To prove this, we assume that $z \in A$ and p, q, p' and $q' \in \mathbb{Z}[t, t^{-1}]$ with $px + qy = p'x + q'y = z$, with $\|p\| + \|q\|$ minimal subject to this condition and $\|p'\| + \|q'\|$ close to minimal. We then need to show that $M(p', q')$ cannot be too much less than $M(p, q)$, and similarly $m(p', q')$ cannot be too much greater than $m(p, q)$. The idea is that $M(p, q)$ and $M(p', q')$ can both be approximated in terms of $d_c(z)$. Similarly, $m(p, q)$ and $m(p', q')$ can both be approximated in terms of $d_e(z)$. The accuracy of these approximations depends only on $R, \{x, y\}$ and (in the case of (p', q')) $\|p'\| + \|q'\| - \|p\| - \|q\|$.

To this end, we first show that $M(p', q')$ can be bounded below (respectively that $m(p', q')$ can be bounded above) based on $\|p'\| + \|q'\| - \|p\| - \|q\|$ and $d_c(z)$ (resp. $d_e(z)$). This bound becomes stricter when $d_c(z)$ or $d_e(z)$ increases. This is the point of Proposition 7.1. We next (in subsection 7.2) show Proposition 7.2, which is the hard part of the proof. It gives us an upper bound on $M(p, q)$ (respectively a lower bound on $m(p, q)$) based on $d_c(z)$ (resp. $d_e(z)$). This bound becomes stricter when $d_c(z)$ or $d_e(z)$ decreases. Proposition 6.6 follows from these two results by comparing the two bounds. We give the statements below.

Proposition 7.1 (lower bound). *Under the usual assumptions, there exist $C_1, C_2 > 0$ with the following property. Let $z \in A$ and let $p, q, p', q' \in \mathbb{Z}[t, t^{-1}]$ be such that $px + qy = p'x + q'y = z$ and $\|p\| + \|q\|$ is minimal subject to this condition. Then*

$$(7.3) \quad d_c(z) \leq |\tau|^{M(p',q')} [C_1(\|p'\| + \|q'\| - \|p\| - \|q\|) + C_2]$$

and

$$(7.4) \quad d_e(z) \leq |\tau|^{-m(p',q')} [C_1(\|p'\| + \|q'\| - \|p\| - \|q\|) + C_2].$$

Proposition 7.2 (upper bound). *Under the usual assumptions, there exists $E > 0$ with the following property. Let $z \in A$ and $p, q \in \mathbb{Z}[t, t^{-1}]$ be such that $px + qy = z$ and $\|p\| + \|q\|$ is minimal subject to this condition. Then $d_c(z) = d_c(px + qy) \geq E|\tau|^{M(p,q)}$ and $d_e(px + qy) \geq E|\tau|^{-m(p,q)}$.*

As advertised, Proposition 6.6 follows straightforwardly from these ingredients.

Proof of Proposition 6.6. The conditions of Propositions 7.2 and 7.1 are clearly satisfied. Thus we have C_1, C_2 and $E > 0$ such that

$$(7.5) \quad E|\tau|^{M(p,q)} \leq d_c(z) \leq |\tau|^{M(p',q')} [C_1(\|p'\| + \|q'\| - \|p\| - \|q\|) + C_2]$$

and

$$(7.6) \quad E|\tau|^{-m(p,q)} \leq d_e(z) \leq |\tau|^{-m(p',q')} [C_1(\|p'\| + \|q'\| - \|p\| - \|q\|) + C_2],$$

where the first inequality in each of the above chains is given by Proposition 7.2 and the second by Proposition 7.1. Note that E, C_1 and C_2 depend only on R and $\{x, y\}$. Since p' and q' are not both 0, neither are p and q , so $|\tau|^{M(p',q')}$ and $|\tau|^{-m(p',q')}$ are neither 0 nor ∞ . Thus we may rearrange the inequalities to get

$$(7.7) \quad E|\tau|^{M(p,q)-M(p',q')} \leq C_1(\|p'\| + \|q'\| - \|p\| - \|q\|) + C_2$$

and

$$(7.8) \quad E|\tau|^{m(p',q')-m(p,q)} \leq C_1(\|p'\| + \|q'\| - \|p\| - \|q\|) + C_2.$$

We may thus take $D_1 = C_1/E$ and $D_2 > C_2/E$. Again, D_1 and D_2 depend only on R and $\{x, y\}$.

If $D_2 \leq 1$, we may clearly increase it without destroying the result. Then, we may similarly increase D_1 to be $> D_2 \ln |\tau|/8$. The proposition is thus proven. \square

To prove Propositions 7.1 and 7.2, we will need some control over the coefficients of the p 's and q 's. This is expressed by the following result.

Lemma 7.3 (coefficient bound). *Under the usual assumptions, there is $D \in \mathbb{N}$ with the following property. Let $p \in \mathbb{Z}[t, t^{-1}]$ and let the $p_i \in \mathbb{Z}$ be such that $p = \sum_{i=-\infty}^{\infty} p_i t^i$. Suppose $\max_{i \in \mathbb{Z}} |p_i| > D$. Then there is $p' \in \alpha_R^{-1}(\alpha_R(p))$ with $\max_{i \in \mathbb{Z}} |p_i| - \max_{i \in \mathbb{Z}} |p'_i| \leq D$ and $\|p'\| < \|p\|$, where the p'_i are defined analogously to the p_i .*

In particular, suppose p is of minimal length in $\alpha_R^{-1}(\alpha_R(p))$. Then

$$(7.9) \quad \max_{i \in \mathbb{Z}} |p_i| \leq D.$$

Proof. Note that, since the eigenvalues of R have different absolute values, $\text{tr } R \neq 0$. We divide the proof of the first paragraph into two cases.

Proof for $|\text{tr } R| > 2$: Let $D = |\text{tr } R|$. Let $n \in \mathbb{Z}$ be such that $|p_n| > D$. Then $\alpha_R(p_R(t)) = \alpha_R(t^2 - (\text{tr } R)t + \det R) = 0$, so adding or subtracting

$$(7.10) \quad t^{n-1}p_R(t) = t^{n+1} - (\text{tr } R)t^n + (\det R)t^{n-1}$$

to or from p yields another element $p' = p \pm t^{n-1}p_R(t)$ with $\alpha_R(p') = \alpha_R(p)$; hence $p' \in \alpha_R^{-1}(\alpha_R(p))$. We choose the sign of $t^{n-1}p_R(t)$ so as to minimize the absolute value of the coefficient of t^n in p' . This choice is unique because of our choice of p_n .

We claim that p' satisfies the conditions imposed in the statement of the lemma. Note that $|\det R| = 1$. Defining the p'_i analogously to the p_i , we see that

$$(7.11) \quad \max_{i \in \mathbb{Z}} |p_i| - \max_{i \in \mathbb{Z}} |p'_i| \leq \max(1, |\text{tr } R|, |\det R|) = \max(1, |\text{tr } R|) = |\text{tr } R|.$$

To see that $\|p'\| < \|p\|$, note that $|p'_n| = |p_n| - |\text{tr } R|$ because of how we chose the sign of $t^{n-1}p_R(t)$. Thus

$$(7.12) \quad \|p'\| \leq \|p\| - |\text{tr } R| + 1 + |\det R| = \|p\| - |\text{tr } R| + 2 < \|p\|,$$

so we are done.

Proof for $|\text{tr } R| = 1$ or 2 : In this case, the last inequality of the above argument fails. We fix this by replacing $t^{n-1}p_R(t)$ with some other multiple of $p_R(t)$. In particular, note that in this case $p_R(t) = t^2 - (\text{tr } R)t - 1$, since R is hyperbolic. Then we use the polynomial $t^{n-2}[t^2 + (\text{tr } R)t - 1][t^2 - (\text{tr } R)t - 1]$. This multiplies out to $t^{n-2}(t^4 - 3t^2 + 1)$ in the case that $|\text{tr } R| = 1$ and to $t^{n-2}(t^4 - 6t^2 + 1)$ in the case that $|\text{tr } R| = 2$. The argument then goes through as in the first case, with $D = 3$ or 6 according to whether $|\text{tr } R|$ is 1 or 2 .

The second paragraph follows trivially. □

We remind the reader that Proposition 7.1 gives a lower bound on $M(p', q')$ (respectively an upper bound on $m(p', q')$) based on how far $\|p'\| + \|q'\|$ is from being minimal over all (p', q') with the same value of $p'x + q'y$ and how far $p'x + q'y$ is from the contracting (resp. expanding) line. Equivalently, it gives an upper bound on $d_c(p'x + q'y)$ (resp. a lower bound on $d_e(p'x + q'y)$) based on how far $\|p'\| + \|q'\|$ is from being minimal (again, over all (p', q') with the same value of $p'x + q'y$) and on $M(p', q')$ (resp. $m(p', q')$). This is a trivial consequence of the following

Lemma 7.4. *Under the usual assumptions, there exist $C_1, C_2 > 0$ with the following property. Suppose $p \in \mathbb{Z}[t, t^{-1}]$ is a minimal-length element of $\alpha_R^{-1}(\alpha_R(p))$. Let $p' \in \mathbb{Z}[t, t^{-1}]$ with $\alpha_R(p) = \alpha_R(p')$. Then, for any $z \in A$,*

$$(7.13) \quad d_c(pz) \leq |\tau|^{M(p')} [C_1(\|p'\| - \|p\|) + C_2] d_c(z)$$

and

$$(7.14) \quad d_e(pz) \leq |\tau|^{-m(p')} [C_1(\|p'\| - \|p\|) + C_2] d_e(z).$$

We prove this lemma by bounding the distance from the expanding and contracting lines of each term of p and adding the bounds.

Proof of Lemma 7.4. Since R is an automorphism of \mathbb{Z}^2 , $|\det R| = 1$, so the other eigenvalue of R (the one other than τ) has absolute value $1/|\tau|$. Thus, we need to

prove only the first statement; the second follows by replacing R with R^{-1} . Also, it suffices to consider the case that $z \neq 0$.

For each $i \in \mathbb{Z}$ let $p'_i \in \mathbb{Z}$ be such that $p' = \sum_{i=-\infty}^{\infty} p'_i t^i$. Let D be as in Lemma 7.3. We claim that

$$(7.15) \quad \max_{i=-\infty}^{\infty} \frac{|p'_i|}{D} \leq \|p'\| - \|p\| + 1.$$

Suppose not. Recall that D depends only on R , not on p' . So then we could apply Lemma 7.3 more than $\|p'\| - \|p\|$ times, shortening p' each time without changing $\alpha_R(p')$. The end result would be some p'' with $\alpha_R(p'') = \alpha_R(p') = \alpha_R(p)$ but $\|p''\| < \|p\|$. This would be a contradiction since p is of minimal length in $\alpha_R^{-1}(\alpha_R(p))$. The claim follows.

Then it follows that, for any z, p and p' satisfying the conditions, we have

$$(7.16) \quad \begin{aligned} \frac{d_c(p'z)}{d_c(z)} &\leq \sum_{i=-\infty}^{\infty} \frac{d_c(p'_i t^i z)}{d_c(z)} = \sum_{i=-\infty}^{\infty} |p'_i| |\tau|^i \\ &\leq \max_{i=-\infty}^{\infty} |p'_i| \sum_{i=0}^{\infty} |\tau|^{M(p')-i} \leq D(\|p'\| - \|p\| + 1) \sum_{i=0}^{\infty} |\tau|^{M(p')-i} \\ &= \frac{D(\|p'\| - \|p\| + 1) |\tau|^{M(p')}}{1 - |\tau|^{-1}}, \end{aligned}$$

where the first equality holds since $d_c(p'_i t^i z) = |p'_i| |\tau|^i d_c(z)$. We are done if we set $C_1 = C_2 = D/(1 - |\tau|^{-1})$. Again, it is clear that $C_1 = C_2 > 0$ and depends only on R . \square

7.2. Proof of the upper bound. In this subsection, we complete the proof of Proposition 6.6 by proving Proposition 7.2, which we repeat for the convenience of the reader.

Proposition 7.2 (upper bound). *Under the usual assumptions, there exists $E > 0$ with the following property. Let $z \in A$ and $p, q \in \mathbb{Z}[t, t^{-1}]$ be such that $px + qy = z$ and $\|p\| + \|q\|$ is minimal subject to this condition. Then $d_c(z) = d_c(px + qy) \geq E|\tau|^{M(p,q)}$ and $d_e(px + qy) \geq E|\tau|^{-m(p,q)}$.*

We will prove only the first clause of the proposition; the proof of the second is analogous.

If $(p, q) \in \mathbb{Z}[t, t^{-1}]^2$, we think of $\|p\| + \|q\|$ as its *length*, and we say that (p, q) represents $px + qy$. In effect, we are considering the infinite set $\{t^i x, t^i y \mid i \in \mathbb{Z}\}$, which generates A as an abelian group. A word (p, q) is *minimal* if $\|p\| + \|q\|$ is minimal over all (p', q') with $p'x + q'y = px + qy$. Then the first clause of Proposition 7.2 states, roughly speaking, that a minimal word $(p, q) \in \mathbb{Z}[t, t^{-1}]^2$ representing an element $z \in A$ cannot have $M(p, q)$ too big compared with $d_c(z)$. This is in some sense a converse to Proposition 7.1, the first clause of which gave a lower bound on $M(p, q)$ compared to the distance from the same line. (Of course, Proposition 7.1 also gave a bound on how fast the lower bound could get worse if we relaxed the requirement that (p, q) be minimal. Proposition 7.2 contains no such bound.)

We define $\text{head}_m(p)$ (for $m \in \mathbb{Z}$ and $p \in \mathbb{Z}[t, t^{-1}]$) to be the sum of all terms of p of degree $\geq m$, and $\text{tail}_m(p)$ to be the sum of all the other terms. Note that,

if (p, q) is minimal, so are $(\text{head}_m(p), \text{head}_m(q))$ and $(\text{tail}_m(p), \text{tail}_m(q))$. Our plan will then be to show (for some m) that $d_c(\text{head}_m(p)x + \text{head}_m(q)y)$ is a definite amount greater than $d_c(\text{tail}_m(p)x + \text{tail}_m(q)y)$. This is expressed in the following

Proposition 7.5. *Under the usual assumptions, there are $C \in \mathbb{N}$ and $n \in \mathbb{Z}$ with the following property. Let $(p, q) \in \mathbb{Z}[t, t^{-1}]^2$ be minimal with p, q not both 0. Let $m = M(p, q) - n$. Then*

$$(7.17) \quad d_c(\text{tail}_m(p)x + \text{tail}_m(q)y) < C(d_c(x) + d_c(y))|\tau|^m$$

and

$$(7.18) \quad d_c(\text{head}_m(p)x + \text{head}_m(q)y) > (C + 1)(d_c(x) + d_c(y))|\tau|^m.$$

Proof of Proposition 7.2 assuming Proposition 7.5. The case that $z = 0$ is trivial, so we assume $z \neq 0$. Thus also p and q are not both 0.

Let C and n be as given in Proposition 7.5. Then, by the triangle inequality,

$$(7.19) \quad d_c(px + qy) > (d_c(x) + d_c(y))|\tau|^m = (d_c(x) + d_c(y))|\tau|^{M(p,q)-n} = E|\tau|^{M(p,q)}$$

if $E = (d_c(x) + d_c(y))|\tau|^{-n}$. This is strictly positive since, as we mentioned before, no nonidentity element of A lies on the expanding or contracting line. Note that, like n , E too is independent of p and q . \square

We will now prove Proposition 7.5. It will follow from two results, Lemma 7.6 and Proposition 7.7. First, Lemma 7.6 will give a C such that, for any $m \in \mathbb{Z}$ and any $(p, q) \in \mathbb{Z}[t, t^{-1}]^2$ minimal,

$$(7.20) \quad d_c(\text{tail}_m(p)x + \text{tail}_m(q)y) < C(d_c(x) + d_c(y))|\tau|^m.$$

(Note that, in the statement of Lemma 7.7, p and q were used to refer to what we here call $\text{tail}_m(p)$ and $\text{tail}_m(q)$, so that $m = M(p, q) + 1$.) It will be proven in much the same way as was Lemma 7.4. The following result, Proposition 7.7, will tell us that, for the same C as before, there exists an $n \in \mathbb{Z}$ such that, for any minimal $(p, q) \in \mathbb{Z}[t, t^{-1}]^2$,

$$(7.21) \quad d_c(\text{head}_{M(p,q)-n}(p)x + \text{head}_{M(p,q)-n}(q)y) > (C + 1)(d_c(x) + d_c(y))|\tau|^{M(p,q)-n}.$$

We will then be done.

Lemma 7.6 (upper bound on tail). *Under the usual assumptions, there is $C \in \mathbb{N}$ with the following property. Let $p, q \in \mathbb{Z}[t, t^{-1}]$ be minimal-length elements of $\alpha_R^{-1}(\alpha_R(p))$ and $\alpha_R^{-1}(\alpha_R(q))$ respectively. Then*

$$(7.22) \quad C(d_c(x) + d_c(y))|\tau|^{M(p,q)+1} > d_c(px + qy).$$

Proof. We claim that, for any $z \in A - \{0\}$,

$$(7.23) \quad d_c(pz)/d_c(z) < C|\tau|^{M(p)+1}$$

and

$$(7.24) \quad d_c(qz)/d_c(z) < C|\tau|^{M(q)+1}$$

for some $C \in \mathbb{N}$ depending only on R . We will then apply this claim to $z = x$ and $z = y$ to prove the lemma. We will show the first inequality; the proof of the other is the same with p replaced by q .

Let $D \in \mathbb{N}$ be as in Lemma 7.3. Let $p_i \in \mathbb{Z}$ be such that $p = \sum_{i=-\infty}^{M(p)} p_i t^i$. Then, by the last sentence of Lemma 7.3, every p_i has absolute value $\leq D$. It follows that

$$(7.25) \quad d_c(pz) = d_c \left(\sum_{i=-\infty}^{M(p)} p_i t^i z \right) \leq \sum_{i=-\infty}^{M(p)} |p_i| d_c(t^i z) \leq \sum_{i=-\infty}^{M(p)} D |\tau|^i d_c(z).$$

Thus

$$(7.26) \quad \frac{d_c(pz)}{d_c(z)} \leq \sum_{i=-\infty}^{M(p)} D |\tau|^i = D \frac{|\tau|^{M(p)+1}}{|\tau| - 1},$$

where the equality is by the formula for the sum of a geometric series. We are done if we take C to be an integer $> D/(|\tau| - 1)$; it is clear that this depends only on R . The claim is proven.

It follows that

$$(7.27) \quad \begin{aligned} d_c(px + qy) &\leq d_c(px) + d_c(qy) \\ &< C(d_c(x)|\tau|^{M(p)+1} + d_c(y)|\tau|^{M(q)+1}) \\ &\leq C(d_c(x) + d_c(y))|\tau|^{M(p,q)+1} \end{aligned}$$

as claimed, where the final inequality is by the definition of $M(p, q)$. □

Proposition 7.7 (lower bound on head). *We make the usual assumptions. Then, for any two positive numbers P and Q , there exists $n \in \mathbb{N}$ with the following property. Let $z \in A - \{0\}$ and let $(p, q) \in \mathbb{Z} [t, t^{-1}]^2$ be minimal with $px + qy = z$. Suppose also that $M(p, q) - m(p, q) \leq n$. Then $(Pd_c(x) + Qd_c(y))|\tau|^{M(p,q)-n} < d_c(z)$.*

We postpone the proof of Proposition 7.7 and instead deduce Proposition 7.5 from it and Lemma 7.6.

Proof of Proposition 7.5. Let C be as in Lemma 7.6. Let n be given by Proposition 7.7 with $P = Q = C + 1$ and let m be $M(p, q) - n$. Note that n is independent of p and q . Then we have

$$(7.28) \quad M(\text{head}_m(p), \text{head}_m(q)) - m(\text{head}_m(p), \text{head}_m(q)) \leq n$$

since $M(\text{head}_m(p), \text{head}_m(q)) = M(p, q)$ and $m(\text{head}_m(p), \text{head}_m(q)) \geq m$ by construction. It then follows from the choice of n that $d_c(\text{head}_m(p)x + \text{head}_m(q)y) > (C + 1)(d_c(x) + d_c(y))|\tau|^{M(p,q)-n}$.

However, $M(\text{tail}_m(p), \text{tail}_m(q)) \leq m - 1$. Also, if (p, q) is minimal, then p and q are of minimal length in $\alpha_R^{-1}(\alpha_R(p))$ and $\alpha_R^{-1}(\alpha_R(q))$, respectively. (We again remind the reader that α_R is the projection from $\mathbb{Z} [t, t^{-1}]$ to $\mathbb{Z}[t]/p_R(t)$.) Thus, by Lemma 7.6, we have

$$(7.29) \quad \begin{aligned} d_c(\text{tail}_m(p)x + \text{tail}_m(q)y) &< C(d_c(x) + d_c(y))|\tau|^m \\ &= C(d_c(x) + d_c(y))|\tau|^{M(p,q)-n}. \end{aligned}$$

□

It remains now (for the proof of Proposition 6.6) to prove Proposition 7.7. This proposition asserts, roughly, that there is n (independent of (p', q') minimal) such that $d_c(\text{head}_{M(p',q')-n}(p')x + \text{head}_{M(p',q')-n}(q')y)$ is a definite fraction bigger than $(d_c(x) + d_c(y))|\tau|^{M(p',q')-n}$. More precisely, suppose that $p = \text{head}_{M(p',q')-n}(p')$

and $q = \text{head}_{M(p',q')-n}(q')$ for some n such that $d_c(px + qy)$ is not much bigger than $(d_c(x) + d_c(y))|\tau|^{M(p',q')-n}$. Then (p, q) is a minimal word with $M(p, q) - m(p, q) \leq n$ and $d_c(px + qy)|\tau|^{n-M(p,q)} \leq C(d_c(x) + d_c(y))$ for some $C \in \mathbb{N}$. We then want to get an upper bound (independent of p and q) for $d_e(px + qy)|\tau|^{M(p,q)-n}$. This will give us an upper bound on $M(p, q) - m(p, q)$, from which Proposition 7.7 will follow.

We will use the following lemma, which tells us that each element of A is represented by only finitely many minimal words in $\mathbb{Z}[t, t^{-1}]^2$.

Lemma 7.8 (Finiteness Lemma). *We make the usual assumptions. Let $z \in A$ and let $P = \{ (p, q) \in \mathbb{Z}[t, t^{-1}]^2 \mid px + qy = z \}$. Then P contains only finitely many minimal elements (p, q) .*

We postpone the proof and instead proceed with proving Proposition 7.7.

Proof of Proposition 7.7. Since $z \neq 0$, $M(p, q) > -\infty$. It will thus suffice for every $P, Q \in \mathbb{N}$ to give $n \in \mathbb{N}$ with the property that, if $(p, q) \in \mathbb{Z}[t, t^{-1}]^2$ is a minimal word such that $M(p, q) = n$ and $m(p, q) \geq 0$, then $Pd_c(x) + Qd_c(y) < d_c(px + qy)$.

To prove this, we will argue that there are only finitely many $z \in A$ which, on the one hand, can be represented by minimal words $px + qy$ such that $m(p, q) \geq 0$ but, on the other hand, have $d_c(z) \leq Pd_c(x) + Qd_c(y)$. We will then apply Proposition 7.8 to show that there are only finitely many such (p, q) for all those z . The proposition will then follow easily.

More precisely, suppose the conclusion does not hold for (p, q) ; that is, suppose that $Pd_c(x) + Qd_c(y) \geq d_c(z)$ where $z = px + qy$. Then applying Proposition 7.1 with $(p', q') = (p, q)$ gives $d_e(z) \leq C_2$, where C_2 depends only on R and $\{x, y\}$. Thus z is a point of \mathbb{Z}^2 constrained to lie within a compact set, since it is confined to the intersection of the width- C_2 band about the expanding line and the width- $Pd_c(x) + Qd_c(y)$ band about the contracting line. Assuming P and Q fixed, there are only finitely many such points z , since \mathbb{Z}^2 is discrete. Thus there are also only finitely many possibilities for $(p, q) \in \mathbb{Z}[t, t^{-1}]^2$ that are minimal words representing such a point z , by Proposition 7.8. Let B be the finite set of all these ordered pairs (p, q) . Let $M = \max \{ M(p, q) \mid (p, q) \in B \}$; this is finite since B is. The result follows by taking $n = M + 1$, greater than the maximal $M(p, q)$. \square

The proof of Proposition 6.6 has now been reduced to that of Lemma 7.8. We will first show that, for any $z \in A$ and any $l \in \mathbb{N} \cup \{0\}$, there is a finite subset $F \subset \mathbb{Z}$ such that any length- l word in $\mathbb{Z}[t, t^{-1}]^2$ representing A contains some term of form ct^i , where $c \in \mathbb{Z}$ and $i \in F$. To be precise, we prove the following

Lemma 7.9. *We make the usual assumptions. Let $z \neq \mathbf{0} \in A$ and $l \in \mathbb{N}$. Then there exists an integer $N = N(R, \{x, y\}, z, l)$ with the following property. Let $p, q \in \mathbb{Z}[t, t^{-1}]$ be such that*

$$(7.30) \quad px + qy = z$$

and $\|p\| + \|q\| \leq l$. Then at least one of p and q must have a nonzero term whose degree (in t) has absolute value less than N .

Proof. We remind the reader that, seen as an automorphism of \mathbb{R}^2 , R has two eigenvalues. One of them, which we call the expanding eigenvalue, has absolute

value > 1 ; the other, the contracting eigenvalue, has absolute value < 1 . Let $\mathbf{v}_e(R), \mathbf{v}_c(R) \in \mathbb{R}^2$ be eigenvectors corresponding to the expanding and contracting eigenvalues respectively. We choose them to have Euclidean norm 1; this will simplify the notation. Let $z_e, z_c \in \mathbb{R}$ be such that, if z is viewed as an element of $A = \mathbb{Z}^2 \subset \mathbb{R}^2$, we have $z = z_e \mathbf{v}_e(R) + z_c \mathbf{v}_c(R)$.

Note that both eigenvalues are irrational. Thus R has no eigenvectors as an automorphism of \mathbb{Z}^2 , so neither the expanding nor the contracting line contains any nonidentity element of A . It follows that neither d_c nor d_e takes any nonidentity element to 0.

Let D be the (Euclidean Hausdorff) distance between $z_c \mathbf{v}_c(R)$ and \mathbb{Z}^2 . We claim that $D > 0$. Suppose not; that is, suppose $z_c \mathbf{v}_c(R) \in \mathbb{Z}^2$. Then $z_e \mathbf{v}_e(R) \in \mathbb{Z}^2$ as well, since $z \in \mathbb{Z}^2$. But, by the preceding paragraph, no eigenvector of R lies in A . It follows that z_c and z_e must both be $\mathbf{0}$, so that $z = \mathbf{0}$, a contradiction; thus the claim is proven.

For any $a \in A$, define a_e and $a_c \in \mathbb{R}$ so that $a = a_e \mathbf{v}_e(R) + a_c \mathbf{v}_c(R)$. Choose $E \in \mathbb{R}$ to be the greatest of $|x_c|, |y_c|, |x_e|$ and $|y_e|$. Let τ be the expanding eigenvalue of R and let $N > \log_{|\tau|}(2El/D)$. If $p \in \mathbb{Z}[t, t^{-1}]$, let $p_{\geq m} \in \mathbb{Z}[t, t^{-1}]$ denote the sum of all terms of p of degree (in t) $\geq m$, and define $p_{\leq m}$ analogously.

Suppose (for a contradiction) that $p = p_{\geq N} + p_{\leq -N}$ and similarly for q . Then

$$(7.31) \quad px + qy = p_{\geq N}x + q_{\geq N}y + p_{\leq -N}x + q_{\leq -N}y.$$

We define $z_{e \geq N} = (p_{\geq N}x + q_{\geq N}y)_e$ and $z_{c \geq N} = (p_{\geq N}x + q_{\geq N}y)_c$, and similarly $z_{e \leq -N}$ and $z_{c \leq -N}$. But, if $i \geq N$, $|(t^i x)_c|$ and $|(t^i y)_c|$ are both $\leq E/|\tau|^N$. For each $i \in \mathbb{Z}$, let a_i and b_i be such that $p = \sum_{i=-\infty}^{\infty} a_i t^i$ and $q = \sum_{i=-\infty}^{\infty} b_i t^i$. Then

$$(7.32) \quad \sum_{i=-\infty}^{\infty} (|a_i| + |b_i|) = \|p\| + \|q\| \leq l.$$

It follows that

$$(7.33) \quad \begin{aligned} |z_{c \geq N}| &= |(p_{\geq N}x + q_{\geq N}y)_c| = \left| \sum_{i=N}^{\infty} [a_i(t^i x)_c + b_i(t^i y)_c] \right| \\ &\leq \frac{E \sum_{i=N}^{\infty} (|a_i| + |b_i|)}{|\tau|^N} \leq \frac{El}{|\tau|^N}. \end{aligned}$$

Similarly, $|z_{e \leq -N}| \leq El/|\tau|^N$.

We know by assumption that

$$(7.34) \quad p_{\leq -N}x + q_{\leq -N}y - z_c \mathbf{v}_c(R) = z_{e \leq -N} \mathbf{v}_e(R) - z_{c \geq N} \mathbf{v}_c(R).$$

But the above implies that this has Euclidean norm

$$(7.35) \quad \leq |z_{e \leq -N}| + |z_{c \geq N}| \leq \frac{2El}{|\tau|^N} < D,$$

where the last inequality is by our choice of N . Since $p_{\leq -N}x + q_{\leq -N}y \in A$, we have that $z_c \mathbf{v}_c(R)$ is within Euclidean distance $< D$ of a point of A . But this contradicts the definition of D . \square

Lemma 7.8 says that every element of A has only finitely many minimal-length preimages in $\mathbb{Z}[t, t^{-1}]^2$. We will deduce this from Lemma 7.9 by induction.

Proof of Lemma 7.8. We remind the reader that P is the set of minimal-length preimages of z in $\mathbb{Z}[t, t^{-1}]^2$. Let $l \in \mathbb{N} \cup \{0\}$ be the length of these minimal-length elements. We will prove the proposition by induction on l . Assume first that $l = 0$. Then the result is trivial, since there is only one length-0 element of $\mathbb{Z}[t, t^{-1}]^2$, namely $(0, 0)$. In what follows we will assume that $l > 0$. It follows that $z \neq 0$.

Each element $(p, q) \in P$ contains some nonzero term whose degree (in t) has absolute value $< N = N(R, \{x, y\}, z, l)$, by Lemma 7.9. Let $(p', q') \in \mathbb{Z}[t, t^{-1}]^2$ be identical to (p, q) except that the coefficient of one such term has its absolute value decreased by 1. Then (p', q') is a length- $(l - 1)$ minimal-length expression for one of the finitely many possibilities $z \pm t^i x$ or $z \pm t^i y$, where $|i| < N$. By the induction hypothesis, there are finitely many such (p', q') for each of these possibilities. But each such (p', q') determines a unique element $(p, q) \in P$. Thus there are finitely many possibilities for (p, q) , so we are done. \square

The proof of Proposition 6.6 is complete.

7.3. Two final lemmas about distortion. To finish the proof of Theorem 1.6, we need to prove two more results, which were used in the proof of Proposition 6.7.

Lemma 7.10. *We make the usual assumptions. Let $m \in \mathbb{N}$ and let r and $s \in \mathbb{Z}$ be such that $|r|, |s| < |\text{tr } R|^m$ and $z = rx + sy$. Then there exist polynomials p and $q \in \mathbb{Z}[t, t^{-1}]$ such that $z = px + qy$, $\|p\| + \|q\| \leq (|\text{tr } R|)(2^{m+1} - 1)$, $M(p), M(q) \leq m$ and $m(p), m(q) \geq -m$.*

We remind the reader that, for $p \in \mathbb{Z}[t, t^{-1}]$, $M(p)$ and $m(p)$ denote the exponents of the highest- and lowest-order terms of p , respectively.

Proof. Since $|r|, |s| < |\text{tr } R|^m$, we can express them in the form

$$(7.36) \quad r = \sum_{i=0}^m r_i (\text{tr } R)^i, \quad s = \sum_{i=0}^m s_i (\text{tr } R)^i,$$

where all the $|r_i|$ and $|s_i| \leq |\text{tr } R|/2$. But, by the Cayley-Hamilton theorem, we have $R^2 - (\text{tr } R)R + (\det R)I = 0$. If we let $\Delta = \det R = \pm 1$, it follows that $(\text{tr } R)I = R + \Delta R^{-1}$, so

$$(7.37) \quad (\text{tr } R)^i I = (R + \Delta R^{-1})^i = R^i (I + \Delta R^{-2})^i = \sum_{j=0}^i \Delta^j \binom{i}{j} R^{i-2j}.$$

Thus

$$(7.38) \quad rI = \sum_{i=0}^m r_i (\text{tr } R)^i I = \sum_{i=0}^m \sum_{j=0}^i \Delta^j r_i \binom{i}{j} R^{i-2j} = p(R),$$

where $p \in \mathbb{Z}[t, t^{-1}]$ is such that

$$(7.39) \quad \begin{aligned} \|p\| &\leq \sum_{i=0}^m \sum_{j=0}^i \left| \Delta^j r_i \binom{i}{j} \right| = \sum_{i=0}^m \sum_{j=0}^i |r_i| \binom{i}{j} \leq \frac{|\text{tr } R|}{2} \sum_{i=0}^m \sum_{j=0}^i \binom{i}{j} \\ &= \frac{|\text{tr } R|}{2} \sum_{i=0}^m 2^i = \frac{|\text{tr } R|(2^{m+1} - 1)}{2}. \end{aligned}$$

Similarly, $sI = q(R)$, where $q \in \mathbb{Z}[t, t^{-1}]$ is such that

$$(7.40) \quad \|q\| \leq \frac{|\operatorname{tr} R|(2^{m+1} - 1)}{2}.$$

We thus have $z = rx + sy = px + qy$, where

$$(7.41) \quad \|p\| + \|q\| \leq |\operatorname{tr} R|(2^{m+1} - 1).$$

□

The result of Lemma 7.10, while true, is not very useful when $|\operatorname{tr} R| = 1$ or 2 , so we also prove the following

Lemma 7.11. *We make the usual assumptions and also require that $|\operatorname{tr} R| = 1$ or 2 . Let $m \in \mathbb{N}$ and let r and $s \in \mathbb{Z}$ be such that $|r|, |s| < (3 \operatorname{tr} R)^m$ and $z = rx + sy$. Then there exist polynomials p and $q \in \mathbb{Z}[t, t^{-1}]$ such that $z = px + qy$, $\|p\| + \|q\| \leq 3|\operatorname{tr} R|(2^{m+1} - 1)$, $M(p), M(q) \leq 2m$ and $m(p), m(q) \geq -2m$.*

Proof. The proof is similar to that of Lemma 7.10; just replace $|\operatorname{tr} R|$ by 3 and 6 , respectively, and the equation $R^2 - (\operatorname{tr} R)R + (\det R)I = 0$ by the equations $R^4 - 3R^2 + I = 0$ and $R^4 - 6R^2 + I = 0$, respectively, according to whether $|\operatorname{tr} R| = 1$ or 2 . These equations hold because, if $|\operatorname{tr} R| \leq 2$, then $\det R = -1$. Then the Cayley-Hamilton theorem says that $R^2 - (\operatorname{tr} R)R - I = 0$, and we need only note that

$$(7.42) \quad R^4 - 3R^2 + I = (R^2 - R - I)(R^2 + R - I)$$

and

$$(7.43) \quad R^4 - 6R^2 + I = (R^2 - 2R - I)(R^2 + 2R - I).$$

□

REFERENCES

- [1] O.V. Bogpolo'skiĭ, *Infinite commensurable hyperbolic groups are bi-Lipschitz equivalent*, Algebra and Logic **36** (1997), no. 3, 155–63. MR1485595 (98h:57002)
- [2] James W. Cannon, *Almost convex groups*, Geom. Dedicata **22** (1987), 197–210. MR877210 (88a:20049)
- [3] Sean Cleary and Tim R. Riley, *A finitely presented group with unbounded dead-end depth*, Proc. Amer. Math. Soc. **134** (2006), no. 2, 343–9. MR2176000 (2006g:20066)
- [4] Sean Cleary and Jennifer Taback, *Dead end words in lamplighter groups and other wreath products*, Q. J. Math. **56** (2005), no. 2, 165–78. MR2143495 (2006h:20055)
- [5] David B.A. Epstein, James W. Cannon, Derek F. Holt, Silvio V.F. Levy, Michael S. Paterson, and William P. Thurston, *Word processing in groups*, Jones and Bartlett, Boston, 1992. MR1161694 (93i:20036)
- [6] Jörg Lehnert, *Some remarks on depth of dead ends in groups*, available from the arXiv at [math.GR/0703636](https://arxiv.org/abs/math/0703636), 2007.
- [7] Tim R. Riley and Andrew D. Warshall, *The unbounded dead-end depth property is not a group invariant*, Internat. J. Algebra Comput. **16** (2006), no. 5, 969–83. MR2274725 (2007h:20040)
- [8] William Thurston, *Three-dimensional geometry and topology*, Princeton Mathematical Series, vol. 35, Princeton University Press, Princeton, 1997. MR1435975 (97m:57016)

DEPARTMENT OF MATHEMATICS, YALE UNIVERSITY, P.O. BOX 208283, NEW HAVEN, CONNECTICUT 06520-8283

E-mail address: andrew.warshall@yale.edu