

© 2022. This manuscript version is made available under the CC-BY-NC-ND 4.0 license
<http://creativecommons.org/licenses/by-nc-nd/4.0/>
The definitive publisher version is available online at <https://doi.org/10.1016/j.tcs.2021.12.022>

Rewriting systems, plain groups, and geodetic graphs [★]

Murray Elder^{a,*}, Adam Piggott^b

^aUniversity of Technology Sydney, Ultimo NSW 2007, Australia

^bAustralian National University, Canberra ACT 0200, Australia

ARTICLE INFO

Keywords:

Length-reducing rewriting system

Plain group

Geodetic graph

ABSTRACT

We take a new step towards an algebraic characterisation of groups presented by length-reducing rewriting systems. We prove that a group is presented by finite convergent length-reducing rewriting systems where each rule has left-hand side of length three if and only if the group is plain.

Our proof rests on proving a new result about embedded circuits in geodetic graphs, whose proof may also be of independent interest to graph theorists.

1. Introduction

The study of rewriting systems connects abstract algebra and theoretical computer science in deep and useful ways. A program of research initiated in the 1980s seeks to characterise algebraically the families of groups that may be presented by various families of rewriting systems (see [13] for a broad introduction). An important part of this program is to characterise the groups that may be presented by length-reducing rewriting systems. Early progress was swift. Diekert [4] (see also [12]) proved that the family of groups admitting presentation by finite convergent length-reducing rewriting systems is properly contained within the family of virtually-free groups; Avenhaus, Madlener and Otto [1] proved that the family of groups admitting presentation by finite convergent length-reducing rewriting systems in which each rule has a left-hand-side of length two is exactly the family of plain groups (a group is *plain* if it is isomorphic to a free product of finitely-many factors, with each factor a finite group or an infinite cyclic group); an explicit construction (described in Section 2.1) shows that any plain group admits presentation by a finite convergent length-reducing rewriting system. From such results the plain groups emerged as the likely family of groups presented by finite convergent length-reducing rewriting systems. In 1987, Madlener and Otto [11] summarised the state of knowledge by highlighting the following two conjectures, the resolution of which would “give a complete algebraic characterisation of groups presented by length-reducing systems”.

Conjecture 1 (Gilman [8]). Let G be a group. Then G admits presentation by a finite convergent length-reducing rewriting system (Σ, T) in which the right-hand side of every rule has length at most one if and only if G is plain.

Conjecture 2 (Madlener and Otto [11]). Let G be a group. Then G admits presentation by a finite convergent length-reducing rewriting system (Σ, T) if and only if G is plain.


Although a special case of Conjecture 2, Gilman’s Conjecture was important enough to consider separately because it seemed more tractable and its resolution may provide clues to the more general problem. The recent positive solution to Gilman’s Conjecture by Eisenberg and the second author [5] motivates the present work. Our main result proves Conjecture 2 in a special case not implied by [5].

Theorem 1. *Let G be a group. Then G admits presentation by a finite convergent length-reducing rewriting system (Σ, T) such that $\Sigma = \Sigma^{-1}$ and the left-hand side of every rule has length at most three if and only if G is plain.*

Our proof is essentially graph theoretic, and exploits the fact that if G and (Σ, T) are as in the theorem, then the undirected Cayley graph $\Gamma = \Gamma(G, \Sigma)$ is geodetic. A simple undirected graph Γ is *geodetic* if between any pair

[★]Research supported by Australian Research Council grant DP210100271.

*Corresponding author

 murray.elder@edu.au (M. Elder); adam.piggott@anu.edu.au (A. Piggott)

 <https://sites.google.com/site/melderau/> (M. Elder); <https://researchers.anu.edu.au/researchers/piggott-a> (A.

Piggott)

ORCID(s): 0000-0002-2438-3945 (M. Elder); 0000-0002-9156-9096 (A. Piggott)

of vertices there exists a unique shortest path. In [14, Problem 3, p.105], Ore posed the problem of giving a general classification of all finite geodetic graphs, but that has proven very difficult. Although planar geodetic graphs have been characterised [20], various structural aspects of geodetic graphs of diameter two and three are understood [15, 16, 18], the geodetic graphs homeomorphic to complete graphs are known [19], and a number of clever procedures have been developed for constructing new geodetic graphs from existing ones (see, for example, [7]), a general classification of geodetic graphs is not close. We prove the following, which is new and may be of independent interest simply because the task of classifying geodetic graphs has proven to be so difficult.

Theorem 2. *If Γ is an undirected simple geodetic graph in which isometrically embedded circuits have length at most five, then all embedded circuits have diameter at most two.*

While Theorem 1 falls well short of resolving Conjecture 2, and Theorem 2 is an incremental contribution to our understanding of geodetic graphs, we think our proof offers insight into the difficulties to be overcome by any argument that takes a primarily graph-theoretic approach to a significant open problem that has defied the efforts of many authors for more than three decades.

2. Definitions

2.1. Rewriting systems

A *rewriting system* is a pair (Σ, T) that formalises the idea of working with products from a set of allowable symbols, using a set of simplifying rules. The set Σ is a nonempty set, called an *alphabet*; its elements are called *letters*. We write Σ^* for the set of all finite words, including the empty word λ , that can be made using letters from the alphabet. For any $w \in \Sigma^*$, we write $|w|$ for the *length* of w ; λ is the unique word of length 0. The second element T is a possibly empty subset of $\Sigma^* \times \Sigma^*$, called a set of *rewriting rules*. The set of rewriting rules determines a relation \rightarrow (read “immediately reduces to”) on the set Σ^* by the following rule: $a \rightarrow b$ if $a = u\ell v$, $b = urv$ and $(\ell, r) \in T$. The reflexive and transitive closure of \rightarrow is denoted $\overset{*}{\rightarrow}$ (read “reduces to”). Thus the rewriting rules specify allowable factor replacements, and $u \overset{*}{\rightarrow} v$ if v can be obtained from u by a sequence of allowable factor replacements. A word $u \in \Sigma^*$ is *irreducible* if no factor of u is the left-hand side of any rewriting rule, and hence $u \overset{*}{\rightarrow} v$ implies that $u = v$.

The reflexive, transitive and symmetric closure of \rightarrow is called “equivalence”, and denoted $\overset{*}{\leftrightarrow}$. The operation of concatenation of representatives is well defined on the set of $\overset{*}{\leftrightarrow}$ -equivalence classes, and hence defines a quotient monoid $M = M(\Sigma, T)$. We say that M is the monoid presented by (Σ, T) . When the equivalence class of every letter (and hence also the equivalence class of every word) has an inverse, the monoid M is a group and we say it is *the group presented by (Σ, T)* .

Example 1. Let $\Sigma = \{a, A\}$ and let $T = \{(aA, \lambda), (Aa, \lambda)\}$. Then (Σ, T) presents a group isomorphic to \mathbb{Z} , the infinite cyclic group.

Example 2. Let G be a finite group, let $\Sigma = G \setminus \{e_G\}$ and let

$$T = \{(gh, k) \mid g, h, k \in \Sigma \text{ and } gh =_G k\} \cup \{(gh, \lambda) \mid g, h \in \Sigma \text{ and } g =_G h^{-1}\}.$$

Then (Σ, T) presents a group isomorphic to G .

A rewriting system (Σ, T) is *finite* if Σ and T are finite sets, *terminating* (or *noetherian*) if there are no infinite sequences of allowable factor replacements, and *length-reducing* if for all $(\ell, r) \in T$ we have that $|\ell| > |r|$. It is clear that length-reducing rewriting systems are terminating. A rewriting system is called *confluent* if for all $w, x, y \in \Sigma^*$, if $w \overset{*}{\rightarrow} x$ and $w \overset{*}{\rightarrow} y$ then there exists $z \in \Sigma^*$ such that $x \overset{*}{\rightarrow} z$ and $y \overset{*}{\rightarrow} z$. A rewriting system is called *convergent* if it is terminating and confluent. The following lemma (see, for example, [2, Theorem 1.13, p.13]) illustrates the utility of convergent rewriting systems.

Lemma 1. *In a convergent rewriting system, rewriting any word in Σ^* until you can rewrite no more is an algorithm for producing the unique irreducible word (the normal form) representing the same element.*

The following simple lemma is provided without proof. The corollary is easily proved by applying the lemma to the rewriting systems exhibited in Examples 1 and 2.

Lemma 2 (Combining rewriting system to present free products). *Suppose that $(\Sigma_1, T_1), \dots, (\Sigma_n, T_n)$ are rewriting systems presenting groups G_1, \dots, G_n respectively and such that the alphabets $\Sigma_1, \dots, \Sigma_n$ are pairwise disjoint. The combined rewriting system $(\bigcup_{i=1}^n \Sigma_i, \bigcup_{i=1}^n T_i)$ presents the free product $G_1 * \dots * G_n$.*

Corollary 1. *If G is a plain group, then G admits presentation by a finite convergent length-reducing rewriting system (Σ, T) where $\Sigma = \Sigma^{-1}$ and the left-hand side of every rule has length equal to two.*

2.2. Graph theory

A simple undirected graph Δ is a pair comprising a nonempty set $V(\Delta)$, the set of *vertices*, and a set of two-element subsets $E(\Delta)$, the set of *edges*. The vertices that form an edge are said to be *adjacent*. All graphs considered in this paper will be simple and undirected. For the remainder of this section, fix a simple undirected graph Δ .

A *path* of length n in Δ from a vertex u to a vertex v is a sequence of vertices $u = u_0, u_1, \dots, u_n = v$ with the property that u_{i-1} and u_i are adjacent for $i = 1, \dots, n$. A path from u and v is called a *geodesic* if there is no shorter path in Δ from u to v . If for each pair (u, v) of distinct vertices in Δ there is at least one path in Δ from u to v , we say that Δ is *connected*; if for each pair (u, v) of distinct vertices in Δ there exists a unique geodesic from u to v , we say that Δ is *geodetic*. If Δ is connected, there is a natural metric d on the vertex set of Δ such that $d(u, v)$ is the length of a shortest path in Δ from u to v .

A *circuit* is a path u_0, u_1, \dots, u_n where $u_0 = u_n$. A *sub-path* of a circuit u_0, u_1, \dots, u_n is either a path u_i, \dots, u_j where $0 \leq i \leq j \leq n$ or a path $u_i, \dots, u_n, u_1, \dots, u_j$ where $1 \leq j \leq i \leq n$. A circuit u_0, u_1, \dots, u_n is *embedded* if the vertices u_0, \dots, u_{n-1} are distinct. An embedded circuit in Δ is *isometrically embedded* if the subgraph comprising the vertices in the circuit and the edges between consecutive vertices is convex in Δ ; that is, $d(u_i, u_j) = \min\{j - i, n + i - j\}$ for all $0 \leq i < j < n$. We will use the acronym IEC for *isometrically embedded circuit*. We note that if u, v are adjacent vertices in Δ , then the path u, v, u is an isometrically embedded circuit of length two. We also note that in a geodetic graph, the unique geodesic joining two vertices of an IEC is a subpath of the IEC.

A vertex v in Δ is a *cut vertex* if Δ is connected, but the graph obtained from Δ by removing v and the edges incident to v is disconnected. A graph is two-connected if it is connected and has no cut vertices. The maximal two-connected subgraphs of a graph Δ are called *blocks*. It follows immediately from the maximality of blocks that any block B in Δ is the subgraph of Δ induced by the vertex set of B . In a connected graph having at least two vertices, each block has at least two vertices. The following well-known characterisation of blocks (see, for example, [14, Theorem 5.4.3, p. 87]) will be useful in this article.

Lemma 3. *Let Δ be a simple undirected graph. Two vertices u, v of Δ lie in the same block if and only if there exists an embedded circuit in Δ that visits both.*

Given a connected graph Δ , the *block-cut tree* $T = T(\Delta)$ is a well-known construction which encodes the block structure of Δ . The graph T has one vertex v_x (of type I) for each vertex x of Δ , and one vertex v_B (of type II) for each block B of Δ ; a type I vertex v_x is adjacent in T to a type II vertex v_B if x is a vertex in the block B . For any connected graph Δ , the block-cut tree $T(\Delta)$ is a tree (a connected graph in which every embedded circuit has length at most two). See for example Figure 1.



Figure 1: Example of a graph and its block-cut tree. Type II vertices are solid black.

2.3. Key lemma and broomlike graphs

The following lemma and its proof are paraphrased from [6, Proposition 6.3].

Lemma 4. *Let Γ be a geodetic graph, and let u_0, u_1, \dots, u_n and u_0, u'_1, \dots, u'_n be equal length geodesics in Γ such that $u_1 \neq u'_1$ and $d(u_n, u'_n) = 1$. Then*

$$u_0, u_1, \dots, u_n, u'_n, \dots, u'_1, u_0$$

is an IEC.

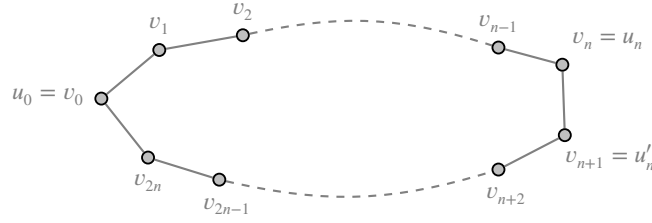


Figure 2: Geodesics in Lemma 4, relabeled as in the proof.

Proof. Since Γ is geodetic and $u_1 \neq u'_1$, the sets $\{u_1, \dots, u_n\}$ and $\{u'_1, \dots, u'_n\}$ are disjoint. It is convenient to relabel the vertices v_0, \dots, v_{2n} so that

$$v_0 = u_0, \dots, v_n = u_n, v_{n+1} = u'_n, \dots, v_{2n} = u'_1.$$

In what follows we shall consider the index i of a vertex v_i modulo $2n + 1$.

Using induction, we shall prove the following statement $S(i)$ for all i : The paths

$$v_i, v_{i+1}, \dots, v_{i+n} \text{ and } v_i, v_{i-1}, \dots, v_{i-n}$$

are geodesics. The result follows immediately.

That $S(0)$ holds is immediate from the hypotheses. Suppose that $S(i)$ holds for some index i . It follows that v_{i+1}, \dots, v_{i+n} is the unique geodesic from v_{i+1} to v_{i+n} , because it is a subpath of the geodesic $v_i, v_{i+1}, \dots, v_{i+n}$. It follows immediately that $d(v_{i+1}, v_{i+n}) = n - 1$.

If $d(v_{i+1}, v_{i+n+1}) < n$, then there is a path of length at most n from v_i to $v_{i+n+1} = v_{i-n}$ through v_{i+1} . This contradicts the fact that $v_i, v_{i-1}, \dots, v_{i-n}$ is the unique geodesic from v_i to v_{i-n} . It follows that $d(v_{i+1}, v_{i+n+1}) \geq n$, from which it follows that $v_{i+1}, v_{i+2}, \dots, v_{i+n+1}$ is the unique geodesic from v_{i+1} to v_{i+n+1} .

If $d(v_{i+1}, v_{i+1-n}) < n$, then there is a path of length at most n from v_{i+1} to $v_{i-n} = v_{i+n+1}$ through v_{i+1-n} . This contradicts the fact, just shown, that $v_{i+1}, v_{i+2}, \dots, v_{i+n+1}$ is the unique geodesic from v_{i+1} to v_{i+n+1} . It follows that $d(v_{i+1}, v_{i+1-n}) \geq n$, from which it follows that $v_{i+1}, v_{i+1-1}, \dots, v_{i+1-n}$ is the unique geodesic from v_{i+1} to v_{i+1-n} . \square

We make the following definition. Our vocabulary borrows from [3].

Definition 1 (*s*-broomlike). Let Δ be a geodetic graph and s a positive integer. We say that Δ is *s*-broomlike if whenever $a_0, \dots, a_{n-1}, a_n, b$ is a path comprising distinct vertices such that a_0, \dots, a_n is a geodesic but a_0, \dots, a_n, b is not, then the geodesic from a_0 to b is $a_0, \dots, a_{n-p}, b_{n-p+1}, \dots, b_n = b$ for $p \leq s$ and $b_{n-p+1} \neq a_{n-p+1}$.

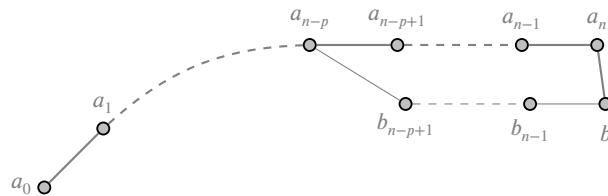


Figure 3: Illustrating the *s*-broomlike property (Definition 1).

Lemma 5. Let Δ be a geodetic graph and s a positive integer. If every IEC in Δ has length at most $2s + 1$, then Δ is *s*-broomlike.

Proof. Let $a_0, \dots, a_{n-1}, a_n, b$ be a path comprising distinct vertices such that $\alpha = a_0, \dots, a_n$ is a geodesic but a_0, \dots, a_n, b is not. Let β be the geodesic from a_0 to b , and let $\tau = a_0, \dots, a_{n-p}$ be the longest prefix shared by α and β , where $0 < p \leq n$. Then $\alpha = \tau\alpha'$ and $\beta = \tau\beta'$ with $\alpha' = a_{n-p}, a_{n-p+1}, \dots, a_n$ and $\beta' = a_{n-p}, b_{n-p+1}, \dots, b$ both geodesics, and $a_{n-p+1} \neq b_{n-p+1}$ for if not we could have made τ longer.

Since Δ is geodetic, $|\alpha'| = |\beta'|$, so $b_n = b$. Then α', β' satisfy the hypothesis of Lemma 4, which means

$$a_{n-p}, a_{n-p+1}, \dots, a_n, b = b_n, b_{n-1}, \dots, b_{n-p+1}, a_{n-p}$$

is an IEC, so its length is bounded by $2s + 1$, which means $|\beta'| = |\alpha'| = p \leq s$. \square

2.4. Cayley graphs

An important and much-studied connection between graph theory and group theory is via the Cayley graph. In this article, we consider the undirected Cayley graph corresponding to a group and a choice of finite generating set. For any group G let e_G denote the identity element.

For a group G and a generating set Σ , the *undirected Cayley graph of G with respect to Σ* is the simple undirected graph $\Gamma = \Gamma(G, \Sigma)$ with vertex set G and in which distinct vertices $g, h \in G$ are adjacent if and only if $g^{-1}h \in \Sigma \cup \Sigma^{-1}$. See for example Figure 4. If Σ is finite then Γ is locally finite. Each path u_0, u_1, \dots, u_n in Γ is labeled by a word $a_1 \dots a_n \in (\Sigma \cup \Sigma^{-1})^*$ where $a_i =_G u_{i-1}^{-1}u_i$. A geodesic path in Γ from e_G to g is a shortest word in $(\Sigma \cup \Sigma^{-1})^*$ spelling the group element g .

Note that by definition if $x \in \Sigma$ and $x =_G e_G$ then x will not appear as the label of any edge in $\Gamma(G, \Sigma)$. Also if $x, y \in \Sigma$ and $x =_G y$ then the unique edge joining adjacent vertices g to gx in $\Gamma(G, \Sigma)$ may be labeled by either x or y .

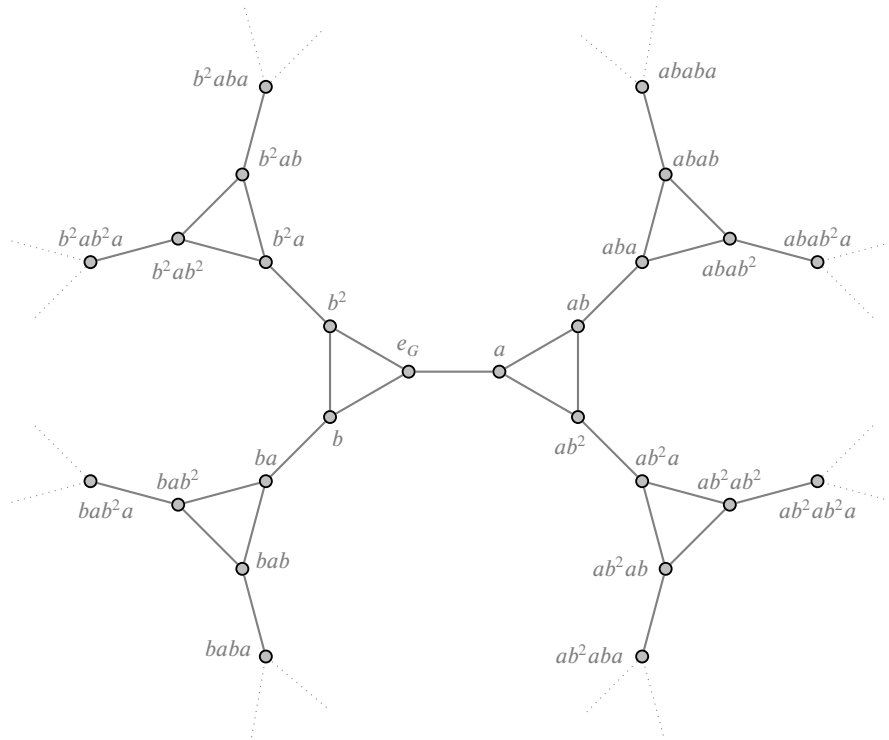


Figure 4: Part of the undirected Cayley graph $\Gamma(G, \{a, b\})$ for $G = C_2 * C_3$ with presentation $\langle a, b \mid a^2 = 1, b^3 = 1 \rangle$.

Remark 1. Note that the undirected Cayley graph for the group $G = C_2 * C_3$ shown in Figure 4 is geodetic, and isometrically embedded circuits have length at most 3. If we consider $G_{2n+1} = C_2 * C_{2n+1}$ with presentation $\langle a, b \mid a^2 = 1, b^{2n+1} = 1 \rangle$ for arbitrarily $n \in \mathbb{N}$, the undirected Cayley graph is geodetic and has isometrically embedded circuits of length at most $2n + 1$. This family of examples shows that geodetic Cayley graphs may contain isometrically

embedded circuits of any (odd) length. By Corollary 1 such groups are presented by finite convergent length-reducing rewriting systems.

3. Embedded circuits in geodetic graphs

In this section we prove Theorem 2. We start with the following lemma.

Lemma 6. *Let Γ be a simple geodetic graph. If ρ is an embedded circuit of diameter exceeding two and that has minimal length among all such embedded circuits in Γ , then ρ contains a geodesic sub-path of length three.*

Proof. Let ρ be an embedded circuit of diameter exceeding two and that has minimal length among all embedded circuits of diameter exceeding two in Γ . Since ρ has diameter at least three, there exist vertices 1 and x visited by ρ such that $d(1, x) = 3$. We choose a basepoint (the vertex 1), an orientation of ρ , and label the vertices visited by ρ in order

$$1, u_1, u_2, \dots, u_m = x = v_n, v_{n-1}, \dots, v_1, 1.$$

For each vertex $w \in \Gamma$, we say that w is in level $d(w, 1)$.

Note that $m, n \geq 3$ since ρ has diameter at least three.

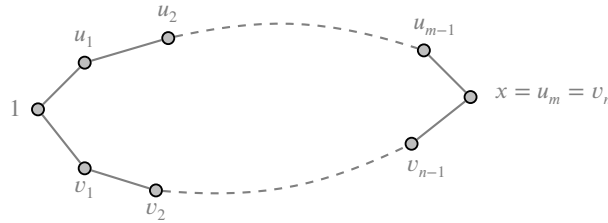


Figure 5: The embedded circuit ρ in Lemma 6.

Claim 1: u_2, v_2 are in level 2.

First we note that, since ρ is an embedded circuit, the vertices $1, \dots, u_{m-1}, v_1, \dots, v_{n-1}, x$ are distinct. Since 1 and u_1 are distinct, u_1 is in level 1. Suppose that u_2 is not in level 2. Then it is either in level 0 or 1, but $u_2 \neq 1$ so it must be in level 1. This implies that u_2 is adjacent to 1, and omitting u_1 from ρ yields a shorter embedded circuit of diameter exceeding two. This contradicts the choice of ρ , and hence proves that u_2 is in level 2.

A symmetric argument shows that v_2 is in level 2.

Since Γ is geodetic, u_1 is the unique level-1 vertex adjacent to u_2 . It follows that u_3 is in level 2 or level 3. Similarly, v_3 is in level 2 or level 3. The result is proved if we can show that u_3 and v_3 cannot both be in level 2.

Claim 2: At least one of u_3, v_3 is in level 3.

Suppose that u_3 and v_3 are both in level 2. Let u'_1 be the unique vertex in level 1 that is adjacent to u_3 ; let v'_1 be the unique vertex in level 1 that is adjacent to v_3 . If ρ does not visit u'_1 , then replacing the subpath $1, u_1, u_2, u_3$ by the path $1, u'_1, u_3$ yields a shorter embedded circuit of diameter at least three, contradicting our choice of ρ . Therefore ρ visits u'_1 . If $u'_1 \neq v_1$, then either $1, v_1, \dots, u'_1, 1$ or $1, u_1, \dots, u'_1, 1$ is an embedded circuit of diameter at least 3, contradicting our choice of ρ . Thus $u'_1 = v_1$. By a symmetric argument, we also have $v'_1 = u_1$, and we are now in the situation shown in Figure 6.

Let ρ' be obtained from ρ by replacing $1, u_1, u_2, u_3$ by $1, v_1, u_3$, and replacing $v_3, v_2, v_1, 1$ by $v_3, u_1, 1$. Since ρ' visits only vertices visited by ρ , and 1 is the only vertex visited twice, we know that ρ' is an embedded circuit which is shorter than ρ . Since the only vertices from ρ omitted were in levels 1 and 2, we know that ρ' still visits a vertex in level 3, and hence it still has diameter at least 3, contradicting our choice of ρ . \square

We will make use of the following fact due to Stemple.

Lemma 7 ([18, Theorem 3.3]). *If a geodetic graph contains an embedded circuit*

$$w_0, w_1, w_2, w_3, w_0$$

of length four, then the induced subgraph on these vertices is a complete graph.

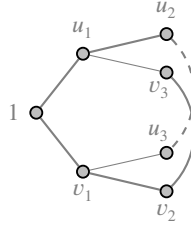


Figure 6: Case $u'_1 = v_1$ and $v'_1 = u_1$ in Lemma 6.

Next we have the following technical result.

Lemma 8. *Let Γ be a geodetic graph in which any IEC has at most five edges. Suppose that ρ is an embedded circuit in Γ of diameter at least three, and ρ has minimal length among all such embedded circuits. Without loss of generality (using Lemma 6), we may label the vertices of ρ such that one traversal of ρ reads*

$$1 = u_0, u_1, \dots, u_m = v_3, v_2, v_1, 1$$

and $1, v_1, v_2, v_3$ is a geodesic subpath. Then $m = 5$, $d(1, u_1) = 1$, $d(1, u_2) = d(1, u_3) = 2$, $d(1, u_4) = 3$ and $d(u_3, v_1) = 1$.

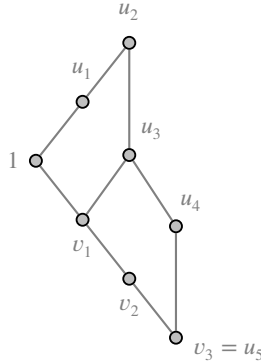


Figure 7: Conclusion of Lemma 8.

Proof. As before, we say that a vertex w is in level $d(w, 1)$. Following the proof of Lemma 6, we have that u_1, v_1 are in level 1, u_2, v_2 are in level 2, and u_3, v_3 are in level 2 or 3 but not both in level 2. We assumed without loss of generality in the hypothesis of this lemma that v_3 that is in level 3.

Claim 1: u_3 is in level 2 and $d(v_1, u_3) = 1$.

Since $1, v_1, v_2, v_3$ is a geodesic and Γ is geodetic, we have $m \geq 4$, and the path $1, u_1, \dots, u_m$ is not a geodesic. So, there exists a unique $i \leq m$ such that $1, u_1, u_2, \dots, u_{i-1}$ is geodesic and $1, u_1, u_2, \dots, u_i$ is not a geodesic. It follows that u_{i-1} and u_i are both in level $i - 1$. Since u_1 is in level 1 and u_2 is in level 2, we know that $i \geq 3$.

By Lemma 5, since $1, u_1, \dots, u_{i-1}$ is geodesic and $1, u_1, \dots, u_{i-1}, u_i$ is not geodesic then by the 2-broomlike property there is either u_{i-2} to u_i are adjacent, or there is a geodesic from u_{i-3} to u_i of length 2. If u_{i-2} and u_i are adjacent, we could omit the vertex u_{i-1} from the path ρ and still have an embedded circuit that visits both 1 and $u_m = v_3$ — a contradiction to our choice of ρ . Thus there is a geodesic from u_{i-3} to u_i of length 2. It follows that there is a vertex $x \neq u_j$ for $0 \leq j \leq i$ such that $1, \dots, u_{i-3}, x, u_i$ is a geodesic. See Figure 8.

Observe that replacing in ρ the subpath $u_{i-3}, u_{i-2}, u_{i-1}, u_i$ with u_{i-3}, x, u_i yields a closed path ρ' that visits both 1 and $u_m = v_3$. The minimality of the length of ρ implies that ρ' is not an embedded circuit; that is, x must be equal to one of the vertices of ρ' . If $x = u_j$ for some $i + 1 \leq j \leq m$, then we can remove a cycle from ρ' and construct a shorter

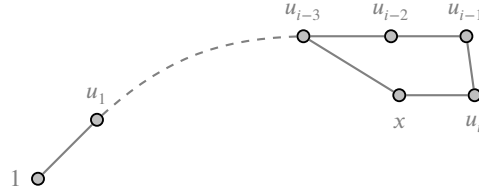


Figure 8: Using the 2-broomlike property in the proof of Claim 1 of Lemma 8.

embedded circuit that visits both 1 and v_3 . It follows that either $x = v_1$ or $x = v_2$. Suppose $x = v_2$. Then x is in level 2 and so $1, u_1, x$ is a geodesic, as is $1, v_1, x$, and since $u_1 \neq v_1$ we contradict that Γ is geodetic. Hence we have that $x = v_1$. This means that $i = 3$ and u_3 is in level 2, and $d(v_1, u_3) = 1$, as required.

Claim 2: $m \geq 5$.

We know that $m \geq 4$. If $m = 4$ then v_1, u_3, u_4 and v_1, v_2, v_3 are two different geodesics between the same endpoints, contradicting geodeticity. Thus $m \geq 5$.

Claim 3: u_4 is in level 3.

Since Γ is geodetic, v_1 is the only vertex in level 1 that is adjacent to u_3 . Since $m \geq 4$ and $u_4 \neq v_1$ (because ρ is an embedded circuit), we have that u_4 is in level 2 or level 3. Suppose that u_4 is in level 2, and let p denote the unique vertex in level 1 that is adjacent to u_4 .

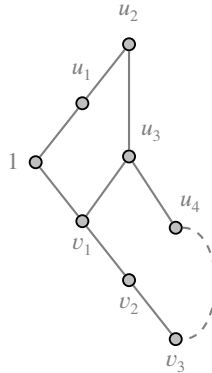


Figure 9: Claim 3 in the proof of Lemma 8: assume u_4 is in level 2.

Now either p is a vertex of ρ , or not. If it does not lie on ρ then we can replace the subpath $1, u_1, u_2, u_3, u_4$ by $1, p, u_4$ and obtain a shorter embedded circuit which visits 1 and v_3 , contradicting the minimality of ρ .

Therefore p is a vertex of ρ .

Case 1: $p = v_1$.

The path $1, u_1, u_2, u_3, u_4, v_1, 1$ is an embedded circuit of length 6. Call this path τ . Since u_1, u_4 are distinct we have $1 \leq d(u_1, u_4) \leq 3$. The paths u_1, u_2, u_3, u_4 and $u_1, 1, v_1, u_4$ are both length 3, so $d(u_1, u_4) \neq 3$ or the graph is not geodetic. If $d(u_1, u_4) = 1$ then we can replace in ρ the path u_1, u_2, u_3, u_4 by u_1, u_4 and find a shorter embedded circuit of diameter exceeding 2. Thus $d(u_1, u_4) = 2$.

It follows that there must be a vertex t that is not visited by τ and is adjacent to both u_1 and u_4 . Since t does not lie on τ , $t \neq v_1$, and since u_4 is in level 2, t is in level 2 (if it were in level 1 we would have two geodesics to u_4 contradicting geodeticity). Since t is adjacent to u_1 and $v_1 \neq u_1$, if $t = v_2$ we would have two geodesics to v_2 , thus $t \neq v_2$. It follows that by replacing in ρ the subpath $1, u_1, u_2, u_3, u_4$ by the path $1, u_1, t, u_4$, and removing a subpath that is a cycle if necessary, we may construct a shorter embedded circuit that visits both 1 and v_3 . This contradiction proves that this case is impossible.

Case 2: $p = u_1$.

Omitting u_2 and u_3 from ρ would yield a shorter embedded circuit that still visits 1 and v_3 . This contradiction proves

that this case is impossible.

Case 3: $u_1 \neq p \neq v_1$.

In this case $p = u_j$ for $5 \leq j < m$ since v_1, v_2, v_3 are all spoken for (only v_1 is in level 1).

Then the path $1, p = u_j, u_{j+1}, \dots, u_m = v_3, v_2, v_1, 1$ is an embedded circuit passing 1 and v_3 so has diameter 3 and is shorter than ρ , a contradiction.

Since all cases are impossible, we conclude that u_4 is not at level 2. Hence u_4 is at level 3.

Claim 4: u_5 is at level 3.

Since u_3 is the unique vertex in level 2 adjacent to u_4 , and $u_5 \neq u_3$, we have that u_5 is not in level 2.

Suppose that u_5 is in level 4, and so $\alpha = 1, v_1, u_3, u_4, u_5$ is a geodesic. Since α is geodesic and $1, v_1, u_3, u_4, u_5, \dots, u_m$ is not a geodesic, there exists a unique integer $i \geq 5$ so that $1, v_1, u_3, u_4, u_5, \dots, u_i$ is geodesic and $1, v_1, u_3, u_4, u_5, \dots, u_i, u_{i+1}$ is not geodesic, and u_i and u_{i+1} are both in level $i - 1$.

If u_{i-1}, u_i, u_{i+1} is not geodesic, omitting u_i from ρ gives a shorter isometrically embedded circuit visiting 1 and v_3 , contradiction. So u_{i-1}, u_i, u_{i+1} is geodesic. By Lemma 5, we must have $u_{i-2}, u_{i-1}, u_i, u_{i+1}$ is not geodesic and there is a geodesic path u_{i-2}, z, u_{i+1} where $u_{i-2} \neq z \neq u_{i-1}$.

Note that by construction z is in level $i - 2 \geq 3$, so z cannot equal v_1, v_2 .

If $z = v_3 = u_m$ then $1, u_1, \dots, u_{i-2}, z, v_2, v_1, 1$ is a shorter isometrically embedded circuit that visits 1 and v_3 , a contradiction. Also note that $z \neq u_6$ since $i \geq 5$ and $u_{i+1} \neq z$.

It follows that if $z = u_j$ then $6 < j \leq m - 1$, and replacing the subpath $u_{i-2}, u_{i-1}, u_i, u_{i+1}$ by u_{i-2}, z, u_{i+1} and possibly removing a cycle, we get a shorter embedded circuit than ρ that visits 1 and $v_3 = u_m$.

This shows that z is not a vertex of ρ . Then replacing $u_{i-2}, u_{i-1}, u_i, u_{i+1}$ by u_{i-2}, z, u_{i+1} again gives a shorter embedded circuit than ρ that visits 1 and v_3 .

This contradiction proves that u_5 is in level 3.

Claim 5: $m = 5$.

We note that u_5 is not adjacent to u_2 or u_3 , otherwise we could omit u_3, u_4 or u_4 respectively from ρ and have a shorter embedded circuit that visits both 1 and v_3 . Since u_5 is in level 3, we have v_1, u_3, u_4 is a geodesic and v_1, u_3, u_4, u_5 is not geodesic, and u_3, u_5 is not an edge so Lemma 5 implies there exists a vertex q adjacent to both v_1 and u_5 such that $u_2 \neq q \neq u_3$. Therefore $1, u_1, u_2, u_3, u_4, u_5, q, v_1, 1$ is an embedded circuit visiting 1 and a vertex at level 3, so by the minimality of ρ we must have $q = v_2$ and $u_5 = v_3$. \square

We can now prove Theorem 2.

Proof of Theorem 2. Suppose that there exists in Γ an embedded circuit of diameter exceeding two. By Lemma 8, there exists an embedded circuit ρ labeled

$$1, u_1, u_2, u_3, u_4, v_3, v_2, v_1, 1$$

with u_1 at level 1, u_2, u_3 at level 2, u_4 at level 3 and $d(u_3, v_1) = 1$, and $1, v_1, v_2, v_3$ is geodesic, as illustrated in Figure 7. Let ρ' be the embedded circuit that begins at v_3 and visits the same vertices as ρ , but in reverse order. That is, ρ' visits vertices in the following order

$$v_3, u_4, u_3, u_2, u_1, 1, v_1, v_2, v_3.$$

Now ρ' is also a minimal length embedded circuit with diameter exceeding two, so Lemma 8 applies to ρ' as well (with u_2 playing the role of u_3 and v_2 the role of v_1), which gives that $d(u_2, v_2) = 1$.

It follows that u_2, v_2, v_1, u_3, u_2 is an embedded circuit of length 4. By Lemma 7, we must have that u_2 and v_1 are adjacent. This contradicts the fact that u_1 is the unique level-1 vertex adjacent to u_2 . This contradiction proves that there are no embedded circuits in Γ with diameter exceeding two. \square

4. Plain groups, blocks and embedded circuits

Bass-Serre theory [10, 17] tells us that a group G is plain if and only if G acts on a locally-finite tree, with a compact quotient, finite vertex stabilisers, trivial edges stabilisers and no edge inversions. See for example [17, Theorem 13].

Another useful characterisation of plain groups then follows from the block-cut tree associated to the graph, described in Section 2.2.

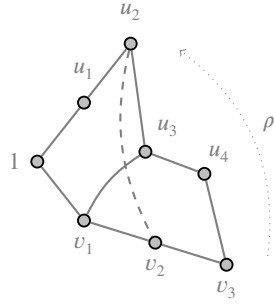


Figure 10: The path ρ' which starts at v_3 and runs in the reverse direction to ρ in the proof of Theorem 2.

For a finite set of vertices S in a graph Γ , the diameter of S is the maximum distance in Γ between any pair of vertices in S . Haring-Smith [9] proved the following result in 1983. We provide a short proof that uses Bass-Serre theory and the block-cut tree.

Theorem 3 (A characterisation of plain groups). *For a group G and a positive integer s , the following are equivalent:*

1. G admits a finite generating set Σ such that, in the associated undirected Cayley graph $\Gamma(G, \Sigma)$, the diameter of any embedded circuit is at most s .
2. G admits a finite generating set Σ such that, in the associated undirected Cayley graph $\Gamma(G, \Sigma)$, the diameter of any block is at most s .
3. G is a plain group.

Proof. 1. \Leftrightarrow 2.: Follows immediately from Lemma 3.

3. \Rightarrow 2.: Suppose that G is a plain group. Then G is a free product of m finite groups G_1, \dots, G_m and n copies of the infinite cyclic group C_1, \dots, C_n . Let Σ be a set comprising each nontrivial element of each finite factor G_i , and one generator a_i and its inverse A_i for each infinite cyclic factor C_i . In the Cayley graph $\Gamma = \Gamma(G, \Sigma)$, the only blocks containing the identity element e_G are the subgraphs induced by $\Gamma(G_i, G_i \setminus \{e_{G_i}\})$ for $1 \leq i \leq m$ (and these are complete graphs), and subgraphs induced by (e_G, a_i) for $1 \leq i \leq n$. Thus all blocks containing e_G have diameter 1. Since Γ is vertex-transitive, all blocks in Γ have diameter one (and hence all blocks in Γ have diameter at most s).

2. \Rightarrow 3.: Suppose that G admits a finite generating set Σ such that in the associated Cayley graph $\Gamma = \Gamma(G, \Sigma)$ all blocks have diameter at most s . Let T denote the block-cut tree of Γ , as described in Section 2.2. The natural left-action of G on Γ induces a left-action of G on T . Since the action of G on Γ is vertex transitive, the action of G on T is transitive on the set of type I vertices and there are finitely many orbits of type II vertices. It follows that the action of G on T is cocompact. In the action of G on Γ , vertices have trivial stabilisers. It follows that in the action of G on T , type I vertices have trivial stabilisers, type II vertices have finite stabilisers (because blocks in Γ comprise finitely many vertices), edges are not inverted (each edge includes a type I and type II vertex which cannot be interchanged) and edge stabilisers are trivial. Since G acts on T , a locally-finite tree, with finite vertex stabilisers, trivial edges stabilisers and no edge inversions, by [17, Theorem 13] G is a plain group. \square

If a rewriting system (Σ, T) presents a group G , then properties of the rewriting system determine properties of the Cayley graph $\Gamma = \Gamma(G, \Sigma)$.

Lemma 9. *Let (Σ, T) be a finite convergent length-reducing rewriting system such that $\Sigma = \Sigma^{-1}$ and (Σ, T) presents a group G . Let Γ denote the undirected Cayley graph of Γ with respect to Σ . Then*

1. Γ is geodetic;
2. If $u_0, u_1, \dots, u_{m-1}, u_m = u_0$ is an IEC in Γ of length $m > 2$, then $m = 2n + 1$ for some positive integer n and $(x_1 \dots x_{n+1}, x_m^{-1} \dots x_{n+2}^{-1}) \in T$ where $x_i =_G u_{i-1}^{-1} u_i \in \Sigma$ for $1 \leq i \leq m$.

Proof. If u_0, \dots, u_n and v_0, \dots, v_n are two geodesics in $\Gamma(G, \Sigma)$ with $u_0 = v_0, u_n = v_n$, then the words

$$u = (u_0^{-1} u_1) \dots (u_{n-1}^{-1} u_n) \in \Sigma^* \quad \text{and} \quad v = (v_0^{-1} v_1) \dots (v_{n-1}^{-1} v_n) \in \Sigma^*$$

are irreducible words representing the same group element. By Lemma 1, $u = v$, which establishes the first claim.

If $u_0, u_1, \dots, u_{m-1}, u_m = u_0$ is an IEC in Γ of length $m > 2$, set $x_i =_G u_{i-1}^{-1} u_i \in \Sigma$ for $1 \leq i \leq m$. If $m = 2n$ then u_0, \dots, u_n and u_0, u_{m-1}, \dots, u_n are two geodesics for the same element, and since the circuit is embedded and $m > 2$, so $n > 1$, we have $u_1 \neq u_{m-1}$, so a, b are distinct words, which contradicts the first claim. Thus $m = 2n + 1$.

Now let $a = x_1 \dots x_{n+1}$ and $b = x_m^{-1} \dots x_{n+2}^{-1}$. Then $a =_G b$. The word b is geodesic since it is a subpath of length n of an IEC of length $2n + 1$. The word a is not geodesic so some rewrite rule must apply. We have $a = u\ell v$ with $(\ell, r) \in T$, $|r| < |\ell|$ and $a =_G urv$. If $|u| + |v| > 0$, then ℓ is geodesic since it is a subpath of length at most n of an IEC of length $2n + 1$. Then $\ell \neq_G r$ for any $r \in \Sigma^*$ with $|r| < |\ell|$. Hence $u = v = \lambda$ and $a = \ell$. But then $r = b$ because b , being geodesic and shorter than a by one letter, is the unique word r with $|r| < |a|$ and $r =_G a$. \square

We are now ready to prove the main theorem.

Proof of Theorem 1. Corollary 1 gives one direction.

Suppose that G admits presentation by a finite convergent length-reducing rewriting system (Σ, T) such that $\Sigma = \Sigma^{-1}$ and the left-hand side of every rule has length at most three. Let Γ be the undirected Cayley graph of G with respect to Σ . By Lemma 9, Γ is geodetic and IECs have length at most five. Since Γ satisfies the hypotheses of Theorem 2, all embedded circuits in Γ have diameter at most two. By Theorem 3, G is plain. \square

Acknowledgments

Research supported by Australian Research Council grant DP210100271. The authors thank the anonymous reviewer for helpful feedback and corrections.

References

- [1] Avenhaus, J., Madlener, K., Otto, F., 1986. Groups presented by finite two-monadic Church-Rosser Thue systems. *Trans. Amer. Math. Soc.* 297, 427–443. doi:10.2307/2000531.
- [2] Book, R.V., Otto, F., 1993. String-rewriting systems. *Texts and Monographs in Computer Science*, Springer-Verlag, New York. doi:10.1007/978-1-4613-9771-7.
- [3] Bridson, M.R., Gilman, R.H., 1993. A remark about combings of groups. *Internat. J. Algebra Comput.* 3, 575–581. doi:10.1142/S0218196793000329.
- [4] Diekert, V., 1987. Some remarks on presentations by finite Church-Rosser Thue systems, in: *STACS 87 (Passau, 1987)*. Springer, Berlin. volume 247 of *Lecture Notes in Comput. Sci.*, pp. 272–285. doi:10.1007/BFb0039612.
- [5] Eisenberg, A., Piggott, A., 2019. Gilman’s conjecture. *J. Algebra* 517, 167–185. doi:10.1016/j.jalgebra.2018.09.022.
- [6] Elvey Price, A., 2014. Geodesics in Cayley graphs. Master’s thesis. University of Melbourne.
- [7] Frasser, C.E., Vostrov, G., 2016. Geodetic graphs homeomorphic to a given geodetic graph. *ArXiv abs/1611.01873*.
- [8] Gilman, R.H., 1984. Computations with rational subsets of confluent groups, in: *EUROSAM 84 (Cambridge, 1984)*. Springer, Berlin. volume 174 of *Lecture Notes in Comput. Sci.*, pp. 207–212. doi:10.1007/BFb0032843.
- [9] Haring-Smith, R.H., 1983. Groups and simple languages. *Trans. Amer. Math. Soc.* 279, 337–356. doi:10.2307/1999388.
- [10] Karrass, A., Pietrowski, A., Solitar, D., 1973. Finite and infinite cyclic extensions of free groups. *J. Austral. Math. Soc.* 16, 458–466. Collection of articles dedicated to the memory of Hanna Neumann, IV.
- [11] Madlener, K., Otto, F., 1987. Groups presented by certain classes of finite length-reducing string-rewriting systems, in: *Rewriting techniques and applications (Bordeaux, 1987)*. Springer, Berlin. volume 256 of *Lecture Notes in Comput. Sci.*, pp. 133–144. doi:10.1007/3-540-17220-3-12.
- [12] Madlener, K., Otto, F., 1988. Commutativity in groups presented by finite Church-Rosser Thue systems. *RAIRO Inform. Théor. Appl.* 22, 93–111.
- [13] Madlener, K., Otto, F., 1989. About the descriptive power of certain classes of finite string-rewriting systems. *Theoret. Comput. Sci.* 67, 143–172. doi:10.1016/0304-3975(89)90002-9.
- [14] Ore, O., 1962. *Theory of graphs*. American Mathematical Society Colloquium Publications, Vol. XXXVIII, American Mathematical Society, Providence, R.I.
- [15] Parthasarathy, K.R., Srinivasan, N., 1984. Geodetic blocks of diameter three. *Combinatorica* 4, 197–206. doi:10.1007/BF02579221.
- [16] Scapellato, R., 1986. Geodetic graphs of diameter two and some related structures. *J. Combin. Theory Ser. B* 41, 218–229. doi:10.1016/0095-8956(86)90045-6.
- [17] Serre, J.P., 2003. *Trees*. Springer Monographs in Mathematics, Springer-Verlag, Berlin. Translated from the French original by John Stillwell, Corrected 2nd printing of the 1980 English translation.
- [18] Stemple, J.G., 1974. Geodetic graphs of diameter two. *J. Combinatorial Theory Ser. B* 17, 266–280. doi:10.1016/0095-8956(74)90033-1.
- [19] Stemple, J.G., 1979. Geodetic graphs homeomorphic to a complete graph, in: *Second International Conference on Combinatorial Mathematics (New York, 1978)*. New York Acad. Sci., New York. volume 319 of *Ann. New York Acad. Sci.*, pp. 512–517.
- [20] Stemple, J.G., Watkins, M.E., 1968. On planar geodetic graphs. *J. Combinatorial Theory* 4, 101–117.