ON STALLINGS' UNIQUE FACTORIZATION GROUPS

DONALD I. CARTWRIGHT AND BERNHARD KRÖN

School of Mathematics and Statistics,
The University of Sydney, NSW 2006
Australia

E-mail: donaldc@maths.usyd.edu.au, bernhard@maths.usyd.edu.au

July 14, 2005

Abstract. Let Γ be a group and Σ a symmetric generating set for Γ. In [8], Stallings called Γ a *unique factorization group* if each group element may be written in a unique way as a product $a_1 \dots a_m$, where $a_i \in \Sigma$ for each i and $a_i a_{i+1} \notin \Sigma \cup \{1\}$ for each $i < m$. In this paper we give a complete combinatorial proof of a theorem, not explicitly stated in [8], characterizing all such pairs (Γ, Σ). We also characterize the unique factorization pairs by a certain tree-like property of their Cayley graphs.

1. Introduction

Let Γ be a group and Σ a generating set for Γ. We always assume that Σ is symmetric ($\Sigma^{-1} = \Sigma$) and that $1 \notin \Sigma$. We do not assume that Σ is finite. Let Σ^* denote the set of all words over Σ. We write $(a_1, \dots, a_m)$ for a word, and $a_1 \dots a_m$ for the group element this word represents. The empty word represents 1. Let L_Σ denote the set of the words $(a_1, \dots, a_m) \in \Sigma^*$ in which $a_i a_{i+1} \notin \Sigma \cup \{1\}$ for all $i < m$ (together with the empty word). Given $g \in \Gamma$, any word in Σ^* of minimal length representing g is in L_Σ. Modifying [8] slightly, we call the (Γ, Σ) a *unique factorization pair* if for each $g \in \Gamma$ there is only one word in L_Σ which represents g. Equivalently:

Definition 1. The pair (Γ, Σ) is called a *unique factorization pair* if the map $(a_1, \dots, a_m) \mapsto a_1 \dots a_m$ is a bijection $L_\Sigma \to \Gamma$.

One goal of this paper is to describe (in Theorem 1 below), up to isomorphism, all possible groups Γ and all possible generating sets Σ on a given group Γ such that (Γ, Σ) is a unique factorization pair. The relevant notion of isomorphism here is the obvious one: (Γ_1, Σ_1) and (Γ_2, Σ_2) are *isomorphic* if there is a group isomorphism $f : \Gamma_1 \to \Gamma_2$ such that $f(\Sigma_1) = \Sigma_2$.

A second goal is to characterize (in Theorem 2 below) the Cayley graphs of unique factorization pairs in terms of a "tree-like" property they have.

We start by listing some examples of unique factorization pairs (Γ, Σ). We shall check that Examples 2 and 3 are unique factorization pairs in Lemma 2.6 below.

Example 1. Let G be a group. Then $(G, G \setminus \{1\})$ is a unique factorization pair.

2000 *Mathematics Subject Classification.* 20F05 (20E06 05C25).

Key words and phrases. unique factorization group, automatic group, Cayley graph, free group, free product, plain group.

Bernhard Krön was supported by projects J2245 and P16004-N05 of the Austrian Science Fund (FWF) .

Example 2. Let F be a free group, with free generators y_k, $k \in K$, for some set K. Write $y_0 = 1$. Let Σ consist of the elements $y_k^{-1} y_\ell$, where $k, \ell \in K \cup \{0\}$, $k \neq \ell$. Then it is not hard to show that (F, Σ) is a unique factorization pair by appealing to the fact that (F, Σ_0) is a unique factorization pair, where $\Sigma_0 = \{y_k^{\pm 1} : k \in K\}$.

Example 3. Let G be a group, and let F be as in Example 2. Let Σ denote the set of elements in the free product $G * F$, other than 1, of the form $y_k^{-1} g y_\ell$, where $g \in G$ and $k, \ell \in K \cup \{0\}$. Then $(G * F, \Sigma)$ is a unique factorization pair (see Lemma 2.6). Examples 1 and 2 are the special cases $K = \emptyset$ and $G = \{1\}$, respectively, of this example.

Example 4. Let (Γ_j, Σ_j), $j \in J$, be a family of unique factorization pairs. Let Γ denote the free product of the Γ_j's, and let Σ denote the union of the sets Σ_j. Then (Γ, Σ) is a unique factorization pair. We shall write $(\Gamma, \Sigma) = *_{j \in J}(\Gamma_j, \Sigma_j)$.

Theorem 1. *Let (Γ, Σ) be any unique factorization pair. Then (Γ, Σ) is isomorphic to a free product $*_{j \in J}(\Gamma_j, \Sigma_j)$, where each (Γ_j, Σ_j) is as in Example 3.*

Stallings' paper [8] is mostly concerned with "partial groups" and their "universal groups". It concludes with a terse discussion of the structure of these partial groups, with only a brief proof sketch. From this discussion, using universal groups it is not a large step to arrive at our Theorem 1, though this is not done in [8]. We feel that the result is of sufficient interest to warrant a clear statement and the complete proof we present in Section 2, particularly as there has been renewed interest in these groups amongst people studying random walks on groups; Mairesse and Mathéus [5, 6] were able to perform very explicit calculations concerning random walks on these groups in which the transitions are of the form $g \mapsto ga$ ($g \in \Gamma, a \in \Sigma$). Our proof uses several of the ideas indicated by Stallings [8], but takes a more direct combinatorial group theory approach, rather than using the methods of partial groups and their universal groups.

It follows from Theorem 1 that if (Γ, Σ) is a unique factorization pair and Σ is finite, then Γ is *plain*, that is, a free product $G_1 * \cdots * G_s * F_r$ of finitely many finite groups $G_1, \ldots, G_s$ and a free group F_r (where $r, s \geq 0$). This much had been deduced from Stallings' results and written down explicitly by Haring-Smith [4], and used by him and others subsequently (e.g., [1, 2]). But Theorem 1 provides more, giving precise information about the generating set Σ. In particular, for each plain group Γ, there are, up to isomorphism, only finitely many generating sets Σ for which (Γ, Σ) is a unique factorization pair.

Example 5. Let $r \geq 1$, and let F_r denote the free group on r free generators. Given any integers $r_1 \geq \cdots \geq r_k \geq 1$ such that $r_1 + \cdots + r_k = r$, for $j = 1, \ldots, k$, let Σ_{r_j} be the generating set on F_{r_j} described in Example 2. Form $*_{j=1}^{k}(F_{r_j}, \Sigma_{r_j})$, in the notation of Example 4. By Example 4, this gives a unique factorization pair (F_r, Σ). By Theorem 1, any generating set Σ on the free group F_r such that (F_r, Σ) is a unique factorization pair is of this type. Since the numbers r_k are the sizes of the equivalence classes $[a]$ (see Lemmas 2.3 and 2.6 below), distinct partitions correspond to non-isomorphic unique factorization pairs. So up to isomorphism, the number of distinct Σ's on F_r is the number of distinct partitions of r. The usual generating set of F_r (i.e., a set of free generators and their inverses) corresponds to the partition $1 + \cdots + 1$ of r.

Recall that the *Cayley graph* $\mathrm{Cay}(\Gamma, \Sigma)$ of a group Γ with respect to the symmetric generating set Σ, with $1 \notin \Sigma$, is the undirected graph having vertex set $V = \Gamma$, and edge set E consisting of the pairs $\{g, ga\}$, where $g \in \Gamma$ and $a \in \Sigma$. If $g_1, g_2 \in \Gamma$, let $d_\Sigma(g_1, g_2)$ denote the distance from g_1 to g_2 in $\mathrm{Cay}(\Gamma, \Sigma)$.

In Section 3, we shall characterize the Cayley graphs of unique factorization pairs. As we shall see below, if (Γ, Σ) is a unique factorization pair, then we obtain an equivalence relation on Σ by writing $a \sim b$ if and only if $a^{-1}b \in \Sigma \cup \{1\}$. This means that the equivalence class $[a]$ of a, together with 1, spans a complete subgraph of $\mathrm{Cay}(\Gamma, \Sigma)$. Since left multiplication by group elements is a graph automorphism, the family

$$\mathcal{C} = \{g([a] \cup \{1\}) : g \in \Gamma, a \in \Sigma\} \tag{1.1}$$

consists of non-empty subsets C of Γ with the following properties: (i) each edge $\{x, y\}$ is contained in some $C \in \mathcal{C}$, and (ii) each C spans a complete subgraph.

If $X = (V, E)$ is any connected undirected graph, and if $\mathcal{C}$ is a family of non-empty subsets of V with property (i), then we can form a connected graph $X_{\mathcal{C}} = (V_{\mathcal{C}}, E_{\mathcal{C}})$ with vertex set $V \cup \mathcal{C}$ and edges $\{x, C\}$, where $C \in \mathcal{C}$ and $x \in C$. We shall show in Theorem 2 below that if (Γ, Σ) is a unique factorization pair then $\mathrm{Cay}(\Gamma, \Sigma)_{\mathcal{C}}$ is a tree, and that this property characterizes unique factorization pairs.

The Cayley graph of a unique factorization pair (Γ, Σ) has other tree-like features. As remarked in [5, Section 3.3], the removal of any vertex disconnects the graph, provided that (Γ, Σ) is not as in Example 1. We shall show in Proposition 2 below that the Cayley graph $\mathrm{Cay}(\Gamma, \Sigma)$ of a unique factorization pair (Γ, Σ) is "2-bounded by a tree". Agostino [2] called a graph X *h-bounded by a tree* if it has a spanning tree T such that the end points of an arbitrary edge of X are at distance at most h in T. Not every pair (Γ, Σ) whose Cayley graph is 2-bounded by a tree is a unique factorization pair. For example, $\Gamma = \mathbb{Z}$, $\Sigma = \{\pm 1, \pm 2\}$.

Since any word of minimal length representing a given group element is in L_Σ, the evaluation map $(a_1, \ldots, a_m) \mapsto a_1 \ldots a_m$ from L_Σ to Γ is surjective for any (Γ, Σ). It also follows that any unique factorization pair (Γ, Σ) has the property that each $g \in \Gamma$ is represented by a unique word in Σ^* of minimal length. The characterization of the pairs (Γ, Σ) with this last property remains an open problem (see [7]).

2. Proof of Theorem 1

Throughout this section, let (Γ, Σ) be a unique factorization pair.

Lemma 2.1. *If $a, b, c, ab, bc \in \Sigma \cup \{1\}$ and $b \neq 1$, then $abc \in \Sigma \cup \{1\}$.*

Proof. We may assume that $a, c, ab, bc \neq 1$. If $g = abc$ were not in $\Sigma \cup \{1\}$, then (ab, c) and (a, bc) would both be in L_Σ and both would represent g. □

Lemma 2.2. *Let H be a group, and let $f_0 : \Sigma \cup \{1\} \to H$ be a map such that $f_0(1) = 1$ and $f_0(ab) = f_0(a)f_0(b)$ whenever $a, b \in \Sigma$ and $ab \in \Sigma \cup \{1\}$. Then there is a unique group homomorphism $f : \Gamma \to H$ which extends f_0.*

Proof. If $w = (a_1, \ldots, a_m) \in \Sigma^*$, define $f^*(w) = f_0(a_1) \ldots f_0(a_m)$, and define $f^*(\emptyset) = 1$, where $\emptyset$ denotes the empty word. Now $f^*(w)$ depends only on the group element w represents. For w can be reduced to a word in L_Σ representing the same element by a succession of steps $w' \mapsto w''$ in which a subword (a, b) (where $a, b \in \Sigma$) of w' is replaced by the word (ab) of length 1 if $ab \in \Sigma$ or by the empty word if $ab = 1$. The condition of this lemma implies that $f^*(w') = f^*(w'')$. If $w_1, w_2 \in \Sigma^*$ both represent $g \in \Gamma$, then the words in L_Σ to which they reduce must be the same, by the unique factorization property. So $f^*(w_1) = f^*(w_2)$. So we may define $f(g) = f^*(w)$ for any $w \in \Sigma^*$ which represents g. It is clear that f is a group homomorphism, and is the only one which extends f_0. □

Definition 2. Let $a, b \in \Sigma$. We write $a \sim b$ if $a^{-1}b \in \Sigma \cup \{1\}$.

Lemma 2.3. *The relation $\sim$ is an equivalence relation on Σ.*

Proof. If $a \sim b$ and $b \sim c$, then $a^{-1}c = (a^{-1})(b)(b^{-1}c) \in \Sigma \cup \{1\}$ by Lemma 2.1. □

Let X denote the set of distinct equivalence classes $[a]$. Write $[a] \approx [b]$ if $[a] = [b]$ or if there is a $c \in \Sigma$ such that $[a] = [c]$ and $[b] = [c^{-1}]$. Note that $[a] \approx [a^{-1}]$.

Lemma 2.4. *The relation $\approx$ is an equivalence relation on X.*

Proof. Suppose that $[a] \approx [b]$ and $[b] \approx [c]$, with $[a] \neq [b]$ and $[b] \neq [c]$. Then there exist $u, v \in \Sigma$ such that $[a] = [u]$, $[b] = [u^{-1}]$, $[b] = [v]$ and $[c] = [v^{-1}]$. Then $u^{-1} \sim v$, so that $uv \in \Sigma \cup \{1\}$. If $uv = 1$, then $[c] = [a]$. If $uv \neq 1$, then $uv \sim u$ and $(uv)^{-1} \sim v^{-1}$ shows that $[a] = [uv]$ and $[c] = [(uv)^{-1}]$. □

Lemma 2.5. *Suppose that (Γ, Σ) is a unique factorization pair. Let $[x_i]$, $i \in I$, be representatives of the distinct $\approx$ classes. Let $\Sigma_i = \{b \in \Sigma : [b] \approx [x_i]\}$. Then each set Σ_i is symmetric, and Σ is the disjoint union of the sets Σ_i. Let Γ_i denote the subgroup of Γ generated by Σ_i. Then (Γ_i, Σ_i) is a unique factorization pair, and (Γ, Σ) is isomorphic to the free product $*_{i\in I}(\Gamma_i, \Sigma_i)$.*

Proof. If $b \in \Sigma_i$, then $[b^{-1}] \approx [b] \approx [x_i]$, and so $b^{-1} \in \Sigma_i$, and Σ_i is symmetric. It is clear that the sets Σ_i are pairwise disjoint and have union Σ.

Let $w = (a_1, \dots, a_m) \in L_{\Sigma_i}$. If $j < m$, then $a_j a_{j+1} \neq 1$. If $a_j a_{j+1} \in \Sigma$, then $a_j a_{j+1} \sim a_j$, so that $[a_j a_{j+1}] = [a_j] \approx [x_i]$. Hence $a_j a_{j+1} \in \Sigma_i$, contradicting $w \in L_{\Sigma_i}$. So $L_{\Sigma_i} \subset L_\Sigma$, and from this it is clear that (Γ_i, Σ_i) is a unique factorization pair.

To see that (Γ, Σ) is isomorphic to the free product $*_{i\in I}(\Gamma_i, \Sigma_i)$, regard $\Sigma \cup \{1\} = \{1\} \cup \bigcup_{i\in I} \Sigma_i$ as a subset of $*_{i\in I} \Gamma_i$ in the usual way. Let $f_0 : \Sigma \cup \{1\} \to *_{i\in I} \Gamma_i$ denote the inclusion map. Let us check the condition of Lemma 2.2. Suppose that $a, b \in \Sigma$ and that $ab \in \Sigma \cup \{1\}$. If $ab = 1$ and $a \in \Sigma_i$, then $b = a^{-1} \in \Sigma_i$ too, and $f_0(a)f_0(b) = ab = 1 = f_0(ab)$. If $ab \in \Sigma$ and $a \in \Sigma_i$, then $ab \sim a$ shows that $[ab] = [a] \approx [x_i]$ and $ab \in \Sigma_i$. So $(ab)^{-1} \in \Sigma_i$, and $b^{-1} \sim b^{-1}a^{-1}$ shows that $[b^{-1}] = [(ab)^{-1}] \approx [x_i]$. Thus $b^{-1} \in \Sigma_i$, and so $b \in \Sigma_i$ too. So $a, b, ab \in \Sigma_i$, and $f_0(a)f_0(b) = ab = f_0(ab)$. So by Lemma 2.2, there is a unique homomorphism $f : \Gamma \to *_{i\in I} \Gamma_i$ extending f_0.

Let $\Sigma' = \bigcup_{i\in I} \Sigma_i$, regarded as a subset of $*_{i\in I} \Gamma_i$. It is evident (Example 4) that $(*_{i\in I} \Gamma_i, \Sigma')$ is a unique factorization pair. Let $h_0 : \Sigma' \cup \{1\} \to \Gamma$ map each $a \in \Sigma_i$, regarded as an element of the free product, to a, regarded as an element of Γ. Clearly h_0 satisfies the condition of Lemma 2.2. The unique extension h of h_0 to $*_{i\in I} \Gamma_i$ is the inverse of f, because of the uniqueness in Lemma 2.2, since $h_0 \circ f_0$ is the identity on Σ and $f_0 \circ h_0$ is the identity on Σ'. Notice that $f(\Sigma) = \Sigma'$, and so f is an isomorphism of unique factorization pairs. □

Lemma 2.6. *The pair $(G * F, \Sigma)$ of Example 3 is a unique factorization pair, and for any $a, b \in \Sigma$ we have $[a] \approx [b]$. If $G = \{1\}$ and $|K| = r < \infty$, then each $[a]$ has r elements.*

Proof. A proof that $(G * F, \Sigma)$ is a unique factorization pair can be given by showing that $G * F$ is a universal group of the partial group Σ, and appealing to [8, Proposition 2.2]. We shall instead give a more direct proof.

Let $\Sigma_0 = (G \setminus \{1\}) \cup \{y_k^{\pm 1} : k \in K\}$. By the uniqueness of normal forms in a free product and by the evident fact that $(F, \{y_k^{\pm 1} : k \in K\})$ is a unique factorization pair, it is clear that $(G * F, \Sigma_0)$ is a unique factorization pair.

Let $w = (a_1, \dots, a_m) \in L_\Sigma$ represent $g \in G * F$. For each i, write $a_i = u_i^{-1} g_i v_i$, where $g_i \in G$ and $u_i, v_i \in \{y_k : k \in K \cup \{0\}\}$ for each i. If $i < m$ then $v_i u_{i+1}^{-1} \neq 1$, since otherwise $a_i a_{i+1} = u_i^{-1} g_i g_{i+1} v_{i+1}$ is in $\Sigma \cup \{1\}$. From w, form the word $\tilde{w} = (u_1^{-1}, g_1, v_1, u_2^{-1}, g_2, \dots, g_m, v_m)$, which has letters in $\Sigma_0 \cup \{1\}$. Let $w_0 = (x_1, \dots, x_\ell)$ be the word obtained from $\tilde{w}$ by discarding all 1's. We claim that $w_0 \in L_{\Sigma_0}$. Notice that if $a, b \in \Sigma_0$ and also $ab \in \Sigma_0$, then a, b must both be

in $G \setminus \{1\}$. So if $x_i x_{i+1} \in \Sigma_0$ for some $i < \ell$, then $x_i = g_j$, $v_j = 1$, $u_{j+1}^{-1} = 1$ and $x_{i+1} = g_{j+1}$ for some $j < m$. But this is impossible because $v_j u_{j+1}^{-1} \neq 1$. If instead $x_i x_{i+1} = 1$, then the pair (x_i, x_{i+1}) is either (y_k, y_k^{-1}) or (y_k^{-1}, y_k) for some k, or (g, g^{-1}) for some $g \in G$, and these possibilities are all excluded because $a_j \neq 1$ and $a_j a_{j+1} \notin \Sigma \cup \{1\}$ for each j.

Notice that the first letter x_1 of w_0 is either u_1^{-1} (if $u_1 \neq 1$), g_1 (if $u_1 = 1$ and $g_1 \neq 1$) or v_1 (if $u_1 = 1$ and $g_1 = 1$).

Suppose that there is an element $g \in G * F$ which is represented by two distinct words, $w = (a_1, \ldots, a_m)$ and $w' = (a'_1, \ldots, a'_{m'})$ in L_Σ. Write $a_i = u_i^{-1} g_i v_i$ and $a'_j = {u'_j}^{-1} g'_j v'_j$ as above. Starting from w and w', we get words $w_0 = (x_1 \ldots, x_\ell)$ and $w'_0 = (w_1, \ldots, w'_{\ell'})$ in L_{Σ_0} as above. Choose such a g so that the number $\ell + \ell'$ of u_i's, g_i's, etc, which are not 1 is minimal. By the unique factorization property of $(G * F, \Sigma_0)$, we have $w_0 = w'_0$. By considering the first letter x_1 of w_0, we see that $u_1 \neq 1$ if and only if $u'_1 \neq 1$, in which case $u_1 = u'_1$. Cancelling u_1^{-1} from both a_1 and a'_1, we find that $u_1 g$ is represented by two distinct words in L_Σ in which the total number of u_i's, etc, is smaller than in w and w', contradicting the minimality in our choice of g. The same contradiction is reached in the case $u_1 = u'_1 = 1$ and $g_1, g'_1 \neq 1$ and in the case $u_1 = u'_1 = 1$, $g_1 = g'_1 = 1$ and $v_1, v'_1 \neq 1$. So $(G * F, \Sigma)$ is a unique factorization pair.

If $G \neq \{1\}$, fix $g_0 \in G \setminus \{1\}$. If $a \in \Sigma$ has the form $g y_\ell$, then $[a] = [g] = [g_0]$. If instead $a = y_k^{-1} g y_\ell$ where $k \in K$, then $[g_0] = [y_k]$ and $[a] = [y_k^{-1}]$, so that again $[a] \approx [g_0]$. If $G = \{1\}$ but $K \neq \emptyset$, fix $k_1 \in K$. If $a = y_\ell$ for some $\ell \in K$, then $[a] = [y_{k_1}]$. If $a = y_k^{-1} y_\ell$ with $k \neq 0$, then $[a] = [y_k^{-1}]$ and $[y_{k_1}] = [y_k]$, so that again $[a] \approx [y_{k_1}]$. Since $y_\ell^{-1} y_k y_{k_1} \notin \Sigma \cup \{1\}$, $a \notin [y_{k_1}]$ in the second case. Hence $[y_{k_1}]$ has exactly r elements if $|K| = r < \infty$. Similarly, each $[y_k^{-1}]$ has r elements. □

By Lemma 2.5, to prove Theorem 1 we may suppose that $[a] \approx [b]$ for all $a, b \in \Sigma$. Fix $a_0 \in \Sigma$. We can choose representatives x_k^{-1} ($k \in K$, say) of the distinct classes $[a]$ other than $[a_0]$ such that $[a_0] = [x_k]$ for each k. We also write $x_0 = 1$.

Lemma 2.7. *The set* $\Pi = \{1\} \cup \{a \in \Sigma : a \sim a_0$ *and* $a^{-1} \sim a_0\}$ *is a subgroup of* Γ.

Proof. Suppose that $a, b \in \Pi \setminus \{1\}$. Then $a^{-1} \sim a_0 \sim b$ and so $ab \in \Sigma \cup \{1\}$. If $ab \neq 1$, then $ab \in \Sigma$ and $ab \sim a \sim a_0$ and $(ab)^{-1} \sim b^{-1} \sim a_0$. So $ab \in \Pi$. □

Lemma 2.8. *Each* $a \in \Sigma$ *can be written in a unique way as a product* $x_k^{-1} g x_\ell$, *where* $k, \ell \in K \cup \{0\}$ *and* $g \in \Pi$. *Moreover,* $[a] = [x_k^{-1}]$ *if* $a \not\sim a_0$ *and* $[a^{-1}] = [x_\ell^{-1}]$ *if* $a^{-1} \not\sim a_0$.

Proof. If $a \in \Pi$, take $k = \ell = 0$ and $g = a$. If $a \in \Sigma$ satisfies $a \sim a_0$ but $a^{-1} \not\sim a_0$, then there is an $\ell \in K$ such that $[a^{-1}] = [x_\ell^{-1}]$. Write $g = a x_\ell^{-1}$. Then $a = g x_\ell = x_0^{-1} g x_\ell$. Also, $g \sim a \sim a_0$ and $g^{-1} \sim x_\ell \sim a_0$ shows that $g \in \Pi$. Similarly, if $a \not\sim a_0$ and $a^{-1} \sim a_0$, then writing $[a] = [x_k^{-1}]$, we have $a = x_k^{-1} g x_0$ for some $g \in \Pi$.

If $a \in \Sigma$ and $a, a^{-1} \not\sim a_0$, then $[a] = [x_k^{-1}]$ and $[a^{-1}] = [x_\ell^{-1}]$ for some $k, \ell \in K$. Then a, x_k, x_ℓ, $x_k a$ and $a x_\ell^{-1}$ are in $\Sigma \cup \{1\}$ and $a \neq 1$. Hence $x_k a x_\ell^{-1} = (x_k a)(a^{-1})(a x_\ell^{-1}) \in \Sigma \cup \{1\}$ by Lemma 2.1. Write $x_k a x_\ell^{-1} = g$. Then $a = x_k^{-1} g x_\ell$. Also, $g \in \Pi$. For $x_k^{-1} g = a x_\ell^{-1} \in \Sigma \cup \{1\}$ shows that $g \sim x_k \sim a_0$, and $g x_\ell = x_k a \in \Sigma \cup \{1\}$ shows that $g^{-1} \sim x_\ell \sim a_0$. If also $a = x_{k'}^{-1} g' x_{\ell'}$, and $k' \neq 0$, then $x_{k'} a = g' x_{\ell'} \in \Sigma \cup \{1\}$ because $g' \sim a_0 \sim x_{\ell'}$ if $g' \neq 1$ and $\ell' \neq 0$, while $x_{k'} a = g' x_{\ell'} \in \Sigma \cup \{1\}$ is clear if $g' = 1$ or $\ell' = 0$. Thus $[x_k^{-1}] = [a] = [x_{k'}^{-1}]$ and $k' = k$. If $k' = 0$, then $a = g' x_{\ell'} \sim g' \sim a_0$, contrary to hypothesis. Similarly $\ell' = \ell$, and therefore $g' = g$. The uniqueness when $a \sim a_0$ or $a^{-1} \sim a_0$ is shown in a similar way. □

Proposition 1. *Suppose that (Γ, Σ) is a unique factorization pair and that $a_0 \in \Sigma$, with $[a] \approx [a_0]$ for all $a \in \Sigma$. Let Π and $\{x_k : k \in K\}$ be as above. Let F denote the subgroup of Γ generated by the x_k's. Then F is a free group, with free generators x_k, $k \in K$, and the pair (Γ, Σ) is isomorphic to the pair of Example 3, where $G = \Pi$ and the y_k's there are the x_k's.*

Proof. Let F' be a free group on a set $\{y_k : k \in K\}$ of free generators in one to one correspondence with $\{x_k : k \in K\}$. Let $y_0 = 1$. Let Σ' denote the generating set of Example 3, where G and F there are Π and F'. Define a function $f_0 : \Sigma \to \Pi * F'$ by writing each $a \in \Sigma$ in its unique form $x_k^{-1} g x_\ell$ ($k, \ell \in K \cup \{0\}$, $g \in \Pi$), and defining $f_0(a) = y_k^{-1} g y_\ell$, regarded as an element of the free product. We now check the condition of Lemma 2.2.

Suppose that $a, b \in \Sigma$ and that $ab \in \Sigma \cup \{1\}$. Write $a = x_k^{-1} g x_\ell$ and $b = x_m^{-1} g' x_n$ as in Lemma 2.8. Assume first that $\ell, m \neq 0$. Then $x_\ell^{-1} \sim a^{-1} \sim b \sim x_m^{-1}$, and so $\ell = m$ and $ab = x_k^{-1} g g' x_n$. If $\ell \neq 0$ and $m = 0$, then $x_\ell^{-1} \sim a^{-1} \sim b = g' x_n \sim a_0$, which is impossible. Similarly, if $\ell = 0$ and $m \neq 0$, then $a_0 \sim g^{-1} x_k = a^{-1} \sim b \sim x_m^{-1}$ is impossible. Finally, if $\ell = 0 = m$, then $ab = x_k^{-1} g g' x_n$. Thus in all cases, $\ell = m$ and $ab = x_k^{-1} g g' x_n$. So $f_0(a) f_0(b) = (y_k^{-1} g y_\ell)(y_m^{-1} g' y_n) = y_k^{-1} g g' y_n = f_0(ab)$. By Lemma 2.2, f_0 lifts uniquely to a group homomorphism $f : \Gamma \to \Pi * F'$. Notice that $f(\Sigma) = \Sigma'$.

Let $h_0 : \Sigma' \to \Gamma$ denote the map which sends each $y_k^{-1} g y_\ell$ to $x_k^{-1} g x_\ell \in \Gamma$. As before, one checks that it satisfies the conditions of Lemma 2.2. Since $(\Pi * F', \Sigma')$ is a unique factorization pair by Lemma 2.6, h_0 extends to a group homomorphism $h : \Pi * F' \to \Gamma$. Since f_0 and h_0 are mutually inverse bijections between Σ and Σ', their extensions are mutually inverse group isomorphisms, by the uniqueness part of Lemma 2.2. □

3. Cayley graphs of unique factorization pairs

Throughout this section, let (Γ, Σ) denote a unique factorization pair, and let $X = \mathrm{Cay}(\Gamma, \Sigma)$ be its Cayley graph.

Lemma 3.1. *If $a \in \Sigma$, then $a([a^{-1}] \cup \{1\}) = [a] \cup \{1\}$.*

Proof. Let $b \in [a^{-1}] \cup \{1\}$. We claim that $ab \in [a] \cup \{1\}$. This is clear if $b = 1$ or $b = a^{-1}$, so assume otherwise. Then $b \sim a^{-1}$ and so $ab \in \Sigma$. Also, $a^{-1}(ab) = b \in \Sigma$, and so $ab \in [a]$. Hence $a([a^{-1}] \cup \{1\}) \subset [a] \cup \{1\}$. Replacing a by a^{-1}, we get the reverse inclusion. □

The fact that $\sim$ is an equivalence relation implies that each set in the family (1.1) spans a complete subgraph of X. The vertices g, ga of any edge in X are both contained in $g([a] \cup \{1\}) \in \mathcal{C}$. The next lemma shows that this is the only $C \in \mathcal{C}$ containing them both.

Lemma 3.2. *If $C, D \in \mathcal{C}$ and $|C \cap D| \geq 2$, then $C = D$.*

Proof. If $g \in \Gamma \setminus \{1\}$, $a \in \Sigma$ and $1 \in g([a] \cup \{1\})$, then $g^{-1} \in [a]$. So by Lemma 3.1, $g([a] \cup \{1\}) = g([g^{-1}] \cup \{1\}) = [g] \cup \{1\}$. Thus the only sets in $\mathcal{C}$ containing 1 are the sets $[a] \cup \{1\}$, $a \in \Sigma$. Now let $C, D \in \mathcal{C}$ with $|C \cap D| \geq 2$. Picking any $g \in C \cap D$, let $C' = g^{-1} C$ and $D' = g^{-1} D$. Then $1 \in C', D' \in \mathcal{C}$, and so $C' = [a] \cup \{1\}$ and $D' = [b] \cup \{1\}$ for some $a, b \in \Sigma$. Since $|C' \cap D'| \geq 2$, there is a $c \neq 1$ in $C' \cap D'$. Hence $a \sim c \sim b$, so that $[a] = [b]$, $C' = D'$ and $C = D$. □

Recall that a *circuit* in a graph is a path $(x_0, x_1, \ldots, x_n)$ whose vertices are distinct except that $x_n = x_0$. We shall always assume that $n \geq 3$.

Lemma 3.3. *Let $(g_0, g_1, \dots, g_n = g_0)$ be a circuit in X. Then there is a $C \in \mathcal{C}$ which contains each g_i. If $S \subset \Gamma$ spans a complete subgraph of X, then $S \subset C$ for some $C \in \mathcal{C}$.*

Proof. Let $\pi = (g_0, g_1, \dots, g_n = g_0)$ be a shortest circuit which is not contained in any $C \in \mathcal{C}$. If $n = 3$, then $g_0^{-1}g_1, g_1^{-1}g_2, g_2^{-1}g_0 \in \Sigma$, and so $g_0^{-1}g_2$ and $g_0^{-1}g_1$ are $\sim$-equivalent. Hence $g_0, g_1, g_2 \in g_0([g_0^{-1}g_1] \cup \{1\})$. So $n \geq 4$ must hold.

If g_i and g_{i+2} are adjacent in X for some $i \leq n-2$, then $(g_0, \dots, g_i, g_{i+2}, \dots, g_n = g_0)$ and $(g_i, g_{i+1}, g_{i+2}, g_i)$ are circuits in X which are shorter than π, and so must be contained in distinct $C, D \in \mathcal{C}$. But $g_i, g_{i+2} \in C \cap D$, and so Lemma 3.2 shows that $C = D$, a contradiction.

So g_i and g_{i+2} are not adjacent in X for any $i \leq n-2$. So $(g_i^{-1}g_{i+1})(g_{i+1}^{-1}g_{i+2}) \notin \Sigma \cup \{1\}$ for each $i \leq n-2$. This shows that the word $(g_0^{-1}g_1, \dots, g_{n-1}^{-1}g_n)$ is in L_Σ, even though it represents $g_0^{-1}g_n = 1$. This contradicts the unique factorization property, and so any circuit in X is contained in some $C \in \mathcal{C}$.

Now let $S \subset \Gamma$ span a complete subgraph of X. We may assume that $|S| \geq 3$. Pick any $s_0, s_1 \in S$ and $C \in \mathcal{C}$ containing s_0, s_1. If $S \not\subset C$, pick $s_2 \in S \setminus C$. As S spans a complete subgraph, s_0, s_1, s_2 are the vertices of a circuit, and so there is a $D \in \mathcal{C}$ containing them all. Then $s_0, s_1 \in C \cap D$, and so $D = C$ by Lemma 3.2. This shows that $s_2 \in C$, a contradiction. So S must be contained in C. □

Definition 3. Let $X = (V, E)$ be any undirected connected graph and let $\mathcal{C}$ be a family of non-empty sets of vertices such that (i) for each edge $\{x, y\}$, there is a $C \in \mathcal{C}$ such that $x, y \in C$, and (ii) each $C \in \mathcal{C}$ spans a complete subgraph of X. We define a graph $X_\mathcal{C}$ by setting $V_\mathcal{C} = \mathcal{C} \cup V$ and $E_\mathcal{C} = \{\{x, C\} : C \in \mathcal{C}, x \in C\}$.

It is easy to see that $X_\mathcal{C}$ is connected (hypothesis (ii) is not needed for this).

Theorem 2. *If (Γ, Σ) is a unique factorization pair, and if $\mathcal{C} = \{g([a] \cup \{1\}) : g \in \Gamma, a \in \Sigma\}$ is the family defined above, then $\mathrm{Cay}(\Gamma, \Sigma)_\mathcal{C}$ is a tree. Conversely, if Γ is a group generated by a finite symmetric subset Σ, with $1 \notin \Sigma$, and if $\mathrm{Cay}(\Gamma, \Sigma)_\mathcal{C}$ is a tree for some family $\mathcal{C}$, then (Γ, Σ) is a unique factorization pair.*

Proof. Suppose there is a circuit in $\mathrm{Cay}(\Gamma, \Sigma)_\mathcal{C}$. Then there is also a circuit of the form

$$\pi = (g_0, C_1, g_1, C_2, \dots, C_n, g_n = g_0),$$

where $n \geq 2$ and $g_i \in \Gamma$ and $C_i \in \mathcal{C}$ for each i. The elements $g_i^{-1}g_{i+2}$, $0 \leq i \leq n-2$, cannot be in Σ. For otherwise g_i, g_{i+1} and g_{i+2} would be pairwise adjacent, and so in C for some $C \in \mathcal{C}$, by Lemma 3.3. But $|C_{i+1} \cap C|, |C_{i+2} \cap C| \geq 2$, so that $C_{i+1} = C = C_{i+2}$ by Lemma 3.2. This contradicts π being a circuit. Thus the word $(g_0^{-1}g_1, g_1^{-1}g_2, \dots, g_{n-1}^{-1}g_n)$ is in L_Σ, is nonempty, and represents 1, contradicting the unique factorization property.

Conversely, suppose that $X = \mathrm{Cay}(\Gamma, \Sigma)$ is a Cayley graph and that $X_\mathcal{C}$ is a tree. Let $g \in \Gamma$ and let $(a_1, a_2, \dots, a_m) \in L_\Sigma$ represent g. For $i = 1, \dots, m$, the vertices $a_1 \dots a_{i-1}$ and $a_1 \dots a_i$ are adjacent in X and so are contained in some $A_i \in \mathcal{C}$. Then

$$\pi = (a_0 = 1, A_1, a_1, A_2, a_1a_2, \dots, A_m, a_1a_2 \dots a_m)$$

is a path $(u_0, u_1, \dots, u_{2m})$ in $X_\mathcal{C}$. We claim that π is a geodesic. Since $X_\mathcal{C}$ is a tree, it is enough to show that $u_k \neq u_{k+2}$ for each $k \leq 2m-2$. So suppose that $u_k = u_{k+2}$. If $k = 2i$, then $a_1 \dots a_{i-1} = a_1 \dots a_i$, which is impossible, as $a_i \neq 1$. If $k = 2i+1$, then $A_{i+1} = A_{i+2} = C$, say, and so $a_1 \dots a_i, a_1 \dots a_{i+1}, a_1 \dots a_{i+2}$ are all in C. Now C spans a complete subgraph, by hypothesis, and so $a_1 \dots a_i$ and $a_1 \dots a_{i+2}$ are equal or adjacent in X. But then $a_{i+1}a_{i+2} \in \Sigma \cup \{1\}$, contradicting $(a_1, a_2, \dots, a_m) \in L_\Sigma$.

Since $X_{\mathcal{C}}$ is a tree, there is only one geodesic from 1 to g. So there is only one word in L_Σ representing g, and (Γ, Σ) is a unique factorization pair. □

We conclude this section with a result mentioned in the introduction:

Proposition 2. *If (Γ, Σ) is a unique factorization pair, then $X = \mathrm{Cay}(\Gamma, \Sigma)$ is 2-bounded by a tree.*

Proof. Let E_0 denote the set of all edges $\{a_1 \dots a_{m-1}, a_1 \dots a_m\}$ of X, where $(a_1, \dots, a_m) \in L_\Sigma$ has length $m \geq 1$. That is, E_0 consists of the edges $\{x, y\}$ of X for which $d_\Sigma(1, x) \neq d_\Sigma(1, y)$. Now $X_0 = (\Gamma, E_0)$ is a tree. For if $\pi = (g_0, \dots, g_n = g_0)$ is a circuit in X_0, we may choose the numbering so that $d_\Sigma(1, g_0) \geq d_\Sigma(1, g_i)$ for $i = 0, \dots, n$. But g_0 has only one neighbour g in X_0 satisfying $d_\Sigma(1, g) < d_\Sigma(1, g_0)$, namely $a_1 \dots a_{m-1}$ if $(a_1, \dots, a_m)$ represents g_0. So $g_1 = g_{n-1}$, in contradiction to π being a circuit. So X_0 is a spanning tree for X.

Let $\{x, y\}$ be an edge in X. If $d_\Sigma(1, x) \neq d_\Sigma(1, y)$, then $\{x, y\} \in E_0$ and $d_{X_0}(x, y) = 1$. If $d_\Sigma(1, x) = d_\Sigma(1, y)$, then $x = a_1 \dots a_m$ and $y = a_1 \dots a_m a$ for some $(a_1, \dots, a_m) \in L_\Sigma$ and $a \in \Sigma$ such that $a_m a \in \Sigma$. So for $z = a_1 \dots a_{m-1}$, (x, z, y) is a path in X_0 of length 2, and so $d_{X_0}(x, y) = 2$. So X is 2-bounded by a tree. □

Acknowledgement. Since completing this paper, we have been informed by Jean Mairesse that a revised version of [5] will contain Theorem 1, stated in the form of an algorithm, which he had independently deduced from [8].

References

1. J. Avenhaus, K. Madlener, and F. Otto. Groups presented by finite two-monadic Church-Rosser Thue systems. *Trans. Amer. Math. Soc.*, 297(2):427–443, 1986.
2. G. D'Agostino. Cayley graphs of virtually free groups. *Internat. J. Algebra Comput.*, 3(2):189–199, 1993.
3. D.B.A. Epstein, J.W. Cannon, D.F. Holt, S.V.F. Levy, M.S. Paterson, and W.P. Thurston. Word processing in groups, Jones and Bartlett Publishers, Boston, 1992.
4. R.H. Haring-Smith. Groups and simple languages. *Trans. Amer. Math. Soc.*, 279(1):337–356, 1983.
5. J. Mairesse. Random Walks on Groups and Monoids with a Markovian Harmonic Measure. Preprint, 2004. (Available at `http://www.liafa.jussieu.fr/~mairesse/Article/` and `http://www.liafa.jussieu.fr/web9/rapportrech/description_en.php?idrapportrech=666`).
6. J. Mairesse and F. Mathéus. Random walks on groups with a tree-like Cayley graph. In *Mathematics and computer science. III. Algorithms, trees, combinatorics and probabilities*, p. 445–460, Trends in Mathematics, Birkhäuser Verlag, 2004.
7. M. Shapiro. Pascal's triangles in abelian and hyperbolic groups. *J. Austral. Math. Soc. Ser. A*, 63(2):281–288, 1997.
8. J. Stallings. A remark about the description of free products of groups. *Proc. Cambridge Philos. Soc.*, 62:129–134, 1966.