On free-group algorithms that sandwich a subgroup between free-product factors

Warren Dicks

May 7, 2014

Abstract. Let $F$ be a finite-rank free group and $H$ be a finite-rank subgroup of $F$. We discuss proofs of two algorithms that sandwich $H$ between an upper-layer free-product factor of $F$ that contains $H$ and a lower-layer free-product factor of $F$ that is contained in $H$.

Richard Stong showed that the unique smallest-possible upper layer, denoted $\text{Cl}(H)$, is visible in the output of the polynomial-time cut-vertex algorithm of J. H. C. Whitehead. Stong’s proof used bi-infinite paths in a Cayley tree and sub-surfaces of a three-manifold. We give a variant of his proof that uses edge-cuts of the Cayley tree induced by edge-cuts of a Bass-Serre tree.

A. Clifford and R. Z. Goldstein gave an exponential-time algorithm that determines whether or not the trivial subgroup is the only possible lower layer. Their proof used Whitehead’s three-manifold techniques. We give a variant of their proof that uses Whitehead’s cut-vertex results, and thereby obtain a somewhat simpler algorithm that yields a lower layer of maximum-possible rank.

2010 Mathematics Subject Classification. Primary: 20E05; Secondary: 20E36, 20E08.

Key words. Sub-bases of free groups. Free-product factors. Cut-vertex algorithm. Cut-vertex lemma. Clifford-Goldstein algorithm.

1 Introduction

1.1 Definitions. For any set $E$, we let $\langle E \mid \rangle$ denote the free group on $E$. By a basis of $\langle E \mid \rangle$, we mean a free-generating set of $\langle E \mid \rangle$. By a sub-basis of $\langle E \mid \rangle$ we mean a subset of a basis of $\langle E \mid \rangle$. We let $\text{Aut}(E \mid \rangle$ denote the group of automorphisms of $\langle E \mid \rangle$ acting on the right as exponents.

For any subset $Z$ of $\langle E \mid \rangle$, we let $\langle Z \rangle$ denote the subgroup of $\langle E \mid \rangle$ generated by $Z$. We let $\text{supp}(Z \text{ rel } E)$ denote the $\subseteq$-smallest subset of $E$ such that $Z \subseteq \langle \text{supp}(Z \text{ rel } E) \rangle$. We let $\text{Cl}(Z)$ denote the intersection of all the free-product factors (generated by sub-bases) of $\langle E \mid \rangle$ that contain $Z$.

*Partially supported by Spain’s Ministerio de Ciencia e Innovación through Project MTM2011-25955.
1.2 Hypotheses. Throughout, let $E$ be a finite set, let $Z$ be a finite subset of $\langle E \rangle$, and let $E_Z$ denote $\text{supp}(Z \text{ rel } E)$.

1.3 History. Recall Hypotheses 1.2.

- In [8, publ. 1936], J. H. C. Whitehead gave his true-word and cyclic-word cut-vertex algorithms, and the former determines whether or not $Z$ is a sub-basis of $\langle E \rangle$. A little later, in [9, publ. 1936], he gave an exponential-time, general-purpose algorithm which has largely overshadowed the easier-to-prove, polynomial-time, limited-use algorithm. We wish to emphasize that the cut-vertex algorithm suffices to efficiently sandwich a subgroup between two free-product factors.

Whitehead defined a certain finite graph which we denote $\text{Wh}_\ast(Z \text{ rel } E_Z)$. He observed that if some vertex of $\text{Wh}_\ast(Z \text{ rel } E_Z)$ is what we call a Whitehead cut-vertex, then it is straightforward to construct an automorphism of $\langle E \rangle$ that strictly reduces the total $E$-length of $Z$. Clearly, one then has an algorithm (with choices) which constructs some $\Psi \in \text{Aut}(\langle E \rangle)$ such that $\text{Wh}_\ast(Z^\Psi \text{ rel } E_Z^\Psi)$ has no Whitehead cut-vertices. It then remains to extract information from $\Psi$ and $Z^\Psi$. For example, it will transpire that the rank of $\text{Cl}(Z)$ is $|E_Z^\ast|$. One reason this is interesting is that Edward C. Turner [7, Theorem 1] showed that the rank of $\text{Cl}(Z)$ is $|E|$ if and only if $Z$ is a test set for injective endomorphisms of $\langle E \rangle$ to be automorphisms, that is, each injective endomorphism of $\langle E \rangle$ that maps $\langle Z \rangle$ onto itself is an automorphism.

Using a three-manifold model of $\text{Wh}_\ast(Z \text{ rel } E_Z)$, Whitehead proved a cut-vertex lemma: If $Z$ is a sub-basis of $\langle E \rangle$, then $Z^\Psi \subseteq E^{\pm 1}$.

Hence, $Z$ is a sub-basis of $\langle E \rangle$ if and only if $Z \cap Z^{-1} = \emptyset$ and $Z^\Psi \subseteq E^{\pm 1}$; in this event, $Z \cup (E^\Psi \setminus Z^{\pm1})$ is a basis of $\langle E \rangle$.

Set $E'_Z := E^{\Psi^{-1}}$ and $E_Z := \text{supp}(Z \text{ rel } E')$. Expressing the elements of $Z^\Psi$ in terms of $E$ is equivalent to expressing the elements of $Z$ in terms of $E'$. The important point is that $\text{Wh}_\ast(Z \text{ rel } E'_Z)$ is isomorphic to $\text{Wh}_\ast(Z^\Psi \text{ rel } E_Z^\Psi)$ and, hence, has no Whitehead cut-vertices.

In [8, publ. 1997], Richard Stong used bi-infinite paths in a Cayley tree and sub-surfaces homologous to an essential disk in a three-manifold to prove a more general cut-vertex lemma: The set $E'_Z$ is a basis of $\text{Cl}(Z)$, and, for each free-product factorization $\text{Cl}(Z) = \bigast_{i \in I} H_i$ such that $Z \subseteq \bigcup_{i \in I} H_i$, the set $E'_Z$ contains a basis of each $H_i$.

Not only can a basis of $\text{Cl}(Z)$ be computed efficiently, but also there are only finitely many possibilities for the sets $\{H_i\}_{i \in I}$, and they can all be computed efficiently. To see how Stong’s cut-vertex lemma generalizes Whitehead’s, notice that if $Z$ is a sub-basis of $\langle E \rangle$, then $\text{Cl}(Z) = \langle Z \rangle = \bigast_{z \in Z} \langle z \rangle$ and $Z \subseteq \bigcup_{z \in Z} \langle z \rangle$, and, here, for $E'_Z$ to contain a basis of each $\langle z \rangle$, which is necessarily $\{z\}$ or $\{z^{-1}\}$, one must have $(E'_Z)^{\pm 1} \supseteq Z$, and, hence, $E^{\pm 1} \supseteq Z^\Psi$.

- In [1, publ. 2010], A. Clifford and R. Z. Goldstein revisited Whitehead’s three-manifold techniques and constructed an ingenious exponential-time algo-
rithm which determines whether or not some element of \langle Z \rangle lies in a basis of \langle E \rangle, and, in the affirmative case, finds such an element.

1.4 Content. What we do in this article is formalize Whitehead’s cut-vertex algorithm, give a Bass-Serre-theoretic proof of Stong’s cut-vertex lemma, and give an algorithm that yields a basis \( E'' \) of \langle E \rangle that maximizes \(|E'' \cap \langle Z \rangle|\).

In Section 2, for completeness and to develop the notation and basic results that will be used, we formalize part of Whitehead’s discussion of cut-vertices and free-group automorphisms, including his true-word cut-vertex algorithm.

In Section 3, Stong’s beautiful true-word cut-vertex lemma is proved using edge-cuts of a Cayley tree induced by edge-cuts of a Bass-Serre tree. At this stage, we will have given a detailed proof for the polynomial-time algorithm for computing a basis of \( \text{Cl}(Z) \) that is more algebraic than Stong’s proof.

In Section 4, we restructure the Clifford-Goldstein argument using Whitehead’s cut-vertex results in place of the topology, and obtain a slightly faster, more powerful algorithm that yields a basis \( E'' \) of \langle E \rangle which maximizes \(|E'' \cap \langle Z \rangle|\). In particular, \( E'' \cap \langle Z \rangle \neq \emptyset \) if and only if some element of \langle Z \rangle lies in a basis of \langle E \rangle.

2 A formalized cut-vertex algorithm

This technical section gives elementary definitions and arguments that formalize part of Whitehead’s discussion \[8, \text{pp.50–52}\] of cut-vertices and free-group automorphisms.

By a graph, we mean a set given as the disjoint union of two sets, called the vertex-set and the edge-set, together with an initial-vertex map and a terminal-vertex map, each of which maps the edge-set to the vertex-set. For any set \( S \), we write \( K(S) \) to denote the graph which has vertex-set \( S \) and edge-set \( S \times 2 := S \times S \), where an edge \((x,y)\) has initial vertex \( x \) and terminal vertex \( y \).

2.1 Notation. Recall Hypotheses 1.2.

- For \( e \in E \), we write \( \overline{e} := e^{-1} \) and \( e^\pm := \{e, \overline{e}\} \). We write \( E^{-1} := \{\overline{e} \mid e \in E\} \) and \( E^{\pm} := E \cup E^{-1} \). We shall be interested in the graph \( K(E^{\pm} \cup \{1\}) \), which has basepoint 1 and an inversion map on the vertices.

- Consider any \( z \in \langle E \rangle \), and let \( e_1 e_2 \cdots e_n \) represent the reduced \( E^{\pm} \)-expression for \( z \).

  - \( \text{supp}(\{z\} \text{ rel } E) = \bigcup_{i=1}^{n} (E \cap e_i^{\pm}) \) and \( \text{supp}(Z \text{ rel } E) = \bigcup_{z \in Z} \text{supp}(\{z\} \text{ rel } E) \).

  - We set \( ||z||_E := n \) and \( ||Z||_E := \sum_{z \in Z} ||z||_E \).

  - We say that a product \( xy \) has no \( E^{\pm} \)-cancellation if \( ||xy||_E = ||x||_E + ||y||_E \), and then sometimes write \( xy \) as \( x \cdot y \) for emphasis.

- Suppose that \( z \neq 1 \). We set \( e_0 := e_{n+1} := 1 \). For \( i \in \{0, 1, \ldots, n\} \), we say that \((e_i, e_{i+1})\) occurs in the reduced \( (E^{\pm} \cup \{1\}) \)-expression for \( z \), and note that
there exist $g', g'' \in \langle E \mid \rangle$ such that $z = g' \cdot e_1 \cdot e_{i+1} \cdot g''$ with no $E^{\pm 1}$-cancellation, $g' = 1$ if $e_1 = 1$, and $g'' = 1$ if $e_{i+1} = 1$. We set

$$\text{WH}_z(z) \triangleq E^{\pm 1}_z \cup \{ 1 \} \cup \{ (\overline{e}, e_{i+1}) \}_{i=0}^n \subseteq \mathbb{K}(E^{\pm 1}_z \cup \{ 1 \})$$

and $\text{WH}_z(\{ 1 \}) \triangleq E^{\pm 1} \cup \{ 1 \}$. For example, for each $e \in E^{\pm 1}$, we have $\text{WH}_z(\{ e \}) \triangleq E^{\pm 1}_z \cup \{ 1 \} \cup \{ (1, e), (\overline{e}, 1) \}$. We also have the pentagonal example $\text{WH}_z(\{ x^2y^2 \} \cup \{ x, y \}) = \{ x, y, \overline{x}, \overline{y}, 1, (1, x), (\overline{x}, x), (\overline{y}, y) \}$. If $\text{WH}_z(\{ e \})$ is not connected, then each element of $E^{\pm 1}$ is a Whitehead cut-vertex, since the set of valence-zero vertices is closed under inversion.

- Let $S$ be a subset of $\langle E \mid \rangle$. If $S \neq \emptyset$, we set

\[
\text{WH}_z(S \cap E) := \bigcup_{z \in S} \text{WH}_z(z) \cap E \subseteq \mathbb{K}(E^{\pm 1} \cup \{ 1 \}),
\]

and we set $\text{WH}_z(\emptyset \cap E) := E^{\pm 1} \cup \{ 1 \}$. In $\text{WH}_z(S \cap E)$, a vertex $e_*$ is said to be a Whitehead cut-vertex if removing $e_*$ and all the edges incident to $e_*$ leaves a basepointed graph that is not connected; this entails $e_* \neq 1$. If $\text{WH}_z(S \cap E)$ is not connected, then each element of $E^{\pm 1}$ is a Whitehead cut-vertex, since the set of valence-zero vertices is closed under inversion.

- We let $\text{cuts}(E)$ denote the set of those ordered triples $(\varnothing D_1 D_1, e_*)$ such that $\varnothing D_1 D_1 = E^{\pm 1}$, $\varnothing D_1 \cap D_1 = \{ e_* \}$, and $D_1 \neq \{ e_* \}$. Clearly, $\varnothing D \subseteq E^{\pm 1}$, $1 D \subseteq E^{\pm 1}$, and $e_* \in E^{\pm 1}$. Suppose that $\mathcal{C} = (\varnothing D_1 D_1, e_*) \in \text{cuts}(E)$.

- For each $(\alpha, \beta) \in \{ 0, 1 \}^2$, we set $\alpha D_\beta \triangleq \alpha D \cap \beta D^{-1}$ and $\alpha E_\beta \triangleq E \cap \alpha D \cap \beta D$. Let $\chi : E^{\pm 1} \to \{ 0, 1 \}$, $e \mapsto \chi(e) := \{ e \} \cap \{ 1 \}$, be the characteristic map of $1 D$. We set $\eta_\mathcal{C} := \chi(\overline{e}_*) \in \{ 0, 1 \}$ and $d_* := e_\eta_\mathcal{C} \in E^{\pm 1}$, that is, $d_* = \overline{e}_*$ if $\overline{e}_* \in 0 D$, while $d_\eta = e_*$ if $\overline{e}_* \in 1 D$. We define $\varphi_\mathcal{C}$ to be the automorphism of $\langle E \mid \rangle$ that fixes $d_*$ and maps $e$ to $d_\chi(e) e_\chi(e)$ for each $e \in E - d^{\pm 1}$.

- We define three subgraphs of $\mathbb{K}(E^{\pm 1} \cup \{ 1 \})$: $\text{WH}_z(\mathcal{C}) := \mathbb{K}(\varnothing D \cup \{ 1 \})$; $\text{WH}_z(\mathcal{C}) := \mathbb{K}(1 D)$; and, $\text{WH}_z(\mathcal{C}) := \mathbb{K}(\varnothing D \cup \{ 1 \}) \cup \mathbb{K}(1 D)$. We say that $\mathcal{C}$ cuts each subgraph of $\text{WH}_z(\mathcal{C})$ with the full vertex-set, $E^{\pm 1} \cup \{ 1 \}$.

If $\mathcal{C}$ cuts $\text{WH}_z(\mathcal{C} \cap E)$, then $e_*$ is a Whitehead cut-vertex of $\text{WH}_z(\mathcal{C} \cap E)$, since $\varnothing D \cup \{ 1 \}$ and $1 D$ have union $E^{\pm 1} \cup \{ 1 \}$ and intersection $\{ e_* \}$, while $\varnothing D \cup \{ 1 \} \neq \{ e_* \} \neq 1 D$.

2.2 Lemma. With Hypotheses 1.2 fix $\mathcal{C} = (\varnothing D_1 D_1, e_*) \in \text{cuts}(E)$, and let $z \in \langle E \mid \rangle$. Then the following hold.

(i) $\hat{E} := \bigcup_{(\alpha, \beta) \in \{ 0, 1 \}^2} (\alpha a E_\beta) \overline{\alpha} \beta$ is a basis of $\langle E \cup \{ a \} \mid \rangle$.

(ii) $||z||_E = ||z||_{\hat{E}}$ if and only if $\mathcal{C}$ cuts $\text{WH}_z(\{ z \}) \cap E$.

(iii) If $\mathcal{C}$ cuts $\text{WH}_z(\{ z \}) \cap E$, then $||z_{\overline{\mathcal{C}}}||_E \leq ||z||_E$.

(iv) If $\mathcal{C}$ cuts $\text{WH}_z(\{ z \}) \cap E$ and $e_*$ has positive valence in the subgraph $\text{WH}_z(\{ z \}) \cap E \cap \{ 1 - \eta_\mathcal{C}, \varphi_\mathcal{C} \}$, then $||z_{\overline{\mathcal{C}}}||_E < ||z||_E$.

Proof. Set $F := \langle E \mid \rangle$, $\hat{F} := \langle E \cup \{ a \} \mid \rangle$, $\eta := \eta_\mathcal{C}$, and $\varphi := \varphi_\mathcal{C}$.

(i). Recall that $e_* \in E^{\pm 1}$.

If $e_* \in E$, then $\varnothing E_\eta \cap 1 E_\eta = \{ e_* \}$ and there are no other overlaps among the $\alpha E_\beta$. Since $\{ a^\alpha e_* \overline{\alpha} \beta, a^\alpha e_* \overline{\alpha} \beta \} \subseteq \hat{E}$ and $(a^\alpha e_* \overline{\alpha} \beta)(a^\alpha e_* \overline{\alpha} \beta)^{-1} = a$, we see easily that $\hat{E}$ is a basis of $\hat{F}$.\hfill \Box
Similarly, if \( e_* \in E^{-1} \), then \( aE_0 \cap \eta E_1 = \{ \tau_* \} \) and there are no other overlaps among the \( aE_i \). Again, \( \tilde{F} \) is a basis of \( \tilde{F} \).

(ii). Let \( e_1 e_2 \cdots e_n \) represent the reduced \( E^{\pm1} \)-expression for \( z \). For any map \( \{0, \ldots, n\} \to \{0, 1\} \), \( i \mapsto \chi_i \), the following three conditions are easily seen to be equivalent.

- the reduced \( \tilde{E}^{\pm1} \)-expression for \( z \) is \((a^{\chi_0}e_1\tau_1)(a^{\chi_1}e_2\tau_2)\cdots(a^{\chi_n}e_ne_n)\).
- \( e_i \in \chi_i-1D_{\chi_i} \), \( i = 1, 2, \ldots, n \), and \( \chi_0 = \chi_n = 0 \).
- \( (\tau_i, e_{i+1}) \in \chi_iD^{x^2} \), \( i = 1, 2, \ldots, n-1 \), \( (\tau_n, e_1) \in \tilde{e}D^{x^2} \), and \( \chi_0 = \chi_n = 0 \).

Now (ii) follows.

(iii). Let \( \tilde{\phi}: \tilde{F} \to F \) denote the retraction that carries \( a \) to \( d_* := \varepsilon_2^{2y-1} \). We apply \( \tilde{\phi} \) to \( \{a^0e_*\tau, a^{-1}e_*\tau^n\} = \{a^0e_*\tau, a^1e_*\tau^n\} \subseteq \tilde{E}^{\pm1} \). Here, we have \((a^0e_*\tau^n)^\tilde{\phi} = e_*d^{\tau-n} = e_* \) and \((a^{-1}e_*\tau^n)^\tilde{\phi} = e_*d^{1-\tau-n} = 1 \). It follows that \( \tilde{\phi} \) carries \( \tilde{E} \) to \( \tilde{E}_\varepsilon \cup \{1\} \). Since \( z\tilde{\phi} = z \), we see that \( ||z||_{E_\varepsilon} \leq ||z||_{\tilde{E}} \). Now \( ||z\tilde{\phi}||_{\tilde{E}} = ||z||_{E_\varepsilon} \leq ||z||_{\tilde{E}} = ||z||_{E} \), by (ii).

(iv). There exists some vertex \( e \) of \( 1-\eta WH(C) \) such that \( (\tau, e_*) \) occurs in the reduced \( (E^{\pm1} \cup \{1\}) \)-expression for \( z \) or \( \tau \). Necessarily, \( e \neq e_* \). Hence, \( e \notin \eta WH(C) \). As in (ii), the element \((a^{-1}e_*\tau^n) \in \tilde{E}^{\pm1} \) occurs in the reduced \( \tilde{E}^{\pm1} \)-expression for \( z \) or \( \tau \). Hence, \((a^{-1}e_*\tau^n) \) or \((a^n\tau_1^{-1}\tau) \) occurs in the reduced \( \tilde{E}^{\pm1} \)-expression for \( z \). As in (iii), each such term is mapped to 1 by \( \tilde{\phi} \). Thus, \( ||z\tilde{\phi}||_{\tilde{E}} = ||z||_{E_\varepsilon} < ||z||_{\tilde{E}} = ||z||_{E} \). \( \square \)

2.3 Algorithm. Recall Hypotheses \[ \text{Whitehead’s cut-vertex subroutine} \]

We consider two cases.

**Case 1**: \( WH_4(Z \text{ rel } E_Z) \) is connected.

Deletions \( e_* \) and its incident edges from \( WH_4(Z \text{ rel } E_Z) \) leaves a subgraph that has a unique expression as the disjoint union of two nonempty subgraphs \( X_0 \) and \( X_1 \) such that \( X_0 \) is connected and contains \( \{1\} \).

Set \( \text{Set } D_0 := (X_0 \cap E_{Z}^{+1} ) \cup \{ e_* \} \cup (E^{\pm1} - E_{Z}^{+1}) \), \( D_1 := (X_1 \cap E_{Z}^{-1} ) \cup \{ e_* \} \), and \( C := (0D_0, 1D_1, e_*) \in \text{cuts}(E) \). Then \( WH_4(Z \text{ rel } E) \subseteq WH_4(C) \), and \( e_* \) has positive valence in both \( WH_4(Z \text{ rel } E) \) and \( WH_4(C) \). Thus, \( e_* \) has positive valence in \( WH_4(Z \text{ rel } E) \) and \( WH_4(C) \). It follows from Lemma \[ \text{Lemma 2.2(iii), (iv)} \] that \( ||Z\tilde{\text{C}}||_E < ||Z||_E \). We return \( C \) and terminate the procedure.

**Case 2**: \( WH_4(Z \text{ rel } E_Z) \) is not connected.

Let \( X \) denote the component of \( WH_4(Z \text{ rel } E_Z) \) containing \( \{1\} \), and let \( D := X \cap E_{Z}^{\pm1} \). If it were the case that \( D^{-1} = D \), then it is not difficult to see that we would have \( Z \subseteq \langle D \rangle \), \( E_{Z}^{\pm1} = D \), and \( X = WH_4(Z \text{ rel } E_Z) \), which would contradict the assumption that \( WH_4(Z \text{ rel } E_Z) \) is not connected. Thus, \( D^{-1} \neq D \), \( D \not\subseteq D^{-1} \), and \( D-D^{-1} \neq \emptyset \).
Choose $e' \in D - D^{-1}$, and set $0 : = D \cup (E^{+1} - E^+_Z)$, $1 : = (E^{+1}_Z - D) \cup \{e'_1\}$, and $C : = (0, 1, D, e'_1) \in \text{cuts}(E)$. It is clear that $WH_e(Z \text{ rel } E) \subseteq WH_e(C)$. Here, $\eta_C = \{|\{e'_{i}\}^{-1}\} \cap 1D| = 1$. Also, $WH_e(Z \text{ rel } E) \cap \phi WH_e(C) \supseteq X$, the component of $WH_e(Z \text{ rel } E_Z)$ that contains $\{e'_1, 1\}$. Since $e'_1$ has positive valence in $X$, it follows from Lemma 2.2(iii),(iv) that $||Z^{+\eta}||_E < ||Z||_E$. We return $C$ and terminate the procedure.

### 2.4 Algorithm

Recall Hypotheses 1.2. Via the mock flow chart

```
Set $\Phi := 1 \in \text{Aut}\langle E \rangle$ and $Z' := Z$.

Find $E_{Z'} := \text{supp}(Z' \text{ rel } E)$ and construct $WH_e(Z' \text{ rel } E_{Z'})$.

Search for a Whitehead cut-vertex $e_*$ of $WH_e(Z' \text{ rel } E_{Z'})$.

Does such an $e_*$ exist?  
  Yes  No  
  \quad \rightarrow  \quad  \text{Return } (\Phi, Z') \rightarrow \text{Stop}.

Algorithm 2.3 yields a $\varphi \in \text{Aut}\langle E \rangle$ such that $||Z^{+\varphi}||_E < ||Z'||_E$.

Reset $\Phi := \varphi \cdot \Phi$ and $Z' := Z^{+\varphi}$, thereby decreasing $||Z'||_E$.
```

Whitehead’s cut-vertex algorithm [8, p. 51] returns a pair $(\Phi, Z')$ such that $\Phi \in \text{Aut}\langle E \rangle$, $Z' = Z^{+\varphi}$, and the isomorphic graphs $WH_e(Z' \text{ rel supp}(Z' \text{ rel } E))$ and $WH_e(Z \text{ rel supp}(Z \text{ rel } E\Phi))$ have no Whitehead cut-vertices. It is then not difficult to find $\text{supp}(Z' \text{ rel } E)$, $E\Phi$, and, hence, $\text{supp}(Z \text{ rel } E\Phi)$.

Information about these will be given in Lemmas 3.4 and 3.7. For example, $|\text{supp}(Z \text{ rel } E\Phi)|$ is smallest-possible over all bases of $\langle E \rangle$, that is, $\text{supp}(Z \text{ rel } E\Phi)$ is a basis of $\text{Cl}(Z)$. Also, $Z$ is a sub-basis of $\langle E \rangle$ if and only if $Z \cap Z^{-1} = \emptyset$ and $Z' \subseteq E^{+1}$; in this event, $Z \cup (E\Phi - Z^{+1})$ is a basis of $\langle E \rangle$.

### 2.5 Notes

Although Whitehead did not mention it, it is possible to implement Algorithm 2.4 in such a way that it terminates in time that is polynomial (linear?) in $|E| + ||Z||_E$. Depth-first searches may be used to find the component $X$ of $WH_e(Z' \text{ rel } E_{Z'})$ that contains $\{1\}$, and to search for an element $e_* \in X \cap E^{+1}$ such that either $\tau_* \notin X$ or removing $e_*$ and its incident edges from $X$ leaves a graph that is not connected. If no such $e_*$ exists then $WH_e(Z' \text{ rel } E_{Z'})$ has no Whitehead cut-vertices, as was seen in Algorithm 2.3. If such an $e_*$ exists, then it may be used to construct a $\varphi$ such that $||Z^{+\varphi}||_E < ||Z'||_E$, as was also seen in Algorithm 2.3.
3 Bass-Serre proofs of cut-vertex lemmas

3.1 Review. Let $F$ be a group.

- Let $S$ be a subset of $F$. We let Cayley($F,S$) denote the graph with vertex-set $F$ and edge-set $F \times S$, where each edge $(g,s) \in F \times S$ has initial vertex $g$ and terminal vertex $gs$; we shall sometimes write edge$(g \cdot^s e \rightarrow gs)$ to denote the pair $(g,s)$ viewed as an edge. Then Cayley($F,S$) is an $F$-graph. It is a tree when $S$ is a basis of $F$. See, for example, [2, Theorem I.7.6].

- Let $I$ be a set and $(H_i)_{i \in I}$ be a family of subgroups of $F$. We let BassSerre($F,(H_i)_{i \in I}$) denote the graph whose vertex-set is the disjoint union
\[ \bigcup_{i \in I} (F \times H_i) \]
and edge-set $\bigcup_{i \in I} (F \times H_i)$, where each edge $(g,i) \in F \times I$ has initial vertex $g$ and terminal vertex $gH_i$; we shall sometimes write edge$(g \cdot^i e \rightarrow gH_i)$ to denote the pair $(g,i)$ viewed as an edge. Then BassSerre($F,(H_i)_{i \in I}$) is an $F$-graph. It is a tree when $F = \star_{i \in I} H_i$, by a result of H. Bass and J.-P. Serre. See, for example, [2, Theorem I.7.6].

Notice that if a subset $S$ of $\langle E \rangle$ contains $E$, then Wh$_*(S \rel E)$ contains the basepointed star Wh$_*(E \rel E)$, and therefore has no Whitehead cut-vertices. The following amazing partial converse can be extracted from the (1)$\Rightarrow$(3) part of [6, Theorem 10]. The case where each free-product factor is cyclic is essentially Whitehead’s cut-vertex lemma [6, Lemma].

3.2 The Strong-Whitehead theorem. For each finite set $E$ and free-product factorization $\langle E \rangle = \star_{i \in I} H_i$ such that $\bigcup_{i \in I} H_i \not\subseteq E$, the graph Wh$_*(\bigcup_{i \in I} H_i \rel E)$ has a Whitehead cut-vertex.

Proof. Set $F := \langle E \rangle$. Recall Review[3.1] and set $T :=$ Cayley($F,E$) and $T^* :=$ BassSerre($F,(H_i)_{i \in I}$). Thus, $T$ and $T^*$ are $F$-trees whose vertex-sets contain $F$.

We work first with $T^*$. We let link$_T(1)$ denote the set of $T^*$-edges incident to the $T^*$-vertex 1, and star$_T(1)$ denote the set of components of the forest $T^* \setminus \text{link}_T(1)$. For each $T^*$-vertex $v$, there exists a unique component $\chi(v)$ of $\text{star}_T(1)$ such that $v \in \chi(v)$. For any $T^*$-vertices $v$ and $w$, we let $T^*[v,w]$ denote the smallest subtree of $T^*$ that contains $\{v,w\}$, and then $\chi(v) \neq \chi(w)$ if and only if $1 \in T^*[v,w]$ and $v \neq w$. Also, $\chi$ restricts to a map $F \rightarrow \text{star}_T(1)$.

In $T$ now, set $\delta := \{\text{edge}(g \cdot v \rightarrow ge) = (g,e) \in F \times E \subseteq T \mid \chi(g) \neq \chi(g e)\}$. Clearly, $\chi$ is constant on the vertex-set of each component of $T \setminus \delta$. An element $(g,e) \in F \times E$ lies in $\delta$ if and only if $1 \in T^*[g,ge]$, or, equivalently, $\delta \in T^*[1,e]$. Since $E$ is nonempty and finite, it is clear that $\delta$ is nonempty and finite. Hence, there exists $(g_0,e_0) \in F \times E^{\pm 1}$ satisfying $\|g_0 e_0\|_E = \|g_0\|_E + 1$ and $\chi(g_0) \neq \chi(g_0 e_0)$ such that $\|g_0\|_E$ has the maximum possible value.

We shall now show that $g_0 \neq 1$. By hypothesis, there exists $e_0 \in E \setminus \bigcup_{i \in I} H_i$. Since $e_0 \neq 1$, there exists some $T^*[1,e_0]$-neighbour of 1, necessarily $1H_{i_0}$ for
some \( i_0 \in I \). Clearly \( e_0 \neq 1H_{i_0} \); thus, there exists some \( T^*[1,e_0] \)-neighbour of \( 1H_{i_0} \) other than 1, necessarily some \( h_0 \in H_{i_0} - \{ 1 \} \). Now \( h_0 \in T^*[1,e_0] \), \( 1 \in T^*[\overline{h_0},\overline{h_0}e_0] \), \( \chi(\overline{h_0}) \neq \chi(\overline{h_0}e_0) \), and \( ||g_3||_E \geq \min \{ ||\overline{h_0}||_E, ||\overline{h_0}e_0||_E \} \). We know that \( e_0 \in E - \{ h_0 \} \) and \( h_0 \in H_{i_0} - \{ 1 \} \). Hence, \( 1 \not\in \{ \overline{h_0}, \overline{h_0}e_0 \} \) and \( g_3 \neq 1 \). There exists a unique \( e_* \in E^{\pm 1} \) such that \( ||ge_*||_E = ||g_3||_E - 1 \). Clearly, \( e_* \not\in \{ 1, e_3 \} \).

Let us review the graph of interest. In \( T \), define link \( T(1) \) and \( \tau T(1) \) as for \( T^* \). For each \( e \in E^{\pm 1} \cup \{ 1 \} \), there exists a unique component \( [e] \in \tau T(1) \) such that \( e \in [e] \). Then the map \( E^{\pm 1} \cup \{ 1 \} \to \tau T(1), e \mapsto [e] \), is bijective. Fix an edge \( (e', e'') \) of \( WH_{\rho}(\cup H_i \text{ rel } E) \). Here, there exist \( i \in I, h \in H_i - \{ 1 \} \), and \( g', g'' \in F \) such that \( h = g'\tau' e'' \cdot g'' \) with no \( E^{\pm 1} \)-cancellation, \( g' = 1 \) if \( e' = 1 \), and \( g'' = 1 \) if \( e'' = 1 \). Thus, \( e'g'h = e''g'' \), \( e'g'H_i = e''g''H_i \), \( e'g' \in [e'] \), and \( e''g'' \in [e''] \); it may happen that \( e' = 1 = g' \) and \( [e'] = \{ 1 \} \).

We now return to \( g_5 \) and \( e_* \). We see that \( 1 \in g_5[e_*], \delta \subseteq g_5 \text{ link } (T(1) \cup g_5[e_*]) \), and \( \chi \) is constant on the vertex-set of each component of \( T - (g_5 \text{ link } T(1) \cup g_5[e_*]) \). We shall show that if \( e_* \not\in \{ e', e'' \} \), then \( \chi(g_5e_*) = \chi(g_5e''). \) As \( e' \neq e_* \), we see \( 1 \not\in g_5[e'] \) and \( \chi \) maps the vertex-set of \( g_5[e'] \) to \{ \chi(g_5e') \}. As \( g_5e' \not\in g_5[e'] \), we see edge \( g_5e' \xrightarrow{\cdot(H_i)} g_5e'g'H_i \not\in \text{ link } T(1) \) and \( \chi(g_5e') = \chi(g_5e''). \) It follows that \( \chi(g_5e') = \chi(g_5e'g'H_i) = \chi(g_5e''g''H_i) = \chi(g_5e'g''). \)

Let \( W \) denote the graph that is obtained from \( WH_{\rho}(\cup H_i \text{ rel } E) \) by removing \( e_* \) and its incident edges. We have now proved that \( \chi(g_5 - ) \) is constant on the vertex-sets of the components of \( W \). Since \( 1 \) and \( e_3 \) are vertices of \( W \) such that \( \chi(g_51) \neq \chi(g_5e_3) \), we see that \( W \) is not connected, and, hence, \( e_* \) is a Whitehead cut-vertex of \( WH_{\rho}(\cup H_i \text{ rel } E) \).

3.3 Corollary. With Hypotheses 1.2, suppose that \( WH_{\rho}(Z \text{ rel } E) \) has no Whitehead cut-vertices. For each free-product factorization \( \langle E| \rangle = \bigstar_{i \in I} H_i \) such that \( Z \subseteq \bigcup_{i \in I} H_i \), the set \( E \) contains a basis of each \( H_i \).

Proof. Let \( i \) range over \( I \). Set \( E_i := E \cap H_i \). Then the \( E_i \) are pairwise disjoint. As it contains \( WH_{\rho}(Z \text{ rel } E) \), \( WH_{\rho}(\cup H_i \text{ rel } E) \) has no Whitehead cut-vertices. By the contrapositive of Theorem 3.2, \( E \subseteq \bigcup_{i \in I} H_i \). Thus, \( E = \bigcup_{i \in I} E_i \). Hence, \( \langle E| \rangle = \bigstar_{i \in I} \langle E_i \rangle \leq \bigstar_{i \in I} H_i = \langle E| \rangle \). It follows that \( \langle E_i \rangle = H_i \) and, hence, \( E_i \) is a basis of \( H_i \).

3.4 Whitehead’s cut-vertex lemma. With Hypotheses 1.2, suppose that \( WH_{\rho}(Z \text{ rel } E_2) \) has no Whitehead cut-vertices. If \( Z \) is a sub-basis of \( \langle E| \rangle \), then \( Z \subseteq E^{\pm 1} \). Hence, \( Z \) is a sub-basis of \( \langle E| \rangle \) if and only if \( Z \cap Z^{-1} = \emptyset \) and \( Z \subseteq E^{\pm 1} \); in this event, \( Z \cup (E - Z^{\pm 1}) \) is a basis of \( \langle E| \rangle \).

Proof. Let \( E' \) be a basis of \( \langle E| \rangle \) that contains \( Z \). A classic \( E' \)-length argument due to Nielsen shows that \( E' \cap \langle E_2 \rangle \) is contained in some basis \( X \) of \( \langle E_2 \rangle \); we shall mention Schreier’s proof in Review 1.1. Now \( \langle E_2 \rangle = \bigstar_{x \in X} \langle x \rangle \) and \( Z \subseteq E' \cap \langle E_2 \rangle \subseteq X \subseteq \bigcup_{x \in X} \langle x \rangle \). By Corollary 3.3, \( E_2 \) contains a basis of each \( \langle x \rangle \), necessarily \( \{ x \} \) or \( \{ x \} \). Thus \( E_2^{\pm 1} \geq X \geq Z \).
We shall use the following strong form in the next section.

3.5 Corollary. If $Z$ is a sub-basis of $\langle E \rangle$ and $Z \not\subseteq E^{+1}$, then there exists some $C \in \text{cuts}(E)$ such that $\text{Wh}_a(Z \text{ rel } E) \subseteq \text{Wh}_a(C)$ and $||Z^{\infty_c}||_E < ||Z||_E$.

Proof. By the contrapositive of Lemma 3.4, $\text{Wh}_a(Z \text{ rel } E)$ has a Whitehead cut-vertex. The result now follows from Algorithm 2.3.

It remains to discuss free-product factors.

3.6 Review. • We now sketch a proof of a result of Kurosh: for any subgroups $H$ and $K$ of any group $F$, if $K$ is a free-product factor of $F$, say $F = K \ast L$, then $H \cap K$ is a free-product factor of $H$. We shall use Bass-Serre theory, although for our purposes the case $F = \langle E \rangle$ and the graph-theoretic techniques of John R. Stallings [5] would suffice. We may view BassSerre($F$, $(K,L)$) as an $H$-tree, and then the vertex $1K$ can be extended to a fundamental $H$-transversal. The resulting graph of groups has $H \cap K$ as one of the vertex-groups and all the edge-groups are trivial. By another result of Bass and Serre, $H \cap K$ is a free-product factor of $H$. See, for example, [2, Theorem I.4.1]. It follows that, for any group, the set of all its free-product factors is closed under finite intersections.

• Recall Hypotheses 1.2 and set $F := \langle E \rangle$. Now $|E|$ bounds the length of any strictly descending chain of free-product factors of $F$. Hence, the set of all the free-product factors of $F$ is closed under arbitrary intersections.

In particular, $\text{Cl}(Z)$, the intersection of all the free-product factors of $F$ containing $Z$, is the $\subseteq$-smallest free-product factor of $F$ containing $Z$.

By Kurosh’s result again, $\text{Cl}(Z) \cap \langle E_Z \rangle$ is a free-product factor of $\langle E_Z \rangle$. However, $\langle E_Z \rangle$ contains $\text{Cl}(Z)$, since $\langle E_Z \rangle$ is a free-product factor of $F$ which contains $Z$. Thus, $\text{Cl}(Z)$ is a free-product factor of $\langle E_Z \rangle$. In particular, the bases of $\text{Cl}(Z)$ are the minimal-size supports of $Z$ with respect to bases of $F$.

3.7 Strong’s cut-vertex lemma. With Hypotheses 1.2, suppose that $\text{Wh}_a(Z \text{ rel } E_Z)$ has no Whitehead cut-vertices. Then $E_Z$ is a basis of $\text{Cl}(Z)$, and, for each free-product factorization $\text{Cl}(Z) = \ast_{i \in I} H_i$ such that $Z \subseteq \bigcup_{i \in I} H_i$, the set $E_Z$ contains a basis of each $H_i$.

Proof. We saw in Review 3.6 that there exists some free-product factorization $\langle E_Z \rangle = \text{Cl}(Z) \ast K$, and it is clear that $Z \subseteq \text{Cl}(Z) \cup K$. By Corollary 3.3, $E_Z$ contains some basis $E'$ of $\text{Cl}(Z)$. Since $Z \subseteq \text{Cl}(Z) = \langle E' \rangle$, we see that $\text{supp}(Z \text{ rel } E) \subseteq E'$, that is, $E_Z \subseteq E'$. Hence, $E_Z$ is a basis of $\text{Cl}(Z)$. The result now follows from Corollary 3.3.
4 A strengthened Clifford-Goldstein algorithm

Clifford and Goldstein [1] produced an ingenious algorithm which returns an element of \( \langle Z \rangle \) that lies in a basis of \( \langle E \rangle \) or reports that no element of \( \langle Z \rangle \) lies in a basis of \( \langle E \rangle \). They used Whitehead’s three-manifold techniques to construct a sufficiently large finite set of finitely generated subgroups of \( \langle E \rangle \) whose elements of sufficiently bounded \( E \)-length give the desired information.

In this section, we restructure their argument, bypassing the topology and obtaining a less complicated, more powerful algorithm which yields as output a basis \( E'' \) of \( \langle E \rangle \) which maximizes \( |E'' \cap \langle Z \rangle| \). In particular, \( E'' \cap \langle Z \rangle = \emptyset \) if and only if no element of \( \langle Z \rangle \) lies in a basis of \( \langle E \rangle \). We construct a smaller sufficiently large finite set of finitely generated subgroups of \( \langle E \rangle \) whose intersections with \( E \) give the desired information.

To fix notation, we sketch the proof of Schreier [11, publ. 1927] that subgroups of free groups are free. The finitely generated case had been proved by J. Nielsen [3, publ. 1921, in Danish].

4.1 Review. With Hypotheses [12], set \( F := \langle E \rangle \) and \( T := \text{Cayley}(F, E) \); see Review 3.1. Let \( H \) be a subgroup of \( F \). The vertices of the Schreier graph \( H \backslash T \) are the cosets \( Hg, g \in F \), the basepoint is \( H1 \), and we write \( \text{edge}(v \cdot e, v) := (v, e) \in (H \backslash F) \times E \). The graph \( H \backslash T \) is connected. Let \( \pi(H \backslash T, H1) \) denote the fundamental group of \( H \backslash T \) at the basepoint \( H1 \). Each (reduced) \( H \backslash T \)-path from \( H1 \) to itself will be viewed as a (reduced) \( E^{\pm1} \)-expression for some element of \( H \); for example, we would view

\[
(H1 \xrightarrow{\varepsilon_1} He_1 \xrightarrow{\varepsilon_2} He_1\overline{e}_2 \xrightarrow{\varepsilon_3} He_1\overline{e}_2e_3 = H1)
\]

as the \( E^{\pm1} \)-expression \( e_1\overline{e}_2e_3 \) for an element of \( H \). Hence, we may identify \( \pi(H \backslash T, H1) \) with \( H \).

Choose a maximal subtree \( Y' \) of \( H \backslash T \) and let \( Y'' \) denote the complement of \( Y' \) in \( H \backslash T \); then \( Y'' \) is a set of edges. Each element \( y'' \) of \( Y'' \) determines the element of \( \pi(H \backslash T, H1) \) that travels in \( Y' \) from \( H1 \) to the initial vertex of \( y'' \), travels along \( y'' \), and then travels in \( Y' \) from the terminal vertex of \( y'' \) to \( H1 \). By letting \( y'' \) range over \( Y'' \), we get a subset \( S \) of \( \pi(H \backslash T, H1) \). By collapsing the tree \( Y' \) to a vertex, we find that \( S \) freely generates \( \pi(H \backslash T, H1) \) (= \( H \)).

The vertices and edges involved in \( S \) form a connected basepointed subgraph of \( H \backslash T \) denoted \( \text{core}_s(H \text{ rel } E) \). An alternative description is that \( \text{core}_s(H \text{ rel } E) \) consists of those vertices and edges that are involved in the reduced \( H \backslash T \)-paths from \( H1 \) to itself. Thus, \( \pi(\text{core}_s(H \text{ rel } E), H1) = H \) and \( \text{core}_s(H \text{ rel } E) \) is the \( \subseteq \)-smallest subgraph of \( H \backslash T \) with this property.

For each \( h \in E \cap H \), it is clear that edge\((H1 \xrightarrow{(h)} Hh = H1)\) is not in the tree \( Y' \), and, hence, \( h \in S \). Thus, \( E \cap H \subseteq S \). (I am indebted to Clifford and Goldstein for this paragraph.)
4.2 Algorithm. Stallings’ core algorithm [5, Algorithm 5.4] has the following structure.

With Hypotheses 1.2 we shall suppress the information that the vertices of core,\( \langle Z \rangle_{rel} E \) are certain cosets, and we shall build a basepointed \( E \)-labelled graph, denoted modelcore,\( \langle (Z) \rangle_{rel} E \), that has an abstract set as vertex-set and is isomorphic to core,\( \langle (Z) \rangle_{rel} E \) as basepointed \( E \)-labelled graph.

For each \( z \in Z \), we easily build modelcore,\( \langle (z) \rangle_{rel} E \) as a basepointed \( E \)-labelled lollipop graph, possibly trivial, using the reduced \( E^\pm \)-expression for \( z \).

We next amalgamate all these lollipop graphs at their basepoints. Throughout the construction, each edge will be assigned an expression of the form \( \text{edge}(v \rightarrow w) \) with \( v, w \) vertices and \( e \in E \), but, for the moment, the expression need not determine the edge. While possible, we identify some distinct pair of edges with expressions \( \text{edge}(v \rightarrow w) \) and \( \text{edge}(v' \rightarrow w') \) where \( v = v' \) or \( w = w' \) or both; identifying the edges entails identifying \( w \) with \( w' \) or \( v \) with \( v' \) or neither, respectively. When no such pair of distinct edges is left, the procedure has yielded a basepointed \( E \)-labelled graph isomorphic to core,\( \langle (Z) \rangle_{rel} E \); here, expressions \( \text{edge}(v \rightarrow w) \) do determine edges.

Stallings gave the name folding to the foregoing edge-identifying process. The process itself had long been used unnamed, notably by Lyndon in his work on planar diagrams, where each nontrivial lollipop graph has a two-cell attached making a contractible CW-complex.

We now give the (strange) key construction of [1, Theorem 1].

4.3 Notation. With Hypotheses 1.2 fix \( C = (D_0, D_1, e_* \in \text{Cuts}(E)) \) and set \( F := \langle E \rangle, \eta := \eta_C, d_* := e_2^{e-1}, \) and \( \varphi := \varphi_C \); see Notation 2.1.

We first construct an \( F \)-map \( \psi_C \) from the edge-set of \( T := \text{Cayley}(F, E) \) to the edge-set of \( T' := \text{Cayley}(F, E^\varphi) \). For any edge \( (g \rightarrow ge) \in F \times E \), there exists a unique \( (\alpha, \beta) \in \{0, 1\} \times 2 \) such that \( e \in E_{\alpha}E_{\beta} \) and \( e^\varphi = d_\alpha d_\beta \); if \( e^\pm \neq e^\pm_1 \), these two conditions are equivalent, while if \( e^\pm = e^\pm_1 \), the two conditions together say that \( \alpha = \beta = \eta \). We set \( (\text{edge}(g \rightarrow ge))^{\psi_C} := \text{edge}(gd_\alpha \rightarrow gd_\beta) \); we emphasize that no action of \( \psi_C \) on vertices is being defined. It is clear that \( \psi_C \) is an \( F \)-map.

Let \( H \) be a finitely generated subgroup of \( F \). Then \( \psi_C \) induces a set map from the edge-set of \( H \backslash T \) to the edge-set of \( H \backslash T' \), and the image of the edge-set of core,\( \langle H \rangle_{rel} E \) under this induced map is then the edge-set of a unique subgraph \( X \) of \( H \backslash T' \) with the full vertex-set, \( H \backslash F \). Let \( K := \pi(X, H1) \leq \pi(H \backslash T', H1) \).

We may identify the latter group with \( H \), where \( (H \backslash T') \)-paths are \( (E^\varphi)^\pm \)-expressions. We set \( \partial CH := K^\varphi \leq H^\varphi \). Recall that modelcore,\( \langle (H) \rangle_{rel} E \) was constructed in Algorithm 4.2 we shall be viewing \( \partial CH \) as a graph operation that converts modelcore,\( \langle (H) \rangle_{rel} E \) into modelcore,\( \langle (\partial CH) \rangle_{rel} E \).
4.4 Lemma. With the foregoing notation, the following hold for $\partial CH \leq H^{\partial \mathcal{C}}$.

(i) modelcore,$(\partial CH \text{ rel } E)$ may be constructed algorithmically.

(ii) core,$(H \text{ rel } E)$ has at least as many edges as core,$(\partial CH \text{ rel } E)$.

(iii) For each $z \in H$, if $WH_z \{z\} \text{ rel } E \subseteq WH_z(C)$, then $z^{\partial \mathcal{C}} \in \partial CH$.

(iv) If $Y$ is any sub-basis of $\langle E \rangle$ such that $Y \subseteq H$ and $Y \not\subseteq E^{\pm 1}$, then there exists some $C' \in \text{CUTS}(E)$ such that $Y^{\partial \mathcal{C}} \subseteq \partial CH$ and $||Y^{\partial \mathcal{C}}||_E < ||Y||_E$.

Proof. (i). Since $K^{\partial \mathcal{C}} = \partial CH$, there is a natural graph isomorphism that maps $\text{core}_a(K \text{ rel } E^{\circ})$ to $\text{core}_a(\partial CH \text{ rel } E)$, changing each $Kg \xrightarrow{\text{core}_a} Kg(e^\circ)$ to $K^{\partial \mathcal{C}}g^{\partial \mathcal{C}} e^\circ$. Hence, there is a natural graph isomorphism that maps $\text{modelcore}_a(K \text{ rel } E^{\circ})$ to $\text{modelcore}_a(\partial CH \text{ rel } E)$, changing each $v \xrightarrow{\text{modelcore}_a} w$ to $v \xrightarrow{\text{modelcore}_a} w$; the labels on the non-basepoint vertices are irrelevant. Thus, it suffices to algorithmically construct $\text{modelcore}_a(K \text{ rel } E^{\circ})$ from $\text{modelcore}_a(H \text{ rel } E)$.

If $d_\ast \in E$, resp. $\overrightarrow{d_\ast} \in E$, we say that a vertex $v$ of $\text{modelcore}_a(H \text{ rel } E)$ has a neighbour $v\overrightarrow{d_\ast}$ if an edge of the form edge$(w \xrightarrow{d_\ast} v)$, resp. edge$(v \xrightarrow{\overrightarrow{d_\ast}} w)$, lies in $\text{modelcore}_a(H \text{ rel } E)$; in this event, we say that $w$ is $v\overrightarrow{d_\ast}$. We simultaneously add to $\text{modelcore}_a(H \text{ rel } E)$, for every vertex $v$ that does not have a neighbour $v\overrightarrow{d_\ast}$, a valence-zero vertex with label $v\overrightarrow{d_\ast}$.

Next, in $\text{modelcore}_a(H \text{ rel } E)$ adorned with the valence-zero vertices, we simultaneously replace each edge$(v \xrightarrow{\text{core}_a} w)$ with edge$(v\overrightarrow{\alpha} \xrightarrow{\text{core}_a} w\overrightarrow{\beta})$ for the unique $(\alpha, \beta) \in \{0, 1\}^2$ such that $e \in \alpha E_\beta$ and $e^\circ = d_\alpha \overrightarrow{\beta}. \overrightarrow{\phi}. \overrightarrow{\epsilon}$. This particular operation alters incidence maps and edge labellings, but not the vertex-set or the edge-set.

In the resulting finite graph, we then keep only the component that has the basepoint. We next successively delete non-basepoint, valence-one vertices and their (unique) incident edges, while possible. When this is no longer possible, we have constructed $\text{modelcore}_a(K \text{ rel } E^{\circ})$ algorithmically.

(ii). It is clear from the constructions that $\text{core}_a(H \text{ rel } E)$ has at least as many edges as $\text{core}_a(K \text{ rel } E^{\circ})$, which in turn has the same number of edges as $\text{core}_a(\partial CH \text{ rel } E)$.

(iii). Consider any expression $Hg \xrightarrow{\text{core}_a} Hge$ corresponding to an edge or inverse edge in $\text{core}_a(H \text{ rel } E)$, and consider any $(\alpha, \beta) \in \{0, 1\}^2$ such that $e \in \alpha D_\beta$.

Then $d_\alpha \overrightarrow{\beta} = \{e^\circ, 1\}$, for, if $d_\alpha \overrightarrow{\beta} \neq e^\circ$, then either $e = e_\ast$, $\alpha = 1 - \eta$, $\beta = \eta$, $d_\alpha \overrightarrow{\beta} = d_\ast^{1-\eta} e_\ast = 1$, or $e = \epsilon_\ast$, $\alpha = \eta$, $\beta = 1 - \eta$, $d_\alpha \overrightarrow{\beta} = d_\ast^{1+\eta} \epsilon_\ast = 1$. This means that the expression $Hg\overrightarrow{\alpha} \xrightarrow{d_\alpha \overrightarrow{\beta}} Hge\overrightarrow{\beta}$ corresponds to an edge, inverse edge, or equality in the graph $X$ of Notation 4.3.

Suppose that $z \in H$ and let $e_1 e_2 \cdots e_n$ represent the reduced $E^{\pm 1}$-expression for $z$. We then have a corresponding reduced $H \setminus T$-path from $H1$ to itself, which we may write in $H \setminus \text{Cayley}(F, E^{\pm 1})$ as $H1 \xrightarrow{\text{core}_a} H e_1 \xrightarrow{\text{core}_a} H e_1 e_2 \xrightarrow{\text{core}_a} \cdots \xrightarrow{\text{core}_a} H e_1 e_2 \cdots e_n = H z = H1.$
The $H \setminus T$-path must then stay within the subgraph $\text{core}_s(H \text{ rel } E)$.

Suppose further that $\forall H, \{ \{ \} \text{ rel } E \} \subseteq \forall H, \{ C \}$. This means that there exists a (unique) set map $\{ \{ 0, 1, \ldots, n \} \rightarrow \{ 0, 1 \}, i \mapsto \chi_i$, such that $e_i \in x_{i+1} \cdot \text{core}_s (x_i, \text{ rel } E)$, $i = 1, 2, \ldots, n$, and $\chi_0 = \chi_n = 0$. In our $\text{core}_s(H \text{ rel } E)$-path, let us change each vertex $H e_1 \cdots e_i$ to $H e_1 \cdots e_i \cdot d_{x_i}^{\chi_i}$ and each step $H e_1 \cdots e_i \cdot e_i$ to $H e_1 \cdots e_i \cdot e_i \cdot d_{x_i}^{\chi_i}$, which we have seen corresponds to an edge, inverse edge, or equality in $X$. We thus obtain an $X$-path from $H_1$ to itself that reads an $(\langle E^* \rangle_{(1)} \cup \{ 1 \})$-expression for $z$. This shows that $z \in \pi(X, H1) = K$, as desired.

(iv). By Corollary 3.5, there exists $\forall C' \in \text{cups}(E)$ such that $|Y^C_1| < |Y|_E$ and $\forall H, \{ \{ \} \text{ rel } E \} \subseteq \forall H, \{ C' \}$. By (iii), $Y^C_1 \subseteq \partial_{C'} H$.

We now give a construction that is a somewhat less complicated variant of the algorithm of Clifford and Goldstein [1].

4.5 Notation. With Hypotheses 1.2 let $\mathcal{F}$ denote the set of all finitely generated subgroups of $\langle E \rangle$. Let $\Gamma$ denote the graph whose vertex-set is $\mathcal{F}$ and whose edge-set is $\mathcal{F} \times \text{cups}(E)$ where each edge $(H, C) \in \mathcal{F} \times \text{cups}(E)$ has initial vertex $H$ and terminal vertex $\partial_C H$; see Notation 1.3.

Set $G := \langle Z \rangle \in \mathcal{F}$. Let $(G \sqsubset)$ denote the subgraph of $\Gamma$ that radiates out from $G$, that is, $(G \sqsubset)$ is the smallest subgraph of $\Gamma$ that has $G$ as a vertex and is closed in $\Gamma$ under the operation of adding to each vertex $H$ each outgoing edge $(H, C)$ and its terminal vertex $\partial_C H$.

For each $n \geq 0$, each element $(C_i)_{i=1}^n$ of $(\text{cups}(E))_{i=1}^n$ determines the oriented $(G \sqsubset)$-path with the edge-sequence $(H_i (H_i, C_i) H_{i+1})_{i=1}^n$ where $H_1 = G$ and $H_{i+1} = \partial_C H_i$ for $i = 1, \ldots, n$. To simplify notation, we shall say that $(C_i)_{i=1}^n$ itself is an oriented $(G \sqsubset)$-path with initial vertex $G$.

We usually think of a vertex $H$ of $(G \sqsubset)$ as the graph model$\text{core}_s(H \text{ rel } E)$, for ease of recognition. We shall see that we are interested in finding a vertex that maximizes the number of loops at the basepoint.

4.6 Theorem. With the foregoing notation, the following hold.

(i) $(G \sqsubset)$ is an algorithmically constructible finite graph whose vertices are viewed as finite, $E$-labelled, basepointed graphs.

(ii) For each vertex $H$ of $(G \sqsubset)$, there is an algorithmically constructible oriented $(G \sqsubset)$-path $(C_i)_{i=1}^n$ from $G$ to $H$, $H = \partial_{C_n} \cdots \partial_{C_1} G \subseteq G \overrightarrow{C_n \cdots C_1}$, and $(E \cap H) \overrightarrow{\partial_{C_n} \cdots \partial_{C_1}} \subseteq E'' \cap G$, where $E'' := E \overrightarrow{\partial_{C_n} \cdots \partial_{C_1}}$.

(iii) For each basis $E''$ of $\langle E \rangle$, there exists some vertex $H$ of $(G \sqsubset)$ such that $|E \cap H| \geq |E'' \cap G|$.

Proof. (i). For each $H \in \mathcal{F}$, if $n$ denotes the number of edges in $\text{core}_s(H \text{ rel } E)$, it is clear from Review 4.4 that $H$ can be generated by $n$-or-less elements of $\langle E \rangle$ of $E$-length $2n$-or-less. By Lemma 4.3(ii), $(G \sqsubset)$ is finite. By Lemma 4.3(i), we
Sandwiching between free-product factors

may use a depth-first search to construct a maximal subtree of \((G\blacklozenge)\). We then add the missing edges of \((G\blacklozenge)\), although this is optional for our purposes.

(ii) is clear.

(iii). It follows from Lemma 1.3(iv) that there exists some \((C_i)_{i=1}^{n}\) such that \((E'' \cap G) \subseteq E^{\pm 1} \cap \partial C_n \cdots \partial C_2 \partial C_1 G\).

We now construct a basis \(E''\) of \(\langle E \rangle\) which maximizes \(\vert E'' \cap \langle Z \rangle \vert\).

4.7 Algorithm. Recall Hypotheses 1.2.

- Set \(G := \langle Z \rangle\) and construct modelcore\(_*\)(\(G\ rel\ E\)); see Algorithm 4.2.
- Construct \((G\blacklozenge)\) from modelcore\(_*\)(\(G\ rel\ E\)); see Theorem 4.6(i).
- In \((G\blacklozenge)\), find a vertex \(H\) maximizing the number of loops at the basepoint of modelcore\(_*\)(\(H\ rel\ E\)), that is, maximizing \(\vert E \cap H \vert\).
- Find an oriented \((G\blacklozenge)-\)path \((C_i)_{i=1}^{n}\) from \(G\) to \(H\); see Theorem 4.6(ii).
- Return \(E'' := E \phi C_n \cdots \phi C_2 \phi C_1\), a basis of \(\langle E \rangle\) which maximizes \(\vert E'' \cap \langle Z \rangle\) by Theorem 4.6(ii),(iii).

References

[1] A. Clifford and R. Z. Goldstein, Subgroups of free groups and primitive elements, J. Group Theory 13 (2010), 601–611.

[2] Warren Dicks and M. J. Dunwoody, Groups acting on graphs, Camb. Stud. Adv. Math. 17, CUP, 1989. xvi + 283 pp. Errata at: http://mat.uab.cat/~dicks/DDerr.html

[3] J. Nielsen, Om Regnung med ikke kommutative Faktoren og dens Anvendelse i Gruppeterorien, Math. Tidsskrift B 107 (1921), 77–94.

[4] O. Schreier, Die Untergruppen der freien Gruppen, Abh. Math. Univ. Hamburg 5 (1927), 161–183.

[5] John R. Stallings, Topology of finite graphs, Invent. Math. 71 (1983), 551–565.

[6] Richard Stong, Diskbusting elements of the free group, Math. Res. Lett. 4 (1997), 201–210.

[7] Edward C. Turner, Test words for automorphisms of free groups, Bull. London Math. Soc. 28 (1996), 255–263.

[8] J. H. C. Whitehead, On certain sets of elements in a free group, Proc. London Math. Soc. 41 (1936), 48–56.

[9] J. H. C. Whitehead, On equivalent sets of elements in a free group, Ann. of Math. 37 (1936), 782–800.