Variations on the Post Correspondence Problem for free groups

Laura Ciobanu and Alan D. Logan

Heriot-Watt University, Edinburgh EH14 4AS, Scotland
{L.Ciobanu,A.Logan}@hw.ac.uk

Abstract. The Post Correspondence Problem is a classical decision problem about equalisers of free monoid homomorphisms. We prove connections between several variations of this classical problem, but in the setting of free groups and free group homomorphisms. Among other results, and working under certain injectivity assumptions, we prove that computing the rank of the equaliser of a pair of free group homomorphisms can be applied to computing a basis of this equaliser, and also to solve the “generalised” Post Correspondence Problem for free groups.

Keywords: Post Correspondence Problem, free group, rational constraint.

1 Introduction

In this article we connect several variations of the classical Post Correspondence Problem in the setting of free groups. The problems we consider have been open since the 1980s, and understanding how they relate and compare to their analogues in free monoids could bring us closer to their resolution. All problems are defined in Table 1 while their status in free groups and monoids is given in Table 2. However, three of these problems deserve proper introductions.

The first problem we consider is the Post Correspondence Problem (PCP) for free groups. This is completely analogous to the classical Post Correspondence Problem, which is about free monoids rather than free groups, and has had numerous applications in mathematics and computer science [11]. The PCP for other classes of groups has been successfully studied (see for example [17, Theorem 5.8]), but it remains open for free groups, where it is defined as follows. Let \( \Sigma \) and \( \Delta \) be two alphabets, let \( g, h : F(\Sigma) \to F(\Delta) \) be two group homomorphisms from the free group over \( \Sigma \) to the free group over \( \Delta \), and store this data in a four-tuple \( I = (\Sigma, \Delta, g, h) \), called an instance of the PCP. The PCP is the decision problem:

Given \( I = (\Sigma, \Delta, g, h) \), is there \( x \in F(\Sigma) \setminus \{1\} \) such that \( g(x) = h(x) \)?

That is, if we consider the equaliser \( \operatorname{Eq}(g, h) = \{ x \in F(\Sigma) \mid g(x) = h(x) \} \) of \( g \) and \( h \), the PCP asks if \( \operatorname{Eq}(g, h) \) is non-trivial. Determining the decidability of this problem is an important question [6, Problem 5.1.4] [17, Section 1.4].

* Supported by EPSRC grant EP/R035814/1
Our second problem asks not just about the triviality of $\text{Eq}(g, h)$, but for a finite description of it. We write $\text{PCP}^{\text{inj}}$ (see Table 1) for the PCP with at least one map injective, in which case $\text{Eq}(g, h)$ is finitely generated \[^{[10]}\] and a finite description relates to bases: The *Basis Problem* (BP) takes as input an instance $I = (\Sigma, \Delta, g, h)$ of the $\text{PCP}^{\text{inj}}$ and outputs a basis for $\text{Eq}(g, h)$. In Section \[^{[7]}\] we show that the BP is equivalent to the *Rank Problem* (RP), which seeks the number of elements in the basis, and was asked by Stallings in 1984. Recent results settle the BP for certain classes of free group maps \[^{[2–4, 8]}\], but despite this progress its solubility remains open in general. The analogous problem for free monoids, which we call the *Algorithmic Equaliser Problem* (AEP) (see \[^{[4]}\] page 2) because it aims to describe the equaliser in terms of automata rather than bases, is insoluble \[^{[14]}\] Theorem 5.2.

Our third problem is the *generalised* Post Correspondence Problem (GPCP), which is an important generalisation of the PCP for both free groups and monoids from 1982 \[^{[7]}\]. For group homomorphisms $g, h : F(\Sigma) \to F(\Delta)$ and fixed elements $u_1, u_2, v_1, v_2$ of $F(\Delta)$, an instance of the GPCP is an 8-tuple $I_{\text{GPCP}} = (\Sigma, \Delta, g, h, u_1, u_2, v_1, v_2)$ and the GPCP itself is the decision problem:

Given $I_{\text{GPCP}} = (\Sigma, \Delta, g, h, u_1, u_2, v_1, v_2)$, is there $x \in F(\Sigma) \setminus \{1\}$ such that $u_1 g(x) u_2 = v_1 h(x) v_2$?

| Problems (for free groups) | Fixed: finite alphabets $\Sigma$ and $\Delta$ and free groups $F(\Sigma), F(\Delta)$. Input: homomorphisms $g, h : F(\Sigma) \to F(\Delta)$ |
|---------------------------|------------------------------------------------------------------------------------------------------------------|
|                           | Additional input for GPCP: $u_1, u_2, v_1, v_2 \in F(\Delta)$                                                  |
|                           | Additional input for $\text{PCP}_R$: rational set $R \subseteq F(\Sigma)$                                    |
|                           | Additional input for $\text{PCP}_{\Sigma \subseteq \Omega}$: $a, b \in \Sigma^\pm 1, \Omega \subseteq \Sigma$ |
|                           | Is it decidable whether:                                                                                         |
| $\text{PCP}$              | there exists $x \in F(\Sigma) \setminus \{1\}$ s.t. $g(x) = h(x)$?                                              |
| $\text{GPCP}$             | there exists $x \in F(\Sigma) \setminus \{1\}$ s.t. $u_1 g(x) u_2 = v_1 h(x) v_2$?                         |
| $\text{PCP}_R$            | there exists $x \neq 1$ in $R$ s.t. $g(x) = h(x)$?                                                            |
| $\text{PCP}_{\Sigma \subseteq \Omega}$ | there exists $x \in F(\Sigma) \setminus \{1\}$ s.t. $g(x) = h(x)$ and $x$ decomposes as a freely reduced word $ayb$ for some $y \in F(\Omega)$ |
| $\text{PCP}^{\text{inj}, \text{inj}}$ | $\text{PCP}$ with neither $g$, nor $h$ injective                                                     |
| $\text{PCP}^{\text{inj}, \text{inj}}$ | $\text{PCP}$ with exactly one of $g$, $h$ injective                                                         |
| $\text{PCP}^{\text{inj}}$ | $\text{PCP}^{\text{inj}, \text{inj}} \cup \text{PCP}^{\text{inj}, \text{inj}}$ (i.e. $\text{PCP}$ with at least one of $g$, $h$ injective) |
| $\text{PCP}^{\text{CI}}$ | $\text{PCP}$ with $g, h$ s.t. $g(y) \neq u^{-1} h(y) u$ for all $u \in F(\Delta), y \in F(\Sigma) \setminus \{1\}$ |
| $\text{PCP}^{\text{inj} + \text{CI}}$ | $\text{PCP}^{\text{inj}} \cup \text{PCP}^{\text{CI}}$                                                    |
| $\text{PCP}(n)$           | $\text{PCP}(n)$ for alphabet size $|\Sigma| = n$                                                              |
| GPCP variants             | $\text{GPCP}^{\text{inj}, \text{inj}}, \text{GPCP}^{\text{inj}}, \text{GPCP}^{\text{inj} + \text{CI}}, \text{GPCP}(n)$, etc. |

Table 1: Summary of certain decision problems related to the PCP
Variations on the Post Correspondence Problem for free groups

For free monoids, the PCP is equivalent to the GPCP [11, Theorem 8]. The corresponding connection for free groups is more complicated, and explaining this connection is the main motivation of this article. In particular, the GPCP for free groups is known to be undecidable [17, Corollary 4.2] but this proof does not imply that the PCP for free groups is undecidable (because of injectivity issues; see Section 2). In Theorem 4 we connect the PCP with the GPCP via a sequence of implications, and require at least one map to be injective.

Main theorem Theorem A summarises the connections proven in this paper (arrows are labeled by the section numbers where the implications are proven), and Section 8 brings all the results together. Note that asking for both maps to be injective refines the results in this theorem, as does restricting the size of the source alphabet $\Sigma$ (see Theorem 9).

Theorem A (Theorem 9) In finitely generated free groups the following implications hold.

\[
\begin{align*}
\text{Rank Problem (RP)} & \quad \downarrow^4 \\
\text{Basis Problem (BP)} & \quad \xrightarrow{3} \text{GPCP}^{\text{inj}} \quad \xrightarrow{5} \text{PCP} \quad \xrightarrow{6.2} \text{GPCP}^{\text{inj}} + \text{CI} \\
\text{PCP}^{\text{inj}}_{\mathcal{R}} & \quad \downarrow^4
\end{align*}
\]

This theorem implies that Stallings’ Rank Problem is of central importance, as we have the chain: $\text{RP} \Rightarrow \text{GPCP}^{\text{inj}} \Rightarrow \text{PCP}$.

Rational constraints The implication $\text{BP} \Rightarrow \text{GPCP}^{\text{inj}}$ above is surprising because the inputs to the problems are very different. The proof of this implication uses the PCP$^{\text{inj}}$ with a certain rational constraint, namely the problem PCP$^{\text{inj}}_{\mathcal{L}}$ (see Table 1). The relationship between the GPCP and the PCP$^{\mathcal{L}}$ still holds if neither map is injective. As the GPCP for free groups is undecidable in general, this connection yields the following result.

Theorem B (Theorem 3) There exists a rational constraint $\mathcal{R}$ such that the PCP$^{\mathcal{R}}$ is undecidable.

Random maps and generic behaviour. A different perspective on the PCP and its variations is to consider the behaviour of these problems when the pairs of homomorphisms are picked randomly (while the two alphabets $\Delta = \{x_1, \ldots, x_m\}$ and $\Sigma = \{y_1, \ldots, y_k\}$, and ambient free groups $F(\Delta)$ and $F(\Sigma)$ remain fixed). Any homomorphism is completely determined by how it acts on the generators, and so picking $g$ and $h$ randomly is to be interpreted as picking $(g(x_1), \ldots, g(x_m))$ and $(h(x_1), \ldots, h(x_m))$ as random tuples of words in $F(\Sigma)$ (see Section 6 for
There is a vast literature (see for example [13]) on the types of objects or behaviours which appear with probability 0, called negligible, or with probability 1, called generic, in infinite groups. In this spirit, the generic PCP refers to the PCP applied to a generic set (of pairs) of maps, that is, a set of measure 1 in the set of all (pairs of) maps, and we say that the generic PCP is decidable if the PCP is decidable for ‘almost all’ instances, that is, for a set of measure 1 of pairs of homomorphisms.

In Section 6 we describe the setup used to count pairs of maps and compute probabilities, and show that among all pairs of maps \( g, h \), the property of being conjugacy inequivalent (that is, for every \( u \in F(\Delta) \) there is no \( x \neq 1 \) in \( F(\Sigma) \) such that \( g(x) = u^{-1}h(x)u \); defined in Table 1 as PCP\(_{\text{CI}}\) and GPCP\(_{\text{CI}}\)) occurs with probability 1; that is, conjugacy inequivalent maps are generic:

**Theorem C (Theorem 5)** *Instances of the PCP\(_{\text{inj} + \text{CI}}\) are generic instances of the PCP. That is, with probability 1, a pair of maps is conjugacy inequivalent.*

Theorem C shows that the implication PCP \( \Rightarrow \) GPCP\(_{\text{inj} + \text{CI}}\) in Theorem A is the generic setting, and hence for ‘almost all maps’ we have PCP \( \Leftrightarrow \) GPCP.

We conclude the introduction with a summary of the status the PCP and its variations for free monoids and groups. We aim to study the computational complexity of these problems and how this complexity behaves with respect to the implications proved in this paper in future work.

**Table 2: Status of results for free monoids and free groups**

| Problems          | In free monoids | References for free monoids | In free groups | References for free groups |
|-------------------|-----------------|------------------------------|----------------|----------------------------|
| general PCP       | undecidable     | [19]                         | unknown        |                            |
| general AEP / BP  | undecidable     | [14] Theorem 5.2             | unknown        |                            |
| PCP\(_{\neg \text{inj}, \neg \text{inj}}\) | undecidable     | [19]                         | decidable      | Lemma 1                    |
| PCP\(_{\text{inj}}\)      | undecidable     | [15]                         | unknown        |                            |
| GPCP              | undecidable     | [11] Theorem 8               | undecidable    | [17] Corollary 4.2         |
| GPCP\(_{\neg \text{inj}, \neg \text{inj}}\) | undecidable     | [11] Theorem 8               | undecidable    | Lemma 2                    |
| GPCP\(_{\text{inj}}\)      | undecidable     | [15]                         | unknown        |                            |
| GPCP\(_{\text{inj} + \text{CI}}\) | undecidable     | unknown                      |                |                            |
| PCP\(_{\text{R}}\)       | undecidable     | [19]                         | unknown        |                            |
| PCP\(_{\text{inj} + \text{CI}}\) | undecidable     | [19]                         | decidable      | Theorem 13                 |
| generic PCP       | decidable       | [9] Theorem 4.4              | decidable      | [5]                        |

2 Non-injective maps

In this section we investigate the PCP\(_{\neg \text{inj}, \neg \text{inj}}\) and GPCP\(_{\neg \text{inj}, \neg \text{inj}}\), which are the PCP and GPCP under the assumption that both maps are non-injective.
The PCP for non-injective maps We first prove that the PCP$(\neg \text{inj}, \neg \text{inj})$ is trivially decidable, with the answer always being “yes”.

**Lemma 1.** If $g, h : F(\Sigma) \to F(\Delta)$ are both non-injective homomorphisms then $\text{Eq}(g, h)$ is non-trivial.

**Proof.** We prove that $\ker(g) \cap \ker(h)$ is non-trivial, which is sufficient. Let $c \in \ker(g)$ and $d \in \ker(h)$ be non-trivial elements. If $\langle c, d \rangle \not\cong \mathbb{Z} = \langle x \rangle$, there exist integers $k, l$ such that $c = x^k$ and $d = x^l$. Then $g(x^{kl}) = 1 = h(x^{kl})$ so $x^{kl} \in \ker(g) \cap \ker(h)$ with $x^{kl}$ non-trivial, as required. If $\langle c, d \rangle \cong \mathbb{Z}$ then $g([c, d]) = 1 = h([c, d])$, so $[c, d] \in \ker(g) \cap \ker(h)$ with $[c, d]$ non-trivial, as required. $\square$

As we can algorithmically determine if a free group homomorphism is injective (e.g. via Stallings’ foldings), Lemma 1 gives us the following:

**Proposition 1.** $\text{PCP} \iff \text{PCP}(\neg \text{inj}, \neg \text{inj})$

The GPCP for non-injective maps Myasnikov, Nikolaev and Ushakov defined the PCP and GPCP for general groups in [17]. Due to this more general setting their formulation is slightly different to ours but, from a decidability point of view, the problems are equivalent for free groups. They proved that the GPCP is undecidable for free groups; however, we now dig into their proof and observe that it assumes both maps are non-injective. Therefore, GPCP$^{\text{inj}}$ remains open.

**Lemma 2.** The GPCP$(\neg \text{inj}, \neg \text{inj})$ is undecidable.

**Proof.** Let $H$ be a group with undecidable word problem and let $\langle x \mid r \rangle$ be a presentation of $H$. Set $\Delta := x$, define

$$\Sigma := \{(x, 1) \mid x \in x\} \cup \{(1, x^{-1}) \mid x \in x\} \cup \{(R, 1) \mid x \in r\} \cup \{(1, R^{-1}) \mid R \in r\}$$

and define $g : (p, q) \mapsto p$ and $h : (p, q) \mapsto q$. Note that neither $g$ nor $h$ is injective, as if $R \in r$ then $g(R, 1)$ may be realised as the image of a word over $\{(x, 1) \mid x \in x\} \cup \{(1, x^{-1}) \mid x \in x\}$, and analogously for $h(1, R)$. Taking $w \in F(\Delta)$, the instance $(\Sigma, \Delta, g, h, w, 1, 1, 1)$ of the GPCP$(\neg \text{inj}, \neg \text{inj})$ has a solution if and only if the word $w$ defines the identity of $H$ [17, Proof of Proposition 4.1]. As $H$ has undecidable word problem it follows that the GPCP$(\neg \text{inj}, \neg \text{inj})$ is undecidable. $\square$

3 The GPCP and extreme-letter restrictions

In this section we connect the GPCP and the PCP under a certain rational constraint. This connection underlies Theorem [3] as well as the implications $\text{BP} \Rightarrow \text{GPCP}^{\text{inj}}$ and $\text{PCP} \Rightarrow \text{GPCP}^{\text{inj} + \text{CI}}$ in Theorem [4].

Our results here, as in much of the rest of the paper, are broken down in terms of injectivity, and also alphabet sizes; understanding for which sizes of
alphabet Σ the classical Post Correspondence Problem is decidable/undecidable is an important research theme [7, 11, 18].

For an alphabet Σ, let Σ−1 be the set of formal inverses of Σ, and write Σ±1 = Σ ∪ Σ−1. For example, if Σ = {a, b} then Σ±1 = {a, b, a−1, b−1}.

The extreme-letter-restricted Post Correspondence Problem for free groups PCPξε (see also Table I) is the following problem: Let g, h : F(Σ) → F(∆) be two group homomorphisms, Ω ⊂ ∆ a set, and a, b ∈ Σ±1 two letters; an instance of the PCPξε is a 6-tuple IPξε = (Σ, ∆, g, h, a, Ω, b) and the PCPξε itself:

Given IPξε = (Σ, ∆, g, h, a, Ω, b), is there x ∈ F(Σ) \ {1} such that:
- g(x) = h(x), and
- x decomposes as a freely reduced word ayb for some y ∈ F(Ω)?

Connecting the GPCP and the PCP. We start with an instance IGPCP = (Σ, ∆, g, h, u1, u2, v1, v2) of the GPCP and consider the instance

IPCP := (Σ ∪ {B, E}, ∆ ∪ {B, E, #}, g′, h′)

of the PCP, where g′ and h′ are defined as follows.

\[ g'(z) := \begin{cases} 
#^{-1}g(z) # & \text{if } z \in \Sigma \\
B#u1# & \text{if } z = B \\
#^{-1}u2#E & \text{if } z = E 
\end{cases} \]

\[ h'(z) := \begin{cases} 
#h(z) #^{-1} & \text{if } z \in \Sigma \\
B#v1#^{-1} & \text{if } z = B \\
#v2#E & \text{if } z = E 
\end{cases} \]

Injectivity is preserved through this construction since \( \text{rk(Im}(g)) + 2 = \text{rk(Im}(g′)) \); this can be seen via Stallings’ foldings, or directly by noting that the image of g′ restricted to \( F(\Sigma) \) is isomorphic to \( \text{Im}(g) \), that \( B \) only occurs in \( g′(a) \) and \( E \) only occurs in \( g′(e) \). Analogously, \( h′ \) is an injection if and only if \( h \) is, as again \( \text{rk(Im}(h)) + 2 = \text{rk(Im}(h′)) \). Thus we get:

**Lemma 3.** The map \( g′ \) is injective if and only if \( g \) is, and the map \( h′ \) is injective if and only if \( h \) is.

We now connect the solutions of \( IGPCP \) to those of \( IPCP \).

**Lemma 4.** A word \( y \in F(\Sigma) \) is a solution to \( IGPCP \) if and only if the word \( 'ByE' \) is a solution to \( IPCP \).

**Proof.** Starting with \( y \) being a solution to \( IGPCP \), we obtain the following sequence of equivalent identities:

\[ u_1g(y)u_2 = v_1h(y)v_2 \]
\[ B#(u_1g(y)u_2)#E = B#(v_1h(y)v_2)#E \]
\[ B#u_1# \cdot #^{-1}g(y)# \cdot #^{-1}u_2#E = B#v_1#^{-1} \cdot #h(y)#^{-1} \cdot #v_2#E \]
\[ g'(B)g'(y)g'(E) = h'(B)h'(y)h'(E) \]
\[ g'(ByE) = h'(ByE). \]

Therefore \( ByE \) is a solution to \( IPCP \), so the claimed equivalence follows. □
Theorem 1. The following hold in a finitely generated free group.

1. \( \text{PCP}^{(\text{inj, inj})}_{\Sigma} (n + 2) \Rightarrow \text{GPCP}^{(\text{inj, inj})}_{\Sigma} (n) \)
2. \( \text{PCP}^{(\text{inj, inj})}_{\Sigma} (n + 2) \Rightarrow \text{GPCP}^{(\text{inj, inj})}_{\Sigma} (n) \)

Proof. Let \( I_{\text{GPCP}} \) be an instance of the GPCP\(^{\text{inj}}\), and construct from it the instance \( I_{\text{PCP}} = (\Sigma \cup \{ B, E \}, \Delta \cup \{ B, E, \# \}, g', h', B, \Sigma, E) \) of the PCP\(_{\Sigma} \), which is the instance \( I_{\text{PCP}} \) defined above under the constraint that solutions have the form \( ByE \) for some \( y \in F(\Sigma) \).

By Lemma 3, \( I_{\text{PCP}} \) is an instance of the PCP\(^{\text{inj, inj}}\)\(_{\Sigma} \)(n + 2) if and only if \( I_{\text{GPCP}} \) is an instance of GPCP\(^{\text{inj, inj}}\)\(_{\Sigma} \)(n), and similarly for PCP\(^{\text{inj, inj}}\)\(_{\Sigma} \)(n + 2) and GPCP\(^{\text{inj, inj}}\)\(_{\Sigma} \)(n). The result then follows from Lemma 4.

The above does not prove that PCP\(^{\text{inj}}\) \( \Leftrightarrow \) GPCP\(^{\text{inj}}\), because \( I_{\text{PCP}} \) might have solutions of the form \( BxB^{-1} \) or \( E^{-1}xE \). For example, if we let \( I_{\text{GPCP}} = (\{ a \}, \{ a, c, d \}, g, h, c, e, d) \) with \( g(a) = a \) and \( h(a) = cac^{-1} \), then there is no \( x \in F(\Sigma) \) such that \( cg(a) = h(a)d \), but defining \( g', h' \) as above then \( BcB^{-1} E \in Eq(g', h') \). In Section 6.2, we consider maps where such solutions are impossible, and there the equivalence PCP\(^{\text{inj}}\) \( \Leftrightarrow \) GPCP\(^{\text{inj}}\) does hold.

4 The PCP under rational constraints

For an alphabet \( A \), a language \( L \subseteq A^* \) is regular if there exists some finite state automaton over \( A \) which accepts exactly the words in \( L \). Let \( \pi : (\Sigma^{\pm 1})^* \rightarrow F(\Sigma) \) be the natural projection map. A subset \( R \subseteq F(\Sigma) \) is rational if \( R = \pi(L) \) for some regular language \( L \subseteq (\Sigma^{\pm 1})^* \).

In this section we consider the PCP\(^{\text{inj}}\)\(_{\mathcal{R}}\), which is the PCP\(^{\text{inj}}\) subject to the rational constraint \( \mathcal{R} \). We prove that the PCP\(^{\text{inj}}\)\(_{\mathcal{R}}\) can be solved via the Basis Problem (BP) (so \( \text{BP} \Rightarrow \text{PCP}^{\text{inj}}_{\mathcal{R}} \)) from Theorem A. We later apply this to prove \( \text{BP} \Rightarrow \text{GPCP}^{\text{inj}}_{\mathcal{R}} \) from Theorem A as the PCP\(^{\text{inj}}\)\(_{\Sigma} \) from Section 3 is simply the PCP\(^{\text{inj}}\) under a specific rational constraint.

Theorem 2. The following hold in a finitely generated free group.

1. \( \text{BP}^{(\text{inj, inj})}_{\mathcal{R}} (n) \Rightarrow \text{PCP}^{(\text{inj, inj})}_{\mathcal{R}} (n) \)
2. \( \text{BP}^{(\text{inj, inj})}_{\mathcal{R}} (n) \Rightarrow \text{PCP}^{(\text{inj, inj})}_{\mathcal{R}} (n) \)

Proof. Let \( g, h \) be homomorphisms from \( F(\Sigma) \) to \( F(\Delta) \) such that at least one of them is injective. Their equaliser \( \text{Eq}(g, h) \) is a finitely generated subgroup of \( F(\Sigma) \), so \( \text{Eq}(g, h) \) is a rational set (see for example Section 3.1 in [1]).

As the Basis Problem is soluble, we can compute a basis for \( \text{Eq}(g, h) \). This is equivalent to finding a finite state automaton \( \mathcal{A} \) (called a “core graph” in the literature on free groups; see [12]) that accepts the set \( \text{Eq}(g, h) \).
Let $R$ be a rational set in $F(\Sigma)$. The PCP$_R$ for $g$ and $h$ is equivalent to determining if there exists any non-trivial $x \in R \cap \text{Eq}(g, h)$. Since the intersection of two rational sets is rational, and an automaton recognising this intersection is computable by the standard product construction of automata, one can determine whether $R \cap \text{Eq}(g, h)$ is trivial or not, and thus solve PCP$_R$.

The following theorem immediately implies Theorem 3 as restrictions on the maps do not affect the rational constraints.

**Theorem 3 (Theorem 3).** PCP$_{E\subseteq \neg \text{inj}}$ is undecidable in free groups.

**Proof.** We have PCP$_{E\subseteq \neg \text{inj}}(n + 2) \Rightarrow \text{GPCP}_{E\subseteq \neg \text{inj}}(n + 2)$ by Lemmas 3 and 4. The result follows as GPCP$_{E\subseteq \neg \text{inj}}(n + 2)$ is undecidable by Lemma 2.

5 Main results, part 1

Here we combine results from the previous sections to prove certain of the implications in Theorem A. The implications we prove refine Theorem A, as they additionally contain information on alphabet sizes and on injectivity.

**Theorem 4.** The following hold in finitely generated free groups.

1. $\text{BP}_{E \subseteq \neg \text{inj}}(n + 2) \Rightarrow \text{GPCP}_{E \subseteq \neg \text{inj}}(n) \Rightarrow \text{PCP}_{E \subseteq \neg \text{inj}}(n)$
2. $\text{BP}_{E \subseteq \text{inj}}(n + 2) \Rightarrow \text{GPCP}_{E \subseteq \text{inj}}(n) \Rightarrow \text{PCP}_{E \subseteq \text{inj}}(n)$

**Proof.** As PCP$_{E \subseteq \neg \text{inj}}$ is an instance of the PCP$_{E \subseteq \text{inj}}$ under a rational constraint, Theorem 2 gives us that BP$_{E \subseteq \neg \text{inj}}(n + 2) \Rightarrow \text{PCP}_{E \subseteq \neg \text{inj}}(n + 2)$, while Theorem 1 gives us that PCP$_{E \subseteq \neg \text{inj}}(n + 2) \Rightarrow \text{GPCP}_{E \subseteq \neg \text{inj}}(n)$, and the implication GPCP$_{E \subseteq \neg \text{inj}}(n) \Rightarrow \text{PCP}_{E \subseteq \neg \text{inj}}(n)$ is obvious as instances of the PCP are instances of the GPCP but with empty constants $u_i, v_i$. Sequence 1, with one map injective, therefore holds, while the proof of sequence 2 is identical.

Removing the injectivity assumptions gives the following corollary; the implications BP $\Rightarrow$ PCP$_{E \subseteq \text{inj}}$ $\Rightarrow$ PCP of Theorem A follow immediately.

**Corollary 1.** BP$(n + 2) \Rightarrow \text{GPCP}_{E \subseteq \text{inj}}(n) \Rightarrow \text{PCP}(n)$

**Proof.** Theorem 4 gives that BP$(n + 2) \Rightarrow \text{GPCP}_{E \subseteq \text{inj}}(n) \Rightarrow \text{PCP}_{E \subseteq \text{inj}}(n)$, while PCP$(n) \Leftrightarrow \text{PCP}_{E \subseteq \text{inj}}(n)$ by Proposition 1.

6 Conjugacy inequivalent maps

In this section we prove genericity results and give conditions under which the PCP implies the GPCP. In particular, we prove Theorem 3 and we prove the implication PCP $\Rightarrow$ PCP$_{E \subseteq \text{inj}}$ from Theorem A.

A pair of maps $g, h : F(\Sigma) \to F(\Delta)$ is said to be conjugacy inequivalent if for every $u \in F(\Delta)$ there does not exist any non-trivial $x \in F(\Sigma)$ such that $g(x) =$
For example, if the images of $g,h : F(\Sigma) \to F(\Delta)$ are conjugacy separated, that is, if $\text{Im}(g) \cap u^{-1} \text{Im}(h)u$ is trivial for all $u \in F(\Delta)$, then $g$ and $h$ are conjugacy inequivalent. We write $\text{PCP}^{\text{inj}} + \text{CI}$ for those instances of the GPCP where the maps are conjugacy inequivalent.

### 6.1 Random maps and genericity

Here we show that among all pairs of maps $g,h : F(\Sigma) \to F(\Delta)$, the property of being conjugacy inequivalent occurs with probability 1; that is, conjugacy inequivalent maps are generic.

**Theorem 5 (Theorem C).** Instances of the $\text{PCP}^{\text{inj}} + \text{CI}$ are generic instances of the PCP. That is, with probability 1, a pair of maps is conjugacy inequivalent.

Before we prove the theorem, we need to describe the way in which probabilities are computed. We fix the two alphabets $\Delta = \{x_1, \ldots, x_m\}$ and $\Sigma = \{y_1, \ldots, y_k\}$, $m \leq k$, and ambient free groups $F(\Delta)$ and $F(\Sigma)$, and pick $g$ and $h$ randomly by choosing $(g(x_1), \ldots, g(x_m))$ and $(h(x_1), \ldots, h(x_m))$ independently at random, as tuples of words of length bounded by $n$ in $F(\Sigma)$. If $P$ is a property of tuples (or subgroups) of $F(\Sigma)$, we say that generically many tuples (or finitely generated subgroups) of $F(\Sigma)$ satisfy $P$ if the proportion of $m$-tuples of words of length $\leq n$ in $F(\Sigma)$ which satisfy $P$ (or generate a subgroup satisfying $P$), among all possible $m$-tuples of words of length $\leq n$, tends to 1 when $n$ tends to infinity.

**Proof.** Let $n > 0$ be an integer, and let $(a_1, \ldots, a_m)$ and $(b_1, \ldots, b_m)$ be two tuples of words in $F(\Sigma)$ satisfying length inequalities $|a_i| \leq n$ and $|b_i| \leq n$ for all $i$. We let the maps $g,h : F(\Sigma) \to F(\Delta)$ that are part of an instance of PCP be defined as $g(x_i) = a_i$ and $h(x_i) = b_i$, and note that the images $\text{Im}(g)$ and $\text{Im}(h)$ in $F(\Delta)$ are subgroups generated by $(a_1, \ldots, a_m)$ and $(b_1, \ldots, b_m)$, respectively.

We claim that among all $2m$-tuples $(a_1, \ldots, a_m, b_1, \ldots, b_m)$ with $|a_i|, |b_i| \leq n$, a proportion of them tending to 1 as $n \to \infty$ satisfy (1) the subgroups $L = \langle a_1, \ldots, a_m \rangle$ and $K = \langle b_1, \ldots, b_m \rangle$ are both of rank $m$, and (2) for every $u \in F(\Delta)$ we have $L^u \cap K = \{1\}$. Claim (1) is equivalent to $g,h$ being generically injective, and follows from [10], while claim (2) is equivalent to $\text{Im}(g)^u \cap \text{Im}(h) = \{1\}$ for every $u \in F(\Delta)$, which implies $g$ and $h$ are generically conjugacy separated, and follows from [5] Theorem 1. More specifically, [5] Theorem 1 proves that for any tuple $(a_1, \ldots, a_m)$, ‘almost all’ (precisely computed) tuples $(b_1, \ldots, b_m)$, with $|b_i| \leq n$, give subgroups $L = \langle a_1, \ldots, a_m \rangle$ and $K = \langle b_1, \ldots, b_m \rangle$ with trivial pullback, that is, for every $u \in F(\Delta)$, $K^u \cap L = \{1\}$. Going over all $(a_1, \ldots, a_m)$ with $|a_i| \leq n$ and counting the tuples $(b_1, \ldots, b_m)$ (as in [5]) satisfying property (2) gives the genericity result for all $2m$-tuples. □

### 6.2 The GPCP for conjugacy inequivalent maps

We now prove that the PCP implies the GPCP$^{\text{inj}} + \text{CI}$ and hence that, generically, the PCP implies the GPCP. Recall that if $I_{\text{GPCP}}$ is a specific instance of
the GPCP we can associate to it a specific instance $I_{PCP} = (\Sigma \sqcup \{B, E\}, \Delta \sqcup \{B, E, \#\}, g', h')$, as in Section 3. We start by classifying the solutions to $I_{PCP}$.

**Lemma 5.** Let $I_{GPCP}$ be an instance of the GPCP inj, with associated instance $I_{PCP}$ of the PCP inj. Every solution to $I_{PCP}$ is a product of solutions of the form $(BxE)^{\pm 1}$, $E^{-1}xE$ and $BxB^{-1}$, for $x \in F(\Sigma)$.

Lemma 5 is proven in the appendix. We now have:

**Theorem 6.** Let $I_{GPCP} = (\Sigma, \Delta, g, h, u_1, v_1)$ be an instance of the GPCP inj, such that there is no non-trivial $x \in F(\Sigma)$ with $u_1 g(x) u_1^{-1} = v_1 h(x) v_1^{-1}$ or $u_2^{-1} g(x) u_2 = v_2^{-1} h(x) v_2$. Then $I_{GPCP}$ has a solution (possibly trivial) if and only if the associated instance $I_{PCP}$ of the PCP inj has a non-trivial solution.

**Proof.** By Lemma 4, if $I_{GPCP}$ has a solution then $I_{PCP}$ has a non-trivial solution. For the other direction, note that the assumptions in the theorem are equivalent to $I_{GPCP}$ having no solutions of the form $BxB^{-1}$ or $E^{-1}xE$, and so by Lemma 5 every non-trivial solution to $I_{GPCP}$ has the form $Bx_1E \cdots Bx_nE$ for some $x_i \in F(\Sigma)$. The $Bx_iE$ subwords block this word off into chunks, and we see that each such word is a solution to $I_{PCP}$. By Lemma 4 each $x_i$ is a solution to $I_{GPCP}$. Hence, if $I_{PCP}$ has a non-trivial solution then $I_{GPCP}$ has a solution. \(\square\)

Theorem 6 depends both on the maps $g$ and $h$ and on the constants $u_i$, $v_i$. The definition of conjugacy inequivalent maps implies that the conditions of Theorem 6 hold always, independent of the $u_i$, $v_i$. We therefore have:

**Theorem 7.** The following hold in finitely generated free groups.

1. $\text{PCP}^{(\neg\text{inj},\text{inj})}(n+2) \Rightarrow \text{GPCP}^{(\neg\text{inj},\text{inj})} + \text{CI}(n)$
2. $\text{PCP}^{(\text{inj},\text{inj})}(n+2) \Rightarrow \text{GPCP}^{(\text{inj},\text{inj})} + \text{CI}(n)$

Removing the injectivity assumptions gives the following corollary; the implication $\text{PCP} \Rightarrow \text{GPCP}^{\text{inj} + \text{CI}}$ of Theorem 6 follow immediately.

**Corollary 2.** $\text{PCP}(n+2) \Rightarrow \text{GPCP}^{\text{inj} + \text{CI}}(n)$

**Proof.** Theorem 7 gives us that $\text{PCP}^{\text{inj}}(n+2) \Rightarrow \text{GPCP}^{\text{inj} + \text{CI}}(n)$, while the $\text{PCP}(n)$ and $\text{PCP}^{\text{inj}}(n)$ are equivalent by Proposition 1. \(\square\)

### 7 The Basis Problem and Stallings’ Rank Problem

In this section we link the Basis Problem to Stallings’ Rank Problem. Clearly the Basis Problem solves the Rank Problem, as the rank is simply the size of the basis. We prove that these problems are equivalent, with Lemma 6 providing the non-obvious direction of the equivalence. Combining this equivalence with Corollary 1 gives: $\text{RP} \Rightarrow \text{GPCP}^{\text{inj}} \Rightarrow \text{PCP}$.

The proof of Lemma 6 is based on the following construction of Goldstein–Turner, which they used to prove that $\text{Eq}(g, h)$ is finitely generated [10]. Let
Let $F = F(\Delta)$ be a finitely generated free group, let $H$ be a subgroup with basis $\mathcal{N} = \{\alpha_1, \ldots, \alpha_k\}$ of $F$, where $\alpha_i \in F$, and let $\phi : H \to F$ be a homomorphism. The derived graph $D_\phi$ of $\phi$ relative to $\mathcal{N}$ is the graph with vertex set $F$, and directed edges labeled by elements of $\mathcal{N}$ according to the rule: if $u = \phi(\alpha_i)v\alpha_i^{-1}$ then connect $u$ to $v$ by an edge with initial vertex $u$, end vertex $v$, and label $\alpha_i$. We shall use the fact that a word $w(\alpha_1, \ldots, \alpha_k)$ is fixed by $\phi$ if and only if the path which starts at the vertex $\epsilon$ (the identity of $F$) and is labeled by $w(\alpha_1, \ldots, \alpha_k)$ is a loop, so also ends at $\epsilon$.

**Lemma 6.** There exists an algorithm with input an instance $I = (\Sigma, \Delta, g, h)$ of the PCP$^{\text{inj}}$ and the rank $\text{rk}(\text{Eq}(g, h))$ of the equaliser of $g$ and $h$, and output a basis for $\text{Eq}(g, h)$.

The following shows that Stallings’ Rank Problem is equivalent to the BP.

**Theorem 8.** The following hold in finitely generated free groups.

1. $\text{BP}^{(\neg \text{inj}, \text{inj})}(n + 2) \iff \text{RP}^{(\neg \text{inj}, \text{inj})}(n)$
2. $\text{BP}^{(\text{inj}, \text{inj})}(n + 2) \iff \text{RP}^{(\text{inj}, \text{inj})}(n)$

**Proof.** Let $I_{\text{PCP}}$ be an instance of the PCP$^{\text{inj}}$. As the rank of a free group is precisely the size of some (hence any) basis for it, if we can compute a basis for $\text{Eq}(g, h)$ then we can compute the rank of $\text{Eq}(g, h)$. On the other hand, by Lemma 6 if we can compute the rank of $\text{Eq}(g, h)$ then we can compute a basis of $\text{Eq}(g, h)$. 

We therefore have:

**Corollary 3.** $\text{BP}(n) \iff \text{RP}(n)$

### 8 Main results, part 2

We now combine results from the previous sections to the following result, from which Theorem 9 follows immediately.

**Theorem 9.** In finitely generated free groups the following implications hold.

\[
\begin{array}{cccccc}
\text{RP}(n) & \iff & \text{BP}(n) & \iff & \text{GPCP}^{\text{inj}}(n) & \iff \text{PCP}(n - 2) & \iff \text{GPCP}^{\text{inj} + \text{CI}}(n) \\
\downarrow & & & & \downarrow & & \\
\text{BP}(n) & \implies & \text{GPCP}^{\text{inj}}(n) & \implies & \text{PCP}(n - 2) & \implies & \text{GPCP}^{\text{inj} + \text{CI}}(n) \\
\end{array}
\]

**Proof.** The proof is a summary of the results already established in the rest of the paper, and we give a schematic version of it here.

- $\text{RP}(n) \iff \text{BP}(n)$ holds by Corollary 6
- $\text{BP}(n) \implies \text{GPCP}^{\text{inj}}(n)$ holds by Theorem 2
- $\text{BP}(n) \implies \text{GPCP}^{\text{inj}}(n) \implies \text{PCP}(n)$ holds by Corollary 4
- $\text{PCP}(n - 2) \implies \text{GPCP}^{\text{inj} + \text{CI}}(n)$ holds by Corollary 2

$\square$
References

1. Bartholdi, L., Silva, P.V.: Rational subsets of groups (2010), https://arxiv.org/pdf/1012.1532.pdf
2. Bogopolski, O., Maslakova, O.: An algorithm for finding a basis of the fixed point subgroup of an automorphism of a free group. Internat. J. Algebra Comput. 26(1), 29–67 (2016)
3. Ciobanu, L., Logan, A.: Fixed points and stable images of endomorphisms for the free group of rank two. arXiv:2009.04937 (2020)
4. Ciobanu, L., Logan, A.: The Post correspondence problem and equalisers for certain free group and monoid morphisms. In: 47th International Colloquium on Automata, Languages, and Programming (ICALP 2020). pp. 120:1–120:16 (2020)
5. Ciobanu, L., Martino, A., Ventura, E.: The generic Hanna Neumann Conjecture and Post Correspondence Problem (2008), http://www-eupm.upc.es/~ventura/ventura/files/3lt.pdf
6. Diekert, V., Kharlampovich, O., Lohrey, M., Myasnikov, A.: Algorithmic problems in group theory. Dagstuhl seminar report 19131 (2019)
7. Ehrenfeucht, A., Karhumäki, J., Rozenberg, G.: The (generalized) Post correspondence problem with lists consisting of two words is decidable. Theoret. Comput. Sci. 21(2), 119–144 (1982)
8. Feighn, M., Handel, M.: Algorithmic constructions of relative train track maps and CTs. Groups Geom. Dyn. 12(3), 1159–1238 (2018)
9. Gilman, R., Miasnikov, A.G., Myasnikov, A.D., Ushakov, A.: Report on generic case complexity (2007), https://arxiv.org/pdf/0707.1364v1.pdf
10. Goldstein, R.Z., Turner, E.C.: Fixed subgroups of homomorphisms of free groups. Bull. London Math. Soc. 18(5), 468–470 (1986)
11. Harju, T., Karhumäki, J.: Morphisms. In: Handbook of formal languages, Vol. 1, pp. 439–510. Springer, Berlin (1997)
12. Kapovich, I., Myasnikov, A.: Stallings foldings and subgroups of free groups. J. Algebra 248(2), 608–668 (2002)
13. Kapovich, I., Myasnikov, A., Schupp, P., Shpilrain, V.: Generic-case complexity, decision problems in group theory, and random walks. J. Algebra 264(2), 665–694 (2003)
14. Karhumäki, J., Saarela, A.: Noneffective regularity of equality languages and bounded delay morphisms. Discrete Math. Theor. Comput. Sci. 12(4), 9–17 (2010)
15. Lecerf, Y.: Récursive insolubilité de l’équation générale de diagonalisation de deux monomorphismes de monoïdes libres $\varphi x = \psi x$. C. R. Acad. Sci. Paris 257, 2940–2943 (1963)
16. Martino, A., Turner, E., Ventura, E.: The density of injective endomorphisms of a free group (2006), http://www-eupm.upc.es/~ventura/ventura/files/23t.pdf
17. Myasnikov, A., Nikolaev, A., Ushakov, A.: The Post correspondence problem in groups. J. Group Theory 17(6), 991–1008 (2014)
18. Neary, T.: Undecidability in binary tag systems and the post correspondence problem for five pairs of words. In: 32nd International Symposium on Theoretical Aspects of Computer Science, LIPIcs. Leibniz Int. Proc. Inform., vol. 30, pp. 649–661. Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern (2015)
19. Post, E.L.: A variant of a recursively unsolvable problem. Bull. Amer. Math. Soc. 52, 264–268 (1946)
Appendix: Additional material to Sections 6 & 7

Proof (Lemma 3). Let $x'$ be a solution to $I_{PCP}$, and decompose it as a freely reduced word

$$x_0\alpha_1x_1\alpha_2\cdots x_{n-1}\alpha_nx_n$$

for $x_i \in F(\Sigma)$ and $\alpha_i \in \{B, E\}^{\pm 1}$.

We shall refer to the letters $B^{\pm 1}, E^{\pm 1}$ as markers. Indeed, they act as “separators” in the word $x'$, because in the definitions of $g'$ and $h'$ the letter $B$ only occurs in $g'(B)$ and $h'(B)$, and the letter $E$ only occurs in $g'(E)$ and $h'(E)$; thus either the $B^{\pm 1}$ and $E^{\pm 1}$ terms in $x'$ are preserved under application of $g'$ and $h'$, or two of these letters cancel in the image. Therefore, the parts of each of $g'(\alpha_1x_1\alpha_2)\text{ and } h'(\alpha_1x_1\alpha_2)$ lying between the markers must be equal, or otherwise there exist some indices $i, j$ such that both $g'(\alpha_i)x_{i+1}\alpha_{i+1}$ and $h'(\alpha_j)x_{j+1}\alpha_{j+1}$ are contained in $F(\Delta)$: this collapsing must happen in each image as the numbers of $B^{\pm 1}$ and $E^{\pm 1}$ terms must be equal in both images. By inspecting the maps, we see that this collapsing requires $x_i \in \ker(g')$ and $\alpha_i = \alpha_i^{-1}$, and $x_j \in \ker(h')$ and $\alpha_j = \alpha_j^{-1}$. However, by Lemma 3 only one of $g'$ or $h'$ is injective, $g'$ say, so then $x_i$ is trivial, and so $\alpha_i x_i\alpha_i^{-1}$ is empty, contradicting the decomposition being freely reduced. Therefore, we have that for all $1 \leq i < n$ the parts of each of $g'(\alpha_1x_1\alpha_2)\text{ and } h'(\alpha_1x_1\alpha_2)$ lying between the markers $B^{\pm 1}, E^{\pm 1}$ are equal. This also implies that the parts of $g'(x_0\alpha_1)$ and $h'(x_0\alpha_1)$ lying before the markers are equal.

We next prove that $x_0$ is empty, $\alpha_1 \in \{B, E^{-1}\}$, $\alpha_2 \in \{B^{-1}, E\}$ (so in particular, non-empty), and that $\alpha_1 x_1\alpha_2$ is a solution to $I_{PCP}$.

Suppose $x_0$ is non-empty. Then either $g'(x_0\alpha_1)$ starts with $\#^{-1}$ or $E$ (when $v_2$ is empty), or $x_0 \in \ker g'$ and the image starts with $B$ or $E^{-1}$, while either $h'(x_0\alpha_1)$ starts with $\#$ or $B^{-1}$ (when $v_1$ is empty), or $x_0 \in \ker h'$ and the image starts with $B$ or $E^{-1}$. As one map is injective, by Lemma 3 we have that $g'(x_0\alpha_1)$ and $h'(x_0\alpha_1)$ start with different letters, contradicting the above paragraph. Hence, $x_0$ is empty. We then have that $\alpha_1 \in \{B, E^{-1}\}$, as this is the only way that the parts of $g'(\alpha_1)$ and $h'(\alpha_1)$ lying before the marker can be equal.

Suppose $\alpha_2$ is empty, so $x' = \alpha_1 x_1$. Then as $x'^{-1}$ is also a solution to $I_{PCP}$, we also have that $x_1$ is empty, and so $x' = \alpha_1 \in \{B, E^{-1}\}$. However, neither $B$ nor $E^{-1}$ is a solution to $I_{PCP}$, a contradiction. Hence, $\alpha_2$ is non-empty. Moreover, $\alpha_2 \in \{B^{-1}, E\}$, as otherwise the parts of each of $g'(\alpha_1x_1\alpha_2)$ and $h'(\alpha_1x_1\alpha_2)$ lying between the markers are non-equal (for example, $g'(Bx_1B) = B\#_{v_1}g(x_1)B\cdots$ while $h'(Bx_1B) = B\#_{v_1}h(x_1)\#^{-1}B\cdots$). Finally, under these restrictions on $\alpha_1$ and $\alpha_2$, and because the parts of $g'(\alpha_1x_1\alpha_2)$ and $h'(\alpha_1x_1\alpha_2)$ lying between the markers are equal, we get that $\alpha_1 x_1\alpha_2$ is a solution to $I_{PCP}$ of the form $(Bx_1E)^{\pm 1}, E^{-1}x_1E, Bx_1B^{-1}$ for $x_1 \in F(\Sigma)$.

We can now prove the result: the product $(\alpha_1x_1\alpha_2)^{-1}x'$ is also a solution to $I_{PCP}$, and it decomposes as $x_2\alpha_3\cdots x_{n-1}\alpha_nx_n$. Applying the above argument, we get that $x_2$ is empty and that $\alpha_3x_3\alpha_4$ is a solution to $I_{PCP}$ of the form $(Bx_3E)^{\pm 1}, E^{-1}x_3E, Bx_3B^{-1}$ for $x_3 \in F(\Sigma)$. Repeatedly reducing the solution like this,
we see that \( x' \) decomposes as \( x''x_n \) where \( x'' \) is a product of solutions of the form \((BxE)^{\pm 1}, E^{-1}xE, \) and \( BxB^{-1} \) for \( x \in F(\Sigma) \). The result then follows as \( x_n \) is empty, which can be seen by applying the above argument to the solution \( x'-1 \), which decomposes as \( x_n \alpha_n \cdot \cdots \).

\( \square \)

**Proof (Lemma 2).** Suppose without loss of generality that \( g \) is injective, and consider the homomorphism \( \phi = h \circ g^{-1} : \text{Im}(g) \to F(\Delta) \). Then \( g(\text{Eq}(g, h)) \) is precisely the fixed subgroup \( \text{Fix}(\phi) = \{ x \in \text{Im}(g) \mid \phi(x) = x \} \), and as \( g \) is injective it restricts to an isomorphism between these two subgroups. We therefore give an algorithm which takes as input \( I = (\Sigma, \Delta, g, h) \) and the rank \( \text{rk}(\text{Eq}(g, h)) \) and outputs a basis \( B \) for \( \text{Fix}(\phi) \); this is sufficient as \( g^{-1}(B) \) is then an algorithmically computable basis for \( \text{Eq}(g, h) \). If \( \text{rk}(\text{Eq}(g, h)) = 0 \) then the basis is the empty set, so we may assume \( \text{rk}(\text{Eq}(g, h)) \geq 1 \) (this reduction is not necessary, but not doing so introduces certain subtleties).

Let \( \Gamma_\phi \) be the union of those loops in \( D_\phi \) which contain no degree-1 vertices, but contain the vertex \( \epsilon \); this is simply the component of the core graph of \( D_\phi \) which contains the specified vertex. As labels of loops in \( D_\phi \) correspond to elements of \( \text{Fix}(\phi) \), any basis of the fundamental group \( \pi_1(\Gamma_\phi) \) corresponds to a basis of \( \text{Fix}(\phi) \). Now, a basis for \( \pi_1(\Gamma_\phi) \) can be computed via standard algorithms (see for example [12, Propositions 6.7]), and therefore to prove the result we only need to construct the graph \( \Gamma_\phi \).

Start with vertex set \( V \) consisting of a single vertex \( \epsilon \) corresponding to the empty word. Now enter a loop, terminating when \( |E| - |V| = \text{rk}(\text{Eq}(g, h)) - 1 \), as follows: For each \( v \in V \) and each \( i \in \{1, \ldots, k\} \), add an edge to \( E \) starting at \( v \) and ending at the vertex corresponding to the element \( \phi(\alpha_i)g\alpha_i^{-1} \) of \( F(\Sigma) \); if there is no such vertex in \( V \) then first add one to \( V \). When the loop terminates, prune the resulting graph to obtain a graph \( \Gamma_\phi' \) by iteratively removing all degree-1 vertices.

Note that \( \text{rk}(\text{Eq}(g, h)) \) is known, so we can determine if a graph satisfies \( |E| - |V| = \text{rk}(\text{Eq}(g, h)) - 1 \); in particular, at each iteration in the looping procedure we know whether to continue or to terminate the loop.

There are two things to prove. Firstly, that the looping procedure terminates (and so the above is actually an algorithm), and secondly that the terminating graph \( \Gamma_\phi' \) is in fact the graph \( \Gamma_\phi \). So, note that the procedure constructs some subgraph of \( D_\phi \) which contains the empty word as a vertex, which has no degree-1 vertices, and which satisfies \( \#\text{edges} - \#\text{vertices} = \text{rk}(\text{Eq}(g, h)) - 1 \), or no such subgraph exists. Now, the graph \( \Gamma_\phi \) satisfies these conditions (because its fundamental group has rank \( \text{rk}(\text{Eq}(g, h)) \)), so the procedure does terminate. Moreover, every loop in \( D_\phi \) which contains the empty word is a loop in \( \Gamma_\phi \), and so the subgraph constructed is in fact a subgraph of \( \Gamma_\phi \). The result then follows because no proper subgraph of \( \Gamma_\phi \) satisfies \( \#\text{edges} - \#\text{vertices} = \text{rk}(\text{Eq}(g, h)) - 1 \) (subgraphs in fact satisfy \( \#\text{edges} - \#\text{vertices} \leq \text{rk}(\text{Eq}(g, h)) - 1 \)).

\( \square \)