Variations on the Post Correspondence Problem for Free Groups

Citation for published version:
Ciobanu, L & Logan, AD 2021, Variations on the Post Correspondence Problem for Free Groups. in N Moreira & R Reis (eds), *Developments in Language Theory. DLT 2021.* Lecture Notes in Computer Science, vol. 12811, Springer, pp. 90-102, 25th International Conference on Developments in Language Theory 2021, Virtual, Online, 16/08/21. https://doi.org/10.1007/978-3-030-81508-0_8

Digital Object Identifier (DOI):
10.1007/978-3-030-81508-0_8

Link:
Link to publication record in Heriot-Watt Research Portal

Document Version:
Peer reviewed version

Published In:
Developments in Language Theory. DLT 2021

Variations on the Post Correspondence Problem for Free Groups[⋆]

Laura Ciobanu ✉[0000−0002−9451−1471] and Alan D. Logan[0000−0003−1767−6798]

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.

We first consider the Post Correspondence Problem (PCP) for free groups. This is analogous to the classical Post Correspondence Problem, which is about free monoids rather than free groups and has 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 $\varSigma$ and $\varDelta$ be two alphabets, let $g, h : F(\varSigma) \to F(\varDelta)$ be two group homomorphisms from the free group over $\varSigma$ to the free group over $\varDelta$, and store this data in a four-tuple $I = (\varSigma, \varDelta, g, h)$, called an *instance* of the PCP. The PCP is the decision problem:

$$\text{Given } I = (\varSigma, \varDelta, g, h), \text{ is there } x \in F(\varSigma) \setminus \{1\} \text{ such that } g(x) = h(x)?$$

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

[⋆] Work supported by EPSRC grant EP/R035814/1.

Our second problem asks not just about the triviality of $\mathrm{Eq}(g,h)$, but for a finite description of it. We write $\mathrm{PCP}^{\mathrm{inj}}$ (see Table 1) for the PCP with at least one map injective, in which case the subgroup $\mathrm{Eq}(g,h)$ is finitely generated [10] and a finite description relates to bases (as defined in Section 2): The *Basis Problem* (BP) takes as input an instance $I = (\Sigma, \Delta, g, h)$ of the $\mathrm{PCP}^{\mathrm{inj}}$ and outputs a basis for $\mathrm{Eq}(g,h)$. In Section 8 we show that the BP is equivalent to the *Rank Problem* (RP), which seeks the number of elements in a 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 $I_{\mathrm{GPCP}} = (\Sigma, \Delta, g, h, u_1, u_2, v_1, v_2)$ and the GPCP itself is the decision problem:

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

Table 1: Summary of certain decision problems related to the PCP

Problems (for free groups)	Fixed: finite alphabets Σ and Δ 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 $\mathrm{PCP}_{\mathcal{R}}$: rational set $\mathcal{R} \subseteq F(\Sigma)$ Additional input for $\mathrm{PCP}_{\mathcal{EL}}$: $a, b \in \Sigma^{\pm 1}$, $\Omega \subset \Sigma$
	Is it decidable whether:
PCP	there exists $x \in F(\Sigma) \setminus \{1\}$ s.t. $g(x) = h(x)$?
GPCP	there exists $x \in F(\Sigma) \setminus \{1\}$ s.t. $u_1 g(x) u_2 = v_1 h(x) v_2$?
$\mathrm{PCP}_{\mathcal{R}}$	there exists $x \neq 1$ in $\mathcal{R}$ s.t. $g(x) = h(x)$?
$\mathrm{PCP}_{\mathcal{EL}}$	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 $y \in F(\Omega)$
$\mathrm{PCP}^{(\neg\,\mathrm{inj}, \neg\,\mathrm{inj})}$	PCP with neither g, nor h injective
$\mathrm{PCP}^{(\neg\,\mathrm{inj}, \mathrm{inj})}$	PCP with exactly one of g, h injective
$\mathrm{PCP}^{(\mathrm{inj}, \mathrm{inj})}$	PCP with both g, h injective
$\mathrm{PCP}^{\mathrm{inj}}$	$\mathrm{PCP}^{(\neg\,\mathrm{inj}, \mathrm{inj})} \cup \mathrm{PCP}^{(\mathrm{inj}, \mathrm{inj})}$ (i.e. PCP with at least one of g, h injective)
$\mathrm{PCP}^{\mathrm{CI}}$	PCP with g, h s.t. $g(y) \neq u^{-1} h(y) u$ for all $u \in F(\Delta), y \in F(\Sigma) \setminus \{1\}$
$\mathrm{PCP}^{\mathrm{inj}+\mathrm{CI}}$	$\mathrm{PCP}^{\mathrm{inj}} \cap \mathrm{PCP}^{\mathrm{CI}}$
$\mathrm{PCP}(n)$	$\mathrm{PCP}(n)$ for alphabet size $\lvert\Sigma\rvert = n$
variants for GPCP & $\mathrm{PCP}_{\mathcal{EL}}$	$\mathrm{GPCP}^{\mathrm{inj}}$, $\mathrm{PCP}_{\mathcal{EL}}^{\mathrm{inj}}$, $\mathrm{GPCP}^{\mathrm{inj}+\mathrm{CI}}$, $\mathrm{GPCP}(n)$, $\mathrm{PCP}_{\mathcal{EL}}(n)$, etc. analogue to PCP variants

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 3). 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 established in this paper (arrows are labeled by the section numbers where the implications are proven), and Section 9 brings all the results together. Given two algorithmic problems $\mathcal{P}$ and $\mathcal{Q}$, we write $\mathcal{P} \implies \mathcal{Q}$ to mean that $\mathcal{Q}$ is Turing reducible to $\mathcal{P}$ (that is, if we can solve $\mathcal{P}$ then we can solve $\mathcal{Q}$). Note that asking for both maps to be injective refines the results in this theorem, as does restricting the size of the source alphabet Σ (see Theorem 9). All our result are for finitely generated free groups, which we abbreviate to *f.g. free groups.*

Theorem A (Theorem 9) *The following implications hold in f.g free groups.*

$$\begin{tikzcd}
\text{Rank Problem (RP)} \arrow[d, Leftrightarrow, "8"'] & & & \\
\text{Basis Problem (BP)} \arrow[r, Rightarrow, "6"] \arrow[d, Rightarrow, "4"] & \mathrm{GPCP}^{\mathrm{inj}} \arrow[r, Rightarrow, "6"] & \mathrm{PCP} \arrow[r, Rightarrow, "7.2"] & \mathrm{GPCP}^{\mathrm{inj}\,+\,\mathrm{CI}} \\
\mathrm{PCP}^{\mathrm{inj}}_{\mathcal{R}} & & &
\end{tikzcd}$$

Establishing the decidability of Stallings' Rank Problem is thus of central importance, as the chain RP $\Rightarrow$ $\mathrm{GPCP}^{\mathrm{inj}}$ $\Rightarrow$ PCP obtained above would lead to the decidability of the PCP.

Rational constraints The proof of the implication BP $\Rightarrow$ $\mathrm{GPCP}^{\mathrm{inj}}$ above uses the $\mathrm{PCP}^{\mathrm{inj}}$ with a certain rational constraint, namely the problem $\mathrm{PCP}^{\mathrm{inj}}_{\mathcal{EL}}$ (see Table 1). The relationship between the GPCP and the $\mathrm{PCP}_{\mathcal{EL}}$ still holds if neither map is injective. As the GPCP for free groups is undecidable in general, this connection yields Theorem B, which specifies a rational constraint $\mathcal{R}$ such that the $\mathrm{PCP}_{\mathcal{R}}$ is undecidable.

Theorem B (Theorem 3) *The* $\mathrm{PCP}_{\mathcal{EL}}$ *is undecidable in f.g. free groups.*

Random homomorphisms 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 $\Sigma = \{x_1, \dots, x_m\}$ and Δ, and ambient free groups $F(\Sigma)$ and $F(\Delta)$ remain fixed). Any map is completely determined by how it acts on the generators, and so picking g and h randomly is to be interpreted as picking $(g(x_1), \dots, g(x_m))$ and

$(h(x_1), \dots, h(x_m))$ as random tuples of words in $F(\Delta)$ (see Section 7 for details). There is a vast literature (see for example [13]) on the types of objects and behaviours which appear 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) homomorphisms, 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 7 we describe the setup used to count pairs of map and compute probabilities, and show that among all pairs of homomorphisms 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 $\mathrm{PCP}^{\mathrm{CI}}$) occurs with probability 1; that is, conjugacy inequivalent maps are generic. This follows from the fact that 'most' pairs of maps are injective *and* conjugacy inequivalent:

Theorem C (Theorem 5) *With probability* 1*, an arbitrary pair of homomorphisms consists of injective homomorphisms that are conjugacy inequivalent. That is, instances of the* $\mathrm{PCP}^{\mathrm{inj}\,+\,\mathrm{CI}}$ *are generic instances of the* PCP*.*

Theorem C shows that the implication PCP $\Rightarrow$ $\mathrm{GPCP}^{\mathrm{inj}\,+\,\mathrm{CI}}$ 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 of 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	[4]
general AEP / BP	undecidable	[14, Theorem 5.2]	unknown	[4]
$\mathrm{PCP}^{(\neg\,\mathrm{inj}, \neg\,\mathrm{inj})}$	undecidable	[19]	decidable	Lemma 1
$\mathrm{PCP}^{\mathrm{inj}}$	undecidable	[15]	unknown	
GPCP	undecidable	[11, Theorem 8]	undecidable	[17, Corollary 4.2]
$\mathrm{GPCP}^{(\neg\,\mathrm{inj}, \neg\,\mathrm{inj})}$	undecidable	[11, Theorem 8]	undecidable	Lemma 2
$\mathrm{GPCP}^{\mathrm{inj}}$	undecidable	[15]	unknown	
$\mathrm{GPCP}^{\mathrm{inj}\,+\,\mathrm{CI}}$	N/A		unknown	
$\mathrm{PCP}_{\mathcal{R}}$	undecidable	[19]	undecidable	Theorem B
$\mathrm{PCP}^{\mathrm{inj}\,+\,\mathrm{CI}}$	N/A		unknown	
generic PCP	decidable	[9, Theorem 4.4]	decidable	[5]

2 Free group preliminaries

For an alphabet Σ, let Σ^{-1} be the set of formal inverses of Σ, and write $\Sigma^{\pm 1} = \Sigma \cup \Sigma^{-1}$. For example, if $\Sigma = \{a, b\}$ then $\Sigma^{\pm 1} = \{a, b, a^{-1}, b^{-1}\}$.

We denote the free group with finite generating set Σ by $F(\Sigma)$, and view it as the set of all *freely reduced words* over $\Sigma^{\pm 1}$, that is, words not containing xx^{-1} or $x^{-1}x$ as subwords, where $x \in \Sigma^{\pm 1}$, together with the operations of concatenation and free reduction (that is, the removal of any xx^{-1} that might occur when concatenating two words). If $S \subset F(\Sigma)$ is a set in the free group, then $\langle S \rangle$ denotes the *subgroup generated by* S, which is the minimal subgroup of $F(\Sigma)$ containing S (equivalently, it is the subgroup of $F(\Sigma)$ consisting of elements corresponding to words over $S^{\pm 1}$). If S has minimal cardinality among all generating sets of $\langle S \rangle$ then S is a *basis* for $\langle S \rangle$, and $|S|$ is the *rank* of $\langle S \rangle$, written $\mathrm{rk}(\langle S \rangle)$; in particular, Σ is a basis for $F(\Sigma)$ and $\mathrm{rk}(F(\Sigma)) = |\Sigma|$. We will often use the fact that a homomorphism $f : F(\Sigma) \to F(\Delta)$ is injective if and only if the image $\mathrm{Im}(f)$ has rank $|\Sigma|$ as a subgroup of $F(\Delta)$.

The above definition of free groups is similar to the definition of the free monoid Σ^* as words over Σ under concatenation. However, the presence of inverse elements is an important difference and gives rise to specific notation: If $u, v \in F(\Sigma)$ then v^u denotes the element $u^{-1}vu$, and we say that v and v^u are *conjugate*, while if $H \subseteq F(\Sigma)$ then H^u denotes the set $\{x^u \mid x \in H\}$. If $u, v \in F(\Sigma)$ then we write $[u, v] := u^{-1}v^{-1}uv$ for their *commutator*.

3 Non-injective Maps: $\mathrm{PCP}^{(\neg\,\mathrm{inj},\neg\,\mathrm{inj})}$ and $\mathrm{GPCP}^{(\neg\,\mathrm{inj},\neg\,\mathrm{inj})}$

The PCP for non-injective maps We first prove that the $\mathrm{PCP}^{(\neg\,\mathrm{inj},\neg\,\mathrm{inj})}$ 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* $\mathrm{Eq}(g, h)$ *is non-trivial.*

Proof. We prove that $\ker(g) \cap \ker(h)$ is non-trivial, which is sufficient. Let $u \in \ker(g)$ and $v \in \ker(h)$ be non-trivial elements. If $\langle u, v \rangle \cong \mathbb{Z} = \langle x \rangle$, there exist integers k, l such that $u = x^k$ and $v = x^l$. 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 $\langle u, v \rangle \ncong \mathbb{Z}$ then $g([u, v]) = 1 = h([u, v])$, so $[u, v] \in \ker(g) \cap \ker(h)$ with $[u, v]$ non-trivial, as required. □

As we can algorithmically determine if a free group homomorphism is injective (e.g. via Stallings' foldings), Lemma 1 gives us that PCP ⇔ $\mathrm{PCP}^{\mathrm{inj}}$ for fixed alphabet sizes:

Proposition 1. $\mathrm{PCP}(n) \iff \mathrm{PCP}^{\mathrm{inj}}(n)$

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, from their proof we observe that it assumes both maps are non-injective. Therefore, $\mathrm{GPCP}^{\mathrm{inj}}$ remains open.

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

Proof. Let H be a group with undecidable word problem and let $\langle \mathbf{x} \mid \mathbf{r} \rangle$ be a finite presentation of H. Let $\Delta := \mathbf{x}$, and let $F(\Sigma)$ have basis

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

Define maps $g : (p, q) \mapsto p$ and $h : (p, q) \mapsto q$ for $(p, q) \in \Sigma$. Neither g nor h is injective as the product $(x, x^{-1})(x^{-1}, x) \in F(\Sigma)$ is in the kernel of both g and h. Taking $w \in F(\Delta)$, the instance $(\Sigma, \Delta, g, h, w, 1, 1, 1)$ of the $\mathrm{GPCP}^{(\neg\,\mathrm{inj},\neg\,\mathrm{inj})}$ has a solution if and only if the word w defines the identity of H [17, Proof of Proposition 4.1]. The result now follows as H has undecidable word problem. □

4 The PCP under Rational Constraints: $\mathrm{PCP}_{\mathcal{R}}$

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 $\pi : (\Sigma^{\pm 1})^* \to F(\Sigma)$ be the natural projection that maps any word over $\Sigma^{\pm 1}$ to the corresponding element in the free group $F(\Sigma)$. 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 $\mathrm{PCP}^{\mathrm{inj}}_{\mathcal{R}}$, which is the $\mathrm{PCP}^{\mathrm{inj}}$ subject to a rational constraint $\mathcal{R}$ (see Table 1). We prove that the $\mathrm{PCP}^{\mathrm{inj}}_{\mathcal{R}}$ under any rational constraint $\mathcal{R}$ can be solved via the Basis Problem (BP) (so BP ⇒ $\mathrm{PCP}^{\mathrm{inj}}_{\mathcal{R}}$ from Theorem A). In Section 5 we apply this to prove BP ⇒ $\mathrm{GPCP}^{\mathrm{inj}}$ from Theorem A, as the $\mathrm{PCP}^{\mathrm{inj}}_{\mathcal{EL}}$ is simply the $\mathrm{PCP}^{\mathrm{inj}}$ under a specific rational constraint.

Our results here, as in much of the rest of the paper, are broken down in terms of injectivity, and also alphabet sizes; see Table 1. Understanding for which sizes of alphabet Σ the classical Post Correspondence Problem is decidable/undecidable is an important research theme [7, 11, 18].

Theorem 1. *The following implications hold in f.g. free groups.*

1. $\mathrm{BP}^{(\neg\,\mathrm{inj},\mathrm{inj})}(n) \implies \mathrm{PCP}^{(\neg\,\mathrm{inj},\mathrm{inj})}_{\mathcal{R}}(n)$
2. $\mathrm{BP}^{(\mathrm{inj},\mathrm{inj})}(n) \implies \mathrm{PCP}^{(\mathrm{inj},\mathrm{inj})}_{\mathcal{R}}(n)$

Proof. Let g, h be homomorphisms from $F(\Sigma)$ to $F(\Delta)$ such that at least one of them is injective. Their equaliser $\mathrm{Eq}(g, h)$ is a finitely generated subgroup of $F(\Sigma)$ [10], so $\mathrm{Eq}(g, h)$ is a rational set (see for example Section 3.1 in [1]).

By assumption the Basis Problem is soluble, so we can compute a basis for $\mathrm{Eq}(g, h)$. 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 $\mathrm{Eq}(g, h)$.

Let $\mathcal{R}$ be a rational set in $F(\Sigma)$. The $\mathrm{PCP}_{\mathcal{R}}$ for g and h is equivalent to determining if there exists any non-trivial $x \in \mathcal{R} \cap \mathrm{Eq}(g, h)$. 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 $\mathcal{R} \cap \mathrm{Eq}(g, h)$ is trivial or not, and thus solve $\mathrm{PCP}_{\mathcal{R}}$. □

In the next section we consider the $\mathrm{PCP}_{\mathcal{EL}}$, which is the PCP under a certain rational constraint, and so is a specific case of $\mathrm{PCP}_{\mathcal{R}}$.

5 The GPCP and Extreme-letter Restrictions

In this section we connect the GPCP and the $\mathrm{PCP}_{\mathcal{EL}}$, as defined in Table 1. This connection underlies Theorem B, as well as the implications BP ⇒ $\mathrm{GPCP}^{\mathrm{inj}}$ and PCP ⇒ $\mathrm{GPCP}^{\mathrm{inj}\,+\,\mathrm{CI}}$ in Theorem A.

Connecting the GPCP and the PCP. We start with an instance $I_{\mathrm{GPCP}} = (\Sigma, \Delta, g, h, u_1, u_2, v_1, v_2)$ of the GPCP and consider the instance

$$I_{\mathrm{PCP}} = (\Sigma \sqcup \{B, E\}, \Delta \sqcup \{B, E, \#\}, g', h')$$

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

$$g'(z) := \begin{cases} \#^{-1}g(z)\# & \text{if } z \in \Sigma \\ B\#u_1\# & \text{if } z = B \\ \#^{-1}u_2\#E & \text{if } z = E \end{cases} \qquad h'(z) := \begin{cases} \#h(z)\#^{-1} & \text{if } z \in \Sigma \\ B\#v_1\#^{-1} & \text{if } z = B \\ \#v_2\#E & \text{if } z = E \end{cases}$$

Injectivity is preserved by this construction as $\mathrm{rk}(\mathrm{Im}(g')) = \mathrm{rk}(\mathrm{Im}(g)) + 2$ (see Section 2 for the connection between injectivity and rank): this can be seen via Stallings' foldings [12], or directly by noting that the image of g' restricted to $F(\Sigma)$ is isomorphic to $\mathrm{Im}(g)$, that B only occurs in $g'(d)$ and E only occurs in $g'(e)$. Analogously, h' is an injection if and only if h is, as again $\mathrm{rk}(\mathrm{Im}(h)) + 2 = \mathrm{rk}(\mathrm{Im}(h'))$. 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 I_{GPCP} to those of I_{PCP}.

Lemma 4. *A word $y \in F(\Sigma)$ is a solution to I_{GPCP} if and only if the word 'ByE' is a solution to I_{PCP}.*

Proof. Starting with y being a solution to I_{GPCP}, we obtain the following sequence of equivalent identities:

$$\begin{aligned} u_1 g(y) u_2 &= v_1 h(y) v_2 \\ B\#(u_1 g(y) u_2)\#E &= B\#(v_1 h(y) v_2)\#E \\ B\#u_1\# \cdot \#^{-1}g(y)\# \cdot \#^{-1}u_2\#E &= B\#v_1\#^{-1} \cdot \#h(y)\#^{-1} \cdot \#v_2\#E \\ g'(B)g'(y)g'(E) &= h'(B)h'(y)h'(E) \\ g'(ByE) &= h'(ByE). \end{aligned}$$

Therefore ByE is a solution to I_{PCP}, so the claimed equivalence follows. □

We now have that $\mathrm{PCP}^{\mathrm{inj}}_{\mathcal{EL}}(n+2) \implies \mathrm{GPCP}^{\mathrm{inj}}(n)$.

Theorem 2. *The following implications hold in f.g. free groups.*

1. $\mathrm{PCP}_{\mathcal{EL}}^{(\neg\,\mathrm{inj},\mathrm{inj})}(n+2) \implies \mathrm{GPCP}^{(\neg\,\mathrm{inj},\mathrm{inj})}(n)$
2. $\mathrm{PCP}_{\mathcal{EL}}^{(\mathrm{inj},\mathrm{inj})}(n+2) \implies \mathrm{GPCP}^{(\mathrm{inj},\mathrm{inj})}(n)$

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

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

The above does not prove that $\mathrm{PCP}^{\mathrm{inj}} \Leftrightarrow \mathrm{GPCP}^{\mathrm{inj}}$, because I_{PCP} might have solutions of the form BxB^{-1} or $E^{-1}xE$. For example, if we let $I_{\mathrm{GPCP}} = (\{a\}, \{a, c, d\}, g, h, c, \epsilon, \epsilon, d)$ with $g(a) = a$ and $h(a) = cac^{-1}$, then there is no $x \in F(a)$ such that $cg(a) = h(a)d$, but defining g', h' as above then $BaB^{-1} \in \mathrm{Eq}(g', h')$. In Section 7.2 we consider maps where such solutions are impossible, and there the equivalence $\mathrm{PCP}^{\mathrm{inj}} \Leftrightarrow \mathrm{GPCP}^{\mathrm{inj}}$ does hold.

Undecidability of $\mathrm{PCP}_{\mathcal{EL}}$ The link between the GPCP and $\mathrm{PCP}_{\mathcal{EL}}$ yields the following theorem, which immediately implies Theorem B.

Theorem 3 (Theorem B). $\mathrm{PCP}_{\mathcal{EL}}^{(\neg\,\mathrm{inj},\neg\,\mathrm{inj})}$ *is undecidable in f.g. free groups.*

Proof. We have $\mathrm{PCP}_{\mathcal{EL}}^{(\neg\,\mathrm{inj},\neg\,\mathrm{inj})} \Rightarrow \mathrm{GPCP}^{(\neg\,\mathrm{inj},\neg\,\mathrm{inj})}$ by Lemmas 3 and 4. The result follows as $\mathrm{GPCP}^{(\neg\,\mathrm{inj},\neg\,\mathrm{inj})}$ is undecidable by Lemma 2. □

6 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 implications hold in f.g. free groups.*

1. $\mathrm{BP}^{(\neg\,\mathrm{inj},\mathrm{inj})}(n+2) \implies \mathrm{GPCP}^{(\neg\,\mathrm{inj},\mathrm{inj})}(n) \implies \mathrm{PCP}^{(\neg\,\mathrm{inj},\mathrm{inj})}(n)$
2. $\mathrm{BP}^{(\mathrm{inj},\mathrm{inj})}(n+2) \implies \mathrm{GPCP}^{(\mathrm{inj},\mathrm{inj})}(n) \implies \mathrm{PCP}^{(\mathrm{inj},\mathrm{inj})}(n)$

Proof. As $\mathrm{PCP}_{\mathcal{EL}}^{(\neg\,\mathrm{inj},\mathrm{inj})}$ is an instance of the $\mathrm{PCP}^{\mathrm{inj}}$ under a rational constraint, Theorem 1 gives us that $\mathrm{BP}^{(\neg\,\mathrm{inj},\mathrm{inj})}(n+2) \Rightarrow \mathrm{PCP}_{\mathcal{EL}}^{(\neg\,\mathrm{inj},\mathrm{inj})}(n+2)$, while Theorem 2 gives us that $\mathrm{PCP}_{\mathcal{EL}}^{(\neg\,\mathrm{inj},\mathrm{inj})}(n+2) \Rightarrow \mathrm{GPCP}^{(\neg\,\mathrm{inj},\mathrm{inj})}(n)$, and the implication $\mathrm{GPCP}^{(\neg\,\mathrm{inj},\mathrm{inj})}(n) \Rightarrow \mathrm{PCP}^{(\neg\,\mathrm{inj},\mathrm{inj})}(n)$ 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 $\Rightarrow$ $\mathrm{GPCP}^{\mathrm{inj}}$ $\Rightarrow$ PCP of Theorem A follow immediately.

Corollary 1. $\mathrm{BP}(n+2) \implies \mathrm{GPCP}^{\mathrm{inj}}(n) \implies \mathrm{PCP}(n)$

Proof. Theorem 4 gives that $\mathrm{BP}(n+2) \Rightarrow \mathrm{GPCP}^{\mathrm{inj}}(n) \Rightarrow \mathrm{PCP}^{\mathrm{inj}}(n)$, while $\mathrm{PCP}(n) \Leftrightarrow \mathrm{PCP}^{\mathrm{inj}}(n)$ by Proposition 1. □

7 Conjugacy Inequivalent Maps: $\mathrm{PCP}^{\mathrm{CI}}$ and $\mathrm{PCP}^{\mathrm{inj}\,+\,\mathrm{CI}}$

In this section we prove genericity results and give conditions under which the PCP implies the GPCP. In particular, we prove Theorem C, and we prove the implication PCP $\Rightarrow$ $\mathrm{GPCP}^{\mathrm{inj}\,+\,\mathrm{CI}}$ 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 $g(x) = u^{-1}h(x)u$ (see Table 1). For example, if the images of $g, h : F(\Sigma) \to F(\Delta)$ are *conjugacy separated*, that is, if $\mathrm{Im}(g) \cap u^{-1}\,\mathrm{Im}(h)u$ is trivial for all $u \in F(\Delta)$, then g and h are conjugacy inequivalent. We write $\mathrm{PCP}^{\mathrm{inj}\,+\,\mathrm{CI}}/\mathrm{GPCP}^{\mathrm{inj}\,+\,\mathrm{CI}}$ for those instances of the $\mathrm{GPCP}^{\mathrm{inj}}/\mathrm{PCP}^{\mathrm{inj}}$ where the maps are conjugacy inequivalent.

7.1 Random Maps and Genericity

Here we show that among all pairs of homomorphisms $g, h : F(\Sigma) \to F(\Delta)$, the property of being conjugacy inequivalent occurs with probability 1; that is, conjugacy inequivalent maps are *generic*. In fact, a stronger result holds: *injective* conjugacy inequivalent maps are already generic, as we show below.

Theorem 5 (Theorem C). *With probability* 1*, an arbitrary pair of maps consists of injective maps that are conjugacy inequivalent. That is, instances of the* $\mathrm{PCP}^{\mathrm{inj}\,+\,\mathrm{CI}}$ *are generic instances of the* PCP*.*

Before we prove the theorem, we need to describe the way in which probabilities are computed. We consider maps sending generators to words of length $\leq n$, and consider asympotics as $n \to \infty$. Formally: Fix the two alphabets $\Sigma = \{x_1, \ldots, x_m\}$ and $\Delta = \{y_1, \ldots, y_k\}$, $m, k \geq 2$, and ambient free groups $F(\Sigma)$ and $F(\Delta)$, 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 $F(\Delta)$. If $\mathcal{P}$ is a property of tuples (or subgroups) of $F(\Delta)$, we say that *generically many* tuples (or finitely generated subgroups) of $F(\Delta)$ satisfy $\mathcal{P}$ if the proportion of m-tuples of words of length $\leq n$ in $F(\Delta)$ which satisfy $\mathcal{P}$ (or generate a subgroup satisfying $\mathcal{P}$), 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 $\mathrm{Im}(g)$ and $\mathrm{Im}(h)$ 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 [16], while claim (2) is equivalent to $\mathrm{Im}(g)^u \cap \mathrm{Im}(h) = \{1\}$ 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. □

7.2 The GPCP for Conjugacy Inequivalent Maps

We now prove that the PCP implies the $\mathrm{GPCP}^{\mathrm{inj}\,+\,\mathrm{CI}}$ and hence that, generically, the PCP implies the GPCP. Recall that if I_{GPCP} is a specific instance of the GPCP we can associate to it a specific instance $I_{\mathrm{PCP}} = (\Sigma \sqcup \{B, E\}, \Delta \sqcup \{B, E, \#\}, g', h')$, as in Section 5. We start by classifying the solutions to I_{PCP}.

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

We now have:

Theorem 6. *Let $I_{\mathrm{GPCP}} = (\Sigma, \Delta, g, h, u_1, u_2, v_1, v_2)$ be an instance of the* $\mathrm{GPCP}^{\mathrm{inj}}$*, 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* $\mathrm{PCP}^{\mathrm{inj}}$ *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. □

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 implications hold in f.g. free groups.*

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

Removing the injectivity assumptions gives the following corollary; the implication PCP ⇒ $\mathrm{GPCP}^{\mathrm{inj}\,+\,\mathrm{CI}}$ of Theorem A follows immediately.

Corollary 2. $\mathrm{PCP}(n+2) \implies \mathrm{GPCP}^{\mathrm{inj}\,+\,\mathrm{CI}}(n)$

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

8 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: RP ⇒ $\mathrm{GPCP}^{\mathrm{inj}}$ ⇒ PCP.

Lemma 6 is proven using the "derived graph" construction of Goldstein–Turner [10].

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

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

Theorem 8. *The following implications hold in f.g. free groups.*

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

Proof. Let I_{PCP} be an instance of the $\mathrm{PCP}^{\mathrm{inj}}$. 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 $\mathrm{Eq}(g,h)$ then we can compute the rank of $\mathrm{Eq}(g,h)$. On the other hand, by Lemma 6 if we can compute the rank of $\mathrm{Eq}(g,h)$ then we can compute a basis of $\mathrm{Eq}(g,h)$. □

9 Main Results, part 2

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

Theorem 9. *The following implications hold in f.g. free groups.*

$$\begin{tikzcd}
\mathrm{RP}(n+2) \arrow[d, Leftrightarrow] & & & \\
\mathrm{BP}(n+2) \arrow[r, Rightarrow] \arrow[d, Rightarrow] & \mathrm{GPCP}^{\mathrm{inj}}(n) \arrow[r, Rightarrow] & \mathrm{PCP}(n) \arrow[r, Rightarrow] & \mathrm{GPCP}^{\mathrm{inj}\,+\,\mathrm{CI}}(n-2) \\
\mathrm{PCP}^{\mathrm{inj}}_{\mathcal{R}}(n+2) & & &
\end{tikzcd}$$

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.

$\mathrm{RP}(n+2) \Leftrightarrow \mathrm{BP}(n+2)$ holds by Theorem 8.

$\mathrm{BP}(n+2) \Rightarrow \mathrm{PCP}^{\mathrm{inj}}_{\mathcal{R}}(n+2)$ holds by Theorem 1.

$\mathrm{BP}(n+2) \Rightarrow \mathrm{GPCP}^{\mathrm{inj}}(n) \Rightarrow \mathrm{PCP}(n)$ holds by Corollary 1.

$\mathrm{PCP}(n) \Rightarrow \mathrm{GPCP}^{\mathrm{inj}\,+\,\mathrm{CI}}(n-2)$ holds by Corollary 2. □

Removing the $\mathrm{GPCP}^{\mathrm{inj}}(n)$-term gives a different picture of alphabet sizes:

Theorem 10. $\mathrm{BP}(n+2) \implies \mathrm{PCP}(n+2) \implies \mathrm{GPCP}^{\mathrm{inj}\,+\,\mathrm{CI}}(n)$

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/31t.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)