THE EMBEDDING PROPERTY, REVISITED

JUNGUK LEE
DEPARTMENT OF MATHEMATICAL SCIENCES, KAIST

Abstract. In this note, we consider the embedding property for profinite groups. We aim to prove the existence and uniqueness of the universal embedding cover for a profinite group.

Using the fact that the category of profinite groups is closed under taking the inverse limit and the fibre product, we show that a profinite group has a universal embedding cover. We recall the notion of the complete system of a profinite group and we define the co-embedding property for complete systems, dual to the embedding property for profinite groups. We see that the theory of a complete system having co-embedding property is $\aleph_0$-categorical and ω-stable. Using the uniqueness of prime models of countable ω-stable theories, we prove the uniqueness of the universal embedding cover.

1. Introduction

For a profinite group G, let $\mathrm{IM}(G)$ be the set of isomorphism classes of finite quotients of G. By abusing notation, we use $\mathrm{IM}(G)$ for the class of finite quotients of G, that is, for a finite group A, $A \in \mathrm{IM}(G)$ if and only if there is an epimorphism $\varphi : G \to A$. We say that G has *the embedding property* (EP) if for $A, B \in \mathrm{IM}(G)$, and for every epimorphisms $\Pi : A \to B$ and $\varphi : G \to B$, there is an epmorphism $\psi : G \to A$ such that $\Pi \circ \psi = \varphi$. As far as I know, the embedding property was first appeared in the work of Iwasawa on the Galois group of the maximal solvable extensions of number fields in [11] and so it is also called *the Iwasawa property* (c.f. [3, 1]). Let $k^{ab} \subseteq k^{sol}$ be the maximal abelian extension and the maximal solvable extension of a number field k respectively. In [11], Iwasawa showed that the Galois group $G(k^{sol}/k^{ab})$ has the embedding property. The embedding property for profinite groups appears surprisingly in field arithmetic and model theory of fields. A Frobenius field is a PAC field whose absolute Galois group has the embedding property. Fried, Haran, and Jarden in [6] developed Galois stratification of definable sets of a Frobenius field. In [9], Haran and Lubotzky gave a primitive recursive procedure to construct the universal embedding cover of a given finite group. Combined with Galois stratification and their primitive recursive procedure, they showed that the theory of perfect Frobenius fields is primitive recursive, and the theory of all Frobenius fields is decidable. In [1], Chatzidakis showed that the complete

The author is supported by KAIST Advanced Institute for Science-X fellowship.

system of a profinite group having the embedding property is ω-stable. Using this with Chatzidakis' independence theorem ([2, Theorem 3.1]), Ramsey in [12, Theorem 3.9.31] showed that the theory of a Frobenius field is NSOP_1.

In this note, we aim to prove that any profintie group has a universal embedding cover and such a universal cover is unique. Chatzidakis in [1] proved the uniqueness of the universal embedding cover for arbitrary profinite groups using the complete system of a profinite group. As fas as I know, this model theoretic proof is the only known proof working for all profinite groups. We will prove the existence and uniqueness based on my recent paper [8].

2. Preliminaries

2.1. Profinite groups. Through this note, we consider only profinite groups. The category of profinite groups, denoted by PG, is consisted the following data:

- $\mathrm{Ob}(\mathrm{PG})$: the family of profinite groups.
- $\mathrm{Mor}_{\mathrm{PG}}$: For $A, B \in \mathrm{Ob}(\mathrm{PG})$, a morphism from A to B is a continuous homomorphism.

We recall the inverse limit and the fibre product in the category PG.

Remark 2.1. Let $(I, \leq)$ be a partially ordered set such that for all $i, j \in I$ there is $k \in I$ such that $i, j \leq k$. Consider the inverse system $(G_i, \pi_{i,j} : G_i \to G_j)_{j \leq i \in I}$ of profintie groups, that is,

- each $\pi_{i,j}$ is an epimorphism.
- $\pi_{i,i} = \mathrm{id}_{G_i}$.
- $\pi_{j,k} \circ \pi_{i,j} = \pi_{i,k}$ for $i \geq j \geq k$.

Then, the inverse limit $G := \varprojlim G_i$ is again a profinite group.

Definition 2.2. Let $\Pi_1 : B_1 \to A$ and $\Pi_2 : B_2 \to A$ be epimorphisms. The *fibre product* of B_1 and B_2 over A along Π_1 and Π_2 is the subgroup of $B_1 \times B_2$,

$$\{(b_1, b_2) \in B_1 \times B_2 : \Pi_1(b_1) = \Pi_2(b_2)\}.$$

The fibre product of B_1 and B_2 over A is again a profinite.

We have the following characterization of the fibre product.

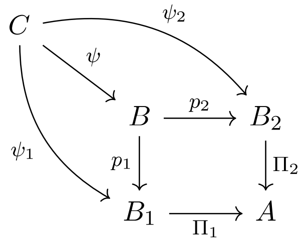
Remark 2.3. [9, Lemma 1.1] Consider a commutative diagram of groups with epimorphisms :

$$\begin{array}{ccc} B & \xrightarrow{p_2} & B_2 \\ {\scriptstyle p_1}\downarrow & & \downarrow{\scriptstyle \Pi_2} \\ B_1 & \xrightarrow[\Pi_1]{} & A \end{array}$$

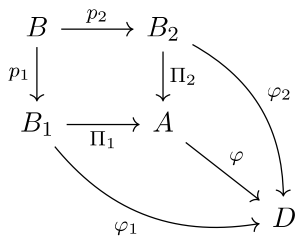
and put $p = \Pi_1 \circ p_1 = \Pi_2 \circ p_2$. The following are equivalent:

(1) B is isomorphic to the fibre product of B_1 and B_2 over A.

(2) B with p_1 and p_2 is a pullback of the pair (Π_1, Π_2), that is, for any morphisms $\psi_i : C \to B$ for $i = 1, 2$ with $\Pi_1 \circ \psi_1 = \Pi_2 \circ \psi_2$, there is a unique morphism $\psi : C \to B$ such that $p_i \circ \psi = \psi_i$ for $i = 1, 2$.



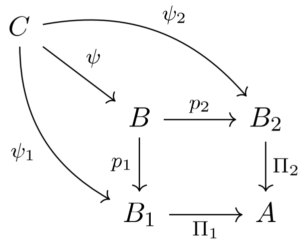
(3) $\operatorname{Ker} p_1 \cap \operatorname{Ker} p_2 = \{e\}$, and A with Π_1, Π_2 is a pushout of the pair (p_1, p_2), that is, for any homomorphism $\varphi_i : B_i \to D$ for $i = 1, 2$ with $\varphi_1 \circ p_1 = \varphi_2 \circ p_2$, there is a unique homomorphism $\varphi : A \to D$ such that $\varphi \circ \Pi_i = \varphi_i$ for $i = 1, 2$.



(4) $\operatorname{Ker} p = \operatorname{Ker} p_1 \times \operatorname{Ker} p_2$.

A diagram satisfying one of the above properties is called *cartesian.*

Remark 2.4. [9, Lemma 1.2] Let $\psi_i : C \to B_i$ be a epimorphism for $i = 1, 2$. Then, there is a commutative diagram:



, where the square is cartesian and ψ is a epimorphism. Moreover, we can take A as $C/ \operatorname{Ker}(\psi_1) \operatorname{Ker}(\psi_2)$.

2.2. **Embedding property.** In this section, we recall the definition of a cover and an embedding cover and we will provide a criterion for a cover not to be an embedding cover.

Definition 2.5. Let G be a profinite group.

(1) A *cover* of G is an epimorphism $\varphi : H \to G$.
(2) A cover $\varphi : H \to G$ is called an *embedding cover* if H has the embedding property.

(3) An embedding cover $\varphi : H \to G$ is called *universal* if any embedding cover $\psi : H' \to G$ factors through φ, that is, there is an epimorphism $\Pi : H' \to H$ such that $\psi = \varphi \circ \Pi$.

We call H a cover, an embedding cover, or a universal embedding cover respectively if the cover $\varphi : H \to G$ is.

Example 2.6. (1) $C_2 \times C_2$ has the embedding property where C_n is the cyclic group of order n.
(2) For a cardinal κ, the free profinite group $\mathbb{F}_\kappa$ of rank κ has EP.
(3) For any finite group G, there is an embedding cover $\varphi : H \to G$ with H finite (c.f. [9, Corollary 1.6]).
(4) (Ershov-Fried in [5, Section 2]) Let $G := S_3 \times C_2 (\cong (C_3 \rtimes C_2) \times C_2)$. Then, G has no EP because $G/S_3 \cong G/(C_3 \times C_2) \cong C_2$ but $S_3 \not\cong C_3 \times C_2$.

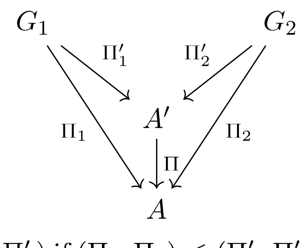
Next, we consider the set of fibre products of given groups G_1 and G_2. Let $p_i : G_1 \times G_2 \to G_i$ be the projection map for $i = 1, 2$. Define

$$\mathcal{H} := \mathcal{H}(G_1, G_2) = \{H \leq G_1 \times G_2 : p_i(H) = G_i, i = 1, 2\},$$

which is partially ordered by inclusion. By Remark 2.4, each group H in $\mathcal{H}$ is a fibre product of G_1 and G_2. Namely, let $A := H/\operatorname{Ker}(p_1 \restriction_H) \operatorname{Ker}(p_2 \restriction_H)$, and for each $i = 1, 2$, let $\Pi_i : G_i \to A, p_i(h) \mapsto h/A$ for $h \in H$. Then, H is the fibre product of G_1 and G_2 over A along Π_1 and Π_2. Now we consider a dual notion to $\mathcal{H}$. Consider the class of pairs of epimorphisms with common images,

$$\mathcal{P} := \mathcal{P}(G_1, G_2) = \{(\Pi_1, \Pi_2) : \Pi_i : G_i \to A, i = 1, 2\},$$

and consider a pre-order relation $\leq$ on $\mathcal{P}$ as follows: For (Π_1, Π_2) and (Π_1', Π_2') in $\mathcal{P}$, $(\Pi_1, \Pi_2) \leq (\Pi_1', \Pi_2')$ if and only if there is an epimorphism $\Pi : A' \to A$ for $A := \operatorname{Im}(\Pi_1)(= \operatorname{Im}(\Pi_2))$ and $A' := \operatorname{Im}(\Pi_1')(= \operatorname{Im}(\Pi_2'))$ such that



We write $(\Pi_1, \Pi_2) \approx (\Pi_1', \Pi_2')$ if $(\Pi_1, \Pi_2) \leq (\Pi_1', \Pi_2')$ and $(\Pi_1', \Pi_2') \leq (\Pi_1, \Pi_2)$.

Remark 2.7. $(\Pi_1, \Pi_2) \approx (\Pi_1', \Pi_2')$ if and only if Π is an isomorphism. Thus, the relation $\approx$ is an equivalence relation.

Proof. It is enough to show the left-to-right direction. Suppose $(\Pi_1, \Pi_2) \approx (\Pi_1', \Pi_2')$. Then, there are epimorphisms Π and Π' witnessing $(\Pi_1, \Pi_2) \leq (\Pi_1', \Pi_2')$ and $(\Pi_1', \Pi_2') \leq (\Pi_1, \Pi_2)$ respectively. Then, we have that $\Pi_i \circ \Pi' \circ \Pi = \Pi_i$ for $i = 1, 2$. Since each Π_i is surjective, $\Pi' \circ \Pi$ is injective.

Therefore, Π is injective and Π is an isomorphism. Similarly, Π' is also an isomorphism. □

Then, the pre-order $\leq$ on $\mathcal{P}$ induces a partial order on the set $\mathcal{P}/\sim$, still denoted by $\leq$. If there is no confusion, we write $(\mathcal{P}, \leq)$ for the partially ordered set $(\mathcal{P}/\approx, \leq)$. Now we define a map $T : \mathcal{P} \to \mathcal{H}$ by sending (Π_1, Π_2) to

$$T(\Pi_1, \Pi_2) := \{(g_1, g_2) \in G_1 \times G_2 : \Pi_1(g_1) = \Pi_2(g_2)\}.$$

Note that $T(\Pi_1, \Pi_2)$ is the fibre product of G_1 and G_2 along Π_1 and Π_2.

Lemma 2.8. [9, Lemma 1.7] *The map T induces an order-reversing bijection between two posets $\mathcal{P}$ and $\mathcal{H}$.*

Proof. It is clear that T is order-reversing. It remains to show that it is bijective. The map T is surjective by Remark 2.4, and injective by Remark 2.3(3). □

Using Zorn's Lemma with the inverse limit, we have the following result:

Lemma 2.9. [9, Lemma 1.8] *For every $(\Pi_1, \Pi_2) \in \mathcal{P}$, there is a maximal element $(\Pi_1', \Pi_2') \in \mathcal{P}$ such that $(\Pi_1, \Pi_2) \leq (\Pi_1', \Pi_2')$. Dually, for every $H \in \mathcal{H}$, there is a minimal $H' \in \mathcal{H}$ with $H' \subset H$.*

We introduce the notion of the *quasi-embedding cover* (q.e.c.) of a profinite group in [9, p. 189], or called the I-cover in [7, Definition 24.4.3].

Definition 2.10. A cover $p : H \to G$ is called a *quasi-embedding cover* (q.e.c.) if for every embedding cover $\varphi : E \to G$, there is an epimorphism $\psi : E \to H$.

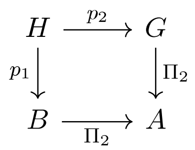
By the definition of the quasi-embedding cover, we have the following properties.

Remark 2.11. Let G be a profinite group whose rank is κ.

(1) If two epimorphisms $p : H \to G$ and $\Pi : G \to A$ are q.e.c., then $\Pi \circ p$ is a q.e.c.
(2) For any q.e.c. $p : H \to G$, the cardinality of H is less than or equal to the cardinality of $\mathbb{F}_\kappa$. Furthermore, if G is finite, then so is H because the universal embedding cover of G is finite (c.f. Example 2.6(2) and (3)).
(3) Let $p : H \to G$ be a q.e.c. which is an embedding cover. Then, p is a universal embedding cover.

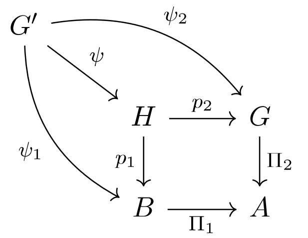
Any maximal element in $\mathcal{P}(B, G)$ for $B \in \mathrm{Im}(G)$ provides a q.e.c. (c.f. in the proof of [7, Lemma 24.4.4]).

Lemma 2.12. *Let G be a profinite group and let $B \in IM(G)$. Let $(\Pi_1, \Pi_2) \in \mathcal{P}(B, G)$ be a maximal element. Consider the following cartesian diagram* *induced from* (Π_1, Π_2)*:*



Then, p_2 *is a q.e.c.*

Proof. Let $\psi_2 : G' \to G$ be an embedding cover. Then, B is in $\mathrm{IM}(G')$. Since G' has EP, there is an epimorphism $\psi_1 : G' \to B$ such that $\Pi_1 \circ \psi_1 = \Pi_2 \circ \psi_2$. Since H is the fibre product of B and G over A, by Remark 2.3(2), there is a homomorphism $\psi : E \to H$ such that the following diagram is commutative:



Then, $\psi[E] \in \mathcal{H}$. Since $\psi[E] \leq H$ and H is minimal (by Lemma 2.9), we have that $\psi[E] = H$ so ψ is an epimorphism. Therefore, we have that $\psi_2 = p_2 \circ \psi$ for an epimorphism ψ, and p_2 is a q.e.c. □

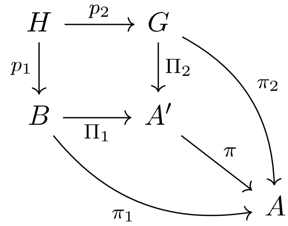
Finally, we have the following characterization of profinite groups having no EP.

Lemma 2.13. [7, Lemma 24.4.4] *If a profinite group* G *does not have EP, then there exists a q.e.c.* $p : H \to G$ *with a non-trivial kernel.*

Proof. Suppose a profinite group G has no EP. So, there exists

- $A, B \in \mathrm{IM}(G)$; and
- epimorphisms $\pi_1 : B \to A$ and $\pi_2 : G \to A$,

such that there is no epimorphism $p : G \to B$ with $\pi_2 = \pi_1 \circ p$. By Lemma 2.9, there is a maximal element $(\Pi_1, \Pi_2) \in \mathcal{P}(B, G)$ such that $(\pi_1, \pi_2) \leq (\Pi_1, \Pi_2)$. Then, we have the following diagram:



,

where H is the fibre product of B and G over A'.

Note that p_2 is a q.e.c. by Lemma 2.12. Suppose p_2 is an isomorphism. Let $p = p_1 \circ p_2^{-1}$. Then, we have that

$$\begin{aligned}\pi_1 \circ p &= \pi_1 \circ (p_1 \circ p_2^{-1}) \\ &= ((\pi \circ \Pi_1) \circ p_1) \circ p_2^{-1} \\ &= \pi \circ (\Pi_2 \circ p_2) \circ p_2^{-1} \\ &= \pi \circ \Pi_2 \\ &= \pi_2,\end{aligned}$$

which is a contradiction. So, p_2 is not an isomorphism and so it has the non-trivial kernel. □

2.3. **Complete systems.** We recall the notion of the complete system of a profinite group (c.f. [1, Section 1] or [10, Subsection 3.2]). For a profinite group G, we denote $\mathcal{N}(G)$ by the set of open normal subgroups of G, which forms a partially ordered set with inclusion. For a given profinite group G, we associate an algebraic structure, called the *complete system*, encoding the inverse system $(G/N, \pi_{N_1,N_2} : G/N_1 \to G/N_2)_{N_2 < N_1 \in \mathcal{N}(G)}$. The complete system $S(G)$ of G is an ω-sorted structure equipped with three different kinds of operations C, $\leq$, and P given as follows:

- For each $k \in \omega$, the sort
$$m(k) = \bigcup_{N \in \mathcal{N}(G), [G:N] \leq k+1} G/N.$$
- For $k' \leq k \in \omega$, $\leq_{k,k'}$ is a binary relation on $m(k) \times m(k')$ defined as follows: For $gN \in m(k)$ and $g'N' \in m(k')$,
$$gN \leq g'N' \Leftrightarrow N \subset N'.$$
- For $k' \leq k \in \omega$, $C_{k,k'}$ is a binary relation on $m(k) \times m(k')$ defined as follows: For $gN \in m(k)$ and $g'N' \in m(k')$,
$$C(gN, g'N') \Leftrightarrow gN \subset g'N'.$$
- For each $k \in \omega$, P_k is a ternary relation on $m(k)^3$ defined as follows: For $g_1N_1, g_2N_2, g_3N_3 \in m(k)$,
$$P(g_1N_1, g_2N_2, g_3N_3) \Leftrightarrow N_1 = N_2 = N_3 (=: N) \wedge g_1g_2N = g_3N.$$

Note that each sort $m(k)$ is disjoint. So, the complete system $S(G)$ is a first order structure in the language $\mathcal{L}_{\mathrm{CS}}$ consisting of the following non-logical symbols:

- a family of binary relations $\leq_{k,k'}$ and $C_{k,k'}$ for $k' \leq k \in \omega$,
- a family of ternary relations P_k for $k \in \omega$.

If there is no confusion, we omit scripts and write $\leq$, C and P for $\leq_{k,k'}$, $C_{k,k'}$, and P_k. Let CS be the theory of all complete systems of profinite groups. Then, CS is axiomatized in the following axioms (c.f. [10, Definition 3.7]):

(1) • (order) $\leq$ is reflexive and transtivie on S.

- (maximal element) $|m(0)| = 1$ and for all $k \in \omega$,
$$(\forall x \in m(0), \forall y \in m(k))(y \le x).$$

(2) Define $x \sim y$ as $x \le y \wedge y \le x$. Denote the $\sim$-class of a by $[a]$ for $a \in m(k)$ and set $[a]_k := [a] \cap m(k)$.
- (extending tuples) For $k' \le k \in \omega$,
$$(\forall a \in m(k'), \exists b \in m(k))(a \le b).$$
- (finiteness) $(\forall a \in m(k))(|[a]_k| \le k)$.
- (degree continuity) For $n \le k \in \omega$,
$$(\forall a \in m(n), \exists a' \in m(k))(a \sim a').$$
- (reducing degree) For $n \le k \in \omega$,
$$(\forall a \in m(k)) \left(|[a]_k| \le n \to \exists a' \in m(n)(a \sim a')\right).$$
- (group) For $k \in \omega$ and $a \in m(k)$, $([a]_k, P \cap [a]_k^3)$ forms a group.

(3)
- (intersection $H \cap H'$) For $k, k', k'' \in \omega$,
$$(\forall a \in m(k), b \in m(k'), c \in m(k''))\big(c \le a \wedge c \le b \to \exists d \in m(kk')(c \le d \wedge d \le a \wedge d \le b)\big).$$
- (subgroup $H \subseteq H'$)) For $k, k' \in \omega$,
$$(\forall a \in m(k), b \in m(k'))\big(a \le b \to (\exists c \in m(k))(b \sim c)\big).$$

(4) (modular lattice) For each $S \models$ CS, $(S/\sim, \le)$ forms a modular lattice, which can be written as $\mathcal{L}_{\mathrm{CS}}$-sentences.

(5)
- $C(a, b) \to a \le b$.
- (projections) For all $a \in m(k)$ and $b \in m(k')$, if $a \le b$, then $C \cap ([a]_k \times [b]_{k'})$ is the graph of a group epimorphism $\pi_{a,b} : [a]_k \to [b]_{k'}$.
- (compatible system) For $k \in \omega$ and $a \in m(k)$, $\pi_{a,a} = \mathrm{id}_{[a]_k}$, and if $a \le b \le c$, then $\pi_{a,c} = \pi_{b,c} \circ \pi_{a,b}$.

(6) (normal subgroups) For $k \in \omega$ and $a \in m(k)$, and for any normal subgroup N of $[a]_k$, there is a unique $b \in m(k)$ such that
$$C(a, b) \wedge N = \{a^{-1}c : c \in [a]_k \wedge C(a, b)\}.$$

(7) (hidden axiom) For $k, k', k'' \in \omega$ and $a \in m(k), b \in m(k'), c \in m(k'')$, if $a \le b \wedge a \le c \wedge \mathrm{Ker}(\pi_{a,b}) = \mathrm{Ker}(\pi_{a,c})$, then $b \sim c$.

Also, any model of CS is a complete system of a profinite group. Namely, let $S \models$ CS. Then, we have an inverse system $([a]_k, \pi_{a,b})_{a \le b \in S}$. Put $G(S) := \varprojlim [a]_k$. Then, for each $N \in \mathcal{N}(G(S))$, there is $a \in m(k)(S)$ such that $N = \mathrm{Ker}(\pi_a)$ where π_a is the natural projection from $G(S)$ to $[a]_k$, which implies that $S(G(S)) \cong S$. Consider the category $\mathcal{CS}$ of complete systems whose morphisms are $\mathcal{L}_{\mathrm{CS}}$-embeddings. Let PG$'$ be a subcategory of PG given as follows:

- $\mathrm{Ob}(\mathrm{PG}') = \mathrm{Ob}(\mathrm{PG})$.

- $\mathrm{Mor}_{\mathrm{PG}'}$: For $A, B \in \mathrm{Ob}(\mathrm{PG}')$, a morphism from A to B is a continuous epimorphism.

Remark 2.14. Two categories PG' and $\mathcal{CS}$ are equivalent via the contravariant functors $S : \mathrm{PG}' \to \mathcal{CS}$ and $G : \mathcal{CS} \to \mathrm{PG}'$.

Definition 2.15. Let $S \models \mathrm{CS}$ be a complete system.

(1) A *subsystem* of S is a substructure of S which is a model of CS.
(2) Let $X \subset S$. By Zorn's Lemma, there is the smallest subsystem S_X containing X. In this case, we say that S_X is *generated by* X. Note that $S_X \subset \mathrm{acl}(X)$.
(3) Let X be a subset of S. We say that X is *full* if for each $x \in X$ and for each $k \in \omega$, $[x] \cap m(k) \subset X$.
(4) A subset X of S is called *relatively dense* if for each $s \in S_X$, there is $x \in X$ such that $x \leq s$.
(5) A subset X of S is called a *presystem* if it is full and relatively dense.

Remark/Definition 2.16. *(1) If X is full, then $S_X \subset \mathrm{dcl}(X)$, and if X is a presystem, then any embedding from S_X to S is uniquely determined by the image on X.*
(2) We say that a subsystem S' is finitely generated *if there is a finite subset X' such that $S' = S_{X'}$. Also, we can take such X' as a presystem. Note that a subsystem S' is finitely generated if and only if $G(S')$ is finite.*

Definition 2.17. Let S_1 and S_2 be finitely generated subsystems of S.

(1) $\min S_1 := \{a \in S_1 : \forall b \in S_1 (a \leq b)\}$.
(2) $S_1 \vee S_2 := \{c \in m(kk') : [c] = [a] \vee [b], a \in \min S_1 \cap m(k), b \in \min S_2 \cap m(k')\}$.

Let A and B be subsets of S. We write $A \leq B$ if $a \leq b$ for every $a \in A$ and $b \in B$. We write $A \sim B$ if $a \sim b$ for every $a \in A$ and $b \in B$. Note that for any subsystems S_1 and S_2 of S, and for $S_3 = S_{S_1 \cup S_2}$, we have that $\min S_3 \sim S_1 \vee S_2$.

From the characterization of the fibre product in Remark 2.3, we have the following.

Lemma 2.18. *Let S_0, S_1, and S_2 be finitely generated subsystems of S such that $S_0 \subset S_1 \cap S_2$, and let $S_3 = S_{S_1 \cup S_2}$. Consider the following inclusions:*

- $\iota_{S_0,S_1} : S_0 \to S_1$, $\iota_{S_0,S_2} : S_0 \to S_2$;
- $\iota_{S_1,S_3} : S_1 \to S_3$;
- $\iota_{S_2,S_3} : S_2 \to S_3$.

(1) *Suppose* $S_1 \vee S_2 \sim \min S_0$. *Then,* S_3 *is the* co-fibre product *of* S_1 *and* S_2 *over* S_0*, that is, we have the following cartesian diagram:*

$$\begin{array}{ccc} G(S_3) & \xrightarrow{G(\iota_{S_2,S_3})} & G(S_2) \\ {\scriptstyle G(\iota_{S_1,S_3})}\downarrow & & \downarrow{\scriptstyle G(\iota_{S_0,S_2})} \\ G(S_1) & \xrightarrow[G(\iota_{S_0,S_1})]{} & G(S_0) \end{array}$$

(2) *Let* S_1' *be a subsystem of* S *such that* $S_0 \subset S_1'$ *and* $S_1' \vee S_2 \sim \min S_0$. *Suppose there is an isomorphism* $f : S_1 \to S_1'$ *making the following diagram commute:*

$$\begin{array}{ccc} S_0 & \xrightarrow{\iota_{S_0,S_1}} & S_1 \\ {\scriptstyle \mathrm{id}}\downarrow & & \downarrow{\scriptstyle f} \\ S_0 & \xrightarrow[\iota_{S_0,S_1'}]{} & S_1' \end{array},$$

then there is an isomorphism from $g : S_3 \to S_3'$ *extending* $f \cup \mathrm{id}_{S_2}$*, where* $S_3' = S_{S_1' \cup S_2}$.

Remark 2.19. For finitely generated subsystems S_1 and S_2 of S, the subsystem $S_{S_1 \cup S_2}$ is a co-fibre product of S_1 and S_2 over S_0, where S_0 is the subsystem generated by $(S_1 \vee S_2) \cap S_1 \cap S_2$.

Next, we introduce a dual notion of embedding property, called the *co-embedding property* for complete systems.

Definition 2.20. We say that S has the *co-embedding property* (co-EP) if for any finitely generated subsystems $S_1, S_2 \subset S$, and for any embeddings $\Pi : S_2 \to S_1$ and $\Phi : S_2 \to S$, there is an embedding $\Psi : S_1 \to S$ such that

$$\begin{array}{ccc} S_2 & \xrightarrow{\Pi} & S_1 \\ {\scriptstyle \Phi}\downarrow & & \downarrow{\scriptstyle \Psi} \\ S_2 & \xrightarrow[\iota]{} & S \end{array},$$

where ι is the inclusion.

Remark 2.21. By Remark/Definition 2.16(1), co-EP is first order axiomatizable in the language $\mathcal{L}_{CS}$ and let CS_{EP} be the theory of complete systems having co-EP.

Since the category PG' of sorted profinite groups and the category $\mathcal{CS}$ of complete systems are equivalent by contravariant functors, we have the following relationship between EP and co-EP.

Remark 2.22. Let G be a profinite group. We have that G has EP if and only if $S(G)$ has co-EP.

For a complete system S, denote $\mathrm{coIM}(S)$ for the set of isomorphism classes of finitely generated subsystems of S.

Lemma 2.23. [1, Theorem 2.2] *Let S_1 and S_2 be complete systems having co-EP. Suppose $|S_1| = |S_2| = \aleph_0$ and $\mathrm{coIM}(S_1) = \mathrm{coIM}(S_2)$. Then, $S_1 \cong S_2$.*

Proof. We will prove by the back-and-forth argument. List $S_1 = \{\alpha_0, \alpha_1, \ldots\}$ and $S_2 = \{\beta_0, \beta_1, \ldots\}$. Inductively, we construct an increasing sequence of isomorphisms $f_i : S_i^1 \to S_i^2$ between finitely generated subsystems of S_1 and S_2 respectively such that for $i \in \omega$, $\alpha_i \in S_i^1$ if i is even, and $\beta_i \in S_i^2$ if i is odd. For each $k = 1, 2$, let S_{-1}^k be the trivial subsystem of $S(G_i)$, that is, $m(k)(S_{-1}^i)$ consists of the $\le$-maximal element for each $k \in \omega$. Let $f_{-1} : S_{-1}^1 \to S_{-1}^2$ be the canonical isomorphism. Suppose that we have constructed f_i. Without loss of generality, we may assume that i is odd. Suppose S_i^1 is generated by a finite presystem X_i of S_1.

If $\alpha_{i+1} \in S_i^1$, put $S_{i+1}^1 := S_i^1$ and put $f_{i+1} := f_i$. If $\alpha_{i+1} \notin S_i^1$, let S_{i+1}^1 be the subsystem generated by the finite subset $X_i \cup [\alpha_{i+1}] \cap m(k)$ where $\alpha_{i+1} \in m(k)$. Since $\mathrm{coIM}(S_1) = \mathrm{coIM}(S_2)$, there is a subsystem $\bar{S}_{i+1}^2$ of S_2 isomorphic to S_{i+1}^1. Let $\bar{\Psi} : S_{i+1}^1 \to \bar{S}_{i+1}^2$ be an isomorphism. Note that $\bar{S}_{i+1}^2$ is also finitely generated because S_{i+1}^1 is finitely generated. Since S_2 has co-EP, there is an embedding $\Psi : \bar{S}_{i+1}^2 \to S_2$ to make the following diagram commute:

$$\begin{array}{ccccc} S_i^2 & \xrightarrow{f_i^{-1}} & S_{i+1}^1 & \xrightarrow{\bar{\Psi}} & \bar{S}_{i+1}^2 \\ \Big\downarrow \mathrm{id} & & & & \Big\downarrow \Psi \\ S_i^2 & & \xrightarrow[\iota]{\qquad\qquad} & & S(G_2) \end{array}$$

Put $S_{i+1}^2 := (\Psi \circ \bar{\Psi})[S_{i+1}^1]$ and put $f_{i+1} = \Psi \circ \bar{\Psi}$. Note that f_{i+1} extends f_i because of the following diagram:

$$\begin{array}{ccc} S_i^2 & \xrightarrow{f_i^{-1}} & S_{i+1}^1 \\ \Big\downarrow \mathrm{id} & & \Big\downarrow f_{i+1} \\ S_i^2 & \xrightarrow[\iota]{} & S_{i+1}^2 \end{array}$$

□

Remark 2.24. Note that for a complete system S and for any finitely generated complete system S', there are $k \in \omega$ and a positive integer N such that

$$S' \in \mathrm{coIM}(S) \Leftrightarrow (\exists X \subset m(k))(|X| \le N \wedge S_X \cong S').$$

Combining Fact 2.23 and Remark 2.24, we have the following results.

Fact 2.25. [1, Theorem 2.3, Theorem 2.4] *Suppose that S has co-EP.*

(1) $Th(S)$ is axiomatized by CS_{EP} together with the following axioms: For every $S_1 \in \mathrm{coIM}(S)$ and $S_2 \notin \mathrm{coIM}(S)$,

- *there is a finite presystem X of S such that $S_X \cong S_1$,*

- *for any finite presystem Y of S, $S_Y \not\cong S_2$.*

(2) Th(S) *is ω-stable.*

3. The universal embedding cover: Existence and Uniqueness

In [9, Theorem 2.12], Haran and Lubotzky first proved the existence and uniqueness of a universal embedding cover for the finitely generated case. And in [7, Proposition 24.4.5, Corollary 24.4.8], Fried and Jarden showed the existence of a universal embedding cover for the general case, and the uniqueness for the countable rank case. Chatzidakis in [1, Theorem 2.7] proved the existence and uniqueness of the universal embedding cover for arbitrary profinite groups using the existence and uniqueness of prime models for countable ω-stable theories. In this section, we will prove the existence of the embedding cover for arbitrary profinite groups using the fact that the category of profinite groups is closed under taking the inverse limit and the fibre product.

3.1. **Existence.** Motivated from the proof of [9, Theorem 1.12], we first prove that the inverse limit of q.e.c. is again a q.e.c.

Lemma 3.1. *For an ordinal α, consider an inverse system $(G_i, \pi_{i,j})_{j\le i<\alpha}$ indexed by ordinals $i < \alpha$ such that*

- *for each $j < i$, the transition map $\pi_{i,j}$ is a q.e.c.,*
- *for each limit ordinal β, G_β is the inverse limit of the inverse system $(G_i)_{i<\beta}$ with transition maps $\pi_{i,j}$,*
- *for each limit ordinal β and for $i < \beta$, the transition map $\pi_{\beta,i}$ is the natural projection from G_β to G_i coming from the inverse limit construction.*

Let G be the inverse limit of $(G_i)_{i<\alpha}$ and let $\pi_i : G \to G_i$ be the canonical projection for each $i < \alpha$. Then, π_0 is a q.e.c.

Proof. If α is a successor ordinal, that is, $\alpha = \alpha' + 1$, then $G = G_{\alpha'}$ and we are done. We assume that α is a limit ordinal. Let $p : G' \to G_0$ be an embedding cover. To show that π is a q.e.c., using transfinite induction, we will construct a sequence $(p_i : G' \to G_i)_{i<\alpha}$ of epimorphisms such that for each $i_0 \le j < i < \alpha$, $p_j = \pi_{i,j} \circ p_i$. Put $p_0 := p$. Suppose we have constructed $(p_i)_{i<\gamma}$ for some $\gamma < \alpha$. If γ is a limit ordinal, there is a desired morphism $p_\gamma : G' \to G_\gamma$ because G_γ is the inverse limit of $(G_i)_{i<\gamma}$. If $\gamma = \gamma' + 1$ is a successor ordinal, there is a epimorphism $r : G' \to G_\gamma$ such that $p_{\gamma'} = \pi_{\gamma,\gamma'} \circ r$ because $\pi_{\gamma,\gamma'}$ is a q.e.c. Put $p_\gamma := r$, which is a desired one.

Since G is the inverse limit of $(G_i)_{i<\beta}$, there is $q : G' \to G$ such that for each $i < \alpha$, $p_i = \pi_i \circ q$. Thus, we have that $p = \pi_0 \circ q$, and π_0 is a q.e.c. □

Theorem 3.2. *Let G be a profinite group. Then, there is a universal embedding cover $p : H \to G$. Furthermore, if G is finitely generated, then p is the unique universal embedding cover (up to isomorphism).*

Proof. If G has EP, then $\mathrm{id} : G \to G$ is a universal embedding cover. Suppose G has no EP. Let κ_0 be the rank of G and let κ_1 be the cardinality of $\mathbb{F}_{\kappa_0}$. Let $\aleph$ be a cardinal with $(\lambda :=) 2^{\kappa_1} < \aleph$.

Using transfinite induction, we will construct an inverse system $(G_i, \pi_{i,j})_{j<i\le\alpha}$ for some ordinal $\alpha < \aleph$ such that

- for each $j < i$, the transition map $\pi_{i,j}$ is a q.e.c. with the non-trivial kernel,
- for each limit ordinal β, G_β is the inverse limit of the inverse system $(G_i, \pi_{i,j})_{j<i<\beta}$,
- for each limit ordinal β and for $i < \beta$, the transition map $\pi_{\beta,i}$ is the natural projection from G_β to G_i coming from the inverse limit construction,
- G_α has EP.

Put $G_0 := G$. Suppose we have constructed such an inverse system $(G_i)_{i<\beta}$ for an ordinal β.

Case. β is a successor ordinal, that is, $\beta = \beta' + 1$. If G_β has EP, then we stop the process. Suppose $G_{\beta'}$ has no EP. By Lemma 2.13, there is a q.e.c. $p : (G', F') \to (G_{\beta'}, F_{\beta'})$ with a non-trivial kernel. Put $G_\beta := G'$ and $\pi_{\beta,\beta'} := p$. For each $i < \beta$, put $\pi_{\beta,i} := \pi_{\beta',i} \circ p$. By Remark 2.11(1), each $\pi_{\beta,i}$ is a q.e.c.

Case. β is a limit ordinal. Let G_β be the inverse limit of $(G_i)_{i<\beta}$. For each $i < \beta$, let $\pi_{\beta,i}$ be the natural projection map from G_β to G_i. By Lemma 3.1, each $\pi_{\beta,i}$ is a q.e.c.

For each $j < i$, $\pi_{i,j}$ has a non-trivial kernel. Namely, suppose there exist $j < i$ such that $\mathrm{Ker}(\pi_{i,j})$ is trivial. Since $\pi_{i,j} = \pi_{j+1,j} \circ \pi_{i,j+1}$, where $\pi_{k,k} = \mathrm{id}$ for each k, $\mathrm{Ker}(\pi_{j+1,j})$ is also trivial, which is a contradiction. In our construction, α should be less than $\aleph$. Suppose not, that is, $\alpha \ge \aleph$. By Remark 2.11(2), we have that $|G_\alpha| \le \kappa_1$. So, $|\mathcal{N}(G_\alpha)| \le 2^{\kappa_1} = \lambda$. Since $|\alpha| \ge \aleph > \lambda$, by the pigeon hole principle, for some $j < i < \alpha$, $\mathrm{Ker}(\pi_{\alpha,j}) = \mathrm{Ker}(\pi_{\alpha,i})$. Since $\pi_{\alpha,j} = \pi_{i,j} \circ \pi_{\alpha,i}$, we have that $\pi_{i,j}$ is injective, which is a contradiction. Therefore, we have a q.e.c. $\pi_{\alpha,0} : G_\alpha \to G$ such that any q.e.c. to G_α is injective. Therefore, by Lemma 2.13, G_α has EP.

We now prove the furthermore part. Suppose G is finitely generated. Let $p_i : G_i \to G$ be a universal embedding cover of G for $i = 1, 2$. By [9, Theorem 1.12], G_1 and G_2 are finitely generated. By universality, there are morphisms $q : G_2 \to G_1$ and $q' : G_1 \to G_2$ such that $p_2 = p_1 \circ q$ and $p_1 = p_2 \circ q'$. Since G_1 and G_2 are finitely generated, by [13, Proposition 7.6], both q and q' are bijective. □

3.2. **Uniqueness.** Following the proof scheme of [1, Theorem 2.7], we will prove the uniqueness of a universal embedding cover for arbitrary profinite groups.

Theorem 3.3. *Any profinite group H has a universal EP-cover G which is unique up to isomorphism over H.*

Proof. We first identify the theory of $S(G)$. By Theorem 3.2, any $A \in \mathrm{IM}(H)$ has the unique universal EP-cover. Let Γ be the set of isomorphism classes of finite groups which is an image of the universal EP-cover of A for some $A \in \mathrm{IM}(H)$. Let T be the theory given by

$$\begin{aligned} T = \mathrm{CS}_{EP} &\cup Diag(S(H)) \\ &\cup \{\exists X(S_X \cong S(A)) : A \in \Gamma\} \\ &\cup \{\forall X(S_X \not\cong S(B) : B \notin \Gamma\}, \end{aligned}$$

which can be written as $\mathcal{L}_{\mathrm{CS}}(S(H))$-sentences by Remark 2.24.

Claim 3.4. *The theory T is consistent and complete.*

Proof. Let Y be a finite subset of $Diag(S(H))$, and let $A_1, \ldots, A_n \in \Gamma$ and $B_1, \ldots, B_m \notin \Gamma$. By Remark 2.24, there are finite subsets $X_1, \ldots, X_n$ of $S(H)$ such that A_i is an image of the universal EP-cover of $G(S_{X_i})$ for each i. Let $S' := S_{(\bigcup_{i\le n} X_i)\cup Y}$ be a subsystem of $S(H)$. Then, $G(S')$ is in $\mathrm{IM}(H)$, and for the universal EP-cover E of $G(S')$, $A_1, \ldots, A_n \in \mathrm{IM}(E)(\subset \Gamma)$ and $B_1, \ldots, B_m \notin \mathrm{IM}(E)$. Thus, T is finitely consistent and so it is consistent. Also, it is complete by Lemma 2.23. □

Since T is ω-stable, there is a prime model S of T over $S(H)$ which is unique up to isomorphism. Let $G := G(S)$ and let $\pi : G \to H$ be the epimorphism dual to the inclusion $\iota : S(H) \to S$.

Claim 3.5. *The epimorphism $\pi : G \to H$ is a universal EP-cover of H.*

Proof. Let $\pi' : G' \to H$ be a universal EP-cover, which exists by Theorem 3.2. Since π is a EP-cover, we have that $\Gamma \subset \mathrm{IM}(G') \subset \mathrm{IM}(G) = \Gamma$ so that $\mathrm{IM}(G') = \Gamma$. Therefore, $S(G')$ is a model of T.

Let $q : M \to H$ be a EP-cover so that $S(M) \models \mathrm{CS}_{EP}$. Since π' is a universal EP-cover, there is $p : M \to G'$ such that $q = \pi' \circ p$. Put $S' = \mathrm{Im}(S(p)) \subset S(M)$, which is a model of T. Since S is a prime model of T, there is an embedding $\Phi : S \to S'$ such that $\Phi(x) = S(q)(x)$ for each $x \in S(H)$. Consider an embedding $\iota \circ \Phi : S \to S' \to S(M)$ where $\iota : S' \to S(M)$ is the inclusion. Then, the dual map $\varphi := G(\iota \circ \Phi) : M \to G$ gives a morphism such that $q = \pi \circ \varphi$. Therefore, $\pi : G \to H$ is a universal EP-cover. □

Therefore, we conclude that the dual group of any prime model of T over $S(H)$ gives a universal EP-cover. Also, the proof of Claim 3.5 shows that the complete system of a universal EP-cover of H is a prime model of T over $S(H)$. By the uniqueness of prime model of T over $S(H)$, every universal EP-covers of H are isomorphic. □

References

[1] Z. Chatzidakis. Model theory of profinite groups having the Iwasawa property. *Illinois J. Math.*, **42** (1998), 70-96.

[2] Z. Chatzidakis. Amalgamation of types in pseudo-algebraically closed fields and applications. *J. Math. Log.*, **19** (2019), 1950006 (28 pages)
[3] G. Cherlin, L. van den Dries, and A. Macintyre. The elementary theory of regularly closed fields. preprint, (1980).
[4] G. Cherlin, L. van den Dries, and A. Macintyre. Decidability and undecidability theorems for PAC-feilds. *Bull. Amer. Math. Soc.*, **4** (1981), 101–104.
[5] Y. Ershov and M. Fried. Frattini covers and projective groups without the extension property. *Math. Ann*, **253** (1980), 233-239.
[6] M. Fried, D. Haran, and M. Jarden. Galois Stratification over Frobenius Fields. *Adv. Math.*, **51** (1984), 1-34.
[7] M. Fried and M. Jarden. Field Arithmetic, 3rd edition. A series of Modern Surveys in Mathematics, Springer, 2008.
[8] J. Lee. The embedding property for sorted profinite groups. arXiv:2012.14149, 2020.
[9] D. Haran and A. Lubotzky. Embedding covers and the theory of Frobenius fields. *Israel J. Math.*, **41** (1982), 181-202.
[10] D. M. Hoffmann and J. Lee. Co-theory of sorted profinite groups for PAC structures. arXiv:1905.09748, 2019.
[11] K. Iwasaw. On solvable extensions of algebraic number fields. *Ann. of Math.*, **58** (1953), 548-572.
[12] N. Ramsey. Independence, amalgamation, and trees. Ph. D. thesis, University of California, Berkeley (2018).
[13] P. Ribes. Introduction of profinite groups and Galois cohomology. Queen Papers in Pure and Applied Mathematics **24**, Queen's University, Kingston, Ontario, 1970.

KAIST, Department of Mathematical Sciences, 291 Daehak-ro Yuseong-gu, 34141, Daejeon, South Korea
Email address: `ljwhayo@kaist.ac.kr`