# Extending partial permtations

draft, pjc, January 2004

**Abstract**

This document describes a simple problem about extending partial permutations which may be recursively unsolvable, and discusses the context.

## 1 Introduction

A *partial permutation* on a set $X$ is a bijection between two subsets of $X$. The domain and range of a partial permutation $p$ will be denoted by $\mathrm{dom}(p)$ and $\mathrm{ran}(p)$ respectively.

A partial permutation $q$ *extends* $p$ if $\mathrm{dom}(p) \subseteq \mathrm{dom}(q)$ and $q(x) = p(x)$ for all $x \in \mathrm{dom}(p)$. It is clear that any partial permutation can be extended to a permutation.

We define the *composition* $p \circ q$ of two partial permutations $p, q$ on $X$ to be the partial permutation $r$ given by

$$r(x) = p(q(x)) \text{ for } x \in p^{-1}(\mathrm{ran}(p) \cap \mathrm{dom}(q).$$

Consider the following decision problem.

*Let $p_1, \ldots, p_m$ be partial permutations of a finite set A. Suppose that*

*(i) $p_1$ is the identity map on A, and*

*(ii) for any $i, j$, there is at most one $k$ such that $p_k$ extends $p_i \circ p_j$.*

*Does there exist a finite set B containing A, and permutations $f_i$ of B extending $p_i$ for $i = 1, \ldots, m$, such that*

*(a) $f_1$ is the identity map on B, and*

*(b) if $p_k$ extends $p_i \circ p_j$, then $f_i \circ f_j = f_k$?*

What is the computational complexity of this problem? How is this affected if we insist that $B = A$?

In the case when $A = B$, it is clear that the problem lies in NP, since given the required set of permutations we can easily check that conditions (a) and (b) hold. So one might ask whether it is NP-complete.

However, if we do not require that $A = B$, then there is no obvious reason why the problem should have an algorithmic solution at all. On the other hand, it seems possible on the face of it that the answer is always "yes", so that the algorithmic solution is trivial.

I conjecture that in fact the problem is recursively undecidable. In this note, I will first give an example to show that the answer is not always "yes", and to show that the problem is connected with issues in combinatorial group theory. I then discuss a recent preprint by Gordon and Vershik [1] on the LEF-property of groups, which appears to be related. Further information about combinatorial group theory, and in particular the unsolvability of various group-theoretic decision problems, can be found in the standard book by Lyndon and Schupp [2].

# 2 An example

The following example involves 13 partial permutations on a set of size 145 which cannot be extended as specified in the problem. I do not know whether it is the smallest possible in any sense. It depends on the following construction due to Graham Higman.

**Proposition 1** *Let*

$$G = \langle a, b, c, d : bab^{-1} = a^2, cbc^{-1} = b^2, dcd^{-1} = c^2, ada^{-1} = a^2 \rangle.$$

*Then G is an infinite group which has no non-trivial finite homomorphic images.*

**Proof** First we show that $G$ is infinite. This uses some of the basic tools of combinatorial group theory, namely free product with amalgamation and HNN-extension. In brief:

- Let $A, B, C$ be groups and $\theta : C \to A$ and $\phi : C \to B$ be embeddings. Then the group
$$A *_C B = \langle A, B : (\forall c \in C)(\theta(c) = \phi(c)) \rangle$$

has "no collapse"; in particular, $A$ and $B$ are subgroups whose intersection is precisely $C$; moreover, an element of $A \setminus C$ and an element of $B \setminus C$ generate their free product.

- Let $A$ be a group, $B, C$ subgroups of $A$, and $\theta : B \to C$ an isomorphism. Then the HNN-extension

$$\langle A, t : (\forall b \in B)(tbt^{-1} = \theta(b)) \rangle$$

has "no collapse"; in particular, $A$ is a subgroup and $t$ is an element of infinite order.

Now $\langle a, b : bab^{-1} = a^2 \rangle$ is an HNN-extension; so it is infinite, and both $a$ and $b$ have infinite order.

Then $\langle a, b, c : bab^{-1} = a^2, cbc^{-1} = b^2$ is the free product of two copies of the preceding group (generated by $a, b$ and $b, c$ respectively) amalgamating the infinite cyclic subgroup generated by $b$; so it is infinite, and both $a$ and $c$ have infinite order.

Finally, $G$ is the free product of two copies of the preceding group (generated by $a, b, c$ and $c, d, a$ respectively) amalgamating the subgroup generated by $a$ and $c$ (which is a free group of rank 2). So $G$ is infinite.

Now suppose that $H$ is a finite homomorphic image of $G$. Thus, $H$ contains elements $a, b, c, d$ which satisfy the defining relations of $G$. Since each of these elements is conjugate to its square, we see that each of them has odd order. If $a = 1$ then $d = d^2$, so $d = 1$, and similarly $c = b = 1$, so that $H = 1$; so we may assume that none of $a, b, c, d$ is the identity. Let $p_a, p_b, p_c, p_d$ be the smallest prime divisors of the orders of $a$, $b$, $c$, $d$ respectively.

Now some power of $a$ has order $p_a$, and is conjugated to its square by $b$. Thus, the order of $b$ is divisible by a prime divisor of $p_a - 1$, and in particular, we have $p_b < p_a$. Continuing, we obtain

$$p_a > p_b > p_c > p_d > p_a,$$

a contradiction.

Now we are ready for the construction. Let $G$ be the above group. Let

$$X = \{1, a, a^2, b, b^2, c, c^2, d, d^2, ba, cb, dc, ad\},$$

and let $A$ be the set of all products of at most two elements of $X$. Clearly $A$ is finite. I have not calculated exactly how many elements are in $A$, but clearly it is at most 145.

For $x \in X$, let $p_x$ be the partial permutation of $A$ given by right multiplication by $x$. That is, $p_x(a) = ax$ whenever $a, ax \in A$. We verify that conditions (i) and (ii) hold. Condition (i) is obvious. Suppose that $p_x \circ p_y$ is contained in two different elements $p_u$ and $p_v$. By construction, $p_x \circ p_y(1)$ is defined, and is equal to $xy$. Thus $u = p_u(1) = xy = p_v(1) = v$, contrary to assumption.

Now suppose that there is a finite set $B$ containing $A$ and permutations $f_x$ of $B$ extending $p_x$ for $x \in X$. We have $f_1 = 1$. Let $f_a = \alpha$, $f_b = \beta$, $f_c = \gamma$ and $f_d = \delta$. We have $f_{a^2} = \alpha^2$, $f_{ba} = \beta\alpha$, and similar equations for the other elements. Now

$$\beta\alpha = f_{ba} = f_{a^2b} = \alpha^2\beta,$$

and three similar equations. So the elements $\alpha, \ldots, \delta$ satisfy the relations of $G$, and the group they generate is a non-trivial homomorphic image of $G$, which is clearly finite since it is contained in the symmetric group on the set $B$. This is a contradiction; so no such extension can exist.

This shows that the decidability of our original problem is closely related to the decidability of various questions about whether certain groups have finite homomorphic images. However, I have not been able to establish that the problem is undecidable.

# 3 LEF-groups

Gordon and Vershik [1] say that a group $G$ is *locally embeddable in the class of finite groups*, or for short an *LEF-group*, if the following holds:

> Given a finite subset $A$ of $G$, there exists a finite group $H$ (with group operation denoted by $*$) containing $A$ such that, for all $a, b \in A$, if $ab \in A$ then $ab = a * b$.

Here $ab$ denotes the product of $a$ and $b$ calculated in $G$; if this product is not in $A$ then we make no assumption about the relationship between $ab$ and $a * b$.

This is a local property, in the sense that a group $G$ has the property if and only if all its finitely generated subgroups do. Among other things, Gordon and Vershik show the following:

(a) A locally residually finite group is an LEF-group.

(b) A finitely presented LEF-group is residually finite.

(c) There exist LEF-groups which are not locally residually finite.

Now it is clear that this is closely connected with the construction in the last section. Given any finite presentation of a group $G$, we can follow the construction by taking $X$ to consist of all initial subwords of the relators and $A$ to consist of all products of at most two elements of $X$, so that the relations can be deduced from all expressions of the form $ab = c$ for $a, b \in A$. Then if $G$ is an LEF-group, the finite set $A$ can be embedded in a finite group, and the partial permutations extended to elements of the group, so that the answer to the decision problem is "yes". I have not tried to write down all the details of this.

# References


[1] E. I. Gordon and A. M. Vershik, Groups that are locally embeddable in the class of finite groups (Russian), *Algebra i Analiz* **9** (1997), 71–97; translation in *St. Petersburg Math. J.* **9** (1998), 49–67.

[2] Roger C. Lyndon and Paul E. Schupp, *Combinatorial group theory*, Reprint of the 1977 edition, Classics in Mathematics, Springer-Verlag, Berlin, 2001.