creative commons

ARS MATHEMATICA CONTEMPORANEA

ISSN 1855-3966 (printed edn.), ISSN 1855-3974 (electronic edn.)
ARS MATHEMATICA CONTEMPORANEA 17 (2019) 535–554
https://doi.org/10.26493/1855-3974.1884.5cb
(Also available at http://amc-journal.eu)

The finite embeddability property for IP loops and local embeddability of groups into finite IP loops

Martin Vodička
Max-Planck-Institut für Mathematik in den Naturwissenschaften, Inselstrasse 22, 04103 Leipzig, Germany

Pavol Zlatoš *
Faculty of Mathematics, Physics and Informatics, Comenius University, Mlynská dolina, 842 48 Bratislava, Slovakia

Received 19 December 2018, accepted 11 September 2019, published online 29 November 2019

Abstract

We prove that the class of all loops with the inverse property (IP loops) has the Finite Embeddability Property (FEP). As a consequence, every group is locally embeddable into finite IP loops. The first one of these results is obtained as a consequence of a more general embeddability theorem, contributing to a list of problems posed by T. Evans in 1978, namely, that every finite partial IP loop can be embedded into a finite IP loop.

Keywords: Group, IP loop, finite embeddability property, local embeddability.

Math. Subj. Class.: 20E25, 20N05, 05B07, 05B15, 05C25, 05C45

The *Finite Embeddability Property* (briefly FEP), was introduced by Henkin [17] for general algebraic systems already in 1956. For groupoids (i.e., algebraic structures $(G, \cdot)$ with a single binary operation), which is sufficient for our purpose, it reads as follows: A class $\mathbf{K}$ of groupoids has the FEP if for every algebra $(G, \cdot) \in \mathbf{K}$ and each nonempty finite subset $X \subseteq G$ there is a *finite* algebra $(H, *) \in \mathbf{K}$ extending $(X, \cdot)$, i.e., $X \subseteq H$ and $x \cdot y = x * y$ for all $x, y \in X$, such that $x \cdot y \in X$. Using this notion an earlier result of Henkin [16] can be stated as follows: The class of all abelian groups has the FEP (see also Grätzer [14]).

A more general notion of local embeddability can be traced back to even earlier papers by Mal'tsev [21, 22] (see also the posthumous monograph [23]). It was explicitly

*The second author acknowledges with thanks the support by the grant no. 1/0333/17 of the Slovak grant agency VEGA.

E-mail addresses: vodicka@mis.mpg.de (Martin Vodička), zlatos@fmph.uniba.sk (Pavol Zlatoš)

This work is licensed under https://creativecommons.org/licenses/by/4.0/

(re)introduced and studied in detail mainly for groups by Gordon and Vershik [28]: A groupoid $(G, \cdot)$ is *locally embeddable into a class of groupoids* $\mathbf{M}$ if for every nonempty finite set $X \subseteq G$ there is $(H, *) \in \mathbf{M}$ such that $X \subseteq H$ and $x \cdot y = x * y$ for all $x, y \in X$ satisfying $x \cdot y \in X$. Informally this means that every finite cut-out from the multiplication table of $(G, \cdot)$ can be embedded into an algebra from $\mathbf{M}$. A standard model-theoretic argument shows that this condition is equivalent to the embeddability of $(G, \cdot)$ into an *ultraproduct* of algebras from $\mathbf{M}$ (for the ultraproduct construction see, e.g., Chang, Keisler [3]).

Thus a class $\mathbf{K}$ has the FEP if and only if every $(G, \cdot) \in \mathbf{K}$ is locally embeddable into the class $\mathbf{K}_{\mathrm{fin}}$ of all finite members in $\mathbf{K}$. As proved by Evans [9], for a variety (equational class) $\mathbf{K}$ this is equivalent to the condition that every finitely presented algebra in $\mathbf{K}$ is residually finite, i.e., embeddable into a direct product of finite algebras from $\mathbf{K}$. The groups locally embeddable into (the class of all) finite groups were called *LEF groups* in [28]. The authors also noticed that, unlike the abelian ones, not all groups are LEF, in other words, the class of all groups doesn't have the FEP. As examples of finitely presented groups which are not residaully finite, hence not locally embeddable into finite groups, can serve the Baumslag-Solitar groups $BS(m, n) = \langle a, b \mid a^{-1}b^m a = b^n \rangle$ for $|m|, |n| > 1$, $|m| \neq |n|$ (see Meskin [24]). A complete list of minimal partial Latin squares embeddable into a closely related infinite group but not embeddable into any finite group, even under a weaker concept of embedding, was recently described by Dietrich and Wanless [6].

This immediately raises the question of finding some classes of finite grupoids into which all the groups were locally embeddable and which, at the same time, would be "as close to groups as possible". The question is of interest for various reasons: The class of all LEF groups properly extends the class of all locally residually finite groups and plays an important role in dynamical systems, cellular automata, etc. (see, e.g., Ceccherini-Silberstein, Coornaert [2], Gordon, Vershik [28]).

Glebsky and Gordon [13] have shown that a group is locally embeddable into finite semigroups if and only if it is an LEF group. It follows that looking for a class of finite groupoids into which one could locally embed all the groups one has to sacrifice the associativity condition. They also noticed that the results about extendability of partial Latin squares to (complete) Latin squares imply that every group is locally embeddable into finite quasigroups. Refining slightly the original argument they have shown that every group can even be locally embedded into finite loops (see also their survey article [12]).

A further decisive step in this direction was done by Ziman [30]. Building upon the methods of extension of partial Latin squares preserving some symmetry conditions (see Cruse [4] and Lindner [20]), he has shown that the class of all loops with *antiautomorphic inverses*, i.e., loops with two-sided inverses satisfying the identity $(xy)^{-1} = y^{-1}x^{-1}$ (briefly *AAIP loops*), has the FEP (though he didn't use this notion explicitly). As a consequence, every group is locally embeddable into finite AAIP loops.

Quasigroups and loops experts consider the class of all AAIP loops still as a "rather far going extension" of the class of all groups. On the other hand, they find the class of all loops with the *inverse property*, i.e., loops with two-sided inverses satisfying the identities $x^{-1}(xy) = y = (yx)x^{-1}$ (briefly IP loops), which is a proper subclass of the class of all AAIP loops, a much more moderate extension of the class of all groups (Drápal [8]). In the present paper we are going to show that Ziman's result can indeed be strengthened in this sense. Using mainly graph-theoretical methods and Steiner triple systems, we will prove that the class of all IP loops still has the FEP. As a consequence, every group is locally

embeddable into finite IP loops.

When the original version of this paper was already submitted, A. Drápal turned our attention towards the point that the problem we are solving was implicitly formulated in Evans' paper [10] in the last line of the table on page 798. At the same time he remarked that we have proved even more, namely that every finite partial IP loop can be embedded into a finite IP loop. Later on, the same point was made by the anonymous referee. We will discuss these issues in the next section, after introducing the respective notions and formulating our results more precisely.

For basic definitions and facts about quasigroups and loops the reader is referred to the monographs Belousov and Belyavskaya [1] and Pflugfelder [26].

1 Formulation of the main results, discussion and plan of the proof

In order to guarantee that the class of all IP loops forms a variety, we define an *IP loop* as an algebra $\left(L, \cdot, 1, {}^{-1}\right)$ with a binary operation of multiplication $\cdot$, a distinguished element 1 denoting the unit, and a unary operation ${}^{-1}$ of taking inverses, satisfying the identities

$$1x = x = x1, \qquad \text{and} \qquad x^{-1}(xy) = y = (yx)x^{-1}.$$

Then the identities $x^{-1}x = 1 = xx^{-1}$ and $\left(x^{-1}\right)^{-1} = x$ easily follow. Also it is clear that, for any $a, b \in L$, the equations $ax = b$, $ya = b$ have unique solutions $x = a^{-1}b$, $y = ba^{-1}$ in L. Since the unit element 1 and the inverse map $x \mapsto x^{-1}$ in every IP loop are uniquely determined by the multiplication $\cdot$, referring to an IP loop $\left(L, \cdot, 1, {}^{-1}\right)$ as just $(L, \cdot)$ is unambiguous. However, usually it will be denoted simply by L.

A *partial IP loop* $(P, \cdot)$ is a set P endowed with a partial binary operation $\cdot$ defined on a subset $D(P, \cdot) \subseteq P \times P$, called the *domain* of the operation $\cdot$, satisfying the following three conditions:

(1) there is an element $1 \in P$, called the *unit* of P, such that $(1, x), (x, 1) \in D(P, \cdot)$ and $1x = x1 = x$ for all $x \in P$;

(2) for each $x \in P$ there is a unique $y \in P$, called the *inverse* of x and denoted by $y = x^{-1}$, such that $(x, y), (y, x) \in D(P, \cdot)$ and $xy = yx = 1$;

(3) for any $x, y \in P$ such that $(x, y) \in D(P, \cdot)$, we have $\left(x^{-1}, xy\right), \left(xy, y^{-1}\right) \in D(P, \cdot)$ and $x^{-1}(xy) = y$, $(xy)y^{-1} = x$.

In most cases we will denote a partial IP loop $(P, \cdot)$ as P and its domain as $D(P)$, only; the more unambiguous notation $(P, \cdot)$ and $D(P, \cdot)$ will be used mainly in case we need to distinguish the operations on two or more (partial) IP loops.

A partial IP loop $(Q, *)$ is called an *extension* of a partial IP loop $(P, \cdot)$ if $P \subseteq Q$, $D(P, \cdot) \subseteq D(Q, *)$ and $x \cdot y = x * y$ for each pair $(x, y) \in D(P)$. Suppressing the names of the operations, we write $P \leq Q$ or $Q \geq P$. Alternatively we say that the partial IP loop P is *embedded* in the partial IP loop Q. Obviously, the relation $\leq$ between partial IP loops is reflexive, antisymmetric and transitive.

Our main results are the following three theorems.

Theorem 1.1. *Every finite partial IP loop P can be embedded into some finite IP loop L.*

Given an IP loop L and a finite set $X \subseteq L$, we can form the finite partial IP loop

$$P = X \cup \{1\} \cup X^{-1},$$

where $X^{-1} = \{x^{-1} : x \in X\}$, by restricting the original loop operation on L to the set

$$D(P) = \{(x, y) \in P \times P : xy \in P\}.$$

Then, obviously, $P \leq L$. Thus Theorem 1.1 readily implies our next, already announced result.

Theorem 1.2. *The class of all IP loops has the Finite Embeddability Property. Equivalently, every finitely presented IP loop is residually finite.*

As a special case of Theorem 1.2 we obtain

Theorem 1.3. *Every group can be locally embedded into the class of all finite IP loops. Equivalently, every group can be embedded into some ultraproduct of finite IP loops.*

The second, equivalent formulation of Theorem 1.2 answers in affirmative the question posed by Evans [10] in the IP loop row and R. F. column of the table on page 798.

In order to discuss the relation of our results to Evans' table we recall the following three abbreviations used in [10]. Unlike the author, who used them for various classes of algebras, we apply them just to the class of all IP loops.

E_1: Every finite partial IP loop can be embedded into some finite IP loop.

E_2: Every finite partial IP loop can be embedded into some (finite or infinite) IP loop.

E_3: Every finite partial IP loop which can be embedded into some IP loop, can be embedded into some finite IP loop.

Obviously, condition E_3 is equivalent to the FEP for IP loops, and condition E_1 is equivalent to the conjunction $E_2 \wedge E_3$, depicted (among other relations) in the chart on the top of page 798 in [10] (the equivalence $E_1 \wedge E_2 \Leftrightarrow E_3$ on page 797 is clearly a typo).

Theorem 1.1 seems to contradict the sign "X" (meaning "No") in the IP loop row and E_1 column of the table in the middle of page 798 in [10]. Evans, however, considered a seemingly weaker notion of a partial IP loop (hence a stronger concept of embeddability) there. Paraphrasing and slightly adapting his definition to apply to our situation, we obtain a rather vague formulation: "A partial IP loop is a set P in which the operations of multiplication and taking inverses are defined on some subsets $D(P) \subseteq P \times P$ and $D'(P) \subseteq P$, respectively, which satisfies the defining IP loop identities, insofar as they can be applied to the partial operations on P" (cf. [10, §3, page 796]). In particular it is not clear (though not crucial) whether P has to contain the unit element 1 or not. Thus, at least at a glance, it seems possible that there could exist some finite partial IP loop in his sense, which is not embeddable into any finite IP loop. However, the responses "X" (i.e. "No") to E_1 and "$\surd$" (meaning "Yes") to E_2 in Evans' table, together with our Theorem 1.2 responding E_3 affirmatively, still contradict the equivalence $E_1 \Leftrightarrow E_2 \wedge E_3$, regardless of the details of the definition of a partial IP loop. Unfortunately, Evans provided neither any counterexample to E_1 nor any proof or reference in favor of E_2 in [10].

A possible clue to resolving this problem lies in the PhD thesis [27] by Evans' student C. Treash from 1969. Her definition of the concept of an *incomplete IP loop* on page 27 is namely equivalent to that of our partial IP loop (cf. our Lemma 2.1). According to her Theorem 1, stated and proved on page 28: *Every (finite or infinite) incomplete IP loop can be embedded into some IP loop*, which implies E_2 as a special case. Thus Evans' negative response to E_1 seems to be indeed a shortcoming or just another typo.

After this digression we are returning to the main theme of our paper.

From the course of our arguments it is clear that it suffices to prove just Theorem 1.1. We divide its proof into three steps consisting of the three propositions below. Their formulation requires some additional notions and notation.

In the absence of associativity there is no obvious way how to define the order of an element. Nonetheless, the sets of elements of order 2 and 3, respectively, can still be defined for any partial IP loop P:

$$O_2(P) = \{x \in P : x \neq 1,\ (x,x) \in D(P) \text{ and } xx = 1\},$$
$$O_3(P) = \{x \in P : x \neq 1,\ (x,x),(x,xx),(xx,x) \in D(P) \text{ and } x(xx) = (xx)x = 1\}.$$

In other words, for $x \neq 1$ in P we have $x \in O_2(P)$ if and only if $x^{-1} = x$, and $x \in O_3(P)$ if and only if $(x,x) \in D(P)$ and $x^{-1} = xx$. The number of elements of the sets $O_2(P)$, $O_3(P)$ in a finite partial IP loop P will be denoted by $o_2(P)$, $o_3(P)$, respectively. The number of elements of any finite set A is denoted by $\#A$.

Proposition 1.4. *Let $(P,\cdot)$ be a finite partial IP loop. Then there exists a finite partial IP loop $(Q,*)$ such that $P \leq Q$ and $3 \mid o_3(Q)$.*

A pair (x,y) in a partial IP loop P will be called a *gap* if $(x,y) \notin D(P)$. The set of all gaps in P will be denoted by

$$\Gamma(P,\cdot) = (P \times P) \setminus D(P,\cdot) = \{(x,y) \in P \times P : (x,y) \notin D(P,\cdot)\},$$

or just briefly by $\Gamma(P)$. Obviously, both $D(P)$, $\Gamma(P)$ are binary relation on the set P, and a partial IP loop P is an IP loop if and only if it contains no gaps, i.e., $\Gamma(P) = \emptyset$.

Proposition 1.5. *Let P be a finite partial IP loop such that $3 \mid o_3(P)$. Then there exists a finite partial IP loop $Q \geq P$ satisfying the following four conditions:*

(4) $3 \mid o_3(Q)$, $\#Q \geq 10$, $\#Q \equiv 4 \pmod 6$ *and* $\Gamma(Q) \subseteq O_2(Q) \times O_2(Q)$.

Proposition 1.6. *Let P be a finite partial IP loop satisfying the above conditions (4), such that $\Gamma(P) \neq \emptyset$. Then there exists a finite partial IP loop $Q \geq P$ satisfying the conditions (4), as well, such that $\#\Gamma(Q) < \#\Gamma(P)$.*

Theorem 1.1 follows from Propositions 1.4, 1.5 and 1.6. Indeed, if P is a finite partial IP loop (such that $\Gamma(P) \neq \emptyset$, because otherwise there is nothing to prove) then, using Proposition 1.4, we can find a finite partial IP loop $Q \geq P$ such that $3 \mid o_3(Q)$. If $\Gamma(Q) = \emptyset$ then $L = Q$ is already a finite IP loop extending P, and we are done. Otherwise, applying Proposition 1.5, we obtain a finite partial IP loop $Q_1 \geq Q$ satisfying conditions (4) from Proposition 1.5. If $\Gamma(Q_1) = \emptyset$ then we are done, again. Otherwise, we can apply Proposition 1.6 and get a finite partial IP loop $Q_2 \geq Q_1$ satisfying conditions (4), as well, such that $\#\Gamma(Q_2) < \#\Gamma(Q_1)$. Iterating this step finitely many times we finally arrive at some finite partial IP loop Q_n extending P such that $\Gamma(Q_n) = \emptyset$. Then $L = Q_n \geq P$ is a finite IP loop we have been looking for.

Thus it is enough to prove Propositions 1.4, 1.5 and 1.6. This will take place in the next four sections.

2 Some preliminary results

In this section we list the auxiliary results we will use in the proofs of Propositions 1.4, 1.5 and 1.6.

Lemma 2.1. *Let P be a partial IP loop and $x, y, z \in P$. Then the following six conditions are equivalent:*

(i) $(x, y) \in D(P)$ *and* $xy = z$;
(ii) $\left(z, y^{-1}\right) \in D(P)$ *and* $zy^{-1} = x$;
(iii) $\left(x^{-1}, z\right) \in D(P)$ *and* $x^{-1}z = y$;
(iv) $\left(y, z^{-1}\right) \in D(P)$ *and* $yz^{-1} = x^{-1}$;
(v) $\left(z^{-1}, x\right) \in D(P)$ *and* $z^{-1}x = y^{-1}$;
(vi) $\left(y^{-1}, x^{-1}\right) \in D(P)$ *and* $y^{-1}x^{-1} = z^{-1}$.

Proof. Using property (3) from the definition of partial IP loops and (if necessary) the fact that $\left(a^{-1}\right)^{-1} = a$ for any $a \in P$, we can get the following cycle of implications:

$$\text{(i)} \implies \text{(ii)} \implies \text{(v)} \implies \text{(vi)} \implies \text{(iv)} \implies \text{(iii)} \implies \text{(i)}.$$

We show just the first implication, leaving the remaining ones to the reader. If $(x, y) \in D(P)$ and $xy = z$ then, according to (3),

$$\left(z, y^{-1}\right) = \left(xy, y^{-1}\right) \in D(P)$$

and $zy^{-1} = x$. □

In particular, we will frequently use the fact that, as a consequence of Lemma 2.1, the conditions $(x, y) \in D(P)$ and $\left(y^{-1}, x^{-1}\right) \in D(P)$ are equivalent for any $x, y \in P$.

In the generic case all the six equivalent conditions in Lemma 2.1 are different. There are just two kinds of exceptions: first the trivial ones, when at least one of the elements x, y, z equals the unit 1 (which never produce gaps), and second, if $x = y \in O_3(P)$, when the six conditions reduce to just two:

(i_3) $(x, x) \in D(P)$ and $xx = x^{-1}$,
(ii_3) $\left(x^{-1}, x^{-1}\right) \in D(P)$ and $x^{-1}x^{-1} = x$.

Since the first condition is satisfied by the definition of order 3 elements, so is the second one, hence this situation produces any gap, neither.

From now on we will preferably use a more relaxed language: when writing $xy = z$ for elements x, y, z of some partial IP loop P we will automatically assume that $(x, y) \in D(P)$, without mentioning it explicitly.

The number of gaps in any finite partial IP loop P is related to the size of P and that of the set $O_3(P)$ of order three elements through a congruence modulo 6.

Lemma 2.2. *Let P be a finite partial IP loop. Then*

$$\#\Gamma(P) \equiv (\#P - 1)(\#P - 2) - o_3(P) \pmod 6.$$

Proof. We know that $(x,1),(1,x),\left(x,x^{-1}\right) \in D(P)$ for any $x \in P$. At the same time, $(a,a) \in D(P)$ for all $a \in O_3(P)$, as well. Except for these pairs, there are other $(\#P-1)(\#P-2)-o_3(P)$ pairs which can be either in $D(P)$ or in $\Gamma(P)$. Those which are in $D(P)$ can be split into sixtuples according to Lemma 2.1, hence their number is divisible by 6, proving the above congruence. □

We will also use the Dirac's theorem from [7], giving a sufficient condition for the existence of a Hamiltonian cycle in a graph. For our purpose, the term *graph* always means an undirected graph without loops and multiple edges. For the basic graph-theoretical concepts the reader is referred to Diestel [5].

Lemma 2.3. *Let G be a graph with $n \geq 3$ vertices in which every vertex has degree at least $n/2$. Then G has a Hamiltonian cycle.*

3 Extensions of partial IP loops and the proof of Proposition 1.4

All the three Propositions 1.4, 1.5 and 1.6 deal with extensions $(Q,*)$ of a partial IP loop $(P,\cdot)$, which can be combined using two more specific types of this construction: first, extensions preserving (the domain of) the binary operation $\cdot$ on the original partial IP loop P and extending the base set of P, and, second, extensions preserving the base set P and extending (the domain of) the binary operation on P. In symbols, the extending partial IP loop $Q \geq P$ satisfies $D(P) = D(Q) \cap (P \times P)$ in the first case, while $P = Q$ and $D(P,\cdot) \subset D(Q,*)$ in the second. We start with the first type of extensions.

Let P, Q be two partial IP loops such that $P \cap Q = \{1\}$, i.e., their base sets have just the unit element 1 in common. Then, obviously, the set $P \cup Q$ can be turned into a partial IP loop, which we denote by $P \sqcup Q$, extending both P and Q, with domain

$$D(P \sqcup Q) = D(P) \cup D(Q),$$

i.e., preserving the original operations on both P and Q, and leaving undefined all the products xy, yx, for $x \in P \setminus \{1\}$, $y \in Q \setminus \{1\}$. The partial IP loop $P \sqcup Q$ is called the *direct sum* of the partial IP loops P and Q.

Let us fix the notation for some particular cases of this construction, considered as extensions of the IP loop P fixed in advance. In all the particular cases below A denotes a nonempty set disjoint from P. Then the set $A \cup \{1\}$ will be turned into a partial IP loop $\big(A \cup \{1\},\cdot\big)$, depending on some map $\sigma\colon A \to A$.

Let $\sigma\colon A \to A$ be an involution, i.e., $\sigma(\sigma(a)) = a$ for any $a \in A$. Then the *minimal partial IP loop* $[A,\sigma]$ has the base set $A \cup \{1\}$ and the partial binary operation given by $1 \cdot 1 = 1$, and

$$1a = a1 = a, \qquad a\sigma(a) = \sigma(a)a = 1,$$

for any $a \in A$, leaving the operation result ab undefined for any other pair of elements $a,b \in A$. The reader is asked to realize that $[A,\sigma]$ is indeed a partial IP loop, and that it is minimal (concerning its domain) among all partial IP loops with the base set $A \cup \{1\}$, which satisfy

$$a^{-1} = \sigma(a)$$

for any $a \in A$. Then, obviously,

$$O_2[A,\sigma] = \{a \in A : \sigma(a) = a\},$$

i.e., order two elements in $[A,\sigma]$ coincide with the fixpoints of the map σ. The direct sum of the partial IP loops P and $[A,\sigma]$ is denoted by

$$P[A,\sigma] = P \sqcup [A,\sigma].$$

Order two elements in $P[A,\sigma]$ split into two disjoint easily recognizable parts

$$O_2(P[A,\sigma]) = O_2(P) \cup O_2[A,\sigma].$$

If $\sigma = \mathrm{id}_A \colon A \to A$ is the identity on A, we write

$$P[A,\mathrm{id}_A] = P[A],$$

in which case

$$O_2(P[A]) = O_2(P) \cup A.$$

If $A = \{a_1,\dots,a_n\}$ is finite, we write

$$P[A] = P[a_1,\dots,a_n].$$

In particular, if $A = \{a\}$ is a singleton (and $\sigma = \mathrm{id}_A$ is the unique map $A \to A$), then

$$P[\{a\}] = P[a].$$

If $A = \{a,a'\}$ where $a \neq a'$, and σ is the transposition exchanging a and a', we denote

$$P[A,\sigma] = P[a \leftrightarrow a'].$$

From among the second type of extensions of a partial IP loop P, preserving its base set P and extending just (the domain of) its operation the simplest ones attempt at filling in just a single gap in P. This type of extension will be called a *simple extension through the relation* $xy = z$. More precisely, having $x,y,z \in P$ such that $(x,y) \in \Gamma(P)$, we want to put $xy = z$. From Lemma 2.1 it follows that then we have to satisfy the remaining five relations, too. This is possible only if all the pairs (x,y), $\left(z,y^{-1}\right)$, $\left(x^{-1},z\right)$, etc., occurring there are gaps in P. This is a sufficient condition, as well, since in that case we can define all the products as required by Lemma 2.1. Thus filling in the gap (x,y) enforces to fill in some other related gaps, too. In that case we automatically assume that the remaining five relations are defined in accord with Lemma 2.1.

Iterating simple extensions through particular relations we have to check in each step whether any new relation $uv = w$ (and its equivalent forms) does not interfere not only with the pairs in $D(P)$ but also with the gaps already filled in by previous simple extensions. In other words, we are interested in situations when we can fill in a whole set of gaps at once.

If $(P,\cdot)$ is a partial IP loop and $*$ is a partial operation on the set P with domain $T \subseteq P \times P$, such that $T \subseteq \Gamma(P)$ then, since $D(P) \cap T = \emptyset$, we can extend the original operation $\cdot$ to the set $D(P) \cup T$ by putting $xy = x * y$ for $(x,y) \in T$. The resulting structure will be called the *extension of the IP loop* P *through the operation* $*$ and denoted by P^*. The next lemma tells us when such an extension gives us a partial IP loop, again. In its formulation x^{-1} denotes the inverse of the element $x \in P$ with respect to the original operation $\cdot$ in P.

Lemma 3.1. *Let $(P,\cdot)$ be a partial IP loop and $*$ be a partial binary operation on the set P with domain $T \subseteq \Gamma(P)$. Then the extension of the operation $\cdot$ through the operation $*$ to the set $D(P) \cup T$ yields a partial IP loop extending P if and only if T and $*$ satisfy the following condition:*

(5) for any $x,y,z \in P$, if $(x,y) \in T$ and $x * y = z$ then also all the pairs

$$\big(z,y^{-1}\big),\ \big(x^{-1},z\big),\ \big(y,z^{-1}\big),\ \big(z^{-1},x\big),\ \big(y^{-1},x^{-1}\big)$$

belong to T and satisfy all the relations

$$z * y^{-1} = x, \qquad x^{-1} * z = y, \qquad y * z^{-1} = x^{-1},$$
$$z^{-1} * x = y^{-1}, \qquad y^{-1} * x^{-1} = z^{-1}.$$

Proof. In view of Lemma 2.1, condition (5) obviously is necessary. By the same reason, condition (5) implies that each of the particular relations $xy = x * y$, for $(x,y) \in T$, can be separately added to P. Since $T \subseteq \Gamma(P)$, no particular relation $xy = x * y$ can interfere with the remaining added relations $uv = u * v$. □

The following simple combination of both the types of extensions will be used in the proof of Proposition 1.4.

Let A be a set (disjoint from P) and $\sigma\colon A \to A$ be a fixpointfree involution (i.e., $\sigma(a) \neq a$ for every $a \in A$). Then $[A,\sigma]_3$ denotes the extension of the minimal partial IP loop $[A,\sigma]$ through (just) the additional relations

$$aa = \sigma(a)$$

for any $a \in A$. Formally, $[A,\sigma]_3$ is the extension of $[A,\sigma]$ through the operation $*$ defined on the set $T = \{(a,a) : a \in A\}$ by $a * a = \sigma(a)$ for any $a \in A$. It is clear that each pair (a,a) is indeed a gap in $[A,\sigma]$ and that the condition (5) from Lemma 3.1 is satisfied. Hence $[A,\sigma]_3$ is a partial IP loop extending $[A,\sigma]$ in which

$$a^{-1} = \sigma(a) = aa$$

for each $a \in A$, i.e., every element $a \in A$ has order three. For the direct sum

$$P[A,\sigma]_3 = P \sqcup [A,\sigma]_3$$

we have

$$O_3(P[A,\sigma]_3) = O_3(P) \cup A.$$

If $A = \{a,a'\}$, where $a \neq a'$, then the denotations $[A, a \leftrightarrow a']_3$ and

$$P[a \leftrightarrow a']_3 = P[A, a \leftrightarrow a']_3$$

are already self-explanatory, and similarly for $[A, a \leftrightarrow a', b \leftrightarrow b']_3$ and

$$P[a \leftrightarrow a', b \leftrightarrow b']_3 = P[A, a \leftrightarrow a', b \leftrightarrow b']_3$$

where the set A consists of four distinct elements a, a', b, b'.

Proof of Proposition 1.4. Let a, a', b, b' be four distinct elements not belonging to P. Let us form the extensions $Q = P[a \leftrightarrow a']_3$ and $R = P[a \leftrightarrow a', b \leftrightarrow b']_3$. Obviously,

$$o_3(Q) = o_3(P) + 2 \qquad \text{and} \qquad o_3(R) = o_3(P) + 4.$$

Since one of the numbers $o_3(P)$, $o_3(P)+2$, $o_3(P)+4$ is divisible by 3, one of the partial IP loops P, Q, R has the desired property. □

4 The proof of Proposition 1.5

A more subtle combination of the two types of extensions introduced in Section 3 will be required in the proof of Proposition 1.5.

Proof of Proposition 1.5. Let P be a finite partial IP loop such that $3 \mid o_3(P)$, and A be a finite set disjoint from P with the number of its elements satisfying

$$\#A \geq \max\bigl\{5(\#P) - 1, \#\Gamma(P)/2\bigr\} \qquad \text{and} \qquad 10 \leq \#P + \#A \equiv 4 \pmod 6.$$

First we construct the minimal extension $P[A]$, in which every element a of A has order two, while

$$O_3(P[A]) = O_3(P).$$

Hence the partial IP loop $P[A]$ has the base set $P \cup A$ with the required number of elements and the same number of elements of order three as P.

Next, we construct an extension of $P[A]$ in which all the original gaps in $\Gamma(P)$ will be filled. We take $T = \Gamma(P) \subseteq \Gamma(P[A])$ and introduce a binary operation $*$ on T, assigning to each pair of gaps $(x, y), \bigl(x^{-1}, y^{-1}\bigr) \in T$ a (self-inverse) element

$$x * y = y^{-1} * x^{-1} = (x * y)^{-1}$$

from A. At the same time we arrange that (with the above exception) $x*y \neq u*v$ whenever (x, y) and (u, v) are different gaps in P. This is possible, as $\#A \geq \#\Gamma(P)/2$. Since all the pairs $(x, y) \in P[A]$ such that $x \in A$ or $y \in A$, except for $(1, a)$, $(a, 1)$ and (a, a) where $a \in A$, are gaps in $P[A]$, condition (5) of Lemma 3.1 is obviously satisfied. Thus we can construct the partial IP loop $P[A]^*$, extending $P[A]$ through the operation $*$. It still has the base set $P \cup A$, while

$$\Gamma\bigl(P[A]^*\bigr) \cap (P \times P) = \emptyset.$$

At the same time, $D\bigl(P[A]^*\bigr) \cap (A \times A) = \{(a, a) : a \in A\}$, so that $ab = 1 \in P$ for any $(a, b) \in D\bigl(P[A]^*\bigr) \cap (A \times A)$.

Finally, we construct an extension Q of $P[A]^*$ with the same base set $P \cup A$, such that

$$\Gamma(Q) \subseteq O_2(Q) \times O_2(Q).$$

As all the elements of A are of order two, and $P[A]^*$ has no gap $(x, y) \in P \times P$, it suffices to manage that $(x, a), (a, x) \in D(Q)$ for all $a \in A$, $x \in P \setminus O_2(P)$, $x \neq 1$.

We will proceed by an induction argument. To this end we represent the set

$$P \setminus \bigl(O_2(P) \cup \{1\}\bigr) = \bigl\{x_1, x_1^{-1}, \ldots, x_n, x_n^{-1}\bigr\},$$

in such a way that each pair of mutually inverse elements $x, x^{-1} \in P \setminus \bigl(O_2(P) \cup \{1\}\bigr)$ occurs in this list exactly once. To start with we put $Q_0 = P[A]^*$. Now we assume that, for some $0 \leq k < n$, we already have an IP loop $Q_k \geq P[A]^*$ with the same base set $P \cup A$, satisfying the following three conditions:

(6) $au, va \in A$ for any $a \in A$, $u, v \in P \setminus \{1\}$ such that $(a, u), (v, a) \in D(Q_k)$,

(7) $ab \in P$ for any $(a, b) \in D(Q_k) \cap (A \times A)$, and

(8) $(x_l, a), (a, x_l) \in D(Q_k)$ for all $0 \leq l \leq k$, $a \in A$.

Observe that Q_0 trivially satisfies all these conditions (with $k = 0$), and condition (8) jointly with Lemma 2.1 imply that $\big(x_l^{-1}, a\big), \big(a, x_l^{-1}\big) \in D(Q_k)$ for all $0 \le l \le k$, $a \in A$, too. For $x = x_{k+1}$, we have to fill in all the gaps in Q_k in which x occurs, preserving all the conditions (6), (7), (8) with k replaced by $k+1$. That way all the gaps in Q_k containing x^{-1} will be filled in, as well.

Let us introduce the sets

$$L_x = \{a \in A : (a, x) \in \Gamma(Q_k)\} \qquad \text{and} \qquad R_x = \{a \in A : (x, a) \in \Gamma(Q_k)\}.$$

Then Lemma 2.1 implies that $(a, x) \in \Gamma(Q_k)$ if and only if $\big(x^{-1}, a\big) \in \Gamma(Q_k)$ for each $a \in A$, hence $L_x = R_{x^{-1}}$ and $R_x = L_{x^{-1}}$.

Claim 1. *We have* $\#L_x = \#R_x$.

Proof. Since $xu = v$ implies $v^{-1}x = u^{-1}$ for any $u, v \in P \cup A$, we have a bijection between the sets

$$(P \cup A) \setminus L_x = \{u \in P \cup A : (x, u) \in D(Q_k)\},$$
$$(P \cup A) \setminus R_x = \big\{v \in P \cup A : \big(v^{-1}, x\big) \in D(Q_k)\big\},$$

which implies that the sets L_x and R_x have the same number of elements. □

Thus there exists a bijective map $\eta\colon L_x \to R_x$ (with inverse map $\eta^{-1}\colon R_x \to L_x$); latter on we will specify some additional requirements concerning it. We intend to use η in defining the extending operation $*$ on the set

$$T_x = \big(L_x \times \{x\}\big) \cup \big(\{x\} \times R_x\big) \cup \big(R_x \times \big\{x^{-1}\big\}\big) \cup \big(\big\{x^{-1}\big\} \times L_x\big) \cup \big\{(a, \eta(a)) : a \in L_x\big\} \cup \big\{(\eta(a), a) : a \in L_x\big\}$$

by putting

$$a * x = \eta(a)$$

for any $a \in L_x$. Then we have to satisfy the remaining five conditions of Lemma 3.1, i.e. (remembering that the elements of A are self-inverse),

$$a * \eta(a) = x, \quad x^{-1} * a = \eta(a), \quad \eta(a) * a = x^{-1}, \quad \eta(a) * x^{-1} = x * \eta(a) = a.$$

The substitution $b = \eta(a)$ into the last two relations yields

$$b * x^{-1} = x * b = \eta^{-1}(b)$$

for any $b \in R_x$. Thus we have to guarantee that each pair $(a, \eta(a))$, where $a \in L_x$, will be a gap in Q_k. Since $(a, a) \in D(Q_k)$ for all $a \in A$, this will imply $\eta(a) \ne a$ for $a \in L_x \cap R_x$ (if any). Additionally, η should avoid any "crossing", i.e., the situation that

$$\eta(a) = b \qquad \text{and} \qquad \eta(b) = a$$

for some distinct $a, b \in L_x \cap R_x$. This namely, according to Lemma 2.1, would imply that $a * b = x = b * a$, and, since $(a * b)^{-1} = b * a$, produce a contradiction $x = x^{-1}$. Now it is clear that once we succeed to satisfy all the above requirements, the partial IP loop Q_{k+1}, to be obtained as the extension of Q_k through the operation $*$ constructed from the

bijection η as described, will satisfy all the conditions (6), (7), (8) (with $k+1$ in place of k). Thus it is enough to show that there is indeed a "crossing avoiding" bijection $\eta\colon L_x \to R_x$ such that

$$(a, \eta(a)) \in \Gamma(Q_k)$$

for each $a \in L_x$. To this end we denote the common value of $\#L_x = \#R_x$ by m, enumerate the sets

$$L_x = \{a_1, \ldots, a_m\}, \qquad R_x = \{b_1, \ldots, b_m\}$$

in such a way that $i = j$ whenever $a_i = b_j \in L_x \cap R_x$, and introduce the graph G_x on the vertex set $V = \{1, \ldots, m\}$, joining two vertices i, j by an edge if and only if $i \neq j$ and both $(a_i, b_j), (a_j, b_i) \in \Gamma(Q_k)$.

Claim 2. *The graph G_x has a Hamiltonian cycle.*

Proof. According to Lemma 2.3, it suffices to show that $m \geq 3$ and that the minimal degree of vertices in G_x is at least $m/2$. We keep in mind that both the right side and the left side multiplication in Q_k by a fixed element are injective maps.

Since $ax \in P \setminus \{1\}$ for every $a \in A$ such that $(a, x) \in D(Q_k)$, there are at most $\#P - 1$ pairs (a, x) in $D(Q_k)$. Hence

$$m = \#L_x \geq \#A - \#P + 1 \geq 4(\#P) > 3.$$

Let i be any vertex in G_x. Then i is not adjacent to a vertex j if and only if at least one of the pairs (a_i, b_j), (a_j, b_i) belongs to $D(Q_k)$. However, for fixed a_i or b_i, all such products $a_i b_j$ or $a_j b_i$ belong to P and, in both cases, every element of P occurs as a result at most once. Thus there are at most $2(\#P)$ vertices in G_x not adjacent to i. Therefore,

$$\deg(i) \geq m - 2(\#P) \geq m - \frac{m}{2} = \frac{m}{2}. \qquad \square$$

Let π be a cyclic permutation of the set V such that $\big(1, \pi(1), \ldots, \pi^{m-1}(1)\big)$ is a Hamiltonian cycle in G_x. We define $\eta\colon L_x \to R_x$ by

$$\eta(a_i) = b_{\pi(i)}$$

for any $i \in V$. Obviously, η is bijective, $(a_i, \eta(a_i)) \in \Gamma(Q_k)$ for each $i \in V$, and, since $m \geq 3$, it avoids any crossing.

It follows that in the extension Q_{k+1} of the partial IP loop Q_k through the operation $*$ all the gaps from the set T_x are filled in, and the conditions (6), (7), (8) are preserved. The last partial IP loop $Q = Q_n$ satisfies already all the requirements of Proposition 1.5. $\square$

5 Steiner triples and the proof of Proposition 1.6

In the proof of Proposition 1.6 we will make use of Steiner loops and Steiner triple systems. A *Steiner loop* is an IP loop satisfying the identity $xx = 1$, i.e., an IP loop in which every element $x \neq 1$ has order two. Steiner loops are closely related to *Steiner triple systems*, which are systems $\mathcal{S}$ of three element subsets of a given base set X such that each two element subset $\{x, y\}$ of X is contained in exactly one set $\{x, y, z\} \in \mathcal{S}$. Namely, if L is a Steiner loop L then $X = L \setminus \{1\}$ becomes a base set of the Steiner triple system

$$\mathcal{S}_L = \big\{\{x, y, xy\} : x, y \in X\big\}.$$

Conversely, if $\mathcal{S}$ is a Steiner triple system with the base set X then, adjoining to X a new element $1 \notin X$, we obtain a Steiner loop with the base set $X^+ = X \cup \{1\}$, the unit 1 and the operation given by the casework

$$xy = \begin{cases} 1, & \text{if } x = y, \\ z, & \text{where } \{x, y, z\} \in \mathcal{S}, \text{ if } x \neq y, \end{cases}$$

for $x, y \in X$. Based on this definition, we will call a *Steiner triple* any three-element set $\{x, y, z\} \subseteq O_2(P)$ in any partial IP loop P, such that the product of any two of its elements equals the third one.

It is well known that there exists a Steiner triple system $\mathcal{S}$ on an n-element set X if and only if $n \equiv 1$ or $n \equiv 3 \pmod 6$ (see, e.g., Hwang [18]).

The construction reducing eventually the number of gaps in a given partial IP loop P, satisfying certain conditions which will be emerging gradually, is composed of several simpler steps, we are going to describe, now. At the same time, it depends on a six term progression $\mathbf{a} = (a_0, a_1, a_2, a_3, a_4, a_5)$ of pairwise distinct order two elements of P chosen in advance; the criteria for its choice will be clarified later on.

The first step is the *triplication construction*, which uses Steiner loops heavily. Given an arbitrary finite partial IP loop P such that $\#P \equiv 2$ or $\#P \equiv 4 \pmod 6$ we denote $n = \#P - 1$. Then Steiner triple systems on n-element sets, as well as Steiner loops on $(n+1)$-element sets exist; assume that Y, Z are two n-element sets, such P, Y, Z are pairwise disjoint, and that both the sets $Y^+ = Y \cup \{1\}$, $Z^+ = Z \cup \{1\}$ are equipped with binary operations turning them into Steiner loops. In rather an ambiguous way, we denote by

$$3P = P \sqcup Y^+ \sqcup Z^+$$

the direct sum of the partial IP loop P with the Steiner loops Y^+ and Z^+ (see Section 4). It is a partial IP loop with the base set $P \cup Y \cup Z$, consisting of $3n + 1$ elements, and the domain

$$D(3P) = D(P) \cup (Y \times Y) \cup (Z \times Z) \cup \big(\{1\} \times (Y \cup Z)\big) \cup \big((Y \cup Z) \times \{1\}\big).$$

We will extend the partial operation on $3P$ by filling in all the gaps consisting of pairs of elements of different sets P, Y, Z. That way we'll obtain an extension $3P^*$ of $3P$ with the same base set $P \cup Y \cup Z$, such that $\Gamma(3P^*) = \Gamma(P)$. The extending operation $*$ is defined on the set

$$T = (P_0 \times (Y \cup Z)) \cup ((Y \cup Z) \times P_0) \cup (Y \times Z) \cup (Z \times Y) \subseteq \Gamma\big(P \sqcup Y^+ \sqcup Z^+\big),$$

where $P_0 = P \setminus \{1\}$. It depends on some arbitrary fixed enumerations

$$P_0 = \{x_0, \dots, x_{n-1}\}, \qquad Y = \{y_0, \dots, y_{n-1}\}, \qquad Z = \{z_0, \dots, z_{n-1}\}$$

of the sets P_0, Y, Z, respectively. Once having them we put

$$y_i * z_{i+k} = x_{i+2k}$$

for $0 \leq i, k < n$, with the addition of subscripts modulo n. Then, in order to satisfy the conditions of Lemma 2.1, we define

$$x_{i+2k} * z_{i+k} = y_i, \qquad y_i * x_{i+2k} = z_{i+k}, \qquad x_{i+2k}^{-1} * y_i = z_{i+k},$$
$$z_{i+k} * x_{i+2k}^{-1} = y_i, \qquad z_{i+k} * y_i = x_{i+2k}^{-1},$$

using the fact that all the elements of Y and Z are self-inverse. As all the pairs (x, y), (y, x), (x, z), (z, x), (y, z), (z, y), where $x \in P_0$, $y \in Y$, $z \in Z$, are gaps in $3P$, Lemma 3.1 guarantees that the extension $3P^*$ of the partial IP loop $3P$ through the operation $*$ is a partial IP loop, again. For lack of better terminology we will call it a *Steiner triplication* of the partial IP loop P and suppress the Steiner loops Y^+, Z^+ and the particular enumerations in its notation.

The Steiner triplication $3P^*$ of P satisfies $\Gamma(3P^*) = \Gamma(P)$, hence it still has the same number of gaps as P. However, Proposition 1.6 requires us to decrease this number. This will be achieved in a roundabout way. First we cancel some pairs in the domain $D(3P^*)$, creating that way the potential to fill in more gaps than we have added. In order to allow for this next step, P has to satisfy some additional conditions, namely, $\#P \geq 10$ (i.e., $n \geq 9$) and $o_2(P) \geq 6$. Though the enumerations of the sets P_0, Y, Z, used in the definition of the extending operation $*$, could have been arbitrary, we now assume that these sets were enumerated in such a way that the six term progression $\mathbf{a} = (a_0, a_1, a_2, a_3, a_4, a_5)$ chosen in advance coincides with the sixtuple $(x_0, x_2, x_1, x_5, x_3, x_{n-3})$ and that $\{y_0, y_1, y_3\}$ is a Steiner triple in Y^+. This artificial trick will facilitate us the description of the next step of our construction.

As special cases of the above defining relations for the operation $*$ in $3P^*$ we get $z_0 = y_0x_0 = y_3x_{n-3}$, $z_1 = y_0x_2 = y_1x_1$ and $z_3 = y_1x_5 = y_3x_3$. In other words, we have the following seven Steiner triples in $3P^*$:

$$\{x_0, y_0, z_0\}, \quad \{x_2, y_0, z_1\}, \quad \{x_1, y_1, z_1\}, \quad \{x_5, y_1, z_3\},$$
$$\{x_3, y_3, z_3\}, \quad \{x_{n-3}, y_3, z_0\}, \quad \{y_0, y_1, y_3\}.$$

We delete these triples from the domain of $3P^*$. More precisely, for any one of these three-element sets we delete from $D(3P^*)$ all the six pairs consisting of its distinct elements. That way we obtain a partial IP loop $3P^- \leq 3P^*$, called the *reduction* of $3P^*$, which still is an extension of P, however, it has 42 more gaps than $3P^*$ (6 for each Steiner triple), and, since $\Gamma(P) = \Gamma(3P^*)$, than P, as well.

Instead we introduce some new triples consisting of the same elements, namely

$$\{x_0, x_2, y_0\}, \quad \{x_2, x_1, z_1\}, \quad \{x_1, x_5, y_1\},$$
$$\{x_5, x_3, z_3\}, \quad \{x_3, x_{n-3}, y_3\}, \quad \{x_{n-3}, x_0, z_0\},$$
$$\{y_0, y_1, z_1\}, \quad \{y_1, y_3, z_3\}, \quad \{y_3, y_0, z_0\},$$

which are intended to become Steiner triples, after we define a partial operation $\circ$ on the set $\{x_0, x_2, x_1, x_5, x_3, x_{n-3}, y_0, y_1, y_3, z_0, z_1, z_3\}$ by putting the product of any pair of distinct elements of a given three-element set from this list equal to the third one. That way we obtain an extending operation of the partial IP loop $3P^-$ if and only if all the pairs entering this new operation are gaps in $3P^-$. This is obviously true for the 18 pairs arising from the three triples in the last row above. However, this need not be the case for the pairs arising from the six triples in the first two rows. The problem can be reduced to the question which of the pairs (x_0, x_2), (x_2, x_1), (x_1, x_5), (x_5, x_3), (x_3, x_{n-3}), (x_{n-3}, x_0) belong to $\Gamma(P)$. If, e.g., $(x_0, x_2) \notin \Gamma(P)$ then we cannot put $x_0 \circ x_2 = y_0$, so that $\{x_0, x_2, y_0\}$ cannot become a Steiner triple.

Therefore, we include just those triples $\{x_i, x_j, y_k\}$ or $\{x_i, x_j, z_k\}$ for which the pair (x_i, x_j) is a gap in P. Every such "good" triple results in filling in six gaps. We already have 18 gaps filled in thanks to the last row. Thus we need at least five "good" triples in the

first two rows in order to fill in additional 30 gaps; this would give $18+30 = 48 > 42$ gaps, while having just four "good" triples results in refilling back 42 gaps, only. In general, we can fill in $6(3+g)$ gaps, where $0 \le g \le 6$ is the number of gaps (x_i, x_j) in the list.

We refer to this last step of the construction as to "filling in the gaps along the path" $\mathbf{a}$ and denote the final resulting extension of the reduction $3P^-$ by $3P\langle\mathbf{a}\rangle$. Obviously, $3P\langle\mathbf{a}\rangle$ is an extension of the original IP loop P, as well, having $6(3+g) - 42 = 6(g-4)$ less gaps than P. This number can be negative, 0 or positive, depending on whether $g < 4$, $g = 4$, or $g > 4$. That's why we are interested just in the case when $g \ge 4$.

After all these preparatory accounts we can finally approach the proof of Proposition 1.6.

Proof of Proposition 1.6. Let P be a finite partial IP loop satisfying the conditions (4), i.e.,

$$3 \mid o_3(P),\ \#P \ge 10,\ \#P \equiv 4 \pmod 6 \text{ and } \Gamma(P) \subseteq O_2(P) \times O_2(P),$$

such that $\Gamma(P) \ne \emptyset$. We are to show that there is a finite partial IP loop $Q \ge P$ satisfying these conditions, as well, with less gaps than P.

Since $\Gamma(P) \subseteq O_2(P) \times O_2(P)$, it is an antireflexive and symmetric relation on the set $O_2(P)$. Thus we can form the *gap graph* $G(P) = (V, E)$ with the set of vertices

$$V = \{x \in O_2(P) : (x, y) \in \Gamma(P) \text{ for some } y \in O_2(P)\}$$

and the set of edges

$$E = \big\{\{x, y\} : (x, y) \in \Gamma(P)\big\}.$$

From the definition of the set of vertices V it follows there are no isolated vertices in $G(P)$. Let's record some less obvious useful facts about this graph.

Claim 3.

(a) The degree of each vertex in $G(P)$ is even.

(b) The number of edges in $G(P)$ is divisible by three.

Proof. (a): Let $x \in O_2(P)$. Then the conditions $xy = z$ and $xz = y$ are equivalent for any $y, z \in P$. Additionally, as $x \ne 1$, from $xy = z$ it follows that $y \ne z$. Thus the elements $y \in P$ such that $(x, y) \in D(P)$ can be grouped into pairs, hence their number is even. As $\#P$ is even, too, so is the degree

$$\deg(x) = \#\{y \in O_2(P) : (x, y) \in \Gamma(P)\} = \#P - \#\{y \in P : (x, y) \in D(P)\}.$$

(b): By Lemma 2.2 we have

$$\#\Gamma(P) \equiv (\#P - 1)(\#P - 2) - o_3(P) \equiv 0 \pmod 6.$$

On the other hand, $\#P \equiv 4 \pmod 6$ and $3 \mid o_3(P)$, yielding $3 \mid \#\Gamma(P)$. Obviously, the number of edges in $G(P)$ is half of the number of gaps $\#\Gamma(P)$, hence the number of edges in $G(P)$ must be divisible by three. □

The structure of connected components in $G(P)$ obeys the following alternative.

Claim 4. *Let C be a connected component of the graph $G(P)$. Then either C contains a triangle or a path of length five, or, otherwise, C is isomorphic to one of the following graphs: the cycle C_4 of length four, the cycle C_5 of length five or the complete bipartite graph $K_{2,m}$ where $m \geq 4$ is even.*

Proof. Let C be any connected component in $G(P)$. As $G(P)$ has no isolated vertices and the degree of every vertex in C is even (and therefore at least two), there is a cycle in C. Assume that C contains no triangle and no path of length five. Then the length of this cycle must be bigger than three and less than six. Thus there are just the following two options:

(a) There is a cycle of length five in C. Then there cannot be any other edge coming out from its vertices since then there would be a path of length five contained in C. Thus C coincides with this cycle.

(b) There is a cycle of length four in C; let us denote it by (v_0, v_1, v_2, v_3). Then, as $G(P)$ contains no triangle, neither $\{v_0, v_2\}$ nor $\{v_1, v_3\}$ is an edge in $G(P)$. If there are no more vertices in C then C is a cycle of length four.

Otherwise, we can assume, without loss of generality, that there is a fifth vertex $u_0 \in C$ adjacent to v_0. As u_0 has an even degree, it must be adjacent to some other vertex, too. If it were adjacent to some vertex u_1, distinct from all the vertices v_0, v_1, v_2, v_3, there would be a path $(u_1, u_0, v_0, v_1, v_2, v_3)$ of length five in C. If u_0 were adjacent to v_1 or to v_3, there would be a triangle (u_0, v_0, v_1) or (u_0, v_0, v_3) in C. That means that $\{u_0, v_2\}$ must be an edge in $G(P)$ and $\deg(u_0) = 2$.

It follows that every other vertex in C must have degree two and it must be adjacent either to v_0 and v_2 or to v_1 and v_3. However, the second option is impossible, since in that case $(u_0, v_0, v_1, u_1, v_3, v_2)$ would be a path of length five. This means that C is isomorphic to the complete bipartite graph $K_{2,m}$, where one term of this partition is formed by the set $\{v_0, v_2\}$ and the second one by the rest of the vertices in C. Since every vertex has an even degree, m must be even. At the same time, $m \geq 4$, as $K_{2,2}$ has just four vertices (and it is isomorphic to the cycle C_4). □

Thus the proof of Proposition 1.6 will be complete once we show how to construct the extension Q in each of the cases listed in Claim 4.

(a) $G(P)$ *contains a triangle,* i.e., a three-element set of vertices $\{x, y, z\}$ such that all its two-element subsets are edges. Then we can extend P through the operation $*$ turning $\{x, y, z\}$ into a Steiner triple. The corresponding extension Q of P has all the properties required and six less gaps than P.

(b) $G(P)$ *contains a path* $\mathbf{a} = (a_0, a_1, a_2, a_3, a_4, a_5)$ *of length five.* Then we can form the Steiner triplication $3P^*$ of P and, filling in the gaps along the path $\mathbf{a}$ in its reduction $3P^-$, we obtain the final extension $Q = 3P\langle\mathbf{a}\rangle$ satisfying the condition (4), again. If (a_5, a_0) is a gap in P (i.e., if $\mathbf{a}$ is a cycle of length five in $G(P)$) then Q has twelve gaps less than P, otherwise it still has six gaps less than P.

We still have to prove Proposition 1.6 in the case there is neither any triangle nor any path of length five in $G(P)$. To this end it is enough to construct, in each of the remaining cases listed in Claim 4, an extension Q of P such that the graph $G(Q)$ has the same number of edges as $G(P)$, however, there is a path $\mathbf{b}$ of length five in $G(Q)$. From such a Q we can construct another extension $3Q\langle\mathbf{b}\rangle \geq Q \geq P$ with a smaller number of gaps and still

satisfying the condition (4), similarly as we did in the case (b). So let us have a closer look at the remaining cases.

(c) *$G(P)$ contains a connected component isomorphic to $K_{2,m}$, where $m \geq 4$.* Let $\{u_0, u_1\}$ be the two-element partition set and $\{v_0, v_1, v_2, v_3\}$ be any four-element subset of the m-element partition set in that component of $G(P)$. We denote by $\mathbf{a}$ the six-term progression $(v_0, u_0, v_1, v_2, u_1, v_3)$ and construct the extension $Q = 3P\langle\mathbf{a}\rangle$ of the partial IP loop P with the gap graph $G(Q)$. Then $\{v_0, u_0\}$, $\{u_0, v_1\}$, $\{v_2, u_1\}$, and $\{u_1, v_3\}$ are edges in $G(P)$, while $\{v_1, v_2\}$ and $\{v_3, v_0\}$ are not. Hence the new graph $G(Q)$ has the same number of edges as $G(P)$ and Q has the same number of gaps as P. At the same time, there are two distinct new vertices y_1, z_3 in $G(Q)$, occurring in the enumerations of the sets Y, Z, respectively. Now, one can easily verify that $\mathbf{b} = (v_0, u_1, v_1, y_1, v_2, u_0)$ is a path of length five in $G(Q)$.

(d) *There are two distinct connected components C and D in $G(P)$, each of them isomorphic to the cycle C_4 or C_5.* Let m and l denote any of the numbers 4 or 5. We assume that $(u_0, u_1, \dots, u_{m-1})$ and $(v_0, v_1, \dots, v_{l-1})$ are the cycles forming the components $C \cong C_m$ and $D \cong C_l$, respectively. Now we take the six term progression $\mathbf{a} = (u_0, u_1, u_2, v_0, v_1, v_2)$ and form the extension $Q = 3P\langle\mathbf{a}\rangle$. Once again, $\{u_0, u_1\}$, $\{u_1, u_2\}$, $\{v_0, v_1\}$ and $\{v_1, v_2\}$ are edges in $G(P)$, while $\{u_2, v_0\}$ and $\{v_2, u_0\}$ are not. Hence $G(Q)$ has the same number of edges as $G(P)$ and Q has the same number of gaps as P. Now, picking the new distinct vertices $y_1 \in Y$, $z_3 \in Z$, we obtain the path $\mathbf{b} = (u_3, u_2, y_1, v_0, v_{l-1}, v_{l-2})$ of length five in $G(Q)$.

(e) *$G(P)$ consists of a single connected component isomorphic either to C_4 or to C_5.* However, this is impossible, since the number of edges in $G(P)$ is divisible by three.

This concludes the proof of Proposition 1.6, as well as of Theorems 1.1, 1.2 and 1.3. □

6 Final remarks

The discussion from the introduction together with Theorem 1.3 naturally lead to the following question.

Problem 6.1. Is there some minimal (ore even the least) axiomatic class $\mathbf{K}$ of IP loops such that every group is locally embeddable into $\mathbf{K}_{\mathrm{fin}}$? Does this class (if it exists) satisfy the Finite Embeddability Property?

The first candidate which should be examined in this connection seems to be the class of all Moufang loops introduced in [25]: A *Moufang loop* is a loop satisfying one (hence all) of the following four equivalent identities

$$x(y(xz)) = ((xy)x)z, \qquad (xy)(zx) = (x(yz))x,$$
$$x(y(zy)) = ((xy)z)y, \qquad (xy)(zx) = x((yz)x),$$

cf. Pflugfelder [26], Kunnen [19]. It is well known that every Moufang loop is an IP loop.

The following is not the usual definition of the concept of a sofic group (see Gromov [15], Weiss [29], Ceccherini-Silberstein, Coornaert [2]), however, as proved by Gordon and Glebsky [12], it is equivalent to it. A group $(G, \cdot, 1)$ is *sofic* if for every nonempty

finite set $X \subseteq G$ and every $\varepsilon > 0$ there exists a finite quasigroup $(Q, *)$ such that $X \subseteq Q$, for all $x, y \in X$ satisfying $xy \in X$ we have $xy = x * y$, as well as

$$\frac{\#\{q \in Q : (x * y) * q \neq x * (y * q)\}}{\#Q} < \varepsilon,$$

and, finally,

$$\frac{\#\{q \in Q : 1 * q \neq q\}}{\#Q} < \varepsilon.$$

No example of a non-sofic group is known up today, however, there is a general belief that not every group is sofic. Theorem 1.3 together with the above description of sofic groups indicate that the sofic groups could perhaps be characterized as groups locally embeddable into some "nice" subclass of the class of finite IP loops, fulfilling some "reasonable amount of associativity". A natural candidate is the class of all finite Moufang loops, once again. For some additional reasons in favor of this choice see [11].

As already indicated, one should start with trying to clarify the following question.

Problem 6.2. Does the class of all Moufang loops have the FEP?

If the answer is negative then it would make sense to elaborate on the following problem.

Problem 6.3. Characterize those groups which are locally embeddable into finite Moufang loops.

Finally, let us formulate two possible responses to Problem 6.3.

Conjecture 6.4. *Every group is locally embeddable into finite Moufang loops.*

Conjecture 6.5. *A group G is sofic if and only if it is locally embeddable into finite Moufang loops.*

Unless every group is sofic, these two conjectures contradict each other. Let us remark that we find the first one more probable to be true than the second one. This would follow from the affirmative answer to Problem 6.2, however it might be true even if the class of Moufang loops failed to have the FEP.

References

[1] V. D. Belousov and G. B. Belyavskaya, *Latin Squares, Quasigroups and Their Applications (in Russian)*, Shtiintsa, Kishinev, 1989.

[2] T. Ceccherini-Silberstein and M. Coornaert, *Cellular Automata and Groups*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2010, doi:10.1007/978-3-642-14034-1.

[3] C. C. Chang and H. J. Keisler, *Model Theory*, volume 73 of *Studies in Logic and the Foundations of Mathematics*, North-Holland, Amsterdam, 3rd edition, 1990.

[4] A. B. Cruse, On embedding incomplete symmetric Latin squares, *J. Comb. Theory Ser. A* **16** (1974), 18–22, doi:10.1016/0097-3165(74)90068-5.

[5] R. Diestel, *Graph Theory*, volume 173 of *Graduate Texts in Mathematics*, Springer, Berlin, 5th edition, 2018, http://diestel-graph-theory.com/.

[6] H. Dietrich and I. M. Wanless, Small partial Latin squares that embed in an infinite group but not into any finite group, *J. Symbolic Comput.* **86** (2018), 142–152, doi:10.1016/j.jsc.2017.04.002.

[7] G. A. Dirac, Some theorems on abstract graphs, *Proc. London Math. Soc.* **2** (1952), 69–81, doi:10.1112/plms/s3-2.1.69.

[8] A. Drápal, personal communication, 2004.

[9] T. Evans, Some connections between residual finiteness, finite embeddability and the word problem, *J. London Math. Soc.* **1** (1969), 399–403, doi:10.1112/jlms/s2-1.1.399.

[10] T. Evans, Word problems, *Bull. Amer. Math. Soc.* **84** (1978), 789–802, doi:10.1090/s0002-9904-1978-14516-9.

[11] S. M. Gagola, III, How and why Moufang loops behave like groups, *Quasigroups Related Systems* **19** (2011), 1–22, http://quasigroups.eu/contents/download/2011/19_1.pdf.

[12] L. Yu. Glebskiĭ and E. I. Gordon, On the approximation of amenable groups by finite quasigroups, *Zapiski Nauchnykh Seminarov (POMI)* **326** (2005), 48–58, doi:10.1007/s10958-007-0446-1, ftp://ftp.pdmi.ras.ru/pub/publicat/znsl/v326/p048.ps.gz.

[13] L. Yu. Glebsky and E. I. Gordon, On approximation of topological groups by finite quasigroups and finite semigroups, *Illinois J. Math.* **49** (2005), 1–16, doi:10.1215/ijm/1258138303.

[14] G. Grätzer, *Universal Algebra*, University Series in Higher Mathematics, Van Nostrand, Princeton, New Jersey, 1968.

[15] M. Gromov, Endomorphisms of symbolic algebraic varieties, *J. Eur. Math. Soc. (JEMS)* **1** (1999), 109–197, doi:10.1007/pl00011162.

[16] L. Henkin, Some interconnections between modern algebra and mathematical logic, *Trans. Amer. Math. Soc.* **74** (1953), 410–427, doi:10.2307/1990810.

[17] L. Henkin, Two concepts from the theory of models, *J. Symb. Logic* **21** (1956), 28–32, doi:10.2307/2268482.

[18] F. K. Hwang and S. Lin, A direct method to construct triple systems, *J. Comb. Theory Ser. A* **17** (1974), 84–94, doi:10.1016/0097-3165(74)90030-2.

[19] K. Kunen, Moufang quasigroups, *J. Algebra* **183** (1996), 231–234, doi:10.1006/jabr.1996.0216.

[20] C. C. Lindner, Embedding theorems for partial Latin squares, in: J. Dénes and A. D. Keedwell (eds.), *Latin Squares: New Developments in the Theory and Applications*, North-Holland, Amsterdam, volume 46 of *Annals of Discrete Mathematics*, 1991 pp. 217–265, doi:10.1016/s0167-5060(08)70968-3.

[21] A. I. Mal'tsev, On a general method for obtaining local theorems in group theory (in Russian), *Uchen. Zap. Ivanovsk. Ped. Inst.* **1** (1941), 3–9.

[22] A. I. Mal'tsev, On homomorphisms onto finite groups (in Russian), *Uchen. Zap. Ivanovsk. Ped. Inst.* **18** (1958), 49–60.

[23] A. I. Mal'tsev, *Algebraic Systems (in Russian)*, Izdat. "Nauka", Moscow, 1970.

[24] S. Meskin, Nonresidually finite one-relator groups, *Trans. Amer. Math. Soc.* **164** (1972), 105–114, doi:10.2307/1995962.

[25] R. Moufang, Zur Struktur von Alternativkörpern, *Math. Ann.* **110** (1935), 416–430, doi:10.1007/bf01448037.

[26] H. O. Pflugfelder, *Quasigroups and Loops: Introduction*, volume 7 of *Sigma Series in Pure Mathematics*, Heldermann Verlag, Berlin, 1990.

[27] A. C. C. Treash, *Inverse Property Loops and Related Steiner Triple Systems*, Ph.D. thesis, Emory University, Atlanta, Georgia, 1969, https://search.proquest.com/docview/302498451.

[28] A. M. Vershik and E. I. Gordon, Groups that are locally embeddable in the class of finite groups, *Algebra i Analiz* **9** (1997), 71–97, http://mi.mathnet.ru/eng/aa751.

[29] B. Weiss, Sofic groups and dynamical systems, *Sankhyā Ser. A* **62** (2000), 350–359.

[30] M. Ziman, Extensions of Latin subsquares and local embeddability of groups and group algebras, *Quasigroups Related Systems* **11** (2004), 115–125, http://www.quasigroups.eu/contents/download/2004/11_13.pdf.