THE EQUATIONAL THEORY OF PARAMEDIAL CANCELLATION GROUPOIDS

Jaroslav Ježek and Tomáš Kepka

0. Introduction

By a paramedial groupoid we mean a groupoid satisfying the equation $xy \cdot zu = uy \cdot zx$. As it is easy to see, the equational theory of paramedial groupoids, as well as the equational theory based on any balanced equation, is decidable.

In this paper we are going to investigate the equational theory of paramedial cancellation groupoids; by this we mean the set of all equations satisfied by paramedial cancellation groupoids. (By a cancellation groupoid we mean a groupoid satisfying both $xz = yz \to x = y$ and $zx = zy \to x = y$.) Clearly, the equational theory of paramedial cancellation groupoids is just the least cancellative equational theory containing the paramedial law. We will show that this equational theory is also decidable (Theorem 4.1), that it is a proper extension of the equational theory of paramedial groupoids (Theorem 4.3), and that whenever two terms are unrelated with respect to this equational theory, then their squares are also unrelated (Theorem 4.7).

The results can be compared with those of [2] and [3] for medial groupoids.

1. The free monoid

We denote by M the free monoid over $\{1, 2\}$. The elements of M are called words. The empty word is the unit of M; it will be denoted by o.

A word f is said to be a subword of a word e if $e = gfh$ for some words g and h.

Two words e and f are called comparable if either e is a beginning of f or f is a beginning of e. In all other cases, the two words are incomparable.

The congruence of M generated by $\langle 11, 22\rangle$ will be denoted by α. Clearly, $e \; \alpha \; f$ implies that the words e, f have the same length. By an α-derivation we mean a finite sequence $e_0, \dots, e_k$ of words such that each e_{i+1} is obtained from e_i by replacing a subword 11 with 22, or by replacing a subword 22 with 11. By an α-derivation of f from e we mean an α-derivation $e_0, \dots, e_k$ such that $e_0 = e$ and $e_k = f$. It is easy to see that $e \; \alpha \; f$ if and only if there exists an α-derivation of f from e.

1.1. Lemma. *α is a cancellative congruence of M.*

Proof. We shall prove only that α is left cancellative, and for this it is sufficient to prove that $ae \; \alpha \; af$ implies $e \; \alpha \; f$, where $a \in \{1, 2\}$. Denote by b the element of $\{1, 2\} - \{a\}$. There exists an α-derivation $e_0, \dots, e_k$ with $e_0 = ae$ and $e_k = af$. We

While working on this paper both authors were partially supported by the Grant Agency of Czech Republic, Grant No 201/96/0312.

shall proceed by double induction, the outer on the length of ae and the inner on k. If either $e = o$ or $k \leq 1$, everything is clear. Let $k \geq 2$. The word e_1 is obtained from ae by replacing either 11 with 22, or 22 with 11. If the replacement is done inside e, then $e_1 = ag$ for some $g \ \alpha \ e$; by the inner induction applied to $e_1, \dots, e_k$ we get $g \ \alpha \ f$ and hence $e \ \alpha \ f$. So, we can assume that $ae = aap$ for some p and $e_1 = bbp$. Quite similarly, we can assume that $af = aaq$ for some q and $e_{k-1} = bbq$. By the inner induction applied to $e_1, \dots, e_{k-1}$ we get $bp \ \alpha \ bq$. Now bp is shorter than ae, so by the outer induction we obtain $p \ \alpha \ q$. So, $e = ap \ \alpha \ aq = f$. □

For two blocks B_1 and B_2 of α, we denote by B_1B_2 the block of the words congruent with ef modulo α, where $e \in B_1$ and $f \in B_2$. This does not depend on the choice of e and f. However, B_1B_2 is not necessarily equal to the set of words that can be decomposed into the product ef with $e \in B_1$ and $f \in B_2$. For example, $\{1\}\{1\} = \{11, 22\}$.

For a subset B of M, we put

$$B^{(1)} = \{e \in M : 1e \in B\},$$
$$B^{(2)} = \{e \in M : 2e \in B\},$$
$$B^{[1]} = \{e \in M : e \ \alpha \ 1f \text{ for some } f \in B\},$$
$$B^{[2]} = \{e \in M : e \ \alpha \ 2f \text{ for some } f \in B\}.$$

1.2. Lemma. *Let B be a block of α. Then:*

1. *each of $B^{(1)}$ and $B^{(2)}$ is either empty or a block of α;*
2. *each of $B^{[1]}$ and $B^{[2]}$ is a block of α;*
3. *$B^{[1](1)} = B$ and $B^{[2](2)} = B$.*

Proof. If $e, f \in B^{(1)}$, then $1e \in B$ and $1f \in B$, so that $1e \ \alpha \ 1f$; by Lemma 1.1, $e \ \alpha \ f$. If $e \in B^{(1)}$ and $e \ \alpha \ f$, then $1f \ \alpha \ 1e \in B$, so $1f \in B$ and $f \in B^{(1)}$. We have proved that $B^{(1)}$ is either empty or a block of α.

We have $B^{[1]} = \{1\}B$, so $B^{[1]}$ is a block of α.

The following are equivalent for a word e:

$e \in B^{[1](1)}$;
$1e \in B^{[1]}$;
$1e \ \alpha \ 1f$ for some $f \in B$;
$e \ \alpha \ f$ for some $f \in B$ (by Lemma 1.1);
$e \in B$.

This means that $B^{[1](1)} = B$. The other statements can be proved dually. □

2. Terms

By a term we mean a groupoid term, i.e., an element of the absolutely free groupoid over the infinite countable set X of variables.

Let t be a term. By induction on the complexity of t we define a finite subset $\mathcal{O}(t)$ of M, and for each $e \in \mathcal{O}(t)$ a term $t[e]$, as follows: If $t \in X$, then $\mathcal{O}(t) = \{o\}$; $t[o] = t$. If $t = uv$, then $\mathcal{O}(t) = \{o\} \cup \{1e : e \in \mathcal{O}(u)\} \cup \{2e : e \in \mathcal{O}(v)\}$; $t[o] = t$, $t[1e] = u[e]$ and $t[2e] = v[e]$. The elements of $\mathcal{O}(t)$ are called occurrences in t. If $e \in \mathcal{O}(t)$ and $t[e] = w$, we say that e is an occurrence of a subterm w in t. We denote by $\mathcal{O}_X(t)$ the (finite) set of occurrences of variables in t.

Let t be a term, e be an occurrence of a subterm in t, and w be a term. There exists a unique term t' such that $t'[e] = w$ and $t'[f] = t[f]$ for any $f \in \mathcal{O}_X(t)$ incomparable with e. This term t' will be denoted by $R_{e:w}(t)$; it can be called the term obtained from t by replacing the occurrence of subterm at e with w.

Let t be a term and e, f be two incomparable occurrences of subterms in t. There exists a unique term t' such that $t'[e] = t[f]$, $t'[f] = t[e]$ and $t'[g] = t[g]$ for any $g \in \mathcal{O}_X(t)$ incomparable with both e and f. This term t' will be denoted by $\tau_{e,f}(t)$; it can be called the term obtained from t by transposing the subterms at e and f.

Let t be a term, x be a variable and B be a subset of M. We denote by $P_B(x,t)$ the set of the occurrences of x in t that belong to B.

2.1. Lemma. *Let u, v be two terms, x be a variable and B be a block of α. Then*

$$|P_B(x, uv)| = |P_{B^{(1)}}(x, u)| + |P_{B^{(2)}}(x, v)|.$$

Proof. It is easy. $\square$

2.2. Lemma. *Let t be a term, x be a variable and φ be a substitution (i.e., an endomorphism of the groupoid of terms). Let B be a block of α. Then*

$$|P_B(x, \varphi(t))| = \sum_{\substack{y \in X \\ B_1 B_2 = B}} |P_{B_1}(y, t)||P_{B_2}(x, \varphi(y))|.$$

Proof. For each triple y, B_1, B_2, where $y \in X$ and B_1, B_2 are blocks of α with $B_1 B_2 = B$, define a mapping H_{y,B_1,B_2} of $P_{B_1}(y,t) \times P_{B_2}(x, \varphi(y))$ into $P_B(x, \varphi(t))$ by $H_{y,B_1,B_2}(e, f) = ef$. One can easily check that these mappings are injective, that their ranges are pairwise disjoint and that $P_B(x, \varphi(t))$ is the union of their ranges. $\square$

3. The relation β

We denote by E the equational theory of paramedial cancellation groupoids.

Define a binary relation β on the set of terms as follows: $u \ \beta \ v$ if and only if $|P_B(x, u)| = |P_B(x, v)|$ for all variables x and all blocks B of α.

3.1. Lemma. *β is a cancellative congruence of the groupoid of terms. Moreover, β is fully invariant, and thus β is an equational theory.*

Proof. Clearly, β is an equivalence. It follows from Lemma 2.1 that β is a congruence. Applying 2.1 and 1.2, we see that β is cancellative. It is a consequence of 2.2 that β is fully invariant, i.e., $u \ \beta \ v$ implies $\varphi(u) \ \beta \ \varphi(v)$ for any substitution φ. $\square$

3.2. Lemma. *$E \subseteq \beta$.*

Proof. Clearly, E is just the least cancellative equational theory containing the paramedial law. It is easy to check that the paramedial law belongs to β, so the result is a consequence of 3.1. $\square$

3.3. Lemma. *Let t be a term and let $e,f\in\mathcal{O}_X(t)$ be such that f can be obtained from e by replacing a subword 11 with 22, or a subword 22 with 11. Then $t\ E\ \tau_{e,f}(t)$.*

Proof. By induction on the length of e (which is the same as the length of f). If e is of length at most 1, there is nothing to prove. Let e be of length at least 2, and let $t=uv$. If $e=1e'$ and $f=1f'$ for some e' and f', then by induction $u\ E\ \tau_{u',v'}(u)$, so that $uv\ E\ \tau_{u'v'}(u)v$, i.e., $t\ E\ \tau_{e,f}(t)$. If both e and f begin with 2, the proof is similar. So, we can assume without loss of generality that $e=11h$ and $f=22h$ for some h. If h is empty, then $t=xp\cdot qy$ and $\tau_{e,f}(t)=yp\cdot qx$ for some variables x,y and terms p,q, and $xp\cdot qy\ E\ yp\cdot qx$ clearly. So, without loss of generality we can assume that h begins with 1. We can write $e=111g$ and $f=221g$ for some g. Put $t=(t_1t_2\cdot t_3)(t_4\cdot t_5t_6)$, $x=t[e]=t_1[g]$ and $y=t[f]=t_5[g]$. Put $t_1'=R_{g:y}(t_1)$ and $t_5'=R_{g:x}(t_5)$, so that $\tau_{e,f}(t)=(t_1't_2\cdot t_3)(t_4\cdot t_5't_6)$. Take an arbitrary quadruple p,q,r,s of terms. In the sequence of terms

$$(t_1t_2\cdot t_3)(t_4\cdot t_5t_6)\cdot(pt_1'\cdot q)(t_5'r\cdot st_5')$$
$$(t_5'r\cdot st_5')(t_4\cdot t_5t_6)\cdot(pt_1'\cdot q)(t_1t_2\cdot t_3)$$
$$(t_5t_6\cdot st_5')(t_4\cdot t_5'r)\cdot(t_3q)(t_1t_2\cdot pt_1')$$
$$(t_5't_6\cdot st_5)(t_4\cdot t_5'r)\cdot(t_3q)(t_1't_2\cdot pt_1)$$
$$(t_5'r\cdot st_5)(t_4\cdot t_5't_6)\cdot(pt_1\cdot q)(t_1't_2\cdot t_3)$$
$$(t_1't_2\cdot t_3)(t_4\cdot t_5't_6)\cdot(pt_1\cdot q)(t_5'r\cdot st_5)$$
$$(t_1't_2\cdot t_3)(t_4\cdot t_5't_6)\cdot(pt_1\cdot q)(t_5r\cdot st_5')$$
$$(t_1't_2\cdot t_3)(t_4\cdot t_5't_6)\cdot(st_5'\cdot q)(t_5r\cdot pt_1)$$
$$(t_1't_2\cdot t_3)(t_4\cdot t_5't_6)\cdot(st_5'\cdot q)(t_5'r\cdot pt_1')$$
$$(t_1't_2\cdot t_3)(t_4\cdot t_5't_6)\cdot(pt_1'\cdot q)(t_5'r\cdot st_5')$$

each two neighbors constitute an equation belonging to E. In all but one cases this is clear, because the equation is a simple consequence of the paramedial law; the only exception is the one relating the eighth and the ninth terms of the sequence. In the 8-related-to-9 case, we need to show that $t_5r\cdot pt_1\ E\ t_5'r\cdot pt_1'$. This follows by induction, since $t_5'r\cdot pt_1'=\tau_{11g,22g}(t_5r\cdot pt_1)$ and $11g$ is shorter than $e=111g$.

So, the first and the last term in the sequence of the above ten terms are related modulo E. Since E is cancellative, we get $(t_1t_2\cdot t_3)(t_4\cdot t_5t_6)\ E\ (t_1't_2\cdot t_3)(t_4\cdot t_5't_6)$, i.e., $t\ E\ \tau_{e,f}(t)$. □

3.4. Lemma. *Let t be a term such that for some nonnegative integer n, all occurrences of variables in t are of length n. Let $e,f\in\mathcal{O}_X(t)$ be such that $e\ \alpha\ f$. Then $u\ E\ \tau_{e,f}(t)$.*

Proof. Let $e_0,\dots,e_k$ be an α-derivation of f from e. By 3.3, t is E-related with the term

$$\tau_{e_0,e_1}\tau_{e_1,e_2}\dots\tau_{e_{k-2},e_{k-1}}\tau_{e_{k-1},e_k}\tau_{e_{k-2},e_{k-1}}\dots\tau_{e_0,e_1}(t).$$

This term is equal to $\tau_{e,f}(t)$, as it is easy to see. □

3.5. Lemma. *Let t be a term and $e,f\in\mathcal{O}_X(t)$ be such that $e\ \alpha\ f$. Then $u\ E\ \tau_{e,f}(t)$.*

Proof. Put $x=t[e]$ and $y=t[f]$. Denote by n the common length of the words e and f. Let u be a term such that $u[e]=y$, $u[f]=x$ and a word belongs to $\mathcal{O}_X(u)$

if and only if it is of length n. (Clearly, there is at least one such term u.) Take arbitrarily two terms p and q. Applying 3.3 twice we get $tp \cdot qu \; E \; \tau_{11e,22e}(tp \cdot qu) = R_{e:y}(t)p \cdot qR_{e:x}(u) \; E \; \tau_{11f,22f}(R_{e:y}(t)p \cdot qR_{e:x}(u)) = \tau_{e,f}(u)p \cdot q\tau_{e,f}(u)$. By3.4 we have $\tau_{e,f}(u) \; E \; u$, so $tp \cdot qu \; E \; \tau_{e,f}(u)p \cdot q\tau_{e,f}(u) \; E \; \tau_{e,f}(u)p \cdot qu$ and by cancellation $t \; E \; \tau_{e,f}(u)$. □

3.6. Lemma. $\beta \subseteq E$.

Proof. Denote by $C(u, v)$ the set of the occurrences $e \in \mathcal{O}_X(u)$ such that either $e \notin \mathcal{O}_X(v)$ or $u[e] \neq v[e]$. Let $u \; \beta \; v$. We shall prove $u \; E \; v$ by induction on $|C(u, v)| + |C(v, u)|$. If this number is zero, then clearly $u = v$ and we are through. Now let e be a shortest word in $C(u, v) \cup C(v, u)$. Without loss of generality, $e \in C(u, v)$. Put $x = u[e]$. By the minimality of e, the word e belongs to $\mathcal{O}(v)$. (Otherwise, a proper beginning of e would belong to $\mathcal{O}_X(v)$, and this beginning would then belong to $C(v, u)$.) Put $w = v[e]$. We have $w \neq x$. Denote by B the block of α containing e. Since $u \; \beta \; v$, we have $|P_B(x, u)| = |P_B(x, v)|$. Now e belongs to $P_B(x, u) - P_B(x, v)$. Consequently, $P_B(x, v) - P_B(x, u)$ is also nonempty. Take a word $f \in P_B(x, v) - P_B(x, u)$. Hence we do not have $u[f] = x$. By the minimality of e, the word f belongs to $\mathcal{O}(u)$. Put $w' = u[f]$, so that $w' \neq x$. Put $u' = R_{f:z}(u)$, where z is a variable not occurring in u. By 3.5 we have $u' \; E \; \tau_{e,f}(u')$. Denote by φ the substitution acting as the identity on every variable except for $\varphi(z) = w'$. Then $\varphi(u') \; E \; \varphi(\tau_{e,f}(u'))$, i.e., $u \; E \; t$ where $t = \tau_{e,f}(u)$. By 3.2 we get $u \; \beta \; t$, and hence $t \; \beta \; v$.

Let $g \in C(t, v)$. If g is incomparable with both e and f, then $t[g] = u[g]$ and hence $g \in C(u, v)$. If g is comparable with e, then $g = eg'$ for some g' and $fg' \in C(u, v)$. Finally, g cannot be comparable with f. From this it follows that $|C(t, v)| \leq |C(u, v)|$.

It is easy to see that $C(v, t) \subset C(v, u)$ (we have $f \in C(v, u) - C(v, t)$). Hence $|C(t, v)| + |C(v, t)| < |C(u, v)| + |C(v, u)|$. Since $t \; \beta \; v$, we get $t \; E \; v$ by induction. But then, $u \; E \; v$. □

4. The equational theory

4.1. Theorem. *An equation $\langle u, v \rangle$ belongs to the equational theory of paramedial cancellation groupoids if and only if $|P_B(x, u)| = |P_B(x, v)|$ for all variables x and all blocks B of α. Consequently, the equational theory is decidable.*

Proof. It follows from 3.2, 3.6 and the definition of β. □

The following is a reformulation:

4.2. Corollary. *An equation $\langle u, v \rangle$ belongs to the equational theory of paramedial cancellation groupoids if and only if there is a bijection F of $\mathcal{O}_X(u)$ onto $\mathcal{O}_X(v)$ such that $e \; \alpha \; F(e)$ and $u[e] = v[F(e)]$ for all $e \in \mathcal{O}_X(u)$.* □

4.3. Theorem. *The equational theory of paramedial groupoids is properly contained in the equational theory of paramedial cancellation groupoids.*

Proof. Of course, if an equation is satisfied in all paramedial groupoids, then it is satisfied in all paramedial cancellation groupoids. By Theorem 4.1, the equation

$$\langle (xy \cdot z)(u \cdot vw), (vy \cdot z)(u \cdot xw) \rangle$$

belongs to the equational theory of paramedial cancellation groupoids. On the other hand, this equation does not belong to the equational theory of paramedial groupoids. In fact, it is easy to see that $\{(xy \cdot z)(u \cdot vw), (vw \cdot z)(u \cdot xy)\}$ is a block of the equational theory of paramedial groupoids. $\square$

For any $n \geq 0$, we define two words I_n and J_n by induction in the following way: $I_0 = J_0 = o$ (the empty word); for n odd, $I_n = 1I_{n-1}$ and $J_n = 2J_{n-1}$; for $n > 0$ even, $I_n = 2I_{n-1}$ and $J_n = 1J_{n-1}$. For example, $I_4 = 2121$ and $J_7 = 2121212$.

4.4. Lemma. *Let $n \geq 0$. The following are true:*

(1) *whenever $e \; \alpha \; I_n$, then $e = I_n$; whenever $e \; \alpha \; J_n$, then $e = J_n$;*
(2) *for n odd we have $I_n 1 \; \alpha \; 2J_n$ and $J_n 2 \; \alpha \; 1I_n$; for n even we have $I_n 1 \; \alpha \; 1J_n$ and $J_n 2 \; \alpha \; 2I_n$.*

Proof. (1) is clear, since the words I_n and J_n contain neither 11 nor 22 as a subword. Let us prove (2) by induction on n. For example, if n is odd, then $I_n 1 = J_{n-1}11 \; \alpha \; J_{n-1}22 \; \alpha \; 2I_{n-1}2 = 2J_n$. $\square$

For a subset B of M put $B^{\langle 1 \rangle} = B^{[1](2)}$, so that $e \in B^{\langle 1 \rangle}$ if and only if $2e \; \alpha \; 1f$ for some $f \in B$. If B is a block of α, then $B^{\langle 1 \rangle}$ is either a block of α or the empty set. By induction, we define $B^{\langle n \rangle}$ for $n \geq 0$ as follows: $B^{\langle 0 \rangle} = B$; $B^{\langle n+1 \rangle} = B^{\langle n \rangle \langle 1 \rangle}$.

4.5. Lemma. *Let B be a block of α and n be a nonnegative integer. If $e \in B^{\langle n \rangle}$, then $J_n e \; \alpha \; I_n f$ for some $f \in B$.*

Proof. By induction on n. For $n = 0$ it is clear. Let $e \in B^{\langle n+1 \rangle}$, so that $2e \; \alpha \; 1f$ for some $f \in B^{\langle n \rangle}$. By induction, $J_n f \; \alpha \; I_n g$ for some $g \in B$. According to 4.4(2) we have $J_{n+1} e = I_n 2e \; \alpha \; I_n 1f \; \alpha \; aJ_n f \; \alpha \; aI_n g = I_{n+1} g$, where $a = 1$ if n is even and $a = 2$ if n is odd. $\square$

4.6. Lemma. *For every block B of α there exists a positive integer n such that $B^{\langle 0 \rangle}, \dots, B^{\langle n-1 \rangle}$ are pairwise different blocks of α and $B^{\langle n \rangle}$ is empty.*

Proof. Suppose that for some $i > 0$, there exists a word $e \in B \cap B^{\langle i \rangle}$. By 4.5 we have $J_i e \; \alpha \; I_i f$ for some $f \in B$. Then $e \; \alpha \; f$, and we get $J_i e \; \alpha \; I_i f \; \alpha \; I_i e$. By 1.1, it follows that $J_i \; \alpha \; I_i$. By 4.4(1) we get $J_i = I_i$, a contradiction with $i > 0$.

So, if $B^{\langle 0 \rangle}, \dots, B^{\langle i \rangle}$ are all nonempty, then they are pairwise disjoint. All these blocks of α contain words of the same length, so their number cannot be arbitrarily large. $\square$

4.7. Theorem. *Let u, v be two terms such that the equation $\langle uu, vv \rangle$ belongs to the equational theory of paramedial cancellation groupoids. Then the equation $\langle u, v \rangle$ also belongs to the equational theory.*

Proof. By Theorem 4.1 we have $|P_B(x, uu)| = |P_B(x, vv)|$ for any variable x and any block B of α. Let a variable x be given. Let us call a block B of α good if $|P_B(x, u)| = |P_B(x, v)$.

By 1.2 and 2.1 we have

$$\begin{aligned} |P_B(x,u)| + |P_{B^{\langle 1 \rangle}}(x,u)| = & |P_{B^{[1](1)}}(x,u)| + |P_{B^{[1](2)}}(x,u)| = \\ & |P_{B^{[1]}}(x,uu)| = \\ & |P_{B^{[1]}}(x,vv)| = \\ & |P_{B^{[1](1)}}(x,v)| + |P_{B^{[1](2)}}(x,v)| = \\ & |P_B(x,v)| + |P_{B^{\langle 1 \rangle}}(x,v)|, \end{aligned}$$

so that $|P_B(x,u)| = |P_B(x,v)|$ if and only if $|P_{B^{\langle 1\rangle}}(x,u)| = |P_{B^{\langle 1\rangle}}(x,v)|$. This means that B is good if and only if $B^{\langle 1\rangle}$ is either good or empty. By 4.6, there exists an n such that $B^{\langle n\rangle}$ is empty and $B^{\langle 0\rangle},\dots,B^{\langle n-1\rangle}$ are blocks of α. Hence $B^{\langle n-1\rangle}$ is good, so that $B^{\langle n-2\rangle}$ is also good, etc., and the block $B = B^{\langle 0\rangle}$ is good. Since B and x were arbitrary, by Theorem 4.1 the equation $\langle u,v\rangle$ belongs to the equational theory. □

4.8. Corollary. *Let G be a free groupoid in the variety generated by paramedial cancellation groupoids. Then the transformation $a \mapsto aa$ of G is injective.* □

5. Quasigroup envelopes

In this section we will make use of 4.8 to solve a question formulated in [1]. In fact, we are going to show that every paramedial cancellative groupoid has a quasigroup envelope which is unique up to isomorphism. First, we have to recall a few notions introduced in [1].

Let H be a subgroupoid of a paramedial groupoid G. Then $Mul(G,H)$ is the transformation semigroup (acting on G) generated by the left and right translations L_x and R_x, for all $x \in H$. By 4.2 of [1], $Mul(G,H)$ is a left uniform semigroup. Further, we denote by $[H]_{G,c}$ the set of all $a \in G$ such that $f(a) \in H$ for at least one $f \in Mul(G,H)$.

5.1. Lemma. *Let H be a subgroupoid of a paramedial cancellative groupoid G and $K = [H]_{G,c}$. Then:*

(1) *$H \subseteq K$ and K is a subgroupoid of G.*
(2) *Every cancellative congruence of H can be extended in a unique way to a cancellative congruence of K.*
(3) *If G is a quasigroup, then K is so.*

Proof. See 4.10 and 4.11 of [1]. □

Let a paramedial (cancellative) groupoid G be a subgroupoid of a paramedial quasigroup Q. We say that Q is a quasigroup envelope of G if $A = Q$ whenever A is a subquasigroup of Q such that $G \subseteq A$.

5.2. Lemma. *Let G be a subgroupoid of a paramedial quasigroup Q. Then Q is a quasigroup envelope of G if and only if $Q = [G]_{Q,c}$.*

Proof. The result follows easily from 5.1(3). □

5.3. Theorem. *Every paramedial cancellative groupoid G has a quasigroup envelope which is determined uniquely up to G-isomorphism.*

Proof. A combination of 5.1(3), 4.8, and 5.4 and 5.5 of [1] yields the existence of a paramedial quasigroup Q such that G is a subgroupoid of Q and $Q = [G]_{Q,c}$, i.e., Q is a quasigroup envelope of G by 5.2. Now, let $\varphi : G \to A$ be a reflexion of G into the category of paramedial quasigroups and let $B = [\varphi(G)]_{A,c}$. There is a (uniquely determined) homomorphism $\psi : A \to Q$ such that $\psi\varphi$ is the identity on G. Then $G \subseteq \psi(B) \subseteq Q$ and $\psi(B)$ is a subquasigroup of Q. Consequently, $\psi(B) = Q$. Moreover, the kernel of $\psi|B$ is a (cancellative) congruence of B extending the kernel of $\psi|\varphi(G)$, i.e., extending the identity on $\varphi(G)$. By 5.1(2), $\psi|B$ is an isomorphism of B onto Q. The rest is clear. □

References

1. J. Cho, J. Ježek and T. Kepka, *Paramedial groupoids*, preprint.
2. J. Ježek and T. Kepka, *Medial groupoids*, Rozpravy ČSAV, Řada mat. a přír. věd **93/2** (1983), 93pp.
3. J. Ježek and T. Kepka, *Equational theories of medial groupoids*, Algebra Universalis **17** (1983), 174–190.

Charles University, Sokolovská 83, 186 00 Praha 8, Czech Republic