# MEMBERSHIP PROBLEMS FOR FINITE ENTROPIC GROUPOIDS 

J. JEŽEK AND M. MARÓTI

Abstract. Some abstract here.

## 1. Introduction

By a medial groupoid we mean a groupoid satisfying the equation $(x y)(u v) \approx$ $(x u)(y v)$. Entropic groupoids are homomorphic images of medial cancellation groupoids. The class of entropic groupoids is a variety. This variety has been introduced in [2]; the paper (some parts can be also found in [3],[4] and [5]) contains several equivalent definitions. The variety is not finitely based.

In [1], the following problem has been raised: Does there exist an algorithm, deciding for any finite groupoid whether it is entropic? In this paper we are going to present such an algorithm. On the other hand, we will show that there is no algorithm deciding for any finite partial groupoid whether it satisfies all the equations of entropic groupoids.

The algorithm that we are going to present is based on Theorem 2. It works as follows: Given a groupoid with $N$ elements, check if it satisfies all the basic entropic equations of depth up to $5 N^{18}$. If it does, the groupoid is entropic according to the theorem; if it does not, then of course it is not entropic. This algorithm is of no practical value: even for $N=2$, the number of equations to be considered is too big. For $N=2$, however, one can do much better: it is easy to see that a two-element groupoid is entropic if and only if it is medial, and this is easy to check. The following problem remains open: Can the membership problem for finite entropic groupoids be decided by an algorithm working in a reasonable time for groupoids with, say, at most 26 elements? Is there an algorithm, working in polynomial time?

For the terminology and basic notions of equational logic, helpful for understanding the following text, the reader is referred to [7].

In order to be able to describe the equational theory of entropic groupoids, we need to introduce the following notation. Given a term $t$ (we mean a term in the

[^0]similarity type containing just one binary operation symbol, for multiplication) and an occurrence $o$ of a variable $x$ in $t$, the weight of $o$ (in $t$ ) is the ordered pair $(a, b)$, where $a$ is the number of southwest turns and $b$ is the number of southeast turns in the path connecting the top of the term's tree with the occurrence $o$; the sum $a+b$ is called the depth of $o$. For example, the weight of the (single) occurrence of $z$ in $(x(y z))(x y)$ is $(1,2)$, and the depth is 3 . Now, an equation $t \approx u$ belongs to the equational theory of entropic groupoids if and only if for any variable $x$ and any ordered pair $\left(w_{1}, w_{2}\right)$ of nonnegative integers, the number of occurrences of $x$ of weight $\left(w_{1}, w_{2}\right)$ in $t$ is the same as the number of occurrences of $x$ of weight $\left(w_{1}, w_{2}\right)$ in $u$ (see [3]). For example, the medial law, and also the equation $(x(y z))((u v) w) \approx(x(y v))((u z) w)$ belong to the equational theory.

The paper [8] contains a construction of an infinite independent base for the equations of entropic groupoids. In this paper we will need the following consequence (which is, however, also easy to prove without relying on [8]).

By a slim term we mean a term $t$ such that whenever $u v$ is a subterm of $t$, then either $u$ or $v$ is a variable. By a linear term we mean a term containing no variable more than once. Let $t, u$ be two slim terms such that the term $t u$ is linear; let $x$ be a variable in $t$ and $y$ be a variable in $u$, such that the weights of $x$ and $y$ in $t u$ are the same, and there is no variable in $t u$ of greater depth. Denote by $t^{\prime}$ the term obtained from $t$ by replacing $x$ with $y$, and by $u^{\prime}$ the term obtained from $u$ by replacing $y$ with $x$. Equations $t u \approx t^{\prime} u^{\prime}$, obtained in this way, will be called basic entropic equations.
Lemma 1. The set of basic entropic equations is a base for the equational theory of entropic groupoids.

By the depth of a term $t$ we mean the maximum of the depths of occurrences of variables in $t$, and by the depth of an equation $t \approx u$ we mean the maximum of the depths of $t$ and $u$. The aim of the next section is to prove the following theorem, yielding the decidability of the membership problem for finite entropic groupoids.
Theorem 2. Let $G$ be a finite groupoid with $N$ elements $(N \geq 2)$. Then $G$ is entropic if and only if it satisfies all the basic entropic equations of depth at most $5 N^{18}$.

## 2. Proof of Theorem 2: shifting around

Let $G$ be a finite groupoid with $N$ elements ( $N \geq 2$ ). Let us fix two symbols $\alpha$ and $\beta$ (they can be thought of as symbols for the southwest and the southeast direction in trees of terms, respectively). For any positive integer $n$ denote by $E_{n}$ the set of finite sequences $e=\left(e_{1}, a_{1}, \ldots, e_{n-1}, a_{n-1}, e_{n}\right)$, where $e_{i} \in\{\alpha, \beta\}$ and $a_{i} \in G$. The elements of $E_{n}$ will be called paths (of length $n$ ).

For $a \in G, e=\left(e_{1}, a_{1}, \ldots, e_{n}\right) \in E_{n}$ and $i \in\{0, \ldots, n-1\}$ define an element $(a * e)_{i}$ of $G$ as follows: $(a * e)_{0}=a$; if $e_{i}=\alpha$, then $(a * e)_{i}=(a * e)_{i-1} a_{i}$; if $e_{i}=\beta$, then $(a * e)_{i}=a_{i}(a * e)_{i-1}$.

For $i \in\{0, \ldots, n\}$ put $\mathrm{w}_{e}^{\alpha}(i)=\left|\left\{j: 1 \leq j \leq i, e_{i}=\alpha\right\}\right|, \mathrm{w}_{e}^{\beta}(i)=\mid\{j: 1 \leq j \leq$ $\left.i, e_{i}=\beta\right\} \mid$ and $\mathrm{w}_{e}(i)=\left(w_{e}^{\alpha}(i), \mathrm{w}_{e}^{\beta}(i)\right)$. The ordered pair $\mathrm{w}_{e}(i)$ will be called the $e$-weight of $i$ (it would be also possible to call it the weight of the $i$-th position in the path $e$, with respect to the paths's bottom). The $e$-weight of $n$ will be called the weight of the path $e$.

Let $(a, b) \in G^{2}$ be fixed. Also, for most of the time, the positive integer $n$ will be fixed.

For $e \in E_{n}$ we define a mapping $\kappa_{e}$ of $\{0, \ldots, n-1\}$ by $\kappa_{e}(i)=\left((a * e)_{i},(b * e)_{i}\right)$.
Two paths $e=\left(e_{0}, a_{1}, \ldots, e_{n}\right)$ and $f=\left(f_{0}, b_{1}, \ldots, f_{n}\right)$ of the same length $n$ are said to be similar if $e_{n}=f_{n}, \kappa_{e}(n-1)=\kappa_{f}(n-1)$ and there is a permutation $\pi$ of $\{0, \ldots, n-1\}$ such that $f_{i}=e_{\pi(i)}$ and $b_{i}=a_{\pi(i)}$ for all $i=1, \ldots, n-1$.

For $0 \leq i<j \leq n$ put $[i, j]=\{i, i+1, \ldots, j\}$. These sets will be called segments. The number $j-i$ is called the length of $[i, j]$. (By definition, the length is always positive.) Two segments $[i, j]$ and $[k, l]$ are said to be nonoverlapping if either $j \leq k$ or $l \leq i$. By the total length of a set $S$ of pairwise nonoverlapping segments we mean the sum of the lengths of all segments in $S$. A segment $[i, j]$ is called regular if $j<n$. For a regular segment $[i, j]$, the two ordered pairs, $\kappa_{e}(i)$ and $\kappa_{e}(j)$, will be called the lower and the upper e-value of $[i, j]$, respectively; if they are the same, we say that the segment is $e$-valued and we call $\kappa_{e}(i)$ the $e$-value of $[i, j]$. A segment is called $e$-correct if it is $e$-valued and of length at most $N^{2}$ (in particular, it must be regular). Since the range of $\kappa$ has at most $N^{2}$ elements, it is easy to see that for a given $e$, every regular segment of length at least $N^{2}$ contains at least one $e$-correct subsegment. A regular segment $[i, j]$ is called $e$-correctly glued if there is a sequence $i=p_{0}<p_{1}<\cdots<p_{r}=j$ such that $\left[p_{k-1}, p_{k}\right]$ is $e$-correct for any $k=1, \ldots, r$. Of course, every $e$-correctly glued segment is $e$-valued.

By an e-assembly we will mean a set of pairwise disjoint, e-correctly glued segments with pairwise different $e$-values. (Clearly, an $e$-assembly contains at most $N^{2}$ sets.) By a gap in $C$ we mean any regular segment $[i, j]$ such that $i$ is either 0 or the last element of a segment in $C, j$ is either $n-1$ or the first element of a segment in $C$, and there is no segment in $C$ contained in $[i, j]$. Clearly, there are at most $N^{2}+1$ gaps in $C$, and the sum of the lengths of all gaps and of all segments in $C$ gives $n-1$ precisely. By a maximal e-assembly we will mean an $e$-assembly $C$ such that for any path $e^{\prime}$ similar to $e$, any $e^{\prime}$-assembly has total length less or equal to the total length of $C$.

Lemma 3. Let $e \in E_{n}$ and $C$ be a maximal e-assembly. Then the total length of $C$ is at least $n-N^{4}$.

Proof. Suppose, on the contrary, that the total length of $C$ is smaller than $n-N^{4}$. This is the same as to say that the sum of the lengths of the gaps in $C$ is at least $N^{4}$. There are at most $N^{2}+1$ gaps. If each of them were of length at most $N^{2}-1$, then the sum of their lengths would be at most $\left(N^{2}+1\right)\left(N^{2}-1\right)=N^{4}-1$, a contradiction. So, there is at least one gap of length at least $N^{2}$. But then, there is an $e$-correct segment $[u, v]$ contained in that gap.

Suppose there is no segment in $C$ having the same $e$-value as $[u, v]$. Then $C \cup\{[u, v]\}$ is an $e$-assembly of greater total length compared to that of $C$, a contradiction.

So, there is precisely one segment $[k, h] \in C$ with the same $e$-value as $[u, v]$. We have either $v \leq k$ or $h \leq u$. Let us consider the first case.

Where $e=\left(e_{1}, a_{1}, \ldots, e_{n}\right)$, let
$e^{\prime}=\left(e_{1}, a_{1}, \ldots, e_{u}, a_{u}, e_{v+1}, a_{v+1}, \ldots, e_{k}, a_{k}, e_{u+1}, a_{u+1}, \ldots, e_{v}, a_{v}, e_{k+1}, a_{k+1}, \ldots\right)$.
Let $C^{\prime}$ be the set obtained from $C$ by replacing $[k, h]$ with $[k-(v-u), h]$ and any segment $[i, j] \in C$, contained in $[v, k]$, with $[i-(v-u), j-(v-u)]$. It is easy to see that $e^{\prime}$ is similar to $e$ and $C^{\prime}$ is an $e^{\prime}$-assembly with total length larger than the total length of $C$, a contradiction.

In the second case, if $h \leq u$, the segment $[u, v]$ could be shifted to hang at the position $h$ and joined to $[k, h]$ in a similar way, yielding a contradiction as well.

Lemma 4. For every path $e \in E_{n}$ there exists a path $e^{\prime}$ similar to $e$ such that there is a set $S$ of pairwise nonoverlapping, $e^{\prime}$-correct segments of total length at least $n-N^{4}$.

Proof. It is an immediate consequence of Lemma 3.

## 3. Proof of Theorem 2 continued: Slopes

Throughout this section let a pair $(a, b) \in G^{2}$ and a path $e \in E_{n}$ be fixed. We will assume that there exists a set $S$ of pairwise nonoverlapping, $e$-correct segments of total length at least $n-N^{4}$, and we will keep $S$ fixed.

Lemma 5. Let $m$ be a positive integer and let $(i, j),(k, l)$ be two pairs of nonnegative integers such that $0<i+j \leq m, 0<k+l \leq m$ and $\frac{i}{i+j} \neq \frac{k}{k+l}$. Then $\left|\frac{i}{i+j}-\frac{k}{k+l}\right| \geq \frac{1}{m^{2}}$.

Proof. We have $\left|\frac{i}{i+j}-\frac{k}{k+l}\right|=\left|\frac{c}{\mid i+j)(k+l)}\right|$ for an integer $c$. Since the fraction is nonzero, we have $|c| \geq 1$ and hence $\left|\frac{c}{(i+j)(k+l)}\right| \geq \frac{1}{m^{2}}$.

For each segment $[i, j]$ put $\lambda_{e}[i, j]=\frac{\mathrm{W}_{e}^{\alpha}(j)-\mathrm{W}_{e}^{\alpha}(i)}{j-i}$. This is a rational number between 0 and 1 ; it will be called the e-slope (or just slope, if $e$ is clear from context) of $[i, j]$. Since

$$
\lambda_{e}[i, j]=\frac{w_{e}^{\alpha}(j)-\mathrm{w}_{e}^{\alpha}(i)}{w_{e}^{\alpha}(j)-\mathrm{w}_{e}^{\alpha}(i)+w_{e}^{\beta}(j)-\mathrm{w}_{e}^{\beta}(i)},
$$

it follows from Lemma 5 that if $\lambda_{1}$ and $\lambda_{2}$ are two different slopes of two segments of length at most $N^{2}$, then $\left|\lambda_{1}-\lambda_{2}\right| \geq \frac{1}{N^{4}}$.

Put $\Lambda_{e}=\lambda_{e}[0, n]=\frac{\mathrm{W}_{e}^{\alpha}(n)}{n}$.
A rational number $r$ will be called large (with respect to e) if $r \geq \Lambda_{e}+\frac{1}{2 N^{4}}$; it will be called small if $r \leq \Lambda_{e}-\frac{1}{2 N^{4}}$; and middle if $\left|r-\Lambda_{e}\right|<\frac{1}{2 N^{4}}$.

Lemma 6. There is at most one middle rational number $r$ with the property that there is a segment of length at most $N^{2}$ with e-slope equal to $r$.

Proof. It follows from Lemma 5 and the definitions.
If it exists, the unique middle rational number from Lemma 6 will be denoted by $\Lambda_{e}^{\prime}$. If it does not exist, we put $\Lambda_{e}^{\prime}=\Lambda_{e}$.

The set $S$ is the disjoint union $S_{-1} \cup S_{0} \cup S_{1}$, where $S_{-1}, S_{0}$ and $S_{1}$ denote the set of the segments in $S$ with small, middle and large slopes, respectively.

For $k \in\{-1,0,1\}$ put $d_{k}=\sum_{[i, j] \in S_{k}}\left(\lambda_{e}[i, j]-\Lambda_{e}\right)(j-i)$.
Lemma 7. We have

$$
\begin{equation*}
\left|d_{-1}+d_{0}+d_{1}\right| \leq N^{4}, \tag{1}
\end{equation*}
$$

$$
-\left|S_{-1}\right| N^{2} \leq d_{-1} \leq-\frac{\left|S_{-1}\right|}{2 N^{4}},
$$

(3) $\left|d_{0}\right| \leq \frac{\left|S_{0}\right|}{2 N^{2}}$,
(4) $\quad \frac{\left|S_{1}\right|}{2 N^{4}} \leq d_{1} \leq\left|S_{1}\right| N^{2}$.

Proof. For each $i=0, \ldots, n$ put $\delta_{e}(i)=\mathrm{w}_{e}^{\alpha}(i)-i \Lambda_{e}$. (This rational number could be called the distance of the $i$-th position on the branch $e$ from the line connecting the top of $e$ with its bottom.) Clearly, $\delta_{e}(0)=\delta_{e}(n)=0$.

It is easy to check that for any segment $[i, j]$ we have $\delta_{e}(j)-\delta_{e}(i)=\left(\lambda_{e}[i, j]-\right.$ $\left.\Lambda_{e}\right)(j-i)$. Denote by $S^{\prime}$ the set of all the segments of length 2 that are not contained in any segment from $S$, so that the total length of $S \cup S^{\prime}$ is precisely $n$ and the total length of $S^{\prime}$ is at most $N^{4}$. We have

$$
\begin{aligned}
0 & =\delta_{e}(n)-\delta_{e}(0)=\sum_{[i, j] \in S \cup S^{\prime}}\left(\delta_{e}(j)-\delta_{e}(i)\right)=\sum_{[i, j] \in S \cup S^{\prime}}\left(\lambda_{e}[i, j]-\Lambda_{e}\right)(j-i) \\
& =d_{-1}+d_{0}+d_{1}+\sum_{[i-1, i] \in S^{\prime}}\left(\lambda_{e}[i-1, i]\right) .
\end{aligned}
$$

The last sum is in absolute value at most $N^{4}$, so $\left|d_{-1}+d_{0}+d_{1}\right| \leq N^{4}$. We have proved (1).

In order to prove (2), (3) and (4), observe that $1 \leq j-i \leq N^{2}$ and $\mid \lambda_{e}[i, j]-$ $\Lambda_{e} \left\lvert\,<\frac{1}{2 N^{4}}\right.$ in the case (3), while $\frac{1}{2 N^{4}} \leq\left|\lambda_{e}[i, j]-\Lambda_{e}\right| \leq 1$ in cases (2) and (4).

Lemma 8. If $n>5 N^{18}$, then at least one of the following two cases takes place: either $\left|S_{0}\right| \geq 2 N^{10}$ or both $\left|S_{-1}\right| \geq N^{10}$ and $\left|S_{1}\right| \geq N^{10}$.

Proof Let $\left|S_{0}\right|<2 N^{10}$. Since the total length of $S$ is at least $n-N^{4}>5 N^{18}-N^{4}$ and each segment in $S$ is of length at most $N^{2}$, we have $\left|S_{-1}\right|+\left|S_{0}\right|+\left|S_{1}\right|=$ $|S|>\frac{5 N^{18}-N^{4}}{N^{2}}=5 N^{16}-N^{2}$. Hence $\left|S_{-1}\right|+\left|S_{1}\right|>5 N^{16}-N^{2}-2 N^{10}$. Then at least one of the two sets, either $S_{-1}$ or $S_{1}$, has more than $\frac{5 N^{16}-N^{2}-2 N^{10}}{2}$ elements. By symmetry, it is sufficient to consider the case $\left|S_{-1}\right|>\frac{5 N^{16}-N^{2}-2 N^{10}}{2}$. This number is larger than $N^{10}$, so it remains to prove that also $S_{1}{ }^{2}$ has at least $N^{10}$ elements. By Lemma 7, $\left|d_{-1}\right|>\frac{5 N^{16}-N^{2}-2 N^{10}}{4 N^{4}}$, so that $d_{1} \geq\left|d_{-1}\right|-\left|d_{0}\right|-$ $N^{4}>\frac{5 N^{16}-N^{2}-2 N^{10}}{4 N^{4}}-\frac{2 N^{10}}{2}-N^{4}$. We can again apply Lemma 7 to see that $\left|S_{1}\right| \geq \frac{d_{1}}{N^{2}}>\frac{5 N^{16}-N^{2}-2 N^{10}}{4 N^{6}}-N^{6}-N^{2}$. However, it is easy to check that this number is larger than $N^{10}$.

Lemma 9. If $n>5 N^{18}$, then there are two disjoint sets $P_{1}, P_{2}$ of pairwise nonoverlapping, e-correct segments and two ordered pairs $\left(p_{1}, q_{1}\right),\left(p_{2}, q_{2}\right)$ of nonnegative integers such that $\left|P_{1}\right| \geq N^{6},\left|P_{2}\right| \geq N^{6},\left(\mathrm{w}_{e}^{\alpha}(j)-\mathrm{w}_{e}^{\alpha}(i), \mathrm{w}_{e}^{\beta}(j)-\mathrm{w}_{e}^{\beta}(i)\right)=$ $\left(p_{1}, q_{1}\right)$ for all $[i, j] \in P_{1},\left(\mathrm{w}_{e}^{\alpha}(j)-\mathrm{w}_{e}^{\alpha}(i), \mathrm{w}_{e}^{\beta}(j)-\mathrm{w}_{e}^{\beta}(i)\right)=\left(p_{2}, q_{2}\right)$ for all $[i, j] \in P_{2}$, and $\frac{p_{1}}{p_{1}+q_{1}} \leq \Lambda_{e}^{\prime} \leq \frac{p_{2}}{p_{2}+q_{2}}$.
Proof. It follows easily from Lemma 8, since any set of $N^{10}$ segments of length at most $N^{2}$ contains necessarily a subset of $N^{6}$ segments $[i, j]$ with identical pairs $\left(\mathrm{w}_{e}^{\alpha}(j)-\mathrm{w}_{e}^{\alpha}(i), \mathrm{w}_{e}^{\beta}(j)-\mathrm{w}_{e}^{\beta}(i)\right)$. (These are ordered pairs $(r, s)$ of nonnegative integers with $0<r+s \leq N^{2}$, and one can easily see that the number of such ordered pairs is at most $N^{4}$.)

## 4. Proof of Theorem 2 completed

Lemma 10. The following two conditions are equivalent for a given quadruple of ordered pairs $\left(c_{i}, d_{i}\right) \neq(0,0)(i=1,2,3,4)$ of nonnegative integers such that $\frac{c_{1}}{c_{1}+d_{1}} \leq \frac{c_{2}}{c_{2}+d_{2}}$ and $\frac{c_{3}}{c_{3}+d_{3}} \leq \frac{c_{4}}{c_{4}+d_{4}}$ :
(1) there exists a quadruple $\left(n_{1}, n_{2}, n_{3}, n_{4}\right) \neq(0,0,0,0)$ of nonnegative integers such that $n_{1} c_{1}+n_{2} c_{2}=n_{3} c_{3}+n_{4} c_{4}$ and $n_{1} d_{1}+n_{2} d_{2}=n_{3} d_{3}+n_{4} d_{4}$;
(2) there is a rational number $r$ such that $\frac{c_{1}}{c_{1}+d_{1}} \leq r \leq \frac{c_{2}}{c_{2}+d_{2}}$ and $\frac{c_{3}}{c_{3}+d_{3}} \leq$ $r \leq \frac{c_{4}}{c_{4}+d_{4}}$.

If (2) is satisfied, then the integers $n_{1}, n_{2}, n_{3}, n_{4}$ can be always selected to be less or equal $m^{3}$, where $m$ is the maximum of the numbers $c_{i}$ and $d_{i}$.
Proof. If (1) is satisfied, we can put

$$
r=\frac{n_{1} c_{1}+n_{2} c_{2}}{n_{1} c_{1}+n_{2} c_{2}+n_{1} d_{1}+n_{2} d_{2}}=\frac{n_{3} c_{3}+n_{4} c_{4}}{n_{3} c_{3}+n_{4} c_{4}+n_{3} d_{3}+n_{4} d_{4}} .
$$

Let (2) be satisfied. If $c_{1} d_{4}=c_{4} d_{1}$, we can take either $\left(c_{4}, 0,0, c_{1}\right)$ or $\left(d_{4}, 0,0, d_{1}\right)$ for $\left(n_{1}, n_{2}, n_{3}, n_{4}\right)$; at least one of the two quadruples is different from $(0,0,0,0)$. Similarly, if $c_{2} d_{3}=c_{3} d_{2}$, we can take either $\left(0, c_{3}, c_{2}, 0\right)$ or $\left(0, d_{3}, d_{2}, 0\right)$. If $c_{1}=$ $c_{2}=c_{3}=c_{4}$, we can take $\left(n_{1}, n_{2}, n_{3}, n_{4}\right)=\left(d_{3}, d_{4}, d_{1}, d_{2}\right)$. In all other cases we can take $n_{1}=c_{4}\left(c_{2} d_{3}-c_{3} d_{2}\right), n_{2}=c_{3}\left(c_{4} d_{1}-c_{1} d_{4}\right), n_{3}=c_{2}\left(c_{4} d_{1}-c_{1} d_{4}\right)$, $n_{4}=c_{1}\left(c_{2} d_{3}-c_{3} d_{2}\right)$; it follows from (2) that these numbers are nonnegative.

In order to prove Theorem 2, it is obviously sufficient to show that for any positive integer $n$, any $(a, b) \in G^{2}$ and any $e, f \in E_{n}$ with the same weights and such that $e_{n}=\alpha$ and $f_{n}=\beta$,

$$
(a * e)_{n-1}(b * f)_{n-1}=(b * e)_{n-1}(a * f)_{n-1} .
$$

Suppose that this is not true and let $n$ be the least positive integer for which there exist $(a, b) \in G^{2}$ and $e, f \in E_{n}$ giving a contradiction. According to the assumption, $n>5 N^{18}$.

By Lemma 4, there exist paths $e^{\prime}$ and $f^{\prime}$ similar to $e$ and $f$ respectively, such that there are a set $S$ of pairwise nonoverlapping, $e^{\prime}$-correct segments and a set $T$ of pairwise nonoverlapping, $f^{\prime}$-correct segments, both $S$ and $T$ of total length at least $n-N^{4}$.

We have $e_{n}=e_{n}^{\prime}=\alpha$ and $f_{n}=f_{n}^{\prime}=\beta$. Since $\mathrm{w}_{e}(n)=\mathrm{w}_{f}(n)=w_{e^{\prime}}(n)=$ $\mathrm{w}_{f^{\prime}}(n)$, we have $\Lambda_{e}=\Lambda_{f}=\Lambda_{e^{\prime}}=\Lambda_{f^{\prime}}$, the four sets of middle rational numbers are the same for all these four paths, and also $\Lambda_{e}^{\prime}=\Lambda_{f}^{\prime}=\Lambda_{e^{\prime}}^{\prime}=\Lambda_{f^{\prime}}^{\prime}$; let us denote this number by $\Lambda$.

Now Lemma 9, applied to the path $e^{\prime}$, produces two sets $P_{1}, P_{2}$ of cardinalities at least $N^{6}$ and two ordered pairs $\left(p_{1}, q_{1}\right),\left(p_{2}, q_{2}\right)$; and applied to $f^{\prime}$, it similarly produces two sets $P_{3}, P_{4}$ and two ordered pairs $\left(p_{3}, q_{3}\right),\left(p_{4}, q_{4}\right)$. We have $0<$ $p_{i}+q_{i} \leq N^{2}(i=1,2,3,4)$ and we have both $\frac{p_{1}}{p_{1}+q_{1}} \leq \Lambda \leq \frac{p_{2}}{p_{2}+q_{2}}$ and $\frac{p_{3}}{p_{3}+q_{3}} \leq$ $\Lambda \leq \frac{p_{4}}{p_{4}+q_{4}}$. It follows by Lemma 10 that there is a quadruple $\left(n_{1}, n_{2}, n_{3}, n_{4}\right) \neq$ $(0,0,0,0)$ of nonnegative integers such that $n_{1} p_{1}+n_{2} p_{2}=n_{3} p_{3}+n_{4} p_{4}, n_{1} q_{1}+$ $n_{2} q_{2}=n_{3} q_{3}+n_{4} q_{4}$ and $n_{i} \leq N^{6}(i=1,2,3,4)$. Take $n_{1}$ segments $\left[r_{i}, s_{i}\right]$ in $P_{1}$ $\left(i=1, \ldots, n_{1}\right)$ and $n_{2}$ segments $\left[r_{i}, s_{i}\right]$ in $P_{2}\left(i=n_{1}+1, \ldots, n_{1}+n_{2}\right)$ and denote by $e^{\prime \prime}$ the path obtained from $e^{\prime}$ by deleting all the members with indexes in one of the sets $\left\{r_{i+1}, \ldots, s_{i}\right\}\left(i=1, \ldots, n_{1}+n_{2}\right)$. This new path is of a length $m<n$, and its weight is $w_{e}(n)-\left(n_{1} p_{1}+n_{2} p_{2}, n_{1} q_{1}+n_{2} q_{2}\right)$. We can similarly obtain a path $f^{\prime \prime}$ from $f^{\prime}$; its weight is $w_{f}(n)-\left(n_{3} p_{3}+n_{4} p_{4}, n_{3} q_{3}+n_{4} q_{4}\right)$, and
we see that $e^{\prime \prime}$ and $f^{\prime \prime}$ are of the same weight. (In particular, $f^{\prime \prime}$ is of the same length $m<n$ as $e^{\prime \prime}$.) By the minimality of $n,\left(a * e^{\prime \prime}\right)_{m-1}\left(b * f^{\prime \prime}\right)_{m-1}=$ $\left(b * e^{\prime \prime}\right)_{m-1}\left(a * f^{\prime \prime}\right)_{m-1}$. Since all the segments that have been 'squeezed to one point' during this process were correct (with respect to the appropriate paths), we have $(a * e)_{n-1}=\left(a * e^{\prime}\right)_{n-1}=\left(a * e^{\prime \prime}\right)_{m-1},(b * e)_{n-1}=\left(b * e^{\prime}\right)_{n-1}=\left(b * e^{\prime \prime}\right)_{m-1}$, $(a * f)_{n-1}=\left(a * f^{\prime}\right)_{n-1}=\left(a * f^{\prime \prime}\right)_{m-1}$ and $(b * f)_{n-1}=\left(b * f^{\prime}\right)_{n-1}=\left(b * f^{\prime \prime}\right)_{m-1}$. It follows that $(a * e)_{n-1}(b * f)_{n-1}=(b * e)_{n-1}(a * f)_{n-1}$.

This completes the proof of Theorem 2.

## References

[1] J. Ježek, A decidable equational theory with undecidable membership problem for finite algebras. (To appear in Algebra Universalis.)
[2] J. Ježek and T. Kepka, Medial groupoids. Rozpravy ČSAV, Řada mat. a přír. věd 93/2 (1983), 93 pp.
[3] J. Ježek and T. Kepka, Equational theories of medial groupoids. Algebra Universalis 17 (1983), 174-190.
[4] J. Ježek and T. Kepka, Free entropic groupoids. Commentationes Math. Univ. Carolinae 22 (1981), 223-233.
[5] J. Ježek and T. Kepka, Semigroup representations of medial groupoids. Commentationes Math. Univ. Carolinae 22 (1981), 513-524.
[6] J. Ježek and T. Kepka, Medial division groupoids. Proceedings of the American Mathematical Society 119 (1993), 423-426.
[7] R. McKenzie, G. McNulty and W. Taylor, Algebras, Lattices, Varieties, Volume I. Wadsworth \& Brooks/Cole, Monterey, CA, 1987.
[8] G. Pollák and Á. Szendrei, Independent basis for the identities of entropic groupoids. Commentationes Math. Univ. Carolinae 22 (1981), 71-85.

Vanderbilt University, Nashville, TN 37240


[^0]:    1991 Mathematics Subject Classification. 20N02, 68W05, 68Q05, 03D35, 03D10.
    While working on this paper the authors were partially supported by the NSF grant No. DMS-9596043 and by the GAČR grant No. 201/96/0312.

