MULTIPLICATION GROUPS OF FREE LOOPS I

Aleš Drápal, Praha

(Received December 6, 1993)

A quasigroup is often defined as an algebra having a binary multiplication $a \cdot b$, which satisfies the condition that for any a, b the equations $a \cdot x = b$ and $y \cdot a = b$ have unique solutions x and y. However, it is well known that the variety generated by such algebras does not consist entirely of quasigroups. To remedy this inconvenience, quasigroups are also defined as algebras with three binary operations that satisfy certain identities. We will use such a definition throughout this paper.

A *quasigroup* is an algebra $Q = Q(\cdot, \backslash, /)$ of type $(2,2,2)$ such that the following identities hold:

$$a \cdot (a\backslash b) = b;\ (a/b) \cdot b = a;\ a\backslash(a \cdot b) = b;\ (a \cdot b)/b = a.$$

From these four identities other two identities can be easily derived:

$$b/(a\backslash b) = a, \quad \text{and} \quad (b/a)\backslash b = a.$$

A *loop* is a quasigroup possessing a nullary operation 1 such that

$$a \cdot 1 = a \text{ and } 1 \cdot a = a.$$

From this we immediately obtain the identities

$$a/a = 1 \text{ and } 1 = a\backslash a.$$

With each element a of a quasigroup Q we associate two permutations of Q, namely the *left translation* $L_a\colon x \to a \cdot x$ and the *right translation* $R_a\colon x \to x \cdot a$. The permutation group $\langle L_a, R_a\,;\, a \in Q\rangle$ is called the (combinatorial) *multiplication group* of $Q(\cdot)$. Its subgroups $\langle L_a\,;\, a \in Q\rangle$ and $\langle R_a\,;\, a \in Q\rangle$ are called the left and the right multiplication group, respectively. The multiplication groups will be denoted $\mathrm{Mlt}(Q)$, $\mathrm{LMlt}(Q)$ and $\mathrm{RMlt}(Q)$, respectively.

As multiplication groups of loops are currently being studied from the viewpoint both of the universal algebra and the group theory [4–8], it appears quite natural to investigate more closely the multiplication group of a free loop.

Even though the classical paper of Evans [2] made the word structure of the free loop transparent, to establish some of the properties of its multiplication group still seems to require quite a number of technical results.

Here we prove that the left multiplication group of a free loop is always a Frobenius group (*i.e.* it is not regular and every non-identical permutation fixes at most one element). This contrasts with the fact that no Frobenius group can be obtained as a (both-sided) multiplication group of a loop [1]. For apparent reasons, the left multiplication group of a finite loop is never a Frobenius group, either.

1. Normal form of a loop word

If X is a set, then the *loop words* over X are recursively defined by

(i) each element in $X \cup \{1\}$ is a loop word;
(ii) if u, v are loop words, then so are $u \cdot v$, u/v and $u\backslash v$.

We shall fix a non-empty set X, $1 \notin X$ for the rest of this paper and we shall also fix a free loop with the basis X. This loop will be denoted by W. Each of its elements can be expressed in many ways as a loop word over X, but only in one way as a reduced word over X.

A loop word w is said to be *reduced* (or in a normal form) iff it contains no subwords u_1, u_2, v for which one of the following possibilities applies: $v = u_1 \cdot (u_1 \backslash u_2)$, $v = (u_1/u_2) \cdot u_2$, $v = u_1 \backslash (u_1 \cdot u_2)$, $v = (u_1 \cdot u_2)/u_2$, $v = u_1/(u_2 \backslash u_1)$, $v = (u_1/u_2) \backslash u_1$, $v = u_1 \cdot 1$, $v = 1 \cdot u_1$, $v = u_1/1$, $v = 1 \backslash u_1$, $v = u_1/u_1$ and $v = u_1 \backslash u_1$.

Thus the elements of W can be identified with the reduced loop words [2]. However, for formal reasons we shall not do that explicitly, and for any $a \in W$ we shall denote the unique reduced loop word over X corresponding to a by $\varrho_X(a)$. For $a, b, c \in W$ we say that $c = a \cdot b$ ($c = a/b$, $c = a\backslash b$) *reduced* iff $\varrho_X(c) = \varrho_X(a) \cdot \varrho_X(b)$ (or $\varrho_X(c) = \varrho_X(a)/\varrho_X(b)$, or $\varrho_X(c) = \varrho_X(a)\backslash\varrho_X(b)$). We shall often deal with situations when an element of W is composed in a reduced way from more than two subwords. To express such knowledge effectively, we introduce the following notational shortcut: $c = a \circ b$ (or $c = a /\!/ b$, or $c = a \backslash\!\backslash b$) means that $c = a \cdot b$ reduced (or $c = a/b$ reduced, or $c = a\backslash b$ reduced). For example, writing $d = (a /\!/ b) \circ c$ means that there exists $a' \in W$ with $a' = a/b$ reduced and $d = a' \cdot c$ reduced.

For $a \in W$ we define recursively its norm $|a|$.

(i) $|1| = 0$ and $|x| = 1$ for every $x \in X$.

(ii) If $a = b \circ c$ (or $a = b /\!\!/ c$, or $a = b \backslash\!\!\backslash c$), then $|a| = |b| + |c|$.

The norm $|a|$ is clearly equal to the number of symbols distinct from 1 that appear in the reduced loop word $\varrho_X(a)$. Note that $|a\backslash 1| = |1/a| = |a|$ for every $a \in W$, but $a\backslash 1 \neq a \neq 1/a$. As $1 \cdot 1 = 1/1 = 1\backslash 1 = 1$, we have $|a| = 0$ iff $a = 1$.

1.1 Lemma. *Let $a, c, e \in W$ be such that $c = L_e(a)$, $e \neq 1 \neq a$. Then exactly one of the following possibilities takes place.*

(i) *$c = e \circ a$ and $|c| = |e| + |a|$,*

(ii) *$a = e \backslash\!\!\backslash c$ and $|c| = |a| - |e|$,*

(iii) *$e = c /\!\!/ a$ and $|c| = |e| - |a|$.*

Proof. If $e \cdot a$ is not reduced, then either $a = e \backslash\!\!\backslash c$ or $e = c /\!\!/ a$. □

Similarly we have

1.2 Lemma. *Let $a, c, e \in W$ be such that $c = L_e^{-1}(a)$, $a \neq e \neq 1$. Then exactly one of the following possibilities takes place.*

(i) *$c = e \backslash\!\!\backslash a$ and $|c| = |e| + |a|$,*

(ii) *$a = e \circ c$ and $|c| = |a| - |e|$,*

(iii) *$e = a /\!\!/ c$ and $|c| = |e| - |a|$.*

1.3 Lemma. *Let $a_j, e_i \in W$, $0 \leqslant j \leqslant 2$, $1 \leqslant i \leqslant 2$ be such that $1 \neq e_i$, $|a_0| > |e_2|$ and $a_i = \varphi_i(a_{i-1})$ for $\varphi_i \in \{L_{e_i}, L_{e_i}^{-1}, R_{e_i}, R_{e_i}^{-1}\}$. If $\varphi_1 \neq \varphi_2^{-1}$ and $|a_1| = |e_1| + |a_0|$, then $|a_2| = |e_2| + |a_1|$.*

Proof. Let $\varphi_2 = L_{e_2}$, then $e_2 \neq a_2 /\!\!/ a_1$ by $|a_1| > |a_0| > |e_2|$. Furthermore, $a_1 = e_2 \backslash\!\!\backslash a_2$ would mean $e_2 = e_1$, $a_2 = a_0$ and $\varphi_1 = L_{e_2}^{-1} = \varphi_2^{-1}$. Therefore 1.1 implies $a_2 = e_2 \circ a_1$ and $|a_2| = |e_2| + |a_1|$. If $\varphi_2 = L_{e_2}^{-1}$, then $e_2 \neq a_1 /\!\!/ a_2$ and $a_1 = e_2 \circ a_2$ implies $a_0 = e_2$ or $a_0 = a_2$. But $a_0 = e_2$ is not possible, and hence $a_1 = e_2 \circ a_2$ provides $a_0 = a_2$, $e_1 = e_2$ and $\varphi_1 = L_{e_2} = \varphi_2^{-1}$. By 1.2 $a_2 = e_2 \backslash\!\!\backslash a_1$, and thus $|a_2| = |e_2| + |a_1|$. The cases $\varphi_2 = R_{e_2}$ and $\varphi_2 = R_{e_2}^{-1}$ are similar. □

1.4 Lemma. *Let $\varphi_i \in \{L_{e_i}, L_{e_i}^{-1}, R_{e_i}, R_{e_i}^{-1}\}$, $1 \neq e_i \in W$ for $1 \leqslant i \leqslant k$. Suppose that $\varphi_i \neq \varphi_{i+1}^{-1}$ for all $1 \leqslant i \leqslant k-1$. Then there exists $a_0 \in W$ with $|\varphi_k \ldots \varphi_1(a_0)| = |a_0| + \sum_{1 \leqslant i \leqslant k} |e_i|$.*

Proof. Let $m = \max\{|e_i|\,;\, 1 \leqslant i \leqslant k\}$ and choose $v_1 = x \in X$. Put $v_{j+1} = v_j \circ x$, $a_{-1} = e_0 = v_{m+1}$, $\varphi_0 = L_{e_0}$ and $a_0 = \varphi_0(a_{-1})$. Then $\varphi_0 \neq \varphi_1^{-1}$, $|a_{-1}| > m$

and $|a_0| = |e_0| + |a_{-1}|$. Let $a_i = \varphi_i \dots \varphi_1(a_0) = \varphi_i(a_{i-1})$ for all $1 \leqslant i \leqslant k$. We prove by induction that $|a_i| = |e_i| + |a_{i-1}|$ and $|a_{i-1}| > m$. This is true for $i = 0$ and the induction step is contained in 1.3. Thus $|a_k| = |e_k| + \dots + |e_1| + |a_0|$. □

1.5 Corollary. *Let W be a free loop with a basis X. Then*

(i) $\mathrm{Mlt}(W)$ *is a free group with a basis* $\{L_a, R_a\,;\, 1 \neq a \in W\}$.
(ii) $\mathrm{LMlt}(W)$ *is a free group with a basis* $\{L_a\,;\, 1 \neq a \in W\}$.
(iii) $\mathrm{RMlt}(W)$ *is a free group with a basis* $\{R_a\,;\, 1 \neq a \in W\}$.

2. Sum of norms

The aim of this paper is to prove that the group $\mathrm{LMlt}(W)$ is a Frobenius group, *i.e.* whenever $\mathrm{id}_W \neq \varphi \in \mathrm{LMlt}(W)$, then $\varphi(a) = a$ for at most one $a \in W$. We shall proceed from the contrary, and assume that there are $1 \neq \psi \in \mathrm{LMlt}(W)$ and $a, b \in W$ such that $a \neq b$, $\psi(a) = a$, $\psi(b) = b$.

Suppose that $\psi = \varphi_k \dots \varphi_1$, $\varphi_i = L_{e_i}^{\pm 1}$, $1 \neq e_i \in W$, $\varphi_i \neq \varphi_{i+1}^{-1}$ for $1 \leqslant i \leqslant k-1$, and put $a_0 = a$, $b_0 = b$, $a_i = \varphi_i(a_{i-1})$, $b_i = \varphi_i(b_{i-1})$ for $1 \leqslant i \leqslant k$. We shall prove (Lemma 3.7 and Lemma 4.5) that $|a_1| + |b_1| > |a_0| + |b_0|$ yields $|a_i| + |b_i| \geqslant |a_{i-1}| + |b_{i-1}|$ for any $1 \leqslant i \leqslant k$. Once this is known, $\varphi_1 \neq \varphi_k^{-1}$ together with $a = \psi(a)$, $b = \psi(b)$ imply $|a_i| + |b_i| = |a| + |b|$ for all $1 \leqslant i \leqslant k$. However, further investigations show that then $a = b$ (Lemma 3.8 and Lemma 4.6).

We start by describing how the sum $|a| + |b|$ changes when $\varphi = L_e^{\pm 1}$, $e \in W$ is applied both to a and b. (By $\varphi = L_e^{\pm 1}$ we mean that either $\varphi = L_e$, or $\varphi = L_e^{-1}$.)

2.1 Lemma. *Let $a, b, c, d, e \in W$ be such that $c = L_e(a)$, $d = L_e(b)$, $a \neq b$, and $e \neq 1$. Then exactly one of the following possibilities takes place.*

(a) $|c| + |d| > |a| + |b|$. *Then either*

(1) $c = e \circ a$, $d = e \circ b$ *or* $c = e$, $a = 1$, $d = e \circ b$ *or* $c = e \circ a$, $b = 1$, $e = d$, *or*
(2) $e = d /\!\!/ b$, $1 \neq d$, *and* $c = e \circ a$ *or* $c = e$, $a = 1$, *or*
(3) $e = c /\!\!/ a$, $1 \neq c$, *and* $d = e \circ b$ *or* $d = e$, $b = 1$.

(b) $|c| + |d| = |a| + |b|$. *Then either*

(1) $b = e \backslash\!\!\backslash d$, *and* $c = e \circ a$ *or* $c = e$, $a = 1$, *or*
(2) $a = e \backslash\!\!\backslash c$, *and* $d = e \circ b$ *or* $d = e$, $b = 1$, *or*
(3) $d = 1$, $e = 1 /\!\!/ b$, *and* $c = e \circ a$ *or* $c = e$, $a = 1$, *or*
(4) $c = 1$, $e = 1 /\!\!/ a$, *and* $d = e \circ b$ *or* $d = e$, $b = 1$.

(c) $|c| + |d| < |a| + |b|$. *Then either*

(1) $a = e \backslash\!\!\backslash c$ *and* $b = e \backslash\!\!\backslash d$, *or*

(2) $e = d/\!/b$ *and* $a = e\backslash\!\backslash c$, *or*
(3) $e = c/\!/a$ *and* $b = e\backslash\!\backslash d$.

Proof. Consider the following table, in which each row (column) describes possible relations of e, d and b (e, c and a). As these descriptions are exhaustive and mutually exclusive, any choice of $a \neq b$, $c \neq d$, $e \neq 1$ corresponds to exactly one cell of the table. Using 1.1 we compute the sum $|c| + |d|$ in terms of $|a|$, $|b|$ and $|e|$, and write it into the cell. By writing $\emptyset$ into the cell we indicate that such situation cannot arise ($a = b$ would hold in such a case).

	$c = e \circ a$ or $a = 1$, $e = c$	$a = e\backslash\!\backslash c$	$e = c/\!/a$, $c \neq 1$	$e = 1/\!/a$, $c = 1$
$d = e \circ b$ or $b = 1$, $e = d$	$2\|e\| + \|a\| + \|b\|$	$\|a\| + \|b\|$	$2\|e\| + \|b\| - \|a\|$	$\|a\| + \|b\|$
$b = e\backslash\!\backslash d$	$\|a\| + \|b\|$	$\|a\| + \|b\| - 2\|e\|$	$\|b\| - \|a\|$	$\|b\| - \|a\|$
$e = d/\!/b$, $d \neq 1$	$2\|e\| + \|a\| - \|b\|$	$\|a\| - \|b\|$	$\emptyset$	$\emptyset$
$e = 1/\!/b$, $d = 1$	$\|a\| + \|b\|$	$\|a\| - \|b\|$	$\emptyset$	$\emptyset$

□

2.2 Lemma. *Let* $a, b, c, d, e \in W$ *be such that* $c = L_e^{-1}(a)$, $d = L_e^{-1}(b)$, $a \neq b$, *and* $e \neq 1$. *Then exactly one of the following possibilities takes place.*

(a) $|c| + |d| > |a| + |b|$. *Then either*

(1) $c = e\backslash\!\backslash a$ *and* $d = e\backslash\!\backslash b$, *or*
(2) $e = b/\!/d$ *and* $c = e\backslash\!\backslash a$, *or*
(3) $e = a/\!/c$ *and* $d = e\backslash\!\backslash b$.

(b) $|c| + |d| = |a| + |b|$. *Then either*

(1) $d = e\backslash\!\backslash b$, *and* $a = e \circ c$ *or* $a = e$, $c = 1$, *or*
(2) $c = e\backslash\!\backslash a$, *and* $b = e \circ d$ *or* $b = e$, $d = 1$, *or*
(3) $b = 1$, $e = 1/\!/d$, *and* $a = e \circ c$ *or* $a = e$, $c = 1$, *or*
(4) $a = 1$, $e = 1/\!/c$, *and* $b = e \circ d$ *or* $b = e$, $d = 1$.

(c) $|c| + |d| < |a| + |b|$. *Then either*

(1) $a = e \circ c$, $b = e \circ d$ *or* $a = e$, $c = 1$, $b = e \circ d$ *or* $a = e \circ c$, $d = 1$, $b = e$, *or*
(2) $e = b/\!/d$, $1 \neq b$, *and* $a = e \circ c$ *or* $a = e$, $c = 1$, *or*
(3) $e = a/\!/c$, $1 \neq a$, *and* $b = e \circ d$ *or* $b = e$, $d = 1$.

Proof. We have $a = L_e(c)$ and $d = L_e(b)$, and the lemma thus follows from 2.1. □

2.3 Lemma. *Let $a_i, b_i, e, f \in W$, $a_i \neq b_i$, $0 \leqslant i \leqslant 2$ be such that for $\varphi_1 = L_e^{\pm 1}$, $\varphi_2 = L_f^{\pm 1}$, $e \neq 1 \neq f$ we have $a_j = \varphi_j(a_{j-1})$, $b_j = \varphi_j(b_{j-1})$, $j = 1, 2$. If $|b_2| + |a_2| < |b_1| + |a_1| > |b_0| + |a_0|$, then $\varphi_2 = \varphi_1^{-1}$.*

Proof. We start with the case $\varphi_1 = L_e$, $a_0 \neq 1 \neq b_0$. By 2.1(a) we can assume that $b_1 = e \circ b_0$. Let first $\varphi_2 = L_f$. As $b_1 \neq f \backslash\!\backslash b_2$, 2.1(c2) applies, and we have $f = b_2 /\!/ b_1$ and $a_1 = f \backslash\!\backslash a_2$. Thus $a_1 \neq e \circ a_0$, and from 2.1(a) we obtain $e = a_1 /\!/ a_0$. Then $b_1 = e \circ b_0 = (a_1 /\!/ a_0) \circ b_0 = ((f \backslash\!\backslash a_2) /\!/ a_0) \circ b_0 = (((b_2 /\!/ b_1) \backslash\!\backslash a_2) /\!/ a_0) \circ b_0$, which cannot be true. Let now $\varphi_2 = L_f^{-1}$, $f \neq e$. We have $b_1 \neq f \circ b_2$, and if $f = b_1$, then $f \neq a_1 /\!/ a_2$. Thus 2.2(c3) does not apply and either $b_2 = 1$, $b_1 = f$, $a_1 = f \circ a_2$, or $f = b_1 /\!/ b_2$. Moreover, in the latter case either $a_1 = f \circ a_2$, or $a_2 = 1$, $a_1 = f$. Assume for a while that $a_1 = e \circ a_0$. Then $e \neq f$ yields $a_1 = f = b_1 /\!/ b_2$, $a_2 = 1$, and thus $e \circ a_0 = a_1 = b_1 /\!/ b_2$, a contradiction. From $a_1 \neq e \circ a_0$, $a_0 \neq 1 \neq b_0$ it follows by 2.1(a) that $e = a_1 /\!/ a_0$. If $b_1 = f$, then $a_1 = f \circ a_2 = (e \circ b_0) \circ a_2 = ((a_1 /\!/ a_0) \circ b_0) \circ a_2$. If $f = b_1 /\!/ b_2$, then $f = (e \circ b_0) /\!/ b_2 = ((a_1 /\!/ a_0) \circ b_0) /\!/ b_2$, and as $a_1 = f \circ a_2$ or $a_1 = f$, we get a contradiction in any case.

To complete the case $\varphi_1 = L_e$, assume now $b_0 = 1 \neq a_0$, $b_1 = e$. By 2.1(a) then either $a_1 = e \circ a_0 = b_1 \circ a_0$, or $e = b_1 = a_1 /\!/ a_0$. Consider first the subcase $\varphi_2 = L_f$. By 2.1(c), $a_1 = f \backslash\!\backslash a_2$ or $e = b_1 = f \backslash\!\backslash b_2$. If $a_1 = e \circ a_0$, then $b_1 = e = f \backslash\!\backslash b_2$, and $f = a_2 /\!/ a_1$ by 2.1(c). Therefore $a_1 = (f \backslash\!\backslash b_2) \circ a_0 = ((a_2 /\!/ a_1) \backslash\!\backslash b_2) \circ a_0$. If $e = b_1 = a_1 /\!/ a_0$, then $a_1 = f \backslash\!\backslash a_2$, $f = b_2 /\!/ b_1$, and we have $a_1 = (b_2 /\!/ b_1) \backslash\!\backslash a_2 = (b_2 /\!/ (a_1 \backslash\!\backslash a_0)) \backslash\!\backslash a_2$. Thus we always get a contradiction, and we can proceed to the subcase $\varphi_2 = L_f^{-1}$, $e \neq f$. By 2.2(c) $e = b_1 = f \circ b_2$ or $a_1 = f \circ a_2$ or $a_1 = f$. If $a_1 = f$, then by 2.2(c) $a_2 = 1$ and either $b_1 = a_1 \circ b_2$, or $a_1 = b_1 /\!/ b_2$. However, none of the both alternatives is compatible with $a_1 = b_1 \circ a_0$ or $b_1 = a_1 /\!/ a_0$, and thus $a_1 \neq f$. If $e = b_1 = f \circ b_2$, then $a_1 = e \circ a_0$, and $e \neq f$ implies $a_1 \neq f \circ a_2$. 2.2(c) then yields $f = a_1 /\!/ a_2$, and we have $a_1 = (f \circ b_2) \circ a_0 = ((a_1 /\!/ a_2) \circ b_2) \circ a_0$. If $a_1 = f \circ a_2$, then $b_1 = a_1 /\!/ a_0$ by $e \neq f$, and $f = b_1 /\!/ b_2$ by 2.2(c). Therefore $a_1 = f \circ a_2 = (b_1 /\!/ b_2) \circ a_2 = ((a_1 /\!/ a_0) /\!/ b_2) \circ a_2$, a contradiction again.

It remains to treat the case $\varphi_1 = L_e^{-1}$. As $a_0 = \varphi_1^{-1}(\varphi_2^{-1}(a_2))$ and $b_0 = \varphi_1^{-1}(\varphi_2^{-1}(b_2))$, we can restrict ourselves to the subcase $\varphi_2 = L_f$, $f \neq e$. With respect to 2.2(a) we can assume that $b_1 = e \backslash\!\backslash b_0$. By 2.1(c), $a_1 = f \backslash\!\backslash a_2$ or $b_1 = f \backslash\!\backslash b_2$. However, the latter cannot be true, and hence $f = b_2 /\!/ b_1$ by 2.1(c) again. From $a_1 = f \backslash\!\backslash a_2$ it follows that $a_1 \neq e \backslash\!\backslash a_0$, and thus $e = a_1 /\!/ a_2$ by 2.2(a). Therefore $a_1 = f \backslash\!\backslash a_2 = (b_2 /\!/ b_1) \backslash\!\backslash a_2 = (b_2 /\!/ (e \backslash\!\backslash b_0)) \backslash\!\backslash a_2 = (b_2 \backslash\!\backslash ((a_1 /\!/ a_2) \backslash\!\backslash b_0)) \backslash\!\backslash a_2$. □

3.1 Lemma. *Let $a, c, d, e \in W$ be such that $e \neq 1 \neq a$ and $c = \varphi(a)$, $d = \varphi(1)$ for $\varphi = L_e^{\pm 1}$. If $|c| + |d| \leqslant |a| = |a| + |1|$, then the equality holds, and exactly one of the following cases applies.*

(i) $e = d$, $\varphi = L_e$ and $a = e \backslash\backslash c$,

(ii) $e = d = 1 /\!/ a$, $\varphi = L_e$ and $c = 1$,

(iii) $d = e \backslash\backslash 1$, $\varphi = L_e^{-1}$, and $a = e \circ c$ or $a = e$, $c = 1$,

(iv) $e = 1 /\!/ d$, $\varphi = L_e^{-1}$, and $a = e \circ c$ or $a = e$, $c = 1$.

Proof. Examination of 2.1 and 2.2 shows that $|c| + |d| < |a| + |b|$ is not possible for $b = 1$. We get the result by considering the alternatives of 2.1(b) and 2.2(b). □

3.2 Lemma. *Let $a_i, b_i, e, f \in W$, $a_i \neq b_i$, $0 \leqslant i \leqslant 2$ be such that for $\varphi_1 = L_e^{\pm 1}$, $\varphi_2 = L_f^{\pm 1}$, $e \neq 1 \neq f$, $\varphi_1 \neq \varphi_2^{-1}$ we have $a_j = \varphi_j(a_{j-1})$, $b_j = \varphi_j(b_{j-1})$, $j = 1, 2$. If $b_1 = 1$ and $|a_2| + |b_2| \leqslant |a_1| + |b_1| \geqslant |a_0| + |b_0|$, then $|a_2| + |b_2| = |a_1| + |b_1| = |a_0| + |b_0|$ and $1 \in \{a_0, a_2\}$.*

Proof. The equalities $|a_2| + |b_2| = |a_1| + |b_1| = |a_0| + |b_0|$ come from 3.1 immediately. Assume $1 \notin \{a_0, a_2\}$ and let $\varphi_2 = L_f$. Then $a_1 = f \backslash\backslash a_2$ by 3.1 and $\varphi_1^{-1} = L_e$ is excluded by $e \neq f$ and 3.1. If $\varphi_1^{-1} = L_e^{-1}$, then $a_1 = e \circ a_0$ by 3.1, which contradicts $a_1 = f \backslash\backslash a_2$. For $\varphi_2 = L_f^{-1}$ we need to consider only the case $\varphi_1^{-1} = L_e^{-1}$. However, $a_1 = f \circ a_2$ and $a_1 = e \circ a_0$ imply $\varphi_1 = \varphi_2^{-1}$. □

3.3 Lemma. *Let $a, d, e \in W$ be such that $e \neq 1$ and $\varphi(a) = 1$, $\varphi(1) = d$ for $\varphi = L_e$. Then $e = d$ and either $a = d \backslash\backslash 1$ or $d = 1 /\!/ a$.*

Proof. This is a special case of 3.1 for $c = 1$. □

3.4 Lemma. *Let $a_i, b_i \in W$, $a_i \neq b_i$, $0 \leqslant i \leqslant k$ be such that $k \geqslant 2$, $b_0 = a_1 = 1$, and for $1 \leqslant i \leqslant k$ let $|a_i| + |b_i| = |a_0| + |b_0| = |a_0|$, $\varphi_i(a_{i-1}) = a_i$, $\varphi_i(b_{i-1}) = b_i$, $\varphi_i = L_{e_i}^{\pm 1}$ with $1 \neq e_i \in W$. Further, let $\varphi_{i+1}^{-1} \neq \varphi_i$ for each $1 \leqslant i \leqslant k-1$. If $e_1 = b_1 = 1 /\!/ a_0$ and $\varphi_1 = L_{e_1}$, then $\varphi_i = L_{e_i}$ for all $1 \leqslant i \leqslant k$, and*

(i) *$e_i = b_i = 1 /\!/ a_{i-1}$, $a_i = 1$ for i odd,*

(ii) *$e_i = a_i = 1 /\!/ b_{i-1}$, $b_i = 1$ for i even.*

Moreover, $(a_i, b_i) \neq (a_j, b_j)$ whenever $0 \leqslant i < j \leqslant k$.

Proof. We shall employ induction over i. For $i = 1$ the assertion follows from the hypothesis. Because of symmetry, we can assume that $k - 1 \geqslant i \geqslant 1$ is odd. Then $e_i = b_i = 1 /\!/ a_{i-1}$, $a_i = 1$, and by 3.1 $\varphi_{i+1} = L_{e_{i+1}}^{-1}$ implies $e_{i+1} = b_i$. This cannot be true, and hence $\varphi_{i+1} = L_{e_{i+1}}$. As $b_i \neq e_{i+1}\backslash\backslash b_{i+1}$, we have again by 3.1 $e_{i+1} = 1/\!/b_i$, $b_{i+1} = 1$.

Further, denote by d_i, $0 \leqslant i \leqslant k$, the total number of occurencies of 1 in the reduced loop words $\varrho_X(a_i)$ and $\varrho_X(b_i)$. Clearly, $d_{i+1} = d_i + 1$ for $0 \leqslant i \leqslant k-1$, and hence $(a_i, b_i) \neq (a_j, b_j)$ for $0 \leqslant i < j \leqslant k$. □

3.5 Lemma. *Let $a_i, b_i \in W$, $a_i \neq b_i$, $0 \leqslant i \leqslant k$ be such that $k \geqslant 2$, $b_0 = a_1 = 1$, and for $1 \leqslant i \leqslant k$ let $|a_i| + |b_i| = |a_0| + |b_0| = |a_0|$, $\varphi_i(a_{i-1}) = a_i$, $\varphi_i(b_{i-1}) = b_i$, $\varphi_i = L_{e_i}^{\pm 1}$ with $1 \neq e_i \in W$. Further, let $\varphi_{i+1}^{-1} \neq \varphi_i$ for each $1 \leqslant i \leqslant k-1$. If $b_1 = a_0\backslash\backslash 1$, $e_1 = a_0$ and $\varphi_1 = L_{e_1}^{-1}$, then $\varphi_i = L_{e_i}^{-1}$ for all $1 \leqslant i \leqslant k$, and*

(i) *$e_i = a_{i-1}$, $b_i = a_{i-1}\backslash\backslash 1$, $a_i = 1$ for i odd,*
(ii) *$e_i = b_{i-1}$, $a_i = b_{i-1}\backslash\backslash 1$, $b_i = 1$ for i even.*

Moreover, $(a_i, b_i) \neq (a_j, b_j)$ whenever $0 \leqslant i < j \leqslant k$.

Proof. Employ induction again, and let $k-1 \geqslant i \geqslant 1$ be odd. If $\varphi_{i+1} = L_{e_{i+1}}$, then 3.1 implies either $b_i = e_{i+1}\backslash\backslash b_{i+1}$ or $e_{i+1} = 1/\!/b_i$. The former case implies $e_{i+1} = e_i$, which contradicts $\varphi_{i+1} \neq \varphi_i^{-1}$. The latter case gives $e_i = a_{i-1} = 1/(a_{i-1}\backslash 1) = 1/b_i = e_{i+1}$ as well. Therefore $\varphi_{i+1} = L_{e_{i+1}}^{-1}$ and by 3.1 $e_{i+1} = b_i$, $b_{i+1} = 1$ and $a_{i+1} = b_i\backslash\backslash 1$. □

3.6 Lemma. *Let $a_i, b_i \in W$, $a_i \neq b_i$, $0 \leqslant i \leqslant k$ be such that $k \geqslant 2$, and for $1 \leqslant i \leqslant k$ let $|a_i| + |b_i| = |a_0| + |b_0|$, $\varphi_i(a_{i-1}) = a_i$, $\varphi_i(b_{i-1}) = b_i$, $\varphi_i = L_{e_i}^{\pm 1}$ with $1 \neq e_i \in W$. Further, let $\varphi_{i+1}^{-1} \neq \varphi_i$ for each $1 \leqslant i \leqslant k-1$. If $1 \in \{a_j, b_j\}$ for any $0 \leqslant j \leqslant k$, then $1 \in \{a_0, b_0, a_k, b_k\}$.*

Proof. Let $1 \in \{a_j, b_j\}$ for $1 \leqslant j \leqslant k-1$. By 3.2 we have $1 \in \{a_{j-1}, b_{j-1}, a_{j+1}, b_{j+1}\}$, and hence we can assume that there exists $0 \leqslant j \leqslant k-1$ with $b_j = 1 = a_{j+1}$. As the inverses φ_i^{-1} can be considered in place of φ_i, we can further assume that $\varphi_j = L_{e_j}$.

By 3.3 either $b_{j+1} = 1/\!/a_j$, or $a_j = b_{j+1}\backslash\backslash 1$. In the former case 3.4 yields $1 \in \{a_k, b_k\}$ and in the latter case $1 \in \{a_0, b_0\}$ follows from 3.5. □

3.7 Lemma. *Let $a_i, b_i \in W$, $a_i \neq b_i$, $0 \leqslant i \leqslant k$ be such that $k \geqslant 3$, and for $1 \leqslant i \leqslant k$ let $\varphi_i(a_{i-1}) = a_i$, $\varphi_i(b_{i-1}) = b_i$, $\varphi_i = L_{e_i}^{\pm 1}$ with $1 \neq e_i \in W$. Further, for each $1 \leqslant i \leqslant k-1$ let $\varphi_{i+1}^{-1} \neq \varphi_i$ and $|a_0| + |b_0| < |a_1| + |b_1| = |a_i| + |b_i| > |a_k| + |b_k|$. Then $1 \in \{a_j, b_j\}$ for no $1 \leqslant j \leqslant k-1$.*

Proof. Assume that $1 \in \{a_j, b_j\}$ for $1 \leqslant j \leqslant k-1$. Then $1 \in \{a_1, b_1, a_{k-1}, b_{k-1}\}$ by 3.6, and 3.1 implies $|a_0| + |b_0| = |a_1| + |b_1|$ or $|a_k| + |b_k| = |a_{k-1}| + |b_{k-1}|$. □

3.8 Lemma. *Let $a_i, b_i \in W$, $a_i \neq b_i$, $0 \leqslant i \leqslant k$ be such that $k \geqslant 2$, and for $1 \leqslant i \leqslant k$ let $|a_i| + |b_i| = |a_0| + |b_0|$, $\varphi_i(a_{i-1}) = a_i$, $\varphi_i(b_{i-1}) = b_i$, $\varphi_i = L_{e_i}^{\pm 1}$ with $1 \neq e_i \in W$. Further, let $\varphi_{i+1}^{-1} \neq \varphi_i$ for each $1 \leqslant i \leqslant k-1$, $\varphi_k \neq \varphi_1^{-1}$ and let $a_k = a_0$, $b_k = b_0$. Then $a_j \neq 1 \neq b_j$ for all $0 \leqslant j \leqslant k$.*

Proof. Start from the contrary and assume $1 \in \{a_i, b_i\}$ for some $0 \leqslant i \leqslant k$. Note that for every $1 \leqslant j \leqslant k$ we have $\varphi_{j-1} \dots \varphi_1 \varphi_k \dots \varphi_j(a_{j-1}) = a_{j-1}$ and $\varphi_{j-1} \dots \varphi_1 \varphi_k \dots \varphi_j(b_{j-1}) = b_{j-1}$. Hence $1 \in \{a_j, b_j\}$ for all $0 \leqslant j \leqslant k$. If $b_0 = 1$ and $\varphi_1 = L_{e_1}$, then by 3.3 $e_1 = b_1$ and either $b_1 = 1 /\!/ a_0$ or $a_0 = b_1 \backslash\!\backslash 1$. In the former case 3.4 applies, and in the latter case 3.5 can be used with $\varphi_1^{-1}, \varphi_k^{-1}, \dots, \varphi_2^{-1}$. Hence 3.4 or 3.5 are applicable in any case, implying $(a_k, b_k) \neq (a_1, b_1)$, a contradiction. □

4. Loop words not containing 1

For $a, b \in W$ write $a \leqslant b$ if the reduced loop word $\varrho_X(a)$ is a subword of the reduced loop word $\varrho_X(b)$. Write also $a < b$ if $a \leqslant b$ and $a \neq b$. By definition, $1 \leqslant a$ for all $a \in W$.

4.1 Lemma. *Let $a, b, c, d, e \in W$, $1 \notin \{a, b, c, d, e\}$ be such that $a \neq b$, $|c| + |d| = |a| + |b|$ and $c = \varphi(a)$, $d = \varphi(b)$ for $\varphi = L_e^{\pm 1}$. If $|c| \leqslant |a|$, then $|c| < |a|$, and we have $a = e \backslash\!\backslash c$, $d = e \circ b$ if $\varphi = L_e$, and $a = e \circ c$, $d = e \backslash\!\backslash b$ for $\varphi = L_e^{-1}$.*

Proof. This follows immediately from 2.1(b) and 2.2(b). □

4.2 Lemma. *Let $a_i, b_i, e, f \in W$, $a_i \neq b_i$, $0 \leqslant i \leqslant 2$ be such that for $\varphi_1 = L_e^{\pm 1}$, $\varphi_2 = L_f^{\pm 1}$, $e \neq 1 \neq f$, $\varphi_1 \neq \varphi_2^{-1}$ we have $1 \neq a_j = \varphi_j(a_{j-1})$, $1 \neq b_j = \varphi_j(b_{j-1})$, $j = 1, 2$. If $|a_2| + |b_2| = |a_1| + |b_1| > |a_0| + |b_0|$ and $|a_2| < |a_1|$, then $a_1 < b_1$.*

Proof. By 4.1 $a_1 = f \backslash\!\backslash a_2$ if $\varphi_2 = L_f$ and $a_1 = f \circ a_2$ if $\varphi_2 = L_f^{-1}$. As $\varphi_1 \neq \varphi_2^{-1}$, we have $b_1 /\!/ b_0 \neq a_1 \neq e \circ a_0$ when $\varphi_1 = L_e$. Then it follows from 2.1(a) that $b_1 = a_1 \circ b_0$ or $b_1 = (a_1 /\!/ a_0) \circ b_0$ or $b_1 = a_1 /\!/ a_0$. If $\varphi_1 = L_e^{-1} \neq \varphi_2^{-1}$, then $a_1 \neq e \backslash\!\backslash a_0$ yields $b_1 = (a_0 /\!/ a_1) \backslash\!\backslash b_0$ by 2.2(a). Thus $a_1 < b_1$ in any case. □

4.3 Lemma. *Let $a_i, b_i, e, f \in W$, $a_i \neq b_i$, $0 \leqslant i \leqslant 2$ be such that for $\varphi_1 = L_e^{\pm 1}$, $\varphi_2 = L_f^{\pm 1}$, $e \neq 1 \neq f$, $\varphi_1 \neq \varphi_2^{-1}$ we have $a_j = \varphi_j(a_{j-1})$, $b_j = \varphi_j(b_{j-1})$, $j = 1, 2$ and $1 \notin \{a_0, b_0, a_1, b_1\}$. If $|a_2| + |b_2| < |a_1| + |b_1| = |a_0| + |b_0|$ and $|a_1| < |a_0|$, then $b_1 < a_1$.*

Proof. Put $a_0' = b_2$, $a_1' = b_1$, $a_2' = b_0$, $b_0' = a_2$, $b_1' = a_1$, $b_2' = a_0$, $\varphi_1' = \varphi_2^{-1}$ and $\varphi_2' = \varphi_1^{-1}$. Then $b_1 = a_1' < b_1' = a_1$ by 4.2. □

4.4 Lemma. *Let $a_i, b_i \in W$, $a_i \neq b_i$, $a_i \neq 1 \neq b_i$, $0 \leqslant i \leqslant k$ be such that $k \geqslant 2$, and for $1 \leqslant i \leqslant k$ let $|a_i| + |b_i| = |a_0| + |b_0|$, $\varphi_i(a_{i-1}) = a_i$, $\varphi_i(b_{i-1}) = b_i$, $\varphi_i = L_{e_i}^{\pm 1}$ with $1 \neq e_i \in W$. Further, let $\varphi_{i+1}^{-1} \neq \varphi_i$ for each $1 \leqslant i \leqslant k-1$, and suppose that $|a_1| < |a_0|$. Then*

(i) $|a_k| < \ldots < |a_1| < |a_0|$, *and*
(ii) $a_0 < b_0$ *implies* $a_i < b_i$ *for all* $0 \leqslant i \leqslant k$.

Proof. We shall show that for all $1 \leqslant i \leqslant k$ either $a_{i-1} = e_i \backslash\backslash a_i$, $b_i = e_i \circ b_{i-1}$ and $\varphi_i = L_{e_i}$, or $a_{i-1} = e_i \circ a_i$, $b_i = e_i \backslash\backslash b_{i-1}$ and $\varphi_i = L_{e_i}^{-1}$. For $i = 1$ this follows from 4.1 and we can continue by induction. Suppose that $1 \leqslant i \leqslant k-1$ and $|b_{i+1}| < |b_i|$. By 4.1 $b_i = e_{i+1} \backslash\backslash b_{i+1}$ if $\varphi_{i+1} = L_{e_{i+1}}$, and $b_i = e_{i+1} \circ b_{i+1}$ if $\varphi_{i+1} = L_{e_{i+1}}^{-1}$. However, this contradicts the induction hypothesis, as $\varphi_i \neq \varphi_{i+1}^{-1}$. Thus $|a_{i+1}| < |a_i|$ and the induction step follows again from 4.1. As $a_i < a_{i-1}$, $b_{i-1} < b_i$, we see that $a_{i-1} < b_{i-1}$ implies $a_i < b_i$. □

4.5 Lemma. *Let $a_i, b_i \in W$, $0 \leqslant i \leqslant k$ be such that $k \geqslant 2$, and for $1 \leqslant i \leqslant k$ let $\varphi_i(a_{i-1}) = a_i$, $\varphi_i(b_{i-1}) = b_i$, $\varphi_i = L_{e_i}^{\pm 1}$, with $1 \neq e_i \in W$. Further, for each $1 \leqslant i \leqslant k-1$ let $\varphi_{i+1}^{-1} \neq \varphi_i$ and $|a_0| + |b_0| < |a_1| + |b_1| = |a_i| + |b_i| > |a_k| + |b_k|$. Then $a_i = b_i$ for all $0 \leqslant i \leqslant k$.*

Proof. Assume that $a_i \neq b_i$ for $0 \leqslant i \leqslant k$. By 2.3, $k \geqslant 3$ and by 3.7 we have $1 \notin \{a_j, b_j\}$ for $1 \leqslant j \leqslant k-1$. Without loss of generality we can assume that $|a_2| < |a_1|$. By 4.2 we have $a_1 < b_1$, and by 4.4 $|a_{k-1}| < |a_{k-2}|$ and $a_{k-1} < b_{k-1}$. However, a_j, b_j, $k-2 \leqslant j \leqslant k$ satisfy the hypotesis of 4.3 for $e = e_{k-1}$, $f = e_k$, and hence $b_{k-1} < a_{k-1}$. We have obtained a contradiction, and thus $a_i = b_i$ for all $0 \leqslant i \leqslant k$. □

4.6 Lemma. *Let $a_i, b_i \in W$, $a_i \neq b_i$, $0 \leqslant i \leqslant k$ be such that $k \geqslant 2$, and for $1 \leqslant i \leqslant k$ let $|a_i| + |b_i| = |a_0| + |b_0|$, $\varphi_i(a_{i-1}) = a_i$, $\varphi_i(b_{i-1}) = b_i$, $\varphi_i = L_{e_i}^{\pm 1}$ with $1 \neq e_i \in W$. Further, let $\varphi_{i+1}^{-1} \neq \varphi_i$ for each $1 \leqslant i \leqslant k-1$ and $\varphi_k^{-1} \neq \varphi_1$. Then $a_k \neq a_0$ or $b_k \neq b_0$.*

Proof. Suppose that $a_k = a_0$, $b_k = b_0$. By 3.8 $a_i \neq 1 \neq b_i$ for all $0 \leqslant i \leqslant k$. We can assume that $|a_1| < |a_0|$. Then 4.4 implies $a_k < a_0$. □

5. Main theorem

5.1 Theorem. *Let W be a free loop with a basis $X \neq \emptyset$. Then the left multiplication group* $\mathrm{LMlt}(W)$ *is a free group of infinite rank and a Frobenius permutation group.*

Proof. Suppose that $\mathrm{LMlt}(W)$ is not a Frobenius group. Then there exist $a_i, b_i \in W$, $a_i \neq b_i$, $0 \leqslant i \leqslant k$ such that $k \geqslant 2$, $a_k = a_0$, $b_k = b_0$, and for $1 \leqslant i \leqslant k$ we have $\varphi_i(a_{i-1}) = a_i$, $\varphi_i(b_{i-1}) = b_i$, $\varphi_i = L_{e_i}^{\pm 1}$ with $1 \neq e_i \in W$. Further, we can assume that $\varphi_{i+1}^{-1} \neq \varphi_i$ for $1 \leqslant i \leqslant k-1$ and $\varphi_k \neq \varphi_1^{-1}$. Let $m = \max\{|a_i| + |b_i|\ ;\ 0 \leqslant i \leqslant k\}$ and $n = \min\{|a_i| + |b_i|\ ;\ 0 \leqslant i < k\}$. By 4.6 $m > n$. As we can cyclically permute the sequences a_i and b_i, it can be assumed that $|a_1| + |b_1| = m$ and $|a_0| + |b_0| < m$. However, then there exists $2 \leqslant r \leqslant k$ such that $|a_j| + |b_j| = |a_1| + |b_1|$ for $1 \leqslant j \leqslant r-1$ and $|a_r| + |b_r| < |a_1| + |b_1| > |a_0| + |b_0|$. By 4.5 this is not possible. □

5.2 Remark. Note that the multiplication group of a loop is never a Frobenius group [1; Lemma 3.20].

References

[1] *A. Drápal and T. Kepka*: Multiplication Groups of Quasigroups and Loops I. Acta Univ. Carol. *34* (1993), 85–99.

[2] *T. Evans*: On multiplicative systems defined by generators and relations. I.. Normal form theorem, Proc. Cambridge Philos. Soc. *47* (1951), 637–649.

[3] *T. Evans*: Varieties of loops and quasigroups. Chapter I., Quasigroups and Loops: Theory and Applications (O. Chein, H. O. Pflugfelder and J. D. H. Smith, eds.). Heldermann Verlag, New York, 1990, pp. 1–26.

[4] *T. Kepka and M. Niemenmaa*: On conjugacy classes in finite loops. Bull. Austral. Math. Soc. *38* (1988), 171–176.

[5] *T. Kepka and M. Niemenmaa*: On multiplication groups of loops. J. of Algebra *135* (1990), 112–122.

[6] *M. Niemenmaa and G. Rosenberger*: On connected transversals in infinite groups. Math. Scand. *70* (1992), 172–176.

[7] *J. D. H. Smith*: Representation Theory of Infinite Groups and Finite Quasigroups. Les Presses de l'Université de Montréal, Montreal, 1986.

[8] *A. Vesanen*: On connected transversals in $PSL(2,q)$. Annales Acad. Sci. Fennicae, Series A, I. Mathematica, Dissertationes 84 (1992). Helsinki.

Author's address: Matematicko-fyzikální fakulta UK, Sokolovská 83, 186 00 Praha 8, Česká republika.