Quasigroups and related systems, **3** (1996), 21–40

Frobenius groups and one-sided S-systems

Evghenii A. Kuznetsov

Abstract

Frobenius groups are studied by the means of systems of orthogonal operations, naturally being built over these groups.

1. Introduction

Definition 1. [4,8] The transitive irregular permutation group G acting on a set E is called a *Frobenius group*, if $St_{ab}(G) = \langle id \rangle$ for any $a, b \in E,\ a \neq b$.

Frobenius groups are one of the classical group classes in permutation group theory. The studying of these groups was begun in the Frobenius article [3] at the beginning of 20th century and was continued by M.Hall [4], H.Wielandt [8] etc. Frobenius proved in [3] by means of character group theory that there exists an invariant regular subgroup consisting of all fixed-point free permutations and the identity permutation in a finite Frobenius group (Frobenius theorem). It is not known any other proof of this theorem (without using of character group theory) till now.

In present article a 1-1 correspondence between Frobenius groups and one-sided S-systems of orthogonal operations [1] (on the same set of symbols E), whose cell permutations form a group, is built.

1991 Mathematics Subject Classification: 20N05, 20N10, 08A55
Keywords: Frobenius group, orthogonal operation

In the section 2 the incident system of (left) cosets in an arbitrary finite Frobenius group G by stabilizer $St_a(G)$ $(a \in E)$ is investigated. It is proved that this incident system is an algebraic m-net [2], where $m = |St_a(G)|$.

In the section 3 the construction of two systems of the orthogonal operations over an arbitrary finite Frobenius group G is given. It is proved that they form a left and a right S-systems [1]. Some other properties of these one-sided S-systems are studied too. A numbering correlation between permutations degree n and $m = |St_a(G)|$ is obtained. As a corollary of this correlation it is proved that finite Frobenius p-groups doesn't exist (the negative answer on the problem 6.55 from [5] in a finite case). At the end of the part 2 the right (left) cell permutations of right (left) S-system are defined and it is shown that the set of all cell permutations forms a group coinciding with the group G.

In the section 3 an arbitrary right (left) S-systems of binary idempotent quasigroups on some set E (finite or infinite) are investigated. In any right (left) S-system of operations the cell functions are introduced, and it is proved that all these functions are permutations on the set E. If the set of all cell permutations forms a group (with respect to natural operation of composition), then this group is a Frobenius group. As a corollary, the proof of Frobenius theorem is obtained (when the set E is finite). Another construction of one-sided S-systems of operations on E over the Frobenius group G, no depending from the cardinality of the set E, are given in order to demonstrate preserving of the correspondence between Frobenius groups and one-sided S-systems of operations on E with the property mentioned above in the case when the set E is infinite.

We will use the following notations:

$H_a = St_a(G)$ is the stabilizer of the element $a \in E$ in the group G,

$0,\ 1$ are two distinguished elements in the set E,

$E^* = \{0\} \cup \{h(1)\ :\ h \in H_0 = St_0(G)\} \subseteq E$.

2. Incident system of cosets

In this paragraph we suppose that the set E is finite, i.e. the permutations from the Frobenius group G have the finite degree $n = |E|$.

In a Frobenius group all subgroups H_a $(a \in E)$ are conjugate and so we can denote

$$m = |H_0| = |H_a|\,.$$

At last, we can suppose the elements from E are renamed so that

$$E^* = \{0, 1, ..., m\}.$$

Let's consider all (left) cosets $H_a^b = \{\alpha \in G \ : \ \alpha(a) = b\}$ in G by the subgroup H_a and define the following incident system $\mathcal{R} =< X, \mathcal{L}, I >$:

points from X are (left) cosets H_a^b,

lines from $\mathcal{L}$ are permutations $\alpha \in G$,

incidence I is a belonging relation, i.e.

$$(a,b)I[\alpha] \ \Leftrightarrow \ (\,point\ H_a^b\,)I(\,line\ \alpha) \overset{def}{\Leftrightarrow} (\,\alpha \in H_a^b\,). \tag{1}$$

Definition 2. By an *algebraic k-net* [2] we mean an incidence system $\mathcal{R} =< X, \mathcal{L}, L_1, ..., L_k, I >$ consisting of the point set X, the line set $\mathcal{L}$ which is separated on k distinct classes of "parallel" lines $l_1, L_2, ..., L_k$, and the incidence relation I between elements from X and $\mathcal{L}$, which satisfy the following two conditions:

1) any two lines from the different classes L_i and L_j are incident to one and only one point from X,
2) every point from X is incident to one and only one line from each class L_i.

Lemma 1. *The system $\mathcal{R} =< X, \mathcal{L}, I >$ defined in (1) is an algebraic m-net.*

Proof. According to Frobenius theorem [8], in a finite Frobenius group G of permutations of degree n all fixed-point-free permutations with the identity permutation form a transitive invariant subgroup A, moreover, $|A| = n$. It is easy to see that A is a group transversal (see [6]) in G to H_a $\forall a \in E$.

Let's define the classes L_i of "parallel" lines in $\mathcal{L}$ by the following:

$$L_i = \{\alpha h_i \ : \ \alpha \in A, \ h_i \in H_0, \quad h_i(1) = i\}, \quad i = 1, ..., n\,.$$

Note that $h_i = id$ and $L_i = A$.

Lemma A. *Let $\alpha, \beta \in \mathcal{L}$ and $\alpha \neq \beta$. The following conditions are equivalent:*

1) *both of lines α and β are in the class L_i for some i,*
2) *$\alpha(t) \neq \beta(t) \quad \forall t \in E$.*

Proof of Lemma A. 1) $\Rightarrow$ 2). Let $\alpha, \beta \in L_i$ and $\alpha \neq \beta$. Let's assume there exists $t_0 \in E$ such that $\alpha(t_0) = \beta(t_0)$. Then we have

$$\alpha_0 h_i(t_0) = \beta_0 h_i(t_0),$$
$$\alpha_0(t_1) = \beta_0(t_1)$$

where $\alpha_0, \beta_0 \in A$, $t_1 = h_i(t_0)$. The last equality contradicts the regularity of the group A. So

$$\alpha(t) \neq \beta(t) \quad \forall t \in E.$$

2) $\Rightarrow$ 1). Let $\alpha, \beta \in \mathcal{L}$, $\alpha \neq \beta$ and

$$\alpha(t) \neq \beta(t) \quad \forall t \in E.$$

The set A is a (left) transversal in G to H_0, so we have

$$\alpha = \alpha_0 h_i, \qquad \beta = \beta_0 h_j,$$

where $\alpha_0, \beta_0 \in A$, $h_i, h_j \in H_0$. It is necessary to prove that $h_i = h_j$. We have

$$\alpha_0 h_i(t) \neq \beta_0 h_j(t) \quad \forall t \in E,$$
$$\alpha_0^{-1} \beta_0 h_j h_i^{-1}(t') \neq t' \quad \forall t' = h_i(t) \in E,$$

i.e. $\gamma_0 = \alpha_0^{-1} \beta_0 h_j h_i^{-1}$ is a fixed-point-free permutation. Then $\gamma_0 \in A$ and we obtain

$$h_j h_i^{-1} = h_k = \beta_0^{-1} \alpha_0 \gamma_0 \in H_0 \cap A = \{id\},$$

i.e. $h_i = h_j$. The proof of Lemma A is completed. □

Let's return to the proof of Lemma 1. It is necessary to check the realization of the conditions 1) and 2) from Definition 2 for the incidence system $\mathcal{R} =< X, \mathcal{L}, I >$.

a) Let α and β be two different lines from the different classes L_i and L_j. Then there exist element $t_0 \in E$ such that

$$\alpha(t_0) = \beta(t_0) = d, \tag{2}$$

(in a contrary case we would have $\alpha(t) \neq \beta(t) \quad \forall t \in E$, and so $\alpha, \beta \in L_k$ for some k according to Lemma A. Moreover, there exist an unique element $t_0 \in E$ satisfying (2), because in a opposite case the permutation $\alpha^{-1}\beta$ would fix two different elements from E and so $\alpha^{-1}\beta = id$ according to Definition 1. So we have:

$$\alpha, \beta \in H_{t_0}^d,$$

i.e. the lines α and β are incident to the unique point $H_{t_0}^d$. The condition 1) is proved.

b) Let H_a^b be an arbitrary point from X. This point is incident to all lines $\alpha_i \in G$ such that $\alpha_i \in H_a^b$, i.e. $\alpha_i(a) = b$. By means of Lemma A we obtain that different such lines α_i lie in different classes L_i. As $|H_a^b| = |H_a| = m$, then the point H_a^b is incident to m different lines α_i from different classes L_i; moreover, it is incident to an unique line in each class L_i. The number of classes L_i is equal to m, so every of these classes consists of a line being incident to the point H_a^b. The condition 2) is proved.

The proof of Lemma 1 is completed. □

3. One-sided S-systems being constructed over a Frobenius group

In this paragraph we will suppose that Frobenius group G is finite.

Let's define the following two binary operations $(\cdot)$ and $(*)$:

$$(\cdot) \ : \ E \times E \to E,$$
$$x \cdot y = z \ \stackrel{def}{\Longleftrightarrow} \ z = \varphi_x(y),$$

where $\varphi_x \in A,\ \varphi_x(0) = x,$

$$(*)\ :\ E^* \times E \to E,$$

$$0 * v \overset{def}{\iff} 0,$$

$$u \neq 0\ :\ u * v = w \overset{def}{\iff} w = h_u(v),$$

where $h_u \in H_0,\ h_u(1) = u$. Note that $(*)$ is a partial operation.

Lemma 2. *The following statements are true:*

1) $< E, \cdot, 0 > \cong A$,
2) $< E^* - \{0\}, *, 1 > \cong H_0$,
3) $x * (y \cdot z) = (x * y) \cdot (x * z) \quad \forall x \in E^*, \quad \forall y, z \in E,$
4) *every permutation* $h \in H_0$ *is an automorphism of the subgroup* A,
5) $G = \{\alpha_{a,b}\ :\ \alpha_{a,b}(x) = a \cdot (b * x),\ \ a \in E\ \ b \in E^* - \{0\}\}$.

Proof. 1) Let's consider the following mapping

$$\alpha\ :< E, \cdot, 0 > \to A\,, \qquad \alpha(x) = \varphi_x$$

where $x \in E$ and the permutation φ_x is defined above. Then α is a bijection, because the group A is regular on the set E. Further we have

$$(\alpha(x \cdot y))(0) = \varphi_{x \cdot y}(0) = x \cdot y.$$

On the other hand we have

$$(\alpha(x)\alpha(y))(0) = \varphi_x \varphi_y(0) = \varphi_x(y) = x \cdot y\,.$$

So we obtain

$$(\alpha(x \cdot y))(0) = x \cdot y = (\alpha(x)\alpha(y))(0),$$

and

$$\alpha(x \cdot y) = \alpha(x)\alpha(y),$$

because the group A is regular (i.e. sharply transitive) on the set E. We obtain that the mapping α is an isomorphism.

2) can be proved analogously, and the isomorphism is determined by the mapping

$$\beta\ :< E^* - \{0\}, *, 1 > \to H_0\,, \quad \beta(u) \overset{def}{=} h_u,$$

where $u \in E^* - \{0\}$ and the permutation h_u is defined above.

3) and 4) can be proved analogously to 3) of Lemma 8 from [7].

5) can be proved analogously to Lemma 9 from [7]. $\square$

Note that $\alpha_{0,1} \equiv id$ and $\alpha_{a,1}(x) = a \cdot x$ is a fixed-point-free permutation if $a \neq 0$; moreover $\{\alpha_{a,1}\}_{a \in E} \equiv A$.

Now let's define the following partial ternary operation

$$(\ , \ , \ ) : E \times E^* \times E \to E,$$

$$(x, a, y) \stackrel{def}{=} x \cdot (a * (x^{-1} \cdot y)), \tag{3}$$

where $a \in E^*$, $x, y \in E$, and x^{-1} is the inverse element to x in $< E, \cdot, 0 >$.

Lemma 3. *The following statements are true:*

1) $(x, 0, y) = x, \quad (x, 1, y) = y,$
$(x, a, x) = x, \quad (0, a, 1) = a, \quad \forall a \in E^*, \quad x, y \in E.$

2) *The system of operations* $A_a(x, y) = (x, a, y)$ $(a \in E^* - \{0\})$ *is a right* S*-system.*

3) *The operations* (x, a, y) *and* (x, b, y) *are orthogonal for any* $a \neq b$, *and they are quasigroups for* $a \neq 0, 1$.

4) *The operations* (x, a, y) *and* $x \circ y = x^{-1} \cdot y$ *are orthogonal for any* $a \in E^*$.

Proof. 1)
$$(x, 0, y) = x \cdot (0 * (x^{-1} \cdot y)) = x \cdot 0 = x,$$
$$(x, 1, y) = x \cdot (1 * (x^{-1} \cdot y)) = x \cdot x^{-1} \cdot y = y,$$
$$(x, a, x) = x \cdot (a * (x^{-1} \cdot x)) = x \cdot (a * 0) = x \cdot 0 = x,$$
$$(0, a, 1) = 0 \cdot (a * (0^{-1} \cdot 1)) = a * 1 = a.$$

2) According to the definition from [1], a system of operations $A_a(x, y)$ $(a \in E^* \subseteq E)$ on some set E is a *right (left)* S*-system*, if for any $a, b \in E^*$ and $x, y \in E$ there exists $c = c(a, b) \in E^*$ such that the following equality

$$(A_a \circ A_b)(x, y) = A_a(x, A_b(x, y)) = A_c(x, y)$$

holds, and moreover, the system $< A_u, \circ, A_1 >$, where $u \neq 0$, is a group (correspondingly, if for any $a, b \in E^*$ and $x, y \in E$ there exist such $c = c(a, b) \in E^*$ that the following equality

$$(A_a \bullet A_b)(x,y) = A_a(A_b(x,y),y) = A_c(x,y)$$

holds, and moreover, the system $< A_u(u \neq 1), \bullet, A_0 >$ is a group).

According to the equality (3) we obtain for the operations $A_a(x,y) = (x,a,y)$ and $A_b(x,y) = (x,b,y)$ (where $a,b \in E^* - \{0\}$):

$$\begin{gathered}(A_a \circ A_b)(x,y) = A_a(x, A_b(x,y)) = (x,a,(x,b,y)) = \\ = x \cdot (a * (x^{-1} \cdot (x \cdot (b * (x^{-1} \cdot y))))) = \\ = x \cdot (a * b * (x^{-1} \cdot y)) = A_{a*b}(x,y).\end{gathered}$$

With the help of Lemma 2, we obtain that the system $< A_u, \circ, A_1 >$, where $u \neq 0$ is a group (this group is isomorphic to the group H_0), i.e. the system of operations $A_a(x,y) = (x,a,y)$ is a right S-system.

3) We notice that for any $a \in E^*$, $z \in E$,

$$(a * z)^{-1} = a * x^{-1}.$$

Really, with the help of Lemma 2, we obtain

$$\begin{gathered}(a * z) \cdot (a * z^{-1}) = a * (z \cdot z^{-1}) = a * 0 = 0, \\ (a * z^{-1}) \cdot (a * z) = a * (z^{-1} \cdot z) = a * 0 = 0.\end{gathered}$$

Further, let we have the following system

$$\begin{cases} (x,a,y) = c, \\ (x,b,y) = d, \end{cases}$$

where $a,b \in E^*$, $a \neq b, c, d \in E$ are arbitrary given elements.

If $a = 0$ then $x = c$, $y = c \cdot (b^{-1} * (c^{-1} \cdot d))$, i.e. this system has an unique solution in $E \times E$; so the operations (x,a,y) and (x,b,y) are orthogonal. If $b = 0$ then we obtain the same result.

Let $a, b \neq 0$. Then we have

$$\begin{cases} (x,a,y) = c \\ (x,b,y) = d \end{cases} \Longleftrightarrow \begin{cases} x \cdot (a * (x^{-1} \cdot y)) = c \\ x \cdot (b * (x^{-1} \cdot y)) = d \end{cases} \Longleftrightarrow$$

$$\begin{cases} a * (x^{-1} \cdot y) = x^{-1} \cdot c \\ b * (x^{-1} \cdot y) = x^{-1} \cdot d \end{cases} \Longleftrightarrow \begin{cases} (a * (x^{-1} \cdot y))^{-1} = c^{-1} \cdot x \\ (b * (x^{-1} \cdot y))^{-1} = d^{-1} \cdot x \end{cases} \Longleftrightarrow$$

$$\begin{cases} a * (y^{-1} \cdot x) = c^{-1} \cdot x \\ b * (y^{-1} \cdot x) = d^{-1} \cdot x \end{cases} \Leftrightarrow a^{(-1)} * (c^{-1} \cdot x) = y^{-1} \cdot x = b^{(-1)} * (d^{-1} \cdot x),$$

where a^{-1} is the inverse element to a in $< E^* - \{0\}, *, 1 >$. From the last equality we obtain

$$c^{-1} \cdot x = (a * b^{-1}) * ((d^{-1} \cdot c) \cdot (c^{-1} \cdot x)),$$

i.e. (see Lemma 2)

$$c^{-1} \cdot x = \alpha_{d^{-1} \cdot c, a * b^{(-1)}}(c^{-1} \cdot x)$$

As $a \neq b$ then $a * b^{(-1)} \neq 1$; so the permutation $\alpha_{d^{-1} \cdot c, a * b^{(-1)}}$ has an unique fixed-point element p_0. So we obtain that $x = c \cdot p_0$, $y = c \cdot p_0 \cdot (a^{(-1)} * p_0)$, i.e. the operations (x, a, y) and (x, b, y) are orthogonal.

4) We have for any $a \in E^* - \{0\}$ and $c, d \in E$:

$$\begin{cases} (x, a, y) = c \\ x \circ y = d \end{cases} \Longleftrightarrow \begin{cases} x \cdot (a * (x^{-1} \cdot y)) = c \\ x^{-1} \cdot y = d \end{cases} \Longleftrightarrow$$

$$\begin{cases} x \cdot (a * d) = c \\ y = x \cdot d \end{cases} \Longleftrightarrow \begin{cases} x = c \cdot (a * d)^{-1} \\ y = c \cdot (a * d)^{-1} \cdot d, \end{cases}$$

i.e. the operations (x, a, y) and $x \circ y$ are orthogonal. □

By an analogical way it can be defined one more partial ternary operation

$$[x, t, y] \; : \; E \times E^* \times E \to E$$
$$[x, a, y] \overset{def}{=} (a * (x \cdot y^{-1})) \cdot y\,, \quad a \in E^*.$$

Lemma 4. *The following statements are true:*

1) $[x, 0, y] = y, \quad [x, 1, y] = x,$
$[x, a, x] = x, \quad [1, a, 0] = a, \quad \forall a \in E^*, \quad x, y \in E.$
2) *The system of operations* $A_a(x, y) = [x, a, y]$ $(a \in E^* - \{0\})$ *is a left* S*-system.*
3) *The operations* $[x, a, y]$ *and* $-[x, b, y]$ *are orthogonal for any* $a \neq b$ *and they are quasigroups for* $a \neq 0, 1$.
4) *The operations* $[x, a, y]$ *and* $x \bullet y = x \cdot y^{-1}$ *are orthogonal for any* $a \in E^*$.

Proof. 1). It is evident.

2)-4) can be proved analogously to the proof of Lemma 3. □

Remark. There is a 1-1 correspondence between algebraic m-net from Lemma 1 and some system of m orthogonal operations on the set E. Defining the partial ternar $< x, t, y >$ by the following:

$$(a, b)I[c, d] \iff < a, c, b >= d,$$

where I is the incidence relation, we obtain

$$< x, a, y >= y \cdot (a * x)^{-1}, \ a \in E^*$$

This system of operations is not a left or a right S-system of operations.

Let's return back to the ternary operation (x, a, y).

Lemma 5. *The following statements are true:*
1) *The mapping* $\alpha_{b,a}(x) = b \cdot (a * x)$, $b \in E$, $a \in E^* - \{0\}$, $x \in E$ *is an isomorphism between operations* (x, c, y) *and* $(x, a * c * a^{-1}, y)$.
2) *The mapping* $\alpha_{b,I}$ *is an automorphism of the operation* (x, c, y) *for any* $b \in E$, $c \in E^*$.

Proof. 1) We have:

$$\alpha_{b,a}((x, c, y)) = b \cdot (a * (x \cdot (c * (x^{-1} \cdot y)))) =$$
$$= b \cdot (a * x) \cdot (a * c * (x^{-1} \cdot y)) =$$
$$= b \cdot (a * x) \cdot ((a * c * a^{(-1)}) * a * (x^{-1} \cdot y)) =$$
$$= b \cdot (a * x) \cdot ((a * c * a^{(-1)}) * ((a * x^{-1}) \cdot (a * y))) =$$
$$= b \cdot (a * x) \cdot ((a * c * a^{(-1)}) * ([(a * x)^{-1} \cdot b^{-1}] \cdot [b \cdot (a * y)])) =$$
$$= (\alpha_{b,a}(x)) \cdot ((a * c * a^{(-1)}) * ((\alpha_{b,a}(x))^{-1} \cdot (\alpha_{b,a}(y)))) =$$
$$= (\alpha_{b,a}(x), a * c * a^{(-1)}, \alpha_{b,a}(y)).$$

It means that the mapping $\alpha_{b,a}$ is an isomorphism between operations (x, c, y) and $(x, a * c * a^{-1}, y)$.

2) is an evident corollary of 1). □

Lemma 6. *The following equality is true:*

$$n-1=km$$

for some $k\in\mathcal{N}$, *i.e.* $(|E^*|-1)\,|\,(|E|-1)$.

Proof. (see [1] too). Let $a_1\in E$ and $a_1\neq 0$. Let's consider the following equalities:

$$A_1(0,a_1)=(0,1,a_1)=1*a_1=a_1$$
$$A_2(0,a_1)=(0,2,a_1)=2*a_1$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$A_m(0,a_1)=(0,m,a_1)=m*a_1.$$

All values in the right sides of the equalities are different. Really, we have

$$a*a_1\neq b*a_1,\quad a\neq b$$

because $<E^*-\{0\},*,1>$ is a group.

Let's denote

$$M_1=\{A_i(0,a_1)\,:\,i=1,...,m\}\,,\quad |M_1|=m.$$

Let $a_2\neq 0$ and $a_2\in E\backslash M_1$. By analogy with above we have:

$$A_1(0,a_2)=a_2$$
$$A_2(0,a_2)=2*a_2$$
$$\cdots\cdots\cdots\cdots$$
$$A_m(0,a_2)=m*a_2$$

and we obtain analogously that the right sides of these equalities are different. Let's denote

$$M_2=\{A_i(0,a_2)\,:\,i=1,...,m\}\,,\quad |M_2|=m$$

If we assume that

$$M_1\,\cap\,M_2\neq\emptyset,$$

i.e. there exists $b\in M_1\,\cap\,M_2$, then there exist such $k,r\in E^*-\{0\}$ that

$$b=A_k(o,a_1)=A_r(o,a_2),$$
$$b=k*a_1=r*a_2$$
$$a_2=r^{(-1)}*k*a_1=k'*a_1\,,\quad k'=r^{(-1)}*k,$$

i.e. $a_2 \in M_1$, contradicting to the choosing of the element a_2. Continuing this process up to the complete exhaustion of the set E, we obtain

$$E \backslash \{0\} = \coprod_{i=1}^{k} M_i \,,$$

moreover, $M_i \cap M_j = \emptyset$ if $i \neq j$, and $|M_i| = m$ for every $i = 1, ..., k$. Then

$$|E - \{0\}| = k \cdot |M_1| \,,$$
$$n - 1 = k \cdot m$$

and Lemma 6 is proved. □

Corollary. *Finite nontrivial (i.e. $m > 1$ and $n > 1$) Frobenius p-group does not exist.*

Proof. Let's assume the contrary and let G be a Frobenius p-group with $m, n > 1$. Then we have

$$|G| = p' \,, \;\; m = |H_0| \mid |G| \;\Rightarrow\; m = p^s, \;\; s > 0,$$
$$n = |A| \mid |G| \;\Rightarrow\; n = p^t, \;\; t > 0.$$

With the help of Lemma 6 we obtain

$$n - 1 = k \cdot m$$
$$p^t - 1 = k \cdot p^s$$
$$p^t - k \cdot p^s = 1$$

that is impossible because the left part of the last equality is divisible by number p, but the right one is not divisible. □

This corollary gives a negative solution of the problem 6.55 from Kourovskaya notebook [5] in the case of a finite Frobenius group.

Lemma 7. *The mappings*

$$\varphi_{b,a}(x) = (b, a, x),$$
$$\psi_{b,a}(x) = (b, a, (0, a^{(-1)}, x)),$$

where $b \in E$, $a \in E^* - \{0, 1\}$ and $a^{(-1)}$ is inverse to a in the group $< E^* - \{0\}, *, 1 >$, form a permutation group, which is isomorphic to *the group G.*

Proof. By means of Lemma 2 we have for $a \in E^*\backslash\{0,1\}$ and $b \in E$:
$\varphi_{b,a}(x) = (b,a,x) = b\cdot(a*(b^{-1}\cdot x)) = b\cdot(a*b^{-1})\cdot(a*x) = \alpha_{c,a}(x)$, where

$$c = b\cdot(a*b^{-1}) = (b,a,0).$$

In a such way it can be represented all the permutations $\alpha_{b,a}$ from G, except the permutations like $\alpha_{b,1}$. Further we obtain

$$\psi_{b,a}(x) = (b,a,(0,a^{(-1)},x)) \\ = b\cdot(a*(b^{-1}\cdot(a^{(-1)}*x))) = b\cdot(a*b^{-1})\cdot x = \alpha_{c,1}(x)$$

where

$$c = b\cdot(a*b^{-1}) = (b,a,0).$$

In a such way it can be represented all the permutations from G like $\alpha_{b,1}$. It means that the set of permutations like $\varphi_{b,a}$ and $\psi_{b,a}$ ($a \in E^*\backslash\{0,1\}$ and $b \in E$) coincides with the set of permutations $\alpha_{b,a}$. By the help of Lemma 2 we obtain that this set of permutations forms a group, which is isomorphic to the group G. □

The mappings like $\varphi_{b,a}$ and $\psi_{b,a}$ are called *right cell permutations of the ternar* (x,t,y) (cf. [7]).

It is evident, that the analogous symmetric constructions can be done for the ternar $[x,t,y]$ too.

4. One sided S-systems of operations, whose cell permutations forms a group

In this paragraph the set E may be as finite as infinite.

Let $A_0(x,y), A_1(x,y), ..., A_m(x,y), ...$ be a collection of binary operations on some set E ($E^* = \{0,1,...,m,...\}$ is the set of indexes of th operations $A_i(x,y)$, and moreover, $E^* \subseteq E$), and let this collection forms a right S-system of indempotent quasigroups $A_1(x,y)$, $i \neq 0,1$, i.e.

$$A_0(x,y) = x\,, \quad A_1(x,y) = y\,, \quad A_i(x,x) = x,$$

$$(A_a \circ A_b)(x, y) = A_a(x, A_b(x, y)) = A_c(x, y) \tag{4}$$

for some $c \in E^* - \{0\}$, moreover, system $< A_u, \circ, A_1 >$, where $u \neq 0$, is a group. Rewrite (4) as a (partial) ternary operation (x, t, y):

$$(\, , \, , \,) \; : \; E \times E^* \times E \to E \,, \quad E^* \subseteq E, \quad 0, 1 \in E,$$
$$(x, t, y) = A_t(x, y),$$

i.e.

$$(x, 0, y) = x \,, \quad (x, 1, y) = y,$$

$$\forall \, a, b \in E^* - \{0\} \; : \; (x, a, (x, b, y)) = (x, c, y) \tag{5}$$

for some $c = c(a, b) \in E^* - \{0\}$,

$$(x, a, x) = x \quad \forall \, x \in E, \quad \forall \, a \in E^*. \tag{6}$$

It is easy to prove that all operations (x, a, y) are mutually orthogonal for different $a \in E^*$. As all the operations (x, a, y) are mutually orthogonal and the identity (6) is true, we obtain that all values $(0, a, 1)$ are different for differenet $a \in E^*$. So renumerating the indexes from E^* it can obtain the following identity $(a \in E^*)$:

$$(0, a, 1) = a. \tag{7}$$

Let's define the following operation $(*)$ on the set E^*:

$$(*) \; : \; E^* * E^* \to E^*,$$
$$0 * a = a * 0 = 0,$$
$$x, y, z \neq 0 \,, \quad x * y = z \Longleftrightarrow (x, a, (x, b, y)) = (x, c, y).$$

As a corollary of (4) and (5) we obtain the system $< E^* - \{0\}, *, 1 >$ is a group. Further we have from (5) when $x = 0$ and $y \in E^* - \{0\}$:

$$(0, a, (0, b, y)) = (0, a * b, 1), \; \forall \, a, b \in E - \{0\}. \tag{8}$$

If $y = 1$, then we obtain from (8) with the help of (7):

$$(0, a, b) = (0, a, (0, b, 1)) = (0, a * b, 1) = a * b.$$

So $\forall \, a, b, y \in E^* - \{0\}$ we obtain from (8):

$$(0, a, (0, b, y)) = (0, a, b * y) = a * (b * y) =$$

$$= (a * b) * y = (0, a * b, y) = (0, (0, a, b), y),$$

i.e. the operation $x \bullet y = (0, x, y)$ on the set $E^* - \{0\}$ is a group, and this operation coincide with the operation $(*)$ from the initial S-system. □

Lemma 8. *The mappings*

$$\varphi_{b,a}(x) = (b, a, x), \quad b \in E, \quad a \in E^* - \{0\},$$
$$\psi_{b,a,d}(x) = (b, a, (d, a^{(-1)}, x)), \quad b, d \in E, \quad a \in E^* - \{0\},$$

are permutations on the set E.

Proof. We have from (5):

$$\varphi_{b,1}(x) = (b, 1, x) = x,$$
$$\psi_{b,a,d}(x) = (b, a, (b, a^{(-1)}, x)) = (b, a * a^{(-1)}, x) = x,$$
$$\psi_{b,1,d}(x) = (b, 1, (d, 1, x)) = x.$$

If $a \in E^* - \{0\}$, then for any arbitrary b and a the mapping $\varphi_{b,a}(x) = L_b^{(a)}(x)$ is a left translation in the quasigroup (x, a, y) with respect to the element b, i.e. it is a permutation. If $a \in E^* - \{0, 1\}$, then for any arbitrary b, a and d we have:

$$\psi_{b,a,d}(x) = L_b^{(a)} L_d^{(a^{(-1)})}(x),$$

i.e. the mapping $\psi_{b,a,d}$ is a composition of two translations: $L_b^{(a)}$ in the quasigroup (x, a, y) and $L_d^{(a^{(-1)})}$ in the quasigroup $(x, a^{(-1)}, y)$; so it is a permutation too. □

Lemma 9. *The following statements are true:*

1) *permutation* $\varphi_{b,a}$ $(b \in E,\ a \in E^* - \{0, 1\})$ *has one and only one fixed element* b,
2) *permutation* $\psi_{b,a,d}$ $(b, d \in E, \quad a \in E^* - \{0, 1\})$ *is a fixed-point-free permutation, if* $b \neq d$,
3) *the set of permutations*
   $T = \{\psi_{b,a_0,0} \ : \ b \in E, \quad a_0$ *is a fixed element from* $E^* - \{0, 1\}\}$
   is transitive on the set E.

Proof. 1) We have

$$\varphi_{b,a}(b) = (b, a, b) = b.$$

Let's assume there exists an element $x_0 \in E,\ x_0 \neq b$ such that

$$\varphi_{b,a}(x_0) = x_0.$$

Then we obtain

$$(b, a, x_0) = x_0.$$

But it is evident that

$$(x_0, a, x_0) = x_0.$$

As the operation (x, a, y) is a quasigroup and $x_o \neq b$ we obtain a contradiction between the last two equalities. So

$$\varphi_{b,a}(x) \neq x$$

for any $x \in E - \{b\}$.

2) Let's assume there exists an element $x_0 \in E$ such that $b \neq d$ and

$$\psi_{b,a,d}(x_0) = x_0,$$

i.e.

$$(b, a, (d, a^{(-1)}, x_0)) = x_0.$$

Then we obtain with the help of (5)

$$(b, a^{(-1)}, x_0) = (b, a^{(-1)}, (b, a, (d, a^{(-1)}, x_0))) =$$
$$= (b, a^{(-1)} * a, (d, a^{(-1)}, x_0)) = (b, 1, (d, a^{(-1)}, x_0)) =$$
$$= (d, a^{(-1)}, x_0),$$

i.e. $b = d$ (because the operation $(x, a^{(-1)}, y)$ is a quasigroup when $a \neq 0, 1$). We obtain a contradiction; so if $b \neq d$, then $\varphi_{b,a,d}(x) \neq x$ for any $x \in E$.

3) Let a_0 be an arbitrary element from $E^* - \{0, 1\}$. We have for an arbitrary fixed element $c \in E$:

$$\varphi_{t,a_0,0}(c) = (t, a_0, (0, a_0^{(-1)}, c)) = (t, a_0, a_0^{(-1)} * c) = R^{(a_0)}_{a_0^{(-1)} * c}(t),$$

where $R_b^{(a)}$ denotes the right translation in the quasigroup (x, a, y) with respect to the element $b \in E$. As the mapping $R^{(a_0)}_{a_0^{(-1)} * c}$ is a permutation on the set E, so for any $c, d \in E$ there exists an element

$t_0 \in E$ such that we have

$$\psi_{t_0,a_0,0}(c) = R^{(a_0)}_{a_0^{(-1)}*c}(t_0) = d,$$

i.e. the set T is a transitive set of permutations on E. □

Lemma 10. *Let permutations $\varphi_{b,a}$ and $\psi_{b,a,d}$ where $b, d \in E$, $a \in E^* - \{0\})$, form a group G under the natural product of permutations. Then G is a Frobenius group.*

Proof is an easy corollary of Lemma 9. □

Lemma 11. *Let the set E be a finite one. If the conditions of Lemma 10 take place, then the set of fixed-point-free permutations*

$$T = \{\psi_{b,a_0,0} \,:\, b \in E, \text{ is any fixed element from } E^* - \{0,1\}\}$$

with the identity permutation $id = \psi_{0,a_0,0}$ is a normal subgroup in the Frobenius group G.

Proof. Let the conditions of Lemma hold. Then G is a finite Frobenius group of permutations of degree n, where $n = |E|$. It is easy to show that the group G contains exactly $n-1$ fixed-point-free permutations (see [4]). As the set T contains exactly $n-1$ different fixed-point-free permutations (see Lemma 9), so T contains all the fixed-point-free permutations of group G.

Let's denote

$$H_a = St_a(G), \quad a \in E.$$

As the set T is a transitive set of permutations on E, so T is a left transversal in the group G to its subgroup H_a for any $a \in E$. So we have

$$t_i^{-1}t_j \notin H_a \quad \forall\, i \neq j.$$

Then we obtain that $t_i^{-1}t_j$ is a fixed-point-free permutation, i.e.

$$t_i^{-1}t_j = t_k$$

for some element $t_k \in T$, because the set T contains all the fixed-point-free permutations of the group G. So all fixed-point-free permutations of the group G with the identity permutation id form a group which is a normal subgroup of the group G. $\square$

By means of Lemmas 10 and 11 we obtain that there exist normal subgroups, consisting from fixed-point-free permutations and the identity permutation, in the finite Frobenius groups, which are groups of cell permutations of the right S-system.

Further we will demonstrate one more method of definition of the operations (x, a, y) by an arbitrary Frobenius group (that method is different from the method described in the part 3; moreover, that method does not use the fact of existing a normal subgroup in the Frobenius group and is independent for the cardinality of the set E.

Let G be an arbitrary Frobenius group of permutations on some set E and $0, 1$ be two distinct distinguished elements from E. As the group G is transitive on the set E, then there exists a set of n permutations $P = \{\sigma_x\}_{x \in E}$ such that $\sigma_x(0) = x \;\; \forall\, x \in E$, and $\sigma_0 = id$. Let's define the operation (x, a, y) as follows:

$$(x, 0, y) = x\,, \quad (x, 1, y) = y\,,$$

$$\begin{gathered} \forall\, a \in E^*,\;\; a \neq 0, 1,\; (x, a, y) = z \Longleftrightarrow z = \alpha(y)\,, \\ \text{where } \alpha \in G,\;\; \alpha(x) = x, \quad \beta(1) = (\sigma_x^{-1} \alpha \sigma_x)(1) = a. \end{gathered} \tag{9}$$

This definition is correct, because there exist an unique permutation $h = H_0 = St_0(G)$ satisfying the condition $h(1) = a$ and so there exist an unique permutation $\alpha \in G$ satisfying the condition (9).

Lemma 12. *The operation* (x, a, y) *(defined by (9)) satisfies the following properties:*

1) $(0, a, 1) = a, \quad (x, a, x) = x,$
2) $\forall\, a, b \in E^* \;:\; (x, a, (x, b, y)) = (x, c, y)$ *for some* $c = c(a, b) \in E^*$.

Proof. 1) We have

$$(0, a, 1) = u \Longleftrightarrow \begin{cases} u = \alpha(1) \\ \alpha(0) = 0 \\ \beta(1) = a \end{cases}$$

which implies $\sigma = id$, $\alpha = \beta$, and in the consequence $u = \alpha(1) = \beta(1) = a$, i.e. $(0, a, 1) = a$.

Similarly

$$(x,a,x)=u \Leftrightarrow \begin{cases} u=\alpha(x) \\ \alpha(x)=x \\ \beta(1)=a \end{cases} \Rightarrow u=\alpha(x)=x,$$

i.e. $(x,a,x)=x$.

2). If $a=0$, then we have

$$(x,a,(x,b,y))=x=(x,0,y) \Rightarrow c=c(0,b)=0.$$

If $b=0$, then we have

$$(x,a,(x,b,y))=(x,a,x)=x=(x,0,y) \Rightarrow c=c(a,0)=0.$$

Let $a,b\neq 0$. Then we obtain

$$(x,a,(x,b,y))=u \Longleftrightarrow \begin{cases} (x,a,v) & = & u \\ (x,b,y) & = & v \end{cases} \Longleftrightarrow$$

$$\Longleftrightarrow \begin{cases} \alpha(x)=x, & \alpha(v)=u \\ \sigma_x^{-1}\alpha\sigma_x=h_a, & h_a(1)=a \\ \alpha_1(x)=x, & \alpha_1(y)=v \\ \sigma_x^{-1}\alpha_1\sigma_x=h_b, & h_b(1)=b \end{cases} \Longleftrightarrow$$

$$\Longleftrightarrow \begin{cases} u=\alpha(v)=\alpha\alpha_1(y) \\ \alpha\alpha_1(x)=\alpha(x)=x \\ \sigma_x^{-1}\alpha\alpha_1\sigma_x=\sigma_x^{-1}\alpha\sigma_x\sigma_x^{-1}\alpha_1\sigma_x=h_ah_b=h_c \\ c=h_c(1)=h_ah_b(1)=h_a(b) \end{cases}$$

$$\Longleftrightarrow \begin{cases} u=\gamma(y)=(c,x,y)=(x,h_a(b),y) \\ \gamma=\alpha\alpha_1 \\ \gamma(x)=x \\ \sigma_x^{-1}\gamma\sigma_x=h_c \end{cases}$$

i.e.

$$(x,a,(x,b,y))=(x,c,y).$$

So we have demonstrated that it can define a right S-system of idempotent operations (x,a,y) over an arbitrary Frobenius group G with the help of equalities (9).

Moreover, it can define the left S-system of idempotent operations

$[x, a, y]$ over an arbitrary Frobenius group G changing symmetrically the definitive equalities (9).

References

[1] **V. D. Belousov**: *Systems of quasigroups with generalized identities*, (Russian), Uspiehi Mat. nauk **20** (1965), 75 – 146.

[2] **V. D. Belousov**: *Algebraic nets and quasigroups* (Russian), "Shtiintsa", Khishinev 1971.

[3] **G. Frobenius**: *Über primitive Gruppen des Grades n under Classe n-1*, S. B. Akad. Berlin, 1902, 455 – 459.

[4] **M. Hall**: *Groups Theory*, (Russian), "Nauka", Moscow 1962.

[5] **Kurovskaya notebook**, 11th edition, Novosibirsk 1992.

[6] **E. A. Kuznetsov**: *Transversal in groups. 1.Elementary properties*, Quasigroups and related systems **1** (1994), 22 – 42.

[7] **E. A. Kuznetsov**: *Sharply 2-transitive permutation groups I.*, Quasigroups and related systems, **2** (1995), 83 – 100.

[8] **H. Wielandt**: *Finite permutation groups*, Acad. Press, N.Y., 1964.

Department of Quasigroups Theory
Institute of Mathematics
Academy of Sciences of Moldova
Academiei str. 5
277028 Kishinau
MOLDOVA

Received November 25, 1995