Zbornik radova Prirodno-matematičkog fakulteta—Univerzitet u Novom Sadu, knjiga 10 (1980)
Review of Research Faculty of Science — University of Novi Sad, Volume 10 (1980)

NONLINEAR MULTIQUASIGROUPS

Zoran Stojaković, Đura Paunić
Prirodno-matematički fakultet. Institut za matematiku.
21 000 Novi Sad, ul. dr Ilije Đuričića 4, Jugoslavija.

In [1] and [2], multiquasigroups, which represent a convenient extension of the class of quasigroups, are defined and their properties and relations to some other structures are investigated. In [2] the notion of linear multiquasigroup is defined and considered. In this paper some properties of isotopies of multiquasigroups are given, and then, the existence of finite nonlinear multiquasigroups is proved. Some mappings by which nonlinear multiquasigroups can be constructed are also given.

1. First we shall give some basic definitions and theorems from [1] and [2]. Notions from the general theory of quasigroups can be found in [3] and [4].

1.1. Let Q be a nonempty set, n, m positive integers and f a mapping of Q^n into Q^m. Then $Q(f)$ is said to be an $[n, m]$-groupoid.

An $[n, m]$-groupoid $Q(f)$ is called an $[n, m]$-quasigroup (or multiquasigroup, when it is not necessary to emphasize n and m) iff for every injection φ from $N_n=\{1, \ldots, n\}$ into N_{n+m} and every $(a_1, \ldots, a_n)\in Q^n$, there exists a unique $n+m$-tuple $(b_1, \ldots, b_{n+m})\in Q^{n+m}$ such that

$$f(b_1, \ldots, b_n)=(b_{n+1}, \ldots, b_{n+m}) \text{ and } b_{\varphi(1)}=a_1, \ldots, b_{\varphi(n)}=a_n.$$

1.2. A sequence $\sum=(f_1, \ldots, f_k)$ of n-ary operations defined on the same nonempty set Q, where $k\geqslant n$, is said to be an orthogonal system of n-ary operations on Q iff for each $(a_1, \ldots, a_n)\in Q^n$ and each injection $\varphi: N_n\to N_k$, there exists a unique $(c_1, \ldots, c_n)\in Q^n$ such that

$$(\forall i\in N_n)\, f_{\varphi(i)}(c_1, \ldots, c_n)=a_i.$$

A sequence $\sum=(f_1, \ldots, f_k)$ of n-ary operations on a set Q is said to be a strongly orthogonal system iff the sequence $\sum_1=(g_1, \ldots, g_n, f_1, \ldots, f_k)$ is an orthogonal system, where $g_1, \ldots, g_n$ are defined by $(\forall i\in N_n)\, g_i(x_1, \ldots, x_n)=x_i$.

In a strongly orthogonal system of n-ary operations on a set Q all n-ary operations are n-quasigroups.

An orthogonal system of n-quasigroups for $n=2$ is a strongly orthogonal system, but for $n>2$ a system of n-quasigroups which is an orthogonal system need not be strongly orthogonal.

1.3. If $Q(f)$ is an $[n, m]$-quasigroup and if n-ary operations $g_1, \ldots, g_{n+m}$ on Q are defined by

$$f(x_1, \ldots, x_n)=(x_{n+1}, \ldots, x_{n+m}) \Leftrightarrow (\forall i \in N_{n+m})\ x_i=g_i(x_1, \ldots, x_n),$$

then an orthogonal system of n-ary operations is obtained. The system $g_{n+1}, \ldots, g_{n+m}$ is a strongly orthogonal system of n-ary quasigroups.

The following proposition shows that there is an equivalence between the notions of the orthogonal system of operations and multiquasigroups:

An $[n, m]$-groupoid $Q(f)$ is an $[n, m]$-quasigroup iff there exists an orthogonal system of n-ary operations $g_1, \ldots, g_{n+m}$ such that

$$f(x_1, \ldots, x_n)=(x_{n+1}, \ldots, x_{n+m}) \Leftrightarrow (\exists\, t_1, \ldots, t_n \in Q)\ (\forall i \in N_{n+m})\ x_i=g_i(t_1, \ldots, t_n).$$

2. Now we shall consider isotopies of multiquasigroups.

2.1. An $[n, m]$-groupoid $Q(g)$ is said to be isotopic to an $[n, m]$-groupoid $Q(f)$ iff there exists a sequence $\varphi_1, \ldots, \varphi_{n+m}$ of permutations of Q such that

$$f(x_1, \ldots, x_n)=(x_{n+1}, \ldots, x_{n+m}) \Leftrightarrow g(\varphi_1(x_1), \ldots, \varphi_n(x_n))=$$

$$(\varphi_{n+1}(x_{n+1}), \ldots, \varphi_{n+m}(x_{n+m})).$$

$Q(g)$ is called an isotope of the multigroupoid $Q(f)$, and the sequence $T=(\varphi_1, \ldots, \varphi_{n+m})$ is called an isotopy of the multigroupoids $Q(f)$ and $Q(g)$. By $Q(g)=Q(f)^T$ we denote that $Q(g)$ is isotopic to $Q(f)$ with the isotopy T.

If $\varphi_1=\ldots=\varphi_n=\varphi_{n+1}^{-1}=\ldots=\varphi_{n+m}^{-1}$ then $Q(f)$ and $Q(g)$ are isomorphic.

2.2. If $[n, m]$-groupoids $Q(f)$ and $Q(g)$ are isotopic then: $Q(f)$ is an $[n, m]$-quasigroup $\Leftrightarrow$ $Q(g)$ is an $[n, m]$-quasigroup.

2.3. The isotopy is an equivalence relation in the set of all $[n, m]$-quasigroups defined on the same set Q.

The set of all isotopies of an $[n, m]$-quasigroup is a group with respect to the multiplication of isotopies defined by

$$(\varphi_1, \ldots, \varphi_{n+m})(\psi_1, \ldots, \psi_{n+m})=(\varphi_1\psi_1, \ldots, \varphi_{n+m}\psi_{n+m}).$$

2.4. Let $Q(f)$ and $Q(g)$ be isotopic $[n, m]$-quasigroups with an isotopy $T=(\varphi_1, \ldots, \varphi_{n+m})$, $Q(g)=Q(f)^T$. The isotope $Q(g)$ of the $[n, m]$-quasigroup $Q(f)$ is called principal iff $\varphi_{n+1}=\ldots=\varphi_{n+m}=\varepsilon$, where ε is the identity mapping of the set Q. The isotopy T is then called a principal isotopy.

The following proposition is then valid.

Let $Q(f)$ be an $[n, m]$-quasigroup. An isotope $Q(g)$, $Q(g)=Q(f)^{(\varphi_1, \ldots, \varphi_{n+m})}$ is isomorphic to a principal isotope of the $[n, m]$-quasigroup $Q(f)$ iff $\varphi_{n+1}=\ldots=\varphi_{n+m}$.

3. In [2] a class of multiquasigroups which are called linear is defined, some of their properties are investigated and some conditions on the existence of such multiquasigroups are given. Here we shall prove the existence of finite nonlinear multiquasigroups, and give mappings by which such multiquasigroups can be constructed.

3.1. Let F be a field and $A=[a_{ij}]$ and $n\times(n+m)$ matrix over F such that every minor of A of order n is nonsingular. If a mapping $f: F^n\to F^m$ is defined by

$$f(x_1, \ldots, x_n)=(x_{n+1}, \ldots, x_{n+m})\Leftrightarrow(\exists\,(t_1, \ldots, t_n)\in F^n)\ \mathbf{x}=\mathbf{t}A,$$

where $\mathbf{x}=[x_1, \ldots, x_{n+m}]$, $\mathbf{t}=[t_1, \ldots, t_n]$, then we get an $[n, m]$-quasigroup $F(f)$.

3.2. Putting in 3.1. $\mathbf{t}=[x_1, \ldots, x_n]$, the following proposition is obtained:

Let $A=[a_{ij}]$ be an $n\times m$ matrix over a field F, such that every minor* of A is nonsingular. If a mapping $f: F^n\to F^m$ is defined by

$$f(x_1, \ldots, x_n)=(y_1 \ldots, y_m)\Leftrightarrow\mathbf{y}=\mathbf{x}A,$$

where $\mathbf{x}=[x_1 \ldots, x_n]$, $\mathbf{y}=[y_1, \ldots\ y_m]$, then an $[n, m]$-quasigroup $F(f)$ is obtained.

It is clear that, if an $n\times m$ matrix A defines an $[n, m]$-quasigroup, then the transpose A^T of the matrix A defines an $[m, n]$-quasigroup. Also, every $p\times q$ submatrix of A defines a $[p, q]$-quasigroup.

3.3. For every Galois field $F=GF(p^k)$, $F\neq GF(2)$ and $F\neq GF(3)$, there exist $p^k(p^k-1)((p^k-2)!-1)$ permutations of F which are not linear functions.

For, there exist $p^k(p^k-1)$ linear functions $f(x)=ax+b$ $(a\neq 0)$, which are permutations of F, but there exist $p^s!$ permutations of F. If

$$p^k!>p^k(p^k-1) \tag{1}$$

then there exist $p^k(p^k-1)((p^k-2)!-1)$ nonlinear permutations of F. If $k=1$ then (1) is satisfied for every prime $p\geq 5$, and for $k\geq 2$ for every prime $p\geq 2$.

It is easy to see that for $GF(2)$ and $GF(3)$ all permutations are linear functions.

3.4. For every linear $[n, m]$-quasigroup $F(f)$ defined a on Galois field $F=GF(p^k)$, $F\neq GF(2)$ and $F\neq GF(3)$, there exist at least $(p^k!)^m-(p^k(p^k-1))^m$ different nonlinear $[n, m]$-quasigroups which are isotopic to $F(f)$.

Proof. Let $F=GF(p^k)$ be a Galois field and $F(f)$ a linear quasigroup. Then, according to 3.2. f can be represented in the form $f(x_1, \ldots, x_n)=(l_1, \ldots, l_m)$, where $l_1, \ldots, l_m$ are linear functions of $x_1, \ldots, x_n$, i. e. $l_j=\sum_{k=1}^{n}\lambda_{jk}x_k$, $\lambda_{jk}\in F$, $j=1, \ldots, m$. We shall consider an isotope $F(f_1)$ of the $[n, m]$-quasigroup $F(f)$ defined by $f(x_1, \ldots, x_n)=(g_1(l_1), \ldots, g_m(l_m))$, where g_j, $j=1, \ldots, m$ are permutations of F. By 2.2. it follows that $F(f_1)$ is also an $[n, m]$-quasigroup, and we shall prove that $F(f_1)$ is a nonlinear $[n, m]$-quasigroup if at least one function g_j is nonlinear.

Every mapping of F is uniquely determined by its interpolating polynomial. For, the degree of an interpolating polynomial which goes through p^k points is at most p^k-1, and different polynomials of degree not greater than p^k-1 always define different functions, because $x^s\neq x$ for every $s<p^k$. $l_1, \ldots, l_m$ are linear functions, so the degree of a polynomial $g(x)$ is the same as the degree of $g(l_j)$.

* of order k, $k=1, \ldots,$ min (n, m).

This means that if a function g_j is nonlinear, then $g_j(l_j)$ is also nonlinear, so $f_1(x_1, \ldots, x_n)=(g_1(l_1), \ldots, g_m(l_m))$ can not be a linear $[n, m]$-quasigroup.

If g_j, h_j are different functions on F, $g_j \neq h_j$, then $g_j(l_j) \neq h_j(l_j)$. So, if $T=(\varepsilon, \ldots, \varepsilon, g_1, \ldots, g_m)$ and $T_1=(\varepsilon, \ldots, \varepsilon, h_1, \ldots, h_m)$, where ε is the identity mapping, are two different isotopies of the $[n, m]$-quasigroup $F(f)$ then $[n, m]$-quasigroups $Q(f)^T$ and $Q(f)^{T_1}$ are different. From 3.3. it follows that there are $(p^k!)^m-(p^k(p^k-1))^m$ different isotopies of the form $(\varepsilon, \ldots, \varepsilon, g_1, \ldots, g_m)$, where at least one g_j is nonlinear. Hence, for linear $[n, m]$-quasigroup $F(f)$ there exist at least $(p^k!)^m-(p^k(p^k-1))^m$ nonlinear isotopic $[n, m]$-quasigroups.

3.5. We shall show how a nonlinear permutation of any Galois field $GF(p^k)$ can be constructed, $p^k \neq 2$, $p^k \neq 3$.

a) $k=1$. Let $g(x)=x^{p-2}$. Because of the small Fermat theorem $x^{p-1}=1$ for $x \neq 0$, hence $g(x)=x^{-1}$ for $x \neq 0$ and $g(0)=0$, so g is a permutation. Suppose that g is linear, i.e. $x^{p-2}-ax-b=0$ for all x from $GF(p)$. Then the polynomial equation of degree $p-2$ has p solutions, which is impossible.

b) $k \geqslant 2$. Let $g(x)=x^p$. The mapping g is an automorphism of $GF(p^k)$, so it is a bijection. If $x^p-ax-b=0$ for all x from $GF(p^k)$ then the polynomial equation of degrree p has p^k solutions which is impossible.

REFERENCES

[1] G. Čupona, J. Ušan, Z. Stojaković, *Multiquasigroups and some related structures*, Prilozi MANU, I/1, 1980.

[2] G. Čupona, Z. Stojaković, J. Ušan, *On finite multiquasigroups*, Publ. Inst. Math., T. 29 (43).

[3] Белоусов В. Д., *n-арные квазигруппы*, Кишинев, 1972.

[4] Dénes J., Keedwell A. D., *Latin squares and their applications*, Akadémiai Kiadó, Budapest, 1974.

NELINEARNE MULTIKVAZIGRUPE

Zoran Stojaković, Đura Paunić

REZIME

U radovima [1] i [2] definisane su multikvazigrupe, koje predstavljaju pogodnu generalizaciju pojma kvazigrupe, i razmotrene njihove osobine i veze sa nekim drugim strukturama. U [2] je definisan pojam linearne multikvazigrupe i navedene su neke osobine takvih multikvazigrupa. U ovom radu najpre su navedene neke osobine izotopije multikvazigrupa, a zatim je dokazana egzistencija konačnih nelinearnih multikvazigrupa. Takođe su date funkcije pomoću kojih se nelinearne multikvazigrupe mogu konstruisati.