PUBLICATIONS DE L'INSTITUT MATHÉMATIQUE
Nouvelle série, tome 29 (43), 1981, pp. 53–59

ON FINITE MULTIQUASIGROUPS

Georgi Čupona, Zoran Stojaković, Janez Ušan

In the present paper multiquasigroups and their relations to orthogonal systems of operations and codes are studied. In the first part of the paper the notion of an $[n, m]$-quasigroup of order q is defined and it is shown that for $n, m, q \geq 2$ it follows that $m \leq q-1$, in the second part, as a corollary of the preceding result, an upper bound for the maximal number of n-ary operations in an orthogonal system of operations on a set with q elements is obtained. In the third part the existence of a class of multiquasigroups is shown, and in the fourth part a connection between multiquasigroups and a special kind of code is pointed out.

In the paper some result from [4] are used, but it is possible to read it independently.

1. Let Q be a finite, nonempty set with q elements, n, m positive integers and f a mapping of Q^n into Q^m. The structure $Q(f)$ is said to be an $[n, m]$-quasigroup, or simply multiquasigroup, iff the following condition is satisfied:

(A) For every injection φ from $N_n = \{1, \dots, n\}$ into N_{n+m} and every sequence $a_1, \dots, a_n \in Q$, there exists a unique sequence $b_1, \dots, b_{n+m} \in Q$ such that:

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

q is called the order of $Q(f)$.

One of the tasks of the paper is to discuss triples of natural numbers (n, m, q) for which $[n, m]$-quasigroups of order q exist. It is clear that: (i) $Q(f)$ is an $[n, 1]$-quasigroup iff $Q(f)$ is an n-quasigroup; (ii) $Q(f)$ is an $[1, m]$-quasigroup iff there exist permutations $f_1, \dots, f_m$ of Q such that $f(x) = (f_1(x), \dots, f_m(x))$; (iii) for each pair of natural numbers n, m there exists an $[n, m]$-quasigroup of order 1. Therefore, in the sequel we shall assume that $n, m, q \geq 2$.

First, we shall prove that the following proposition:

1°. If $m, n, q \geq 2$ and if there exists an $[n, m]$-quasigroup of order q, then

$$m \leq q-1. \tag{1}$$

PROOF. First, we note that if $Q(f)$ is a $[2,m]$-quasigroup and if we put

$$\begin{aligned}
&P = \{(x_1,\dots,x_{m+2}) \mid f(x_1,x_2) = (x_3,\dots,x_{m+2})\},\\
&b_x^i = \{(x_1,\dots,x_{m+2}) \in P \mid x_i = x\},\\
&B_v = \{b_x^v \mid x \in Q\}, \quad B_1 = B_1 \cup \dots \cup B_{m+2},
\end{aligned}$$

we get a $m+2$-net (where P is the set of points, B is the set of blocks i.e. lines, and the incidence is the ordinary belonging) of order q ([4]). It is well known that from here it follows (see [1], p. 9) that $m+2 \le q+1$, e.i. (1).

Now, we shall assume that $Q(f)$ is an $[n,m]$-quasigroup of order q, where $n = p+2$, $p \ge 1$. If $a_1,\dots,a_p$ is an arbitrary sequence of elemets from Q, and if we put

$$f'(x,y) = f(a_1,\dots,a_p,x,y),$$

we get a $[2,m]$-quasigroup $Q(f')$. From here, considering the preceding result, it follows that $m \le q-1$.

As a corollary of the preceding we get:

1.1. If $m,n \ge 2$, then there does not exist an $[n,m]$-quasigroup of order 2.

2. Let $\Sigma = (f_1,\dots,f_k)$ be a sequence of n-ary operations defined on the same set Q, where $k \ge n$. Σ is said to be an orthogonal system of n-ary operations on Q (OSnO) iff the following condition is satisfied:

(B) For every injection $\varphi\colon N_n \to N_k$ the maping

$$(x_1,\dots,x_n) \mapsto (y_{\varphi(1)},\dots,y_{\varphi(n)})$$

is a permutation of Q^n, where $y_v = f_v(x_1,\dots,x_n)$.

A sequence $\Sigma = (f_1,\dots,f_k)$ on n-ary operations on a set Q is said to be a strongly orthogonal system, iff the sequence $\Sigma_1 = (g_1,\dots,g_n,f_1,\dots,f_k)$ is an orthogonal system, where $g_1,\dots,g_n$ are defined by:

$$(\forall i \in N_n) g_i(x_1,\dots,x_n) = x_i.$$

It can be easily proved that in a strongly orthogonal system all n-ary operations are n-quasigroups.

A system of binary quasigroups is orthogonal iff it is strongly orthogonal, but for $n > 2$ a system of n-quasigroups which is orthogonal need not be strongly orthogonal[1]).

We shall show that:

2°**.** If n, $q \ge 2$ and if $(f_1,\dots,f_k)$ is an OSnO on a set Q with q elements, then

$$k \le n+q-1. \tag{2}$$

[1]An example fot this are four ternary quasgroups given in [2] on pages 181 and 182.

Proof. For $k = n$ and $k = n + 1$ there is nothing to prove. So, we shall assume that $k = n + m$, where $m \geq 2$. If a mapping $f\colon Q^n \to Q^m$ is defined by

$$f(x_1, \dots, x_n) = (x_{n+1}, \dots, x_k) \Leftrightarrow$$
$$(\exists t_1, \dots, t_n \in Q) x_1 = f_1(t_1, \dots, t_n), \dots, x_k = f_k(t_1, \dots, t_n),$$

we get an $[n, m]$-quasigroup $Q(f)$, and from 1° it follows that $m = k - n \leq\geq q - 1$, i.e. (2).

As a corollary of 2° we get the following:

2.1. If n, $q \geq 2$, then the number of n-ary operations in an OSnO defined on a set with q elements is bounded, and if $\omega_n(q)$ is the maximal number of elements in such a system, then

$$\omega_n(q) \leq n + q - 1. \tag{2.1}$$

From 2° it follows also that the maximal number of n-ary operations in a stongly orthogonal system on a set with q elements is not greater than $q - 1$.

We note that in [3] (the same result is quoted in [2]) the following theorem is proved:

2.2. If $n \geq 2$, $q \geq 3$ and if $\pi_n(q)$ denotes the maximal number of n-quasigroups which make an orthogonal system of n-quasigroups on a set with Q elements, then

$$\pi_n(q) \leq (n-1)(q-1). \tag{2.2}$$

Since every orthogonal system of n-quasigroups is also an OSnO, we have $\pi_n(q) \leq \omega_n(q)$, so (2.1) improves (2.2).

It is easy to see that the upper bound for $\pi_n(q)$ is:

(i) better in (2.2) for $n = q = 3$ and for $n = 2$, q arbitrary;

(ii) the same in (2.1) and (2.2) for $n = 3$, $q = 4$ and for $n = 4$, $q = 2$;

(iii) better in (2.1) in all other cases.

Using the corresponding result on the nonexistence of an OSnO, we get that:

2.3. If n, $m \geq 2$ then there does not exist an $[n, m]$-quasigroup of order 6.

Proof. If $Q(f)$ is an $[n, m]$-quasigroup and if $f_1, \dots, f_m$ are defined by

$$f(x_1, \dots, x_n) = (y_1, \dots, y_m) \Leftrightarrow y_v = f_v(x_1, \dots, x_n)$$

a system of n-quasigroups is obtained. For $m \geq n$ this system is orthogonal. So, if we define a $[2, m]$-quasigroup $Q(f')$ as in the proof of 1°, then we obtain an orthogonal system of binary quasigroups $f_1{}', \dots, f_m{}'$ and such a system, as it is well known, for $m \geq 2$, $q = 6$ does not exist.

3. All the results of the two preceding have "negative character", i.e. they consider the cases in which there do not exist multiquasigroups. Here, we shall show the existence of a class of multiquasigroups which we shall call linear multi-quasigroups.

3°. Let F be a field and $A = [a_{ij}]$ an $n \times (m+n)$ matrix over F such that every minor of A of order n is nonsingular. If a mapping $f\colon F^n \to F^m$ is defined by

$$f(x_1, \dots, x_n) = (x_{n+1}, \dots, x_{n+m}) \Leftrightarrow (\exists \mathbf{t} \in F^n)\mathbf{x} = \mathbf{t}A, \tag{3}$$

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

Proof. Let $\mathbf{c} = (c_1, \dots, c_n) \in F^n$ be a sequence of elements from F, and φ an injection from N_n into N_{n+m}. The matrix $B = [b_{ij}]$ of order n, where $b_{ij} = a_{i\varphi(j)}$, is nonsingular, which means that the equation $\mathbf{c} = \mathbf{t}B$ has a unique solution $\mathbf{t} = \mathbf{c}B^{-1}$, and from here we get that there exist a unique sequence $\mathbf{b} = (b_1, \dots, b_{n+m}) \in F^{n+m}$ such that $b_{\varphi(v)} = c_v$ and $\mathbf{b} = \mathbf{t}A$, i.e. $f(b_1, \dots, b_n) = (b_{n+1}, \dots, b_{n+m})$.

Putting in 3° $\mathbf{t} = (x_1, \dots, x_n)$ the following proposition is obtained:

3.1. Let $A = [a_{ij}]$ be an $n \times m$ matrix over a field F, such that every minor[2] of A is nonsingular. If a mapping $f\colon F^n \to F^m$ is defined by

$$f(x_1, \dots, x_n) = (y_1, \dots, y_m) \Leftrightarrow \mathbf{y} = \mathbf{x}A, \tag{3.1}$$

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

It is clear that, if an $n \times m$ matrix A defines an $[m,n]$-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.

From 3.1. it follows that if a matrix A with nonsigular minors can be defined over a Galois field $F = GF(p^\alpha)$, then the corresponding linear multiquasigroup is obtained. We get some examples.

3.1) $F = GF(3) = \{0, 1, -1\}$, $n = m = 2$, $A = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$,

$$f(x,y) = (u,v) \Leftrightarrow u = x + y, \quad v = x - y.$$

3.2) $F = GF(5) = \{0, 1, 2, -1, -2\}$

$$A_1 = \begin{bmatrix} 1 & 1 \\ 1 & 2 \\ 1 & -1 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & -1 \end{bmatrix}, \quad A_3 = \begin{bmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{bmatrix}$$

$$f_1(x,y,z) = (u,v) \Leftrightarrow z = x + y + z, \quad v = x + 2y - z,$$

$$f_2(x,y) = (u,v,w) \Leftrightarrow u = x + y, \quad v = x + 2y, \quad w = x - y$$

$$f_3(x,y,z) = (u,v,w) \Leftrightarrow u = 2x + y + z, \quad v = x + 2y + z, \quad w = x + y + 2z.$$

[2] Of order k, $k = 1, \dots, \min(n,m)$.

It is natural to ask when a matrix A with nonsingular minors can be constructed over a field F. A sufficient condition gives the following proposition.

3.2. If F is a finite field with q elements and if m and n are positive integers such that

$$\sum_i \binom{n-1}{i} \binom{m-1}{i} < q, \tag{3.2}$$

then there exists an $n \times m$ matrix $A = [a_{ij}]$ such that every minor of A is nonsingular.

PROOF. It is clear that the proposition is true for $n = 1$ or $m = 1$, hence, we shall assume that $n, m \geq 2$. If (3.2) is true then the inequality

$$\sum_i \binom{k-1}{i} \binom{s-1}{i} < q \tag{3.2$'$}$$

is also true for every $k \leq n$, $s \leq m$. We shall suppose that $k < n$, $s < m$ and that we have constructed the matrices

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ a_{k1} & a_{k2} & \cdots & a_{km} \end{bmatrix} = B, \qquad \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1s} \\ a_{21} & a_{22} & \cdots & a_{2s} \\ \cdots & \cdots & \cdots & \cdots \\ a_{k1} & a_{k2} & \cdots & a_{ks} \\ a_1 & a_2 & \cdots & a_s \end{bmatrix} = C,$$

with nonsingular minors. The proof will be completed if we show that there exists an element $b \in F$ such that all minors of the matrix

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1s} & a_{1s+1} \\ a_{21} & a_{22} & \cdots & a_{2s} & a_{2s+1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{k1} & a_{k2} & \cdots & a_{ks} & a_{ks+1} \\ a_1 & a_2 & \cdots & a_s & b \end{bmatrix} = D,$$

are nonsingular. It is clear that D has

$$\binom{k}{0} \binom{s}{0} + \binom{k}{1} \binom{s}{1} + \binom{k}{2} \binom{s}{2} + \cdots$$

minors in which b appears, and every such minor is singular only for one value of b, i.e. there exist at most $\sum_i \binom{k}{i} \binom{s}{i}$ values of b for which a minor of D in which b appears is singular. From (3.2) it follows that we can find b such that all minors of D are nonsigular, which completes the proof.

The matrix A_3 from the example 3.2) shows that, in general, the condition (3.2) is not necessary for the existence of a matrix with the given property.

A corollary of 3.2. is the following:

3.3. For every pair of natural numbers $m, n \geq 2$ and every prime p, there exist an infinite number of natural numbers α such that ther exist an $[n, m]$-quasigroup of order $q = p^{\alpha}$.

It is clear that the propositions 3° and 3.1. can be formulated in a more general form, where instead of a field we use a commutative and associative ring with identity, and the term "nonsigular minor" we replace by "invertible square submatrix". As a consequence of such more general proposition, we get:

3.4. If there exists an integer $n \times m$ matrix $A = [a_{ij}]$, such that every minor A is relatively prime with q, then there exists an $[n, m]$-quasigroup of order q.

Proof. If we consider A as a matrix over the ring $Z_q = Z/qZ$ (of residue classes modulo q) we get that every minor of A is invertible.

We give some examples.

3.3) Using the matrix $\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$ we can construct a $[2, 2]$-quasigroup of any odd oder.

The matrix

$$\begin{bmatrix} -2 & 1 & -1 \\ -1 & 2 & -1 \\ 1 & -1 & 2 \end{bmatrix}$$

defines a $[3, 3]$-quasigroup of order q, where q is any natural number relatively prime with 6.

4. Multiquasigroups can be interpreted as a special kind of relations, i.e. codes. First, every subset K of Q^k is called a k-code over Q. Two elements $a_1 \cdots a_k$ and $b_1 \cdots b_k$ form Q^k are said to be on a distance d iff they differ in exactly d components. If d is the minimal distance between different sequences from K, then we say that K has the code distance d. It is easy to see that the following proposition is valid:

4° If $Q(f)$ is an $[n, m]$-quasigroup of order q and if a code K is defined by

$$a_1 \cdots a_{m+n} \in K \Leftrightarrow f(a_1, \ldots, a_n) = (a_{n+1}, \cdots, a_{n+m}), \tag{4}$$

then a $m + n$-code with q^n elements and of the code distance $m + 1$ is obtained. And conversely, if K is a $m + n$-code with q^n elements and of the code distance $m + 1$ over a set Q with q elements, then by (4) an $[n, m]$-quasigroup of order q is defined.

From the above proposition it follows that there exists an equivalence between multiquasigroups and a special kind of codes.

It is natural to ask what structure $Q(f)$ is defined by (4) if it is given only that K is a $m + n$-code of the code distance $d = m + 1$. In this case, a partial $[n, m]$-quasigroup $Q(f)$ is obtained (the definition of which we shall not give here). In [4] it is shown that every partial $[n, m]$-quasigroup can be completed to an $[n, m]$-quasigroup, but then the carrier of the multiquasigroup is essentially enlarged, and this is not of interest in the case when the carrier is finite.

REFERENCES

[1] В. Д. Белоусов, *Конфигурации в алгебраических сетях*, Кишинев, Штиинца, 1979.

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

[3] L. Humblot, *Sur une extension de la notion de carrés latin,* C. R. Acad. Sci. Paris 273 (1971), 795–798.

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