Zbornik radova Prirodno-matematičkog fakulteta — Univerzitet u Novom Sadu, knjiga 8 (1978)
Review of Research Faculty of Science — University of Novi Sad, Volume 8 (1978)

Janez Ušan, Zoran Stojaković

ORTHOGONAL SYSTEMS OF PARTIAL OPERATIONS

In this paper we consider some properties of orthogonal systems of partial operations and partial quasigroups and establish connections between these systems and a class of codes of fixed code distance.

Let Q be a nonempty set and $D \subseteq Q \times Q$, $D \neq \emptyset$. If A is a mapping of D into Q, then (Q, A) is said to be a partial groupoid.

A partial quasigroup is a partial groupoid (Q, A) such that if the equations $A(x, b)=c$ and $A(a, y)=c$ have solutions for x and y in Q, then these solutions are unique.

Let (Q, A) and (Q, B) be partial groupoids of the same domain $D=\mathcal{D}A=\mathcal{D}B$, $D \subseteq Q \times Q$. A and B are said to be orthogonal iff for every $a, b \in Q$ for which the system of equations

$$A(x, y)=a, \quad B(x, y)=b,$$

has a solution, this solution is unique[1].

If we introduce

$$O_{AB}(x, y) \overset{\text{def.}}{=\!=} (A(x, y), B(x, y)),$$

then A and B can be said to be orthogonal, iff O_{AB} is a bijection of the set D on the set $\mathcal{R}O_{AB}$ (by $\mathcal{R}O_{AB}$ we denote the range of O_{AB}).

The orthogonal operations A and B will be said to be regularly orthogonal iff for every $(i, j) \in \mathcal{R}O_{AB}$ there exists $j' \in Q$, $j' \neq j$, such that $(i, j') \in \mathcal{R}O_{AB}$ or there exists $i' \in Q$, $i' \neq i$, such that $(i', j) \in \mathcal{R}O_{AB}$ ([4]).

The orthogonal operations A and B will be called compatibly orthogonal iff $\mathcal{D}A=(\mathcal{D}B=)\ \mathcal{R}O_{AB}$.

In non-partial case every pair of orthogonal operations is regularly orthoigonal and compatibly orthogonal.

The set of different partial operations of the same domain will be said to be an orthogonal system of partial operations (OSPO) iff each pair of the operations of this set is orthogonal. If each pair of the operations is regularly orthogonal then we call such a system a regularly orthogonal system of partial operations, and if each pair of the operations is compatibly orthogonal then we call such a system a compatibly orthogonal systems of partial operations.

[1] If (Q, A) is a partial groupoid such that the set Q has q elements and the set $\mathcal{D}A$ has p elements, then if $p \leqslant q$ it is possible that (Q, A) be orthogonal to itself. If $p > q$ two orthogonal operations are always different.

Let θ be a permutation of the set $\mathcal{D}A$ and let

$$\theta A(x, y) \overset{\text{def.}}{=\!=} A\theta(x, y)$$

and

$$\theta\{A_1, A_2, \ldots, A_n\} \overset{\text{def.}}{=\!=} \{\theta A_1, \theta A_2, \ldots, \theta A_n\},$$

where the partial operations $A_1, A_2, \ldots, A_n$ have the same domain.

Theorem 1. (i) If F and E are in turn left and right partial identity operations of the same domain[1] then F and E are orthogonal.

(ii) A partial operation K is orthogonal to F and E iff K is a partial quasigroup.

(iii) If Σ is an orthogonal system of partial operations and $A_t \in \Sigma$, θ is a permutation of $\mathcal{D}A_t$, then $\theta\Sigma$ is an orthogonal system of partial operations.

(iv) If in an orthogonal system of partial operations at least one pair of operations is compatibly orthogonal, then there exists a permutation θ of the set $\mathcal{D}A_t$ $A_t \in \Sigma$, such that operations F and E belong to $\theta\Sigma$ and the system $\theta\Sigma \setminus \{F, E\}$, when it contains more than two elements, consists only of partial quasigroups,

(v) A regular and compatible orthogonality of a system Σ are invariant. under a permutation θ of the set $\mathcal{D}A_t$, $A_t \in \Sigma$.

Proof. From the definition of orthogonality and compatible orthogonality of operations A, B and the fact that

$$\mathcal{D}A = \mathcal{D}B = \mathcal{RO}_{AB} = \mathcal{RO}_{\theta A\, \theta B}$$

where $\theta \in (\mathcal{D}A)!$, we find that (iii) and (v) are valid.

The proofs of (i), (ii) and (iv) are similar to the proofs of corresponding theorems in non-partial case.

Because of (iii) we can define the conjugacy as in the non-partial case:

OSPO Σ is conjugate to OSPO Σ' iff there exists θ such that $\Sigma' = \theta\Sigma$.

From (iv) we get that we can define, as in the non-partial case, an orthogonal system of partial quasigroups (OSPQ):

An OSPO Σ is OSPQ iff Σ contains partial identity operations F and E.

The following theorem generalizes the main result from [2].

Theorem 2. To every orthogonal system of partial operations $\Sigma = \{A_1, A_2, \ldots, A_k\}$, $k \geqslant 2$, in which all operations are defined on a set Q of $q \in N$ elements, the set $\mathcal{D}A_t$ has p elements and $q < p \leqslant q^2$, there corresponds a code of p k-sequences of code distance[2] k-1 over an alphabet of q letters, $q < p \leqslant q^2$, and vice versa.

---

[1] $F(x, y) \overset{\text{def.}}{=\!=} x$, $E(x, y) \overset{\text{def.}}{=\!=} y$ for every $(x, y) \in \mathcal{D}F = \mathcal{D}E$.

[2] A code of k-sequences from a nonempty set Q is said to be of distance d iff each two different sequences from the code differ in at least d coordinates.

Proof. If

$$(1)\quad \begin{cases} (z_1^{(1)}, \ldots, z_i^{(1)}, \ldots, z_j^{(1)}, \ldots, z_k^{(1)}), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ (z_1^{(s)}, \ldots, z_i^{(s)}, \ldots, z_j^{(s)}, \ldots, z_k^{(s)}), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ (z_1^{(t)}, \ldots, z_i^{(t)}, \ldots, z_j^{(t)}, \ldots, z_k^{(t)}), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ (z_1^{(p)}, \ldots, z_i^{(p)}, \ldots, z_j^{(p)}, \ldots, z_k^{(p)}), \end{cases}$$

is a code of p k-sequences over the alphabet of q letters, then the following equivalence is valid:

(1) is a code of the code distance k-1 iff for every $i, j \in \{1, 2, \ldots, k\}$, $i \neq j$, and every $s, t \in \{1, 2, \ldots, p\}$, $s \neq t$, we have $z_i^{(s)} \neq z_i^{(t)}$ or $z_j^{(s)} \neq z_j^{(t)}$.

Since the domain $\mathcal{D} A_i$ has p elements we can index its elements by elements from the set $\{1, 2, \ldots, p\}$. The result of applying the operation A_i to the pair $(x_1, x_2) \in \mathcal{D}A_i$, which is indexed by s ,we shall denote by

$$A_i(x_1, x_2) = z_i^{(s)}.$$

The following equivalence is then valid:

Σ is an OSPO defined on the set Q iff for every $i, j \in \{1, 2, \ldots, k\}$, $i \neq j$, and for every $s, t \in \{1, 2, \ldots, p\}$, $s \neq t$, we have $(z_i^{(s)}, z_j^{(s)}) \neq (z_i^{(t)}, z_j^{(t)})$.

Since $\mathcal{R}O_{AB} \subseteq Q \times Q$ and the code is of code distance $k-1$, we get that $p \leqslant q^2$.

These two equivalences prove the theorem.

The main result from [2] considers the non-partial case: $p = q^2$. When there exists an OSO of $k \geqslant 2$ elements the corresponding code is maximal and has $p = q^2$ elements. However, for example, for $k = 4$ and $q = 6$ an OSO does not exist[3]. According to Theorem 2 of the present paper, the determination of the maximal code of 4-sequences of code distance 3 over an alphabet of 6 letters is equivalent to the determination of the OSPO of 4 operations defined on the set of 6 elements, with the maximal cardinality of its domain.

In a similar way the n-ary analogue (Theorem 1 from [3]) of the main result from [2] can be generalised for the partial case:

Theorem 2'. To every orthogonal system of n-ary partial operations $\Sigma = \{A_1, A_2, \ldots, A_k\}$, $k \geqslant n$, in which all partial operations are defined on a set of q elements, the set $\mathcal{D} A_i$ has p elements and $q < p \leqslant q^n$, there corresponds a code of p k-sequences, $k \geqslant n$, of code distance $k-(n-1)$ over an alphabet of q letters, $q < p \leqslant q^n$, and vice versa.

[3] Because there does not exist a pair of orthogonal quasigroups on the set of 6 elements.

Theorem 3. To every code of p k-sequences, $k \geqslant 2$, of code distance k-1 over an alphabet of q letters, $q<p$, there corresponds an OSPQ of k partial quasigroups defined on a set of q elements, with the domain of p elements, $q<p$, and vice versa.[4]

Proof. Let $a_i^{(s)}$ and $a_j^{(s)}$ be in turn i-th and j-th coordinate of the s-th k-sequence of the given code, where i and j are fixed numbers from the set $\{1, 2, \ldots, k\}$, $i \neq j$. We put

$$\mathcal{D}A_u = \{(a_i^{(t)}, a_j^{(t)}) \mid t \in \{1, 2, \ldots, p\}\} \tag{2}$$

and

$$(\forall t \in \{1, 2, \ldots, p\})\,(A_u\,(a_i^{(t)}, a_j^{(t)}) = a_u^{(t)}), \tag{3}$$

for every $u \in \{1, 2, \ldots, k\}$.

According to the proof of Theorem 2 we find that the operations A_u from (3) make an OSPO.

From (2) and (3) follows that A_i and A_j are F and E respectively.

Finally, from Theorem 1, (iv), we get that the constructed system of partial operations is an OSPQ.

Since every OSPQ is an OSPO, according to Theorem 2 we get that the inverse part of this theorem is also true.

From Theorems 2 and 3 we get that the following theorem is valid.

Theorem 4. To every OSPO Σ there corresponds an OSPQ Σ', where Σ and Σ' do not necessarilly have the same domain.

From our Theorem 3 and Theorem 4 from[4] we get:

Theorem 5. To every k-seminet, $k \geqslant 3$, with p points in which the family of lines of maximal cardinality has q lines, $q<p$, there corresponds a code of p k-sequences, $k \geqslant 3$, of code distance k—1, over an alphabet of q letters.

At the end we shall make some remarks concerning the connection between codes and k-nets and k-seminets, and formulate a problem.

To every code of q^2 k-sequences, $k>3$, of code distance k—1 over an alphabet of q letters, there corresponds a k-net. If for some q and $k>3$ k-net does not exist, then the maximal code of code distance k—1 over an alphabet of q elements, has the cardinality smaller then q^2. In this case the maximal code should be searched for among the OSPQ of cardinality $k>3$ defined on the set of q elements. To the maximal code then there corresponds an OSPQ of maximal cardinality of the domain of its elements.

Does there a k-seminet correspond to the searched OSPQ (and when it does, under which conditions)? This question is equivalent to the following: can every OSPQ defined on a finite set Q (and if it can, under which conditions) be embedded in a regularly orthogonal system of regular partial quasigroups ([4]) defined on the same set Q?

These problems were the initial motive for the introduction of k-seminets ([4]).

[4] In the non-partial case the analogous theorem was proved by Golomb and Posner in 1964 ([2]).

REFERENCES

[1] Белоусов В. Д., *Сети и квазигруппы*, Кишинев, 1971.
[2] Dénes J., Gergely E., *Groupoids and codes*, Colloquia Mathematica Societatis János Bolyai, 16. Topics in Information Theory, Keszthely (Hungary), 1975, 155–162.
[3] Ušan J., *Orthogonal systems of n-ary operations and codes*, Matematički vesnik, No 2, 1978.
[4] Ušan Y., *k-seminets*, Matem. bilten, Kniga 1 (XXVII), Skopje, 1977, 41-46.

Janez Usan, Zoran Stojaković

ORTOGONALNI SISTEMI PARCIJALNIH OPERACIJA

Rezime

U ovom radu razmatraju se osobine ortogonalnih sistema parcijalnih operacija i parcijalnih kvazigrupa i utvrđuju veze tih sistema sa jednom klasom kodova fiksiranog kodovskog rastojanja.

Utvrđena su osnovna svojstva ortogonalnih sistema parcijalnih operacija koja predstavljaju uopštenje odgovarajućeg tvrđenja za ortogonalne sisteme operacija. Dokazano je da svakom ortogonalnom sistemu parcijalnih operacija odgovara jedan kod fiksiranog kodovskog rastojanja i obrnuto, što predstavlja generalizaciju osnovnog rezultata rada [2]. Takođe je uspostavljena veza između ortogonalnih sistema parcijalnih kvazigrupa i kodova fiksiranog kodovskog rastojanja, što predstavlja generalizaciju rezultata Golomba i Posnera iz 1964. g. Na kraju je utvrđena veza između *k*-semirešetki, uvedenih u [4], i kodova fiksiranog kodovskog rastojanja.