Quasigroups and Related Systems **20** (2012), 157 − 168

Recursively r-differentiable quasigroups within S-systems and MDS-codes

Galina B. Belyavskaya

Abstract. We study recursively r-differentiable binary quasigroups and such quasigroups with an additional property (strongly recursively r-differentiable quasigroups). These quasigroups we find in S-systems of quasigroups and give a lower bound of the parameters of idempotent 2-recursive MDS-codes that respect to strongly recursively r-differentiable quasigroups. Some illustrative examples are given.

1. Introduction

In the article [7], the notion of a recursively r-differentiable k-ary quasigroup which arise in the connect complete k-recursive codes is introduced. The minimum Hamming distance of these codes achieves the Singleton bound.

Let $Q = \{a_1, a_2, \dots, a_q\}$ be a finite set. Any subset $K \subseteq Q^n$ is called a *code of length* n or an n-*code* over the alphabet Q. An n-code is called an $[n, k]_Q$-*code* if $\mid K \mid= q^k$. An $[n, k, d]_Q$-code is an $[n, k]_Q$-code with the minimum Hamming distance d between code words. An $[n, k, d]_Q$-code is an MDS-*code* if $d = n - k + 1$ ($d \leqslant n - k + 1$ is the Singleton bound).

A code K is a *complete* k-*recursive code* if there exists a function $f : Q^k \to Q$ ($k \leqslant n$) such that K is the set of all words $u(\overline{0, n-1}) = (u(0), \dots, u(n-1))$ satisfying the condition $u(i + k) = f(u(i), \dots, u(i + k - 1))$ for $i \in \overline{0, n-k-1}$, where $u(0), \dots, u(k-1)$ are arbitrary elements of Q.

This code is a error-correcting code and is denoted by $K(n, f)$. Any subcode $K_1 \subseteq K$ of a complete k-recursive code is called k-*recursive*.

A complete k-recursive code $K(n, f)$ is called *idempotent* if the function f is idempotent, that is $f(x, x, \dots, x) = x$.

Let $n^r(k, q)$ ($n^{ir}(k, q)$) denote the maximal number n such that there exists a complete k-recursive MDS-code (a complete idempotent k-recursive MDS-code) over an alphabet of q elements.

By Theorem 6 of [7], the equality $n^r(2, q) = q+1$ holds for any primary number (prime power) $q = p^\alpha \geqslant 3$ and by Corollary 4 of [7],

$$n^r(2, q) \geqslant \min\{p_1^{\alpha_1} + 1, p_2^{\alpha_2} + 1, \dots, p_t^{\alpha_t} + 1\}$$

2010 Mathematics Subject Classification: 20N05, 94B60, 05B15
Keywords: quasigroup, S-system of quasigroups, orthogonal operations, balanced incomplete block design, recursively r-differentiable quasigroup, recursive MDS-code

if $q = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t}$ is the canonical decomposition of the number q.

According to Proposition 10 from [7], $n^{ir}(2, q) \geqslant q - 1$ for any primary $q \geqslant 3$. By Proposition 11 from [7], $n^{ir}(2, p) \geqslant p$ if p is a prime number.

For binary function f a code $K(n, f)$ the system of check functions has the form $f^{(t)}(x, y) = f(f^{(t-2)}(x, y), f^{(t-1)}(x, y))$ for $t \geqslant 2$, where $f^{(0)}(x, y) = f(x, y)$ and $f^{(1)}(x, y) = f(y, f^{(0)}(x, y))$.

In [7] it is proved that r-differentiable quasigroups correspond to complete recursive codes and various methods of constructions of binary recursively 1-differentiable quasigroups are suggested. Moreover, in [7] it is proved that for any $q \in N$, excepting $1, 2, 6$ and possibly $14, 18, 26, 42$, there exist recursively 1-differentiable quasigroups of order q, that is $n^r(2, q) \geqslant 4$.

A quasigroup operation f is called *recursively r-differentiable* if all its *recursive derivatives* $f^{(1)}, f^{(2)}, \dots, f^{(r)}$ are quasigroups. By Theorem 4 of [7], a quasigroup (Q, f) is recursively r-differentiable if and only if the code $K(r+3, f)$ is an MDS-code. In this case the code words are $(x, y, f^{(0)}(x, y), f^{(1)}(x, y), \dots f^{(r)}(x, y))$, $(x, y) \in Q^2$.

A. Abashin in [1] consider special linear recursive MDS-codes with k=2 or 3. V. Izbash and P. Syrbu in [9] prove that for any k-ary ($k \geqslant 2$) operation f the equality $f^{(r)} = f\theta^r$ holds, where $\theta : Q^k \to Q^k$, $\theta(x_1^k) = (x_2, x_3, \dots, x_k, f(x_1^k))$ for all $(x_1^k) \in Q^k$. (Note that this result for $k = 2$ was announced in [4]). They also establish a connection between recursive differentiability of a binary group and the Fibonacci sequence.

In this article we establish properties of binary recursively r-differentiable quasigroups, introduce the notion of a strongly recursively r-differentiab-le quasigroup, and find such idempotent quasigroups in S-systems of quasigroups. A lower bound of $n_s^{ir}(2, q)$ for complete idempotent strongly 2-recursive MDS-codes with primary q is found and illustrative examples are given.

2. Preliminaries

Let Q be a finite or infinite set, Λ_Q be the set of all binary operations defined on Q. On the set Λ_Q it can be defined the *Mann's right* (*left*) *multiplication* $A \cdot B$ ($A \circ B$) of operations $A, B \in \Lambda_Q$ in the following way:

$$(A \cdot B)(x, y) = A(x, B(x, y)) = A(F, B)(x, y),$$

$$(A \circ B)(x, y) = A(B(x, y), y) = A(B, E)(x, y),$$

where $E(x, y) = y$, $F(x, y) = x$ are the right and the left identity operations.

For any operations $A, B \in \Lambda_Q$ the equality $(A \circ B)^* = A^* \cdot B^*$ holds, where $A^*(x, y) = A(y, x)$ (Lemma 4.5 in [2]).

The set $\Lambda_r(\cdot)$ (the set $\Lambda_l(\circ)$) of all invertible from the right (from the left) operations given on a set Q forms the group $\Lambda_r(\cdot)$ (the group $\Lambda_l(\circ)$) under the right (under the left) multiplication of operations.

The operation E, F are the identity elements of the group $\Lambda_r(\cdot)$ and $\Lambda_l(\circ)$, respectively, and $A^{-1} \cdot A = A \cdot A^{-1} = E$, ${}^{-1}\!A \circ A = A \circ {}^{-1}\!A = F$, where

$$A^{-1}(x,y) = z \Leftrightarrow A(x,z) = y, \quad {}^{-1}\!A(x,y) = z \Leftrightarrow A(z,y) = x.$$

Every pair (A, B) of operations of the set Λ_Q defines a mapping θ of the set Q^2 into Q^2 in the following way:

$$\theta(x,y) = (A(x,y), B(x,y)), \quad x, y \in Q.$$

And conversely, any mapping θ of the set Q^2 into Q^2 uniquely defines the pair of operations $A, B \in \Lambda_Q$: if $\theta(a,b) = (c,d)$, then $c = A(a,b)$, $d = B(a,b)$, and $(A,B) = (C,D)$ if and only if $A = C$, $B = D$.

If θ is a permutation on a set Q^2, then operations A, B defined by θ are *orthogonal* (shortly, $A \perp B$), that is the system of equations $\{A(x,y) = a,\ B(x,y) = b\}$ has a unique solution for any $a, b \in Q$. And conversely, an orthogonal pair of operations, given on a set Q, corresponds to the permutation θ on the set Q^2.

If $A, B, C \in \Lambda_Q$, then the new binary operation D can be defined by the following superposition:

$$D(x,y) = A(B(x,y), C(x,y))$$

or shortly, $D = A(B,C) = A\theta$, where $\theta = (B,C)$, that is $D(x,y) = A\theta(x,y)$.

The identity operations F, E of Λ_Q define the identity permutation $(F,E) = \overline{\varepsilon}$ on Q^2. The equality $(A,B)\theta = (A\theta, B\theta)$ holds [2, 3].

3. Recursively r-differentiable quasigroups

Let (Q,A) be a finite quasigroup given on a set Q. Then, the sequence of operations $A^{(0)}, A^{(1)}, \dots, A^{(t)}, \dots$ for A is defined in the following way:

$$A^{(0)}(x,y) = A(x,y), \quad A^{(1)}(x,y) = A(y, A^{(0)}(x,y)),$$

$$A^{(t)}(x,y) = A(A^{(t-2)}(x,y), A^{(t-1)}(x,y))$$

for $t \geqslant 2$. This sequence can be written shortly as:

$$A^{(0)} = A(F,E), \quad A^{(1)} = A(E, A^{(0)}), \quad A^{(t)} = A(A^{(t-2)}, A^{(t-1)}),\ t \geqslant 2.$$

According to [7], the operation $A^{(r)}$ of this sequence is called the *r-th recursive derivative* of a quasigroup (Q,A).

By definition, a quasigroup (Q,A) is *recursively r-differentiable* if all its recursive derivatives $A^{(1)}, A^{(2)}, \dots, A^{(r)}$ are quasigroup operations. In this case, the system of operations $\Sigma = \{F, E, A, A^{(1)}, A^{(2)}, \dots, A^{(r)}\}$ is orthogonal (Proposition 7 of [7]).

By Theorem 4 of [7], a quasigroup (Q, A) is recursively r-differentiable if and only if the 2-recursive code $K(r+3, A)$ is an MDS-code.

First we establish some properties of finite binary recursively r-differentiable quasigroups.

Theorem 1. *Let $A^{(i)}$ be the i-th recursive derivative of a quasigroup (Q, A) and $\theta = (E, A)$, then $A^{(i)} = A\theta^i$, $\theta^i = (A^{(i-2)}, A^{(i-1)})$, $\theta^2 \neq (F, E)$.*

Proof. Note that the mapping $\theta = (E, A)$ of Q^2 into Q^2 is a permutation since A is a quasigroup operation. By the definition,

$$A^{(1)}(x, y) = A(y, A(x, y)) = A(E, A)(x, y) = A\theta(x, y),$$
$$A^{(2)} = A(A, A(E, A)) = A(A, A\theta) = A\theta^2,$$

since $(E, A)^2 = (E, A)(E, A) = (A, A(E, A)) = (A, A\theta)$ whence $(E, A)^2 \neq (F, E)$ as $A \neq F$.

Let $A^{(k)} = A\theta^k$ for all k, $1 \leqslant k \leqslant i-1$, then by the induction we have $A^{(i)} = A(A^{(i-2)}, A^{(i-1)}) = A(A\theta^{i-2}, A\theta^{i-1}) = A(A, A\theta)\theta^{i-2} = A\theta^2\theta^{i-2} = A\theta^i$. From these equalities the second equality of the theorem follows.

Note that, in the general case, the equality $A\theta_1 = A\theta_2$, where θ_1, θ_2 are two permutations not necessarily implies $\theta_1 = \theta_2$. □

The result of Theorem 1 for binary quasigroups was announced in [4] and was generalized for k-ary quasigroups in [9].

Let $A^*(x, y) = A(y, x)$, then $A^* = ({}^{-1}(A^{-1}))^{-1} = {}^{-1}(({}^{-1}A)^{-1})$ (see [3]).

Corollary 1. *If $A^{(1)}, A^{(2)}, \dots, A^{(t)}, \dots$ are the sequence of the recursive derivatives of a quasigroup (Q, A), then for $i \geqslant 1$ we have*

$$A^{(i)} = (A^{(i-1)} \cdot A^*)^* = (A^{(i-1)})^* \circ A,$$

where $(\cdot)$ and $(\circ)$ are the right and left multiplication of the operations given on the set Q.

Proof. Indeed, by Theorem 1,

$$A^{(i)} = A\theta^i = A^{(i-1)}(E, A) = (A^{(i-1)})^* \circ A = (A^{(i-1)} \cdot A^*)^*,$$

since $A(E, B) = A^* \circ B$ and $(A \circ B)^* = A^* \cdot B^*$. □

Proposition 1. *Let a quasigroup (Q, A) be recursively r-differentiable. Then,*

$A^{(i)} \perp {}^{-1}(A^{-1})$ for any $i = 0, 1, 2, \dots, r-1$, $r \geqslant 1$.

If $A^{(r+1)} = F$, $r \geqslant 0$, then $A^{(r)} = {}^{-1}(A^{-1})$ and $A^{(r+2)} = E$.

If $A^{(r+2)} = E$, $r \geqslant 0$, then $A^{(r+1)} = F$.

Proof. By the criterion of orthogonality of two quasigroups (cf. [2]), $A \perp B$ if and only if $A \cdot B^{-1}$ is a quasigroup operation. But by Corollary 1, the operations $A^{(i+1)} = (A^{(i)} \cdot A^*)^*$ by $i \geqslant 0$ are quasigroup operations, and therefore the operation $(A^{(i+1)})^* = A^{(i)} \cdot A^*$ is a quasigroup operation. Taking into account that $A^* = ({}^{-1}(A^{-1}))^{-1}$, we have $A^{(i)} \perp {}^{-1}(A^{-1})$ for any $i = 0, 1, 2, \ldots, r-1$.

Let $A^{(r+1)} = F$, then by Corollary 1, $A^{(r+1)} = (A^{(r)})^* \circ A = F$ for $r \geqslant 0$, so $(A^{(r)})^* = {}^{-1}A$ since $\Lambda_l(\circ)$ is a group with the identity F and the quasigroup ${}^{-1}A$ is inverse for A in this group. Thus, $A^{(r)} = {}^{-1}(A^{-1})$. In this case we have $A^{(r+2)} = A(A^{(r)}, A^{(r+1)}) = A(A^{(r)}, F) = A^*(F, A^{(r)}) = A^* \cdot A^{(r)} = A^* \cdot {}^{-1}(A^{-1}) = E$ because $A^* = ({}^{-1}(A^{-1}))^{-1}$, $\Lambda_r(\cdot)$ is a group with the identity E and A^* is the inverse quasigroup for ${}^{-1}(A^{-1})$ in this group.

Let $A^{(r+2)} = E$, $r \geqslant 0$, then $(A^{(r+2)})^* = F$ and according to Corollary 1, $A^{(r+3)} = (A^{(r+2)})^* \circ A = F \circ A = A$ since $\Lambda_l(\circ)$ is a group with the identity F. But then

$$A^{(r+3)} = A(A^{(r+1)}, A^{(r+2)})) = A(A^{(r+1)}, E) = A \circ A^{(r+1)} = A$$

and so $A^{(r+1)} = F$. □

Definition 1. A quasigroup (Q, A) is called *strongly recursively r-differentiable* if it is r-differentiable and $A^{(r+1)} = F$ (or $A^{(r+2)} = E$). A quasigroup (Q, A) is *strongly recursively* 0*-differentiable* if $A^{(1)} = F$.

Note that a quasigroup not always is strongly recursively 0-differentiable, although any quasigroup is recursively 0-differentiable. In contrast to recursively r-differentiable quasigroups, a strongly recursively r-differentiable quasigroup is not strongly recursively r_1-differentiable if $r_1 < r$.

Recall that a quasigroup (Q, A) is called *semisymmetric* if in (Q, A) the identity $A(x, A(y, x)) = y$ holds.

Corollary 2. *Let (Q, A) be a strongly recursively r-differentiable quasigroup, then $A^{(r)} = {}^{-1}(A^{-1})$, $A^{(r+2)} = E$ for any $r \geqslant 0$. A quasigroup (Q, A) is strongly recursively* 0*-differentiable* (1*-differentiable*) *if and only if it is semisymmetric* ($A^{(1)} = {}^{-1}(A^{-1})$ *respectively*).

Proof. The first statement follows from Proposition 1. It is easy to see that a quasigroup (Q, A) is semisymmetric if and only if $A^* = A^{-1}$ (or $A = {}^{-1}(A^{-1})$), so for a semisymmetric quasigroup $A^{(1)} = A^* \circ {}^{-1}(A^{-1}) = A^{-1} \circ {}^{-1}(A^{-1}) = F$. If $A^{(1)} = F$, then by Proposition 1, $A = A^{(0)} = {}^{-1}(A^{-1})$, that is (Q, A) is semisymmetric.

Let $A^{(1)} = {}^{-1}(A^{-1})$, then $A^{(2)} = (A^{(1)})^* \circ A = ({}^{-1}(A^{-1}))^* \circ A = {}^{-1}A \circ A = F$. If $A^{(2)} = F$, then, by Proposition 1, $A^{(1)} = {}^{-1}(A^{-1})$. □

Proposition 2. *A recursively r-differentiable quasigroup (Q, A) is strongly recursively r-differentiable if and only if the permutation $\theta = (E, A)$ has order $r + 3$.*

Proof. Let the permutation $\theta = (E, A)$ have order $r + 3$, that is $\theta^{r+3} = (F, E)$, then by Theorem 1, $(A^{(r+1)}, A^{(r+2)}) = (F, E)$ and so $A^{(r+1)} = F$.

Conversely, suppose that a quasigroup (Q, A) is strongly recursively r-differentiable, then r is the least number such that $A^{(r+1)} = F$. By Proposition 1, $A^{(r+2)} = E$, so $\theta^{r+3} = (A^{(r+1)}, A^{(r+2)}) = (F, E)$. □

Proposition 3. *The direct product of strongly recursively r-differentiable quasigroups is a strongly recursively r-differentiable quasigroup.*

Proof. Suppose that (Q, A) and (P, B), $|Q| = q_1$, $|P| = q_2$, are strongly recursively r-differentiable quasigroups. Then, the direct product $A \times B$ of these quasigroups is an r-differentiable quasigroup since

$$(A \times B)^{(i)} = A^{(i)} \times B^{(i)},\ i \in N$$

(see the proof of Proposition 9 of [7]). Furthermore, from $A^{(r+1)} = F_Q$ and $B^{(r+1)} = F_P$ it follows that $(A \times B)^{(r+1)} = A^{(r+1)} \times B^{(r+1)} = F_Q \times F_P$. But $F_Q \times F_P$ is the left identity operation under the left multiplication of operations given on the set $Q \times P$, so by the definition, the operation $A \times B$ given on the set $Q \times P$ is a strongly recursively r-differentiable quasigroup of order $q_1 q_2$. □

4. Strongly recursively r-differentiable quasigroups

In the theory of binary quasigroups the notion of a Stein system (shortly, an S-system) is known. This system can be defined in the following way [2].

Definition 2. [2] A system $Q(\Sigma)$ of operations given on a finite set Q is called an *S-system* if

1) Σ contains the operation F, E, the rest operations are quasigroup operations;
2) if $A, B \in \Sigma'$, where $\Sigma' = \Sigma \backslash F$, then $A \cdot B \in \Sigma'$;
3) if $A \in \Sigma$, then $A^* \in \Sigma$.

In this case, $\Sigma'(\cdot)$, $\Sigma''(\circ)$, where $\Sigma' = \Sigma \backslash F$ and $\Sigma'' = \Sigma \backslash E$, are isomorphic groups.

We recall some necessary information about S-systems. Let s be the number of operations in an S-system $Q(\Sigma)$, n be the order of the set Q. Then, by Theorem 4.3 of [2], the number $s - 1$ divides $n - 1$ and $k = (n - 1)/(s - 1) \geqslant s$ or $k = 1$.

The number k is called *the index of an S-system* $Q(\Sigma)$. In the case $k = 1$ we say that $Q(\Sigma)$ is a *complete* S-system.

Complete S-systems are described by V. Belousov in [2]. Incomplete S-systems are described by G. Belyavskaya and A. Cheban in [5, 6].

All operations of an S-system $Q(\Sigma)$ are orthogonal and by Theorem 4.2 [2], are idempotent if $s \geqslant 4$, that is $A(x, x) = x$ for all $x \in Q$ and $A \in \Sigma$.

If $Q(\Sigma)$ is an S-system, then according to Theorem 4.1 [2], for any $A, B, C \in \Sigma$ the operation $C(A, B)$:

$$C(A, B)(x, y) = C(A(x, y), B(x, y))$$

belongs to Σ and the set Δ of all mappings $\theta = (B, C)$, where $B, C \in \Sigma$, $B \neq C$, is a group.

Recall that an algebra $(Q, +, \cdot)$ with two operations is called a *near-field* if $(Q, +)$ is an abelian group with the identity 0, $(Q', \cdot)$ is a group, where $Q' = Q \backslash \{0\}$ and the right distributive law: $(x + y)z = xz + yz$ holds [10].

By Theorem 4.6 of [2], any complete S-system $Q(\Sigma)$ is a system over some near-field $Q(+, \cdot)$, that is any its operation has the form

$$A_a(x, y) = a(y - x) + x$$

for a fixed element $a \in Q$.

Thus, for a complete S-system $Q(\Sigma)$ containing s quasigroups of order q we have $s = q = p^\alpha$ for some primary number since any near-field has such order, and for any prime power there exists a near-field of this order [10]. If a near-field is a field, then the quasigroups are linear over the group $(Q, +)$ and have the form

$$A_a(x, y) = (1 - a)x + ay.$$

All S-systems that are not complete are described in the article [5] by means of near-fields (by means of complete S-systems) and balanced incomplete block designs $BIB(v, b, r, k, 1)$.

A *balanced incomplete block design* $BIB(v, b, r, k, 1)$ is an arrangement of v elements by b blocks such that

every block contains exactly k different elements;

every element appears in exactly r different blocks;

every pair of different elements appears in exactly one block.

The parameters r and k of a $BIB(v, b, r, k, 1)$ define the number v and b [11].

By Theorem 1 of [5], an S-system with operations of order q, of index k containing s operations exists if and only if there exists a $BIB(q, b, , k, p^\alpha, 1)$ with a prime p. In this case,

$$q = ks - k + 1, \quad b = ((ks - k + 1)/s)k, \quad s = p^\alpha.$$

Below S-systems will be used to finding of strongly recursively r-differentiable idempotent quasigroups. Since we consider only recursively r-differentiable quasigroups sometimes the word "recursively" will be omitted.

Theorem 2. *A quasigroup (Q, A) of an S-system $Q(\Sigma)$ is (strongly) recursively r-differentiable if and only if r is the least number such that $A^{(r+1)} = F$ (the permutation $\theta = (E, A)$ has order $r + 3$).*

Proof. If a quasigroup (Q, A) of an S-system $Q(\Sigma)$ is strongly r-differentiable, then by the definition, $A^{(r+1)} = F$ and $A^{(1)}, A^{(2)}, \ldots, A^{(r)}$ are quasigroups.

For the proof of the converse statement we first note that from the properties of S-systems $Q(\Sigma)$ pointed above it follows that all recursive derivatives of any quasigroup (Q, A), where $A \in \Sigma$, are in Σ. So, they can be quasigroup operations or the identity operations F, E.

Let a quasigroup operation A be in Σ, r be the least number such that $A^{(r+1)} = F$, then the recursive derivatives $A^{(i)}$, $1 \leqslant i \leqslant r$, of A either all are quasigroup operations or $A^{(i_0)} = E$ for some $i_0 \leqslant r$, and all operations $A^{(i)}$, $i < i_0$, are quasigroup operations.

In the first case, A is a strongly r-differentiable quasigroup. In the second case, the quasigroup A is $(i_0 - 1)$-differentiable. On the other hand, by Proposition 1, we have $A^{(i_0-1)} = F$ since $A^{(i_0)} = E$. But $A^{(i_0-1)}$ is a quasigroup, that is we obtain the contradiction.

Let the permutation $\theta = (E, A)$ have order $r+3$, then $\theta^{(r+3)} = (A^{(r+1)}, A^{(r+2)}) = (F, E)$ whence $A^{(r+1)} = F$, $A^{(r+2)} = E$, moreover, this number r is the least one with such property. In this case, as has been shown above, the quasigroup (Q, A) is strongly r-differentiable. The converse follows from Proposition 2. $\square$

Theorem 3. *Let $Q(\Sigma)$ be an S-system containing $p^\alpha \geqslant 3$ operations, A be a quasigroup operation of Σ, and the permutations $\theta_A = (E, A)$ have order $r + 3$ for some $r \geqslant 0$. Then*

$$(r + 3) \mid p^\alpha(p^\alpha - 1).$$

Proof. Let $\Sigma = \{F, E, A_1, A_2, \dots A_{s-2}\}$ be an S-system containing $s = p^\alpha$ operations of order $q = p^\alpha$ if the system Σ is complete, and of order $q = ks - k + 1$ if Σ is an S-system of index k.

By Theorem 4.1 of [2], the set $\triangle$ of all mappings $\theta = (B, C)$, $B, C \in \Sigma$, $B \neq C$, of any S-system is a group. The order of the group $\triangle$ is $s(s - 1) = p^\alpha(p^\alpha - 1)$.

The permutation $\theta_A = (E, A) \in \triangle$ for any operation A of Σ, $A \neq E$.

If for $A \in \Sigma$ the permutation θ_A has order $r + 3$, then $\theta_A^{r+3} = (F, E)$. Thus $(r + 3) \mid p^\alpha(p^\alpha - 1)$. $\square$

Theorem 4. *Let $p^\alpha \geqslant 5$ be an odd prime power, $Q(\Sigma)$ be an S-system containing p^α operations. Then in Σ there exists a quasigroup operation A such that the permutation $\theta_A = (E, A)$ has order $r + 3$ for some $r + 3 = p^{\alpha_1}$, $\alpha_1 \leqslant \alpha$, and A is a strongly recursively idempotent r-differentiable quasigroup operation of order $q = p^\alpha$. If there exists a $BIB(q, b, k, p^\alpha, 1)$, then A has order $q = kp^\alpha - k + 1$.*

Proof. Let $p^\alpha \geqslant 5$ be an odd prime power, $Q(\Sigma)$ be an S-system containing $s = p^\alpha$ operations. Then by Theorem 4.1 of [2] the set $\triangle$ of all mappings $\theta = (B, C)$, $B, C \in \Sigma$, $B \neq C$ is a group. Moreover, from the proof of Theorem 4.6 in [2] it follows that this group is twice transitive on Σ and contains a strongly transitive on Σ invariant abelian subgroup $\triangle_0$. It is obvious that the group $\triangle_0$ has order $s = p^\alpha$.

Let $\overline{\theta}_C$ be the permutation of $\triangle_0$ such that $F\overline{\theta}_C = C$. Then $F\overline{\theta}_E = E$ and $\overline{\theta}_E = (E, A) = \theta_A$ for a unique operation A of Σ. Moreover, $A \neq F$. Indeed, if $A = F$, then $\overline{\theta}_E^2 = (E, F)(E, F) = (F, E)$, so $p^\alpha = 2^\alpha$ and the subgroup $\triangle_0$ has even order.

Suppose that the permutation $\overline{\theta}_E$ has order $r+3$. Then $r+3 = p^{\alpha_1}$ for $\alpha_1 \leqslant \alpha$ since $(r+3) \mid p^\alpha$. Hence, $\overline{\theta}_E^{r+3} = \theta_A^{r+3} = (F, E)$. By Theorem 2, (Q, A) is strongly r-differentiable quasigroup of order $q = p^\alpha$ if the S-system $Q(\Sigma)$ is complete, and has order $q = kp^\alpha - k + 1$ if it is incomplete with index k. Recall that by Theorem 4.2 of [2] any operation of an S-system is idempotent if $s \geqslant 4$.

According to Corollary 2, $A^r =^{-1} (A^{-1})$, $A^{(r+1)} = F$, $A^{(r+2)} = E$. Thus, we have the subsystem

$\Sigma_1 = \{A, A^{(1)}, A^{(2)}, \dots, A^{(r)} =^{-1} (A^{-1}), A^{(r+1)} = F, A^{(r+2)} = E\} \subset \Sigma$

for $r = p^{\alpha_1} - 3$. □

Corollary 3. *For any prime p, $p \geqslant 5$, there exists a strongly recursively $(p-3)$-differentiable idempotent quasigroup of order $q = p$ (of order $q = kp - k + 1$ if there exists a $BIB(q, b, k, p, 1)$).*

Proof. In this case the subgroup $\triangle_0$ of the group $\triangle$ of an S-system has odd order p, that is, $\triangle_0$ is a cyclic group and so the permutation $\overline{\theta}_E = (E, A)$ of $\triangle_0$ has order p. Now the statements of the corollary follow from Theorem 4 by $q = p$. □

Proposition 4. *For any prime power p^α, $p \geqslant 5$, there exists a strongly recursively idempotent $(p-3)$-differentiable quasigroup of order $q = p^\alpha$ (respectively, of order $q = (kp - k + 1)^\alpha$ if there exists a $BIB(q, b, k, p, 1)$).*

Proof. By Corollary 3 there exists a strongly $(p-3)$-differentiable quasigroup of order p. Using Proposition 3 and taking the direct product of α copies of this quasigroup, we get a strongly $(p-3)$-differentiable idempotent quasigroup of order p^α. It is obvious that the direct product of idempotent quasigroups is an idempotent quasigroup. □

Remark. Note that the direct product of two strongly recursively r-differentiable idempotent quasigroups of order $p_1^{\alpha_1}$ and $p_2^{\alpha_2}$, $p_1 \neq p_2$, over near-fields of the respective orders already is not a quasigroup over some near-field since has order $p_1^{\alpha_1} p_2^{\alpha_2}$ which is not a prime power.

Corollary 4. *There exist strongly recursively 2-differentiable idempotent quasigroups of order $q = 21, 25, 41, 45, 61$; strongly recursively 4-differentiable idempotent quasigroups of order $q = 49, 91$ and strongly recursively 8-differentiable idempotent quasigroups of order $q = 121$.*

Proof. These statements follow from Corollary 3 and the existence of the following designs:

$BIB(21, 21, 5, 5, 1)$ (N7), $BIB(25, 30, 6, 5, 1)$ (N11),

$BIB(41, 82, 10, 5, 1)$ (N42), $BIB(45, 99, 11, 5, 1)$ (N51),

$BIB(61, 183, 15, 5, 1)$ (N108) (for these designs we have $(2 = 5 - 3)$-differentiable idempotent quasigroups of order $q = 21, 25, 41, 45, 61$ respectively.

The designs $BIB(49, 56, 8, 7, 1)$ (N24) and $BIB(91, 195, 15, 7, 1)$ (N111) give a strongly $(4 = 7 - 3)$-differentiable idempotent quasigroups of order $q = 49, 91$.

The design $BIB(121, 132, 12, 11, 1)$ (N68) corresponds to a strongly $(8 = 11–3)$ -differentiable idempotent quasigroup of order $q = 121$.

All these BIB-designs exist (near with each design we point its number in Table of Application I of [11]. □

Definition 3. An MDS-code $K(n, A)$ is said to be *strongly recursive* if the quasigroup (Q, A) is strongly recursively $(n-3)$-differentiable.

Corollary 5. *For any prime power p^α, $p \geqslant 5$, there exists an idempotent strongly 2-recursive code $K(p, A)$, where A is a quasigroup of order p^α.*

Proof. By Theorem 4 of [7], a quasigroup A is r-differentiable if and only if the code $K(r+3, A)$ is an MDS-code. Next use Corollary 3 for $r = p-3$ and Proposition 4. □

Denote by $K_s^i(n, A)$ the idempotent strongly 2-recursive MDS-code corresponding to a quasigroup (Q, A) and let $n_s^{ir}(2, q)$ denote the maximal number n such that there exists a (complete) idempotent strongly 2-recursive MDS-code $K_s^i(n, A)$ over an alphabet of q elements.

From Corollary 5 it follows

Corollary 6. *$n_s^{ir}(2, p^\alpha) \geqslant p$ for any prime p, $p \geqslant 5$ and $\alpha \in N$.* □

Corollary 7. *If there exist strongly recursively r-differentiable quasigroups of order q_1 and q_2, then*

$$n_s^{ir}(2, q_1 q_2) \geqslant r + 3.$$

Proof. That follows from Proposition 3 and Theorem 4 of [7]. □

Below, we give some illustrative examples of strongly recursively r-differentiable idempotent quasigroups over fields.

Example 1. Consider the following quasigroup operation A_2 of the S-system of quasigroups over the field $GF(5)$: $A_2(x, y) = 2(y-x)+x = 4x+2y$. The recursive derivatives of this quasigroup are:

$A_2^{(1)}(x, y) = A_2(y, A_2(x, y)) = 4y + 2(4x + 2y) = 3x + 3y$;

$A_2^{(2)}(x, y) = A_2(A_2(x, y), A_2^{(1)}(x, y)) = 4(4x + 2y) + 2(3x + 3y) = 2x + 4y$;

$A_2^{(3)}(x, y) = A_2(A_2^{(1)}(x, y), A_2^{(2)})(x, y) = 4(3x + 3y) + 2(2x + 4y) = x$.

Hence, A_2 is a strongly 2-differentiable quasigroup operation of the S-system over the field $GF(5)$, and the orthogonal system $\Sigma = \{F, E, A_2, A_2^{(1)}, A_2^{(2)}\}$ corresponds to the code $K_s^i(5, A_2)$.

Example 2. Consider the quasigroup operation of the same form over the field $GF(7)$:

$A_2(x, y) = 2(y-x)+x = 6x+2y$; $A_2^{(1)}(x, y) = 5x+3y$; $A_2^{(2)}(x, y) = 4x+4y$;

$A_2^{(3)}(x, y) = 3x+5y$; $A_2^{(4)}(x, y) = 2x+6y$; $A_2^{(5)}(x, y) = x$.

Thus, this quasigroup is strongly $(7 - 3 = 4)$-differentiable. The orthogonal system $\Sigma = \{F, E, A_2, A_2^{(1)}, A_2^{(2)}, A_2^{(3)}, A_2^{(4)}\}$ corresponds to the code $K_s^i(7, A_2)$.

Note that for a quasigroup operation A over $GF(7)$ the group Δ (see the proof of Theorem 3) has order $7 \cdot 6$, so a permutation $\theta = (E, A)$ for $A \in \Sigma$ can have only order 3 or 7 ($(E, A)^2 \neq (F, E)$ if A is a quasigroup operation).

For the quasigroup operation $A_3(x, y) = 3(y - x) + x = 5x + 3y$ over $GF(7)$ the permutation $\theta = (E, A_3)$ has order 3 since $A_3^{(1)}(x, y) = A_3(y, A_3(x, y)) = 5y + 3(5x + 3y) = x$. In this case, the quasigroup operation A_3 is strongly 0-differential, $\theta \in \Delta \backslash \Delta_0$ since $\mid \Delta_0 \mid = 7$.

The subsystem $\Sigma_1 = \{F, E, A_3\}$ of the complete S-system over $GF(7)$ corresponds to the code $K_s^i(3, A_3)$.

Example 3. Among of quasigroups over the field $GF(11)$ necessarily there are strongly $(11 - 3 = 8)$-differentiable quasigroups (by Corollary 3) and a priori can be strongly $(5 - 3 = 2)$- or $(10 - 3 = 7)$-differentiable quasigroups since the group Δ has order $11 \cdot 10$. Show that all these cases are possible.

The quasigroup operation $A_2(x, y) = 2(y - x) + x = 10x + 2y$ is strongly 8-differentiable with the following recursive derivatives:

$A_2^{(1)}(x, y) = 9x + 3y$; $A_2^{(2)}(x, y) = 8x + 4y$; $A_2^{(3)}(x, y) = 7x + 5y$;

$A_2^{(4)}(x, y) = 6x + 6y$; $A_2^{(5)}(x, y) = 5x + 7y$; $A_2^{(6)}(x, y) = 4x + 8y$;

$A_2^{(7)}(x, y) = 3x + 9y$; $A_2^{(8)}(x, y) = 2x + 10y$; $A_2^{(9)}(x, y) = x$.

The system $\Sigma = \{F, E, A_2, A_2^{(1)}, A_2^{(2)}, \dots, A_2^{(8)}\}$ corresponds to $K_s^i(11, A_2)$.

The commutative quasigroup operation $A_6(x, y) = 6(y - x) + x = 6x + 6y$ over the field $GF(11)$ is strongly 2-differentiable: $A_6^{(1)}(x, y) = 3x + 9y$; $A_6^{(2)}(x, y) = 10x + 2y$; $A_6^{(3)}(x, y) = x$, corresponds to the subsystem $\Sigma_1 = \{F, E, A_6, A_6^{(1)}, A_6^{(2)}\}$ and to the code $K_s^i(5, A_6)$. The permutation $\theta = (E, A_6)$ has order 5 and is in the subset $\Delta \backslash \Delta_0$.

Finally, consider the quasigroup operation $A_9(x, y) = 9(y - x) + x = 3x + 9y$ over $GF(11)$:

$A_9^{(1)}(x, y) = 5x + 7y$; $A_9^{(2)}(x, y) = 10x + 2y$; $A_9^{(3)}(x, y) = 6x + 6y$;

$A_9^{(4)}(x, y) = 7x + 5y$; $A_9^{(5)}(x, y) = 4x + 8y$; $A_9^{(6)}(x, y) = 2x + 10y$;

$A_9^{(7)}(x, y) = 8x + 4y$; $A_9^{(8)}(x, y) = x$.

Thus, the quasigroup operation A_9 is strongly 7-differentiable and corresponds to the subsystem Σ_1 of 10 (from 11) operations and to the code $K_s^i(10, A_9)$.

Note that the direct product of the strongly 2-differentiable quasigroups $A_2 = 4x + 2y$ over $GF(5)$ (Example 1) and $A_6(x, y) = 6x + 6y$ over the field $GF(11)$ (Example 3) is a strongly 2-differentiable quasigroup of order 55 and corresponds to the code $K_s^i(5, A_2 \times A_6)$ by Proposition 3 and Theorem 4 of [7].

References

[1] **A.S. Abashin**, *Linear recursive MDS-codes of dimention* 2 *and* 3, (Russian), Discret. Mat. **12** (1998), 140 – 153.

[2] **V.D. Belousov**, *Systems of quasigroups with generalized identities*, (Russian), Uspehi Matem. Nauk **20(121)** (1965), 75 – 146.

[3] **V.D. Belousov**, *Systems of orthogonal operations*, (Russian), Mat. Sbornik **77(119)** (1968), 38 – 58.

[4] **G.B. Belyavskaya**, *On r-differentiable quasigroups*, Abstracts Int. Conf. Pure Applied Math., Kiev 2002, 11 – 12.

[5] **G.B. Belyavskaya and A.M. Cheban**, *S-systems of arbitrary index, I*, (Russian), Mat. Issled. **7** (1972), vyp.1, 27 – 43.

[6] **G.B. Belyavskaya and A.M. Cheban**, *S-systems of arbitrary index, II*, Mat. Issled. **7** (1972), vyp.2, 3 – 13.

[7] **E. Couselo, S. Gonsalez, V. Markov and A. Nechaev**, *Recursive MDS-codes and recursive differentiable quasigroup*, Discrete Math. Appl. **8** (1998), 217 – 245.

[8] **E. Couselo, S. Gonzzlez, V. Markov and A. Nechaev**, *Parameters of recursive MDS-codes*, Discrete Math. Appl. **10** (2000), 443 – 453.

[9] **V.I. Izbash and P. Syrbu**. *Recursively differentiable quasigroups and complete recursive codes*, Comm. Math. Univ. Carolinae **45** (2004), 257 – 263.

[10] **M. Hall**, *The theory of groups*, The Macmillian Company, New York, 1959.

[11] **M. Hall**, *Combinatorial Theory*, Blaisdell Publishing Company, Toronto-London, 1967.

Received March 1, 2012

Institute of Mathematics and Computer Science Academy of Sciences of Moldova
str. Academiei 5, MD-2028 Chisinau, Moldova
E-mail: gbel1@rambler.ru