Recursively differentiable quasigroups and complete recursive codes

V. Izbash, P. Syrbu

Abstract. Criteria of recursive differentiability of quasigroups are given. Complete recursive codes which attains the Joshibound are constructed using recursively differentiable k-ary quasigroups.

Keywords: k-recursive code, strong orthogonal system of quasigroups, recursively differentiable quasigroups.

Classification: 11T71

Let q, n be positive integers and Q be a nonempty set of q elements. A code $C \subseteq Q^n$ of length n over the alphabet Q is called an $[n,k]_Q$-*code* if $|C| = q^k$. An $[n,k,d]_Q$-code is a $[n,k]_Q$-code with the minimal Hamming distance d [1].

According to D.D. Joshi's theorem [2], if C is an $[n,k,d]_Q$-code, then $|C| \leq q^{n-d+1}$, where $|Q| = q$.

If an $[n,k,d]_Q$-code C has the cardinal number $|C| = q^{n-d+1}$ then we say that C *attains the Joshibound*. The problem of description of the parameters q, n and d for which there exist $[n,k,d]_Q$-codes, where $|Q| = q$, attaining the Joshibound is open [1].

It is known that using strong orthogonal systems of k-ary quasigroups ($k \geq 2$), in particular, orthogonal systems of latin squares, such codes can be constructed.

For example, if $\{f_1, f_2, \ldots, f_t\}$, $t \geq 2$, is an orthogonal system of binary quasigroups defined on a set Q of q elements, then

$$C = \{(x, y, f_1(x,y), f_2(x,y), \ldots, f_t(x,y)) \mid x, y \in Q\}$$

is an $[t+2, 2, t+1]_Q$-code, so C attains the Joshibound [2].

This article deals with complete k-recursive codes and recursive differentiability of k-ary quasigroups.

A code C of length n over an alphabet Q is called *complete k-recursive*, where $1 \leq k \leq n$, if there exists a mapping $f : Q^k \longrightarrow Q$ such that every code word $u = (u_0, u_1, \ldots, u_{n-1}) \in C$ satisfies the conditions

$$u_{i+k} = f(u_i, u_{i+1}, \ldots, u_{i+k-1}),$$

for every $i = 0, 1, \ldots, n-k$.

A complete k-recursive code $C \subseteq Q^n$ defined by the mapping f is denoted by $C(n, f)$.

In what follows we will use the notation (x_1^k) for $(x_1, \ldots, x_k)$.

It is proved in [1] and it is easy to see that if $C(n, f)$ is a complete k-recursive code over an alphabet Q then

$$C(n,f) = \{(x_1, \ldots, x_k, f^{(0)}(x_1^{k-1}), \ldots, f^{(n-k-1)}(x_1^k)) \mid x_1, \ldots, x_k \in Q\},$$

where the functions $f^{(0)}, f^{(1)}, \ldots, f^{(n-k-1)}$ are called *k-recursive derivatives* of f and are defined as follows:

$$f^{(0)}(x_1^k) = f(x_1^k),$$
$$f^{(1)}(x_1^k) = f(x_2^k, f^{(0)}(x_1^k)),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$f^{(t)}(x_1^k) = f(x_{t+1}^k, f^{(0)}(x_1^k), f^{(1)}(x_1^k), \ldots, f^{(t-1)}(x_1^k)), \quad \text{for} \quad t < k,$$
$$f^{(t)}(x_1^k) = f(f^{(t-k)}(x_1^k), \ldots, f^{(t-1)}(x_1^k)), \quad \text{for} \quad t \geq k.$$

A k-ary quasigroup operation f $(k \geq 2)$ is called *recursively s-differentiable* if its k-recursive derivatives $f^{(0)}, f^{(1)}, \ldots, f^{(s)}$ are k-ary quasigroup operations. Let $k \in \mathbb{N}$, $k \geq 2$, and let $f_1, f_2, \ldots, f_k$ be k-ary operations defined on a set Q. The operations $f_1, f_2, \ldots, f_k$ are called *orthogonal* if the system of equations $\{f_i(x_1, x_2, \ldots, x_k) = a_i\}_{i=1}^k$ has a unique solution for every $a_1, \ldots, a_k \in Q$. It is known and it is easy to see that the k-ary operations $f_1, f_2, \ldots, f_k$, defined on a set Q are orthogonal if and only if the mapping

$$\theta : Q^k \to Q^k, \quad \theta(x_1^k) = (f_1(x_1^k), f_2(x_1^k), \ldots, f_k(x_1^k)) = (f_1, f_2, \ldots, f_k)(x_1^k)$$

is a bijection. In this case we will denote $\theta = (f_1, f_2, \ldots, f_k)$.

A system $\Sigma = \{f_1, f_2, \ldots, f_t\}_{t \geq k}$ of k-ary operations defined on a set Q is called *orthogonal* if every k operations from Σ are orthogonal. A system $\{f_1, f_2, \ldots, f_s\}_{s \geq 1}$ of k-ary operations defined on a set Q is called *strong orthogonal* if the system $\{E_1, \ldots, E_k, f_1, f_2, \ldots, f_s\}$ is orthogonal, where $E_i(x_1^k) = x_i$, for every $(x_1, \ldots, x_k) \in Q^k$ and for every $i = 1, 2, \ldots, k$ (the k-ary selectors).

It follows from the definition that each operation of a strong orthogonal system, which is not a selector, is a quasigroup operation. Every orthogonal system of binary quasigroups is strong orthogonal.

It is proved in [1] that a complete k-recursive code $C(n, f)$ attains the Joshibound if and only if the system of k-recursive derivatives $\{f^{(0)}, f^{(1)}, \ldots, f^{(n-k-1)}\}$ is strong orthogonal. In this case the k-recursive derivatives $f^{(0)}, f^{(1)}, \ldots, f^{(n-k-1)}$ of f are k-ary quasigroup operations, so f is recursively $(n-k-1)$-differentiable. The converse is not true for $k \geq 3$. But for $k = 2$ the following criterion holds.

Proposition 1 ([1]). *A complete 2-recursive code*

$$C(n,f)=\{(x,y,f^{(0)}(x,y),f^{(1)}(x,y),\dots,f^{(n-3)}(x,y))\mid x,y\in Q\}$$

attains the Joshibound if an only if the 2-recursive derivatives $f^{(0)},f^{(1)},\dots,f^{(n-3)}$ *of* f *are quasigroup operations.*

So a complete 2-recursive code $C(n,f)$ attains the Joshibound if and only if the binary operation f is recursively $(n-3)$-differentiable.

As was announced by G. Belyavskaya in [7] if $Q(f)$ is a binary quasigroup then $f^{(i)}=f\theta^i$, $\forall\, i\in\mathbb{N}$, where θ is the following mapping:

$$\theta : Q^2\longrightarrow Q^2,\ \theta(x,y)=(y,f(x,y)),\quad \forall\,(x,y)\in Q^2.$$

So Proposition 1 has the following algebraic meaning: a binary quasigroup $Q(f)$ is recursively s-differentiable ($s\in\mathbb{N}$) if and only if $f,f\theta,\dots,f\theta^s$, where $\theta=(E_2,f)$, are quasigroup operations. The result announced in [7] is generalized in the following proposition.

Proposition 2. *If* f *is a* k*-ary operation* ($k\geq 2$) *then* $f^{(n)}=f\theta^n$ *for all* $n\in\mathbb{N}$, *where*

$$\theta : Q^k\longrightarrow Q^k,\ \theta(x_1^k)=(x_2,\dots,x_k,f(x_1^k)) \tag{1}$$

for every $(x_1^k)\in Q^k$.

Proof: To prove this proposition we will use the mathematical induction.

For $n=0$ and $n=1$, according to the definition of k-recursive derivatives, we have $f^{(0)}=f=f\theta^0$ and $f^{(1)}=f(E_2,\dots,E_k,f)=f\theta$.

Let us suppose that Proposition 2 is true for every n, satisfying the inequalities: $0\leq n\leq s-1<k$. Then for $n=s$, using this assumption, we get:

$$\begin{aligned}f^{(s)}&=f(E_{s+1},\dots,E_k,f^{(0)},\dots,f^{(s-1)})=f(E_{s+1},\dots,E_k,f,f\theta,\dots,f\theta^{s-1})\\&=f(E_s,\dots,E_k,f,f\theta,\dots,f\theta^{s-2})\theta=f\theta^{s-1}\theta=f\theta^s.\end{aligned}$$

For $n=k$ have

$$f^{(k)}=f(f^{(0)},f^{(1)},\dots,f^{(k-1)})=f(E_k,f^{(0)},f^{(1)},\dots,f^{(k-2)})\theta=f\theta^{k-1}\theta=f\theta^k.$$

Let us suppose now that Proposition 2 is true for every $n\leq m-1$, where $m\geq k+1$. Then

$$\begin{aligned}f^{(m)}&=f(f^{(m-k)},\dots,f^{(m-2)},f^{(m-1)})\\&=f(f^{(m-k-1)},\dots,f^{(m-3)},f^{(m-2)})(E_2,\dots,E_k,f)=f\theta^{m-1}\theta=f\theta^m.\end{aligned}$$

So Proposition 2 is true for every $n\in\mathbb{N}$. □

Corollary. *Let $Q(f)$ be an k-ary quasigroup, $k \geq 2$ and $s \in \mathbb{N}$. If $\{f, f\theta, \ldots, f\theta^s\}$, where θ is the mapping defined in (1), is a strong orthogonal system of k-ary operations then $Q(f)$ is recursively s-differentiable.*

As was shown above for $k = 2$ the converse of this corollary is true as well.

Proposition 3. *Let $Q(f)$ be an k-ary quasigroup, $k \geq 2$. Every $k+1$ consecutive k-recursive derivatives $\{f^{(i)}, f^{(i+1)}, \ldots, f^{(i+k)}\}$ of f are orthogonal.*

Proof: If $Q(f)$ is an k-ary quasigroup, $k \geq 2$, then the system $\Sigma = \{E_1, \ldots, E_k, f\}$ is orthogonal, so its subsystem $\{E_2, \ldots, E_k, f\}$ is orthogonal as well, i.e. the mapping

$$\theta : Q^k \longrightarrow Q^k,\ \theta(x_1^k) = (x_2, \ldots, x_k, f(x_1^k)),\quad \forall\, (x_1^k) \in Q^k,$$

is a bijection. Hence each of the following systems is orthogonal:

$$\begin{aligned}
\Sigma\theta &= \{E_2, \ldots, E_k, f, f\theta\} = \{E_2, \ldots, E_k, f^{(0)}, f^{(1)}\},\\
\Sigma\theta^2 &= \{E_3, \ldots, E_k, f, f\theta, f\theta^2\} = \{E_3, \ldots, E_k, f^{(0)}, f^{(1)}, f^{(2)}\}, \ldots,\\
\Sigma\theta^{k-1} &= \{E_k, f, f\theta, \ldots, f\theta^{k-1}\} = \{E_k, f^{(0)}, f^{(1)}, \ldots, f^{(k-1)}\},\\
\Sigma\theta^k &= \{f, f\theta, \ldots, f\theta^k\} = \{f^{(0)}, f^{(1)}, \ldots, f^{(k)}\}
\end{aligned}$$

and

$$\Sigma\theta^s = \{f\theta^{s-k}, \ldots, f\theta^s\} = \{f^{(s-k)}, \ldots, f^{(s)}\},$$

for every $s \geq k+1$. □

Corollary 1. *A binary quasigroup $Q(f)$ is recursively 1-differentiable if and only if the pair of operations $\{E_1, f^{(1)}\}$ is orthogonal.*

Proof: As $\{E_1, E_2, f\}$ is an orthogonal system, the mapping $\theta = (E_2, f)$ is a bijection and the system $\{E_2, f, f^{(1)}\} = \{E_1, E_2, f\}\theta$ is orthogonal too. Hence, $f^{(1)}$ is a quasigroup operation if and only if the pair $\{E_1, f^{(1)}\}$ is orthogonal. □

Corollary 2. *A ternary quasigroup $Q(f)$ is recursively 1-differentiable iff the systems of ternary operations $\{E_1, E_2, f^{(1)}\}$ and $\{E_1, E_3, f^{(1)}\}$ are orthogonal.*

Let $Q(\cdot)$ be a binary group and let denote by $(\overset{n}{\triangle})$ the n-th 2-recursive derivative of $(\cdot)$, for every $n \in \mathbb{N}$.

Lemma 1. *If $Q(\cdot)$ is an abelian group, then for all $x, y \in Q$ and $n \in \mathbb{N}$ the following equality holds:*

$$x \overset{n}{\triangle} y = x^{b_n} y^{b_{n+1}} \tag{2}$$

where $(b_n)_{n\in\mathbb{N}}$ is the Fibonacci sequence.

Proof: We will use the mathematical induction.

For $n = 0$ have $x \overset{0}{\triangle} y = x \cdot y$ so $x \overset{0}{\triangle} y = x^{b_0} \cdot y^{b_1}$.

For $n = 1$ have $x \overset{1}{\triangle} y = y \cdot xy = x \cdot y^2 = x^{b_1} \cdot y^{b_2}$.

Suppose that Lemma 1 is true for every $n \leq k$. Using this assumption and the definition of the Fibonacci sequence, for $n = k + 1$ we get

$$\begin{aligned} x \overset{k+1}{\triangle} y = (x \overset{k-1}{\triangle} y)(x \overset{k}{\triangle} y) &= x^{b_{k-1}} \cdot y^{b_k} \cdot x^{b_k} \cdot y^{b_{k+1}} \\ &= x^{b_{k-1}+b_k} \cdot y^{b_k+b_{k+1}} = x^{b_{k+1}} \cdot y^{b_{k+2}}. \end{aligned}$$

So the equality (2) is true for every $x, y \in Q$ and for every $n \in \mathbb{N}$. □

Theorem 1. *A binary abelian group $Q(\cdot)$ is recursively s-differentiable, where $s \geq 1$, if and only if the mappings $x \mapsto x^{b_i}$, where $(b_n)_{n\in\mathbb{N}}$ is the Fibonacci sequence, are bijections for all $i \in \{0, 1, 2, \ldots, s + 1\}$.*

Proof: According to the definition a group $Q(\cdot)$ is recursively s-differentiable if and only if its 2-recursive derivatives $(\overset{1}{\triangle}), (\overset{2}{\triangle}), \ldots, (\overset{s}{\triangle})$ are quasigroup operations. Hence $Q(\cdot)$ is recursively s-differentiable if and only if each of the equations $x \overset{i}{\triangle} a = c$, $a \overset{i}{\triangle} y = c$, $i \in \{0, 1, 2, \ldots, s\}$, has a unique solution for every $a, c \in Q$. Now, using the equalities (2) we get: $x \overset{i}{\triangle} a = c \Leftrightarrow x^{b_i} \cdot a^{b_{i+1}} = c \Leftrightarrow x^{b_i} = c \cdot a^{-b_{i+1}}$ and $a \overset{i}{\triangle} y = c \Leftrightarrow y^{b_{i+1}} \cdot a^{b_i} = c \Leftrightarrow y^{b_{i+1}} = c \cdot a^{-b_i}$ for every $a, c \in Q$ and for every $i \in \{0, 1, 2, \ldots, s\}$. So $(\overset{1}{\triangle}), (\overset{2}{\triangle}), \ldots, (\overset{s}{\triangle})$ are quasigroup operations if and only if the mappings $x \mapsto x^{b_i}$, where $(b_i)_{i\in\mathbb{N}}$ is the Fibonacci sequence, are bijections for every $i \in \{0, 1, 2, \ldots, s + 1\}$. □

Proposition 4. *If $Q(\cdot)$ is an arbitrary recursively s-differentiable binary group, where $s \geq 1$, then the mappings $x \mapsto x^{b_i}$, where $(b_i)_{i\in\mathbb{N}}$ is the Fibonacci sequence, are bijections for all $i \in \{0, 1, 2, \ldots, s + 1\}$.*

Proof: If $Q(\cdot)$ is recursively s-differentiable, with unit e, then each of the equations $e \overset{i}{\triangle} x = c$ and $y \overset{i}{\triangle} e = c$, $i \in \{0, 1, 2, \ldots, s\}$, has a unique solution. So as

$e\overset{i}{\triangle}x = c \Leftrightarrow x^{b_{i+1}} = c$ and $y\overset{i}{\triangle}e = c \Leftrightarrow y^{b_i} = c$, we get that each of the mappings $x \mapsto x^{b_i}, \ \ i \in \{0, 1, 2, \ldots, s+1\}$, is a bijection. □

When $s = 1$ Theorem 1 is true for an arbitrary binary group as we can see from the following proposition.

Proposition 5. *A binary group $Q(\cdot)$ is recursively 1-differentiable if and only if the mapping $z \mapsto z^2$ is a bijection.*

Proof: According to the definition, a binary group $Q(\cdot)$ is recursively 1-differentiable if and only if its 2-recursive derivative $(\overset{1}{\triangle})$ is a quasigroup operation. So as $a\overset{1}{\triangle}x = b \Leftrightarrow x \cdot ax = b \Leftrightarrow xaxa = ba \Leftrightarrow (xa)^2 = ba$, for every $a, b \in Q$, we get that the mapping $z \mapsto z^2$ is a bijection if and only if the equation $a\overset{1}{\triangle}(za^{-1}) = b$ has a unique solution z for every $a, b \in Q$.

From the equivalences $x\overset{1}{\triangle}a = b \Leftrightarrow a \cdot xa = b \Leftrightarrow x = a^{-1}ba^{-1}$ it follows that in a binary quasigroup $Q(\cdot)$ the equation $x\overset{1}{\triangle}a = b$ has always a unique solution for every $a, b \in Q$. So if $Q(\cdot)$ is a group then $Q(\overset{1}{\triangle})$ is a quasigroup if and only if the mapping $z \mapsto z^2$ is a bijection. □

Corollary. *A finite binary group is recursively 1-differentiable if and only if it is of odd order.*

Indeed, it is known [3] that a finite group is of odd order if and only if the mapping $z \mapsto z^2$ is a bijection.

Proposition 6. *If $Q(\cdot)$ is a binary group with unit e, then $Q(\overset{1}{\triangle})$ is a semigroup if and only if $x^2 = e$, for every $x \in Q$.*

Proof: So as $(x\overset{1}{\triangle}y)\overset{1}{\triangle}z = zyxyz$ and $x\overset{1}{\triangle}(y\overset{1}{\triangle}z) = zyzxzyz$, for all $x, y, z \in Q$, we get that the operation $(\overset{1}{\triangle})$ is associative if and only if $x = zxz$, for every $x, z \in Q$. Taking $x = e$ in the last equality we get $z^2 = e$, for all $z \in Q$. Conversely, if $x^2 = e$, for all $x \in Q$, then $x = x^{-1}$ and $xz \cdot xz = e, \forall\, x, z \in Q$, so $zxz = x^{-1} = x$, for all $x, z \in Q$, i.e. $(\overset{1}{\triangle})$ is associative. □

Corollary. *If $Q(\cdot)$ is a nontrivial recursively 1-differentiable group then its 2-recursive derivative $Q(\overset{1}{\triangle})$ cannot be a group.*

Proof: Indeed, if $Q(\cdot)$ is recursively 1-differentiable and $Q(\overset{1}{\triangle})$ is a group, then according to Proposition 5, the mapping $z \mapsto z^2$ is a bijection and by Proposition 6 we get $|Q| = 1$. □

Acknowledgment. The research described here in this publication was made possible in part by Award No. MM1-3040 of the Moldovan Research and Development Association (MRDA) and the U.S. Civilian Research Development Foundation for the Independent States of the Former Soviet Union (CRDF).

References

[1] Couselo E., Gonzalez S., Markov V., Nechaev A., *Recursive MDS-codes and recursively differentiable quasigroups*, Diskret. Mat. **10** (1998), no. 2, 3–29 (in Russian).

[2] Couselo E., Gonzalez S., Markov V., Nechaev A., *The parameters of recursive MDS-codes*, Diskret. Mat. **12** (2000), no. 4, 3–24 (in Russian).

[3] Dénes J., Keedwell A.D., *Latin Squares and Their Applications*, Academic Press, New York, 1974.

[4] Abashin A.S., *Linear recursive MDS-codes of dimension* 2 *and* 3, Diskret. Mat. **12** (2000), no. 2, 140–153 (in Russian).

[5] Izbash V., Syrbu P., *On recursively differentiable binary quasigroups*, Proceedings of the 11-th Conf. on Applied and Industrial Mathematics, 2003, May 29–31, Oradea, Romania, Vol. 1, pp. 149–152.

[6] MacWilliams F.J., Sloane N.J.A., *Theory of error correcting codes*, Sviazi, Moscow, 1979 (in Russian).

[7] Belyavskaya G.B., *On r-differentiable quasigroups*, Abstracts of the Int. Conf. on Pure and Applied Math. dedicated to D.A. Grave, Kiev, 2002, pp. 11–12.

Institute of Mathematics and Computer Science, Academy of Sciences, Academiei str. 5, MD-2028 Chisinau, Moldova

E-mail: vizb@math.md

State University of Moldova, Mateevici str. 60, MD-2009 Chisinau, Moldova

E-mail: psyrbu@mail.md

(*Received* October 11, 2003, *revised* December 22, 2003)