On the order of recursive differentiability of finite binary quasigroups

Parascovia Syrbu

Abstract. The recursive derivatives of an algebraic operation are defined in [1], where they appear as control mappings of complete recursive codes. It is proved in [1], in particular, that the recursive derivatives of order up to \( r \) of a finite binary quasigroup \((Q, \cdot)\) are quasigroup operations if and only if \((Q, \cdot)\) defines a recursive MDS-code of length \( r + 3 \). The author of the present note gives an algebraic proof of an equivalent statement: a finite binary quasigroup \((Q, \cdot)\) is recursively \( r \)-differentiable \((r \geq 0)\) if and only if the system consisting of its recursive derivatives of order up to \( r \) and of the binary selectors, is orthogonal. This involves the fact that the maximum order of recursive differentiability of a finite binary quasigroup of order \( q \) does not exceed \( q - 2 \).


Keywords and phrases: quasigroup, recursive derivative, recursively differentiable quasigroup.

The notions of recursive derivative and recursively differentiable quasigroup have been introduced in [1], where the authors considered recursive MDS-codes (Maximum Distance Separable codes).

Let denote by \( A^{(t)} \) the recursive derivative of order \( t \geq 0 \) of a binary groupoid \((Q, A)\), which is defined as follows:

\[
A^{(0)} = A, \\
A^{(1)}(x, y) = A(y, A^{(0)}(x, y)), \\
A^{(t)}(x, y) = A(A^{(t-2)}(x, y), A^{(t-1)}(x, y)), \quad \forall t \geq 2, \forall x, y \in Q.
\]

A quasigroup \((Q, A)\) is called recursively \( r \)-differentiable if the recursive derivatives \( A^{(0)}, A^{(1)}, ..., A^{(r)} \) are quasigroup operations \((r \geq 0)\).

The notion of recursive derivative of a \( k \)-ary quasigrup \((Q, A)\), where \( k \geq 2 \), is defined in a similar way:

\[
A^{(0)} = A, \\
A^{(t)}(x_1^k) = A(x_{t+1}, ..., x_k, A^{(0)}(x_1^k), ..., A^{(t-1)}(x_1^k)), \text{ if } 1 \leq t < k; \\
A^{(t)}(x_1^k) = A(A^{(t-k)}(x_1^k), ..., A^{(k-1)}(x_1^k)), \text{ if } t \geq k, \forall x_1, ..., x_k \in Q
\]

(we denote by \( x_1^k \) the sequence \( x_1, x_2, ..., x_k \)).

The length \( n \) of the codewords in a \( k \)-recursive code

\[
C(n, A) = \{(x_1, ..., x_k, A^{(0)}(x_1^k), ..., A^{(n-k-1)}(x_1^k)) | x_1, ..., x_k \in Q\}
\]
given on an alphabet $Q$ of $q$ elements, where $A : Q^k \rightarrow Q$ is the defining $k$-ary operation, satisfies the condition $n \leq r + k + 1$, where $r$ is the maximum order of the used recursive derivatives of $(Q, A)$. On the other hand, $C(n, A)$ is an MDS-code if and only if $d = n - k + 1$, where $d$ is the minimum Hamming distance of this code. At present it is an open problem to determine all triplets $(n, d, q)$ of natural numbers such that there exists an MDS-code $C$ of length $n$, on an alphabet of $q$ elements, with $|C| = q^k$ and with the minimum Hamming distance $d$, for each $k \geq 2$. This general question implies, in particular, the problem of determining the maximum order of recursive differentiability of finite $k$-ary quasigroups ($k \geq 2$).

It is known that there exist recursively 1-differentiable finite binary quasigroups of each order, excepting 1, 2, 6, and possibly 14, 18, 26 [1, 2]. Estimations of the maximum order $r$ of recursive differentiability of finite $n$-quasigroups ($n \geq 2$) are given in [1,3–6]. General properties of recursively differentiable binary quasigroups are studied in [5,8].

The recursive differentiability of quasigroups is closely connected to the orthogonality of the recursive derivatives [1,5,8]. It is shown in [1] that a $k$-quasigroup defines an MDS-code of length $n$ if and only if its first $n - k - 1$ recursive derivatives are strongly orthogonal. Hence the defining $k$-quasigroup operation of a recursive MDS-code of length $n$ is recursively $(n - k - 1)$-differentiable. On the other hand, it is known that a system of binary quasigroups is strongly orthogonal if and only if it is (simply) orthogonal [7]. It is proved in [1] that the recursive derivatives of order up to $r$ of a finite binary quasigroup $(Q, *)$ are quasigroup operations if and only if $(Q, *)$ defines a recursive MDS-code of length $r + 3$.

In the present note we give an algebraic proof of the statement: a finite binary quasigroup $(Q, *)$ is recursively $r$-differentiable if and only if the system consisting of its recursive derivatives of order up to $r$ is strongly orthogonal. This statement implies the fact that $r \leq q - 2$, where $q = |Q|$ and $r$ is the maximum order of the recursive differentiability of the quasigroup $Q$.

Two binary operations $A$ and $B$, defined on a set $Q$, are called orthogonal if the system of equations $A(x, y) = a, B(x, y) = b$ has a unique solution in $Q$, for every $a, b \in Q$. It follows from the previous definition that two binary operations $A$ and $B$, defined on a set $Q$, are orthogonal if and only if the mapping

$$\sigma : Q \times Q \mapsto Q \times Q, \sigma(x, y) = (A(x, y), B(x, y))$$

is a bijection.

A system of binary operations $\{A_1, A_2, ..., A_n\}$, $n \geq 2$, is said to be orthogonal if each two operations are orthogonal.

Denoting by $F$ and $E$ the binary selectors on a set $Q$: $F(x, y) = x$ and $E(x, y) = y$, $\forall x, y \in Q$, we get that a binary groupoid $(Q, A)$ is a quasigroup if and only if $A$ is orthogonal to each of two selectors.

Let $(Q, A)$ be a binary quasigroup. It was observed by G. Belyavskaya [8] that $A^{(k)} = A\theta^n, \forall k \geq 1$, where $\theta = (E, A)$. An analogous representation for the recursive derivatives of $k$-ary operations ($k \geq 2$) was given in [5].
Theorem 1. A finite binary quasigroup \((Q, A)\) is recursively \(n\)-differentiable if and only if the system \(\{F, E, A, A^{(1)}, \ldots, A^{(n)}\}\) is orthogonal.

Proof. Let \((Q, A)\) be a recursively \(n\)-differentiable finite binary quasigroup. Then the recursive derivatives \(A^{(1)}, \ldots, A^{(n)}\) are quasigroup operations, so each recursive derivative \(A^k\) of the system is orthogonal to the selectors \(F\) and \(E\).

Now, let \(k\) and \(s\) be two distinct numbers between 0 and \(n\): \(0 \leq k < s \leq n\). As \(\langle A^{(k)}, A^{(s)} \rangle = \langle A^{(s-k)} \theta, A^k \rangle\), where \(\theta = (E, A)\) is a bijection, we get that \(A^{(k)}\) and \(A^{(s)}\) are orthogonal if and only if \(A\) and \(A^{(s-k)}\) are orthogonal, i.e. if and only if \(A\) and \(A^{(m)}\) are orthogonal, for every \(m = 1, 2, \ldots, n\). On the other hand,

\[
A^{(m)}(x, y) = A^{(m-1)}(E, A)(x, y) = A^{(m-1)}(y, A(x, y)),
\]

hence the system of equations

\[
\begin{align*}
    A(x, y) &= a, \\
    A^{(m)}(x, y) &= b,
\end{align*}
\]

is equivalent to

\[
\begin{align*}
    A(x, y) &= a, \\
    A^{(m-1)}(y, a) &= b,
\end{align*}
\]

which has a unique solution as \(A\) and \(A^{(m-1)}\) are quasigroup operations. Therefore the system \(\{F, E, A, A^{(1)}, \ldots, A^{(n)}\}\) is orthogonal.

Conversely, if the system \(\{F, E, A, A^{(1)}, \ldots, A^{(n)}\}\) is orthogonal, then each of the recursive derivatives \(A, A^{(1)}, \ldots, A^{(n)}\) is orthogonal to the selectors \(F\) and \(E\), hence the recursive derivatives of order up to \(n\) are quasigroup operations, i.e. \((Q, A)\) is recursively \(n\)-orthogonal.

Corollary 1. The maximum order \(r\) of recursive differentiability of a finite binary quasigroup of order \(q\) does not exceed \(q - 2\).

Proof. The proof follows from the fact that there exist at most \(q - 1\) pairwise orthogonal latin squares of order \(q\), which implies that the maximum order \(r\) of recursive differentiability satisfies the inequality \(r + 1 \leq q - 1\), hence \(r \leq q - 2\).

It is shown in [1] that there exist recursively \((q - 2)\)-differentiable finite binary quasigroups of every primary order \(q \geq 3\). However, it is an open problem to find the maximum order of recursive differentiability of finite \(k\)-ary quasigroups of order \(q\), for \(k \geq 2\) and an arbitrary non-primary \(q\).

Acknowledgment. This work is partially supported by National Agency for Research and Development of the Republic of Moldova, project 20.80009.5007.25.
References


Parascovia Syrbu

Moldova State University,
Department of Mathematics
E-mail: parascovia.syrbu@gmail.com

Received July 21, 2022