Chapter 3

MDS codes based on orthogonality of quasigroups

A Latin square corresponding to set with cardinality n, is an $n \times n$ array arranged in such a manner that each symbol occurs exactly once in each row and column. It is known that a binary quasigroup is an algebraic equivalent of a Latin squares. In [33, 34], Dénes and Keedwell defined mutually orthogonal Latin squares (MOLS) as a set in which every pair of distinct Latin squares is orthogonal. In general, superimposition of k Latin squares yields a k-dimensional hypercube (also known as k-hypercube). It is an $n \times n \times \cdots \times n$ (k-times) array with n^k ordered tuples containing entries from a set with n symbols. Further in 1998, Mullen and Whittle [79] classified a k-hypercube as type-j if any j elements out of the k coordinates are fixed, and each of n-symbols appears n^{k-j-1} times in that subarray. In particular, a Latin square is a 2-dimensional hypercube of type-1. This work led to observe orthogonality of k-hypercubes. A k sized set with k-hypercubes is said to be k-orthogonal if, when superimposed, each of the n^k ordered k-tuples occur exactly once. A set of $m(\geq k)$ k-hypercubes is called *mutually k-orthogonal* if its every k sized subset is k-orthogonal. In 2012, Ethier and Mullen [46] defined that for $2 \leq j \leq k$, a j sized set of k-hypercubes is said to be j-orthogonal if, superimposed each of the n^j ordered j-tuples occurs exactly n^{k-j} times. For more literature on Latin squares, the reader may refer a good survey [31, 33–35]. In 1998, Couselo et al. [29] defined a recursive MDS codes of dimension 2 and 3 using quasigroup. In 2001, Abashin [1] proposed a linear complete recursive codes with dimension 2 and 3 using the k-orthogonality of quasigroup.

The code $\mathcal{K}$ is said to be complete k-recursive code [29] if there exists a map $f : Q^k \to Q$, where $k \leq n$ and Q is a finite set, such that

$$\mathcal{K} = \{(u_0, u_1, \ldots, u_{n-1}) \in Q^n \ : \ u_{i+k} = f(u_i, \ldots, u_{i+k-1}),\ 0 \leq i \leq n-k-1\}.$$

Thus, $\mathcal{K}$ is denoted as $\mathcal{K}(n|f)$. There are some generic constructions for linear recursive maximum distance separable (MDS) codes and their related parameters are discussed in [1, 29]. More broadly, there are other classes of error-correcting codes like almost MDS codes, near MDS codes, Linear complimentary dual (LCD) MDS codes and self-dual MDS codes have been described in [19, 54, 82, 129]. In [74], Krotov proposed the 4-ary MDS code with distance 2 based on the n-ary quasigroups of order 4. In conclusion, design of these classes of error-correcting codes are of practical importance as there is always a need for optimization in terms of channel bandwidth and error correction capacity.

In this chapter, we work towards the extended invertibility and orthogonality of k-ary operations. We propose a novel construction of MDS codes using extended invertibility of k-ary operations and the orthogonality of quasigroups.

This chapter is divided into several sections: In Section 3.1, we discuss some basics of orthogonality and recursive derivatives of a quasigroup. Additionally, we discuss the definition of recursive codes. In Section 3.2, we define the notion of extended-i-invertibility of a k-ary operation and we provide various methods for constructing the orthogonal system of k-ary operations over Q^2. In Section 3.3, we propose a class of recursive MDS codes of dimensions 2 and 3 based on the mutually strong k-orthogonality of the system of k-ary operations over Q^2. We also include some examples to support our theory along with the enumeration of such codes using SageMath.

3.1 Recursive derivatives and orthogonality of quasigroups

Definition 3.1.1. [89] Consider a non-empty set Q and let g be a k-ary operation defined over Q such that for each k-tuple $(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_k, a_{k+1}) \in Q^k$, if there exists a unique 'x' for the equation

$$g(a_1, \ldots, a_{i-1}, x, a_{i+1}, \ldots, a_k) = a_{k+1}, \tag{3.1}$$

then g is said to be *i-invertible* operation.

It follows that (Q, g) is a k-ary quasigroup if g is an i-invertible operation for each $i \in \{1, 2, \ldots, k\}$. Let ${}^{[i]}g$, $1 \leq i \leq k$ be the i^{th} inverse operation of g. Then, the following identities in algebra $(Q, g, {}^{[i]}g)$ holds:

$$g\left(x_1, \ldots, x_{i-1}, {}^{[i]}g(x_1, \ldots, x_k), x_{i+1}, \ldots, x_k\right) = x_i;$$
$${}^{[i]}g\left(x_1, \ldots, x_{i-1}, g(x_1, \ldots, x_k), x_{i+1}, \ldots, x_k\right) = x_i.$$

Definition 3.1.2. [14] For $1 \leq l \leq k$, an l-tuple $\langle G_1, \ldots, G_l \rangle$ of different k-ary operations over an n-sized set Q is called an *orthogonal* system if the system of l-equations $\{G_i(x_1, \ldots, x_k) = a_i\}_{i=1}^{l}$ has exactly n^{k-l} solutions for any $(a_1, \ldots, a_l) \in Q^l$. In particular if $l = k$, such a k-tuple $\langle G_1, \ldots, G_k \rangle$ of different k-ary operations is orthogonal if the system $\{G_i(x_1, \ldots, x_k) = a_i\}_{i=1}^{k}$ has a unique solution for each $(a_1, \ldots, a_k) \in Q^k$.

Definition 3.1.3. [14] A set $\{G_1, G_2, \ldots, G_m\}$ of k-ary operations is said to be k-orthogonal, if for $k \leq m$, if every k-tuple $\langle G_{i_1}, G_{i_2}, \ldots, G_{i_k} \rangle$ of distinct k-ary operations is orthogonal.

Definition 3.1.4. [46] A set $\omega = \{G_1, \ldots, G_r\}$ of distinct k-ary operations over Q is said to be k-strong orthogonal if the set $\{e_1, e_2, \ldots, e_k, G_1, G_2, \ldots, G_r\}$ is k-orthogonal, where $e_i(x_1, x_2, \ldots, x_k) = x_i$, for $1 \leq i \leq k$.

Theorem 3.1.5. [83] (The Singleton Bound) *For any $[n, k, d_H]$-code, the distance $d_H \leq n - k + 1$. Codes in which the distance $d_H = n - k + 1$, are called maximum distance separable (MDS) codes. An MDS code can correct up to $\left\lfloor \frac{n-k}{2} \right\rfloor$ errors.*

For a k-ary operation g over Q, the *recursive derivatives* of g at $x = (x_1, x_2, \ldots, x_k) \in Q^k$are defined as:

$$\begin{aligned}
d^0 g(x) &= g(x_1, x_2 \ldots, x_k), \\
d^1 g(x) &= g\left(x_2, x_3, \ldots, x_k, d^0 g(x)\right), \\
d^2 g(x) &= g\left(x_3, x_4, \ldots, x_k, d^0 g(x), d^1 g(x)\right), \\
&\vdots \\
d^{k-1} g(x) &= g\left(x_k, d^0 g(x), d^1 g(x), \ldots, d^{k-2} g(x)\right), \\
d^k g(x) &= g\left(d^0 g(x), d^1 g(x), \ldots, d^{k-2} g(x), d^{k-1} g(x)\right). \qquad (3.2)
\end{aligned}$$

Using above notion, a complete k-recursive $[2k+1, k]$ code $\mathcal{K}$ over Q is:

$$\mathcal{K}\left((2k+1) \mid g\right) = \left\{\left(x_1, \ldots, x_k, d^0 g, d^1 g, \ldots, d^k g\right) \in Q^{2k+1}\right\}.$$

Here, in the right side of the equality $d^i g$ denotes $d^i g(x)$ as described in (3.2) for $0 \leq i \leq k$.

Definition 3.1.6. [29] A k-ary quasigroup operation g over Q is said to be *recursively t-differentiable* for $t \in \mathbb{N}$, if $(Q, d^i g)$ forms k-ary quasigroups for $0 \leq i \leq k$, where $d^i g$ are described in (3.2).

Proposition 3.1.7. [29] *For any k-ary quasigroup (Q, g), the code $\mathcal{K}\left((k+1) \mid d^0 g\right) = \left\{(x_1, \ldots, x_k, d^0 g) \in Q^{k+1}\right\}$ is an MDS code.*

Definition 3.1.8. [80] A polynomial $g \in \mathbb{F}_q[x_1, \ldots, x_k]$ is said to be a *permutation polynomial over* $\mathbb{F}_q$ if the equation $g(x_1, \ldots, x_k) = \alpha$ has exactly q^{k-1} solutions in $\mathbb{F}_q^k$ for every $\alpha \in \mathbb{F}_q$.

As a consequence, a linear polynomial $g(x_1, \ldots, x_k) = a_1x_1 + \cdots + a_kx_k$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $(a_1, \ldots, a_k) \neq (0, \ldots, 0)$. Following Definition 3.1.2, since multivariate polynomials in $\mathbb{F}_q[x_1, \ldots, x_k]$ are k-ary operations, a set of l such polynomials $\{g_1, \ldots, g_l\}$ with $1 \leq l \leq k$ forms an orthogonal system if the system of l-equations $g_i(x_1, \ldots, x_k) = \alpha_i$, $i = 1, \ldots, l$ has exactly q^{k-l} solutions in $\mathbb{F}_q^l$ for each l-tuple $(\alpha_1, \ldots, \alpha_l)$ in $\mathbb{F}_q^l$.

Theorem 3.1.9. [46] *Consider a set of r-linear polynomials $g_i(x_1, \ldots, x_k) = a_{i,1}x_1 + a_{i,2}x_2 + \cdots + a_{i,k}x_k$, for $1 \leq i \leq r$ over $\mathbb{F}_q$. Then, the set of r-tuple $\langle g_1, \ldots, g_r \rangle$ forms a set of mutually strong k-orthogonal system of order q and dimension k if and only if every square sub-matrix of the $r \times k$ matrix $M = (a_{i,j})$ is invertible.*

Theorem 3.1.10. [46] *Consider a set of r-linear polynomials $g_i(x_1, \ldots, x_k) = a_{i,1}x_1 + a_{i,2}x_2 + \cdots + a_{i,k}x_k$, for $1 \leq i \leq r$ and $r \geq k$ over $\mathbb{F}_q$. Then, the set of r-tuple $\langle g_1, \ldots, g_r \rangle$ forms a set of mutually k-orthogonal system of order q and dimension k if and only if every k rows of the $r \times k$ matrix $M = (a_{i,j})$ are linearly independent.*

As an application to Theorem 5 of [29], it is easy to observe the following:

Theorem 3.1.11. *Consider a k-recursive code $\mathcal{K}(n \mid G_1, G_2, \ldots, G_k)$ over $\mathbb{F}_q$ in which $G_i(x_1, \ldots, x_{n-k}) = a_{1,i}x_1 + a_{2,i}x_2 + \cdots + a_{n-k,i}x_{n-k}$ for $1 \leq i \leq k$. Let $M = (a_{i,j})_{r \times k}$ be the coefficient matrix as defined in Theorem 3.1.9. If every sub-matrix of M is invertible, then $\mathcal{K}$ is an MDS $[n, n-k]$-code i.e., if $\langle G_i \ : \ 1 \leq i \leq k \rangle$ forms a mutually strong k-orthogonal system.*

For detailed theory on quasigroups and MDS codes, reader may refer (see, [83, 116])

3.2 Orthogonal system of k-ary operations

Definition 3.2.1. Let g and h be i-invertible k-ary operations over Q. Let G, a k-ary operation over Q^2, be defined as

$$G((a_1, a_2), (a_3, a_4), \ldots, (a_{2k-1}, a_{2k})) = (g(a_1, a_3, \ldots, a_{2k-1}), h(a_2, a_4, \ldots, a_{2k})). \tag{3.3}$$

Then G is said to be *extended-i-invertible* operation if each tuple $(a_1, a_2, \ldots, a_{2i-2}, a_{2i+1}, \ldots, a_{2k}, a_{2k+1}, a_{2k+2}) \in Q^{2k}$ determines a unique $(x, y) \in Q^2$ such that

$$G((a_1, a_2), \ldots, \underbrace{(x, y)}_{i^{th}}, \ldots, (a_{2k-1}, a_{2k})) = (a_{2k+1}, a_{2k+2}). \tag{3.4}$$

Thus the extended-i-invertibility is an extension of two i-invertible operations, which can be further extended too. This extension provide new algebraic properties to explore and an application of these can be observed in various fields like coding theory and cryptography. We explore properties in constructing new family of MDS code.

Note. Throughout the chapter $G_i^{(j)}$ means $G_i^{(j)}(x_j, x_{j+2}, \ldots, x_{j+2k-2})$ for $x_1, x_2, \ldots, x_{2k} \in Q$ and $j \in \{1, 2\}$.

Theorem 3.2.2. *Let g_i be an i-invertible k-ary operation over Q for $i = 1, 2, \ldots, k$. Then the k-tuple $\langle G_1, G_2, \ldots, G_k \rangle$ defined by:*

$$\begin{aligned}
G_1(x_1, \ldots, x_{2k}) &= (g_1(x_1, x_3, \ldots, x_{2k-1}), g_1(x_2, x_4, \ldots, x_{2k})) = \left(G_1^{(1)}, G_1^{(2)}\right); \\
G_2(x_1, \ldots, x_{2k}) &= \left(g_2(G_1^{(1)}, x_3, x_5, \ldots, x_{2k-1}), g_2(G_1^{(2)}, x_4, x_6, \ldots, x_{2k})\right) = \left(G_2^{(1)}, G_2^{(2)}\right); \\
G_3(x_1, \ldots, x_{2k}) &= \left(g_3(G_1^{(1)}, G_2^{(1)}, x_5, \ldots, x_{2k-1}), g_3(G_1^{(2)}, G_2^{(2)}, x_6, \ldots, x_{2k})\right) = \left(G_3^{(1)}, G_3^{(2)}\right); \\
&\vdots \\
G_k(x_1, \ldots, x_{2k}) &= \left(g_k(G_1^{(1)}, G_2^{(1)}, \ldots, G_{k-1}^{(1)}, x_{2k-1}), g_k(G_1^{(2)}, G_2^{(2)}, \ldots, G_{k-1}^{(2)}, x_{2k})\right) = \left(G_k^{(1)}, G_k^{(2)}\right).
\end{aligned} \tag{3.5}$$

is an orthogonal system of k-ary operations over Q^2.

Proof. Let $(a_1^{(1)}, a_1^{(2)}, a_2^{(1)}, a_2^{(2)}, \ldots, a_k^{(1)}, a_k^{(2)}) \in (Q^2)^k$ be fixed. Consider the system $\left\{G_i(x_1, x_2, \ldots x_{2k}) = (G_i^{(1)}, G_i^{(2)}) = (a_i^{(1)}, a_i^{(2)})\right\}_{i=1}^{k}$. On substituting the values of $(G_i^{(1)}, G_i^{(2)})_{1 \le i \le k-1}$ in the last equality of (3.5), we obtain

$$G_k(x_1, \ldots, x_{2k}) = (a_k^{(1)}, a_k^{(2)}) = G_k(a_1^{(1)}, a_1^{(2)}, a_2^{(1)}, a_2^{(2)}, \ldots, a_{k-1}^{(1)}, a_{k-1}^{(2)}, x_{2k-1}, x_{2k}). \tag{3.6}$$

Since g_k is k-invertible, we obtain a unique solution for (x_{2k-1}, x_{2k}), i.e., (say (b_{2k-1}, b_{2k})). Therefore G_k is an extended-k-invertible operation. Again, on substituting (x_{2k-1}, x_{2k}) as (b_{2k-1}, b_{2k}) and the values of $(G_i^{(1)}, G_i^{(2)})_{1 \le i \le k-2}$ into the $(k-1)^{th}$ equality of (3.5), we obtain

$$\begin{aligned}
G_{k-1}(x_1, \ldots, x_{2k-2}, b_{2k-1}, b_{2k}) &= \left(g_{k-1}(a_1^{(1)}, \ldots, a_{k-2}^{(1)}, x_{2k-3}), g_{k-1}(a_1^{(2)}, \ldots, a_{k-2}^{(2)}, x_{2k-2})\right) \\
&= \left(a_{k-1}^{(1)}, a_{k-1}^{(2)}\right).
\end{aligned}$$

As before, using the $(k-1)$-invertibility of g_{k-1}, we obtain a unique solution for (x_{2k-3}, x_{2k-2}), i.e.,(say (b_{2k-3}, b_{2k-2})). Therefore G_{k-1} is also extended-$(k-1)$-invertible. Proceeding in same manner till the first equality of (3.5), we have

$$G_1(x_1, \ldots, x_{2k}) = (g_1(x_1, b_3, b_5, \ldots, b_{2k-1}), g_1(x_2, b_4, b_6, \ldots, b_{2k})) = (a_1^{(1)}, a_1^{(2)}). \quad (3.7)$$

Finally we obtain a unique solution $(x_1, x_2) = (b_1, b_2)$ using 1-invertibility of g_1. As a conclusion, $\langle G_1, G_2, \ldots, G_k\rangle$ is an orthogonal system of k-ary operations over Q^2. □

It should be noted that instead of taking two coordinate-evaluations, the result can be easily extended for further coordinates.

Example 3.2.3. In Theorem 3.2.2, consider $Q = \mathbb{Z}_9$, g_1, g_2 and g_3 be 3-ary operations over $\mathbb{Z}_9$ which are defined as $g_1(a_1, a_2, a_3) = 2a_1 + 3a_3 + 3a_3$, $g_2(a_1, a_2, a_3) = 6a_1 + a_2 + 6a_3$ and $g_3(a_1, a_2, a_3) = 3a_1 + 3a_2 + 5a_3$. Then the 3-tuple $\langle G_1, G_2, G_3\rangle$ as defined in (3.2.2) as $G_i(x_1, \ldots, x_6) = (g_i(x_1, x_3, x_5), g_i(x_2, x_4, x_6))$, for $i \in \{1, 2, 3\}$. One can see that g_1, g_2 and g_3 are 1, 2 and 3-invertible 3-ary operations over $\mathbb{Z}_9$ respectively. So, G_i is extended-i-invertible operation over $\mathbb{Z}_9^2$ for each $i \in \{1, 2, 3\}$ respectively. Here the matrix M, as defined in Theorem 3.1.10, corresponding to the system $\langle g_1, g_2, g_3\rangle$ is $\begin{bmatrix} 2 & 3 & 3 \\ 3 & 1 & 6 \\ 6 & 3 & 5 \end{bmatrix}$ and $\det(M) = 1 \pmod 9 \neq 0$. This means $\langle g_1, g_2, g_3\rangle$ is mutually 3-orthogonal system over $\mathbb{Z}_9$ and hence the tuple $\langle G_1, G_2, G_3\rangle$ is also a 3-orthogonal system over $\mathbb{Z}_9^2$.

Theorem 3.2.4. *Let g_i be an $(k-i+1)$-invertible k-ary operation over Q for $i = 1, 2, \ldots, k$. Then the k-tuple $\langle G_1, G_2, \ldots, G_k\rangle$ defined by:*

$$\begin{aligned}
G_1(x_1, \ldots, x_{2k}) &= (g_1(x_1, x_3, \ldots, x_{2k-1}), g_1(x_2, x_4, \ldots, x_{2k})) = \left(G_1^{(1)}, G_1^{(2)}\right) \\
G_2(x_1, \ldots, x_{2k}) &= \left(g_2(x_1, x_3, \ldots, x_{2k-3}, G_1^{(1)}), g_2(x_2, x_4, \ldots, x_{2k-2}, G_1^{(2)})\right) = \left(G_2^{(1)}, G_2^{(2)}\right) \\
G_3(x_1, \ldots, x_{2k}) &= \left(g_3(x_1, x_3, \ldots, x_{2k-5}, G_1^{(1)}, G_2^{(1)}), g_3(x_2, x_4, \ldots, x_{2k-4}, G_1^{(2)}, G_2^{(2)})\right) = \left(G_3^{(1)}, G_3^{(2)}\right) \\
&\vdots \\
G_k(x_1, \ldots, x_{2k}) &= \left(g_k(x_1, G_1^{(1)}, G_2^{(1)}, G_3^{(1)}, \ldots, G_{k-1}^{(1)}), g_k(x_2, G_1^{(2)}, G_2^{(2)}, G_3^{(2)}, \ldots, G_{k-1}^{(2)})\right) = \left(G_k^{(1)}, G_k^{(2)}\right)
\end{aligned}$$

is an orthogonal system of k-ary operations over Q^2.

Intuitively, we can observe that the above results are also valid for arbitrary positions of $G_i^{(j)}$s in recursive definition of $\langle G_1, \ldots, G_k\rangle$. We prove this result in the following Theorem:

Theorem 3.2.5. *Let σ and π be permutations of $\{1,3,\ldots,2k-1\}$ and $\{2,4,\ldots,2k\}$ respectively. Let g_i and h_i be $\sigma(2i-1)$ and $\pi(2i)$-invertible k-ary operations respectively over Q for each $i \in \{1,2,\ldots,k\}$. Then the k-tuple $\langle G_1, G_2, \ldots, G_k\rangle$ defined by:*

$$\begin{aligned}
G_1(x_1,\ldots,x_{2k}) &= (g_1(x_1,x_3,\ldots,x_{2k-1}), h_1(x_2,x_4,\ldots,x_{2k})) = \left(G_1^{(1)}, G_1^{(2)}\right);\\
G_2(x_1,\ldots,x_{2k}) &= \left(g_2(x_1,\ldots,x_{\sigma(1)-2}, G_1^{(1)}, x_{\sigma(1)+2},\ldots,x_{2k-1}), h_2(x_2,\ldots,x_{\pi(2)-2}, G_1^{(2)}, x_{\pi(2)+2},\ldots,x_{2k})\right)\\
&= \left(G_2^{(1)}, G_2^{(2)}\right);\\
G_j(x_1,\ldots,x_{2k}) &= \left(g_j(y_1,y_3,\ldots,y_{2k-1}), h_j(y_2,y_4,\ldots,y_{2k})\right) = \left(G_j^{(1)}, G_j^{(2)}\right),\ \textit{for } 3 \le j \le k, \qquad (3.8)
\end{aligned}$$

where $y_{\sigma(1)} = G_1^{(1)}$, $y_{\sigma(3)} = G_2^{(1)},\ldots,y_{\sigma(2j-3)} = G_{j-1}^{(1)}$; $y_{\pi(2)} = G_1^{(2)}$, $y_{\pi(4)} = G_2^{(2)},\ldots,$ $y_{\pi(2j-2)} = G_{j-1}^{(2)}$; and $y_\ell = x_\ell$ for $\ell \notin \{\sigma(1),\sigma(3),\ldots,\sigma(2j-3),\pi(2),\pi(4),\ldots,$ $\pi(2j-2)\}$. Then the k-tuple $\langle G_1, G_2, \ldots, G_k\rangle$ is an orthogonal system of k-ary operations over Q^2.

Proof. Let $(a_1^{(1)}, a_1^{(2)}, a_2^{(1)}, a_2^{(2)}, \ldots, a_k^{(1)}, a_k^{(2)}) \in (Q^2)^k$ be fixed. Consider the following system of k-ary operations over Q^2:

$$\left\{G_i(x_1,\ldots,x_{2k}) = (G_i^{(1)}, G_i^{(2)}) = (a_i^{(1)}, a_i^{(2)})\right\}_{i=1}^{k} \qquad (3.9)$$

On substituting the values of $(G_i^{(1)}, G_i^{(2)})_{1\le i\le k-1}$ into the last equality of (3.8), we get

$$G_k(x_1,\ldots,x_{2k}) = (g_k(y_1,y_3,\ldots,y_{2k-1}), h_k(y_2,y_4,\ldots,y_{2k})) = (a_k^{(1)}, a_k^{(2)}),$$

where $y_{\sigma(1)} = a_1^{(1)}, y_{\sigma(3)} = a_2^{(1)},\ldots,y_{\sigma(2k-3)} = a_{k-1}^{(1)}, y_{\pi(2)} = a_1^{(2)}, y_{\pi(4)} = a_2^{(2)},\ldots,$ $y_{\pi(2k-2)} = a_{k-1}^{(2)}$. Since $y_{\sigma(2k-1)} = x_{\sigma(2k-1)}$, $y_{\pi(2k)} = x_{\pi(2k)}$ and g_k and h_k are $\sigma(2k-1)$ and $\pi(2k)$-invertible operations, we obtain a unique solution for $(x_{\sigma(2k-1)}, x_{\pi(2k)})$, i.e., (say $(b_{\sigma(2k-1)}, b_{\pi(2k)})$). Again, on substituting the values of $(x_{\sigma(2k-1)}, x_{\pi(2k)})$ and $(G_i^{(1)}, G_i^{(2)})_{1\le i\le k-2}$ into the $(k-1)^{th}$ equality, we have

$$G_{k-1}(x_1,\ldots,b_{\pi(2k)},\ldots,b_{\sigma(2k-1)},\ldots,x_{2k}) = (g_{k-1}(y_1,y_3,\ldots,y_{2k-1}), h_k(y_2,y_4,\ldots,y_{2k})) = \left(a_{k-1}^{(1)}, a_{k-1}^{(2)}\right),$$

where $y_{\sigma(1)} = a_1^{(1)}, y_{\sigma(3)} = a_2^{(1)},\ldots,y_{\sigma(2k-5)} = a_{k-2}^{(1)};\ y_{\pi(2)} = a_1^{(2)}, y_{\pi(4)} = a_2^{(2)},\ldots,$ $y_{\pi(2k-4)} = a_{k-2}^{(2)}$ and $y_{\sigma(2k-1)} = b_{\sigma(2k-1)}, y_{\pi(2k)} = b_{\pi(2k)}$. Since $y_{\sigma(2k-3)} = x_{\sigma(2k-3)}$, $y_{\pi(2k-2)} = x_{\pi(2k-2)}$ and g_{k-1} and h_{k-1} are $\sigma(2k-3)$ and $\pi(2k-2)$-invertible operations, we obtain a unique solution for $x_{\sigma(2k-3)} = b_{\sigma(2k-3)}$, $x_{\pi(2k-4)} = b_{\pi(2k-4)}$. On continuing the same process, finally we obtain unique solution for $(x_{\sigma(1)}, x_{\pi(2)})$. Therefore, (3.9) has a unique solution, implying $\langle G_1,\ldots,G_k\rangle$ is an orthogonal

system of k-ary operations over Q^2. □

The next result is an immediate consequence of Theorem 3.2.5, considering a particular case when $g_1 = g_2 = \cdots = g_k (= g)$ and $h_1 = h_2 = \cdots = h_k (= h)$, where g and h are k-ary quasigroup operations.

Corollary 3.2.6. *Let σ and π be permutations of $\{1, 3, \ldots, 2k-1\}$ and $\{2, 4, \ldots, 2k\}$ respectively. Let (Q, g_1) and (Q, g_2) be k-ary quasigroups. Let the system of k-tuple $\langle G_1, \ldots, G_k\rangle$ be defined as:*

$$\begin{aligned}
G_1(x_1, \ldots, x_{2k}) &= (g_1(x_1, x_3, \ldots, x_{2k-1}), g_2(x_2, x_4, \ldots, x_{2k})) = \left(G_1^{(1)}, G_1^{(2)}\right);\\
G_2(x_1, \ldots, x_{2k}) &= \left(g_1(x_1, \ldots, x_{\sigma(1)-2}, G_1^{(1)}, x_{\sigma(1)+2}, \ldots, x_{2k-1}), g_2(x_2, \ldots, x_{\pi(2)-2}, G_1^{(2)}, x_{\pi(2)+2}, \ldots, x_{2k})\right)\\
&= \left(G_2^{(1)}, G_2^{(2)}\right);\\
G_j(x_1, \ldots, x_{2k}) &= (g_1(y_1, y_3, \ldots, y_{2k-1}), g_2(y_2, y_4, \ldots, y_{2k})) = \left(G_j^{(1)}, G_j^{(2)}\right), \ \textit{for } 3 \le j \le k, \quad (3.10)
\end{aligned}$$

where $y_{\sigma(1)} = G_1^{(1)}$, $y_{\sigma(3)} = G_2^{(1)}, \ldots, y_{\sigma(2j-3)} = G_{j-1}^{(1)}$; $y_{\pi(2)} = G_1^{(2)}$, $y_{\pi(4)} = G_2^{(2)}, \ldots, y_{\pi(2j-2)} = G_{j-1}^{(2)}$; and $y_\ell = x_\ell$ for $\ell \notin \{\sigma(1), \sigma(3), \ldots, \sigma(2j-3), \pi(2), \pi(4), \ldots, \pi(2j-2)\}$. Then the k-tuple $\langle G_1, G_2, \ldots, G_k\rangle$ is an orthogonal system of k-ary operations over Q^2.

Theorem 3.2.7. *Let the k-tuple $\langle g_1, g_2, \ldots, g_k\rangle$ be a collection of 1-invertible k-ary operations over Q. Then the k-tuple $\langle G_1, G_2, \ldots, G_k\rangle$ of k-ary operations defined as:*

$$\begin{aligned}
G_1(x_1, x_2, \ldots, x_{2k}) &= (g_1(x_1, x_3, \ldots, x_{2k-1}), g_1(x_2, x_4, \ldots, x_{2k}) = \left(G_1^{(1)}, G_1^{(2)}\right);\\
G_2(x_1, x_2, \ldots, x_{2k}) &= \left(g_2(x_3, x_5, \ldots, x_{2k-1}, G_1^{(1)}), g_2(x_4, x_6, \ldots, x_{2k}, G_1^{(2)})\right) = \left(G_2^{(1)}, G_2^{(2)}\right);\\
G_3(x_1, x_2, \ldots, x_{2k}) &= \left(g_3(x_5, x_7, \ldots, x_{2k-1}, G_1^{(1)}, G_2^{(1)}), g_3(x_6, x_8, \ldots, x_{2k}, G_1^{(2)}, G_2^{(2)})\right) = \left(G_3^{(1)}, G_3^{(2)}\right);\\
&\vdots\\
G_k(x_1, x_2, \ldots, x_{2k}) &= \left(g_k(x_{2k-1}, G_1^{(1)}, G_2^{(1)}, \ldots, G_{k-1}^{(1)}), g_k(x_{2k}, G_1^{(2)}, , \ldots, G_{k-1}^{(2)})\right) = \left(G_k^{(1)}, G_k^{(2)}\right).
\end{aligned} \quad (3.11)$$

is an orthogonal system of k-ary operations over Q^2.

Proof. Let $(a_1^{(1)}, a_1^{(2)}, a_2^{(1)}, a_2^{(2)}, \ldots, a_k^{(1)}, a_k^{(2)}) \in (Q^2)^k$ be fixed. Consider the system $\left\{G_i(x_1, x_2, \ldots, x_{2k}) = (G_i^{(1)}, G_i^{(2)}) = (a_i^{(1)}, a_i^{(2)})\right\}_{i=1}^{k}$ and substitute the values of $(G_i^{(1)}, G_i^{(2)})_{1 \le i \le k-1}$ into the last equality of (3.11), we obtain

$$G_k(x_1, x_2, \ldots, x_{2k}) = \left(g_k(x_{2k-1}, a_1^{(1)}, a_2^{(1)}, \ldots, a_{k-1}^{(1)}), g_k(x_{2k}, a_1^{(2)}, a_2^{(2)}, \ldots, a_{k-1}^{(2)})\right) = \left(a_k^{(1)}, a_k^{(2)}\right).$$

Since the g_k is 1-invertible, and G_k is extended-k-invertible operation, we get a unique solution (x_{2k-1}, x_{2k}), i.e., (say (b_{2k-1}, b_{2k})). Continuing in similar way as before, at last using the 1-invertibility of g_1, we have

$$G_1(x_1, x_2, b_3, \ldots, b_{2k-1}, b_{2k}) = (g_1(x_1, b_3, b_5, \ldots, b_{2k-1}), g_1(x_2, b_4, b_6, \ldots, b_{2k})) = \left(a_1^{(1)}, a_1^{(2)}\right)$$

and finally we get a unique solution of $(x_1, x_2) = (b_1, b_2)$. As a conclusion, the k-tuple $\langle G_1, G_2, \ldots, G_k\rangle$ is an orthogonal system of k-ary operations over Q^2. □

Example 3.2.8. In Theorem 3.2.7, consider $Q = \mathbb{Z}_9$, and the 1-ary operations g_1, g_2 and g_3 be $g_1(a_1, a_2, a_3) = a_1 + 3a_2 + 3a_3$, $g_2(a_1 + a_2 + a_3) = 2a_1 + 6a_2 + 3a_3$ and $g_3(a_1, a_2, a_3) = 5a_1 + 6a_2 + 6a_3$. Then the 3-tuple $\langle G_1, G_2, G_3\rangle$, defined in (3.11), where $G_i(x_1, \ldots, x_6) = (g_i(x_1, x_3, x_5), g_i(x_2, x_4, x_6))$ for $i \in \{1, 2, 3\}$. It is easy to observe that g_1, g_2 and g_3 are 1-invertible 3-ary operations over $\mathbb{Z}_9$. So, it can be readily perceived that G_i are extended-i-invertible 3-ary operations over $\mathbb{Z}_9^2$ respectively. Here the coefficient matrix M, as defined in Theorem 3.1.10, corresponding to the system $\langle g_1, g_2, g_3\rangle$ is $\begin{bmatrix} 1 & 3 & 3 \\ 3 & 2 & 0 \\ 6 & 3 & 8 \end{bmatrix}$ and $det(M) = 7 \pmod 9 \neq 0$. This means $\langle g_1, g_2, g_3\rangle$ is mutually 3-orthogonal system over $\mathbb{Z}_9$ and hence the tuple $\langle G_1, G_2, G_3\rangle$ is a 3-orthogonal system over $\mathbb{Z}_9^2$.

As a generalization to the above Theorems, we now do not restrict to the position of i-invertibility of any k-ary operation. Additionally, the underlying k-ary operations can also be distinct. Using these criterion, we now derive some more results.

In this direction, recall from Definition 3.1.3 that the set $\{G_1, G_2, \ldots, G_{k+1}\}$ of k-ary operations is said to be k-orthogonal, if every k-tuple $\langle G_{i_1}, G_{i_2}, \ldots, G_{i_k}\rangle$ of distinct k-ary operations from $\{G_1, G_2, \ldots, G_{k+1}\}$ is orthogonal.

Motivated by this, note that in Corollary 3.2.6 we proved that the k-tuple $\langle G_1, \ldots, G_k\rangle$ is an orthogonal system of k-ary operations over Q^2. We now extend a particular version of Corollary 3.2.6 to a $(k+1)$-tuple $\langle G_1, \ldots, G_k, G_{k+1}\rangle$ system in the following result:

Theorem 3.2.9. *Let (Q, g_1) and (Q, g_2) be k-ary quasigroups, then a $(k+1)$-tuple $\langle G_1, G_2, \ldots, G_{k+1}\rangle$ defined as:*

$$\begin{aligned}
G_1(x_1, \ldots, x_{2k}) &= (g_1(x_1, x_3, \ldots, x_{2k-1}), g_2(x_2, x_4, \ldots, x_{2k})) = \left(G_1^{(1)}, G_1^{(2)}\right), \\
G_2(x_1, \ldots, x_{2k}) &= \left(g_1(x_1, x_3, \ldots, x_{2k-3}, G_1^{(1)}), g_2(x_2, x_4, \ldots, x_{2k-2}, G_1^{(2)})\right) = \left(G_2^{(1)}, G_2^{(2)}\right), \\
G_3(x_1, \ldots, x_{2k}) &= \left(g_1(x_1, \ldots, x_{2k-5}, G_1^{(1)}, G_2^{(1)}), g_2(x_2, \ldots, x_{2k-4}, G_1^{(2)}, G_2^{(2)})\right) = \left(G_3^{(1)}, G_3^{(2)}\right), \\
&\vdots
\end{aligned}$$

$$G_k(x_1,\dots,x_{2k}) = \left(g_1(x_1, G_1^{(1)}, G_2^{(1)}\dots, G_{k-1}^{(1)}), g_2(x_2, G_1^{(2)}, G_2^{(2)}, \dots, G_{k-1}^{(2)})\right) = \left(G_k^{(1)}, G_k^{(2)}\right),$$
$$G_{k+1}(x_1,\dots,x_{2k}) = \left(g_1(G_1^{(1)}, G_2^{(1)}, \dots, G_k^{(1)}), g_2(G_1^{(2)}, G_2^{(2)}, \dots, G_k^{(2)})\right) = \left(G_{k+1}^{(1)}, G_{k+1}^{(2)}\right).$$

is a k-orthogonal system of k-ary operations over Q^2.

Proof. It suffices to show that every k-subsystem of $\langle G_1, G_2, \dots, G_{k+1}\rangle$ is orthogonal. A general k-subsystem is given by:

$$\left\{G_i(x_1,\dots,x_{2k}) = \left(G_i^{(1)}, G_i^{(2)}\right) = \left(a_i^{(1)}, a_i^{(2)}\right)\right\}_{i\in\{1,2,\dots,k+1\}\setminus j} \tag{3.12}$$

where $j \in \{1, 2, \dots, k, k+1\}$.

Firstly, when $j = 1$ have the following k-subsystem:

$$\left\{G_i(x_1,\dots,x_{2k}) = \left(G_i^{(1)}, G_i^{(2)}\right) = \left(a_i^{(1)}, a_i^{(2)}\right)\right\}_{i=2}^{k+1} \tag{3.13}$$

Since $G_{k+1}(x_1,\dots,x_{2k}) = (a_{k+1}^{(1)}, a_{k+1}^{(2)})$ and $(g_1(x_1,\dots,x_{2k-1}),\ g_2(x_2,\dots,x_{2k})) = (G_1^{(1)}, G_1^{(2)})$, it follows that $(g_1(g_1(x_1,\dots,x_{2k-1}), a_2^{(1)},\dots,a_k^{(1)}), g_2(g_2(x_2,\dots,x_{2k}), a_2^{(2)},\ \dots, a_k^{(2)})) = (a_{k+1}^{(1)}, a_{k+1}^{(2)})$. Hence $G_1(x_1,\dots,x_{2k})$ is given as

$$\begin{aligned}(g_1(x_1,\dots,x_{2k-1}), g_2(x_2,\dots,x_{2k})) &= \left({}^{[1]}g_1(a_{k+1}^{(1)}, a_2^{(1)},\dots,a_k^{(1)}), {}^{[1]}g_2(a_{k+1}^{(2)}, a_2^{(2)},\dots,a_k^{(2)})\right)\\ &= \left(a_1^{(1)}, a_1^{(2)}\right)\end{aligned} \tag{3.14}$$

for some $(a_1^{(1)}, a_1^{(2)}) \in Q^2$, where $(Q, {}^{[1]}g_1)$ and $(Q, {}^{[1]}g_2)$ are 1-inverses of the k-ary quasigroups (Q, g_1) and (Q, g_2) respectively. Substituting these values in $G_1^{(1)}$ and $G_1^{(2)}$, we arrive at the $k+1$ system:

$$\left\{G_i(x_1,\dots,x_{2k}) = \left(G_i^{(1)}, G_i^{(2)}\right) = \left(a_i^{(1)}, a_i^{(2)}\right)\right\}_{i=1}^{k+1}$$

In particular the subsystem for $1 \le i \le k$ has a unique solution $x_1 = b_1, x_2 = b_2, \dots, x_{2k} = b_{2k}$ over Q using Corollary 3.2.6. Now in order to show (3.13) satisfies this solution, it remains to verify this for last equality, i.e.

$$G_{k+1}^{(1)}(b_1, b_3, \dots, b_{2k-1}) = g_1(G_1^{(1)}(b_1, b_3, \dots, b_{2k-1}), G_2^{(1)}(b_1, b_3, \dots, b_{2k-1}), \dots, G_k^{(1)}(b_1, b_3, \dots, b_{2k-1})),$$
$$G_{k+1}^{(2)}(b_2, b_4, \dots, b_{2k}) = g_2(G_1^{(2)}(b_2, b_4, \dots, b_{2k}), G_2^{(2)}(b_2, b_4, \dots, b_{2k}), \dots, G_k^{(2)}(b_2, b_4, \dots, b_{2k}))$$

and using (3.14), it implies

$$G_{k+1}^{(1)}(b_1, b_3, \dots, b_{2k-1}) = g_1({}^{[1]}g_1(a_{k+1}^{(1)}, a_2^{(1)}, \dots, a_k^{(1)}), a_2^{(1)}, \dots, a_k^{(1)}) = a_{k+1}^{(1)},$$
$$G_{k+1}^{(2)}(b_2, b_4, \dots, b_{2k}) = g_2({}^{[1]}g_2(a_{k+1}^{(2)}, a_2^{(2)}, \dots, a_k^{(2)}), a_2^{(2)}, \dots, a_k^{(2)}) = a_{k+1}^{(2)}.$$

So, we have $x_1 = b_1, x_2 = b_2, \ldots, x_{2k} = b_{2k}$ as the unique solution of the k-subsystem (3.13), which establishes its orthogonality.

Next, consider the k-subsystem by assuming $j \in \{2, 3, \ldots, k+1\}$ in (3.13). Note that

$$G_j(x_1, \ldots, x_{2k}) = \left(g_1\left(x_1, x_3, \ldots, x_{2(k-j)+1}, a_1^{(1)}, \ldots, a_{j-1}^{(1)}\right), g_2\left(x_2, x_4, \ldots, x_{2(k-j+1)}, a_1^{(2)}, \ldots, a_{j-1}^{(2)}\right)\right).$$

By substituting the values of G_t for $t \in \{1, 2, \ldots, k\}\backslash j$ in the equation $G_{k+1}(x_1, \ldots, x_{2k})$ $= (G_{k+1}^{(1)}, G_{k+2}^{(2)}) = (a_{k+1}^{(1)}, a_{k+1}^{(2)})$, we get

$$g_1(a_1^{(1)}, a_2^{(1)}, \ldots, a_{j-1}^{(1)}, g_1(x_1, x_3, \ldots, x_{2(k-j)+1}, a_1^{(1)}, \ldots, a_{j-1}^{(1)}), a_{j+1}^{(1)}, \ldots, a_k^{(1)}) = a_{k+1}^{(1)},$$
$$g_2(a_1^{(2)}, a_2^{(2)}, \ldots, a_{j-1}^{(2)}, g_2(x_2, x_4, \ldots, x_{2(k-j+1)}, a_1^{(2)}, \ldots, a_{j-1}^{(2)}), a_{j+1}^{(2)}, \ldots, a_k^{(2)}) = a_{k+1}^{(2)}.$$

Using j-invertibility of g_1 and g_2, we have

$$g_1\left(x_1, x_3, \ldots, x_{2(k-j)+1}, a_1^{(1)}, \ldots, a_{j-1}^{(1)}\right) =^{[j]} g_1\left(a_1^{(1)}, a_3^{(1)}, \ldots, a_{j-1}^{(1)}, a_{k+1}^{(1)}, a_{j+1}^{(1)}, \ldots, a_k^{(1)}\right) = a_j^{(1)},$$
$$g_2\left(x_2, x_4, \ldots, x_{2(k-j+1)}, a_1^{(2)}, \ldots, a_{j-1}^{(2)}\right) =^{[j]} g_2\left(a_1^{(2)}, a_3^{(2)}, \ldots, a_{j-1}^{(2)}, a_{k+1}^{(2)}, a_{j+1}^{(2)}, \ldots, a_k^{(2)}\right) = a_j^{(2)},$$

for some $(a_j^{(1)}, a_j^{(2)}) \in Q^2$. As the system

$$\left\{G_i(x_1, \ldots, x_{2k}) = \left(G_i^{(1)}, G_i^{(2)}\right) = \left(a_i^{(1)}, a_i^{(2)}\right)\right\}_{i=1}^{k}$$

has unique solution $x_1 = b_1$, $x_2 = b_2, \ldots, x_{2k} = b_{2k}$ over Q, it remains to verify this for the last equality i.e.,$G_{k+1}(b_1, \ldots, b_{2k}) = (G_{k+1}^{(1)}(b_1, b_3, \ldots, b_{2k-1}), G_{k+1}^{(2)}(b_2, b_4, \ldots, b_{2k}))$ and

$$\begin{aligned} G_{k+1}^{(1)}(b_1, \ldots, b_{2k-1}) &= g_1\left(a_1^{(1)}, \ldots, a_{j-1}^{(1)},^{[j]} g_1\left(a_1^{(1)}, \ldots, a_{j-1}^{(1)}, a_{k+1}^{(1)}, a_{j+1}^{(1)}, \ldots, a_k^{(1)}\right), a_{j+1}^{(1)}, \ldots, a_k^{(1)}\right) \\ &= a_{k+1}^{(1)}, \\ G_{k+1}^{(2)}(b_2, b_4, \ldots, b_{2k}) &= g_2\left(a_1^{(2)}, \ldots, a_{j-1}^{(2)},^{[j]} g_2\left(a_1^{(2)}, \ldots, a_{j-1}^{(2)}, a_{k+1}^{(2)}, a_{j+1}^{(2)}, \ldots, a_k^{(2)}\right), a_{j+1}^{(2)}, \ldots, a_k^{(2)}\right) \\ &= a_{k+1}^{(2)}. \end{aligned}$$

Finally, we conclude that (3.12) has a unique solution over Q for each j, thus the result holds. □

As a consequence, an immediate generalization of above Theorem 3.2.9 can be stated as the following result.

Theorem 3.2.10. *Let (Q, g_1) and (Q, g_2) be two k-ary quasigroups of order n, where σ and π be permutations of $\{1, 3, \ldots, 2k-1\}$ and $\{2, 4, \ldots, 2k\}$ respectively.*

Let the $(k+1)$-tuple $\langle G_1, \ldots, G_{k+1}\rangle$ be defined as:

$$\begin{aligned}
G_1(x_1,\ldots,x_{2k}) &= \left(g_1\left(x_1,x_3,\ldots,x_{2k-1}\right), g_2\left(x_2,x_4,\ldots,x_{2k}\right)\right) = \left(G_1^{(1)}, G_1^{(2)}\right);\\
G_2(x_1,\ldots,x_{2k}) &= \left(g_1\left(x_1,\ldots,x_{\sigma(1)-2},G_1^{(1)},x_{\sigma(1)+2},\ldots,x_{2k-1}\right), g_2\left(x_2,\ldots,x_{\pi(2)-2},G_1^{(2)},x_{\pi(2)+2},\ldots,x_{2k}\right)\right)\\
&= \left(G_2^{(1)}, G_2^{(2)}\right);\\
G_j(x_1,\ldots,x_{2k}) &= \left(g_1\left(y_1,y_3,\ldots,y_{2k-1}\right), g_2\left(y_2,y_4,\ldots,y_{2k}\right)\right) = \left(G_j^{(1)}, G_j^{(2)}\right),\ \textit{for } 3\le j\le k+1,
\end{aligned} \tag{3.15}$$

where $y_{\sigma(1)} = G_{j-1}^{(1)}$, $y_{\sigma(3)} = G_{j-2}^{(1)}, \ldots, y_{\sigma(2j-3)} = G_1^{(1)}$; $y_{\pi(2)} = G_{j-1}^{(2)}$, $y_{\pi(4)} = G_{j-2}^{(2)}, \ldots, y_{\pi(2j-2)} = G_1^{(2)}$; and $y_\ell = x_\ell$ for $\ell \notin \{\sigma(1),\sigma(3),\ldots,\sigma(2j-3),\pi(2),\ldots \pi(4),\pi(2j-2)\}$. Then the $(k+1)$-tuple $\langle G_1, G_2, \ldots, G_{k+1}\rangle$ is a k-orthogonal system of k-ary operations over Q^2.

Proof. To show that every k-subsystem of $\langle G_1, G_2, \ldots, G_{k+1}\rangle$ is orthogonal. A general k-subsystem is given by:

$$\left\{G_i(x_1,\ldots,x_{2k}) = (G_i^{(1)}, G_i^{(2)}) = (a_i^{(1)}, a_i^{(2)})\right\}_{i\in\{1,2,\ldots,k+1\}\setminus j} \tag{3.16}$$

where $j \in \{1, 2, \ldots, k, k+1\}$.

Firstly, when $j = 1$ have the following k-subsystem:

$$\left\{G_i(x_1,\ldots,x_{2k}) = \left(G_i^{(1)}, G_i^{(2)}\right) = \left(a_i^{(1)}, a_i^{(2)}\right)\right\}_{i=2}^{k+1} \tag{3.17}$$

Since $G_{k+1}(x_1,\ldots,x_{2k}) = (g_1(y_1,y_3,\ldots,y_{2k-1}), g_2(y_2,y_4,\ldots,y_{2k})) = (a_{k+1}^{(1)}, a_{k+1}^{(2)})$, where $y_{\sigma(1)} = a_k^{(1)}, y_{\sigma(3)} = a_{k-1}^{(1)}, \ldots, y_{\sigma(2k-3)} = a_2^{(1)}$; $y_{\pi(2)} = a_k^{(2)}, y_{\pi(4)} = a_{k-1}^{(2)}, \ldots,$ $y_{\pi(2k-2)} = a_2^{(2)}$ and $(y_{\sigma(2k-1)}, y_{\pi(2k)}) = (g_1(x_1,x_3,\ldots,x_{2k-1}), g_2(x_2,x_4,\ldots,x_{2k})) = G_1(x_1,\ldots,x_{2k})$. It follows that

$$\begin{aligned}
g_1(y_1,y_3,\ldots,\underbrace{g_1(x_1,x_3,\ldots,x_{2k-1})}_{\sigma(2k-1)^{th}\ position},\ldots,y_{2k-1}) &= a_{k+1}^{(1)},\ \text{and}\\
g_2(y_2,y_4,\ldots,\underbrace{g_2(x_2,x_4,\ldots,x_{2k})}_{\pi(2k)^{th}\ position},\ldots,y_{2k}) &= a_{k+1}^{(2)}.
\end{aligned}$$

Hence $G_1(x_1,x_2,\ldots,x_{2k}) = (g_1(x_1,x_3,\ldots,x_{2k-1}), g_2(x_2,x_4,\ldots,x_{2k}))$ is given as

$$\begin{aligned}
g_1(x_1,x_3,\ldots,x_{2k-1}) &=^{[\sigma(2k-1)]} g_1(y_1,y_3,\ldots,a_{k+1}^{(1)},\ldots,y_{2k-1}) = a_1^{(1)},\ \text{and}\\
g_2(x_2,x_4,\ldots,x_{2k}) &=^{[\pi(2k)]} g_2(y_2,y_4,\ldots,a_{k+1}^{(2)},\ldots,y_{2k}) = a_1^{(2)}.
\end{aligned}$$

So, for some $(a_1^{(1)}, a_1^{(2)}) \in Q^2$, where $(Q, {}^{[\sigma(2k-1)]}\, g_1)$ and $(Q, {}^{[\pi(2k)]}\, g_2)$ are σ and π

inverses of the k-ary quasigroups (Q, g_1) and (Q, g_2) respectively.

Substituting the values of $(G_1^{(1)}, G_1^{(2)})$ in $G_k(x_1, \ldots, x_{2k})$, we get the unique solution for $(x_{\sigma(2k-1)}, x_{\pi(2k)})$ as $(b_{\sigma(2k-1)}, b_{(2k)}) \in Q^2$ due to the $\sigma(2k-1)$ and $\pi(2k)$ invertibility of the quasigroups g_1 and g_2 respectively. For $i \in \{k-1, k-2, \ldots, 2\}$, we substitute $(G_1^{(1)}, G_1^{(2)}) = (a_1^{(1)}, a_1^{(2)})$ and the unique set of new values $(b_{\sigma(2k-1)}, b_{\pi(2k)}), (b_{\sigma(2k-3)}, b_{\pi(2k-2)}), \ldots, (b_{\sigma(2i+1)}, b_{\pi(2i+2)})$ from $(G_k^{(1)}, G_k^{(2)}), \ldots, (G_{i+1}^{(1)}, G_{i+1}^{(2)})$ respectively, and we get

$$G_i(x_1, \ldots, x_{2k}) = (g_1(y_1, y_3, \ldots, y_{2k-1}), g_2(y_2, y_4, \ldots, y_{2k})) = (a_i^{(1)}, a_i^{(2)}),$$

where $y_{\sigma(2i-1)} = x_{\sigma(2i-1)}, y_{\sigma(2i-3)} = a_1^{(1)}, y_{\sigma(2i-5)} = a_2^{(1)}, y_{\sigma(2i-7)} = a_3^{(1)}, \ldots, y_{(\sigma(2k-3))} = a_{\sigma(2k-3)}$ and $y_{\sigma(2k-1)} = b_{\sigma(2k-1)}$. Similarly, $y_{\pi(2i)} = x_{\pi(2i)}, y_{\pi(2i-2)} = a_1^{(2)}, y_{\pi(2i-5)} = a_1^{(2)}, \ldots, y_{\pi(2k-2)} = a_1^{(2)}, y_{(\pi(2k))} = b_{\pi(2k)}$ and $y_{\sigma(1)} = a_{i-1}^{(1)}, y_{\sigma(3)} = a_{i-2}^{(1)}, \ldots, y_{\sigma(2i-3)} = a_1^{(1)}, y_{\pi(2)} = a_{i-1}^{(2)}, y_{\pi(4)} = a_{i-2}^{(2)}, \ldots, y_{\pi(2i-2)} = a_1^{(2)}$. Since (g_1, g_2) is $(\sigma(2i-1), \pi(2i))$-invertible operations, leads to a unique solution $(x_{\sigma(2i-1)}, x_{\pi(2i)}) = (b_{\sigma(2i-1)}, b_{\pi(2i)})$.

Finally, in equality $G_1(x_1, x_2, \ldots, x_{2k}) = (G_1^{(1)}, G_1^{(2)}) = (a_1^{(1)}, a_1^{(2)})$, we replace $(x_{\sigma(3)}, x_{\pi(4)}) = (b_{\sigma(3)}, b_{\pi(4)})$; $(x_{\sigma(5)}, x_{\pi(6)}) = (b_{\sigma(5)}, b_{\pi(6)}); \ldots \quad ; (x_{\sigma(2k-1)}, x_{\pi(2k)}) = (b_{\sigma(2k-1)}, b_{\pi(2k)})$. Since, (g_1, g_2) are $(\sigma(1), \pi(2))$-invertible operations respectively. So, we obtain a unique solution $(x_{\sigma(1)}, x_{\pi(2)}) = (b_{\sigma(1)}, b_{\pi(2)})$. So, the system

$$\left\{G_i(x_1, \ldots, x_{2k}) = \left(G_i^{(1)}, G_i^{(2)}\right) = \left(a_i^{(1)}, a_i^{(2)}\right)\right\}_{i=2}^{k+1}$$

is orthogonal.

In order to complete the proof, it suffices to show that for $2 \leq j \leq k+1$, the system

$$\left\{G_i(x_1, \ldots, x_{2k}) = \left(G_i^{(1)}, G_i^{(2)}\right) = \left(a_i^{(1)}, a_i^{(2)}\right)\right\}_{i \in \{1,2,\ldots,k+1\} \setminus j} \tag{3.18}$$

is orthogonal. For that aim, consider the system of equations

$$\left\{G_i(x_1, x_2, \ldots, x_{2k}) = (a_i^{(1)}, a_i^{(2)})\right\}_{i=1, i \neq j}^{k+1}$$

for some $2 \leq j \leq k+1$. We have

$$G_{k+1}(x_1, x_2, \ldots, x_{2k}) = (g_1(y_1, y_3, \ldots, y_{2k-1}), g_2(y_2, y_4, \ldots, y_{2k})) = (a_{k+1}^{(1)}, a_{k+1}^{(2)}),$$

where $y_{\sigma(2k-1)} = a_1^{(1)}, y_{\sigma(2k-3)} = a_2^{(1)}, \ldots, y_{\sigma(2k-2j+3)} = a_{j+1}^{(1)}, y_{\sigma(2k-2j-1)} = a_{j-1}^{(1)}, \ldots, y_{\sigma(1)} = a_k^{(1)}, y_{\pi(2k)} = a_1^{(2)}, y_{\pi(2k-2)} = a_2^{(2)}, \ldots, y_{\pi(2k-2j)} = a_{j+1}^{(2)}, y_{\pi(2k-2j+4)} = a_{j-1}^{(2)}, \ldots,$

$y_{\pi(2)} = a_k^{(2)}$ and $(y_{\sigma(2(k-j)+1)}, y_{\pi(2(k-j)+2)}) = (G_j^{(1)}, G_j^{(2)})$. From the equalities

$$g_1(y_1, \ldots, g_1(x_1, x_3, \ldots, x_{2k-1}), \ldots, y_{2k}) = a_{k+1}^{(1)}, \text{ and}$$
$$g_2(y_2, \ldots, g_2(x_2, x_4, \ldots, x_{2k}), \ldots, y_{2k}) = a_{k+1}^{(2)},$$

it follows that

$$G_j^{(1)} =^{[\sigma(2(k-j)+1)]} g_1(y_1, \ldots, y_{\sigma(2(k-j)+1)-2}, a_{k+1}^{(1)}, y_{\sigma(2(k-j)+1)+2}, \ldots, y_{2k-1}) \in Q, \text{ and}$$
$$G_j^{(2)} =^{[\pi(2(k-j)+2)]} g_2(y_2, \ldots, y_{\pi(2(k-j)+2)-2}, a_{k+1}^{(2)}, y_{\pi(2(k-j)+2)+2}, \ldots, y_{2k}) \in Q$$

Since $y_t \in Q$ for all t. Hence, we have $(G_j^{(1)}, G_j^{(2)}) = (a_j^{(1)}, a_j^{(2)})$ for some $(a_j^{(1)}, a_j^{(2)}) \in Q^2$.

There are two cases we need to consider:

Case For $j = k$. We have $(G_k^{(1)}, G_k^{(2)}) = (a_k^{(1)}, a_k^{(2)})$ and the system

$$\left\{ G_i(x_1, x_2, \ldots, x_{2k}) = (G_i^{(1)}, G_i^{(2)}) = (a_i^{(1)}, a_i^{(2)}) \right\}_{i=1}^{k}$$

has a unique solution $b_1, b_2, \ldots, b_{2k}$, according to Theorem 3.2.5, we compute

$$G_{k+1}(b_1, \ldots, b_{2k}) = (g_1(y_1, y_3, \ldots, y_{2k-1}), g_2(y_2, y_4, \ldots, y_{2k}))$$

where $y_{\sigma(2k-1)} = G_1^{(1)}, y_{\sigma(2k-3)} = G_2^{(1)}, \ldots, y_{\sigma(3)} = G_{k-1}^{(1)}, y_{\sigma(1)} = G_k^{(1)}$ and $y_{\pi(2k)} = G_1^{(2)}, y_{\pi(2k-2)} = G_2^{(2)}, \ldots, y_{\pi(4)} = G_{k-1}^{(2)}, y_{\pi(2)} = G_k^{(2)}$,

$$y_{\sigma(1)} = G_1^{(1)}(b_1, b_3, \ldots, b_{2k-1}) =^{[\sigma(1)]} g_1(y_1, \ldots, y_{\sigma(1)-3}, a_{k+1}^{(1)}, y_{\sigma(1)+1}, \ldots, y_{2k-1})$$
$$y_{\pi(2)} = G_1^{(2)}(b_2, b_4, \ldots, b_{2k}) =^{[\pi(2)]} g_2(y_2, \ldots, y_{\pi(2)-2}, a_{k+1}^{(2)}, y_{\pi(2)+2}, \ldots, y_{2k})$$

The last equation implies $(g_1(y_1, \ldots, y_{2k-1}), g_2(y_2, \ldots, y_{2k})) = (a_{k+1}^{(1)}, a_{k+1}^{(2)})$, *i.e.*, $G_{k+1}(b_1, \ldots, b_{2k}) = (a_{k+1}^{(1)}, a_{k+1}^{(2)})$, hence $b_1, b_2, \ldots, b_{2k}$ is the unique solution of the system

$$\left\{ G_i(x_1, x_2, \ldots, x_{2k}) = (G_i^{(1)}, G_i^{(2)}) = (a_i^{(1)}, a_i^{(2)}) \right\}_{i=1, i\neq k}^{k+1}.$$

So, the k-tuple $\langle G_i \mid i = 1, \ldots, k-1, k+1 \rangle$ is orthogonal system of k-ary operations on Q^2.

Case For $j < k$. We replace the value of $(a_j^{(1)}, a_j^{(2)})$ of $(G_j^{(1)}, G_j^{(2)})$ in the equation $(G_k^{(1)}, G_k^{(2)})$, obtaining $(G_k^{(1)}, G_k^{(2)}) = (g_1(y_1, y_3, \ldots, y_{2k-1}), g_2(y_2, y_4, \ldots, y_{2k}))$ where $y_{\sigma(2k-1)} = x_{\sigma(2k-1)}, y_{\sigma(2(k-j)-1)} = a_j^{(1)}$ and $y_{\sigma(2k-3)} = a_1^{(1)}, y_{\sigma(2k-5)} = a_2^{(1)}, \ldots, y_{\sigma(1)} = a_{k-1}^{(1)}$ and $y_{\pi(2k)} = x_{\pi(2k)}, y_{\pi(2(k-j))} = a_j^{(2)}$ and $y_{\pi(2k-2)} = a_1^{(2)}, y_{\pi(2k-4)} = a_2^{(2)}, \ldots, y_{\pi(1)} = a_{k-1}^{(2)}$. Since (g_1, g_2) are $\sigma(2k-1)$ and $\pi(2k)$ invertible operations (being quasigroups), we obtain a unique $(x_{\sigma(2k-1)}, x_{\pi_{2k}}) = (b_{\sigma(2k-1)}, b_{\pi(2k)})$.

Proceeding in the same way, from $G_{k-1}(x_1,\ldots,x_{2k}) = (g_1(y_1,y_3,\ldots,y_{2k-1}), g_2(y_2, y_4,\ldots,y_{2k})) = (a^{(1)}_{k-1}, a^{(2)}_{k-1})$ where $y_{\sigma(2k-1)} = x_{\sigma(2k-1)} = b_{\sigma(2k-1)}, y_{\sigma(2k-3)} = x_{\sigma(2k-3)} = b_{2k-3},\ldots, y_{\sigma(2(k-j)-1)} = a^{(1)}_j, y_{\sigma(1)} = a^{(1)}_1\ y_{\pi(2k)} = x_{\pi(2k)} = b_{\pi(2k)}, y_{\pi(2k-2)} = x_{\pi(2k-2)} = b_{2k-2},\ldots, y_{\pi(2(k-j)-2)} = a^{(2)}_j, y_{\pi(2)} = a^{(2)}_1$. We compute the values $(x_{\sigma(2k-3)}, x_{\pi(2k-2)}) = (b_{2k-3}, b_{2k-2})$ since, (g_1, g_2) is $\sigma(2k-3)$ and $\pi(2k-2)$ invertible respectively. Continuing, we can compute the values $(x_{\sigma(2k-1)}, x_{\pi(2k)}) = (b_{2k-1}, b_{2k}),\ldots,(x_{\sigma(2j+1)}, x_{\pi(2j+2)}) = (b_{\sigma(2j+1)}, b_{\pi(2j+2)})$.

For $i = j-1,\ldots,1$, we substitute and obtain a new set of values in the equation for $G_i = (G^{(1)}_i, G^{(2)}_i)$ and we obtain $G_i(x_1,\ldots,x_{2k}) = (g_1(y_1,y_3,\ldots,y_{2k-1}), g_2(y_2,y_4, \ldots,y_{2k})) = (a^{(1)}_i, a^{(2)}_i)$ where $y_{\sigma(2i-1)} = x_{\sigma(2i-1)}, y_{\sigma(2(i-k)+1)} = b_{\sigma(2(i-k)+1)},\ldots,y_{\sigma(1)} = b_{\sigma(1)}, y_{\pi(2i)} = x_{\pi(2i)}, y_{\pi(2(i-k)+2)} = b_{\pi(2(i-k)+2)},\ldots,y_{\pi(2)} = b_{\pi(2)}$ and $y_{\sigma(1)} = a^{(1)}_1, y_{\sigma(2)} = a^{(1)}_2,\ldots,\ y_{\sigma(2i-3)} = a^{(1)}_{i-1}, y_{\pi(2)} = a^{(2)}_1, y_{\pi(4)} = a^{(2)}_2,\ldots,y_{\pi(2i-2)} = a^{(2)}_{i-1}$. Because (g_1, g_2) is $\sigma(2i-1)$ and $\pi(2i)$ invertible operation, this leads to a unique $(x_{\sigma(2i-1)}, x_{\pi(2i)})$ $= (b_{\sigma(2i-1)}, b_{\pi(2i)})$.

Finally, in the equation $G_j(x_1,\ldots,x_{2k}) = (G^{(1)}_j, G^{(2)}_j) = (a^{(1)}_j, a^{(2)}_j)$ we replace $(x_{\sigma(1)}, x_{\pi(2)}) = (b_{\sigma(1)}, b_{\pi(2)}); (x_{\sigma(3)}, x_{\pi(4)}) = (b_{\sigma(3)}, b_{\pi(4)}); \ldots, ; (x_{\sigma(2k-1)}, x_{\pi(2k)}) = (b_{\sigma(2k-1)}, b_{\pi(2k)})$. Because of (g_1, g_2) be $(\sigma(2j-1), \pi(2j))$ invertible operation, we obtain a unique solution $(x_{\sigma(2j-1)}, x_{\pi(2j)}) = (b_{\sigma(2j-1)}, b_{\pi(2j)})$. We compute

$$G_{k+1}(b_1, b_2, \ldots, b_{2k}) = (G^{(1)}_{k+1}, G^{(2)}_{k+1}) = (g_1(y_1,\ldots,y_{2k-1}), g_2(y_2,\ldots,y_{2k}))$$

where $y_{\sigma(2k-1)} = G^{(1)}_1(b_1,\ldots,b_{2k-1}), y_{\sigma(2k-3)} = G^{(1)}_2(b_1,\ldots,b_{2k-1}),\ldots,\ y_{\sigma(1)} = G^{(1)}_k(b_1,\ldots,b_{2k-1}); y_{\pi(2k)} = G^{(2)}_1(b_2,\ldots,b_{2k}),\ldots y_{\pi(2)} = G^{(2)}_k(b_2,\ldots,b_{2k})$, and

$$y_{(\sigma(2(k-j)-1)} = G_l\,(b_1,\ldots,b_{2k}) =^{[\sigma(2(k-j)-1)]} g_1\left(y_1,\ldots,y_{\sigma(2(k-j)-3}, a^{(1)}_{k+1}, y_{\sigma(2(k-j)+1)},\ldots,y_{2k-1}\right),$$
$$y_{(\pi(2(k-j))} = G_l\,(b_1,\ldots,b_{2k}) =^{[\pi(2(k-j))]} g_2\left(y_2,\ldots,y_{\pi(2(k-j)-2)}, a^{(2)}_{k+1}, y_{\pi(2(k-j)+2},\ldots,y_{2k}\right).$$

The last equality implies $(g_1(y_1,\ldots,y_{2k-1}), g_2(y_2,\ldots,y_{2k})) = (a^{(1)}_{k+1}, a^{(2)}_{k+1})$ i.e.,

$$G_{k+1}(b_1,\ldots,b_{2k}) = (a^{(1)}_{k+1}, a^{(2)}_{k+1})$$

. Hence, $b_1,\ldots,b_{2k}$ is the unique solution of the system

$$\left\{G_i(x_1,x_2,\ldots,x_{2k}) = (G^{(1)}_i, G^{(2)}_i) = (a^{(1)}_i, a^{(2)}_i)\right\}^{k+1}_{i=1,i\neq k}$$

So, the k-tuple $\langle G_i \mid i = 1,\ldots j-1, j+1,\ldots,k+1\rangle$ is k-orthogonal system of k-ary operations over Q^2. □

Now let us consider more generalized case in which we do not restrict to the existence of only two quasigroups, instead we can have all distinct quasigroups in

each equation of G_i for $1 \leq i \leq k+1$.

Theorem 3.2.11. *Let $(Q, g_1^{(i)})$ and $(Q, g_2^{(i)})$ be quasigroups over Q for $1 \leq i \leq k+1$. Then a $(k+1)$-tuple $\langle G_1, G_2, \ldots, G_{k+1}\rangle$ defined as:*

$$
\begin{aligned}
G_1(x_1,\ldots,x_{2k}) &= \left(g_1^{(1)}\left(x_1,x_3,\ldots,x_{2k-1}\right), g_2^{(1)}\left(x_2,x_4,\ldots,x_{2k}\right)\right) = \left(G_1^{(1)}, G_1^{(2)}\right),\\
G_2(x_1,\ldots,x_{2k}) &= \left(g_1^{(2)}\left(x_1,x_3,\ldots,x_{2k-3},G_1^{(1)}\right), g_2^{(2)}\left(x_2,x_4,\ldots,x_{2k-2},G_1^{(2)}\right)\right) = \left(G_2^{(1)}, G_2^{(2)}\right),\\
G_3(x_1,\ldots,x_{2k}) &= \left(g_1^{(3)}\left(x_1,\ldots,x_{2k-5},G_1^{(1)},G_2^{(1)}\right), g_2^{(3)}\left(x_2,\ldots,x_{2k-4},G_1^{(2)},G_2^{(2)}\right)\right) = \left(G_3^{(1)}, G_3^{(2)}\right),\\
&\vdots\\
G_k(x_1,\ldots,x_{2k}) &= \left(g_1^{(k)}\left(x_1,G_1^{(1)},G_2^{(1)}\ldots,G_{k-1}^{(1)}\right), g_2^{(k)}\left(x_2,G_1^{(2)},G_2^{(2)},\ldots,G_{k-1}^{(2)}\right)\right) = \left(G_k^{(1)}, G_k^{(2)}\right),\\
G_{k+1}(x_1,\ldots,x_{2k}) &= \left(g_1^{(k+1)}\left(G_1^{(1)},G_2^{(1)},\ldots,G_k^{(1)}\right), g_2^{(k+1)}\left(G_1^{(2)},G_2^{(2)},\ldots,G_k^{(2)}\right)\right) = \left(G_{k+1}^{(1)}, G_{k+1}^{(2)}\right)
\end{aligned}
$$

is a k-orthogonal system of k-ary operations over Q^2.

Theorem 3.2.12. *Let (Q, g_i) be a k-ary quasigroup over Q for $i \in \{1, 2, \ldots, k+1\}$. Then, the $(k+1)$-tuple $\langle G_1, G_2, \ldots, G_{k+1}\rangle$ defined as:*

$$
\begin{aligned}
G_1(x_1,x_2,\ldots,x_{2k}) &= \left(g_1\left(x_1,x_3,\ldots,x_{2k-1}\right), g_1\left(x_2,x_4,\ldots,x_{2k}\right)\right) = \left(G_1^{(1)}, G_1^{(2)}\right),\\
G_2(x_1,x_2,\ldots,x_{2k}) &= \left(g_2\left(x_3,x_5,\ldots,x_{2k-1},G_1^{(1)}\right), g_2\left(x_4,x_6,\ldots,x_{2k},G_1^{(2)}\right)\right) = \left(G_2^{(1)}, G_2^{(2)}\right),\\
G_3(x_1,x_2,\ldots,x_{2k}) &= \left(g_3\left(x_5,\ldots,x_{2k-1},G_1^{(1)},G_2^{(1)}\right), g_3\left(x_6,\ldots,x_{2k},G_1^{(2)},G_2^{(2)}\right)\right) = \left(G_3^{(1)}, G_3^{(2)}\right),\\
&\vdots\\
G_k(x_1,x_2,\ldots,x_{2k}) &= \left(g_k\left(x_{2k-1},G_1^{(1)},\ldots,G_{k-1}^{(1)}\right), g_k\left(x_{2k},G_1^{(2)},,\ldots,G_{k-1}^{(2)}\right)\right) = \left(G_k^{(1)}, G_k^{(2)}\right)\\
G_{k+1}(x_1,x_2,\ldots,x_{2k}) &= \left(g_{k+1}\left(G_1^{(1)},\ldots,G_k^{(1)}\right), g_{k+1}\left(G_1^{(2)},,\ldots,,G_k^{(2)}\right)\right) = \left(G_{k+1}^{(1)}, G_{k+1}^{(2)}\right)
\end{aligned}
$$

is a k-orthogonal system of k-ary operations over Q^2.

3.3 MDS code

Now we construct linear recursive codes over rings for dimension 2 and 3 utilizing Theorem 3.2.12. Expanding the work of [29], we provide the conditions under which these codes achieve singleton bound *i.e.*, they become MDS codes. For better understanding we give some examples and enumerate such codes using SageMath.

Theorem 3.3.1. *Let Q be a commutative ring. For some fixed a_1, a_2, a_3 and $a_4 \in Q$, suppose (Q, g_1) and (Q, g_2) be two binary quasigroups where $g_1(y_1, y_2) = a_1y_1 + a_3y_2$ and $g_2(y_1, y_2) = a_2y_1 + a_4y_2$. Consider a 2-recursive code over Q^2 as $\mathcal{K}(5 \mid G_1, G_2, G_3) = \{((x_1, x_2), (x_3, x_4), (G_1^{(1)}, G_1^{(2)}), (G_2^{(1)}, G_2^{(2)}), (G_3^{(1)}, G_3^{(2)}))\} \subseteq$*

$(Q^2)^5$, *where* $G_{i+1}(x_1, x_2, x_3, x_4) = (d^i g_1(x_1, x_3), d^i g_2(x_2, x_4)) = (G_{i+1}^{(1)}, G_{i+1}^{(2)})$ *for* $0 \leq i \leq 2$. *On evaluation, we obtain*

$$(G_1^{(1)}, G_1^{(2)}) = (a_1x_1 + a_3x_3,\ a_2x_2 + a_4x_4);$$
$$(G_2^{(1)}, G_2^{(2)}) = ((a_1a_3)x_1 + (a_1 + a_3^2)x_3,\ (a_2a_4)x_2 + (a_2 + a_4^2)x_4);$$
$$(G_3^{(1)}, G_3^{(2)}) = ((a_1^2 + a_1a_3^2)x_1 + (2a_1a_3 + a_3^2)x_3,\ (a_2^2 + a_2a_4^2)x_2 + (2a_2a_4 + a_4^2)x_4).$$

Then $\mathcal{K}$ *is an MDS code of dimension 2 over* Q^2 *if and only if* $\langle G_1, G_2, G_3\rangle$ *is a system of binary strong-orthogonal operations over* Q^2 *equivalently* $a_1, a_2, a_3, a_4, (a_1 + a_3^2),\ (2a_1 + a_3^2),\ (a_2 + a_4^2),\ (2a_2 + a_4^2)$ *are units in* Q.

Proof. We construct the coefficient matrices

$$M_1 = \begin{bmatrix} a_1 & a_3 \\ a_1a_3 & a_1 + a_3^2 \\ a_1^2 + a_1a_3^2 & 2a_1a_3 + a_3^2 \end{bmatrix}, M_2 = \begin{bmatrix} a_2 & a_4 \\ a_2a_4 & a_2 + a_4^2 \\ a_2^2 + a_2a_4^2 & 2a_2a_4 + a_4^2 \end{bmatrix}$$

The set $\mathcal{K}$ forms an MDS code for dimension 2 over Q^2 if every square submatrix of M_1 and M_2 must be invertible this yields the conditions $a_1 \neq 0, a_2 \neq 0, a_3 \neq 0, a_4 \neq 0, (a_1 + a_3^2) \neq 0, 2a_1 + a_3^2 \neq 0, (a_2 + a_4^2) \neq 0, 2a_2 + a_4^2 \neq 0$. □

Theorem 3.3.2. *Let* Q *be a commutative ring and for some fixed* a_1,a_2,a_3,a_4,a_5,$a_6 \in Q$, *suppose* (Q, g_1) *and* (Q, g_2) *be two binary quasigroups where* $g_1(y_1, y_2, y_3) = a_1y_1 + a_3y_2 + a_5y_3$ *and* $g_2(y_1, y_2, y_3) = a_2y_1 + a_4y_2 + a_6y_3$. *Consider a* 3*-recursive code over* Q^2 *as:*

$$\mathcal{K}(7 \mid G_1, G_2, G_3, G_4) = \{(x_1, x_2), (x_3, x_4), (x_5, x_6), (G_1^{(1)}, G_1^{(2)}), (G_2^{(1)}, G_2^{(2)}), (G_3^{(1)}, G_3^{(2)}), (G_4^{(1)}, G_4^{(2)})\} \subseteq (Q^2)^7$$

where $G_{i+1}(x_1, x_2, x_3, x_4, x_5, x_6) = ((d^i g_1(x_1, x_3, x_5), d^i g_2(x_2, x_4, x_6)) = (G_{i+1}^{(1)}, G_{i+1}^{(2)})$ *for* $0 \leq i \leq 3$. *On evaluation, we obtain*

$$\left(G_1^{(1)}, G_1^{(2)}\right) = (a_1x_1 + a_3x_3 + a_5x_5,\ a_2x_2 + a_4x_4 + a_6x_6);$$
$$\left(G_2^{(1)}, G_2^{(2)}\right) = \left((a_1a_5)x_1 + (a_1 + a_3a_5)x_3 + (a_3 + a_5^2)x_5,\ (a_6a_2)x_2 + (a_2 + a_4a_6)x_3 + (a_4 + a_6^2)x_6\right);$$
$$\left(G_3^{(1)}, G_3^{(2)}\right) = \Big((a_1a_3 + a_1a_5^2)x_1 + (a_3^2 + a_1a_5 + a_3a_5^2)x_3 + (a_1 + 2a_3a_5 + a_5^3)x_5,\ (a_2a_4 + a_2a_6^2)x_2$$
$$+ (a_4^2 + a_2a_6 + a_4a_6^2)x_4 + (a_2 + 2a_4a_6 + a_6^3)x_6\Big);$$
$$\left(G_4^{(1)}, G_4^{(2)}\right) = \Big(a_1^2 + 2a_1a_3a_5 + a_1a_5^3)x_1 + (2a_1a_3 + 2a_3^2a_5^2 + a_1a_5^2 + a_3a_5^3)x_3 + (2a_1a_5 + a_3^2 + 3a_3a_5^2 + a_5^4)x_5,$$
$$(a_2^2 + 2a_2a_4a_6 + a_2a_6^3)x_2 + (2a_2a_4 + 2a_4^2a_6^2 + a_2a_6^2 + a_4a_6^3)x_4 + (2a_2a_6 + a_4^2 + 3a_4a_6^2 + a_6^4)x_6\Big).$$

Then, $\mathcal{K}$ *is an MDS code of dimension* 3 *over* Q^2 *if and only if* $\langle G_1, G_2, G_3, G_4\rangle$ *is*

a system of 3*-ary strong-orthogonal operations over* Q^2 *equivalently the following are units of* Q*:*

- a_1, a_3, a_5
- a_2, a_4, a_6
- $a_1 + a_3a_5$
- $a_2 + a_4a_6$
- $a_3 + a_5^2$
- $a_4 + a_6^2$
- $2a_1a_5 - a_3^2$
- $2a_2a_6 - a_4^2$
- $a_3^2 - a_1a_5$
- $a_4^2 - a_2a_6$
- $a_3^2 + a_1a_5 + a_3a_5^2$
- $a_4^2 + a_2a_6 + a_4a_6^2$
- $a_1^2 + 2a_1a_3a_5 - a_3^3$
- $a_2^2 + 2a_2a_4a_6 - a_4^3$
- $a_3^2a_5^2 + a_3^2 - a_1a_5^3$
- $a_4^2a_6^2 + a_4^2 - a_2a_6^3$
- $a_1 + 2a_3a_5 + a_5^3$
- $a_2 + 2a_4a_6 + a_6^3$
- $a_1a_5^2 - a_3^2a_5 - a_1a_3$
- $a_2a_6^2 - a_4^2a_6 - a_2a_4$
- $2a_1a_5 + 3a_3a_5^2 + a_3^2 + a_5^4$
- $2a_2a_6 + 3a_4a_6^2 + a_4^2 + a_6^4$
- $2a_1a_3 + 2a_3^2a_5 + a_1a_5^2 + a_3a_5^2$
- $2a_2a_4 + 2a_4^2a_6 + a_2a_6^2 + a_4a_6^2$
- $2a_1^2a_5 + 2a_1a_3a_5^2 - a_1a_3^2 - a_3^2a_5$
- $-2a_1^2a_3 + a_1^2a_5^2 - 3a_1a_3^2a_5 + a_3^4$
- $-2a_2^2a_4 + a_2^2a_6^2 - 3a_2a_4^2a_6 + a_4^4$
- $2a_2^2a_6 + 2a_2a_4a_6^2 - a_2a_4^2 - a_4^2a_6$.

Example 3.3.3. Consider $Q = \mathbb{F}_{2^2} = \mathbb{F}_2(\alpha)$, the number of MDS codes of length 5, dimension 2 and distance 4 over Q^2 as described in Theorem 3.3.1 is 36. The list of possible values of (a_1, a_3) and (a_2, a_4) are given by

$$\{(\alpha,\alpha),\ \ (\alpha,1),\ \ (\alpha+1,\alpha+1),\ \ (\alpha+1,1),\ \ (1,\alpha),\ \ (1,\alpha+1)\}$$

In particular, one of such codes is described by assuming $a_1 = a_2 = a,\ a_3 = a_4 = 1$ in Theorem 3.3.1.

Example 3.3.4. Consider $Q = \mathbb{F}_{2^3} = \mathbb{F}_2(\alpha)$, the number of MDS codes of length 7, dimension 3 and distance 5 over Q^2 as described in Theorem 3.3.2 is 900. The list of possible values of (a_1, a_3, a_5) and (a_2, a_4, a_6) are given by

$$\begin{array}{lll}
\{(\alpha,\ \alpha^2,\ \alpha^2+\alpha), & (\alpha,\ \alpha^2+\alpha,\ \alpha^2+1), & (\alpha,\ \alpha^2+\alpha+1,\ 1),\\
(\alpha,\ 1,\ \alpha^2), & (\alpha^2,\ \alpha,\ \alpha^2+\alpha+1), & (\alpha^2,\ \alpha+1,\ 1),\\
(\alpha^2,\ \alpha^2+\alpha,\ \alpha), & (\alpha^2,\ 1,\ \alpha^2+\alpha), & (\alpha+1,\ \alpha,\ 1),\\
(\alpha+1,\ \alpha^2+\alpha+1,\ \alpha^2+\alpha), & (\alpha+1,\ \alpha^2+1,\ \alpha^2+\alpha+1), & (\alpha+1,\ 1,\ \alpha^2+1),\\
(\alpha^2+\alpha,\ \alpha,\ \alpha^2) & (\alpha^2+\alpha,\ \alpha^2,\ \alpha+1), & (\alpha^2+\alpha,\ \alpha^2+1,\ 1)\\
(\alpha^2+\alpha,\ 1,\ \alpha) & (\alpha^2+\alpha+1,\ \alpha+1,\ \alpha^2+1), & (\alpha^2+\alpha+1,\ \alpha^2+\alpha,\ 1),\\
(\alpha^2+\alpha+1,\ \alpha^2+1,\ \alpha^2) & (\alpha^2+\alpha+1,\ 1,\ \alpha+1), & (\alpha^2+1,\ \alpha^2,\ 1),\\
(\alpha^2+1,\ \alpha+1,\ \alpha), & (\alpha^2+1,\ \alpha^2+\alpha+1,\ \alpha+1), & (\alpha^2+1,\ 1,\ \alpha^2+\alpha+1),\\
(1,\ \alpha,\ \alpha), & (1,\ \alpha^2,\ \alpha^2), & (1,\ \alpha+1,\ \alpha+1),\\
(1,\ \alpha^2+\alpha,\ \alpha^2+\alpha), & (1,\ \alpha^2+\alpha+1,\ \alpha^2+\alpha+1), & (1,\ \alpha^2+1,\ \alpha^2+1)\}
\end{array}$$

In particular, one of such code can be described by assuming $a_1 = a_2 = \alpha$, $a_3 = \alpha^2$, $a_4 = a_5 = \alpha^2 + \alpha$ and $a_6 = \alpha^2 + 1$ in Theorem 3.3.2.

Example 3.3.5. Consider $Q = \mathbb{F}_{2^4} = \mathbb{F}_2(\alpha)$, the number of MDS codes, built as per the illustrated construction using Theorem 3.3.2, having length 7, dimension 3 and distance 5 over Q^2 is 876096. In particular, two such codes can be described using Theorem 3.3.2 with parameters

$$(a_1, a_2, a_3, a_4, a_5, a_6) = (\alpha, \alpha, \alpha^2, \alpha^2, \alpha + 1, \alpha + 1),$$
$$(a_1, a_2, a_3, a_4, a_5, a_6) = (\alpha, \alpha, \alpha^2, \alpha^2, \alpha^3 + \alpha + 1, \alpha^3 + \alpha + 1).$$