Constructions of pairs of orthogonal latin cubes

Vladimir N. Potapov

Sobolev Institute of Mathematics, Novosibirsk, Russia

Correspondence
Vladimir N. Potapov, Sobolev Institute of Mathematics, acad. Koptyug ave. 4, Novosibirsk 630090, Russia
Email: vpotapov@math.nsc.ru

Funding information
Russian Science Foundation, Grant/Award Number: 18-11-00136

Abstract
A pair of orthogonal latin cubes of order $q$ is equivalent to a maximum distance separable code with distance 3 or to an $OA_1(3, 5, q)$ orthogonal array. We construct pairs of orthogonal latin cubes for sequences of previously unknown orders $q_i = 16(18i - 1) + 4$ and $q_i' = 16(18i + 5) + 4$. The minimal new obtained parameters of orthogonal arrays are $OA_i(3, 5, 84)$.

KEYWORDS
block design, latin cube, latin square, MDS code, MOLS, orthogonal array, Steiner system

JEL CLASSIFICATION
05B05; 05B15; 94B05

1 | INTRODUCTION

A latin square of order $q$ is a $q \times q$ array of $q$ symbols where each symbol occurs exactly once in every row and in every column. A $k$-dimensional array satisfying the same condition is called a latin $k$-cube. Any two-dimensional axis-aligned plane (face) of a latin $k$-cube of order $q$ is a latin square of order $q$ by definition. Two latin squares are orthogonal if, when they are superimposed, every ordered pair of symbols appears exactly once. For brevity, a pair of orthogonal latin squares is called POLS. If in a set of latin squares, any two latin squares are orthogonal, then this set is called a system of Mutually Orthogonal Latin Squares (MOLS). Two latin $k$-cubes are orthogonal if any pair of corresponding two-dimensional faces of these cubes is a POLS. Bose, Shrikhande, and Parker [1] proved that for each positive integer $q$, $q \neq 2, 6$, there exists POLS of order $q$ and POLS of orders 2 and 6 do not exist. As a corollary we obtain the nonexistence of pairs of orthogonal latin $k$-cubes of orders 2 and 6. The nonexistence of pairs of orthogonal latin $k$-cubes of orders $q$ if $k > q - 1$ follows from the sphere-packing (Hamming) bound. But the complete spectrum of possible orders of pairs of orthogonal latin $k$-cubes remains unknown for any $k \geq 3$. Ten is the minimum order for which it is not known whether pairs of orthogonal latin 3-cubes exist. In this paper we construct pairs of orthogonal latin 3-cubes for sequences of previously unknown orders $q_i = 16(18i - 1) + 4$ and
Let $q_q = \{0, ..., q-1\}$. A subset $C$ of $Q_q^d$ is called a maximum distance separable code $MDS(t, d, q)$ (of order $q$, code distance $t + 1$, and length $d$) if $|C \cap \Gamma| = 1$ for each $t$-dimensional axis-aligned plane $\Gamma$. Ethier and Mullen [3] proved that $MDS(2, 2 + s, q)$ codes are equivalent to pairs of orthogonal latin $s$-cubes of order $q$. There are two well-known methods for constructing MDS codes. If $q$ is a prime power, then we can consider $Q_q$ as the Galois field $GF(q)$. MDS codes obtained as the solution of an appropriate system of linear equations over $GF(q)$ are known as Reed-Solomon codes. If there exists an $MDS(t, d, p_1)$ code and an $MDS(t, d, p_2)$ code, then we get an $MDS(t, d, p_1 p_2)$ code by a product construction (McNeish’s theorem). We represent a new construction of $MDS(2, 5, q)$ codes that is similar to Wilson’s construction for pairs of orthogonal latin squares with aligned subsquares (see [2,5]).

The problem of existence of MDS codes with non-prime-power orders is connected to the problem of existence of Steiner block designs. By methods of random graph theory Keevash [6] and Glock et al [4] proved that the natural divisibility conditions are sufficient for the existence of the Steiner system $S(t, k, n)$ apart from a finite number of exceptional $n$’s for given fixed $t$ and $k$. It is not difficult to prove that any MDS code is equivalent to a transversal in an appropriate multipartite hypergraph (see [9]). Then the existence of $MDS(t, d, q)$ codes follows from [7, Theorem 1.7] apart from a finite number of exceptional $q$’s for given fixed $t$ and $d$. In Section 4, we propose a construction of pairs of orthogonal latin 3-cubes based on Steiner block designs.

Note that an $MDS(2, q + 1, q)$ code (a pair of orthogonal $(q - 1)$-cubes) is a 1-error correcting perfect code. The existence of such codes is a well-known problem if $q$ is not a prime power (see [8]).

## 2 | CONNECTION BETWEEN MDS CODES AND ORTHOGONAL SYSTEMS

An $OA_{\lambda}(s, d, q)$ orthogonal array is a $\lambda q^s \times d$ array whose entries are from $Q_q$ such that in every subset of $s$ columns of the array, every $s$-tuple from $Q_q^s$ appears in exactly $\lambda$ rows. Further we consider only orthogonal arrays with $\lambda = 1$. In this case every column of the orthogonal array is a function $f : Q_q^s \rightarrow Q_q$. A set of columns of an orthogonal array with $\lambda = 1$ is called an orthogonal system. In other words, a system consisting of $d$ functions $f_1, ..., f_d, \hat{f}_i : Q_q^s \rightarrow Q_q (d \geq s)$ is orthogonal if for each subsystem $f_i, ..., f_i$ consisting of $s$ functions it holds that

$$\{(f_i(x), ..., f_i(x)) | x \in Q_q^s\} = Q_q^s.$$  

If the system remains orthogonal after substitution any constants for each subset of variables, then it is called strong-orthogonal. If the number of variables is two, then such a system is a system of MOLS (see [3]). If $s = 3$, it is a set of Mutually Orthogonal Latin Cubes (MOLC). Ethier and Mullen [3] proved that MDS codes are equivalent to strong-orthogonal systems. Moreover, by a replacement of variables it is possible to obtain a strong-orthogonal system consisting of $d - s$ functions from any orthogonal system consisting of $d$ functions over $Q_q^s$.
**Proposition 1.** The following conditions are equivalent:

1. a system consisting of \( t \) functions \( f_1, \ldots, f_t: Q_q^d \to Q_q \) is strong-orthogonal;
2. the set \( C = \{(x_1, \ldots, x_s, f_i(\overline{x})): x_i \in Q_q\} \) is an MDS \((t, t + s, q)\) code;
3. the array consisting of all elements of \( C \) as rows is an OA(s, t + s, q) orthogonal array.

A projection (punctured code) of an MDS \((t, t + s, q)\) code onto a hyperplane is equal to a removal of one of the functions \( f_i \). The punctured code is an MDS \((t - 1, t + s - 1, q)\) code by Proposition 1. Consequently, the existence of MDS \((2, 2 + s, q)\) code or a pair of orthogonal latin \( s \)-cubes of order \( q \) follows from the existence of an MDS \((t, t + s, q)\) code if \( t \geq 2 \).

Sometimes the terms “latin cube” and “\( t \) mutually orthogonal latin cubes” are used for \( OA_q(2, 4, q) \) and \( OA_q(2, t + 3, q) \) orthogonal arrays, respectively. It is easy to see that our definition of a system of MOLC is stronger.

## 3 CONSTRUCTIONS OF MDS CODES

The Hamming distance \( \rho \) between two elements of \( Q_q^d \) is the number of positions at which the corresponding symbols are different. In this paper we use only the Hamming distance. The code distance of \( C \subset Q_q^d \) is \( \rho(C) = \min_{x \in C, y \in C, x \neq y} \rho(x, y) \). The distance between two subsets \( A, B \subset Q_q^d \) is \( \min_{x \in A, y \in B} \rho(x, y) \). The Singleton bound for the cardinality of a code \( C \subset Q_q^d \) with distance \( t + 1 \) is \( |C| \leq q^{d-t} \). MDS codes achieve equality in this bound.

**Proposition 2.** A subset \( C \subset Q_q^d \) with code distance \( t + 1 \) is an MDS code if and only if \(|C| = q^{d-t}\).

The Hamming bound for the cardinality of code \( C \subset Q_q^d \) with distance \( 3 \) is \(|C| \leq \frac{q^d}{1 + (q - 1)d} \). Then the inequalities \( q^{d-2} \leq \frac{q^d}{1 + (q - 1)d} \) or \( d \leq q + 1 \) are a necessary condition for the existence of an MDS \((2, d, q)\) code. Consequently, an MDS \((2, 5, 3)\) code or a pair of orthogonal latin cubes of order \( 3 \) do not exist. Moreover, by puncturing codes we have a necessary condition \( s \leq q - 1 \) for the existence of an MDS \((t, t + s, q)\) if \( t \geq 2 \). For linear codes this condition \( s \leq q - 1 \) is in [8].

Let \( q \) be a prime power and let \( Q_q = GF(q) \). A linear \( k \)-dimensional subspace \( C \subset Q_q^d \) with distance \( t \) is called \([d, k, t]\) code over \( GF(q) \). By Proposition 2 we see that any \([d, d - t, t + 1]\) code over \( GF(q) \) is an MDS \((t, d, q)\) code. By using a well-known construction of a linear MDS code (see [8, Chapters 10 and 11] or [4, Theorem 9.1]) by means of an appropriate parity-check matrix over \( GF(q) \) we can conclude that the following proposition is true.

**Proposition 3.** Let \( q \) be a prime power. Then for each integer \( d \leq q + 1 \) and \( \varphi \), \( 3 \leq \varphi < d \), there exists a linear (over \( GF(q) \)) MDS code \( C \subset Q_q^d \) with code distance \( \varphi \).

We will say that an MDS \((t, d, q)\) code \( M_0 \) is a super MDS \((t, d, q)\) code if there exist MDS \((t + 1, d, q)\) code \( M_1 \) and MDS \((t + 2, d, q)\) code \( M_2 \) such that \( M_2 \subset M_1 \subset M_0 \).

By removal of any row from a parity-check matrix of a linear MDS code with distance \( t + 1 \), we obtain a parity-check matrix of an MDS code with distance \( t \) that contains the original code. Thus Propositions 4 and 5 follow from Proposition 3.
**Proposition 4.** Let $q$ be a prime power. Then for each integer $d \leq q + 1$ and $\varphi$, $3 \leq \varphi < d - 2$, there exists a linear super MDS code over $GF(q)$ with length $d$ and code distance $\varphi$.

**Proposition 5.** Let $q$ be a prime power. Then for each integer $d \leq q + 1$ and $\varphi$, $3 \leq \varphi < d - 1$, there exists a linear MDS code over $GF(q)$ with length $d$ and code distance $\varphi$ that is a union of $q$ disjoint linear MDS codes over $GF(q)$ with code distance $\varphi + 1$.

The set $Q_{q,t}$ can be considered as the Cartesian product $Q_{q,t}$, Consequently, we can identify $Q_{q,t}$ and the hypercube $Q_{q,t}$. Thus if $C_1 \subset Q_{q,t}$ and $C_2 \subset Q_{q,t}$, then

$$C_1 \times C_2 = \{((x_1, y_1), (x_2, y_2), ..., (x_d, y_d)) : (x_1, ..., x_d) \in C_1, (y_1, ..., y_d) \in C_2\} \subset Q_{q,t}.$$

**Proposition 6 (McNeish).** Suppose $M_1$ is a (super) MDS $(t, d, q_1)$ code and $M_2$ is a (super) MDS $(t, d, q_2)$ code. Then $M_1 \times M_2$ is a (super) MDS $(t, d, q_1 q_2)$ code.

By combining the results of Propositions 3 and 6 we obtain that MDS $(2, 5, q)$ codes exist if $q = 2^3 \cdot 3^5 \cdot 5^5 \cdot \ldots$, where $\delta_5 \neq 1$ and $\delta_5 \neq 1$.

Let $A \subset Q_q$. Denote by $\pi_A$ a function mapping from $Q_q \times Q_q$ to $Q_{q-|A|+|A|}$ by the following rule: $\pi_A(x, y) = (x, y)$ if $y \notin A$, and $\pi_A(x, y) = y$ if $y \in A$. Let $C_1 \subset Q_{d,q}$ and $C_2 \subset Q_{q,d}$. Denote $C_1 \times A \subset C_2 \subset \{z_1, z_2, ..., z_d\}$: $z \in C_1 \times C_2$. For any $C' \subset Q_{q,d}$ we denote by $U_t(C)$ the $t$-neighborhood of $C$, that is, $U_t(C) = \{x \in Q_{q,d} : \exists y \in C, p(x, y) \leq t\}$.

A set $D \subset Q_{q,d}$ is called an MDS $(t, d, q)$ with $j$-A-hole $(t + 1 \leq j \leq d)$ if

1. the code distance of $D$ is equal to $t + 1$;
2. $D \cap U_{d-j+t}(A_t) = \emptyset$;
3. $U_{d-j+t}(D) = Q_{d,q}\setminus A_t$;
4. $|D| = \sum_{k=0}^{j-t-1} \binom{d-k}{k} (q - |A|)^d-t-k |A|^k$.

For $t = 2$ and $d = 5$ we get that an MDS $(2, 5, q)$ code with 5-A-hole has cardinality $q^3 - |A|^3$ and an MDS $(2, 5, q)$ code with 4-A-hole has cardinality $(q - |A|)^3 + 3(q - |A|)^2 |A|$. Suppose that $M$ is an MDS $(t, d, q)$ code, $a \in Q_q$, and $\sigma = (a, ..., a) \in M$. It is easy to see that $M \setminus \{\sigma\}$ is an MDS $(t, d, q)$ with $d\{-a\}$-hole. Let $A \subset Q_q$ and let $M$ be an MDS code, $M \subset Q_{q,d}$. A subset $M \cap A$ is called a subcode of $M$ if it is an MDS code in $A$ with the same code distance as $M$. If $M \cap A$ is a subcode, then $M \setminus A$ is an MDS $(t, d, q)$ with $d\{-A\}$-hole.

Let us formulate a known construction of a POLS (see [2, Chapter 4]) in introduced terms.

**Proposition 7.** Suppose that

- $M_1 \subset M$ is MDS $(3, 4, p)$ code and $M$ is MDS $(2, 4, p)$ code,
- $D$ is an MDS $(2, 4, q)$ code,
- $E$ is an MDS $(2, 4, q_1 - q)$ code on alphabet $A$,
- $F$ is an MDS $(2, 4, q_1)$ code with 4-A-hole, where $|A| = q_1 - q$.

Then the set $C = E \cup (M_1 \times A F) \cup ((M \setminus M_1) \times D)$ is an MDS $(2, 4, (p - 1)q + q_1)$ code.

Consider an example of code $C$ that is described in Proposition 7. An MDS $(2, 4, p)$ code is equivalent to a POLS. Determine $p = q_1 = 4$ and $q = 3$. Let $M$ corresponds to the pair
and let $M_1$ corresponds to main diagonals of this squares. Suppose that $D$ corresponds to the pair

$$
\begin{array}{cccc}
b & c & e & b \\
c & e & b & e \\
e & b & c & c \\
e & e & b &
\end{array}
$$

$F$ corresponds to the pair

$$
\begin{array}{cccc}
a & b & c & e \\
c & e & a & b \\
b & a & e & c \\
e & c & b &
\end{array}
$$

and $E = (a, a, a, a)$. Then the constructed code $C$ is equivalent to the following POLS of order 13:

$$
\begin{array}{ccccccccccccccc}
a & 0b & 0c & 1b & 1c & 1e & 2b & 2c & 2e & 3b & 3c & 3e & 0e \\
0c & 0e & a & 1c & 1e & 1b & 2c & 2e & 2b & 3c & 3e & 3b & 0b \\
0b & a & 0e & 1e & 1b & 1c & 2e & 2b & 2c & 3e & 3b & 3c & 0c \\
3b & 3c & 3e & a & 2b & 2c & 1b & 1c & 1e & 0b & 0e & 0e & 2e \\
3c & 3e & 3b & 2e & 2e & a & 1c & 1e & 1b & 0c & 0e & 0b & 2b \\
3b & 3b & 3c & 2b & a & 2e & 1e & 1b & 1c & 0e & 0b & 0c & 2c \\
1b & 1c & 1e & 0b & 0c & 0e & a & 3b & 3c & 2b & 2c & 2e & 3e \\
1c & 1e & 1b & 0c & 0e & 0b & 3c & 3e & a & 2e & 2b & 2b & 3b \\
1e & 1b & 1c & 0e & 0b & 0c & 3b & a & 3e & 2e & 2b & 2c & 3c \\
2b & 2c & 2e & 3b & 3c & 3e & 0b & 0c & 0e & a & 1b & 1c & 1e \\
2c & 2e & 2b & 3e & 3e & 3b & 0c & 0e & 0b & 1c & 1e & a & 1b \\
2e & 2b & 2c & 3e & 3b & 3c & 0e & 0b & 0c & 1b & a & 1e & 1c \\
0e & 0c & 0b & 2e & 2c & 2b & 3e & 3c & 3b & 1e & 1b & 1c & a
\end{array}
$$
Theorem 1. Suppose that

- \( M_2 \subset M_1 \subset M \) is a super MDS \((2, 5, p)\) code,
- \( D \) is an MDS \((2, 5, q)\) code,
- \( E \) is an MDS \((2, 5, q_1 - q)\) code on alphabet \( A \),
- \( F \) is an MDS \((2, 5, q)\) code with 4-\( A \)-hole,
- \( G \) is an MDS \((2, 5, q)\) code with 5-\( A \)-hole, where \(|A| = q_1 - q|).

Then the set \( C = E \cup (M_2 \times_A G) \cup ((M_1 \setminus M_2) \times_A F) \cup ((M \setminus M_1) \times D) \) is an MDS \((2, 5, (p - 1)q + q_1)\) code.

Proof. By the hypotheses of the theorem for any \( y \in G \) there exist three \( i \in \{1, \ldots, 5\} \) such that \( y_i \not\in A \). Since the code distance of \( M_2 \) equals 5, for any \( x, x' \in M_2 \) all coordinates are different. Consequently, if \( (x, y) \neq (x', y') \) for \( x, x' \in M_2 \) and \( y, y' \in G \), then \(|M_2 \times_A G| = |M_2 \times G| = |M_2| |G| \). By the same way we can prove that \(|M_2 \times_A F| = |M_2| |F| \) and \(|M_1 \times_A F| = |M_1| |F| \). Then it holds that

\[
|C| = |E| + |M_2||G| + (|M_1| - |M_2|)|F| + (|M| - |M_1|)|D| \\
= (q_1 - q)^3 + p(q_1^3 - (q_1 - q)^3) + (p^2 - p)(q^3 + 3q^2(q_1 - q)) \\
+ (p^3 - p^2)q^3 = (pq + q_1 - q)^3.
\]

The code distance of \( X \times Y \) is the minimum of the code distances of \( X \) and \( Y \). If elements of \( Y \) contain not more than \( k \) symbols from \( A \), then \( \rho(X \times_A Y) \geq \min(\rho(X) - k, \rho(Y)) \). Hence the interior distances of the codes \( E, M_2 \times_A G, (M_1 \setminus M_2) \times_A F \), and \((M \setminus M_1) \times D \) are not less than 3 by the hypotheses of the theorem. The distance between codes \((M \setminus M_1) \times D \) and \( E \) equals 5. The distance between \((M_1 \setminus M_2) \times_A F \) (or \( M_2 \times_A G \)) is not less than the distance between \((M \setminus M_1) \times D \) and \((M_1 \setminus M_2) \times F \) (or \( M_2 \times G \)). This distance is not less than the distance between \( M_1 \setminus M_2 \setminus M_1 \) and \( M_1 \setminus M_2 \) (or \( M_2 \)), that is, it is not less than the code distance of \( M \).

We have that \( U_2(E) \cap F = U_2(E) \cap G = \emptyset \) by the definition of a code with \( j \)-\( A \)-hole. Thus the distance between \( E \) and \((M_1 \setminus M_2) \times_A F \) (or \( M_2 \times_A G \)) is not less than the distance between \( E \) and \( F \) or \( G \), that is, it is not less than 3.

The distance between \( M_1 \setminus M_2 \) and \( M_2 \) is equal to 4. Take \((x_0, x_1, x_2, x_3, x_4)\) from \( M_1 \setminus M_2 \). Each element of \((x_0, x_1, x_2, x_3, x_4) \times_A F \) contains not more than one symbol from \( A \). Consequently, the distance between \((x_0, x_1, x_2, x_3, x_4) \times_A F \) and \( M_2 \times_A G \) is not less than \( 4 - 1 = 3 \).

By the Singleton bound (Proposition 2) \( C \) is an MDS code. \( \square \)

It is easy to see that the MDS code \( C \) constructed by using the theorem above contains subcodes of orders \( q \) and \( q_1 \). These subcodes are \( x \times D \), where \( x \in M \setminus M_1 \), and \( E \cup (x \times_A G) \), where \( x \in M_2 \).
Proposition 8. Let \( k \leq p \) and \( i \in \{1, ..., k\} \). Suppose

- \( M \) is an MDS \((2, 5, p)\) code that contains \( k \) disjoint MDS \((3, 5, p)\) codes \( C_i \),
- \( D \) is an MDS \((2, 5, q)\) code,
- \( F_i \) is an MDS \((2, 5, q_i)\) code over alphabet \( Q_i \cup A_i \) with \( 4-A_i \)-hole, where \( |A_i| = q_i - q \), \( A_i \cap A_j = \emptyset \) if \( i \neq j \).

Then the set \( S = \left( \bigcup_{i=1}^{k} C_i \times A_i \right) \cup \left( \left( M \setminus \bigcup_{i=1}^{k} C_i \right) \times D \right) \) is an MDS \((2, 5, (p - k)q + kq_i)\) code with \( 4-B \)-hole, where \( B = \bigcup_{i=1}^{k} A_i \).

Proof. By the hypotheses of the proposition for any \( y \in F_i \) there exists \( x, x' \in C_i \) coincide in one coordinate at most. Consequently, if \( (x, y) \neq (x', y') \), then \( \pi_{A_i}(x, y) \neq \pi_{A_i}(x', y') \) for \( x, x' \in C_i \) and \( y, y' \in F_i \). Then \( |C_i \times A_i F_i| = |C_i||F_i| = |C_i||F_i| \). By direct calculation we obtain the following equalities:

\[
|S| = k |C_i||F_i| + (|M| - k |C_i|) |D| = kp^2(q^3 + 3q^2(q_i - q)) + (p^3 - kp^2)q^3 = (pq)^3 + 3(pq)^2k(q_i - q).
\]

The distance between \( \left( M \setminus \bigcup_{i=1}^{k} C_i \right) \times D \) and \( \bigcup_{i=1}^{k} (C_i \times A_i F_i) \) is not less than the distance between \( M \left( \bigcup_{i=1}^{k} C_i \right) \) and \( \bigcup_{i=1}^{k} C_i \). Since \( A_i \cap A_j = \emptyset \) if \( i \neq j \), the distance between \( C_i \times A_i F_i \) and \( C_j \times A_j F_j \) is not less than the distance between \( C_i \) and \( C_j \). For \( i = 1, ..., k \) we have \( \rho(C_i \times A_i F_i) \geq \min(\rho(C_i) - 1, \rho(F_i)) = 3 \). The code distance of \( \left( M \setminus \bigcup_{i=1}^{k} C_i \right) \times D \) is not less than the minimum of the code distances of \( D \) and \( M \). Therefore, the code distance of \( S \) equals 3.

Let us prove that \( S \cap U_3 \left( \left( \bigcup_{i=1}^{k} A_i \right)^5 \right) = \emptyset \). By definition of \( 4-A_i \)-hole, each element of \( F_i \) contains not more than one symbol from \( A_i \). So, each element of \( S \) contains not more than one symbol from \( \bigcup_{i=1}^{k} A_i \).

Let us prove that \( U_3(S) = \left( Q_i \cup \left( \bigcup_{i=1}^{k} A_i \right)^5 \right) \setminus \left( \bigcup_{i=1}^{k} A_i \right)^5 \). Consider any vector \( \bar{w} \) with four or less coordinates from \( \bigcup_{i=1}^{k} A_i \). Without loss of generality, we take \( \bar{w} = ((x_0, y_0), a_1, w_2, w_3, w_4) \), where \( a_i \in A_i \). Since \( F_i \) is an MDS \((2, 5, q_i)\) code with \( 4-A_i \)-hole, there is a vector \( \bar{z} = (y_0, a_1, z_2, z_3, z_4) \) \( F_i \). Since \( C_i \) is an MDS \((3, 5, p)\) code, there exists a vector \( \bar{x} = (x_0, x_1, x_2, x_3, x_4) \in C_i \). Then the distance between vectors \( \bar{x} \times A_i \bar{x} \) and \( \bar{w} \) is equal to 3.

Lemma 1. There exists an MDS \((2, 5, 6)\) code with \( 4-[a, b]-\)hole.

The proof is by direct verification of the table below.

<table>
<thead>
<tr>
<th>a</th>
<th>b</th>
<th>2</th>
<th>3</th>
<th>0</th>
<th>1</th>
<th>0</th>
<th>1</th>
<th>b</th>
<th>a</th>
<th>3</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>b</td>
<td>a</td>
<td>2</td>
<td>3</td>
<td>a</td>
<td>b</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>b</td>
<td>a</td>
<td>0</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>a</td>
<td>b</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>a</td>
<td>b</td>
<td>1</td>
<td>0</td>
<td>b</td>
<td>a</td>
<td>3</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>.</td>
<td>.</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>3</td>
<td>.</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>3</td>
<td>0</td>
<td>.</td>
<td>.</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td>0</td>
<td>.</td>
<td></td>
</tr>
</tbody>
</table>

\( P \) \text{ POTAPOV}
Theorem 2. If \( q = 16(6s \pm 1) + 4 \), then there exists an MDS \((2, 5, q)\) code.

Proof. By Lemma 1 and Propositions 5 and 8 \((p = q = 4, k = 2, q_1 = 6)\), there exists an MDS \((2, 5, 20)\) code with 4-A-hole, where \(|A| = 4\). By Theorem 1 \((q_1 = 20, q = 16, k = 4)\) we can obtain an MDS \((2, 5, 16p + 4)\) code if there exists a super MDS \((2, 5, p)\) code. Since any integer \( p = 6s \pm 1 \) is not divisible by 2 and 3, there exists a super MDS \((2, 5, p)\) code by Propositions 4 and 6.

By Proposition 1 all MDS \((2, 5, q)\) codes are equivalent to pairs of orthogonal latin cubes of order \( q \). If \( 6s - 1 = 18i - 1 \) or \( 6s - 1 = 18i + 5 \), then pairs of orthogonal latin cubes of order \( q = 16(6s - 1) + 4 \) were not previously known because in these cases \( q \) is divisible by 3 but it is
not divisible by 9. Ten minimal new obtained orders (not only of type \( q = 16(6s - 1) + 4 \)) are 84, 132, 276, 372, 516, 564, 660, 852, 948, and 1140.

4 | CONNECTION BETWEEN MDS CODES AND COMBINATORIAL DESIGNS

A Steiner system with parameters \( \tau, d, q \), written \( S(\tau, d, q) \), is a set of \( d \)-element subsets of \( Q_q \) (called blocks) with the property that each \( \tau \)-element subset of \( Q_q \) is contained in exactly one block.

**Theorem 3.** If \( D_2 \) and \( D_3 \) are Steiner systems \( S(2, 5, q) \) and \( S(3, 5, q) \), respectively, and \( D_2 \subseteq D_3 \), then there exits an MDS \( (2, 5, q) \) code.

**Proof.** Consider a block \( X = \{x_1, x_2, x_3, x_4, x_5\} \in D_3 \backslash D_2 \). Define a set \( M_X = \{(x_{i_1}, x_{i_2}, x_{i_3}, x_{i_4}, x_{i_5}) \mid \tau \in \text{Alt}(5)\} \), where \( \text{Alt}(5) \) is the alternating group.

By Proposition 3 there exists an MDS \( (2, 5, 5) \) code that contains \( (a, a, a, a, a) \) for all \( a \in Q_5 \). Suppose that \( X = \{x_1, x_2, x_3, x_4, x_5\} \in D_2 \). Let us define an MDS \( (2, 5, 5) \) code \( M_X \) over the alphabet \( X \) such that \( M_X \) contains \( (a, a, a, a, a) \) for all \( a \in Q_q \). Let us prove that \( M = \bigcup_{X \in D_3} M_X \) is an MDS \( (2, 5, q) \) code. The following holds:

\[
|M| = q + |D_2| \cdot (5^3 - 5) + (|D_3| - |D_2|) \cdot |\text{Alt}(5)|
\]

\[
= q + 5 \cdot 2 \cdot 4 \cdot \frac{q(q - 1)}{4 \cdot 5} + 3 \cdot 4 \cdot 5 \cdot \left( \frac{q(q - 1)(q - 2)}{3 \cdot 4 \cdot 5} - \frac{q(q - 1)}{4 \cdot 5} \right) = q^3.
\]

Suppose that \( X \in D_3 \backslash D_2 \), \( Y \in D_3 \) and \( X \neq Y \). The distance between codes \( M_X \) and \( M_Y \) is not less than 3 because \( |X \cap Y| \leq 2 \). Suppose \( X, Y \in D_2 \) and \( X \neq Y \). Then \( |X \cap Y| \leq 1 \). If \( x \in M_X \) is not a constant vector, then it contains not more than 2 equal symbols. If \( x \in M_X \) and \( y \in M_Y \) are not constant vectors, then \( \rho(x, y) \geq 3 \) by direct verification.

If \( x, y \in M_X \) and \( X \in D_2 \), then \( \rho(x, y) \geq 3 \) by the definition of \( M_X \). Any nonconstant permutation from \( \text{Alt}(5) \) permutes three or more elements. Therefore for \( X \in D_3 \backslash D_2 \) we obtain that \( \rho(x, y) \geq 3 \) for any distinct \( x, y \in M_X \).

Thus we proved that the code distance of \( M \) is at least 3. So, \( M \) is an MDS \( (2, 5, q) \) code by the Singleton bound (Proposition 2). \( \square \)

The natural divisibility condition for the existence of Steiner systems \( S(2, 5, n) \) and \( S(3, 5, n) \) simultaneously is that \( n = 5 \) or \( 41 \mod 60 \). Steiner systems \( S(3, 5, 41) \) are unknown. Steiner systems \( S(2, 5, 65) \) and \( S(3, 5, 65) \) exist. Systems \( S(2, q + 1, q^3 + 1) \) are unitals and systems \( S(3, q + 1, q^3 + 1) \) are spherical geometries if \( q \) is a prime power (\( q = 4 \) in this case). But it is unknown whether the system \( S(3, 5, 65) \) contains the system \( S(2, 5, 65) \). Keevash [6] and Glock et al [4] proved that the natural divisibility conditions are sufficient for the existence of the Steiner system \( S(t, k, n) \) (and inserted Steiner systems) apart from a finite number of exceptional \( n \)'s given fixed \( t \) and \( k \). Therefore it is possible to use the theorem above for constructing MDS \( (2, 5, q) \) codes if \( q \) is large enough.
ACKNOWLEDGMENTS
My sincere thanks are due to D.S. Krotov who programmed the proposed method and calculated a series of new pairs of orthogonal latin cubes (see https://ieee-dataport.org/open-access/graeco-latin-cubes). The research was carried out at the Sobolev Institute of Mathematics at the expense of the Russian Science Foundation (18-11-00136).

ORCID
Vladimir N. Potapov http://orcid.org/0000-0001-9461-2064

REFERENCES

How to cite this article: Potapov VN. Constructions of pairs of orthogonal latin cubes. J Combin Des. 2020;28:604–613. https://doi.org/10.1002/jcd.21718