On the number of frequency hypercubes $\mathsf{F}^n(4;2,2)$[*]

Minjia Shi[†], *Shukai Wang*, *Xiaoxiao Li*, *and Denis S. Krotov*[‡]

Abstract

A frequency n-cube $\mathrm{F}^n(4;2,2)$ is an n-dimensional $4 \times \cdots \times 4$ array filled by 0s and 1s such that each line contains exactly two 1s. We classify the frequency 4-cubes $\mathrm{F}^4(4;2,2)$, find a testing set of size 25 for $\mathrm{F}^3(4;2,2)$, and derive an upper bound on the number of $\mathrm{F}^n(4;2,2)$. Additionally, for any n greater than 2, we construct an $\mathrm{F}^n(4;2,2)$ that cannot be refined to a latin hypercube, while each of its sub-$\mathrm{F}^{n-1}(4;2,2)$ can.

Keywords: frequency hypercube, frequency square, latin hypercube, testing set, MDS code

1 Introduction

A *frequency hypercube* (*frequency n-cube*) $\mathrm{F}^n(q;\lambda_0,\ldots,\lambda_{m-1})$ is an n-dimensional $q \times \cdots \times q$ array, where $q = \lambda_0 + \cdots + \lambda_{m-1}$, filled by the numbers $0,\ldots,m-1$ with the property that each line contains exactly λ_i cells with i, $i = 0,\ldots,m-1$ (a *line* consists of q cells of the array differing in one coordinate). Frequency hypercubes generalize both frequency squares, $n = 2$, and latin hypercubes, $\lambda_0 = \cdots = \lambda_{q-1} = 1$ (alternatively, the frequency hypercubes $\mathrm{F}^{n+1}(q;1,q-1)$ are also equivalent to latin n-cubes), see respectively [2], [7] and [9] for the enumeration of the objects of small size. In their turn, frequency squares and latin hypercubes are different generalizations of latin squares, which have parameters $\mathrm{F}^2(q;1,\ldots,1)$, in our notation.

In the current work, we study frequency hypercubes of order $q = 4$. The latin hypercubes of order 4, corresponding to $\mathrm{F}^n(4;1,1,1,1)$ and $\mathrm{F}^n(4;1,3)$ are characterized in [5], and their structures are now rather well understood; in particular, not only the asymptotics [12], but also an effective recursive formula for

[*] The work of M. J. Shi is supported by the National Natural Science Foundation of China (61672036), the Excellent Youth Foundation of Natural Science Foundation of Anhui Province (1808085J20), the Academic Fund for Outstanding Talents in Universities (gxbjZD03); the work of D. S. Krotov is supported within the framework of the state contract of the Sobolev Institute of Mathematics (project no. 0314-2019-0016).

[†] M. Shi, S. Wang and X. Li are with the School of Mathematical Sciences, Anhui University, Hefei, 230601, China

[‡] D. Krotov is with the Sobolev Institute of Mathematics, Novosibirsk, 630090, Russia

their number is known [13], see sequences A211214 and A211215 in OEIS [1]. Another case, $\mathrm{F}^n(4;1,1,2)$, is solved in [10], where it is proved that every frequency n-cube $\mathrm{F}^n(4;1,1,2)$ can be subdivided to $\mathrm{F}^n(4;1,1,1,1)$. We focus on the remaining case $\mathrm{F}^n(4;2,2)$. It should also be mentioned that all frequency hypercubes with $q < 4$ correspond to latin hypercubes of order q, which form only one isotopy class, for each n and q.

The goal of our paper is, at first, to enumerate all fruency hypercubes $\mathrm{F}^3(4;2,2)$ and $\mathrm{F}^4(4;2,2)$, and second, to improve the trivial upper bound 2^{3^n} on the number of fruency hypercubes $\mathrm{F}^n(4;2,2)$. The second result is also based on some calculations in small dimensions, where we study some more general class of objects than the frequency hypercubes, called unitrades. We use the language of coding theory as the working language in this paper. We study sets of vertices of the Hamming graph, called codes, and, in particular, the frequency hypercubes $\mathrm{F}^n(4;2,2)$ are represented by the special codes called double-MDS-codes in the Hamming graph $H(n,4)$, in such a way that a frequency hypercube $\mathrm{F}^n(4;2,2)$ is the characteristic function of a double-MDS-code.

The new upper bound is obtained by finding an appropriate testing set of size α^n, where $\alpha < 3$. Note that a lower bound of form $2^{2^{n+o(1)}}$ on the number of $\mathrm{F}^n(4;2,2)$ is immediate from the similar lower bound for $\mathrm{F}^n(4;1,1,1,1)$ (see [12]). So, the number of objects is double-exponential. In the framework of our study, the following questions are actual and remain open: What is the asymptotics of the double-logarithm of the number of $\mathrm{F}^n(4;2,2)$ (as well as $\mathrm{F}^n(q;\lambda_0,\ldots,\lambda_{m-1})$ for any fixed $q > 4$, $\lambda_0,\ldots, \lambda_{m-1}$)? What is the minimum size of a testing set for $\mathrm{F}^n(4;2,2)$ (in general, for $\mathrm{F}^n(q;\lambda_0,\ldots,\lambda_{m-1})$, $q > 3$), in particular, for $\mathrm{F}^3(4;2,2)$?

As follows from the definition, double-MDS-codes are equivalent to simple orthogonal arrays $\mathrm{OA}(2^{2n-1}, n, 4, n-1)$, see [3] for the definition and notation. In [11], based on a lower bound on the number of double-MDS-codes, Potapov derived a lower bound on the number of n-ary balanced correlation immune (resilient) Boolean functions of order $n/2$ (equivalently, simple orthogonal arrays $\mathrm{OA}(2^{n-1}, n, 2, n/2)$). Substituting the results of our computing of the number of $\mathrm{F}^4(4;2,2)$ to his arguments straightforwardly improves this lower bound for $n = 8$.

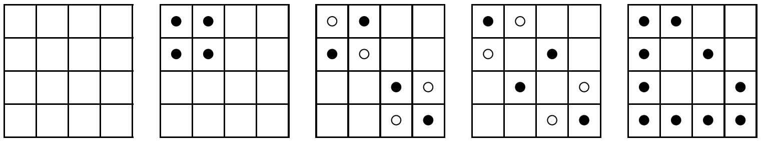
The material is organized as follows. Section 2 sets up the basic notations and definitions. Section 3 gives a straightforward algorithm to classify double-MDS-codes and unitrades. The results are shown in tables. Section 4 introduces the splittable property of double-MDS-codes. The main result of this paper is shown in Section 5. We give a testing set of size 25 for $\mathrm{F}^3(4;2,2)$, and derive an upper bound on the number of $\mathrm{F}^n(4;2,2)$.

2 Basic notations and definitions

2.1 Double-codes and related objects.

Let $\Sigma = \{0, 1, \ldots, q-1\}$ and Σ^n be the set of words of length n over the alphabet Σ. We set $q = 4$ in this paper, while the definitions are valid for arbitrary q. The *Hamming graph* $H(n, q)$ is a graph on the vertex set Σ^n, where two vertices are adjacent if they differ in one coordinate. We call a set of q pairwise adjacent vertices in $H(n, q)$ a *line* (essentially, a line is a maximal clique in $H(n, q)$). A (distance-2) *MDS code* is a subset of Σ^n intersecting every line in exactly one element (we consider only the minimum-distance-2 MDS codes, while in coding theory this concept is more general). A set $S \subset \Sigma^n$ is called a *double-MDS-code*, or a 2*-MDS*, for short, if each line of Σ^n contains exactly two elements from S. A set $S \subset \Sigma^n$ is called a *unitrade* if each line of Σ^n contains even number of elements from S. If each line of Σ^n contains zero or two elements from S, then S is called a *double-code.* A double-code is called *splittable* if it can be represented as a union of two independent sets (if the double-code is 2-MDS, then these two sets are MDS codes). The characteristic function $\chi_S : \Sigma^n \to \{0, 1\}$ of a 2-MDS code is a frequency n-cube $\mathrm{F}^n(q; q-2, 2)$.

For example, the picture below illustrates an incomplete collection of unitrades in $H(2, 4)$; the first four of them (and the complement of the 5th) are double-codes, while only the 3rd one and the 4th one are 2-MDS, both splittable.



Given a set $M \subset \Sigma^n$, a *layer* of M consists of all elements of M that have some fixed value a in a given coordinate i (referred to as the *direction* of the layer): $\{(c_0, \ldots, c_n) \in C \mid c_i = a\}$. We identify a layer with the corresponding subset of Σ^{n-1} by ignoring the fixed coordinate. Note that any layer inherits the property of the set to be an MDS code, double-MDS-code, double-code, or unitrade.

2.2 Isotopy and equivalence

An *isotopy* in Σ^n is an n-tuple of permutations $\theta_i : \Sigma \to \Sigma$, $i \in \{1, \ldots, n\}$. For an isotopy $\bar\theta = (\theta_1, \ldots, \theta_n)$ and a set $S \subset \Sigma^n$, we put

$$\bar\theta S = \{(\theta_1 x_1, \ldots, \theta_n x_n) \mid (x_1, \ldots, x_n) \in S\}.$$

Two sets $S_1 \subset \Sigma^n$ and $S_2 \subset \Sigma^n$ are *isotopic* if there exists an isotopy $\bar\theta$ such that $\bar\theta S_1 = S_2$. An *autotopy* of a set $S \subset \Sigma^n$ is an isotopy $\bar\theta$ such that $\bar\theta S = S$.

Two sets $S_1 \subset \Sigma^n$ and $S_2 \subset \Sigma^n$ are *equivalent* if there exists an isotopy $\bar\theta$ and a permutation σ of n coordinates such that $\sigma\bar\theta S_1 = S_2$, where

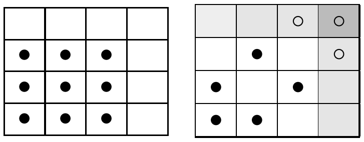
$$\sigma S = \{(x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)}) \mid (x_1, \ldots, x_n) \in S\}.$$

If $\sigma\bar{\theta}S = S$ holds for some set $S_1 \subset \Sigma^n$, isotopy $\bar{\theta}$ and coordinate permutation σ, then the pair $(\sigma, \bar{\theta})$ is called an *automorphism* of S. The group of all automorphisms (autotopies) of a set S with the composition as the group operation is denoted $\mathrm{Aut}(S)$ (respectively $\mathrm{Atop}(S)$).

Two frequency n-cubes χ_{S_1} and χ_{S_2} are *isotopic* (*equivalent*) if S_1 is isotopic (equivalent) to S_2 or $\Sigma^n \backslash S_2$. So, we see that the number of equivalence classes of frequency n-cubes $\mathrm{F}^n(4;2,2)$ is in general smaller than that of double-MDS-codes in $H(n,4)$: a double-MDS-code can be inequivalent to its complement, but the corresponding two frequency n-cubes are equivalent by the definition. An *autotopy* of a frequency n-cube χ_S is an isotopy that sends the corresponding double-MDS-code S to itself or to its complement $\Sigma^n \backslash S$. The *automorphisms* of a frequency n-cube are defined similarly. So, the set of autotopies (automorphisms) of a frequency n-cube $\mathrm{F}^n(4;2,2)$ either coincides with the set of autotopies (automorphisms) of the corresponding double-MDS-code, or is twice larger of it.

2.3 Testing sets

A subset T of Σ^n is a *testing set* for double-MDS-codes (or, equivalently, for any other class of subsets of Σ^n) if $C_1 \cap T \neq C_2 \cap T$ for any two different double-MDS-codes in $H(n,4)$.



●	●	●	
●	●	●	
●	●	●	

▨	▨	○	○
	●		○
●		●	▨
●	●		▨

Tab. 1: A double-MDS-code (right table) is reconstructed by its intersection with the testing set (left table)

For example, $\{0,1,2\}^n$ (see, e.g., Table 1) is a testing set for double-MDS-codes in $H(n,4)$; its size is 3^n, and it is not difficult to show that it is minimum for $n = 1$, 2. However, we can find a smaller testing set for $n = 3$; the minimum size of a testing set in the three-dimensional case is still unknown.

3 Classification

3.1 Algorithm

Using a computational approach, we classify double-MDS-codes in $H(3,4)$ and $H(4,4)$ and unitrades in $H(3,4)$. The algorithm is rather straightforward, and we describe it by the example of double-MDS-codes.

Assume that, as a result of the past classification, we have that the number of double-MDS-codes of length $n-1$ is N_{n-1} and they are partitioned into a equivalence classes.

We consider a double-MDS-code of length n as the union of 4 of its layers in the last direction, essentially, 4 double-MDS-codes of length $n-1$. As the fourth layer is uniquely reconstructed from the first three ones, we can run through N_{n-1}^3 triples of double-MDS-codes of length $n-1$ and check if they can be completed by the fourth layer to form a double-MDS-code of length n. In such a way, we construct all double-MDS-codes of length n. However, simple calculations show that the number N_{n-1}^3 is too large to manage all these possibilities. A standard way to make the search faster is, at each step, to choose only nonequivalent cases (this procedure is often called *isomorph rejection*).

At **step 1**, we choose the first layer from a nonequivalent double-MDS-codes of length $n-1$ (representatives of the equivalence classes).

At **step 2**, for each choice of the first layer, we choose the second layer from all N_{n-1} double-MDS-codes of length $n-1$. So, we process $a \cdot N_{n-1}$ cases at this step. Among all possible unions of the first layer and the second layer, called *semi-codes*, we choose only nonequivalent a' representatives, where a' is the number of the equivalence classes of semi-codes (the equivalence of codes is tested by the standard way described in [4], by representing codes as graphs and using the software [8] that deals with graph isomorphism).

At **step 3**, for each of a' representatives of semi-codes, we choose the third layer from N_{n-1} different double-MDS-codes of length $n-1$. So, we process $a' \cdot N_{n-1}$ cases at this step. Some of the resulting cases cannot be completed to a double-MDS-code of length n (for example, if there are already three codewords in some line of the last direction); for the remaining cases, the completion is unique, and we use isomorph rejection to keep only nonequivalent representatives of the resulting double-MDS-codes of length n.

Validation. We can check the results of the classification using a general double-counting approach described in [4, 10.2]. We know that the number of semi-codes is N_{n-1}^2. And for a representative of every their equivalence classes, we know the number of continuations to a double-MDS-code of length n. This number is the same for all semi-codes from the same equivalence class. Hence, the total number N_n of double-MDS-codes of length n satisfies

$$N_n = \sum_{i=1}^{a'} M_i R_i, \tag{1}$$

where M_i is the number of semi-codes in the ith equivalence class and R_i is the number of double-MDS-codes of length n that continue each representative of the ith class. The numbers M_i can be easily counted from the automorphism group of the corresponding representative; additionally, we have $\sum_{i=1}^{a'} M_i = N_{n-1}^2$. The total number N_n can be alternatively found as

$$N_n = \sum_i T_i, \qquad T_i = \frac{4!^n \times n!}{|\mathrm{Aut}(C_i)|}, \tag{2}$$

where T_i is the size of the ith equivalence class and C_i is its representative. Coinciding the values of N_n obtained from (1) and (2) certifies that our algorithm gives correct numbers R_i and, in particular, it did not miss anything.

3.2 Results of the classification

The results of the classification are reflected in following theorems and Tables 2, 3 and 4.

Theorem 3.1. *There are* 51678 *double-MDS-codes of length* 3*, divided into* 10 *equivalence classes or* 26 *isotopy classes. There are* 51678 *frequency* $F^3(4;2,2)$ *cubes, divided into* 10 *equivalence classes or* 26 *isotopy classes.*

Theorem 3.2. *There are* 55720396530 *double-MDS-codes of length* 4*, divided into* 8895 *equivalence classes or* 192214 *isotopy classes. There are* 55720396530 *frequency* $F^4(4;2,2)$ *hypercubes, divided into* 7203 *equivalence classes or* 154078 *isotopy classes.*

Theorem 3.3. *There are* 2^{27} *unitrades in* $H(3,4)$*, divided into* 2528 *equivalence classes. Representatives of* 312 *of them are equivalent to their complement.*

3.3 The number of unitrades of length 3 of order 4

For a unitrade of length n of order 4, there are 8 cases for each line by definition. So, the number of unitrades of length n of order 4 is $8^{3^{n-1}}$ since a unitrade can be reconstructed from only 3 of 4 layers in any direction. This number is 8^9 when $n = 3$. Then, we can get 2528 classes by the definition of general equivalence. The results are as follows.

the size of unitrades	the number of classes
0 and 64	1
8 and 56	1
12 and 52	1
14 and 50	1
16 and 48	9
18 and 46	5
20 and 44	22
22 and 42	26
24 and 40	121
26 and 38	125
28 and 36	329
30 and 34	328
32	590
total:	2528

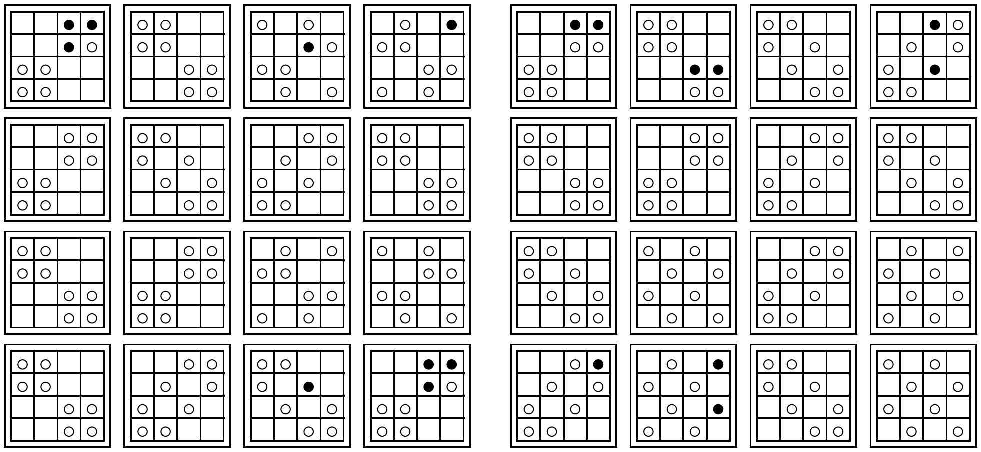
Tab. 2: Unitrades in $H(3,4)$

3.4 Double-MDS-codes in $H(4,4)$

We have known the number of double-MDS-codes in $H(3,4)$ is 51678. And for length 4, each layer is a code of length 3. Therefore, the total number of codes of length 4 is no more than 51678^4. We use the computer to search these, and obtain 55720396530 double-MDS-codes of length 4 in total. From the three steps in Subsection 3.1, we get 8895 classes.

From the definitions, we can get the relationship between the splittability of a code and the splittability of each of its layers. If a double-MDS-code is splittable, then each layer of this code is splittable. If there exists a non-splittable layer, then the entire code is non-splittable. But if all layers are splittable, it does not necessarily mean that the code itself is splittable.

In fact, all double-MDS-codes in $H(4,4)$ are splittable if their layers are splittable except for the following two (in the diagram below, the black vertices induce a cycle of length 9).



In the next section, we prove the existence of splittable double-MDS-codes with non-splittable layers for any length.

4 Splittable double-MDS-codes with non-splittable layers

The theorem proved in this section is important for us to understand the interrelation between the classes of double-MDS-codes and splittable double-MDS-codes. The double-MDS-code is defined by a local property; a code is a double-MDS-code if and only if each of its layers in each direction is a double-MDS-code. As we will see below, the same is not true for splittable double-MDS-codes.

We first introduce some notations. Two adjacent vertices of the Hamming graph differ in one coordinate, whose number is called the *direction* of the corresponding edge. Edges of the same direction are called *parallel*. We color all edges of $H(n,4)$ by three colors depending on the values of the two words in the coordinate in which they are different. If the values are either 0 and 1 or 2 and 3, then the color is 1; if the values are either 0 and 2 or 1 and 3, the color is 2; for 0, 3 or 1, 2, the color is 3. If a double-MDS-code is not splittable, then its induced subgraph of the Hamming graph is not bipartite. In this case, there is an odd-length cycle in this subgraph.

$\lvert\mathrm{Aut}(C)\rvert$	N	N'	N''	N^*
$24 \cdot 2048$	1	1	1	1
$4' \cdot 512$	1	1	1	1
$6 \cdot 256$	1	1	1	1
$2' \cdot 256$	1	1	1	1
$24 \cdot 128$	1	1	1	1
$8 \cdot 128$	2	2	2	2
$6 \cdot 128$	1	1	1	1
$4' \cdot 128$	1	1	1	1
$2' \cdot 128$	2	2	2	2
$2'' \cdot 128$	1	1	1	1
$6 \cdot 64$	1	1	1	1
$4' \cdot 64$	2	2	2	2
$2' \cdot 64$	3	3	3	2
$1 \cdot 64$	1	1	1	
$8 \cdot 32$	1	1	1	1
$6 \cdot 32$	1	1	1	1
$4' \cdot 32$	3	3	3	
$2' \cdot 32$	22	22	22	1
$1 \cdot 32$	7	7	7	
$24 \cdot 16$	2	2	2	2
$6 \cdot 16$	4	4	4	3
$4' \cdot 16$	8	8	8	7
$3 \cdot 16$	1	1	0	
$2' \cdot 16$	27	27	25	6
$2'' \cdot 16$	4	4	2	
$1 \cdot 16$	18	16	15	
$24 \cdot 8$	2	2	2	2
$8 \cdot 8$	2	2	2	2
$6 \cdot 8$	10	10	10	3
$4' \cdot 8$	10	10	10	2
$3 \cdot 8$	1	1	1	
$2' \cdot 8$	58	58	57	2
$2'' \cdot 8$	7	7	7	1
$1 \cdot 8$	71	65	63	
$12 \cdot 4$	1	1	0	
$6 \cdot 4$	3	3	3	
$4' \cdot 4$	18	16	16	
$3 \cdot 4$	1	1	0	
$2' \cdot 4$	173	169	169	
$2'' \cdot 4$	6	6	6	
$1 \cdot 4$	220	212	207	
$24 \cdot 2$	1	1	1	
$6 \cdot 2$	12	10	10	
$4' \cdot 2$	38	30	30	
$3 \cdot 2$	7	3	1	
$2' \cdot 2$	297	279	273	
$2'' \cdot 2$	46	40	36	
$1 \cdot 2$	1057	917	875	
$8 \cdot 1$	4	0	0	
$6 \cdot 1$	21	19	19	
$4' \cdot 1$	16	0	0	
$4^\circ \cdot 1$	12	0	0	
$3 \cdot 1$	16	10	6	
$2' \cdot 1$	728	506	506	
$2'' \cdot 1$	78	0	0	
$1 \cdot 1$	5862	3018	2781	
total :	8895	5511	5200	50

Tab. 3: The table reflects the number of non-equivalent double-MDS-codes in $H(n,4)$, $n=4$, with the given number of automorphisms. In the first column, the number of automorphisms of a double-MDS-code C is represented in the form $P \cdot T$, where $T = \lvert\mathrm{Atop}(C)\rvert$ and P is the order of the group $\mathrm{Aut}(C)/\mathrm{Atop}(C)$ acting on the four coordinates. The accents reflect the type of this group: groups of type $2'$ and $4'$ contain a transposition; groups of type $2''$ and $4''$ consist of the identity permutation and involutions without fixed point; group of type 4° corresponds to the cyclic group of order 4; all other groups of permutations of the four coordinated are defined by their orders up to conjugancy. The second column contains the number N of inequivalent double-MDS-codes with the corresponding restrictions on the automorphism set. The third column contains the number N' of such codes that are equivalent to their complement. The fourth column contains the number N'' of such codes that are isotopic to their complement. N^* in the fifth column is the number of splittable double-MDS-codes. Using these data, the following numbers can be found for each row. The number of isotopy classes of double-MDS-codes is $N \cdot n!/P$. The number of inequivalent frequency n-cubes $\mathrm{F}^n(4;2,2)$ is $(N+N')/2$; and $(N-N')/2$ of them have $P \cdot T$ automorphisms, while the remaining N' have twice more (including the automorphisms that change the value of the function). The number of non-isotopic frequency n-cubes $\mathrm{F}^n(4;2,2)$ is $(N+N') \cdot n!/2P$; and $(N+N'-2N'') \cdot n!/2P$ of them have T autotopies, while the remaining $N'' \cdot n!/P$ have twice more.

$\lvert\mathrm{Aut}(C)\rvert$	N	N'	N''	N^*
$6 \cdot 256$	1	1	1	1
$2 \cdot 64$	1	1	1	1
$6 \cdot 32$	1	1	1	1
$2 \cdot 32$	1	1	1	1
$2 \cdot 16$	1	1	1	1
$2 \cdot 8$	1	1	1	0
$1 \cdot 8$	1	1	1	0
$6 \cdot 4$	1	1	1	0
$3 \cdot 4$	1	1	0	0
$2 \cdot 2$	1	1	1	0
total :	10	10	9	5

Tab. 4: The table reflects the number of non-equivalent double-MDS-codes in $H(n,4)$, $n = 3$, with the given number of automorphisms. The notation and calculation of the derived values are the same as those in Table 3.

Lemma 4.1. *Any odd-length cycle in $H(n,4)$ contains three parallel edges of three different colors.*

Proof. If the cycle contains edges of at most two colors of some direction, then the number of the edges of this direction in the cycle is even. For example, if the cycle only has edges of color 2 and 3 in direction i, then each edge of these direction changes the value of the ith coordinate between the sets $\{0,1\}$ and $\{2,3\}$. Walking along all the edges of the cycle, we have even number of such changes because finally we return to the starting vertex.

For a cycle of odd length, there is an odd number of edges of some direction. Hence, the edges of these directions are colored by three different colors. □

Theorem 4.2. *For any n larger than 2, there is an unsplittable double-MDS-code in $H(n,4)$ whose all layers in all directions are splittable.*

Proof. The idea of the construction is based on Lemma 4.1. We will construct an unsplittable double-MDS-code, with an induced cycle of odd length $2n+1$, such that the edges of the induced graph satisfy

(i) the edges of any direction from 1 to $n-1$ are colored by only two colors;

(ii) for any two edges of direction n and colors 1 and 2, the distance between them is $n-1$ (i.e., two words from different edges differ in each coordinate from 1 to $n-1$).

Property (i) guarantees that every layer in the nth direction is splittable by Lemma 4.1. On the other hand, Property (ii) guarantees that every layer in any other direction is splittable, again by Lemma 4.1.

To construct such a code, we divide the vertex set of $H(n,4)$ into 2^{n-1} *sectors* V_a, $a \in \{0,2\}^{n-1} \times \{0\}$, where $V_a = \{a+b \mid b \in \{0,1\}^{n-1} \times \{0,1,2,3\}\}$. Define three $\{0,1\}$-valued functions α, β, γ on $\{0,1,2,3\}$:

x	0	1	2	3
$\alpha(x)$	1	1	0	0
$\beta(x)$	1	0	1	0
$\gamma(x)$	0	1	1	0

On $\{0,1,2,3\}^n$, define the function

$$f(x) = \begin{cases} x_1 + ... + x_{n-1} + \alpha(x_n) \bmod 2 & \text{if } x \in V_{(0,...,0,0)}, \\ x_1 + ... + x_{n-1} + \beta(x_n) + 1 \bmod 2 & \text{if } x \in V_{(2,...,2,0,...,0,0)} \ (n-2 \text{ sectors}), \\ x_1 + ... + x_{n-1} + \gamma(x_n) \bmod 2 & \text{if } x \in V_{(2,...,2,0)}, \\ x_1 + ... + x_{n-1} + \beta(x_n) \bmod 2 & \text{otherwise.} \end{cases}$$

Denote M the set of ones of f. It is straightforward that f is an $\mathrm{F}^n(4;2,2)$ frequency hypercube, and so M is a double-MDS-code. Any edge of $H(n,4)$ of color 1 and direction from 1 to $n-1$ is in one sector, and the values of f on the two vertices of the edge are different. Hence, such an edge does not lie in M, and (i) is satisfied. Further, any edge in M of color 1 and direction n lies in the sector $V_{(0,...,0,0)}$, while any edge in M of color 3 and direction n lies in $V_{(2,...,2,0)}$. Hence, (ii) is also satisfied. As was mentioned above, properties (i) and (ii) imply that any layer of M is splittable. It remains to find a cycle of length $2n+1$:

- $(0,...,0,0)$, $(0,...,0,1)$,
- $(2,0,...,0,1)$, $(2,2,0,...,0,1)$, $\dots$, $(2,...,2,0,1)$, $(n-2$ vertices$)$,
- $(2,...,2,1)$, $(2,...,2,2)$,
- $(2,...,2,0,2)$, $(2,...,2,0,0)$, $(2,...,2,0,0,0)$, $\dots$, $(2,0,...,0,0)$, $(n-1$ vertices$)$.

□

5 An upper bound on the number of double-MDS-codes

The number of double-MDS-codes of length n has a trivial upper bound 2^{3^n} because every code can be reconstructed from only 3 of 4 layers in any direction. Thus, the size of the minimum testing set is no more than 3^n. For $n=3$, this value is 27.

Let $\mathcal{U}$ be the set of all unitrades of length n. And we denote $X = (x_{\bar{0}}, x_{\bar{1}}, ..., x_{\overline{q^n-1}})^T$, where $\bar{t} \in \Sigma^n$ is t in quaternary expansion.

Lemma 5.1. *D is a unitrade if and only if D corresponds to a solution of $AX = 0$ (mod 2), where A is a matrix over $\mathbb{F}_2$.*

It is obvious by the definition of unitrade. Here, $X = (x_{\bar{0}}, x_{\bar{1}}, ..., x_{\overline{4^n-1}})^T$ where $x_{\bar{i}} = 1$ if $\bar{i}$ belongs to D, otherwise $x_{\bar{i}} = 0$. For unitrade of length 2, the sum of each line is 0 (mod 2), that is,

$$\sum_{i=0}^{3} x_{ij} = 0, \ j = 0,1,2,3, \quad \text{and} \quad \sum_{j=0}^{3} x_{ij} = 0, \ i = 0,1,2,3.$$

In this case,

$$A = \begin{pmatrix} A_1^{(2)} \\ A_2^{(2)} \end{pmatrix} = \begin{pmatrix} I_4 \otimes (1,1,1,1) \\ (1,1,1,1) \otimes I_4 \end{pmatrix}.$$

(Here and below, the symbol $\otimes$ denotes the Kronecker product of matrices, and I_m is the identity matrix of order m.) Similarly, the form of A is as follows:

$$A = \begin{pmatrix} A_1^{(n)} \\ A_2^{(n)} \\ \vdots \\ A_n^{(n)} \end{pmatrix}, \qquad A_i^{(n)} = \begin{cases} I_4 \otimes A_i^{(n-1)} & 1 \le i \le n-1, \\ (1,1,1,1) \otimes I_{4^{n-1}} & i = n. \end{cases}$$

Let $\mathcal{D}$ be the set of all possible symmetric differences of double-MDS-codes in $H(n,4)$:

$$\mathcal{D} = \{C_1 \triangle C_2 \mid C_1, C_2 \text{ are double-MDS-codes}\}.$$

The following proposition can give a testing set.

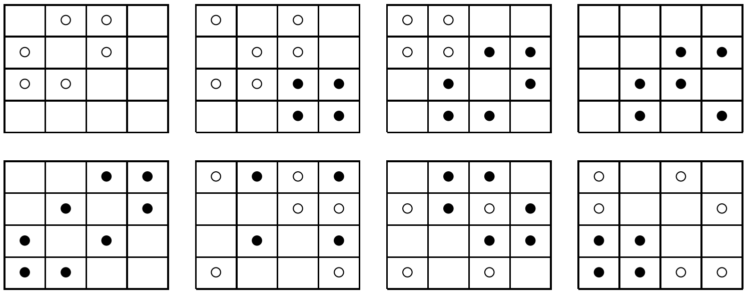
Proposition 5.2. *Let D be a unitrade. If no non-empty set from $\mathcal{D}$ is a subset of D, then there exists a testing set $T \subseteq \Sigma^n \backslash D$ of size $3^n - k$, where 2^k is the number of subsets of D that are unitrades, k being the dimension of the kernel of some linear operator.*

Proof. Denote $\overline{D} = \Sigma^n \backslash D$ and $N = |\overline{D}|$. Let $\overline{D} = \{\bar{u}_0, \bar{u}_1, ..., \bar{u}_{N-1}\}$, and $\overline{D}$ is also a unitrade. We define the matrix $B = (b_{ij})_{N \times 4^n}$ corresponding to $\overline{D}$ by

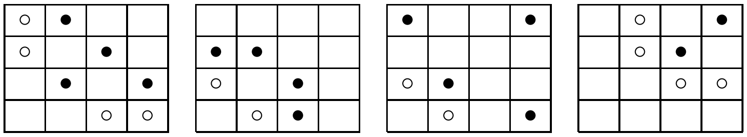
$$b_{ij} = \begin{cases} 1 & \text{if } j \text{ is the quaternary expansion of } \bar{u}_i, \\ 0 & \text{otherwise.} \end{cases}$$

Then, the solution space P of $\begin{pmatrix} A \\ B \end{pmatrix} X = 0$ is $\{X_P \mid P \subset D \text{ and } P \in \mathcal{U}\}$. So, the rank of the matrix $\begin{pmatrix} A \\ B \end{pmatrix}$ is $4^n - k$, where $2^k = |\{P \mid P \subset D \text{ and } P \in \mathcal{U}\}|$. The rank of A is $4^n - 3^n$ (its kernel corresponds to the set $\mathcal{U}$ of all unitrades), so we can find $3^n - k$ rows of B, with numbers i_1, ..., i_{3^n-k}, forming a $(3^n - k) \times 4^n$ matrix B' such that the rank of $\begin{pmatrix} A \\ B' \end{pmatrix}$ is also $4^n - k$. Each row of B' has 1 in exactly one position, corresponding to some $\bar{u}_i$. We state that the set $T = \{\bar{u}_i \mid i = i_1, ..., i_{3^n-k}\}$ is testing for double-MDS-codes. Indeed, if two double-MDS-codes C_1 and C_2 meet $C_1 \cap T = C_2 \cap T$, then $C = C_1 \triangle C_2$ does not intersect with T. Hence, X_C is in the kernel of B'. Since C is a unitrade, X_C is in the kernel of A. We conclude that $\begin{pmatrix} A \\ B \end{pmatrix} X_C = 0$, which means that C is in $\{P \mid P \subset D \text{ and } P \in \mathcal{U}\}$. By the hypothesis of the proposition, C is the empty set. It follows that $C_1 = C_2$ and T is a testing set. □

The straightforward checking shows that there are two inequivalent unitrades D, of cardinalities 32 and 38, that satisfy the hypothesis of the proposition with $k = 2$ (in the diagram below, white and black bullets indicate proper subunitrades),



and there are no unitrades D that satisfy it with $k = 3$. The second unitrade has the following complement,



where removing any white vertex results in a testing set of size 25.

This result is generalized by the following lemma, a special case of [6, Proposition 26] (for completeness, we give a proof).

Lemma 5.3. *Let $T \subset \Sigma^3$ be a testing set for double-MDS-codes of length 3. Then the Cartesian product of testing sets $T^l \subset \Sigma^{3l}$ is a testing set for double-MDS-codes of length $3l$.*

Proof. We prove this theorem by induction. Let $C_1 \mid_{T^l} = C_2 \mid_{T^l}$ where C_1 and C_2 are two double-MDS-codes. Then, by the induction hypothesis, for any $c \in T$, $C_1 \mid_{T^{l-1} \times \{c\}} = C_2 \mid_{T^{l-1} \times \{c\}}$ implies $C_1 \mid_{\Sigma^{(l-1)3} \times \{c\}} = C_2 \mid_{\Sigma^{(l-1)3} \times \{c\}}$. Hence, for any $\omega \in \Sigma^{(l-1)3}$, we have $C_1 \mid_{\{\omega\} \times T} = C_2 \mid_{\{\omega\} \times T}$. The set $\{\omega\} \times T$ is testing on $\{\omega\} \times \Sigma^3$. Then $C_1 \mid_{\{\omega\} \times \Sigma^3} = C_2 \mid_{\{\omega\} \times \Sigma^3}$ for any $\omega \in \Sigma^{(l-1)3}$. □

Corollary 5.4. *The number of double-MDS-codes in Σ^n, where n is divisible by 3, is at most 2^{α^n}, where $\alpha = (2^3 - 2)^{\frac{1}{3}} < 3$.*

With a slightly worth constant α, the result is generalized to an arbitrary $n \geq 3$.

Theorem 5.5. (upper bound) *The number of double-MDS-codes in Σ^n, $n \geq 3$, is at most 2^{α^n}, where $\alpha < 3$.*

Proof. According to Corollary 5.4, we know that if $n = 3k$ for any positive integer k, then the size of a testing set is no more than $(3^3 - 2)^k = \alpha_n^n$, where $\alpha_n = ((3^3 - 2)^k)^{\frac{1}{n}} < 3$.

For $n = 3k{+}1$, a double-MDS-code can be considered as the union of 4 layers, 4 double-MDS-codes of length $3k$. Moreover, each of them can be determined by the other three codes. Therefore, the minimum size of a testing set is no more than $(3^3 - 2)^k \times 3 = \alpha_n^n$, where $\alpha_n = ((3^3 - 2)^k \times 3)^{\frac{1}{n}} < 3$.

For $n = 3k + 2$, similarly, the size of a testing set is no more than $(3^3 - 2)^k \times 3 \times 3 = \alpha_n^n$. Here, $\alpha_n = ((3^3 - 2)^k \times 3 \times 3)^{\frac{1}{n}} < 3$.

The value of α_n depends on n, and it remains to show that it is upperbounded by some constant less than 3. Since the derivative functions of $f(x) = ((3^3 - 2)^x \times 3)^{\frac{1}{3x+1}}$ and $g(x) = ((3^3 - 2)^x \times 3 \times 3)^{\frac{1}{3x+2}}$, $x > 0$ are both negative, α_n is a decreasing sequence when big enough $n = 3k + 1$ or $n = 3k + 2$. So, the statement of the theorem holds with $\alpha = \max_{n\geq 3} \alpha_n = \max\{25^{\frac{1}{3}}, 75^{\frac{1}{4}}, 225^{\frac{1}{5}}\} = 225^{\frac{1}{5}} < 3$. □

Remark 1. It worthed to check if the same approach works for more general class of objects, double-codes. Direct computations show that the set of symmetric differences of double-codes in $H(3, 4)$ is the whole $\mathcal{U}$, and a testing set of size less than 27 cannot be found in the way described. So, the best upper bound on the number of double-codes remains trivial, 2^{3^n}.

6 Acknowledgement

The authors are grateful to Vladimir Potapov for useful discussions.

References

[1] The On-Line Encyclopedia of Integer Sequences. Published electronically.

[2] L. J. Brant and Mullen G. L. Some results on enumeration and isotopic classification of frequency squares. *Util. Math.*, 29:231–244, 1986.

[3] M Greig and C. J. Colbourn. Orthogonal arrays of index more than one. In C. J. Colbourn and J. H. Dinitz, editors, *Handbook of Combinatorial Designs*, Discrete Mathematics and Its Applications, pages 219–223. Chapman & Hall/CRC, Boca Raton, London, New York, second edition, 2006.

[4] P. Kaski and P. R. J. Östergård. *Classification Algorithms for Codes and Designs*, volume 15 of *Algorithms Comput. Math.* Springer, Berlin, 2006. DOI: 10.1007/3-540-28991-7.

[5] D. S. Krotov and V. N. Potapov. n-Ary quasigroups of order 4. *SIAM J. Discrete Math.*, 23(2):561–570, 2009. DOI: 10.1137/070697331.

[6] D. S. Krotov and V. N. Potapov. On the cardinality spectrum and the number of latin bitrades of order 3. *Probl. Inf. Transm.*, 55(4):343–365, 2019. DOI: 10.1134/S0032946019040021 translated from Probl. Peredachi Inf. 55(4) (2019), 55–75.

[7] V. Krčadinac. Frequency squares of orders 7 and 8. *Util. Math.*, 72:89–95, 2007.

[8] B. D. McKay and A. Piperno. Practical graph isomorphism, II. *J. Symb. Comput.*, 60:94–112, 2014. DOI: 10.1016/j.jsc.2013.09.003.

[9] B. D. McKay and I. M. Wanless. A census of small Latin hypercubes. *SIAM J. Discrete Math.*, 22(2):719–736, 2008. DOI: 10.1137/070693874.

[10] V. N. Potapov. On extensions of partial n-quasigroups of order 4. *Sib. Adv. Math.*, 22(2):135–151, 2012. DOI: 10.3103/S1055134412020058 translated from Mat. Tr. 14(2):147-172, 2011.

[11] V. N. Potapov. A lower bound on the number of boolean functions with median correlation immunity. In *2019 XVI International Symposium "Problems of Redundancy in Information and Control Systems" (REDUNDANCY)*, pages 45–46. IEEE, 2019. DOI: 10.1109/REDUNDANCY48165.2019.9003342.

[12] V. N. Potapov and D. S. Krotov. Asymptotics for the number of n-quasigroups of order 4. *Sib. Math. J.*, 47(4):720–731, 2006. DOI: 10.1007/s11202-006-0083-9 translated from Sib. Mat. Zh. 47(4) (2006), 873-887.

[13] V. N. Potapov and D. S. Krotov. On the number of n-ary quasigroups of finite order. *Discrete Math. Appl.*, 21(5-6):575–585, 2011. DOI10.1515/dma.2011.035, translated from Diskretn. Mat. 24:1 (2012), 60–69.