The existence of perfect codes in Doob graphs

Denis S. Krotov

***Abstract*—We solve the problem of existence of perfect codes in the Doob graph. It is shown that 1-perfect codes in the Doob graph $D(m,n)$ exist if and only if $6m+3n+1$ is a power of 2; that is, if the size of a 1-ball divides the number of vertices.**

***Index Terms*—Perfect codes, Doob graphs, Eisenstein–Jacobi integers.**

I. Introduction

The codes in Doob graphs are special cases of codes over Eisenstein–Jacobi integers, see, e.g., [10], [20], which can be used for the information transmission in the channels with two-dimensional or complex-valued modulation. The vertices of a Doob graph can be considered as words in the mixed alphabet consisting of elements of the quotient (modulo 4 and modulo 2) rings of the ring of Eisenstein–Jacobi integers, see, e.g., [13]. In contrast to the cases considered in [10], [20], the number 4 is not prime, and the quotient ring is not a field. This fact is not a problem from the point of view of the modern coding theory, which has a rich set of algebraic and combinatorial tools to deal with rings, see, e.g., [24]; moreover, studying codes in Doob graphs is additionally motivated by the application of association schemes in coding theory [3]: the algebraic parameters of the schemes associated with these graphs are the same as for the quaternary Hamming scheme (this fact can be also treated from the point of view of the corresponding distance-regular graphs).

In this paper, we completely solve the problem of existence of perfect codes in the class of Doob graphs. Namely, we show the existence of 1-perfect codes in the Doob graph $D(m,n)$ for all m and n that satisfy the obvious necessary condition: the size $6m+3n+1$ of a ball of radius 1 divides the number 4^{2m+n} of vertices. In the previous papers [11], [13], [25], the problem was solved only for the cases when the parameters satisfy additional conditions admitting the existence of linear or additive perfect codes, or for small values of m.

The class of Doob graphs is a class of distance-regular graphs of unbounded diameter, and the problem considered can be viewed in the general context of the problem of existence of perfect codes in distance-regular graphs. We mention some known results in this area, mainly concentrating on distance-regular graphs important for coding theory. A connected graph is called distance-regular if there are constants s_{ij} such that for every i, j and for every vertex x, every vertex y at distance i from x has exactly s_{ij} neighbors at distance j from x. In the Hamming graphs $H(n,q)$, the problem of complete characterization of parameters of perfect codes is solved only for the case when q is a prime power [28], [33]: there are no nontrivial perfect codes except the e-perfect repetition codes in $H(2e+1,2)$, the 3- and 2-perfect Golay codes [6] in $H(23,2)$ and $H(11,3)$, respectively, and the 1-perfect codes in $H((q^k-1)/(q-1),q)$. In the case of a non-prime-power q, no nontrivial perfect codes are known, and the parameters for which the nonexistence is not proven are restricted by 1- and 2-perfect codes (the last case is solved for some values of q), see [9] for a survey of the known results in this area. The problem of the (non)existence of perfect codes in the Johnson graphs $J(n,w)$ is known as Delsarte's conjecture, see [4] and [7] for the known nonexistence results; in general, the problem remains open. An interesting open problem is connected with the problem of existence of 1-perfect codes in the doubled Johnson (doubled Odd) graph $J(2w+1,w,w+1)$ (the subgraph of $H(2w+1,2)$ induced by the words of weight w and $w+1$): the existence of such codes is equivalent to the existence of Steiner systems $S(w,w+1,2w+2)$; in particular, the Steiner quadruple system $S(3,4,8)$ and the small Witt design $S(5,6,12)$ [1], [32] correspond to nontrivial 1-perfect codes in $J(7,3,4)$ and $J(11,5,6)$; the nonexistence of Steiner systems $S(4,5,15)$ [21] and $S(4,5,17)$ [22] implies the nonexistence of 1-perfect codes in $J(19,9,10)$ and $J(23,11,12)$ (in general, the problem remains open, with the first open case in $J(31,15,16)$). In the Grassmann graphs $J_q(n,w)$ and the bilinear forms graphs $B_q(m,n)$, nontrivial perfect codes do not exist [2], see also [19]. Some perfect codes in dual polar graphs are discussed in [26, p.659], including the examples of 1-perfect codes found in [27] in graphs of diameter 3. Studying diameter-3 antipodal distance-regular graphs with 1-perfect codes (usually, with some assumptions on the graph automorphisms) is a separate topic, see [5], [16]–[18], [29]–[31].

The Doob graph $D(m,n)$ is the Cartesian product of m copies of the Shrikhande graph and n copies of the complete graph of order 4 (detailed definitions are given in the next section). It is a distance-regular graph of diameter $2m+n$ with the same parameters (intersection array) as the Hamming graph $H(2m+n,4)$. On the other hand, the vertices of the Doob graph can be naturally associated with the elements of the module $\mathrm{GR}(4^2)^m \times \mathbb{F}_4^n$ over the Galois ring $\mathrm{GR}(4^2)$ or with the elements of the module $\mathbb{Z}_4^{2m} \times \mathbb{Z}_2^{2n'} \times \mathbb{Z}_4^{n''}$ over $\mathbb{Z}_4$, where $n'+n''=n$. In this way, the Doob graph is a Cayley graph on the corresponding module. The submodules of the first module are called the linear codes in $D(m,n)$; the submodules of $\mathbb{Z}_4^{2m} \times \mathbb{Z}_2^{2n'} \times \mathbb{Z}_4^{n''}$ are called the additive codes in $D(m,n)$. The history of studying perfect codes in Doob graphs started from the paper [11], where it was shown that nontrivial e-perfect codes in $D(m,n)$ can only exist when $e=1$ and $2m+n=(4^k-1)/3$ for some

D. S. Krotov is with the Sobolev Institute of Mathematics, Novosibirsk 630090 Russia e-mail: krotov@math.nsc.ru

This work was funded by the Russian Science Foundation (18-11-00136).

The results of this work were presented in part at the Sixteenth International Workshop on Algebraic and Combinatorial Coding Theory, Svetlogorsk, Russia, 2–8 September 2018.

This is the accepted version of the paper published in the IEEE Transactions on Information Theory, 66:3 (2020), 1423–1427, https://doi.org/10.1109/TIT.2019.2946612

integer k and two 1-perfect codes, in $D(2,1)$ and $D(1,3)$, were constructed. In [13], infinite series of perfect codes in Doob graphs were obtained. In particular, it was shown that the necessary condition $2m+n=(4^k-1)/3$ is sufficient if $m<n-o(2m+n)$; the class of linear perfect codes was completely characterized; a class of additive perfect codes was constructed and necessary conditions on m, n', n'' for the existence of additive perfect codes in $D(m,n'+n'')$ were obtained (in a recent work [25], it was shown that those conditions are also sufficient).

II. Definitions

The Shrikhande graph Sh can be naturally defined on the pairs of elements from $\mathbb{Z}_4$. Two such pairs (x_1,x_2) and (y_1,y_2) are adjacent if their difference (x_1-y_1,x_2-y_2) is one of $(0,1)$, $(0,3)$, $(1,0)$, $(3,0)$, $(1,1)$, $(3,3)$ (so, Sh is a Cayley graph on $\mathbb{Z}_4^2$).

We will use two representations of the complete graph K_4. In the first one, $K_4(\mathbb{Z}_4)$, its vertices are the elements 0, 1, 2, 3 of $\mathbb{Z}_4$; in the second, $K_4(\mathbb{F}_4)$, the elements 0, 1, ξ, ξ^2 of the finite field $\mathbb{F}_4$ of order 4.

If m is even, then $D(m,n)$ will be considered as the Cartesian product of m copies of Sh and n copies of $K_4(\mathbb{F}_4)$ (in particular, $D(0,n)$ is the Hamming graph $H(n,4)$). If m is odd, then $D(m,n)$ will be considered as the Cartesian product of m copies of Sh, two copies of $K_4(\mathbb{Z}_4)$ and $n-2$ copies of $K_4(\mathbb{F}_4)$ (note that in the considered class of parameters, $6m+3n+1$ is a power of 4, so n is odd and $n=1$ implies even m). So, the vertex set is the set of words of length $2m+n$ from $(\mathbb{Z}_4^2)^m\times\mathbb{F}_4^n$ or $(\mathbb{Z}_4^2)^m\times\mathbb{Z}_4^2\times\mathbb{F}_4^{n-2}$, and two vertices are adjacent if their coordinatewise difference has exactly one non-zero position i, $i>2m$, or exactly one non-zero position i, $i\le 2m$, with value 1 or 3, or exactly two nonzero positions $2i-1$, $2i$, where $i\in\{1,\dots,m\}$, with values $1,1$ or $3,3$.

The distance between two vertices $\bar x$ and $\bar y$ of $D(m,n)$ (as well as in any other connected graph) is defined as the number of edges in the shortest path connecting $\bar x$ and $\bar y$. Equivalently, the distance is equal to the sum of distances between the corresponding components of $\bar x$ and $\bar y$: m Shrikhande components and n K_4-components. The distance form some vertex $\bar x$ of $D(m,n)$ to the all-zero vertex of $D(m,n)$ is referred to as the weight of $\bar x$.

In any graph, an e-perfect code is defined as a set of vertices such that every ball of radius e contains exactly one code vertex. We define a 1-perfect Hamming code $\mathcal{H}$ in $H(n,4)$, $n=(4^k-1)/3$, by the check matrix consisting of all columns of height k whose first nonzero element is 1. To be explicit, we require the columns to be inverse-lexicographically ordered, for example ($k=3$),

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0\\ \xi^2 & \xi^2 & \xi^2 & \xi^2 & \xi & \xi & \xi & \xi & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0\\ \xi^2 & \xi & 1 & 0 & \xi^2 & \xi & 1 & 0 & \xi^2 & \xi & 1 & 0 & \xi^2 & \xi & 1 & 0 & \xi^2 & \xi & 1 & 0 & 1 \end{bmatrix}.$$

III. Construction

The approach of the construction for 1-perfect codes in $D(m,n)$ is partially similar to that of [11] for tight 2-designs (the codes formally dual to 1-perfect). We start with the Hamming code $\mathcal{H}$ over $\mathbb{F}_4$ in $H(2m+n,4)$ and replace subwords of length 4 corresponding to the positions $4i-3$, $4i-2$, $4i-1$, $4i$ of the codewords by subwords of length 4 over $\mathbb{Z}_4$, treated as elements of $D(2,0)$ if $i\le[m/2]$ or $D(1,2)$ if $i=(m+1)/2$.

In details, there are some differences with the construction in [11]. For the code dual to $\mathcal{H}$, there are only 16 possibilities for subwords in the considered quadruples of coordinates, and the substitution function used in [11] is an isometry from the corresponding subcode in $H(4,4)$ into $D(2,0)$ ($D(1,2)$). In our case, all 256 possible length-4 words occur as subwords, and there is no such isometry (indeed, the graphs $H(4,4)$, $D(1,2)$, $D(2,0)$ are not isomorphic). However, for the resulting code being 1-perfect, we need not control the distance between any two codewords; it is sufficient only to ensure that this distance cannot be 1 or 2. To do this, we construct the substitution bijection between $H(4,4)$ and $D(2,0)$ ($D(1,2)$) using the principles of the generalized concatenated construction [34]. It occurs that the resulting construction is close to a variant of the generalized concatenated construction for 1-perfect codes in $H(n,q)$ presented in [23].

A. Codes in $D(1,2)$, $D(2,0)$ and $H(4,4)$.

To construct a substitution function with the desired properties, in each of the graphs $D(1,2)$, $D(2,0)$, $H(4,4)$, we need two additive codes, of distance 3 and 2 and cardinality 16 and 64, respectively.

Lemma 1. *Denote*

$$\begin{aligned}\bar x=(0,1,2,3),\ \bar y=(1,0,1,2)&\in\mathbb{Z}_4^4;\\ \bar z=(0,0,1,1)&\in\mathbb{Z}_4^4;\\ \bar u=(0,0,0,2),\ \bar v=(0,0,2,0)&\in\mathbb{Z}_4^4;\\ \bar x'=(1,1,1,1),\ \bar y'=(0,1,\xi,\xi^2)&\in\mathbb{F}_4^4;\\ \bar z'=(0,0,1,1)&\in\mathbb{F}_4^4.\end{aligned}$$

Define

$$\begin{aligned} C''&=\langle\bar x,\bar y\rangle, & C'&=\langle\bar x,\bar y,\bar z\rangle;\\ D''&=\langle\bar x,\bar y\rangle, & D'&=\langle\bar x,\bar y,\bar u,\bar v\rangle;\\ E''&=\langle\bar x',\bar y'\rangle, & E'&=\langle\bar x',\bar y',\bar z'\rangle.\end{aligned}$$

We state that

(a) $C''\subset C'$, $D''\subset D'$, $E''\subset E'$;
(b) C', D', E' *are distance-*2 *codes of cardinality* 64 *in* $D(1,2)$, $D(2,0)$, $H(4,4)$, *respectively;*
(c) C'', D'', E'' *are distance-*3 *codes of cardinality* 16 *in* $D(1,2)$, $D(2,0)$, $H(4,4)$, *respectively.*

Proof. We note that since the considered codes are closed under addition, the code distance coincides with the minimum nonzero weight of a codeword.

(a) is trivial.

(b). Every codeword of C' is orthogonal to $(1,1,1,3)$, as this is true for $\bar x$, $\bar y$, and $\bar z$. It is easy to check that each of the 12 words $(0,0,0,1)$, $(0,0,0,2)$, $(0,0,0,3)$, $(0,0,1,0)$, $(0,0,2,0)$, $(0,0,3,0)$, $(0,1,0,0)$, $(0,3,0,0)$, $(1,0,0,0)$, $(3,0,0,0)$, $(1,1,0,0)$, $(3,3,0,0)$ of weight 1 in $D(1,2)$ is not orthogonal to $(1,1,1,3)$. Hence, C' does not contain weight-1 words and has code distance larger than 1. The cardinality of C' is $4\cdot4\cdot4$, as $\bar x$, $\bar y$, $\bar z$ are linearly independent.

Each codeword of D' is orthogonal to both $(0,2,0,2)$ and $(2,0,2,0)$, while this is not true for each of the 12 weight-1 words $(0,0,0,1)$, $(0,0,0,3)$, $(0,0,1,0)$, $(0,0,3,0)$, $(0,0,1,1)$, $(0,0,3,3)$, $(0,1,0,0)$, $(0,3,0,0)$, $(1,0,0,0)$, $(3,0,0,0)$, $(1,1,0,0)$, $(3,3,0,0)$ in $D(2,0)$. Hence, D' does not contain weight-1 words and has code distance larger than 1. Since D' is spanned by independent elements of order 4, 4, 2, and 2, its cardinality is $4 \cdot 4 \cdot 2 \cdot 2$.

Similar arguments work for E', orthogonal to $(1,1,1,1)$.

(c). Each of C'', D'', E'' is the span of two linearly independent words of order 4, so the cardinality is 16 in each case. Next, it is easy to see that each of the 15 nontrivial linear combinations of $\bar{x}'$ and $\bar{y}'$ has at most one zero symbol; so, the minimum weight (and hence the code distance) of E'' is 3. For the codes C'' and D'', the minimum weight (in $D(1,2)$ and $D(2,0)$, respectively) can be easily found from the complete list of codewords:

$$\begin{aligned} C'' = D'' = \{&(0,0,0,0),\ (0,1,2,3),\ (0,2,0,2),\ (0,3,2,1),\\ &(1,0,1,2),\ (1,1,3,1),\ (1,2,1,0),\ (1,3,3,3),\\ &(2,0,2,0),\ (2,1,0,3),\ (2,2,2,2),\ (2,3,0,1),\\ &(3,0,3,2),\ (3,1,1,1),\ (3,2,3,0),\ (3,3,1,3)\}. \end{aligned}$$

□

Lemma 2. *Let $\bar{c} = (c_1, \ldots, c_n)$ be a codeword of the Hamming code $\mathcal{H}$, and let $\bar{e} = (e_1, e_2, e_3, e_4)$ be a codeword of the code E'' defined in Lemma 1. Then for every j, $0 \le j < (n-1)/4$, the word $\bar{b} = (b_1, \ldots, b_n)$ whose components are*

$$b_i = \begin{cases} c_i + e_{i-4j} & \text{if } i \in \{4j+1, 4j+2, 4j+3, 4j+4\}, \\ c_i & \text{otherwise} \end{cases}$$

is also a codeword of $\mathcal{H}$.

Proof. It is sufficient to prove the statement for the case when $\bar{c}$ is the all-zero word.

For the all-zero $\bar{c}$, the word $\bar{b}$ has the form $(0, \ldots, 0, e_1, e_2, e_3, e_4, 0, \ldots, 0)$, and its syndrome $P\bar{b}$ coincides with $P_{(4j+1,4j+2,4j+3,4j+4)}\bar{e}$, where the matrix $P_{(4j+1,4j+2,4j+3,4j+4)}$ is composed from the four corresponding columns of P. By the construction of P (recall, it consists of all different columns whose first nonzero element is 1 placed in the inverse lexicographical order), the considered submatrix has the last row $(\xi^2, \xi, 1, 0)$, while the other rows are multiples of $(1,1,1,1)$. From the definition of the code E'' in Lemma 1, we see that its codewords are orthogonal to both $(\xi^2, \xi, 1, 0)$ as $(1,1,1,1)$ (indeed, this is true for the base codewords $\bar{x}'$ and $\bar{y}'$). It follows that $P_{(4j+1,4j+2,4j+3,4j+4)}\bar{e} = \bar{0}$ and, hence, $P\bar{b} = \bar{0}$. That is, $\bar{b}$ belongs to $\mathcal{H}$. □

Lemma 3. *For every two cosets C''_1, C''_2 of C'' that are not subsets of the same coset of C', for every $\bar{x}$ from C''_1, there is $\bar{y}$ from C''_2 at distance 1 from $\bar{x}$. The same holds for the cosets of D'' that are not in one coset of D' and for the cosets of E'' that are not in one coset of E'.*

Proof. The statement is proven by the following counting argument. The word $\bar{x}$ has exactly 12 neighbors. Two neighbors cannot belong to the same coset of C'', because C'' is distance-3. No one of these 12 neighbors belongs to the same coset of C' as $\bar{x}$, because C' is distance-2. Since there are 16 cosets of C'' and 4 of them are subsets of the same coset of C' containing $\bar{x}$, each of the remaining 12 cosets contains exactly one neighbor of $\bar{x}$. □

B. Main theorem

For the construction, we need two maps, ϕ and ψ. The bijective map ϕ between the vertex sets of $H(4,4)$ and $D(2,0)$ is required to satisfy the following conditions:

(a) $\bar{a}$ and $\bar{b}$ belong to the same coset of E'' if and only if $\phi(\bar{a})$ and $\phi(\bar{b})$ belong to the same coset of D'';
(b) $\bar{a}$ and $\bar{b}$ belong to the same coset of E' if and only if $\phi(\bar{a})$ and $\phi(\bar{b})$ belong to the same coset of D'.

To construct ϕ, we represent each of the 256 vertices of $H(4,4)$ as $\bar{e}'_i + \bar{e}''_j + \bar{e}'''_k$, $i,j \in \{0,1,2,3\}$, $k \in \{0, \ldots, 15\}$, where

- $\bar{e}'_0$, $\bar{e}'_1$, $\bar{e}'_2$, $\bar{e}'_3$ are representatives of the four cosets of E';
- $\bar{e}''_0$, $\bar{e}''_1$, $\bar{e}''_2$, $\bar{e}''_3$ are representatives of the four cosets of E'' in E';
- $E'' = \{\bar{e}'''_0, \ldots, \bar{e}'''_{15}\}$.

Now, the bijection ϕ is defined by

$$\phi(\bar{e}'_i + \bar{e}''_j + \bar{e}'''_k) = \bar{d}'_i + \bar{d}''_j + \bar{d}'''_k$$

for every i from $\{0,1,2,3\}$, every j from $\{0,1,2,3\}$, and every k from $\{0, \ldots, 15\}$. In a similar manner, each of the 256 vertices of $D(2,0)$ is represented as $\bar{d}'_i + \bar{d}''_j + \bar{d}'''_k$, $i,j \in \{0,1,2,3\}$, $k \in \{0, \ldots, 15\}$, where

- $\bar{d}'_0$, $\bar{d}'_1$, $\bar{d}'_2$, $\bar{d}'_3$ are representatives of the four cosets of D';
- $\bar{d}''_0$, $\bar{d}''_1$, $\bar{d}''_2$, $\bar{d}''_3$ are representatives of the four cosets of D'' in D';
- $D'' = \{\bar{d}'''_0, \ldots, \bar{d}'''_{15}\}$.

The bijective map ψ between the vertex sets of $H(4,4)$ and $D(1,2)$ is constructed similarly, involving the cosets of C' and C'', and satisfies the following conditions:

(c) $\bar{a}$ and $\bar{b}$ belong to the same coset of E'' if and only if $\psi(\bar{a})$ and $\psi(\bar{b})$ belong to the same coset of C'';
(d) $\bar{a}$ and $\bar{b}$ belong to the same coset of E' if and only if $\psi(\bar{a})$ and $\psi(\bar{b})$ belong to the same coset of C'.

Theorem 1. *Let $\mathcal{H}$ be the Hamming code in $H((4^k-1)/3, 4)$ whose check matrix consists of all columns with first nonzero element 1, in the inverse lexicographical order. Let the codes E'', E' in $H(4,4)$, the codes C'', C' in $D(1,2)$, the codes D'', D' in $D(2,0)$ be defined as in Lemma 1. Let ϕ and ψ be bijective maps from the vertex set of $H(4,4)$ to the vertex sets of $D(2,0)$ and $D(1,2)$, respectively, satisfying conditions (a), (b) and (c), (d) above. Let m and n be positive integers such that $2m+n = (4^k-1)/3$. If m is even, then*

$$\begin{aligned} \mathcal{C} = \Big\{ &\big(\phi(x_1, ..., x_4), \ldots, \phi(x_{2m-3}, ..., x_{2m}), \\ &x_{2m+1}, \ldots, x_{2m+n}\big) : \\ &(x_1, \ldots, x_{2m+n}) \in \mathcal{H} \Big\} \end{aligned}$$

is a 1*-perfect code in* $D(m,n)$*. If* m *is odd, then*

$$\mathcal{C} = \Big\{ \big(\phi(x_1,...,x_4),\dots,\phi(x_{2m-5},...,x_{2m-2}), \psi(x_{2m-1},...,x_{2m+2}),x_{2m+1},\dots,x_{2m+n}\big) : (x_1,\dots,x_{2m+n}) \in \mathcal{H}\Big\}$$

is a 1*-perfect code in* $D(m,n)$*.*

Proof. We will consider the case when m is even; the odd case is similar. Assume the receiver get a word $\bar{y} = (y_1,\dots,y_{2m+n}) \in \mathbb{Z}_4^{2m} \times \mathbb{F}_4^n$, associated with a vertex of $D(m,n)$. To decode the message under the assumption that an error of weight at most 1 occurred, one should find a codeword $\bar{c}$ at distance at most 1 from $\bar{y}$. Consider

$$\bar{x} = \big(\phi^{-1}(y_1,y_2),\dots,\phi^{-1}(y_{2m-1},y_{2m}),y_{2m+1},\dots,y_{2m+n}\big) \in {\mathbb{F}_4}^{2m+n}.$$

If $\bar{x}$ is a codeword of $\mathcal{H}$, then, by the definition of $\mathcal{C}$, we have $\bar{c} = \bar{y} \in \mathcal{C}$. Assume that $\bar{x} \notin \mathcal{H}$. Since $\mathcal{H}$ is a 1-perfect code, there is $\bar{b} = (b_1,\dots,b_{2m+n}) \in \mathcal{H}$ at distance 1 from $\bar{x}$. We consider the codeword $\bar{z} \in \mathcal{C}$ defined as

$$\begin{aligned}\bar{z} &= (z_1,\dots,z_{2m+n})\\ &= \big(\phi(b_1,b_2,b_3,b_4),\dots,\phi(b_{2m-3},...,b_{2m}),b_{2m+1},\dots,b_{2m+n}\big).\end{aligned}$$

Note that $\bar{z}$ is not necessarily the required $\bar{c}$. However, we can state the following.

(i) *If* $\bar{b}$ *differs from* $\bar{x}$ *in one of the last* n *coordinates, then* $\bar{z}$ *and* $\bar{y}$ *differ in exactly one, the same as* $\bar{b}$ *and* $\bar{x}$*, coordinate; so,* $\bar{c} = \bar{z}$ *in this case.* Indeed, $\bar{z}$ and $\bar{y}$ trivially coincide in the other coordinates.

(ii) *If* $\bar{b}$ *differs from* $\bar{x}$ *in one of the first* $2m$ *coordinates, say,* $(b_{4i-3},b_{4i-2},b_{4i-1},b_{4i}) \neq (x_{4i-3},x_{4i-2},x_{4i-1},x_{4i})$*, then there is* $(c_{4i-3},c_{4i-2},c_{4i-1},c_{4i}) \in \mathbb{Z}_4^4$ *in the same coset of* D'' *as* $(z_{4i-3},z_{4i-2},z_{4i-1},z_{4i})$ *such that*

$$\bar{c} = (z_1,\dots,z_{4i-4},c_{4i-3},c_{4i-2},c_{4i-1},c_{4i},z_{4i+1},\dots,z_{2m+n})$$

at distance 1 *from* $\bar{y}$*. Moreover,* $\bar{c}$ *is a codeword of* $\mathcal{C}$*.* Indeed, the first part of the claim is straightforward from Lemma 3 and the definition of the map ϕ. From Lemma 2 and the construction of $\mathcal{C}$, we have $\bar{c} \in \mathcal{C}$.

In any case, there is a codeword $\bar{c} \in \mathcal{C}$ at distance at most 1 from $\bar{y}$. From standard counting arguments (the size of the space equals the size of the code multiplied by the size of a radius-1 ball), we see that such a codeword is unique. Therefore, the code is 1-perfect. □

So, if there is a 1-perfect code in a 4-ary Hamming graph, then there is a 1-perfect code in every Doob graph of the same diameter.

Corollary 1. *The Doob graph* $D(m,n)$ *has a non-trivial* e*-perfect code if and only if* $e = 1$ *and there is a positive integer* k *such that* $2m + n = (4^k - 1)/3$*.*

Proof. The "if" and "only if" parts of the statement come from Theorem 1 and [11, Theorem 3], respectively. □

IV. Concluding remarks

In this section we briefly discuss some related questions, including those suggested by the reviewers.

Remark 1 (Unrestricted 1-perfect codes vs additive 1-perfect codes)**.** For every Doob graph $D(m,n)$ that satisfies the obvious ball-packing necessary condition on the existence of 1-perfect codes, we can construct such a code by Theorem 1. In general, the code constructed is not linear or even additive (closed with respect to addition). Moreover, as was shown in [13, Theorem 1], the existence of additive 1-perfect codes implies additional conditions on the parameters m and n. Namely,

$$\begin{aligned} 2m + n &= (2^{\Gamma+2\Delta} - 1)/3,\\ 3n &= 2^{\Gamma+\Delta} - 1 - 2n'',\\ 1 \neq n'' &\leq 2^{\Delta} - 1 \end{aligned} \tag{1}$$

for some nonnegative integer Γ, Δ, n''. Examples of Doob graphs for which additive 1-perfect codes do not exist, while unrestricted 1-perfect codes can be constructed by Theorem 1, are $D(6,9)$, $D(9,3)$, $D(10,1)$. As can be seen from the proof of the theorem, we do not need additivity to have a good decoding algorithm. Indeed, decoding the constructed code in the Doob graph is not more complicate than decoding the original 4-ary Hamming code of length $2m+n$; all additional operations (mainly, applying ϕ and ϕ^{-1}) take $o(2m+n)$ time.

Remark 2 (dual codes)**.** The codes formally dual to the 1-perfect codes are known as simplex codes or tight 2-designs (the formal duality of two codes means that the MacWilliams transform of the distance distribution of one code gives the distance distribution of the other code). A *simplex code* in a Hamming graph $H(N,q)$ or a Doob graph $D(m,n)$ has $N(q-1)+1$ codewords at mutual distance $(N(q-1)+1)/q$ from each other (for $D(m,n)$, we put $N = 2m+n$ and $q = 4$). In every $D(m,n)$ such that $2m + n = (4^k - 1)/3$ for some k, simplex codes were constructed in [11]. So, it is safe to say that for every 1-perfect code C in a Doob graph there is a simplex code (tight 2-design) that is formally dual to C. However, to treat duality in the usual sense, as a duality between two submodules, we need additive codes (note that the duality should be defined in a special way to be compatible with the MacWilliams transform, see [14]). Since additive 1-perfect codes (and hence, additive simplex codes) exist only if the parameters satisfy the additional conditions (1), for any other parameters meeting $2m + n = (4^k - 1)/3$ the class of 1-perfect codes is connected with the class of simplex codes only in the way of formal duality (there is still a challenge in finding a more strict connection, as was done, for example, in [8] for the formally dual classes of Preparata-like codes and Kerdock-like codes). It should also be noted that the parameters of simplex codes (tight 2-designs) are not proven to be restricted by the case $2m + n = (4^k - 1)/3$ only. The problem of existence of simplex codes for other parameters is open for Doob graphs, as well as for Hamming graphs, where the most attempts are focused on the binary case (see the Hadamard conjecture).

Remark 3 (from $H(2m+n,4)$ to $D(m,n)$)**.** To solve the problem of parameters of perfect codes in Doob graphs, we apply the strategy of "switching" between the graphs $D(m,n)$

and $H(2m+n,4)$ by transforming the Shrikhande components of the Cartesian product, in groups of one or two, to Hamming (K_4) components. This general approach is not new and was applied for different purposes before; however, the realizations depend on concrete problems. In [11], isometries between special vertex sets in $H(4,4)$, $D(1,2)$, and $D(2,0)$ were used to construct a simplex code in a Doob graph from a special (not arbitrary) simplex code in a Hamming graph. In [12], any maximum independent set in a Doob graph is mapped to a maximum independent set (unrestricted distance-2 MDS code) in the corresponding Hamming graph; again, the map is constructed based on a map in the smallest case, from $D(1,0)$ to $H(2,4)$, but the map is set-to-set and cannot be treated in a point-wise manner. In the current paper, we use point-to-point maps ϕ and ψ that preserve some metrical properties of a special coset partition in $H(4,4)$ to construct perfect codes in Doob graphs from a special Hamming code (we cannot apply the same maps to an arbitrary 1-perfect code or even to an equivalent Hamming code because we need to control which subcodes occur in subsequent groups of coordinates). As shown in [15], one can obtain $D(m,n)$ from $H(2m+n,4)$ by a sequence of m Godsil–McKay switchings, each switching replacing one Shrikhande component in the Cartesian product by two K_4-components. Godsil–McKay switching can be treated as a bigective map between the vertex set of two graphs, and it is also induces, in an algebraic way, an isomorphism between eigenspaces of the graphs with the same eigenvalues (so the graphs related by Godsil–McKay switching are always cospectral). However, it obviously changes the distances between some vertices, and so cannot serve the purpose of constructing error-correcting codes in a straightforward way. It is still a very interesting question if some bijections ϕ and ψ with the desired properties (Section III-B) can be treated as a combination of Godsil–McKay switchings, but even if they can, this would hardly simplify the construction or its proof.

[1] R. D. Carmichael, "Configurations of rank two," *Am. J. Math.*, vol. 53, no. 1, pp. 217–240, 1931, DOI: 10.2307/2370885.

[2] L. Chihara, "On the zeros of the Askey–Wilson polynomials, with applications to coding theory," *SIAM J. Math. Anal.*, vol. 18, no. 1, pp. 191–207, 1987, DOI: 10.1137/0518015.

[3] P. Delsarte, *An Algebraic Approach to Association Schemes of Coding Theory*, ser. Philips Res. Rep., Supplement, vol. 10, 1973.

[4] T. Etzion, "Configuration distribution and designs of codes in the Johnson scheme," *J. Comb. Des.*, vol. 15, no. 1, pp. 15–34, 2007, DOI: 10.1002/jcd.20102.

[5] C. D. Godsil, R. A. Liebler, and C. E. Praeger, "Antipodal distance transitive covers of complete graphs," *Eur. J. Comb.*, vol. 19, no. 4, pp. 455–478, May 1998, DOI: 10.1006/eujc.1997.0190.

[6] M. J. E. Golay, "Notes on digital coding," *Proc. IRE*, vol. 37, no. 6, p. 657, 1949, DOI: 10.1109/JRPROC.1949.233620.

[7] D. M. Gordon, "Perfect single error-correcting codes in the Johnson scheme," *IEEE Trans. Inf. Theory*, vol. 52, no. 10, pp. 4670–4672, 2006, DOI: 10.1109/TIT.2006.881744.

[8] A. R. Hammons, Jr, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, "The Z_4-linearity of Kerdock, Preparata, Goethals, and related codes," *IEEE Trans. Inf. Theory*, vol. 40, no. 2, pp. 301–319, 1994, DOI: 10.1109/18.312154.

[9] O. Heden, "On perfect codes over non prime power alphabets," in *Error-Correcting Codes, Finite Geometries and Cryptography*, ser. Contemp. Math., A. A. Bruen and D. L. Wehlau, Eds. AMS, 2010, vol. 523, pp. 173–184.

[10] K. Huber, "Codes over Eisenstein–Jacobi integers," in *Finite Fields: Theory, Applications, and Algorithms (Las Vegas, NV, 1993)*, ser. Contemp. Math., vol. 168. Providence, RI: Amer. Math. Soc., 1994, pp. 165–179.

[11] J. H. Koolen and A. Munemasa, "Tight 2-designs and perfect 1-codes in Doob graphs," *J. Stat. Plann. Inference*, vol. 86, no. 2, pp. 505–513, 2000, DOI: 10.1016/S0378-3758(99)00126-3.

[12] D. S. Krotov, "On the number of maximum independent sets in Doob graphs," *Sib. Èlektron. Mat. Izv.*, vol. 12, pp. 508–812, 2015, DOI: 10.17377/semi.2015.12.043.

[13] D. S. Krotov, "Perfect codes in Doob graphs," *Des. Codes Cryptography*, vol. 80, no. 1, pp. 91–102, July 2016, DOI: 10.1007/s10623-015-0066-6.

[14] D. S. Krotov, "On dual codes in the Doob schemes," in *IEEE International Symposium on Information Theory, Paris, France, July 7–12, 2019*. IEEE, 2019, pp. 1917–1921, DOI: 10.1109/ISIT.2019.8849850.

[15] S. Kubota, "Unification of graph products and compatibility with switching," *Graphs Comb.*, vol. 33, no. 5, pp. 1347–1355, Sept. 2017, DOI: 10.1007/s00373-017-1848-6.

[16] A. A. Makhnev, D. V. Paduchikh, and L. Y. Tsiovkina, "Edge-symmetric distance-regular coverings of cliques: The affine case," *Sib. Math. J.*, vol. 54, no. 6, pp. 1076–1087, Nov 2013, DOI: 10.1134/S0037446613060141.

[17] A. A. Makhnev, D. V. Paduchikh, and L. Y. Tsiovkina, "Arc-transitive distance-regular covers of cliques with $\lambda = \mu$," *Proc. Steklov Inst. Math.*, vol. 284, no. Suppl.1, pp. 124–134, Apr. 2014, DOI: 10.1134/S0081543814020114.

[18] A. A. Makhnev, D. V. Paduchikh, and L. Y. Tsiovkina, "Edge-symmetric distance-regular coverings of complete graphs: the almost simple case," *Algebra Logic*, vol. 57, no. 2, pp. 141–152, June 2018, DOI: 10.1007/s10469-018-9486-5.

[19] W. J. Martin and X. J. Zhu, "Anticodes for the Grassman and bilinear forms graphs," *Des. Codes Cryptography*, vol. 6, no. 1, pp. 73–79, 1995, DOI: 10.1007/BF01390772.

[20] C. Martínez, E. Stafford, R. Beivide, and E. M. Gabidulin, "Modeling hexagonal constellations with Eisenstein–Jacobi graphs," *Probl. Inf. Transm.*, vol. 44, no. 1, pp. 1–11, 2008, DOI: 10.1134/S0032946008010018 Translated from Probl. Peredachi Inf. 44:1 (2008), 3–14.

[21] N. S. Mendelsohn and S. H. Y. Hung, "On the Steiner systems $S(3,4,14)$ and $S(4,5,15)$," *Util. Math.*, pp. 5–95, 1972.

[22] P. R. J. Östergård and O. Pottonen, "There exists no Steiner system $S(4,5,17)$," *J. Comb. Theory, Ser. A*, vol. 115, no. 8, pp. 1570–1573, Nov. 2008, DOI: 10.1016/j.jcta.2008.04.005.

[23] A. M. Romanov, "A generalized concatenation construction for q-ary 1-perfect codes," arXiv:1711.00189 [Update: "On perfect and Reed–Muller codes over finite fields," *Probl. Inf. Transm.*, vol. 57, no. 3, pp. 199–211, 2021, DOI: 10.1134/S0032946021030017, translated from Probl. Peredachi Inf. 57:3 (2021), 3-16.]

[24] M. Shi, A. Alahmadi, and P. Solé, *Codes and Rings: Theory and Priactice*, ser. Pure and Applied Mathematics. Academic Press, 2017.

[25] M. Shi, D. Huang, and D. S. Krotov, "Additive perfect codes in Doob graphs," *Des. Codes Cryptography*, vol. 87, no. 8, pp. 1857–1869, Aug. 2019, DOI: 10.1007/s10623-018-0586-y.

[26] D. Stanton, "Some q-Krawtchouk polynomials on Chevalley groups," *Am. J. Math.*, vol. 10, no. 4, pp. 625–662, Aug. 1980, DOI: 10.2307/2374091.

[27] J. Thas, "Two infinite classes of perfect codes in metrically regular graphs," *J. Comb. Theory, Ser. B*, vol. 23, pp. 236–238, 1977.

[28] A. Tietäväinen, "On the nonexistence of perfect codes over finite fields," *SIAM J. Appl. Math.*, vol. 24, no. 1, pp. 88–96, 1973, DOI: 10.1137/0124010.

[29] L. Y. Tsiovkina, "On affine distance-regular covers of complete graphs," *Sib. Èlektron. Mat. Izv.*, vol. 12, pp. 998–1005, 2015, DOI: 10.17377/semi.2015.12.086.

[30] L. Y. Tsiovkina, "Two new infinite families of arc-transitive antipodal distance-regular graphs of diameter three with $\lambda = \mu$ related to groups $Sz(q)$ and ${}^2g_2(q)$," *J. Algebr. Comb.*, vol. 41, no. 4, pp. 1079–1087, June 2015, DOI: 10.1007/s10801-014-0566-x.

[31] L. Y. Tsiovkina, "Arc-transitive antipodal distance-regular covers of complete graphs related to $SU_3(q)$," *Discrete Math.*, vol. 340, no. 2, pp. 63–71, Feb. 2017, DOI: 10.1016/j.disc.2016.08.001.

[32] V. E. Witt, "Über Steinersche systeme," *Abh. Math. Semin. Univ. Hamb.*, vol. 12, no. 1, pp. 265–275, 1937, DOI: 10.1007/BF02948948.

[33] V. Zinoviev and V. Leontiev, "The nonexistence of perfect codes over Galois fields," *Probl. Control Inf. Theory*, vol. 2, no. 2, pp. 123–132, 16–24[Engl. transl.], 1973.

[34] V. A. Zinoviev, "Generalized concatenated codes," *Probl. Inf. Transm.*, vol. 12, no. 1, pp. 2–9, 1976, translated from *Probl. Peredachi Inf.*, 12(1): 5-15, 1976.