ON THE LENGTHS OF MDS CODES WITH A TWO-TRANSITIVE PERMUTATION AUTOMORPHISM GROUP

HAIHUA DENG, TAO FENG, ANDREY V. VASIL'EV

Abstract. Let C be an $[n,k]_q$ maximum distance separable (MDS) code with $4 \le k \le q-3$, and suppose that it has a 2-transitive permutation automorphism group. In this paper we show that $n \le q+1$, so the MDS conjecture holds for this class of codes.

1. Introduction

Let q be a prime power, and let $\mathbb{F}_q$ be the finite field with q elements. An $[n,k,d]_q$ code C is a k-dimensional subspace of $\mathbb{F}_q^n$ with minimum Hamming distance d. If d is unspecified, we refer to C as an $[n,k]_q$ code. If $2 \le k \le n-2$, then we call the code C *nontrivial*. We say that it is a *maximum distance separable* (MDS) code if it attains equality in the Singleton bound, i.e., $d = n-k+1$ [42]. The MDS conjecture, which we state below, is a fundamental and long-standing problem in coding theory.

Conjecture 1.1. *Let C be a nontrivial $[n,k]_q$ MDS code. Then $n \le q+1$, except when q is even and $k \in \{3, q-1\}$, in which case $n \le q+2$.*

The MDS conjecture has its roots in a statistical problem discussed in 1952 by Bush in [11]. Segre started the influential geometric approach to this problem in [41], which was widely adopted and eventually led to the breakthrough of Ball [1] in 2012. We give a brief description of the relation with finite geometry as follows. Let C be an $[n,k]_q$ MDS code with $k \ge 2$, and let $\mathrm{PG}(k-1,q)$ be the projective space whose points are the one-dimensional subspaces of $\mathbb{F}_q^k$. Let M be a generator matrix of C, and let $\mathcal{M}$ be the set of n projective points corresponding to the column vectors of M. It is well known that any k column vectors of M are linearly independent, cf. [26] or [35]. It follows that any k points of $\mathcal{M}$ do not lie on a hyperplane, i.e., $\mathcal{M}$ is a n-arc of $\mathrm{PG}(k-1,q)$. Conversely, every n-arc gives rise to an $[n,k]_q$ MDS code, cf. [22]. Segre [41] associated an algebraic curve to an n-arc, and this perspective led to important progress towards the MDS conjecture by using deep tools from algebraic geometry, cf. [6, 7, 44, 43, 20, 21]. For an exposition of geometric techniques and recent progress on the MDS conjecture, we refer the reader to the comprehensive survey [2].

The permutation automorphism group $\mathrm{PAut}(C)$ of a code C (see Section 2 for definition), referred to as the permutation group of C for short, is an important research topic in coding theory. MacWilliams explored $\mathrm{PAut}(C)$ to develop efficient permutation decoding algorithms [34], and the same idea has recently been developed into automorphism ensemble decoding for Reed–Muller codes [17]. In 2012 Kaufman and Lubotzky [27] constructed the first family

2020 *Mathematics Subject Classification.* Primary 94B05, 20B20, 20C20; Secondary 94B65, 05B25.

Key words and phrases. MDS code, MDS conjecture, permutation automorphism group, 2-transitive group.

of asymptotically good symmetric LDPC codes, where a code C of length n is symmetric if $\mathrm{PAut}(C)$ is transitive on the n coordinate positions. The extremal self-dual codes over small fields with 2-transitive permutation groups have been studied in [36, 13]. We refer to [30, 29, 39] for group-based constructions of linear codes, [5, 16, 18, 33] for recent progress on the permutation groups of cyclic codes, and refer to [25] for a detailed description of the relation between codes and groups.

In this paper, we initiate the study of the length of an MDS code C with large transitive permutation group $\mathrm{PAut}(C)$. We list the known MDS codes with a 2-transitive permutation group as follows; a complete classification of such codes is still unavailable.

Example 1.2.

(1) *The repetition code J of length n over $\mathbb{F}_q$ spanned by the all-1 vector is an $[n,1,n]_q$ code; the code $A = J^\perp$ is an $[n,n-1,2]_q$ code, and the whole space $\mathbb{F}_q^n$ is an $[n,n,1]_q$ code. They are all trivial MDS codes with permutation automorphism group $\mathrm{Sym}(n)$.*

(2) *Let $\mathbb{F}_r \subseteq \mathbb{F}_q$ and $1 \le k \le r$. We define*

$$\mathrm{RS}_{r,k}(\mathbb{F}_q) = \left\{ (f(x))_{x\in\mathbb{F}_r} : f \in \mathbb{F}_q[X],\ \deg f < k \right\}.$$

This is an $[r,k,r-k+1]_q$ MDS code, and $\mathrm{AGL}_1(r) \le \mathrm{PAut}(C)$ acts 2-transitively on the set $\mathbb{F}_r$ of coordinate positions.

(3) *Let $r = 2^h$, $\mathbb{F}_r \subseteq \mathbb{F}_q$, and take $1 \le e < h$ and $\gcd(e,h) = 1$. Let*

$$\mathcal{T}_e(r) = \left\langle (1)_{x\in\mathbb{F}_r}, (x)_{x\in\mathbb{F}_r}, (x^{2^e})_{x\in\mathbb{F}_r} \right\rangle_{\mathbb{F}_q} \le \mathbb{F}_q^r,$$

and for $r \ge 8$ let

$$\mathcal{B}_e(r) = \left\langle (1)_{x\in\mathbb{F}_r}, (x)_{x\in\mathbb{F}_r}, (x^{2^e})_{x\in\mathbb{F}_r}, (x^{2^e+1})_{x\in\mathbb{F}_r} \right\rangle_{\mathbb{F}_q} \le \mathbb{F}_q^r.$$

Then $\mathcal{T}_e(r)$ and $\mathcal{B}_e(r)$ are $[r,3,r-2]_q$ and $[r,4,r-3]_q$ MDS codes respectively. The group $\mathrm{AGL}_1(r)$ acts 2-transitively on the set $\mathbb{F}_r$ of coordinate positions. These codes arise from a translation hyperoval and Segre's $(r+1)$-arc respectively, cf. [2, Examples 4.1 and 4.2]. *If $e = 2$ and $\gcd(e,h) = 1$, Berger showed that the dual of $\mathcal{T}_2(r)$ is an affine-invariant MDS code not equivalent to Reed–Solomon codes* [4].

(4) *Let $\mathcal{H}_6$ be the $[6,3,4]_4$ hexacode. If $\mathbb{F}_4 \subseteq \mathbb{F}_q$, then the $\mathbb{F}_q$-span of all its codewords is a $[6,3,4]_q$ MDS code. Its permutation automorphism group contains $\mathrm{PSL}_2(5) \cong A_5$, which is 2-transitive on the 6 coordinate positions.*

Our main result in this paper is the following theorem.

Theorem 1.3. *Let C be an $[n,k]_q$ MDS code with $4 \le k \le q-3$. If $\mathrm{PAut}(C)$ is 2-transitive on the n coordinate positions, then $n \le q+1$.*

The rest of this paper is organized as follows. In Section 2, we fix the notation and prove some preliminary lemmas that we shall use later. In Section 3, we apply Mortimer's results on modular representations of 2-transitive permutation groups from [37] and some related results from [19] to reduce the proof of Theorem 1.3 to the case where $\mathrm{PAut}(C)$ is one of some infinite

families of almost simple groups. In Section 4 we treat those infinite families and complete the proof of Theorem 1.3. We conclude this paper with some related research problems in Section 5.

2. Preliminaries

Let C be an $[n,k]_q$ code whose coordinates are labeled by an n-element set Ω. It is conventional to take $\Omega = \{1,2,\ldots,n\}$, but we will allow Ω to be other sets. The support of a codeword $c \in C$ is $\mathrm{supp}(c) = \{\omega \in \Omega : c_\omega \neq 0\}$, and its Hamming weight is the size of $\mathrm{supp}(c)$. We write $d(C)$ for the smallest nonzero Hamming weight of codewords in C.

Let $\mathbb{F} = \mathbb{F}_q$ for the finite field with q elements, where $q = p^f$ with p prime. Let $\mathbb{F}^\Omega$ be the set of all functions $f : \Omega \to \mathbb{F}$. For each $\omega \in \Omega$, let e_ω be the function that takes 1 at ω and takes 0 otherwise. For a subset $\Delta \subseteq \Omega$, write $\mathbf{1}_\Delta = \sum_{\omega\in\Delta} e_\omega$, and put $\mathbf{1} = \mathbf{1}_\Omega$. For $f, f' \in \mathbb{F}^\Omega$, their standard inner product is $\langle f, f'\rangle = \sum_{\omega\in\Omega} f(\omega)f'(\omega)$. We identify C as a subspace of $\mathbb{F}^\Omega$ via

$$c = (c_\omega)_{\omega\in\Omega} \mapsto \sum_{\omega\in\Omega} c_\omega e_\omega,$$

and write c for $\sum_{\omega\in\Omega} c_\omega e_\omega$ by abuse of notation. The *dual code* of C is $C^\perp = \{x \in \mathbb{F}^\Omega : \langle x, c\rangle = 0 \text{ for each } c \in C\}$, which has dimension $n-k$.

Let $\mathrm{Sym}(\Omega)$ be the set of all permutations of Ω. It induces an action on $\mathbb{F}^\Omega$ as follows:

$$(f^g)(\omega) = f(\omega^{g^{-1}}), \quad \text{for } g \in \mathrm{Sym}(\Omega),\ \omega \in \Omega,\ f \in \mathbb{F}^\Omega.$$

In particular, we have $e_\omega^g = e_{\omega^g}$. This action preserves the standard inner product:

$$\langle f^g, f'^g\rangle = \langle f, f'\rangle \text{ for } f, f' \in \mathbb{F}^\Omega,\ g \in \mathrm{Sym}(\Omega). \tag{2.1}$$

We define the permutation (automorphism) group of the code C as follows:

$$\mathrm{PAut}(C) = \{g \in \mathrm{Sym}(\Omega) : c^g \in C \text{ for each } c \in C\}.$$

By (2.1), we immediately deduce the following result.

Proposition 2.1. *We have* $\mathrm{PAut}(C) = \mathrm{PAut}(C^\perp)$.

If $\mathrm{PAut}(C)$ acts transitively on the set $\{(\alpha,\beta) \in \Omega^2 : \alpha \neq \beta\}$, then we say that $\mathrm{PAut}(C)$ is 2-transitive on the coordinate set Ω. The 2-transitive permutation groups have been classified, and the complete list can be found in [12, Tables 7.3, 7.4] or [15, Section 7.7].

Remark 2.2. *Here is a matrix description of $g \in \mathrm{PAut}(C)$. Let B_g be the $n \times n$ permutation matrix such that $B_g(\omega,\omega') = 1$ if $\omega' = \omega^g$ and $= 0$ otherwise. Let M be a generator matrix of C. Since g stabilizes C, the row space of MB_g is C. There is a corresponding invertible matrix P_g of order k such that $P_gM = MB_g$. We call B_g the permutation matrix associated with g, and call P_g the companion matrix with respect to the generator matrix M.*

We shall make use of the following well-known duality fact multiple times.

Lemma 2.3. *Let C be a nontrivial $[n,k]_q$ code. Then C is MDS if and only if $C^\perp$ is MDS.*

Let $G = \mathrm{PAut}(C)$. The vector space $\mathbb{F}^\Omega$ is naturally an $\mathbb{F}G$-module, and C is its submodule. Let E be an extension field of $\mathbb{F}$. We write $C \otimes E$ for the E-span of C, which is a subspace of E^Ω. It has dimension k over E, where $k = \dim_{\mathbb{F}}(C)$. Moreover, if $v_1, \cdots, v_k$ form a basis of C over $\mathbb{F}$, then they also form a basis of $C \otimes E = \langle v_1, \ldots, v_k \rangle_E$.

Lemma 2.4. *Let E be an extension field of $\mathbb{F}$, and let $C \leq \mathbb{F}^\Omega$ be an MDS code. Then $C \otimes E$ is an MDS code over E with the same parameters as C, and* $\mathrm{PAut}(C) = \mathrm{PAut}(C \otimes E)$.

Proof. Let $C' = C \otimes E$ in this proof. We choose a generator matrix M of C which has entries in $\mathbb{F}$, and it is also a generator matrix of $C \otimes E$. Let k be the dimension of C. Any k columns of C are linearly independent over $\mathbb{F}$, so they are also linearly independent over E. It follows that $C \otimes E$ is also an MDS code, cf. [35, Chapter 11].

We clearly have $\mathrm{PAut}(C) \leq \mathrm{PAut}(C')$. Take $g \in \mathrm{PAut}(C')$, and let B_g be its permutation matrix, cf. Remark 2.2. There is an invertible matrix P_g of order k over E such that $P_g M = MB_g$. Let M_0 and N_0 be the matrices formed by the first k columns of M and MB_g respectively. Then M_0 is invertible by the fact C is an MDS case, and M_0, N_0 both have entries in $\mathbb{F}$. It follows that $P_g = N_0 M_0^{-1}$ and it has entries in $\mathbb{F}$. We conclude that g stabilizes C, i.e., $g \in \mathrm{PAut}(C)$ as desired. This completes the proof. □

Lemma 2.5. *If C is a nontrivial $[n,k]_q$ MDS code, then $n \leq q + \min\{k, n-k\} - 1$. In particular, we have $n \leq 2q - 2$.*

Proof. We have $n \leq q + k - 1$ by [1, Lemma 1.2]. Since $C^\perp$ is also an MDS code, we have $n \leq q + (n-k) - 1$ by the same reason. This proves the first claim. Since $\min\{k, n-k\} \leq n/2$, it follows that $n \leq q - 1 + n/2$, i.e., $n \leq 2q - 2$. □

The following result is an immediate corollary of Lemma 2.5.

Corollary 2.6. *If there exists a nontrivial $[n,k]_q$ MDS code with $n > q+1$, then $\frac{n+2}{2} \leq q \leq n-2$.*

Let $\overline{\mathbb{F}}$ be the algebraic closure of $\mathbb{F}$. In particular, each polynomial of positive degree in $\mathbb{F}[x]$ factorizes into the product of degree 1 polynomials in $\overline{\mathbb{F}}[x]$. To utilize Lemma 2.5 more efficiently, we need the following lemma. We define the Frobenius map

$$\sigma : \overline{\mathbb{F}}^\Omega \to \overline{\mathbb{F}}^\Omega, \quad (x_\omega)_{\omega \in \Omega} \mapsto (x_\omega^p)_{\omega \in \Omega}. \tag{2.2}$$

Lemma 2.7. *Let U be an $\overline{\mathbb{F}}G$-submodule of $\overline{\mathbb{F}}^\Omega$, where G is a subgroup of* $\mathrm{Sym}(\Omega)$. *Then $\sigma(U)$ is also an $\overline{\mathbb{F}}G$-submodule of $\overline{\mathbb{F}}^\Omega$, and* $\dim(U) = \dim(\sigma(U))$.

Proof. It is routine to verify that elements of G and σ commute. It follows that $\sigma(U)$ is invariant under the action of G, i.e., it is an $\overline{\mathbb{F}}G$-module. Since σ is a bijection of $\overline{\mathbb{F}}^\Omega$, we clearly have $\dim(U) = \dim(\sigma(U))$. This completes the proof. □

Lemma 2.8. *Suppose that U is a subspace of $\overline{\mathbb{F}}^\Omega$ such that $\sigma^b(U) = U$ for some positive integer b. Then $U' := U \cap \mathbb{F}_{p^b}^\Omega$ has the same dimension as U, and $U = U' \otimes \overline{\mathbb{F}}$.*

Proof. Take a basis $\mathcal{B}$ of U, whose coordinates all lie in some finite fields. Let E be the smallest field that contains $\mathbb{F}_{p^b}$ and all those coordinates, which is again a finite field. Take a basis $\gamma_0, \ldots, \gamma_{m-1}$ of E over $\mathbb{F}_{p^b}$. Let $U' := U \cap \mathbb{F}_{p^b}^\Omega$. For each vector $v \in \mathcal{B}$ and $0 \le i \le m-1$, define $u_i = \sum_{j=0}^{m-1} \gamma_i^{p^{bj}} \sigma^{bj}(v) \in U$. We have $u_i \in U'$ upon direct check. The matrix $(\gamma_i^{p^{bj}})_{0 \le i,j \le m-1}$ is nonsingular by [32, Corollary 2.38], so v lies in the E-span of $u_0, \ldots, u_{m-1}$. It follows that $U \le U' \otimes \overline{\mathbb{F}}$, and U is generated by a set of vectors in U'. The two claims then follow immediately. This completes the proof. □

Let U be an $\overline{\mathbb{F}}G$-submodule of $\overline{\mathbb{F}}^\Omega$, and let $m = \dim_{\overline{\mathbb{F}}} U$. We say that U can be realized over $\mathbb{F}_{p^s}$ if $U \cap \mathbb{F}_{p^s}^\Omega$ has dimension m, i.e., U has a basis that is contained in $\mathbb{F}_{p^s}^\Omega$. By Lemma 2.8, we deduce that U can be realized over $\mathbb{F}_{p^s}$ if and only if $\sigma^s(U) = U$.

Lemma 2.9. *Let $U \le \overline{\mathbb{F}}^\Omega$ be a nontrivial $[n,k]$ MDS code. If $\sigma^b(U) = U$ for some positive integer b, then $n \le 2p^b - 2$.*

Proof. Let $U' := U \cap \mathbb{F}_{p^b}^\Omega$, and write $d(U')$ for its minimum weight. By Lemma 2.8, it has dimension k over $\mathbb{F}_{p^b}$, and $U = U' \otimes \overline{\mathbb{F}}$. By the Singleton bound, we have $d(U') \le n - k + 1$. By the fact $U' \subseteq U$, we have $d(U') \ge n - k + 1$. It follows that U' is also an $[n,k]$ MDS code. The claim then follows by applying Lemma 2.5 to the code U'. □

A nonzero $\overline{\mathbb{F}}G$-submodule U of $\overline{\mathbb{F}}^\Omega$ is *irreducible* if its only submodule are 0 and U. The *socle* of $\overline{\mathbb{F}}^\Omega$ is the sum of all its irreducible submodules. An irreducible submodule of $C \otimes \overline{\mathbb{F}}$ is an irreducible submodule of $\overline{\mathbb{F}}^\Omega$, so is contained in the socle of $\overline{\mathbb{F}}^\Omega$. If G is 2-transitive on Ω, the $\overline{\mathbb{F}}G$-module structure of $\overline{\mathbb{F}}^\Omega$ has been extensively studied, cf. Burichenko [9], Landrock and Michler [31], Mortimer [37], Hiss [23, 24], Guralnick and Tiep [19]. In particular, Mortimer's result [37] provides the motivation for the research in this paper. Despite of the fact that its title is about known 2-transitive groups, his result covers all of them modulo the classification of finite simple groups, cf. [12].

3. Reduction to the reducible hearts

In this and the next section, we present the proof of Theorem 1.3. We first fix some notation that we shall use throughout the remaining part of this paper. Let $q = p^f$ with p prime, and let $\mathbb{F} = \mathbb{F}_q$ be the finite field with q elements. We write $\overline{\mathbb{F}}$ for the algebraic closure of $\mathbb{F}$. Let C be a nontrivial $[n,k]_q$ MDS code. Let Ω be the set of n coordinate positions of C, so that C is a subspace of $\mathbb{F}^\Omega$. Let $G = \mathrm{PAut}(C)$, and assume that G acts 2-transitively on the set Ω. By Proposition 2.1 and Lemma 2.3, we assume without loss of generality that $k \le n/2$.

Lemma 3.1. *Take notation as above. Let G_α be the stabilizer of some $\alpha \in \Omega$ in G. If (G, G_α, p) is one of the cases in Table 3.1, then we have $n \le q + 1$.*

Proof. Let (G, G_α) be one of the cases in Table 3.1. Suppose to the contrary that $n > q + 1$. Then by Corollary 2.6, we have $\frac{n+2}{2} \le q \le n - 2$. This gives the possible values of $q = |\mathbb{F}|$ in the last column of the table. If $G = HS$ and $(n,q) = (176, 128)$, we would have $\min\{k, n-k\} \ge n + 1 - q = 49$ if C is a nontrivial MDS code by Lemma 2.5. We check with Magma [8]

that all G-invariant codes over $\mathbb{F}_{128}$ of length 176 and dimension in the range $[2, 174]$ have dimensions $21, 22, 154$ or 155, none of which satisfies $\min\{k, 176-k\} \geq 49$. If $G = Co_3$ and $q = 243$, the parameters of all G-invariant codes of length 276 and dimension in the range $[2, 274]$ are $[276, 126, \leq 102]_{243}$, $[276, 127, \leq 105]_{243}$, $[276, 149, \leq 84]_{243}$ and $[276, 150, \leq 86]_{243}$. If $G = Co_3$ and $q = 256$, all G-invariant codes of length 276 and dimension in the range $[2, 274]$ are $[276, 23, \leq 132]_{256}$ and $[276, 253, \leq 14]_{256}$ codes. None of those codes are MDS codes. For the other cases, we list all the G-invariant $[n, k, d]_q$ codes with $2 \leq k \leq n-2$ as follows:

(1) $G = {}^2G_2(3)$: one $[28, 7, 12]_{16}$ code, two $[28, 8, 12]_{16}$ codes and one $[28, 9, 10]_{16}$ code.
(2) $G = M_{24}$: one $[24, 12, 8]_{16}$ code.
(3) $G = M_{23}$: one $[23, 11, 8]_{16}$ code and one $[23, 12, 7]_{16}$ code.
(4) $G = M_{22}$: one $[22, 10, 8]_{16}$ code, one $[22, 11, 6]_{16}$ code, two $[22, 11, 7]_{16}$ code, fourteen $[22, 11, 8]_{16}$ codes and one $[22, 12, 6]_{16}$ code.
(5) $G = M_{11}$: one $[12, 6, 6]_9$ code.

None of the above codes are MDS codes. This completes the proof. □

TABLE 3.1. The (G, G_α, p) tuples. Here, $P \in \mathrm{Syl}_3(\mathrm{PSL}_2(8))$ for line 1, and the possible values of $q = |\mathbb{F}|$ follows from Corollary 2.6.

G	G_α	$\lvert\Omega\rvert = [G : G_\alpha]$	$p = \mathrm{char}(\mathbb{F})$	Possible $q = \lvert\mathbb{F}\rvert$
$G = {}^2G_2(3) \cong \mathrm{P\Gamma L}_2(8)$	$G_\alpha = N_G(P)$	28	2	16
$G = M_{24}$	$G_\alpha = M_{23}$	24	2	16
$G = M_{23}$	$G_\alpha = M_{22}$	23	2	16
$G = M_{22}$	$G_\alpha = \mathrm{PSL}_3(4)$	22	2	16
$G = M_{11}$	$G_\alpha = \mathrm{PSL}_2(11)$	12	3	9
$G = HS$	$G_\alpha = \mathrm{PSU}_3(5){:}2$	176	2	128
$G = Co_3$	$G_\alpha = \mathrm{McL}{:}2$	276	3	243
			2	256

By Lemma 2.4, the code $C \otimes \overline{\mathbb{F}}$ is also an MDS code. By abuse of notation, we assume that $\mathbb{F}$ is algebraically closed and write C for $C \otimes \overline{\mathbb{F}}$ from now on. Let $M = \overline{\mathbb{F}}^{\Omega}$, so that C is a $\overline{\mathbb{F}}G$-submodule of M. We define two subspaces of M as follows:

$$J = \overline{\mathbb{F}}\mathbf{1}, \qquad A = \left\{ (a_\omega)_{\omega\in\Omega} : \sum_{\omega\in\Omega} a_\omega = 0 \right\}.$$

We have $A = J^\perp$, $A \cap J = 0$ if $p \nmid n$ and $J \leq A$ if $p \mid n$. Both J and A are invariant under the action of $\mathrm{Sym}(\Omega)$, so are $\mathbb{F}G$-submodules of M. The *heart* of M is the quotient module

$$\overline{A} = A/(A \cap J).$$

By Lemma 2 of [37], we have the following result.

Lemma 3.2. *Take notation as above. If the heart $\overline{A}$ is a simple $\mathbb{F}G$-module, then the only G-submodules of M are 0, J, A and M.*

The *socle* of G, denoted by $\mathrm{soc}(G)$, is the subgroup generated by all the minimal normal subgroups of G. By Burnside's theorem [10, Theorem IX on p. 214], a finite 2-transitive group is either affine or almost simple, cf. [12, Table 7.4] and [15, Section 7.7]. In the almost simple case, there is a nonabelian simple group S such that $\mathrm{soc}(G) = S$ and $S \leq G \leq \mathrm{Aut}(S)$. In the affine case, $\mathrm{soc}(G) \cong (\mathbb{F}_\ell^a, +)$ is an elementary abelian ℓ-group with ℓ prime, and it acts regularly on Ω. We regard it as an vector space over $\mathbb{F}_\ell$, and denote it by V. We identify Ω with V via $\alpha^v \mapsto v$, where α is a fixed point of Ω and v ranges in V. We then have $G = V \rtimes G_0$, where $G_0 \leq \mathrm{GL}(V)$ is the stabilizer of 0 in G. The group G_0 is transitive on $V \setminus \{0\}$ by the 2-transitivity assumption.

Proposition 3.3. *Let C be a nontrivial $[n,k]_q$ MDS code. If $G = \mathrm{PAut}(C)$ is a 2-transitive subgroup of $\mathrm{Sym}(\Omega)$ of affine type, then we have $n \leq q$.*

Proof. Let ℓ^a be the order of $\mathrm{soc}(G)$, where ℓ is a prime. We have $C \notin \{0, J, A, M\}$ by the assumption $\min\{k, n-k\} \geq 2$. By Lemma 3.2, the heart $\overline{A}$ is reducible. By line 4 of [37, Table 1], we deduce that $p = \ell$. Hence, $n = p^a$ and $q = p^f$. Suppose to the contrary that $n \geq q+1$, i.e., $a > f$. By Lemma 2.5, we have $n \leq 2q - 2$. It follows that $p^a = n \leq 2p^f - 2 < p^{f+1}$, i.e., $a < f + 1$: a contradiction. Therefore, we have $n \leq q$ as desired. □

Proposition 3.4. *Take notation as above, and assume that G is 2-transitive on the set Ω. If $n = |\Omega| > q + 1$, then (G, Ω, q) occur in Table 3.2.*

Proof. Assume that $n > q + 1$. By Proposition 3.3, G is an almost simple group, so the case $G = A_4 \cong \mathrm{AGL}_1(4)$ in the line 3 of [37, Table 1] is excluded. Let $S = \mathrm{soc}(G)$, which is a nonabelian simple group. By Lemma 3.2, the heart $\overline{A} = A/(A \cap J)$ is reducible, so it must be one of the cases in [37, Table 1]. By Theorems 61 and 63 of [2], we know that the MDS conjecture holds if $\min\{k, n-k\} \leq 5$ and so the case $G = \mathrm{PSL}_2(11)$ in the third row from the bottom of [37, Table 1] is ruled out. If $S = {}^2G_2(3)'$, then $S \cong \mathrm{PSL}_2(8)$ and $G = \mathrm{P\Gamma L}_2(8)$ by [37, Table 1]. This case has been excluded by Lemma 3.1. If $S = \mathrm{Sp}_4(2)'$, then $S \cong \mathrm{PSL}_2(9)$, and it has a unique 2-transitive action on 10 elements. Hence this case is covered by the action of $\mathrm{PSL}_2(9)$ on the projective points of $\mathrm{PG}(1, 9)$. If $S = {}^2G_2(r)$ with $r = 3^{2a+1} \geq 27$, the possibility that $p \mid r - \sqrt{3r} + 1$ left open in [37, Table 1] has been eliminated in [19, Section 4.3]. We have excluded the cases in Table 3.1 by Lemma 3.1, and the remaining cases in [37, Table 1] are recorded in Table 3.2. This completes the proof. □

4. Almost simple actions

Our main result in this section is the following result.

Theorem 4.1. *Let C be a nontrivial $[n,k]_q$ MDS code such that $C \leq \mathbb{F}_q^\Omega$, and assume that $G = \mathrm{PAut}(C)$ is a 2-transitive subgroup of $\mathrm{Sym}(\Omega)$ of almost simple type in Table 3.2. Then q is a power of 4, $\mathrm{PSL}_2(5) \trianglelefteq G$, and C is a $[6,3,4]_q$ code.*

TABLE 3.2. The candidate 2-transitive actions, where $p = \mathrm{char}(\mathbb{F})$ and $a \geq 1$

$S = \mathrm{soc}(G)$	Ω	$n = \lvert\Omega\rvert$	Conditions
$\mathrm{PSL}_d(r)$	points of $\mathrm{PG}(d-1, r)$	$(r^d-1)/(r-1)$	$d \geq 3$, $r = p^s$
$\mathrm{Sp}_{2m}(2)$	quadratic forms of type ε	$2^{m-1}(2^m + \varepsilon 1)$	$p = 2$, $m \geq 3$, $\varepsilon = \pm$
$\mathrm{PSL}_2(r)$	points of $\mathrm{PG}(1, r)$	$r+1$	$p = 2$, $r \geq 5$ odd
$\mathrm{Sz}(r)$	Suzuki-Tits ovoid	r^2+1	$r = 2^{2a+1}$, $p \mid r + \sqrt{2r} + 1$
$\mathrm{PSU}_3(r)$	points of the classical unital	r^3+1	$r \geq 3$, $p \mid r+1$
${}^2G_2(r)$	Ree–Tits ovoid	r^3+1	$r = 3^{2a+1}$, $p \mid 2(r+1)(r+\sqrt{3r}+1)$

In view of Proposition 3.4, Theorem 4.1 would complete the proof of Theorem 1.3. We take the same notation as introduced in the beginning of Section 3, and further assume that $G = \mathrm{PAut}(C)$ is a 2-transitive permutation group of Ω that appears in Table 3.2. Let $S = \mathrm{soc}(G)$, which is a nonabelian simple group. We have $S \leq G \leq \mathrm{Aut}(S)$.

Lemma 4.2. *Suppose that the $\overline{\mathbb{F}}S$-submodules of M form a chain under inclusion. Then $|\Omega| = n \leq 2p-2$, where p is the characteristic of $\mathbb{F}$.*

Proof. Let σ be as defined in (2.2). By Lemma 2.7, $\sigma(C)$ is also an $\overline{\mathbb{F}}S$-submodule of the same dimension. There is at most one submodule of a given dimension by assumption, so $\sigma(C) = C$. The claim then follows from Lemma 2.9. □

4.1. **The case $S = \mathrm{PSL}_d(p^s)$, $d \geq 3$.** Let $r = p^s$ and $d \geq 3$, where p is the characteristic of $\mathbb{F}$ and s is a positive integer. We set $W = \mathbb{F}_r^d$, and let Ω be the set of all one-dimensional $\mathbb{F}_r$-subspaces of W. We have $n = |\Omega| = \frac{r^d-1}{r-1}$, and $S = \mathrm{PSL}_d(r)$. A *hyperplane* of W is an $(d-1)$-dimensional subspace of W. For a hyperplane H, let $\mathrm{PG}(H)$ be the set of 1-dimensional subspaces contained in H. Let D be the $\overline{\mathbb{F}}S$-submodule of $M = \overline{\mathbb{F}}^{\Omega}$ spanned by $\mathbf{1}_{\mathrm{PG}(H)}$ with H ranging over all hyperplanes of W, which is referred to as *the hyperplane design module* in the literature. We have $J \leq D$, since each element of Ω is contained in $n_0 = \frac{r^{d-1}-1}{r-1}$ hyperplanes. We have $\dim(D \cap A) = \dim(D) - 1$ and $M = J \oplus A$ by the fact $p \nmid n$. We refer to [3] for the detailed descriptions of $\overline{\mathbb{F}}S$-module structure of $M = \overline{\mathbb{F}}^{\Omega}$.

Theorem 4.3. *Take notation as above. Then $\mathrm{soc}(G)$ can not be $\mathrm{PSL}_d(p^s)$, $d \geq 3$.*

Proof. Suppose to the contrary that $\mathrm{soc}(G)$ is $S = \mathrm{PSL}_d(p^s)$, $d \geq 3$. By replacing C with $C^{\perp}$, we assume without loss of generality that $k \leq n/2$. It is shown in the proof of [14, Lemma 9.2] that $A \cap D$ is the unique minimal submodule of A by using the results in [3]. That is, $\mathrm{soc}(A) = D \cap A$. Since $\dim(C) \geq 2$, we deduce that $C \cap A$ contains $D \cap A$.

Let H_1, H_2 be two distinct hyperplanes of W. We have $\mathbf{1}_{\Omega \setminus \mathrm{PG}(H_1)}, \mathbf{1}_{\Omega \setminus \mathrm{PG}(H_2)} \in D \cap A$, since $n - |\mathrm{PG}(H_i)| \equiv 0 \pmod{p}$ for $i \in \{1, 2\}$. It follows that they are codewords of C, and so

$$\mathbf{1}_{\Omega \setminus \mathrm{PG}(H_1)} - \mathbf{1}_{\Omega \setminus \mathrm{PG}(H_2)} = \mathbf{1}_{\mathrm{PG}(H_2)} - \mathbf{1}_{\mathrm{PG}(H_1)} \in C.$$

This codeword has weight $2r^{d-2}$, since $\dim_{\mathbb{F}_r}(H_1 \cap H_2) = d-2$. It follows that

$$\frac{n}{2} + 1 \leq n - k + 1 = d(C) \leq 2r^{d-2},$$

i.e., $\frac{r^d-1}{r-1} + 2 \leq 4r^{d-2}$. This inequality holds for no (r, d) pairs with $d \geq 3$ upon direct check: a contradiction. This completes the proof. □

4.2. **The case $S = \mathrm{Sp}_{2m}(2)$, $m \geq 3$.** Let $V = \mathbb{F}_2^{2m}$ with $m \geq 3$, and let b be the alternating form on V such that $b(x, y) = \sum_{i=1}^{2m} x_i y_{2m+1-i}$ for $x, y \in V$. Let $S = \mathrm{Sp}_{2m}(2)$ be the corresponding symplectic group. For a quadratic form $Q : V \to \mathbb{F}_2$, its associated bilinear form is $f(x, y) = Q(x+y) - Q(x) - Q(y)$. Since the characteristic is 2, the bilinear form f is an alternating form, i.e., $f(x, x) = 0$ for all $x \in V$. A subspace U of V is *totally singular* if $Q(u) = 0$ for all $u \in U$. The Witt index of Q is the maximal dimension of its totally singular subspaces.

Let $\mathcal{X}$ be the set of all quadratic forms on V with associated bilinear form b. Let $e_1, \ldots, e_{2m}$ be the standard basis of V. For each $Q \in \mathcal{X}$, we have

$$Q(x) = \sum_{i=1}^{m} x_i x_{2m+1-i} + \sum_{i=1}^{2m} Q(e_i) x_i. \tag{4.1}$$

Here, we use the fact that $a^2 = a$ for $a \in \mathbb{F}_2$. For $Q \in \mathcal{X}$, we say that it is hyperbolic or has type $+$ if its Witt index is m, and say that it is elliptic or has type $-$ if its Witt index is $m-1$. Let Ω^ε be the set of quadratic forms in $\mathcal{X}$ of type ε for $\varepsilon \in \{+, -\}$. We have $|\Omega^\varepsilon| = 2^{m-1}(2^m + \varepsilon 1)$. Since $G = S$, the group S acts 2-transitively on both sets via $Q \mapsto Q^g$ for $Q \in \mathcal{X}$ and $g \in S$, where $Q^g(x) = Q(x^{g^{-1}})$ for $x \in V$. We refer to [40] for more details.

Lemma 4.4. *For $Q \in \mathcal{X}$, let $\mu(Q) = \sum_{i=1}^{m} Q(e_i)Q(e_{2m+1-i})$. We have $\Omega^+ = \{Q \in \mathcal{X} : \mu(Q) = 0\}$ and $\Omega^- = \{Q \in \mathcal{X} : \mu(Q) = 1\}$.*

Proof. Let $a_j = Q(e_j)$ for $1 \leq j \leq 2m$, and fix an integer i such that $1 \leq i \leq m$. The quadratic form $a_i x_i^2 + x_i x_{2m+1-i} + a_{2m+1-i} x_{2m+1-i}$ on the subspace $\langle e_i, e_{2m+1-i} \rangle$ is elliptic if $a_i = a_{2m+1-i} = 1$ and is hyperbolic otherwise. That is, its type depends on the value of $a_i a_{2m+1-i}$. The claim then follows by taking summation over $1 \leq i \leq m$. □

Suppose that $\Omega = \Omega^\varepsilon$ with $\varepsilon \in \{+, -\}$. We have $p = 2$ in this case by Table 3.2. We extend a quadratic form in Ω to a quadratic form over $V \otimes \overline{\mathbb{F}}$ in the natural way. We also extend b to a bilinear form over $V \otimes \overline{\mathbb{F}}$ similarly. By [40, Proposition 8.4] (i), J is the socle of $M = \overline{\mathbb{F}}^\Omega$, i.e., the unique irreducible $\overline{\mathbb{F}}S$-submodule of M. By [40, Proposition 8.4] (ii), M/J has a unique irreducible module N^ε isomorphic to $V \otimes \overline{\mathbb{F}}$.

We now construct the full preimage of N^ε in M. We define

$$Q^+(x) = \sum_{i=1}^{m} x_i x_{2m+1-i}, \quad Q^-(x) = x_1 + x_{2m} + Q^+(x),$$

so that $Q^+ \in \Omega^+$ and $Q^- \in \Omega^-$. For each $Q \in \Omega$, $Q(x) + Q^\varepsilon(x)$ is linear map from $V \otimes \overline{\mathbb{F}}$ to $\overline{\mathbb{F}}$. For $w \in V$, define $\lambda_w \in M$ by

$$(\lambda_w)_Q = Q(w) + Q^\varepsilon(w), \quad \text{for } Q \in \Omega.$$

Proposition 4.5. *Let $B^\varepsilon = \langle \mathbf{1}, \lambda_w : w \in V\rangle_{\overline{\mathbb{F}}}$. Then B^ε is the full preimage of N^ε in $M = \overline{\mathbb{F}}^\Omega$, and we have $B^\varepsilon \le C \cap C^\perp$.*

Proof. First, we claim that $\lambda_{u+v} = \lambda_u + \lambda_v$ for $u, v \in V \otimes \overline{\mathbb{F}}$. Indeed, we have

$$\begin{aligned}\lambda_{u+v}(Q) &= Q(u+v) + Q^\varepsilon(u+v)\\ &= Q(u) + Q(v) + b(u,v) + Q^\varepsilon(u) + Q^\varepsilon(v) + b(u,v)\\ &= \lambda_u(Q) + \lambda_v(Q)\end{aligned}$$

for $Q \in \Omega$. For $g \in S$, we have $\lambda_w^g = \lambda_{w^g} + (Q^\varepsilon(w^g) + Q^\varepsilon(w))\,\mathbf{1} \in B^\varepsilon$, since

$$(\lambda_w^g)(Q) = \lambda_w(Q^{g^{-1}}) = Q(w^g) + Q^\varepsilon(w) = \lambda_{w^g}(Q) + Q^\varepsilon(w^g) + Q^\varepsilon(w)$$

for $Q \in \Omega$. It follows that B^ε is a $\overline{\mathbb{F}}S$-submodule of M.

We claim that $B^\varepsilon \neq J$. Take $Q \in \Omega$ with $Q \neq Q^\varepsilon$. Since $Q(x) + Q^\varepsilon(x)$ is a nonzero linear map from $V \otimes \overline{\mathbb{F}}$ to $\overline{\mathbb{F}}$, there is $w \in V \otimes \overline{\mathbb{F}} \setminus \{0\}$ such that $Q(w) + Q^\varepsilon(w) \neq 0$, i.e., $\lambda_w(Q) \neq 0$. On the other hand, we have $\lambda_w(Q^\varepsilon) = 0$. Hence $\lambda_w \notin J$. This proves the claim.

By [40, Proposition 8.4], we deduce that B^ε/J contains N^ε. They are equal by considering dimensions. Since an irreducible submodule of C is also an irreducible submodule of M, we deduce that C contains J. Since $\dim(C) \ge 2$, we have $C \neq J$, and so C/J contains N^ε. We conclude that C contains B^ε. The same arguments yield that $C^\perp$ contains B^ε. □

Let $\mu = \mu(Q^\varepsilon)$, so that $\mu(Q) = \mu$ for $Q \in \Omega$, cf. Lemma 4.4. For $Q \in \Omega$, let $v_Q = (Q(e_1), \ldots, Q(e_{2m})) \in \mathbb{F}_2^{2m}$ and $T^\varepsilon = \{v_Q : Q \in \Omega\}$. We have a bijection between Ω and T via $Q \mapsto v_Q$, cf. (4.1). We have $T^\varepsilon = \{v \in \mathbb{F}_2^{2m} : Q^+(v) = \mu\}$ by Lemma 4.4 and the fact $\mu(Q) = Q^+(v_Q)$. In particular, we have

$$\begin{aligned}\Omega = \Omega^\varepsilon &= \left\{ \sum_{i=1}^{m} x_i x_{2m+1-i} + \sum_{i=1}^{2m} v_{2m+1-i} x_i : v \in T^\varepsilon \right\}\\ &= \{Q^+(x) + b(v,x) : v \in \mathbb{F}_2^{2m} \text{ such that } Q^+(v) = \mu\}. \end{aligned} \tag{4.2}$$

For a property $\mathbf{P}$, let $[\![\mathbf{P}]\!] = 1$ if it holds and $[\![\mathbf{P}]\!] = 0$ otherwise.

Theorem 4.6. *Take notation as above. Then* $\mathrm{soc}(G)$ *can not be* $\mathrm{Sp}_{2m}(2)$*, $m \ge 3$.*

Proof. We continue with the above arguments. By Proposition 4.5, we have $B^\varepsilon \le C \cap C^\perp$. We take a nonzero vector $w \in \mathbb{F}_2^{2m}$ such that $Q^+(w) = 0$, and take $c = Q^+(w) + Q^\varepsilon(w) \in \mathbb{F}_2$. By the paragraph preceding this theorem, we deduce that $(\lambda_w)_Q = c + b(v,w) \in \mathbb{F}_2$ for $Q \in \Omega$ such that $Q(x) = Q^+(x) + b(v,x)$ with $Q^+(v) = \mu$. The codeword $\lambda_w + c\mathbf{1}$ is in $\mathbb{F}_2^\Omega$ and the number of its zero coordinates is

$$\begin{aligned}&\sum_{v \in \mathbb{F}_2^{2m}} [\![Q^+(v) = \mu]\!] \cdot [\![b(v,w) = 0]\!] = \frac{1}{4} \sum_{v \in \mathbb{F}_2^{2m}} \left(1 + (-1)^{Q^+(v)+\mu}\right)\left(1 + (-1)^{b(v,w)}\right)\\ &= 2^{2m-2} + \frac{1}{4} \sum_{v \in \mathbb{F}_2^{2m}} (-1)^{Q^+(v)+\mu} + \frac{1}{4} \sum_{v \in \mathbb{F}_2^{2m}} (-1)^{Q^+(v)+\mu+b(v,w)}.\end{aligned}$$

Here, we used the fact $\frac{1}{4}\sum_{v\in\mathbb{F}_2^{2m}}(-1)^{b(v,w)}=0$. Since $Q^+(x)=x_1x_{2m}+\cdots+x_mx_{m+1}$, it is elementary to deduce that the above number is $2^{2m-2}+(-1)^\mu 2^{m-1}$. Since the all-one vector is in $C\cap C^\perp$ and has Hamming weight $n=2^{2m-1}+(-1)^\mu 2^{m-1}$, we deduce that either $\lambda_w+c\mathbf{1}$ or $\lambda_w+(c+1)\mathbf{1}$ has weight less than $\frac{1}{2}n$. It follows that

$$n+2=d(C)+d(C^\perp)<\frac{1}{2}n+\frac{1}{2}n=n.$$

This contradiction completes the proof. □

4.3. **The case $S=\mathrm{PSL}_2(r)$, r odd.** The group $\mathrm{PSL}_2(3)$ is solvable, so we have $r\geq 5$ in this case. Let $r=\ell^s\geq 5$ with ℓ an odd prime, and let Ω be the set of 1-dimensional subspaces of $V=\mathbb{F}_r^2$. By Table 3.2, the characteristic of $\mathbb{F}$ is $p=2$. We identify Ω with $\mathbb{F}_r\cup\{\infty\}$ via $\langle(1,a)\rangle\mapsto a$ for $a\in\mathbb{F}_r$ and $\langle(0,1)\rangle\mapsto\infty$. By [19, Lemma 4.1 (i)], the socle of $M=\overline{\mathbb{F}}^\Omega$ is J, i.e., J is the unique irreducible submodule of M.

Let Δ be the set of nonzero squares of $\mathbb{F}_r$, and let u be a root of $X^2+X+1=0$ in $\overline{\mathbb{F}}$. By pp. 14-15 of [37], the heart $\overline{A}=A/J$ is the direct sum of two irreducible $\overline{\mathbb{F}}S$-submodules $N_1\oplus N_2$, and N_1,N_2 are the only proper submodules of $\overline{A}$. For $i=1,2$, the module N_i is generated by an element $a_ie_0+b_ie_\infty+\mathbf{1}_\Delta$, where the a_i's and b_i's are as in the following table. Let C_1,C_2 be the full preimage of N_1,N_2 in M respectively. They are the only $\overline{\mathbb{F}}S$-submodules

$r \pmod 8$	a_1	b_1	a_2	b_2	realized over
1	0	0	1	1	$\mathbb{F}_2$
3	u	u^2	u^2	u	$\mathbb{F}_4$
5	u	u	u^2	u^2	$\mathbb{F}_4$
7	0	1	1	0	$\mathbb{F}_2$

of A that contains J. Moreover, they are orthogonal to each other when $r\equiv 1 \pmod 4$, and are both self-dual when $r\equiv 3 \pmod 4$ by [37]. Since $\dim(C_i)=\frac{r+1}{2}$ for $i=1,2$, we deduce that $C_1=C_2^\perp$ when $r\equiv 1 \pmod 4$.

Theorem 4.7. *Take notation as above. If $S=\mathrm{PSL}_2(r)$ with $r\geq 5$ odd, then $r=5$ and C is a $[6,3,4]$ code.*

Proof. Let $q_0=2^{f_0}$, where $f_0=1$ if $r\equiv\pm 1 \pmod 8$ and $f_0=2$ if $r\equiv\pm 3 \pmod 8$. Let σ be as defined in (2.2). By considering dimensions, we deduce that both C and $C^\perp$ contains J. It follows that $J\leq C\leq J^\perp$. Since $\dim(C)\geq 2$, it is either C_1 or C_2 by the paragraph preceding this theorem. It follows that C can be realized over $\mathbb{F}_{q_0}$, i.e., it has a basis consisting of elements in $\mathbb{F}_{q_0}^\Omega$. We thus have $\sigma^{f_0}(C)=C$. By Lemma 2.9, we have $n=r+1\leq 2q_0-2$. Since $r\geq 5$, we deduce that $r=5$, $q_0=4$. It follows that $k=\dim(C)=\frac{r+1}{2}=3$. There is a unique $[6,3,4]_4$ code up to equivalence, i.e., the hexacode. This completes the proof. □

4.4. **The case $S=\mathrm{Sz}(2^{2a+1})$.** Let $r=2^{2a+1}\geq 8$ and $m=2^{a+1}$. In this case, we have $|\Omega|=r^2+1$ and $p\mid r+m+1$ by Table 3.2, where p is the characteristic of $\mathbb{F}$. The $\overline{\mathbb{F}}S$-submodules of $M=\overline{\mathbb{F}}^\Omega$ are described in Appendix D.1 of [23]; see also [19, Section 4.2]. They

form a chain under inclusion: $0 < J < B_1 < B_2 < A < M$. Here, B_1/J, B_2/B_1 and A/B_2 are simple modules of dimensions $\frac{m}{2}(r-1)$, $(r-1)(r+1-m)$ and $\frac{m}{2}(r-1)$ respectively.

Theorem 4.8. *Take notation as above. Then* $\mathrm{soc}(G)$ *can not be* $S = \mathrm{Sz}(2^{2a+1})$, $a \geq 1$.

Proof. We continue with the above arguments. By Lemma 4.2, we deduce that $n = r^2 + 1 \leq 2p - 2$. On the other hand, we have $2m = 2^{a+2} \leq r = 2^{2a+1}$ and $p \mid r + m + 1$, so $2p - 2 \leq 2r + 2m \leq 3r < r^2 + 1$: a contradiction. This completes the proof. □

4.5. **The case** $S = \mathrm{PSU}_3(r)$**,** $r > 2$**.** Let $r = \ell^s > 2$, where ℓ is a prime. Let $W = \mathbb{F}_{r^2}^3$, and define $H(x) = x_1x_3^r + x_2^{r+1} + x_3x_1^r$. We have $\Omega = \{\langle u\rangle_{\mathbb{F}_{r^2}} : u \in W \setminus \{0\}, H(u) = 0\}$, $|\Omega| = r^3 + 1$. If $\langle u\rangle_{\mathbb{F}_{r^2}}, \langle v\rangle_{\mathbb{F}_{r^2}}$ are two distinct elements in Ω, then $\{\langle au + bv\rangle_{\mathbb{F}_{r^2}} : a, b \in \mathbb{F}_{r^2}^2 \setminus \{(0,0)\}\} \cap \Omega$ has size $r + 1$, and we call it a block of Ω. Let Δ be the set of all such blocks. The pair (Ω, Δ) with the inclusion relation defines a 2-$(r^3 + 1, r + 1, 1)$ design, i.e., the classical unital. We refer to [37, p. 15] for more details.

We have $p \mid r + 1$ by Table 3.2, where p is the characteristic of $\mathbb{F}$. Let $D = \langle \mathbf{1}_B : B \in \Delta\rangle_{\overline{\mathbb{F}}} \leq M = \overline{\mathbb{F}}^{\Omega}$, and we call D the design module. The dimension of D is $r(r^2 - r + 1)$ by [24, Corollary 5.1], so $\dim(D^{\perp}) = r^2 - r + 1$. We have $J \leq D, D^{\perp} \leq A = J^{\perp}$, and D/J is not isomorphic to $D^{\perp}/J$ by considering dimensions.

Lemma 4.9. *The modules* D *and* $D^{\perp}$ *are not MDS codes.*

Proof. It suffices to consider D by Lemma 2.3. The length is $n = r^3 + 1$. The dimension of D is $k = r(r^2 - r + 1)$ by [24, Corollary 5.1]. For a block $B \in \Delta$, $\mathbf{1}_B$ is in D and has weight $r + 1$. It follows that $n - k + 1 = d(D) \leq r + 1$, i.e., $(r - 1)^2 \leq 0$, which contradicts $r > 2$. □

By [24, Theorem 4.1] and [19, Lemma 4.1 and Section 4.4], we have the following information on the $\overline{\mathbb{F}}S$-module structure of $M = \overline{\mathbb{F}}^{\Omega}$:

(1) If p is odd and $p \neq 3$, or if $p = 2$ and $r \equiv 3 \pmod 4$, then all the proper $\overline{\mathbb{F}}S$-submodules form the chain $J < D^{\perp} < D < A$.
(2) If $p = 2$ and $r \equiv 1 \pmod 4$, then D/J and $D^{\perp}/J$ are nonisomorphic irreducible modules and their direct sum is $\overline{A} = A/J$.
(3) If $p = 3$, then $J < D^{\perp} < D < A$, and $D/D^{\perp}$ is an irreducible $\overline{\mathbb{F}}\mathrm{PGU}_3(r)$-module which splits into the direct sum of 3 irreducible $\overline{\mathbb{F}}S$-submodules.

Theorem 4.10. *Take notation as above. Then* $\mathrm{soc}(G)$ *can not be* $S = \mathrm{PSU}_3(r)$, $r > 2$.

Proof. We continue with the above arguments. For the cases (1) and (2) listed preceding this theorem, D and $D^{\perp}$ are all the proper $\overline{\mathbb{F}}S$-submodules of M of dimension larger than 1, which we have excluded in Lemma 4.9. It remains to consider the case $p = 3$. We have $D^{\perp} < C, C^{\perp} < D$ by Lemma 4.9. By the information about the decomposition matrix of the irreducible complex character χ_{q^3} (corresponding to A) in [38], we deduce that $D/D^{\perp} = V_1 \oplus V_2 \oplus V_3$, where the V_i's are pairwise nonisomorphic irreducible $\overline{\mathbb{F}}S$-submodules of dimension $m = (r-1)(r^2 - r + 1)/3$. The fact the V_i's are nonisomorphic $\overline{\mathbb{F}}S$-modules also follows from [28, Lemma 3.14]. It follows that $C/D^{\perp}$, $C^{\perp}/D^{\perp}$ are the direct sums of one or two of the V_i's, and so $k = \dim(C) =$

$r^2 - r + 1 + im$ for some $i \in \{1, 2\}$. By considering $C^\perp$ instead of C if necessary, we assume $i = 1$ without loss of generality.

Let σ be as defined in (2.2) with $p = 3$. Then σ fixes $\mathbf{1}_B$ for each block B, and so it stabilizes both D and $D^\perp$. There are exactly three candidate modules for C, and σ permutes them by Lemma 2.7. It follows that either $\sigma^2(C) = C$ or $\sigma^3(C) = C$. By Lemma 2.9, we deduce that $n = r^3 + 1 \leq 2 \cdot 3^3 - 2 = 52$. On the other hand, we have $r > 3$ since $3 \mid r + 1$ by Table 3.2, a contradiction. □

4.6. **The case $S = {}^2G_2(3^{2a+1})$, $a \geq 1$.** Let $r = 3^{2a+1}$ with $a \geq 1$, and set $m = 3^{a+1}$. In this case, we have $n = |\Omega| = r^3 + 1$, $S = {}^2G_2(3^{2a+1})$. The $\overline{\mathbb{F}}S$-submodule structure of $M = \overline{\mathbb{F}}^\Omega$ are available in Appendix D.2 of [23] and [31, Proposition 3.8]; see also [19, Section 4.3].

Lemma 4.11. *We have $p = 2$.*

Proof. By Table 3.2, either p is odd and p divides $r + 1$ or $r + m + 1$, or $p = 2$. Suppose to the contrary that p is odd. By [19, Section 4.3], the $\overline{\mathbb{F}}S$-submodules of M form a chain under inclusion. By Lemma 4.2, we deduce that $r^3 + 1 \leq 2p - 2$. It follows that $3^{6a+3} + 1 \leq 2 \cdot 3^{2a+1} + 2 \cdot 3^{a+1}$, which never holds for $a \geq 1$. This completes the proof. □

By [19, Section 4.3], there is a $\overline{\mathbb{F}}S$-submodule B of M such that $J < B < B^\perp < A$, where $J = \mathrm{soc}(M)$ and $B/J = \mathrm{soc}(M/J)$. Both J and B/J are irreducible. Moreover, there are pairwise nonisomorphic irreducible $\overline{\mathbb{F}}S$-modules U_1, U_2, U_1^* such that $B^\perp/B \cong U_1 \oplus U_2 \oplus U_1^*$, and $\dim(U_2) < \dim(U_1) = \dim(U_1^*)$.

Theorem 4.12. *Take notation as above. Then* $\mathrm{soc}(G)$ *can not be $S = {}^2G_2(3^{2a+1})$, $a \geq 1$.*

Proof. We continue with the above arguments. By Lemma 4.11, we have $p = 2$. Since $J = \mathrm{soc}(M)$ and $B/J = \mathrm{soc}(M/J)$ are irreducible, both C and $C^\perp$ contain B. Consequently, $B \leq C \leq B^\perp$ and $B \leq C^\perp \leq B^\perp$. Let σ be as defined in (2.2) with $p = 2$. By Lemma 2.7, $\sigma(B)$, $\sigma(C)$ and $\sigma(B^\perp)$ are also $\overline{\mathbb{F}}S$-submodules of M. By comparing dimensions, we deduce that $\sigma(B) = B$ and $\sigma(B^\perp) = B^\perp$. If $C = B$ or $B^\perp$, then $\sigma(C) = C$ by considering dimensions. By Lemma 2.9 we deduce that that $n = r^3 + 1 \leq 2p - 2 = 2$: a contradiction. Therefore, we have $B < C < B^\perp$. We similarly have $B < C^\perp < B^\perp$. By replacing C with $C^\perp$, we assume without loss of generality that $\dim(C) \leq \dim(C^\perp)$. Since $B^\perp/B \cong U_1 \oplus U_2 \oplus U_1^*$ and the three direct summands are nonisomorphic, we deduce that $C/B \in \{U_1, U_2, U_1^*\}$. By comparing dimensions, we deduce that either $C = \sigma(C)$, or $C = \sigma^2(C)$. By Lemma 2.9, we deduce that $r^3 + 1 \leq 2 \cdot 2^2 - 2 = 6$: a contradiction. This completes the proof. □

We have examined the six cases in Table 3.2 in Theorems 4.3, 4.6, 4.7, 4.8, 4.10 and 4.12 respectively, and this completes the proof of Theorem 4.1. Together with Proposition 3.4, this completes the proof of Theorem 1.3.

5. Conclusions

In this paper, we verify the MDS conjecture for $[n, k]_q$ codes $C \leq \mathbb{F}_q^\Omega$ with a 2-transitive permutation automorphism group $G = \mathrm{PAut}(C) \leq \mathrm{Sym}(\Omega)$. When (G, Ω) are the infinite

families of almost simple type in Table 3.2, then C is equivalent to the scalar extension of the hexacode from $\mathbb{F}_4$ to $\mathbb{F}_q$ in Example 1.2 (4). The codes in (2) and (3) of Example 1.2 admit 2-transitive permutation group G of affine type. The classification theorems in Section 4 heavily rely on the detailed information about the modular representations of the respective nonabelian simple groups. It is conceivably more challenging to determine all the MDS codes with a 2-transitive permutation group G of affine type, since such information is not available in general. We leave it an open problem to determine all the MDS codes with a 2-transitive permutation group.

Our main theorem, Theorem 1.3, initiates the study of MDS codes with a highly transitive permutation group. It will be of great theoretical interest to verify the MDS conjecture for linear codes that satisfy weaker symmetry hypotheses, particularly for cyclic codes. Further progress in this direction will require new insights and new techniques to overcome our heavy reliance on deep results in modular representation theory.

Acknowledgments. The authors used large language model to help with the understanding of modular representations of finite 2-transitive groups, and they are responsible for the correctness of all the results in this paper. This work is supported in part by the National Key R&D Program of China under Grant No. 2025YFA1017700. Haihua Deng is supported by the National Natural Science Foundation of China under Grant No. 123B2011, and the Postdoctoral Fellowship Program and China Postdoctoral Science Foundation under Grant No. BX20250059. The research of Andrey V. Vasil'ev was carried out within the framework of the Sobolev Institute of Mathematics project FWNF-2026-0017.

References

[1] S. Ball, *On sets of vectors of a finite vector space in which every subset of basis size is a basis*, J. Eur. Math. Soc. (JEMS) **14** (2012), no. 3, 733–748.

[2] S. Ball and M. Lavrauw, *Arcs in finite projective spaces*, EMS Surv. Math. Sci. **6** (2019), no. 1–2, 133–172.

[3] M. Bardoe and P. Sin, *The permutation modules for* $\mathrm{GL}(n+1,\mathbb{F}_q)$ *acting on* $\mathbb{P}^n(\mathbb{F}_q)$ *and* $\mathbb{F}_q^{n+1}$, J. London Math. Soc. (2) **61** (2000), no. 1, 58–80.

[4] T. P. Berger, *Groupes de permutations des codes MDS affine-invariants*, Comm. Algebra **21** (1993), no. 1, 239–254.

[5] R. Bienert and B. Klopsch, *Automorphism groups of cyclic codes*, J. Algebraic Combin. **31** (2010), no. 1, 33–52.

[6] A. Blokhuis, A. A. Bruen, and J. A. Thas, *On M.D.S. codes, arcs in* $\mathrm{PG}(n,q)$ *with q even, and a solution of three fundamental problems of B. Segre*, Invent. Math. **92** (1988), no. 3, 441–459.

[7] A. Blokhuis, A. A. Bruen, and J. A. Thas, *Arcs in* $\mathrm{PG}(n,q)$*, MDS-codes and three fundamental problems of B. Segre: some extensions*, Geom. Dedicata **35** (1990), 1–11.

[8] W. Bosma, J. J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3–4, 235–265.

[9] V. P. Burichenko, *Extensions of abelian 2-groups by means of* $\mathrm{L}_2(q)$ *with irreducible action*, Algebra and Logic **39** (2000), no. 3, 160–183.

[10] W. Burnside, *Theory of Groups of Finite Order*, 2nd ed., Cambridge University Press, Cambridge, 1911.

[11] K. A. Bush, *Orthogonal arrays of index unity*, Ann. Math. Statist. **23** (1952), no. 3, 426–434.

[12] P. J. Cameron, *Permutation Groups*, London Mathematical Society Student Texts, vol. 45, Cambridge University Press, Cambridge, 1999.

[13] N. Chigira, M. Harada, and M. Kitazume, *On the classification of extremal doubly even self-dual codes with 2-transitive automorphism groups*, Des. Codes Cryptogr. **73** (2014), no. 1, 33–35.

[14] A. Devillers, M. Giudici, D. R. Hawtin, L. Klawuhn, and L. Morgan, *Linear dimension of group actions*, arXiv:2512.16079 [math.GR], 2025.

[15] J. D. Dixon and B. Mortimer, *Permutation Groups*, Graduate Texts in Mathematics, vol. 163, Springer-Verlag, New York, 1996.

[16] T. Feng, H. D. L. Hollmann, W. Li, and Q. Xiang, *The permutation automorphism groups of irreducible cyclic codes*, arXiv:2603.01904 [math.CO], 2026.

[17] M. Geiselhart, A. Elkelesh, M. Ebada, S. Cammerer, and S. ten Brink, *Automorphism ensemble decoding of Reed–Muller codes*, IEEE Trans. Commun. **69** (2021), no. 10, 6424–6438.

[18] K. Guenda and T. A. Gulliver, *On the permutation groups of cyclic codes*, J. Algebraic Combin. **38** (2013), no. 1, 197–208.

[19] R. M. Guralnick and P. H. Tiep, *First cohomology groups of Chevalley groups in cross characteristic*, Ann. of Math. (2) **174** (2011), no. 1, 543–559.

[20] J. W. P. Hirschfeld and G. Korchmáros, *On the embedding of an arc into a conic in a finite plane*, Finite Fields Appl. **2** (1996), 274–292.

[21] J. W. P. Hirschfeld and G. Korchmáros, *On the number of rational points on an algebraic curve over a finite field*, Bull. Belg. Math. Soc. Simon Stevin **5** (1998), 313–340.

[22] J. W. P. Hirschfeld and J. A. Thas, *General Galois Geometries*, Clarendon Press, Oxford, 1991.

[23] G. Hiss, *Zerlegungszahlen endlicher Gruppen vom Lie-Typ in nicht-definierender Charakteristik*, Habilitationsschrift, RWTH Aachen, 1990.

[24] G. Hiss, *Hermitian function fields, classical unitals, and representations of 3-dimensional unitary groups*, Indag. Math. (N.S.) **15** (2004), no. 2, 223–243.

[25] W. C. Huffman, *Codes and groups*, in *Handbook of Coding Theory*, vol. 2, edited by V. S. Pless, W. C. Huffman, and R. A. Brualdi, pp. 1345–1440, North-Holland, Amsterdam, 1998.

[26] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, Cambridge, 2003.

[27] T. Kaufman and A. Lubotzky, *Edge transitive Ramanujan graphs and symmetric LDPC good codes*, in *STOC'12—Proceedings of the 2012 ACM Symposium on Theory of Computing*, pp. 359–366, ACM, New York, 2012.

[28] A. S. Kleshchev and P. H. Tiep, *Representations of finite special linear groups in non-defining characteristic*, Adv. Math. **220** (2009), no. 2, 478–504.

[29] W. D. Knapp and B. G. Rodrigues, *A useful tool for constructing linear codes*, J. Algebra **585** (2021), 422–446.

[30] W. Knapp and P. Schmid, *Codes with prescribed permutation group*, J. Algebra **67** (1980), no. 2, 415–435.

[31] P. Landrock and G. O. Michler, *Principal 2-blocks of the simple groups of Ree type*, Trans. Amer. Math. Soc. **260** (1980), no. 1, 83–111.

[32] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd ed., Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, Cambridge, 1997.

[33] J. Ma and G. Yan, *On automorphism groups of binary cyclic codes*, Des. Codes Cryptogr. **93** (2025), no. 5, 1271–1282.

[34] F. J. MacWilliams, *Permutation decoding of systematic codes*, Bell System Tech. J. **43** (1964), no. 1, 485–505.

[35] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.

[36] A. Malevich and W. Willems, *On the classification of the extremal self-dual codes over small fields with* 2*-transitive automorphism groups*, Des. Codes Cryptogr. **70** (2014), no. 1–2, 69–76.

[37] B. Mortimer, *The modular permutation representations of the known doubly transitive groups*, Proc. London Math. Soc. (3) **41** (1980), no. 1, 1–20.

[38] T. Okuyama and K. Waki, *Decomposition numbers of* $\mathrm{SU}(3, q^2)$, J. Algebra **255** (2002), no. 2, 258–270.

[39] N. Pace and A. Sonnino, *On linear codes admitting large automorphism groups*, Des. Codes Cryptogr. **83** (2017), no. 1, 115–143.

[40] N. S. N. Sastry and P. Sin, *On the doubly transitive permutation representations of* $\mathrm{Sp}(2n, \mathbb{F}_2)$, J. Algebra **257** (2002), no. 2, 509–527.

[41] B. Segre, *Curve razionali normali e k-archi negli spazi finiti*, Ann. Mat. Pura Appl. **39** (1955), 357–379.

[42] R. C. Singleton, *Maximum distance q-nary codes*, IEEE Trans. Inform. Theory **10** (1964), 116–118.

[43] L. Storme and J. A. Thas, *M.D.S. codes and arcs in* $\mathrm{PG}(n, q)$ *with q even: an improvement of the bounds of Bruen, Thas, and Blokhuis*, J. Combin. Theory Ser. A **62** (1993), no. 1, 139–154.

[44] J. F. Voloch, *Complete arcs in Galois planes of non-square order*, in *Advances in Finite Geometries and Designs*, edited by J. W. P. Hirschfeld, D. R. Hughes, and J. A. Thas, pp. 401–406, Oxford University Press, Oxford, 1991.

Haihua Deng, School of Mathematical Sciences, Zhejiang University, 866 Yuhangtang Road, Hangzhou 310058, Zhejiang, China

Email address: haihua.deng@zju.edu.cn

Tao Feng, School of Mathematical Sciences, Zhejiang University, 866 Yuhangtang Road, Hangzhou 310058, Zhejiang, China

Email address: tfeng@zju.edu.cn

Andrey V. Vasil'ev, Sobolev Institute of Mathematics, Novosibirsk, 630000, Russia

Email address: vasand@math.nsc.ru