Innovations in Incidence Geometry
Volume 1 (2005), Pages 197–219
ISSN 1781-6475

On dimensional dual hyperovals $\mathcal{S}^{d+1}_{\sigma,\phi}$

Hiroaki Taniguchi   Satoshi Yoshiara

Abstract

A d-dimensional dual hyperoval $\mathcal{S}^{d+1}_{\sigma,\phi}$ inside $PG(2d+1,2)$ ($d \geq 2$) is constructed in [5], for a generator σ of $\mathrm{Gal}(GF(q)/GF(2))$ and an o-polynomial $\phi(X)$ of $GF(q)[X]$ ($q = 2^{d+1}$). There, its automorphism group is determined and a criterion is given for these dimensional dual hyperovals to be isomorphic, assuming that the map ϕ on $GF(q)$ induced by $\phi(X)$ lies in $\mathrm{Gal}(GF(q)/GF(2))$. In this paper, we extend these results for a monomial o-polynomial ϕ. We show that $\mathrm{Aut}(\mathcal{S}^{d+1}_{\sigma,\phi}) \cong GL_3(2)$ or $Z_{q-1}.Z_{d+1}$ according as $d = 2$ or $d \geq 3$, if $\phi(X)$ is monomial but $\phi \not\in \mathrm{Gal}(GF(q)/GF(2))$. In particular, a special member $X(0)$ of $\mathcal{S}^{d+1}_{\sigma,\phi}$ is always fixed by any automorphism of $\mathcal{S}^{d+1}_{\sigma,\phi}$. Furthermore, $\mathcal{S}^{d+1}_{\sigma,\phi} \cong \mathcal{S}^{d+1}_{\sigma',\phi'}$ if and only if either $(\sigma,\phi) = (\sigma',\phi')$ or $\sigma\sigma' = \phi\phi' = \mathrm{id}$.

Keywords: dimensional dual hyperoval, o-polynomial

MSC 2000: 51,12,20

1 Introduction

A d-dimensional dual hyperoval with ambient space $PG(n,q)$ is defined to be a family $\mathcal{S}$ of $((q^{d+1}-1)/(q-1))+1$ d-subspaces of $PG(n,q)$ enjoying the following properties:

(1) any two distinct members of $\mathcal{S}$ intersect in a projective point.

(2) any three mutually distinct members of $\mathcal{S}$ intersect trivially.

(3) the members of $\mathcal{S}$ span $PG(n,q)$.

For a generator σ of $\mathrm{Gal}(GF(q)/GF(2))$ and an o-polynomial $\phi(X)$ over $GF(q)$ ($q = 2^{d+1}$), one can construct a d-dimensional dual hyperoval $\mathcal{S}^{d+1}_{\sigma,\phi}$

inside $PG(2d+1,2)$ by [5, Lemma 1]. (See also Proposition 2.1). When the permutation ϕ on $GF(q)$ induced by $\phi(X)$ lies in $\mathrm{Gal}(GF(q)/GF(2))$, its automorphism group is determined [5, Proposition 7]. Furthermore, for $\sigma, \sigma', \phi, \phi'$ generating $\mathrm{Gal}(GF(q)/GF(2))$, it is shown that $\mathcal{S}^{d+1}_{\sigma,\phi}$ is isomorphic to $\mathcal{S}^{d+1}_{\sigma',\phi'}$ if and only if either $(\sigma,\phi) = (\sigma',\phi')$ or $\sigma\sigma' = \phi\phi' = \mathrm{id}$ [5, Proposition 11]. In this paper we extended these results to the case when ϕ and ϕ' are induced by monomial o-polynomials. We always assume that $d \geq 2$.

Theorem 1.1. *Let ϕ be a bijection on $GF(q)$ induced by a monomial o-polynomial which is not contained in $\mathrm{Gal}(GF(q)/GF(2))$. Then $G = \mathrm{Aut}(\mathcal{S}^{d+1}_{\sigma,\phi})$ stabilizes $X(0)$. We have $G \cong GL_3(2)$ if $d = 2$, while $G \cong Z_{q-1} : Z_{d+1}$ for $d \geq 3$.*

Theorem 1.2. *Let σ and σ' be generators of $\mathrm{Gal}(GF(q)/GF(2))$, and let $\phi(X)$ and $\phi'(X)$ be monomial o-polynomials in $GF(q)[X]$ such that neither ϕ nor ϕ is contained in $\mathrm{Gal}(GF(q)/GF(2))$.*

Then two dimensional dual hyperovals $\mathcal{S}^{d+1}_{\sigma,\phi}$ and $\mathcal{S}^{d+1}_{\sigma',\phi'}$ are isomorphic if and only if either $(\sigma,\phi) = (\sigma',\phi')$ or $\sigma\sigma' = \phi\phi' = \mathrm{id}_{GF(q)}$.

Recall that two d-dimensional dual hyperovals $\mathcal{S}$ and $\mathcal{S}'$ with common ambient space $PG(V)$, where V is a vector space over $GF(2)$, are called *isomorphic* if there is a $GF(2)$-linear map f of V sending every member of $\mathcal{S}$ to a member of $\mathcal{S}'$.

Theorem 1.1 shows that $\mathcal{S}^{d+1}_{\sigma,\phi}$ is never isomorphic to $\mathcal{S}^{d+1}_{\sigma',\phi'}$ if ϕ' is contained in $\mathrm{Gal}(GF(q)/GF(2))$ but ϕ is not, because $\mathrm{Aut}(\mathcal{S}^{d+1}_{\sigma,\phi})$ fixes the special member $X(0)$, while $\mathrm{Aut}(\mathcal{S}^{d+1}_{\sigma',\phi'})$ is doubly transitive on the members of $\mathcal{S}^{d+1}_{\sigma',\phi'}$ [5, Proposition 7]. Thus Theorem 1.2 together with [5, Proposition 11] gives a criterion for two dimensional dual hyperovals $\mathcal{S}^{d+1}_{\sigma,\phi}$ and $\mathcal{S}^{d+1}_{\sigma',\phi'}$ to be isomorphic, if both ϕ and ϕ' are multiplicative o-polynomials.

The subsidiary aim of this paper is to supply a corrected proof for [5, Lemma 6]. The original proof does not work, as it confuses the trace function for $GF(q)/GF(2)$ with that for $GF(2^k)/GF(2)$. Step 3 and Step 4 of the proof of Theorem 1.1 provide a proof for [5, Lemma 6], as they do not assume that $\phi \notin \mathrm{Gal}(GF(q)/GF(2))$. When $\phi \in \mathrm{Gal}(GF(q)/GF(2))$, we have an explicit group T of translations [5, Section 4]. One can also establish Step 3 by showing that T is normal in G, because then $C_V(T) = X(\infty)$ is G-invariant.

Two new ideas are used to establish Theorem 1.1. One is to exploit a classical result [2] on a group with a split BN-pair of rank one, namely a doubly transitive group in which one point stabilizer contains a normal subgroup acting regularly on the remaining points. The other is to show the invariance of a certain subspace $X(\infty)$ of the ambient space under some automorphism groups, using Lemma 2.3.

The proof of Theorem 1.2 is along the same line with the proof of [5, Proposition 11]. However, we are required more careful treatment because $GF(q)$ is not necessarily generated by $b^{(\sigma\phi-1)/(\phi-1)}$ ($b \in GF(q)^\times$) (compare Step 3 with the third paragraph of the proof of [5, proposition 11]). We exploit a polynomial representation of a certain function to overcome this difficulty (see Step 4). Furthermore, Lemma 2.3 is used to simplify reduction arguments in Step 1.

The next section provides the definition of $\mathcal{S}^{d+1}_{\sigma,\phi}$ with the description of its ambient space (Proposition 2.1). It also supplies the notation used throughout the paper and Lemma 2.3. Sections 3 and 4 are respectively devoted to the proofs of Theorems 1.1 and 1.2. In the last section, Proposition 5.1 is given which explains why we require that σ is a generator of $\mathrm{Gal}(GF(q)/GF(2))$ and $\phi(X)$ is an o-polynomial in the definition of $\mathcal{S}^{d+1}_{\sigma,\phi}$.

2 Preliminaries

Throughout this paper, let $q = 2^{d+1}$ be a power of 2 with $d \geq 2$. Let σ be an automorphism of $GF(q)$ over $GF(2)$ defined by

$$x^\sigma = x^{2^m} \text{ for some integer } m \in \{1, \dots, d\} \text{ with } (m, d+1) = 1.$$

Then σ is a generator of the Galois group for an extension $GF(q)/GF(2)$, whence the map

$$\sigma - 1 : GF(q)^\times \ni x \mapsto x^\sigma/x \in GF(q)^\times$$

is a bijection preserving each subfield of $GF(q)$. The inverse map of $\sigma - 1$ is denoted $1/(\sigma - 1)$.

Choose an *o-polynomial* $\phi(X)$ in $GF(q)[X]$, namely, $\phi(X)$ is a permutation polynomial with $\phi(0) = 0$ and $\phi(1) = 1$, and the polynomial ϕ_s defined by $\phi_s(X) := (\phi(X+s) - \phi(s))/X$ for every $s \in GF(q)$ is a permutation polynomial. If ϕ is a *monomial* polynomial, that is, $\phi(X) = X^N$ for some integer N in $\{2, \dots, q-2\}$, it is an o-polynomial if and only if the following three conditions are satisfied:

$$(N, q-1) = (N-1, q-1) = 1 \text{ and } \phi_1(X) \text{ is a permutation polynomial.}$$

We use the same letter ϕ to denote the bijection on $GF(q)$ induced by $\phi(X)$: $x^\phi = \phi(x)$ for all $x \in GF(q)$. Then the map

$$\phi - 1 : GF(q)^\times \ni x \mapsto x^\phi/x \in GF(q)^\times$$

is a bijection, because it is induced by the polynomial $\phi_0(X)$. The inverse map of $\phi - 1$ is denoted $1/(\phi - 1)$. Note that if ϕ is a monomial o-polynomial, then

$\phi - 1$ is multiplicative, whence it induces an automorphism of a multiplicative group $GF(q)^{\times}$. In particular, it preserves the order of each element of $GF(q)^{\times}$, whence it preserves each subfield of $GF(q)$.

Throughout this paper, we use $\mathrm{Tr} = \mathrm{Tr}_{GF(q)/GF(2)}$ to denote the trace function for the field extension $GF(q)/GF(2)$. Furthermore, we regard

$$V := GF(q) \oplus GF(q) = \{(x, y) \mid x, y \in GF(q)\}$$

as a $2(d+1)$-dimensional vector space over $GF(2)$.

Proposition 2.1. *Let σ be a generator of $\mathrm{Gal}(GF(q)/GF(2))$ with $q = 2^{d+1}$, $d \geq 2$, and let $\phi(X)$ be an o-polynomial $\phi(X)$ of $GF(q)[X]$. For each $t \in GF(q)$, define a subspace $X(t)$ of V by*

$$X(t) := \{(x, x^{\sigma}t + xt^{\phi}) \mid x \in GF(q)\}.$$

Then the family $\mathcal{S}^{d+1}_{\sigma,\phi} := \{X(t) \mid t \in GF(q)\}$ is a d-dimensional dual hyperoval with ambient space $PG(W)$ or $PG(V)$, according as $\sigma\phi$ is the identity on $GF(q)$ or not, where $W = \{(x, y) \mid \mathrm{Tr}(y) = 0\}$ is a hyperplane of V.

Proof. Except the statement for the ambient space, Proposition was shown in [5, Lemma 1]. This part is also verified in view of the following expression of intersections of two members.

$$X(0) \cap X(t) = [(t^{(\phi-1)/(\sigma-1)}, 0)] = [(\phi_0(t)^{1/(\sigma-1)}, 0)]. \tag{1}$$

$$X(s) \cap X(t) = [\left((\frac{s^{\phi} + t^{\phi}}{s+t})^{1/(\sigma-1)}, (\frac{s^{\phi} + t^{\phi}}{s+t})^{1/(\sigma-1)} (\frac{s^{\phi}t + t^{\phi}s}{s+t}) \right)]. \tag{2}$$

We will determine the subspace $U := \langle X(t) \mid t \in GF(q) \rangle$ of V. For each $t \in GF(q)^{\times}$, we set $A(t) := \{x^{\sigma}t + xt^{\phi} \mid x \in GF(q)\}$. It is straightforward to verify that $A(t) = \{x \in GF(q) \mid \mathrm{Tr}(t^{(1-\phi\sigma)/(\sigma-1)}x) = 0\}$ for every $t \in GF(q)^{\times}$. Consider $A := \langle A(t) \mid t \in GF(q) \rangle$, the subspace of $GF(q)$ consisting of sums of elements in $A(t)$'s. As $\langle X(0), X(t) \rangle = \{(x, y) \mid x \in GF(q), y \in A(t)\}$, we have $U = \{(x, y) \mid x \in GF(q), y \in A\}$. As $A(1) = \{x \in GF(q) \mid \mathrm{Tr}(x) = 0\}$ is a hyperplane of $GF(q)$, we have either $A = GF(q)$ or $A = A(1)$. Accordingly we have $U = V$ or $U = W$.

Assume that $U = W$. Then $A = A(1) = A(t)$ for all $t \in GF(q)^{\times}$. It is well known that every hyperplane of $GF(q)$ is uniquely written as the kernel of the $GF(2)$-linear form $x \mapsto \mathrm{Tr}(ax)$ for some $a \in GF(q)^{\times}$. Thus we have $t^{(1-\phi\sigma)/(\sigma-1)} = 1$, or equivalently $t^{\phi\sigma} = t$ for all $t \in GF(q)^{\times}$. Thus $\phi\sigma = \mathrm{id}$ on $GF(q)$. Conversely if $\phi = \sigma^{-1}$, we have $A(t) = A(1)$ for all $t \in GF(q)^{\times}$, whence $A = A(1)$ and $U = W$. ∎

We sometimes denote $\mathcal{S}^{d+1}_{\sigma,\phi}$ by $\mathcal{S}^{d+1}_{2^m,N}$, where m and N are integers such that $x^\sigma = x^{2^m}$ and $x^\phi = x^N$ for all $x \in GF(q)$.

The 'if' part of Theorem 1.2 holds under mild restriction for o-polynomials ϕ and ϕ'.

Lemma 2.2. *Let σ and σ' be generators of $\mathrm{Gal}(GF(q)/GF(2))$, and let $\phi(X)$ and $\phi'(X)$ be o-polynomials in $GF(q)[X]$ with $\phi, \phi' \notin \mathrm{Gal}(GF(q)/GF(2))$. Assume that $\sigma'\phi = \phi\sigma'$.*

If either $(\sigma, \phi) = (\sigma', \phi')$ or $\sigma\sigma' = \phi\phi' = \mathrm{id}_{GF(q)}$, then $\mathcal{S}^{d+1}_{\sigma,\phi}$ and $\mathcal{S}^{d+1}_{\sigma',\phi'}$ are isomorphic.

Proof. If $\sigma = \sigma'$ and $\phi = \phi'$, the dimensional dual hyperovals $\mathcal{S} := \mathcal{S}^{d+1}_{\sigma,\phi}$ and $\mathcal{S}' := \mathcal{S}^{d+1}_{\sigma',\phi'}$ are identical. If $\sigma\sigma' = \mathrm{id} = \phi\phi'$, consider the $GF(2)$-linear bijection τ on V given by $(x, y) \mapsto (x, y^{\sigma'})$. Then a vector $(x, x^\sigma t + xt^\phi)$ of $X(t)$ is sent under τ to a vector $(x, xt^{\sigma'} + x^{\sigma'} t^{\phi\sigma'})$. As $\sigma'\phi = \phi\sigma'$, we have $x(t^{\phi\sigma'})^{\phi'} = x(t^{\sigma'\phi\phi'}) = xt^{\sigma'}$. Then $(x, xt^{\sigma'} + x^{\sigma'} t^{\phi\sigma'})$ lies in a member $X(t^{\phi\sigma'})$ of $\mathcal{S}^{d+1}_{\sigma',\phi'}$. Thus τ sends each $X(t)$ to $X(t^{\phi\sigma'})$, whence it induces an isomorphism of $\mathcal{S}$ with $\mathcal{S}'$. □

Now we specialize the case when both ϕ and ϕ' are monomial o-polynomials. We introduce important automorphisms m_b and f_θ of $\mathrm{Aut}(\mathcal{S}^{d+1}_{\sigma,\phi})$ defined for $b \in GF(q)^\times$ and $\theta \in \mathrm{Gal}(GF(q)/GF(2))$:

$$m_b : \ (x, y) \mapsto (bx, b^{(\sigma\phi-1)/(\phi-1)} y) \tag{3}$$

$$f_\theta : \ (x, y) \mapsto (x^\theta, y^\theta) \tag{4}$$

Observe that for $t \in G(q)$, $b \in GF(q)^\times$, $\theta \in \mathrm{Gal}(GF(q)/GF(2))$ we have

$$X(t)^{m_b} = X(b^{(\sigma-1)/(\phi-1)} t), \tag{5}$$

$$X(t)^{f_\theta} = X(t^\theta). \tag{6}$$

In the sequel, we set as follows:

$\mathcal{S} := \mathcal{S}^{d+1}_{\sigma,\phi}$, $G := \mathrm{Aut}(\mathcal{S})$ and $A :=$ the stabilizer of $X(0)$ in G.
$M := \{m_b \mid b \in GF(q)^\times\}$ and $F := \{f_\theta \mid \theta \in \mathrm{Gal}(GF(q)/GF(2))\}$.

The group M is a cyclic group generated by m_η for a generator η of $GF(q)^\times$, because we have $m_{bb'} = m_b m_{b'}$ from Equation (3). The group F of 'field' automorphisms, which is isomorphic to the cyclic group of order $d + 1$, normalizes M. We have $A \geq MF \cong Z_{q-1} : Z_{d+1}$.

As both σ and ϕ are induced by monomial polynomials, they induce automorphisms of the multiplicative group $GF(q)^\times$. Moreover $\phi-1$ and $1/(\phi-1)$ induce automorphisms of $GF(q)^\times$. Suppose $b^{(\sigma-1)/(\phi-1)} = 1$ for some $b \in GF(q)^\times$. Then $b^\sigma/b = 1$ and $b^\sigma = b$. Thus $b = 1$, as σ generates $\mathrm{Gal}(GF(q)/GF(2))$. Hence it follows from Equation (5) that the cyclic group M is a subgroup of A acting regularly on the members of $\mathcal{S} \setminus \{X(0)\}$.

Consider the following map

$$(\sigma\phi - 1)/(\phi - 1) : GF(q)^\times \ni x \mapsto x^{(\sigma\phi-1)/(\phi-1)} \in GF(q)^\times. \tag{7}$$

It is a multiplicative homomorphism of $GF(q)^\times$. Thus it preserves every subfield of $GF(q)$. The map $(\sigma\phi - 1)/(\phi - 1)$ is not necessarily injective. However, it is never additive, because of the following lemma applied to $GF(q)$ itself.

Lemma 2.3. *Let σ be a generator of $\mathrm{Gal}(GF(q)/GF(2))$ and let $\phi(X)$ be a monomial o-polynomial in $GF(q)[X]$. Then for every non-prime subfield $GF(2^k)$ of $GF(q)$, the restriction of the map $(\sigma\phi - 1)/(\phi - 1)$ on $GF(2^k)$ does not coincide with any automorphism in $\mathrm{Gal}(GF(2^k)/GF(2))$.*

Proof. We denote the restriction of σ and ϕ on $GF(2^k)$ by the same letters. Then σ is a generator of $\mathrm{Gal}(GF(2^k)/GF(2))$ and ϕ is induced by a monomial o-polynomial in $GF(2^k)[X]$, written also as $\phi(X)$. There exists an integer m with $1 \leq m \leq k-1$ coprime with k such that $x^\sigma = x^{2^m}$ for all $x \in GF(2^k)$. As $GF(2^k) \neq GF(2)$, σ is not the identity and $\sigma - 1$ is bijective on $GF(2^k)$. Then $(\sigma\phi - 1)/(\phi - 1)$ is not the identity on $GF(2^k)$, for otherwise we would have $(\sigma - 1)\phi = 0$, whence $x^\phi = 1$ for every $x \in GF(q)$, as $\sigma - 1$ is bijective on $GF(2^k)$.

Suppose $(\sigma\phi - 1)/(\phi - 1)$ coincides with $\tau^{-1} \in \mathrm{Gal}(GF(2^k)/GF(2))$. By the above remark, $\tau \neq \mathrm{id}$, so that there exists an integer l with $1 \leq l \leq k-1$ such that $x^\tau = x^{2^l}$ for all $x \in GF(2^k)$. In particular, $2 \leq m + l \leq 2(k-1)$. From $(\sigma\phi - 1)/(\phi - 1) = 1/\tau$,

$$(\sigma\tau - 1) = \phi^{-1}(\tau - 1). \tag{8}$$

Take an integer N with $1 \leq N \leq 2^k - 1$ such that $x^\phi = x^N$ for all $x \in GF(2^k)$. As ϕ is bijective on $GF(q)^\times$, N is prime to $2^k - 1$, whence the inverse of N modulo $2^k - 1$ exists. We denote it by N'. Namely N' is an integer with $1 \leq N' \leq 2^k - 1$ such that $NN' \equiv 1$ (modulo $2^k - 1$). Then Equation (8) is rewritten as

$$2^{m+l} - 1 \equiv N'(2^l - 1) \pmod{2^k - 1}. \tag{9}$$

Recall that $\phi^{-1}(X) = X^{N'}$ is also an o-polynomial (see e.g. [1, Result 8]). It follows from Glynn's criterion for monomial o-polynomials [1, Theorem A] that for every $d \in \{1, \ldots, 2^k - 2\}$, we have $d \not\preceq (dN' \pmod{2^k - 1})$ with respect to the following ordering $\preceq$ on $\{0, \ldots, 2^k - 1\}$.

For integers $a = \sum_{i=0}^{k-1} a_i 2^i$ and $b = \sum_{i=0}^{k-1} b_i 2^i$ with $a_i, b_i \in \{0,1\}$, we define $a \preceq b$ if and only if $a_i \leq b_i$ for all $i = 0, \ldots, k-1$.

Note that $(dN' \pmod{2^k - 1})$ denotes the unique integer M in $\{1, \ldots, 2^k - 1\}$ with $M \equiv dN'$ (modulo $2^k - 1$).

Assume that $2 \leq m + l \leq k$. Then $1 \leq 2^{m+l} - 1 \leq 2^k - 1$, whence we have $((2^l - 1)N' \pmod{2^k - 1}) = 2^{m+l} - 1$ by Equation (9). However, as $2^{m+l} - 1 = \sum_{i=0}^{m+l-1} 2^i$ and $2^l - 1 = \sum_{i=0}^{l-1} 2^i$, we have $2^l - 1 \preceq 2^{m+l} - 1$, which contradicts Glynn's criterion. Thus we have $k + 1 \leq m + l \leq 2(k-1)$. In this case, we consider the equation

$$(2^{m+l} - 1)N \equiv 2^l - 1 \pmod{2^k - 1},$$

equivalent to Equation (9). We have $2^{m+l} - 1 \equiv 2^f - 1$ (modulo $2^k - 1$), where $f := m + l - k$. Then $1 \leq f < l \leq k - 1$, as $m < k$. Since $2^l - 1 \equiv (2^{m+l} - 1)N \equiv (2^f - 1)N$ (modulo $2^k - 1$), we have $((2^f - 1)N \pmod{2^k - 1}) = 2^l - 1$. Then Glynn's criterion applied to $d = 2^f - 1$ yields that $\sum_{i=0}^{f-1} 2^i = 2^f - 1 \not\preceq 2^l - 1 = \sum_{i=0}^{l-1} 2^i$, which contradicts $f < l$. Hence we have contradiction in any case. $\square$

3 Automorphism group of $\mathcal{S}^{d+1}_{\sigma,\phi}$

In this section, we prove Theorem 1.1. We first treat the case when $d = 2$.

Step 1. *If $d = 2$, G fixes $X(0)$ and $G \cong GL_3(2)$.*

Proof. There are three monomial o-polynomials in $GF(8)[X]$: X^2, X^4 and X^6. Thus the only choice for $\phi(X)$ is X^6. As the map $x \mapsto x^4$ is the inverse map of the map $x \mapsto x^2$ on $GF(8)$, we have $\mathcal{S}^3_{2,6} \cong \mathcal{S}^3_{4,6}$ by Lemma 2.2. Thus we may assume that $\mathcal{S} = \mathcal{S}^3_{2,6}$.

Let η be a generator of $GF(8)^\times$ with $\eta^3 = \eta + 1$. Consider the following involutive $GF(2)$-linear transformation v on V:

$(1,0)^v = (1,0)$, $(\eta,0)^v = (\eta^2,0)$, $(\eta^2,0)^v = (\eta,0)$;
$(0,1)^v = (0,1)$, $(0,\eta)^v = (\eta+\eta^2,\eta)$, $(0,\eta^2)^v = (\eta^2,\eta+\eta^2)$.

Then we can verify that v induces the following permutation on the members of $\mathcal{S}$:

$$(X(0))(X(1))(X(\eta))(X(\eta^5))(X(\eta^2)X(\eta^4))(X(\eta^3)X(\eta^6)).$$

Now the stabilizer A of $X(0)$ in G is isomorphic to a subgroup of $GL_3(2)$, as A acts faithfully on $X(0)$ [5, Lemma 4(1)]. As A contains $MF \cong Z_7.Z_3$ and the above involution v, we have $A \cong GL_3(2)$. In particular, A acts doubly transitively on $\mathcal{S} \setminus \{X(0)\}$.

We can also verify that $\langle X(1), X(\eta)\rangle$ contains $X(\eta^5)$ but not $X(0)$. In particular, G does not act triply transitively on the members of $\mathcal{S}$. Thus G does not move $X(0)$, whence $G = A \cong GL_3(2)$. □

In the following, we consider the generic case with $d \geq 3$. We first determine the stabilizer A in G of $X(0)$. From Step 2 to Step 4, we do not assume that $\phi \notin \mathrm{Gal}(GF(q)/GF(2))$.

Step 2. *One of the following occurs.*

(1) $A = MF$.

(2) We have $d+1 = 2k$ *with* $k \geq 2$ *and* $A = LF$*, where* $L = Z \times S$ *is a normal subgroup of* A *isomorphic to* $GL_2(2^k)$ *with direct factors* $Z := Z(L) \cong Z_{2^k-1}$ *and* $S := L' \cong SL_2(2^k)$*. We also have* $|L \cap F| = |S \cap F| = 2$*.*

Proof. As A acts on $X(0)$ faithfully by [5, Lemma 4(1)], A is isomorphic to a subgroup of $GL(X(0)) \cong GL_{d+1}(2)$, regarding $X(0)$ as a $(d+1)$-dimensional space over $GF(2)$. Now M is a cyclic subgroup of order $q-1$ acting regularly on the nonzero vectors $(X(0) \cap X(t))^\times$ $(t \in GF(q)^\times)$ of $X(0)$, whence it is a Singer cycle of $GL(X(0))$. As A is a subgroup of $GL(X(0))$ containing a Singer cycle M on $X(0)$, it follows from Kantor's result [4] that A has a normal subgroup isomorphic to $GL_{(d+1)/e}(2^e)$ for some divisor e of $d+1$. If $e = d+1$, this normal subgroup coincides with the Singer cycle M, whence A is contained in the normalizer of M in $GL_{d+1}(2)$. It is easy to verify that the normalizer is MF. Thus in this case we have $A = MF$. Assume that $e < d+1$. As $d \geq 3$, one of the following holds from the arguments in [5, Lemma 5]:

(a) $d+1 = 4$ and $A \cong GL_{d+1}(2)$.

(b) $d+1 = 2k$ and A contains a normal subgroup isomorphic to $GL_2(2^k)$.

We eliminate Case (a) first. Assume that Case (a) holds. There are only three monomial o-polynomials in $GF(16)[X]$: X^2, X^8 and X^{14}. As $\mathcal{S}^4_{2,14}$ is isomorphic to $\mathcal{S}^4_{8,14}$ by Lemma 2.2, we may assume that $\mathcal{S} = \mathcal{S}^4_{2,14}$. Observe that for $t \in GF(16) \setminus GF(2)$

$$\langle X(0), X(1)\rangle \cap X(t) = \{(x, x^\sigma t + xt^\phi) \mid \mathrm{Tr}(x^\sigma t + xt^\phi) = 0\},$$

where Tr denotes the trace function for $GF(16)/GF(2)$. As $\mathrm{Tr}(x^\sigma t + xt^\phi) = \mathrm{Tr}(x^\sigma(t + t^{\phi\sigma}))$, the member $X(t)$ is contained in $\langle X(0), X(1)\rangle$ if and only if $t + t^{\phi\sigma} = t + t^{-2} = 0$, namely $t \in GF(4)^\times$. In particular, $\langle X(0), X(1)\rangle \cap X(t)$ is of dimension 4 or 3 according as $t \in GF(4)^{\times}$ or not. However, as $A \cong GL_4(2)$ is doubly transitive on $\mathcal{S} \setminus \{X(0)\}$, the stabilizer of $X(1)$ in A is transitive on $\mathcal{S}\setminus\{X(0), X(1)\}$, whence the dimension of $\langle X(0), X(1)\rangle \cap X(t)$ does not depend on the choice of $t \in GF(16) \setminus GF(2)$. This contradiction shows that Case (a) does not occur.

Assume that Case (b) occurs. As $d \geq 3$, we have $k \geq 2$. Let L be a normal subgroup of A isomorphic to $GL_2(2^k)$. Then $M \leq L$ and $L = Z \times S$, where $S \cong SL_2(2^k)$ and $Z = Z(L) \cong Z_{2^k-1}$. Let η be a generator of $GF(q)^{\times}$. Then $\zeta := \eta^{2^k+1}$ is a generator of $GF(2^k)^{\times}$ and m_ζ is a generator of Z. In particular, $Z \leq M$. Moreover, $M = Z \times (M \cap S)$, as $|Z| = 2^k - 1$ is coprime with $[M : Z] = 2^k + 1$.

A Singer cycle M in $GL(GF(q)) \cong GL_{d+1}(2)$ is self-centralizing. In particular, $C_A(L) \leq C_A(M) = M = Z \times (M \cap S)$. As S is simple and so $C_{M\cap S}(S) = 1$, we have $C_A(L) = Z$. Then $Z \leq C_A(S) \leq C_A(L) = Z$, whence $C_A(S) = Z$. Now A normalizes $S \cong \mathrm{Inn}(S)$, and hence $A/SC_A(S)$ is isomorphic to a subgroup of $\mathrm{Out}(S)$, which is known to be the group of field automorphisms induced by $\mathrm{Gal}(GF(2^k)/GF(2))$. Each element f_θ of F induces an automorphism on $GF(2^k)$. It induces a $GF(2^k)$-linear map on $GF(q)$ if and only if θ fixes every element of $GF(2^k)$, whence $\theta \in \langle \sigma^k \rangle$. Thus $F \cap L = \langle f_\sigma^k \rangle$ of order 2, which lies in S, as $[L : S] = 2^k - 1$ is odd. Then $F \cap L = F \cap S = \langle u \rangle$ with $u = (f_\sigma)^k$, and $F/(F \cap S)$ is isomorphic to $\mathrm{Out}(S)$. Thus $A/SC_A(S) \cong \mathrm{Out}(S) \cong F/(F \cap S)$, whence $A = (C_A(S) \times S)F = (Z \times S)F$. $\square$

Step 3. *A acts on* $X(\infty) := \{(0, y) \mid y \in GF(q)\}$.

Proof. This is clear if $A = MF$, as both M and F act on $X(\infty)$ in view of Equations (3) and (4). Thus we may assume that Case (2) occurs in Step 2. We use the notation there.

We first examine the Z-orbits on $V^{\times} := V \setminus \{0\}$. Regard $GF(q)$ as a 2-dimensional space over $GF(2^k)$ and let ζ_i $(i = 0, \dots, 2^k)$ be elements of $GF(q)^{\times}$ no two of which lie in the same 1-dimensional subspace over $GF(2^k)$ of $GF(q)$. For each ζ_i $(i = 0, \dots, 2^k)$ and $c \in GF(q)^{\times}$, set

$$Z(\zeta_i, c) := \{(\zeta_i x, c x^{(\sigma\phi-1)/(\phi-1)}) \mid x \in GF(2^k)^{\times}\}.$$

As $Z = \langle m_\zeta \rangle$, each $Z(\zeta_i, c)$ is a Z-orbit of length $2^k - 1$ from Equation (3). Moreover, it is easy to see that $X(0)^{\times}$ is a disjoint union of $Z(\zeta_i, 0)$ for $i = 0, \dots, 2^k$ and that $V \setminus (X(0) \cup X(\infty))$ is a disjoint union of $Z(\zeta_i, c)$ for $i = 0, \dots, 2^k$ and $c \in GF(q)^{\times}$. On the other hand, each Z-orbit in $X(\infty)^{\times}$ is of the form

$$Z(c) := \{(0, c y^{(\sigma\phi-1)/(\phi-1)} \mid y \in GF(2^k)^{\times}\}$$

for some $c \in GF(q)^\times$ by Equation (3). In particular, each Z-orbit in $X(\infty)^\times$ is of length l, where $l := {}^\#\{y^{(\sigma\phi-1)/(\phi-1)} \mid y \in GF(2^k)^\times\}$.

Suppose $l < 2^k - 1$. Then every Z-orbit in $X(\infty)^\times$ has length l, which is different from the length $2^k - 1$ of each Z-orbit in $V \setminus X(\infty)$. As Z is normal in A, every element of A permutes the Z-orbits in $V^\times$. Thus A acts on the union of Z-orbits of length l, which is $X(\infty)^\times$. Hence in this case A acts on $X(\infty)$.

Thus we may assume that $l = 2^k - 1$, that is, the restriction of a map $(\sigma\phi-1)/(\phi-1)$ on $GF(2^k)$ is a (multiplicative) bijection. We denote its inverse map by $(\phi-1)/(\sigma\phi-1)$.

Now take any involution v of S. As v stabilizes $X(0)$, there exist $GF(2)$-linear maps a, c, d on $GF(q)$ such that

$$(x, y)^v = (x^a + y^c, y^d) \tag{10}$$

for every $x, y \in GF(q)$. As v centralizes $Z = \{m_b \mid b \in GF(2^k)^\times\}$, Equations (3) and (10) show that $(x, y)^{m_b v} = ((bx)^a + (b^{(\sigma\phi-1)/(\phi-1)}y)^c, (b^{(\sigma\phi-1)/(\phi-1)}y)^d)$ coincides with $(x, y)^{v m_b} = (b \cdot x^a + b \cdot y^c, (b^{(\sigma\phi-1)/(\phi-1)}) \cdot y^d)$ for all $b \in GF(2^k)^\times$ and $x, y \in GF(q)$. In particular, we have $b \cdot y^c = (b^{(\sigma\phi-1)/(\phi-1)}y)^c$, or equivalently

$$(by)^c = (b^{(\phi-1)/(\sigma\phi-1)}) \cdot y^c \tag{11}$$

for all $y \in GF(q)$ and $b \in GF(2^k)^\times$. From Equation (11) and the linearity of c, we have $(b_1 + b_2)^{(\phi-1)/(\sigma\phi-1)} \cdot y^c = ((b_1 + b_2)y)^c = (b_1 y)^c + (b_2 y)^c$, which is equal to $b_1^{(\phi-1)/(\sigma\phi-1)} \cdot y^c + b_2^{(\phi-1)/(\sigma\phi-1)} \cdot y^c$. Thus

$$((b_1 + b_2)^{(\phi-1)/(\sigma\phi-1)} + b_1^{(\phi-1)/(\sigma\phi-1)} + b_2^{(\phi-1)/(\sigma\phi-1)}) \cdot y^c = 0$$

for all $b_1 \neq b_2 \in GF(2^k)^\times$ and $y \in GF(q)$. If there exists $y \in GF(q)$ with $y^c \neq 0$, then we have

$$(b_1 + b_2)^{(\phi-1)/(\sigma\phi-1)} = b_1^{(\phi-1)/(\sigma\phi-1)} + b_2^{(\phi-1)/(\sigma\phi-1)}$$

for all $b_1 \neq b_2 \in GF(2^k)^\times$. Thus the map $(\phi - 1)/(\sigma\phi - 1)$ on $GF(2^k)$ is $GF(2)$-linear. Then its inverse map, which is $(\sigma\phi - 1)/(\phi - 1)$ restricted to $GF(2^k)$, is both multiplicative and additive on $GF(2^k)$. Thus it coincides with an automorphism τ in $\mathrm{Gal}(GF(2^k)/GF(2))$. However, this is impossible by Lemma 2.3, as $k \geq 2$. Hence we have $y^c = 0$ for all $y \in GF(q)$. This shows that the involution v acts on $X(\infty)$.

As $S \cong SL_2(2^k)$ is generated by involutions, the above conclusion implies that $A = (Z \times S)F$ also acts on $X(\infty)$. $\square$

Step 4. *Case (2) in Step 2 does not occur.*

Proof. By Step 3, $X(0)$ and $X(\infty)$ are A-invariant subspaces of V. As $V = X(0) \oplus X(\infty)$, for each $g \in A$ there are $GF(2)$-linear maps $\overline{g}$ and $\tilde{g}$ on $GF(q)$ such that

$$(x,y)^g = ((x)\overline{g}, (y)\tilde{g}) \tag{12}$$

for all $x, y \in GF(q)$. On the other hand, g induces a permutation on $\mathcal{S}$. We denote $X(t)^g = X(t\hat{g})$ for each $t \in GF(q)$. As $X(0) \cap X(t) = [(t^\varepsilon, 0)]$ with $\varepsilon := (\phi-1)/(\sigma-1)$, applying g to this equation we have $X(0) \cap X(t\hat{g}) = [(t^\varepsilon)\overline{g}, 0]$, whence $(t\hat{g})^\varepsilon = (t^\varepsilon)\overline{g}$. Thus we obtain the following relation for all $t \in GF(q)^\times$:

$$(t)\hat{g} = ((t^\varepsilon)\overline{g})^{1/\varepsilon}. \tag{13}$$

Each vector $(x, x^\sigma t^{1/\varepsilon} + xt^{\phi/\varepsilon})$ of $X(t^{1/\varepsilon})$ is mapped by g to the vector $(x\overline{g}, (x^\sigma t^{1/\varepsilon} + xt^{\phi/\varepsilon})\tilde{g})$, which lies in $X((t^{1/\varepsilon})\hat{g}) = X((t\overline{g})^{1/\varepsilon})$. Thus for all $t, x \in GF(q)^\times$ we have

$$(x^\sigma t^{1/\varepsilon} + xt^{\phi/\varepsilon})\tilde{g} = (x\overline{g})^\sigma (t\overline{g})^{1/\varepsilon} + (x\overline{g})(t\overline{g})^{\phi/\varepsilon}. \tag{14}$$

We now choose any element ρ from $GF(q) \backslash GF(2^k)$. Then $(1, \rho)$ forms a basis for a 2-dimensional vector space $GF(q)$ over $GF(2^k)$. Consider a $GF(2^k)$-linear map $l(\rho)$ on $GF(q)$ determined by $1 \mapsto 1$ and $\rho \mapsto 1 + \rho$. Then $l(\rho)$ is a $GF(2^k)$-linear involution on $GF(q)$ with determinant 1. We denote by $SL(GF(q))$ the group of $GF(2^k)$-linear bijections on $GF(q)$ with determinant 1. For every $a \in GF(2^k)^\times$, the involution $l(a^{-1}\rho)$ is represented as $\left(\begin{smallmatrix} 1 & 0 \\ a & 1 \end{smallmatrix}\right)$ with respect to a basis $(1, \rho)$ over $GF(2^k)$ for $GF(q)$. Thus $\{l(a^{-1}\rho) \mid a \in GF(2^k)^\times\}$ generates a Sylow 2-subgroup of $SL(GF(q)) \cong SL_2(2^k)$.

Now $S \cong SL_2(2^k)$ ($\leq A$) acts faithfully on $X(0)$, as every nonzero vector of $X(0)$ is expressed as $(X(0) \cap X(t))^\times$ for some $t \in GF(q)^\times$. Thus, identifying $X(0)$ with $GF(q)$ via $(x, 0) \mapsto x$, the map $g \mapsto \overline{g}$ gives an isomorphism of S with $SL(GF(q))$. Then the vectors of $X(0)$ fixed by an involution of S forms a k-dimensional subspace of $X(0)$ over $GF(2)$. Furthermore, for every $\rho \in GF(q) \setminus GF(2^k)$, there exists a unique involution $g = g(\rho)$ of S such that $\overline{g} = l(\rho)$. From the definition of $l(\rho)$, the subspace $\{(x, 0) \mid x \in GF(2^k)\}$ of $X(0)$ coincides with the subspace of vectors of $X(0)$ fixed by every $g(a\rho)$ ($a \in GF(2^k)^\times$).

The group S acts on $X(\infty)$ as well by Step 3. As the involution u in $F \cap S$ (see Step 2) induces on $X(\infty)$ the action $(0, y) \mapsto (0, y^{2^k})$ by Equation (4), the action of S is not trivial. As $k \geq 2$, S is simple, and hence the action of S on $X(\infty)$ is faithful as well. Identifying $X(\infty)$ with $GF(q)$ via $(0, x) \mapsto x$, the map $g \mapsto \tilde{g}$ gives an isomorphism from S to $SL(GF(q))$. In particular, there is a k-dimensional subspace K of $X(\infty)$ consisting of vectors fixed by $g(a\rho)$ for all $a \in GF(2^k)^\times$. As $l(a\rho)$ fixes each element of $GF(2^k)$ and ε preserves $GF(2^k)$, it follows from Equation (14) that vectors $(0, x^\sigma t^{1/\varepsilon} + xt^{\phi/\varepsilon})$ for all $x, t \in GF(2^k)$ lie in K. Note that, if $\sigma\phi$ is not the identity on $GF(2^k)$, these vectors span $GF(2^k)$ by the arguments in [5, Lemma 2], whence $K = \{(0, y) \mid GF(2^k)\}$.

We now claim:

$\sigma\phi$ is not the identity map on $GF(q)$.

For otherwise, $\eta^{(\sigma\phi-1)/(\phi-1)} = 1$ for a generator η of $GF(q)^\times$, whence a generator $m_\eta^{2^k-1}$ of a Singer cycle $M \cap S$ in S acts trivially on $X(\infty)$ from Equation (3). This contradicts the faithfulness of S on $X(\infty)$.

Next we claim:

if $\sigma\phi$ is not the identity map on $GF(2^k)$, then we have a contradiction.

To show the claim, take any $\rho \in GF(q)\setminus GF(2^k)$ and choose an involution $g \in S$ with $\overline{g} = l(\rho)$. By Equation (14), applying to this g, $x = \rho$ and $t = 1$, we have

$$(\rho^\sigma + \rho)\tilde{g} = (1 + \rho)^\sigma + (1 + \rho) = \rho^\sigma + \rho.$$

Thus for every $\rho \in GF(q) \setminus GF(2^k)$, the vector $(0, \rho + \rho^\sigma)$ lies in $K = \{(0, y) \mid y \in GF(2^k)\}$ by the remark above. As $x + x^\sigma = y + y^\sigma$ $(x, y \in GF(q))$ occurs exactly when $x + y = (x + y)^\sigma \in GF(2)$, there are $(q - 2^k)/2 = 2^{2k-1} - 2^{k-1}$ elements in the form $\rho + \rho^\sigma$ for some $\rho \in GF(q) \setminus GF(2^k)$. Hence we have $2^{2k-1} - 2^{k-1} \le 2^k$, from which $2^k \le 2 + 1 = 3$ or equivalently $k = 1$. However, this contradicts that $k \ge 2$.

Finally we claim:

if $\sigma\phi$ is the identity map on $GF(2^k)$, we have a contradiction as well.

In this case, the vectors $(0, x^\sigma t^{1/\varepsilon} + xt^{\phi/\varepsilon})$ for all $x, t \in GF(2^k)$ span a hyperplane $H := \{(0, y) \mid y \in GF(2^k), \mathrm{Tr}_{GF(2^k)/GF(2)}(y) = 0\}$ of the subspace $\{(0, y) \mid y \in GF(2^k)\}$. The corresponding hyperplane of $GF(2^k)$ is denoted H': $H' := \{y \in GF(2^k) \mid \mathrm{Tr}_{GF(2^k)/GF(2)}(y) = 0\}$.

Take any $\rho \in GF(q) \setminus GF(2^k)$. We claim that there are at least $2^{k-1} - 1$ elements $a \in GF(2^k)^\times$ such that $(a\rho) + (a\rho)^\sigma \in H'$. If $(a\rho) + (a\rho)^\sigma \in H'$ for all $a \in GF(2^k)$, this clearly holds. Thus we may assume that $\rho + \rho^\sigma \notin H'$, replacing ρ by its suitable multiple by an element of $GF(2^k)^\times$. The subspace of $X(\infty)$ fixed by $g(\rho)$ is $\{(0, y) \mid y \in K'\}$, where K' denotes the k-dimensional subspace of $GF(q)$ over $GF(2)$ spanned by $\rho + \rho^\sigma$ and all $y \in H'$. As we observed before, every vector of $\{(0, y) \mid y \in K'\}$ is fixed by $g(a\rho)$ for all $a \in GF(2^k)^\times$. If we replace ρ by $a\rho$ at the calculation of $\rho + \rho^\sigma$ in the proof of the last claim, we conclude that $(0, (a\rho) + (a\rho)^\sigma)$ is fixed by $g(a\rho)$. Hence

$$(a\rho) + (a\rho)^\sigma \in K'$$

for all $a \in GF(2^k)^\times$. Then we can define a map κ from $GF(2^k)$ to K' by $\kappa(a) := (a\rho)+(a\rho)^\sigma$. This is a $GF(2)$-linear map. It is injective, because $\kappa(a) = 0$ implies that $a\rho = (a\rho)^\sigma \in GF(2)$ but $a\rho \in GF(q)-GF(2^k)$ unless $a = 0$. Then κ is an isomorphism from $GF(2^k)$ with K'. In particular, there are exactly $2^{k-1}-1$ elements $a \in GF(2^k)^\times$ with $(a\rho) + (a\rho)^\sigma \in H'$.

Let $\rho_1, \ldots, \rho_m$ $(m = 2^k)$ be a set of representatives for projective points of a projective line $PG(GF(q))$, distinct from the projective point $[1] = GF(2^k)$, where we regard $GF(q)$ as a 2-dimensional vector space over $GF(2^k)$. The above paragraph shows that for each ρ_i $(i = 1, \ldots, m)$, there are at least $2^{k-1}-1$ elements $a \in GF(2^k)^\times$ such that $(a\rho_i)+(a\rho_i)^\sigma \in H'$. Remark that $(a\rho_i)+(a\rho_i)^\sigma$ lies in H' implies that it lies in $(H')^\times$, as $(a\rho_i) = (a\rho_i)^\sigma \in GF(2)$ would imply that $\rho_i \in GF(2^k)$.

Thus the number of nonzero vectors x in $GF(q) \setminus GF(2^k)$ satisfying $x + x^\sigma \in (H')^\times$ is at least $(2^{k-1} - 1)2^k$. As $x + x^\sigma = y + y^\sigma$ if and only if $x + y \in GF(2)$, we conclude that

$$2^k(2^{k-1} - 1)/2 \leq |(H')^\times| = 2^{k-1} - 1.$$

Then $k \leq 1$, which is a contradiction. $\square$

Remark 3.1. Up to the above step, we do not use the assumption that ϕ does not lie in $\mathrm{Gal}(GF(q)/GF(2))$. Thus the conclusion in Step 4 also holds in the case when $\phi = \tau$ is a generator of $\mathrm{Gal}(GF(q)/GF(2))$. This corresponds to [5, Lemma 6].

Note that the proof given there is incorrect, as it confuses the trace function for $GF(q)/GF(2)$ with that for $GF(2^k)/GF(2)$. Thus Step 2, Step 3, Step 4 provide a correction to the proof of [5, Lemma 6].

We have determined the structure of A as $A = MF$. Now suppose that $G = \mathrm{Aut}(\mathcal{S})$ contains an automorphism which sends $X(0)$ to a member of $\mathcal{S}\setminus\{X(0)\}$. Then G is doubly transitive on $\mathcal{S}$, as M is transitive on $\mathcal{S} \setminus \{X(0)\}$.

Step 5. *There is a normal subgroup N of G which acts regularly on $\mathcal{S}$. In particular, N is an elementary abelian 2-group of order $q = 2^{d+1}$.*

Proof. From Step 2, the one point stabilizer A of a doubly transitive group G has a normal subgroup M acting regularly on the remaining members. By a classical result [2] by Hering, Kantor and Seitz, such doubly transitive groups are classified. Thus G has a normal subgroup N which either acts regularly on $\mathcal{S}$ or is isomorphic to one of the following simple groups. In each case, the permutation representation of G on $\mathcal{S}$ is equivalent to its action via conjugation on the set of Sylow p-subgroups of N, where p is a prime dividing r:

$N \cong PSL_2(r)$, $Sz(r)$ ($r = 2^{2e+1}$), $PSU_3(r)$, or a group of Ree type ($^2G_2(r)$) with $r = 3^{2e+1}$.

Thus $|\mathcal{S}| = r+1$, r^2+1, r^3+1 or r^3+1, according as $N \cong PSL_2(r)$, $Sz(r)$, $PSU_3(r)$ or a group of Ree type. As $|\mathcal{S}| = 2^{d+1}$, N is not $Sz(r)$. If $N \cong PSU_3(r)$ or a group of Ree type, then $|\mathcal{S}| = 2^{d+1} = r^3+1 = (r+1)(r^2-r+1)$, whence both $r+1$ and r^2-r+1 are power of 2 larger than 1. However, $(r+1, r^2-r+1) = 1$ or 3, which is a contradiction. If $N \cong PSL_2(r)$ with $r+1 = 2^{d+1}$, the two point stabilizer is a cyclic group of order $(r-1)/2$. As the two point stabilizer in G is a cyclic group of order $d+1$, we conclude that $(2^{d+1}-2)/2 = 2^d - 1$ divides $d+1$, which occurs only when $d = 1$ or $d = 2$. This contradicts our assumption that $d \geq 3$.

Thus G has a regular normal subgroup N. Then N is an elementary abelian 2-subgroup of order 2^{d+1} by a standard argument. □

As N is a regular normal subgroup on $\mathcal{S}$, the action of A on $\mathcal{S} \setminus \{X(0)\}$ is equivalent to the action of A via conjugation on $N \setminus \{1\}$. In particular, the group M acts regularly on $N \setminus \{1\}$ under conjugation. Thus the dimensions of $[V, \tau'] := \{v + v^{\tau'} \mid v \in V\}$ for involutions τ' of N do not depend on the choice of τ'. We next observe the action of N on V, specifically the commutator subspace $[V, N] := \langle v + v^{\tau'} \mid \tau' \in N\rangle$. As N is normalized by G, the subspace $[V, N]$ is invariant under the action of G. By standard arguments for 2-groups, $[V, N]$ is a proper subspace of V.

Step 6. *We have $[V, N] = X(\infty)$. In particular, $X(\infty)$ is G-invariant.*

Proof. For short, we set $W = [V, N]$ for a while. (The arguments in the few paragraphs below work for any G-invariant proper subspace W of V. This fact will be used in Step 1 of the proof of Theorem 1.2.)

Assume that W contains a point of form $X(a) \cap X(b)$ for some $a \neq b \in GF(q)$. As G is doubly transitive on $\mathcal{S} = \{X(t) \mid t \in GF(q)\}$ and W is G-invariant, this implies that W contains $X(a) = \langle X(a) \cap X(b) \mid b \in GF(q) \setminus \{a\}\rangle$ for all $a \in GF(q)$, whence $W = \langle X(a) \mid a \in GF(q)\rangle = V$, a contradiction. Thus W does not contain a point of form $X(a) \cap X(b)$ for any $a \neq b \in GF(q)$, or equivalently $W \cap X(a) = \{(0,0)\}$ for all $a \in GF(q)$.

Assume now that W contains two vectors (x, y) and (x', y) for some $x \neq x'$ and $y \in GF(q)$. Then W contains $(x - x', 0) = (x, y) - (x', y)$, which is a nonzero vector of $X(0)$. This contradicts the above conclusion. Thus for each $y \in GF(q)$, there is at most one element $x \in GF(q)$ such that $(x, y) \in W$. Hence $|W| \leq q = 2^{d+1}$.

Now assume that W is not contained in $X(\infty)$. Then there is a vector (x, y) in W with $x \neq 0$. As W is invariant under M, it follows from the action of m_b (see

Equation (3)) that W contains a vector of form (x', y') for every $x' \in GF(q)$. Thus $|W| \geq q$.

Together with the above conclusions, we have either $W \leq X(\infty)$ or $\dim W = d{+}1$. Assume that W is not contained in $X(\infty)$. Then, as M acts on W, it follows from Equation (3) that $W = Y(c) := \{(x, cx^{(\phi\sigma-1)/(\phi-1)}) \mid x \in GF(q)\}$ for some $c \in GF(q)^{\times}$ (compare the arguments in [5, Lemma 10] with τ replaced by ϕ). However, then the map $(\sigma\phi - 1)/(\phi - 1)$ is additive on $GF(q)^{\times}$, as $Y(c)$ is a subspace. This contradicts Lemma 2.3. Thus we have $W \subseteq X(\infty)$.

Up to here, arguments can be applied to any G-invariant proper subspace W of V. Now we specialize to $[V, N]$.

As N acts regularly on $\mathcal{S}$, there is a unique involution $\tau(t)$ of N exchanging $X(0)$ and $X(t)$ for each $t \in GF(q)^{\times}$. Then $(x, 0) + (x, 0)^{\tau(t)} \in [X(0), \tau(t)] \leq [V, N]$. Notice here that $[V, N] = W \leq X(\infty) = \{(0, y) \mid y \in GF(q)\}$ by the conclusion in the previous paragraph. Thus $(x, 0)^{\tau(t)} = (x, y)$ for some $y \in GF(q)$. As $(x, 0)^{\tau(t)} \in X(0)^{\tau(t)} = X(t)$, we have $y = x^{\sigma}t + xt^{\phi}$. Hence

$$[X(0), \tau(t)] = \{(0, x^{\sigma}t + xt^{\phi}) \mid x \in GF(q)\}. \tag{15}$$

The map $X(0) \ni (x, 0) = v \mapsto v + v^{\tau(t)} \in [X(0), \tau(t)]$ is a $GF(2)$-linear surjection with kernel $C_{X(0)}(\tau(t)) = X(0) \cap X(t)$ of dimension 1. Thus $[X(0), \tau(t)]$ is a subspace of $[V, N]$ of dimension d. On the other hand, $[V, N]$ is contained in the $(d + 1)$-dimensional subspace $X(\infty)$ by the conclusion in the above paragraph. Thus we have either $\dim[V, N] = d$ or $[V, N] = X(\infty)$. In the former case, we have $[V, N] = [X(0), \tau(t)]$ for all $t \in G(q)^{\times}$. In particular, $[X(0), \tau(t)] = [X(0), \tau(1)]$. Then it follows from Equation (15) that for every $x \in GF(q)$ and $t \in GF(q)^{\times}$ we have $x^{\sigma}t + xt^{\phi} = y^{\sigma} + y$ for some $y \in GF(q)$. Thus $\mathrm{Tr}(x^{\sigma}t + xt^{\phi}) = 0$ for all $x \in GF(q)$ and $t \in GF(q)^{\times}$, where $\mathrm{Tr} = \mathrm{Tr}_{GF(q)/GF(2)}$. As $\mathrm{Tr}(x^{\sigma}t + xt^{\phi}) = \mathrm{Tr}(x^{\sigma}(t + t^{\phi\sigma}))$, this implies that $t = t^{\phi\sigma}$ for all $t \in GF(q)^{\times}$. Hence $\phi = \sigma^{-1} \in \mathrm{Gal}(GF(q)/GF(2))$, which contradicts our hypothesis. Thus we have $[V, N] = X(\infty)$. ☐

Step 7. *We have a contradiction, if G contains an automorphism sending $X(0)$ to a member distinct from $X(0)$.*

Proof. We denote by τ the unique involution of N which sends $X(0)$ to $X(1)$. From regularity of the action of N on $\mathcal{S}$, such an element uniquely exists. As N is an elementary abelian 2-group, τ is an involution and it exchanges $X(0)$ and $X(1)$.

We examine the action of τ on V. Since τ is $GF(2)$-linear on V and stabilizes $X(\infty)$ by Step 6, we can display the action of τ as follows.

$$(x, y)^{\tau} = (x^{a}, x^{b} + y^{d}), \tag{16}$$

where a, b and d are $GF(2)$-linear maps from $GF(q)$ to itself. They can be determined as follows. We have $(x, y) + (x, y)^{\tau} \in [V, \tau] \leq [V, N] = X(\infty)$, whence $x = x^{a}$ for every $x \in GF(q)$, that is, $a = \mathrm{id}$, the identity map on $GF(q)$. As $(x, 0)^{\tau} = (x, x^{b}) \in X(0)^{\tau} = X(1)$, we have $x^{b} = x^{\sigma} + x$ for every $x \in GF(q)$. Thus $b = \sigma + \mathrm{id}$. Then we have $(x, x^{\sigma} + x)^{\tau} = (x, x^{\sigma} + x + (x + x^{\sigma})^{d})$, which is a vector of $X(1)^{\tau} = X(0)$. Hence from the linearity of d we have $x + x^{d} = x^{\sigma} + x^{\sigma d}$ for all $x \in GF(q)$. Now remark that τ commutes with a generator f_{σ} of F, because both τ and $\tau^{f_{\sigma}}$ are involutions of N which send $X(0)$ to $X(1)$, whence $\tau = \tau^{f_{\sigma}}$. This implies that $x^{d\sigma} = x^{\sigma d}$ for all $x \in GF(q)$ from Equation (16). Then we have $x + x^{d} = x^{\sigma} + x^{d\sigma} = (x + x^{d})^{\sigma}$ for all $x \in GF(q)$. Hence $\varepsilon(x) := x + x^{d} \in GF(2)$ for all $x \in GF(2)$.

Summarizing, we have

$$(x, y)^{\tau} = (x, x^{\sigma} + x + y + \varepsilon(y)) \tag{17}$$

for all $x, y \in GF(q)$, where $\varepsilon(y)$ is an element of $GF(2)$ uniquely determined by y.

We write $X(t)^{\tau} = X(\bar{t})$ for $t \in GF(q)^{\times}$. From Equation (17), we have $(x, x^{\sigma}t + xt^{\phi})^{\tau} = (x, x^{\sigma} + x + x^{\sigma}t + xt^{\phi} + \varepsilon(x^{\sigma}t + xt^{\phi}))$, which lies in $X(t)^{\tau} = X(\bar{t})$. Thus

$$x^{\sigma}(\bar{t} + t + 1) + x((\bar{t})^{\phi} + t^{\phi} + 1) = \varepsilon(x^{\sigma}t + xt^{\phi}) \tag{18}$$

for all $t \in GF(q)^{\times}$ and $x \in GF(q)$. Putting $x = 1$, we have

$$t + \bar{t} + t^{\phi} + (\bar{t})^{\phi} = \varepsilon(t + t^{\phi}). \tag{19}$$

Substituting Equation (19) into Equation (18), we have

$$(1 + t + \bar{t})(x + x^{\sigma}) = x\varepsilon(t + t^{\phi}) + \varepsilon(x^{\sigma}t + xt^{\phi}). \tag{20}$$

Suppose $\varepsilon(t + t^{\phi}) = 1$ for some $t \in GF(q)^{\times}$. Then for every $x \in GF(q) \setminus GF(2)$, we have $x^{\sigma} + x \neq 0$ and $1 + t + \bar{t} = (x + \varepsilon(x^{\sigma}t + xt^{\phi}))/(x^{\sigma} + x)$ from Equation (20). As this holds for every $x \in GF(q)$, we have

$$\frac{x + \varepsilon(x^{\sigma}t + xt^{\phi})}{x^{\sigma} + x} = \frac{y + \varepsilon(y^{\sigma}t + yt^{\phi})}{y^{\sigma} + y} \tag{21}$$

for all $x, y \in GF(q) \setminus GF(2)$. Write $\varepsilon(x^{\sigma} + xt^{\phi}) = \varepsilon_{x}$ and $\varepsilon(y^{\sigma} + yt^{\phi}) = \varepsilon_{y}$, elements of $GF(2)$. Then Equation (21) can be rewritten as

$$xy^{\sigma} + yx^{\sigma} = \varepsilon_{x}(y^{\sigma} + y) + \varepsilon_{y}(x^{\sigma} + x),$$

whence

$$\mathrm{Tr}(xy^{\sigma} + yx^{\sigma}) = 0$$

for all $x, y \in GF(q) \setminus GF(2)$. Hence we have $0 = \mathrm{Tr}(x^\sigma(y + y^{\sigma^2}))$ for all $x, y \in GF(q)$, from which we have $y = y^{\sigma^2}$ for all $y \in GF(q)$. However, this implies that $d + 1$, the order of a generator σ of $\mathrm{Gal}(GF(q)/GF(2))$, is 2. This contradicts $d \geq 2$.

Hence we have $\varepsilon(t+t^\phi) = 0$ for all $t \in GF(q)$. Then it follows from Equation (20) that $(1 + t + \bar{t})(x + x^\sigma) = \varepsilon(x^\sigma t + xt^\phi)$ for all $x, t \in GF(q)$. Thus

$$1 + t + \bar{t} = \varepsilon_x/(x + x^\sigma)$$

for all $x \in GF(q) \setminus GF(2)$ with $\varepsilon_x = \varepsilon(x^\sigma t + xt^\phi) \in GF(2)$. Suppose $\varepsilon_x = 1$ for all $x \in GF(q) \setminus GF(2)$. As t and $\bar{t}$ are independent of x, then we have $1/(x + x^\sigma) = 1/(y + y^\sigma)$ for every $x, y \in GF(q) \setminus GF(2)$. However, this is equivalent to the condition that $x + y = (x + y)^\sigma \in GF(2)$ for all $x, y \in GF(q)$, which contradicts $q = 2^{d+1} \geq 8$. Hence $\varepsilon_x = 0$ for some $x \in GF(q) \setminus GF(2)$. This implies that for all $t \in GF(q)^\times$ we have

$$\bar{t} = t + 1.$$

From Equation (19) and $\varepsilon(t + t^\phi) = 0$, then we have $1 + t^\phi = (1 + t)^\phi$ for all $t \in GF(q)^\times$. However, as ϕ is multiplicative, this shows that for $s, t \in GF(q)$ with $t \neq 0$ we have

$$(s + t)^\phi = s^\phi((s/t)^\phi + 1)^\phi = s^\phi((s/t)^\phi + 1) = s^\phi + t^\phi.$$

Thus ϕ is additive as well. Hence ϕ is a field automorphism on $GF(q)$, which contradicts our assumption that $\phi \notin \mathrm{Gal}(GF(q)/GF(2))$. $\square$

By Step 7, the automorphism group G stabilizes $X(0)$. Hence $G = A = MF$, and Theorem 1.1 is proved.

4 Isomorphism

In this section, we prove Theorem 1.2.

We set $\mathcal{S} := \mathcal{S}^{d+1}_{\sigma,\phi}$ with $\mathcal{S}' := \mathcal{S}^{d+1}_{\sigma',\phi'}$. To distinguish members of $\mathcal{S}$ from $\mathcal{S}'$, we denote members of $\mathcal{S}$ and $\mathcal{S}'$ as $X(t)$ and $X'(t)$ respectively. The normal subgroup of $\mathrm{Aut}(\mathcal{S})$ acting regularly on $\mathcal{S} \setminus \{X(0)\}$ (see Theorem 1.1) is denoted $M_{\sigma,\phi}$. The corresponding group for $\mathcal{S}'$ is denoted $M_{\sigma',\phi'}$. To distinguish elements m_b (see Definition 3) of $M_{\sigma,\phi}$ from the corresponding elements in $M_{\sigma',\phi'}$, we denote the latter by m'_b ($b \in GF(q)^\times$).

In view of Lemma 2.2, it suffices to show the 'only if ' part of Theorem 1.2. In the case when $d = 2$, $\mathcal{S}^3_{2,6}$ and $\mathcal{S}^3_{4,6}$ are the only candidates for $\mathcal{S}$ and $\mathcal{S}'$

(see Step 1 in the previous section), and there is nothing to prove. Thus we may assume that $d \geq 3$. Let τ be a $GF(2)$-linear bijection on V inducing an isomorphism of $\mathcal{S}$ with $\mathcal{S}'$.

Step 1. *We may assume that τ satisfies the following conditions.*

$$X(0)^\tau = X'(0), X(1)^\tau = X'(1), M_{\sigma,\phi}^\tau = M_{\sigma',\phi'} \text{ and } X(\infty)^\tau = X(\infty)\,.$$

Proof. As $X(0)$ is the unique member of $\mathcal{S}$ fixed by $\mathrm{Aut}(\mathcal{S})$ by Theorem 1.1, it is sent by τ to the unique member $X'(0)$ of $\mathcal{S}' = \mathcal{S}^\tau$ fixed by $\mathrm{Aut}(\mathcal{S}')$. As $d \geq 3$, $M_{\sigma,\phi}^\tau$ and $M_{\sigma',\phi'}$ are normal subgroups of $\mathrm{Aut}(\mathcal{S}') \cong Z_{q-1}.Z_{d+1}$ (see Theorem 1.1) acting regularly on $\mathcal{S}' \setminus \{X'(0)\}$. Thus $M_{\sigma,\phi}^\tau = M_{\sigma',\phi'}$.

The subspace $X(\infty)^\tau$ is a $(d+1)$-dimensional subspace of V which is invariant under $\mathrm{Aut}(\mathcal{S})^\tau = \mathrm{Aut}(\mathcal{S}')$. Thus it follows from the argument in the first part of the proof for Step 6 (or [5, Lemma 10] together with Lemma 2.3) that $X(\infty)^\tau = X(\infty)$. As $M_{\sigma',\phi'}$ is transitive on $\mathcal{S}' \setminus \{X'(0)\}$, we may furthermore assume that $X(1)^\tau = X'(1)$, replacing τ by $\tau m'$ for a suitable element m' of $M_{\sigma',\phi'}$. ☐

As τ stabilizes both $X(0) = X'(0) = \{(x,0) \mid x \in GF(q)\}$ and $X(\infty) = \{(0,y) \mid y \in GF(q)\}$, there exist $GF(2)$-linear bijections a and d on $GF(q)$ such that

$$(x,y)^\tau = (x^a, y^d) \tag{22}$$

for all $x, y \in GF(q)$.

Step 2. *In Expression (22), we may assume that $a = \mathrm{id}$, the identity on $GF(q)$.*

Proof. As $M_{\sigma,\phi}^\tau = M_{\sigma',\phi'}$, there is a positive integer i with $m_\eta^\tau = (m'_\eta)^i$, whence $m_b^\tau = (m'_b)^i$ for all $b \in GF(q)^\times$. Applying $m_b\tau = \tau(m'_b)^i$ to (x,y), we have

$$(bx)^a = b^i \cdot x^a \tag{23}$$

$$(b^{(\sigma\phi-1)/(\phi-1)}y)^d = ((b^i)^{(\sigma'\phi'-1)/(\phi'-1)}) \cdot y^d \tag{24}$$

for all $b \in GF(q)^\times$, $x, y \in GF(q)$. From Equation (23) and the linearity of a, we have $(b_1 + b_2)^i = b_1^i + b_2^i$ for every $b_1 \neq b_2 \in GF(q)^\times$. Hence the map $GF(q) \ni x \mapsto x^i \in GF(q)$ is both additive and multiplicative, whence $x^i = x^\theta$ $(x \in GF(q))$ for some $\theta \in \mathrm{Gal}(GF(q)/GF(2))$. Then all the conditions in Step 1 are satisfied with τ replaced by $\tau' := \tau f'_{\theta^{-1}}$, where $f'_{\theta^{-1}}$ denotes the field automorphism of $\mathrm{Aut}(\mathcal{S}')$ corresponding to θ^{-1}. Moreover, we have $m_b\tau' = \tau' m'_b$. Thus replacing τ by τ', we may assume that $(bx)^a = b \cdot x^a$ for all $b, x \in GF(q)$. As $X(0) \cap X(1) = [(1,0)]$ is mapped by τ to $X'(0) \cap X'(1) = [(1,0)]$ by Step 1, we have $1^a = 1$. Thus $b^a = b \cdot 1^a = b$ for all $b \in GF(q)$. Hence we conclude that $a = \mathrm{id}$, whence $i = 1$ in Equations (23),(24). ☐

Step 3. *There is a non-prime subfield F of $GF(q)$ such that in Expression (22) we have $d = \mu g$ for some $\mu \in \mathrm{Gal}(GF(q)/GF(2))$ and an F-linear bijection g on $GF(q)$. Furthermore, $((\sigma\phi - 1)/(\phi - 1))\mu\nu' = (\sigma'\phi' - 1)/(\phi' - 1)$ on $GF(q)^\times$ for every $\nu' \in \mathrm{Gal}(GF(q)/F)$.*

Proof. Let $I := \{b^{(\sigma\phi-1)/(\phi-1)} \mid b \in GF(q)\}$ and $I' := \{b^{(\sigma'\phi'-1)/(\phi'-1)} \mid b \in GF(q)\}$. From Equation (24), for $b \in GF(q)^\times$ we have $b^{(\sigma\phi-1)/(\phi-1)} = 1$ if and only if $b^{(\sigma'\phi'-1)/(\phi'-1)}$. Thus the endomorphisms $(\sigma\phi - 1)/(\phi - 1)$ and $(\sigma'\phi' - 1)/(\phi' - 1)$ of $GF(q)^\times$ have the same kernel. As I and I' are images of these endomorphisms, they are subgroups of a cyclic group $GF(q)^\times$ of the same order, whence $I = I'$.

Let F be the set of sums of elements of $I = I'$. As I is closed under multiplication, F is closed under both addition and multiplication. Thus F is a subfield of $GF(q)$. If F is $GF(2)$, then $I = \{1\}$, whence $x^{\sigma\phi-1} = 1$ for all $x \in GF(q)^\times$. However, this implies that $\sigma\phi = \mathrm{id}$ on $GF(q)$, which contradicts our assumption that ϕ is not contained in $\mathrm{Gal}(GF(q)/GF(2))$. Thus F properly contains $GF(2)$.

Then it follows from Equation (24) (with $i = 1$ by Step 2) and the linearity of d that there exists an additive map μ on F such that

$$(fy)^d = f^\mu \cdot y^d \tag{25}$$

$$(b^{(\sigma\phi-1)/(\phi-1)})^\mu = b^{(\sigma'\phi'-1)/(\phi'-1)} \tag{26}$$

for all $f \in F$, $b \in GF(q)^\times$ and $y \in GF(q)$. From Equation (26), μ is multiplicative on I, whence μ is multiplicative on F, as every element of F is a sum of elements in I. Thus μ is an automorphism in $\mathrm{Gal}(F/GF(2))$. We also denote by μ an automorphism in $\mathrm{Gal}(GF(q)/GF(2))$ whose restriction on F is μ. Then it follows from Equation (25) that $(fy)^{d\mu^{-1}} = f(y^{d\mu^{-1}})$ for all $f \in F$ and $y \in GF(q)$. Hence $d\mu^{-1} =: h$ is an F-linear bijection on $GF(q)$. Thus $d = h\mu = \mu g$, where $g := \mu^{-1}h\mu$ is an F-linear bijection.

As $b^{(\sigma\phi-1)/(\phi-1)} \in F$ for all $b \in GF(q)^\times$, the last claim in Step follows from Equation (26). □

Step 4. *Let $F \cong GF(2^s)$ with $sr = d+1$, and let ν be an automorphism of $GF(q)$ defined by $x^\nu = x^{2^s}$. There exists some i with $0 \leq i \leq r-1$ such that one of the following occurs, where μ is the element of $\mathrm{Gal}(GF(q)/GF(2))$ in Step 3.*

(a) $\sigma = \sigma'$ *and* $\mu\nu^i = \mathrm{id}$.

(b) $\sigma\sigma' = \mathrm{id}$ *and* $\mu\nu^i = \sigma'$.

Proof. For $t \in GF(q)$, we write $X(t)^\tau = X'(\bar{t})$. As a vector $(x, x^\sigma t + xt^\phi)$ of $X(t)$ is mapped by τ to a vector $(x, ((x^\sigma t + xt^\phi)^\mu)^g)$ of $X'(\bar{t})$ by Step 2 and Step 3, we have

$$(x^{\sigma\mu}t^{\mu} + x^{\mu}t^{\phi\mu})^g = x^{\sigma'}\overline{t} + x(\overline{t})^{\phi'} \tag{27}$$

for all $x, t \in GF(q)$. Putting $t = 1$, for all $x \in GF(q)$ we have

$$(x^{\sigma\mu} + x^{\mu})^g = x^{\sigma'} + x. \tag{28}$$

Now there is a unique polynomial $g(X)$ in $GF(q)[X]$ of degree at most $q-1$ such that $g(x) = x^g$ for all $x \in GF(q)$. As g is F-linear for $F = GF(2^s)$, we have

$$g(X) = \sum_{i=0}^{r-1} b_i X^{2^{si}}$$

for some $b_i \in GF(q)$ $(i = 0, \ldots, r-1)$. Recall that there are positive integers m, k with $1 \leq m, k \leq d$ coprime with $d+1$ so that $x^{\sigma} = x^{2^m}$ and $x^{\sigma'} = x^{2^k}$ for all $x \in GF(q)$. We also define a with $0 \leq a \leq d$ by $x^{\mu} = x^{2^a}$ for all $x \in GF(q)$. Then it follows from Equation (28) that

$$\sum_{i=0}^{r-1} b_i x^{2^{m+a+is}} + \sum_{i=0}^{r-1} b_i x^{2^{a+is}} = x^{2^k} + x \tag{29}$$

for all $x \in GF(q)$. Choose integers α_i and β_i with $0 \leq \alpha_i, \beta_i \leq q-1$ so that

$$X^{\alpha_i} \equiv X^{2^{m+a+is}}, X^{\beta_i} \equiv X^{2^{a+is}} \text{ modulo } X^q - X$$

$(i = 0, \ldots, r-1)$. Then the left hand side of Equation (29) is given as $L(x)$ $(x \in GF(q))$ for a polynomial $L(X) := \sum_{i=0}^{r-1} b_i X^{\alpha_i} + \sum_{i=0}^{r-1} b_i X^{\beta_i}$ of degree at most $q-1$, while the right hand side is $R(x)$ $(x \in GF(q))$ for $R(X) = X^{2^k} + X$ of degree at most $q-1$. Thus Equation (29) implies that $L(X) = R(X)$ as polynomials of $GF(q)[X]$, that is,

$$\sum_{i=0}^{r-1} b_i X^{\alpha_i} + \sum_{i=0}^{r-1} b_i X^{\beta_i} = X^{2^k} + X. \tag{30}$$

Now it is easy to verify that $\alpha_i \neq \alpha_j$ and $\beta_i \neq \beta_j$ if $0 \leq i \neq j \leq r-1$. If $\alpha_i = \beta_j$ for some i, j, then $X^{2^{m+a+is}} \equiv X^{2^{a+js}}$ (modulo $X^q - X$). This implies that $m \equiv (j-i)s$ (modulo $d+1$). However, s is a divisor of $d+1$ with $s \geq 2$, as $GF(2)$ is a proper subfield of $F = GF(2^s)$ by Step 3. This contradicts that m is coprime with $d+1$. Hence $\alpha_i \neq \beta_j$ for every $0 \leq i, j \leq q-1$.

Thus the monomials in the left hand side of Equation (30) are distinct from each other. As X^{α_i} and X^{β_i} has the same coefficient b_i, we conclude that there exists a unique i with $0 \leq i \leq r-1$ such that $b_i = 1$, $b_j = 0$ for every $j \neq i$, and that either $X^{\alpha_i} = X^{2^k}$ and $X^{\beta_i} = X$ or $X^{\alpha_i} = X$ and $X^{\beta_i} = X^{2^k}$. Accordingly, we have Case (a) or Case (b) in the claim of this Step. □

Step 5. *We have either* $(\sigma, \phi) = (\sigma', \phi')$ *or* $\sigma\sigma' = \mathrm{id} = \phi\phi'$.

Proof. Note that $\nu' := \nu^i$ in Step 4 lies in $\mathrm{Gal}(GF(q)/F)$ as $F = GF(2^s)$. Then it follows from the last remark in Step 3 that we have

$$(\sigma\phi - 1)\mu\nu'(\phi' - 1) = (\sigma'\phi' - 1)(\phi - 1).$$

If Case (a) in Step 4 holds, then $(\sigma\phi - 1)(\phi' - 1) = (\sigma\phi' - 1)(\phi - 1)$, from which we have $(\sigma - 1)(\phi - \phi') = 0$. Thus $\phi = \phi'$ as $\sigma - 1$ is bijective. If Case (b) in Step 4 holds, then we have $(\sigma\phi - 1)\sigma'(\phi' - 1) = (\sigma'\phi' - 1)(\phi - 1)$. Multiplying both sides by σ and using $\sigma\sigma' = \mathrm{id}$, we have $(\sigma\phi - 1)(\phi' - 1) = (\phi' - \sigma)(\phi - 1)$. It follows that $(\sigma - 1)(\phi\phi' - 1) = 0$, whence $\phi\phi' = \mathrm{id}$ as $\sigma - 1$ is bijective. □

This completes the proof of the 'only if' part of Theorem 1.2. Thus Theorem 1.2 is established by Lemma 2.2.

5 Some general setting

In the definition of $\mathcal{S}^{d+1}_{\sigma,\phi}$, we only consider a generator σ of $\mathrm{Gal}(GF(q)/GF(2))$. In fact, this is naturally required, as the following proposition shows.

Proposition 5.1. *For any polynomials $a(X)$ and $b(X)$ in $GF(q)[X]$, we define $\mathcal{S}^{d+1}_{a,b}$ to be the collection of $X(t)$ over $t \in GF(q)$, where*

$$X(t) := \{(x, a(x)t + xb(t)) \mid x \in GF(q)\}.$$

Assume that $\mathcal{S}^{d+1}_{a,b}$ is a d-dimensional dual hyperoval. Then there exist $\alpha, \beta \in GF(q)^\times$, $\gamma \in GF(q)$, a generator σ of $\mathrm{Gal}(GF(q)/GF(2))$ and an o-polynomial $\phi(X)$ of $GF(q)[X]$ such that $a'(x) = \alpha x^\sigma$ and $b'(x) = \beta x^\phi + \gamma$ for all $x \in GF(q)$ and $\mathcal{S}^{d+1}_{a,b} = \mathcal{S}^{d+1}_{a',b'}$.

In particular, $\mathcal{S}^{d+1}_{a,b}$ is isomorphic to $\mathcal{S}^{d+1}_{\sigma,\phi}$.

We first prepare a lemma.

Lemma 5.2. *Let $c(X)$ be a polynomial of $GF(q)[X]$ such that*

$$(c(t_1) + c(t_2))/(t_1 + t_2) \neq (c(t_1) + c(t_3))/(t_1 + t_3)$$

for every mutually distinct elements t_1, t_2, t_3 of $GF(q)$. Then there exist $\lambda \in GF(q)$ and an o-polynomial $f(X)$ such that for all $t \in GF(q)$ we have

$$c(t) = (c(0) + c(1) + \lambda)f(t) + \lambda t + c(0),$$

where λ is the unique value of $GF(q)$ which cannot be written as $(c(t_1) + c(t_2))/(t_1 + t_2)$ for any $t_1 \neq t_2 \in GF(q)$.

Proof. Recall that three points $[a_{i1}, a_{i2}, a_{i3}]$ $(i = 1, 2, 3)$ of $PG(2, q)$ are not in a line in common if and only if $\det(a_{ij}) \neq 0$. Thus no three distinct points of $\mathcal{A} := \{[1, t, c(t)] \mid t \in GF(q)\} \cup \{[0, 0, 1]\}$ are collinear from the hypothesis. Then $\mathcal{A}$ is uniquely extended to a hyperoval $\mathcal{O}$ of $PG(2, q)$. As the nucleus does not lie on any line through two distinct points of $\mathcal{A}$, it is of form $[0, 1, \lambda]$, where λ is the unique value of $GF(q)$ which cannot be written as $(c(t_1) + c(t_2))/(t_1 + t_2)$ for some $t_1 \neq t_2 \in GF(q)$.

As $(1, 0, c(0))$, $(1, 1, c(1))$ and $(0, 1, \lambda)$ are linearly independent, there is a unique $GF(q)$-linear bijection F on $GF(q)^3$ for which $F(1, 0, 0) = (1, 0, c(0))$, $F(1, 1, 1) = (1, 1, c(1))$ and $F(0, 1, 0) = (0, 1, \lambda)$. Then

$$F(0, 0, 1) = (0, 0, c(0) + c(1) + \lambda),$$

and the hyperoval $F^{-1}(\mathcal{O})$ of $PG(2, q)$ contains four points $[1, 0, 0]$, $[1, 1, 1]$, $[0, 0, 1]$ and $[0, 1, 0]$. Thus $F^{-1}(\mathcal{O})$ has a canonical description $\{[1, t, f(t)] \mid t \in GF(q)\} \cup \{[0, 0, 1], [0, 1, 0]\}$ with an o-polynomial $f(X)$. As $F(1, t, f(t))) = F(1, 0, 0) + tF(0, 1, 0) + f(t)F(0, 0, 1) = (1, t, (c(0) + c(1) + \lambda)f(t) + \lambda t + c(0))$ corresponds to a point of $\mathcal{O}$, we have $c(t) = (c(0) + c(1) + \lambda)f(t) + \lambda t + c(0)$ for every $t \in GF(q)$. □

Now we prove Proposition 5.1. As each $X(t) = \{(x, a(x)t + xb(t)) \mid x \in GF(q)\}$ is a subspace over $GF(2)$, $a(X)$ is additive: $a(x_1 + a_2) = a(x_1) + a(x_2)$ for all $x_1, x_2 \in GF(q)$. Take any mutually distinct values t_i $(i = 1, 2, 3)$ of $GF(q)$. As $\mathcal{S}$ is a dimensional dual hyperoval, $X(t_1) \cap X(t_2)$ contains a unique nonzero vector, but $X(t_1) \cap X(t_2) \cap X(t_3) = \{(0, 0)\}$. This implies that $a(x)/x = (b(t_1) + b(t_2))/(t_1 + t_2)$ has a unique solution x in $GF(q)^\times$, while $(b(t_1) + b(t_2))/(t_1 + t_2) \neq (b(t_1) + b(t_3))/(t_1 + t_3)$. In particular, $b(X)$ satisfies the hypothesis of Lemma 5.2, and the map $t \mapsto (b(t_1)+b(t))/(t_1+t)$ is a bijection of $GF(q) \setminus \{t_1\}$ with $GF(q) \setminus \{\lambda\}$. Thus the map $x \mapsto a(x)/x$ gives a bijection of $GF(q)^\times$ with $GF(q) \setminus \{\lambda\}$. Then

$$\frac{a(x_1) + a(x_2)}{x_1 + x_2} = \frac{a(x_1 + x_2)}{x_1 + x_2} \neq \frac{a(x_1 + x_3)}{x_1 + x_3} = \frac{a(x_1) + a(x_3)}{x_1 + x_3}$$

for all triple of distinct elements x_i $(i = 1, 2, 3)$ of $GF(q)$. Hence the polynomial $a(X)$ also satisfies the hypothesis of Lemma 5.2. Then there exist $\lambda, \lambda' \in GF(q)$ and o-polynomials π and ϕ in $GF(q)[X]$ such that $a(t) = (a(0) + a(1) + \lambda)\pi(t) + \lambda t + a(0)$ and $b(t) = (b(0) + b(1) + \lambda')\phi(t) + \lambda' t + b(0)$ for all $t \in GF(q)$.

Note that we have $\lambda = \lambda'$, because the above argument also shows that the values $(a(x_1) + a(x_2))/(x_1 + x_2)$ for $x_1 \neq x_2 \in GF(q)$ form a set $GF(q) \setminus \{\lambda\}$. We set $\alpha := a(0) + a(1) + \lambda$ and $\beta := b(0) + b(1) + \lambda$, which are nonzero elements of $GF(q)$.

As $a(X)$ is additive, $a(0) = 0$ and $\pi(X)$ is an additive o-polynomial. Thus it follows from [3, Theorem 8.41] that $\pi(X) = X^{2^\sigma}$ for some generator σ of $\mathrm{Gal}(GF(q)/GF(2))$. Then $a(x) = \alpha x^\sigma + \lambda x$ for all $x \in GF(q)$. However, as $a(x)t + xb(t) = (\alpha x^\sigma + \lambda x)t + x(\beta t^\phi + \lambda t + b(0)) = \alpha x^\sigma t + x(\beta t^\phi + b(0))$, we have $a(x)t + xb(t) = a'(x)t + xb'(t)$, where $a'(t) := \alpha x^\sigma$ and $b'(t) := \beta t^\phi + \gamma$ with $\gamma := b(0)$. Thus $X(t)$ in $\mathcal{S}^{d+1}_{a,b}$ is identical with $X(t)$ in $\mathcal{S}^{d+1}_{a',b'}$, whence $\mathcal{S}^{d+1}_{a,b} = \mathcal{S}^{d+1}_{a',b'}$.

Finally, define $GF(2)$-linear transformations G, H and I by $G : (x, y) \mapsto (x, \gamma x + y)$, $H : (x, y) \mapsto (\delta x, \delta^\sigma y)$ for $\delta \in GF(q)^\times$ with $\delta^{\sigma-1} = \alpha/\beta$ and $I : (x, y) \mapsto (x, \alpha^{-1} y)$. As $X(t) = \{(x, \alpha x^\sigma t + x(\beta t^\phi + \gamma)) \mid x \in GF(q)\}$, we can easily see that $X(t)^{GHI} = \{(x, x^\sigma t + xt^\phi \mid x \in GF(q)\}$. Thus $(\mathcal{S}^{d+1}_{a,b})^{GHI} = (\mathcal{S}^{d+1}_{a',b'})^{GHI} = \mathcal{S}^{d+1}_{\sigma,\phi}$.

References

[1] **D. G. Glynn**, Two new sequences of ovals in finite Desarguesian planes of even order, *Combinatorial Mathematics X*, Springer Lecture Notes in Mathematics **1063** (1983), 217–229.

[2] **C. Hering**, **W. M. Kantor** and **G. M. Seitz**, Finite groups with split BN-pair of rank 1. I, *J. Algebra* **20** (1972), 453–475.

[3] **J. W. P. Hirschfeld**, *Projective Geometries over Finite Fields*, 2nd edn, Oxford Mathematical Monographs, Clarendon Press, Oxford, 1998.

[4] **W. M. Kantor**, Linear groups containing a Singer cycle, *J. Algebra* **62** (1980), 232–234.

[5] **S. Yoshiara**, A family of d-dimensional dual hyperovals in $PG(2d+1, 2)$, *Europ. J. Combin.* **20** (1999), 589–603.

Hiroaki Taniguchi

TAKUMA NATIONAL COLLEGE OF TECHNOLOGY, 551 TAKUMA, KAGAWA 769-1192, JAPAN

e-mail: taniguchi@dg.takuma-ct.ac.jp

Satoshi Yoshiara

DEPARTMENT OF MATHEMATICS, TOKYO WOMAN'S CHRISTIAN UNIVERSITY, 2-6-1 ZEMPUKUJI, SUGINAMI-KU, TOKYO 167-8585, JAPAN

e-mail: yoshiara@lab.twcu.ac.jp