A characterization of a class of dimensional dual hyperovals with doubly transitive automorphism groups and its applications

Satoshi Yoshiara

Department of Mathematics, Tokyo Woman’s Christian University, Suginami-ku, Tokyo 167-8585, Japan

Received 3 September 2007; accepted 5 January 2008
Available online 4 March 2008

Abstract

A characterization theorem is given for d-dimensional hyperovals over $GF(2)$ with doubly transitive automorphism group, if it has the ambient space of dimension $2(d + 1)$. Based on this theorem, some classification of those dual hyperovals are obtained.

© 2008 Elsevier Ltd. All rights reserved.

1. Introduction

Let $U$ be a vector space over a finite field $GF(q)$ with $q$ elements. A family $A$ of $(d + 1)$-dimensional subspaces of $U$ is called a $d$-dimensional dual arc (abbreviated to $d$-dual arc) over $GF(q)$ if it satisfies the following conditions.

1. $\dim(X \cap Y) = 1$ for every distinct members $X$ and $Y$ of $A$.
2. $X \cap Y \cap Z = \{0\}$ for mutually distinct members $X$, $Y$, $Z$ of $A$.

The subspace of $U$ spanned by the members of $A$ is called the ambient space of $A$. It is easy to see that a $d$-dual arc has at most $((q^{d+1} - 1)/(q - 1)) + 1$ members. If the upper bound is attained, $A$ is called a $d$-dimensional dual hyperoval (abbreviated to $d$-dual hyperoval).

Recall that the automorphism group $\text{Aut}(S)$ of a $d$-dual hyperoval $S$ with ambient space $V$ is defined to be the subgroup of automorphisms of the projective space $PG(V)$ associated with $V$ which preserve $S$. 
This paper is a continuation of [4], where the structure of the automorphism group $\text{Aut}(S)$ is restricted if it acts doubly transitively on $S$ and $d \geq 2$. In particular, $q = 2$ or 4 and $S$ is explicitly determined if $q = 4$. If $q = 2$, any subgroup $G$ of $\text{Aut}(S)$ acting doubly transitively on $S$ is of affine type, namely, it has a normal subgroup $N$ acting regularly on $S$. Then $G = N : G_X$, a semidirect product of $N$ with the stabilizer $G_X$ of a member $X$ of $S$ in $G$. In the rest of this paper, $N$ always denotes the regular normal subgroup of $G$ on $S$.

In this paper, we investigate such $S$ with ambient space of small dimension. In Section 3, we establish the following characterization theorem of a family of $d$-dual hyperovals $S^{d+1}$ with $\sigma, \tau \in \text{Gal}(GF(2^{d+1})/GF(2))$ [3]. We use the symbol $Z_m$ to denote a cyclic group of order $m$. Recall that a group acting on a set is called half-transitive if its orbits all have equal length greater than 1.

**Theorem 1.** Let $d$ be a positive integer with $d \geq 2$. Let $S$ be a $d$-dual hyperoval over $GF(2)$ with ambient space $V$ of dimension $2d + 2$ on which a subgroup $G$ of $\text{Aut}(S)$ acts doubly transitively. Assume that the stabilizer in $G$ of a member $X \in S$ contains a cyclic subgroup $S$ which is regular on the set $X^\#$ of nonzero vectors of $X$. If $d = 5$, assume further that $S$ is half-transitive on the nonzero vectors of $[V, N]$, where $N$ is the normal subgroup of $G$ which is regular on $S$.

Then $S$ is isomorphic to the dual hyperoval $S^{d+1}$ for some field automorphisms $\sigma$ and $\tau$ in $\text{Gal}(GF(2^{d+1})/GF(2))$ with $\sigma \tau \neq i d_{GF(2^{d+1})}$. In particular, $\text{Aut}(S)$ is the semidirect product of $N$ with the stabilizer of a member $X$ of $S$, which is isomorphic to $\Gamma L_1(2^{d+1}) \cong Z_{2^{d+1}} : Z_{d+1}$ or $SL_3(2)$ according as $d \geq 3$ or $d = 2$.

In Section 4, some classifications are obtained using **Theorem 1**. In these theorems, $d$ is a positive integer with $d \geq 2$.

**Theorem 2.** Let $S$ be a $d$-dual hyperoval over $GF(2)$ with ambient space $V$ of dimension $2d + 1$. Assume that $G$ is a subgroup of $\text{Aut}(S)$ which is doubly transitive on $S$. Then $G = N : G_X$ is a semidirect product of the regular normal subgroup $N$ on $S$ with the stabilizer $G_X$ of a member $X$ of $S$, which is isomorphic to a subgroup of $Z_{2^{d+1} - 1} : Z_{d+1}$, acting transitively on $X^\#$.

**Theorem 3.** Let $S$ be a $d$-dual hyperoval over $GF(2)$ with ambient space $V$ of dimension $2d + 2$. Assume that $G$ is a subgroup of $\text{Aut}(S)$ which is doubly transitive on $S$. Then $G = N : G_X$ is a semidirect product of a regular normal subgroup $N$ on $S$ with the stabilizer $G_X$ of a member $X$ of $S$, which is isomorphic to one of the following groups:

(1) $\Gamma L_1(2^{d+1}) \cong Z_{2^{d+1}} : Z_{d+1}$, acting transitively on $X^\#$.

(2) a subgroup of $\text{GL}_2(r) : Z_{(d+1)/2}$ containing a normal subgroup $\text{SL}_2(r)$, where $r = 2^{(d+1)/2}$.

This occurs only when $d$ is odd.

(3) $\text{SL}_3(2)$ with $d = 2$; $A_6$ or $S_6$ with $d = 3$; and $G_2(2)'$, $G_2(2)$ or $Sp_{6}(2)$ with $d = 5$.

If $d$ is even and $2^{d+1} - 1$ is coprime with $d + 1$, then cases (2), (3) above do not occur, except $d = 2$ in case (3). In case (1), the normal subgroup $Z_{2^{d+1} - 1}$ is the unique subgroup acting regularly on $X^\#$. Thus from **Theorems 1 and 3** we obtain:

**Corollary 4.** Assume that $d$ is even and $2^{d+1} - 1$ is coprime with $d + 1$. Then a $d$-dual hyperoval $S$ over $GF(2)$ with ambient space of dimension $2d + 2$ admits an automorphism group acting doubly transitively on $S$ if and only if $S$ is isomorphic to $S^{d+1}_{\sigma, \tau}$ for some $\sigma, \tau \in \text{Gal}(GF(2^{d+1})/GF(2))$. 

The paper is organized as follows. In Section 2, some general lemma are derived on the commutator space $[V, N]$ of the action of $N$ on the ambient space $V$ of $S$. Section 3 is the main part of the paper, where Theorem 1 is proved: we first determine the actions on both $X$ and $[V, N]$ of a certain cyclic subgroup $S$ of $G_X$, and then specify $S$ by exploiting functional methods. In Section 4, we derive Theorems 2 and 3, using group theory, based on an observation that some substructures of $S$ inherit the property of $S$ (Lemma 15).

2. Some general results

In this section, we assume that $S$ is a $d$-dual hyperoval over $GF(2)$ with ambient space $V$ admitting an automorphism group $G (\leq Aut(S))$ which acts doubly transitively on $S$. Then $G$ is of affine type by [4]. Let $N$ be the normal subgroup of $G$ acting regularly on $S$, and let $X$ be a given member of $S$. Then $G = N : G_X$ is a semidirect product of $N$ with $G_X$.

Notice that there is a bijection $\nu$ from the set $X^#$ of nonzero vectors of $X$ to the set $N^# = N \setminus \{1\}$ of involutions of $N$:

$$x^# \ni x \mapsto \nu(x) := \text{the unique involution of } N^\# \text{ such that } x \in X \cap X^{\nu(x)}.$$

There are three actions of $G_X$: the first one is on $S \setminus \{X\}$, the second is on $X^# = PG(X)$, and the third is on $N^#$ by conjugation. Notice that they are equivalent to each other, via $Y \mapsto \nu(Y)$. In particular, $\nu(x)^g = \nu(x^g)$ for $x \in X^#$ and $g \in G_X$. As $G$ is doubly transitive on $S$, $G_X$ is transitive on $X^#$.

Let $[V, N]$ be the smallest subspace $W$ of $V$ such that $N$ acts trivially on $V/W$. It is spanned by all commutators $[v, n] = -v + v^n = v + v^n$ for $v \in V$ and $n \in N$. As $V$ is spanned by all $X^n (n \in N)$, $[V, N]$ is spanned by $x + x^n$ for $x \in X$ and $n \in N$.

**Lemma 5.** (1) We have $V = X \oplus [V, N]$.
(2) For each involution $n \in N$, we have $\{x + x^n \mid x \in X\} = [X, n] = \langle X, X^n \rangle \cap [V, N]$ and $\langle X, X^n \rangle = X \oplus [X, n]$.

**Proof.** (1) Since $[V, N]$ is $G$-invariant, $X \cap [V, N]$ is a $G_X$-invariant subspace of $X$. As $G_X$ acts transitively on $X^#$, we have either $X \subseteq [V, N]$ or $X \cap [V, N] = \{0\}$. In the former case, $V = \langle X^n \mid n \in N \rangle$ is contained in $[V, N]$. However, $[V, N] \not= V$, as $V$ is a nontrivial 2-group on which $G_X$ acts 2-regularly. Thus we have $X \cap [V, N] = \{0\}$. As $N$ acts trivially on $V/([V, N])$, $N$ acts on $\langle X, [V, N] \rangle = X \oplus [V, N]$. Thus this subspace contains all members $X^n (n \in N)$ of $S$, and therefore $V = \langle X^n \mid n \in N \rangle = X \oplus [V, N]$.

(2) As the map $X \ni x \mapsto x + x^n \in [X, n]$ is a $GF(2)$-linear surjection with kernel $C_X(n)$, we have $X/C_X(n) \cong [X, n]$. As $X \not= X^n$, $X \cap X^n = C_X(n)$ is a projective point on $X$, whence $\dim_{GF(2)}[X, n] = d$. From claim 1, $\langle X, X^n \rangle = X \oplus ([X, X^n] \cap [V, N])$. Thus $\langle X, X^n \rangle \cap [V, N]$ is of dimension $\dim([X, X^n]) = 2(d + 1) - 1 = (d + 1) = d$. As $\langle X, X^n \rangle \cap [V, N]$ contains $[X, n]$, we have $\langle X, X^n \rangle \cap [V, N] = [X, n]$ by comparing the dimensions. \hfill \Box

**Lemma 6.** Let $T$ be a subgroup of $G_X$ which acts on $N$ irreducibly, that is, $N$ is the only nontrivial $T$-invariant subgroup of $N$. If $\dim(V) \geq 2(d + 1)$, then $T$ does not centralize $[V, N]$.

**Proof.** Take an involution $n$ of $N^#$, and let $M$ be the subgroup of $N$ generated by $g^{-1}ng$ for all $g \in T$. Then $M$ is a nontrivial $T$-invariant subgroup of $N$, whence $M = N$ by the assumption. Suppose that $T$ centralizes $Y : = [V, N]$. Then $T$ acts on $H : = \langle X, X^n \rangle = X \oplus [X, n]$, and 

$[X, n] = \langle X, X^n \rangle \cap Y$ (see Lemma 5(2)) is centralized by $T$ and $T \subseteq G_X$. Since the involution
Theorem 1

Suppose that \( n \) normalizes \( H \), then \( g^{-1}ng \) normalizes \( H \) for all \( g \in T \). Thus \( N = M = \langle g^{-1}ng \mid g \in T \rangle \) normalizes \( H \). However, as \( N \) acts transitively on \( S \), this implies that \( H \) contains all the members of \( S \), whence \( H = V \), the ambient space. Then \( \dim(V) = \dim(X \oplus [X, n]) = (d + 1) + d = 2d + 1 \). \( \square \)

3. Proof of Theorem 1

Throughout this section, we assume the hypothesis in Section 2 and that \( \dim_{GF(2)}(V) = 2(d + 1) \). Since \( \dim(V) = 2(d + 1) \), we have \( \dim([V, N]) = d + 1 \) by Lemma 5(1). The group \( G \) acts on \([V, N]\), whence \( N \) acts on \([V, N]\), and the stabilizer \( G_X \) acts both on \( X \) and \([V, N]\). We begin with examining the actions of \( G_X \) and \( N \) on \([V, N]\).

Lemma 7. Assume that \( S \) is a cyclic subgroup of \( G_X \) acting regularly on the set \( X^\# \) of nonzero vectors of \( X \). If \( \dim(V) = 2(d + 1) \), then \( S \) acts irreducibly on \([V, N]\) unless \( d = 5 \). In the exceptional case, if \( S \) is half-transitive on \([V, N]^\# \), then the same conclusion holds.

Proof. Suppose that \( d \neq 5 \). Then it follows from the Zsigmondy theorem (e.g. [1, VIII, 8.3 Theorem]) that there exists a 2-primitive prime divisor \( p \) of \( 2^{d+1} - 1 \), that is, \( p \) is a prime dividing \( 2^{d+1} - 1 \), but \( p \) is coprime with \( 2^i - 1 \) for all \( 1 \leq i \leq d \). Let \( T \) be the unique subgroup of the cyclic group \( S \) of order \( p \). Notice that \( T \) acts irreducibly on \( N \), for otherwise there would be a subgroup of order \( 2^i \) (for \( 1 \leq i \leq d \)) of \( N \) on which \( T \) acts faithfully, then \( p \) would divide \( 2^i - 1 \). Then it follows from Lemma 6 that \( T \) does not centralize \([V, N]\), as we have \( \dim(V) = 2(d + 1) \) by the assumption in this lemma.

Suppose that \( S \) acts on \([V, N]\) reducibly. As \( S \) is of odd order, its action on \([V, N]\) is semisimple. Thus \([V, N] = W_1 \oplus W_2 \) for some nontrivial proper \( S \)-invariant subspaces \( W_1 \) and \( W_2 \). Since \( p \) is a 2-primitive prime divisor of \( 2^{d+1} - 1 \), the group \( T \) acts trivially on both \( W_1 \) and \( W_2 \). Thus \( T \) centralizes \([V, N]\), which contradicts the conclusion above. Hence \( S \) acts irreducibly on \([V, N]\) if \( d \neq 5 \).

Consider the case \( d = 5 \). In this case there is no 2-primitive prime divisor. However, we can verify that a subgroup \( T \) of \( S \) acts irreducibly on \( N \), if \( |T| = 9 \) or 21. Then it follows from Lemma 6 that the action of such \( T \) on \([V, N]\) is nontrivial.

Now the half-transitivity of \( S \) on \([V, N]^\# \) implies that \( S \) has the same orbit length \( s \) on \([V, N]^\# \) for \( s = 3, 7, 9, 21 \) or 63. As every nontrivial \( S \)-invariant subspace is a union of some \( S \)-orbits together with the zero vector, we have two possibilities if \( S \) acts reducibly on \([V, N]\). In the first possibility, \([V, N]\) is the sum of two 3-spaces \( W_i \) (for \( i = 1, 2 \)) such that \( S \) induces \( Z_7 \) on each \( W_i \). In the second possibility, \([V, N]\) is the sum of three 2-spaces \( W_i \) (for \( i = 1, 2, 3 \)) such that \( S \) induces \( Z_3 \) on each \( W_i \). Accordingly, the kernel \( T \) of the action of \( S \) on \([V, N]\) is of order 9 or 21. However, this contradicts the conclusion in the above paragraph. \( \square \)

Lemma 8. Under the assumption of Lemma 7, we have \( C_Y(N) = [V, N] \).

Proof. As \( N \) is a 2-group acting on a nontrivial 2-group \( Y := [V, N] \), we have \( C_Y(N) \neq \{0\} \). As \( C_Y(N) \) is \( G_X \)-invariant subspace of \( Y \), we have \( C_Y(N) = Y \) by Lemma 7. As \( X \cap C_Y(N) = \{0\} \), we have \( C_Y(N) = [V, N] \) from Lemma 5(1). \( \square \)

Now we assume the hypothesis of Theorem 1. Then it follows from Lemma 7 that the cyclic group \( S \) acting regularly on \( X^\# \) acts irreducibly on the \((d + 1)\)-space \([V, N]\) over \( GF(2) \). Let \( g \) be a generator of \( S \) and let \( K \) be the kernel of the action of \( S \) on \([V, N]\). Notice that we may have \( K \neq 1 \). Then \( S/K \) is isomorphic to an irreducible cyclic subgroup of \( GL([V, N]) \cong GL_{d+1}(2) \).
It is well known (e.g. [2, Proposition 19.8]) that then we can identify $[V, N]$ with the finite field $GF(2^{d+1})$ such that the action of $S/K$ is given by the multiplication by elements of $GF(2^{d+1})^\times$. In particular, there is an element $\omega \in GF(2^{d+1})^\times$ such that $y^\omega = \omega y$ for all $y \in [V, N]$. Hence for every element $h = g^i$ of $S$, there exists an element $\omega_2(h) = \omega^i$ of $GF(2^{d+1})^\times$ such that $y^h = \omega_2(h)y$ for all $y \in [V, N]$. If $g^i$ lies in $K$ for some $i$, $0 \leq i \leq 2^{d+1} - 2$, then $\omega^i = 1$.

As $S$ acts regularly on $X^\#$, $S$ is also an irreducible cyclic subgroup of $GL(X) \cong GL_{d+1}(2)$. Thus we can identify $X$ with $GF(2^{d+1})$ such that for each $h \in S$ there exists an element $\omega_1(h)$ satisfying $x^h = \omega_1(h)x$ ($x \in X$). Notice that $\omega_1$ gives a bijection of $S$ with $GF(2^{d+1})^\times$, as $S$ acts regularly on $X^\#$. On the other hand, the image of $\omega_2$ is a subgroup of $GF(2^{d+1})^\times$. Thus there exists an integer $\varepsilon$ with $0 \leq \varepsilon \leq 2^{d+1} - 2$ such that $\omega_2(g) = \omega_1(g)^\varepsilon$. Then we have $\omega_2(h) = \omega_2(g)^i = \omega_1(g)^{i\varepsilon} = \omega_1(h)^\varepsilon$ for all $h = g^i \in S$.

For each $t \in GF(2^{d+1})^\times$, there is a unique element $h \in S$ with $\omega_1(h) = t$. We denote $h$ by $g(t)$. Notice that $S = \{g(t) \mid t \in GF(2^{d+1})^\times\}$ and $g(t^{-1}) = g(t)^{-1}$. The conclusion in the above paragraph shows that under suitable identifications of $X$ and $[V, N]$ with $GF(q)$, $q := 2^{d+1}$, we have $x^{g(t)} = tx$ and $y^{g(t)} = t^{\varepsilon}y$ for every $x \in X$ and $y \in [V, N]$. Now, we identify $V = X \oplus [V, N]$ with $GF(q) \oplus GF(q)$ by sending $v = x + y$ ($x \in X$, $y \in [V, N]$) to $(x, y)$, where $x$ in the first entry (resp. $y$ in the second entry) is the correspondent to $x$ (resp. $y$) under the above identification of $X$ (resp. $[V, N]$) with $GF(q)$. Summarizing, we have obtained the following lemma.

**Lemma 9.** Assume the hypothesis of Theorem 1. Then there exist an identification of $V$ with $GF(q) \oplus GF(q)$, $q = 2^{d+1}$, and an integer $\varepsilon$ with $0 \leq \varepsilon \leq 2^{d+1} - 2$ such that the following properties hold:

1. $X$ and $[V, N]$ are identified with $\{(x, 0) \mid x \in GF(q)\}$ and $\{(0, y) \mid y \in GF(q)\}$ respectively.
2. For each $t \in GF(q)^\times$, there is a unique element $g(t)$ of the cyclic group $S$ satisfying $(x, y)^{g(t)} = (tx, t^{\varepsilon}y)$ and $g(t)^{-1} = g(t^{-1})$ for every $x, y \in GF(q)$.

Take an involution $n$ of $N^\#$. Then for every $x \in GF(q)$, the element $(x, 0) + (x, 0)^n$ lies in $[V, N] = \{(0, y) \mid y \in GF(q)\}$. Thus there exists a map $f$ from $GF(q)$ to itself such that

$$(x, 0)^n = (x, 0) + (0, f(x)) = (x, f(x))$$

for all $x \in GF(q)$. As $n$ is $GF(2)$-linear on $V$, we see that the map $f$ is $GF(2)$-linear as well. Thus $f$ is represented by a polynomial of the following shape for some $a_i$ in $GF(q)$ ($0 \leq i \leq d$):

$$f(X) = a_0X + a_1X^2 + \cdots + a_iX^{2^i} + \cdots + a_dX^{2^d}. \quad (1)$$

Notice that $f$ is not the zero map, for otherwise $n \in N^\#$ would fix all vectors of $X$ and whence $X = X^n$, contradicting the regularity of $N$ on $S$. Thus there is at least one $i$ with $0 \leq i \leq d$ such that $a_i \neq 0$. Notice also that there is $x_0 \in GF(q)^\times$ such that $f(x_0) = 0$, as $[X, n] = \{(0, f(x)) \mid x \in GF(q)\}$ is of dimension $d$.

Using the above index $i$ and the above element $x_0$ of $GF(q)^\times$, we introduce a new identification of $V$ with $GF(q) \oplus GF(q)$ by shifting the original identification. Tentatively we denote by $[x, y]$ the vector of $GF(q) \oplus GF(q)$ corresponding to $x + y \in V = X \oplus [V, N]$ via the new identification.

$$(x, y) = [x_0^{-1}x, ((a_i x_0^{2^i})^{-1}y)^{2^{d+1-i}}], \quad \text{or equivalently}$$

$$[x, y] = (x_0x, a_i x_0^{2^i} y^{2^i}).$$
Then the following hold for \( x \in GF(q) \), \( t \in GF(q)^\times \) and the involution \( n \in N \).

\[
[x, y]^{g(t)} = (t x_0 x, t^e a_i x_0^{2^i} y^{2^j}) = [t x, t^e x^{2d+1-i} y].
\]

\[
[x, 0]^n = (x_0 x, f(x_0 x)) = [x, ((a_i x_0^{2^i})^{-1} f(x_0 x))^{2d+1-i}].
\]

With the new identification, the first equation above shows that the property2 in Lemma 9 holds, if we replace \( \varepsilon \) by \( \varepsilon 2^{d+1-i} \) (modulo \( 2^{d+1} - 1 \)). Furthermore, the second equation above shows that, with the new identification, the linear map \( \tilde{f} \) on \( GF(q) \) defined by \([x, 0]^n = [x, \tilde{f}(x)]\) is given by the polynomial \((a_i x_0^{2^i})^{-1} f(x_0 X)^{2d+1-i}\) (modulo \( X^{2d+1} - X \)). In particular, if we denote \( \tilde{f}(X) = \sum_{j=0}^{d} \tilde{a}_j X^{2^j} \), then we have \( \tilde{a}_0 = 1 \) and \( \tilde{f}(1) = \sum_{j=0}^{d} \tilde{a}_j = 0 \).

Hence, if we replace the original identification (resp. \( \varepsilon \) and \( \tilde{f}(X) \)) by the new one (resp. \( \varepsilon 2^{d+1-i} \) and \( \tilde{f}(X) \)), then the following lemma holds.

**Lemma 10.** In Eq. (1), we may assume that \( a_0 = 1 \) and \( f(1) = 1 + a_1 + \cdots + a_d = 0 \) by a suitable change of identification of \( V \) with \( GF(q) \oplus GF(q) \). In particular, there is at least one index \( i_0 \) with \( 1 \leq i_0 \leq d \) such that \( a_{i_0} \neq 0 \).

In this section, we use the symbols \( a_k \) (\( 0 \leq k \leq d \)) to denote the coefficients of the polynomial \( f(X) \) above satisfying the conditions in Lemma 10. Note that \( a_k \) (\( 0 \leq k \leq d \)) are uniquely determined by \( n \in N \).

As \( N \) acts trivially on \([V, N]\) by Lemma 8, for every \( x, y \in GF(q) \) we have

\[
(x, y)^n = (x, 0)^n + (0, y)^n = (x, f(x)) + (0, y) = (x, f(x) + y).
\]  

(2)

Now take any \( t \in GF(q)^\times \) and consider the unique element \( g(t) \) of \( S \) in Lemma 9. We calculate the action of an involution \( g(t)^{-1} n g(t) \) of \( N \). From property2 of Lemma 9 together with Eq. (2), for every \( x, y \in GF(q) \) we have

\[
(x, y)^{g(t)^{-1} n g(t)} = (t^{-1} x, t^{-e} y)^{g(t)}
= (t^{-1} x, f(t^{-1} x) + t^{-e} y)^{g(t)} = (x, t^e f(t^{-1} x) + y).
\]  

(3)

In particular, \( X^{g(t)^{-1} n g(t)} = \{ (x, t^{e} f(t^{-1} x)) \mid x \in GF(q) \} \).

Since \( S \) acts regularly on \( X^\# \), it acts on \( N^\# \) regularly as well by conjugation, via the equivalence remarked earlier. Since for every \( s, t \in GF(q)^\times \) with \( s \neq t \) the element \( g(s)^{-1} n g(s) \cdot g(t)^{-1} n g(t) \) lies in \( N^\# \), there is a unique element \( u \in GF(q)^\times \) with \( g(s)^{-1} n g(s) \cdot g(t)^{-1} n g(t) = g(u)^{-1} n g(u) \). Applying both sides of this equation to \((x, 0)\), the following formula is obtained from Eq. (3):

\[
(x, 0)^{g(s)^{-1} n g(s) \cdot g(t)^{-1} n g(t)} = (x, s^{e} f(s^{-1} x))^{g(t)^{-1} n g(t)}
= (x, s^{e} f(s^{-1} x) + t^{e} f(t^{-1} x)) = (x, u^{e} f(u^{-1} x)).
\]

Hence we have

\[
s^{e} f(s^{-1} x) + t^{e} f(t^{-1} x) = u^{e} f(u^{-1} x)
\]

for every \( x \in GF(q) \). Now we rewrite both sides of this formula, using Eq. (1). As \( t^{e} f(t^{-1} x) = \sum_{i=0}^{d} t^{e-2^i} a_i x^{2^i} \), we then obtain the following equation for all \( x \in GF(q) \):

\[
\sum_{i=0}^{d} (s^{e-2^i} + t^{e-2^i} - u^{e-2^i})a_i x^{2^i} = 0.
\]
It can be verified that this happens only when \((s^{e-2i} + t^{e-2i} - u^{e-2i})a_i\) are all 0 \((i = 0, \ldots, d)\).
Remark that \(u\) is uniquely determined by the distinct elements \(s\) and \(t\) of \(GF(q)^*\), but is independent of \(i\) \((0 \leq i \leq d)\). Hence we proved:

**Lemma 11.** For every \(s, t \in GF(q)^*\) with \(s \neq t\), there is a unique element \(u \in GF(q)^*\) such that one of the following holds for each \(i = 0, \ldots, d\):

1. \(a_i = 0\).
2. \(s^{e-2i} + t^{e-2i} = u^{e-2i}\).

**Lemma 12.** Let \(i_0\) be an integer such that \(1 \leq i_0 \leq d\) and \(a_{i_0} \neq 0\) as in Lemma 10, and let \(\sigma = 2^{i_0}\). Then \(e - 1\) is invertible modulo \(2^{d+1} - 1\) and \((e - \sigma)(e - 1)^{-1} = 2^a\) for some \(0 \leq a \leq d\) modulo \(2^{d+1} - 1\).

**Proof.** From Lemma 11 applied to \(i = 0\) and to the index \(i_0\) in the statement of the lemma, we conclude that for every distinct \(s, t \in GF(q)^*\) there exists \(u \in GF(q)^*\) such that

\[ s^{e-1} + t^{e-1} = u^{e-1} \quad \text{and} \quad s^{e-\sigma} + t^{e-\sigma} = u^{e-\sigma}. \]

Suppose that \(s^{e-1} = t^{e-1}\) for some distinct \(s, t \in GF(q)^*\). Then we have \(u^{e-1} = 0\) for an element \(u \in GF(q)^*\), which is a contradiction. Hence \(GF(q)^* \ni x \mapsto x^{e-1} \in GF(q)\) is an injection and then a bijection. Therefore \(e - 1\) is an invertible element in the quotient ring \(Z/(2^{d+1} - 1)\).

From the above equations we have

\[ (s^{e-1} + t^{e-1})^{e-\sigma} = u^{(e-1)(e-\sigma)} = (s^{e-\sigma} + t^{e-\sigma})^{e-1}. \]

Dividing both sides by \(u^{(e-\sigma)(e-1)}\), we have \((s/t)^{e-1} + 1)^{e-\sigma} = ((s/t)^{e-\sigma} + 1)^{e-1}\) for every distinct \(s, t \in GF(q)^*\). Then, setting \(\delta := (e - \sigma)(e - 1)^{-1}\) and \(v = (s/t)^{e-1}\), we have

\[ (v + 1)^\delta = v^\delta + 1 \]

for all \(v \in GF(q)^*\). As \(\delta\) preserves the multiplication, it follows from this equation that \(\delta\) preserves the addition as well. Hence, by defining \(0^\delta = 0\), the map \(GF(q) \ni x \mapsto x^\delta \in GF(q)\) is a Galois automorphism of \(GF(q)\). Hence modulo \(2^{d+1} - 1\), we have \(\delta \equiv 2^a\) modulo \(2^{d+1} - 1\) for some \(a\) with \(0 \leq a \leq d\). \(\square\)

**Lemma 13.** There is exactly one integer \(i\) with \(1 \leq i \leq d\) such that \(a_i \neq 0\).

To prove Lemma 13, we prepare a result on the solutions of some congruence relations modulo \(2^{d+1} - 1\).

**Lemma 14.** Let \(i_k\) \((k = 1, \ldots, 5)\) be integers modulo \(d + 1\) which satisfy

\[ 1 + 2^{i_1} + 2^{i_2} \equiv 2^{i_3} + 2^{i_4} + 2^{i_5} \pmod{2^{d+1} - 1}. \]

Then one of the following holds modulo \(d + 1\) after suitably permuting \(\{i_1, i_2\}\) and \(\{i_3, i_4, i_5\}\):

- (o) \((i_3, i_4, i_5) \equiv (0, i_1, i_2)\).
- (p) \(i_1 \equiv i_2\) and \((i_3, i_4, i_5) \equiv (0, i_1, i_1)\).
- (p') \(i_1 \equiv i_2\) and \((i_3, i_4, i_5) \equiv (-1, -1, i_1 + 1)\).
- (q) \(i_1 \equiv 0 \neq i_2, i_3 \equiv i_4 \equiv 0\) and \(i_5 \equiv i_2\).
- (q') \(i_1 \equiv 0 \neq i_2, i_3 \equiv i_4 \equiv i_2 - 1\) and \(i_5 \equiv 1\).
Lemma 12. Suppose there exist 1

For integers $i, j, k, i', j'k'$, we use the symbol $(i, j, k) \equiv (i', j', k')$ to denote the following congruence relations, after suitably permuting entries $i, j, k$ and $i', j', k'$: $i \equiv i', j \equiv j'$ and $k \equiv k'$ modulo $d + 1$.

For $k = 1, \ldots, 5$, let $j_k$ be the integer in $\{0, \ldots, d\}$ such that $j_k \equiv i_k$ modulo $d + 1$. Then we have

$$1 + 2^{j_1} + 2^{j_2} - (2^{j_3} + 2^{j_4} + 2^{j_5}) = l(2^{d+1} - 1) \quad (4)$$

for some integer $l$. Suppose that $j_1, \ldots, j_5$ are distinct integers in $\{0, \ldots, d\}$. Then $d \geq 4$ and

$$|l|(2^{d+1} - 1) \leq 1 + 2^d + 2^{d-1} + 2^{d-2} + 2^{d-3} + 2^{d-4} = 1 + 2^{d-4}(1 + 2 + \cdots + 4)$$

$$= 1 + 2^{d-4}(2^5 - 1) = 2^{d+1} - (2^{d-4} - 1).$$

The last value is at most $2^{d+1} - 1$ if $d \geq 5$. In particular, if $l \neq 0$, then $l = \pm 1$ and we have either $d = 4$ and $(j_1, \ldots, j_5) = \{0, \ldots, 4\}$ or $d = 5$ and $(j_1, \ldots, j_5) = \{1, \ldots, 5\}$. However, we can verify that equality (4) does not hold in these cases. Thus we have $l = 0$ and

$$1 + 2^{j_1} + 2^{j_2} = 2^{j_3} + 2^{j_4} + 2^{j_5}.$$

If all $j_k$ ($k = 1, \ldots, 5$) are positive, this equality does not hold. Thus one of $(j_1, j_2)$ is 0 or one of $(j_3, j_4, j_5)$ is 0. In the latter case, we may assume that $j_3 = 0$. Then we have $2^{j_1} + 2^{j_2} = 2^{j_4} + 2^{j_5}$ from the above equality. However, this is impossible, as $j_k$ ($k = 1, 2, 4, 5$) are distinct positive integers. In the former case, we may assume that $j_1 = 0$. Then we have

$$1 + 2^{j_2-1} = 2^{j_3-1} + 2^{j_4-1} + 2^{j_5-1}.$$

From [1, VIII, Lemma 4.5(b)], this holds only when $(i_3 - 1, i_4 - 1, i_5 - 1) \equiv (0, i_2 - 2, i_2 - 2)$ or $(-1, -1, i_2 - 2)$. Both cases do not hold, as $i_3, i_4, i_5$ are mutually distinct.

Hence we conclude that some of $j_1, \ldots, j_5$ are the same. In the case $j_1 = j_2$, we have $1 + 2^{i_1+1} \equiv 2^{i_3} + 2^{i_4} + 2^{i_5}$ (mod $2^{d+1} - 1$). From [1, VIII, Lemma 4.5(b)] we have $(i_3, i_4, i_5) \equiv (0, i_1, i_1)$ or $(-1, -1, i_1 + 1)$. These are the first two solutions $(p)$ and $(p')$ of the lemma.

In the remaining case, we have $j_1 \neq j_2$. Without loss of generality, we may assume that either $j_1 = j_4$ or $j_3 = j_4$. In the former case, we have $1 + 2^{j_2} \equiv 2^{j_3} + 2^{j_5}$ (mod $2^{d+1} - 1$). Then $(0, i_2) \equiv (i_3, i_5)$ by [1, VIII, Lemma 4.4(c)]. This gives solution $(o)$ in the lemma. In the latter case, we have

$$1 + 2^{i_3+1} - i_5 \equiv 2^{-i_5} + 2^{i_1-i_5} + 2^{i_2-i_5} \quad \text{(mod $2^{d+1} - 1$)}$$

from the given congruence relation. Then we have $(-i_5, i_1 - i_5, i_2 - i_5) \equiv (0, i_3 - i_5, i_3 - i_5)$ or $(-1, -1, i_3 - i_5 + 1)$ by [1, VIII, Lemma 4.5(b)]. Hence $(0, i_1, i_2) \equiv (i_3, i_3, i_5)$ or $(i_5 - 1, i_5 - 1, i_3 + 1)$. In the former case, $(i_1, i_2) \equiv (i_3, i_5)$, as $j_1 \neq j_2$. Then $i_3 \equiv 0$ and we have solution $(q)$ in the lemma after suitably permuting $\{i_1, i_2\}$ and $\{i_3, i_4, i_5\}$. In the latter case where $(0, i_1, i_2) \equiv (i_5 - 1, i_5 - 1, i_3 + 1)$, one of $i_1, i_2$ is $i_5 - 1$ and the other is $i_3 + 1$, as we assumed $j_1 \neq j_2$. In particular, $j_5 = 1$. By replacing $i_1$ and $i_2$ if necessarily, we have the last solution $(q')$. \(\square\)

Proof of Lemma 13. Suppose there exist $1 \leq i < j \leq d$ such that $a_i \neq 0$ and $a_j \neq 0$. Then it follows from Lemma 12 that

$$(\varepsilon - 2^i)(\varepsilon - 1)^{-1} \equiv 2^a \quad \text{and} \quad (\varepsilon - 2^j)(\varepsilon - 1)^{-1} \equiv 2^b \quad \text{(modulo $2^{d+1} - 1$)}$$

for some integers $a, b$ with $0 \leq a, b \leq d$. Notice that $a, b \neq 0$, for otherwise $i$ or $j$ would be 0. By a similar argument, $a \neq b$. 

\(\varepsilon - 2^i\)
Now from the above two congruence relations we have \( \varepsilon(2^a - 1) \equiv 2^a - 2^i \) and \( \varepsilon(2^b - 1) \equiv 2^b - 2^j \) modulo \( 2^{d+1} - 1 \). Hence we have

\[
(2^a - 2^i)(2^b - 1) \equiv \varepsilon(2^a - 1)(2^b - 1) \equiv (2^b - 2^j)(2^a - 1) \pmod{2^{d+1} - 1}.
\]

Developing both sides of this congruence equation and dividing by \( 2^i \), we have

\[
1 + 2^{b-i} + 2^{a+j-i} \equiv 2^b + 2^{a-i} + 2^{j-i} \pmod{2^{d+1} - 1}.
\]

(5)

Notice that \( b \) and \( j - i \) are nonzero integers modulo \( d + 1 \) by the remark above and assumption that \( i < j \).

We apply Lemma 14 with \( (i_1, i_2) \equiv (b - i, a + j - i) \) and \( (i_3, i_4, i_5) \equiv (b, a - i, j - i) \) to find solutions for Eq. (5). In the following two paragraphs, congruence relations are considered modulo \( d + 1 \). If case (o) in the lemma holds, then the unique possibility is \( a - i \equiv 0, b - i \equiv j - i \), and \( a + j - i \equiv b \), because \( i \neq 0 \). Then we have a solution \( a \equiv i \) and \( b \equiv j \) for Eq. (5).

We show that this is the unique solution for Eq. (5). If case (p) of Lemma 14 holds, we have \( i_1 = b - i \equiv a + j - i = i_2 \) and \( (b, a - i, j - i) \equiv (0, i_1, i_1) \). As \( b \neq 0 \) and \( j - i \neq 0 \), we have \( a - i \equiv 0 \) and \( b = j - i \equiv a + j - i \). In particular, we have \( a \equiv 0 \), which contradicts the above remark. If case (q) of Lemma 14 holds, we have \( i_1 = b - i \equiv i_2 = a + j - i \) and three choices for \( (b, a - i, j - i) \) to be congruent to \( i_1 + 1 \) (the rest are congruent to \(-1\)). If \( i_1 + 1 \equiv b \) (resp. \( a - i \) or \( j - i \)) then we can verify that \( a \equiv 0 \) (resp. \( i \equiv 0 \) or \( j \equiv 0 \)), which is a contradiction. Since two of \( (b, a - i, j - i) \) are nonzero modulo \( d + 1 \), the above congruence relation does not have a solution of type \( (q) \) in Lemma 14. If case \( (q') \) of Lemma 14 holds, we have in total 6 cases to examine: \( (0, i_2) \equiv (b - i, a + j - i) \) or \( (a + j - i, b - i) \), and \( (1, i_2 - 1, i_1 - 1) \equiv (b, a - i, j - i), (a - i, b, j - i) \) or \( (j - i, b, a - i) \), each of which can be deleted by straightforward calculations. Thus there is no solution for Eq. (5) other than \( a \equiv i \) and \( b \equiv j \).

Now we show that \( a \neq i \). Suppose that \( a \equiv i \) modulo \( d + 1 \). Then \( 2^a \equiv (\varepsilon - 2^a)(\varepsilon - 1)^{-1} \) from which we have \( \varepsilon(2^a - 1) \equiv 0 \pmod{2^{d+1} - 1} \). This implies that

\[
(x^\varepsilon)^a = x^\varepsilon \quad \text{for all } x \in GF(q),
\]

where \( \sigma \) denotes the Galois automorphism of \( GF(q) \) sending \( y \in GF(q) \) to \( y^{2^a} \in GF(q) \). Thus the subfield \( F \) generated by \( x^\varepsilon \) for all \( x \in GF(q) \) lies in the subfield of \( GF(q) \) fixed by \( \sigma \in Gal(GF(q)/GF(2)) \). Recall that the action of the cyclic group \( S \) on \( [V, N] \) is given by the multiplication by elements \( t^k \) \( (i \in GF(q)^\times) \) under the identification of \( [V, N] \) with \( GF(q) \) (see Lemma 9(2)). Hence the subfield \( F \) of \( GF(q) \) corresponds to the subspace of \( [V, N] \) spanned by the \( S \)-orbits on \( [V, N]^\times \). However, \( S \) acts on \( [V, N] \) irreducibly by Lemma 7. This implies that \( F = GF(q) \), corresponding to \( [V, N] \). Hence \( \sigma \) fixes all the elements of \( GF(q) \), whence \( \sigma = id_{GF(q)} \). This contradicts that \( a \equiv i \neq 0 \pmod{d + 1} \). Hence we do not have \( a \equiv i \) (mod \( d + 1 \)).

This eliminates all the solutions for Eq. (5). Thus there are no distinct \( i, j \) in \( \{1, \ldots, d\} \) with \( a_i \neq 0 \) and \( a_j \neq 0 \). \( \square \)

Remark. Observe that the assumption that \( \dim([V, N]) = d + 1 \) is crucial in the last part of the above proof. This is the main reason why we cannot apply the arguments in the proof of Theorem 1 to obtain a similar result in the case \( \dim(V) = 2d + 1 \). In this case, \( \dim([V, N]) = d \), whence \( S \) acts trivially on \( [V, N] \). Thus \( \varepsilon = 0 \). Up to Lemma 13, many arguments go through with \( \varepsilon = 0 \). For example, Lemma 12 trivially holds, as \( (\varepsilon - \sigma)(\varepsilon - 1)^{-1} = \sigma \). However, we do
not establish the uniqueness of \(i\) with \(1 \leq i \leq d\) and \(a_i \neq 0\), because the field \(F\) in the proof above is just \(GF(2)\) if \(\varepsilon = 0\).

**Proof of Theorem 1.** Now we can complete the proof of Theorem 1. From Lemma 13, there is exactly one integer \(i\) with \(1 \leq i \leq d\) such that \(a_i \neq 0\). Then we have \(f(X) = X + a_iX^{2^i}\). As \(f(1) = 0\) by Lemma 10, we have \(a_i = 1\). Let \(\sigma = 2^i\), identified with the field automorphism \(GF(q) \ni x \mapsto x^{2^i} \in GF(q)\). Then for each \(t \in GF(q)^\times\) and \(x \in GF(q)\) we have

\[t^\varepsilon f(t^{-1}x) = t^{\varepsilon - 1}x + t^{\varepsilon - \sigma}x^\sigma.\]

Since \((\varepsilon - \sigma)(\varepsilon - 1)^{-1}\) can be considered as a field automorphism of \(GF(q)\) over \(GF(2)\) by Lemma 12, it has the inverse map \(\tau = (\varepsilon - \sigma)^{-1}(\varepsilon - 1)\), lying also in \(Gal(GF(q)/GF(2))\). Setting \(s := t^{\varepsilon - \sigma}\), we have \(t^s f(t^{-1}x) = s^tx + sx^\sigma\). Thus from Eq. (3) we have

\[X^{\delta(t)^{-1}ng(t)} = ((x, t^s f(t^{-1}x)) | x \in GF(q)) = ((x, sx^\sigma + s^tx) | x \in GF(q))\]

for every \(t \in GF(q)^\times\) and \(x \in GF(q)\). This is the presentation of the member \(X(s)\) in the \(d\)-dual hyperoval \(S_{\sigma, \tau}^{d+1}\) (see [3]). As \(X(0) = X\), we have \(S = \{X, X^{\delta(t)^{-1}ng(t)} | t \in GF(q)^\times\} = S_{\sigma, \tau}^{d+1}\) with both \(\sigma\) and \(\tau\) lying in \(Gal(GF(q)/GF(2))\). This establishes Theorem 1. \(\square\)

4. Some classifications

In this section, we prove Theorems 2 and 3. We always assume that \(d\) is a positive integer with \(d \geq 2\). We first give some preliminary remarks.

Let \(S\) be a \(d\)-dual hyperoval over \(GF(2)\) with ambient space \(V\) of dimension \(2d + 1\) or \(2d + 2\). Assume that a subgroup \(G\) of \(Aut(S)\) acts doubly transitively on \(S\). Then \(G = N: G_X\) for the regular normal subgroup \(N\) and the stabilizer \(G_X\) of \(X \in S\). From [4], either \(G_X\) is a subgroup of \(L_1(2^{d+1}) \cong Z_{2d+1}: Z_{d+1}\) acting regularly on \(X^#\) or \(G_X\) contains one of the following groups as a normal subgroup \(L_X\) (here \(H'\) denotes the commutator subgroup of \(H\)):

\[SL_1(r)\text{ for some divisor } l \text{ of } d + 1 \text{ with } l \geq 2 \text{ and } r = 2^{(d+1)/l},\]

\[Sp_{2l}(r)' \text{ for some divisor } 2l \text{ of } d + 1 \text{ with } 2l \geq 4 \text{ and } r = 2^{(d+1)/(2l)},\]

\[G_2(r)' \text{ for some } r = 2^{(d+1)/6}, \text{ where 6 divides } d + 1.\]

Notice that \((l, r) \neq (2, 2)\) if \(L_X \cong SL_1(r)\), as \(d \neq 1\). Thus \(L_X = L'_X\) in each case above. Moreover, if \(L_X \cong Sp_{2l}(r)'\) (resp. \(L_X \cong G_2(r)\)′), it is not isomorphic to \(Sp_{2l}(r)\) (resp. \(G_2(r)\)) if and only if \((d, 2l, r) = (3, 4, 2)\) (resp. \((d, r) = (5, 2))\).

In the proofs of Theorems 2 and 3, the letter \(L_X\) is used to denote the above normal subgroup of \(G_X\).

It follows from the classification of doubly transitive groups of affine type that the action of \(L_X\) on \(X\) is natural. Namely, if \(L_X \cong SL_1(r)\), the action of \(L_X\) on \(X\) is equivalent to the action of the matrix group \(SL_1(r)\) on the row vector space \(GF(r)^1\) given by the matrix multiplication from the right. If \(L_X \cong Sp_{2l}(r)\)' the action of \(L_X\) on \(X\) is equivalent to the action of matrix group \(Sp_{2l}(r)\)' preserving symplectic form \(f(x, y) = \sum_{i=1}^{2l} x_iy_{2l+1-i}\) on \(GF(r)^{2l}\), given by the matrix multiplication from right. In the proofs of Theorems 2 and 3, subspaces of \(X\) corresponding to totally isotropic subspaces of \(GF(r)^{2l}\) with respect to \(f\) are just called totally isotropic subspaces. If \(L_X \cong G_2(r)'\), recall that \(G_2(r)\)' is a subgroup of the 7-dimensional orthogonal group \(SO_7(r)\) preserving orthogonal form \(Q(x) = x_1^2 + \sum_{i=1}^{6} x_ix_{7-i}\) on \(GF(r)^7\). The symplectic form \(f_Q(x, y) = Q(x + y) + Q(x) + Q(y) = \sum_{i=1}^{6} x_iy_{7-i}\) associated with \(Q\).
has the 1-dimensional radical $R$ in $GF(r)^7$, whence the action of $SO_7(r)$ on $GF(r)^7$ induces an action of $SO_7(r)$ on $GF(r)^7/R$. The action of $L_X \cong G_2(r)'$ on $X$ is equivalent to the restriction onto $G_2(r)'$ of this action of $SO_7(r)$ on $GF(r)^7/R$. Remark that $G_2(r)'$ preserves a generalized hexagon consisting of some 1- and 2-dimensional subspaces of $GF(r)^7/R$ which correspond to totally singular subspaces of $GF(r)^7$ with respect to $Q$. In the proofs of Theorems 2 and 3, subspaces of $X \cong GF(r)^7/R$ corresponding to totally singular subspaces of $GF(r)^7$ with respect to $Q$ are just called totally singular subspaces.

Notice that in each case above, if $L_X$ acts on a vector space $W$ over $GF(2)$ of dimension smaller than $d + 1$, the action of $L_X$ on $W$ is trivial. This observation follows from the existence of a Sylow $p$-subgroup for a 2-primitive prime divisor $p$ of $2^{d+1} - 1$ or its modification, according as $d \neq 5$ or $d = 5$. See the argument in Lemma 7.

**Proof of Theorem 2.** Let $S$ be a $d$-dual hyperoval over $GF(2)$ with ambient space $V$ of dimension $2d + 1$. Assume that a subgroup $G$ of $Aut(S)$ acts doubly transitively on $S$. Then $G = N : G_X$ for the regular normal subgroup $N$ and the stabilizer $G_X$ of $X \in S$. From [4], either $G_X$ is a group described in the theorem or $G_X$ contains a normal subgroup $L_X$ in the remark above:

Suppose that $G_X$ has the normal subgroup $L_X$ above. Then $L_X$ acts on $[V, N]$, which is of dimension $d$ over $GF(2)$. The last remark previous to the proof shows that $L_X$ acts trivially on $[V, N]$. Let $a$ be a nonzero vector, a nonzero vector, or a nonzero singular vector of $X$, according as $L_X \cong SL_d(r)$, $Sp_{2d}(r)'$, or $G_2(r)'$. As $L_X$ naturally acts on $X$, the stabilizer $P_a$ of $a$ in $L_X$ is a parabolic subgroup of $L_X$ and it acts nontrivially on the factor space $X/\langle a \rangle$.

On the other hand, let $n$ be the unique involution of $N$ with $a \in X \cap X^n$. Then $P_a$ centralizes $n$ by the regularity of $N$ on $S$. Moreover, $P_a (\leq L_X)$ centralizes $[X, n] (\leq [V, N])$. Thus for each $x \in X$ and any $g \in P_a$ we have $x + x^n = (x + x^n)^g = x^g + x^g$, whence $x + x^g = (x + x^g)^n$. This implies that $x + x^g$ lies in $X \cap X^n = \{0, a\}$ for every $x \in X$, or equivalently, $x^g \in x + \langle a \rangle$ for every $x \in X$. Thus $P_a$ acts trivially on $X/\langle a \rangle$, which contradicts the remark in the above paragraph. □

Next we make an observation, which is a refinement of [3, Lemma 4].

**Lemma 15.** Let $S$ be a $d$-dual hyperoval over $GF(2)$ on which a group $G = N : G_X$ acts doubly transitively with a regular normal subgroup $N$. Assume that there is a subgroup $P$ of $G_X$ and a normal subgroup $U$ of $P$ such that $P$ acts transitively on $C_X(U)#$, the set of nonzero vectors of $X$ fixed by all elements of $U$. Let

$$S(U) := \{ Y \in S \mid Y^u = Y (\forall u \in U) \} \quad \text{and} \quad S[U] := \{ C_Y(U) \mid Y \in S(U) \}.$$ 

If $C_X(U)$ has a dimension $e + 1$ over $GF(2)$ with $e \geq 1$, then $S[U]$ is an $e$-dual hyperoval over $GF(2)$ on which $C_N(U) : (P/U)$ acts doubly transitively.

**Proof.** The argument in [3, Lemma 4] shows that $S[U]$ is an $e$-dual hyperoval. By construction, $U$ acts trivially on the ambient space of $S[U]$. We show that

$$S(U) \setminus \{X\} = \{ Y \in S \setminus \{X\} \mid X \cap Y \subset C_X(U) \} = \{ X^n \mid n \in C_{N^#}(U) \}.$$ 

If $X^n (n \in N^#)$ lies in $S(U)$, we have $X^{u^{-1}nu} = X^{nu} = X^n$ for all $u \in U$. By the regularity of $N$ on $S$, we have $u^{-1}nu = n$ for all $u \in U$. Thus $n \in C_N(U)$. In particular, $X \cap X^n \subset C_X(U)$. Conversely, take any projective point of $C_X(U)$ and write it as $X \cap Y$ for some $Y \in S \setminus \{X\}$. Take $n \in N$ with $Y = X^n$. Then $X \cap X^n = X \cap X^{nu}$ for all $u \in U$, as $X \cap Y \subset C_X(U)$. As three distinct members of $S$ intersect trivially, we have $X^n = X^{nu}$ for all $u \in U$. Thus $Y = X^n \in S(U)$. 


From the above description of $S(U)$, it is immediate to see that $C_N(U)$ acts regularly on it. Since $e \geq 1$, then $C_N(U)$ acts regularly on $S[U]$. As $P/U$ is transitive on $C_X(U)^\#$, we conclude that $C_N(U) : (P/U)$ acts doubly transitively on $S[U]$. □

**Proof of Theorem 3.** Let $S$ be a $d$-dual hyperoval over $GF(2)$ admitting a doubly transitive group $G$ with ambient space of dimension $2d + 2$. Then $G = N : G_X$ for the regular normal subgroup $N$ and the stabilizer $G_X$ of a member $X$ of $S$. Then either $G_X$ is a subgroup of $\Gamma L_1(2^{d+1})$ acting regularly on $X^\#$ or $G_X$ has a normal subgroup $L_X$ described in the remarks previous to the proof of Theorem 2.

We will eliminate the latter case, except possibly the cases where either $d = 2, 3, 5$ or $l = 2$ and $L_X \cong SL_2(r)$ with $r = 2^{(d+1)/2}$. These exceptional cases are summarized as cases (2) and (3) in the theorem.

Notice that $L_X \cong Sp_{2l}(r)' \neq Sp_{2l}(r)$ if and only if $l = 2 = r$ and $(d + 1)/2l = 1$. Then we have case (3) in the theorem with $d = 3$ and $G_X \cong Sp_4(2)' \cong A_6$ or $S_6$. We do not have $G_X \cong M_{10}$, $PGL_2(9)$, or $Aut(A_8)$, for otherwise one of these groups would be a subgroup of $Aut(N) \cong GL_4(2)$. Similarly, if $L_X \cong G_2(r)' \neq G_2(r)$ then $r = 2$ and $(d + 1)/6 = 1$. Then we have case (3) with $d = 5$ and $G_X \cong G_2(2)' = G_2(2)$. Hence in the following we may assume that $L_X \cong SL_l(r)$, $Sp_{2l}(r) = Sp_{2l}'$ or $G_2(r) = G_2(r)'$.

We choose $U$ and $P$ to apply Lemma 15. Recall that the action of $L_X$ on $X$ is natural. If $L_X \cong SL_l(r)$, let $P$ be the stabilizer of an $(l - 1)$-dimensional subspace $W$ of $X$ over $GF(r)$, and let $U$ be the vectorwise stabilizer of $W$. Then $P/U \cong GL_{l-1}(r)$ acts naturally on $W = C_X(U)$. In particular, $P/U$ is transitive on $C_X(U)^\#$. If $L_X \cong Sp_{2l}(r)$, take $P$ to be the stabilizer of an $l$-dimensional totally isotropic subspace $W$ of $X$ and $U$ to be the vectorwise stabilizer of $W$. Then $P/U \cong GL_l(r)$ acts naturally on $W = C_X(U)$. In particular, $P/U$ is transitive on $C_X(U)^\#$. If $L_X \cong G_2(q)$, let $P$ be the stabilizer of a 2-dimensional singular subspace $W$ of $X$ corresponding to a line of the generalized hexagon associated with $L_X$, and let $U$ be the vectorwise stabilizer of $W$. Then $P/U \cong GL_2(r)$ acts naturally on $W = C_X(U)$. In particular, $P/U$ is transitive on $C_X(U)^\#$.

We set $e + 1 := \dim_{GF(2)}(C_X(U))$. Then we have $e + 1 = (l - 1) \times (d + 1)/l, l \times (d + 1)/2l$ or $(d + 1)/6$, according as $L_X \cong SL_l(r)$, $Sp_{2l}(r)$ or $G_2(r)$. Notice that $P/U$ contains a cyclic subgroup $S_U \cong Z_{e+1} \otimes GL(C_X(U))$ acting regularly on $C_X(U)^\#$.

We examine the cases where $0 \leq e \leq 2$. If $L_X \cong SL_l(r)$ for a divisor $l$ of $d + 1$ with $l \geq 2$ and $r = 2^{(d+1)/l}$, we have $e + 1 = (l - 1)(d + 1)/l$, or equivalently, $l - 1 = (e + 1)/(d - e)$. If $e = 0, 1$ or 2, we have $l - 1 = (1/d), 2/(d - 1)$ or $3/(d - 2)$, respectively. As $l - 1$ is a positive integer and $d \geq 2$, the possibility $e = 0$ does not occur. Furthermore, $e = 1$ if and only if $(d, l, r) = (2, 3, 2)$ and $L_X \cong SL_3(2)$ or $(d, l, r) = (3, 2, 4)$ and $L_X \cong SL_2(4) \cong A_5$, both of which are contained in case (2) of the theorem. (In the latter case, $G_X \cong A_5$ or $S_5$.) We have $e = 2$ if and only if $(d, l, r) = (3, 4, 2)$ and $(L_X, P/U) \cong (SL_4(2), SL_3(2))$, or $(d, l, r) = (5, 2, 3)$ and $(L_X, P/U) \cong (SL_2(8), Z_7)$. In the latter case, $G_X \cong SL_2(3) \otimes SL_2(2)^3 \otimes Z_3$, and this case is contained in case (2) of the theorem. Similarly, if $L_X \cong Sp_{2l}(r)$ for a divisor $2l$ of $d + 1$ with $2l \geq 4$ and $r = 2^{(d+1)/2l}$, we have $e + 1 = (d + 1)/2l$. Thus $e = 0$ does not occur, as $d \geq 2$. We have $e = 1$ if and only if $(d, 2l, r) = (3, 4, 2)$, which is contained in case (3). In this case, $L_X \cong Sp_4(2) \cong S_6$ is a normal subgroup of $G_X$. Notice that $G_X \cong Sp_4(2)$, because none of $\cong M_{10}, PGL_2(9)$ and $Aut(A_6)$ is a subgroup of $Aut(N) \cong SL_4(2) \cong A_8$. We have $e = 2$ if and only if $(d, 2l, r) = (5, 6, 2)$. In this case, $L_X = G_X \cong Sp_6(2)$ and $P/U \cong GL_3(2)$. This is contained in case (3).
Finally, if \( L_X \cong G_2(r) \) for a multiple \( d + 1 \) of 6 and \( r = 2^{(d+1)/6} \), we have \( e + 1 = (d + 1)/3 \). Thus \( e \neq 0 \) and \( e \neq 2 \), as \( d + 1 \) is a multiple of 6. Furthermore, \( e = 1 \) if and only if \( (d, r) = (5, 2) \), which is contained in case (3).

Summarizing, we have \( e \geq 1 \) for each case. Furthermore, if \( e = 1 \) or \( e = 2 \), then one of the possibilities in cases (2) and (3) of the theorem holds, except when \( e = 2, (d, l, r) = (3, 4, 2) \) and \( (L_X, P/U) \cong (SL_4(2), SL_3(2)) \).

We will remark that the centralizer \( C_{[V,N]}(U) \) of \( U \) in \([V, N] \) is of dimension at most \( e + 1 \) over \( GF(2) \). Fix a nonzero vector \( u \) of \( C_X(U) \), and let \( n := v(u) \) be the unique involution of \( N \) such that \( X \cap X^n = \{0, w\} \). From the regularity of the action of \( N \) on \( S \), we have \( n \in C_N(U) \). As \([X, n] \cong X/C_X(n) = X/(X \cap X^n) \) is of dimension \( d \), the subspace \([X, n] = \{x + x^n \mid x \in X\}\) is a hyperplane of \([V, N]\). Thus in order to show that \( \dim_{GF(2)}(C_{[V,N]}(U)) \leq e + 1 \), it suffices to show that \( \dim_{GF(2)}(C_{[X,n]}(U)) = e \).

Observe that \( C_{[X,n]}(U) \) contains a subspace \( \{x + x^n \mid x \in C_X(U)\} \), which is isomorphic to a space \( C_X(U)/[0, u] \) of dimension \( e \) over \( GF(2) \). Conversely, let \( x \) be an element of \( X \) such that \( U \) centralizes \( x + x^n \). Then \( (x + x^n)^u = x + x^n \) for every \( u \in U \), whence \( x + x^n = (x + x^n)^y \) for all \( u \in U \), as \([n, U] = 1 \). Thus \( x + x^n \) lies in \( C_X(n) = \{0, w\} \) for all \( u \in U \). On the other hand, we have \([U] = l^{-1} = 2^{e+1} \) (resp. \( r^{(d+1)/2} = (2^{e+1})^{(d+1)/2} \) and \( r^6 = (2^{e+1})^5/2 \) if \( L_X \cong SL_2(r) \) (resp. \( Sp_{2l}(r) \) and \( G_2(r) \)). As \( e \geq 1 \), we have \([U] \geq 4 \) in any case. Then, using the explicit matrix representation of \( L_X \) on the natural module \( X \), we can verify that for every \( y \in X \setminus C_X(U) \) there are distinct elements \( u \) and \( v \) of \( U \) such that \( y + y^u \) and \( y + y^v \) are distinct nonzero elements of \( X \). As \( x + x^n \in \langle u \rangle \) for every \( u \in U \), this implies that \( x \in C_X(U) \). Thus \( C_{[X,n]}(U) = \{x + x^n \mid x \in C_X(U)\} \) and \( \dim_{GF(2)}(C_{[X,n]}(U)) = e \), as we desired.

We now consider the \( e \)-dual hyperoval \( S[U] \) constructed by Lemma 15 with the above choice of \( U \) and \( P \). From the preceding two paragraphs, the subspace \( C_Y(U) = C_X(U) \oplus C_{[X,N]}(U) \) is of dimension at most \( 2(e + 1) \). The ambient space \( A(U) \) of the \( e \)-dual hyperoval \( S[U] \) over \( GF(2) \) lies in \( C_Y(U) \), whence \( \dim_{GF(2)}(A(U)) = 2e + 1 \) or \( 2e + 2 \).

As we saw above, we have \( e \geq 1 \). Moreover, the possibilities of \((d, l, r, L_X)\) for \( e = 1 \) are contained in cases (2) and (3) of the theorem. Thus we may assume that \( e \geq 2 \).

If \( \dim_{GF(2)}(A(U)) = 2e + 1 \) for \( e \geq 2 \), the \( e \)-dual hyperoval \( S[U] \) over \( GF(2) \) satisfies the hypotheses of Theorem 2 with doubly transitive automorphism group \( C_N(U) : (P/U) \). Thus it follows from Theorem 2 that \( P/U \) is isomorphic to a subgroup of the metacyclic group \( Z_{2^{d+1}+1} \). Assume that \( L_X \cong G_2(r) \) for a multiple \( d + 1 \) of 6 and \( r = 2^{(d+1)/6} \). In this case, \( e + 1 = (d + 1)/3 \) and \( P/U \cong GL_2(r) \). As \( GL_2(r) \) is metacyclic if and only if \( 2 = r = 2^{(d+1)/6} \), we have \( e = 1 \), which is a contradiction. If \( L_X \cong Sp_{2l}(r) \) for a divisor \( 2l \) of \( d + 1 \) with \( 2l \geq 4 \) and \( r = 2^{(d+1)/2l} \), we have \( e + 1 = (d + 1)/2 \) and \( P/U \cong GL_l(r) \). This is metacyclic if and only if \( l = 2 = r = 2^{(d+1)/2l} \), from which we have \( e = 1 \), a contradiction. If \( L_X \cong SL_l(r) \) for a divisor \( l \) of \( d + 1 \) with \( l \geq 2 \) and \( r = 2^{d+1/l} \), we have \( e + 1 = (l-1)(d+1)/l \) and \( P/U \cong GL_{l-1}(r) \). Thus \( P/U \) is metacyclic if and only if either \( l = 2 \) or \( (l, r) = (3, 2) \). In the latter case, we have \( d = 2 \) and \( e = 1 \), which is a contradiction. Summarizing, if \( \dim_{GF(2)}(A(U)) = 2e + 1 \) for \( e \geq 2 \), the only remaining possibility is \( l = 2 \). As this implies that \( d \) is odd and \( r = 2^{(d+1)/2} \), \( L_X \cong SL_2(2^{(d+1)/2}) \), this is contained in case (2) of the theorem.

Hence it remains to treat the case where \( \dim_{GF(2)}(A(U)) = 2e + 2 \) with \( e \geq 2 \). In this case, \( S[U] \) is an \( e \)-dual hyperoval over \( GF(2) \) with ambient space of dimension \( 2e + 2 \) (\( e \geq 2 \)), on which \( C_N(U) : (P/U) \) acts doubly transitively. Moreover, as we remarked above, \( P/U \) contains a cyclic subgroup \( S_U \) of order \( 2^{e+1} - 1 \) acting regularly on \( C_X(U)^\# \). Thus \( S[U] \) satisfies the hypotheses of Theorem 1. It follows from Theorem 1 that one of the following holds:
(i) \( e = 2 \) and \( \text{Aut}(\mathcal{S}[U]) \cong 2^3 : SL_3(2) \), or
(ii) \( e \geq 3 \) and \( \text{Aut}(\mathcal{S}[U]) \cong 2^{e+1} : (Z_{2^{e+1}-1} : Z_{e+1}) \).

If case (i) occurs, then \( e = 2 \). As we saw above, in this case, either one of the possibilities in case (3) of theorem occurs or \( (d, l, r) = (3, 4, 2) \) and \( (L_X, P/U) \cong (SL_4(2), SL_3(2)) \). In the exceptional case, \( SL_4(2) \) contains a cyclic subgroup of order 15 acting regularly on \( X^\# \). Then \( \mathcal{S} \) is isomorphic to \( S_{\sigma, r}^e \) and \( \text{Aut}(\mathcal{S}) \cong \text{Aut}(S_{\sigma, r}^e) \) is solvable by Theorem 1. However, this contradicts that \( \text{Aut}(\mathcal{S}) \) involves \( SL_4(2) \). Thus the exceptional case does not occur.

Hence we may assume that the case (ii) holds. In particular, \( P/U \) is metacyclic, as it is a subgroup of \( \text{Aut}(\mathcal{S}[U]) \) for a divisor \( l \) of \( d + 1 \) with \( l \geq 2 \) and \( r = 2^{(d+1)/2} \). Then \( P/U \cong GL_{l-1}(r) \) is metacyclic. This is possible only when \( l = 2 \). In this case, \( G_X \) is a subgroup of \( \text{Aut}(L_X) \cong GL_2(2^{(d+1)/2}) : Z_{d+2} \). Thus we have case (2). Assume that \( L_X \cong Sp_2(r) \) with a divisor \( 2l \) of \( d + 1 \) with \( 2l \geq 4 \) and \( r = 2^{(d+1)/2l} \). Then \( P/U \cong GL_1(r) \) is metacyclic, which occurs only when \( l = 2 = r \). Then \( d + 1 = 2l = 4 \). But \( e = (d - 1)/2 = 1 \), a contradiction. Finally assume that \( L_X \cong G_2(r) \) with a multiple \( d + 1 \) of 6 and \( r = 2^{(d+1)/6} \). Then \( P/U \cong GL_2(r) \) is metacyclic, which implies that \( r = 2 \) and \( d + 1 = 6 \). But then \( e = (d - 2)/3 = 1 \), a contradiction. We now exhausted all the cases. \( \square \)

Remark 16. In case (2) of Theorem 3, if \( \dim(A(U)) = 2e + 2 \) with \( e \geq 2 \), then we conclude that \( G_X \) does not contain \( GL_2(2^{(d+1)/2}) \).

This is verified as follows. Return to the last paragraph in the proof of Theorem 3. Assume that \( d \) is odd and \( L_X \cong SL_2(2^{(d+1)/2}) \). Suppose that \( G_X \) contains \( GL_2(2^{(d+1)/2}) \). Then \( G_X \) contains a cyclic group of order \( 2^{d+1} - 1 \) acting regularly on \( X^\# \), and we can apply Theorem 1 to \( \mathcal{S} \). Then we have either \( d = 2 \) or \( \text{Aut}(\mathcal{S}) \) is solvable. As \( d + 1 \) is even, \( d \neq 2 \). Furthermore, since \( L_X \cong SL_2(2^{(d+1)/2}) \) and \( (d + 1)/2 \geq 2 \) for \( d \geq 2 \), the group \( L_X \) involved in \( \text{Aut}(\mathcal{S}) \) is not solvable. This contradiction shows that \( G_X \) does not contain \( GL_2(2^{(d+1)/2}) \).

References