Doubly Transitive Dimensional Dual Hyperovals:
Universal Covers and Non-Bilinear Examples

Ulrich Dempwolff
Department of Mathematics,
University of Kaiserslautern, Erwin-Schroedinger-Strasse,
67653 Kaiserslautern, Germany
email: dempwolff@mathematik.uni-kl.de

Abstract

In [5] we showed, that a doubly transitive, non-solvable dimensional
dual hyperoval \( D \) is either isomorphic to the Mathieu dual hyperoval or
to a quotient of a Huybrechts dual hyperoval. In order to determine the
doubly transitive dimensional dual hyperovals, it remains to classify the
doubly transitive, solvable dimensional dual hyperovals and this paper is
a contribution to this problem. A doubly transitive, solvable dimensional
dual hyperoval \( D \) of rank \( n \) is defined over \( \mathbb{F}_2 \) and has an automorphism
of the form \( ES, E \) elementary abelian of order \( 2^n \) and \( S \leq \Gamma L(1, 2^n) \)
(see Yoshiara [13]). The known doubly transitive, solvable dimensional
dual hyperovals \( D \) are bilinear. In [2] the bilinear, doubly transitive,
solvable dimensional dual hyperovals \( D \) of rank \( n \) with \( GL(1, 2^n) \leq S \)
have been classified. Here we present two new classes of non-bilinear,
doubly transitive dimensional dual hyperovals. We also consider universal
covers of doubly transitive dimensional dual hyperovals, since they are
again doubly transitive dimensional dual hyperovals (see [3, Cor. 1.3]).
We shall determine the universal covers of the presently known doubly
transitive dimensional dual hyperovals.

1 Introduction

A set \( D \) of \( n \)-dimensional subspaces of a finite dimensional vector space \( V \) over
a finite field (say \( V = V(m, q) \)) is called a dual hyperoval of rank \( n \), we use the
symbol DHO as an abbreviation, if \( |D| = (q^n - 1)/(q - 1) + 1, \dim X_1 \cap X_2 = 1 \)
and \( X_1 \cap X_2 \cap X_3 = 0 \) for three different \( X_1, X_2, X_3 \in D \). The DHO splits over
the subspace \( Y \), if \( V = X \oplus Y \) for all \( X \in D \). The space \( U(D) = \langle X \mid X \in D \rangle \)
is called the ambient space of \( D \). Usually DHOs of rank \( n \) are called \( (n - 1)\)-
dimensional dual hyperovals. However in our context it seems more natural to
use the notion of vector spaces than the language of projective geometry. In
this paper we study exclusively DHOs over \( \mathbb{F}_2 \), in particular \( |D| = 2^n \).
Two DHOs $D$ and $D'$ are isomorphic, if there exists an invertible linear operator $\Psi$, that sends the ambient space of $D$ onto the ambient space of $D'$, such that $D' = D\Psi$. We usually will write linear mappings on the right hand side of an argument. Isomorphisms of $D$ onto $D$ are automorphisms, they form the automorphism group $\text{Aut}(D)$.

An elementary abelian 2-subgroup $T$ of the automorphism group of $D$ is a translation group, if $T$ acts regularly on $D$, such that the DHO splits over $C_U(T) = \{u \in U \mid u\tau = u, \tau \in T\}$ (the centralizer of $T$ in $U$). It was shown in $[1, \text{Thm. 3.2}]$, that, if the rank of the DHO is $\geq 3$, $T$ has quadratic action on $U$, i.e. $[U, T] \subseteq C_U(T)$, where $[U, T] = \langle u(1+\tau) \mid u \in U, \tau \in T \rangle$ is the commutator of $U$ and $T$. DHOs, that admit a translation group, are called bilinear.

Let $D$ and $D'$ be DHOs of rank $n$ with ambient spaces $U$ and $U'$ respectively. An epimorphism $\Psi : U' \to U$ is called a covering map, if $D = D'\Psi$. One says, that $D$ is a quotient of $D'$ and $D'$ a cover of $D$. In this case $D' \simeq D/W$, where $W = \ker \Psi$ and $D/W = \{(X+W)/W \mid X \in D\}$. The cover is proper, if $\Psi$ is not an isomorphism. A DHO is simply connected, if it has no proper cover. Every DHO $D$ has a unique, simply connected cover $\tilde{D}$, that is called the universal cover of $D$ (see $[3, \text{Thm. 1.1}]$).

A DHO is called solvable, non-solvable or doubly transitive, if its automorphism group is solvable, non-solvable or doubly transitive (on the members of $D$). The presently known doubly transitive DHOs are the Mathieu DHO over $\mathbb{F}_4$ (see $[12], [14]$) and bilinear DHOs over $\mathbb{F}_2$ consisting of the Yoshiara DHOs of type $S^n_{a,b}$ (see $[12], [11]$), quotients of the Huybrechts DHO (see $[4], [8], [12]$), and the DHOs of type $D[n,k]$ $^1$ (see $[2, \text{Example 3.3}]$). One might speculate, that all doubly transitive DHOs over $\mathbb{F}_2$ are bilinear. But contrary to this expectation (of the author), there exists a (new) class of solvable, non-bilinear doubly transitive DHOs:

**Theorem 1.1.** Let $1 < d < n$ be divisor of $n$, such that $n/d$ is odd. Let $1 < b < n$ be a multiple of $d$, such that $(b,n) = d$. Then there exist a DHO $D = D[n,d,b]$, such that the following hold.

(a) $G = \text{Aut}(D) \simeq \text{AGL}(1,2^n)$ acts doubly transitive on $D$.

(b) The ambient space of $D$ has dimension $2n + d - 1$.

(c) $D[n,d,b]$ is isomorphic to $D[n,d',b']$, iff $d = d'$ and $b = b$ or $n - b$.

(d) $D$ has no doubly transitive, bilinear quotient; in particular $D$ is not a bilinear DHO.

For odd $n_0$ we also present a second class of doubly transitive DHOs denoted by $\tilde{D}[2n_0]$ (see Definition 3.10), which turns out to be the universal covers of DHOs of type $D[n, -2^n/2+1 - 1]$ as well as the universal covers of DHOs of type $D[n, 2, n/2 \pm 1]$ (see assertions (b) and (c) of the next Theorem 1.2).

$^1$The DHOs of type $D[n,k]$ were called of type $D[k]$ in $[2]$. For clarity we include now the rank $n$ in the denotation of these DHOs.
The universal cover of a doubly transitive DHO is again doubly transitive by [3, Cor. 1.3]. So a necessary step in the classification of the doubly transitive DHOs is the determination of the universal covers of the known doubly transitive DHOs. The Mathieu DHO is simply connected [14] as well as the Huybrechts DHOs [12]. For the remaining, known doubly transitive DHOs the question of the universal cover is answered by:

**Theorem 1.2.** Let $D$ be a doubly transitive DHO over $\mathbb{F}_2$ of rank $n$.

(a) A DHO $D = S_{m,h}^n$, $h \neq m$, is simply connected.

(b) A DHO $D = D[n,k]$ is simply connected, except when $k = -2^{n_0+1} - 1$, $n = 2n_0$. In the latter case $D \simeq \hat{D}[2n_0]$.

(c) A DHO $D = D[n,d,b]$ is simply connected, except when $n = 2n_0$, $n_0$ odd, $d = 2$, $b = n_0 \pm 1$. In the latter case $\bar{D} \simeq \hat{D}[2n_0]$.

**Remark 1.3.** The DHOs $S_{h,h}^n$ are quotients of the Huybrechts DHO and thus are not simply connected for $n > 3$. [4] contains a discussion of the doubly transitive quotients of the Huybrechts DHOs. For a DHO $D = S_{h,m}^n$ the simple connectedness of a DHO $D$ over $\mathbb{F}_2$ has been established if $n = h + m$ by Pasinini and Yoshiara [10, Cor. 1.6] (and when $h \neq m$ with $n \leq 4$ [10, Result 4.4]), by showing the simple connectedness of the incidence geometry $Af(D)$ obtained from $D$.

In Section 2 we collect necessary results mainly needed in the proof of Theorem 1.2. We revise in Section 3 some known doubly transitive DHOs and present the construction of two series of non-bilinear, doubly transitive DHOs. In the last Section we determine the universal covers of the presently known doubly transitive DHOs.

### 2 Preliminaries

#### 2.1 Some notation

For a (given) positive number $n$ the symbol $F$ stands for the field $\mathbb{F}_{2^n}$. We set

1. $r_n = 2^n - 1$
2. $I_n = [0, r_n - 1] \cap \mathbb{Z}$ and
3. $R_{c,d} = c \frac{2^d - 1}{2^d - 2}$ for a divisor $d < n$ of $n$ and $0 \leq c < 2^d - 1$.
4. $Z$ will always denote a cyclic group of order $r_n$; we sometimes identify such a group with $(F^*, \cdot)$, the multiplicative group of $F$.

We call $k, m \in I_n$ equivalent and write $k \sim m$, if there exist a non-negative integer $s$, such that

$$m \equiv 2^s k \pmod{r_n}.$$
Usually one calls the equivalence classes cyclotomic cosets of $2$ modulo $n$. We call a cyclotomic coset long, if it has size $n$, and short otherwise.

Let $U, V$ be finite dimensional vector spaces, $U = U_1 \oplus U_2$, $V = V_1 \oplus V_2$ be vector space decompositions and $T : U \to V$ a linear mapping. We write

$$T = \begin{pmatrix} T_{11} & T_{12} \\ T_{21} & T_{22} \end{pmatrix},$$

where $T_{ij} = T_{U_i} \circ P_j$ (here $T_{U_i}$ is the restriction of $T$ to $U_i$ and $P_j$ is the projection of $V$ onto $V_j$). This convention will also be generalized in the obvious way.

### 2.2 Representations of cyclic groups

An operator $\sigma \in \text{GL}(n, q)$ of order $q^n - 1$ is called a Singer cycle and we call the group $S$ generated by $\sigma$ a Singer group. The following result is well known, see for instance [2], [7, II Satz 7.3].

**Lemma 2.1.** For every $n$ and every prime power $q$ the group $\text{GL}(U)$, $U = V(n, q)$, contains Singer groups. Moreover:

(a) Every two Singer groups are conjugate in $\text{GL}(U)$.

(b) Let $S = \langle \sigma \rangle$ be a Singer group. Then $N_{\text{GL}(U)}(S) = S \langle \phi \rangle$, $\phi$ has order $n$ and can be chosen such that $\sigma^\phi = \sigma^q$.

(c) Let $A \leq \text{GL}(U)$ be an irreducible abelian group. Then $A$ is cyclic and $C_{\text{GL}(U)}(A)$ is a Singer group.

For $1 \leq k < r_n$ define $D^k : Z \to \text{GL}(F)$, $Z = (F^*, \cdot)$, by $uD^k(b) = b^ku$, $u \in F$, $b \in Z$. Clearly, the eigenvalues of $D^k(b)$ lie in $F$, i.e. the degree of the minimal polynomial of a $D^k(b)$ is a divisor $d$ of $n$. As a direct consequence of Lemma 2.1 one has:

**Lemma 2.2.** Let $\zeta$ be a generator of $Z$.

(a) Equivalent are:

(1) $F$ as a $D^k(Z)$-module splits into a direct sum of $n/d$ isomorphic, simple modules all of degree $d$.

(2) The minimal polynomial of $D^k(\zeta)$ has degree $d$.

(b) Every irreducible representation of $Z$ over $F_2$ is isomorphic to a simple constituent of some representation $D^k$, $k \in I_n$.

(c) The representation $D^k$ is irreducible, iff $k$ lies in a long coset modulo $2$, and $D^k$ is faithful, iff $(k, r_n) = 1$.

(d) The irreducible constituents of $D^k$ and $D^\ell$ are isomorphic, iff $\ell \equiv 2^ak \pmod{r_n}$ for some integer $a$, i.e. the irreducible $F_2$-representations of $Z$ are in one-to-one correspondence with the cyclotomic cosets of $2$ modulo $n$. 

4
For $0 \leq k < n$ and $a \in F$ define the $F_2$-linear mapping $T_k(a) \in \text{End}(F)$ by

$$xT_k(a) = ax^{2^k}.$$ 

It is well known, that an $F_2$-linear operator $T$ on $F$ can be written uniquely in the form

$$T = T((a)) = \sum_{i=0}^{n-1} T_i(a_i),$$

with $a = (a_0, \ldots, a_{n-1}) \in F^n$. A Singer group $Z$ can be identified with $T_0(F^*)$. Also $T_0(\zeta)$ is a Singer cycle for $\zeta$ primitive in $F$. Set $\Phi = T_1(1)$. Then $T_0(\zeta)\Phi = \Phi^{-1}T_0(\zeta)\Phi = T_0(\zeta)^2$ and $N_{\text{GL}(F)}(Z) = Z(\Phi)$.

The space $E = \text{End}(F)$ is a module for the representation $D^{(k, \ell)} : Z \to \text{GL}(E)$, where $TD^{(k, \ell)}(e) = T_0(e)^{-1}TT_0(e^\ell)$, $T \in E$, $e \in Z$, which is induced by $D^k$ and $D^\ell$. The next result is [2, Lemma 2.15]:

**Lemma 2.3.** We use the preceding notation and consider $E = \text{End}(F)$ as a module for the representation $D^{(k, \ell)}$.

(a) $E = T_0(F) \oplus T_1(F) \oplus \ldots \oplus T_{n-1}(F)$ is a decomposition into $Z$-modules.

(b) The module $T_i(F)$ affords the representation $D^{\ell - 2^i k}$, with the identification of $F$ and $T_i(F)$ via $a \mapsto T_i(a), T_i(a)D^{\ell - 2^i k}(e) = T_i(e^{\ell - 2^i k}a)$ for $a \in F, e \in F^*$.

We repeat key results from [2] with some details added.

**Lemma 2.4.** We use the preceding notation and consider $E$ as a $Z$-module of the representation $D^{(k, \ell)}$. Let $(k, r_n) = 1$. Assume that $T_0(F)$ induces $D^1$ and that $D^1$ occurs at least three times in $E$. The following hold:

(a) There exist a divisor $d$ of $n$, $d < n/2$, and $0 < c < 2^d - 1$, such that up to equivalence

$$k \equiv -1 + R_{c, d} \quad \text{and} \quad \ell \equiv R_{c, d} \quad \text{or} \quad k \equiv -1 \quad \text{and} \quad \ell \equiv 0 \pmod{r_n}.$$ 

(b) The module $T_i(F)$ affords the representation $D^i$ iff $d$ divides $i$.

(c) Let $\Psi$ be an element of $\sum_{i=0}^{n/d-1} T_{id}(F)$ and $x \in F^*$. Then $T_0(x^k)^{-1}\Psi T_0(x^\ell) = T_0(x)\Psi$.

**Proof.** (a) Assume, that $T_n(F)$ induces $D^1$ for $0 \leq i < 2$ and $a_0 = 0$. By Lemma 2.3 there exist integers $b$, such that $2^b \equiv \ell - 2^i k \pmod{r_n}$. Note, that $2^{b_0} \equiv \ell - k$ implies $1 \equiv \ell' - k' \pmod{r_n}$ with $k' \equiv 2^{n-b_0} k \sim k$ and $\ell' \equiv 2^{n-b_0} \ell \sim \ell \pmod{r_n}$, so that we may assume up to equivalence $a_0 = b_0 = 0$. According to [2, Lemma 2.3] (and it’s proof), there exist a divisor $d$ of $n$, $d < n/2
and \( 0 \leq c < 2^d - 1 \), such that \( k \equiv -1 + c \frac{2^n-1}{2^d-1} \pmod{r_n} \) and \( \ell \equiv c \frac{2^n-1}{2^d-1} \pmod{r_n} \). The assertion follows.

(b) We compute (note \( 2^d R_{c,d} \equiv R_{c,d} \pmod{r_n} \)):

\[
2^d k \equiv -2^d + 2^d R_{c,d} \equiv -2^d + R_{c,d} \equiv \ell - 2^d \pmod{r_n}
\]

Together with (a) our second assertion follows.

(c) We have \( \Psi = \sum_{i=0}^{n/d-1} T_{id}(a_i), a_i \in F \). Thus:

\[
T_0(x^k)^{-1} \Psi T_0(x^\ell) = \sum_{i=0}^{n/d-1} T_0(x^k)^{-1} T_{id}(a_i) T_0(x^\ell)
= \sum_{i=0}^{n/d-1} T_{id}(a_i x^{\ell-2^d k})
= \sum_{i=0}^{n/d-1} T_{id}(a_i x^{-2^d}) = T_0(x) \Psi
\]

The following Lemma allows us to simplify slightly the notation for Example 3.3 below.

**Lemma 2.5.** Let \( n = 2n_0 \), \( n_0 \) odd and \( k \equiv \frac{2^{2n_0+2n_0+1}-2}{3} \pmod{r_n} \). Then \( k \) is invertible modulo \( r_n \) and \( k^{-1} \equiv \frac{2^{2n_0+2n_0+1}+1}{3} \pmod{r_n} \).

**Proof.** Set \( A = (2^{2n_0} + 2^{2n_0+1} - 2)(2^{2n_0+1} + 1) \). We compute

\[
A = (2^{2n_0+1} - 1 + 6)(2^n - 1) + 3 \equiv 3 \pmod{3r_n},
\]

since \( 2^{2n_0+1} - 1 + 6 \) is divisible by 3. The assertion follows. □

**Lemma 2.6.** Let \( k, \ell, m \) be integers, \( (k, r_n) = 1 \), and let \( \ell \) and \( m \) belong to different cyclotomic cosets of 2 modulo \( n \). Let \( E_i = \text{End}(F), i = \ell, m \), be the \( \mathbb{Z} \)-module, that induces \( D^{(k,i)} \) and assume, that \( D^1 \) occurs in \( E_i \) at least two times. Then \( D^{(k,i)} \) contains \( D^1 \) for each \( i \) precisely two times. Moreover, one of the following holds:

(a) There exist a divisor \( d \) of \( n \), \( d < n/2 \), and \( 0 \leq c < 2^d - 1 \), \( 0 < u, v < n/d \), \( u \neq v \), such that up to equivalence \( \ell = \ell_u \), \( m = \ell_v \), where

\[
k \equiv 1 + R_{c,d}, \quad \ell_u \equiv 1 + 2^d + R_{c,d} \pmod{r_n}
\]

with \( w = u, v \).

(b) \( n = 2n_0 \), \( n_0 \) odd. Up to equivalence \( T_0(F) \) and \( T_{n_0}(F) \) are the submodules of \( E_m \), that induce \( D^1 \). Moreover, one of the following four cases (1)-(4) holds:
(1) $k \equiv 2^{2n+3n^2-2}, \ell \equiv k + 2^{n+1}$ and $m \equiv k + 1 \pmod{r_n}$. The submodules of $E_{k'}$ that induce $D^{1}$ are $T_{0}(F)$ and $T_{2}(F)$. Furthermore $\ell \equiv 2^2k + 1, m \equiv 2^{n}k + 2^{n+1} \pmod{r_n}$.

(2) $k \equiv 2^{n+1} + 1, \ell \equiv k + 2^2$ and $m \equiv k + 1 \pmod{r_n}$. The submodules of $E_{k'},$ that induce $D^{3}$ are $T_{0}(F)$ and $T_{n_0+1}(F)$. Furthermore $\ell \equiv 2^{n+1}k + 1, m \equiv 2^{n}k + 2^{n+1} \pmod{r_n}$.

(3) $k \equiv -\frac{2^{2n+3n^2-2}}{2}, \ell \equiv k + 1$ and $m \equiv k + 2^{n} \pmod{r_n}$. The submodules of $E_{k'},$ that induce $D^{1}$ are $T_{0}(F)$ and $T_{2}(F)$. Furthermore $\ell \equiv 2^2k + 2^{n+1}, m \equiv 2^{n}k + 1 \pmod{r_n}$.

(4) $k \equiv -2^{n+1} - 1, \ell \equiv k + 1$ and $m \equiv k + 2^{n} \pmod{r_n}$. The submodules of $E_{k'},$ that induce $D^{1}$ are $T_{0}(F)$ and $T_{n_0+1}(F)$. Furthermore $\ell \equiv 2^{n+1}k + 1, m \equiv 2^{n}k + 1 \pmod{r_n}$.

Proof. Let $T_{a_0}(F), T_{a_1}(F) \subseteq E_{\ell}$ and $T_{a_2}(F), T_{a_3}(F) \subseteq E_{m}$ be submodules, that induce the representation $D^{1}$ of $Z$. According to Lemma 2.3, there exist numbers $b_{0}, \ldots, b_{1}$, such that $2^{a_0} k \equiv \ell - 2^{b_0}, 2^{a_1} k \equiv \ell - 2^{b_1}, 2^{a_2} k \equiv m - 2^{b_2}$, and $2^{a_3} k \equiv m - 2^{b_3}$. The submodules $T_{a_0}(F), T_{a_1}(F), T_{a_2}(F), T_{a_3}(F)$ are submodules of $E_{k'}$, that induce the representation $D^{1}$ of $Z$. According to Lemma 2.3, there exist numbers $b_{0}, \ldots, b_{1}$, such that $2^{a_0} k \equiv \ell - 2^{b_0}, 2^{a_1} k \equiv \ell - 2^{b_1}, 2^{a_2} k \equiv m - 2^{b_2}$, and $2^{a_3} k \equiv m - 2^{b_3}$. The submodules $T_{a_0}(F), T_{a_1}(F), T_{a_2}(F), T_{a_3}(F)$ are submodules of $E_{k'}$, that induce the representation $D^{1}$ of $Z$. According to Lemma 2.3, there exist numbers $b_{0}, \ldots, b_{1}$, such that $2^{a_0} k \equiv \ell - 2^{b_0}, 2^{a_1} k \equiv \ell - 2^{b_1}, 2^{a_2} k \equiv m - 2^{b_2}$, and $2^{a_3} k \equiv m - 2^{b_3}$. The submodules $T_{a_0}(F), T_{a_1}(F), T_{a_2}(F), T_{a_3}(F)$ are submodules of $E_{k'}$, that induce the representation $D^{1}$ of $Z$. According to Lemma 2.3, there exist numbers $b_{0}, \ldots, b_{1}$, such that $2^{a_0} k \equiv \ell - 2^{b_0}, 2^{a_1} k \equiv \ell - 2^{b_1}, 2^{a_2} k \equiv m - 2^{b_2}$, and $2^{a_3} k \equiv m - 2^{b_3}$. The submodules $T_{a_0}(F), T_{a_1}(F), T_{a_2}(F), T_{a_3}(F)$ are submodules of $E_{k'}$, that induce the representation $D^{1}$ of $Z$. According to Lemma 2.3, there exist numbers $b_{0}, \ldots, b_{1}$, such that $2^{a_0} k \equiv \ell - 2^{b_0}, 2^{a_1} k \equiv \ell - 2^{b_1}, 2^{a_2} k \equiv m - 2^{b_2}$, and $2^{a_3} k \equiv m - 2^{b_3}$. The submodules $T_{a_0}(F), T_{a_1}(F), T_{a_2}(F), T_{a_3}(F)$ are submodules of $E_{k'}$, that induce the representation $D^{1}$ of $Z$. According to Lemma 2.3, there exist numbers $b_{0}, \ldots, b_{1}$, such that $2^{a_0} k \equiv \ell - 2^{b_0}, 2^{a_1} k \equiv \ell - 2^{b_1}, 2^{a_2} k \equiv m - 2^{b_2}$, and $2^{a_3} k \equiv m - 2^{b_3}$. The submodules $T_{a_0}(F), T_{a_1}(F), T_{a_2}(F), T_{a_3}(F)$ are submodules of $E_{k'}$, that induce the representation $D^{1}$ of $Z$. According to Lemma 2.3, there exist numbers $b_{0}, \ldots, b_{1}$, such that $2^{a_0} k \equiv \ell - 2^{b_0}, 2^{a_1} k \equiv \ell - 2^{b_1}, 2^{a_2} k \equiv m - 2^{b_2}$, and $2^{a_3} k \equiv m - 2^{b_3}$.
2.3 Representations of solvable, doubly transitive DHOs

Let $D$ be a solvable, doubly transitive DHO of rank $n$ over $\mathbb{F}_2$ with an ambient space $U = U(D)$. By $[13]$ we know $\text{Aut}(D) \leq A\Gamma L(1,F)$ and therefore $\text{Aut}(D)$ contains a subgroup $G = E \cdot S$, such that $(F,+) \simeq E \leq G$ acts regularly on $D$ and $S = G_X$ is the stabilizer of some $X \in D$ and $S$ acts transitively on $D - \{X\}$ as well as on $E - 1$ by conjugation. Using this notation we have by $[5, \text{Lemma 3.2}]$ (proof):

Lemma 2.8. Set $Y = [U,E]$ and let $X \in D$. Then $Y = [X,E]$ and $D$ splits over $Y$. In particular $U = X \oplus Y$.

By our assumptions there is a monomorphism $\tau : F \to E$, i.e. $E = \{\tau_e \mid e \in F\}$. We are interested in the case, that $S = Z = (F^*,\cdot)$ is cyclic of order $r_n$. As $Z$ acts transitively on $E^*$ by conjugation, it induces a Singer group of $\text{GL}(E)$. On the other hand $T_0(\zeta), \zeta \in F^*$ primitive, is a Singer cycle in $\text{GL}(F)$. So by Lemma 2.1 we can choose the identifying isomorphism $\tau$ between $F$ and $E$, and a monomorphism $z : F^* \to Z$, such that

$$z_e^{-1} \tau_x z_e = \tau_{xe}$$

for $x,e \in F$, $e \neq 0$. These conventions for the homomorphisms $\tau$ and $z$ will be used throughout Section 3. The decomposition $U = X \oplus Y$ is a decomposition into $Z$-modules. Using the convention from Subsection 2.1 we write

$$z_e = \begin{pmatrix} (z_e)x & 0 \\ 0 & (z_e)y \end{pmatrix}$$

for $e \in F^*$ and $\tau_e \in E$ has the form

$$\tau_e = \begin{pmatrix} 1 & A(e) \\ 0 & B(e) \end{pmatrix},$$

$A(e) \in \text{Hom}(X,Y), B(e) \in \text{GL}(Y)$. Set $X(0) = X$ and $X(e) = X(0)\tau_e$. Then

$$X(e) = \{(x,xA(e)) \mid e \in F\} \text{ and } D = \{X(e) \mid e \in F\}.$$

Moreover, $B : F \to \text{GL}(Y)$ is the representation obtained by the restriction of the representation of $E$ on $Y$. The DHO is bilinear, if $E$ has a quadratic action on $U$. But this is equivalent to the fact, that $B$ is the trivial representation of $F$, i.e. $B(e) = 1_Y$ all $e \in F$. Finally we observe:

Lemma 2.9. The representation of $Z$ on $X$ is irreducible and faithful, i.e. it is equivalent to a representation $D^k$ with $(k,r_n) = 1$.

Proof. The decomposition $D = \{X(0)\} \cup \{X(e) \mid 0 \neq e \in F\}$ is the disjoint union of $Z$-orbits. Hence $X(0) - \{0\} = \{(X(0) \cap X(e)) - \{0\} \mid 0 \neq e \in F\}$ is a $Z$-orbit too and thus $Z$ acts faithfully on $X$. \qed

8
2.4 Congruences

For \( u \in I_n \) let

\[ u = 2^{x_1} + \cdots + 2^{x_i} \]

be it’s unique 2-adic expansion, i.e. \( 0 \leq x_1 < x_2 < \cdots < x_i < n \), and \( t < n \). We call \( wt(u) = t \) the weight of \( u \). An expression \( 2^b + 2^{b+1} + \cdots + 2^{b+c-2} + 2^{b+c-1} \), \( c < n \), (modulo \( r_n \)) has weight \( c \) and we call it a string of length \( c \). A string of length \( c \) in \( u \) is a string \( 2^{x_1} + 2^{x_1+1} + \cdots + 2^{x_1+c-2} + 2^{x_1+c-1} \), where \( x_a - x_{a-1} > 1 \), \( x_{a+i} = x_{a+i} + 1 \), for \( 1 \leq i < c \), and \( x_{a+c} = x_{a+c-1} + 1 \). For an expression \( x = 2^{a_1} + \cdots + 2^{a_k} \), \( a_1 < \cdots < a_k, k < n \), we define the sequence of gaps \((a_{i+1} - a_i \mod n) \mid 1 \leq i \leq k \), (with the identification \( k+1 = 1 \)).

Two sequences of gaps are identified, if they are obtained from each other by a cyclic permutation. We shall consider congruences of the form

\[ u \equiv 2^{v_1} + \cdots + 2^{v_s} \pmod{r_n} \]

with \( 0 \leq v_i < n \) and \( s < n \). If the \( v_i \)'s are pairwise different, we deduce \( s = t \) and \( x_i = v_i \), with some permutation \( i \leftrightarrow i' \).

Now assume, that not all \( v_i \)'s are different. If for instance \( v_1 = v_2 \) and \( v'_1 \equiv v_1 + 1 \pmod{n} \), \( 0 \leq v'_1 < n \), then \( u \equiv 2^{v_1} + 2^{v_1} + \cdots + 2^{v_1} \pmod{r_n} \). So iterating if necessary, we finally reach the congruence \( u \equiv 2^{x_1} + \cdots + 2^{x_1} \pmod{r_n} \), which we will call the reduced congruence for \( u \), in particular \( t \leq s \). For the remainder of this section we will deal with congruences of the form \( \ast \equiv \ast \pmod{n} \) and of the form \( \ast \equiv \ast \pmod{n} \). We often omit the "mod" symbol, if it is clear from the context, whether we have a congruence modulo \( r_n \) or modulo \( n \). For \( 0 \leq a \leq b \), \( b - a < n - 1 \) we use the abbreviation \( \sum_{a}^{b} \) for the \((b-a+1)\)-string \( 2^a + 2^{a+1} + \cdots + 2^b \) read modulo \( r_n \). In particular \( \sum_{b}^{b} = 2^a + \cdots + 2^{b-1} + 1 + \cdots + 2^{n-b} \) if \( b \geq n \).

**Lemma 2.10.** Let \( S \equiv \sum_{a}^{b} + \sum_{c}^{d} \pmod{r_n} \), \( b + d - a - c + 2 < n \).

(a) Let \( a \leq c \leq b \leq d \). Then:

<table>
<thead>
<tr>
<th>( S ) reduced</th>
<th>weight</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \sum_{a}^{b} + \sum_{c}^{d} + 2^{d+1} )</td>
<td>( b - a + 1 )</td>
<td>( a &lt; c &lt; b &lt; d )</td>
</tr>
<tr>
<td>( \sum_{a}^{b} + 2^{d+1} )</td>
<td>( b - a + 1 )</td>
<td>( a &lt; c = b &lt; d )</td>
</tr>
<tr>
<td>( 2^{d+1} )</td>
<td>1</td>
<td>( a = c = b &lt; d )</td>
</tr>
</tbody>
</table>

(b) Let \( c \leq a < b \leq d \). Then:

<table>
<thead>
<tr>
<th>( S ) reduced</th>
<th>weight</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \sum_{a}^{b} + 2^{d+1} )</td>
<td>( b - c + 1 )</td>
<td>( a = c &lt; b \leq d )</td>
</tr>
<tr>
<td>( \sum_{c}^{b} + \sum_{a}^{b} + 2^{d+1} )</td>
<td>( b - c + 1 )</td>
<td>( c &lt; a &lt; b &lt; d )</td>
</tr>
<tr>
<td>( \sum_{c}^{b} + 2^{d+1} )</td>
<td>( b - c + 1 )</td>
<td>( c &lt; a &lt; b \leq d )</td>
</tr>
</tbody>
</table>
Proof. Assume $a < c < b < d$. Then

$$S \equiv \sum_{a}^{c-1} + 2 \sum_{c}^{b} + \sum_{b+1}^{d}$$

$$\equiv \sum_{a}^{c-1} + \sum_{c+1}^{b} + (2b+1 + \sum_{b+1}^{d})$$

$$\equiv \sum_{a}^{c-1} + \sum_{c+1}^{d} + 2d+1.$$

The other cases are similar. \[\square\]

Lemma 2.11. Let $n = 2n_0$, $n_0$ odd > 3. Let $k \equiv -2n_0+1 - 1$, $\ell \equiv k + 1$, and

$$2^a + \ell \equiv 2^c + 2^k (\text{mod } r_n),$$

with $0 \leq a, b, c < n$, $b > 0$. Then $a = n_0 + 1$ and $c \equiv b + n_0 + 1$ (mod $n$), for $b$ arbitrary.

Proof. As $\ell \equiv -2n_0+1$ we get the congruence $2^a + 2^{n_0+b+1} \equiv 2^c + 2^{n_0+1}$ (mod $r_n$). Since $b > 0$ we get $a = n_0 + 1$ and $c = n_0 + b + 1$. \[\square\]

Lemma 2.12. Let $n = 2n_0$, $n_0$ odd > 3. Let $k \equiv 2n_0+1 + 1$, $\ell \equiv k + 4$, and $2^a + \ell \equiv 2^c + 2^k (\text{mod } r_n)$, with $0 \leq a, b, c < n$, $b > 0$. Then $(a, b, c) \in \{(n_0 - 1, n_0 - 1, 2), (n_0 + 3, n_0 + 1, 0)\}$.

Proof. Now $\ell = 2n_0+1 + 4 + 1$, so that we obtain the congruence:

$$2^a + 2^{n_0+1} + 4 + 1 \equiv 2^c + 2^{n_0+b+1} + 2^{b+2} + 2^b \quad (\text{mod } r_n) \quad (2)$$

Assume first, that Equation (2) is reduced. Then $b \in \{a, n_0 + 1, 2\}$.

If $b = a$ Equation (2) becomes $2^{n_0+1} + 2^2 + 1 \equiv 2^c + 2^{n_0+b+1} + 2^{b+2}$ and $n_0 + b + 1 \equiv 0$ or 2. If $n_0 + b + 1 = 0$, we have $2^{n_0+1} + 2^2 \equiv 2^c + 2^{n_0+1}$ and $(a, b, c) = (n_0 - 1, n_0 - 1, 2)$ follows, whereas $n_0 + b + 1 = 2$ leads to a contradiction.

In a similar fashion the case $b = n_0 + 1$ leads to the solution $(a, b, c) = (n_0 + 3, n_0 + 1, 0)$, while the case $b = 2$ yields a contradiction.

Assume next, that Equation (2) is not reduced. Then $c \in \{n_0 + b + 1, b + 2, b\}$ and $a \in \{0, 2, n_0 + 1\}$. We have

<table>
<thead>
<tr>
<th>$a$</th>
<th>$b$</th>
<th>$c$</th>
<th>RHS</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>$2^{n_0+1} + 2^2 + 2$</td>
<td>$n_0 + b + 1$</td>
<td>$2^{n_0+b+1} + 2^{n_0+1} + 2^b$</td>
</tr>
<tr>
<td>2</td>
<td>$2^{n_0+1} + 2^4 + 1$</td>
<td>$b + 2$</td>
<td>$2^{n_0+b+1} + 2^{n_0+1} + 2^b$</td>
</tr>
<tr>
<td>$n_0 + 1$</td>
<td>$2^{n_0+2} + 2^2 + 1$</td>
<td>$b$</td>
<td>$2^{n_0+b+1} + 2^{n_0+1} + 2^b$</td>
</tr>
</tbody>
</table>

If an expression for the LHS is equal to an an expression for the RHS the sequences of gaps have to agree. But in each such case we obtain $b = 0$, a contradiction. \[\square\]

Lemma 2.13. Let $n = 2n_0$, $n_0$ odd > 3. Let $k \equiv \frac{2^{n+2n_0+1}-2}{3}$, $\ell \equiv k + 2n_0+1$, and $2^a + \ell \equiv 2^c + 2^k (\text{mod } r_n)$, with $0 \leq a, b, c < n$. Then:
(a) If $n_0 > 5$, then $(a, b, c) \in \{(n_0 + 3, 2, 0), (n - 2, n - 2, n_0 + 1)\}$.

(b) If $n_0 = 5$, then $(a, b, c) = (8, 2j, 2j - 2)$, $0 \leq j < 5$. Moreover $2^n + \ell \equiv 2^4k + 2^e + 2^f \pmod{r_n}$, iff $(d, e, f) = (2j, 2j - 2, 2j - 4)$ (modulo 10), $0 \leq j < 5$ (up to symmetry in $e$ and $f$).

Proof. We only prove (a), since (b) follows from a simple computer calculation. As $\ell \equiv \frac{2^3 + 2^{n+1} - 2}{3}$ we get $2^n + \frac{2^3 + 2^{n+1} - 2}{3} \equiv 2^e + 2^b \cdot \frac{2^n + 2^{n+1} - 2}{3} \pmod{r_n}$. Multiplying with 3 we obtain the congruence:

$$\sum_{a}^{a+1} + \sum_{b}^{n_0 + 2} + \sum_{c}^{n_0 + b + 2} \equiv \sum_{a}^{c+1} + \sum_{b}^{n_0 + b + 2} \pmod{r_n}$$

(3)

Assume first, that Equation (3) is reduced (i.e. both sides have weight $n_0 + 5$). Suppose, that on both sides two strings occur, one of length 2 the other of length $n_0 + 3$. Then the strings of the same length on both sides agree, i.e. $b = 0$, a contradiction. So both sides are one string of length $n_0 + 5$. One obtains immediately $(a, b, c) \in \{(n_0 + 3, 2, 0), (n - 2, n - 2, n_0 + 1)\}$.

Assume now, that Equation (3) is not reduced, i.e. both sides have weight $< n_0 + 5$.

If both sides have weight 2, we deduce from Lemma 2.10, that $a = 0$ or $n - 1$ and $b = c$ or $b = c + 1$. The resulting four possibilities each lead to a contradiction.

If both sides have weight 3, then $a = 1$ and the LHS is $1 + 2^2 + 2^{n+1}$. Also $c = b + 1$ and the RHS is $2b + 2b + 2^{n+1} + b + 3$, which is impossible, as $b > 0$.

If both sides have a weight $> 3$, then by Lemma 2.10 on both sides there is precisely one string of length $> 1$. These two strings must agree. One string starts with $b$, the other one with 0, i.e. $b = 0$, a contradiction. □

Lemma 2.14. Let $n = 2n_0$, $n_0$ odd $> 3$. Let $k \equiv \frac{2^n + 2^{n+1} - 2}{3}$, $\ell \equiv k + 1$, and $2^n + \ell \equiv 2^e + 2^b \ell \pmod{r_n}$, with $0 \leq a, b, c < n, b > 0$. Then $(a, b, c) \in \{(2, 2, n_0 + 1), (n_0 + 1 - n - 2, 0), (n_0 + 1, n_0 + 1)\}$.

Proof. As $\ell \equiv \frac{2^n + 2^{n+1} - 5}{3}$ we get $2^n + \frac{2^n - 2^{n+1} + 5}{3} \equiv 2^e + 2b \cdot \frac{2^n - 2^{n+1} + 5}{3} \pmod{r_n}$. Multiplying with 3 we obtain the congruence:

$$\sum_{a}^{a+1} + \sum_{b}^{n_0 + b} + \sum_{c}^{n_0 + b + 2} \equiv \sum_{a}^{c+1} + \sum_{b}^{n_0 + b} + \sum_{c}^{n_0 + b + 2} \pmod{r_n}$$

(4)

Assume first, that Equation (4) is reduced (i.e. both sides have weight $n_0 + 1$). Suppose, that on both sides two strings occur, one of length 2 the other of length $n_0 - 1$. Then the strings of the same length on both sides agree, i.e. $b = 0$, a contradiction. So both sides are one string of length $n_0 + 1$. One obtains immediately $(a, b, c) \in \{(2, 2, n_0 + 1), (n_0 - 1, n - 2, 0)\}$.

Assume now, that Equation (4) is not reduced, i.e. both sides have weight $< n_0 + 1$ and are not reduced.
If both sides have weight 2, we deduce from Lemma 2.10, that $a = b + 1$ or $b + 2$ and $c = 1$ or $c = 2$. The case $a = b + 1$, $c = 1$ results in the solution $(a, b, c) = (n_0 + 1, n_0, 1)$. The remaining three possibilities each lead to a contradiction. The cases, where both sides have a weight $> 2$ are ruled out similarly, as in the proof of previous Lemma.

**Lemma 2.15.** Let $n = 2n_0$, $n_0$ odd and $(k, m) \in \{(2^{n_0+1}+1, k+1), (-2^{n_0+1}-1, k + 2n_0)\} \pmod{r_n}$. Assume $m + 2^a \equiv 2^b m + 2^c \pmod{r_n}$, $0 \leq a, b, c < n$, $b > 0$. Then $a = c$ and $b = n_0$.

**Proof.** First we observe, that in any case $m$ is divisible by $2^n + 1$: For instance $(2^{n_0+1}+1)^{-1} + 1 = (2^{n_0+1}+1)^{-1} = \frac{(2^{n_0}+1)^2}{2^{n_0}+1}$ and $(-2^{n_0+1}+1)^{-1} + 2^{n_0} = -2^{n_0}+2^{n_0} = -2^{n_0-1}(2^{n_0}+1)$. Then the LHS in the congruence $(2^b-1)m \equiv 2^a - 2^c \pmod{r_n}$ is divisible by $2^{n_0}+1$. Therefore $2^a - 2^c$ is divisible by $2^{n_0}+1$.

As $n_0$ is odd, this implies $a = c$ and $2^b m \equiv m$. Clearly, $b = n_0$ fulfills this requirement and in any case $m/(2^{n_0}+1)$ lies in a long cyclotomic coset of 2 modulo $n$, i.e. $2^b m \not\equiv m$ for a divisor $0 < b < n_0$ of $n$. Hence $b = n_0$.

**Lemma 2.16.** Let $n_0 > 3$ be odd, $n = 2n_0$ and $k \equiv \frac{2^n+2^{n_0+1}-2}{2^n+2^{n_0}} \pmod{r_n}$ and $m \equiv k + 2n_0 \pmod{r_n}$. Assume $s = 1 + 2\ell \equiv 2^b + 2^c m \pmod{r_n}$. Then one of the following hold:

(a) $(a, b, c) \in \{(0, n_0 + 1, 0), (0, n_0 + 1, n_0)\}$.

(b) $(a, b, c) \in \{(n - 2, n - 2, 0), (n - 2, n - 2, n_0)\}$.

**Proof.** Multiply the congruence $1 + 2\ell \equiv 2^b + 2^c m \pmod{r_n}$ by 3 and we obtain

$$1 + 2 + 2^a(2^{n_0+3} - 1) \equiv 2^b + 2^b + 2^c(2^{n_0+3} + 2) \pmod{r_n}.$$ 

The RHS has weight 2 if $b = c + 1$ or $c = n_0 + 1$, weight 3 if $b = c$ or $b = c + n_0$, and weight 4 otherwise. So the LHS has weight 2, 3 or 4. By Lemma 2.10 the LHS has weight 2 if $a = 0, 1$, has weight 3, iff $a = n - 1$ and weight 4, iff $a = n - 2$.

**Case weight is 2.** Now $b = c + 1$ or $c + 1 + n_0$. Eliminating $c$ on the RHS it becomes in both cases $2^b + 2^c + 2^{n_0+5}$, which has the gap sequence $(n_0 - 2, n_0 + 2)$. For $a = 0$ the LHS becomes $2^{n_0+3} + 2$, which has the same gap sequence and we get the two solutions $(a, b, c) = (0, n_0 + 1, 0), (0, n_0 + 1, n_0)$. For $a = 1$ the LHS becomes $2^{n_0+4} + 1$, which has the gap sequence $(n_0 + 4, n_0 - 4)$. So $a = 1$ yields no solution.

**Case weight is 3.** Here $a = n - 1$ and the LHS is $2 + 2^{n_0+2} + 2^{n_0-1}$. As $b = c$ or $c = n_0$. RHS is in both cases $2^b + 2^b + 2^{n_0+b+1} \pmod{r_n}$. That implies $b = n - 1$ and then $2^{n_b} = 2^{n_0+b+1} \equiv 2^{n_0} + 2^{n_0} + 2^{n_0} \equiv 2^b + 2^b + 2^b \equiv 2^c + n_0 + 1 \pmod{r_n}$ holds. $2^{n_0} + 2^{n_0} + 2^{n_0} - 1$ is the only 2-string on the LHS and then $2^b + 2^b$ is the only 2-string on the RHS. That leads to the two solutions $(a, b, c) = (n - 2, n - 2, 0), (n - 2, n - 2, n_0)$. **
The next three results have similar verifications as Lemma 2.16.

**Lemma 2.17.** Let \( n_0 > 3 \) be odd, \( n = 2n_0 \) and \( k \equiv 2^{n_0+1} + 1 \pmod{r_n} \), \( \ell \equiv k + 4 \pmod{r_n} \), and \( m \equiv k + 1 \pmod{r_n} \). Assume \( s = 1 + 2^n \ell \equiv 2^b + 2^m \pmod{r_n} \). Then one of the following hold:

(a) \((a,b,c) \in \{(0,2,0),(0,2,n_0)\}\).

(b) \((a,b,c) \in \{(n_0 - 1,n_0 - 1,0),(n_0 - 1,n_0 - 1,n_0)\}\).

**Lemma 2.18.** Let \( n_0 > 3 \) be odd, \( n = 2n_0 \) and \( k \equiv -2^{n_0+1} - 1 \pmod{r_n} \), \( \ell \equiv k + 1 \pmod{r_n} \), and \( m \equiv k + 2^{n_0} \pmod{r_n} \). Assume \( s = 1 + 2^n \ell \equiv 2^b + 2^m \pmod{r_n} \), \( d \leq e \). Then one of the following hold:

(a) \((a,b,c) \in \{n_0 - 2,n - 1,0),(n_0 - 2,n - 1,n_0)\}\).

(b) \((a,b,c) \in \{(n_0,n_0,0),(n_0,n_0,n_0)\}\).

**Lemma 2.19.** Let \( n_0 > 3 \) be odd, \( n = 2n_0 \) and \( k \equiv -2^{n_0+1} - 1 \pmod{r_n} \), \( \ell \equiv k + 1 \pmod{r_n} \), and \( m \equiv k + 2^{n_0} \pmod{r_n} \). Assume \( s = 1 + 2^n \ell \equiv 2^b + 2^m \pmod{r_n} \), \( d \leq e \). Then one of the following hold:

(a) \((a,b,c) \in \{(n - 1,1,0),(n - 1,n_0)\}\).

(b) \((a,b,c) \in \{(n_0,n_0,0),(n_0,n_0,n_0)\}\).

We only sketch the proof of Lemma 2.19, which is the simplest one. The other verifications are left to the reader.

**Proof.** (Lemma 2.19) We have \( \ell \equiv -2^{n_0+1}, m \equiv -2^{n_0} - 1 \pmod{r_n} \). The equation \( 1 + 2^n \ell \equiv 2^b + 2^m \pmod{r_n} \) implies

\[
1 + 2^c + 2^{c+n_0} \equiv 2^b + 2^{x+n_0+1} \pmod{r_n}.
\]

Clearly, if \((a,b,c)\) is a solution, then \((a,b,c+n_0)\) is a solution too. Moreover our equation has weight \( \leq 2 \), i.e. \( c \in \{0,n_0\} \). So wlog. \( c = 0 \) and \( 2 + 2^{n_0} \equiv 2^b + 2^{x+n_0+1} \). This forces \((a,b) = (n-1,1)\) or \((n_0,n_0)\). \( \square \)

**Lemma 2.20.** Let \( s \equiv 2^x - 2^b - 1 \equiv 2^z - 2^{b+y} - 2^y \pmod{r_n} \) with \( 0 < b, y < n \), \( 1 < d = (n,b) \) and \( n/d \) odd. Then one of the following hold:

(a) \( s \equiv -1 \pmod{r_n} \) and \( x \equiv -y \equiv -z \equiv b \pmod{r_n} \).

(b) \( s \equiv -2^b \pmod{r_n} \) and \( x \equiv 0, y \equiv b, z \equiv 2b \pmod{r_n} \).

(c) \( d = 2, n = 2n_0, n_0 \text{ odd and } b = n_0 + 1 \). Moreover \( s \equiv -2^{n_0} - 1 \pmod{r_n} \) and \( x \equiv y \equiv n_0, z \equiv 0 \pmod{r_n} \).

(d) \( d = 2, n = 2n_0, n_0 \text{ odd and } b = n_0 - 1 \). Moreover \( s \equiv -2^{n_0-1} - 2^{n-1} \pmod{r_n} \) and \( x \equiv n - 1, y \equiv n_0, z \equiv n_0 - 1 \pmod{r_n} \).
Suppose first, that Equation (5) is reduced. This forces (since $b, y > 0$) $b = x$ or $y = 0$ and $b + y = 0$ or $z$. The case $b = x, b + y = 0$ immediately implies assertion (a), whereas $b = y, b + y = z$ yields assertion (b). If $b = y, b + y = 0$, we have $2b \equiv 0 \pmod{n}$, which contradicts the assumption, that $n/(n, b)$ is odd. If $b = x$ and $b + y = z$ we get $y = 0$, contradicting again our assumption.

So assume now, that Equation (5) is not reduced. This forces (since $b, y > 0$) $x = y$ or $b + y$ and $z = 0$ or $b$.

If $x = y$ and $z = b$ Equation (5) becomes $2^{b+y} + 2y + 2^x \equiv 2^b + 2^z + 1 \pmod{r_n}$ (mod $r_n$).

That implies $y \equiv -1$ or $b$ (mod $n$). In the first case $b - 1 \equiv b + 1$, which is absurd. In the second case $b + y \equiv 0$ or $2b \equiv 0$ (mod $n$), which is impossible as we have seen before.

The case $x = b + y$ and $z = 0$ leads in a similar fashion to a contradiction.

Assume $x = y$ and $z = 0$. Equation (5) becomes $2^{b+y} + 2y + 1 \equiv 2^b + 2^y + 1 \pmod{r_n}$. As $y > 0$, we have $b \equiv y + 1$ and $1 \equiv b + y$ (mod $n$). This shows $2b \equiv 2$ and $2y \equiv 0$ (mod $n$). Then $y = n/2 = n_0$, and $b \equiv n_0 + 1$ (mod $n$). As $d = (n, b) = 2$, assertion (c) follows.

The case $x = b + y$ and $z = b$ leads in a similar fashion to assertion (d).

### 2.5 Computing covers of small DHOs

Let $\mathcal{D}$ be a DHO over $\mathbb{F}_2$ of rank $n$ with ambient space $U = \mathbb{F}_2^n \oplus \mathbb{F}_2^n$. Let $\mathcal{D}$ split over $Y = 0 \oplus \mathbb{F}_2^n$ and let $X = \mathbb{F}_2^n \oplus 0 \in \mathcal{D}$. Then there exist matrices $\beta(e) \in \mathbb{F}_2^{n \times m}, e \in \mathbb{F}_2^n, \beta(0) = 0$, such that $\mathcal{D} = \{X(e) \mid e \in \mathbb{F}_2^n\}$ with $X(e) = \{(x, x\beta(e)) \mid x \in \mathbb{F}_2^n\}$. In particular $X(0) = X$. One calls $\mathcal{D} = \{\beta(e) \mid e \in \mathbb{F}_2^n\}$ a DHO set for $\mathcal{D}$.

Let $\tilde{\mathcal{D}}$ be a DHO with ambient space $\tilde{U} = \mathbb{F}_2^n \oplus \mathbb{F}_2^n \oplus \mathbb{F}_2^n$, such that $\tilde{\mathcal{D}} = \tilde{U}/\tilde{W}, \tilde{W} = 0 \oplus 0 \oplus \mathbb{F}_2^n$. Then $\tilde{\mathcal{D}}$ has a DHO set $\tilde{\mathcal{D}} = \{\beta(e) \mid e \in \mathbb{F}_2^n\}$ with $\beta(e) = (\beta(e), \gamma(e)), \gamma(e) \in \mathbb{F}_2^n$ (considered as a column space). Even $\beta(0) = 0$ holds, if we choose a basis of the ambient space of $\tilde{\mathcal{D}}$ properly.

A doubly transitive DHO $\mathcal{D}$ has a doubly transitive universal cover $\tilde{\mathcal{D}}$, that splits over $[U(\tilde{\mathcal{D}}), O_2(\text{Aut}(\tilde{\mathcal{D}}))]$ by Lemma 2.8. Then $\mathcal{D} = \tilde{\mathcal{D}}/\tilde{W}, \tilde{W} \subseteq [U(\tilde{\mathcal{D}}), O_2(\text{Aut}(\tilde{\mathcal{D}}))]$. Assume, that $\tilde{\mathcal{D}}$ is a proper cover. Let $\tilde{W}$ be a subspace of $W$ of codimension 1. Then $\tilde{\mathcal{D}} = \tilde{\mathcal{D}}/\tilde{W}$ is a cover of $\mathcal{D}$ as described above. Suppose, there exists an algorithm, which computes a cover $\tilde{\mathcal{D}}$ of $\mathcal{D}$ with $\dim U(\tilde{\mathcal{D}})/U(\mathcal{D}) = 1$. Such an algorithm can be iterated until we get $\tilde{\mathcal{D}}$. We describe a simple procedure of this kind:

For $e \in \mathbb{F}_2^n - 0$ let $\mathcal{V}(e)$ be the set of vectors $v \in \mathbb{F}_2^n$, such that $\ker(\beta(e), v) = \ker(\beta(e))$ and let $\mathcal{V}$ be the disjoint union of the $\mathcal{V}(e)$’s. We define a $[\mathbb{F}_2^n - 0]_\mathcal{D}$-partite graph on $\mathcal{V}$, by joining $v \in \mathcal{V}(e)$ with $v' \in \mathcal{V}(e')$, $e \neq e'$, iff $\dim \ker((\beta(e), v) - (\beta(e'), v')) = 1$. A clique $\mathcal{C} = \gamma(e) \in \mathcal{V}(e) \mid e \in \mathbb{F}_2^n - 0$ defines a DHO set
\[ \mathcal{D} = \{ \hat{\beta}(e) = (\beta(e), \gamma(e)) \mid e \in \mathbb{F}_2^n \}, \hat{\beta}(0) = 0, \] of a proper cover \( \mathcal{D} \), iff

\[ \dim \left( \sum_{e \in \mathbb{F}_2^n} \text{Im} \hat{\beta}(e) \right) = \dim \left( \sum_{e \in \mathbb{F}_2^n} \text{Im} \beta(e) \right) + 1. \]

This sets up a straightforward GAP-procedure (see [6]) for the computation of the universal cover of a doubly transitive DHO. This procedure is feasible for ranks \( \leq 6 \). Our computations lead to:

**Lemma 2.21.** *Theorem 1.2 holds for rank \( n = 6 \).*

## 3 Examples and the proof of Theorem 1.1

We start with the description of bilinear DHOs, that occur in the proof of Theorem 1.2. We shall use the conventions of Subsection 2.3, i.e. in each of the examples there exist monomorphisms \( \tau : E \rightarrow E, z : F^* \rightarrow Z, \) such that \( EZ \simeq \text{AGL}(1,F) \) is a doubly transitive group of automorphisms for the constructed DHO and that \( z^{-1}_e \tau_f z_e = \tau_{ef}, e, f \in F, e \neq 0 \) holds.

**Example 3.1.** (The DHOs \( S^m_{n,h} \) of Yoshiara [11], [12]) Let \( 0 < h, m < n, \) such that \( (n,h) = (n,m) = 1. \) Let \( (2^m - 1)^{-1} \) be the inverse of \( 2^m - 1 \) modulo \( r_n. \) Set \( a \equiv (2^h - 1)(2^m - 1)^{-1}, \) \( \ell \equiv k + 2h \equiv (2^{h+m} - 1)(2^m - 1)^{-1} \) (mod \( r_n) \) and \( U = F \oplus F. \) For \( e \in F \) define \( \tau_e = \begin{pmatrix} 1 & A(e) \\ 0 & 1 \end{pmatrix} \) \( \in \text{GL}(U), \) with \( A(e) = T_0(e^2) + T_m(e). \) For \( e \in F^* \) set \( z_e = \text{diag}(T_0(e^2), T_0(e^2)). \) Then \( E = \{ \tau_e \mid e \in F \} \) is elementary abelian of order \( 2^n \) and \( Z = \{ z_e \mid e \in F^* \} \) is cyclic of order \( r_n. \) Set \( X(0) = F \oplus 0, X(e) = X(0)\tau_e \) for \( e \in F \) and \( D = \{ X(e) \mid e \in F \}. \)

Then \( S^m_{n,h} = D \) is a bilinear DHO, that admits \( EZ \simeq \text{AGL}(1,F) \) as a group of automorphisms.

**Remark 3.2.**

(a) \( U(S^m_{n,h}) = F \oplus F \) if \( h + m \neq 0 \) (mod \( n) \) and \( U(S^m_{n-h,h}) = F \oplus F_0, F_0 = \{ x \in F \mid \text{Tr}_{F,F_2}(x) = 0 \} \) by [12].

(b) \( S^m_{n-h,h} \simeq S^n_{n-h',h'} \) for all \( h, h' \) coprime to \( n \) by [2].

(c) Assume \( h + m \neq 0 \) (mod \( n) \). Then \( S^m_{n,h} \simeq S^n_{m',h'}, \) iff \( (h', m') \in \{(h, m), (n-h, n-m)\} \) by [12].

(d) \( S^m_{h,h} \) is a quotient of the Huybrechts DHO of rank \( n \) [12].

(e) For later purposes we note \( \ell \equiv -2^a \) (mod \( r_n), \) iff \( a \equiv -m, h \equiv -2^a \) (mod \( n) \): namely if \( \ell \equiv (2^{h+m} - 1)(2^m - 1)^{-1} \equiv -2^a \) (mod \( r_n), \) then \( 2^{h+m} + 2^{a+m} \equiv 2^a + 1, \) forcing \( a + m \equiv 0 \) and \( h + m \equiv a \) (mod \( n) \).

**Example 3.3.** (The DHOs \( D[n,k] \) of [2], Ex. 3.3) For \( n = 2n_0, n_0 \) odd, we set \( U = F \oplus F \oplus F. \) For parameters \( k, \ell, m \) specified below we define a subgroup
Example 3.5. (DHOs of type EZ is a proper divisor of n by (1)

Remark 3.4. (a) \(U(D[n,k]) = F \oplus F \oplus F, F_0 = F^{2n_0}, \) except for the case \((n_0,k) = (3, (2n_0 + 1)^{±1})\), when \(\dim U(D[6,k]) = 13.\)

(b) In Example 3.3 of [2] we assumed, that the representation of \(F^*\) induced on \(E\) is \(D^k\) rather than \(D^1\) (which we do now in view of the conventions of Subsections 2.3). That lead to a slightly different description of the DHOs \(D[n,k]\) in [2]. Moreover, a DHO \(D[k^{±1}]\) of [2] is now the DHO \(D[n,k^{±1}].\)

We now describe a class of non-bilinear, doubly transitive DHOs.

**Example 3.5.** (DHOs of type \(D[n,d,b]\)) Let \(0 < b < n,\) such that \(1 < d = (n,b)\) is a proper divisor of \(n\) and \(n/d\) is odd. For \(e \in F^*\) define \(z_e \in GL(U),\) \(U = F \oplus F \oplus F\) by

\[z_e = \text{diag}(T_0(e^k), T_0(e^i), T_0(e^n)) \in GL(U).\]

Then \(Z = \{z_e \mid e \in F^*\}\) is a cyclic group of order \(r_n.\) Set further \(A = T_0(1) + T_{n-b}(1)\) and \(D = \sum_{j=0}^{n/d-1} (T_j d(1) + T_{j d(1)})\) and

\[
\tau_1 = \begin{pmatrix} 1 & A & D \\ 1 & D & 1 \\ 1 & 1 & 1 \end{pmatrix}
\]

\[2\text{In Example 3.3 of [2] occurs a sign error. There one has to replace } k = (-2^{2n_0+1} - 1)^{±1}\] by \((-2^{2n_0+1} - 1)^{±1}.\)
and for $e \in F^*$ set $\tau_e = z_e^{-1} \tau_1 z_e$. Then

$$
\tau_e = \begin{pmatrix}
1 & A(e) & C(e) \\
1 & B(e) & 1 \\
1 & 1 & 1
\end{pmatrix}
$$

with $A(e) = T_0(e^{2d}) + T_{n-b}(e^{2^{n-b}})$, $B(e) = \sum_{j=0}^{n/d-1} (T_{jd}(e^{2^{jd}})) + T_{jd+1}(e^{2^{jd+1}}))$ and $C(e) = \sum_{j=0}^{n/d-1} (T_{jd}(e^{2^{jd}+2^{jd+1}})) + T_{jd+1}(e^{2^{jd+1}+2^{jd+1}}))$. Finally, set $\tau_0 = 1 \in \text{GL}(U)$.

The subsequent claims (1), (2) and (7) show the existence of solvable, doubly transitive DHOs, that are not bilinear.

(1) $\tau_e \tau_{e^1} = \tau_{e+e^1}$, i.e. $E = \{\tau_e \mid e \in F\}$ is an elementary abelian group of order $2^n$ and $E \cdot Z \cong AGL(1, 2^n)$. The functions $A$ and $B$ are additive, so that:

$$
\tau_e \tau_{e^1} = \begin{pmatrix}
1 & A(e + e^1) & C(e + C(e^1) + A(e)B(e^1)) \\
1 & B(e + e^1) & 1 \\
1 & 1 & 1
\end{pmatrix}
$$

We have to show, that $C(e + e^1) = C(e) + C(e^1) + A(e)B(e^1)$. We compute:

$$
A(e)B(e^1) = (T_0(e^{2d}) + T_{n-b}(e^{2^{n-b}}))( \sum_{j=0}^{n/d-1} (T_{jd}(e^{2^{jd}})) + T_{jd+1}(e^{2^{jd+1}}))
$$

$$
= \sum_{j=0}^{n/d-1} (T_{jd}(e^{2^{jd}+2^{jd+1}}) + T_{jd+1}(e^{2^{jd+1}+2^{jd+1}})) + \sum_{j=0}^{n/d-1} (T_{jd}(e^{2^{jd}+2^{jd+1}}) + T_{jd+1}(e^{2^{jd+1}+2^{jd+1}}))
$$

$$
= \sum_{j=0}^{n/d-1} (T_{jd}(e^{2^{jd}+2^{jd+1}}) + T_{jd+1}(e^{2^{jd+1}+2^{jd+1}})) + \sum_{j=0}^{n/d-1} (T_{jd}(e^{2^{jd}+2^{jd+1}}) + T_{jd+1}(e^{2^{jd+1}+2^{jd+1}}))
$$

On the other hand $e \mapsto T_i(e)$ is additive and the entries of $C(e)$ are quadratic functions in $e$, i.e. $(e + e^1)^2 + 2^y = e^{2^y} + e^{2^y} + e^{2^y} + e^{2^y}$. Specializing $\{x, y\} = \{jd, b+jd\}$, $\{jd+1, b+jd+1\}$, we observe $C(e + e^1) = C(e) + C(e^1) + A(e)B(e)$.

(2) Define $\beta : F \to \text{Hom}(F, F \oplus F)$ by $\beta(e) = (A(e), C(e))$. Then $D = \{X(e) \mid e \in F\}$, with $X(e) = \{(x, x \beta(e)) \mid x \in F\} = \{(x, xA(e), xC(e)) \mid x \in F\}$ is a DHO.

We claim $\ker \beta(1) = \{1\}$:

Now $0 \neq x \in \ker A(1)$ implies $x + x^{2^{n-b}} = 0$ or $x^{2^{n-b} - 1} = 1$, forcing $x \in F_{2^n}$.

Moreover $xC(1) = Tr_{F:F_{2^n}}(x) + Tr_{F:F_{2^n}}(x^2) = Tr_{F:F_{2^n}}(x) + Tr_{F:F_{2^n}}(x^2)$. For
We observe, that \( \text{Im} C(1) \subseteq 0 \oplus F \oplus F_0 \). As \( [U, E] \) covers \( U_1 \cup U_0 \), where \( U_1 = 0 \oplus F \oplus F \), \( U_0 = 0 \oplus 0 \oplus F \). Clearly, \( [U_1, E] = 0 \oplus 0 \oplus F_0 \). The assertion follows.

(4) Define \( \Phi \in \text{GL}(U) \) by \( \Phi = \text{diag}(T_1(1), T_1(1), T_1(1)) \). Then \( Z(\Phi) \simeq \Gamma L(1, F) \) and \( EZ(\Phi) \simeq \text{AGL}(1, F) \) lies in \( \text{Aut}(D) \).

We leave the straightforward verification to the reader.

(5) \( E \) is not a translation group.

We have seen in (3), that \( [U, E] = 0 \oplus F \oplus F_0 \), which is not centralized by \( \tau_1 \). Thus \( E \) is not a translation group.

(6) \( \text{Aut}(D) = EZ(\Phi) \simeq \text{AGL}(1, F) \).

Otherwise by [13] \( \text{Aut}(D) \) is non-solvable and contains by [5] a normal translation group \( T \). As \( T \) is self-centralizing (see [1]), we see, that \( 1 < \langle T, E \rangle < T \)
is a proper subgroup invariant under $Z$. But $E$ is simple as a $Z$-module and $[T, E]$ is a non-trivial proper submodule, a contradiction.

(7) $D$ is not bilinear.

Assume, that $T \leq \text{Aut}(D)$ is a translation group. If $\text{Aut}(D)$ would contain more than one translation group, it would act imprimitively on $D$ (see [1, Thm. 4.6]), a contradiction. Hence $T = O_2(\text{Aut}(D)) = E$, contradicting (5).

(8) $D$ has no doubly transitive, bilinear quotient.

Assume $W \subset U(D) = F \oplus F \oplus F_0$, such that $D/W = \{(X(e) + W)/W \mid e \in F\}$ is a bilinear DHO. The verification of (6) also shows, that $EZ(\Phi)$ is (isomorphic to) the automorphism group of the universal cover of $D$ and by [3, Cor. 1.4] the automorphism group of $D/W$ is isomorphic to a doubly transitive subgroup of $EZ(\Phi)$. This shows, that $E$ lies in $\text{Aut}(D/W)$ and that $E$ leaves $W$ invariant. Now $E$ has a quadratic action on $U(D)/W$, i.e. $[[U(D)/W, E], E] = 0$ or equivalently $0 \oplus 0 \oplus F_0 = [[U(D), E], E] \subseteq W$. But then $F \ni e \mapsto A(e) \in \text{End}(F)$ defines a (bilinear) DHO (namely $D/[[U(D), E], E]$). But $D/[[U(D), E], E]$ is no DHO, since $\ker A(1) = \ker A(e)$ for $e \in F_{2d} - \{0,1\}$.

**Definition 3.6.** Let $n, d, b$ be as in Example 3.5. We denote the DHO constructed in this Example by $D[n, d, b]$.

**Remark 3.7.** We have shown in Example 3.5, that assertions (a), (b) and (d) of Theorem 1.1 hold. It remains to show assertion (c).

**Lemma 3.8.** Let $D = D[n, d, b]$ and $D' = D[n', d', b']$. Then $D \simeq D'$, iff $d = d'$ and $b' = b$ or $n - b$.

**Proof.** We have $d = d'$ by assertion (3) of Example 3.5. Let $U = F \oplus F \oplus F$ as in Example 3.5. For $D$ we use the notation of this Example and we denote entities related to $D'$ similarly by adding a ”prime” symbol. For instance $E' = O_2(\text{Aut}(D')) = \{\tau'_e \mid e \in F\}$ with

$$
\tau'_e = \begin{pmatrix} 1 & A'(e) & C'(e) \\ 1 & B'(e) & 1 \end{pmatrix}.
$$

(1) $D \simeq D'$ for $b' = n - b$.

Define $\Psi \in \text{GL}(U)$ by $\Psi = \text{diag}(T_{n-b}(1), 1, 1)$. We calculate $\Psi^{-1}z_e \Psi = z'_e$ and $\Psi^{-1}\tau_1 \Psi = \tau'_1$. This shows $\Psi^{-1}EZ\Psi = E'Z'$. As $D = XEZ$ and $D' = XE'Z'$ and $X\Psi = X$ with $X = F \oplus 0 \oplus 0$, we get $D\Psi = D'$ and claim (1) follows.

(2) If $D \simeq D'$, then $b' = b$ or $n - b$.

Let $\Psi \in \text{GL}(W)$, $W = F \oplus F \oplus F_0$ be the common ambient space of $D$ and $D'$, such that $D' = D\Psi$. Then $\text{Aut}(D') = \Psi^{-1}\text{Aut}(D)\Psi$. Therefore
\( E' = O_2(\text{Aut}(D')) = \Psi^{-1}O_2(\text{Aut}(D))\Psi = \Psi^{-1}E\Psi. \) So \( \Psi \) fixes \( Y = [W, E] = [W, E'] = 0 \oplus F \oplus F_0. \) Adjusting \( \Psi \) by an element of \( \text{Aut}(D) \), we may even assume, that \( Z' = \Psi^{-1}Z\Psi. \) Hence \( \Psi \) fixes \( W_1 = C_W(Z) = C_W(Z') = 0 \oplus 0 \oplus F_0 \) and \( W_2 = 0 \oplus F \oplus 0 \), which is the only non-trivial, simple module of \( Z \) in \( Y \) and the only non-trivial, simple module \( Z' \) in \( Z' \) as well. The groups \( Z \) and \( Z' \) have only one more non-trivial, simple module, namely \( W_1 = F \oplus 0 \oplus 0 \), which is therefore fixed by \( \Psi \). So with respect to the decomposition \( W = W_1 \oplus W_2 \oplus W_3 \) we may write \( \Psi = \text{diag}(\Psi_1, \Psi_2, \Psi_3) \) and \( \Psi_i \in N_\text{GL}(F)/T_0(F^*) = T_0(F^*)/T_1(1) \), \( i = 1, 2 \) (use Lemma 2.1), as the restriction of \( Z \) and \( Z' \) to \( W_i \) is \( T_0(F^*) \). Thus \( \Psi^{-1} = T_1(x) \), \( \Psi_2 = T_m(y) \) for some \( \ell, m \in I_n \) and \( x, y \in F^* \).

For \( e \in F \) there exists \( e' \), such that \( X(e)\Psi = X'(e') \). So for a typical element in \( (u, uA(e), uC(e)) \in X(e) \) we get

\[
(u, uA(e), uC(e))\Psi = (v, vT_1(x)A(e)T_m(y), vT_1(x)C(e)\Psi_3) \in X'(e'),
\]

where \( v = uT_1(x)^{-1} \). Hence

\[
A'(e') = T_0((e')^{2^\ell}) + T_{n-\ell}((e')^{2^n-1})
\]
\[
= T_1(x)A(e)T_m(y)
\]
\[
= T_{\ell+m}((xe^{2^\ell})^2^m y) + T_{\ell+m-\ell}((xe^{2^\ell}) y).
\]

Thus either \( \ell + m \equiv 0 \pmod{n} \) and \( b = b' \) or \( \ell + m - b \equiv 0 \pmod{n} \) and \( n - b' = \ell + m \). Claim (2) follows. Claims (1) and (2) complete the proof. \( \square \)

**Proof of Theorem 1.1.** Theorem 1.1 is a consequence of Remark 3.7 and Lemma 3.8.

Finally, we describe another series of non-bilinear, doubly transitive DHOs, that is closely related to the series from Examples 3.3 and 3.5.

**Example 3.9.** Let \( n = 2n_0 \), \( n_0 \) odd. Set \( k \equiv -2n_0 - 1, \ell \equiv -2n_0 + 1 \), and \( m \equiv -2n_0 - 1 \pmod{r_n} \). Set \( U = F \oplus F \oplus F \oplus F \). For \( e \in F \) we define linear operators \( A_1(e) = T_0(e^k) + T_{n_0}((e^k)^2), A_2(e) = T_0(e^{2n_0}), B(e) = \sum_{i=0}^{n_0 - 1} T_i(e^{2n_0 + i}) \) and \( C(e) = \sum_{i=0}^{n_0 - 1} T_i(e^{2n_0 + i + 1}) \) in End\((F)\) and

\[
\tau_e = \begin{pmatrix}
1 & A_1(e) & A_2(e) & C(e) \\
0 & 1 & 0 & B(e) \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1
\end{pmatrix} \in \text{GL}(U).
\]

As in Example 3.5 we check for \( e, e_1 \in F \), that \( C(e + e_1) = C(e) + C(e_1) + A_1(e)B(e_1) \). Then \( E = \{ \tau_e \mid e \in F \} \) is elementary abelian of order \( 2^n \). Define for \( e \in F^* \) the operator \( z_e = \text{diag}(T_0(e^k), T_0(e^k), T_0(e^m), 1) \). Then \( Z = \{ z_e \mid e \in F^* \} \) is cyclic of order \( r_n \) and it normalizes \( E \), so that \( EZ \approx \text{AGL}(1, F) \). Set \( X(0) = F \oplus 0 \oplus 0 \oplus 0 \), \( X(e) = X(0)\tau_e \) and \( D = \{ X(e) \mid e \in F \} \). Now \( \dim(X(0) \cap X(1)) = 1 \) as \( \ker(A_1(1), A_2(1), C(1)) = \langle 1 \rangle \). This shows, that \( D \) is a doubly transitive DHO.
Claim: \( D[2n_0, -2^{n_0+1} - 1] \) and \( D[2n_0, 2, n_0 + 1] \) are quotients of \( D \).

Set \( Y = 0 \oplus 0 \oplus 0 \oplus F \). It follows from the description of Example 3.3, that \( D/Y \simeq D[2n_0, -2^{n_0+1} - 1] \). Define the transformed \( D' = D\Psi \) with \( \Psi = diag(1, T_{n_0-1}(1), 1, 1) \). Then \( A\Psi B\Psi \) is a doubly transitive automorphism group of \( D' \) and \( z_{\Psi} = diag(T_0(e^k), T_0(e^{-1}), T_0(e^m), 1) \) and

\[
\tau_{\Psi} = \begin{pmatrix}
1 & A_1(e)T_{n_0-1}(1) & A_2(e) & C(e) \\
0 & 1 & 0 & T_{n_0+1}(1)B(e) \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1
\end{pmatrix}
\]

where \( A_1(e)T_{n_0-1}(1) = T_0(e^{2n_0+1}) + T_{n_0-1}(e^{2n_0-1}) \) and \( T_{n_0+1}(1)B(e) = \sum_{i=0}^{n-1} T_i(e^{2^i}) \). Now set \( Y = 0 \oplus 0 \oplus F \oplus 0 \). It follows from the description of Example 3.5, that \( D'/Y \simeq D[2n_0, 2, n_0 + 1] \).

Definition 3.10. Let \( n, n_0, k, \ell \) and \( m \) be as in Example 3.9. We denote the DHO constructed in this Example by \( \hat{D}[2n_0] \).

Remark 3.11. 1. We will see, that the DHO \( \hat{D}[2n_0] \) is simply connected and is therefore the universal cover of \( D[2n_0, 2, n_0 + 1] \) and of \( D[2n_0, -2^{n_0+1} - 1] \).

2. One can easily see, that \( \text{Aut}(\hat{D}[2n_0]) \simeq A\Gamma L(1, 2^{2n_0}) \).

3. \( \hat{D}[2n_0] \) is a non-bilinear DHO.

4. The ambient space of \( \hat{D}[2n_0] \) is \( F \oplus F \oplus F_{2n_0} \oplus F_2 \).

4 The proof of Theorem 1.2

In this section we shall prove Theorem 1.2.

Let \( D_0 \) be a known, solvable, doubly transitive DHO of rank \( n \) over \( F_2 \), i.e. this DHO has type \( S_{m,b}^n, h \neq m \), \( D[n,k] \) or type \( D[n,d,b] \). Because of Lemma 2.21,

we only will consider DHOs of rank \( \neq 6 \).

Since \( D_0 \) admits \( G = EZ \simeq A\Gamma L(1, F) \), \( E = O_2(G) \), \( Z \) cyclic of order \( r_n \), the universal cover admits \( G \) too [3, Cor. 1.4]. As we prove Theorem 1.2 by the way of contradiction:

\( D_0 \) is a proper quotient of it’s universal cover.

It is convenient, to consider a minimal \( G \)-cover: The DHO \( D \) is a proper, \( G \)-admissible cover of \( D_0 \) and every \( G \)-admissible quotient of \( D \), that covers \( D_0 \) properly is \( D \).

We denote by \( U \) the ambient space of \( D \) and let \( W \) be a \( G \)-invariant subspace, such that \( D_0 \simeq D/W \). We have:
Lemma 4.1. \( W \) is a trivial \( E \)-module and simple as an \( Z \)-module.

Proof. Assume, that \( E \) has a non-trivial action on \( W \), i.e. \( W \subset [W,E] \neq 0 \). Then \([W,E] \) is \( G \)-admissible and \( D/[W,E] \) is a quotient of \( D \), covering \( D_0 \simeq D/W \simeq ([D/[W,E]]/[W,E]) \) properly, a contradiction to the choice of \( D \). So \( E \) has a trivial action on \( W \). If \( 0 \subset W_0 \subset W \) would be a proper \( Z \)-submodule of \( W \), then \( D_0 \simeq (D/W_0)/(W/W_0) \) admits \( G \), and we have the same contradiction as before. \( \square \)

Notation. Assume, that \( D \) is a minimal \( G \)-cover of \( D_0 \). By Maschke’s Theorem the \( Z \)-module \( W \) has a \( Z \)-complement \( Y^0 \) in \( Y \), i.e. we have a decomposition

\[
U = X \oplus Y^0 \oplus W
\]

into \( Z \)-spaces. Hence for \( e \in F \) there exist \( A(e) \in \text{Hom}(X,Y^0) \), \( B(e) \in \text{End}(Y^0) \), \( L_1(e) \in \text{Hom}(X,W) \), and \( L_2(e) \in \text{Hom}(Y^0,W) \), such that

\[
\tau_e = \begin{pmatrix}
1_X & A(e) & L_1(e) \\
B(e) & L_2(e) \\
1_W
\end{pmatrix},
\]

is the representation of \( \tau_e \) with respect to the above decomposition. Note, that the DHO \( D_0 \) is bilinear, if \( B(e) = 1 \) for all \( e \). The representation of \( z_e \in Z \) has the form \( z_e = \text{diag}(T_0(e^k), (z_e)_Y, 0) \), where \( X \) induces the representation \( D^k \) and \( W \) the representation \( D^s \) of \( Z \). The space \( X(e) = X\tau_e \in D \) has the form \( \{ (x, xA(e), xL_1(e)) \mid x \in F \} \). The representations of \( \tau_e \) and \( z_e \) on the ambient space of \( D_0 \) are obtained by deleting the last row and column of the representation on \( U \). Now \( z_f^{-1}\tau_ee_f = \tau_{ef} \) implies

\[

t_0(e^{-k})A(1)(z_e)_Y = A(e), \quad (z_e)_Y^{-1}B(1)(z_e)_Y = B(e),
\]

\[
T_0(e^{-k})L_1(1)T_0(e^s) = L_1(e), \quad (z_e)_Y^{-1}L_2(1)T_0(e^s) = L_2(e).
\]

Refining our basic decomposition into a decomposition of simple \( Z \)-modules, shows that the blocks \( A(*) \), \( B(*) \), \ldots, \( L_2(*) \) decompose into smaller blocks, that can be expressed in the form \( T((*) \) ). Then the preceding equations show, that for \( \tau_e \) the entries in these small blocks are monomials in \( e \), i.e. have the form \( T((a(e)) \) with \( a(e) = (a_0e^{k_0}, \ldots, a_{n-1}e^{k_{n-1}}) \), \( a_i \in F \), \( k_i \in I_n \). On the other had for \( e, e_1 \in F \) the equation

\[
\tau_{e+e_1} = \tau_e \tau_{e_1}
\]

implies

\[
A(e + e_1) = A(e_1) + A(e)B(e_1), \quad B(e + e_1) = B(e)B(e_1)
\]

and

\[
L_1(e + e_1) = L_1(e) + L_1(e_1) + A(e)L_2(e_1), \quad L_2(e + e_1) = B(e)L_2(e_1) + L_2(e_1).
\]

22
If for instance \( D_0 \) is bilinear \((B(e) = 1)\), then the functions \( A \) and \( L_2 \) are additive.

Our basic approach to Theorem 1.2: We will consider a minimal \( G \)-cover \( D \) of a given \( DHO D_0 \). The results of Subsection 2.4 will enable us, to determine the functions \( L_1 \) and \( L_2 \). Then we invoke the basic Equations (6) and (7). They will either lead to the concrete description of the minimal \( G \)-cover or force a contradiction.

Remark 4.2. (1) If \( D_0 \) is bilinear we can and do assume, that \( D \) is not bilinear: Otherwise \( D \) is known by [2]. But it is clear, that none of the DHOs from [2] has a proper quotient of type \( S_{m,h}^n, m \neq h \), or \( D[n,k] \).

(2) Frequently we use the following observation: \( X(0) \cap X(1) = \{(x, xA(x), xL_1(x)) \mid x \in \ker A(1)\} \) and by our conventions \( \ker A(1) = \langle 1 \rangle \) in any case. Hence \( 1 \in \ker L(1) \) too.

4.1 Covers of \( S_{m,h}^n \)

In this Subsection we show:

Proposition 4.3. A DHO of type \( S_{m,h}^n, m \neq h \), is simply connected.

Proof. The DHO \( S_{m,n-m}^n \) is simply connected by [10, Cor. 1.6]. So we can assume \( m + h \neq n \). Let \( D \) be a minimal \( G \)-cover of \( D_0 \simeq S_{m,h}^n \). In this case \( D_0 \) is bilinear and \( Y^0 \) a simple \( Z \)-module. So we can write \( \tau_e \in E \ e \in F \), in the form

\[
\tau_e = \begin{pmatrix} 1 & A(e) & L_1(e) \\ 1 & L_2(e) & 1 \end{pmatrix}.
\]

Here \( Y^0 \) can be identified with \( F \) and \( A(e) = T_0(e^{2^n}) + T_m(e) \). The element \( z_e \in Z, e \in F^n \), has the form

\[
z_e = \text{diag}(T_0(e^k), T_0(e^l), T_0(e^s))\]

where \( k \equiv (2^h - 1)/(2^m - 1) \) and \( l \equiv (2^h + m - 1)/(2^m - 1) \) (mod \( r_n \)). By Remark 4.2 \( D \) is non-bilinear, i.e. \( L_2 : F \to \text{Hom}(Y^0, W) \) is non-trivial, and, as observed above, even \( L_2(1) \neq 0 \). On the other hand \( \tau_1 \) has order 2, which forces \( A(1)L_2(1) = 0 \). Since \( A(1) \) has rank \( n - 1 \) the transformation \( L_2(1) \) has rank 1. So we may even assume \( \text{Im} L_2(1) = \mathbb{F}_2 \), i.e. \( L_2(1) = \sum_{i=0}^{n-1} T_i(a^{2^i}) \) for some \( 0 \neq a \in F \). As \( L_2(e) = T_0(e^{-s})L_2(1)T_0(e^s) \), we see that the representation \( D^1 \) occurs \( n \) times in \( \text{Hom}(Y^0, W) \) (which we identify with \( \text{End}(F) \) with respect to the \( Z \)-representation \( D^{(\ell,s)} \)): Namely, the module \( L_2(F) \) (which affords \( D^1 \)) is a subconstituent of \( D^{(\ell,s)} \), which splits into the modules \( T_i(F) \) (affording \( D^{i-2^\ell} \) by Lemma 2.3), \( 1 \leq i \leq n \). As \( L_2(1) \) and hence \( L_2(e), e \neq 0 \) has a contribution from each \( T_i(F) \) the claim follows.

From Lemma 2.4 (a) and (b) we deduce \( \ell = -2a \) and \( s = 0 \). Then by Remark 3.2 (e) we have \( a \equiv -m, h \equiv -2m \) (mod \( n \)). Therefore we may identify \( W \) with \( \mathbb{F}_2 \) and we can write \( L_1(1) = \sum_{i=0}^{n-1} T_i(b^{2^i}) \) for some \( b \in F \).
Since $h$ is coprime to $n$ we conclude, that $n$ is odd. Moreover $k \equiv -2^{-2m} - 2^{-m}$ and $\ell \equiv -2^{-m} \pmod{r_n}$. We get

$$L_2(e) = T_0(e^{2^{-m}})L_2(1) = \sum_{i=0}^{n-1} T_i(a^2 e^{2^{i-m}})$$

and

$$L_1(e) = T_0(e^{2^{-m}+2^{-2m}})L_1(1) = \sum_{i=0}^{n-1} T_i(b^2 e^{2^{i-m}+2^{i-2m}}).$$

By Equation (7) $L_1(e + e_1) + L_1(e) + L_1(e_1) = A(e)L_2(e_1)$. We compute

$$A(e)L_2(e_1) = (T_0(e^{2^{-m}}) + T_m(e))(\sum_{i=0}^{n-1} T_i(a^2 e^{2i-1}\overline{m}))$$

$$= \sum_{i=0}^{n-1} T_i(a^2 e^{2i-2m} e_1^{i-m} + a^{i-m} e^{2i-2m} e_1^{i-2m}).$$

For the entry in $T_i(*)$ of $L_1(e + e_1)$ we have

$$b^{2i}(e + e_1)^{2i-m+2^{i-2m}} = b^{2i}(e^{2i-m+2^{i-2m}} + e_1^{i-2m} + e^{2i-2m} e_1^{i-2m}).$$

Thus for all $i$ and all $e, e_1$ we have the identity

$$b^{2i}(e^{2i-m} e_1^{i-2m} + e^{2i-2m} e_1^{i-m}) = a^{i-m} e^{2i-2m} e_1^{i-2m} + a^{2i-m} e^{2i-2m} e_1^{i-2m}.$$

We conclude ($i = 0$) $b = a = a^{2^{n-m}}$, i.e. $a = 1$, since $a \neq 0$ and $(n, m) = 1$. On the other hand we know $\ker A(1) = \langle 1 \rangle$ and $X(0) \cap X(1) = \langle (1, 0, 0) \rangle$, where $X(e) = X_{\tau e}$ as usual. Hence $1L_1(1) = Tr_{F_{2^d}}(1) = 0$, a contradiction, as $n$ is odd. The proof is complete. \hfill $\square$

4.2 Covers of $D[n, d, b]$

We show in this Subsection:

**Proposition 4.4.** Let $0 < b, d < n$, $(n, b) = d$, such that $n/d$ is odd. The following hold:

(a) If $(d, b) \neq (2, \frac{n}{2} \pm 1)$, then $D[n, d, b]$ is simply connected.

(b) Let $(d, b) = (2, \frac{n}{2} \pm 1)$, $2n_0 = n$. Then $D_0 = D[n, d, b]$ has a unique minimal $G$-cover $D \simeq \tilde{D}[2n_0]$.

We prove Proposition 4.4 by series of lemmas and assume, that $D$ is a minimal $G$-cover of $D_0 = D[n, d, b]$. We will obtain a contradiction, if $(d, b) \neq (2, \frac{n}{2} \pm 1)$ and if $(d, b) = (2, \frac{n}{2} \pm 1)$ we show assertion (b). We recall from Example 3.5, that $U_0 = F \oplus F \oplus F_0$, $F_0 = \{ x \in F_{2^d} | Tr_{F_{2^d}}(x) = 0 \}$, is the
ambient space of $D_0$. Note, that by assumption $\dim U(D) > \dim U_0$. We embed the ambient space of $D$ into $U = U_0 \oplus F$, so that we get representations of $E$ and $Z$ of the form

$$
\tau_e = \left( \begin{array}{cccc}
1 & A(e) & C(e) & L_1(e) \\
1 & B(e) & C(e) & L_2(e) \\
1 & D(e) & C(e) & L_3(e) \\
1 & F(e) & C(e) & L_4(e)
\end{array} \right),
$$

and for $e \neq 0$ we have

$$
z_e = \text{diag}(T_0(e^b), T_0(e^{-1}), 1, T_0(e^{e^a})),
$$

with $k \equiv -2^b - 1 \mod r_n$ and $A(e), B(e), C(e)$ are described in Example 3.5.

**Lemma 4.5.** $L_3$ is trivial.

**Proof.** The function $L_3$ is additive as $\tau_{e+e_1} = \tau_e + \tau_{e_1}$ (use the same argument, that leads to Equations (7)). As $L_3(e) = L_3(1)T_0(e^a)$, we see, that $s$ is a 2-power. Wlog. we can assume $s = 1$. Then

$$
L_2(e) = T_0(e)L_2(1)T_0(e).
$$

Exploiting Equations (7), we can express $L_2(e+e_1) + L_2(e) + L_2(e_1) = B(e)L_3(e_1)$ as

$$
T_0(e+e_1)L_2(1)T_0(e+e_1) + T_0(e)L_2(1)T_0(e_1) + T_0(e_1)L_2(1)T_0(e) = T_0(e)DL_3(1)T_0(e_1)
$$

where $D = B(1)$ is defined as in Example 3.5. Suppose $L_2(1) = \sum_{i=0}^{n-1} T_i(a_i)$ and $DL_3(1) = \sum_{i=0}^{n-1} T_i(b_i)$ we get for all $i, e, e_1$ the equations $b_i e^{2^i} e_1 = a_i (e^a e_1 + e^e_1)$. Setting $e = e_1$ we obtain $b_i = 0$ for all $i$. Therefore $DL_3(1) = 0$. Since $L_3(1)$ maps $F_0 = \text{Im } D$ into $W$, we deduce $L_3(1) = 0$ and hence $L_3(e) = L_3(1)T_0(e) = 0$. \hfill $\square$

**Lemma 4.6.** $L_2$ is trivial.

**Proof.** Assume, that $L_2$ is non-trivial. By Lemma 4.5 $L_2$ is additive and $D^1$ occurs in $D^{(-1,s)}$. Note, that $\tau_2 = 1$ implies $A(1)L_2(1) = 0$ and as rk $A(1) > n/2$ we get rk $L_2(1) < n/2$. So writing $L_2(1) = \sum_{i=0}^{n-1} T_i(a_i)$, there are at least three distinct $0 \leq i < n - 1$, such that $a_i \neq 0$, i.e. $D^1$ occurs in $D^{(-1,s)}$ at least three times. By assertion (a) Lemma 2.4 (with $-1$ in the role of $k$) we see $s = 0$ and $\dim U(D) = \dim U_0 + 1$. So we may assume, that the ambient space has the shape $U(D) = U_0 \oplus F_2$. This implies $a_i = a^{2^i}$ for some $a \in F$ and all $i$ and by the same token $L_1(1) = \sum_{i=0}^{n-1} T_i(b^{2^i})$ for some $b \in F$.

Then $L_2(e) = \sum_{i=0}^{n-1} T_i(a^{2^i} b^{2^i})$ and $L_1(e) = \sum_{i=0}^{n-1} T_i(b^{2^i} e^{2^i+1+2^i})$. For all $e, e_1$ we obtain the equation $L_1(e+e_1) = L_1(e) + L_1(e_1) + A(e)L_2(e_1)$. This leads for all $i, e, e_1$ to the equations $a^{2^i} e^{2^i+1} e_1^{2^i+1} + a^{2^{i+1}+2^i+2} e_1^{2^i+1} = b^{2^i} (e^{2^{i+1}+1} e_1^{2^i+1} + e^{2^i+1} e_1^{2^i+1})$, forcing $b = a = a^{2^i} \in F_{2^{2^i}}$. Hence $L_1(1) = L_2(1)$ and $\text{Tr}_{F_2}(a) = \sum_{i} a^{2^i} = 0$,
This implies \( C \) for all \( e \).

Then as \( 1 \in L_1(1) = 0 \) (see (2) of Remark 4.2). As \( 0 = \text{Tr}_{F:F_2}(a) = \frac{a}{d} \text{Tr}_{F:F_2}(a) = \text{Tr}_{F:F_2}(a) \), there exists \( c \in F_2 \) with \( a^{2i} = c^{2i} + c^{2i-1} \) for all \( i \). Set \( R = \sum_{i=0}^{d-1} T_i(c^{2i}) \) and

\[
\Psi = \begin{pmatrix} 1 & 1 & R \\ 1 & 1 \end{pmatrix}.
\]

Then

\[
DR = (\sum_{j=0}^{n/d-1} T_{jd}(1) + T_{jd+1}(1)) \left( \sum_{i=0}^{d-1} T_i(c^{2i}) \right)
\]

\[
= \sum_{j=0}^{n/d-1} (\sum_{i=0}^{d-1} T_{jd+i}(c^{2i} + c^{2i-1})) = \sum_{j=0}^{n/d-1} (\sum_{i=0}^{d-1} T_{jd+i}(c^{2i}))
\]

\[
= L_1(1).
\]

This implies \( C(e)R + L_1(e) = T_0(e^{-k})(DR + L_1(1)) = 0 \). Hence \( X(e)\Psi \subseteq U_0 \) for all \( e \), a contradiction, as \( \dim U(D) > \dim U_0 \).

\[ \square \]

**Lemma 4.7.** \( d = 2, b = \frac{n}{2} \pm 1 \) and \( D \cong \hat{D}[2n_0], n_0 = n/2 \).

**Proof.** By Lemmas 4.5 and 4.6 \( L_1 \) is additive. Write \( L_1(1) = \sum_{i=0}^{n-1} T_i(a_i) \). Since \( 1 \in \ker L_1(1) \) (by (2) of Remark 4.2), this operator has rank \( < n \). So there are at least two distinct \( 0 \leq i \leq n - 1 \), such that \( a_i \neq 0 \). We also may assume, that \( L_1(1) \) projects non-trivially into \( T_0(F) \). Hence \( D^{(k,s)} \) contains \( D^1 \) at least two times and, that \( s - k \equiv s + 2^k + 1 \equiv 2^x \) and \( s - 2^k \equiv s + 2^{xy}y + 2y \equiv 2^x \) (mod \( r_n \)) for some \( x, y, z \in \{0, 1, ..., n - 1\}, y > 0 \).

We can apply Lemma 2.20 and assume first, that assertion (a) of that Lemma holds: \( s \equiv -1 \) (mod \( r_n \)), \( x \equiv -y \equiv -z \equiv b \) (mod \( n \)). Then \( L_1(1) = T_0(a) + T_{n-b}(a) \) (as \( 1L_1(1) = 0 \)) for some \( a \neq 0 \). Thus

\[
L_1(e) = T_0(e^{-k})L_1(1)T_0(e^{-1}) = T_0(a^e^{2^x}) + T_{n-b}(a^e^{2^x}).
\]

We observe \( A(e)T_0(a) = L_1(e) \). Set

\[
\Psi = \begin{pmatrix} 1 & T_0(a) \\ 1 & 1 \end{pmatrix}.
\]

Then \( X(e)\Psi \subseteq U_0 \) for all \( e \), we reach the same contradiction as in the proof of the previous Lemma. Assertion (b) of Lemma 2.20 leads similarly to a contradiction.

So assertion (c) or (d) of Lemma 2.20 hold and \( d = 2, b = \frac{n}{2} \pm 1 \). By Lemma 3.8 \( D[n, 2, \frac{n}{2} + 1] \) and \( D[n, 2, \frac{n}{2} - 1] \) are isomorphic, so that we can assume \( b = n_0 + 1, n_0 = n/2 \). Then \( s \equiv -2^{n_0} - 1 \) (mod \( r_n \)) and \( L_1(1) = T_0(a) + T_{n_0}(a) \).
again by Lemma 2.20. Transforming with $\text{diag}(1, 1, 1, T_0(a^{-1}))$ we even may assume $a = 1$. Then

$$
\tau^\Phi_e = \begin{pmatrix}
1 & A_1(e) & A_2(e) & C(e) \\
1 & 1 & B(e) & 1 \\
1 & 1 & 1 & 1
\end{pmatrix},
$$

where $\Phi = \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix}$ and $A_1(e) = A(e), A_2(e) = L_1(e)$. Then $\tau^\Phi_e$ has precisely the form of $\tau^\Psi_e$ in Example 3.9 and hence $D$ is isomorphic to $D' \simeq \hat{D}[2n_0]$ (in the notation of this example).

Proposition 4.4 follows from Lemmas 4.5, 4.6, and 4.7.

### 4.3 Covers of $D[n, k]$  

In this Subsection we prove:

**Proposition 4.8.** Let $n = 2n_0$, $n_0 > 3$ odd. The following hold:

(a) If $k \not\equiv -2n_0 + 1 \pmod{r_n}$, then $D[n, k]$ is simply connected.

(b) Let $k \equiv -2n_0 + 1 \pmod{r_n}$. Then $D[n, k]$ has a unique minimal $G$-cover $D \simeq \hat{D}[2n_0]$.

We prove Proposition 4.8 by series of lemmas and assume, that $D$ is a minimal $G$-cover of $D_0 = D[n, k]$. We will obtain a contradiction, if $k \neq -2n_0 + 1$ and if $k = -2n_0 + 1$ we show assertion (b). We recall form Example 3.3, that $U_0 = F \oplus F \oplus F_0$, $F_0 = \mathbb{F}_{2n_0}$, is the ambient space of $D_0$. We embed the ambient space of $D$ into $U = U_0 \oplus F$, so that we get representations of $E$ and $Z$ of the form

$$
\tau_e = \begin{pmatrix}
1 & A_1(e) & A_2(e) & L_1(e) \\
1 & 1 & L_2(e) & 1 \\
1 & 1 & 1 & 1
\end{pmatrix},
$$

and for $e \neq 0$ we have

$$
z_e = \text{diag}(T_0(e^k), T_0(e^\ell), T_0(e^m), T_0(e^s)),
$$

where $A_1(e), A_2(e)$ and the numbers $k, \ell$ and $m$ are described in Example 3.3. By Remark 4.2 at least one of $L_2$ or $L_3$ in non-trivial. The determination of the $L_i$’s will rest on the results of Subsection 2.4.

**Lemma 4.9.** $L_2$ is non-trivial.
Proof. Suppose, that $L_2$ is trivial. Then $\tau_1^2 = 1$ implies $A_2(1)L_3(1) = 0$, i.e. $rk L_3(1) < n$ and $D^1$ occurs at least two times in $D^{(m,s)}$. We also may assume, that $L_3(1)$ projects non-trivially into $T_0(F)$. Thus we have $s - m \equiv 2^a$ and $s - 2^b m \equiv 2^s$ (mod $r_n$) for some $0 \leq a, b, c < n$, $b > 0$. By Lemma 2.15 $a = c$ and $b = n_0$. Therefore $L_3(1) = T_0(u) + T_{n_0}(v)$, $u, v \neq 0$. As $0 = A_2(1)L_3(1) = T_0(u+v) + T_{n_0}(u+v)$, we get $u = v$ and

$$L_3(e) = T_0(u e^{2s}) + T_{n_0}(u e^{2s}) = L_3(1)T_0(e^{2s})$$

for $e \in F$. On the other hand $A_2(e) = T_0(e)A_2(1)$ for $k = (2^{n_0} + 1)^{\pm 1}$ and $A_2(e) = T_0(e^{2^{n_0}})A_2(1)$ for $k = (2^{n_0} - 1)^{\pm 1}$ by Example 3.3. Thus for all $e, e_1 \in F$ we have

$$A_2(e)L_3(e_1) = T_0(e^*)A_2(1)L_3(1)T_0(e^{2s}) = 0,$$

which implies, that $L_1$ is additive. Hence $\tilde{E} = \{\tilde{T}_e \mid e \in F\}$ with

$$\tilde{T}_e = \begin{pmatrix} 1 & A_1(e) & A_2(e) & L_1(e) \\ 1 & 1 & 1 & 1 \end{pmatrix},$$

is an elementary abelian group of order $2^n$ in $GL(U)$ with a quadratic action. As $D = \{X(0)\tilde{T}_e \mid e \in F\}$, i.e. $\tilde{E} \leq \text{Aut}(D)$, we conclude, that $D$ is a bilinear DHO, contradicting Remark 4.2.

**Lemma 4.10.** $L_3$ is trivial.

Proof. By Lemma 4.9 $L_2$ is non-trivial. Assume, that $L_3$ is non-trivial too. Then $L_1$ is a homomorphism and the representations $D^{(\ell,s)}$ and $D^{(m,s)}$ have at least one constituent $D^1$. Therefore we may assume (defining $s$ appropriately) $s \equiv 1 + 2^a \ell \equiv 2^b + 2^c m$ (mod $r_n$). The integer $s$ is given in Lemmas 2.15 and 2.19. We shall show for any $e, e_1 \in F$, that $A(e)L(e_1) = 0$, where $A(e) = (A_1(e), A_2(e))$ and $L(e_1) = (L_2(e_1), L_3(e_1))^T$, which in turn will lead to the contradiction $L_2 = 0$. By the choice of our notation we have $1 \in ker(A(1))$.

Case $k \equiv 2^a + 2^b + 2^c - 2^x (mod r_n)$. In this case we have by (b) of Lemma 2.6 (or Example 3.3) $\ell \equiv k + 2^{n_0} + 1 \equiv 2^k + 1$ (mod $r_n$), $m \equiv 2^{n_0} k + 2^{n_0} \equiv k + 1$ (mod $r_n$), and for the equation $s \equiv 1 + 2^a \ell \equiv 2^b + 2^c m$ (mod $r_n$), the numbers $a, b, c$ are given by Lemma 2.16, in particular $a = 0$ or $n - 2$. Recall $A_1(e) = T_0(e^{2^{n_0} + 1}) + T_2(e)$ and $A_2(e) = T_0(e) + T_{n_0}(e^{2^{n_0}})$. The representation $D^1$ occurs in $D^{(\ell,s)}$ only once: Otherwise we would have $2^{n_0}s \equiv 2^{n_0} \ell \equiv 2^x + 2^y \ell$ (mod $r_n$) with $0 \leq x, y < n, y \neq 0$. By Lemma 2.13 $n - a \in \{n_0 + 3, n - 2\}$ for $n_0 > 5$ and $n - a = 8$ for $n_0 = 5$, a contradiction.

Assume first $a = 0$, i.e. $(b, c) \in \{(n_0 + 1, 0), (n_0 + 1, n_0)\}$ and $s \equiv \ell + 1$. Then $L_2(1) = T_0(\alpha)$ for some $\alpha \in F$ and by the same token $L_3(1) = T_0(\beta) + T_{n_0}(\gamma)$,
\(\beta, \gamma \in F\). Moreover \(L_2(e) = T_0(e^\ell)T_0(\alpha)T_0(e^s) = T_0(\alpha e^e)\) and similarly \(L_3(e) = T_0(\beta e^{2n_1}) + T_{m_0}(\gamma e^{2n_1+1})\). For \(e, e_1 \in F\) we compute:

\[
A(e)L(e_1) = A_1(e)A_2(e)A_3(e_1) + T_0((\beta + \gamma)e^{2n_1}e_1) + T_0((\beta + \gamma)e^{2n_1-1}e_1) + T_0((\beta + \gamma)e^{2n_1}e_1) + T_0((\beta + \gamma)e^{2n_1-1}e_1)
\]

As \(A(e)B(e) = 0\) we get \(\alpha = 0\) and \(\beta = \gamma\). This implies \(L_2 = 0\), a contradiction.

Assume next \(a = n - 2\) and \(s \equiv 1 + 2^{n-2}t \equiv 2^{n-2} + m \equiv 2^{n-2} + 2^m\). Now we get \(L_2(e) = T_{n-2}(\alpha e)\) and \(L_3(e) = T_0(\beta e^{2n-2}) + T_{m_0}(\gamma e^{2n-2})\). Finally

\[
A(e)L(e_1) = T_0(\alpha e^{2n-2}e_1) + T_{n-2}(\alpha e^{2n-2}e_1) + T_0((\beta + \gamma)e^{2n_1}e_1) + T_{m_0}((\beta + \gamma)e^{2n_1}e_1)
\]

showing again \(\alpha = 0\) and \(\beta = \gamma\) and hence \(A(e)L(e_1) = 0\). Again \(L_2 = 0\), a contradiction as before.

The cases \(k \equiv -2^{n+1} \pm 2^m (\text{mod } r_n)\) and \(k \equiv 2^{n+1} + 1 (\text{mod } r_n)\) (using Lemmas 2.14, 2.12, 2.17 and 2.18) have very similar verifications, that we leave to the reader.

Case \(k \equiv 2^{n+1}+1 (\text{mod } r_n)\). Now \(\ell \equiv k+1 \equiv 2^{n+1}k+2^2, m \equiv k+2^m \equiv 2^k+1 (\text{mod } r_n)\), \(A_1(e) = T_0(e) + T_{n+1}(\alpha e^e)\) and \(A_2(e) = T_0(\beta e^{2n-2}) + T_{m_0}(\gamma e^{2n-2})\). Moreover \(a = n - 1\) or \(n_0 = n - 1\) by Lemma 2.19. If \(D_1\) would occur two times in \(D^{(\ell,s)}\), then \(s2^{n-a} \equiv 2^{\ell+1}+2\gamma (\text{mod } r_n)\) with \(y > 0\). By Lemma 2.11 \(n - a = n_0 + 1, a\) contradiction. So \(D_1\) occurs only once in \(D^{(\ell,s)}\).

Assume first \(a = n-1\). Then \((b, c) \in \{(1, 0), (1, n_0)\}\) and our usual arguments show \(L_2(e) = T_{n-1}(\alpha e)\) and \(L_3(e) = T_0(\beta e^e) + T_{m_0}(\gamma e^e)\). Then

\[
A(e)L(e_1) = T_{m_0}(\alpha e^{2n_1}e_1) + T_{n-1}(\alpha e^{2n_1-1}e_1) + T_0((\beta + \gamma)e^{2n_1}e_1) + T_{m_0}((\beta + \gamma)e^{2n_1}e_1)
\]

showing \(\alpha = 0\), \(\beta = \gamma\), if we specialize \(e = e_1\). Hence \(L_2 = 0\) and we end up with the same contradictions as before.

Assume now \(a = n_0\). Now \(L_2(e) = T_{n_0}(\alpha e)\) and \(L_3(e) = T_0(\beta e^{2n}) + T_{m_0}(\gamma e^{2n})\). Now

\[
A(e)L(e_1) = T_{n_0}(\alpha e^{2n_1}e_1) + T_{n_1}(\alpha e^{2n_1+2}e_1) + T_0((\beta + \gamma)e^{2n_1}e_1) + T_{m_0}((\beta + \gamma)e^{2n_1}e_1)
\]

showing \(\alpha = 0\), \(\beta = \gamma\) (by specializing \(e = e_1\)) and thus \(L_2 = 0\), the usual contradiction.

\[\square\]

**Lemma 4.11.** \(k \equiv -2^{n+1} - 1 (\text{mod } r_n)\) and \(D\) is isomorphic to \(\hat{D}[2n_0]\).

**Proof.** By Equation (7) and Lemma 4.10 we have \(L_1(e + e_1) + L_1(e) + L_1(e_1) = A_1(e)B_1(e_1)\). Moreover \(A_1(e)\) and \(B_1(e_1)\) are additive in \(e\) and \(e_1\) respectively. Therefore the non-trivial entries in \(L_1(e)\) have to be quadratic polynomials in \(e\).
Moreover as $\tau^2 = 1$ (i.e. $A_1(1)L_2(1) = 0$) the operator $L_2(1)$ has contributions from at least two $T_i(F)$’s.

**Case $k = 2^s+2^{n_0+1}−2$.** Assume $n_0 = 5$. By Example 3.3 we have $A_1(e) = T_0(e^{\hbar^6}) + T_2(e)$ and considering $L_2$ we have $2^s \equiv s - \ell, 2^s \equiv s - 2^\ell$ (mod $r_n$) for some $a, b, c, d > 0$. From Lemma 2.13 we obtain $L_2(e) = \sum_{i=0}^{n-1} b_i(a_2 e^{2i-2} + a_1 e^{0})$, and $L_1(e) = \sum_{i=0}^{n-1} b_i(a_2 e^{2i-2} + a_1 e^{0})$ (if $L_1(1)$ has a contribution from $T_0(F)$, then $2^s + 2^\ell \equiv s - 2^\ell$ (mod $r_n$) for some $e, f$). As $0 = A_1(1)L_2(1) = \sum_{i=0}^{n-1} b_i(a_2 + a_1)$, we conclude $a = a_0 = \cdots = a_8$ as some $a \in F$. Furthermore for arbitrary $e, e_1 \in F$ we get $A_1(e)L_2(e_1) = \sum_{i=0}^{n-1} T_2(a_2 e_1 e^{2i-2} + a_1 e_1^{0})$ and $L_1(e + e_1) + L_1(e)L_1(e_1) = \sum_{i=0}^{n-1} T_2(b_2 e_1 e^{2i-2} + b_1 e_1^{0})$. Hence $a = b_2$ for all $i$. As $0 = 1L_1(1) = \sum_{i=0}^{n-1} b_2 = 5a = a$, we obtain $L_2 = 0$, a contradiction.

Assume now $n_0 > 5$. For arbitrary $e, e_1 \in F$ we shall compute $A_1(e)L_2(e_1)$ again. Recall, that $A_1(e) = T_0(e^{2^{n_0+1}}) + T_2(e)$. Assertion (a) of Lemma 2.13 implies, that two cases can occur, namely

$L_2(e_1) = T_0(ace_{1}^{0} e^{3^{n_0+3}}) + T_2(be_{1})$ or $L_2(e_1) = T_0(ae_{1}^{0} + T_{n-2}(be_{1}2^{n_{0}+1}))$,

with $0 \neq a, b \in F$. A computation shows

$A_1(e)L_2(e_1) = T_0(ace_{1}^{0} e^{3^{n_0+3}}) + T_2(ae_{1}^{0} e^{3^{n_0+3}}) + T_4(1be_{1})$

in the first case and

$A_1(e)L_2(e_1) = T_0(ace_{1}^{0} e^{3^{n_0+3}}) + T_2(ae_{1}^{0} e^{3^{n_0+3}}) + T_{n-2}(be_{1}2^{n_{0}+1})$

in the second case. Now $A_1(1)L_2(1) = 0$ forces $a = b = 0$, a contradiction.

Cases $k \equiv -2^{n_0+1} \mod r_n$. Using Lemmas 2.14 and 2.12, these two cases can be treated in a completely similar fashion as the second part of Case $k \equiv 2^{n_0+1} - 2$. We finally turn to:

**Case $k \equiv 2^{n_0+1} - 1 \mod r_n$.** Then $\ell \equiv -2^{n_0+1}$ and by Lemma 2.11 $s = \ell + 2^{n_0+1} = 0$, i.e. $W$ is the trivial $\mathbb{Z}$-module, which we can identify with $\mathbb{F}_2$. Then $L_2(1) = \sum_{i=0}^{n-1} T_i(a_2^\ell)$ and $L_1(1) = \sum_{i=0}^{n-1} T_i(b_2^\ell)$ for some $a, b \in F$.

As $A_1(1) = T_0(1)+T_{n_0+1}(1)$, we get $0 = A_1(1)L_2(1) = \sum_{i=0}^{n-1} T_i(a_2^\ell + a_1^2 e^{2n_0-1})$, which shows $a = a_2^2 e^{2n_0-1}$ or $a \in \mathbb{F}_4$, as $(n, n_0 + 1) = 2$. Finally, we have $A_1(e) = T_0(e) + T_{n_0+1}(e^2)$, $L_2(e) = T_0(1-e)L_2(1) = \sum_{i=0}^{n-1} T_i(a_2^\ell e^{2n_0+1})$ and $L_1(e) = T_0(e) + T_{n_0+1}(e^2L_1(1) = \sum_{i=0}^{n-1} T_i(b_2^\ell e^{2n_0+1})$. Exploiting the equation $L_1(e + e_1) = L_1(e) + L_1(e_1) + A_1(e)L_2(e_1)$, we see, that $a = b$. Finally, $0 = L_1(1) = T_{F,F_2}(a) = T_{F,F_1}(T_{F_2,F_2}(a)) = n_0 T_{F_2,F_2}(a)$. Since $n_0$ is odd, we conclude $a = 1$ and $D$ is isomorphic to $D[2n_0]$. □

Proposition 4.8 follows from Lemmas 4.9, 4.10 and 4.11. To finish the proof of Theorem 1.2 we need:

**Lemma 4.12.** $D[2n_0]$ is simply connected.
Proof. Let $D$ be a minimal $G$-cover of $D_0 \simeq \hat{D}[2n_0]$. Then (using the notation of Example 3.9)

$$
\tau_e = \begin{pmatrix}
1 & A_1(e) & A_2(e) & C(e) & L_1(e) \\
0 & 1 & 0 & B(e) & L_2(e) \\
0 & 0 & 1 & 0 & L_3(e) \\
0 & 0 & 0 & 1 & L_4(e) \\
0 & 0 & 0 & 0 & 1
\end{pmatrix}
$$

and for $e \neq 0$ we have $z_e = \text{diag}(T_0(e^k), T_0(e^f), T_0(e^m), 1, T_0(e^s))$. Note, that $A_1, A_2, B, L_3$ and $L_4$ are additive and

(i) $C(e + e_1) = C(e) + C(e_1) + A_1(e)B(e_1)$,
(ii) $L_2(e + e_1) = L_2(e) + L_2(e_1) + B(e)L_4(e_1)$, and
(iii) $L_1(e + e_1) = L_1(e) + L_1(e_1) + A_1(e)L_2(e_1) + A_2(e)L_3(e_1) + C(e)L_4(e_1)$.

Assume, that $L_4$ is trivial. Then $\tilde{E} = \{\tilde{\tau}_e \mid e \in F\}$ with

$$
\tilde{\tau}_e = \begin{pmatrix}
1 & A_1(e) & A_2(e) & L_1(e) \\
0 & 1 & 0 & L_2(e) \\
0 & 0 & 1 & L_3(e) \\
0 & 0 & 0 & 1
\end{pmatrix}
$$

is elementary abelian of order $2^n$ (using (i)-(iii)) and is normalized by $\tilde{Z} = \{\tilde{z}_e \mid e \in F^*\}$, where $\tilde{z}_e = \text{diag}(T_0(e^k), T_0(e^f), T_0(e^m), T_0(e^s))$. So $\tilde{E}\tilde{Z} \simeq AGL(1, F)$ defines a $G$-cover of a DHO of type $D[n, -2^{n_0+1} - 1]$. We conclude from Proposition 4.4, that $L_3$ is trivial too and $\dim W = 1$. But by the same token (and using again (i)-(iii)) $\tilde{E} = \{\tilde{\tau}_e \mid e \in F\}$ with

$$
\tilde{\tau}_e = \begin{pmatrix}
1 & A_1(e) & C(e) & L_1(e) \\
0 & 1 & 0 & B(e) \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1
\end{pmatrix}
$$

is elementary abelian of order $2^n$ and is normalized by $\tilde{Z} = \{\tilde{z}_e \mid e \in F^*\}$, where $\tilde{z}_e = \text{diag}(T_0(e^k), T_0(e^f), 1, T_0(e^s))$. So $\tilde{E}\tilde{Z} \simeq AGL(1, F)$ defines a $G$-cover of a DHO of type $D[n, 2, n_0 + 1]$. We conclude from Proposition 4.4, that $L_2$ is trivial too and $\dim W = n_0$, a contradiction.

So $L_4$ is non-trivial. Assume now, that $L_3$ is trivial. Then again $\tilde{E} = \{\tilde{\tau}_e \mid e \in F\}$ with

$$
\tilde{\tau}_e = \begin{pmatrix}
1 & A_1(e) & C(e) & L_1(e) \\
0 & 1 & 0 & B(e) \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1
\end{pmatrix}
$$

is elementary abelian of order $2^n$ and $\tilde{E}\tilde{Z} \simeq AGL(1, F)$, with the same $\tilde{Z}$ as above and $\tilde{E}\tilde{Z}$ defines a $G$-cover of a $D[2n_0, 2, n_0 + 1]$. Again using Proposition 4.4 we conclude, that $L_4$ is trivial. But that case was ruled our already.
Therefore \( L_3 \) and \( L_4 \) are both non-trivial. As \( L_4(e) = L_4(1)T_0(e^s) \) and as \( L_4 \) is additive, we conclude, that \( s \) is a 2-power, say \( 2^a \). Also \( L_3(e) = T_0(e^{-m})L_3(1)T_0(e^s) \), and \( L_3 \) is additive. Hence \( D^3 \) occurs in \( D^{(m,s)} \). So \( 2^a - 2^b m \equiv 2^c \pmod{r_n} \) for some integers \( b \) and \( c \). As \( m = -2^a - 1 \) we get

\[
2^a + 2^b + 2^{m+b} \equiv 2^c \pmod{r_n}.
\]

However the LHS of this congruence has a weight \( \geq 2 \), whereas the RHS has weight 1. This final contradiction completes the proof.

Theorem 1.2 follows from Propositions 4.3, 4.4, 4.8 and Lemma 4.12.

References