

Automorphisms and Equivalence of Bent Functions and of Difference Sets in Elementary Abelian 2-groups

U. Dempwolff

Abstract

The problem of computing the automorphism groups of elementary abelian Hadamard difference sets or equivalently of bent functions seems to have attracted not much interest so far. We describe some series of such sets and compute their automorphism group. For some of these sets the construction is based on the nonvanishing of the degree 1-cohomology of certain Chevalley groups in characteristic two. We also classify bent functions f such that $\text{Aut}(f)$ together with the translations from the underlying vector space induce a rank 3 group of automorphisms of the associated symmetric design. Finally we discuss computational aspects associated with such questions.

1 Introduction.

Let $V = V(N, 2)$ be an N -dimensional $\text{GF}(2)$ -space and B a subset of V . We assume that $B + v \neq B$ for $0 \neq v \in V$ and set $\mathbf{B} = \{B + v \mid v \in V\}$. If the incidence structure $\mathbf{D}(B) = (V, \mathbf{B})$ is a symmetric $(2^N, k, \lambda)$ -design one calls B an (elementary abelian) *Hadamard difference set*, we abbreviate and call B a *B-set*. By a theorem of Mann [Ma] $N = 2n$ is even and $(k, \lambda) = (2^{n-1}(2^n - 1), 2^{n-1}(2^{n-1} - 1))$ or $(2^{n-1}(2^n + 1), 2^{n-1}(2^{n-1} + 1))$. The function $f_B = \chi_B + 1$, where $\chi_B : V \rightarrow \text{GF}(2)$ is the characteristic function of B , is called a *bent function*, i.e. it's zeros are the B-set B . Since the set $\overline{B} = V - B$ is a B-set too also $f_B + 1 = f_{\overline{B}}$ is a bent function. Any function $f : V \rightarrow \text{GF}(2)$ can be represented by a unique boolean polynomial $p_f = p(x_1, \dots, x_{2n})$ in $2n$ variables. In the case of f_B this polynomial has degree $2 \leq \deg f_B \leq n$ (see [Di2] for instance). Two B-sets B, B' are *equivalent* iff there is an affine transformation $\beta = T[v] \in \text{AGL}(V)$, $\beta : x \mapsto xT + v$, such that $B' = B\beta = \{xT + v \mid x \in B\}$. Since affine transformations do not change the degree of a boolean polynomial this degree is a useful invariant for equivalence. $\beta \in \text{AGL}(V)$ is an *automorphism* of B iff $B = B\beta$. The group $\text{Aut}(B) = \{\beta \in \text{AGL}(V) \mid B = B\beta\} \leq \text{AGL}(V)$ is the *automorphism group* of B .

Let $A = \text{Aut}(\mathbf{D}(B))$ be the automorphism group of the associated symmetric design. Then the semidirect product of $\text{Aut}(B)$ with the translation group $[V]$ is

$$N_A(V) = \text{Aut}(B)[V].$$

In general it seems difficult to decide as to whether or not this group is equal to A .

The most prominent bent functions are nondegenerate quadratic forms on V . Up to equivalence these are $\Theta = \Theta^+ = x_1x_{2n} + x_2x_{2n-1} + \cdots + x_nx_{n+1}$ and $\Theta = \Theta^- = \Theta^+ + x_n + x_{n+1} \sim \overline{\Theta} = \Theta^+ + 1$ and the associated B-sets are the isotropic and anisotropic vectors of V with respect to Θ^+ . We call these B-sets *standard* and denote them by the symbols B^0 and \overline{B}^0 .

In this paper we are concerned with the equivalence and automorphism problem of B-sets. Contributions to the equivalence problem are contained for instance in [Bd], [Di1], [Di2], [Hou], [Ka2], [Ro]. As expected invariants play a decisive role. The computation of the automorphism group of B-sets seems to have attracted not much attention yet. However in [CRB1] and [CRB2] automorphisms of some homogeneous cubic bent functions have been computed with the help of MAGMA [MAG]. The thesis of Bending [Bd] contains the computation of some automorphism groups of bent functions in dimension 8 with the help of GAP.

We will introduce in the next section more notation and a few observations on B-sets. We also collect some results on representations and 1-cohomology of finite groups of Lie type in even characteristic and some number theoretic results. These results will be used in the proofs of the main results which we describe now.

In section 3 we describe in (3.1.a-d) and B-sets which will be called *standard parabolic*, *twisted parabolic*, *special parabolic*, and *sporadic parabolic*. They are obtained by distortions of the standard B-sets B^0 and \overline{B}^0 . Associated with every such B-set is a totally singular subspace U say of dimension m of the orthogonal space $V = (V, \Theta)$, $\Theta = \Theta^\epsilon$. The standard parabolic B-sets are defined for $\epsilon = +$ and these sets depend only on the parameter m called the degree which ranges between 3 and n . The twisted parabolic B-sets depend on m and two more parameters b, ϵ where m ranges between 1 and $n - 2$ and b divides $n - m$ and $\epsilon = +$ or $-$. The special parabolic B-sets exist if $n = m$, $\epsilon = +$ and 3 divides n . The sporadic parabolic B-sets exist only for $n = m = 12$, $\epsilon = +$. The automorphism problem is solved by the following theorem.

Theorem A. *Let V be a $2n$ -dimensional $\text{GF}(2)$ -space and Θ a nondegenerate quadratic form. Let B be a B-set of one of the parabolic types and let U be the totally singular subspace of dimension m associated with B . Let $\text{Sp}(V)$ be the symplectic group with respect to the bilinear form obtained by polarisation of Θ and let $P_U = \text{Sp}(V)_U$ be the maximal parabolic subgroup of $\text{Sp}(V)$ which is the stabilizer of U . Set $Q = O_2(P_U)$. Then $\text{Aut}(B) \simeq QL \leq P_U$, $L \cap Q = 1$. The group L has the following structure:*

- (a) *Let B be standard parabolic. Then $L = L_1 \times L_2$, $L_1 \simeq \text{SL}(m, 2)$ and $L_2 \simeq \text{Sp}(2(n - m), 2)$. In particular $\text{Aut}(B) \simeq P_U$.*
- (b) *Let B be twisted parabolic with parameters m, b, ϵ . Then $L = L_1 \times L_2$ where L_1 is as in (a) and*

$$L_2 \simeq \begin{cases} \text{Sp}(2a, 2^b), & m = 1, ab = n - 1, \\ \text{O}^+(2a, 2^b), & m > 1, ab = n - m, \epsilon = + \\ \text{O}^-(2a, 2^b), & m > 1, ab = n - m, \epsilon = -. \end{cases}$$

- (c) *Let B be special parabolic. Then $m = n = 3b$ and $L \simeq \text{SL}(3, 2^b) \cdot Z$ with $Z \simeq \text{Gal}(\text{GF}(2^b))$.*

- (d) Let B be sporadic parabolic. Then $m = n = 12$ and $L \simeq \mathbf{G}_2(4) \cdot Z$ where Z is cyclic of order 2 and induces the field automorphism on $\mathbf{G}_2(4)$.

This theorem of course settles the equivalence problem for B-sets of parabolic type too. See also the remark after (6.8).

Set $F = \mathbf{GF}(2^n)$. Denote by $\varphi(k)$, $0 \leq k < 2^n - 1$ the endomorphism $x \mapsto x^k$ of the multiplicative group F^* of F . Let $\varphi(k)$ be an automorphism, i.e. $(k, 2^n - 1) = 1$. Then we associate with $\varphi(k)$ two B-sets $B_i^{(k)}$, $i = 1, 2$, $|B_i^{(k)}| = 2^{n-1}(2^n + (-1)^i)$ (see (3.2)) which are called *cyclic of trace type*. We say that two numbers k, k' are equivalent and write $k \sim k'$ iff $k' \equiv 2^a k \pmod{2^n - 1}$. Let $k \sim -1$. It follows from the definition that in this case $B_2^{(k)}$ is a standard B-set and $B_1^{(k)}$ is standard parabolic with $m = n$. The equivalence problem for the B-sets of cyclic trace type is solved by:

Theorem B. Let B and B' be B-sets of cyclic trace type of the same size.

- (a) Let $B = B_1^{(k)}$ and $B' = \overline{B}_2^{(k)}$. Then these B-sets are equivalent iff $k \sim 1$.
- (b) Let $B = B_i^{(k)}$ and $B' = B_i^{(k')}$ or $B' = \overline{B}_j^{(k')}$, $\{i, j\} = \{1, 2\}$. Equivalent are:
- (1) $B \sim B'$.
 - (2) $k \sim k'$. Moreover if $k \not\sim 1$ also $B' = B_i^{(k')}$.

The automorphism groups of the B-sets of cyclic trace type are described by the next theorem.

Theorem C. Let $B = B_i^{(k)}$ be a B-set of cyclic trace type in $V = V(2n, 2)$ and assume $k \not\sim -1$. Set $K = \text{Aut}(B)$. Then V contains a n -dimensional, K -invariant subspace U . Moreover $K = QL$, $Q \cap L = 1$, with $Q = O_2(K) = \{x \in K | x_U = 1_U, x_{V/U} = 1_{V/U}\}$. $L \simeq Z \cdot \langle t \rangle$ is the semidirect product of the group Z isomorphic to the multiplicative group of F with the group $\langle t \rangle$ where t induces the Frobenius automorphism on Z . The group Q has a decomposition $Q = X \oplus Y \oplus T$ into L -invariant subgroups such that the following holds:

- (a) Assume $n \neq 6$ Then there is at most one $a \in \{0, \dots, n-1\}$ such that $|(F^*)^{2^a k - 1}|$ divides some $2^c - 1$, $1 \leq c \leq n-1$. In that case choose c as small as possible. Then $|T| = 2^{c(d-1)}$ where $n = cd$. In the case $n = 6$ one has either $T = 1$ or $|T| = 2^7$ and $k \sim 11$ or $k \sim 23$.
- (b) $Y \neq 1$ iff there exists an $a \in \{0, \dots, n-1\}$ with $k \sim 1 - 2^a$. In this case a is uniquely determined and $|Y| = 2^n$. Moreover $T = 1$ and $|X| = 2^n$ if $k \not\sim 1$ and $|T| = 2^{n-1}$ and $X = 1$ if $k \sim 1$.
- (c) $|X| = 2^{\ell n}$ where ℓ is the number of pairs $\{a, b\} \subseteq \{0, \dots, n-1\}$ with $1 - 2^a k \sim 1 - 2^b k$.

Indeed statement (c) makes sense as there do not exist triples $\{a, b, c\} \subseteq \{0, \dots, n-1\}$ with $1 - 2^a k \sim 1 - 2^b k \sim 1 - 2^c k$ (see (2.12.a)). The explicit action of L on Q is given in (5.4). Theorems B and C will be proved in section 5.

In section 6 we classify the B-sets admitting $\text{Aut}(B)[V]$ as a rank 3 group of automorphisms of the associated symmetric design $\mathbf{D}(B)$. A consequence of [De2] is that if $\text{Aut}(B)[V]$ acts primitively as a rank 3 group then B is a standard B-set. We now allow also an imprimitive action and prove:

Theorem D. *Let $B \subseteq V = V(2n, 2)$, be a B-set such that $\text{Aut}(B)[V]$ acts as a rank 3 group on V . Then one of the following holds:*

- (a) B is standard.
- (b) B is standard parabolic of degree n .
- (c) B is special parabolic.
- (d) B is sporadic parabolic.
- (e) $B = B_i^{(k)}$ is of cyclic trace type and $k \sim 1 - 2^a$, a suitable a .

This result implies a classification of symmetric designs which admit a rank 3 group of automorphisms with a normal, elementary abelian, regular 2-subgroup.

In the last section we discuss computational aspects of the equivalence and automorphism problem.

An appendix contains a few results of general nature. First we determine subgroups of $\text{GL}(2n, 2)$ which contain a semiregular cyclic subgroup of order $2^n - 1$. Important are some unpublished results of P. Sin about the degree 1-cohomology of the groups $G_2(2^m)$.

Our group theoretic notations follow the usual conventions (see [As1] for instance) but note that $X^{(1)}$ stands for the commutator group of X .

2 Notation and preliminary results.

In this sections we start with some facts and some notations for B-sets. We add results about group representations and 1-cohomology and some number theoretic observations. The reader may continue after the introductory material about B-sets with section 3 and skip back whenever it is necessary.

In the sequel the letter B usually stands for a B-set and $\overline{B} = V - B$ will be the complementary B-set. The letter K will stand for a subgroup of $\text{Aut}(B)$ and by $H \leq \text{GL}(V)$ we denote the stabilizer of 0 in the semi-direct product $G = K[V]$. Then H and K are two complements of $[V]$ in G . Hence there is a uniquely determined 1-cocycle $c = c_B : H \rightarrow V$ such that $K = \{h[c(h)] \mid h \in H\}$ and the map $\kappa : H \rightarrow K$, $h \mapsto h\kappa = h[c(h)]$ is an isomorphism.

As before $\Theta = \Theta^+ = x_1x_{2n} + x_2x_{2n-1} + \dots + x_nx_{n+1}$ denotes the usual quadratic form which makes V into a nondegenerate orthogonal space of type $V^+(2n, 2)$. We denote the associated symplectic bilinear form by $\phi(x, y)$. We recall that the set $B^0 = I(V)$ of isotropic vectors in V and the anisotropic vectors \overline{B}^0 form B-sets of sizes $2^{n-1}(2^n + 1)$ and $2^{n-1}(2^n - 1)$ respectively. Up to equivalence we call these B-sets *standard*. In this case $K^0 = \text{Aut}(B^0) \simeq$

$\mathrm{Sp}(V, \phi) \simeq \mathrm{Sp}(2n, 2)$ [Ka1]. Analogously to κ and c we define $\kappa^0 : H^0 = K^0[V]_0 \rightarrow K^0$ and a 1-cocycle c^0 by $H^0 \ni h \mapsto h\kappa^0 = h[c^0(h)]$.

One knows that for any function $g = g(x_{n+1}, \dots, x_{2n})$ the function $f = \Theta + g$ is a bent function [Di2; thm. 10]. We give another description via B-sets:

(2.1) Lemma. *Let $V = V^+(2n, 2)$ be an nondegenerate, $2n$ -dimensional, orthogonal $\mathrm{GF}(2)$ -space of $(+)$ -type and let $V = U \oplus U'$ be a decomposition with totally singular spaces. For $v \in U'$ set $\mathcal{U}_v = \{U \cap \langle v \rangle^\perp, U - \langle v \rangle^\perp\}$, and set $\mathcal{U} = \bigcup_{v \in U'} \mathcal{U}_v$. Let $\sigma : U' \rightarrow \mathcal{U}$ be a map such that $\sigma(v) \in \mathcal{U}_v$. Then*

$$B_\sigma = \bigcup_{v \in U'} \sigma(v) + v$$

is a B-set.

Proof. For convenience we write Θ in the equivalent form $\Theta(x) = x_1 x_{n+1} + \dots + x_n x_{2n}$. We denote by U the subspace of vectors whose entries in positions $n+1, \dots, 2n$ are 0 and by U' the subspace of vectors whose entries in positions $1, \dots, n$ are 0. Let g be any function on U' . For $u \in U$, $v \in U'$ we have $g(u+v) = g(v)$ and $(\Theta + g)(u+v) = u \cdot v + g(v)$. If $v \neq 0$ then $\Theta + g$ vanishes on one of the sets in \mathcal{U}_v and has value 1 on the other. Moreover $\Theta + g$ either vanishes on U or has constant value 1. This shows that $\Theta + g$ has a B-set of type B_σ . Since there are 2^{2^n} functions g and 2^{2^n} sets B_σ the lemma follows.

Remark. For any B-set of type B_σ the automorphism group contains $O_2(K_U^0) \simeq O_2(\mathrm{Sp}(V, \phi)_U)$ as this group not only fixes every coset of U in V but also both sets in \mathcal{U}_v , $v \in U'$.

(2.2) Lemma. *Let B be a B-set in $V = V(2n, 2)$ and $\alpha \in N_{\mathrm{GL}(V)}(B)$ be of odd order > 1 . Assume that α acts fixed-point-freely on B . Then $C_V(\alpha) = 0$.*

Proof. If $|B| = 2^{n-1}(2^n + \epsilon)$, $\epsilon = \pm 1$ then $|\alpha|$ divides $2^n + \epsilon$. Take $v \in C_V(\alpha)$ then α normalizes $B \cap (v + B)$. If $v \neq 0$ then $|\alpha|$ would divide $2^{n-1} + \epsilon$, a contradiction.

Remark. Suppose $Z \leq \mathrm{Aut}(B)_0$ and $V = U \oplus U'$ is a decomposition into irreducible nonisomorphic n -dimensional Z -modules. Assume $U \subseteq B$ or $U \cap B = \emptyset$. Then:

(E) $C_{\mathrm{Aut}(B)_0}(Z)$ contains no elementary abelian p -group A of order p^2 , p odd.

By assumption A fixes U and U' and we have an element $1 \neq x \in A$ with $C_V(x) = U$. Thus x acts semiregularly on B or \overline{B} which is in conflict with (2.2). We refer to this application as argument (E).

Results about Group Representations

(2.3) Let X be a group and U, W be $F[X]$ -modules, $F = \mathrm{GF}(q)$, $q = p^f$, p a prime. Then X acts on $\mathrm{Hom}(U, W) = \mathrm{Hom}_{\mathrm{GF}(p)}(U, W)$ by $u(\sigma \cdot g) =$

$ug^{-1}\sigma g$; $u \in U$, $g \in G$, $\sigma \in \text{Hom}(U, W)$. Let φ be the Frobenius automorphism of F . Denote by $H_i(U, W)$ the φ^i -semilinear maps from U to W . Then (see [Be])

$$\text{Hom}(U, W) = \bigoplus_{i=0}^{f-1} H_i(U, W) \simeq \bigoplus_{i=0}^{f-1} U^* \varphi^i \otimes_F W \simeq \bigoplus_{i=0}^{f-1} U^* \otimes_F W \varphi^i$$

where M^* denotes the dual module of M and $M\varphi^i$ is the twist of the $F[X]$ -module M by φ^i .

In applications in the succeeding sections we will consider $X \leq \text{GL}(V)$, $V = V(2n, 2)$, and a X -invariant, n -dimensional subspace U . Assume $n = ab$ and $U \simeq M_1$, $V/U \simeq M_2$ with $F[X]$ -modules M_i and $F = \text{GF}(2^b)$. Let E be the centralizer of the flag $0 \subset U \subset V$, i.e. $E = \{x \in \text{GL}(V) \mid x_U = 1_U, x_{V/U} = 1_{V/U}\}$. For $\sigma \in \text{Hom}(V/U, U)$ and $v \in V$ define $v\sigma' = v + (v + U)\sigma$. Then $\sigma \mapsto \sigma'$ defines an isomorphism of the X -module $\text{Hom}(V/U, U)$ onto the module E where X acts on E by conjugation. Hence

$$E \simeq \bigoplus_{i=0}^{f-1} M_2^* \varphi^i \otimes_F M_1 \simeq \bigoplus_{i=0}^{f-1} M_2^* \otimes_F M_1 \varphi^i$$

where $\text{Gal}(F) = \langle \varphi \rangle$. Also note that $X \cap E$ is the kernel of the action of X on E , i.e. X induces XE/E on E .

(2.4) Lemma. *Let V, U, E, X be as in (2.3). Assume further that one of the following holds $\overline{X} = X/E \simeq \text{SL}(a, 2^b)$, $ab = n$, $a > 1$; $\overline{X} \simeq \text{Sp}(2a, 2^b)^{(1)}$, $2ab = n$, $a > 1$; or $\overline{X} \simeq \text{G}_2(2^b)^{(1)}$, $6b = n$ and that $U \simeq M$, $V/U \simeq M^*$ where M is the natural \overline{X} -module. Set $M_i = M \otimes_{\text{GF}(2^b)} M\varphi^i$. Then E is the direct sum of the M_i , $0 \leq i \leq b-1$, and the following holds.*

- (a) *Let $i \neq 0, b/2$. Then M_i is an absolutely irreducible $\text{GF}(q)[\overline{X}]$ -module viewed as a $\text{GF}(2)[\overline{X}]$ -module and as $\text{GF}(2)[\overline{X}]$ -modules $M_i \simeq M_{b-i}$ but $M_i \not\simeq M_j$ for $j \neq i, b-i$.*
- (b) *Let $b = 2c$. Then M_c is the direct sum of two isomorphic, absolutely irreducible $\text{GF}(2^c)[\overline{X}]$ -modules viewed as $\text{GF}(2)[\overline{X}]$ -modules. The irreducible composition factor of M_c does not occur in M_j , $j \neq c$.*
- (c) *M_0 has a flag $0 \subset N_1 \subset N_2 \subset M_0$ of \overline{X} -submodules with $N_2/N_1 \simeq M\varphi \simeq M$, $N_1 \simeq \wedge^2(M)$ and $N_2 \simeq S^2(M)$. Let \overline{X} be linear or of G_2 -type. Then the smallest submodule of M_0 which covers the quotient M is N_2 .*

Proof. (a) As $\text{GF}(2)[\overline{X}]$ -modules one has

$$M_i = M \otimes M\varphi^i \simeq (M \otimes M\varphi^i)\varphi^{b-i} \simeq M\varphi^{b-i} \otimes M \simeq M \otimes M\varphi^{b-i} = M_{b-i}.$$

Consider M_i as a $\text{GF}(2)[\overline{X}]$ -module and tensor with the splitting field $\text{GF}(2^b)$. Then this module splits into the direct sum of the Galois conjugates of M_i as $\text{GF}(2^b)[\overline{X}]$ -modules (see [As1; (25.10), (26.2)]). By Steinbergs tensor product theorem these modules are pairwise nonisomorphic so that $\text{GF}(2^b)$ is the field of definition. This also implies $M_i \not\simeq M_j$ for $j \neq i, b-i$. Hence (a) holds.

(b) Since $(M \otimes M\varphi^c)\varphi^c \simeq M\varphi^c \otimes M \simeq M_c$ as $\text{GF}(2^b)[\overline{X}]$ -modules we see that $\text{GF}(2^c)$ is the field of definition of this module. Then $M_c \otimes_{\text{GF}(2)} \text{GF}(2^c)$ splits into the direct sum of the Galois conjugates of the $\text{GF}(2^c)[\overline{X}]$ -module M_c . Since $\dim_{\text{GF}(2)} M_c = 2c \cdot (\dim M)^2$ we conclude that as an $\text{GF}(2)[\overline{X}]$ -module M_c splits into two isomorphic irreducible modules.

(c) Let $N_2 = S^2(M)$ be the symmetric part of $M \otimes M$ which is generated by elements of the form $v \otimes w + w \otimes v$ and $v \otimes v$. The alternating part is the submodule $N_1 = \wedge^2(M)$ generated by the first type of elements. Then $\dim N_2 = \binom{n+1}{2}$, $\dim N_1 = \binom{n}{2}$ and $N_2/N_1 \simeq M\varphi \simeq M$ as $\text{GF}(2)[\overline{X}]$ -modules. It is well known that in the case of $\overline{X} \simeq \text{SL}(a, 2^b)$ the module N_1 is simple and N_2 indecomposable. In the case of $\overline{X} \simeq \text{G}_2(2^b)^{(1)}$ the module N_1 has $\text{GF}(2^b)$ -composition factors of dimension 1 and 14. However N_2 is the smallest module in $M \otimes M$ which has the quotient $M\varphi$ by theorem 4 of the appendix.

We keep the assumptions of the previous lemma and determine the composition factors of $S^2(V)$ and $\wedge^2(V)$.

(2.5) Lemma. *Let V, U, E, X be as in (2.3) and assume that $\overline{X} \simeq \text{SL}(a, 2^b)$, $n = ab$. Denote by E_1 the submodule of E isomorphic to $\wedge^2(V)$ (the module of alternating forms on V) and by E_2 the submodule isomorphic to $S^2(V)$ (the module of symmetric forms on V). Let M_i, N_j have the meaning as in (2.4). Then the following holds.*

(a) *If b is odd we have for $i = 1, 2$ the decomposition*

$$E_i = (M_0 \cap E_i) \oplus \bigoplus_{i>0} ((M_i \oplus M_{b-i}) \cap E_i)$$

and if $b = 2c$ we have

$$E_i = (M_0 \cap E_i) \oplus (M_c \cap E_i) \oplus \bigoplus_{i \neq 0, c} ((M_i \oplus M_{b-i}) \cap E_i).$$

Moreover $(M_i \oplus M_{b-i}) \cap E_1 = (M_i \oplus M_{b-i}) \cap E_2$; $i \neq 0, c$, and $M_c \cap E_1 = M_c \cap E_2$ are irreducible while $M_0 \cap E_1 = N_1$, $M_0 \cap E_2 = N_2$.

(b) *Let \widetilde{M} be the largest \overline{X} -submodule of $M_i \oplus M_{b-i}$, $i \neq 0, c$, or of M_c such that \widetilde{M} leaves invariant the N_2 -orbits on the cosets $U + v$, $v \in V - U$. Then $\widetilde{M} = (M_i \oplus M_{b-i}) \cap E_1$ or $\widetilde{M} = M_c \cap E_1$ respectively.*

Proof. (a) As $\text{GF}(2)[\overline{X}]$ -modules $\wedge^2(V)$ is isomorphic to $V \otimes V/S^2(V)$ while $S^2(V)/\wedge^2(V)$ is isomorphic to M as a $\text{GF}(2)[\overline{X}]$ -module [Gr; lemma 2]. By (2.4) the assertion follows.

(b) As $(M_i \oplus M_{b-i}) \cap E_1$ (or $M_c \cap E_1$) leaves the N_2 -orbits on nontrivial cosets of U in V invariant we have $(M_i \oplus M_{b-i}) \cap E_1$ or $M_c \cap E_1 \subseteq \widetilde{M}$. However as M_i is transitive on the coset we have equality.

We stay in the situation of the previous lemmas and consider the first cohomology of the \overline{X} -module E . We record two instances where $H^1(\overline{X}, E)$ gives a nontrivial contribution to $H^1(\overline{X}, E/E_2)$. This will be used for the construction of B-sets of special and sporadic parabolic type.

(2.6) Lemma. *Let V, U, E, X be as in (2.5).*

(a) *Assume $\overline{X} \simeq \mathrm{SL}(3, 2^b)$, $n = 3b$, $b > 1$. Then $H^1(\overline{X}, E/E_2)$ is nontrivial.*

(b) *Assume $\overline{X} \simeq \mathrm{G}_2(4)$, $n = 12$. Then $H^1(\overline{X}, E/E_2)$ is nontrivial.*

Proof. (a) By [Be; thm. (3.2)] $H^1(\mathrm{SL}(3, 2^b), M_i)$ is nontrivial iff $i = 1$ or $b - 1$. Apply (2.5). (b) follows by (2.5) and Sin's theorem 4 (b) of the appendix.

Remark. Let $Y \simeq \mathrm{SL}(3, F)$ or $\mathrm{G}_2(F)$ with $F = \mathrm{GF}(2^b)$, $n = 3b$ or $F = \mathrm{GF}(4)$, $n = 12$. Let $M = M_i$, $i = 1, b - 1$ be as above and set $A = \mathrm{Gal}(F)$. Then M is a $\mathrm{GF}(2)[YA]$ -module. Let X be an arbitrary root subgroup of Y with respect to a fixed Cartan subgroup. The concrete computation of $H^1(Y, M)$ shows that one can choose a cocycle $c \in C^1(Y, M) - B^1(Y, M)$ such that c induces an A -isomorphism of X on to a one-dimensional subspace in $C_M(X)$. Then A normalizes the group $\{xc(x)|x \in X\}$ and thus $\{yc(y)|y \in Y\}$. Therefore $H^1(YA, M) \neq 0$.

The next lemma is required for the construction of twisted parabolic B-sets.

(2.7) Lemma. *Let W be a $2n$ -dimensional, nondegenerate symplectic vector space over $\mathrm{GF}(q)$ with respect to $(\ , \)$. Denote by $G = \mathrm{Sp}(W)$ the associated symplectic group and assume $n = ab$. Then there exists an element $z \in \mathrm{GL}(W)$, $|z| = q^b - 1$ such that the following holds:*

$$C_G(z) = \{x \in G \mid (vzx, wzx) = (vz, wz); v, w \in W\} \simeq \mathrm{Sp}(2a, q^b)$$

Proof. Choose a symplectic basis $\mathcal{B} = \{v_1, \dots, v_n, w_1, \dots, w_n\}$, i.e. the $\{v_i, w_i\}$ are pairwise orthogonal hyperbolic pairs with $(v_i, w_i) = 1$. Take $z_0 \in \mathrm{GL}(b, q)$ with $|z_0| = q^b - 1$ and $z_0^t = z_0$ (see [Ba]). Then $F = \langle z_0 \rangle \cup \{0\} \simeq \mathrm{GF}(q^b)$ is a subfield of the ring $\mathrm{GF}(q)^{b \times b}$. With respect to the above basis define $z = \mathrm{diag}(z_0, \dots, z_0)$. Then $C = C_{\mathrm{GL}(W)}(z)$ is the set of invertible $2a \times 2a$ -block matrices with entries in F . Hence $C \simeq \mathrm{GL}(2a, q^b)$. The matrix $x = (x_{ij}) \in C$, $x_{ij} \in F$ lies in $C_G(z)$ iff $x\Gamma x^t = \Gamma$, where

$$\Gamma = \begin{pmatrix} 0 & 1_{n \times n} \\ -1_{n \times n} & 0 \end{pmatrix}$$

is the Gram matrix with respect to \mathcal{B} . This implies $C_G(z) \simeq \mathrm{Sp}(2a, q^b)$. Define a new symplectic form on W by

$$[v, w] = (vz, wz).$$

The Gram matrix of this new form with respect to \mathcal{B} has the form

$$\Gamma_0 = z\Gamma z^t = \begin{pmatrix} 0 & J \\ -J & 0 \end{pmatrix},$$

where $J = \mathrm{diag}(z_0^2, \dots, z_0^2)$ is a $2a \times 2a$ -block matrix. If $x \in G$ leaves the form $[\ , \]$ invariant we have $x\Gamma x^t = \Gamma$ and $x\Gamma_0 x^t = \Gamma_0$. Therefore $\Gamma_0\Gamma^{-1} = z^2$ commutes with x and all assertions follow.

The next two results deal with the possibility of a nonsplit group extension inside a split group extension. These observations will be used in the proof of theorem D.

(2.8) Lemma. *Let X be a group and V a $F[X]$ -module, F a field.*

(a) *Let $G = XV$ denote the semidirect product of X with V and let $H \leq G$ be a subgroup with $G = HV$ and set $U = H \cap V$.*

(1) *Suppose $V = W \oplus T$ is a X -decomposition such that $U = (U \cap W) \oplus (U \cap T)$ and T is completely reducible. Then V has a complement Y in G with $Y \leq HW$ and H has a subgroup $H_1 \leq YW$ with $H_1U = H$ and $H_1 \cap V \leq U \cap W$.*

(2) *Suppose H does not split over U . Then the complements H/U and XU/U of V/U in G/U are not conjugate. In particular $H^1(X, V/U) \neq 0$.*

(b) *Let V be an indecomposable X -module which is the extension of F by a simple module W or the extension of W by F . Assume $\dim H^1(X, W) = 1$ and that $\text{Hom}(X/X^{(1)}, F)$ is trivial. Then $\dim H^1(X, V) = 0$.*

Proof. (a.1) Let $T = T_0 \oplus T_1$, $T_0 = U \cap T$ be a X -decomposition. For $h \in H$ there exist $x \in X$, $w(x) \in W$, $t_i(x) \in T_i$, with $h = x(w(x) + t_0(x) + t_1(x))$. Set $Y = \langle xt_1(x) \mid x \in X \rangle \leq HW \cap XT_1$. Then $Y \cap V \leq (HW \cap V) \cap (XT_1 \cap V) \leq (W \oplus T_0) \cap T_1 = 0$ and $H_1 = \langle x(w(x) + t_1(x)) \mid x \in X \rangle = \langle yw(x) \mid y = xt_1(x) \in Y \rangle \leq H$. Then $H_1 \cap V \leq (H \cap V) \cap (YW \cap V) \leq U \cap W$.

(a.2) Suppose $v \in V$ with $XU/U = H^v/U$. Then $XU = H^v$ or $X^{v^{-1}}U = H$ and $X^{v^{-1}}$ is a complement of U in H , a contradiction.

(b) Assume first that the socle of V is W . For $v \in V$ define $c(v) : X \rightarrow V$ by $c(v)(x) = v - vx$. Then $c(v)$ is a coboundary and $c : V \rightarrow B^1(X, V)$ is a surjection onto the space of 1-coboundaries. Next we observe that $C^1(X, W)$ and $C^1(X, V)$ are canonically isomorphic: Let f be a cocycle from X into V . The composition with the canonical epimorphism from V onto V/U is a homomorphism. By assumption this map is trivial, i.e. $f \in C^1(X, W)$. By definition $c(W) = B^1(X, W)$ and if $v \in V - W$ then as V is indecomposable $c(v) \notin B^1(X, W)$. As $\dim H^1(X, W) = 1$ we see that $c : V \rightarrow C^1(X, W)$ is a surjection. Now we have $B^1(X, V) = C^1(X, W) = C^1(X, V)$ and therefore $\dim H^1(X, V) = 0$. Using dual modules we also have $\dim H^1(X, V) = 0$ if the socle of V is F .

(2.9) Lemma. *Let V be a $2n$ -dimensional $\text{GF}(2)[X]$ -module, $n \geq 5$, and U a n -dimensional submodule. Let $Q = O_2(X) = \{x \in X \mid x_U = 1_U, x_{V/U} = 1_{V/U}\}$ be the 2-radical and $X/Q \simeq \text{SL}(a, 2^b)$, $n = ab$, $a \geq 2$, or $X/Q \simeq \text{G}_2(2^b)^{(1)}$, $n = 6b$, and assume that U and V/U are faithful $\text{GF}(2)[X/Q]$ -modules. Then X splits over Q .*

Proof. Let E be as before the centralizer of the chain $0 \subset U \subset V$ in $\text{GL}(V)$. Then $Q = X \cap E$ and $G = XE$ is the semidirect product of E with a group $Y \simeq \overline{X} = X/Q$. Set $W = V/U$ and consider U as the natural $F[\overline{X}]$ -module, $F = \text{GF}(2^b)$, viewed as a $\text{GF}(2)[\overline{X}]$ -module. Now $U \simeq W$ or W^* and $E \simeq$

$\oplus_i W^* \otimes U \varphi^i$ where φ is the Frobenius automorphism. Set $M = M_0 = W^* \otimes U$. Then E/M is completely reducible and hence by (2.8.a.1) there exists a subgroup $X_1 \leq X$ with $X = X_1 Q$ and $X_1 \cap E \leq M$. Replacing X by X_1 we may assume $Q \leq M$ and $X \leq YM$.

Case $\bar{X} \simeq \text{SL}(a, 2^b)$. Assume first $U \simeq W$. Then $M \simeq F \oplus A$ if a is odd and if a is even then M is a uniserial, indecomposable module with composition factors F, A, F where A denotes the adjoint module (see [Be] or [JP]). If a is odd (2.8.a.1) implies that X splits over Q . So assume that a is even. Then $\text{H}^2(\text{SL}(a, 2^b), F) = 0$ so that we may assume $X \cap Q \leq L$ where L is the second term of the socle series of M , i.e. $\text{soc}(L) = F$. We apply (2.8.a.2) with YM/F in the role of G , YF/F in the role of X , XF/F in the role of H , M/F in the role of V and L/F in the role of U . As $YL/L = XL/L$ we see that XF/F splits over L/F . So we may assume $X \cap Q \leq F$ and the assertion follows.

Now we assume $U \simeq W^*$ as $\text{GF}(2)[\bar{X}]$ -modules and we also assume $a > 2$ as $a = 2$ was covered before. As we have noted before M is uniserial with $0 \subset N_1 \subset N_2 \subset M$ such that $N_1 \simeq M/N_2 \simeq \wedge^2(U)$ and $N_2/N_1 \simeq S^2(U)/\wedge^2(U) \simeq U^{(2)} \simeq U$ as $\text{GF}(2)[\bar{X}]$ -modules. By [Be] $\text{H}^1(\text{SL}(a, 2^b), U) = 0$ and $\text{H}^1(\text{SL}(a, 2^b), \wedge^2(U)) = 0$ so that X splits again by the same argument as before.

Case $\bar{X} \simeq \text{G}_2(2^b)^{(1)}$. The module $M = U \otimes U = V(6, 2^b) \otimes V(6, 2^b)$ has the submodules $N_1 = \wedge^2(U)$ and $N_2 = S^2(U)$. Then as M is selfdual $N_1 \simeq M/N_2 \simeq A \oplus F$ and $N_2/N_1 \simeq S^2(U)/\wedge^2(U) \simeq U^{(2)} \simeq U$ as $\text{GF}(2)[\bar{X}]$ -modules, where A is the 14-dimensional adjoint module (see the proof of thm. 4 of the appendix). By proposition 5 of the appendix $\text{H}^1(\bar{X}, A) = 0$ and of course $\text{H}^1(\bar{X}, F) = 0$. As $X \leq YM$ and M/N_2 is completely reducible we can assume by (2.8.a.1) that $Q \leq N_2$ and $X \leq YN_2$. If $Q = N_2$ we are done. If $Q \leq N_1$ then YN_1/N_1 and XN_1/N_1 are two complements of M/N_1 in YM/N_1 . By (2.8.b) these complements are conjugate. By (2.8.a.2) we see that X splits over Q .

We finish the group theoretic section with a technical lemma.

(2.10) Lemma. *Let V be a finite dimensional vector space over $\text{GF}(q)$ and $X \leq \text{GL}(V)$ such that V is the direct sum of n irreducible, isomorphic X -modules. Let V_0 be such a submodule and denote by X_0 the restriction of X to this submodule. Then $N_{\text{GL}(V)}(X)/C_{\text{GL}(V)}(X) \simeq N_{\text{GL}(V_0)}(X_0)/C_{\text{GL}(V_0)}(X_0)$.*

Proof. Take $y \in N_{\text{GL}(V)}(X)$. One has $C_{\text{GL}(V)}(X) \simeq \text{GL}(n, q^s)$ where $\text{End}_{X_0}(V_0) \simeq \text{GF}(q^s)$ and $C_{\text{GL}(V)}(X)$ acts transitively on the X -irreducible subspaces of V . Norming if necessary y with an element from $C_{\text{GL}(V)}(X)$ we may assume that y fixes V_0 . Then the restriction y_0 of y to V_0 lies in $N_{\text{GL}(V_0)}(X_0)$ and as $X \ni x \mapsto x_0 \in X_0$ is bijective we conclude that the automorphism induced by y on X corresponds to the automorphism induced by y_0 on X_0 .

Number Theoretic Observations

These results are used in the proofs of theorem C and D. The first one has a routine verification.

(2.11) Lemma. *Let q be a prime power and $n \geq 2$ an integer. Then:*

$$(a) (q^n + q^{n-1} + \cdots + 1, q-1) = (n+1, q-1).$$

- (b) Set $M = q^{n-2} + q^{n-3} + \dots + 1$. Then $(q^n - 1, M) = (q - 1, n - 1)$.
- (c) $q^{n-r} - 1 \equiv q^{n-r+1}M(q^r - 1) \pmod{q^n - 1}$ for $1 \leq r \leq n - 1$.
- (d) $1 - q^{n-r+1}M \equiv q^{n-r}(1 - q^{r+1}M) \pmod{q^n - 1}$ for $1 \leq r \leq n - 1$.

(2.12) Lemma. Let k be a unit modulo $N = 2^n - 1$.

- (a) Suppose $1 - k \equiv 2^a(1 - 2^b k) \equiv 2^x(1 - 2^y k) \pmod{N}$ with $0 \not\equiv b \pmod{n}$. Then $y \equiv 0$ or $b \pmod{n}$.
- (b) Suppose $k \equiv 2^{-a}(1 - 2^b) \pmod{N}$ with $0, 1, -1 \not\equiv b \pmod{n}$. If $1 - 2^x k \equiv 2^y(1 - 2^z k) \pmod{N}$ and $x \not\equiv z \pmod{n}$ then (x, z) or $(z, x) \equiv (a+1, a-b)$ modulo n .
- (c) Assume $(1 - 2^a k)(1 - 2^c) \equiv 0 \pmod{N}$ for a divisor c of n , $c < n$. Then the equation $1 - 2^a k \equiv 2^x(1 - 2^y k) \pmod{N}$ has for y only the solution $y \equiv a \pmod{n}$.
- (d) Suppose $1 - 2^a \equiv 2^b \pmod{N}$ and $(1 - 2^x k)(2^y - 1) \equiv 0 \pmod{N}$ for a divisor $y < n$ of n . Then $k \equiv -2^\ell \pmod{N}$, ℓ suitable.

Proof. (a) As

$$(2^a - 1)(2^{x+y} - 1) \equiv (2^{a+b} - 1)k(2^{x+y} - 1) \equiv (2^{a+b} - 1)(2^x - 1)$$

we get

$$2^{a+z} + 2^x + 2^c \equiv 2^{c+x} + 2^z + 2^a$$

where $c \equiv a + b$ and $z \equiv x + y$ modulo n . Since $a \not\equiv c$ modulo n we get from [De1; (2.3)] the assertion.

(b) As $y \equiv 0$ implies $x \equiv z$ we have $y \not\equiv 0$. Replacing in the second equation of (b) k by $2^{-a}(1 - 2^b)$ we obtain two expressions for some positive integer M :

$$M = 2^{x-a+b} + 2^{y+z-a} + 1 = 2^{y+z-a+b} + 2^{x-a} + 2^y$$

where exponents are reduced modulo n .

Assume first that the 2-adic expansion of M has three terms. Since $y \neq 0$ we have $x - a = 0$ or $y + z - a + b = 0$. In the first case $x \equiv z \equiv a \pmod{n}$, which is a contradiction. In the second case we obtain $x - a \equiv -b$ and $y \equiv x - a + b$ modulo n . But then $y \equiv 0$, a contradiction.

Assume next that M has a 2-adic expansion with two terms. We have $y + z - a = 0$, $x - a + b = 0$ or $y + z - a = x - a + b$. We treat only the second case, the other cases are similar. Here:

$$2^{y+z-a} + 2 = 2^{y+z-a+b} + 2^{-b} + 2^y$$

and the right side reduces to two terms. If $-b \equiv y$ then $z - a = y + z - a + b \equiv 1$ so that $x \equiv a - b$, $z \equiv a + 1$ follows. If $y \equiv y + z - a + b$ then $z \equiv a - b \equiv x$, a contradiction. $-b \equiv y + z - a + b$ leads to $z \equiv a - b \equiv x$, again a contradiction.

Finally assume that M is a 2-power. Then on both sides of the equation two exponents coincide while the third one exceeds this number by 1. Let $\{\alpha, \beta\}$ be the left duo and $\{\gamma, \delta\}$ the right duo. If $0 \in \{\alpha, \beta\}$ then $y \notin \{\gamma, \delta\}$. But then

$0 = x - a = y + z - a + b = y + z - a$ or $x - a + b$ giving a contradiction in each case. If however $0 \notin \{\alpha, \beta\}$ then $x - a \notin \{\gamma, \delta\}$ giving $x - a + b = y + z - a = y + z - a + b = y$, again a contradiction.

(c) Rewrite the second equation in (c) as $1 - 2^y k \equiv 2^{n-x}(1 - 2^a k) \pmod{N}$. Then:

$$\begin{aligned} 0 &\equiv 2^{n-x}(1 - 2^a k)(1 - 2^c) \equiv (1 - 2^y k)(1 - 2^c) = \\ &= (1 - 2^{y-a} 2^a k)(1 - 2^c) = (1 - 2^{y-a} + 2^{y-a} - 2^{y-a} 2^a k)(1 - 2^c) \\ &= 2^{y-a}(1 - 2^a k)(1 - 2^c) + (1 - 2^{y-a})(1 - 2^c) \equiv (1 - 2^{y-a})(1 - 2^c) \pmod{N} \end{aligned}$$

By Zsigmondys theorem $y \equiv a \pmod{n}$ if $n \neq 6$ while the case $n = 6$ follows by inspection.

(d) is proved by similar arguments as (c).

(2.13) Lemma. *Set $N = 2^n - 1$.*

(a) *Suppose $m = 2^a + 2^b + 2^c + 2^d = 2^\alpha + 2^\beta + 2^\gamma + 2^\delta$ with exponents between 0 and $n - 1$ such that $\alpha \neq b, c, d$; $\beta \neq a, c, d$; $\gamma \neq a, b, c$ and $\delta \neq a, b, c$. Then one of the following holds:*

(1) $a = \alpha, b = \beta, c = \gamma, d = \delta$.

(2) *The 2-adic expansion of m has two terms. Up to a permutation of (a, \dots, d) we have $a = b, c = a + 1$ and $m = 2^{a+2} + 2^d$. Moreover there is a permutation $(\varepsilon, \rho, \sigma, \tau)$ of $(\alpha, \beta, \gamma, \delta)$ such that $\sigma = \tau, \varepsilon = \sigma + 1$ and $m = 2^{\sigma+2} + 2^\rho$ and $\rho = c + 1, d = \varepsilon + 1$.*

(b) *Suppose $1 - k \equiv 2^a(1 - 2^b k) \pmod{N}$ with $0 \not\equiv a, b, a + b \pmod{n}$ and $(a, n) = (a + b, n) = 1$. If $1 - 2^x k \equiv 2^y(1 - 2^z k) \pmod{N}$, $x \not\equiv z \pmod{n}$, then $k \equiv -2^\ell \pmod{N}$, ℓ suitable or $(x, z) = (0, b)$ or $(b, 0)$.*

Proof. (a) The assertion is obvious if the 2-adic expansion of m has 4 terms. If the 2-adic expansion of m has one term then wlog. $a = b, c = a + 1, d = c + 1$ and $m = 2^{d+1} = 2^{c+2}$ or $a = b = c = d = c, m = 2^{a+2}$. Similarly $m = 2^{\rho+1} = 2^{\tau+2}$ or $2^{\rho+2}$ with $\rho, \tau \in \{\alpha, \dots, \delta\}$. Then by our assumptions on both sides only the first alternative occurs. Hence $\rho = d$ and (1) follows by induction.

Assume that the 2-adic expansion of m has three terms. Wlog. $a = b$ and $m = 2^{a+1} + 2^c + 2^d$. Similarly there is a permutation $(\varepsilon, \rho, \sigma, \tau)$ of $(\alpha, \beta, \gamma, \delta)$ such that $\sigma = \varepsilon$ and $m = 2^{\sigma+1} + 2^\tau + 2^\rho$. If $\sigma = \varepsilon = a = b$ we get (1) again. Otherwise - choosing the notation suitably - $m = 2^{a+1} + 2^c + 2^d = 2^\alpha + 2^\beta + 2^{\gamma+1}$ which contradicts the assumptions.

Assume finally that the 2-adic expansion of m has two terms. Up to symmetry we have (1) $a = b, c = d, m = 2^{a+1} + 2^{c+1}$ or (2) $a = b, c = a + 1, m = 2^{c+1} + 2^d$. Assume $\sigma = \tau, \rho = \varepsilon, m = 2^{\varepsilon+1} + 2^{\sigma+1}$. If we have case (1) then wlog. $a = \varepsilon, c = \sigma$ and (1) follows. If however (2) holds we get $c = \varepsilon = \rho$ or $c = \sigma = \tau$, a contradiction. By symmetry we conclude $m = 2^{c+1} + 2^d = 2^{\varepsilon+1} + 2^\rho$ with $\sigma = \tau, \varepsilon = \sigma + 1$. If $c = \varepsilon, d = \rho$ we have (1) while the remaining case gives (2).

(b) is verified again by considering 2-adic expansions. We omit the straightforward but lengthy computations.

(2.14) Lemma. *Let $n = ds, d$ odd, such that $\{q, d\}, q = 2^s$ is a Dickson pair [Lü; p. 33]. Then:*

- (a) Every prime which divides $2^n - 1$ divides $(2^n - 1)/d$ too.
- (b) Assume $(k, (2^n - 1)/d) = 1$ and $2^b \equiv 1 - 2^a k \pmod{(2^n - 1)/d}$, $0 \leq a, b < n$. Then:
- (1) $(b, n) = 1$.
 - (2) If $2^c \equiv 1 - 2^y k \pmod{(2^n - 1)/d}$, $0 \leq c, y < n$ then $c = b$ and $y = a$.

Proof. (a) Every prime which divides d also divides $q - 1$ and d divides $(2^n - 1)/(q - 1)$ too [Lü; p. 32, (4)]. The claim follows.

(b) Assume $(b, n) \neq 1$. Then there exists a prime t which divides $(2^b - 1, 2^n - 1)$ and therefore $(2^n - 1)/d$ by (a). Hence $2^a k \equiv 1 - 2^b \equiv 0 \pmod{t}$, a contradiction. Thus (1) holds.

Assertion (2) is verified again by considering 2-adic expansions. These calculations are omitted too.

3 Constructions.

We describe series of B-sets whose automorphism groups will be computed in the next two sections. Although we are convinced that these series are included in the constructions of Dillon, Rothaus and others we take the liberty to present them again in a fashion suitable for our computations.

(3.1) Parabolic B-sets. Let $\Theta = \Theta^\epsilon$ (use the notation of the introduction) be a quadratic form on $V = V(2n, 2)$ and U a totally singular subspace of dimension m - say $U = \langle e_1, \dots, e_m \rangle$. In the following cases $\epsilon = +$ except case (b) where ϵ is arbitrary. Set $W = U^\perp$.

(a) *Standard parabolic type.* Denote by $I(V)$ the set of isotropic and by $A(V)$ the set of anisotropic vectors in V and set $B = (I(V) \cap W) \cup (A(V) \cap (V - W))$. Then $f_B = \Theta \chi_W + (\Theta + 1) \chi_{V-W} = \Theta + \chi_{V-W}$ is the boolean polynomial whose zeros are B . Clearly $\chi_{V-W} = 1 + (x_{2n-m+1} + 1)(x_{2n-m+2} + 1) \cdots (x_{2n} + 1)$. Hence f_B is a bent function (see [Di2, Thm. 10]) and B a B-set of size $2^{n-1}(2^n + 1)$. As $\deg f_B = \max(\deg \Theta, \deg \chi_{V-W})$ B is standard iff $m \leq 2$. In any case $P = H_U^0$ is a maximal parabolic subgroup of $H^0 = \text{Sp}(V)$. The corresponding subgroup K_U in K^0 is a subgroup of $K = \text{Aut}(B)$. Later we will show $K = K_U$ if $m > 2$. We call these B-sets and their complements *standard parabolic of degree m* .

(b) *Twisted parabolic type.* Assume $\dim U = m < n - 1$. Then Θ induces on W/U a quadratic form such that W/U becomes a space of type $V^\epsilon(2(n - m), 2)$. Let $D \subseteq W$ be a set satisfying the following properties:

- (1) $D + U = D$, (2) D/U is a B-set in W/U .

Define $B = B(D) = D \cup (I(V) \cap (V - W))$. We claim:

- (*) B is a B-set of size $2^{n-1}(2^n + 1)$.

This claim is verified below. The characteristic function of D is a boolean polynomial of the form $\chi_D = p(x_{m+1}, x_{m+2}, \dots, x_{2n-m})$ and has (as a B-set in W/U) degree $2 \leq \deg \chi_D \leq n - m$. Then we have for B the bent function:

$$f_B = \Theta \chi_{V-W} + p \chi_W = \Theta + (\Theta + p) \chi_W = \Theta + (\Theta + p)(x_{2n-m+1} + 1) \cdots (x_{2n} + 1)$$

Let Θ_1 be the sum of the monomials in Θ in the variables x_{m+1}, \dots, x_{2n-m} and set $\Theta_0 = \Theta - \Theta_1$. Then $f_B = \Theta_0 \chi_W + \Theta + (\Theta_1 + p) \chi_W$. If $\deg(\Theta_1 + p) = r \geq 1$ then $\deg(\Theta_1 + p) \chi_W = r + n - m$ and no monomial in $(\Theta_1 + p) \chi_W$ of degree $r + n - m$ occurs in $\Theta_0 \chi_W + \Theta$. Hence $\deg f_B \geq r + n - m$ and B is nonstandard if this number is larger than 2. We will always choose the set D as a linear transform of a standard B-set:

Assume $W = U \perp W_0$ with $W_0 = V^\epsilon(2(n-m), 2)$ and pick $T \in \text{GL}(W_0)$. Set $\tau = 1_U \oplus T$. It is easy to see that $D = (I(V) \cap W)\tau$ satisfies (1)-(2). Moreover B is nonstandard if $T \in \text{GL}(W_0) - \text{O}(W_0)$.

Assume now that $n - m = ab \geq b \geq 2$. By (2.7) we can choose $\tau = 1_U \oplus T$ in such a way that $C_{\text{Sp}(W_0)}(T) \simeq \text{Sp}(2a, 2^b)$. We say in this case that B is *twisted parabolic* with *parameters* m, b, ϵ . For this particular kind of twisted parabolic B-sets we will compute the automorphism group.

Verification of (*) in the case $\epsilon = 1$: Set $I = I(V)$, $A = A(V)$ and $I_1 = I \cap W$, $I_2 = I \cap (V - W)$. Note that for $D = I_1$ (i.e. $B = I = B^0$) assertion (*) is true. Take $0 \neq v \in V$.

Case 1. $v = u \in U$. Then

$$|B \cap (B + u)| = |D| + |I_2 \cap (I_2 + u)| = 2^{n-1}(2^{n-1} + 1)$$

as $|I_1| = |D|$.

Case 2. $v = w \in W - U$. Then

$$|B \cap (B + w)| = |D \cap (D + w)| + |I_2 \cap (I_2 + w)| = 2^{n-1}(2^{n-1} + 1)$$

by the same argument as in case 1.

Case 3. $v \in V - W$. Choose $u \in U$ with $(u, v) = 1$ and set $D_0 = D \cap \langle v \rangle^\perp$, $D_1 = D - D_0$. For a coset $x + U \subseteq D$ choose x such that $(x, v) = 0$. Then

$$x + U = (x + (U \cap \langle v \rangle^\perp)) \cup (x + (u + (U \cap \langle v \rangle^\perp)))$$

is a partition into sets of equal size. Hence $|D_0| = |D_1| = 2^{m-1}(2^{n-m-1}(2^{n-m} + 1))$. For $i = 0, 1$ define further $D_i^+ = \{x \in D_i \mid x + v \in I\}$ and $D_i^- = \{x \in D_i \mid x + v \in A\}$ and set $x_i = |D_i^+|$, $y_i = |D_i^-|$. Then $x_i + y_i = 2^{n-2}(2^{n-m} + 1)$ and $D_0^+ + u = D_1^-$, $D_0^- + u = D_1^+$, i.e. $x_0 = y_1$ and $x_1 = y_0$. Moreover

$$|B \cap (B + v)| = |I_2 \cap (D + v)| + |D \cap (I_2 + v)| + |I_2 \cap (I_2 + v)|$$

and $|I_2 \cap (D + v)| = |D \cap (I_2 + v)|$. Finally

$$|I_2 \cap (D + v)| = |D_0^+| + |D_1^+| = x_0 + x_1 = x_0 + y_0 = 2^{n-2}(2^{n-m} + 1).$$

As I is a B-set we have $|I_2 \cap (I_2 + v)| = 2^{n-1}(2^{n-1} + 1) - 2 \cdot 2^{n-2}(2^{n-m} + 1)$ and therefore $|B \cap (B + v)| = |I_2 \cap (I_2 + v)| + 2 \cdot |I_2 \cap (D + v)| = 2^{n-1}(2^{n-1} + 1)$.

(c) *Special parabolic type.* Assume $\dim U = n = 3b$. Set $E_2 = E \cap \text{Sp}(V)$ where E is the centralizer of the chain $0 \subset U \subset V$ in $\text{GL}(V)$ (compare with (2.5)) and let K_U^0 be the stabilizer of U in $K^0 = \text{Aut}(B^0)$. The 2-radical $Q = O_2(K_U^0)$ has the form $Q = \{x[c(x)] \mid x \in E_2\}$ with an epimorphism $c : E_2 \rightarrow U$. Set $U' = \langle u_{n+1}, \dots, u_{2n} \rangle$ where $\{u_1, \dots, u_{2n}\}$ is a symplectic basis. Let $X \leq K_{U,U'}^0$ be a subgroup isomorphic to $\text{SL}(3, 2^b)$. Pick $[\Phi] \in \text{Ext}_{\text{GF}(2)[X]}(V/U, U) \simeq H^1(X, E)$. Define $X_\Phi = \{x_\Phi \mid x \in X\} \simeq X$ by $vx_\Phi = vx + (vx + U)\Phi(x)$, $v \in V$. By (2.6) we can choose the 1-cocycle Φ in such a way that the restriction to E/E_2 is not a coboundary. X_Φ normalizes Q but $X_\Phi Q \not\leq K^0$. Now X_Φ is transitive on $V/U - 0$ and each coset $v + U$, $v \notin U$ splits into two Q -orbits. Thus either X_Φ is transitive on all Q -orbits in $V - U$ or X_Φ has precisely two orbits each intersecting a coset $v + U$ in one Q -orbit. However the first case can not occur as the stabilizer in $\text{SL}(3, F)$, $F = \text{GF}(2^b)$ of a nontrivial vector v in F^3 has no subgroup of index 2. Thus $X_\Phi Q$ has two orbits in $V - U$ which are B-sets by (2.1). We call these B-sets (and their complements) of *special parabolic type*. Now F^* has an action on V which commutes with the action of X . From [Be] one deduces that $\dim_F H^1(E/E_2) = 1$. Hence the type does not depend on the choice of $[\Phi]$ and the two orbits of X_Φ result (up to equivalence and complementation) in at most two B-sets. See also the more explicit remark after (6.8). Set $A = \text{Gal}(F)$. By the remark to (2.6) we see that even $AX_\Phi Q$ lies in the automorphism group of the constructed B-sets. Note that A fixes both $X_\Phi Q$ -orbits, as otherwise the Frobenius automorphism would interchange both orbits and act therefore fixed-point-freely on $V - U$ which is absurd.

(d) *Sporadic parabolic type.* Assume $\dim V = 12$. Define U' as in (c). Choose $X \leq K_{U,U'}^0$, $X \simeq \text{G}_2(4)$ and $[\Phi] \in \text{Ext}_{\text{GF}(2)[X]}(V/U, U)$ such that the restriction of $\Phi : X \rightarrow E/E_2$ is not a coboundary. The same arguments as (c) show that $X_\Phi Q$ has two orbit on $V - U$ which are B-sets and also that $X_\Phi Q \not\leq K^0$. We call these B-sets (and their complements) of *sporadic parabolic type*. Again as in (c) these B-sets depend up to equivalence not on $[\Phi]$ and $AX_\Phi Q$ lies in the automorphism group of the B-sets where $A = \text{Gal}(\text{GF}(4))$.

(3.2) B-sets of trace type. Identify $V = V(2n, 2)$ with F^2 , $F = \text{GF}(q)$, $q = 2^n$. Let $\alpha \mapsto \bar{\alpha}$ be any permutation of F^* and let $F_0 = \{\beta \in F \mid \text{tr } \beta = 0\}$ be the $\text{GF}(2)$ -subspace of elements with trace 0. Define $B_1 = \{(\alpha\beta, \bar{\alpha}) \mid \alpha \in F^*, \beta \in F_0\}$, *small trace type*, and $B_2 = B_1 \cup U$, $U = (1, 0)F$, *big trace type*. Then it is easy to see that B_1 and B_2 are B-sets of sizes $2^{n-1}(2^{n-1} - 1)$ and $2^{n-1}(2^{n-1} + 1)$ respectively. In fact it is also not difficult to see that these B-sets are of the type described by McFarland [McF]. We will only consider the case where $\alpha \mapsto \bar{\alpha}$ is an automorphism of the multiplicative group F^* , i.e. $\bar{\alpha} = \alpha^k$, $(k, 2^n - 1) = 1$. We see that the mappings $z(\alpha) : V \rightarrow V$, $(x, y) \mapsto (\alpha x, \alpha^k y)$ define automorphisms of the B_i 's. We therefore call these B-sets of *cyclic trace type* and denote them by the symbols $B_i^{(k)}$. Note that $\Gamma\text{L}(1, F) \simeq Z\langle t \rangle \leq \text{Aut}(B_i^{(k)})$ where Z is the group of the $z(\alpha)$'s and $(x, y)t = (x^2, y^2)$.

4 Proof of Theorem A.

We keep the general notations from the introduction of section 2. Moreover with the notation of (3.1) B denotes a B-set of parabolic type, $V = V(2n, 2)$ is an othogonal space with quadratic form Θ and $U = \langle e_1, \dots, e_m \rangle$ is a totally singular subspace with respect to Θ . This quadratic form is of (+)-type in all cases except the twisted parabolic case where also Θ can be of (-)-type. Then $V = U \oplus W_0 \oplus U'$ with a totally singular subspace $U' = \langle e_{2n-m+1}, \dots, e_{2n} \rangle$ and a nondegenerate $2(n-m)$ -dimensional subspace $W_0 = \langle e_{m+1}, \dots, e_{2n-m} \rangle$ which has the same type as V . The structure of $K = \text{Aut}(B)$ is closely related to $K_U^0 = H_U^0 \kappa^0$, the stabilizer of U in the automorphism group of a standard B-set B^0 . We describe the latter group. We have $H_U^0 = L_0 Q$ where the 2-radical $Q = O_2(H_U^0)$ is the centralizer of the chain $0 \subset U \subseteq U^\perp = W \subset V$ and L_0 is the stabilizer of U' in H_U^0 . Moreover $L_0 = L_1 \times L_2$ with $L_1 = C_{L_0}(W_0) \simeq \text{SL}(U)$ and $L_2 = C_{L_0}(U) \simeq \text{Sp}(W_0, \phi)$. Then $L_1 = L_1 \kappa^0 \leq K_U^0$. We will show $Q\kappa = Q\kappa^0$ and $H = K\kappa^{-1} = LQ$ with a group L isomorphic to a group between L_1 and $L_1 \times L_2$. Finally we do assume $n > 4$: For $n = 4$ theorem A can be verified by a computer calculation. Possible approaches for such a computations are described in the remark after (7.1).

(4.1) Lemma. *The centralizer of the chain $0 \subset U \subseteq U^\perp = W \subset V$ in K is $Q\kappa^0$, i.e. $Q \leq H$.*

Proof. Let \overline{Q} be this centralizer. By definition

$$B = \bigcup_{w \in W_0} ((w + U) \cap B) \cup \bigcup_{v \in U' - 0} ((v + W) \cap B)$$

and $(w + U) \cap B = w + U$ or \emptyset while $(v + W) \cap B = (v + W) \cap B^0$ or $(v + W) \cap \overline{B}^0$. Thus $Q\kappa^0$ fixes B , i.e. $Q\kappa^0 \leq \overline{Q}$. Any element in \overline{Q} fixes every coset $w + U$ and both sets in $\{(v + W) \cap B^0, (v + W) \cap \overline{B}^0\}$. Hence \overline{Q} fixes B^0 and thus $Q\kappa^0 \geq \overline{Q}$.

(4.2) Lemma. *Set $P = H_U$ Then:*

- (a) c maps P into W .
- (b) W is P -invariant. In particular $Q \trianglelefteq P$.
- (c) The P -modules U and V/W are dual with respect to the duality induced by ϕ .
- (d) $H_W = P$.

Proof. Set $\overline{\Theta} = f_B$.

(a) Assume $c(x) \in V - W$ for some $x \in P$. Then $ux\kappa = ux + c(x) \in V - W$ for $u \in U$. By definition of $\overline{\Theta}$ (in any case):

$$0 = \overline{\Theta}(u) = \overline{\Theta}(ux\kappa) = \overline{\Theta}(c(x)) + \phi(ux, c(x)).$$

However one can choose u such that $\overline{\Theta}(c(x)) \neq \phi(ux, c(x))$, a contradiction.

(b) We can assume $U \neq W$. Then we are in the standard parabolic or twisted parabolic case. Suppose $w \in W$, $x \in P$ but $wx \in V - W$. By (a) $wx + c(x) \in V - W$. Pick $u \in U$. Then:

$$\begin{aligned}
0 &= \overline{\Theta}(w) + \overline{\Theta}(u + w) \\
&= \overline{\Theta}(wx + c(x)) + \overline{\Theta}(ux + wx + c(x)) \\
&= \Theta(wx + c(x)) + \Theta(ux + wx + c(x)) \\
&= \Theta(ux) + \phi(ux, wx + c(x)) \\
&= \phi(ux, wx + c(x))
\end{aligned}$$

However ranging with u over U we see that the right side is not constant, a contradiction.

(c) Set $Q_0 = C_Q(W) = C_Q(V/U)$. Let $\mathcal{S} \subseteq \text{GF}(2)^{m \times m}$ be the set of symmetric matrices and $\mathcal{S}_0 = \mathcal{S}J_m$ where J_m is obtained from $\mathbf{1}_{m \times m}$ by reversing the order of the columns. Using the given basis we have an isomorphism $A : Q_0 \rightarrow \mathcal{S}_0$ and matrix representations $D_U : P \rightarrow \text{GL}(m, 2)$, $D_{V/W} : P \rightarrow \text{GL}(m, 2)$ such that $A(y^x) = D_{V/W}(x)^{-1}A(y)D_U(x)$ for $y \in Q_0$, $x \in P$. Note that the same assertion holds if we choose $x \in H_U^0$. From $\mathcal{S}_0 = D_{V/W}(x)^{-1}\mathcal{S}_0D_U(x)$ we conclude $D_{V/W}(x) = J_mD_U(x)^{-t}J_m$. The assertion follows.

(d) In this case we may assume that B is standard parabolic or twisted parabolic. $(w_1, w_2) \mapsto \overline{\phi}(w_1, w_2) = \overline{\Theta}(w_1 + w_2) + \overline{\Theta}(w_1) + \overline{\Theta}(w_2)$ defines an alternating form on W whose radical is U . A straightforward computation shows that this form is invariant under the action of H_W . The assertion follows.

(4.3) Lemma. *Let B be standard parabolic or twisted parabolic and $P = H_U$. Then:*

- (a) $C_P(U)/Q$ acts on W/U as a subgroup of $\text{Sp}(W_0, \phi)$.
- (b) $P = H_U^0$ in the standard parabolic case and $C_P(W/U) = L_1Q$ in the twisted parabolic case.

Proof. (a) With respect to the chosen basis of V we see that $y \in Q$ is represented by a matrix of the form

$$\begin{pmatrix} 1 & & & \\ A(y) & 1 & & \\ * & C(y) & 1 & \end{pmatrix}$$

with $A(y) = J_mC(y)^tJ_{m'}$, where $m' = 2(n - m)$ and J_k as in the proof of (4.2.c). $x \in C_P(U)$ is represented by a matrix of the form

$$\begin{pmatrix} 1 & & & \\ * & D(x) & & \\ * & * & 1 & \end{pmatrix}.$$

Thus $A(y^x) = D(x^{-1})A(y)$, $C(y^x) = C(y)D(x)$ and hence $C(y)D(x)J_{m'} = C(y)J_{m'}D(x)^{-t}$. As $C : Q \rightarrow \text{GF}(2)^{m \times m'}$ is an epimorphism with kernel $Q_0 = C_Q(W) = C_Q(V/W)$ we see that Q/Q_0 as a $C_P(U)$ -module is isomorphic to the direct sum of m copies of W_0 and $C_P(U)$ induces on W/U a subgroup of $\text{Sp}(W_0, \phi)$ since $J_{m'}$ is the Gram matrix of ϕ restricted to $W_0 \times W_0$.

(b) By definition $H_U^0 \leq P$ in the standard parabolic case and $L_1Q \leq C_P(W/U)$ in the twisted parabolic case. By (4.2) and (a) equality holds in both cases.

(4.4) Lemma. *Theorem A holds in the standard, special, and sporadic parabolic case.*

Proof. Let B first be standard parabolic. If $m \leq 2$ then $\deg f_B = 2$ and $B \sim B^0$ (see [Di2]). So assume $m \geq 3$. By (4.3) $H_U = H_U^0$ and $0 \subset U \subseteq U^\perp = W \subset V$ is the unique H_U -composition series. If $H = H_U$ we are done. Otherwise H would be irreducible by (4.2). We can apply a result of Mc Laughlin [McL] and conclude $H \simeq \text{Sp}(V)$ or $\text{SL}(V)$. But then by [De2] B is standard and $\deg f_B = 2$, a contradiction.

Let B now be special parabolic. Using the notation of (3.1.c) we know already that $K_0 = AX_\Phi Q\kappa^0$ lies in K . If H would not be irreducible then again with [McL] and [De2] we reach a contradiction. So $H = H_U$ (and $K = K_U$) and $Q = O_2(H)$. Set $H_0 = K_0\kappa^{-1}$. If $\overline{S} = E(H_0/Q)$ is not normal in H/Q we apply the result of Hering [He1, He2, Li2] and see that $H_1/Q = E(H/Q) \simeq \text{SL}(a, 2^c)$, $ac = n$ and $a > 3$. Since $X_\Phi \simeq \overline{S} \leq H_1/Q$ the nontrivial class $[\Phi] \in \text{Ext}_{\text{GF}(2)[\overline{S}]}(V/U, U)$ extends to the group ring $\text{GF}(2)[H_1/Q]$ which is in conflict with [Be]. Hence $\overline{S} \trianglelefteq H/Q$. Assume $H_0 < H$. As H_0/Q covers $\Gamma\text{L}(3, 2^b)/\text{GL}(3, 2^b)$ we would find an $h \in H$ such that h induces a nontrivial diagonal automorphism on \overline{S} by conjugation. But the nontrivial diagonal automorphisms act fixed-point-freely on $\text{Ext}_{\text{GF}(2)[\overline{S}]}(V/U, U)$, a contradiction.

Let B be finally sporadic parabolic. As before $H = H_U$. Set $K_0 = AX_\Phi Q\kappa$, $H_0 = K_0\kappa^{-1}$ and $\overline{S} = E(H_0/Q) \simeq X_\Phi \simeq \text{G}_2(4)$. If \overline{S} is normal in H_1/Q then $H = H_0$ and we are done. Otherwise by Herings theorem $\text{Sp}(6, 4)$, $\text{SL}(6, 4)$, $\text{Sp}(12, 2)$ or $\text{SL}(12, 2) \trianglelefteq H/Q$. In any case we have a subgroup $\text{SL}(2, 2^6)$ in H/Q . The proof of theorem D will show that B is either standard or standard parabolic, so that we have $H/Q \simeq \text{SL}(12, 2)$ anyway and again $[\Phi]$ would extend to a nontrivial class of $\text{Ext}_{\text{GF}(2)[H/Q]}(V/U, U)$ which is impossible.

(4.5) Lemma. *Theorem A holds twisted parabolic case.*

Proof. Set $P = H_U$. Let m, b, ϵ be the parameters of B and define a by $ab = n - m$. Set $\overline{\Theta} = f_B$. The restriction of $\overline{\Theta}$ to W is a quadratic form with radical U such that W_0 is a nondegenerate space of type ϵ . Let $\overline{\phi}$ be the polarisation of $\overline{\Theta}$ on W . First we claim:

$$(1) \quad \begin{aligned} \text{O}^\epsilon(2a, 2^b) &\simeq \text{O}(W_0, \Theta) \cap \text{O}(W_0, \overline{\Theta}) \leq C_P(U)/Q \\ &\leq \text{Sp}(W_0, \phi) \cap \text{Sp}(W_0, \overline{\phi}) \simeq \text{Sp}(2a, 2^b) \end{aligned}$$

By the observation in the proof of (4.2.d) and by (4.3.a) we have $C_P(U)/Q \leq \text{Sp}(W_0, \phi) \cap \text{Sp}(W_0, \overline{\phi})$ which is isomorphic to $\text{Sp}(2a, 2^b)$ by (2.7). On the other hand $L_2 \cap H^0 \simeq \text{O}^\epsilon(2(n - m), 2) \simeq \text{O}(W_0, \Theta)$ and by (2.7) $\text{O}(W_0, \Theta) \cap \text{Sp}(W_0, \overline{\phi}) = \text{O}(W_0, \Theta) \cap \text{O}(W_0, \overline{\Theta}) \simeq \text{O}^\epsilon(2a, 2^b)$. Since an element in $L_2 \cap H^0$ leaves Θ_W and $\overline{\Theta}_W$ invariant it even lies in $C_P(U) \cap K$ and (1) follows.

Let S be the subgroup in $\mathrm{GL}(V)$ which acts trivially on $U \oplus U'$ fixes W_0 and is isomorphic to $\mathrm{Sp}(W_0, \bar{\phi})$. Then there exists a unique 1-cocycle $\bar{c} : S \rightarrow W_0$ such that $\{s[\bar{c}(s)] \mid s \in S\}$ is the automorphism group of the (standard) B-set $B \cap W_0$. Let S_0 be the subgroup of S which corresponds to $\mathrm{Sp}(W_0, \phi) \cap \mathrm{Sp}(W_0, \bar{\phi})$. We claim.

(2) Let $m = 1$. Then $C_P(U)/Q \simeq \mathrm{Sp}(2a, 2^b)$.

For $x \in S_0$ we define $\bar{x} \in \mathrm{GL}(V)$ by $\bar{x}_W = x_W$ and $e_{2n}\bar{x} = e_{2n} + c^0(x) + \bar{c}(x)$. We check that $\bar{x}[\bar{c}(x)]$ lies in K . For $w \in W$ we have

$$\bar{\Theta}(w\bar{x}[\bar{c}(x)]) = \bar{\Theta}(wx + \bar{c}(x)) = \bar{\Theta}(w)$$

by definition of \bar{c} . Also $\Theta = \bar{\Theta}$ on $V - W$. Thus:

$$\begin{aligned} \bar{\Theta}((w + e_{2n})\bar{x}[\bar{c}(x)]) &= \bar{\Theta}(wx + e_{2n} + c^0(x)) = \Theta((w + e_{2n})x[c^0(x)]) \\ &= \Theta(w + e_{2n}) = \bar{\Theta}(w + e_{2n}). \end{aligned}$$

Together with (1) we get claim (2).

(3) Let $m > 1$. Then $C_P(U)/Q \simeq \mathrm{O}^\epsilon(2a, 2^b)$.

Assume $C_P(U)/Q \simeq \mathrm{Sp}(2a, 2^b)$. Use (4.3.b) and choose $t \in L_1$, $|t| = 2^m - 1$. Note that $t \in H$. If $x \in C_P(U)$ then $[x, t]$ centralizes the chain $0 \subset U \subset W \subset V$, i.e $[x, t] \in Q$. Then Glaubermans fixed-point-theorem implies $C_P(U) = Q \cdot C$ with $C = C_{C_P(U)}(t)$. Pick $x \in C$. Then x fixes $W_0 = C_V(t)$ and $U \oplus U' = [V, t]$ as t and x commute. Thus $u'x = u' + u_{u'}(x)$, $u' \in U'$, with $u_{u'}(x) \in U$. As $C \cap Q$ lies in the center of C this group contains a subgroup $C_0 \simeq \mathrm{Sp}(2a, 2^b)$. The map $u_{u'} : C_0 \rightarrow U$ is a homomorphism. As C_0 is simple we see that $u_{u'}$ is trivial and therefore U' is C_0 -invariant. As $x\kappa = x[c(x)]$, $x \in C_0$ commutes with t we get $c(x) \in W_0$. Now

$$\begin{aligned} \Theta(u') &= \bar{\Theta}(u') = \bar{\Theta}(u'x\kappa) \\ &= \Theta(u' + c(x)) = \Theta(u') + \Theta(c(x)) + \phi(u', c(x)) \\ &= \Theta(u') + \Theta(c(x)). \end{aligned}$$

This implies $\Theta(c(x)) = 0$ for all $x \in C_0$. Hence x lies in $\mathrm{O}(W_0, \Theta)$ and thus $C \leq \mathrm{O}(W_0, \Theta) \cap \mathrm{Sp}(W_0, \bar{\phi}) \simeq \mathrm{O}^\epsilon(2a, 2^b)$, a contradiction.

(4) $H = P$: Assume $P < H$. If H would be irreducible then $H \simeq \mathrm{Sp}(V)$ or $\mathrm{GL}(V)$ and the same argument as in the standard parabolic case (proof of (4.4)), leads to a contradiction. So H is reducible. Then W/U is reducible as otherwise $P < H$ and (4.2) would imply that H is irreducible. This shows $a = 1$, $\epsilon = +$ and $P^{W/U} \simeq \mathrm{O}^+(2, 2^b)$, $b = n - m$, is dihedral of order $2(2^b - 1)$. Again this group is irreducible if $b > 2$. Thus $b = 2$ and $P^{W/U} \simeq \mathrm{Sym}(3)$. In this case there is a unique P -invariant subspace U_1 between U and W and $\dim U_1/U = 2$ in this case. As neither U nor W are H -invariant we see that U_1 and V/U_1 are H -irreducible and by MacLaughlins theorem [McL] $H^{U_1} \simeq H^{V/U_1} \simeq \mathrm{GL}(n, 2)$. Also

$$|O_2(H) \cap P| \geq 2^{\binom{n-1}{2} + 2(n-1)} > 2^{\binom{n}{2}}.$$

As U and V/W are dual with respect to the action of $L_1 \simeq \mathrm{GL}(n-2, 2)$ we conclude using the information of [Gr] that even $|O_2(H)| \geq 2^{\binom{n+1}{2}}$. But then $|O_2(P^{W/U})| > 1$ contradicting $P^{W/U} \simeq \mathrm{Sym}(3)$.

5 Proof of Theorems B and C.

In this section we consider B-sets $B = B_i^{(k)}$, $i = 1, 2$, of cyclic trace type as defined in (3.2). We note that if $k = -1$ and then (if B is big) $f_B(x, y) = \text{trace } xy$ showing that $B_1^{(-1)}$ is standard parabolic and $B_2^{(-1)}$ is standard. Also we observe that $B_i^{(k)} \sim B_i^{(k')}$ if $k \sim k'$: Namely if $k' \equiv 2^\ell k \pmod{2^n - 1}$ then $(x, y) \mapsto (x, y^{2^\ell})$ maps $B_i^{(k)}$ on $B_i^{(k')}$. To prove theorem C we are therefore interested in the computation of $K = \text{Aut}(B)$ if $k \not\sim -1$. Theorem C will be used to show theorem B afterwards.

As usual we set $H = K[V]_0$. We will follow the pattern of the proof of theorem A and first determine H_U , with U as in (3.2). We then show $H = H_U$. Both steps rest completely on group theory. In particular step two is difficult and requires a description of irreducible subgroups of $\text{GL}(V)$ which contain a cyclic, semiregular subgroup of order $2^n - 1$ (see theorems 3 and 4 in the appendix). By the same reason as in the proof of theorem A we will assume $n > 4$ in this section.

For the remainder of this section we keep the notation of (3.2) and add some more. Set $U' = (0, 1)F$. Then $V = U \oplus U'$ is a $Z\langle t \rangle$ -decomposition and if $k \not\sim 1$ this decomposition is even unique. For $0 \leq a \leq n - 1$, $\beta \in F$, and we define $\text{GF}(2)$ -linear mappings $t_a(\beta)$ on V by:

$$(x, y)t_a(\beta) = (x + y^{2^a}\beta, y)$$

Then we have the following relations

$$\begin{aligned} [t_a(\beta), [u]] &= [t_a(\beta), t_b(\gamma)] = 1, \quad t_a(\beta)^{z(\alpha)} = t_a(\alpha^{1-2^a k}\beta), \\ [u]^{z(\alpha)} &= [u\alpha], \quad t_a(\beta)^t = t_a(\beta^2), \quad z(\alpha)^t = z(\alpha^2) \end{aligned}$$

for $u \in U$, $0 \leq a, b \leq n - 1$, $\alpha \in F^*$, $\beta, \gamma \in F$. Clearly $Z\langle t \rangle \leq K \cap H$. Let E be the centralizer of the flag $0 \subset U \subset V$ in $\text{GL}(V)$ and set $\widehat{E} = E[U] \leq \text{AGL}(V)$. We first intend to determine the intersection of \widehat{E} with K . For this purpose we define $Z\langle t \rangle$ -invariant subgroups of \widehat{E} by $T_\infty = [U]$ and $T_a = \{t_a(\beta) \mid \beta \in F\}$, $0 \leq a < n$. We say that a $\text{GF}(2)[Z]$ -module of dimension n is of type $M(m)$ if $z(\alpha)$ acts via multiplication with α^m when this module is identified with F . Note that $M(m) \simeq M(m')$ if $m \sim m'$. The following lemma describes the Z -module structure of \widehat{E} .

(5.1) Lemma. *With the above notation the following holds:*

- (a) $T_\infty \simeq M(1)$ and $T_a \simeq M(1 - 2^a k)$, $0 \leq a \leq n - 1$, as $\text{GF}(2)[Z]$ -modules.
- (b) For each a the Z -module T_a is homogeneous (i.e. the direct sum of isomorphic irreducible Z -modules) and T_a is not irreducible iff $(1 - 2^a k)(1 - 2^c) \equiv 0 \pmod{2^n - 1}$ for some proper divisor c of n .
- (c) There is a partition $\mathcal{I} = \{\infty, 0, 1, \dots, n - 1\} = \mathcal{P} \cup \mathcal{Q}$ such that $\mathcal{P} = \{a_1, b_1\} \cup \dots \cup \{a_s, b_s\}$ is a partition into pairs and the following holds:
 - (1) If $a \in \mathcal{Q}$, then the irreducible Z -composition factor of T_a occurs in no T_c , $c \in \mathcal{I} - \{a\}$.

- (2) $T_{a_i} \simeq_Z T_{b_i}$ for $1 \leq i \leq s$. The irreducible Z -composition factor of T_{a_i} occurs in no T_c , $c \in \mathcal{I} - \{a_i, b_i\}$.

Proof. (a) and (b) are clear by the relations above. Assume $0 \leq a < b < c \leq n-1$ and $T_a \simeq T_b \simeq T_c$. Then

$$1 - 2^a k \equiv 2^x(1 - 2^b k) \equiv 2^y(1 - 2^c k) \pmod{2^n - 1}$$

with x, y suitable. Replacing if necessary k by $k2^a$ we may even assume $a = 0$. But then (2.12.a) yields a contradiction. Finally $T_\infty \simeq T_a$ gives $1 - 2^a k \equiv 2^x \pmod{2^n - 1}$. But then a is unique. Now (c) follows.

The following groups will occur in $\widehat{E} \cap Q\kappa$. For $0 \leq a, b, c \leq n-1$ we define $Y_{a,b} = \{t_a(\beta^{2^b})[(\beta, 0)] \mid \beta \in F\}$ and $X_{a,c;b} = \{t_a(\beta^{2^b})t_c(\beta) \mid \beta \in F\}$, $a \neq c$, which are elementary abelian of order 2^n .

(5.2) Lemma.

- (a) Suppose $\{a, c\}$ belongs to the partition of \mathcal{P} and $1 - 2^a k \equiv 2^b(1 - 2^c k) \pmod{2^n - 1}$. Then $X_{a,c;b} \leq K \cap H$ and Z normalizes this group.
- (b) Suppose $0 \leq a, b \leq n-1$ and $1 - 2^a k \equiv 2^b \pmod{2^n - 1}$. Then $Y_{a,b} \leq K$ is Z -invariant. Moreover $X_{a-b, a+1; -b} \leq K \cap H$ if $k \not\equiv 1$.

Proof. Since U is invariant under \widehat{E} we may assume that B is small. Now:

$$((t_a(\gamma^{2^b})t_c(\gamma))^{z(\alpha)^{-1}} = t_a(\alpha^{1-2^a k} \gamma^{2^b})t_c(\alpha^{1-2^c k} \gamma) = t_a((\alpha^{1-2^c k} \gamma)^{2^b})t_c(\alpha^{1-2^c k} \gamma)$$

Therefore Z normalizes $X_{a,c;b}$ in case (a). A similar computation shows that Z normalizes $Y_{a,b}$ in case (b). Take a typical element $(\alpha\beta, \alpha^k)$ in B and $x = (t_a(\gamma^{2^b})t_c(\gamma)) \in X_{a,c;b}$. Then $(\alpha\beta, \alpha^k)x = (\beta, 1)z(\alpha)x = (\beta, 1)x^{z(\alpha)^{-1}}z(\alpha)$. So as obviously $(\beta, 1)X_{a,c;b} \subseteq B$ we see $BX_{a,c;b} = B$. A similar argument shows in case (b) that $BY_{a,b} = B$. Finally in case (b) $2^b \equiv 1 - 2^a k$ implies $2^b - 2^a k \equiv 1 - 2^{a+1}k$ and thus $1 - 2^{a-b}k \equiv 2^{-b}(1 - 2^{a+1}k)$. Apply (a).

Remark. For $k = 1$ one has $1 - 2^{n-1}k \equiv 2^{n-1}$, so that $a - b \equiv a + 1 \equiv 0 \pmod{n}$. So in this case the group $X_{*,*,*}$ in (5.2.b) is not present.

(5.3) Lemma.

- (a) $T_{a,B} \neq 1$ iff there exists a proper divisor c of n such that $(2^a k - 1)(2^c - 1) \equiv 0 \pmod{2^n - 1}$. If c is the smallest divisor with this property and $n = cd$ then $|T_{a,B}| = 2^{c(d-1)}$.
- (b) Set $\mathcal{Q}_0 = \{a \in \mathcal{Q} \mid T_{a,B} \neq 1\}$. Then $|\mathcal{Q}_0| \leq 1$ if $n \neq 6$.

Proof. (a) Assume $Bt_a(u) = B$ for some $0 \neq u \in F$, i.e. $(\alpha\beta + \alpha^{2^a k}u, \alpha^k) \in B$ for $\alpha \in F^*$ and $\beta \in F_0$. This is equivalent to $\alpha^{2^a k - 1}u \in F_0$ for all $\alpha \in F^*$. But also $t_a(u)^{z(\alpha)} = t_a(\alpha^{1-2^a k}u)$ fixes B . These elements generate a subgroup of T_a which is isomorphic to $\langle \alpha^{1-2^a k}u \mid \alpha \in F^* \rangle$ as a subgroup of the additive group of F_0 . Therefore the $(2^a k - 1)$ -th power of Z does not act irreducibly on

U . Hence $(2^a k - 1)(2^c - 1) \equiv 0 \pmod{2^n - 1}$ for some $0 < c < n$, $c|n$. Choose c minimal with this property. Set $\text{GF}(2^c) \simeq F_1 \subset F$ and denote by $F_{00} \subseteq F_0$ the kernel of the trace map on F relative to F_1 . Then F_{00} is a maximal F_1 -subspace of F_0 and $T_{a,B} = \{t_a(u) \mid u \in F_{00}\}$.

(b) Assume $(2^a k - 1)(2^c - 1) \equiv 0 \pmod{2^n - 1}$ and $(2^b k - 1)(2^d - 1) \equiv 0 \pmod{2^n - 1}$ with proper divisors c, d of n . Since $n \neq 6$ there exists a 2-primitive prime divisor r of $2^n - 1$. Then r divides $2^a k - 1$ and $2^b k - 1$ and hence $k(2^a - 2^b)$. If $a \neq b$ then r divides k and hence $(k, 2^a k - 1)$, a contradiction. Assertion (b) follows.

Remark. The case $n = 6$ is exceptional with respect to (5.3.b): For $k = 11$ we have $|T_{1,B}| = 16$, $|T_{5,B}| = 8$ and for $k = 23$ we get $|T_{1,B}| = 8$, $|T_{5,B}| = 16$.

(5.4) Proposition. *Denote by Q the centralizer of the flag $0 \subset U \subset V$ in H . Then $Q = O_2(H_U)$ and we have a $Z \langle t \rangle$ -invariant decomposition $Q\kappa = X \oplus Y \oplus T$ with the following properties:*

(a)

$$X = \bigoplus_{i=1}^s X_{a_i, b_i; c_i}$$

with c_i suitable and the sum ranges over these pairs of \mathcal{P} which do not contain ∞ .

(b) $Y = Y_{a,b}$, with b suitable if $\{\infty, a\}$ is a part of \mathcal{P} and $Y = 1$ otherwise.

(c) Let $n \neq 6$. Then $T = T_{a,B}$ if $\mathcal{Q}_0 = \{a\}$ and $T = 1$ otherwise.

Proof. As Z is irreducible on U and V/U we see that $O_2(H_U) = H \cap E = Q$. The image $Q\kappa$ lies in $E[V]$. We claim that $Q\kappa$ even lies in \widehat{E} : Otherwise $Q\kappa$ would cover $E[V]/\widehat{E} \simeq_Z V/U \simeq M(k)$. As $Q\kappa \cap [V] = 1$ we see that $\widehat{E}/[U] \simeq E$ has a quotient of type $M(k)$, i.e. $T_a \simeq M(k)$ for some a . Hence $1 - 2^a k \equiv 2^b k \pmod{2^n - 1}$ or $k^{-1} \equiv 2^a + 2^b \pmod{2^n - 1}$ with a suitable b . Thus this factor is unique. In particular $Q\kappa$ contains a group $\{y[c(y)] \mid y \in T_a\}$ such that the map $T_a \ni y \mapsto c(y)[U] \in [V]/[U] \simeq V/U$ is an isomorphism. However if $1 \neq y \in T_a$ then $C_V(y) = [V, y]$ showing that $(y[c(y)])^2$ is a nontrivial element in $K \cap [U]$, a contradiction.

By lemmas (5.1-3) the groups X, Y and T all lie in $Q\kappa$. By (2.12.c) we see $T_{a,B} = 1$ if a belongs to a pair in \mathcal{P} . This shows $|(T_a \times T_b)_B| = 2^n$ if $\{a, b\}$ belongs to \mathcal{P} . All assertions follow.

In view of theorem D the following special case is of particular interest and we give a more direct description of $Q\kappa$ in this case.

(5.5) Corollary. *Suppose $Y = Y_{a,b} \neq 1$. Then $ZY[V]$ induces a rank 3 group on V . If $k \not\sim 1$ then $T = 1$ and $X = X_{a-b, a+1; -b}$. If $k \sim 1$ then $X = 1$ and $|T| = |T_{0,B}| = 2^{n-1}$.*

Proof. Clearly $T_a \leq Q$ and $T_a\kappa = Y$. The first assertion follows as ZT_a has 3 orbits on V . Assume $k \not\sim 1$. Then $X_{a-b, a+1; -b} \leq X$ by (5.2.b) and (2.12.b)

shows that equality holds. Moreover $T = 1$ by (2.11.d). Assume $k \sim 1$. Then $Y = Y_{-1,-1}$ and $|T_{a,B}| = 2^{n-1}$ by (5.3). Together with the remark following (5.2) we have $X = 1$.

Remarks. (a) Suppose $1 - 2^a k \equiv 2^b(1 - 2^c k) \pmod{2^n - 1}$, $a \neq c$, and assume $(2^b - 1, 2^n - 1) = 1$ (i.e. $(b, n) = 1$). Then $X = X_{a,c;b}$ by (2.13.b) as $k \sim 2^a k$.

However $\log_2 |X|$ is not bounded linearly by n . Of course in the exceptional case $k \sim -1$ we have $|X| = 2^{mn}$ if $n = 2m + 1$ or $n = 2(m + 1)$ respectively. But also for the generic cases there is no such bound:

Assume $n = mt$, $m \geq 3$, $(m - 1, 2^t - 1) = 1$ and set $q = 2^t$, $k = q^{m-2} + q^{m-3} + \dots + 1$. By (2.11.d) for $1 \leq r \leq m - 1$ and $a = t(m - r + 1)$, $b = t(n - r)$ and $c = t(r + 1)$ we have $X_{a,c;b} \leq X$. Hence $|X| \geq 2^{(m-1)n}$. I.e. $\log_2 |X| \geq (m - 1)n$.

(b) We will show in the sequel that $K = Z \langle t \rangle Q \kappa$. If $Y = 1$ we observe that $Q = Q \kappa$ has at least two orbits on every nontrivial coset of U in V . This implies that $K[V] = H[V]$ has at least rank 4 as a permutation group on V . In other words $K[V]$ is a rank 3 group iff Y is nontrivial.

(5.6) Proposition. *Let $k \not\sim -1$. Then $H_U = Z \langle t \rangle Q$.*

Proof. Using the classification of 2-transitive affine groups [He1], [He2], [Lie2] and Hupperts information about Singer-groups [Hu] we observe:

(*) Let $W = V(m, p)$, p a prime and $\Gamma L(1, p^m) \leq G \leq \text{GL}(W)$. Then there is a factorization $m = ab$ and $G \simeq \Gamma L(a, p^b)$.

Hence $H_U^U \simeq \Gamma L(a, 2^b)$ with $n = ab$. A similar statement holds for H_U^W , $W = V/U$. Using argument (E) we see that the kernel of the action of H_U on U and on W is in both cases Q . Therefore $H_U/Q \simeq H_U^U/Q \simeq H_U^W/Q$. If $a = 1$ we are done. Assume $a > 1$. We define subgroups $Q \trianglelefteq H_0 \trianglelefteq H_1 \trianglelefteq H_U$ by $H_0/Q \simeq \text{SL}(a, 2^b)$, $H_1/Q \simeq \text{GL}(a, 2^b)$. As $C_V(Z) = 0$ we have $Z \leq H_1 \cap K$. By (2.9) H_0 splits over Q and by a well known theorem of Gaschütz H_1 splits over Q too. So we find subgroups $L_0 \leq L_1 \leq H_1$ such that $L_0 = L_1 \cap H_0 \simeq \text{SL}(a, 2^b)$, $L_1 \simeq \text{GL}(a, 2^b)$ with $H_i = L_i Q$ and $Z \leq L_1$. We do indentify U with the natural L_0 -module. As $\text{GF}(2)[L_0]$ -modules $W \simeq U$ or U^* .

We claim that we may assume $L_1 \leq H \cap K$: If $a < n$ then $1 \neq Z_0 = Z(L_1) \leq Z$ and $Z_0 = Z_0 \kappa$. Then $C_{H_1 \kappa}(Z_0 \kappa) = C_{H_1 \kappa}(Z_0) \simeq L_1$ and as this group fixes $C_V(Z_0) = 0$ we see that this group is L_1 . If $a = n$ then $L_1 = L_0$ and $H^1(L_1, U) = H^1(L_1, W) = 0$. Thus c induces a coboundary from L_1 in V/U . Conjugating with a suitable element from $[V]$ (i.e. and replacing B by an equivalent B-set) we may assume that the induced map is even trivial. But now $c : L_1 \rightarrow U$ is a coboundary and adjusting with an element from $[U]$ we may assume that $c = 0$, i.e. $L_1 \leq K$.

As we have seen in (2.3) Q is isomorphic to a submodule of $\text{Hom}(W, U) \simeq \bigoplus_i W^* \varphi^i \otimes U$ where φ is the Frobenius automorphism of $F = \text{GF}(2^b)$.

Assume first $k = 1$. Then U and W are isomorphic as Z -modules and therefore $W \simeq U$ as a $\text{GF}(2)[L_0]$ -module. Also $|Q| = 2^{2n-1}$ and $|C_Q(Z)| = 2^{n-1}$ by (5.6). Now $Z \cap L_0$ has no nontrivial fixed-points in $U^* \varphi^i \otimes U$, $i > 0$, so that by (5.5) the centralizer of this group in $(U^* \otimes U) \cap Q$ has dimension $n - 1$. Let A be the irreducible adjoint module. As we have seen in (2.9) we have $U^* \otimes U \simeq A \oplus F$ if a is odd whereas this module is uniserial with factors F, A, F in this order if a

is even. This shows that a is even and that Q contains the bottom factors F, A . But then $|Q| \geq 2^{b+(a^2-2)b} > 2^{2n}$, a contradiction. So from now on assume $k \not\sim 1$. We choose a basis $\{v_1, \dots, v_{2n}\}$ of V such that $U = \langle v_1, \dots, v_n \rangle$ and that the associated matrix representation

$$L_0 \ni x \mapsto D(x) = \begin{pmatrix} D_1(x) & 0 \\ 0 & D_2(x) \end{pmatrix} \begin{pmatrix} 1 & 0 \\ A(x) & 1 \end{pmatrix}$$

has the property $D_2(x) = D_1(x)$ if $W \simeq U$ and $D_2(x) = D_1(x)^{-t}$ if $W \simeq U^*$. We use the notation of (2.3) and write $A(x) = \sum_{i=0}^{b-1} A_i(x)$ where $A_i(x)$ corresponds to the component in $H_i(W, U)$. The map A_i defines a class $[A_i]$ in $H^1(L_0, W^* \varphi^i \otimes U) \simeq \text{Ext}_{\text{GF}(2)[L_0]}(W \varphi^i, U)$. We now invoke the result of Bell [Be; thm. 3.2]: These cohomology groups are always trivial with the exception $a = 3$, $W \simeq U^*$ and $i = 1$ or $b - 1$. In all other cases U has a L_0 -invariant complement and even a L_1 -invariant complement as $|L_1 : L_0|$ is odd. As $k \not\sim 1$ this complement is U' . Choose $0 \neq v \in U'$ and set $\widehat{L} = L_{0,v}$.

Case 1: V is a completely reducible L_0 -module. Assume first $a > 2$ and $U \simeq U' \simeq W$ as L_0 -modules. Then \widehat{L} has on U and U' precisely 2^b orbits of length 1 and one orbit of length $2^{ab} - 2^b = 2^n - 2^b$. Also $C = B \cap (v + U)$ is a \widehat{L} -invariant set of size 2^{n-1} implying $2^{n-1} \geq 2^n - 2^b$, a contradiction. So assume $U^* \simeq U' \simeq W$ and note that for $a = 2$ automatically $U^* \simeq U$ holds. This time \widehat{L} fixes an irreducible, $(n - b)$ -dimensional subspace U_0 of U and $U - U_0$ splits into $2^b - 1$ orbits of length 2^{n-b} . By definition of the B-set $C = B \cap (v + U) = v + U_1$ with a hyperplane U_1 of U . This implies $U_0 \subseteq U_1$. Clearly L_0 leaves invariant the quadratic form $\Theta = \sum_{i=1}^n x_i x_{i+n}$. Conjugation with a suitable element of the form $z = z_0 \oplus 1_{U'}$, $z_0 \in Z(\text{GL}_F(U))$ fixes L_0 and moves U_1 onto $U \cap v^\perp$ (the \perp symbol refers to the bilinear form induced by Θ). Thus we may assume $C = B^0 \cap (v + U)$ with the standard B-set B^0 . But $CL_0 \cup U$ is the standard parabolic B-set and as $B = CL_0$ or $CL_0 \cup U$ we see that B is standard parabolic or standard. Hence $k \sim -1$, a contradiction.

Case 2: V is an indecomposable L_0 -module, i.e. $a = 3, U \simeq W^*$ as observed above. Using again Bells result we can choose our basis in such a way that $A(x) = A_1(x) + A_{b-1}(x)$, $x \in L_0$. As before $C = B \cap (v + U) = v + U_1$, $U_0 \subseteq U_1$. Conjugating again with an element z as above we may assume $C = B^0 \cap (v + U)$ but we have to replace L_0 and \widehat{L} by L_0^z and \widehat{L}^z . Let E_1 be the submodule of E corresponding to $\wedge^2(U)$ (see (2.5)). If A induces a coboundary on the module E/E_1 then L_0^z lies in $K^0 = \text{Aut}(B^0)$ and again B is either standard or standard parabolic, a contradiction. In the other case A induces a 1-cocycle which is not a coboundary. Thus $B = CL_0$ or $CL_0 \cup U$ is of special parabolic type according to the definition of (3.1.c). But by theorem A the group H does not contain a cyclic, semiregular subgroup of order $2^n - 1$, again a contradiction.

Our goal for the remainder of this section is to show that we already have found the full automorphism group of B , i.e. to show that $H = H_U$ holds. The next result excludes the possibility that H fixes U' but not U .

(5.7) Lemma. *Assume $O_2(H_{U'}) \neq 1$. Then $Q = O_2(H_U) \neq 1$ too.*

Proof. As $Q \neq 1$ for $k = 1$ we can exclude the case $k \sim 1$. Let E' be the centralizer of the flag $0 \subset U' \subset V$. For $0 \leq a < n$, $u \in F$, define a linear map $s_a(u)$ by $(x, y)s_a(u) = (x, y + x^{2^a}u)$. Then $s_a(u)^{z(\alpha)} = s_a(\alpha^{k-2^a}u)$. Set $T'_a = \{s_a(u) \mid u \in F\}$. Then $E' = \bigoplus_{a=0}^{n-1} T'_a$ is a Z -invariant decomposition and $T'_a \simeq_Z M(k-2^a) \simeq_Z M(2^{-a}k-1)$. Set $T'_\infty = [U']$. The same argument as in the beginning of the proof of (5.4) shows $Q'\kappa \subseteq \widehat{E}' = E'T'_\infty$ where $Q' = O_2(H_{U'})$. First we note:

(1) B is big and $B = \{(\alpha, \alpha^k\beta^{-k}) \mid 0 \neq \alpha \in F, 0 \neq \beta \in F_0\} \cup U \cup U'$: Assume that B is small and $0 \neq s = t[v] \in Q'\kappa$, $t \in E'$, $v \in U'$. Then for $w \in V - U'$ the set $C = B \cap (w + U')$ has size $2^{n-1} - 1$. Also $ws = w + (w + U')t_0 + v$ where $t_0 : V/U' \rightarrow U'$ is a linear map such that $yt = y + (y + U')t_0$. As $t_0 \neq 0$ we can choose w in such a way that $(w + U')t_0 \neq v$. Then s acts fixed-point-freely on C which is impossible. Hence B is big. The second assertion is obvious.

Since we have an analogue statement as (5.1) for \widehat{E}' we see that $Q' \neq 1$ implies $T'_{a,B} \neq 1$ or $(T'_a \times T'_\infty)_B \neq 1$ for some $0 \leq a < n$ or that $(T'_a \times T'_c)_B \neq 1$ for some $0 \leq a < c < n$.

(2) Assume $T'_{a,B} \neq 1$. Then $T_{-a,B} \neq 1$: Let $1 \neq s_a(u) \in T'_{a,B}$ and $(\alpha, \alpha^k\beta^{-k}) \in B$. Then $(\alpha, \alpha^k\beta^{-k} + \alpha^{2^a}u) \in B$ showing $\alpha^k\beta^{-k} + \alpha^{2^a}u = 0$ or $= \alpha^k\beta_0^{-k}$ for some $0 \neq \beta_0 \in F_0$. Set $F_0^{-1} = \{\beta^{-1} \mid 0 \neq \beta \in F_0\} \cup \{0\}$. We conclude that for all $0 \neq \alpha \in F$, $\beta^{-k} \in F_0^{-k}$:

$$\beta^{-k} + \alpha^{k-2^a}u \in F_0^{-k}.$$

In particular $F_0^{-k} + F_0 = F_0^{-k}$ where F_0 is the additive group generated by the $\alpha^{k-2^a}u$'s. As in (5.3) we conclude that $|F_0|$ divides $2^c - 1$ for some proper divisor c of n . Again by (5.3) we deduce $T_{-a,B} \neq 1$.

(3) Assume $(T'_a \times T'_c)_B \neq 1$. Then $(T_{-a} \times T_{-c})_B \neq 1$: Because of (2) we assume $T'_a \simeq_Z T'_c$ and hence $k - 2^a \equiv 2^b(k - 2^c) \pmod{2^n - 1}$, b suitable. This shows $1 - 2^{-a}k \equiv 2^{b+c-a}(1 - 2^{-c}k) \pmod{2^n - 1}$ and we can apply (5.2).

(4) Assume $(T'_a \times T'_\infty)_B \neq 1$. Then $(T_{-a-1} \times T_{b-b})_B \neq 1$, b suitable: Again this is a consequence of (5.2).

(2)-(4) show $Q \neq 1$.

The next lemma rules out the possibility that H is irreducible but leaves invariant the set $\{U, U'\}$.

(5.8) Lemma. *Let H be irreducible and $k \not\sim \pm 1$. Then $O^2(H)$ is irreducible too.*

Proof. Assume that $O^2(H)$ is reducible. As $k \not\sim 1$ this group has two nonisomorphic composition factors on V . This implies that there exists a normal subgroup $O^2(H) \leq H_0$ of index 2 such that $V = U \oplus U'$ is a H_0 -decomposition and $h \in H - H_0$ interchanges U and U' . By a Frattini argument we find such an $h \in H \cap K$ which normalizes Z . Then $(x, y)h = (yh_1, xh_2)$ with GF(2)-linear mappings h_i on F . Since $z(\alpha)^h \in Z$ we see that h_1 and h_2 lie in the normalizer of the multiplicative group F^* of F in $\text{GL}(F)$. This normalizer is $\langle \varphi \rangle F^*$, φ the Frobenius automorphism. Modifying h with an element from $\langle t \rangle Z$ we can even assume $h_2 = 1$. Hence $(x, y)h = (y^{2^n}\gamma, x)$ with some $\gamma \in F^*$ and some number

u. Take $(\alpha\beta, \alpha^k) \in B$. Then $(\alpha^{k2^u}, \alpha\beta) \in B$. If $\beta \neq 0$ set $\delta^k = \alpha\beta$. Then $(\delta(\beta^{-k2^u}\gamma), \delta^k) \in B$ and thus $F_0^{-k}\gamma = F_0$. Using proposition 3 of the appendix we deduce $k \sim -1$, a contradiction.

Remark. Suppose $k \not\sim 1$. The proof of (5.8) shows:

(I) Let $h \in N_H(Z)$ interchange U and U' . Then $k \sim -1$.

We will apply this as argument (I) in the sequel.

(5.9) Lemma. *Suppose $Z \leq G \leq H$, $n = 2m$, $m \neq 3$. Assume further:*

- (1) $E = E(G) \simeq \text{SL}(2, 2^m)$.
- (2) V is an irreducible $\text{GF}(2)[E]$ -module, isomorphic to $M \otimes M^\sigma$ where M is the natural E -module and $\sigma = 2^b$ is a Galois automorphism with $\sigma^2 \neq 1$.

Then E is not normal in H .

Proof. By the assumption $G_1 = N_{\text{GL}(V)}(E) \simeq \text{GL}(2, 2^m)$. Let G_0 be the normal subgroup of G_1 which corresponds to $\text{GL}(2, 2^m)$ and set $Z_0 = Z(G_0)$. Let r be a 2-primitive prime divisor of $2^n - 1$ and S a Sylow r -subgroup of G . As $r \geq n + 1$ we see that $S \leq E$ and since $|S| = |Z|_r$ we may even assume $S \leq Z$. Hence $Z \leq C_{G_1}(S) = C_{G_0}(S) = Z_0 \times Z_1$ where $Z_1 = C_E(S)$ is cyclic of order $2^m + 1$. We conclude $Z = Z_0 \times Z_1$ and $G_0 \leq G$.

Let λ be a generator of $\text{GF}(2^n)^*$. The eigenvalues of a generator z_0 of Z_0 are the m Galois conjugates of $\lambda^{2^{m+1}}$ (each eigenvalue has multiplicity 4). The eigenvalues of a generator z_1 of Z_1 are the n Galois conjugates of $\lambda^{(2^m-1)(1+2^b)}$ and the n Galois conjugates of $\lambda^{(2^m-1)(2^m+2^b)}$. Then $z = z_0 z_1$ is a generator of Z and as a $\text{GF}(2)[Z]$ -module V splits as $V = U \oplus U'$ where U and U' are nonisomorphic, irreducible Z -modules. Of course U and U' have the usual meaning. Up to a reversal of the roles of U and U' we have that z has on U the Galois conjugates of $\mu_1 = \lambda^{2^{m+1} + (2^m-1)(1+2^b)} = \lambda^{2^{m+1} + 2^{m+b} - 2^b}$ and on U' the Galois conjugates of $\mu_2 = \lambda^{2^{m+1} + (2^m-1)(2^m+2^b)} = \lambda^{2^{m+1} + 2^{m+b} - 2^b}$ as eigenvalues. As both cases are symmetric we just consider one of them.

We may identify z with the map $z(\mu_1)$ (see (3.2)). Then

$$t_a(u)^z = t_a(\mu_1 \mu_2^{-2^a} u).$$

Hence z has the Galois conjugates of $\mu_1 \mu_2^{-2^a}$ as eigenvalues on the module T_a :

$$T_a \simeq M(2^{m+1} + 2^{m+b} - 2^b - 2^{a+1} - 2^{m+a+b} + 2^{a+b})$$

In particular

$$T_0 \simeq M(2(2^m - 1)) \simeq M(2^{b+1}(2^m - 1)) \simeq T_m$$

as Z -modules. Then $Y \neq 1$ in the sense of (5.2-4) and $Y\kappa^{-1} \leq H$. As $Y\kappa^{-1} \cap E = 1$ the assertion follows.

(5.10) Proposition. *Assume $k \not\sim -1$. Then $H = H_U$.*

Proof. Suppose $H \neq H_U$. Then $G = O^2(H)$ is irreducible: If $k \not\sim 1$ the spaces U and U' are not Z -isomorphic and the claim follows from (5.7-8). If $k \sim 1$ then $Q \cap G \neq 1$ again implying the claim.

As we want to use Zsigmondy's theorem we exclude first the case $n = 6$. Then up to equivalence $k = 1, 5, 11, 13$ or 23 . According to (5.4) in case $k = 1$ H_U has 3 orbits on V and in the remaining cases H has orbits of lengths 1, 63, 2016, 2016. Now $H \neq H_U$ would imply that $H[V]$ is 2-transitive or a primitive rank 3 group. So by [De2] B would be standard, a contradiction to (5.6).

So from now on $n \neq 6$. Hence there exists a 2-primitive prime divisor r of $2^n - 1$. We apply proposition 1 of the appendix to the groups G and Z and examine the various cases.

First we rule out the generic case (e), i.e. $E = E(G)$ is irreducible and quasisimple. By [De2] $H[V]$ is not 2-transitive or a rank 3 group. Using theorems 3 and 4 of the appendix we see that G fulfills the assertions of (5.9). But then E is not normal in H , a contradiction.

We now treat the nongeneric cases of proposition 1 and start with (a), i.e. $F^*(G)$ is homogeneous and cyclic and contains the r -part of Z . Hence $C_{\text{GL}(V)}(R) \simeq \text{GL}(2, 2^n)$ contains Z and $F^*(G)$ as $R \text{ char } F^*(G)$. If $F^*(G)$ is irreducible then $|F^*(G)|$ divides $2^{2n} - 1$ and $(|F^*(G)|, 2^n + 1) \neq 1$. As $F^*(G)$ has odd order we may assume $F^*(G) \leq K$. Since $F^*(G)$ acts semiregularly on $V - 0$ we see that the order of $F^*(G)$ divides $|B|$ if B is small and $|B| - 1$ if B is big, which is impossible. Hence $F^*(G)$ is reducible, i.e. $|F^*(G)| \leq 2^n - 1$ and $|G/F^*(G)| \leq n$. But then $|G| \leq |O^2(H_U)|$, a contradiction.

Assume next that we are in case (b) or (d) of the proposition. Then $E(G)$ has at most two components and the components are normal. One component - say E_1 - lies in \mathcal{H} . According to theorem 3 of the appendix $E_1/Z(E_1)$ is of Lie type in characteristic 2. By [He1, He2, Li2] (see also [GPPS]) we have $E_1/Z(E_1) \simeq \text{PSL}(a, 2^b)$, $ab = n$; $E_1/Z(E_1) \simeq \text{Sp}(2a, 2^b)$ or $\Omega^-(2a, 2^b)$, $2ab = n$; $E_1/Z(E_1) \simeq \text{PSU}(a, 2^b)$, $2ab = n$, a odd; $E_1/Z(E_1) \simeq G_2(2^b)$, $6b = n$; $E_1/Z(E_1) \simeq Sz(2^b)$, $4b = n$. Moreover $C_{\text{GL}(V)}(E_1) \simeq \text{GL}(2, 2^b)$ in all cases with the exception of the unitary case where $C_{\text{GL}(V)}(E_1) \simeq \text{GL}(2, 2^{2b})$. Now $F^*(G) \leq E_1 \times C_G(E_1) \leq E_1 \times C_{\text{GL}(V)}(E_1)$. The list of subgroups of $\text{SL}(2, 2^c)$, $c = b$ or $2b$, (see [HB; II, 8.27]) shows us $F^*(G) = E_1 \times D$ and $D = O^2(C_G(E_1)) = Z_0 \times S$ where Z_0 is isomorphic to a subgroup of $Z(\text{GL}(2, 2^c))$ and $S \simeq \text{SL}(2, 2^d)$, $d|c$ or S is a cyclic subgroup of odd order in $\text{SL}(2, 2^c)$. Moreover if $E_1 \not\cong \text{SL}(2, 2^b)$ then r does not divide $|D|$.

We first treat the case $E_1 \not\cong \text{SL}(2, 2^b)$. Now $R \in \text{Syl}_r(Z)$ is a Sylow r -subgroup of E_1 and H . As $C_{E_1}(R) = C_{\text{Aut}(E_1)}(R)$ we have $Z \leq C_{E_1}(R)C_{\text{GL}(V)}(E_1)$. An upper bound for the order of Z is:

$$(*) \quad |Z| \leq |C_{E_1}(R)| \cdot \mu(C_{\text{GL}(V)}(E_1))$$

Here $\mu(X)$ denotes the maximal order of cyclic group of odd order in X . Moreover if we replace the μ -term by the order of a suitable cyclic group of odd order in $C_{\text{GL}(V)}(E_1)$ we see that $|Z|$ divides the right hand side. Set $m_0 = \mu(C_{\text{GL}(V)}(E_1))$.

If $E_1 \simeq G_2(2^b)$ then $|C_{E_1}(R)|$ divides $(2^{3b} + 1)/(2^b + 1)$, $m_0 = 2^{2b} - 1$ contradicting (*).

If $E_1 \simeq \text{Sz}(2^b)$ then $|C_{E_1}(R)| = 2^b + 2^{c+1} + 1$, $b = 2c$, $m_0 = 2^{2b} - 1$ contradicting (*) again.

If $E_1/Z(E_1) \simeq \text{PSU}(a, 2^b)$ then $|C_{E_1}(R)| = (2^{ab} + 1)/(2^b + 1)$, $m_0 = 2^{4b} - 1$. Now (*) implies $a = 3$ and $n = 6b$. Then $(2^{3b} - 1, |\text{GL}(2, 2^{2b})|_{2'}) = 2^b - 1$, which is impossible too by the remark which follows (*).

If $E_1 \simeq \Omega^-(2a, 2^b)$ or $\text{Sp}(2a, 2^b)$ then $|C_{E_1}(R)| = 2^{ab} + 1$, $m_0 = 2^{2b} - 1$ which implies $a = 2$. Set $q = 2^b$. As $|C_{\text{Aut}(E_1)}(R)|_{2'} = |C_{E_1}(R)| = q^2 + 1$ we have $Z = Z_1 \times Z_2$ where $Z_1 = Z \cap E_1$ has order $q^2 + 1$ and $Z_2 \leq Z \cap C_G(E_1)$ has order $q^2 - 1$. Since $E_1 \leq C_G(Z_2)$ we see that Z_2 acts homogeneously on V . Therefore we can consider V as a 4-dimensional $\text{GF}(q^2)[E_1 \times Z_2]$ -module where Z_2 induces the group of scalars. Let z_i be a generator of Z_i , $i = 1, 2$. Then (with respect to the $\text{GF}(q^2)$ -structure) z_2 induces on V a multiplication with $\tau \in \text{GF}(q^2)$, $|\tau| = q^2 - 1$ and z_1 has a minimal polynomial of the form $\mu = (x^2 + ax + b)(x^2 + a^q x + b^q)$ with $a = \gamma + \gamma^{q^2}$, $b = \gamma\gamma^{q^2}$ where γ is an element of order $q^2 + 1$ in $\text{GF}(q^4)$. Considering V as a $\text{GF}(2)[Z]$ -module again we see that $z = z_1 z_2$ has on U the Galois conjugates of $\tau\gamma$ as eigenvalues and on U' the Galois conjugates of $\tau\gamma^q$. Then $k \sim q^3 - q^2 + q + 1$. As $|(F^*)^{q^3 - q^2 + q + 1 - 2}| = |(F^*)^{(q^2 + 1)(q - 1)}|$ divides $q^2 - 1$ we can apply (5.3.a). Hence $C_H(Z_1)$ contains an elementary abelian 2-group T of order q^2 , i.e. q^2 divides $|C_H(Z_1)|$ and thus $|\text{GL}(2, q)|$, a contradiction.

If $E_1 \simeq \text{SL}(a, 2^b)$, $a \geq 3$ then $V \simeq M \oplus M$ with the standard $\text{SL}(a, 2^b)$ -module M viewed as a $\text{GF}(2)[E_1]$ -module. Then E_1 has on $V - 0$ precisely $2^b + 1$ orbits of length $2^{ab} - 1 = 2^n - 1$ and one orbit of length $(2^n - 1)(2^n - 1)$. Also as $H^1(\text{SL}(a, 2^b), M) = 0$ we may assume $E_1 \leq K$ which is impossible.

Now we handle the case $E_1 \simeq \text{SL}(2, q)$, $q = 2^b$. We claim that $Z \leq F^*(G) = E_1 \times D$. Let $\langle y \rangle$ be a Sylow r -subgroup of Z and write $y = y_1 y_2$ with $y_1 \in E_1$ and $y_2 \in D$. Let $g \in G$ of odd order centralize y . Then g centralizes both components of y as g normalizes E_1 and D . If $y_2 \neq 1$ then $E_1 \leq C_{\text{GL}(V)}(y_2) \simeq \text{GL}(2, q)$ which implies $O^2(C_G(y_2)) \leq O^2(C_G(E_1))E_1 \leq F^*(G)$. If $y_1 \neq 1$ and $g \in C_G(y_1)$ then g induces an inner automorphism on E_1 and therefore $g \in C_G(E_1)E_1$. We deduce $Z \leq F^*(G)$.

First observe $k \not\sim 1$: Otherwise $C_{H \cap K}(Z)$ contains an elementary abelian 2-group of order $2^{n-1} > q$. But clearly $F^*(G) = F^*(H)$ and $|C_{F^*(G)}(y)|_2 \leq q$, a contradiction.

This observation implies $U \not\sim_Z U'$ and as $C_{\text{GL}(V)}(Z)$ is the direct product of two cyclic groups of order $2^n - 1$ we apply argument (E) and obtain $C_G(Z) = Z$. The involution $u = t^b$ normalizes Z and fixes U and U' . Let v be another involution in $N_H(Z)$. If v interchanges U and U' then $k \sim -1$ by argument (I), a contradiction. Hence v fixes both spaces too and therefore induces the same automorphism on Z as u . Therefore:

(**) $N_H(Z)$ contains only one class of involutions.

Write a generator z of Z as $z = z_1 z_0 s$ with $z_1 \in E_1$, $z_0 \in Z_0$ and $s \in S$. Then $Z \leq C_{E_1}(z_1) \times Z_0 \times C_S(s) \leq C_G(Z)$. If an odd prime p divides the order of two of the components of the direct product then $C_G(Z)$ contains an elementary abelian p -group of order p^2 contradicting argument (E). Therefore the odd parts of the orders of the components are pairwise coprime. This implies $\langle z_1 \rangle = Z_1 = Z \cap E_1$ and $|Z_1|$ and $|Z_2|$ are coprime where $Z_2 = \langle z_0 s \rangle$. An involution v in $N_{E_1}(Z_1)$ induces the same automorphism on Z as the involution

u . Then $|Z_2|$ divides $q - 1 = |C_Z(u)|$ and $|Z_1|$ divides $q + 1 = |[Z, u]|$. Thus $|Z_i| = q - (-1)^i$, $i = 1, 2$. As $|Z_0|_{2'}$ and $|C_S(s)|_{2'}$ are coprime also $Z_2 = \langle z_0 \rangle \times \langle s \rangle$. If S would be nonabelian then an involution v in $N_S(\langle s \rangle)$ normalizes Z and centralizes Z_1 contradicting (**). So S is abelian and $D = F(G)$ is cyclic. Again with argument (E) we conclude $D = Z_2$. As an abelian subgroup of order $(q - 1)^2$ in $C_{\text{GL}(V)}(E_1)$ leaves precisely two n -dimensional E_1 -spaces invariant we see $V = W_1 \oplus W_2$ with $E_1 \times D$ -modules W_i . Also by (5.8) $F^*(G) = E_1 \times D$ acts homogeneously on V . Thus $W_1 \simeq W_2$ as $F^*(G)$ -modules implying $k \sim 1$, a contradiction.

Finally assume that we are in case (c) of proposition 1. Hence r divides the order of $Z_0 = F(G)$ and $E = E(G) \simeq \text{SL}(2, 2^m)$ where m divides n . Then $m < n$ as otherwise E is transitive on $V - 0$. The case $2m = n$ is a subcase of (d). So assume $m < n/2$. Let $\langle y \rangle$ be a Sylow r -subgroup of $F^*(G)$. Then $\langle y \rangle \leq Z_0$ and $F^*(G) \leq C_G(y) \leq C_{\text{GL}(V)}(y) \simeq \text{GL}(2, 2^m)$. Again an inspection of the subgroups of $\text{GL}(2, 2^m)$ shows $Z \leq C_G(y) = F^*(G)$ and as $|F^*(G)|_2 = 2^m < 2^{n-1}$ we exclude the possibility $k \sim 1$. Then argument (E) implies $Z = Z_0 \times Z_1$ with $Z_1 = Z \cap E_1$ and again (**) holds. An involution v in $N_{E_1}(Z_1)$ normalizes Z and centralizes y . This contradicts (**). Thus case (c) is ruled out too.

Theorem C now follows by propositions (5.4), (5.6) and (5.10).

(5.11) Proof of theorem B.

(a) We first decide as to whether or not $B = B_1^{(k)}$ and $B' = \overline{B}_2^{(k)}$ can be equivalent. For $k = 1$ we observe $Bt_0(\gamma) = B'$, $\text{trace } \gamma \neq 0$ while for $k = -1$ B is standard parabolic of degree n while B' is standard, i.e. the sets are inequivalent.

So we assume $k \not\sim \pm 1$ and $B' = Bg$, $g \in \text{AGL}(V)$. The automorphism group of K of B and B' contains precisely one conjugacy class of cyclic groups of order $2^n - 1$ with representative Z . Adjusting g with an element from K we may therefore assume $g \in N_{\text{AGL}(V)}(Z) = N_{\text{GL}(V)}(Z)$. Then g fixes the set $\{U, U'\}$ since these are the only proper Z -spaces. However $B \cap U = \emptyset \neq B \cap U'$ and $B' \cap U = \emptyset = B' \cap U'$, a contradiction.

(b) We already observed in the introduction of this section that the implication (2) \Rightarrow (1) holds.

(1) \Rightarrow (2): We may assume $B = B_1^{(k)}$ and $B' = B_1^{(k')}$ or $B' = \overline{B}_2^{(k')}$. Now B-sets of type $k \sim -1$ are characterized by the fact that the automorphism group K is nonsolvable and B-sets of type $k \sim 1$ are characterized by the fact that for the cyclic subgroup Z of K one has $|C_Q(Z)| = 2^{n-1}$.

So from now on we assume $k \not\sim \pm 1 \not\sim k'$. Let $B' = Bg$, $g \in \text{AGL}(V)$. Denote by K' the automorphism group of B' and denote by Z' a cyclic subgroup of order $2^n - 1$ fixing U' . Arguing as in (a) we may assume $Z^g = Z'$ and as $C_V(Z) = C_V(Z') = 0$ also $g \in \text{GL}(V)$. Then again arguing as in (a) we obtain that g fixes the subspaces U and U' and that $B' \neq \overline{B}_2^{(k')}$. Choosing generators z of Z and z' of Z' appropriately we also can assume $z_U = z'_U$. Modifying g with an element from $N_K(Z)$ we can even assume $g_U = 1_U$. By definition of the B-sets B and B' the projections of the groups Z and Z' to U' are the same.

This shows that $g_{U'}$ normalizes $Z_{U'} = Z'_{U'}$. Identifying U' with F we see that $g_{U'}$ is a map of the form $x \mapsto \gamma x^{2^\ell}$. Hence $B' = \{(\alpha\beta, \gamma\alpha^{k2^\ell}) \mid \alpha \in F^*, \beta \in F_0\}$. Therefore $\alpha \mapsto \alpha^{k'} = \gamma\alpha^{k2^\ell}$ is an automorphism of the multiplicative group F^* . Hence $\gamma = 1$ and $k \sim k'$.

6 Proof of Theorem D

In this section $B \subseteq V = V(2n, 2)$ is a B-set and K is a subgroup of $\text{Aut}(B)$ such that $G = K[V]$ acts as a rank 3 group on V . As usual we set $H = G_0 \leq \text{GL}(V)$ and by $\kappa : H \rightarrow K$ we denote the canonical isomorphism with $h\kappa = h[c(h)]$ and a 1-cocycle $c : H \rightarrow V$. In view of [De2] we may assume that G is imprimitive and B is nonstandard. Hence there is an H -invariant subspace $0 \subset U \subset V$ such that the H -orbits are $V - U$, $U - 0$ and 0 . We denote by m the dimension of U . By $\bar{c} : H \rightarrow V/U$, $\bar{c}(h) = c(h) + U$ we define a 1-cocycle of H into the module V/U . The kernels of the action of H on V/U and U define normal subgroups $N_1 = C_H(V/U)$, $N_2 = C_H(U)$. Set $Q = N_1 \cap N_2$. Again we can assume $n > 4$: The case $n = 4$ is covered by our computer calculations which we describe in the next section. The following lemma is obvious.

(6.1) Lemma. *H acts transitively on the nontrivial vectors of U and V/U and $Q = O_2(H)$.*

The subgroups of $\text{GL}(d, q)$ which act transitively on the nontrivial vectors of $V(d, q)$ are classified by Hering [He1], [He2] and Liebeck [Li2]. Information about the first cohomology groups of these groups are in [Be], [JP], [Si1], and the appendix. We summarize the relevant facts:

(6.2) Lemma. *Set $W = V(d, 2)$ and let $X \leq \text{GL}(V)$ be transitive on the nontrivial vectors of W .*

(a) *Either $X \leq \Gamma\text{L}(1, 2^d)$ or $T \trianglelefteq X$ and:*

- (1) $T \simeq \text{SL}(a, 2^b)$, $a \geq 2$, $ab = d$.
- (2) $T \simeq \text{Sp}(2a, 2^b)^{(1)}$, $a \geq 1$, $2ab = d$.
- (3) $T \simeq \text{G}_2(2^b)^{(1)}$, $6b = d$.
- (4) $T \simeq \text{Alt}(7)$, $d = 4$.

(b) *For the first cohomology groups in cases (1)-(4) of (a) we have:*

- (1) $\dim \text{H}^1(\text{SL}(a, 2^b), V(a, 2^b)) = 1$ if $a = 2$, $b > 1$, or $a = 3$, $b = 1$, and this dimension is 0 otherwise.
- (2) $\dim \text{H}^1(\text{Sp}(2a, 2^b)^{(1)}, V(2a, 2^b)) = 1$.
- (3) $\dim \text{H}^1(\text{G}_2(2^b)^{(1)}, V(6, 2^b)) = 1$.
- (4) $\dim \text{H}^1(\text{Alt}(7), V(4, 2)) = 0$.

(c) *Let T be as in (b.1-3) and $c : T \rightarrow W$ be a 1-cocycle but not a 1-coboundary. Set $Y = \{t[c(t)] \mid t \in T\} \leq \text{AGL}(W)$. Then Y has on W orbits of lengths $2^{f-1}(2^f + 1)$, $2^{f-1}(2^f - 1)$, $d = 2^f$ except in the case $T = \text{SL}(3, 2)$ when Y is transitive on W .*

(6.3) Lemma. $\bar{c}(Q) = 0$. Moreover $\bar{c}(N_1) = 0$ or $m = 2n - 1$.

Proof. Since N_1 acts trivially on V/U the cocycle $\bar{c} : N_1 \rightarrow V/U$ is a homomorphism and as $\bar{c}(x^h) = \bar{c}(x)h$, $x \in N_1, h \in H$, this map is a morphism of H -modules. As V/U is irreducible we have $\bar{c}(N_1) = V/U$ or 0 .

Suppose $\bar{c}(N_1) = V/U$. First we claim: (*) $\bar{c}(Q) = 0$.

Assume instead $\bar{c}(Q) = V/U$. Suppose $1 \neq y \in \ker \bar{c} \cap Q$. Then choose $x \in Q$ with $c(x)y \neq c(x)$. But as $xy = yx$ and $c(y) \in U$ we obtain

$$1 = (x[c(x)]y[c(y)])^2 = x^2y^2[c(x)y + c(x)] = [c(x)y + c(x)] \neq 1,$$

a contradiction. Hence: $\bar{c} : Q \rightarrow V/U$ is an isomorphism. Also N_1/Q acts faithfully on Q but trivially on V/U showing $N_1 = Q$ and thus $|N_1| = |Q| = |V/U| = 2^{2n-m}$.

Any element $1 \neq x[c(x)] \in Q\kappa$ acts fixed-point-freely on V/U and therefore on V too. This implies that 2^{2n-m} divides $|B|$, i.e. $m \geq n + 1$. Assume first $m \neq 6$ and let r be a 2-primitive divisor of $2^m - 1$. Then r divides $|H/N_2|$ which in turn divides $|H/N_1| = |H/Q|$. This is impossible as H/N_1 is isomorphic to a subgroup of $\text{GL}(V/U) \simeq \text{GL}(2n - m, 2)$. If $m = 6$ then $n = 5$ and $2n - m = 4$. But no quotient group of $H/Q \leq \text{GL}(V/U) \simeq \text{GL}(4, 2)$ can induce a transitive subgroup of $H/N_2 \leq \text{GL}(U) \simeq \text{GL}(6, 2)$. Thus (*) holds and $N_1^{(1)}Q \leq \ker \bar{c}$.

Also $N_1/Q \simeq N_1N_2/N_2 \trianglelefteq H/N_2$ has an elementary abelian quotient of order 2^{2n-m} . Inspecting (6.2) this can only happen if $m = 2n - 1$.

(6.4) Lemma. $m = n$.

Proof. Assume that the assertion is false and let r be a 2-primitive prime divisor of $\max\{2^m - 1, 2^{2n-m} - 1\}$. Note that such a prime divisor always exists with the only exception of $n = 5$ and $m \in \{4, 6\}$. We treat the latter case at the end of the proof.

Pick $R \in \text{Syl}_r(H)$. We also may assume $R \leq K$ replacing if necessary B by a suitable translate. We distinguish two cases: (I) \bar{c} is a coboundary. Then V/U splits into two orbits $\mathcal{B}_1, \mathcal{B}_2$ with $|\mathcal{B}_1| = 1, |\mathcal{B}_2| = 2^{2n-m} - 1$ (i.e. we can assume $\bar{c} = 0$ and $\mathcal{B}_1 = \{U\}$). (II) \bar{c} is not a coboundary. By (6.2.c) V/U splits into two orbits $\mathcal{B}_1, \mathcal{B}_2$ with $|\mathcal{B}_1| = 2^{d-1}(2^d - \epsilon), |\mathcal{B}_2| = 2^{d-1}(2^d + \epsilon), 2n - m = 2d, \epsilon = \pm 1$. We also assume that B is one K -orbit while \bar{B} splits in the two remaining K -orbits. The elements of B map into one of the orbits \mathcal{B}_1 or \mathcal{B}_2 . Choosing ϵ suitably we can assume that B maps into \mathcal{B}_2 in any case. In case (II) however we have

$$2^{n-1}(2^n - 1) \leq |B| \leq |\mathcal{B}_2| \cdot |U| \leq 2^{2n-1} + \epsilon 2^{2n-d-1}.$$

Therefore $\epsilon = 1$.

CASE $n > m$. Then $R \in \text{Syl}_r(N_2)$. In case (I) R acts fixed-point-freely on \mathcal{B}_2 and hence on B too. By (2.2) $|C_V(R)| = 1$, a contradiction. But in case (II) again R acts fixed-point-freely on \mathcal{B}_2 as $C_{V/U}(R) = 0$ and $(|\mathcal{B}_1|, r) = 1$. We have the same contradiction.

CASE $n < m$. Then $R \in \text{Syl}_r(N_1)$. By (6.2) either H^U is solvable or N_1 is nonsolvable and transitive on $U - 0$.

Assume first that N_1 is nonsolvable. As a N_1/Q -module the centralizer E of the chain $0 \subset U \subset V$ is the direct sum of $2n - m$ copies of U . As $Q \leq E$ by (2.8.a.1) N_1 splits over Q , say $N_1 = LQ$, $L \leq N_1$, $L \cap Q = 1$. By (6.2.c) and (6.3) $L\kappa$ has on each coset $v + U$ either two orbits of lengths 1 and $2^m - 1$ or two orbits of lengths $2^{f-1}(2^f - 1)$, $2^{f-1}(2^f + 1)$, $m = 2f$. This implies $|B| = |\mathcal{B}_2|2^m$, $|\mathcal{B}_2|(2^m - 1)$, or $|\mathcal{B}_2|2^{f-1}(2^f \pm 1)$. But in any case $|B|_2 \neq 2^{n-1}$, a contradiction.

So assume that N_1 is solvable. Then $RQ/Q \trianglelefteq H/Q$ and $H = N_H(R)Q$ by a Frattini argument. Also $N_H(R) \cap Q = 1$ as R acts fixed-point-freely on Q . Moreover $V = U \oplus U'$, $U' = C_V(R)$ is a $N_H(R)$ -decomposition and as H has three orbits on V we see $Q \neq 1$. Assume first case (I). Any $u' \in U'$ defines a R -morphism from $Q\kappa$ into U by $x\kappa \mapsto [x\kappa, u'] = (u' + c(x))(x + 1) = u'(x + 1)$ (as $c(x) \in U$ by (6.3)). As U is R -irreducible we find an $u' \in U'$ such that $[Q\kappa, u'] = U$. But then

$$2^{n-1}(2^n + 1) \geq |B| = |\mathcal{B}_2| \cdot |U| = 2^{2n} - 2^m,$$

implying $m = 2n - 1$ and $|B| = 2^m$, a contradiction. So assume case (II). Then $H^{V/U}$ is nonsolvable, i.e. N_2 is nonsolvable. Hence N_2 contains a cyclic group $S \neq 1$, the order $|S|$ divides $2^d + 1$ and $C_V(s) = U$ for $1 \neq s \in S$. Let s be of prime order. As $(|\mathcal{B}_1|, |s|) = 1$ we have the same contradiction against (2.2) as before.

Finally we rule out the possibility $n = 5$, $m = 4$ or 6 . Using (6.2) one observes that K must contain a group $L = L_1 \times L_2$, $L_1 \leq \text{GL}(6, 2)$ and $L_2 \leq \text{GL}(4, 2)$ such that $L_2 \simeq Z_5$ and $L_1 \simeq \text{SL}(2, 8)$ or L_1 is cyclic of order 21. A Computer computation (the methods are described in the next section) shows that only standard B-sets are L -admissible.

(6.5) Lemma. \bar{c} is a coboundary.

Proof. Assume that \bar{c} is not a coboundary. Then K has on V/U two orbits $\mathcal{B}_1, \mathcal{B}_2$ of lengths $2^{d-1}(2^d - 1)$ and $2^{d-1}(2^d + 1)$, $2d = n$ by (6.2.c). Assume that B is one K -orbit and \bar{B} is the union of the two remaining orbits. Then as in the proof of (6.4)

$$B = \bigcup_{b+U \in \mathcal{B}_2} ((b+U) \cap B),$$

and

$$\bar{B} = \left(\bigcup_{b+U \in \mathcal{B}_1} (b+U) \right) \cup \bigcup_{b+U \in \mathcal{B}_2} ((b+U) \cap \bar{B}).$$

Therefore $|\bar{B}| = 2^{n-1}(2^n + 1)$. But if $0 \neq u \in U$ then

$$2^{4d-2} + 2^{2d-1} = |\bar{B} \cap (u + \bar{B})| \geq \left| \bigcup_{b+U \in \mathcal{B}_1} (b+U) \right| = 2^{4d-1} - 2^{3d},$$

a contradiction.

Remark. By the previous lemma we can and do assume (replacing B if necessary by a suitable translate) that $\bar{c} = 0$. Moreover U is invariant under K and U can not split under K into two orbits as one of the orbits would be a

B-set. Thus U is a K -orbit. We may assume wlog. that B is a K -orbit and \overline{B} is the union of U and another K -orbit. Then $|(U+v) \cap B| = |(U+v) \cap \overline{B}| = 2^{n-1}$ for every $v \in V - U$.

(6.6) Lemma. H/Q acts faithfully on U and V/U .

Proof. Assume first $n \neq 6$. Let $R \in \text{Syl}_r(H)$ where r is a 2-primitive prime divisor of $2^n - 1$.

(1) R is a cyclic group and its order r^α is the r -part of $2^n - 1$. R is faithful on U and V/U . If H/N_i is nonsolvable then $(H/N_i)^{(\infty)} = E(H/N_i)$ has an order divisible by r^α :

Using argument (E) we see that R can not contain an elementary abelian group of order r^2 . Hence R is cyclic and as $r^\alpha \parallel |H/N_i|$, $i = 1, 2$, the first assertions follow. The last one is a consequence of (6.2).

(2) Let H/N_i be nonsolvable, $i \in \{1, 2\}$. Then H/N_j , $i \neq j$, is nonsolvable too. Moreover $E(H/Q) \simeq E(H/N_1) \simeq E(H/N_2)$:

We know by (1) that r^α divides $|E(H/N_i)|$. Suppose H/N_j is solvable. Then $(H/N_j)^{(\infty)} = 1$. As r^α divides H/N_j the Jordan Hölder Theorem implies that $r^{2\alpha}$ divides $|H|$, a contradiction. Hence H/N_j is nonsolvable. If N_k/Q , $k = 1$ or 2 would be nonsolvable then $(N_k/Q)^{(\infty)} \simeq (N_k N_\ell / N_\ell)^{(\infty)} = E(H/N_\ell)$, $\{k, \ell\} = \{1, 2\}$ and again r^α divides $|H/N_k|$ and $|N_k|$, a contradiction. Hence N_k/Q is solvable for $k = 1, 2$.

Set $\overline{H} = H/Q$. The map $\overline{H} \ni \overline{h} \mapsto (\overline{hN_1}, \overline{hN_2}) \in \overline{H}/\overline{N_1} \times \overline{H}/\overline{N_2}$ is a monomorphism and it projects surjective on both components. Hence \overline{H} has precisely one nonsolvable composition factor which occurs in $E(\overline{H})$ as well as in $E(\overline{H}/\overline{N_k})$, $k = 1, 2$. Using (6.2) we get assertion (2).

(3) The assertion of the lemma holds if H is nonsolvable:

Suppose $1 \neq \overline{N_2}$. Then $\overline{N_2} \simeq \overline{N_2 N_1} / \overline{N_1}$ is a solvable normal subgroup of $\overline{H}/\overline{N_1}$. Therefore this group is cyclic of odd order and is contained in $C_{\overline{H}/\overline{N_1}}(E(\overline{H}/\overline{N_1}))$. Then $N_2 = CQ$ with a cyclic group C of odd order. As C has odd order wlog. $C \leq K$ and $C_V(C) = U$, which contradicts (2.2).

So assume $1 \neq \overline{N_1}$. The same argument as before shows $N_1 = CQ$, $C \leq K$ is a cyclic group of odd order and $V = U \oplus U'$ with $U' = C_V(C)$. A Frattini argument shows $H = QN_H(C)$ and $Q \cap N_H(C) = 1$ as $C_Q(C) = 1$. Now $\overline{c} = 0$ implies $N_H(C) \leq K$. Lemma (2.2) excludes the possibilities $U' \subseteq B$ or \overline{B} . As $N_H(C)$ is transitive on $U' - 0$ we may therefore assume $U' \cap \overline{B} = 0$, $U' \cap B = U' - 0$. Then $|B \cap (B+u') \cap U'| = 2^n - 2$ for $0 \neq u' \in U'$ and C acts semiregularly on $(B \cap (B+u')) - U'$. Thus $|C|$ divides $(2^n - 1, 2^{n-1}(2^{n-1} - 1) - (2^n - 2)) = 1$, a contradiction.

(4) The assertion of the lemma holds if H is solvable:

Now $RN_i/N_i \trianglelefteq H/N_i$. Therefore $[\overline{N_i}, \overline{R}] \leq \overline{R} \cap \overline{N_i} = 1$. Now we can use the same arguments as in (3) to obtain $N_1 = N_2 = Q$.

Finally if $n = 6$ one can modify our arguments suitable using the primes 3 and 7 instead of r . We leave the details to the reader.

(6.7) Lemma. Q contains a H -invariant subgroup Q_0 such that Q/Q_0 and U are isomorphic as H/Q -modules.

Proof. Since $c(H) \subseteq U$ we can dismiss the symbol c_2 and we identify from now on c with c_1 . As U is a trivial Q -module $c : Q \rightarrow U$ is even a group homomorphism and a quick computation shows that this map is even a H/Q -morphism. Set $Q_0 = \ker c$. As U is irreducible either $Q = Q_0$ or $U \simeq Q/Q_0$ as H/Q -modules.

Assume $Q = Q_0$. Then $\bar{c}(hQ) = c(h)$ defines a 1-cocycle of H/Q into U which is not a 1-coboundary. By (6.2) we see $\mathrm{Sp}(n/b, 2^b)^{(1)} \trianglelefteq H/Q$ or $\mathrm{G}_2(2^b) \trianglelefteq H/Q$, $n = 6b$, and the image $c(H) = \bar{c}(H/Q)$ has size $2^{d-1}(2^d \pm 1)$, $n = 2d$. But then U is not a K -orbit, a contradiction.

Remark. In the following lemma we investigate the case where H is nonsolvable. By (6.2) there exists $Q \trianglelefteq T \trianglelefteq H$ such that T/Q is quasisimple. As T has three orbits on V we can assume $H = T$. Because $\mathrm{SL}(2, 2^{ab}) \leq \mathrm{Sp}(2a, 2^b)$ we also dismiss the case $H/Q \simeq \mathrm{Sp}(2a, 2^b)$, $a > 1$.

Suppose $H/Q \simeq \mathrm{SL}(a, 2^b)$, $a \geq 3$. We identify U with the natural module $M = V(a, 2^b)$ (considered as a $\mathrm{GF}(2)[H/Q]$ -module). Then V/U considered as a $\mathrm{GF}(2)[H/Q]$ -module is isomorphic to M^* : Otherwise this module is isomorphic to M as a $\mathrm{GF}(2)[H/Q]$ -module. By (2.3) and (2.4) Q is isomorphic to a submodule of $\bigoplus_{i=0}^{b-1} M^* \otimes M\varphi^i$, φ the Frobenius automorphism. None of the modules $M^* \otimes M\varphi^i$ has a composition factor isomorphic to M as a $\mathrm{GF}(2)[H/Q]$ -module, a contradiction to the preceding lemma.

(6.8) Lemma. *Let H be nonsolvable. Then assertions (a)-(c) of theorem D hold.*

Proof. According to the above remark and (6.2) we only have to consider the cases $H/Q \simeq \mathrm{SL}(a, 2^b)$, $n = ab, a > 1$, or $H/Q \simeq \mathrm{G}_2(2^b)$, $6b = n$. By (2.9) H contains a subgroup X_0 with $H = X_0Q$, $X_0 \cap Q = 1$. We now use the notations of (2.4-5). As $U \simeq M$, $V/U \simeq M^*$ the group E has a decomposition as

$$E = \bigoplus_{i=0}^{b-1} M_i, \quad M_i \simeq M \otimes M\varphi^i,$$

φ the Frobenius automorphism. M_i has the composition factor M iff $i = 0$ and then N_2/N_1 is the unique section with this property (for the G_2 -case we use theorem 6 of the appendix). As Q is a submodule of E we deduce from (6.7) that $Q \cap M_0 = N_2$. Set $N = N_2\kappa = \{y[c(y)] \mid y \in N_2\}$. Then $c : N_2 \rightarrow U$ is a H/Q -morphism with kernel N_1 . Note that N lies in the 2-radical $O_2(\mathrm{Aut}(B^0)_U)$ of the stabilizer of U in the automorphism group of a suitably chosen standard B-set B^0 . Also E_1 lies in this radical. Therefore any N -orbit is invariant under E_1 . This implies that $NE_1 \leq Q\kappa$, $N_2E_1 \leq Q$.

We observe that X_0Q has three orbits. Our goal for the remainder of the proof is to show that X_0 can be chosen in such a way that $NX_0\kappa$ can be identified with a subgroup of the automorphism group of a standard B-set or a parabolic B-set of the kind we like to classify. Since the orbits of $NX_0\kappa$ recover the B-set we can identify then B with the desired type. In particular if we can show $X_0 \leq H \cap K$ and that U has a X_0 -invariant complement we know that our B-set is standard or standard parabolic.

CASE $H/Q \simeq \text{SL}(a, 2^b)$, $a > 3$. Here $H^1(X_0, M) = 0$ and $H^1(X_0, M_i) = 0$ for $i > 0$ and $H^1(X_0, \wedge^2 M) = 0$ [Be ; 3.1, 3.2]. This shows that c restricted to X_0 is a coboundary and replacing K if necessary by a suitable conjugate we can assume $X_0 \leq H \cap K$. Also by the structure of E the vanishing of the cohomology groups shows that U has a X_0 -invariant complement. Thus B is standard or standard parabolic.

For the remaining cases we choose a basis $\mathcal{B}_1 = \{u_1, \dots, u_n\}$ of U and extend it with $\mathcal{B}_2 = \{w_1, \dots, w_n\}$ to a basis $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2$ of V . Let $D(x)$, $x \in H$ be the matrix of x_U with respect to \mathcal{B}_1 . We choose \mathcal{B}_2 in such a way that $x_{V/U}$ has with respect to \mathcal{B}_2 (modulo U) the matrix $D(x)^{-t}$. With respect to \mathcal{B} one has a representation for x as:

$$\begin{pmatrix} D(x) & 0 \\ 0 & D(x)^{-t} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \Phi(x) & 1 \end{pmatrix}$$

Here the second matrix represents an element from E . According to the decomposition of E we write $\Phi(x) = \sum_{i=0}^{b-1} \Phi_i(x)$ where $\Phi_i(x)$ represents the part which lies in M_i . The maps $\Phi_i : X_0 \rightarrow M_i$ are 1-cocycles.

CASE $H/Q \simeq \text{SL}(3, 2^b)$. Again as $H^1(X_0, M) = 0$ we can assume $X_0 \leq H \cap K$. This time $H^1(X_0, M_i) = 0$ except for $i = 1$ or $b - 1$. Modifying the elements in \mathcal{B}_2 with suitable elements from U we can achieve for $i \neq 1, b - 1$ that $\Phi_i(x) = 0, x \in X_0$. Set $W = E_1 \cap (M_1 \oplus M_{b-1})$ and $W_1 = M_1 \oplus M_{b-1}$. Now $x \mapsto \Phi(x) + W$ defines a 1-cocycle of X_0 into W_1/W . If this map is a coboundary we can adjust the elements in \mathcal{B}_2 with suitable elements from U in such a way that $\Phi(x) \in W$ for $x \in X_0$. As $W \leq E_1$ we can replace X_0 by a group $X_1 \leq X_0 W \leq K$, $X_1 \simeq X_0$, such that $\Phi(x) = 0$ for $x \in X_1$. Now with X_1 in the role of X_0 we conclude that B is standard or standard parabolic.

Suppose now that the above map is not a coboundary. Then $X_0 = X_\Phi$ in the sense of (3.1.c). We conclude that B is a special parabolic B-set.

CASE $H/Q \simeq \text{SL}(2, 2^b)$. Again $H^1(X_0, M_i) = 0$ for $i > 0$. Therefore we can assume $\Phi(x) \in M_0, x \in X_0$. Suppose that $c : X_0 \rightarrow U$ is not a coboundary. We claim that we can replace $X_0 \kappa$ by a suitable subgroup $X_1 \leq X_0 \kappa N$ such that $X_1 \leq H \cap K$. Consider the X_0 -module $W = (U + N_2)/N_1 \simeq M \oplus M$. Then $x \mapsto (\Phi(x) + c(x)) + N_1$ defines a 1-cocycle of X_0 into W . The submodule N/N_1 of W projects surjectively on both components N_2/N_1 and $(U + N_1)/N_1$. We can adjust x by a suitable element $n(x) \in N$ such that we obtain a group $\hat{X} = \langle x \kappa n(x) \mid x \in X_0 \rangle \leq H \cap K$ with $\hat{X} \cap N_2 \leq N_1$. As the Schur multiplier of $\text{SL}(2, 2^b)$, $b > 2$, is trivial we find inside of \hat{X} a group $X_1 \simeq X_0$. Thus renaming X_1 by X_0 we now have $X_0 \leq H \cap K$ and $\Phi(x) \in M_0$. By (2.8.b) however $H^1(X_0, M_0) = 0$ (or use [Al; thm. 3]). So as usual B is standard or standard parabolic.

CASE $H/Q \simeq \text{G}_2(2^b)^{(1)}$. Assume first $b \neq 2$. Then $H^1(X_0, M_i) = 0$ for $i > 0$. As in the case before we may assume that $\Phi_i(x) = 0$ for $x \in X_0$. If c restricted to X_0 is not a coboundary we can argue as in the previous case and replace X_0 by a group $X_1 \leq H \cap K$, $X_1 \simeq X_0$. So assume $X_0 \leq H \cap K$ anyway. $M_0/N_2 \simeq A \oplus F$ where $F = \text{GF}(2^b)$ is the trivial module and A the adjoint

module. Apply theorem 6 of the appendix. So adjusting \mathcal{B}_2 again we achieve $\Phi(x) \in N_2$. Then by (2.8.b) Φ restricted to X_0 is a coboundary into N_2 . So as usual B is standard or standard parabolic.

Next we turn to the case $b = 2$. Arguing as before we can assume $X_0 \leq H \cap K$ and Φ_0 restricted to X_0 is trivial. Consider the module $W = M_1/(M_1 \cap E_1)$. Then $x \mapsto \Phi_1(x) + (M_1 \cap E_1)$ defines a 1-cocycle from X_0 into W . Now we argue completely similar as in the case $H/Q \simeq \text{SL}(3, 2^b)$: If this map is a coboundary B is standard or standard parabolic and if it is not a coboundary B is sporadic parabolic.

Remark. In the special or sporadic parabolic case we have at most two equivalence classes (up to complementation): Let $C \simeq \text{GF}(2^b)^*$ be the centralizer of $\{D(x) \mid x \in X_0\}$ in $\text{GL}(n, 2)$ where $X_0 \simeq \text{SL}(3, 2^{n/3})$ or $\text{G}(2^{n/6})$ and let X be the group of block diagonal matrices of the form $\text{diag}(D(x), D(x)^{-t})$, $x \in X_0$. Then the block diagonal matrices with diagonal (z, z^{-t}) , $z \in C$ induce a transitive action on $H^1(X, M_0/N_2)$. Choose any cocycle $\Phi \in C^1(X_0, M_0/N_2)$ and define X_Φ as in (3.1). Then the two orbits of $X_\Phi N$ on $V - U$ represent at most two equivalence classes of B-sets.

The next lemma is useful to reduce the number of cases which have to be considered when H is solvable.

(6.9) Lemma. *Let $X \leq \Gamma\text{L}(1, F)$, $F = \text{GF}(2^n)$, be transitive on $F^* = F - 0$. Then X contains a sharply transitive subgroup.*

Proof. Let ω be a generator of F^* . Then $Y = \Gamma\text{L}(1, F)$ is generated by the maps z and φ with $z : x \mapsto \omega x$, $\varphi : x \mapsto x^2$. Set $e = |Y : X \langle z \rangle|$, $m = n/e$, $\langle a \rangle = X \cap \langle z \rangle$ and $d = |\langle z \rangle : \langle a \rangle|$. Then $X = \langle a, b \rangle$ with $a : x \mapsto \omega^d x$, $b : x \mapsto \omega^t x^q$, $q = 2^e$, t suitable.

(1) d divides $(q^m - 1, m)$ and $(d, t) = 1$:

We have $m = |X \langle z \rangle : \langle z \rangle| = |X : \langle a \rangle|$ and as $q^m - 1$ divides $|X|$ we see that $d = (q^m - 1)/|\langle a \rangle|$ divides m and the first assertion follows. Since $X = \langle a \rangle \langle b \rangle$ we see that the orbit of 1 under X lies in the group $\langle \omega^d, \omega^t \rangle \leq F^*$. Transitivity of X on F^* implies the second assertion.

We now proceed by induction on m/d . If $m = d$ then $|X| = q^n - 1$ and we are done. So assume $m = df$, $f > 1$. We get:

(2) $q^d \equiv 1 \pmod{(q-1)d}$ and $q^i \not\equiv 1 \pmod{(q-1)d}$ for $1 \leq i < d$:

The stabilizer X_1 of 1 in X has order f . As $X/\langle a \rangle$ is cyclic and $X_1 \cap \langle a \rangle = 1$ we have $X_1 \leq \langle a, b^d \rangle$ and $\langle a \rangle X_1 = \langle a, b^d \rangle$. Therefore

$$1 \cdot b^d = \omega^{t \frac{q^d - 1}{q - 1}}$$

lies in the orbit of 1 under $\langle a \rangle$. By (1) d divides $q^m - 1$ and therefore $q^d \equiv 1 \pmod{(q-1)d}$. Assume $q^i \equiv 1 \pmod{(q-1)d}$ for some i between 1 and $d-1$. Choose $\lambda \in \mathbf{Z}$ such that $\lambda d = t(q^i - 1)/(q-1)$. Then $b^i a^{-\lambda}$ fixes 1 which is in conflict with $b^i a^{-\lambda} \in X - \langle a, b^d \rangle$. We apply now [HB; XII, (9.6)] to obtain:

(3) Every prime divisor of d is also a divisor of $q-1$.

Suppose the prime r divides f but not d . Then $X = X_1 \langle a, b^r \rangle$ so that $\langle a, b^r \rangle$ is transitive on F^* and we are done by induction. So assume that every prime divisor of f also divides d . Then:

(4) Every prime divisor of m also divides $q - 1$.

By (1) and (4) the group $\langle a^f, b \rangle$ satisfies the assumptions of [HB; XII, (9.7)] and is therefore sharply transitive.

Let $m = ds$, $q = 2^s$, such that $\{q, d\}$ is a Dickson pair in the sense of [Lü, p. 33]. For the corresponding Dickson nearfield group $X \leq \Gamma\text{L}(1, F)$, $F = \text{GF}(q^d)$ we can choose generators a, b such that

$$xa = \omega_0 x, \quad xb = \omega x^q, \quad x \in F,$$

where ω is a suitable generator of F^* and $\omega_0 = \omega^d$. Note that $b^d = a^\mu$ with $\mu = (q^d - 1)/d(q - 1)$. With this notation we have:

(6.10) Lemma. *Let $D : X \rightarrow \text{GL}(F)$ be a faithful representation. Then there exists a number k , $(k, (q^d - 1)/d) = 1$, such that D is up to $\text{GF}(2)[X]$ -equivalence defined by $xD(a) = \omega_0^k x$, $xD(b) = \omega^k x^q$, $x \in F$.*

Proof. Up to $\text{GF}(2)[X]$ -equivalence one has

$$xD(a) = \omega_0^k x, \quad xD(b) = \omega^\ell x^{q^i}, \quad x \in F,$$

for some numbers i, k, ℓ with $(k, (q^d - 1)/d) = 1$. As $a \mapsto D(a)$, $b \mapsto D(b)$ induces an isomorphism we get $i = 1$. Now $D(a)^\mu = D(b)^d$ implies $\omega^{d\mu k} = \omega^\ell \frac{q^d - 1}{q - 1} = \omega^{d\mu\ell}$. Hence $\omega^\ell = \omega^k \nu$ with $\nu \in \langle \omega^{q-1} \rangle$. Choose an integer t such that $\nu = (\omega^t)^{q-1}$. Then $D(a^{z^t}) = D(a)$ and $xD(b^{z^t}) = \omega^k x^q$ where z is defined as in the proof of previous lemma. The assertion follows.

(6.11) Lemma. *Let H be solvable. Then assertion (d) of theorem D holds.*

Proof. By (6.9) H/Q contains a subgroup which is sharply transitive on $V/U - 0$. Hence H has a subgroup D of order $2^n - 1$ which has the same property. By (2.2) D sharply transitive on $V/U - 0$ too. Therefore we may assume $H = DQ$, $Q \leq H \cap K$ and D is cyclic of order $2^n - 1$ or a nearfield group belonging to a Dickson nearfield (see [HB; XII, (9.7)] for instance). Also by Maschkes theorem Q is a completely reducible D -module. In particular $Q = Q_0 \oplus Q_1$ with D -modules Q_i where $Q_0 = K \cap Q$ and Q_1 is D -isomorphic to U . We identify $V = F \oplus F$ and $U = F(1, 0)$. ω will denote a generator of F^* . As usual E is the centralizer of the chain $0 \subset U \subset V$ in $\text{GL}(V)$.

Assume first $D = \langle z \rangle$ is cyclic and that z is the mapping $(x, y) \mapsto (\omega x, \omega^k y)$, $(k, 2^n - 1) = 1$ (like in (3.2)). By (2.14.b) (see also (5.2.b), (5.4.b)) there is precisely one pair $0 \leq a, b \leq n - 1$ with $2^b \equiv 1 - 2^a k \pmod{2^n - 1}$ such that $U \simeq_D T_a \leq E$ where T_a is defined as in the introduction to section 5. Hence

$$Q_1 \kappa = \{t_a(\beta^{2^b})[(c_0 \beta, 0)] \mid \beta \in F\}$$

with $0 \neq c_0 \in F$ suitable. A transformation with the operator $(x, y) \mapsto (c_0^{-1}x, c_0^{-2^a}y)$ shows that we may assume $c_0 = 1$ (i.e. $Q_1 \kappa = Y_{a,b}$ in the notation of section 5). However the orbits of lengths $2^{n-1}(2^n - 1)$ of $DQ_1 \kappa$ and their unions with U are B-sets of the desired cyclic trace type.

Assume now that D is not cyclic. So we are in the situation of (6.10) and with that notation we have $n = ds$, $q = 2^s$, $s > 1$ and $\{q, d\}$ is a Dickson pair. Moreover $D = \langle \rho, \sigma \rangle$ and there exists a number k , $(k, (q^d - 1)/d) = 1$, such that

$$(x, y)\rho = (\omega_0 x, \omega_0^k y), \quad (x, y)\sigma = (\omega x^q, \omega^k y^q),$$

$\omega_0 = \omega^d$. By (2.14.b) there is exactly one module $U \simeq_D T_a \leq E$. Hence we have a unique number b with $(b, n) = 1$ such that $\omega_0^{1-2^a k} = \omega_0^{2^b}$ and $Q_1 \kappa$ contains an element of the form $t_a(e)[(1, 0)]$, $e \in F^*$ suitable. As

$$(t_a(e)[(1, 0)])^{\rho^x} = t_a(e\omega_0^{x2^b})[(\omega_0^x, 0)]$$

we have

$$Q_1 \kappa = \{t_a(eu^{2^b})[(u, 0)] \mid u \in F\}.$$

Also as $Q_1 \kappa$ leaves invariant a B-set $|Q_1 \kappa_{(0,1)}| = 2$ and there is some $u_0 \in F^*$ with $(0, 1)t_a(eu_0^{2^b})[(u_0, 0)] = (0, 1)$, i.e. $eu_0^{2^b} = u_0$. Thus we can represent $Q_1 \kappa$ in the form

$$Q_1 \kappa = \{t_a(u_0 u^{2^b})[(u_0 u, 0)] \mid u \in F\}.$$

We have $\omega^{1-2^a k} = \omega^{2^b} \nu$ for some $\nu \in (F^*)^{(q^n - 1)/d}$. Therefore

$$(t_a(u_0)[(u_0, 0)])^\sigma = t_a(u_0^q \omega^{1-2^a k})[(u_0^q \omega, 0)] = t_a(u_0^q \nu \omega^{2^b})[(u_0^q \omega, 0)] \in Q_1 \kappa$$

and thus $u_0^{q-1} \nu \omega^{2^b} = (u_0^{q-1} \omega)^{2^b}$ showing

$$\nu = u_0^{(q-1)(2^b-1)} \text{ and } u_0 \in (F^*)^{(q^n-1)/d(q-1)}.$$

We compute the orbit $\Sigma = (0, 1)Q_1 \kappa D$. First

$$\Sigma_0 = Q_1 \kappa \langle \rho \rangle = \{(u_0(u^{2^b} + u)\alpha, \alpha^k) \mid \alpha \in \langle \omega_0 \rangle, u \in F\}.$$

Next

$$(u_0(u^{2^b} + u)\alpha, \alpha^k)\sigma^i = (u_0^{q^i}(u^{2^b} + u)^{q^i} \alpha^{q^i} \omega^{\frac{q^i-1}{q-1}}, \alpha^{kq^i} \omega^{k\frac{q^i-1}{q-1}}).$$

Since the Frobenius automorphism fixes $\langle \omega_0 \rangle$ and the set of elements with trace 0 we get

$$\Sigma = \bigcup_{i=1}^d \{(u_0^{q^i}(u^{2^b} + u)\alpha \omega^{\frac{q^i-1}{q-1}}, \alpha^k \omega^{k\frac{q^i-1}{q-1}}) \mid \alpha \in \langle \omega_0 \rangle, u \in F\}.$$

Set $\mu = u_0^{q-1}$. Then

$$\Sigma = \bigcup_{i=1}^d \{(u_0(u^{2^b} + u)\alpha(\mu\omega)^{\frac{q^i-1}{q-1}}, \alpha^k \omega^{k\frac{q^i-1}{q-1}}) \mid \alpha \in \langle \omega_0 \rangle, u \in F\}.$$

By [Lü, p. 32, (4)] d divides $(q^d - 1)/(q - 1)$ and any prime divisor of d also divides $q - 1$. Hence every prime divisor of $q^d - 1$ also divides $(q^d - 1)/d$. Now $\mu \in (F^*)^{(q^d - 1)/d}$, i.e. $\mu = \omega^{a(q^d - 1)/d}$ and $|\omega^{1+a(q^d - 1)/d}| = |\omega| = q^d - 1$. Therefore there is a number x of the form $x = y(q^d - 1)/d$ with $\omega^{x(1+a(q^d - 1)/d)} = \omega^{-ka(q^d - 1)/d}$ showing $(\mu\omega)^{k+x} = \omega^k$. Also we have $\alpha^{k+x} = \alpha^k$. Thus

$$\Sigma = \{(u_0(u^{2^b} + u)\alpha, \alpha^{k+x}) \mid \alpha \in F^*, u \in F\}.$$

We conclude that our B-set has cyclic trace type.

7 Computations

In this section we discuss computational methods for bent functions and results obtained by computer calculations. To compute automorphisms of a B-set or to test two B-sets on equivalence are closely related problems. A key for a successful approach to these problems are effective invariants. We discuss two invariants displayed in (7.1-2) below which lead to an acceptable performance of equivalence and automorphism programs. These procedures were written in the GAP code. We further present various results on B-sets obtained by computer applications in dimensions 8,10, and 12. For details, a descriptions of more results, and relevant files in GAP format the reader is referred to my homepage: www.mathematik.uni-kl.de/~dempw/

(7.1) Plane Matrices and Intersection Numbers. Let B be a B-set in $V = V(2n, 2)$.

(1) Choose $u \in B$. Define a symmetric matrix $P = P^u(B) = (p_{vw})$; $v, w \in B$, the *plane matrix* with respect to (B, u) by

$$p_{vw} = \begin{cases} 0, & u + v + w \notin B, \\ 1, & u + v + w \in B. \end{cases}$$

I.e. $p_{vw} = 1$ means that the affine plane determined by u, v, w lies completely in B . Of course also for any nonempty subset of B on can define similarly plane matrices.

(2) For $v_1, \dots, v_k \in B$ denote by $x_B(v_1, \dots, v_k)$ the number of blocks in $\mathbf{D}(B)$ which contain v_1, \dots, v_k .

(7.2) Applications. Recall that a frame $\mathcal{F} = \{u_0, \dots, u_{2n}\}$ in $V = V(2n, 2)$ is a set of vectors such that for all $0 \leq k \leq 2n$ the sets $\mathcal{B}_k = \{u_i - u_k \mid 0 \leq i \leq 2n, i \neq k\}$ are bases. Any pair $\mathcal{F}, \mathcal{F}'$ of frames determines a unique affine transformation $\beta \in \text{AGL}(V)$ with $u'_i = u_i\beta$, $0 \leq i \leq 2n$, where $\mathcal{F}' = \{u'_0, \dots, u'_{2n}\}$. Let B, B' be B-sets in V .

(1) Our first application describes the core of an inductive algorithm for the computation of $\text{Aut}(B)$ or for a test on the equivalence of B and B' .

Suppose that we have reached the following situation: $\mathcal{F} = \{u_0, \dots, u_{2n}\} \subseteq B$ is a fixed frame and $\mathcal{F}'_0 = \{u'_0, \dots, u'_{k-1}\}$ is a partial frame in B' such that there exists possibly an affine transformation sending B into B' and u_i onto u'_i , $0 \leq i \leq k-1$.

Find if possible all candidates $u'_k \in B'$ such that $\mathcal{F}'_0 \cup \{u'_k\}$ is a partial frame with the same property!

The invariants now decide if we allow $u'_k \in B' - \mathcal{F}'_0$ to be a candidate: Let $P = P^{u_0}(B) = (p_{vw})$ be the plane matrix with respect to (B, u_0) and $P' = P^{u'_0}(\mathcal{F}'_0 \cup \{u'_k\}) = (p'_{v'w'})$ be the plane matrix with respect to $(\mathcal{F}'_0 \cup \{u'_k\}, u'_0)$. Then u'_k is admissible iff:

I $(p_{u_i u_j}) = (p'_{u'_i u'_j})$ for $1 \leq i, j \leq k$.

II $x_B(u_0, \dots, u_k) = x_{B'}(u'_0, \dots, u'_k)$.

This sets up in an obvious way an inductive procedure for an equivalence test or a procedure for the computation of the automorphism group of a B-set. The pattern of such an algorithm is outlined for instance in [CD].

(2) Next we describe an invariant derived from the plane matrix which allows us to detect nonequivalence of B-sets before we have to enter the more costly computations of (1). Let P^u be the plane matrix of B with respect to $u \in B$. Set $S^u = (P^u)^2 = (s_{vw}^u)$. The diagonal entry s_{vv}^u counts the number of affine planes in B which contain u, v . The nondiagonal entry s_{vw}^u , $v \neq w$, counts the number of pairs of affine planes in B which contain u, v and u, w respectively and whose intersection has size 2. Let S_{v*}^u be the v -th row ordered decreasingly and let T_u be the set of these rows ordered lexicographically. Finally denote by $\mathcal{T}(B)$ be the set of T_u , $u \in B$. A B-set B' can only be equivalent to B if:

$$\text{III } \mathcal{T}(B) = \mathcal{T}(B').$$

Thus $\mathcal{T}(B) \neq \mathcal{T}(B')$ means that B and B' are inequivalent. In our applications it turned out that a pair B, B' of B-sets always was equivalent if the equation (III) did hold.

(3) The invariant $\mathcal{T}(B)$ also induces a partition of B according to the different values of T_u for $u \in B$. If this partition is nontrivial the expense for the computation of automorphisms is reduced substantially.

Remark. Our main applications of the routines in (7.2) were in dimension 8. The precalculation of the invariant $\mathcal{T}(B)$ is already rather time consuming in dimension 10. In practise it turned out that the simultaneous use of both invariants is advisable as for special examples the use of only one invariant led to a poor performance.

There are also other ways to compute the automorphism groups of B-sets. One can describe $\mathbf{D}(B)$ by the incidence graph and use the GRAPE-package for GAP of L. Soicher to compute $\text{Aut}(\mathbf{D}(B))$. Then one obtains $\text{Aut}(B)$ by computing $N_{\text{Aut}(\mathbf{D}(B))}(V)$ with GAP. MAGMA [MAG] has in particular powerful procedures which determine automorphisms and isomorphisms of designs and can therefore be applied to $\mathbf{D}(B)$.

Both approaches work effectively - MAGMA in particular - and produce even more (namely $\text{Aut}(\mathbf{D}(B))$ instead of only $\text{Aut}(B)$). However for certain B-sets in dimension 10 it turns out that the verification of the inequivalence via the invariant $\mathcal{T}(B)$ is less expensive than the use of the equivalence procedure of MAGMA.

We will call a B-set $B \subseteq V$ irreducible, solvable, nonsolvable etc. if $H = \text{Aut}(B)[V]_0$ is an irreducible, solvable, nonsolvable etc. subgroup of $\text{GL}(V)$.

(7.3) Computations in Dimension 8. Set $V = V(8, 2)$.

(a) **B-sets of Partial Spread Type.** A partial spread \mathcal{S} in $V(2n, 2)$ is a collection of n -dimensional subspaces which intersect pairwise trivially. A partial spread is a spread if $|\mathcal{S}| = 2^n + 1$ and there is a well known correspondence

between spreads and translation planes. In dimension 8 there are precisely 8 nonisomorphic spreads $\mathcal{S}_1, \dots, \mathcal{S}_8$ [DR]. Let \mathcal{T} be a partial spread of size $2^{n-1}+1$ in $V(2n, 2)$. Then

$$B_{\mathcal{T}} = \bigcup_{X \in \mathcal{T}} X$$

is a B-set [Di1], [Di2]. We showed that up to equivalence there are precisely 543 B-sets $B = B_{\mathcal{T}}$ such that \mathcal{T} lies in one of the spreads $\mathcal{S}_1, \dots, \mathcal{S}_8$. It turned out that the automorphism groups of these B-sets $B_{\mathcal{T}}$ were usually quite small: we obtained in 166 cases $|\text{Aut}(B_{\mathcal{T}})| = 1$, in 133 cases $|\text{Aut}(B_{\mathcal{T}})| = 2$, and in 71 cases $|\text{Aut}(B_{\mathcal{T}})| = 3$. Of course non embeddable partial spreads of size 9 may produce even more B-sets.

(b) B-sets of Trace Type. Set $F = \text{GF}(16)$, $F_0 = \{\beta \in F \mid \text{tr } \beta = 0\}$, and identify $V = F \oplus F$. For any $\pi \in \text{Sym}(F^*) = \text{Sym}(15)$ we define the B-set (see (3.1))

$$B_{\pi} = \{(\alpha\beta, \alpha^{\pi}) \mid \alpha \in F^*, \beta \in F_0\}.$$

We used a random choice procedure of GAP to pick 500 permutations π . The equivalence test reduced the set of B-sets to a set of 456 nonequivalent B-sets. As orders of $\text{Aut}(B)$ we got 32, 64, 128, 192, 256 with multiplicities 429, 24, 1, 1, 1.

(c) Irreducible B-sets. Set $V = V(8, 2)$ and let B be a B-set with $K = \text{Aut}(B)$ such that $H = K[V]_0$ is irreducible. The following lemma is easy to verify:

Lemma. *Let $H \leq G(V)$ be irreducible. Then H contains a subgroup H_0 such that one of the following holds:*

- (a) $H_0 \simeq C_{15}$ or C_{17} is semiregular.
- (b) $H_0 \simeq C_5 \times C_5$.
- (c) $H_0 \leq C_3 \text{ wr } C_4$ or $\leq C_3 \text{ wr } E_4$ and H_0 is irreducible.
- (d) H_0 is a Frobenius-group of order 18 or 21.

In all case $O(H_0)$ acts fixed-point-freely on V . So if B is a B-set with $H = \text{Aut}(B)[V]_0$ as before we can even assume $H_0 \leq K$. This sets up a naive but feasible computer search:

For all cases we computed all unions of H_0 -orbits which formed B-sets of size 120. The union of all B-sets was reduced by equivalence and the automorphism group was tested on irreducibility.

It turned out that only 5 B-sets are irreducible and except for the standard B-set all automorphism groups are solvable.

For dimensions 10 and 12 we were mainly interested in irreducible B-sets with a nonsolvable automorphism group. For various almost simple groups H we turned to the ATLAS home page [At] to obtain the concrete matrix representations $D : H \rightarrow \text{GL}(V)$. We also set up a straightforward GAP-procedure which did calculate $H^1(D(H), V)$ as well as concrete descriptions of 1-cocycles

$c : D(H) \rightarrow V$. The various representatives of 1-cocycles $c_1 = 0, c_2, c_3, \dots$ produced various candidates $K_1 (= H), K_2, K_3, \dots$ for stabilizers of B-sets. As before in all these cases unions of K_i -orbits which form B-sets have been calculated.

(7.4) Some Irreducible B-sets in Dimension 10. Set $V = V(10, 2)$. The group $H = \text{PSL}(2, 11)$ has an absolutely irreducible representation $D_1 : H \rightarrow \text{GL}(V)$ such that $H^1(D_1(H), V) = 0$. Besides the standard B-set of size 496 this representation also produces a B-set of size 496 with $\text{Aut}(B) \simeq \text{PGL}(2, 11)$. There are also two irreducible, but not absolutely irreducible representations $D_i : H \rightarrow \text{GL}(V)$, $i = 2, 3$, with $\dim H^1(D_i(H), V) = 1$ resulting in 4 candidates for K . However no candidate produced B-sets. Our results on irreducible, solvable B-sets are incomplete: The group $E_{81} \cdot C_5$ only produced the standard B-set and the semiregular group $C_{31} \times C_3$ produced no B-set at all. An irreducible group $C_{31} \cdot C_2$ has on $V - 0$ one orbit of length 62 and 31 nontrivial orbits of length 31 and the irreducible, semiregular group C_{11} has 93 orbits. Therefore our usual naive approach is not suitable in both cases.

(7.5) Some Irreducible B-sets in Dimension 12. Set $V = V(12, 2)$. The group $H_0 = \text{Aut}(\text{SL}(3, 2))$ has a completely reducible representation on V with two isomorphic composition factors of dimension 6. Hence $H = H_0 \times C_3$ has an irreducible representation on V . This group produced 9 irreducible B-sets of size 2016 among them one standard B-set. The triple cover $H_0 = 3.\text{Alt}(6)$ of $\text{Alt}(6)$ has a representation on V such that $V = V_1 \oplus V_2$ is a decomposition into nonisomorphic, irreducible $\text{GF}(2)[H_0]$ -modules of dimension 6. $N_{\text{GL}(V)}(H_0)$ contains an involution u interchanging V_1 and V_2 . The group $H = H_0 \langle u \rangle$ produced 5 irreducible B-set among them one standard B-set.

Final Remarks. (1) The proofs of theorems A-D almost exclusively relied on group theory. In particular the computation of the harmless, solvable automorphism groups of B-sets of cyclic trace type required rather involved results about simple groups! It would be desirable if one could find geometric means - like invariants useful for theoretical applications - which would lead to better, more illuminating proofs.

(2) The B-sets in dimensions ≤ 6 have been classified by Kibler and Rothaus (see [Di1], [Di2], [Ro]). For dimensions 2 and 4 only the standard B-sets occur and for dimension 6 there are up to equivalence and complementation only four B-sets. The above computer applications indicate that already in dimension 8 the enumeration of all B-sets is not only a difficult problem but in view of the large number of B-sets is also not a very sensible task.

(3) Our computations in dimensions 8 to 12 indicate that irreducible, nonsolvable B-sets are rare. So the construction of series of irreducible, nonsolvable bent functions (V, f) is an interesting problem. However one should add a condition like $\deg f \geq c \cdot \dim V$ where c is a constant in order to avoid examples like the following:

Let (V_i, f_i) , $1 \leq i \leq r$, be bent functions. Then $f = f_1 + \dots + f_r$ is a bent function on $V = V_1 \oplus \dots \oplus V_r$ (see [Di1] for instance). If in particular all the

(V_i, f_i) 's are pairwise equivalent we see that

$$\text{Aut}(f_1) \text{ wr } \text{Sym}(r) \leq \text{Aut}(f).$$

Moreover $\text{Aut}(f)$ is irreducible if f_1 is irreducible. In view of (5.5-7) we have for $\dim V \in \{8r, 10r, 12r\}$, $r \geq 1$, irreducible, nonstandard (nonsolvable if $r \geq 5$ or $\deg f_1 = 5, 6$) bent functions of degrees 4, 5, 6 respectively.

(4) Our computations in dimension 8 gave no hint about the relation between $\text{Aut}(\mathbf{D}(B))$ and its subgroup $\text{Aut}(B)[V]$. All B-sets of partial spread type in (7.3.a) have the property that both groups are the same and only for one of the groups of trace type in (7.3.b) the two groups are different. On the other hand it can be shown that if $B \subseteq V = V(2n, 2)$ is a B-set of standard parabolic type of degree 3 that

$$\text{Aut}(B)[V] < \text{Aut}(\mathbf{D}(B)) \simeq \text{Aut}(\mathbf{D}(B^0)) = \text{Aut}(B^0)[V] \simeq \text{Sp}(2n, 2)[V],$$

with the usual standard B-set B^0 related with B . As we have seen in (3.1.b) the twisted parabolic construction admits many variations. Some of them lead in dimension 8 to B-sets where the groups $\text{Aut}(\mathbf{D}(B))$ and $\text{Aut}(B)[V]$ are different. For instance we obtained a twisted parabolic B-set B with $\text{Aut}(B) \simeq 2^{11} \cdot \text{SL}(2, 4)$ and $|\text{Aut}(\mathbf{D}(B)) : \text{Aut}(B)[V]| = 6$. In this case $\text{Aut}(\mathbf{D}(B))$ even has no regular normal subgroup of order 2^8 .

Acknowledgement. I like to thank the persons who developed GAP. This package was essential for the computations of the previous section. It was also very useful for the theoretical results as computations in small cases often indicated a general statement.

Appendix

In this appendix we first consider subgroups of $\text{GL}(2n, 2)$ which are generated by elements x of prime order such that all nontrivial, proper x -subspaces of $V(2n, 2)$ have dimension n . In the second part we present some results of P. Sin on the degree one cohomology of the groups $G_2(2^n)$.

Denote by r a 2-primitive prime divisor of $2^n - 1$, $n \neq 6$. Let \mathcal{H} be the list of subgroups of $\text{GL}(n, 2)$ having an order divisible by r . This list is a consequence of the work of Hering [He1], [He2] and Liebeck [Li2] (see also [GPPS]). Here we consider subgroups of $\text{GL}(2n, 2)$ having a nontrivial, semiregular r -subgroup. A complete description seems to be not available yet but [De3] contains some information and in particular the work of Guralnik, Penttila, Praeger, and Saxl [GPPS] comes quite close to a complete enumeration. First we investigate the normal structure of such groups in the sense of Aschbacher's paper on subgroups of classical groups [As2]. However we do not refer to this work as in our restricted situation one has a short, self-contained ad hoc proof of the following result:

Proposition 1. *Let V be a $2n$ -dimensional $\text{GF}(2)$ -space and G an irreducible subgroup of $\text{GL}(V)$ which has no subgroups of index 2. Denote by X the subgroup of G generated by all semiregular r -subgroups and assume $X \neq 1$. Then one of the following holds.*

- (a) $F^*(G) = F(G)$ is cyclic and homogeneous and $X \leq F(G)$.
- (b) $E(G) = E_1 \times E_2$ with quasisimple groups E_i . Then r divides $|E_1|$, $E_1 \in \mathcal{H}$ and $E_2 \simeq \mathrm{SL}(2, 2^m)$, with $m < n$ and $m|n$. Moreover V is irreducible as an $E(G)$ -module.
- (c) $E(G)$ is quasisimple and reducible and r divides $|F(G)|$. Moreover $F^*(G) = F(G) \times E(G)$, $E(G) \simeq \mathrm{SL}(2, 2^m)$, with $m|n$.
- (d) $E(G)$ is quasisimple and reducible and r divides $|E(G)|$. Moreover $E(G) \in \mathcal{H}$ and $F(G) \leq C_{\mathrm{GL}(V)}(E(G)) \simeq \mathrm{GL}(2, 2^m)$, with $m < n$ and $m|n$.
- (e) $E(G)$ is quasisimple and irreducible. Moreover r divides $|E(G)|$.

We start with:

Lemma 2. *With the assumptions of the proposition we have that $F(G)$ is cyclic.*

Proof. Assume that N is an elementary abelian normal p -group of G , p odd. Assume $|N| > p$. Then $V = V_1 \oplus \cdots \oplus V_s$, $s > 1$, where the V_i 's are the homogeneous N -components. Suppose that the r -subgroup R induces a nontrivial permutation on the homogeneous components, say induces a cycle (containing V_1) of length $t \geq r$. Then $2n = \dim V \geq r \cdot \dim V_1 \geq (n+1)2$, a contradiction. Thus every homogeneous component is fixed by R which implies $s = 2$. Since G has no subgroup of index 2 we conclude that G is reducible, a contradiction. Thus N is cyclic and therefore any $O_p(G)$, p odd, is of symplectic type.

Now $F(G) = O_{p_1}(G) \times \cdots \times O_{p_s}(G)$ where $\{p_1, \dots, p_s\} = \pi(G) - \{2\}$. We claim that all $O_{p_i}(G)$ are cyclic: If $P = O_p(G) \neq 1$ would be not cyclic a similar argument as in [De3; 2.8], [He1; Thm. 1] or [GPPS; 4.3] shows $p = 2$, a contradiction. Hence $F(G)$ is cyclic.

Proof of the proposition. By lemma 2 $F = F(G)$ is cyclic. Let $1 \neq R$ be a semiregular r -subgroup.

(1) Assume $F^*(G) = F$. Then assertion (a) holds:

As $C_V(F) = 0$ every homogeneous F -component has dimension ≥ 2 and using the same argument about homogeneous components as in the proof of the lemma, we see that V is F -homogeneous and $2n = km$ where m is the dimension of an irreducible F -module in V . Then $|G/F| = |N_G(F)/C_G(F)|$ divides m by (2.10). Since $r \equiv 1 \pmod{n}$ we get $X \leq F$ and (a) follows.

From now on we have $1 \neq E = E(G) = E_1 \cdots E_t$ where the E_i 's are the components of E .

(2) $t \leq 2$ and each E_i is normal in G . Moreover if $E_i = [E_i, R]$ then r divides $|E_i|$ and $E_i \simeq \mathrm{SL}(2, 2^m)$, $m|n$ if $E_i \leq C_G(R)$. Finally (b) holds if $t = 2$:

Let m_i be the degree of a nontrivial representation of E_i in characteristic 2, i.e. $m_i \geq 2$. An obvious induction shows

$$2n = \dim V \geq m_1 + \cdots + m_t.$$

Hence $t \leq n < r$. Therefore X normalizes every component. If $E_i \leq C_G(R)$ then $E_i \simeq \mathrm{SL}(2, 2^m)$, $m|n$ as $C_{\mathrm{GL}(V)}(R) \simeq \mathrm{GL}(2, 2^n)$. Moreover there is at

most one component which is centralized by R . Assume next $E_i = [E_i, R]$. If r does not divide the order of E_i then there exists an $S \in \text{Syl}_2(E_i)$ which is normalized by R . Then $C_V(S) = [V, S]$ is an R -space of dimension n and S is abelian. By a well known result of J. Walter $E_i \simeq \text{PSL}(2, q)$, $q = 2^N$ or $q \equiv 3, 5 \pmod{8}$; ${}^2\text{G}_2(3^N)$, $N = 3f + 1$, or J_1 . If $E_i \simeq \text{PSL}(2, q)$, $q = 2^N$ then $n + 1 \leq r|N$. This is impossible as a nontrivial $\text{GF}(2)[E_i]$ -module has dimension at least $2N$. If $E_i \simeq \text{PSL}(2, q)$, $q \equiv 3, 5 \pmod{8}$, $q = p^f$, p and odd prime, we have $r|f$. However by [SZ]

$$2n \geq \frac{q-1}{2} \geq \frac{p^{n+1}-1}{2},$$

a contradiction. Similarly the Ree groups are excluded while J_1 does not occur as $\text{Out}(\text{J}_1) = 1$. Therefore r divides $|E_i|$.

Assume $t \geq 2$ and $[R, E_1] = E_1$. The group E_1 is reducible as E_2 centralizes E_1 . Then V is E_1 -homogeneous as otherwise $t = 2$ and $V = [V, E_1] \oplus [V, E_2]$ imply that G has a normal subgroup of index 2, a contradiction. Hence $C_{\text{GL}(V)}(E_1) \simeq \text{GL}(2, 2^d)$, $d|n$. Therefore $t = 2$ and $E_2 \simeq \text{SL}(2, 2^m)$, $m|n$.

Assume from now on $t = 1$.

(3) Assume $E \leq C_G(X)$. Then assertion (c) holds:

If $[R, F] = 1$ we get $R \leq C_G(F^*(G)) \leq F$ and $F^*(G) = F \times E$, $E \simeq \text{SL}(2, 2^m)$, $m|n$ and (c) holds. The assumption $[R, F] \neq 1$ leads to a similar contradiction as in (1).

(4) Assume $E = [E, R]$. Then (d) or (e) holds:

We assume that E is reducible as otherwise (e) holds. V is a homogeneous E -module and r divides $|E|$ by (2). Then as in (3) $C_{\text{GL}(V)}(E) \simeq \text{GL}(2, 2^m)$, $m < n$, $m|n$. Assertion (d) holds.

The next two results determine irreducible subgroups of $\text{GL}(2n, 2)$ which contain a cyclic semiregular subgroup of order $2^n - 1$. A more useful result would be a classification of the irreducible subgroups which contain a semiregular subgroup of order r with a 2-primitive prime divisor r of $2^n - 1$. However this would require a more detailed analysis which we want to avoid. Because $\text{Alt}(5) \simeq \text{SL}(2, 4)$, $\text{Alt}(6) \simeq \text{Sp}(4, 2)'$, $\text{Alt}(8) \simeq \text{SL}(4, 2)$, $\text{PSL}(2, 7) \simeq \text{SL}(3, 2)$, $\text{P}\Omega(5, 3) \simeq \text{PSp}(4, 3) \simeq \text{PSU}(4, 2)$ these groups are considered by us as groups of Lie type in characteristic 2 and they do therefore not occur in the next theorem.

Theorem 3. *Let V be a $2n$ -dimensional $\text{GF}(2)$ -space, $n \geq 4$ and $X \leq \text{GL}(V)$ a group which has a quasisimple, normal component E whose order is divisible by a 2-primitive prime divisor r of $2^n - 1$. Also let $Z \leq X$ be a semiregular cyclic group of order $2^n - 1$ and assume that V is homogeneous as an E -module. Then E is of Lie type of characteristic 2 or $E/Z(E) \simeq \text{Alt}(7)$, $r = n + 1 = 5$.*

Proof. Assume that $E/Z(E)$ is a simple group which is not of Lie type of characteristic 2. As r divides $|E|$ we see that V is either E -irreducible or $V \simeq W \oplus W$ with an irreducible E -module W .

We denote by $\ell(E)$ (or $\ell_0(E)$) the minimal degree of a nontrivial projective linear (or linear) representation of E in characteristic 2. Set $\widehat{C} = \text{End}_E(V)$.

Then with f suitable one has $\widehat{C} \simeq \text{GF}(2^f)^{i(V) \times i(V)}$ where $i(V) = 1$ or 2 if V is E -irreducible or E -reducible respectively. Set $C = C_{\text{GL}(V)}(E)$. Then

$$(1) \quad \frac{\ell_0(E)fi(V)}{2} \leq n.$$

We denote by $\alpha(E)$ an upper bound for a prime dividing $|E|$. Then

$$(2) \quad \alpha(E) \geq r = bn + 1,$$

$b \geq 1$ suitable. Combining the inequalities we have:

$$(3) \quad \frac{\ell_0(E)fi(V)}{2} \leq n \leq \frac{\alpha(E) - 1}{b}.$$

These inequalities hold with $\ell(E)$ in place of $\ell_0(E)$ too. Denote by $\beta(E)$ an upper bound for the order for a cyclic subgroup of odd order in E and by d an upper bound for the order of such a group in $\text{Out}(E)$. Let Z_0 be the subgroup of Z which induces inner automorphisms on E . Then $|Z/Z_0| \leq d$, $|Z_0/C_Z(E)| \leq \beta(E)$ and $|C_Z(E)| \leq 2^{i(V)f} - 1$. Hence

$$(4) \quad 2^n - 1 \leq \beta(E)(2^{i(V)f} - 1)d.$$

Often one has $\beta(E) = \beta(\text{Aut}(E))$ and in this case we can replace d by 1 in the inequality. Usually we will show $i(V), b \leq 2$ and $r \nmid d$. If $r > 5$ then r does not divide $|C|$ too. Then E contains every Sylow s -subgroup Z_s for every 2-rimitive prime divisor s of $\Phi_n^*(2)$. If s^2 divides $|Z|$ then even

$$(5) \quad n < \sqrt{\beta(E)}$$

as $s \geq n + 1$. If however $|Z_s| = s$ for any such prime we can deduce by [He1; (3.9)] that $\Phi_n^*(2) = r$ is a prime and either $r = n + 1$, $n \in \{10, 12, 13\}$ or $r = 2n + 1$, $n \in \{8, 20\}$.

Case $E/Z(E) \simeq \text{Alt}(m)$.

Assume first $m \geq 9$. By a result of A. Wagner [Wa] $\ell(E) = \ell_0(E) = m - \varepsilon(m)$ where $\varepsilon(m) = 1$ if m is odd and $\varepsilon(m) = 2$ if m is even. Moreover $r = bn + 1 \leq \alpha(E) \leq m$. Hence

$$(m - \varepsilon(m)) \frac{fi(V)}{2} \leq \frac{m - 1}{b}.$$

Therefore $b, f \leq 2$ and if $b = 2$ then $f = i(V) = d = 1$. No 2-primitive prime divisor of $\Phi_n^*(2)$ divides $|C|$. Then (5) can not hold and therefore $\Phi_n^*(2) = r$. If $b = 2$ as we observed $n = 8, 20$ and $(n, m) \in \{(8, 17), (8, 18), (20, 41), (20, 42)\}$. Let

$$2^n - 1 = p_1^{a_1} \cdots p_r^{a_r}$$

be the prime factorization then

$$m \geq p_1^{a_1} + \cdots + p_r^{a_r}$$

which is impossible.

If $b = 1$ we have $(n, r) \in \{(10, 11), (12, 13), (18, 19)\}$. If V is E -irreducible then $|Z \cap E| \geq (2^n - 1)/(2^f - 1)$. If $f = 2$ then $m = n + 1$ or $n + 2$ and using the prime factorization of $|Z \cap E|$ we get a similar contradiction as before. If $f = 1$ then $m \leq 22, 26$ or 38 for $n = 10, 12, 18$ respectively and we reach similar contradiction. If V is E -reducible then $n = m + 1$ or $m + 2$ and it is easy to see that $\text{Alt}(m) \times C_{15}$ has no cyclic subgroup of order $2^n - 1$.

Finally if $m < 9$ then $m = 7$ and $r = 5$ as $n \geq 4$.

Case $E/Z(E)$ sporadic

We take the bounds for $\ell_0(E)$ from the homepage of the Modular Atlas [MoAt] (also see the Modular Atlas [JLPW] for more details) while the bounds for $\alpha(E)$ and $\beta(E)$ can be read of the Atlas [CCNPW].

Inequality (3) rules out the "large cases"

$$E/Z(E) \simeq \text{McL}, \text{He}, \text{ON}, \text{Fi}_{22}, \text{HN}, \text{Ly}, \text{Th}, \text{F}_{23}, \text{J}_4, \text{Fi}_{24}^{(1)}, \text{B}, \text{M}$$

and the cases $E \simeq \text{J}_3, \text{Suz}$.

Assume $E \simeq \text{M}_{11}, \text{M}_{12}$ or M_{22} . Then $\ell_0(E) = 10$ and $\alpha(E) = \beta(E) = 11$. By [He1] $b = 1$ and $2^n - 1 = 2^{10} - 1 \leq \beta(E)(2^{fi(V)} - 1)$, $fi(V) \leq 2$ which is impossible. If $E \simeq 3\text{M}_{22}$ then $\beta(E) = 33$ and $6 \leq n \leq 10$ contradicting $2^6 - 1 > \beta(E) \cdot 3$.

If $E \simeq \text{J}_2$ then $\ell_0(E) = 6$ and if $f = 1$ then $\text{GF}(2)$ is the field of definition of the representation and we can replace the lower bound $\ell_0(E)$ by 36. Then $i(V) = 1$ and $\alpha(E) = 7$, $\beta(E) = 15$. We reach the usual contradiction.

Assume $E \simeq \text{M}_{23}, \text{M}_{24}$. Then $\alpha(E) = \beta(E) = 23$ and $\ell_0(E) = 11$. If $i(V) = 1$ and $f = 1$ then $n \geq 6$ and E has a cyclic subgroup of order $2^n - 1$ which is false. If $i(V) = 2$ or $f = 2$ then $n \geq 11$ and as usual $2^n - 1 > \beta(E)(2^{2f} - 1)$.

The remaining cases $\text{J}_1, 3\text{J}_3, \text{HS}, \text{Ru}, 3\text{Suz}, \text{Co}_1, \text{Co}_2, \text{Co}_3$ are ruled out by the same pattern.

Case $E/Z(E)$ is a group of Lie type of odd characteristic and not classical

Combining the information of [SZ], [He1], [He2] and considering the subgroup structure of the Ree groups [HB] we obtain the following table:

| $E/Z(E)$ | $\ell(E)$ | $\alpha(E)$ |
|---------------------|--|---------------------------------------|
| $\text{E}_6(q)$ | $q^9(q^2 - 1)$ | $q^6 + q^3 + 1$ |
| $\text{E}_7(q)$ | $q^{15}(q^2 - 1)$ | $(q^7 - 1)/(q - 1)$ |
| $\text{E}_8(q)$ | $q^{27}(q^2 - 1)$ | $q^8 + q^7 - q^5 - q^4 - q^3 + q + 1$ |
| $\text{F}_4(q)$ | $q^6(q^2 - 1)$ | $q^4 + 1$ |
| $\text{G}_2(q)$ | $q(q^2 - 1), \ell(\text{G}_2(3)) = 14$ | $q^2 + q + 1$ |
| ${}^2\text{E}_6(q)$ | $q^9(q^2 - 1)$ | $q^6 - q^3 + 1$ |
| ${}^2\text{G}_2(q)$ | $q(q - 1)$ | $q + 3^{N+1} + 1, q = 3^{2N+1}$ |
| ${}^3\text{D}_4(q)$ | $q^3(q^2 - 1)$ | $q^4 - q^2 + 1$ |

Inequality (3) rules out immediately the cases $\text{E}_6, \text{E}_7, \text{E}_8, \text{F}_4, {}^2\text{E}_6, {}^3\text{D}_4$. In the exceptional case $E/Z(E) \simeq \text{G}_2(3)$ we have $\ell_0(3\text{G}_2(3)) = 27$, $\alpha(E) = 13$ and $\beta(\text{G}_2(3)) = 13$, $\beta(3\text{G}_2(3)) = 39$. This shows $n = 12, b = 1, fi(V) = 1$. But

then (4) is violated. If $E/Z(E) \simeq G_2(q)$, $q \geq 5$; or ${}^2G(q)$ again (3) and (4) give a contradiction.

Case $E/Z(E)$ is a classical group of odd characteristic

We use [GPPS] and [SZ] and in some exceptional cases also [JLPW] for lower bounds of the degree of linear representations.

Assume $E/Z(E) \simeq \text{PSL}(2, p)$, $p \geq 11$ a prime. Then $\ell(E) = (p-1)/2$ and $\alpha(E) = \beta(E) = p$. As $EC_{\text{GL}(V)}(E)$ contains a cyclic group of order $2^n - 1 \geq 2^M - 1$, $M = (p-1)fi(V)/4$ we have $2^M - 1 \leq p(2^{fi(V)} - 1)$ by (4) implying $p \leq 17$. But then $p = 11, 13$, or 17 and $n = 10, 12$, or 8 , which is impossible.

Assume $E/Z(E) = E \simeq \text{PSL}(2, q)$, $q = p^\epsilon \geq 25$, p a prime, $\epsilon > 1$. Now $\ell(E) = (q-1)/2$, $\alpha(E) = (q+1)/2$. Set $M = (q-1)fi(V)$ then $\beta(E) = \beta(\text{Aut}(E))$ and as before we get $2^M - 1 \leq (q+1)(2^{fi(V)} - 1)/2$, which is impossible.

In the exceptional case $E/Z(E) \simeq \text{PSL}(4, 3)$ one has $\ell(E) = 26$, $\alpha(E) = \beta(E) = 13$ which is in conflict with (3).

Suppose $E/Z(E) \simeq \text{PSL}(m, q)$, $m \geq 3$, $(m, q) \neq (4, 3)$, $q = p^\epsilon$, p a prime. Then by [GPPS; Thm. 9.1.5] $\ell(E) = ((q^m - 1)/(q - 1)) - 2$ while $\alpha(E) = (q^m - 1)/(q - 1)$, $\beta(E) = (q^m - 1)/2$. Then (3) shows $b, f \leq 2$ and by (4) ($d = 1$ by the remark following (4)) $2^M - 1 < 3\epsilon(q^m - 1)/2$ with $M = ((q^m - 1)/(q - 1) - 2)/2$ which is not possible.

In the exceptional case $E/Z(E) \simeq \text{PSU}(4, 3)$ we have $\alpha(E) = 7$ and $\ell_0(\text{PSU}(4, 3)) = 20$, $\beta(\text{PSU}(4, 3)) = 9$ while $\ell_0(3\text{SU}(4, 3)) = 6$, $\beta(3\text{SU}(4, 3)) = 21$. Hence $n = 6$, $i(V) = 1$, $f = 2$. But $C_3 \times 3\text{SU}(4, 3)$ contains no C_{63} .

Assume $E/Z(E) = E \simeq \text{PSU}(m, q)$, m even, $q = p^\epsilon$, p a prime. Then $\ell(E) = (q^m - 1)/(q + 1)$ and

$$\alpha(E) = \begin{cases} q^2 + 1, & m = 4, \\ \frac{q^{m-1} + 1}{q + 1}, & m \geq 6. \end{cases}$$

In both cases (3) is not fulfilled.

Assume $E/Z(E) = E \simeq \text{PSU}(m, q)$, m odd, $q = p^\epsilon$, p a prime. Then by [GPPS; (9.3.2)] $\ell(E) = (q^m - q)/(q + 1)$ and $\alpha(E) = (q^m + 1)/(q + 1)(m, q + 1)$. Then (3) implies $(m, q + 1) = 1$ and therefore $(q^m - q)fi(V)/2 \leq q^m + 1$. In particular $f \leq 2$ and $f = 1$ if $i(V) = 2$. Moreover $\beta(E) = q^m + 1$ (see [Hu]). But then (4) can not hold.

The orthogonal and symplectic groups are ruled out by the same pattern.

Theorem 4. *Let V be a $2n$ -dimensional $\text{GF}(2)$ -space and $E \leq \text{GL}(V)$ be a quasisimple and irreducible subgroup so that $E/Z(E)$ is a group of Lie type over the field $\text{GF}(2^e)$. Assume that the order of E is divisible by a 2-primitive prime divisor r of $2^n - 1$ and let $Z \leq N_{\text{GL}(V)}(E)$ be a semiregular cyclic group of order $2^n - 1$. Then one of the following holds:*

- (a) E has at most three orbits on V and hence is known by [Li2].
- (b) $E \simeq \text{SL}(2, 2^e)$ and V is as a $\text{GF}(2)[E]$ -module isomorphic to $M \otimes M^\sigma$ where M is the natural E -module and σ is a Galois automorphism with $\sigma^2 \neq 1$

Proof. We denote by R a Sylow r -subgroup of E . Assume $\text{End}_E(V) \simeq \text{GF}(2^f)$ so that $C = C_{\text{GL}(V)}(E) \simeq C_{2^f-1}$. We then can consider V as an absolutely irreducible $\text{GF}(2^f)[E]$ -module and $\text{GF}(2^f)$ is the field of definition (see for instance [As1; 26.6.(4)]). By Steinbergs twisted tensor product theorem one knows that $f|te$ where $t = 1$ if E is untwisted or of type ${}^2\text{B}_2, {}^2\text{F}_4$, $t = 2$ if E is of type ${}^2\text{A}_\ell, {}^2\text{D}_\ell, {}^2\text{E}_6$ and $t = 3$ if E is of type ${}^3\text{D}_4$. Denote by $\mu(E)$ the largest integer such that $|E|$ is divisible by a 2-primitive prime divisor of $2^{\mu(E)e} - 1$. Then

$$(1) \quad n \leq \mu(E)e.$$

We assume first that E is untwisted or of type ${}^2\text{B}_2, {}^2\text{F}_4$ and $e = fa$. By [KL; 5.4.6, 5.4.7] we obtain

$$(2) \quad 2n \geq m(E)^a f,$$

where $m(E)$ is the minimal degree of an absolutely irreducible nontrivial representation of E in characteristic 2. Hence

$$(3) \quad \frac{1}{2}m(E)^a \leq \mu(E)a.$$

This inequality will restrict possible candidates for V to a small list. Sylow r -subgroups of $\text{GL}(V)$ are abelian. So by a suitable choice of R we can assume that the group $Z = C_{2^n-1}$ satisfies

$$(4) \quad Z \leq C_E(R)CA$$

where $A/(A \cap EC)$ is isomorphic to a suitable cyclic group of odd order of $\text{Out}(E)$. Usually with (4) we get rid of the remaining candidates for the module V .

Case $E/Z(E) \simeq \text{PSL}(m, 2^e)$, $m \geq 2$. Here $\mu(E) = m(E) = m$ so that (3) implies $m^{a-1}/2 \leq a$. This implies $a \leq 4$ for $m = 2$, $a \leq 2$ for $3 \leq m \leq 4$ and $a = 1$ otherwise. By the twisted tensor product theorem V as a $\text{GF}(2)[E]$ -module is isomorphic to $M(\lambda^{(0)})^{(0)} \otimes M(\lambda^{(1)})^{(1)} \otimes \dots \otimes M(\lambda^{(e-1)})^{(e-1)}$ with basic modules $M(\lambda^{(i)})$ in the terminology of Liebeck [Li1] and $M^{(k)}$ is the Galois conjugate of the $\text{GF}(2^e)[E]$ -module M under the k -th power of the Frobenius automorphism. So if $a = 1$ and more then one of the basic modules in the tensor product is nontrivial we have $2n \geq m^2e$ and $n \leq me$ which implies $m = 2$, $n = 2e$, $V \simeq M \otimes M^\sigma$ with the standard module M and a nontrivial field automorphism σ . Also $\sigma^2 \neq 1$ as otherwise the field of definition is $\text{GF}(2^{e/2})$, i.e. assertion (b) holds.

Assume next $a > 1$ and $m = 2$. As r divides $|E|$ our inequalities imply $n = e$ or $2e$. If $a = 4$ then at least four Galois conjugates of M occur in the tensor product. Then $4e \geq 2n \geq 16f$ which implies $2n = e$. Also $C_E(R) \simeq C_{2^e+1}$, $C \simeq C_{2^f-1}$ and $|\text{Out}(E)|_{2'}$ divides f . But then (4) is violated. If $a = 3$ then the inequalities imply that V is the tensorproduct of three Galois conjugates of M . Hence $2n = 8f$ but $n = 3f$ or $6f$, a contradiction. If $a = m = 2$ of course $2e = n$ and V can be considered as the standard $\Omega^-(4, 2^f)$ -module and we have assertion (a).

Assume now $m = 3$ or 4 and $a = 2$. If more the one Galois conjugate of M (the standard module M or its dual) occurs in the tensor peoduct then our

inequalities imply that V is the tensor product of two Galois conjugates of M . But as $2n = m^2 f$ the case $m = 3$ is excluded. For $m = 4$ we get $n = 4e$. Then $|C_E(R)| = (2^{4e} - 1)/(2^e - 1)$ and $|C| = 2^f - 1$ which is in conflict with (4).

Suppose next that M is not the standard module (or its dual). In case $m = 3$ one has then $\dim M \geq 8$ ruling out this case. In case $m = 4$ one has $\dim M \geq 6$ so that $6^2 f/2 \leq 2 \cdot 4 \cdot f$, a contradiction too.

Form now on we assume $a = 1$ and V is $\text{GF}[E](2)$ -isomorphic to a basic E -module say $M(\lambda)$. The natural module (or its dual, i.e. $\lambda = \lambda_1$ or λ_{m-1}) implies assertion (a). So we assume that $M(\lambda)$ is not standard, i.e. $m \geq 3$. By (1) and (2) we get $\dim M(\lambda) \leq 2m$. By [Li2; 2.2] then $(\lambda, \dim M(\lambda)) \in \{(\lambda_2, m(m-1)/2), (\lambda_{m-2}, m(m-1)/2)\}$ and $4 \leq m \leq 5$. Again by [Li2] we have assertion (a).

The cases $E/Z(E) \simeq \text{Sp}(2m, 2^e)$, $m \geq 2$ or $\Omega^+(2m, 2^e)$, $m \geq 4$ are handled similar.

Cases $E/Z(E) \simeq \text{E}_6(2^e), \text{E}_7(2^e), \text{E}_8(2^e), \text{F}_4(2^e)$. Here $\mu(E) = 12, 18, 30, 12$ and $m(E) = 27, 56, 248, 26$ respectively. This is in conflict with (3).

Case $E/Z(E) \simeq \text{G}_2(2^e)$. Now $\mu(E) = m(E) = 6$ and (3) implies $a = 1$ and V is $\text{GF}(2)$ -isomorphic to a basic E -module $M(\lambda)$ with $\dim M(\lambda) \leq 12$. But then by [Li2] $\lambda = \lambda_1$ and $\dim M(\lambda) = 6$ and (a) holds.

Case $E/Z(E) \simeq {}^2\text{B}_2(2^e)$. Then $\mu(E) = m(E) = 4$ and by [KL; 5.4.7] and (3) we have $4^a/2 \leq 4a$ with an odd a . Hence $a = 1$. As irreducible E -modules are tensor products of Galois conjugates of the standard module we see that V is the standard module viewed as a $\text{GF}(2)[E]$ -module. Then $2n = 4e$. But r divides also $|E/Z(E)|_{2'} = (2^{2e} + 1)(2^e - 1)$, a contradiction.

Case $E/Z(E) \simeq {}^2\text{F}_4(2^e)$. Here $\mu(E) = 12$, $m(E) = 26$ which contradicts (3).

We now turn to the cases ${}^2\text{A}_\ell, {}^2\text{D}_\ell, {}^2\text{E}_6, {}^3\text{D}_4$. We define $m_0(E)$ as a lower bound for the degree of a nontrivial absolutely irreducible representation which can be written over $\text{GF}(2^e)$. Using [KL; 5.4.6] we replace (2) now by the two inequalities:

$$(2') \quad 2n \geq \begin{cases} m_0(E)^a f, & \text{if } f | e, e = af, \\ m(E)^a f, & \text{if } f \nmid e, 2e = af. \end{cases}$$

Case $E/Z(E) \simeq {}^2\text{A}_m(2^e) \simeq \text{PSU}(m+1, 2^e)$, $m \geq 2$. Now $\mu(E) = 2(m+1)$ if m is even and $\mu(E) = 2m$ if m is odd. If $e = af$ we get from (1) and (2') $m_0(E)^a \leq 4(m+1)a$ if m is even and $m_0(E)^a \leq 4ma$ if m is odd. If $2e = af$, $f \nmid e$, then $m(E)^a \leq 2(m+1)a$ if m is even and $m(E)^a \leq 2ma$ if m is odd.

First we observe $a = 1$: Assume $a > 1$. If $2e = af$, $f \nmid e$, then $a \geq 3$, a contradiction as $m(E) = m+1$. If $e = af$ we use for $m_0(E)$ the bounds of [KL; 5.4.8]. Again our inequalities rule out the assumption $a > 1$. Hence $a = 1$ in any case and $f = 2e$ or e .

Assume $f = 2e$. Considering V as a $\text{GF}(2^f)[E]$ -module its dimension is $\leq 2(m+1)$ if m is even and $\leq 2m$ if m is odd. This $\text{GF}(2^f)[E]$ -module is the restriction of an absolutely irreducible $\text{GF}(2^f)[\text{SL}(m+1, 2^f)]$ -module to E (see [KL; 5.4.1]). Using the bounds of [Li2; 2.2] we see that V has type $M(\lambda)$ with $(\lambda, \dim M(\lambda)) \in \{(\lambda_1, m+1), (\lambda_m, m+1), (\lambda_2, m(m+1)/2), (\lambda_{m-1}, m(m+1)/2)\}$ and $m \leq 4$ if the dimension is $m(m+1)/2$. If $\dim M(\lambda) = m+1$ we get assertion (a). So assume dimension $m(m+1)/2$ which excludes $m = 2$. If $m = 3$ however

the case $\lambda = \lambda_2$ does not occur as in this case $\text{GF}(2^e)$ is the field of definition. In case $m = 4$ we get $n = 10e$. Then $|C_E(R)|$ divides $2^{5e} + 1$ and $|C| = 2^{2e} - 1$ which is in conflict with (4).

Assume $f = e$. Considering V as a $\text{GF}(2^e)[E]$ -module its dimension is $\leq 4(m+1)$ if m is even and $\leq 4m$ if m is odd. Also $V^{\tau_0} \simeq V$ where τ_0 has the meaning of [KL: 5.4.6]. Again V has a type $M(\lambda)$ described in [Li2; 2.2] with the additional property that λ is invariant under the graph symmetry. If $m = 2$ then $M(\lambda)$ is the 8-dimensional adjoint module (see [Bu]). This shows $n = 4e$. However then r does not divide $|E|$ a contradiction. If $m = 3$ the module $M(\lambda_2)$ is the natural, 6-dimensional $O^-(6, 2^e)$ -module and assertion (a) holds. The adjoint module has dimension 14. This would imply $n = 7e$ and again $(r, |E|) = 1$, a contradiction. For $m \geq 4$ the adjoint module can not occur as its dimension is $\geq (m+1)^2 - 2$. This leaves the possibility $m = 5$ and the module $M(\lambda_3)$ of dimension 20. Thus $n = 10e$. However as R has a centralizer of dimension 1 in the natural module we see that $|C_E(R)|$ divides $(2^{5e} + 1)(2^e + 1)$. Again this case is ruled out by (4) as $|C| = 2^e - 1$.

The cases $E/Z(E) \simeq {}^2D_m(2^2) \simeq \text{P}\Omega^-(2m, 2^m)$, $m \geq 4$, $E/Z(E) \simeq {}^2E_6(2^e)$, and $E/Z(E) \simeq {}^3D_4(2^e)$ are treated similar.

The next result implies in particular that the 2-powers are the only powermaps of $\text{GF}(2^n)$ preserving the set of elements of trace 0. P. Müller pointed out to me a similar elementary argument which shows that any trace preserving powermap of a finite field is a power of the Frobenius automorphism implying also proposition 5.

Proposition 5. *Set $F = \text{GF}(2^n)$, $F_0 = \{\beta \mid \text{trace } \beta = 0\}$ add let $\varphi(k) : F \rightarrow F$, $x \mapsto x^k$ be an invertible powermap. If $F_0\varphi(k) = F_0^k = F_0c$ with some $0 \neq c \in F$ then $k = 2^j$, j suitable.*

Proof. Define $f : F \rightarrow F$ by $x \mapsto dx^k$, $d = c^{-1}$. Since F_0 is a $\text{GF}(2)$ -hyperplane of F and as $(aF_0)f = da^kF_0^k = a^kF_0$ this map permutes the set of hyperplanes. This implies that f also permutes the spaces of codimension 2 etc.. Since f preserves inclusion we deduce that this map is a collineation of the projective geometry $\text{PG}_{\text{GF}(2)}(F)$. By the main theorem of projective geometry this map is induced by a linear map. However $\text{PGL}(F) = \text{GL}(F)$ which shows that f is linear. Therefore $dx^k = a_0x + a_1x^2 + \dots + a_{n-1}x^{2^{n-1}}$ with suitable $a_i \in F$. This implies that precisely one $a_j \neq 0$ and $x^k = x^{2^j}$.

In [Si1] P. Sin gives a comprehensive study of the degree 1-cohomology of the groups $G_2(2^n)$, $n > 6$. We add two results without the restriction $n > 6$. We thank Professor P. Sin [Si3] for the permission to present his results and his proofs (with modest changes). In the sequel $X^{(2^k)}$ denotes the Galois twist with the k -th power of the Frobenius automorphism of a $\text{GF}(2^n)$ -module X .

Theorem 6 (P. Sin). *Set $G = G_2(2^n)^{(1)}$, $n \geq 1$, $F = \text{GF}(2^n)$, and let V be the natural 6-dimensional G -module.*

- (a) *Let A be the 14-dimensional adjoint module of G . Then $V \otimes V$ has a filtration with layers $F \oplus A$, $V^{(2)}$, $F \oplus A$. This filtration is the radical and*

socle series. In particular each submodule which covers the composition factor $V^{(2)}$ also contains the bottom module $F \oplus A$.

- (b) $H^1(G, V \otimes V^{(2^k)}) = 0$ for $1 \leq k < n$ and $n > 2$.
- (c) $\dim H^1(G, V \otimes V^{(2)}) = 1$ for $n = 2$.

Proof. (a) Set $L = \text{Sp}(6, F)$, i.e. $G \leq L$. Act with K on $V \otimes V \simeq V^* \otimes V \simeq \text{End}(V)$ by $x \cdot k = k^t x k$. One has the natural L -series $0 \subset \wedge^2(V) \subset S^2(V) \subset V \otimes V$ with $\wedge^2(V) \simeq (V \otimes V)/S^2(V)$ and $V^{(2)} \simeq S^2(V)/\wedge^2(V)$. Obvious linear algebra arguments even show $\wedge^2(V) \simeq F \oplus A$ and by [Si1; (2.1.a)] all these statements also hold for $V \otimes V$ as a G -module.

In order to prove the last statement it suffices to consider the case $n = 1$ and to show that the smallest submodule X which has $V = V^{(2)}$ as a composition factor also contains $\wedge^2(V)$. A direct GAP-computation shows that the module $S^2(V)/A$ is indecomposable where as before A is the adjoint module. Hence X contains the bottom F .

Denote by Y the subquotient of $V \otimes V$ which omits the bottom and top trivial factor, i.e. Y is selfdual with a filtration A, V, A . We are done once we show that Y is uniserial. Denote by $K \simeq \text{SL}(3, 2)$ the subgroup generated by the long root subgroups. The restriction of V to K is isomorphic to $W \oplus W^*$, W the natural 3-dimensional K -module. Then as an K -module we have

$$\wedge^2(V) = \wedge^2(W) \oplus \wedge^2(W^*) \oplus W \otimes W^* = W^* \oplus W \oplus F \oplus S$$

where S is the 8-dimensional irreducible K -module (of trace zero matrices under conjugation). Thus A is semisimple as an K -module.

Suppose that Y is not uniserial as a G -module. Then the Loewy length is at most 2 as a K -module. As an K -module

$$V \otimes V = (W \oplus W^*) \otimes (W \oplus W^*).$$

Therefore as an K -module Y has a subquotient isomorphic to the 9-dimensional uniserial module $W \otimes W$ with factors W^*, W, W^* , a contradiction. Hence Y is uniserial and assertion (a) follows.

(b) Let α, β be the fundamental roots, α long. We use standard notations for root subgroups and diagonal subgroups. Let $L_1 = \langle H, X_\beta, X_{-\beta} \rangle$ be the Levi subgroup corresponding to β and $L_2 = \langle H, X_{\alpha+\beta}, X_{-\alpha-\beta} \rangle$ and the Levi subgroup corresponding to $\alpha + \beta$, so that $H = L_1 \cap L_2$.

Then $G = \langle L_1, L_2 \rangle$: The Chevalley commutator formula applied to $X_{-\beta}$ and $X_{\alpha+\beta}$ shows $X_\alpha \leq \langle L_1, L_2 \rangle$ and by symmetry also $X_{-\alpha} \leq \langle L_1, L_2 \rangle$. Hence $\langle L_1, L_2 \rangle$ contains two elements $r_\alpha, r_\beta \in N_G(H)$ which induce the fundamental reflections of the Weyl group. Thus $\langle L_1, L_2 \rangle$ contains all root subgroups and the claim follows.

Set $M = V \otimes V^{(2^k)}$. As $1 \leq k < n$ one observes that $C_M(H) = 0$. Assertion (b) follows if we show $H^1(L_i, M) = 0$. This follows from [Si2; lemma 1]. Sin's result generalizes [AG] and [KaLi; p. 9, (β)] which could be applied too. As the L_i 's are conjugate we consider only the case L_1 . One has $L_1 = L_0 \times Z$, $L_0 = \langle X_\beta, X_{-\beta} \rangle \simeq \text{SL}(2, F)$ and $Z = H_{2\alpha+3\beta} \simeq C_{2^{n-1}}$. Let W be the natural L_0 -module and denote by $[m]$ the character of Z which sends $h_{2\alpha+3\beta}(t)$ onto t^m . The $F[L_1]$ -composition factors of V are $W \otimes [1]$, $W^{(2)} \otimes [0]$, $W \otimes [-1]$. Therefore

the composition factors of M are of the form $W^{(2^i)} \otimes W^{(2^j)} \otimes [m]$, i, j, m suitable. However $H^1(\mathrm{SL}((2, 2^n), W^{(2^i)} \otimes W^{(2^j)})) = 0$ for all i, j (for $i = j$ this result is [Al; thm 3]). Assertion (b) follows.

(c) The double cover \widehat{G} of G has an ordinary character χ_{33} (in the ATLAS notation) of degree 12. Modulo 2 it decomposes as $\chi_{33} = \varphi_2 + \varphi_3$ (the φ_i 's as in [JLPW]), i.e. a corresponding $F[\widehat{G}]$ -module E has composition factors V and $V^{(2)}$. Then the central involution z of \widehat{G} must act trivially on E , i.e. E is even a $F[G]$ -module. By a result of Thompson [La; I,17.4] this module E can be chosen such that $\mathrm{soc}(E) \simeq V$. Hence $\mathrm{Ext}_{F[G]}^1(V, V^{(2)}) \simeq H^1(G, V \otimes V^{(2)}) \neq 0$.

Set $M = V \otimes V^{(2)}$ and let $X = GM$ be a split extension of G by M . Let H, α, β and $X_\alpha, X_\beta \leq G$ have the same meaning as before. Let $w_\alpha = x_\alpha(1)x_{-\alpha}(1)x_\alpha(1)$ and $w_\beta = x_\beta(1)x_{-\beta}(1)x_\beta(1)$ be fundamental reflections in the normalizer of H . Then $J = \langle X_\beta, H, d \rangle$, $d = (w_\alpha w_\beta)^2$, is isomorphic to the Janko group J_2 . Let $K \leq X$ be an other complement to M which is not conjugate to G in X . As $H^1(J, M) = 0$ [Si2] we may assume $J \leq G \cap K$ and $K = \{c(g)g \mid g \in G\}$ with a 1-cocycle $c : G \rightarrow M$ with $c(J) = 0$. Then $w_\beta \in N_G(N)$, $N = \langle H, d \rangle$ and $G = \langle J, w_\beta \rangle$. Therefore $c(w_\beta)w_\beta \in N_K(N)$ and $K = \langle J, c(w_\beta)w_\beta \rangle$. For any $n \in N$ we have $[c(w_\beta)w_\beta, n] = [c(w_\beta), n]^{w_\beta}[w_\beta, n] \in N$. Thus $[c(w_\beta), n] \in N \cap M = 0$ or $c(w_\beta) \in C_M(N)$. As $|c(w_\beta)w_\beta| = 2$ even $0 \neq c(w_\beta) \in C_M(N) \cap C_M(w_\beta)$ which has dimension 1. So up to a nontrivial scalar the vector $c(w_\beta)$ is uniquely determined and $\dim H^1(G, V \otimes V^{(2)}) \leq 1$. (c) follows.

Proposition 7 (P. Sin). *Let $G = G_2(2^n)$, $F = \mathrm{GF}(2^n)$ (or $G = G_2(2)^{(1)}$) and A be the 14-dimensional, adjoint $F[G]$ -module. Then $H^1(G, A) = 0$.*

Proof. By [Si2] $H^1(G, A) = 0$ for $n = 1$. Assume $n > 1$ and let m be a divisor of n such that n/m is a prime. Set $G_1 = G_2(2^m)$ and let $G_2 \simeq \mathrm{SL}(3, 2^n)$ be the subgroup of G generated by the long root subgroups. Then $\mathrm{SL}(3, 2^m) \simeq G_0 \leq G_1 \cap G_2$ and $G = \langle G_1, G_2 \rangle$ by [Co]. The module A is as an $\mathrm{GF}(2^m)[G_1]$ -module the adjoint module whose coefficients are extended to the field F . So still $H^1(G_1, A) = 0$ by induction. As a G_2 -module A contains the 8-dimensional, irreducible part W of the adjoint $F[\mathrm{SL}(3, 2^n)]$ -module as a composition factor. Since A is selfdual it is now easy to see that $A = W \oplus N \oplus N^*$, where N is the natural module of G_2 . Hence $H^1(G_2, A) = 0$ by [JP]. Also $C_A(G_0) = 0$. From [Si2; lemma 1] we conclude $H^1(G, A) = 0$.

References

- AG J. Alperin, D. Gorenstein, A vanishing theorem for cohomology, Proc. Amer. Mat. Soc. 32(1972), 87-88.
- Al J. Alperin, "Projective modules for $\mathrm{SL}(2, 2^n)$ ", J. Pure. Appl. Algebra 15(1979), 219-234.
- As1 M. Aschbacher, "Finite Group Theory", Cambridge Univ. Press, 2000.
- As2 M. Aschbacher, On the maximal subgroups of the finite classical groups, Invent. Math., 71(1984), 469-514.

- At "ATLAS of Finite Group Representations", <http://for.mat.bham.ac.uk/atlas/>
- Ba B. Baumann, Symmetrische Singer-Zyklen über Körpern der Charakteristik 2, Mitt. Math. Sem. Gießen, 163(1984), 135-140.
- Be G. Bell, Cohomology of degree 0,1 and 2 of $SL_n(q)$ I-II, J. Algebra 54(1978), 216-238, 239-259.
- Bd T. Bending, Bent functions, SDP designs and their automorphism groups, Thesis, Queen Mary and Westfield College, Univ. London, 1993.
- Bu R. Burkhardt, Über die Zerlegungszahlen der unitären Gruppen $PSU(3, 2^{2f})$, Jour. Alg. 61(1979), 548-581.
- CCNPW J. Conway et al., "An Atlas of Finite Groups", Clarendon Press, 1985.
- CD C. Charnes, U. Dempwolff, The eight dimensional ovoids over $GF(5)$, Math. of Computations, 70(2000), 853-861.
- CRB1 C. Charnes, M. Rötteler, T. Beth, Homogeneous bent functions, invariants, and designs, Designs, Codes, Crypt., 26(2002), 139-154.
- CRB2 C. Charnes, M. Rötteler, T. Beth, On the stabilizers of homogeneous bent functions in the affine group, 7th Finite Fields Symposium, Toulouse France, May 2003.
- Co B. Cooperstein, Maximal subgroups of $G_2(2^n)$, Jour. Algebra 70(1981), 23-36.
- De1 U. Dempwolff, A characterization of the generalized twisted field planes, Arch. Math. 50(1988), 477-480.
- De2 U. Dempwolff, Affine rank 3 groups on Symmetric designs, Designs, Codes, Crypt., 31(2004), 159-168.
- De3 U. Dempwolff, Linear groups with large cyclic subgroups and translation planes, Rend. Sem. Mat. Univ. Padova, 77(1984), 69-113.
- Di1 J. Dillon, A survey of bent functions, NSA Tech. Jour., Special Issue, 1972, 191-215.
- Di2 J. Dillon, Elementary Hadamard difference sets, in Proc. 6-th. S.E. Conf. Comb., Graph Theory and Computing, Utilitas Math. Boca Raton, 1975, 237-249.
- DR U. Dempwolff, A. Reifart, The classification of the translation planes of order 16, I, Geom. Ded. 15(1983), 137-153.
- GAP "GAP - Groups, Algorithms, and Programming, V4.2", The GAP group, Aachen, St Andrews, www-gap.dcs.st-and.ac.uk.
- Gr R. Griess, On a subgroup of order $2^{15}|GL(5, 2)|$ in $E_8(\mathbf{C})$, the Dempwolff group and $Aut(D_8 \circ D_8 \circ D_8)$, Jour. Alg. 40(1976), 271-279.
- GPPS R. Guralnik, T. Penttila, C. Praeger, J. Saxl, Linear groups with orders having certain large prime divisors, Proc. Lond. Math. Soc. III Ser. 78(1999), 167-214.

- HB B. Huppert, N. Blackburn, "Endliche Gruppen I" and "Finite Groups II-III", Springer, 1967, 1982.
- He1 C. Hering, Transitive linear groups and linear groups which contain irreducible subgroups of prime order I, *Geom. Ded.* 2(1974), 425-460.
- He2 C. Hering, Transitive linear groups and linear groups which contain irreducible subgroups of prime order II, *Jour. Alg.* 93(1985), 151-164.
- Hou X. Hou, Cubic bent functions, *Discrete Math.*, 189(1998), 149-161.
- Hu B. Huppert, Singer-Zyklen in klassischen Gruppen, *Math. Z.*, 117(1970), 141-150.
- JLPW C. Jansen et al, "An Atlas of Brauer Characters", Clarendon Press, 1995.
- JP W. Jones, B. Parshall, On the 1-cohomology of finite groups of Lie type, in "Proc. Conf. Finite Groups 1975", W. Scott, F. Gross ed., Academic Press, 1975, pp. 313-327.
- Ka1 W. Kantor, Symplectic groups, symmetric designs and line ovals, *Jor. Alg.* 33(1975), 43-58.
- Ka2 W. Kantor, Exponential numbers of two weight codes, difference sets and symmetric designs, *Discrete Math.*, 46(1983), 95-98.
- KaLi W. Kantor, R. Liebler, The rank 3 permutation representations of the finite classical groups, *Trans. Amer. Math. Soc.* 271(1982), 1-71.
- Kl P. Kleidman, The maximal subgroups of the Steinberg triality groups ${}^3D_4(q)$ and of their automorphism groups, *Jou. Alg.* 115(1988), 182-199.
- KL P. Kleidman, M. Liebeck, "The Subgroup Structure of the Finite Classical Groups", Cambridge Univ. Press, 1990.
- La P. Landrock, "Finite Group Algebras and their Modules", Cambridge Univ. Press, 1983.
- Li1 M. Liebeck, On the orders of maximal subgroups of finite classical groups, *Proc. Lond. Math. Soc.* (3)50(1985), 426-446.
- Li2 M. Liebeck, The affine permutation groups of rank three, *Proc. Lond. Math. Soc.* (3)54(1987), 477-516.
- Lü H. Lüneburg, "Translation Planes", Springer, 1980.
- MAG "The Magma Computational Algebra System", <http://magma.maths.usyd.edu.au/magma/>
- Ma B. Mann, Difference sets in elementary abelian groups, *Ill. Jour. Math.* 9(1965), 212-219.
- McF R. McFarland, A family of noncyclic difference sets, *Jour. Comb. Theory (A)*, 15(1973), 1-10.
- McL J. McLaughlin, Some subgroups of $SL_n(F_2)$, *Ill. Jour. Math.* 13(1969), 108-115.

- MoAt "Modular Atlas Homepage", www.rwth-aachen.de/homes/MOC/.
- Qy T. Oyama, On quasifields, Osaka J. Math. 22(1985), 35-54.
- Ro O. Rothaus, On "bent" functions, Jour. Comb. Theory (A), 20(1976), 300-305.
- Si1 P. Sin, On the 1-cohomology of the groups $G_2(2^n)$, Comm. in Algebra, 20(1992), 2653-2662.
- Si2 P. Sin, Modular representations of the Hall-Janko group, Comm. in Algebra, 24(1996), 4513-4547.
- Si3 P. Sin, Personal communication.
- SZ G. Seitz, A. Zalesskii, On the minimal degree of projective representation of the finite Chevalley groups, Jour. Alg. 158(1993), 233-243.
- Wa A. Wagner, The faithful linear representations of least degree of S_n and A_n over a field of characteristic 2, Math. Z. 151(1976), 127-137.