Isomorphisms and Automorphisms of Extensions of Bilinear Dimensional Dual Hyperovals and Quadratic APN Functions

Ulrich Dempwolff
Department of Mathematics,
University of Kaiserslautern,
Kaiserslautern, Germany

Yves Edel *
Department of Mathematics,
Ghent University,
Ghent, Belgium

Abstract

In [5] an extension construction of $(n+1)$-dimensional dual hyperovals using n-dimensional bilinear dual hyperovals was introduced. Related to this construction, is a construction of APN functions in dimension $n+1$ using two APN functions in dimension n. In this paper we show that the isomorphism problem for the $(n+1)$-dimensional extensions can be reduced to the isomorphism problem of the initial n-dimensional objects. The automorphism problem can be reduced in an analogous way.

1 Introduction

In [5] we introduced a construction that transforms any symmetric, bilinear n-dimensional dual hyperoval over $\mathbb{F}_2$ into an $(n+1)$-dimensional dual hyperoval over $\mathbb{F}_2$. Taniguchi [7] shows that this construction can be generalized in a straightforward way to any bilinear n-dimensional dual hyperoval over $\mathbb{F}_2$. He uses this construction to provide new examples of simply connected DHOs — we use the abbreviation DHO for "dimensional dual hyperoval". We also showed that given an APN function defined in an n-dimensional $\mathbb{F}_2$-space one can define an APN function in an $(n+1)$-dimensional $\mathbb{F}_2$-space. This construction can be easily generalized to a construction using two (not necessarily different) APN functions instead of one.

In [5] these extension constructions were considered in detail for the special case of DHOs that are extensions of *symmetric* DHOs, and for the special case of APN functions that are extensions of *one quadratic* APN function. This led to DHOs and APN functions with many translation groups. In [5] the isomorphism and automorphism problem for the dimensional dual hyperovals and the APN

[*] The research of this author was partly supported by Research Programme G.0140.09N of the Research Foundation - Flanders (FWO).

functions in the special cases were also treated. In the present paper we discuss these questions without the restrictions made in [5].

In the next section we introduce basic notions and describe the extension constructions. These constructions guarantee, for bilinear DHOs as well as for quadratic APN functions, the existence of a large elementary abelian subgroup N of the automorphism group, which will be crucial for the further investigation of the extensions.

In Section 3 we introduce the notion of an extension group of a DHO or an APN function. The existence of an extension group characterizes those DHOs or APN functions that are extensions. Indeed it will turn out later that extension groups are just conjugates of the group N introduced in Section 2. We also present a detailed study of the embedding of the group N in the automorphism group.

In Section 4 we consider the isomorphism problem. Theorems 4.1 and 4.3 provide the complete answer. We characterize bilinear extensions of bilinear DHOs (Theorem 4.2) and quadratic extensions of APN functions (Theorem 4.4). Finally we show that the extension construction is the source of large numbers of inequivalent APN functions of degree three (see Proposition 4.8 and Example 4.9).

In Section 5 it is shown that any two extension groups of a DHO or an APN function have the same size of the intersection and that they are conjugate in the group, which they generate.

In Section 6 we show that those DHOs or APN functions that have many extension groups are obtained as multiple extensions and present examples with this property. Moreover we give a direct construction of the k-fold extension, for $k > 2$, as well as some of its automorphisms.

Automorphism groups are treated in Section 7 (Theorems 7.1 and 7.3). The group theoretic notation follows standard texts such as [1]. A survey article on dimensional dual hyperovals is Yoshiara [9].

2 Definitions, preliminary results, extensions

We start with with dimensional dual hyperovals

2.1 Extensions of bilinear DHOs

Definitions and preliminary results. (a) A set $\mathcal{S}$ of n-dimensional subspaces of a finite dimensional $\mathbb{F}_2$-vector space U is called a *dual hyperoval of rank* n[1] – we use the symbol DHO as an abbreviation – if $|\mathcal{S}| = 2^n$, $\dim S \cap S' = 1$ and $S \cap S' \cap S'' = 0$ for three different $S, S', S'' \in \mathcal{S}$. We call $\langle S \mid S \in \mathcal{S} \rangle$ the *ambient space* of the DHO and say $\mathcal{S}$ *is ambient in* U or *ambient in its defining space*, if U coincides with the ambient space. Of course, for properties of a DHO only the ambient space is important, however for proof theoretic purposes

[1] One also speaks of *dimensional dual hyperovals*. However the notion "dimension" is not used uniformly, compare for instance [5] and [9]

overspaces also come into play. If Y is a subspace of U, such that $Y \oplus S = U$ for all $S \in \mathcal{S}$, then the DHO *splits* over Y. Two DHOs are *isomorphic*, if there exists an isomorphism of the ambient spaces that maps one DHO onto the other. An *automorphism* is an isomorphism of a DHO ambient in its defining space on itself. The automorphisms form the *automorphism group* of the DHO. A subgroup T of the automorphism group of $\mathcal{S}$ is a *translation group*, if T acts regularly on $\mathcal{S}$, such that the DHO splits over $C_U(T) = \{u \in U \mid u\tau = u,\ \tau \in T\}$.

(b) Let X, Y be finite dimensional $\mathbb{F}_2$-spaces with $\dim X = n$, and let $\beta : X \to \mathrm{Hom}(X, Y)$ be a monomorphism, such that

$$\mathcal{S}_\beta = \{S_e \mid e \in X\}, \quad S_e = \{(x, x\beta(e)) \mid x \in X\},$$

is a DHO in $U = X \oplus Y$. Then $\mathcal{S}_\beta$ is called a *bilinear* DHO (i.e. the mapping $X \times X \ni (x, e) \mapsto x\beta(e) \in Y$ is bilinear). We also say that β *defines* $\mathcal{S}_\beta$. The elements $\tau_e \in \mathrm{GL}(U)$, $e \in X$, satisfying $(x, y)\tau_e = (x, y + x\beta(e))$ are automorphisms, and form a translation group. Conversely, it is shown in [5], that a DHO ambient in its defining space with a translation group is always bilinear. The mapping $\beta^o : X \to \mathrm{Hom}(X, Y)$, defined by $x\beta^o(e) = e\beta(x)$, defines a bilinear DHO $\mathcal{S}_{\beta^o}$ too, the DHO *opposite* to $\mathcal{S}_\beta$. We call β or $\mathcal{S}_\beta$ *symmetric*, if $\beta = \beta^o$.

(c) Let $\beta : X \to \mathrm{Hom}(X, Y)$ and $\beta' : X \to \mathrm{Hom}(X, Y)$ define DHOs. A triple (λ, μ, ρ), where $\lambda, \mu \in \mathrm{GL}(X)$, $\rho \in \mathrm{GL}(Y)$ is called an *isotopism* from β to β', if $\lambda \circ \beta'(e\mu) = \beta(e)\rho$ for all $e \in X$. In this case we write $\beta \sim \beta'$. Isotopisms from β to β are called *autotopisms*; they form a group in the obvious manner, the *autotopism group* of β. If (λ, μ, ρ) is an autotopism of β, then (μ, λ, ρ) is an autotopism of β^o. Moreover, if (λ, μ, ρ) is an isotopism from β to β', then $\mathrm{diag}(\lambda, \rho) : U \to U$ is an isomorphism from $\mathcal{S}_\beta$ onto $\mathcal{S}_{\beta'}$, which maps $S_e \in \mathcal{S}_\beta$ onto $S_{e\mu} \in \mathcal{S}_{\beta'}$. Here we use the following convention for the representation of linear operators.

Convention. The space $U = X \oplus Y$ is identified with $X \times Y$ and elements in $\alpha \in \mathrm{GL}(U)$ are written in the form

$$\begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix}$$

with $\alpha_{11} \in \mathrm{End}(X)$, $\alpha_{12} \in \mathrm{Hom}(X, Y), \alpha_{22} \in \mathrm{End}(Y)$, and $\alpha_{21} \in \mathrm{Hom}(Y, X)$, i.e. $(x, y)\alpha = (x\alpha_{11} + y\alpha_{21}, x\alpha_{12} + y\alpha_{22})$. This convention will also be generalized in the obvious way. From [5] we take the following, slightly generalized construction (see also [7]).

Theorem 2.1. *Let X, Y be finite dimensional $\mathbb{F}_2$-spaces, let $\beta : X \to \mathrm{Hom}(X, Y)$ define a bilinear DHO $\mathcal{S} = \mathcal{S}_\beta$. Set $\overline{X} = \mathbb{F}_2 \oplus X$ and $\overline{Y} = X \oplus Y$. For $e \in X$ define two subspaces of $\overline{X} \oplus \overline{Y}$ by*

$$S_{0,e} = \{(b, be, be + x, (be + x)\beta(e)) \mid (b, x) \in \overline{X}\},$$

$$S_{1,e} = \{(b, be + x, be, (be + x)\beta^o(e)) \mid (b, x) \in \overline{X}\},$$

and set $\overline{\mathcal{S}} = \overline{\mathcal{S}}_\beta = \{S_{a,e} \mid (a, e) \in \overline{X}\}$. *The following hold.*

(a) The set $\overline{\mathcal{S}}$ *is a DHO in* $\overline{X} \oplus \overline{Y}$.

(b) For $e \in X$ *set*

$$n_{1,e} = \begin{pmatrix} 1 & e & & \\ & \mathbf{1} & & \\ & & \mathbf{1} & \beta(e) \\ & & & \mathbf{1} \end{pmatrix}, \quad n_{0,e} = \begin{pmatrix} 1 & & e & \\ & \mathbf{1} & & \beta^o(e) \\ & & \mathbf{1} & \\ & & & \mathbf{1} \end{pmatrix}.$$

Then $N_a = \{n_{a,e} \mid e \in X\}$, $a = 0, 1$, *are elementary abelian* 2*-subgroups of* $\mathrm{Aut}(\overline{\mathcal{S}})$. *The group* N_a *fixes all elements in* $\mathcal{S}_a = \{S_{a,e} \mid e \in X\}$ *and it acts regularly on* $\mathcal{S}_{a+1}$. *In particular,* $S_{0,e}n_{1,f} = S_{0,e+f}$ *and* $S_{1,e}n_{0,f} = S_{1,e+f}$. *Moreover,* $N = N_0 \times N_1$ *is an elementary abelian group of order* $|X|^2$.

(c) Let $\alpha = (\lambda, \mu, \rho)$ *be an autotopism of* β. *Then* $u_\alpha = \mathrm{diag}(1, \mu, \lambda, \rho)$, *is an automorphism of* $\overline{\mathcal{S}}$. *The group* $L_0 = \{u_\alpha \mid \alpha \text{ autotopism of } \beta\} \leq \mathrm{Aut}(\overline{\mathcal{S}})\}$ *is isomorphic to the autotopism group of* β.

(d) Let $\phi = (\lambda, \mu, \rho)$ *be an isotopism from* β *to* β^o. *Then*

$$\tau = \begin{pmatrix} 1 & & & \\ & & \mu & \\ & \lambda & & \\ & & & \rho \end{pmatrix}$$

is an automorphism of $\overline{\mathcal{S}}$ *which normalizes* N *and interchanges* $\mathcal{S}_0$ *and* $\mathcal{S}_1$.

(e) $X \oplus Y$ *is the ambient space of* $\mathcal{S}$ *if and only if* $\overline{X} \oplus \overline{Y}$ *is the ambient space of* $\overline{\mathcal{S}}$.

Proof. For assertions (a)-(d) the proof of [5, Thm. 5.1] carries over after replacing equations of the form $x\beta(e) = e\beta(x)$ by $x\beta(e) = e\beta^o(x)$ where necessary.

For (e) we first we observe that $\mathcal{S} = \mathcal{S}_\beta$ and $\mathcal{S}^o = \mathcal{S}_{\beta^o}$ have the same ambient spaces since

$$\langle \mathcal{S} \rangle = \langle (x, 0), (0, x\beta(e)) \mid x, e \in X \rangle = \langle (x, 0), (0, e\beta^o(x)) \mid x, e \in X \rangle = \langle \mathcal{S}^o \rangle.$$

In particular $\langle \mathcal{S} \rangle = \langle \mathcal{S}^o \rangle = X \oplus Y_0$, where $Y_0 = \sum_{e \in X} \mathrm{Im}\,\beta(e)$. For the ambient space of $\overline{\mathcal{S}}$ we have $\langle \overline{\mathcal{S}} \rangle = \langle (1, 0, 0, 0), (0, 0, x, x\beta(e)), (0, x, 0, x\beta^0(e)) \mid x, e \in X \rangle$, which shows $\langle \overline{\mathcal{S}} \rangle = \mathbb{F}_2 \oplus X \oplus X \oplus Y_0$. This implies assertion (e). □

Definition. We call the DHO $\overline{\mathcal{S}}$ of Theorem 2.1 the *extension* of $\mathcal{S}$.

Remark 2.2. Let $1 \neq \nu \in N$. Then we have $\mathrm{rk}\,(\nu + \mathbf{1}) \geq n$ and if $1 \neq \nu \in N_0 \cup N_1$ then even $\mathrm{rk}\,(\nu + \mathbf{1}) = n$ holds. Here we use that $\mathrm{rk}\,\beta(e) = \mathrm{rk}\,\beta^o(e) = n - 1$ for $0 \neq e \in X$.

Notation. With the notation of the preceding theorem we set

$$L = \left\{ \begin{array}{rl} L_0\langle\tau\rangle, & \beta \sim \beta^o, \\ L_0, & \beta \not\sim \beta^o. \end{array} \right.$$

Proposition 2.3. *Let $\beta : X \to \mathrm{Hom}(X, Y)$ and $\beta' : X \to \mathrm{Hom}(X, Y)$ define bilinear DHOs. The following hold.*

(a) $\overline{\mathcal{S}}_\beta$ is isomorphic to $\overline{\mathcal{S}}_{\beta^o}$.

(b) Let β be isotopic to β'. Then $\overline{\mathcal{S}}_\beta$ are $\overline{\mathcal{S}}_{\beta'}$ isomorphic.

(c) Let γ define a symmetric DHO and assume that β is isotopic to γ. Then $\overline{\mathcal{S}}_\beta$ is a bilinear DHO.

Proof. (a) The operator

$$\tau = \begin{pmatrix} 1 & & & \\ & & \mathbf{1} & \\ & \mathbf{1} & & \\ & & & \mathbf{1} \end{pmatrix}$$

defines an isomorphism of $\overline{\mathcal{S}}_\beta$ onto $\overline{\mathcal{S}}_{\beta^o}$.

(b) Let (λ, μ, ρ) be an isotopism from β onto β'. Define $\alpha = \mathrm{diag}(1, \mu, \lambda, \rho)$. A typical element $(a, ae, (ae + x)\beta(e))$ of $S_{0,e}$ (as a subspace of $\overline{\mathcal{S}}_\beta$) is mapped onto

$$(a, ae\mu, (ae + x)\lambda, (ae + x)\rho) = (a, ae\mu, (ae + x)\lambda, (aex)\lambda\beta'(e\mu)),$$

which is an element in $S_{0,e\mu}$ (as a subspace of $\overline{\mathcal{S}}_{\beta'}$). Similarly,

$$\alpha : \overline{\mathcal{S}}_\beta \ni S_{1,e} \mapsto S_{1,e\lambda} \in \overline{\mathcal{S}}_{\beta'},$$

which shows the claim.

(c) By (b) we have $\overline{\mathcal{S}}_\beta \simeq \overline{\mathcal{S}}_\gamma$. Now [5, Theorem 3.2] completes the proof. □

2.2 Extensions of APN functions

Definitions and preliminary results. (a) Let X and Y be two finite dimensional $\mathbb{F}_2$-spaces and let $f : X \to Y$ be a function. We call f *normed* if $f(0) = 0$ and the set $\mathcal{S}_f = \{(x, f(x)) \mid x \in X\} \subseteq U = X \oplus Y$ is called the *graph* of f. The space $\langle \mathcal{S}_f \rangle$ is the *ambient space* of f. Usually $\langle x + y \mid x, y \in \mathcal{S}_f \rangle$ is a proper subspace of the ambient space, but if f is normed both spaces coincide. We say

$X \oplus Y$ is *ambient to f* or *f is ambient in its defining space*, if f is normed and $X \oplus Y$ is the ambient space. Mostly we will consider normed functions that are ambient in their defining space, however for proof theoretic purposes also non-ambient functions also come into play.

Two functions $f_i : X \to Y$ are *equivalent*, if there exists an affine transformation Γ of $X \oplus Y$ with $\mathcal{S}_{f_1} = \mathcal{S}_{f_0}\Gamma$. We also say that Γ is an *isomorphism* from f_0 to f_1. An *automorphism* is an isomorphism of a function on itself. The automorphisms form the *automorphism group* $\mathrm{Aut}(f)$ of the function f. With respect to automorphism groups we will usually only consider functions that are ambient in their defining space. Then the automorphism group acts faithfully on the graph $\mathcal{S}_f$ (see [5, Sec. 2]).

A function $f : X \to Y$ is an *APN function*, if for each $0 \neq x_0 \in X$ and each $y_0 \in Y$ the equation $f(x + x_0) + f(x) = y_0$ has at most two solutions. Note that if x is one solution, then $x + x_0$ is the second solution. We call $\dim X$ the *rank* of the APN function. If not otherwise stated, we will always assume, **that APN functions are normed**. From [3, Thm. 5] we take:

Lemma 2.4. *(Four-sum-condition) The normed function $f : X \to Y$ is APN, if and only if for every four every quadruple $s_1, \ldots, s_4 \in \mathcal{S}_f$ we have $s_1 + s_2 + s_3 + s_4 \neq 0$.*

We denote elements of $\mathrm{AGL}(U)$ by symbols $\overline{\tau} = \tau + c_\tau$ with $\tau \in \mathrm{GL}(U)$, $c_\tau \in U$ if

$$u\overline{\tau} = u\tau + c_\tau, \quad u \in U.$$

We call the linear transformation τ the *linear part* of $\overline{\tau}$ and c_τ the *translation part.* By [5, Lemma 2.1] we know that for an APN function f, with U ambient to f, the restriction of the epimorphism $\phi : \mathrm{AGL}(U) \to \mathrm{GL}(U)$, $\overline{\tau} \mapsto \tau$, to the group $\mathrm{Aut}(f)$, is a group monomorphism. By $\mathbf{A}(f)$ we denote the image of ϕ of $\mathrm{Aut}(f)$ and call it *the linear part* of the automorphism group.

In the sequel we will frequently use the isomorphism

$$\mathrm{Aut}(f) \simeq \mathbf{A}(f)$$

and switch back and forth between these groups whenever it is convenient.

For a function $f : X \to Y$ we associate a mapping $\beta_f : X \times X \to Y$ by

$$\beta_f(x, x') = f(x + x') + f(x) + f(x') + f(0)$$

and call f *quadratic*, if and only if β_f is a (symmetric) bilinear mapping. If f is quadratic, we also identify β_f with an element of $\mathrm{Hom}(X, \mathrm{Hom}(X, Y))$ by defining

$$x\beta_f(y) = \beta_f(x, y).$$

We recall a basic connection between quadratic APN functions and alternating DHOs (see [5, Thm. 2.4], [6], or [10]): If f is a quadratic (ambient) APN function, then β_f defines an alternating DHO, and if β defines an alternating DHO, then there exists a quadratic APN function, such that $\beta = \beta_f$.

(b) Let $f_i : X \to Y$, $i = 0, 1$, be two functions. A triple (λ, ρ, γ), where $\lambda \in \mathrm{GL}(X)$, $\rho \in \mathrm{GL}(Y)$, and $\gamma \in \mathrm{Hom}(X, Y)$ is called an *isotopism* from f_0 to f_1, if

$$f_1(x\lambda) = f_0(x)\rho + x\gamma;$$

we then write $f_0 \sim f_1$. Then

$$\phi = \begin{pmatrix} \lambda & \gamma \\ & \rho \end{pmatrix} \in \mathrm{GL}(U)$$

is an isomorphism from $\mathcal{S}_{f_0}$ to $\mathcal{S}_{f_1}$. Isotopisms from f to f are called *autotopisms*; they form a group in the obvious manner, $\mathrm{Autop}(f)$, the *autotopism group of f*. Again we will only consider autotopisms of functions ambient in their defining spaces.

(c) Let U be an $\mathbb{F}_2$-space, Y a subspace and $\phi, \psi \in \mathrm{GL}(U)$ that fix Y. We say that ϕ and ψ are *linked (with respect to Y)*, if $\phi_Y = \psi_Y$. Let $U = X \oplus Y$, let $f_i : X \to Y$, $0 \leq i \leq 3$, be APN functions, and let $\phi : f_0 \to f_2$ and $\phi' : f_1 \to f_3$ be isotopisms. Then we say that the pair (f_0, f_1) is *isotopically linked to the pair* (f_2, f_3), if ϕ and ϕ' are linked (with respect to Y). In the case where $f_2 = f_1$ and $f_3 = f_0$ we simply say that f_0 and f_1 are *isotopically linked.*

From [5] we take (with minimal changes) the following construction.

Theorem 2.5. *Let X, Y be finite dimensional $\mathbb{F}_2$-spaces and let $f_i : X \to Y$, $i = 0, 1$, be two APN functions. Set $\overline{X} = \mathbb{F}_2 \oplus X$ and $\overline{Y} = X \oplus Y$. Then $F = F_{f_0,f_1} : \overline{X} \to \overline{Y}$ defined by*

$$F(a, x) = (ax, (a + 1)f_0(x) + af_1(x))$$

is an APN function. Moreover, $\langle \mathcal{S}_F \rangle = \overline{X} \oplus \overline{Y}$, if and only if $\langle \mathcal{S}_{f_i} \rangle = X \oplus Y_i$, $i = 0, 1$, such that $Y = Y_0 + Y_1$.

Proof. The APN property of F has the same simple verification as in [5, Theorem 5.3]. For the ambient spaces we observe that

$$\langle \mathcal{S}_F \rangle = (\mathbb{F}_2 \oplus 0 \oplus 0 \oplus 0) + W_0 + W_1$$

with

$$W_0 = \{(0, x, 0, y) \mid (x, y) \in \langle \mathcal{S}_{f_0} \rangle\}, \quad W_1 = \{(0, x, x, y) \mid (x, y) \in \langle \mathcal{S}_{f_1} \rangle\}.$$

Hence $\langle \mathcal{S}_F \rangle = \overline{X} \oplus \overline{Y}$ if and only if $X \subseteq \langle \mathcal{S}_{f_0} \rangle \cap \langle \mathcal{S}_{f_1} \rangle$ and $Y = (\langle \mathcal{S}_{f_0} \rangle \cap Y) + (\langle \mathcal{S}_{f_1} \rangle \cap Y)$. □

Definition. We call the function F_{f_0,f_1} of Theorem 2.5 the *extension* of f_0 and f_1. If f_i, $i = 0, 1$, are ambient in $X \oplus Y$, we also call F_{f_0,f_1} *fully ambient (in $\overline{X} \oplus \overline{Y}$).*

Usually we will only consider fully ambient extensions. However sometimes we will also need to use extensions that are ambient in their defining space, but not fully ambient.

Proposition 2.6. *Let $f_0, f_1 : X \to Y$ be two APN functions. The following hold.*

(a) F_{f_0,f_1} is equivalent to F_{f_1,f_0}.

(b) Let $\overline{\alpha}_i$, $i = 0, 1$, be affine operators from X to Y. Then F_{f_0,f_1} is equivalent to $F_{f_0+\overline{\alpha}_0,f_1+\overline{\alpha}_1}$.

(c) Let F_{f_0,f_1} be quadratic. Then f_0 and f_1 are quadratic, $\beta_{f_0} = \beta_{f_1}$ and F_{f_0,f_1} is equivalent to F_{f_0,f_0}.

Proof. (a) The operator $\overline{\tau} \in \mathrm{AGL}(\overline{X} \oplus \overline{Y})$ defined by

$$\overline{\tau} = \tau + c_\tau,\ \tau = \begin{pmatrix} 1 & & & \\ & \mathbf{1} & \mathbf{1} & \\ & & \mathbf{1} & \\ & & & \mathbf{1} \end{pmatrix},\ c_\tau = (1, 0, 0, 0),$$

interchanges the graphs of F_{f_0,f_1} and F_{f_1,f_0}.

(b) Let α_i be the linear part of $\overline{\alpha}_i$ and a_i its translation part. Set

$$\overline{\tau} = \tau + c_\tau,\ \tau = \begin{pmatrix} 1 & & & a_0 + a_1 \\ & \mathbf{1} & & \alpha_1 \\ & & \mathbf{1} & \alpha_0 + \alpha_1 \\ & & & \mathbf{1} \end{pmatrix},\ c_\tau = (0, 0, 0, a_1),$$

A typical element $(a, x, ax, af_0(x)+(a+1)f_1(x))$ of the graph of F_{f_0,f_1} is mapped onto

$$(a, x, ax, a(f_0(x) + x\alpha_0 + a_0) + (a + 1)(f_1(x) + x\alpha_1 + a_1)),$$

which is an typical element of the graph of $F_{f_0+\overline{\alpha}_0,f_1+\overline{\alpha}_1}$.

(c) Set $B = \beta_{F_{f_0,f_1}}$, $\beta_0 = \beta_{f_0}$, and $\beta_1 = \beta_{f_1}$. A computation shows that

$$B((a, x), (b, x')) = (ax' + bx, (a + b + 1)\beta_0(x, x') + (a + b)\beta_1(x, x')).$$

Set $\Delta = B((a, x), (b_0 + b_1, x_0 + x_1)) + B((a, x), (b_0, x_0)) + B((a, x), (b_1, x_1))$, which is by assumption 0 for all $(a, x), (b_0, x_0), (b_1, x_1)$. Now $\Delta = (0, Q + P)$ with

$$Q = (a+b_0+b_1+1)\beta_0(x, x_0+x_1)+(a+b_0+1)\beta_0(x, x_0)+(a+b_1+1)\beta_0(x, x_1)$$

and

$$P = (a + b_0 + b_1)\beta_1(x, x_0 + x_1) + (a + b_0)\beta_1(x, x_0) + (a + b_1)\beta_1(x, x_1).$$

Setting $a = b_0 = b_1 = 0$ shows that β_0 is bilinear and setting $a = 1$, $b_0 = b_1 = 0$ shows that β_1 is bilinear too. This shows that

$$\Delta = (0, b_0(\beta_0(x, x_0) + \beta_1(x, x_0)) + b_1(\beta_0(x, x_1) + \beta_1(x, x_1)))$$

and $\beta_0 = \beta_1$ follows. Assume first that f_0 and f_1 are normed. By [5, Thm. 2.4] we obtain $f_1 = f_0+\alpha$ where $\alpha \in \mathrm{Hom}(X, Y)$. Apply part (b) of this proposition. In the general case we can apply part (b) of this proposition and reduce this case to the normed case. □

A transformation and some automorphisms. Let $F = F_{f_0,f_1} : \overline{X} \to \overline{Y}$ be the extension of two normed, APN functions $f_i : X \to Y$ and assume that F is ambient in $\overline{X} \oplus \overline{Y}$. We apply the linear transformation

$$\tau = \begin{pmatrix} 1 & & & \\ & \mathbf{1} & & \\ & \mathbf{1} & \mathbf{1} & \\ & & & \mathbf{1} \end{pmatrix}$$

to the graph of F. Then $\mathcal{S} := \mathcal{S}_F \tau$ has a more symmetric appearance $\mathcal{S} = \mathcal{S}_0 \cup \mathcal{S}_1$ with

$$\mathcal{S}_0 = \{(0, x, 0, f_0(x)) \mid x \in X\}, \quad \mathcal{S}_1 = \{(1, 0, x, f_1(x)) \mid x \in X\}.$$

Suppose that $\phi = \begin{pmatrix} \lambda & \gamma \\ & \rho \end{pmatrix} \in \mathrm{Autop}(f_0)$ and $\phi' = \begin{pmatrix} \mu & \delta \\ & \rho \end{pmatrix} \in \mathrm{Autop}(f_1)$ is a pair of linked autotopisms. Set

$$\Phi_{\phi,\phi'} = \begin{pmatrix} 1 & & & \\ & \lambda & & \gamma \\ & & \mu & \delta \\ & & & \rho \end{pmatrix}.$$

Then $\Phi_{\phi,\phi'}$ is an automorphism of F, which fixes $\mathcal{S}_0$ and $\mathcal{S}_1$. Also

$$L_0 = \{\Phi_{\phi,\phi'} \mid \phi \in \mathrm{Autop}(f_0),\ \phi' \in \mathrm{Autop}(f_1),\ \phi \text{ linked to } \phi'\}$$

is obviously a subgroup $L_0 \leq \mathrm{Aut}(F) \cap \mathbf{A}(F)$.

Finally assume that there exist linked isotopisms $\phi = \begin{pmatrix} \lambda & \gamma \\ & \rho \end{pmatrix}$ from f_0 to f_1 and $\phi' = \begin{pmatrix} \mu & \delta \\ & \rho \end{pmatrix}$ from f_1 to f_0, i.e. f_0 and f_1 are isotopically linked. Define $\overline{\Psi}_{\phi,\phi'} = \Psi_{\phi,\phi'} + c_\psi$ by

$$\Psi_{\phi,\phi'} = \begin{pmatrix} 1 & & & \\ & & \lambda & \gamma \\ & \mu & & \delta \\ & & & \rho \end{pmatrix}, \quad c_\Psi = (1, 0, 0, 0).$$

Then $\overline{\Psi}_{\phi,\phi'}$ is an automorphism of F, which interchanges $\mathcal{S}_0$ and $\mathcal{S}_1$. If $\overline{\Psi}_{\varphi,\varphi'}$ is an automorphism to the linked pair φ, φ' too, then

$$\overline{\Psi}_{\phi,\phi'} \circ \overline{\Psi}_{\varphi,\varphi'} = \Phi_{\phi\circ\varphi,\phi'\circ\varphi'}.$$

We set

$$\overline{L} = \begin{cases} L_0 = \overline{L}_0, & \text{if } f_0 \text{ and } f_1 \text{ are not isotopically linkend,} \\ L_0\langle \overline{\Psi}_{\phi,\phi'} \rangle, & \text{if } f_0 \text{ and } f_1 \text{ are isotopically linkend.} \end{cases}$$

Note that the definition of L is independent of the choice of $\overline{\Psi}_{\phi,\phi'}$.

We now assume in addition that f_0 and f_1 are quadratic. For $i \in \mathbb{F}_2$ and $e \in X$ define $\overline{n}_{i,e} = n_{i,e} + c_{i,e}$, where

$$n_{0,e} = \begin{pmatrix} 1 & & e & f_1(e) \\ & \mathbf{1} & & \\ & & \mathbf{1} & \beta_1(e) \\ & & & \mathbf{1} \end{pmatrix}, \; n_{1,e} = \begin{pmatrix} 1 & e & & f_0(e) \\ & \mathbf{1} & & \beta_0(e) \\ & & \mathbf{1} & \\ & & & \mathbf{1} \end{pmatrix},$$

$\beta_i = \beta_{f_i}$, and $c_{0,e} = 0$, $c_{1,e} = (0, e, 0, f_0(e))$. Then $\overline{n}_{i,e} \in \mathrm{Aut}(F)$. The groups $\overline{N}_i = \{\overline{n}_{i,e} \mid e \in X\}$ are elementary abelian of order $|X|$. Moreover, $\overline{N}_i$ fixes $\mathcal{S}_i$ pointwise and acts regularly on $\mathcal{S}_{i+1}$. The group $\overline{N} = \overline{N}_0 \times \overline{N}_1$ is elementary abelian too. A routine verification shows that the group $\overline{L}$ normalizes $\overline{N}$. The two subgroups $\overline{N}_i$, $i = 0, 1$, are normalized by $\overline{L}_0$ too, while elements in $\overline{L} - \overline{L}_0$ interchange both groups under conjugation.

Remark 2.7. Let $1 \neq \nu \in N$. Then we have $\mathrm{rk}\,(\nu + \mathbf{1}) \geq n$ and if $1 \neq \nu \in N_0 \cup N_1$, then even $\mathrm{rk}\,(\nu + \mathbf{1}) = n$ holds. Here we use that $\mathrm{rk}\,\beta_0(e) = \mathrm{rk}\,\beta_0(e) = n - 1$ for $0 \neq e \in X$.

We add two observations on APN functions. Firstly we give an intrinsic characterization for isotopic APN functions to be isotopically linked.

Lemma 2.8. *Let $f_0, f_1 : X \to Y$ be two APN functions and let $\phi : f_0 \to f_1$ be an isotopism. The following are equivalent:*

(a) There exists $\alpha \in \mathrm{Autop}(f_0)$, such that ϕ^2 and α are linked with respect to Y.

(b) f_0 and f_1 are isotopically linked.

Proof. (a)⇒(b) Set $\rho = \phi_Y$ and let $\alpha_Y = \rho^2$. Define $\phi' : f_1 \to f_0$ by $\phi' = \phi^{-1} \circ \alpha$. Then $\phi'_Y = \rho^{-1}\rho^2 = \rho$ and (b) follows.

(b)⇒(a) Let $\phi' : f_1 \to f_0$ be linked to ϕ i.e. $\rho = \phi_Y = \phi'_Y$. Then we have $\alpha = \phi \circ \phi' \in \mathrm{Autop}(f_0)$ and $\rho^2 = \alpha_Y = \phi^2_Y$. □

Let f be a quadratic APN function and $\beta = \beta_f$ the associated bilinear form. If f is not ambient in its defining space, the ambient space of f and the ambient space of the DHO defined by β can be different. However if f is ambient, such unwanted side effects do not occur:

Lemma 2.9. *Let X, Y be finite dimensional $\mathbb{F}_2$-spaces.*

(a) Let $\beta : X \to \mathrm{Hom}(X, Y)$ be a monomorphism defining an alternating DHO that is ambient in $X \oplus Y$. Let $f : X \to Y$ be a quadratic APN function, such that $\beta = \beta_f$. Then f is ambient in $X \oplus Y$.

(b) Let $f : X \to Y$ be a quadratic APN function, such that f is ambient in $X \oplus Y$. Set $\beta = \beta_f$. Then $\beta : X \to \mathrm{Hom}(X, Y)$ is a monomorphism defining an alternating DHO that is ambient in $X \oplus Y$.

Proof. (a) By assumption $x\beta(e) = f(x+e) + f(x) + f(e)$, $x, e \in X$, which shows that $\sum_{e\in X} \operatorname{Im}\beta(e) \subseteq Y \cap \langle \mathcal{S}_f \rangle$. By assumption we have also $X \oplus Y = \langle X(e) \mid e \in X \rangle$, where $X(e) = \{(x, x\beta(e)) \mid x \in X\}$. As $X = X(0)$, we get $Y = \sum_{e\in X} \operatorname{Im}\beta(e) \subseteq \langle \mathcal{S}_f \rangle$. But then $X \subseteq \langle \mathcal{S}_f \rangle$ too.

(b) Set $Y_0 = \sum_{e\in X} \operatorname{Im}\beta(e) \subseteq Y$. We claim $Y = Y_0$, which in turn implies the assertion. The DHO defined by β lies in $X \oplus Y_0$. By [5, Thm. 2.4], there exists a quadratic APN function $g : X \to Y_0$, such that $\beta_g = \beta = \beta_f$ and $f = g + \delta$ for some $\delta \in \operatorname{Hom}(X, Y)$. Clearly, the DHO defined by β has the ambient space $X \oplus Y_0$ and by (a) this is the ambient space of g too. If we define $\delta \in \operatorname{GL}(X \oplus Y)$ by $(x, y)\delta = (x, x\delta + y)$, we see that $\langle \mathcal{S}_g \rangle = \langle \mathcal{S}_f \rangle\delta$. Hence $\dim X + \dim Y_0 = \dim\langle \mathcal{S}_g \rangle = \dim\langle \mathcal{S}_f \rangle = \dim X + \dim Y$. Thus $Y = Y_0$. □

3 Extension groups

Motivated by the properties of the group N of the last section we introduce the notion of an extension group. We shall show that the existence of an extension group characterizes extensions of bilinear DHOs and extensions of quadratic APN functions (Theorem 3.2). The main result of this section (Theorem 3.6) states that extension groups form a conjugacy class in the automorphism group of the DHO (or the APN function) and that an extension group is weakly closed in every Sylow 2-subgroup of the automorphism group, which contains this extension group.

From now on we use the label (DHO) and speak of the **DHO case**, if we work with a dual hyperoval. We use the label (APN) and speak of the **APN case**, if we work with an APN function.

Definition. Let $\mathcal{S} \subseteq U$ be a DHO of rank $n+1$ over $\mathbb{F}_2$ or the graph of an APN function F of rank $n+1$ ambient in its defining space. Let $E = \langle E_0, E_1 \rangle$ be a subgroup of $\operatorname{Aut}(\mathcal{S})$ (DHO) (or of $\mathbf{A}(F)$ (APN)). Set $\mathcal{T}_i = \operatorname{Fix}_{\mathcal{S}}(E_i)$ (DHO) and $\mathcal{T}_i = \operatorname{Fix}_{\mathcal{S}}(\overline{E}_i)$ (APN) and set further $V_i = \langle S \cap S' \mid S, S' \in \mathcal{T}_i, S \neq S' \rangle$ (DHO) and $V_i = \langle x + y \mid x, y \in \mathcal{T}_i \rangle$ (APN), $i = 0, 1$. We call E a *weak extension group* if:

(E1) $\mathcal{S} = \mathcal{T}_0 \cup \mathcal{T}_1$ is a partition and $|\mathcal{T}_i| = 2^n$ for $i = 0, 1$.

(E2) E_i (DHO) respectively $\overline{E}_i$ (APN) acts regularly on $\mathcal{T}_j$, $\{i, j\} = \{0, 1\}$.

(E3) Set $C_U(E) = Y$. Then $V_0 + V_1 + Y$ has codimension 1 in U and the dimension $(V_0 + V_1 + Y)/Y = 2n$.

If, in addition,

(E4) $Y = V_0 \cap V_1$

holds, we call E an *extension group*.

Remark 3.1. (a) Clearly, E_0 and E_1 intersect trivially and the two groups centralize each other, i.e. $E = E_0 \times E_1$. Also $V_0 \cap V_1 \subseteq Y$, as E_i centralizes

V_i. We justify the name "extension group" by proving the reconstruction result Theorem 3.2 below. Note that the group N of the last section, which acted on the extension of a DHO or the graph of two APN functions is indeed an extension group in the case of a DHO. In the case of the extension $F_{f_0.f_1}$ of two quadratic APN functions f_i, $i = 0, 1$, the group N is a weak extension group. Moreover, N is actually an extension group if and only if F_{f_0,f_1} is fully ambient.

(b) In [5] we defined translation groups for DHOs and APN functions, which lie ambient in their defining space. We need slight generalizations of the basic results of translation groups in the non-ambient case. Let $\mathcal{S}$ be a DHO (not necessarily ambient) in U. Let T be a subgroup of $\mathrm{GL}(U)$, such that (1) $\mathcal{S}\tau = \mathcal{S}$, $\tau \in T$, (2) T acts regularly on $\mathcal{S}$, and (3) DHO splits over $C_U(T)$. We call T a *translation group* of the DHO. Let $\mathcal{S} = \mathcal{S}_f \subseteq U = X \oplus Y$ be the graph of the normed APN function $f : X \to Y$ (f not necessarily ambient in $U = X \oplus Y$). Let $\overline{T}$ be a subgroup of $\mathrm{AGL}(U)$ and T its the linear part. We call $\overline{T}$ or T a *translation group* if (1) $\overline{T} \simeq T$, (2) $\overline{T}$ acts regularly on $\mathcal{S}$, and (3) $\mathcal{S}$ is a set of coset representatives for $C_U(T)$. If $\dim U/C_U(T) \geq 4$, it is then not difficult to show that in both cases the group T still satisfies Hypothesis A of [5, Section 3]. Then by [5, Thm. 3.1] T is elementary abelian and T has a quadratic action on U. Also Theorems 3.2 and 3.5 of [5] are still true, i.e. DHOs with a translation group are bilinear and APN functions with a translation group are quadratic.

Theorem 3.2. *Let E be a weak extension group with $\mathcal{S}$, U, etc. being as in the definition, and assume in addition that $n \geq 4$. Then the weak extension group $E = E_0 \times E_1$ is elementary abelian of order 2^{2n}. Moreover:*

(a) (DHO) $\mathcal{S}$ is the extension of a bilinear DHO $\mathcal{S}_\beta$ in V_0 of rank n and E is an extension group. Moreover, V_0 is the ambient space of $\mathcal{S}_\beta$.

(b) (APN) $\mathcal{S} = \mathcal{S}_F$, where $F = F_{f_0,f_1}$ is the extension of quadratic APN functions f_0 and f_1. Moreover, E is an extension group, if and only if F is fully ambient.

Proof. (a) DHO CASE. Since $V_0 + V_1 + Y$ is a proper subspace, there exist $S_i \in \mathcal{T}_i$, $i = 0, 1$, such that $v \notin V_0 + V_1 + Y$, where $S_0 \cap S_1 = \langle v \rangle$. As E acts transitively on the pairs $(S, S') \in \mathcal{T}_0 \times \mathcal{T}_1$, we see $S \cap S' \nsubseteq V_0 + V_1 + Y$ for all such pairs. So if $\{i, j\} = \{0, 1\}$ and $S \in \mathcal{T}_i$, then

$$(S \cap V_i) - 0 = \bigcup_{S' \in \mathcal{T}_i - \{S\}} ((S \cap S') - 0) \text{ and } S - (S \cap V_i) = \bigcup_{S' \in \mathcal{T}_j} ((S \cap S') - 0)$$

are partitions. As an immediate consequence we observe, that $\mathcal{D}_i = \{S \cap V_i \mid S \in \mathcal{T}_i\}$, $i = 0, 1$, is a DHO in V_i and thus in $V_i + Y$ too.

Pick $S \in \mathcal{T}_i$, $i = 0, 1$. Then $S \cap Y = \bigcap_{\tau \in E_j} (S \cap Y)\tau \subseteq \bigcap_{\tau \in E_j} S\tau = 0$, $\{i, j\} = \{0, 1\}$, by the basic properties of a DHO. Hence $\dim(V_i + Y)/Y \geq n$, $i = 0, 1$, as $\dim S \cap V_i = n$. Then $\dim(V_0 + V_1 + Y)/Y = 2n$ implies $V_0 + V_1 + Y = (S_0 \cap V_0) \oplus (S_1 \cap V_1) \oplus Y$ and the DHO $\mathcal{D}_i$ in $V_i + Y$ splits over Y. Also as E_0 acts regularly on $\mathcal{D}_1$, we see that E_0 induces a translation group on this DHO.

By [5, Theorem 3.2] (here we need $n \geq 4$) and (b) of Remark 3.1 there exist homomorphisms $\tau : S_0 \cap V_0 \to E_0$ and $\beta : S_0 \cap V_0 \to \mathrm{Hom}(S_1 \cap V_1, Y)$, such that the restriction of the element $\tau_e \in E_0$ to $V_1 + Y = (S_1 \cap V_1) \oplus Y$ has with respect to this decomposition, the form

$$\begin{pmatrix} \mathbf{1} & \beta(e) \\ & \mathbf{1} \end{pmatrix}$$

and with respect to the decomposition $U = \langle v \rangle \oplus (S_0 \cap V_0) \oplus (S_1 \cap V_1) \oplus Y$ (note that E_0 acts regularly on $S_0 - (S_0 \cap V_0) = v + (S_0 \cap V_0)$) we get the description

$$\tau_e = \begin{pmatrix} 1 & e & & \\ & \mathbf{1} & & \\ & & \mathbf{1} & \beta(e) \\ & & & \mathbf{1} \end{pmatrix}.$$

By symmetry there are homomorphisms $\tau' : S_1 \cap V_1 \to E_1$, and $\beta' : S_1 \cap V_1 \to \mathrm{Hom}(S_0 \cap V_0, Y)$, such that a typical element $\tau'_f \in E_1$ is represented in the form

$$\tau'_f = \begin{pmatrix} 1 & & f & \\ & \mathbf{1} & & \beta'(f) \\ & & \mathbf{1} & \\ & & & \mathbf{1} \end{pmatrix}.$$

Since τ_e and τ'_f commute, we get $f\beta(e) = e\beta'(f)$, i.e. $\beta' = \beta^o$. The identification $S_0 \cap V_0 \simeq S_1 \cap V_1 \simeq \mathbb{F}_2^n$ shows that $\mathcal{S}$ is the extension of $\mathcal{D}_0$.

Let $(S_0 \cap V_0) \oplus W$, $W \subseteq Y$, be the ambient space of β. Then the ambient space of β^o is $(S_1 \cap V_1) \oplus W$. Thus $\langle v \rangle \oplus (S_0 \cap V_0) \oplus (S_1 \cap V_1) \oplus W$ is the ambient space of $\mathcal{S}$. The last assertion follows too.

(b) APN CASE. We choose the notation so that $0 \in \mathcal{T}_0$. In particular $V_0 = \langle \mathcal{T}_0 \rangle$. Since $V_0 + V_1 + Y$ is a proper subspace of U, then (using the definition of the ambient space), there is a $v \in \mathcal{S} - (V_0 + V_1 + Y)$. This forces $v \in \mathcal{T}_1$ and $\mathcal{T}_1$ lies in the flat $v + V_1$, respectively $v + \mathcal{T}_1 \subseteq V_1$. As $\overline{E}_0$ fixes $\mathcal{T}_0$ pointwise, we have $\overline{E}_0 = E_0$ and $\mathcal{T}_1 = \{v\tau \mid \tau \in E_0\}$.

Define R_i by $V_i + Y = R_i \oplus Y$. Suppose $1 \neq \tau \in E_0$ such that $y = v\tau + v \in Y$. Let $1 \neq \tau' \in E_0$, $\tau' \neq \tau$ and set $u = v + v\tau'$. Then $v\tau\tau' = v\tau' + y\tau' = v + u + y$. This implies $v + v\tau + v\tau' + v\tau\tau' = 0$, which is in conflict with the four-sum-condition. We conclude that

$$2^n = |\{v + v\tau \mid \tau \in E_0\}| = |\{v + t + Y \mid t \in \mathcal{T}_1\}|.$$

Since $\mathcal{T}_0 = \{0\overline{\sigma} \mid \overline{\sigma} \in \overline{E}_1\}$, we have $\mathcal{T}_0 = \{c_\sigma \mid \sigma \in E_1\}$, where $\overline{\sigma} = \sigma + c_\sigma$. Suppose $1 \neq \sigma \in E_1$, such that $c_\sigma \in Y$. Pick $\sigma' \in E_1$, $\sigma' \neq 1, \sigma$. Then

$$c_{\sigma\sigma'} = 0\overline{\sigma}\overline{\sigma}' = c_\sigma\sigma' + c_{\sigma'} = c_\sigma + c_{\sigma'}.$$

But then $0 = 0 + c_\sigma + c_{\sigma'} + c_{\sigma\sigma'}$, contradicting the four-sum-condition. Again

$$2^n = |\{c_\sigma \mid \sigma \in E_1\}| = |\{t + Y \mid t \in \mathcal{T}_0\}|.$$

Write $w \in V_0$ as $w = x_w + y_w$, $x_w \in R_0$, $y_w \in Y$ and define $f_0 : R_0 \to Y$ by $f_0(x) = y_{c_w}$, where $c_w \in \mathcal{T}_0$ is the unique element with $x_{c_w} = x$. Then $\mathcal{T}_0$ is the graph of f_0. The four-sum-condition shows that f_0 is an APN function. Moreover $\overline{E}_1$ is a translation group on $\mathcal{T}_0$, i.e. f_0 is quadratic and E_1 is elementary abelian by Remark 3.1 (b) and [5, Theorem 3.5].

Similarly, write $w \in V_1$ as $w = z_w + y_w$, where $z_w \in R_1$ and $y_w \in Y$. Define $f_1 : R_1 \to Y$ by $f_1(z) = y_{c_w}$, where $v + c_w$ is the unique element in $\mathcal{T}_1$, such that $z_{c_w} = z$. Then $\mathcal{T}_1 + v$ is the graph of f_1 and f_1 is APN by the four-sum-condition. Define $\phi : E_0 \to \mathrm{AGL}(V_1)$ by

$$w\phi(\tau) = w\tau + v\tau + v.$$

Then

$$w\phi(\tau)\phi(\tau') = w\tau\tau' + v\tau\tau' + v\tau' + v\tau' + v = w\phi(\tau\tau'),$$

i.e. ϕ is a homomorphism, and is, in fact, a monomorphism as the $v\tau + v$'s are pairwise different. Moreover $\phi(E_0)$ induces a translation group on the graph of f_1. Thus f_1 is quadratic too and E_0 is elementary abelian. Identifying R_i with $\mathbb{F}_2^n$ we observe that $\mathcal{S}$ is the graph of the extension of f_0 and f_1. The last assertion of (b) follows from Theorem 2.5. □

Remark 3.3. With respect to extension groups there is a significant difference between the DHO case and the APN case. For DHOs the notion of a weak extension group and the notion of an extension group coincide, which is not true in the APN case. If an extension $F = F_{f_0,f_1}$ is quadratic however, then by Theorem 4.4 both functions f_0 and f_1 are ambient in $\mathbb{F}_2^n \oplus Y$, i.e. F is fully ambient and therefore N is an extension group (and thus by Theorem 3.6 every weak extension group is an extension group).

Lemma 3.4. *Weak extension groups of a DHO or an APN function are self-centralizing in the automorphism group.*

Proof. We assume the notation of the definition of an extension group. Pick $\sigma \in C_{\mathrm{Aut}(\mathcal{S})}(N)$ (DHO), respectively $\overline{\sigma} \in C_{\mathrm{Aut}(f)}(\overline{N})$ (APN). Then this element leaves both E-orbits (DHO), respectively both $\overline{E}$-orbits (APN), $\{\mathcal{T}_0, \mathcal{T}_1\}$ as a set invariant. Clearly, this element does not interchange both sets. We can now adjust σ (DHO) or $\overline{\sigma}$ (APN) by some element in E (DHO), respectively in $\overline{E}$ (APN), such that this element has fixed points in $\mathcal{T}_0$ and $\mathcal{T}_1$. Now E (DHO), respectively $\overline{E}$ (APN), acts on the set of fixed points of σ, respectively $\overline{\sigma}$, in $\mathcal{T}$. We deduce that σ, respectively $\overline{\sigma}$, fixes $\mathcal{T}$ pointwise. We conclude that $\sigma = 1$ (as $\mathcal{T}$ is ambient in the defining space) and the proof is complete. □

Remark 3.5. For the remainder of this section X, Y will denote $\mathbb{F}_2$-spaces with $\dim X = n$ and $\dim Y = m$. We set $\overline{X} = \mathbb{F}_2 \oplus X$, $\overline{Y} = X \oplus Y$, and $U = \overline{X} \oplus \overline{Y}$. We will consider simultaneously two situations:

DHO The monomorphism $\beta : X \to \mathrm{Hom}(X, Y)$ defines a bilinear DHO $\mathcal{S}_\beta$ ambient in $X \oplus Y$. We denote by $\mathcal{S} = \overline{\mathcal{S}}_\beta$ the extension of $\mathcal{S}_\beta$.

APN $f_0, f_1 : X \to Y$ denote normed, quadratic APN functions ambient in $X \oplus Y$ and $F = F_{f_0,f_1} : \overline{X} \to \overline{Y}$ will be the extension of f_0 and f_1. Moreover $\mathcal{S} = \mathcal{S}_F$ will be the graph of F.

So in both cases the group N of Section 2 is an **extension group (and not only a weak extension group)**. For the remainder of this section we denote by G the automorphism group of the extension (DHO) or the linear part of the extension (APN). The subgroups N, N_0, N_1, L, …etc. and the symbols $\mathcal{S}_0$ and $\mathcal{S}_1$ will have the same meaning as Subsections 2.1 and 2.2 (more precisely in the APN case we refer to the more symmetric representation of the graph introduced *after* Proposition 2.6). In particular we set

$$W_0 = 0 \oplus X \oplus 0 \oplus Y, \quad W_1 = 0 \oplus 0 \oplus X \oplus Y,$$

and $U_0 = W_0 \cap W_1$. **We assume in addition**

$$n \geq 4.$$

The following characterization of the group N will be important.

Theorem 3.6. *With the assumptions of Remark 3.5 the following hold: Any weak extension group in G is conjugate to N (and is therefore an extension group), and N is the only (and thus normal) extension group in every Sylow 2-subgroup of G that contains N.*

Corollary 3.7. *Let G (DHO), respectively $\overline{G}$ (APN), be transitive on $\mathcal{S}$. Then $N_G(N)$, respectively $N_{\overline{G}}(\overline{N})$, is transitive too.*

Proof. We only treat the DHO case; the APN case is completely similar. We have $|G : G_S| = 2^{n+1}$ for $S \in \mathcal{S}$. Let T be a Sylow 2-subgroup of G containing N. By Sylow's theorem we can also assume that $T \cap G_S = T_S \in \mathrm{Syl}_2(G_S)$. Then T is transitive: Otherwise $|T : T_S| = 2^n$, which implies

$$|T| = |G|_2 = |G : G_S|_2 \cdot |G_S|_2 = 2^{n+1} \cdot |T_S| = 2 \cdot |T|,$$

a contradiction (here k_2 denotes here the 2-part of the number k). Since $T \leq N_G(N)$ by Theorem 3.6, the proof is complete. □

We prove the theorem by a series of lemmas.

Lemma 3.8. *Let $\mathcal{S} \subseteq U$ be the extension of a DHO of rank n or the graph of the APN function F, which is the extension of APN functions of rank n. Assume in either case that the extension is ambient in its defining space. Let σ (DHO), respectively $\overline{\sigma}$ (APN), be an automorphism that fixes the set $\{\mathcal{S}_0, \mathcal{S}_1\}$. Then one of the following hold:*

(a) σ, respectively $\overline{\sigma}$, fixes $\mathcal{S}_0$ and $\mathcal{S}_1$ and

$$\sigma = \begin{pmatrix} 1 & \sigma_{12} & \sigma_{13} & \sigma_{14} \\ & \sigma_{22} & & \sigma_{24} \\ & & \sigma_{33} & \sigma_{34} \\ & & & \sigma_{44} \end{pmatrix}$$

with $\sigma_{22}, \sigma_{33} \in \mathrm{GL}(X)$, $\sigma_{44} \in \mathrm{GL}(Y)$, $\sigma_{12}, \sigma_{13} \in X$, $\sigma_{14} \in Y$, and $\sigma_{24}, \sigma_{34} \in \mathrm{Hom}(X, Y)$.

(b) σ, respectively $\overline{\sigma}$, interchanges $\mathcal{S}_0$ and $\mathcal{S}_1$ and

$$\sigma = \begin{pmatrix} 1 & \sigma_{12} & \sigma_{13} & \sigma_{14} \\ & & \sigma_{23} & \sigma_{24} \\ & \sigma_{32} & & \sigma_{34} \\ & & & \sigma_{44} \end{pmatrix}$$

with $\sigma_{23}, \sigma_{32} \in \mathrm{GL}(X)$, and all other σ_{ij} are as in (a).

Proof. The automorphism σ (DHO) or the linear part σ (APN) either fixes both W_0 and W_1 or interchanges them (according as to whether or not σ respectively $\overline{\sigma}$ fixes or interchanges $\mathcal{S}_0$ or $\mathcal{S}_1$). Therefore U_0 is σ-invariant. Decompose $U = \langle u_0 \rangle \oplus W'_0 \oplus W'_1 \oplus U_0$, where $W_a = W'_a \oplus U_0$, $(a = 0, 1)$, and $U = \langle u_0 \rangle \oplus (W_0 + W_1)$. If σ fixes W_0 and W_1 we get assertion (a) and the other case leads to assertion (b). □

Lemma 3.9. *The normalizer of N in G is*

$$N_G(N) = N \cdot L = H,$$

where H (DHO) respectively $\overline{H}$ (APN) is the stabilizer of the set $\{\mathcal{S}_0, \mathcal{S}_1\}$ in G respectively in $\overline{G}$.

Proof. We begin with the DHO case. As $N_G(N)$ permutes the N-orbits we have $N \cdot L \leq N_G(N) \leq H$.

Assume now that $\sigma \in H$. We want to show, that σ lies in $N \cdot L$. Using the action of N on $\mathcal{S}$ we can modify σ if necessary by some element in N, such that either σ fixes $S_{0,0} \in \mathcal{S}_0$ and $S_{1,0} \in \mathcal{S}_{1,0}$ or that σ interchanges these two spaces.

Consider the first case. By the assumption and Lemma 3.8 σ fixes the decomposition $U = (S_{0,0} \cap S_{1,0}) \oplus S'_0 \oplus S'_1 \oplus U_0$, where $S'_a = \langle S_{a,0} \cap S \mid S \in S_a \rangle$ $(a = 0, 1)$. So, with respect to this decomposition, we may write $\sigma = \mathrm{diag}(1, \mu, \lambda, \rho)$ with $\mu, \lambda \in \mathrm{GL}(X)$, $\rho \in \mathrm{GL}(Y)$ as $S'_0 = 0 \oplus X \oplus 0 \oplus 0$, $S'_1 = 0 \oplus 0 \oplus X \oplus 0$, and $U_0 = 0 \oplus 0 \oplus 0 \oplus Y$. The element $(b, x, be, (be + x)\beta(e)) \in \mathcal{S}_{0,e}$ is mapped by σ onto $(b, x\mu, be\lambda, (be + x)\beta(e)\rho)$, which must lie in $\mathcal{S}_{0,e\lambda}$. Hence $(be + x)\beta(e)\rho = (be\lambda + x\mu)\beta(e\lambda)$, which implies that (λ, μ, ρ) is an autotopism of β, i.e. $\sigma \in L$.

In the second case we see that σ is represented with respect to the decomposition $U = S_{0,0} \cap S_{1,0} \oplus S'_0 \oplus S'_1 \oplus U_0$ as

$$\sigma = \begin{pmatrix} 1 & & & \\ & & \lambda & \\ & \mu & & \\ & & & \rho \end{pmatrix}.$$

This time $S_{0,e}$ will be mapped onto some $S_{1,e'}$ and a similar computation as before shows that (λ, μ, ρ) is an isotopism of β onto β^0. Again we have $\sigma \in L$.

We turn to the APN case. As in the DHO case $\overline{N} \cdot \overline{L} \leq N_{\overline{G}}(\overline{N}) \leq \overline{H}$. Assume that $\overline{\sigma} \in \overline{H}$. We want to show that $\overline{\sigma}$ normalizes $\overline{N}$. Suppose first that this element fixes $\mathcal{S}_0$ and $\mathcal{S}_1$. We can adjust this element by some element from $\overline{N}$, so that $\overline{\sigma}$ fixes $(1,0,0,0)$ and $(0,0,0,0)$ too. Hence $\overline{\sigma} = \sigma \in \mathbf{A}(F)$ and this element has the shape of assertion (a) of Lemma 3.8. As σ fixes $(1,0,0,0)$ we also have $\sigma_{1i} = 0$ for $i = 2,3,4$. Apply σ to a typical element of $\mathcal{S}_0$ and we get

$$(0, x, 0, f_0(x))\sigma = (0, x\sigma_{22}, 0, f_0(x)\sigma_{44} + x\sigma_{24}),$$

which shows $f(x\sigma_{22}) = f_0(x)\sigma_{44} + x\sigma_{24}$ for all $x \in X$. Hence $\phi = \begin{pmatrix} \sigma_{22} & \sigma_{24} \\ & \sigma_{44} \end{pmatrix}$ is an autotopism of f_0. Considering the other orbit, we similarly obtain that $\phi' = \begin{pmatrix} \sigma_{33} & \sigma_{34} \\ & \sigma_{44} \end{pmatrix}$ is an autotopism of f_1. In particular ϕ and ϕ' are linked. Hence $\sigma = \Phi_{\phi,\phi'} \in L_0$.

Assume now that $\overline{\sigma}$ interchanges the two sets. Adjusting this element by some element in $\overline{N}$, we can also assume that $\overline{\sigma}$ interchanges $(1,0,0,0)$ and $(0,0,0,0)$. This implies that $c_\sigma = (1,0,0,0)$ and σ has the shape of assertion (b) of Lemma 3.8. Now

$$(0, x, 0, f_0(x))\overline{\sigma} = (1, 0, x\sigma_{23}, 0, f_0(x)\sigma_{44} + x\sigma_{24}),$$

which implies that $f_1(x\sigma_{23}) = f_0(x)\sigma_{44} + x\sigma_{24}$. Thus $\phi = \begin{pmatrix} \sigma_{23} & \sigma_{24} \\ & \sigma_{44} \end{pmatrix}$ is an isotopism from f_0 to f_1. Similarly, we obtain an isotopism $\phi' = \begin{pmatrix} \sigma_{32} & \sigma_{34} \\ & \sigma_{44} \end{pmatrix}$ from f_1 to f_0. This implies that $\overline{\sigma} = \overline{\Psi}_{\phi,\phi'} \in \overline{L}$. □

Lemma 3.10. *The following statements hold.*

(a) Let τ be a non-identity element in $N_0 \cup N_1$. Then $C_G(\tau) \leq NL_0$. In particular N is the only group conjugate to N that contains τ.

(b) $N_G(N_i) = NL_0$ for $i = 0, 1$.

(c) Let $E = E_0 \times E_1$ be a weak extension group and assume that $1 \neq \tau \in E_0 \cup E_1$ normalizes N. Then τ normalizes N_i and fixes $\mathcal{S}_i$, $i = 0, 1$.

(d) $C_G(N_i) = N$ for $i = 0, 1$.

Proof. We work mainly in the DHO case and comment only on the APN case when necessary.

(a) Let $1 \neq \tau \in N_0$ and $\sigma \in C_G(\tau)$. In this case σ fixes $\mathcal{S}_0 = \mathrm{Fix}_{\mathcal{S}}(\tau)$ and $\mathcal{S}_1 = \mathcal{S} - \mathcal{S}_0$. Hence $\sigma \in N_G(N) = NL$ by Lemma 3.9 and thus even $\sigma \in NL_0$. Assertion (a) follows by symmetry.

(b) Let $\sigma \in G$ normalize N_0. Then σ fixes $\mathcal{S}_0 = \mathrm{Fix}_{\mathcal{S}}(N_0)$ and $\mathcal{S}_1 = \mathcal{S} - \mathcal{S}_0$. Again the assertion follows by Lemma 3.9.

(c) As τ normalizes the group N, it either fixes $\mathcal{S}_0$ and $\mathcal{S}_1$ or it interchanges these sets. But τ has precisely 2^n fixed-points in $\mathcal{S}$, which rules out the second case. Thus τ must normalize N_0 and N_1.

(d) By (a) we have $N \leq C_G(\tau) \leq NL_0$. We first consider the DHO case. Assume that $u_\alpha = \mathrm{diag}(1, \mu, \lambda, \rho) \in C_{L_0}(N_0)$ and $e \in X$. A computation shows

$$\begin{pmatrix} 1 & & e & \\ & \mu & & \mu\beta^o(e) \\ & & \lambda & \\ & & & \rho \end{pmatrix} = u_\alpha n_{0,e} = n_{0,e} u_\alpha = \begin{pmatrix} 1 & & e\lambda & \\ & \mu & & \beta^o(e)\rho \\ & & \lambda & \\ & & & \rho \end{pmatrix}.$$

Thus $\lambda = 1$ and $\alpha = \mathrm{diag}(1, \mu, \rho)$ is an autotopism of β, such that $\beta(e\mu) = \beta(e)\rho$ for $e \in X$. Hence $\ker \beta(e\mu) = \ker \beta(e)\rho = \ker \beta(e)$ which implies $\mu = 1$ and then $\rho = 1$. Therefore $C_{L_0}(N_0) = 1$ and (b) follows by symmetry.

Assume now the APN case and let $\Phi_{\phi,\phi'} \in C_{L_0}(N_0)$, with $\Phi_{\phi,\phi'}$ as in subsection 2.6. The equation $\Phi_{\phi,\phi'} n_{0,e} = n_{0,e}\Phi_{\phi,\phi'}$ shows that $e = e\mu$, $f_1(e) = f_1(e)\rho + e\delta$, and $\mu\beta_1(e) = \beta_1(e)\rho$ for all $e \in X$. This shows that $\mu = 1$. We conclude from the equation $\beta_1(e) = \beta_1(e)\rho$, that $\rho|_{\mathrm{Im}\,\beta(e)} = 1_{\mathrm{Im}\,\beta(e)}$ for all $e \in X$. By Lemma 2.9 $Y = \langle \mathrm{Im}\,\beta_1(e) \mid e \in X\rangle$. This implies that $\rho = 1$. Therefore $\delta = 0$ must hold too, i.e. $\Phi_{\phi,\phi'} = 1$. The assertion follows by symmetry. □

Lemma 3.11. *Let $E = E_0 \times E_1$ be a weak extension group that normalizes N. Then $E = N$.*

Proof. We treat only the DHO case, the APN case is completely similar. By (c) of Lemma 3.10 E_i fixes the orbits of N. This shows that E and N have the same orbits. Assume that $\mathrm{Fix}_{\mathcal{S}}(E_0) = \mathcal{S}_0$. Then $E_0 \leq C_G(N_1) = N$ and therefore $E_0 = N_0$. The assertion follows by symmetry. □

Proof. (Theorem 3.6) Let S a Sylow 2-subgroup, which contains the extension group N and the weak extension group E.

Claim. The extension group N is normal in S.

Assume that N is not normal, i.e. $N_S(N) < S$. Then $N_S(N) < N_S(N_S(N))$ by a basic result on p-groups. Pick $\gamma \in N_S(N_S(N)) - N_S(N)$. Then $N^\gamma \neq N$, and N^γ is normal in $N_S(N)^\gamma = N_S(N)$. So N and N^γ normalize each other. By Lemma 3.11 $N = N^\gamma$, a contradiction. The claim follows.

By Lemma 3.11 we also obtain $E = N$. The proof is complete. □

4 Isomorphisms

In this section we solve the isomorphism problem for extensions of bilinear DHOs and extensions of quadratic APN functions. We also characterize those extensions of DHOs and APN functions that have a translation group. Finally, we will show that the number of inequivalent extensions obtained form the isotopes of *one* quadratic (Gold) APN function grows exponentially with the dimension.

We will assume in this section that extensions are ambient in their defining spaces.

4.1 DHO case

Theorem 4.1. *Let X and Y be finite dimensional $\mathbb{F}_2$-spaces, with $\dim X \geq 4$, and let $\beta, \beta' : X \to \mathrm{Hom}(X, Y)$ define bilinear DHOs ambient in $X \oplus Y$. The following are equivalent:*

- *(a) β' is isotopic to β or β^o.*
- *(b) $\mathcal{S}_{\beta'}$ is isomorphic to $\mathcal{S}_\beta$ or $\mathcal{S}_{\beta^o}$.*
- *(c) $\overline{\mathcal{S}}_{\beta'}$ and $\overline{\mathcal{S}}_\beta$ are isomorphic.*

Proof. The implication (a)⇒(b) is trivial, whereas (b)⇒(a) is [5, Theorem 3.12]. The implication (a)⇒(c) follows from Proposition 2.3. We have to show the implication (c)⇒(b).

We index objects associated with β by a subscript β and objects associated with β' by an index β'. Set $G_\beta = \mathrm{Aut}(\mathcal{S})$ and $G_{\beta'} = \mathrm{Aut}(\mathcal{S}')$. Let $\phi \in \mathrm{GL}(\overline{U})$, where $U = X \oplus Y$, be an isomorphism from $\overline{\mathcal{S}}$ onto $\overline{\mathcal{S}}'$. Then $G_{\beta'} = \phi^{-1} G_\beta \phi$. Using Theorem 3.6 ϕ can be chosen in such a way that $N_{\beta'} = \phi^{-1} N_\beta \phi$.

So ϕ fixes or interchanges the two subspaces W_0 and W_1 from Lemma 3.8. Thus ϕ has a shape as described in that lemma. In fact, as $\overline{\mathcal{S}}_\beta$ and $\overline{\mathcal{S}}_{\beta^o}$ are isomorphic, we may assume that ϕ fixes the two spaces and we can represent ϕ in form (a) of that lemma (replace a symbol σ_{ij} by ϕ_{ij}). We can now argue exactly as in the proof of Lemma 3.9 and obtain the equation

$$\phi_{33}^{-1} \beta(e) \phi_{44} = \beta'(e\phi_{22})$$

for all $e \in X$. Hence β and β' are isotopic and therefore the implication (c)⇒(b) follows. □

Theorem 4.2. *Let X and Y be finite dimensional $\mathbb{F}_2$-spaces, with $\dim X \geq 4$, and let $\beta : X \to \mathrm{Hom}(X, Y)$ define a bilinear DHO ambient in $X \oplus Y$. The following are equivalent:*

- *(a) There exists some $\gamma \in \mathrm{GL}(X)$, such that $\widetilde{\beta} : X \to \mathrm{Hom}(X, Y)$ defined by $x\widetilde{\beta}(e) = x\gamma\beta(e)$ defines a symmetric DHO.*
- *(b) There exists some $\gamma \in \mathrm{GL}(X)$ such that $(\gamma^{-1}, \gamma, \mathbf{1})$ is an isotopism from β to β^o.*
- *(c) $\overline{\mathcal{S}}_\beta$ is isomorphic to a bilinear DHO.*

Proof. (a) ⇔ (b) Assume (b), i.e. that $(\gamma^{-1}, \gamma, \mathbf{1})$ is an isotopism from β to β^o, i.e. $x\beta(e) = x\gamma^{-1}\beta^o(e\gamma)$ for all $x, e \in X$. Hence

$$x\gamma\beta(e) = e\beta^o(x\gamma) = e\gamma\gamma^{-1}\beta^o(x\gamma) = e\gamma\beta(x),$$

i.e. $\widetilde{\beta}$ is symmetric and assertion (a) holds. Clearly, the argument can be reversed.

(a)⇒(c) By assumption $\phi = (\gamma, \mathbf{1}, \mathbf{1})$ is an isotopism which maps β onto $\widetilde{\beta}$ and $\overline{\mathcal{S}}_{\widetilde{\beta}}$ is bilinear by [5]. The assertion follows from Proposition 2.3.

(c)⇒(b) By assumption $\mathrm{Aut}(\mathcal{S})$, where $\mathcal{S} = \overline{\mathcal{S}}_\beta$, contains a translation group T and since all translation groups are conjugate (use [5, Thm. 3.11]), we may assume that N and T lie in a common Sylow 2-subgroup of the automorphism group. Again by [5, Thm. 3.11] T is normalized by N and as both groups are self-centralizing (Lemma 3.4), we have

$$[N, T] = N \cap T = C_N(T) = C_T(N).$$

Since T acts regularly on $\mathcal{S}$, we have $|T| = 2^{n+1}$ and $T \cap N_a = 1$, $a = 0, 1$. Thus $|N \cap T| \leq 2^n$. Hence N is a proper subgroup of NT. By a basic result on p-groups there exists $\tau \in N_{NT}(N) - T$. We may adjust τ by an element in N, i.e. we may assume $\tau \in T - (N \cap T)$. Clearly, τ leaves the set $\{\mathcal{S}_0, \mathcal{S}_1\}$ of N-orbits invariant.

Assume that τ fixes the sets $\mathcal{S}_0$ and $\mathcal{S}_1$ and therefore normalizes N_a, $a = 0, 1$. This implies that $[\tau, N_a] \leq N_a \cap T = 1$ and thus $\tau \in C_G(N) = N$, a contradiction. Therefore τ interchanges both orbits, i.e. $S_{0,0}\tau = S_{1,e}$. Now $n_{0,e}$ moves $S_{1,0}$ onto $S_{1,e}$. So, replacing τ by $n_{0,e}\tau n_{0,e}$ if necessary, we may even assume $S_{0,0}\tau = S_{1,0}$. Use Lemma 3.8 to see that τ has, with respect to the decomposition $(S_{0,0} \cap S_{1,0}) \oplus S_0' \oplus S_1' \oplus U_0$ (here $S_{a,0} = (S_{0,0} \cap S_{1,0}) \oplus S_a'$), the shape

$$\tau = \begin{pmatrix} 1 & & & \\ & & \gamma & \\ & \gamma^{-1} & & \\ & & & \rho \end{pmatrix}$$

and, as rk $(1 + \tau) = n$ (see [5, Thm. 3.2]), we also see that $\rho = 1$. The the typical element $(b, be, be + x, (be + x)\beta(e))$ of $S_{0,e}$ is mapped under τ onto $(b, (be + x)\gamma^{-1}, be\gamma, (be + x)\beta(e))$, which must lie in $S_{1,e\gamma}$. So there exists $y \in X$ with $(be + x)\gamma^{-1} = be\gamma + y$. Hence $(be + x)\beta(e) = (be + x)\gamma^{-1}\beta^o(e\gamma)$ and assertion (b) follows. □

4.2 APN case

Theorem 4.3. *Let $f_i : X \to Y$ be quadratic APN functions for $i = 0, \ldots, 3$ with $\dim X \geq 4$. Set $F = F_{f_0,f_1}$ and $F' = F_{f_2,f_3}$. Assume moreover that F and F' are fully ambient. The following are equivalent:*

(a) F and F' are equivalent.

(b) (f_0, f_1) is isotopically linked to (f_2, f_3) or (f_3, f_2).

Proof. (a)⇒(b) We index objects associated with F by a subscript F and objects associated with F' by an index F'. Let $\Phi \in \mathrm{AGL}(\overline{U})$, where $U = X \oplus Y$, map $\mathcal{S}_F$ onto $\mathcal{S}_{F'}$. Then $\overline{G}_{F'} = \mathrm{Aut}(F') = \Phi^{-1}\mathrm{Aut}(F)\Phi = \Phi^{-1}\overline{G}_F\Phi$. According to

Theorem 3.6 we can adjust Φ by some element in $\overline{G}_F$ such that $N_{F'} = \Phi^{-1}N_F\Phi$. Considering the orbits, we see that

$$\{\mathcal{S}_{0,F}, \mathcal{S}_{1,F}\}\Phi = \{\mathcal{S}_{0,F'}, \mathcal{S}_{1,F'}\}.$$

Assume first that $\mathcal{S}_{0,F}\Phi = \mathcal{S}_{0,F'}$ and $\mathcal{S}_{1,F}\Phi = \mathcal{S}_{1,F'}$. We can further adjust Φ with some element from $\overline{N}_{F'}$, such that Φ fixes $(0,0,0,0)$ and $(1,0,0,0)$. Then $\Phi \in \mathrm{GL}(U)$ and we can argue as in the proof of Lemma 3.8 to see that this operator has the shape

$$\Phi = \begin{pmatrix} 1 & \Phi_{12} & \Phi_{13} & \Phi_{14} \\ & \Phi_{22} & & \Phi_{24} \\ & & \Phi_{33} & \Phi_{34} \\ & & & \Phi_{44} \end{pmatrix}.$$

The same computation as in the proof of Lemma 3.9 shows, that $\phi = \begin{pmatrix} \Phi_{22} & \Phi_{24} \\ & \Phi_{44} \end{pmatrix}$ is an isotopism from f_0 to f_2 and $\phi' = \begin{pmatrix} \Phi_{33} & \Phi_{34} \\ & \Phi_{44} \end{pmatrix}$ is an isotopism from f_1 to f_3.

The case where $\mathcal{S}_{0,F}\Phi = \mathcal{S}_{1,F'}$ and $\mathcal{S}_{1,F}\Phi = \mathcal{S}_{0,F'}$ leads similarly to linked iosotopisms $\phi : f_0 \mapsto f_3$ and $\phi' : f_1 \mapsto f_2$.

The implication (b)⇒(a) follows by the obvious construction of an equivalence operator Φ with the help of linked isotopisms ϕ and ϕ'. □

Assertion (c) of Proposition 2.6 can be generalized to:

Theorem 4.4. *Let X and Y be finite dimensional $\mathbb{F}_2$-spaces and let $f_0, f_1 : X \to Y$ be quadratic APN functions, with $\dim X \geq 4$. Set $F = F_{f_0,f_1}$ and assume that F is ambient in its defining space. The following are equivalent:*

(a) f_0 and f_1 are ambient in $X \oplus Y$ (i.e. F is fully ambient) and there exist $\gamma \in \mathrm{GL}(X)$ and $\varepsilon \in \mathrm{Hom}(X,Y)$ such that $f_1(x) = f_0(x\gamma) + x\varepsilon$ for $x \in X$.

(b) f_0 and f_1 are isotopic and every isotopism from f_0 to f_1 is linked to an an autotopism of f_0.

(c) F_{f_0,f_1} is equivalent to the quadratic APN function F_{f_0,f_0}.

(d) F_{f_0,f_1} is equivalent to a quadratic APN function.

Proof. The implication (c)⇒(d) is trivial.

(a)⇒(b) By assumption $\psi = \begin{pmatrix} \gamma & \varepsilon \\ & \mathbf{1} \end{pmatrix}$ is an isotopism from f_0 to f_1. Let $\phi = \begin{pmatrix} \mu & \delta \\ & \rho \end{pmatrix}$ be an arbitrary isotopism from f_0 to f_1. Then the autotopism $\phi \circ \psi^{-1}$ of f_0 is linked to ϕ.

(b)⇒(c) Suppose $\phi = \begin{pmatrix} \mu & \delta \\ & \rho \end{pmatrix} : f_0 \mapsto f_1$ is an isotopism. Then ϕ is linked with an autotopism of f_0 of the form $\begin{pmatrix} \tau & \alpha \\ & \rho \end{pmatrix}$. Define

$$\sigma = \begin{pmatrix} 1 & & & \\ & \tau & & \alpha \\ & & \mu & \delta \\ & & & \rho \end{pmatrix}.$$

A computation shows that $\mathcal{S}_0\sigma = \mathcal{S}_0$ and

$$\mathcal{S}_1\sigma = \{(1, 0, x\mu, f_0(x\mu)) \mid x \in X\}.$$

Hence σ is an equivalence map from F_{f_0,f_1} onto F_{f_0,f_0}.

(d)⇒(a) Suppose now that F is quadratic and ambient. By Lemma 2.9 there exist subspaces Y_0, Y_1 of Y, such that $Y = Y_0 + Y_1$ and $\langle \mathcal{S}_{f_i} \rangle = X \oplus Y_i$, $i = 0, 1$. By [5] $\mathrm{Aut}(F)$ possesses a translation group T and by [5, Thm. 3.11] all translation groups are conjugate, self-centralizing, and normal in any Sylow 2-subgroup that contains the translation group. We may therefore choose T, such that T and N lie in a common Sylow 2-subgroup of the automorphism group. In particular N normalizes T, NT is a 2-group, and $C_T(N) = T \cap N$ (as T is self-centralizing). As $\overline{T}$ has a regular action on $\mathcal{S}$, we have $T \cap N_i = 1$, $i = 0, 1$. Thus $|T \cap N| \leq 2^n$, i.e. $T \cap N$ is a proper subgroup of T and $N < NT$. By a basic result on p-groups there exists $\tau \in N_{NT}(N) - N$. We may adjust τ with an element in N, i.e. we may assume $\tau \in T - (N \cap T)$. Then $\mathcal{S}_i\overline{\tau} \in \{\mathcal{S}_0, \mathcal{S}_1\}$, $i = 0, 1$.

Assume, $\mathcal{S}_i\overline{\tau} = \mathcal{S}_i$, $i = 0, 1$. Then τ normalizes N_i and hence $[N_i, \tau] \leq N_i \cap T = 1$, i.e, $\tau \in C_{\mathbf{A}(F)}(N) = N$ or $\tau \in T \cap N$, a contradiction.

Hence $\mathcal{S}_0\overline{\tau} = \mathcal{S}_1$, i.e.

$$(0, 0, 0, 0)\overline{\tau} = (1, 0, e, f_1(e)), \quad e \in X.$$

As $(1, 0, 0, 0)n_{0,e} = (1, 0, e, f_1(e))$, we see $(0, 0, 0, 0)n_{0,e}\overline{\tau}n_{0,e} = (1, 0, 0, 0)$, or if we replace τ by $n_{0,e}\tau n_{0,e}$, we may assume that $(0, 0, 0, 0)\overline{\tau} = (1, 0, 0, 0)$, i.e. $c_\tau = (1, 0, 0, 0)$. With respect to the decomposition $U = \langle (1, 0, 0, 0) \rangle \oplus W_0' \oplus W_1' \oplus U_0$ (with W_0', W_1' as in the proof of Lemma 3.8) τ has the shape

$$\tau = \begin{pmatrix} 1 & & & \\ & & \gamma & \varepsilon \\ & \gamma^{-1} & & \delta \\ & & & \rho \end{pmatrix}.$$

But, arguing as in the proof of Theorem 4.2, we see that $\rho = 1$. Thus $\mathcal{S}_0\overline{\tau} = \{(1, 0, x\gamma, f_0(x) + x\varepsilon) \mid x \in X\}$ and $\mathcal{S}_1\overline{\tau} = \{(0, x\gamma^{-1}, 0, f_1(x) + x\delta) \mid x \in X\}$. Therefore for all $x \in X$

$$f_1(x\gamma) = f_0(x) + x\varepsilon, \quad f_0(x\gamma^{-1}) = f_1(x) + x\delta.$$

This implies $x\beta_1(e\gamma) = x\beta_0(e)$ with $\beta_i = \beta_{f_i}$. By Lemma 2.9 $Y_0 = \sum_{e \in X} \mathrm{Im}\,\beta_0(e) = \sum_{e \in X} \mathrm{Im}\,\beta_1(e) = Y_1$. We conclude that $Y = Y_0 = Y_1$. Assertion (a) follows. □

4.3 Counting APN functions

Definition. (a) Let G be a finite group with subgroups H, K. Define $[H : G : K]$ to be the number of double cosets of the form HxK, $x \in G$. Furthermore, we write $[H : G : K]_0$ for the number of sets of the form $HxK \cup Hx^{-1}K$ (so that, in the case $H = K$, these are the equivalence classes of the relation that is obtained by the natural action of the inversion map on the set of double cosets).

(b) Let $f : X \to Y$ be a quadratic APN function. We denote by A_f the restriction of $\mathrm{Autop}(f)$ to Y. So if $\begin{pmatrix} \lambda & \gamma \\ & \rho \end{pmatrix} \in \mathrm{Autop}(f)$, then $\rho \in \mathrm{A}_f$.

Remark 4.5. A lower bound for $[H : G : K]$ is $\lfloor \frac{|G|}{|H||K|} \rfloor$ and $\lfloor \frac{|G|}{2|H||K|} \rfloor$ is a lower bound of $[H : G : K]_0$.

Theorem 4.6. *Let $f, g : X \to Y$ be quadratic APN functions, $f \not\sim g$.*

(a) There exist precisely $[A_g : \mathrm{GL}(Y) : \mathrm{A}_f]$ pairwise inequivalent APN functions of the form $F_{f,g\alpha}$, $\alpha \in \mathrm{GL}(Y)$.

(b) There exist precisely $[A_f : \mathrm{GL}(Y) : \mathrm{A}_f]_0$ pairwise inequivalent APN functions of the form $F_{f,f\alpha}$, $\alpha \in \mathrm{GL}(Y)$.

Proof. (a) Suppose $F_{f,g\alpha} \sim F_{f,g\beta}$, where $\alpha, \beta \in \mathrm{GL}(Y)$. By Theorem 4.3 there exist $\rho \in \mathrm{GL}(Y)$, $\lambda, \mu \in \mathrm{GL}(X)$, and $\gamma, \delta \in \mathrm{Hom}(X, Y)$ with

$$f(x\lambda) = f(x)\rho + x\gamma, \quad g(x\mu)\alpha = g(x)\beta\rho + x\delta,$$

for $x \in X$. This implies

$$\begin{pmatrix} \lambda & \gamma \\ & \rho \end{pmatrix} \in \mathrm{Autop}(f), \quad \begin{pmatrix} \mu & \delta\alpha^{-1} \\ & \beta\rho\alpha^{-1} \end{pmatrix} \in \mathrm{Autop}(g).$$

Thus $\rho \in \mathrm{A}_f \cap \beta^{-1}\mathrm{A}_g\alpha$ or equivalently $\mathrm{A}_g\alpha\mathrm{A}_f = \mathrm{A}_g\beta\mathrm{A}_f$. So $F_{f,g\alpha} \sim F_{f,g\beta}$ implies that $\mathrm{A}_g\alpha\mathrm{A}_f = \mathrm{A}_g\beta\mathrm{A}_f$. Since the arguments can be read backwards we get assertion (a).

(b) Suppose $F_{f,f\alpha} \sim F_{f,f\beta}$, where $\alpha, \beta \in \mathrm{GL}(Y)$. By Theorem 4.3 there exist $\rho \in \mathrm{GL}(Y)$, $\lambda, \mu \in \mathrm{GL}(X)$, and $\gamma, \delta \in \mathrm{Hom}(X, Y)$ with

$$(1) \quad f(x\lambda) = f(x)\rho + x\gamma, \quad f(x\mu)\alpha = f(x)\beta\rho + x\delta,$$

or

$$(2) \quad f(x\lambda) = f(x)\beta\rho + x\gamma, \quad f(x\mu)\alpha = f(x)\rho + x\delta.$$

Case (1) leads as in (a) to $\mathrm{A}_f\alpha\mathrm{A}_f = \mathrm{A}_f\beta\mathrm{A}_f$. In case (2) we see that

$$\begin{pmatrix} \lambda & \gamma \\ & \beta\rho \end{pmatrix}, \begin{pmatrix} \mu & \delta\alpha^{-1} \\ & \rho\alpha^{-1} \end{pmatrix} \in \mathrm{Autop}(f),$$

which implies that $\mathrm{A}_f\alpha\mathrm{A}_f = \mathrm{A}_f\beta^{-1}\mathrm{A}_f$. Again all arguments can be reversed. □

Remark 4.7. For $\alpha, \beta \in \mathrm{GL}(Y)$ one observes that $F_{f\alpha, g\beta} \sim F_{f, g\beta\alpha^{-1}}$. Hence Theorem 4.6 counts all APN functions of type $F_{f\alpha, g\beta}$ and $F_{f\alpha, f\beta}$.

Proposition 4.8. *Let* $\dim X = n \geq 7$ *and let* $f : X \to Y = X$ *be a Gold APN function (i.e.* $f(x) = x^{2^k+1}$, $(n, k) = 1$*). Then there exist at least*

$$2^{3+\binom{n-5}{2}} \prod_{i=2}^{n-2} (2^i - 1)$$

inequivalent APN functions of the form $F_{f, f\alpha}$, $\alpha \in \mathrm{GL}(X)$*.*

Proof. From [2] we deduce that A_f is a subgroup of $\mathrm{C}_{2^n-1} \cdot \mathrm{C}_n$. So

$$[A_f : \mathrm{GL}(Y) : \mathrm{A}_f]_0 \geq 2^{\binom{n}{2}} \prod_{i=2}^{n} (2^i - 1)/(2^n - 1)^2 \cdot n^2 \cdot 2,$$

which leads, together with Theorem 4.6, to the assertion. □

Example 4.9. A recent study [11] shows that there are more than 470 quadratic APN functions $f : \mathbb{F}_2^7 \to \mathbb{F}_2^7$ such that $|A_f| = 1$. Hence there are more than

$$\left(\frac{471}{2} + \binom{471}{2}\right) |\mathrm{GL}(7, 2)| = 18,097,231,719,038,976,000$$

inequivalent APN functions $f : \mathbb{F}_2^8 \to \mathbb{F}_2^{14}$, one of degree 2 and the others of degree 3.

5 Groups generated by extension groups

In this section the symbol $\mathcal{S}$ denotes the extension of a bilinear DHO $\mathcal{S}_\beta$ in the DHO case, while in the APN case this symbol denotes the graph of the extension $F = F_{f_0, f_1}$ of quadratic APN functions f_0 and f_1. We shall assume in both cases that $\mathcal{S}$ is ambient in the defining space, and in the APN case we also assume that F is fully ambient. In particular, by Theorem 3.6, weak extension groups are actually extension groups. Also set $G = \mathrm{Aut}(\mathcal{S})$ in the DHO case, while in the APN case we have $\overline{G} = \mathrm{Aut}(F)$ and $G = \mathbf{A}(F)$ is the linear part of $\overline{G}$. Denote by $\mathcal{C}$ the conjugacy class of extension groups in G (see Theorem 3.6, i.e.

$$\mathcal{C} = \{N^\gamma \mid \gamma \in G\}.$$

We assume that $\mathcal{S}$ admits more than one extension group and collect results about groups that are generated by more than one extension group. Our main purpose is to show:

Theorem 5.1. *Let* $\mathcal{S}$ *be an* $(n+1)$*-dimensional DHO or the graph of an APN function of rank* $n+1$, $n \geq 4$*. Then any two extension groups* M, N *are conjugate in* $\langle M, N \rangle$ *and their intersection has size* $|M \cap N| = 2^{n-1}$*. In particular* $\mathcal{C}$ *is a conjugacy class in* $\langle \mathcal{C} \rangle$*.*

For our proofs Timmesfeld's result on weakly closed TI subgroups [8] will be instrumental. A first application of this theorem leads to the structure of $\langle N, N^\gamma\rangle$, $N^\gamma \in \mathcal{C} - \{N\}$, if $|N \cap N^\gamma|$ is maximal (Lemma 5.4). In a second application we determine the the structure of the group generated by the conjugates of N_0 in the stabilizer of a point of $\mathcal{S}$ (Lemma 5.9). As a consequence we will see that $|N \cap N^\gamma|$ has the same size for all $N^\gamma \in \mathcal{C} - \{N\}$ (Lemma 5.10). Then, by a somewhat tedious induction, we will obtain in Section 7 the structure of $\langle \mathcal{C} \rangle$ (Theorem 7.11).

Lemma 5.2. *Let $Q \leq N$ be a subgroup with $Q \cap N_0 = Q \cap N_1 = 1$ and $|Q| < 2^n$. Then $C_{M/Q}(N/Q) = N/Q$, where M is the common normalizer of Q and N in G.*

Proof. Let γQ lie in $C_{G/Q}(N/Q)$. Hence $[N, \gamma] \leq Q$, in particular $\gamma \in N_G(N)$. We can adjust γ by some element in N, such that $\gamma \in L$.

DHO case. We first consider the DHO case.

Case 1. $\gamma \in L_0$. Hence

$$\gamma = \begin{pmatrix} 1 & & & \\ & \mu & & \\ & & \lambda & \\ & & & \rho \end{pmatrix}.$$

Pick $\nu \in N$, i.e.

$$\nu = \begin{pmatrix} 1 & e & e_1 & * \\ & \mathbf{1} & & \beta^o(e_1) \\ & & \mathbf{1} & \beta(e) \\ & & & \mathbf{1} \end{pmatrix}.$$

Then

$$\gamma^{-1}\nu\gamma = \begin{pmatrix} 1 & e\mu & e_1\lambda & * \\ & \mathbf{1} & & \mu^{-1}\beta^o(e_1)\rho \\ & & \mathbf{1} & \lambda^{-1}\beta(e)\rho \\ & & & \mathbf{1} \end{pmatrix},$$

so that

$$[\gamma, \nu] = \begin{pmatrix} 1 & e(\mu + \mathbf{1}) & e_1(\lambda + \mathbf{1}) & * \\ & \mathbf{1} & & * \\ & & \mathbf{1} & * \\ & & & \mathbf{1} \end{pmatrix}.$$

Choose ν with $e_1 = 0$. Then $[\gamma, \nu] \in N_0 \cap Q = 1$. As we can choose e arbitrarily we get $\mu = \mathbf{1}$. Similarly $\lambda = \mathbf{1}$. But then we also have $\rho = \mathbf{1}$ and $\gamma = \mathbf{1}$.

Case 2. $\gamma \in L - L_0$. Hence

$$\gamma = \begin{pmatrix} 1 & & & \\ & & \mu & \\ & \lambda & & \\ & & & \rho \end{pmatrix}.$$

Now we have

$$\gamma^{-1}\nu\gamma = \begin{pmatrix} 1 & e_1\lambda & e\mu & * \\ & \mathbf{1} & & \lambda^{-1}\beta(e)\rho \\ & & \mathbf{1} & \mu^{-1}\beta^o(e_1)\rho \\ & & & \mathbf{1} \end{pmatrix},$$

so that

$$[\gamma, \nu] = \begin{pmatrix} 1 & e + e_1\lambda & e_1 + e\mu & * \\ & \mathbf{1} & & \beta^o(e_1) + \lambda^{-1}\beta(e)\rho \\ & & \mathbf{1} & \beta(e) + \mu^{-1}\beta^o(e_1)\rho \\ & & & \mathbf{1} \end{pmatrix}.$$

Choose, for an arbitrary $e \in X$, the element $e_1 = e\mu$. Then

$$[\gamma, \nu] \in N_0 \cap Q = 1.$$

This implies that $e + e_1\lambda = 0$ or $\lambda = \mu^{-1}$.

Next take arbitrary e and $e_1 = 0$. Then

$$[\gamma, \nu] = \begin{pmatrix} 1 & e & e\mu & * \\ & \mathbf{1} & & \lambda^{-1}\beta(e)\rho \\ & & \mathbf{1} & \beta(e) \\ & & & \mathbf{1} \end{pmatrix} \in Q$$

and $|Q| \geq 2^n$, which is excluded.

APN CASE. We now assume the APN case and distinguish again the cases $\gamma \in L_0$ and $\gamma \in L - L_0$.

In the first case we have (for the linear part)

$$\gamma = \begin{pmatrix} 1 & & & \\ & \mu & & \delta \\ & & \lambda & \omega \\ & & & \rho \end{pmatrix}$$

and the linear part ν of a typical element $\overline{\nu} \in \overline{N}$ is represented as

$$\nu = \begin{pmatrix} 1 & e & e_1 & * \\ & \mathbf{1} & & \beta_0(e_1) \\ & & \mathbf{1} & \beta_1(e) \\ & & & \mathbf{1} \end{pmatrix}.$$

A quick computation shows that

$$[\gamma, \nu] = \begin{pmatrix} 1 & e(\mu + \mathbf{1}) & e_1(\lambda + \mathbf{1}) & * \\ & \mathbf{1} & & * \\ & & \mathbf{1} & * \\ & & & \mathbf{1} \end{pmatrix}$$

(as in the DHO case). The same argument as in the DHO case leads to $\gamma = \mathbf{1}$. In a similar way CASE 2 can be adapted to the APN situation, leading to the contradiction $|Q| \geq 2^n$.

□

5.1 Groups generated by two extension groups

Lemma 5.3. *Let N^γ be in $\mathcal{C} - \{\ N\}$. Set $Q = N \cap N^\gamma$.*

(a) $Q \cap N_i = 1$ *for* $i = 0, 1$.

(b) Assume that Q *has maximal order. Then* $|Q| < 2^n$ *and* N/Q *is a self-centralizing TI subgroup in* H/Q, $H = \langle N, N^\gamma \rangle$.

Proof. We start with the DHO case.

(a) As $N^\gamma \not\leq N_G(N)$ (see Theorem 3.6) we have by Lemma 3.9, that the N-orbits $\{\mathcal{S}_0, \mathcal{S}_1\}$ are different from the N^γ-orbits $\{\mathcal{S}_0\gamma, \mathcal{S}_1\gamma\}$. Assume that σ, with $1 \neq \sigma$, is in $(N_0 \cup N_1) \cap Q$. Then N^γ leaves invariant the set of fixed points of σ that are $\mathcal{S}_0$ or $\mathcal{S}_1$. But then N and N^γ would have the same orbits, a contradiction. Thus $Q \cap N_i = 1$ for $i = 0, 1$ and $|Q| \leq 2^n$.

(b) By (a) Q acts fixed point freely on $\mathcal{S}$ and $|Q| \leq 2^n$. Assume $|Q| = 2^n$. Then Q would have the orbits $\{\mathcal{S}_0, \mathcal{S}_1\}$. But as $Q \leq N^\gamma$ we conclude by symmetry that $\{\mathcal{S}_0\gamma, \mathcal{S}_1\gamma\} = \{\mathcal{S}_0, \mathcal{S}_1\}$, a contradiction. This implies that $|Q| < 2^n$. By Lemma 5.2 N/Q is self-centralizing in H/Q.

Finally, $Q \leq Z(H)$, i.e. $H \leq N_G(Q)$. By the choice of N^γ, the group N/Q has the TI property in H/Q.

In the APN case we argue with $\overline{N}$ and $\overline{N}^{\overline{\gamma}}$ instead of N and N^γ. Then all the arguments from the DHO case can be repeated. □

Lemma 5.4. *Assume* $N^\gamma \in \mathcal{C} - \{N\}$, *such that* $|N \cap N^\gamma|$ *is maximal, and set* $H = \langle N, N^\gamma \rangle$, $Q = N \cap N^\gamma$, $R = N_N(N^\gamma)$, $R_1 = N_{N^\gamma}(N)$, *and* $P = O_2(H)$. *The following hold:*

(a) $P = RR_1$, $Q = R \cap R_1$ *has order* 2^{n-1} *and* $|P| = 2^{3n-1}$. *The group* P *is transitive on* $\mathcal{S}$.

(b) $H/P \simeq \mathrm{SL}(2, 2)) \simeq \mathrm{Sym}(3)$.

(c) $|N_i \cap P| = |N_i^\gamma \cap P| = 2^{n-1}$, $i = 0, 1$. *The group* $P_0 = (N_0 \cap P)(N_0^\gamma \cap P)Q$ *is elementary abelian of order* 2^{3n-3}. *This group is characteristic in* P.

(d) The set of orbits of the group P_0 *is* $\{\mathcal{S}_i \cap \mathcal{S}_j\gamma \mid i, j = 0, 1\}$ *and each orbit has length* 2^{n-1}.

(e) The group H/P *acts faithfully on* P/P_0.

Proof. By Lemmas 5.2 and 5.3 N/Q is a self-centralizing TI subgroup in H/Q. By [8, p. 243], we have that N/Q is weakly closed in $C_{H/Q}(\tau Q)$ for $\tau \in N - Q$ (i.e. $N^\sigma/Q \leq C_{H/Q}(\tau Q)$, $\sigma \in H$ implies $N = N^\sigma$). Clearly, as $Q \leq R \cap R_1$ we have $Q = R \cap R_1$. Also $H = \langle N^\sigma \mid \sigma \in H \rangle$ (see [8, (2.5), (2.14)] and [5, Lemma 4.3]).

DHO case. Since $\{\mathcal{S}_0\sigma, \mathcal{S}_1\sigma\} \neq \{\mathcal{S}_0, \mathcal{S}_1\}$ for $\sigma \in H$ with $N \neq N^\sigma$, the group H is transitive on $\mathcal{S}$.

Assume first that $N_N(N^\sigma) = Q$ for all elements $\sigma \in H$ with $N^\sigma \neq N$. Then N/Q is strongly closed in $C_{H/Q}(\tau Q)$ for every element $\tau \in N - Q$ (see [8, Proof of (2.14)] or [5, Lemma 4.3]). By [8, (2.5)] we get that $H/Q \simeq \mathrm{L}_2(q)$, $\mathrm{Sz}(q)$ or $(H/Q)/Z(H/Q) \simeq \mathrm{U}_3(q)$, $q \geq 2^{n+1}$. But as Q acts fixed point freely and since $|H : H_S| = 2^{n+1}$, we see that H/Q has a proper subgroup of 2-power index, which is impossible (see the proof of [5, Lemma 4.4]). In particular $Q > 1$ holds.

So we may assume that $R > Q$. We apply [8, (2.14)] to H/Q and obtain that $H/O_2(H) \simeq \mathrm{D}_{2k}$, k odd, $\mathrm{L}_2(q)$, or $\mathrm{Sz}(q)$, q a 2-power. Moreover, we have $O_2(H) = P = RR^\gamma$. As we have seen, H is transitive on $\mathcal{S}$. We distinguish the cases $H_SP < H$ and $H = H_SP$, $S \in \mathcal{S}$.

Case $H_SP < H$. As we have noticed, $\mathrm{L}_2(q)$ and $\mathrm{Sz}(q)$ do not have proper subgroups of 2-power index, i.e. $H/O_2(H) \simeq \mathrm{D}_{2k}$, k odd. Since the dihedral group D_k contains for every divisor k_0 of k a subgroup D_{k_0}, we may assume that we have chosen γ in such a way that k is a nontrivial prime. Then a cyclic subgroup of H of order k has a fixed point on $\mathcal{S}$, i.e. k divides the order of H_SP. Hence $|H : H_SP| = 2$. Then P is not transitive: Otherwise $2^{n+1} = |H_SP : (H_SP)_S| = |H_SP : H_S|$ and $2^{n+1} = |H : H_S| = |H : H_SP| \cdot |H_SP : H_S| = 2^{n+2}$, a contradiction.

As $|P \cap N| = 2^{2n-1}$, N_0 and N_1 cannot not both be contained in $P \cap N$. Assume $N_0 \not\subseteq P \cap N$ and pick $S \in \mathcal{S}_0$. Then $|N \cap P : (N \cap P)_S| = |N \cap P : N_0 \cap P| \geq 2^{2n-1}/2^{n-1} = 2^n$. This implies that $\mathcal{S}_0$ lies in one of the P-orbits. As H is transitive all P-orbits have the same length, i.e. $\{\mathcal{S}_0, \mathcal{S}_1\}$ is the set of P-orbits. By symmetry, we have $\{\mathcal{S}_0\gamma, \mathcal{S}_1\gamma\} = \{\mathcal{S}_0, \mathcal{S}_1\}$, a contradiction.

Case $H_SP = H$. Let ρ be in H such that $N^\rho \neq N$. Note that the elements of $\langle N_0 \cap P, N_0^\rho \cap P\rangle$ fix all elements in $\mathcal{S}_0 \cap \mathcal{S}_0\rho \neq \emptyset$. Thus $[N_0 \cap P, N_0^\rho \cap P] \leq Q$ fix these elements too, i.e. $[N_0 \cap P, N_0^\rho \cap P] = 1$. By Lemma 5.3, $(N_0 \cap P) \cap (N_0^\rho \cap P) = 1$, and as $N_0Q/Q \cap N_0^\rho Q/Q = 1$, we get $(N_0 \cap P)(N_0^\rho \cap P) \cap Q = 1$, and we see that $(N_0 \cap P)(N_0^\rho \cap P)Q = (N_0 \cap P) \times (N_0^\rho \cap P) \times Q$ elementary abelian. Hence, $P_0 = \langle Q, N_0^\rho \cap P \mid \rho \in H\rangle$ is a normal, elementary abelian group of H.

The group P is transitive, as

$$2^{n+1} = |H : H_S| = |H_SP : H_S| = |P : (H_S \cap P)| = |P : P_S|.$$

Consider the 2-group $T = PN = NR^\rho$. Then N is normal in T, i.e. T stabilizes the set $\{\mathcal{S}_0, \mathcal{S}_1\}$. The transitivity of T shows that there exists a $\nu' \in R^\rho$ such that $\mathcal{S}_0^{\nu'} = \mathcal{S}_1$ and $\mathcal{S}_1^{\nu'} = \mathcal{S}_0$. Write $\nu' = \sigma\nu$ with $\sigma \in L - L_0$ and $\nu \in N$. In particular

$$\sigma = \begin{pmatrix} 1 & & & \\ & & \mu & \\ & \lambda & & \\ & & & \rho \end{pmatrix}, \quad \nu = \begin{pmatrix} 1 & * & * & * \\ & \mathbf{1} & & * \\ & & \mathbf{1} & * \\ & & & \mathbf{1} \end{pmatrix}.$$

As $(\nu')^2 = \mathbf{1}$, we deduce that $\lambda = \mu^{-1}$ and $\rho^2 = \mathbf{1}$. Moreover, $[N_0, \nu'] \leq R < P$ and $|[N_0, \nu']| = |N_0|$, $N_0 \cap [N_0, \nu'] = 1$ by Lemma 5.3. Thus $N = [N_0, \nu'] \times N_0 = [N_0, \nu'] \times N_1$ and $NP = N_0P$.

Assume that $|NP/P| = 2^a$. Then, $a = 1$ if $H/P \simeq \mathrm{D}_{2k}$ and if $2^a = q$, if $H/P \simeq \mathrm{SL}(2,q)$ or $H/P \simeq \mathrm{Sz}(q)$ (note that we have $NP/P = \Omega_1(T/P)$ for $N \leq T \in \mathrm{Syl}_2(H)$). If $H/P \simeq \mathrm{SL}(2,q)$ or $H/P \simeq \mathrm{Sz}(q)$, then by [8, (3.2)] P/Q is the direct sum of natural H/P-modules, i.e. $|P/Q| \geq 2^{2a}$ in the first case and $|P/Q| \geq 2^{4a}$ in the second case.

We claim $a < n$. Otherwise, $N_0 \cap P = 1$: Let T be a Sylow 2-subgroup of H that contains N. Then $N_H(T) = TC$, with a cyclic group C of order $2^a - 1$ (as H/P is isomorphic to $\mathrm{SL}(2,2^a)$ or $\mathrm{Sz}(2^a)$), which acts regularly by conjugation on $\Omega_1(T/P) - 1$. We know, that $N_0 \not\leq P$ and N_0 is normalized by C as $N_H(T) \leq N_H(N)$. This implies $\Omega_1(T/P) = [N_0, C]P/P$ and hence $|[N_0, C]P/P| = 2^a \geq 2^n$, i.e. $N_0 \cap P = 1$. So we have $|N^\rho \cap P| \leq 2^n$ for all $\rho \in H$ and $H/P \simeq \mathrm{SL}(2,q)$ or $H/P \simeq \mathrm{Sz}(q)$, $q = 2^n$. Since, $P/Q = R/Q \times R^\gamma/Q$ we have $2^{2n} \leq |P/Q| \leq |N/Q|^2 = \frac{2^{2n}}{|Q|^2}$, which forces $|Q| = 1$, a contradiction.

Hence $|N_0 \cap P| = 2^{n-a} > 1$ and as $[N_0 \cap P, \nu'] \leq Q$, we have $|Q| \geq 2^{n-a}$. Also P is non-abelian, since $[(N_0 \cap P), \nu'] \neq 1$. By the modular law $R = P \cap N = [N_0, \nu'] \times (N_0 \cap P)$. Since $P/Q = (R/Q)(R^\gamma/Q)$, we get $|P/Q| = |R/Q| \cdot |R^\gamma/Q| \leq \frac{2^{2n-a}}{|Q|} \cdot \frac{2^{2n-a}}{|Q|} \leq 2^{2n}$. Clearly, $[N_0, \nu'] \cap P_0$ and $N_0 \cap P$ are contained in P_0, so that $|P_0/Q| \geq |(N_0 \cap P)/Q| \cdot |(N_0^\gamma \cap P)/Q| \geq 2^{2n-2a}$ and finally

$$1 < |P/P_0| \leq 2^{2a}$$

holds ($P/P_0 \neq 1$, as P is non-abelian).

As P/P_0 contains a natural H/P-module, this immediately rules out the possibility that $H/P \simeq \mathrm{Sz}(2^a)$. Assume next that $H/P \simeq \mathrm{SL}(2,2^a)$. Then P/P_0 is the natural $\mathrm{SL}(2,2^a)$-module and $N^\gamma P/P$ is a Sylow 2-subgroup of H/P. As before there exists a cyclic group C of order $2^a - 1$, such that CP/P normalizes $N^\gamma P/P$ and which acts regularly on $N^\gamma P/P - 1$ and on $R^\gamma P_0/P_0 - 1 = \{(\nu')^\kappa P_0/P_0 \mid \kappa \in C\}$. Since the elements in $P_0 \leq N_H(N_0)$ leave the sets $\mathcal{S}_0$ and $\mathcal{S}_1$ fixed, and as $R^\gamma P_0/P_0 - 1 = \{(\nu')^\kappa P_0/P_0 \mid \kappa \in C\}$, all elements in $R^\gamma - P_0$ interchange the two sets, forcing $|R^\gamma P_0/P_0| = 2$, a contradiction. So we have $a = 1$, $|Q| = |[N_0 \cap P, \nu']| = 2^{n-1}$, (Lemma 5.3) and $|P/P_0| = 4$.

We finally claim that $k = 3$, i.e. $H/P \simeq \mathrm{SL}(2,2) \simeq \mathrm{Sym}(3)$. Let $C \leq H$ be a cyclic group of order k, such that CP/P is the unique subgroup of index 2 in H/P. The group C acts on the four group P/P_0. Hence there exists a subgroup C_0 of C, with $|C : C_0| \leq 3$, which acts trivially on P/P_0. By [8, (3.1)] we know $C_{P/Q}(\sigma) = R^\rho Q/Q$ for $\sigma \in N^\rho - P$. For $1 \neq \rho \in C_0$ we have $N \neq N^\rho$ and

$$NP/P = (NP/P)^\rho = N^\rho P/P \neq NP/P,$$

a contradiction.

Assertions (a), (b) and the first two statements of (c) are now clear. If $\sigma \in P - P_0$, then $|C_{P_0}(\sigma)| \leq 2^{2n-2}$, which shows that P_0 is the only elementary subgroup of P of maximal order. So (c) holds. Clearly, P_0 fixes every set $\mathcal{S}_i, \mathcal{S}_i\gamma$, $i = 0, 1$ and Q acts regularly on each intersection $\mathcal{S}_i \cap \mathcal{S}_j\gamma$, $i, j = 0, 1$. This implies (d). We have already seen that $C \simeq \mathrm{C}_3$ acts faithfully on P/P_0. This shows (e).

APN case. We now argue with the group $\overline{H}$ and its action on $\mathcal{S}$. Now all arguments of the DHO case can be repeated, only that in Case $\overline{H}_S\overline{P} = \overline{H}$ the linear part of the element $\overline{\sigma}$ now has the shape

$$\sigma = \begin{pmatrix} 1 & & & \\ & & \mu & \gamma \\ & \lambda & & \delta \\ & & & \rho \end{pmatrix}.$$

However this slight difference is irrelevant. The arguments of the DHO case show again that $\mu = \lambda^{-1}$ and $\rho^2 = \mathbf{1}$. □

5.2 More properties of N_0 and N_1

For the remainder of this section we only work in the DHO case: all arguments can be carried over directly to the APN case. We can do so, as we do not need the linear representation of the automorphism group on the vector space U any more (we just use the permutation representation on the set $\mathcal{S}$).

Lemma 5.5. *Let τ be an involution in $NL - N$ that is conjugate to an element in $N_0 \cup N_1$. Set $\mathcal{T}_0 = \mathrm{Fix}_{\mathcal{S}}(\tau)$ and $\mathcal{T}_1 = \mathcal{S} - \mathcal{T}_0$. Then the following hold:*

(a) $\tau \in NL_0 - N$.

(b) Let $\nu \in N_1$. Then one of the following holds:

(1) $\nu \in C_{N_1}(\tau)$ and ν fixes $\mathcal{S}_0 \cap \mathcal{T}_0$ and $\mathcal{S}_0 \cap \mathcal{T}_1$.

(2) $\nu \notin C_{N_1}(\tau)$ and ν interchanges $\mathcal{S}_0 \cap \mathcal{T}_0$ and $\mathcal{S}_0 \cap \mathcal{T}_1$.

The analogous statement holds for $\nu \in N_0$.

(c) $|C_{N_i}(\tau)| = |\mathrm{Fix}_{\mathcal{S}_i}(\tau)| = 2^{n-1}$ for $i = 0, 1$.

(d) Let $\nu_i \in N_i - C_{N_i}(\tau)$, $i = 0, 1$. Then:

(1) $\nu_0\nu_1$ interchanges $\mathcal{T}_0$ with $\mathcal{T}_1$.

(2) $\nu_0\nu_1 \in N_N(M)$, where M is the unique conjugate of N that contains τ.

(3) $1 \neq [\tau, \nu_0\nu_1] \in M \cap N$.

Proof. Part (a) follows from assertion (c) of Lemma 3.10.

To (b) and (c): By assumption we have $N_i^\tau = N_i$, $i = 0, 1$ and $[\tau, N_i] \neq 1$ by Lemma 3.10.

(1) Let $\nu \in N_1$ with $(\mathcal{T}_0 \cap \mathcal{S}_0) \cap (\mathcal{T}_0 \cap \mathcal{S}_0)\nu \neq \emptyset$. Then $\nu \in C_{N_1}(\tau)$.

Let $S \in (\mathcal{T}_0 \cap \mathcal{S}_0) \cap (\mathcal{T}_0 \cap \mathcal{S}_0)\nu$, then S is fixed by $(\nu\tau)^2$. But $(\nu\tau)^2$ lies in N_1 and fixes $S \in \mathcal{S}_0$, which forces $(\nu\tau)^2 = 1$, i.e. $\nu \in C_{N_1}(\tau)$.

(2) We have $|\mathcal{T}_0 \cap \mathcal{S}_0| = |\mathcal{T}_0 \cap \mathcal{S}_1| = 2^{n-1}$.

Assume for instance $|\mathcal{T}_0 \cap \mathcal{S}_0| > 2^{n-1}$. Choose an element $\nu \in N_1 - C_{N_1}(\tau)$. Then $(\mathcal{T}_0 \cap \mathcal{S}_0) \cap (\mathcal{T}_0 \cap \mathcal{S}_0)\nu \neq \emptyset$ and (1) implies $\nu \in C_{N_1}(\tau)$, a contradiction. The assertion follows by symmetry.

(3) Let $\nu \in N_1 - C_{N_1}(\tau)$. Then $(\mathcal{T}_0 \cap \mathcal{S}_0)\nu = \mathcal{T}_1 \cap \mathcal{S}_0$.

By (1) $(\mathcal{T}_0 \cap \mathcal{S}_0) \cap (\mathcal{T}_0 \cap \mathcal{S}_0)\nu = \emptyset$, and $(\mathcal{T}_0 \cap \mathcal{S}_0)\nu \subseteq \mathcal{S}_0$, as τ normalizes N_1. With (2) this implies the assertion.

(4) We have $|C_{N_i}(\tau)| = 2^{n-1}$ for $i = 0, 1$.

By (3) we have that the group N_1 induces a permutation representation on $\{\mathcal{T}_0 \cap \mathcal{S}_0, \mathcal{T}_1 \cap \mathcal{S}_0\}$ and $C_{N_1}(\tau)$ is the kernel of this permutation representation. This implies $|N_1 : C_{N_1}(\tau)| = 2$.

By (1) - (4) the assertions (b) and (c) follow.

To (d): By the choice of the elements ν_i we have $1 \neq [\tau, \nu_i] \in N_i$, in particular $1 \neq [\tau, \nu_0\nu_1] \in N$. By (a.2) we have $(\mathcal{S}_0 \cap \mathcal{T}_0)\nu_0\nu_1 = \mathcal{S}_0 \cap \mathcal{T}_1$ and $(\mathcal{S}_1 \cap \mathcal{T}_0)\nu_0\nu_1 = \mathcal{S}_1 \cap \mathcal{T}_1$, i.e. $\nu_0\nu_1$ interchanges $\mathcal{T}_0$ and $\mathcal{T}_1$. Then $\nu_0\nu_1 \in N_G(M)$ by Lemma 3.9 and thus $[\tau, \nu_0\nu_1] \in M$, so (d) holds. □

Lemma 5.6. *Let $\tau = \tau_0^\gamma \in NL - N$ be an involution where $\tau_0 \in N_0 \cup N_1$. Set $M = N^\gamma$ and $M_i = N_i^\gamma$, $i = 0, 1$. Then:*

(a) $|M \cap N| = 2^{n-1}$. In particular the assertions of Lemma 5.4 hold for the group $H = \langle M, N \rangle$.

(b) Set $\mathcal{T}_0 = \mathcal{S}_0\gamma$, $\mathcal{T}_1 = \mathcal{S}_1\gamma$ and $\mathcal{D} = \{\mathcal{S}_i \cap \mathcal{T}_j \mid 0 \leq i, j \leq 1\}$. Then $\mathcal{D}$ is the set of $(M \cap N)$-orbits on $\mathcal{S}$.

(c) $C_{N_i}(N_{M_j}(N)) = N_{N_i}(M)$ and $C_{M_i}(N_{N_j}(M)) = N_{M_i}(N)$ for $0 \leq i, j \leq 1$.

(d) The group H acts on $\mathcal{D}$ and P_0 is the kernel of this action. P/P_0 induces a Klein four group on $\mathcal{D}$ and $H/P_0 \simeq \mathrm{Sym}(\mathcal{D}) \simeq \mathrm{Sym}(4)$ (here P and P_0 have the meaning of Lemma 5.4).

(e) We have $P_0 = (N_{M_0}(N) \times N_{M_1}(N))(N_{N_0}(M) \times N_{N_1}(M))$ and $P_0 = (M \cap N) \times N_{M_0}(N) \times N_{N_0}(M) = (M \cap N) \times N_{M_1}(N) \times N_{N_1}(M)$

Proof. By Lemma 5.5 $|C_{N_i}(\tau)| = 2^{n-1}$ for $i = 0, 1$. Thus $C_{N_0}(\tau) \times C_{N_1}(\tau) \leq C_G(\tau) \leq N_G(M)$ by Lemma 3.10 (a). As $C_{N_0}(\tau)$ fixes $\mathcal{S}_i$, $i = 0, 1$, as well as $\mathrm{Fix}_{\mathcal{S}}(\tau)$ this group fixes every set in $\mathcal{D}$. For $\nu_i \in N_i - C_{N_i}(\tau)$ the element $\nu = \nu_1\nu_2$ interchanges $\mathcal{T}_0$ with $\mathcal{T}_1$ (assertion (d.1) of Lemma 5.5), i.e. $(C_{N_0}(\tau) \times C_{N_1}(\tau))\langle\nu\rangle \leq N_N(M)$. Then Theorem 3.6 implies $N_N(M) = (C_{N_0}(\tau) \times C_{N_1}(\tau))\langle\nu\rangle$. Also by symmetry we have $N_M(N) = (C_{M_0}(\sigma) \times C_{M_1}(\sigma))\langle\omega\rangle$ for any element $1 \neq \sigma \in N_{N_0}(M) \cup N_{N_1}(M)$ and an ω in N, which interchanges $\mathcal{S}_0$ with $\mathcal{S}_1$. In particular $|C_{M_0}(\sigma)| = 2^{n-1}$ and $C_{M_0}(\sigma)^\nu \leq M_1$. Thus we have that $|[C_{M_0}(\sigma), \nu]| = 2^{n-1}$, $[C_{M_0}(\sigma), \nu] \leq M \cap N$, and $M \cap N = [C_{M_0}(\sigma), \nu]$ by Lemma 5.4. This implies (a) and (b).

By Theorem 3.6, Lemma 3.10 and Lemma 5.5 $N_{N_i}(M) = C_{N_i}(\tau')$, $i = 0, 1$, for all $1 \neq \tau' \in N_{M_0}(N) \cup N_{M_1}(N)$. Hence we have $N_{N_i}(M) = C_{N_i}(N_{M_j}(N))$ for $0 \leq i, j \leq 1$ and by symmetry we obtain assertion (c).

In particular $\widehat{P} = (N_{M_0}(N) \times N_{M_1}(N))(N_{N_0}(M) \times N_{N_1}(M))$ is elementary abelian and this group acts trivially on $\mathcal{D}$. From Lemma 5.4 we conclude $\widehat{P} = P_0$ as P_0 is the only elementary abelian subgroup of P of index 4. Assertions (d) and (e) now follow from Lemma 5.4. □

Remark 5.7. (a) With the notation as in the Lemma, one has

$$N_{M_0}(N) = M_0 \cap NL_0.$$

(b) Again set $H = \langle M, N\rangle$ as in Lemmas 5.4 and 5.6. For later purposes we record that, with the notation as in these lemmas:

(1) Every H-composition factor in the group P/Q is the natural H/P-module (i.e. as $P/N \simeq \mathrm{SL}(2,2)$ this composition factor has order 4).

(2) $Z(H) = M \cap N$.

Because of Lemma 5.6 (d) for assertion (1) it suffices to consider a composition factor W in P_0/Q. As P is a 2-group, we have $1 < C_W(P)$ (see [1, (5.5)]), i.e. $W = C_W(P)$ (as $C_W(P)$ is H-invariant). So W is an H/P-module and hence either trivial or W is the natural $\mathrm{SL}(2,2)$-module. Let $C = \langle\delta\rangle$ be cyclic of order three. By Lemma 5.6 (d) we may assume that $\mathcal{S}_0 \cap \mathcal{S}_0\gamma$ is invariant under δ, and that δ permutes the sets $\mathcal{S}_0 \cap \mathcal{S}_1\gamma$, $\mathcal{S}_1 \cap \mathcal{S}_0\gamma$, and $\mathcal{S}_1 \cap \mathcal{S}_1\gamma$ cyclically. Then $\mathcal{S}_0 \cap \mathcal{S}_0\gamma \subseteq \mathrm{Fix}_{\mathcal{S}_0} N_0^\delta \neq \mathcal{S}_0$. This shows that $N_{N_0}(N^\gamma) \cap N_{N_0}(N^\gamma)^\delta = 1$ and $Q \cap N_{N_0}(N^\gamma)N_{N_0}(N^\gamma)^\delta = 1$. We conclude that δ acts fixed-point-freely on P_0/Q, i.e. W is not the trivial $\mathrm{SL}(2,2)$-module.

Clearly, $Q = M \cap N \leq Z(H)$ as $H = \langle M, N\rangle$ and $Z(H) \leq P$. Assertion (2) follows from (1).

5.3 N_0 as a TI group

The goal of this subsection is the proof of Proposition 5.10. For this purpose we consider the group generated by conjugates of N_0 in the stabilizer of a point.

Let $S_0 \in \mathcal{S}$ be fixed by N_0. Let $\mathcal{F}$ be the set of N_0^γ, $\gamma \in G$, such that N_0^γ fixes S_0 and set

$$F = \langle \mathcal{F}\rangle.$$

Lemma 5.8. *The following statements hold.*

(a) F is a normal subgroup of the stabilizer of S_0 in G.

(b) $\mathcal{F}$ is a conjugacy class of self-centralizing TI subgroups of F.

(c) $O(F) = 1$.

Proof. Part (a) is clear by the definition of F.

(b) By Lemma 3.10

$$C_F(N_0) = N \cap F = N_0$$

i.e. N_0 is self-centralizing in F. Assume $1 \neq \tau \in N_0 \cap N_0^\gamma$. Then

$$\mathcal{S}_0 = \mathrm{Fix}_{\mathcal{S}}(N_0) = \mathrm{Fix}_{\mathcal{S}}(\tau) = \mathrm{Fix}_{\mathcal{S}}(N_0^\gamma) = \mathcal{S}_0\gamma,$$

which implies that $\gamma \in N_G(N_0)$, i.e. $N_0 = N_0^\gamma$.

(c) Set $R = O(F)$ and $X = N_0R$. It follows that X satisfies the assumptions of [5, Lemma 4.2]. Since $|N_0| > 2$ we have $X = N_0 \times R$ and hence $R = 1$ by Lemma 3.10. □

Lemma 5.9. *Let $N_0^\gamma \in \mathcal{F} - \{N_0\}$ and set $F_0 = \langle N_0, N_0^\gamma\rangle$. Then:*

(a) $O_2(F_0) = N_{N_0}(N_0^\gamma)N_{N_0^\gamma}(N_0)$ is elementary abelian of order 2^{2n-2}.

(b) $F_0/O_2(F_0) \simeq \mathrm{Sym}(3)$.

Proof. We show that:

(1) There *exists a pair* N_0, N_0^γ, which satisfies assertions (a) and (b):

Pick $\gamma \in G$ such that $|N \cap N^\gamma| = 2^{n-1}$, i.e. the assumptions of Lemma 5.4 are satisfied. We know that $|\mathrm{Fix}_{\mathcal{S}}(N_0) \cap \mathrm{Fix}_{\mathcal{S}}(N_0^\gamma)| = 2^{n-1}$, i.e. by choosing the notation in a suitable way we may assume that $N_0^\gamma \in \mathcal{F}$. Moreover neither N_0 nor N_0^γ are subgroups of $P = O_2(\langle N, N^\gamma\rangle)$, so that $F_0/(F_0 \cap P) \simeq F_0P/P \simeq \mathrm{Sym}(3)$. Now assertions (a) and (b) follow by [8, 2.8].

(2) We have $F/O_2(F) \simeq \mathrm{L}_m(2)$, A_6, A_7, A_8, A_9, M_{22}, M_{23}, or M_{24}.

The possible structures of $F/O_2(F)$ are listed in [8, Theorem A] (by Lemma 5.8 the assumptions of this theorem hold). The cases $F/O_2(F) \simeq \mathrm{L}_m(q)$, $\mathrm{U}_3(q)$, or $\mathrm{Sz}(q)$, $q > 2$ are ruled out by (1). The remaining cases imply (2).

Assertions (a) and (b) are now a consequence of (2). □

Proposition 5.10. *Let N^γ be an element of $\mathcal{C} - \{N\}$. Then $|N \cap N^\gamma| = 2^{n-1}$.*

Proof. Assume that $\mathrm{Fix}_{\mathcal{S}}(N_0) \cap \mathrm{Fix}_{\mathcal{S}}(N_0^\gamma) = \emptyset$. Then N_0^γ centralizes N_0, i.e. $N_0^\gamma \leq C_G(N_0) = N$ and $N_0^\gamma = N_1$, follows. But then $N = N^\gamma$, a contradiction.

Hence $\mathrm{Fix}_{\mathcal{S}}(N_0) \cap \mathrm{Fix}_{\mathcal{S}}(N_0^\gamma) \neq \emptyset$. Thus $F_0 = \langle N_0, N_0^\gamma\rangle$ satisfies the assumptions of Lemma 5.9. In particular $|N_{N_0^\gamma}(N_0)| = |N_{N_0}(N_0^\gamma)| = 2^{n-1}$ and $[N_{N_0^\gamma}(N_0), N_{N_0}(N_0^\gamma)] = 1$ by Lemma 5.9. Thus $N_{N_0^\gamma}(N_0)$ fixes $\mathcal{S}_0 = \mathrm{Fix}_{\mathcal{S}}(N_{N_0}(N^\gamma))$ and thus $\mathcal{S}_1$ too. It follows that $N_{N_0^\gamma}(N_0)$ normalizes N. Assertion (a) of Lemma 5.6 completes the proof. □

Proof. (Theorem 5.1) This theorem is an immediate consequence of Lemma 5.4 and Proposition 5.10. □

6 Recognition results and examples

We will show that the existence of more than one extension group, shows that an extension of a DHO or an APN function is, in fact, at least a two-fold iterated extension. Moreover we shall generalize this result if there are more than three extension groups and give a direct construction of the k-fold extension in this case, as well as some of its automorphisms.

We illustrate our results on extension groups by some examples. We also comment, how the results on automorphism groups of the next Section 7, fit into these concrete examples.

In this section the symbol $\mathcal{S}$ denotes the extension of a bilinear DHO $\mathcal{S}_\beta$ in the DHO case, while in the APN case this symbol denotes the graph of the extension $F = F_{f_0,f_1}$ of quadratic APN functions f_0 and f_1. We shall assume in both cases that $\mathcal{S}$ is ambient in the defining space and in the APN case we additionally assume that F is fully ambient. In particular by Theorem 3.6 weak extension groups are actually extension groups and the results of Sections 3 and 5 are available.

Theorem 6.1. *The following statements hold.*

(a) Let $\mathcal{S}$ be a DHO of rank ≥ 6, which is ambient in its defining space and which admits at least two extension groups. Then

$$\mathcal{S} = \overline{\mathcal{S}}_{\overline{\beta}}, \quad \mathcal{S}_{\overline{\beta}} = \overline{\mathcal{S}}_{\beta},$$

where $\mathcal{S}_\beta$ is a symmetric bilinear DHO, i.e. $\mathcal{S}$ is a two-fold extension of a symmetric DHO.

(b) Let F_{f_0,f_1} be the extension of an APN function of rank ≥ 6, which admits at least two extension groups and assume that f_0 and f_1 are ambient in their defining space. Then $f_0 = F_{g_0,g_0}$ and $f_1 = F_{g_1,g_1}$ with quadratic APN functions g_0 and g_1, i.e. F is a two-fold extension of quadratic APN functions.

We prove this Theorem by a series of lemmas and distinguish the APN and DHO case.

6.1 The DHO case

Let M, N be two extension groups of a DHO $\mathcal{S}$ of rank $n+1$ and with an ambient space U of dimension $2n+1+m$. Denote by $\mathcal{S}_0$, $\mathcal{S}_1$, the orbits of $N = N_0 \times N_1$ and by $\mathcal{T}_0$, $\mathcal{T}_1$, the orbits of $M = M_0 \times M_1$. For $i = 0, 1$ we set

$$\begin{array}{ll} V_i^N = \langle S \cap S' \mid S, S' \in \mathcal{S}_i,\ S \neq S' \rangle, & V_i^M = \langle S \cap S' \mid S, S' \in \mathcal{T}_i,\ S \neq S' \rangle, \\ Y^N = V_0^N \cap V_1^N, & Y^M = V_0^M \cap V_1^M, \\ U^N = V_0^N + V_1^N, & U^M = V_0^M + V_1^M. \end{array}$$

Finally, for $i = 0, 1$ we define $M_N = N_M(N)$, $M_{i,N} = N_{M_i}(N)$, $N_M = N_N(M)$, and $N_{i,M} = N_{N_i}(M)$. By Lemma 5.4 and Proposition 5.10 we have $|M_N| = |N_M| = 2^{2n-1}$ and $|M_{i,N}| = |N_{i,M}| = 2^{n-1}$, $i = 0, 1$.

Lemma 6.2. *With the above notation we have:*

(a) $Y^M \subseteq U^N$ and $Y^N \subseteq U^M$.

(b) $\dim Y^M \cap Y^N \geq m - n + 1$.

Proof. (a) Assume $y \in Y^M - U^N$. Pick $\tau \in N_{0,M}$, $\tau' \in M_{0,N} \times M_{1,N}$. By assertion (c) of Lemma 5.4 the elements commute and we have

$$y(1+\tau)(1+\tau') = y(1+\tau')(1+\tau) = 0,$$

which shows that $y(1+\tau) \in (Y^M \cap V_0^N) - Y^N$. Pick $\mu \in M_N - M_{0,N} \times M_{1,N}$. Then $V_0^N \mu = V_1^N$. As μ centralizes Y^M, we see that

$$Y^M \cap V_0^N = (Y^M \cap V_0^N)\mu = Y^M \cap V_1^N, \quad \text{i.e.} \quad Y^M \cap V_0^N \subseteq Y^N.$$

This implies $y(1+\tau) \in Y^M \cap Y^N$, a contradiction.

(b) Let $S \in \mathcal{S}_0 \cap \mathcal{T}_0$, i.e. $V_0^N = (S \cap V_0^N) \oplus Y^N$. We first note that $V_0^N \not\subseteq U^M$: Otherwise $V_1^N = V_0^N \mu \subseteq U^M$ (μ as above) and it follows $U^N = U^M$. If, however, $S' \in \mathcal{S}_0 \cap \mathcal{T}_1$, then $S \cap S' \subseteq U^N$ but $S \cap S' \not\subseteq U^M$, a contradiction.

Now (a) and the modular law imply that

$$U^M \cap V_0^N = (S \cap V_0^N \cap U^M) \oplus Y^N$$

and it follows that

$$V_0^N = (S \cap S') \oplus (S \cap V_0^N \cap U^M) \oplus Y^N$$

follows.

Let $\widetilde{S}$ be in $\mathcal{S}_1 \cap \mathcal{T}_0$. Then by symmetry

$$V_1^N = (\widetilde{S} \cap \widetilde{S}') \oplus (\widetilde{S} \cap V_1^N \cap U^M) \oplus Y^N$$

with $\widetilde{S}' \in \mathcal{S}_1 \cap \mathcal{T}_1$. Since $U^N = (S \cap V_0^N) \oplus (\widetilde{S} \cap V_1^N) \oplus Y_N$, we finally obtain

$$U^N = (S \cap S') \oplus (S \cap V_0^N \cap U^M) \oplus (\widetilde{S} \cap \widetilde{S}') \oplus (\widetilde{S} \cap V_1^N \cap U^M) \oplus Y^N.$$

Moreover, as U^N and U^M have codimension 1 in U we see that $U^N \cap U^M$ has codimension 1 in U^N and $(S \cap V_0^N \cap U^M) \oplus (\widetilde{S} \cap V_1^N \cap U^M) \oplus Y^N \subseteq U^N \cap U^M$. So if $S \cap S' = \langle z \rangle$ and $\widetilde{S} \cap \widetilde{S}' = \langle \widetilde{z} \rangle$ then

$$U^N \cap U^M = \langle z + \widetilde{z} \rangle \oplus (S \cap V_0^N \cap U^M) \oplus (\widetilde{S} \cap V_1^N \cap U^M) \oplus Y^N.$$

We claim that $Y^M \subseteq (S \cap V_0^N \cap U^M) \oplus (\widetilde{S} \cap V_1^N \cap U^M) \oplus Y^N$.

Otherwise, there exists $w \in Y^M$ of the form

$$w = z + \widetilde{z} + s + \widetilde{s} + y$$

with $s \in S \cap V_0^N \cap U^M$, $\widetilde{s} \in \widetilde{S} \cap V_1^N \cap U^M$, and $y \in Y^N$.

Let $1 \neq \tau \in M_{0,N}$. Then $0 \neq u = z(1+\tau) \in S \cap V_0^N \cap U^M$, $0 \neq u' = \widetilde{z}(1+\tau) \in \widetilde{S} \cap V_1^N \cap U^M$, $y(1+\tau) \in Y^N$, and $0 = s(1+\tau) = \widetilde{s}(1+\tau)$. In particular $w\tau \neq w$, a contradiction. The claim follows.

For $w \in Y^M$ we again write $w = s + \widetilde{s} + y$ with $s, \widetilde{s}, y$ as above. Then

$$s + \widetilde{s} + y = w = w\mu = s\mu + \widetilde{s}\mu + y\mu,$$

so that

$$s = \widetilde{s}\mu \pmod{Y^N}, \quad \widetilde{s} = s\mu \pmod{Y^N}.$$

Therefore

$$(Y^M + Y^N)/Y^N \cap ((S \cap V_0^N \cap U^M) + Y^N)/Y^N = 0$$

and it follows that

$$\dim Y^M/(Y^N \cap Y^N) = \dim(Y^M + Y^N)/Y^N \leq n - 1.$$

This finally implies that

$$\dim(Y^N \cap Y^N) \geq \dim Y^M - (n-1) = m - n + 1.$$

□

Lemma 6.3. *With the above notation we have that:*

(a) $\mathcal{S}(0) = \{S \cap V_0^N \mid S \in \mathcal{S}_0\}$ *is a DHO on* V_0^N*.*

(b) The group $M_{0,N} \times M_{1,N}$ *induces an extension group on* V_0^N*.*

Proof. Part (a) is obvious.

(b) From assertion (b) of Lemma 6.2 (and with the notation of the proof) and $\dim V_0^N = n + m$ we deduce that

$$V_0^N = (S \cap S') \oplus (S \cap V_0^N \cap U^M) \oplus (S' \cap V_0^N \cap U^M) \oplus (Y^M \cap Y^N).$$

Also $\langle S_1 \cap S_2 \cap V_0^N \mid S_1, S_2 \in \mathcal{S}_0 \cap \mathcal{T}_0,\ S_1 \neq S_2\rangle \subseteq (S \cap V_0^N \cap U^M) \oplus (Y^M \cap Y^N)$ and $\langle S_1 \cap S_2 \cap V_0^N \mid S_1, S_2 \in \mathcal{S}_0 \cap \mathcal{T}_1,\ S_1 \neq S_2\rangle \subseteq (S' \cap V_0^N \cap U^M) \oplus (Y^M \cap Y^N)$. As $M_{i,N}$ acts regularly on $\mathcal{S}_0 \cap \mathcal{T}_j$ and fixes $\mathcal{S}_0 \cap \mathcal{T}_i$ pointwise $\{i, j\} = \{0, 1\}$, we deduce that $M_{0,N} \times M_{1,N}$ satisfies axioms (E1)-(E3) of a weak extension group. Then by Theorem 3.2 $M_{0,N} \times M_{1,N}$ actually induces an extension group on V_0^N. □

The assertion of Theorem 6.1 for the DHO case is a consequence of Lemma 6.3 and Theorem 3.2.

6.2 The APN case

Let M and N be the linear parts of two extension groups of an $n+1$-dimensional APN function, with an ambient space of dimension $2n+1+m$. Denote by $\mathcal{S}_0$ and $\mathcal{S}_1$, the orbits of $\overline{N} = \overline{N}_0 \times \overline{N}_1$ and by $\mathcal{T}_0$ and $\mathcal{T}_1$, the orbits of $\overline{M} = \overline{M}_0 \times \overline{M}_1$. For $i = 0, 1$ we set

$$\begin{array}{ll} V_i^N = \langle x + x' \mid x, x' \in \mathcal{S}_i\rangle, & V_i^M = \langle x + x' \mid x, x' \in \mathcal{T}_i\rangle, \\ Y^N = V_0^N \cap V_1^N, & Y^M = V_0^M \cap V_1^M, \\ U^N = V_0^N + V_1^N, & U^M = V_0^M + V_1^M. \end{array}$$

We choose the notation such that $0 \in \mathcal{S}_0 \cap \mathcal{T}_0$, in particular, we have $\overline{M}_0 = M_0$ and $\overline{N}_0 = N_0$. For $i = 0, 1$ we define $M_N = N_M(N)$, $M_{i,N} = N_{M_i}(N)$, $N_M = N_N(M)$, and $N_{i,M} = N_{N_i}(M)$. Finally, we set $H = \langle N, M \rangle$ and denote by E the third extension group in H (see Lemma 5.4). By our assumption $\mathcal{S}$ is the graph of a function $F = F_{f_0, f_1}$, such that $f_i : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is a quadratic APN function ambient in $\mathbb{F}_2^n \oplus \mathbb{F}_2^m$. It follows from Remark 3.3 and Theorem 4.4 that $C_U(N) = Y^N$ and $\dim U/(V_0^N + V_1^N) = 1$ and by Lemma 5.4 the analogous assertion holds for M and E too.

Lemma 6.4. *For each* 2*-set* $\{R, Q\}$ *in* $\{E, M, N\}$*, the vector space* $U^R \cap U^Q$ *has codimension* 1 *in* U^R*.*

Proof. As $0 \in \mathcal{S}_0$ we have $V_0^N = \langle \mathcal{S}_0 \rangle$. We know $U = \langle v \rangle \oplus U^N$ for some $v \in \mathcal{S}$. Hence $v \in \mathcal{S}_1$ and $\mathcal{S}_1$ is contained in the flat $v + V_1^N$. Since $v + V_1^N = v' + V_1^N$ for all $v' \in \mathcal{S}_1$, we even have $U = \langle v' \rangle \oplus U^N$. Pick $v \in \mathcal{S}_1 \cap \mathcal{T}_0$ and suppose that $U^N = U^M$. Then $U = \langle v \rangle \oplus U^N = \langle v \rangle + U^M = U^M$, a contradiction. The assertion of the lemma follows by symmetry. □

Lemma 6.5. *We have* $Y^R \subseteq U^Q$ *for each* 2*-set* $\{R, Q\}$ *in* $\{E, M, N\}$*.*

Proof. By symmetry it suffices to assume that $R = M$ and $Q = N$. Assume that $y \in Y^M - U^N$. Pick $\tau \in N_{0,M}$, $\tau' \in M_{0,N} \times M_{1,N}$. By assertion (c) of Lemma 5.4 the elements commute and we have

$$y(1 + \tau)(1 + \tau') = y(1 + \tau')(1 + \tau) = 0$$

which shows that $y(1 + \tau) \in (Y_M \cap V_0^N) - Y_N$. Pick $\mu \in M_N - M_{0,N} \times M_{1,N}$. Then $V_0^N \mu = V_1^N$. As μ centralizes Y^M, we see that

$$Y^M \cap V_0^N = (Y^M \cap V_0^N)\mu = Y^M \cap V_1^N, \quad \text{i.e.} \quad Y^M \cap V_0^N \subseteq Y^N.$$

This implies that $y(1 + \tau) \in Y^M \cap Y^N$, a contradiction. □

Lemma 6.6. *For each* 2*-set* $\{R, Q\}$ *in* $\{E, M, N\}$*, we have* $Y^R \cap Y^Q = Y^E \cap Y^M \cap Y^N$*.*

Proof. We know that $Y^R = C_U(R)$. Then $Y^R \cap Y^Q = C_U(H)$ as $H = \langle R, Q \rangle$ and the assertion follows. □

Lemma 6.7. *For each* 2*-set* $\{R, Q\}$ *in* $\{E, M, N\}$*, we have* $U^R \cap U^Q = U^E \cap U^M \cap U^N$*.*

Proof. By symmetry it suffices to assume that $R = M$ and $Q = N$. Suppose that $W = U^E \cap U^M \cap U^N$ is a proper subspace of $U^M \cap U^N$. This shows by Lemma 6.4 that W has codimension 3 in U. Let $v \in U - U^N$. We know that the map $\phi : N \to U^N/Y^N$ defined by $\phi(\tau) = v(1 + \tau)$ is an isomorphism of the abelian groups N and U^N/Y^N.

First we observe that $O_2(H)$ centralizes the quotient $U/(U^M \cap U^N)$. Namely if $\tau \in O_2(H) = \langle N_M, M_N \rangle$, then τ fixes U^N and U^M and therefore we have $U(1 + \tau) \subseteq U^M \cap U^N$, which shows the claim.

By symmetry $O_2(H)$ also centralizes the quotient U/W. Now $N_M \leq O_2(H)$, which implies that $\phi(N_M) \subseteq W/Y^N$ (note that by Lemma 6.5 $Y^N \subseteq W$). This implies that $2^{2n-1} = |N_M| = |\phi(N_M)| \leq |W/Y^N| = 2^{2n-2}$, a contradiction. □

Lemma 6.8. *We have* $V_0^N \cap Y^M \subseteq Y^N$, $V_1^N \cap Y^M \subseteq Y^N$, *and* $\dim(Y^E \cap Y^M \cap Y^N) = \dim(Y^M \cap Y^N) \geq m - n + 1$.

Proof. First we observe that $V_i^N \not\subseteq U^M$: If for instance $V_0^N \subseteq U^M$, then also $V_1^N = V_0^N \mu \subseteq U^M$ for $\mu \in M_N - (M_{0,N} \times M_{1,N})$ contradicting Lemma 6.4.

Hence there exist elements $s_0 \in (V_0^N \cap \mathcal{S}_0) - (U^M \cap V_0^N)$ and (considering the action of μ) we may even assume $s_0 \in \mathcal{T}_1$. Thus $V_0^N = \langle s_0 \rangle \oplus (U^M \cap V_0^N)$. Apply μ and we obtain $V_1^N = \langle s_1 \rangle \oplus (U^M \cap V_1^N)$ with $s_1 = s_0\mu$. Note that $s_0\overline{\mu} \in \mathcal{S}$ but $s_1 \notin \mathcal{S}$. From Lemma 6.4 we deduce that

$$U^N = \langle s_0 \rangle \oplus \langle s_1 \rangle \oplus ((U^M \cap V_0^N) + (U^M \cap V_1^N)).$$

Note that $U^M \cap U^N = \langle s_0 + s_1 \rangle \oplus ((U^M \cap V_0^N) + (U^M \cap V_1^N))$ as this space is μ-invariant. We recall that $|\mathcal{S}| = |(\mathcal{S} + Y^N)/Y^N|$, i.e. $V_0^N/Y^N = (\mathcal{S}_0 + Y^N)/Y^N$. As $s_0 + Y^N \notin (U^M \cap V_0^N)/Y^N$, we deduce that $\dim(W_0^N + Y^N)/Y^N = n - 1$ for $W_0^N = \langle \mathcal{S}_0 \cap \mathcal{T}_0 \rangle$ and hence $V_0^N \cap U^M = W_0^N + Y^N$. Similarly, we obtain that $V_1^N \cap U^M = W_1^N + Y^N$ with $W_1^N = W_0^N \mu$.

Claim: We have $Y^M \subseteq (U^M \cap V_0^N) + (U^M \cap V_1^N)$

Suppose, $Y^M \not\subseteq (U^M \cap V_0^N) + (U^M \cap V_1^N)$. Then there exist elements $w \in Y^M$ of the form

$$w = s_0 + s_1 + u + u' + y$$

with $u \in W_0^N$, $u' \in W_1^N$ and $y \in Y^N$. For $1 \neq \tau \in M_{0,N}$ we have $0 = w(1+\tau) = u(1+\tau) = u'(1+\tau)$ and $y(1+\tau) \in Y^N$. This shows that $s_0(1+\tau) + s_1(1+\tau) \in Y^N$. As $s_0(1+\tau) \in V_0^N \cap U^M$, $s_1(1+\tau) \in V_1^N \cap U^M$, we also have that $s_0(1+\tau), s_1(1+\tau) \in Y^N$. Moreover $s_0\tau \neq s_0$ are different elements in $\mathcal{S}$. Hence $s_0 + Y^N$ and $s_0\tau + Y_N$ are different elements in V_0^N/Y^N, a contradiction. The claim follows.

Let $w = u + u' + y \in Y^M$, u, u', y as before. Then

$$u + u' + y = w = w\mu = u\mu + u'\mu + y\mu,$$

showing $u' \equiv u\mu \pmod{Y^N}$, $u \equiv u'\mu \pmod{Y^N}$. This implies that

$$(Y^M + Y^N)/Y^N \cap (V_0^N \cap U^M)/Y^N = 0$$

and therefore $V_0^N \cap Y^M \subseteq Y^N$ and

$$\dim Y^M/(Y^M \cap Y^N) = \dim(Y^M + Y^N)/Y^N \leq n - 1.$$

We obtain that $\dim Y^M \cap Y^N \geq \dim Y^M - n + 1 = m - n + 1$. The assertion $V_1^N \cap Y^M \subseteq Y^N$ follows by symmetry. □

Lemma 6.9. *Set* $V_{i,j} = \langle x+y \mid x,y \in \mathcal{S}_i \cap \mathcal{T}_j\rangle$, $i,j=0,1$. *Then* $\dim(V_{i,j} + (Y^M \cap Y^N))/(Y^M \cap Y^N) = n-1$ *for all* i,j *and* $\dim Y^M \cap Y^N = m-n+1$. *Moreover,* $(V_i^N \cap U^M)/(Y^M \cap Y^N) = (V_{i,0} + (Y^M \cap Y^N))/(Y^M \cap Y^N) \oplus (V_{i,1} + (Y^M \cap Y^N))/(Y^M \cap Y^N)$ *for* $i=0,1$, *and the similar assertions hold for* $(V_i^M \cap U^M)/(Y^M \cap Y^N)$.

Proof. We have $V_{i,j} \subseteq U^M \cap U^N$ for all i,j. By Lemma 6.8 $V_{0,0} \cap V_{0,1} \subseteq V_0^M \cap V_1^M \cap V_0^N = Y^M \cap V_0^N \subseteq Y^M \cap Y^N$, i.e. $(V_{i,0} + (Y^M \cap Y^N))/(Y^M \cap Y^N) \cap (V_{i,1} + (Y^M \cap Y^N))/(Y^M \cap Y^N) = 0$.

Also $|(\mathcal{S}_0 \cap \mathcal{T}_0 + (Y^M \cap Y^N))/(Y^M \cap Y^N)| = 2^{n-1}$ showing that $\dim(V_{0,0} + (Y^M \cap Y^N))/(Y^M \cap Y^N) \geq n-1$. By symmetry $\dim(V_{i,j} + (Y^M \cap Y^N))/(Y^M \cap Y^N) \geq n-1$ for all i,j. Therefore again by Lemma 6.8

$$m+n-1 = \dim V_0 \cap U^M \geq 2(n-1) + m - n + 1,$$

so that equality must hold and we have $\dim(V_{0,j} + (Y^M \cap Y^N))/(Y^M \cap Y^N) = n-1$ and $\dim Y^M \cap Y^N = m-n+1$. By symmetry all assertions follow. □

Proof. (of Theorem 6.1) Let $V_i^N = R_i \oplus Y^N$ for $i=0,1$. By Theorem 3.2 there exist quadratic APN-functions $f_i : R_i \to Y^N$, such that $\mathcal{S}_0 = \{z + f_0(z) \mid z \in R_0\}$ is the graph of f_0 and $v + \mathcal{S}_1 = \{z + f_1(z) \mid z \in R_1\}$ is the graph of f_1. Here $U = \langle v\rangle \oplus U^N$. Without loss of generality we may assume that $v \in \mathcal{S}_1 \cap \mathcal{T}_0$. We shall show that both graphs admit extension groups. The assertion of Theorem 6.1 is then a consequence of Theorem 3.2.

Case (V_0^N, f_0) We claim that $M_{0,N} \times \overline{M}_{1,N}$ is an extension group. Conditions (E1) and (E2) of the definition of extension groups follow immediately by the definition of $M_{0,1} \times \overline{M}_{1,N}$. We have $V_{0,j} = \langle \mathcal{S}_0 \cap \mathcal{T}_j\rangle$, $j=0,1$. By Lemma 6.9 we get $C_{V_0^N}(M_{0,N} \times M_{1,N}) = Y = Y^M \cap Y^N$, $\dim V_0/(V_0^N \cap U^M) = V_0/(V_{0,0} + V_{0,1} + Y) = 1$, and $\dim(V_{0,0} + V_{0,1} + Y)/Y = 2(n-1)$. This shows (E3) and therefore $M_{0,N} \times \overline{M}_{1,N}$ is a weak extension group of f_0. Since f_0 is quadratic, we deduce by Theorem 4.4 and Remark 3.3 that this group is in fact an extension group.

Case (V_1^N, f_1) We first observe that $r : M_{1,N} \to U$ defined by $r(\tau) = v(1+\tau)$, is a 1-coboundary (i.e. $r(\tau\tau') = r(\tau)\tau' + r(\tau')$). Thus $\widetilde{c} : M_{1,N} \to U$, defined by $\widetilde{c}_\tau = c_\tau + r(\tau)$ (here $\overline{\tau} = \tau + c_\tau$), is a 1-cocycle. We define $\widetilde{\tau} = \tau + \widetilde{c}_\tau$ and $\widetilde{M}_{1,N} = \{\widetilde{\tau} \mid \tau \in M_{1,N}\}$ and observe that $M_{0,N} \times \widetilde{M}_{1,N}$ is elementary abelian, as the $r(\tau)$'s lie in Y^M.

We claim that this group is an extension group. Clearly, as v is fixed by $M_{0,N}$, the set $v + (\mathcal{S}_1 \cap \mathcal{T}_0)$ is fixed pointwise by this group and this group acts regularly on $v + (\mathcal{S}_1 \cap \mathcal{T}_1)$. For $v+u \in v + \mathcal{S}_1$ and $\widetilde{\tau} \in \widetilde{M}_{1,N}$ we compute

$$(v+u)\widetilde{\tau} = (v\tau + r(\tau)) + u\overline{\tau} = v + u\overline{\tau}.$$

This shows that $\widetilde{M}_{1,N}$ fixes the set $v + (\mathcal{S}_1 \cap \mathcal{T}_1)$ pointwise and on $v + (\mathcal{S}_1 \cap \mathcal{T}_0)$ this group acts regularly. Hence conditions (E1) and (E2) hold. Condition (E3) follows, again by Lemma 6.9. Thus $M_{0,N} \times \widetilde{M}_{1,N}$ is a weak extension group.

The same argument as in the previous case shows that this group is in fact an extension group. □

In [4] the diagonally represented DHOs were characterized as those DHOs that admit at least three (and thus infinitely many) iterated extensions. Theorem 6.1 leads to:

Corollary 6.10. *Let $\mathcal{S}$ be a DHO of rank $n+k$, $n \geq 4$, $k \geq 2$, which admits at least 2^k extension groups. Then there exists a symmetric, diagonally represented DHO $\mathcal{S}_\beta$ of rank n, such that $\mathcal{S}$ is the $(k+1)$-fold extension of $\mathcal{S}_\beta$.*

Proof. Let N be an extension group with orbits $\mathcal{S}_i$, $i = 0, 1$ and set $V_i = \langle S \cap S' \mid S, S' \in \mathcal{S}_i, S \neq S' \rangle$. Let E, M be two extension groups $\neq N$. By Lemma 6.3 we have that $\mathcal{S}(0) = \{S \cap V_0 \mid S \in \mathcal{S}_0\}$ is a DHO and the groups $N_{R_0}(N) \times N_{R_1}(N)$, $R = E, M$, induce extension groups on $\mathcal{S}(0)$.

Assume that both groups induce the same extension group on $\mathcal{S}(0)$. So for $\varepsilon \in N_{E_0}(N) \times N_{E_1}(N)$, there exists an element $\mu \in N_{M_0}(N) \times N_{M_1}(N)$, such that $\varepsilon\mu$ fixes each $S \in \mathcal{S}(0)$. This implies that $\varepsilon\mu$ lies in the common normalizer of the groups N_0 and N_1. As N_1 acts faithfully on $\mathcal{S}_0$, we see that $\varepsilon\mu$ lies in the centralizer of N_1, which is N (see Lemma 3.10). Thus $\varepsilon \in \langle N, M \rangle$. However this group contains precisely three extension groups (Lemma 5.4). Thus $\mathcal{S}(0)$ admits at least $\lceil \frac{2^k-1}{2} \rceil = 2^{k-1}$ extension groups. By Theorem 6.1 $\mathcal{S}(0)$ is the 2-fold extension of a symmetric DHO $\mathcal{S}'$, and $\mathcal{S}$ is, in fact, the 3-fold extension of $\mathcal{S}'$. By [4, Thm. 3.2] $\mathcal{S}'$ is diagonally represented. Now a routine induction finishes the proof. □

For APN functions we have an analogous corollary:

Corollary 6.11. *Let $F = F_{f_0,f_1}$ be a fully ambient APN function of rank $n+k$, where $n \geq 4$ and $k \geq 2$, which admits at least 2^k extension groups. Then there exist quadratic APN functions g_0, g_1 of rank n, such that f_i, for $i = 0, 1$, is the k-fold extension of g_i.*

Proof. We know by Theorem 3.2 that f_0 and f_1 are quadratic APN functions and by the proof of Theorem 6.1 (APN case), we know that for an extension group $E = E_0 \times E_1 \neq N$ the group $N_{E_0}(N) \times N_{E_1}(N)$ is the linear part of an extension group of f_i, $i = 0, 1$. Our claim follows by induction using Theorem 4.4 if we show that the groups of the form $N_{E_0}(N) \times N_{E_1}(N)$ induce at least 2^{k-1} extension groups on each f_i. By symmetry it suffices to show that f_0 admits at least 2^{k-1} extension groups.

Let $E = E_0 \times E_1$ and $M = E_0 \times M_1$ be the linear parts of two extension groups that are not equal to N, and which induce the same extension group on $\mathcal{S}_0$, the graph of f_0. Then for each $\overline{\varepsilon} \in N_{\overline{E}_0}(\overline{N}) \times N_{\overline{E}_1}(\overline{N})$ there exists an element $\overline{\mu} \in N_{\overline{M}_0}(\overline{N}) \times C_{\overline{M}_1}(\overline{N})$, such that $\overline{\varepsilon\mu}$ fixes each vector in $\mathcal{S}_0$. As $\overline{\varepsilon\mu}$ normalizes $\overline{N}$, we see that $\overline{\varepsilon\mu}$ centralizes $\overline{N}_1$, i.e. $\overline{\varepsilon\mu} \in \overline{N}$. Hence $E \leq \langle N, M \rangle$. By Lemma 5.4 we see that there are at most two extension groups inducing the same extension group on f_0. As in the proof of the previous corollary we conclude, that f_0 admits at least 2^{k-1} extension groups. □

6.3 A non-recursive version of the k-fold extension

In this subsection we present, for $k > 2$, an explicit non-recursive representation of a k-fold extended DHO, respectively of a k-fold extended APN function. These non-recursive representations allow a concrete description of $2^k - 1$ extension groups and and a group $GL(k, 2)$ (compare also Section 7).

We start with the DHO-case. We say a DHO $\mathcal{S}_\beta$, $\beta : X \to \mathrm{Hom}(X, Y)$, is diagonally represented by $z \in X$, if and only if for its diagonal map, $x\delta = x\beta(x)$, we have that $x\delta = x\beta(z)$. In [4] it is shown that DHOs that admit at least three iterated extensions are diagonally represented. By [4, Theorem 3.2] the extension $\overline{\mathcal{S}}_\beta$ of a diagonally represented DHO $\mathcal{S}_\beta$ is isomorphic to $\mathcal{S}_{\widetilde{\beta}}$, with

$$(u, x)\widetilde{\beta}(v, e) = (vx + ue + (vu)z, x\beta(e)), \quad (u, x), (v, e) \in \overline{X} \tag{1}$$

For this subsection we will use $\mathcal{S}_{\widetilde{\beta}}$ as extension of $\mathcal{S}_\beta$.

Notation. For some l-dimensional $\mathbb{F}_2$-space W with a fixed basis $\{f_1, \ldots, f_l\}$, denote by $\wedge^2(W)$ the second component of the exterior algebra over W, i.e. the $\binom{l}{2}$-dimensional space with basis $\{f_i \wedge f_j \mid 1 \leq i < j \leq l\}$. Let $u = \sum_i u_i f_i, v = \sum_i v_i f_i$. Define

$$\begin{array}{rll} \cdot : & W \times W \to \mathbb{F}_2, & u \cdot v = \sum_{i=1}^{l} u_i v_i, \\ \wedge : & W \times W \to \wedge^2(W), & u \wedge v = \sum_{1 \leq i < j \leq l} (v_i u_j + v_j u_i) f_i \wedge f_j \\ * : & W \times W \to W, & u * v = \sum_{i=1}^{l} u_i v_i f_i \end{array}$$

Observe that $u * u = u$ holds.

Let $V = V^k$ be a k-dimensional $\mathbb{F}_2$-space with basis $\{e_1, \ldots, e_k\}$. Furthermore, let $\{b_1, \ldots, b_n\}$ be a basis of the $\mathbb{F}_2$-space X. Set $X^k = V^k \oplus X$, and define $\beta^k : X^k \to \mathrm{Hom}(X^k, \wedge^2(X^k) \oplus Y)$ by

$$(u, x)\beta^k(v, e) = (u \wedge v + v \wedge x + u \wedge e + (u * v) \wedge z, x\beta(e)). \tag{2}$$

Note that $\wedge^2(V \oplus X)$ decomposes as $\wedge^2(V \oplus X) = \wedge^2(V) \oplus (V \wedge X) \oplus \wedge^2(X)$, where $V \wedge X$ denotes the space with basis $\{e_i \wedge b_j \mid 1 \leq i \leq k, 1 \leq j \leq n\}$. Set $Y^k = \wedge^2(V) \oplus (V \wedge X) \oplus Y \subseteq \wedge^2(X^k) \oplus Y$.

Lemma 6.12. *Let $k \geq 0$ and $\beta : X \to \mathrm{Hom}(X, Y)$ define a DHO $\mathcal{S}_\beta$ that is symmetric and diagonally represented by $z \in X$. Then $\mathcal{S}_{\beta^k}$ is isomorphic to the k times iterated extension of $\mathcal{S}_\beta$. Moreover β^k is symmetric and diagonally represented by $(0, z) \in X^k$ and $X^k \oplus Y^k$ is the ambient space of $\mathcal{S}_{\beta^k}$.*

Proof. By definition (Equation (2)) β^k is symmetric and a direct verification shows that it is diagonally represented by $(0, z)$. Moreover it is obvious from the definition that $L/Y^k = 0$, where L is the space generated by the images of $\beta^k(v, e), (v, e) \in X^k$. Thus the ambient space of $\mathcal{S}_{\beta^k}$ is a subspace of $X^k \oplus Y^k$. The claim about the ambient space follows by dimensional reasons from Theorem 2.1, as soon as the main claim is proven.

For $k = 0$, $\wedge^2(V^0)$ and $V^0 \wedge X$ are 0-dimensional, thus $\mathcal{S}_{\beta^0}$ is isomorphic to $\mathcal{S}_\beta$. Let $k > 0$; we will show that $\mathcal{S}_{\beta^k}$ is the extension of $\mathcal{S}_{\beta^{k-1}}$.

Set $\overline{X}^{k-1} = \mathbb{F}_2 \times X^{k-1}$ and $\overline{Y}^{k-1} = X^{k-1} \times Y^{k-1}$. We define $\pi : \overline{X}^{k-1} \oplus \overline{Y}^{k-1} \to X^k \oplus Y^k$ sending $\overline{X}^{k-1}$ onto X^k and $\overline{Y}^{k-1}$ onto Y^k as follows.

$$\overline{X}^{k-1} \ni (a, \overline{x}) \mapsto (\overline{x} + ae_k) \in X^k, \quad \overline{Y}^{k-1} \ni (\overline{x}, \overline{y}) \mapsto (\overline{y} + \overline{x} \wedge e_k) \in Y^k,$$

(with $a \in \mathbb{F}_2, \overline{x} \in X^{k-1}$ and $\overline{y} \in Y^{k-1}$). Let $\mathcal{S}_\gamma$ be the extension of $\mathcal{S}_{\beta^{k-1}}$. Using u_k, v_k instead of u and v, Equation (1) gives that

$$(u_k, \overline{u}, x)\gamma(v_k, \overline{v}, e) = (v_k(\overline{u}, x) + u_k(\overline{v}, e) + (v_k u_k)(0, z), (\overline{u}, x)\beta^{k-1}(\overline{v}, e)) \in \overline{Y}^{k-1}.$$

We have

$$v_k(\overline{u}, x) + u_k(\overline{v}, e) + (v_k u_k)(0, z) = (v_k\overline{u} + u_k\overline{v}, v_k x + u_k e + (v_k u_k)z)$$

and

$$(\overline{u}, x)\beta^{k-1}(\overline{v}, e) = (\overline{u} \wedge \overline{v} + \overline{v} \wedge x + \overline{u} \wedge e + (\overline{u} * \overline{v}) \wedge z, x\beta(e)).$$

We apply π to $(u_k, \overline{u}, x)\gamma(v_k, \overline{v}, e)$ and obtain

$$((v_k\overline{u} + u_k\overline{v}) \wedge e_k + \overline{u} \wedge \overline{v} + (v_k x + u_k e) \wedge e_k + \overline{v} \wedge x + \overline{u} \wedge e + ((\overline{u} + u_k e_k) * (\overline{v} + v_k e_k)) \wedge z, x\beta(e)).$$

But this is $(\overline{u} + u_k e_k, x)\beta^k(\overline{v} + v_k e_k, e)$.

□

Let $\mathcal{S} = \{S_{(v,e)} \mid (v, e) \in X^k\}$, with $S_{(v,e)} = \{S_{(v,e)}(u, x) \mid (u, x) \in X^k\}$, $S_{(v,e)}(u, x) = (u, x, (u, x)\beta^k(v, e))$, be the k times iterated extension of $\mathcal{S}_\beta$.

Notation. For an arbitrary, but fixed $t \in V^*$ define the partition

$$\mathcal{S}^t_a = \{S_{(v,e)} \mid (v, e) \in X^k, v \cdot t = a\}, \quad a \in \mathbb{F}_2,$$

of $\mathcal{S}$. Let $t^\perp = \{u \in V \mid u \cdot t = 0\}$. For an arbitrary, but fixed $s \in V \setminus t^\perp$ let $^- : V \to t^\perp$, defined by $\bar{w} = w + (w \cdot t)s$, be the projection onto $t^\perp$ in direction s. For $(w, f) \in X^k$ let

$$n^t_{w,f} = \mathbf{1} + \begin{pmatrix} A^t_{w,f} & (w \cdot t)B^t_{w,f} \\ & D^t_{w,f} \end{pmatrix} \in \mathrm{Hom}(X^k \oplus Y^k, X^k \oplus Y^k), \text{ with}$$

$$\begin{aligned}
A^t_{w,f} &= \begin{pmatrix} \cdot t\bar{w} & \cdot tf \\ \mathbf{0} & \mathbf{0} \end{pmatrix} \in \mathrm{Hom}(X^k, X^k) \\
B^t_{w,f} &= \begin{pmatrix} \wedge\bar{w} & \wedge f + (*\bar{w}) \wedge z + (\cdot t)\bar{w} \wedge z & (\cdot t)z\beta(f) \\ \mathbf{0} & \wedge\bar{w} & \beta(f) \end{pmatrix} \in \mathrm{Hom}(X^k, Y^k) \\
D^t_{w,f} &= \begin{pmatrix} (\pi_{t\wedge} \wedge \bar{w}) & \pi_{t\wedge} \wedge f + \pi_{t\wedge} * \bar{w} \wedge z + (\cdot\Lambda(t))\bar{w} \wedge z & (\cdot\Lambda(t))z\beta(f) \\ \mathbf{0} & \pi_{t\wedge} \wedge \bar{w} & \pi_{t\wedge}\beta(f) \\ \mathbf{0} & \mathbf{0} & \mathbf{0} \end{pmatrix} \in \mathrm{Hom}(Y^k, Y^k)
\end{aligned}$$

with respect to the decomposition $X^k = V \oplus X$, $Y^k = \wedge^2(V) \oplus (V \wedge X) \oplus Y$ and where

$$\begin{array}{rll} \Lambda: & V \to \wedge^2(V), & v \mapsto \sum_{i<j} v_i v_j (e_i \wedge e_j), \\ \pi_{t\wedge}: & \wedge^2(X^k) \to X^k, & (v \wedge u) \mapsto (v \cdot t)u + (u \cdot t)v \\ \wedge w: & X^k \to \wedge^2(X^k), & v \mapsto v \wedge w, \\ \cdot t: & V \to \mathbb{F}_2, & v \mapsto v \cdot t \\ *w: & V \to V, & v \mapsto v * w, \end{array}$$

The last three maps should be understood as applications of the corresponding bilinear map on the "omitted" argument. The proofs of the subsequent lemmas on the automorphisms are obtained by straightforward standard verifications and therefore are omitted. The following useful identities are also straightforward to prove:

$$\begin{array}{rcl} u \wedge v & = & \Lambda(u) + \Lambda(u+v) + \Lambda(v), \\ u * v & = & (u \cdot v)u + \Lambda(u)\pi_{v\wedge}, \\ (v \cdot t)(u \cdot t) & = & (u * v) \cdot t + (u \wedge v) \cdot \Lambda(t), \end{array}$$

Set $N_a^t = \{n_{w,f}^t \mid w \cdot t = a, f \in X\}$, $N^t = \langle N_0^t, N_1^t \rangle$. Note that N_a^t does not depend on the choice of s in the definition of $\bar{w}$ (choosing $\tilde{s} \in V \setminus t^\perp$ instead would lead to the maps $n_{w+w\cdot t(s+\tilde{s}),f}^t$, a permutation on the elements of N_a^t).

Lemma 6.13. *The group N_a^t fixes $\mathcal{S}_a^t$ elementwise and acts regularly on $\mathcal{S}_{a+1}^t$. More precisely,*

$$S_{(v,e)}(u,x)n_{w,f}^t = S_{(v,e)+((v+w)\cdot t)(\bar{w},f)}((u,x) + (u \cdot t)(\bar{w}, f)).$$

Corollary 6.14. *Let $t \in V^*$. Then $N^t = N_0^t \times N_1^t$ is an extension group of $\mathcal{S}$, the k times iterated extension of $\mathcal{S}_\beta$, whose orbits on $\mathcal{S}$ are $\mathcal{S}_0^t$, $\mathcal{S}_1^t$. The k times iterated extension of $\mathcal{S}_\beta$ has $2^k - 1$ extension groups.*

Notation. Let $\alpha \in G = GL(V)$ and $(a_{i,j})$, the matrix of the map α with respect to the basis e_i, i.e. $u\alpha = \sum_{i,j} u_i a_{i,j} e_j$. Denote by a_i the i-th row of $(a_{i,j})$. Define

$$\mu_\alpha = \begin{pmatrix} A_\alpha & \\ & F_\alpha \end{pmatrix}, \quad A_\alpha = \begin{pmatrix} \alpha & \\ & \mathbf{1} \end{pmatrix}, \quad F_\alpha = \begin{pmatrix} \alpha_\wedge & \rho_\alpha \wedge z & \\ & \alpha_\wedge & \\ & & \mathbf{1} \end{pmatrix},$$

where $\alpha_\wedge = \wedge^2(\alpha \oplus 1_X) \in GL(\wedge^2(V \oplus X))$, i.e.

$$\begin{array}{rlll} \alpha_\wedge: & \wedge^2(V) \to \wedge^2(V), & v \wedge u \mapsto v\alpha \wedge u\alpha, & \\ \alpha_\wedge: & V \wedge X \to V \wedge X, & v \wedge x \mapsto v\alpha \wedge x, & \text{and} \\ \rho_\alpha: & \wedge^2(V) \to V, & e_i \wedge e_j \mapsto a_i * a_j. & \end{array}$$

A comment about the map $\rho: G \to \mathrm{Hom}(V, \wedge^2(V))$ given by $\alpha \mapsto \rho_\alpha$: It is well known, that the $\mathbb{F}_2 G$-module $S^2(V)$ is indecomposable, has the unique submodule $\wedge^2(V)$, and that $S^2(V)/\wedge^2(V)$ is isomorphic, as an $\mathbb{F}_2G$-module, to the natural module V. Hence ρ_α can be interpreted as an element of the extension product $\mathrm{Ext}^1(V, \wedge^2(V))$ and

$$G \ni \alpha \mapsto \begin{pmatrix} \alpha & \rho_\alpha \\ 0 & \wedge^2(\alpha) \end{pmatrix}$$

stands for the representation of G on $S^2(V)$.

Lemma 6.15. *Let $\alpha \in G$. Then*

$$S_{(v,e)}(u, x)\mu_\alpha = S_{(v\alpha,e)}(u\alpha, x).$$

Proof. A straightforward verification. Observe that $u\alpha * v\alpha = (u * v)\alpha + (u \wedge v)\rho_\alpha$. □

As the hyperplanes $t^\perp$ of V form one orbit under G, the partitions $(\mathcal{S}_0^t, \mathcal{S}_1^t)$ and thus the extension groups form one orbit under the automorphisms $\{\mu_\alpha \mid \alpha \in G\}$.

We now turn to the APN case and continue to use the notation introduced in the DHO-section. Let $\mathbf{f}(V) = (f_v \mid v \in V)$ be a family of (APN) functions $f_v : X \to Y$ (indexed with $v \in V$). Define

$$F_{\mathbf{f}(V)} : X^k \to Y^k, \quad (v, x) \mapsto (\Lambda(v), v \wedge x, f_v(x)). \tag{3}$$

Observe that for $k = 0$ we have $\mathbf{f}(V^0) = (f_0)$, $\wedge^2(V^0)$ and $V^0 \wedge X$ are 0-dimensional and hence $F_{\mathbf{f}(V^0)}$ is f_0 itself.

Lemma 6.16. *Let $k > 0$. Then $F_{\mathbf{f}(V)}$ is the k-fold extension with respect to the functions in the family $\mathbf{f}(V)$. More precisely: Let $\overline{V} \subset V$ be the space generated by $e_1, \ldots, e_{k-1}$ and $\tilde{f}_v = f_{v+e_k}$. Then $F_{\mathbf{f}(V)}$ is isomorphic to the extension of the functions $F_{\mathbf{f}(\overline{V})}$ and $F_{\tilde{\mathbf{f}}(\overline{V})}$.*

Proof. The extension of f_0, f_1 is defined to be $F_{f_0,f_1}(v, x) = (vx, vf_1(x) + (v + 1)f_0(x))$, $(v, x) \in \mathbb{F}_2 \oplus X$. In our situation we put $f_0 = F_{\mathbf{f}(\overline{V})}$, $f_1 = F_{\tilde{\mathbf{f}}(\overline{V})}$ and we have to adapt the notation by substituting x by $(\bar{v}, x), \in X^{k-1} = \overline{V} \oplus X$ and $v \in \mathbb{F}_2$ by v_k. With this the extension is $F = F_{f_0,f_1} : \mathbb{F}_2 \times X^{k-1} \to X^{k-1} \times Y^{k-1}$, defined by

$$F(v_k, \bar{v}, x) = (v_k(\bar{v}, x), v_k f_1(\bar{v}, x) + (1 + v_k)f_0(\bar{v}, x))$$

Then $f_0(\bar{v}, x) = (\Lambda(\bar{v}), \bar{v} \wedge x, f_{\bar{v}}(x))$, $f_1(\bar{v}, x) = (\Lambda(\bar{v}), \bar{v} \wedge x, f_{\bar{v}+e_k}(x))$, and so

$$F(v_k, \bar{v}, x) = (v_k(\bar{v}, x), \Lambda(\bar{v}), \bar{v} \wedge x, v_k f_{\bar{v}+e_k}(x) + (1 + v_k)f_{\bar{v}}(x))$$

Apply the projection $\pi : (\mathbb{F}_2 \times X^{k-1}) \oplus (X^{k-1} \times Y^{k-1}) \to X^k \oplus Y^k$ as defined in the proof of Lemma 6.12. We have

$$\begin{aligned} F(\bar{v} + v_k e_k, x) &= (\Lambda(\bar{v}) + v_k \bar{v} \wedge e_k, \bar{v} \wedge x + v_k e_k \wedge x, v_k f_{\bar{v}+e_k}(x) + (1 + v_k)f_{\bar{v}}(x)) \\ &= (\Lambda(v), v \wedge x, f_v(x)) = F_{\mathbf{f}(V)}(v, x), \text{ with } v = v_k e_k + \bar{v}. \end{aligned}$$

□

We now turn to Extensions $F_{\mathbf{f}(V)}$ which are quadratic APN functions. By Proposition 2.6, $F_{\mathbf{f}(V)}$ is equivalent to a k-fold extension where the f_v, for $v \in V$, are all equal to the a quadratic APN function f. From now on we restrict ourselves to this case.

Notation. Denote the graph of $F_{\mathbf{f}(V)}$ by $\mathcal{S} = \mathcal{S}_{F_{\mathbf{f}(V)}} = \{S(v,x) \mid (v,x) \in X^k\}$ where,

$$S(v,x) = (v, x, F_{\mathbf{f}(V)}(v,x)) = (v, x, \Lambda(v), v \wedge x, f(x)).$$

Let $\alpha \in G$, and let $L(\alpha) : V \to V \wedge V$ be the function $u \mapsto \sum_i u_i(\Lambda(a_i))$, with a_i the i-th column of the matrix of α with respect to the basis $e_1, \dots e_k$. Define

$$\mu_\alpha = \begin{pmatrix} \alpha & & L(\alpha) & & \\ & \mathbf{1} & & & \\ & & \alpha_\wedge & & \\ & & & \alpha_\wedge & \\ & & & & \mathbf{1} \end{pmatrix} \in GL(X^k \oplus Y^k).$$

Lemma 6.17. *We have*

$$S(v,x)\mu_\alpha = S(v\alpha, x), \quad \alpha \in G, (v,x) \in X^k$$

Proof. A straightforward verification. Observe that $\Lambda(u)\alpha_\wedge = \Lambda(u\alpha) + uL(\alpha)$. □

Notation. We define

$$\eta_w^t = \mathbf{1} + \begin{pmatrix} A & B \\ & D \end{pmatrix}, \quad \overline{\eta}_w^t = \eta_w^t + (w \cdot t)(\bar{w}, 0, \Lambda(\bar{w}), 0, 0),$$

where

$$\begin{aligned} A &= \begin{pmatrix} \cdot t\bar{w} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}, \\ B &= \begin{pmatrix} \wedge((w \cdot t)\bar{w}) + (\cdot t)\Lambda(\bar{w}) + (*t) \wedge \bar{w} & 0 & 0 \\ 0 & \wedge((w \cdot t)\bar{w}) & 0 \end{pmatrix}, \\ D &= \begin{pmatrix} (\pi_{t\wedge} \wedge \bar{w}) & & \\ & (\pi_{t\wedge} \wedge \bar{w}) & \\ & & \mathbf{0} \end{pmatrix}. \end{aligned}$$

Lemma 6.18. *We have*

$$S(v,x)\overline{\eta}_w^t = S(v + (v+w) \cdot t\, \bar{w}, x), \quad t \in V^*$$

Notation. We define

$$\delta_{w,y}^t = \begin{pmatrix} 1 & \cdot ty & & *t \wedge y + \wedge(w \cdot t)y & \cdot tf(y) \\ & 1 & & & \beta(w \cdot t\, y) \\ & & 1 & \pi_{t\wedge} \wedge y & \\ & & & 1 & \pi_{t\wedge}\beta(y) \\ & & & & 1 \end{pmatrix},$$

and set

$$\overline{\delta}^t_{w,y} = \delta^t_{w,y} + (w \cdot t)(0, y, 0, 0, f(y)).$$

Lemma 6.19. *We have*

$$S(v, x)\overline{\delta}^t_{w,y} = S(v, x + (v + w) \cdot t\, y), \quad t \in V^*$$

Hence

$$\overline{\nu}^t_{w,y} = \overline{\delta}^t_{w,y}\overline{\eta}^t_w : S(v, x) \mapsto S(v + (v + w) \cdot t\, \bar{w}, x + (v + w) \cdot t\, y), \quad (w, y) \in X^k,$$

and thus we have the extension groups.

Corollary 6.20. *Let $t \in V^*$ $a \in \mathbb{F}_2$, $N^t_a = \{\overline{\nu}^t_{w,y} \mid w \cdot t = a, w \in V, y \in X\}$ and $\mathcal{S}^t_a = \{S(v, x) \mid v \cdot t = a, v \in V, x \in X\}$. The group N^t_a stabilizes $\mathcal{S}^t_a$ element wise and acts regularly on $\mathcal{S}^t_{a+1}$.*

As in the DHO case, the $2^k - 1$ extensions groups are conjugated by the μ_α.

6.4 Small DHOs and further examples

We now give examples with more than one extension group. We start with a discussion of the DHOs of small rank, which naturally lead to the Huybrechts DHOs and the Buratti-Del Fra DHOs, being examples of DHOs with more than one extension group. We end the subsection with examples of APN functions with this property.

We modify the definition of a DHO $\mathcal{S}$ of Section 2 by defining $\mathcal{S}$ as a family, instead of a set, of subspaces. For $n \geq 2$ both definitions coincide due to the DHO condition that any two members of a DHO intersect 1-dimensionally. With that the (uniquely determined) DHO of rank 0 is the null-space and the DHO of rank 1 consists of two copies of $\mathbb{F}_2$. The DHOs of rank 2 and 3 are known (see e.g. [5, Appendix]).

The DHO of rank 0 can be realized as $\mathcal{S}_\beta$, for β the zero-map. It is diagonally represented with respect to zero. Applying the extension (still in the form of Equation (1)) leads us to the DHO $\mathcal{S}_{\tilde{\beta}}$ of rank 1, with $\tilde{\beta}$ the zero-map. The DHO of rank 1 has the trivial group as extension group.

Further extensions of the DHO of rank 1, with respect to $z = 0$, lead to the standard form of the Huybrechts DHO $\mathcal{S}_\beta$ with $x\beta(e) = x \wedge e$. Thus the Huybrechts DHO of rank k can be seen as the k-th extension of the DHO of rank 0, i.e. the null-space. This also nicely 'explains' the the $2^k - 1$ extension groups of the Huybrechts DHO.

The DHO of rank 1, $\mathcal{S}_{\tilde{\beta}}$ ($\tilde{\beta}(e) = 0$), is also diagonally represented with respect to $z = 1$. The DHO of rank 2 is unique, has a unique elementary abelian translation group and only one class, of length 3, of extension groups. Thus the extensions of the DHO of rank 1, with respect to $z = 1$, lead to an isomorphic representation with another 'β'.

Denote the twofold extensions of the DHO of rank 1, with respect to z as $\mathcal{S}_{\beta_z}$, $z \in \{0,1\}$. Again, there is only one DHO of rank 3 in $\mathbb{F}_2^6$ with a translation group, thus $\mathcal{S}_{\beta_0}$ and $\mathcal{S}_{\beta_1}$ are isomorphic. However the standard translation groups of these two representations differ. The standard translation group of $\mathcal{S}_{\beta_0}$ is normal and the standard translation group of $\mathcal{S}_{\beta_1}$ is in a class of length 7 in the full automorphism group (these are the two only classes of translation groups for this DHO, see [5, Appendix]). The DHO has only one class, of length 7, of extension groups (as it should being the Huybrechts DHO).

There are two further DHO of rank 3; both have no extension groups.

For each $k > 2$, the k-fold extension of the DHO of rank 1, with respect to $z = 1$, $\mathcal{S}_{\beta_1}^k$, is the Buratti Del-Fra DHO (which has $2^k - 1$ extension groups). An easy way to see this identification, is to observe that $\mathcal{S}_{\beta_1}^3$ is identical to a coordinatized form of the Buratti Del-Fra DHO of rank 4 given in [4, Example 3.6.]. Then use the fact that the Buratti Del-Fra DHO of higher rank can be obtained as an iterated extension of this one (see again [4]).

Set $X = \mathbb{F}_2^n$ with canonical basis $B = \{e_1, \dots, e_n\}$ and $Y = \wedge^2(X)$. The Huybrechts map $\Lambda : X \to Y$, $\Lambda(x) = \sum_{i<j} x_i x_j e_i \wedge e_j$, as already defined in Section 6.3, is a quadratic APN function. Analogously to the Huybrechts DHO, it is the k-fold extension of the zero-function (of rank 0) and thus has $2^k - 1$ extension groups.

6.5 Non-quadratic extensions of APN functions

We now discuss non-quadratic extensions of quadratic APN functions that have the property that N is not normal in the automorphism group.

Example 6.21. Set $f_0 = \Lambda$, the Huybrechts map, $e_{ij} = e_i \wedge e_j$ and let $n \geq 4$. We consider extensions $F = F_{f_0,f_1}$, where $f_1(x) = f_0(x)\alpha$, $\alpha \in \mathrm{GL}(Y)$.

Claim: The extension F is not quadratic if α is a transvection in $\mathrm{GL}(Y)$. In particular F is not quadratic in the following examples (a) and (b).

Assume the converse. By assertion (b) of Theorem 4.4 there exists $\phi \in \mathrm{Autop}(f_0)$ of the form $\phi = \begin{pmatrix} \lambda & \gamma \\ & \alpha \end{pmatrix}$. On the other hand, by Theorem [5, Thm. 3.10] $\mathrm{Autop}(f_0) \simeq \mathrm{Autop}(\mathcal{H}_n)$, where $\mathcal{H}_n$ is the Huybrechts DHO of rank n, which is the alternating DHO associated with f_0 in the sense of Theorem [5, Thm. 2.4]. By [9] $\mathrm{Aut}(\mathcal{H}_n) \simeq 2^n \cdot \mathrm{SL}(n,2)$, which implies that $\mathrm{Autop}(f_0) \simeq \mathrm{SL}(n,2)$. Note that ϕ acts on $Y = C_U(T)$, T the translation group, as a transvection α. But, as an $\mathrm{SL}(n,2)$-module, Y is isomorphic to $\wedge^2(X)$, with X the natural $\mathrm{SL}(n,2)$-module. Since $n > 3$, a transvection in $\mathrm{SL}(n,2)$ does not induce a transvection on $Y \simeq \wedge^2(X)$, a contradiction. This shows the claim.

(a) Define the linear map $\alpha \in \mathrm{GL}(Y)$ by $(\sum_{i<j} z_{ij} e_{ij})\alpha = \sum_{i<j} z_{ij} e_{ij} + z_{2,n-1} e_{n-1,n}$. Define $f_1 : X \to Y$ by $f_1(x) = f_0(x)\alpha$ and denote by F the

extension of f_0 and f_1. A typical element from $\mathcal{S}_0$ has (in coordinates) the form

$$(0 \mid x \mid 0 \mid x_1x_2, x_1x_3, \ldots, x_1x_n, \ldots, x_{n-1}x_n)$$

and a typical element from $\mathcal{S}_1$ has (in coordinates) the form

$$(1 \mid 0 \mid y \mid y_1y_2, \ldots, y_1y_n, \ldots, y_{n-2}y_n, y_2y_n + y_{n-1}y_n).$$

Define $\tau \in \mathrm{GL}(\overline{U})$ by $(a \mid x \mid y \mid z)\tau = (a' \mid x' \mid y' \mid z')$, with $a' = a + x_2 + y_2$, $x' = (x_1 + z_{12}, y_2, x_3 + z_{23}, \ldots, x_n + z_{2,n})$, $y' = (y_1 + z_{12}, x_2, y_3 + z_{23}, \ldots, y_n + z_{2,n})$, and $z' = (z_{12}, \ldots, z_{n-2,n}, z_{2,n} + z_{n-1,n})$.

Claim: The map τ is an automorphism that does not fix $\mathcal{S}_0$ or $\mathcal{S}_1$. In particular G has more than one extension group.

Let $v = (a \mid x \mid y \mid z)$ be an element in $\mathcal{S}$. Consider for instance the case $a = y_2 = 1$. Then v lies in $\mathcal{S}_1$ (i.e. $x = 0$) and it has the form

$$v = (1 \mid 0 \mid y \mid y_1y_2, \ldots, y_{n-2}y_n, y_2y_n + y_{n-1}y_n).$$

Then

$$\begin{aligned} v\tau &= (0 \mid y, \mid 0 \mid y_1y_2, \ldots, y_{n-2}y_n, y_2y_n + (y_2y_n + y_{n-1}y_n)) \\ &= (0 \mid y, \mid 0 \mid y_1y_2, \ldots, y_{n-2}y_n, y_{n-1}y_n) \end{aligned}$$

lies in $\mathcal{S}_0$. For $a = 1$ and $y_2 = 0$ again v lies in $\mathcal{S}_1$ (i.e. $x = 0$) and it has the form

$$v = (1 \mid 0 \mid y \mid y_1y_2, \ldots, y_{n-2}y_n, y_2y_n + y_{n-1}y_n) = (1 \mid 0 \mid y \mid y_1y_2, \ldots, y_{n-2}y_n, y_{n-1}y_n).$$

We compute $v\tau = v$. Similar computations for $v = (a \mid x \mid y \mid z) \in \mathcal{S}$ and (a, x_2) equal to $(0,0)$ or $(0,1)$ show that $v \in \mathcal{S}_0$ and $v\tau \in \mathcal{S}$. The claim follows.

(b) Define the linear map $\alpha \in \mathrm{GL}(Y)$ by $(\sum_{i<j} z_{ij}e_{ij})\alpha = \sum_{i<j} z_{ij}e_{ij} + z_{1,2}e_{n-1,n}$. Define $f_1 : X \to Y$ by $f_1(x) = f_0(x)\alpha$ and denote by F the extension of f_0 and f_1. A typical element from $\mathcal{S}_0$ has (in coordinates) the form

$$(0 \mid x \mid 0 \mid x_1x_2, x_1x_3, \ldots, x_1x_n, \ldots, x_{n-1}x_n)$$

and a typical element from $\mathcal{S}_1$ has (in coordinates) the form

$$(1 \mid 0 \mid y \mid y_1y_2, \ldots, y_1y_n, \ldots, y_{n-2}y_n, y_1y_2 + y_{n-1}y_n).$$

Define $\tau_r \in \mathrm{GL}(\overline{U})$, $r = 1, 2$, by

$$(a \mid x \mid y \mid z)\tau_r = (a(r) \mid x(r) \mid y(r) \mid z(r)),$$

with (using the convention $z_{ij} = z_{ji}$)

1. $a(r) = a + x_r + y_r$,

2. $x(r)_r = y_r$ and $x(r)_i = x_i + z_{ir}$ for $i \neq r$,

3. $y(r)_r = x_r$ and $y(r)_i = y_i + z_{ir}$ for $i \neq r$,

4. $z(r) = (z_{12}, \ldots, z_{1n}, z_{23}, \ldots, z_{n-2,n}, z_{n-1,n} + z_{12})$.

Claim: The maps τ_r's are automorphisms and $|\mathcal{S}_0 \cap \mathcal{S}_0\tau_1 \cap \mathcal{S}_0\tau_2| = 2^{n-2}$. In particular F admits more than three extension groups.

We consider first the case $\tau = \tau_1$. Let $v = (a \mid x \mid y \mid z)$ be an element in $\mathcal{S}$.

Case $a = 0$ (i.e. $v \in \mathcal{S}_0$, $y = 0$). Then

$$v\tau = (x_1 \mid 0, x_2{+}x_1x_2, \ldots, x_n{+}x_1x_n \mid 0, x_1x_2, \ldots, x_1x_n \mid x_1x_2, \ldots, x_{n-2}x_n, x_1x_2{+}x_{n-1}x_n).$$

If $x_1 = 0$ then $v = v\tau$ and if $x_1 = 1$ then

$$v\tau = (1 \mid 0 \mid 0, x_2, \ldots, x_n \mid x_1x_2, \ldots, x_{n-2}x_n, x_1x_2 + x_{n-1}x_n) \in \mathcal{S}_1.$$

In particular $\mathcal{S}_0 \cap \mathcal{S}_0\tau_1$ is the set of elements in $\mathcal{S}_0$ with $x_1 = 0$.

Case $a = 1$ (i.e. $v \in \mathcal{S}_1$, $x = 0$). Then

$$v\tau = (1{+}y_1 \mid y_1, y_1y_2, \ldots, y_1y_n \mid 0, y_2{+}y_1y_2, \ldots, y_n{+}y_1y_n \mid y_1y_2, \ldots, (y_1y_2{+}y_{n-1}y_n){+}y_1y_2).$$

If $y_1 = 0$, then $v = v\tau$ and if $y_1 = 1$, then

$$v\tau = (0 \mid 1, y_2, \ldots, y_n \mid 0 \mid y_1y_2, \ldots, y_{n-1}y_n) \in \mathcal{S}_0.$$

Thus τ_1 is an automorphism.

By symmetry τ_2 is an automorphism too and $\mathcal{S}_0 \cap \mathcal{S}_0\tau_2$ is the set of elements in $\mathcal{S}_0$ with $x_2 = 0$. The claim follows.

7 Automorphisms

Let G be the automorphism group of a DHO or the linear part of the automorphism group of an APN function. We assume that the conjugacy class $\mathcal{C}$ of extension groups in G is not empty. We will determine the group $H = \langle \mathcal{C} \rangle$ generated by extension groups. It turns out that the structure of H only depends on the size of $\mathcal{C}$. It will be shown that this group is the extension of a 2-group of nilpotency class ≤ 2 by $\mathrm{SL}(k+1, 2)$, $k > 0$. The proof is purely group theoretic, i.e. it does not depend on the action of the extension groups on the underlying space. As a consequence we get a factorization $G = HN_G(N)$, $N \in \mathcal{C}$, of the automorphism group. We assume again that X and Y are $\mathbb{F}_2$-spaces with $\dim X = n$ and $\dim Y = m$. We always assume

$$\dim X = n \geq 4.$$

Theorem 7.1. *Let $\beta : X \to \mathrm{Hom}(X, Y)$ be a monomorphism that defines a bilinear DHO $\mathcal{S}_\beta$ that is ambient in $X \oplus Y$. Set $G = \mathrm{Aut}(\mathcal{S})$, $\mathcal{S} = \overline{\mathcal{S}}_\beta$. Let $\mathcal{C}$ be the set of extension groups, $G^* = \langle \mathcal{C} \rangle$ and $N \in \mathcal{C}$. Then $G = G^*N_G(N)$, $N_G(N) = NL$, where L is given in Section 2. Moreover one of the following holds:*

(a) β and β^o are not isotopic, $\mathcal{C} = \{N\}$, G is not transitive on $\mathcal{S}$, and G is equal to $N_G(N)$.

(b) β and β^o are isotopic, $\mathcal{C} = \{N\}$, G is transitive on $\mathcal{S}$, and $G = N_G(N)$.

(c) β and β^o are isotopic, $|\mathcal{C}| > 1$, G is transitive on $\mathcal{S}$. There exists k with $k \in \{1, \ldots, n\}$ such that $G^*/P \simeq \mathrm{SL}(k+1, 2)$, where $P = O_2(G^*)$. Moreover $Q = Z(G^*)$ is elementary abelian of order 2^{n-k}, $[P, P] \leq Q$, P/Q has order $2^{(k+1)(n-k+1)}$, and all composition factors of G^* on P/Q are natural $\mathrm{SL}(k+1, 2)$*-modules.*

Remark 7.2. If G contains a translation group T, we are in case (b) or (c). Then $|T : T \cap N| = 2$ and $\tau \in T - (T \cap N)$ interchanges the two N-orbits. If $|\mathcal{C}| > 3$, then by Corollary 6.10 $\mathcal{S}$ is a symmetric, diagonally represented DHO, in particular G contains translation groups.

Theorem 7.3. *Let $f_i : X \to Y$ be quadratic APN functions for $i = 0, 1$, which are ambient in $X \oplus Y$. Set $F = F_{f_0,f_1}$, $\overline{G} = \mathrm{Aut}(F)$ and $G = \mathbf{A}(F)$. Let $\mathcal{C}$ be the set of extension groups, $G^* = \langle \mathcal{C} \rangle$ and $N \in \mathcal{C}$. Then $G = G^* N_G(N)$, $N_G(N) = NL$, where L is given in Section 2. Moreover one of the following holds:*

(a) f_0 and f_1 are not isotopically linked, $\mathcal{C} = \{N\}$, $\overline{G}$ is not transitive on $\mathcal{S} = \mathcal{S}_F$, and $G = N_G(N)$.

(b) f_0 and f_1 are isotopically linked, $\mathcal{C} = \{N\}$, $\overline{G}$ is transitive on $\mathcal{S}$, and G is equal to $N_G(N)$.

(c) f_0 and f_1 are isotopically linked, $|\mathcal{C}| > 1$, $\overline{G}$ is transitive on $\mathcal{S}$. There exists k with $k \in \{1, \ldots, n\}$ such that $G^*/P \simeq \mathrm{SL}(k+1, 2)$, where $P = O_2(G^*)$. Moreover $Q = Z(G^*)$ is elementary abelian of order 2^{n-k}, $[P, P] \leq Q$, P/Q has order $2^{(k+1)(n-k+1)}$, and all composition factors of G^* on P/Q are natural $\mathrm{SL}(k+1, 2)$*-modules.*

Remark 7.4. If G contains a translation group T, we are in case (b) or (c). Then $|T : T \cap N| = 2$ and $\overline{\tau} \in \overline{T} - (\overline{T} \cap \overline{N})$ interchanges the two N-orbits.

We prove the two theorems by a series of lemmas. The symbol $\mathcal{S}$ denotes the extension of a bilinear DHO $\mathcal{S}_\beta$ (which is ambient in its defining space) in the DHO case, while in the APN case this symbol denotes the graph of the extension $F = F_{f_0,f_1}$ of quadratic APN functions f_0 and f_1 (which are both ambient in the *same* defining space). Also $G = \mathrm{Aut}(\mathcal{S})$ in the DHO case, while in the APN case we have $\overline{G} = \mathrm{Aut}(F)$ and $G = \mathbf{A}(F)$ is the linear part of $\overline{G}$.

By Theorem 5.1 $\mathcal{C}$ is at conjugacy class in G^*, i.e.

$$\mathcal{C} = \{N^\gamma \mid \gamma \in G^*\}.$$

Our main task will be to determine the group $\langle \mathcal{C} \rangle$. By our assumptions all results of Sections 3 and 5 are available. The starting point is the case $|\mathcal{C}| = 3$, where

Lemma 5.4 provides the structure of $\langle \mathcal{C} \rangle$. The general case will be obtained by a somewhat tedious induction on $|\mathcal{C}|$, which results in Theorem 7.11.

Again we only work in the DHO case as all arguments can be carried over one to one to the APN case: Namely, we do not need the linear representation of the automorphism group on the vector space U any more, but only use the permutation representation on the set $\mathcal{S}$. The following proposition is part of the folklore on linear groups.

Proposition 7.5. *Let W be a finite dimensional space over $\mathbb{F}_q$ and $G = \mathrm{SL}(W)$. For a subspace U of W let $G_U = \{\sigma \in G \mid \sigma_U = 1,\ \sigma_{W/U} = 1\}$ be the centralizer of the chain $0 \subseteq U \subseteq W$. If H is a hyperplane, then $G_H - \{1\}$ is the set of all transvections that act trivially on H. Let $\mathcal{H}$ be a set of hyperplanes, $D = \bigcap_{H \in \mathcal{H}} H$, $\dim W/D = k$, and set $X = \langle G_H \mid H \in \mathcal{H} \rangle$. Let p be the characteristic of $\mathbb{F}_q$. Then the following hold:*

(a) $X/O_p(X) \simeq \mathrm{SL}(k, q)$.

(b) $O_p(X)$ is an elementary abelian p-group of order $q^{k(n-k)}$ and $O_p(X)$ is generated by the $\sigma \in G_H$, $H \in \mathcal{H}$, with $\sigma_{W/D} = 1$. Moreover $O_p(X)$ is the direct sum of $n-k$ natural $\mathrm{SL}(k, q)$ modules (with $X/O_p(X) \simeq \mathrm{SL}(k, q)$ acting by conjugation).

(c) Let H be any hyperplane containing D. Then for any $K \in \mathcal{H}$ there exists a $\gamma \in X$, such that $H = K\gamma$ and $G_H = G_K^\gamma$.

(d) Let U_1 and U_2 be subspaces of D such that $U_1 \subset U_2$ and $\dim U_2/U_1 = 1$. Let $E_i = \{\sigma \in O_p(X) \mid W(1-\sigma) \subseteq U_i\}$ for $i = 1, 2$. Then E_2/E_1 is a natural $\mathrm{SL}(k, q)$-module.

(e) Let $\sigma \in X$, such that σ normalizes each group G_H, $H \in \mathcal{H}$. Then $\sigma \in O_p(X)$.

Lemma 7.6. *Let $N^\gamma, N^\delta \in \mathcal{C} - \{N\}$, be such that $N^\gamma \neq N^\delta$, but $N^\gamma \cap N$ is equal to $N^\delta \cap N$. Then:*

(a) N, N^γ, N^δ are the elements of $\mathcal{C}$ that lie in $H = \langle N, N^\delta \rangle$.

(b) $N_{N^\gamma}(N) \leq N_{N^\delta}(N)N$.

Proof. By Lemma 5.4 we can assume that $\delta \in H$ has order 3, so that $N^{\delta^2} \leq H$ too. Let $\mathcal{T}_0$ and $\mathcal{T}_1$ be the orbits of N^δ. Then N^{δ^2} has (as we have seen) the orbits $(\mathcal{S}_0 \cap \mathcal{T}_0) \cup (\mathcal{S}_1 \cap \mathcal{T}_1)$ and $(\mathcal{S}_0 \cap \mathcal{T}_1) \cup (\mathcal{S}_1 \cap \mathcal{T}_0)$.

Pick $1 \neq \tau \in N_{N_0^\gamma}(N)$. By assumption τ centralizes the group $N^\delta \cap N$ and therefore this group leaves invariant $\mathcal{U}_0 = \mathrm{Fix}_{\mathcal{S}}(\tau)$ and $\mathcal{U}_1 = \mathcal{S} - \mathcal{U}_0$. So the two sets are the union of the orbits of $N^\delta \cap N$. But as $N^\gamma \neq N^\delta$ we see that $\{\mathcal{U}_0, \mathcal{U}_1\} = \{(\mathcal{S}_0 \cap \mathcal{T}_0) \cup (\mathcal{S}_1 \cap \mathcal{T}_1), (\mathcal{S}_0 \cap \mathcal{T}_1) \cup (\mathcal{S}_1 \cap \mathcal{T}_0)\}$, which shows that N^{δ^2} and N^γ have the same orbits. In particular these groups normalize each other and (a) follows by Theorem 3.6.

By Lemma 5.4 $O_2(H) = N_N(N^\delta)N_{N^\delta}(N)$ and $N_{N^\gamma}(N) \leq O_2(H)$ and (b) follows. □

Lemma 7.7. *Let $N^\delta \in \mathcal{C} - \{N\}$. Set $H = \langle N, N^\delta \rangle$ and let N, N^γ, N^δ be the elements of $\mathcal{C}$ that lie in H. Suppose $\tau \in L_0 N - N$ is conjugate in G to some element in N_0 and let $\tau' \in N_0^\gamma$ induce the same automorphism on N_0 as τ. Then τ lies in N_i^δ or N_i^γ, $i = 0$ or 1.*

Proof. By assumption $\tau\tau' \in C_G(N_0) = N$, say $\tau\tau' = \nu_0\nu_1$, where $\nu_i \in N_i$, $i = 0, 1$. As τ' normalizes the groups N_i's, we have

$$1 = \tau^2 = \nu_0 \nu_0^{\tau'} \nu_1 \nu_1^{\tau'},$$

which implies that τ and τ' centralize ν_0 and ν_1. By Lemma 5.5 (with $\mathcal{T}_0 = \mathrm{Fix}_{\mathcal{S}}(\tau')$, $\mathcal{T}_1 = \mathcal{S} - \mathcal{T}_0$) we have

$$|\mathrm{Fix}_{\mathcal{S}_i}(\tau)| = |\mathcal{S}_i \cap \mathcal{T}_j| = 2^{n-1}$$

for $i, j \in \{0, 1\}$. We have $\mathrm{Fix}_{\mathcal{S}_0}(\tau'\nu_0) = \mathcal{S}_0 \cap \mathcal{T}_0$. If $\nu_1 = 1$, then $\mathrm{Fix}_{\mathcal{S}_0}(\tau) = \mathcal{S}_0 \cap \mathcal{T}_0$.

Now assume that $\nu_1 \neq 1$; then ν_1 fixes or interchanges the sets $\mathcal{S}_0 \cap \mathcal{T}_0$ and $\mathcal{S}_0 \cap \mathcal{T}_1$. If, however, ν_1 interchanges these sets, then $\mathrm{Fix}_{\mathcal{S}_0}(\tau) = \emptyset$, a contradiction. So ν_1 fixes both sets and $\tau = \tau'\nu_0\nu_1$ acts fixed-point-freely on $\mathcal{S}_0 \cap \mathcal{T}_0$. So $\mathrm{Fix}_{\mathcal{S}_0}(\tau) = \mathcal{S}_0 \cap \mathcal{T}_1$ in this case.

Arguing by symmetry, we get that $\mathrm{Fix}_{\mathcal{S}_1}(\tau)$ equals $\mathcal{S}_1 \cap \mathcal{T}_0$ or $\mathcal{S}_1 \cap \mathcal{T}_1$. This implies that the sets $\mathcal{U}_0 = \mathrm{Fix}_{\mathcal{S}}(\tau)$ and $\mathcal{U}_1 = \mathcal{S} - \mathcal{U}_0$ coincide with the orbits of N^γ or N^δ. Thus by Lemma 3.10 τ lies in one of these groups. The proof is complete. □

Lemma 7.8. *Let $\emptyset \neq \mathcal{M} \subseteq \mathcal{C} - \{N\}$. Set $H = \langle N_M(N) \mid M \in \mathcal{M} \rangle N$, $H_0 = H \cap NL_0$, and $\widetilde{N}_0 = \bigcap_{M \in \mathcal{M}} N_{N_0}(M)$. Let $|\widetilde{N}_0| = 2^{n-k}$. Then:*

(a) $|H : H_0| = 2$.

(b) $H_0/N \simeq E \cdot \mathrm{SL}(k, 2)$ and E is elementary abelian of order $2^{k(n-k)}$.

(c) $H/O_2(H) \simeq \mathrm{SL}(k, 2)$ and $O_2(H)/N$ is elementary abelian. Moreover, we have $\bigcap_{M' \in \mathcal{M}} N_M(M') \cap N_M(N) \leq O_2(H)$ for $M \in \mathcal{M}$.

(d) Let $\widehat{N}_0$ be a subgroup of index 2 in N_0 which contains $\widetilde{N}_0$. Then there exist precisely two groups M and M' in $\mathcal{C}$, such that $\widehat{N}_0 = N_{N_0}(M) = N_{N_0}(M')$. Moreover $\widehat{N}_0 = N_{N_0}(M) = N_{N_0}(M') \leq H_0$.

Proof. Using $C_G(N) = C_G(N_0) = N$ we can (and will) consider H/N as a subgroup of $\mathrm{SL}(N)$ and H_0/N as a subgroup of $\mathrm{SL}(N_0)$.

(a) We know $H \leq N_G(N) = NL$, $H_0 \leq NL_0$, and $|NL : NL_0| \leq 2$, that is, $|H : H_0| \leq 2$. By (d.1) of Lemma 5.5 there is an element in $N_M(N)$ that interchanges $\mathcal{S}_0$ with $\mathcal{S}_1$. Hence $|N_M(N) : N_M(N_0)| = 2$ and we get assertion (a).

(b) By Lemma 5.4 $|N_M(N)| = 2^{2n-1}$ and $(M \cap N) \times N_{M_0}(N)$ has order 2^{2n-2}, so that $N_M(N_0) = (M \cap N) \times N_{M_0}(N)$ follows. Thus $N_M(N_0)N/N$

induces on N_0 (as a subgroup of $\mathrm{SL}(N_0)$) an elementary abelian group of order 2^{n-1}, which fixes the subspace $N_{N_0}(M)$ of dimension $n-1$ pointwise, i.e. $N_M(N_0)N/N$ is the full centralizer in $\mathrm{SL}(N_0)$ of the hyperplane $N_{N_0}(M)$. We recall from Proposition 7.5 that the centralizer of the subspace (and subgroup) $\widetilde{N}_0$ in $\mathrm{SL}(N_0)$ has the shape $X = E \cdot \mathrm{SL}(k,2)$, with E as in assertion (b). Then by Proposition 7.5 $\langle N_M(N_0) \mid M \in \mathcal{M}\rangle$ already induces the group X. But H_0/N is isomorphic to a subgroup of X, i.e. $H_0/N \simeq X$.

(c) As $N_M(N_0) = N_M(N_1)$, we see that this group induces in $\mathrm{SL}(N_1)$ an elementary abelian group of order 2^{n-1}, which fixes the subspace $N_{N_1}(M)$. Set $P_0 = O_2(H_0)$ and $\widetilde{N}_1 = \bigcap_{M\in\mathcal{M}} N_{N_1}(M)$. Then $H_0/P_0 \simeq \mathrm{SL}(k,2)$ induces on $N_i/\widetilde{N}_i$, for $i = 0,1$, the group $\mathrm{SL}(N_i/\widetilde{N}_i)$. Let $\sigma \in H - H_0$, then σ interchanges N_0 with N_1 by conjugation. In particular the mapping $H_0/P_0 \ni \tau P_0 \mapsto \sigma^{-1}\tau\sigma P_0 \in H_0/P_0$ induces an equivalence transformation between the two representations of H_0/P_0 on $N_0/\widetilde{N}_0$ and $N_1/\widetilde{N}_1 = N_0\sigma/\widetilde{N}_0\sigma$. Then σ induces an inner automorphism on H_0/P_0. But this group is isomorphic to its group of inner automorphisms. This shows that the 2-radical $O_2(H/P_0)$ of H/P_0 has order 2.

Let P be the pre-image of $O_2(H/P_0)$. Then $|P : P_0| = 2$. Now $N_M(N)P/P = N_{M_0}(N)P/P$ (as $N_{M_0}(N)P/P$ is self-centralizing in $H/P \simeq \mathrm{SL}(k,2)$), i.e $P = (P \cap N_M(N))P_0 = \langle\tau\rangle P_0$ for some $\tau \in P \cap N_M(N)$. We have $C_{P_0/N}(\tau) \geq N_{M_0}(N)N/N$. By symmetry $N_{M'}(N)$ covers P/P_0 for each $M' \in \mathcal{M}$. Hence there exists a $\sigma \in P_0$, such that $\tau\sigma \in N_{M'}(N)$. Thus $N_{M'_0}(N)N/N \leq C_{P_0/N}(\tau\sigma) = C_{P_0/N}(\tau)$. By assertion (a) of Proposition 7.5 τ centralizes P_0/N and hence P/N is elementary abelian.

Now assume that $\sigma \in \bigcap_{M'\in\mathcal{M}} N_M(M') \cap N_M(N)$. Let $M^1 \in \mathcal{M}$. Then $(M_0^1)^\sigma = M_a^1$ for some $a \in \{0,1\}$. Also by Lemma 5.4 $N_{M_0^1}(N) \equiv N_{M_1^1}(N)$ (mod N), so that $N_{M_0^1}(N)^\sigma N/N = N_{M_0^1}(N)N/N$. By (f) of Proposition 7.5 (applied to H/P) we see that $\sigma \in P$.

(d) By assertion (d) of Lemma 7.5 there exists $\gamma \in H_0$, such that $(M'_0)^\gamma$ is the group of elements in $\mathrm{SL}(N_0)$ that fix the hyperplane $\widehat{N}_0$ pointwise. Since $M^\gamma \leq \langle M^\gamma, N\rangle$, assertion (d) follows from Lemma 7.6. □

Remark 7.9. (a) Let M be in $\mathcal{M} - \{N\}$. By Lemma 5.4 the groups $N_M(N_0)$ and $N_N(N_0)$ centralize each other. So both groups $\widetilde{N}_i$, $i = 0,1$, lie in the center of P_0. As we have seen $\sigma \in P - P_0$ interchanges $\widetilde{N}_0$ and $\widetilde{N}_1$, so that $[\widetilde{N}_0 \times \widetilde{N}_1, \sigma] = [\widetilde{N}_0 \times \widetilde{N}_1, P]$ has order 2^{n-k}. For a given $M \in \mathcal{M}$ we may choose $\sigma \in N_M(N)$. From Lemma 5.4 we deduce that $[\widetilde{N}_0 \times \widetilde{N}_1, P] \leq M \cap N$. This implies that $|N \cap \bigcap_{M\in\mathcal{M}} M| \geq 2^{n-k}$.

(b) Under the assumptions of the lemma the group H contains precisely $2(2^k-1)+1 = 2^{k+1}-1$ groups, which lie in $\mathcal{C}$. Moreover $E \in \mathcal{C}$ lies in H, if and only if $N_{N_0}(E)$ contains $\bigcap_{M\in\mathcal{M}} N_{N_0}(M)$: By Lemma 5.4 all groups from $\mathcal{C}$, which lie in H, are already conjugate in H. So for any $M \in \mathcal{C}$, $M \leq H$ we have that $N_{M_0}(N)$ contains $\widetilde{N}_0 = \bigcap_{M\in\mathcal{M}} N_{N_0}(M)$ by assertion (b). On the other hand, as $H_0/O_2(H_0) \simeq \mathrm{SL}(k,2)$, the group H_0 contains precisely 2^k-1 groups of the form $N_M(N_0)N$, $M \in \mathcal{C} - \{N\}$. By Lemma 7.7 we see that for

$E \in \mathcal{C} - \{N\}$, $N_E(N_0)N \leq H_0$, there is precisely one more $E' \in \mathcal{C}$ for which $N_E(N_0)N$ and $N_{E'}(N_0)N$ induce the same automorphism group on N_0. Also there exists $\gamma \in H_0$ and $M \in \mathcal{M}$, such that $N_E(N_0)N$ and $N_{M^\gamma}(N_0)N$ induce the same automorphism group on N_0. By Lemma 7.7 $E = M^\gamma$ or $E' = M^\gamma$. The assertion follows.

For a subgroup $K \leq G$ and a subset $\mathcal{M} \subseteq \mathcal{C}$, in what follows we write $\mathcal{M} \cap K$ for the set of those $M \in \mathcal{M}$ that lie in K.

Lemma 7.10. *Let $N \in \mathcal{M} \subseteq \mathcal{C}$, $|\mathcal{M}| > 1$ and set $\mathcal{M}^\star = \langle M \rangle \cap \mathcal{C}$. Then:*

(a) $|\mathcal{M}^\star| = 2^{k+1} - 1$ for some $k \in \{1, \ldots, n\}$.

(b) The group $\bigcap_{M \in \mathcal{M}} N_N(M) = \bigcap_{M^\star \in \mathcal{M}^\star} N_N(M^\star)$ has order 2^{2n-k} and the group $\bigcap_{M \in \mathcal{M}} N_{N_0}(M) = \bigcap_{M^\star \in \mathcal{M}^\star} N_{N_0}(M^\star)$ has order 2^{n-k}.

Proof. Set $\widetilde{N}_i = \bigcap_{M \in \mathcal{M}} N_{N_i}(M)$, for $i = 0, 1$ and define k by $|\widetilde{N}_0| = 2^{n-k}$ ($= |\widetilde{N}_1|$ by Lemma 7.8). Then (a) holds by Remark 7.9. We prove assertion (b) by induction on k.

Case $k = 1$. Then $\mathcal{M}^\star = \{E, M, N\} \subseteq H = \langle M, N \rangle$, where $M \in \mathcal{M} - \{N\}$. With the notation of Lemma 5.4 we have $P \cap N = N_N(M) = N_N(E)$, $P_0 \cap N = N_{N_0}(M) \times N_{N_1}(M) = N_{N_0}(E) \times N_{N_1}(E)$ and assertion (b) follows.

Assume now $k > 1$ and pick two $M, M' \in \mathcal{M}$, such that $N \not\leq \langle M, M' \rangle$. Let $\{M, M', E\} = \langle M, M' \rangle \cap \mathcal{C}$. An element $\tau \in N_N(M) \cap N_N(M')$ normalizes M, M' and $\langle M, M' \rangle$ and hence E too. Thus

$$N_N(M) \cap N_N(M') \quad = \quad N_N(M) \cap N_N(M') \cap N_N(E). \tag{4}$$

Similarly,

$$N_{N_0}(M) \cap N_{N_0}(M') \quad = \quad N_{N_0}(M) \cap N_{N_0}(M') \cap N_{N_0}(E). \tag{5}$$

Denote by $\widetilde{\mathcal{M}}$ the set of all those $\widetilde{M} \in \mathcal{C}$ that lie in groups of the form $\langle M, M' \rangle$, $M, M' \in \mathcal{M}$. Then the $k = 1$ case and Equations (4) and (5) show that $\bigcap_{M \in \mathcal{M}} N_N(M) = \bigcap_{\widetilde{M} \in \widetilde{\mathcal{M}}} N_N(\widetilde{M})$ and $\bigcap_{M \in \mathcal{M}} N_{N_0}(M) = \bigcap_{\widetilde{M} \in \widetilde{\mathcal{M}}} N_{N_0}(\widetilde{M})$. Induction on the size of $\mathcal{M}$ shows that these equation remain to be true if we replace $\widetilde{\mathcal{M}}$ by $\mathcal{M}^\star$.

It remains to show that $|\bigcap_{M \in \mathcal{M}} N_N(M)| = 2^{2n-k}$ and $|\bigcap_{M \in \mathcal{M}} N_{N_0}(M)| = 2^{2n-k}$. To see this we choose $M^1, \ldots, M^k \in \mathcal{M}$, such that $\widetilde{N}_0 = \bigcap_i N_{N_0}(M^i)$ and we set $\mathcal{M}_0 = \{N, M^1 \ldots, M^k\}$. Then $\mathcal{M}_0$ satisfies the assumptions of the lemma, in particular $\mathcal{M}^\star = \langle \mathcal{M}_0 \rangle \cap \mathcal{C}$ and $\widetilde{N} = \bigcap_{M \in \mathcal{M}} N_N(M) = \bigcap_i N_N(M^i)$. Since $|N : N_N(M^i)| = 2$ we have $|\widetilde{N}| \geq 2^{2n-k}$ and $|\widetilde{N}_0| \geq 2^{n-k}$. However a nontrivial H_0/N-module has dimension at least k (as $H_0/O_2(H_0) \simeq \mathrm{SL}(k, 2)$), which implies that $|N_0/\widetilde{N}_0| \geq 2^k$, and thus $|\widetilde{N}_0| = 2^{n-k}$. Also $N/\widetilde{N}$ is a nontrivial $H/O_2(H)$-module implying (as before) that $|N/\widetilde{N}| \geq 2^k$. Hence we obtain that $|\widetilde{N}| = 2^{2n-k}$. □

We call a non-empty subset $\mathcal{M}$ of $\mathcal{C}$ *saturated* if $\mathcal{M} = \langle \mathcal{M} \rangle \cap \mathcal{C}$. We know by Remark 7.9 that $|\mathcal{M}| = 2^{k+1} - 1$ for some $k > 0$. For any $M \in \mathcal{M}$ and $a = 0$ or 1 we set:

$$\widetilde{M} = \bigcap_{M' \in \mathcal{M}} N_M(M'), \quad \widetilde{M}_a = \bigcap_{M' \in \mathcal{M}} N_{M_a}(M').$$

With these conventions we prove the following generalization of Lemma 5.4:

Theorem 7.11. *Let $\mathcal{M}$ be a saturated subset of $\mathcal{C}$ such that $|\mathcal{M}| = 2^{k+1} - 1$, and set $H = \langle \mathcal{M} \rangle$. Then the following hold:*

(a) $Q = Z(H) = \bigcap_{M \in \mathcal{M}} M$ is elementary abelian of order 2^{n-k}.

(b) For any $N^0, N^1, \ldots, N^\ell \in \mathcal{M}$, $1 \leq \ell < k$, with $|N^0 \cap N^1 \cap \cdots \cap N^\ell| = 2^{n-\ell}$, there exist $N^{\ell+1}, \ldots, N^k \in \mathcal{M}$ with $H = \langle N^0, N^1, \ldots, N^k \rangle$. Moreover, we have $Q = N^0 \cap \cdots \cap N^k$. For the remaining assertions $N^0, N^1, \ldots, N^k$ will be as here.

(c) Let $\mathcal{S}^j_a$ be the two orbits of N^j on $\mathcal{S}$, where $0 \leq j \leq k$ and $a = 0, 1$. For $\underline{a} = (a_0, a_1, \ldots, a_k) \in \{0,1\}^{k+1}$ define

$$\mathcal{S}(\underline{a}) = \mathcal{S}(a_0, a_1, \ldots, a_k) = \bigcap_{i=0}^{k} \mathcal{S}^i_{a_i}$$

and set

$$\mathcal{D} = \{\mathcal{S}(\underline{a}) \mid \underline{a} \in \{0,1\}^{k+1}\}.$$

Then $|\mathcal{S}(\underline{a})| = 2^{n-k}$ for all $\underline{a} \in \{0,1\}^{k+1}$ and $|\mathcal{D}| = 2^{k+1}$. Moreover Q acts regularly on $\mathcal{S}(\underline{a})$ for all $\underline{a}$ and $\mathcal{D}$ is the set of Q-orbits.

(d) Set $P_0 = \langle \widetilde{M}_a \mid M \in \mathcal{M},\ a = 0, 1 \rangle$. Then P_0 is elementary abelian of order $2^{(k+2)(n-k)}$ and

$$P_0 = Q \times \widetilde{N}^0_0 \times \cdots \times \widetilde{N}^k_0 = Q \times \widetilde{N}^0_1 \times \cdots \times \widetilde{N}^k_1.$$

(e) Set $P = \langle \widetilde{M} \mid M \in \mathcal{M} \rangle$. Then $P = O_2(H) = \langle \widetilde{N}^0, \ldots, \widetilde{N}^k \rangle$ and P_0 is the kernel of the action of P on $\mathcal{D}$. The group P has nilpotency class at most 2 and P/Q is elementary abelian. The group P/P_0 has order 2^{k+1} and it acts regularly on $\mathcal{D}$.

(f) $H/P \simeq \mathrm{SL}(k+1, 2)$ and every H-composition factor on P/Q is the natural $\mathrm{SL}(k+1, 2)$-module.

Proof. We prove the theorem by induction on k. We also may assume without loss of generality that $N \in \mathcal{M}$.

Case $k = 1$. Let M, N be two extension groups in $\mathcal{M}$. By Lemma 5.4 the group $H = \langle M, N \rangle$ contains three groups from $\mathcal{C}$, i.e. $H = \langle \mathcal{M} \rangle$. Lemma 5.4, Lemma 5.6, and Remark 5.7 imply assertions (a) - (f).

Case $k > 1$. We start with assertions (a) and (b). Set $H_\ell = \langle N^0, N^1, \dots, N^\ell\rangle$, $\mathcal{M}^\ell = H_\ell \cap \mathcal{C}$ and assume $|\mathcal{M}^\ell| = 2^{s+1} - 1$. Without loss of generality $N = N^0$. As $|N_{N_0}(N^i)| = 2^{n-1}$ for $i \geq 1$, we have $|\bigcap_{0\le i\le \ell} N_{N^0_0}(N^i)| = 2^{n-s} \geq 2^{n-\ell}$, i.e. $s \leq \ell$. By Lemma 7.10 $\bigcap_{0\le i\le\ell} N_{N^0_0}(N^i) = \bigcap_{M\in\mathcal{M}^\ell} N_{N^0_0}(M)$. If $s < \ell$, then by induction $Z(H_\ell) = N^0 \cap \dots \cap N^\ell$ has order 2^{n-s}, contradicting our assumption.

Hence $|\bigcap_{M\in\mathcal{M}^\ell} N_{N^0_0}(M)| = 2^{n-\ell}$ and $|\mathcal{M}^\ell| = 2^{\ell+1} - 1$ by Remark 7.9. Pick $N^{\ell+1} \in \mathcal{M} - \mathcal{M}^\ell$. If $\bigcap_{M\in\mathcal{M}^\ell} N_{N^0_0}(M) \leq N_{N^0_0}(N^{\ell+1})$, we get $N^{\ell+1} \in \mathcal{M}^\ell$ by Remark 7.9 (b), a contradiction. Thus $|\bigcap_{0\le i\le\ell} N_{N^0_0}(N^i) : \bigcap_{0\le i\le \ell+1} N_{N^0_0}(N^i)| = 2$.

By part (a) of Remark 7.9 we know $|N^0 \cap \ldots \cap N^{\ell+1}| \geq 2^{n-\ell-1}$, i.e. $|N^0 \cap \ldots \cap N^\ell : N^0 \cap \ldots \cap N^{\ell+1}| \leq 2$. We claim that equality holds. Write $\sigma \in Z(H_\ell) = N^0 \cap \ldots \cap N^\ell$ as $\sigma = \sigma_0\sigma_1$, where $\sigma_i \in N_i$, $i = 0, 1$. Then each mapping $Z(H_\ell) \ni \sigma \mapsto \sigma_i \in N_i$ is injective, as $Z(H_\ell) \cap N_i = 1$. Moreover, if $\sigma \in N^0 \cap \ldots \cap N^{\ell+1}$ then $\sigma_0 \in \bigcap_{0\le i\le \ell+1} N_{N_0}(N^i)$, which has order $2^{n-\ell-1}$. This shows the claim. Now induction on ℓ implies assertions (a) and (b).

To (c): Let $\mathcal{B}$ be the set of Q-orbits on $\mathcal{S}$. Since Q acts semiregularly on $\mathcal{S}$, each orbit has length 2^{n-k}, so that $|\mathcal{B}| = 2^{k+1}$. By (b) (and Lemma 5.4) each $\mathcal{S}(\underline{a})$ is Q-invariant. So $\mathcal{D} = \mathcal{B}$, once we show that each $\mathcal{S}(\underline{a}) \neq \emptyset$. For a sequence $(a_0, \dots, a_{k-2}) \in \{0,1\}^{k-1}$ and $a, b \in \{0,1\}$ we consider the sets $\mathcal{T}^a = \bigcap_{0\le i<k-1} \mathcal{S}^i_{a_i} \cap \mathcal{S}^{k-1}_a$, $\mathcal{T}_b = \bigcap_{0\le i<k-1} \mathcal{S}^i_{a_i} \cap \mathcal{S}^k_b$, and $\mathcal{T}^a_b = \mathcal{T}^a \cap \mathcal{T}_b = \mathcal{S}(a_0, \dots, a_{k-2}, a, b)$. By induction $|\mathcal{T}^a| = |\mathcal{T}_b| = 2^{n-k+1}$ and we have partitions $\mathcal{T}^a = \mathcal{T}^a_0 \cup \mathcal{T}^a_1$ and $\mathcal{T}_b = \mathcal{T}^0_b \cup \mathcal{T}^1_b$. We have to show that all the $\mathcal{T}^a_b$ are non-empty.

Assume, for instance, that $\mathcal{T}^0_1 = \emptyset$. Then $\mathcal{T}^0 = \mathcal{T}^0_0 = \mathcal{T}_0$ has size 2^{n-k+1}. In particular $Q^0 = \bigcap_{0\le i<k} N^i$ and $Q_1 = \bigcap_{0\le i\le k, i\neq k-1} N^i$ act faithfully and regularly on $\mathcal{T}^0$. Set $\overline{Q} = \langle Q^0, Q_1\rangle$, which is elementary abelian, as $\overline{Q} \leq N^0$. Since $|Q^0 \cap Q_1| = 2^{n-k}$, we have $|\overline{Q}| = 2^{n-k+2}$. If $k > 2$, then $\overline{Q}$ ($\leq N^0 \cap N^1$) acts semiregularly on $\mathcal{S}$, i.e $|\mathcal{T}^0| \geq |\overline{Q}|$, a contradiction.

So assume $k = 2$ and, without loss of generality, assume that $a_0 = 0$. Then $\mathcal{S}^0_0 \cap \mathcal{S}^1_0 = \mathcal{S}^0_0 \cap \mathcal{S}^2_0$ and $\mathcal{S}^0_0 \cap \mathcal{S}^1_1 = \mathcal{S}^0_0 \cap \mathcal{S}^2_1$ are sets of size 2^{n-1} and by Lemma 5.4 the two groups $N_{N^i_1}(N^0_0)$, $i = 1, 2$, act faithfully and semiregularly on the first set. Pick $S \in \mathcal{S}^0_0 \cap \mathcal{S}^1_0$. There exist precisely 2^{n-1} elements $\nu \in N^0_1$ with $S\nu \in \mathcal{S}^0_0 \cap \mathcal{S}^1_0$. For $\mu \in N_{N^i_1}(N^0_0)$ we have

$$S\nu = S\nu\mu = S\mu\nu^\mu = S\nu^\mu,$$

which forces $\nu = \nu^\mu$. Hence $C_{N^0_1}(N_{N^1_1}(N^0_0)) = C_{N^0_1}(N_{N^2_1}(N^0_0))$ is a group of order 2^{n-1}. This shows that $N_{N^1_1}(N^0_0)N$ and $N_{N^2_1}(N^0_0)N$ induce in $\mathrm{SL}(N^0_1)$ the same group of transvections centralizing the hyperplane $C_{N^0_1}(N_{N^1_1}(N^0_0))$. By Remark 7.9 (b) (or Lemma 7.7) we conclude that $N^2 \leq \langle N^0, N^1\rangle$, a contradiction. Now assertion (c) follows.

To (d): Set $P_{00} = \langle Q, \widetilde{N}^0_0, \dots, \widetilde{N}^k_0\rangle$. We claim that (1) $P_{00} = Q \times \widetilde{N}^0_0 \times \dots \times \widetilde{N}^k_0$ and (2) $P_0 = P_{00}$.

By Lemma 7.10 we know $\widetilde{N}^j_0 = \bigcap_{0\le i\le k} N_{N^j_0}(N^i)$ and $|\widetilde{N}^j_0| = 2^{n-k}$. By assertion (a) of Lemma 5.5 each orbit $\mathcal{S}^\ell_a$, where $0 \leq \ell \leq k$, $a = 0, 1$, is fixed under $\widetilde{N}^j_0$. Thus P_{00} fixes each Q-orbit in $\mathcal{D}$.

Assume that we have already shown

$$\langle \widetilde{N}_0^1, \ldots, \widetilde{N}_0^k \rangle = \widetilde{N}_0^1 \times \cdots \times \widetilde{N}_0^k.$$

The group $\widetilde{N}_0^0$ acts faithfully on $\mathcal{S}(1,0,0,\ldots,0)$, whereas $\widetilde{N}_0^1 \times \cdots \times \widetilde{N}_0^k$ fixes this set pointwise. Hence $\widetilde{N}_0^0 \cap (\widetilde{N}_0^1 \times \cdots \times \widetilde{N}_0^k) = 1$ and

$$\langle \widetilde{N}_0^0, \widetilde{N}_0^1, \ldots, \widetilde{N}_0^k \rangle = \widetilde{N}_0^0 \times \widetilde{N}_0^1 \cdots \times \widetilde{N}_0^k.$$

follows. Considering the actions of Q and $\widetilde{N}_0^0 \times \cdots \times \widetilde{N}_0^k$ on $\mathcal{S}(0,0,0,\ldots,0)$, we finally obtain assertion (1).

We turn to assertion (2). We observe that $P_{00} \cap N^0 = Q \times \widetilde{N}_0^0$: Otherwise (as $Q \times \widetilde{N}_0^0 \leq P_{00} \cap N^0$) we would have $N^0 \cap \widetilde{N}_0^1 \times \cdots \times \widetilde{N}_0^k \neq 1$. But non-identity elements from this group have fixed-points in $\mathcal{S}_0^0$ *and* $\mathcal{S}_1^0$, which is impossible. Thus $|P_{00}N^0/N^0| = 2^{k(n-k)}$ and $P_{00}N^0/N^0$ (as a subgroup of $\mathrm{SL}(N_0^0)$) stabilizes the chain $1 \leq \widetilde{N}_0^0 \leq N_0^0$. The stabilizer of this chain in $\mathrm{SL}(N_0^0)$ however has order $2^{k(n-k)}$, i.e. $P_{00}N^0/N^0$ is the *full* stabilizer of this chain. Also P_0N^0/N^0 stabilizes this chain, i.e.

$$P_0 \leq P_{00}N^0 = N^0(\widetilde{N}_0^1 \times \cdots \times \widetilde{N}_0^k),$$

and, as we have seen before, $N_0^0 \cap (\widetilde{N}_0^1 \times \cdots \times \widetilde{N}_0^k) = 1$. Let $1 \neq \sigma$ be in P_0. Adjusting σ if necessary with an element from P_{00}, we may also assume that $\sigma \in N^0$ and that σ has fixed-points in $\mathcal{S}_0^0$. But then $\sigma \in N_0^0$ and σ fixes every $\mathcal{S}(0,*,\ldots,*)$ pointwise, but acts fixed-point-freely on each orbit of the form $\mathcal{S}(1,*,\ldots,*)$. This implies that $\sigma \in \widetilde{N}_0^0$: otherwise $\widetilde{N}_0^0 < \langle \widetilde{N}_0^0, \sigma \rangle \leq N_0^0$ and therefore the orbits of this group in $\mathcal{S}_1^0$ would have a length strictly greater than 2^{n-k}, which is impossible. Thus claim (2) is also true. Assertion (d) follows from (1) and (2).

To (e): Clearly,

$$[\widetilde{N}^0, \widetilde{N}^1] \leq N^0 \cap N^1.$$

Let $\tau_i \in \widetilde{N}^i$, $i = 0,1$. Then $\sigma = \tau_0\tau_1 \in O_2(H^k)$, $H^k = \langle N_M(N^k) \mid M \in \mathcal{M} \rangle N^k$ by assertion (c) of Lemma 7.8. As $O_2(H^k)/N^k$ is elementary abelian, we get $[\tau_0, \tau_1] = \sigma^2 \in N^k$. Hence $[\widetilde{N}^0, \widetilde{N}^1] \leq Q$ by an obvious induction. Since any pair $M, E \in \mathcal{M}$ is conjugate in H to N^0, N^1, we see that $[\widetilde{M}, \widetilde{E}] \leq Q$. So P/Q is an elementary abelian 2-group.

By definition P is a normal subgroup of H. We claim, that P_0 is the kernel of the action of P on $\mathcal{D}$:

Denote by $\widehat{P}$ this kernel (of course $P_0 \leq \widehat{P}$). The group $\widehat{P}N^0/N^0$ stabilizes the chain $1 \leq \widetilde{N}_0^0 \leq N_0^0$, since $\widehat{P}$ normalizes N_0^0 and $\widehat{P}N^0/N^0$ lies in the stabilizer of the chain $1 \leq \widetilde{N}_0^0 \leq N_0^0$ as a subgroup of $\mathrm{SL}(N_0^0)$. As before we obtain $\widehat{P} \leq P_0N$. Let σ be an element in $\widehat{P}$. Adjusting this element with an element from P_0, we may even assume that $\sigma \in N$ and as in the verification of (d) this leads to $\sigma \in Q \times \widetilde{N}_0^0 \times \widetilde{N}_1^0$, i.e. $\widehat{P} = P_0$. In particular P/P_0 acts faithfully on $\mathcal{D}$.

Claim: We have $|P/P_0| = 2^{k+1}$ and P/P_0 acts regularly on $\mathcal{D}$.

By Lemma 7.10, we have $2^n = |\widetilde{N}^0 : \widetilde{N}^0_0| = |\mathcal{S}^0_0|$. So $\widetilde{N}^0$ is transitive on $\mathcal{S}^0_0$ and (by symmetry) on $\mathcal{S}^0_1$. Therefore $\widetilde{N}^0$ permutes transitively all orbits of the form $\mathcal{S}(0, *, \ldots, *)$ and all orbits of the form $\mathcal{S}(1, *, \ldots, *)$. These two subsets of $\mathcal{D}$ have size 2^k. Hence $|\widetilde{N}^0 P_0/P_0| = 2^k = |\widetilde{N}^0 : \widetilde{N}^0_0|$, i.e. $\widetilde{N}^0 \cap P_0 = \widetilde{N}^0_0$. This shows that $\widetilde{N}^0 P_0/P_0$ acts regularly on both subsets of $\mathcal{D}$. Of course P/P_0 is transitive on $\mathcal{D}$ and P/P_0 is abelian and therefore P/P_0 is regular on $\mathcal{D}$. This implies that $|P/P_0| = 2^{k+1}$ and hence the claim.

Finally we show that $P = O_2(H)$:

Set $R = O_2(H)$ (i.e. $P \leq R$). The group R acts by conjugation on the set $\mathcal{M}$ of size $2^{k+1} - 1$. Thus R normalizes one and hence all subgroups in $\mathcal{M}$. Set $K_1 = \langle N_M(N) \mid M \in \mathcal{M}\rangle RN \leq N_G(N)$ (where $N = N^0$). By Theorem 3.6 there exists a normal subgroup K_0, with $|K_1 : K_0| \leq 2$, such that K_0 normalizes N_0 and N_1. But we have seen that P does not leave invariant the orbits $\mathcal{S}^0_0$ and $\mathcal{S}^0_1$, i.e. $|K_1 : K_0| = 2$.

By Lemma 7.8 K_0/N induces on N^0_a, for $a = 0, 1$, by conjugation the centralizer of the subspace $\widetilde{N}^0_a$ in $\mathrm{SL}(N^0_a)$, whereas P_0N/N induces the 2-radical of this group. As $PN > P_0N$ and $|K_1 : K_0| = 2$ we have that $PN/N = RN/N$ is the 2-radical of K_1/N, in particular

$$PN = RN.$$

Assume $R > P$. As $PN = RN$, we have $R \cap N > P \cap N$. We know that $P \cap N$ is transitive on $\mathcal{S}^0_0$, so that $2^n = |\mathcal{S}^0_0| = |P \cap N : P \cap N_0| = |R \cap N : R \cap N_0|$ and thus $R \cap N_0 > P \cap N_0$.

Let $\sigma \in (R \cap N_0) - (P \cap N_0)$, i.e. $|\langle \widetilde{N}_0, \sigma\rangle : \widetilde{N}_0| = 2$, as $P \cap N_0 = \widetilde{N}_0$. Pick $M \in \mathcal{M}$, such that $\langle \widetilde{N}_0, \sigma\rangle \leq N_{N_0}(M)$. In fact, $\sigma \in N_{N_0}(M_0)$, by Lemma 5.6 (a). Then σ induces an involution on $M_0/\widetilde{M}_0$, i.e. we have $\sigma_{M_0/\widetilde{M}_0} \neq 1_{M_0/\widetilde{M}_0}$ (as $\sigma \in N_0 - \widetilde{N}_0$). By Lemma 7.8 there exist a $M' \in \mathcal{M}$ and $\sigma' \in N_{M'_0}(M)$, such that $(\sigma\sigma')_{M_0/\widetilde{M}_0}$ has order 3. This contradicts $\sigma \in R = O_2(H)$. The verification of (e) is complete.

To (f): We observe that $H = \langle N^i \mid 0 \leq i \leq k\rangle$ acts as a permutation group on $\mathcal{D}$ and that, by (e), P_0 is a normal subgroup of H. Note that every H composition factor on P/Q is a $\mathbb{F}_2[H/P]$-module by [1, (5.5)].

We first provide an H-decomposition of P_0/Q. For $R \leq Q$ denote by $P_0(R)$ the kernel of the action of P_0 on the R-orbits. Decompose $\rho \in R$ as $\rho = \rho_0\rho_1$, $\rho_i \in N^0_i$, $i = 0, 1$. Then ρ_0 and ρ_1 are in $P_0(R)$ (For instance ρ_1 acts on $\mathcal{S}_0$ like ρ and it acts trivially on $\mathcal{S}_1$, i.e. $\rho_1 \in P_0(R)$). Hence $|P_0(R) \cap N^i_0| = |R|$. Moreover $P_0(R) \cap P_0(R') = 1$ for $R' \leq Q$ and $R \cap R' = 1$, as a non-trivial intersection of an R-orbit with an R'-orbit has size 1, since Q acts faithfully and regularly on each of its orbits. Clearly, each $P_0(R)$ is normal in H, as R and P_0 are normal subgroups. Let $Q = R_0 \times \cdots \times R_{n-k}$ with subgroups R_i of order 2. Then $X_i = (P_0(R_i) \cap \widetilde{N}^0_0) \times \cdots \times (P_0(R_i) \cap \widetilde{N}^0_k)$ has order 2^{k+1} and hence $Q \times X_1 \times \cdots \times X_{n-k}$ has order $2^{(k+2)(n-k)}$, i.e. $P_0 = Q \times X_1 \times \cdots \times X_{n-k}$.

Then

$$P_0/Q = X_1Q/Q \times \cdots \times X_{n-k}Q/Q$$

is an H-invariant decomposition.

Set $K^0 = \langle N_{N^1}(N^0), \dots, N_{N^k}(N^0)\rangle$.

We know from Lemma 7.8 that K^0N/N has the form $E \cdot \mathrm{SL}(k,2)$, where E is the elementary abelian 2-radical of K^0N/N. Hence $K^0/\widehat{P} \simeq \mathrm{SL}(k,2)$, where $\widehat{P} = O_2(K^0)$.

Set $H^0 = \langle N^1, \dots, N^k\rangle$ and $P^0 = O_2(H^0)$. By induction $H^0/P^0 \simeq \mathrm{SL}(k,2)$ and all H^0-composition factors in $P^0/Z(H^0)$ are *natural.* Here we call a composition factor natural, if it is the natural module for $\mathrm{SL}(k,2) \simeq H^0/P^0$. Now K^0P^0/P^0 is isomorphic to a subgroup of $\mathrm{SL}(k,2)$ and as $K^0 \cap P^0 \leq \widehat{P}$, we see that $K^0/(K^0 \cap P^0)$ is the extension of a 2-group by $\mathrm{SL}(k,2)$. This shows that $K^0/(K^0 \cap P^0) \simeq \mathrm{SL}(k,2)$ and $K^0 \cap P^0 = \widehat{P}$.

Clearly, $\widehat{P} \cap Z(H^0) = Q$, so that all composition factors in $\widehat{P}/Q$ of K^0 are natural. This shows that K^0 has in X_iQ/Q one natural and one trivial composition factor. Indeed, the trivial composition factor is given by $\widetilde{N}_0^0Q/Q \cap X_iQ/Q$. As $\widetilde{N}^i \leq \widehat{P}$ for $1 \leq i \leq k$, we see that $\widehat{P} \not\leq P^0$. Thus $\widehat{P}/(\widehat{P} \cap P^0)$ contains at least one natural composition factor.

The group $K^1 = \langle N_{N^0}(N^1), N_{N^2}(N^1), \dots, N_{N^k}(N^1)\rangle$ has the analogous properties to those of K^0 (but leaves invariant $\widetilde{N}^1$ instead of $\widetilde{N}^0$). So the group $K = \langle K^0, K^1\rangle$ induces on X_iQ/Q as well on P/P_0 the (maximal possible) group $\mathrm{SL}(k+1,2)$ and all composition factors of H on P/Q are natural. □

7.1 Proofs of Theorems 7.1 and 7.3

Proof. (Theorem 7.1) The first assertion follows from a Frattini argument: Let σ be an element in G. Then $N^\sigma \in \mathcal{C}$. By Proposition 5.1 there exists a $\gamma \in G^*$ with $N^{\sigma\gamma} = N$, i.e. $\sigma\gamma \in N_G(N)$ or $G = G^*N_G(N)$.

Assume first that G is not transitive on $\mathcal{S}$. Then $\mathcal{S}_0$ and $\mathcal{S}_1$ are the G-orbits. Assertion (a) follows from Lemma 3.9.

Assume from now on that G is transitive on $\mathcal{S}$. By Corollary 3.7 $N_G(N)$ is transitive too, i.e. there exists an element $\sigma \in N_G(N)$ that interchanges $\mathcal{S}_0$ and $\mathcal{S}_1$. The proof of Lemma 3.9 shows that β and β^o are isotopic.

If $\mathcal{C} = \{N\}$, then N is normal in G, and we have assertion (b) by Lemma 3.9. If N is not normal, we get assertion (c) by Theorem 7.11. □

Proof. (Theorem 7.3) The assertion $G = G^*N_G(N)$ has the same verification as in the previous proof.

Assume first that $\overline{G}$ is not transitive on $\mathcal{S}$. Then $\mathcal{S}_0$ and $\mathcal{S}_1$ are the $\overline{G}$-orbits. Assertion (a) now follows from Lemma 3.9.

Assume from now on that $\overline{G}$ is transitive on $\mathcal{S}$. By Corollary 3.7 $N_{\overline{G}}(\overline{N})$ is transitive too, i.e. there exists an element $\overline{\sigma} \in N_{\overline{G}}(\overline{N})$ that interchanges $\mathcal{S}_0$ and $\mathcal{S}_1$. So f_0 and f_1 are isotopically linked by the proof of Lemma 3.9. If $\mathcal{C} = \{N\}$, then N is normal, we get assertion (b) of Theorem 7.1 by Lemma 3.9. If N is not normal, we obtain assertion (c) by Theorem 7.11. □

Remark 7.12. Let $\mathcal{S}$ be the extension of a bilinear DHO or the graph of the extension of quadratic APN functions. Assume in addition in the DHO case that $\mathcal{S}$ is bilinear and in the APN case assume, that the extension is quadratic. We sketch in this situation a simpler, alternative way, to prove Theorems 7.1 and 7.3. The basis for this approach is the following lemma, which is implicitly contained in [5].

Lemma 7.13. *Let T be a translation group of $\mathcal{S}$ that is normalized by the extension group N. Let U be the ambient space of $\mathcal{S}$. Then N induces as a subgroup of $\mathrm{GL}(U/C_U(T))$ the 2-radical of the stabilizer of a hyperplane of $U/C_U(T)$.*

Proof. As N normalizes T, we see that TN is a 2-group and hence by Theorem 3.6 both groups normalize each other. Therefore $C_U(T) = [U,T] \subseteq W_0 + W_1$, where W_i is defined as in Remark 3.5. As N normalizes T, it fixes the subspace $C_U(T)$. Thus NT/T is the stabilizer of the hyperplane $(W_0+W_1)/C_U(T)$ of $U/C_U(T)$. □

Proof. (Sketch of the simplified verification) Let G be the automorphism group of $\mathcal{S}$ (DHO) or the linear part of the automorphism group of $\mathcal{S}$ (APN) and let $\mathcal{C}$ be the class of extension groups in G. We assume $|\mathcal{C}| > 1$.

Then T is normal in G: Let K be the group generated by the the conjugates of T and assume that $T < K$. By [5, Thm. 5.9] $M = O_2(K) \in \mathcal{C}$. As M *char* $K \trianglelefteq G$, we obtain $M \trianglelefteq G$, which contradicts $|\mathcal{C}| > 1$.

Set $H = \langle \mathcal{C} \rangle$. Then HT/T is canonically isomorphic to a subgroup of the autotopism group. Therefore HT/T acts faithfully on $U/C_U(T)$ by [5, Prop. 3.9]. Assume that $\mathcal{S}$ has rank $n+1$. By Lemma 7.13 and Proposition 7.5 there exists a number k ($1 \leq k \leq n$) such that $H/(T \cap H) \simeq HT/T \simeq E \cdot S$ with E elementary abelian of order $2^{(k+1)(n-k)}$ and $S \simeq \mathrm{SL}(k+1,2)$. By [5, Lemma 4.5] $T \cap N$ is a hyperplane of T, so that $T = \langle T \cap N, T \cap M \rangle$ for any two $M, N \in \mathcal{C}$, i.e. $T \leq H$. Pick $N_1, \ldots, N_{k+1} \in \mathcal{C}$, such that $H = \langle N_1, \ldots, N_{k+1} \rangle T$. Then we have $Q = T \cap N_1 \cap \cdots N_{k+1} \leq Z(H)$ and $|Q| \geq 2^{n-k}$. But as a cyclic group of order $2^{k+1}-1$ in H centralizes this group, we get $|Q| = 2^{n-k}$. Set $P = O_2(H)$. It is now easy to see that $[T,P] \leq Q = Z(H)$. Hence P has class at most 2, P/Q is elementary abelian of order $2^{(k+1)(n-k+1)}$, and all composition factors of P/Q are natural $\mathrm{SL}(k+1,2)$-modules. □

We add an observation about the natural composition factors of $\mathrm{SL}(k+1,2)$. For $k \geq 2$ the natural $\mathrm{SL}(k+1,2)$-module is not equivalent to its dual module (for instance the roles of stabilizers of points and hyperplanes are interchanged). Indeed the $\mathrm{SL}(k+1,2)$-composition factors of P/Q are not pairwise equivalent: the factor T/Q is dual to the composition factors in P/T. Inspecting the proof of Theorem 7.11 one observes a further phenomenon: the composition factors in P_0/Q are dual to the composition factor P/P_0.

References

[1] M. Aschbacher: *Finite Group Theory*, Cambridge Univ. Press, 1986.

[2] T. Berger: On the automorphism groups of affine-invariant Codes, Des., Codes and Cryptogr., 7(1996), 215-221.

[3] C. Carlet, P. Charpin, and V. Zinoviev: Codes, bent functions and permutations suitable for DES-like cryptosystems, Des., Codes and Cryptogr., 15(1998), 125–156.

[4] U. Dempwolff: Symmetric extensions of bilinear dual hyperovals, Finite Fields Appl. 22(2013), 51-56.

[5] U. Dempwolff, Y. Edel: Dimensional dual hyperovals and APN functions with translation groups, J. Algebraic Combin. 39(2014), 457-496.

[6] Y. Edel, On quadratic APN functions and dimensional dual hyperovals, Des. Codes Cryptogr., 57(2010), 35-44.

[7] H. Taniguchi: Some examples of simply connected dual hyperovals, Finite Fields Appl. 22(2013), 45-50.

[8] F. Timmesfeld: Groups with weakly closed TI-subgroups, Math. Z. 143(1975), 243-275.

[9] S. Yoshiara: Dimensional dual arcs – A survey, in *Finite Geometries, Groups and Computation*, Proc. of Conf. Pingree Park 2004, Col. USA, pp. 247-266, 2006.

[10] S. Yoshiara, Dimensional dual hyperovals associated with quadratic APN functions, Innov. Incidence Geom., 8(2008), 147–169.

[11] Y. Yu, M. Wang, Y. Li: A matrix approach for constructing quadratic APN functions, Des. Codes Cryptogr. 73(2014), 587-600.