Dimensional Dual Hyperovals and APN Functions with Translation Groups

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

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

Abstract

In this paper we develop a theory of translation groups for dimensional dual hyperovals and APN functions. It will be seen that both theories can be treated, to a large degree, simultaneously. For small ambient spaces it will be shown that the translation groups are normal in the automorphism group of the respective geometric object. For large ambient spaces there may be more than one translation group. We will determine the structure of the normal closure of the translation groups in the automorphism group and we will exhibit examples which in fact do admit more than one translation group.

1 Introduction

In this paper we investigate dimensional dual hyperovals and APN functions which admit translation groups (the notion translation group refers to regular action on the underlying geometric object together with a natural assumption on the fixed points of such a group). It turns out that both cases lead to similar theories and can be studied to a large part simultaneously.

In Section 2 we introduce translation groups for APN functions and dimensional dual hyperovals. We also exhibit a one-to-one correspondence between alternating dimensional dual hyperovals and quadratic APN functions (Theorem 2.4).

In Chapter 3 we introduce a common hypothesis (Hypothesis A) shared by translation groups of dual hyperovals and APN functions. This implies (Theorems 3.2 and 3.5) that translation groups are elementary abelian 2-groups which have a quadratic action on the underlying $\mathbb{F}_2$-space. Moreover these theorems

*The research of this author took place within the project "Linear codes and cryptography" of the Research Foundation – Flanders (FWO) (Project nr. G.0317.06), and was supported by the Interuniversitary Attraction Poles Programme - Belgian State - Belgian Science Policy: project P6/26-Bcrypt.

show that the existence of a translation group implies, in the case of a dimensional dual hyperoval, that this hyperoval is bilinear. In the case of an APN function we are lead to quadratic APN functions. In Theorem 3.10 we show that the automorphism group of an alternating dimensional dual hyperoval is isomorphic to the normalizer of a translation group in the automorphism group of the associated quadratic APN function. The notion of a nucleus of a bilinear dimensional dual hyperoval is introduced, which is an analogue of the notion of nuclei in semifields. Then we prove (Theorem 3.11) that the translation groups form a conjugacy class of self-centralizing TI subgroups in the automorphism group.

Chapter 4 is devoted to the investigation of the normal closure of the translation groups in the automorphism group of a dimensional dual hyperoval or an APN function respectively. This section is mainly of group theoretic nature and it is based on the theory of weakly closed TI subgroups of Timmesfeld [23]. Using this strong tool from group theory we get in Theorem 4.6 a pretty precise description of the normal closure of the translation groups in the automorphism group. However this result will be even improved in the subsequent section by Corollary 5.13. In the sequel we also pin down the action of this group on the underlying $\mathbb{F}_2$-space. In particular we show that the ambient space of an n-dimensional dual hyperoval has a dimension $\geq 3(n-1)$ (Theorem 4.10), if the hyperoval admits more than one translation group. The analogous assertion holds for APN functions too.

In Chapter 5 we give extension constructions of dimensional dual hyperovals (Theorem 5.1) and APN functions (Theorem 5.3). These lead to examples of dimensional dual hyperovals and APN functions whose automorphism groups contain more than one translation group. Nontrivial nuclei of dual hyperovals will provide a useful criterion for the existence of more than one translation group. We also show that each dimensional dual hyperovals or APN function, which admits more than one translation group, can be recovered as an extension of a dimensional dual hyperoval or an extension of an APN function respectively (Theorem 5.10).

In Chapter 6 we provide concrete examples of dimensional dual hyperovals and APN functions which admit at least two translation groups.

We always assume that hyperovals are at least 4-dimensional and APN functions are defined on at least 4-dimensional spaces since for $n \leq 3$ some special phenomena can occur. Indeed the appendix addresses the n-dimensional dual hyperovals for $n \leq 3$ (which are all known) and explains these special phenomena.

2 APN functions and dual hyperovals with translation groups

Notation. The group theoretic notation of our text follows standard references like [10], [12], or [16]. Linear transformations are usually denoted by Greek letters and, following the conventions of group theory, we write them on the right side of their argument. Also, if U is a vector space and H a group (set) of invertible linear operators, the fixed points of H on U are denoted by

$$C_U(H) = \{u \in U \mid u\sigma = u, \text{ all } \sigma \in H\},$$

while the space

$$[U, H] = \langle [u, \sigma] \mid u \in U, \ \sigma \in H \rangle,$$

with $[u, \sigma] = u(1 - \sigma)$, is called the *commutator* of U and H.

Definition. Let U be an $n + m$-dimensional space over $\mathbb{F}_2$, $n > 1$, $m \geq 1$.

(a) A set $\mathcal{S}$ of size 2^n of n-dimensional subspaces of U is called a *dimensional* or *n-dimensional dual hyperoval* if for any $S \in \mathcal{S}$ and any one-dimensional subspace V of S there exists precisely one $S' \in \mathcal{S}$ such that $V = S \cap S'$. We also denote a dimensional dual hyperoval by the symbol DHO. We call $\langle \mathcal{S} \rangle$ the *ambient space* of the DHO. If Y is a subspace of U such that $Y \oplus S = U$ for all $S \in \mathcal{S}$ then we say that the DHO *splits* over Y. The group

$$\mathrm{Aut}(\mathcal{S}) = \{\sigma \in \mathrm{GL}(\langle \mathcal{S} \rangle) \mid \mathcal{S}\sigma = \mathcal{S}\}$$

is the *automorphism group* of $\mathcal{S}$. A subgroup $T \leq \mathrm{Aut}(\mathcal{S})$ which acts regularly on $\mathcal{S}$, such that the DHO splits over $Y = C_U(T)$, is called a *translation group* of the DHO. Clearly, $|T| = 2^n$.

(b) Let $U = X \oplus Y$, $\dim X = n$. A function $f : X \to Y$ is called an *almost perfect nonlinear function* or an *APN function* if for $0 \neq a \in X$ and $b \in Y$ the equation

$$f(x + a) + f(x) = b$$

has at most two solutions. Note that if x is a solution then $x + a$ is a second solution. The set

$$\mathcal{S}_f = \{x + f(x) \mid x \in X\}$$

is the *graph of f*. Two APN functions $f, g : X \to Y$ are *equivalent* if there exists an affine isomorphism of U which maps $\mathcal{S}_f$ onto $\mathcal{S}_g$. The APN function f is *normed* if $f(0) = 0$. Clearly, every APN function is equivalent to a normed APN function. Let f be normed. The space $\langle \mathcal{S}_f \rangle$ is the *ambient space* of the APN function. The *automorphism group* $\mathrm{Aut}(f)$ is the stabilizer of $\mathcal{S}_f$ in $\mathrm{AGL}(\langle \mathcal{S}_f \rangle)$. We say that the normed APN function f *splits* over the subspace W of U iff $\dim W = m$ and $\mathcal{S}_f \cap W = 0$.

(c) 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

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

From now on we always assume that APN functions are normed. We will also assume that the ambient space of a DHO, or an APN function, coincides with the space U on which they are defined.

We note that the automorphism group of a DHO $\mathcal{S}$ (of an APN function f) acts faithfully as a permutation group on $\mathcal{S}$ (on $\mathcal{S}_f$). For the case of a DHO see [26, Lemma 4.1] while for the case of an APN function the property follows from the fact that $\mathcal{S}_f$ contains 0 and a basis of the ambient space.

Before we can define translation groups for APN functions we need:

Lemma 2.1. *Assume the notation of the definition and let f be an APN function. 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.*

Proof. Let $\overline{\tau} = \mathbf{1} + c_\tau \in \ker \phi$. Assume $c_\tau \neq 0$. For $x \in X$ we get $(x + f(x))\overline{\tau} = x + c_X + f(x) + c_Y \in \mathcal{S}_f$, where c_X and c_Y are the projections of c_τ into X and Y. Hence $f(x + c_X) = f(x) + c_Y$ for $x \in X$. Clearly, $c_X \neq 0$. So $|X| \leq 2$ by the APN property, a contradiction as $n > 1$. $\square$

Definition and Remark. We denote by $\mathrm{A}(f)$ the image of $\mathrm{Aut}(f)$ under ϕ and call it the *linear part of the automorphism group* of f. We constantly will make use of the isomorphism

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

So for any $\tau \in \mathrm{A}(f)$ there exists a unique $c_\tau \in U$ such that $\overline{\tau} = \tau + c_\tau$ lies in $\mathrm{Aut}(f)$. We also call $\overline{\tau}$ the *pre-image* of τ. Since

$$\sigma\tau + c_{\sigma\tau} = \overline{\sigma\tau} = \overline{\sigma}\,\overline{\tau} = \sigma\tau + c_\sigma\tau + c_\tau$$

we observe that the map $c : \mathrm{A}(f) \to U$, $\tau \mapsto c_\tau$, is an 1-cocycle. Let $\overline{T}$ be a subgroup of $\mathrm{Aut}(f)$ and T its the linear part. We call $\overline{T}$ or T a *translation group* if $\overline{T}$ acts regularly on $\mathcal{S}_f$ and f splits over $C_U(T)$. Clearly, $|T| = 2^n$.

Definition. Let $U = X \oplus Y$, $\dim X = n$, and $\dim Y = m$.

(a) Let $\mathcal{S}$ be an n-dimensional DHO in U which splits over Y. Then there exists an injection $\beta : X \to \mathrm{Hom}(X, Y)$ such that

$$\mathcal{S} = \{S_e \mid e \in X\}, \quad \text{where} \quad S_e = \{x + x\beta(e) \mid x \in X\}.$$

If in addition the mapping β is linear, one calls $\mathcal{S}$ a *bilinear* DHO. In fact then the mapping

$$X \times X \to Y, \quad (x, e) \mapsto x\beta(e)$$

is bilinear. Bilinearity guarantees the existence of at least one translation group, the *standard translation group (with respect to β)* $T = T_\beta = \{\tau_e \mid e \in X\} \leq \mathrm{GL}(U)$ with

$$(x + y)\tau_e = x + y + x\beta(e), \quad x \in X, \quad y \in Y.$$

We call a bilinear DHO defined by β *symmetric* if

$$x\beta(e) = e\beta(x), \quad x, e \in X,$$

and *alternating* if in addition

$$x\beta(x) = 0, \quad x \in X,$$

holds.

(b) Let $f : X \to Y$ be a *quadratic* APN function, i.e. an APN function f such that the mapping

$$X \times X \to Y, \quad (x, e) \mapsto f(x + e) + f(x) + f(e)$$

is bilinear. For $e \in X$ define $\overline{\tau}_e = \tau_e + c_e \in \mathrm{AGL}(U)$, $c_e = e + f(e)$, by

$$(x + y)\tau_e = x + y + f(x + e) + f(x) + f(e), \quad x \in X, \quad y \in Y.$$

Then $\overline{\tau}_e$ is an automorphism of f and the group

$$\overline{T} = \overline{T}_f = \{\overline{\tau}_e \,|\, e \in X\}$$

is a translation group of f, the *standard translation group of f with respect to Y*.

Example 2.2. Let $X = \mathbb{F}_q$, $q = 2^n$, $n \geq 3$.

(a) Typical examples of bilinear DHOs are the DHOs of Yoshiara [24] which are defined by $\beta : X \to \mathrm{Hom}(X, X)$, $x\beta(e) = x^\sigma e + xe^\tau$, where σ and τ are suitably chosen field automorphisms of X. A survey article with more examples of DHOs is [27]. Other bilinear DHOs can be found in [5].

(b) Typical examples of quadratic APN functions are the Gold functions $f : X \to X$ defined by $f(x) = x^{2^k+1}$, $(k, n) = 1$. An account of APN functions in small dimensions can be found in [8].

Notation. Let X and Y be finite dimensional $\mathbb{F}_2$-spaces. Let α be in $\mathrm{Hom}(X, \mathrm{Hom}(X, Y))$. Then α defines canonically a bilinear map $X \times X \to Y$ by $(x, x') \mapsto x\alpha(x')$ and $\mathrm{Hom}(X, \mathrm{Hom}(X, Y))$ can be identified with the vector space of bilinear mappings from X to Y. The elements α which are symmetric form the subspace $\mathrm{Hom}(X, \mathrm{Hom}(X, Y))_{sym}$ of symmetric bilinear mappings and the elements α which are alternating form the subspace $\mathrm{Hom}(X, \mathrm{Hom}(X, Y))_{alt}$ of alternating bilinear mappings. The following lemma is well known and has a straightforward verification (using the dimensions of the spaces of bilinear, symmetric and alternating mappings).

Lemma 2.3. *Let X and Y be finite dimensional $\mathbb{F}_2$-spaces and $\alpha \in \mathrm{Hom}(X, \mathrm{Hom}(X, Y))$. Define $\alpha^t \in \mathrm{Hom}(X, \mathrm{Hom}(X, Y))$ by $x\alpha^t(x') = x'\alpha(x)$. The following holds.*

(a) The mapping $\alpha \mapsto \alpha + \alpha^t$ is an epimorphism of $\mathrm{Hom}(X, \mathrm{Hom}(X, Y))$ onto $\mathrm{Hom}(X, \mathrm{Hom}(X, Y))_{alt}$ whose kernel is $\mathrm{Hom}(X, \mathrm{Hom}(X, Y))_{sym}$.

(b) For $\sigma \in \mathrm{Hom}(X, \mathrm{Hom}(X, Y))_{sym}$ define $\lambda_\sigma : X \to Y$ by $x\lambda_\sigma = x\sigma(x)$. Then λ is an epimorphism of $\mathrm{Hom}(X, \mathrm{Hom}(X, Y))_{sym}$ onto $\mathrm{Hom}(X, Y)$ which has the kernel $\mathrm{Hom}(X, \mathrm{Hom}(X, Y))_{alt}$.

The following result explains the connection between quadratic APN functions and alternating DHOs. This was already observed in [7] for $n = m$. The direction, that quadratic APN functions define alternating DHOs was already shown in [9] and [28].

Theorem 2.4. *Let X and Y be finite dimensional $\mathbb{F}_2$-spaces.*

(a) Let $f : X \to Y$ be a quadratic APN function. Then $\beta : X \to \mathrm{Hom}(X, Y)$, defined by

$$x\beta(e) = f(x + e) + f(x) + f(e),$$

defines an alternating DHO. There exists an $\alpha \in \mathrm{Hom}(X, \mathrm{Hom}(X, Y))$ such that $\beta = \alpha + \alpha^t$ and $f(x) = x\alpha(x)$.

(b) Let the homomorphism $\beta : X \to \mathrm{Hom}(X, Y)$ define an alternating DHO. Let α be in $\mathrm{Hom}(X, \mathrm{Hom}(X, Y))$ such that $\beta = \alpha + \alpha^t$. Then $f = f_\alpha : X \to Y$, defined by $f(x) = x\alpha(x)$, is a quadratic APN function such that $x\beta(e) = f(x+e)+f(x)+f(e)$. Assume that also $\beta = \gamma+\gamma^t$. Then $f_\alpha+f_\gamma$ is a linear function.

Proof. (a) Clearly, the bilinear form defined by a quadratic APN function is alternating, in particular $\beta(e)$, $e \in X$, is linear. Define in $U = X \oplus Y$ for $e \in X$ the subspace $S_e = \{x + x\beta(e) \,|\, x \in X\}$. The equation $x\beta(d) = x\beta(e)$, $d, e \in X$, $d \neq e$, leads to

$$f(x + d) + f(x + e) = f(d) + f(e)$$

which has only the solutions $x = 0$ and $x = d + e$ as f is an APN function. Hence $S_d \cap S_e = \langle e + d + (e + d)\beta(d)\rangle$ which shows that $\mathcal{S} = \{S_e \,|\, e \in X\}$ is an alternating DHO. Using Lemma 2.3 we choose $\alpha \in \mathrm{Hom}(X, \mathrm{Hom}(X, Y))$ with $\beta = \alpha + \alpha^t$. Define $g : X \to Y$ by $g(x) = x\alpha(x)$. A calculation shows that the function $f + g$ is linear. By (b) of Lemma 2.3 there exists a symmetric $\sigma : X \to \mathrm{Hom}(X, Y)$ such that $(f + g)(x) = x\sigma(x)$. Then $f(x) = x(\alpha + \sigma)(x)$ and $\beta = (\alpha + \sigma) + (\alpha + \sigma)^t$ (as $\sigma^t = \sigma$) and the assertion follows.

(b) Clearly, f is a quadratic function. Let $a \in X - 0$, $b \in Y$. Consider the equation

$$f(x + a) + f(x) = b, \quad \text{i.e.} \quad x\beta(a) = x\alpha(a) + a\alpha(x) = b + a\alpha(a).$$

As β defines a DHO this equation has either 0 or 2 solutions (of the form x and $x + a$ as β is alternating). So f is an APN function.

Assume that γ has been chosen as in the assertion. Then $\sigma = \alpha + \gamma$ is symmetric and thus $f_\gamma = f_\alpha+\lambda_\sigma$ with a linear function λ_σ (see Lemma 2.3). □

Definition. Let $f : X \to Y$ be a quadratic APN function. We call the alternating DHO defined in (a) of Theorem 2.4 the *alternating DHO associated with f*.

Lemma 2.5. *Let X and Y be finite dimensional $\mathbb{F}_2$-spaces.*

(a) *Let $f : X \to Y$ be a quadratic APN function and $\overline{T}$ the standard translation group. Then the normalizer of $\overline{T}$ in the automorphism group is*

$$N_{\mathrm{Aut}(f)}(\overline{T}) = \overline{T} \cdot A$$

with $A = \mathrm{Aut}(f)_{0,Y}$.

(b) *Let the homomorphism $\beta : X \to \mathrm{Hom}(X, Y)$ define a bilinear DHO $\mathcal{S} = \mathcal{S}_\beta$ on $X \oplus Y$. Let T be the standard translation group. Then the normalizer of T in the automorphism group is*

$$N_{\mathrm{Aut}(\mathcal{S})}(T) = T \cdot A$$

with $A = \mathrm{Aut}(\mathcal{S})_{X,Y}$.

Proof. (a) Since $0 \in \mathcal{S}_f$ and as $\overline{T}$ acts regularly on $\mathcal{S}_f$ we get $N_{\mathrm{Aut}(f)}(\overline{T}) = \overline{T} \cdot A$ with $A = N_{\mathrm{Aut}(f)}(\overline{T})_0$. By definition $\mathrm{Aut}(f) \cap \mathrm{A}(f) = \mathrm{Aut}(f)_0$, so that $A \leq \mathrm{A}(f)$. As the image of A under ϕ (ϕ as in Lemma 2.1) lies in $N_{\mathrm{A}(f)}(T)$ and as ϕ is the identity on A we see that A fixes $Y = C_U(T)$, i. e. $A \leq \mathrm{Aut}(f)_{0,Y}$.

We now show that T is the centralizer in $\mathrm{A}(f)$ of U/Y and Y. Since the abelian group $\overline{T}$ acts regularly on $\mathcal{S}_f$ and as $\mathrm{Aut}(f)$ acts faithfully on $\mathcal{S}_f$ we see $C_{\mathrm{Aut}(f)}(\overline{T}) = \overline{T}$ (see [12, II.3.1] or exercise 6, [16], p. 57) and hence $C_{\mathrm{A}(f)}(T) = T$. If $\tau \in \mathrm{A}(f)$ centralizes U/Y and Y then τ centralizes T, i. e. $\tau \in T$. So T is the centralizer of U/Y and Y in $\mathrm{A}(f)$, in particular T is normal in $\mathrm{A}(f)_Y$. This implies by Lemma 2.1 that $\mathrm{Aut}(f)_{0,Y} = \mathrm{A}(f)_{0,Y}$ lies in $N_{\mathrm{Aut}(f)}(\overline{T})$. We deduce $A = \mathrm{Aut}(f)_{0,Y}$.

(b) Since $X \in \mathcal{S} = \mathcal{S}_\beta$ and as T acts regularly and faithfully on $\mathcal{S}$ we get $N_{\mathrm{Aut}(\mathcal{S})}(T) = T \cdot A$ with $A = N_{\mathrm{Aut}(\mathcal{S})}(T)_X$. Similarly as in (a) one observes that the centralizer of Y and U/Y in $\mathrm{Aut}(\mathcal{S})$ is T. This shows that $\mathrm{Aut}(\mathcal{S})_{X,Y}$ normalizes T and $A = \mathrm{Aut}(\mathcal{S})_{X,Y}$ follows. $\square$

3 Properties of translation groups

The main result of this section is that the translation groups of a DHO, or an APN function, form in their automorphism group a conjugacy class of self-centralizing, elementary abelian TI subgroups which have quadratic action on the underlying space (see Theorems 3.2, 3.5, and 3.11). The basis for the common study of translation groups of APN functions and DHOs is described by the following group theoretic property:

Hypothesis A. Let U be an $n + m$-dimensional $\mathbb{F}_2$ space and $T \leq \mathrm{GL}(U)$, $|T| = 2^n$, $n \geq 3$. Then the following hold.

(1) $\dim C_U(T) = m$.

(2) Let σ be in T. Then $\dim C_U(\sigma) = m + 1$ (equivalently $\mathrm{rk}\,(1 + \sigma) = n - 1$) if σ is an involution and $C_U(\sigma) = C_U(T)$ if $|\sigma| > 2$.

(3) $C_U(\sigma) \cap C_U(\tau) = C_U(T)$ for two non-identity elements $\sigma \neq \tau$ in T.

Proposition 3.1. *Let U and $T \leq GL(U)$ satisfy Hypothesis A. The following hold:*

(a) T is elementary abelian.

(b) The group T has a quadratic action on U, i. e. $[U,T] \subseteq C_U(T)$.

Proof. (a) Let σ be a 2-element in $\mathrm{GL}(U)$ of order 2^r. Since $(t-1)^{2^r} = t^{2^r} - 1$ in the polynomial ring over $\mathbb{F}_2$ we can apply the theorem of the Jordan normal form to σ, i.e. $U = U_1 \oplus \cdots \oplus U_s$ with indecomposable, uniserial σ-spaces and all composition factors of an U_i have dimension 1. A moment's thought shows $\dim U_i \leq 2^r$ for all i and there is at least one indecomposable space - say U_s - such that $\dim U_s > 2^{r-1}$.

Suppose that $\sigma \in T$, $|\sigma| = 4$, and decompose U as above into indecomposable σ-spaces. Then $m = \dim C_U(\sigma) = s$. Also $\dim C_{U_i}(\sigma^2) = 2$ if $\dim U_i \geq 2$ and as $\dim C_U(\sigma^2) = m+1$ we conclude that U_m is the only space whose dimension is not 1. Also $\dim U_m \leq 4$. Thus $m + n = m - 1 + \dim U_m \leq m + 3$. Hence $n = 3$, $\dim U_m = 4$, $|T| = 8$, $\langle\sigma\rangle \trianglelefteq T$, and therefore $\langle\sigma^2\rangle \leq Z(T)$ (the only nonabelian groups of order 8 are D_8 and Q_8). We conclude that $X = [U, \sigma^2] = [U_m, \sigma^2]$ has dimension 2 and is invariant under T. Then $|C_T(X)| \geq 4$, $\sigma \notin C_T(X)$, and we have a $\tau \in T - \langle\sigma\rangle$ such that

$$C_U(T) + X = C_U(\sigma) + X \subseteq C_U(\tau), \quad \text{i.e.} \quad C_U(\tau) = C_U(\sigma^2),$$

contradicting (3) of Hypothesis A. Thus T has exponent 2 and is elementary abelian.

(b) Set $Y = C_U(T)$. As every nontrivial element has order 2 we deduce by conditions (2) and (3) of Hypothesis A that $\{C_U(\sigma)/Y \mid 1 \neq \sigma \in T\}$ is the set of points of $\mathrm{PG}(U/Y)$.

Assume now that T acts nontrivially on U/Y, i.e. there is a $\sigma \in T$ such that $\sigma_{U/Y}$ is not the identity. Then there exists nonzero $x_1, x_2 \in U$, $x_1 \not\equiv x_2 \pmod{Y}$ and $y \in Y$, such that $x_1\sigma = x_1 + x_2 + y$. As $x_1 = x_1\sigma^2 = x_1 + x_2 + x_2\sigma$ we have $C_U(\sigma) = \langle x_2, Y\rangle$. There exists $\tau \in T$ such that $C_U(\tau) = \langle x_1, Y\rangle$. As $x_1 \not\equiv x_2$ one has $\sigma \neq \tau$ by property (3). Now $x_1\tau\sigma = x_1\sigma = x_1 + x_2 + y$ and $x_1\sigma\tau = x_1 + x_2\tau + y$. As T is commutative we have $0 = x_1\sigma\tau + x_1\tau\sigma = x_2 + x_2\tau$ hence $C_U(\tau) \supseteq \langle x_1, x_2, Y\rangle$, a contradiction as $\dim C_U(\tau) = m+1$. Thus $[U,T] \subseteq Y$ holds. ☐

Theorem 3.2. *Let $\mathcal{S}$ be an n-dimensional DHO, $n \geq 3$, in the $n+m$-dimensional space U and let T be a translation group of $\mathcal{S}$. Then T satisfies Hypothesis A, i. e. T is elementary abelian and has quadratic action on U. Pick $X \in \mathcal{S}$ and set $Y = C_U(T)$. Let $\tau : X \to T$, $e \mapsto \tau_e$, be any isomorphism from X to T. Then $\beta : X \to \mathrm{Hom}(X,Y)$, defined by $x\beta(e) = [x, \tau_e]$, is a homomorphism, i. e. $\mathcal{S}$ is a bilinear DHO with respect to β and T is the standard translation group.*

Proof. By assumption $X \cap Y = 0$. This shows property (1) of Hypothesis A. Let $1 \neq \tau \in T$. If τ is an involution we have $C_X(\tau) \subseteq X \cap X\tau \subseteq C_X(\tau)$ as $X, X\tau \in \mathcal{S}$, i.e. $C_X(\tau) = X \cap X\tau$ has dimension 1. Assume now $|\tau| > 2$. We claim $C_U(\tau) = Y$. As $Y \subseteq C_U(\tau)$ it suffices to show $C_X(\tau) = 0$ and to assume $|\tau| = 4$. We know $C_X(\tau) \subseteq C_X(\tau^2) = X \cap X\tau^2$. As $X \cap X\tau \cap X\tau^2 = 0$ the claim follows. This implies properties (2) and (3) of the Hypothesis. By Proposition 3.1 the first assertion of the corollary holds. Defining τ and β as above and using the quadratic action we get immediately that β is linear. $\square$

Lemma 3.3. *Let $f : V \to W$ be an APN function. Assume that f has a translation group whose linear part is T. The following hold.*

(a) $U/Y = \{s + Y | s \in \mathcal{S}_f\}$, where $Y = C_U(T)$.

(b) T and $U = V \oplus W$ satisfy Hypothesis A.

Proof. Let $\overline{T}$ be the pre-image of T in $\mathrm{Aut}(f)$. By definition of a translation group property (1) of Hypothesis A is satisfied.

To (a): Since $0 \in \mathcal{S}_f$ we obtain

$$\mathcal{S}_f = \{0\overline{\tau} | \overline{\tau} \in \overline{T}\} = \{c_\tau \,|\, \overline{\tau} = \tau + c_\tau \in \overline{T}\}.$$

Suppose $c_\sigma \equiv c_\tau \pmod{Y}$ for $\sigma, \tau \in T$, $\sigma \neq \tau$. Hence $c_\sigma = c_\tau + y$ with $y \in Y$. Using that c is an 1-cocycle we obtain

$$0 = c_1 = c_{\sigma\sigma^{-1}} = c_\sigma\sigma^{-1} + c_{\sigma^{-1}} = c_\tau\sigma^{-1} + c_{\sigma^{-1}} + y\sigma^{-1} = c_{\tau\sigma^{-1}} + y.$$

So we may assume that $c_\tau = y \in Y$ for some $1 \neq \tau \in T$. But as T acts regularly on the graph $y = c_\tau \in \mathcal{S}_f - \{0\}$, which is impossible as f splits over Y. Assertion (a) follows.

To (b): We turn to the verification of properties (2) and (3) of Hypothesis A. Assume first that σ is an involution. Then $\overline{\sigma}$ is an involution too, showing $c_\sigma \in C_U(\sigma)$. Assume $x \in C_U(\sigma) - \langle c_\sigma, Y\rangle$. Using that $\mathcal{S}_f$ is a set of representatives of U/Y there exists a $1 \neq \tau \in T$, $\sigma \neq \tau$, such that $c_\tau \equiv x \pmod{Y}$. Thus $c_\tau \in C_U(\sigma)$. Again as c is a cocycle

$$c_{\tau\sigma} = c_\tau\sigma + c_\sigma = c_\tau + c_\sigma.$$

We view this equation as an equation among elements from the graph. Hence there exist $0 \neq v, v_1 \in V$, $v \neq v_1$, such that $(v + f(v)) + (v_1 + f(v_1)) = (v + v_1) + f(v + v_1)$. So the equation $f(v + v_1) + f(v) = f(v_1)$ has the solutions 0, v, and $v + v_1$, contradicting the APN property. Hence

$$C_U(\sigma) = \langle c_\sigma, Y\rangle.$$

Assume now $|\sigma| = 4$. Set $\tau = \sigma^2$. Then $C_U(\sigma) \subseteq C_U(\tau) = \langle c_\tau, Y\rangle$. If $c_\tau\sigma = c_\tau$ then

$$c_\sigma\tau + c_\tau = c_{\sigma\tau} = c_{\tau\sigma} = c_\tau + c_\sigma$$

which implies $c_\sigma \equiv c_\tau \pmod{Y}$, a contradiction. Thus $C_U(\sigma) = Y$. But again as $C_U(\sigma) \subseteq C_U(\sigma^2)$ for every $\sigma \in T$ we obtain property (2) of Hypothesis A. Since $c_\sigma \not\equiv c_\tau \pmod{Y}$ for $\sigma \neq \tau$ also property (3) is true. $\square$

Lemma 3.4. *Let $f : V \to W$ be an APN function. Set $U = V \oplus W$ and let Y be a subspace of U isomorphic to W, such that the canonical surjection from U onto U/Y becomes injective, when it is restricted to $\mathcal{S}_f$. Let $U = X \oplus Y$ and π_X (π_Y) the projection of U onto X (Y). Let $\widehat{\pi}_X$ be the restriction of π_X onto $\mathcal{S}_f$. Then $\widehat{\pi}_X : \mathcal{S}_f \to X$ is bijective. Moreover the function $g : X \to Y$ defined by $g(x) = \pi_Y(\widehat{\pi}_X^{-1}(x))$ is an APN function equivalent to f.*

Proof. The bijectivity of $\widehat{\pi}_X$ follows immediately from the assumptions. Let $x + g(x) \in \mathcal{S}_g$. Define $s = \widehat{\pi}_X^{-1}(x) \in \mathcal{S}_f$. Then

$$x + g(x) = \pi_X(s) + \pi_Y(s) = s \in \mathcal{S}_f,$$

i. e. $\mathcal{S}_g \subseteq \mathcal{S}_f$ and equality must hold. Then $\phi = \mathbf{1}$ is an equivalence map, i. e. g is an APN function equivalent to f. □

Theorem 3.5. *Let T be the linear part of a translation group of an APN function $f : V \to W$, $\dim V \geq 3$. Then T satisfies Hypothesis A and the following hold.*

(a) T is elementary abelian and has quadratic action on $U = V \oplus W$.

(b) Let $U = X \oplus Y$, with $Y = C_U(T)$, and let $\tau : X \to T$ be an isomorphism. The function $g : X \to Y$ defined by $g(x) = \pi_Y(c_{\tau_x})$ (here π_Y is the projection into Y with respect to the decomposition $U = X \oplus Y$) is equivalent to f (and hence APN).

(c) The APN function g is quadratic and $\overline{T}$ is the standard translation group of g.

Proof. Assertion (a) follows from Lemma 3.3 and Proposition 3.1.

We know $\mathcal{S}_f = \{c_\tau \mid \overline{\tau} = \tau + c_\tau \in \overline{T}\}$. By assertion (a) of Lemma 3.3 $U/Y = \{s + Y \mid s \in \mathcal{S}_f\}$. Let X be a complement of Y in U and τ as in the theorem. Then g is equivalent to f by Lemma 3.4, assertion (b) follows.

In order to verify that g is quadratic we have to show that the mapping $b : X \times X \to Y$, defined by $b(x, t) = g(x + t) + g(x) + g(t)$, is bilinear. A computation shows

$$b(x, t) = \pi_Y(c_{\tau_x}\tau_t + c_{\tau_x}).$$

Since $c_{\tau_x}\tau_t + c_{\tau_x} = \pi_Y(c_{\tau_x}\tau_t + c_{\tau_x})$ (quadratic action) we obtain (as $g(x)\tau_t = g(x)$)

$$[x, \tau_t] = x + x\tau_t = (c_{\tau_x} + g(x)) + (c_{\tau_x} + g(x))\tau_t = c_{\tau_x}\tau_t + c_{\tau_x} = b(x, t),$$

which shows linearity in x. Since b is invariant under the transposition of the arguments we see that b is bilinear. So indeed $\overline{T}$ is the standard translation group associated with the quadratic APN function g. □

We now show that alternating DHOs admit precisely one translation group. For a DHO $\mathcal{S}$ and $S, S' \in \mathcal{S}$, $S \neq S'$, we denote by $[S \cap S']$ the nontrivial vector in $S \cap S'$. Moreover if $S'' \in \mathcal{S}$, $S \neq S'' \neq S'$, we set

$$p(S, S', S'') = [S \cap S'] + [S \cap S''] + [S' \cap S''],$$

and

$$P(\mathcal{S}) = \langle p(S, S', S'') \,|\, S, S', S'' \in \mathcal{S},\ S \neq S' \neq S'' \neq S \rangle.$$

We have the following generalization of [7, Theorem 1]:

Theorem 3.6. *Let $\mathcal{S}$ be a DHO in the ambient space U. Equivalent are:*

(a) The DHO $\mathcal{S}$ splits with respect to $P(\mathcal{S})$.

(b) There exist a decomposition $U = X \oplus Y$ and a homomorphism $\beta : X \to \mathrm{Hom}(X, Y)$ such that β defines the alternating DHO $\mathcal{S} = \mathcal{S}_\beta$. Moreover $C_U(T) = Y = P(\mathcal{S})$, where T is the standard translation group with respect to β.

Proof. Set $Y = P(\mathcal{S})$.

(a)$\Rightarrow$(b). Pick $X \in \mathcal{S}$. Choose the injection $\beta : X \to \mathrm{Hom}(X, Y)$ such that $\mathcal{S} = \{S_e \,|\, e \in X\}$, $S_0 = X$ (i.e. $\beta(0) = 0$), $S_e = \{x + x\beta(e) \,|\, x \in X\}$, and $[S_0 \cap S_e] = e$ for $0 \neq e \in X$ (i.e. $e\beta(e) = 0$). We have for $0 \neq e, e' \in X$, $e \neq e'$, that $[S_e \cap S_{e'}] = x + y$ where $x \neq 0$ and $x\beta(e) = y = x\beta(e')$. Now

$$Y \ni [S_0 \cap S_e] + [S_0 \cap S_{e'}] + [S_e \cap S_{e'}] = e + e' + x + y$$

which shows $x = e + e'$ and $(e + e')\beta(e) = (e + e')\beta(e')$ or

$$e'\beta(e) = e\beta(e'),$$

as $e\beta(e) = e'\beta(e') = 0$. Since

$$e\beta(x) + e\beta(x') = x\beta(e) + x'\beta(e) = e\beta(x + x')$$

for $x, x', e \in X$, we see that β is linear, i.e. $\mathcal{S}$ is a bilinear DHO. By definition, $\mathcal{S}$ is even alternating with respect to β and $C_U(T) = Y = P(\mathcal{S})$.

(b)$\Rightarrow$(a). By definition $x\beta(x) = 0$ for $x \in X$. This implies $[S_e \cap S_e'] = e + e' + e\beta(e')$ and we see that $C_U(T) = Y = P(\mathcal{S})$. $\square$

Corollary 3.7. *Let $\mathcal{S}$ be an alternating DHO. Every alternating homomorphism which defines the DHO is associated with the same standard translation group. In particular this translation group is normal in* $\mathrm{Aut}(\mathcal{S})$*.*

Proof. Let U be the ambient space. Let $U = X \oplus Y$ and $U = X_1 \oplus Y_1$ be decompositions such that the alternating homomorphisms $\beta : X \to \mathrm{End}(X, Y)$ and $\beta_1 : X_1 \to \mathrm{End}(X_1, Y_1)$ both define $\mathcal{S}$ and $T = T_\beta$ and $T_1 = T_{\beta_1}$ be the corresponding standard translation groups.

Form Theorem 3.6 we deduce $Y = C_U(T) = P(\mathcal{S}) = C_U(T_1) = Y_1$. Then using the quadratic action $T_1 \leq C_{\mathrm{Aut}(\mathcal{S})}(T)$. Thus $T = T_1$ by Proposition 3.8.

As the conjugate of a standard translation group, corresponding to an alternating bilinear form, is again a standard translation group, corresponding to an alternating bilinear form, we have shown that T is normal. $\square$

Recall that a subgroup H of a group G is *self-centralizing* iff $H = C_G(H)$.

Proposition 3.8. *Translation groups of DHOs or APN functions are self-centralizing in their automorphism group.*

Proof. A regular abelian subgroup of the symmetric group $\mathrm{S}(\Omega)$, Ω a finite set, is self-centralizing in $\mathrm{S}(\Omega)$ (see [12, II.3.1] or exercise 6, [16], p. 57). The automorphism group of a DHO is faithfully represented on the DHO (see [27]) and the automorphism group of an APN is faithfully represented on its graph as the graph generates the ambient space. By Theorems 3.2 and 3.5 in both cases translation groups are regular abelian groups. The assertion follows. $\square$

Definition. Let X, Y be finite dimensional $\mathbb{F}_2$-spaces and $\beta : X \to \mathrm{Hom}(X, Y)$ be a homomorphism which defines a bilinear DHO $\mathcal{S}$.

(a) An automorphism of $\mathcal{S}$ fixing X and Y is written as $\mathrm{diag}(\lambda, \rho)$ if $x + y \mapsto x\lambda + y\rho$ with $\lambda \in \mathrm{GL}(X)$ and $\rho \in \mathrm{GL}(Y)$. Such automorphisms are called *autotopisms*. Note that there exists $\mu \in \mathrm{GL}(X)$ such that

$$\beta(e)\rho = \lambda\beta(e\mu)$$

if $S_{e\mu}$ is the image of the space S_e under the autotopism since

$$(x + x\beta(e))\mathrm{diag}\,(\lambda, \rho) = y + y\lambda^{-1}\beta(e)\rho$$

with $y = x\lambda$. It is sometimes convenient to denote an autotopism by a triple (λ, μ, ρ) too.

(b) We say that this autotopism is *special* if $\lambda = \mu$ and we call it *nuclear* $\rho = 1$.

(c) We define the *nucleus* of the DHO as

$$\mathcal{K} = \{(\lambda, \mu) \in \mathrm{End}(X) \times \mathrm{End}(X) \,|\, \lambda\beta(e) = \beta(e\mu),\ e \in X\}.$$

Remarks. (a) The terms "autotopisms", "nuclear" and "nucleus" refer to related definitions in semifield planes (cf. [13]).

(b) Let G be the automorphism group of $\mathcal{S}$ and let T be the translation group induced by β. By Lemma 2.5 the normalizer of T has the form $N_G(T) = T \cdot A$, where A is the group of autotopisms.

(c) The notions "autotopism", "special", etc. depends on the splitting of U as $X \oplus Y$; namely, it depends on the choice of the translation group T with $C_U(T) = Y$. However, since we show later that all translation groups are conjugate, this dependency will become irrelevant.

Proposition 3.9. *With the notation of the definition the following hold:*

(a) The projections of the elements of the nucleus on the first (or the second) components are injective.

(b) The nucleus is a field with component-wise addition and multiplication.

(c) The mapping $\mathcal{K}^* \ni (\lambda, \mu) \to (\lambda, \mu^{-1}, 1)$ *(which corresponds to* $\mathrm{diag}(\lambda, 1)$*) is a isomorphism of the multiplicative group of the nucleus onto the group of nuclear autotopisms.*

(d) Let β *be symmetric and* (λ, μ, ρ) *an autotopism. Then* (μ, λ, ρ) *is an autotopism too.*

(e) Let β *be alternating. Then every autotopism is special.*

(f) Let β *be alternating. The nucleus is isomorphic to* $\mathbb{F}_2$ *or* $\mathbb{F}_4$*. If the second case occurs* $\dim X$ *is even.*

Proof. Clearly, $(0,0), (1,1)$ are elements of the nucleus and the nucleus is closed under component-wise addition.

Suppose, λ is not invertible for $(\lambda, \mu) \in \mathcal{K}$. Let $0 \neq e \in X$ lie in the kernel of λ. Then for all $f \in X$ we get $0 = e\lambda\beta(f) = e\beta(f\mu)$. This shows that the rank of μ can be at most 1 (by the DHO property for $e \neq 0$ the linear mapping $x \mapsto e\beta(x)$ has rank $n-1$). So there exists a hyperplane H of X such that $0 = x\beta(f\mu) = x\lambda\beta(f)$ for all $x \in X$ and $f \in H$. We deduce $\lambda = 0$ which implies that $\beta(e\mu) = 0$ for all $e \in X$ or $(\lambda, \mu) = (0, 0)$. Similarly, if μ is not invertible, we get the same equation. This shows (a) and that the components of elements in $\mathcal{K}^*$ are elements of $\mathrm{GL}(X)$.

Form

$$\lambda\lambda'\beta(e) = \lambda\beta(e\mu') = \beta(e\mu'\mu)$$

we deduce that the nucleus is closed under the multiplication

$$(\lambda, \mu)(\lambda', \mu') = (\lambda\lambda', \mu'\mu).$$

It is obvious that (λ^{-1}, μ^{-1}) is the inverse of (λ, μ). Since the projection of the nucleus to the first component is a homomorphism, we conclude that $\mathcal{K}$ is a finite skew field, i. e. a finite field by Wedderburn's theorem. In particular we can interchange the roles of μ and μ' in the above multiplication rule. This implies (a) and (b) while (c) follows from the definition of the nucleus.

Let β be symmetric and (λ, μ, ρ) an autotopism. Then

$$y\mu\beta(x\lambda) = x\lambda\beta(y\mu) = x\beta(y)\rho = y\beta(x)\rho$$

for all $x, y \in X$ which shows (d). If β is even alternating then $0 = e\beta(e)\rho = e\lambda\beta(e\mu)$ implies that $e\lambda$ generates the kernel of $\beta(e\mu)$ and since $\mathcal{S}$ is an alternating DHO $e\lambda = e\mu$ and (e) follows.

To (f): By (e) nuclear autotopisms have the form $(\lambda, \lambda, 1)$, i. e. the nontrivial elements of the nucleus have the form (λ, λ^{-1}). Thus the field $F = \{0\} \cup \{\lambda \mid (\lambda, \lambda^{-1}) \in \mathcal{K}^*\}$ admits an automorphism $0 \mapsto 0$, $F^* \ni \lambda \mapsto \lambda^{-1} \in F^*$.

Assume $0, 1 \neq x \in F$. Then $x^{-1} + 1 = (x+1)^{-1}$, which leads to $x^2 + x + 1 = 0$, i. e. $|x| = 3$. So $\mathcal{K} \simeq F \simeq \mathbb{F}_2$ or $\simeq \mathbb{F}_4$. Assume $F \simeq \mathbb{F}_4$. Clearly, X is an F-vector space (as $\mathcal{K}$ is represented faithfully as a *field* on X). Thus $\dim_{\mathbb{F}_2} X = 2 \cdot \dim_{\mathbb{F}_4} X$. This shows the second assertion of (f). □

Definition and Remark. (a) Let (λ, μ) be an element of the nucleus $\mathcal{K}$ of a *symmetric* bilinear DHO. By (b) and (c) of Proposition 3.9 also $(\mu, \lambda) \in \mathcal{K}$ and $\iota : \mathcal{K} \ni (\lambda, \mu) \mapsto (\mu, \lambda) \in \mathcal{K}$ is a field automorphism of order ≤ 2. We call the set of fixed points $\mathcal{K}_0 = \{(\lambda, \mu) \in \mathcal{K} | \lambda = \mu\}$ the *symmetric nucleus* of the DHO. In particular either $|\iota| = 1$ and $\mathcal{K}_0 = \mathcal{K}$ or $|\iota| = 2$ and $|\mathcal{K}_0|^2 = |\mathcal{K}|$. If the DHO is even alternating then $\mathcal{K}_0 \simeq \mathbb{F}_2$ by (e) of Proposition 3.9. The relevance of the symmetric nucleus becomes apparent in Theorem 5.7.

(b) Some alternating DHOs associated with Gold APN-functions have a nucleus isomorphic to $\mathbb{F}_4$ (see Example 6.4).

Theorem 3.10. *Let X and Y be finite dimensional $\mathbb{F}_2$-spaces and $f : X \to Y$ a quadratic APN function. Let $\mathcal{S}$ be the associated alternating DHO. Then*

$$\mathrm{Aut}(\mathcal{S}) \simeq N_{\mathrm{Aut}(f)}(\overline{T})$$

where $\overline{T}$ is the standard translation group in $\mathrm{Aut}(f)$.

Proof. Set $U = X \oplus Y$ and define $\beta : X \to \mathrm{Hom}(X, Y)$ as in Theorem 2.4, i. e. $\mathcal{S} = \mathcal{S}_\beta$ is the associated DHO to f. By Corollary 3.7 and Lemma 2.5

$$\mathrm{Aut}(\mathcal{S}) = T \cdot A$$

where T is the standard translation group and $A = \mathrm{Aut}(\mathcal{S})$ is the group of autotopisms. Recall that $T = \{\tau_e \,|\, e \in X\}$, $(x + y)\tau_e = x + y + x\beta(e)$ and by (e) of Proposition 3.9 the elements in A have the form $\mathrm{diag}\,(\lambda, \rho)$ such that $\lambda\beta(e\lambda) = \beta(e)\rho$. Again by Lemma 2.5

$$N_{\mathrm{Aut}(f)}(\overline{T}) = \overline{T} \cdot L$$

where $\overline{T}$ is the standard translation group and $L = \mathrm{Aut}(f)_{0,Y}$. Typical elements in $\overline{T}$ have the form $\overline{\tau}_e = \tau_e + c_e$, $c_e = e + f(e)$. An element $\phi \in L$ is written formally as

$$\phi = \begin{pmatrix} \lambda & \gamma \\ & \rho \end{pmatrix} \quad \text{where} \quad x + y \mapsto x\lambda + x\gamma + y\rho,$$

with $\lambda \in \mathrm{GL}(X)$, $\rho \in \mathrm{GL}(Y)$ and $\gamma \in \mathrm{Hom}(X, Y)$ such that $f(x\lambda) = x\gamma + f(x)\rho$.

Define

$$\Psi : N_{\mathrm{Aut}(f)}(\overline{T}) \to \mathrm{GL}(U) \quad \text{by} \quad \overline{\tau}_e\phi \mapsto \tau_e \mathrm{diag}\,(\lambda, \rho).$$

A calculation shows that Ψ is an homomorphism and of course T is the image of $\overline{T}$ under Ψ. Moreover, since γ is linear, and using $f(x\lambda) = x\gamma + f(x)\rho$, we see for $x, e \in X$ that

$$x\beta(e)\rho = x\lambda\beta(e\lambda)$$

showing by Proposition 3.9 that $\mathrm{diag}\,(\lambda, \rho)$ is an autotopism. So $L\Psi \leq A$, i. e. $\mathrm{Im}\,\Psi \leq \mathrm{Aut}(\mathcal{S})$. It remains to show that every element in A is an image of an element in L.

Choose $\alpha \in \mathrm{Hom}(X, \mathrm{Hom}(X, Y))$ such that $\beta = \alpha + \alpha^t$ and $f(x) = x\alpha(x)$ (Theorem 2.4) and let $\mathrm{diag}\,(\lambda, \rho)$ be an element in A. By (e) of Proposition 3.9 we have $\beta(e)\rho = \lambda\beta(e\lambda)$ which implies

$$\lambda\alpha(e\lambda) + \alpha(e)\rho = \lambda\alpha^t(e\lambda) + \alpha^t(e)\rho.$$

Hence $\kappa : X \to \mathrm{Hom}(X, Y)$ defined by

$$\kappa(e) = \lambda\alpha(e\lambda) + \alpha(e)\rho$$

is symmetric. Thus $\gamma : X \to Y$ defined by

$$x\gamma = x\kappa(x)$$

is linear (see (b) of Lemma 2.3). Set $\phi = \begin{pmatrix} \lambda & \gamma \\ & \rho \end{pmatrix}$. Now for $x \in X$ we have

$$(x + f(x))\phi = x\lambda + x\gamma + x\alpha(x)\rho = x\lambda + (x\lambda)\alpha(x\lambda) = x\lambda + f(x\lambda)$$

which implies $\phi \in L$. Hence $\phi\Psi = \mathrm{diag}\,(\lambda, \rho)$ and the proof is complete. □

Autotopisms of quadratic APN functions. Let $f : X \to Y$ be a quadratic APN function, $\overline{T}$ the standard translation group, and $\mathcal{S}$ the associated alternating DHO. We use the preceding theorem to translate the terms autotopisms and nucleus from DHOs to APN functions: We know by this theorem that $N_{\mathrm{Aut}(f)}(\overline{T}) = \overline{T}L$, $L = \mathrm{Aut}(f)_{0,Y} \leq \mathrm{A}(f)$. As we have seen a typical element in L has the shape $\begin{pmatrix} \lambda & \gamma \\ & \rho \end{pmatrix}$ with $\lambda \in \mathrm{GL}(X)$, $\rho \in \mathrm{GL}(Y)$, and $\gamma \in \mathrm{Hom}(X, Y)$. Moreover, for all $x \in X$ the equation

$$f(x\lambda) = x\gamma + f(x)\rho$$

holds. By the proof of Theorem 3.10 we know that

$$L \ni \begin{pmatrix} \lambda & \gamma \\ & \rho \end{pmatrix} \mapsto \mathrm{diag}(\lambda, \rho) \in \mathrm{Aut}(\mathcal{S})_{X,Y}$$

is an isomorphism on the autotopism group of $\mathcal{S}$. Therefore we call the elements of L *autotopisms of* f and such an element is *nuclear* if its image in $\mathrm{Aut}(\mathcal{S})_{X,Y}$ is nuclear.

The following group theoretic notion is central:

Definition. A subgroup $T \neq 1$ of the group G is called a *TI group* if for $\sigma \in G$ either $T = T^\sigma$ or $T \cap T^\sigma = 1$ holds.

Theorem 3.11. *Let $n > 3$. The translation groups of an n-dimensional DHO over $\mathbb{F}_2$ and the translation groups of an APN function defined on an n-dimensional $\mathbb{F}_2$-space, respectively, form a conjugacy class of self-centralizing, elementary abelian TI subgroups in their automorphism group.*

Proof. Let G be the automorphism group of the DHO (the linear part of automorphism group of the APN function) and T a (linear part of a) translation group. By Proposition 3.8 we have $C_G(T) = T$. Note also that $C_U(T) = C_U(\sigma) \cap C_U(\tau)$ for $1 \neq \sigma, \tau \in T$, $\sigma \neq \tau$ since Hypothesis A is satisfied by Theorems 3.2 and 3.5. We claim next: Let T, T' be two different translation groups. Then $T \cap T' = 1$.

Assume $1 \neq T \cap T'$. Set $U_0 = C_U(T) \cap C_U(T')$, $U_1 = C_U(T) + C_U(T')$, and $H = \langle T, T' \rangle$. We have $C_U(T) \neq C_U(T')$ as otherwise $T' \leq C_G(T)$ (quadratic action) which contradicts Proposition 3.8. By Proposition 3.1 we infer that H acts trivially on U_0 and U/U_1.

Let $1 \neq \sigma \in T \cap T'$. Then $U_1 \leq C_U(\sigma)$, i.e. $\dim U_1 \leq m + 1$. Hence $\dim U_0 \geq m - 1$ and $\dim U_1/U_0 \leq 2$ and in both cases equality holds since $C_U(T) \neq C_U(T')$.

Case 1. T is not a Sylow 2-subgroup in H. Let $T \leq S$, $S \in \mathrm{Syl}_2(H)$. Then $T < N_S(T)$ (see [10, 1.2.11] or [16, 3.1.10]). Choose $\sigma \in N_S(T) - T$ such that σT has order 2 in $N_S(T)/T$. We may assume $|\sigma| \geq 4$: If σ is an involution there exists by Proposition 3.8 a τ in T which does not commute with σ. We can replace σ by $\sigma\tau$. As U/U_1 is centralized by H we have $U(1+\sigma) \subseteq U_1$ and since $U_0 \subseteq C_{U_1}(H)$ and $1 + \sigma^2 = (1+\sigma)^2$ we see that

$$\dim U(1+\sigma^2) \leq \dim U_1(1+\sigma) \leq \dim U_1/U_0 = 2.$$

But since σ^2 is a nontrivial element in T we get, as by Hypothesis A $\dim C_U(\sigma^2) = m + 1$,

$$n - 1 = \mathrm{rk}\,(1+\sigma^2) \leq 2,$$

a contradiction. So we have:

Case 2. T is a Sylow 2-subgroup of H. Denote by Q the normal subgroup of the elements of H which act trivially on U_1/U_0. Then Q is a 2-group since Q stabilizes the series $0 \subset U_0 \subset U_1 \subset U$ (see [10, 5.3.3]). Then, as T and T' are Sylow 2-subgroups of H, we have $Q \leq T \cap T'$. Moreover H/Q is isomorphic to a subgroup of $\mathrm{GL}(U_1/U_0) \simeq \mathrm{GL}(2,2) \simeq \mathrm{S}_3$. Now $Q = T \cap T'$ and $H/Q \simeq \mathrm{S}_3$ follows. Also $Q \leq Z(H)$ as H is generated by T and T'.

Let R be a Sylow 3-subgroup of H. Consider the group $R \times Q$ of order $3 \cdot 2^{n-1}$. The group Q (the group $\overline{Q}$) has two orbits, say $\mathcal{B}_1$, $\mathcal{B}_2$ on the DHO $\mathcal{S}$ (on the graph $\mathcal{S}_f$). The group R (the group $\overline{R}$) must fix both orbits as R centralizes Q and has order 3. The group Q (group $\overline{Q}$) acts regularly on both orbits, i.e. this group restricted to $\mathcal{B}_i$ is self-centralizing in the symmetric group $\mathrm{S}(\mathcal{B}_i)$ (see [12, II.3.1] or exercise 6, [16], p. 57). Thus the restriction of R (of $\overline{R}$) acts trivially on both orbits, i.e. on $\mathcal{S}$ (on $\mathcal{S}_f$), a contradiction.

We now know that the translation groups are TI subgroups. Let T be a translation group which lies in the Sylow 2-subgroup S of G. Then $1 \neq Z(S) \leq$

T, as $Z(S) = C_S(S) \leq C_G(T) = T$. This shows that a Sylow 2-subgroup contains at most one and thus precisely one translation group (Sylow's theorem). The translation groups are therefore all conjugate. □

Remark. Corollary 3.7 and the theorem show that, for $n \geq 4$, a n-dimensional alternating DHO, contains precisely one translation group. In Sections 5 and 6 we will provide examples of DHOs which admit more than one translation group.

CCZ equivalence, EA equivalence and all that. Assume that for two functions $f : X \to Y$ and $g : X \to Y$ there exists $\overline{\gamma} \in \mathrm{AGL}(U)$, $U = X \oplus Y$, with $\mathcal{S}_g = \mathcal{S}_f\overline{\gamma}$, i. e. f and g are equivalent. Let γ be the linear part of $\overline{\gamma}$. One calls f and g *affine equivalent* iff γ fixes X and Y and *extended affine equivalent* or *EA equivalent* iff γ fixes Y. Whereas the more general notion of equivalence often is called *CCZ equivalence*. Suppose now that f and g are quadratic APN functions and that $\overline{\gamma}$ is a CCZ equivalence map from $\mathcal{S}_f$ onto $\mathcal{S}_g$. Let T_f be the linear part of the standard translation group of f. Then $\gamma^{-1}T_f\gamma$ is the linear part of a translation group of g. Hence there exists an $\alpha \in \mathrm{A}(g)$ with $T_g = \alpha^{-1}\gamma^{-1}T_f\gamma\alpha$ where T_g is the linear part of the standard translation group of g. Set $\delta = \gamma\alpha$. Then

$$Y\delta = C_U(T_f)\delta = C_U(\delta^{-1}T_f\delta) = C_U(T_g) = Y.$$

Hence $\overline{\delta}$ is an EA equivalence map form $\mathcal{S}_f$ onto $\mathcal{S}_g$. We summarize (using Theorem 3.11):

Theorem 3.12. *Let $f : X \to Y$ and $g : X \to Y$ be quadratic APN functions,* $\dim X \geq 4$. *Then f and g are CCZ equivalent iff they are EA equivalent.*

This generalizes [30, Theorem 1] (special case $m = n$) and [1, Theorem 8] (special case $m = n$ for a restricted class of functions). A DHO version of the preceding theorem is:

Proposition 3.13. *Two n-dimensional, bilinear DHOs $\mathcal{S}_\beta$ and $\mathcal{S}_\gamma$, $n \geq 4$, are isomorphic iff they are isotopic, i. e. if there exists a triple (λ, μ, ρ) of invertible operators such that $\beta(e)\rho = \lambda\gamma(e\mu)$ for all e.*

The following generalizes [20, Proposition 3] from the case $m \leq n$ to the case that m is arbitrary.

Corollary 3.14. *A n-dimensional, bilinear DHO $\mathcal{S}_\beta$, $n \geq 4$, is isomorphic to an alternating DHO iff the map*

$$e \mapsto \begin{cases} 0, & e = 0, \\ [\ker \beta(e)], & e \neq 0, \end{cases}$$

is linear.

Here again $[K]$ denotes the nontrivial vector of the 1-dimensional vector space K.

Proof. It is sufficient to deal with $e \neq 0$. If $\mathcal{S}_\beta$ is isomorphic to an alternating DHO, then, by the proposition, there exists also an isotopism (λ, μ, ρ) to this alternating DHO. Hence $\lambda\beta(e\mu)\rho^{-1}$ is alternating, thus $e \mapsto [\ker \beta(e)] = e\mu\lambda^{-1}$ is linear.

Assume now the map $\kappa : e \mapsto [\ker \beta(e)]$ is linear. By the DHO condition κ is a permutation. The image of β under the isotopism $(\kappa, 1, 1)$ is alternating. $\square$

4 Groups generated by translation groups

In this section we study the structure of the automorphism groups of a DHO or an APN function which contain more than one translation group. Starting point for our investigation is Theorem 3.11. It will allow us to use the structure result of Timmesfeld on weakly closed TI subgroups [23]. Together with structure results of finite simple groups we are then in the position to pin down, to a great extend, the structure of the group G^*, the group generated by translation groups. For the most part the case of DHOs and the case of APN functions can be handled simultaneously. But to describe the operation of G^* on the underlying vector space both cases must be treated differently. The next lemma is (implicitly) contained in [23]. For convenience we provide a proof.

Lemma 4.1. *Let T be a TI subgroup of the finite group G and assume that T is self-centralizing and an elementary abelian 2-subgroup. Let N be a nontrivial, elementary abelian, normal 2-subgroup in G. Then the following holds:*

(a) $1 \neq C_N(T) = T \cap N$.

(b) $T \trianglelefteq NT$ *and* $[T, N] \leq T \cap N$.

(c) TN/N *is a TI-subgroup of* G/N.

Proof. (a) As NT is a 2-group with the normal subgroup N we have $1 \neq N \cap Z(NT) \leq C_N(T) \leq C_G(T) = T$. Hence $1 \neq C_N(T)$ and as $N \cap T \leq C_N(T) \leq T$ the assertion follows.

(b) Suppose T is not normal in NT. Choose $1 \leq N_1 < N_2 \leq N$, such that $|N_2 : N_1| = 2$ and $T \trianglelefteq N_1T$, but T is not normal in N_2T. Then $T \neq T^\nu$ for $\nu \in N_2 - N_1$ and T, T^ν are normal subgroups of N_1T (note that N_1T is normal in N_2T as $|N_2T : N_1T| \leq 2$). Then TT^ν is a 2-group and hence $1 \neq C_T(T^\nu) \leq T^\nu$. Hence $T = T^\nu$, a contradiction. The second assertion is a consequence of the first one.

(c) Suppose $T \neq T^\gamma$, $TN/N \cap T^\gamma N/N \neq 1$. Then there exist $\tau, \tau_1 \in T - N$ and some $\nu \in N$ such that $\tau^\gamma = \tau_1\nu$. Using (b)

$$[\tau^\gamma, N] = [\tau_1, N] \leq T^\gamma \cap T \cap N = 1.$$

This shows $\tau^\gamma \in T^\gamma \cap N$ by (a), a contradiction. $\square$

Remark. By (2.11) of [23] the group TN/N is even a self-centralizing TI subgroup of G/N, if N lies in the maximal normal 2-subgroup of the group G^*, where G^* is the group generated by the conjugates of T.

Lemma 4.2. *Let T be a TI subgroup of the finite group G and assume that T is an elementary abelian 2-subgroup. Let $G = NT$, $N = O(G)$. Then $|T| = 2$ or $T \leq Z(G)$ (i. e. $G = T \times N$).*

Proof. Assume that G is a minimal counter example. In particular T does not lie in $Z(G)$ and $|T| > 2$.

Assume first that N is abelian. Then by a theorem of Suzuki [16, 8.4.2], [10, Theorem 5.2.3]

$$N = N_0 \times N_1, \quad N_0 = C_N(T), \quad N_1 = [N, T].$$

As $|T| > 2$ we deduce from [16, 8.3.4], [10, Theorem 6.2.4], that

$$N_1 = \langle C_{N_1}(\tau) \,|\, 1 \neq \tau \in T \rangle.$$

By assumption $N_1 \neq 1$. So pick $1 \neq \tau \in T$ commuting with $1 \neq \nu \in N_1$. Then $\tau \in T \cap T^\nu$, i. e. $T^\nu = T$. Hence

$$[\nu, T] \leq T \cap N = 1,$$

i. e. $\nu \in C_N(T) \cap N_1 = N_0 \cap N_1 = 1$, a contradiction.

So assume now that N is nonabelian. Then the derived subgroup M of N is a proper subgroup of N by the Odd Order Theorem and hence N/M is a nontrivial abelian group. The group TM satisfies the assumptions and is not a counter example. Thus $M \leq C_N(T)$.

One knows from [16, 8.2.2], [10, Theorem 5.3.5], that $C_{G/M}(TM/M) = C_G(T)M/M$. Moreover TM/M is a TI-subgroup in G/M: If $1 \neq \tau M \in T^\gamma M/M \cap TM/M$ we have that τ lies in a Sylow 2-subgroup of $TM = T \times M$ and $T^\gamma M = T^\gamma \times M$, i. e. $\tau \in T \cap T^\gamma$, i. e. $T = T^\gamma$. Thus G/M satisfies the assumptions of the lemma. By induction $TM/M \leq Z(G/M)$, i. e. $G/M = C_{G/M}(TM/M) = C_G(T)M/M$. This shows $T \leq Z(G)$, a contradiction. ☐

We assume for the remainder of this section, that $n \geq 4$ and that $\mathcal{S}$ is an n-dimensional dual hyperoval or the graph of a quadratic APN function defined on an n-dimensional $\mathbb{F}_2$-space. In both cases U will be the ambient $\mathbb{F}_2$-space and $n + m$ will denote its dimension. If we need to distinguish the two situations we speak of the

DHO case or the **APN case** respectively.

By the symbol $G \leq \mathrm{GL}(U)$ we denote a subgroup of the automorphism group in the DHO case, while in the APN case this is the linear part of a subgroup $\overline{G}$ of the automorphism group. **We assume that $T \leq G$ is a translation group which is not normal in G. In particular**

$$|\mathcal{C}| > 1, \quad \mathcal{C} = \{T^\gamma \,|\, \gamma \in G\}.$$

Finally in the APN case we have the convention: If $H \leq G$ and $S \in \mathcal{S}$ in then

H_S is the linear part of the stabilizer $\overline{H}_S$

Notation. Assume $A \leq H \leq G$ with an abelian 2-group A. One says that A is *strongly closed in H with respect to G* if for every $\alpha \in A$, $\alpha^\gamma \in H$ $(\gamma \in G)$ one has $\alpha^\gamma \in A$.

Lemma 4.3. *Suppose $N_{T^\gamma}(T) = 1$ for all $T^\gamma \in \mathcal{C} - \{T\}$. Then T is strongly closed in $C_G(\tau)$ with respect to G for every $1 \neq \tau \in T$.*

Proof. Let $\gamma \in G$ be such that $\tau^\gamma \in C_G(\tau_1)$ for $1 \neq \tau, \tau_1 \in T$. The group T is weakly closed in $C_G(\tau_1)$ (see the introduction of [23]), in particular T is a normal subgroup of $C_G(\tau_1)$. Thus $\tau^\gamma \in N_{T^\gamma}(T)$. By our assumption $T^\gamma = T$ and hence $\tau^\gamma \in T$. $\square$

Lemma 4.4. *There exists $T^\gamma \in \mathcal{C} - \{T\}$ such that $N_{T^\gamma}(T) \neq 1$.*

Proof. Assume the converse. Then T is strongly closed in every $C_G(\tau)$, $1 \neq \tau \in T$ by Lemma 4.3. Set $G^* = \langle \mathcal{C} \rangle$. By (2.5) of [23] one has $G^* = Z^*(G^*)$, $G^* \simeq \mathrm{L}_2(q)$, $\mathrm{Sz}(q)$, or $G^*/Z(G^*) \simeq \mathrm{U}_3(q)$ for some 2-power q. We know that the first case cannot occur by Lemma 4.2 and as $n > 3$. So we exclude this case. Since $T \leq G^*$ we see that G^* ($\overline{G}^*$ in the APN case) acts transitively on $\mathcal{S}$. In particular G^* has a subgroup of index 2^n. But none of the groups $\mathrm{L}_2(q)$, $\mathrm{Sz}(q)$, or $\mathrm{U}_3(q)$ has a subgroup of 2-power index by [12, II.8.27], [11, p. 157], [17, Thm. 9]. $\square$

Lemma 4.5. *Let $T^\gamma \in \mathcal{C} - \{T\}$ such that $N_{T^\gamma}(T) \neq 1$. Set $H = \langle T, T^\gamma \rangle$. Then one has.*

(a) $N = O_2(H) = L \times L_1$ with $L = N_T(T^\gamma)$ and $L_1 = N_{T^\gamma}(T)$.

(b) $C_N(\tau) = L$ for $\tau \in T - N$. Every involution in $H - N$ is conjugate to τ.

(c) Let $S \in \mathcal{S}$. Then $|H : H_S N| = 2$.

(d) $H/N \simeq \mathrm{D}_{2k}$, $1 < k$ odd.

(e) Let $1 \neq \mu \in H$ be of odd order. Then $C_N(\mu) = 1$.

Proof. By (2.14) of [23] (a) holds and $H/N \simeq \mathrm{D}_{2k}$ (k odd), $\mathrm{L}_2(q)$, or $\mathrm{Sz}(q)$, q a 2-power > 2.

To (b): Let $\tau \in T - N$. By the second section of the proof of [23, (2.14)] we have $C_N(\tau) = L$. As $|[N, \tau]| = |\{\tau^\nu \tau | \nu \in N\}| = |N : C_N(\tau)|$ and $[N, \tau] \leq C_N(\tau)$, we get $C_N(\tau) = [N, \tau]$. This implies that the involutions in the coset $N\tau$ are in $L\tau$ and they are conjugate under N. On the other hand all involutions in H/N are conjugate. Now (b) is verified.

Let $S \in \mathcal{S}$ and assume that we are in the DHO case. In the APN case we replace the linear part H by its affine pre-image $\overline{H}$. All arguments remain unchanged and the assertions follow from Lemma 2.1. We distinguish the cases $H_S N < H$ and $H_S N = H$. We show that in the first case the assumptions of the lemma hold while the second case does not occur.

Case 1 $H_S N < H$. We have $2^n = |H : H_S|$. Thus $|H : H_S N|$ is a nontrivial 2-power. If H is nonsolvable, then the group $\mathrm{L}_2(q)$ or $\mathrm{Sz}(q)$ has a proper subgroup of 2-power index which is excluded as in the proof of the previous lemma. Thus $H/N \simeq \mathrm{D}_{2k}$ and (c) and (d) hold.

To (e): Let C be a cyclic group of order k in H and $1 \neq C_0 = \langle \mu \rangle$ a subgroup of C, say of order k_0. We want to show $C_N(C_0) = 1$. We already know $H_0/N = \langle C_0, T \rangle N \simeq \mathrm{D}_{2k_0}$ for $H_0 = \langle T, T^\mu \rangle$. Assume $1 \neq C_N(C_0)$. Then $1 \neq C_N(C_0) \leq Z(M)$, $M = NC_0$. Since $H_0/M \simeq \mathrm{C}_2$, we even have $1 \neq C_N(M) \cap C_N(T) \leq Z(H_0)$. But $Z(H_0) \leq T \cap T^\mu = 1$, a contradiction. So (e) holds.

Case 2 $H_S N = H$. We know that TN/N is a self-centralizing TI subgroup in H/N (remark after Lemma 4.1). Write $\omega \in (TN \cap H_S) - N$ as $\omega = \tau\eta\eta_1$ with $1 \neq \tau \in T$, $\eta \in L$, and $\eta_1 \in L_1$. If $\eta_1 = 1$, then $1 \neq \omega \in T$, a contradiction. Hence $\eta_1 \neq 1$. Then $\sigma = \omega^2 = [\eta_1, \tau] \neq 1$ and $\sigma \in T \cap H_S$, again a contradiction. □

Theorem 4.6. *Set $G^* = \langle \mathcal{C} \rangle$ and $N = O_2(G^*)$. The following hold:*

(a) The group N is elementary abelian of order 2^{2n-2}.

(b) The group N in the DHO case, respectively the group $\overline{N}$ in the APN case, has two orbits $\mathcal{S}_0$, $\mathcal{S}_1$ on $\mathcal{S}$ such that $|\mathcal{S}_0| = |\mathcal{S}_1| = 2^{n-1}$. Moreover $N = N_0 \times N_1$, where N_i ($\overline{N}_i$ in the APN case) is the pointwise stabilizer of $\mathcal{S}_i$, $i = 0, 1$.

(c) $G^* > G^*_S N$ for $S \in \mathcal{S}$.

(d) Let M be the pre-image of $O(G^*/N)$ in G^*. Then $|G^* : M| = 2$. The group M leaves both orbits $\mathcal{S}_0$ and $\mathcal{S}_1$ invariant, while the elements in $G^* - M$ interchange both orbits.

Proof. By the main result of [23] the group N is elementary abelian. We know that TN/N is an elementary abelian TI group such that $C_{G/N}(TN/N) = TN/N$ (see the remark following Lemma 4.1). We will work in the DHO case. For the APN case one has to replace the linear parts by their affine pre-images. All arguments remain unchanged and the assertions follow from Lemma 2.1. We distinguish the case $G^* > G^*_S N$ and $G^* = G^*_S N$ and show in the first case that the assertions of the theorem hold, whereas the second case does not occur.

Assume first, that $G^* > G^*_S N$ for $S \in \mathcal{S}$ and that G^* is solvable. By the main result of Timmesfeld [23] and Lemma 4.2 we get $|(G^*/N)/O(G^*/N)| = 2$. Thus $|T \cap N| = 2^{n-1}$. Then N is not transitive on $\mathcal{S}$. Otherwise N would be regular (as N is abelian), i. e. $|N| = 2^n$. But if $T \neq T' \leq G^*$ is another translation group we see $1 \neq T \cap T' \cap N$ (as $|T| > 4$), a contradiction. Let $\mathcal{S}_0$ be an orbit of N. Since $T \cap N$ acts semiregularly on $\mathcal{S}$ we get $|\mathcal{S}_0| \geq 2^{n-1}$. Thus we have precisely two orbits both of length 2^{n-1}. Also $|N| \geq |(N \cap T) \times (N \cap T')| = 2^{2n-2}$ for two translation groups $T, T' \leq G^*$. Let N_0 be the kernel of the action of N on $\mathcal{S}_0$. As N is abelian we have $2^{n-1} = |N : N_0|$ and as N_0 acts faithfully and semiregularly on $\mathcal{S}_1$ we see $|N| \leq 2^{2n-2}$. This implies $N = N_0 \times N_1$. Define M as in assertion (d). Since $|M/N|$ is odd the group M leaves each of the orbits $\mathcal{S}_0$ and $\mathcal{S}_1$ invariant. So in this case all assertions of the theorem hold.

Suppose still $G^* > G^*_S N$ but that G^* is nonsolvable. Now $G^*_S N/N$ is a proper subgroup of 2-power index in G^*/N. This index is $\leq 2^n$ as $G^* = G^*_S T$. As in the proof of Lemma 4.4 one sees that G^*/N cannot be the covering group of a Bender group. If G^*/N is the covering group of a group $L_r(2)$ then TN/N is a self-centralizing TI subgroup of order 2^{r-1}, i. e. $|G^*/N : G^*_S N/N| \leq 2^{r-1}$. But by [14, Theorem 1] for $r > 5$ and by [3] for $r = 5$ the index of a maximal subgroup of $L_r(2)$ is $\geq 2^r - 1$. So this case is ruled out too. For the remaining groups the subgroup structure is given by the ATLAS of finite groups [3]. This implies $G^*/N \simeq \mathrm{A}_8 \simeq \mathrm{SL}(4,2)$ or $G^*/N \simeq \mathrm{L}_2(7) \simeq \mathrm{SL}(3,2)$. Also $|TN/N| = 2^2$ or 2^3 if $G^*/N \simeq \mathrm{SL}(3,2)$ or $\simeq \mathrm{SL}(4,2)$ respectively. Since $|T| > 2^3$ we get $N \neq 1$. It suffices to rule out the case $G^*/N \simeq \mathrm{SL}(3,2)$: If $G^*/N \simeq \mathrm{SL}(4,2)$, then this group contains two classes of subgroups (maximal parabolic subgroups), which are the extension of the $\mathrm{SL}(3,2)$ by its natural module $\mathbb{F}_2^3$. Both contain translation groups since they have odd index in G^*/N. So at least one of these subgroups is generated by translation groups. Thus G^* contains a subgroup H^* generated by translation groups such that $H^*/O_2(H^*) \simeq \mathrm{SL}(3,2)$ and we can argue with H^* instead with G^*.

As $|G^* : G^*_S N|$ is a nontrivial 2-power and as $G^*_S N/N$ is isomorphic to a subgroup of $G^*/N \simeq \mathrm{SL}(3,2)$ we conclude that $G^*_S N/N$ is a maximal subgroup of G^*/N, namely a Frobenius group of order 21. We know that N is not transitive on $\mathcal{S}$ as otherwise $G^* = G^*_S N$. Let $\mathcal{S}_0$ be an N-orbit on $\mathcal{S}$, $S \in \mathcal{S}_0$. Then $G^*_S N$ lies in the stabilizer $G^*_{\mathcal{S}_0}$ of the set $\mathcal{S}_0$ and $G^*_{\mathcal{S}_0} < G^*$. The maximality of $G^*_S N$ in G^* shows $G^*_{\mathcal{S}_0} = G^*_S N$. Hence N has precisely $8 = |G^* : G^*_S N|$ orbits on $\mathcal{S}$, each of size $2^n/8 = 2^{n-3}$. On the other hand $|TN/N| = 4$, i. e. $|N \cap T| = 2^{n-2}$ and $N \cap T$ acts semiregularly on $\mathcal{S}_0$. This shows $|\mathcal{S}_0| \geq 2^{n-2}$, a contradiction.

Assume now $G^* = G^*_S N$. Then N is a transitive abelian normal subgroup, i. e. N acts regularly on $\mathcal{S}$. Thus $|N| = 2^n$. Assume that G^* is solvable. Then as before $|T \cap N| = 2^{n-1}$ which is impossible.

So assume that $(G^*/N)/Z(G^*/N)$ is nonabelian simple. By Lemma 4.4 and Lemma 4.5 we have that $\langle TN/N, T^\gamma N/N \rangle$ is solvable for some $TN/N \neq T^\gamma N/N$. Inspecting the list of [23] we see that G^*/N has to be among the following groups $\mathrm{L}_r(2)$, A_6, A_7, A_8, A_9, M_{22}, M_{23}, or M_{24}. Let K be the number of conjugates of TN/N in G^*/N, $2^k = |T \cap N|$. Since the sets $(T^\gamma \cap N) - 1$ are pairwise disjoint

$$(2^k - 1)K \leq 2^n - 1.$$

We claim that $G^*/N \simeq \mathrm{L}_r(2)$ and that N is the natural G^*/N-module:

Assume first $G^*/N \simeq \mathrm{L}_r(2)$. Then $K = 2^r - 1$, $|TN/N| = 2^{r-1}$, i. e. $k = n - r + 1$. Hence $(2^k - 1)(2^r - 1) \leq 2^{k+r-1} - 1$ which implies $k = 1$ and $n = r$. It follows from (2.9) [23] that N is the natural module (or its dual, but this distinction is irrelevant).

If $G^*/N \simeq \mathrm{A}_6$ then $n - k = 2$ and $K = 15$ which implies $(2^k - 1)(2^4 - 1) < 2^{k+2}$, a contradiction. Similarly the cases A_7 and A_9 are ruled out while $\mathrm{A}_8 \simeq \mathrm{L}_4(2)$ was treated already. If $G^*/N \simeq \mathrm{M}_{22}$ then $n - k = 4$ and $K \geq 77$ by the information from the ATLAS of finite groups [3]. Hence $(2^k - 1)2^6 < 2^{k+4}$, again a contradiction. Similarly the remaining cases are ruled out.

Now $G_S^* \simeq \mathrm{GL}(n,2) \simeq \mathrm{L}_n(2)$, $n \geq 4$, $G_S^* \cap N = 1$, so that G^* is a split extension of $\mathrm{GL}(n,2)$ by its natural module. Let η be an element in the preimage of $N_{G^*/N}(TN/N)$. Then $\langle T^\eta, T\rangle$ is a 2-group, i.e. $T^\eta = T$, which shows that $N_{G^*}(T)$ covers $N_{G^*/N}(TN/N)$. In particular $N_{G^*}(T)$ contains a cyclic group C of order $2^{n-1}-1$ which normalizes the extraspecial (see Lemma 4.1) 2-group $E = NT$ of order 2^{2n-1}. Since all cyclic groups of order $2^{n-1}-1$ are conjugate in $\mathrm{GL}(n,2)$ and thus in G^* we may assume $C \leq G_S^*$ (choose S in a suitable way). We view the quotient $E/(N \cap T)$ as a symplectic space of dimension $2(n-1)$ (cf. [12, Satz III.13.7-8]). Thus the representation of C on the isotropic space $N/(N \cap T)$ is dual to the representation of C on E/N and both representations are inequivalent (consider the eigenvalues and use $n > 3$). Thus the $\mathbb{F}_2C$-module $E/(N \cap T)$ has precisely two invariant C-spaces, namely $T/(N \cap T)$ and $N/(N \cap T)$. Also $EC \cap G_S^* = FC$, $F = E \cap G_S^*$, with F elementary of order 2^{n-1} by the modular law. This implies $F \leq T$. But nontrivial elements in F do not fix S, a contradiction. □

We remark that the theorem implies

$$N_{T^\gamma}(T) \neq 1 \quad \text{for each} \quad T^\gamma \in \mathcal{C} - \{T\}.$$

Hence the assumptions of Lemma 4.5 are automatically satisfied.

Lemma 4.7. *Let $T^\gamma \in \mathcal{C} - \{T\}$. Set $H = \langle T, T^\gamma\rangle$. Then $N = O_2(G^*) = O_2(H)$ and $H/N \simeq \mathrm{D}_{2k}$, $1 < k$ odd. Let C be a cyclic subgroup of H of order k. The group C in the DHO case, respectively, in the APN case, the group $\overline{C}$, fixes precisely two elements $S, S' \in \mathcal{S}$. Moreover $N_H(C) = C\langle\mu\rangle$ with an involution μ conjugate to some element in T. Finally, $H = \langle T, \mu\rangle$ for a suitable choice of μ.*

Proof. As before it suffices to consider the DHO case. We can apply Theorem 4.6 to H in the role of G^*. Thus $H/N \simeq \mathrm{D}_{2k}$, $1 < k$ odd, and $O_2(H) = N$ by Lemma 4.5. Also $N = O_2(G^*)$ as $|N| = |O_2(G^*)|$.

Let $\mathcal{S}_0$, $\mathcal{S}_1$, N_0, N_1 be defined as in Theorem 4.6. Since $C_N(C) = 1$ (Lemma 4.5) and, as N_0 acts regularly on $\mathcal{S}_1$, we deduce that C fixes precisely one space S' in $\mathcal{S}_1$. Similarly, C fixes precisely one space S in $\mathcal{S}_0$. By a Frattini argument $H = N_H(C)N$. But $[N_N(C), C] \leq C \cap N = 1$, so $N_N(C) = C_N(C) = 1$ which implies $N_H(C) = C\langle\mu\rangle$ with an involution μ. Choosing a suitable μ we see $C \leq \langle T, \mu\rangle$. □

Lemma 4.8. *Consider the $\mathbb{F}_2$-block matrices*

$$L = \begin{pmatrix} \mathbf{1}_t & A & B \\ & \mathbf{1}_t & \\ & & \mathbf{1}_s \end{pmatrix}, \quad L' = \begin{pmatrix} \mathbf{1}_t & & \\ C & \mathbf{1}_t & D \\ & & \mathbf{1}_s \end{pmatrix},$$

and assume that

$$(LL')^2 = \begin{pmatrix} \mathbf{1}_t & X & Y \\ & \mathbf{1}_t & \\ & & \mathbf{1}_s \end{pmatrix}.$$

Then $X = 0$ and $Y = AD$.

Proof. A computation shows

$$(LL')^2 = \begin{pmatrix} \mathbf{1}_t + AC + (AC)^2 & ACA & AC(AD+B) + AD \\ CAC & \mathbf{1}_t + CA & C(AD+B) \\ & & \mathbf{1}_s \end{pmatrix}.$$

We conclude $CA = 0$ and then $AC = 0$ and finally $CB = 0$. The proof is complete. □

Lemma 4.9. *Let $T, T^\gamma \in \mathcal{C}$ be two translation groups. Set $H = \langle T, T^\gamma \rangle$, $N = O_2(H)$, $Y = C_U(T)$ and $Y' = C_U(T^\gamma)$. The following holds.*

(a) Set $U_0 = C_U(H)$, $U_1 = Y + Y'$. Then $\dim U_0 = m - n + 1$, $\dim U_1/U_0 = 2(n-1)$ and $\dim U/U_1 = 1$. Moreover H acts trivially on U_0 and U/U_1.

(b) $[U_1, T \cap N] \subseteq U_0$.

(c) $\dim U \geq 3(n-1)$.

Proof. The APN case: Since $U_0 = Y \cap Y'$ and $\dim U_1 \leq m + n$ we have

$$\dim U_0 \geq m - n.$$

We claim:

(1) U_1 is a proper subspace of U.

Assume the converse. Then

$$U/U_0 = Y/U_0 \oplus Y'/U_0$$

is a decomposition into n-spaces. Choose subspaces $Z \subseteq Y$, $Z' \subseteq Y'$, such that $U = Z' \oplus Z \oplus U_0$. If we adjust to this decomposition a basis of U we get for $\tau \in T$ and $\tau' \in T^\gamma$ matrix representations

$$\tau = \begin{pmatrix} \mathbf{1}_n & A(\tau) & B(\tau) \\ & \mathbf{1}_n & \\ & & \mathbf{1}_{m-n} \end{pmatrix}, \quad \text{and} \quad \tau' = \begin{pmatrix} \mathbf{1}_n & & \\ C(\tau') & \mathbf{1}_n & D(\tau') \\ & & \mathbf{1}_{m-n} \end{pmatrix}.$$

Choose in particular $\tau \in T - N$. Then

$$T^\gamma \cap N \ni \tau' \mapsto [\tau, \tau'] = (\tau\tau')^2 \in T \cap N$$

is an injection since $C_N(\tau) = C_N(T) = T \cap N$. By Lemma 4.8 the elements in $T \cap N$ are represented by the matrices

$$\begin{pmatrix} \mathbf{1}_n & & A(\tau)D(\tau') \\ & \mathbf{1}_n & \\ & & \mathbf{1}_{m-n} \end{pmatrix}$$

where τ' ranges over the elements of $T^\gamma \cap N$. Hence $C_{Z'}(T \cap N) \neq 0$ as $\ker A(\tau) \subseteq \ker A(\tau)D(\tau')$ and therefore $\dim C_U(\sigma, \sigma') \geq m + 1$ for $1 \neq \sigma, \sigma' \in T \cap N$,

$\sigma \neq \sigma'$. But $\dim C_U(\sigma, \sigma') = \dim Y = m$ by Theorem 3.5, a contradiction. Hence assertion (1) holds. So we have

$$\dim U_0 = m - n + k, \quad k > 0.$$

Denote by N_0 the stabilizer in $\overline{N}$ of $0 \in \mathcal{S}$. Then $N_0 \leq N \leq H$. We know by Theorem 4.6 that $|\mathcal{S}_0| = 2^{n-1}$ for $\mathcal{S}_0 = \mathrm{Fix}_{\mathcal{S}}(N_0)$. Moreover $|(\mathcal{S}_0+Y)/Y| = 2^{n-1}$ by Lemma 3.3. So either $U = W+Y$ or $\dim U/(W+Y) = 1$ where $W = C_U(N_0)$. Assume the first case. As $C_U(T) = C_U(T \cap N)$ and $C_U(T') = C_U(T' \cap N)$ we have $C_U(N) = U_0$. Hence $n = \dim(W+Y)/Y = \dim W/(W \cap Y) = \dim W/U_0$. By symmetry $\dim Y/U_0 = n$ and $U/U_0 = Y/U_0 \oplus W/U_0$ is a decomposition into n-spaces which forces $\dim U_0 = m - n$, i.e. $k = 0$, a contradiction.

So we have $\dim(W+Y) = m+n-1$ and $n-1 = \dim(W+Y)/Y = \dim W/U_0$, i.e. $\dim W = m + k - 1$. Let $\tau \in T - N$, $N_1 = N_0^\tau$ and $W' = C_U(N_1)$. Then $\dim W' = m + k - 1$ too. Since τ centralizes Y and U/Y we see

$$W + Y = (W + Y)\tau = W' + Y.$$

Therefore

$$m + n - 1 \geq \dim(W + W') = 2(m + k - 1) - (m - n + k) = m + n + k - 2$$

which shows $k = 1$. Assertion (a) follows.

To (b) and (c): We write $U_1 = Z' \oplus Z \oplus U_0$, with $(n-1)$-spaces $Z \subseteq Y$ and $Z' \subseteq Y'$. Then

$$U = \langle v_0 \rangle \oplus Z' \oplus Z \oplus U_0$$

where $v_0 \in U - U_1$. If we adjust to this decomposition a basis of U we get for $\tau \in T$ and $\tau' \in T^\gamma$ matrix representations

$$\tau = \begin{pmatrix} 1 & & a(\tau) & b(\tau) \\ & \mathbf{1}_{n-1} & A(\tau) & B(\tau) \\ & & \mathbf{1}_{n-1} & \\ & & & \mathbf{1}_{m-n+1} \end{pmatrix}, \quad \text{and} \quad \tau' = \begin{pmatrix} 1 & c(\tau') & & d(\tau') \\ & \mathbf{1}_{n-1} & & \\ & C(\tau') & \mathbf{1}_{n-1} & D(\tau') \\ & & & \mathbf{1}_{m-n+1} \end{pmatrix}.$$

Choosing $\tau \in T - N$ and using Lemma 4.8 again we see that the elements in $T \cap N$ are represented by matrices of the form

$$\begin{pmatrix} 1 & & \star & \star \\ & \mathbf{1}_{n-1} & & A(\tau)D(\tau') \\ & & \mathbf{1}_{n-1} & \\ & & & \mathbf{1}_{m-n+1} \end{pmatrix}$$

where τ' ranges over the elements of $T^\gamma \cap N$. Since $N = (T^\gamma \cap N) \times (T \cap N)$ and by symmetry this implies assertion (b). As $1 + \sigma$ has rank $n - 1$ for $1 \neq \sigma = (\tau\tau')^2 \in T \cap N$ we see that the matrix $A(\tau)D(\tau')$ must have at least $n - 2$ columns, i.e. $m - n + 1 \geq n - 2$. Thus $\dim U \geq 1 + 2(n-1) + n - 2 = 3(n-1)$ and assertion (c) holds too.

THE DHO CASE: Let $S \in \mathcal{S}_0$ and $\sigma \in N_0$ ($\mathcal{S}_0$ and N_0 as in Theorem 4.6). Then $S \cap S\sigma \subseteq C_S(N_0)$, which implies $\dim C_S(N_0) \geq n-1$. On the other hand N_0 acts regularly on $\{S \cap S'\sigma \,|\, \sigma \in N_0\}$ for $S' \in \mathcal{S}_1$ (again $\mathcal{S}_1$ as in Theorem 4.6). This shows $\dim C_S(N_0) = n-1$ and $S - C_S(N_0)$ is an N_0-orbit. Since $U(\sigma+1) \subseteq U_1$ for $\sigma \in H$ we deduce $S(\sigma+1) \subseteq S \cap U_1$ if $\sigma \in N_0$. This implies

$$S \cap U_1 = C_S(N_0) = [S, N_0] \quad \text{and} \quad S = (S \cap U_1) \oplus (S \cap S').$$

Thus $C_U(T) \oplus (S \cap U_1) \subseteq U_1$, i. e. $\dim U_1 \geq m+n-1$. But we have seen $U_1 \neq U$. This shows $\dim U_1 = m+n-1$ and $\dim U_0 = m-n+1$ and (a) holds. We are now in the same situation as in the APN case. We can argue as before and obtain assertions (c) and (d) in the DHO case too. $\square$

A consequence of part (c) of Lemma 4.9 is:

Theorem 4.10. *Let U be the ambient space of an n-dimensional bilinear DHO which admits at least two translation groups or the ambient space of a quadratic APN function which is defined on an n-space and which admits at least two translation groups. Then* $\dim U \geq 3(n-1)$.

Remark. In the case of APN functions the lower bound of Theorem 4.10 will be improved by Corollary 5.11.

5 Extensions

In this section we construct extensions of bilinear, symmetric DHOs (see Theorem 5.1) and extensions of alternating, quadratic APN functions (see Theorem 5.3). Such extensions are candidates for DHOs or APN functions which admit more than one translation group (see Corollary 5.2 and Corollary 5.5). It will be shown, that if such a DHO or APN function admits more than one translation group, then the automorphism group of this extension is already determined by the automorphism group of the extended object (see Theorem 5.7 and Theorem 5.9). Finally, we show that any DHO or APN function which admits more than one translation group can be constructed as an extension of a symmetric bilinear DHO or a quadratic APN function respectively (see Theorem 5.10). As a consequence one obtains the complete information on the structure of the normal closure of the translation groups (see Corollary 5.13).

In the subsequent section we will apply the results of the present section and give concrete examples of bilinear DHOs and APN functions with many translation groups.

Theorem 5.1. *Let X, Y be finite dimensional $\mathbb{F}_2$-spaces, $\beta : X \to \mathrm{Hom}(X, Y)$ a homomorphism which defines a symmetric, bilinear DHO $\mathcal{S} = \mathcal{S}_\beta$. Set $\overline{X} = \mathbb{F}_2 \times X$ and $\overline{Y} = X \times Y$. For $(a, e) \in \overline{X}$ define a subspace of $\overline{X} \times \overline{Y}$ by*

$$S_{a,e} = \{(b, be + ax, be + (a+1)x, (be+x)\beta(e)) \,|\, (b, x) \in \overline{X}\}.$$

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

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

(b) For $(a,e) \in \overline{X}$ set

$$\tau_{a,e} = \begin{pmatrix} 1 & e & e & e\beta(e) \\ & (a+1)\mathbf{1} & a\mathbf{1} & \beta(e) \\ & a\mathbf{1} & (a+1)\mathbf{1} & \beta(e) \\ & & & \mathbf{1} \end{pmatrix}.$$

Then $T = \{\tau_{a,e} \mid (a,e) \in \overline{X}\}$ is a translation group of $\overline{\mathcal{S}}$.

(c) For $e \in X$ set

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

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 $\overline{\mathcal{S}}_a = \{S_{a,e} \mid e \in X\}$ and it acts regularly on $\overline{\mathcal{S}}_{a+1}$. The group $N = N_0 \times N_1$ is an elementary abelian group of order $|X|^2$ and the groups N and T normalize each other.

(d) Let $\alpha = (\lambda, \mu, \rho)$ be an autotopism of $\mathcal{S}$. Then $u_\alpha = \mathrm{diag}(1, \lambda, \mu, \rho)$, is an automorphism $\overline{\mathcal{S}}$.

(e) We have $T^{u_\alpha} = T$ iff α is a special autotopism.

Notation. We write elements from $\overline{X} \times \overline{Y}$ as (a, x, y, z) with $a \in \mathbb{F}_2$, $x, y \in X$, and $z \in Y$.

Proof. (a) + (b) A simple calculation (which uses the symmetry of β) shows that $\tau_{a,e}\tau_{b,f} = \tau_{a+b,e+f}$, i. e. T is an elementary abelian group of order 2^{n+1}. A typical element of $S_{0,0}$ has the shape $(b, 0, x, 0)$. Then

$$(b, 0, x, 0)\tau_{a,e} = (b, eb + ax, eb + (a+1)x, (eb + x)\beta(e))$$

which implies $S_{0,0}\tau_{a,e} = S_{a,e}$. Hence T acts regularly on $\overline{\mathcal{S}}$. We also observe

$$S_{0,0} \cap S_{0,e} = \langle (0, 0, x, 0) \rangle$$

for $0 \neq e \in X$ and $\ker \beta(e) = \langle x \rangle$ and

$$S_{0,0} \cap S_{1,e} = \langle (1, 0, e, 0) \rangle.$$

Using the action of T we conclude that $\overline{\mathcal{S}}$ is a DHO. Finally,

$$C_{\overline{X} \times \overline{Y}}(T) = \{(0, x, x, y) \mid (x, y) \in X \times Y\}.$$

This space intersects trivially with every subspace of the DHO. Hence T is a translation group.

(c) Simple block matrix multiplication shows that all $n_{a,e}$, $(a,e) \in \overline{X}$, commute, i. e. N is elementary abelian of order $|X|^2$. Let $v = (b, be, be + x, (be + x)\beta(e))$ be a typical element in $S_{0,e}$. Then (using again the symmetry of β)

$$vn_{0,f} = (b, be, b(e + f) + x, be\beta(f) + (be + x)\beta(e)) = (b, be, be + y, (be + y)\beta(e)),$$

$y = bf+x$, which lies again in $S_{0,e}$. Thus $S_{0,e}n_{0,f} = S_{0,e}$. A similar computation shows $vn_{1,f} \in S_{1,e+f}$. A computation shows that $\tau_{1,0}$ interchanges the the groups N_0 and N_1 (via conjugation) and that each $\tau_{0,e}$ commutes with elements in N_a, $a = 0, 1$, i.e. T normalizes N. Also $[\tau_{1,0}, n_{a,e}] \in T$ (computation), so that N normalizes T too. By symmetry all assertions of (c) follow.

(d) Let $v = (b, be, be + x, (be + x)\beta(e))$ be a typical element in $S_{0,e}$. Then

$$vu_\alpha = (b, be\lambda, (be + x)\mu, (be + x)\beta(e)\rho) = (b, be\lambda, be\lambda + y, (be\lambda + y)\beta(e\lambda)),$$

$y = be\lambda+(be+x)\mu$, since $(be\lambda+y)\beta(e\lambda) = (be+x)\beta(e)\rho$ by (d) of Proposition 3.9. Hence $S_{0,e}u_\alpha = S_{0,e\lambda}$. Similarly, we see that $S_{1,e}u_\alpha = S_{1,e\mu}$ holds. So all assertions of (b) follow.

(e) A computation shows that $u_\alpha^{-1}\tau_{1,0}u_\alpha \in T$ iff α is special. $\square$

Remark. Assume in the theorem that $X \times Y$ is the ambient space of $\mathcal{S}$. It is not hard to see that the ambient space of $\overline{\mathcal{S}}$ is $\overline{X} \times \overline{Y}$.

Definition. Let X, Y be finite dimensional $\mathbb{F}_2$-spaces, $\beta : X \to \mathrm{Hom}(X, Y)$ a homomorphism which defines a symmetric DHO $\mathcal{S} = \mathcal{S}_\beta$. Set $\overline{X} = \mathbb{F}_2 \times X$ and $\overline{Y} = X \times Y$. We call the bilinear DHO $\overline{\mathcal{S}}$ in $\overline{X} \times \overline{Y}$ (defined in Theorem 5.1) the *extension of* $\mathcal{S}$.

As a corollary of assertion (e) from Theorem 5.1 we have.

Corollary 5.2. *The extension of a symmetric, bilinear DHO $\mathcal{S}$ admits more than one translation group if $\mathcal{S}$ admits non-special autotopisms.*

We now treat extensions of APN functions.

Theorem 5.3. *Let $f : X \to Y$ be a normed APN function. Set $\overline{X} = \mathbb{F}_2 \times X$ and $\overline{Y} = X \times Y$. Then $F : \overline{X} \to \overline{Y}$, $(a, x) \mapsto (ax, f(x))$ is a normed APN function.*

Proof. Let $0 \neq (a_0, x_0) \in \overline{X}$ and consider g defined by $g(a, x) = F(a + a_0, x + x_0)+F(a, x)$. Let $(\overline{x}, \overline{y}) = g(a, x)$ be an element in the image of g. Let (a', x') be a second pre-image, then (1) $a_0(x+x') = (a+a')x_0$ and (2) $f(x+x_0)+f(x) = f(x' + x_0) + f(x')$. We have to show $(a', x') = (a, x) + (a_0, x_0)$.

If $x_0 = 0$ then $a_0 = 1$ and we get $x = x'$ and $a' = a + 1$ as desired. If $x_0 \neq 0$ then $x' = x + x_0$ by the APN property of f and (2). Then by equation (1) $a' = a + a_0$ and the proof is complete. $\square$

Definition. Let $f : X \to Y$ be a normed APN function. The APN function $F : \overline{X} \to \overline{Y}$ defined in Theorem 5.3 is called the *extension of* f.

We now proof the analogue of Theorem 5.1 for quadratic APN functions.

Theorem 5.4. *Let $f : X \to Y$ be a normed, quadratic APN function and denote by $\beta : X \to \mathrm{Hom}(X, Y)$ the monomorphism which defines the associated DHO. Let $F : \overline{X} \to \overline{Y}$ be the normed APN function in the sense of Theorem 5.3. The following hold:*

(a) The function F is quadratic. For $(a, e) \in \overline{X}$ set

$$\tau_{a,e} = \begin{pmatrix} 1 & & e & \\ & \mathbf{1}_n & a\mathbf{1}_n & \beta(e) \\ & & \mathbf{1}_n & \\ & & & \mathbf{1}_m \end{pmatrix}.$$

Then $T = \{\tau_{a,e} | (a, e) \in \overline{X}\}$ is the linear part of the standard translation group. Moreover the pre-image of $\tau_{a,e}$ in $\overline{T}$ is $\overline{\tau}_{a,e} = \tau_{a,e} + c_{a,e}$ and $c_{a,e} = (a, e) + F(a, e) = (a, e, ae, f(e))$ is the associated 1-cocycle.

(b) For $e \in X$ define

$$\nu_e = \begin{pmatrix} 1 & e & e & f(e) \\ & \mathbf{1}_n & & \\ & & \mathbf{1}_n & \beta(e) \\ & & & \mathbf{1}_m \end{pmatrix}.$$

Then $N_0 = \{\nu_e | e \in X\}$ is an elementary abelian group of order 2^n in $\mathrm{A}(F) \cap \mathrm{Aut}(F)$.

(c) For $a \in \mathbb{F}_2$ define $\mathcal{S}_a = \{(a, e, ae, f(e)) | e \in X\}$. Then $\mathcal{S}_F$ is the disjoint union of $\mathcal{S}_0$ and $\mathcal{S}_1$. The group N_0 fixes $\mathcal{S}_0$ pointwise and acts regularly on $\mathcal{S}_1$. Set

$$N = \langle N_0, \tau_{0,e} | e \in X \rangle.$$

Then N is an elementary abelian 2-group in $A(F)$ of order 2^{2n} and the groups N and T normalize each other. The pre-image $\overline{N}$ of N has the orbits $\mathcal{S}_0$ and $\mathcal{S}_1$ on $\mathcal{S}_F$.

(d) Let

$$\begin{pmatrix} \lambda & \varphi \\ & \rho \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} \gamma & \psi \\ & \rho \end{pmatrix}$$

be autotopisms of f (note that φ and ψ are functions of the pairs (λ, ρ) and (γ, ρ) respectively). Define

$$\phi(\lambda, \gamma, \rho) = \begin{pmatrix} 1 & & & \\ & \lambda & & \varphi \\ & \lambda + \gamma & \gamma & \varphi + \psi \\ & & & \rho \end{pmatrix}$$

Then $\phi(\lambda, \gamma, \rho)$ is an automorphism of F which fixes $(0, 0, 0, 0)$ and $(1, 0, 0, 0)$ (i. e. the automorphism lies in $\mathrm{A}(F) \cap \mathrm{Aut}(F)$). The automorphism normalizes T iff $\lambda = \gamma$. The set L of automorphisms $\phi(\lambda, \gamma, \rho)$ forms a group.

Proof. (a) Denote by β the bilinear form associated to f. Then

$$F(a+a',x+x')+F(a,x)+F(a',x')=(ax'+a'x,\beta(x,x')).$$

This shows that F is quadratic. Moreover a calculation shows $\tau_{a,e}\tau_{b,d}=\tau_{a+b,e+d}$. Hence T is an elementary abelian 2-group of order 2^{n+1}. A routine computation shows $(b,x,F(b,x))\overline{\tau}_{a,e}=(a+b,e+x,F(a+b,e+x))$. Hence $\overline{T}$ is the standard translation group ($\overline{T}$ acts regularly on $\mathcal{S}_F$ and $\overline{Y}=C_{\overline{U}}(T)$).

(b) + (c) A computation shows that N_0 fixes all elements in $\mathcal{S}_0$ and acts on $\mathcal{S}_1$ by $(1,x,x,f(x))\nu_e=(1,x+e,x+e,f(x+e))$. It is easy to see that the elements in N commute with every $\tau_{0,e}$. Then N is an elementary abelian 2-group of order 2^{2n} which is normalized by $\tau_{1,0}$ (calculation). But elements of the form $\tau_{0,e}$ even commute with N, i.e. T normalizes N. But a calculation shows that T is also normalized by N. Hence TN is a 2-group of order 2^{2n+1}. The orbits of $\overline{N}$ on $\mathcal{S}_F$ are $\mathcal{S}_0$ and $\mathcal{S}_1$.

(d) Let $(a,x,ax,f(x))$ be a typical element in $\mathcal{S}_F$. We compute

$$(a,x,ax,f(x))\phi(\lambda,\gamma,\rho)=(a,x\lambda+ax(\lambda+\gamma),ax\gamma,x\varphi+ax(\varphi+\psi)+f(x)\rho).$$

So clearly $\phi(\lambda,\gamma,\rho)$ fixes $(0,0,0,0)$ and $(1,0,0,0)$. By our assumption the equations $f(x\lambda)=x\varphi+f(x)\rho$ and $f(x\gamma)=x\psi+f(x)\rho$ hold. This implies $(a,x,ax,f(x))\phi(\lambda,\gamma,\rho)=(0,x\lambda,0,f(x\lambda))$ if $a=0$ and for $a=1$ we obtain $(1,x\gamma,x\gamma,f(x\gamma))$. Hence $\phi(\lambda,\gamma,\rho)\in \mathrm{A}(F)\cap \mathrm{Aut}(F)$. A simple computation shows that $\phi(\lambda,\gamma,\rho)$ normalizes N. Moreover $\phi(\lambda,\gamma,\rho)^{-1}\tau_{1,0}\phi(\lambda,\gamma,\rho)\in T$ iff $\lambda=\gamma$. Namely, the quadratic block submatrix with respect to the positions (k,l), $k,l\in\{2,3\}$, of $\phi(\lambda,\gamma,\rho)^{-1}\tau_{1,0}\phi(\lambda,\gamma,\rho)$ has the form

$$\begin{pmatrix} \lambda^{-1}\gamma & \lambda^{-1}\gamma \\ \lambda^{-1}\gamma+\gamma^{-1}\lambda & \lambda^{-1}\gamma \end{pmatrix}.$$

So if $\phi(\lambda,\gamma,\rho)^{-1}\tau_{1,0}\phi(\lambda,\gamma,\rho)\in T$ we conclude $\lambda^{-1}\gamma=\gamma^{-1}\lambda$ and $\lambda^{-1}\gamma=\mathbf{1}$. This implies $\lambda=\gamma$. Since the mappings $\phi(\lambda,\gamma,\rho)$ are defined by autotopisms of f and as the autotopisms of f are a group, an obvious matrix multiplication shows that L is a group too. $\square$

Remark. The group L can be viewed as a direct product with identified factor group ("direktes Produkt mit vereinigter Faktorgruppe") in the sense of [12, I. 9.10]. Indeed we have

$$L\simeq\{(\phi,\varepsilon)\in A\times A|\phi K=\varepsilon K\}$$

where A is the autotopism group of f and K is the normal subgroup of nuclear autotopisms.

Corollary 5.5. *The extension of a quadratic APN function f admits more than one translation group if f admits nontrivial nuclear autotopisms.*

Proof. This corollary is an immediate consequence of assertion (d) of Theorem 5.4. $\square$

Let G be the automorphism group of an extension of a symmetric, bilinear DHO. By Theorem 5.1 G contains an elementary abelian 2-group N which has precisely two orbits on the DHO. Suppose that G contains more than one translation group and denote by G^* the group generated by the translation groups. By Theorem 4.6 we know that $O_2(G^*)$ has the same order as N and it also has a similar action on the DHO. We now show that these groups do indeed coincide and that for extensions of APN functions an analogous assertion holds.

Proposition 5.6. *Let G be the automorphism group of an extension of a n-dimensional, symmetric, bilinear DHO, $n \geq 4$, or the linear part of the automorphism group of the extension of a quadratic APN function defined on a $\mathbb{F}_2$-space of dimension ≥ 4. Suppose that G contains more then one translation group and denote by G^* the group generated by the translation groups. Let N be the group defined in Theorem 5.1 (DHO case) or in Theorem 5.4 (APN case). Then $N = O_2(G^*)$.*

Proof. We set $\mathcal{N} = O_2(G^*)$ and denote by T a translation group which normalizes N (notation as in 5.1 and 5.4). Thus TN is a 2-group and as $\mathcal{N}$ is a normal 2-group in G also $S = TN\mathcal{N}$ is a 2-group. We also define n by $|N| = |\mathcal{N}| = 2^{2n}$ (i.e. $|T| = 2^{n+1}$). Let M be either N or $\mathcal{N}$.

(1) Consider T as a $(n+1)$-dimensional $\mathbb{F}_2$-space. Then $MT/T \simeq M/(M \cap T)$ is the centralizer in $\mathrm{GL}(T)$ of the hyperplane $M \cap T$.

Clearly, $|M \cap T| = |MT/T| = 2^n$ and as $C_G(T) = T$ we see that MT/T is isomorphic to an elementary abelian 2-group of order 2^n in $\mathrm{GL}(T)$. Moreover MT/T centralizes $M \cap T$. On the other hand it is well known that the centralizer of a hyperplane in $\mathrm{GL}(T)$ is elementary abelian of order 2^n. Claim (1) follows.

(2) $N = \mathcal{N}$.

Assume first $N \cap T = \mathcal{N} \cap T$. So for $\tau \in N$ there exists by (1) a $\sigma \in \mathcal{N}$ such that both elements induce the same automorphism on T. Hence $\sigma^{-1}\tau \in C_G(T) = T$ or $\tau \in \mathcal{N}T$. So N is an elementary abelian 2-group of order 2^{2n} in $\mathcal{N}T$. However $\mathcal{N}$ is the *only* elementary abelian 2-group of order 2^{2n} in $\mathcal{N}T$ (we know that $|C_{\mathcal{N}}(\tau)| = 2^n$ for $\tau \in \mathcal{N}T - \mathcal{N}$). Hence $N = \mathcal{N}$.

Assume now $N \cap T \neq \mathcal{N} \cap T$. Then $Z = T \cap N \cap \mathcal{N}$ is a subspace of codimension 2 in T and NT/T and $\mathcal{N}T/T$ induce two different groups of order 2 on the space T/Z of dimension 2 (note that $(T \cap N)/Z \neq (T \cap \mathcal{N})/Z$). But $\mathrm{GL}(T/Z) \simeq \mathrm{GL}(2,2) \simeq \mathrm{S}_3$. Hence $\langle T, N, \mathcal{N} \rangle$ induces the symmetric group of degree 3 on T/Z. But then the order of S is divisible by 3, a contradiction. So (2) holds and the proof is complete. □

Theorem 5.7. *Let $\overline{\mathcal{S}}$ be the extension of the bilinear, symmetric DHO $\mathcal{S} = \mathcal{S}_\beta$ and let G be the automorphism group of $\overline{\mathcal{S}}$. We assume the notation of Theorem 5.1. The following hold.*

(a) The normalizer of N in G has the form

$$N_G(N) = \langle \tau_{1,0} \rangle LN, \quad L \cap N = 1,$$

where L is a group which is isomorphic to the autotopism group of $\mathcal{S}$.

(b) *Assume now that $\overline{\mathcal{S}}$ has dimension ≥ 4, that G has more than one translation group and denote by G^* the normal closure of the translation groups. Then $G = \langle\tau_{1,0}\rangle LN$ and $G^* = \langle\tau_{1,0}\rangle L_0 N$, where L_0 is isomorphic to the multiplicative group of the symmetric nucleus of $\mathcal{S}$. Moreover, G contains precisely $|L_0|$ translation groups.*

Proof. (a) Set $M = N_G(N)$. Then M leaves $\{\mathcal{S}_0, \mathcal{S}_1\}$ as a set invariant. Let H be the normal subgroup of index 2 of M which fixes the two N-orbits $\mathcal{S}_0$ and $\mathcal{S}_1$. Since $\tau_{1,0}$ interchanges $\mathcal{S}_0$ with $\mathcal{S}_1$, one has $M = \langle\tau_{1,0}\rangle H$ and $N \leq H$. Since N is transitive on $\mathcal{S}_0$ we get $H = NK$, where K is the stabilizer of $S_{0,0}$ in H. Also $N \cap K = N_0$. But N_0 acts regularly on $\mathcal{S}_1$. Hence $K = N_0 L$, where L is the stabilizer of $S_{1,0}$ in K. Now

$$L \cap N = L \cap K \cap N = L \cap N_0 = 1,$$

and

$$H = KN = LN_0N = LN.$$

As L fixes $S_{0,0}$ and $S_{1,0}$ it fixes the intersection of these spaces too. Also L fixes $C_{\overline{X}\times\overline{Y}}(N) = \{(0,0,0,y)|y \in Y\}$. So $\sigma \in L$ has the form

$$\sigma = \mathrm{diag}\,(1, \lambda, \mu, \rho).$$

Since σ normalizes both groups N_0 and N_1 we see that

$$\beta(x\lambda) = \mu^{-1}\beta(x)\rho, \quad \beta(x\mu) = \lambda^{-1}\beta(x)\rho$$

for all $x \in X$. Using (d) of Proposition 3.9 we see that (λ, μ, ρ) is an autotopism of $\mathcal{S}$ and by (d) of Theorem 5.1 every autotopism of this DHO lifts to an element of L.

(b) By Proposition 5.6 N is normal in G, i. e. the first assertion holds. Note that $\tau_{1,0}$ normalizes L as $\sigma^{\tau_{1,0}} = \mathrm{diag}\,(1, \mu, \lambda, \rho)$ with a σ defined as above. Hence the commutator

$$[\sigma, \tau_{1,0}] = \sigma^{-1}\sigma^{\tau_{1,0}} = \mathrm{diag}\,(1, \lambda^{-1}\mu, \mu^{-1}\lambda, 1)$$

lies in the group $L_0 = \{\mathrm{diag}(1, \delta^{-1}, \delta, 1)|(\delta^{-1}, \delta, 1) \text{ nuclear}\}$. Clearly, this group is isomorphic to the multiplicative group of the symmetric nucleus of $\mathcal{S}$ (see (c) of the Proposition 3.9 and the definition of the symmetric nucleus). Moreover, L_0 is a normal subgroup of L (since the group of nuclear autotopisms of $\mathcal{S}$ is cyclic, i. e. every subgroup is characteristic) and we have $\tau_{1,0}^{\sigma} L_0 = \tau_{1,0} L_0$ for all $\sigma \in L$.

We claim $G^* = \langle\tau_{1,0}\rangle L_0 N$. As all involutions in $T - N$ are conjugate under N to $\tau_{1,0}$, it suffices to show that the RHS contains the conjugacy class of $\tau_{1,0}$ in G. A typical element in G can be written as $\omega = \omega_0\omega_1$ with $\omega_0 \in TN$ and $\omega_1 \in L$. Hence

$$\tau_{1,0}^{\omega} = (\tau_{1,0}^{\omega_0})^{\omega_1} \in \tau_{1,0}^{\omega_1} N^{\omega_1} = \tau_{1,0}^{\omega_1} N \subseteq \tau_{1,0} L_0 N$$

as desired.

Since G^*/N is a dihedral group of order $2|L_0|$ ($\tau_{1,0}N$ acts invertingly on the cyclic group L_0N/N), we have $N_{G^*/N}(TN/N) = TN/N$. This implies $N_{G^*}(T) = TN$ and hence G^* and thus G has precisely $|L_0| = |G^* : N_{G^*}(T)|$ translation groups. $\square$

We now turn to the computation of the automorphism group of extensions of quadratic APN functions. We need the following Lemma.

Lemma 5.8. *Let F be the extension of a quadratic APN function. Assume the notation of Theorem 5.4. The stabilizer of $(0,0,0,0)$ and $(1,0,0,0) \in \mathcal{S}_F$ in the normalizer of $\overline{N}$ in $\mathrm{Aut}(F)$ is L.*

Proof. It is convenient to use the basis transformation represented by

$$\begin{pmatrix} 1 & & & \\ & \mathbf{1}_n & & \\ & \mathbf{1}_n & \mathbf{1}_n & \\ & & & \mathbf{1}_m \end{pmatrix}.$$

This results in somewhat simpler representations of $\mathcal{S}_F$, T, N, and L. We have for the graph

$$\mathcal{S}_0 = \{(0,x,0,f(x))|x \in X\} \quad \text{and} \quad \mathcal{S}_1 = \{(1,0,x,f(x))|x \in X\}.$$

The elements in N_0 and $\tau_{1,0}$ have now the form

$$\nu_e = \begin{pmatrix} 1 & & e & f(e) \\ & \mathbf{1}_n & & \\ & & \mathbf{1}_n & \beta(e) \\ & & & \mathbf{1}_m \end{pmatrix}, \quad \tau_{1,0} = \begin{pmatrix} 1 & & & \\ & & \mathbf{1}_n & \\ & \mathbf{1}_n & & \\ & & & \mathbf{1}_m \end{pmatrix}$$

and $c_{1,0} = (1,0,0,0)$. Let $\overline{N}_1$ be the pointwise stabilizer of $\mathcal{S}_1$ in $\overline{N}$. Then $N_1 = \langle \mu_e | e \in X\rangle$ where

$$\mu_e = \begin{pmatrix} 1 & e & & f(e) \\ & \mathbf{1}_n & & \beta(e) \\ & & \mathbf{1}_n & \\ & & & \mathbf{1}_m \end{pmatrix}, \quad c_{\mu_e} = (0,e,0,f(e)).$$

Finally elements in L have now the shape

$$\phi(\lambda,\gamma,\rho) = \begin{pmatrix} 1 & & & \\ & \lambda & & \varphi \\ & & \gamma & \psi \\ & & & \rho \end{pmatrix}$$

such that

$$\begin{pmatrix} \lambda & \varphi \\ & \rho \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} \gamma & \psi \\ & \rho \end{pmatrix}$$

are autotopisms of f.

Pick a $\phi \in N_{\mathrm{Aut}(F)}(\overline{N})$ which fixes $(0,0,0,0)$ and $(1,0,0,0)$. This implies $\phi \in \mathrm{A}(F)$ and therefore ϕ also normalizes N_0 and N_1. So this automorphism leaves invariant $C_{\overline{X}\times\overline{Y}}(N) = \{(0,0,0,y)|y \in Y\}$ and $C_{\overline{X}\times\overline{Y}}(N_i)$, $i = 0,1$. This implies that the automorphism is represented as

$$\phi = \begin{pmatrix} 1 & & & \\ & \lambda & & \varphi \\ & & \gamma & \psi \\ & & & \rho \end{pmatrix}.$$

We have to show: $\begin{pmatrix} \lambda & \varphi \\ & \rho \end{pmatrix}$ and $\begin{pmatrix} \gamma & \psi \\ & \rho \end{pmatrix}$ are autotopisms of f.

We have

$$\phi^{-1}\nu_e\phi = \begin{pmatrix} 1 & & e\gamma & f(e)\rho + e\psi \\ & \mathbf{1}_n & & \\ & & \mathbf{1}_n & \gamma^{-1}\beta(e)\rho \\ & & & \mathbf{1}_m \end{pmatrix} \in N_0$$

and

$$\phi^{-1}\mu_e\phi = \begin{pmatrix} 1 & e\lambda & & f(e)\rho + e\varphi \\ & \mathbf{1}_n & & \lambda^{-1}\beta(e)\rho \\ & & \mathbf{1}_n & \\ & & & \mathbf{1}_m \end{pmatrix} \in N_1.$$

This shows $f(e\gamma) = f(e)\rho + e\psi$ and $f(e\lambda) = f(e)\rho + e\varphi$ and indeed this pair of equations proves the claim. □

Theorem 5.9. *Let F be the extension of a quadratic APN function f and let $G = \mathrm{A}(F)$ be the linear part of the automorphism group of F. We assume the notation of Theorem 5.4. The following hold.*

(a) The normalizer of N in G has the form

$$N_G(N) = \langle\tau_{1,0}\rangle LN, \quad L \cap N = 1.$$

(b) Assume now that F is defined on a space of dimension $n \geq 4$, that G has more than one translation group and denote by G^* the normal closure of the translation groups. Then $G = \langle\tau_{1,0}\rangle LN$ and $G^* = \langle\tau_{1,0}\rangle L_0 N$, where L_0 is isomorphic to the group of nuclear autotopisms of f, i. e. $L_0 \simeq \mathrm{C}_3$ and G contains precisely three translation groups. Moreover n is odd.

Proof. (a) Set $M = N_G(N)$. We can now proceed completely similar as in the proof of Theorem 5.7 (with $\overline{M}$ in the role of M and the graph of $\mathcal{S}_F$ in the role of $\overline{\mathcal{S}}$) and obtain (using Lemma 5.8: L is the stabilizer of the given two points of the graph in $\overline{M}$)

$$N_G(N) = \langle\tau_{1,0}\rangle LN, \quad L \cap N = 1.$$

(b) By Proposition 5.6 $N = O_2(G^*)$. This shows the first assertion of (b). We use the same basis transformation as in the proof of Lemma 5.8. Let $\phi(\lambda, \gamma, \rho)$ be a typical element from L. A computation shows

$$\tau_{1,0}\phi(\lambda, \gamma, \rho)\tau_{1,0} = \phi(\gamma, \lambda, \rho).$$

In particular $\phi = \phi(\lambda, \gamma, \rho) \in L$ is inverted by $\tau_{1,0}$ iff $\rho = 1$ and $\gamma = \lambda^{-1}$. This implies (one can use precisely the same arguments as in the proof of part (b) of Theorem 5.7) $L \cap G^* = L_0 = [L, \tau_{1,0}] \simeq \mathrm{C}_3$ and there exist a nontrivial nuclear autotopism of f of the form $\begin{pmatrix} \lambda & \varphi \\ & \mathbf{1} \end{pmatrix}$. Here we also use that f is associated with an alternating DHO and use (f) of Proposition 3.9. As in the proof of Theorem 5.7 we see that G has precisely three translation groups. Also n is odd by (f) of Proposition 3.9. $\square$

We now show that bilinear DHOs which admit more than one translation group are extensions of symmetric bilinear DHOs and we prove the analogous result for quadratic APN functions.

Theorem 5.10. *Let $U = X \oplus Y$ be an $\mathbb{F}_2$-space with $\dim X = n \geq 4$ and $\dim Y = m$.*

(a) Let $\mathcal{S}$ be a n-dimensional, bilinear DHO in U, which admits at least two translation groups. Then $\mathcal{S}$ is the extension of a symmetric $(n-1)$-dimensional DHO.

(b) Let $F : X \to Y$ be a quadratic APN function, which admits at least two translation groups. Then n is odd and F is equivalent to the extension of a quadratic APN function $g : \mathbb{F}_2^{n-1} \to \mathbb{F}_2^{m-n+1}$.

Proof. We consider the group $H = \langle T, T^\gamma \rangle$ generated by two translation groups. Form Lemma 4.5 we know that $H = NC\langle\gamma\rangle$ with $N = O_2(H)$, C a cyclic group of odd order, and we may assume that γ is an involution conjugate in H to some element in $T - N$. Also we assume wlog. $Y = C_U(T)$ (cf. Theorem 3.11).

Define again as in Lemma 4.9 $U_1 = Y + Y'$, $U_0 = Y \cap Y'$ with $Y' = C_U(T^\gamma)$. We have shown in Lemma 4.9 that $[U_1, N \cap T] \subseteq U_0$ and since N is normal in H, also $[U_1, N \cap T^\gamma] \subseteq U_0$, so that finally $[U_1, N] \subseteq U_0$ holds. We now split our argument into the DHO and the APN case.

(a) (DHO case) Here $\mathcal{S}$ is a bilinear DHO. From the proof of Lemma 4.9 we deduce further that

$$(*) \quad U = \langle v_0 \rangle \oplus (S' \cap U_1) \oplus (S \cap U_1) \oplus U_0,$$

$v_0 \in U - U_1$, $S \in \mathcal{S}_0$, $S' \in \mathcal{S}_1$, and that the mapping $N_0 \ni \tau \mapsto [v_0, \tau] \in S \cap U_1$ is injective. Hence there is an isomorphism $\nu : \mathbb{F}_{2^{n-1}} \simeq S \cap U_1 \to N_0$, $e \mapsto \nu_e$ such that $[v_0, \nu_e] = e$. We may assume that S and S' are interchanged under γ.

So we can choose a basis of U adapted to the decomposition $(*)$ such that we have matrix representations of the form

$$\nu_e = \begin{pmatrix} 1 & & e & \\ & \mathbf{1}_{n-1} & & \beta(e) \\ & & \mathbf{1}_{n-1} & \\ & & & \mathbf{1}_{m-n+1} \end{pmatrix} \quad \text{and} \quad \gamma = \begin{pmatrix} 1 & & & \\ & & \mathbf{1}_{n-1} & \\ & \mathbf{1}_{n-1} & & \\ & & & \mathbf{1}_{m-n+1} \end{pmatrix}$$

with a homomorphism $\beta : \mathbb{F}_2^{n-1} \to \mathrm{Hom}(\mathbb{F}_2^{n-1}, \mathbb{F}_2^{m-n+1})$. As $\mathcal{S}_0$ is a subset of an n-dimensional DHO the mapping $\overline{\beta}(e) : \langle v_0 \rangle \oplus (S' \cap U_1) \to (S \cap U_1) \oplus U_0$ represented by $\begin{pmatrix} e & \\ & \beta(e) \end{pmatrix}$ has rank $n-1$ for $0 \neq e$, which implies that $\beta(e)$ has rank $n-2$, i.e. β defines an $(n-1)$-dimensional, bilinear DHO. Conjugating with γ we see that there is an isomorphism $\nu' : \mathbb{F}_2^{n-1} \to N_1$ such that the elements of N_1 are represented as

$$\nu'_f = \begin{pmatrix} 1 & f & & \\ & \mathbf{1}_{n-1} & & \\ & & \mathbf{1}_{n-1} & \beta(f) \\ & & & \mathbf{1}_{m-n+1} \end{pmatrix}.$$

As ν_e and ν'_f commute we see $f\beta(e) = e\beta(f)$, i.e. β is symmetric. It now follows that $\mathcal{S}$ is the extension of the DHO defined by the homomorphism β.

(b) (APN case) Now $\mathcal{S} = \mathcal{S}_F$ is the graph of the quadratic APN function F. Since γ interchanges the spaces Y and $Y\gamma$ we see $\dim C_{U_1}(\gamma) \leq m$. As $\mathrm{rk}\,(1+\gamma) = n-1$ (all involutions in $T - NC$ are conjugate in H by (b) of Lemma 4.5) we see $C_U(\gamma) \not\subseteq U_1$. Then for any involution $\sigma \in H - CN$ we have $\mathrm{rk}\,(1+\sigma)_{U_1/U_0} = n-1$ and $C_U(\sigma) \not\subseteq U_1$.

In order to investigate the graph more closely we turn from the element γ to an element π in $T - N$. Pick $v_0 \in C_U(\pi) - U_1$. By the modular law $U_1 = (U_1 \cap X) \oplus Y$ and as $\mathrm{rk}\,(1+\pi)_{U_1/U_0} = \mathrm{rk}\,(1+\pi) = n-1$ we see that $Z = [U_1 \cap X, \pi]$ has dimension $n-1$ and $Y = Z \oplus U_0$. We obtain the decomposition

$$(**) \qquad U = \langle v_0 \rangle \oplus Z' \oplus Z \oplus U_0$$

where $Y' = Z' \oplus U_0$ and v_0 is some element in $U - U_1$. Let $\tau : \mathbb{F}_2^{n-1} \to N \cap T$, $e \mapsto \tau_e$, be an isomorphism (which will be specified later) and adapt a basis of U to the decomposition $(**)$. This choice of the basis will be refined at a later stage. Since $[U_1, N \cap T] \subseteq U_0$ and $[U, T] \subseteq Y$ we have for the elements in $N \cap T$ a matrix representation of the form

$$\tau_e = \begin{pmatrix} 1 & & a(e) & b(e) \\ & \mathbf{1}_{n-1} & & \beta(e) \\ & & \mathbf{1}_{n-1} & \\ & & & \mathbf{1}_{m-n+1} \end{pmatrix} \quad \text{and} \quad \pi = \begin{pmatrix} 1 & & & \\ & \mathbf{1}_{n-1} & A & \\ & & \mathbf{1}_{n-1} & \\ & & & \mathbf{1}_{m-n+1} \end{pmatrix}$$

with $A \in \mathrm{GL}(n-1, 2)$, $a(e) \in \mathbb{F}_2^{n-1}$, $b(e) \in \mathbb{F}_2^{m-n+1}$, and $\beta(e) \in \mathbb{F}_2^{(n-1)\times(m-n+1)}$. But choosing the basis of the complement Z in a suitable way we may even assume

$$A = \mathbf{1}_{n-1}.$$

From now on we identify the elements u of U with their coordinates (a, x, y, z), $a \in \mathbb{F}_2$, $x, y \in \mathbb{F}_2^{n-1}$, $z \in \mathbb{F}_2^{m-n+1}$, with respect to the given basis; in particular $u \in U_1$ iff $a = 0$. We know from the proof of Lemma 4.9 that the fixed points $\mathcal{S}_0$ of N_0 in $\mathcal{S}$ lie in U_1. We conclude that the set $\mathcal{S}_0$ are represented by elements of the form $(0, x, y, z)$ whereas the elements in $\mathcal{S}_1$ have the shape $(1, x, y, z)$. Now $\mathcal{S}_F$ is the orbit of 0 under $\overline{T}$, i.e. $\mathcal{S}_F = \{c_\sigma | \sigma \in T\}$ and thus $\{c_\sigma | \sigma \in N \cap T\} = \mathcal{S}_0$ or $\mathcal{S}_1$. However from the cocycle rule $c_{\tau\sigma} = c_\tau \sigma + c_\sigma$ we deduce that the second case cannot occur. So if $\tau_e \in T \cap N$ then the pre-image has the form $\overline{\tau}_e = \tau_e + c_{\tau_e}$ where the 1-cocycle c evaluated at τ_e has (in coordinates) the form

$$c_{\tau_e} = (0, x_e, y_e, z_e).$$

Again using the cocycle rule we deduce

$$x_{e+f} = x_e + x_f, \quad y_{e+f} = y_e + y_f, \quad z_{e+f} = z_e + z_f + x_e\beta(f).$$

Thus the mappings $x : \mathbb{F}_2^{n-1} \to \mathbb{F}_2^{n-1}$, $y : \mathbb{F}_2^{n-1} \to \mathbb{F}_2^{n-1}$ are homomorphisms. By assertion (a) of Lemma 3.3 the mapping x is bijective. Since $\overline{\pi}$ interchanges $\mathcal{S}_0$ and $\mathcal{S}_1$ and as π and c_π commute we see that

$$c_\pi = (1, 0, \overline{y}, \overline{z}).$$

Next we exploit the equation $\overline{\pi}\overline{\tau}_e = \overline{\tau}_e\overline{\pi}$, i.e.

$$c_\pi \tau_e + c_{\tau_e} = c_{\pi\tau_e} = c_{\tau_e\pi} = c_{\tau_e}\pi + c_\pi.$$

This implies the equations $x_e = a(e)$ and $b(e) = 0$. However by a suitable choice of v_0 we may even assume $\overline{y} = 0$ and $\overline{z} = 0$. We now choose the isomorphism τ such that $x_e = a(e) = e$. We get

$$\tau_e = \begin{pmatrix} 1 & & e & \\ & \mathbf{1}_{n-1} & & \beta(e) \\ & & \mathbf{1}_{n-1} & \\ & & & \mathbf{1}_{m-n+1} \end{pmatrix}, \quad \pi = \begin{pmatrix} 1 & & & \\ & \mathbf{1}_{n-1} & \mathbf{1}_{n-1} & \\ & & \mathbf{1}_{n-1} & \\ & & & \mathbf{1}_{m-n+1} \end{pmatrix}$$

and

$$c_{\tau_e} = (0, e, e\delta, z_e), \quad \text{and} \quad c_\pi = (1, 0, 0, 0),$$

where $\delta : \mathbb{F}_2^{n-1} \ni e \mapsto e\delta = y_e \in \mathbb{F}_2^{n-1}$ is a linear mapping. So with this choice of the basis the graph has the shape

$$\mathcal{S}_F = \{(a, x, ax + x\delta, z_x) | (a, x) \in \mathbb{F}_2 \times \mathbb{F}_2^{n-1}\},$$

i.e. $F(a, x) = (ax + x\delta, z_x)$. Define a linear mapping $\gamma : \mathbb{F}_2 \times \mathbb{F}_2^{n-1} \to \mathbb{F}_2^{n-1} \times \mathbb{F}_2^{m-n+1}$ by $(a, x)\gamma = (x\delta, 0)$ and set $\overline{F} = F + \gamma$. Then $\overline{F}(a, x) = (ax, z_x)$ and $\overline{F}$ is quadratic and equivalent to F. The restriction of $\overline{F}$ to the subspace $0 \times \mathbb{F}_2^{n-1}$ is a quadratic APN function too, i.e. $g : \mathbb{F}_2^{n-1} \to \mathbb{F}_2^{m-n+1}$ defined by $x \mapsto z_x$, is a quadratic APN function. Clearly $\overline{F}$ is the extension of g. Hence n is odd by Theorem 5.9. The proof is complete. $\square$

The lower bound of Theorem 4.10 can be improved somewhat for APN functions.

Corollary 5.11. *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$, $n \geq 4$, be a quadratic APN function such that the automorphism group contains at least two translation groups. Then the ambient space of f has dimension $\geq 3(n-1)+1$.*

Proof. By Lemma 4.9 we already know that the ambient space has dimension $\geq 3(n-1)$. Suppose that equality holds. Then it follows from Theorem 5.10 that there exists a quadratic APN function $g : \mathbb{F}_2^{n-1} \to \mathbb{F}_2^{n-2}$. But this is in conflict with the following Lemma 5.12. □

Lemma 5.12. *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a normed APN function, $n \geq 3$. Then $m \geq n$.*

Proof. Assume that the assertion is false. Then the elements of the graph of f, for $x \neq 0$, span a space of dimension at most $2n-1$, contradicting [2, Corollary 1 (i)] or [6, Thm. 1.1]. □

Assume that a bilinear DHO or a quadratic APN function admits more than one translation group. Then we know by Theorem 4.6 that the quotient of the normal closure of the translation groups modulo the 2-radical is the extension of a group of odd order by a group of order 2. Theorem 5.10 leads to much more precise information.

Theorem 5.13. *(a) Let $\mathcal{S}$ be a bilinear, n-dimensional DHO, $n \geq 4$, such that $G = \mathrm{Aut}(\mathcal{S})$ contains more than one translation group. Let G^* be the normal closure of the translation groups in G. Then $G^*/O_2(G^*)$ is isomorphic to a dihedral group of order $2k$, $1 < k$ odd. Moreover, G^* can be generated by two translation groups.*

(b) Let f be a quadratic APN-function defined on an $\mathbb{F}_2$ space of dimension ≥ 4, such that $G = \mathrm{A}(f)$ contains more than one translation group. Let G^* be the normal closure of the translation groups in G. Then $G^*/O_2(G^*)$ is isomorphic to a dihedral group of order 6. Moreover, G^* can be generated by two translation groups.

Proof. (a) By Theorem 5.10 $\mathcal{S}$ is the extension of a bilinear, symmetric DHO $\mathcal{S}'$. By Theorem 5.7 $G^*/O_2(G^*)$ is a dihedral group of order $2k$, where k is the order of the multiplicative group of the symmetric nucleus of $\mathcal{S}'$. The claim follows.

(b) follows in the same manner by Theorems 5.10 and 5.9. □

6 Examples

In this section we give concrete examples of extensions of DHOs and APN functions, in particular examples with many translation groups.

Example 6.1. Let $\mathbf{S}$ be the set of skew symmetric 3×3-matrices over $\mathbb{F}_2$. Define $\beta : \mathbb{F}_2^3 \to \mathbf{S}$ by $\beta(0) = 0$ and for $e \neq 0$ let $\beta(e)$ be the unique matrix in $\mathbf{S}$ with $\ker \beta(e) = \langle e \rangle$. Then β defines an alternating DHO (see also case $n = 3$ in the appendix). One has $\mathrm{Aut}(\mathcal{S}_\beta)/T \simeq \mathrm{GL}(3, 2)$ (T the standard translation group). Computer calculations show that the extension $\overline{\mathcal{S}}$ is the Huybrecht DHO (see [27, Sec. 5.3]) of dimension 4 and $\mathrm{Aut}(\overline{\mathcal{S}})/\overline{T} \simeq \mathrm{A}_8 \simeq \mathrm{GL}(4, 2)$ ($\overline{T}$ the standard translation group). This shows that the group N of Theorem 5.1 is in general *not a normal subgroup* of $\mathrm{Aut}(\overline{\mathcal{S}})$, i. e. the group $N_G(N)$ in Theorem 5.7 cannot be replaced by G if $\mathrm{Aut}(\overline{\mathcal{S}})$ contains only one translation group.

The next two examples are based on the following observation (compare with [4, Example 1.2(a)] or [19, Proposition 3]): Let $V = \mathbb{F}_2^n$ and $\beta : V \to \mathrm{GL}(V) \cup 0$, $\beta(0) = 0$, be an injection which defines a spread on $V \times V$ (i. e. $\mathcal{S} = \{S_e \,|\, e \in V\} \cup \{0 \times V\}$, $S_e = \{(x, x\beta(e)) \,|\, e \in V\}$, is a spread). Let $\pi : V \to H$ be a projection on a hyperplane H. Then $\beta \circ \pi : V \to \mathrm{Hom}(V, H)$ defines a DHO on $V \times H$.

Example 6.2. Set $X = \mathbb{F}_{2^n}$ and let $Tr : X \to \mathbb{F}_2$ be the absolute trace. Set $Y = \{x \in X \,|\, Tr(x) = 0\}$ then $Y = \mathrm{Im}\,\pi$ where $x\pi = x + x^2$. Define $\beta : X \to \mathrm{Hom}(X, Y)$ by

$$x\beta(e) = (xe)\pi, \quad x, e \in X.$$

Then β defines a DHO $\mathcal{S} = \mathcal{S}_\beta$ on $X \times Y$, where a typical space of $\mathcal{S}$ has the form $S_e = \{(x, x\beta(e)) \,|\, x \in X\}$. In fact $\mathcal{S}$ is isomorphic to a bilinear DHO of Yoshiara denoted by $\mathcal{S}^d_{d-1,1}$ in [27]: Namely if we define for $e \in X$ the element $a \in X$ by $a^{2^{n-1}} = e$ we observe

$$S_e = S_{a^{2^{n-1}}} = \{(x, a^{2^{n-1}}x + ax^2) | x \in X\},$$

which leads exactly to the description of the DHO of Yoshiara. The automorphism group of $\mathcal{S}$ has the form $T \cdot A$, with T the standard translation group and the autotopism group A. According to [24] the group A is isomorphic to the semidirect product $\mathbb{F}^*_{2^n} \cdot \mathrm{Gal}(\mathbb{F}_{2^n} : \mathbb{F}_2) \simeq \mathrm{C}_{2^n-1} \cdot \mathrm{C}_n$ for $n > 3$.

Clearly, β is symmetric. Let $\overline{\mathcal{S}}$ be the extension of $\mathcal{S}$. Set $G = \mathrm{Aut}(\overline{\mathcal{S}})$.

Let $e, f \in X$, $f \neq 0$. Then $f\beta(e) = \beta(ef)$. Therefore the nucleus $\mathcal{K}$ of $\mathcal{S}$ has the maximal possible order 2^n and it is also the symmetric nucleus, i. e. $\mathcal{K} = \mathcal{K}_0$. By Theorem 5.7 G contains a cyclic subgroup $L_0 \simeq \mathrm{C}_{2^n-1}$, which is inverted by $\tau_{1,0}$ and which acts regularly on the $2^n - 1$ translation groups in G. More precisely, it is easy to see that

$$G/N \simeq \mathrm{C}_{2^n-1} \cdot (\mathrm{C}_n \times \mathrm{C}_2).$$

with $N = O_2(G) = O_2(G^*)$. In fact, $2^n - 1$ is the maximal number of translation groups, which the extension of a symmetric, n-dimensional, bilinear DHO can admit: By Theorem 4.6 $N = O_2(G)$ is elementary abelian of order 2^{2n}. Now $|T \cap N| = 2^n$ and the groups N_0, N_1 lie in N and are disjoint from any translation group. So there can be at most $2^n - 1$ translation groups.

Example 6.3. Let X, Tr, π, and Y have the same meaning as in the previous example. Let $* : X \times X \to X$ be a bilinear composition such that $(X, +, *)$ is a commutative pre-semifield (for background information on (pre-)semifields and the associated translation planes consult [13]). Define $\beta : X \to \mathrm{Hom}(X, Y)$ by

$$x\beta(e) = (x * e)\pi, \quad x, e \in X.$$

Then β defines again a bilinear DHO.

Clearly, β is symmetric. Let $\overline{\mathcal{S}}$ be the extension of $\mathcal{S}$. Set $\mathcal{M} = \{e \in X \mid (x * e) * f = x * (e * f),\ x, f \in X\}$ (in the case of a semifield $\mathcal{M}$ is called the middle nucleus). We see that $\mathcal{M}$ is closed under addition and the $*$-multiplication. Then for $e \in \mathcal{M}$:

$$(x * e)\beta(f) = ((x * e) * f)\pi = (x * (e * f))\pi = (x * (f * e))\pi = x\beta(f * e)$$

Thus $\{(e, e) | e \in \mathcal{M}\}$ is a subring, and hence a subfield, of the symmetric nucleus $\mathcal{K}_0$. Set $G = \mathrm{Aut}(\overline{\mathcal{S}})$. Then by Theorem 5.7 G has at least $|\mathcal{M}^*|$ translation groups, in particular $G = N \cdot A\langle \tau_{1,0} \rangle$, ($A$ isomorphic to the autotopism group of $\mathcal{S}$) if $|\mathcal{M}^*| > 1$.

Consider in particular the pre-semifields defined in [15]: Let $X = \mathbb{F}_q^m$, q a 2-power ≥ 4, and m odd. Then

$$x * y = xy + \left(x \sum_{i=1}^{n} T_i(\zeta_i y) + y \sum_{i=1}^{n} T_i(\zeta_i x) \right)^2$$

defines a commutative pre-semifield multiplications associated with the following data:

1. fields $X = F_0 \supset F_1 \supset \cdots \supset F_n = \mathbb{F}_q$, $n \geq 1$
2. trace maps $T_i : X \to F_i$
3. by a sequence $(\zeta_1, \ldots, \zeta_n)$ of elements $\zeta_i \in X^*$

Clearly, $(x * e) * y = x * (e * y)$ for $e \in F_n$. Thus $\mathcal{M}$ contains a subfield isomorphic to $\mathbb{F}_q$. Therefore $\overline{\mathcal{S}}$ has at least $|F_n| = q - 1 > 1$ translation groups.

Clearly, $\alpha \in \mathrm{Gal}(X : \mathbb{F}_2(\zeta_1, \ldots, \zeta_n))$ induces an automorphism on the pre-semifield $(X, +, *)$ and in turn special autotopisms of $\mathcal{S}$ and $\overline{\mathcal{S}}$. So $\mathrm{Aut}(\overline{\mathcal{S}})$ contains a group of special autotopisms isomorphic to $\mathrm{Gal}(X : \mathbb{F}_2(\zeta_1, \ldots, \zeta_n))$.

Example 6.4. Consider the Gold APN function $f(x) = x^{2^k+1}$, $(k, n) = 1$ on $X = \mathbb{F}_2^n$, n even. If k is odd, then $f(x) = f(x\zeta)$ where $\zeta \in X$ is a primitive third root of unity. This means that f admits nontrivial group of nuclear autotopisms. By Corollary 5.13 the automorphism group $\mathrm{Aut}(F)$ of the extension F of f contains precisely three translation groups.

Appendix: Translation groups for DHOs in small spaces

The n-dimensional DHOs and thus quadratic APN functions defined on n-spaces are known for $n \leq 3$ (note $n > 1$ by definition). The facts with respect to the groups were, unless stated otherwise, obtained by computer.

(1) For $n = 2$ it is easy to see that the ambient space has to have dimension 3. A DHO $\mathcal{S}$ is the dual of an ordinary hyperoval in $PG(2, q)$, and thus, for $q = 2$, unique up to isomorphism. The splitting space Y is one-dimensional, the DHO consist of the 2-spaces which intersect Y trivially and $\mathrm{Aut}(\mathcal{S}) = \mathrm{GL}(3, 2)_Y \simeq \mathrm{S}_4$. The action of this group on the DHO is permutation equivalent to the natural action of the group S_4. The Klein four group T is the unique elementary abelian translation group, in particular the DHO is bilinear. The 3 cyclic groups of order 4 form a class of TI translation groups, each intersects T in a group of order 2.

(2) For $n = 3$ the DHOs $\mathcal{S}$ have been classified by Del Fra [4]. The dimension of the ambient space is either 5 or 6.

There is, up to isomorphism, exactly one DHO $\mathcal{S}$ with an ambient space of dimension 5. This DHO is bilinear and it admits just one elementary abelian translation group. Note that this DHO and the 2-dimensional DHO have a common construction (see [18, Proposition 3]).

If the ambient space has dimension 6 there are, up to isomorphism, two different DHO s. One is the Veronesean DHO [21, 22, 25], which is splitting [29, Lemma 3] but is the union of two orbits under its automorphism group (see [26, Proposition 3.1] or [27, Section 5.2]). It thus can have no translation group and therefore is not equivalent to a bilinear DHO.

The second can be realized as bilinear dimensional DHO $\mathcal{S}_\beta$, where $\beta : \mathbb{F}_2^3 \to \mathrm{End}(\mathbb{F}_2^3)$ is any isomorphism into the space of skew symmetric matrices. It is also Yoshiara's DHO $\mathcal{S}^3_{1,1}$ [27] which is associated with the Gold function $\mathbb{F}_8 \ni x \mapsto x^3 \in \mathbb{F}_8$ (see Example 6.4). The automorphism group has the form $\mathrm{Aut}(\mathcal{S}) \simeq T_\beta \cdot G$, $G \simeq \mathrm{GL}(3, 2)$ (see [24, Proposition 7]). The standard translation group T_β forms one class of translation groups. There is a second class $\mathcal{C}$ of self-centralizing, elementary abelian TI translation groups of size 7. Each member of $\mathcal{C}$ intersects T_β in a group of order 2.

We summarize:

- For $1 < n \leq 3$ any DHO with a translation group is equivalent to an bilinear DHO. The standard translation group T_B is normal in $\mathrm{Aut}(\mathcal{S})$.
- For $1 < n \leq 3$ there are bilinear DHOs having two different conjugacy classes of translation groups in $\mathrm{Aut}(\mathcal{S})$. Each class is a class of TI subgroups but members from different classes intersect nontrivially. For $n = 3$ any translation group is elementary abelian, for $n = 2$ not.

The DHO classification shows that there is, up to isomorphism, exactly one quadratic APN function f on $X = \mathbb{F}_2^n$ for $n = 2$ and one for $n = 3$. Both can be realized as Gold APN function $x \mapsto x^3$ (observe that for $n = 2$ the dimension of its ambient space is only 3).

For $n = 2$, $\mathrm{Aut}(f) \simeq \mathrm{S}_4$. The standard translation group is the unique elementary abelian translation group. The 3 cyclic groups of order 4 form a class of TI translation groups.

For $n = 3$, $\mathrm{Aut}(f) \simeq \mathrm{S}_8$. There is only one orbit of translation groups. It has length 30 and the translations are not TI groups.

Acknowledgements and Remarks. (a) We thank the referees for helpful comments and suggestions. Referee 1 pointed out a gap in the original proof of a weaker version of Theorem 5.7 prompting a significant extension and improvement of Section 5. Clarifications of definitions and proofs are due to both referees 1 and 2.
(b) Satoshi Yoshiara [31] independently obtained the main results of Section 4.

References

[1] C. Bracken, E. Byrne, G. McGuire, G. Nebe. On the equivalence of quadratic APN functions, *Designs, Codes and Cryptography*, 61:261–272, 2011.

[2] C. Carlet, P. Charpin, and V. Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Designs, Codes and Cryptography*, 15(2):125–156, 1998.

[3] J. Conway, R. Curtis, R. Parker, R. Wilson. *Atlas of finite Groups*, Clarendon Press, 1985.

[4] A. Del Fra. On d-dimensional dual hyperovals. *Geometriae Dedicata*, 79:157–178, 2000.

[5] U. Dempwolff. Doubly dual dimensional hyperovals and bent functions. *Innovations in Incidence Geometry*, to appear.

[6] J. Dillon. On the dimension of an APN code. *Cryptogr. Commun.*, 3:275–279, 2011.

[7] Y. Edel. On quadratic APN functions and dimensional dual hyperovals. *Des. Codes Cryptogr.*, 57(1):35–44, 2010.

[8] Y. Edel, A. Pott. A new almost perfect nonlinear function which is not quadratic. *Adv. Math. Commun.*, 3:59–81, 2010.

[9] F. Göloğlu and A. Pott. Almost perfect nonlinear functions: A possible geometric approach. In *Proceedings of the Contact Forum* Coding Theory and Cryptography II *at The Royal Flemish Academy of Belgium for Science and the Arts 2007*, pages 75–100.

[10] D. Gorenstein. *Finite Groups*, Harper and Row, 1968.

[11] R. Hartley. Determination of the ternary linear collineation groups whose coefficients lie in GF(2^n), *Ann. Math.*, 27:140-158, 1925.

[12] B. Huppert. *Endlichen Gruppen I*, Springer, 1967.

[13] N. Johnson, M. Biliotti, V. Jha. *Handbook of Finite Translation Planes*, CRC, 2007.

[14] W. M. Kantor. Permutation representations of the finite classical groups of small degree or rank, *J. Algebra* 60:158-168, 1979.

[15] W. M. Kantor. Commutative semifields and symplectic spreads, *J. Algebra* 270:98-114, 2003.

[16] H. Kurzweil, B. Stellmacher. *Theorie der endlichen Gruppen*, Springer, 1998.

[17] M. Suzuki. A class of doubly transitive groups, *Ann. Math.* 75:105-145, 1962.

[18] H. Taniguchi. On some d-dimensional dual hyperovals in $PG(2d, 2)$. *Finite Fields And Their Applications*, 14:1010–1019, 2008.

[19] H. Taniguchi. On the duals of certain d-dimensional dual hyperovals in $PG(2d + 1, 2)$. *Finite Fields And Their Applications*, 15:673–681, 2009.

[20] H. Taniguchi. On the dual of the dual hyperoval from APN function $f(x) = x^3 + tr(x^9)$. *Finite Fields And Their Applications*, 18:210–221, 2012. Personal communication, 2010.

[21] J. A. Thas and H. Van Maldeghem. Characterizations of quadric and hermitian veroneseans over finite fields. *Journal of Geometry*, 76(1-2):282–293, 2003.

[22] J. A. Thas and H. Van Maldeghem. Characterizations of the finite quadric veroneseans V_n^{2n}. *The Quarterly Journal of Mathematics*, 55(1):99–113, 2004.

[23] F. Timmesfeld. Groups with weakly closed TI-subgroups, *Math. Z.* 143:243–278, 1975.

[24] S. Yoshiara. A family of d-dimensional dual hyperovals in $\mathrm{PG}(2\mathrm{d} + 1, 2)$. *European Journal of Combinatorics*, 20(6):589–603, 1999.

[25] S. Yoshiara. Ambient spaces of dimensional dual arcs. *J. Alg. Combin.*, 19:5–23, 2004.

[26] S. Yoshiara. Automorphism Groups of Dimensional Dual Hyperovals. *RIMS Kôkyûroku*, 1476:214–233, 2006.

[27] S. Yoshiara. Dimensional dual arcs – a survey. In *Finite Geometries, Groups, and Computation: Proceedings of the Conference 'Finite Geometries, Groups, and Computation', September 4-9, 2004 Pingree Park, Colorado*, 2006.

[28] S. Yoshiara. Dimensional dual hyperovals associated with quadratic APN functions. *Innovations in Incidence Geometry*, 8:147–169, 2008.

[29] S. Yoshiara. Notes on split dimensional dual hyperovals. Manuscript, 2009.

[30] S. Yoshiara. Equivalences of quadratic APN functions. *Journal of Algebraic Combinatorics*, 35:461–475, 2012. Personal communication, 2010.

[31] S. Yoshiara. Personal communication, 2012.