INTEGRAL AUTOMORPHISMS OF AFFINE SPACES OVER FINITE FIELDS

ISTVÁN KOVÁCS, KLAVDIJA KUTNAR, JÁNOS RUFF, AND TAMÁS SZŐNYI

ABSTRACT. A permutation of the point set of the affine space $\mathrm{AG}(n,q)$ is called an integral automorphism if it preserves the integral distance defined among the points. In this paper, we complete the classification of the integral automorphisms of $\mathrm{AG}(n,q)$ for $n \geq 3$.

1. INTRODUCTION

Throughout the paper p stands for an odd prime. Let $\mathbb{F}_q$ be the finite field with $q = p^h$ elements and $\mathrm{AG}(n,q)$ be the n-dimensional affine space defined over $\mathbb{F}_q$. The *Euclidean distance* d is defined as

$$d(\mathbf{x},\mathbf{y}) = \sum_{i=1}^{n}(x_i - y_i)^2$$

for the points $\mathbf{x} = (x_1,\dots,x_n)$ and $\mathbf{y} = (y_1,\dots,y_n) \in \mathbb{F}_q^n$. Two points $\mathbf{x}$ and $\mathbf{y}$ are said to be at *integral distance* if $d(\mathbf{x},\mathbf{y})$ is a square element in $\mathbb{F}_q$, and a set of points is called *integral* if any two of its points are at integral distance. Recently, the finite field analog of the classical probem about integral point sets in $\mathbb{R}^n$ has attracted considerable attention. See, for example, [5] and the references therein. Besides integral point sets, permutations, preserving the integral distances, are also considered in [7, 8, 9, 10]. By an *integral automorphism* of $\mathrm{AG}(n,q)$ we mean any bijective mapping $\gamma : \mathbb{F}_q^n \to \mathbb{F}_q^n$ satisfying

$$d(\mathbf{x},\mathbf{y}) \in \square_q \iff d(\mathbf{x}^\gamma,\mathbf{y}^\gamma) \in \square_q$$

for all $\mathbf{x}$, $\mathbf{y} \in \mathbb{F}_q^n$. Here and in what follows $\square_q$ denotes the set of all square elements of $\mathbb{F}_q$. We adopt the notation used in [7] and denote the group of all integral automorphisms by $\mathrm{Aut}(\mathbb{F}_q^n)$.

Integral automorphisms of the plane $\mathrm{AG}(2,q)$ were determined in [7, 8, 9]. In particular, $\mathrm{Aut}(\mathbb{F}_q^2)$ was found by Kurz [9] for $q \equiv 3 \pmod 4$, and by Kovács and Ruff [8] for $q \equiv 1 \pmod 4$. We remark that the special case $q = p$ was settled earlier by Kiermaier and Kurz [7]. It turns out that there exist integral automorphisms of $\mathrm{AG}(2,q)$ which are not semiaffine transformations, and this occurs exactly when $q \equiv 1 \pmod 4$. As for higher dimensions, Kurz and Meyer [10] desrcibed the integral automorphisms which are also semiaffine transformations. In what follows we denote by $\mathbb{F}_q^\times$ the multiplicative group of $\mathbb{F}_q$, by $\mathrm{GL}(n,q)$ the group of invertable n-times-n matricies with entries from $\mathbb{F}_q$, and by σ the semiaffine transformation defined by $(x_1 \dots, x_n) \mapsto (x_1^p,\dots,x_n^p)$.

2010 Mathematics Subject Classification. 20B25.
Key words and phrases. finite field, affine space, integral automorphism.

Theorem 1 (Kurz and Meyer [10]). *If $q = p^h$ and $n \geq 3$, then the semiaffine transformations contained in* $\mathrm{Aut}(\mathbb{F}_q^n)$ *are given as*

$$\mathbf{x} \mapsto a\mathbf{x}^{\sigma^i}A + \mathbf{b}$$

where $a \in \mathbb{F}_q^\times, i \in \{0, \dots, h-1\}, A \in \mathrm{GL}(n,q)$ with $AA^T = I$ and $\mathbf{b} \in \mathbb{F}_q^n$.

Our goal in this paper is to show that, in contrast with the plane, all integral automorphisms of $\mathrm{AG}(n,q)$ are semiaffine transformations whenever $n \geq 3$. This together with Theorem 1 result in the following classification theorem.

Theorem 2. *Let $q = p^h$ for an odd prime p and suppose that $n \geq 3$. Then the integral automorphisms of* $\mathrm{AG}(n,q)$ *are the mappings*

$$\mathbf{x} \mapsto a\mathbf{x}^{\sigma^i}A + \mathbf{b}$$

where $a \in \mathbb{F}_q^\times, i \in \{0, \dots, h-1\}, A \in \mathrm{GL}(n,q)$ with $AA^T = I$ and $\mathbf{b} \in \mathbb{F}_q^n$.

2. The proof of Theorem 2

The key part in the proof of Theorem 2 will be to show that every integral automorphism $\gamma \in \mathrm{Aut}(\mathbb{F}_q^n)$ satisfies

$$d(\mathbf{x}, \mathbf{y}) = 0 \iff d(\mathbf{x}^\gamma, \mathbf{y}^\gamma) = 0 \text{ for all } \mathbf{x},\, \mathbf{y} \in \mathbb{F}_q^n. \tag{1}$$

This enables us to use the result of Lester [12] about cone preserving mappings. Let V be a nonsingular metric vector space over a field $\mathbb{F}$ not of characteristic two, upon which is defined a nonsingular symmetric bilinear form $\langle ., . \rangle$. The *cone* $C(\mathbf{a})$ with vertex $\mathbf{a} \in V$ is defined to be the set $C(\mathbf{a}) := \{\mathbf{x} \in V : \langle \mathbf{x} - \mathbf{a}, \mathbf{x} - \mathbf{a} \rangle = 0\}$, and a mapping $f : V \to V$ is said to *preserve the cones* if $(C(\mathbf{a}))^f = C(\mathbf{a}^f)$ for all $\mathbf{a} \in V$.

Theorem 3 (Lester [12]). *Let V be a nonsingular metric vector space over the field $\mathbb{F}$, with bilinear form $\langle ., . \rangle$; assume that* $\dim(V) \geq 3$ *and that V is not anisotropic (that is, $\langle \mathbf{x}, \mathbf{x} \rangle = 0$ for some nonzero vecor $\mathbf{x}$). Let $f : V \to V$ be a bijection of V which preserves cones. Then f is in the form*

$$f : \mathbf{x} \mapsto L(\mathbf{x}) + \mathbf{b}$$

where $\mathbf{b} \in V$, and (L, ρ) is a semilinear transformation of V satisfying $\langle L(\mathbf{x}), L(\mathbf{y}) \rangle = a\langle \mathbf{x}, \mathbf{y} \rangle^\rho$ for some nonzero $a \in \mathbb{F}$ and for all $\mathbf{x}$, $\mathbf{y} \in V$.

Now, if $\gamma \in \mathrm{Aut}(\Gamma)$ satisfies (1), then it preserves the cones of the metric vector space $V := \mathbb{F}_q^n$ endowed with the symmetric bilinear form $\langle ., . \rangle$ defined by $\langle \mathbf{x}, \mathbf{y} \rangle := \mathbf{x}\mathbf{y}^T$ for all vectors $\mathbf{x}$, $\mathbf{y} \in V$. Therefore, by Theorem 3, γ is a semiaffine transformation, and Theorem 2 follows. In fact, we are going to derive (1) in the end of this section following two preparatory lemmas.

For the rest of the paper we let $G = \mathrm{Aut}(\mathbb{F}_q^n)$, $n \geq 3$, and let $G_{\mathbf{0}}$ be the stabilizer of $\mathbf{0}$ in G where $\mathbf{0} = (0, \dots, 0) \in \mathbb{F}_q^n$. We start by introducing two subgroups of G:

$$\begin{aligned} E &= \big\{\mathbf{x} \mapsto \mathbf{x} + \mathbf{b} : \mathbf{b} \in \mathbb{F}_q^n\big\}, \\ M &= \big\{\mathbf{x} \mapsto a\mathbf{x}A : a \in \mathbb{F}_q^\times, A \in \mathrm{GL}(n,q) \text{ and } AA^T = I\big\}. \end{aligned}$$

Notice that, by Theorem 1, both E and M are subgroups of G. The elements of E are also called *translations*. Clearly, E is an elementary abelian group of order p^{hn}, and it is regular on $\mathbb{F}_q^n$. The group M normalizes E, hence $\langle E, M\rangle = EM$.

Define the subsets of $\mathbb{F}_q^n$ as

$$\begin{aligned} S_0 &= \Big\{\mathbf{x} \in \mathrm{AG}(n,q) : \sum_{i=1}^n x_i^2 = 0, \mathbf{x} \neq \mathbf{0}\Big\},\\ S_+ &= \Big\{\mathbf{x} \in \mathrm{AG}(n,q) : \sum_{i=1}^n x_i^2 \in \square_q \setminus \{0\}\Big\},\\ S_- &= \Big\{\mathbf{x} \in \mathrm{AG}(n,q) : \sum_{i=1}^n x_i^2 \notin \square_q\Big\}. \end{aligned}$$

Lemma 1. *With the above notation,*

(i) The M-orbits are $\{\mathbf{0}\}, S_0, S_+$ and S_-.
(ii) EM is primitive on $\mathbb{F}_q^n$.

Proof. Part (i) is proved in [10, Lemma 3.17].

To settle (ii) we apply [2, Theorem 3.2A], that is, EM is primitive if and only if $\mathrm{Graph}(\Delta)$ is connected for each nondiagonal orbital Δ of EM. Observe that, a nondiagonal orbital Δ consists of the ordered pairs in the form $(\mathbf{x}, \mathbf{x}+\mathbf{y})$, where $\mathbf{x}$ runs over $\mathbb{F}_q^n$ and $\mathbf{y}$ runs over S_ε for a fixed $\varepsilon \in \{0,+,-\}$. Now, the connectedness of $\mathrm{Graph}(\Delta)$ follows because each of S_0, S_+ and S_- spans the vector space $\mathbb{F}_q^n$. $\square$

By Lemma 1(i), EM has nontrivial subdegrees $|S_\varepsilon|, \varepsilon \in \{0,+,-\}$. The exact values were computed in [10, Theorem 4.3]:

$$|S_0| = \begin{cases} q^{n-1} - 1 & \text{if } n \text{ is odd}\\ q^{n-1} + (-1)^{\frac{\varepsilon n}{2}} q^{\frac{n}{2}} - (-1)^{\frac{\varepsilon n}{2}} q^{\frac{n-2}{2}} - 1 & \text{if } n \text{ is even} \end{cases} \tag{2}$$

$$|S_+| = \begin{cases} \frac{1}{2}\Big(q^n - q^{n-1} + (-1)^{\frac{\varepsilon(n+3)}{2}} q^{\frac{n+1}{2}} - (-1)^{\frac{\varepsilon(n-1)}{2}} q^{\frac{n-1}{2}}\Big) & \text{if } n \text{ is odd}\\ \frac{1}{2}\Big(q^n - q^{n-1} - (-1)^{\frac{\varepsilon n}{2}} q^{\frac{n}{2}} + (-1)^{\frac{\varepsilon n}{2}} q^{\frac{n-2}{2}}\Big) & \text{if } n \text{ is even} \end{cases} \tag{3}$$

$$|S_-| = \begin{cases} \frac{1}{2}\Big(q^n - q^{n-1} - (-1)^{\frac{\varepsilon(n+3)}{2}} q^{\frac{n+1}{2}} + (-1)^{\frac{\varepsilon(n-1)}{2}} q^{\frac{n-1}{2}}\Big) & \text{if } n \text{ is odd}\\ \frac{1}{2}\Big(q^n - q^{n-1} - (-1)^{\frac{\varepsilon n}{2}} q^{\frac{n}{2}} + (-1)^{\frac{\varepsilon n}{2}} q^{\frac{n-2}{2}}\Big) & \text{if } n \text{ is even} \end{cases} \tag{4}$$

where $\varepsilon = 0$ if $q \equiv 1 \pmod 4$ and $\varepsilon = 1$ otherwise.

The set $S_0 \cup S_+$ consists of the points being at integral distance from $\mathbf{0}$. Therefore, every $\gamma \in G_{\mathbf{0}}$ maps $S_0 \cup S_+$ to itself, and this leaves us with two possibilities for the nontrivial $G_{\mathbf{0}}$-orbits, namely, these are either S_0, S_+ and S_-, or $S_0 \cup S_+$ and S_-. In particular, the group G has rank either 3 with nontrivial subdegrees $|S_0| + |S_+|$ and $|S_-|$, or 4 with nontrivial subdegrees $|S_0|, |S_+|$ and $|S_-|$.

As the next step, we find the *socle* $\mathrm{Soc}(G)$. Recall that $\mathrm{Soc}(G)$ is the subgroup of G generated by all its minimal normal subgroups.

Lemma 2. *With the above notation, the socle* $\mathrm{Soc}(G) = E$.

Proof. Let $H = \mathrm{Soc}(G)$. Since $EM \leq G$ is primitive, see Lemma 1(ii), G is primitive as well. Thus H is a direct product of isomorphic simple groups (see [2, Corollary 4.3B]), and we may write $H = T \times \cdots \times T = T^k$ for some simple group T and $k \geq 1$. By the O'Nan-Scott theorem, G and H are described by one of the following types (see, for example, [2, pp. 137]):

(T1) H is an elementary abelian p-group of order q^n which is regular on $\mathbb{F}_q^n$.
(T2) H is nonabelian and regular on $\mathbb{F}_q^n$.
(T3) $H = T$ is nonabelian, it is not regular on $\mathbb{F}_q^n$, and $G \leq \mathrm{Aut}(H)$.
(T4) H is nonabelian and G is a subgroup of a wreath product with the diagonal action. In this case $k \geq 2$ and $|T|^{k-1} = q^n$.
(T5) H is nonabelian, $k = k_1k_2$ and $k_2 > 1$. The group G is isomorphic to a subgroup of the wreath product $U\,wr\,S_{k_2}$ with the product action, where U is a primitive permutation group of degree d such that $q^n = d^{k_2}$, U has socle T^{k_1}, and U is of type (T3) or (T4).

We show below that G is of type (T1). It is not hard to show that this yields $H = E$ (see, for example, [8]). Now, suppose to the contrary that G is one of types $(T2)-(T5)$. In either case T is a nonabelian simple group. This observation excludes at once types (T2) and (T4).

Suppose next that G is of type (T3). Then $T = H$, and since it is a normal subgroup of a primitive group, it acts transitively on $\mathbb{F}_q^n$. It was proved by Guralnick [4] that, if a finite nonabelian simple group L acts transitively on a set Ω such that $|\Omega|$ is a prime power, then L acts 2-transitively unless $L \cong \mathrm{PSU}(4,2)$ and $|\Omega| = 27$ with nontrivial subdegrees 10 and 16 (see [4, Corollary 2]). Since G cannot be 2-transitive, $q^n = 27$ and the nontrivial subdegrees of G are 10 and 16. This, however, contradicts that $|S_-| = 12$ is a subdegree, see the remark before the lemma and (4).

We are left with the case that G is of type (T5). Denote by r_G and r_U the rank of G and U, respectively. Recall that $r_G \in \{3,4\}$. By [2, Exercise 4.8.1],

$$r_G \geq \binom{r_U + k_2 - 1}{k_2}. \tag{5}$$

The group U is of type (T3) or (T4). In the latter case $|T| = p^a$ for some a, a contradiction. Thus U is of type (T3), $k_1 = 1$, $k = k_2$ and T is a transitive permutation group of a set X of size $|X| = q^{n/k_2}$. By the aforementioned result of Guralnick, U is 2-transitive unless $T \cong \mathrm{PSU}(4,2)$, $q^{n/k_2} = 27$, and $r_U = 3$. In the latter case, however, we find in (5) that $r_G \geq \frac{1}{2}(k_2+2)(k_2+1) \geq 6$ (recall that $k_2 > 1$), a contradiction. Thus $r_U = 2$, implying in (5) that $k = k_2 = 2$ and $r_G = 3$, or $k = k_2 = 3$ and $r_G = 4$.

Case 1. $k_2 = 2$, $r_G = 3$ and $G \leq U\,wr\,S_2$.

The wreath product $U\,wr\,S_2$ acts by the product action. This means that $\mathbb{F}_q^n$ can be written as $\mathbb{F}_q^n = X \times X$, $|X| = q^{n/2}$, and U is a permutation group of X. We have $U\,wr\,S_2 = \langle U \times U, \tau\rangle = \langle U \times U\rangle \rtimes \langle\tau\rangle$, where $U \times U$ acts on $X \times X$ naturally, and τ acts by switching the coordinates. The socle $H = T \times T \leq U \times U$, and since T is 2-transitive on X, $\Delta_1 := \{(x_0, x) : x \in X \setminus \{x_0\}\}$ and $\Delta_2 := \{(x, x_0) : x \in X \setminus \{x_0\}\}$ are orbits under the stabilizer $(U \times U)_{(x_0,x_0)}$, and any other orbit different from $\{(x_0, x_0)\}$ is contained in the set $\Delta_3 := \{(x, y) : x, y \in X \setminus \{x_0\}\}$. Now, $G_{(x_0,x_0)} = (U \times U)_{(x_0,x_0)} \rtimes \langle\tau\rangle$, and this gives that any $G_{(x_0,x_0)}$-orbit different from $\{(x_0,x_0)\}$ is contained in either $\Delta_1 \cup \Delta_2$ or Δ_3. Since the rank $r_G = 3$, we find that the nontrivial subdegrees of G are $|\Delta_1 \cup \Delta_2| = 2(q^{n/2}-1)$ and $|\Delta_3| = (q^{n/2}-1)^2$. On the other hand $|S_-|$ is a subdegree which is divisible by q, see (4) (we use here that $n \geq 3$).

Case 2. $k_2 = 3$, $r_G = 4$ and $G \leq U\, wr\, S_3$.

In this case $\mathbb{F}_q^n$ can be written as $\mathbb{F}_q^n = X \times X \times X$, $|X| = q^{n/3}$, and U is a permutation group of X. The wreath product $U\, wr\, S_3 = \langle U \times U \times U\rangle \rtimes K$, where $U \times U \times U$ acts on $X \times X \times X$ naturally, $K \cong S_3$, and K acts by permuting the coordinates. The socle $H = T \times T \times T \leq U \times U \times U$ and T is 2-transitive on X. Now, $G_{(x_0,x_0,x_0)} \leq (U \times U \times U)_{(x_0,x_0,x_0)} \rtimes K$, and this gives that any $G_{(x_0,x_0,x_0)}$-orbit different from $\{(x_0,x_0,x_0)\}$ is contained in one of the sets $\{(x,x_0,x_0),(x_0,x,x_0),(x_0,x_0,x) : x \in X \setminus \{(x_0,x_0,x_0)\}\}$, $\{(x,y,x_0),(x,x_0,y),(x_0,x,y) : x,y \in X \setminus \{(x_0,x_0,x_0)\}\}$ and $\{(x,y,z) : x,y,z \in X \setminus \{(x_0,x_0,x_0)\}\}$. Because of this and $r_G = 4$ we find that the nontrivial subdegrees of G are $3(q^{n/3}-1)$, $3(q^{n/3}-1)^2$ and $(q^{n/3}-1)^3$. On the other hand these subdegress are $|S_\varepsilon|$, $\varepsilon \in \{0,+,-\}$, and as $q^{\lceil \frac{n-2}{2} \rceil}$ divides both $|S_+|$ and $|S_-|$ and n is divisible by 3, we obtain that $(q,n) = (3,3)$, and therefore, $U \cong S_3$ and $T \cong \mathbb{Z}_3$, contradicting that T is nonabelian. □

Finally, we are ready to settle (1).

Lemma 3. *Let $\gamma \in \mathrm{Aut}(\mathbb{F}_q^n)$ be an arbitrary automorphism and let $n \geq 3$. Then γ satisfies* (1).

Proof. Suppose for the moment that $q = p$. By Lemma 1, $E = \mathrm{Soc}(G)$, in particular, E is normal in G. Now, since $q = p$, we obtain that γ is an affine transformation, and this implies that it satisfies (1).

From now it will be assumed that $q \neq p$. Assume to the contrary that there exist vectors $\mathbf{a}$ and $\mathbf{b}$ such that either $d(\mathbf{a},\mathbf{b}) = 0$ and $d(\mathbf{a}^\gamma,\mathbf{b}^\gamma) \neq 0$, or $d(\mathbf{a},\mathbf{b}) \neq 0$ and $d(\mathbf{a}^\gamma,\mathbf{b}^\gamma) = 0$. Here we deal only with the first case because the second one can be treated in a very similar way. Consider the product $\gamma' := \gamma_1\gamma\gamma_2$ where γ_1 and γ_2 are the translations $\mathbf{x} \mapsto \mathbf{x}+\mathbf{a}$ and $\mathbf{x} \mapsto \mathbf{x}-\mathbf{a}^\gamma$, respectively. Then $\mathbf{0}^{\gamma'} = \mathbf{0}$, $\mathbf{b}-\mathbf{a} \in S_0$, and $(\mathbf{b}-\mathbf{a})^{\gamma'} = \mathbf{b}^\gamma - \mathbf{a}^\gamma \in S_+$. These imply that the $G_{\mathbf{0}}$-orbits are $\{\mathbf{0}\}, S_0 \cup S_+$ and S_- (see also the remark before Lemma 2), and thus G has nontrivial subdegress:

$$|S_0| + |S_+| \text{ and } |S_-|. \tag{6}$$

By Lemma 2, G is of type (T1). All possible nontrivial subdegress of a finite primitive affine permutation group of rank 3 were computed by Foulser [3] and Liebeck [11]. If L is such a group acting an a vector space V of cardinality p^d, and L_0 denotes the stabilizer of the zero vector 0, then one of the following holds:

Infinite classes (A): L is in one of 11 inifinite classes of permutation groups labeled by (A1)–(A11). If L is in class (A1), then L_0 is isomorphic to a subgroup of $\Gamma\mathrm{L}(1,p^d)$; and if L is in class (A2)–(A11), then $d = 2r$ and L has nontrivial subdegrees listed in Table 2 (see [11, Table 12]).

'Extraspecial' classes (B): L is one of a finite set of permutation groups whose degree is equal to one of the following numbers ([11, Table 1]):

$$2^6,\ 3^4,\ 3^6,\ 3^8,\ 5^4,\ 7^2,\ 7^4,\ 13^2,\ 17^2,\ 19^2,\ 23^2,\ 29^2,\ 31^2,\ 47^2. \tag{7}$$

row	subdegrees	conditions
1.	$(p^s+1)(p^r-1), \quad p^s(p^r-1)(p^{r-s}-1)$	$s=0$ or $s \mid r$ or $s=2r/5$ and $5 \mid r$ or $s=3r/4$ and $4 \mid r$ or $s=3r/8$ and $8 \mid r$
2.	$(p^{r-s}+1)(p^r-1), \quad p^{r-s}(p^r-1)(p^s-1)$	$s \mid r$
3.	$(p^{r-s}-1)(p^r+1), \quad p^{r-s}(p^r+1)(p^s-1)$	$s \mid r$ and $s \neq r$

Table 1. Nontrivial subdegrees of affine groups of rank 3 in classes (A2)–(A11).

'Exceptional' classes (C): L is one of a finite set of permutation groups whose degree is equal to one of the following numbers ([11, Table 2]):

$$2^6,\ 2^8,\ 2^{11},\ 2^{12},\ 3^4,\ 3^5,\ 3^6,\ 3^{12},\ 5^4,\ 5^6,\ 7^4,\ 31^2,\ 41^2,\ 71^2,\ 79^2,\ 89^2. \tag{8}$$

We are going to arrive at a contradiction after comparing the subdegress described in classes (A)–(C) with our subdegrees in (6).

Suppose that G is in class (A). If G is in class (A1), then $G_{\mathbf{0}}$ is isomorphic to a subgroup of $\Gamma\mathrm{L}(1,q^n)$, hence $|G_{\mathbf{0}}|$ divides $|\,\Gamma\mathrm{L}(1,q^n)|=hn(q^n-1)$. Each subdegree of G divides $|G_{\mathbf{0}}|$. In particular, $|S_-| \mid |G_{\mathbf{0}}|$, and by (4), $p^{h\lceil\frac{n-2}{2}\rceil} \mid hn(q^n-1)$. From this we obtain that $p^m \le 4m$ where p is an odd prime and $m=h\lceil\frac{n-2}{2}\rceil \ge 2$ (recall that $n \ge 3$ and $h \ge 2$ because of $q \ne p$). This, however, contradicts the inequality $p^m > 4m$, which can be easily settled by induction on m.

Let G be in class (Ai) for $i>1$. As before, let $m=h\lceil\frac{n-2}{2}\rceil$. By (4), p^m is the largest p-power dividing the subdegree $|S_-|$, and we get $2|S_-|/p^m \equiv \pm 1 \pmod q$. Thus

$$2|S_-|/p^m \equiv \pm 1 \pmod{p}^2. \tag{9}$$

Let us compute the residue of $2|S_-|/p^m$ modulo p^2 by the help of Table 1. Since $q^n=p^{2r}$, it follows that $2r=hn$, and hence $r \ge 3$. Suppose that $|S_-|$ occurs in the 1st row of Table 1. In this case $m=s$. It follows that if $r \ne 4$ and $s \ne 3$, then $r-s \ge 2$, and this implies that $2|S_-|/p^m \equiv 2 \pmod{p^2}$, contradicting (9). Let $r=4$ and $s=3$. Then $hn=8$, thus m is even, which contradicts that $m=s=3$. Now, suppose that $|S_-|$ occurs in the 2nd or the 3rd row of Table 1. In this case $m=r-s$, and if $s \ne 1$, then $2|S_-|/p^m \equiv \pm 2 \pmod{p^2}$, contradicting (9). Let $s=1$. Then $h\frac{n}{2}-1=r-1=m=h\lceil\frac{n-2}{2}\rceil$. We obtain that $h=2$ and n is odd. Then $q=p^2 \equiv 1 \pmod 4$. If $|S_-|$ is equal to number in the 2nd row, then by (4), $p^{n+1}-p^{n-1}-p^2+1=2p^{n+1}-2p^n-2p+2$, and if it is equal to number in the 3rd row, then $p^{n+1}-p^{n-1}-p^2+1=2p^{n+1}-2p^n+2p-2$. It is easy to see that none of these equations holds for $n \ge 3$ and an odd prime p.

Suppose that the group G is in class (B). We obtain from (7) that $(q,n)=(9,3)$ or $(9,4)$. By [3, Theorem 1.1] in the first case and by [11, Table 13] in the second case, the corresponding subdegress are:

q^n	nontrivial subdegrees
9^3	104, 624
9^4	1440, 5120

However, none of these match the numbers given in (6).

Finally, suppose that G is in class (C). Then we obtain from (8) that $(q,n) \in \{(9,3),(25,3),(81,3),(27,4),(9,6)\}$. By [11, Table 14], the corresponding nontrivial subdegrees are:

q^n	nontrivial subdegrees
3^6	224, 504
5^6	7560, 8064
3^{12}	65520, 465920

However, none of these match the numbers in (6). The lemma is proved. □

Remark 1. We would like to note that in our earlier approach we gave a proof of Theorem 2, which also relies on Lemmas 1-3, but instead of invoking Lester's result (Theorem 3), we used the results of Iosevich et al. [5] on maximum point sets with any two of its points being at distance 0. Here we give an outline. Let $\gamma \in \mathrm{Aut}(\mathbb{F}_q^n)$ be an integral automorphism which fixes the zero vector $\mathbf{0}$. We need to prove that γ is a semilinear transformation. By the fundamental theorem of projective geometry we are done if we show that γ preserves both the point and the line set of the projective space $\mathrm{PG}(n-1,q)$. Let us consider the nonsingular quadric $\mathcal{Q}$ of $\mathrm{PG}(n-1,q)$ induced by the quadratic form $x_1^2 + \cdots + x_n^2$. A projective subspace of maximum dimension on $\mathcal{Q}$ is called a *generator* (cf. [6, Chapter 22]). Observe that, any subspace U of $\mathbb{F}_q^n$ corresponding to a generator has the property that any two of its points are at distance 0. It follows from [5, Theorem 2 and Lemma 4] that U is a maximum point set with the latter property, and thus γ maps U to a subspace. The latter subspace is contained in S_0, see Lemma 3, and we conclude that γ permutes the generators among themselves. This observation and the fact that any point of $\mathcal{Q}$ can be expressed as the intersection of some generators yield that γ preserves the set of points on $\mathcal{Q}$. Then, using Lemma 2, we find that any line of $\mathrm{PG}(n-1,q)$ through two points of $\mathcal{Q}$ is mapped by γ to a line. If $(n,q) \neq (3,3)$, then any point of $\mathrm{PG}(n-1,q)$ can be expressed as the intersection of some lines connecting two points of $\mathcal{Q}$, and this with the previous observation yield that γ preserves the point set of $\mathrm{PG}(n-1,q)$. Finally, using again Lemma 2, we conclude that γ preserves the line set of $\mathrm{PG}(n-1,q)$ as well.

Acknowledgements

The authors are grateful to Marko Orel for drawing their attention to the work of Lester [12]. This research was supported in part by the bilateral Slovenian-Hungarian Joint Research Project, grant no. NN 114614 (in Hungary) and N1-0032 (in Slovenia). The first two authors also thank the Slovenian Research Agency ARRS (research program P1-0285 and research projects N1-0038, J1-5433, J1-6720 and J1-6743), and the second author was also supported in part by WoodWisdom-Net+, $\mathrm{W}^3\mathrm{B}$.

References

[1] W. Bosma, J. Cannon, and C. Playoust, The Magma Algebra System I: The User Language, *J. Symbolic Comput.* **24** (1997), 235–265.

[2] J. D. Dixon and B. Mortimer, Permutation groups, Graduate Texts in Mathematics 163, Springer-Verlag 1996.

[3] D. A. Foulser, Solvable primitive permutation groups of law rank, *Trans. Amer. Math. Soc.* **143** (1969), 1–54.
[4] R. M. Guralnick, Subgroups of prime power index in a simple group, *J. Algebra* **81** (1983), 304–311.
[5] A. Iosevich, I. E. Shparlinski, M. Xiong, Sets with integral distances in finite fields, *Trans. Amer. Math. Soc.* **362** (2010), 2189–2204.
[6] J. W. P. Hirschfeld, J. A. Thas, General Galois geometries, Clarendon Press, Oxford 1991.
[7] M. Kiermaier, S. Kurz, Maximal integral point sets in affine planes over finite fields, *Discrete Math.* **309** (2009), 4564–4575.
[8] I. Kovács, J. Ruff, Integral automorphisms of affine planes over finite fields, *Finite Fields Appl.* **27** (2014), 104–114.
[9] S. Kurz, Integral point sets over finite fields, *Australas J. Combin* **43** (2007), 3–29.
[10] S. Kurz, H. Meyer, Integral point sets in higher dimensional affine spaces over finite fields, *J. Combin. Theory Ser. A* **116** (2009), 1120–1139.
[11] M. W. Liebeck, The affine permutation groups of rank three, *Proc. London Math. Soc.* (3) **54** (1987), 477–516.
[12] J. A. Lester, Cone preserving mappings for quadratic cones over arbitrary fields, *Canad. J. Math.,* **29** (6) (1977), 1247–1253.

I. Kovács, IAM and FAMNIT, University of Primorska, Glagoljaška 8, 6000 Koper, Slovenia
E-mail address: istvan.kovacs@upr.si

K. Kutnar, IAM and FAMNIT, University of Primorska, Glagoljaška 8, 6000 Koper, Slovenia
E-mail address: klavdija.kutnar@upr.si

Institute of Mathematics and Informatics, University of Pécs, Ifjúság útja 6, 7624 Pécs, Hungary
E-mail address: janosruff@gmail.com

Institute of Mathematics, Eötvös University, Pázmány P. s. 1/C, 1117 Budapest, Hungary & MTA-ELTE Geometric and Algebraic Combinatorics Research Group
E-mail address: szonyi@cs.elte.hu