Adv. Geom. **2** (2002), 81–98

Advances in Geometry

Right nuclear decomposition of generalized André systems

Dean E. Draayer

(Communicated by W. Kantor)

Abstract. The structure of generalized André systems is described in terms of their right nuclei. Necessary and sufficient numerical conditions for the existence of generalized André planes with a homology group of specified index are determined, providing also a numerical characterization of the sharply transitive subsets of $\Gamma L(1, p^t)$. Finally, a multiple net replacement procedure in Dickson nearfield planes is developed, yielding generalized André planes possessing an affine homology group of prescribed index.

1 Introduction

In a translation plane of order q, the order of a homology group is $(q-1)/d$ for some d. We call d the *index* of the homology group. It is well-known that finite translation planes admitting an index 1 homology group are nearfield planes, of which all but seven are also generalized André planes (the so-called Dickson nearfield planes). The structure of Dickson nearfield spreads was determined by Ellers and Karzel [1].

In [3], Hiramine and Johnson undertook a study of generalized André planes that admit an index 2 homology group. They were able to effect a classification (but see below) and describe the corresponding spreads. They also showed that nearly all such planes could be constructed from Dickson nearfield planes via net replacement.

This article was motivated by a desire to generalize the results in the index 1 and 2 cases to arbitrary finite generalized André planes. There is an enormous variety of generalized André planes; the results presented here fall under the theme of classifying these planes with regard to groups of homologies that they support.

In this article, we consider finite generalized André planes that admit an affine homology group of arbitrary index d. We obtain a general decomposition and also a determination of necessary and sufficient numerical conditions for the existence of such a plane (Section 4). The proofs are almost entirely number-theoretic, relying primarily on the factorization of numbers of the form $q^n - 1$ (Theorem 2.4). We remark that these results also give a characterization and structural decomposition of sharply transitive subsets of $\Gamma L(1, p^t)$ via their identification with spread map sets of generalized André systems.

The index 1 and 2 results mentioned above follow directly from the main results presented here. In the index 2 case, our results make it apparent that the classification in [3] overlooked an infinite class of planes (Section 5).

Finally, we present a generalization of the "Type 2" replacements in [3] which applies to a far greater range of indexes. This construction is a "nub preserving" multiple net replacement on a (q, n)-Dickson nearfield plane which yields a generalized André plane admitting a homology group of index d for choices of d dividing n.

2 Number-theoretic preliminaries

All variables are understood to be integer-valued. For integers m and n, we write $m \mid n$ to signify that m divides n. The greatest common divisor of m and n is denoted by (m, n). For a prime u, we define the u-part $\lfloor n \rfloor_u$ of n by: $\lfloor n \rfloor_u = u^e$ where $u^e \mid n$ but $u^{e+1} \nmid n$. We extend this notation to sets of primes U: $\lfloor n \rfloor_U = \prod_{u \in U} \lfloor n \rfloor_u$, and $\lfloor n \rfloor_{U'} = n / \lfloor n \rfloor_U$. For a single prime u, we also write $\lfloor n \rfloor_{u'} = n / \lfloor n \rfloor_u$.

Our arguments depend heavily on divisibility results concerning numbers of the form $q^n - 1$. Among the more elementary of these results is the following. Parts (a) and (b) are well-known, and part (c) follows from (b) and Euler's theorem.

Lemma 2.1. *Let q, m, and n be positive integers with $q > 1$. Then*:

(a) $(q^m - 1) \mid (q^n - 1)$ *if and only if* $m \mid n$.

(b) $(q^m - 1, q^n - 1) = q^{(m,n)} - 1$.

(c) *Let u be a prime. Then $u^d \mid (q^n - 1)$ if and only if $u^d \mid (q^{(n, u^{d-1}(u-1))} - 1)$. In particular, $u \mid (q^n - 1)$ if and only if $u \mid (q^{(n, u-1)} - 1)$.*

For any epimorphism $G \to H$ between finite cyclic groups, the image of each generator of G is also a generator of H. It is also true that every generator of H is the image of some generator of G, the proof of which hinges on the following fact.

Lemma 2.2. *Let m, n, and a be integers such that $m \mid n$ and $(a, m) = 1$. Then there exists an integer k such that $(a + km, n) = 1$.*

Proof. Let U be the set of all prime factors of n that divide a. Let

$$k = (1 + \lfloor n \rfloor_U) \cdot \lfloor n \rfloor_{U'}.$$

Let w be any prime factor of n. If $w \in U$, then $w \mid a$ (so $w \nmid m$) and $w \nmid k$, so $w \nmid (a + km)$. Otherwise $w \notin U$, in which case $w \nmid a$ and $w \mid k$, so that $w \nmid (a + km)$. Thus, no prime factor of n divides $a + km$. □

Lemma 2.3. *Let $q > 1$ and $n > 0$.*

(a) *If $m \mid (q - 1)$, then $(q^n - 1)/(q - 1) \equiv n \bmod m$. In particular, if $n \mid (q - 1)$ then $n \mid (q^n - 1)/(q - 1)$.*

(b) *Let u be a prime factor of $q-1$. Then $\lfloor q^n-1\rfloor_u = \lfloor q^{\lfloor n\rfloor_u}-1\rfloor_u$. In particular, if $u \nmid n$ then $\lfloor q^n-1\rfloor_u = \lfloor q-1\rfloor_u$.*

Proof. In (a), suppose $q \equiv 1 \bmod m$. Then

$$\frac{q^n-1}{q-1} = 1+q+q^2+\cdots+q^{n-1} \equiv 1+1+1+\cdots+1 \equiv n \bmod m.$$

For (b), let $m = \lfloor n\rfloor_{u'}$. By (a), $(q^{\lfloor n\rfloor_u m}-1)/(q^{\lfloor n\rfloor_u}-1) \equiv m \not\equiv 0 \bmod u$. Thus,

$$\lfloor q^n-1\rfloor_u = \left\lfloor \frac{q^n-1}{q^{\lfloor n\rfloor_u}-1}\right\rfloor_u \cdot \lfloor q^{\lfloor n\rfloor_u}-1\rfloor_u = \lfloor q^{\lfloor n\rfloor_u}-1\rfloor_u,$$

as claimed. □

The following factorization theorem is of critical importance to the arguments presented in later sections. A proof appears in [5, Theorem 6.3].

Theorem 2.4. *Let $q>1$ and $n>0$, and let u be any prime factor of $q-1$. Then*:

(a) $\lfloor n\rfloor_u \lfloor q-1\rfloor_u \leqslant \lfloor q^n-1\rfloor_u$.

(b) *If $u \neq 2$, or if $u=2$ but either $q \not\equiv -1 \bmod 4$ or n is odd, then*

$$\lfloor q^n-1\rfloor_u = \lfloor n\rfloor_u \lfloor q-1\rfloor_u.$$

(c) *If $q \equiv -1 \bmod 4$ and n is even, then*

$$\lfloor q^n-1\rfloor_2 = \lfloor n\rfloor_2 \lfloor q+1\rfloor_2.$$

Corollary 2.5. *Let q, n, and i be positive integers with $q>1$ and such that every prime factor of n divides $q-1$.*

(a) *If $n \mid i$, then $n \mid (q^i-1)/(q-1)$.*

(b) *Conversely, suppose $n \mid (q^i-1)/(q-1)$. If $q \not\equiv -1 \bmod 4$ or i is odd, then $n \mid i$. If $q \equiv -1 \bmod 4$ and i is even, then $\lfloor n\rfloor_{2'} \mid i$ and $\lfloor n\rfloor_2 \leqslant \lfloor i\rfloor_2 \lfloor q+1\rfloor_2$.*

Corollary 2.6. *Let $q>1$ and $n>0$, and let $u \neq 2$ be a prime factor of q^n-1. Then*

$$\lfloor q^n-1\rfloor_u > \lfloor n\rfloor_u.$$

Proof. Put $\bar{q} = q^{(n,u-1)}$ and $\bar{n} = n/(n,u-1)$. By Lemma 2.1(c), we have $u \mid (\bar{q}-1)$. Applying Lemma 2.3(b) and Theorem 2.4(b) and the fact that $\lfloor \bar{n}\rfloor_u = \lfloor n\rfloor_u$, we obtain

$$\begin{aligned}\lfloor q^n-1\rfloor_u &= \lfloor \bar{q}^{\bar{n}}-1\rfloor_u = \lfloor \bar{q}^{\lfloor \bar{n}\rfloor_u}-1\rfloor_u \\ &= \lfloor \bar{q}^{\lfloor n\rfloor_u}-1\rfloor_u = \lfloor n\rfloor_u \lfloor \bar{q}-1\rfloor_u,\end{aligned}$$

from which the result follows. □

3 Spread maps and generalized André systems

We assume the reader is familiar with the representation of translation planes via (right) quasifields $X(+,\circ)$ and spread map sets $\Sigma \subseteq \mathrm{GL}(X)$ (e.g., see [5] or [4]). The correspondence between these representations is as follows: For each $a \in X^*$, define $\sigma_a : X \to X$ by $x^{\sigma_a} = x \circ a$. Then $\Sigma(X^*(\circ)) = \{\sigma_a : a \in X^*\} \subseteq \mathrm{GL}(X)$ is a spread map set of X with $1 \in \Sigma(X^*(\circ))$. Conversely, spread map sets Σ of X with $1 \in \Sigma$ determine quasifields $X(+,\circ)$.

Let X be a finite-dimensional vector space. Spread map sets of X coincide with sharply transitive subsets $\Sigma \subseteq \mathrm{GL}(X)$ acting on X^*. More generally, a partial spread map set of X coincides with a subset $\Sigma \subseteq \mathrm{GL}(X)$ acting sharply on X^*. (By acting sharply, we mean that $x^\sigma \neq x^\tau$ for all $x \in X^*$ whenever $\sigma, \tau \in \Sigma$ with $\sigma \neq \tau$.)

For a quasifield $X(+,\circ)$, the right and middle nuclei are defined by $N_r(\circ) = \{a \in X^* : (x \circ y) \circ a = x \circ (y \circ a) \text{ for all } x, y \in X^*\}$ and $N_m(\circ) = \{a \in X^* : (x \circ a) \circ y = x \circ (a \circ y) \text{ for all } x, y \in X^*\}$. These nuclei correspond in the spread map set $\Sigma = \Sigma(X^*(\circ))$ to the right-absorbed and left-absorbed maps $\Sigma_r = \{\rho \in \Sigma : \Sigma\rho \subseteq \Sigma\} = \{\sigma_a : a \in N_r(\circ)\}$ and $\Sigma_l = \{\rho \in \Sigma : \rho\Sigma \subseteq \Sigma\} = \{\sigma_a : a \in N_m(\circ)\}$. In the translation plane $\mathscr{A}(X(+,\circ)) = \mathscr{A}(\Sigma)$, these notions correspond to homology groups $\mathscr{H}_{(0)} = \{(x,y) \mapsto (x, y \circ a) : a \in N_r(\circ)\} = \{1 \oplus \rho : \rho \in \Sigma_r\}$ and $\mathscr{H}_{(\infty)} = \{(x,y) \mapsto (x \circ a, y) : a \in N_m(\circ)\} = \{\rho \oplus 1 : \rho \in \Sigma_l\}$.

Recall that a generalized André system is a (right) quasifield $F(+,\circ)$ for which there exists a skewfield structure $F(+,\cdot)$ on F and a map $\lambda : F^* \to \mathrm{Aut}\,F(+,\cdot)$ such that $x \circ a = x^{\lambda(a)} \cdot a$ for all $x, a \in F^*$. Equivalently, a generalized André system is a quasifield $F(+,\circ)$ such that $\Sigma(F^*(\circ)) \subseteq \Gamma\mathrm{L}(1, F(+,\cdot))$ for some underlying skewfield $F(+,\cdot)$. We call λ the companion automorphism map.

Definition 3.1. Let $F(+,\cdot) = \mathrm{GF}(q^n)$ and let $\lambda : F^* \to \mathrm{Aut}_{\mathrm{GF}(q)}\,F(+,\cdot)$ be any map. Define $\Sigma(\lambda) \subseteq \Gamma\mathrm{L}_q(1, q^n)$ by $\Sigma(\lambda) = \{x \mapsto x^{\lambda(a)} \cdot a : a \in F^*\}$. Let $F(+,\circ)$ be $F(+)$ endowed with the operation $\circ : F \times F \to F$ defined by: $x \circ 0 = 0$ and $x \circ a = x^{\lambda(a)} \cdot a$ for all $x \in F$ and $a \in F^*$. Fix a primitive element ω of $F(+,\cdot)$, and let $h_i \in \mathbb{Z}_n$ (for $i \in \mathbb{Z}_{q^n-1}$) be such that $\lambda(\omega^i) = (x \mapsto x^{q^{h_i}})$.

The following generalization of [2, Lemma 2.1] (or see [5, Lemma 10.1]), which occurs here with $M = 1$, is crucial for the arguments in Section 4.

Theorem 3.2. *In Definition* 3.1, *suppose λ is constant on the cosets of a subgroup $M \leqslant F^*(\cdot)$ of order $(q^n - 1)/m$ (i.e., suppose m is a divisor of $q^n - 1$ such that $h_i \equiv h_j \bmod n$ whenever $i \equiv j \bmod m$). Then $\Sigma(\lambda)$ is sharply transitive on F^* if and only if*:

$$i \not\equiv j \bmod (m, q^{h_i} - q^{h_j}) \quad \textit{whenever } i \not\equiv j \bmod m. \tag{3.1}$$

Proof. Note that $F^* = \bigcup_{i \in \mathbb{Z}_m} \omega^i M$ since $M = \omega^{m\mathbb{Z}}$. Thus, $\Sigma(\lambda) = \bigcup_{i \in \mathbb{Z}_m} \Sigma_i$ where $\Sigma_i = \Sigma(\omega^i M)$. Since λ is constant on the cosets of M, this represents $\Sigma(\lambda)$ as a union of certain cosets Σ_i of some subgroup Σ_0 of $\Gamma\mathrm{L}_q(1, q^n)$. Clearly each Σ_i acts sharply on F^*, so $\Sigma(\lambda)$ will be sharply transitive on F^* if and only if $\Sigma_i \cup \Sigma_j$ acts sharply on F^* for all $i, j \in \mathbb{Z}_m$. Take $\Sigma_i \neq \Sigma_j$, i.e., $i \not\equiv j \bmod m$. Then:

$$\begin{aligned}
&\Sigma_i \cup \Sigma_j \text{ acts sharply on } F^* \\
&\quad \Leftrightarrow \forall a, k, l\colon (\omega^a)^{\lambda(\omega^{i+km})} \cdot \omega^{i+km} \neq (\omega^a)^{\lambda(\omega^{j+lm})} \cdot \omega^{j+lm} \\
&\quad \Leftrightarrow \forall a, k, l\colon \omega^{aq^{h_i}} \cdot \omega^{i+km} \neq \omega^{aq^{h_j}} \cdot \omega^{j+lm} \\
&\quad \Leftrightarrow \forall a\colon a(q^{h_i} - q^{h_j}) + (i - j) \notin m\mathbb{Z} \\
&\quad \Leftrightarrow i - j \notin m\mathbb{Z} + (q^{h_i} - q^{h_j})\mathbb{Z} \\
&\quad \Leftrightarrow i \not\equiv j \bmod (m, q^{h_i} - q^{h_j}).
\end{aligned}$$

The result now follows. □

As a corollary, $F(+, \circ)$ as in Definition 3.1 is a generalized André system if and only if $\lambda(1) = 1$ and (3.1) holds. Every sharply transitive subset $\Sigma \subseteq \Gamma\mathrm{L}_q(1, q^n)$ and every generalized André system of order q^n can be represented in the form indicated in Definition 3.1.

Let us define the *nub* Z of a generalized André system $F(+, \circ)$ by $Z = \{a \in N_m \cap N_r : \lambda(a) = 1\} = \{a \in F^* : \lambda(a \circ x) = \lambda(x) = \lambda(x \circ a) \text{ for all } x \in F^*\}$. Thus, Z is the intersection of the kernels of the homomorphisms $\lambda|_{N_r(\circ)}$ and $\lambda|_{N_m(\circ)}$ (these kernels coincide when F is finite). Note that $\lambda(Z) = 1$ and $Z(\circ) = Z(\cdot) \leqslant F^*(\cdot)$. The nub is the largest subgroup Z of $F^*(\cdot)$ such that λ is constant on the cosets of Z.

Suppose $F(+, \circ)$ in Definition 3.1 is in fact a generalized André system. Define $v = \operatorname{lcm}\{q^d - 1 : d \mid n \text{ and } d < n\}$, with $v = 1$ if $n = 1$. It can be shown that v is a proper divisor of $q^n - 1$ (except in the trivial case $q^n = 2$). Taking $M = 1$ (i.e., $m = q^n - 1$) in Theorem 3.2, it is easy to show that $i \equiv j \bmod v$ implies $i \equiv j \bmod q^n - 1$. Thus, λ is constant on the cosets of $Z_0 = \omega^{v\mathbb{Z}} \leqslant F^*(\cdot)$, so Z_0 is a subgroup of the nub Z. This yields a lower bound $(q^n - 1)/v$ for the order of Z and in particular shows that the nub is never trivial (unless $q^n = 2$). The corresponding plane $\mathscr{A}(F(+, \circ))$ has a collineation group $\{(x, y) \mapsto (x \circ a, y \circ b) : a, b \in Z\}$ induced by Z as a subgroup of both the right and middle nuclei.

4 Right nuclear decomposition of a generalized André system

In this section, we describe the structure of a generalized André system by decomposing it in terms of a subgroup of the right nucleus (Theorem 4.1). We then determine necessary and sufficient numerical conditions for a generalized André system to have a right nuclear subgroup of a prescribed index (Theorem 4.2 and Theorem 4.3). In a broad special case (Proposition 4.4 and Proposition 4.5), we determine suitable values for the parameters appearing in the decomposition.

When discussing a generalized André system $F(+, \circ)$, care must be taken to distinguish between the operation $\circ$ and the multiplication $\cdot$ of the underlying field. The notation $a^i = a \cdot a \dots a$ (i factors) will be used to indicate a power in $F(+, \cdot)$, whereas we write $a^{\circ i}$ to denote a power in $F^*(\circ)$ with left-to-right association (i.e., $a^{\circ 0} = 1$ and $a^{\circ i} = a^{\circ(i-1)} \circ a$ for $i > 0$); the rule of association is critical since $\circ$ is generally not associative.

Theorem 4.1. *Let $F(+, \circ)$ be a generalized André system of order p^t (p prime and $t \geqslant 1$) with underlying field $F(+, \cdot) = \mathrm{GF}(p^t)$ and companion automorphism map $\lambda : F^* \to \operatorname{Aut} F(+, \cdot)$. Let $H(\circ)$ be any subgroup of the right nucleus, and put $|H| = (p^t - 1)/d$. Let $\Lambda = \lambda(H)$, $n = |\Lambda|$, $Z(\circ) = \ker(\lambda|_{H(\circ)})$, let q be the order of the fixed field of Λ, and let ω be a primitive element of $F(+, \cdot)$. Then:*

(a) *$q^n = p^t$ and $nd \mid (q^n - 1)$.*

(b) *$Z(\circ) = Z(\cdot) = \omega^{nd\mathbb{Z}}$ is cyclic of order $(q^n - 1)/nd$, and $H(\circ)/Z$ is cyclic of order n.*

(c) *Let $\omega^s \in H$ such that $\lambda(\omega^s) = (x \mapsto x^q)$, and let $s_i = s(q^i - 1)/(q - 1)$ for $i \geqslant 0$. Then $\omega^s \cdot Z$ generates $H(\circ)/Z$, $(\omega^s \cdot Z)^{\circ i} = \omega^{s_i} \cdot Z = \omega^{s_i + nd\mathbb{Z}}$, and*

$$H(\circ) = \bigcup_{0 \leqslant i < n} (\omega^s \cdot Z)^{\circ i} = \bigcup_{0 \leqslant i < n} \omega^{s_i} \cdot Z.$$

Furthermore, $\lambda(\omega^{s_i} \cdot Z) = \{x \mapsto x^{q^i}\}$, so

$$\forall x \in F^* \ \forall a \in H \colon x \circ a = x^{q^i} \cdot a \quad \text{where } a \in \omega^{s_i} \cdot Z.$$

(d) *F^* admits a partition*

$$F^*(\circ) = \bigcup_{0 \leqslant k < d} \omega^{r_k} \circ H(\circ) = \bigcup_{0 \leqslant k < d} \ \bigcup_{0 \leqslant i < n} \omega^{r_k q^i + s_i + nd\mathbb{Z}}$$

where $R = \{r_k : 0 \leqslant k < d\}$ is any set with $r_0 \equiv 0 \bmod nd$ and such that $\{r_k q^i + s_i : 0 \leqslant k < d \text{ and } 0 \leqslant i < n\}$ constitutes a transversal of $\mathbb{Z}_{nd}$. Furthermore, there exists a set $T = \{t_k : 0 \leqslant k < d\}$, with $t_0 \equiv 0 \bmod t$, such that $\lambda(\omega^{r_k q^i + s_i + nd\mathbb{Z}}) = \{x \mapsto x^{p^{t_k} q^i}\}$. Thus,

$$\forall x, a \in F^* \colon x \circ a = x^{p^{t_k} q^i} \cdot a \quad \text{where } a \in \omega^{r_k q^i + s_i} \cdot Z.$$

Proof. First, $\dim_{\mathrm{GF}(q)} F = |\Lambda| = n$, so $q^n = p^t$. The map $\lambda|_H : H(\circ) \to \Lambda$ is a group homomorphism with kernel $Z(\circ)$ and image Λ, so $H(\circ)/Z \cong \Lambda \leqslant \operatorname{Aut} F(+, \cdot)$ is cyclic of order n and $|Z| = |H|/|\Lambda| = (q^n - 1)/nd$. Clearly $x \circ a = x \cdot a$ for all $x \in F$ and $a \in Z$, so $Z(\circ) = Z(\cdot) \leqslant F^*(\cdot)$. Thus, Z is cyclic and $Z = \omega^{nd\mathbb{Z}}$. This proves (a) and (b).

Now $H(\circ)/Z$ is generated by $\omega^s \cdot Z$ for any $\omega^s \in H(\circ)$ such that $\lambda(\omega^s) = (x \mapsto x^q)$. Thus, $H(\circ) = \bigcup_{0 \leqslant i < n} (\omega^s \cdot Z)^{\circ i}$ and $\lambda((\omega^s \cdot Z)^{\circ i}) = \{x \mapsto x^{q^i}\}$.

Claim: $a^{\circ i} = a^{(q^i - 1)/(q - 1)}$ for all $a \in \omega^s \cdot Z$ and $i \geqslant 0$. This is clear for $i = 0$. Proceeding by induction and using the fact that $\lambda(a) = (x \mapsto x^q)$, we obtain

$$a^{\circ(i+1)} = a^{\circ i} \circ a = (a^{(q^i - 1)/(q - 1)})^q \cdot a = a^{1 + q + \cdots + q^i} = a^{(q^{i+1} - 1)/(q - 1)}.$$

It follows that $(\omega^s \cdot Z)^{\circ i} = (\omega^{s+nd\mathbb{Z}})^{\circ i} = \omega^{s_i+nd\mathbb{Z}} = \omega^{s_i} \cdot Z$, so (c) holds. For (d), we have $F^* = \bigcup_{a \in F^*} a \circ H(\circ)$ since $1 \in H(\circ)$. Further, since $H(\circ) \leqslant N_r(\circ)$, $b \in a \circ H(\circ)$ if and only if $b \circ H(\circ) = a \circ H(\circ)$. Thus, $\{a \circ H(\circ) : a \in F^*\}$ constitutes a partition of F^*. Let $\{\omega^{r_k} : 0 \leqslant k < d\}$ be a transversal of this partition. Then

$$\begin{aligned} F^*(\circ) &= \bigcup_{0 \leqslant k < d} \omega^{r_k} \circ H(\circ) = \bigcup_{0 \leqslant k < d} \bigcup_{0 \leqslant i < n} \omega^{r_k} \circ (\omega^s \cdot Z)^{\circ i} \\ &= \bigcup_{0 \leqslant k < d} \bigcup_{0 \leqslant i < n} (\omega^{r_k} \circ \omega^{s_i}) \cdot Z = \bigcup_{0 \leqslant k < d} \bigcup_{0 \leqslant i < n} \omega^{r_k q^i} \cdot \omega^{s_i} \cdot Z. \end{aligned}$$

The rest of (d) follows directly. □

We now investigate necessary numerical constraints on the quantities involved in the structural decomposition given by Theorem 4.1. A pair of positive integers (q, n) is called a Dickson pair if: (i) q is a power of a prime; (ii) every prime factor of n also divides $q - 1$; and (iii) if $q \equiv -1 \bmod 4$, then $4 \nmid n$.

Theorem 4.2. *In the context of Theorem* 4.1:

(a) *Let u be a prime factor of $q - 1$. If $u \neq 2$, or if $u = 2$ but $q \not\equiv -1 \bmod 4$ or n is odd, then $\lfloor d \rfloor_u \leqslant \lfloor (s, q-1) \rfloor_u$.*

(b) *Let u be a prime factor of n. Then $u \mid (q-1)$. Furthermore*:

  (i) *If $u \neq 2$, or if $u = 2$ but $q \not\equiv -1 \bmod 4$, then $\lfloor s \rfloor_u = \lfloor d \rfloor_u < \lfloor q - 1 \rfloor_u$.*

  (ii) *If $u = 2$ and $q \equiv -1 \bmod 4$, then s is odd and $2\lfloor d \rfloor_2 \leqslant \lfloor q + 1 \rfloor_2$. Furthermore, if $4 \mid n$, then $2\lfloor d \rfloor_2 = \lfloor q + 1 \rfloor_2$.*

(c) *Either (q, n) is a Dickson pair or else $q \equiv -1 \bmod 4$ and $n \equiv 0 \bmod 4$, in which case s is odd and $2\lfloor d \rfloor_2 = \lfloor q + 1 \rfloor_2$.*

(d) *Let $\tilde{s} = (s, d)$. There exists a primitive element $\tilde{\omega}$ of $F(+, \cdot)$ such that $\lambda(\tilde{\omega}^{\tilde{s}}) = (x \mapsto x^q)$. (Thus, it is possible to select the primitive element ω in Theorem* 4.1 *so that $s \mid d$.)*

(e) *For $i \geqslant 0$: $nd \mid s_i \Leftrightarrow n \mid i \Leftrightarrow (nd, q^i - 1) \mid s_i$.*

(f) *For $0 \leqslant i < n$ and $0 \leqslant k, l < d$,*

$$(nd, p^{t_k} q^i - p^{t_l}) \nmid ((r_k - r_l) + r_k(q^i - 1) + s_i) \tag{4.1}$$

unless $k = l$ and $i = 0$. In particular, $\{r_k q^i + s_i : 0 \leqslant k < d \text{ and } 0 \leqslant i < n\}$ constitutes a transversal of $\mathbb{Z}_{nd}$.

Proof. Since $\omega^s \cdot Z$ has $\circ$-order n, we have $(\omega^s \cdot Z)^{\circ i} = Z$ if and only if $n \mid i$, i.e.,

$$nd \mid s_i \quad \text{if and only if} \quad n \mid i. \tag{4.2}$$

Now λ is constant on the cosets of Z. Further, by (4.2), $s_i \not\equiv 0 \bmod nd$ when $n \nmid i$, and $\lambda((\omega^s \cdot Z)^{\circ i}) = (x \mapsto x^{q^i})$, so by (3.1), $s_i \not\equiv 0 \bmod (nd, q^i - 1)$ unless $n \mid i$. That is,

$$(nd, q^i - 1) \mid s_i \quad \text{if and only if} \quad n \mid i. \tag{4.3}$$

Thus, (e) holds. From (4.2) and Theorem 4.1(a), we also get

$$nd \mid (q^n - 1, s_n) = (s, q-1) \cdot \frac{q^n - 1}{q - 1}. \tag{4.4}$$

Claim 1: If $q \equiv -1 \bmod 4$ and n is even, then $2\lfloor d \rfloor_2 \leqslant (s,2) \cdot \lfloor q+1 \rfloor_2$. This follows from (4.4) and Theorem 2.4(c): $\lfloor nd \rfloor_2 \leqslant \lfloor (s, q-1) \rfloor_2 \cdot \lfloor q^n - 1 \rfloor_2 / \lfloor q - 1 \rfloor_2 = (s,2) \cdot \lfloor n \rfloor_2 \lfloor q+1 \rfloor_2 / 2$.

Claim 2: Let u be a prime factor of $q-1$. If $u \neq 2$, or if $u = 2$ but $q \not\equiv -1 \bmod 4$ or n is odd, then $\lfloor d \rfloor_u \leqslant \lfloor (s, q-1) \rfloor_u$. To see this, (4.4) and Theorem 2.4(b) yield $\lfloor nd \rfloor_u \leqslant \lfloor (s, q-1) \rfloor_u \cdot \lfloor q^n - 1 \rfloor_u / \lfloor q - 1 \rfloor_u = \lfloor (s, q-1) \rfloor_u \lfloor n \rfloor_u$, and the claim follows.

Claim 3: For each prime factor u of n, $\lfloor (nd, q^{n/u} - 1) \rfloor_u > \lfloor s_{n/u} \rfloor_u$. For this, by (4.3) there exists some prime v such that $\lfloor (nd, q^{n/u} - 1) \rfloor_v > \lfloor s_{n/u} \rfloor_v$. Suppose $v \neq u$. Note that $v \mid (q^{n/u} - 1)$, so Lemma 2.3(b) yields $\lfloor q^n - 1 \rfloor_v = \lfloor (q^{n/u})^u - 1 \rfloor_v = \lfloor (q^{n/u})^{\lfloor u \rfloor_v} - 1 \rfloor_v = \lfloor q^{n/u} - 1 \rfloor_v$, and thus $\lfloor s_n \rfloor_v = \lfloor s_{n/u} \rfloor_v$. But then we obtain $\lfloor (nd, q^{n/u} - 1) \rfloor_v > \lfloor s_n \rfloor_v$, contrary to (4.3). Thus, $v = u$ here, and the claim holds.

Claim 4: For each prime factor u of n, we have $u \mid (q-1)$ and $\lfloor s \rfloor_u < \lfloor q - 1 \rfloor_u$. This follows from Claim 3: $\lfloor q^{n/u} - 1 \rfloor_u > \lfloor s \rfloor_u \lfloor q^{n/u} - 1 \rfloor_u / \lfloor q - 1 \rfloor_u$, so $\lfloor q - 1 \rfloor_u > \lfloor s \rfloor_u$.

Claim 5: If $q \equiv -1 \bmod 4$ and n is even, then s is odd and $2\lfloor d \rfloor_2 \leqslant \lfloor q+1 \rfloor_2$; further, if $4 \mid n$, then $2\lfloor d \rfloor_2 = \lfloor q+1 \rfloor_2$. To see this, observe that Claim 4 yields $\lfloor s \rfloor_2 < \lfloor q-1 \rfloor_2 = 2$, so s is odd. Claim 1 then gives $2\lfloor d \rfloor_2 \leqslant \lfloor q+1 \rfloor_2$. Now suppose that $4 \mid n$. Then $n/2$ is even, so from Claim 3 and Theorem 2.4(c) we obtain $\lfloor nd \rfloor_2 > \lfloor s \rfloor_2 \lfloor q^{n/2} - 1 \rfloor_2 / \lfloor q - 1 \rfloor_2 = \lfloor n/2 \rfloor_2 \lfloor q+1 \rfloor_2 / 2$, so $4\lfloor d \rfloor_2 > \lfloor q+1 \rfloor_2$. Thus, $2\lfloor d \rfloor_2 \geqslant \lfloor q+1 \rfloor_2$ as well.

Claim 6: Let u be any prime factor of n. If $u \neq 2$, or if $u = 2$ but $q \not\equiv -1 \bmod 4$, then $\lfloor d \rfloor_u = \lfloor s \rfloor_u$. For this, first note that $u \mid (q-1)$ by Claim 4. So by Claim 2, we have $\lfloor d \rfloor_u \leqslant \lfloor s \rfloor_u$. From Claim 3 and Theorem 2.4(b), we obtain $\lfloor nd \rfloor_u > \lfloor s \rfloor_u \lfloor q^{n/u} - 1 \rfloor_u / \lfloor q - 1 \rfloor_u = \lfloor s \rfloor_u \lfloor n/u \rfloor_u$, so $\lfloor d \rfloor_u \geqslant \lfloor s \rfloor_u$ as well.

Note that Claim 2 proves (a), Claims 4–6 prove (b), and (c) follows immediately from (b). To prove (d), put $s = \tilde{s}s'$ and $d = \tilde{s}d'$. For each prime factor u of n, we have $\lfloor s \rfloor_u \leqslant \lfloor d \rfloor_u$ by Claims 5 and 6, so $u \nmid s'$. Therefore, $(s', nd') = 1$. By Lemma 2.2, there exists some k such that $(s' + knd', q^n - 1) = 1$. Then $\tilde{\omega} = \omega^{s' + knd'}$ is a primitive element such that $\tilde{\omega}^{\tilde{s}} = \omega^{s + ndk} \in \omega^s \cdot Z$, so $\lambda(\tilde{\omega}^{\tilde{s}}) = \lambda(\omega^s) = (x \mapsto x^q)$.

It remains to prove (f). Now λ is constant on the cosets of Z, so Theorem 3.2 yields the sequence of implications (taking $i \geqslant j$ without loss of generality):

$$\begin{aligned} & r_k q^i + s_i \not\equiv r_l q^j + s_j \bmod nd \\ & \quad \Rightarrow r_k q^i + s_i \not\equiv r_l q^j + s_j \bmod (nd, p^{t_k} q^i - p^{t_l} q^j) \\ & \quad \Rightarrow (nd, p^{t_k} q^{i-j} - p^{t_l}) \nmid (r_k q^{i-j} - r_l + s_{i-j}), \end{aligned}$$

which is equivalent to (4.1). The final statement in (f) (which is just a restatement of Theorem 4.1(d)) follows by taking $l = 0$ in (4.1). □

We now consider the converse of Theorem 4.1 and Theorem 4.2. The following theorem shows that the necessary conditions in Theorem 4.2 are also sufficient for the construction of a generalized André system of the form appearing in Theorem 4.1.

Theorem 4.3. *Let p be prime and $t \geqslant 1$. Let q, n, d, and s be positive integers such that $q^n = p^t$, every prime factor of n divides $q-1$, and $nd \mid (q^n - 1)$. Suppose further that for every prime factor u of $q-1$:*

(i) *If $u \nmid n$, then $\lfloor s \rfloor_u \geqslant \lfloor d \rfloor_u$;*

(ii) *If $u \mid n$ and either $u \neq 2$ or $q \not\equiv -1 \bmod 4$, then $\lfloor s \rfloor_u = \lfloor d \rfloor_u < \lfloor q-1 \rfloor_u$;*

(iii) *If n is even and $q \equiv -1 \bmod 4$, then s is odd and $2\lfloor d \rfloor_2 \leqslant \lfloor q+1 \rfloor_2$, with equality if $4 \mid n$.*

(a) *Let $S = \{s_i : i \geqslant 0\}$ where $s_i = s(q^i - 1)/(q-1)$. Define $\oplus : S \times S \to S$ by $s_i \oplus s_j = s_{i+j} = s_i q^j + s_j$. The operation $\oplus$ induces (via the canonical epimorphism $\hat{}\, : \mathbb{Z} \to \mathbb{Z}_{nd}$) an operation on $\hat{S} \subseteq \mathbb{Z}_{nd}$ that makes $\hat{S}(\oplus)$ into a cyclic group of order n. Furthermore, $nd \mid s_i \Leftrightarrow n \mid i \Leftrightarrow (nd, q^i - 1) \mid s_i$.*

(b) *Extend the definition of $\oplus : \mathbb{Z} \times S \to \mathbb{Z}$ by $a \oplus s_i = aq^i + s_i$. Then $\{\hat{a} \oplus \hat{S} : a \in \mathbb{Z}\}$ is a partition of $\mathbb{Z}_{nd}$.*

(c) *Let $R = \{r_k : 0 \leqslant k < d\}$, with $r_k \geqslant 0$ and $r_0 \equiv 0 \bmod nd$, be any set such that $\hat{R}$ is a transversal of the partition in (b) (equivalently, such that $\{r_k \oplus s_i : 0 \leqslant k < d$ and $0 \leqslant i < n\}$ constitutes a transversal of $\mathbb{Z}_{nd}$). Suppose $T = \{t_k : 0 \leqslant k < d\}$, with $t_k \geqslant 0$ and $t_0 \equiv 0 \bmod t$, is such that for all $0 \leqslant i < n$ and $0 \leqslant l < k < d$,*

$$(nd, p^{t_k} q^i - p^{t_l}) \nmid ((r_k - r_l) + r_k(q^i - 1) + s_i). \tag{4.5}$$

Let $F = \mathrm{GF}(q^n)$ with primitive element ω, and define $\lambda : F^* \to \operatorname{Aut} F$ by $\lambda(\omega^{r_k \oplus s_i + nd\mathbb{Z}}) = \{x \mapsto x^{p^{t_k} q^i}\}$. Then Definition 3.1 yields a generalized André system $F(+, \circ)$ having a right nuclear subgroup $H(\circ) = \bigcup_{0 \leqslant i < n} \omega^{s_i + nd\mathbb{Z}}$ of order $(q^n - 1)/d$. The system $F(+, \circ)$ thus obtained is independent of the choice of R.

Proof. First, it follows readily from Lemma 2.1(a) that $s_i \mid s_j$ whenever $i \mid j$.

Claim: If $i \equiv j \bmod n$, then $s_i \equiv s_j \bmod nd$. For this, assume that $i \equiv j \bmod n$ with $i \geqslant j$. Observe that $s_i - s_j = sq^j(q^{i-j} - 1)/(q-1) = s_{i-j} q^j$ and that $s_n \mid s_{i-j}$. Thus, it suffices to show that $nd \mid s_n$, or equivalently, that $\lfloor nd \rfloor_u \leqslant \lfloor s_n \rfloor_u$ for every prime factor u of nd. First assume that $u \nmid (q-1)$. Then since $nd \mid (q^n - 1)$, we have $\lfloor nd \rfloor_u \leqslant \lfloor q^n - 1 \rfloor_u \leqslant \lfloor s(q^n - 1)/(q-1) \rfloor_u = \lfloor s_n \rfloor_u$. Assume then that $u \mid (q-1)$. Suppose first that $u \neq 2$ or $q \not\equiv -1 \bmod 4$ or n is odd. Then $\lfloor s \rfloor_u \geqslant \lfloor d \rfloor_u$ by hypothesis, and Theorem 2.4(b) gives $\lfloor s_n \rfloor_u = \lfloor s \rfloor_u \lfloor n \rfloor_u$, so $\lfloor s_n \rfloor_u \geqslant \lfloor nd \rfloor_u$. Suppose finally that $u = 2$, $q \equiv -1 \bmod 4$, and n is even. Then by the hypothesis $2\lfloor d \rfloor_2 \leqslant \lfloor q+1 \rfloor_2$, we obtain from Theorem 2.4(c) that $\lfloor s_n \rfloor_2 = \lfloor s \rfloor_2 \lfloor n \rfloor_2 \lfloor q+1 \rfloor_2 / 2 \geqslant \lfloor n \rfloor_2 \lfloor d \rfloor_2$. We've shown that $\lfloor nd \rfloor_u \leqslant \lfloor s_n \rfloor_u$ in all cases, so the claim is justified.

The claim ensures that the map $\mathbb{Z}_n \to \hat{S} \subseteq \mathbb{Z}_{nd}$ defined by $i \mapsto \hat{s}_i$ is well-defined.

This map is easily seen to be a group epimorphism $\mathbb{Z}_n(+) \to \hat{S}(\oplus)$. We claim that it is in fact an isomorphism, i.e., that $\hat{S}(\oplus)$ has order n. To prove this, it suffices to show that $\lfloor nd \rfloor_u \nmid s_{n/u}$ for every prime factor u of n. Note that $u \mid (q-1)$ by hypothesis. If $u \neq 2$ or $q \not\equiv -1 \bmod 4$, then $\lfloor s \rfloor_u = \lfloor d \rfloor_u$ by hypothesis, so Theorem 2.4(b) gives $\lfloor s_{n/u} \rfloor_u = \lfloor s \rfloor_u \lfloor n/u \rfloor_u = \lfloor nd \rfloor_u / u$, so that $\lfloor nd \rfloor_u \nmid s_{n/u}$. Suppose then that $u = 2$ and $q \equiv -1 \bmod 4$. Then s is odd by hypothesis. If $n \equiv 2 \bmod 4$, then $n/2$ is odd, so by Theorem 2.4(b), $\lfloor s_{n/2} \rfloor_2 = \lfloor s \rfloor_2 \lfloor q^{n/2} - 1 \rfloor_2 / \lfloor q-1 \rfloor_2 = \lfloor n/2 \rfloor_2 = 1$; and if $n \equiv 0 \bmod 4$, then by Theorem 2.4(c) and the hypothesis that $2\lfloor d \rfloor_2 = \lfloor q+1 \rfloor_2$, $\lfloor s_{n/2} \rfloor_2 = \lfloor s \rfloor_2 \lfloor q^{n/2} - 1 \rfloor_2 / \lfloor q-1 \rfloor_2 = \lfloor n/2 \rfloor_2 \lfloor q+1 \rfloor_2 / 2 < \lfloor n \rfloor_2 \lfloor q+1 \rfloor_2 / 2 = \lfloor nd \rfloor_2$. In either case, we obtain $\lfloor nd \rfloor_2 \nmid s_{n/2}$. The claim has been verified.

It follows from the fact that $\hat{S}(\oplus)$ is cyclic of order n that $nd \mid s_i \Leftrightarrow n \mid i$. We now show that $(nd, q^i - 1) \mid s_i \Leftrightarrow n \mid i$. First, if $n \mid i$, then $nd \mid s_i$, so $(nd, q^i - 1) \mid s_i$. Suppose then that $n \nmid i$, and let u be a prime such that $\lfloor n \rfloor_u > \lfloor i \rfloor_u$. It suffices to show that $\lfloor s_i \rfloor_u < \lfloor nd \rfloor_u$ and $\lfloor s_i \rfloor_u < \lfloor q^i - 1 \rfloor_u$. The hypotheses ensure that $u \mid (q-1)$, $\lfloor s \rfloor_u \leqslant \lfloor d \rfloor_u$, and $\lfloor s \rfloor_u < \lfloor q-1 \rfloor_u$. The latter yields $\lfloor s_i \rfloor_u = \lfloor s \rfloor_u \lfloor q^i - 1 \rfloor_u / \lfloor q-1 \rfloor_u < \lfloor q^i - 1 \rfloor_u$. To get $\lfloor s_i \rfloor_u < \lfloor nd \rfloor_u$, if $u \neq 2$ or $q \not\equiv -1 \bmod 4$ or i is odd, Theorem 2.4(b) yields $\lfloor s_i \rfloor_u = \lfloor s \rfloor_u \lfloor i \rfloor_u < \lfloor d \rfloor_u \lfloor n \rfloor_u$. Otherwise, we have $u = 2$, $q \equiv -1 \bmod 4$, and i even, so s is odd, $4 \mid n$, and $2\lfloor d \rfloor_2 = \lfloor q+1 \rfloor_2$. By Theorem 2.4(c), $\lfloor s_i \rfloor_2 = \lfloor s \rfloor_2 \lfloor i \rfloor_2 \cdot \lfloor q+1 \rfloor_2 / 2 < \lfloor n \rfloor_2 \lfloor d \rfloor_2$. In any case, we obtain $\lfloor s_i \rfloor_u \leqslant \lfloor nd \rfloor_u$. This completes the proof of (a).

Now, it is readily seen that $(\hat{a} \oplus \hat{s}_i) \oplus \hat{s}_j = \hat{a} \oplus (\hat{s}_i \oplus \hat{s}_j)$ for all $\hat{a} \in \mathbb{Z}_{nd}$ and $\hat{s}_i, \hat{s}_j \in \hat{S}$. It follows immediately that if $\hat{a} \in \hat{b} \oplus \hat{S}$ then $\hat{a} \oplus \hat{S} = \hat{b} \oplus \hat{S}$. This shows that $\{\hat{a} \oplus \hat{S} : a \in \mathbb{Z}\}$ constitutes a partition of $\mathbb{Z}_{nd}$, which proves (b).

To prove (c), first note that (b) ensures that λ is well-defined. We use Theorem 3.2 to show that $F(+, \circ)$ is a generalized André system. By (b), every integer can be expressed in the form $r_k \oplus s_i + ndj$ for some $0 \leqslant k < d$, $0 \leqslant i < n$, and $j \in \mathbb{Z}$. Condition (3.1) becomes: for all $0 \leqslant k, l < d$ and $0 \leqslant i, j < n$,

$$(nd, p^{t_k} q^i - p^{t_l} q^j) \nmid (r_k \oplus s_i - r_l \oplus s_j) \quad \text{if } k \neq l \text{ or } i \neq j.$$

Since we may arrange it so that $i \geqslant j$, this is equivalent to: for all $0 \leqslant k, l < d$ and $0 \leqslant i < n$,

$$(nd, p^{t_k} q^i - p^{t_l}) \nmid (r_k q^i - r_l + s_i) \quad \text{if } k \neq l \text{ or } i \neq 0. \tag{4.6}$$

When $l < k$, this is merely the hypothesis (4.5) placed on T, so it remains only to prove that (4.6) holds for $l \geqslant k$.

First suppose $l = k$. Then (4.6) becomes $(nd, q^i - 1) \nmid (r_k(q^i - 1) + s_i)$ if $i \neq 0$, that is, $(nd, q^i - 1) \nmid s_i$ if $i \neq 0$, which by (a) is indeed the case. Suppose then that $l > k$. Multiplying by q^{n-i}, we obtain the following sequence of statements equivalent to (4.6):

$$(nd, p^{t_k} - p^{t_l} q^{n-i}) \nmid (r_k q^n - r_l q^{n-i} + s_i q^{n-i}) \quad \text{if } k \neq l \text{ or } i \neq 0.$$

$$(nd, p^{t_l} q^{n-i} - p^{t_k}) \nmid ((r_l q^{n-i} - r_k) - r_k(q^n - 1) - (s_n - s_{n-i})) \quad \text{if } k \neq l \text{ or } i \neq 0$$

$$(nd, p^{t_l} q^{n-i} - p^{t_k}) \nmid ((r_l q^{n-i} - r_k) + s_{n-i}) \quad \text{if } k \neq l \text{ or } i \neq 0$$

The latter is essentially (4.5) with k and l reversed, so it holds by hypothesis. □

In Theorem 4.3, note for later reference that $\{r_k \oplus s_i : 0 \leqslant k < d \text{ and } 0 \leqslant i < n\}$ constitutes a transversal of $\mathbb{Z}_{nd}$ if and only if: for $0 \leqslant l \leqslant k < d$ and $0 \leqslant i < n$, the condition

$$nd \mid ((r_k - r_l) + r_k(q^i - 1) + s_i) \tag{4.7}$$

implies that $k = l$ and $i = 0$.

For the remainder of this section, we consider the case where every prime factor of d divides $q - 1$. By Theorem 4.2(a) and Theorem 4.3, this is equivalent to assuming that $d \mid (q - 1)$. By Theorem 4.2(d), it is then possible to arrange it so that

$$s = \begin{cases} d & \text{if } q \not\equiv -1 \bmod 4 \text{ or } n \text{ is odd} \\ \lfloor d \rfloor_{2'} & \text{if } q \equiv -1 \bmod 4 \text{ and } n \text{ is even.} \end{cases} \tag{4.8}$$

In Proposition 4.4, we determine suitable choices for the r_k's when $d \mid (q - 1)$. (Here we do not assume that s satisfies (4.8).) Parts (a) and (b) cover all cases, but the alternate choices in (c) and (d) are more convenient in certain circumstances (e.g., see Theorem 5.2).

Proposition 4.4. *In the context of Theorem* 4.2 *and Theorem* 4.3, *suppose* $d \mid (q - 1)$. *Without loss of generality, one may choose* r_k (*for* $0 \leqslant k < d$) *as follows*:

(a) *If* $q \not\equiv -1 \bmod 4$ *or if n or d is odd, let* $r_k = k$.

(b) *If* $q \equiv -1 \bmod 4$ *and n and d are even, let* $r_k = 2k$.

(c) *If* (q, n) *is a Dickson pair or d is odd, and if* $(n, s) = 1$, *let* $r_k = nk$.

(d) *If* (q, n) *is not a Dickson pair, d is even, and* $(n, s) = 1$, *let* $r_k = 2k\lfloor n \rfloor_{2'}$.

Proof. Our proof is phrased so that it holds whether one starts with the hypotheses of Theorem 4.2 or of Theorem 4.3. It must be shown that the indicated choices for r_k make $\{r_k q^i + s_i : 0 \leqslant k < d \text{ and } 0 \leqslant i < n\}$ a transversal of $\mathbb{Z}_{nd}$. We do so by assuming that (4.7) holds and show that it follows that $k = l$ and $i = 0$. Note that $\lfloor d \rfloor_{2'} \mid s$ in all cases since $d \mid (q - 1)$. In fact, we have $d \mid s$ except in the case when $q \equiv -1 \bmod 4$ and n and d are even.

In (a), we have $d \mid s$. So (4.7) implies that $d \mid (r_k - r_l) = (k - l)$. Thus, $k = l$, and it then follows from (4.7) that $(nd, q^i - 1) \mid s_i$, which requires $i = 0$.

In (b), s_i is odd if i is odd, and for i even we have $\lfloor s_i \rfloor_2 = \lfloor i \rfloor_2 \lfloor q + 1 \rfloor_2 / 2 \geqslant \lfloor i \rfloor_2 \lfloor d \rfloor_2$. In particular, (4.7) forces i to be even, so $d \mid s_i$, and thus $d \mid 2(k - l)$. But (4.7) then yields $2\lfloor d \rfloor_2 \mid (2(k - l) + 2k(q^i - 1) + s_i)$. So $\lfloor d \rfloor_2 \mid (k - l)$. Therefore, $d \mid (k - l)$, and it follows as in the proof of (a) that $i = 0$.

In (c), (4.7) reduces to $nd \mid (n(k - l) + s_i)$. This implies that $n \mid s_i$, and therefore $n \mid (q^i - 1)/(q - 1)$ (since $(n, s) = 1$), yielding $\lfloor n \rfloor_{2'} \mid i$ (by Corollary 2.5(b)). Now, if $d \mid s$, this yields $nd \mid s_i$ and $d \mid (k - l)$, so $i = 0$ and $k = l$. If $d \nmid s$, then $q \equiv -1 \bmod 4$ and $n \equiv 2 \bmod 4$ (since (q, n) is a Dickson pair). But i must be even since $n \mid s_i$. Thus, $n \mid i$, yielding $i = 0$ and $d \mid (k - l)$.

In (d), we have $q \equiv -1 \bmod 4$, $4 \mid n$, and $2\lfloor d \rfloor_2 = \lfloor q+1 \rfloor_2$. Here (4.7) becomes $nd \mid (2n'(k-l) + 2n'k(q^i - 1) + s_i)$, where $n' = \lfloor n \rfloor_{2'}$. This implies that i is even and $\lfloor d \rfloor_{2'} \mid (k-l)$ (since $(n, s) = 1$). Now $\lfloor s_i \rfloor_2 = \lfloor i \rfloor_2 \lfloor d \rfloor_2$ and $\lfloor 2n'k(q^i - 1) \rfloor_2 = 2\lfloor ki \rfloor_2 \lfloor q+1 \rfloor_2 = 4\lfloor ki \rfloor_2 \lfloor d \rfloor_2$. So (4.7) gives $2\lfloor d \rfloor_2 \mid 2n'(k-l)$, and thus $\lfloor d \rfloor_2 \mid (k-l)$. Hence, $d \mid (k-l)$, so $k = l$; (4.7) then yields $(nd, q^i - 1) \mid s_i$, so $i = 0$. □

As for the t_k's when $d \mid (q-1)$, Proposition 4.5 indicates choices that suffice to construct generalized André systems. (We do not claim that these choices are necessary.)

Proposition 4.5. *Under the hypotheses of Theorem* 4.3, *suppose that* $d \mid (q-1)$. *Let s be as in* (4.8), *and select r_k and t_k* (*for* $0 \leqslant k < d$) *as follows*:

(a) *If* $q \not\equiv -1 \bmod 4$ *or if n or d is odd, let $r_k = k$ and choose t_k so that* $d \mid (p^{t_k} - 1)$.

(b) *If* $q \equiv -1 \bmod 4$ *and n and d are even, let $r_k = 2k$ and choose t_k so that* $2d \mid (p^{t_k} - 1)$. (*Note that t_k will then be even.*)

These choices for r_k and t_k in Theorem 4.3 *yield a generalized André system having a right nuclear subgroup of order* $(q^n - 1)/d$.

Proof. By Proposition 4.4 and the remarks preceeding it, we have appropriate choices for s and the r_k's. It remains to show that the choices for the t_k's satisfy (4.5) in Theorem 4.3(c). First, observe that $d \mid (p^{t_k}(q^i - 1) + (p^{t_k} - 1) - (p^{t_l} - 1)) = (p^{t_k} q^i - p^{t_l})$, so $d \mid (nd, p^{t_k} q^i - p^{t_l})$. Let $0 \leqslant i < n$ and $0 \leqslant l < k < d$, and assume that

$$(nd, p^{t_k} q^i - p^{t_l}) \mid ((r_k - r_l) + r_k(q^i - 1) + s_i). \tag{4.9}$$

In case (a), we have $r_k = k$ and $s = d$, so (4.9) yields $d \mid ((k-l) + k(q^i - 1) + s_i)$, which implies $d \mid (k-l)$, a contradiction. Thus, (4.5) is satisfied in this case.

Now consider case (b). Here we have $r_k = 2k$ and $s = \lfloor d \rfloor_{2'}$. From (4.9) we obtain $d \mid (2(k-l) + 2k(q^i - 1) + s_i)$. This requires that s_i be even, and therefore i is even as well. Then $2d \mid (q^i - 1)$, so $2d \mid (nd, p^{t_k} q^i - p^{t_l})$. By Theorem 2.4(c), $\lfloor s_i \rfloor_2 = \lfloor s \rfloor_2 \lfloor q^i - 1 \rfloor_2 / \lfloor q - 1 \rfloor_2 = \lfloor i \rfloor_2 \lfloor q+1 \rfloor_2 / 2 \geqslant \lfloor q+1 \rfloor_2 \geqslant 2\lfloor d \rfloor_2$, so $2d \mid s_i$. From $2d \mid (2(k-l) + 2k(q^i - 1) + s_i)$ we then obtain $d \mid (k-l)$, a contradiction. So (4.5) is satisfied here as well. □

5 Low-index cases

We now specialize the results in Section 4 to the index 1 and 2 cases. When $d = 1$, the generalized André system in question is in fact a Dickson nearfield. In this case, we immediately obtain the following theorem of Ellers and Karzel [1, §1] and its converse from Theorem 4.1, Theorem 4.2, and Theorem 4.3. This result will be used in Section 6.

Theorem 5.1. *Let* $F(+, \circ)$ *be a Dickson nearfield of order* p^t (p *prime*), *and let* $F(+, \cdot) = \mathrm{GF}(p^t)$ *be the underlying field with primitive element* ω. *Put* $q^n = p^t$ *where q is the order of the kernel, and let* $Z = \{a \in F^* : x \circ a = x \cdot a \ \forall x \in F\}$ *be the nub.*

Then (q, n) is a Dickson pair, $Z = \{\omega^{nj} : j \in \mathbb{Z}\}$, and there exists s such that $(s, n) = 1$ and

$$F^* = \bigcup_{0 \leqslant i < n} \omega^{s(q^i-1)/(q-1)} \cdot Z.$$

Furthermore, the nearfield multiplication $\circ$ is described by

$$\begin{gathered} x \circ 0 = 0 \\ x \circ \omega^{s(q^i-1)/(q-1)+nj} = x^{q^i} \cdot \omega^{s(q^i-1)/(q-1)+nj} \end{gathered} \tag{5.1}$$

for all $x \in F$, $0 \leqslant i < n$, and $0 \leqslant j < (q^n - 1)/n$. Furthermore, ω can be chosen so that $s = 1$.

Conversely, for any Dickson pair (q, n) with $q^n = p^t$ and any s such that $(s, n) = 1$, the operation $\circ$ on F defined by (5.1) yields a Dickson nearfield $F(+, \circ)$ of order p^t.

The index $d = 2$ case was considered by Hiramine and Johnson in [3, (4.1), (4.3)], where they classified the generalized André planes that possess an index 2 homology group. However, their classification overlooked an infinite class of such planes, namely, those corresponding to the case where (q, n) is not a Dickson pair. These occur in part (c) below.

Theorem 5.2. *Let $F(+, \cdot) = \mathrm{GF}(p^t)$, where p is an odd prime. Let $q^n = p^t$ such that every prime factor of n divides $q - 1$.*

(a) *If $q \not\equiv -1 \bmod 4$ or n is odd, let $s = 2$, $r_1 = 1$, and $t_1 \geqslant 0$.*

(b) *If $q \equiv -1 \bmod 4$ and $n \equiv 2 \bmod 4$, let $s = 1$, $r_1 = n$, and $t_1 \geqslant 0$ with t_1 even.*

(c) *If $q \equiv 3 \bmod 8$ and $n \equiv 0 \bmod 4$, let $s = 1$, $r_1 = 2\lfloor n \rfloor_{2'}$, and $t_1 \geqslant 0$ with t_1 even.*

Let ω be a primitive element of $F(+, \cdot)$. Then

$$F^* = \bigcup_{0 \leqslant k < 2} \bigcup_{0 \leqslant i < n} \omega^{kr_1q^i} \cdot \omega^{s(q^i-1)/(q-1)} \cdot \omega^{2n\mathbb{Z}}.$$

Define a multiplication $\circ : F \times F \to F$ by

$$\begin{gathered} x \circ 0 = 0 \\ x \circ \omega^{s(q^i-1)/(q-1)+2nj} = x^{q^i} \cdot \omega^{s(q^i-1)/(q-1)+2nj} \\ x \circ \omega^{r_1q^i+s(q^i-1)/(q-1)+2nj} = x^{p^{t_1}q^i} \cdot \omega^{r_1q^i+s(q^i-1)/(q-1)+2nj} \end{gathered}$$

for all $x \in F$, $0 \leqslant i < n$, and $0 \leqslant j < (q^n - 1)/2n$. Then $F(+, \circ)$ is a generalized André system of order p^t having a right nuclear subgroup of order $(p^t - 1)/2$.

Conversely, every generalized André system of order p^t having a right nuclear subgroup $H(\circ)$ of order $(p^t-1)/2$ can (for some choice of ω) be represented in the above form, where n is the order of the companion automorphism group of $H(\circ)$.

Proof. Most of this follows directly from the results in Section 4. In particular, the choices for s and r_1 are in accord with (4.8) and Proposition 4.4. The statements of greatest interest concern the choices for t_1; we justify that the indicated choices, and only these choices, satisfy (4.5). For convenience, let $\alpha_i = (2n, p^{t_1}q^i - 1)$ and $\beta_i = r_1 q^i + s(q^i - 1)/(q-1)$. Condition (4.5) then reads: $\alpha_i \nmid \beta_i$ for all $0 \leqslant i < n$.

In (a), (4.5) is satisfied for all choices of $t_1 \geqslant 0$ since α_i is even and β_i is odd for all $0 \leqslant i < n$.

Consider (b) and (c) together. Note that (4.5) automatically holds when i is odd since then β_i is also odd. Suppose first that t_1 is even. Then $4 \mid \alpha_i$ but $\beta_i \equiv 2 \bmod 4$ when i is even, so (4.5) holds for all i. Now suppose that t_1 is odd, and consider $i = n/2$. We have $\lfloor \alpha_{n/2} \rfloor_2 = 2$, so $\lfloor \alpha_{n/2} \rfloor_2 \mid \beta_{n/2}$. Also, $\lfloor n \rfloor_{2'} \mid (q^{n/2}-1)/(q-1)$, so $\lfloor n \rfloor_{2'} \mid \beta_{n/2}$. But $\lfloor \alpha_{n/2} \rfloor_{2'} \mid n$, so $\alpha_{n/2} \mid \beta_{n/2}$. Thus, (4.5) cannot be satisfied for $i = n/2$ when t_1 is odd. □

A few remarks are in order. First, there are no generalized André systems that possess an index 2 right or middle nucleus when $q \equiv -1 \bmod 8$ and $n \equiv 0 \bmod 4$. Second, the necessity that t_1 be even in (b) settles in the affirmative the conjecture [3, (4.4)] of Hiramine and Johnson. Finally, in [3, (2.4)], Hiramine and Johnson incorrectly state that in the above context (q, n) must be a Dickson pair. This resulted in the omission in their classification [3, (4.3)] of the index 2 planes in the non-Dickson pair case. As Theorem 5.2(c) above illustrates, there is in fact an infinite family of index 2 generalized André systems where (q, n) is not a Dickson pair.

Example 5.3. In Theorem 5.2(c), take $q = 3$, $n = 4$, $s = 1$, $r_1 = 2$, and $t_1 = 0$. Note that $(q, n) = (3, 4)$ is not a Dickson pair. Let $F = \mathrm{GF}(3^4)$ and $F^* = \langle \omega \rangle$. The corresponding companion automorphism map $\lambda : F^* \to \operatorname{Aut} F$ is given by $\lambda(\omega^i) = (x \mapsto x^{3^{h_i}})$ where

$$h_i = \begin{cases} 0 & \text{if } i \equiv 0, 2 \bmod 8 \\ 1 & \text{if } i \equiv 1, 7 \bmod 8 \\ 2 & \text{if } i \equiv 4, 6 \bmod 8 \\ 3 & \text{if } i \equiv 5, 3 \bmod 8. \end{cases}$$

The resulting generalized André system $F(+, \circ)$ has kernel of order 3, nub $Z = \omega^{8\mathbb{Z}}$ of index 8, and nuclei $N_r(\circ) = \omega^{\{0,1,4,5\}+8\mathbb{Z}}$ and $N_m(\circ) = \omega^{\{0,3,4,7\}+8\mathbb{Z}}$, both of index 2. Since $N_r \neq N_m$, the corresponding plane is neither a nearfield nor an André plane.

Example 5.3 provides a minimum order example of the non-Dickson pair case. Perhaps of greater interest is the fact that $N_r \neq N_m$, even though both nuclei have index 2. This provides a counterexample to the claim made in [3, (5.1)] (the proof there errs in the assumption that $g\Sigma_l$ is contained in Σ^*).

6 Replacements in Dickson nearfield planes

In this section we develop a replacement procedure in Dickson nearfield planes that generalizes the "Type 2" replacements of Hiramine and Johnson [3, Section 3.2]. The resulting planes are generalized André planes that admit a homology group of prescribed size. The procedure is nub preserving in the sense that the nub of the resulting generalized André system contains the nub of the original nearfield. We determine necessary and sufficient numerical conditions under which this procedure actually succeeds. Furthermore, we determine decomposition parameters for the resulting generalized André systems when represented as in Theorem 4.1.

Let $F(+,\circ)$ be a (q,n)-Dickson nearfield, and represent it as in Theorem 5.1 with $s=1$. Let d be any divisor of n. As $F^*(\circ)/Z$ is cyclic of order n with a generator $\omega\cdot Z$, there is a unique subgroup $H(\circ)/Z \leqslant F^*(\circ)/Z$ of index d with generator $\omega^{\circ d}\cdot Z$. Thus, there is a unique subgroup $H(\circ)\leqslant F^*(\circ)$ of order $(q^n-1)/d$ containing Z. Furthermore, $Z \trianglelefteq H(\circ) \trianglelefteq F^*(\circ)$ and

$$H(\circ) = \bigcup_{0\leqslant i<n/d} \omega^{\circ di}\cdot Z = \bigcup_{0\leqslant i<n/d} \omega^{(q^{di}-1)/(q-1)+n\mathbb{Z}}$$

$$F^*(\circ) = \bigcup_{0\leqslant k<d} H_k = \bigcup_{0\leqslant k<d}\ \bigcup_{0\leqslant i<n/d} \omega^{\circ(k+di)}\cdot Z,$$

where $H_k = \omega^k \circ H(\circ) = \omega^{(q^{k+di}-1)/(q-1)+n\mathbb{Z}}$ (for $0\leqslant k<d$) are the cosets of $H(\circ)$ in $F^*(\circ)$.

Let $\Sigma_k = \Sigma(H_k) = \{x\mapsto x\circ h : h\in H_k\} \subseteq \Gamma\mathrm{L}(1,F(+,\cdot))$. These Σ_k's partition the spread map set of the nearfield plane $\mathscr{A}(F(+,\circ))$ along the cosets of $H(\circ)$ in $F^*(\circ)$. Our aim is to find replacements for the partial spreads determined by the Σ_k's so as to obtain a generalized André plane admitting a homology group (induced by $H(\circ)$) of order $(q^n-1)/d$. (Note: two partial spreads are replacements for each other if their components cover exactly the same points.)

To this end, let $\rho : x\mapsto x^{p^e}$ be any automorphism of $F(+,\cdot)$, let $0\leqslant k<d$, and define

$$\begin{aligned}\tilde{\Sigma}_k &= \rho\Sigma_k = \{x\mapsto x^\rho\circ h : h\in H_k\}\\ &= \{x\mapsto x^{p^e q^{k+di}}\cdot \omega^{(q^{k+di}-1)/(q-1)+nj} : 0\leqslant i<n/d \text{ and } 0\leqslant j<(q^n-1)/n\}.\end{aligned}$$

Since $\Sigma_k \subseteq \Gamma\mathrm{L}(1,F(+,\cdot))$, it is clear that $\tilde{\Sigma}_k \subseteq \Gamma\mathrm{L}(1,F(+,\cdot))$ as well.

Claim 6.1. *$\tilde{\Sigma}_k$ is a partial spread map set of F (considered as a vector space over* $\mathrm{GF}(p)$*) such that $\tilde{\Sigma}_k\sigma = \tilde{\Sigma}_k$ for all $\sigma\in\Sigma(H)$ and $\sigma\tilde{\Sigma}_k = \tilde{\Sigma}_k$ for all $\sigma\in\Sigma(Z)$.*

Proof. First, $\rho\in\mathrm{GL}(F,p)$ and $\Sigma_k\subseteq\mathrm{GL}(F,p)$, so $\tilde{\Sigma}_k\subseteq\mathrm{GL}(F,p)$. Since Σ_k acts sharply on F^*, so does $\rho\Sigma_k$. Thus, $\tilde{\Sigma}_k$ is a partial spread map set of F. For $\sigma(h)\in\Sigma(H)$, we have $\tilde{\Sigma}_k\sigma(h) = \rho\Sigma(H_k)\sigma(h) = \rho\Sigma(H_k\circ h) = \rho\Sigma(H_k) = \rho\Sigma_k = \tilde{\Sigma}_k$. Finally, let $\sigma(z)\in\Sigma(Z)$. Then $z^\rho\in Z$ since Z is a characteristic subgroup of $F^*(\cdot)$.

Also $x^{\sigma(z)\rho} = (x \cdot z)^{\rho} = x^{\rho} \cdot z^{\rho}$, i.e., $\sigma(z)\rho = \rho\sigma(z^{\rho})$. Thus, $\sigma(z)\tilde{\Sigma}_k = \sigma(z)\rho\Sigma(H_k) = \rho\sigma(z^{\rho})\Sigma(H_k) = \rho\Sigma(z^{\rho} \circ H_k) = \rho\Sigma(H_k) = \tilde{\Sigma}_k$. □

Claim 6.2. *$\tilde{\Sigma}_k$ is a replacement for Σ_k if and only if $d \mid (p^e - 1)$.*

Proof. First we elucidate what it means for $\tilde{\Sigma}_k$ to replace Σ_k:

$$
\begin{aligned}
&\tilde{\Sigma}_k \text{ replaces } \Sigma_k \\
&\quad \Leftrightarrow \forall x \in F^* : x^{\rho} \circ H_k = x \circ H_k \\
&\quad \Leftrightarrow \forall x \in F^*\ \forall i\ \exists j\colon x^{\rho} \circ \omega^{\circ(k+dj)} \cdot Z = x \circ \omega^{\circ(k+di)} \cdot Z \\
&\quad \Leftrightarrow \forall a\ \forall i\ \exists j \geqslant i\colon \omega^{ap^e q^{k+dj}} \cdot \omega^{(q^{k+dj}-1)/(q-1)} \in \omega^{aq^{k+di}} \cdot \omega^{(q^{k+di}-1)/(q-1)} \cdot Z \\
&\quad \Leftrightarrow \forall a\ \forall i\ \exists j \geqslant i\colon \omega^{aq^k(p^e q^{dj} - q^{di})} \cdot \omega^{q^k(q^{dj}-q^{di})/(q-1)} \in Z \\
&\quad \Leftrightarrow \forall a\ \forall i\ \exists j \geqslant i\colon q^{k+di}\left(a(p^e q^{d(j-i)} - 1) + \frac{q^{d(j-i)} - 1}{q-1}\right) \equiv 0 \bmod n \\
&\quad \Leftrightarrow \forall a\ \exists j \geqslant 0\colon (ap^e(q-1)+1) \cdot \frac{q^{dj}-1}{q-1} + a(p^e - 1) \equiv 0 \bmod n. \qquad (6.1)
\end{aligned}
$$

Suppose $\tilde{\Sigma}_k$ is a replacement for Σ_k, so that (6.1) holds. Now $d \mid n$, so d divides the left-hand side of (6.1). Furthermore, every prime factor of d divides $q-1$, so $d \mid (q^{dj}-1)/(q-1)$ by Corollary 2.5(a), and therefore $d \mid a(p^e - 1)$. As this must hold in particular when $a = 1$, we obtain $d \mid (p^e - 1)$.

Conversely, suppose $d \mid (p^e - 1)$. In (6.1), let $\alpha = ap^e(q-1)+1$ and $\beta = -a(p^e-1)$. Now every prime factor of n divides $q-1$, so $(\alpha, n) = 1$. Thus, the congruence $\alpha x \equiv \beta \bmod n$ has a unique solution for x modulo n. But $\{(q^i - 1)/(q-1) : 1 \leqslant i \leqslant n\}$ is a complete set of remainders modulo n, so there is a unique solution to $\alpha x \equiv \beta \bmod n$ of the form $(q^f - 1)/(q-1)$ with $1 \leqslant f \leqslant n$.

To show that (6.1) holds, it suffices to show that $d \mid f$ (for then we can take $j = f/d$). To this end, first note that $d \mid \beta$ by hypothesis. Further, $(d, \alpha) = 1$ since every prime factor of d divides $q-1$, so $d \mid (q^f - 1)/(q-1)$. By Corollary 2.5(b), we get $d \mid f$ except possibly in the case where $q \equiv -1 \bmod 4$ and f is even. In the latter case, we have $\lfloor d \rfloor_{2'} \mid f$; furthermore, $\lfloor d \rfloor_2 \leqslant 2$ in this situation since (q, n) is a Dickson pair, so $\lfloor d \rfloor_2 \mid f$. In all cases, we obtain $d \mid f$, as required. □

Theorem 6.3. *Let $F(+, \circ)$ be a (q, n)-Dickson nearfield, with $q = p^r$ and p prime. Represent $F(+, \circ)$ as in Theorem 5.1 with $s = 1$. Let d be any divisor of n.*

(a) *There exists a unique subgroup $H(\circ) \leqslant F^*(\circ)$ of order $(q^n - 1)/d$ such that $Z \leqslant H(\circ)$. Furthermore, $Z \trianglelefteq H(\circ) \trianglelefteq F^*(\circ)$, and the cosets of $H(\circ)$ in $F^*(\circ)$ are (for $0 \leqslant k < d$):*

$$H_k = \omega^{\circ k} \circ H = \{\omega^{(q^{k+di}-1)/(q-1)+nj} : 0 \leqslant i < n/d \text{ and } 0 \leqslant j < (q^n - 1)/n\}.$$

(b) *For each* $0 \leqslant k < d$, *select an automorphism* $\rho_k : x \mapsto x^{p^{t_k}}$ *of* $F(+,\cdot)$ *with* $\rho_0 = 1$, *let* $\Sigma_k = \{x \mapsto x \circ h : h \in H_k\}$ *and* $\tilde{\Sigma}_k = \rho_k \circ \Sigma_k = \{x \mapsto x^{\rho_k} \circ h : h \in H_k\}$, *and put* $\Sigma = \bigcup_{0 \leqslant k < d} \Sigma_k$ *and* $\tilde{\Sigma} = \bigcup_{0 \leqslant k < d} \tilde{\Sigma}_k$.

Σ_k *and* $\tilde{\Sigma}_k$ *are partial spread map sets of* F (*as a vector space over* $\mathrm{GF}(p)$) *of the form*:

$$\Sigma_k = \left\{ x \mapsto x^{q^{k+di}} \cdot \omega^{(q^{k+di}-1)/(q-1)+nj} : 0 \leqslant i < \frac{n}{d} \text{ and } 0 \leqslant j < \frac{q^n - 1}{n} \right\}$$

$$\tilde{\Sigma}_k = \left\{ x \mapsto x^{p^{t_k} q^{k+di}} \cdot \omega^{(q^{k+di}-1)/(q-1)+nj} : 0 \leqslant i < \frac{n}{d} \text{ and } 0 \leqslant j < \frac{q^n - 1}{n} \right\}.$$

(c) $\tilde{\Sigma}$ *is a spread map set of* F *if and only if* $d \mid (p^{t_k} - 1)$ *for all* $0 \leqslant k < d$.

(d) *Suppose* $\tilde{\Sigma}$ *is a spread map set of* F, *and let* $\mathscr{A}(\tilde{\Sigma})$ *denote the corresponding translation plane with point set* $F \oplus F$. *Then* $\mathscr{A}(\tilde{\Sigma})$ *is a generalized André plane of order* q^n *obtained from the nearfield plane* $\mathscr{A}(\Sigma)$ *by multiple net replacement*. $\mathscr{A}(\tilde{\Sigma})$ *admits a group of homologies* $\mathscr{H}_{(0)} = \{(x, y) \mapsto (x, y \circ h) : h \in H\}$ *of order* $(q^n - 1)/d$ *and a group of homologies* $\mathscr{Z}_{(\infty)} = \{(x, y) \mapsto (x \circ z, y) : z \in Z\}$ *of order* $(q^n - 1)/n$. *The kernel of* $\mathscr{A}(\tilde{\Sigma})$ *has order* p^g *where* $g = \gcd\{t_k + rk : 1 \leqslant k \leqslant d\}$ (*where* $t_d = 0$). *In particular, the kernel is a subfield of* $\mathrm{GF}(q^d)$.

Proof. Parts (a) and (b) are clear from considerations made above; part (c) follows from Claim 6.2. For part (d), $\mathscr{A}(\tilde{\Sigma})$ is a generalized André plane since $\Sigma \subseteq \Gamma\mathrm{L}(1, F(+,\cdot))$. The statement concerning the homology groups follows from Claim 6.1. The rest follows from the fact that the kernel is the fixed field of the set of companion automorphisms $\lambda(\tilde{\Sigma}) = \{x \mapsto x^{p^{t_k} q^{k+di}} : 0 \leqslant k < d$ and $0 \leqslant i < n/d\}$ ([5, Theorem 10.7]).

Example 6.4. The case $d = 2$. (This case was considered in [3, (3.4)], but the claim that the kernel must be a subfield of $\mathrm{GF}(q)$ is in error.) Since $2 \mid n$ and $n \mid (q^n - 1)$, p must be odd. So $2 \mid (p^{t_1} - 1)$ for all t_1. Thus, any choice for t_1 leads to a spread. By appropriate choice of t_1, one can obtain planes with any subfield of $\mathrm{GF}(q^2)$ as kernel. In particular, by taking t_1 to be an odd multiple of r, we see that the kernel can in fact grow to $\mathrm{GF}(q^2)$.

Example 6.5. The case $d = 3$. Here we have $3 \mid n$, so $3 \mid (q - 1)$. If $3 \mid (p - 1)$ (in particular, when r is odd), then any choices for t_1 and t_2 yield a spread. If $3 \mid (p + 1)$, then any choices with t_1 and t_2 even will yield a spread.

The generalized André systems resulting from Theorem 6.3 can be subjected to the decomposition in Theorem 4.1. Here we determine appropriate values for the parameters in this decomposition. Quantities appearing in Theorem 4.1 will be adorned with overbars to distinguish them from those that occur in Theorem 6.3. The groups H and Z correspond directly in both theorems. Thus, $\bar{d} = d$ and $\bar{n}\bar{d} = n$, from which we obtain $\bar{q}^{\bar{n}} = p^t = q^n = q^{\bar{n}d}$, so $\bar{q} = q^d$. Further, $p^{\bar{r}} = \bar{q} = q^d = p^{rd}$, so $\bar{r} = rd$. To determine $\bar{s}$, observe that $\lambda(\omega^{\bar{s}}) = (x \mapsto x^{\bar{q}}) = (x \mapsto x^{q^d}) = \lambda(\omega^{\circ d}) = \lambda(\omega^{(q^d-1)/(q-1)})$, so we can take $\bar{s} = (q^d - 1)/(q-1)$. To determine choices for the $\bar{r}_k$'s, we compare the exponents on ω for arbitrary elements of F^* under both representations:

$$\begin{aligned}\frac{q^{k+di}-1}{q-1} + nj &= q^{di} \cdot \frac{q^k - 1}{q-1} + \frac{q^{di}-1}{q-1} + nj \\ &= \frac{q^k-1}{q-1} \cdot \bar{q}^i + \bar{s} \cdot \frac{\bar{q}^i - 1}{\bar{q}-1} + \bar{n}\,\overline{dj},\end{aligned}$$

so we can take $\bar{r}_k = (q^k - 1)/(q-1)$. Finally, to determine the $\bar{t}_k$'s, the automorphisms $\lambda(\omega^{\bar{r}_k \bar{q}^i + \bar{s}(\bar{q}^i - 1)/(\bar{q}-1)}) = (x \mapsto x^{p^{\bar{t}_k} \bar{q}^i})$ and $\lambda(\omega^{(q^{k+di}-1)/(q-1)}) = (x \mapsto x^{p^{t_k} q^{k+di}})$ must coincide. Hence, we can take $\bar{t}_k \equiv t_k + rk \bmod t$.

Acknowledgment. The author would like to thank the referee for uncovering an error in the original version of this article.

References

[1] E. Ellers, H. Karzel, Endliche Inzidenzgruppen. *Abh. Math. Sem. Univ. Hamburg* **27** (1964), 250–264. MR 29 #3934 Zbl 123.37901

[2] D. A. Foulser, A generalization of André's systems. *Math. Z.* **100** (1967), 380–395. MR 37 #3436 Zbl 152.18903

[3] Y. Hiramine, N. L. Johnson, Generalized André planes of order p^t that admit a homology group of order $(p^t - 1)/2$. *Geom. Dedicata* **41** (1992), 175–190. MR 92m:51016 Zbl 753.51002

[4] N. Knarr, *Translation planes.* Springer 1995. MR 98e:51019 Zbl 843.51004

[5] H. Lüneburg, *Translation planes.* Springer 1980. MR 83h:51008 Zbl 446.51003

Received 17 January, 2001; revised 7 June, 2001

Dean E. Draayer, 20 Brookwood Drive, South Burlington, VT 05403-6202, USA
Email: draayer@surfglobal.net