A note on some flag-transitive affine planes

William M. Kantor[*] and Chihiro Suetake

ABSTRACT

New nondesarguesian flag-transitive affine planes of order q^n are constructed whenever $n \geq 3$ is an odd integer and $q^n > 27$ is a prime power such that $q^n \equiv 3 \pmod 4$.

Relatively few finite nondesarguesian flag-transitive affine planes are known whose collineation groups are solvable. With a single exception (see below), all of the known ones of odd order fall into two families studied in [Ka; Su1]; those references also contain some historical remarks. The purpose of this note is to construct an additional family of such planes, explain why they are new, and estimate how many pairwise nonisomorphic planes are obtained by this construction.

Theorem. Suppose that the prime power q and the odd integer $n \geq 3$ are such that $q^n \equiv 3 \pmod 4$. Then, for each nontrivial element $\sigma \in \mathrm{Gal}(GF(q^n)/GF(q))$ and each $b \in GF(q^{2n})$ such that $b^{q^n-1} = -1$, there is an affine plane $\pi(b,\sigma)$ for which the following hold:

(i) $\pi(b,\sigma)$ is a nondesarguesian plane of order q^n;

(ii) $\pi(b,\sigma)$ admits a solvable flag-transitive group;

(iii) $\pi(b,\sigma)$ does not admit a cyclic group transitive on the line at infinity; and

(iv) The number of pairwise nonisomorphic planes $\pi(b,\sigma)$ of order q^n is at least $\frac{1}{2}(n/n^* - 1)(q^{n^*} - 1)/2en^*$, where $q = p^e$ with p prime and n/n^* is the smallest prime factor of n.

Our construction also works when $q^n \equiv 1 \pmod 4$, but in that case it produces members of one of the two families of planes constructed in [Ka; Su1]. The members of the second family in [Ka; Su1] have the same orders as planes in the Theorem but do not satisfy condition (iii). One further plane is in the literature that behaves as in the Theorem [NRKRS], but a computer investigation has shown that this plane of order 27 is one of those in the Theorem [Su2]; it is the only plane in the Theorem that is not new.

Throughout this note let $F = GF(q^{2n})$, $L = GF(q^n)$ and $K = G(F(q))$, where $n \geq 3$ and $q = p^e$ for an odd prime p. We will use a field automorphism $\sigma \neq 1$ and field elements t, b and d behaving as follows: $t \in F^*$ has order $(q^n + 1)(q - 1)/2$; L has odd degree over the fixed field K' of $\sigma \in \mathrm{Gal}(L/K)$; $b \in F$ satisfies $b = -b$ (where bar denotes the involutory automorphism of F); and $d \in F^*$ is such that $d\overline{d}$ is an element of K' that is not a square in L. Since $|L^*:K'^*|$ is odd, there is

---

such an element d.

We will view F as a 2n-dimensional vector space over K. Write $h(x) = x + bx^\sigma$ for $x \in L$. Then $h(L)$ is a K-subspace of F. Set

$$\mathscr{S}(b,\sigma) = \{ h(L)t^i \mid 0 \le i \le (q^n - 1)/2 \} \cup \{ \overline{h(L)} \ dt^i \mid 0 \le i \le (q^n - 1)/2 \}.$$

Lemma 1. (i) $\mathscr{S}(b,\sigma)$ is a spread.

(ii) The group of permutations of F generated by $z \longrightarrow tz$ and $z \longrightarrow d\bar{z}$ is a collineation group transitive on the line at infinity of the corresponding affine plane $\pi(b,\sigma)$.

Proof. First of all, h is injective: if $x + bx^\sigma = 0$ with $x \in L$ then also $\overline{x + bx^\sigma} = 0$, so that $x = 0$. Thus, $\mathscr{S}_{b,\sigma}$ consists of n-dimensional K-spaces. The map $z \longrightarrow tz$ permutes the members of $\mathscr{S}(b,\sigma)$ since $t^{(q^n+1)/2} \in tK$. Also, $z \longrightarrow d\bar{z}$ sends $h(L)t^i$ to $\overline{h(L)t}$ ^id and $\overline{h(L)}$ dt^i to $dh(L)\overline{dt}$ ^{i}, where $d\bar{d}$ $h(L) = h(L)$ since $d\bar{d}(x + bx^\sigma) = (d\bar{d} \ x) + b(d\bar{d} \ x)^\sigma$. This proves (ii) if (i) is presupposed.

A verbatim repetition of the proof of [Ka, Theorem 2(i)] yields that $h(L) \cap h(L)t^i = 0$ if $1 \le i \le (q^n - 1)/2$.

In view of transitivity, it remains to eliminate the possibility that $h(x) = \overline{h(y)}$ dt^i for some $x, y \in L^*$ and some i. This equation implies that

$$x^2 - b^2 x^{2\sigma} = (x + bx^\sigma)(x + \overline{bx^\sigma}) = t^i \overline{t}{}^i d\bar{d}(y + by^\sigma)(y - by^\sigma) = kd\bar{d} \ [b^2 y^2 - b^2(by)^{2\sigma}],$$

where $k = t^i \overline{t}$ ^{i} is a square in K. Then $x^2 - kd\bar{d}$ $y^2 = b^2(x^2 - kd\bar{d}$ $y^2)^\sigma$ since $(d\bar{d})^\sigma = d\bar{d}$. However, $(x^2 - kd\bar{d}$ $y^2)^{\sigma-1}$ is the square of an element of L while b^2 is not, so it follows that $x^2 - kd\bar{d}$ $y^2 = 0$. α

Thus, $(x/y)^2/k = d\bar{d}$, whereas $d\bar{d}$ was assumed not to be a square in L. $\square$

Lemma 2. The spread $\mathscr{S}(b,\sigma)$ does not depend on the choice of d.

Proof. Recall that $d\bar{d}$ is an element of K' that is not a square in L. Assume that u is another element of F satisfying these conditions. Then $(u/d)\overline{u/d} \in K'$, and $(u/d)\overline{u/d} = m^2$ with $m \in L$. However, $|L^*:K'^*|$ is odd, so that $m \in K'$. Moreover, $(u/dm)\overline{u/dm} = 1$, so that $u = dmt^i$ for some i. Consequently, $(x - bx^\sigma)u = (mx - b(mx)^\sigma)dt^i$ whenever $x \in L$, and hence $\overline{h(L)}$ $u = \overline{h(L)}$ dt^i. $\square$

Remark 1. The kernel of the plane $\pi(b,\sigma)$ corresponding to $\mathscr{S}(b,\sigma)$ contains K'. Moreover, if we had started with K' in place of K but used the same σ, b and d, then we would have obtained the same spread $\mathscr{S}(b,\sigma)$ and plane $\pi(b,\sigma)$. In other words, there would have been no loss of generality if we had assumed from the outset that K was the fixed field of σ. In that case, our assumption concerning the degree of L is simply that n is odd. Moreover, we can then see what d looks like: in view of Lemma 2, we can choose d to be an element of order

$(q^n + 1)(q - 1)$, and even one whose square is t.

Remark 2. While the construction used the fact that $|L^*:K'^*|$ is odd, it did not use the assumption $q^n \equiv 3 \pmod 4$ appearing in the Theorem. However, when $q^n \equiv 1 \pmod 4$ the plane $\pi(b,\sigma)$ is not new: it is one of those studied in [Ka; Su1]. In order to see this, let τ be an automorphism of F whose restriction to L is σ and whose fixed field is K' (so that $|\tau| = 2|\sigma|$). Write $h'(x) = x + bx^\tau$ for $x \in F$, so that $h'(L) = h(L)$. We claim that $\mathscr{S}(b,\sigma)$ coincides with the spread

$$\{ h'(L)t^i \mid 0 \le i \le \tfrac{1}{2}(q^n - 1) \} \cup \{ h'(bL)t^i \mid 0 \le i \le \tfrac{1}{2}(q^n - 1) \}$$

appearing in [Ka; Su1]. By Lemma 2, we are free to choose a convenient element d.

Let $d = b^{1+\tau+\cdots+\tau^{m-1}}$, where m is the dimension of L over K'. Then $d\bar{d} = -(b^2)^{1+\tau+\cdots+\tau^{m-1}}$ is the product of a square element of L (namely, -1) and an odd number of nonsquare elements, and hence is a nonsquare in L. Also, $d^\tau = (b^{1+\tau+\cdots+\tau^{m-1}})^\tau = -d$ since τ^m is the involutory automorphism of F, and hence $(d\bar{d})^\sigma = d\bar{d}$. Finally, if $x \in L$ and we write $y = (b/d)x$, then $y \in L$ and

$$\overline{h(y)} \, d = ((b/d)x - b((b/d)x)^\sigma)d = bx - (d/d^\tau)bb^\tau x = bx + bb^\tau x = h'(bx).$$

This proves our claim. $\square$

We now turn briefly to isomorphisms among the planes $\pi(b,\sigma)$. Consider the set $bL^* = \{z \in F^* \mid z = -z\}$. For each $\alpha \in L^*$ and each $\varphi \in \mathrm{Aut}F$ the permutation $z \to \alpha^{1-\sigma}z^\varphi$ of F acts on bL^*; let α and φ vary, and let $H(\sigma)$ be the group of permutations of bL^* all of these permutations induce. Note that $|H(\sigma)| = 2ne|L^*:K'^*|$. The same arguments used to prove [Ka, Lemma 2 and Theorem 2(iii)] yield the following lemma (but the proof is much simpler here, since n is odd).

Lemma 3. Let $c \in bL^*$ and $1 \ne \sigma \in \mathrm{Gal}(L/K)$.

(i) $\pi(b,\sigma) \cong \pi(b^{-1},\sigma^{-1})$.

(ii) If b and c are in the same $H(\sigma)$-orbit then $\pi(b,\sigma) \cong \pi(c,\sigma)$.

(iii) If $\pi(b,\sigma) \cong \pi(c,\tau)$ then $\tau = \sigma^{\pm 1}$.

(iv) If $\pi(b,\sigma) \cong \pi(c,\sigma)$ then b and c are in the same $H(\sigma)$-orbit.

(v) $\pi(b,\sigma)$ does not admit a cyclic group transitive on the line at infinity.

The Theorem is now an easy consequence of Lemmas 1-3 (exactly as in [Ka, Theorem 1(iii)]).

References

[Ka]   W. M. Kantor, Two families of flag-transitive affine planes (to appear in Geom. Ded.).

[NRKRS] M. L. Narayana Rao, K. Kuppuswamy Rao and K. Satyanarayana, A third flag transitive affine plane of order 27. Houston J. Math. 10 (1984) 127-145.

[Su1]   C. Suetake, Flag transitive planes of order q^n with a long cycle on ℓ_∞ as a collineation. Graphs and Combinatorics 7 (1991) 183-195.

[Su2]   C. Suetake, On flag-transitive affine planes of order q^3 (submitted).

University of Oregon   Amagasakiminami High School
Eugene, OR 97403   Amagasaki, Hyogo 660
USA   Japan