Journal of Combinatorial Theory, Series A **95**, 158–168 (2001)
doi:10.1006/jcta.2000.3158, available online at http://www.idealibrary.com on IDEAL®

A Trace Conjecture and Flag-Transitive Affine Planes

R. D. Baker

Department of Mathematics, West Virginia State College, Institute, West Virginia 25112-1000

G. L. Ebert[1]

Department of Mathematical Sciences, University of Delaware, Newark, Delaware 19716-2553

K. H. Leung[2]

Department of Mathematics, University of Singapore, Kent Ridge, Singapore 119260

and

Q. Xiang[3]

Department of Mathematical Sciences, University of Delaware, Newark, Delaware 19716-2553

Communicated by the Managing Editors

Received April 12, 2000; published online May 10, 2001

For any odd prime power q, all $(q^2 - q + 1)$th roots of unity clearly lie in the extension field $\mathbb{F}_{q^6}$ of the Galois field $\mathbb{F}_q$ of q elements. It is easily shown that none of these roots of unity have trace -2, and the only such roots of trace -3 must be primitive cube roots of unity which do not belong to $\mathbb{F}_q$. Here the trace is taken from $\mathbb{F}_{q^6}$ to $\mathbb{F}_q$. Computer based searching verified that indeed -2 and possibly -3 were the only values omitted from the traces of these roots of unity for all odd $q \leqslant 200$. In this paper we show that this fact holds for all odd prime powers q. As an application, all odd order three-dimensional flag-transitive affine planes admitting a cyclic transitive action on the line at infinity are enumerated. © 2001 Academic Press

[1] Research partially supported by NSA grant MDA 904-00-1-0029.
[2] Research partially supported by NUS research grant RP 3982723.
[3] Research partially supported by NSA grant MDA 904-99-1-0012. This author thanks Department of Mathematics, National University of Singapore for its hospitality during the time of this research.

0097-3165/01 $35.00

1. INTRODUCTION

This article deals with a cyclotomic question in the Galois field $\mathbb{F}_{q^6}$ of order q^6, where q is any odd prime power. This question is motivated by the classification of certain flag-transitive affine planes. Our arguments will reduce the problem to showing the existence of some irreducible polynomial in $\mathbb{F}_q[x]$. We denote the set of all nonzero squares of $\mathbb{F}_q$ by $\square_q$, the set of nonsquares by $\not\square_q$, and the nonzero elements of $\mathbb{F}$ by $\mathbb{F}^*$. Let Tr be the trace from $\mathbb{F}_{q^6}$ to $\mathbb{F}_q$; that is, $\mathrm{Tr}(x) = x + x^q + x^{q^2} + x^{q^3} + x^{q^4} + x^{q^5}$ for $x \in \mathbb{F}_{q^6}$.

With the exception of the Lüneburg planes and the Hering plane, all known finite flag-transitive affine planes have a translation complement which contains a linear cyclic subgroup that either is transitive or has two equal-sized orbits on the line at infinity. Under a mild number-theoretic condition involving the order and dimension of the plane (see [5]), it can be shown that one of these actions must occur. We call flag-transitive planes of the first kind C-planes and those of the second kind H-planes.

Subject to the number-theoretic condition mentioned above, all odd order two-dimensional flag-transitive affine planes are H-planes, and these have been completely classified in [1]. In particular, there are precisely $\frac{1}{2}(q-1)$ such (nondesarguesian) planes of order q^2 for any odd prime q. In [2] it is shown that every odd order three-dimensional flag-transitive affine plane of type C arises from a "perfect" Baer subplane partition of $PG(2, q^2)$. Perfect Baer subplane partitions by definition are an orbit of some Baer subplane under a Singer subgroup of order $q^2 - q + 1$. Moreover, in [3] it is shown that every perfect Baer subplane partition is equivalent to one which is an orbit of a Baer subplane which may be represented (as a root space in $\mathbb{F}_{q^6}$) by a linearized polynomial of the form $x^{q^3} + mx^{q^2} + nx^q + x$, where m and n are elements of $\mathbb{F}_{q^6}$ satisfying four conditions. The last condition says that $t = mn^{q^2} + m^{q^3}n^{q^5}$ is an element of $\mathbb{F}_q$, other than -1, which is not expressible as $\mathrm{N}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(1+u)$ for any $u \in \mathbb{F}_{q^6}$ with $u^{q^2-q+1} = 1$. Here $\mathrm{N}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}$ denotes the norm from $\mathbb{F}_{q^6}$ to $\mathbb{F}_{q^2}$, where one notes that $\mathrm{N}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(1+u) \in \mathbb{F}_q$ whenever $u^{q^2-q+1} = 1$. The conjecture made in [3] was that for any odd prime power q,

$$\mathbb{F}_q \backslash \{\mathrm{N}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(1+u) \mid u^{q^2-q+1} = 1\} = \begin{cases} \{0\} & \text{if} \quad q \not\equiv 1 \pmod 3 \\ \{0, -1\} & \text{if} \quad q \equiv 1 \pmod 3 \end{cases}.$$

Since the perfect Baer subplane partitions (and the resulting flag-transitive planes) corresponding to $t = 0$ are known, the proof of this conjecture would lead to a complete classification of three-dimensional odd order flag-transitive affine planes of type C. Here we prove this conjecture.

It will suit our purposes to first reformulate the conjecture in terms of traces from $\mathbb{F}_{q^6}$ to $\mathbb{F}_q$. If $u \in \mathbb{F}_{q^6}$ and $u^{q^2-q+1}=1$, then $u^{q^2+1}=u^q$, $u^{q^3}=u^{-1}$, $u^{1-q}=u^{-q^2}=u^{q^5}$, and $u^{q^2-q}=u^{-1}=u^{q^3}$. Thus $\mathrm{N}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(1+u)=(1+u)^{1+q^2+q^4}=(1+u)(1+u^{q^2})(1+u^{-q})=2+\mathrm{Tr}(u)$. Hence what we must show is that

$$\mathbb{F}_q \backslash \{\mathrm{Tr}(u) \mid u^{q^2-q+1}=1\} = \begin{cases} \{-2\} & \text{if} \quad q \not\equiv 1 \pmod 3 \\ \{-2, -3\} & \text{if} \quad q \equiv 1 \pmod 3 \end{cases}.$$

Our approach is based on the observation that any $u \in U = \{u \in \mathbb{F}_{q^6} \mid u^{q^2-q+1}=1\}$ which does not belong to the subfield $\mathbb{F}_{q^2}$ has minimal polynomial $p(x)$ over $\mathbb{F}_q$ which is irreducible, self-reciprocal, of degree 6, and has $-\mathrm{Tr}(u)$ as the coefficient of x^5. Thus the value set in question can be studied by examining these irreducible polynomials. We actually work "backwards" by counting the number of irreducible cubics $f(x)$ over $\mathbb{F}_q$ in a certain one parameter family, and then "lifting" each $f(x)$ to a degree 6 polynomial $p(x)=x^3 f(x+\frac{1}{x})$. This lifted polynomial will be monic, self-reciprocal, and irreducible over $\mathbb{F}_q$. The final step will be to show that $p(x)$ is, in fact, a minimal polynomial for an element of U. We end up showing not only that the values $\mathrm{Tr}(u)$, for $u \in U$, cover $\mathbb{F}_q \backslash \{-2, -3\}$, but that in addition the coverage is very "uniform." This depends upon early work of Hasse [6, 7], and thus we begin by reviewing quadratic characters.

2. QUADRATIC CHARACTER SUMS

In this section we collect a few facts about sums involving quadratic characters. Hence, let η denote the quadratic character of $\mathbb{F}_q$, so that

$$\eta(x) = \begin{cases} 1 & \text{if} \quad x \in \Box_q \\ 0 & \text{if} \quad x = 0 \\ -1 & \text{if} \quad x \in \not\Box_q. \end{cases}$$

We begin with a well known result. All sums are over $\mathbb{F}_q$ unless otherwise noted.

PROPOSITION 1. *Let q be an odd prime power and $f(x)=ax^2+bx+c \in \mathbb{F}_q[x]$ with $a \neq 0$. Then*

$$\sum_{x \in \mathbb{F}_q} \eta(ax^2+bx+c) = \begin{cases} -\eta(a) & \textit{if} \quad b^2-4ac \neq 0 \\ (q-1)\,\eta(a) & \textit{if} \quad b^2-4ac = 0. \end{cases}$$

Proof. The standard argument multiplies the sum by $\eta(4a^2)=1$, distributing through $\eta(4a)$ and completing the square to get $\eta(a)\cdot\sum_x \eta((2ax+b)^2-(b^2-4ac))=\eta(a)\sum_y \eta(y^2-d)$, where we have replaced $2ax+b$ by y and written d for b^2-4ac. The case when $d=0$ is clear. For $d\neq 0$ one counts the solutions of $y^2-d=z^2$. This is easy once we rewrite this equation as $(y+z)(y-z)=d$, and observe that y is just the average of complementary divisors of d. ∎

The following result is a special case of the Hasse–Weil bound, first proved by Hasse [6, 7] (cf. [8, p. 1]) in 1936.

THEOREM 2. *Let q be a prime power, and let N be the number of solutions $(x, y)\in\mathbb{F}_q\times\mathbb{F}_q$ of the equation $y^2=f(x)$, where $f(x)\in\mathbb{F}_q[x]$ is a polynomial of degree* 4 *with distinct roots. Then*

$$|N+1-q|\leqslant 2\sqrt{q}.$$

Stating this theorem in terms of quadratic character sums, we have

COROLLARY 3. *Let q be an odd prime power, let $f(x)\in\mathbb{F}_q[x]$ be a polynomial of degree* 4 *with distinct roots, and let η be the quadratic character of $\mathbb{F}_q$. Then*

$$\left|1+\sum_{x\in\mathbb{F}_q}\eta(f(x))\right|\leqslant 2\sqrt{q}.$$

Proof. Let N be the number of solutions $(x, y)\in\mathbb{F}_q\times\mathbb{F}_q$ of $y^2=f(x)$. Given x, there are 0, 1, or 2 choices for y accordingly as $f(x)$ belongs to $\not\square_q$, $\{0\}$, or $\square_q$. Thus $N=\sum_{x\in\mathbb{F}_q}(1+\eta(f(x)))=q+\sum_{x\in\mathbb{F}_q}\eta(f(x))$, and the corollary follows from Theorem 2. ∎

We now state and prove a useful lemma about the number of irreducible cubic polynomials in a family of polynomials parameterized by the coefficient of x.

LEMMA 4. *Let q be an odd prime power, $a\in\mathbb{F}_q$ with $a\neq -3$ or -4, and set $c=-(a+4)^2$. Let $\mathscr{P}=\{f(x)=x^3+ax^2+bx+c\mid b\in\mathbb{F}_q,\ -f(4)\in\not\square_q\}$, a family of cubic polynomials parameterized by the coefficient b of x. Then $\mathscr{P}$ contains $(q-1)/2$ polynomials, of which at least $\frac{1}{6}(q+1-2\sqrt{q})$ but not more than $\frac{1}{6}(q+1+2\sqrt{q})$ are irreducible over $\mathbb{F}_q$. In particular, $\mathscr{P}$ contains at least one polynomial $f(x)$ which is irreducible over $\mathbb{F}_q$.*

Proof. There are obviously q polynomials $f(x)=x^3+ax^2+bx-(a+4)^2$ as b varies over $\mathbb{F}_q$. With the restriction $-f(4)=-(64+16a+4b-(a+4)^2)\in\not\square_q$, the number of choices for b (hence the number of $f(x)$) is reduced to $(q-1)/2$ since $-f(4)$ is a linear expression in b.

We consider the subset $\mathscr{P}_0$ of those polynomials which are reducible over $\mathbb{F}_q$. We wish to develop a character sum for the cardinality of $\mathscr{P}_0$. Let $f(x) \in \mathscr{P}_0$, and let $t \in \mathbb{F}_q$ be a root of $f(x)$. Since $f(0) = c \neq 0$, we know $t \neq 0$ and thus the equation $f(t) = 0$ can be solved for b to obtain

$$b = -[t^3 + at^2 + c]/t = -[t^2 + at + c/t].$$

Since b is uniquely determined by t, any element of $\mathbb{F}_q$ is a root of at most one polynomial of $\mathscr{P}$. Define the mapping $\phi\colon \mathbb{F}_q^* \to \mathbb{F}_q$ by $\phi(t) = -[t^2 + at + c/t]$. Using this expression for b, we compute

$$\begin{aligned} -f(4) &= -[64 + 16a + 4b - (a+4)^2] \\ &= (a+4)^2 - 16a - 64 + 4[t^2 + at - (a+4)^2/t] \\ &= (t-4)[4t + 4(a+4) + (a+4)]^2/t \\ &= t(t-4)[4 + 4(a+4)/t + (a+4)^2/t^2] \\ &= t(t-4)[2 + (a+4)/t]^2. \end{aligned}$$

Thus we set $Q = \{t \mid t(t-4)[2 + (a+4)/t]^2 \in \not\square_q\}$, and observe that $\mathscr{P}_0 = \{f(x) = x^3 + ax^2 + \phi(t)\, x + c \mid t \in Q\}$. Moreover, we have that every polynomial of $\mathscr{P}_0$ looks like $f(x) = (x - t)[x^2 + (a+t)\, x - c/t]$. In order to determine the number of polynomials in $\mathscr{P}_0$ we need to look at all roots of $f(x)$, and hence the possible roots of $h_t(x) = x^2 + (a+t)\, x - c/t = x^2 + (a+t)\, x + (a+4)^2/t$. If $f(x) = (x-t)^3$, then we find $-2t = a + t$ and $t^2 = -c/t$, which imply $a^3 - 27c = a^3 + 27(a+4)^2 = 0$. Since $a^3 + 27(a+4)^2 = (a+3)(a+12)^2$, we have either $a = -3$, which we excluded, or $a = -12$. But the latter requires $t = 4$, whereas $4 \notin Q$. Hence $f(x)$ cannot have a root of multiplicity 3. Since $t \neq 0$ we can use the discriminant $\delta(t) = (a+t)^2\, t^2 + 4tc = (a+t)^2\, t^2 - 4t(a+4)^2$ of $t \cdot h_t(x)$ to sort out any additional roots. Toward that end we observe that $\delta(t) = t(t-4)[t^2 + (2a+4)\, t + (a+4)^2]$ and set $\delta_0(t) = t^2 + (2a+4)\, t + (a+4)^2$. Let $\gamma(t) = t(t-4)$, so that $\delta(t) = \gamma(t)\, \delta_0(t)$. Since $\gamma(t) \in \not\square_q$ for all $t \in Q$, it follows that the quadratic character of $\delta_0(t)$ is the opposite of that of $\delta(t)$ for all $t \in Q$. Note that t is the unique root of $f(x)$ if and only if $\delta(t) \in \not\square_q$. If $\delta(t) = 0$, then $f(x)$ has a double root since $h_t(x)$ has a double root. Let $f(x) = (x - t_1)(x - t_2)^2$ be such a polynomial. Then $\delta(t_1) = 0$, and t_1 must be one of at most 2 roots of $\delta_0(t)$. On the other hand, $\delta(t_2) \in \square_q$ since relative to this root $f(x)$ factors to leave $h_{t_2}(x) = (x - t_1)(x - t_2)$. Of course, if t is a root of an $f(x)$ with three distinct roots, then we also must have $\delta(t) \in \square_q$. Hence we claim that the number of reducible polynomials is given by

$$|\mathscr{P}_0| = \sum_{t \in Q} \tfrac{1}{3}[2 - \eta(\delta(t))] = \sum_{t \in Q} \tfrac{1}{3}[2 + \eta(\delta_0(t))].$$

Those $f(x)$ with a unique root get a value of $\frac{2+(1)}{3}=1$ from that root. Those $f(x)$ with three distinct roots get a value of $\frac{2+(-1)}{3}=\frac{1}{3}$ from each root, and hence a total of 1 as required. Finally, for $f(x)=(x-t_1)(x-t_2)^2$ the root t_1 contributes $\frac{2+0}{3}=\frac{2}{3}$ while the root t_2 contributes $\frac{2+(-1)}{3}=\frac{1}{3}$, and the total is again 1. In order to actually evaluate the sum we need to use the characteristic function for Q to convert to a sum over all of $\mathbb{F}_q$. But for $t\neq 0, 4$ or $-(a+4)/2$, we have $\eta(\gamma(t))=-1$ or 1 according as $t\in Q$ or $t\notin Q$, so the characteristic function for Q viewed as a subset of $\mathbb{F}_q\setminus\{0, 4, -\frac{a+4}{2}\}$ is just $\frac{1}{2}[1-\eta(\gamma(t))]$. Therefore we have shown that

$$\begin{aligned}|\mathscr{P}_0| &= \frac{1}{6}\sum_{t\in\mathbb{F}_q\setminus\{0,\,4,\,-(a+4)/2\}}[1-\eta(\gamma(t))][2+\eta(\delta_0(t))]\\ &=\frac{1}{6}\sum_{t\in\mathbb{F}_q}[1-\eta(\gamma(t))][2+\eta(\delta_0(t))]\\ &\quad-\frac{1}{6}\sum_{t\in\{0,\,4,\,-(a+4)/2\}}[1-\eta(\gamma(t))][2+\eta(\delta_0(t))].\end{aligned}$$

In order to evaluate the sum with range $\{0, 4, -\frac{a+4}{2}\}$ we compute that $\gamma(0)=\gamma(4)=0$, $\delta_0(0)=(a+4)^2$, $\delta_0(4)=(a+4)(a+12)$, and $\gamma(-\frac{a+4}{2})=\delta_0(-\frac{a+4}{2})=\frac{1}{4}(a+4)(a+12)$. Thus, if $a\neq -12$, the sum is $\frac{1}{6}[6]=1$. When $a=-12$, this sum has only two summands since $-\frac{a+4}{2}=4$ and becomes $\frac{1}{6}[5]=\frac{5}{6}$. Thus in either case the sum is given by the expression $\frac{1}{6}[5+\eta((a+12)^2)]$. Hence

$$\begin{aligned}|\mathscr{P}_0| &=\frac{1}{6}\sum_{t\in\mathbb{F}_q}[1-\eta(\gamma(t))][2+\eta(\delta_0(t))]-\frac{1}{6}[5+\eta((a+12)^2)]\\ &=\frac{q}{3}+\frac{1}{6}\sum_{t\in\mathbb{F}_q}[\eta(\delta_0(t))-2\eta(\gamma(t))-\eta(\delta(t))]-\frac{1}{6}[5+\eta((a+12)^2)].\end{aligned}$$

By Proposition 1 we have that $\sum\eta(\gamma(t))$ and $\sum\eta(\delta_0(t))$ are both -1. In the special case $a=-12$, we observe that $\delta(t)=t(t-4)^2\,(t-16)$. Again using Proposition 1 we have that $\sum\eta(\delta(t))=\sum\eta(t(t-16))-\eta(-48)=-1-\eta(-3)$. Substituting these values we obtain

$$|\mathscr{P}_0|=\begin{cases}\dfrac{q-2}{3}-\dfrac{1}{6}\left\{1+\sum_{t\in F_q}[\eta(\delta(t))]\right\} & \text{for}\quad a\neq -12\\[2ex] \dfrac{q-2}{3}+\dfrac{1}{6}\{1+\eta(-3)\} & \text{for}\quad a=-12\end{cases}.$$

By Theorem 3, since $\delta(t)$ has distinct roots for $a \neq -12$, we have $|1+\sum \eta(\delta(t))| \leqslant 2q^{1/2}$. Therefore, after noting that the case $a=-12$ clearly satisfies $|1+\eta(-3)| \leqslant 2q^{1/2}$, we conclude that

$$\tfrac{1}{3}(q-2-\sqrt{q}) \leqslant |\mathscr{P}_0| \leqslant \tfrac{1}{3}(q-2+\sqrt{q}).$$

Hence, we have that $|\mathscr{P}_0| < (q-1)/2$, and $\mathscr{P} \backslash \mathscr{P}_0 \neq \emptyset$. The bounds on $|\mathscr{P} \backslash \mathscr{P}_0|$ are just $\frac{q-1}{2} - \frac{1}{3}(q-2 \pm \sqrt{q}) = \frac{1}{6}(q+1 \pm 2\sqrt{q})$. The proof is complete. ∎

3. SELF-RECIPROCAL POLYNOMIALS

In this section we will exploit the connection between a self-reciprocal degree 6 polynomial $p(x)$ and a naturally related cubic polynomial $f(x)$, thereby allowing us to establish the existence results we seek. First we translate Lemma 4 to the exact form required.

LEMMA 5. *Let q be an odd prime power. Then for every $a' \in \mathbb{F}_q$, $a' \neq 2$ or 3, there exists $b' \in \mathbb{F}_q$ such that the polynomial $f(x) = x^3 + a'x^2 + b'x + (2b' + 4 - a'^2)$ is irreducible over $\mathbb{F}_q$ and $a'^2 - 4(a' + b' + 3) \in \not\square_q$. Indeed, the number of such b' lies between $\frac{1}{6}(q+1-2\sqrt{q})$ and $\frac{1}{6}(q+1+2\sqrt{q})$.*

Proof. Note that $f(x-2) = x^3 + (a'-6)\,x^2 + (b' - 4a' + 12)\,x - (a'-2)^2$. Let $a = a' - 6$, $b = b' - 4a' + 12$, and $c = -(a'-2)^2$. As $a' \neq 2$ or 3, we have $a = a' - 6 \neq -4$ or -3. Also $c = -(a+4)^2$, and $a'^2 - 4(a' + b' + 3) = -f(2) = -f(4-2)$. Thus, we may apply Lemma 4 to the polynomial $f(x-2)$ to get the desired result. ∎

The conditions of Lemma 5 that force $-f(2)$ and $-f(-2)$ to have opposite quadratic character are critical in showing the irreducibility of the associated degree 6 polynomial in the following lemma.

LEMMA 6. *Let q be an odd prime power. If $f(x) = x^3 + ax^2 + bx + (2b + 4 - a^2) \in \mathbb{F}_q[x]$ is irreducible over $\mathbb{F}_q$ and $a^2 - 4(a+b+3) \in \not\square_q$, then $p(x) = x^3 f(x + \frac{1}{x}) = x^6 + ax^5 + (3+b)\,x^4 + (2a + 2b + 4 - a^2)\,x^3 + (3+b)\,x^2 + ax + 1$ is a monic, self-reciprocal polynomial which is irreducible over $\mathbb{F}_q$. Moreover, there exists $u \in U = \{u \in \mathbb{F}_{q^6} \mid u^{q^2-q+1} = 1\}$ such that $p(x)$ is the minimal polynomial of u over $\mathbb{F}_q$*

Proof. Since $p(0)=1\neq 0$, any root u of $p(x)$ is nonzero and must have $u+\frac{1}{u}$ a root of $f(x)$. Thus $p(x)$ cannot have any roots in $\mathbb{F}_{q^2}$ as the roots of $f(x)$ lie in $\mathbb{F}_{q^3}\backslash\mathbb{F}_q$. Thus it suffices to show that $p(x)$ cannot factor as the product of two irreducible cubics in $\mathbb{F}_q[x]$. Suppose to the contrary that $r(x)=x^3+r_2x^2+r_1x+r_0\in\mathbb{F}_q[x]$ is an irreducible cubic which divides $p(x)$. Let u be a root of $r(x)$. Hence $u\in\mathbb{F}_{q^3}$ and u, u^q, u^{q^2} are the three distinct roots of $r(x)$. Since $p(x)$ is a self-reciprocal polynomial, it follows that u^{-1} also is a root of $p(x)$. If u^{-1} were u, u^q, or u^{q^2}, then $u^2=1$ as 2 is the gcd of q^3-1 and any one of $2, q+1$, or q^2+1. But this implies $u=\pm 1$, an obvious contradiction. Thus the reciprocal polynomial $r^*(x)=x^3r(\frac{1}{x})=r_0x^3+r_1x^2+r_2x+1$ of $r(x)$ must be its complementary factor, yielding the factorization $cp(x)=r(x)\,r^*(x)$ of an associate of $p(x)$. Evaluation of the identity at 0 shows $c=r_0$. Next evaluation at 1 yields $-r_0\cdot[a^2-4a-4b-12]=[r(1)]^2$ as $r^*(1)=r(1)$. Then evaluation at -1 yields $r_0(a-2)^2=-[r(-1)]^2$ since $r^*(-1)=-r(-1)$. If $a=2$, then $f(x)=(x+2)(x^2+b)$, contradicting the irreducibility of $f(x)$. Thus $(a-2)^2\in\square_q$, forcing $a^2-4(a+b+3)\in\square_q$, a contradiction. Therefore $p(x)$ is irreducible as claimed.

Let u be a root of $p(x)$. Since $p(x)$ is irreducible over $\mathbb{F}_q$, we have $u\in\mathbb{F}_{q^6}\backslash\mathbb{F}_{q^2}$. Again, since $p(x)$ is self-reciprocal, $\frac{1}{u}$ is also a root of $p(x)$. Hence u^{-1} is equal to one of $u, u^q, u^{q^2}, u^{q^3}, u^{q^4}, u^{q^5}$. Rewriting $u^{-1}=u^{q^i}$ as $u^{q^i+1}=1$, we see that the choices u, u^q, or u^{q^5} would imply that the order of u divides $q+1$, and hence $u\in\mathbb{F}_{q^2}$, a contradiction. Similarly the choices u^{q^2} or u^{q^4} are not possible since $u^{1+q^2+q^4}\in\mathbb{F}_{q^2}$ and hence either of these choices would force $u\in\mathbb{F}_{q^2}$. Thus we conclude that $u^{q^3+1}=1$.

Now, it can be easily verified that $a=-\mathrm{Tr}(u)$, $b=\mathrm{Tr}(u^{1+q})+\mathrm{Tr}(u^{1-q})$ and

$$2b+4-a^2=-\mathrm{Tr}(u^{1+q+q^2})-(u^{1-q+q^2}+u^{-1+q-q^2}). \tag{1}$$

Observe that $a^2=6+\mathrm{Tr}(u^2)+\mathrm{Tr}(u^{1+q})+\mathrm{Tr}(u^{1-q})+\mathrm{Tr}(u^{1+q^2})+\mathrm{Tr}(u^{1-q^2})$. Substituting a^2, a and b into Eq. (1), and noting that $\mathrm{Tr}(u^{1-q})=\mathrm{Tr}(u^{1+q^2})$ and $\mathrm{Tr}(u^{1+q})=\mathrm{Tr}(u^{1-q^2})$, we then get

$$v+v^{-1}+\mathrm{Tr}(u^{1+q+q^2})-2-\mathrm{Tr}(u^2)=0, \tag{2}$$

where $v=u^{1-q+q^2}$. Using the definition of v, we have $u^{1+q+q^2}=u^{1-q+q^2}u^{2q}=vu^{2q}$. Since $v^{q+1}=1$, we see that $\mathrm{Tr}(u^{1+q+q^2})=\mathrm{Tr}(v^{-1}u^2)$. Write $d=u^2+u^{2q^2}+u^{2q^4}$, so that $\mathrm{Tr}(v^{-1}u^2)=v^{-1}d+vd^q$. Hence, we obtain from Eq. (2) that

$$v+v^{-1}+v^{-1}d+vd^q-2-d-d^q=(v-1)[v(1+d^q)-(1+d)]/v=0.$$

If $v=1$, then $u\in U$ and we are done.

Suppose $v \neq 1$. Then $v(1+d^q)-(1+d)=0$. We will deduce a contradiction. Note that $\gcd(1+q, 1-q+q^2)=\gcd(3, 1+q)$. So if we let $3^e \parallel (1+q)$, then $e>0$ if and only if $q \equiv 2 \pmod 3$. Let

$$U' = \{x \in \mathbb{F}_{q^6} \mid x^{3^e(1-q+q^2)} = 1\} \qquad \text{and}$$
$$R = \{x \in \mathbb{F}_{q^6} \mid x^{(1+q)/3^e} = 1\}.$$

As $u^{1+q^3}=1$, there exist $t \in R$ and $y \in U'$ such that $u=ty$. Note that $v = u^{1-q+q^2} = t^3 s$ where s is an element such that $s^{3^e}=1$. In fact, $s=y^{1-q+q^2}$, and $s^{q+1}=1$. Hence, the equation $v(1+d^q)-(1+d)=0$ becomes $t^3 - s^{-1}d + t^3 d^q - s^{-1} = 0$. Let $w = s^{-1}y^2$. Now

$$\begin{aligned} d &= (ty)^2 + (ty)^{2q^2} + (ty)^{2q^4} \\ &= t^2(y^2 + y^{2q^2} + y^{2q^4}) \\ &= t^2 s(w + w^{q^2} + w^{q^4}). \end{aligned}$$

Moreover, as $y^{2(1-q+q^2)} = s^2$, $y^{2(1+q^2)} = s^2 y^{2q}$. we see that

$$\begin{aligned} d^q &= t^{-2}(y^{2q} + y^{2q^3} + y^{2q^5}) \\ &= t^{-2}s^{-2}(y^{2+2q^2} + y^{2+2q^4} + y^{2q^2+2q^4}) \\ &= t^{-2}(w^{1+q^2} + w^{1+q^4} + w^{q^2+q^4}). \end{aligned}$$

Finally,

$$w^{1+q^2+q^4} = s^{-3}y^{2+2q^2+2q^4} = s^{-3}(y^{1-q+q^2})^{2+2q+2q^2} = s^{-3}s^{2(1+q+q^2)} = s^{-1}.$$

Substituting d and d^q into the equation $t^3 - s^{-1}d + t^3 d^q - s^{-1} = 0$, we obtain

$$t^3 - t^2(w + w^{q^2} + w^{q^4}) + t(w^{1+q^2} + w^{1+q^4} + w^{q^2+q^4}) - w^{1+q^2+q^4} = 0. \tag{3}$$

Obviously, the only solutions for t satisfying Eq. (3) are w, w^{q^2} and w^{q^4}. Recalling that $w = s^{-1}y^2 = y^{1+q-q^2}$, $y \in U'$ and $t \in R$, straightforward gcd computations show that any of the above three choices for t yield $y=1$, $t=1$, and thus $u=ty=1$. This is a contradiction since $u \neq 1$. Therefore $v=1$ and $u \in U$. The proof is complete. ∎

4. THE TRACES

We now prove the main theorem on the traces of the (q^2-q+1)th roots of unity.

THEOREM 7. *Let q be an odd prime power. For any $s \in \mathbb{F}_q$, $s \neq -2$, or -3, there exists $u \in U = \{u \in \mathbb{F}_{q^6} \mid u^{q^2-q+1} = 1\}$ such that* $\mathrm{Tr}(u) = u + u^q + u^{q^2} + u^{q^3} + u^{q^4} + u^{q^5} = s$. *In fact,*

$$q + 1 - 2\sqrt{q} \leqslant |\{u \in U \mid \mathrm{Tr}(u) = s\}| \leqslant q + 1 + 2\sqrt{q}.$$

Proof. For $s \neq 6$, the inequalities come directly from Lemma 5 and Lemma 6. There are six u's for each of the $(q-1)/2 - |\mathscr{P}_0|$ irreducible polynomials. For $s = 6$ we must remember to add in the case of $u = 1$, but in this case the number of polynomials $p(x)$ is $\frac{1}{6}[q - \eta(-3)]$ (about the midpoint of the interval of values), and the result also holds here. ∎

The bounds on $|\{u \in U \mid \mathrm{Tr}(u) = s\}|$ found in Theorem 7 are known to be sharp for all small q in the following sense: For every integer N between $\frac{1}{6}(q + 1 - 2\sqrt{q})$ and $\frac{1}{6}(q + 1 + 2\sqrt{q})$ there exists an $a \neq 2, 3$ such that the number of polynomials $p(x)$ is exactly N. Hence with $s = -a$ we have $|\{u \mid u \neq 1, \mathrm{Tr}(u) = s\}| = 6N$. This has been verified with the computational software package MAGMA [4] for all odd prime powers $q \leqslant 100$.

5. CONCLUSION

In the discussion after Theorem 4.2 in [3] it is shown that $-2 \in \mathbb{F}_q \setminus \{\mathrm{Tr}(u) \mid u \in U\}$ for all odd prime powers q, and $-3 \in \mathbb{F}_q \setminus \{\mathrm{Tr}(u) \mid u \in U\}$ if $q \equiv 1 \pmod 3$. Moreover, $\mathrm{Tr}(1) = 6 = -3$ if $q \equiv 0 \pmod 3$, while $\mathrm{Tr}(u) = -3$ for any primitive cube root of unity $u \in U$ when $q \equiv 2 \pmod 3$. To see the latter fact, simply observe that $u^{q^3} + u = u^{-1} + u = u^2 + u = -1$ if $o(u) = 3$, and such elements u exist in U precisely when $q \equiv 2 \pmod 3$. Thus Theorem 7 shows that the conjecture stated in [3] is true, and hence all odd order three-dimensional flag-transitive affine planes of type C are known (see Theorem 5.1 of [3]). In particular, if the order of such planes is q^3, where q is an odd prime, then the number of isomorphism classes is precisely $\frac{1}{2}(q-1)$, the same as the number of two-dimensional flag-transitive affine planes of type H with order q^2 for odd primes q. It should be noted that in the three-dimensional case there are known examples of odd order planes of type H and even order planes of type C, but enumerating these planes would require different techniques.

REFERENCES

1. R. D. Baker and G. L. Ebert, Two-dimensional flag-transitive planes revisited, *Geom. Dedicata* **63** (1996), 1–15.
2. R. D. Baker, J. Dover, G. L. Ebert, and K. Wantz, Baer subgeometry partitions, *J. Geom.* **67** (2000), 23–34.

3. R. D. Baker, J. Dover, G. L. Ebert, and K. Wantz, Perfect Baer subplane partitions and three-dimensional flag-transitive planes, *Des. Codes Cryptogr.* **21** (2000), 19–39.
4. J. Cannon and C. Playoust, “An Introduction to MAGMA,” Univ. of Sydney, Sydney, Australia, 1993.
5. G. L. Ebert, Partitioning problems and flag-transitive planes, *Rend. Circ. Mat. Palermo Ser. II Suppl.* **53** (1998), 27–44.
6. H. Hasse, Zur Theorie der abstrakte elliptischen Funktionenkörper. II. Automorphismen und Meromorphismen. Das Additionstheorem, *J. Reine Angrew. Math.* **175** (1936), 69–88.
7. H. Hasse, Zur Theorie der abstrakte elliptischen Funktionenkörper. III. Struktur des Meromorphismenringes. Die Riemannsche Vermutung, *J. Reine Angew. Math.* **175** (1936), 193–208.
8. W. M. Schmidt, “Equations over Finite Fields, An Elementary Approach,” Lecture Notes in Mathematics, Vol. 536, Springer-Verlag, Berlin/New York, 1976.