Subplanes of order 3 in Hughes Planes

Cafer Caliskan
Department of Mathematical Sciences
Florida Atlantic University,
Boca Raton, FL 33431, U.S.A.
caliska@fau.edu

G. Eric Moorhouse
Department of Mathematics
University of Wyoming,
Laramie, WY 82071, U.S.A.
moorhous@uwyo.edu

To Prof. Spyros Magliveras on his 70th birthday

Abstract
In this study we show the existence of subplanes of order 3 in
Hughes planes of order $q^2$, where $q$ is a prime power and $q \equiv 5 \pmod{6}$. We further show that there exist finite partial linear spaces which
cannot embed in any Hughes plane.

1 Introduction

L. Puccio and M. J. de Resmini [5] showed that subplanes of order 3 exist
in the Hughes plane of order 25. (We refer always to the ordinary Hughes planes; equivalently, all our nearfields are regular.) Computations of the
second author [2] show that among the known projective planes of order 25
(including 99 planes up to isomorphism/duality), exactly four have sub-
planes of order 3. These four planes are the ordinary Hughes plane and
three closely related planes. Recently, Caliskan and Magliveras [1] showed
that there are exactly 2 orbits on subplanes of order 3 in the Hughes plane
of order 121. In this study we show that every Hughes plane of order $q^2$,
where $q$ is a prime power and $q \equiv 5 \pmod{6}$, has subplanes of order 3.
We begin with the construction of the Hughes plane $H(q^2)$ of order $q^2$, $q$ an odd prime power, as given by Rosati [6] and Zappa [9]. Throughout this paper, $K$ denotes a finite field of order $q^2$, and $F$ its subfield of order $q$, where $q$ is an odd prime power. For any $\theta \in K$ with $\theta \notin F$, we have $K = F[\theta]$ and $\{1, \theta\}$ is a basis for $K$ over $F$. We will always choose $\theta$ such that $\theta^2 = d \in F$, where $d$ is a nonsquare in $F$. We now define the regular nearfield $N$ of order $q^2$, where $N$ has the same elements as $K$ and the same addition. However, multiplication in $N$ is defined as follows: $a \circ b = ab$ if $a$ is a square in $K$, and $a \circ b = ab^\theta$ otherwise. Let $V = \{(x, y, z) \mid x, y, z \in N\}$ be the 3-dimensional left vector space over $N$. Define the set of points (set of lines) of $H(q^2)$ to be the set of all equivalence classes of elements of $V \setminus \{(0, 0, 0)\}$, under the equivalence $(x, y, z) \sim (k \circ x, k \circ y, k \circ z)$ for $k \in N^*$. We may take $\{1, \theta\}$ as a basis for $N$ as a vector space over $F$. The incidence relation for $H(q^2)$ is defined as follows: Point $(x, y, z)$ is incident with line $[a, b, c]$, where $a = a_1 + a_2\theta$, $b = b_1 + b_2\theta$, and $c = c_1 + c_2\theta$, if and only if $xa_1 + yb_1 + zb_1 + (xa_2 + yb_2 + zb_2) \circ \theta = 0$. It is well known that different choices of $\theta$ give isomorphic planes of order $q^2$.

In order to implement nearfield multiplication in $N$, the following is useful for readily identifying squares in $K$.

**Lemma 1.1** Consider a quadratic extension $K = F[\theta] \supset F$ where $F$ is a field of odd order $q$, and $\theta^2 = d \in F$. A typical element $x = a + b\theta$ (where $a, b \in F$) is a square in $K$, iff its norm $x^{q+1} = a^2 - db^2$ is a square in $F$.

Proof: We may assume $x \neq 0$. The element $x \in K$ is a square in $K$ iff $x^{(q^2-1)/2} = 1$ iff $(x^{q+1})^{(q-1)/2} = 1$, iff the element $x^{q+1} \in F$ is a square in $F$. Note that $x^{q+1} = x^2x = (a - b\theta)(a + b\theta) = a^2 - db^2$. \qed

It has long been recognized by M. J. de Resmini and others that Hughes planes have subplanes of order 2; for completeness we include a proof of this fact in Section 2. On the other hand, this is not totally surprising since for a quadrilateral to generate a subplane of order 2 only requires a single algebraic condition to hold. In order for a quadrilateral to generate a subplane of order 3, several inequivalent conditions must hold. We show the existence of subplanes of order 3 in the Hughes plane $H(q^2)$ in Section 3 in case $q \equiv 5 \pmod{12}$, and in Section 4 in case $q \equiv 11 \pmod{12}$.

2 Subplanes of order 2

We require the following technical lemma.
Lemma 2.1 Let $F$ be a finite field of odd order $q$, and let $d \in F$ be a nonsquare.

(a) If $q \equiv 1 \pmod{4}$ then there exists a nonzero element $b \in F$ such that $b^4 + db^2 + d^2$ is a nonsquare in $F$.

(b) If $q \equiv 3 \pmod{4}$ then there exist $(q+1)/2$ nonzero values of $b \in F$ such that $b^2 + 1$ is a nonsquare in $F$.

Proof: (a) The equation $x^2 + dxz + d^2z^2 = dy^2$ defines a nondegenerate conic in the classical projective plane coordinatized by $F$, with homogeneous coordinates $(x, y, z)$. Since $d$ is a nonsquare in $F$, all $q+1$ points of this conic must have $xz \neq 0$ and so all points of the conic have the form $(x, y, 1)$ with $x \neq 0$. No more than two such points share the same $x$-coordinate, so the points $(x, y, 1)$ of the conic have at least $(q+1)/2$ distinct nonzero $x$-coordinates. Since $F$ contains only $(q-1)/2$ nonsquares, the conic must contain a point of the form $(b^2, y, 1)$ with $b \neq 0$.

(b) The equation $x^2 + y^2 + z^2 = 0$ defines a nondegenerate conic in the classical projective plane coordinatized by $F$. Since $-1$ is a nonsquare in $F$, all $q+1$ points of the conic have the form $(x, 1, z)$ in homogeneous coordinates with $xz \neq 0$. No more than two such points $(x, 1, \pm z)$ share the same $x$-coordinate, yielding $(q+1)/2$ values of $x$ for which $x^2 + 1$ equals a nonsquare $-z^2$.

Theorem 2.2 Every Hughes plane has a subplane of order 2.

Proof: Let $d$ be a nonsquare in $F$, so that $K = F[\theta]$ where $\theta \in K$ satisfies $\theta^2 = d$. We consider two cases.

Suppose first that $q \equiv 1 \pmod{4}$. In this case $-1$ is a square in $F$, and $\theta$ is a nonsquare in $K$ since its norm $\theta^q \theta = (-\theta)\theta = -d$ is a nonsquare in $F$. Choose $b \in F$ such that $b^4 + db^2 + d^2$ is a nonsquare in $F$ as in Lemma 2.1(a). Write $c = (b/d) + (1/b) \in F$, so that $1 \pm c\theta$ is a nonsquare in $K$ by Lemma 1.1. The seven points $p_0, p_1, \ldots, p_6$ of the Hughes plane with coordinates

$$(1, 0, 0), (0, 1, 0), (1, -d/b, \theta), (1, \theta, b), (1/b, -(b/d)\theta, 1), (1, b+\theta, 0), (1, b, \theta)$$

and the seven lines $\ell_0, \ell_1, \ldots, \ell_6$ with coordinates

$$[0, \theta, -b], [0, 0, 1], [\theta, 0, -1], [0, -b, \theta], [-b, 0, 1], [-b-\theta, 1, 1+c\theta], [-b-\theta, 1, 1]$$

satisfy $p_i \in \ell_j$ iff $j - i \in \{0, 1, 3\}$ mod 7. This gives a subplane of order 2 in the Hughes plane of order $q^2$. 

\qed
Now suppose that $q \equiv 3 \mod 4$. In this case we may take $d = -1$, a nonsquare in $F$, and $\theta$ is a square in $K$ since its norm $\theta^{q+1} = -d = 1$ is a square in $F$. By Lemma 2.1(b), there exists $b \in F$ such that $b^2 + 1$ is a nonsquare in $F$. By Lemma 1.1, the elements $1 \pm b\theta$ and $b \pm \theta$ are nonsquares in $K$. The seven points of the Hughes plane

$$(1, 0, 0), (0, 1, 0), (0, 0, 1), (1, \theta, 0), (0, 1, 1 - b\theta), (1, \theta, b + \theta), (1, 0, b + \theta)$$

and the seven lines

$$[0, 0, 1], [1, 0, 0], [1, \theta, 0], [-b - \theta, -1 + b\theta, 1], [0, -1 + b\theta, 1], [-b - \theta, 0, 1], [0, 1, 0]$$

give a subplane of order 2, where as before we have $p_i \in \ell_j$ iff $j - i \in \{0, 1, 3\}$ mod 7.

### 3 Case: $q \equiv 5 \mod 12$

Let $q \equiv 5 \mod 12$. We may take $d = -3$, a nonsquare in $F$, and $K = F[\theta]$ where $\theta^2 = -3$. There is an element $i \in F$ satisfying $i^2 = -1$, since $q \equiv 1 \mod 4$. Also $\omega = (-1 + i\theta)/2 \in K$ is a primitive cube root of unity, and the other is $\omega^2 = (-1 - i\theta)/2$. Furthermore, $\zeta = i\omega = (-i + i\theta)/2 \in K$ is a primitive 12-th root of unity. We compute that $\zeta^2 = (1 + \theta)/2$, $\zeta^4 = \omega = (-1 + \theta)/2$, and $\zeta^5 = i\omega^2 = (-i - i\theta)/2$. Moreover, $\zeta + \zeta^7 = \zeta^2 + \zeta^8 = \zeta^4 + \zeta^{10} = \zeta^5 + \zeta^{11} = 0$, since $\zeta^6 = -1$. Hence, $\zeta^7 = (i - i\theta)/2$, $\zeta^8 = (-1 - \theta)/2$, $\zeta^{10} = (1 - \theta)/2$, and $\zeta^{11} = (i + i\theta)/2$. The following Lemma follows easily from Lemma 1.1.

**Lemma 3.1** $1 \pm \theta$ are squares and $\theta$, $3 \pm \theta$ not squares in $K$.

We now define $\alpha$, a set of 13 points, and $\beta$, a set of 13 lines, as follows:
Theorem 3.2 Let \( q \) be a prime power, \( q \equiv 5 \pmod{12} \). Then \( \alpha \) is the set of points, and \( \beta \) the set of lines, of a subplane of order 3 in the Hughes plane \( H(q^2) \). This subplane is invariant under the polarity \((x, y, z) \leftrightarrow [x^q, y^q, z^q]\) of \( H(q^2) \).

Proof: It is known that all elements of \( F \) are squares in \( K \). We use the Lemma 3.1 and the incidence relation described by Rosati [6] to determine whether \( p_i \) and \( \ell_j \) are incident for each pair of a point \( p_i, 1 \leq i \leq 13 \), in \( \alpha \) and a line \( \ell_j, 1 \leq j \leq 13 \), in \( \beta \). This gives rise to the following incidence matrix \( M \):

\[
M = \begin{bmatrix}
0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0
\end{bmatrix}
\]

An easy computation shows that \( MM^T = J_{13} + 3I_{13} \), where \( J_{13} \) denotes the 13 \( \times \) 13 matrix in which every entry is a “1” and \( I_{13} \) the 13 \( \times \) 13 identity matrix.
By Rosati [7], the map \((x, y, z) \mapsto [x^q, y^q, z^q]\) is a polarity of \(H(q^2)\). One easily checks that this map interchanges \(\alpha\) and \(\beta\). This completes the proof of Theorem 3.2.

\[\square\]

4 Case: \(q \equiv 11 \pmod{12}\)

Let us now assume that \(q \equiv 11 \pmod{12}\), so that both \(-1\) and \(-3\) are nonsquares in \(\mathbb{F}\), and in particular \(3\) is a square in \(\mathbb{F}\).

Lemma 4.1 There exists \(c \in \mathbb{F}\) such that \(c^2 - c + 1\) is a nonsquare in \(\mathbb{F}\).

Proof: By the Chevalley-Warning Theorem [8, p.5], there exist \(a, b, c \in \mathbb{F}\), not all zero, such that \(c^2 - bc + b^2 + a^2 = 0\). Clearly \(b \neq 0\), so \((c/b)^2 - (c/b) + 1 = -(a/b)^2\), a nonsquare in \(\mathbb{F}\).

Fixing \(c \in \mathbb{F}\) as in Lemma 4.1, we readily obtain the following from the Lemma 1.1.

Lemma 4.2 The elements \(\theta, 1 \pm \theta\) and \(3 \pm \theta\) are squares in \(K\). The elements \(c - 2 \pm c \theta, c + 1 \pm (c - 1) \theta\) and \(2c - 1 \pm \theta\) are nonsquares in \(K\).

We shall use Lemma 4.2 along with the fact that \(c \notin \{0, 1\}\). Now we define \(\alpha'\), a set of 13 points, and \(\beta'\), a set of 13 lines, as follows:

\[
\begin{align*}
\alpha' : & \quad p_1 (1, \omega, \omega^2) & \quad \ell_1 [1, \omega, \omega^2] \\
& \quad p_2 (1, 0, -\omega) & \quad \ell_2 [0, -\omega, 1] \\
& \quad p_3 (-\omega, 1, 0) & \quad \ell_3 [1, 0, -\omega] \\
& \quad p_4 (0, -\omega, 1) & \quad \ell_4 [-\omega, 1, 0] \\
& \quad p_5 (1/(c - 1), \omega, \omega^2) & \quad \ell_5 [\omega^2, c/(1 - c), \omega] \\
& \quad p_6 (-c, \omega, \omega^2) & \quad \ell_6 [\omega^2, c - 1, \omega] \\
& \quad p_7 ((1 - c)/c, \omega, \omega^2) & \quad \ell_7 [\omega^2, -1/c, \omega] \\
& \quad p_8 (\omega^2, (1 - c)/c, \omega) & \quad \ell_8 [\omega, \omega^2, c/(1 - c)] \\
& \quad p_9 (\omega^2, 1/(c - 1), \omega) & \quad \ell_9 [\omega, \omega^2, c - 1] \\
& \quad p_{10} (\omega^2, -c, \omega) & \quad \ell_{10} [\omega, \omega^2, -1/c] \\
& \quad p_{11} (\omega, \omega^2, 1/(c - 1)) & \quad \ell_{11} [c - 1, \omega, \omega^2] \\
& \quad p_{12} (\omega, \omega^2, -c) & \quad \ell_{12} [-1/c, \omega, \omega^2] \\
& \quad p_{13} (\omega, \omega^2, (1 - c)/c) & \quad \ell_{13} [c/(1 - c), \omega, \omega^2]
\end{align*}
\]

Theorem 4.3 Let \(q\) be a prime power, \(q \equiv 11 \pmod{12}\). Then \(\alpha'\) is the set of points, and \(\beta'\) the set of lines, of a subplane of order 3 in the Hughes plane \(H(q^2)\).
Proof: By Lemma 4.1 and 4.2, our computation gives rise to the following
incidence matrix $M'$, where $M'M^T = J_{13} + 3I_{13}$. This proves Theorem
4.3.

\[
M' = \begin{pmatrix}
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0
\end{pmatrix}
\]

\[
\]

5 Further Substructures of Hughes Planes

No subplanes of order 3 have ever been found in Hughes planes of order $q^2$ for $q \equiv 1 \pmod{6}$; and computational evidence for small values of $q$ suggests that subplanes of order 3 do not occur in this case. It is also
an open problem whether there exists a Hughes plane with a subplane of
order 4. However, the following argument, first used in [3], shows that there
exist finite partial linear spaces which cannot embed in any Hughes plane.

First, some terminology: Let $L$ be a finite partial linear space (a point-
line incidence structure, in which every line has at least two points, and
any two distinct points lie on at most one line of $L$). As before, we denote
by $H(q^2)$ a Hughes plane of order $q^2$. We say that $f : L \to H(q^2)$ is an embedding if $f$ injectively maps points of $L$ to points of $H(q^2)$, and $f$
injectively maps lines of $L$ to lines of $H(q^2)$, such that $f(P)$ lies on $f(\ell)$ (in $H(q^2)$) if and only if the point $P$ lies on the line $\ell$ (in $L$). (Replacing “if
and only if” by “if” in the latter definition, does not change the essential
difficulty of the embedding problem, or the validity of Theorem 5.1 below;
see [3, Lemma 1].) In this language, our main result (above) is that the
projective plane of order 3 embeds in $H(q^2)$ whenever $q \equiv 5 \pmod{6}$.

**Theorem 5.1** There exists a finite partial linear space which does not em-
bed in any Hughes plane.

Proof: Let $L_0$ be a finite partial linear space which does not embed in any
Desarguesian plane of odd order. (We may take $L_0$ to be a projective plane of order 2, or a configuration violating Desargues' Theorem.) Let $\Gamma_0$ be the incidence graph of $L_0$, i.e. the graph whose vertices correspond to points and lines of $L_0$; and whose edges correspond to incident point-line pairs of $L_0$. Thus $\Gamma_0$ is a bipartite graph with no 4-cycle. By [4, Theorem 6.3] (see also [3, Lemma 2]), there exists a bipartite graph $\Gamma$ having no 4-cycle, such that for every 2-coloring of the edges of $\Gamma$, there exists a subgraph isomorphic to $\Gamma_0$, all of whose edges have the same color. We may regard $\Gamma$ as the point-line incidence graph of a partial linear space $L$.

Suppose that $q$ is an odd prime power and that $f : L \to H(q^2)$ is an embedding. For each point $P_i$ and line $\ell_j$ of $L$, denote $f(P_i) = (x_i, y_i, z_i)$ and $f(\ell_j) = [a_j, b_j, c_j]$. (We have chosen arbitrary but fixed nonzero vectors in $N^3$ representing $f(P_i)$ and $f(\ell_j)$. The ambiguity in the choice of coordinates may be resolved by first using nonzero elements of $K$ over $F$ to scale all vectors so their first nonzero coordinate is 1.) Now write

$$(a_j, b_j, c_j) = (a_{j1} + a_{j2}\theta, b_{j1} + b_{j2}\theta, c_{j1} + c_{j2}\theta), \quad (a_{jk}, b_{jk}, c_{jk}) \in F^3$$

for all $j, k$, where $\{1, \theta\}$ is a fixed basis for $K$ over $F$.

Assuming $P_i \in \ell_j$, we color the incident point-line pair $(P_i, \ell_j)$ red or blue according as $a_{j2}x_i + b_{j2}y_i + c_{j2}z_i \in K$ is a square or a nonsquare.

Case 1: $\Gamma$ has a subgraph isomorphic to $\Gamma_0$, all of whose edges are red. In this case the map

$$P_i \mapsto (x_i, y_i, z_i), \quad \ell_j \mapsto (a_j, b_j, c_j)$$

restricts to an embedding of $\Gamma_0$ in a Desarguesian plane of order $q^2$, since

$$a_jx_i + b_jy_i + c_jz_i = (a_{j1}x_i + b_{j1}y_i + c_{j1}z_i) + (a_{j2}x_i + b_{j2}y_i + c_{j2}z_i) \circ \theta = 0$$

for every red incident point-line pair $P_i \in \ell_j$. This contradicts the choice of $\Gamma_0$.

Case 2: $\Gamma$ has a subgraph isomorphic to $\Gamma_0$, all of whose edges are blue. In this case the map

$$P_i \mapsto (x_i, y_i, z_i), \quad \ell_j \mapsto (a_j^\theta, b_j^\theta, c_j^\theta)$$

restricts to an embedding of $\Gamma_0$ in a Desarguesian plane of order $q^2$, since

$$a_j^\theta x_i + b_j^\theta y_i + c_j^\theta z_i = (a_{j1}x_i + b_{j1}y_i + c_{j1}z_i) + (a_{j2}x_i + b_{j2}y_i + c_{j2}z_i) \circ \theta = 0$$

for every blue incident point-line pair $P_i \in \ell_j$. Again, this contradicts the choice of $\Gamma_0$. \qed
The proof of Theorem 5.1 reveals a straightforward strategy for trying to embed a given finite partial linear space $L$ (such as a finite projective plane) in a Hughes plane $H(q^2)$: Choose an appropriate 2-coloring of the incident point-line pairs of $L$ (i.e. the edges of its incidence graph $\Gamma$), such that both of the resulting monochromatic subgraphs of $\Gamma$ correspond to partial linear spaces embeddable in a Desarguesian plane of order $q^2$. Unfortunately there are exponentially many 2-colorings of the edges of $\Gamma$ to consider; and even for a projective plane of order 4, with 105 incident point-line pairs, this seems a daunting task. On the other hand, it is easy to 2-color these 105 incident point-line pairs without rendering any monochromatic subplane of order 2; so the argument of Theorem 5.1 seems ineffective in ruling out subplanes of order 4 in Hughes planes.

Acknowledgments

We are grateful to the referee for catching errors in the original submitted version of this work. The first author would also like to thank Professor Tim Penttila for his valuable suggestions and Professor Paul Yiu for his contributions in Field Theory.

References


