Note di Matematica
Note Mat. 29 (2009), suppl. n. 1, 45-59
ISSN 1123-2536, e-ISSN 1590-0932
DOI 10.1285/i15900932v29n1supplp45
http://siba-ese.unisalento.it, © 2009 Università del Salento

On the Multiplicative Structure of Quasifields and Semifields: Cyclic and Acyclic Loops

M. Cordero [i]
Dept. of Mathematics
Univ. of Texas at Arlington
Arlington, TX, 76019
cordero@uta.edu
http://www2.uta.edu/math/cordero

V. Jha
Dept. of Mathematics
Univ. of Texas at Arlington
Arlington, TX, 76019
vjha267@googlemail.com

Abstract. This note is concerned with the multiplicative loop L of a finite quasifield or semifield, and the associated geometry. It investigates when the principal powers of some element of the multiplicative loop L ranges over the whole loop: in this situation the loop L is *cyclic* (or *primitive*) and is *acyclic* otherwise. A conjecture of Wene essentially asserts that a finite semifield cannot be acyclic. No counterexamples to the Wene conjecture are known for semifields of order > 32; in fact, in many situations the Wene conjecture is known to hold, as established in various papers by Wene, Rúa and Hamilton. The primary aim of this note is to show that, in contrast to the above situation, there exists at least one acyclic *quasifield* for every square prime power order $p^{2r} > 4$. Additionally, we include a simple conceptual proof of a theorem of Rúa, that establishes the primitivity of three-dimensional semifields.

Keywords: loops, quasifields, semifields, derivation

MSC 2000 classification: Primary: 51A40; Secondary: 17A35

1 Introduction

Let $(X, \circ)$ be a loop with identity e. The (right) *principal powers* of an element $x \in X$ are the elements of X that are of the form $x^{n)}$, for arbitrary integer $n \geq 0$, where $x^{n)}$ is defined recursively by the conditions $x^{0)} = e, x^{n+1)} = x^{n)} \circ x$. An element $x_0 \in X$ is (right) *cyclic* if the (right) principal powers of x_0 cover X; thus x_0 is *cyclic* if $X = \{e \circ x_0^{k)} : k \in \mathcal{N}\}$. A loop $(X, \circ)$ is right *cyclic* (or (right) *primitive*) if it has at least one (right) cyclic element; otherwise the

[i]This work was done when the second author was a visiting professor at the University of Texas at Arlington. He would like to express his gratitude to the Mathematics Department for their hospitality, and especially to Professor Jianping Zhu for making this visit possible.

loop is (right) *acyclic*. The analogous 'left' concepts are easily defined, starting with left principal powers $x^{(0} = e, x^{(n+1} = x^{(n} \circ x$.

Cyclic (non-associative) loops are analogues of cyclic groups defined in terms of the principal powers associated with loop multiplication. We usually restrict ourselves to *right* principal powers and related notions such as (right) cyclic loops. All our results turn out to be valid for the analogous concept arising from the corresponding notion of left principal powers. Except when special emphasis is desirable, e.g. when relating our results to existing results, we usually drop the laborious 'left/right' prefix.

In this paper we are generally concerned with the multiplicative loops of quasifields, the planar ternary rings that coordinatize finite translation planes. Thus, according to the coordinatization scheme used, the quasifields satisfy at least one distributive law[1].

1 Definition. Let $(Q, +, \circ)$ be a quasifield. Then Q is *cyclic* or *acyclic* according to whether its multiplicative loop $(Q^*, \circ)$ is cyclic or acyclic. If Q is a distributive quasifield, or a *semifield*, then Q is considered a *primitive* or an *imprimitive* semifield according to whether or not it is cyclic or acyclic.

1 Notes. (1) This definition, and similar ones ahead, could be made for the multiplicative loops of arbitrary planar ternary rings, coordinatizing arbitrary projective and affine planes. However, we have not investigated the general situation.

(2) We depart from Wene's convention, by using 'cyclic' instead of 'primitive', to emphasize the difference between the semifield and the (strict) quasifield case, and to avoid a misreading of the Wene conjecture below, which is concerned with semifields only.

Wene conjectured, [12, 13], that every finite semifield is (right) primitive. Since finite fields have cyclic multiplicative groups, this conjecture holds for them. Rúa, [5], showed that one of the Knuth semifields of order 32 yields a counterexample to the Wene conjecture. However, a fairly intensive computer-based investigation by Rúa and Henzel, [3], has not yielded any further counterexamples to the Wene conjecture for semifields of order > 32.

Thus, perhaps one ought to interpret the Wene conjecture as asking for a description of the semifields that are imprimitive (i.e. with acyclic loops). A first step in this direction, and also of independent interest, is to consider the following broader question.

[1]The left or right distributive law assumed for quasifields are never required to synchronize with the type of principal powers adopted (left or right) used in describing the multiplicative loop of the quasifield.

2 Problem. Find the parameters (p, r), $r > 1$ and p prime, such that there is some quasifield of order p^r with an acyclic multiplicative loop.

In this paper we shall adopt this view of Wene's conjecture, or rather its negation. Hence, we seek a description of the parameters of the finite translation planes coordinatizable with quasifields with acyclic multiplicative loops: the Wene conjecture asserts that semifields of order > 32 satisfying these conditions do not exist. One of the main aims of this paper is to consider the putative ubiquity of acyclic loops that are the multiplicative loops of finite quasifields. However, in order to stress that the results on the ubiquity problem in this paper are all related to *strict* quasifields, rather than to *semifields* as in the original Wene conjecture, we split Problem 2 into two parts:

3 Problem (Loop-Ubiquity)**.** Let p be any prime, and $r > 0$ an integer.

(1) Find the parameters (p, r) such that there exists an acyclic quasifield of order p^r.

(2) Find all parameters (p, r) such that there exists an acyclic semifield (= imprimitive in Wene's terminology) of order p^r.

Notice that (2) above asks for a description to all counterexamples to the Wene conjecture, and (1) asks for a description of the counterexamples 'to Wene' among the class of finite quasifields.

There is a related combinatorial/geometric problem which we formulate in terms of a *covering* of an affine or projective plane. We arbitrarily restrict our definition to affine translation planes.

4 Definition. Let π be a finite affine translation plane with a proper subaffine plane π_0. Then a *covering* of π *over* π_0, is a collection of proper subaffine planes, $\mathcal{P} = \{\pi_i : i \in I\}$ of π, such that every π_i in $\mathcal{P}$ contains π_0 and every point of π lies in some $\pi_i \in \mathcal{P}$. The plane π admits a *cover* or *covering* if it admits a covering relative to some proper subplane.

It will be evident that the quasifields Q coordinatizing such geometrically-covered π, based on axes selected in π_0, are always acyclic. We introduce the related terminology.

5 Definition. Let Q be a finite quasifield with a collection of *proper* subquasifields $\mathcal{Q} := \{Q_i : 1 \leq i \leq n\}$ such that $Q = \cup\mathcal{Q}$. Then $\mathcal{Q}$ is a *covering* of Q, and Q is a quasifield admitting a *covering*, or Q is a *covered* quasifield.

Since every quasifield in $\mathcal{Q}$ is closed under multiplication, we have

6 Remark. A quasifield Q with a covering is acyclic, in the strong sense, i.e. each element $a \in Q$ is neither left-primitive nor right-primitive.

The essential equivalence between translation planes with coverings and quasifields admitting coverings immediately yield:

7 Remark. The following are mutually equivalent conditions for an affine translation plane π.

(1) π admits a geometric cover.

(2) π admits a geometric cover relative to a subplane π_0.

(3) π may be coordinatized by a quasifield with a covering.

(4) π contains a subplane π_0 such that every quasifield coordinatizing π with axes in π_0 is a covered quasifield.

(5) π contains a subplane π_0 such that some quasifield coordinatizing π with axes in π_0 is a covered quasifield.

Proof. The only point worth noting is that all the quasifields in a cover $\mathcal{Q}$ of a quasifield Q share a common sub-quasifield, e.g., the prime sub-quasifield Q_0; hence the corresponding affine subplanes associated with the quasifields in $\mathcal{Q}$ form a geometric cover of $\pi(Q)$ relative to $\pi(Q_0)$. The other remarks follow easily. QED

We note that a Desarguesian plane cannot admit a covering since that would imply the plane is coordinatizable by a Galois field which is a union of proper fields. More generally, in view of Remark 6 and Remark 7, we have

8 Remark. Any finite translation plane that admits a geometric cover, or is coordinatizable by a covered quasifield, is acyclic with no right-primitive or left-primitive elements. In particular, the covered quasifield itself is acyclic with no element being right-primitive or left-primitive.

In particular, if π were a semifield plane, and π_0 a sub-semifield plane, we would obtain an imprimitive semifield, contrary to the Wene conjecture. This specialization of Remark 7 is recorded below:

9 Remark. Suppose a semifield plane π of order p^r admits a covering by a collection of subplanes $(\pi_i)_{i\in I}$, any two intersecting a proper subplane π_0 that contains the shears point. Then any semifield D coordinatizing π, when the axes are chosen in π_0, is both left imprimitive and right imprimitive.

So translation planes π of order p^r with coverings contribute parameters (p, r) satisfying the condition of Problem 3.1, and also those of Problem 3.2 if π is a semifield plane and π_0 a sub-semifield plane.

10 Problem (Plane Cover)**.** Let p be any prime, and $r > 0$ an integer.

(1) Find the parameters (p, r) such that there exists a translation plane π of order p^r that admits a cover relative to some subplane π_0.

(2) Find the parameters (p, r) such that there exists a semifield plane π of order p^r that admits a cover relative to some subplane π_0.

We note that the parameters (p, r) associated with the cover problem, Problem 10, also satisfy the requirements for the loop-ubiquity problem, Problem 3. However, the converse is false quite often, as we note in Section 2.

The main result of the paper classifies the square prime powers $n = p^{2r}$ such that at least one translation plane of order n admits a geometric cover, cf. Theorem 23.

Theorem A. *There exists a translation plane of square order $n = p^{2r}$ with a geometric cover iff the integer $r > 1$.*

As an immediate corollary we note that for any square order q^2 a left acyclic and a right acyclic quasifield both exist, cf. Corollary 24:

Corollary B. An acyclic right (left) quasifield of square order q^2 exists iff $q > 4$.

Before turning to the proof of Theorem A, which deals only with the square order situation, we briefly consider acyclic quasifields of non-square order. There are many of these, as easily seen by considering nearfields, but we do not have enough for 'complete ubiquity' in this situation: that is, there are infinitely many parameters p^r, r odd, for which we do not know whether or not acyclic quasifields exist. The case of the nearfields also shows that there are many parameters p^r for which no geometric covers exist, yet acyclic quasifields do exist.

We end by providing a new conceptual proof of Rúa's Theorem that asserts that all semifields of order q^3 with center (containing) $GF(q)$ are cyclic. Rúa's Theorem is a generalization of Wene's Theorem which proved the same result under the stronger assumption that the semifield is commutative. Rúa's proof relies on computational results developed in Menichetti's work, [6], that led to the classification of the semifields of order q^3 as being either fields or the twisted fields of Albert (i.e. his solution of the Kaplansky conjecture). The proof we provide is based on standard properties of the Desarguesian planes and a property of $GF(q^3)$.

2 Nearfields as Acyclic Quasifields

Since any nearfield has associative multiplication, the principal powers correspond to powers. Hence the loop is cyclic iff the nearfield has cyclic multiplication, which means it is a field. Hence any proper nearfield is acyclic.

The structure of finite nearfields is thoroughly understood, and apart from the finite number of exceptional nearfields, they all have order q^n, where (q, n) is a Dickson pair, see e.g., [1, p 333].

1 Result (Dickson Pairs)**.** Let (q, n) be a Dickson pair: so q is a prime power, the integer $n > 1$ divides $q - 1$, and for $q \equiv 3 \pmod 4$ the condition $n \not\equiv 0 \pmod 4$ holds. Then there is a Dickson nearfield of order q^n.

11 Corollary. *There are acyclic nearfields for each of the following orders M:*

(1) $M = p^u$, whenever p is an odd prime and u is any prime dividing $p - 1$.

(2) $M = q^2$, whenever q is any odd prime power. Hence acyclic nearfields exist for every odd square prime-power. In particular, there are acyclic nearfields of order $p^2 > 4$ for all odd primes p.

Note that for non-square orders q^n several cases remain open, at least in the sense that for such orders nearfields do not furnish examples of acyclic quasifields. For instance if $q^n = p^u$, where p, u are odd primes such that u does not divide $p - 1$. We are unable to resolve this case. Similarly, there are no nearfields of order $q^n = 2^{2^m}, m > 1$. However, we shall show ahead that acyclic quasifields with these orders always exist.

Before leaving this section, we note that some Dickson nearfields are acyclic quasifields that cannot arise from a geometric covering: thus translation planes admitting geometric covers form a strictly smaller subclass of the planes coordinatizable by acyclic quasifields.

12 Corollary. *For every odd prime power p^3, there are planar acyclic loops such that the corresponding translation planes (viz. nearfield planes) do not admit a geometric cover.*

Proof. We have seen that Dickson nearfields of these order have acyclic multiplicative loops, and they do not admit geometric covers by the Baer condition. QED

3 Derivation Of Linear Planar Ternary Rings

The main part of the following proposition dates back to the sixties, reflecting the genesis of the concept of derivation, originating in the observation of Albert and Hughes about coordinate 'switching', and Ostrom's geometric interpretation. It is valid for finite linear planar ternary rings which are rank two left

vector spaces over a subfield[2]. We have, however, restricted ourselves to quasifields since this simplifies the statement of the proposition and contains the only case we need: semifields that are 2-dimensional over their middle nucleus.

13 Proposition. *Suppose $D = (V, +, \circ)$ is a quasifield of order q^2 with subfield $(F, +, \circ) = GF(q)$ such that $(V, +)$ is a left vector space over F. Fixing $t \in V \setminus F$, we have $V = F + F \circ t$. Let $\pi(D)$ denote the projective plane coordinatized by D. Then the following hold.*

(1) The affine plane $\pi = \pi(D)^{[\infty]}$ is derivable relative to the slope set of the subplane $\pi(F)$, viz., $\pi(F) \cap [\infty]$.

(2) The derived plane π' may be coordinatized by a quasifield

$$D' = (F + F \circ t, +, *), \text{ such that } f \circ x = f * x, \forall f \in F, x \in V;$$

thus D and D' induce the same left vector space operations (addition and left multiplication by F) on $F \oplus F \circ t$; in particular, we have identical fields $(F, +, \circ) = (F, +, *)$.

(3) Suppose K is a subfield of F and $x \in D \setminus F$ is such that the vector subspace $D_x := (K + K \circ x, +, \circ)$ is a sub-quasifield of D. Then $D'_x := (K + K \circ x, +, *)$ is a sub-quasifield of the derived sub-quasifield D'.

(4) The sub-quasifield D'_x is centralized multiplicatively by K iff D_x is centralized multiplicatively by K.

Proof. (1) holds because $\pi(F)$ defines a rational Desarguesian net, covered by Baer subplanes. To prove (2), choose the coordinatization of the derived plane π' so that the general affine points with coordinates $(x_1 + x_2 \circ t, y_1 + y_2 \circ t)$ in $\pi(D)$ are assigned coordinates $(x_1 + y_1 \circ t, x_1 + y_2 \circ t)$ in π'. This is sufficiently constraining so that the derived linear planar ternary ring is uniquely determined and satisfies the conditions stated. The other parts follow by closely inspecting the selected coordinatization. QED

4 Geometric Covers based on Transitive Quasifields

14 Definition. Let Q be a finite quasifield and F a subfield of Q. Then Q is *tangentially transitive relative to F* if $Aut(Q)_F$, the elementwise stabilizer of F in $Aut(Q)$, is transitive on $Q \setminus F$.

[2]This depends on using the Hughes coordinatization scheme: Hall coordinates require a right vector space. Since we apply the process to semifields 2-dimensional over their middle nucleus, the distinction is irrelevant.

It is well-known that all tangentially transitive quasifields are obtained by deriving semifields two-dimensional over a middle nucleus subfield. Since the semifield is permitted to be a field of square order, such tangentially transitive semifields exist for all square orders.

2 Result. (See [11] for details.) Let D be a (semi)field of order q^2 containing a subfield $F = GF(q)$ in a middle nucleus subfield $F = GF(q)$. Then D is derivable with respect to F and the derived quasifield D' is tangentially transitive relative to the subfield F, cf. Proposition 13. In particular, tangentially transitive quasifields exist for all square prime powers q^2.

The relevance of tangentially transitive planes to the construction of geometric covers lies in the fact that a *proper* subclass of the tangentially transitive quasifields coordinatize translation planes with geometric covers.

15 Lemma. *Let Q be a quasifield tangentially transitive relative to a subfield F and suppose K is a proper subfield of the field F. Suppose Q contains an element $\lambda \in Q \setminus F$ such that K centralizes λ multiplicatively and that the additive group $K + K\lambda$ is a sub-quasifield, Q_λ, of Q. Then the translation plane $\pi = \pi(F)$ admits a geometric cover over the subplane $\pi(K)$.*

Proof. Let $x \in Q \setminus F$. Since $\lambda \in Q \setminus F$ centralizes K, the transitivity of $Aut(Q)_F$ on $Q \setminus F$, plus the invariance of K under this group, implies x centralizes K. Hence, since $\{\lambda, K\}$ generates a sub-quasifield Q_λ of Q, on the additive group $K + K\lambda$, it follows similarly that $\{x, K\}$ generates a quasifield Q_x on the additive group $K + Kx$. Thus, we have a collection of sub-quasifields $\mathcal{Q} = \{Q_x : x \in Q \setminus F\}$ such that $\cup\mathcal{Q} = (Q \setminus F) \cup K$ and $\cap\mathcal{Q} = K$. Now clearly $\mathcal{Q} \cup \{F\}$ is a collection of *proper* sub-quasifields of Q such that they cover Q and any two intersect in K. Hence, the set of associated subplanes $\{\pi(R) : R \in \mathcal{Q} \cup \{F\}\}$ is a cover of the desired type. QED

16 Note. If Q is any Hall quasifield of order p^{2^n}, $n \geq 1$, then Q cannot admit a geometric cover.

Thus, to apply Lemma 15 above to find geometric covers we need tangentially transitive quasifields with *proper* sub-quasifields of the type indicated in the lemma. It turns out that we may achieve this by using two sources of tangentially transitive quasifields: the Hall quasifields (excluding those indicated in Note 16) and the derived Hughes-Kleinfeld quasifields. Notice that these two classes provide enough parameters to prove our main covering-theorem, cf. 23, although neither class on its own provides sufficiently many parameters. We start with the latter class; this requires a certain non-standard subclass of the Hughes-Kleinfeld semifields.

5 Geometric Covers: Derived Hughes-Kleinfeld Semifields; Hall Semifields

The following construction defines the finite Hughes-Kleinfeld semifields, [10, Theorem 1].

17 Theorem. *Let $S = F \oplus F\lambda$, where F is a finite field and λ an indeterminate; thus $S \cong F \oplus F$ is a rank 2 left-vector space over F. Define the multiplication on S by*

$$(x + y\lambda) \circ (u + v\lambda) = (xu + \delta_0 y^\sigma v) + (yu + x^\sigma v + \delta_1 y^\sigma v)\lambda, \qquad (1)$$

where the non-identity automorphism $\sigma \in Gal(G)$ is subject only to the condition $w^{1+\sigma} + w\delta_1 - \delta_0 = 0$ has no solution for w in F. Then S is a semifield with F as its middle and right nucleus.

We require a Hughes-Kleinfeld semifield of the above type such that σ is an involutory automorphism of F and the coefficients occurring in equation (1) all lie in $K = \mathrm{Fix}(\sigma)$. For this type of non-standard choice of σ we require:

18 Lemma. *Let $F = GF(q^2) > GF(q) = K$, and let σ be the involution in $Gal(F/K)$. Suppose $x^2 + d_1x + d_2 \in K[x]$ is any irreducible quadratic over K, with $d_1 \neq 0$. Then $x^{\sigma+1} + d_1x + d_2 \in K[x]$ has no roots in F.*

Proof. Assume if possible that $t \in F$ is a root of $x^{\sigma+1} + d_1x + d_2 = 0$. Consider the case $t \in F \setminus K$. Then $t^{\sigma+1} \in K$, since this corresponds to the norm map. Thus $t^{\sigma+1} + d_1t + d_2 = d_1t + (t^{\sigma+1} + d_2) \neq 0$, since $t^{\sigma+1} + d_2 \in K$ but $d_1t \notin K$. It remains to consider $t \in K$. But now $t^{\sigma+1}+d_1t+d_2 = t^2+d_1t+d_2 \neq 0$, since $x^2 + d_1x + d_2 \in K[x]$ is an irreducible quadratic in K. QED

Continuing with the notation in Theorem 17, it follows from Lemma 18:

19 Corollary. *Suppose the field $F = GF(q^2) > GF(q) = K$ is any square order finite field. Then the 2-dimensional F-space $S = F + F\lambda$, λ an F-indeterminate, admits a multiplication $\circ$ such that $(S, +, \circ)$ is a (non-associative) Hughes-Kleinfeld semifield $\mathfrak{HK}_{(F)}$ with middle nucleus $F > K$, such that both of the following hold:*

$$\exists\ \delta_0, \delta_1 \in K \text{ such that } \lambda \circ \lambda = \delta_0 + \delta_1 \circ \lambda$$

and

$$\forall\ u \in K, \quad u \circ \lambda = \lambda \circ u.$$

Hence, the K-subspace $Q_K = K + K\lambda$ is a subfield of the semifield $\mathfrak{HK}_{(F)}$.

Proof. Only the final sentence deserves attention. Q_K is clearly a semifield, with K in its center. But since also K is two-dimensional over the central field K, Q_K is a field. QED

20 Theorem. *Let $Q := \mathfrak{HK}_{(F,\sigma)}$ be the Hughes-Kleinfeld semifield specified in Corollary 19: based on the middle nucleus $F = GF(q^2) > GF(q) = K$, the involutory automorphism $\sigma \in Gal(F, K)$, and defined on the vector space $F + F\lambda$, $\lambda \in Q \setminus F$. Let Q' be the derived quasifield relative to F, cf. Proposition 2. For each $x \in Q \setminus F$, let Q_x be the vector K-subspace, of Q generated by $\{x\} \cup K$. Then*

(1) Q_x is a subfield of Q.

(2) When Q is derived to Q', Q_x derives to a sub-quasifield Q'_x of Q'.

(3) Q'_x is a Hall quasifield.

(4) The kernel of Q'_x is K and $Q'_x \cap F = K$.

(5) The collection of (quasi)fields

$$\mathcal{C} := \{Q_x : x \in (Q' \setminus F)\} \cup \{F\},$$

is a covering of Q', based on the subfield K.

(6) Any two members of the cover $\mathcal{C}$ intersect precisely on the field K:

$$A, B \in \mathcal{C} \implies A \cap B = K.$$

(7) Every member of the cover $\mathcal{C}$ of Q', other than the field F, is a Hall quasifield, although Q' is not a Hall quasifield.

Proof. By Proposition 13, the standard derivation of the Hughes-Kleinfeld semifield $\mathfrak{HK}$ relative to the middle-nucleus field F yields a quasifield Q' that contains F as a subfield, and this quasifield has as a sub-quasifield the vector K-subspace $Q'_K := K + K\lambda$ — the sub-quasifield obtained by deriving the field $Q_K < Q$ relative to K. Since the derived quasifield arising from a field is a Hall quasifield, $Q'_K := K + K\lambda$ must be a Hall quasifield with kernel K such that K centralizes Q'_K. Since also $Aut(Q')_F$ is transitive on $Q \setminus F$ and leaves $K < F$ elementwise fixed, it follows each $Q'_x := K + Kx$ is a Hall-system for every $x \in Q' \setminus F$ with kernel K and the remaining elements in $Q' \setminus F$. Note, however, that the elements of $x \in Q' \setminus F$ satisfy quadratic equations in F that are reducible, viz. their coefficients are in the Baer subfield K. Hence Q' itself cannot be a Hall quasifield since in Hall quasifields every non-kern element satisfies an irreducible quadratic in K. QED

We emphasize a particular part of this theorem:

21 Theorem. *There are tangentially transitive planes ψ of order q^2, for every square prime power q, obtained by deriving a subclass of the Hughes-Kleinfeld semifields of order q^2, such that there is a Baer chain of subplanes $\psi \supset \psi_F \supset \psi_K$ for which the following hold:*

(1) ψ admits a geometric cover $\mathcal{C}$ consisting of Hall Baer subplanes along with exactly one Desarguesian subplane, such that any two members of $\mathcal{C}$ have as their intersection ψ_K.

(2) ψ is not a Hall plane nor a Desarguesian plane.

Thus, the plane in the above theorem has the fairly noteworthy feature that it contains subplanes that are neither Desarguesian nor of the same type as the class from which the plane is selected. In general this phenomenon seems to be rather rare: classes of sub-regular spreads have this property, but otherwise few other cases seem to be known.

Returning to Theorem 20, we note it does not apply to planes of square order q^2, unless q itself is a square. Thus, it is adequate to consider quasifields of order q^2, where $q = p^m$, and $m > 1$ is not a power of 2. These case may be dealt by using Hall quasifields as follows[3].

Let $F = GF(q)$, as above, and choose K to be any subfield of F such that $[F : K] = r > 1$ is odd: this choice is possible since $m > 1$, not being a power of 2, admits an odd divisor r. Let $f(x) \in K[x]$ be any irreducible quadratic polynomial over K. Then $f(x)$ may also be considered an F-irreducible polynomial. Hence there is a Hall quasifield $Q_\lambda(F)$ on $F + F\lambda$, λ an F-indeterminate, [1, Corollary 14.3.9,(3),(4)], with product $\circ$ uniquely specified by the conditions

$$\lambda \circ \lambda = f(\lambda), \quad f \circ \lambda = \lambda \circ f \ \ \forall\ f \in F,$$

and the assumption that the quasifield $Q_\lambda(F)$ has F as its kernel.

Now since $\lambda \circ \lambda = f(\lambda) \in K$, the vector K-subspace $Q_\lambda(K) := K \oplus K\lambda$ is such that K is in its kernel and of course every element in $(K \oplus K\lambda) \setminus K$ satisfies the same quadratic equation $f(x) \in K[x]$: this makes $Q_\lambda(K)$ a Hall sub-quasifield of the Hall quasifield $Q_\lambda(F)$. Moreover, since $Aut(Q)_F$ is transitive on $Q \setminus F$, Lemma 15 yields

22 Theorem. *The Hall quasifield Q of order q^2 with $q = p^r$, and $r > 1$ not a power of 2 admits a cover by proper Hall sub-quasifields along with the kern field $F = GF(q)$, such that any two of these sub-(quasi)fields intersect precisely on a fixed proper subfield $K < F$.*

Combining the theorems above, we have

[3]The properties of Hall quasifields are summarized in [1, Corollary 14.3.9].

23 Theorem. *There exists a translation plane of square order $n = p^{2r}$ with a geometric cover iff the integer $r > 1$.*

24 Corollary. *An acyclic quasifield of square order q^2 exists iff $q > 4$.*

PROOF. If q is non-prime the theorem applies, and if $q = p$ is an odd prime, then the nearfields of order p^2 are acyclic: they exist for all p odd. QED

6 Ruá's Theorem Revisited

In [6], Menichetti proved some fundamental results on three-dimensional semifields, which he used to prove the Kaplansky conjecture, [7], that such semifields are either Desarguesian or Albert semifields. The paper by Rúa, [5], used Menichetti's results to show that three-dimensional semifields are primitive, thereby generalizing a theorem of Wene, [12], who established this result, but for right-primitivity, for the special case when the semifields are additionally commutative of odd characteristic.

In this section we give an alternative proof of Rúa's Theorem that provides a conceptual geometric approach to Rúa's result and does not rely on Menichetti's intensive calculations.

Let $D = (V, +, \circ)$ be a semifield of order q^3, with subfield $K = GF(q)$ in its center, $q = p^r$, p prime. The slope map of an element $d \in D$ is the K-linear map of $(V, +)$ specified by $T_d : x \mapsto d \circ x,\ x \in V$; we regard each T_d as a 3×3 K-matrix. Now $\tau_D = \{T_d : d \in V\}$, the slope set of D, is an additive group of K-matrices of order q^3, with all non-zero elements non-singular. Observe that τ_D includes the matrix field $\tau_K := \{k\mathbf{1}_3 : k \in K\}$, which we identify with K, via the field isomorphism $k\mathbf{1}_3 \mapsto k, k \in K$; so the slope map T_k of $k \in K$ will be written as k. The following well known fact is easily verified and reflects the fact that τ_D consists of τ_K-linear elements.

25 Remark. For $k \in K$ and $A \in \tau_D$, we have $Ak = kA \in \tau_D$.

Now fix $A \in \tau_D \setminus K$, so the (multiplicative) cyclic group $\langle A \rangle = P \otimes R$, where P is its p-Sylow subgroup and R its p' subgroup. Then

26 Lemma. *The matrix $A \in GL(V, K)$ acts irreducibly on V.*

PROOF. Since A is a non-singular K-linear map of $V = K^3$, we may identify A with a collineation of $\pi = PG(V, K)$, which is the Desarguesian projective plane of order $|K|$. Since the non-zero elements of D form a multiplicative loop, $Ax = kx$ is impossible for $k \in K$. Hence A cannot fix any projective point of $PG(V, K)$. This further implies that A cannot fix any hyperplane, since the number of fixed (projective) points of A is the number of fixed hyperplanes, as we have a symmetric design, e.g., [8, 12,p 81]. Thus A does not fix any subspace of V, as required. QED

We require the following theorem on Galois fields.

3 Result (Mills and McNay, [4])**.** Let F_{q^3} be a cubic extension of any finite field F_q with q elements, where q is any prime power. Then for any given element $\theta \in F_{q^3} \setminus F_q$, there exist $a, b \in F_q$ such that $a\theta + b$ is a primitive root of F_{q^3}

We now have the desired proof of Rúa's result.

27 Theorem. *Suppose a semifield D of order q^3 contains $K = GF(q)$ in its center. Then D is primitive: the multiplicative loop of D contains both a right primitive element and a left primitive element.*

Proof. By Lemma 26, A is irreducible. Hence, by Schur's Lemma, its centralizer in $GL(3, K)$ is a field of matrices $F < GL(3, K) \cup \{0\}$ such that $F \cong GF(q^3)$, and since $F > K$ the field F must contain the K-subspace $K + KA$. Now, by Result 3, $K + KA$ contains a primitive element B. However, by Remark 25, $K + KA \in \tau_D$, the slope set of D. Thus, τ_D includes a matrix R of order $q^3 - 1$. Let ρ be the element with slope map R. Now, for any non-zero a, the R-orbit

$$\{a, Ra, \dots R^{q^3-1}a = \{a, \rho \circ a, \rho \circ (\rho \circ a), \dots\} = V \setminus \{0\},$$

so ρ is a left primitive element of D.

We had chosen to work with slope maps of the form $T_d : x \mapsto d \circ x$. If instead we had worked with slope maps of type $\theta_d : x \mapsto x \circ d$, we would see that D has a right primitive element. This completes the proof. QED

7 Concluding Remarks

The main focus of this article has been the study of translation subplanes admitting geometric covers, an apparently innocuous geometric condition. Any such plane admits coordinatization by quasifields that are guaranteed to be simultaneously left acyclic and right acyclic: but the converse is false. Hence, in the terminology of Wene and other authors, a semifield plane π that admits a geometric cover, based on a sub-semifield plane π_0, admits coordinatization by semifields that are imprimitive relative to left principal powers and right principal powers.

Hence, we end with a conjecture that is more provocative than the Wene conjecture:

Conjecture. *A semifield plane of order > 32 does not admit a geometric cover relative to a sub-semifield plane.*

This conjecture being geometric in nature, enables all the tools of modern translation plane theory to be applied to solve the Wene conjecture. Ad-

ditionally, the study of this geometric conjecture might, we hope, lead to the development of new geometric methods that may be useful in other contexts.

Acknowledgements. Dedicated to Norman L. Johnson on the occasion of his 70th birthday.

References

[1] M. Biliotti, V.Jha, N. L. Johnson: Foundations of Translation Planes, Marcel Dekker, Inc., New York, Basel.

[2] M. Abrams, N. Doraswamy, A. Mathur: *Chitra*, TR 92–24.

[3] I. R. Hentzel, I. F. Rúa: *Primitive and Non-Primitive Finite Semifields*, International J. Algebra and Computation, **17** (2007), 1411–1429.

[4] D. Mills, G. McNay: Primitive roots in cubic extensions of finite fields. Finite fields with applications to coding theory, cryptography and related areas (Oaxaca, 2001), Springer, Berlin, 2002, 239–250.

[5] I. F. Rúa: *Primitive and Non-Primitive Finite Semifields*: Communications in Algebra, **22**, (2004), 791–803.

[6] G. Menichetti: *Algebre tridimensionali su un campo di Galois*, Ann. Mat. Pura Appl., **97** (2004), 293–302.

[7] G. Menichetti: *On a Kaplansky conjecture concerning three-dimensional division algebras over a finite field*, J. Algebra, **47** (1977), 400–410.

[8] P. Dembowski: Finite Geometries, Springer Verlag, Berlin, Heidelberg, New York, 1968.

[9] D. R. Hughes, F. C. Piper: Projective Planes, Springer Verlag, New York, 1973.

[10] D. R. Hughes, E. Kleinfeld: *Seminuclear extension of Galois fields*, Amer J. Math, **82** (1960), 389–392.

[11] V. Jha: *On tangentially transitive translation planes and related systems*, Geom. Dedicata, **4** (1975), 457–483.

[12] G. P. Wene: *On the multiplicative structure of finite division rings*, Aequationes Math., **41** (1991), 222–233.

[13] G. P. Wene: *Semifields of dimension* $2n$*,* $n \geq 3$*, over* $GF(p^m)$ *that have left primitive elements*, Geom. Dedicata, **41** (1992), 1–3.