to appear in *Note di Matematica* revised 02 Nov 2009

Partial Spreads and Flocks over Infinite Fields

G. Eric Moorhouse, University of Wyoming

We investigate the possible deficiencies of partial flocks of quadrics over some infinite fields; also deficiencies of partial spreads of projective spaces over infinite fields.

1. Introduction and Results

Let $\mathfrak{C}$ be a classical circle plane (also known as a classical Benz plane) defined over a field K. Thus $\mathfrak{C}$ is a point-block incidence structure embeddable in projective 3-space $\mathbb{P}^3K$ over K. The point set of $\mathfrak{C}$, denoted by $\mathcal{Q}$, is a hyperbolic or elliptic quadric in $\mathbb{P}^3K$, or a quadratic cone minus its vertex. These three choices for $\mathcal{Q}$ yield a classical Minkowski, Möbius (i.e. inversive) or Laguerre plane, respectively. Blocks of $\mathfrak{C}$, called *circles*, are simply nondegenerate plane intersections $\mathcal{Q} \cap \pi$ where π is a plane of $\mathbb{P}^3K$. Further properties of circle planes may be found in [5,9].

A *partial flock* of $\mathfrak{C}$ is a collection of mutually disjoint circles. The following question was posed in a talk by Norm Johnson at the 1996 TedFest:

(1) *Is it possible for a partial flock to cover all but one point of the classical Laguerre plane over K?*

(This question appears not to have been recorded in the proceedings; but several related questions are described in [2,7].) The answer to (1) is clearly 'no' if K is finite. We find that for infinite fields K, the answer to (1) depends on the particular choice of K. We define the *deficiency*[1] of a partial flock to be the cardinality of the set of points not covered. A *flock* of $\mathfrak{C}$ is a partition of the point set of $\mathfrak{C}$ into circles, i.e. a partial flock of deficiency zero. In answer to (1), we list here the possible deficiencies of partial flocks in classical circle planes for certain choices of the field K:

1.1 Theorem. *Let K be a finite field, or the field $\mathbb{Q}$ of rationals, or the real field $\mathbb{R}$. The possible values for the deficiency δ of a partial flock of a classical circle plane over K, are as follows.*

K	*Laguerre*	*Möbius*	*Minkowski*	
$\mathbb{F}_q$	$\delta = k(q{+}1)$	$\delta = 2 + k(q{+}1)$	$\delta = k(q{+}1)$	$0 \leqslant k \leqslant q{+}\varepsilon^*$
$\mathbb{Q}$	*any* $\delta \leqslant \aleph_0$	*any* $\delta \leqslant \aleph_0$	*any* $\delta \leqslant \aleph_0$	
$\mathbb{R}$	$\delta = 0$ *or* $2^{\aleph_0}$	$\delta = 2$ *or* $2^{\aleph_0}$	$\delta = 0$ *or* $2^{\aleph_0}$	

(*) $\varepsilon = 0, -1, +1$ *for finite Laguerre, Möbius, Minkowski planes respectively*

[1] This definition differs from the conventional definition (see e.g. [2, Definition 2.6]) which, in the case of Laguerre planes, only applies to partial flocks missing the same number of points in each point class. It is well-known that in the case of infinite fields, a partial flock may not meet this condition.

Here $\aleph_0 = |\mathbb{Q}|$ and $2^{\aleph_0} = |\mathbb{R}|$; and we have indicated the exact set of possible values for the deficiency in each case. For example, for every given cardinal number δ, there exists a partial flock of a classical Laguerre plane over $\mathbb{Q}$ with deficiency δ, iff $\delta \leqslant \aleph_0$. Thus the answer to (1) is negative in the case $K = \mathbb{R}$, but affirmative in the case $K = \mathbb{Q}$. Theorem 1.1 follows from more general results from Sections 5,6,8 on existence and extendibility of partial flocks.

As a warmup to the indicated results on partial flocks, we first review some results on existence and extendibility of partial spreads of $\mathbb{P}^{2n-1}K$ over a field K. By a *partial spread* of $\mathbb{P}^{2n-1}K$, we mean a collection of mutually disjoint projective $(n-1)$-subspaces of $\mathbb{P}^{2n-1}K$. The *deficiency*[2] of such a partial spread is the cardinality of the set of points not covered by the partial spread.

1.2 Theorem. *Let K be a finite field, or the field $\mathbb{Q}$ of rationals, or the real field $\mathbb{R}$. The possible values for the deficiency δ of a partial spread of $\mathbb{P}^{2n-1}K$, are as follows.*

K	*Deficiency* δ	
$\mathbb{F}_q$	$\delta = k(q+1)$,	$0 \leqslant k \leqslant q^2+1$
$\mathbb{Q}$	*any* $\delta \leqslant \aleph_0$	
$\mathbb{R}$	*any* $\delta \leqslant 2^{\aleph_0}$	

Moreover if K is an arbitrary infinite field, then every cardinal number $\delta \leqslant |K|$ arises as the deficiency of some partial spread of $\mathbb{P}^{2n-1}K$.

The proof of Theorem 1.2 is by now folklore; see [1] for a sample of such proofs in geometry. We provide a proof here (Section 3) since it serves to prepare the reader for our similar (but less obvious) results on partial flocks.

The existence results described in this paper typically requires some form of the Axiom of Choice, and so are not strictly 'constructions'. We in fact use the language of transfinite induction (see e.g. [1,3]). We note, however, that for our affirmative answer to (1) in the case $K = \mathbb{Q}$, the Axiom of Choice is not a genuine issue: since $\mathbb{Q}$ is countable, the argument reduces to ordinary induction. Even when the Axiom of Choice is not strictly required, the language of transfinite induction provides a convenient common framework for such proofs. The equivalent language of Zorn's Lemma may in each case be used in place of transfinite induction, if so desired. At no time is the Continuum Hypothesis ever an issue for us: this statement is neither assumed nor denied.

We intend this collection of results as a sample of what is possible using transfinite induction, and not a very comprehensive list. The reader is invited to try extending these results to more general fields or other geometric constructions.

Finally, we highlight the following easy consequence of Theorem 1.2.

[2] Again, this definition differs from the standard one, which applies to the case $K=\mathbb{F}_q$; here one refers to the deficiency as k rather than $k(q+1)$ in our notation above.

1.3 Corollary. *Let O be a single point of Euclidean 3-space $\mathbb{R}^3$. There exists a partition of $\mathbb{R}^3 \smallsetminus \{O\}$ into lines.*

We ask the reader: can such a partial spread be described explicitly?

2. Recursive Extension

We shall occasionally use the following facts regarding the arithmetic of cardinal numbers; see e.g. [3].

2.1 Proposition. *Let X and Y be sets with X infinite and Y nonempty.*

(a) *We have $|X||Y| = |X| + |Y| = \max\{|X|, |Y|\}$.*
(b) *For every positive integer n, we have $|X|^n = |X|$.*
(c) *Consider arbitrary sets A, B with $|A|, |B| < |X|$. Then $|A| + |B| < |X|$.*

Proof. For (a) and (b), see [3, p.126]. If both A and B are finite, then $|A| + |B|$ is finite and (c) is clear. On the other hand, if A and B are not both finite, then (a) yields $|A| + |B| = \max\{|A|, |B|\} < |X|$. $\square$

Partial spreads of projective spaces, and partial flocks of circle planes, are two special instances of the following general framework. Let $(\mathcal{X}, \mathcal{B})$ be a point-block incidence system with an infinite point set $\mathcal{X}$. Thus $\mathcal{X}$ is an infinite set, and $\mathcal{B}$ is a collection of subsets of $\mathcal{X}$, called *blocks*. A *partial spread of* $(\mathcal{X}, \mathcal{B})$ (or simply, *of* $\mathcal{X}$) is a collection of blocks $\Sigma \subseteq \mathcal{B}$, such that any two distinct blocks in Σ are disjoint. We proceed to describe a general class of existence questions for partial spreads, amenable to transfinite induction, of which partial spreads of projective spaces and partial flocks of circle planes are but special instances. The equivalent conditions (i) and (ii) of Lemma 2.2 below are not the most general assumptions under which transfinite induction proceeds, but they are convenient and sufficiently general for our purposes. Note that we do not require members of $\mathcal{B}_0$ to be mutually disjoint.

2.2 Lemma. *Let $(\mathcal{X}, \mathcal{B})$ be a point-block incidence structure with $\mathcal{X}$ infinite. Then the following two conditions are equivalent.*

(i) *Given any collection $\mathcal{B}_0 \subseteq \mathcal{B}$ of blocks with $|\mathcal{B}_0| < |\mathcal{X}|$ members, and any point $P \in \mathcal{X}$ not covered by $\mathcal{B}_0$, i.e. $P \notin \bigcup \mathcal{B}_0$, there exists a block $B \in \mathcal{B}$ containing P with $\big(\bigcup \mathcal{B}_0\big) \cap B = \varnothing$.*

(ii) *Given any collection $\mathcal{B}_0 \subseteq \mathcal{B}$ of blocks with $|\mathcal{B}_0| < |\mathcal{X}|$ members, and any point $P \in \mathcal{X}$ not covered by $\mathcal{B}_0$, i.e. $P \notin \bigcup \mathcal{B}_0$, and any point subset $\mathcal{X}_0 \subset \mathcal{X}$ with $|\mathcal{X}_0| < |\mathcal{X}|$ and $P \notin \mathcal{X}_0$, there exists a block $B \in \mathcal{B}$ containing P with $\big(\bigcup \mathcal{B}_0\big) \cap B = \mathcal{X}_0 \cap B = \varnothing$.*

Proof. Clearly (i) follows from (ii) by taking $\mathcal{X}_0 = \varnothing$. Now suppose (i) holds, and let $\mathcal{B}_0 \subseteq \mathcal{B}$ be a collection of blocks with $|\mathcal{B}_0| < |\mathcal{X}|$ members. Consider a point $P \notin \bigcup \mathcal{B}_0$ and a set of points $\mathcal{X}_0 \subset \mathcal{X}$ of cardinality $|\mathcal{X}_0| < |\mathcal{X}|$ with $P \notin \mathcal{X}_0$. For every point $x \in \mathcal{X}_0$, by the hypothesis (i) there exists a block $B_x \in \mathcal{B}$ containing x but not P. Also by (i) there exists a block $B \in \mathcal{B}$ containing P, with B disjoint from every block B_x ($x \in \mathcal{X}_0$) and disjoint from every member of $\mathcal{B}_0$; here we use the fact that $|\mathcal{X}_0| + |\mathcal{B}_0| < |\mathcal{X}|$ by Proposition 2.1(c). $\square$

We say that partial spreads of $(\mathcal{X}, \mathcal{B})$ *extend recursively* if the equivalent conditions of Lemma 2.2 are satisfied. This property supplies the inductive step in a transfinite induction proof of the following.

2.3 Theorem. *Let $(\mathcal{X}, \mathcal{B})$ be an incidence system with $\mathcal{X}$ infinite, and suppose that partial spreads of $(\mathcal{X}, \mathcal{B})$ extend recursively. Let Σ_0 be a partial spread of $\mathcal{X}$ with $|\Sigma_0| < |\mathcal{X}|$ members. Then:*

(a) There exists an extension of Σ_0 to a spread $\Sigma \supseteq \Sigma_0$ of $\mathcal{X}$.

(b) Suppose that $\mathcal{X}_0 \subset \mathcal{X}$ is a subset of the points of cardinality $|\mathcal{X}_0| < |\mathcal{X}|$, with $\left(\bigcup \Sigma_0\right) \cap \mathcal{X}_0 = \varnothing$. Then Σ_0 extends to a partial spread $\Sigma \supseteq \Sigma_0$ omitting precisely *the points of $\mathcal{X}_0$ (i.e. $\bigcup \Sigma = \mathcal{X} \setminus \mathcal{X}_0$).*

Proof. It suffices to prove (b), since this implies (a) by taking $\mathcal{X}_0 = \varnothing$. Index the points of $\mathcal{X} \setminus \mathcal{X}_0$ using the least ordinal α with $|\alpha| = |\mathcal{X}| = |\mathcal{X} \setminus \mathcal{X}_0|$, thus:

$$\mathcal{X} \setminus \mathcal{X}_0 = \{P_\beta\}_{\beta \in \alpha}.$$

We recursively define a chain $\{\Sigma_\beta\}_{\beta \in \alpha}$ of partial spreads of $(\mathcal{X}, \mathcal{B})$ satisfying

(i) Σ_0 is the initial partial spread given;
(ii) $\Sigma_\beta \subseteq \Sigma_\gamma$ whenever $\beta \leqslant \gamma < \alpha$;
(iii) $P_\beta \in \bigcup \Sigma_\gamma$ whenever $\beta < \gamma < \alpha$;
(iv) $\bigcup \Sigma_\beta \subseteq \mathcal{X} \setminus \mathcal{X}_0$; and
(v) $|\Sigma_\beta| \leqslant |\Sigma_0| + |\beta| < |\alpha|$ whenever $\beta < \alpha$.

The recursive definition of Σ_β begins with the given partial spread Σ_0. For every limit ordinal β satisfying $0 < \beta \leqslant \alpha$, define

$$\Sigma_\beta = \bigcup_{\gamma < \beta} \Sigma_\gamma .$$

Finally, for every ordinal $\beta < \alpha$,

- If $P_\beta \in \bigcup \Sigma_\beta$, set $\Sigma_{\beta+1} = \Sigma_\beta$.
- If $P_\beta \notin \bigcup \Sigma_\beta$, choose a block $B \in \mathcal{B}$ containing P_β, with $\left(\bigcup \Sigma_\beta\right) \cap B = \mathcal{X}_0 \cap B = \varnothing$. The existence of such a block B follows from the hypothesis of recursive extendibility, as in Lemma 2.2. Set $\Sigma_{\beta+1} = \Sigma_\beta \cup \{B\}$.

Clearly the partial spread $\Sigma = \Sigma_\alpha = \bigcup_{\beta < \alpha} \Sigma_\beta$ has the required properties. $\square$

3. Partial Spreads of Projective Spaces

In order to satisfy the conditions of Section 2 for extendibility of partial spreads, we require the following, in which K is an arbitrary field, finite or infinite.

3.1 Lemma. *Let V be a finite-dimensional vector space over a field K. Then V cannot be covered by fewer than $|K|+1$ proper subspaces.*

Proof. Suppose the conclusion fails, and let V be a vector space of minimal finite dimension n for which $V = \bigcup \mathcal{H}$ for some collection $\mathcal{H}$ of proper subspaces of V, with $|\mathcal{H}| < |K|+1$. Without loss of generality, we may assume each $H \in \mathcal{H}$ has dimension $n-1$. Clearly we must have $n \geqslant 3$. Since

$$|\mathcal{H}| < |K|+1 \leqslant |K|^n + |K|^{n-1} + \cdots + |K| + 1,$$

we see that V has a subspace U of codimension 1 which is not among the subspaces $H \in \mathcal{H}$. But then U is covered by the subspaces $H \cap U$ of dimension $n-2$ for $H \in \mathcal{H}$, contradicting the minimality of n. $\square$

In the following, n is a positive integer.

3.2 Corollary. *Let V be a $2n$-dimensional vector space over an infinite field K, and let $\mathcal{S}$ be a collection of n-dimensional subspaces of V with $|\mathcal{S}| < |K|$. Then there exists an n-dimensional subspace $U < V$ such that $\left(\bigcup \mathcal{S}\right) \cap U \subseteq \{0\}$.*

Proof. We may assume that $\mathcal{S}$ is nonempty. Let $U < V$ be a subspace of maximal dimension m subject to the constraint that $\left(\bigcup \mathcal{S}\right) \cap U = \{0\}$. Clearly $m \leqslant n$. We suppose that $m < n$ and seek a contradiction. In the quotient vector space V/U of dimension $2n - m \geqslant n+1$, we have a collection $\overline{\mathcal{S}}$ of proper subspaces of dimension n induced by $\mathcal{S}$, namely $\overline{\mathcal{S}}$ is the collection of subspaces $(S+U)/U < V/U$ for $S \in \mathcal{S}$. By Lemma 3.1 there exists a vector $\overline{v} = v + U \in V/U$ with $\overline{v} \notin \bigcup \overline{\mathcal{S}}$; but then the $(m+1)$-dimensional subspace $U + \langle v \rangle < V$ satisfies $\left(\bigcup \mathcal{S}\right) \cap (U + \langle v \rangle) = \{0\}$, contradicting the maximality of m. The result follows. $\square$

A *spread* of $\mathbb{P}^{2n-1}K$ is a collection of projective $(n-1)$-subspaces which partitions the set of projective points. A *partial spread* is a collection of mutually disjoint projective $(n-1)$-subspaces. The *deficiency* of a partial spread is the cardinality of the set of points not covered. In particular, a spread is the same as a partial spread of deficiency zero. The validity of Theorem 1.2 and Corollary 1.3 is a consequence of the following.

3.3 Theorem. *Let K be an infinite field. Then*

(a) Every partial spread of $\mathbb{P}^{2n-1}K$ having fewer than $|K|$ members, extends to a spread.

(b) Let $\mathcal{X}_0$ be a set of projective points of cardinality $|\mathcal{X}_0| < |K|$, and let $\mathcal{X}_1$ be its complement (in the set of projective points). Then $\mathcal{X}_1$ may be partitioned into projective $(n-1)$-subspaces.

Generalizing both (a) and (b),

(c) Let $\mathcal{X}_0$ and $\mathcal{X}_1$ be as in (b). Let Σ_0 be a partial spread of $\mathbb{P}^{2n-1}K$ not meeting $\mathcal{X}_0$, i.e. $\bigcup\Sigma_0 \subseteq \mathcal{X}_1$, with $|\Sigma_0| < |K|$. Then Σ_0 extends to a partial spread $\Sigma \supseteq \Sigma_0$ such that $\bigcup\Sigma = \mathcal{X}_1$.

Proof. It suffices to prove (c). The cardinality of the point set of $\mathbb{P}^{2n-1}K$ is

$$|K|^{2n-1} + |K|^{2n-2} + \cdots + |K| + 1 = |K|$$

since K is infinite and $n \geqslant 1$ is finite. By Corollary 3.2, partial spreads extend recursively in the terminology of Section 2. The result follows by Theorem 2.3. $\square$

4. Rational Squares and Nonsquares

Here we establish some technical results required in Sections 5 and 6. We first recall the p-adic norm on $\mathbb{Q}$ defined for every prime p by

$$\|p^r \tfrac{a}{b}\|_p = p^{-r} \quad \text{where } p \nmid ab, \quad a,b,r \in \mathbb{Z};$$

also $\|0\|_p = 0$. For all $x, y \in \mathbb{Q}$ we have $\|xy\|_p = \|x\|_p\|y\|_p$ and the *ultra-metric inequality*

$$\|x+y\|_p \leqslant \max\{\|x\|_p\,,\ \|y\|_p\}$$

holds; moreover we have equality $\|x+y\|_p = \max\{\|x\|_p\,,\ \|y\|_p\}$ whenever $\|x\|_p \neq \|y\|_p$. For these and further properties of the p-adic norm, see e.g. [4]. For each prime p we have the subring

$$\mathbb{Z}_{(p)} = \{x \in \mathbb{Q} : \|x\|_p \leqslant 1\} = \left\{\frac{a}{b} : a,b \in \mathbb{Z},\ p \nmid b\right\} \subset \mathbb{Q}.$$

(Readers acquainted with the ring $\mathbb{Z}_p$ of p-adic numbers will observe that $\mathbb{Z}_{(p)} = \mathbb{Q} \cap \mathbb{Z}_p$; others may safely disregard this observation.) The ring $\mathbb{Z}_{(p)}$ has a unique maximal ideal

$$p\mathbb{Z}_{(p)} = \{x \in \mathbb{Q} : \|x\|_p < 1\},$$

with residue field $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \cong \mathbb{F}_p$. The group of units of $\mathbb{Z}_{(p)}$ is

$$\mathbb{Z}_{(p)}^\times = \{x \in \mathbb{Q} : \|x\|_p = 1\} = \mathbb{Z}_{(p)} \smallsetminus p\mathbb{Z}_{(p)}.$$

Now suppose p is an odd prime. We extend the usual Legendre symbol (defined on the units of the ring $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$) to a multiplicative character, defined for $a \in \mathbb{Z}_{(p)}^\times$ by

$$\left(\frac{a}{p}\right) = \begin{cases} +1, & \text{if there exists } b \in \mathbb{Z}_{(p)} \text{ such that } \|b^2 - a\|_p < 1; \\ -1, & \text{otherwise.} \end{cases}$$

(Indeed, as observed by Serre [8,p.20], one obtains such an extension to all of $\mathbb{Z}_p^\times$.) We consider the Legendre symbol $\left(\frac{a}{p}\right)$ to be undefined unless $\|a\|_p = 1$. (Thus in designating a particular value for $\left(\frac{a}{p}\right)$, we are implicitly asserting that $\|a\|_p = 1$.)

4.1 Lemma. *Let $a \in \mathbb{Q}$ be a nonsquare. Then there exist infinitely many odd primes p such that $\left(\frac{a}{p}\right) = -1$.*

Proof. For $a \in \mathbb{Z}$ this follows from [6, p.57, Theorem 3]. In the general case, choose a nonzero integer k such that $k^2 a \in \mathbb{Z}$; then there are infinitely many odd primes p not dividing k such that $\left(\frac{k^2 a}{p}\right) = -1$. For each such p, we have also $\left(\frac{a}{p}\right) = -1$. $\square$

4.2 Lemma. *Let $a, b, c \in \mathbb{Q}$ such that $b^2 - 4ac$ is not a rational square. Then there exist infinitely many primes p such that every rational solution (x, y) of the equation $ax^2 + bxy + cy^2 = 1$ satisfies $\|x\|_p \leqslant 1$ and $\|y\|_p \leqslant 1$.*

Proof. By hypothesis, we have $a \neq 0$. Choose a positive integer d such that the quantities

$$M = \frac{d^2(b^2 - 4ac)}{4a^2} \quad \text{and} \quad N = \frac{d^2}{a}$$

are integers. Since the integer M is a nonsquare, by Lemma 4.1 there exist infinitely many primes p such that $\left(\frac{M}{p}\right) = -1$. Since there are only finitely many primes p satisfying $\|d\|_p \neq 1$ or $\|\frac{b}{2a}\|_p > 1$, there exist infinitely many primes p satisfying

$$(*) \qquad \|d\|_p = 1, \ \left\|\frac{b}{2a}\right\|_p \leqslant 1 \ \text{ and } \left(\frac{M}{p}\right) = -1\,.$$

Now let p be any prime satisfying (*), and let (x, y) be an integer solution of $ax^2 + bxy + cy^2 = 1$. Write

$$\left(x + \frac{b}{2a}y\right)d = \frac{X}{Z}\,, \quad y = \frac{Y}{Z}$$

where $X, Y, Z \in \mathbb{Z}$ with $\gcd(X, Y, Z) = 1$. Then

$$X^2 - MY^2 = NZ^2.$$

For every prime p satisfying (*), we must have $p \nmid Z$; otherwise $X^2 - MY^2 \equiv 0 \mod p$ with $\left(\frac{M}{p}\right) = -1$ implies $p \mid X$ and $p \mid Y$, contradicting $\gcd(X, Y, Z) = 1$. Thus $\|Z\|_p = 1$ and

$$\begin{aligned}
\|y\|_p &= \left\|\frac{Y}{Z}\right\|_p = \|Y\|_p \leqslant 1; \\
\left\|x + \frac{b}{2a}y\right\|_p &= \left\|\frac{X}{Zd}\right\|_p = \|X\|_p \leqslant 1; \\
\left\|\frac{b}{2a}y\right\|_p &= \left\|\frac{b}{2a}\right\|_p \|y\|_p \leqslant 1 \cdot 1 = 1; \\
\|x\|_p &= \left\|x + \frac{b}{2a}y - \frac{b}{2a}y\right\|_p \leqslant \max\left\{\left\|x + \frac{b}{2a}y\right\|_p, \left\|\frac{b}{2a}y\right\|_p\right\} \leqslant 1.
\end{aligned}$$

$\square$

4.3 Lemma. *Let $a, b, c \in \mathbb{Q}$ such that $b^2 - 4ac \neq 0$. Then there exists $t \in \mathbb{Q}$ such that $at^2 + bt + c$ is not a rational square.*

Proof. If $a = 0$, then by hypothesis we have $b \neq 0$ and the conclusion holds for $t = (2-c)/b$. Hence we may assume $a \neq 0$. Suppose the conclusion fails, i.e. the quantity

$$at^2 + bt + c = a\Big(t + \frac{b}{2a}\Big)^2 - \frac{b^2 - 4ac}{4a}$$

is a rational square for all $t \in \mathbb{Q}$. This means that there exist nonzero rationals a, r such that

$$au^2 + r$$

is a rational square for all $u \in \mathbb{Q}$. Clearly $a, r > 0$. We may choose a positive integer d such that $a' = d^2 a$ and $r' = d^2 r$ are (positive) integers; now

$$a'u^2 + r'$$

is an integer square for all $u \in \mathbb{Z}$. In particular this holds for $u = 0$, so $r' = m^2$ for some positive integer m. Choose a prime $p > \max\{2m, \sqrt{a' + 2m}\}$. Now $a'p^2 + m^2 = n^2$ for some positive integer n, so

$$a'p^2 = (n + m)(n - m).$$

Here $n > m > 0$ since $a' > 0$. Since $\gcd(n + m, n - m) = gcd(n - m, 2m) \leqslant 2m < p$, we have either $p^2 \mid (n + m)$ or $p^2 \mid (n - m)$; thus $n \geqslant p^2 - m > 0$. But

$$a'p^2 = n^2 - m^2 \geqslant (p^2 - m)^2 - m^2 = (p^2 - 2m)p^2 > a'p^2,$$

a contradiction. □

4.4 Lemma. *Let $f_1(t), f_2(t), \ldots, f_m(t) \in \mathbb{Q}[t]$ be quadratic polynomials, and suppose there exist rational numbers r_i such that $f_i(r_i)$ is a rational nonsquare for $i = 1, 2, \ldots, m$. Then there exists $r \in \mathbb{Q}$ such that $f_i(r)$ is a rational nonsquare for $i = 1, 2, \ldots, m$.*

Proof. Write $f_i(t) = \lambda_i t^2 + \mu_i t + \nu_i$ where $\lambda_i, \mu_i, \nu_i \in \mathbb{Q}$. Since $f_i(r_i) \in \mathbb{Q}$ is a nonsquare, it follows from Lemma 4.1 that there exist *distinct* odd primes $p_1, p_2, \ldots, p_m$ such that

$$\|\lambda_i\|_{p_i} \leqslant 1,\ \|\mu_i\|_{p_i} \leqslant 1,\ \|r_i\|_{p_i} \leqslant 1,\ \text{and}\ \Big(\frac{f_i(r_i)}{p_i}\Big) = -1 \quad \text{for } i = 1, 2, \ldots, m.$$

By the Weak Approximation Theorem [4, p.22], there exists $r \in \mathbb{Q}$ such that $\|r - r_i\|_{p_i} < 1$ for $i = 1, 2, \ldots, m$. Now

$$\|r + r_i\|_{p_i} = \|r - r_i + 2r_i\|_{p_i} \leqslant \max\big\{\|r - r_i\|_{p_i}\,,\ \|2r_i\|_{p_i}\big\} \leqslant 1$$

and

$$\begin{aligned}\|f_i(r)-f_i(r_i)\|_{p_i} &= \|\lambda_i(r^2-r_i^2)+\mu_i(r-r_i)\|_{p_i}\\ &= \|\lambda_i(r+r_i)+\mu_i\|_{p_i}\|r-r_i\|_{p_i}\\ &\leqslant \|r-r_i\|_{p_i}\\ &< 1\end{aligned}$$

for all i. This implies that $\big(\frac{f_i(r)}{p_i}\big)=-1$. (If $b\in\mathbb{Z}_{(p)}$ such that $\|b^2-f_i(r)\|_{p_i}<1$, then

$$\begin{aligned}\|b^2-f_i(r_i)\|_{p_i} &= \|b^2-f_i(r)+f_i(r)-f_i(r_i)\|_{p_i}\\ &\leqslant \max\big\{\|b^2-f_i(r)\|_{p_i}\,,\ \|f_i(r)-f_i(r_i)\|_{p_i}\big\}\\ &< 1,\end{aligned}$$

contradicting $\big(\frac{f_i(r_i)}{p_i}\big)=-1$.) □

5. Classical Laguerre Planes over $\mathbb{Q}$

A classical Laguerre plane $\mathfrak{L}_{\mathbb{Q}}$ defined over $\mathbb{Q}$ may be embedded in affine 3-space $\mathbb{Q}^3$, with point set given by the affine cylinder

$$\mathcal{Q}=\big\{(x,y,z)\in\mathbb{Q}^3\ :\ \lambda x^2+\mu xy+\nu y^2=1\big\}.$$

Circles of $\mathfrak{L}_{\mathbb{Q}}$ are represented by conics lying in the cylinder, these being sections of $\mathcal{Q}$ by planes of the form $z=ax+by+c$ where $a,b,c\in\mathbb{Q}$. Here $\lambda,\mu,\nu\in\mathbb{Q}$ such that the quadratic polynomial $\lambda x^2+\mu xy+\nu y^2\in\mathbb{Q}[x,y]$ is irreducible over $\mathbb{Q}$, i.e. $\mu^2-4\lambda\nu$ is a rational nonsquare. The resulting Laguerre plane may be more precisely designated as $\mathfrak{L}_{\mathbb{Q};\lambda,\mu,\nu}$ since its isomorphism type depends on the choice of coefficients λ,μ,ν; but we continue to write simply $\mathfrak{L}_{\mathbb{Q}}$ instead.

5.1 Theorem. *Let Σ_0 be a finite partial flock of $\mathfrak{L}_{\mathbb{Q}}$, and let $\mathcal{X}_0$ be a finite set of points of $\mathfrak{L}_{\mathbb{Q}}$ not lying on any of the circles C_i. Then there exists a partial flock $\Sigma\supseteq\Sigma_0$ covering all points of $\mathfrak{L}_{\mathbb{Q}}$ except the points of $\mathcal{X}_0$.*

Proof. By Theorem 2.3, it suffices to show that partial flocks of $\mathfrak{L}_{\mathbb{Q}}$ extend recursively in the language of Section 2. Let $C_1,C_2,\dots,C_m$ be finitely many circles of $\mathfrak{L}_{\mathbb{Q}}$. We may assume that C_i is the intersection of the cylinder $\mathcal{Q}$, as above, with the plane

$$z=a_ix+b_iy+c_i$$

where $a_i,b_i,c_i\in\mathbb{Q}$; i=$1,2,\dots,m$. Consider a point $P=(x_0,y_0,z_0)$ of $\mathfrak{L}_{\mathbb{Q}}$ with $P\notin C_1\cup\dots\cup C_m$; then

$$z_0\neq a_ix_0+b_iy_0+c_i\quad\text{for } i=1,2,\dots,m.$$

We will choose C to be the intersection of $\mathcal{Q}$ with the plane

$$z = z_0 + a(x - x_0) + b(y - y_0)$$

passing through P, where $a, b \in \mathbb{Q}$ are to be determined. Choose distinct primes $p_1, \dots, p_m$ such that

(i) every rational solution (x, y) of $\lambda x^2 + \mu xy + \nu y^2 = 1$ has $\|x\|_{p_i} \leqslant 1$ and $\|y\|_{p_i} \leqslant 1$; and

(ii) $\|a_i x_0 + b_i y_0 + c_i - z_0\|_{p_i} = 1$.

Such primes $p_1, \dots, p_m$ exist since there are infinitely many choices for the prime p_i satisfying (i) by Lemma 4.2; and since $a_i x_0 + b_i y_0 + c_i - z_0$ is a nonzero rational number for each i, only finitely many of these choices for p_i are excluded by condition (ii).

By Weak Approximation [4, Theorem 3.1], we may choose $a, b \in \mathbb{Q}$ such that

$$\|a - a_i\|_{p_i} < 1, \quad \|b - b_i\|_{p_i} < 1$$

for $i = 1, 2, \dots, m$. Since $P \in \mathcal{Q}$, by (i) we have $\|x_0\|_{p_i} \leqslant 1$ and $\|y_0\|_{p_i} \leqslant 1$ and so

$$\|(a - a_i)x_0 + (b - b_i)y_0\|_{p_i} \leqslant \max\left\{ \|a - a_i\|_{p_i}, \|b - b_i\|_{p_i} \right\} < 1.$$

Now (ii) yields

$$\|ax_0 + by_0 + c_i - z_0\|_{p_i} = \|(a - a_i)x_0 + (b - b_i)y_0 + (a_i x_0 + b_i y_0 + c_i - z_0)\|_{p_i} = 1.$$

The planes of C and C_i intersect in a line, all of whose points (x, y, z) satisfy

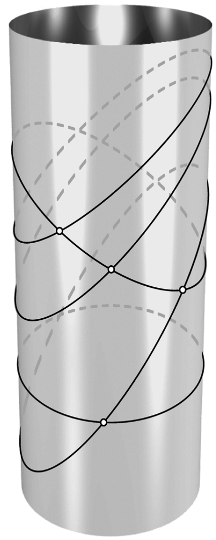
$$(a - a_i)x + (b - b_i)y = ax_0 + by_0 + c_i - z_0 \,.$$

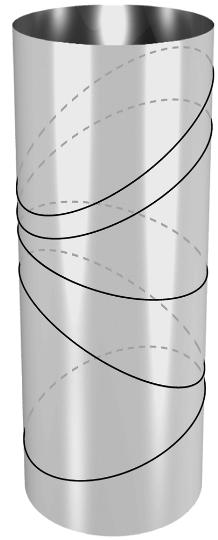
All such pairs (x, y) of rationals must satisfy $\|x\|_{p_i} > 1$ or $\|y\|_{p_i} > 1$ and so $\lambda x^2 + \mu xy + \nu y^2 \neq 1$, i.e. such points cannot lie on the cylinder $\mathcal{Q}$.

Thus $P \in C$ and $C_i \cap C = \varnothing$ for $i = 1, 2, \dots, m$, i.e. $\mathfrak{L}_{\mathbb{Q}}$ extends recursively in the terminology of Section 2. The result follows from Theorem 2.3. $\square$

As a consequence, we obtain the following fact, which was asserted in Theorem 1.1:

Partial flocks of $\mathfrak{L}_{\mathbb{Q}}$
constructed via
Theorem 5.1





Partial flocks of $\mathfrak{L}_{\mathbb{Q}}$
constructed via
Theorem 5.3

5.2 Corollary. *Let δ be any countable cardinal, i.e. $\delta \leqslant \aleph_0$. Then $\mathfrak{L}_{\mathbb{Q}}$ has a partial flock of deficiency δ.*

For the partial flocks of $\mathfrak{L}_{\mathbb{Q}}$ constructed above, pairs of circles have of course no rational intersection points; but they *may* have real intersection points. If this feature seems like cheating, it is however avoidable! We proceed to describe an alternative proof of Corollary 5.2, using partial flocks defined over $\mathbb{Q}$, but whose circles have no real points of intersection (i.e. their closures in $\mathbb{R}^3$ are mutually disjoint)!

Denote by $\mathfrak{L}_{\mathbb{R}}$ the classical real Laguerre plane whose points are represented by the affine cylinder

$$\overline{\mathcal{Q}} = \big\{(x,y,z) \in \mathbb{R}^3 \,:\, \lambda x^2 + \mu xy + \nu y^2 = 1\big\}.$$

Here, and for the remainder of this section, the bar $\overline{}$ denotes closure in $\mathbb{R}^3$ with respect to the standard (Euclidean metric) topology. We continue to assume that $\lambda x^2 + \mu xy + \nu y^2 \in \mathbb{Q}[x,y]$ is irreducible over $\mathbb{Q}$, but now we suppose it is also positive definite (and hence irreducible over $\mathbb{R}$). Circles of $\mathfrak{L}_{\mathbb{R}}$ are represented by conics lying on $\overline{\mathcal{Q}}$, these being intersections of $\overline{\mathcal{Q}}$ with non-vertical planes of $\mathbb{R}^3$. Thus $\mathfrak{L}_{\mathbb{Q}}$ is naturally embedded in $\mathfrak{L}_{\mathbb{R}}$: its points and circles are the $\mathbb{Q}$-rational points and circles of $\mathfrak{L}_{\mathbb{R}}$. Given two circles C, C' of $\mathfrak{L}_{\mathbb{Q}}$, we say C and C' *have no real points of intersection* if their closures (in $\mathbb{R}^3$) satisfy $\overline{C} \cap \overline{C'} = \varnothing$.

5.3 Theorem. *Let $\mathcal{X}_0 = \{R_1, R_2, \ldots, R_n\}$ be a set of n points of $\mathfrak{L}_{\mathbb{Q}}$. Then there exists a partial flock Σ of $\mathfrak{L}_{\mathbb{Q}}$ omitting precisely the points of $\mathcal{X}_0$, and so having deficiency n. Moreover Σ may be chosen such that no two of its circles have real points of intersection.*

The partial flock Σ will be constructed inductively, using the following for the inductive step.

5.4 Lemma. *Let $\Sigma_0 = \{C_1, C_2, \ldots, C_m\}$ be a partial flock of $\mathfrak{L}_{\mathbb{Q}}$. Assume that no two circles of Σ_0 have real points of intersection. Let $P, R_1, R_2, \ldots, R_n$ be a set of distinct points of $\mathfrak{L}_{\mathbb{Q}}$, none of which are covered by Σ_0. Then there exists a circle C of $\mathfrak{L}_{\mathbb{Q}}$ containing P but none of the points $R_1, \ldots, R_m$, and having no real points of intersection with any of the circles of Σ_0.*

Proof. Let $P = (x_0, y_0, z_0)$ and $R_i = (x_i, y_i, z_i)$ for $i = 1, 2, \ldots, n$. The non-vertical (real) planes through P have the form $\pi_{a,b} : z = z_0 + a(x{-}x_0) + b(y{-}y_0)$ for $(a, b) \in \mathbb{R}^2$. Let $U \subset \mathbb{R}^2$ be the set of all pairs (a, b) such that $\pi_{a,b}$ is disjoint from every member of Σ_0. Clearly U is open, and it is not hard to see that U is nonempty. [The circles $\overline{C_1}, \overline{C_2}, \ldots, \overline{C_m}$ divide the cylinder $\overline{\mathcal{Q}}$ into $m{+}1$ connected components, two of which are unbounded. If P lies in a connected component bordered by $\overline{C_1}$ and $\overline{C_2}$, for example, then $\big(ta_1{+}(1{-}t)a_2,\ tb_1{+}(1{-}t)b_2\big) \in U$ where t is the unique solution of

$$t(a_1x_0{+}b_1y_0{+}c_1) + (1{-}t)(a_2x_0{+}b_2y_0{+}c_2) = z_0\,.$$

The case P lies in an unbounded component is easier: if this unbounded component is bordered by $\overline{C_1}$, say, then π_{a_1,b_1} is parallel to the plane of $\overline{C_1}$, and $(a_1, b_1) \in U$.] We let $\overline{C}$ be the intersection of the cylinder $\overline{\mathcal{Q}}$ with the plane $\pi_{a,b}$ where $(a, b) \in U$ is chosen such that

(i) $a, b \in \mathbb{Q}$;

(ii) $(x_i{-}x_0)a + (y_i{-}y_0)b \neq z_i{-}z_0$ for $i = 1, 2, \ldots, n$. (This guarantees that $\pi_{a,b}$ does not pass through any of the points R_i.)

Such $(a, b) \in U$ exists since $U \subset \mathbb{R}^2$ is nonempty and open; $\mathbb{Q}^2 \subset \mathbb{R}^2$ is dense; and (ii) restricts (a, b) to the complement of finitely many lines in $\mathbb{R}^2$ (the requirement that $P \notin \{R_1, R_2, \ldots, R_n\}$). The result of the lemma follows. $\square$

Proof of Theorem 5.3. Enumerate the points of $\mathfrak{L}_{\mathbb{Q}}$ outside $\mathcal{X}_0$ as $P_0, P_1, P_2, \ldots$. We recursively define a chain

$$\Sigma_0 \subseteq \Sigma_1 \subseteq \Sigma_2 \subseteq \cdots$$

of partial flocks of $\mathfrak{L}_{\mathbb{Q}}$ such that

(i) $P_i \in \bigcup \Sigma_j$ whenever $i < j$;

(ii) the partial flock $\Sigma = \bigcup_{j\geqslant 0} \Sigma_j$ satisfies $\bigcup \Sigma = \mathcal{Q} \smallsetminus \mathcal{X}_0$; and

(iii) no two circles in Σ_j, or in Σ, have real points of intersection.

We first set $\Sigma_0 = \varnothing$. For every $j \geqslant 0$:

- If $P_j \in \bigcup \Sigma_j$, set $\Sigma_{j+1} = \Sigma_j$.

- If $P_j \notin \bigcup \Sigma_j$, choose a circle C of $\mathfrak{L}_{\mathbb{Q}}$, passing through P_j, disjoint from $\mathcal{X}_0$ and having no real intersection points with any of the circles of Σ_j . Such a conic exists by Lemma 5.2. Set $\Sigma_{j+1} = \Sigma_j \cup \{C\}$.

Clearly Σ is a partial flock of $\mathfrak{L}_{\mathbb{Q}}$ with the required properties. □

The analogue of Corollary 5.2 holds for classical Minkowski and Möbius planes defined over $\mathbb{Q}$, by a similar argument. The details are left as an exercise.

6. Classical Möbius and Minkowski Planes over $\mathbb{Q}$

Let $\mathfrak{M}_{\mathbb{Q}}$ be a classical Minkowski or Möbius plane over $\mathbb{Q}$, embedded in $\mathbb{P}^3\mathbb{Q}$ as a nondegenerate quadric $\mathcal{Q}$. Let P be a point of $\mathfrak{M}_{\mathbb{Q}}$, and let $C_1, C_2, \ldots, C_m$ be conics in $\mathfrak{M}_{\mathbb{Q}}$ not passing through P.

6.1 Lemma. *We may choose homogeneous coordinates (x, y, z, w) for $\mathbb{P}^3\mathbb{Q}$ with respect to which*

(a) the quadric $\mathcal{Q}$ has equation $\alpha x^2 + \beta y^2 + zw = 0$ for some nonzero rational numbers α and β;

(b) $P = \langle(0, 0, 0, 1)\rangle$;

(c) for each $i = 1, 2, \ldots, m$, the conic C_i lies in the plane $a_i x + b_i y + c_i z + w = 0$ for some $a_i, b_i, c_i \in \mathbb{Q}$ with $\beta a_i^2 + \alpha b_i^2 + 4\alpha\beta c_i \neq 0$;

(d) for each $i = 1, 2, \ldots, m$, we have $(a_i^2 + 4\alpha c_i)c_i \neq 0$; and

(e) for each $i = 1, 2, \ldots, m$, the expression $-(\beta a_i^2 + \alpha b_i^2 + 4\alpha\beta c_i)c_i$ is not a rational square.

Proof. Since the quadric is nonsingular, we may choose a point R of the quadric with $R \notin P^\perp$. Let S, T be two nonsingular points of $\mathbb{P}^3\mathbb{Q}$ spanning the line $\langle P, R\rangle^\perp$ (which is elliptic or hyperbolic, according as $\mathfrak{M}_{\mathbb{Q}}$ is a Möbius plane or a Minkowski plane, respectively). Choose homogeneous coordinates for $\mathbb{P}^3\mathbb{Q}$ such that S, T, R, P are spanned by the four standard basis vectors of $\mathbb{Q}^4$, respectively, and the quadratic form defining the quadric $\mathcal{Q}$ is

$$Q(x, y, z, w) = \alpha x^2 + \gamma xy + \beta y^2 + zw.$$

In particular, (b) holds. In the Minkowski case we may further suppose that $\alpha x^2 + \gamma xy + \beta y^2 = x^2 - y^2$, and in particular $\gamma = 0$. In the Möbius case, we may replace T by $S^\perp \cap \langle S, T\rangle$ if necessary to ensure that $\gamma = 0$ and $\mathcal{Q}$ has the desired form (a). The conic C_i is the intersection of the quadric with a plane defined by

$$a_i x + b_i y + c_i z + w = 0, \qquad a_i, b_i, c_i \in \mathbb{Q};$$

the nonzero coefficient of w is required by the condition that $P \notin C_i$. Since the conic C_i is nondegenerate, we have $\beta a_i^2 + \alpha b_i^2 + 4\alpha\beta c_i \neq 0$. We have now satisfied (a)–(c).

If (d) fails, then we apply an orthogonal transformation

$$(x, y, z, w) \mapsto (x', y', z', w') := (x,\ y{+}sz,\ z,\ w{-}2\beta sy{-}\beta s^2 z)$$

for some $s \in \mathbb{Q}$ to be chosen shortly. The new equation for the plane of C_i is

$$a_i'x' + b_i'y' + c_i'z' + w' = a_i x' + (b_i{+}2\beta s)y' + (c_i{-}b_i s{-}\beta s^2)z' + w' = 0$$

where

$$c_i' = c_i{-}b_i s{-}\beta s^2;$$
$$(a_i')^2 + 4\alpha c_i' = (a_i^2 + 4\alpha c_i) - 4\alpha b_i s - 4\alpha\beta s^2.$$

Since $\alpha\beta \neq 0$, it is possible to choose $s \in \mathbb{Q}$ such that the latter two quantities are nonzero. Replacing the old coordinates (x, y, z, w) and coefficients a_i, b_i, c_i by the new ones, we check that the expression in (c) remains unchanged, and (a)–(d) hold.

To achieve (e), we apply another orthogonal transformation

$$(x, y, z, w) \mapsto (x', y', z', w') := (x{+}tz,\ y,\ z,\ w{-}2\alpha tx{-}\alpha t^2 z)$$

for a rational number t to be chosen shortly. In the new coordinates, the plane of C_i has equation

$$a_i'x' + b_i'y' + c_i'z' + w' = (a_i{+}2\alpha t)x' + b_i y' + (c_i{-}a_i t{-}\alpha t^2)z' + w' = 0.$$

The conditions (a)–(d) remain valid for the new coordinates x, y, z, w and coefficients a_i', b_i', c_i'. The expression in (e) transforms to

$$-\big[\beta(a_i')^2 + \alpha(b_i')^2 + 4\alpha\beta c_i'\big]c_i' = \lambda_i\big(\alpha t^2 + a_i t - c_i\big)$$

where $\lambda_i = \beta a_i^2 + \alpha b_i^2 + 4\alpha\beta c_i$. The latter quadratic polynomial in t has discriminant $\lambda_i^2(a_i^2 + 4\alpha c_i) \neq 0$ for each $i = 1, 2, \ldots, m$. So by Lemma 4.3, there exist $t_1, t_2, \ldots, t_m \in \mathbb{Q}$ such that $\lambda_i(\alpha t_i^2 + a_i t_i - c_i)$ is a rational nonsquare for $i = 1, 2, \ldots, m$. Now by Lemma 4.4, there exists $t \in \mathbb{Q}$ such that $\lambda_i(\alpha t^2 + a_i t - c_i)$ is a rational nonsquare for $i = 1, 2, \ldots, m$. Replacing the old variables x, y, z, w and coordinates a_i, b_i, c_i by the new ones x', y', z', w' and a_i', b_i', c_i', we see that all conclusions (a)–(e) hold. □

6.2 Theorem. *Let Σ_0 be a finite partial flock of $\mathfrak{M}_\mathbb{Q}$, and let $\mathcal{X}_0$ be a finite set of points of $\mathfrak{M}_\mathbb{Q}$ with $\big(\bigcup \Sigma_0\big) \cap \mathcal{X}_0 = \varnothing$. Then there exists a partial flock $\Sigma \supseteq \Sigma_0$ covering all points of $\mathfrak{M}_\mathbb{Q}$ except the points of $\mathcal{X}_0$.*

Proof. By Theorem 2.3, it suffices to show that partial flocks of $\mathfrak{M}_\mathbb{Q}$ extend recursively. Let $C_1, C_2, \ldots, C_m$ be circles of $\mathfrak{M}_\mathbb{Q}$ not passing through a point P. We assume the notation and conclusions of Lemma 6.1; thus $\mathcal{Q} \subset \mathbb{P}^3\mathbb{Q}$ is given by $\alpha x^2 + \beta y^2 + zw = 0$, etc. We will choose C to be the intersection of $\mathcal{Q}$ with the plane

$$ax + by + z = 0$$

passing through P, where $a, b \in \mathbb{Q}$ are to be determined. Recall that for each $i = 1, 2, \ldots, m$, the quantity $-(\beta a_i^2 + \alpha b_i^2 + 4\alpha\beta c_i)c_i$ is a rational nonsquare; thus the binary quadratic form appearing in (i) below has nonsquare discriminant. Choose distinct odd primes $p_1, \ldots, p_m$ such that

(i) every rational solution (x, y) of $(a_i^2 + 4\alpha c_i)x^2 + 2a_ib_ixy + (b_i^2 + 4\beta c_i)y^2 = 1$ has $\|x\|_{p_i} \leqslant 1$ and $\|y\|_{p_i} \leqslant 1$; and

(ii) $\|2c_i\|_{p_i} = 1$.

Such primes $p_1, \ldots, p_m$ exist since there are infinitely many choices for a prime p_i satisfying (i) by Lemma 4.2; and since $c_i \neq 0$, only finitely many of these choices for p_i are excluded by condition (ii).

By Weak Approximation [4, Theorem 3.1], we may choose $a, b \in \mathbb{Q}$ such that

$$\Big\|a - \frac{a_i}{2c_i}\Big\|_{p_i} < 1, \quad \Big\|b - \frac{b_i}{2c_i}\Big\|_{p_i} < 1$$

for $i = 1, 2, \ldots, m$. More is required: In order that C be a nondegenerate conic, it is necessary and sufficient that $ab \neq 0$. We may guarantee this by choosing an additional prime $p_{m+1} \notin \{p_1, p_2, \ldots, p_m\}$ and imposing the further conditions

$$\|a - 1\|_{p_{m+1}} < 1, \quad \|b - 1\|_{p_{m+1}} < 1.$$

By Weak Approximation, we may assume that all these conditions are satisfied by $a, b \in \mathbb{Q}$, and in particular $ab \neq 0$.

Every point of $C \cap C_i$ has the form

$$\langle v_{x,y} \rangle = \langle (x,\ y,\ -ax-by,\ (ac_i-a_i)x+(bc_i-b_i)y) \rangle.$$

One checks that

$$Q(v_{x,y}) = \tfrac{1}{4c_i}\big[(a_i^2+4\alpha c_i)x^2 + 2a_ib_ixy + (b_i^2+4\beta c_i)y^2 - \Delta^2\big]$$

where

$$\Delta = 2c_i\big[\big(a - \tfrac{a_i}{2c_i}\big)x + \big(b - \tfrac{b_i}{2c_i}\big)y\big].$$

Observe that the quadratic form $(a_i^2+4\alpha c_i)x^2 + 2a_ib_ixy + (b_i^2+4\beta c_i)y^2$ cannot vanish nontrivially, since its discriminant $-16(\beta a_i^2 + \alpha_i b_i^2 + 4\alpha\beta c_i)c_i$ is a rational nonsquare.

This means that $Q(v_{x,y})$ and Δ cannot vanish simultaneously for any nonzero rational values of (x, y). Thus every rational solution (x, y) of $Q(v_{x,y}) = 0$ gives a rational solution of

$$(a_i^2+4\alpha c_i)\big(\frac{x}{\Delta}\big)^2 + 2a_ib_i\big(\frac{x}{\Delta}\big)\big(\frac{y}{\Delta}\big) + (b_i^2+4\beta c_i)\big(\frac{y}{\Delta}\big)^2 = 1.$$

By Lemma 4.2, this requires that

$$\Big\|\frac{x}{\Delta}\Big\|_{p_i} \leqslant 1, \quad \Big\|\frac{y}{\Delta}\Big\|_{p_i} \leqslant 1$$

and so

$$\max\big\{\|x\|_{p_i}\,,\ \|y\|_{p_i}\big\} \leqslant \|\Delta\|_{p_i} = \Big\|\Big(a - \frac{a_i}{2c_i}\Big)x + \Big(b - \frac{b_i}{2c_i}\Big)y\Big\|_{p_i} < \max\big\{\|x\|_{p_i}\,,\ \|y\|_{p_i}\big\},$$

a contradiction. We obtain $C \cap C_i = \varnothing$ since the intersection of their respective planes contains no points of $\mathcal{Q}$. Moreover $P \in C$. Thus partial flocks of $\mathfrak{M}_{\mathbb{Q}}$ extend recursively in the terminology of Section 2. The result follows from Theorem 2.3. $\square$

7. Some Partitions of Euclidean Point Sets

We collect here some results required in Section 8.

7.1 Proposition. *Consider a (possibly unbounded) open interval $(a, b) \subseteq \mathbb{R}$ with $-\infty \leqslant a < b \leqslant \infty$, and let $\mathfrak{I} = \big\{[a_\alpha, b_\alpha]\big\}_{\alpha\in A}$ be a family of mutually disjoint closed intervals in (a, b). (Note that α ranges over an index set A; and for every $\alpha \in A$ we have $-\infty < a_\alpha < b_\alpha < \infty$.) Then $|(a, b) \smallsetminus \bigcup\mathfrak{I}| = 2^{\aleph_0}$.*

Proof. The index set A has a total order defined naturally by the condition that $\alpha < \beta$ whenever $a_\alpha < a_\beta$ (or equivalently, the entire interval $[a_\alpha, b_\alpha]$ lies to the left of $[a_\beta, b_\beta]$ on the real line). Suppose that $|(a, b) \smallsetminus \bigcup\mathfrak{I}| < 2^{\aleph_0}$; we aim for a contradiction. Note that $(A, <)$ is dense in the sense that whenever $\alpha < \beta$ in A, then there exists $\gamma \in A$ such that $\alpha < \gamma < \beta$. (Otherwise the open interval (b_α, a_β) of cardinality $2^{\aleph_0}$ is a subset of $(a, b) \smallsetminus \bigcup\mathfrak{I}$, contrary to our assumption.) Clearly A has no least or greatest element, for similar reasons. In particular A is infinite. Actually A is *countably* infinite, as we now explain. For every integer $n \geqslant 1$, let A_n be the set of all $\alpha \in A$ such that the interval $[a_\alpha, b_\alpha]$ has length $b_\alpha - a_\alpha > \frac{1}{n}$. Since every such interval $[a_\alpha, b_\alpha]$ contains a positive finite number of rationals of the form $\frac{k}{n}$ for $k \in \mathbb{Z}$, it is clear that A_n is countable; thus $A = \bigcup_{n\geqslant1} A_n$ is countable. By the theorem on the uniqueness of countable dense total orders without endpoints (see e.g. [3, p.99]) the ordered set $(A, <)$ is equivalent to $(\mathbb{Q}, <)$ and so without loss of generality, $A = \mathbb{Q}$ with the usual order relation '$<$'. For every irrational $r \in \mathbb{R} \smallsetminus \mathbb{Q}$, let $x_r = \sup\{a_\alpha : \alpha \in \mathbb{Q},\ \alpha < r\}$. It is an easy exercise to check that the map $\mathbb{R} \smallsetminus \mathbb{Q} \to (a, b)$, $r \mapsto x_r$ is strictly increasing and hence injective; and that none of the points $x_r \in (a, b)$ are covered by $\mathfrak{I}$. This is a contradiction and so the conclusion of Proposition 7.1 must hold. $\square$

7.2 Corollary. *Let $U \subset \mathbb{R}^2$ be an open disk, and let $\mathcal{D}$ be a collection of mutually disjoint open disks properly contained in U. Then the point set*

$$U \smallsetminus \bigcup_{D\in\mathcal{D}} \overline{D}$$

has cardinality $2^{\aleph_0}$. (Here $\overline{D}$ denotes the closure of D in $\mathbb{R}^2$.)

Proof. The collection $\mathcal{D}$ is countable, since $\mathcal{D} = \bigcup_{n\geqslant 1}\mathcal{D}_n$ where $\mathcal{D}_n$ is the (finite) set of all disks in $\mathcal{D}$ of radius $\geqslant \frac{1}{n}$. Now there are countably many pairs of disks in $\mathcal{D}$, hence countably many points of tangency between pairs of these disks. (We take 'tangent to an open disk D' to mean 'tangent to the circle ∂D bounding D'.) There are also only countably many horizontal lines in $\mathbb{R}^2$ tangent to some disk in $\mathcal{D}$. (A *horizontal line in* $\mathbb{R}^2$ is one parallel to the x-axis.) We may therefore choose a horizontal line ℓ in $\mathbb{R}^2$ such that

$\ell \cap U$ is a (nonempty) open interval;
ℓ is not tangent to any circle in $\mathcal{D}$; and
ℓ does not pass through any point of tangency between two disks in $\{U\}\cup\mathcal{D}$.

It is straightforward to see that the nonempty intersections of the form $\ell\cap\overline{D}$ (for $D\in\mathcal{D}$) is a collection of mutually disjoint closed intervals in the open interval $\ell\cap U$, and therefore $\ell\cap U$ contains $2^{\aleph_0}$ points outside $\bigcup_{D\in\mathcal{D}}\ell\cap\overline{D}$ by Proposition 7.1. $\square$

7.3 Proposition. *Let $U \subset \mathbb{R}^2$ be an open disk, and let Σ be a collection of mutually disjoint circles in U. Then the point set $U\smallsetminus\bigcup\Sigma$ is nonempty.*

Proof. Denote the radius of U by $R>0$. Suppose Σ is a partition of U into circles; we seek a contradiction. Let $C_1\in\Sigma$ be the unique member passing through the center of U; and for every $n\geqslant 1$, let $C_{n+1}\in\Sigma$ be the unique member passing through the center of C_n. Then $C_1, C_2, C_3, \ldots \in \Sigma$ is a nested sequence of circles such that C_n has diameter less than $2^{-n}R$. Let $P\in U$ be the unique point interior to all of the circles C_n. Let $C\in\Sigma$ be the unique member passing through P. Choose $n\geqslant 1$ such that $2^{-n}R$ is less than the diameter of C; then C_n intersects C, a contradiction. $\square$

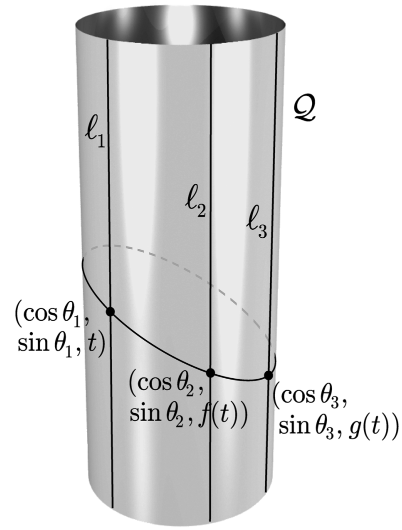
8. Classical Circle Planes over $\mathbb{R}$

Consider first the classical Laguerre plane $\mathfrak{L}_{\mathbb{R}}$ over $\mathbb{R}$, which we may embed in $\mathbb{R}^3$ with point set given by the affine cylinder

$$\mathcal{Q} = \big\{(x,y,z)\in\mathbb{R}^3 \,:\, x^2+y^2=1\big\}.$$

Circles of $\mathfrak{L}_{\mathbb{R}}$ are represented by elliptical intersections of the cylinder with non-vertical planes.

8.1 Theorem. *A partial flock* Σ *of* $\mathfrak{L}_{\mathbb{R}}$ *has deficiency* 0 *or* $2^{\aleph_0}$.



Proof. Suppose Σ has deficiency less than $2^{\aleph_0}$. Then we may choose three distinct lines of the cylinder:

$$\ell_i = \{(\cos\theta_i, \sin\theta_i, z) \,:\, z \in \mathbb{R}\},$$
$$0 \leqslant \theta_1 < \theta_2 < \theta_3 < 2\pi,$$

each of which is covered by Σ. The points of intersection of a typical circle in Σ with the lines ℓ_1, ℓ_2, ℓ_3 have the form

$$(\cos\theta_1, \sin\theta_1, t), \quad (\cos\theta_2, \sin\theta_2, f(t)),$$
$$(\cos\theta_3, \sin\theta_3, g(t))$$

for some $t \in \mathbb{R}$, where the functions $f, g : \mathbb{R} \to \mathbb{R}$ are bijective and increasing, hence continuous. Now the circles of Σ must cover the entire cylinder $\mathcal{Q}$. $\square$

A variant of the latter proof works for the classical Minkowski plane $\mathfrak{M}_{\mathbb{R}}$ over $\mathbb{R}$, which we represent as the ruled quadric

$$\mathcal{Q} = \big\{\langle(x, y, z, w)\rangle \,:\, 0 \neq (x, y, z, w) \in \mathbb{R}^4,\ xy = zw\big\}$$

in $\mathbb{P}^3\mathbb{R}$. The quadric $\mathcal{Q}$ has two families of ruling lines, i.e. reguli. One of these, $\mathcal{R}_1$, consists of the lines

$$\ell_\infty = \langle(1,0,0,0)\,,\ (0,0,0,1)\rangle, \qquad \ell_a = \langle(a,0,1,0)\,,\ (0,1,0,a)\rangle \quad \text{for } a \in \mathbb{R}\,;$$

and the other, $\mathcal{R}_2$, consists of the lines

$$\ell'_\infty = \langle(1,0,0,0)\,,\ (0,0,1,0)\rangle, \qquad \ell'_a = \langle(a,0,0,1)\,,\ (0,1,a,0)\rangle \quad \text{for } a \in \mathbb{R}\,.$$

Every circle of $\mathfrak{M}_{\mathbb{R}}$ meets each line of $\mathcal{R}_1$ exactly once, and also meets each line of $\mathcal{R}_2$ exactly once. The Minkowski plane $\mathfrak{M}_{\mathbb{R}}$ admits a group $G_1 \times G_2$ of automorphisms, where $G_i \cong PGL_2(\mathbb{R})$ permutes the lines of $\mathcal{R}_i$ three-transitively, while fixing every line the other regulus.

8.2 Theorem. *Every partial flock Σ of $\mathfrak{M}_{\mathbb{R}}$ has deficiency* 0 *or* $2^{\aleph_0}$*.*

Proof. Consider a partial flock of deficiency less than $2^{\aleph_0}$. Then there exist three lines of $\mathcal{R}$ (which we may take to be $\ell_0, \ell_1, \ell_\infty$ without loss of generality), each of which is covered by Σ. Similarly, we may assume that each of the lines ℓ'_0, ℓ'_1, ℓ'_∞ is covered by Σ. Moreover, using the group $G_1 \times G_2$, we may assume that the unique circle passing through the three points

$$\ell_0 \cap \ell'_0 = \langle (0,1,0,0) \rangle, \qquad \ell_1 \cap \ell'_1 = \langle (1,1,1,1) \rangle, \qquad \ell_\infty \cap \ell'_\infty = \langle (1,0,0,0) \rangle$$

belongs to Σ. A typical circle in Σ meets the lines $\ell_0, \ell_1, \ell_\infty$ in the points

$$\begin{aligned} \ell_0 \cap \ell'_{\tan t} &= \langle (0, \cos t, \sin t, 0) \rangle, \\ \ell_1 \cap \ell'_{\tan[\frac{\pi}{4}+f(t)]} &= \langle (\cos f(t))(1,1,1,1) + (\sin f(t))(1,-1,1,-1) \rangle, \\ \ell_\infty \cap \ell'_{\tan[\frac{\pi}{2}+g(t)]} &= \langle (\cos g(t), 0, 0, -\sin g(t)) \rangle \end{aligned}$$

for some $t \in [0, \pi)$, respectively, where the functions $f, g : [0,\pi) \to [0,\pi)$ are bijective and satisfy $f(0) = g(0) = 0$. Moreover, both f and g are increasing since no two circles in Σ intersect. It follows that f and g are continuous, and so Σ covers the entire cylinder $\mathcal{Q}$, i.e. its deficiency is zero. $\square$

For the remainder of this section we consider a partial spread Σ of a classical Möbius (i.e. inversive) plane $\mathfrak{I}_{\mathbb{R}}$ over $\mathbb{R}$. We may take $\mathfrak{I}_{\mathbb{R}}$ to be embedded in $\mathbb{R}^3$ with point set given by the sphere

$$\mathcal{Q} = \{(x,y,z) \in \mathbb{R}^3 \,:\, x^2 + y^2 + z^2 = 1\},$$

and with nondegenerate plane sections of $\mathcal{Q}$ as its circles. For every circle C of $\mathfrak{I}_{\mathbb{R}}$, the complement of C consists of two connected components which we call the two *open disks bounded by* C. It is clear that Σ *has deficiency at least 2.* (For if $D_1, D_2 \subset \mathcal{Q}$ are the two open disks bounded by $C \in \Sigma$, then each D_i contains a point not covered by Σ. This follows by stereographically projecting D_i into $\mathbb{R}^2$ and applying Proposition 7.3.)

Let A and B be two distinct points in $\mathfrak{I}_{\mathbb{R}}$; or more generally, two disjoint nonempty point sets in $\mathfrak{I}_{\mathbb{R}}$. We say that a circle C of $\mathfrak{I}_{\mathbb{R}}$ *separates* A *from* B if A lies in one of the two open disks bounded by C, and B lies in the other. The following analogue of Theorems 8.1 and 8.2 applies only when the circles of Σ are 'nested' in a single sequence.

8.3 Theorem. *Let Σ be a partial flock of $\mathfrak{I}_{\mathbb{R}}$. Suppose there exists a pair of points $P, Q \in \mathfrak{I}_{\mathbb{R}}$ such that every circle $C \in \Sigma_0$ separates P from Q. Then the deficiency of Σ is either* 2 *or* $2^{\aleph_0}$.

Proof. We may assume $P = (0,0,1)$ and $Q = (0,0,-1)$, since the automorphism group of $\mathfrak{I}_{\mathbb{R}}$ is doubly (in fact, triply) transitive on points. By a *meridian,* we mean an arc of a great circle from P to Q, i.e. a point set of the form

$$m_\theta = \{(\cos\theta\sin t,\, \sin\theta\sin t,\, \cos t) \,:\, 0 < t < \pi\}, \quad 0 \leqslant \theta < 2\pi.$$

The hypotheses clearly imply that every circle $C \in \Sigma$ meets each meridian exactly once, and that the circles in Σ are totally ordered by height. A straightforward variant of the proof of Theorems 8.1 and 8.2, with meridians of the sphere in place of ruling lines, shows that the set of points of $\mathcal{Q} \smallsetminus \{P, Q\}$ not covered by Σ has cardinality either 0 or $2^{\aleph_0}$. Of course the two points P and Q are themselves not covered by Σ. The result follows. $\square$

We are ready to prove the general case.

8.4 Theorem. *Every partial flock Σ of $\mathfrak{I}_{\mathbb{R}}$ has deficiency* 0 *or* $2^{\aleph_0}$.

Proof. By Theorem 8.3, we may assume that Σ contains three circles C_0, C_1, C_2, none of which separates the other two. For each $C \in \Sigma$, let $D_C \subset \mathcal{Q}$ be the unique open disk bounded by C, containing at most one of the circles C_0, C_1, C_2. (The other open disk bounded by C contains at least two of the circles C_0, C_1, C_2.) If two such open disks D_C and $D_{C'}$ overlap (i.e. $D_C \cap D_{C'} \neq \varnothing$ where $C, C' \in \Sigma$), then one contains the other. Thus the collection of open disks $\widehat{\mathcal{D}} = \{D_C : C \in \Sigma\}$ is partitioned into maximal chains with respect to inclusion. The union of disks in every such maximal chain, is an open disk $D \subset \mathcal{Q}$; and the collection of such open disks D (one for each maximal chain in $\widehat{\mathcal{D}}$) yields a collection $\mathcal{D}$ of open disks in $\mathcal{Q}$ with the following properties, which are easily verified.

(i) $D \cap D' = \varnothing$ for all $D \neq D'$ in $\mathcal{D}$;
(ii) For every $C \in \Sigma$, we have $C \subset \overline{D}$ for some $D \in \mathcal{D}$;
(iii) $|\mathcal{D}| \geqslant 3$.

Choose a disk $D_0 \in \mathcal{D}$ and consider the open disk $U = \mathcal{Q} \smallsetminus \overline{D_0}$. The collection of open disks $\mathcal{D}_1 := \{D \in \mathcal{D} : D \neq D_0\}$ satisfies

(i) $D \cap D' = \varnothing$ for all $D \neq D'$ in $\mathcal{D}_1$;
(ii) Each $D \in \mathcal{D}_1$ is a proper subset of U;
(iii) Every point of $\left(\bigcup \Sigma\right) \cap U$ is covered by $\overline{D}$ for some $D \in \mathcal{D}_1$.

By Corollary 7.2, applied to U (after stereographically projecting into $\mathbb{R}^2$), there are $2^{\aleph_0}$ points of U not covered by $\bigcup_{D\in\mathcal{D}_1} \overline{D}$, hence not covered by Σ. $\square$

References

[1] A. Beutelspacher and P. J. Cameron, 'Transfinite methods in geometry', *Bull. Belg. Math. Soc.* **3** (1994), 337–347.

[2] M. Billiotti and N. L. Johnson, 'Variations on a theme of Dembowski', in: *Mostly Finite Geometries, In Celebration of T. G. Ostrom's 80th Birthday,* ed. N. L. Johnson, Marcel Dekker, N.Y., 1997, pp.139–168.

[3] P. J. Cameron, *Sets, Logic and Categories,* Springer-Verlag, London, 1998.

[4] J. W. S. Cassels, *Local Fields,* Cambridge Univ. Press, Cambridge, 1986.

[5] A. Delandtsheer, 'Dimensional linear spaces', pp.193–294 in: *Handbook of Incidence Geometry: Buildings and Foundations,* ed. F. Buekenhout, Elsevier, Amsterdam, 1995.

[6] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory,* 2nd ed., Springer-Verlag, New York, 1990.

[7] N. L. Johnson and S. E. Payne, 'Flocks of Laguerre planes and associated geometries', in: *Mostly Finite Geometries, In Celebration of T. G. Ostrom's 80th Birthday,* ed. N. L. Johnson, Marcel Dekker, N.Y., 1997, pp.51–122.

[8] J.-P. Serre, *A Course in Arithmetic,* Springer-Verlag, New York, 1973.

[9] G. F. Steinke, 'Topological circle geometries', pp.1325–1354 in: *Handbook of Incidence Geometry: Buildings and Foundations,* ed. F. Buekenhout, Elsevier, Amsterdam, 1995.