50 Fake Planes

Donald Cartwright, University of Sydney
Tim Steger, Università degli Studi di Sassari

completing a project started by

Gopal Prasad, University of Michigan
Sai-Kee Yeung, Purdue University

25 February–1 March, 2019, Luminy

Basic idea of the whole project: suppose $\Pi \subseteq PU(2,1)$ is such that

- Π is a uniform lattice in $\mathrm{PU}(2,1)$,
- Π is torsion free,
- $\Pi/[\Pi,\Pi]$ is finite, and
- $\mathrm{covol}(\Pi)) = 1$.

Then $X = \Pi \backslash B(\mathbf{C}^2)$, the associated quotient of $B(\mathbf{C}^2)$ is a fake projective plane. The first condition implies that X is a compact complex surface, possibly singular. The second implies that X is smooth. The third implies that $b_1(X) = 0$, and so that $b_3(X) = 0$. The fourth implies that $\chi(X) = 3$, hence $b_1(X) = 1$.

Conversely several deep results together imply that any fake projective plane arises in this way. Finally, one knows that such a Π must be arithmetic: Yeung and Klingler, independently.

As was explained yesterday

[Prasad, Yeung, 2007] *Fake projective planes*, Invent. Math. **168**, 321–370

gives a short list of possibilities for *maximal* arithmetic subgroups $\bar{\Gamma} \subset PU(2,1)$ which might contain such a Π. In particular, it gives the covolume of each of these $\bar{\Gamma}$. The covolume calculation depends on Prasad's Covolume Formula from:

[Prasad, 1989] *Volumes of S-arithmetic quotients of semi-simple groups*, Publ. Math., Inst. Hautes Etud. Sci. **69**, 91–117

The idea of starting this project arose because the Covolume Formula was available. Prasad and Yeung also proved the existence of some (but not all) of the fake planes arising from subgroups of these $\bar{\Gamma}$.

Each of the $\bar{\Gamma}$ was described in terms of

- A totally real field k.
- A totally complex extension field ℓ with $[\ell : k] = 2$.
- A central simple algebra $\mathcal{D}$ of degree 3 (and dimension 9) over ℓ.
- A certain collection of *parahoric* groups giving integrality conditions for the elements of $\bar{\Gamma}$.

As it happens, all fake projective planes arise from cases where $\mathcal{D}$ is a division algebra, so I concentrate on that situation. The other possibility is $\mathcal{D} \cong \mathrm{Mat}_{3\times 3}(\ell)$.

The end goal of this lecture is to give more detail on the last item.

Recall that in each case $\mathcal{D}$ admits an involution of the second kind, denoted ι. That is:

1. $\iota^2 = \iota$,

2. $\iota(xy) = \iota(y)\iota(x)$,

3. $\iota(cx) = \bar{c}\iota(x)$ for $c \in \ell$.

We need to use an ι which behaves in the right way at the real places of k. Using a certain Hasse principal, plus some elementary facts about forms over nonarchimedean local fields, one deduces that any two possibilities for such an ι are conjugate by some automorphism of $\mathcal{D}$.

One might consider the following version of the unitary group:

$$\mathbb{U}(k) = \mathbb{U}_\iota(k) = \{x \in \mathcal{D}\,;\ \iota(x)x = 1\}$$

Each $x \in \mathbb{U}(k)$ gives rise to an ℓ-linear automorphism of $\mathcal{D}$ denoted C_x defined by $C_x(y) = xyx^{-1}$. One checks that C_x satisfies $C_x\iota = \iota C_x$. This gives us a map from $\mathbb{U}(k)$ to

$$\mathbb{P}\mathbb{U}(k) = \mathbb{P}\mathbb{U}_\iota(k) = \{C : \mathcal{D} \to \mathcal{D}\,;\ C \text{ is an } \ell\text{-linear automorphism with } C\iota = \iota C\}$$

Using the Skolem–Noether Theorem, which states that all ℓ-linear automorphisms of $\mathcal{D}$ are inner, one sees that each $C \in \mathbb{P}\mathbb{U}(k)$ is in fact C_x for some $x \in \mathbb{U}(k)$. Clearly $C_x = \text{id}$ if and only if x is central, so if and only if $x \in \ell$.

Conclusion: $\mathbb{P}\mathbb{U}(k)$ is a version of the projective unitary group.

Consider a place v of k. This gives rise to an inclusion of fields: $k \to k_v$. For instance if $k = \mathbf{Q}$, and $v = \infty$, then the map is $\mathbf{Q} \to \mathbf{Q}_\infty \cong \mathbf{R}$, while if v "is" some rational prime p, the map is $\mathbf{Q} \to \mathbf{Q}_p$, the p-adic numbers. If $[k : \mathbf{Q}] > 1$ the situation is analogous.

A good reference for places is:

[Weil, 1974] Basic Number Theory, Third Edition, Die Grundlehren der mathematischen Wissenschaften, Band 144, Springer-Verlag, Berlin.

which also has an excellent exposition of central simple algebras in general and of central simple algebras over local fields and over number fields.

What is meant by $\mathbb{PU}(k_v)$? If you know about linear algebraic groups, you already know the answer. A good reference for linear algebraic groups and arithmeticity is

[Zimmer, 1984] Ergodic Theory and Semisimple Groups, Birkhäuser, Boston

First we need to think about $\mathcal{D}_v = \mathcal{D} \otimes_k k_v$.
$\dim(\mathcal{D}/k) = \dim(\mathcal{D}/\ell)\dim(\ell/k) = 18$. Identify $\mathcal{D}$ with k^{18} by fixing a basis $(e_j)_{1\le j\le 18}$. The algebra structure is given by

$$e_j e_k = \sum_m c_{jk}^m e_m$$

for structure constants $c_{jk}^m \in k$.

One concrete way to construct $\mathcal{D}_v$ is to let $\mathcal{D}_v = k_v^{18}$, with multiplication defined by the same structure constants using the inclusion $k \to k_v$.

In the same way one constructs $\ell_v = \ell \otimes_k k_v$, and one has:

$$k_v \hookrightarrow \ell_v \hookrightarrow \mathcal{D}_v$$

From ι one constructs $\iota_v : \mathcal{D}_v \to \mathcal{D}_v$. This is $\iota_v = \iota \otimes \mathrm{id} : \mathcal{D} \otimes_k k_v \to D \otimes_k k_v$. Or more concretely, ι_v is the k_v-linear map $k_v^{18} \to k_v^{18}$ which has the same matrix as the k-linear map $\iota : k^{18} \to k^{18}$.

Similarly, the conjugation map $\ell \to \ell$ gives rise to a conjugation map $\ell_v \to \ell_v$. It is easy to see that ι_v is an involution of the second kind of the algebra $\mathcal{D}_v/\ell_v$ relative to the conjugation map on ℓ_v.

Then

$$\mathbb{P}\mathbb{U}(k_v) = \mathbb{P}\mathbb{U}_\iota(k_v) =$$
$$\{C : \mathcal{D}_v \to \mathcal{D}_v\,;\; C \text{ is an } \ell_v\text{-linear automorphism with } C\iota_v = \iota_v C\}$$

and there is a natural inclusion

$$\mathbb{P}\mathbb{U}(k) \to \mathbb{P}\mathbb{U}(k_v)$$

induced by the inclusion $k \to k_v$.

If $k_v \cong \mathbf{R}$, then $\ell_v \cong \mathbf{C}$ (because ℓ is totally complex) and necessarily $\mathcal{D}_v \cong \mathrm{Mat}_{3\times 3}(\mathbf{C})$. Also $\iota(x) = F^{-1}x^*F$ for some F with $F^* = F$. It follows that $\mathbb{P}\mathbb{U}(k_v) \cong PU(3)$ or $\mathbb{P}\mathbb{U}(k_v) \cong PU(2,1)$, depending on the signature of F.

To get an arithmetic subgroup of $PU(2,1)$ from this construction, it must be that

- For one real place v, $\mathbb{PU}(k_v) \cong PU(2,1)$.
- For any other real place w, $\mathbb{PU}(k_w) \cong PU(3)$.

Since all the fields k on Prasad–Yeung's list satisfy $[k : \mathbf{Q}] \leq 2$, there is at most one place of the second sort.

Then $\mathbb{PU}(k) \hookrightarrow \mathbb{PU}(k_v) \cong PU(2,1)$. This is the sense in which $\mathbb{PU}(k)$ and its subgroups can be considered as subgroups of $PU(2,1)$.

In this situation $\mathbb{PU}(k)$ is what is called a k-form of $PU(2,1)$.

If $k = \mathbf{Q}$, then $\mathbb{PU}(\mathbf{Q})$ is called a rational form of $PU(2,1)$. To get an arithmetic subgroup of $PU(2,1)$ we need to identify a corresponding "integral" form of $PU(2,1)$.

As usual, let $\mathfrak{o}_k$ denote the ring of algebraic integers in k. One has that $x \in \mathfrak{o}_k$ if and only x is integral as an element of k_v for every non-archimedean place v. For $k = \mathbf{Q}$, this translates to saying that $x \in \mathbf{Q}$ is integral if and only if for every prime p it can be expressed using no factor of p in its denominator (duh).

As before, any basis for $\mathcal{D}$ over k determines a bijection $\mathcal{D} \cong k^{18}$. For a very particular sort of basis, the maximal arithmetic subgroups $\bar{\Gamma}$ which Prasad–Yeung specified are given by

$$\bar{\Gamma} = \{C \in \mathbb{PU}(k)\,;\ C(\mathfrak{o}_k^{18}) = \mathfrak{o}_k^{18}\}$$

The condition is that the entries of the matrices for C and C^{-1} must be algebraic integers.

There are many possible bases. If two of them are conjugate under the action of $\mathbb{PU}(k)$, they give rise to conjugate arithmetic subgroups. But even up to conjugacy, there are many possible bases. And only some of them give *maximal* arithmetic subgroups. This looks terribly complicated.

Fortunately, a place by place analysis, based on the **Strong Approximation Theorem** and the Bruhat–Tits theory of buildings, brings order out of chaos.

One fundamental point is that given any two bases of $\mathcal{D}$, the matrix in $GL(18, k)$ converting one to the other is integral in k_v for all but finitely many places v.

The Strong Approximation Theorem is a super-duper version of the Chinese Remainder Theorem. It implies that for each non-archimedean place v of k we can choose which v-adic integrality condition to use, and these choices can be made independently, so long as we make the "standard" choice for all but finitely many primes. Also, the overall condition will be determined, up to conjugacy, by the conjugacy classes of the various v-adic conditions. To be precise, this last depends also on some case-by-case class number calculations.

To specify the integrality condition at the place v, it is necessary and sufficient to specify a subgroup $P_v \subset \mathbb{PU}(k_v)$ so that the v-adic integrality condition is $x \in P_v$ where $x \in \mathbb{PU}(k) \hookrightarrow \mathbb{PU}(k_v)$.

To get a *maximal* arithmetic subgroup, it is necessary that each P_v be maximal compact in $\mathbb{PU}(k_v)$. For the $\bar{\Gamma}$ on Prasad–Yeung's list, the P_v are always of the sort known as *parahoric subgroups*. We proceed to give a little detail about the various possibilities for the P_v.

One says that a place v of k splits over ℓ when there exist a pair of maps $\ell \to k_v$ extending $k \to k_v$. If, for example $\ell = k[\sqrt{-3}]$, then v splits if and only if there is some square root of -3 in k_v.

If v splits over ℓ, then $\ell_v \cong k_v \oplus k_v$ and $\overline{c \oplus d} = d \oplus c$. Also $\mathcal{D}_v = \hat{\mathcal{D}}_v \oplus \hat{\mathcal{D}}_v^{\mathsf{op}}$ where $\hat{\mathcal{D}}_v$ is a central simple algebra of degree 3 over k_v. Moreover, in this case, $\iota_v : \mathcal{D}_v \to \mathcal{D}_v$ maps $\hat{x} \oplus \hat{y}^{\mathsf{op}}$ to $\hat{y} \oplus \hat{x}^{\mathsf{op}}$. From this it follows without difficulty that $\mathbb{PU}(k_v)$ is the projectived version of $\hat{D}_v^{\times}$.

CASE A: v splits over ℓ and $\hat{\mathcal{D}}_v$ is a division algebra.

In this case $\mathbb{PU}(k_v) \cong \mathbb{P}(\hat{D}_v^{\times})$ is itself compact, and one necessarily takes $P_v = \mathbb{PU}(k_v)$. This means that at the place v one doesn't impose any non-trivial integrality condition.

Recall that $\mathcal{T}_0$ is the set of places of this sort. As Cartwright pointed out, for each of the items on Prasad–Yeung's $|\mathcal{T}_0| \leq 1$, and $|\mathcal{T}_0| = 1$ if and only if $\mathcal{D}$ is a division algebra.

CASE B: v splits over ℓ and $\hat{\mathcal{D}}_v \cong \mathrm{Mat}_{3\times 3}(k_v)$.

In this case $\mathbb{PU}(k_v) \cong PGL(3,k_v)$. Let $\mathfrak{o}_v$ denote the integral elements of k_v. Here we take $P_v = PGL(3,\mathfrak{o}_v)$.

Equivalently, if $\mathcal{L} = \mathfrak{o}_v^3$, one may define P_v as the image in $PGL(3,k_v)$ of

$$\{x \in GL(3,k_v)\,;\; x(\mathcal{L}) = \mathcal{L}\} \subset GL(3,k_v)$$

Here $\mathcal{L}$ is what is called a **lattice** in k_v^3, namely a free $\mathfrak{o}_v$-submodule with a 3-element basis. All lattices are in a single orbit under $GL(3,k_v)$. If one changed the lattice in the definition of P_v, it would amount to conjugating P_v by an element of $\mathbb{PU}(k_v) \cong PGL(3,k_v)$. The effect of such a change on $\bar{\Gamma}$ is likewise a conjugation, basically irrelevant.

The set of lattices (modulo multiplication by scalars) give the vertex set of the **building** of $PGL(3,k_v)$. Thus, another way of describing P_v is as the stabilizer of a vertex of that building.

CASE C: v doesn't split over ℓ; **Type 1** parahoric.

When v doesn't split over ℓ, there is exactly one place of ℓ which lies over v. Denote this likewise by v. Then if we define $\ell_v = \ell \otimes_k k_v$, as before, ℓ_v is a field, and the map $\ell \to \ell_v$ is indeed the map associated to the place v of ℓ. We have $[\ell_v : k_v] = 2$, and the conjugation map on ℓ_v is the nontrivial automorphism of ℓ_v over k_v.

Here $\mathcal{D}_v$ is a central simple algebra of degree 3 over ℓ_v. The existence of ι implies that $\mathcal{D}_v \cong \mathcal{D}_v^{\mathsf{op}}$. For a division algebra of degree 3 (or any degree > 2) over a non-archimidean local field, this is impossible. Thus $\mathcal{D}_v \cong \mathrm{Mat}_{3\times 3}(\ell_v)$.

The map $\iota_v : \mathrm{Mat}_{3\times 3}(\ell_v) \to \mathrm{Mat}_{3\times 3}(\ell_v)$ must be of the form $\iota_v(x) = F^{-1}x^*F$ where x^* is calculated using the conjugation map on ℓ_v and where F is some self-adjoint matrix in $\mathrm{Mat}_{3\times 3}(\ell_v)$.

Tracing through the definition of $\mathbb{PU}(k_v) = \mathbb{PU}_\iota(k_v)$, one finds $\mathbb{PU}(k_v) \cong PU(\ell_v^3) = PU(\ell_v^3, \langle \cdot, \cdot \rangle_F)$ where

$$\langle u, v \rangle_F = u^* F v$$

Actually, up to scalars, there is only one conjugacy class of sesquilinear forms on ℓ_v^3, so a change of basis would permit one to use $F = \mathrm{id}$.

For a lattice $\mathcal{L} \in \ell_v^3$, define its **dual** lattice by

$$\mathcal{L}' = \{x \in \ell_v^3; \langle x, \mathcal{L} \rangle_F \subseteq \mathfrak{o}_v\}$$

where here $\mathfrak{o}_v$ stands for the integral subring of ℓ_v. It is easy to verify that $(\mathcal{L}')' = \mathcal{L}$ and that for $x \in U(\ell_v^3)$ one has $(x(\mathcal{L}))' = x(\mathcal{L}')$.

In analogy with CASE B, P_v is defined as the image in $PU(\ell_v^3)$ of

$$\{x \in U(\ell_v^3)\,;\; x(\mathcal{L}) = \mathcal{L}\}$$

for some lattice in ℓ_v^3. In this case, different choices of lattice give rise to non-conjugate P_v. Indeed, only some choices of lattice lead to P_v which are maximal compact.

Here's the problem. If $x \in U(\ell_v^3)$ stabilizes $\mathcal{L}$, it also stabilizes $\mathcal{L}'$. Thus it also stabilizes $\mathcal{L} + \mathcal{L}'$, which is again a lattice. For an arbitrary choice of $\mathcal{L}$, the stabilizer of $\mathcal{L} + \mathcal{L}'$ can be a larger group than the stabilizer of $\mathcal{L}$, and if that is so, then the stabilizer of $\mathcal{L}$ is not maximal compact (and not parahoric either).

In this case, CASE C, one chooses a **Type 1** parahoric; that means one chooses $\mathcal{L}$ self-dual: $\mathcal{L} = \mathcal{L}'$. All Type 1 parahorics are conjugate; equivalently the self-dual lattices lie in a single orbit of $U(\ell_v^3)$.

As Cartwright explained, the building associated to $PU(\ell_v^3)$ is a tree, and (modulo scalars) the self-dual lattices correspond to "half" of its vertices, known as Type 1 vertices.

When v doesn't split over ℓ, the "standard" condition is a Type 1 condition. Thus, one must use a Type 1 condition for all but finitely many places. However, there is another possibility, which can be chosen at finitely many places.

CASE D: v doesn't split over ℓ; **Type 2** parahoric.

All is as in CASE C, but we make a different sort of choice for $\mathcal{L}$. Let $\pi_v \in \mathfrak{o}_v$ be a uniformizer of ℓ_v. Choose $\mathcal{L}$ so that $\pi_v \mathcal{L} \subset \mathcal{L}' \subset \mathcal{L}$. As before define P_v as the image in $PU(\ell_v^3)$ of

$$\{x \in U(\ell_v^3)\,;\; x(\mathcal{L}) = \mathcal{L}\}$$

This parahoric stabilizes both $\mathcal{L}$ and $\mathcal{L}'$.

As Cartwright mentioned, the Type 2 parahorics (or the corresponding lattices $\mathcal{L}$) correspond to the other "half" of the vertices of the tree of $PU(\ell_v^3)$. The action of $PU(\ell_v^3)$ is transitive on either type of vertex, but it never exchanges the two types. Equivalently, any two Type 2 parahorics are conjugate, but they are not conjugate to the Type 1 parahorics.

This means that if two examples of $\bar{\Gamma}$, say $\bar{\Gamma}_1$ and $\bar{\Gamma}_2$ are conjugate, then the corresponding parahorics must be Type 2 at exactly the same places of k.

Let $\mathcal{T}_1$ be the set of places where we are going to use Type 2 parahorics. Then $\mathcal{T}_1$ is part of the data which determine the conjugacy class of $\bar{\Gamma}$. As Cartwright explained, the choice of $\mathcal{T}_1$ influences the covolume of $\bar{\Gamma}$, and for a given choice of k, ℓ, and $\mathcal{D}$, there are never more than 6 possibilities for $\mathcal{T}_1$.

The *only* choice available is the choice between a Type 1 and a Type 2 parahoric when v doesn't split. So the set $\mathcal{T}_1$ gives *all* the additional information needed to determine $\bar{\Gamma}$.

How does this work for concrete calculations? First of all, we choose a basis of $\mathcal{D}$ over k. In principle the choice is arbitrary, but in practice a good choice significantly reduces the work to be done. Using this basis, we identify $\mathcal{D}$ with k^{18}. If if $k = \mathbf{Q}$, this makes $\mathcal{D} \cong \mathbf{Q}^{18}$. If $[k : \mathbf{Q}] = 2$ we also choose a basis of $k/\mathbf{Q}$, and so identify $\mathcal{D}$ with $\mathbf{Q}^{36}$. One chooses the basis of $k/\mathbf{Q}$ so that $\mathbf{Z}^2$ corresponds to $\mathfrak{o}_k$.

Any potential element $x \in \bar{\Gamma}$ has to satisfy the integrality conditions given by the choice of parahorics, more precisely, the choice of the types of the parahorics, in short by the choice of $\mathcal{T}_1$. We start with the naive condition $x \in \mathbf{Z}^{18}$ or $x \in \mathbf{Z}^{36}$. Only rarely will this be just right, but it needs modification at only finitely many primes. Indeed the naive condition as above will correspond to the "standard" integrality condition at all but finitely many places; at all but finitely many places the standard integrality condition is what we wish to use.

To be explicit, when v splits, the standard integrality condition is as in CASE B; when v doesn't split the standard integrality condition is as in CASE C, where the parahoric is Type 1. Thus, the only places where we need a non-standard integrality condition are those in $\mathcal{T}_0$, where we use the non-condition of CASE A, and those of $\mathcal{T}_1$ where we use a condition as in CASE D, a parahoric of Type 2.

As to the unique place in $\mathcal{T}_0$, this always corresponds to a single rational prime, p. No condition should be used at that prime; consequently one should allow powers of p in the denominators of the elements of $x \in \mathbf{Z}^{18}$ or $x \in \mathbf{Z}^{36}$. One knows that the size of that power is limited; in practice it was always enough to ask that $p^4 x$ have integral entries.

For places in $\mathcal{T}_1$, explicit calculations are needed to find a replacement for the naive integrality condition. In particular, one needs to find some explicit lattice $\mathcal{L} \in \ell_v^3$ satisfying $\pi_v \mathcal{L} \subset \mathcal{L}' \subset \mathcal{L}$. Next, one needs to express membership in the corresponding parahoric in terms of congruence conditions on elements of $x \in \mathbf{Z}^{18}$ or $x \in \mathbf{Z}^{36}$.

Similar calculations are necessary for places where a standard integrality condition is desired, but where the naive integrality condition doesn't give one. This tends to happen whenever a place v of k ramifies over ℓ.

These calculations were done by Steger using `GAP` and independently by Cartwright using `REDUCE`.

Once the integrality conditions for $\bar{\Gamma}$ are translated into concrete conditions, one can proceed to search for elements of $\bar{\Gamma}$.

How can one ever be sure that enough elements have been found? That is doable because one knows the covolume of $\bar{\Gamma}$.