

## NOTES ON FINITE LINEAR PROJECTIVE PLANES

### 1. PROJECTIVE PLANES

A *projective plane* is a structure  $\Pi = \langle P, L, \in \rangle$  where  $P$  is a set of points,  $L$  is a set of lines, and  $p \in \ell$  means that the point  $p$  is on the line  $\ell$ , satisfying the following axioms.

- I. Any two points lie on a unique line.
- II. Any two lines intersect in a unique point.
- III. There exist four points, no three on a line.

It follows easily that:

- IV. There exist four lines, no three through a common point.

Since the roles of points and lines are symmetric in a projective plane, we see that the *dual* of a plane,  $\Pi^d = \langle L, P, \ni \rangle$  is also a projective plane. The *duality principle* states that for any property true in all projective planes, the corresponding dual property (obtained by interchanging points and lines) is also true.

**Lemma 1.** *Let  $\Pi$  be a projective plane. If  $p$  is a point not on a line  $\ell$  in  $\Pi$ , then there is a one-to-one correspondence between the lines through  $p$  and the points on  $\ell$ .*

**Theorem 2.** *In a projective plane, the number of points on every line is the same, and that is the same as the number of lines through any point.*

**Corollary 3.** *If  $\Pi$  is a finite projective plane with  $n + 1$  points on every line (and hence  $n + 1$  lines through every point), then  $\Pi$  has  $n^2 + n + 1$  points and  $n^2 + n + 1$  lines.*

The number  $n$  in the above corollary is called the *order* of  $\Pi$ .

The standard construction on a projective plane (to be generalized later) is as follows. Let  $\mathbf{F}$  be a field or a division ring (noncommutative field). The points of  $\Pi_{\mathbf{F}}$  are the standard points  $(x, y)$  with  $x, y \in F$ ; the ideal points  $(m)$  with  $m \in F$ , and the ideal point  $(\infty)$ . The lines are

$$\begin{aligned} \ell_{(m,b)} &= \{(x, y) : y = xm + b\} \cup \{(m)\}, \\ \ell_c &= \{(x, y) : x = c\} \cup \{(\infty)\}, \\ \ell_{\infty} &= \{(m) : m \in F\} \cup \{(\infty)\}. \end{aligned}$$

Now check that  $\Pi_{\mathbf{F}}$  satisfies the axioms (I)–(III).

If  $\mathbf{F}$  is a finite field with  $n$  elements, then  $\Pi_{\mathbf{F}}$  is a finite projective plane of order  $n$ . There is a field  $\mathbf{F}$  with  $n$  elements if and only if  $n$  is a prime power, i.e.,  $n = p^k$  for some prime  $p$  and  $k \geq 1$ . Thus there exists a projective plane

of order  $n$  for every prime power  $n$ . There are other finite planes besides the type just constructed, but so far all the known ones have prime power order. The question we want to address is: *Is there a finite projective plane of non-prime-power order?* More generally, *For what numbers  $n$  is there a projective plane of order  $n$ ?*

The classical result goes as follows.

**Theorem 4.** *A projective plane which satisfies Desargues' Law is isomorphic to  $\Pi_{\mathbf{F}}$  for some division ring  $\mathbf{F}$ .*

Thus we are looking for non-Desarguean planes.

## 2. OTHER STRUCTURES RELATED TO PROJECTIVE PLANES

Let  $\mathbf{A}$  be the  $n^2 + n + 1 \times n^2 + n + 1$  matrix of 0's and 1's which is the *incidence matrix* of a finite projective plane of order  $n$ :  $a_{ij} = 1$  if  $p_i \in \ell_j$ , and  $a_{ij} = 0$  otherwise. If  $\mathbf{I}$  is the identity matrix and  $\mathbf{J}$  is the matrix of all 1's, then  $\mathbf{A}^t \mathbf{A} = n\mathbf{I} + \mathbf{J} = \mathbf{A} \mathbf{A}^t$ . Conversely, if there exists a 0-1 matrix of size  $n^2 + n + 1 \times n^2 + n + 1$  satisfying those equations, then it is the incidence matrix of a projective plane.

A *latin square* is an  $n \times n$  array with entries  $0, \dots, n - 1$  such that each integer  $k$  with  $0 \leq k \leq n - 1$  occurs exactly once in each row and column. For example, the operation table for a loop is always a latin square. Two  $n \times n$  latin squares  $\mathbf{A}$  and  $\mathbf{B}$  are *orthogonal* if the  $n^2$  pairs  $(a_{ij}, b_{ij})$  are all distinct, in which case each of the  $n^2$  possible pairs  $(c, d)$  occurs exactly once.

**Theorem 5.** *For every  $n \geq 2$ , there are at most  $n - 1$  mutually orthogonal latin squares of size  $n$ . There exists a set of  $n - 1$  mutually orthogonal  $n \times n$  latin squares if and only if there is a projective plane of order  $n$ .*

As an example, let  $\mathbf{F}$  be a finite field with  $n = p^k$  elements, which we denote by the integers  $0, 1, \dots, n - 1$ . For each  $x \neq 0$ , let  $\mathbf{L}^x$  be the  $n \times n$  array with  $\mathbf{L}_{ij}^x = xi + j$ . Then  $\mathbf{L}^1, \dots, \mathbf{L}^{n-1}$  is a set of  $n - 1$  mutually orthogonal latin squares. Note that  $\mathbf{L}^1$  is the addition table for  $\mathbf{F}$ , and the rows of the other squares are permutations of that.

Another representation of projective planes is that they correspond to complemented modular lattices of length 3 with at least 3 points on each line. We have not discussed this, but it is often a useful way to look at them.

An *affine plane* is a structure  $\mathbf{A} = \langle P, L, \in \rangle$  where  $P$  is a set of points,  $L$  is a set of lines, and  $p \in \ell$  means that the point  $p$  is on the line  $\ell$ , satisfying the following axioms.

- I. Any two points lie on a unique line.
- II'. Given a point  $p$  and a line  $\ell$ , there is exactly one line  $k$  through  $p$  parallel to  $\ell$ , i.e., such that  $\ell \cap k = \emptyset$ .
- III. There exist three noncolinear points.

It follows from (I) that two distinct lines intersect in at most one point. Moreover, parallelism is transitive: if  $a \parallel b \parallel c$ , then  $a \parallel c$  by (II'). Hence we can divide the lines into equivalence classes of parallel lines.

The fundamental theorem relating projective and affine planes goes as follows.

**Theorem 6.** *Given a projective plane, we can obtain an affine plane by removing any line and all the points it contains. Given an affine plane, we can construct a projective plane by adding one point for each equivalence class of parallel lines and a line containing all these points.*

For example, if  $\mathbf{F}$  is a field, we obtain an affine plane  $\mathbf{A}_{\mathbf{F}}$  by removing the line  $\ell_{\infty}$ , leaving just the standard points  $(x, y)$  and the lines of the form  $\ell_{(m,b)}$  and  $\ell_c$ . An affine plane of order  $n$  has  $n^2$  points and  $n^2 + n$  lines; each line contains  $n$  points and each point is on  $n + 1$  lines.

### 3. DOUBLE LOOPS

In this section we want to generalize the construction of projective planes coordinatized by a field given earlier.

A *loop* is an algebra  $\mathbf{L} = \langle L, *, e \rangle$  with the properties

- (1)  $a * e = a$  and  $e * a = a$  for every  $a \in R$ ,
- (2) every equation  $a * x = b$  has a unique solution,
- (3) every equation  $y * c = d$  has a unique solution.

(No other properties are assumed for the operation  $*$ .)

A *double loop* is an algebra  $\mathbf{R} = \langle R, +, \cdot, 0, 1 \rangle$  such that

- (1)  $\langle R, +, 0 \rangle$  is a loop,
- (2)  $\langle R - \{0\}, \cdot, 1 \rangle$  is a loop,
- (3)  $x0 = 0$  and  $0x = 0$  for every  $x \in R$ .

For example, every field is a double loop.

**Lemma 7.** *A finite algebra  $\mathbf{R} = \langle R, +, \cdot, 0, 1 \rangle$  is a double loop if and only if it satisfies the following properties.*

- (1)  $x + y = x + z$  implies  $y = z$ .
- (2)  $y + x = z + x$  implies  $y = z$ .
- (3)  $x + 0 = x$ .
- (4)  $0 + x = x$ .
- (5)  $x0 = 0$ .
- (6)  $0x = 0$ .
- (7)  $xy = xz$  implies  $y = z$  for  $x \neq 0$ .
- (8)  $yx = zx$  implies  $y = z$  for  $x \neq 0$ .
- (9)  $x1 = x$ .
- (10)  $1x = x$ .

**Theorem 8.** *A double loop coordinatizes a projective plane if and only if it has the following two properties.*

- A. Given  $m, m', b, b'$  with  $m \neq m'$ , there is a unique  $x \in R$  such that  $xm + b = xm' + b'$ .
- B. Given  $a, a', c, c'$  with  $a \neq a'$ , there is a unique pair  $x, y \in R$  such that  $ax + y = c$  and  $a'x + y = c'$ .

The first property reflects the fact that, in an affine plane, two nonparallel lines should intersect in a unique point. The second property says that two points determine a unique line. Note that property (B) says exactly that the squares  $\mathbf{L}^a$  defined by  $\mathbf{L}_{xy}^a = ax + y$  are pairwise orthogonal. (For  $a \neq 0$  these are latin squares.)

A double loop which coordinatizes a projective plane is called a *coordinatizing* double loop, and a projective plane which can be coordinatized by a double loop is called a *linear* projective plane.

Of course, every field is a coordinatizing double loop. *Hall quasifields* provide another type of example. Let  $\mathbf{F}$  be a field, and let  $f(x) = x^2 - rx - s$  be an irreducible polynomial over  $\mathbf{F}$ . Then let  $\mathbf{H} = \langle H, +, \circ, 0, 1 \rangle$  where  $H$  is the set of all expressions  $a + bu$  with  $a, b \in F$ . Addition is defined naturally, and multiplication by

$$(a + bu) \circ (c + du) = \begin{cases} ac + bcu & \text{if } d = 0, \\ (ac - bd^{-1}f(c)) + (ad - bc + br)u & \text{if } d \neq 0. \end{cases}$$

As long as  $\mathbf{F}$  has more than two elements,  $\mathbf{H}$  is a coordinatizing double loop which is not a field.

Not every projective plane is linear. Coordinatizing nonlinear projective planes requires a more general type of structure known as a *ternary ring*. Ternary rings have a ternary operation  $T(x, m, b)$ , which in the special case of linear planes is given by  $T(x, m, b) = xm + b$ . They must also satisfy certain conditions, which for double loops become properties (A) and (B) above.

**Theorem 9.** *In a finite double loop, property (A) and property (B) are equivalent.*

*Proof.* Index the equations in property (A) by quadruples  $(m, m', b, b')$  with  $m \neq m'$ , and index the systems in property (B) by quadruples  $(a, a', c, c')$  with  $a \neq a'$ . In each case there are  $n^3(n-1)$  quadruples (disregarding the fact that the equations/systems are equivalent in pairs by interchanging primed and unprimed elements).

First, let  $\mathbf{R}$  satisfy property (A), and suppose some system as in (B) had two solutions,  $x, y$  and  $x', y'$ . Then

$$\begin{aligned} ax + y = c &= ax' + y' \\ a'x + y = c' &= a'x' + y' \end{aligned}$$

whence by property (A), as  $a \neq a'$ , we get  $x = x'$ . It then follows that also  $y = y'$ .

Now note that each pair  $x, y$  is the solution of  $n(n-1)$  such systems with  $a \neq a'$ . There are  $n^2$  pairs  $x, y$  none of which is the solution of two systems. Hence all  $n^3(n-1)$  systems have a solution.

Conversely, assume that  $\mathbf{R}$  satisfies property (B). Suppose  $m \neq m'$  and that the equation  $xm + b = xm' + b'$  had two solutions, say

$$\begin{aligned} xm + b = c &= xm' + b' \\ ym + b = d &= ym' + b' \end{aligned}$$

with  $x \neq y$ . Then the system

$$\begin{aligned} xs + t &= c \\ ys + t &= d \end{aligned}$$

has two solutions  $(m, b)$  and  $(m', b')$ , contrary to assumption.

There are  $n^3(n-1)$  equations  $xm + b = xm' + b'$  with  $m \neq m'$ , and each  $x$  solves  $n^2(n-1)$  of them (varying  $b'$ ). Since no equation has two solutions, all  $n^3(n-1)$  equations have a solution.  $\square$

Recall that two planes  $\Pi = \langle P, L, \in \rangle$  and  $\Psi = \langle Q, K, \in \rangle$  are *isomorphic* if there exist one-to-one, onto maps  $\sigma : P \rightarrow Q$  and  $\tau : L \rightarrow K$  such that  $p \in \ell$  if and only if  $\sigma(p) \in \tau(\ell)$ .

The multiplicative identity element 1 has played no role so far. Define a *pre-double loop* to be an algebra  $\mathbf{R} = \langle R, +, \cdot, 0 \rangle$  satisfying the remaining properties 1–8 of Lemma 7. A *coordinatizing pre-double loop* is one which satisfies the properties (A) and (B), which are still equivalent, and are still sufficient to construct a projective plane.

The next two lemmate combine to show that we can transform a coordinatizing pre-double loop  $\mathbf{R}$  into a coordinatizing double loop  $\mathbf{R}''$ . Moreover, in doing so, the multiplicative identity element 1 can be chosen arbitrarily from among the nonzero elements of  $R$ .

**Lemma 10.** *Let  $\mathbf{R} = \langle R, +, \cdot, 0 \rangle$  be a coordinatizing pre-double loop. Let  $k$  be a nonzero element of  $R$ . For each  $x \in R$ , let  $\alpha(x)$  be the unique element such that  $\alpha(x)k = x$ . Define  $x * y = \alpha(x)y$ . Then  $\mathbf{R}' = \langle R, +, *, 0 \rangle$  is a coordinatizing pre-double loop and  $x * k = x$  for all  $x \in R$ . Moreover,  $\Pi_{\mathbf{R}}$  is isomorphic to  $\Pi_{\mathbf{R}'}$ .*

*Proof.* Note that  $\alpha$  is a permutation of  $R$ , and  $\alpha(0) = 0$ . Then check that the properties for a coordinatizing pre-double loop are preserved. The isomorphism of  $\Pi_{\mathbf{R}}$  to  $\Pi_{\mathbf{R}'}$  is given by  $\sigma(x, y) = (\alpha^{-1}(x), y)$ ,  $\sigma(m) = (m)$ ,  $\sigma(\infty) = (\infty)$  and  $\tau(\ell_{(m,b)}) = \ell_{(m,b)}^*$ ,  $\tau(\ell_c) = \ell_{\alpha^{-1}(c)}$ ,  $\tau(\ell_\infty) = \ell_\infty$ .  $\square$

**Lemma 11.** *Let  $\mathbf{R}' = \langle R, +, *, 0 \rangle$  be a coordinatizing pre-double loop. Further assume that  $\mathbf{R}'$  contains an element  $k$  such that  $x * k = x$  for all  $x \in R$ . Let  $u$  be a nonzero element of  $R$ . For each  $y \in R$ , let  $\beta(y)$  be the unique element such that  $u * \beta(y) = y$ . Define  $x \circ y = x * \beta(y)$ . Then  $\mathbf{R}'' = \langle R, +, \circ, 0 \rangle$  is a coordinatizing double loop with  $u$  as the identity element for multiplication. Moreover,  $\Pi_{\mathbf{R}'}$  is isomorphic to  $\Pi_{\mathbf{R}''}$ .*

*Proof.* Note that  $\beta$  is a permutation of  $R$ ,  $\beta(0) = 0$  and  $\beta(u) = k$ . Then check that the properties for a coordinatizing pre-double loop are preserved.

The isomorphism of  $\Pi_{\mathbf{R}'}$  to  $\Pi_{\mathbf{R}''}$  has  $\sigma(x, y) = (x, y)$ ,  $\sigma(m) = (\beta^{-1}(m))$ ,  $\sigma(\infty) = (\infty)$  and  $\tau(\ell_{(m,b)}^*) = \ell_{(\beta^{-1}(m),b)}^\circ$ ,  $\tau(\ell_c) = \ell_c$ ,  $\tau(\ell_\infty) = \ell_\infty$ .  $\square$

#### 4. THE ORDER OF A FINITE PROJECTIVE PLANE

The classic result on the order of finite projective planes is the Bruck-Ryser Theorem.

**Theorem 12.** *If  $n \equiv 1$  or  $n \equiv 2 \pmod{4}$  and  $n$  is not the sum of two squares, then there is no projective plane of order  $n$ .*

The following table summarizes what is known about small orders.

- (1) Too small.
- (2) Yes - one plane up to isomorphism.
- (3) Yes - one plane up to isomorphism.
- (4) Yes - one plane up to isomorphism.
- (5) Yes - one plane up to isomorphism.
- (6) No - Tarry (1900) or Bruck-Ryser.
- (7) Yes - one plane up to isomorphism.
- (8) Yes - one plane up to isomorphism.
- (9) Yes - four planes up to isomorphism.
- (10) No - C. Lam et. al. (1989).
- (11) Yes
- (12) Unknown.
- (13) Yes
- (14) No - Bruck-Ryser.
- (15) Unknown.
- (16) Yes.
- (17) Yes.
- (18) Unknown.
- (19) Yes.
- (20) Unknown.
- (21) No - Bruck-Ryser.
- (22) No - Bruck-Ryser.
- (23) Yes.
- (24) Unknown.
- (25) Yes.
- (26) Unknown.
- (27) Yes.
- (28) Unknown.
- (29) Yes.
- (30) No - Bruck-Ryser.

Let  $\lambda(n)$  denote the size of the largest set of mutually orthogonal latin squares of order  $n$  ( $\geq 2$ ). Here is a summary of what we know about  $\lambda(n)$ .

- (1)  $\lambda(n) \leq n - 1$  with equality holding if  $n$  is a prime power (since there is a projective plane of order  $n = p^k$ ).

- (2) For all  $n \neq 2$  or  $6$ ,  $\lambda(n) \geq 2$ .
- (3) For all  $n \geq 52$ ,  $\lambda(n) \geq 4$ .
- (4)  $\lambda(12) \geq 5$ .

A *cartesian group* is a coordinatizing double loop in which the additive loop is associative (a group). For example, a Hall quasifield is a cartesian group. The next two results are due to Baumert and Hall, and Studnicka, respectively.

**Theorem 13.** *There is no cartesian group of order 12.*

**Theorem 14.** *There is no finite cartesian group of order  $n = 2m$  with  $m$  odd and  $m \geq 3$ .*

For  $p = 2, 3, 5, 7, 11$  and  $13$ , the field is the only cartesian group of order  $p$ . It is not known whether this is true for all primes  $p$  (though it may be known for some higher values than  $13$ ).

Now let us start to concentrate on planes of order 12. A result of Bierbrauer states that the addition table of a coordinatizing double loop of order 12 (if one exists) cannot have a  $5 \times 5$  latin subsquare. There are similar restrictions on subsquares of the addition table for other orders.

It is useful to have estimates on the number of double loops  $\mathbf{R} = \langle R, +, \cdot, 0, 1 \rangle$  of order  $n$ . Let  $\alpha(n)$  be the number of loop tables on the set  $\{0, \dots, n-1\}$  with 0 as the additive identity element. Let  $\delta(n)$  be the number of double loops on  $\{0, \dots, n-1\}$  with 0 as the additive identity and 1 the multiplicative identity. Clearly  $\delta(n) = \alpha(n) \cdot \alpha(n-1)$ . For  $n \leq 9$ ,  $\alpha(n)$  is known.

$$\begin{aligned}
 \alpha(1) &= 1 \\
 \alpha(2) &= 1 \\
 \alpha(3) &= 1 \\
 \alpha(4) &= 4 \\
 \alpha(5) &= 56 \\
 \alpha(6) &= 9408 \\
 \alpha(7) &= 16,942,080 \\
 \alpha(8) &= 535,281,401,856 \\
 \alpha(9) &= 377,597,570,964,258,816
 \end{aligned}$$

For larger  $n$  we have the following rough estimates, which give us some idea of the size of the problem.

**Lemma 15.** *The number  $\alpha(n)$  of additive loop tables  $\mathbf{L} = \langle L, +, 0 \rangle$  on a set of  $n$  elements satisfies*

$$\begin{aligned}
 (n-1)(n-3)^3(n-4)^2(n-5)^5(n-6)^4 \dots 1 &\leq \alpha(n) \\
 &\leq (n-1)(n-2)^3(n-3)^5(n-4)^7 \dots 1.
 \end{aligned}$$

**Corollary 16.** *The number of additive loop tables on  $\{0, \dots, 11\}$  is between  $1.8 \times 10^{28}$  and  $1.8 \times 10^{63}$ . The number of multiplicative loop tables per addition table is between  $7.5 \times 10^{21}$  and  $1.2 \times 10^{49}$ . Thus the total number of double loop tables (with 0 and 1) is between  $1.3 \times 10^{50}$  and  $2.2 \times 10^{112}$ .*

That's a lot.

Our division into cases is based on the cycle structure of the operation  $x \mapsto 1 + x$ , with the cycle containing 0 being distinguished and listed first. The cases are as follows.

- (1) 2-2-2-2-2-2 (TAB)
- (2) 2-2-2-3-3
- (3) 2-2-2-2-4
- (4) 2-2-2-6
- (5) 2-2-3-5
- (6) 2-2-4-4
- (7) 2-3-3-4
- (8) 2-3-7
- (9) 2-4-6
- (10) 2-5-5
- (11) 2-10 (TEN)
- (12) 3-3-3-3 (MKB)
- (13) 3-3-2-4 (ASD)
- (14) 3-3-2-2-2 (ZXC)
- (15) 3-3-6
- (16) 3-2-2-5
- (17) 3-2-7
- (18) 3-4-5 (RTY)
- (19) 3-9
- (20) 4-2-2-2-2
- (21) 4-4-2-2
- (22) 4-4-4 (FOR)
- (23) 4-3-3-2
- (24) 4-3-5
- (25) 4-2-6
- (26) 4-8
- (27) 5-2-2-3
- (28) 5-2-5
- (29) 5-3-4
- (30) 5-7
- (31) 6-2-2-2 (QWE)
- (32) 6-2-4
- (33) 6-3-3
- (34) 6-6 (SIX)
- (35) 7-3-2
- (36) 7-5 (SEV)

(37) 8–2–2

(38) 8–4

(39) 9–3

(40) 10–2

(41) 12

The cases marked with three letters (e.g., TAB) are the ones we are currently investigating. So far, between these cases, we have shown that roughly 77 million addition tables are not the addition for a coordinatizing double loop.

### 5. QUASIFIELDS

The most general class of double loops which has been studied systematically is the class of quasifields. A *quasifield* is a double loop  $\mathbf{Q} = \langle Q, +, \cdot, 0, 1 \rangle$  such that

- (1)  $+$  is associative,
- (2)  $(a + b)c = ac + bc$  for all  $a, b, c \in Q$ ,
- (3) Given  $m, m', c$  with  $m \neq m'$ , there is a unique  $x \in Q$  such that  $xm = xm' + c$ .

In other words, a quasifield is a cartesian group which satisfies the right distributive law.

**Lemma 17.** *Let  $\mathbf{Q}$  be a finite double loop in which addition is associative and the right distributive law holds. Then*

- (1)  $(-a)b = -ab$  for all  $a, b \in Q$ ,
- (2)  $\langle Q, +, 0 \rangle$  is an elementary abelian  $p$ -group, i.e., there is a prime  $p$  such that  $|Q| = p^k$  and every element of  $\mathbf{Q}$  has additive order  $p$ , and
- (3) property (3) above also holds, so  $\mathbf{Q}$  is a quasifield.

*Proof.* The first two properties follow from the fact that, for any  $m \neq 0$ , the map  $\tau_m : x \mapsto xm$  is an automorphism of  $\langle Q, +, 0 \rangle$ . In particular, the automorphism group of  $\langle Q, +, 0 \rangle$  is transitive.

For the third property, we note that our assumptions ensure that for  $m \neq m'$  the map  $\sigma_{m,m'} : x \mapsto -xm' + xm$  is one-to-one (and hence onto).  $\square$

Let  $\mathbf{F}$  be a finite field of order  $q = p^k$  say, and let  $Q = \mathbf{F}^d$  be a vector space of dimension  $d$  over  $\mathbf{F}$ . (It is convenient to regard the elements of  $Q$  as row vectors.) The first projection embeds  $\mathbf{F}$  into  $\mathbf{Q}$ , so we can identify  $c \in \mathbf{F}$  with the vector  $(c, 0, \dots, 0) \in \mathbf{Q}$ . Suppose that we can find a set of linear transformations  $\rho(m)$  ( $m \in Q$ ) such that

- i.  $\rho(0) = O$ ,
- ii.  $\rho(1) = I$  and the first row of  $\rho(v)$  is  $v$ ,
- iii.  $\rho(m) - \rho(m')$  is nonsingular whenever  $m \neq m'$ .

If we define multiplication by  $u \circ v = u\rho(v)$ , then  $\mathbf{Q}$  is a quasifield.

For example, we obtain the Hall quasifields by taking  $Q = \mathbf{F}^2$  and, for an irreducible quadratic  $x^2 - rx - s$  over  $\mathbf{F}$ ,

$$\rho(c, 0) = \begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix}$$

and, for  $d \neq 0$ ,

$$\rho(c, d) = \begin{pmatrix} c & d \\ -d^{-1}f(c) & -c + r \end{pmatrix}.$$

Similarly, the *Walker quasifields* are constructed by taking  $\mathbf{F}$  to be a field of order  $q$  with  $q \equiv 5 \pmod{6}$ , letting  $\mathbf{Q} = \mathbf{F}^2$ , and

$$\rho(c, d) = \begin{pmatrix} c & d \\ -\frac{1}{3}d^3 & c - d^2 \end{pmatrix}.$$

The construction of *generalized André quasifields* is a little more sophisticated, and requires some finite field theory. Let  $\mathbf{F}$  be a field of order  $q = p^k$ , and let  $\mathbf{Q}$  be a field of order  $q^d$ . Recall that

- (1)  $\mathbf{F} \leq \mathbf{Q}$  and  $\mathbf{Q}$  is a vector space over  $\mathbf{F}$ ,
- (2) the elements of  $\mathbf{F}$  satisfy  $x^q = x$ ,
- (3) the elements of  $\mathbf{Q}$  satisfy  $x^{q^d} = x$ ,
- (4) for any  $r \geq 0$  and  $a, b \in \mathbf{Q}$  we have  $(a + b)^{p^r} = a^{p^r} + b^{p^r}$ .

Let  $\lambda : \mathbf{Q} \rightarrow \mathbf{Z}_d$  be any map such that

- i.  $\lambda(0) = 0$ ,
- ii.  $\lambda(1) = 0$ ,
- iii. if  $m \neq m'$  are nonzero, then the equation  $x^{q^{\lambda(m)} - q^{\lambda(m')}} = m'm^{-1}$  has no solution.

Then the mappings  $\rho(m) : a \mapsto a^{q^{\lambda(m)}}m$  are linear transformations on  $\mathbf{Q}$  satisfying the conditions for a quasifield.

The next result shows that every finite quasifield can be obtained by the general construction described above.

**Theorem 18.** *Let  $\mathbf{Q}$  be a finite quasifield. Let*

$$K = \{k \in \mathbf{Q} : k(ab) = (ka)b \text{ and } k(a + b) = ka + kb \text{ for all } a, b \in \mathbf{Q}\}.$$

*Then  $K$  is a field,  $Q$  is a left vector space over  $K$ , and  $\rho(m) : x \mapsto xm$  is a linear transformation. Thus  $\mathbf{Q}$  can be obtained by the above construction.*

The proof is long but not hard, so we will omit it.

## 6. SUBPLANES

Let  $\Pi = \langle P, L, \in \rangle$  be a projective plane. We say that a plane  $\Pi^* = \langle P^*, L^*, \in \rangle$  is a *subplane* of  $\Pi$  if

- (1)  $P^* \subseteq P$ ,
- (2)  $L^* \subseteq L$ ,
- (3) the line through any two points in  $P^*$  is in  $L^*$ ,
- (4) the intersection of any two lines in  $L^*$  is a point in  $P^*$ .

Unless  $\Pi^* = \Pi$ , the points in  $P^*$  will also be on lines not in  $L^*$ , and the lines in  $L^*$  will also contain points not in  $P^*$ .

Let  $\mathbf{R} = \langle R, +, \cdot, 0, 1 \rangle$  be a double loop. We say that  $\mathbf{S} = \langle S, +, \cdot, 0, 1 \rangle$  is a *sub-double loop* of  $\mathbf{R}$  if

- (1)  $S \subseteq R$ ,
- (2)  $0, 1 \in S$ ,
- (3) if  $s, t \in S$ , then  $s + t \in S$  and  $st \in S$ ,
- (4) if  $s, t \in S$  and  $s \neq 0$ , then the solutions of the equations  $x + s = t$ ,  $s + y = t$ ,  $zs = t$  and  $sw = t$  are also in  $S$ .

We write  $\mathbf{S} \leq \mathbf{R}$  to indicate that  $\mathbf{S}$  is a sub-double loop of  $\mathbf{R}$ . (Sub-pre-double loops are defined similarly, except we do not require  $1 \in S$ , and the results which follow are valid for sub-pre-double loops.)

For example, a subfield  $\mathbf{F}$  of a field  $\mathbf{K}$  is a sub-double loop. Likewise, in our construction of quasifields above, the field  $\mathbf{F}$  is a sub-double loop of the quasifield  $\mathbf{Q}$ .

**Theorem 19.** *If  $\mathbf{R}$  is a finite coordinatizing double loop, and  $\mathbf{S} \leq \mathbf{R}$ , then  $\mathbf{S}$  is a coordinatizing double loop, and the plane  $\Pi_{\mathbf{S}}$  is naturally embedded as a subplane of  $\Pi_{\mathbf{R}}$ .*

*Proof.* Let  $\mathbf{S} \leq \mathbf{R}$ . In  $\Pi_{\mathbf{R}}$ , let  $P^*$  consist of the points  $(s, t)$  with  $s, t \in S$ ; the ideal points  $(u)$  with  $u \in S$ , and the ideal point  $(\infty)$ . Let  $L^*$  consist of the lines  $\ell_{(s,t)}$  with  $s, t \in S$ ; the lines  $\ell_u$  with  $u \in S$ , and the line  $\ell_{\infty}$ . In order to show that this is a subplane of  $\Pi$ , it suffices to show that  $\mathbf{S}$  satisfies condition (A).

Let  $|S| = m$ . Then there are  $m^3(m-1)$  quadruples  $(s, t, s', t')$  in  $S^4$  with  $s \neq s'$ . Each  $x \in S$  solves  $m^2(m-1)$  of the equations  $xs + t = xs' + t'$ , since  $x, s, t$  and  $s'$  determine  $t'$ . If one of these equations had no solution in  $S$ , then another would have two solutions, which is impossible because  $\mathbf{R}$  satisfies (A).

(The analogous theorem is true when  $\mathbf{R}$  is a possibly infinite quasifield.)

□

However, not every subplane comes from a sub-double loop. Hanna Neumann showed that every plane coordinatized by a Hall quasifield contains a 7-element subplane of order 2.

The following theorem of Bruck shows that the order of a subplane is relatively small.

**Theorem 20.** *Let  $\Pi$  be a projective plane of order  $n$ . If  $\Pi^*$  is a proper subplane of order  $m$ , then either  $m^2 = n$  or  $m^2 + m \leq n$ .*

**Corollary 21.** *Let  $\mathbf{R}$  be a coordinatizing double loop of order  $n$ . If  $\mathbf{S}$  is a proper sub-double loop of order  $m$ , then either  $m^2 = n$  or  $m^2 + m \leq n$ .*

Another approach to trying to find planes of non-prime power order is to look for subplanes of non-Desarguean planes whose structure is tractable, e.g., planes coordinatized by quasifields.

## 7. COORDINATIZATION

Let  $\Pi = \langle P, L, \in \rangle$  be a projective plane. In this section, we want to find an algebra  $\mathbf{R}$  which coordinatizes  $\Pi$ , i.e.,  $\mathbf{R}$  should provide coordinates for the points and equations for the lines of  $\Pi$ . In general,  $\mathbf{R}$  will not be a double loop, but rather a *ternary ring*, an algebra with a single ternary operation  $T(x, y, z)$  satisfying certain properties given below.

Let  $X, Y, O, I$  be any quadrangle (4 points, no 3 on a line) in  $\Pi$ . The idea is to make  $O = (0, 0)$  and  $I = (1, 1)$ . The line  $OI$  will be the line  $y = x$ . The line  $XY$  will be the line at infinity, with  $OX$  the  $x$ -axis and  $OY$  the  $y$ -axis. With this scheme in mind, we proceed with the official definitions.

Let  $O = (0, 0)$  and  $I = (1, 1)$  and  $XY \cap OI = (1)$ . Choose a set  $R$  which contains 0, 1 and is in one-to-one correspondence with the points of  $OI - (1)$ , and let  $B = R - \{0, 1\}$ . For example, if  $\Pi$  has order  $n$  we could take  $B = \{2, \dots, n-1\}$ . Assign the rest of the points on  $OI$  distinct labels  $(b, b)$  with  $b \in B$ . For any point  $P$  not on  $XY$  or  $OI$ , assign  $P$  the coordinates  $(a, b)$  where  $YP \cap OI = (a, a)$  and  $XP \cap OI = (b, b)$ . For any point  $Q$  on  $XY$  with  $Q \neq Y$ , the line  $OQ$  contains a unique point  $(1, m)$  with first coordinate 1; assign  $Q$  the coordinate  $(m)$ . Finally, let  $Y = (\infty)$ .

Now let us label the lines of  $\Pi$ . Let  $\ell_\infty$  denote the line  $XY$ . Note that  $\ell_\infty$  contains  $(1)$ . If  $\ell$  is any other line through  $Y$  except  $\ell_\infty$ , then  $\ell$  intersects  $OI$  in some point  $(c, c)$ . In this case, every point except  $Y$  on  $\ell$  has coordinates  $(c, y)$  for some  $y$ , and we let  $\ell = \ell_c$ . We have labelled all the lines through  $Y$ . If  $k$  is a line not through  $Y$ , then  $k \cap \ell_\infty = (m)$  and  $k \cap \ell_0 = (0, b)$  for some pair  $m, b$ . In this case, let  $k = \ell_{(m, b)}$ .

Now we observe that the lines  $\ell_{(m, b)}$  have the property that they never contain two points with the same  $x$ -coordinate, since the line through  $(c, y)$  and  $(c, y')$  is  $\ell_c$ . On the other hand, for every  $c \in R$ ,  $\ell_{(m, b)} \cap \ell_c$  is some standard point  $(c, y)$ . Thus we can use these lines to define a ternary operation  $T(x, m, b)$  on  $R$  by

$$T(x, m, b) = y \quad \text{iff} \quad (x, y) \in \ell_{(m, b)}.$$

The geometric properties of  $\Pi$  are reflected in the algebraic properties of  $T$ .

**Theorem 22.** *The ternary operation  $T$  defined above satisfies the following.*

- T1.  $T(0, m, c) = T(a, 0, c) = c$ .
- T2.  $T(1, m, 0) = T(m, 1, 0) = m$ .
- T3. Given  $m, b, d$  with  $m \neq 0$  there exists exactly one  $x$  such that  $T(x, m, b) = d$ .
- T4. Given  $a, b, d$  with  $a \neq 0$  there exists exactly one  $y$  such that  $T(a, y, b) = d$ .
- T5. Given  $a, m, d$  there exists exactly one  $z$  such that  $T(a, m, z) = d$ .
- T6. Given  $m, m', b, b'$  with  $m \neq m'$  there exists exactly one  $x$  such that  $T(x, m, b) = T(x, m', b')$ .
- T7. Given  $a, a', c, c'$  with  $a \neq a'$  there exists exactly one pair  $m, b$  such that  $T(a, m, b) = c$  and  $T(a', m, b) = c'$ .

A ternary algebra  $\mathbf{R} = \langle R, T, 0, 1 \rangle$  satisfying T1–T7 is called a *ternary ring*. Of course, we have already met some ternary rings.

**Theorem 23.** *Let  $\mathbf{D} = \langle D, +, \cdot, 0, 1 \rangle$  be a double loop satisfying conditions (A) and (B). Define  $T(x, m, b) = xm + b$ . Then  $\mathbf{D}' = \langle D, T, 0, 1 \rangle$  is a ternary ring.*

Note that the ternary ring  $\mathbf{R}$  constructed to coordinatize  $\Pi$  depends on the choice of the quadrangle  $X, Y, O, I$ . In general, different quadrangles can give non-isomorphic (even non-isotropic) ternary rings. The exception to this is the class of Desargean planes. These are the planes  $\Pi_{\mathbf{F}}$  for some division ring  $\mathbf{F}$ ; in this case, the ternary rings are always isomorphic to the one obtained by taking  $T(x, m, b) = xm + b$  with the operations in  $\mathbf{F}$ . This is because the automorphism group of  $\Pi_{\mathbf{F}}$  is transitive on the quadrangles, i.e., there is always an automorphism taking any quadrangle to any other quadrangle.

The conditions T1–T7 are not independent. T1 and T6 together imply T3, and T1 and T7 imply T4. Moreover, if  $R$  is finite, then using T5 we see that T6 is equivalent to T7, exactly as in the proof of Theorem 9.

Given a ternary ring  $\mathbf{R}$ , we can construct a projective plane  $\Pi_{\mathbf{R}}$  in the usual way, except that now we use  $\ell_{(m,b)} = \{(x, y) : y = T(x, m, b)\}$ . In fact, we don't even need all the properties of a ternary ring.

**Theorem 24.** *Let  $\mathbf{R} = \langle R, T \rangle$  be a ternary algebra satisfying T5–T7. Then  $\Pi_{\mathbf{R}}$  is a projective plane, and the order of  $\Pi_{\mathbf{R}}$  is the cardinality of  $R$ .*

As an application, suppose that  $\mathbf{L}^{(1)}, \dots, \mathbf{L}^{(n-1)}$  are a set of  $n - 1$  mutually orthogonal  $n \times n$  latin squares on  $n = \{0, \dots, n - 1\}$ . Define a ternary operation  $T$  by

$$T(i, j, k) = \begin{cases} k & \text{if } i = 0, \\ \mathbf{L}_{jk}^{(i)} & \text{if } i \neq 0. \end{cases}$$

Then  $\mathbf{N} = \langle n, T \rangle$  is a ternary algebra satisfying T5–T7. Thus the existence of  $n - 1$  MOLSS of order  $n$  implies the existence of a projective plane of order  $n$  (coordinatized by  $\mathbf{N}$ ).

For the converse, suppose there exists a projective plane  $\Pi$  of order  $n$ . Let  $\mathbf{R} = \langle n, T \rangle$  be a ternary ring coordinatizing  $\Pi$ . For each  $i \neq 0$ , let  $\mathbf{L}^i$  be the  $n \times n$  square with  $\mathbf{L}_{jk}^i = T(i, j, k)$ . Then conditions T1 and T7 imply that  $\mathbf{L}^1, \dots, \mathbf{L}^{n-1}$  is a set of  $n - 1$  mutually orthogonal latin squares.

Finally, we note that for any ternary ring  $\mathbf{R}$ , we can define addition and multiplication by

$$\begin{aligned} x + b &= T(x, 1, b) \\ xm &= T(x, m, 0). \end{aligned}$$

Then conditions T1 and T2 give us the familiar properties

$$\begin{aligned} 0 + a &= a + 0 = a \\ 0m &= m0 = 0 \\ 1m &= m1 = m. \end{aligned}$$

However, in general there is no reason for  $T(x, m, b) = xm + b$ , i.e., the equation  $T(x, m, b) = T(T(x, m, 0), 1, b)$ , to hold. When this does happen for some ternary ring  $\mathbf{R}$  coordinatizing  $\Pi$ , we say that  $\Pi$  is *linear*. The smallest nonlinear projective plane has order 9.

### 8. HOMOGENEOUS COORDINATES AND DUALITY

If  $\mathbf{D}$  is a division ring, then the lattice representing  $\Pi_{\mathbf{D}}$  is isomorphic to the lattice of subspaces of the vector space  $\mathbf{D}^3$ . In this section we will introduce homogeneous coordinates to see how this comes about. With a slight adjustment, we can introduce homogeneous coordinates for planes coordinatized by a class of Cartesian groups including quasifields, which is useful for calculating in these planes. This leads to a natural coordinatization of the dual  $\Pi_{\mathbf{R}}^d$  of a plane coordinatized by a cartesian group  $\mathbf{R}$ .

So let  $\mathbf{D}$  be a division ring, and let  $\mathbf{V} = {}_{\mathbf{D}}\mathbf{D}^3$  be the left vector space. Define an equivalence relation  $\approx$  on the nonzero vectors of  $\mathbf{V}$  by  $\mathbf{x} \approx \mathbf{y}$  if there exists  $a \in \mathbf{D}$  such that  $\mathbf{x} = a\mathbf{y}$ . Let  $[\mathbf{x}]$  denote the  $\approx$ -equivalence class of  $\mathbf{x}$ . Clearly these correspond to one dimensional subspaces of  $\mathbf{V}$ .

Similarly, let  $\mathbf{V}' = \mathbf{D}^3_{\mathbf{D}}$  be the right vector space, and let  $\equiv$  be the equivalence relation defined on the nonzero vectors of  $\mathbf{V}'$  by  $\mathbf{x} \equiv \mathbf{y}$  if  $\mathbf{x} = \mathbf{y}b$  for some  $b \in \mathbf{D}$ . Let  $\langle \mathbf{x} \rangle$  denote the  $\equiv$ -equivalence class of  $\mathbf{x}$ .

Let  $\mathbf{x} \cdot \mathbf{y} = x_1y_1 + x_2y_2 + x_3y_3$  be the standard dot product in  $\mathbf{D}^3$ .

**Lemma 25.** *There is a one-to-one correspondence between the 2-dimensional subspaces of  $\mathbf{V}$  and the  $\equiv$ -classes, such that  $\mathbf{x} \in \langle \mathbf{z} \rangle$  if and only if  $\mathbf{x} \cdot \mathbf{z} = 0$ .*

Thus we can coordinatize  $\Pi_{\mathbf{D}}$  as follows. The points are labeled by  $\approx$ -classes  $[\mathbf{x}]$  and the lines by  $\equiv$ -classes  $\langle \mathbf{z} \rangle$ , corresponding to one and two dimensional subspaces of  $\mathbf{V}$ , respectively. Incidence is determined by  $[\mathbf{x}] \in \langle \mathbf{z} \rangle$  if and only if  $\mathbf{x} \cdot \mathbf{z} = 0$ .

To mimic the homogeneous coordinates for an arbitrary coordinatizing double loop  $\mathbf{R}$ , we must abandon the projective equivalences  $\approx$  and  $\equiv$ , since multiplication is not in general associative. Instead, points will correspond to certain subsets of  $\mathbf{R}^3$ , which we will still denote by  $\mathbf{x} = [x_1, x_2, x_3]$ , and lines will correspond to a slightly different set, and will be denoted by  $\langle \mathbf{z} \rangle = \langle z_1, z_2, z_3 \rangle$ . Incidence will still be determined by  $[\mathbf{x}] \in \langle \mathbf{z} \rangle$  if and only if  $\mathbf{x} \cdot \mathbf{z} = 0$ , where in the absence of associativity we specify that  $\mathbf{x} \cdot \mathbf{z} = (x_1z_1 + x_2z_2) + x_3z_3$ .

To avoid confusion, we proceed carefully. Let  $\mathbf{R} = \langle R, +, \cdot, 0, 1 \rangle$  be a double loop satisfying conditions (A) and (B). Let  $\Pi_{\mathbf{R}}$  denote the projective

plane constructed from  $\mathbf{R}$  with points  $(x, y)$ ,  $(m)$  and  $(\infty)$ , and lines  $\ell_{mb}$ ,  $\ell_c$  and  $\ell_\infty$ , as usual.

We construct a second plane  $\mathbf{T}_\mathbf{R}$  from  $\mathbf{R}$  as follows. The points of  $\mathbf{T}_\mathbf{R}$  are all triples of one of the following forms:

$$[x, 1, y] \quad \text{or} \quad [1, 0, m] \quad \text{or} \quad [0, 0, 1].$$

The lines of  $\mathbf{T}_\mathbf{R}$  are all triples of one of the following forms:

$$\langle m, b, 1 \rangle \quad \text{or} \quad \langle 1, c, 0 \rangle \quad \text{or} \quad \langle 0, 1, 0 \rangle.$$

Again,  $[\mathbf{x}] \in \langle \mathbf{z} \rangle$  if the left associated dot product  $\mathbf{x} \cdot \mathbf{z} = 0$ .

**Theorem 26.** *If  $\mathbf{R}$  is a coordinatizing double loop, then  $\mathbf{T}_\mathbf{R}$  is a projective plane isomorphic to  $\Pi_\mathbf{R}$ .*

*Proof.* Let  $-y$  denote the element such that  $y + (-y) = 0$ . (The element  $y^-$  such that  $(y^-) + y = 0$  might be different.) Let  $\tau : \Pi_\mathbf{R} \rightarrow \mathbf{T}_\mathbf{R}$  be the mapping such that

$$\begin{aligned} (x, y) &\mapsto [x, 1, -y] \\ (m) &\mapsto [1, 0, -m] \\ (\infty) &\mapsto [0, 0, 1] \\ \ell_{(m,b)} &\mapsto \langle m, b, 1 \rangle \\ \ell_c &\mapsto \langle 1, -c, 0 \rangle \\ \ell_\infty &\mapsto \langle 0, 1, 0 \rangle. \end{aligned}$$

Clearly  $\tau$  is a bijection, and we must check that  $p \in \ell$  if and only if  $\tau(p) \in \tau(\ell)$ . The critical calculation is that

$$\begin{aligned} (x, y) \in \ell_{(m,b)} &\text{ iff } xm + b = y \\ &\text{ iff } (xm + b) + (-y) = 0 \\ &\text{ iff } (x, 1, -y) \cdot (m, b, 1) = 0 \\ &\text{ iff } [x, 1, -y] \in \langle m, b, 1 \rangle. \end{aligned}$$

□

Recall that if  $\Pi$  is a projective plane, the dual plane  $\Pi^d$  is obtained by interchanging the points and lines of  $\Pi$  and reversing its incidence relation. Homogeneous coordinates show that, at least for a Cartesian group, the dual plane  $\pi_\mathbf{R}^d$  is coordinatized by  $\mathbf{R}^{opp}$ .

If  $\mathbf{R} = \langle R, +, \cdot, 0, 1 \rangle$  is a double loop, then  $\mathbf{R}^{opp} = \langle R, \oplus, \circ, 0, 1 \rangle$  is the double loop with  $x \oplus y = y + x$  and  $x \circ y = y \cdot x$ .

**Theorem 27.** *Let  $\mathbf{R}$  be a Cartesian group. Then  $\mathbf{T}_\mathbf{R}$  is isomorphic to  $\mathbf{T}_{\mathbf{R}^{opp}}^d$ .*

*Proof.* First, note that in a group  $zyx = e$  if and only if  $xzy = e$ , and that the opposite algebra of a group is a group. Now consider the bijection

$\delta : \mathbf{T}_{\mathbf{R}} \rightarrow \mathbf{T}_{\mathbf{R}^{opp}}$  such that  $\delta : [a, b, c] \mapsto \langle a, c, b \rangle$  and  $\delta : \langle d, e, f \rangle \mapsto [d, f, e]$ .  
 We claim that  $\delta$  is a dual isomorphism, i.e.,  $p \in \ell$  if and only if  $\delta(p) \ni \delta(\ell)$ .

In fact, using the observation above,

$$\begin{aligned}
 [a, b, c] \in \langle d, e, f \rangle & \text{ iff } ad + be + cf = 0 \\
 & \text{ iff } f \circ c \oplus e \circ b \oplus d \circ a = 0 \\
 & \text{ iff } d \circ a \oplus f \circ c \oplus e \circ b = 0 \\
 & \text{ iff } [d, f, e] \circ \langle a, c, b \rangle = 0 \\
 & \text{ iff } \delta(\langle d, e, f \rangle) \in \delta([a, b, c]).
 \end{aligned}$$

□