J. Aust. Math. Soc. **106** (2019), 184–199
doi:10.1017/S1446788718000095

COORDINATISING PLANES OF PRIME POWER ORDER USING FINITE FIELDS

ROBERT S. COULTER

(Received 10 December 2017; accepted 7 February 2018; first published online 22 August 2018)

Communicated by M. Giudici

Abstract

We revisit the coordinatisation method for projective planes by considering the consequences of using finite fields to coordinatise projective planes of prime power order. This leads to some general restrictions on the form of the resulting planar ternary ring (PTR) when viewed as a trivariate polynomial over the field. We also consider how the Lenz–Barlotti type of the plane being coordinatised impacts the form of the PTR polynomial, thereby deriving further restrictions.

2010 *Mathematics subject classification*: primary 51E15; secondary 12E05, 05B25.

Keywords and phrases: projective planes, polynomials over finite fields, planar ternary rings, coordinatisation method.

1. Introduction

This paper is concerned with two interlinked areas in the study of projective planes—namely the coordinatisation method and the Lenz–Barlotti classification—and their study through the medium of polynomials over finite fields. The coordinatisation method takes an arbitrary projective plane and produces a trivariate function known as a *planar ternary ring* (PTR) over whatever set is used as the labelling set during the coordinatisation process. The Lenz–Barlotti classification is a coarse classification system for affine and projective planes centred on the transitive behaviour exhibited by the full automorphism group of the plane. There is a well-known interaction between the properties exhibited by the PTR and the Lenz–Barlotti type of the plane, and this interaction has played a pivotal role in the theory of projective planes over the past 60 years. Our objective in this paper is to introduce the theory of polynomials over finite fields as an additional tool to be used in this interaction, at least in the case of planes of prime power order. Given the breadth of background knowledge involved, the paper

The results of this article were presented as part of a plenary talk given at the National Conference on Coding Theory and Cryptography 2017 (1–4 September), in Hangzhou, China.

is, at times, somewhat expository in nature, and the theory developed herein should be viewed mainly as a tool. It offers multiple avenues of future research.

We begin, in Section 2, by discussing the coordinatisation method, and describe how this leads to the concept of the planar ternary ring. We then restrict ourselves to projective planes of prime power order. (Of course, anyone who believes the prime-power conjecture is true would view this as no restriction at all; the present author is not willing to express any view on that conjecture's validity, at least not in print!) This allows us to use finite fields in the coordinatisation process, and so the resulting PTR can be treated as a reduced trivariate polynomial over a finite field, what we call a *PTR polynomial*. In Section 4 we derive restrictions on the form of the PTR polynomial using the functional properties that any PTR must exhibit. As will be seen, several forms of reduced permutation polynomials and κ-polynomials (both of which we shall define below) naturally arise from this relation. The culmination of the results of this section, and the main statement in this general situation, is given in Theorem 4.8.

In Section 5 we outline the Lenz–Barlotti classification system for projective planes. It is generally well known that knowledge of the Lenz–Barlotti type of a projective plane $\mathcal{P}$ can lead to additional algebraic properties of the PTR obtained from coordinatising it, but this only occurs when some effort is made to coordinatise the plane in an optimal way. We make explicit what we mean by optimal coordinatisation, and utilise this concept to obtain further restrictions on the form of the PTR polynomial under various assumptions concerning the Lenz–Barlotti type. (While the idea of optimal coordinatisation has been known in a folklore sense for many years, the author is not aware of anywhere specific where this is recorded.) We show how, in suitable circumstances, one can coordinatise suitable planes so that either the additive or multiplicative loop resulting from the coordinatisation is exactly the same as its corresponding field operation, and consider how this can affect the form of the PTR polynomial. Theorems 5.2 and 5.4 are the main results of this section. We end with some concluding remarks concerning potential future directions; in particular, we outline the two main ideas the author had in mind when originally turning to the research of this paper.

2. Coordinatisation

The method of coordinatisation has been used now for over 70 years. There are at least three standard coordinatisation methods. Although they are all essentially equivalent, they produce slightly different properties in the resulting PTRs. We shall use the process outlined by Hughes and Piper in [8, Ch. 5]: they give the two other methods at the end of that same chapter. An extended version of this paper, containing a full description of the method along with diagrams, can be found on arXiv.

Let $\mathcal{P}$ be a projective plane of order n and let $\mathcal{R}$ be any set of cardinality n; this set and the symbol ∞ are the only symbols required to produce a coordinate system for the plane. We designate two special elements of $\mathcal{R}$ by 0 and 1 for reasons which will become clear. The coordinatisation process begins by choosing a quadrangle $\mathbf{O\,x\,y\,I}$

https://doi.org/10.1017/S1446788718000095 Published online by Cambridge University Press

of the plane. These four points, which play the critical role in the method, are labelled $\mathbf{O} = (0,0)$, $\mathbf{x} = (0)$, $\mathbf{y} = (\infty)$ and $\mathbf{I} = (1,1)$.

The coordinatisation method now proceeds to introduce coordinates to all points and lines of the plane. At its conclusion, the plane $\mathcal{P}$ consists of:

- the points $(x,y) \in \mathcal{R} \times \mathcal{R}$;
- the points (a) with $a \in \mathcal{R} \cup \{\infty\}$;
- the lines $[m,k]$, $m,k \in \mathcal{R}$, which are specifically the lines joining (m) with $(0,k)$;
- the lines $[a]$ with $a \in \mathcal{R}$, which consist of the points (a,y) with $y \in \mathcal{R}$ and (∞);
- the line $[\infty]$, which consists of the points (a), $a \in \mathcal{R}$, and (∞).

From this coordinatisation, one now defines a trivariate function T on $\mathcal{R}$, called a *planar ternary ring*, by setting $T(m,x,y) = k$ if and only if $(x,y) \in [m,k]$. This PTR will exhibit certain properties and is actually equivalent to the projective plane as any three variable function exhibiting those properties can be used to define a projective plane. More precisely, we have the following important result, essentially due to Hall [6]; see also Hughes and Piper, [8, Theorem 5.1].

Lemma 2.1 (Hall [6, Theorem 5.4]). *Let $\mathcal{P}$ be a projective plane of n and $\mathcal{R}$ be any set of cardinality n. Let $T : \mathcal{R}^3 \to \mathcal{R}$ be a PTR obtained from coordinatising $\mathcal{P}$. Then T must satisfy the following properties:*

(a) $T(a,0,z) = T(0,b,z) = z$ *for all* $a,b,z \in \mathcal{R}$;
(b) $T(x,1,0) = x$ *and* $T(1,y,0) = y$ *for all* $x,y \in \mathcal{R}$;
(c) *if* $a,b,c,d \in \mathcal{R}$ *with* $a \neq c$, *then there exists a unique* x *satisfying* $T(x,a,b) = T(x,c,d)$;
(d) *if* $a,b,c \in \mathcal{R}$, *then there is a unique* z *satisfying* $T(a,b,z) = c$;
(e) *if* $a,b,c,d \in \mathcal{R}$ *with* $a \neq c$, *then there is a unique pair* (y,z) *satisfying* $T(a,y,z) = b$ *and* $T(c,y,z) = d$.

Conversely, any trivariate function T defined on $\mathcal{R}$ which satisfies properties (c)–(e) can be used to define an affine plane $\mathcal{A}_T$ of order q as follows:

- *the points of $\mathcal{A}$ are (x,y), with $x,y \in \mathcal{R}$;*
- *the lines of $\mathcal{A}$ are the symbols $[m,a]$, with $m,a \in \mathcal{R}$, defined by*

$$[m,a] = \{(x,y) \in \mathcal{R} \times \mathcal{R} : a = T(m,x,y)\},$$

and the symbols $[c]$, with $c \in \mathcal{R}$, defined by

$$[c] = \{(c,y) : y \in \mathcal{R}\}.$$

It is customary to define an addition $\oplus$ and multiplication $\odot$ by

$$x \oplus y = T(1,x,y),$$
$$x \odot y = T(x,y,0),$$

for all $x,y \in \mathcal{R}$. It is well known that the properties of the plane guarantee that both $\oplus$ and $\odot$ are loops with identities 0 and 1 over $\mathcal{R}$ and $\mathcal{R}^\star$, respectively. A PTR is

https://doi.org/10.1017/S1446788718000095 Published online by Cambridge University Press

called *linear* over $\mathcal{R}$ if $T(x, y, z) = (x \odot y) \oplus z$ for all $x, y, z \in \mathcal{R}$; that is, if T can be reconstructed from only knowing the operations $\oplus$ and $\odot$. We mention an important example. Consider the polynomial $T(X, Y, Z) = XY + Z$. It is easily checked that the polynomial T is a linear PTR over any field $\mathcal{K}$; it defines the Desarguesian plane in every case. It cannot be overemphasised that the same plane can yield many different PTRs as choosing different quadrangles as the reference points $\mathbf{O}, \mathbf{x}, \mathbf{y}$ and $\mathbf{I}$ may yield very different PTRs. This is discussed further in Section 5.

3. Coordinatising using finite fields

Throughout the remainder of the paper we fix $q = p^e$ for some prime p and natural number e. We use $\mathbb{F}_q$ to denote the finite field of q elements and $\mathbb{F}_q^\star$ its nonzero elements. Every function on $\mathbb{F}_q$ can be represented uniquely by a polynomial in $\mathbb{F}_q[X]$ of degree less than q; this follows at once from Lagrange interpolation, and indeed this observation is easily extended to the multivariate case. Any polynomial whose degree in each variable is less than q is called *reduced*.

One can choose any set $\mathcal{R}$ of cardinality n for the labelling of points in the coordinatisation process, but since the coordinatisation method will produce an algebraic structure on the set chosen, there are obviously good and bad choices. The resulting function will often exhibit additional algebraic structure, inherited from the plane, so algebraic sets are obvious candidates. For example, regardless of the plane, the points $\mathbf{O}$ and $\mathbf{I}$ determine two special elements, zero and one respectively, of the coordinatisation which have properties much the same as 0 and 1 in any ring with unity. Since the labelling during the coordinatisation process is arbitrary, by choosing a ring of order n with unity, we may label the zero and one of the coordinatisation as the 0 and 1 of the ring.

We now move to make the previous paragraph much more formal in the case where the plane has prime power order q. Let $\mathcal{P}$ be a projective plane of order q. In the coordinatisation process, if we use the finite field $\mathbb{F}_q$ as the labelling set, then the PTR obtained through coordinatisation will be a function in three variables defined over $\mathbb{F}_q$, and consequently can be viewed as (reduced) polynomial $T \in \mathbb{F}_q[X, Y, Z]$. Furthermore, since the correspondence of elements in the coordinatisation and the elements of $\mathbb{F}_q$ is arbitrary, we may set the zero and one of the coordinatisation of $\mathcal{P}$ to be the elements 0 and 1 of $\mathbb{F}_q$.

Definition 3.1. A *PTR polynomial* $T(X, Y, Z)$ *over* $\mathbb{F}_q$ is any three-variabled polynomial in $\mathbb{F}_q[X, Y, Z]$ resulting from the coordinatisation of a plane $\mathcal{P}$ of order q through labelling the points of $\mathcal{P}$ using elements of $\mathbb{F}_q$ and where we label $\mathbf{O} = (0, 0)$ and $\mathbf{I} = (1, 1)$.

Note that for a PTR polynomial, we are guaranteed that the zero and one of the PTR and the 0 and 1 of $\mathbb{F}_q$ coincide. An equivalent definition is that $T \in \mathbb{F}_q[X, Y, Z]$ is a PTR polynomial over $\mathbb{F}_q$ if it satisfies properties (a)–(e) of Lemma 2.1 over $\mathbb{F}_q$.

https://doi.org/10.1017/S1446788718000095 Published online by Cambridge University Press

4. Restrictions on the form of PTR polynomials

We now look to exploit the conditions on T described in Lemma 2.1 to obtain restrictions on the possible forms of T. Throughout we assume T is a reduced polynomial.

THEOREM 4.1. *Suppose $T \in \mathbb{F}_q[X, Y, Z]$ satisfies property (a). Then*

$$T(X, Y, Z) = Z + XYZ\, M_1(X, Y, Z) + M_2(X, Y), \tag{4.1}$$

where

$$M_1(X, Y, Z) = \sum_{i=0}^{q-2} \sum_{j=0}^{q-2} \sum_{k=0}^{q-2} b_{ijk} X^i Y^j Z^k,$$

$$M_2(X, Y) = \sum_{i=1}^{q-1} \sum_{j=1}^{q-1} c_{ij} X^i Y^j.$$

In particular,

$$x \odot y = T(x, y, 0) = M_2(x, y) \tag{4.2}$$

for all $x, y \in \mathbb{F}_q$.

PROOF. As a polynomial, we may represent T as

$$T(X, Y, Z) = \sum_{i,j,k=0}^{q-1} a_{ijk} X^i Y^j Z^k.$$

By property (a), $T(0, 0, z) = z$ for all z. Viewing this as a polynomial identity in Z, we immediately find

$$a_{00k} = \begin{cases} 1 & \text{if } k = 1, \\ 0 & \text{if } k \neq 1. \end{cases}$$

Noting that $T(x, 0, Z) = Z$ for all x, we again view this as a polynomial identity in X, Z, and obtain

$$Z = T(X, 0, Z) = \sum_{i=0}^{q-1} X^i \Big(\sum_{k=0}^{q-1} a_{i0k} Z^k \Big).$$

For $i \neq 0$, this now forces

$$\sum_{k=0}^{q-1} a_{i0k} Z^k = 0.$$

As a polynomial identity, we get $a_{i0k} = 0$ for all $i \neq 0$. A similar argument shows $a_{0jk} = 0$ for all $j \neq 0$. Hence,

$$T(X, Y, Z) = Z + \sum_{i,j=1}^{q-1} \sum_{k=0}^{q-1} a_{ijk} X^i Y^j Z^k = Z + XY\, T_1(X, Y, Z),$$

for some reduced $T_1 \in \mathbb{F}_q[X, Y, Z]$. It is clear we can now rewrite T_1 as claimed in (4.1). □

https://doi.org/10.1017/S1446788718000095 Published online by Cambridge University Press

So we see that property (a) alone isolates the behaviour of $\odot$, though of course it does not *define* the behaviour of $\odot$.

A polynomial $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ is called a *permutation polynomial* (PP) over $\mathbb{F}_q$ if the evaluation map $\mathbf{x} \mapsto f(\mathbf{x})$ is equidistributive on $\mathbb{F}_q$; that is, for each $y \in \mathbb{F}_q$, the equation $f(\mathbf{x}) = y$ has q^{n-1} solutions $\mathbf{x} \in \mathbb{F}_q^n$. (In the case where $n = 1$, the evaluation map is a bijection.) It follows from Hermite's criterion that if a reduced polynomial $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ is a PP over $\mathbb{F}_q$, then the degree of f in each X_i is at most $q - 2$. We now show how PPs are intimately related to PTR polynomials. Though this result could just as easily be established by considering the plane directly, we choose instead to use as few of the properties of Lemma 2.1 as is necessary in each case.

THEOREM 4.2. *Let $T \in \mathbb{F}_q[X, Y, Z]$. The following statements hold.*

(i) *Suppose T satisfies properties (a) and (c). Then $T(X, y, z)$ is a PP in X for every choice of $(y, z) \in \mathbb{F}_q^\star \times \mathbb{F}_q$.*

(ii) *Suppose T satisfies properties (a) and (e). Then $T(x, Y, z)$ is a PP in Y for every choice of $(x, z) \in \mathbb{F}_q^\star \times \mathbb{F}_q$.*

(iii) *Suppose T satisfies property (d). Then $T(x, y, Z)$ is a PP in Z for every choice of $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$.*

PROOF. For (i), an appeal to property (c) with $c = 0 \neq a, b, d$ arbitrary shows that the equation $T(x, a, b) = T(x, 0, d)$ has a unique solution x. By property (a), $T(x, 0, d) = d$, and so $T(x, a, b) = d$ has a unique solution x for each $d \in \mathbb{F}_q$.

For (ii), fix $a = 0$. By property (e), for any b, c, d with $c \neq 0$ there exists a unique (y, z) such that $T(0, y, z) = b$ and $T(c, y, z) = d$. By property (a), $T(0, y, z) = z$, and so z is fixed: $z = b$. Thus, as we range over all $d \in \mathbb{F}_p$, we have a unique preimage y, proving the claim.

For (iii), fix x, y. Property (d) tells us that for any c, we can always solve uniquely for z in $T(x, y, z) = c$. Thus $T(x, y, z_1) = T(x, y, z_2)$ implies $z_1 = z_2$, so that $T(x, y, Z)$ is a PP in Z for every x, y. □

COROLLARY 4.3. *Suppose $T \in \mathbb{F}_q[X, Y, Z]$ satisfies properties (a), (c), (d) and (e). Then T has degree at most $q - 2$ in each of X, Y, and Z.*

PROOF. By assumption, T has the form given in (4.1). Since $T(x, y, Z)$ is a PP for all $x, y \in \mathbb{F}_q$, Hermite's criterion tells us

$$\sum_{i,j=1}^{q-1} a_{ij(q-1)} x^i y^j = 0$$

for all x, y. This holds as a polynomial identity in X, Y, and so $b_{ij(q-1)} = 0$ for all i, j. Similar arguments can be used to obtain the bounds on the degrees of X and Y. □

A concept related to PPs is that of a κ-polynomial. A polynomial $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ is a *κ-polynomial over $\mathbb{F}_q$* if

$$k_a = \#\{\mathbf{x} \in \mathbb{F}_\mathbf{q}^\mathbf{n} : \mathbf{f}(\mathbf{x}) = \mathbf{a}\}$$

https://doi.org/10.1017/S1446788718000095 Published online by Cambridge University Press

is independent of a for $a \in \mathbb{F}_q^\star$. In direct contrast to the study of permutation polynomials, there are almost no results in the literature directly discussing κ-polynomials. This seems altogether surprising since the specified regularity on preimages of all nonzero elements of the field suggests such polynomials must almost certainly appear in many guises. As an example of how they may arise, recall that a *skew Hadamard difference set* (SHDS) $D \subset \mathbb{F}_q^\star$ is a set of order $(q-1)/2$ where every element of $\mathbb{F}_q^\star$ can be written as a difference of elements of D in precisely $(q-3)/4$ ways. Let D be any SHDS, and define a two-to-one map $\phi : \mathbb{F}_q^\star \to D$ in an arbitrary way. Extending ϕ to all of $\mathbb{F}_q$ by setting $\phi(0) = 0$, we can associate with ϕ a reduced polynomial $f \in \mathbb{F}_q[X]$. It is straightforward to confirm the polynomial $M(X,Y) = f(X) - f(Y)$ is a κ-polynomial over $\mathbb{F}_q$ with $k_a = q-1$ for all $a \in \mathbb{F}_q^\star$. (One could generalise this construction in a suitable way to obtain κ-polynomials in more than two variables using difference families.) The thesis of Matthews [13] contains some general results on κ-polynomials. Some of these results are given in the *Handbook of Finite Fields* [14, Section 9.4]. Theorem 9.4.8 of [14], which is straightforward to prove, shows how κ-polynomials play a role in the study of projective planes. We now prove a slightly extended version of that result.

THEOREM 4.4. *Suppose $T \in \mathbb{F}_q[X,Y,Z]$ satisfies property (a) and either property (c) or (e). Then $T(X,Y,z) - z$ is a κ-polynomial for any $z \in \mathbb{F}_q$.*

PROOF. Fix z and consider the polynomial $f_z \in \mathbb{F}_q[X,Y]$ given by $f_z(X,Y) = T(X,Y,z)$. If $d = z$, then by property (a), $T(0,y,z) = T(x,0,z) = d$ for all $x, y \in \mathbb{F}_q$. Thus $f_z(x,y) = d$ has (at least) $2q-1$ solutions. If $d \neq z$, then by Theorem 4.2(i) or (ii), there are precisely $q-1$ solutions $(x,y) \in \mathbb{F}_q^\star \times \mathbb{F}_q^\star$ to the equation $f_z(x,y) = d$. Since this accounts for all q^2 images, we see that

$$f_z(x,y) = d \quad \begin{cases} \text{has } q-1 \text{ solutions when } d \neq z, \\ \text{has } 2q-1 \text{ solutions when } d = z. \end{cases}$$

Consequently, the polynomial $f_z(X,Y) - z = T(X,Y,z) - z$ is a κ-polynomial over $\mathbb{F}_q$. □

COROLLARY 4.5. *Suppose $T \in \mathbb{F}_q[X,Y,Z]$ satisfies either property (a) and one of properties (c) or (e); or property (d). Then $T(X,Y,Z)$ is a PP over $\mathbb{F}_q$.*

PROOF. Suppose first that T satisfies property (a) and one of properties (c) or (e). Fixing $z, d \in \mathbb{F}_q$, we see from the proof of Theorem 4.4 that

$$T(x,y,z) = d \quad \begin{cases} \text{has } q-1 \text{ solutions when } z \neq d, \\ \text{has } 2q-1 \text{ solutions when } z = d. \end{cases}$$

Consequently, as we range over all $z \in \mathbb{F}_q$, a given d has $(2q-1) + (q-1)(q-1) = q^2$ preimages $(x,y,z) \in \mathbb{F}_q^3$.

Now suppose property (d) is satisfied. Then by Theorem 4.2(iii), the polynomial $T(x,y,Z)$ is a PP for all choices of $(x,y) \in \mathbb{F}_q \times \mathbb{F}_q$. It follows at once that $T(x,y,z) = d$ has precisely q^2 solutions (x,y,z). □

https://doi.org/10.1017/S1446788718000095 Published online by Cambridge University Press

At this point, we have shown that properties (a), (c) and (d) can lead to PPs. Property (e) can also be used to derive a PP result, but not over $\mathbb{F}_q$. Suppose $T \in \mathbb{F}_q[X, Y, Z]$. Let $\{1, \beta\}$ be a basis for $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$. For any $a, b \in \mathbb{F}_q$, we define the function $S_{a,b} : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ by

$$S_{a,b}(x) = S_{a,b}(y + \beta z) = T(a, y, z) + \beta T(b, y, z).$$

When we talk of the polynomial $S_{a,b}$ we will mean the polynomial of least degree in $\mathbb{F}_{q^2}[X]$ which when induced produces the function just defined. The following lemma is now immediate.

LEMMA 4.6. *Suppose $T \in \mathbb{F}_q[X, Y, Z]$ satisfies property (e). Then $S_{a,b}$ is a permutation polynomial over $\mathbb{F}_{q^2}$ whenever $a \neq b$.*

Finally, we consider how property (b) impacts the form of the PTR polynomial. We have already seen how property (a) alone isolates the behaviour of $\odot$; see (4.2) above. One interesting outcome of combining properties (a) and (b) is that the behaviour of $\oplus$ is also isolated.

LEMMA 4.7. *Suppose $T \in \mathbb{F}_q[X, Y, Z]$ satisfies properties (a) and (b). Then T has the shape (4.1) and*

$$\sum_{i=1}^{q-1} c_{ij} = \sum_{i=1}^{q-1} c_{ji} = \begin{cases} 1 & \text{if } j = 1, \\ 0 & \text{if } j > 1. \end{cases}$$

Moreover,

$$y \oplus z = T(1, y, z) = y + z + yz\, M_1(1, y, z) \tag{4.3}$$

for all $y, z \in \mathbb{F}_q$.

PROOF. From property (b), we know $T(X, 1, 0) = X$. Combining this polynomial identity with (4.1) forces the first set of conditions on the coefficients, while using $T(1, Y, 0) = Y$ forces the second set. In addition, applying $T(1, y, 0) = y$ to (4.1), we also find $T(1, y, z) = y + z + yz\, M_1(1, y, z)$, as claimed. □

Now, if we combine all of the above, we obtain the following result about PTR polynomials, the proof of which is immediate from the above statements.

THEOREM 4.8. *Suppose $T(X, Y, Z)$ is a PTR polynomial over $\mathbb{F}_q$. Then*

$$T(X, Y, Z) = Z + XYZ\, M_1(X, Y, Z) + M_2(X, Y), \tag{4.4}$$

with

$$M_1(X, Y, Z) = \sum_{i=0}^{q-3} \sum_{j=0}^{q-3} \sum_{k=0}^{q-3} b_{ijk} X^i Y^j Z^k,$$

$$M_2(X, Y) = \sum_{i=1}^{q-2} \sum_{j=1}^{q-2} c_{ij} X^i Y^j.$$

In addition, T is linear if and only if for all $x, y, z \in \mathbb{F}_q$, $z \neq 0$, we have

$$xy\, M_1(x, y, z) = M_2(x, y) M_1(1, M_2(x, y), z). \tag{4.5}$$

https://doi.org/10.1017/S1446788718000095 Published online by Cambridge University Press

We get an immediate corollary which extends Lemma 4.7 for linear PTR polynomials.

COROLLARY 4.9. *For a linear PTR polynomial $T \in \mathbb{F}_q[X, Y, Z]$ of the form (4.4), we have*

$$\sum_{i=0}^{q-3} b_{ijk} = \sum_{i=0}^{q-3} b_{jik}$$

for all $0 \le j \le q-3$ and $1 \le k \le q-3$.

The result follows by substituting $y = 1$ into (4.5), whereby one obtains $xM_1(x, 1, z) = xM_1(1, x, z)$ for all $x, z \in \mathbb{F}_q$. This can be viewed as a polynomial equation in X, Z and the statement of the corollary follows.

5. The Lenz–Barlotti classification

Let $\mathcal{P}$ be a projective plane and Γ denote the full collineation group of $\mathcal{P}$. If a collineation fixes a line $\mathcal{L}$ pointwise and a point $\mathbf{p}$ linewise, then it is called a *central* collineation, and $\mathcal{L}$ and $\mathbf{p}$ are called the *axis* and *centre* of the collineation, respectively. It is well known that every central collineation in Γ has a unique centre $\mathbf{p}$ and unique axis $\mathcal{L}$. Let $\Gamma(\mathbf{p}, \mathcal{L})$ be the subgroup of Γ consisting of all central collineations of $\mathcal{P}$ with centre $\mathbf{p}$ and axis $\mathcal{L}$. The plane $\mathcal{P}$ is said to be $(\mathbf{p}, \mathcal{L})$-*transitive* if for every two distinct points $\mathbf{q}, \mathbf{r}$ that are (a) collinear with $\mathbf{p}$ but not equal to $\mathbf{p}$, and (b) not on $\mathcal{L}$, there exists a necessarily unique collineation $\gamma \in \Gamma(\mathbf{p}, \mathcal{L})$ which maps $\mathbf{q}$ to $\mathbf{r}$. Now let $\mathcal{M}$ be a second line of $\mathcal{P}$, not necessarily distinct from $\mathcal{L}$. If $\mathcal{P}$ is $(\mathbf{p}, \mathcal{L})$-transitive for all $\mathbf{p} \in \mathcal{M}$, then $\mathcal{P}$ is said to be $(\mathcal{M}, \mathcal{L})$-*transitive*; the concept of $(\mathbf{p}, \mathbf{q})$-*transitivity* is defined dually. If $\mathcal{P}$ is $(\mathcal{L}, \mathcal{L})$-transitive, then $\mathcal{L}$ is called a *translation line* and $\mathcal{P}$ is called a *translation plane* with respect to the line $\mathcal{L}$. The definitions of *translation point* and *dual translation plane* are defined dually also.

The Lenz–Barlotti classification for projective planes is based on the possible sets

$$\mathcal{T} = \{(\mathbf{p}, \mathcal{L}) : \mathcal{P} \text{ is } (\mathbf{p}, \mathcal{L})\text{-transitive}\}$$

of point–line transitivities that the full collineation group of a plane can exhibit. Developed by Lenz [10] and refined by Barlotti [1], the classification has a hierarchy of types, starting with few or no point–line transitivities in types I and II, through to type VII.2, which represents the Desarguesian plane and where $\mathcal{T}$ consists of every possible point–line flag. There are no type VI planes at all: the type arises naturally in the study of potential permutation groups, but no plane can exist of this type. For any Lenz–Barlotti type where a finite example is known, one can also find an infinite example. The converse is not true; infinite examples of types III.1, III.2 and VII.1 are known, while it can be shown that finite examples of each of these types are impossible: in the case of type VII.1, this is due to the Artin–Zorn theorem which states that any finite alternative division ring is a field, (see [8], Theorem 6.20); type III.1 was ultimately resolved by Hering and Kantor [7] and type III.2 was completed by Lüneberg [12] and

https://doi.org/10.1017/S1446788718000095 Published online by Cambridge University Press

Yaqub [15]. It should be noted that several finite cases remain open: the question of existence of finite projective planes of Lenz–Barlotti types I.2, I.3, I.4 and II.2 remains unresolved.

Our motivation for discussing the Lenz–Barlotti types for projective planes is made clear when we return to considering the coordinatisation of planes. In parallel with the Lenz–Barlotti classification, there is a corresponding structural hierarchy for properties of PTRs as one ascends through the Lenz–Barlotti types, though one now assumes that the coordinatisation is done in such a fashion that the resulting PTR exhibits the most structure. In Lenz–Barlotti type I.1, the PTR has no additional structure beyond Lemma 2.1. All other planes can be coordinatised to produce a linear PTR. A Lenz–Barlotti type II plane can be coordinatised to produce a PTR T which is linear and where $\oplus$ is associative (so $\oplus$ describes a group operation on the coordinatising set $\mathcal{R}$). Any plane which is at least Lenz–Barlotti type IV is a translation plane. Lenz–Barlotti type IV planes can be coordinatised to produce quasifields, Lenz–Barlotti type V planes can produce semifields, and the Desarguesian case, of course, can produce a field. More specifically, we have the following lemma.

LEMMA 5.1. *The following statements hold.*

(i) *A plane $\mathcal{P}$ which is* only $((0),[0])$*-transitive is necessarily Lenz–Barlotti type I.2. The plane $\mathcal{P}$ is* $((0),[0])$*-transitive if and only if it can be coordinatised by a linear PTR with associative multiplication $\odot$. In such cases,* $\Gamma((0),[0])$ *is isomorphic to the group described by $\odot$. Moreover. during coordinatisation,* $\mathbf{x}$ *is chosen to be the point* (0).

(ii) *A plane $\mathcal{P}$ which is* only $((0),[0])$*-transitive and* $((\infty),[0,0])$*-transitive is necessarily Lenz–Barlotti type I.3. The plane $\mathcal{P}$ is* $((0),[0])$*-transitive and* $((\infty),[0,0])$*-transitive if and only if it can be coordinatised by a linear PTR with associative multiplication $\odot$ and displaying a left distributive law.*

(iii) *A plane $\mathcal{P}$ which is* $((\infty),[\infty])$*-transitive is necessarily Lenz–Barlotti type at least II. The plane $\mathcal{P}$ is* $((\infty),[\infty])$*-transitive if and only if it can be coordinatised by a linear PTR with associative addition $\oplus$. In such cases,* $\Gamma((\infty),[\infty])$ *is isomorphic to the group described by $\oplus$. Moreover, during coordinatisation,* $\mathbf{y}$ *is chosen to be the point* (∞).

(iv) *A plane $\mathcal{P}$ which is a translation plane or dual translation plane is necessarily Lenz–Barlotti type at least IV. The plane $\mathcal{P}$ is a translation plane (respectively, dual translation plane) if and only if it can be coordinatised by a linear PTR with associative addition $\oplus$ and a right distributive law $(x \oplus y) \odot z = x \odot z + y \odot z$ (respectively, a left distributive law $x \odot (y \oplus z) = x \odot y + x \odot z$). In such cases, the order of $\mathcal{P}$ must be a prime power q and the group described by $\oplus$ is elementary abelian. Moreover, during coordinatisation,* $\overline{\mathbf{x}\,\mathbf{y}}$ *is the translation line (respectively,* $\mathbf{y}$ *is the translation point).*

(v) *A plane $\mathcal{P}$ which is both a translation plane and a dual translation plane (so* $[\infty]$ *is a translation line and* (∞) *is a translation point) is necessarily Lenz–Barlotti type at least V. The plane $\mathcal{P}$ is Lenz–Barlotti type at least V if and only*

https://doi.org/10.1017/S1446788718000095 Published online by Cambridge University Press

if it can be coordinatised by a linear PTR with associative addition $\oplus$ and both a left and right distributive law. In such cases, the order of $\mathcal{P}$ must be a prime power q and the group described by $\oplus$ is elementary abelian. Moreover, during coordinatisation, the $\overline{\mathbf{x}\,\mathbf{y}}$ is the translation line and $\mathbf{y}$ is the translation point.

These results come from [3, Ch. 3], and [8, Chs. 5 and 6], and we refer the reader to these references for further information on the Lenz–Barlotti classification and the corresponding properties of PTRs.

The use of the word 'can' in the last result underlines an important point regarding how to optimise properties in the coordinatisation process. Lemma 5.1 makes clear the following strategy to be used during the coordinatisation process:

- if $\mathcal{T}$ contains an incident point–line flag, one such flag must always be $((\infty), [\infty])$;
- if $\mathcal{T}$ contains a nonincident point–line flag, one such flag must always be $((0), [0])$.

Unless the plane is Lenz–Barlotti type I.1, at least one, and possibly both, of these strategems can be met during the initiation phase of the coordinatising process, when one chooses the triangle $\mathbf{O}\,\mathbf{x}\,\mathbf{y}$. *In the following, we assume that the planes have been coordinatised optimally with respect to the properties exhibited by the PTR, and in accordance with the above strategy.* As part of such an 'optimising' strategy, we prioritise associativity of the operations $\oplus$ and $\odot$ of the PTR over distributivity whenever there is such a choice available.

This optimal coordinatisation can be exploited even further during the coordinatisation process by understanding the actions of the additive and multiplicative loops on the lines $\overline{\mathbf{O}\,\mathbf{x}}$ and/or $\overline{\mathbf{O}\,\mathbf{y}}$. (These actions can be made explicit: the details are omitted here, but the extended version of this paper on arXiv does contain them.) For example, if $\mathcal{P}$ is $((\infty), [\infty])$-transitive and the group $\Gamma((\infty), [\infty])$ is known, one can use that group (or a representation of that group in the additive group of $\mathbb{F}_q$; see [2] for more details) as the labelling set and use the action of $\oplus$ on $\overline{\mathbf{O}\,\mathbf{y}}$ to ensure that $\oplus$ is actually the operation of the group. Likewise, if the plane is $((0), [0])$-transitive and the group $\Gamma((0), [0])$ is known, one can use that group, along with an additional element 0, as the labelling set to ensure that $\odot$ is a representation of the operation of the group.

Linking these optimising strategies to PTR polynomials, the most obvious cases we might be interested in are when either $\Gamma((\infty), [\infty])$ is elementary abelian, or when $\Gamma((0), [0])$ is cyclic. In the former case, through optimal coordinatisation, we can assume $\oplus$ is field addition, while in the latter case, we can force $\odot$ to be field multiplication through coordinatising optimally. (It should be noted that one cannot simultaneously assume optimal coordinatisation for both $\oplus$ and $\odot$ as the labelling of the line $\overline{\mathbf{O}\,\mathbf{y}}$ is determined by exactly one of the representations of $\oplus$ and $\odot$ in the above optimising strategies.) In cases where neither of these conditions arise, a representation theory for representing groups by polynomials is needed; such a theory was recently developed by Castillo and the author (see [2]).

For the remainder of this paper, we consider how knowing that either $\oplus$ or $\odot$ is a field operation affects the PTR polynomial. We begin with the case where $\oplus$ is assumed

https://doi.org/10.1017/S1446788718000095 Published online by Cambridge University Press

to be field addition; this situation is actually quite common, especially in the study of semifields, dating back to the first proper examples given by Dickson in [4]. In fact, if the plane is Lenz–Barlotti type IV or higher, then you are guaranteed that any optimal coordinatisation will force $\oplus$ to be field addition.

THEOREM 5.2. *Let $\mathcal{P}$ be a projective plane of order $q = p^e$ for some prime p which is $((\infty), [\infty])$-transitive and where $\Gamma((\infty), [\infty])$ is elementary abelian. Suppose $T \in \mathbb{F}_q[X, Y, Z]$ is a PTR polynomial obtained from coordinatising $\mathcal{P}$ optimally, so that the resulting additive loop is field addition.*

(i) *If $\mathcal{P}$ is strictly Lenz–Barlotti type II.1, then*

$$T(X, Y, Z) = M_2(X, Y) + Z, \tag{5.1}$$

where $M_2(X, Y)$ is as in (4.4).

(ii) *If $\mathcal{P}$ is strictly Lenz–Barlotti type II.2, then $T \in \mathbb{F}_q[X, Y, Z]$ is of the shape (5.1), where*

$$M_2(x, M_2(y, z)) = M_2(M_2(x, y), z)$$

for all $x, y, z \in \mathbb{F}_q$.

(iii) *If $\mathcal{P}$ is a translation plane of Lenz–Barlotti type at least IV, then $T \in \mathbb{F}_q[X, Y, Z]$ is of the shape (5.1), where*

$$M_2(X, Y) = \sum_{i=0}^{e-1} \sum_{j=1}^{q-1} c_{ij} X^{p^i} Y^j. \tag{5.2}$$

(iv) *If $\mathcal{P}$ is a dual translation plane of Lenz–Barlotti type at least IV, then $T \in \mathbb{F}_q[X, Y, Z]$ is of the shape (5.1), where*

$$M_2(X, Y) = \sum_{i=1}^{q-1} \sum_{e=0}^{e-1} c_{ij} X^i Y^{p^j}. \tag{5.3}$$

(v) *If $\mathcal{P}$ is Lenz–Barlotti type at least V, then $T \in \mathbb{F}_q[X, Y, Z]$ is of the shape (5.1), where*

$$M_2(X, Y) = \sum_{i=0}^{e-1} \sum_{j=0}^{e-1} c_{ij} X^{p^i} Y^{p^j}. \tag{5.4}$$

PROOF. By our hypotheses, the plane $\mathcal{P}$ is necessarily Lenz–Barlotti type at least II.1, and $y \oplus z = y + z$, so that in (4.3) we see $M_1 = 0$. Claim (i) now follows at once from Theorem 4.8. The extension to Lenz–Barlotti type II.2 is immediate from the fact that, in an optimal coordinatisation, the plane will be both $((\infty), [\infty])$-transitive and $((0), [0])$-transitive, and $x \odot y = M_2(x, y)$ will act isomorphically to $\Gamma((0), [0])$. Thus the condition given on M_2 is nothing more than the associative property of the operation $\odot$.

For (iii), Lemma 5.1 tells us we must have equation (5.1), as well as a right distributive law. Thus $M_2(X, Y)$ must satisfy $M_2(a + b, y) = M_2(a, y) + M_2(b, y)$ for all $a, b, y \in \mathbb{F}_q$. It follows at once that $M_2(X, Y)$ is a linearised polynomial in X. Thus M_2

https://doi.org/10.1017/S1446788718000095 Published online by Cambridge University Press

has the form claimed. A similar argument deals with the case (iv). The claims of (v) now follow at once as a Lenz–Barlotti type V plane is both a translation plane and a dual translation plane. □

It is worth noting that whenever we consider a projective plane of Lenz–Barlotti type at least IV, we are guaranteed that we can obtain a PTR polynomial of one of the shapes (5.2), (5.3), or (5.4), via Lemma 5.1.

A polynomial $f \in \mathbb{F}_q[X]$ is called a *complete mapping on* $\mathbb{F}_q$ if both $f(X)$ and $f(X) + X$ are PPs over $\mathbb{F}_q$. Complete mappings and their extensions have been studied in several situations. For example, they are connected to the construction of Latin squares. Our next result shows how complete mappings arise completely naturally and in numbers when we look at PTR polynomials.

LEMMA 5.3. *Let $\mathcal{P}$ be a projective plane of order $q = p^e$ for some prime p which is $((\infty), [\infty])$-transitive and where $\Gamma((\infty), [\infty])$ is elementary abelian. Suppose $T \in \mathbb{F}_q[X, Y, Z]$ is a PTR polynomial obtained from coordinatising $\mathcal{P}$ optimally, so that the resulting additive loop is field addition. Then, for any $a \in \mathbb{F}_q \setminus \{0, 1\}$, the polynomial $f_a(X) = M_2(X, a) - X$, is a complete mapping on $\mathbb{F}_q$.*

PROOF. By Theorem 5.2, we know that $T(X, Y, Z) = M_2(X, Y) + Z$. We now appeal to properties (b) and (c). By property (c), for $a, b, c, d \in \mathbb{F}_q$ with $a \neq c$, there exists a unique x satisfying $M(x, a) + b = M(x, c) + d$. Setting $b = 0$, $c = 1$ and appealing to property (b), we find that for all $a \neq 1$, $M(x, a) - M(x, 1) = M(x, a) - x = d$ has a unique solution in x for any d. Thus $f_a(X) = M(X, a) - X$ is a permutation polynomial over $\mathbb{F}_q$ for all $a \neq 1$. Additionally, $f_a(X) + X = M(X, a) = T(X, a, 0)$ is a permutation polynomial for all $a \neq 0$ by Theorem 4.2(i). □

It remains to consider what can be said about PTR polynomials when we know $\odot$ coincides with field multiplication. Our initial assumption, then, must be that the plane is at least $((0), [0])$-transitive. We note that in this case, by starting with a finite projective plane with a nonincident flag transitivity, the only Lenz–Barlotti types possible are I.2, I.3, I.4, II.2, the planar nearfields of type IV, or VII.2 We may ignore the planar nearfields case, as the multiplicative groups involved in that case are necessarily nonabelian, so can never be cyclic. Additionally, it was shown by Ghinelli and Jungnickel [5] that I.3 and I.4 planes correspond to the nonabelian and abelian case, respectively, of the same existence problem for neo-difference sets. Consequently, Lenz–Barlotti type I.3 can be omitted from our considerations. Since II.2 strictly contains only I.2, in the hierarchy of Lenz–Barlotti types under consideration, we have two distinct strings: I.2 ⊆ I.4 ⊆ VII.2, and I.2 ⊆ II.2 ⊆ VII.2. We have the following statement.

THEOREM 5.4. *Let $\mathcal{P}$ be a projective plane of order $q = p^e$ for some prime p which is $((0), [0])$-transitive and where $\Gamma((0), [0])$ is cyclic. Suppose $T \in \mathbb{F}_q[X, Y, Z]$ is a PTR polynomial obtained from coordinatising $\mathcal{P}$ optimally, so that the resulting multiplicative loop is field multiplication.*

https://doi.org/10.1017/S1446788718000095 Published online by Cambridge University Press

(i) *If $\mathcal{P}$ is strictly Lenz–Barlotti I.2, then*

$$T(X,Y,Z) = Z + XY + XYZ\,M_1(X,Y,Z), \tag{5.5}$$

where

$$M_1(X,Y,Z) = \sum_{i,j=0}^{q-3} b_{ij}(XY)^i Z^j.$$

(ii) *If $\mathcal{P}$ is strictly Lenz–Barlotti I.4, then T is of the shape (5.5), where*

$$M_1(X,Y,Z) = \sum_{i=0}^{q-3} b_i(XY)^i Z^{q-2-i}.$$

(iii) *If $\mathcal{P}$ is strictly Lenz–Barlotti II.2, then T is of the shape (5.5), where*

$$\begin{aligned} yz + xy\,M_1(1,x,y)(1 + z\,M_1(1,x+y+xy\,M_1(1,x,y),z)) \\ = xy + yz\,M_1(1,y,z)(1 + x\,M_1(1,x,y+z+yz\,M_1(1,y,z))) \end{aligned}$$

for all $x,y,z \in \mathbb{F}_q$.

Proof. By hypothesis, $x \odot y = xy$, and Lemma 5.1 tells us the PTR is linear. Thus $T(x,y,z) = (xy) \oplus z$, and now an appeal to Theorem 4.8 produces claim (i), where we define b_{ij} by $b_{ij} = b_{iij}$.

For (ii), we use the fact that the PTR polynomial T obtained from optimal coordinatisation must have a left distributive law. Since $x(y \oplus z) = xy \oplus xz$ for all $x,y,z \in \mathbb{F}_q$, we have the identity

$$xyz\,M_1(1,y,z) = x^2yz\,M_1(1,xy,xz)$$

for all x,y,z. Now this equation has no higher powers of y or z beyond the $(q-2)$th, and so we can view this as a polynomial identity in Y,Z. Equating coefficients, we find for all $x \in \mathbb{F}_q$ and all $0 \le i,j \le q-3$,

$$b_{ij}x = b_{ij}x^{2+i+j}.$$

Thus $b_{ij} = 0$ unless $2+i+j = q$, which proves we may index the (potentially) nonzero coefficients by a single counter, and this yields (ii).

For (iii), the proof is essentially the same as for Lenz–Barlotti type II.2 in Theorem 5.2, in that we know $\oplus$ will be associative in an optimal coordinatisation of the plane $\mathcal{P}$ and the condition on M_1 given above is equivalent. □

6. Concluding remarks

As stated in the introduction, the objective of this paper is to lay the groundwork for enabling the theory of polynomials over finite fields to be incorporated into the study of projective planes of prime power order. The results of Sections 4 and 5 achieve this, but in the author's opinion they should be viewed as the starting point, a tool, for

https://doi.org/10.1017/S1446788718000095 Published online by Cambridge University Press

future research. We therefore wish to conclude this paper by mentioning the main two motivating problems we had in mind when originally developing this material.

Much is known about the allowable groups for central collineation groups involved in some of the Lenz–Barlotti classes. Castillo and the author [2] provide a representation theory for groups using polynomials over finite fields. That body of theory could be used in conjunction with the results of the present paper to pursue both computational and theoretical existence/nonexistence results with regard to some of these classes. The lack of knowledge regarding the open Lenz–Barlotti classes, even in small orders, is truly staggering. Also staggering is the fact that there remains no classification of projective planes of order n for any $n \geq 11$, order 10 having famously been classified using a computer by Lam, Thiel and Swiercz in the late 1980s (see [9]); this despite the immense increase in computer power in the last 30-odd years.

Even a casual perusal of Mathematical Reviews will show PPs have been a significant research topic in their own right for many years (effectively since historical times), with a wide array of applications. Problem P2 of [11], which states 'Find new classes of PPs of $\mathbb{F}_q$', is as relevant today as it was in 1988. At the other end of the spectrum is our knowledge of κ-polynomials. The results concerning PPs and κ-polynomials from Section 4 offer a method for constructing classes of these polynomials. Any class of projective planes can be used to construct them. Under optimal coordinatisation, Lenz–Barlotti type V.1 and VII.2 planes will only produce additive polynomials, but any other known example of a projective plane will produce nonadditive examples, and even type V.1 planes will produce nonadditive examples if they are coordinatised suboptimally. The options here are basically endless, though there are undoubtedly many technical issues to be overcome.

References

[1] A. Barlotti, 'Le possibili configurazioni del sistema delle coppie punto-retta (A, a) per cui un piano grafico risulta (A, a)-transitivo', *Boll. Unione Mat. Ital. (9)* **12** (1957), 212–226.
[2] C. Castillo and R. S. Coulter, 'A general representation theory for constructing groups of permutation polynomials', *Finite Fields Appl.* **35** (2015), 172–203.
[3] P. Dembowski, *Finite Geometries* (Springer, Berlin, 1968), reprinted 1997.
[4] L. E. Dickson, 'On commutative linear algebras in which division is always uniquely possible', *Trans. Amer. Math. Soc.* **7** (1906), 514–522.
[5] D. Ghinelli and D. Jungnickel, 'On finite projective planes in Lenz–Barlotti class at least I.3', *Adv. Geom.* (Suppl) (2003), S28–S48.
[6] M. Hall, 'Projective planes', *Trans. Amer. Math. Soc.* **54** (1943), 229–277.
[7] C. H. Hering and W. M. Kantor, 'On the Lenz–Barlotti classification of projective planes', *Arch. Math.* **22** (1971), 221–224.
[8] D. R. Hughes and F. C. Piper, *Projective Planes*, Graduate Texts in Mathematics, 6 (Springer, New York, 1973).
[9] C. W. H. Lam, L. Thiel and S. Swiercz, 'The non-existence of finite projective planes of order 10', *Canad. J. Math.* **41** (1989), 1117–1123.
[10] H. Lenz, 'Zur Begründung der analytischen Geometrie', *S.-B. Math.-Nat. Kl. Bayer. Akad. Wiss.* (1954), 17–72.
[11] R. Lidl and G. L. Mullen, 'When does a polynomial over a finite field permute the elements of the field?', *Amer. Math. Monthly* **95** (1988), 243–246.

https://doi.org/10.1017/S1446788718000095 Published online by Cambridge University Press

[12] H. Lüneberg, 'Zur Frage der Existenz von endlichen projektiven Ebenen vom Lenz–Barlotti-Typ III.2', *J. reine angew. Math.* **220** (1965), 63–67.
[13] R. W. Matthews, 'Permutation polynomials in one and several variables', PhD Thesis, University of Tasmania, Hobart, 1990.
[14] G. L. Mullen and D. Panario, *Handbook of Finite Fields*, Discrete Mathematics and Its Applications, 78 (CRC Press, Boca Raton, FL, 2013).
[15] J. C. D. S. Yaqub, 'The non-existence of finite projective planes of Lenz–Barlotti class III.2', *Arch. Math.* **18** (1967), 308–312.

ROBERT S. COULTER, 520 Ewing Hall,
Department of Mathematical Sciences, University of Delaware,
Newark, DE 19716, USA
e-mail: coulter@udel.edu

https://doi.org/10.1017/S1446788718000095 Published online by Cambridge University Press