Ovoids and Translation Planes from Lattices

G. ERIC MOORHOUSE Dept. of Mathematics, University of Wyoming, Laramie WY 82071–3036, U.S.A. moorhous@UWyo.edu

Dedicated to Professor T. G. Ostrom

Abstract Translation planes admitting $2Alt_6 \cong SL(2,9)$, and those of 'extraspecial type' (admitting $2_-^{1+4}Alt_5$), have been studied by Ostrom, Mason, Shult and others. We show the existence of such planes of order p^2 for all odd primes p. We construct such planes using ovoids obtained from lattices by the constructions of Conway et al. [5] and this author [14], [15].

1 INTRODUCTION

The author is grateful to Ted Ostrom for motivating this research, in particular through his survey [21] which was the first paper the author read as a graduate student.

Throughout this paper, all translation planes considered are two-dimensional over $F = GF(q)$ where q is a power of an odd prime p. Translation planes of dimension two, the most extensively studied case, can be viewed in at least three equivalent ways (as described in [9], [8], [13]):

(i) π is an *affine translation plane* of order q^2 and kernel containing $F = GF(q)$. Thus π has point set $V = F^4$, and lines consisting of the cosets of certain mutually complementary two-dimensional subspaces $V_0, V_1, \ldots, V_{q^2} < V$ called the spread components of π. We may suppose $V_i = \{(x, xM_i) : x \in F^2\}$ for $0 \le i < q^2$ and $V_{q^2} = \{(0,0)\} \oplus F^2$, where the *spread matrices* $M_0, M_1, \ldots, M_{q^2-1}$ are 2×2 matrices over F such that $M_i - M_j$ is nonsingular whenever $i \ne j$;

(ii) $\mathcal{S}$ is a *spread* of $PG(3,q)$, i.e. a collection of q^2+1 lines of $PG(3,q)$ which partition the point set; or

(iii) $\mathcal{O}$ is an *ovoid* of the Klein quadric, i.e. a set of q^2+1 points on a hyperbolic quadric in $PG(5,q)$, no two of which are on a line of the quadric.

Now consider a subgroup G of the linear translation complement of π; thus $G \le GL(4,q)$ preserves the set of spread components. We are especially interested in the following two possibilities:

Type A $G \cong SL(2,9)$. We assume that $p > 3$, so that the choice of $G \cong SL(2,9)$ is unique up to conjugacy in $GL(4,q)$, and G acts irreducibly on V; see [17]. The corresponding subgroup of $PSL(4,q)$ given by $\overline{G} = G/\{\pm I\} \cong PSL(2,9) \cong Alt_6$ preserves the corresponding spread $\mathcal{S}$, and $\overline{G}$ acts irreducibly on $PG(5,q)$ preserving both the Klein quadric and the corresponding ovoid $\mathcal{O}$. (The restriction $p \neq 3$ eliminates Desarguesian planes of order 3^{2t}, among others, admitting $SL(2,9)$ in a less interesting representation.)

Type B ('Extraspecial type') G has a normal subgroup $Q \cong D_8 * Q_8$, a central product of a dihedral group of order 8 and a quaternion group of order 8, and $G/Q \cong Alt_5$. See [12], [13] for a more precise description of the isomorphism type of G and its representation on V. The corresponding group acting on $\mathcal{S}$ and on $\mathcal{O}$ is $\overline{G} = G/\{\pm I\} \cong 2^4 Alt_5$, a split extension of an elementary abelian group of order 2^4 by Alt_5. Although G acts irreducibly on V (preserving a symplectic form), $\overline{G}$ fixes a unique point of $PG(5,p)$ outside the Klein quadric.

Ostrom [19] shows that types A and B are the 'largest' two possibilities for G, assuming that $G' = G$ acts irreducibly on V, and $p \not| \, |G|$. Examples of such planes for small *prime* values of q have been given by Mason and Ostrom [12], Mason, Shult and Cabaniss [13], Mason [10], [11], Ostrom [20], [21], Biliotti and Korchmáros [1], and Nakagawa [18]. Remarkably, no examples are known except when $q = p$ is prime; more will be said about this mystery in Section 4. However, in Section 3 we construct examples over every odd prime field:

THEOREM 1 For every odd prime p there exist self-polar translation planes of order p^2 of types A and B. Valid examples are provided by Constructions 1.1 and 1.2 when $p \equiv 1 \mod 4$, and Construction 1.3 when $p \equiv 1 \mod 3$.

The self-polar property implies that the corresponding spread is invariant under a correlation of $PG(3,p)$, as we explain in the context of our examples.

1.1 Construction Let $p \equiv 1 \mod 4$ be prime. List all integer solutions of

$$x_1^2 + x_2^2 + \cdots + x_6^2 = 6p, \qquad x_i \equiv 1 \mod 4\,.$$

Here are the two smallest cases.

$p = 5:$	$(5, 1^5)$	6 vectors		$p = 13:$	$(5^3, 1^3)$	20 vectors
	$(-3^3, 1^3)$	20 "			$(-7, 5, 1^4)$	30 "
	total	$26 = 5^2 + 1$			$(5^2, -3^3, 1)$	60 "
					$(-7, -3^3, 1^2)$	60 "
					total	$170 = 13^2 + 1$

There are always $p^2 + 1$ solutions, and the resulting 6-tuples, taken modulo p, yield an ovoid $\mathcal{O}$ in $PG(5,p)$ with respect to the standard quadratic form. This ovoid is invariant under a group $\overline{G} \cong 2 \times Sym_6 < PO_6^+(p)$ generated by coordinate permutations and the reflection $x \mapsto x - \frac{1}{3}(\sum x_i)(1^6)$. By the Klein correspondence, we obtain a translation plane π of order p^2 of type A. We may identify $\overline{G} \cong 2 \times Sym_6$ with a subgroup of $Aut(PSL(4,p))$ preserving the corresponding spread $\mathcal{S}$, such that half of $\overline{G}$ (a subgroup $\cong Sym_6$) acts as collineations, and the remaining elements are correlations. The preimage of $\overline{G}$ given by $G < Aut(SL(4,p))$ has a subgroup $\cong \Sigma L(2,9)$ in the translation complement of π. Here $\Sigma L(2,9) = SL(2,9)\langle\sigma\rangle$ where σ is the Frobenius automorphism of $GF(9)$.

DEFINITION Let π, $\mathcal{S}$, $\mathcal{O}$ be a triple consisting of a plane, spread and ovoid as described above, and let π', $\mathcal{S}'$, $\mathcal{O}'$ be another such triple. We say that π' is the *polar* of π if any of the following three equivalent conditions is satisfied:

(i) π' is isomorphic to the translation plane with spread matrices $M_i^\top$, where M_i are the spread matrices of π;
(ii) $\mathcal{S}' = \mathcal{S}^\rho$ for some correlation ρ of $PG(3,q)$;
(iii) $\mathcal{O}' = \mathcal{O}^g$ for some orthogonal transformation g such that $\det(g) = -1$.

If in addition π' is isomorphic to π, we say π is self-polar.

If $p \equiv 3 \mod 4$ then the 'standard' quadratic form $\sum x_i^2$ is elliptic rather than hyperbolic. In this case, a modification (Section 3, case II) yields analogues of Construction 1.1.

1.2 Construction Let $p \equiv 1 \mod 4$ be prime. List all integer solutions of

$$x_1^2+x_2^2+\cdots+x_6^2 = p, \qquad x_1+1 \equiv x_2 \equiv x_3 \equiv \cdots \equiv x_6 \mod 2\,, \qquad \sum x_i \equiv 3 \mod 4.$$

Here are the two smallest cases.

$p=5:$	$(0\mid \pm 1^5)$	16 vectors		$p=13:$	$(0\mid \pm 3, \pm 1^4)$	80 vectors
	$(1\mid \pm 2, 0^4)$	10 "			$(1\mid \pm 2^3, 0^2)$	80 "
	total	$26 = 5^2+1$			$(-3\mid \pm 2, 0^4)$	10 "
					total	$170 = 13^2+1$

There are always p^2+1 solutions, and these vectors, taken modulo p, yield an ovoid $\mathcal{O}$ in $PG(5,p)$ with respect to the standard quadratic form. This ovoid is clearly invariant under a group of projective orthogonal transformations $\overline{G} \cong 2 \times 2^4 Sym_5$ generated by all permutations and sign changes of the last five coordinates. The corresponding translation plane π of order p^2 is of type B. We identify $\overline{G}$ with a subgroup of $Aut(SL(4,p))$ preserving the corresponding spread $\mathcal{S}$. Half of $\overline{G}$ (a subgroup $\cong 2^4 Sym_5$) consists of collineations, and the other half consists of correlations.

1.3 Construction Let $p \equiv 1 \mod 3$ be prime. The *root lattice of type* E_6 may be identified as

$$L = \{x = (x_1, x_2, \ldots, x_6) \,:\, x_i \in \mathbb{Z},\ \sum x_i \equiv 0 \mod 3\}$$

using the quadratic form $Q(x) = \sum x_i^2 - \frac{1}{9}\big(\sum x_i\big)^2$. Let $e = (1^6) \in L$. List all vectors $v \in e + 2L$ such that $Q(v) = 2p$, but omit the vector $-v$ if v has already been listed. Here are the two smallest cases.

$p=7:$	$(1^3,3^3)$	20	vectors	$p=13:$	$(3^3,-1^3)$	20	vectors
	$(3,1,-1^4)$	30	"		$(3^2,1^3,-3)$	60	"
	total	$50=7^2+1$			$(5,1^3,-1^2)$	60	"
					$(5,3^4,1)$	30	"
					total	$170=13^2+1$	

In every case, p^2+1 vectors are obtained. Reducing modulo p gives an ovoid in $PG(5,p)$ with respect to $Q \pmod p$ invariant under $\overline{G} \cong 2 \times Sym_6$ generated by coordinate permutations and the reflection in $e^\perp$. The corresponding translation plane π of order p^2 is of type A.

If $p \equiv 1 \mod 12$ then Constructions 1.1 and 1.3 give two ovoids of type A in $O_6^+(p)$, and these are not necessarily equivalent under $PGO_6^+(p)$; in particular for $p=13$ our examples are inequivalent.

We remark that if $p \equiv 2 \mod 3$ then $Q \pmod p$ gives instead a quadratic form of elliptic type. It is known (see [24]) that elliptic quadrics in $PG(5,q)$ (also known as generalized quadrangles of type $Q^-(5,q)$) do not admit ovoids. In this case (odd $p \equiv 2 \mod 3$) the above construction gives *caps* (sets of pairwise noncollinear points) of size $\frac{5}{4}(p^2-1)$ in the associated generalized quadrangles; however, we have found that larger caps than these are obtainable by other means.

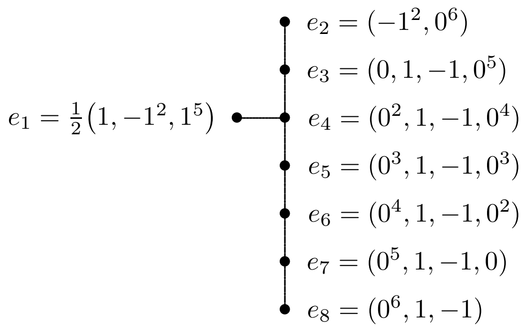
2 THE BINARY OVOIDS

Let $V = F^{2n}$, $F = GF(q)$ where q is an odd prime power, and let $Q : V \to F$ be a nondegenerate quadratic form. Thus $Q(x) = \frac{1}{2}xAx^\top$ for some nonsingular symmetric $2n \times 2n$ matrix A over F. A point (one-dimensional subspace) $\langle v \rangle$ of $PG(V)$ is *singular* if $Q(v)=0$. A subspace $U \le V$ is *totally singular* if $Q(u)=0$ for all $u \in U$. We suppose that Q is of *hyperbolic type,* which is to say that V has totally singular subspaces of dimension n; equivalently, $(-1)^n \det(A)$ is a nonzero square in F. We denote by $O_{2n}^+(q)$ either the isometry type of the pair (V,Q), or the associated isometry group, depending on the context. An *ovoid* in $O_{2n}^+(q)$ is a collection $\mathcal{O}$ of singular points, such that every maximal totally singular subspace contains exactly one point of $\mathcal{O}$; equivalently, $\mathcal{O}$ consists of $q^{n-1}+1$ singular points, no two of which are perpendicular with respect to the bilinear form $(x,y) := xAy^\top$. Ovoids in $O_{2n}^+(q)$ are not known to exist for $n \ge 5$. Ovoids in $O_6^+(q)$ (projectively, the Klein quadric in $PG(5,q)$) were featured in Section 1. The known ovoids in $O_8^+(q)$ are listed in [8], [14]. Of these, the most important family we shall require are the *binary ovoids* of Conway et al. [5], which we proceed to construct.

Our terminology and basic facts regarding root systems, and their Weyl groups and lattices, are well-known; see [6], [7]. Consider the root lattice of type E_8 defined by

$$E = \left\{ \tfrac{1}{2}(a_1,a_2,\ldots,a_8) \,:\, a_i \in \mathbb{Z},\ a_1 \equiv a_2 \equiv \cdots \equiv a_8 \mod 2,\ \textstyle\sum a_i \equiv 0 \mod 4 \right\}.$$

It is well-known that the points of E determine the unique densest lattice packing of uniform spheres in $\mathbb{R}^8$. The *root vectors* of E are the 240 vectors $e \in E$ such that $\|e\|^2 = 2$. Among these we choose a system of *fundamental roots:*



Edges of this Dynkin diagram represent pairs of roots at an angle $2\pi/3$; unjoined nodes represent perpendicular pairs of roots. Let r_i be the reflection $E \to E$, $x \mapsto x - (x \cdot e_i)e_i$. Then $r_1, \ldots, r_8$ generate the *Weyl group* $W(\mathsf{E}_8) \cong O_8^+(2)$.

For any prime p, $\overline{E} := E/pE$ is an 8-dimensional vector space over $F = GF(p)$, with quadratic form $Q(\overline{v})$ $(\overline{v} := v + pE,\ v \in E)$ of hyperbolic type, obtained by reducing $\frac{1}{2}\|v\|^2$ modulo p. Fix a root vector e and an odd prime p. There are exactly $2(p^3+1)$ vectors $v \in e + 2E$ such that $\|v\|^2 = 2p$, which come in pairs $\pm v$. These vectors determine exactly p^3+1 coset pairs $\pm(v+pE)$ in E, forming a *binary ovoid* in $\overline{E} \simeq O_8^+(p)$. This ovoid, denoted $\mathcal{O}_{2,p}(e)$, is invariant under the stabilizer of $\mathbb{Z}e$ in $W(\mathsf{E}_8)$, namely $2 \times W(\mathsf{E}_7) \cong 2^2 \times Sp_6(2)$.

3 SLICING THE BINARY OVOIDS

Let $\mathcal{O}$ be an ovoid in $O_{2n}^+(q)$, and suppose $\langle w \rangle \notin \mathcal{O}$ is a singular point. Then Q induces a quadratic form of hyperbolic type on $w^\perp/\langle w \rangle$, and $\mathcal{O} \cap w^\perp$ yields an ovoid in $w^\perp/\langle w \rangle \simeq O_{2n-2}^+(q)$, called a *slice* of $\mathcal{O}$; see [8]. By appropriately slicing the binary ovoids $\mathcal{O}_{2,p}(e)$ of Section 3, we shall obtain ovoids in $O_6^+(p)$ of types A and B.

We require some facts about the representability of integers by integral quadratic forms.

LEMMA 1 Let p be a prime, and n a positive integer. Then

(i) $p = a^2 + b^2$ for some integers a, b, iff $p \equiv 1 \mod 4$;
(ii) $p = a^2 - ab + b^2$ for some integers a, b, iff $p \equiv 1 \mod 3$;
(iii) $n = a^2 + b^2 + c^2$ for some integers a, b, c, iff n is not of the form $4^k(8\ell - 1)$ where $k, \ell \in \mathbb{Z}$;
(iv) $n = a^2 - ab + b^2 + c^2$ for some integers a, b, c, iff n is not of the form $9^k(9\ell - 3)$ where $k, \ell \in \mathbb{Z}$.

Proof: Conclusions (i)–(iii) are well-known; see [4, pp.10,77], [23, p.45]. We prove (iv) using the theory of rational quadratic forms (see [23], especially Corollary 1 on p.43 therein, and the Corollary on p.37). The quadratic form $Q(a,b,c) = a^2 - ab + b^2 + c^2$ is rationally equivalent to the diagonal form $X^2 + 3Y^2 + Z^2$ where $a = X + Y,\ b = 2Y,\ c = Z$. Computing local invariants, we find that Q represents n in $\mathbb{Q}_p$ for every prime $p \neq 3$, and that Q represents n in $\mathbb{Q}_3$ if and only if $-3n$ is a nonsquare in the group of units of $\mathbb{Q}_3$. The latter condition on n is equivalent to

(*) n is not of the form $9^k(9\ell - 3)$ where $k, \ell \in \mathbb{Z}$.

Thus (*) is a necessary and sufficient condition for n to be represented as $Q(a,b,c)$ for some $(a,b,c) \in \mathbb{Q}^3$. To see that (a,b,c) may in fact be chosen in $\mathbb{Z}^3$, we apply the following:

LEMMA 2 (Davenport-Cassels) Consider a positive definite rational quadratic form $Q(x_1,\ldots,x_r) = \sum_{1\leq i,j\leq r} a_{ij}x_i x_j$ where $a_{ij} = a_{ji} \in \frac{1}{2}\mathbb{Z},\ a_{ii} \in \mathbb{Z}$. Suppose furthermore that for all $x \in \mathbb{Q}^r$, there exists $x' \in \mathbb{Z}^r$ such that $Q(x' - x) < 1$. Then for any integer n, we may represent $n = Q(x)$ for some $x \in \mathbb{Q}^r$ if and only if $n = Q(x')$ for some $x' \in \mathbb{Z}^r$.

This is shown in [23, p.46] under the additional hypothesis that $a_{ij} \in \mathbb{Z}$, which is stronger than necessary, as the proof in [23] shows.

We show that our form $Q(a,b,c) = a^2 - ab + b^2 + c^2$ satisfies the hypothesis of Lemma 2. Fix $a,b,c \in \mathbb{Q}$. Choose $c' \in \mathbb{Z}$ such that $|c' - c| \leq \frac{1}{2}$. Now observe that $Q(a,b,0)$ is the squared length of the Euclidean vector $ae + bf$ where $e = (1,0),\ f = \frac{1}{2}\big(-1, \sqrt{3}\big)$. Since every point of $\mathbb{R}^2$ lies at distance $\leq 1/\sqrt{3}$ from some point of the root lattice $\mathbb{Z}e + \mathbb{Z}f$ of type A_2, we may choose $a', b' \in \mathbb{Z}$ such that $Q(a' - a, b' - b, c' - c) \leq \frac{1}{3} + \frac{1}{4} < 1$. Now the statement of Lemma 1(iv) follows from Lemma 2. □

LEMMA 3 Let $\overline{w} = w + pE \in \overline{E}$, and suppose $\langle\overline{w}\rangle \in \mathcal{O}_{2,p}(e)$ where $e \in E$ is a root vector.

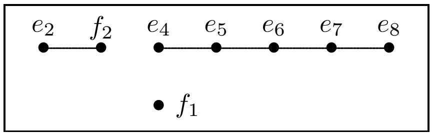
(i) If $p > 3$ and $f \in E \cap w^\perp$ is a root vector, then $e \cdot f$ is even.
(ii) If $p \equiv 3 \mod 4$, $\|w\|^2 = 2p$ and $w \cdot e$ is even, then $w \in e + 2E$.

Proof: By hypothesis, we have $v \in \lambda w + pE$ for some $v \in e + 2E$, $\|v\|^2 = 2p$, $p \not| \lambda$.

If $f \in E \cap w^\perp$ is a root vector, then $v \cdot f \equiv \lambda w \cdot f \equiv 0 \mod p$. But $|v \cdot f| \leq \|v\|\|f\| = 2\sqrt{p}$ and since $p > 3$, we must have $v \cdot f = 0$. Now $e \cdot f \equiv v \cdot f \equiv 0 \mod 2$.

Under the hypotheses of (ii), we have $|v \cdot w| \leq \|v\|\|w\| = 2p$ and $v \cdot w \equiv 0 \mod p$, and so $v \cdot w \in \{0, \pm p, \pm 2p\}$. Also $v \cdot w \equiv e \cdot w \equiv 0 \mod 2$. If $v \cdot w = \pm 2p$ then $w = \pm v \equiv e \mod 2E$ and we are done. Hence we may assume that $v \cdot w = 0$. Then $v - \lambda w \in pE$ implies that $\|v - \lambda w\|^2 = \|v\|^2 + \lambda^2\|w\|^2 \equiv 0 \mod 2p^2$ and $1 + \lambda^2 \equiv 0 \mod p$, contradicting $p \equiv 3 \mod 4$. □

We proceed to prove Theorem 1 in five cases. In cases I and II we refer to the following decomposable root subsystem of E:



where $f_1 = (1, -1, 0^6)$,
$f_2 = \frac{1}{2}(1^8)$.

Case I Suppose $p \equiv 1 \mod 4$. By Lemma 1(i), we may write $p = a^2 + b^2$ for some integers a, b. We may suppose that a is odd, b is even, and $a + b \equiv 1 \mod 4$ (otherwise replace a by $-a$). Let $w = ae_2 + bf_1 = (-a + b, -a - b, 0^6) \in E$, so that $\|w\|^2 = 2p$. By Lemma 3(i), the singular point $\langle \overline{w} \rangle$ does not lie in the ovoid $\mathcal{O} := \mathcal{O}_{2,p}(f_2)$ (since $f_3 := (0^6 1^2) \in w^\perp$ but $f_3 \cdot f_2 = 1$). The slice $\mathcal{O} \cap \overline{w}^\perp$ is an ovoid invariant under $\langle r_4, r_5, \ldots, r_8 \rangle \cong W(\mathsf{A}_5) \cong Sym_6$ consisting of all permutations of the last six coordinates. To see that this is equivalent to Construction 1.1, it clearly suffices to establish:

$$\left.\begin{array}{l} v \in f_2 + 2E, \ \|v\|^2 = 2p, \\ v \cdot w \equiv 0 \mod p \end{array}\right\} \iff \left\{\begin{array}{l} v = \pm\frac{1}{2}\big(a - b, a + b, v_3, \ldots, v_8\big), \\ v_3 \equiv v_4 \equiv \cdots \equiv v_8 \equiv 1 \mod 4, \\ v_3^2 + \cdots + v_8^2 = 6p\,. \end{array}\right.$$

First suppose that $v = \frac{1}{2}\big(v_1, \ldots, v_8\big) \in f_2 + 2E$, $\|v\|^2 = 2p$, $v \cdot w \equiv 0 \mod p$. Then $|v \cdot w| \le \|v\|\|w\| = 2p$, so $v \cdot w \in \{0, \pm p, \pm 2p\}$. Also $v \cdot w \equiv f_2 \cdot w \equiv -a \equiv 1 \mod 2$, so $v \cdot w = \pm p$. We may assume that $v \cdot w = -p$. Since $2v \cdot w = (b - a)v_1 - (b + a)v_2 = -2p$ where $gcd(b - a, b + a) = 1$, we have

$$v_1 = a - b + (b + a)k, \qquad v_2 = a + b + (b - a)k$$

for some $k \in \mathbb{Z}$. Then $\|v\|^2 = \frac{1}{4}(2p + 2pk^2 + v_3^2 + \cdots + v_8^2) = 2p$ implies $|k| \le 1$. Now $v \in f_2 + 2E$ implies $v_1 \equiv v_2 \equiv \cdots \equiv v_8 \mod 4$. In particular, $v_1 \equiv 1 + k \equiv v_2 \equiv 1 - k \mod 4$, so $k = 0$ and $v_3^2 + \cdots + v_8^2 = 6p$ as required.

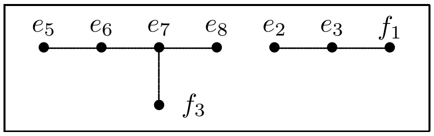
Conversely, we may suppose $v = \frac{1}{2}\big(a - b, a + b, v_3, \ldots, v_8\big)$ where $v_3 \equiv v_4 \equiv \cdots \equiv v_8 \equiv 1 \mod 4$ and $v_3^2 + \cdots + v_8^2 = 6p$. Clearly $v \cdot w = -p$, $\|v\|^2 = 2p$. We must show that

$$v - f_2 = \tfrac{1}{2}\big(a - b - 1, a + b - 1, v_3 - 1, \cdots, v_8 - 1\big) \in 2E.$$

Clearly $a - b - 1 \equiv a + b - 1 \equiv v_3 - 1 \equiv \cdots \equiv v_8 - 1 \equiv 0 \mod 4$. It remains to be shown that $2a + \sum v_i \equiv 0 \mod 8$ (sum over $i = 3, 4, \ldots, 8$). However, $\sum(v_i - 1)^2 \equiv 0 \mod 16$ implies that $2\sum v_i \equiv 6 + \sum v_i^2 \equiv 6(p + 1) \mod 16$. Therefore $2a + \sum v_i \equiv (2 - 2b) + 3(p + 1) \equiv 2 - 2b + 3a^2 + 3b^2 + 3 \equiv 3b(b + 2) \equiv 0 \mod 8$, as required.

Case II Suppose that $p \equiv 3 \mod 4$. By Lemma 1(iv), we may choose integers a, b, c such that $a^2 - ab + b^2 + c^2 = p$. Let $w = ae_2 + bf_2 + cf_1$, so that $\|w\|^2 = 2p$. Clearly a, b cannot both be even. We may suppose a is odd, so $(w - f_1) \cdot f_2 = -a + 2b \equiv 1 \mod 2$ and therefore $w - f_1 \notin 2E$. By Lemma 3(ii), the singular point $\langle \overline{w} \rangle$ is not in the ovoid $\mathcal{O} := \mathcal{O}_{2,p}(f_1)$. As in case I, the ovoid $\mathcal{O} \cap \overline{w}^\perp$ is invariant under $\langle r_4, r_5, \ldots, r_8 \rangle \cong Sym_6$.

In cases III and IV we refer to the following decomposable root subsystem of E:



where $f_1 = (1, -1, 0^6)$,
$f_3 = (0^6 1^2)$.

Case III Suppose again that $p \equiv 1 \mod 4$. As in case I, we have $p = a^2 + b^2$, a odd, b even, $a + b \equiv 1 \mod 4$. Let $w = ae_2 + bf_1$, so that $\|w\|^2 = 2p$. By Lemma 3(i), the singular point $\langle \overline{w} \rangle$ does not lie in the ovoid $\mathcal{O} := \mathcal{O}_{2,p}(e_3)$ (since $e_4 \in w^\perp$ but $e_4 \cdot e_3 = -1$). The ovoid $\mathcal{O} \cap \overline{w}^\perp$ is invariant under the group $\cong 2^4 Sym_5$ consisting of all permutations, and an even number of sign changes, of the last five coordinates. Note that this group is the Weyl group of type D_5 generated by the reflections corresponding to the roots e_5, e_6, e_7, e_8, f_3. To see that this is equivalent to Construction 1.2, it clearly suffices to prove:

$$\left.\begin{array}{l} v \in e_3 + 2E,\ \|v\|^2 = 2p, \\ v \cdot w \equiv 0 \mod p \end{array}\right\} \iff \left\{\begin{array}{l} v = \pm(a, b, v_3, \ldots, v_8) = (\text{OEEOOOOO}) \\ \text{or } \pm(b, a, v_3, \ldots, v_8) = (\text{EOOEEEEE}) \\ \qquad \text{where E} = \textit{even},\ \text{O} = \textit{odd}, \\ v_3 + \cdots + v_8 \equiv 3 \mod 4, \quad v_3^2 + \cdots + v_8^2 = p\,. \end{array}\right.$$

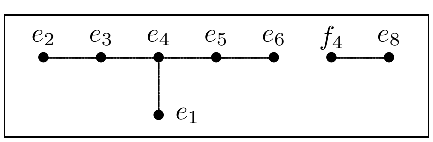
First suppose that $v \in e_3 + 2E$, $\|v\|^2 = 2p$, $v \cdot w \equiv 0 \mod p$. The first condition implies that $v = (v_1, v_2, \ldots, v_8) \in \mathbb{Z}^8$ where $v_1 \equiv v_2 + 1 \equiv v_3 + 1 \equiv v_4 \equiv \cdots \equiv v_8 \mod 2$. As in case I, we may suppose $v \cdot w = -p$. Since $v \cdot w = (b-a)v_1 - (b+a)v_2 = -p$ where $gcd(b-a, b+a) = 1$, we have

$$v_1 = a + (b+a)k, \qquad v_2 = b + (b-a)k$$

for some $k \in \mathbb{Z}$. Then $\|v\|^2 = p + 2pk(k+1) + v_3^2 + \cdots + v_8^2 = 2p$ implies $k \in \{-1, 0\}$ and $v_3^2 + \cdots + v_8^2 = p$. Also, $a + b \equiv 1 \mod 4$ implies that $v_3 + \cdots + v_8 \equiv 3 \mod 4$. The converse is straightforward.

Case IV Assume that $p \equiv 3 \mod 4$. Since $2p \equiv 6 \mod 8$, by Lemma 3(iii) there exist odd integers a, b, c such that $2p = a^2 + b^2 + 4c^2$. We may assume that $a \equiv b \mod 4$; otherwise replace b by $-b$. Then $\alpha = \frac{1}{2}(b-a) + c$ and $\beta = \frac{1}{2}(b-a) - c$ are odd integers. Let $w = \alpha e_2 + b e_3 + \beta f_1$, so that $\|w\|^2 = 2p$. Now $w \cdot e_3 = 2b - \alpha - \beta \equiv 0 \mod 2$, and $(w - e_3) \cdot e_1 = \beta \equiv 1 \mod 2$ so $w - e_3 \notin 2E$. By Lemma 3(ii), the singular point $\langle \overline{w} \rangle$ is not in the ovoid $\mathcal{O} := \mathcal{O}_{2,p}(e_3)$. As in case III, the ovoid $\mathcal{O} \cap \overline{w}^\perp$ is invariant under $2^4 Sym_5$.

It remains only to justify Construction 1.3, for which we consider the decomposable root subsystem



where $f_4 = \frac{1}{2}(1, -1^6, 1)$
$= -3e_1 - 2e_2 - 4e_3 - 6e_4$
$-5e_5 - 4e_6 - 3e_7 - 2e_8$.

Case V Suppose $p \equiv 1 \mod 3$. Let $L = \mathbb{Z}e_1 + \mathbb{Z}e_2 + \cdots + \mathbb{Z}e_6$, a root sublattice of type E_6 isometric to the lattice of Construction 1.3. By Lemma 3.1(ii), there exist integers a, b such that $p = a^2 - ab + b^2$. Clearly a, b are not both even, so we may suppose that a is odd. Let $w = af_4 + be_8$, so that $\|w\|^2 = 2p$. By Lemma 3.3(i), $\langle\overline{w}\rangle \notin \mathcal{O} := \mathcal{O}_{2,p}(e_1)$ (since $e_4 \in w^\perp$ but $e_4 \cdot e_1 = -1$). We wish to show that the ovoid $\mathcal{O} \cap \overline{w}^\perp$ is equivalent to Construction 1.3. Since the Weyl group of type E_6 is transitive on its 72 roots, our root e_1 is equivalent to the root e chosen in Construction 1.3. Therefore it remains only to show that

$$\left.\begin{array}{l} v \in e_1 + 2E,\ \|v\|^2 = 2p, \\ v \cdot w \equiv 0 \mod p \end{array}\right\} \iff v \in e_1 + 2L, \quad \|v\|^2 = 2p.$$

We need only prove the '⇒' implication. Suppose $v \in e_1 + 2E$, $\|v\|^2 = 2p$, $v \cdot w \equiv 0 \mod p$. Then $|v \cdot w| \le \|v\|\|w\| = 2p$, so $v \cdot w \in \{0, \pm p, \pm 2p\}$. But $v \cdot w \ne \pm 2p$, since otherwise $w = \pm v$, contradicting $\langle\overline{w}\rangle \notin \mathcal{O}$. Also, $v \cdot w \equiv e_1 \cdot w \equiv 0 \mod 2$, so $v \cdot w = 0$. It is clear from the expression above for f_4 that $3E \subset L + \mathbb{Z}f_4 + \mathbb{Z}e_8$. Therefore $3v = \alpha f_4 + \beta e_8 + z$ for some $z \in L$. Now $0 = 3v \cdot w = (2a-b)\alpha + (2b-a)\beta$ where $gcd(2a-b, 2b-a) = 1$, and so

$$\alpha = (a-2b)k, \qquad \beta = (2a-b)k$$

for some $k \in \mathbb{Z}$. Now $18p = \|3v\|^2 = 6pk^2 + \|z\|^2$ and so $|k| \le 1$. However, $3(v - e_1) \cdot e_8 = 2\beta - \alpha = 3ak$ is even since $v - e_1 \in 2E$. Thus $k = 0$ and $3v = z \in L$. This means that $v \in L$ and the desired conclusion follows.

4 REMARKS

Much more general examples of translation planes of types A and B are available than those presented in Section 3, using the more general ovoids in $O_8^+(p)$ constructed in [14], [15] using the E_8 root lattice. Choose a vector $x \in E$ and primes $r < p$ such that $-\frac{p}{2}\|x\|^2$ is a quadratic residue modulo r. List all vectors $v \in \mathbb{Z}x + rE$ such that $\|v\|^2 = 2i(r-i)p$ where $1 \le i \le \lfloor\frac{r}{2}\rfloor$. This gives an ovoid $\mathcal{O} = \mathcal{O}_{r,p}(x)$ in $\overline{E} = E/pE$. Let $\langle\overline{w}\rangle \notin \mathcal{O}$ be a singular point. Then the slice $\mathcal{O} \cap \overline{w}^\perp$ is invariant under the group of all $g \in W(\mathsf{E}_8)$ preserving both $\mathbb{Z}x + rE$ and $\mathbb{Z}w + pE$. We may arrange that this group is a suitably large Weyl group, for example of type A_5 or D_5 as in Section 3.

We find the computer implementation of all ovoid constructions described here to be very efficient using available techniques for finding short vectors in lattices; see [3, pp.102–104]. In general, the best available method for comparing isomorphism classes by computer is J. H. Conway's invariant known as the fingerprint; see [2], [16]. However, for ovoids of type A or B, isomorphism testing is greatly simplified; see [1, Step 4], [13, (2.8)].

In Table 4.1 we have listed the number of equivalence classes (under the general orthogonal group) of ovoids of type A or B in $O_6^+(p)$ for small primes p, as enumerated by computer. (Warning: There are slight disagreements between this table and similar lists found in at least three of the references.) The full stabilizers $\overline{G} < PO_6^+(p)$ of these ovoids, namely the five groups $2 \times Sym_6$, $2 \times Alt_6$, Sym_6, $2 \times 2^4 Sym_5$, $2^4 Sym_5$, all contain reflections. Each of the associated translation planes is self-polar, with full translation complement H and kernel K satisfying $H/K \cong Sym_6$, Alt_6, Alt_6, $2^4 Sym_5$ or $2^4 Alt_5$ respectively. Although for $p \le 37$ we

p	3	5	7	11	13	17	19	23	29	31	37
$2 \times Sym_6$		1	2	3	2	2	6	6	2	12	6
$2 \times Alt_6$		0	0	2	0	0	0	0	0	0	0
Sym_6		0	0	3	1	2	2	17	5	2	5
total type A		1	2	8	3	4	8	23	7	14	11
$2 \times 2^4 Sym_5$	1	1	1	3	2	2	5	7	8	6	7
$2^4 Sym_5$	0	0	0	1	0	1	0	7	3	4	2
total type B	1	1	1	4	2	3	5	14	11	10	9

Table 4.1 Number of ovoids of type A, B in $O_6^+(p)$ for small p

found that $\overline{G} \not\cong Alt_6$, $H/K \not\cong 2 \times 2^4 Alt_5$, and π is self-polar, we have no evidence that these must be true in general.

The lack of known examples for $q = p^t$, $t \geq 2$ is quite perplexing. By exhaustive computer search, we have concluded that there is no ovoid in $O_6^+(25)$ admitting Alt_6, and no ovoid in $O_6^+(q)$ admitting $2^4 Alt_5$ for $q = 9, 25, 27, 49$. Similarly, for $t \geq 2$, a lack of known ovoids in $O_8^+(p^t)$ invariant under $Sp_6(2)$ was observed in [15]. The best nonexistence result we have in this direction is the following:

LEMMA 4 There is no ovoid of type B in $O_6^+(3^{2t})$.

Proof: Suppose $\mathcal{O}$ is an ovoid in $O_6^+(q)$ invariant under $\overline{G} \cong 2^4 Alt_5$. We use the quadratic form $Q(x) = -x_0^2 + \sum_{j=1}^5 x_j^2$ of hyperbolic type, and $\overline{G}$ acts by even permutations, and an even number of sign changes, of the last five coordinates. If $q = 3^{2t}$ then $|\mathcal{O}| = q^2+1 \equiv 2 \mod 5$, so $(12345) \in Alt_5$ fixes at least two points of $\mathcal{O}$. However, (12345) fixes exactly two singular points, namely $\langle(\theta, 1^5)\rangle$ and $\langle(-\theta, 1^5)\rangle$, where $\theta^2 = -1$. So both these points must belong to $\mathcal{O}$. But then $\mathcal{O}$ also contains $\langle(\theta, -1^2, 1^3)\rangle$, which is orthogonal to $\langle(-\theta, 1^5)\rangle$, a contradiction. □

Because of slicing, Lemma 4 implies the nonexistence of ovoids in $O_8^+(3^{2t})$ invariant under $Sp_6(2)$.

Does every known translation plane of type A or B arise from a lattice-type construction? We believe not. From the known ovoids in $O_8^+(q)$ for small q, as listed in [14], we have determined all possible $O_6^+(q)$-slices; and in general, these do not include all ovoids listed in Table 4.1. The smallest examples of this are for $q = 11$, where the five known ovoids in $O_8^+(11)$ yield 85 slices in $O_6^+(11)$, but these account for only 5 = 1+0+1+3+0 of the 12 = 3+2+3+3+1 ovoids of types A and B.

Finally, we emphasize the most striking feature of these constructions of ovoids and translation planes: their apparent dependence on some nonelementary number theory. In addition to Lemma 1, the construction of $\mathcal{O}_{r,p}(e)$ (see [5], [14], [15]) relies on the following theorem (see [23]). Here $N_\Lambda(n)$ denotes the number of vectors v in an integral lattice Λ such that $\|v\|^2 = n$. Also $\sigma_k(n) = \sum_{1 \leq d|n} d^k$.

THEOREM 2 For every positive integer n, we have $N_E(2n) = 240\sigma_3(n)$ and $N_{E\oplus E}(2n) = 480\sigma_7(n)$.

Sarnak's interesting book [22] describes similar 'applications of modular forms' to analysis, ergodic theory and graph theory, in particular making use of the following:

THEOREM 3 (Jacobi) $N_{\mathbb{Z}^4}(n) = 8\sum\{d : 1 \leq d \,|\, n,\ 4 \not| \, d\}$. In particular, $N_{\mathbb{Z}^4}(p) = 8(p+1)$ for every prime p.

Unlike Sarnak's examples, where the asymptotic behaviour of $N_{\mathbb{Z}^4}(p)$ is more important than the exact value $8(p+1)$, however, in the constructions of the ovoids $\mathcal{O}_{r,p}(x)$ the exact values $N_E(2p) = 240(p^3+1)$ and $N_{E\oplus E}(2p) = 480(p^7+1)$ are indispensable. A very interesting research problem is to find similar constructions in finite geometry which make use of the exact values $N_{\mathbb{Z}^4}(p) = 8(p+1)$.

REFERENCES

1. M. Biliotti and G. Korchmáros, Some finite translation planes arising from A_6-invariant ovoids of the Klein quadric, *J. Geom., 37:* 29–47 (1990).
2. C. Charnes, Quadratic matrices and the translation planes of order 5^2, in *Coding Theory, Design Theory, Group Theory,* ed. D. Jungnickel and S. A. Vanstone, pp.155–161, Wiley, New York (1993).
3. H. Cohen, *A Course in Computational Algebraic Number Theory,* Springer-Verlag, Berlin (1993).
4. D. A. Cox, *Primes of the Form $x^2 + ny^2$*, Wiley, New York (1989).
5. J. H. Conway, P. B. Kleidman and R. A. Wilson, New families of ovoids in O_8^+, *Geom. Dedicata, 26:* 157–170 (1988).
6. J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups,* 2nd ed., Springer-Verlag, New York (1993).
7. J. E. Humphreys, *Introduction to Lie Algebras and Representation Theory,* Springer-Verlag, New York (1972).
8. W. M. Kantor, Ovoids and translation planes, *Canad. J. Math., 34:* 1195–1207 (1982).
9. H. Lüneburg, *Translation Planes,* Springer-Verlag, New York (1980).
10. G. Mason, Orthogonal geometries over $GF(2)$ and actions of extra-special 2-groups on translation planes, *Europ. J. Combinatorics, 4:* 347–357 (1983).
11. G. Mason, Some translation planes of order 7^2 which admit $SL_2(9)$, *Geom. Dedicata, 17:* 297–305 (1985).
12. G. Mason and T. G. Ostrom, Some translation planes of order p^2 and of extra-special type, *Geom. Dedicata, 17:* 307–322 (1985).
13. G. Mason and E. E. Shult, The Klein correspondence and the ubiquity of certain translation planes, *Geom. Dedicata, 21:* 29–50 (1986).
14. G. E. Moorhouse, Ovoids from the E_8 root lattice, *Geom. Dedicata, 46:* 287–297 (1993).
15. G. E. Moorhouse, Root lattice constructions of ovoids, in *Finite Geometry and Combinatorics,* ed. F. De Clerck et al., pp.269–275, Camb. Univ. Press, Cambridge (1993).
16. G. E. Moorhouse, Two-graphs and skew two-graphs in finite geometries, *Linear Algebra Appl., 226–228:* 529–551 (1995).

17. B. Mwene, On some subgroups of $PSL(4,q),\ q$ odd, *Geom. Dedicata, 12:* 189–199 (1982).
18. N. Nakagawa, Some translation planes of order 11^2 which admit $SL(2,9)$, *Hokkaido Math. J., 20:* 91–107 (1991).
19. T. G. Ostrom, Collineation groups whose order is prime to the characteristic, *Math. Z., 156:* 59–71 (1977).
20. T. G. Ostrom, Elementary abelian 2-groups on the line at infinity of translation planes, *J. Geometry, 17:* 128–139 (1981).
21. T. G. Ostrom, *Lectures on Finite Translation Planes, Conf. Sem. Mat. Univ. Bari,* vol. 191, 31 pp. (1983).
22. P. Sarnak, *Some Applications of Modular Forms*, Camb. Univ. Press, Cambridge (1990).
23. J.-P. Serre, *A Course in Arithmetic,* Springer-Verlag, New York (1973).
24. J. A. Thas, Ovoids and spreads of finite classical polar spaces, *Geom. Dedicata, 10:* 135–144 (1981).