G. ERIC MOORHOUSE

OVOIDS FROM THE E_8 ROOT LATTICE

ABSTRACT. New families of ovoids are constructed in $O_8^+(p)$ for p prime, using the E_8 root lattice, generalising a construction of Conway, Kleidman and Wilson [2]. Using this construction, it appears likely that $O_8^+(p)$ has unboundedly many ovoids as $p \to \infty$.

1. INTRODUCTION

Conway, Kleidman and Wilson [2] have used the E_8 root lattice to construct four infinite families of ovoids in O_8^+ spaces over finite prime fields. This discovery is of great interest to anyone intrigued by the mysteries of lattices; moreover it is significant to finite geometers for two reasons.

(i) It shows that $O_8^+(p)$ contains at least one ovoid for any prime p. (Previously no ovoids were known in $O_8^+(q)$ for $q \equiv 1 \bmod 6,\ q > 7$.)

(ii) Because of their 'unusually' small stabilisers, 'slicing' these ovoids yields large numbers of nonisomorphic ovoids in $O_6^+(p)$, and hence (via the Klein correspondence) large numbers of translation planes, perhaps 'more' than any previous construction (and this may be reasonably interpreted in a precise way).

The main point of this paper (see Theorem 2.1) is to generalise the construction of Conway et al, by showing that for any distinct primes r and p, the E_8 root lattice yields *r-ary* ovoids in $O_8^+(p)$. There is much work left to do: we have not determined the full automorphism groups of these ovoids, nor have we determined all isomorphisms between members of different families. And many such isomorphisms must occur, since Theorem 2.1 gives infinitely many constructions for ovoids in the finite orthogonal space $O_8^+(p)$.

We first introduce the families of r-ary ovoids with $r \leq 7$ in Theorem 1.1, along with certain (not necessarily the full) automorphism groups in $PGO_8^+(p)$ for each respective family. The ovoids $\mathcal{O}_{r,p}(\mathbf{x})$ are defined in Section 2, and Theorem 1.1 is proven in Sections 3 and 4.

1.1 THEOREM. *For any distinct primes r and p, the E_8 root lattice yields r-ary ovoids $\mathcal{O}_{r,p}(\mathbf{x})$ in $O_8^+(p)$, constructed as in Section 2. For $r \in \{2,3\}$ these are the ovoids of Conway et al [2], namely the ovoids*

$\mathcal{O}_{2,p}\big(\frac{1}{2}(1^8)\big)$ *(binary ovoids) for $p>2$, admitting $2\times Sp_6(2)$;*

$\mathcal{O}_{3,p}(2,0^7)$ *(ternary ovoids of the first kind) for $p\equiv 1$ mod 3, admitting $2^6{:}S_7$;*

$\mathcal{O}_{3,p}\big(\frac{1}{2}(1^8)\big)$ *(ternary ovoids of the second kind) for $p\equiv 2$ mod 3, $p>2$, admitting $2\times Sp_6(2)$; and*

$\mathcal{O}_{3,p}(1^7,-1)$ *(ternary ovoids of the third kind) for $p\equiv 2$ mod 3, admitting S_9.*

There are six families of quintary ovoids: for $p\equiv\pm 1$ mod 5, we have

$\mathcal{O}_{5,p}\big(\frac{1}{2}(1^8)\big)$ *admitting $2\times Sp_6(2)$,*

$\mathcal{O}_{5,p}(1^7,-1)$ *admitting S_8, and*

$\mathcal{O}_{5,p}(2^3,0^5)$ *admitting $S_3\times 2^4{:}S_5$;*

while for $p\equiv\pm 2$ mod 5, we have

$\mathcal{O}_{5,p}(2,0^7)$ *(for $p>3$) admitting $2^6{:}S_7$,*

$\mathcal{O}_{5,p}(1^6,0^2)$ *(for $p>2$) admitting $2\times U_4(2){:}2$, and*

$\mathcal{O}_{5,p}\big(\frac{1}{2}(7,1^6,-1)\big)$ *admitting $2\times S_7$.*

There are eleven families of heptary ovoids: for $p\equiv 1,2,4$ mod 7 we have

$\mathcal{O}_{7,p}(1^6,0^2)$ *(for $p>2$) admitting $2\times U_4(2){:}2$,*

$\mathcal{O}_{7,p}(3,1,0^6)$ *(for $p>2$) admitting $2^5{:}S_6$,*

$\mathcal{O}_{7,p}(2^3,0^5)$ *(for $p>2$) admitting $S_3\times 2^4{:}S_5$,*

$\mathcal{O}_{7,p}(2^5,0^3)$ *admitting $S_4\times S_5$, and*

$\mathcal{O}_{7,p}(3^2,1^5,-1)$ *admitting $2\times S_6$;*

while for $p\equiv 3,5,6$ mod 7, we have

$\mathcal{O}_{7,p}\big(\frac{1}{2}(1^8)\big)$ *(for $p>3$) admitting $2\times Sp_6(2)$,*

$\mathcal{O}_{7,p}(2,0^7)$ *(for $p>5$) admitting $2^6{:}S_7$,*

$\mathcal{O}_{7,p}(1^7,-1)$ *(for $p>3$) admitting S_8,*

$\mathcal{O}_{7,p}(3,1^7)$ *admitting S_7,*

$\mathcal{O}_{7,p}(4,1^2,0^5)$ *admitting $2\times 2^4{:}S_5$, and*

$\mathcal{O}_{7,p}\big(\frac{1}{2}(5^3,3^4,-3)\big)$ *admitting $2\times S_3\times S_5$.*

The presently known ovoids in $O_8^+(q)$ are summarised in [2], [4] and herein; and in case $q=p$ is prime, these are just the unitary ovoids of [4] and the r-ary ovoids $\mathcal{O}_{r,p}(\mathbf{x})$. We list these below (List 1.2) for $p\le 11$. The isomorphisms and nonisomorphisms implicit in List 1.2 are justified in Section 4. Only one ovoid in this list (item (x)) is actually new, and an explicit coördinate description of this ovoid is given in Section 3. However using

computer construction, we have found evidence of large numbers of new r-ary ovoids for large p. Indeed it is now reasonable to hope that as the prime $p \to \infty$, the number of inequivalent ovoids in $O_8^+(p)$ tends to ∞. Previously, at most four ovoids were known in $O_8^+(p)$ for any prime p.

1.2 LIST. The known (isomorphism types of) ovoids in $O_8^+(p)$ for primes $p \leq 11$ are as follows, together with their full automorphism groups in $PGO_8^+(p)$.

For $p = 2$, a unique ovoid:

(i) $\mathcal{O}_{3,2}(1^7, -1)$, admitting S_9.

For $p = 3$, a unique ovoid:

(ii) $\mathcal{O}_{2,3}\big(\frac{1}{2}(1^8)\big)$, admitting $2 \times Sp_6(2)$.

For $p = 5$, three known ovoids:

(iii) $\mathcal{O}_{2,5}\big(\frac{1}{2}(1^8)\big) = \mathcal{O}_{3,5}\big(\frac{1}{2}(1^8)\big)$ admitting $2 \times Sp_6(2)$,

(iv) the Cooperstein ovoid $\mathcal{O}_{3,5}(1^7, -1)$ admitting S_{10}, and

(v) a unitary ovoid (see [4]) admitting $PGU(3, 5)$.

For $p = 7$, two known ovoids:

(vi) $\mathcal{O}_{2,7}\big(\frac{1}{2}(1^8)\big) \cong \mathcal{O}_{5,7}(1^6, 0^2)$ admitting $2 \times Sp_6(2)$, and

(vii) the Shult ovoid $\mathcal{O}_{3,7}(2, 0^7) \cong \mathcal{O}_{5,7}(2, 0^7) \cong \mathcal{O}_{5,7}\big(\frac{1}{2}(7, 1^6, -1)\big)$ admitting $2 \times 2^6{:}S_7$.

For $p = 11$, five known ovoids:

(viii) $\mathcal{O}_{2,11}\big(\frac{1}{2}(1^8)\big) \cong \mathcal{O}_{7,11}(1^6, 0^2)$ admitting $2 \times Sp_6(2)$;

(ix) $\mathcal{O}_{3,11}\big(\frac{1}{2}(1^8)\big) = \mathcal{O}_{5,11}\big(\frac{1}{2}(1^8)\big) \cong \mathcal{O}_{7,11}(3, 1, 0^6)$ admitting $2 \times Sp_6(2)$;

(x) $\mathcal{O}_{3,11}(1^7, -1) \cong \mathcal{O}_{5,11}(1^7, -1) \cong \mathcal{O}_{7,11}(2^5, 0^3)$ admitting S_9;

(xi) $\mathcal{O}_{5,11}(2^3, 0^5) \cong \mathcal{O}_{7,11}(2^3, 0^5) \cong \mathcal{O}_{7,11}(3^2, 1^5, -1)$ admitting $S_3 \times 2^5{:}S_6$; and

(xii) a unitary ovoid (see [4]) admitting $PGU(3, 11)$.

Each of the ovoids (i)–(iv),(vi)–(xi) above admits many (probably infinitely many) r-ary constructions, although we have chosen here to list no more than three constructions per ovoid. It is conceivable that new ovoids may yet appear by the r-ary construction for $p \in \{5, 7, 11\}$, although this seems unlikely, and would require $r \geq 17$, since we have exhaustively considered all possibilities with $p \leq 11$ and $r \leq 13$ by computer.

2. The Construction

Let E denote the E_8 root lattice, i.e. E is the set of all vectors in $\mathbb{R}^8$ of the form $\frac{1}{2}(a_1, a_2, \ldots, a_8)$ such that $a_i \in \mathbb{Z}$, $a_1 \equiv a_2 \equiv \ldots \equiv a_8 \mod 2$, and $\sum a_i \equiv 0 \mod 4$. It

is well known that E is self-dual, and that every vector $\mathbf{v} \in E$ has even norm. (Recall that the *norm* of $\mathbf{v} \in E$ is $\mathbf{v} \cdot \mathbf{v}$, where '$\cdot$' denotes the standard inner product on $\mathbb{R}^8$.) Let

$$E_{2m} = \{\mathbf{v} \in E \,:\, \mathbf{v} \cdot \mathbf{v} = 2m\}, \quad N_E(2m) = |E_{2m}|,$$

and for a positive integer n, let $nE_{2m} = \{n\mathbf{v} \,:\, \mathbf{v} \in E_{2m}\}$. Observe that E_2 is just the set of 240 *root vectors* of the lattice E. It is also known (see [3]) that

$$N_E(2m) = \begin{cases} 1, & m = 0; \\ 240\sigma_3(m), & m = 1, 2, 3, \ldots . \end{cases}$$

where $\sigma_k(m) = \sum d^k$, summing over all positive d dividing m. For any prime p, the quotient E/pE is an 8-dimensional vector space over $\mathbb{F}_p$. Let $\overline{\ }$ denote the reduction modulo p, so that $\overline{\mathbf{x}} \in \overline{E} = E/pE$ for $\mathbf{x} \in E$, and $\overline{a} \in \mathbb{F}_p$ for $a \in \mathbb{Z}$. For $\mathbf{x} \in E \smallsetminus pE$, the *point* represented by $\overline{\mathbf{x}}$ is the one-dimensional subspace $\langle \overline{\mathbf{x}} \rangle = \mathbb{F}_p \overline{\mathbf{x}}$. Now $\overline{E}$ inherits from E a quadratic form, namely

$$Q : \overline{E} \to \mathbb{F}_p, \qquad Q(\overline{\mathbf{x}}) = \overline{\tfrac{1}{2}\mathbf{x} \cdot \mathbf{x}}\,.$$

The associated bilinear form is just the reduction of the inner product on E, and we denote this also by '$\cdot$', thus:

$$\overline{\mathbf{x}} \cdot \overline{\mathbf{y}} = Q(\overline{\mathbf{x}} + \overline{\mathbf{y}}) - Q(\overline{\mathbf{x}}) - Q(\overline{\mathbf{y}}) = \overline{\mathbf{x} \cdot \mathbf{y}}\,.$$

The quadratic form Q is nondegenerate, and $\overline{E}$ has Witt defect 0 with this form, and so $\overline{E}$ becomes an $O_8^+(p)$ orthogonal space with quadratic form $Q(\overline{\mathbf{x}}) = \overline{\frac{1}{2}\mathbf{x} \cdot \mathbf{x}}$. Points $\langle \overline{\mathbf{x}} \rangle$ and $\langle \overline{\mathbf{y}} \rangle$ are *perpendicular* if $\overline{\mathbf{x}} \cdot \overline{\mathbf{y}} = 0$; point $\langle \overline{\mathbf{x}} \rangle$ is *singular* if $Q(\overline{\mathbf{x}}) = 0$. A *$k$-cap* in $\overline{E}$ is a set of k mutually nonperpendicular singular points of $\overline{E}$. It is well known that any cap in $\overline{E}$ has size $\leq p^3 + 1$, and a (p^3+1)-cap in $\overline{E}$ is called an *ovoid*.

Now assume that r and p are distinct primes, and for each positive integer $i \leq \lfloor \frac{r}{2} \rfloor$, let $n_i = n_i(r)$ be the integer uniquely determined by $1 \leq n_i \leq \lfloor \frac{r}{2} \rfloor$, $i^2 n_i^2 \equiv 1 \mod r$. Define

$$\mathcal{S}_{r,p} = \bigcup_{i=1}^{\lfloor r/2 \rfloor} n_i E_{2i(r-i)p}, \quad \mathcal{S}'_{r,p} = \bigcup_{i=1}^{\lfloor r/2 \rfloor} n_i p E_{2i(r-i)/p} \subset \mathcal{S}_{r,p}$$

where $E_{2i(r-i)/p} = \emptyset$ unless $p \mid i(r-i)$. Next, partition $\mathcal{S}_{r,p}$ into its congruence classes modulo rE, as follows. For each $\mathbf{x} \in E$ such that $-p(\mathbf{x} \cdot \mathbf{x})/2$ is a nonzero square modulo r, let $n_{\mathbf{x}} = n_{\mathbf{x}}(r,p)$ be the unique integer satisfying $1 \leq n_{\mathbf{x}} \leq \lfloor \frac{r}{2} \rfloor$, $(\mathbf{x} \cdot \mathbf{x}) n_{\mathbf{x}}^2 \equiv -2p \mod r$ (so that $n_{\mathbf{v}} = 1$ for all $\mathbf{v} \in \mathcal{S}_{r,p}$) and define

$$[\mathbf{x}]_{r,p} = \{\mathbf{v} \in \mathcal{S}_{r,p} \,:\, \mathbf{v} \equiv n_{\mathbf{x}} \mathbf{x} \mod rE\}.$$

Reducing each class $[\mathbf{x}]_{r,p}$ modulo p gives

$$\mathcal{O}_{r,p}(\mathbf{x}) = \left\{ \langle \overline{\mathbf{v}} \rangle \in \overline{E} \,:\, \mathbf{v} \in [\mathbf{x}]_{r,p} \smallsetminus pE \right\},$$

where $\overline{E} = E/pE$. The deletion of pE in the latter definition, ensures that $\mathcal{O}_{r,p}(\mathbf{x})$ consists of (singular) points of $\overline{E}$.

2.1 THEOREM. *Let r and p be distinct primes, and suppose $\mathbf{x} \in E$ such that $-p(\mathbf{x}\cdot\mathbf{x})/2$ is a nonzero square modulo r. Then $\mathcal{O}_{r,p}(\mathbf{x})$ is an ovoid if and only if $\big(n_{\mathbf{x}}\mathbf{x} + rE\big) \cap \mathcal{S}'_{r,p}$ is empty. If $r < p$ then the latter criterion is necessarily satisfied, and if $r > p$, there exists $\mathbf{x} \in E$ satisfying this criterion.*

We use a series of lemmas to prove Theroem 2.1. The binary ovoids of [2] are just the ovoids $\mathcal{O}_{2,p}(\mathbf{x})$ for $\mathbf{x} \in E_2$, and so for the remainder of Section 2 we assume that r is odd.

2.2 LEMMA. *Suppose that $\mathbf{u}, \mathbf{v} \in [\mathbf{x}]_{r,p}$. Then $Q(\overline{\mathbf{u}}) = 0$, and $\mathbf{u}\cdot\mathbf{v} \equiv 0 \mod p$ if and only if $\mathbf{u} = \mathbf{v}$.*

Proof of Lemma 2.2. The first conclusion is obvious. To prove the second conclusion, suppose that $\mathbf{u}, \mathbf{v} \in [\mathbf{x}]_{r,p}$ with $\mathbf{u}\cdot\mathbf{v} \equiv 0 \mod p$. Since $\mathbf{u} \equiv n_{\mathbf{x}}\mathbf{x} \equiv \mathbf{v} \mod rE$, we have $\mathbf{u} - \mathbf{v} \in rE$, so that $\|\mathbf{u}-\mathbf{v}\|^2 \equiv 0 \mod 2r^2$. Also $\|\mathbf{u}-\mathbf{v}\|^2 = \|\mathbf{u}\|^2 + \|\mathbf{v}\|^2 - 2\mathbf{u}\cdot\mathbf{v} \equiv 0 \mod 2p$, and so $\|\mathbf{u}-\mathbf{v}\|^2 \equiv 0 \mod 2r^2p$. We have $\mathbf{u} \in n_i E_{2i(r-i)p}$ and $\mathbf{v} \in n_j E_{2j(r-j)p}$ for some i, j.

Consider first the case $i = j$. Then $\mathbf{u} - \mathbf{v} \in n_i E$, so $\|\mathbf{u}-\mathbf{v}\|^2 \equiv 0 \mod 2n_i^2$, and together with the previous congruence, this implies $\|\mathbf{u}-\mathbf{v}\|^2 \equiv 0 \mod 2r^2pn_i^2$. However,

$$\|\mathbf{u}-\mathbf{v}\|^2 \le \big(\|\mathbf{u}\| + \|\mathbf{v}\|\big)^2 = \Big(n_i\sqrt{2i(r-i)p} + n_i\sqrt{2i(r-i)p}\Big)^2 = 8i(r-i)pn_i^2 < 2r^2pn_i^2.$$

Consequently $\|\mathbf{u}-\mathbf{v}\|^2 = 0$, i.e. $\mathbf{u} = \mathbf{v}$.

Henceforth assume that $i \ne j$. Then $\mathbf{u}\cdot\mathbf{v} \equiv 0 \mod n_i n_j$, and so $\mathbf{u}\cdot\mathbf{v} \equiv 0 \mod n_i n_j p$. Write $\mathbf{u}\cdot\mathbf{v} = n_i n_j pk$, where $|k| \le \sqrt{4ij(r-i)(r-j)} < r^2/2$ by the Cauchy-Schwarz inequality. Furthermore from $\|\mathbf{u}-\mathbf{v}\|^2 \equiv 0 \mod 2r^2p$ we obtain

$$n_i n_j k \equiv i(r-i)n_i^2 + j(r-j)n_j^2 \mod r^2.$$

Now define $k_0 = (i+j)r - 2ij$. The reader may verify that

$$k_0^2 = \big[(i+j)r - 2ij\big]^2 = (i-j)^2r^2 + 4ij(r-i)(r-j)\,.$$

Since $i^2n_i^2 \equiv j^2n_j^2 \equiv 1 \mod r$, we have $\big[i(r-i)n_i^2 - j(r-j)n_j^2\big]^2 \equiv 0 \mod r^2$, and so

$$n_i^2n_j^2k_0^2 \equiv 4ij(r-i)(r-j)n_i^2n_j^2 \equiv \big[i(r-i)n_i^2 + j(r-j)n_j^2\big]^2 \equiv n_i^2n_j^2k^2 \mod r^2.$$

Since $\gcd(n_i^2n_j^2,\, r^2) = 1$, we have $k^2 \equiv k_0^2 \mod r^2$, i.e. $r^2 \mid (k+k_0)(k-k_0)$. Clearly $r \nmid k_0$, and so either $r^2 \mid (k+k_0)$ or $r^2 \mid (k-k_0)$, i.e. $k \equiv \pm k_0 \mod r^2$. Also $|k| < r^2/2$ and $|k_0| < r^2/2$, so necessarily $k = \pm k_0$; but then $|k| = |k_0| = \sqrt{(i-j)^2r^2 + 4ij(r-i)(r-j)} > \sqrt{4ij(r-i)(r-j)}$, a contradiction. This completes the proof of Lemma 2.2.

2.3 LEMMA. *If* $(n_{\mathbf{x}}\mathbf{x}+rE)\cap\mathcal{S}'_{r,p}\neq\emptyset$, *then* $\big|[\mathbf{x}]_{r,p}\big|=1$ *and* $\mathcal{O}_{r,p}(\mathbf{x})=\emptyset$. *If* $\big|[\mathbf{x}]_{r,p}\big|\geq 2$ *then* $(n_{\mathbf{x}}\mathbf{x}+rE)\cap\mathcal{S}'_{r,p}=\emptyset$ *and* $\mathcal{O}_{r,p}(\mathbf{x})$ *is a cap in* $\overline{E}$ *of size* $\big|\mathcal{O}_{r,p}(\mathbf{x})\big|=\big|[\mathbf{x}]_{r,p}\big|\leq p^3+1$.

Proof of Lemma 2.3. Suppose first that $p\mathbf{v}\in(n_{\mathbf{x}}\mathbf{x}+rE)\cap n_i pE_{2i(r-i)/p}$. Then Lemma 2.2 gives $[\mathbf{x}]_{r,p}=\{p\mathbf{v}\}$ and we are done.

Now suppose that $\big|[\mathbf{x}]_{r,p}\big|\geq 2$. Then Lemma 2.2 shows that $[\mathbf{x}]_{r,p}\cap pE=\emptyset$ and that the reduction $[\mathbf{x}]_{r,p}\to\mathcal{O}_{r,p}(\mathbf{x})$, $\mathbf{v}\mapsto\overline{\mathbf{v}}$ is one-to-one, and furthermore that $\mathcal{O}_{r,p}(\mathbf{x})$ is a cap in $\overline{E}$. Since every cap in $\overline{E}$ has size $\leq p^3+1$, the proof of Lemma 2.3 is complete.

2.4 LEMMA. $\big|\mathcal{S}_{r,p}\big|+p^3\big|\mathcal{S}'_{r,p}\big|=r^3(r^4-1)(p^3+1)$.

Proof of Lemma 2.4. Since p cannot divide both i and $r-i$,

$$\big|\mathcal{S}'_{r,p}\big|=240\sum_{\substack{1\leq i\leq\frac{r-1}{2}\\ p\mid i}}\sigma_3\big(\frac{i}{p}\big)\sigma_3\big(r-i\big)\;+\;240\sum_{\substack{1\leq i\leq\frac{r-1}{2}\\ p\mid(r-i)}}\sigma_3\big(i\big)\sigma_3\big(\frac{r-i}{p}\big)$$

using the multiplicativity of σ_3. Also

$$\big|\mathcal{S}_{r,p}\big|=240\sum_{1\leq i\leq(r-1)/2}\sigma_3\big(i(r-i)p\big).$$

In case $p\,\big|\,i$, it is easy to show that $\sigma_3\big(ip\big)+p^3\sigma_3\big(\frac{i}{p}\big)=(p^3+1)\sigma_3\big(i\big)$. In case $p\,\big|\,(r-i)$ a similar identity holds, and so term-by-term comparison yields

$$\begin{aligned}\big|\mathcal{S}_{r,p}\big|+p^3\big|\mathcal{S}'_{r,p}\big|&=240(p^3+1)\sum_{i=1}^{(r-1)/2}\sigma_3(i)\sigma_3(r-i)\\&=120(p^3+1)\sum_{i=1}^{r-1}\sigma_3(i)\sigma_3(r-i)\,,\\\frac{480}{p^3+1}\Big(\big|\mathcal{S}_{r,p}\big|+p^3\big|\mathcal{S}'_{r,p}\big|\Big)&=\sum_{i=1}^{r-1}N_E(2i)N_E(2r-2i)\\&=-480(r^3+1)+\sum_{i=0}^{r}N_E(2i)N_E(2r-2i)\\&=-480(r^3+1)+N_{E\oplus E}(2r)\end{aligned}$$

where $N_{E\oplus E}(2r)$ is the number of vectors of norm $2r$ in the lattice $E^2=E\oplus E$. It is known (see [6]) that $N_{E\oplus E}(2r)=480\sigma_7(r)=480(r^7+1)$, whence Lemma 2.4 follows.

It is generally known that an $O_8^+(r)$ space has $r^3(r^4+r-1)$ singular vectors, and $r^3(r^4-1)(r-1)$ nonsingular vectors, whose Q-values are evenly distributed among the $r-1$ nonzero values of $\mathbb{F}_r$. Partition $\mathcal{S}_{r,p}$ into its congruence classes modulo rE as

$$\mathcal{S}_{r,p}=\bigcup_{\mathbf{v}\in T}[\mathbf{v}]_{r,p},$$

where $T = T(r,p)$ is a set of representatives of the distinct nonempty classes $[\mathbf{v}]_{r,p}$ in $\mathcal{S}_{r,p}$. Now $|T| \le r^3(r^4-1)$, in which equality holds if and only if $\mathcal{S}_{r,p}$ meets each of the $r^3(r^4-1)$ cosets $\mathbf{v}+rE$ in E such that $\mathbf{v}\cdot\mathbf{v} \equiv -2p \mod r$. Also Lemma 2.3 gives $\big|[\mathbf{v}]_{r,p}\big| = 1$ for $\mathbf{v} \in \mathcal{S}'_{r,p} \subseteq T$, and $\big|[\mathbf{v}]_{r,p}\big| \le p^3+1$ for $\mathbf{v} \in T \setminus \mathcal{S}'_{r,p}$. Thus

$$\begin{aligned}\big|\mathcal{S}_{r,p}\big| &\le \big|\mathcal{S}'_{r,p}\big| + (p^3+1)\big|T \setminus \mathcal{S}'_{r,p}\big| \\ &= (p^3+1)\big|T\big| - p^3\big|\mathcal{S}'_{r,p}\big| \\ &\le (p^3+1)r^3(r^4-1) - p^3\big|\mathcal{S}'_{r,p}\big|.\end{aligned}$$

But by Lemma 2.4, we must have equality in the above. This gives $\big|[\mathbf{v}]_{r,p}\big| = p^3+1$ and $\mathcal{O}_{r,p}(\mathbf{v})$ is and ovoid in $\overline{E}$ whenever $\mathbf{v} \in T \setminus \mathcal{S}'_{r,p}$; also $|T| = r^3(r^4-1)$ and $\mathcal{S}_{r,p}$ meets every coset $\mathbf{v}+rE$ such that $\mathbf{v}\cdot\mathbf{v} \equiv -2p \mod r$. Thus $[\mathbf{x}]_{r,p} = [\mathbf{v}]_{r,p}$ for some $\mathbf{v} \in T$, and the first conclusion of Theorem 2.1 follows.

If $r < p$ then $p \not| \, i(r-i)$ for all positive $i \le \lfloor \frac{r}{2} \rfloor$, so $\mathcal{S}'_{r,p} = \emptyset$. If $r > p$ then there exists $i \le \lfloor \frac{r}{2} \rfloor$ such that $p \not| \, i(r-i)$, so $\mathcal{S}'_{r,p} \subsetneq \mathcal{S}_{r,p}$. This proves the second conclusion of the Theorem.

3. Automorphisms of Ovoids

By definition, the *full stabiliser* of the ovoid $\mathcal{O} = \mathcal{O}_{r,p}(\mathbf{x})$ is the largest subgroup of $G = PGO_8^+(p)$ leaving $\mathcal{O}$ invariant, denoted $N_G(\mathcal{O})$. The *full automorphism group* of $\mathcal{O}$ is $\mathrm{Aut}(\mathcal{O}) = N_G(\mathcal{O})/C_G(\mathcal{O})$, where $C_G(\mathcal{O})$ is the pointwise stabiliser of $\mathcal{O}$, so $C_G(\mathcal{O}) \supseteq Z = Z(G)$. The most obvious subgroups of $\mathrm{Aut}(\mathcal{O})$ are those induced by subgroups of the Weyl group W of the lattice E, as given by the following proposition, whose proof is left to the reader.

3.1 PROPOSITION. *Suppose $\mathcal{O}_{r,p}(\mathbf{x})$ is an ovoid (i.e. r and p are distinct primes, $\mathbf{x} \in E$ such that $-p(\mathbf{x}\cdot\mathbf{x})/2$ is a nonzero square modulo r, and $(n_{\mathbf{x}}\mathbf{x}+rE) \cap \mathcal{S}'_{r,p} = \emptyset$). Then*

(i) $\mathcal{O}_{r,p}(a\mathbf{x}^g + r\mathbf{u}) \cong \mathcal{O}_{r,p}(\mathbf{x})$ whenever $g \in W$, $\mathbf{u} \in E$ and $r \not| \, a \in \mathbb{Z}$, and in particular,

(ii) $\mathrm{Aut}\big(\mathcal{O}_{r,p}(\mathbf{x})\big)$ contains $W_{\mathbf{x}+rE}\langle -1\rangle / \langle -1\rangle$, where $W_{\mathbf{x}+rE}$ is the stabiliser in W of the coset $\mathbf{x}+rE$ in E.

The subgroups of $\mathrm{Aut}(\mathcal{O})$ listed in Theorem 1.1 for $r \le 7$ are just those guaranteed by Proposition 3.1(ii). We have $W_{\mathbf{x}+rE} \supseteq W_{\mathbf{x}}$ with equality in case $r \in \{5,7\}$ where $\mathbf{x}$ is the unique shortest vector in $\mathbf{x}+rE$, so these groups may be found by referring to Proposition 3.2 and Table 3.3. Note that W is transitive on E_{2m} for $2m \in \{2,4,6,10,12\}$,

and in Table 3.3 we have chosen a representative $\mathbf{x} \in E_{2m}$ and denoted the stabiliser $W_{\mathbf{x}}$ by W_{2m}. For $2m \in \{8, 14, \ldots, 30\}$, W is no longer transitive on E_{2m}, and in this case $E_{2m}^* \subset E_{2m}$ is the W-orbit having the indicated representative $\mathbf{x}$, and $W_{2m}^* = W_{\mathbf{x}}$. (Warning: $W_{\mathbf{x}+rE} \supsetneq W_{\mathbf{x}}$ is possible for $r \leq 3$. For example, $W_{\mathbf{x}+2E} = W_{\mathbf{x}}\langle -1 \rangle$ for any $\mathbf{x} \in E_2$; and in case $\mathbf{x} \in E_8^*$, we have $W_{\mathbf{x}+3E} \cong S_9$ and $W_{\mathbf{x}} \cong S_8$. These cases are treated in [2].)

3.2 PROPOSITION. *Table 3.3 lists several W-orbits on E and their stabilisers. Furthermore,*

(i) $2E_4 \cup E_6 \cup 2E_{14}^*$ *is a set of representatives of the 78000 distinct cosets* $\mathbf{x} + 5E$ *in E such that* $\mathbf{x} \cdot \mathbf{x} \equiv 1 \mod 5$, *and* $E_2 \cup 2E_8^* \cup E_{12}$ *is a set of reps of the 78000 cosets* $\mathbf{x} + 5E$ *in E with* $\mathbf{x} \cdot \mathbf{x} \equiv 2 \mod 5$.

(ii) $2E_2 \cup 3E_4 \cup E_8^* \cup 2E_{16}^* \cup 3E_{18}^* \cup 2E_{30}^*$ *is a set of representatives of the 823200 distinct cosets* $\mathbf{x}+7E$ *such that* $\mathbf{x} \cdot \mathbf{x} \equiv 1 \mod 7$, *and* $2E_6 \cup E_{10} \cup 3E_{12} \cup 2E_{20}^* \cup E_{24}^*$ *is a set of reps of the 823200 cosets* $\mathbf{x} + 7E$ *with* $\mathbf{x} \cdot \mathbf{x} \equiv 3 \mod 7$.

The proof of Proposition 3.2 is omitted. Coset representatives for rE with other norms modulo $r \in \{5, 7\}$ are obtained by appropriately scaling the representatives given in Proposition 3.2; for example, for the 78000 cosets $\mathbf{x} + 5E$ with $\mathbf{x} \cdot \mathbf{x} \equiv 3 \mod 5$, as a set of coset representatives we may choose $2E_2 \cup E_8^* \cup 2E_{12}$. Since 1 and 2 represent the squares and nonsquares in $\mathbb{F}_5$ (similarly 1 and 3 in $\mathbb{F}_7$), the representatives given in Prop. 3.2 suffice for $\mathbf{x} \cdot \mathbf{x} \not\equiv 0 \mod r$. We remark that the analogue of Proposition 3.2 was obtained by computer for $r = 11, 13$, with significantly more numerous W-orbits, yielding exactly 34 families of 11-ary ovoids and 55 families of 13-ary ovoids.

The entries in Table 3.3 may be verified with little more than a knowledge that $|W| = 696,729,600$ and $|E_{2m}| = 240\sigma_3(m)$ for $m \geq 1$. In most cases the stabiliser of the chosen representative in W can be readily identified within the monomial subgroup $2^7{:}S_8 < W$.

The ovoids listed in List 1.2, and their full automorphism groups, are previously known, with the exception of $\mathcal{O}_{5,11}(2^3, 0^5)$. Transforming $\mathcal{O}_{5,11}(2^3, 0^5)$ by $\left(\begin{smallmatrix} 5 & 4 & 2 \\ 4 & 5 & 2 \\ 2 & 2 & 2 \end{smallmatrix}\right) \oplus I_5 \in PGO_8^+(11)$ gives an equivalent ovoid $\mathcal{O}$ in $O_8^+(11)$. (Here I_n is the $n \times n$ identity matrix.) One may verify that $\mathcal{O}$ admits $G_1 G_2 < PGO_8^+(11)$ where $G_1 = \left\langle \left(\begin{smallmatrix} 5 & 3 \\ 8 & 5 \end{smallmatrix}\right) \oplus I_6 \,,\, \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \oplus I_6 \right\rangle \cong S_3$ and $G_2 \cong 2^5{:}S_6$ acting monomially on the last six coördinates. Furthermore $\mathcal{O}$ has four orbits under $G_1 G_2 = G_1 \times G_2$, with respective lengths $36 + 240 + 480 + 576 = 1332$ and representatives $\langle (1^2, 0^5, 3) \rangle$, $\langle (0^2, 1^4, 3, 8) \rangle$, $\langle (1^2, 0^3, 5^3) \rangle$ and $\langle (1, 10, 4, 5^5) \rangle$. From this description and [5], one easily checks that $G_1 \times G_2$ is in fact the full automorphism group of $\mathcal{O}$.

Orbit of W	Representative	Length of Orbit	Stabiliser in W
E_2	$\frac{1}{2}(1^8)$	240	$W_2 \cong 2 \times Sp_6(2)$
E_4	$(2, 0^7)$	2160	$W_4 \cong 2^6{:}S_7$
E_6	$(1^6, 0^2)$	6720	$W_6 \cong 2 \times U_4(2){:}2$
$E_8^* = E_8 \searrow 2E_2$	$(1^7, -1)$	17280	$W_8^* \cong S_8$
E_{10}	$(3, 1, 0^6)$	30240	$W_{10} \cong 2^5{:}S_6$
E_{12}	$(2^3, 0^5)$	60480	$W_{12} \cong S_3 \times 2^4{:}S_5$
$E_{14}^* \subset E_{14}$	$\frac{1}{2}(7, 1^6, -1)$	69120	$W_{14}^* \cong 2 \times S_7$
$E_{16}^* = E_{16} \searrow 2E_4$	$(3, 1^7)$	138240	$W_{16}^* \cong S_7$
$E_{18}^* = E_{18} \searrow 3E_2$	$(4, 1^2, 0^5)$	181440	$W_{18}^* \cong 2 \times 2^4{:}S_5$
$E_{20}^* \subset E_{20}$	$(2^5, 0^3)$	241920	$W_{20}^* \cong S_4 \times S_5$
$E_{24}^* = E_{24} \searrow 2E_6$	$(3^2, 1^5, -1)$	483840	$W_{24}^* \cong 2 \times S_6$
$E_{30}^* \subset E_{30}$	$\frac{1}{2}(5^3, 3^4, -3)$	483840	$W_{30}^* \cong 2 \times S_3 \times S_5$

TABLE 3.3: Selected W-orbits on E

The full automorphism groups for $r = 2, 3$ were determined by Conway et al [2], using largely the classification of maximal subgroups of G found in [5]. We have not yet progressed this far in the case $r \geq 5$. One problem is that as r increases, the stabilisers in W typically decrease, and so we can expect that there are many more overgroups in G to be eliminated.

4. Isomorphisms Between Ovoids

We first describe an isomorphism invariant of ovoids in $O^+_{2n}(q)$ spaces for q odd, which is highly effective in distinguishing non-isomorphic ovoids by computer. For $n = 3$ this is an isomorphism invariant of the corresponding translation plane of order q^2, and is due to Conway; see [1].

Let $\{v_i \,:\, 1 \leq i \leq q^{n-1}+1\}$ be nonzero vectors in $O^+_{2n}(q)$ representing the points of a given ovoid $\mathcal{O}$. For $1 \leq i, j \leq q^{n-1}+1$, define a_{ij} to be 0 if $i = j$, or ± 1 according as the bilinear form value $(v_i\,, v_j)$ is or is not a square in $\mathbb{F}_q$. The square matrix $A = \big(a_{ij}\big)$ is determined by $\mathcal{O}$ to within conjugation by a ± 1-monomial matrix, as is AA^{T}. Let $|AA^{\mathrm{T}}|$ denote the $(q^{n-1}+1) \times (q^{n-1}+1)$ matrix over $\mathbb{Z}$, obtained by replacing each entry of AA^{T}

by its absolute value. The *fingerprint* of $\mathcal{O}$ is the list of those integers occurring as entries in $|AA^{\mathrm{T}}|$, together with their frequencies, and this is an isomorphism invariant of $\mathcal{O}$. It is not known whether two nonisomorphic ovoids in $O^+_{2n}(q)$ for q odd and $n \geq 3$ can have the same fingerprint, although for $n = 2$ such examples are easily obtained.

These fingerprints successfully distinguished between the known ovoids for $p \in \{5, 7, 11\}$, thereby confirming the nonisomorphisms implicit in List 1.2. For example for $p = 7$ the two fingerprints obtained were, respectively,

(vi) $6^{40320}18^{1512}22^{32256}34^{40320}82^{1512}202^{2016}234^{56}343^{344}$,

(vii) $2^{37632}10^{6720}14^{22400}18^{20160}26^{6720}34^{20160}58^{2240}118^{280}146^{840}242^{840}343^{344}$.

Obtaining isomorphisms between ovoids having the same fingerprint was not particularly easy unless the ovoids happened to coincide. Those isomorphisms claimed in List 1.2 were found by computer, using a Monte Carlo approach. Here we state only one of these isomorphisms explicitly, by way of example: the orthogonal transformation

$$\begin{pmatrix} 1 & 6 & 1 & 1 & 1 & 6 & 6 & 6 \\ 6 & 4 & 4 & 3 & 3 & 4 & 4 & 4 \\ 6 & 4 & 3 & 3 & 4 & 4 & 4 & 4 \\ 6 & 4 & 3 & 3 & 3 & 4 & 4 & 3 \\ 6 & 3 & 3 & 3 & 3 & 4 & 4 & 4 \\ 6 & 4 & 3 & 3 & 3 & 3 & 4 & 4 \\ 6 & 4 & 3 & 3 & 3 & 4 & 3 & 4 \\ 1 & 3 & 4 & 3 & 4 & 3 & 3 & 3 \end{pmatrix} \in PGO^+_8(7)$$

takes $\mathcal{O}_{5,7}\big(\frac{1}{2}(7, 1^6, -1)\big)$ to $\mathcal{O}_{3,7}(2, 0^7)$.

6. Further Questions

This construction raises more questions than it answers. Some are as follows.

(i) Does the number of inequivalent r-ary ovoids in $O^+_8(p)$ tend to ∞ as $p \to \infty$?

(ii) The subgroups of $\mathrm{Aut}(\mathcal{O})$ promised by Proposition 3.1 can be made arbitrarily small for large p. How small can $\mathrm{Aut}(\mathcal{O})$ be? Especially, do there exist ovoids with trivial automorphism group?

(iii) Settle the isomorphism questions, especially between r-ary and s-ary ovoids in $O^+_8(p)$ for distinct primes r, s and p. Also show, if possible, that $\mathcal{O}_{r,p}(\mathbf{x})$ is never a unitary ovoid.

(iv) Does $O^+_8(p)$ contain ovoids other than $\mathcal{O}_{r,p}(\mathbf{x})$ and (in case $p \equiv 0$ or $2 \mod 3$, $p \geq 11$) unitary ovoids?

(v) Can other lattices be used in place of the E_8 root lattice, giving large caps, if not ovoids?

(vi) Is there any way to extend this to $O_8^+(p^e)$ in place of $O_8^+(p)$? Although $O_8^+(9)$ has no $Sp_6(2)$-invariant ovoids (see [2]), one must wonder why the possibilities do not improve as the exponent e increases. At least the possibilities for ovoids in $O_6^+(p^e)$ improve greatly as e increases.

(vii) What is really going on in this construction? Is the occurrence of $E \oplus E$ in Section 2 just a computational convenience, or is there some overlying object in $E \oplus E$ which yields the r-ary ovoids as sections?

REFERENCES

1. C. Charnes, Ph. D. thesis, Cambridge University.
2. J. H. Conway, P. B. Kleidman and R. A. Wilson, 'New families of ovoids in O_8^+', *Geom. Ded.* **26** (1988), 157–170.
3. J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, Springer, New York, Berlin, 1988.
4. W. M. Kantor, 'Ovoids and translation planes', *Can. J. Math.* **34** (1982), 1195–1207.
5. P. B. Kleidman, 'The maximal subgroups of the finite 8-dimensional orthogonal groups $\mathrm{P}\Omega_8^+(q)$ and of their automorphism groups', *J. Alg.* **110** (1987), 173–242.
6. J.-P. Serre, *A Course in Arithmetic*, Springer, New York, Berlin, 1973, p. 110.

Author's address:

G. Eric Moorhouse,
Dept. of Mathematics,
University of Wyoming,
Laramie, WY 82071, U.S.A.