Root Lattice Constructions of Ovoids

G. Eric Moorhouse *

Abstract

Recently the author [5] has constructed new ovoids in $O_8^+(p)$ for p prime, using the E_8 root lattice, generalising a construction of Conway et al. [1]. Here we present a nine-dimensional lattice which greatly simplifies the description of these ovoids.

1. Introduction

An *orthogonal space* is a vector space V equipped with a quadratic form Q. We consider only finite-dimensional vector spaces over a finite field $F = GF(q)$. A *singular point* in such a space is a 1-dimensional subspace $\langle v\rangle$ such that $Q(v)=0$. Usually we take Q to be nondegenerate, in which case (V,Q) is called an $O_{2m-1}(q)$*-space* if $\dim V=2m-1$, or an $O_{2m}^{\pm}(q)$*-space* if $\dim V=2m$, using superscript $+$ or $-$ according as Q has Witt defect 0 or 1. An *ovoid* in an orthogonal space (V,Q) is a set $\mathcal{O}$ consisting of singular points, such that every maximal totally singular subspace of V contains a unique point of $\mathcal{O}$. In a space of type $O_{2m}^+(q)$, $O_{2m-1}(q)$ or $O_{2m-2}^-(q)$, an ovoid is equivalently defined (see [3], [7]) as a set of $q^{m-1}+1$ singular points of which no two are orthogonal. Ovoids are not known to exist in orthogonal spaces of 9 or more dimensions. Ovoids in $O_3(q)$ and in $O_4^-(q)$ necessarily consist of all singular points; viewed projectively, these are nondegenerate plane conics and elliptic quadrics in projective 3-space. We emphasise that the latter are discrete analogues of classical round objects in Euclidean space, and so the name 'ovoid' seems well-deserved. Ovoids in $O_6^+(q)$ (including ovoids in $O_5(q)$ as a special case under the natural embedding) are equivalent (see [4]) to translation planes of order q^2 with kernel containing $GF(q)$. These are known to exist in great abundance, and in general do not appear to originate from any Euclidean 'round' objects.

*Department of Mathematics, University of Wyoming, Laramie, WY 82071–3036, U.S.A.

The known ovoids in $O_8^+(q)$ are listed in [4], [1] and [5]. The majority of these occur in $O_8^+(p)$ for p prime, and are constructed by taking lattice points on a certain Euclidean sphere, then reducing modulo p, as we shall describe in Sections 2 and 3. It is intriguing that such discrete geometric objects would appear to owe their existence to properties of the Euclidean metric (seemingly requiring the Cauchy-Schwarz inequality in $\mathbb{R}^8$ or $\mathbb{R}^9$), and again justice is done to the term 'ovoid'.

2. An Eight-Dimensional Description

We first indicate, without proof, the ovoid construction from 8-dimensional lattices. This description remains the most useful for computer implementation.

Let E be the root lattice of type E_8; that is, E consists of all vectors $\frac{1}{2}(a_1, a_2, \ldots, a_8)$ with $a_i \in \mathbb{Z}$ such that $a_1 \equiv a_2 \equiv \cdots \equiv a_8 \bmod 2$ and $\sum a_i \equiv 0 \bmod 4$. A detailed description of E, including the following properties, may be found in [2]. Let p be any prime. Then $\overline{E} = E/pE$ is an 8-dimensional vector space over $F = GF(p)$, and for $v \in E$ we write $\overline{v} = v + pE \in \overline{E}$. We call $\|v\|^2$ the *norm* of $v \in E$, and since E is an even lattice, $\|v\|^2 \in 2\mathbb{Z}$. For any positive integer m, the number of vectors in E of norm $2m$ is $240\sigma_3(m) = 240\sum d^3$, summing over all positive integers d dividing m. In particular E has 240 vectors of norm 2, the *root vectors* of E. Define $Q : \overline{E} \to F$ by $Q(\overline{v}) = \frac{1}{2}\|v\|^2 \bmod p$. Then Q is a nondegenerate quadratic form on $\overline{E}$ with Witt defect 0, and Q is preserved by the Weyl group $W = W(E_8)$.

The *binary ovoids* of Conway et al. [1] are defined in $\overline{E}$ for p odd by

$$\mathcal{O}_{2,p}(x) = \mathcal{O}_{2,p}(\mathbb{Z}x + 2E) = \{\langle\overline{v}\rangle \;:\; \|v\|^2 = 2p,\; v \in \mathbb{Z}x + 2E\}$$

where $x \in E$ such that $\frac{1}{2}\|x\|^2$ is odd. The sphere of norm 2p (radius $\sqrt{2p}$, centre 0) has exactly $2(p^3+1)$ points of the lattice $\mathbb{Z}x + 2E$, and these occur in p^3+1 antipodal pairs. Reducing modulo p, we obtain p^3+1 points (one-dimensional subspaces) $\langle\overline{v}\rangle$, which are singular since $Q(\overline{v}) \equiv \frac{1}{2}(2p) \equiv 0 \bmod p$. Moreover [1] no two points of $\mathcal{O}_{2,p}(x)$ are orthogonal, so $\mathcal{O}_{2,p}(x)$ is an ovoid. Since there are just 120 choices of sublattice $\mathbb{Z}x + 2E \subset E$ with $\frac{1}{2}\|x\|^2$ odd, all equivalent under W, we obtain 120 binary ovoids in $O_8^+(p)$, all of which are equivalent. We may take $x \in E$ to be our favourite root vector, and then the stabiliser $W_x \cong W(E_7) \cong 2 \times Sp_6(2)$ acts on the ovoid $\mathcal{O}_{2,p}(x)$. (Remark: if $x \in E$ is a root vector, then $\mathbb{Z}x + 2E = \mathbb{Z}x \oplus 2E_7^*$ where E_7^* is the dual of $E_7 = E \cap x^\perp$ in $x^\perp$. Thus the binary ovoids are computable from a knowledge [2] of the 'shells' of E_7^*.)

More generally, for primes $r \neq p$ we define

$$\mathcal{O}_{r,p}(x) = \mathcal{O}_{r,p}(\mathbb{Z}x + rE) = \bigcup_{1 \le i \le \lfloor \frac{r}{2} \rfloor} \Big\{ \langle \overline{v} \rangle \ : \ \|v\|^2 = 2i(r-i)p, \ v \in \mathbb{Z}x + rE \Big\}$$

where $x \in E$ such that $-\frac{p}{2}\|x\|^2$ is a nonzero square modulo r. If $r > p$, it sometimes happens that $\mathcal{O}_{r,p}(x) = \{\langle 0 \rangle\}$, but in all other cases $\mathcal{O}_{r,p}(x)$ is an ovoid in $\overline{E}$, called an *r-ary ovoid* in $O_8^+(p)$. In Section 3 we will see an explanation for the 'failed ovoids' of the form $\{\langle 0 \rangle\}$. The cases $r \in \{2,3\}$ give the binary and ternary ovoids of Conway et al. [1]; for general r the above definition is a slight simplification of that given in [5]. By varying the choices of r and x, we expect from the computational evidence available that the number of isomorphism classes of r-ary ovoids in $O_8^+(p)$ is unbounded as $p \to \infty$, but this has not been proven.

The above definition of $\mathcal{O}_{r,p}(x)$ requires that we take lattice points on a *union* of $\lfloor \frac{r}{2} \rfloor$ spheres in $\mathbb{R}^8$. In Section 3 we shall interpret these spheres as hyperplane sections of a single sphere in $\mathbb{R}^9$, achieving a more concise definition of $\mathcal{O}_{r,p}(x)$ and a simplified proof that in fact we obtain ovoids.

3. A Nine-Dimensional Description

Throughout this section, r and p are distinct *odd* primes, which allows for a simpler presentation. The industrious reader will find that our presentation may be adapted to the general case; however the case $r = 2$ has already been treated by the description of the binary ovoids in Section 2, and the case $p = 2$ is trivial since $O_8^+(2)$ has a unique ovoid.

For each odd prime p, define a nine-dimensional Euclidean lattice by

$$\Lambda = \Lambda(p) = \sqrt{2}E \oplus \sqrt{p}\mathbb{Z}\,.$$

That is, Λ consists of vectors $\sqrt{2}e + \lambda z$ with $e \in E$ and $\lambda \in \mathbb{Z}$, where $z = (0,0,\ldots,0,\sqrt{p})$, and $\|\sqrt{2}e + \lambda z\|^2 = 2\|e\|^2 + p\lambda^2$. Note that Λ admits a group of isometries $G \cong 2 \times W$ generated by $W = W(E_8)$ acting naturally on the first eight coördinates and fixing z, together with the reflection in the hyperplane $z^\perp = \langle E \rangle$.

Now let r be an odd prime distinct from p. The quotients $\Lambda/p\Lambda$ and $\Lambda/r\Lambda$ are 9-dimensional vector spaces over $GF(p)$ and $GF(r)$, respectively. Each inherits from Λ a G-invariant quadratic form obtained by reducing $2\|e\|^2 + p\lambda^2 \in \mathbb{Z}$ modulo the corresponding prime. The quotient $\Lambda/r\Lambda$ is a (non-degenerate) $O_9(r)$-space.

However, the orthogonal space $\overline{\Lambda} = \Lambda/p\Lambda$ is degenerate, consisting of an $O_8^+(p)$-space over a 1-dimensional radical $\langle \overline{z} \rangle = \langle z + p\Lambda \rangle$; projectively, $\Lambda/p\Lambda$

is a 'hyperbolic cone over a point'. From the definition given in Section 1, we see that two types of ovoids are possible in $\overline{\Lambda} = \Lambda/p\Lambda$:

(i) The singleton $\{\langle\overline{z}\rangle\}$ is an ovoid in $\overline{\Lambda}$ since every maximal totally singular subspace of $\overline{\Lambda}$ is 5-dimensional and contains $\langle\overline{z}\rangle$. We call this the *degenerate ovoid* of $\overline{\Lambda}$.

(ii) Any set $\mathcal{O}$ consisting of p^3+1 mutually nonperpendicular singular points of $\overline{\Lambda}$ is an ovoid in $\overline{\Lambda}$. Such an ovoid does not contain $\langle\overline{z}\rangle$ and is called *nondegenerate.* For such an ovoid, $\{\langle\overline{v}\rangle+\langle\overline{z}\rangle \;:\; \langle\overline{v}\rangle \in \mathcal{O}\}$ is an ovoid in the $O_8^+(p)$-space $\overline{\Lambda}/\langle\overline{z}\rangle$, and conversely, ovoids in $O_8^+(p)$ lift to ovoids in $\overline{\Lambda}$.

Our construction in fact gives ovoids in $\overline{\Lambda} = \Lambda/p\Lambda$ of both types (although degenerate ovoids never occur for $r<p$), and thereby ovoids in $O_8^+(p)$ as described in (ii) above. Let π_r and π_p denote the natural maps from Λ to points of $\Lambda/r\Lambda$ and $\Lambda/p\Lambda$ respectively. That is, for $v \in \Lambda \smallsetminus r\Lambda$, we have $\pi_r(v) = \langle v + r\Lambda\rangle \leq \Lambda/r\Lambda$, and similarly for p in place of r. Consider the points of the lattice Λ which lie on the sphere of radius $r\sqrt{p}$, other than the 'poles' $\pm rz$, denoted thus:

$$\Lambda_{r^2p} = \{v \in \Lambda \;:\; \|v\|^2 = r^2p\} \smallsetminus \{\pm rz\}.$$

Our main result, as follows, will be proven later in this section.

Theorem 3.1 *(i) $\pi_r(\Lambda_{r^2p})$ is the set of singular points of $\Lambda/r\Lambda$ outside the hyperplane $H = \pi_r(E)$.*

(ii) Let $X = \langle x + r\Lambda\rangle$ be a singular point of $\Lambda/r\Lambda$ outside H, and let $\mathcal{X} = \{v \in \Lambda_{r^2p} \;:\; \pi_r(v) = X\}$. Then $\pi_p(\mathcal{X})$ is an ovoid of $\Lambda/p\Lambda$.

(iii) An ovoid of the form $\pi_p(\mathcal{X})$ as in (ii) is nondegenerate whenever $r<p$. If $r>p$ then $\pi_p(\mathcal{X})$ is nondegenerate for some $X, \mathcal{X}$.

The situation of Theorem 3.1 may be appreciated from Figure 1, where typical points of the quadric in $\Lambda/r\Lambda$ outside the hyperplane H, are denoted by $\bullet$, $*$ and $\diamond$. These points are lifted back to the sphere Λ_{r^2p} and then projected down to the degenerate quadric in $\Lambda/p\Lambda$, obtaining in each case an ovoid, although the ovoid obtained from $\diamond$ is degenerate. Observe that, as pictured, the lattice points in Λ_{r^2p} lie on certain hyperplanes of $\mathbb{R}^9$ parallel to $z^\perp$.

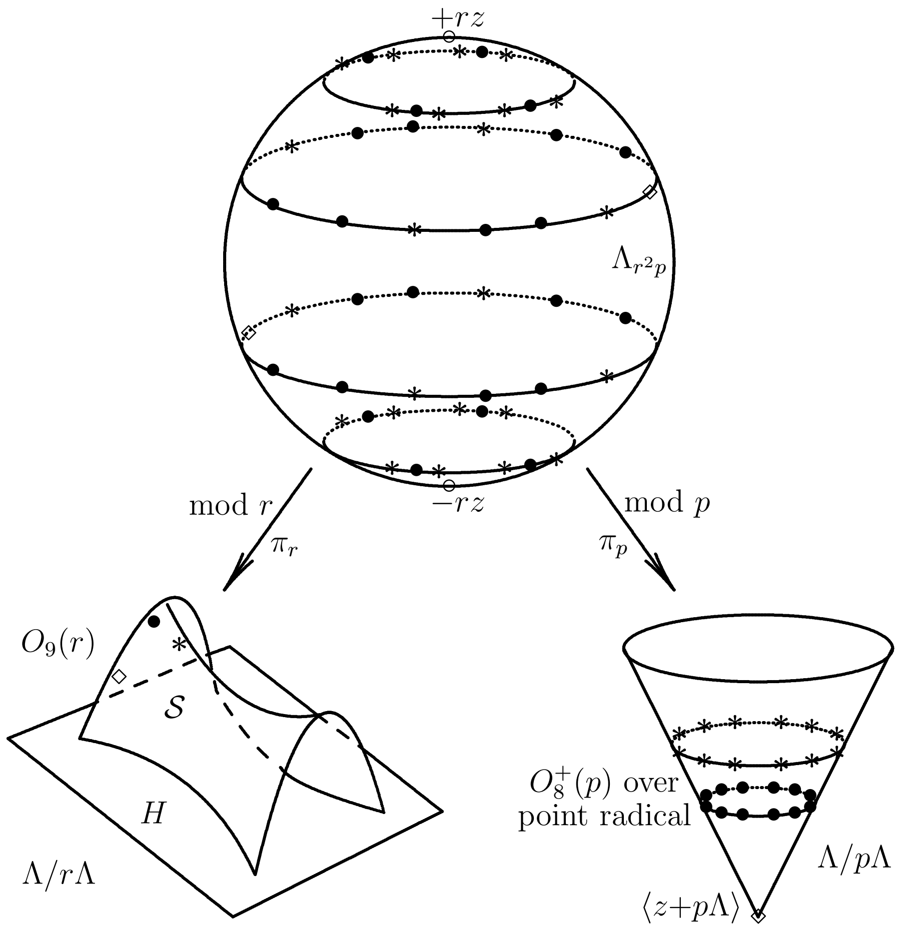

Figure 1. Two Projections of Λ_{r^2p}

We further illustrate the construction with an example in which $p=3$ and $r=5$. Now $\Lambda_{r^2p}=\{\sqrt{2}e\pm z : e\in E,\ \|e\|^2=36\}\cup\{\sqrt{2}e\pm 3z : e\in E,\ \|e\|^2=24\}$. For $X=\pi_5(\sqrt{2}(2^6,0^2)+3z)$ we obtain

$$\mathcal{X}=\Big\{\pm(\sqrt{2}(2^6;0^2)+3z),\ \pm(\sqrt{2}\cdot\tfrac{1}{2}(-7,3^5;-5,5)+z),\\ \pm(\sqrt{2}(4^2,-1^4;0^2)+z),\ \ldots\Big\}$$

where '...' denotes similar vectors obtained by arbitrarily permuting the first six coördinates of E, and permuting the last two coördinates of E. Then $|\mathcal{X}|=56$ and $\mathcal{X}$ projects to a nondegenerate ovoid of size 28 in $\Lambda/3\Lambda$, antipodal points of $\mathcal{X}$ giving the same ovoid point. Choosing $X'=\pi_5(\sqrt{2}(6,0^7)+z)$, however, we obtain $\mathcal{X}'=\{\pm(\sqrt{2}(6,0^7)+z)\}$, which projects to the degenerate ovoid of $\Lambda/3\Lambda$.

Observe that by definition if $u=\sqrt{2}e+\lambda z\in\Lambda_{r^2p}$ then $\|u\|^2=2\|e\|^2+p\lambda^2=r^2p$, which implies that $|\lambda|<r$ and λ is odd, so that $\pi_r(u)$ is a singular

point of $\Lambda/r\Lambda$ which does not lie in the hyperplane $H=\pi_r(E)$; this proves half of conclusion (i) of Theorem 3.1.

Lemma 3.2 *If $u\cdot v\equiv 0$ mod p for some $u,v\in\Lambda_{r^2p}$ such that $\pi_r(u)=\pi_r(v)$, then $u=\pm v$.*

Proof: The hypotheses imply that $u-\alpha v\in r\Lambda$ for some $\alpha\in\mathbb{Z}$ not divisible by r. Thus $2\alpha\, u{\cdot}v=\|u\|^2+\alpha^2\|v\|^2-\|u-\alpha v\|^2\equiv 0$ mod r^2, so $u{\cdot}v\equiv 0$ mod r^2. Also $u{\cdot}v\equiv 0$ mod p by hypothesis, so $u{\cdot}v\equiv 0$ mod r^2p. But $|u{\cdot}v|\le\|u\|\|v\|=r^2p$ by Cauchy-Schwarz, so $|u{\cdot}v|=0$ or r^2p. If $|u\cdot v|=r^2p$, then again by Cauchy-Schwarz, $u=\pm v$ and we are done. Otherwise $u\cdot v=0$. But it is easy to see that $u\cdot v$ must be odd. For we have $u=\sqrt{2}e+\lambda z,\ v=\sqrt{2}e'+\mu z$ for some $e,e'\in E$ and odd integers λ,μ satisfying $2\|e\|^2+p\lambda^2=2\|e'\|^2+p\mu^2=r^2p$; thus $u\cdot v=2e{\cdot}e'+p\lambda\mu\equiv 1$ mod 2, a contradiction. □

Define $\Lambda'_{r^2p}=\Lambda_{r^2p}\cap(p\Lambda+\mathbb{Z}z)$, the set of all vectors in Λ_{r^2p} which project to the radical of $\Lambda/p\Lambda$.

Lemma 3.3 $|\Lambda_{r^2p}|+p^3|\Lambda'_{r^2p}|=2r^3(r^4-1)(p^3+1)$.

Proof: This is proven in exactly the same way as Lemma 2.4 of [5], using the multiplicativity of σ_3, and the fact [6] that $E\oplus E$ has $480\sigma_7(m)$ vectors of norm $2m$ for every positive integer m. □

A *cap* in an orthogonal space is a set of singular points which are mutually nonperpendicular. Any cap in $O_8^+(p)$ has size at most p^3+1, and caps attaining this maximum size are ovoids (see [3], [7]). Consequently, caps in $\Lambda/p\Lambda$ have size at most p^3+1, and caps attaining this maximum size are nondegenerate ovoids; the radical point is a maximal cap of size 1.

Let $\mathcal{S}$ be the set of singular points of $\Lambda/r\Lambda$. Well-known counting arguments give $|\mathcal{S}|=(r^8-1)/(r-1)$ and $|\mathcal{S}\cap H|=(r^3+1)(r^4-1)/(r-1)$ since the hyperplane H is of type $O_8^+(r)$; thus $|\mathcal{S}\smallsetminus H|=|\mathcal{S}|-|\mathcal{S}\cap H|=r^3(r^4-1)$. By Lemma 3.2, for each point $X\in\mathcal{S}\smallsetminus H$, its preimage $\mathcal{X}=\{v\in\Lambda_{r^2p}:\pi_r(v)=X\}$ (which could conceivably be empty) projects to a cap $\pi_p(\mathcal{X})$ of $\Lambda/p\Lambda$. Also $|\pi_p(\mathcal{X})|=|\langle\overline{z}\rangle|=1$ if $\mathcal{X}\subseteq\Lambda'_{r^2p}$; otherwise $\mathcal{X}\subseteq\Lambda_{r^2p}\smallsetminus\Lambda'_{r^2p}$ and $0\le|\pi_p(\mathcal{X})|\le p^3+1$. Furthermore, Lemma 3.2 shows that the projection $\mathcal{X}\to\pi_p(\mathcal{X})$ is two-to-one. Therefore

$$\begin{aligned}|\Lambda_{r^2p}|-|\Lambda'_{r^2p}|=|\Lambda_{r^2p}\smallsetminus\Lambda'_{r^2p}|&=\sum_{\substack{X\in\mathcal{S}-H:\\ \mathcal{X}\subseteq\Lambda_{r^2p}-\Lambda'_{r^2p}}}|\mathcal{X}|\le\sum_{\substack{X\in\mathcal{S}-H:\\ \mathcal{X}\subseteq\Lambda_{r^2p}-\Lambda'_{r^2p}}}2(p^3+1)\\ &=2(p^3+1)|\mathcal{S}\smallsetminus H|-2(p^3+1)|\{X\in\mathcal{S}\smallsetminus H\,:\,\mathcal{X}\subseteq\Lambda'_{r^2p}\}|\\ &=2(p^3+1)r^3(r^4-1)-(p^3+1)|\Lambda'_{r^2p}|\,,\end{aligned}$$

in which equality holds by Lemma 3.3. Therefore $|\pi_p(\mathcal{X})| = p^3+1$ whenever $\mathcal{X} \subset \Lambda_{r^2p} \smallsetminus \Lambda'_{r^2p}$, thereby proving (i) and (ii) of Theorem 3.1. It is clear that $\Lambda'_{r^2p} = \emptyset$ whenever $r<p$, and that in any case $\Lambda_{r^2p} \supsetneq \Lambda'_{r^2p}$, whence not all ovoids $\pi_p(\mathcal{X})$ are degenerate, so (iii) follows as well, completing the proof of Theorem 3.1.

One checks without difficulty that for $x = \sqrt{2}e + \lambda z \in \Lambda_{r^2p}$, the ovoid of $\overline{\Lambda} = \Lambda/p\Lambda$ constructed from x as in Theorem 3.1, projects to the ovoid $\mathcal{O}_{r,p}(e)$ of $\overline{\Lambda}/\overline{z}$ described in Section 2, in the nondegenerate case ($e \notin pE$).

4. Further Remarks

Let X, $\mathcal{X}$, etc. be as in Theorem 3.1, and as before, let $G \cong 2 \times W$ be the isometry group of Λ, having natural orthogonal representations on both $\Lambda/r\Lambda$ and on $\Lambda/p\Lambda$. The stabiliser G_X acts on the ovoid $\pi_r(\mathcal{X})$, with kernel of order 2 or 4 in the nondegenerate case. In general, however, the stabilisers of these ovoids in the full orthogonal group, remain undetermined; cf. [5].

It is disappointing that the r-ary ovoid construction does not seem to work in $O_8^+(p^e)$ for $e>1$. This contrasts sharply with the situation in $O_6^+(p^e)$, where ovoid constructions generally proliferate as e increases. The problem with $O_8^+(p^e)$ is more than a lack of inspiration: although $O_8^+(p)$ has at least one $Sp_6(2)$-invariant ovoid for every odd prime p (say, $\mathcal{O}_{2,p}(\frac{1}{2}(1^8))$, and evidently many more as p increases), we have checked that no $Sp_6(2)$-invariant ovoids exist in $O_8^+(p^e)$ for $p^e \in \{2^2, 2^3, 2^4, 3^2, 3^3, 5^2\}$. (For $p^e=9$, this is proven in [1].)

Can variations of the above constructions give new ovoids from other lattices, or perhaps even nonexistence results for higher-dimensional ovoids? Certainly any ovoid may be lifted back from L/pL to a lattice L, with great freedom in the choice of lifting and of L itself. We cannot expect all such preimages to be as elegant as the spheres arising in our construction; nevertheless can it be shown that every ovoid lifts to some subset of a lattice with high density? And could the apparent lack of ovoids in $O_{10}^+(q)$ be due to a lack of a suitably dense lattice packing in $\mathbb{R}^{10}$? These are mere speculations.

References

[1] Conway J. H., Kleidman P. B. and Wilson R. A., *New families of ovoids in O_8^+. Geom. Ded.* **26** *(1988), 157–170.*

[2] Conway J. H. and Sloane N. J. A., *Sphere Packings, Lattices and Groups. Springer, New York and Berlin, 1988.*

[3] Hirschfeld J. W. P. and Thas J. A., *General Galois Geometries. Oxford Univ. Press, Oxford and New York, 1991.*

[4] Kantor W. M., *Ovoids and translation planes. Can. J. Math.* **34** *(1982), 1195–1207.*

[5] Moorhouse G. E., *Ovoids from the* E_8 *root lattice. Geom. Ded., to appear.*

[6] Serre J.-P., *A Course in Arithmetic. Springer, New York and Berlin, 1973, p. 110.*

[7] Thas J. A., *Ovoids and spreads of finite classical polar spaces. Geom. Ded.* **10** *(1981), 135–144.*