Classification Results for Hyperovals of Generalized Quadrangles

Bart De Bruyn(✉)

Ghent University, 9000 Gent, Belgium
Bart.DeBruyn@UGent.be

Abstract. A hyperoval of a point-line geometry is a nonempty set of points meeting each line in either 0 or 2 points. We discuss a combination of theoretical and practical techniques that are helpful for classifying hyperovals of generalized quadrangles. These techniques are based on the connection between hyperovals, even sets and pseudo-embeddings of point-line geometries.

Keywords: Generalized quadrangle · Hyperoval · Pseudo-embedding · Even set · Ideal

1 Introduction

A *(point-line) geometry* is a triple $\mathcal{S} = (\mathcal{P}, \mathcal{L}, \mathrm{I})$ consisting of a nonempty point set $\mathcal{P}$, a line set $\mathcal{L}$ and an incidence relation $\mathrm{I} \subseteq \mathcal{P} \times \mathcal{L}$ between these sets. One of the most important classes of geometries are the so-called *(axiomatic) projective planes* [17]. A finite projective plane π contains n^2+n+1 points and n^2+n+1 lines for some $n \in \mathbb{N}$, called the *order* of π. The standard examples are the Desarguesian projective planes $\mathrm{PG}(2,q)$ with q some prime power. Axiomatic projective planes have been intensively investigated, in particular several construction and classification results have been obtained about them. Some of these results have been obtained by means of computer computations, like the classifications of all projective planes of order 8, 9 and 10 [15,18,19].

Besides classification results and constructions, also special sets of points in projective planes have been investigated. Certain of these sets have relationships with other mathematical areas, like coding theory, or certain geometries can be constructed from them, like partial geometries and generalized quadrangles. One of the substructures of finite projective planes that have been thoroughly investigated are the *hyperovals*. These are nonempty sets of points meeting each line in either 0 or 2 points, in which case it can be shown that the hyperoval has size $n+2$ with n the (necessarily even) order of the plane. The classical examples of hyperovals here are those in $\mathrm{PG}(2,q)$, q even, by adding to an irreducible conic $\mathcal{C}$ its *nucleus*, that is the point that lies in all tangent lines of $\mathcal{C}$. The construction and classification problem of hyperovals in arbitrarily not necessarily Desarguesian projective planes has been intensively studied. Hyperovals

A. M. Bigatti et al. (Eds.): ICMS 2020, LNCS 12097, pp. 153–161, 2020.
https://doi.org/10.1007/978-3-030-52200-1_15

also play a crucial role in the nonexistence proof for the projective plane of order 10 [19]. Indeed this proof essentially relies on the fact that a plane of order 10 cannot have hyperovals [20].

The concept of a hyperoval, namely a nonempty set of points meeting each line in either 0 or 2 points, can be defined for general point-line geometries. Two families of point-line geometries that have attracted attention here are the *generalized quadrangles (GQ's)* [25] and the *polar spaces* [2]. The standard examples of polar spaces are related to symplectic polarities, quadrics and Hermitian varieties in projective spaces [16], but also every generalized quadrangle is an example of a polar space. A *generalized quadrangle of order* (s,t), or shortly a $\mathrm{GQ}(s,t)$, is defined as a geometry that satisfies the following three properties:

1. Every two distinct points are incident with at most one line.
2. Every line is incident with exactly $s+1$ points and every point is incident with precisely $t+1$ lines.
3. For every non-incident point-line pair (x,L), there exists a unique point y on L collinear with x (i.e. y is in some line together with x).

Hyperovals of polar spaces, in particular of GQ's, are not only interesting point sets. They are also related to other combinatorial structures in finite geometry. Hyperovals (or *local subspaces*) of polar spaces were first considered in [1] because of their connection with so-called *locally polar spaces*. Hyperovals of GQ's have a number of additional applications. They naturally arise in the study of *extended generalized quadrangles* and play a fundamental role in their study, see [3,21–23]. Lower and upper bounds for the size of a hyperoval H in a $\mathrm{GQ}(s,t)$ were obtained in [3, Lemmas 3.9 and 3.11] and [14, Theorems 2.1 and 2.2]. The size $|H|$ is even and satisfies $\max(2(t+1),(t-s+2)(s+1)) \leq |H| \leq 2(st+1)$.

In recent years, many construction and classification results for hyperovals in GQ's have been obtained. These regard theoretical constructions of infinite families [4–9,14,24], or computer backtrack searches as in [22,23]. We will emphasise here on a number of techniques that can help in studying and classifying hyperovals, both from a theoretical as a computational point of view. Hyperovals are special cases of *even sets*, these are sets of points that meet each line in an even number of points. The intention is to discuss some tools for classifying hyperovals inside the family of all even sets. The complements of the even sets were coined *pseudo-hyperplanes* in [11]. There exist close relationships between pseudo-hyperplanes and certain representations of the geometry in projective spaces, called *pseudo-embeddings*. Some of these relationships will be mentioned in Sect. 2. Via the connection with pseudo-embeddings, we show in Sect. 3 that the family of hyperovals is related to certain ideals in polynomial rings and that Gröbner bases can sometimes help in their study and/or classification.

2 Pseudo-embeddings, Pseudo-hyperplanes and Even Sets

Suppose $\mathcal{S} = (\mathcal{P}, \mathcal{L}, \mathrm{I})$ is a geometry for which the number of points on each line is finite and at least 3. A *pseudo-embedding* of $\mathcal{S}$ is a map ϵ from $\mathcal{P}$ to the point set of a projective space $\mathrm{PG}(V)$ defined over the field $\mathbb{F}_2$ of order 2 such that:

- the image of ϵ generates the whole projective space $\mathrm{PG}(V)$;
- ϵ maps every line $L \in \mathcal{L}$ to a *frame* of a subspace of $\mathrm{PG}(V)$, i.e. $\epsilon(L)$ is a set of the form $\{\langle \bar{v}_1 \rangle, \langle \bar{v}_2 \rangle, \ldots, \langle \bar{v}_k \rangle\}$, where k is the size of L, $\bar{v}_1, \bar{v}_2, \ldots, \bar{v}_{k-1}$ are $k-1$ linearly independent vectors of V and $\bar{v}_k = \bar{v}_1 + \bar{v}_2 + \ldots + \bar{v}_{k-1}$.

We denote such a pseudo-embedding also by $\epsilon : \mathcal{S} \to \mathrm{PG}(V)$. A pseudo-embedding thus maps the lines of a geometry $\mathcal{S}$ to frames of subspaces of a projective space $\mathrm{PG}(V)$. This is different from the notion of an (ordinary) embedding of $\mathcal{S}$ which maps the lines of $\mathcal{S}$ to lines of $\mathrm{PG}(V)$.

Two pseudo-embeddings $\epsilon_1 : \mathcal{S} \to \mathrm{PG}(V_1)$ and $\epsilon_2 : \mathcal{S} \to \mathrm{PG}(V_2)$ of the same point-line geometry $\mathcal{S}$ are called *isomorphic* if there exist a linear isomorphism θ between the vector spaces V_1 and V_2 such that $\epsilon_2 = \theta \circ \epsilon_1$.

If $\epsilon : \mathcal{S} \to \mathrm{PG}(V)$ is a pseudo-embedding, then projecting the image of ϵ from a (suitable) subspace on a complementary subspace can give rise to another pseudo-embedding ϵ', which is called a *projection* of ϵ. If ϵ_1 and ϵ_2 are two pseudo-embeddings of the same point-line geometry $\mathcal{S}$, then we write $\epsilon_1 \geq \epsilon_2$ if ϵ_2 is isomorphic to a projection of ϵ_1. If $\widetilde{\epsilon}$ is a pseudo-embedding of $\mathcal{S}$ such that $\widetilde{\epsilon} \geq \epsilon$ for any other pseudo-embedding ϵ of $\mathcal{S}$, then $\widetilde{\epsilon}$ is called *universal*. If $\mathcal{S}$ has pseudo-embeddings, then it also has a universal pseudo-embedding which is moreover unique, up to isomorphism. The vector dimension of the universal pseudo-embedding is called the *pseudo-embedding rank*, and (in case $|\mathcal{P}| < \infty$) is equal to $|\mathcal{P}| - \dim(C)$, where C is the binary code of length $|\mathcal{P}|$ generated by the characteristic vectors of the lines of $\mathcal{S}$. Note that $\dim(C)$ equals the $\mathbb{F}_2$-rank of an incidence matrix of $\mathcal{S}$. We thus see that there exist connections between pseudo-embeddings and coding theory. There also exist connections between pseudo-embeddings and modular representation theory of groups.

Pseudo-hyperplanes and hence also even sets are closely related to pseudo-embeddings as the following theorem shows.

Theorem 1 ([11]). *If $\epsilon : \mathcal{S} \to \mathrm{PG}(V)$ is a pseudo-embedding, then for every hyperplane Π of $\mathrm{PG}(V)$, the set $\epsilon^{-1}(\epsilon(\mathcal{P}) \cap \Pi)$ is a pseudo-hyperplane of $\mathcal{S}$. Every pseudo-hyperplane of $\mathcal{S}$ arises in this way from the universal pseudo-embedding of $\mathcal{S}$.*

More background information about pseudo-embeddings, pseudo-hyperplanes and the above facts can be found in [10–13]. In [11] it was also shown that all GQ's have pseudo-embeddings and hence also universal pseudo-embeddings.

Hyperovals of GQ's can often be computationally classified without implementing a backtrack algorithm. One way to achieve this goal is to determine all (isomorphism classes of) even sets, and subsequently to verify which even sets

are also hyperplanes. The number of even sets can be determined in advance: it equals 2^k, with k the pseudo-embedding rank. As soon as a computer model of the geometry has been implemented along with its automorphism group (e.g. with GAP [27]), it is easy to generate even sets, the size of the orbit to which a given even set belongs can readily be computed, and it can easily be verified whether two hyperovals are isomorphic. Based on these three principles, it is often easy to compute all isomorphism classes of even sets. This has been illustrated in the papers [12,13]. We mention two reasons why it is so easy to generate even sets with a computer:

1. An even set can be found as a set whose characteristic vector is $\mathbb{F}_2$-orthogonal with all characteristic vectors of the lines.
2. The symmetric difference of any two even sets is again an even set.

The above method (as well as a backtrack search) has the disadvantage that it does not provide unified and explicit descriptions for the hyperovals. The method which we will discuss in the following section does have this potential. It is still based on the connection with even sets but it also takes into account a description of the universal pseudo-embedding.

3 Related Ideals in Polynomial Rings

The material discussed in this section is new with exception of Theorem 4, which is taken from [13, Corollary 1.3]. We continue with the notation in Sect. 2. We suppose that $\mathcal{S}$ has pseudo-embeddings and we denote by $\widetilde{\epsilon} : \mathcal{S} \to \mathrm{PG}(\widetilde{V})$ the universal pseudo-embedding of $\mathcal{S}$. If $k := \dim(\widetilde{V})$, then there exist k maps $f_i : \mathcal{P} \to \mathbb{F}_2$ ($i \in \{1, 2, \ldots, k\}$) such that $\widetilde{\epsilon}$ maps a point p of $\mathcal{S}$ to the point $(f_1(p), f_2(p), \ldots, f_k(p))$ of $\mathrm{PG}(\widetilde{V})$. Using these f_i's, Theorem 1 can now be rephrased as follows.

Theorem 2. *The even sets of $\mathcal{S}$ are precisely the subsets of $\mathcal{P}$ satisfying an equation of the form $\sum_{i=1}^{k} a_i f_i(p) = 1$ with $a_1, a_2, \ldots, a_k \in \mathbb{F}_2$.*

We denote by $E(\bar{a})$ the even set corresponding to a tuple $\bar{a} = (a_1, a_2, \ldots, a_k)$. Suppose $\alpha = \{p_1, p_2, \ldots, p_l\}$ is a line of $\mathcal{S}$. The condition that the point p_i of α belongs to $E(\bar{a})$ implies by Theorem 2 that a certain linear combination $L_i(\bar{a})$ of the a_i's is equal to 1. If $E(\bar{a})$ is a hyperoval of $\mathcal{S}$, then the number of i's for which $L_i(\bar{a})$ is equal to 1 is therefore either 0 to 2.

Theorem 3. *There exists a $g_\alpha(a_1, a_2, \ldots, a_k) \in \mathbb{F}_2[a_1, a_2, \ldots, a_k]$ such that the following two conditions are equivalent for any $\bar{a} = (a_1, a_2, \ldots, a_k) \in \mathbb{F}_2^k$:*

- *the number of i's for which $L_i(\bar{a})$ is equal to 1 is either 0 to 2;*
- *$g_\alpha(a_1, a_2, \ldots, a_k) = 0$.*

Proof. We define $h(a_1, a_2, \ldots, a_k) := (L_1(\bar{a}) + 1)(L_2(\bar{a}) + 1) \cdots (L_l(\bar{a}) + 1) + 1$ and $h_{uv}(a_1, a_2, \ldots, a_k) := 1 + L_u(\bar{a}) \cdot L_v(\bar{a}) \cdot \prod_{w \notin \{u,v\}} (L_w(\bar{a}) + 1)$ for all $u, v \in \{1, 2, \ldots, l\}$ with $u < v$. Then the following hold:

- $h(a_1, a_2, \ldots, a_k) = 0$ if and only if there are no i's for which $L_i(\bar{a}) = 1$;
- $h_{uv}(a_1, a_2, \ldots, a_k) = 0$ if and only if u, v are the only i's for which $L_i(\bar{a}) = 1$.

We can then put $g_\alpha(a_1, a_2, \ldots, a_k)$ equal to the product of h and all h_{uv}'s with $1 \leq u < v \leq l$.

There exists such a polynomial $g_\alpha(a_1, a_2, \ldots, a_k) \in \mathbb{F}_2[a_1, a_2, \ldots, a_k]$ for each line α of $\mathcal{S}$. Such a polynomial is not unique. If I is the ideal generated by the polynomials $a_i^2 + a_i$, $i \in \{1, 2, \ldots, k\}$, then any polynomial in $g_\alpha(a_1, a_2, \ldots, a_k) + I$ also satisfies the required property. By the above discussion, we know:

Corollary 1. *The even set $E(\bar{a})$ with $\bar{a} \in \mathbb{F}_2^k \setminus \{\bar{o}\}$ is a hyperoval if and only if $g_\alpha(a_1, a_2, \ldots, a_k) = 0$ for all $\alpha \in \mathcal{L}$.*

If we know all g_α's, we can directly determine all $\bar{a} \in \mathbb{F}_2^k$ for which $E(\bar{a})$ is a hyperoval. From a computational point of view, this can go faster (see example later) than verifying which of the sets $E(\bar{a})$ with $\bar{a} \in \mathbb{F}_2^k$ intersects each line of the geometry in either 0 or 2 points. In the latter approach we first need to determine the set $E(\bar{a})$ by solving the equation mentioned in Theorem 2 (with respect to p) before verifying that $E(\bar{a})$ intersects each of the lines in 0 or 2 points. The method of working with the polynomials g_α has two additional benefits.

1. If ϕ is an automorphism of $\mathcal{S}$, then the fact that $\widetilde{\epsilon}$ is so-called homogeneous (see e.g. [12]) implies that there exists a linear automorphism ϕ' of $\mathbb{F}_2^k$ such that ϕ maps the even set $E(\bar{a})$ to the even set $E(\bar{a}^{\phi'})$. If α and β are lines of $\mathcal{S}$ such that $\alpha = \beta^\phi$, then we have $g_\beta(\bar{a}) = g_\alpha(\bar{a}^{\phi'})$. Information about automorphisms of $\mathcal{S}$ and their corresponding actions on $\mathbb{F}_2^k$ thus implies that certain of the g_α's can be derived from others. In particular, if we have such information for a set of automorphisms that generate a line-transitive automorphism group, then one of the g_α's determines all the others.
2. If we take the ideal $\mathcal{G}$ generated by I and all g_α's, then any polynomial in $\mathcal{G}$ determines a necessary condition for a set $E(\bar{a})$ to be a hyperoval. In particular, we can look for polynomials that have a simple form. Such polynomials can often be found with the aid of Gröbner bases (implemented in computer algebra systems), and can be useful for theoretical and computational purposes.

Both benefits are illustrated by the following example. Consider in the projective space PG(3, 4) the Hermitian variety $\mathcal{H}$ with equation $X_1X_2^2 + X_2X_1^2 + X_3X_4^2 + X_4X_3^2 = 0$. The points and lines contained in $\mathcal{H}$ then define a generalized quadrangle $H(3, 4)$ of order $(4, 2)$ [25]. The universal pseudo-embedding of $H(3, 4)$ was described in [13, Section 1] and has vector dimension 24. From this description, we easily deduce the following (see also [13, Corollary 1.3]).

Theorem 4. *The even sets of $H(3,4)$ are precisely the subsets of $\mathcal{H}$ satisfying an equation of the form*

$$\sum_1(a_iX_i^3) + a_5(\omega X_3X_4^2 + \omega^2 X_4X_3^2) + a_6\Big((X_1^3 + X_2^3 + X_1^3X_2^3)(X_3^3 + X_4^3 + X_3^3X_4^3) + 1\Big) + \sum_2(b'_{ij}X_iX_j^2 + (b'_{ij})^2X_jX_i^2) + \sum_3\Big(b'_{ijk}X_iX_jX_k + (b'_{ijk})^2X_i^2X_j^2X_k^2\Big) = 1,$$

with the a_i's belonging to $\mathbb{F}_2$ and the b'_{ij}'s and b'_{ijk}'s belonging to $\mathbb{F}_4$.

In Theorem 4, $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$ is the finite field of order 4, Σ_1 denotes the summation over all $i \in \{1,2,3,4\}$, Σ_2 denotes the summation over all $i, j \in \{1,2,3,4\}$ with $i < j$ and $(i,j) \neq (3,4)$, and Σ_3 denotes the summation over all $i, j, k \in \{1,2,3,4\}$ with $i < j < k$. We can now put $b'_{ij} = b_{ij} + \omega c_{ij}$ and $b'_{ijk} = b_{ijk} + \omega c_{ijk}$, where all b_{ij}'s, c_{ij}'s, b_{ijk}'s and c_{ijk}'s belong to $\mathbb{F}_2$. Using the terminology of Theorem 2, the maps $f_i(p)$ with $i \in \{1, 2, \ldots, 24\}$ and $p = (X_1, X_2, X_3, X_4)$ can then be taken as follows:

$$f_1(p) = X_1^3, f_2(p) = X_2^3, f_3(p) = X_3^3, f_4(p) = X_4^3, f_5(p) = \omega X_3X_4^2 + \omega^2 X_3^2X_4,$$

$$f_6(p) = (X_1^3 + X_2^3 + X_1^3X_2^3)(X_3^3 + X_4^3 + X_3^3X_4^3) + 1, f_7(p) = X_1X_2^2 + X_2X_1^2,$$

$$f_8(p) = \omega X_1X_2^2 + \omega^2 X_2X_1^2, \ \ldots\ , f_{24}(p) = \omega X_2X_3X_4 + \omega^2 X_2^2X_3^2X_4^2.$$

We now determine one of the g_α's.

Theorem 5. *If α is the line of $H(3,4)$ with equation $X_2 = X_4 = 0$, then g_α is equal to $a_1 + a_3 + (b_{13} + c_{13} + b_{13}c_{13})(a_1 + a_3 + a_6 + a_1a_3 + a_1a_6 + a_3a_6)$.*

Proof. The even set determined by the tuple $(a_1, a_2, \ldots, c_{234}) \in \mathbb{F}_2^{24}$ intersects α in either 0 or 2 points if the equation $a_1X_1^3 + a_3X_3^3 + a_6(X_1^3X_3^3 + 1) + b'_{13}X_1X_3^2 + (b'_{13})^2X_3X_1^2 = 0$ has 0 or 2 solutions for $(X_1, X_3) \in \{(0,1), (1,x) \mid x \in \mathbb{F}_4\}$. This means that precisely two of the equations $a_3 + a_6 = 1$, $a_1 + a_6 = 1$, $a_1 + a_3 + b'_{13} + (b'_{13})^2 = 1$, $a_1 + a_3 + b'_{13}\omega^2 + (b'_{13})^2\omega = 1$, $a_1 + a_3 + b'_{13}\omega + (b'_{13})^2\omega^2 = 1$ are satisfied. We denote these equations respectively by (1), (2), (3), (4) and (5).

Suppose $b'_{13} = 0$. If $a_1 + a_3 = 1$, then (3), (4) and (5) imply that at least three of the equations are satisfied which is impossible. So, $a_1 + a_3 = 0$, but then (3), (4) and (5) are never satisfied. As $a_1 + a_3 = 0$, either (1), (2) are satisfied or none of them is satisfied. So, if $b'_{13} = 0$, then necessarily $a_1 + a_3 = 0$.

Suppose $b'_{13} \neq 0$ and $a_1 + a_3 = 1$. Then precisely one of (1), (2) is satisfied. As precisely one of b'_{13}, $b'_{13}\omega^2$, $b'_{13}\omega$ belongs to $\mathbb{F}_2$, we also see that precisely one of (3), (4), (5) is satisfied. So, this case is always OK.

Suppose $b'_{13} \neq 0$ and $a_1 + a_3 = 0$. As precisely one of b'_{13}, $b'_{13}\omega^2$, $b'_{13}\omega$ belongs to $\mathbb{F}_2$, precisely two of the equations (3), (4), (5) are satisfied. So, none of (1), (2) can be satisfied. This implies that $a_3 + a_6 = 0$.

The overall condition is thus $((b'_{13})^3 + 1)(a_1 + a_3) + (b'_{13})^3((a_1 + a_3 + 1)(a_3 + a_6)) = 0$ which simplifies to $a_1 + a_3 + (b'_{13})^3(a_1 + a_3 + a_6 + a_1a_3 + a_1a_6 + a_3a_6) = a_1 + a_3 + (b_{13} + c_{13} + b_{13}c_{13})(a_1 + a_3 + a_6 + a_1a_3 + a_1a_6 + a_3a_6)$.

In Section 5 of [13], we described a list of 6 generators $\phi_1, \phi_2, \ldots, \phi_6$ for the (line-transitive) automorphism group of $H(3,4)$, along with their corresponding actions on the even sets $E(\bar{a})$, see [13, Tables 1 and 2]. From this information, the corresponding actions of $\phi_1', \phi_2', \ldots, \phi_6'$ on $\mathbb{F}_2^{24}$ (see above) can easily be derived:

- $\bar{a}^{\phi_1'} = (a_3,\ a_4,\ a_1,\ a_2,\ c_{12},\ a_6,\ b_{12},\ a_5,\ b_{13}{+}c_{13},\ c_{13},\ b_{23}{+}c_{23},\ c_{23},\ b_{14}{+}c_{14},\ c_{14},\ b_{24}{+}c_{24},\ c_{24},\ b_{134},\ c_{134},\ b_{234},\ c_{234},\ b_{123},\ c_{123},\ b_{124},\ c_{124})$;
- $\bar{a}^{\phi_2'} = (a_1,\ a_2,\ a_3,\ a_4,\ a_5,\ a_6,\ b_{12},\ c_{12},\ c_{13},\ b_{13}{+}c_{13},\ c_{14},\ b_{14}{+}c_{14},\ c_{23},\ b_{23}{+}c_{23},\ c_{24},\ b_{24}{+}c_{24},\ b_{123}{+}c_{123},\ b_{123},\ b_{124}{+}c_{124},\ b_{124},\ c_{134},\ b_{134}{+}c_{134},\ c_{234},\ b_{234}{+}c_{234})$;
- $\bar{a}^{\phi_3'} = (a_1{+}a_3{+}a_6{+}c_{13},\ a_2,\ a_3,\ a_4{+}a_2{+}a_6{+}c_{24},\ a_5{+}c_{23}{+}c_{234},\ a_6,\ b_{12}{+}b_{123}{+}c_{123}{+}b_{234},\ c_{12}{+}c_{123}{+}c_{23},\ b_{13}{+}a_3{+}a_6,\ c_{13},\ b_{14}{+}b_{12}{+}b_{23}{+}c_{23}{+}b_{123}{+}c_{123}{+}b_{124}{+}b_{134}{+}c_{134}{+}b_{234},\ c_{14}{+}a_5{+}c_{12}{+}c_{23}{+}c_{123}{+}c_{124}{+}c_{134}{+}c_{234},\ b_{23},\ c_{23},\ b_{24}{+}a_2{+}a_6,\ c_{24},\ b_{123},\ c_{123},\ b_{124}{+}a_6{+}b_{234},\ c_{124}{+}c_{234},\ b_{134}{+}a_6{+}b_{123},\ c_{134}{+}c_{123},\ b_{234},\ c_{234})$;
- $\bar{a}^{\phi_4'} = (a_1,\ a_2,\ a_3,\ a_4{+}a_3{+}a_5,\ a_5,\ a_6,\ b_{12}{+}a_3,\ c_{12},\ b_{13},\ c_{13},\ b_{14}{+}b_{13}{+}b_{134},\ c_{14}{+}c_{13}{+}c_{134},\ b_{23},\ c_{23},\ b_{24}{+}b_{23}{+}b_{234},\ c_{24}{+}c_{23}{+}c_{234},\ b_{123},\ c_{123},\ b_{124}{+}b_{123},\ c_{124}{+}c_{123},\ b_{134},\ c_{134},\ b_{234},\ c_{234})$;
- $\bar{a}^{\phi_5'} = (a_1,\ a_2,\ a_3{+}a_4{+}a_5,\ a_4,\ a_5,\ a_6,\ b_{12}{+}a_4,\ c_{12},\ b_{13}{+}b_{14}{+}b_{134},\ c_{13}{+}c_{14}{+}c_{134},\ b_{14},\ c_{14},\ b_{23}{+}b_{24}{+}b_{234},\ c_{23}{+}c_{24}{+}c_{234},\ b_{24},\ c_{24},\ b_{123}{+}b_{124},\ c_{123}{+}c_{124},\ b_{124},\ c_{124},\ b_{134},\ c_{134},\ b_{234},\ c_{234})$;
- $\bar{a}^{\phi_6'} = (a_1,\ a_2,\ a_3,\ a_4,\ a_5,\ a_6,\ b_{12}{+}c_{12}{+}a_5,\ c_{12},\ b_{13}{+}c_{13},\ c_{13},\ b_{14}{+}c_{14},\ c_{14},\ b_{23}{+}c_{23},\ c_{23},\ b_{24}{+}c_{24},\ c_{24},\ b_{123}{+}c_{123},\ c_{123},\ b_{124}{+}c_{124},\ c_{124},\ b_{134}{+}c_{134},\ c_{134},\ b_{234}{+}c_{234},\ c_{234})$.

Based on this information, we have computed with the aid of SageMath [26] all g_α's. The ideal $\mathcal{G}$ generated by I and the g_α's contains polynomials that have fewer terms than the g_α's themselves. These have been found by computing Gröbner bases of ideals generated by some of these g_α's. Specifically, $\mathcal{G}$ contains the eight polynomials that are obtained from $a_1a_3b_{13} + a_1a_6b_{13} + a_3a_6b_{13} + a_6b_{13}$ and $a_1a_3c_{13} + a_1a_6c_{13} + a_3a_6c_{13} + a_6c_{13}$ by applying one of the permutations (), (12), (34), (12)(34) on the subindices. $\mathcal{G}$ also contains the eight polynomials that are obtained from $a_1b_{13}c_{13} + a_6b_{13}c_{13} + a_1a_3 + a_1a_6 + a_3a_6 + a_1b_{13} + a_6b_{13} + a_1c_{13} + a_6c_{13} + a_1$ by applying one of the permutations (), (12), (13), (34), (132), (143), (12)(34), (14)(23) on the subindices.

4 Summary

We have discussed here three methods by which hyperovals can be computed:

(1) via the connection with even sets discussed at the end of Sect. 2;
(2) by finding all $\bar{a} \in \mathbb{F}_2^k$ for which $E(\bar{a})$ is a hyperoval (via Theorem 2);
(3) by finding all $\bar{a} \in \mathbb{F}_2^k$ for which $g_\alpha(\bar{a}) = 0$ holds for all lines $\alpha \in \mathcal{L}$.

For the example of hyperovals of $H(3,4)$, our implementation of the methods (1) and (2) had similar performances ($\pm$ 1h40min, iMac, 2.7 GHz Intel Core i5-4570R processor). Methods (1) and (2) were already used in [13] to show that

$H(3,4)$ has 23 nonisomorphic hyperovals. The third method was almost three times faster. Note also that the three polynomials of $\mathcal{G}$ mentioned at the end of Sect. 3 give the conditions $(a_1+a_6)(a_3+a_6)b_{13} = (a_1+a_6)(a_3+a_6)c_{13} = (a_1+a_6)(b_{13}c_{13}+b_{13}+c_{13}+a_1+a_3) = 0$, and that the remaining polynomials give similar equations. This means that certain of the entries of $\bar{a}$ are 0 or can be expressed in terms of the others, a fact that would allow to speed up further the computations for the third method. Some of the code (in SageMath [26] and GAP [27]) used in our computations can be found on https://cage.ugent.be/geometry/preprints.php.

Our main intention here was to discuss theoretical and computational techniques that are useful for classifying hyperovals of generalized quadrangles. These techniques suffice so far for classifying all hyperovals of all finite generalized quadrangles of order (s,t) with $s \leq 4$. These GQ's comprise the 3×3, 4×4 and 5×5-grids as well as the GQ's $W(2)$, $Q(5,2)$, $W(3)$, $Q(4,3)$, GQ$(3,5)$, $Q(5,3)$, $H(3,4)$, $W(4)$, GQ$(4,6)$, $H(4,4)$ and GQ$(5,4)$ (see [25] for definitions). With exception of the GQ's $W(4)$, GQ$(4,6)$, $H(4,4)$ and $Q(5,4)$, these classifications have already appeared in the literature (below).

Our work on classifying hyperovals of generalized quadrangles is work in progress where on the one hand we try to obtain additional classification results (for larger GQ's) and on the other hand we try to obtain computer free uniform descriptions for all the hyperovals of a given GQ. As in [13], the latter problem can involve that algebraic descriptions of the universal pseudo-embeddings need to be found.

References

1. Buekenhout, F., Hubaut, X.: Locally polar spaces and related rank 3 groups. J. Algebra **45**, 391–434 (1977)
2. Buekenhout, F., Shult, E.: On the foundations of polar geometry. Geometriae Dedicata **3**, 155–170 (1974)
3. Cameron, P.J., Hughes, D.R., Pasini, A.: Extended generalized quadrangles. Geom. Dedicata **35**, 193–228 (1990)
4. Cossidente, A.: Hyperovals on $H(3,q^2)$. J. Combin. Theor. Ser. A **118**, 1190–1195 (2011)
5. Cossidente, A., King, O.H., Marino, G.: Hyperovals of $H(3,q^2)$ when q is even. J. Combin. Theor Ser. A **120**, 1131–1140 (2013)
6. Cossidente, A., King, O.H., Marino, G.: Hyperovals arising from a Singer group action on $H(3,q^2)$, q even. Adv. Geom. **16**, 481–486 (2016)
7. Cossidente, A., Marino, G.: Hyperovals of Hermitian polar spaces. Des. Codes Crypt. **64**, 309–314 (2012)
8. Cossidente, A., Pavese, F.: Hyperoval constructions on the Hermitian surface. Finite Fields Appl. **25**, 19–25 (2014)
9. Cossidente, A., Pavese, F.: New infinite families of hyperovals on $H(3,q^2)$, q odd. Des. Codes Crypt. **73**, 217–222 (2014)
10. De Bruyn, B.: The pseudo-hyperplanes and homogeneous pseudo-embeddings of AG$(n,4)$ and PG$(n,4)$. Des. Codes Crypt. **65**, 127–156 (2012)

11. De Bruyn, B.: Pseudo-embeddings and pseudo-hyperplanes. Adv. Geom. **13**, 71–95 (2013)
12. De Bruyn, B.: The pseudo-hyperplanes and homogeneous pseudo-embeddings of the generalized quadrangles of order $(3, t)$. Des. Codes Crypt. **68**, 259–284 (2013)
13. De Bruyn, B., Gao, M.: The homogeneous pseudo-embeddings and hyperovals of the generalized quadrangle $H(3, 4)$. Linear Algebra Appl. **593**, 90–115 (2020)
14. Del Fra, A., Ghinelli, D., Payne, S.E.: $(0, n)$-sets in a generalized quadrangle. In: Annals of Discrete Mathematics, vol. 52, pp. 139–157, Gaeta (1990), North-Holland (1992)
15. Hall Jr., M., Swift, J.D., Walker, R.J.: Uniqueness of the projective plane of order eight. Math. Tables Aids Comput. **10**, 186–194 (1956)
16. Hirschfeld, J.W.P., Thas, J.A.: General Galois Geometries. Springer Monographs in Mathematics. Springer, London (2016). https://doi.org/10.1007/978-1-4471-6790-7
17. Hughes, D.R., Piper, F.C.: Projective planes. In: Graduate Texts in Mathematics, vol. 6. Springer, New York (1973)
18. Lam, C.W.H., Kolesova, G., Thiel, L.: A computer search for finite projective planes of order 9. Discrete Math. **92**, 187–195 (1991)
19. Lam, C.W.H., Thiel, L., Swiercz, S.: The nonexistence of finite projective planes of order 10. Canad. J. Math. **41**, 1117–1123 (1989)
20. Lam, C.W.H., Thiel, L., Swiercz, S., McKay, J.: The nonexistence of ovals in a projective plane of order 10. Discrete Math. **45**, 319–321 (1983)
21. Makhnev, A.A.: Extensions of $GQ(4, 2)$, the description of hyperovals. Discrete Math. Appl. **7**, 419–435 (1997)
22. Pasechnik, D.V.: The triangular extensions of a generalized quadrangle of order $(3, 3)$. Bull. Belg. Math. Soc. Simon Stevin **2**, 509–518 (1995)
23. Pasechnik, D.V.: The extensions of the generalized quadrangle of order $(3, 9)$. Eur. J. Combin. **17**, 751–755 (1996)
24. Pavese, F.: Hyperovals on $H(3, q^2)$ left invariant by a group of order $6(q + 1)^3$. Discrete Math. **313**, 1543–1546 (2013)
25. Payne, S.E., Thas, J.A.: Finite generalized quadrangles. In: EMS Series of Lectures in Mathematics, 2nd edn. European Mathematical Society (2009)
26. Sage Mathematics Software (Version 6.3), The Sage Developers (2014). http://www.sagemath.org
27. The GAP Group, GAP - Groups, Algorithms, and Programming, Version 4.7.5 (2014). (http://www.gap-system.org)