On ovoids of the generalized quadrangle $H(3, q^2)$

Bart De Bruyn

Department of Mathematics: Algebra and Geometry, Ghent University, Krijgslaan 281 (S25), 9000 Gent, Belgium, Email: Bart.DeBruyn@Ugent.be, ORCID: 0000-0003-4941-7934

Abstract

We construct examples and families of locally Hermitian ovoids of the generalized quadrangle $H(3, q^2)$. We also obtain a computer classification of all locally Hermitian ovoids of $H(3, q^2)$ for $q \leq 4$, and compare the obtained classification for $q = 3$ with the classification of all ovoids of $H(3, 9)$ which is also obtained by computer.

MSC2010: 51E12, 51E20, 11T06
Keywords: ovoid, locally Hermitian, (Hermitian) generalized quadrangle, indicator set, polynomial

1 Introduction

Consider the finite field $\mathbb{F}_{q^2}$ of order q^2, where q is some prime power. A map $f : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ is said to be an *I-map* if $\frac{f(y)-f(x)}{y-x} \notin \mathbb{F}_q$ for all $x, y \in \mathbb{F}_{q^2}$ with $x \neq y$. Every I-map must be bijective. A polynomial $p(x) \in \mathbb{F}_{q^2}[x]$ for which the map $x \mapsto p(x)$ defines an I-permutation of $\mathbb{F}_{q^2}$ is called an *I-polynomial*. Having an I-map $f : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$, we can construct several others:

(C1) $x \mapsto f(x^{\phi^{-1}})^{\phi}$ for every automorphism ϕ of $\mathbb{F}_{q^2}$;
(C2) $x \mapsto f(x + k)$ for every $k \in \mathbb{F}_{q^2}$;
(C3) $x \mapsto f(x) + k$ for every $k \in \mathbb{F}_{q^2}$;
(C4) $x \mapsto \frac{1}{k} f(kx)$ for every $k \in \mathbb{F}_{q^2}^* := \mathbb{F}_{q^2} \setminus \{0\}$;
(C5) $x \mapsto f(x) + kx$ for every $k \in \mathbb{F}_q$;
(C6) $x \mapsto kf(x)$ for every $k \in \mathbb{F}_q^* := \mathbb{F}_q \setminus \{0\}$;
(C7) f^{-1}.

Two I-permutations of $\mathbb{F}_{q^2}$ are called *equivalent* if one of them can be obtained from the other by successively applying the constructions mentioned in (C1)–(C7). Two I-polynomials are called *equivalent* when their associated I-permutations are.

The reason why the above maps are called I-maps is because of their connection with **I**ndicator sets of $\mathrm{AG}(2, q^2)$. Suppose $\mathrm{AG}(2, q^2)$ is the affine plane obtained from the projective plane $\mathrm{PG}(2, q^2)$ by removing a line L_∞. Let B be a Baer subline of L_∞. Then a

set X of q^2 points of $\mathrm{AG}(2,q^2)$ is called an *indicator set (with respect to B)* [4, 13, 14] if any line of $\mathrm{PG}(2,q^2)$ containing two distinct points of X is disjoint from B. Two indicator sets X_1 and X_2 are called *equivalent* if there exists an automorphism of $\mathrm{PG}(2,q^2)$ stabilizing B and mapping X_1 to X_2.

The coordinates of a generic point of $\mathrm{PG}(2,q^2)$ will be denoted by (X_1,X_2,X_3). We will assume L_∞ has equation $X_1=0$ and that the Baer subline B of L_∞ consists of all points of the form $(0,k_1,k_2)$, where $(k_1,k_2)\in\mathbb{F}_q\times\mathbb{F}_q$ with $(k_1,k_2)\neq(0,0)$. Any map $f:\mathbb{F}_{q^2}\to\mathbb{F}_{q^2}$ defines a set $O_f:=\{(1,x,f(x))\,|\,x\in\mathbb{F}_{q^2}\}$ of q^2 points in $\mathrm{AG}(2,q^2)$. It is straightforward to verify that O_f is an indicator set if and only if f is an I-permutation ([5, Section 6]). The following is the first result of this paper.

Theorem 1.1. *If f_1 and f_2 are two I-permutations of $\mathbb{F}_{q^2}$, then the indicator sets O_{f_1} and O_{f_2} of $\mathrm{AG}(2,q^2)$ are equivalent if and only if the maps f_1 and f_2 are equivalent.*

With the aid of the computer algebra systems GAP [17] and SageMath [12], we have classified all indicator sets of $\mathrm{AG}(2,q^2)$ for $q\in\{2,3,4\}$. We found that there are up to equivalence one, three or seven such indicator sets depending on whether q is equal to 2, 3 or 4. For each indicator set O we found with the computer search, we can use (Lagrange) interpolation to find a polynomial $p(x)\in\mathbb{F}_{q^2}[x]$ such that $O=\{(1,x,p(x))\,|\,x\in\mathbb{F}_{q^2}\}$. Our results are summarised in the following theorem.

Theorem 1.2. (1) *Up to equivalence, $\mathbb{F}_4$ has only one I-permutation. Any such permutation is equivalent with $x\mapsto\alpha x$, where α is a root of the irreducible polynomial $x^2+x+1\in\mathbb{F}_2[x]$.*

(2) *Up to equivalence, $\mathbb{F}_9$ has three I-permutations. Any such permutation is equivalent with either $x\mapsto\beta x$, $x\mapsto\beta x^3$ or $x\mapsto\beta^2x^5$, where β is a root of the irreducible polynomial $x^2-x-1\in\mathbb{F}_3[x]$.*

(3) *Up to equivalence, $\mathbb{F}_{16}$ has seven I-permutations. Any such permutation is equivalent with either $x\mapsto\gamma x$, $x\mapsto x^4+\gamma x$, $x\mapsto x^{11}+x^6+\gamma x$, $x\mapsto x^8+\gamma^7x^2$, $x\mapsto x^{10}+x^9+x^8+x^4+x^3+\gamma x$, $x\mapsto x^{11}+x^{10}+x^6+x^5+x^4+\gamma x$ or $x\mapsto x^{11}+\gamma^7x^8+\gamma^8x^5+x^2$, where γ is a root of the irreducible polynomial $x^4+x+1\in\mathbb{F}_2[x]$.*

There are two standard examples of indicator sets ([5]):

(1) The lines of $\mathrm{AG}(2,q^2)$ whose points at infinity do not belong to B. These are called the *classical indicator sets*.

(2) The sets of the form $\mathcal{B}\setminus L$, where $\mathcal{B}$ is a Baer subplane of $\mathrm{PG}(2,q^2)$ intersecting L in a Baer subline disjoint from B. These are called the *semiclassical indicator sets*.

The I-permutations of $\mathbb{F}_{q^2}$ corresponding to classical indicator sets have the form $x\mapsto bx+c$ where $b,c\in\mathbb{F}_{q^2}$ with $b\notin\mathbb{F}_q$. All I-permutations of $\mathbb{F}_{q^2}$ corresponding to semiclassical indicator sets have a description of the form $x\mapsto ax^q+bx+c$, where $a,b,c\in\mathbb{F}_{q^2}$ with $a\neq0$. Up to the construction (C3), these I-permutations are all additive, a map $f:\mathbb{F}_{q^2}\to\mathbb{F}_{q^2}$

being called *additive* if $f(u+v) = f(u) + f(v)$ for all $u, v \in \mathbb{F}_{q^2}$. Obviously, such an additive map is an I-map if and only if $\frac{f(x)}{x} \notin \mathbb{F}_q$ for all $x \in \mathbb{F}_{q^2}^*$.

Now, let $\mathcal{H}$ be a nonsingular Hermitian variety in $\mathrm{PG}(3, q^2)$ with associated polarity ζ ([8]). Let x be a point of $\mathcal{H}$. Then there are $q+1$ lines $K_1, K_2, \ldots, K_{q+1}$ of $\mathcal{H}$ through x which all lie in the tangent plane $\Pi_x = x^\zeta$. Consider the quotient projective space $\mathcal{P}_x \cong \mathrm{PG}(2, q^2)$ whose points and lines are the lines and planes of $\mathrm{PG}(3, q^2)$ through x. The plane Π_x is a line of $\mathcal{P}_x$ and $B = \{K_1, K_2, \ldots, K_{q+1}\}$ is a Baer subline of this line. Suppose $\mathcal{A}_x \cong \mathrm{AG}(2, q^2)$ is the affine plane that arises from $\mathcal{P}_x$ by considering Π_x as line at infinity.

The points and lines of $\mathrm{PG}(3, q^2)$ contained in $\mathcal{H}$ define a generalized quadrangle $H(3, q^2)$, see [11]. An *ovoid* of a point-line geometry is a set of points meeting each line in a singleton. An ovoid O of $H(3, q^2)$ is said to be a *translation ovoid* with respect to a point $y \in O$ if there exists a group G of automorphisms of $H(3, q^2)$ fixing each line of $H(3, q^2)$ through y and acting regularly on $O \setminus \{y\}$. An ovoid of $H(3, q^2)$ is called *classical* if it is obtained by intersecting $\mathcal{H}$ with a nontangent plane.

Suppose $\mathcal{L}$ is an indicator set of $\mathcal{A}_x$ (with respect to the Baer subline B of the line at infinity Π_x of $\mathcal{A}_x$). By [14, Section 1.1.3], the set $\mathcal{O}_\mathcal{L} := \bigcup_{L \in \mathcal{L}} (L \cap \mathcal{H})$ is then an ovoid of $H(3, q^2)$. Any ovoid of $H(3, q^2)$ that arises in this way is called *locally Hermitian*. If $\mathcal{L}$ is a classical indicator set, then $\mathcal{O}_\mathcal{L}$ is a classical ovoid of $H(3, q^2)$. The ovoids of $H(3, q^2)$ arising from semiclassical indicator sets are called *semiclassical ovoids*. Every ovoid of $H(3, q^2)$ associated with an indicator set that is described by an additive I-polynomial is a translation ovoid, see [5, Section 6]. By [6, Theorem 3.2], two locally Hermitian ovoids of $H(3, q^2)$ are isomorphic if and only if their associated indicator sets are equivalent, i.e. if and only if the associated I-maps are equivalent. This fact in combination with Theorem 1.2 gives the following result.

Corollary 1.3. *Up to isomorphism, $H(3, q^2)$ has one, three or seven locally Hermitian ovoids depending on whether q is equal to 2, 3 or 4.*

In Section 7, we compare the classification of the locally Hermitian ovoids of $H(3, 9)$ with the (computer) classification of all ovoids of $H(3, 9)$.

In this paper, we construct several examples and families of indicator sets of $\mathrm{AG}(2, q^2)$ which we didn't find in the literature. Certain of these indicator sets are associated with I-monomials of $\mathbb{F}_{q^2}[x]$. We denote by $E(q^2)$ the set of all $e \in \{1, 2, \ldots, q^2 - 1\}$ for which there exists an $\lambda \in \mathbb{F}_{q^2}$ such that λx^e is an I-polynomial. Regarding I-monomials, the following can be proved.

Theorem 1.4. (1) *If q is odd, then $q \in E(q^2)$. In fact, $x \mapsto \lambda x^q$ with $\lambda \in \mathbb{F}_{q^2}$ is an I-permutation of $\mathbb{F}_{q^2}$ if and only if λ is a nonsquare, and any two such maps are always equivalent.*

(2) *If $q = p^h$ with p an odd prime and $h \in \mathbb{N}^* := \mathbb{N} \setminus \{0\}$, then $p^i \in E(q^2)$ for any $i \in \{1, 2, \ldots, 2h - 1\}$.*

(3) *If $q = 2^h$ with $h \in \mathbb{N}^*$, then 2^i with $i \in \{1, 2, \ldots, 2h-1\}$ belongs to $E(q^2)$ if and only if the largest power of 2 dividing i is bigger than the largest power of 2 dividing h.*

(4) *If q is an odd prime power, then $\frac{q^2+1}{2} \in E(q^2)$.*

(5) *Suppose $q \equiv 3 \pmod 6$, $q \equiv 5 \pmod 6$ or $q = 2^{2e+1}$ for some $e \in \mathbb{N}^*$. Then*[1] *$q+2, (q+2)^{-1} \in E(q^2)$.*

Parts (1), (2) and (3) of Theorem 1.4 are all consequences of the treatment that we will give in Section 4. Among these results, Theorem 1.4(2) was already proved in [4, Theorem 3.1] (see also Proposition 4.5 of [5] for a special case of that result). It could be that parts (1) and (2) are also known, but we found no mentioning of them in the literature.

Parts (4) and (5) of Theorem 1.4 will respectively be proved in Sections 5 and 6. The indicator sets arising from the examples mentioned in (4) can also be found in Section 2 of [5] (using another description). We found no mentioning of Theorem 1.4(5) in the literature, nor of the associated ovoids of $H(3, q^2)$.

Based on computer computations, we would also like to propose the following open problem (which is confirmed by computer computations for $q \leq 100$).

Open Problem Is it true that $(2q+3), (2q+3)^{-1} \in E(q^2)$ whenever $q \not\equiv 1 \pmod 5$ and $q \not\equiv 4 \pmod 5$?

Remark: If $e \in \{1, 2, \ldots, q^2-1\}$ with $\gcd(e, q^2-1) = 1$ and $f : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2} : x \mapsto \lambda x^e$ is an I-map, then the inverse of f is equal to $f' : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2} : x \mapsto \lambda' x^{e'}$, where $e' = e^{-1}$ and $\lambda' = (\lambda^{e'})^{-1}$. Hence, if $e \in E(q^2)$, then also $e^{-1} \in E(q^2)$. If q is an odd prime power, then $(\frac{q^2+1}{2})^{-1} = \frac{q^2+1}{2}$.

2 Proof of Theorem 1.1

Suppose f is an I-permutation of $\mathbb{F}_{q^2}$. In (G1)–(G7) below, we describe automorphisms of $\mathrm{PG}(2, q^2)$ which all together generate[2] the group of all automorphisms of $\mathrm{PG}(2, q^2)$ stabilizing B. Each of these automorphisms θ maps the indicator set O_f of $\mathrm{AG}(2, q^2)$ to another indicator set O_g of $\mathrm{AG}(2, q^2)$. For the automorphism θ described under (Gi), $i \in \{1, 2, \ldots, 7\}$, we show that the permutation g of $\mathbb{F}_{q^2}$ can be obtained from f in the way as described in construction (Ci). This then allows to conclude that two indicator sets are equivalent if and only if their corresponding I-permutations of $\mathbb{F}_{q^2}$ are.

(G1) Suppose $\theta : (x_1, x_2, x_3) \mapsto (x_1^\phi, x_2^\phi, x_3^\phi)$ for some automorphism ϕ of $\mathbb{F}_{q^2}$. Since $(1, x, f(x))^\theta = (1, x^\phi, f(x)^\phi)$, we see that $g(x) = f(x^{\phi^{-1}})^\phi$ for every $x \in \mathbb{F}_{q^2}$.

[1] If $\gcd(a, q^2-1)$, then a^{-1} denotes the inverse of a modulo q^2-1.

[2] Note that the group generated by the automorphisms mentioned under (G1), (G5), (G6), (G7) induces the full group of automorphisms of L stabilizing B.

(G2)-(G3)-(G4) Suppose θ fixes each point of L. Then there exist $a, b, c \in \mathbb{F}_{q^2}$ with $a \neq 0$ such that $(x_1, x_2, x_3)^\theta = (ax_1, bx_1 + x_2, cx_1 + x_3)$. Since $(1, x, f(x))^\theta = (a, b + x, c + f(x)) = (1, \frac{b}{a} + \frac{x}{a}, \frac{c}{a} + \frac{f(x)}{a})$, we have $g(x) = \frac{c}{a} + \frac{1}{a} f(ax - b)$ for every $x \in \mathbb{F}_{q^2}$. We can consider the following three special cases of this.

(G2) Suppose $a = 1$, $b = -k \in \mathbb{F}_{q^2}$ and $c = 0$. Then $g(x) = f(x + k)$ for every $x \in \mathbb{F}_{q^2}$.

(G3) Suppose $a = 1$, $b = 0$ and $c = k \in \mathbb{F}_{q^2}$. Then $g(x) = f(x) + k$ for every $x \in \mathbb{F}_{q^2}$.

(G4) Suppose $a = k \in \mathbb{F}_{q^2}^*$ and $b = c = 0$. Then $g(x) = \frac{1}{k} f(kx)$ for every $x \in \mathbb{F}_{q^2}$.

(G5) Suppose $\theta : (x_1, x_2, x_3) \mapsto (x_1, x_2, x_3 + kx_2)$ where $k \in \mathbb{F}_q$. Since $(1, x, f(x))^\theta = (1, x, f(x) + kx)$, we have $g(x) = f(x) + kx$ for every $x \in \mathbb{F}_{q^2}$.

(G6) Suppose $\theta : (x_1, x_2, x_3) \mapsto (x_1, x_2, kx_3)$ where $k \in \mathbb{F}_q^*$. Since $(1, x, f(x))^\theta = (1, x, kf(x))$, we have $g(x) = kf(x)$ for every $x \in \mathbb{F}_{q^2}$.

(G7) Suppose $\theta : (x_1, x_2, x_3) \mapsto (x_1, x_3, x_2)$. Since $(1, x, f(x))^\theta = (1, f(x), x)$, we have $g(x) = f^{-1}(x)$ for every $x \in \mathbb{F}_{q^2}$.

We have completed the proof of Theorem 1.1.

3 Proof of Theorem 1.2

Continuing with the notation of Section 1, we define a point-line geometry $\mathcal{S}_q$ whose points are the points of $\mathrm{AG}(2, q^2)$ and whose lines are all the lines of $\mathrm{AG}(2, q^2)$ whose corresponding points at infinity belong to B, with incidence being the one derived from $\mathrm{AG}(2, q^2)$. The point-line geometry $\mathcal{S}_q$ has order $(q^2 - 1, q)$ and is an example of a net (in the sense of Bruck [3]). If L is a line of $\mathrm{AG}(2, q^2)$ whose corresponding point at infinity does not belong to B, then L is also called an *imaginary line* of $\mathcal{S}_q$, while the ordinary lines of $\mathcal{S}_q$ are also called *real lines*. We denote by $\mathcal{A}(\mathcal{S}_q)$ the group of automorphisms of $\mathcal{S}_q$ that arise from automorphisms of $\mathrm{PG}(2, q^2)$ that stabilize B. Then $\mathcal{A}(\mathcal{S}_q)$ consists of all automorphisms of $\mathcal{S}_q$ that do not only map real lines to real lines, but also every imaginary line to an imaginary line.

The ovoids of the geometry $\mathcal{S}_q$ are precisely the indicator sets of $\mathrm{AG}(2, q^2)$ with respect to B. Two ovoids of $\mathcal{S}_q$ are equivalent as indicator sets if there exists an element of $\mathcal{A}(\mathcal{S}_q)$ mapping one of them to the other. In Section 4 of [1], computer code in SageMath [12] can be found for classifying ovoids of point-line geometries. With the aid of this code and some computations in GAP [17], we classified all ovoids of $\mathcal{S}_q$ for $q \in \{2, 3, 4\}$, see [7]. Our results are summarised in Table 1.

It turns out that up to equivalence the number of ovoids of $\mathcal{S}_q$ is equal to one, three or seven depending on whether q is equal to 2, 3 or 4. For each ovoid, we have also listed some information, like the size of its equivalence class (column 3) and its intersection pattern (column 4). The *intersection pattern* of an ovoid O of $\mathcal{S}_q$ is defined as the sequence $0^{e_0} 1^{e_1} \cdots (q^2)^{e_{q^2}}$, where e_i for $i \in \{0, 1, \ldots, q^2\}$ denotes the total number of imaginary lines meeting O in precisely i points. We have hereby followed the convention to omit each term "i^{e_i}" for which $e_i = 0$.

Ovoid	q	#	Intersection Pattern	$f(x)$
O_1	2	8	$0^3 1^4 4^1$	αx
O_2	3	54	$0^8 1^{45} 9^1$	βx
O_3	3	108	$0^{24} 1^{18} 3^{12}$	βx^3
O_4	3	486	$0^{24} 1^{12} 2^{16} 5^2$	$\beta^2 x^5$
O_5	4	192	$0^{15} 1^{176} 16^1$	γx
O_6	4	960	$0^{60} 1^{112} 4^{20}$	$x^4 + \gamma x$
O_7	4	9216	$0^{65} 1^{75} 2^{50} 6^1 11^1$	$x^{11} + x^6 + \gamma x$
O_8	4	9600	$0^{84} 1^{48} 2^{48} 4^{12}$	$x^8 + \gamma^7 x^2$
O_9	4	23040	$0^{78} 1^{66} 2^{25} 3^{20} 5^2 6^1$	$x^{10} + x^9 + x^8 + x^4 + x^3 + \gamma x$
O_{10}	4	46080	$0^{75} 1^{72} 2^{25} 3^{15} 5^5$	$x^{11} + x^{10} + x^6 + x^5 + x^4 + \gamma x$
O_{11}	4	153600	$0^{78} 1^{66} 2^{27} 3^{15} 4^3 5^3$	$x^{11} + \gamma^7 x^8 + \gamma^8 x^5 + x^2$

Table 1: The ovoids of $\mathcal{S}_q$, $q \leq 4$

For each ovoid O of $\mathcal{S}_q$ we find with the computer search, we can use interpolation to find a polynomial $p(x) \in \mathbb{F}_{q^2}[x]$ (necessarily being an I-polynomial) such that $O = \{(1, x, p(x)) \mid x \in \mathbb{F}_{q^2}\}$. In this way, we found a suitable polynomial for each equivalence class of ovoids. Such a polynomial is listed in the last column of Table 1, where α, β and γ play the same role as in Theorem 1.2.

As mentioned in the introduction, the problem of finding the equivalence classes of I-permutations of $\mathbb{F}_{q^2}$ is equivalent with finding the equivalence classes of indicator sets of $\mathrm{AG}(2, q^2)$, i.e. the equivalence classes of ovoids of $\mathcal{S}_q$. Theorem 1.2 is thus a consequence of our computer classification of the ovoids of $\mathcal{S}_q$. We also wish to note that we have used the constructions (C1)–(C7) to find the "easiest forms" for the mentioned polynomials.

4 Additive I-monomials

The I-polynomials of degree 1 in $\mathbb{F}_{q^2}[x]$ are precisely the maps $x \mapsto bx + c$, where $b, c \in \mathbb{F}_{q^2}$ with $b \notin \mathbb{F}_q$. Regarding I-polynomial of degree 2, we can say the following.

Proposition 4.1. *There are no I-polynomials of degree 2 in $\mathbb{F}_{q^2}[x]$.*

Proof. Consider a polynomial $f(x) = ax^2 + bx + c$ of degree 2 in $\mathbb{F}_{q^2}[x]$. If $x, y \in \mathbb{F}_{q^2}$ with $x \neq y$, then $\frac{f(y)-f(x)}{y-x} = a(x+y) + b$ and, as $a \neq 0$, this can attain any value in $\mathbb{F}_{q^2}$ if q is odd and any value in $\mathbb{F}_{q^2} \setminus \{b\}$ if q is even. □

We now consider I-permutations of $\mathbb{F}_{q^2}$ that are of the form $x \mapsto \lambda x^e$, where $e \in \{1, 2, \ldots, q^2-1\}$ and $\lambda \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. As such a map must be bijective, we have $gcd(e, q^2-1) = 1$. As $\frac{\lambda x^e - \lambda 0^e}{x-0} = \lambda x^{e-1} \notin \mathbb{F}_q$ for all $x \in \mathbb{F}_{q^2}^*$, we have $gcd(e-1, q^2-1) \neq 1$. For each prime power $q \leq 32$, we have determined all possibilities for the exponent e, see Appendix A.

We now assume that $q = p^h$ and $e = p^i$, where p is prime, $h \in \mathbb{N}^*$ and $i \in \{1, 2, \ldots, 2h-1\}$. In this case the map $x \mapsto \lambda x^e$ is additive. Put $d := \gcd(e-1, q+1)$.

Lemma 4.2. *The set*

$$A = \{x^{e-1}y \,|\, x \in \mathbb{F}_{q^2}^* \text{ and } y \in \mathbb{F}_q^*\}$$

consists of all dth powers of the elements of $\mathbb{F}_{q^2}^*$. As a consequence, $|A| = \frac{q^2-1}{d}$.

Proof. Let γ be a primitive element of $\mathbb{F}_{q^2}$. Then the elements of the form $x^{e-1}y$ with $x \in \mathbb{F}_{q^2}^*$ and $y \in \mathbb{F}_q^*$ are precisely the elements of the from $\gamma^{(e-1)i} \cdot \gamma^{(q+1)j} = \gamma^{(e-1)i+(q+1)j}$ where $i, j \in \mathbb{Z}$. By Bézout's theorem, we know that these elements are all elements of the form γ^{dk} where $k \in \mathbb{Z}$. □

Theorem 4.3. *The map $x \mapsto \lambda x^e$ is an I-permutation if and only if λ is not a dth power in $\mathbb{F}_{q^2}$.*

Proof. We should have that $\lambda x^{e-1} \notin \mathbb{F}_q$ for all $x \in \mathbb{F}_{q^2}^*$, or equivalently, $\lambda \notin \{(x^{-1})^{e-1}y \,|\, x \in \mathbb{F}_{q^2}^* \text{ and } y \in \mathbb{F}_q^*\} = A$. The claim then follows from Lemma 4.2. □

By Lemma 4.2 and Theorem 4.3, we thus have:

Corollary 4.4. *$e = p^i \in E(q^2)$ if and only if $d = \gcd(e-1, q+1) > 1$.*

The following proposition proves Theorem 1.4(1).

Proposition 4.5. *We have $q \in E(q^2)$ if and only if q is odd, in which case there is only one equivalence class of I-permutations of $\mathbb{F}_{q^2}$ of the form $x \mapsto \lambda x^q$ (comprising all such permutations for which λ is a nonsquare).*

Proof. We have $\gcd(q-1, q+1) > 1$ if and only if q is odd. This in combination with Corollary 4.4 proves the first claim of the theorem.

If q is odd, we know by Theorem 4.3 that the map $f_\lambda : x \mapsto \lambda x^q$ is an I-map if and only if λ is a nonsquare. If λ_1 and λ_2 are two nonsquares of $\mathbb{F}_{q^2}^*$, then $\lambda_2 = \beta^2\lambda_1$ for some $\beta \in \mathbb{F}_{q^2}^*$. For such a β, we see that f_{λ_1} and $f_{\lambda_1\beta^{q+1}}$ are equivalent by construction (C6) and $f_{\lambda_1\beta^{q+1}}$ and $f_{\lambda_1\beta^2} = f_{\lambda_2}$ are equivalent by construction (C4). □

Lemma 4.6. *Put $f = \gcd(i, h)$. If $\frac{i}{f}$ is even and $\frac{h}{f}$ is odd, then $\gcd(e-1, q+1) = p^f + 1 \geq 3$. If this is not the case, then $\gcd(e-1, q+1)$ is equal to 2 or 1 depending on whether p is odd or even.*

Proof. If $\epsilon_1, \epsilon_2 \in \{1, -1\}$ and $i_1, i_2 \in \mathbb{N}^*$ with $i_1 < i_2$, then any common divisor of $p^{i_1} + \epsilon_1$ and $p^{i_2} + \epsilon_2$ is also a common divisor of $p^{i_2-i_1} - \epsilon_1\epsilon_2$. By Euclid's algorithm for computing gcd's, we thus see that $\gcd(e-1, q+1) = \gcd(p^i - 1, p^h + 1) = \gcd(p^i - 1, p^h + 1, p^f + \epsilon)$ for some $\epsilon \in \{1, -1\}$.

If $\frac{i}{f}$ is even and $\frac{h}{f}$ is odd, then $p^f + 1$ is a divisor of $p^i - 1$ and $p^h + 1$, and in this case, we thus see that $\gcd(p^i - 1, p^h + 1) = p^f + 1$.

If $\frac{h}{f}$ is even, then $p^f + \epsilon$ is a divisor of $p^h - 1$ and so we have $\gcd(p^i - 1, p^h + 1) = \gcd(p^i - 1, p^h + 1, 2)$. If $\frac{i}{f}$ and $\frac{h}{f}$ are odd, then $p^f + \epsilon$ is a divisor of $p^i + 1$ if $\epsilon = 1$ and $p^f + \epsilon$ is a divisor of $p^h - 1$ if $\epsilon = -1$. In any case, we also have $\gcd(p^i - 1, p^h + 1) = \gcd(p^i - 1, p^h + 1, 2)$. Now, $\gcd(p^i - 1, p^h + 1, 2)$ is equal to 2 if p is odd and equal to 1 otherwise. □

The following is an immediate consequence of Corollary 4.4 and Lemma 4.6. It proves parts (2) and (3) of Theorem 1.4.

Corollary 4.7.
- *If p is odd, then $e = p^i \in E(q^2)$.*
- *If $p = 2$, then $e = 2^i \in E(q^2)$ if and only if the largest power of 2 dividing i is bigger than the largest power of 2 dividing h.*

5 Proof of Theorem 1.4(4)

Let q be an odd prime power and α a primitive element of $\mathbb{F}_{q^2}$. Then α cannot be a square. We put $\beta = \alpha^{(q+1)/2}$. The following property of finite fields is well-known, see e.g. [10, Exercise 2.13].

Lemma 5.1. *If $x \in \mathbb{F}_{q^2}^*$, then $x^{(q^2-1)/2}$ is equal to 1 or -1 depending on whether x is a square or not.*

Lemma 5.2. *We have $\beta^q = -\beta$. As a consequence, $\beta \notin \mathbb{F}_q$.*

Proof. As α is a nonsquare, we have $\alpha^{(q^2-1)/2} = -1$. We then have $\beta^q = \alpha^{(q^2+q)/2} = \alpha^{(q^2-1)/2}\alpha^{(q+1)/2} = -\beta$. □

Theorem 5.3. *The map $\mathbb{F}_{q^2} \to \mathbb{F}_{q^2} : x \mapsto \beta x^{(q^2+1)/2}$ is an I-map.*

Proof. We need to show that

$$g(x, y) = \frac{\beta(y^{(q^2+1)/2} - x^{(x^2+1)/2})}{y - x} \notin \mathbb{F}_q$$

for all $x, y \in \mathbb{F}_{q^2}$ with $x \neq y$. Since $\beta \notin \mathbb{F}_q$ and $z^{(q^2-1)/2} = \left(z^{(q-1)/2}\right)^{q+1} \in \mathbb{F}_q^*$ for every $z \in \mathbb{F}_{q^2}^*$, this is certainly true if one of x, y is zero. We therefore suppose that $0 \neq x \neq y \neq 0$.

Suppose x and y are two distinct nonzero squares in $\mathbb{F}_{q^2}$. By Lemma 5.1,

$$g(x, y) = \beta\frac{y - x}{y - x} = \beta \notin \mathbb{F}_q.$$

Suppose x and y are two distinct nonsquares in $\mathbb{F}_{q^2}$. By Lemma 5.1,

$$g(x, y) = \beta\frac{-y + x}{y - x} = -\beta \notin \mathbb{F}_q.$$

Suppose one of x, y in a nonzero square and the other is a nonsquare. Then there exists an $\epsilon \in \{1, -1\}$ such that $g(x, y) = \epsilon\beta\frac{x+y}{x-y}$. If $g(x, y) \in \mathbb{F}_q$, then we would have

$$0 = \Big(\beta\frac{x+y}{x-y}\Big) - \Big(\beta\frac{x+y}{x-y}\Big)^q = \beta\Big(\frac{x+y}{x-y} + \frac{x^q+y^q}{x^q-y^q}\Big) = 2\beta\frac{x^{q+1}-y^{q+1}}{(x-y)(x^q-y^q)}.$$

So, $\left(\frac{x}{y}\right)^{q+1} = 1$, i.e. $\frac{x}{y}$ is a $(q-1)$th power. But then $\frac{x}{y}$ is a square which is obviously not possible here. □

We now show that the indicator set of $\mathrm{AG}(2, q^2)$ corresponding to the I-map $x \mapsto \alpha^{(q+1)/2}x^{(q^2+1)/2}$ is equivalent with the indicator set described in Section 2 of [5].

Let (X_1, X_2, X_3) denote the coordinates of a point of $\mathrm{PG}(2, q^2)$. Let L_∞ denote the line of $\mathrm{PG}(2, q^2)$ with equation $X_1 = 0$ and regard it as the line at infinity of $\mathrm{PG}(2, q^2)$. Let B' be the Baer subline of L_∞ consisting of all points $(0, 1, z)$ where $z^{q+1} = 1$. By [5, Section 2], the set

$$\{(1, 0, 0)\} \cup \{(1, x, 0) \,|\, x \text{ is a square of } \mathbb{F}_{q^2}^*\} \cup \{(1, 0, y) \,|\, y \text{ is a nonsquare of } \mathbb{F}_{q^2}\}$$

is an indicator set of $\mathrm{AG}(2, q^2)$ with respect to B'.

Now, the indicator set X of $\mathrm{AG}(2, q^2)$ corresponding to the I-map $x \mapsto \alpha^{(q+1)/2}x^{(q^2+1)/2}$ consists of all points of the form

$$(1, x, \alpha^{(q+1)/2}x^{(q^2+1)/2}),$$

where $x \in \mathbb{F}_{q^2}$. If $x = 0$, then this is the point $(1, 0, 0)$.

If x is a nonzero square, i.e. $x = y^2$ for some $y \in \mathbb{F}_{q^2}^*$, then

$$x^{(q^2+1)/2} = y^{q^2+1} = y^2 = x.$$

If x is a nonsquare, i.e. $x = \alpha y^2$ for some $y \in \mathbb{F}_{q^2}^*$, then

$$x^{(q^2+1)/2} = \alpha^{(q^2+1)/2}y^{q^2+1} = \alpha^{(q^2-1)/2}\alpha y^2 = -\alpha y^2 = -x.$$

Now, let θ be the automorphism of $\mathrm{PG}(2, q^2)$ determined by

$$(X_1, X_2, X_3) \mapsto (X_1, \frac{1}{2}(X_2 + \alpha^{-(q+1)/2}X_3), \frac{1}{2}(X_2 - \alpha^{-(q+1)/2}X_3)).$$

Then $L_\infty^\theta = L_\infty$ and X^θ consists of the following points:

- $(1, 0, 0)$,
- $(1, x, 0)$ where x is a nonzero square of $\mathbb{F}_{q^2}$;
- $(1, 0, y)$ where y is a nonsquare of $\mathbb{F}_{q^2}$.

Moreover, θ maps the Baer subline $B = \{(0, k_2, k_3) \,|\, k_2, k_3 \in \mathbb{F}_q \text{ with } (k_2, k_3) \neq (0, 0)\}$ to

$$B^\theta = \{(0, k_2 + \alpha^{-(q+1)/2}k_3, k_2 - \alpha^{-(q+1)/2}k_3) \,|\, k_2, k_3 \in \mathbb{F}_q \text{ with } (k_2, k_3) \neq (0, 0)\}.$$

We show that $B^\theta = B'$. To that end, it suffices to prove that

$$\Big(\frac{k_2 - k_3\alpha^{-(q+1)/2}}{k_2 + k_3\alpha^{-(q+1)/2}}\Big)^{q+1} = 1, \qquad \forall k_2, k_3 \in \mathbb{F}_q \text{ with } (k_2, k_3) \neq (0,0).$$

Indeed, as $(\alpha^{-(q+1)/2})^q = -\alpha^{-(q+1)/2}$, we have

$$\frac{k_2 - k_3\alpha^{-(q+1)/2}}{k_2 + k_3\alpha^{-(q+1)/2}} \cdot \frac{(k_2 - k_3\alpha^{-(q+1)/2})^q}{(k_2 + k_3\alpha^{-(q+1)/2})^q} = \frac{k_2 - k_3\alpha^{-(q+1)/2}}{k_2 + k_3\alpha^{-(q+1)/2}} \cdot \frac{k_2 + k_3\alpha^{-(q+1)/2}}{k_2 - k_3\alpha^{-(q+1)/2}} = 1.$$

6 Proof of Theorem 1.4(5)

Lemma 6.1. *Let $q = p^h$ with p prime and $h \in \mathbb{N}^*$. If $i \in \mathbb{N}$ with $3 \leq i \leq q-1$, then $\binom{q+2}{i} \equiv 0 \pmod{p}$.*

Proof. Note that $q \geq 4$. We have

$$\begin{aligned}\binom{q+2}{i} &= \frac{(q+2)(q+1)\cdots(q+3-i)}{1\cdot 2\cdot\cdots\cdot i} \\ &= \frac{(q-1)(q-2)\cdots(q-i)}{1\cdot 2\cdot\cdots\cdot i} \cdot \frac{(q+2)(q+1)q}{(q-i)(q-i+1)(q-i+2)}.\end{aligned}$$

For every $j \in \{1, 2, \ldots, i\}$, the largest power of p dividing j equals the largest power of p dividing $q-j$. The largest power of p dividing $(q+2)(q+1)q$ is $q = p^h$ if p is odd and 2^{h+1} if $p = 2$. The largest power of p dividing $(q-i)(q-i+1)(q-i+2)$ is smaller than $q = p^h$ if p is odd and smaller than 2^{h+1} if $p = 2$. We conclude that

$$\binom{q+2}{i} \equiv 0 \pmod{p}.$$

□

Now, suppose that p is a prime and $h \in \mathbb{N}^*$ such that precisely one of the following cases occurs (with $q = p^h$):

(a) $p = 2$ and $h \geq 3$ is an odd integer;

(b) $p = 3$;

(c) q is congruent to 5 modulo 6.

Let α be a primitive element of $\mathbb{F}_{q^2}$ and define $\beta := \alpha^{(q^2-1)\cdot\gcd(p,6)/6}$. Also, let f be the the map $\mathbb{F}_{q^2} \to \mathbb{F}_{q^2} : x \mapsto \alpha' x^{q+2}$, where $\alpha' = \alpha^{(q+1)\cdot\gcd(p,6)/6}$. Note that the number $(q+1)\cdot\gcd(p,6)/6$ (and hence also $(q^2-1)\cdot\gcd(p,6)/6$) is always an integer in each of the cases (a), (b), (c).

Lemma 6.2. *We have $(\alpha')^q = \beta\alpha'$.*

Proof. We have

$$(\alpha')^q = \alpha^{(q^2+q)\cdot \gcd(p,6)/6} = \alpha^{(q^2-1)\cdot \gcd(p,6)/6} \cdot \alpha^{(q+1)\cdot \gcd(p,6)/6} = \beta\alpha'.$$

□

Lemma 6.3. *We have $\beta \neq 1$ and $\alpha' \notin \mathbb{F}_q$.*

Proof. The (multiplicative) order of the primitive element α is equal to q^2-1. So, for the element β to be equal to 1, we should have that $\gcd(p,6) = 6$. This condition is never satisfied. As $(\alpha')^q = \beta\alpha' \neq \alpha'$, we have $\alpha' \notin \mathbb{F}_q$. □

Lemma 6.4. *We have $\beta^3 = -1$, $\beta^2 = \beta - 1$ and $\beta^q = 1 - \beta$. If $p = 3$, then $\beta = -1$.*

Proof. Suppose first that $p = 3$. Then $\beta = \alpha^{(q^2-1)/2}$ and so $\beta^2 = 1$. As $\beta \neq 1$, we have $\beta = -1$. One then readily verifies that $\beta^3 = -1$, $\beta^2 = \beta - 1$ and $\beta^q = 1 - \beta$.

So, we may suppose that $p \neq 3$. Since $\beta^6 = \alpha^{(q^2-1)\cdot \gcd(p,6)} = 1$, we have $\beta^3 \in \{1, -1\}$. In case (a), we have $1 = -1$ (as $p = 2$) and in case (c), we have $\beta^3 = \alpha^{(q^2-1)/2} \neq 1$ (since α has multiplicative order q^2-1). In any case, we have $\beta^3 = -1$.

We thus also have $(\beta+1)(\beta^2-\beta+1) = 0$. In case (a), we have $\beta \neq 1 = -1$ by Lemma 6.3 and in case (c), we have $\beta^2 = \alpha^{(q^2-1)/3} \neq 1$. In any case, $\beta \neq -1$. So, $\beta^2 - \beta + 1 = 0$ and $\beta^2 = \beta - 1$.

Suppose now that $\beta \in \mathbb{F}_q$, i.e. $\beta^{q-1} = 1$. In case (a) the fact that h is odd implies that $\gcd(3, q-1) = 1$. This in combination with $\beta^3 = \beta^{q-1} = 1$ then implies that $\beta = 1$, a contradiction. In case (6), the facts that $\beta^6 = \beta^{q-1} = 1$ and $\gcd(6, q-1) = 2$ then imply that $\beta^2 = 1$, in contradiction with $1 \neq \beta \neq -1$. So, $\beta \notin \mathbb{F}_q$ and $\beta^q \neq \beta$.

Now, as $\beta^2 - \beta + 1 = 0$, we also have $(\beta^q)^2 - \beta^q + 1 = 0$, implying that $\beta^q \in \{\beta, 1-\beta\}$. By the previous paragraph, we then know that $\beta^q = 1 - \beta$. □

Theorem 6.5. *f is an I-map.*

Proof. Recall that $(\alpha')^q = \beta\alpha'$. As $\alpha' \notin \mathbb{F}_q$ and $z^{q+1} \in \mathbb{F}_q^*$ for all $z \in \mathbb{F}_{q^2}^*$, we know that the condition

$$\alpha' \frac{y^{q+2} - x^{q+2}}{y - x} \notin \mathbb{F}_q$$

for distinct $x, y \in \mathbb{F}_{q^2}$ is certainly valid if one of x, y is zero. So, we may suppose that x and y are nonzero. Then

$$\alpha' \frac{y^{q+2} - x^{q+2}}{y - x} = \alpha' x^{q+1} \frac{z^{q+2} - 1}{z - 1} = \alpha' x^{q+1} \frac{(u+1)^{q+2} - 1}{u},$$

where $z = \frac{y}{x}$ and $u = z - 1$. As $x^{q+1} \in \mathbb{F}_q^*$, we need to prove that

$$\alpha' \frac{(u+1)^{q+2} - 1}{u} \notin \mathbb{F}_q$$

for all $u \in \mathbb{F}_{q^2}^*$. By Lemma 6.1, we need to prove that

$$\alpha'(u^{q+1} + 2u^q + u^{q-1} + u + 2) \notin \mathbb{F}_q$$

for all $u \in \mathbb{F}_{q^2}^*$. Suppose to the contrary that $\alpha'(u^{q+1} + 2u^q + u^{q-1} + u + 2) \in \mathbb{F}_q$ for a certain $u \in \mathbb{F}_{q^2}^*$. As $(\alpha')^q = \beta\alpha'$, this condition is equivalent with

$$(u^{q+1} + 2u^q + u^{q-1} + u + 2) - \beta(u^{q+1} + 2u^q + u^{q-1} + u + 2)^q$$

$$= (u^{q+1} + 2u^q + u^{q-1} + u + 2) - \beta(u^{q+1} + 2u + \frac{1}{u^{q-1}} + u^q + 2) = 0.$$

Multiplying by u^{q+1} and rearranging terms, we find

$$\Big((1-\beta)u^2 + (2-\beta)u + 1\Big)u^{2q} + \Big((1-2\beta)u^2 + (2-2\beta)u\Big)u^q - \beta u^2 = 0.$$

Taking into account that $\beta^2 - \beta + 1 = 0$, this is equivalent with

$$\Big(((1-\beta)u + 1)u^q - (\beta-1)u\Big) \cdot \Big((u+1)u^q - (\beta-1)u\Big) = 0.$$

As $\beta \neq 1$ and $u \neq 0$, at least one of the following cases occurs:
(1) $u + 1 \neq 0$ and $u^q = \frac{(\beta-1)u}{u+1}$;
(2) $(1-\beta)u + 1 \neq 0$ and $u^q = \frac{(\beta-1)u}{(1-\beta)u+1}$.
If case (1) occurs, then

$$u = \frac{(\beta^q - 1)u^q}{u^q + 1} = \frac{(1 - \beta - 1) \cdot \frac{(\beta-1)u}{u+1}}{\frac{(\beta-1)u}{u+1} + 1} = \frac{-\beta(\beta-1)u}{\beta u + 1},$$

implying that $\beta u = -\beta^2 + \beta - 1 = 0$, in contradiction with $u \neq 0$.

If case (2) occurs, then

$$u = \frac{(\beta^q - 1)u^q}{(1-\beta^q)u^q + 1} = \frac{\frac{-\beta(\beta-1)u}{(1-\beta)u+1}}{\frac{\beta(\beta-1)u}{(1-\beta)u+1} + 1} = \frac{-\beta(\beta-1)u}{(\beta^2 - 2\beta + 1)u + 1},$$

implying that $(\beta-1)^2 u = -\beta^2 + \beta - 1 = 0$, in contradiction with $u \neq 0$ and $\beta \neq 1$. □

Remark. The only prime powers $q = p^h$ for which $q + 2 \in E(q^2)$ are those considered in the cases (a), (b) and (c) above. Indeed, the map $x \mapsto x^{q+2}$ should be bijective, implying that $1 = \gcd(q+2, q^2-1) = \gcd(q+2, (q+1)(q-1)) = \gcd(q+2, q-1) = \gcd(3, q-1)$. So, q cannot be congruent to 1 modulo 3.

7 The ovoids of $H(3,9)$

Consider again the Hermitian variety $\mathcal{H}$ associated with a Hermitian polarity ζ of $\mathrm{PG}(3,q^2)$. A line L of $\mathrm{PG}(3,q^2)$ is called a *hyperbolic line* if it intersects $\mathcal{H}$ in precisely $q+1$ points. This intersection of $q+1$ points is a Baer subline of L and is called a *chord*. If L is a hyperbolic line, then also L^ζ is a hyperbolic line and the chord $L^\zeta \cap \mathcal{H}$ is called the *opposite chord* of $L \cap \mathcal{H}$.

As before, let $H(3,q^2)$ denote the generalized quadrangle associated with $\mathcal{H}$. If O is an ovoid of $H(3,q^2)$ containing a chord C, then the point set which arises from O by replacing C with its opposite chord is also an ovoid of $H(3,q^2)$, see [15, 16]. This process of constructing ovoids of $H(3,q^2)$ from others is called *derivation*.

By [2], the generalized quadrangle $H(3,4)$ has two isomorphism classes of ovoids, the classical ovoids and the ovoids that arise from classical ovoids by means of one derivation. From Table 1, we know that there are up to isomorphism three locally Hermitian ovoids of $H(3,9)$. We obtained this conclusion by classifying all ovoids of the point-line geometry $\mathcal{S}_3$. The computational techniques we used to compute all ovoids of $\mathcal{S}_q$ with $q \leq 4$ can also be used to compute all ovoids of $H(3,9)$, see [7]. Our results are summarized in Table 2. It turns out that there are up to isomorphism 26 ovoids in $H(3,9)$. The number of ovoids in each isomorphism class has been listed in the second column. The locally Hermitian ovoids of $H(3,9)$ are the ovoids of types 1, 2 and 7, respectively corresponding to the I-polynomials βx, βx^3 and $\beta^2 x^5$. Computations show that the isomorphism class to which an ovoid O belongs is uniquely determined by two combinatorial parameters:

- D: the number of classical ovoids disjoint from O;
- S: the number of classical ovoids intersecting O in a singleton.

We explain a number of other entries in the table, hereby denoting by G the full automorphism group of $H(3,9)$ and by G_O the setwise stabiliser (in G) of an ovoid O:

- N_1 is the number of orbits of G_O on O;
- N_2 is the number of orbits of G_O on the complement of O;
- C is the number of chords contained in O;
- a symbol i^e occurring in the column "Derivation" means that there are precisely e chords in O for which derivation yields an ovoid of type i;
- in case O can be obtained by successive derivations from a classical ovoid, the last column denotes the minimal number M of such derivations that are necessary.

We thus see that among the 26 ovoids of $H(3,9)$, there are 12 that can be obtained from classical ovoids by means of successive derivations (the M hyperbolic lines involved in the derivation process can in fact all be chosen in the same plane, namely the plane from which the classical ovoid arises). It would be interesting to have explicit computer free constructions for the 26 ovoids.

Type	#	D	S	C	Derivation	N_1	N_2	M
1	540	0	224	63	4^{63}	1	1	0
2	30240	0	240	9	10^9	2	2	—
3	34020	12	160	15	$5^3 9^{12}$	2	3	3
4	34020	37	96	31	$1^1 5^6 14^{24}$	2	4	1
5	102060	40	96	15	$3^1 4^2 8^4 13^8$	3	6	2
6	136080	76	24	7	$7^1 13^6$	2	7	4
7	136080	51	24	15	$6^1 14^6 21^8$	3	6	3
8	204120	17	144	7	$5^2 9^1 14^4$	3	7	3
9	204120	20	112	7	$3^2 8^1 13^4$	3	7	4
10	272160	50	96	1	2^1	2	7	—
11	272160	24	112	3	12^3	3	6	—
12	272160	24	160	3	11^3	3	6	—
13	408240	44	96	7	$5^2 6^2 9^2 14$	4	11	3
14	408240	34	80	15	$4^2 7^2 8^2 13^1 22^8$	5	10	2
15	622080	42	126	0	—	2	8	—
16	725760	36	108	0	—	3	11	—
17	725760	45	96	0	—	3	11	—
18	816480	50	88	1	19^1	3	14	—
19	816480	34	96	1	18^1	4	13	—
20	933120	35	126	0	—	3	13	—
21	1088640	52	69	4	$7^1 22^3$	5	20	4
22	1088640	27	109	6	$14^3 21^3$	5	17	3
23	1088640	51	70	0	—	3	15	—
24	1866240	29	126	0	—	3	22	—
25	2177280	39	126	3	26^3	6	30	—
26	3265920	49	80	2	25^2	7	39	—

Table 2: The ovoids of $H(3, 9)$

A Determination of some $E_l(q^2)$'s

If λx^e is an I-monomial of $\mathbb{F}_{q^2}[x]$, then the map $x \mapsto \lambda x^e$ is bijective and hence $gcd(e, q^2-1) = 1$. Also, as $\frac{\lambda x^e - \lambda 0^e}{x-0} = \lambda x^{e-1} \notin \mathbb{F}_q$ for all $x \in \mathbb{F}_{q^2}^*$, we have $\lambda \notin \mathbb{F}_q$ and $gcd(e-1, q^2-1) \neq 1$. For each prime power $q \leq 32$, we computed all I-monomials λx^e, see [7]. If we denote by $E(q^2)$ the set of all $e \in \{1, 2, \ldots, q^2-1\}$ for which there exists an I-monomial of $\mathbb{F}_{q^2}[x]$ of the form λx^e, then we have:

- $E(2^2) = \{1\}$,
- $E(3^2) = \{1, 3, 5\}$,
- $E(4^2) = \{1\}$,
- $E(5^2) = \{1, 5, 7, 13\}$,
- $E(7^2) = \{1, 7, 17, 25\}$,
- $E(8^2) = \{1, 4, 10, 16, 19\}$,
- $E(9^2) = \{1, 3, 9, 11, 27, 41, 51\}$,
- $E(11^2) = \{1, 11, 13, 37, 61\}$,
- $E(13^2) = \{1, 13, 29, 85\}$,
- $E(16^2) = \{1\}$,
- $E(17^2) = \{1, 17, 19, 37, 91, 109, 145\}$,
- $E(19^2) = \{1, 19, 181\}$,
- $E(23^2) = \{1, 23, 25, 49, 97, 169, 265\}$,
- $E(25^2) = \{1, 5, 25, 53, 125, 313, 365\}$,
- $E(27^2) = \{1, 3, 9, 27, 29, 57, 81, 99, 113, 243, 281, 365, 393, 477, 603\}$,
- $E(29^2) = \{1, 29, 31, 271, 421\}$,
- $E(31^2) = \{1, 31, 481\}$,
- $E(32^2) = \{1, 4, 16, 34, 64, 67, 256, 331, 397\}$.

More generally, if $l \in \mathbb{N}^*$, then $E_l(q^2)$ denotes the set of all subsets $\{e_1, e_2, \ldots, e_l\} \subseteq \mathbb{N}^*$ such that $1 \leq e_1 < e_2 < \cdots < e_l \leq q^2 - 1$ and there exist $\lambda_1, \lambda_2, \ldots, \lambda_l \in \mathbb{F}_{q^2}^*$ such that $x \mapsto \sum_{i=1}^{l} \lambda_i x^{e_i}$ is an I-permutation of $\mathbb{F}_{q^2}$. We denote by $E'_l(q^2)$ the subset of $E_l(q^2)$ consisting of all $\{e_1, e_2, \ldots, e_l\} \subseteq \mathbb{N}^*$ satisfying the above conditions but with the extra requirement that $\lambda_1 \notin \mathbb{F}_q$ if $e_1 = 1$. If $I \in E_l(q^2) \setminus E'_l(q^2)$ for some $l \in \mathbb{N}^*$, then $l \geq 2$, $1 \in I$ and $I \setminus \{1\} \in E'_{l-1}(q^2)$ by construction (C5). Conversely, by construction (C5) we know that if $l \geq 2$ and $I \in E'_{l-1}(q^2)$ with $1 \notin I$, then $I \cup \{1\} \in E_l(q^2)$. If one is interested in finding only one representative for each equivalence class of I-polynomials, it suffices to consider the sets $E'_l(q^2)$. With the aid of a computer, we found all sets $E'_2(q^2)$ for $q \leq 9$ and all sets $E'_3(q^2)$ for $q \leq 5$ ([7]):

- $E'_2(2^2) = E'_2(3^2) = \{\}$,
- $E'_2(4^2) = \{\{1, 4\}, \{2, 8\}\}$,
- $E'_2(5^2) = \{\{1, 5\}, \{7, 19\}\}$,
- $E'_2(7^2) = \{\{1, 7\}, \{5, 17\}, \{5, 29\}, \{17, 41\}\}$,
- $E'_2(8^2) = \{\{1, 8\}, \{2, 16\}, \{4, 32\}, \{16, 37\}\}$,
- $E'_2(9^2) = \{\{1, 9\}, \{3, 27\}, \{11, 27\}, \{21, 61\}, \{29, 61\}, \{31, 71\}\}$,
- $E'_3(2^2) = E'_3(3^2) = \{\}$,
- $E'_3(4^2) = \{\{1, 6, 11\}\}$,

(q,e)	λ	(q,e)	λ	(q,e)	λ	(q,e)	λ	(q,e)	λ
$(3,5)$	α^2	$(9,51)$	α^5	$(17,109)$	α^7	$(25,313)$	α^{13}	$(27,477)$	α^{14}
$(5,7)$	α	$(11,13)$	α^2	$(17,145)$	α^9	$(25,365)$	α^{13}	$(27,603)$	α^7
$(5,13)$	α^3	$(11,37)$	α^2	$(19,181)$	α^{10}	$(27,29)$	α^{14}	$(29,31)$	α^5
$(7,17)$	α	$(11,61)$	α^6	$(23,25)$	α^4	$(27,57)$	α^7	$(29,271)$	α^5
$(7,25)$	α^4	$(13,29)$	α^5	$(23,49)$	α^5	$(27,99)$	α^7	$(29,421)$	α^{15}
$(8,10)$	α^3	$(13,85)$	α^7	$(23,97)$	α^5	$(27,113)$	α^{14}	$(31,481)$	α^{16}
$(8,19)$	α^3	$(17,19)$	α^3	$(23,169)$	α^4	$(27,281)$	α^7	$(32,34)$	α^{11}
$(9,11)$	α^5	$(17,37)$	α^7	$(23,265)$	α^{12}	$(27,365)$	α^{14}	$(32,67)$	α^{11}
$(9,41)$	α^5	$(17,91)$	α^3	$(25,53)$	α^{13}	$(27,393)$	α^{14}	$(32,331)$	α^{11}
—	—	—	—	$(32,397)$	α^{11}	—	—	—	—

Table 3: The nonadditive I-monomials λx^e of $\mathbb{F}_{q^2}[x]$, $q \leq 32$

$q = p^h$	$f(x)$	$q = p^h$	$f(x)$
2	$x^2 + x + 1$	16	$x^8 + x^4 + x^3 + x^2 + 1$
3	$x^2 - x - 1$	17	$x^2 - x + 3$
4	$x^4 + x + 1$	19	$x^2 - x + 2$
5	$x^2 - x + 2$	23	$x^2 - 2x + 5$
7	$x^2 - x + 3$	25	$x^4 - x^2 - x + 2$
8	$x^6 + x^4 + x^3 + x + 1$	27	$x^6 - x^4 + x^2 - x - 1$
9	$x^4 - x^3 - 1$	29	$x^2 - 5x + 2$
11	$x^2 - 4x + 2$	31	$x^2 - 2x + 3$
13	$x^2 - x + 2$	32	$x^{10} + x^6 + x^5 + x^3 + x^2 + x + 1$

Table 4: A primitive polynomial $f(x)$ of degree $2h$ in $\mathbb{F}_p[x]$, $q = p^h \leq 32$

- $E_3'(5^2) = \{\{1, 7, 13\}, \{1, 9, 17\}, \{3, 11, 19\}\}$.

For additive I-polynomials, the corresponding ovoids of $H(3, q^2)$ are translation ovoids related to so-called semifield spreads of PG$(3, q)$, see [5]. These spreads and their related semifields have extensively been discussed in the literature, see e.g. [9].

Let us now turn our attention to non-additive I-monomials of $\mathbb{F}_{q^2}[x]$ with $q \leq 32$, non-additive I-binomials of $\mathbb{F}_{q^2}[x]$ with $q \leq 9$ and non-additive I-trinomials of $\mathbb{F}_{q^2}[x]$ with $q \leq 5$. We have verified by computer that for each $q = p^h \leq 32$ and each $e \in E(q^2)$ not being a power of p, there exists up to equivalence a unique I-polynomial of the form λx^e. These I-monomials have been listed in Table 3. In this table, α is a primitive element of $\mathbb{F}_{q^2}$ that is a root of the polynomial mentioned in Table 4.

We have also verified that each subset of $E_2'(q^2)$, $q = p^h \leq 9$, and each subset of $E_3'(q^2)$, $q = p^h \leq 5$, not entirely consisting of powers of p, is associated with either one or two I-polynomials (up to equivalence). These have been listed in Table 5. Also here, α is a

q	$E_l'(q^2)$	$f(x)$
5	$\{7, 19\}$	$x^7 + \alpha^9 x^{19}$, $\alpha^3 x^7 + \alpha^9 x^{19}$
7	$\{5, 17\}$	$\alpha^2 x^5 + x^{17}$
7	$\{5, 29\}$	$x^5 + \alpha^{25} x^{29}$, $\alpha^2 x^5 + \alpha^{46} x^{29}$
7	$\{17, 41\}$	$x^{17} + \alpha^4 x^{41}$
8	$\{16, 37\}$	$\alpha x^{16} + \alpha^{36} x^{37}$
9	$\{11, 27\}$	$\alpha^5 x^{11} + \alpha^5 x^{27}$
9	$\{21, 61\}$	$\alpha x^{21} + \alpha^5 x^{61}$, $\alpha^5 x^{21} + \alpha^{25} x^{61}$
9	$\{29, 61\}$	$\alpha x^{29} + \alpha^5 x^{61}$
9	$\{31, 71\}$	$\alpha^5 x^{31} + \alpha^{25} x^{71}$
4	$\{1, 6, 11\}$	$\alpha x + x^6 + x^{11}$
5	$\{1, 7, 13\}$	$\alpha x + x^7 + \alpha^{21} x^{13}$
5	$\{1, 9, 17\}$	$\alpha x + \alpha^7 x^9 + \alpha^5 x^{17}$
5	$\{3, 11, 19\}$	$\alpha x^3 + \alpha^5 x^{11} + \alpha^{15} x^{19}$, $\alpha x^3 + \alpha^{23} x^{11} + \alpha^3 x^{19}$

Table 5: Some I-binomials and I-trinomials

primitive element of $\mathbb{F}_{q^2}$ that is a root of the polynomial mentioned in Table 4.

Finally, we wish to mention that we found more subsets of the $E_l(q^2)$'s than the ones mentioned above. Through ad-hoc searches we found for instance that $\{1, 17, 33\} \in E_3'(7^2)$ and $\{1, 7, 13, 19\} \in E_4'(5^2)$.

References

[1] A. Bishnoi and B. De Bruyn. On generalized hexagons of order $(3, t)$ and $(4, t)$ containing a subhexagon. *European J. Combin.* 62 (2017), 115–123.

[2] A. E. Brouwer and H. A. Wilbrink. Ovoids and fans in the generalized quadrangle $Q(4, 2)$. *Geom. Dedicata* 36 (1990), 121–124.

[3] R. H. Bruck. Finite nets. I. Numerical invariants. *Canadian J. Math.* 3 (1951), 94–107.

[4] A. Bruen. Spreads and a conjecture of Bruck and Bose. *J. Algebra* 23 (1972), 519–537.

[5] A. Cossidente, G. L. Ebert, G. Marino and A. Siciliano. Shult sets and translation ovoids of the Hermitian surface. *Adv. Geom.* 6 (2006), 523–542.

[6] A. Cossidente, G. Lunardon, G. Marino and O. Polverino. Hermitian indicator sets. *Adv. Geom.* 7 (2007), 357–373.

[7] B. De Bruyn. Computer code for "On ovoids of the generalized quadrangle $H(3, q^2)$". Available online from `http://cage.ugent.be/geometry/preprints.php`.

[8] J. W. P. Hirschfeld and J. A. Thas. *General Galois geometries.* Springer Monographs in Mathematics. Springer, 2016.

[9] N. L. Johnson, V. Jha and M. Biliotti. *Handbook of finite translation planes.* Pure and Applied Mathematics 289. Chapman & Hall/CRC, 2007.

[10] R. Lidl and H. Niederreiter. *Finite fields.* Encyclopedia of Mathematics and its Applications 20. Cambridge University Press, 1997.

[11] S. E. Payne and J. A. Thas. *Finite generalized quadrangles.* EMS Series of Lectures in Mathematics. European Mathematical Society (EMS), Zürich, 2009.

[12] *Sage Mathematics Software (Version 6.3)*, The Sage Developers, 2014, `http://www.sagemath.org`.

[13] F. A. Sherk and G. Pabst. Indicator sets, reguli, and a new class of spreads. *Canad. J. Math.* 29 (1977), 132–154.

[14] E. E. Shult. Problems by the wayside. *Discrete Math.* 294 (2005), 175–201.

[15] J. A. Thas. Semi-partial geometries and spreads of classical polar spaces. *J. Combin. Theory Ser. A* 35 (1983), 58–66.

[16] J. A. Thas and S. E. Payne. Spreads and ovoids in finite generalized quadrangles. *Geom. Dedicata* 52 (1994), 227–253.

[17] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.7.5, 2014. (http://www.gap-system.org)