Journal of Combinatorial Theory, Series A 175 (2020) 105279

Contents lists available at ScienceDirect

Journal of Combinatorial Theory, Series A

www.elsevier.com/locate/jcta

On m-ovoids of symplectic polar spaces

Tao Feng [a], Ye Wang [a], Qing Xiang [b,*]

[a] *School of Mathematical Sciences, Zhejiang University, 38 Zheda Road, Hangzhou 310027, Zhejiang PR China*
[b] *Department of Mathematical Sciences, University of Delaware, Newark, DE 19716, USA*

ARTICLE INFO

Article history:
Received 16 September 2019
Received in revised form 24 May 2020
Accepted 25 May 2020
Available online 4 June 2020

Keywords:
Cyclotomic class
Intriguing set
m-ovoid
Strongly regular graph
Symplectic polar space

ABSTRACT

In this paper, we develop a new method for constructing m-ovoids in the symplectic polar space $\mathrm{W}(2r-1,p^e)$ from some strongly regular Cayley graphs constructed in [6]. Using this method, we obtain many new m-ovoids which can not be derived by field reduction.

1. Introduction

Let $e \geq 1, r \geq 2$ be integers, p be a prime, and $\mathbb{F}_{p^e}$ be the finite field of size p^e. Let V be a $2r$-dimensional vector space over $\mathbb{F}_{p^e}$ and f be a non-degenerate alternating form defined on V. The symplectic polar space $\mathrm{W}(2r-1,p^e)$ associated with the form f is the geometry consisting of subspaces of $\mathrm{PG}(V)$ induced by the totally isotropic subspaces with respect to f. The symplectic polar space $\mathrm{W}(2r-1,p^e)$ contains totally isotropic

* Corresponding author.
E-mail addresses: tfeng@zju.edu.cn (T. Feng), ye_wang@zju.edu.cn (Y. Wang), qxiang@udel.edu (Q. Xiang).

https://doi.org/10.1016/j.jcta.2020.105279
0097-3165/

points, lines, planes, etc. Note that since f is alternating, every point of $\mathrm{PG}(V)$ is totally isotropic. Therefore the set of points of $\mathrm{W}(2r-1,p^e)$ coincides with the set of points of $\mathrm{PG}(V)$. The (totally isotropic) subspaces of maximum dimension are called *maximals* (or *generators*) of $\mathrm{W}(2r-1,p^e)$. The *rank* of $\mathrm{W}(2r-1,p^e)$ is the vector space dimension of its maximals, namely r.

In this paper, we are concerned with m-ovoids in $\mathrm{W}(2r-1,p^e)$. An *m-ovoid* in $\mathrm{W}(2r-1,p^e)$ is a set $\mathcal{M}$ of points such that every maximal of $\mathrm{W}(2r-1,p^e)$ meets $\mathcal{M}$ in exactly m points. A 1-ovoid in $\mathrm{W}(2r-1,p^e)$ is simply called an *ovoid*. Ovoids in $\mathrm{W}(2r-1,p^e)$ (and more generally in any classical polar space) were first defined by Thas [20] in 1981. The existence problem for ovoids in $\mathrm{W}(2r-1,p^e)$ is completely solved: $\mathrm{W}(3,p^e)$ has an ovoid if and only if $p=2$; and $\mathrm{W}(2r-1,p^e)$, $r>2$, has no ovoids. The concept of an m-ovoid was first defined by Thas [21] for generalized quadrangles, and then generalized to that in classical polar spaces by Shult and Thas [19]. There are some closely related objects, called i-tight sets, in $\mathrm{W}(2r-1,p^e)$. We will not study i-tight sets in this paper, but simply mention that m-ovoids and i-tight sets of $\mathrm{W}(2r-1,p^e)$ can be unified under the umbrella of intriguing sets [2] of $\mathrm{W}(2r-1,p^e)$.

Intriguing sets (in particular, m-ovoids) in classical polar spaces have close connections with other geometric and combinatorial structures such as strongly regular graphs and projective two-weight codes, cf. [2–4,8]. For example, m-ovoids in $\mathrm{W}(2r-1,p^e)$ turn out to be projective two-intersection sets in $\mathrm{PG}(2r-1,p^e)$ and thus give rise to strongly regular graphs, cf. [2]. There is also a significant relation between projective two-intersection sets and two-weight codes, cf. [8]. A construction of m-ovoids in $\mathrm{Q}^-(5,p^e)$ via strongly regular Cayley graphs was given in [3].

The main problem concerning m-ovoids in $\mathrm{W}(2r-1,p^e)$ is: For which $m\geq 1$ does there exist an m-ovoid in $\mathrm{W}(2r-1,p^e)$? As we mentioned above, when $m=1$, this problem is completely solved. In sharp contrast, the existence problem for m-ovoids with $m\geq 2$ is wide open. We give a brief summary of known results here. We start with $\mathrm{W}(3,p^e)$: When p is odd, there are no ovoids in $\mathrm{W}(3,p^e)$, cf. [17]; but there is a partition of $\mathrm{W}(3,p^e)$ into 2-ovoids, so there exists an m-ovoid in $\mathrm{W}(3,p^e)$ for each even positive integer m, cf. [4]; moreover Cossidente et al. gave a construction of $\frac{(p^e+1)}{2}$-ovoids in $\mathrm{W}(3,p^e)$ when p is odd in [7]. When $p=2$, Cossidente et al. gave a construction of m-ovoids for all possible m in $\mathrm{W}(3,p^e)$ in [7]. Next we consider the case of $\mathrm{W}(5,p^e)$: First there are some sporadic examples of m-ovoids in $\mathrm{W}(5,p^e)$, cf. [2]; when $p=2$, Cossidente and Pavese [9] gave two constructions of nonclassical (p^e+1)-ovoids in $\mathrm{W}(5,p^e)$ by utilizing relative hemisystems and embedded Suzuki-Tits ovoids of a Hermitian surface. For general $\mathrm{W}(2r-1,p^e)$, in terms of necessary conditions, it is proved in [2] that if there exists an m-ovoid in $\mathrm{W}(2r-1,p^e)$ with $r>2$, then $m\geq \frac{(-3+\sqrt{9+4p^{er}})}{2p^e-2}$; as for constructions, Cossidente and Pavese [10] gave a partition of $\mathrm{W}(4n-1,p^e)$ into a $\frac{(p^{e(2n-2)}-1)}{p^e-1}$-ovoid, a $p^{e(2n-2)}$-ovoid and some $2p^{e(2n-2)}$-ovoids for p^e even. Shult and Thas [19] introduced the notion of m-systems in finite classical polar spaces, and showed that the points underlying the subspaces of an m-system of $W(2r-1,p^e)$ yield a $\frac{(p^{e(m+1)}-1)}{p^e-1}$-ovoid. In [19, Theorem 14],

they further showed that if $H(r-1,p^{2e})$, r odd, contains an m-system, then a $(2m+1)$-system of $W(2r-1,p^e)$ can be obtained by field reduction. Hence, when $r=3$, there is a 1-system of $W(5,p^e)$ arising from a 0-system in $H(2,p^{2e})$, and so we obtain a (p^e+1)-ovoid in $W(5,p^e)$. Also we should mention an important construction method: by using field reduction, an m'-ovoid in low rank classical polar spaces gives rise to an m-ovoid in higher rank classical polar space. Specifically with the method of field reduction, an m'-ovoid in $W(2r'-1,p^{e'})$ gives rise to an m-ovoid in $W(2r-1,p^e)$ if $r' \mid r$ and $re = r'e'$, cf. [14]. In the end of Section 3 of this paper, we will construct m-ovoids in $W(2r-1,p^e)$, with r being a prime, say p_0; since p_0 has only two factors 1 and p_0, an m-ovoid in $W(2p_0-1,p^e)$ can not be constructed from an m'-ovoid in a symplectic polar space with rank lower than p_0.

As can be seen from the above summary there has been very little work on m-ovoids in high rank symplectic polar spaces. In terms of constructions, when q is odd, the only known construction method for m-ovoids in high rank symplectic polar spaces is the field reduction method, cf. [14]. In this paper, we develop a new construction method which allows us to construct many new m-ovoids in high rank symplectic polar spaces. Specifically we show that there are many m-ovoids in $W(2r-1,p^e)$ with new parameters arising from the partial difference sets in Theorem 3.5. To facilitate the description of our method, we give the following equivalent definition of m-ovoids in $\mathrm{W}(2r-1,p^e)$.

Lemma 1.1. *Let $\mathcal{M}$ be a set of points of $\mathrm{W}(2r-1,p^e)$. Then $\mathcal{M}$ is an m-ovoid if and only if*

$$|P^{\perp}\cap\mathcal{M}| = \begin{cases} m(p^{e(r-1)}+1)-p^{e(r-1)}, & \text{if } P\in\mathcal{M},\\ m(p^{e(r-1)}+1), & \text{otherwise.}\end{cases} \tag{1.1}$$

For a proof of the lemma, we refer the reader to [2]. The basic idea of our construction of m-ovoids is to use a partial converse to Theorem 11 in [2]. Concerning $\mathrm{W}(2r-1,p^e)$, Theorem 11 in [2] says that an m-ovoid gives rise to a strongly regular Cayley graph over $(\mathbb{F}_{p^e}^{2r},+)$ of negative Latin square type. A partial converse to this statement is true; that is, a strongly regular Cayley graph over $(\mathbb{F}_{p^e}^{2r},+)$ of negative Latin square type with some special property can give rise to an m-ovoid in $\mathrm{W}(2r-1,p^e)$ (the special property is the "self-dual" property; this will be made precise in Theorem 3.2). To implement this strategy, we start with some strongly regular Cayley graphs $\mathrm{Cay}(\mathbb{F}_q,D)$ in [6], and equip the ambient finite field $\mathbb{F}_q$, now viewed as a vector space over a subfield $\mathbb{F}_{p^e}$, with an appropriate non-degenerate alternating form f, and show that with respect to f, D is "self-dual", hence the set $\mathcal{M}$ of projective points obtained from D will satisfy (1.1), giving rise to an m-ovoid in the symplectic polar space $\mathrm{W}(2r-1,p^e)$ of rank r. The organization of this paper is as follows. In Section 2, we give some preliminaries on strongly regular graphs and describe the construction using cyclotomic classes of finite fields in [6]. In Section 3, we first describe our construction strategy, and then give the details of our construction of m-ovoids. We conclude the paper with Section 4.

2. Preliminaries

A *strongly regular graph* $\mathrm{srg}(v,k,\lambda,\mu)$ is a simple and undirected graph, neither complete nor edgeless, that has the following properties:

(1) It is a regular graph of order v and valency k.

(2) For each pair of adjacent vertices x,y, there are exactly λ vertices adjacent to both x and y.

(3) For each pair of nonadjacent vertices x,y, there are exactly μ vertices adjacent to both x and y.

For example, the pentagon is an $\mathrm{srg}(5,2,0,1)$ and the Petersen graph is an $\mathrm{srg}(10,3,0,1)$. The parameters of an $\mathrm{srg}(v,k,\lambda,\mu)$ satisfy the following basic relation.

Lemma 2.1. [13, Section 10.1] *Let Γ be an srg(v,k,λ,μ). Then*

$$k(k-\lambda-1)=\mu(v-k-1).$$

Let Γ be a (simple, undirected) graph. The adjacency matrix of Γ is the $(0,1)$-matrix A with both rows and columns indexed by the vertices of Γ, where $A_{xy}=1$ when there is an edge between x and y in Γ and $A_{xy}=0$ otherwise. The *eigenvalues* of Γ are defined to be those of its adjacency matrix A. For convenience we call an eigenvalue of Γ *restricted* if it has an eigenvector which is not a multiple of the all-ones vector $\mathbf{1}$. (For a k-regular connected graph, the restricted eigenvalues are simply the eigenvalues different from k.)

Theorem 2.2. *For a simple graph Γ of order v, neither complete nor edgeless, with adjacency matrix A, the following are equivalent:*

1. *Γ is strongly regular with parameters (v,k,λ,μ) for certain integers k,λ,μ,*
2. *$A^2=(\lambda-\mu)A+(k-\mu)I+\mu J$ for certain real numbers k,λ,μ, where I,J are the identity matrix and the all-ones matrix, respectively,*
3. *A has precisely two distinct restricted eigenvalues α_1,α_2.*

For a proof of Theorem 2.2, we refer the reader to [5]. For later use, we write down the explicit relations between the parameters of an $\mathrm{srg}(v,k,\lambda,\mu)$ and its restricted eigenvalues α_1,α_2.

Lemma 2.3. [13, Section 10.2] *Let Γ be an srg(v,k,λ,μ) with restricted eigenvalues α_1, α_2, where $\alpha_1>\alpha_2$. Then*

$$\begin{aligned}\alpha_1&=\frac{(\lambda-\mu)+\sqrt{(\lambda-\mu)^2+4(k-\mu)}}{2},\\ \alpha_2&=\frac{(\lambda-\mu)-\sqrt{(\lambda-\mu)^2+4(k-\mu)}}{2},\end{aligned}\tag{2.1}$$

with multiplicities

$$m_1 = \frac{1}{2}\left((v-1) - \frac{2k+(v-1)(\lambda-\mu)}{\sqrt{(\lambda-\mu)^2+4(k-\mu)}}\right) \quad \textit{and}$$
$$m_2 = \frac{1}{2}\left((v-1) + \frac{2k+(v-1)(\lambda-\mu)}{\sqrt{(\lambda-\mu)^2+4(k-\mu)}}\right),$$

respectively.

An effective method to construct strongly regular graphs is by the Cayley graph construction. Let G be an additively written abelian group of order v, and let D be a subset of G such that $0 \notin D$ and $-D = D$, where $-D = \{-d \mid d \in D\}$. The *Cayley graph on G with connection set D*, denoted by $\mathrm{Cay}(G, D)$, is the graph with the elements of G as vertices; two vertices are adjacent if and only if their difference belongs to D. Let $\hat{G}$ be the (complex) character group of G. All the eigenvalues of $\mathrm{Cay}(G, D)$ are given by $\psi(D) := \sum_{d\in D} \psi(d)$, $\psi \in \hat{G}$. Note that $\psi_0(D) = |D|$, where ψ_0 is the principal character of G. By Theorem 2.2, the graph $\mathrm{Cay}(G, D)$ is strongly regular if and only if D generates G and $\{\psi(D) : \psi \in \hat{G} \setminus \{\psi_0\}\} = \{\alpha_1, \alpha_2\}$ with $\alpha_1 \neq \alpha_2$. If this is the case, then the connection set D is called a *partial difference set*, and the Delsarte *dual* of D is defined to be either of $\{\psi \in \hat{G} : \psi(D) = \alpha_i\}$, $i = 1, 2$.

An $\mathrm{srg}(v, k, \lambda, \mu)$ is said to be of *Latin square type* (resp. *negative Latin square type*) if $(v, k, \lambda, \mu) = (n^2, a(n-\epsilon), \epsilon n + a^2 - 3\epsilon a, a^2 - \epsilon a)$ and $\epsilon = 1$ (resp. $\epsilon = -1$).

Let G and D be the same as above. Suppose that $\mathrm{Cay}(G, D)$ is an $\mathrm{srg}(v, k, \lambda, \mu)$. Then, by Lemma 2.3, one of the duals of D has the same size as that of D if and only if

$$k = \frac{1}{2}\left((v-1) - \frac{2k+(v-1)(\lambda-\mu)}{\sqrt{(\lambda-\mu)^2+4(k-\mu)}}\right) \text{ or}$$
$$k = \frac{1}{2}\left((v-1) + \frac{2k+(v-1)(\lambda-\mu)}{\sqrt{(\lambda-\mu)^2+4(k-\mu)}}\right),$$

which in turn is equivalent to

$$\frac{(2k+(v-1)(\lambda-\mu))^2}{(\lambda-\mu)^2+4(k-\mu)} = (v-1-2k)^2. \tag{2.2}$$

After some tedious computations, we see that when (2.2) is satisfied, v must be a square, and $\mu = (\frac{k}{\sqrt{v}-1})^2 - \frac{k}{\sqrt{v}-1}$ or $\mu = (\frac{k}{\sqrt{v}+1})^2 + \frac{k}{\sqrt{v}+1}$. Note that by Lemma 2.1, $\lambda = k - 1 + (1 - \frac{v-1}{k})\mu$. Consequently if one of the duals of D has the same size as that of D, then the strongly regular graph $\mathrm{Cay}(G, D)$ must be of Latin square or negative Latin square type.

Conversely, when $(v, k, \lambda, \mu) = (n^2, a(n-1), n + a^2 - 3a, a^2 - a)$, by Lemma 2.3, $\alpha_1 = n - a$ with multiplicity $f = a(n-1)$, and $\alpha_2 = -a$ with multiplicity $g = (n + 1 -$

$a)(n-1)$. Thus the dual $\{\psi \in \hat{G} : \psi(D) = \alpha_1\}$ has the same size as that of D. When $(v,k,\lambda,\mu) = (n^2, a(n+1), -n+a^2+3a, a^2+a)$, by Lemma 2.3, $\alpha_1 = a$ with multiplicity $f = (n-1-a)(n+1)$, and $\alpha_2 = a-n$ with multiplicity $g = a(n+1)$. Thus the dual $\{\psi \in \hat{G} : \psi(D) = \alpha_2\}$ has the same size as that of D.

We will use Cayley graphs $\mathrm{Cay}(\mathbb{F}_q, D)$, where the connection sets are unions of cyclotomic classes, for the purpose of constructing m-ovoids in symplectic polar spaces. To this end, we define cyclotomic classes of finite fields. Let $q = p^s$ be a prime power, and let γ be a fixed primitive element of $\mathbb{F}_q$. Let $N > 1$ be a divisor of $q-1$. We define the N^{th} *cyclotomic classes* $C_i^{(N,q)}$ of $\mathbb{F}_q$ by

$$C_i^{(N,q)} = \{\gamma^{jN+i} \mid 0 \le j \le \frac{q-1}{N} - 1\},$$

where $0 \le i \le N-1$. That is, $C_0^{(N,q)}$ is the subgroup of $\mathbb{F}_q^*$ consisting of all nonzero N^{th} powers in $\mathbb{F}_q$, and $C_i^{(N,q)} = \gamma^i C_0^{(N,q)}$, for $1 \le i \le N-1$. In the sequel, if N, q are clear from the context, we will simply write $C_i^{(N,q)}$ as C_i.

Suppose that $q = p^s$ with p a prime, and let e be any positive divisor of s. Let $\mathrm{Tr}_{q/p^e} : \mathbb{F}_q \to \mathbb{F}_{p^e}$ be the trace function from $\mathbb{F}_q$ to $\mathbb{F}_{p^e}$, i.e.,

$$\mathrm{Tr}_{q/p^e}(x) = x + x^{p^e} + \cdots + x^{p^{e(s/e-1)}}, \ \forall x \in \mathbb{F}_q.$$

Set $\omega_p := \exp\left(\frac{2\pi\sqrt{-1}}{p}\right)$. Define $\psi_{\mathbb{F}_q}\colon \mathbb{F}_q \to \mathbb{C}^*$ by

$$\psi_{\mathbb{F}_q}(x) = \omega_p^{\mathrm{Tr}_{q/p}(x)}, \ \forall x \in \mathbb{F}_q.$$

The map $\psi_{\mathbb{F}_q}$ is a character of the additive group of $\mathbb{F}_q$, and it is called the *canonical* additive character of $\mathbb{F}_q$. For any $y \in \mathbb{F}_q$, we define $\psi_{\mathbb{F}_q,y}\colon \mathbb{F}_q \to \mathbb{C}^*$ by

$$\psi_{\mathbb{F}_q,y}(x) = \psi_{\mathbb{F}_q}(xy), \ \forall x \in \mathbb{F}_q.$$

It is well known that $\{\psi_{\mathbb{F}_q,y} \mid y \in \mathbb{F}_q\} = \widehat{(\mathbb{F}_q, +)}$.

Next we recall the following construction of strongly regular Cayley graphs given in [6], see also [5, Section 9.8.5]. Suppose that $q = p^s$ with p prime, and let N be a proper divisor of $q-1$ such that $p^\ell \equiv -1 \pmod N$ for some positive integer ℓ. Choose ℓ minimal and write $s = 2\ell t$. Take a proper subset $J \subset \mathbb{Z}_N$ of size u. If q is even, then the choice of J is arbitrary; if q is odd, then we require that $N | \frac{q-1}{2}$ and $J + \frac{q-1}{2} = J$. Set $D_J = \cup_{i\in J} C_i$. Then the graph $\mathrm{Cay}(\mathbb{F}_q, D_J)$ is strongly regular with eigenvalues

$$\begin{aligned} k &= \frac{q-1}{N}u, \quad \text{with multiplicity } 1, \\ \alpha_1 &= \frac{u}{N}(-1 + (-1)^t\sqrt{q}), \quad \text{with multiplicitiy } q-1-k, \\ \alpha_2 &= \frac{u}{N}(-1 + (-1)^t\sqrt{q}) + (-1)^{t+1}\sqrt{q}, \quad \text{with multiplicity } k. \end{aligned} \tag{2.3}$$

To be specific, for $i = 0, 1, \ldots, N-1$, we have

$$\psi_{\mathbb{F}_q}(\gamma^i D) = \begin{cases} \alpha_2, & \text{if } \varepsilon^s = 1 \text{ and } i \in -J \pmod N \\ & \quad \text{or } \varepsilon^s = -1 \text{ and } i \in -J + N/2 \pmod N, \\ \alpha_1, & \text{otherwise,} \end{cases} \tag{2.4}$$

where $\varepsilon = \begin{cases} -1, & \text{if } N \text{ is even and } \frac{p^\ell+1}{N} \text{ is odd;} \\ 1, & \text{otherwise.} \end{cases}$

The graph $\mathrm{Cay}(\mathbb{F}_q, D_J)$ is of Latin square type (resp. negative Latin square type) if t is odd (resp. even).

3. Constructions of m-ovoids in $\mathbf{W(2r-1, p^e)}$ via strongly regular Cayley graphs

Throughout the rest of this paper, we fix the following notation. Let $q = p^s$, where p is an odd prime and $s = 2er$ for some positive integers e and $r \geq 2$. We view $\mathbb{F}_q$ as a $2r$-dimensional vector space over $\mathbb{F}_{p^e}$ (a subfield of $\mathbb{F}_q$), and denote this $\mathbb{F}_{p^e}$-vector space by V. As usual, for a nonzero $v \in V$, we write $\langle v \rangle$ for the projective point in the projective space $\mathrm{PG}(V)$ corresponding to the 1-dimensional $\mathbb{F}_{p^e}$-subspace spanned by v. We will equip a bilinear form on V as follows. Let $L(X) = \sum_{i=0}^{2r-1} c_i X^{p^{ie}} \in \mathbb{F}_q[X]$ be a linearized polynomial. Define $f : V \times V \to \mathbb{F}_{p^e}$ by

$$f(x, y) = \mathrm{Tr}_{q/p^e}(xL(y)), \forall (x, y) \in V \times V.$$

Then f is an $\mathbb{F}_{p^e}$-bilinear form on V.

Lemma 3.1. *With notation as above, the $\mathbb{F}_{p^e}$-bilinear form f on V is alternating if and only if $c_0 = 0$ and $c_{2r-i}^{p^{ie}} = -c_i$ for $1 \leq i \leq 2r-1$. Moreover, the form f is non-degenerate if and only if $x \mapsto L(x)$ is a bijection from $\mathbb{F}_q$ to itself.*

Proof. The form f is alternating if and only if $f(x, x) = 0$ for all $x \in V$. We have

$$\begin{aligned} f(x, x) &= \sum_{i=0}^{2r-1} \mathrm{Tr}_{q/p^e}\left(c_i x^{1+p^{ie}}\right) = \sum_{i,j=0}^{2r-1} c_i^{p^{je}} x^{p^{je}+p^{(i+j)e}} \\ &= \sum_{0 \leq i < k \leq 2r-1} (c_{k-i}^{p^{ie}} + c_{2r-k+i}^{p^{ke}}) x^{p^{ie}+p^{ke}} + \sum_{j=0}^{2r-1} c_0^{p^{je}} x^{2p^{je}}. \end{aligned}$$

We view $f(x, x)$ as a polynomial in x with coefficients in $\mathbb{F}_q$. As can be seen from the above expression, $f(x, x)$ has degree less than or equal to $q-1$. The polynomial $f(x, x)$ vanishes at every element of $\mathbb{F}_q$ if and only if it is the zero polynomial. The first claim of the lemma now follows by comparing the coefficients.

Assume that f is non-degenerate. Suppose that $f(x,y) = \mathrm{Tr}_{q/p^e}(xL(y)) = 0$ for all $x \in \mathbb{F}_q$. We must have $L(y) = 0$ since Tr_{q/p^e} is a nontrivial linear form on V. By the assumption that f is non-degenerate, we have $y = 0$. It follows that $x \mapsto L(x)$ is a bijection since L is linearized. The proof of the converse is straightforward. This proves the second claim of the lemma. □

Let $L(X) = \sum_{i=1}^{2r-1} c_i X^{p^{ie}} \in \mathbb{F}_q[X]$ be a linearized permutation polynomial such that $f(x,y) = \mathrm{Tr}_{q/p^e}(xL(y))$ is a non-degenerate alternating form. Equip $V = (\mathbb{F}_q, +)$ with the alternating form f, and this will be our model for the symplectic polar space $\mathrm{W}(2r-1, p^e)$ of rank r. For any nonzero $y \in V$, we define

$$\langle y \rangle^{\perp} = \{\langle x \rangle \mid f(x,y) = 0,\ x \in V \setminus \{0\}\}.$$

Also for any $y \in V$ we define $\Psi_y \in \widehat{(\mathbb{F}_q, +)}$ as follows:

$$\Psi_y(x) = \psi_{\mathbb{F}_q}(xL(y)) = \psi_{\mathbb{F}_{p^e}}(f(x,y)).$$

It is well known that $\{\Psi_y \mid y \in V\} = \widehat{(\mathbb{F}_q, +)}$. We now give the definition of self-dual partial difference sets in $(\mathbb{F}_q, +)$. (Note that such a self-dual partial difference set is necessarily of Latin square type or negative Latin square type by the discussion in the last section.) Let D be an $\mathbb{F}_{p^e}^*$-invariant subset of $\mathbb{F}_q^*$. That is, D is a union of some cosets of $\mathbb{F}_{p^e}^*$ in $\mathbb{F}_q^*$. Assume that $\mathrm{Cay}(\mathbb{F}_q, D)$ is a strongly regular graph of negative Latin square type, and with parameters

$$\left(q, |D|, -\sqrt{q} + (\frac{|D|}{\sqrt{q}+1})^2 + \frac{3|D|}{\sqrt{q}+1}, (\frac{|D|}{\sqrt{q}+1})^2 + \frac{|D|}{\sqrt{q}+1}\right).$$

Let $D^* \subset \mathbb{F}_q \setminus \{0\}$ be such that $\{\Psi_y \in \widehat{(\mathbb{F}_q, +)} \mid y \in D^*\}$ is one of the Delsarte duals. We say that D is *self-dual* if $D^* = D$. Now we state the connection between m-ovoids in $\mathrm{W}(2r-1, p^e)$ and self-dual partial difference sets in $(\mathbb{F}_q, +)$ explicitly.

Theorem 3.2. *With notation as above, let D be an $\mathbb{F}_{p^e}^*$-invariant subset of $\mathbb{F}_q^*$ such that $|D| \equiv 0 \pmod{(\sqrt{q}+1)(p^e-1)}$. Then the set $\mathcal{M} = \{\langle v \rangle : v \in D\}$ is a $\frac{|D|}{(p^e-1)(\sqrt{q}+1)}$-ovoid in $\mathrm{W}(2r-1, p^e)$ if and only if D is a self-dual partial difference set with parameters $(q, |D|, -\sqrt{q} + (\frac{|D|}{\sqrt{q}+1})^2 + \frac{3|D|}{\sqrt{q}+1}, (\frac{|D|}{\sqrt{q}+1})^2 + \frac{|D|}{\sqrt{q}+1})$.*

Proof. Assume that D is a self-dual partial difference set with the above parameters. Then by Lemma 2.3, the graph $\mathrm{Cay}(\mathbb{F}_q, D)$ has two eigenvalues $\alpha_1 = \frac{|D|}{\sqrt{q}+1}$ (with multiplicity $m_1 = q - 1 - |D|$), and $\alpha_2 = \frac{|D|}{\sqrt{q}+1} - \sqrt{q}$ (with multiplicity $m_2 = |D|$); and furthermore since D is self-dual, we have $\Psi_y(D) = \alpha_2$ if $y \in D^* = D$ and $\Psi_y(D) = \alpha_1$ if $y \in \mathbb{F}_q^* \setminus D$.

Write $\mathcal{M} := \{\langle v_i \rangle : 1 \le i \le M\}$, where $M = |D|/(p^e - 1)$. Then $D = \{\theta v_i : 1 \le i \le M,\ \theta \in \mathbb{F}_{p^e}^*\}$. For any nonzero $y \in V$, we have

$$\begin{aligned}\Psi_y(D) &= \sum_{i=1}^{M} \sum_{\theta \in \mathbb{F}_{p^e}^*} \Psi_y(\theta v_i) \\ &= \sum_{i=1}^{M} \sum_{\theta \in \mathbb{F}_{p^e}^*} \psi_{\mathbb{F}_{p^e}}(\theta f(v_i, y)) \\ &= -M + \sum_{i=1}^{M} \sum_{\theta \in \mathbb{F}_{p^e}} \psi_{\mathbb{F}_{p^e}}(\theta f(v_i, y)) \\ &= -M + p^e \cdot |\{1 \le i \le M : f(v_i, y) = 0\}| \\ &= p^e \cdot |\langle y \rangle^\perp \cap \mathcal{M}| - |\mathcal{M}|.\end{aligned}$$

Now from $\Psi_y(D) = \alpha_2$ if $y \in D$, we obtain

$$|\langle y \rangle^\perp \cap \mathcal{M}| = \frac{|D|}{(p^e - 1)(\sqrt{q} + 1)} \cdot (p^{e(r-1)} + 1) - p^{e(r-1)} \text{ if } \langle y \rangle \in \mathcal{M};$$

and from $\Psi_y(D) = \alpha_1$ if $y \in \mathbb{F}_q^* \setminus D$, we obtain

$$|\langle y \rangle^\perp \cap \mathcal{M}| = \frac{|D|}{(p^e - 1)(\sqrt{q} + 1)} \cdot (p^{e(r-1)} + 1) \text{ if } \langle y \rangle \notin \mathcal{M}.$$

Therefore $\mathcal{M}$ is a $\frac{|D|}{(p^e-1)(\sqrt{q}+1)}$-ovoid in $\mathrm{W}(2r-1, p^e)$ by Lemma 1.1. The converse can be proved by simply running the above reasoning backwards. The proof is complete. □

We make some comments on self-duality. Let D be an $\mathbb{F}_{p^e}^*$-invariant subset of $\mathbb{F}_q^*$. Assume that $\mathrm{Cay}(\mathbb{F}_q, D)$ is a strongly regular graph of negative Latin square type, and with parameters

$$\left(q, |D|, -\sqrt{q} + (\frac{|D|}{\sqrt{q}+1})^2 + \frac{3|D|}{\sqrt{q}+1}, (\frac{|D|}{\sqrt{q}+1})^2 + \frac{|D|}{\sqrt{q}+1}\right).$$

Define

$$D' = \{y \in \mathbb{F}_q \mid \psi_{\mathbb{F}_q, y}(D) = \alpha_2\}. \tag{3.1}$$

Noting that $\Psi_y(D) = \psi_{\mathbb{F}_q, L(y)}(D)$, we see that D is self-dual if and only if $L(D) = D'$.

We will use Theorem 3.2 for the purpose of constructing m-ovoids in $\mathrm{W}(2r-1, p^e)$. The first step is to equip V with a concrete non-degenerate alternating form by choosing $L(X)$ carefully. Let γ be a primitive element of $\mathbb{F}_q$ (recall that $q = p^s$ is an odd prime power, and $s = 2er$), and set $\delta = \gamma^{\frac{\sqrt{q}+1}{2}} \in \mathbb{F}_q$. Then we have $\delta^{\sqrt{q}} = -\delta$. Let $L(X) = \delta X^{\sqrt{q}}$. By Lemma 3.1, $f(x, y) := \mathrm{Tr}_{q/p^e}(xL(y))$ is a non-degenerate alternating form defined on V. We will take V equipped with this f as our model for the symplectic polar space $\mathrm{W}(2r-1, p^e)$ in the rest of this paper.

We further assume that $q = p^s$ with $s = 2\ell t$ and t even. Take $N = p^\ell + 1$, and let $C_0, \ldots, C_{N-1}$ be the N^{th} cyclotomic classes of $\mathbb{F}_q$. In this case, it is easy to verify that $N | \frac{q-1}{2}$. Let J be a proper subset of $\mathbb{Z}_N$ of size u, and set $D_J = \cup_{i\in J} C_i$. By [6] (see the discussion in the end of Section 2), the graph $\mathrm{Cay}(\mathbb{F}_q, D_J)$ is a strongly regular graph with negative Latin square type parameters

$$\left(q, \frac{u(\sqrt{q}-1)}{N}(\sqrt{q}+1), -\sqrt{q} + (\frac{u(\sqrt{q}-1)}{N})^2 + \frac{3u(\sqrt{q}-1)}{N}, \right.$$
$$\left. (\frac{u(\sqrt{q}-1)}{N})^2 + \frac{u(\sqrt{q}-1)}{N}\right).$$

Moreover, its eigenvalues are

$$\psi_{\mathbb{F}_q}(\gamma^i D_J) = \begin{cases} \frac{u}{N}(\sqrt{q}-1) - \sqrt{q}, & \text{if } -i \pmod N \in J, \\ \frac{u}{N}(\sqrt{q}-1), & \text{otherwise.} \end{cases} \tag{3.2}$$

It follows that $D'_J = \cup_{-i\in J} C_i$, where D'_J is defined in (3.1). In order to use Theorem 3.2 to obtain m-ovoids in $\mathrm{W}(2r-1, p^e)$, we need D_J to be self-dual. To avoid possible overlap with the m-ovoids obtained by the field reduction method, we further assume that r is odd.

Lemma 3.3. *With notation as above, D_J is self-dual if and only if J is σ-invariant, where $\sigma : i \mapsto -1 - i \pmod N$.*

Proof. We have $L(C_i) = \gamma^{\frac{\sqrt{q}+1}{2}+\sqrt{q}i} C_0$, i.e., L maps C_i to $C_{\tau(i)}$, where $\tau(i) := \frac{\sqrt{q}+1}{2} + \sqrt{q}i \pmod N$. Note that $\sqrt{q} \equiv 1 \pmod N$, and $\frac{\sqrt{q}-1}{2} = \frac{(p^{\ell t}-1)}{(p^{2\ell}-1)} \cdot \frac{(p^\ell-1)}{2} \cdot N \equiv 0 \pmod N$ since t is even by assumption. Therefore $\tau(i) \equiv i+1 \pmod N$. The partial difference set D_J is self-dual if and only if $L(D_J) = D'_J$ which in turn is equivalent to $\{i+1 \pmod N : i \in J\} = \{-i \pmod N : i \in J\}$, i.e., $-J - 1 = J$. The proof of the lemma is complete. □

Lemma 3.4. *With notation as above, D_J is $\mathbb{F}_{p^e}^*$-invariant if and only if J is invariant under the map $\rho : i \mapsto i + 2d_0 \pmod N$, where d_0 is an odd integer defined by*

$$d_0 := \gcd\left(\frac{N}{2}, \frac{\sqrt{q}-1}{p^e-1}\right). \tag{3.3}$$

Proof. Note that $\mathbb{F}_{p^e}^* = \langle \gamma^{(q-1)/(p^e-1)} \rangle$. So D_J is $\mathbb{F}_{p^e}^*$-invariant if and only if J is invariant under the map $i \mapsto i + \frac{q-1}{p^e-1} \pmod N$. We have $\sqrt{q}+1 \equiv 2 \pmod N$ by the assumption that t is even. It follows that $\gcd(N, \frac{q-1}{p^e-1}) = \gcd(N, \frac{2(\sqrt{q}-1)}{p^e-1}) = 2d_0$ with d_0 as defined in (3.3). The conclusion of the lemma follows. □

Theorem 3.5. *Let p be an odd prime, and $q = p^s$ with $s = 2er = 2\ell t$ for some positive integers e, r, ℓ, t, where r is odd and t is even. Set $N = p^\ell + 1$, and let d_0 be defined as in (3.3). If $d_0 > 1$, then there exists a $\frac{b(\sqrt{q}-1)}{d_0(p^e-1)}$-ovoid in $\mathrm{W}(2r-1, p^e)$ for each integer $1 \le b \le d_0 - 1$.*

Proof. We continue with the above notation. By Lemma 3.3 and Lemma 3.4, the set D_J is $\mathbb{F}_{p^e}^*$-invariant and satisfies $L(D_J) = D'_J$ if and only if J is invariant under the map $\rho : i \mapsto i + 2d_0 \pmod N$ and $\sigma : i \mapsto -1 - i \pmod N$. We claim that $\langle \rho, \sigma \rangle = \{1, \rho, \rho^2, ..., \rho^{\frac{N}{2d_0}-1}, \sigma, \rho\sigma, \rho^2\sigma, ..., \rho^{\frac{N}{2d_0}-1}\sigma\}$ by the fact that $\langle \rho, \sigma \rangle$ is a dihedral group $D_{\frac{N}{d_0}}$, cf. [18, 2.24]. Thus each $\langle \rho, \sigma \rangle$-orbit $\mathcal{O}$ on $\mathbb{Z}_N$ has equal length $\frac{N}{d_0}$, and the corresponding union $D_{\mathcal{O}} = \cup_{i \in \mathcal{O}} C_i$ of cyclotomic classes has size $|C_0| \cdot \frac{N}{d_0} = \frac{q-1}{d_0}$. This number is divisible by $(\sqrt{q}+1)(p^e-1)$, since d_0 divides $\frac{\sqrt{q}-1}{p^e-1}$ by (3.3). Therefore, $D_{\mathcal{O}}$ is an m-ovoid in $\mathrm{W}(2r-1, p^e)$ with $m = \frac{\sqrt{q}-1}{d_0(p^e-1)}$. By taking a union of b many $D_{\mathcal{O}}$'s, we get bm-ovoids in $\mathrm{W}(2r-1, p^e)$ for $1 \le b \le d_0 - 1$. □

Remark 3.6. The m-ovoids in $W(2r-1, p^e)$ arising from Theorem 3.5 have the following automorphisms: $g_1 : x \mapsto \eta x$, where $\eta \in \mathbb{F}_q^*$ has multiplicative order $\frac{(\sqrt{q}+1)(p^e-1)}{2}$, and $g_2 : x \mapsto x^{\sqrt{q}}$; together they generate a metacyclic group. This metacyclic group is also an automorphism group of the associated strongly regular Cayley graph $\mathrm{Cay}(\mathbb{F}_q, D_{\mathcal{O}})$. It is an interesting problem to completely determine the full automorphism group of the m-ovoids in Theorem 3.5 and further explore the connection between the automorphism groups of the m-ovoids we have constructed and those of the associated strongly regular Cayley graphs.

For the following discussion, we choose r to be an odd prime p_0, and give explicit conditions that guarantee $d_0 > 1$, where d_0 is defined in (3.3). This excludes the possibility that the resulting m-ovoids from Theorem 3.5 come from field reduction. Recall that $s = 2ep_0 = 2\ell t$ with t even. We consider two cases.

(A) First consider the case where $p_0 \mid t$. Write $t = p_0 t_0$. So t_0 is even and $e = \ell t_0$, and

$$\frac{\sqrt{q}-1}{p^e-1} = \sum_{i=0}^{p_0-1} p^{ie} = \sum_{i=0}^{p_0-1} p^{i\ell t_0} \equiv p_0 \pmod{p^\ell + 1}.$$

Therefore, $d_0 = \gcd(N/2, p_0) = \gcd(N, p_0)$. In this case, $d_0 > 1$ if and only if $p_0 \mid (p^\ell + 1)$, which in turn is equivalent to $d_0 = p_0$. In Table 1, we give some examples of m-ovoids constructed by using Theorem 3.5 in this case.

(B) Next consider the case where p_0 does not divide t. In this case, from $p_0 e = \ell t$, we deduce that $p_0 \mid \ell$. Write $\ell = \ell_0 p_0$. Then $e = \ell_0 t$. We claim that $d_0 = \gcd(N/2, \frac{\sqrt{q}-1}{p^e-1})$ is always greater than 1. We have $\sqrt{q} - 1 = p^{\ell t} - 1 \equiv (-1)^t - 1 = 0 \pmod N$ by the fact t is even, so $N/2$ divides $\sqrt{q} - 1$. On the other hand, $\gcd(p^e - 1, N/2)$ divides $\gcd(p^e - 1, p^{2\ell} - 1) = p^{\gcd(e, 2\ell)} - 1 = p^{2\ell_0} - 1$ by the fact $p_0 \nmid t$. Since

Table 1
m-ovoids constructed from Theorem 3.5 in the case $r = p_0$ odd prime, $p_0 \mid t$.

p_0	p	ℓ	t	d_0	$W(2p_0-1, p^e)$	m
3	p odd	1	$6k$, $k \in \mathbb{Z}^+$	3	$W(5, p^{2k})$	$\frac{b}{3}(p^{4k}+p^{2k}+1)$, $b \in \{1,2\}$
5	3	2	$10k$, $k \in \mathbb{Z}^+$	5	$W(9, 3^{4k})$	$\frac{b(3^{20k}-1)}{5(3^{4k}-1)}$, $1 \le b \le 4$
5	7	2	$10k$, $k \in \mathbb{Z}^+$	5	$W(9, 7^{4k})$	$\frac{b(7^{20k-1})}{5(7^{4k}-1)}$, $1 \le b \le 4$
5	13	2	$10k$, $k \in \mathbb{Z}^+$	5	$W(9, 13^{4k})$	$\frac{b(13^{20k}-1)}{5(13^{4k}-1)}$, $1 \le b \le 4$
5	17	2	$10k$, $k \in \mathbb{Z}^+$	5	$W(9, 17^{4k})$	$\frac{b(17^{20k}-1)}{5(17^{4k}-1)}$, $1 \le b \le 4$
5	19	1	$10k$, $k \in \mathbb{Z}^+$	5	$W(9, 19^{2k})$	$\frac{b(19^{10k}-1)}{5(19^{2k}-1)}$, $1 \le b \le 4$
7	3	3	$14k$, $k \in \mathbb{Z}^+$	7	$W(13, 3^{6k})$	$\frac{b(3^{42k}-1)}{7(3^{6k}-1)}$, $1 \le b \le 6$
7	5	3	$14k$, $k \in \mathbb{Z}^+$	7	$W(13, 5^{6k})$	$\frac{b(5^{42k}-1)}{7(5^{6k}-1)}$, $1 \le b \le 6$
7	13	3	$14k$, $k \in \mathbb{Z}^+$	7	$W(13, 13^{6k})$	$\frac{b(13^{42k}-1)}{7(13^{6k}-1)}$, $1 \le b \le 6$
11	7	5	$22k$, $k \in \mathbb{Z}^+$	11	$W(21, 7^{10k})$	$\frac{b(7^{110k}-1)}{11(7^{10k}-1)}$, $1 \le b \le 10$
11	13	5	$22k$, $k \in \mathbb{Z}^+$	11	$W(21, 13^{10k})$	$\frac{b(13^{110k}-1)}{11(13^{10k}-1)}$, $1 \le b \le 10$
11	17	5	$22k$, $k \in \mathbb{Z}^+$	11	$W(21, 17^{10k})$	$\frac{b(17^{110k}-1)}{11(17^{10k}-1)}$, $1 \le b \le 10$
11	19	5	$22k$, $k \in \mathbb{Z}^+$	11	$W(21, 19^{10k})$	$\frac{b(19^{110k}-1)}{11(19^{10k}-1)}$, $1 \le b \le 10$
13	5	2	$26k$, $k \in \mathbb{Z}^+$	13	$W(25, 5^{4k})$	$\frac{b(5^{52k}-1)}{13(5^{4k}-1)}$, $1 \le b \le 12$
13	7	6	$26k$, $k \in \mathbb{Z}^+$	13	$W(25, 7^{12k})$	$\frac{b(5^{156k}-1)}{13(5^{12k}-1)}$, $1 \le b \le 12$

Table 2
m-ovoids constructed from Theorem 3.5 in the case $r = p_0$ odd prime, $p_0 \nmid t$.

p_0	p	ℓ	t	d_0	$W(2p_0-1, p^e)$	m
3	3	3	$2k$, $3 \nmid k$	7	$W(5, 3^{2k})$	$\frac{b(3^{6k}-1)}{7(3^{2k}-1)}$, $1 \le b \le 6$
3	5	3	$2k$, $3 \nmid k$	21	$W(5, 5^{2k})$	$\frac{b(5^{6k}-1)}{21(5^{2k}-1)}$, $1 \le b \le 20$
3	7	3	$2k$, $3 \nmid k$	43	$W(5, 7^{2k})$	$\frac{b(7^{6k}-1)}{43(7^{2k}-1)}$, $1 \le b \le 42$
5	3	5	$2k$, $5 \nmid k$	61	$W(9, 3^{2k})$	$\frac{b(3^{10k}-1)}{61(3^{2k}-1)}$, $1 \le b \le 60$
5	5	5	$2k$, $5 \nmid k$	521	$W(9, 5^{2k})$	$\frac{b(5^{10k}-1)}{521(5^{2k}-1)}$, $1 \le b \le 520$
7	3	7	$2k$, $7 \nmid k$	547	$W(13, 3^{2k})$	$\frac{b(3^{14k}-1)}{547(3^{2k}-1)}$, $1 \le b \le 546$
7	5	7	$2k$, $7 \nmid k$	13021	$W(13, 5^{2k})$	$\frac{b(5^{14k}-1)}{13021(5^{2k}-1)}$, $1 \le b \le 13020$
11	3	11	$2k$, $11 \nmid k$	44287	$W(21, 3^{2k})$	$\frac{b(3^{22k}-1)}{44287(3^{2k}-1)}$, $1 \le b \le 44286$

$p^{2\ell_0} - 1 < N/2 = (p^{\ell_0 p_0}+1)/2$, we see that $N/2$ does not divide $p^e - 1$. We conclude that $d_0 > 1$. In Table 2, we give some examples of m-ovoids constructed by using Theorem 3.5 in this case.

It was conjectured in [1] that if an m-ovoid exists in $\mathrm{W}(2r-1, p^e)$ with $r > 2$, then $m \ge cp^{e(r-2)}$ for some positive constant $c > 0$. From Theorem 3.5, we know that there exist m-ovoids in $\mathrm{W}(2r-1, p^e)$ with $m = \frac{b(\sqrt{q}-1)}{d_0(p^e-1)}$ if $d_0 > 1$. We compute

$$\frac{m}{p^{e(r-2)}} = \frac{b(\sqrt{q}-1)}{d_0(p^e-1)p^{e(r-2)}} = \frac{b(p^{er}-1)}{d_0(p^{e(r-1)}-p^{e(r-2)})}$$

In the following we show that the aforementioned conjecture is false.

Example 3.7. In Case (B), when $p = 3, r = p_0 = 5, t = 2$, we have $d_0 = \gcd(\frac{3^{5\ell_0}+1}{2}, \frac{3^{10\ell_0}-1}{3^{2\ell_0}-1})$. It follows that $\frac{3^{5\ell_0}+1}{3^{\ell_0}+1} \mid d_0$; thus $\frac{m}{p^{e(p_0-2)}} \leq \frac{b(3^{4\ell_0}+3^{3\ell_0}+3^{2\ell_0}+3^{\ell_0}+1)}{3^{6\ell_0}}$, for some fixed b, and $\lim_{\ell_0\to\infty} \frac{m}{p^{e(p_0-2)}} = 0$.

Example 3.8. In Case (B), when $p = 5, r = p_0 = 7, t = 2$, we have $d_0 = \gcd(\frac{5^{7\ell_0}+1}{2}, \frac{5^{14\ell_0}-1}{5^{2\ell_0}-1})$. It follows that $\frac{5^{7\ell_0}+1}{5^{\ell_0}+1} \mid d_0$; thus $\frac{m}{p^{e(p_0-2)}} \leq \frac{b(5^{7\ell_0}-1)}{(5^{\ell_0}-1)5^{10\ell_0}}$, for some fixed b, and $\lim_{\ell_0\to\infty} \frac{m}{p^{e(p_0-2)}} = 0$.

Example 3.9. In Case (B), when $p = 5, r = p_0 = 11, t = 2$, we have $d_0 = \gcd(\frac{5^{11\ell_0}+1}{2}, \frac{5^{22\ell_0}-1}{5^{2\ell_0}-1})$. It follows that $\frac{5^{11\ell_0}+1}{5^{\ell_0}+1} \mid d_0$; thus $\frac{m}{p^{e(p_0-2)}} \leq \frac{b(5^{11\ell_0}-1)}{(5^{\ell_0}-1)5^{18\ell_0}}$, for some fixed b, and $\lim_{\ell_0\to\infty} \frac{m}{p^{e(p_0-2)}} = 0$.

4. Conclusion

In this paper, we develop a new method for constructing m-ovoids in finite symplectic spaces. We use some "special" strongly regular Cayley graphs $\mathrm{Cay}(\mathbb{F}_q, D)$ from uniform cyclotomy in [6] and equip the ambient finite field $\mathbb{F}_q$ with a non-degenerate alternating form f so that the connection set D gives rise to an m-ovoid in the symplectic space $(\mathbb{F}_q, f)$. In this way we are able to obtain m-ovoids in high rank symplectic spaces which do not come from field reduction. We remark that there have been extensive efforts in the constructions of strongly regular Cayley graphs from cyclotomy in recent years, cf. [12,15,11,16], and it will be of interest to examine whether new m-ovoids can arise from Theorem 3.2.

We mention in passing that we only considered constructing m-ovoids in symplectic spaces from strongly regular graphs of negative Latin square type, but did not discuss similar constructions of i-tight sets in symplectic spaces from strongly regular graphs of Latin square type. The reason is as follows: each component of a spread of $\mathrm{W}(2r-1, p^e)$ is a 1-tight set, thus there exist i-tight sets for all i in $\mathrm{W}(2r-1, p^e)$.

The results in this paper show that there are many more m-ovoids in finite symplectic spaces than previously thought. Still it remains an interesting problem to determine for which values of m there exists an m-ovoid in $\mathrm{W}(2r-1, p^e)$.

Acknowledgments

The research of Tao Feng and Ye Wang is supported by the National Natural Science Foundation of China grant 11771392, and the research of Qing Xiang is supported by an NSF grant DMS 1855723. The authors would like to thank the anonymous reviewers for their detailed comments and suggestions.

References

[1] J. Bamberg, Finite Geometries Fifth Irsee Conference, http://cage.ugent.be/~ml/irsee5/slides/Bamberg.pdf, 2017.

[2] J. Bamberg, S. Kelly, M. Law, T. Penttila, Tight sets and m-ovoids of finite polar spaces, J. Comb. Theory, Ser. A 114 (7) (2007) 1293–1314.

[3] J. Bamberg, M. Lee, K. Melissa, Q. Xiang, A new infinite family of hemisystems of the Hermitian surface, Combinatorica 38 (1) (2018) 43–66.

[4] J. Bamberg, M. Law, T. Penttila, Tight sets and m-ovoids of generalised quadranles, Combinatorica 29 (1) (2009) 1–17.

[5] A.E. Brouwer, W.H. Haemers, Spectra of Graphs, Universitext, Springer, New York, 2012.

[6] A.E. Brouwer, R.M. Wilson, Q. Xiang, Cyclotomy and strongly regular graphs, J. Algebraic Comb. 10 (1) (1999) 25–28.

[7] A. Cossidente, C. Culbert, G.L. Ebert, G. Marino, On m-ovoids of $W_3(q)$, Finite Fields Appl. 14 (1) (2008) 76–84.

[8] R. Calderbank, W.M. Kantor, The geometry of two-weight codes, Bull. Lond. Math. Soc. 18 (2) (1986) 97–122.

[9] A. Cossidente, F. Pavese, Intriguing sets of $W(5, q)$, q even, J. Comb. Theory, Ser. A 127 (2014) 303–313.

[10] A. Cossidente, F. Pavese, On intriguing sets of finite symplectic spaces, Des. Codes Cryptogr. 86 (5) (2018) 1161–1174.

[11] T. Feng, K. Momihara, Q. Xiang, Constructions of strongly regular Cayley graphs and skew Hadamard difference sets from cyclotomic classes, Combinatorica 35 (4) (2015) 413–434.

[12] T. Feng, Q. Xiang, Strongly regular graphs from unions of cyclotomic classes, J. Comb. Theory, Ser. B 102 (4) (2012) 982–995.

[13] C. Godsil, G. Royle, Algebraic Graph Theory, Graduate Texts in Mathematics, Springer-Verlag, New York, 2001.

[14] S. Kelly, Constructions of intriguing sets of polar spaces from field reduction and derivation, Des. Codes Cryptogr. 43 (1) (2007) 1–8.

[15] K. Momihara, Certain strongly regular Cayley graphs on $\mathbb{F}_{2^{2(2s+1)}}$ from cyclotomy, Finite Fields Appl. 25 (2014) 280–292.

[16] K. Momihara, Q. Xiang, Strongly regular Cayley graphs from partitions of subdifference sets of the Singer difference sets, Finite Fields Appl. 50 (2018) 222–250.

[17] S.E. Payne, J.A. Thas, Finite Generalized Quadrangles, Research Notes in Mathematics, vol. 110, Pitman, 1984.

[18] J.S. Rose, A Course on Group Theory, Cambridge University Press, Cambridge-New York-Melbourne, 1978.

[19] E.E. Shult, J.A. Thas, m-systems of polar space, J. Comb. Theory, Ser. A 68 (1) (1994) 184–204.

[20] J.A. Thas, Ovoids and spreads of finite classical polar spaces, Geom. Dedic. 10 (1981) 135–143.

[21] J.A. Thas, Interesting pointsets in generalized quadrangles and partial geometries, Linear Algebra Appl. 114/115 (1989) 103–131.