Generalised Veroneseans

A. Klein, J. Schillewaert and L. Storme

October 8, 2011

Abstract

In [8], a characterization of the finite quadric Veronesean $\mathcal{V}_n^{2^n}$ by means of properties of the set of its tangent spaces is proved. These tangent spaces form a *regular generalised dual arc*. We prove an extension result for regular generalised dual arcs. To motivate our research, we show how they are used to construct a large class of secret sharing schemes.

1 Introduction

A typical problem in (finite) geometry is the study of highly symmetrical substructures. For example, arcs are configurations of points in $\mathrm{PG}(n,q)$ such that each $n+1$ of them are in general position, while n_1-dimensional dual arcs are sets of n_1-spaces such that each two intersect in a point and any three of them are skew. These two structures appear naturally in cryptographical applications.

In this article, we define objects, called (generalised) dual arcs; a class of objects that contain classical arcs and d-dimensional dual arcs as special cases. These (generalised) dual arcs have applications in cryptography as well.

We give a construction method for a wide class of parameters and show, under certain restrictions, that for this class of parameters, the construction is unique.

In Section 2, we give the necessary definitions, constructions, and examples of applications in cryptography. Section 4 refers to known classification results, and Section 5 states our main characterization theorem (Theorem 13). We now start with the required definitions to make this article self-contained.

2 Definitions and constructions

Definition 1
A generalised dual arc $\mathcal{F}$ *of order* d *with dimensions* $n = n_0 > n_1 > n_2 > \cdots > n_{d+1} > -1$ *of* $PG(n,q)$ *is a set of* n_1*-dimensional subspaces of* $PG(n,q)$ *such that:*

1. *each* j *of these subspaces intersect in a subspace of dimension* n_j, $1 \leq j \leq d+1$,

2. *each $d+2$ of these subspaces have no common intersection.*

We call $(n = n_0, n_1, \ldots, n_{d+1})$ the parameters *of the generalised dual arc.*

Definition 2
A generalised dual arc of order d with parameters $(n = n_0, \ldots, n_{d+1})$ is regular *if, in addition, the n_1-dimensional spaces span $PG(n, q)$ and if it satisfies the property that if π is the intersection of j elements of $\mathcal{F}$, $j \leq d$, then π is spanned by the subspaces of dimension n_{j+1} which are the intersections of π with the remaining elements of $\mathcal{F}$.*

Construction 1
Let $PG(V)$ be an n-dimensional space with basis e_i $(0 \leq i \leq n)$.

Let $PG(W)$ be an $\left(\binom{n+d+1}{d+1} - 1\right)$-dimensional space with basis $e_{i_0,\ldots,i_d}$ $(0 \leq i_0 \leq i_1 \leq \cdots \leq i_d \leq n)$.

We now define a multilinear mapping from $PG(V)$ to $PG(W)$. In the description of this multilinear mapping and in the remainder of this article, the vector $e_{i_0,\ldots,i_d}$, for $0 \leq i_0, i_1, \ldots, i_d \leq n$, is identical to the vector $e_{i_{\sigma(0)},\ldots,i_{\sigma(d)}}$, where σ is a permutation of $\{0, \ldots, d\}$ with $0 \leq i_{\sigma(0)} \leq \cdots \leq i_{\sigma(d)} \leq n$. For example, $e_{001}, e_{010}, e_{001}$ all denote the same vector e_{001}.

Let $\theta : V^{d+1} \to W$ be the multilinear mapping

$$\theta : (\sum_{i_0=0}^{n} x_{i_0}^{(0)} e_{i_0}, \ldots, \sum_{i_d=0}^{n} x_{i_d}^{(d)} e_{i_d}) \mapsto \sum_{0 \leq i_0,\ldots,i_d \leq n} x_{i_0}^{(0)} \cdot \ldots \cdot x_{i_d}^{(d)} e_{i_0,\ldots,i_d} \ . \qquad (1)$$

For example, $\theta(x_0^{(0)} e_0 + x_1^{(0)} e_1, x_0^{(1)} e_0 + x_1^{(1)} e_1) = x_0^{(0)} x_0^{(1)} e_{0,0} + (x_0^{(0)} x_1^{(1)} + x_1^{(0)} x_0^{(1)}) e_{0,1} + x_1^{(0)} x_1^{(1)} e_{1,1}$.

For each point $P = [x]$ of $PG(V)$, we define a subspace $D(P)$ of $PG(W)$ by

$$D(P) = \langle \theta(x, v_1, \ldots, v_d) \mid v_1, \ldots, v_d \in V \rangle \ . \qquad (2)$$

.

Theorem 3 ([5])
The set $\mathcal{D} = \{D(P) \mid P \in PG(V)\}$ is a generalised dual arc with dimensions $d_i = \binom{n+d+1-i}{d+1-i} - 1, i = 0, \ldots, d+1$.

For q odd and $\frac{q^n-1}{q-1} \geq \binom{n+d}{d+1}$, there is an alternative construction.

Construction 2
We define $\zeta : PG(V) \to PG(W)$ by

$$\zeta : [\sum_{i=0}^{n} x_i e_i] \mapsto [\sum_{0 \leq i_0 \leq \cdots \leq i_d \leq n} x_{i_0} \cdots x_{i_d} e_{i_0,\ldots,i_d}].$$

This mapping ζ is a generalisation of the well-known quadratic Veronesean map (see [3]). We call it the generalised Veronesean.

With b and B respectively, we denote the standard scalar product of V and W, i.e.,

$$b(\sum_{i=0}^{n} x_i e_i, \sum_{i=0}^{n} y_i e_i) = \sum_{i=0}^{n} x_i y_i,$$

and

$$B(\sum_{0\le i_0\le\cdots\le i_d\le n} x_{i_0,\ldots,i_d} e_{i_0,\ldots,i_d}, \sum_{0\le i_0\le\cdots\le i_d\le n} y_{i_0,\ldots,i_d} e_{i_0,\ldots,i_d}) = \sum_{0\le i_0\le\cdots\le i_d\le n} x_{i_0,\ldots,i_d} y_{i_0,\ldots,i_d}.$$

For each $x \in V$, we denote by $x^\perp$ the subspace of V perpendicular to x with respect to b. So

$$x^\perp = \{y \in V \mid b(x, y) = 0\}.$$

Then

$$D(P) = \{[z] \in PG(W) \mid B(z, \zeta(y)) = 0 \text{ for all } y \in x^\perp\} \tag{3}$$

is a generalised dual arc.

We will not use Construction 2 in this article. Hence, we refer to [5] for a proof that Construction 2 gives generalised dual arcs isomorphic to the ones described by Construction 1.

For the second construction, we call the arcs of form $\mathcal{D} = \{D(P)|P \in PG(V)\}$ *Veronesean dual arcs.*

Below, we give two examples of our general construction.

Example 1
Starting with $PG(2, q)$, the mapping $\zeta : PG(2, q) \to PG(5, q)$ with

$$\zeta([x_0, x_1, x_2]) = [x_0^2, x_1^2, x_2^2, x_0x_1, x_0x_2, x_1x_2]$$

defines the quadratic Veronesean $\mathcal{V}_2^4$.

If $P = [a, b, c]$, the planes $D(P)$ defined above have the equation

$$D(P) = \{[ax_0, bx_1, cx_2, ax_1 + bx_0, ax_2 + cx_0, bx_2 + cx_1] \mid x_0, x_1, x_2 \in \mathbb{F}_q\} .$$

These planes form a regular generalised dual arc of $q^2 + q + 1$ planes with parameters $(5, 2, 0)$.

Example 2
The map $\zeta : PG(2, q) \to PG(9, q)$ with

$$\zeta([x_0, x_1, x_2]) = [x_0^3, x_1^3, x_2^3, x_0^2x_1, x_0^2x_2, x_1^2x_0, x_1^2x_2, x_2^2x_0, x_2^2x_1, x_0x_1x_2]$$

defines a cubic Veronesean. Construction 1 associates to each of the $q^2 + q + 1$ points a 5-dimensional space in $PG(9, q)$. Each two of these 5-spaces intersect in a plane. Each three 5-spaces share a common point and each four 5-spaces are skew.

Three of the q^2+q+1 5-spaces are:

$$\pi_0 := D([1,0,0]) = \{[e_0,0,0,e_1,e_2,e_3,0,e_4,0,e_5] \mid e_i \in \mathbb{F}_q\},$$
$$\pi_1 := D([0,1,0]) = \{[0,e_0,0,e_1,0,e_2,e_3,0,e_4,e_5] \mid e_i \in \mathbb{F}_q\},$$
$$\pi_2 := D([0,0,1]) = \{[0,0,e_0,0,e_1,0,e_2,e_3,e_4,e_5] \mid e_i \in \mathbb{F}_q\}.$$

In each 5-space, the other q^2+q 5-spaces intersect in a configuration of q^2+q planes. These planes are a part of the Veronesean described in Example 1.

For π_0, the corresponding Veronesean has the form

$$\mathcal{V}_0 := [x_0^2,0,0,x_0x_1,x_0x_2,x_1^2,0,x_2^2,0,x_1x_2].$$

This Veronesean $\mathcal{V}_0$ has q^2+q+1 tangent planes; where q^2+q of the tangent planes are intersections of π_0 with the other 5-spaces. The extra plane has the form

$$E_0 := \{[e_0,0,0,e_1,e_2,0,0,0,0,0] \mid e_0,e_1,e_2 \in \mathbb{F}_q\}\ .$$

Similarly, we see in π_1 the Veronesean

$$\mathcal{V}_1 := [0,x_1^2,0,x_0^2,0,x_0x_1,x_1x_2,0,x_2^2,x_0x_2]$$

and the extra plane

$$E_1 := \{[0,e_0,0,0,0,e_1,e_2,0,0,0] \mid e_0,e_1,e_2 \in \mathbb{F}_q\},$$

and in π_2, we have the Veronesean

$$\mathcal{V}_2 := [0,0,x_2^2,0,x_0^2,0,x_1^2,x_0x_2,x_1x_2,x_0x_1]$$

and the extra plane

$$E_2 := \{[0,0,e_0,0,0,0,0,e_1,e_2,0] \mid e_0,e_1,e_2 \in \mathbb{F}_q\}\ .$$

Generalised dual arcs can be used to construct message authentication codes [5]. Below we give another application, namely secret sharing schemes.

3 Secret sharing

Now we will investigate applications of generalised dual arcs in secret sharing schemes. For an overview of secret sharing and the links with geometry we refer to [4]. A recent overview of different adversary models in secret sharing can be found in [6].

We only consider a particular class of secret sharing schemes here, which is defined below.

Definition 4
In a k-out-of-n secret sharing scheme a dealer *generates* n *shares* $s_1, \ldots, s_n$ *and a secret* s*. The shares are given to different* participants*. Each* k *participants can reconstruct the secret with their shares.*

Less than k *participants cannot reconstruct the share. By* p_i *we denote the probability that* $i < k$ *participants may guess that share correctly. The probabilities* p_i *are called the* attack probabilities*. If* $p_{i+1}/p_i > 1$ *the system* leaks *information about the share.*

Actually, we don't apply generalised dual arcs directly. But the dual of these structures, which we call *generalised arcs*.

Definition 5
A generalised arc $\mathcal{A}$ *of order* d *with dimensions* $n_1 < n_2 < \cdots < n_{d+1}$ *of* $PG(n, q)$ *is a set of* n_1*-dimensional subspaces of* $PG(n, q)$ *such that:*

1. *each* j *of these subspaces generate a subspace of dimension* n_j*,* $1 \leq j \leq d + 1$*,*
2. *each* $d + 2$ *of these subspaces span* $PG(n, q)$*.*

We call $(n, n_1, \ldots, n_{d+1})$ *the* parameters *of the arc.*

If in addition the common intersection of all n_{j+1}*-dimensional subspaces spanned by* $j+1$ *elements of the arc containing a given* n_j*-dimensional subspace* π *spanned by* j *elements of the arc is* π*, we call the arc* regular*.*

Theorem 6
The dual of an arc with parameters $(n, n_1, \ldots, n_{d+1})$ *is a dual arc with parameters* $(n, n - 1 - n_1, \ldots, n - 1 - n_{d+1})$ *and vice versa.*

Furthermore, the dual arc is regular if and only if the arc is regular.

Proof. Dualising in $PG(n, q)$ maps every k-dimensional subspace onto an $(n - 1 - k)$-dimensional subspace. Dualising exchanges the concepts "span" and "intersection". □

Dual to Construction 1, we have the following construction of generalised arcs.

Construction 3
As in Construction 1, let $PG(V)$ *be an* n*-dimensional space with basis* e_i *(*$0 \leq i \leq n$*).*

Let $PG(W)$ *be a* $\left(\binom{n+d+1}{d+1} - 1\right)$*-dimensional space with basis* $e_{i_0,\ldots,i_d}$ *(*$0 \leq i_0 \leq i_1 \leq \cdots \leq i_d \leq n$*).*

We define $\zeta : PG(V) \to PG(W)$ *by*

$$\zeta : [\sum_{i=0}^{n} x_i e_i] \mapsto [\sum_{0 \leq i_0 \leq \cdots \leq i_d \leq n} x_{i_0} \cdot \ldots \cdot x_{i_d} e_{i_0,\ldots,i_d}] \ .$$

With b and B respectively, we denote the standard scalar product of V and W, i.e.,

$$b(\sum_{i=0}^{n} x_i e_i, \sum_{i=0}^{n} y_i e_i) = \sum_{i=0}^{n} x_i y_i,$$

and

$$B(\sum_{0\le i_0\le\cdots\le i_d\le n} x_{i_0,\ldots,i_d} e_{i_0,\ldots,i_d}, \sum_{0\le i_0\le\cdots\le i_d\le n} y_{i_0,\ldots,i_d} e_{i_0,\ldots,i_d}) = \sum_{0\le i_0\le\cdots\le i_d\le n} x_{i_0,\ldots,i_d} y_{i_0,\ldots,i_d}.$$

For each $x \in V$, we denote by $x^\perp$ the subspace of V perpendicular to x with respect to b. So

$$x^\perp = \{y \in V \mid b(x, y) = 0\}.$$

For each point $P = [x]$ of $PG(V)$, we define a subspace $A(P)$ of $PG(W)$ by

$$A(P) = \left\langle \zeta(y) \mid y \in x^\perp \right\rangle. \tag{4}$$

Theorem 7
The set $\mathcal{A} = \{A(P) \mid P \in PG(n, q)\}$, defined in Construction 3, is a generalised arc with parameters $n_i = \binom{n+d+1}{d+1} - \binom{n+d+1-i}{d+1-i} - 1$, $i = 1, \ldots, d+1$.
The generalised dual arc described in Construction 1 is the dual of that arc.

Proof. By Definition (check Equation (3)), we have $D(P) = A(P)^\perp$ with respect to the bilinear form B. Since B is a non-degenerate form, this means that $D(P)$ is dual to $A(P)$. Thus we may apply Theorem 6, which together with Theorem 3 shows that $\mathcal{A}$ is indeed an arc. □

Before we describe the construction of a secret sharing scheme in general, we give two examples that use the dual arc with parameters $(9, 5, 2, 0)$ we have seen in Example 2.

Example 3
The dual of the dual arc with parameters $(9, 5, 2, 0)$ is an arc consisting of $q^2 + q + 1$ different 3-dimensional spaces in $PG(9, q)$, with the following properties:

1. *Each two 3-dimensional spaces generate a 6-space.*
2. *Each three 3-dimensional spaces generate an 8-space.*
3. *Each four 3-dimensional spaces generate $PG(9, q)$.*

Now take the space $PG(10, q)$. Select any hyperplane as the secret. In that hyperplane select the above configuration of $q^2 + q + 1$ 3-dimensional spaces as shares.

If the attacker does not have a share, he has a probability of $\frac{q-1}{q^{11}-1}$ to guess the secret 9-space.

If the attacker knows only one share, he has to guess a 9-space through the known 3-dimensional space, so he has a probability of $\frac{q-1}{q^7-1}$ to guess the secret.

Similarly, an attacker that knows 2 or 3 shares has a probability of $\frac{q-1}{q^4-1}$ *or* $\frac{q-1}{q^2-1} = \frac{1}{q+1}$ *to guess the share.*

Any 4 shares reconstruct the secret.

Example 4

As in the previous example, we select a hyperplane Π *in* $PG(10, q)$ *and an arc consisting of* $q^2 + q + 1$ *3-dimensional spaces with the same properties as above. One of these 3-dimensional spaces* π *will be the secret. The other 3-dimensional spaces are the shares.*

Furthermore, we select a 4-dimensional space Π_4 *through* π *not contained in* Π *and make it public. If an attacker wants to find the secret space, he has to reconstruct* Π *and then the secret space is the intersection* $\Pi \cap \Pi_4$*. A short calculation shows that an attacker who knows* i $(i \leq 4)$ *shares has a probability of* $\frac{q-1}{q^{5-i}-1}$ *to guess the secret.*

Another way to vary the attack probabilities is the following. Recall that the $q^2 + q + 1$ *different 5-spaces of the dual arc are of the form* $D(P)$ *where* P *is a point of a 2-dimensional space* $PG(2, q)$*. The* $q + 1$ *different 5-spaces that correspond to the* $q + 1$ *points of a line of* $PG(2, q)$ *lie in a common 8-space. In the dual setting, this means that the* $q + 1$ *corresponding 3-dimensional spaces intersect in a common point.*

So if we fix one such 3-dimensional space π*, it has* $q+1$ *different intersection points with the other* $q^2 + q$ *3-spaces. Suppose* π *is the image of the point* $P_0 = [1, 0, 0]$*. Furthermore, let* $P_1 = [0, 1, 0]$ *and* $P_2 = [0, 0, 1]$*. Consider lines of the form* $\langle P_0, aP_1+P_2\rangle$ *and* $\langle P_0, P_1\rangle$*. Then they define* $q+1$ *different intersection points forming the twisted cubic arc consisting of the points* $P_a = [1, a, a^2, a^3]$ $(a \in \mathbb{F}_q)$ *and* $P_\infty = [0, 0, 0, 1]$*. Choose a plane in* π *which contains no intersection point. This is possible, since* $\mathbb{F}_q[X]$ *contains an irreducible polynomial of degree* 3*.*

Now we select this plane as the secret. We select a 3-dimensional space Π_3 *through this plane not contained in* Π *and make this public. An attacker who knows* i $(i < 4)$ *shares has attack probabilities* $p_0 = p_1 = \frac{1}{q^3+q^2+q+1}$*,* $p_2 = \frac{1}{q^2+q+1}$ *and* $p_3 = \frac{1}{q+1}$ *to guess the secret. Thus the new scheme leaks no information if only one share is known.*

By selecting the correct subspace of π*, we can also construct schemes that have no information leak for 2 or 3 shares. Then we must select a line or a point inside* π *as the secret and take a plane* Π_2 *or line* Π_1 *through the selected line or point not in* Π*, and make this public.*

Now we give two theorems which use generalised arcs to construct secret sharing schemes.

Theorem 8

In $PG(n+1, q)$*, select an* n*-dimensional subspace* Π *as the secret. In* Π*, select a generalised arc* $\mathcal{A}$ *of order* $k-2$ *with* n *elements and parameters* $(n, d_1, \ldots, d_{k-1})$*. The elements of* $\mathcal{A}$ *are the shares.*

This describes a k-out-of-n secret sharing scheme with the attack probabilities

$$p_i = \frac{q-1}{q^{n+1-d_i}-1}$$

for $0 \le i < k$ (formally, we set $d_0 = -1$).

Proof. Every k shares span Π, since $\mathcal{A}$ is a generalised arc of order $k-2$.

Less than k participants can take their shares $\pi_1, \ldots, \pi_i$ and compute the d_i-dimensional space $\langle \pi_1, \ldots, \pi_i \rangle$. They know that Π must contain that space. But for every n-dimensional space Π' containing $\langle \pi_1, \ldots, \pi_i \rangle$, there exists an arc which has $\pi_1, \ldots, \pi_i$ as elements. Thus the best attack is to guess an n-dimensional space through $\langle \pi_1, \ldots, \pi_i \rangle$. The number of such spaces is $\frac{q^{n+1-d_i}-1}{q-1}$. □

Theorem 9
In $PG(n+1,q)$, select a (d_1+1)-dimensional subspace π' and make it public. In π', select a d_1-dimensional subspace π as the secret. Choose any hyperplane Π of $PG(n+1,q)$ that contains π but not π'. Let $\mathcal{A}$ be a generalised dual arc of Π of order $k-2$ with $n+1$ elements and parameters $(n, d_1, \ldots, d_{k-1})$. The subspace π should be an element of $\mathcal{A}$. The n elements of $\mathcal{A}$ different from π are the shares.

This describes a k-out-of-n secret sharing scheme with the attack probabilities

$$p_i = \frac{q-1}{q^{d_{i+1}-d_i+1}-1}$$

for $0 \le i < k-1$ (formally, we set $d_0 = -1$ and $d_k = n$).

Proof. Every k shares span Π, since $\mathcal{A}$ is a generalised arc of order $k-2$. Thus k participants can compute $\Pi \cap \pi'$ which is the secret π.

Less than k participants can take their shares $\pi_1, \ldots, \pi_i$ and compute the d_i-dimensional space $\langle \pi_1, \ldots, \pi_i \rangle$. Since the secret π is also an element of the arc $\mathcal{A}$, we find that $\langle \pi_1, \ldots, \pi_i, \pi \rangle$ has dimension d_{i+1}. This means that

$$\dim(\langle \pi_1, \ldots, \pi_i \rangle \cap \pi) = d_i + d_1 - d_{i+1} \ .$$

Since by construction $\pi' \cap \Pi = \pi$, we also have

$$\dim(\langle \pi_1, \ldots, \pi_i \rangle \cap \pi') = d_i + d_1 - d_{i+1} \ .$$

The i participants know that π is a d_1-dimensional subspace of π' containing the $(d_i + d_1 - d_{i+1})$-dimensional subspace $\langle \pi_1, \ldots, \pi_i \rangle \cap \pi'$. But for every d_1-dimensional subspace $\bar{\pi}$ through $\langle \pi_1, \ldots, \pi_i \rangle \cap \pi'$ in π', there exists a generalised arc containing $\pi_1, \ldots, \pi_i$ and $\bar{\pi}$. So the i participants have no further information and must guess a d_1-dimensional subspace of π' through $\langle \pi_1, \ldots, \pi_i \rangle \cap \pi'$. The probability for guessing this correctly is

$$p_i = \frac{q-1}{q^{d_{i+1}-d_i+1}-1} \ .$$

□

4 Known results

In 1947, Bose studied ovals in [1]. In that paper, he proved that an oval in $PG(2,q)$ has at most $q+1$ points if q is odd and at most $q+2$ points if q is even.

Special cases of generalised dual arcs have a long history. A generalised dual arc of order 0 is just a (partial) spread of $PG(n,q)$. The generalised dual arc of order $n-1$ in $PG(n,q)$ with parameters $(n, n-1, \ldots, 1, 0)$ is just the dual of an ordinary arc of points in $PG(n,q)$.

Generalised dual arcs of order 1 with $n_2 = 0$ are known as n_1-dimensional dual arcs. It is known that the dimension n of the ambient space $PG(n,q)$ of an n_1-dimensional dual arc satisfies $2n_1 \leq n \leq \frac{1}{2}n_1(n_1+3)$ (see [9]).

Definition 10
A family $\mathcal{A}$ of $\frac{q^{l+1}-1}{q-1}+1$ l-dimensional subspaces of $PG(n,q)$ with $n \geq 2$ is called an l-dimensional dual hyperoval if it satisfies the following three axioms:

- *Every two elements of $\mathcal{A}$ intersect in a point.*
- *Every three elements of $\mathcal{A}$ have no point in their intersection.*
- *All members of $\mathcal{A}$ span the whole space $PG(n,q)$.*

The next theorem is the translation to Veronesean dual arcs of the well-known fact that ovals in $PG(2,q)$, q odd, are maximal, but ovals in $PG(2,q)$, q even, can be extended to hyperovals (see also [9]).

Theorem 11
For q odd, the Veronesean dual arc is maximal while for q even, the Veronesean dual arc can be extended by an n_1-dimensional space to an n_1-dimensional dual hyperoval. The extension element is called the nucleus.

Proof. In every arc element $\Omega = D([x_0, \ldots, x_{n_1}])$, there is only one point not covered by a second arc element. This point is

$$\zeta([x_0, \ldots, x_{n_1}]) = (x_0^2, \ldots, x_{n_1}^2, 2x_0x_1, \ldots, 2x_{n_1-1}x_{n_1}),$$

where ζ is the Veronesean map.

For odd q, these points $\zeta([x_0, \ldots, x_{n_1}])$ span $PG(\frac{1}{2}n_1(n_1+3), q)$, i.e. the Veronesean dual arc is not extendable. For q even, they form an n_1-dimensional space which extends the Veronesean dual arc. This space is called the nucleus. □

In 1958, Tallini [7] (see also [3]) showed that every 2-dimensional dual arc of q^2+q+1 elements in $PG(5,q)$, q odd, must be isomorphic to the dual arc defined by Construction 1. This result was generalised in [8] to the following characterization of the finite quadric Veronesean $\mathcal{V}_n^{2^n}$.

Result 12
Let $\mathcal{F}$ be a set of $\frac{q^{n+1}-1}{q-1}$ n-dimensional spaces in $PG(\frac{n(n+3)}{2}, q)$ with the following properties:

(VS1) Each two elements of $\mathcal{F}$ intersect in a point.

(VS2) Each three elements of $\mathcal{F}$ are skew.

(VS3) The elements of $\mathcal{F}$ span $PG(\frac{n(n+3)}{2}, q)$.

(VS4) Any proper subspace of $PG(\frac{n(n+3)}{2}, q)$ that is spanned by a collection of elements of $\mathcal{F}$ is a subspace of dimension $\frac{i(2n-i+3)}{2} - 1$, for some $i \in \{0, \ldots, n\}$.

(VS5) If q is even, at least one space spanned by two elements of $\mathcal{F}$ contains more than two elements of $\mathcal{F}$.

Then either $\mathcal{F}$ is a Veronesean dual arc with respect to a quadric Veronesean $\mathcal{V}_n^{2^n}$ or q is even and there are two members $\Omega_1, \Omega_2 \in \mathcal{F}$ such that the $2n$-dimensional space $\langle \Omega_1, \Omega_2 \rangle$ only contains 2 elements of $\mathcal{F}$ and there is a unique subspace Ω of dimension n such that $\{\Omega\} \cup \mathcal{F}$ is a Veronesean dual arc with the nucleus space as constructed in Theorem 11. In particular, if $n = 2$, then the statement holds under the weaker hypotheses of $\mathcal{F}$ satisfying $(VS1)$, $(VS2)$, $(VS3)$ and $(VS5)$.

For order $d = 1$ and q even, there are non-Veronesean dual arcs with the property that every space spanned by two elements of $\mathcal{F}$ contains exactly these two elements of $\mathcal{F}$. For $n = 2$, one can classify all examples that do not satisfy $(VS5)$ by a result of [2]; the only possibilities are for $q = 2$ and $q = 4$. This classification remains open for $n \geq 3$, although an infinite class of examples is known, described in [8].

5 The case $d = 1$

We prove that for $\delta > 0$, δ small, a dual arc with parameters (n_0, n_1, n_2) of size $\frac{q^{n+1}-1}{q-1} - \delta$ is not maximal. The proof techniques are similar to the techniques used in [3] to give an algebraic characterisation of a dual arc of size $\frac{q^{n+1}-1}{q-1}$. The main difference is that the deficiency δ makes simple counting arguments impossible, so we have to use more difficult structural arguments.

Theorem 13
Assume that $\delta \leq \frac{q-7}{2}$ for q odd and $\delta \leq \frac{q-8}{2}$ for q even, and let $\mathcal{F}$ be a set of $\frac{q^{n+1}-1}{q-1} - \delta$ different n-dimensional spaces in $PG(\frac{n(n+3)}{2}, q)$ with the following properties:

(1) Each two elements of $\mathcal{F}$ intersect in a point.

(2) Each three elements of $\mathcal{F}$ are skew.

(3) The elements of $\mathcal{F}$ span $PG(\frac{n(n+3)}{2}, q)$.

(4) Any proper subspace of $PG(\frac{n(n+3)}{2}, q)$ that is spanned by a collection of elements of $\mathcal{F}$ is a subspace of dimension $\frac{i(2n-i+3)}{2} - 1$, for some $i \in \{0, \ldots, n\}$.

(5) If q is even, at least one space spanned by two elements of $\mathcal{F}$ contains more than two elements of $\mathcal{F}$.

Then $\mathcal{F}$ is extendable to a regular generalised dual arc of size $\frac{q^{n+1}-1}{q-1}$. (In the case q even, this dual arc of size $\frac{q^{n+1}-1}{q-1}$ is even extendable to a dual hyperoval.)

The idea of the proof is in the same spirit as the proof of Result 12, so the proofs of some results describing the general structure will look very similar as the ones used for that result. The main work lies in the lemmata which actually deal with the deficiency itself, where we have to reconstruct the missing elements.

Definition 14
A contact point *is a point belonging to at most one element of $\mathcal{F}$.*

Property (4) seems very technical. Our next lemma shows that for large q, property (4) is no restriction. This motivates property (4).

Lemma 15
Let $q \geq n$, then any configuration $\mathcal{F}$ which satisfies the properties (1)-(3) also satisfies property (4).

Proof. Assume that the claim of the lemma is wrong, i.e. there exists a sequence $\pi_0, \ldots, \pi_k$ of elements in $\mathcal{F}$ with the property:

- $\Pi_j = \langle \pi_0, \ldots, \pi_j \rangle$, for $j \leq k$,
- $\dim \Pi_j = \frac{(j+1)(2n-j+2)}{2} - 1$, for $j < k$,
- $\frac{k(2n-k+3)}{2} - 1 < \dim \Pi_k < \frac{(k+1)(2n-k+2)}{2} - 1$.

By induction, we will construct a sequence $\pi_{k+1}, \ldots, \pi_{n+1}$ of members of $\mathcal{F}$ with the properties:

(I) the subspace defined recursively by $\Pi_i = \langle \Pi_{i-1}, \pi_i \rangle$ has at least an i-dimensional subspace in common with π_{i+1},

(II) the space π_{i+1} is not contained in Π_i.

For $i = n$, these two conditions yield a contradiction, because the elements of $\mathcal{F}$ have dimension n. This proves the lemma.

Now we construct π_{j+1} from the sequence $\pi_0, \ldots, \pi_j$. Note that $\dim \Pi_j$ is bounded by

$$\dim \Pi_k + (n-k) + \cdots + (n-(j-1)) \leq$$
$$\frac{(k+1)(2n-k+2)}{2} - 2 + \frac{(j-k)(2n-k-j+1)}{2} \leq \frac{n(n+3)}{2} - 1 \ .$$

Thus Π_j is not the whole space. By property (3), we know that there exists a space $\bar{\pi}_{j+1}$ of $\mathcal{F}$ not in Π_j. There are at least $q^n - 1 - \delta$ elements of $\mathcal{F}$ meeting $\bar{\pi}_{j+1}$ in a point outside of Π_j. Thus there are at least $q^n - \delta$ elements of $\mathcal{F}$ not in Π_j. Since π_{i+1} has at most an $(n-1)$-dimensional space in common with Π_i $(i < k)$, we conclude that at most $\frac{q^n-1}{q-1}$ elements of $\mathcal{F}$ intersect π_{i+1} in a point of Π_i. Thus for at most $j\frac{q^n-1}{q-1}$ elements of $\mathcal{F}$, there exists an $i < j$ such that this element intersects π_{i+1} in a point of Π_i. Because $k \leq n \leq q$,

$$q^n - \delta - k\frac{q^n-1}{q-1} > 0,$$

implying that there is an element π_{j+1} of $\mathcal{F}$ with the property that π_{j+1} is not in Π_j and $\pi_{j+1} \cap \pi_{i+1} \notin \Pi_i$. Especially, we have $\dim \langle \pi_{j+1} \cap \pi_{i+1} \mid -1 \leq i < j \rangle = j$, i.e. $\pi_{j+1} \cap \Pi_j$ is at least a j-dimensional space.

Thus, by induction, we have found the members of $\mathcal{F}$ with the properties (I) and (II), which proves the lemma. □

Property (4) allows us to compute the dimensions of many objects related to $\mathcal{F}$. An important special case is the following result.

Remark. Let Π be a $2n$-dimensional space spanned by two elements of $\mathcal{F}$. Then an element of $\mathcal{F}$ either lies inside Π or intersects Π in a line.

The next lemma gives us an upper bound on the number of elements of $\mathcal{F}$ contained in a space having one of the dimensions mentioned in property (4).

Lemma 16
Every $\left(\frac{i(2n-i+3)}{2} - 1\right)$*-dimensional space contains at most* $\frac{q^i-1}{q-1}$ *elements of* $\mathcal{F}$.

Proof. Let Π be an $\left(\frac{i(2n-i+3)}{2} - 1\right)$-dimensional space spanned by i elements $\pi_1, \ldots, \pi_i$ of $\mathcal{F}$.

An element of $\mathcal{F}$, not contained in Π, intersects Π in an $(i-1)$-dimensional space Π_i (this is part of property (4)). Each element of $\mathcal{F}$, contained in Π, must share a point with Π_i. Furthermore, no two elements of $\mathcal{F}$ in Π intersect Π_i in the same point, so Π contains at most $\frac{q^i-1}{q-1}$ elements of $\mathcal{F}$. □

To understand the goal of the next lemma, consider the dual arc obtained by Construction 1. In this example, every element of $\mathcal{F}$ corresponds to a point of a projective space $PG(n,q)$. The $2n$-dimensional spaces spanned by two elements of $\mathcal{F}$ correspond to the lines of $PG(n,q)$. Thus if a dual arc with $\frac{q^{n+1}-1}{q-1} - \delta$

elements is a subset of this example, then the following is true:

Every $2n$-dimensional space spanned by two elements of $\mathcal{F}$ contains at least $q+1-\delta$ elements of $\mathcal{F}$.

Lemma 17 is the first step in that direction.

Lemma 17
Every $2n$-dimensional space contains 0, 1, 2 or at least $q-\delta$ ($\delta \leq (q-7)/2$ for q odd and $\delta \leq (q-8)/2$ for q even) elements of $\mathcal{F}$.

If q is odd, no $2n$-dimensional space contains exactly 2 elements of $\mathcal{F}$.

Proof. Let Π be a $2n$-dimensional space which contains k elements of $\mathcal{F}$, where $2 \leq k < q-\delta$.

Let π' be any element of $\mathcal{F}$ not contained in Π. This element π' intersects Π in a line l' by the remark after Lemma 15. At least $q-\delta$ points of l' must be covered by a second element of $\mathcal{F}$. Since $q-\delta-k>0$, there must be a second element π'' of $\mathcal{F}$, not contained in Π, which intersects l'. Let $\pi'' \cap \Pi = l''$.

The lines l' and l'' span a plane π. Since every one of the k elements of $\mathcal{F}$ in Π must intersect π' and π'', these k elements intersect π' and π'' in a point on l', respectively on l'', different from $l' \cap l''$. Hence, they intersect π in lines.

Assume that π''' is another element of $\mathcal{F}$, not contained in Π, that intersects Π in l'''. We prove that if l''' has a point in common with l', then it has also a point in common with l''.

Suppose that l''' intersects l'. If l''' does not intersect l'', then every element of $\mathcal{F}$ contained in Π must share a line with the plane spanned by l' and l'', and has a point in common with l'''. Thus these elements share a plane with the 3-dimensional space spanned by l', l'' and l'''. Especially, two of these elements intersect each other in a line, a contradiction.

This proves that the elements of $\mathcal{F}$, not contained in Π, can be partitioned into *groups*. The elements from one group intersect each other in Π, and elements from different groups intersect each other outside of Π. Each group defines a plane inside Π and the k elements of $\mathcal{F}$ contained in Π must intersect such a plane in lines.

Let π_1 and π_2 be two planes inside Π defined by such groups. We distinguish several cases for the intersection $\pi_1 \cap \pi_2$.

(1) The planes π_1 and π_2 cannot be skew to each other. Otherwise, they would span a 5-dimensional space Ω. Now every element of $\mathcal{F}$ in Π shares a line with π_1 and π_2, so shares at least a 3-dimensional space with Ω, but then the elements of $\mathcal{F}$ in Π intersect each other in at least a line, which is false.

(2) If π_1 and π_2 intersect in a line, then at most one element of $\mathcal{F}$ contained in Π contains the line $\pi_1 \cap \pi_2$. So at least $k-1$ elements of $\mathcal{F}$ contained in Π must share a plane with the 3-dimensional space spanned by π_1 and π_2. Thus each two of these elements must share a line, a contradiction for $k>2$. We now eliminate the case $k=2$, where one of the two elements of $\mathcal{F}$ in Π, for instance π, passes through the line $\ell = \pi_1 \cap \pi_2$.

For $k = 2$, all groups have size at least $q-\delta-1$. For, consider a first element π' of $\mathcal{F}$ not in Π, then consider the line $\ell' = \pi' \cap \Pi$. This line has at most $\delta+1$ contact points, so it is intersected in a point by at least $q-2-\delta$ elements of $\mathcal{F}$, not lying in Π. This shows that a group of elements of $\mathcal{F}$, not lying in Π, has at least size $q-\delta-1$.

But now consider the line $\ell = \pi_1 \cap \pi_2$, lying in an element π of $\mathcal{F}$ in Π, and in the two planes π_1 and π_2 containing at least $q-\delta-1$ lines lying in elements of $\mathcal{F}$, not contained in Π. Since no point of ℓ lies in three elements of $\mathcal{F}$, and every point of ℓ already lies in the element π of $\mathcal{F}$, we must have $q+1 \geq 2(q-\delta-1)+1$, where the $+1$ arises from the second element of $\mathcal{F}$ in Π. This implies $q \leq 2\delta+2$, a contradiction.

(3) Thus π_1 and π_2 intersect in a point Q. But then the only possibility for an element of $\mathcal{F}$ contained in Π to intersect π_1 and π_2 in lines is that Q is a point of that element. Thus all elements of $\mathcal{F}$ contained in Π contain Q. Since every three elements of $\mathcal{F}$ are skew, this means that $k = 2$.

Assume now that we are in the case $k = 2$ and q is odd. Since there are $\frac{q^{n+1}-1}{q-1} - 2 - \delta$ elements of $\mathcal{F}$ not contained in Π, and since for odd q a dual arc of lines in $PG(2,q)$ contains at most $q+1$ elements, each group can contain at most $q-1$ elements, so there are at least

$$\frac{1}{q-1}\left(\frac{q^{n+1}-1}{q-1} - 2 - \delta\right) > \frac{q^n-1}{q-1}$$

different groups.

Each group defines a plane through Q which intersects an element of $\mathcal{F}$ contained in Π in a line. Since an n-dimensional space only contains $\frac{q^n-1}{q-1}$ different lines through Q, there must exist two groups which define planes π_1 and π_2 intersecting in a line. But this is impossible as we already proved.

So the case $k = 2$ is only possible for q even. □

Even if we could not exclude the case $k = 2$ for q even, we have proven in step (3) the following characterisation:

Corollary 18
Let q be even and let $\langle \pi, \pi' \rangle$ be a $2n$-space that contains only π and π' as elements of $\mathcal{F}$. Then the elements of $\mathcal{F} \backslash \{\pi, \pi'\}$ intersect $\langle \pi, \pi' \rangle$ in groups of pairwise intersecting lines. Furthermore, there can be at most $\frac{q^n-1}{q-1}$ such groups.

We call a $2n$-dimensional space *big* if it contains at least $q-\delta$ elements of $\mathcal{F}$. The next lemma associates with each big $2n$-dimensional space Π a plane $\bar{\pi}$ which will be very important in the remaining part of this section.

Lemma 19
Let Π be a $2n$-dimensional space containing $q+1-\delta_i \geq q-\delta$ elements of $\mathcal{F}$. Then Π contains a plane $\bar{\pi}$ which intersects the $q+1-\delta_i$ elements of $\mathcal{F}$ in Π in lines. The elements of $\mathcal{F}$, not in Π, intersect Π in a line. These lines either lie in $\bar{\pi}$, or they are skew to $\bar{\pi}$ and then contain δ_i contact points. Moreover, those

latter lines skew to $\bar{\pi}$ which are the intersection of Π with an element of $\mathcal{F}$ not lying in Π are pairwise disjoint.

Proof. Assume that two elements $\tilde{\pi}_1$ and $\tilde{\pi}_2$ of $\mathcal{F}$, not in Π, intersect Π in two intersecting lines ℓ_1 and ℓ_2. Let $\bar{\pi}$ be the plane spanned by ℓ_1 and ℓ_2.

We are not in the case which is assumed in the beginning of the proof of Lemma 17. However, the same kind of arguments as the ones used in the proof of Lemma 17 show that

1. Every line in Π that intersects $\bar{\pi}$ and that comes from an element of $\mathcal{F}$ not in Π must lie in $\bar{\pi}$.

2. Every element of $\mathcal{F}$ in Π must intersect $\bar{\pi}$ in a line.

3. The lines in Π that come from an element of $\mathcal{F}$ not in Π and that do not lie in $\bar{\pi}$ must be pairwise disjoint.

Property 3 is proven in the following way. Otherwise we have two planes $\bar{\pi}_1$ and $\bar{\pi}_2$ corresponding with two different groups of lines as in the proof of Lemma 17. We have shown in the proof of Lemma 17 that $\bar{\pi}_1$ and $\bar{\pi}_2$ must intersect in a point Q which lies on every element of $\mathcal{F}$ in Π. But this implies that Π has only 2 elements of $\mathcal{F}$ which is not the case.

So, from now on, we may assume that all the elements of $\mathcal{F}$, not in Π, intersect Π in pairwise disjoint lines. Now we construct the plane $\bar{\pi}$.

Let π_1, π_2 and π_3 be three elements of $\mathcal{F}$ in Π. Let $Q_{12} = \pi_1 \cap \pi_2$, $Q_{13} = \pi_1 \cap \pi_3$ and $Q_{23} = \pi_2 \cap \pi_3$.

The points Q_{12}, Q_{13}, Q_{23} generate a plane $\bar{\pi}$, since otherwise, π_1, π_2, π_3 share a line. Assume that an element of $\mathcal{F}$, not in Π, intersects Π in a line ℓ that meets $\bar{\pi}$. We claim that ℓ must lie in $\bar{\pi}$. Suppose the contrary. Without loss of generality, we may assume that $\ell \cap \bar{\pi} \notin \pi_1 \cup \pi_2$. But then π_1 and π_2 share a plane with the 3-dimensional space $\langle \bar{\pi}, \ell \rangle$, i.e. they share a line, a contradiction.

At most one line in Π that comes from an element of $\mathcal{F}$ not in Π lies in $\bar{\pi}$, since these lines are pairwise disjoint. Since every element of $\mathcal{F}$ has only $\delta + 1$ contact points, this proves that at least $q - \delta - 1$ points of $Q_{12}Q_{13}$ lie in an element of $\mathcal{F}$ in Π, different from π_1.

Assume that there exists an element π of $\mathcal{F}$ in Π which intersects π_1 in a point Q not on $Q_{12}Q_{13}$. The above arguments show that $Q_{12}Q_{13}$, QQ_{12} and QQ_{13} must contain at least $3(q - \delta - 1) - 3 > q + 1$ points in π_1 which lie on two elements of $\mathcal{F}$ inside Π, a contradiction with Lemma 16.

Thus every element π of $\mathcal{F}$ in Π meets $Q_{12}Q_{13}$, $Q_{12}Q_{23}$ and $Q_{13}Q_{23}$, i.e. it has a line in common with $\bar{\pi}$. □

The next series of lemmas deal with the case q even and $k = 2$. Let us again have a look at the example that comes from Construction 1. In this example, every $2n$-dimensional space containing at least one element of $\mathcal{F}$ contains either 1 or $q + 1$ elements of $\mathcal{F}$. If q is even, we can extend the dual arc of size $\frac{q^{n+1}-1}{q-1}$ by one element π. This element π has the special property that for all other

elements $\pi' \in \mathcal{F}$, the $2n$-space $\langle \pi, \pi' \rangle$ contains no other element of $\mathcal{F}$, see [8]. We call this element the *nucleus* of $\mathcal{F}$.

We will prove in Lemma 22 that this property holds for every regular generalised dual arc for q even.

Lemma 20
Let q be even and let $\pi, \pi' \in \mathcal{F}$ be such that the $2n$-dimensional space $\langle \pi, \pi' \rangle$ contains no other element of $\mathcal{F}$. Let $Q = \pi \cap \pi'$.

Let Π be a big $2n$-dimensional space containing π and let $\bar{\pi}$ be the plane inside Π described by Lemma 19. Then $Q \in \bar{\pi}$.

Proof. Let $\Pi = \langle \pi, \pi'' \rangle$, $\pi'' \in \mathcal{F} \backslash \{\pi, \pi'\}$. Let $\bar{\pi}' = \langle Q = \pi \cap \pi', \pi'' \cap \pi, \pi'' \cap \pi' \rangle$. As we have already seen in Corollary 18, this gives us a group of intersecting lines in this plane. But Lemma 19 states that the only plane in Π which contains a group of intersecting lines is $\bar{\pi}$, i.e. $\bar{\pi} = \bar{\pi}'$. $\square$.

Lemma 21
Let q be even. For each $\pi \in \mathcal{F}$ either all $2n$-dimensional spaces $\langle \pi, \pi' \rangle$ with $\pi \neq \pi' \in \mathcal{F}$ contain exactly two elements of $\mathcal{F}$, or there exists at most one element $\pi \neq \pi' \in \mathcal{F}$ such that $\langle \pi, \pi' \rangle$ contains exactly two elements of $\mathcal{F}$.

Proof. Assume that π lies in a big $2n$-dimensional space Π, and let $\bar{\pi}$ be the plane described by Lemma 19 and let ℓ be the line $\bar{\pi} \cap \pi$. By Lemma 20, we know that an element π' of $\mathcal{F}$ for which $\langle \pi, \pi' \rangle$ contains no other element of $\mathcal{F}$ must intersect π in a point of ℓ.

Since ℓ has only $q+1$ points and $|\mathcal{F}| = \frac{q^{n+1}-1}{q-1} - \delta$, this means that π must lie in more than one big $2n$-space Π'. But then we have a second line $\ell' = \bar{\pi}' \cap \pi$ and every element π' of $\mathcal{F}$ for which $\langle \pi, \pi' \rangle$ contains no other element of $\mathcal{F}$ must intersect π in a point of $\ell \cap \ell'$. (ℓ and ℓ' are different, since ℓ must meet the $q - \delta$ elements of $\mathcal{F}$ in Π, ℓ' must meet the $q - \delta$ elements of $\mathcal{F}$ in Π' and $2q - 2\delta - 2 > q + 1$, see also step (2) of Lemma 17.) This proves the lemma. $\square$

Lemma 22
Let q be even and assume that there exists a $2n$-dimensional space Π which contains exactly two elements of $\mathcal{F}$. Then there exists one element $\pi \in \mathcal{F}$ such that for every $\pi \neq \pi' \in \mathcal{F}$, the $2n$-space $\langle \pi, \pi' \rangle$ contains exactly two elements of $\mathcal{F}$.

Proof. Let $\Pi = \langle \pi, \pi' \rangle$. Assume that both elements π and π' lie in a big $2n$-dimensional space. Then all other elements of $\mathcal{F}$ generate with π and π', respectively, a big $2n$-dimensional space (Lemma 21). Let π'' be such an element and $\Pi_0 = \langle \pi, \pi'' \rangle$ with the special plane $\bar{\pi}_0$ and $\Pi_1 = \langle \pi', \pi'' \rangle$ with the special plane $\bar{\pi}_1$. By the proof of Lemma 20, we know that $\bar{\pi}_0 = \langle \pi \cap \pi', \pi \cap \pi'', \pi' \cap \pi'' \rangle = \bar{\pi}_1$.

But this is a contradiction since this plane cannot contain $2(q-\delta)-1 > q+2$ different lines coming from elements of $\mathcal{F}$ in Π_0 and Π_1. Thus either π or π' does not lie in big $2n$-dimensional spaces. They cannot both lie only in $2n$-spaces which contain 2 elements of $\mathcal{F}$ or else by condition (5) of Theorem 13 which

we assume to be valid for $\mathcal{F}$, we find a $\pi'' \in \mathcal{F}\backslash\{\pi, \pi'\}$ lying in at least one big $2n$-space and in two $2n$-spaces with only two elements of $\mathcal{F}$, a contradiction with Lemma 21. □

If q is even and the special element π from Lemma 22 exists, we simply remove it from $\mathcal{F}$. This increases the deficiency by 1.

Remark. Thus from now on, we assume that a $2n$-space cannot contain 2 elements of $\mathcal{F}$ and that $\delta \leq (q-6)/2$ when q is even and $\delta \leq (q-7)/2$ when q is odd.

Our next goal is a stronger version of Lemma 19 which states that an element of $\mathcal{F}$, not in a big $2n$-space Π, must be skew to the plane $\bar{\pi}$. We will reach this goal with Lemma 28.

Lemma 23
Let Π_1, Π_2 and Π_3 be distinct $2n$-dimensional spaces containing at least $q-\delta$ elements of $\mathcal{F}$.
Then $\dim(\Pi_1 \cap \Pi_2 \cap \Pi_3) \leq n$.

Proof. By property (4), we know that $\dim(\Pi_1 \cap \Pi_2) \leq n+1$.

Assume that $\Pi_1 \cap \Pi_2 \cap \Pi_3$ is an $(n+1)$-dimensional space Π. Since two elements of $\mathcal{F}$ span a $2n$-dimensional space, the space Π contains at most one element of $\mathcal{F}$ and the other elements of $\mathcal{F}$ in Π_i intersect Π in a line.

Let ℓ be such a line in Π that comes from an element of $\mathcal{F}$ in Π_1. The elements in Π_2 and Π_3 intersect ℓ in a point. Since $2(q-\delta-1) > q+1$, some point of ℓ lies on an element of $\mathcal{F}$ in Π_1, Π_2 and Π_3. A contradiction since each point lies on at most 2 elements of $\mathcal{F}$. □

In the case of Construction 1, we know that the big $2n$-dimensional spaces correspond to the lines of an n-dimensional projective space $PG(n,q)$. Thus in that case, every element of $\mathcal{F}$ lies in exactly $\frac{q^n-1}{q-1}$ big $2n$-spaces. Now we can prove this for a regular generalised dual arc.

Lemma 24
Let $\pi \in \mathcal{F}$. Consider all $2n$-dimensional spaces through π containing at least $q-\delta$ elements of $\mathcal{F}$. Then the planes $\bar{\pi}$ of these $2n$-spaces intersect π in different lines through a common point.
Moreover, there are exactly $\frac{q^n-1}{q-1}$ different big $2n$-spaces through π.

Proof. Let Π and Π' be two different $2n$-spaces through π, and let $\bar{\pi}$ and $\bar{\pi}'$ be the corresponding planes defined by Lemma 19. By Lemma 19, we know that $\pi \cap \bar{\pi}$ and $\pi \cap \bar{\pi}'$ are lines. These lines must be different since otherwise $\pi \cap \bar{\pi} = \pi \cap \bar{\pi}'$ would contain at least $2(q-\delta-1) > q+1$ points lying on π and on another element of $\mathcal{F}$.

By the proof of Lemma 19, we know that at most $\delta+2$ elements of $\mathcal{F}$ not in Π' intersect Π' in lines contained in $\bar{\pi}'$. The other elements intersect Π' in pairwise skew lines. Thus Π contains at least $q-2\delta-3 \geq 3$ elements of $\mathcal{F}$ that

intersect Π' in pairwise skew lines; we call this set of lines $\mathcal{L}_1$. By symmetry, we know that Π' contains at least $q - 2\delta - 3 \geq 3$ elements of $\mathcal{F}$ that intersect Π in pairwise skew lines; we call this set of lines $\mathcal{L}_2$.

Each line in $\mathcal{L}_1$ must intersect each line of $\mathcal{L}_2$, in the intersection point of the corresponding elements of $\mathcal{F}$. Thus $\mathcal{L}_1$ and $\mathcal{L}_2$ are the lines of two opposite reguli of a hyperbolic quadric $Q^+(3, q)$.

By Lemma 19, we know that every element of $\mathcal{F}$ in Π has a line in common with $\bar{\pi}$. Thus the line $\pi \cap \bar{\pi}$ intersects all lines of $\mathcal{L}_1$, i.e. it lies in the regulus defined by $\mathcal{L}_2$. By symmetry, $\pi \cap \bar{\pi}'$ lies in the regulus defined by $\mathcal{L}_1$. Thus $\pi \cap \bar{\pi}$ and $\pi \cap \bar{\pi}'$ intersect. In addition we see that every element of Π different from π must lie in the regulus defined by $\mathcal{L}_1$, i.e. all elements of Π intersect Π' in pairwise skew lines not in $\bar{\pi}'$. Thus the first case in Lemma 19 cannot occur. Especially the intersection point of $\pi \cap \bar{\pi}$ and $\pi \cap \bar{\pi}'$ must be a contact point, since it can lie only in elements of $\mathcal{F}$ that lie in the intersection $\Pi \cap \Pi'$.

This proves that either the lines of the form $\pi \cap \bar{\pi}$ share a common point or they lie in a common plane since they pairwise share a point. But the lines of the form $\pi \cap \bar{\pi}$ must additionally cover all non-contact points in π and intersect only in contact points. Thus the lines of the form $\pi \cap \bar{\pi}$ share a common contact point and there are at most $\frac{q^n-1}{q-1}$ lines of the form $\pi \cap \bar{\pi}$. That there are at least that many such lines follows from the fact that each big $2n$-space contains at most $q + 1$ elements of $\mathcal{F}$ and hence π is contained in at least $(\frac{q^{n+1}-1}{q-1} - \delta - 1)/q > \frac{q^n-1}{q-1} - 1$ big $2n$-spaces. □

Remark. We note that in this proof, we encounter the strongest condition on δ, namely $q - 2\delta - 3 \geq 3$; equivalently, $\delta \leq (q - 6)/2$ for $d = 1$.

An important consequence of Lemma 24 is the following result.

Corollary 25
Let $\Pi_1, \ldots, \Pi_{\frac{q^n-1}{q-1}}$ be the big $2n$-spaces containing a given element π of $\mathcal{F}$. Let the space Π_i contain $q + 1 - \delta_i$ elements of $\mathcal{F}$. Then $\sum_{i=1}^{\frac{q^n-1}{q-1}} \delta_i = \delta$.

Especially, most big $2n$-dimensional spaces through π contain $q+1$ elements of $\mathcal{F}$. Moreover, each $2n$-space contains at least $q + 1 - \delta$ elements of $\mathcal{F}$.

Proof. We already know that every $2n$-space containing more than two elements of $\mathcal{F}$, contains $q + 1 - \delta_i \geq q - \delta$ elements of $\mathcal{F}$ (Lemma 17).

Since $\sum_{i=1}^{\frac{q^n-1}{q-1}} \delta_i = \delta$, necessarily $\delta_i \leq \delta$, so we can conclude that every $2n$-space containing more than two elements of $\mathcal{F}$, contains $q + 1 - \delta_i \geq q + 1 - \delta$ elements of $\mathcal{F}$. □

The next lemma allows us to reduce the case of an $(\frac{n(n+3)}{2}, n, 0)$-arc to the case of a $(5, 2, 0)$-arc.

Lemma 26
Let $\hat{\Pi}$ be a $(3n - 1)$-space spanned by three elements of $\mathcal{F}$. Let $\hat{\mathcal{F}}$ be the set of elements of $\mathcal{F}$ in $\hat{\Pi}$.

For every π in $\hat{\mathcal{F}}$, define

$$\hat{\pi} := \left\langle \pi \cap \pi' \mid \pi \neq \pi' \in \hat{\mathcal{F}} \right\rangle.$$

For every π in $\hat{\mathcal{F}}$, the space $\hat{\pi}$ is a plane and these planes form a dual arc in 5 dimensions.

Proof. For each element π in $\hat{\mathcal{F}}$, we define a linear space $\mathcal{L}$ with the following properties:

(i) The points of the linear space are the points $\pi \cap \pi'$, with $\pi \neq \pi' \in \hat{\mathcal{F}}$.

(ii) The lines of the linear space are the lines of π through two points of the form $\pi \cap \pi'$ and $\pi \cap \pi''$ ($\pi' \neq \pi, \pi'' \neq \pi \in \hat{\mathcal{F}}$).

If π is not contained in the $2n$-dimensional space Π spanned by π' and π'', then it intersects Π in a line containing $\pi \cap \pi'$ and $\pi \cap \pi''$; in fact, this line contains at least $q - \delta$ elements of the form $\pi \cap \pi'''$, with $\pi''' \neq \pi \in \hat{\mathcal{F}}$ (Lemma 17).

If π is contained in the $2n$-space Π, then $\pi \cap \pi'$ and $\pi \cap \pi''$ lie on the intersection line of π with the plane $\bar{\pi}$ of Π (Lemma 19) which contains at least $q - \delta - 1$ intersection points of π with other planes of $\hat{\mathcal{F}}$.

The number of points in $\mathcal{L}$ is at least $3(q - \delta - 1) - 3$ (Lemma 17) and at most $q^2 + q + 1$ (Lemma 16).

If P_0, P_1 and P_2 are three non-collinear points of the linear space, then P_0P_1 contains at least $q-\delta-1$ intersection points of two elements of $\mathcal{F}$ and thus there are at least $q-\delta-1$ lines through P_2 and therefore at least $(q-\delta-1)(q-\delta-2)+1$ intersection points in the plane $\langle P_0, P_1, P_2 \rangle$.

By the same arguments, four points P_0, P_1, P_2 and P_3 of the linear space $\mathcal{L}$ that do not lie in a plane would imply that the linear space $\mathcal{L}$ contains at least $(q - \delta - 2)[(q - \delta - 1)(q - \delta - 2) + 1] + 1$ points. But this is not possible since the number of points in $\mathcal{L}$ is bounded by $q^2 + q + 1$.

Thus $\hat{\pi} := \left\langle \pi \cap \pi' \mid \pi \neq \pi' \in \hat{\mathcal{F}} \right\rangle$ is a plane.

It remains to be proven that the planes $\hat{\pi}$ span a 5-space. Their span has at most dimension 5 as we know from [9]. Assume that they only span a 4-space. Then the three elements of $\mathcal{F}$ that span $\hat{\Pi}$ would have a plane in common with this 4-dimensional space. This would imply that $\hat{\Pi}$ has at most dimension $4 + 3(n - 2) = 3n - 2$, but this is false. □

Corollary 27
Every big $2n$-space lies in exactly $\frac{q^{n-1}-1}{q-1}$ different $(3n-1)$-spaces spanned by three elements of $\mathcal{F}$.

Proof. Every big $2n$-space Π through π corresponds to a line $\bar{\pi} \cap \pi$ and all these lines go through a common point Q. A $(3n-1)$-space defined by three elements of $\mathcal{F}$ through π corresponds to the lines in one plane through Q inside π by

Lemma 26. Thus the $(3n-1)$-spaces defined by three elements of $\mathcal{F}$ through Π correspond to planes inside π through $\bar{\pi} \cap \pi$. There are exactly $\frac{q^{n-1}-1}{q-1}$ such planes. □

Now we are able to improve the result of Lemma 19.

Lemma 28
With the notations of Lemma 19, the following result holds: No element of $\mathcal{F}$ not in Π intersects $\bar{\pi}$.

Proof. We know from the preceding lemma that $\bar{\pi}$ shares a line with every element π of $\mathcal{F}$ in Π, passing through a fixed contact point of π. Assume that $\bar{\pi}$ contains an extra line from an element π' of $\mathcal{F}$ not contained in Π. Let $\{R\} = \pi \cap \pi' \cap \bar{\pi}$.

The elements π and π' define a big $2n$-dimensional space Π', and Π' contains a plane $\bar{\pi}'$. The intersection $\bar{\pi}' \cap \pi$ is a line which contains R and the fixed contact point. Thus $\pi \cap \bar{\pi}' = \pi \cap \bar{\pi}$, a contradiction.

Thus $\bar{\pi}$ contains no line that comes from an element of $\mathcal{F}$ not in Π. Elements of $\mathcal{F}$ inside Π intersect $\bar{\pi}$ in a dual arc of $q+1-\delta_i$ lines. □

Remark. If $\bar{\pi}$ contains lines of contact points, these lines extend the dual arc of $q+1-\delta_i$ lines induced by the elements of $\mathcal{F}$ in Π. For $\delta_i = 1$ and q odd, we find one line of contact points, and for $\delta_i = 1$ and q even, we find two lines of contact points.

Now we are reaching our final goal to prove that $\mathcal{F}$ is not maximal. As a first step, we prove that the planes $\bar{\pi}$ contain lines of contact points.

Lemma 29
Let Π_1 and Π_2 be two big $2n$-spaces with the property that $\langle \Pi_1, \Pi_2 \rangle$ is a $(3n-1)$-dimensional space. Assume that Π_1 and Π_2 share no element of $\mathcal{F}$. Let $\bar{\pi}_1$ and $\bar{\pi}_2$ be the planes in Π_1 and Π_2 which exist by Lemmas 19 and 28. Then $\bar{\pi}_1 \cap \Pi_2$ is a line of contact points.

Proof. First of all, it is impossible that the plane $\bar{\pi}_1$ is contained in Π_2. For assume the contrary. We obtain a contradiction in the following way. Every element π of $\mathcal{F}$ in Π_1 intersects Π_2 in a line. If $\bar{\pi}_1$ lies completely in Π_2, then the intersection line $\ell = \Pi_2 \cap \pi$ equals the line $\bar{\pi}_1 \cap \pi$. This line contains at least $q - \delta_1$ points lying in two elements of $\mathcal{F}$ in Π_1. But the $q+1-\delta_2$ elements of $\mathcal{F}$ in Π_2 must intersect π in a point. So at least $q+1-\delta_2$ points of ℓ still lie in an element of $\mathcal{F}$ in Π_2. Then there are points of ℓ lying in three elements of $\mathcal{F}$. This is false.

Note that the plane $\bar{\pi}_1$ lies in the 5-space $\hat{\Pi}_1 \subseteq \Pi_1$ spanned by the planes $\hat{\pi}$ defined in Lemma 26. Then Π_2 cannot contain $\hat{\Pi}_1$, since otherwise every element of $\hat{\mathcal{F}}$ would intersect Π_2 at least in a plane, contradicting the remark after Lemma 15. Thus $\Pi_2 \cap \hat{\Pi}_1$ is a 4-dimensional space, spanned by two planes $\hat{\pi}$ and $\hat{\pi}'$ corresponding to elements π and π' of $\mathcal{F}$ in Π_2. The plane $\bar{\pi}_1$ lies in the

5-dimensional space $\hat{\Pi}_1$ and thus it intersects the 4-dimensional space $\Pi_2 \cap \hat{\Pi}_1$, and therefore Π_2, in at least a line.

Consider again the intersection line $\ell = \Pi_2 \cap \pi$ of an element π of $\mathcal{F}$ in Π_1 with Π_2. This line contains $q + 1 - \delta_2$ points lying on an element of $\mathcal{F}$ in Π_2 and δ_2 contact points (Lemma 19 and Lemma 28). So the points of ℓ do not lie in an other element of $\mathcal{F}$ in Π_1.

Now ℓ and $\pi \cap \bar{\pi}_1$ intersect in a point, since both lines lie in the plane $\hat{\pi}$ defined by Lemma 26. This point must be a contact point, for else, it lies in a second plane of $\mathcal{F}$ in Π_1, but this was excluded in the preceding paragraph.

So π shares a contact point with Π_2, which also lies on the intersection line of Π_2 with $\bar{\pi}_1$.

This proves that the line $\bar{\pi}_1 \cap \Pi_2$ intersects the dual arc in $\bar{\pi}_1$, consisting of lines of the form $\bar{\pi}_1 \cap \pi$, where π is an element of $\mathcal{F}$ in Π_1, only in contact points, i.e. $\bar{\pi}_1 \cap \Pi_2$ only contains points covered by at most one element of $\mathcal{F}$.

This proves the theorem. □

Lemma 30
Let Π_1 and Π_2 be two big $2n$-dimensional spaces with the property that $\langle \Pi_1, \Pi_2 \rangle$ is a $(3n-1)$-space. Assume that Π_1 and Π_2 share no element of $\mathcal{F}$ and let $q+1-\delta_1$ be the number of elements of $\mathcal{F}$ in Π_1 and let $q+1-\delta_2$ be the number of elements of $\mathcal{F}$ in Π_2.

Let $\bar{\pi}_1$ and $\bar{\pi}_2$ be the planes in Π_1 and Π_2 which exist by Lemma 19.

Then the lines $\mathcal{L}_1 = \{\bar{\pi}_2 \cap \Pi_1\} \cup \{\pi_1 \cap \Pi_2 \mid \pi_1 \in \mathcal{F}, \pi_1 \subset \Pi_1\}$ and $\mathcal{L}_2 = \{\bar{\pi}_1 \cap \Pi_2\} \cup \{\pi_2 \cap \Pi_1 \mid \pi_2 \in \mathcal{F}, \pi_2 \subset \Pi_2\}$ are lines of two opposite reguli of a hyperbolic quadric $Q^+(3,q)$.

Especially this implies that $\delta_1 > 0$ and $\delta_2 > 0$ since a regulus has only $q+1$ lines, and that $\bar{\pi}_2 \cap \Pi_1$ and $\bar{\pi}_1 \cap \Pi_2$ are concurrent.

Proof. By Lemma 28, we know that the elements of $\mathcal{F}$ in Π_1 intersect Π_2 in pairwise skew lines. Thus $\mathcal{L}'_1 = \{\pi_1 \cap \Pi_2 \mid \pi_1 \in \mathcal{F}, \pi_1 \subset \Pi_1\}$ and $\mathcal{L}'_2 = \{\pi_2 \cap \Pi_1 \mid \pi_2 \in \mathcal{F}, \pi_2 \subset \Pi_2\}$ are sets of pairwise skew lines. Since $\pi_1 \cap \pi_2 \subset \Pi_1 \cap \Pi_2$, every line of $\mathcal{L}'_1$ intersects every line of $\mathcal{L}'_2$.

Since both sets contain more than 2 lines, it follows that the lines of $\mathcal{L}'_1$ and $\mathcal{L}'_2$ are lines of opposite reguli.

Now consider the line $\bar{\pi}_2 \cap \Pi_1$, which exists by Lemma 29. By Lemma 28, the plane $\bar{\pi}_2$ is skew to all elements of $\mathcal{F}$ in Π_1. Thus $\bar{\pi}_2 \cap \Pi_1$ is different from all lines in $\mathcal{L}'_1$. But every element π_2 of $\mathcal{F}$, contained in Π_2, has a line in common with $\bar{\pi}_2$. Thus $\bar{\pi}_2 \cap \Pi_1$ intersects all lines of $\mathcal{L}'_2$. This proves that $\mathcal{L}_1 = \{\bar{\pi}_2 \cap \Pi_1\} \cup \mathcal{L}'_1$ are the lines of a regulus. By symmetry, the same is true for $\mathcal{L}_2$. □

Recall that the final goal is to prove that $\mathcal{F}$ is given by Construction 1. Thus every element of $\mathcal{F}$ should correspond to a point of $PG(n,q)$. Since $\mathcal{F}$ has only $\frac{q^{n+1}-1}{q-1} - \delta$ elements, δ points of $PG(n,q)$ are not used in Construction 1. The next lemma will identify these *holes*.

Consider the linear space $\mathcal{L}$ with the elements of $\mathcal{F}$ as points and the $2n$-spaces generated by two elements of $\mathcal{F}$ as lines. This is a linear space with $\frac{q^{n+1}-1}{q-1} - \delta$ points.

As planes of $\mathcal{L}$, we define the $(3n-1)$-dimensional spaces generated by three elements of $\mathcal{F}$.

Lemma 31
Every plane of $\mathcal{L}$ is a projective plane of order q with possibly some holes.

Proof. Let P be a $(3n-1)$-dimensional space generated by three elements of $\mathcal{F}$.

Let $\Pi \subset P$ be a $2n$-dimensional space that contains $q+1$ elements of $\mathcal{F}$. This $2n$-space Π exists since there are $q+1$ different big $2n$-dimensional spaces through an element π of $\mathcal{F}$ in P and at most δ of them contain less than $q+1$ elements of $\mathcal{F}$ (Corollary 25). Let Π' be an other big $2n$-dimensional space in P. By Lemma 30, we know that Π and Π' share an element of $\mathcal{F}$.

Let Π_1 and Π_2 be two big $2n$-dimensional spaces in P. Let π be an element of $\mathcal{F}$ in Π_1, but not in Π_2. Since Π_2 contains at least $q+1-\delta$ elements of $\mathcal{F}$, there must be at least $q+1-\delta$ big $2n$-dimensional spaces in P through π.

At most δ of the $\frac{q^n-1}{q-1}$ different big $2n$-dimensional spaces through π contain less than $q+1$ elements of $\mathcal{F}$ (Corollary 25). Each of the at least $q+1-\delta$ elements of Π_2 spans together with π a big $2n$-dimensional space in P. Thus there are at least $q+1-2\delta \geq 2$ big $2n$-spaces in P through π which contain exactly $q+1$ elements of $\mathcal{F}$. We denote these $2n$-dimensional spaces by Π_1 and Π_2.

By the same arguments we find an additional $2n$-dimensional space Π_3 which contains $q+1$ elements of $\mathcal{F}$, and which intersects Π_1 and Π_2 in different elements of $\mathcal{F}$.

Thus that plane P of $\mathcal{L}$ contains a triangle Π_1, Π_2, Π_3, and each side of the triangle contains $q+1$ points of $\mathcal{L}$. Every other big $2n$-dimensional space in P intersects Π_1, Π_2 and Π_3 in elements of $\mathcal{F}$ (Lemma 30), thus a direct counting argument shows us that P contains $(q-1)^2 + 3(q-1) + 3 = q^2+q+1$ lines of $\mathcal{L}$, where $(q-1)^2$ is the number of lines intersecting the side of the triangle in different points, $3(q-1)$ is the number of lines through a vertex different from the sides and 3 is the number of sides of the triangle. The number of elements of $\mathcal{F}$ in P is at most q^2+q+1 (by Lemma 16) and at least $q^2+q+1-\delta$ (by Corollary 25).

Now consider any line ℓ of P with $q+1-x$ points ($x \geq 1$). Then $q(q+1-x)$ lines intersect ℓ and thus there are xq lines skew to ℓ. Every point not on ℓ lies on x lines that do not intersect ℓ. Thus there must exist a point not on ℓ that lies on a line ℓ' disjoint to ℓ with at least $\frac{[q^2+q+1-\delta-(q+1-x)]x}{qx} > q-1$ points. By Lemma 30, ℓ' has q points.

As we have seen above, there are q lines of P skew to ℓ' and every point not on ℓ' lies on such a line. We may extend $\mathcal{L}$ by a point that lies on ℓ' and all lines skew to ℓ'. Extending $\mathcal{L}$ stepwise by at most δ points, we obtain a $2-(q^2+q+1, q+1, 1)$ design, i.e. a projective plane of order q. □

Lemma 32
Let $\mathcal{F}$ be a dual arc that satisfies the assumptions of Theorem 13. Let $\delta > 0$, then $\mathcal{F}$ is not maximal.

Proof. Since $\delta > 0$, we find a big $2n$-space which contains less than $q+1$ elements of $\mathcal{F}$ (Corollary 25). Every $(3n-1)$-dimensional space spanned by three elements of $\mathcal{F}$ through such a $2n$-space contains less than q^2+q+1 elements of $\mathcal{F}$. Let P be such a $(3n-1)$-space.

Select a $2n$-space Π in P that contains exactly q elements of $\mathcal{F}$. Such a space exists, because by Lemma 31, the linear space $\mathcal{L}$ is a projective plane with at most δ holes and such linear spaces contain lines with exactly q points.

Consider the $(3n-1)$-spaces through Π generated by three elements of $\mathcal{F}$. By Lemma 31, these $(3n-1)$-spaces define projective planes with holes. We will call a big $2n$-space Π' parallel to Π if it "goes through" the unique hole of Π in the corresponding projective plane defined by Lemma 31.

The $2n$-spaces parallel to Π partition the set $\mathcal{F}$. By Corollary 27, we know that every big $2n$-space lies in $\frac{q^{n-1}-1}{q-1}$ different $(3n-1)$-spaces spanned by three elements of $\mathcal{F}$. Thus there are exactly

$$q\left(\frac{q^{n-1}-1}{q-1}\right)+1=\frac{q^n-1}{q-1}$$

$2n$-spaces parallel to Π, including Π itself.

Consider two big $2n$-spaces Π_1 and Π_2 parallel to Π. If $\Pi_2 \not\subset \langle \Pi, \Pi_1\rangle$, then $\langle \Pi, \Pi_1, \Pi_2\rangle$ is a $(4n-3)$-dimensional space (Property (4)). Since $2n < \dim\langle \Pi_1, \Pi_2\rangle < \dim\langle \Pi, \Pi_1, \Pi_2\rangle = 4n-3$, Property (4) implies that $\dim\langle \Pi_1, \Pi_2\rangle = 3n-1$. Thus any two elements in the parallel class satisfy the conditions of Lemma 29 and Lemma 30, i.e. they lie in a $(3n-1)$-space.

Let q be odd. Choose any $2n$-space Π' parallel to Π which contains exactly q elements of $\mathcal{F}$. By a direct counting argument we find that at least $\frac{q^n-1}{q-1}-(\delta-1)$ of the $\frac{q^n-1}{q-1}$ elements in the parallel class have this property. Then by Lemma 28, the plane $\bar{\pi}'$ of Π' contains exactly one line of contact points. By Lemma 29, these lines must lie in the common intersection Ω of all $2n$-spaces parallel to Π. Thus Ω contains $\frac{q^n-1}{q-1}-(\delta-1)$ lines of contact points that share a common point Q (Lemma 30). This proves that Ω is an n-dimensional space; it cannot be bigger by Lemma 23. Now look at any big $2n$-space Π'' parallel to Π containing $q+1-\delta_i$ elements of $\mathcal{F}$. By Lemma 29 and Lemma 30, the plane $\bar{\pi}''$ must share a line through Q with every other $2n$-space parallel to Π. This line must lie in Ω since otherwise $\bar{\pi}''$ would need different lines for each $2n$-space. Thus Ω contains $\frac{q^n-1}{q-1}$ lines of contact points through Q, i.e., it only contains contact points and we can extend $\mathcal{F}$ by Ω.

For q even, the situation is more complicated. We have always two lines of contact points and we must choose the correct one. Let Π_1 be a $2n$-space which contains exactly q elements of $\mathcal{F}$. By Lemma 29, the plane $\bar{\pi}_1$ of Π_1 must share a line of contact points with each $2n$-space parallel to Π_1. By the pigeon hole principle there are at least $\frac{1}{2}[\frac{q^n-1}{q-1}-\delta]$ different $2n$-spaces parallel to Π_1, which

contain q elements of $\mathcal{F}$ and which intersect $\bar{\pi}_1$ in the same line ℓ_1 of contact points.

Let Π_2 and Π_3 be two such spaces. Choose Π_2 and Π_3 such that $\dim(\Pi_1 \cap \Pi_2 \cap \Pi_3) = n$. For $n = 2$, this is always the case since the intersection of three 4-spaces in a 5-space is at least a plane, and since Lemma 23 states that $\dim(\Pi_1 \cap \Pi_2 \cap \Pi_3) \leq 2$. For $n > 2$, we can choose Π_2 and Π_3 such that $\dim \langle \Pi_1, \Pi_2, \Pi_3 \rangle = 4n - 3$ and then we obtain $\dim(\Pi_1 \cap \Pi_2 \cap \Pi_3) = n$ by the dimension formula.

Let ℓ_2 be the line $\bar{\pi}_2 \cap \Pi_1$. Consider the hyperbolic quadric with the two reguli $\mathcal{L}_1 = \{\bar{\pi}_2 \cap \Pi_1\} \cup \{\pi_1 \cap \Pi_2 \mid \pi_1 \in \mathcal{F}, \pi_1 \subset \Pi_1\}$ and $\mathcal{L}_2 = \{\bar{\pi}_1 \cap \Pi_2\} \cup \{\pi_2 \cap \Pi_1 \mid \pi_2 \in \mathcal{F}, \pi_2 \subset \Pi_2\}$ (see Lemma 30).

Then Π_3 contains the line $\ell_1 = \bar{\pi}_1 \cap \Pi_2$ of this hyperbolic quadric since Π_1 shares the same line of $\bar{\pi}_1$ with Π_2 and Π_3. Hence, Π_3 must contain a second line of this hyperbolic quadric. We prove this as follows. We know that $\dim(\Pi_1 \cap \Pi_2) = n+1$ and that $\dim(\Pi_1 \cap \Pi_2 \cap \Pi_3) = n$. The hyperbolic quadric $\mathcal{L}_1 \cup \mathcal{L}_2$ cannot lie in $\Pi_1 \cap \Pi_2 \cap \Pi_3$, or else every space $\pi_1 \in \mathcal{F}$ of Π_1 shares the same line with Π_2 and Π_3. Then some points of this line necessarily lie on three elements of $\mathcal{F}$ (false). So $\Pi_1 \cap \Pi_2 \cap \Pi_3$ intersects the solid containing the hyperbolic quadric $\mathcal{L}_1 \cup \mathcal{L}_2$ in a plane. This plane contains already one line ℓ_1 of this hyperbolic quadric $\mathcal{L}_1 \cup \mathcal{L}_2$, so it contains a second line of $\mathcal{L}_1 \cup \mathcal{L}_2$.

But for each $\pi_1 \in \Pi_1$, we find that the line $\pi_1 \cap \Pi_2$ cannot lie in Π_3 since otherwise $\pi_1 \cap \Pi_2$ would meet q elements of $\mathcal{F}$ in Π_2 and q elements of $\mathcal{F}$ in Π_3, a contradiction. Thus $\ell_2 = \bar{\pi}_2 \cap \Pi_1$ must be the second line of the hyperbolic quadric in Π_3.

By symmetry, we also find that $\bar{\pi}_3$ intersects Π_1 and Π_2 in the same line.

Applying this argument for all the $\frac{1}{2}[\frac{q^n-1}{q-1} - \delta] + 1$ different parallel spaces found in the first step, we obtain a space Ω in the common intersection which contains $\frac{1}{2}[\frac{q^n-1}{q-1} - \delta] + 1$ different lines of contact points. This proves that Ω must have dimension n and we can copy the final steps of the case q odd to prove that Ω contains only contact points. □

Concluding arguments. Applying Lemma 32 precisely δ times, we find that $\mathcal{F}$ can be extended to a dual arc $\mathcal{F}'$ of size $\frac{q^{n+1}-1}{q-1}$. Even in the case q even, no $2n$-dimensional space contains exactly 2 elements of $\mathcal{F}'$. By Result 12, this implies that $\mathcal{F}'$ is the dual arc given by Construction 1. As we know from Theorem 11, in the case q even this dual arc can be extended by one extra element.

Acknowledgements The authors would profoundly like to thank W. M. Kantor and E. E. Shult for their helpful comments on an earlier version of this paper. The research of the first and the second author took place within the project "Linear codes and cryptography" of the Fund for Scientific Research Flanders (FWO-Vlaanderen) (Project nr. G.0317.06), and the research of the three authors is supported by the Interuniversitary Attraction Poles Programme-Belgian State-Belgian Science Policy: project P6/26-Bcrypt.

Address of the authors:

A. Klein and L. Storme: Ghent University, Dept. of Mathematics, Krijgslaan 281-S22, 9000 Ghent, Belgium

J. Schillewaert: Département de Mathématique, Université Libre de Bruxelles, U.L.B., CP 216, Bd. du Triomphe, B-1050 Bruxelles, Belgique

A. Klein: klein@cage.ugent.be, `http://cage.ugent.be/~klein`
J. Schillewaert: jschille@ulb.ac.be
L. Storme: ls@cage.ugent.be, `http://cage.ugent.be/~ls`

References

[1] R. C. Bose. Mathematical theory of the symmetrical factorial design, *Sankhyā*, (1947), 107–166.

[2] A. Del Fra. On d-dimensional dual hyperovals, *Geom. Dedicata*, **79**, (2000), 157–178.

[3] J. W. P. Hirschfeld and J. A. Thas. *General Galois geometries.* Oxford University Press, Oxford, 1991.

[4] W.-A. Jackson, K. M. Martin and C. M. O'Keefe. Geometrical contributions to secret sharing theory, *J. Geom.*, **79**, (2004), 102–133.

[5] A. Klein, J. Schillewaert and L. Storme. Generalised dual arcs and Veronesean surfaces, with applications to cryptography, *J. Combin. Theory, Ser. A*, **116**, (2009), 684–698.

[6] K. M. Martin. Challenging the Adversary Model in Secret Sharing Schemes. *Proceedings of the Contact Forum* Coding Theory and Cryptography II, September 21, 2007, at The Royal Flemish Academy of Belgium for Science and the Arts, Brussels, Belgium, (2008), 45–64.

[7] G. Tallini. Una proprietà grafica caratteristica della superficie di Veronese negli spazi finiti. I, II. *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Nat. (8)*, **24**, (1958), 19–23, 135–138.

[8] J. A. Thas and H. Van Maldeghem. Characterizations of the finite quadric Veroneseans $V_n^{2^n}$, *The Quarterly Journal of Mathematics*, **55**, (2004), 99–113.

[9] S. Yoshiara. Ambient spaces of dimensional dual arcs, *J. Algebraic Combin.*, **19**, (2004), 5–23.