Journal of Combinatorial Theory, Series A 116 (2009) 684–698

Contents lists available at ScienceDirect

Journal of Combinatorial Theory, Series A

www.elsevier.com/locate/jcta

Generalised dual arcs and Veronesean surfaces, with applications to cryptography

A. Klein, J. Schillewaert, L. Storme

Ghent University, Department of Pure Mathematics and Computer Algebra, Krijgslaan 281-S22, 9000 Ghent, Belgium

ARTICLE INFO

Article history:
Received 11 June 2007
Available online 9 December 2008
Communicated by Francis Buekenhout

Keywords:
Generalised dual arcs
Veronesean surfaces
Message authentication codes

ABSTRACT

We start by defining generalised dual arcs, the motivation for defining them comes from cryptography, since they can serve as a tool to construct authentication codes and secret sharing schemes. We extend the characterisation of the tangent planes of the Veronesean surface V_2^4 in $PG(5,q)$, q odd, described in [J.W.P. Hirschfeld, J.A. Thas, General Galois Geometries, Oxford Math. Monogr., Clarendon Press/Oxford Univ. Press, New York, 1991], as a set of q^2+q+1 planes in $PG(5,q)$, such that every two intersect in a point and every three are skew. We show that a set of q^2+q planes generating $PG(5,q)$, q odd, and satisfying the above properties can be extended to a set of q^2+q+1 planes still satisfying all conditions. This result is a natural generalisation of the fact that a q-arc in $PG(2,q)$, q odd, can always be extended to a $(q+1)$-arc. This extension result is then used to study a regular generalised dual arc with parameters $(9,5,2,0)$ in $PG(9,q)$, q odd, where we obtain an algebraic characterisation of such an object as being the image of a *cubic* Veronesean.

1. Introduction

The quadratic Veronesean V_2^4 is one of the most important substructures in $PG(5,q)$. It is the image of the plane $PG(2,q)$ under the mapping

$$\eta : PG(2,q) \to PG(5,q) : (x_0,x_1,x_2) \mapsto \left(x_0^2, x_1^2, x_2^2, x_0x_1, x_0x_2, x_1x_2\right).$$

This quadratic Veronesean V_2^4 has been studied in great detail, and characterised in different ways.

E-mail addresses: klein@cage.ugent.be (A. Klein), jschille@cage.ugent.be (J. Schillewaert), ls@cage.ugent.be (L. Storme).
URLs: http://cage.ugent.be/~klein (A. Klein), http://cage.ugent.be/~ls (L. Storme).

0097-3165/$ – see front matter
doi:10.1016/j.jcta.2008.11.001

A particular characterisation uses the tangent planes to the Veronesean V_2^4 in $PG(5,q)$, q odd.

Theorem 1. *(See Tallini [7].) Let $\mathcal{F}$ be a set of q^2+q+1 planes in $PG(5,q)$, q odd, satisfying the following properties*:

1. *the elements of $\mathcal{F}$ generate $PG(5,q)$,*
2. *two distinct elements of $\mathcal{F}$ intersect in a point,*
3. *three distinct elements of $\mathcal{F}$ have an empty intersection.*

Then $\mathcal{F}$ consists of the set of q^2+q+1 tangent planes to a Veronesean surface V_2^4.

We extend this result by proving that a set of q^2+q planes of $PG(5,q)$, $q>3$ odd, spanning $PG(5,q)$ and satisfying the properties above, is equal to a set of q^2+q tangent planes of a quadratic Veronesean V_2^4.

Our motivation for solving this problem is to characterise regular $(9,5,2,0)$-dimensional dual arcs, for q odd, $q>3$, containing q^2+q+1 5-spaces. This is a set of q^2+q+1 distinct 5-spaces of $PG(9,q)$, generating $PG(9,q)$, such that two distinct 5-spaces intersecting in a plane, three distinct 5-spaces intersecting in a point, and such that every four distinct 5-spaces have an empty intersection.

It follows from the preceding definition that in every 5-space, the intersections with the other 5-spaces form q^2+q planes satisfying the properties above, thus, by the extension result presented in Theorem 15, they are tangent planes to a Veronesean variety V_2^4 in this 5-space.

This information on the planes forming the intersections of a given 5-space with the other q^2+q distinct 5-spaces enables us to characterise the regular $(9,5,2,0)$-dimensional dual arcs, for q odd, $q>3$, having q^2+q+1 distinct 5-spaces in a unique way.

Our characterisation result also will imply that any regular $(9,5,2,0)$-dimensional dual arc, for q odd, $q>3$, contains at most q^2+q+1 5-spaces.

Our motivation for characterising these $(9,5,2,0)$-dimensional dual arcs follows from the fact that they can be used to define message authentication codes (MAC). We present this link in the final section of the paper.

2. Generalised dual arcs

Definition 2. A *generalised dual arc* $\mathcal{D}$ of order l with dimensions $d_1>d_2>\cdots>d_{l+1}$ of $PG(n,q)$ is a set of subspaces of dimension d_1 such that:

1. each j of these subspaces intersect in a subspace of dimension d_j, $1\leqslant j\leqslant l+1$,
2. each $l+2$ of these subspaces have no common intersection.

We call $(n,d_1,\dots,d_{l+1})$ the *parameters* of the dual arc.

Example 1.

- Take a dual arc in a plane π. Embed π in a 3-dimensional space. Now we have a generalised dual arc with parameters $(3,1,0)$. But the 3-space is not really used.
- Take a dual arc with k elements in a plane π. Embed π in a space of dimension $k+2$ and choose planes through the k lines of the dual arc that span $PG(2+k,q)$. This is a generalised dual arc with parameters $(k+2,2,0)$. Even if the planes span $PG(2+k,q)$, the interesting part of the construction is contained only in the plane π.
- The following planes of $PG(4,q)$ form a generalised dual arc with parameters $(4,2,0)$:

$$\pi_1=\{[a,b,c,0,0]\mid a,b,c\in\mathbb{F}_q\},$$

$$\pi_2=\{[a,0,b,b,c]\mid a,b,c\in\mathbb{F}_q\},$$

$$\pi_3 = \{[0, a, b, c, b] \mid a, b, c \in \mathbb{F}_q\},$$
$$\pi_4 = \{[a, a, 0, b, c] \mid a, b, c \in \mathbb{F}_q\}.$$

The intersection points of π_1 with the other planes lie on the line $X_2 = X_3 = X_4 = 0$. So only that line of π_1 is a real part of the generalised dual arc.

These examples motivate the notion of a regular generalised dual arc.

Definition 3. A generalised dual arc $\mathcal{D}$ of order l with parameters $(n = d_0, \ldots, d_{l+1})$ is *regular* if, in addition, the d_1-dimensional spaces span $PG(n,q)$ and it satisfies the property that if π is the intersection of j elements of $\mathcal{D}$, $j \leqslant l$, then π is spanned by the subspaces of dimension d_{j+1} which are the intersections of π with the remaining elements of $\mathcal{D}$.

A normal d-dimensional dual arc in $PG(n,q)$ has parameters $(n, d, 0)$. A generalised dual arc of order 0 is a partial d_1-spread.

In particular, a regular generalised dual arc with parameters $(9, 5, 2, 0)$ is a set of 5-spaces in $PG(9,q)$, generating $PG(9,q)$, such that each two intersect in a plane, each three in a point, and each four are skew. This is the particular regular generalised dual arc we will characterise later on for q odd, $q > 3$.

Construction 1. *Let $PG(V)$ be a d-dimensional space and let e_i $(0 \leqslant i \leqslant d)$ be a basis of V.*

Let $PG(W)$ be a $(\binom{d+l+1}{l+1} - 1)$-dimensional space and let $e_{i_0,\ldots,i_l}$ $(0 \leqslant i_0 \leqslant i_1 \leqslant \cdots \leqslant i_l \leqslant d)$ be a basis of W.

Below, we define a map which is a generalisation of the well-known quadratic Veronesean map (*see* [4]).

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

$$\zeta : \left[\sum_{i=0}^{d} x_i e_i\right] \mapsto \left[\sum_{0 \leqslant i_0 \leqslant \cdots \leqslant i_l \leqslant d} x_{i_0} \cdots x_{i_l} e_{i_0,\ldots,i_l}\right].$$

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

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

and

$$B\left(\sum_{0 \leqslant i_0 \leqslant \cdots \leqslant i_l \leqslant d} x_{i_0,\ldots,i_l} e_{i_0,\ldots,i_l}, \sum_{0 \leqslant i_0 \leqslant \cdots \leqslant i_l \leqslant d} y_{i_0,\ldots,i_l} e_{i_0,\ldots,i_l}\right) = \sum_{0 \leqslant i_0 \leqslant \cdots \leqslant i_l \leqslant d} x_{i_0,\ldots,i_l} y_{i_0,\ldots,i_l}.$$

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 $D(P)$ of $PG(W)$ by

$$D(P) = \{[z] \in W \mid B(z, \zeta(y)) = 0 \text{ for all } y \in x^\perp\}. \tag{1}$$

Before we prove that this construction indeed gives a generalised dual arc, we show two examples.

Example 2. 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 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 generalised dual arc of $q^2 + q + 1$ planes with parameters $(5, 2, 0)$.

Example 3. 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 configuration of $q^2 + q + 1$ 5-dimensional spaces 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 2.

For π_0, the corresponding Veronesean has the equation

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

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 equation

$$E_0 := \{[a_0, 0, 0, a_1, a_2, 0, 0, 0, 0, 0] \mid a_0, a_1, a_2 \in \mathbb{F}_q\}.$$

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

$$E_1 := \{[0, a_0, 0, 0, 0, a_1, a_2, 0, 0, 0] \mid a_0, a_1, a_2 \in \mathbb{F}_q\},$$

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

$$E_2 := \{[0, 0, a_0, 0, 0, 0, 0, a_1, a_2, 0] \mid a_0, a_1, a_2 \in \mathbb{F}_q\}.$$

Let q be odd. Assume that the generalised dual arc of $q^2 + q + 1$ 5-spaces can be extended to a generalised dual arc of size $q^2 + q + 2$. The additional 5-space must intersect each of the three 5-spaces π_0, π_1, π_2 in the extra planes E_0, E_1, E_2. But E_0, E_1, E_2 span an 8-space. Thus our example with $q^2 + q + 1$ 5-spaces is a maximal dual arc.

For q even, the situation is a bit more complicated. Now the dual arc of Example 2 can be extended to a dual arc of size $q^2 + q + 2$, see [4, Theorem 25.1.17]. Thus π_0, π_1, π_2 contain two extra planes. But we can check that no three extra planes lie in a common 5-space. Thus the example with $q^2 + q + 1$ 5-spaces is a maximal generalised dual arc.

Theorem 4. *The set $\mathcal{D} = \{D(P) \mid P \in PG(V)\}$ is a regular generalised dual arc with dimensions $d_i = \binom{d+l+1-i}{l+1-i} - 1$, $i = 0, \ldots, l+1$.*

Proof. *Step* 1: The dimension of $D(P)$.

Let $P=[x]$, then $x^{\perp}$ is a d-dimensional subspace of V. By ζ, this d-dimensional subspace is mapped to a $\binom{d+l}{l+1}$-dimensional subspace W' of W. (Here we need $q>l$ since otherwise the points of the generalised Veronesean do not span the whole space.)

Since the bilinear form B is non-degenerate, the space

$$\{z\in W \mid B(z,y)=0 \text{ for } y\in W'\}$$

has dimension $\binom{d+l+1}{l+1}-\binom{d+l}{l+1}=\binom{d+l}{l}$.

Thus $D(P)$ has projective dimension $\binom{d+l}{l}-1$.

Step 2: The intersection of two spaces.

We now give an alternative description of $D(P)$.

For each permutation σ, let $e_{i_{\sigma(0)},\dots,i_{\sigma(l)}}$ be equal to $e_{i_0,\dots,i_l}$.

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

$$\theta:\left(\sum_{i=0}^{d}x_i^{(0)}e_i,\dots,\sum_{i=0}^{d}x_i^{(l)}e_i\right)\mapsto\sum_{0\leqslant i_0,\dots,i_l\leqslant d}x_{i_0}^{(0)}\cdot\dots\cdot x_{i_l}^{(l)}e_{i_0,\dots,e_l}. \tag{2}$$

A simple check shows us that for $b(x,y)=0$, we have

$$B\big(\theta(x,v_1,\dots,v_l),\zeta(y)\big)=0$$

for all possible vectors $v_1,\dots,v_l$ of V.

Thus for $P=[x]$, we have

$$\big\langle\theta(x,v_1,\dots,v_l)\ \big|\ v_1,\dots,v_l\in V\big\rangle\subseteq D(P).$$

Since the vector space $\langle\theta(x,v_1,\dots,v_l)\mid v_1,\dots,v_l\in V\rangle$ has dimension $\binom{d+l}{l}$ (choose $v_1,\dots,v_l$ as basis vectors), we find

$$\big\langle\theta(x,v_1,\dots,v_l)\ \big|\ v_1,\dots,v_l\in V\big\rangle=D(P). \tag{3}$$

Since $PGL(V)$ acts doubly transitively on V, it is sufficient to check the dimension of $D(P)\cap D(P')$ for two fixed points. We choose $P=[1,0,\dots,0]$ and $P'=[0,1,0,0,\dots,0]$. From (3), we see directly that in this case

$$D(P)\cap D(P')=\big\{[e_{0,1,i_2,\dots,i_l}]\ \big|\ 0\leqslant i_j\leqslant d\big\}.$$

Thus $D(P)\cap D(P')$ has projective dimension $\binom{d+l-1}{l-1}-1$.

Step 3: The intersection of more than two spaces.

If $P=[x]$ and $P'=[y]$, we see from (3) that

$$\big\langle\theta(x,y,v_2,\dots,v_l)\ \big|\ v_2,\dots,v_l\in V\big\rangle\subseteq D(P)\cap D(P').$$

Since we now know the dimension of the intersection $D(P)\cap D(P')$, we even see that

$$\big\langle\theta(x,y,v_2,\dots,v_l)\ \big|\ v_2,\dots,v_l\in V\big\rangle=D(P)\cap D(P').$$

Thus for a fixed point P, the set $\mathcal{D}'=\{D(P)\cap D(P')\mid P'\neq P\}$ is a set of subspaces of dimension $\binom{d+l-1}{l-1}-1$ which is defined by a generalised dual arc of order $l-1$. By induction, we know the dimension of the intersections.

This proves that the intersection of $D(P)$ with two or more other spaces has the correct dimension. $\square$

Remark. Even if Eq. (1) is only defined for $q>l$, a generalised dual arc defined by Eq. (3) works for any q and l.

3. An extension result for $q^2 + q$ planes satisfying the properties of the tangent planes of the Veronesean surface V_2^4 in $PG(5, q)$, q odd

In Example 3, we have constructed a regular generalised dual arc with parameters $(9, 5, 2, 0)$ consisting of $q^2 + q + 1$ distinct 5-spaces of $PG(9, q)$. In each of these 5-spaces, we have a set of $q^2 + q$ planes forming a regular generalised dual arc with parameters $(5, 2, 0)$. For q odd, $q > 3$, we will show that we can always find an extra plane in such a 5-space, in order to obtain a set of $q^2 + q + 1$ planes forming a regular generalised dual arc with parameters $(5, 2, 0)$. Such a set of $q^2 + q + 1$ planes in $PG(5, q)$, q odd, is the set of tangent planes to a Veronesean variety V_2^4 [4, Theorem 25.2.12].

Therefore, in $PG(5, q)$, consider a set $\mathcal{F}$ of $q^2 + q$ planes generating $PG(5, q)$, such that each two of them intersect in a point, and each three of them are skew.

Let q be odd.

Each plane π of $\mathcal{F}$ contains 2 points that are covered only once. We call these points *contact points* of this plane π of $\mathcal{F}$. The lemmas below are paraphrases of the lemmas of the characterisation of V_2^4, q odd, which can be found in [4].

Lemma 5. *Every hyperplane Π of $PG(5, q)$ contains at most $q + 1$ planes of $\mathcal{F}$.*

Proof. A plane of $\mathcal{F}$ not contained in Π intersects Π in a line ℓ. Each plane of $\mathcal{F}$ contained in Π must share a point with that line ℓ. Furthermore, no two planes of $\mathcal{F}$ in Π intersect ℓ in the same point, so Π contains at most $q + 1$ planes of $\mathcal{F}$. $\square$

Lemma 6. *Every hyperplane Π of $PG(5, q)$ contains 0, 1, $q - 1$, q, or $q + 1$ planes of $\mathcal{F}$.*

Proof. Let Π be a hyperplane that contains k planes of $\mathcal{F}$, where $2 \leqslant k < q - 1$.

Let π' be any plane of $\mathcal{F}$ not contained in Π. This plane π' intersects Π in a line l'. At least $q - 1$ points of l' must be covered by a second plane of $\mathcal{F}$. Since $q + 1 - k - 2 > 0$, there must be a second plane 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 planes of $\mathcal{F}$ in Π must intersect π' and π'', these k planes intersect π' and π'' in a point on l', respectively on l'', hence, they intersect π in lines.

Assume that π''' is another plane 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 plane of $\mathcal{F}$ contained in Π must share a line with the plane spanned by l' and l'', and have a point in common with l'''. Thus these planes lie in the 3-dimensional space spanned by l', l'' and l'''. Especially they must share a line, a contradiction.

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

If π_1 and π_2 intersect in a line, then at most one plane of $\mathcal{F}$ contained in Π contains the line $\pi_1 \cap \pi_2$. So at least $k - 1$ planes of $\mathcal{F}$ contained in Π must lie in the 3-dimensional space spanned by π_1 and π_2. Thus each two of the planes must share a line, a contradiction for $k > 2$. We now eliminate the case $k = 2$, where one of the two planes 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 $q - 2$. For, consider a first plane π' of $\mathcal{F}$ not in Π, then consider the line $\ell' = \pi' \cap \Pi$. This line has at most two contact points, so it is intersected by at least $q - 3$ planes of $\mathcal{F}$, not lying in Π, in a point. This shows that a group of planes of $\mathcal{F}$, not lying in Π, has at least size $q - 2$.

But now consider the line $\ell = \pi_1 \cap \pi_2$, lying in the plane π of $\mathcal{F}$, also lying in Π, and in the two planes π_1 and π_2 containing at least $q - 2$ lines lying in planes of $\mathcal{F}$, not contained in Π. Since no point lies in three planes of $\mathcal{F}$, and every point of ℓ already lies in the plane π of $\mathcal{F}$, we must have $q+1 \geqslant 2(q-2)+1$, where the $+1$ arises from the second plane of $\mathcal{F}$ in Π. This implies $q \leqslant 3$.

Thus π_1 and π_2 intersect in a point Q. But then the only possibility for a plane of $\mathcal{F}$ contained in Π to intersect π_1 and π_2 in lines is that Q is a point of that plane. Thus all planes of $\mathcal{F}$ contained in Π contain Q. Since every three planes of $\mathcal{F}$ are skew, this means that $k=2$. Since there are q^2+q-2 planes of $\mathcal{F}$ not contained in Π, and each group can contain at most $q-1$ planes, there are at least $q+2$ different groups.

Each group defines a plane through Q which intersects a plane of $\mathcal{F}$ contained in Π in a line. Since a plane contains only $q+1$ 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. □

Lemma 7. *Let Π be a hyperplane of $PG(5,q)$ that contains $q+1$ planes $\pi_0,\dots,\pi_q$ of $\mathcal{F}$. Then $q+1$ of the $2q+2$ contact points in Π form a conic.*

Proof. First of all, Π contains exactly $2q+2$ contact points. Namely, every plane π of $\mathcal{F}$ not in Π intersects Π in a line l. Every plane $\pi_0,\dots,\pi_q$ contains one point of l, so l has no contact points. So Π only contains the contact points of $\pi_0,\dots,\pi_q$. Let $Q_2=\pi_0\cap\pi_1$, $Q_1=\pi_0\cap\pi_2$ and $Q_0=\pi_1\cap\pi_2$.

The points Q_0, Q_1, Q_2 generate a plane, since otherwise, π_0, π_1, π_2 share a line. Assume that the line Q_1Q_2 contains no contact point of π_0. Then Q_1Q_2 contains at least one point Q that lies on a plane π of $\mathcal{F}\backslash\{\pi_0,\dots,\pi_q\}$. More precisely, $\{Q\}=\pi_0\cap\pi$. Let $l=\pi\cap\Pi$.

Suppose that l is not a line of the plane $Q_0Q_1Q_2$. Each of the planes π_1 and π_2 has one point in common with l. This point differs from Q, i.e. it does not lie in $Q_0Q_1Q_2$. This proves that π_1 and π_2 are contained in the solid spanned by $Q_0Q_1Q_2$ and l. It follows that π_1 and π_2 have a common line, a contradiction. So l is a line of $Q_0Q_1Q_2$.

Every plane $\pi_1,\dots,\pi_q$ which has a point in common with Q_1Q_2 must also share a point with l, i.e. all these planes intersect $Q_0Q_1Q_2$ in a line. Together with the lines in $Q_0Q_1Q_2$ coming from planes in $\mathcal{F}\backslash\{\pi_0,\dots,\pi_q\}$, these lines form a dual $(q+2)$-arc. A contradiction to q odd, see [3].

Let Q' be the intersection point $\pi_3\cap\pi_0$. The argument above proves that Q_1Q_2, Q_1Q' and Q_2Q' must contain a contact point of π_0. Since π_0 has only two contact points, this proves that $Q'\in Q_1Q_2$.

The same argument proves that $\pi_3\cap\pi_1\in Q_0Q_2$. Thus each of the $q+1$ planes $\pi_0,\dots,\pi_q$ shares a line with $Q_0Q_1Q_2$. These lines form a dual $(q+1)$-arc. Each of the lines contains a contact point and these contact points form a conic, since every dual $(q+1)$-arc in $PG(2,q)$, q odd, consists of the tangent lines to a conic in $PG(2,q)$, q odd, see [3]. □

Lemma 8. *Let Π be a hyperplane of $PG(5,q)$ that contains q planes $\pi_0,\dots,\pi_{q-1}$ of $\mathcal{F}$. Then Π contains a plane $\bar{\Pi}$ which intersects the q planes of $\mathcal{F}$ in Π in a line.*

The plane $\bar{\Pi}$ contains at least q contact points which lie on a conic.

Furthermore, every plane of $\mathcal{F}$ not contained in Π intersects Π in a line. This line contains a contact point and is either skew to $\bar{\Pi}$, or lies completely in $\bar{\Pi}$. The latter case can occur only once.

Proof. The same arguments as in the previous proof show that every plane of $\mathcal{F}$, not contained in Π but containing a point of Q_0Q_1, intersects $\bar{\Pi}=Q_0Q_1Q_2$ in a line; equivalently, such a plane does not intersect $\pi_0,\dots,\pi_{q-1}$ in a point of the plane $\bar{\Pi}$, or it intersects all planes $\pi_0,\dots,\pi_{q-1}$ in a point of $\bar{\Pi}$.

We investigate three planes π_0, π_1, and π_2 of $\mathcal{F}$ contained in Π. Let $Q_2=\pi_0\cap\pi_1$, $Q_1=\pi_0\cap\pi_2$ and $Q_0=\pi_1\cap\pi_2$. As in the previous proof, we find that Q_1Q_2 contains a contact point of π_0. The same arguments as in the previous proof show that every plane of $\mathcal{F}$ contained in Π intersects $\bar{\Pi}=Q_0Q_1Q_2$ in a line.

The only difference is that this time we cannot exclude the case that a plane π' of $\mathcal{F}$, not in Π, intersects Π in a line l' contained in $\bar{\Pi}$. Thus we see in $\bar{\Pi}$ either a dual q-arc or a dual $(q+1)$-arc of lines lying in planes of $\mathcal{F}$. But in any case, there are contact points that lie on a conic. □

Definition 9. A *Q-hyperplane* of $\mathcal{F}$ is a hyperplane Π of $PG(5,q)$ containing q planes of $\mathcal{F}$, such that the plane $\bar{\Pi}$ of Π intersecting the q planes of $\mathcal{F}$ in Π in a line contains exactly q lines lying in a plane of $\mathcal{F}$.

Equivalently, the line in $\bar{\Pi}$ extending the dual q-arc consisting of the intersection lines of the planes of $\mathcal{F}$ in Π with $\bar{\Pi}$ consists of q contact points lying in the planes of $\mathcal{F}$ in Π.

Lemma 10. *Let Π be a hyperplane of $PG(5,q)$ that contains $q-1$ planes of $\mathcal{F}$. Then Π contains a plane $\bar{\Pi}$ which intersects the $q-1$ planes of $\mathcal{F}$ in Π in a line, and which contains a conic of contact points.*

Proof. The arguments of the previous lemma are still valid. The only difference is that $\bar{\Pi}$ must contain one line l' that is induced from a plane of $\mathcal{F}$ not in Π. Namely, if no such line exists, then the intersection lines of the planes of $\mathcal{F}$ in Π with $\bar{\Pi}$ form a dual $(q-1)$-arc. But then every such line contains three contact points, which is impossible.

Furthermore, $\bar{\Pi}$ may contain at most two such lines. Thus we see in $\bar{\Pi}$ either a dual q-arc or a dual $(q+1)$-arc of intersection lines of planes of $\mathcal{F}$. $\square$

Lemma 11. *Every plane of $\mathcal{F}$ is contained in exactly one Q-hyperplane of $PG(5,q)$. Hence, there are $q+1$ such Q-hyperplanes.*

Proof. Let π be any plane of $\mathcal{F}$, then the other elements of $\mathcal{F}$ lie in hyperplanes $\Pi_1,\dots,\Pi_k$ through π which contain either $q-1$, q or $q+1$ planes of $\mathcal{F}$. To each hyperplane Π_i, there corresponds a plane $\bar{\Pi}_i$ which contains a conic of contact points and all intersections $\pi \cap \pi'$, where π' is a plane of $\mathcal{F}$ contained in Π_i.

The planes $\bar{\Pi}_i$ intersect π in lines l_i. These lines always go through a contact point and cover π. Thus there exists a unique hyperplane Π through π for which $\bar{\Pi}$ contains both contact points. The hyperplane Π then must contain $q-1$ elements of $\mathcal{F}\backslash\{\pi\}$ which intersect π in the $q-1$ non-contact points of $\bar{\Pi} \cap \pi$.

By Lemma 8, since Π contains q planes of $\mathcal{F}$, and since $\bar{\Pi} \cap \pi$ contains two contact points, it is impossible that some plane of $\mathcal{F}$ not contained in Π intersects $\bar{\Pi}$ in a line, so, again by Lemma 8, every plane of $\mathcal{F}$ not contained in Π is skew to $\bar{\Pi}$. The intersections of the planes of $\mathcal{F}$ contained in Π with $\bar{\Pi}$ form a dual q-arc. We know by a famous theorem of Segre, see [6], that a q-arc in $PG(2,q)$, q odd, can always be extended to a $(q+1)$-arc. This proves that the $2q$ contact points contained in $\bar{\Pi}$ lie on a conic and a line.

We have shown that Π is a Q-hyperplane. This Q-hyperplane Π through π must be unique since the corresponding plane $\bar{\Pi}$ must contain the line of π through the two contact points in π. Hence, by Lemma 8, this Q-hyperplane contains π and the $q-1$ planes of $\mathcal{F}$ intersecting π in a point of the line of π through the two contact points of π.

We have proved that every plane of $\mathcal{F}$ is contained in exactly one Q-hyperplane. Thus there are $(q^2+q)/q = q+1$ Q-hyperplanes. $\square$

From here on, assume $q > 3$.

Lemma 12. *Let Π_1 and Π_2 be Q-hyperplanes. Let $\bar{\Pi}_1$ and $\bar{\Pi}_2$ be the planes in Π_1 and Π_2 intersected by the planes of $\mathcal{F}$ in Π_1 and Π_2 in lines, and containing the "conic" of contact points. Let $\tilde{l}_1$ be the line extending the dual q-arc in $\bar{\Pi}_1$ consisting of the intersection lines of the planes of $\mathcal{F}$ in Π_1 with $\bar{\Pi}_1$. Then $\tilde{l}_1$ consists of q tangent points and $\tilde{l}_1$ is completely contained in Π_2.*

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 plane 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 $q-1$ points lying in two planes of $\mathcal{F}$ in Π_1. But the q planes of $\mathcal{F}$ in Π_2 must intersect π in a point. So at least q points of ℓ lie still in a plane of $\mathcal{F}$ in Π_2. Then there are points of ℓ lying in three planes of $\mathcal{F}$. This is false.

So $\bar{\Pi}_1$ intersects Π_2 in a line.

Consider again the intersection line $\ell = \Pi_2 \cap \pi$ of a plane π of $\mathcal{F}$ in Π_1 with Π_2. This line contains q points lying on a plane of $\mathcal{F}$ in Π_2. So these points do not lie in another plane of $\mathcal{F}$ in Π_1. The remaining point on ℓ is a contact point by Lemma 8.

Now ℓ and $\pi \cap \bar{\Pi}_1$ intersect in a point. 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 $\bar{\Pi}_1$.

The preceding arguments show that the plane $\bar{\Pi}_1$ contains a line having at least q contact points.

But then this line is the line $\tilde{l}_1$ in $\bar{\Pi}_1$ extending the dual q-arc consisting of the intersection lines of the planes of $\mathcal{F}$ in Π_1 with $\bar{\Pi}_1$.

The preceding arguments already show that this line $\tilde{l}_1$ lies in Π_2. $\square$

Corollary 13. *Let $\Pi_1, \dots, \Pi_{q+1}$ be the Q-hyperplanes and $\bar{\Pi}_1, \dots, \bar{\Pi}_{q+1}$ the planes containing the lines $M_1, \dots, M_{q+1}$ containing q contact points.*

Then the lines $M_1, \dots, M_{q+1} \subset \Pi_1 \cap \dots \cap \Pi_{q+1}$.

Lemma 14. *No three Q-hyperplanes Π_1, Π_2, Π_3 intersect in a 3-space.*

Proof. Suppose that three Q-hyperplanes intersect in a 3-space Δ. Let $\pi \in \mathcal{F}$, $\pi \in \Pi_2$. Let $\pi \cap \Delta$ be a line ℓ. Then the q planes of $\mathcal{F} \cap \Pi_1$ intersect π in a point; this point lies in $\Delta = \Pi_1 \cap \Pi_2$, so this point lies on ℓ. Similarly, the q planes of $\mathcal{F} \cap \Pi_3$ intersect π in a point, this point lies again on ℓ. Then there are points on ℓ lying on 3 planes of $\mathcal{F}$, a contradiction. $\square$

Conclusion. The lines $M_1, \dots, M_{q+1}$ lie in the intersection of all $q+1$ different Q-hyperplanes, and by the preceding lemma, they intersect in a plane Ω. So $M_1, \dots, M_{q+1} \subset \Omega$. So there is a plane Ω containing q^2+q contact points. Every plane of $\mathcal{F}$ must share at least one point with Ω, since every plane of $\mathcal{F}$ has one point of a line M_i. No plane of $\mathcal{F}$ shares a line with Ω, else we obtain points of Ω on 2 planes of $\mathcal{F}$. This contradicts with the fact that they are contact points. This argument shows that Ω extends $\mathcal{F}$ to a set of q^2+q+1 planes pairwise intersecting in a point, where still three planes have an empty intersection, so $\mathcal{F} \cup \{\Omega\}$ is the set of tangent planes to a Veronesean surface V_2^4 in $PG(5,q)$, q odd [7] and [4, Theorem 25.2.12.]. So we have proven the following extension result.

Theorem 15. *A set of q^2+q planes $\mathcal{F}$ in $PG(5,q)$, q odd, $q>3$, such that*:

(i) *the planes generate $PG(5,q)$,*
(ii) *every two planes intersect in a point,*
(iii) *every three planes are skew,*

can be extended to a set of q^2+q+1 planes in $PG(5,q)$ having the same properties.

Equivalently, such a set of q^2+q planes is a set of q^2+q tangent planes to a Veronesean variety V_2^4 of $PG(5,q)$, q odd, $q>3$.

4. An algebraic characterisation of the regular generalised dual arc with parameters (9, 5, 2, 0), *q* odd, *q* > 3

We are going to use the extension result of the previous section in order to study the regular generalised dual arc $\mathcal{D}$ with parameters $(9,5,2,0)$, q odd. So we have a set $\mathcal{F}$ of q^2+q+1 distinct 5-spaces in $PG(9,q)$ that generate $PG(9,q)$. Furthermore, the 5-spaces intersect in planes and the planes coming from the intersections of a given 5-space Ω with the other 5-spaces of $\mathcal{D}$ span Ω. We know from Theorem 15 that the q^2+q intersection planes in a 5-space Ω are tangent planes to a Veronesean variety V_2^4 in this 5-space Ω. This will play a crucial role in the characterisation result. Also the following observation is of great importance.

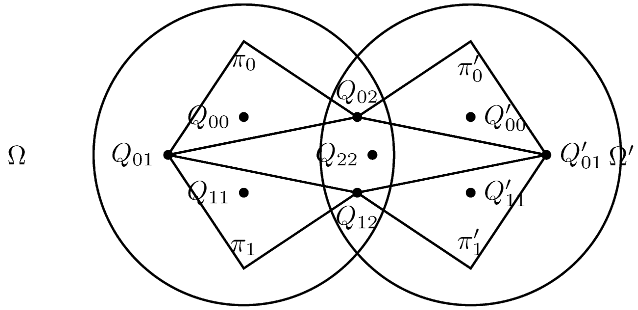

Fig. 1. The 5-spaces Ω and Ω' with the extra planes π_0 and π_0'.

Remark. The Veronesean surface V_2^4, q odd, can be determined uniquely in the following way, as indicated in the proof of Theorem 25.2.12 in [4].

Let Q_{00}, Q_{11} and Q_{22} be three distinct points of V_2^4 which are not contained in a plane of V_2^4. This means that their corresponding tangent planes π_{00}, π_{11} and π_{22} are not lying in a common hyperplane with $q+1$ tangent planes of V_2^4. Let $Q_{ij} = Q_{ji} = \pi_{ii} \cap \pi_{jj}$, $i, j \in \{0, 1, 2\}$. Then the plane generated by Q_{ii}, Q_{jj} and Q_{ij} contains a conic $C_{ij} = C_{ji}$ of contact points.

Then for a point U of V_2^4, $U \notin C_{01} \cup C_{02} \cup C_{12}$, select the coordinates such that $Q_{00} = e_0$, $Q_{11} = e_1$, $Q_{22} = e_2$, $Q_{01} = e_3$, $Q_{02} = e_4$ and $Q_{12} = e_5$, where e_i is the vector having coordinate 1 in position i and 0 in all other positions, and $U = (1, 1, \ldots, 1)$. Then the unique Veronesean surface V_2^4, passing through U, having Q_{00}, Q_{11} and Q_{22} as contact points and π_{00}, π_{11} and π_{22} as tangent planes in Q_{00}, Q_{11} and Q_{22}, is the Veronesean surface V_2^4 in standard form

$$\left(x_0^2, x_1^2, x_2^2, x_0x_1, x_0x_2, x_1x_2\right).$$

Lemma 16. *For q odd and $q > 3$, let Ω and Ω' be two of the 5-dimensional spaces of $\mathcal{D}$. In each of the 5-dimensional spaces, we see a configuration of q^2+q planes, such that each two intersect in a point, and each three are skew. By Theorem* 15, *this configuration can be extended by a plane to a set of q^2+q+1 tangent planes to a Veronesean surface. Let π_0 and π_0' denote these extension planes in Ω and Ω', respectively, and let the respective sets of q^2+q+1 planes be the tangent planes to the Veronesean surfaces V_2^4 and $V_2^{4'}$ in Ω and Ω', respectively.*

Then π_0 and π_0' are skew.

Proof. Consider Ω and Ω'. (See Fig. 1.) The plane $\pi_2 = \Omega \cap \Omega'$ has 2 contact points. Assume that the extension planes in Ω and Ω' use the same contact point Q_{02} in $\Omega \cap \Omega'$.

Step 1: The coordinates in Ω.

Let Q_{22} be the other contact point in the plane $\pi_2 = \Omega \cap \Omega'$. In the extra plane π_0, we have the contact point Q_{00} and $Q_{02} = \pi_0 \cap \pi_2$. In π_2, select a point Q_{12} not on $Q_{02}Q_{22}$. This point lies in a plane π_1 of Ω; this plane π_1 contains the contact point Q_{11}, and the point $Q_{01} = \pi_0 \cap \pi_1$. Take $U \in V_2^4$ in Ω, not in the planes $C_{01} = \langle Q_{01}, Q_{00}, Q_{11}\rangle$, $C_{02} = \langle Q_{02}, Q_{00}, Q_{22}\rangle$, $C_{12} = \langle Q_{12}, Q_{11}, Q_{22}\rangle$. Then choose the coordinates as indicated in the remark above, so that V_2^4 is equal to the Veronesean surface in standard form, i.e.:

$$\left(x_0^2, x_1^2, x_2^2, x_0x_1, x_0x_2, x_1x_2, 0, 0, 0, 0\right).$$

Step 2: The coordinates in Ω'.

Let the plane π_1' be the second tangent plane of the Veronesean surface $V_2^{4'}$ in Ω' through Q_{12}. Then also Q_{11}' and Q_{01}' are uniquely determined as the contact point in π_1' and the intersection point $\pi_0' \cap \pi_1'$. Then since π_0' is fixed, also the contact point Q_{00}' is fixed. So the six points Q_{00}', Q_{11}',

$Q'_{22} = Q_{22}$, Q'_{01}, $Q'_{02} = Q_{02}$, $Q'_{12} = Q_{12}$ are fixed. It is possible to take in $V_2^{4'}$ in Ω' the point U' corresponding to the same point V in π_2 as U.

Indeed, if we have chosen U in Ω, then we find after projection a point V in π_2. Let U vary over $V_2^4 \backslash (C_{01} \cup C_{02} \cup C_{12})$, so $q^2+q+1-3q = q^2-2q+1$ choices for U. In π_2, V cannot lie on the three lines defined by the points Q_{02}, Q_{12} and Q_{22}, so we also have q^2-2q+1 choices for V. Furthermore, a direct calculation shows that the point $U = (a^2, b^2, c^2, ab, ac, bc, 0, 0, 0, 0)$, with $a, b, c \neq 0$, projects on $V = (0, 0, c^2, 0, ac, bc, 0, 0, 0, 0) = (0, 0, c, 0, a, b, 0, 0, 0, 0)$. So different points U give different projections V.

We select U' to be the unit point in Ω'; we have the Veronesean variety $V_2^{4'}$ in Ω' in standard form defined by $Q'_{02} = e_4$, $Q'_{12} = e_5$, $Q'_{22} = e_2$, $Q'_{00} = e_6$, $Q'_{11} = e_7$, $Q'_{01} = e_8$. Then $V_2^{4'}$ can be represented in coordinates in the following way

$$\left(0, 0, x_2'^2, 0, x_0'x_2', x_1'x_2', x_0'^2, x_1'^2, x_0'x_1', 0\right).$$

Step 3: Take a line l in π_0 through Q_{02}, but not through Q_{00}, and let P_1 be a point of l different from Q_{02}. There is a 5-space $\Omega_1 \in \mathcal{D}$, different from Ω, through P_1 since $P_1 \neq Q_{00}$. There cannot be two such 5-spaces since P_1 lies in the extra plane of Ω. Let $\Omega \cap \Omega_1 = \pi_{P_1}$. Then $\pi_{P_1} \cap \pi_2$ is a point $R_1 = \Omega \cap \Omega' \cap \Omega_1$. It must lie in a second plane $\pi'_{P'_1}$ of Ω'. Now the intersection of Ω_1 and Ω' is a plane of the induced Veronesean $V_2^{4'}$ in Ω' through R_1, so $\pi'_{P'_1} = \Omega' \cap \Omega_1$. Set $P'_1 = \pi'_0 \cap \pi'_{P'_1}$.

Step 4: The geometrical properties we know are: P_1 defines a second tangent plane π_{P_1} of V_2^4 in Ω. This second plane which lies in Ω_1, intersects π_2 in a point R_1. This point R_1 lies in a second tangent plane of $V_2^{4'}$ in Ω', and this second plane is $\pi'_{P'_1}$, and P'_1 is $\pi'_0 \cap \pi'_{P'_1}$. This correspondence between the points P_1 and R_1 is bijective when P_1 varies over $\pi_0 \backslash \{Q_{00}, Q_{02}\}$. We have the same correspondence for the points P'_1 in π'_0. It is the same function since V_2^4 and $V_2^{4'}$ are both in standard form. The line $P_1P'_1$ lies in Ω_1. If P_1 has coordinates $(a, 0, 0, b, c, 0, 0, 0, 0, 0)$, then P'_1 has coordinates $(0, 0, 0, 0, c, 0, a, 0, b, 0)$. Hence, it is easy to see that all these lines have a point in common if we let P_1 vary over a fixed line through Q_{02} in π_0. This yields a contradiction since every four 5-dimensional spaces of $\mathcal{D}$ are skew. $\square$

Theorem 17. *Every regular generalised dual arc $\mathcal{D}$ with parameters* $(9, 5, 2, 0)$ *in* $PG(9, q)$, *q odd and $q > 3$, is isomorphic to the one given by Construction* 1, *discussed in detail in Example* 3.

Proof. *Step* 1: Selection of Ω_0, Ω_1 and Ω_2. (See Fig. 2.)

Choose any two 5-spaces Ω_0 and Ω_1 of $\mathcal{D}$. They intersect in a plane π_{01} which contains two contact points.

Assume that the q^2 other 5-spaces Ω of $\mathcal{D}$ that intersect π_{01} in a point not collinear with the two contact points of π_{01} are all contained in the 8-dimensional space spanned by Ω_0 and Ω_1. Let Ω' be a 5-space of $\mathcal{D}$ which generates together with Ω_0 and Ω_1 the whole space $PG(9, q)$. The other 5-spaces intersect Ω' in a plane and at least q^2+2 of the planes must lie in the 4-space $\Omega' \cap \langle \Omega_0, \Omega_1 \rangle$. But this contradicts Lemma 5.

Let π_i be the extra plane of Ω_i $(i = 0, 1, 2)$ which exists by Theorem 15. Then π_i and the q^2+q intersection planes of Ω_i with the other elements in $\mathcal{D}$ are the tangent planes to a Veronesean surface V_i in Ω_i. Denote by P_{iii} the contact point of π_i with respect to the Veronesean surface V_i in Ω_i. The plane π_i intersects the plane $\pi_{ij} = \Omega_i \cap \Omega_j$ in P_{iij}. Note that by the proof of Lemma 16, P_{iij} is the contact point of Π_{ij} to V_j in Ω_j; alternatively, it is the intersection of Π_i and Π_{ij}; so again by Lemma 16, π_i and π_j are skew, implying $P_{iij} \neq P_{jji}$.

Thus there exists a 5-space Ω_2 which intersects π_{01} in a point not collinear with the contact points P_{001} and P_{110}, and such that Ω_0, Ω_1, Ω_2 span $PG(9, q)$.

Let π_{02} be the intersection plane of Ω_0 and Ω_2, and let π_{12} be the intersection plane of Ω_1 and Ω_2. The intersection point of Ω_0, Ω_1, Ω_2 is P_{012}. We determine the conic plane α in the 4-space spanned by π_{01} and π_{12} in Ω_1. This is the plane that is generated by the two contact points P_{001}, P_{221} and the intersection point $P_{012} = \pi_{01} \cap \pi_{12}$. The arguments of Lemma 5 show that every tangent plane to the Veronesean surface V_1 in Ω_1 is either skew to α or intersects α in a line. Since P_{012},

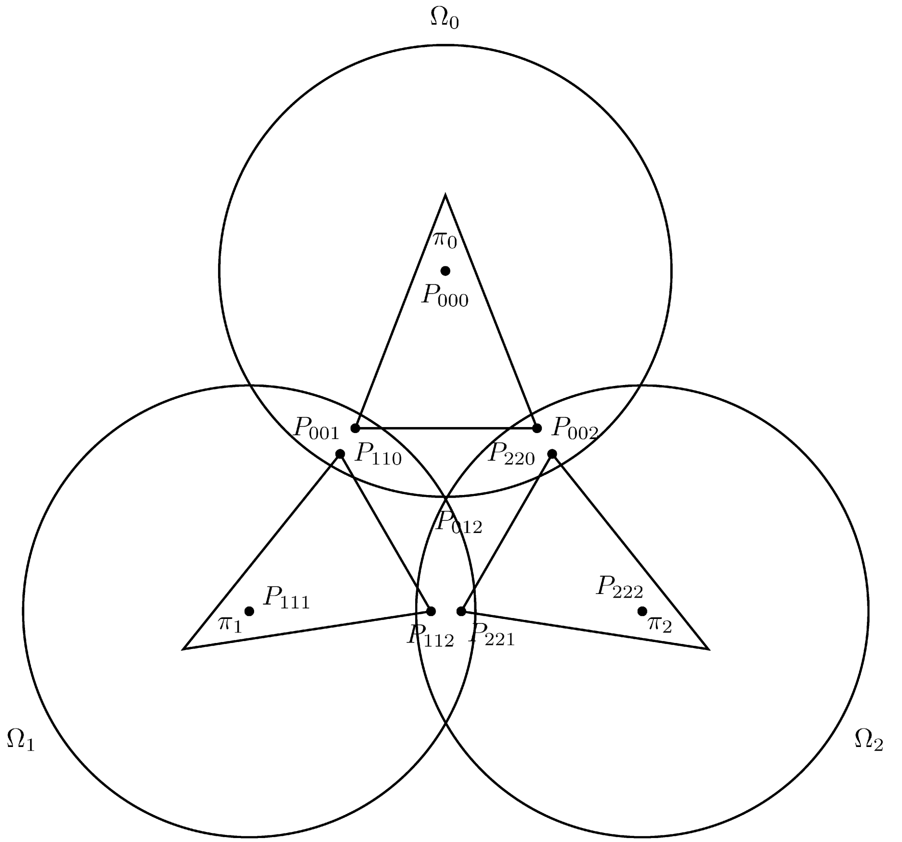

Fig. 2. The three 5-spaces Ω_0, Ω_1, Ω_2 together with the extension planes π_0, π_1 and π_2.

P_{001} and P_{110} are chosen to be non-collinear, π_1 cannot intersect the conic plane generated by the points P_{012}, P_{001}, and P_{221} in a line. Otherwise this line should intersect the line $P_{001}P_{012}$ in a point. The only possible intersection point is $\pi_1 \cap \pi_{01} = P_{110}$, but this is not collinear with P_{001} and P_{012}. Thus P_{012}, P_{221} and P_{112} are non-collinear. The same argument in Ω_2 shows that P_{012}, P_{002} and P_{220} are non-collinear.

Step 2: Construction of the coordinates.

Since we have chosen Ω_0, Ω_1 and Ω_2 such that P_{012}, P_{001} and P_{110} are non-collinear, the planes π_{01}, π_{02} and π_0 must span Ω_0 by the structure of the Veronesean surface V_0 in Ω_0. For, the only candidate for their conic plane when they would define a 4-space is the plane generated by the points P_{001}, P_{012} and P_{002}, which does not contain the contact point P_{110} of π_{01} with respect to V_0. Furthermore, π_{01} is spanned by P_{012}, P_{001}, P_{110}, π_{02} is spanned by P_{012}, P_{002}, P_{220}, and π_0 is spanned by P_{001}, P_{002}, P_{000}, because the contact point P_{000} does not lie in the 4-space defined by Π_{01} and Π_{02}.

Thus Ω_0 is spanned by P_{000}, P_{001}, P_{002}, P_{110}, P_{220} and P_{012}; the points with at least one index zero. Similarly, Ω_1 is spanned by P_{111}, P_{110}, P_{112}, P_{001}, P_{221} and P_{012}, and Ω_2 is spanned by P_{222}, P_{220}, P_{221}, P_{112}, P_{002} and P_{012}, which are the points with at least one index one or two, respectively. Thus the ten points P_{000}, P_{111}, P_{222}, P_{001}, P_{002}, P_{110}, P_{112}, P_{220}, P_{221} and P_{012} span $PG(9,q)$. Choose these points as the vectors $e_0, \dots, e_9$ in this order.

Choose a 5-space Ω of $\mathcal{D}$ different from Ω_0, Ω_1 and Ω_2. We may choose Ω such that $\Omega \cap \Omega_0 \cap \Omega_1$ is a point that does not lie on the lines $P_{001}P_{012}$, $P_{110}P_{012}$ and $P_{001}P_{110}$.

Then Ω intersects Ω_0, Ω_1 and Ω_2 in the planes $\bar{\pi}_0$, $\bar{\pi}_1$ and $\bar{\pi}_2$, respectively. Let $U_0 = (1,0,0,1,1,1,0,1,0,1)$, $U_1 = (0,1,0,1,0,1,1,0,1,1)$, $U_2 = (0,0,1,0,1,0,1,1,1,1)$ be the contact points of the Veronesean surfaces V_0, V_1, V_2 in Ω_0, Ω_1, Ω_2 in the respective planes $\bar{\pi}_0$, $\bar{\pi}_1$, $\bar{\pi}_2$. This indeed is possible since $\bar{\pi}_i$ and $\bar{\pi}_j$ intersect π_{ij} in the same point, namely $\Omega_i \cap \Omega_j \cap \Omega$.

With these choices, the Veronesean surface in Ω_0 is in standard form and has the equation:

$$V_0 = \left(x_0^2, 0, 0, x_0x_1, x_0x_2, x_1^2, 0, x_2^2, 0, x_1x_2\right).$$

Similarly, the Veronesean surfaces in Ω_1 and Ω_2 have the equations

$$V_1 = \left(0, x_1^2, 0, x_0^2, 0, x_1x_0, x_1x_2, 0, x_2^2, x_0x_2\right),$$
$$V_2 = \left(0, 0, x_2^2, 0, x_0^2, 0, x_1^2, x_2x_0, x_2x_1, x_0x_1\right).$$

Step 3: Identification of the 5-spaces.

Now let Ω be a 5-space of $\mathcal{D}$ different from Ω_0, Ω_1 and Ω_2. Then Ω intersects π_{01} in a point Q_{01} with coordinates $(0,0,0,a,0,b,0,0,0,c)$.

In Ω_0, the point Q_{01} lies in the tangent plane $\tilde{\pi}_0$ of the Veronesean surface V_0 with equation

$$\tilde{\pi}_0 : (ax_0, 0, 0, ax_1 + bx_0, ax_2 + cx_0, bx_1, 0, cx_2, 0, bx_2 + cx_1).$$

By the same arguments, we find that the intersection plane $\tilde{\pi}_1$ of Ω with Ω_1 has the equation

$$\tilde{\pi}_1 : (0, bx_1, 0, ax_0, 0, ax_1 + bx_0, cx_1 + bx_2, 0, cx_2, cx_0 + ax_2).$$

Now $\tilde{\pi}_0$ is the intersection of Ω with Ω_0, and Ω intersects π_{02} in the point $Q_{02} = \pi_{02} \cap \tilde{\pi}_0$ with coordinates $(0,0,0,0,a,0,0,c,0,b)$. Consequently, from the description of this point and V_2, the intersection plane $\tilde{\pi}_2$ of Ω and Ω_2 has the equation

$$\tilde{\pi}_2 : (0, 0, cx_2, 0, ax_0, 0, bx_1, cx_0 + ax_2, cx_1 + bx_2, bx_0 + ax_1).$$

Then Ω intersects π_{12} in the point Q_{12} with coordinates $(0,0,0,0,0,0,0,b,0,c,a)$, and Ω also contains the points Q_0, Q_1 and Q_2 with coordinates

$$Q_0 : (a,0,0,b,c,0,0,0,0,0) \in \tilde{\pi}_0,$$
$$Q_1 : (0,b,0,0,0,a,c,0,0,0) \in \tilde{\pi}_1,$$
$$Q_2 : (0,0,c,0,0,0,0,a,b,0) \in \tilde{\pi}_2.$$

As we can see from the coordinates, the points Q_{01}, Q_{02}, Q_{12}, Q_0, Q_1, Q_2 are independent if at least two of the three values a, b and c are non-zero. But this is the case since Ω intersects π_{01} neither in P_{001}, P_{110} or P_{012}. Thus Ω is uniquely defined by the points Q_{01}, Q_{02}, Q_{12}, Q_0, Q_1, Q_2.

Now we can check the definition of $D(P)$ in Eq. (1) to see that the 5-space Ω is the space $D((a,b,c))$. Alternatively, it is possible to use the trilinear form θ from Eq. (2) to check that Q_{01}, Q_{02}, Q_{12}, Q_0, Q_1, Q_2 are the points $\theta((a,b,c), e_i, e_j)$, ($e_i$, e_j are basis vectors).

This proves that Ω is of the form as defined in Construction 1, and discussed in Example 3. □

We know that in every 5-space Π of the regular generalised dual arc $\mathcal{D}$ in $PG(9,q)$, q odd, $q > 3$, with parameters $(9,5,2,0)$, there is one plane extending the set of q^2+q intersection planes of Π with the other 5-spaces of the generalised dual arc to a set of tangent planes of a Veronesean variety V_2^4 in Π.

As indicated in Example 3, it might be possible that these q^2+q+1 extension planes in the q^2+q+1 distinct 5-spaces of the generalised dual arc define a Veronesean variety in a 5-space $\tilde{\Pi}$, extending the generalised dual arc of q^2+q+1 distinct 5-spaces to a generalised dual arc of q^2+q+2 distinct 5-spaces.

This however is impossible, as was shown in Example 3. So we have found the maximal size for a regular generalised dual arc in $PG(9,q)$, q odd, $q > 3$, with parameters $(9,5,2,0)$.

Corollary 18. *A regular generalised dual arc in* $PG(9,q)$, *q odd*, $q>3$, *with parameters* $(9,5,2,0)$ *contains at most* q^2+q+1 *elements.*

Proof. Assume that the dual arc contains at least q^2+q+1 elements. By Theorem 17, these q^2+q+1 elements form a configuration isomorphic to the configuration of Example 3. But we have seen in Example 3 that this configuration cannot be extended. □

5. Applications to cryptography

In this section, we describe an application of generalised dual arcs in cryptography.
Let us recall the definition of a message authentication code [5].

Definition 19. A *message authentication code* (*MAC*) is a 4-tuple $(\mathcal{S},\mathcal{A},\mathcal{K},\mathcal{E})$ with:

1. $\mathcal{S}$ a finite set of source states (messages).
2. $\mathcal{A}$ a finite set of authentication tags.
3. $\mathcal{K}$ a finite set of keys.
4. For each $K\in\mathcal{K}$, we have an authentication rule $e_K\in\mathcal{E}$ with $e_K:\mathcal{S}\to\mathcal{A}$.

The security of a MAC is measured by the following probabilities.

Definition 20. Let p_i denote the probability of an attacker to construct a pair $(s,e_K(s))$ without knowledge of the key K, if he only knows i different pairs $(s_j,e_K(s_j))$. The smallest value r for which $p_{r+1}=1$ is called the *order* of the scheme.

For $r=1$, the probability p_0 is also known as the probability of an *impersonation attack* and the probability p_1 is called the probability of a *substitution attack*.

The next theorem bounds the number of keys by the attack probabilities. For $r=1$ and $p_0=p_1$, it is stated in [2], and for arbitrary r with $p_0=p_1=\cdots=p_r$, it was proven in [1].

Theorem 21. *If a MAC has attack probabilities* $p_i=1/n_i$ $(0\leqslant i\leqslant r)$, *then* $|\mathcal{K}|\geqslant n_0\cdots n_r$.

Proof. Suppose that we send the messages $(s_1,e_K(s_1)),\dots,(s_r,e_K(s_r))$. Let $\mathcal{K}_i$ be the set of all keys which give the same authentication tag for the first i messages, i.e.

$$\mathcal{K}_i=\bigl\{\hat{K}\in\mathcal{K}\bigm| e_{\hat{K}}(s_j)=e_K(s_j)\text{ for } j\leqslant i\bigr\}.$$

By definition, we have $\mathcal{K}_0=\mathcal{K}$. Formally, we define $\mathcal{K}_{r+1}=\{K\}$.

An attacker who knows the first i messages can create a false signature by guessing a key $\hat{K}\in\mathcal{K}_i$ and computing $e_{\hat{K}}(s_{i+1})$. The attack is successful if $\hat{K}\in\mathcal{K}_{i+1}$. Therefore

$$p_i\leqslant\frac{|\mathcal{K}_{i+1}|}{|\mathcal{K}_i|}.$$

Multiplying these inequalities proves the theorem. □

A MAC that satisfies this theorem with equality is called *perfect*.

Theorem 22. *Let* $p_i=1/n_i$, *with* $n_i\in\mathbb{N}$. *If a MAC has* $|\mathcal{K}|=n_0\cdot\cdots\cdot n_r$, *then* $|\mathcal{S}|\leqslant\frac{n_{r-1}n_r-1}{n_r-1}+r-1$.

Proof. After $r-1$ messages, the number of possible keys is reduced to $n_{r-1}n_r$. After $r-1$ messages, we call the possible keys *points*. A set of points that produce the same authentication tag for an rth message will be called a *block*.

Since the MAC is perfect, we know that two blocks have at most one common point, because otherwise the probability $p_r \geqslant 2/n_r$. The equation $p_r = 1/n_r$ says that each block contains at least n_r points, and $p_{r-1} = 1/n_{r-1}$ says that each block belongs to a parallel class of at least n_{r-1} blocks. It follows that every point lies on at most $(n_{r-1}n_r - 1)/(n_r - 1)$ blocks. This bounds the number of remaining messages, since every message defines a unique block. $\square$

Now we show how to use generalised dual arcs to construct perfect MACs.

Theorem 23. *Let Π be a hyperplane of $PG(n+1,q)$ and let $\mathcal{D}$ be a generalised dual arc of order l in Π with parameters $(n, d_1, \ldots, d_{l+1})$.*

The elements of $\mathcal{D}$ are the messages and the points of $PG(n+1,q)$ not in Π are the keys. The authentication tag that belongs to a message and a key is the generated (d_1+1)-dimensional subspace.

This defines a perfect MAC of order $r = l+1$ with attack probabilities

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

Proof. After i message tag pairs $(m_1,t_1),\ldots,(m_i,t_i)$ are sent, the attacker knows that the key must lie in the (d_i+1)-dimensional space $\pi = t_1 \cap \cdots \cap t_i$. This space contains q^{d_i+1} different keys. A message m_{i+1} intersects $m_1 \cap \cdots \cap m_i$ in a d_{i+1}-dimensional space π'. Two keys K and $\bar{K}$ generate the same authentication tag if and only if K and $\bar{K}$ generate together with π' the same $(d_{i+1}+1)$-dimensional space. Thus the keys form groups of size $q^{d_{i+1}+1}$ and keys from the same group give the same authentication tag.

The attacker has to guess a group. The probability to guess the correct group is $p_i = q^{d_{i+1}+1}/q^{d_i+1}$. $\square$

Acknowledgments

The research of the second and third author takes place within the project "Linear codes and cryptography" of the Fund for Scientific Research Flanders (FWO-Vlaanderen) (Project No. 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.

References

[1] V. Fåk, Repeated use of codes which detect deception, IEEE Trans. Inform. Theory IT-25 (2) (1979) 233–234.
[2] E.N. Gilbert, Codes which detect deception, Bell Syst. Tech. J. 53 (3) (1974) 405–421.
[3] J.W.P. Hirschfeld, Projective Geometries over Finite Fields, second edition, Oxford Math. Monogr., Clarendon Press/Oxford Univ. Press, New York, 1998.
[4] J.W.P. Hirschfeld, J.A. Thas, General Galois Geometries, Oxford Math. Monogr., Clarendon Press/Oxford Univ. Press, New York, 1991.
[5] D. Pei, Authentication Codes and Combinatorial Designs, Discrete Math. Appl. (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2006.
[6] B. Segre, Introduction to Galois geometries, Atti Accad. Naz. Lincei Mem. Cl. Sci. Fis. Mat. Natur. Sez. I (8) 8 (1967) 133–236.
[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. Natur. (8) 24 (1958) 19–23, 135–138.