A note on Segre varieties in characteristic two

Hans Havlicek

TECHNISCHE UNIVERSITÄT WIEN
Vienna University of Technology

Research Group
Differential Geometry and Geometric Structures
Institute of Discrete Mathematics and Geometry

Workshop & Summer School on Finite Semifields, Padova,
September 13th, 2013

Joint work with
Boris Odehnal (Vienna) and Metod Saniga (Tatranská Lomnica)

Our Segre varieties

Let $\boldsymbol{V}_1, \boldsymbol{V}_2, \ldots, \boldsymbol{V}_m$ be $m \geq 1$ two-dimensional vector spaces over a commutative field F.

$\mathbb{P}(\boldsymbol{V}_k) = \mathrm{PG}(1, F)$ are projective lines over F for $k \in \{1, 2, \ldots, m\}$.

The non-zero decomposable tensors of $\bigotimes_{k=1}^{m} \boldsymbol{V}_k$ determine the *Segre variety*

$$\mathcal{S}_{\underbrace{1,1,\ldots,1}_{m}}(F) = \mathcal{S}_{(m)}(F) = \left\{ F\boldsymbol{a}_1 \otimes \boldsymbol{a}_2 \otimes \cdots \otimes \boldsymbol{a}_m \mid \boldsymbol{a}_k \in \boldsymbol{V}_k \setminus \{0\} \right\}$$

with ambient projective space $\mathbb{P}\left(\bigotimes_{k=1}^{m} \boldsymbol{V}_k\right) = \mathrm{PG}(2^m - 1, F)$.

Bases

Given a basis $(\boldsymbol{e}_0^{(k)}, \boldsymbol{e}_1^{(k)})$ for each vector space $\boldsymbol{V}_k$, $k \in \{1, 2, \ldots, m\}$, the tensors

$$\boldsymbol{E}_{i_1, i_2, \ldots, i_m} := \boldsymbol{e}_{i_1}^{(1)} \otimes \boldsymbol{e}_{i_2}^{(2)} \otimes \cdots \otimes \boldsymbol{e}_{i_m}^{(m)} \quad \text{with} \quad (i_1, i_2, \ldots, i_m) \in I_m := \{0, 1\}^m \tag{1}$$

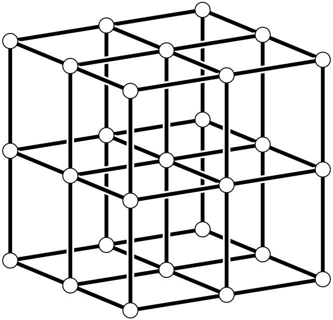
constitute a basis of $\bigotimes_{k=1}^{m} \boldsymbol{V}_k$.

For any multi-index $\boldsymbol{i} = (i_1, i_2, \ldots, i_m) \in I_m$ the *opposite* multi-index $\boldsymbol{i}' \in I_m$ is characterised by

$$i_k \neq i'_k \quad \text{for all} \quad k \in \{1, 2, \ldots, m\}.$$

Examples

- $\mathcal{S}_1(F) = \mathrm{PG}(1, F)$.
- $\mathcal{S}_{1,1}(F)$ is a hyperbolic quadric of $\mathrm{PG}(3, F)$.
- $\mathcal{S}_{1,1,1}(2)$ has 27 points and contains precisely 27 lines (three through each point). The ambient $\mathrm{PG}(7, 2)$ has 255 points.



Collineations

The subgroup of $\mathrm{GL}\left(\bigotimes_{k=1}^{m} \boldsymbol{V}_k\right)$ preserving decomposable tensors is generated by the following transformations:

$$f_1 \otimes f_2 \otimes \cdots \otimes f_m \quad \text{with} \quad f_k \in \mathrm{GL}(\boldsymbol{V}_k) \text{ for } k \in \{1, 2, \ldots, m\}. \qquad (2)$$

$$f_\sigma \quad \text{with} \quad \boldsymbol{E}_{(i_1, i_2, \ldots, i_m)} \mapsto \boldsymbol{E}_{(i_{\sigma^{-1}(1)}, i_{\sigma^{-1}(2)}, \ldots, i_{\sigma^{-1}(m)})} \quad \text{for all} \quad \boldsymbol{i} \in I_m, \qquad (3)$$

where $\sigma \in S_m$ is arbitrary.

This subgroup induces the stabiliser $G_{\mathcal{S}_{(m)}(F)}$ of the Segre $\mathcal{S}_{(m)}(F)$ within the projective group $\mathrm{PGL}\left(\bigotimes_{k=1}^{m} \boldsymbol{V}_k\right)$.

Bilinear forms

Each of the vector spaces $\boldsymbol{V}_k$ admits a symplectic bilinear form

$$[\cdot,\cdot] : \boldsymbol{V}_k \times \boldsymbol{V}_k \to F.$$

Consequently, $\bigotimes_{k=1}^{m} \boldsymbol{V}_k$ is equipped with a bilinear form which is given by

$$\left[\boldsymbol{a}_1 \otimes \boldsymbol{a}_2 \otimes \cdots \otimes \boldsymbol{a}_m, \boldsymbol{b}_1 \otimes \boldsymbol{b}_2 \otimes \cdots \otimes \boldsymbol{b}_m\right] := \prod_{k=1}^{m} [\boldsymbol{a}_k, \boldsymbol{b}_k] \quad \text{for } \boldsymbol{a}_k, \boldsymbol{b}_k \in \boldsymbol{V}_k, \tag{4}$$

and extending bilinearly.

All these bilinear forms are unique up to a non-zero factor in F.

Bilinear forms (cont.)

Given $\boldsymbol{i}, \boldsymbol{j} \in I_m$ we have

$$
\begin{aligned}
[\boldsymbol{E_i}, \boldsymbol{E_{i'}}] &= \prod_{k=1}^{m} [\boldsymbol{e}_{i_k}^{(k)}, \boldsymbol{e}_{i'_k}^{(k)}] = (-1)^m [\boldsymbol{E_{i'}}, \boldsymbol{E_i}] \neq 0, && (5) \\
[\boldsymbol{E_i}, \boldsymbol{E_j}] &= 0 \quad \text{for all} \quad \boldsymbol{j} \neq \boldsymbol{i}'. && (6)
\end{aligned}
$$

Hence the form $[\cdot,\cdot]$ on $\bigotimes_{k=1}^{m} \boldsymbol{V}_k$ is non-degenerate. Furthermore, it is

- symmetric when m is even and $\mathrm{Char}\, F \neq 2$;
- alternating otherwise (*i. e.*, when m is odd or $\mathrm{Char}\, F = 2$).

The fundamental polarity

In projective terms the form $[\cdot,\cdot]$ on $\bigotimes_{k=1}^{m} \boldsymbol{V}_k$ (or any proportional one) determines the fundamental polarity of the Segre $\mathcal{S}_{(m)}(F)$, *i. e.*, a polarity of $\mathbb{P}(\bigotimes_{k=1}^{m} \boldsymbol{V}_k)$ which sends $\mathcal{S}_{(m)}(F)$ to its dual.

This polarity is

- associated with a regular quadric when m is even and $\operatorname{Char} F \neq 2$;
- null otherwise (*i. e.*, when m is odd or $\operatorname{Char} F = 2$).

The associated quadric

Let m be even and $\mathrm{Char}\, F \neq 2$.

The mapping

$$Q : \bigotimes_{k=1}^{m} \boldsymbol{V}_k \to F : \boldsymbol{X} \mapsto [\boldsymbol{X}, \boldsymbol{X}]$$

is a quadratic form with Witt index 2^{m-1} and rank 2^m.

The fundamental polarity of the Segre $\mathcal{S}_{(m)}(F)$ is the polarity of the regular quadric given by Q.

The Segre coincides with this quadric precisely when $m = 2$.

Characteristic two

Let $\operatorname{Char} F = 2$.

Here $[\cdot,\cdot]$ is a symplectic bilinear form on $\bigotimes_{k=1}^{m} \boldsymbol{V}_k$ for all $m \geq 1$, whence the fundamental polarity of the Segre $\mathcal{S}_{(m)}(F)$ is always null.

Furthermore, (5) simplifies to

$$[\boldsymbol{E}_{\boldsymbol{i}}, \boldsymbol{E}_{\boldsymbol{i}'}] = \prod_{k=1}^{m} [\boldsymbol{e}_0^{(k)}, \boldsymbol{e}_1^{(k)}] = [\boldsymbol{E}_{\boldsymbol{i}'}, \boldsymbol{E}_{\boldsymbol{i}}] \neq 0. \tag{7}$$

A quadratic form

Proposition

Let $m \geq 2$ and $\mathrm{Char}\, F = 2$. Then there is a unique quadratic form

$$Q : \bigotimes_{k=1}^{m} \boldsymbol{V}_k \to F$$

satisfying the following two properties:

1. *Q vanishes for all decomposable tensors.*
2. *The symplectic bilinear form*

$$[\cdot,\cdot] : \bigotimes_{k=1}^{m} \boldsymbol{V}_k \times \bigotimes_{k=1}^{m} \boldsymbol{V}_k \to F$$

   is the polar form of Q.

Proof

We denote by $I_{m,0}$ the set of all multi-indices $(i_1, i_2, \ldots, i_m) \in I_m$ with $i_1 = 0$.

In terms of our basis (1) a quadratic form is given by

$$Q : \bigotimes_{k=1}^{m} \boldsymbol{V}_k \to F : \boldsymbol{X} \mapsto \sum_{\boldsymbol{i} \in I_{m,0}} \frac{[\boldsymbol{E}_{\boldsymbol{i}}, \boldsymbol{X}][\boldsymbol{E}_{\boldsymbol{i}'}, \boldsymbol{X}]}{[\boldsymbol{E}_{\boldsymbol{i}}, \boldsymbol{E}_{\boldsymbol{i}'}]}. \tag{8}$$

Proof (cont.)

Given an arbitrary decomposable tensor we have

$$
\begin{aligned}
Q(\boldsymbol{a}_1 \otimes \cdots \otimes \boldsymbol{a}_m) &= \sum_{\boldsymbol{i} \in I_{m,0}} \frac{[\boldsymbol{E}_{\boldsymbol{i}}, \boldsymbol{a}_1 \otimes \cdots \otimes \boldsymbol{a}_m][\boldsymbol{E}_{\boldsymbol{i}'}, \boldsymbol{a}_1 \otimes \cdots \otimes \boldsymbol{a}_m]}{[\boldsymbol{E}_{\boldsymbol{i}}, \boldsymbol{E}_{\boldsymbol{i}'}]} \\
&= \sum_{\boldsymbol{i} \in I_{m,0}} \frac{[\mathbf{e}_0^{(1)}, \boldsymbol{a}_1][\mathbf{e}_1^{(1)}, \boldsymbol{a}_1] \cdots [\mathbf{e}_0^{(m)}, \boldsymbol{a}_m][\mathbf{e}_1^{(m)}, \boldsymbol{a}_m]}{[\mathbf{e}_0^{(1)}, \mathbf{e}_1^{(1)}] \cdots [\mathbf{e}_0^{(m)}, \mathbf{e}_1^{(m)}]} \\
&= 2^{m-1} \frac{[\mathbf{e}_0^{(1)}, \boldsymbol{a}_1][\mathbf{e}_1^{(1)}, \boldsymbol{a}_1] \cdots [\mathbf{e}_0^{(m)}, \boldsymbol{a}_m][\mathbf{e}_1^{(m)}, \boldsymbol{a}_m]}{[\mathbf{e}_0^{(1)}, \mathbf{e}_1^{(1)}] \cdots [\mathbf{e}_0^{(m)}, \mathbf{e}_1^{(m)}]} \\
&= 0,
\end{aligned}
$$

where we used (7), $\# I_{m,0} = 2^{m-1}$, $m \geq 2$, and $\operatorname{Char} F = 2$. This verifies property 1.

Proof (cont.)

Let $\boldsymbol{j}, \boldsymbol{k} \in I$ be arbitrary multi-indices. Polarising Q gives

$$\begin{aligned} Q(\boldsymbol{E_j}+\boldsymbol{E_k})+Q(\boldsymbol{E_j})+Q(\boldsymbol{E_k}) &= Q(\boldsymbol{E_j}+\boldsymbol{E_k})+0+0 \\ &= \sum_{\boldsymbol{i}\in I_{m,0}} \frac{[\boldsymbol{E_i},\boldsymbol{E_j}+\boldsymbol{E_k}][\boldsymbol{E_{i'}},\boldsymbol{E_j}+\boldsymbol{E_k}]}{[\boldsymbol{E_i},\boldsymbol{E_{i'}}]}. \end{aligned}$$

The numerator of a summand of the above sum can only be different from zero if

$$\boldsymbol{i} \in \{\boldsymbol{j}',\boldsymbol{k}'\} \text{ and } \boldsymbol{i}' \in \{\boldsymbol{j}',\boldsymbol{k}'\}.$$

These conditions can only be met for $\boldsymbol{k} = \boldsymbol{j}'$, whence in fact at most one summand, namely the one with $\boldsymbol{i} \in \{\boldsymbol{j},\boldsymbol{j}'\} \cap I_{m,0}$ can be non-zero.

Proof (cont.)

So

$$Q(\boldsymbol{E_j} + \boldsymbol{E_k}) + Q(\boldsymbol{E_j}) + Q(\boldsymbol{E_k}) = 0 = [\boldsymbol{E_j}, \boldsymbol{E_k}] \quad \text{for} \quad \boldsymbol{k} \neq \boldsymbol{j}'.$$

Irrespective of whether $\boldsymbol{i} = \boldsymbol{j}$ or $\boldsymbol{i} = \boldsymbol{j}'$, we have

$$Q(\boldsymbol{E_j}+\boldsymbol{E_{j'}})+Q(\boldsymbol{E_j})+Q(\boldsymbol{E_{j'}}) = \frac{[\boldsymbol{E_j}, \boldsymbol{E_j} + \boldsymbol{E_{j'}}][\boldsymbol{E_{j'}}, \boldsymbol{E_j} + \boldsymbol{E_{j'}}]}{[\boldsymbol{E_j}, \boldsymbol{E_{j'}}]} = [\boldsymbol{E_j}, \boldsymbol{E_{j'}}].$$

This implies that the quadratic form Q polarises to $[\cdot, \cdot]$, *i. e.*, also the second property is satisfied.

Proof (cont.)

Let $\widetilde{Q}$ be a quadratic form satisfying properties 1 and 2. Hence the polar form of $Q - \widetilde{Q} = Q + \widetilde{Q}$ is zero.

We consider F as a vector space over its subfield $F^\square$ comprising all squares in F. So

$$(Q + \widetilde{Q}) : \bigotimes_{k=1}^{m} \boldsymbol{V}_k \to F$$

is a semilinear mapping with respect to the field isomorphism $F \to F^\square : x \mapsto x^2$.

The kernel of $Q + \widetilde{Q}$ is a subspace of $\bigotimes_{k=1}^{m} \boldsymbol{V}_k$ which contains all decomposable tensors and, in particular, our basis (1). Hence $Q + \widetilde{Q}$ vanishes on $\bigotimes_{k=1}^{m} \boldsymbol{V}_k$, and $Q = \widetilde{Q}$ as required. $\square$

Explicit equation

From (8) and (7), the quadratic form Q can be written in terms of tensor coordinates $x_{\boldsymbol{j}} \in F$ as

$$Q\Big(\sum_{\boldsymbol{j}\in I_m} x_{\boldsymbol{j}}\boldsymbol{E}_{\boldsymbol{j}}\Big) = \sum_{\boldsymbol{i}\in I_{m,0}} [\boldsymbol{E}_{\boldsymbol{i}}, \boldsymbol{E}_{\boldsymbol{i}'}] x_{\boldsymbol{i}} x_{\boldsymbol{i}'} = \prod_{k=1}^{m} [\boldsymbol{e}_0^{(k)}, \boldsymbol{e}_1^{(k)}] \cdot \sum_{\boldsymbol{i}\in I_{m,0}} x_{\boldsymbol{i}} x_{\boldsymbol{i}'}. \tag{9}$$

Remarks

The previous results may be slightly simplified by taking symplectic bases, *i. e.*,

$$[\boldsymbol{e}_0^{(k)}, \boldsymbol{e}_1^{(k)}] = 1 \text{ for all } k \in \{1, 2, \ldots, m\},$$

whence also

$$[\boldsymbol{E}_{\boldsymbol{i}}, \boldsymbol{E}_{\boldsymbol{i}'}] = 1 \text{ for all } \boldsymbol{i} \in I_m.$$

Proposition 1 fails to hold for $m = 1$: A quadratic form Q vanishing for all decomposable tensors of $\boldsymbol{V}_1$ is necessarily zero, since any element of $\boldsymbol{V}_1$ is decomposable. Hence the polar form of such a Q cannot be non-degenerate.

Main result

Theorem

Let $m \geq 2$ and $\mathrm{Char}\, F = 2$. There exists in the ambient space of the Segre $\mathcal{S}_{(m)}(F)$ a regular quadric $\mathcal{Q}(F)$ with the following properties:

1. *The projective index of $\mathcal{Q}(F)$ is $2^{m-1} - 1$.*
2. *$\mathcal{Q}(F)$ is invariant under the group of projective collineations stabilising the Segre $\mathcal{S}_{(m)}(F)$.*

Proof

Any $f_k \in \mathrm{GL}(\boldsymbol{V}_k)$, $k \in \{1, 2, \dots, m\}$, preserves the symplectic form $[\cdot, \cdot]$ on $\boldsymbol{V}_k$ up to a non-zero factor.

Any linear bijection f_σ as in (3) is a symplectic transformation of $\bigotimes_{k=1}^{m} \boldsymbol{V}_k$.

Hence any transformation from the stabiliser group $G_{\mathcal{S}_{(m)}(F)}$ preserves the symplectic form (4) up to a non-zero factor.

By the proposition, also Q is invariant up to a non-zero factor under the action of $G_{\mathcal{S}_{(m)}(F)}$.

Proof (cont.)

From (9) the linear span of the tensors $\boldsymbol{E}_{\boldsymbol{j}}$ with $\boldsymbol{j}$ ranging in $I_{m,0}$ is a singular subspace with respect to Q.

So the Witt index of Q equals $\#I_{m,0} = 2^{m-1}$, because $[\cdot,\cdot]$ being non-degenerate implies that a greater value is impossible.

We conclude that the quadric with equation $Q(\boldsymbol{X}) = 0$ has all the required properties. $\square$

Conclusion

We call $\mathcal{Q}(F)$ the *invariant quadric* of the Segre $\mathcal{S}_{(m)}(F)$.

The case $m = 2$ deserves special mention, as the Segre $\mathcal{S}_{1,1}(F)$ coincides with its invariant quadric $\mathcal{Q}(F)$ given by

$$Q\Big(\sum_{\boldsymbol{j} \in I_2} x_{\boldsymbol{j}} \boldsymbol{E}_{\boldsymbol{j}}\Big) = x_{00}x_{11} + x_{01}x_{10} = 0.$$

This result parallels the situation for $\operatorname{Char} F \neq 2$.

Problem: Is there a "better" definition of the quadratic form Q?

References

This presentation:

H. Havlicek, B. Odehnal, and M. Saniga.
On invariant notions of Segre varieties in binary projective spaces.
Des. Codes Cryptogr. 62 (2012), 343–356.

References (cont.)

Related Work ($F = \mathrm{GF}(2)$, $m = 3$):

R. M. Green and M. Saniga.
The Veldkamp space of the smallest slim dense near hexagon.
Int. J. Geom. Methods Mod. Phys. 10(2) (2013), 1250082, 15 pp.

R. Shaw, N. Gordon, and H. Havlicek.
Aspects of the Segre variety $\mathcal{S}_{1,1,1}(2)$.
Des. Codes Cryptogr. 62 (2012), 225–239.

R. Shaw, N. Gordon, and H. Havlicek.
Tetrads of lines spanning $\mathrm{PG}(7, 2)$.
Simon Stevin, in print.