Remark on a paper by J.W.P. Hirschfeld

bg6565

TECHNISCHE HOGESCHOOL EINDHOVEN

Onderafdeling der Wiskunde

Memorandum 1976-08

mei 1976

Remark on a paper by J.W.P. Hirschfeld

by

J.J.M. Cuppen

Technische Hogeschool
Onderafdeling der Wiskunde
PO Box 513, Eindhoven
Nederland

1. Introduction

In the paper: Ovals in Desarguesian Planes of Even Order [1] Hirschfeld shows (theorem 4, corollary 1) that there exist no more projectively distinct ovals with representation D(k) than D(2), D(4) and D(6). Below we shall show that the ovals, thus represented, are indeed mutually projectively distinct.

2. Preliminary considerations

In this paper we shall restrict ourselves to ovals $\mathcal{O}$ in PG(2,32) which have a representation of the form D(k) (for definitions and notation see [1], p. 79).

Representations D(k) of an oval $\mathcal{O}$ in PG(2,32) depend completely on the frame used to define a coordinate system in PG(2,32).*) We shall only use frames (P,Q,R,S) with $P = (0,0,1)$, $Q = (0,1,0)$, $R = (1,0,0)$, $S = (1,1,1)$ where P, Q, R and S all are points on the oval $\mathcal{O}$ under consideration.

Let $\mathcal{O}$ be an oval with representation D(k) for a suitable frame (P,Q,R,S). Let $a \in \gamma_0$ ($\gamma = GF(32)$). Since

$$\{(1,t,t^k) \mid t \in \gamma\} = \{(1,a^{-1}t,(a^{-1}t)^k \mid t \in \gamma\} = \{(1,a^{-1}t,a^{-k}t^{-k} \mid t \in \gamma\} .$$

D(k) is also the representation of $\mathcal{O}$ for any frame (P,Q,R,S') with $S' \notin \{P,Q,R\}$, S' on $\mathcal{O}$ (for the frame (P,Q,R,S): $S' = (1,a,a^k)$). (1)

If $\mathcal{O}$ has a representation as a translation oval and this representation is D(k) then by definition ([1], p. 79) we have for $a \in \gamma$:

$$\{(1,t,t^k) \mid t \in \gamma\} = \{1,(t+a),(t+a)^k \mid t \in \gamma\} = \{(1,t+a,t^k+a^k) \mid t \in \gamma\}$$

so if D(k) is the representation of $\mathcal{O}$ for some frame (P,Q,R,S) it is also the representation of $\mathcal{O}$ for any frame (P,Q,R',S) with $R' \in \mathcal{O}\backslash\{P,Q,S\}$ and with (1) for any frame (P,Q,R',S') with $\{R',S'\} \subset \mathcal{O}\backslash\{P,Q\}$ $(R' = (1,a,a^k))$. (2)

If $\mathcal{O}$ has representation D(2) for some frame (P,Q,R,S) then $\mathcal{O}$ has also representation D(2) for the frame (R,Q,P,S) since

$$\{(1,t,t^2) \mid t \in \gamma_0\} = \{(1,t^{-1},t^{-2}) \mid t \in \gamma_0\} = \{(t^2,t,1) \mid t \in \gamma_0\}$$

and the transformation $(x_0,x_1,x_2) \to (x_2,x_1,x_0)$ belongs to the transition

*) field automorphisms φ of γ have the form φ: $t \to t^j$, $1 \le j \le 30$, and $D(k) = \{(1,t,t^k) \mid t \in \gamma\} \cup \{(010),(001)\} = \{(1,t^j,(t^j)^k) \mid t \in \gamma\} \cup \{(010),(001)\} =$
$= \{(1,t^j,(t^k)^j) \mid t \in \gamma\} \cup \{(010),(001)\}$.

from frame (P,Q,R,S) to frame (R,Q,P,S). From (1) and (2) and the fact that $(x + y)^2 = x^2 + y^2$ for all x and y in γ we can conclude that $\mathcal{O}$ has representation D(2) for any frame (P',Q,R',S') on $\mathcal{O}$. (3)
A transformation will always work on coordinates, not on the points themselves.

3. Representations equivalent to D(2)

Let $\mathcal{O}$ be an oval with representation D(k) for the frame (P_k,Q_k,R_k,S_k) on $\mathcal{O}$ and representation D(2) for the frame (P_2,Q_2,R_2,S_2) on $\mathcal{O}$. We shall show that exactly one of the following three cases holds (4)

i) $k = 2$, $Q_k = Q_2$ and D(k) is the representation of $\mathcal{O}$ for any frame (P_k',Q_k,R_k',S_k') on $\mathcal{O}$,

ii) $k = 16$, $R_k = Q_2$ and D(k) is the representation of $\mathcal{O}$ for any frame (P_k',Q_k',R_k,S_k') on $\mathcal{O}$,

iii) $k = 30$, $P_k = Q_2$ and D(k) is the representation of $\mathcal{O}$ for any frame (P_k,Q_k',R_k',S_k') on $\mathcal{O}$.

Now assume $Q_k \neq Q_2$. Let $Q_k' \in \mathcal{O}\setminus\{P_k,R_k,Q_2\}$. We can choose R and S on $\mathcal{O}$ and, if necessary, change S_k (with (1)) in such a way that $\{P_k,R_k,S_k\} = \{Q_2,R,S\}$. Now of course $\{Q_k,Q_k',Q_2\} \cap \{R,S\} = \emptyset$. We have: For the frames (Q_k,Q_2,R,S) and (P_k,Q_k,R_k,S_k) the oval $\mathcal{O}$ has representations D(2) and D(k), respectively.

The transformation T which satisfies for the frame (Q_k,Q_2,R,S) $TP_k = (001)$, $TQ_k = (010)$, $TR_k = (100)$, $TS_k = (111)$ has also $TD(2) = D(k)$ since $\mathcal{O}$ has representation D(k) for the frame (P_k,Q_k,R_k,S_k).
For the frame (Q_k',Q_2,R,S) the oval $\mathcal{O}$ has representation D(2) (by (3)) and P_k, R_k and S_k have the same coordinates as for the frame (Q_k,Q_2,R,S). So, for (Q_k',Q_2,R,S), $T(P_k,Q_k',R_k,S_k) = ((001),(010),(100),(111))$. For this frame $\mathcal{O}$ has representation $TD(2) = D(k)$. So we can conclude:

> If $\mathcal{O}$ has representation D(k) for some frame (P_k,Q_k,R_k,S_k) and $Q_k \neq Q_2$ then $\mathcal{O}$ has this representation for any frame (P_k,Q_k',R_k,S_k) on $\mathcal{O}$ with $Q_k' \neq Q_2$.

The same argument for the cases $P_k \neq Q_2$ and $R_k \neq Q_2$ leads to a similar conclusion for P_k and R_k.

Now consider the following cases:

i) $P_k \neq Q_2$ and $R_k \neq Q_2$. Now we are free to choose $P'_k = R_k$ and $R'_k = P_k$ and know that $\mathcal{O}$ has representation D(k) for the frame (P'_k, Q_k, R'_k, S_k). This yields:

$$\forall_{t\in\gamma_0} \exists_{s\in\gamma_0} [(1,t,t^k) = (s^k,s,1)], \text{ so } \forall_{s\in\gamma_0} [(s^{1-k})^k = s^{-k}],$$

so $k(1-k) \equiv -k \pmod{31}$, so $k = 0$ or $k = 2$.
Since D(0) represents no oval we find $k = 2$.

ii) $P_k \neq Q_2$ and $Q_k \neq Q_2$. We choose $P'_k = Q_k$ and $Q'_k = P_k$ and get:

$$\forall_{t\in\gamma} \exists_{s\in\gamma} [(1,t,t^k) = (1,s^k,s)] \text{ so } \forall_{s\in\gamma} [s^{k^2} = s]$$

so $k^2 \equiv 1 \pmod{31}$ so $k = 1$ or $k = 30$.
Since D(1) represents no oval we find $k = 30$ (with [1], theorem 1, p. 81).
But this result excludes that of i) so we may conclude: $R_k = Q_2$ and in case i): $Q_k = Q_2$.
Now the only other possibility is:

iii) $P_k = Q_2$. We choose $Q'_k = R_k$ on $R'_k = Q_k$ we find:

$$\forall_{t\in\gamma_0} \exists_{s\in\gamma_0} [(1,t,t^k) = (s,1,s^k)] \text{ so } \forall_{s\in\gamma_0} [s^{-k} = s^{k-1}]$$

so $-k \equiv k-1 \pmod{31}$ so $k = 16$.
To prove (4) we still have to show that D(16) and D(30) are indeed representations of $\mathcal{O}$. This follows in exactly the same manner:

$$\{(1,t,t^2) \mid t \in \gamma\} = \{(1,t^{16},t) \mid t \in \gamma\}$$

so if D(2) is the representation of $\mathcal{O}$ for (P,Q,R,S) then D(16) is the representation for (Q,P,R,S) and:

$$\{(1,t,t^2) \mid t \in \gamma_0\} = \{(t^{-1},1,t) \mid t \in \gamma_0\} = \{(t^{30},1,t) \mid t \in \gamma_0\}$$

so if D(2) is the representation of $\mathcal{O}$ for the frame (P,Q,R,S) then D(30) is the representation of $\mathcal{O}$ for the frame (R,P,Q,S). q.e.d.

With (4) we have directly: The only representations D(k) equivalent with D(2) are: D(2), D(16) and D(30).

4. The relation between the representations D(4) and D(6)

In this section we shall show that the assumption $D(4) \sim D(6)$ leads to a contradiction.

Assume that there exists an oval $\mathcal{O}$ with representations D(4) and D(6) for the frames (P_4,Q_4,R_4,S_4) and (P_6,Q_6,R_6,S_6) respectively.
We distinguish two cases:

i) $\{P_4,Q_4\} \cap \{P_6,Q_6,R_6\} \neq \emptyset$.
With (1) and (4) we can choose R_4, S_4 and S_6 such that $\{P_4,Q_4,R_4,S_4\} = \{P_6,Q_6,R_6,S_6\}$.
Let T be the transformation with respect to (P_4,Q_4,R_4,S_4) with $TP_6 = P_4$, $TQ_6 = Q_4$, $TR_6 = R_4$, $TS_6 = S_4$ and $TD(4) = D(6)$. Now $R_4 \neq S_6$ or $S_4 \neq S_6$, say $R_4 \neq S_6$.
Then $P_6 = R_4$ or $Q_6 = R_4$ or $R_6 = R_4$, say $P_6 = P_4$.
Let $P_6' \in \mathcal{O}\backslash\{P_6,Q_6,R_6,S_6\}$. Now (P_4,Q_4,P_6',S_4) is a frame for which $\mathcal{O}$ has representation D(4). Also for this frame $T(P_6',Q_6,R_6,S_6) = (001),(101),(100),(111))$ and $\mathcal{O}$ has representation $TD(4) = D(6)$ for this frame. This implies:
If $P_6 = R_4$ then for any frame (P_6',Q_6,R_6,S_6) $\mathcal{O}$ has representation D(6).
By applying the same argument we get:
If P_6 (Q_6 or R_6) $\in \{R_4,S_4\}$ then $\mathcal{O}$ has representation D(6) for any frame (P_6',Q_6,R_6,S_6) on $\mathcal{O}$ ((P_6,Q_6',R_6,S_6) or (P_6,Q_6,R_6',S_6) resp.). The conclusion is that in the frame that yields representation D(6) for $\mathcal{O}$ we can choose besides S_6 (with (1)) at least one other point arbitrarily.

i1) If this point is R_6 then we can transform via $(P_6,Q_6,R_6,S_6) \to (P_6,Q_6,S_6,R_6)$ and we get:

$$\forall_{t\in\gamma_{01}} \exists_{s\in\gamma_{01}} [(1,t,t^6) = (1,1+s,1+s^6)], \text{ so } \forall_{s\in\gamma_{01}} [(1+s)^6 = 1+s^6],$$

so $\forall_{s\in\gamma_{01}} [s^2 + s^4 = 0]$ and this is not true.

i2) If this point is P_6, we transform $(P_6,Q_6,R_6,S_6) \to (S_6,Q_6,R_6,P_6)$ and find:
$\forall_{t\in\gamma_1} \exists_{s\in\gamma_1} [(1,t,t^6) = (1+s^6,s+s^6,s^6)]$ so

$$\forall_{s\in\gamma_1} \left[\left(\frac{s+s^6}{1+s^6}\right)^6 = \frac{s^6}{1+s^6}\right], \text{ so } \forall_{s\in\gamma} [(1+s^5)^6 = (1+s^6)^5]$$

but since $(1+s^5)^6 + (1+s^6)^5$ is a polynomial of degree less than 31 and $(1+s^5)^6 + (1+s^6)^5 = s^6 + s^{10} + s^{20} + s^{24} \neq 0$ this cannot be true.

i3) If this point is Q_6 then we transform via $(P_6,Q_6,R_6,S_6) \to (P_6,S_6,R_6,Q_6)$ and find:

$$\forall_{t\in\gamma_1} \exists_{s\in\gamma_1} [(1,t,t^6) = (1+s,s,s+s^6)], \text{ so } \forall_{s\in\gamma_1} [(\frac{s}{1+s})^6 = \frac{s+s^6}{1+s}],$$

so $\forall_{s\in\gamma_1} [s^5 = (1+s^5)(1+s)^5 = 1+s+s^4+s^6+s^9+s^{10}]$, so $\forall_{s\in\gamma_1} [1+s+s^4+s^5+s^6+s^9+s^{10}=0]$ and also this cannot be true on the same grounds.

So we find: the assumption $\{P_4,Q_4\} \cap \{P_6,Q_6,R_6\} \neq \emptyset$ leads to a contradiction.

ii) $\{P_4,Q_4\} \cap \{P_6,Q_6,R_6\} = \emptyset$.
We choose $S_6 = P_4$, $S_4 = P_6$, $R_4 = R_6$ and have, for the frame (P_4,Q_4,R_4,S_4): $Q_6 = (1,a,a^4)$ for some $a \in \gamma_{01}$. The transformation T:

$$(x_0,x_1,x_2) \to ((a+a^2+a^3)x_0 + (1+a+a^2+a^3)x_1 + x_2, x_1+x_2, x_1a^3+x_2)$$

transforms P_6 in $(0,0,1)$, R_6 in $(1,0,0)$, Q_6 in $(0,1,0)$ and S_6 in $(1,1,1)$. So it must transform $D(4)$ in $D(6)$. But then we must have $TQ_4 \in D(6)$, so: $TQ_4 = (1+a+a^2+a^3,1,a^3) = (1,s,s^6)$, for some $s \in \gamma$, so

$$(\frac{1}{1+a+a^2+a^3})^6 = \frac{a^3}{1+a+a^2+a^3}, \text{ so } (\frac{1+a}{1+a^4})^6 = \frac{a^3(1+a)}{1+a^4}$$

so $(1+a^4)^5a^3 = (1+a)^5$, so $(1+a^4)^4a^3 = 1+a$, so $(1+a^{32})a^6 = (1+a)^2$, so $a^6 = 1+a$.
But a^6+a+1 is an irreducible polynomial over $GF(2)$ so $a \in \gamma \cap GF(2^6) = GF(2)$ and this leads to the desired contradiction since $a^6+a = 0$ for $a \in GF(2)$.

We have now that $D(4) \sim D(6)$ leads to a contradiction and conclude, with [2], theorem 12, corollary 1, p. 790 that there are exactly three projectively distinct $D(k)$ over $GF(32)$ i.e. $D(2)$, $D(4)$ and $D(6)$.

References

[1] J.W.P. Hirschfeld, Ovals in Desarguesian Planes of Even Order. Ann. di. Mat. 102 (1975), pp. 79-89.

[2] J.W.P. Hirschfeld, Rational Curves on quadrics over finite fields of characteristic two. Rend. Mat. e Appl. (6) 3 (1971), pp. 772-795.