Ovals in Desarguesian Planes of Even Order (*).

J. W. P. Hirschfeld (Brighton, England)

A Beniamino Segre per il settantesimo compleanno:
con memorie felici d'Italia

Sunto. – *Si dimostra con metodi semplici che gli ovali di traslazione sono tutti di un tipo noto. Un'ovale nuovo in $PG(2, 128)$ è anche trovato.*

1. – Introduction.

In $PG(2, q)$, the projective plane over the Galois field $GF(q)$ of q elements, the maximum number of points such that no three are collinear is $q+1$ or $q+2$ according as q is odd or even [1]. A set of points in the plane containing this number is an *oval*. For q odd, a non-singular conic is an oval and, conversely, every oval is a non-singular conic, [6] p. 270. For q even, a non-singular conic plus its nucleus (the meet of its tangents) is an oval: this type is called a *regular* oval. The converse problem of classifying ovals remains to be done.

For $q = 2$, 4 and 8, every oval is regular. For $q = 2^h$ with $h = 4$, 5 and $h \geqslant 7$, there exist irregular ovals. In fact, Segre showed that the set $\{(1, t, t^k) | t \in GF(2^h), k = 2^n\} \cup \{(0, 1, 0), (0, 0, 1)\}$ is an oval if and only if $(n, h) = 1$, [6] p. 286. Such an oval is irregular if $2 \leqslant n \leqslant h-2$. This means that irregular ovals exist for $h = 5$ and $h \geqslant 7$. An irregular oval for $h = 4$ was found by computer, [4].

Let $\gamma = GF(q)$, $\gamma^+ = \gamma \cup \{\infty\}$, $\gamma_0 = \gamma \setminus \{0\}$. Let $\gamma[t]$ be the ring of polynomials over γ in the indeterminate t. If $f(t) \in \gamma[t]$ and $f(0) = 0$, $f(1) = 1$, write

$$D(f) = \{(1, t, f(t)) | t \in \gamma^+\} \cup \{(0, 1, 0)\}.$$

If $\deg f > 1$, then $t = \infty$ gives the point $(0, 0, 1)$. If $f(t) = t^m$, write $D(f) = D(m)$. Then Segre's result states that $D(2^n)$ is an oval in $PG(2, 2^h)$ if and only if $(n, h) = 1$.

If $D(f)$ is an oval and $f(x+y) = f(x) + f(y)$ for all x, y in γ, then $D(f)$ is called a *translation* oval, since it remains fixed under the translation $x_0 \to x_0$, $x_1 \to x_1 + cx_0$, $x_2 \to x_2 + f(c)x_0$ for any c in γ. Then $D(2^n)$ with $(n, h) = 1$ is a translation oval. Conversely, using the results of Segre and Bartocci [7], [8], Payne [5] showed

(*) Entrata in Redazione il 14 maggio 1973.

that every translation oval is of the type $D(2^n)$. These papers all relied on circulants. Our main objective is prove this characterisation of translation ovals without the use of circulants.

2. – Permutation polynomials.

With $\gamma = \mathrm{GF}(q)$, let $\Gamma[t] = \gamma[t]/(t^q - t)$. Then any two polynomials in $\gamma[t]$ with the same image in $\Gamma[t]$ take the same value for all elements of γ. Let $G[t] = \{f \in \gamma[t] | \deg f < q\}$. Then there is a bijection $\varphi: G[t] \to \Gamma[t]$ given by $\varphi(f) = f(t) + (t^q - t)\gamma[t]$.

LEMMA 1. – Any function $f: \gamma \to \gamma$ is defined by an element of $G[t]$.

PROOF. – By Lagrange's interpolation formula,

$$f(t) = -\sum_{\lambda \in \gamma} [f(\lambda)(t^q - t)/(t - \lambda)] .$$

So f has degree at most $q-1$.

LEMMA 2. – If, in lemma 1, f is a bijection, then $\deg f \leqslant q-2$.

PROOF. – $\sum_{\lambda \in \gamma} f(\lambda) = \sum_{\lambda \in \gamma} \lambda = 0$. So, by the above formula, $\deg f \leqslant q-2$.

LEMMA 3. – If $f: \gamma \to \gamma$ is given by a polynomial f of degree less than $q-1$ and if $f|\gamma_0$ is a bijection, then $f(0) = 0$ and f is a bijection.

PROOF. – $f(t) = f(0)(1 - t^{q-1}) - \sum_{\lambda \in \gamma_0} f(\lambda)(t^q - t)/(t - \lambda)$. Also, $\sum_{\lambda \in \gamma_0} f(\lambda) = \sum_{\lambda \in \gamma_0} \lambda = 0$. So, the coefficient of t^{q-1} in $f(t)$ is $-f(0)$. Since $\deg f < q-1$, $f(0) = 0$ and f is a bijection.

Write $\mathcal{T}(q; t) = \{f \in G[t] | f \text{ gives a bijection of } \gamma\}$. The elements of $\mathcal{T}(q; t)$ are called *permutation polynomials*. For any polynomial over γ, DICKSON [2], p. 59 gave the following useful criterion that it should be a permutation polynomial.

DICKSON'S THEOREM. – If $f(t) \in G[t]$, then $f(t) \in \mathcal{T}(q; t)$, $q = p^h$, if and only if

a) for $r \not\equiv 0 \pmod p$ and $r \leqslant q-2$, the degree of $f(t)^r$ modulo $t^q - t$ is at most $q-2$;

b) $f(t) = 0$ has exactly one solution in γ.

In the particular case that $p = 2$ and $f(0) = 0$, these conditions become

A) for r odd and $r \leqslant q-2$, the degree of $f(t)^r$ modulo $t^q - t$ is at most $q-2$;

B) $f(t) = 0 \Rightarrow t = 0$.

3. – Canonical form for an oval.

Let $\mathcal{K}$ be a $(q+1)$-arc in PG$(2, q)$ with q even. Let $X_0X_1X_2$ denote the triangle of reference and U the unit point of the coordinate system. Choose X_1 as the nucleus of $\mathcal{K}$ and X_0, X_2 and U as any three points of $\mathcal{K}$. Write $\mathcal{O} = \mathcal{K} \cup \{X_1\}$. Then $\mathcal{O}$ contains X_1 and X_2 on $x_0 = 0$ and so no other points on this line. Each of the remaining points of $\mathcal{O}$ can be written $(1, t_i, s_i)$. Since each line through X_2 contains exactly one other point of $\mathcal{O}$, so $t_i \neq t_j$ for $i \neq j$. Similarly, since each line through X_1 contains exactly one other point of $\mathcal{O}$, so $s_i \neq s_j$ for $i \neq j$. Therefore there exists a unique $f \in \mathcal{T}(q; t)$ such that $\mathcal{O} \setminus \{X_1, X_2\} = \mathcal{K} \setminus \{X_2\} = \{(1, t, f(t)) | t \in \gamma\}$. Equivalently, since $\deg f > 1$, $\mathcal{K} = \{(1, t, f(t)) | t \in \gamma^+\}$, where $t = \infty$ parametrizes X_2. Since X_0 and U lie on $\mathcal{K}$, $f(0) = 0$ and $f(1) = 1$. Since the set $\{(1, t, f(t)) | t \in \gamma^+\} \cup \{X_1\}$ where $f(0) = 0$ and $f(1) = 1$ has been named $D(f)$, an oval $\mathcal{O}$ can always be written in the form $D(f)$ with $f \in \mathcal{T}(q; t)$. The complete description of an oval is given by the following.

THEOREM 1. – In PG$(2, q)$ with q even, $D(f)$ is an oval if and only if

a) $f(t) \in \mathcal{T}(q; t)$;

b) $g(t; s) = [f(t + s) + f(s)]/t \in \mathcal{T}(q; t)$ for each $s \in \gamma$ and $g(0; s) = 0$.

PROOF. – From the form of $D(f)$, each line through X_2 is a chord of $D(f)$. Condition (*a*) is exactly the condition that each line through X_1 is a chord of $D(f)$.

It remains to show that (*b*) is necessary and sufficient for no three points of $D(f) \setminus \{X_1, X_2\}$ to be collinear. This is true if and only if

$$\begin{vmatrix} 1 & t_1 & f(t_1) \\ 1 & t_2 & f(t_2) \\ 1 & t_3 & f(t_3) \end{vmatrix} \neq 0$$

for all distinct $t_1, t_2, t_3 \in \gamma$. That is,

$$\frac{f(t_1) + f(t_2)}{t_1 + t_2} \neq \frac{f(t_1) + f(t_3)}{t_1 + t_3}.$$

Equivalently, for each $s \in \gamma$, $[f(t) + f(s)]/(t + s)$ takes a different value in γ_0 for each $t \in \gamma \setminus \{s\}$; or, $[f(t + s) + f(s)]/t$ takes a different value in γ_0 for each $t \in \gamma_0$; that is, for each $s \in \gamma$, $g(t; s) = [f(t + s) + f(s)]/t$ defines a permutation of γ_0. However, $g(t; s)$ is a polynomial in t of degree less than $q - 1$. So, by lemma 3, $g(0; s) = 0$ and $g(t; s) \in \mathcal{T}(q; t)$. Thus (*b*) is the condition that no three points of $D(f) \setminus \{X_1, X_2\}$ are collinear.

COROLLARY 1. – In PG(2, q) with q even, if $f(t)=\sum_{i=1}^{q-2} a_i t^i$ and $D(f)$ is an oval, then $f(t)=a_2t^2+a_4t^4+\ldots+a_{q-2}t^{q-2}$.

PROOF. – Since $g(t;s)=[f(t+s)+f(s)]/t$, so

$$g(0;s)=a_1+a_3s^2+a_5s^4+\ldots+a_{q-3}s^{q-3}\,.$$

Since $g(0;s)=0$ for all s in γ, so $a_1=a_3=a_5=\ldots=a_{q-3}=0$.

When f is a monomial, the conditions of the theorem can be simplified.

COROLLARY 2. – In PG(2, q) with q even, $D(k)$ is an oval if and only if

a) $(k, q-1)=1$;

b) $(k-1, q-1)=1$;

c) $[(t+1)^k+1]/t\in\mathcal{T}(q;t)$.

PROOF. – $t^m\in\mathcal{T}(q;t)\Leftrightarrow t^m=c$ has a unique solution in γ for each c in $\gamma\Leftrightarrow$ $\Leftrightarrow(m, q-1)=1$. So condition ($a$) of the theorem becomes (a) here. Similarly, condition (b) of the theorem for $s=0$ becomes (b) here. For $s\neq 0$, $g(t;s)=[(t+s)^k+s^k]/t=$ $=s^k[(t/s+1)^k+1]/t$, which is in $\mathcal{T}(q;t)$ if and only if $[(t+1)^k+1]/t$ is.

COROLLARY 3. – In PG(2, 2^h), $D(2^n)$ is an oval if and only if $(n, h)=1$.

PROOF. – If $k=2^n$, then $[(t+1)^k+1]/t=t^{k-1}$. So, in corollary 2, $(c)\Leftrightarrow(b)$ Now, $(2^n, 2^h-1)=1$; so (a) is satisfied. Also $(2^n-1, 2^h-1)=2^{(n,h)}-1$. Therefore ($b$) is satisfied if and only if $(n, h)=1$.

COROLLARY 4. – In PG(2, 2^h), $D(2^n)$ is a regular oval if and only if $n=1$ or $h-2$.

COROLLARY 5. – In PG(2, 2^h), irregular ovals exist for $h=5$ and $h\geqslant 7$.

For $h=1$, 2 and 3, every oval is regular. For $h=4$, all ovals can be computed [4] and, for example, $D(f)$ with

$$f(t)=(\eta^5t^7+\eta^6t^6+\eta^{10}t^5+\eta^2t^4+\eta^{12}t^3+t^2+\eta^5t)^2\,,$$

where η is a primitive root of GF(16) satisfying $\eta^4=\eta+1$, is an irregular oval. For $h=6$, the existence of an irregular oval is still an open question.

4. – Characterisation of translation ovals.

As defined in the introduction, $D(f)$ is a translation oval if it is an oval and if f induces an endomorphism of γ as an additive group. Thus, from Theorem 1, the necessary and sufficient conditions for $D(f)$ to be a translation oval are

T1) $f(x+y)=f(x)+f(y)$ for all x, y in γ;

T2) $f(t)\in \mathcal{T}(q;t)$;

T3) $f(t)/t\in \mathcal{T}(q;t)$.

In fact, we would like to show that every translation oval $D(f)$ has the form $D(2^n)$. Firstly, three lemmas are required.

LEMMA 4. – Every endomorphism of $GF(q)$, $q=p^h$, as an additive group is given by a polynomial of the form

$$f(t)=a_0t+a_1t^p+\ldots+a_{h-1}t^{p^{h-1}}.$$

PROOF. – $GF(q)$ is a vector space over $GF(p)$. So, let it have a basis $\{x_1,\ldots,x_h\}$. Then an endomorphism of $GF(q)$ is determined once the images of all the x_i are given. As each x_i can have any element of $GF(q)$ as its image, there are q^h endomorphisms of $GF(q)$. However, each polynomial of the above form induces a distinct endomorphism of $GF(q)$ and there are q^h such polynomials. Therefore, each endomorphism of $GF(q)$ is given by such a polynomial.

LEMMA 5. – If $a_ma_n\neq 0$ and $m<n<h$, then $a_mt^{2^m-1}+a_nt^{2^n-1}\notin \mathcal{T}(2^h;t)$.

PROOF. – By Dickson's theorem, it suffices to show that there exists an odd integer $r\leqslant 2^h-2$ such that $(a_mt^{2^m-1}+a_nt^{2^n-1})^r$ modulo $t^{2^h}-t$ contains a term in t^{2^h-1}. The power of the general term in this expression expanded is

$$r(2^m-1)+k(2^n-2^m).$$

Let $r=(2^h-1)-z(2^n-2^m)$. Then, since we require that

$$r(2^m-1)+k(2^n-2^m)\equiv 0 \pmod{2^h-1},$$

so

$$k(2^n-2^m)-z(2^m-1)(2^n-2^m)\equiv 0.$$

Now, $k=z(2^m-1)$ is a solution of this equation. Let $d=2^{(n-m,h)}-1$ and let $R=(2^h-1)/d$. Then, as $(2^n-2^m,2^h-1)=d$, there are d solutions given by

$$k\equiv z(2^m-1)+RN,\qquad N=0,1,2,\ldots,d-1.$$

We require z such that there is a unique k with $0<k<r$. In particular, $r=2^h-1-z(2^n-2^m)$ and $k=z(2^m-1)$ fulfil our requirements if $k<r<R$.

Put $z = 2^{h-n}$. Then

$$\begin{aligned} k = 2^{h-n+m} - 2^{h-n} < 2^{h-n+m} - 1 &= r \\ &\leqslant (2^{h-n+m} - 1)(2^{n-m} - 1)/d \\ &< (2^h - 1)/d = R\,. \end{aligned}$$

So $r = 2^{h-n+m} - 1$ and $k = 2^{h-n+m} - 2^{h-n}$. Then $(1 + x)^r = \sum_0^r x^i$; in particular, the coefficient of x^k is 1.

Thus it has been shown that $(a_m t^{2^m-1} + a_n t^{2^n-1})^{2^{h-n+m}-1}$ has exactly one term in t^{2^h-1} and so, if $a_m a_n \neq 0$, $a_m t^{2^m-1} + a_n t^{2^n-1}$ is not in $\mathcal{T}(2^h; t)$.

LEMMA 6. – If $a_m a_n \neq 0$ and $m < n < h$, then

$$a_m t^{2^m-1} + a_{m+1} t^{2^{m+1}-1} + \ldots + a_n t^{2^n-1} \notin \mathcal{T}(q; t)\,.$$

PROOF. – As in the last lemma, we use Dickson's theorem and, in fact, the same r to show that, if $r = 2^{h-n+m} - 1$, then

$$(a_m t^{2^m-1} + a_{m+1} t^{2^{m+1}-1} + \ldots + a_n t^{2^n-1})^r \qquad \text{modulo } t^{2^h} - t$$

always contains a term in t^{2^h-1}.

The previous lemma used the identity

$$(2^{h-n+m} - 1)(2^m - 1) + (2^{h-n+m} - 2^{h-n})(2^n - 2^m) = (2^m - 1)(2^h - 1)$$

or

$$(2^{h-n} - 1)2^m + (2^{h-n+m} - 2^{h-m})2^n = 2^{h-n+m} - 1 + (2^m - 1)(2^h - 1)\,.$$

It suffices to consider

$$\begin{aligned} &(t^{2^m-1} + t^{2^{m+1}-1} + \ldots + t^{2^n-1})^{2^{h-n+m}-1} = \\ &\qquad = (t^{2^m} + t^{2^{m+1}} + \ldots + t^{2^n})^{1+2+2^2+\ldots+2^{h-n+m-1}}/t^{2^{h-n+m}-1} = \\ &\qquad = (t^{2^m} + \ldots + t^{2^n})(t^{2^{m+1}} + \ldots + t^{2^{n+1}}) \ldots (t^{2^{h-n+2m-1}} + \ldots + t^{2^{h+m-1}})/t^{2^{h-n+m}-1} = \\ &\qquad = \sum t^{2^{m_0}+2^{m_1}+\ldots+2^{m_s}-2^{h-n+m}+1} \end{aligned}$$

where $s = h - n + m - 1$ and $m + i \leqslant m_i \leqslant n + i$ for $i = 0, 1, \ldots, s$. We require solutions for

$$2^{m_0} + 2^{m_1} + \ldots + 2^{m_s} \equiv 2^{h-n+m} - 1 \qquad (\text{mod } 2^h - 1)\,.$$

From the previous lemma (or by the above identity), there is a solution

$$m_i = m + i\,, \qquad i = 0, 1, \ldots, h-n-1\,;$$

$$m_i = n + i\,, \qquad i = h-n, \ldots, s\,.$$

It must be shown that this is the only solution.

Put $m_i = m + r_i$; then $i \leqslant r_i \leqslant n - m + i$, $i = 0, 1, \ldots, s$. The equation now becomes

$$2^m(2^{r_0} + \ldots + 2^{r_s}) \equiv 2^{h-n+m} - 1 \qquad (\operatorname{mod} 2^h - 1)\,.$$

Since $(2^m, 2^h - 1) = 1$ and $2^{h-m}\cdot 2^m - (2^h - 1) = 1$,

$$2^{r_0} + 2^{r_1} + \ldots + 2^{r_s} \equiv 2^{h-m}(2^{h-n+m} - 1) \equiv 2^{2h-n} - 2^{h-m}\,.$$

As $r_i \geqslant i$, so $\sum 2^{r_i} \geqslant 1 + 2 + \ldots + 2^s = 2^{h-n+m} - 1$. As $r_i \leqslant n - m + i$, so $\sum 2^{r_i} \leqslant 2^{n-m}(2^{h-n+m} - 1) = 2^h - 2^{n-m}$. However, $(2^h - 2^{n-m}) - (2^{h-n+m} - 1) < 2^h - 1$. Therefore, $\sum 2^{r_i}$ takes a definite value such that $2^{h-n+m} - 1 \leqslant \sum 2^{r_i} \leqslant 2^h - 2^{n-m}$. In fact, $(2^{2h-n} - 2^{h-m}) - (2^{h-n} - 1)(2^h - 1) = 2^h - 2^{h-m} + 2^{h-n} - 1$, which lies in the required range. Thus,

$$\sum 2^{r_i} = 2^h - 2^{h-m} + 2^{h-n} - 1 = 1 + 2 + \ldots + 2^{h-n-1} + 2^{h-m} + \ldots + 2^{h-1}\,.$$

Written in the binary scale, the number on the right has exactly $h - n + m$ unit digits, which is the number of summands on the left. As $i \leqslant r_i \leqslant n - m + i$, the unique solution is

$$r_i = i \qquad \text{for } i = 0, 1, \ldots, h-n-1$$

and

$$r_i = n - m + i \qquad \text{for } i = h-n, \ldots, h-n+m-1\,.$$

So there is always a term in t^{2^h-1} in the expansion of

$$(a_m t^{2^m-1} + \ldots + a_n t^{2^n-1})^{2^{h-n+m}-1} \qquad \text{provided } a_m a_n \neq 0\,.$$

Theorem 2. – In $PG(2, 2^h)$, $D(f)$ is a translation oval if and only if $D(f) = D(2^n)$ with $(n, h) = 1$.

Proof. – If $D(f) = D(2^n)$ with $(n, h) = 1$, then by theorem 1, corollary 3, $D(f)$ is an oval. Since $f(t) = t^{2^n}$ satisfies T1, $D(f)$ is a translation oval.

Conversely, if $D(f)$ is a translation oval, then by T1 and lemma 4

$$f(t) = a_0 t + a_1 t^2 + \ldots + a_{h-1} t^{2^{h-1}} .$$

By theorem 1, corollary 1, $a_0 = 0$. By T3 and lemma 6, $f(t) = a_n t^{2^n}$ for some n in $0 < n < h$. Since $f(1) = 1$, so $a_n = 1$. Finally, by theorem 1, corollary 3, for $D(2^n)$ to be an oval, it is necessary that $(n, h) = 1$. So $D(f) = D(2^n)$ with $(n, h) = 1$.

5. – Further examples of ovals.

If $D(f)$ is an oval in PG(2, q) with q even, then by limiting the degree of f, the form of f or the size of q, further information can be obtained. Firstly, we limit the degree of f and then consider, for small q, f as a monomial.

THEOREM 3. – In PG (2, q) with q even,

a) if $\deg f = 2$, then $D(f)$ is an oval if and only if $D(f) = D(2)$;

b) if $\deg f = 4$, then $D(f)$ is an oval if and only if h is odd and $D(f) = D(4)$;

c) if $\deg f = 6$, then $D(f)$ is an oval if and only if h is odd and $f(t) = (t^6 + \lambda t^4 + \lambda^2 t^2)/(1 + \lambda + \lambda^2)$ for some $\lambda \in \gamma$. In this case, $D(f)$ is projectively equivalent to $D(6)$.

PROOF. – See [3], p. 792.

In PG(2, 2), PG(2, 4) and PG(2, 8), every oval is regular. Although the problem of classifying ovals in general is difficult, there is a type that can be managed. When $D(f) = D(m)$ for some integer m, then the problem can be attacked for small q. Write $D(m) \sim D(l)$ when these two sets are projectively equivalent.

THEOREM 4. – Suppose $D(k)$ is an oval in PG(2, q) with q even. Then

$$D(k) \sim D(k_1) \sim D(k_2) \sim D(k_3) ,$$

where k_1, k_2, k_3 are defined by

$$kk_1 \equiv 1 \pmod{q-1} \quad \text{and} \quad 1 < k_1 < q-1 ;$$

$$(k-1)(k_2-1) \equiv 1 \pmod{q-1} \quad \text{and} \quad 1 < k_2 < q-1 ;$$

$$k + k_3 = q .$$

PROOF. – See [3], p. 789.

COROLLARY 1. – In PG $(2, q)$ for $q = 16$, 32 and 64, the only projectively distinct ovals of the form $D(k)$ are

a) for $q = 16$, $D(2)$;

b) for $q = 32$, $D(2)$, $D(4)$ and $D(6)$;

c) for $q = 64$, $D(2)$.

PROOF. – See [3], p. 790.

THEOREM 5. – In PG$(2, 128)$, there are five projectively distinct ovals of the form $D(k)$: $D(2)$, $D(4)$, $D(6)$, $D(8)$, $D(20)$.

PROOF. – By theorem 1, corollary 1, k is odd. By theorem 4, the following table can be calculated.

k	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32
k_1	64	32	106	16	89	53	118	8	120	108	52	90	44	59	72	4
k_2	2	86	52	110	114	105	89	18	16	108	122	117	62	81	93	42
k_3	126	124	122	120	118	116	114	112	110	108	106	104	102	100	98	96

k	34	36	38	40	42	44	46	48	50	52	54	56	58	60	62	64
k_1	71	60	117	54	124	26	58	45	94	22	40	93	46	36	84	2
k_2	78	99	104	115	32	66	49	101	71	6	13	98	79	29	26	126
k_3	94	92	90	88	86	84	82	80	78	76	74	72	70	68	66	64

Therefore the only possible candidates for projectively distinct ovals are $D(2)$, $D(4)$, $D(6)$, $D(8)$, $D(20)$ and $D(26)$, where the $D(k)$ with lowest k among several projectively equivalent $D(k)$ has been chosen. By theorem 1, corollary 3, $D(2)$, $D(4)$ and $D(8)$ are ovals. By theorem 3, $D(6)$ is an oval. It remains to show that $D(26)$ is not an oval but that $D(20)$ is. Writing $g_m(t) = [(t+1)^m + 1]/t$, it must be shown that $g_{26}(t)$ is not in $\mathcal{T}(128; t)$ but that $g_{20}(t)$ is.

Let β be a primitive root of GF(128) satisfying $\beta^7 + \beta + 1 = 0$. The table below lists, for each i in $1 \leqslant i \leqslant 126$, the integers $r(i)$ and $s(i)$ where

$$\beta^{r(i)} = 1 + \beta^i \quad \text{and} \quad \beta^i = g_{20}(\beta^{s(i)}) .$$

Also $g_{20}(0) = 0$ and $g_{20}(1) = 1$. Thus, from the table, $g_{20}(t)$ is a permutation polynomial. On the other hand, $g_{26}(\beta^5) = g_{26}(\beta^9) = \beta^{123}$. So $g_{26}(t)$ is not a permutation polynomial. This completes the proof.

i	$r(i)$	$s(i)$	i	$r(i)$	$s(i)$	i	$r(i)$	$s(i)$
1	7	15	43	17	57	85	72	92
2	14	30	44	94	70	86	34	114
3	63	79	45	68	101	87	11	119
4	28	60	46	37	107	88	61	13
5	54	38	47	22	111	89	20	4
6	126	31	48	119	121	90	9	75
7	1	51	49	122	26	91	70	45
8	56	120	50	83	72	92	74	87
9	90	11	51	40	8	93	52	106
10	108	76	52	93	78	94	44	95
11	87	81	53	18	23	95	65	3
12	125	62	54	5	1	96	111	115
13	55	83	55	13	90	97	32	108
14	2	102	56	8	27	98	117	52
15	31	110	57	21	47	99	103	91
16	112	113	58	38	41	100	39	17
17	43	49	59	104	85	101	84	61
18	53	22	60	124	59	102	80	16
19	29	68	61	88	63	103	99	80
20	89	25	62	30	5	104	59	29
21	57	56	63	3	6	105	25	37
22	47	35	64	67	71	106	36	46
23	82	117	65	95	103	107	69	123
24	123	124	66	27	19	108	10	2
25	105	36	67	64	89	109	35	86
26	110	39	68	45	69	110	26	53
27	66	64	69	107	104	111	96	65
28	4	77	70	91	105	112	16	54
29	19	84	71	79	55	113	115	109
30	62	93	72	85	88	114	42	94
31	15	66	73	78	34	115	113	40
32	97	99	74	92	28	116	76	82
33	77	73	75	41	122	117	98	125
34	86	98	76	116	18	118	81	43
35	109	116	77	33	32	119	48	96
36	106	44	78	73	42	120	121	118
37	46	14	79	71	33	121	120	20
38	58	9	80	102	100	122	49	126
39	100	21	81	118	58	123	24	48
40	51	50	82	23	7	124	60	10
41	75	67	83	50	74	125	12	24
42	114	112	84	101	97	126	6	12

BIBLIOGRAPHY

[1] R. C. BOSE, *Mathematical theory of the symmetrical factorial design*, Sankhya, **8** (1947), pp. 107-166.
[2] L. E. DICKSON, *Linear groups*, Dover, 1958.

[3] J. W. P. HIRSCHFELD, *Rational curves on quadrics over finite fields of characteristic two*, Rend. Mat. e Appl., (6), **3** (1971), pp. 772-795.
[4] L. LUNELLI - M. SCE, *K-archi completi nei piani proiettivi desarguesiani di rango* 8 *e* 16, Centro calcoli numerici, Politecnico di Milano, 1958.
[5] S. E. PAYNE, *A complete determination of translation ovoids in finite Desarguian planes*, Atti Accad. Naz. Lincei Rend. Cl. Sc. Fis. Mat. Natur., (8), **51** (1971), pp. 328-331.
[6] B. SEGRE, *Lectures on modern geometry*, Cremonese, 1961.
[7] B. SEGRE, *Ovali e curve* σ *nei piani di Galois di caratteristica due*, Atti Accad. Naz. Lincei Rend. Cl. Sc. Fis. Mat. Natur., (8), **32** (1962), pp. 785-790.
[8] B. SEGRE - U. BARTOCCI, *Ovali ed altre curve nei piani di Galois di caratteristica due*, Acta Arith., **18** (1971), pp. 423-449.