On regular semiovals in $PG(2, q)$

András Gács*

Abstract

In this paper we prove that a point set in $PG(2, q)$ meeting every line in 0, 1 or r points and having a unique tangent at each of its points is either an oval or a unital. This answers a question of Blokhuis and Szőnyi [1].

1 Introduction

In $PG(2, q)$ ovals and unitals have the common property that they have a unique tangent at each of their points. For the definiton and properties of ovals and unitals, we refer to [2]. Such a set in general is called a *semioval*. For more examples, see [3] and [4].

In [1] the authors raise the question, whether the extra property, that every secant of such a set meets it in a constant number of points characterizes ovals and unitals. Such sets were called *regular semiovals*. In this paper we answer this question affirmatively. The proof is based on the technique often refered to as Segre's lemma. Our approach is similar to that of Thas in [5]. The main difference is in the choice of the base points and that we also need an extra lemma (Lemma 2.4) which separates Hermitian curves from another possible example.

We end this introduction by recalling some results from Blokhuis-Szőnyi [1] and stating our theorem.

Result 1.1 *Suppose K is a regular semioval in $PG(2, q)$ with line intersection sizes $\{0, 1, r\}$, which is neither a unital, nor an oval. Then the following holds.*

(i) $r|q-1$ *([1] Thm. 2);*

(ii) $r-1$ *is not* 0 *in* $GF(q)$ *([1] Thm. 4);*

(iii) tangents through points of any r-secant are concurrent ([1] Thm. 5);

(iv) through any point out of the semioval, there are either 0*, or r tangents, in the latter case the points of tangency are collinear ([1] Thm. 2, Thm. 5).*

Note that by (iv), tangents in the dual plane form a regular semioval with the same parameters.

Our aim is to use these properties to deduce the following.

Theorem 1.2 *In $PG(2, q)$ any regular semioval is either an oval or a unital.*

*Research was partially supported by OTKA Grants T 043758, F 043772; the preparation of the final version was supported by OTKA Grant T 049662 and TÉT grant E-16/04.

2 Proof of Theorem 1.2

Throughout this text we use homogeneous coordinates for points and lines in $PG(2,q)$, where $q=p^e$ is an arbitrary prime power. The point (a,b,c) is incident to the line $[A,B,C]$ if and only if $Aa+Bb+Cc=0$. The points $(0,0,1),(0,1,0),(1,0,0)$ will be called *base points*, the lines $[0,0,1],[0,1,0],[1,0,0]$ *base lines*, finally, the union of points of the base lines will be called *base triangle*. Let K denote the semioval and r the intersection size besides 0 and 1. Suppose that K is neither an oval (hence $r\geq 3$), nor a unital (hence $r-1$ is not zero modulo p by 1.1 (ii)).

Choose homogeneous coordinates in such a way that $(1,0,0)$, $(0,1,0)$ and $(0,0,1)$ are points of K and let the equation of tangents at these points be

$$X_2=CX_1, X_0=BX_2, X_1=AX_0.$$

Note that $ABC\neq 1$, since otherwise these lines would be concurrent, contradicting 1.1 (iv). A simple calculation shows that the intersection points of the tangents above are $P(1,A,AC)$, $Q(BC,1,C)$, $R(B,AB,1)$.

Let the intersection of K and the base triangle (without vertices) be

$$\{(1,\epsilon_i,0): i=1,\ldots,r-2\},$$

$$\{(\delta_i,0,1): i=1,\ldots,r-2\},$$

$$\{(0,1,\gamma_i): i=1,\ldots,r-2\}.$$

Lemma 2.1

$$(\epsilon_1\cdots\epsilon_{r-2}\cdot\delta_1\cdots\delta_{r-2}\cdot\gamma_1\cdots\gamma_{r-2})\cdot(ABC)^{r-1}=(-1)^{r-1}.$$

Proof: Let $P_1,\ldots,P_{|K|-3r+3}$ denote the points of K not on any base line. Let P_i be the intersection of lines

$$X_1=a_iX_0, X_0=b_iX_2, X_2=c_iX_1.$$

Note that this implies $a_ib_ic_i=1$. Multiplicities of field elements in the multi-set $\{a_1,...,a_{|K|-3r+3}\}$ correspond to intersection sizes of non-base lines through $(0,0,1)$ and the part of K out of the base triangle. Hence A has multiplicity zero, the ϵ_is have multiplicity $r-2$, all other non-zero field elements have multiplicity $r-1$. Since the product of all non-zero field elements is (-1), we get

$$a_1\cdots a_{|K|-3r+3}A^{r-1}\cdot\epsilon_1\cdots\epsilon_{r-2}=(-1)^{r-1}.$$

The same argument for lines through the other two base points gives

$$b_1\cdots b_{|K|-3r+3}B^{r-1}\cdot\delta_1\cdots\delta_{r-2}=(-1)^{r-1},$$

$$c_1\cdots c_{|K|-3r+3}C^{r-1}\cdot\gamma_1\cdots\gamma_{r-2}=(-1)^{r-1}.$$

Multipying the three equations and using $a_ib_ic_i=1$ for every i, we get the promised equation. □

Lemma 2.2 $(ABC)^r = 1$.

Proof: We wish to use the previous lemma in the dual plane. By 1.1 (iii) and (iv), in the dual setting the original tangents become points of the semioval and vice versa, r-secants become points out of the oval with r tangents and lines not meeting K become points on zero tangents.

The three tangents will play the role of the base points, instead of tangents at base points, we have to consider points of tangencies, finally, instead of points on the base triangle, we will need the tangent lines through these points.

We apply a transformation which takes the three tangents $X_1 = AX_0, X_0 = BX_2, X_2 = CX_1$ to the lines $X_2 = 0$, $X_1 = 0$, $X_0 = 0$, respectively. A little calculation shows that the following matrix is appropriate:

$$\begin{pmatrix} 0 & C & -1 \\ -1 & 0 & B \\ A & -1 & 0 \end{pmatrix}.$$

It is easy to see that after the transformation, the tangency points of the base lines will be the images of the base points, that is $(0, -1, A)$, $(C, 0, -1)$ and $(-1, B, 0)$, which means that in the new setting $A' = \frac{1}{B}$, $B' = \frac{1}{C}$ and $C' = \frac{1}{A}$.

To find the image of the tangent at the point $(1, \epsilon_i, 0)$, first note that (by 1.1 (iii)) the original tangent was the line joining the point $(1, \epsilon_i, 0)$ to the point $Q(BC, 1, C)$, hence we are looking for the line joining the images of these two points, which turns out to be $[1, C\epsilon_i, 0]$. Similarly, we get that the tangent through the image of $(\delta_i, 0, 1)$ is $[A\delta_i, 0, 1]$ and of $(0, 1, \gamma_i)$ is $[0, 1, B\gamma_i]$.

Now we can use the previous lemma to get

$$((C\epsilon_1) \cdots (C\epsilon_{r-2}) \cdot (A\delta_1) \cdots (A\delta_{r-2}) \cdot (B\gamma_1) \cdots (B\gamma_{r-2})) \cdot (\frac{1}{BCA})^{r-1} = (-1)^{r-1}.$$

This equation and the one from the previous lemma gives $(ABC)^r = 1$. □

Lemma 2.3

$$\{\epsilon_i : i = 1, \ldots, r-2\} = \frac{1}{BC}\{\frac{ABC - \eta}{1 - \eta} : \eta^r = 1, \eta \neq 1, \eta \neq ABC\}; \tag{1}$$

$$\{\delta_i : i = 1, \ldots, r-2\} = \frac{1}{AC}\{\frac{ABC - \eta}{1 - \eta} : \eta^r = 1, \eta \neq 1, \eta \neq ABC\}; \tag{2}$$

$$\{\gamma_i : i = 1, \ldots, r-2\} = \frac{1}{AB}\{\frac{ABC - \eta}{1 - \eta} : \eta^r = 1, \eta \neq 1, \eta \neq ABC\}. \tag{3}$$

Proof: We use a transformation which fixes $(0, 1, 0)$ and $(0, 0, 1)$, but takes $(1, \epsilon_i, 0)$ to $(1, 0, 0)$ (here i is any fixed index). After the transformation we calculate the new A, B and C and use the previous lemma.

The following matrix is easily seen to be appropriate:

$$\begin{pmatrix} 1 & 0 & 0 \\ -\epsilon_i & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

To calculate equations of the new tangents at base points (that is, to find out the new A, B and C), first note that the tangent at $(1,0,0)$ will be the line joining it to the image of $Q(BC,1,C)$ (which is $(BC, 1-BC\epsilon_i, C)$), this turns out to be $[0,-C,1-BC\epsilon_i]$, hence $C' = \frac{C}{1-BC\epsilon_i}$.

Similarly, the tangent at $(0,1,0)$ is the line joining it to the image of Q, this gives $B' = B$.

Finally, for A' we have to calculate the image of $R(B, AB, 1)$ (which is $(B, B(A-\epsilon_i), 1)$) and consider the line joining it to $(0,0,1)$, this is $[A-\epsilon_i, -1, 0]$, hence $A' = A - \epsilon_i$.

Now from the previous lemma, we get

$$(\frac{(A-\epsilon_i)BC}{1-BC\epsilon_i})^r = 1.$$

Write $\eta = \frac{(A-\epsilon_i)BC}{1-BC\epsilon_i}$ for the corresponding r-th root of unity. A little calculation shows that this implies

$$\epsilon_i = \frac{1}{BC}\frac{ABC-\eta}{1-\eta}.$$

Since there are $r-2$ different choices for ϵ_i, we get (1). The proof of (2) and (3) are similar. □

Proof of Theorem 1.2.

We study further the transformation investigated in the previous lemma. It is easy to see that the points $(0,1,\gamma_j)$ are all fixed, so using (3), this implies

$$\frac{1}{AB}\{\frac{ABC-\eta}{1-\eta} : \eta^r = 1, \eta \neq 1, \eta \neq ABC\} = \frac{1}{A'B'}\{\frac{A'B'C'-\eta}{1-\eta} : \eta^r = 1, \eta \neq 1, \eta \neq A'B'C'\}.$$

On the other hand, we had $A' = A - \epsilon_i$, $B' = B$ and $C' = \frac{C}{1-BC\epsilon_i}$, hence

$$\frac{1}{AB}\{\frac{ABC-\eta}{1-\eta} : \eta^r = 1, \eta \neq 1, \eta \neq ABC\} = \frac{1}{(A-\epsilon_i)B}\{\frac{u-\eta}{1-\eta} : \eta^r = 1, \eta \neq 1, \eta \neq u\},$$

where $u = A'B'C' = \frac{(A-\epsilon_i)BC}{1-BC\epsilon_i}$. We conclude that

$$\frac{A-\epsilon_i}{A}\{\frac{ABC-\eta}{1-\eta} : \eta^r = 1, \eta \neq 1, \eta \neq ABC\} = \{\frac{u-\eta}{1-\eta} : \eta^r = 1, \eta \neq 1, \eta \neq u\}.$$

Note that by Lemma 2.2, $u^r = 1$. Using the lemma after this proof (with $x = \frac{A-\epsilon_i}{A}$, $y = ABC$, $z = u$), we find the following equation:

$$u(1+ABC)^2 = ABC(1+u)^2.$$

Here ABC is fixed, while u can take any r-th root of unity except for 1 (to see this, note that different choices of ϵ_i give different values for u by $ABC \neq 1$, and $u = ABC$ is also appropriate, this corresponds to the case when we put 0 in the place of ϵ_i).

Hence we have the following divisibility condition of polynomials:

$$X^r - 1 | (X-1)(ABC(X+1)^2 - (ABC+1)^2 X).$$

This immediately implies $r \leq 3$, so we only have to exclude $r = 3$.

For $r = 3$ there is a unique $u \notin \{ABC, 1\}$, we have $u^2 = ABC$, $u(ABC) = 1$, and also $u^2 + u + 1 = (ABC)^2 + (ABC) + 1 = 0$. In the equation $\epsilon_1 = \frac{1}{BC}\frac{ABC-\eta}{1-\eta}$, η is necessarily u and we have $\epsilon_1 = \frac{1}{BC}\frac{u^2-u}{1-u} = \frac{-u}{BC}$.

Note that for $r = 3$ we can also use the other equation from the next lemma ($y = -1$ is not possible, because it would imply $(-1)^3 = 1$, that is $-1 = 1$, so $ABC = 1$, a contradiction). Equation $x = \frac{z+1}{y+1}$ gives $\frac{A-\epsilon_1}{A} = \frac{u+1}{ABC+1}$. Using $u+1 = -u^2$ and $ABC+1 = -u$, this implies $\frac{A-\epsilon_1}{A} = u$. On the other hand, $\frac{A-\epsilon_1}{A} = \frac{A+u/BC}{A} = \frac{ABC+u}{ABC} = -\frac{1}{u^2} = -u$. Hence $u = -u$, so the characteristic is 2, but this contradicts Result 1.1 (ii). □

Lemma 2.4 *Suppose x, y and z are field elements with $y^r = z^r = 1$; $y \neq 1$, $z \neq 1$; $r | q-1$ and satisfying*

$$x\{\frac{y-\eta}{1-\eta} : \eta^r = 1, \eta \neq 1, \eta \neq y\} = \{\frac{z-\eta}{1-\eta} : \eta^r = 1, \eta \neq 1, \eta \neq z\}.$$

If $r-1$ is not divisible by the characteristic of the field, then

$$y(z+1)^2 = z(y+1)^2.$$

If $y = z = -1$ does not hold, then we also have

$$x = \frac{z+1}{y+1}.$$

Proof: First note that we can ommit the conditions $\eta \neq y$ and $\eta \neq z$, since this adds zero to both sets. The set $x\{\frac{y-\eta}{1-\eta} : \eta^r = 1, \eta \neq 1\}$ is exactly the set of zeros of the polynomial $f(T) = (T-xy)^r - (T-x)^r$. This can be seen by writing $(T-xy) = (T-x)\eta$ for an r-th root of unity η, and expressing T in terms of η.

Similarly, $\{\frac{z-\eta}{1-\eta} : \eta^r = 1, \eta \neq 1\}$ is the set of zeros of the polynomial $g(T) = (T-z)^r - (T-1)^r$. Since these are non-zero polynomials of degree at most $r-1$, the condition we have is equivalent to the equation $f(T) \equiv cg(T)$ for a constant c. Calculating the coefficients of T^{r-1}, T^{r-2}, T^2 and T on both sides we find the following four equations for x, y, z and c:

$$-r(xy - x) = -rc(z-1);$$

$$\binom{r}{2} x^2(y^2-1) = \binom{r}{2} c(z^2-1);$$

$$\binom{r}{r-2}(-1)^{r-2}(x^{r-2}y^{r-2} - x^{r-2}) = \binom{r}{r-2}(-1)^{r-2}c(z^{r-2}-1);$$

$$\binom{r}{r-1}(-1)^{r-1}(x^{r-1}y^{r-1}-x^{r-1}) = \binom{r}{r-1}(-1)^{r-1}c(z^{r-1}-1).$$

The conditions of the lemma assure that r, $\binom{r}{2}$, $\binom{r}{r-2}$ and $\binom{r}{r-1}$ are non-zero, so after dividing with them and for the third and fourth equations also using $y^r = z^r = 1$, we find

$$x(y-1) = c(z-1);$$
$$x^2(y^2-1) = c(z^2-1);$$
$$x^{r-2}(\frac{1}{y^2}-1) = c(\frac{1}{z^2}-1);$$
$$x^{r-1}(\frac{1}{y}-1) = c(\frac{1}{z}-1).$$

Since $y \neq 1$, $z \neq 1$, we can have zero on both sides of any of these equations if $y = z = -1$. In this case $y(z+1)^2 = z(y+1)^2$ is obviously true.

If $y = z = -1$ does not hold, then dividing the first two equations with each other, we have

$$x = \frac{1+z}{1+y},$$

while dividing the third and fourth and after a little manipulation we find

$$x = \frac{(1+y)z}{(1+z)y}.$$

Comparing the two right hand sides, we get $y(z+1)^2 = z(y+1)^2$. □

References

[1] A. Blokhuis, T. Szőnyi, Note on the structure of semiovals in finite projective planes. *Discrete Mathematics* **106/107** (1992) 61-65.

[2] J. W. P. Hirschfeld, *Projective geometries over finite fields*, Clarendon Press, Oxford, 1979, 2nd edition, 1998.

[3] Gy. Kiss, J. Ruff, Note on small semiovals, *Annales Univ. Sci. Budapest*, **47** (2004) 143-151.

[4] Gy. Kiss, Small semiovals in $PG(2,q)$, *J. of Gemetry*, submitted.

[5] J.A. Thas, A combinatorial characterization of Hermitan curves, *Journal of Algebraic Combinatorics* **1** (1992) 97-102.

Authors address: András Gács
Department of Computer Science, Eötvös Loránd University,
H-1117 Budapest, Pázmány Péter sétány 1/C, HUNGARY

e-mail: gacs@cs.elte.hu