On Unitals with many Baer sublines

Simeon Ball, Aart Blokhuis and Christine M. O'Keefe

Abstract

We identify the points of $\mathrm{PG}(2,q)$ with the directions of lines in $\mathrm{GF}(q^3)$, viewed as a 3-dimensional affine space over $\mathrm{GF}(q)$. Within this framework we associate to a unital in $\mathrm{PG}(2,q)$ a certain polynomial in two variables, and show that the combinatorial properties of the unital force certain restrictions on the coefficients of this polynomial. In particular, if $q = p^2$ where p is prime then we show that a unital is classical if and only if at least $(q-2)\sqrt{q}$ secant lines meet it in the points of a Baer subline.

1 Introduction

A *unital* $\mathcal{U}$ in a projective plane π of square order q is a set of $q\sqrt{q}+1$ points, such that each line meets it in either 1 or $\sqrt{q}+1$ points. A line is a *tangent* or a *secant* of $\mathcal{U}$ if it contains 1 or $\sqrt{q}+1$ points of $\mathcal{U}$ respectively. A point P of $\mathcal{U}$ lies on one tangent and q secants, while a point Q not on $\mathcal{U}$ lies on $\sqrt{q}+1$ tangents and $q-\sqrt{q}$ secants. It follows that $\mathcal{U}$ has $q\sqrt{q}+1$ tangents and $q^2-q\sqrt{q}+q$ secants, and 'that the set of tangents of $\mathcal{U}$ form the *dual* unital in the dual plane.

An example of a unital in $\mathrm{PG}(2,q)$ is given by the set of absolute points of a unitary polarity (see Hirschfeld [4]). This is called a *classical unital* (or *Hermitian curve),* and any classical unital is the image under an element of $\mathrm{P\Gamma L}(3,q)$ of the set of points (x_0,x_1,x_2) satisfying the equation $x_0^{\sqrt{q}+1}+x_1^{\sqrt{q}+1}+x_2^{\sqrt{q}+1}=0$.

In 1976, Buekenhout [1] proved the existence of unitals in every translation plane π of square order q with kernel containing $\mathrm{GF}(\sqrt{q})$. In particular, he noted that his construction gave a family of non-classical unitals in $\mathrm{PG}(2,q)$ for $\sqrt{q}>2$ even and not a square. Metz [7], in 1979, extended this observation to the case of $\sqrt{q}$ even and square, and $\sqrt{q}$ odd; hence, for any prime power $\sqrt{q}>2$, there exist non-classical unitals in $\mathrm{PG}(2,q)$. A *Buekenhout-Metz unital* in π is a unital which arises by the construction due to Buekenhout [1, Section 4., Remark (4)]. Since the classical unital in $\mathrm{PG}(2,q)$ can be constructed in this way, it is included in the class of Buekenhout-Metz unitals.

We note that every unital in $\mathrm{PG}(2,2^2)$ is classical and hence is a Buekenhout-Metz unital. Penttila and Royle [8] have shown that every unital in $\mathrm{PG}(2,3^2)$ is a Buekenhout-Metz unital. Further, every known unital in $\mathrm{PG}(2,q)$ is a Buekenhout-Metz unital [2].

The classes of classical and Buekenhout-Metz unitals have been characterised in the class of unitals in $\mathrm{PG}(2,q)$ by various authors; Theorems 1 and 2 are of particular interest to us in this context. Note that a *Baer subplane* of π is a subplane of order $\sqrt{q}$, and any line of π meets a Baer subplane in 1 or $\sqrt{q}+1$ points. A set of $\sqrt{q}+1$ points which is the intersection of a line with a Baer subplane is a *Baer subline.*

Theorem 1 ([3, 6]) Let $\mathcal{U}$ be a unital in $\mathrm{PG}(2,q)$, where q is square. Then $\mathcal{U}$ is classical if and only if each secant to $\mathcal{U}$ intersects it in a Baer subline.

Theorem 2 ([2, 9]) Let $\mathcal{U}$ be a unital in $\mathrm{PG}(2,q)$, where q is square. Then $\mathcal{U}$ is a Buekenhout-Metz unital if and only if there exists a point T of $\mathcal{U}$ such that the points of $\mathcal{U}$ on each of the q secants to $\mathcal{U}$ through T form a Baer subline.

We are interested in the question of how many Baer sublines among secants suffice to characterise the classical unital in $\mathrm{PG}(2,q)$. We know that a classical unital has $q^2 - q\sqrt{q}+q$ Baer sublines while a Buekenhout-Metz unital has at least q Baer sublines, and that a unital with a particular configuration of $q+1$ Baer sublines must be classical, as follows:

Theorem 3 ([6]) Let $\mathcal{U}$ be a unital in $\mathrm{PG}(2,q)$, where q is square. Then $\mathcal{U}$ is classical if and only if there exists a point T of $\mathcal{U}$ such that the points of $\mathcal{U}$ on each of the q secant lines to $\mathcal{U}$ through T form a Baer subline and $\mathcal{U}$ has one further Baer subline among its secants.

Our main result is:

Theorem 4 Let $\mathcal{U}$ be a unital in $\mathrm{PG}(2,q)$, where $q = p^2$ and p is a prime. Then $\mathcal{U}$ is a classical unital if and only if it admits at least $(q-2)\sqrt{q}$ Baer sublines among its secants.

2 Preliminaries

The basic idea of our proof is to first identify the points of $\mathrm{PG}(2,q)$ with the directions of lines in $\mathrm{GF}(q^3)$, viewed as a 3-dimensional affine space over $\mathrm{GF}(q)$. Within this framework we associate to a unital in $\mathrm{PG}(2,q)$ a certain polynomial in two variables, and show that the combinatorial properties of the unital force certain restrictions on the coefficients of this polynomial.

In this section we first describe the representation for $\mathrm{PG}(2,q)$ and then make a preliminary investigation of some polynomials associated with a unital. Finally we review some useful combinatorial identities involving binomial coefficients.

2.1 A representation for PG$(2,q)$

Let $\mathcal{R}$ be the set of (q^2+q+1)-st roots of unity in $\mathrm{GF}(q^3)$, $q>2$. Thus

$$\mathcal{R} = \{x : x \in \mathrm{GF}(q^3) \text{ and } x^{q^2+q+1} = 1\} = \{y^{q-1} : y \in \mathrm{GF}(q^3) \setminus \{0\}\}$$

since for $y \in \mathrm{GF}(q^3) \setminus \{0\}$ we have $(y^{q-1})^{q^2+q+1} = y^{q^3-1} = 1$. We remark that $\mathcal{R}$ is invariant under the automorphism group of $\mathrm{GF}(q^3)$ and the map $x \mapsto x^{-1}$.

We view $\mathrm{GF}(q^3)$ as a 3-dimensional affine space over $\mathrm{GF}(q)$. Each 1-dimensional subspace is associated with an element of $\mathcal{R}$, since the vectors $a, b \in \mathrm{GF}(q^3) \setminus \{0\}$ are linearly dependent over

GF(q) if and only if $a^{q-1} = b^{q-1}$. Thus the points of PG$(2,q)$ are identified with the elements of $\mathcal{R}$. The 2-dimensional subspaces are, for $b \in \mathrm{GF}(q^3) \setminus \{0\}$,

$$\begin{aligned} & \{z \in \mathrm{GF}(q^3) : \mathrm{Tr}(bz) = bz + b^q z^q + b^{q^2} z^{q^2} = 0\} \\ = \; & \{z \in \mathrm{GF}(q^3) \setminus \{0\} : \text{ and } 1 + (by)^{q-1} + (by)^{q^2-1} = 0\} \cup \{0\}. \end{aligned}$$

Writing $x = y^{q-1}$ and $\delta = b^{q-1}$ gives:

$$\{x : x \in \mathcal{R} \text{ and } 1 + \delta x + \delta^{q+1} x^{q+1} = 0\} = \{x : x \in \mathcal{R} \text{ and } x^{q+1} + \delta^{-q} x + \delta^{q^2} = 0\}.$$

We substitute $\epsilon = \delta^{-q} \in \mathcal{R}$, so that the lines of PG$(2,q)$ are, for $\epsilon \in \mathcal{R}$,

$$\ell_\epsilon = \{x : x \in \mathcal{R} \text{ and } x^{q+1} + \epsilon x + \epsilon^{-q} = 0\}.$$

The line of PG$(2,q)$ joining the points $x, y \in \mathcal{R}$ is ℓ_ϵ where $\epsilon = -(x^{q+1} - y^{q+1})/(x-y)$. It follows that points $x, y, z \in \mathcal{R}$ are collinear if and only if

$$\frac{x^{q+1} - y^{q+1}}{x - y} = \frac{x^{q+1} - z^{q+1}}{x - z};$$

so the points $1/x, y, z \in \mathcal{R}$ are collinear if and only if

$$\frac{1 - x^{q+1} y^{q+1}}{1 - xy} = \frac{1 - x^{q+1} z^{q+1}}{1 - xz}$$

which is if and only if

$$xy(1-xy)^{q-1} = xz(1-xz)^{q-1}$$

(using the observation that $1 - (1 - z^{q+1})/(1-z) = -z(1-z)^{q-1}$). In this way, with each line on $1/x$ there is associated an element $u(1-u)^{q-1}$ for some $u \in \mathcal{R} \setminus \{1\}$. There are $q+1$ such lines, and the set of values associated with them is exactly the set of roots of the equation $1 + t + t^{q+1} = 0$. To see this, let $t = u(1-u)^{q-1}$ where $u \in \mathcal{R} \setminus \{1\}$ and note that

$$(1-u)(1 + t + t^{q+1}) = 1 - u + u - u^{q+1} + u^{q+1} - u^{q^2+q+1} = 0.$$

It follows that if $y_0, y_1, \ldots, y_q$ are $q+1$ points of PG$(2,q)$, no two of which are collinear with $1/x$, then the values $xy_i(1-xy_i)^{q-1}$ for $i = 0, 1, \ldots, q$ are exactly the roots of the equation $1+t+t^{q+1} = 0$ in GF(q^3). In other words,

$$\prod_{i=0}^{q} \left(t - xy_i(1-xy_i)^{q-1}\right) = 1 + t + t^{q+1}$$

and hence

$$\begin{aligned} \prod_{i=0}^{q} \left(1 + xy_i(1-xy_i)^{q-1} t\right) &= 1 - t^q + t^{q+1} \\ \prod_{i=0}^{q} \left(1 - \frac{1 - (xy_i)^{q+1}}{1 - xy_i} t\right) &= 1 - t + t^{q+1} \end{aligned}$$

2.2 Unitals in $\mathbf{PG}(2,q)$

Let $\mathcal{U}\subset\mathcal{R}$ be a unital in $\mathrm{PG}(2,q)$, where q is a square. We define the polynomial $F\in \mathrm{GF}(q^3)[t,x]$ in two variables and the polynomials $\alpha_j\in\mathrm{GF}(q^3)[x]$ in one variable, for $j=0,1,\ldots,q^2-q\sqrt{q}+q$, by

$$F(t,x)=\prod_{c\in\mathcal{R}\setminus\mathcal{U}}\Big(1+cx(1-cx)^{q-1}t\Big)=\sum_{j=0}^{q^2-q\sqrt{q}+q}\alpha_j(x)\,t^j. \tag{1}$$

Let $1/x_0\in\mathcal{U}$. The tangent to $\mathcal{U}$ on $1/x_0$ contains q points of $\mathcal{R}\setminus\mathcal{U}$, while each other line on $1/x_0$ contains $q-\sqrt{q}$ points of $\mathcal{R}\setminus\mathcal{U}$. Thus in the multiset $\{cx_0(1-cx_0)^{q-1}:c\in\mathcal{R}\setminus\mathcal{U}\}$ each root of $1-t^q+t^{q+1}=0$ occurs $q-\sqrt{q}$ times and one root occurs a further $\sqrt{q}$ times; so

$$\begin{aligned}F(t,x_0)&=\Big(1-t^q+t^{q+1}\Big)^{q-\sqrt{q}}(1+\beta t)^{\sqrt{q}}\quad\text{for some }\beta\in\mathrm{GF}(q^3)\\&=\Big(1-t^q+t^{q+1}\Big)^{q-\sqrt{q}}\Big(1+\alpha_{\sqrt{q}}(x_0)t^{\sqrt{q}}\Big)\end{aligned}\tag{2}$$

where the coefficient of $t^{\sqrt{q}}$ in the last factor is determined by comparing coefficients with Equation (1).

Similarly, consider $1/x_0\in\mathcal{R}\setminus\mathcal{U}$. Each of the $\sqrt{q}+1$ tangents to $\mathcal{U}$ on $1/x_0$ contains $q-1$ points of $\mathcal{R}\setminus(\mathcal{U}\cup\{1/x_0\})$, and each of the $q-\sqrt{q}$ secants to $\mathcal{U}$ on $1/x_0$ contains $q-\sqrt{q}-1$ points of $\mathcal{R}\setminus(\mathcal{U}\cup\{1/x_0\})$. Hence, in the multiset $\{cx_0(1-cx_0)^{q-1}:c\in\mathcal{R}\setminus\mathcal{U}\}$ the value 0 occurs once (when $c=1/x_0$), each root of $1-t^q+t^{q+1}=0$ occurs $q-\sqrt{q}-1$ times and $\sqrt{q}+1$ roots each occur a further $\sqrt{q}$ times. Then

$$F(t,x_0)=\Big(1-t^q+t^{q+1}\Big)^{q-\sqrt{q}-1}L(t,x_0)$$

where $L(t,x_0)$ is the polynomial in t which is the product of $\sqrt{q}+1$ terms of the form $(1+\beta t^{\sqrt{q}})$ for β a root of $1-t^q+t^{q+1}=0$ corresponding to a tangent on $1/x_0$. In particular it is a $\sqrt{q}$th power polynomial with degree $q+\sqrt{q}$. It follows immediately that $F(t,x_0)=L(t,x_0)\,(1+t^q-t^{q+1}+$ *terms of degree at least* $2q)$, and comparing this with Equation (1) shows that

$$L(t,x_0)=\sum_{i=0}^{\sqrt{q}-1}\alpha_{i\sqrt{q}}(x_0)t^{i\sqrt{q}}+(\alpha_q(x_0)-1)t^q+(\alpha_{q+\sqrt{q}}(x_0)-\alpha_{\sqrt{q}}(x_0))t^{q+\sqrt{q}}. \tag{3}$$

We emphasise that L is a $\sqrt{q}$-th power of a polynomial in t, and for $1/x_0\in\mathcal{R}\setminus\mathcal{U}$ the $\sqrt{q}+1$ roots of $L(t,x_0)=0$ correspond to the directions of the tangents on $1/x_0$. This observation will be important later, since our eventual aim will be to control the coefficients of L. The first step is to show that many of the α_j are identically zero.

For $1/x_0\in\mathcal{U}$, we see that $F(t,x_0)$ is a $\sqrt{q}$-th power, so if $j\not\equiv 0\pmod{\sqrt{q}}$ then $\alpha_j(x_0)=0$ for all $1/x_0\in\mathcal{U}$. For $1/x_0\in\mathcal{R}\setminus\mathcal{U}$, the polynomial $F(t,x_0)$ is the product of the polynomial $(1+t^q+$ *higher order terms*) with $L(t,x_0)$. Thus for $j<q$ and $j\not\equiv 0\pmod{\sqrt{q}}$ we have $\alpha_j(x_0)=0$ for all $1/x_0\in\mathcal{R}\setminus\mathcal{U}$. It follows that for $j<q$ and $j\not\equiv 0\pmod{\sqrt{q}}$ we have $\alpha_j(x_0)=0$ for all $1/x_0\in\mathcal{R}$, so α_j is a polynomial with at least q^2+q+1 zeros but with degree less than q^2 (for by definition α_j has degree at most jq). Hence for $j<q$ and $j\not\equiv 0\pmod{\sqrt{q}}$ the polynomial α_j is identically zero; so

$$F(t,x)=\sum_{j=0}^{\sqrt{q}}\alpha_{j\sqrt{q}}(x)t^{j\sqrt{q}}+\sum_{j=q+1}^{q^2-q\sqrt{q}+q}\alpha_j(x)\,t^j. \tag{4}$$

2.3 Some combinatorial identities

Throughout the paper we shall be investigating polynomials and at various times use some well-known binomial identities and Lucas' theorem. We list the possibly less well-known identities here.

Lemma 5 Let b be a non-negative integer and let $q = p^{2h}$ for some prime p and integer h. Then

1.
$$\binom{a}{b} = (-1)^b \binom{-a+b-1}{b}$$

2.
$$\sum_{e=0}^{b} \binom{a}{b-e}\binom{c}{e} = \binom{a+c}{b}$$

3. (Lucas' Theorem). Let $a = a_0 + a_1 p + a_2 p^2 + \ldots$ and $b = b_0 + b_1 p + b_2 p^2 + \ldots$ be the p-ary expansions of the non-negative integers a and b. Then
$$\binom{a}{b} = \binom{a_0}{b_0}\binom{a_1}{b_1}\binom{a_2}{b_2}\cdots \pmod p. \tag{5}$$
In particular, when $b < q$ we have
$$\binom{q-1}{b} = (-1)^b \pmod p.$$

3 Further technical results on unital polynomials

Let $q = p^{2h}$ for some prime p and let $\mathcal{U}$ be a unital in $\mathrm{PG}(2, q)$.

Recall from Section 2.2 that with $\mathcal{U}$ there are associated polynomials α_j for $j = 0, \ldots, q^2 - q\sqrt{q} + q$, which are symmetric expressions in the collection of points of $\mathcal{R} \setminus \mathcal{U}$. The fact that many of these polynomials α_j are identically zero therefore gives many relations that must be satisfied by the points of $\mathcal{R} \setminus \mathcal{U}$. However these relations are a bit hard to handle; it turns out that multiplying each α_j by a suitable locator polynomial $\overline{U}$, as follows, makes them much more managable. In this section we further investigate the polynomials α_j via the products $\overline{U}\alpha_j$ which are written in terms of symmetric functions which we denote by $\varepsilon_{s,n}$. In particular, Lemma 6 shows that many of the $\varepsilon_{s,n}$ are functions of those of the form $\varepsilon_{r\sqrt{q},n}$, which are then the subject of Lemma 9.

First we define three *locator polynomials* in $\mathrm{GF}(q^3)[x]$. The locator polynomial for $\mathcal{U}$ is
$$U(x) = \prod_{c \in \mathcal{U}} (1 - cx),$$
while the locator polynomial for the complement $\mathcal{R} \setminus \mathcal{U}$ is
$$\overline{U}(x) = \prod_{c \in \mathcal{R}\setminus\mathcal{U}} (1 - cx) = \sum_{j=0}^{q^2 - q\sqrt{q} + q} (-1)^j \sigma_j x^j$$

where σ_j is the j-th elementary symmetric function of the elements of $\mathcal{R}\setminus\mathcal{U}$. The locator polynomial for $\mathcal{R}$ is

$$Z(x) = \prod_{c\in\mathcal{R}}(1-cx) = U(x)\overline{U}(x) = 1 - x^{q^2+q+1}.$$

For non-negative integers s and n let

$$\varepsilon_{s,n} = \sum (c_1\dots c_s)^{q+1}c_{s+1}\dots c_{n-sq}$$

where the sum is over all possible choices of distinct $c_1,\dots,c_{n-sq}\in\mathcal{R}\setminus\mathcal{U}$. We note that $\varepsilon_{0,n}=\sigma_n$ and use the convention that $\varepsilon_{s,n}=0$ for $n-sq<s$ and $n-sq>|\mathcal{R}\setminus\mathcal{U}|$, that is, for $n<s(q+1)$ and $n>q^2-q\sqrt{q}+q+sq$.

It follows that, for $j=0,\dots,q^2-q\sqrt{q}+q$,

$$\begin{aligned}\overline{U}(x)\alpha_j(x) &= \sum c_1\dots c_j x^j(1-c_1^q x^q)\dots(1-c_j^q x^q)(1-c_{j+1}x)\dots(1-c_{|\mathcal{R}\setminus\mathcal{U}|}x)\\ &= \sum_{s=0}^{j}\sum_{n=0}^{\infty}\binom{n-sq-s}{j-s}\varepsilon_{s,n}(-1)^{n-j}x^n \qquad (6)\end{aligned}$$

where, in the first line, the sum is over all choices of distinct elements $c_1,\dots,c_j\in\mathcal{R}\setminus\mathcal{U}$ and $\{c_1,\dots,c_{|\mathcal{R}\setminus\mathcal{U}|}\}=\mathcal{R}\setminus\mathcal{U}$.

In the next lemma we show that many of the $\varepsilon_{s,n}$ are functions of those of the form $\varepsilon_{r\sqrt{q},n}$.

Lemma 6 For non-negative integers $0\le r,i<\sqrt{q}$ and $n\ge(r\sqrt{q}+i)(q+1)$ we have:

$$\varepsilon_{r\sqrt{q}+i,n} = \binom{i-n-1}{i}\varepsilon_{r\sqrt{q},n}.$$

Proof: First, the relation holds when $i=0$ and for all $0\le r<\sqrt{q}$ and $n\ge r\sqrt{q}(q+1)$. For the inductive hypothesis assume that for $r\sqrt{q}\le s<r\sqrt{q}+i$ and $0\le r<\sqrt{q}$, but $s\ge 1$, we have

$$\varepsilon_{s,n} = \binom{s-r\sqrt{q}-n-1}{s-r\sqrt{q}}\varepsilon_{r\sqrt{q},n}$$

for all $n\ge(r\sqrt{q}+i)(q+1)$. By the discussion preceding Equation (4), $\overline{U}\alpha_{r\sqrt{q}+i}$ is identically zero, hence the coefficient of $(-1)^{n-r\sqrt{q}-i}x^n$ is zero, that is,

$$\sum_{s=0}^{r\sqrt{q}+i}\binom{n-sq-s}{r\sqrt{q}+i-s}\varepsilon_{s,n}=0$$

for all n. Now the coefficient of $\varepsilon_{r\sqrt{q}+i,n}$ in this expression is 1; so $\varepsilon_{r\sqrt{q}+i,n}$ is a linear combination of the $\varepsilon_{s,n}$ with $0\le s<r\sqrt{q}+i$ and we prove the lemma by checking that the corresponding linear combination still holds when we have substituted according to our claim. Applying Lucas' Theorem to the binomial coefficient (to reduce the upper entry modulo q) and writing $s=d\sqrt{q}+e$ gives:

$$\sum_{d=0}^{r-1}\sum_{e=0}^{\sqrt{q}-1}\binom{n-d\sqrt{q}-e}{r\sqrt{q}+i-d\sqrt{q}-e}\varepsilon_{d\sqrt{q}+e,n}+\sum_{e=0}^{i}\binom{n-r\sqrt{q}-e}{i-e}\varepsilon_{r\sqrt{q}+e,n}=0$$

and, on substitution, we see that we must prove that the following expression is zero:

$$\sum_{d=0}^{r-1}\sum_{e=0}^{\sqrt{q}-1}\binom{n-d\sqrt{q}-e}{r\sqrt{q}+i-d\sqrt{q}-e}\binom{e-n-1}{e}\varepsilon_{d\sqrt{q},n}+\sum_{e=0}^{i}\binom{n-r\sqrt{q}-e}{i-e}\binom{e-n-1}{e}\varepsilon_{r\sqrt{q},n}.$$

By Lemma 5(3), this is:

$$=\sum_{d=0}^{r-1}\sum_{e=0}^{\sqrt{q}-1}\binom{-n+r\sqrt{q}+i-1}{r\sqrt{q}+i-d\sqrt{q}-e}\binom{n}{e}(-1)^{r+i-d}\varepsilon_{d\sqrt{q},n}+\sum_{e=0}^{i}\binom{-n+r\sqrt{q}+i-1}{i-e}\binom{n}{e}(-1)^{i}\varepsilon_{r\sqrt{q},n}.$$

Now using Lucas' Theorem several times and rearranging yields:

$$\begin{aligned}
= \ & \sum_{d=0}^{r-1}\binom{-n+r\sqrt{q}+i-1}{r\sqrt{q}-d\sqrt{q}}(-1)^{r+i-d}\sum_{e=0}^{i}\binom{-n+i-1}{i-e}\binom{n}{e}\varepsilon_{d\sqrt{q},n}\\
& +\sum_{d=0}^{r-1}\binom{-n+r\sqrt{q}+i-1}{r\sqrt{q}-d\sqrt{q}-\sqrt{q}}(-1)^{r+i-d}\sum_{e=i+1}^{\sqrt{q}-1}\binom{-n+i-1}{\sqrt{q}+i-e}\binom{n}{e}\varepsilon_{d\sqrt{q},n}\\
+ \ & \sum_{e=0}^{i}\binom{-n+i-1}{i-e}(-1)^{i}\binom{n}{e}\varepsilon_{r\sqrt{q},n}.
\end{aligned}$$

This is zero since

$$\sum_{e=0}^{i}\binom{-n+i-1}{i-e}\binom{n}{e}=\binom{i-1}{i}=0$$

and, for $e=i+1,\ldots,\sqrt{q}-1$ then (using Lemma 5(1))

$$\binom{-n+i-1}{\sqrt{q}+i-e}\binom{n}{e}=(-1)^{i-e+1}\binom{n+\sqrt{q}-e}{\sqrt{q}+i-e}=0$$

since otherwise, with $n_0=n \pmod{\sqrt{q}}$, we have $n_0\ge e$ and $n_0-e\ge\sqrt{q}+1-e$ which is impossible as $n_0<\sqrt{q}$. □

We now direct our attention to the polynomials $\overline{U}\alpha_{r\sqrt{q}}$ for $r=2,3,\ldots,\sqrt{q}-1$, by substituting the expressions for $\varepsilon_{s,j}$ in terms of $\varepsilon_{r\sqrt{q},j}$ determined in Lemma 6 into the expression in Equation (6).

Lemma 7 For $r=2,3,\ldots,\sqrt{q}-1$ we have:

$$\overline{U}(x)\alpha_{r\sqrt{q}}(x)=\sum_{d=0}^{r}\sum_{n=d\sqrt{q}(q+1)}^{\infty}(-1)^{n+r}\binom{n_1-d}{r-d}\varepsilon_{d\sqrt{q},n}x^n$$

where $n=n_0+n_1\sqrt{q} \pmod q$ for $0\le n_0,n_1<\sqrt{q}$.

Proof: By Equation (6), we have

$$\overline{U}(x)\alpha_{r\sqrt{q}}(x)=\sum_{s=0}^{r\sqrt{q}}\sum_{n=0}^{\infty}\binom{n-sq-s}{r\sqrt{q}-s}\varepsilon_{s,n}(-1)^{n+r}x^n=\sum_{n=0}^{\infty}c_nx^n.$$

As in the proof of Lemma 6, we apply Lucas' Theorem and write $s = d\sqrt{q} + e$ to obtain:

$$c_n = \left(\sum_{d=0}^{r-1}\sum_{e=0}^{\sqrt{q}-1}\binom{n-d\sqrt{q}-e}{r\sqrt{q}-d\sqrt{q}-e}\varepsilon_{d\sqrt{q}+e,n}(-1)^{n+r}\right) + \varepsilon_{r\sqrt{q},n}(-1)^{n+r}$$

which, by Lemma 6, is

$$= \left(\sum_{d=0}^{r-1}\sum_{e=0}^{\sqrt{q}-1}\binom{n-d\sqrt{q}-e}{r\sqrt{q}-d\sqrt{q}-e}\binom{e-n-1}{e}\varepsilon_{d\sqrt{q},n}(-1)^{n+r}\right) + \varepsilon_{r\sqrt{q},n}(-1)^{n+r}.$$

Write $n_0 = n \pmod{\sqrt{q}}$. If $e > 0$ then

$$\binom{n-d\sqrt{q}-e}{r\sqrt{q}-d\sqrt{q}-e}\binom{e-n-1}{e} = 0,$$

for the second binomial coefficient is zero unless $n_0 \geq e$ in which case the first binomial coefficient is zero unless $n_0 - e > \sqrt{q} - e$; which is impossible. Thus

$$c_n = \left(\sum_{d=0}^{r-1}\binom{n-d\sqrt{q}}{r\sqrt{q}-d\sqrt{q}}\varepsilon_{d\sqrt{q},n}(-1)^{n+r}\right) + \varepsilon_{r\sqrt{q},n}(-1)^{n+r}$$

and the lemma is proved. □

Looking again at Equation (2), for $r = 2, 3, \ldots, \sqrt{q}-1$ we have $\alpha_{r\sqrt{q}}(1/x_0) = 0$ for all $1/x_0 \in \mathcal{U}$; so U divides $\alpha_{r\sqrt{q}}$ and we now calculate the corresponding quotient polynomials.

Lemma 8 For $r = 2, 3, \ldots, \sqrt{q}-1$, we have $\overline{U}\alpha_{r\sqrt{q}} = ZQ_r$ where

$$Q_r(x) = \sum_{d=0}^{r-2}\sum_{n=d\sqrt{q}(q+1)}^{(r-1)q\sqrt{q}-1}(-1)^{n+r}\binom{n_1-d}{r-d}\varepsilon_{d\sqrt{q},n}x^n$$

and has degree at most $(r-1)q\sqrt{q}-1$.

Proof: Since $U|\alpha_{r\sqrt{q}}$ and $U\overline{U} = Z$, we see that $Z|\overline{U}\alpha_{r\sqrt{q}}$. Let Q_r be such that $\overline{U}\alpha_{r\sqrt{q}} = ZQ_r$; it follows that the degree of Q_r is at most $(r-1)q\sqrt{q}-1 < q^2 - q\sqrt{q} - 1$. Now $\overline{U}(x)\alpha_{r\sqrt{q}}(x) = Z(x)Q_r(x) = Q_r(x) - x^{q^2+q+1}Q_r(x)$; so $Q_r(x)$ coincides with the terms of degree up to $(r-1)q\sqrt{q}-1$ in $\overline{U}(x)\alpha_{r\sqrt{q}}(x)$ and the result follows. □

Now we prove some further relationships between the $\varepsilon_{s,n}$.

Lemma 9 1. For $2 \leq d < \sqrt{q}$ and $d\sqrt{q}(q+1) \leq n < q^2+q+1$ we have:

$$\varepsilon_{d\sqrt{q},n} = (-1)^{d+1}\left(\binom{n_1-1}{d-1}\varepsilon_{\sqrt{q},n} + (d-1)\binom{n_1}{d}\sigma_n\right).$$

2. For $2 \le r < \sqrt{q}$ and $(r-1)\sqrt{q}(q+1) \le n < r\sqrt{q}(q+1)$ we have:

$$\binom{n_1-1}{r-1}\varepsilon_{\sqrt{q},n} + (r-1)\binom{n_1}{r}\sigma_n = 0.$$

Proof: (1) For $2 \le r < \sqrt{q}$ and $r\sqrt{q}(q+1) \le n < q^2+q+1$, looking at the coefficient of x^n in the identity $\overline{U}\alpha_{r\sqrt{q}} = ZQ_r$ yields:

$$\sum_{d=0}^{r}\binom{n_1-d}{r-d}\varepsilon_{d\sqrt{q},n} = 0$$

where $n = n_0 + n_1\sqrt{q} \pmod{q}$ for $0 \le n_0, n_1 < \sqrt{q}$ (see Lemma 7). Since $\varepsilon_{r\sqrt{q},n}$ occurs with coefficient 1 in this expression, we prove the lemma by substituting for $\varepsilon_{d\sqrt{q},n}$, for $2 \le d < r$, according to our claim. We therefore consider

$$\begin{aligned}
&\sum_{d=0}^{r}\binom{n_1-d}{r-d}(-1)^{d+1}\left(\binom{n_1-1}{d-1}\varepsilon_{\sqrt{q},n} + (d-1)\binom{n_1}{d}\sigma_n\right)\\
=\ &\sum_{d=0}^{r}\left(\binom{n_1-1}{r-1}(-1)^{d+1}\binom{r-1}{d-1}\varepsilon_{\sqrt{q},n} + \binom{d-1}{1}(-1)^{d+1}\binom{r}{d}\binom{n_1}{r}\sigma_n\right)\\
=\ &-\sum_{d=0}^{r}\binom{n_1-1}{r-1}\binom{\sqrt{q}-1}{\sqrt{q}-1-d}\binom{r-1}{d-1}\varepsilon_{\sqrt{q},n} - \sum_{d=2}^{r}\binom{\sqrt{q}-2}{\sqrt{q}-d}\binom{r}{d}\binom{n_1}{r}\sigma_n + \binom{n_1}{r}\sigma_n.
\end{aligned}$$

Now by Lemma 5(2), this expression is

$$= -\binom{\sqrt{q}+r-2}{\sqrt{q}-2}\binom{n_1-1}{r-1}\varepsilon_{\sqrt{q},n} - \binom{\sqrt{q}+r-2}{\sqrt{q}}\binom{n_1}{r}\sigma_n + \binom{n_1}{r}\sigma_n.$$

Since $2 \le r < \sqrt{q}$, the first term is zero and the remaining two terms cancel.

(2) Again, for $2 \le r < \sqrt{q}$ and $(r-1)\sqrt{q}(q+1) \le n < r\sqrt{q}(q+1)$, looking at the coefficient of x^n in the identity $\overline{U}\alpha_{r\sqrt{q}} = ZQ_r$ gives:

$$0 = \sum_{d=0}^{r-1}\binom{n_1-d}{r-d}\varepsilon_{d\sqrt{q},n}$$

where $n = n_0 + n_1\sqrt{q} \pmod{q}$ for $0 \le n_0, n_1 < \sqrt{q}$ (see Lemma 7). By Part (1) of this lemma, this is:

$$= \sum_{d=1}^{r-1}(-1)^d\binom{n_1-1}{r-1}\binom{r-1}{d-1}\varepsilon_{\sqrt{q},n} + \sum_{d=0}^{r-1}\binom{d-1}{1}(-1)^d\binom{n_1}{r}\binom{r}{d}\sigma_n$$

and similar manipulations to those used in Part (1) yield:

$$= \sum_{d=1}^{r-1}\binom{n_1-1}{r-1}\binom{r-1}{d-1}\binom{\sqrt{q}-1}{\sqrt{q}-1-d}\varepsilon_{\sqrt{q},n} + \left[-1 + \sum_{d=2}^{r-1}\binom{-2}{d-2}\binom{r}{r-d}\right]\binom{n_1}{r}\sigma_n.$$

By Lemma 5(2), we have:

$$= \left(\binom{\sqrt{q}+r-2}{\sqrt{q}-2} - (-1)^r\right)\binom{n_1-1}{r-1}\varepsilon_{\sqrt{q},n} + \left(-1+1-\binom{-2}{r-2}\right)\binom{n_1}{r}\sigma_n$$

$$\begin{aligned}
&= -(-1)^r\binom{n_1-1}{r-1}\varepsilon_{\sqrt{q},n} + (-1)^{r+1}\binom{r-1}{1}\binom{n_1}{r}\sigma_n \\
&= \binom{n_1-1}{r-1}\varepsilon_{\sqrt{q},n} + \binom{r-1}{1}\binom{n_1}{r}\sigma_n.
\end{aligned}$$

□

4 Unitals with many Baer sublines

¿From now on we assume that q is an odd square and let $\mathcal{U}$ be a unital in $\mathrm{PG}(2,q)$. We are interested in the case in which $\mathcal{U}$ admits many Baer sublines among its secants. We find it more convenient to use the dual unital; noting that if the points of $\mathcal{U}$ on a secant line form a Baer subline then the tangents of the dual unital on a point of $\mathrm{PG}(2,q)\setminus\mathcal{U}$ have the structure of a dual Baer subline.

In this section we define dual Baer sublines and demonstrate some of their properties. We then restrict our attention to the case of $q=p^2$, where p is prime, and show that a unital in $\mathrm{PG}(2,q)$ with many Baer sublines among its secants must be classical.

4.1 Dual Baer sublines

Throughout this subsection, we assume that q is an odd square. A *dual Baer subline* is a collection of lines on a point x of $\mathrm{PG}(2,q)$ which are also lines of a Baer subplane on x. In other words, the lines of a dual Baer subline form a Baer subline in the dual of $\mathrm{PG}(2,q)$. In the next lemma we calculate a polynomial associated with such a dual Baer subline.

Lemma 10 Let q be an odd square and let $\ell_0,\dots,\ell_{\sqrt{q}}$ be distinct lines on a point $1/x$ of $\mathrm{PG}(2,q)$. For $i=0,\dots,\sqrt{q}$ let $z_i\in\ell_i\cap\mathcal{B}$. Then $\{\ell_0,\dots,\ell_{\sqrt{q}}\}$ is a dual Baer subline if and only if

$$\prod_{i=0}^{\sqrt{q}}\left(1-\frac{1-(xz_i)^{q+1}}{1-xz_i}t\right) = 1+a\,t+d\,t^{\sqrt{q}}+e\,t^{\sqrt{q}+1}$$

for some $a,d,e\in\mathrm{GF}(q^3)$ such that $1+a\,t+d\,t^{\sqrt{q}}+e\,t^{\sqrt{q}+1}$ divides $1-t^q+t^{q+1}$.

Proof: First suppose that $\{\ell_0,\dots,\ell_{\sqrt{q}}\}$ is a dual Baer subline; so $\{\ell_0,\dots,\ell_{\sqrt{q}}\}$ are all lines of a Baer subplane $\mathcal{B}$ on $1/x$. Now $\mathcal{B}$ corresponds to a 3-dimensional vector subspace of $\mathrm{GF}(q^3)$ of order $\sqrt{q}$, and without loss of generality let $1,b,c\in\mathrm{GF}(q^3)\setminus\{0\}$ be such that this vector subspace is:

$$\{(\alpha+\beta b+\gamma c):\alpha,\beta,\gamma\in\mathrm{GF}(\sqrt{q})\}.$$

Then $1/x=1$, $y_0=b^{q-1}$ and $y_i=(b+c\lambda_i)^{q-1}$, for $i=1,\dots,\sqrt{q}$ (where $\{\lambda_i : i=1,\dots,\sqrt{q}\} = \mathrm{GF}(\sqrt{q})$), are points of $\mathrm{PG}(2,q)$, which lie in $\mathcal{B}$. In particular, the points $y_0,\dots,y_{\sqrt{q}}$ lie one on each of the $\sqrt{q}+1$ lines of $\mathcal{B}$ on $1/x$. Thus the product we seek is:

$$\prod_{i=0}^{\sqrt{q}}\left(1-\frac{1-(xy_i)^{q+1}}{1-xy_i}t\right) = \left(1-\frac{1-c^{q^2-1}}{1-c^{q-1}}t\right)\prod_{i=1}^{\sqrt{q}}\left(1-\frac{1-(b+c\lambda_i)^{q^2-1}}{1-(b+c\lambda_i)^{q-1}}t\right)$$

$$= \left(1-\frac{c-c^{q^2}}{c-c^q}t\right)\prod_{i=1}^{\sqrt{q}}\left(1-\frac{(b+c\lambda_i)-(b+c\lambda_i)^{q^2}}{(b+c\lambda_i)-(b+c\lambda_i)^q}t\right)$$
$$= \frac{(z-vt)}{z}\prod_{i=1}^{\sqrt{q}}\left(1-\frac{u+v\lambda_i}{w+z\lambda_i}t\right)$$

where $u=b-b^{q^2}, v=c-c^{q^2}, w=b-b^q$ and $z=c-c^q$. Now rearranging and using the fact that $\prod_{i=1}^{\sqrt{q}}(A+B\lambda_i)=A^{\sqrt{q}}-AB^{\sqrt{q}-1}$ this product is:

$$\begin{aligned}
&= \frac{(z-vt)}{z}\left(\frac{\prod_{i=1}^{\sqrt{q}}((w-ut)-(vt-z)\lambda_i)}{\prod_{i=1}^{\sqrt{q}}(w-(-z)\lambda_i)}\right)\\
&= \frac{(z-vt)}{z}\left(\frac{(w-ut)^{\sqrt{q}}-(w-ut)(vt-z)^{\sqrt{q}-1}}{w^{\sqrt{q}}-wz^{\sqrt{q}-1}}\right)\\
&= \frac{(w-ut)^{\sqrt{q}}(z-vt)-(w-ut)(z-vt)^{\sqrt{q}}}{w^{\sqrt{q}}z-wz^{\sqrt{q}}}\\
&= 1+\frac{uz^{\sqrt{q}}-w^{\sqrt{q}}v}{w^{\sqrt{q}}z-wz^{\sqrt{q}}}t+\frac{wv^{\sqrt{q}}-u^{\sqrt{q}}z}{w^{\sqrt{q}}z-wz^{\sqrt{q}}}t^{\sqrt{q}}+\frac{u^{\sqrt{q}}v-uv^{\sqrt{q}}}{w^{\sqrt{q}}z-wz^{\sqrt{q}}}t^{\sqrt{q}+1}\\
&= 1+a\,t+d\,t^{\sqrt{q}}+e\,t^{\sqrt{q}+1}
\end{aligned}$$

which, by definition, divides $1-t^q+t^{q+1}$.

For the converse, let $g(t)=1+a\,t+d\,t^{\sqrt{q}}+e\,t^{\sqrt{q}+1}$, for some $a,d,e\in\mathrm{GF}(q^3)$, divide $1-t^q+t^{q+1}$; so in particular g is reducible into distinct linear factors. We note that g also divides $g^{\sqrt{q}}$; so g divides

$$\begin{aligned}
&(1+at+dt^{\sqrt{q}}+et^{\sqrt{q}+1})^{\sqrt{q}}(1-t)+(1-t^q+t^{q+1})(d^{\sqrt{q}}+e^{\sqrt{q}}t^{\sqrt{q}})\\
=\ &(1+d^{\sqrt{q}})-t+(a^{\sqrt{q}}+e^{\sqrt{q}})t^{\sqrt{q}}-a^{\sqrt{q}}t^{\sqrt{q}+1}.
\end{aligned}$$

But this polynomial has the same degree as g, so they differ by a constant multiple. Equating coefficients shows that $d=-a^{\sqrt{q}+1}(a+1)^q$, $e=a^{\sqrt{q}+1}$ and a satisfies the equation

$$a^{q\sqrt{q}+q+\sqrt{q}+1}+a^{q+\sqrt{q}+1}-a-1=(a^{q+1}+a+1)(a^{q+1}(a^{q+1}+a+1)^{\sqrt{q}-1}-1)=0.$$

But if $a^{q+1}+a+1=0$ then $e=ad$ and $g(t)=(1+at)(1+dt^{\sqrt{q}})$, contradicting the fact that g reduces into different linear factors. Hence a satisfies the equation $a^{q+1}(a^{q+1}+a+1)^{\sqrt{q}-1}-1=0$ of degree $(q+1)\sqrt{q}$. To finish the proof, we just observe that the number of dual Baer sublines on a point of $\mathrm{PG}(2,q)$ is $\sqrt{q}(q+1)$. □

Now let $\mathcal{S}\subseteq\mathcal{R}\setminus\mathcal{U}$ be the set of points s such that the tangents to $\mathcal{U}$ on s form a dual Baer subline. Define the polynomial

$$S(x)=\prod_{s\in\mathcal{S}}(1-sx).$$

Now for $1/x_0\in\mathcal{R}\setminus\mathcal{U}$ and for $r=2,3,\ldots,\sqrt{q}-1$, the coefficient of $t^{r\sqrt{q}}$ in $L(t,x_0)$ is just $\alpha_{r\sqrt{q}}(x_0)$, see Equation (3). But by the previous Lemma, this is zero, so for all $r=2,3,\ldots,\sqrt{q}-1$ we have $\alpha_{r\sqrt{q}}(x_0)=0$ for all $1/x_0\in\mathcal{S}$; so $S\mid\alpha_{r\sqrt{q}}$ for all $r=2,3,\ldots,\sqrt{q}-1$. Further, we observe that $S\mid Q_r$ since $\overline{U}\alpha_{r\sqrt{q}}=\overline{U}UQ_r$ and S and U have no common factors.

Lemma 11 With the notation introduced above, suppose that $|\mathcal{S}| \geq (q-2)\sqrt{q}$ where $q = p^{2h}$ and p is an odd prime. For $2 \leq k < p$ and $n < (k-1)q\sqrt{q}$ we have

$$\binom{n_1}{k}\sigma_n = 0 \quad \text{and} \quad \binom{n_1-1}{k-1}\varepsilon_{\sqrt{q},n} = 0,$$

where $n = n_0 + n_1\sqrt{q} \pmod q$ for $0 \leq n_0, n_1 < \sqrt{q}$.

Proof: We prove this by induction on $k \geq 2$. First, note that the coefficient of x^n in $Q_2(x)$ is zero unless $n_1 \geq 2$, equivalently $n \geq 2\sqrt{q}$, so $x^{2\sqrt{q}}|Q_2(x)$. Also, $S|Q_2$ and the degree of $x^{2\sqrt{q}}S$ is at least $q\sqrt{q}$ which is greater than the degree of Q_2; so $Q_2 \equiv 0$. Thus, by Lemma 8,

$$Q_2(x) = \sum_{n=0}^{q\sqrt{q}-1} (-1)^n \binom{n_1}{2}\sigma_n x^n \equiv 0.$$

Since also $\varepsilon_{\sqrt{q},n} = 0$ for $n < \sqrt{q}(q+1)$, the claim is true for $k = 2$.

Assume that the lemma holds for all $2 \leq r < k$. In particular, when $r = k-1$ then for all $n < (k-2)q\sqrt{q}$,

$$\binom{n_1}{k-1}\sigma_n = 0 \quad \text{and} \quad \binom{n_1-1}{k-2}\varepsilon_{\sqrt{q},n} = 0$$

and since $k < p$ it follows that

$$\binom{n_1}{k}\sigma_n = 0 \quad \text{and} \quad \binom{n_1-1}{k-1}\varepsilon_{\sqrt{q},n} = 0.$$

Now we examine the remaining cases $(k-2)q\sqrt{q} \leq n < (k-1)q\sqrt{q}$. For $(k-2)q\sqrt{q} \leq n < (k-2)\sqrt{q}(q+1)$ we have

$$\binom{n_1}{k-1} = \binom{n_1-1}{k-2} = 0;$$

and using Lemma 9(2) we have:

$$\binom{n_1-1}{k-2}\varepsilon_{\sqrt{q},n} + (k-2)\binom{n_1}{k-1}\sigma_n = 0.$$

By Lemma 8,

$$\begin{aligned} Q_k(x) &= \sum_{d=1}^{k-2}\left(\sum_{n=d\sqrt{q}(q+1)}^{(k-1)q\sqrt{q}-1} (-1)^{n+k+d+1}\binom{n_1-1}{k-1}\binom{k-1}{d-1}\varepsilon_{\sqrt{q},n}x^n\right) \\ &+ \sum_{d=0}^{k-2}\left(\sum_{n=d\sqrt{q}(q+1)}^{(k-1)q\sqrt{q}-1} (-1)^{n+k+d+1}(d-1)\binom{n_1}{k}\binom{k}{d}\sigma_n x^n\right). \end{aligned}$$

Since $n \geq (k-2)q\sqrt{q}$ and the coefficient of x^n in $Q_k(x)$is zero unless $n_1 \geq k$, we see that $x^{(k-2)q\sqrt{q}+k\sqrt{q}}|Q_k$. Further, S divides Q_k, hence $x^{(k-2)q\sqrt{q}+k\sqrt{q}}S(x)$ divides $Q_k(x)$. But $x^{(k-2)q\sqrt{q}+k\sqrt{q}}S(x)$ has degree at least $(k-2)q\sqrt{q}+k\sqrt{q}+(q-2)\sqrt{q}=(k-1)q\sqrt{q}+(k-2)\sqrt{q}$ which is greater than the degree of $Q_k(x)$, and therefore $Q_k\equiv 0$.

Looking at the coefficient of x^n for $(k-2)q\sqrt{q}\le n<(k-1)q\sqrt{q}$ gives

$$\begin{aligned} 0 &= \binom{n_1-1}{k-1}\varepsilon_{\sqrt{q},n}+\sum_{d=2}^{k-2}\binom{n_1-d}{k-d}(-1)^{d+1}\binom{n_1-1}{d-1}\varepsilon_{\sqrt{q},n} \\ &+ \binom{n_1}{k}\sigma_n+\sum_{d=2}^{k-2}\binom{n_1-d}{k-d}(-1)^{d+1}(d-1)\binom{n_1}{d}\sigma_n. \end{aligned}$$

Now

$$\begin{aligned} &\sum_{d=2}^{k-2}\binom{n_1-d}{k-d}(-1)^{d+1}\binom{n_1-1}{d-1} = \sum_{d=2}^{k-2}\binom{-n_1+k-1}{k-d}\binom{n_1-1}{d-1}(-1)^{k+1} \\ =\ & (-1)^{k+1}\binom{k-2}{k-1}-\binom{n_1-1}{k-1}-(-1)^k\binom{n_1-k+1}{1}\binom{n_1-1}{k-2}-(-1)^{k+1}\binom{n_1-1}{k-1} \\ =\ & (-1-(-1)^k(k-2))\binom{n_1-1}{k-1}. \end{aligned}$$

Similarly,

$$\begin{aligned} &\sum_{d=2}^{k-2}\binom{n_1-d}{k-d}(-1)^{d+1}(d-1)\binom{n_1}{d} = -\binom{n_1}{k}\sum_{d=2}^{k-2}\binom{-2}{d-2}\binom{k}{k-d} \\ =\ & -\binom{n_1}{k}\left[\binom{k-2}{k-2}-k\binom{-2}{k-3}-\binom{-2}{k-2}\right]=(-1+(-1)^k(-k^2+3k-1))\binom{n_1}{k}. \end{aligned}$$

Substituting back now shows that

$$(k-2)\binom{n_1-1}{k-1}\varepsilon_{\sqrt{q},n}+(k^2-3k+1)\binom{n_1}{k}\sigma_n=0.$$

Recall that also

$$\binom{n_1-1}{k-2}\varepsilon_{\sqrt{q},n}+(k-2)\binom{n_1}{k-1}\sigma_n=0,$$

and solving for $k>2$ implies

$$\binom{n_1}{k}\sigma_n=0 \quad\text{and}\quad \binom{n_1-1}{k-1}\varepsilon_{\sqrt{q},n}=0.$$

□

4.2 The case $q=p^2$ where p is a prime

Theorem 4 Let $\mathcal{U}$ be a unital in $\mathrm{PG}(2,q)$ where $q=p^2$ for some prime p. Then $\mathcal{U}$ is classical if and only if there exist at least $(q-2)\sqrt{q}$ secants that meet $\mathcal{U}$ in a Baer subline.

Proof: If $\mathcal{U}$ is classical then every secant meets it in a Baer subline. For the converse, we suppose that p is odd for every unital in $\mathrm{PG}(2,4)$ is classical. Let $\mathcal{U}^*$ be a unital in $\mathrm{PG}(2,q)$ such that at least $(q-2)\sqrt{q}$ secants meet it in a Baer subline. The dual unital $\mathcal{U}$ is such that there are at least $(q-2)\sqrt{q}$ points $s \in \mathrm{PG}(2,q) \setminus \mathcal{U}$ such that the tangents to $\mathcal{U}$ on s form a dual Baer subline. By Lemmas 8, 9 and 11 applied to the polynomials associated with $\mathcal{U}$, we see that for $r = 2, \ldots, p-1$ Q_r is identically zero and hence also $\alpha_{r\sqrt{q}}$ is identically zero. Thus

$$L(t, x_0) = 1 + \alpha_{\sqrt{q}} t^{\sqrt{q}} + (\alpha_q - 1)t^q + (\alpha_{q+\sqrt{q}} - \alpha_{\sqrt{q}})t^{q+\sqrt{q}}$$

for all $1/x_0 \in \mathcal{R} \setminus \mathcal{U}$. By definition L divides $1 - t^q + t^{q+1}$, hence by Lemma 10 the tangents to $\mathcal{U}$ on $1/x_0$ form a dual Baer subline (recalling that L is a $\sqrt{q}$-th power of a polynomial in t, and for $1/x_0 \in \mathcal{R} \setminus \mathcal{U}$ the $\sqrt{q}+1$ roots of $L(t,x_0) = 0$ correspond to the directions of the tangents on $1/x_0$). It is now immediate that every secant meets $\mathcal{U}^*$ in a Baer subline, so by Theorem 1, the unital $\mathcal{U}^*$ is classical. $\square$

Acknowledgements: This work was supported by the Australian Research Council and was carried out at the Vrije Universiteit Amsterdam, The University of Adelaide and The University of Western Australia.

References

[1] F. Buekenhout, Existence of unitals in finite translation planes of order q^2 with a kernel of order q, *Geom. Dedicata* **5** (1976), 189–194.

[2] L.R.A. Casse, C.M. O'Keefe and T. Penttila, Characterizations of Buekenhout-Metz Unitals, *Geom. Dedicata* **59** (1996), 29–42.

[3] G. Faina and G. Korchmáros, A graphic characterization of Hermitian curves, *Ann. Discrete Math.* **18** (1983), 335–342.

[4] J.W.P. Hirschfeld *Projective Geometries over Finite Fields,* Second Edition, Oxford University Press, New York, 1998.

[5] C. Lefèvre-Percsy, Characterization of Buekenhout-Metz unitals, *Arch. Math.* **36** (1981), 565–568.

[6] C. Lefèvre-Percsy, Characterization of Hermitian curves, *Arch. Math.* **39** (1982), 476–480.

[7] R. Metz, On a class of unitals, *Geom. Dedicata* **8** (1979), 125–126.

[8] T. Penttila and G.F. Royle, Sets of type (m,n) in projective and affine planes of order 9, *Des., Codes, Cryptogr.* **6** (1995), 229–245.

[9] C.T. Quinn and L.R.A. Casse, Concerning a characterisation of Buekenhout-Metz unitals, *J. Geom.* **52** (1995), 159–167.

Addresses of the authors:

Simeon Ball
Technische Universiteit Eindhoven, PO Box 513, 5600 MB Eindhoven, The Netherlands
`simeon@win.tue.nl`

Aart Blokhuis
Technische Universiteit Eindhoven, PO Box 513, 5600 MB Eindhoven, The Netherlands
Vrije Universiteit Amsterdam, De Boelelaan 1081, Amsterdam, The Netherlands
`aartb@win.tue.nl`

Christine M. O'Keefe
Department of Pure Mathematics, The University of Adelaide, Adelaide, SA 5005, Australia
`cokeefe@maths.adelaide.edu.au`