On embedding partial unitals and large (k,n)-arcs

Éva Hadnagy* and Tamás Szőnyi**

June 11, 2001

Abstract

Using algebraic curves it will be proven that large partial unitals can be embedded into unitals and large (k,n)-arcs into maximal arcs.

1 Introduction

A (k,n)-*arc* in a projective plane of order q is a set of k points no $n+1$ on a line. $(k,2)$-arcs are simply called k-*arcs*. If the order of the plane is q, where q is a square, a *unital* $\mathcal{U}$ is defined to be a $(q\sqrt{q}+1, \sqrt{q}+1)$-arc meeting all lines in 1 or $\sqrt{q}+1$ points. A *partial unital* is a $(k, \sqrt{q}+1)$-arc $\mathcal{X}$ such that each point of $\mathcal{X}$ lies on a 1-secant. With respect to a set $\mathcal{A}$ in a projective plane a line is called an *i-secant*, if it meets $\mathcal{A}$ in exactly i points. Here we only present a very brief introduction, for more details, see [1], [2], [8].

Barlotti [4] proved that for a (k,n)-arc $k \leq qn-q+n$, if $1 < n < q+1$, and equality can only occur when n divides q. For q even, Denniston [6] constructed (k,n)-arcs with $k = nq-q+n$ in PG$(2,q)$ for every divisor of q. Sometimes these arcs are called *maximal arcs*. Recently Ball, Blokhuis and Mazzocca [3] proved the long-standing conjecture that in PG$(2,q)$, q odd, there are no maximal arcs. It is then natural to ask whether a (k,n)-arc with $k \geq qn-q+n-\epsilon$ points can be embedded in a maximal arc or not. The first result in this direction is due to Thas [9] for $\epsilon = 1$. Using purely combinatorial arguments he showed that a $(qn-q+n-1, n)$-arc can always be embedded in a maximal arc. For $\epsilon = 2$ Wilson [10] obtained

*Research of this author was supported by OTKA Grant F-030737

**Research of this author was supported by OTKA Grants N 26673, T 032455 and FKFP Grant B-07/97

some nice results, but the complete solution was not known. Using algebraic techniques Ball and Blokhuis [2] proved the following:

Let K be a (k,n)-arc in $PG(2,q)$, $n|q$ with $k \geq qn-q+n-\varepsilon$. If $\varepsilon < n/2$ for $q/n > 3$ or $\varepsilon < 0.476n$ if $n = q/3$, or $\varepsilon < 0.381n$ for $n = q/2$, then there is a maximal arc containing K.

There is a similar result in [8], where the same conclusion was obtained for $q = p^h$, $n = p$, and $\varepsilon = [\sqrt[4]{q}/2]$.

The situation is analogous for partial unitals; an easy counting argument gives that $k \leq q\sqrt{q}+1$, and Ball [1] proved that a partial unital $\mathcal{X}$ in $PG(2,q)$ with $q\sqrt{q}+1-\sqrt{q} < |\mathcal{X}| < q\sqrt{q}+1$ can be extended to a unital.

The aim of this paper is to give a proof of Ball's theorem for the embedding of partial unitals (Theorem 4.1), and to prove a slight improvement of the Ball–Blokhuis theorem for embedding large (k,n)-arcs (Theorem 3.1). Our proof uses the Rédei polynomial of a set and is motivated by algebraic curves, although curves are explicitly used in only one step of the proof. We believe that the use of the Rédei polynomial makes the proof more transparent. Besides this, the counting argument of Ball and Blokhuis is improved.

2 Preliminaries

Throughout this paper $q = p^h$, p prime, and n is a divisor of q. We shall work on the plane $\mathrm{PG}(2,q)$ coordinatized by the finite field $\mathrm{GF}(q)$. The line at infinity will be denoted by ℓ_∞, and $\mathrm{AG}(2,q)$ will denote the affine plane $\mathrm{PG}(2,q) \setminus \ell_\infty$.

To recall the definition of the Rédei polynomial let $\mathcal{S}$ be our set, S its affine part, that is $\mathcal{S} \setminus \ell_\infty$. Let $S := \{(a_i, b_i) : i = 1, \ldots, N\}$. The line at infinity will be denoted by ℓ_∞. The Rédei polynomial of S is defined as follows:

$$H(X,Y) := \prod_i^N (X + a_i Y - b_i) = X^N + h_1(Y) X^{N-1} + \ldots + h_N(Y). \quad (1)$$

Note that for all $j = 1, \ldots, N$: $deg(h_j) \leq j$. $H(X,Y)$ is often considered for a fixed $Y = y$ as a polynomial of X; then we write $H(X,y)$. For properties of the Rédei polynomial, see [7].

From the combinatorial properties of unitals and maximal arcs we know what their Rédei polynomials, $H^*(X,Y)$ look like.

Remark 2.1 *1) Let $H^*(X,Y)$ be the Rédei polynomial of a maximal arc $\mathcal{A}$. Then for any infinite point $(y) \notin \mathcal{A}$, $H^*(X,y)$ is an n-th power, and since n divides q, it only contains exponents of X that are divisible by n.*

2) Let $H^*(X,Y)$ be the Rédei polynomial of a unital $\mathcal{U}$ Then for any infinite point $(y) \notin \mathcal{U}$, $H^*(X,y) = (X^q - X)\overline{H}(X,y)$, where $\overline{H}$ is a $\sqrt{q}$-th power. Again the exponents of X that are larger than $|\mathcal{U}| - |\mathcal{U} \cap \ell_\infty| - q + 1$ are divisible by n.

If some points are deleted from a maximal arc or a unital, then the deleted linear factors in the Rédei polynomial give a polynomial $a(X,Y)$ of degree ϵ with the property that $H(X,Y)a(X,Y) = H^*(X,Y)$. We wish to find such an $a(X,Y)$ without knowing that the set is a maximal arc or a unital, minus ϵ points. The consequence is that the above equality for the Rédei polynomials will not hold automatically for every (y).

Definition 2.2 *1) Let $\mathcal{A}$ be a (k,n)-arc. If there are $t_i(P)$ $(n-i)$-secants through P, then the* index of P *is defined by $i(P) = \sum_{i=1}^{n-1} i \cdot t_i(P)$.*

2) Let $\mathcal{X}$ be a partial unital. If there are $t_i(P)$ $(\sqrt{q}+1-i)$-secants through P, then the index of P *is defined by $i(P) = t_{\sqrt{q}+1}(P) + \sum_{i=1}^{\sqrt{q}-1} i \cdot t_i(P)$.*

Note that for a point $P \in \mathcal{A}$ or $\mathcal{X}$, $i(P) = \epsilon$. The following lemma is immediate.

Lemma 2.3 *1) Let $\mathcal{A}$ be a (k,n)-arc. If there are $q/n - \ell$ 0-secants through a point $P \notin \mathcal{A}$ with $\ell \geq 0$, then the index of P is $\ell n + \epsilon$.* ∎

2) Let $\mathcal{X}$ be a partial unital. If there are $\sqrt{q} - \ell$ 0- or 1-secants through a point $P \notin \mathcal{X}$ with $\ell \geq 0$, then the index of P is $\ell\sqrt{q} + \epsilon$. ∎

Proposition 2.4 *Let S be a (k,n)-arc or a partial unital, and $H(X,Y)$ be its Rédei polynomial. Let (y) be any infinite point of index $i((y)) = \epsilon$. Suppose that ℓ_∞ is an $(n-j)$-secant or a $(\sqrt{q}+1-j)$-secant. Let $j' \equiv j \pmod{n}$ (or $\sqrt{q}$), with $0 \leq j' < n$ (or $< \sqrt{q}$). Then:*
(1) There is a unique polynomial $a(X,y)$, such that $H(X,y)a(X,y) = H^*(X,y)$, where $H^*(X,y)$ is of the form described in Remark 2.1,
(2) The degree of $a(X,Y)$ as a polynomial in two variables is l to $\epsilon - j'$,
(3) $a(X,y)$ has only linear factors, if (y) has index ϵ.

Proof: Suppose that (y) has index ϵ, and consider $H(X,Y)$. If $(X-a)$ is a factor corresponding to an $(n-i)$-secant or a $(\sqrt{q}+1-i)$-secant, and we multiply $H(X,Y)$ by $(X-a)^i$ [or $(X-a)$ if $i = \sqrt{q}+1$ in case of partial unitals], then we obtain a polynomial H^*, which is an n-th power or $(X^q - X)$ times a $\sqrt{q}$-th power. So $\prod(X-a)^i = a(X,y)$ satisfies $H(X,y) \cdot a(X,y) = H^*(X,y)$ and the degree of $a(X,Y)$ in X is $\epsilon - j'$, since the contribution of ℓ_∞ to $i(y)$ is j'. If $a(X,y) = \sum_{i=0} a_i(y) X^{A-i}$,

then the coefficients of a can be found uniquely, since $H^*(X,Y)$ contains a lot of 0 coefficients on the top. A comparison of the coefficients gives $a_1(y) = -h_1(y)$, $a_2(y) = -h_2(y) - a_1(y)h_1(y)$, and in general $a_i(y) = -h_i(y) - \sum_{k=1}^{i-1} a_k(y)h_k(y)$. This system of linear equations can be solved uniquely, and the degree of $a_i(y)$ is at most i. ∎

3 Embedding (k,n)−arcs

In this section our main result for embedding large (k,n)-arcs in maximal arcs will be proven.

Theorem 3.1 *An $(qn-q+n-\varepsilon,n)$−arc can be embedded into a maximal arc, provided that $\varepsilon \le c\cdot n$, c is a constant satisfying $0 < c < 2/3$, n divides q, and $K = q/n$ is large enough. More precisely, $K \ge 2$, when $0 \le c \le 1/3$, $K \ge 3$, when $0 < c \le 0.449$, $K \ge 4$, when $0.449 < c \le 1/2$, $K \ge (1+2c)(1-c)/(1-c-c^2)$, when $1/2 < c \le 3/5$ and $K \ge (1+2c)(4-5c)/(4-6c)$, when $3/5 < c < 2/3$.*

Lemma 3.2 *Let T_i denote the total number of $(n-i)$-secants of a (k,n)-arc $\mathcal{A}$, satisfying the conditions in Theorem 3.1. Then*

(1) $\sum_{i=1}^{n-1} iT_i = \sum_{P\in\ell_\infty} i(P)$, if ℓ_∞ is a 0- or n-secant, $\sum_{i=1}^{n-1} iT_i = \sum_{P\in\ell_\infty} i(P) - jq$, if ℓ_∞ is an $(n-j)$-secant for $0 < j < n$.

(2) There are 0-secants.

Proof: (1) is immediate. If there were no 0-secants, then points would have index ε or $q+\varepsilon$. Since $|\mathcal{A}|\varepsilon = \sum_{j=1}^{n-1}(n-j)jT_j \ge (n-\varepsilon)\sum jT_j = (n-\varepsilon)\sum_{P\in\ell_\infty} i(P) = n\varepsilon + (q+1-n)(q+\varepsilon)$, this gives a contradiction. ∎

Remark. With the parameter j' introduced in Proposition 2.4, (1) of 3.2 means that $\sum_{i=1}^{n-1} iT_i = \sum_P i(P) - j'q$.

Lemma 3.3 *Let ℓ_∞ be a 0-secant. If there are s points with index more than ε on l_∞, then for their index $i(y) > q+1-s-\varepsilon$ holds true.*

Proof: For points (y) of index ε, $H(X,y)a(X,y)$ is an n-th power. For other points, there is a maximal $e \ge 0$, such that $(Ha)(X,y)$ is a polynomial in X^{p^e}. If $p^e \ge n$ for a (y), then the index of (y) would be ε; whence $p^e < n$. Define $W(U,y)$ by replacing X^{p^e} in $(Ha)(X,y)$ by U. If $e = 0$, then W is just (Ha). If $(U-c)$ is a factor of W, such that $U - c = (X-\overline{c})^{p^e}$), and $X-\overline{c}$ is a root of $(Ha)(X,y)$ with multiplicity n, then $U-c$ has multiplicity n/p^e as a root of $X(U,y)$, hence $U-c$ will have the same multiplicity in W'_U. Thus the degree of W'_U will differ from the degree of W, if there is a factor $U-b$ of W with multiplicity not divisible by p. For such a factor put $U - b = (X-\overline{b})^{p^e}$. Then $X-\overline{b}$ will have multiplicity

at most $n-p^e$, or at least $n+p^e$ as a root of $(Ha)(X,y)$. If $X-\bar{b}$ is a factor of $H(X,y)$, and we are in the first case, then there could be at most $i((y))/p^e$ such points, since $i((y)) \geq p^e \sum_{i=p^e} t_i$. If $X-\bar{b}$ is not a factor of $H(X,y)$ or its multiplicity in $(Ha)(X,y)$ is at least $n+p^e$, then $X-\bar{b}$ has a multiplicity at least p^e in $a(X,y)$, hence there are at most ε/p^e such points (y). Thus $\deg_U(W'_U) \geq (qn-q+n-i(y)-\varepsilon)/p^e$. On the other hand, for points of index ε, $(Ha)(X,y)$ contains only terms whose exponent is divisible by n. Thus $h_i(y)=0$, for points of index ε if n does not divide i. Since there are $q+1-s$ points of index ε, $h_i(y)$ is identically zero, if i is not divisible by n and $i < q+1-s$. Using $p^e < n$ we get $\deg_U(W'_U) < (qn-q+n-(q+1-s))/p^e$, from which the Lemma follows. ∎

The next lemma is the cornerstone of our proof. The cases $c \leq 3/5$ and $3/5 < c < 2/3$ will be distinguished. In both cases first we show, using purely combinatorial methods, that a positive percentage of the points have index ε. Then, using Lemma 3.3, we show that there are only three possible indices that are larger than ε.

Lemma 3.4 *For $q/n \geq 5$ the only possible indices are ε, $q-2n+\varepsilon$, $q-n+\varepsilon$ and $q+\varepsilon$, for $q/n=4$ or 3, only ε, $q-n+\varepsilon$ and $q+\varepsilon$ are possible.*

Proof: Case 1: $0 < c \leq 3/5$.

Let ℓ_∞ be a 0-secant. Count the incident (point, short line) pairs. On one hand, we get $|\mathcal{A}|\varepsilon$, on the other hand $\sum_{j=1}^{n-1}(n-j)jT_j$, which is at least $(n-\varepsilon)\sum_{j=1}^{n-1} jT_j$, hence

$$\sum_{P \in \ell_\infty} i(P) \leq \frac{(qn-q+n-\varepsilon)\varepsilon}{n-\varepsilon}. \tag{2}$$

If there are s points of index at least $n+\varepsilon$, then, by (2), $s < qc^2/(1-c)$. By Lemma 3.3 these indices are larger than $q+1-qc^2/(1-c)-\varepsilon$, which is larger than $n+\varepsilon$, because $K \geq (1+2c)(1-c)/(1-c-c^2)$. With this newly obtained bound for the indices we can proceed and use (2) and Lemma 3.3 repeatedly to prove the Lemma.

For $K=3$, $n+\varepsilon$ is the only index to eliminate, for that c has to be less than 0.449. Provided that $K=4$ and $c \leq 0.5$, $n+\varepsilon$ and $2n+\varepsilon$ can eliminated.

In general it is enough to prove, that if the "high" indices are at least $mn+\varepsilon$ and $m < q/n-2$, then by applying (2) and Lemma 3.3, the newly obtained bound for the indices has to be more than $mn+\varepsilon$, showing that this situation is impossible. Consequently, it is enough to show, that for

$q/n \geq 5$

$$q - \frac{q}{m}\frac{c^2}{1-c} - \epsilon \geq mn + \epsilon, \quad for \quad m = 1 \ldots K-3. \tag{3}$$

$$0 \geq m^2 - m(K-2c) + \frac{Kc^2}{1-c}, \quad for \quad m = 1 \ldots K-3. \tag{4}$$

Since this is a quadratic expression in m, it is satisfied for any m, if it is true for $m = 1$ and for $m = K-3$. $m = 1$ is already dealt with. Now, for $m = K-3$, K has to be larger than $(9-6c)(1-c)/(3-5c+c^2)$, which is precisely the constant appearing in the Theorem.

Case 2: $3/5 < c < 2/3$.
In this case we need a simple Lemma.

Lemma 3.5 *If* $3/5 \leq c < 2/3$, *for a point* P *of index* $nl + \epsilon$,

$$\sum_{j=\epsilon/2}^{\epsilon} (j - \epsilon/2) j \cdot t_j(P) \leq \frac{5c^2 - 5c + 2}{2c^2} l\epsilon^2. \tag{5}$$

Proof: The goal is to find the maximum of the sum $\sum_i (x_i - 1/2)\, x_i$, if $\sum_i x_i \leq (nl+\epsilon)/\epsilon$ and for all i, $1/2 < x_i \leq 1$. It is easy to see that the maximum is achieved when as many x_i's are 1 as possible, and there might be one more term if $\{l/c + 1\} \geq 1/2$.

Actually, the fraction $(5c^2 - 5c + 2)/2c^2$ only appears for $l = 1$. For $l > 1$ it can be omitted. (Note that this fraction is at least 1, if $c < 2/3$.) ∎

Now for $3/5 \leq c < 2/3$ (2) is slightly modified. Let ℓ_∞ be a 0-secant again. Those secants, that intersect $\mathcal{A}$ in less than $n - \epsilon/2$ points are separated, because at most one secant like that can go through a point of $\mathcal{A}$.

$$\sum_{j=1}^{n-1} (n-j) j T_j \geq (n - \epsilon/2) \sum_{j=1}^{n-1} j T_j - \sum_{j=\epsilon/2}^{\epsilon} (j - \epsilon/2) j T_j. \tag{6}$$

Suppose that the number of points of index $ni + \epsilon$ is s_i on ℓ_∞, and that the smallest index bigger than ϵ is $nl + \epsilon$. Note that $\sum_{i=0}^{q/n-1} s_i = q + 1$.

$$|\mathcal{A}|\epsilon \;>\; (n - \epsilon/2)(s_0\epsilon + \sum_{i=1}^{q/n-1} s_i(ni + \epsilon)) - \frac{5c^2 - 5c + 2}{2c^2} \sum_{i=1}^{q/n-1} s_i i \epsilon^2$$

$$(q+1)n\epsilon \;>\; (n - \epsilon/2)((q+1)\epsilon + n \sum_{i=1}^{q/n-1} i s_i) - \frac{5c^2 - 5c + 2}{2c^2} \sum_{i=1}^{q/n-1} s_i i \epsilon^2$$

$$(q+1)\frac{\epsilon^2}{2} > (n^2 - \epsilon n/2 - \frac{5c^2-5c+2}{2c^2}\epsilon^2)\sum_{i=1}^{q/n-1} is_i$$

$$\frac{(q+1)c}{4-5c} > \sum_{i=1}^{q/n-1} is_i$$

Since $c/(4-5c) < 1$, a positive percentage of points has index ϵ.

If the smallest index that is higher than ϵ is $mn+\epsilon$, then from the estimate for $\sum is_i$, we get that $s < \frac{q+1}{m}\frac{c}{4-5c}$. Repeating the same arguments as before, all that remained to show, is that

$$q - \frac{q}{m}\frac{c}{4-5c} - \epsilon \geq mn + \epsilon, \quad for \quad m = 1 \ldots K-3. \tag{7}$$

$$0 \geq m^2 - m(K-2c) + \frac{Kc}{4-5c}, \quad for \quad m = 1 \ldots K-3. \tag{8}$$

(Here $q+1$ was replaced by q, which can be done, since $1 - \frac{1}{m}\frac{c}{4-5c} \geq 0$.) For $m = 1$, K has to be larger than $(1+2c)(4-5c)/(4-6c)$, for $m = K-3$, K has to be larger than $(9-6c)(4-5c)/(12-24c+10c^2)$, which is less than $(1+2c)(4-5c)/(4-6c)$ for all values of c, $3/5 < c < 2/3$. ∎

Proof of Theorem 3.1: On a 0-secant there are only points of index ϵ, $q-2n+\epsilon$ and index $q-n+\epsilon$. If there are only points of index ϵ, then the 0-secants to $\mathcal{A}$ form a maximal $(k, q/n)$-arc. Its dual will be a maximal arc containing $\mathcal{A}$, so we are done in this case.

Suppose that there are $s \geq 1$ points of index $q-2n+\epsilon$ or $q-n+\epsilon$ on ℓ_∞. Then the total number of 0-secants is between $1+(q+1-s)(q/n-1)$ and $1+(q+1-s)(q/n-1)+s$. The total number of points of index $q-2n+\epsilon$ or $q-n+\epsilon$ is then at least $(1+(q+1-s)(q/n-1))s/2$. Points lying on no 0-secants have index $q+\epsilon$, by Lemma 2.3 (1). Let us try to estimate how many points of index different from ϵ there can be on an $(n-i)$-secant ℓ. Counting the 0-secants intersecting ℓ we see $(n-i)$ points of $\mathcal{A}$, and x further points with at most two 0-secant through them, and finally $q+1-n+i-x$ points with q/n 0-secants. Counting the total number of 0-secants gives $x \leq (s(q/n-1)+iq/n)/(q/n-2)$. Now look at the lines through a point. Counting the points of indices different from ϵ along the lines through a point of index ϵ we get $(s(q/n-1)(q+1)+\epsilon q/n)/(q/n-2)$, which is much smaller than $(1+(q+1-s)(q/n-1))s/2$, if $q/n > 4$. This contradiction shows that $s \geq 1$ is not possible.

Since for $q/n = 3$ or 4 the only possible indices are ϵ, $q-n+\epsilon$, and $q+\epsilon$, in these cases the above estimate reduces to $s(q+1)+\epsilon\frac{q/n}{q/n-1} \geq s+(q+1-s)(q/n-1)s$, from which $s = 0$ follows. For $q/n = 2$, the theorem follows immediately from (2) and Lemma 3.3. ∎

Remarks. 1) $c = 2/3$ is a natural boundary of our method. If we consider just one line, then it may happen that through almost all points of this line there are two lines of index ϵ and one line of index $\epsilon/2$.

2) For $q/n = 2$, we obtain $\epsilon \leq n/3$, for $q/n = 3$, $\epsilon \leq 0.449n$, and for $n = q/4$, $\epsilon = n/2$. For $q/n = 2, 3$ our constants are worse than the ones of Ball, Blokhuis, for $q/n = 4$ we get exactly the same constant. The method of this paper (slightly) improves Ball and Blokhuis's results, when q/n is at least 5. Already for $q/n \geq 7$ we get $c = 0.556$. For example, for $c = 3/5$ K has to be larger than 22, for $c = 0.66$ $K \geq 41$ is enough.

4 Embedding partial unitals

In this section we will prove Ball's theorem on embedding partial unitals into unitals.

Theorem 4.1 (Ball [1]) *If a partial unital contains at least* $q\sqrt{q}+1-(\sqrt{q}-1)$ *points, then it is embeddable into a unital.*

Let us denote our partial unital by $\mathcal{X}$, and put $|\mathcal{X}| = q\sqrt{q} + 1 - \epsilon$.

Lemma 4.2 *If* ℓ_∞ *is a* j*-secant with* $j = 0, 1$*, then there are at least* $q - \epsilon + (j-1)(\sqrt{q}-2)$ *infinite points having index* ϵ*.*

Proof: The total number of 1-secants is at least $q\sqrt{q}+1-\epsilon$, and through each point there are at most $\sqrt{q}+1$ 0- or 1-secants. ∎

First of all define $a(X, Y)$ according to Proposition 2.4. In order to repeat the argument of the previous section, we need that $X^q - X$ divides $H(X, y)a(X, y)$ for any point that has index ϵ. We shall consider $a(X, Y)$ as a curve and use different lines at infinity.

Proposition 4.3 *Let* ℓ *be a* 0*-secant of* $\mathcal{X}$*. Then there is a point* $P(a, b) \in \ell$ *such that* $(X + aY - b)$ *divides* $a(X, Y)$*.*

Lemma 4.4 *Let* ℓ_∞ *be a* 0- *or* 1*-secant and let* $h(X, Y)$ *be an irreducible component of* $a(X, Y)$*, with* $h'_X \neq 0$ *Then* $\deg(h) = 1$*, and the multiplicity of* h *is* 1*.*

Proof: By Lemma 4.2 there are at least $q - \epsilon + (j-1)(\sqrt{q}-2)$ points (y) of index $\epsilon - j$ on ℓ_∞. For these y-s, $a(X, y)$, and hence $h(X, y)$ have only linear factors over GF(q). So the number of GF(q)-rational points on h, counted with multiplicity, is at least $(q - \epsilon + (j-1)(\sqrt{q}-2))\deg(h)$. To get the number, say N, of points without multiplicity, we have to subtract

the number of affine intersections of h and h'_X, see [5]. Bézout's theorem gives $(q-\epsilon+(j-1)(\sqrt{q}-2))\deg(h)-\deg(h)(\deg(h)-1)\leq N$. From above, Weil's estimate gives $N\leq q+1+(\deg(h)-1)(\deg(h)-2)\sqrt{q}$. Using $\deg(h)\leq\deg(a)=\epsilon-j\leq\sqrt{q}-1-j$, we indeed get $\deg(h)=1$. If $h=X+aY-b$, then through $P(a,b)$ there are at least $q-\epsilon+(j-1)(\sqrt{q}-2)$ short lines, namely the lines joining P to a point of ℓ_∞ having index $\epsilon-j$; hence h has to be simple, otherwise the index of P would be at least $2(q-\epsilon+(j-1)(\sqrt{q}-2))$. ∎

Proof of Proposition 4.3: Take our 0-secant ℓ as the line at infinity and write the curve a^ℓ corresponding to it. By Lemma 4.4 it will have s linear components for some $s\equiv\epsilon-1 \pmod p$, since the partial derivative of the non-linear components with respect to X is zero, and hence their degree is divisible by p. These components correspond to s points P_i that have at least $q-\epsilon+(j-1)(\sqrt{q}-2)$ short lines passing though them. Choose the line at infinity ℓ^*, as a 1-secant not containing any P_i. By Bézout's theorem the linear components corresponding to P_i are all components of a^{ℓ^*}. The curve a^{ℓ^*} must have $t\equiv\epsilon \pmod p$ linear components, so the number of components is at least one more. It cannot contain linear components corresponding to a point $P^*\notin\ell$, since through P^* there were at least $q-\epsilon$ short lines, and by Bézout's theorem, P^* would correspond to a linear component of a^ℓ. Hence P^* must be a point of ℓ. ∎

Proof of Theorem 4.1: Since there is a point on each 0-secant such that the linear factor corresponding to it divides $a(X,Y)$, we have that X^q-X divides $(Ha)(X,y)$ for every point (y) that has index ϵ.

Lemma 4.5 *If there are s points with index more than ϵ on ℓ_∞, then for their index $i(y)>q+1-s-\epsilon$ holds.*

Proof of Lemma 4.5 After dividing $(Ha)(X,Y)$ by X^q-X, the proof of Lemma 3.3 can be copied. ∎

Let us fix ℓ_∞ to be a 1-secant. Then by Lemma 4.2 there are at most ϵ points of ℓ_∞ having index larger than ϵ, and their index is at least $q-2\sqrt{q}+\epsilon$, by Lemma 4.5. This means that through these points there are at most two 0- or 1-secants. If there are s of these points, then counting the 1-secants implies that

$$2s+(q-s)\sqrt{q}\geq q\sqrt{q}+1-\epsilon.$$

¿From this, s is either 0, or $s=1$ and $\epsilon=\sqrt{q}-1$. If there is one point of high index, then this index has to be at least $q-\sqrt{q}+\epsilon$ by Lemmas 4.5 and 2.2. In the latter case the proof of Theorem 3.1 can be copied to show, that $s=1$ provides a contradiction, if $q>4$.