Interpolation in affine and projective space over a finite field

M. Hellus and R. Waldi

Preprint Nr. 18/2013
Interpolation in affine and projective space over a finite field

M. Hellus and R. Waldi

September 18, 2013

Abstract

Let \( s(n, q) \) be the smallest number \( s \) such that any \( n \)-fold \( \mathbb{F}_q \)-valued interpolation problem in \( \mathbb{P}^k_{\mathbb{F}_q} \) has a solution of degree \( s \), that is: For any pairwise different \( \mathbb{F}_q \)-rational points \( P_1, \ldots, P_n \) there exists a hypersurface \( H \) of degree \( s \) defined over \( \mathbb{F}_q \) such that \( P_1, \ldots, P_{n-1} \in H \) and \( P_n \notin H \). This function \( s(n, q) \) was studied by Ernst Kunz and the second author in [KuW] and completely determined for \( q = 2 \) and \( q = 3 \). For \( q \geq 4 \), we improve the results from [KuW]. The affine analogue to \( s(n, q) \) is the smallest number \( s = s_a(n, q) \) such that any \( n \)-fold \( \mathbb{F}_q \)-valued interpolation problem in \( \mathbb{A}^k(\mathbb{F}_q) \), \( k \in \mathbb{N}_{>0} \) has a polynomial solution of degree \( \leq s \). We exactly determine this number.

1 Introduction

Let \( R = K[X_0, \ldots, X_k] \) denote the standard graded polynomial ring in \( k+1 \geq 1 \) variables over an arbitrary field \( K \) and \( \mathbb{P}^k(K) \subseteq \mathbb{P}^k_K = \text{Proj} R \) the set of all \( K \)-rational points.

We start with an arbitrary finite subset \( X \subseteq \mathbb{P}^k(K) \) consisting of \( n =: \deg X \geq 1 \) pairwise different \( K \)-rational points. By

\[
I_X := (\{ F \in R \text{ homogenous} \mid F(P) = 0 \text{ for all } P \in X \})
\]

we denote its homogenous vanishing ideal. Let \( S := \bigoplus_{d \geq 0} S_d := R/I_X \) and

\[
H_X(d) := \dim_K(S_d)
\]

(for \( d \in \mathbb{N} \)) the Hilbert function of \( X \). The Castelnuovo-Mumford regularity of \( X \) is the uniquely determined number \( r_X \) such that

\[
H_X(d) = n \text{ for } d \geq r_X \text{ and } H_X(r_X - 1) \leq n - 1.
\]

It is well known that \( H_X \) is strictly increasing for \( 0 \leq d \leq r_X \); in particular, \( r_X \leq n - 1 \).

From now on we assume that \( K = \mathbb{F}_q \) is the finite field with \( q \) elements, where \( q \) is an arbitrary prime power. One would like to know which Hilbert
functions $H_X$ resp. which regularities $r_X$ are possible. For infinite fields $K$, the answer to the first (and hence also to the second) question was given by Geramita, Maroscia and Roberts ([GMR, sections 1 and 3]).

$r_X$ has the following geometric description:

**Remark.** For every $P \in X$, there exists a hypersurface $H_P \subseteq \mathbb{P}^k_{\mathbb{F}_q}$ defined over $\mathbb{F}_q$, of degree $r_X$ and such that $H_P \cap X = X \setminus \{P\}$, and $r_X$ is the smallest such number.

Therefore, the following definition of $s(n, q)$ agrees with the one from the abstract:

$$s(n, q) = \max\{r_X| \text{ there exist } k \geq 1, X \subseteq \mathbb{P}^k(\mathbb{F}_q) \text{ with } \deg X = n\}$$

(the latter holds since the embedding dimension of $X$ is at most $n - 1$).

It is known ([KuW, Lemma 1.2]) that

$$s(n, q) \leq s(n + 1, q) \leq s(n, q) + 1 \text{ for } n \in \mathbb{N}_{>0}.$$ 

The function $s(n, q)$ can be extended to a step function $s(x, q)$ on $\mathbb{R}_{>0}$, its steps ("jump discontinuities") have height 1 and are precisely at those $x = n \in \mathbb{N}_{>1}$ where $s(n, q) = s(n - 1, q) + 1$. Trivially, the function $s(x, q)$ is determined by its initial value $s(1, q) = 0$ and its jump discontinuities $a_1 < a_2 < \ldots$ For $q = 2$ and $q = 3$, the function $s(n, q)$ was completely computed in ([KuW, Cor. 1.4]).

So far, for $q \geq 4$, the following was known (loc. cit.):

a) $a_i = i + 1$ for $i = 1, \ldots, q - 1$.

b) $a_{(m-1)(q-1)+1} = \frac{2^{m-1}}{q-1}$ and $a_{m(q-1)} = q^m$ for every $m \geq 2$.

c) For every $m \geq 2$ and for $r = 2, \ldots, q-2$ the jump discontinuity $a_{(m-1)(q-1)+r}$ lies in the half-open interval $I_{m,r} = \left(\frac{2^{m-1}}{q-1}, (r+1)q^{m-1}\right]$, but its precise position was unknown. For $m = 2$ we show

**Proposition 1.1.** For $q \geq 4$ and $r = 2, \ldots, q - 2$,

$$a_{q-1+r} = (r + 1)q$$

i. e., the first $2q-1$ jump discontinuities are: $2, \ldots, q, q+1, 3q, \ldots, (q-1)q, q^2, q^2 + q + 1$. Therefore $s(x, q)$ is known in the interval $[1, q^q + q + 1]$.

One may conjecture that the unknown jump discontinuities of $s(x, q)$ are at the right edges of the intervals $I_{m,r}$.

In the proof of this proposition we will study, for $1 \leq k < n \leq \frac{k+1}{q-1}q^{k+1}$ (i. e., where it makes sense), the invariants

$$s(n, k, q) := \max\{r_X| X \subseteq \mathbb{P}^k(\mathbb{F}_q) \text{ nondegenerate and of degree } n\}$$

(recall that a set $X \subseteq \mathbb{P}^k_{\mathbb{F}_q}$ is nondegenerate if it spans the whole space). [KrW, Cor. 2.2 a)] says that $s(n, k, q)$ is increasing in $n$. In contrast to this:
Proposition 1.2. $s(n, k, q)$ is decreasing in $k$.

Together with [KrW, Prop. 1.6] we shall see that this already implies Proposition 1.1. In addition, we are able to show the following improvement of [KrW, Prop. 1.4 b]):

Proposition 1.3. For every $k \geq 2$ (and every prime power $q$),

\[ s(2q + k, k, q) = q \]

(note that the left hand side is well-defined since $k < 2q + k \leq q^k + q^{k-1} + \ldots + 1$).

We shall now define and study the following affine version of the function $s(n, q)$: Embed $\mathbb{A}^k(\mathbb{F}_q)$ into $\mathbb{P}^k(\mathbb{F}_q) = \{ \mathbb{F}_q \cdot v | v \in \mathbb{F}_q^{k+1} \setminus \{0\} \}$ by $(x_1, \ldots, x_k) \mapsto (1, x_1, \ldots, x_k) = \mathbb{F}_q \cdot (1, x_1, \ldots, x_k)$. For an arbitrary set $\mathcal{X} \subseteq \mathbb{A}^k(\mathbb{F}_q)$, by a remark from above, $r_\mathcal{X}$ is the smallest number $r$ such that any interpolation problem

\[ \varphi(P) = w_P \text{ (for } P \in \mathcal{X}, w_P \in \mathbb{F}_q) \]

has a polynomial solution $\varphi$ of degree $\leq r$ ($r_\mathcal{X}$ is the interpolation degree of $\mathcal{X}$ in the sense of [E, section 4A]).

Definition. a) We call a subset $\mathcal{X} \subseteq \mathbb{P}^k(\mathbb{F}_q)$ affine if there exists a hyperplane $H \subseteq \mathbb{P}^k(\mathbb{F}_q)$, defined over $\mathbb{F}_q$ and disjoint from $\mathcal{X}$.

b) $s_a(n, q) := \max \{ r_\mathcal{X} | \text{ there exist } k \geq 1, \mathcal{X} \subseteq \mathbb{P}^k(\mathbb{F}_q), \mathcal{X} \text{ affine}, \deg \mathcal{X} = n \}$.

By what was just said, this definition agrees with the one from the abstract. The following proposition describes $s_a(n, q)$ completely:

Proposition 1.4. Let $r, m, n \in \mathbb{N}_>0$ and $r \leq q - 1$.

For $rq^{m-1} \leq n < (r + 1)q^{m-1}$,

\[ s_a(n, q) = (m - 1)(q - 1) + r - 1. \]

It turns out (see section 4) that this is a simple application of the Cayley-Bacharach conjecture ([EGH, CB12]). However with regard to the function $s$ of our main interest, we have:

Remark 1.5. The functions $s_a$ and $s$ are different.

In fact, for any $m \geq 2$, by [KuW, Theorem 1.3],

\[ s \left( \frac{q^m - 1}{q - 1}, q \right) = (m - 1)(q - 1) + 1, \]

whereas, by Proposition 1.4 with $r = 1$

\[ s_a \left( \frac{q^m - 1}{q - 1}, q \right) = (m - 1)(q - 1). \]
2 The function $s(n, k, q)$ and proofs of 1.1, 1.2

The invariants $s(n, k, q)$ are finer than $s(n, q)$: It is easily seen that one always has

$$s(n, q) = \max \left\{ s(n, k, q) \mid 1 \leq k < n \leq \frac{q^{k+1} - 1}{q - 1} \right\}.$$  

$s(n, k, q)$ was studied by Martin Kreuzer and the second author in [KrW]: $s(n, k, q)$ is increasing in $n$ ([KrW, Cor. 2.2 a]) and $s(n, k, q)$ was completely computed in both cases $q = 2$ and $k = 2$ ([KrW, Prop. 1.2 resp. Prop. 1.6]).

Proof of 1.2: Let $q = p^e$ be a prime power, $e \geq 1$ and

$$2 \leq k < n \leq \frac{q^k - 1}{q - 1} \quad \left( = |\mathbb{P}^{k-1}(\mathbb{F}_q)| \right).$$

We have to show that $s(n, k, q) \leq s(n, k - 1, q)$: It is clear from our hypothesis that both numbers $s(n, k, q)$ and $s(n, k - 1, q)$ are defined. Now, let $\mathcal{X} \subseteq \mathbb{P}^k(\mathbb{F}_q)$ be nondegenerate of degree $n$ and $r_{\mathcal{X}} = s(n, k, q)$.

In any case the dimension of the $\mathbb{F}_q$-vector space

$$(\mathbb{F}_q[X_0, \ldots, X_k]/I_{\mathcal{X}})_{r_{\mathcal{X}} - 1}$$

is smaller than $n$, therefore $\mathbb{F}_q[I_{\mathcal{X}}] := \mathbb{F}_q[X_0, \ldots, X_k]$ contains no polynomial $p$ of degree $r_{\mathcal{X}} - 1$ with (if necessary we renumber the points $P_i$)

$$P_1 \notin V^+(p) \quad \quad P_2, \ldots, P_n \in V^+(p)$$

We claim there exists a line $l \subseteq \mathbb{P}^k(\mathbb{F}_q)$ with $l \cap \mathcal{X} = \{P_1\}$.

Proof of this claim: For the lines $P_1 \lor P_i$ connecting $P_1$ with $P_i$ we have:

$$\left| \left( \bigcup_{i=2}^n P_1 \lor P_i \right) \right| \leq 1 + (n - 1) \cdot q \leq 1 + \left( \frac{q^k - 1}{q - 1} - 1 \right) \cdot q = \frac{q^{k+1} - q^2 + q - 1}{q - 1}$$

and the latter is

$$< \frac{q^{k+1} - 1}{q - 1} = |\mathbb{P}^k(\mathbb{F}_q)|. \quad \square$$

We choose $P \in l \setminus \{P_1\}$ and take the projection with center $P$:

$$\mathbb{P}^k(\mathbb{F}_q) \setminus \{P\} \xrightarrow{\pi} \mathbb{P}^{k-1}(\mathbb{F}_q).$$

$l = P_1 \lor P$ connects $P_1$ with $P$, and $l \setminus \{P\}$ is the fibre over $\pi(P_1)$. Because of $l \cap \mathcal{X} = \{P_1\}$, the restriction

$$\pi|_{\mathcal{X}} : \mathcal{X} \to \mathbb{P}^{k-1}(\mathbb{F}_q)$$
has only $P_1$ in its fibre over $\pi(P_1)$. Let $Y_0, \ldots, Y_{k-1}$ be the coordinates of $P_{k-1}(\mathbb{F}_q)$. Algebraically, $\pi$ corresponds to a homogenous, injective ring homomorphism

$$\iota : \mathbb{F}_q[Y] := \mathbb{F}_q[Y_0, \ldots, Y_{k-1}] \to \mathbb{F}_q[X_0, \ldots, X_k]$$

(under which the $Y_i$ are mapped to certain linear forms). The ring $\mathbb{F}_q[Y]$ contains no polynomial $p_0$ of degree $r_X - 1$ with

$$\pi(P_1) \not\in V^+(p_0)$$

$$\pi(P_2), \ldots, \pi(P_n) \in V^+(p_0),$$

because otherwise $\iota(p_0) \in \mathbb{F}_q[X]$ would be a polynomial of degree $r_X - 1$ and $P_1 \not\in V^+(\iota(p_0)), P_2, \ldots, P_n \in V^+(\iota(p_0)).$

By construction, $\pi(P_1)$ is not contained in $\{\pi(P_2), \ldots, \pi(P_n)\}$. In particular, from (1) above we conclude

$$r_{\pi(X)} \geq r_X$$

and furthermore (note that $\pi(X) \subseteq \mathbb{P}^{k-1}(\mathbb{F}_q)$ is nondegenerate because $I_X$ contains no linear form, a fortiori $I_{\pi(X)} = I_X \cap \mathbb{F}_q[Y]$ contains no linear form) by [KrW, Cor. 2.2 a)],

$$s(n, k - 1, q) = s(|\pi(X)|, k - 1, q) \geq r_X = s(n, k, q).$$

\[ \square_{1.2} \]

1.2 implies 1.1: Note that the first jump discontinuities $a_1 = 2, \ldots, a_q = q + 1$ as well as $a_{2q-2} = q^2, a_{2q-1} = q^2 + q + 1$ are known by [KuW, Cor. 1.4]. To determine the jump discontinuities $a_{q+1}, \ldots, a_{2q-3}$ which are missing in between (at least for $q \geq 4$), we use the following consequence of proposition 1.2:

**Corollary 2.1.** In the interval $\left(\frac{q^m - 1}{q-1}, \frac{q^{m+1} - 1}{q-1}\right], m \geq 1$, one has

$$s(n, k, q) = s(n, m, q).$$

**Proof:** $s(n, k, q)$ is decreasing in $k$ and we simply take the smallest possible value for $k$ where $s(n, k, q)$ is defined. \[ \square_{2.1} \]

In particular, for $n \in \{q + 2, \ldots, \frac{q^2 - 1}{q-1} = q^2 + q + 1\}$,

$$s(n, q) = s(n, 2, q)$$

and the latter function was concretely computed in [KrW, Prop. 1.6]. Hence we can read off all jump discontinuities in this range of $n$. \[ \square_{1.2 \Rightarrow 1.1} \]

**Remark 2.2.** Let $s_a(n, k, q)$ be the largest interpolation degree that any non-degenerate $X \subseteq \mathbb{A}^k(\mathbb{F}_q)$ of degree $n$ can achieve. Similar arguments as above show, that

$$s_a(n, k, q) = s_a(n, q), \text{ for } q^{k-1} < n \leq q^k,$$

hence, by 1.4, $s_a(n, k, q)$ is well known in this range.
3 Proof of 1.3

Note that, for every $k \geq 2$ and every prime power $q$, $s(2q + k, k, q)$ is defined since $2q + k \leq q^{k+1} + \ldots + q + 1$. To prove 1.3, we need some preparations:

Let $K$ be a field and $k \geq 2$. For a vector $a = (a_0, \ldots, a_k) \in K^{k+1}$, we call
\[
supp a := \{i | a_i \neq 0\} \subseteq \{0, \ldots, k\}
\]
its support and
\[
\|a\| := |supp a|
\]
its weight. We start with the map
\[
\tilde{\varphi} : K^{k+1} \rightarrow K^{(k+1)/2}, (a_0, \ldots, a_k) \mapsto (a_0a_1, \ldots, a_{k-1}a_k)
\]
(strictly speaking we once and for all fix an arbitrary order on the set of all pairs $(a_i, a_j)$ for $j > i$ on the right-hand side).

Lemma 3.1. Let $v_1, v_2, v_3 \in K^{k+1} \setminus \{0\}$, write $v_i = (v_{ij})_{i=0,\ldots,k}$.

1. Assume that $v_1$ and $v_2$ have the same support and weight at least three.
   If $v_1$ and $v_2$ are linearly independent then $\tilde{\varphi}(v_1)$ and $\tilde{\varphi}(v_2)$ are likewise linearly independent.

2. If $v_1$, $v_2$ and $v_3$ have pairwise different support and $\|v_i\| \geq 2$ for $i = 1, 2, 3$, then $\tilde{\varphi}(v_1)$, $\tilde{\varphi}(v_2)$ and $\tilde{\varphi}(v_3)$ are linearly independent.

Proof: 1.: W.l.o.g. we assume that $\{0, 1, 2\} \subseteq supp v_1 (= supp v_2)$ and that
\[
det \begin{pmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{pmatrix} \neq 0.
\]
Then
\[
\tilde{\varphi}(v_i) = (v_{i0} \cdot v_{i1}, v_{i0} \cdot v_{i2}, \ldots), i = 1, 2
\]
with
\[
det \begin{pmatrix} v_{10} \cdot v_{11} & v_{10} \cdot v_{12} \\ v_{20} \cdot v_{21} & v_{20} \cdot v_{22} \end{pmatrix} = v_{10}v_{20} \cdot det \begin{pmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{pmatrix} \neq 0;
\]
in particular $\tilde{\varphi}(v_1)$ and $\tilde{\varphi}(v_2)$ are linearly independent.

2.: W.l.o.g. $\|v_3\| \leq \|v_2\| \leq \|v_1\|$. The $\left(\frac{k+1}{2}\right)$-tuples $\tilde{\varphi}(v_1)$, $\tilde{\varphi}(v_2)$, $\tilde{\varphi}(v_3)$ have pairwise different support (since this property holds for $v_1$, $v_2$, $v_3$). In particular, whenever $i \neq j$, the vectors $\tilde{\varphi}(v_i)$ and $\tilde{\varphi}(v_j)$ are linearly independent. We assume to the contrary that $\tilde{\varphi}(v_1)$, $\tilde{\varphi}(v_2)$, $\tilde{\varphi}(v_3)$ are linearly dependent. Since any two of them are linearly independent there exist $\lambda, \mu \in K \setminus \{0\}$ such that
\[
\tilde{\varphi}(v_3) = \lambda \tilde{\varphi}(v_1) + \mu \tilde{\varphi}(v_2).
\]
\[
\|v_2\| \leq \|v_1\| \text{ and } supp v_1 \neq supp v_2, \text{ hence } supp v_1 \not\subseteq supp v_2. \text{ Therefore we may assume that } supp v_1 = \{0, \ldots, d\} \text{ with } 1 \leq d \leq k \text{ and } 0 \not\subseteq supp v_2.
\]
\[
v_{10}v_{11} \neq 0, \ldots, v_{10}v_{1d} \neq 0,
\]
\[ v_{20}v_{21} = \ldots = v_{20}v_{2d} = 0 \]

and (\#) implies

\[ v_{30}v_{31} = \lambda v_{10}v_{11} \neq 0, \ldots, v_{30}v_{3d} = \lambda v_{10}v_{1d} \neq 0, \]

hence supp \( v_1 = \{0, \ldots, d\} \subseteq \text{supp} \ v_3 \); because of \( \|v_3\| \leq \|v_1\| \) we get supp \( v_1 = \text{supp} \ v_3 \) which contradicts our hypothesis. \( \square \)

For any given subset \( M \subseteq \{0, \ldots, k\} \), \(|M| \geq 2\) set

\[ \mathbf{P}_M^k = \{(v) \in \mathbf{P}^k(K) | \text{supp} \ v = M\} \]

and

\[ \overline{M} := \text{supp} \tilde{\varphi}(v), \text{if sup} \sup v = M \]

(\( \overline{M} \) does not depend on the choice of \( v \)). The map

\[ \tilde{\varphi} : \mathbf{P}_M^k \to \mathbf{P}^{(k+1)-1}_{\overline{M}}, \langle v \rangle \mapsto \langle \tilde{\varphi}(v) \rangle \]

is well-defined and Lemma 3.1.1. implies:

**Corollary 3.2.** In case \(|M| \geq 3\), \( \tilde{\varphi} : \mathbf{P}_M^k \to \mathbf{P}^{(k+1)-1}_{\overline{M}} \) is injective.

Furthermore we need [KuW, Remark 5.1] in the following form: Let \( \mathcal{X} = \{P_1, \ldots, P_n\} \subseteq \mathbf{P}^k(F_q) \), deg \( \mathcal{X} = n \). For every \( i \), choose \( v_i \in F_{k+1}^q \) with \( P_i = \langle v_i \rangle \). Define

\[ ev_d : R_d \to F_q^n, F \mapsto (F(v_1), \ldots, F(v_n))^T; \quad V(d) := \text{im}(ev_d) \]

Then ker(\( ev_d \)) = (\( I_\mathcal{X} \)) and hence

\[ \dim V(d) = \dim \frac{R_d}{(I_\mathcal{X})_d}. \]

By \( A_d \) we denote the coefficient matrix of \( ev_d \) with respect to the basis \( B = \{X^\alpha | \alpha = d\} \) of \( R_d \). We have \( H_\mathcal{X}(d) = \text{rank} A_d \). The rows of \( A_d \) are the vectors \( \langle X^\alpha(v_i) | \alpha \in \mathbb{N}^{k+1}, \alpha = d \rangle \), for \( i = 1, \ldots, n \) (assuming \( B \) is suitably ordered).

**Proof of 1.3:** By [KrW, Prop. 1.4 b)] one has \( s(2q + k - 1, k, q) = q \) and, by using [KrW, Prop. 2.1 e)] twice, it is easy to see that

\[ q \leq s(2q + k, k, q) \leq q + 1. \]

Therefore we have to show \( r_\mathcal{X} \neq q + 1 \) for every \( \mathcal{X} \subseteq \mathbf{P}^k(F_q) \), nondegenerate and with deg \( \mathcal{X} = 2q + k \): We claim that \( H_\mathcal{X}(2) \geq k + 4 \).

**Proof of this claim:** W.l.o.g. we may assume that \( \mathcal{X}_1 := \{\langle e_0\rangle, \ldots, \langle e_k\rangle\} \subseteq \mathcal{X} \), where \( e_i \) is the \( i \)-th standard basis vector in \( F_{q+1}^k \). We choose \( v_1, \ldots, v_{2q - 1} \in F_{q+1}^k \) such that

\[ \mathcal{X} = \mathcal{X}_1 \cup \{\langle v_1\rangle, \ldots, \langle v_{2q - 1}\rangle\}. \]
We define
\[ \varphi : \mathbb{F}_q^{k+1} \to \mathbb{F}_q^{(k+2)} \]
\[ a = (a_0, \ldots, a_k) \to (a_0^2, \ldots, a_k^2, a_0a_1, \ldots, a_{k-1}a_k) = (X^\alpha(a) \mid |\alpha| = 2). \]

The rows of \( A_2 \) are \( \varphi(e_0), \ldots, \varphi(e_k), \varphi(v_1), \ldots, \varphi(v_{2q-1}) \):
\[
\begin{pmatrix}
1 & 0 & & & \cdots & & 0 & \cdots & 0 & 1 \\
& & \ddots & & & & & & & \\
& & & & 0 & & & & & \\
& & & & & 1 & & & & \\
& & & & & & A & & & \\
\end{pmatrix},
\]
with \( \varphi \) being taken from Lemma 3.1. To prove our claim \( H_X(2) \geq k + 4 \), we have to show that rank \( \tilde{A} \geq 3 \) (since \( H_X(2) = \text{rank} \ A_2 = k + 1 + \text{rank} \tilde{A} \)):

Let \( M \subseteq \{0, \ldots, k\}, |M| \geq 2 \) and \( X_M := \mathcal{X} \cap \mathbb{P}_M \) (\( = (\mathcal{X} \setminus \mathcal{X}_1) \cap \mathbb{P}_M \)). Clearly,
\[ |L \cap \mathbb{P}_M| \leq q - 1 \text{ for every line } L \subseteq \mathbb{P}^k(\mathbb{F}_q) \]  
(1)
\[ \text{If } |M| = 2, \text{ then } |\mathbb{P}_M^k| = q - 1. \]  
(2)

To finish the proof of our claim, we distinguish between two cases:

a) If \( \mathcal{X} \setminus \mathcal{X}_1 \) contains three points \( \langle w_1 \rangle, \langle w_2 \rangle \) and \( \langle w_3 \rangle \) with pairwise different supports, then the vectors \( \varphi(w_1), \varphi(w_2), \varphi(w_3) \) are linearly independent and rank \( \tilde{A} \geq 3 \), by Lemma 3.1.2.

b) If there are at most two \( M \) with \( |M| \geq 2 \) and \( X_M \neq \emptyset \), then, because of \( |\mathcal{X} \setminus \mathcal{X}_1| = 2q - 1 \), there exists such an \( M \) with \( |X_M| \geq q \). By (2) from above, we get \( |M| \geq 3 \) and then, by Corollary 3.2, \( |\varphi(X_M)| \geq q \). By (1) it is clear that the set \( \varphi(X_M) \subseteq \mathbb{P}^{(k+2)}_{\mathbb{F}_q} \) is not contained in a line, therefore, rank \( \tilde{A} \geq 3 \).

\[ \square \text{claim} \]

\( H_X(2) = k + 1 + \text{rank} \tilde{A} \geq k + 4 \). Assume that \( r_X = q + 1 \): The first difference function \( \Delta H_X = H_X(d) - H_X(d - 1) \) has the form
\[
\Delta H_X : 1, k, h_2, h_3, \ldots, h_{q+1}, 0, 0, \ldots \text{ with } h_j \geq 1 \text{ (} j = 2, \ldots, q + 1 \text{).} 
\]

\( H_X(2) \geq k + 4 \) implies
\[ h_2 = H_X(2) - H_X(1) \geq k + 4 - (k + 1) = 3. \]

Furthermore we have \( h_j \geq 2 \) for \( j = 3, \ldots, q \): Because if \( h_j \) was equal to 1 for some \( j \in \{3, \ldots, q\} \), then, by [KrW, Prop. 2.1 c)], also both \( h_q \) and \( h_{q+1} \) would be equal to 1; by [KrW, Prop. 2.1 d)], there would be a line \( L \subseteq \mathbb{P}^k(\mathbb{F}_q) \) with
\[ |\mathcal{X} \cap L| \geq r_X + 1 = q + 2 > q + 1 = |L|, \]
(in this context, see also [GMR, Prop. 5.2]) which is absurd.

Hence, we finally get

\[ \deg \mathcal{X} = \sum_{d \in \mathbb{N}} \Delta H_{\mathcal{X}}(d) \]
\[ = 1 + k + h_2 + (h_3 + \ldots + h_q) + h_{q+1} \]
\[ \geq 1 + k + 3 + (q - 2) \cdot 2 + 1 \]
\[ = 2q + k + 1, \]

which contradicts our assumptions. Therefore, \( r_X \neq q + 1 \). \( \square_{1.3} \)

4 Proof of 1.4

Similarly to [KuW, Lemma 1.2] we have

**Remark 4.1.** For all \( n \in \mathbb{N}_{>0} \),

\[ s_a(n, q) \leq s_a(n + 1, q) \leq s_a(n, q) + 1. \]

**Proof of 1.4:** From the proof of [KuW, Prop. 1.6 b)] we know there is an affine complete intersection \( X \subseteq \mathbb{A}^m(F_q) \subseteq \mathbb{P}^m(F_q) \) of degree \( rq^{m-1} \) and regularity \( (m-1)(q-1) + r - 1 \); hence

\[ s_a(n, q) \geq s_a(rq^{m-1}, q) \geq r_X = (m-1)(q-1) + r - 1 \text{ for } n \geq rq^{m-1}. \]

Conversely, let \( k \geq 1 \) and \( X \subseteq \mathbb{P}^k(F_q) \) affine with \( \deg X < (r + 1)q^{m-1} \). We have to show that \( r_X \leq (m-1)(q-1) + r - 1 \) and may assume that \( \mathcal{X} \) does not meet the hyperplane \( X_0 = 0 \). Then for \( \mathfrak{S} := R/I_X + (X_0) = F_q[X_1, \ldots, X_k]/J \),

\[ \{X_1^q, \ldots, X_k^q\} \subseteq J \text{ and } \dim_{F_q} \mathfrak{S} = \deg X < (r + 1)q^{m-1}. \]

Finally, by the following simple combinatorial lemma, we have \( \mathfrak{S}_d = 0 \) for \( d = (m-1)(q-1) + r \), i.e. \( r_X \leq (m-1)(q-1) + r - 1 \).

**Lemma 4.2.** Let \( k, m \) and \( q \) be natural numbers, \( k \geq 1 \) and \( 1 \leq r \leq q - 1 \). Let \( \alpha := (\alpha_1, \ldots, \alpha_k) \in \mathbb{N}^k \) be of degree \( |\alpha| := \alpha_1 + \ldots + \alpha_k = m(q-1) + r \) and such that \( 0 \leq \alpha_j \leq q - 1 \) for \( j = 1, \ldots, k \). Then

\[ (\alpha_1 + 1) \cdot \ldots \cdot (\alpha_k + 1) \geq (r + 1)q^m. \]

This follows from [KuW, Lemma 2.2 b)] and is easily seen anyway.

Assume \( \mathfrak{S}_d \neq 0 \) for \( d = (m-1)(q-1) + r \). By Macaulay’s Theorem [BH, Theorem 4.2.3] there is an order ideal \( \mathfrak{M} \) of monomials in \( F_q[X_1, \ldots, X_k] \) such that the elements \( X^\alpha + J, X^\alpha \in \mathfrak{M} \) form an \( F_q \)-basis of \( \mathfrak{S} \). Since \( \mathfrak{S}_d \neq 0 \) and \( \{X_1^q, \ldots, X_k^q\} \subseteq J \), there is a monomial \( X^\alpha \in \mathfrak{M} \) \( 0 \leq \alpha_j \leq q - 1 \) for \( j = 1, \ldots, k \) of degree \( d \). Hence by the lemma, \( \dim_{F_q} \mathfrak{S} = |\mathfrak{M}| \geq |\{X^\beta \mid X^\beta \text{ divides } X^\alpha \}| = (\alpha_1 + 1) \cdot \ldots \cdot (\alpha_k + 1) \geq (r + 1)q^{m-1} \), a contradiction. \( \square \)
5 More general considerations

For \( k \geq 1, q \geq 2 \) (not necessarily a prime power), let \( I(k, q) \subseteq \mathbb{Z}[X_0, \ldots, X_k] \) be the ideal generated by the \( 2 \times 2 \)-minors of the matrix \( \begin{pmatrix} X_0^q & \cdots & X_k^q \\ X_0 & \cdots & X_k \end{pmatrix} \).

For instance, if \( q \) is a prime power, then \( I(k, q) \cdot \mathbb{F}_q[X_0, \ldots, X_k] \) is the homogeneous vanishing ideal of \( \mathcal{X} = \mathbb{P}^k(\mathbb{F}_q) \subseteq \mathbb{P}^k_{\mathbb{F}_q} \). More generally, let \( K \) be the cyclotomic extension of degree \( q-1 \) of \( \mathbb{Q} \) or of a prime field \( \mathbb{F}_l \) with \( l \mid (q-1) \). Then \( I(k, q) \) defines a smooth finite subscheme \( \mathcal{P}_q^k(K) \subseteq \mathbb{P}^k(K) \subseteq \mathbb{P}^k_K \) of degree \( \frac{q^{k+1}-1}{q-1} \) and its ideal is given by \( I(k, q) \cdot R \) (note that this ideal is saturated).

Questions. What are the Hilbert functions of the subschemes \( \mathcal{X} \subseteq \mathcal{P}_q^k(K) \)? Does the answer depend on \( K \)? Simpler problem: Which numbers are occurring as the regularities of such \( \mathcal{X} \) of a given degree \( n \)? Find a formula for

\[
s(n, q; K) := \max \{ r_{\mathcal{X}} \mid \text{there exist } k \geq 1 \text{ and } \mathcal{X} \subseteq \mathcal{P}_q^k(K) \text{ with } \deg \mathcal{X} = n \}.
\]

And again: Does \( s(n, q; K) \) depend on \( K \)?

These considerations were suggested by the referee of the paper [KuW] and are motivated by the following results: Analyzing the proof of Theorem 1.3 in [KuW], we see that its statements remain true if one allows \( q \) to be an arbitrary integer \( \geq 2 \) and replaces \( \mathbb{F}_q \) by a cyclotomic field \( K \) as above. In particular if \( q \) is a prime power we have

\[
s(n, q; K) = s(n, q)
\]

for all such \( K \) and all \( n \) for which theorem 1.3 (loc. cit.) applies. Moreover, the functions \( s(n, 2; K) = s(n, 2) \) and \( s(n, 3; K) = s(n, 3) \) are well-known and independent from \( K \).

Acknowledgement. We thank Martin Kreuzer for his valuable comments to the proof of Proposition 1.4.

References


Authors’ address: Fakultät für Mathematik, D 93040 Regensburg, Germany. Email: michael.hellus@mathematik.uni-regensburg.de, rolf.waldi@mathematik.uni-regensburg.de