JOURNAL OF COMMUTATIVE ALGEBRA
Volume 7, Number 2, Summer 2015

INTERPOLATION IN AFFINE AND PROJECTIVE SPACE OVER A FINITE FIELD

MICHAEL HELLUS AND ROLF WALDI

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 Kunz and the second author in [**8**] and completely determined for $q = 2$ and $q = 3$. For $q \geq 4$, we improve the results from [**8**].

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 $\mathbb{P}^k(K) \subseteq \mathbb{P}^k_K = \operatorname{Proj} R$ the set of all K-rational points.

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

$$I_{\mathcal{X}} := (\{F \in R \text{ homogenous } | F(P) = 0 \text{ for all } P \in \mathcal{X}\}),$$

we denote its homogenous vanishing ideal. Let $S := \bigoplus_{d \geq 0} S_d := R/I_{\mathcal{X}}$ and

$$H_{\mathcal{X}}(d) := \dim_K(S_d)$$

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

$$H_{\mathcal{X}}(d) = n \text{ for } d \geq r_{\mathcal{X}} \text{ and } H_{\mathcal{X}}(r_{\mathcal{X}} - 1) \leq n-1.$$

It is well known that $H_{\mathcal{X}}$ is strictly increasing for $0 \leq d \leq r_{\mathcal{X}}$; in particular, $r_{\mathcal{X}} \leq n-1$.

2010 AMS *Mathematics subject classification.* Primary 14G15.
Received by the editors on September 18, 2013, and in revised form on January 2, 2014.
DOI:10.1216/JCA-2015-7-2-207

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 $H_{\mathcal{X}}$ respectively, for which regularities $r_{\mathcal{X}}$ 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 ([**6,** Sections 1 and 3]).

$r_{\mathcal{X}}$ has the following geometric description:

Remark. $r_{\mathcal{X}}$ is the smallest number such that for every $P \in \mathcal{X}$, there exists a hypersurface $H_P \subseteq \mathbb{P}^k_{\mathbb{F}_q}$ defined over $\mathbb{F}_q$, of degree $r_{\mathcal{X}}$ which separates P from $\mathcal{X}$, that is $H_P \cap \mathcal{X} = \mathcal{X} \setminus \{P\}$.

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

$$\begin{aligned} s(n,q) &= \max\{r_{\mathcal{X}} \mid \text{ there exist } k \geq 1, \mathcal{X} \subseteq \mathbb{P}^k(\mathbb{F}_q) \text{ with } \deg \mathcal{X} = n\} \\ &= \max\{r_{\mathcal{X}} | \mathcal{X} \subseteq \mathbb{P}^{n-1}(\mathbb{F}_q), \deg \mathcal{X} = n\} \end{aligned}$$

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

It is known ([**8,** 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 $a_1 < a_2 < \dots$. For $q = 2$ and $q = 3$, the function $s(n, q)$ was completely computed in ([**8,** Corollary 1.4]). So far, for $q \geq 4$, the following was known (loc. cit.):

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

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

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

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

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

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* $[1, 2(q^2+q+1)]$.

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 $1 \leq k < n \leq (q^{k+1}-1)/(q-1)$ (i.e., where it makes sense), the invariants

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

(recall that a set $\mathcal{X} \subseteq \mathbb{P}^k_{\mathbb{F}_q}$ is **nondegenerate** if it spans the whole space). [**7,** 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 [**7,** Proposition 1.6] we shall see that this already implies Proposition 1.1. In addition, we are able to show the following improvement of [**7,** Proposition 1.4b)]:

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* $k < 2q+k \leq q^k + q^{k-1} + \cdots + 1$).

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 $(x_1, \ldots, x_k) \mapsto \langle 1, x_1, \ldots, x_k \rangle = \mathbb{F}_q \cdot (1, x_1, \ldots, x_k)$. 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 φ of degree $\leq r$ ($r_{\mathcal{X}}$ is the *interpolation degree* of $\mathcal{X}$ in the sense of [**3,** section 4A]).

Definition 1.4. 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) $s_a(n,q) := \max\{r_{\mathcal{X}} |$ there exist $k \geq 1, \mathcal{X} \subseteq \mathbb{P}^k(\mathbb{F}_q), \mathcal{X}$ 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 1.5. *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 ([**4,** CB12]). However, with regard to the function s of our main interest, we have:

Remark 1.6. The functions s_a and s are different.

In fact, for any $m \geq 2$, by [**8,** Theorem 1.3],

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

whereas, by Proposition 1.5 with $r = 1$

$$s_a\left(\frac{q^m-1}{q-1}, q\right) = (m-1)(q-1).$$

2. The function $\mathbf{s(n,k,q)}$ 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

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

$s(n,k,q)$ was studied by Kreuzer and the second author in [**7**]:

$s(n,k,q)$ is increasing in n ([**7,** Corollary 2.2a)]) and $s(n,k,q)$ was completely computed in both cases $q = 2$ and $k = 2$ ([**7,** Proposition 1.2, respectively, Proposition 1.6]).

Proof that $s(n,k,q)$ is decreasing in k (Proposition 1.2). Let $q = p^e$ be a prime power, $e \geq 1$ and

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

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 $\mathcal{X} = \{P_1, \dots P_n\} \subseteq \mathbb{P}^k(\mathbb{F}_q)$ 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

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

is smaller than n; therefore, according to the remark from the introduction, $\mathbb{F}_q[\underline{X}] := \mathbb{F}_q[X_0, \dots, X_k]$ contains no homogenous polynomial p of degree $r_{\mathcal{X}} - 1$ with (if necessary we renumber the points P_i)

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

where $V^+(p)$ denotes the zero set of p in $\mathbb{P}^k(\mathbb{F}_q)$.

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

Proof of claim. For the lines $P_1 \vee P_i$ connecting P_1 with P_i we have:

$$\left|\left(\bigcup_{i=2}^{n} P_1 \vee P_i\right)\right| \leq 1 + (n-1) \cdot q \leq 1 + \left(\frac{q^k - 1}{q - 1} - 1\right) \cdot q$$
$$= \frac{q^{k+1} - q^2 + q - 1}{q - 1} < \frac{q^{k+1} - 1}{q - 1} = \left|\mathbb{P}^k(\mathbb{F}_q)\right|.$$

So there is at least one point $P \in \mathbb{P}^k(\mathbb{F}_q)$ not on the union of the lines $P_1 \vee P_i$; take l to be the line connecting P and P_1. $\square_{\text{claim}}$

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

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

$l = P_1 \vee P$ 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

$$\pi|\mathcal{X} : \mathcal{X} \longrightarrow \mathbb{P}^{k-1}(\mathbb{F}_q)$$

has only P_1 in its fibre over $\pi(P_1)$.

Let $Y_0, \dots, Y_{k-1}$ be the coordinates of $\mathbb{P}^{k-1}(\mathbb{F}_q)$. Algebraically, π corresponds to a homogenous, injective ring homomorphism

$$\iota : \mathbb{F}_q[\underline{Y}] := F_q[Y_0, \dots, Y_{k-1}] \longrightarrow \mathbb{F}_q[X_0, \dots, X_k]$$

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

$$\begin{aligned} \pi(P_1) &\notin V^+(p_0) \\ \pi(P_2), \dots, \pi(P_n) &\in V^+(p_0), \end{aligned} \tag{2.1}$$

because otherwise $\iota(p_0) \in \mathbb{F}_q[\underline{X}]$ would be a polynomial of degree $r_{\mathcal{X}} - 1$ with $P_1 \notin V^+(\iota(p_0)), P_2, \dots, P_n \in V^+(\iota(p_0))$.

By construction, $\pi(P_1)$ is not contained in $\{\pi(P_2), \dots, \pi(P_n)\}$. In particular, from (2.1) above we conclude

$$r_{\pi(\mathcal{X})} \geq r_{\mathcal{X}},$$

and furthermore (note that $\pi(\mathcal{X}) \subseteq \mathbb{P}^{k-1}(\mathbb{F}_q)$ is nondegenerate because $I_{\mathcal{X}}$ contains no linear form, a fortiori $I_{\pi(\mathcal{X})} = I_{\mathcal{X}} \cap \mathbb{F}_q[\underline{Y}]$ contains no linear form) by [**7,** Corollary 2.2a)],

$$s(n, k-1, q) \geq s(|\pi(\mathcal{X})|, k-1, q) \geq r_{\pi(\mathcal{X})} \geq r_{\mathcal{X}} = s(n, k, q). \quad \square_{1.2}$$

Proposition 1.2 *implies Proposition* 1.1. Note that the first jump discontinuities $a_1 = 2, \dots, a_q = q+1$ as well as $a_{2q-2} = q^2, a_{2q-1} = q^2 + q + 1$ are known by [**8,** Corollay 1.4]. To determine the jump discontinuities $a_{q+1}, \dots, a_{2q-3}$ 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* $((q^m - 1)/(q-1), (q^{m+1} - 1)/(q-1)]$, $m \geq 1$, *one has*

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

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 $n \in \{q+2, \dots, (q^3 - 1)/(q-1) = q^2 + q + 1\}$,

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

and the latter function was concretely computed in [**7,** Proposition 1.6]. Furthermore, by [**8,** Theorem 1.3a)], $s(n,q) = 2q-1$ for $q^2+q+1 \leq n \leq 2(q^2+q+1)$. $\square_{1.2 \Rightarrow 1.1}$

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

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

hence, by Proposition 1.5, $s_a(n,k,q)$ 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 $2q+k \leq q^k + \ldots + q + 1$. To prove Proposition 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

$$\operatorname{supp} a := \{i | a_i \neq 0\} \subseteq \{0, \ldots, k\}$$

its support and

$$\|a\| := |\operatorname{supp} a|$$

its weight. We start with the map

$$\widetilde{\varphi} : K^{k+1} \to K^{\binom{k+1}{2}}, (a_0, \ldots, a_k) \longmapsto (a_0 a_1, \ldots, a_{k-1} a_k)$$

(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 $v_1, v_2, v_3 \in K^{k+1} \setminus \{0\}$, and write $v_i = (v_{ij})_{\substack{j=0,\ldots,k \\ i=1,2,3}}$.*

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

Proof. (i) Without loss of generality, we assume that $\{0,1,2\} \subseteq \operatorname{supp} v_1$ $(= \operatorname{supp} v_2)$ and that $\det \left(\begin{smallmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{smallmatrix}\right) \neq 0$. Then

$$\widetilde{\varphi}(v_i) = (v_{i0}v_{i1}, v_{i0}v_{i2}, \ldots), \quad i = 1, 2,$$

with

$$\det \begin{pmatrix} v_{10}v_{11} & v_{10}v_{12} \\ v_{20}v_{21} & v_{20}v_{22} \end{pmatrix} = v_{10}v_{20} \cdot \det \begin{pmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{pmatrix} \neq 0;$$

in particular $\widetilde{\varphi}(v_1)$ and $\widetilde{\varphi}(v_2)$ are linearly independent.

(ii) Without loss of generality, $\|v_3\| \leq \|v_2\| \leq \|v_1\|$. The $\binom{k+1}{2}$-tuples $\widetilde{\varphi}(v_1)$, $\widetilde{\varphi}(v_2)$, $\widetilde{\varphi}(v_3)$ have pairwise different support (since this property holds for v_1, v_2, v_3). In particular, whenever $i \neq j$, the vectors $\widetilde{\varphi}(v_i)$ and $\widetilde{\varphi}(v_j)$ are linearly independent. We assume to the contrary that $\widetilde{\varphi}(v_1)$, $\widetilde{\varphi}(v_2)$, $\widetilde{\varphi}(v_3)$ are linearly dependent. Since any two of them are linearly independent there exist $\lambda, \mu \in K \setminus \{0\}$ such that

$$(*) \qquad \widetilde{\varphi}(v_3) = \lambda\widetilde{\varphi}(v_1) + \mu\widetilde{\varphi}(v_2).$$

$\|v_2\| \leq \|v_1\|$ and $\operatorname{supp} v_1 \neq \operatorname{supp} v_2$; hence, $\operatorname{supp} v_1 \nsubseteq \operatorname{supp} v_2$. Therefore, we may assume that $\operatorname{supp} v_1 = \{0, \ldots, d\}$ with $1 \leq d \leq k$ and $0 \notin \operatorname{supp} v_2$.

$$v_{10}v_{11} \neq 0, \ldots, v_{10}v_{1d} \neq 0,$$
$$v_{20}v_{21} = \cdots = v_{20}v_{2d} = 0$$

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, $\operatorname{supp} v_1 = \{0, \ldots, d\} \subseteq \operatorname{supp} v_3$. Because of $\|v_3\| \leq \|v_1\|$, we get $\operatorname{supp} v_1 = \operatorname{supp} v_3$ which contradicts our hypothesis. □

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

$$\mathbb{P}^k_M = \{\langle v \rangle \in \mathbb{P}^k(K) | \operatorname{supp} v = M\}$$

and

$$\overline{M} := \operatorname{supp} \widetilde{\varphi}(v), \text{ if } \operatorname{supp} v = M$$

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

$$\widetilde{\varphi} : \mathbb{P}^k_M \longrightarrow \mathbb{P}^{\binom{k+1}{2}-1}_{\overline{M}}, \langle v \rangle \longmapsto \langle \widetilde{\varphi}(v) \rangle$$

is well defined and Lemma 3.1.i. implies:

Corollary 3.2. *In case* $|M| \geq 3$, $\widetilde{\varphi} : \mathbb{P}^k_M \to \mathbb{P}^{\binom{k+1}{2}-1}_{\overline{M}}$ *is injective.*

Furthermore we need [**8,** Remark 5.1] in the following form: Let $\mathcal{X} = \{P_1, \ldots, P_n\} \subseteq \mathbb{P}^k(\mathbb{F}_q)$, $\deg \mathcal{X} = n$. For every i, choose $v_i \in \mathbb{F}_q^{k+1}$ with $P_i = \langle v_i \rangle$. Define

$$ev_d : R_d \to \mathbb{F}_q^n, F \longmapsto (F(v_1), \ldots, F(v_n))^T; \quad V^{(d)} := \operatorname{im}(ev_d)$$

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

$$\dim V^{(d)} = \dim R_d/(I_{\mathcal{X}})_d.$$

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

Proof of Proposition 1.3. By [**7,** Proposition 1.4b)] one has $s(2q + k - 1, k, q) = q$ and, by using [**7,** Proposition 2.1e)] 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 $\mathcal{X} \subseteq \mathbb{P}^k(\mathbb{F}_q)$, nondegenerate and with $\deg \mathcal{X} = 2q + k$.

Claim. $H_{\mathcal{X}}(2) \geq k + 4$.

Proof of claim. Without loss of generality, we may assume that $\mathcal{X}_1 := \{\langle e_0 \rangle, \ldots, \langle e_k \rangle\} \subseteq \mathcal{X}$, where e_i is the ith standard basis vector in $\mathbb{F}_q^{k+1}$. Let $v_1, \ldots, v_{2q-1} \in \mathbb{F}_q^{k+1}$ be such that

$$\mathcal{X} = \mathcal{X}_1 \cup \{\langle v_1 \rangle, \ldots, \langle v_{2q-1} \rangle\}.$$

We define

$$\begin{aligned} \varphi : \mathbb{F}_q^{k+1} &\longrightarrow \mathbb{F}_q^{\binom{k+2}{2}} \\ a = (a_0, \ldots, a_k) &\longmapsto (a_0^2, \ldots, a_k^2, a_0 a_1, \ldots, a_{k-1} a_k) \\ &= (\, X^\alpha(a) | \, |\alpha| = 2) \,. \end{aligned}$$

The rows of A_2 are $\varphi(e_0),\ldots,\varphi(e_k),\varphi(v_1),\ldots,\varphi(v_{2q-1})$:

$$A_2 = \left(\begin{array}{ccc|c} 1 & & 0 & \\ & \ddots & & 0 \\ 0 & & 1 & \\ \hline & * & & \widetilde{A} \end{array}\right), \quad \text{where } \widetilde{A} = \begin{pmatrix} \widetilde{\varphi}(v_1) \\ \vdots \\ \widetilde{\varphi}(v_{2q-1}) \end{pmatrix},$$

with $\widetilde{\varphi}$ being taken from Lemma 3.1. To prove our claim $H_{\mathcal{X}}(2) \geq k+4$, we have to show that $\mathrm{rank}\widetilde{\mathrm{A}} \geq 3$ (since $H_{\mathcal{X}}(2) = \mathrm{rank}\mathrm{A}_2 = \mathrm{k}+1+\mathrm{rank}\widetilde{\mathrm{A}}$):

Let $M \subseteq \{0,\ldots,k\}$, $|M| \geq 2$ and $\mathcal{X}_M := \mathcal{X} \cap \mathbb{P}^k_M$ $(= (\mathcal{X} \setminus \mathcal{X}_1) \cap \mathbb{P}^k_M)$. Clearly, since every line has exactly $q+1$ $\mathbb{F}_q$-rational points,

$$|L \cap \mathbb{P}^k_M| \leq q-1 \text{ for every line } L \subseteq \mathbb{P}^k(\mathbb{F}_q) \tag{3.1}$$

$$\text{If } |M| = 2, \text{ then } \left|\mathbb{P}^k_M\right| = q-1. \tag{3.2}$$

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 $\widetilde{\varphi}(w_1)$, $\widetilde{\varphi}(w_2)$ and $\widetilde{\varphi}(w_3)$ are linearly independent and $\mathrm{rank}\widetilde{\mathrm{A}} \geq 3$, by Lemma 3.1.ii.
(b) If there are at most two M with $|M| \geq 2$ and $\mathcal{X}_M \neq \emptyset$, then, because of $|\mathcal{X} \setminus \mathcal{X}_1| = 2q-1 = q+q-1$, there exists such an M with $|\mathcal{X}_M| \geq q$. By equation (3.2), we get $|M| \geq 3$ and then, by Corollary 3.2, $|\widetilde{\varphi}(\mathcal{X}_M)| \geq q$. By equation (3.1) it is clear that the set $\widetilde{\varphi}(\mathcal{X}_M) \subseteq \mathbb{P}^{\binom{k+1}{2}-1}_{\overline{M}}$ is not contained in a line; therefore, $\mathrm{rank}\widetilde{\mathrm{A}} \geq 3$. $\square_{\text{claim}}$

$H_{\mathcal{X}}(2) = k+1+\mathrm{rank}\widetilde{\mathrm{A}} \geq \mathrm{k}+4$. Assume that $r_{\mathcal{X}} = q+1$: The first difference function $\Delta H_{\mathcal{X}} = H_{\mathcal{X}}(d) - H_{\mathcal{X}}(d-1)$ has the form

$$\Delta H_{\mathcal{X}} : 1, k, h_2, h_3, \ldots, h_{q+1}, 0, 0, \ldots \text{ with } h_j \geq 1 \quad (j = 2,\ldots,q+1).$$

$H_{\mathcal{X}}(2) \geq k+4$ implies

$$h_2 = H_{\mathcal{X}}(2) - H_{\mathcal{X}}(1) \geq k+4-(k+1) = 3.$$

Furthermore, we have $h_j \geq 2$ for $j = 3,\ldots,q$. If h_j was equal to 1 for some $j \in \{3,\ldots,q\}$, then, by [**7,** Proposition 2.1 c)], also both h_q and h_{q+1} would be equal to 1; by [**7,** Proposition 2.1 d)], there would be a line $L \subseteq \mathbb{P}^k(\mathbb{F}_q)$ with

$$|\mathcal{X} \cap L| \geq r_{\mathcal{X}} + 1 = q + 2 > q + 1 = |L|,$$

(in this context, see also [**6,** Proposition 5.2]), which is absurd.

Hence, we finally get

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

which contradicts our assumptions. Therefore, $r_{\mathcal{X}} \neq q + 1$. $\square_{1.3}$

4. Proof of Proposition 1.5. Similarly to [**8,** 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 Proposition 1.5. From the proof of [**8,** Proposition 1.6 b)], we know that there is an affine complete intersection $\mathcal{X} \subseteq \mathbb{A}^m(\mathbb{F}_q) \subseteq \mathbb{P}^m(\mathbb{F}_q)$ of degree rq^{m-1} and regularity $(m-1)(q-1) + r - 1$; hence,

$$\begin{aligned} s_a(n, q) &\geq s_a(rq^{m-1}, q) \geq r_{\mathcal{X}} \\ &= (m-1)(q-1) + r - 1 \quad \text{for } n \geq rq^{m-1}. \end{aligned}$$

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

$$\{X_1^q, \ldots, X_k^q\} \subseteq J \quad \text{and} \quad \dim_{\mathbb{F}_q} \overline{S} = \deg \mathcal{X} < (r+1)q^{m-1}.$$

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

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 $0 \le \alpha_j \le q-1$ for $j=1,\dots,k$. Then

$$(\alpha_1+1)\cdot\ldots\cdot(\alpha_k+1) \ge (r+1)q^m.$$

This follows from [**8,** Lemma 2.2 b)] and is easily seen anyway.

Assume $\overline{S}_d \neq 0$ for $d=(m-1)(q-1)+r$. By Macaulay's theorem [**1,** Theorem 4.2.3], there is an order ideal $\mathfrak{M}$ of monomials in $\mathbb{F}_q[X_1,\dots,X_k]$ such that the elements $X^\alpha + J$, $X^\alpha \in \mathfrak{M}$ form an $\mathbb{F}_q$-basis of $\overline{S}$. Since $\overline{S}_d \neq 0$ and $\{X_1^q,\dots,X_k^q\} \subseteq J$, there is a monomial $X^\alpha \in \mathfrak{M}$ $(0 \le \alpha_j \le q-1$ for $j=1,\dots,k)$ of degree d. Hence, by Lemma 4.2, $\dim_{\mathbb{F}_q}\overline{S} = |\mathfrak{M}| \ge |\{X^\beta \mid X^\beta \text{ divides } X^\alpha\}| = (\alpha_1+1)\cdot\ldots\cdot(\alpha_k+1) \ge (r+1)q^{m-1}$, a contradiction.

Alternatively, $\overline{S}_d = 0$ by the AU-conjecture [**5,** Conjecture 3.5], which is known to be true for pure powers (see [**2**]). $\square_{1.5}$

5. More general considerations. For $k \ge 1$, $q \ge 2$ (not necessarily a prime power), let $I(k,q) \subseteq \mathbb{Z}[X_0,\dots,X_k]$ be the ideal generated by the 2×2-minors of the matrix $\begin{pmatrix} X_0^q & \dots & X_k^q \\ X_0 & \dots & X_k \end{pmatrix}$.

For instance, if q is a prime power, then $I(k,q)\cdot\mathbb{F}_q[X_0,\dots X_k]$ is the homogenous 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 $l \nmid (q-1)$. 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 $(q^{k+1}-1)/(q-1)$ 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? A simpler problem is: which numbers occur as the regularities of such $\mathcal{X}$ of a given degree n? Find a formula for*

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

And, again, does $s(n,q;K)$ depend on K?

These considerations were suggested by the referee of the paper [**8**] and are motivated by the following results. Analyzing the proof of Theorem 1.3 in [**8**], we see that its statements remain true if one allows q to be an arbitrary integer ≥ 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.

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

REFERENCES

1. W. Bruns and J. Herzog, *Cohen-Macaulay rings*, Cambr. Stud. Adv. Math. **39**, Cambridge University Press, Cambridge, 1993.

2. G.F. Clements and B. Lindström, *A generalization of a combinatorial theorem of Macaulay*, J. Combin. Theor. **7** (1969), 230–238.

3. D. Eisenbud, *The geometry of syzygies*, Grad. Texts Math. **229**, Springer, New York, 2005.

4. D. Eisenbud, M. Green and J. Harris, *Cayley-Bacharach theorems and conjectures*, Bull. Amer. Math. Soc. **33** (1996), 295–324.

5. A.V. Geramita and M. Kreuzer, *On the uniformity of zero-dimensional complete intersections*, J. Algebra **391** (2013), 82–92.

6. A.V. Geramita, P. Maroscia and L.G. Roberts, *The Hilbert function of a reduced k-algebra*, J. Lond. Math. Soc. **28** (1983), 443–452.

7. M. Kreuzer and R. Waldi, *On the Castelnuovo-Mumford regularity of a projective system*, Comm. Alg. **25** (1997), 2919–2929.

8. E. Kunz and R. Waldi, *On the regularity of configurations of $\mathbb{F}_q$-rational points in projective space*, J. Comm. Alg. **5** (2013), 269–280.

Fakultät für Mathematik, Universität Regensburg, D 93040 Regensburg, Germany
Email address: **michael.hellus@mathematik.uni-regensburg.de**

Fakultät für Mathematik, Universität Regensburg, D 93040 Regensburg, Germany
Email address: **rolf.waldi@mathematik.uni-regensburg.de**