JOURNAL OF COMMUTATIVE ALGEBRA
Volume 5, Number 2, Summer 2013

ON THE REGULARITY OF CONFIGURATIONS OF $\mathbf{F}_q$-RATIONAL POINTS IN PROJECTIVE SPACE

E. KUNZ AND R. WALDI

Dedicated to Jürgen Herzog on the occasion of his 70th birthday

ABSTRACT. We are interested in the smallest number $s = s(n, q)$ such that, for any given n distinct $\mathbf{F}_q$-rational points $P_1, \dots, P_n \in \mathbf{P}^{n-1}$, there exists a hypersurface H of degree s and defined over $\mathbf{F}_q$ such that $P_1, \dots, P_{n-1} \in H, P_n \notin H$. Alternately, $s(n, q)$ is the maximal Castelnuovo-Mumford regularity of a set of n $\mathbf{F}_q$-rational points in some projective space. Finally, $s(n, q)$ is the index of stability of certain one-dimensional local Cohen-Macaulay rings.

1. Introduction. Let K be a field and $\mathbf{P}^k(K)$ the set of all K-rational points in the k-dimensional projective space over K $(k \geq 1)$. We consider subsets $\mathfrak{X} \subset \mathbf{P}^k(K)$ with $\deg \mathfrak{X} = |\mathfrak{X}| =: n \geq 1$.

Let $R = K[X_0, \dots, X_k]$ be the polynomial ring over K in the variables $X_0, \dots, X_k$, and let

$$I_{\mathfrak{X}} := (\{F \in R \text{ homogenous} \mid F(P) = 0 \text{ for all } P \in \mathfrak{X}\})$$

be the homogenous vanishing ideal of $\mathfrak{X}$. Then $S := R/I_{\mathfrak{X}}$ is a standard graded ring. The Hilbert function $H_{\mathfrak{X}}$ of $\mathfrak{X}$ is defined as

$$H_{\mathfrak{X}}(d) = \dim_K S_d \quad (d \in \mathbf{N}),$$

where S_d is the homogenous component of degree d of S. As is well known, there is a number $r_{\mathfrak{X}}$, such that $H_{\mathfrak{X}}(d) = n$ for $d \geq r_{\mathfrak{X}}$ and $H_{\mathfrak{X}}(r_{\mathfrak{X}} - 1) < n$. It is called the *regularity* (Castelnuovo-Mumford regularity) of $\mathfrak{X}$. For $0 \leq d \leq r_{\mathfrak{X}}$, the function $H_{\mathfrak{X}}$ is strictly increasing; hence, $r_{\mathfrak{X}} \leq n - 1$.

2010 AMS *Mathematics subject classification.* Primary 14G15.
Keywords and phrases. Castelnuovo-Mumford regularity, rational points in projective spaces over finite fields, Hilbert function, index of stability.
Received by the editors on June 13, 2012, and in revised form on October 31, 2012.
DOI:10.1216/JCA-2013-5-2-269

We are mainly interested in the case where $K = \mathbf{F}_q$ is a finite field with q elements. Systems $\mathfrak{X} \subset \mathbf{P}^k(\mathbf{F}_q)$ play a role, for example, in algebraic coding theory, see [**3, 4**]. We set

$$s(n,q) := \operatorname{Max}\{r_{\mathfrak{X}} \mid \mathfrak{X} \subset \mathbf{P}^k(\mathbf{F}_q) \text{ with } \deg \mathfrak{X} = n \text{ and arbitrary } k \geq 1\}.$$

Obviously, $s(1,q) = 0$. The function $s(n,q)$ has the following geometric description.

1.1. *Remark.* $s(n,q)$ is the smallest number s such that, for any given n distinct points $P_1, \dots, P_n \in \mathbf{P}^{n-1}(\mathbf{F}_q)$, there exists in $\mathbf{P}^{n-1}$ a hypersurface H of degree s and defined over $\mathbf{F}_q$ with $P_1, \dots, P_{n-1} \in H$, $P_n \notin H$.

A simple explanation will be given in Section 5.

About regularity, the following facts are known. Let $\overline{\mathbf{F}_q}$ be the algebraic closure of $\mathbf{F}_q$. Choose in $\overline{S} := \overline{\mathbf{F}_q} \otimes_{\mathbf{F}_q} S$ a homogenous non-zerodivisor z of degree 1. Then

$$\Delta H_{\mathfrak{X}}(d) := H_{\mathfrak{X}}(d) - H_{\mathfrak{X}}(d-1) = \dim_{\overline{\mathbf{F}_q}} \overline{S_d}/z\overline{S}_{d-1} \quad (d \geq 1)$$

and $r_{\mathfrak{X}}$ is the degree of the highest non-vanishing component of $\overline{S}/(z)$.

For $\mathfrak{Y} \subset \mathbf{P}^k(\mathbf{F}_q)$ with $\mathfrak{X} \subset \mathfrak{Y}$ and $|\mathfrak{Y}| = |\mathfrak{X}| + 1$ we have $r_{\mathfrak{X}} \leq r_{\mathfrak{Y}} \leq r_{\mathfrak{X}} + 1$ ([**2**, 2.1e]). This implies

1.2. Lemma. $s(n,q) \leq s(n+1,q) \leq s(n,q) + 1$ $(n \geq 1)$.

We may extend $s(n,q)$ to a step function $s(x,q)$, $x \in \mathbf{R}$, $x \geq 1$, with its jump discontinuities being the $n \in \mathbf{N}$ with $s(n,q) = s(n-1,q) + 1$. By the initial value $s(1,q) = 0$ and the jump discontinuities $a_1 < a_2 < \cdots$, the function s is completely determined:

$$s(x,q) = i \text{ for } x \in \mathbf{R} \text{ with } a_i \leq x < a_{i+1} \quad (i = 1, 2, \dots).$$

In the following let m, r and n always be integers. We shall show

1.3. Theorem. *Assume $m \geq 2$. Then*

a) *For* $x \in \mathbf{R}$ *with* $(q^m - 1)/(q-1) \le x \le 2 \cdot (q^m - 1)/(q-1)$, *we have*

$$s(x, q) = (m-1)(q-1) + 1.$$

b) *For all* r *with* $2 \le r \le q-1$ *and* $x \in \mathbf{R}$ *with* $(r+1)q^{m-1} \le x \le (r+1)(q^m - 1)/(q-1)$, *we have*

$$s(x, q) = (m-1)(q-1) + r.$$

1.4. Corollary. *The following numbers are jump discontinuities of* s:

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

b) $a_{(m-1)(q-1)+1} = (q^m - 1)/(q-1)$ *for* $m = 2, 3, \dots$.

c) *For* $q = 2$, *all jump discontinuities of* s *are given by* a) *and* b). *If* $q \ge 3$, *then in each of the semiopen intervals* $(r(q^m - 1)/(q-1), (r+1)q^{m-1}]$ $(r = 2, \dots, q-1)$ *there is exactly one more jump discontinuity* $a_{(m-1)(q-1)+r}$ $(m = 2, 3, \dots)$. *For* $r = q-1$, *this is* $a_{m(q-1)} = q^m$; *for* $r < q-1$, *its precise locus is unfortunately not known to us.*

Here, statement a) of the corollary follows from Lemma 1.2 and part a) of the theorem for $m = 2$, since $s(q+1, q) = q$. Also observe that, for $r = q-1$, the semi-open interval contains exactly one natural number.

For $q = 2$ and $q = 3$, the corollary catches all jump discontinuities, and s is completely known: If $x \ge 2$, then

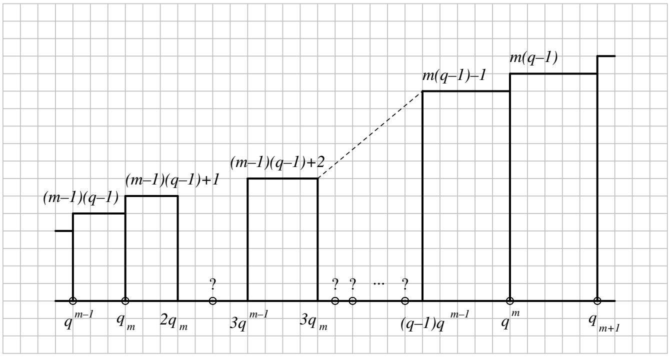
$$s(x, 2) = m \quad \text{for } 2^m - 1 \le x \le 2(2^m - 1) \ [\mathbf{2}]$$

$$s(x, 3) = \begin{cases} 2m - 1 & \text{if } (3^m - 1)/2 \le x < 3^m \\ 2m & \text{if } 3^m \le x < (3^{m+1} - 1)/2. \end{cases}$$

In the general case, from $(m-1)(q-1) + 1 \le s(x, q) \le m(q-1)$ for $(q^m - 1)/(q-1) \le x \le q(q^m - 1)/(q-1)$, it follows that

$$\lim_{x \to \infty} \frac{s(x, q)}{\log_q x} = q - 1,$$

which was conjectured in [**2**].



Set $q_m := (q^m - 1)/(q-1)$. The (symbolic) sketch above illustrates the theorem and its corollary for $q \geq 4$ in the closed interval $[q^{m-1} - 1, q_{m+1} + 1]$. Notice that $(q-1)q_m = q^m - 1$ and $q \cdot q_m = q_{m+1} - 1$. The jump discontinuities are marked by circles.

From Lemma 1.2, it follows that Theorem 1.3 is implied by the following two propositions:

1.5. Proposition. *Let* $m \geq 1$ *and* $1 \leq r \leq q-1$. *Then, for* n *with* $2 \leq n \leq (r+1)(q^m - 1)/(q-1)$,

$$s(n,q) \leq (m-1)(q-1) + r.$$

1.6. Proposition. *Let* $m \geq 1$ *and* $1 \leq r \leq q-1$. *Then*:

a) $s((r+1)q^{m-1}, q) \geq (m-1)(q-1) + r$.

b) $s((q^{m+1} - 1)/(q-1), q) \geq m(q-1) + 1$.

The proof of the propositions will be given in the next three sections.

2. A combinatorial lemma. We need a lemma about the number of certain divisors of monomials. For $X^\alpha = X_0^{\alpha_0} \cdots X_k^{\alpha_k}$, let $|\alpha| := \sum_{i=0}^{k} \alpha_i$ be the degree of X^α and $T_\alpha(d)$ the number of divisors X^β of X^α of degree d.

2.1. Rule. *Let* $\alpha, \gamma, \gamma' \in \mathbf{N}^{k+1}$ *with* $\gcd(X^\alpha, X^\gamma) = \gcd(X^\alpha, X^{\gamma'}) = 1$ *be given. If* $T_{\gamma'}(d) \geq T_\gamma(d)$ *for all* $d \in \mathbf{N}$, *then* $T_{\alpha+\gamma'}(d) \geq T_{\alpha+\gamma}(d)$ *for all* $d \in \mathbf{N}$.

This is a consequence of the formula

$$T_{\alpha+\gamma}(d) = \sum_{\nu=0}^{d} T_\alpha(\nu) T_\gamma(d-\nu) \quad (d \in \mathbf{N}).$$

2.2. Lemma. *Let* $q \geq 2$, $k \geq m \geq 0$, $q-1 \geq r \geq s \geq 1$ *and* $X^\rho := X_0^{q-1} \cdots X_{m-1}^{q-1} X_m^r$ $(\rho = (q-1, \ldots, q-1, r, 0, \ldots, 0) \in \mathbf{N}^{k+1})$. *Then*:

a) *The monomial* X^ρ *has exactly* $(r+1)(q^m-1)/(q-1)+1$ *divisors* X^β *with* $\beta \neq 0$ *and* $|\beta| \equiv s \bmod (q-1)$.

b) *For all* $\alpha \in \mathbf{N}^{k+1}$ *with* $|\alpha| = |\rho|$, $0 \leq \alpha_j \leq q-1$ $(j = 0, \ldots, k)$ *and all* $d \in \mathbf{N}$, *we have* $T_\alpha(d) \geq T_\rho(d)$.

In particular, X^α *has at least* $(r+1)(q^m-1)/(q-1)+1$ *divisors* X^β *with* $\beta \neq 0$ *and* $|\beta| \equiv s \bmod (q-1)$.

Proof. a) Use induction on m. Since, for $m = 0$, the statement is trivial, let $m \geq 1$. By induction hypothesis X^ρ has exactly $(r+1)(q^{m-1}-1)/(q-1)+1$ divisors $X^\beta \neq 1$ with $\beta_0 = 0$ and $|\beta| \equiv s \bmod (q-1)$. The monomial $X_1^{q-1} \cdots X_{m-1}^{q-1} X_m^r$ has $(r+1)q^{m-1}$ divisors $X^{\beta'} = X_1^{\beta_1} \cdots X_m^{\beta_m}$. Associate to each such divisor the divisor $X^\beta = X_0^{\beta_0} X^{\beta'}$ of X^ρ with $\beta_0 \equiv (s - |\beta'|) \bmod (q-1)$, $1 \leq \beta_0 \leq q-1$. Then all divisors $X^\beta \neq 1$ of X^ρ with $|\beta| \equiv s \bmod (q-1)$ and $\beta_0 \neq 0$ are obtained. Altogether, X^ρ has

$$(r+1)\frac{q^{m-1}-1}{q-1} + 1 + (r+1)q^{m-1} = (r+1)\frac{q^m-1}{q-1} + 1$$

such divisors.

b) Let $\alpha \in \mathbf{N}^{k+1}$ with $|\alpha| = m(q-1)+r$, $0 \leq \alpha_j \leq q-1$ for $j = 0, \ldots, k$ be given. Since T_α does not change, if we change the order of entries of α, it suffices to prove assertion b) for the $(k+1)$-tuples of the set

$$N := \{\alpha \in \mathbf{N}^{k+1} \mid q-1 \geq \alpha_0 \geq \cdots \geq \alpha_k \geq 0,\ |\alpha| = m(q-1)+r\}.$$

We use descending induction with respect to the lexicographic ordering $\geq_{\text{lex}}$ of N. We have $\rho = \text{Max}_{\text{lex}}(N)$, and b) trivially holds for $X^\alpha = X^\rho$.

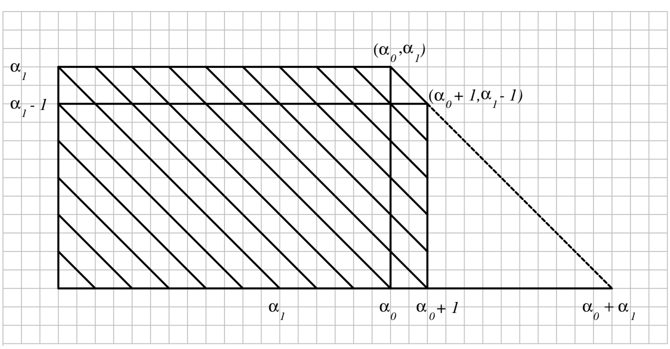
Now consider $\alpha \in N$ with $X^\alpha \neq X^\rho$, and let b) be proved for all $\beta \in N$ with $\rho \geq_{\text{lex}} \beta >_{\text{lex}} \alpha$. Since $\alpha <_{\text{lex}} \rho$, we have $k \geq 1$. In order to show $T_\alpha \geq T_\rho$, it suffices, thanks to Rule 2.1, to take only those exponents in X^α and X^ρ into regard which are distinct. Therefore, we may assume that $\alpha_j \neq \rho_j$ for $j = 0, \ldots, k$. Then $q-1 > \alpha_0 \geq \cdots \geq \alpha_k \geq 1$, $k \geq 1$, since from $\alpha_k = 0$ it would follow that $m(q-1) + r = \alpha_0 + \cdots + \alpha_{k-1} \leq k(q-1)$, $k > m$ and $\rho_k = \alpha_k$.

Replacing α by $\alpha' := (\alpha_0 + 1, \alpha_1, \ldots, \alpha_{k-1}, \alpha_k - 1)$, we also have $\alpha' \in N$. Further, $\rho \geq_{\text{lex}} \alpha' >_{\text{lex}} \alpha$. By induction hypothesis $T_{\alpha'} \geq T_\rho$. Thus, we have to show $T_\alpha \geq T_{\alpha'}$. Since α' and α differ only at their first and last entry, we can assume by Rule 2.1 that $k = 1$, i.e., that $\alpha' = (\alpha_0 + 1, \alpha_1 - 1)$, $\alpha = (\alpha_0, \alpha_1)$ with $q - 1 > \alpha_0 \geq \alpha_1 \geq 1$ and $q - 1 \geq \alpha_0 + 1 > \alpha_1 - 1 \geq 0$.

Quite generally, for $\beta = (\beta_0, \beta_1) \in \mathbf{N}^2$ with $\beta_0 \geq \beta_1$, we have

$$T_\beta(d) = \begin{cases} d+1 & \text{for } 0 \leq d \leq \beta_1 \\ \beta_1 + 1 & \text{for } \beta_1 \leq d \leq \beta_0 \\ \beta_0 + \beta_1 - d + 1 & \text{for } \beta_0 \leq d \leq \beta_0 + \beta_1 \\ 0 & \text{for } d > \beta_0 + \beta_1 \end{cases}$$

and $T_\alpha(d) \geq T_{\alpha'}(d)$ follows. □



3. Proof of Proposition 1.5. For $\mathfrak{X} \subset \mathbf{P}^k(\mathbf{F}_q)$ with $\deg \mathfrak{X} = n$, $2 \leq n \leq (r+1)(q^m-1)/(q-1)$ and $1 \leq r \leq q-1$, we have to show the estimation $r_{\mathfrak{X}} \leq (m-1)(q-1)+r$.

In $R = \mathbf{F}_q[X_0, \dots, X_k]$, we consider the homogenous vanishing ideal $I_{\mathfrak{X}}$ of $\mathfrak{X}$ and the ideal $I := (\{F^q - F\}_{F \in R}) = (\{X_i^q - X_i\}_{i=0,\dots,k})$. Set $T_{\mathfrak{X}} := R/I_{\mathfrak{X}} + I$, and let x_i denote the image of X_i in $T_{\mathfrak{X}}$ ($i = 0, \dots, k$).

3.1. *Remark.* For $d \in \mathbf{N}$, the canonical map $\varphi : R_d \to T_{\mathfrak{X}}$ has kernel $(I_{\mathfrak{X}})_d$, i.e.,

$$H_{\mathfrak{X}}(d) = \dim_{\mathbf{F_q}} \varphi(R_d).$$

Moreover, $\varphi(R_{d+1}) \subset \varphi(R_{d+q})$.

Proof. Clearly, $(I_{\mathfrak{X}})_d \subset \ker \varphi$. Let $F \in R_d$ and $\varphi(F) = 0$; hence, $F = G + H$ ($G \in I_{\mathfrak{X}}, H \in I$). Then, for all $P \in \mathfrak{X}$, it follows that $F(P) = G(P) + H(P) = 0$; hence, $F \in (I_{\mathfrak{X}})_d$. The second assertion follows from $x_i^q = x_i$ for $i = 0, \dots, k$.

Set $V_d := \varphi(R_d)$. We have $V_{(m-1)(q-1)+r} \subset V_{m(q-1)+r}$. As $H_{\mathfrak{X}}$ is increasing, it suffices to show the equality of the vector spaces, that is, $x^\alpha \in V_{(m-1)(q-1)+r}$, if $|\alpha| = m(q-1)+r$ and $0 \leq \alpha_j \leq q-1$ ($j = 0, \dots, k$).

Assume there exists such an α with $x^\alpha \notin V_{(m-1)(q-1)+r}$. Choose α maximal with respect to $\geq_{\text{lex}}$. Since $|\alpha| = m(q-1)+r$, $0 \leq \alpha_j \leq q-1$, we have $k \geq m$, and we can apply Lemma 2.2 b).

Set $\mathfrak{T}(\alpha) := \{\beta \in \mathbf{N}^{k+1} | \beta \neq 0,\ X^\beta | X^\alpha \text{ and } |\beta| \equiv |\alpha| \bmod (q-1)\}$. By the lemma, we have $|\mathfrak{T}(\alpha)| \geq (r+1)(q^m-1)/(q-1) + 1 > |\mathfrak{X}|$, but $\dim_{\mathbf{F}_q} V_{m(q-1)+r} = H_{\mathfrak{X}}(m(q-1)+r) \leq |\mathfrak{X}|$. Thus, the family x^β, $\beta \in \mathfrak{T}(\alpha)$ of vectors from $V_{m(q-1)+r}$ is linearly dependent over $\mathbf{F}_q$. Hence, there is a relation

$$x^\beta = \sum_\gamma \lambda_\gamma x^\gamma \quad \text{with } \lambda_\gamma \in \mathbf{F}_q \quad (\beta \in \mathfrak{T}(\alpha)),$$

where the summation is over the $\gamma \in \mathfrak{T}(\alpha)$ with $|\gamma| \leq |\beta|$ and $\gamma >_{\text{lex}} \beta$, if $|\gamma| = |\beta|$. Multiplying both sides by $x^{\alpha-\beta}$ gives a relation

$$x^\alpha = \sum_{\gamma'} \mu_{\gamma'} x^{\gamma'} \quad (\mu_{\gamma'} \in \mathbf{F}_q) \tag{3.2}$$

with summation over the γ' with $\gamma' \in \mathbf{N}^{k+1} \setminus \{0\}$, $|\gamma'| \le |\alpha|$, $|\gamma'| \equiv |\alpha| \bmod (q-1)$ and $\gamma' >_{\text{lex}} \alpha$, if $|\gamma'| = |\alpha|$.

a) If $|\gamma'| < |\alpha|$, $|\gamma'| \equiv |\alpha| \bmod (q-1)$, then $x^{\gamma'} \in V_{(m-1)(q-1)+r}$.

b) If $|\gamma'| = |\alpha|$ and $\gamma'_j \ge q$ for some $j \in \{0, \dots, k\}$, then since $x_j^q = x_j$, we likewise have $x^{\gamma'} \in V_{(m-1)(q-1)+r}$.

c) If $|\gamma'| = |\alpha|$, $\gamma' >_{\text{lex}} \alpha$ and $0 \le \gamma'_j \le q-1$ $(j = 0, \dots, k)$, then by the choice of α again $x^{\gamma'} \in V_{(m-1)(q-1)+r}$.

From (3.2), it follows that $x^\alpha \in V_{(m-1)(q-1)+r}$, a contradiction. □

4. Regularity in special cases and proof of Proposition 1.6. Let $S_i \subset \mathbf{F}_q$ with $|S_i| = r_i + 1$ be given $(i = 1, \dots, k)$, and let

$$\mathfrak{X} := S_1 \times \cdots \times S_k \subset \mathbf{F}_q^k \subset \mathbf{P}^k(\mathbf{F}_q),$$

where we identify $(a_1, \dots, a_k) \in \mathfrak{X}$ with $\langle 1, a_1, \dots, a_k \rangle \in \mathbf{P}^k(\mathbf{F}_q)$. Then $I_{\mathfrak{X}} = (\{F_1, \dots, F_k\})$ with $F_i := \prod_{a \in S_i}(X_i - aX_0)$ $(i = 1, \dots, k)$ is the homogenous vanishing ideal of $\mathfrak{X}$ and

$$\begin{aligned} R/I_{\mathfrak{X}} + (X_0) &= \mathbf{F}_q[X_1, \dots, X_k]/(X_1^{r_1+1}, \dots, X_k^{r_k+1}) \\ &= \bigotimes_{i=1}^{k} \mathbf{F}_q[X_i]/(X_i^{r_i+1}). \end{aligned}$$

Therefore,

$$r_{\mathfrak{X}} = \sum_{i=1}^{k} r_i.$$

In particular, for $\mathfrak{X} = \mathbf{F}_q^k$, we have $r_{\mathfrak{X}} = k(q-1)$.

For the proof of Proposition 1.6 a), we choose for $S_1 \subset \mathbf{F}_q$ a set of $r+1$ elements, and set $S_i = \mathbf{F}_q$ $(i = 2, \dots, k)$. Then $\deg \mathfrak{X} = (r+1)q^{k-1}, r_{\mathfrak{X}} = (k-1)(q-1) + r$, and it follows that

$$s((r+1)q^{k-1}, q) \ge (k-1)(q-1) + r \quad (r = 1, \dots, q-1).$$

For the proof of Proposition 1.6 b), consider $\mathfrak{X} := \mathbf{P}^k(\mathbf{F}_q)$ and, as in Section 3, the ring $T_{\mathfrak{X}} = R/I_{\mathfrak{X}} + I$ with $I = (\{X_i^q - X_i\}_{i=0,\dots,k})$.

Further, let

$$T := R/I = \bigotimes_{i=0}^{k} \mathbf{F}_q[X_i]/(X_i^q - X_i) = \bigoplus_{0\le\alpha_i\le q-1} \mathbf{F}_q x_0^{\alpha_0}\cdots x_k^{\alpha_k}$$

with $x_i := X_i + I$ $(i = 0, \dots, k)$. As an $\mathbf{F}_q$-vector space, we identify T with the subspace of R generated by the monomials $X^\alpha = X_0^{\alpha_0}\cdots X_k^{\alpha_k}$ $(0 \le \alpha_i \le q-1)$.

4.1. Lemma. *We have $I_{\mathfrak{X}} \subset I$; hence, $T_{\mathfrak{X}} = T$.*

Proof. Obviously, I is the vanishing ideal of $\mathbf{F}_q^{k+1}$, and hence $I_{\mathfrak{X}} \subset I$.

Write $T = \mathbf{F}_q \oplus \bigoplus_{s=1}^{q-1} T_s$, with

$$T_s := \langle\{X^\alpha \mid \alpha \ne 0,\ 0 \le \alpha_i \le q-1 \text{ and } |\alpha| \equiv s \bmod (q-1)\}\rangle.$$

Lemma 2.2 a) with $r = q-1$ implies

$$\dim_{\mathbf{F}_q} T_s = q\frac{q^k-1}{q-1} + 1 = \frac{q^{k+1}-1}{q-1} \quad (s = 1, \dots, q-1).$$

The canonical epimorphism $\varphi : R \to T$ maps $R_{k(q-1)+s}$ into T_s. By Remark 3.1, we have $H_{\mathfrak{X}}(k(q-1)+s) = \dim_{\mathbf{F}_q}\varphi(R_{k(q-1)+s})$ and $\varphi(R_{k(q-1)+s}) = \sum_{j=0}^{k}\varphi(R_{j(q-1)+s}) = T_s$. Thus,

$$H_{\mathfrak{X}}(k(q-1)+s) = \frac{q^{k+1}-1}{q-1} \quad (s = 1, \dots, q-1).$$

On the other hand, $\varphi : R_{k(q-1)} \to T_{q-1}$ is not surjective, since the monomial $X_0^{q-1}\cdots X_k^{q-1} \in T_{q-1}$ has no preimage in $R_{k(q-1)}$. Therefore,

$$H_{\mathfrak{X}}(k(q-1)) < \frac{q^{k+1}-1}{q-1},$$

and consequently $r_{\mathfrak{X}} = k(q-1)+1$. Since $\deg\mathfrak{X} = (q^{k+1}-1)/(q-1)$, we obtain

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

what we had to show in Proposition 1.6 b). ◻

Remark. For a complete description of $H_{\mathfrak{X}}$, see, for example, [**3**].

5. Alternate views. Now let K be an arbitrary field. In this section we use the following description of the Hilbert function $H_{\mathfrak{X}}$ for $\mathfrak{X} \subset \mathbf{P}^k(K), \mathfrak{X} = \{P_1, \dots, P_n\}$ where the P_i are not necessarily distinct.

5.1. *Remark.* Let $P_i = \langle a_{i0}, \dots, a_{ik} \rangle$ $(i = 1, \dots, n)$. For $l \in \mathbf{N}$, let $\varphi_l : R_l \to K^n$ be the linear map given by $F \mapsto (F(P_1), \dots, F(P_n))$, where $F(P_i) = F(a_{i0}, \dots, a_{ik})$ $(i = 1, \dots, n)$. Then $H_{\mathfrak{X}}(l) = \dim_K(\operatorname{im} \varphi_l)$. Here $\operatorname{im} \varphi_1 =: V$ is the vector space spanned by columns of the matrix $(a_{ij})_{i=1,\dots,n, j=0,\dots,k}$, and $V^{(l)} := \operatorname{im} \varphi_l$ is generated by all vectors $v_1 \cdots v_l$ with $v_j \in V$ $(j = 1, \dots, l)$, where the multiplication of the vectors is performed componentwise.

These assertions are clear since $(I_{\mathfrak{X}})_l = \ker \varphi_l$.

Remark 1.1 asks for which s to given distinct points $P_1, \dots, P_n \in \mathbf{P}^{n-1}(\mathbf{F}_q)$ there exist polynomials $F_1, \dots, F_n \in R_s$ with $F_i(P_j) = \delta_{ij}$ $(i, j = 1, \dots, n)$? By Remark 5.1, this is equivalent to $H_{\mathfrak{X}}(s) = n$, which is correct for $s \geq s(n, q)$ and false for $s < s(n, q)$.

There is also a connection between the function $s(n, q)$ and the index of stability of certain one-dimensional local Cohen-Macaulay rings. If $(R, \mathfrak{m})$ is such a ring and $\mathfrak{a}$ an $\mathfrak{m}$-primary ideal, then $\mathfrak{a}$ is called *stable* if there exists an $x \in \mathfrak{a}$ such that $\mathfrak{a}^2 = x\mathfrak{a}$. For large l, the ideal $\mathfrak{a}^l$ is always stable, and one defines $r(\mathfrak{a}) := \operatorname{Min}\{l \in \mathbf{N}_+ | \mathfrak{a}^l \text{ is stable}\}$. The number $s(R) := \sup\{r(\mathfrak{a}) \mid \mathfrak{a}\ \mathfrak{m}\text{-primary}\}$ is called the *index of stability* of R. See [**1**] for numerous references, assertions and examples about the index of stability.

In the following, let $P = K[[Y_1, \dots, Y_n]]$ be the formal power series ring over K in the variables $Y_1, \dots, Y_n$. Set $I := (\{Y_i Y_j\}_{1 \leq i < j \leq n})$, and let $Q_n := P/I$ be the completion of the local ring at the origin of the curve in $\mathbf{A}^n$ which is the union of the coordinate axes. Let y_i be the image of Y_i in Q_n and $\mathfrak{m}$ the maximal ideal of Q_n.

5.2. Proposition. *Let $\alpha := (\alpha_1, \dots, \alpha_n) \in \mathbf{N}_+^n$ and $V \subset K^n$ be a linear subspace of dimension d which is not contained in a coordinate hyperplane. Then*:

a) *The elements $a_1 y_1^{\alpha_1} + \dots + a_n y_n^{\alpha_n}$ with $(a_1, \dots, a_n) \in V$ generate an $\mathfrak{m}$-primary ideal $\mathfrak{a}$ in Q_n.*

b) *If the vectors* $(a_{1j}, \dots, a_{nj})$ $(j = 1, \dots, d)$ *form a basis of* V, *then the elements* $a_{1j}y_1^{\alpha_1} + \cdots + a_{nj}y_n^{\alpha_n}$ $(j = 1, \dots, d)$ *form a minimal system of generators of* $\mathfrak{a}$. *In particular,* $\mu(\mathfrak{a}) = \dim_K \mathfrak{a}/\mathfrak{m}\alpha = \dim_K V$.

c) *If* V *contains the* i*th unit vector* $e_i = (0, \dots, 1, \dots, 0)$ *for some* $i \in \{1, \dots, n\}$, *then* α_i *is the smallest number such that* $y_i^{\alpha_i} \in \mathfrak{a}$. *Otherwise* $\alpha_i + 1$ *is the smallest such number.*

Proof. Choose for $i \in \{1, \dots, n\}$ a vector $(a_1, \dots, a_n) \in V$ with $a_i \neq 0$. Then $y_i \sum_{j=1}^n a_j y_j^{\alpha_j} = a_i y_i^{\alpha_i+1} \in \mathfrak{a}$, and hence $\mathfrak{a}$ is $\mathfrak{m}$-primary. If $e_i \in V$, then already $y_i^{\alpha_i} \in \mathfrak{a}$. The assertions of the proposition follow easily. □

Write $\mathfrak{a} =: \mathfrak{a}(\alpha, V)$ if $\mathfrak{a}$ is an ideal as in Proposition 5.2 a).

5.3. Proposition. *Any* $\mathfrak{m}$*-primary ideal* $\mathfrak{a}$ *of* Q_n *has the form* $\mathfrak{a} = \mathfrak{a}(\alpha, V)$ *with* α *and* V *as in Proposition* 5.2.

Proof. For an $\mathfrak{m}$-primary ideal $\mathfrak{a}$ of Q_n and any $i \in \{1, \dots, n\}$, there is a smallest number $\alpha_i \in \mathbf{N}_+$ such that $y_i^{\alpha_i} \in \mathfrak{a} + (y_1, \dots, y_{i-1}, y_{i+1}, \dots, y_n)$. Therefore, $y_i^{\alpha_i+1} \in \mathfrak{m}a$, and any $f \in \mathfrak{a}$ can be written $f = \sum_{i=1}^n f_i$ with $f_i \in y_i^{\alpha_i} K[[y_i]]$, i.e., $f \equiv \sum_{i=1}^n a_i y_i^{\alpha_i} \bmod \mathfrak{m}a$ with $a_1, \dots, a_n \in K$. By Nakayama's lemma, the assertion follows. □

If $\mathfrak{a}$ is a principal ideal, then $\mathfrak{a}$ is stable and $r(\mathfrak{a}) = 1$. Therefore, we assume in the following that $\dim V := k+1 \geq 2$. Then we also have only to consider the case $n \geq 2$. For $\mathfrak{a} = \mathfrak{a}(\alpha, V)$ we have $\mathfrak{a}^l = \mathfrak{a}(l\alpha, V^{(l)})$ where, as above, $V^{(l)}$ is the vector space spanned by all $v_1 \cdots v_l$ with $v_i \in V$ and componentwise multiplication.

Now choose a basis $v_j = (a_{1j}, \dots, a_{nj})$ $(j = 0, \dots, k)$ of V, and consider the points $P_i = \langle a_{i0}, \dots, a_{ik} \rangle \in \mathbf{P}^k(K)$ $(i = 1, \dots, n)$ corresponding to the rows of the matrix $(a_{ij})_{i=1,\dots,n, j=0,\dots,k}$. For $\mathfrak{X} := \{P_1, \dots, P_n\}$ and $\mathfrak{a} = \mathfrak{a}(\alpha, V)$, Remark 5.1 implies that $\dim V^{(l)} = H_{\mathfrak{X}}(l) = \mu(\mathfrak{a}^l)$. In particular,

$$\dim V = \dim V^{(1)} < \dim V^{(2)} < \cdots < \dim V^{(r_{\mathfrak{X}})} = \dim V^{(l)} = \deg \mathfrak{X} \leq n$$

for $l \geq r_{\mathfrak{X}}$.

5.4. Proposition. $r(\mathfrak{a}) = r_{\mathfrak{X}}$.

Proof. For $1 \leq l < r_{\mathfrak{X}}$, we have $\mu(\mathfrak{a}^l) = \dim V^{(l)} < \dim V^{(2l)} = \mu(\mathfrak{a}^{2l})$; hence, $\mathfrak{a}^l$ is not stable.

Conversely, we can assume that $\mathfrak{X} = \{P_1, \dots, P_{n'}\}$, $\deg \mathfrak{X} = n' \le n$. By Remark 5.1, there is an $F \in R_{r_\mathfrak{X}}$ with $F(P_i) = 1$ for $i = 1, \dots, n'$. Then $v := (F(P_1), \dots, F(P_n)) \in V^{(r_\mathfrak{X})}$ and $F(P_i) \neq 0$ for $i = 1, \dots, n$. Since $\dim V^{(r_\mathfrak{X})} = \dim V^{(2r_\mathfrak{X})}$, we obtain $V^{(2r_\mathfrak{X})} = v \cdot V^{(r_\mathfrak{X})}$, and with $x := \sum_{i=1}^n F(P_i) y_i^{r_\mathfrak{X}\alpha_i}$, it follows that $(\mathfrak{a}^{r_\mathfrak{X}})^2 = x \cdot \mathfrak{a}^{r_\mathfrak{X}}$, i.e., $\mathfrak{a}^{r_\mathfrak{X}}$ is stable, $r(\mathfrak{a}) = r_\mathfrak{X}$.

If K is an infinite field one can choose pairwise distinct $a_1, \dots, a_n \in K$. For the vector space V generated by $(1, \dots, 1)$ and $(a_1, \dots, a_n)$, we have by van der Monde that $\dim_K V^{(l)} = l + 1$ for $l = 1, \dots, n-1$ and $\dim_K V^{(l)} = n$ for $l \ge n$. For $\mathfrak{a} = \mathfrak{a}(\alpha, V)$ with any $\alpha \in \mathbf{N}_+^n$, we obtain $r(\mathfrak{a}) = n - 1$; hence, $s(Q_n) = n - 1 = m(Q_n) - 1$, where $m(Q_n)$ denotes the multiplicity of Q_n.

For $K = \mathbf{F}_q$ the situation is quite different. Proposition 5.4 implies that, in this case, $s(Q_n) = s(n, q)$, so that Theorem 1.3 and its conclusions can also be applied to the index of stability $s(Q_n)$. In particular, we have

$$\lim_{n\to\infty} \frac{s(Q_n)}{\log_q n} = q - 1. \qquad \square$$

Acknowledgments. We are grateful to Helmut Knebl for his support and to the referee for his ideas for possible generalizations.

REFERENCES

1. J. Herzog and R. Waldi, *A note on the Hilbert function of a one-dimensional Cohen-Macaulay ring*, Manuscr. Math. **16** (1975), 251–260.

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

3. A.B. Sorensen, *Projective Reed-Muller codes*, IEEE Trans. Inf. Theor. **37** (1991), 1567–1576.

4. M. Tsfasman, S. Vladut and D. Nogin, *Algebraic-geometric codes*: *Basic notions*, Math. Surv. Mono. **139**, American Mathematical Society, Providence, R.I., 2007.

Fakultät für Mathematik, Universität Regensburg, D 93040 Regensburg, Germany
Email address: ernst.kunz@mathematik.uni-regensburg.de

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