Advances in Mathematics of Communications
Volume 6, No. 1, 2012, 69–94

doi:10.3934/amc.2012.6.69

SINGULARITIES OF SYMMETRIC HYPERSURFACES AND REED–SOLOMON CODES

Antonio Cafure

Instituto del Desarrollo Humano, Universidad Nacional de General Sarmiento
J.M. Gutiérrez 1150, Los Polvorines (B1613GSX) Buenos Aires, Argentina
and
Ciclo Básico Común, Universidad de Buenos Aires
Ciudad Universitaria, Pabellón III (1428) Buenos Aires, Argentina
and
National Council of Research and Technology (CONICET)
Buenos Aires, Argentina

Guillermo Matera and Melina Privitelli

Instituto del Desarrollo Humano, Universidad Nacional de General Sarmiento
J.M. Gutiérrez 1150, Los Polvorines (B1613GSX) Buenos Aires, Argentina
and
National Council of Research and Technology (CONICET)
Buenos Aires, Argentina

(Communicated by Iwan Duursma)

Abstract. We determine conditions on q for the nonexistence of deep holes of the standard Reed–Solomon code of dimension k over $\mathbb{F}_q$ generated by polynomials of degree $k+d$. Our conditions rely on the existence of q–rational points with nonzero, pairwise–distinct coordinates of a certain family of hypersurfaces defined over $\mathbb{F}_q$. We show that the hypersurfaces under consideration are invariant under the action of the symmetric group of permutations of the coordinates. This allows us to obtain critical information concerning the singular locus of these hypersurfaces, from which the existence of q–rational points is established.

1. Introduction

Let $\mathbb{F}_q$ be the finite field of q elements of characteristic p, let $\overline{\mathbb{F}}_q$ denote its algebraic closure and let $\mathbb{F}_q^*$ denote the group of units of $\mathbb{F}_q$. Let $\mathbb{F}_q[T]$ and $\mathbb{F}_q[X_1,\ldots,X_n]$ denote the rings of univariate and n-variate polynomials with coefficients in $\mathbb{F}_q$, respectively.

Given a subset $\mathsf{D} := \{x_1,\ldots,x_n\} \subset \mathbb{F}_q$ and a positive integer $k \le n$, the Reed–Solomon code of length n and dimension k over $\mathbb{F}_q$ is the following subset of $\mathbb{F}_q^n$:

$$C(\mathsf{D},k) := \{(f(x_1),\ldots,f(x_n)) : f \in \mathbb{F}_q[T],\ \deg f \le k-1\}.$$

The set D is called the evaluation set and the elements of $C(\mathsf{D},k)$ are called codewords of the code. When $\mathsf{D} = \mathbb{F}_q^*$, we say that $C(\mathsf{D},k)$ is the standard Reed–Solomon code.

2000 *Mathematics Subject Classification:* Primary: 11G25, 14G15; Secondary: 14G50,05E05.

Key words and phrases: Finite fields, Reed–Solomon codes, deep holes, symmetric polynomials, singular hypersurfaces, rational points.

The authors were partially supported by the grants UNGS 30/3084, PIP 11220090100421 CONICET, MTM 2007-62799.

Let $C := C(\mathsf{D}, k)$. For $\mathbf{w} \in \mathbb{F}_q^n$, we define the distance of $\mathbf{w}$ to the code C as

$$\mathsf{d}(\mathbf{w}, C) := \min_{\mathbf{c}\in C} \mathsf{d}(\mathbf{w}, \mathbf{c}),$$

where d is the Hamming distance of $\mathbb{F}_q^n$. The minimum distance $\mathsf{d}(C)$ of C is the shortest distance between any two distinct codewords. The covering radius of C is defined as

$$\rho := \max_{\mathbf{y}\in\mathbb{F}_q^n} \mathsf{d}(\mathbf{y}, C).$$

It is well–known that $\mathsf{d}(C) = n - k + 1$ and $\rho = n - k$ hold. Finally, we say that a "word" $\mathbf{w} \in \mathbb{F}_q^n$ is a deep hole if $\mathsf{d}(\mathbf{w}, C) = \rho$ holds.

A decoding algorithm for the code C receives a word $\mathbf{w} \in \mathbb{F}_q^n$ and outputs the message, namely the codeword that is most likely to be received as $\mathbf{w}$ after transmission, roughly speaking. One of the most important algorithmic problems in this setting is that of the *maximum–likelihood decoding*, which consists in computing the closest codeword to any given word $\mathbf{w} \in \mathbb{F}_q^n$. It is well–known that the maximum–likelihood decoding problem for Reed–Solomon codes is NP-complete ([10]; see also [4]).

Suppose that we receive a word $\mathbf{w} := (w_1, \dots, w_n) \in \mathbb{F}_q^n$. Solving the maximum–likelihood decoding for $\mathbf{w}$ amounts at finding a polynomial $f \in \mathbb{F}_q[T]$ of degree at most $k-1$ satisfying the largest number of conditions $f(x_i) = w_i$, $1 \le i \le n$. By interpolation, there exists a unique polynomial $f_{\mathbf{w}}$ of degree at most $n-1$ such that $f_{\mathbf{w}}(x_i) = w_i$ holds for $1 \le i \le n$. In this case, we say that the word $\mathbf{w}$ was generated by the polynomial $f_{\mathbf{w}}$. If $\deg f_{\mathbf{w}} \le k-1$, then $\mathbf{w}$ is a codeword.

In this paper our main concern will be the existence of deep holes of the given Reed–Solomon code C. According to our previous remarks, a deep hole can only arise as the word generated by a polynomial $f \in \mathbb{F}_q[T]$ with $k \le \deg f \le n-1$. In this sense, we have the following result.

Proposition 1.1 ([4, Corollary 1])**.** *Polynomials of degree k generate deep holes.*

Next we reduce further the set of polynomials $f \in \mathbb{F}_q[T]$ which are candidates for generating deep holes. Suppose that we receive a word $\mathbf{w} \in \mathbb{F}_q^n$, which is generated by a polynomial $f_{\mathbf{w}} \in \mathbb{F}_q[T]$ of degree greater than k. We want to know whether $\mathbf{w}$ is a deep hole. We can decompose $f_{\mathbf{w}}$ as a sum $f_{\mathbf{w}} = g + h$, where g consists of the sum of the monomials of $f_{\mathbf{w}}$ of degree greater than or equal to k and h consists of those of degree less than or equal to $k-1$.

Remark 1.2. Let $\mathbf{w}_g$ and $\mathbf{w}_h$ be the words generated by g and h respectively. Observe that $\mathbf{w}_h$ is a codeword. Let $\mathbf{u} \in C$ be a codeword with $\mathsf{d}(\mathbf{w}, \mathbf{u}) = \mathsf{d}(\mathbf{w}, C)$. From the identities

$$\mathsf{d}(\mathbf{w}, C) = \mathsf{d}(\mathbf{w}, \mathbf{u}) = \mathsf{d}(\mathbf{w} - \mathbf{w}_h, \mathbf{u} - \mathbf{w}_h) = \mathsf{d}(\mathbf{w}_g, \mathbf{u} - \mathbf{w}_h)$$

and the fact that $\mathbf{u} - \mathbf{w}_h \in C$ holds, we conclude

$$\mathsf{d}(\mathbf{w}_g, C) \le \mathsf{d}(\mathbf{w}, C).$$

On the other hand, for $\mathbf{u}' \in C$ with $\mathsf{d}(\mathbf{w}_g, C) = \mathsf{d}(\mathbf{w}_g, \mathbf{u}')$, we have

$$\mathsf{d}(\mathbf{w}_g, C) = \mathsf{d}(\mathbf{w}_g, \mathbf{u}') = \mathsf{d}(\mathbf{w}_g + \mathbf{w}_h, \mathbf{u}' + \mathbf{w}_h) = \mathsf{d}(\mathbf{w}, \mathbf{u}' + \mathbf{w}_h) \ge \mathsf{d}(\mathbf{w}, C).$$

Therefore we have $\mathsf{d}(\mathbf{w}, C) = \mathsf{d}(\mathbf{w}_g, C)$. Hence $\mathbf{w}$ is a deep hole if and only if $\mathbf{w}_g$ is a deep hole.

From Remark 1.2 it follows that any deep hole of the Reed–Solomon code C is obtained as the word $\mathbf{w}_f$ generated by a polynomial $f \in \mathbb{F}_q[T]$ of the form

$$f := T^{k+d} + f_{d-1}T^{k+d-1} + \cdots + f_0T^k, \tag{1}$$

where d is a nonnegative integer with $k+d < q-1$. In view of Proposition 1.1, we shall only discuss the case $d \geq 1$.

From now on we shall consider the standard Reed–Solomon code $C := C(\mathbb{F}_q^*, k)$. In [4] it is conjectured that the reciprocal of Proposition 1.1 also holds, namely a word $\mathbf{w}$ is a deep hole of C if and only if it is generated by a polynomial $f \in \mathbb{F}_q[T]$ of degree k. Furthermore, the existence of deep holes of C is related to the nonexistence of q–rational points, namely points whose coordinates belong to $\mathbb{F}_q$, of a certain family of hypersurfaces, in the way that we now explain. Fix $f \in \mathbb{F}_q[T]$ as in (1) and let $\mathbf{w}_f$ be the generated word. Let $X_1, \ldots, X_{k+1}$ be indeterminates over $\overline{\mathbb{F}}_q$ and let $Q \in \mathbb{F}_q[X_1, \ldots, X_{k+1}][T]$ be the polynomial

$$Q = (T - X_1) \cdots (T - X_{k+1}).$$

We have that there exists $R_f \in \mathbb{F}_q[X_1, \ldots, X_{k+1}][T]$ with $\deg R_f \leq k$ such that the following relation holds:

$$f \equiv R_f \mod Q. \tag{2}$$

Assume that R_f has degree k and denote by $H_f \in \mathbb{F}_q[X_1, \ldots, X_{k+1}]$ its leading coefficient. Suppose that there exists a vector $\mathbf{x} \in (\mathbb{F}_q^*)^{k+1}$ with pairwise–distinct coordinates such that $H_f(\mathbf{x}) = 0$ holds. This implies that $r := R_f(\mathbf{x}, T)$ has degree at most $k-1$ and hence generates a codeword $\mathbf{w}_r$. By (2) we deduce that

$$d(\mathbf{w}_f, C) \leq d(\mathbf{w}_f, \mathbf{w}_r) \leq q - k - 2$$

holds, and thus $\mathbf{w}_f$ is not a deep hole.

As a consequence, we see that the given polynomial f does not generate a deep hole of C if and only if there exists a zero $\mathbf{x} := (x_1, \ldots, x_{k+1}) \in \mathbb{F}_q^{k+1}$ of H_f with nonzero, pairwise–distinct coordinates, namely a solution $\mathbf{x} \in \mathbb{F}_q^{k+1}$ of the following system of equalities and non-equalities:

$$H_f(X_1, \ldots, X_{k+1}) = 0, \quad \prod_{1 \leq i < j \leq k+1} (X_i - X_j) \neq 0, \quad \prod_{1 \leq i \leq k+1} X_i \neq 0. \tag{3}$$

1.1. Related work.

As explained before, in [4] the nonexistence of deep holes of the standard Reed–Solomon code C is reduced to the existence of q–rational points, namely points whose coordinates belong to $\mathbb{F}_q$, with nonzero, pairwise–distinct coordinates of the hypersurfaces V_f defined by the family of polynomials H_f of (3), where f runs through the set of polynomials $f \in \mathbb{F}_q[T]$ as in (1). The authors prove that all the hypersurfaces V_f are absolutely irreducible. This enables them to apply the explicit version of the Lang–Weil estimate of [3] in order to obtain sufficient conditions for the nonexistence of deep holes of Reed–Solomon codes. More precisely, the following result is obtained.

Theorem 1.3 ([4, Theorem 1])**.** *Let k, d be given positive integers and suppose that q is a prime number. If $q > \max\{k^{4+\epsilon}, d^{13/3+\epsilon}\}$ holds, then no word $\mathbf{w}_f$ generated by a polynomial $f \in \mathbb{F}_q[T]$ of degree $k+d < q-1$ is a deep hole of the standard Reed–Solomon code over $\mathbb{F}_q$ of dimension k.*

In [16] the existence of deep holes is reconsidered. Using the Weil estimate for certain character sums as in [20], the authors obtain the following result.

Theorem 1.4 ([16, Theorem 1.4]). *Let k, d be given positive integers. If $q > \max\{d^{2+\epsilon}, (k+1)^2\}$ and $k > (\frac{2}{\epsilon}+1)d + \frac{8}{\epsilon} + 2$ holds for a constant $\epsilon > 0$, then no word $\mathbf{w}_f$ generated by a polynomial $f \in \mathbb{F}_q[T]$ of degree $k+d < q-1$ is a deep hole of the standard Reed–Solomon code over $\mathbb{F}_q$ of dimension k.*

1.2. Our results. We determine further threshold values $\lambda_1(d,k)$ and $\lambda_2(d)$ such that for $q > \lambda_1(d,k)$ and $k > \lambda_2(d)$ the standard Reed–Solomon code over $\mathbb{F}_q$ of dimension k has no deep holes generated by polynomials of degree $k+d$. In fact, we have the following result (see Theorems 5.5 and 5.6 for precise versions).

Theorem 1.5. *Let k, d be positive integers and $0 < \epsilon < 1$. Suppose that $q > \max\{14d^{2+\epsilon}, (k+1)^2\}$ and $k > (\frac{2}{\epsilon}+1)d$ hold. Let $f \in \mathbb{F}_q[T]$ be an arbitrary polynomial of degree $k+d < q-1$ and let $\mathbf{w}_f \in \mathbb{F}_q^{q-1}$ be the word generated by f. Then $\mathbf{w}_f$ is not a deep hole of the standard Reed–Solomon code over $\mathbb{F}_q$ of dimension k.*

This result is obtained from a lower bound on the number of q–rational points with nonzero, pairwise–distinct coordinates of the family of hypersurfaces V_f introduced above. Our result improves that of [4] by means of a deeper study of the geometry of these hypersurfaces. In fact, we show that each hypersurface V_f has a singular locus of dimension at most $d-1$ (Corollary 3.3), which in particular implies that it is absolutely irreducible (as proved by [4]). We further prove that for $p := \operatorname{char} \mathbb{F}_q > d+1$, the singular locus of the hypersurfaces V_f of interest has dimension at most $d-2$ (Theorem 4.2, Lemma 4.3 and Proposition 4.5).

For this purpose, we show that the polynomials $H_f \in \mathbb{F}_q[X_1, \dots, X_{k+1}]$ defining the hypersurfaces V_f are symmetric, namely invariant under any permutation of the variables $X_1, \dots, X_{k+1}$. More precisely, for any polynomial $f \in \mathbb{F}_q[T]$ as in (1) of degree $k+d$, we prove that H_f can be expressed as a polynomial in the first d elementary symmetric polynomials $\Pi_1, \dots, \Pi_d$ of $\mathbb{F}_q[X_1, \dots, X_{k+1}]$ (Propositions 2.2 and 2.3). Such an expression involves the number of different partitions of d (admitting repetition) and resembles the Waring formula.

The result on the dimension of the singular locus of the hypersurfaces V_f is then combined with estimates on the number of q–rational points of singular complete intersections [8], yielding our main result Theorem 1.5.

Our results also constitute an improvement of that of [16], as can be readily deduced by comparing the statements of Theorems 1.4 and 1.5. Nevertheless, as the "main" exponents in both results are similar, we would like to stress here the methodological aspect. As mentioned before, the critical point for our approach is the invariance of the family of hypersurfaces V_f under the action of the symmetric group of $k+1$ elements. In fact, our results on the dimension of the singular locus and the estimates on the number of q–rational points can be extended *mutatis mutandis* to any symmetric hypersurface whose projection on the set of primary invariants (using the terminology of invariant theory) defines a nonsingular hypersurface. This might be seen as a further source of interest of our approach, since hypersurfaces with symmetries arise frequently in coding theory and cryptography (for example, in the study of almost perfect nonlinear polynomials or differentially uniform mappings; see, e.g., [18] or [2]).

2. H_f in terms of the elementary symmetric polynomials

Fix positive integers d and k such that $d < k$, and consider the first d elementary symmetric polynomials $\Pi_1, \dots, \Pi_d$ of $\mathbb{F}_q[X_1, \dots, X_{k+1}]$. For convenience of notation, we shall denote $\Pi_0 := 1$. In Section 1 we associate a polynomial $H_f \in \mathbb{F}_q[X_1, \dots, X_{k+1}]$ to every polynomial $f \in \mathbb{F}_q[T]$ of degree $k + d$ as in (1). As asserted above, the word $\mathbf{w}_f$ generated by a given polynomial f is not a deep hole of the standard Reed–Solomon code of dimension k over $\mathbb{F}_q$ if H_f has a q–rational zero with nonzero, pairwise–distinct coordinates.

The main purpose of this section is to show how the polynomials H_f can be expressed in terms of the elementary symmetric polynomials $\Pi_1, \dots, \Pi_d$. In order to do this, we first obtain a recursive expression for the polynomial H_d associated to the monomial T^{k+d}.

Lemma 2.1. *Fix $H_0 := 1$. For any $d \geq 1$, the following identity holds:*

$$H_d = \Pi_1 H_{d-1} - \Pi_2 H_{d-2} + \cdots + (-1)^{d-1} \Pi_d H_0. \tag{4}$$

Proof. Let as before $Q := (T - X_1) \cdots (T - X_{k+1})$. We have

$$T^{k+1} \equiv \Pi_1 T^k - \Pi_2 T^{k-1} + \cdots + (-1)^{d-1} \Pi_d T^{k-(d-1)} + \cdots + (-1)^k \Pi_{k+1} \mod Q.$$

Multiplying this congruence relation by T^{d-1} we obtain:

$$T^{k+d} \equiv \Pi_1 T^{k+d-1} - \Pi_2 T^{k+d-2} + \cdots + (-1)^{d-1} \Pi_d T^k + \mathcal{O}(T^{k-1}) \mod Q,$$

where $\mathcal{O}(T^{k-1})$ represents a sum of terms of $\mathbb{F}_q[X_1, \dots, X_{k+1}][T]$ of degree at most $k-1$ in T. Recall that we define H_{d-j} as the unique polynomial of $\mathbb{F}_q[X_1, \dots, X_{k+1}]$ satisfying the congruence relation

$$T^{k+d-j} \equiv H_{d-j} T^k + \mathcal{O}(T^{k-1}) \mod Q$$

for $1 \leq j \leq d - 1$. Hence, we obtain the equality

$$H_d = \Pi_1 H_{d-1} - \Pi_2 H_{d-2} + \cdots + (-1)^{d-1} \Pi_d.$$

This finishes the proof of the lemma. □

Our second step is to obtain an explicit expression of the polynomial H_d in terms of the elementary symmetric polynomials $\Pi_1, \dots, \Pi_d$. From this expression we readily obtain an expression for the polynomial H_f associated to an arbitrary polynomial f as in (1) of degree $k + d$.

Proposition 2.2. *Let $H_d \in \mathbb{F}_q[X_1, \dots, X_{k+1}]$ be the polynomial associated to the monomial T^{k+d}. Then the following identity holds:*

$$H_d = \sum_{i_1 + 2i_2 + \cdots + di_d = d} (-1)^{\Delta(i_1, \dots, i_d)} \frac{(i_1 + \cdots + i_d)!}{i_1! \cdots i_d!} \Pi_1^{i_1} \cdots \Pi_d^{i_d}, \tag{5}$$

where $0 \leq i_j \leq d$ holds for $1 \leq j \leq d$ and $\Delta(i_1, \dots, i_d) := i_2 + i_4 + \cdots + i_{2\lfloor d/2 \rfloor}$ denotes the sum of indices i_j for which j is an even number.

Proof. We argue by induction on d. The case $d = 1$ follows immediately from (4).

Assume now that $d > 1$ holds and (5) is valid for $1 \leq j \leq d - 1$. From (5) we easily conclude that H_j is a homogeneous symmetric polynomial of $\mathbb{F}_q[X_1, \dots, X_{k+1}]$ of degree j for $1 \leq j \leq d - 1$. Furthermore, from Lemma 2.1 we deduce that H_d is also a homogeneous symmetric polynomial of degree d. Combining the inductive hypotheses and Lemma 2.1 we see that H_d can be expressed in the form

$$H_d = \sum_{i_1 + \cdots + di_d = d} a_{i_1, \dots, i_d} \Pi_1^{i_1} \cdots \Pi_d^{i_d},$$

for suitable elements $a_{i_1,\dots,i_d}\in\mathbb{F}_q$. As a consequence, it only remains to prove that the terms $a_{i_1,\dots,i_d}$ have the asserted form, namely

$$a_{i_1,\dots,i_d}=(-1)^{\Delta(i_1,\dots,i_d)}\frac{(i_1+\cdots+i_d)!}{i_1!\cdots i_d!}.$$

Fix $(i_1,\dots,i_d)\in(\mathbb{Z}_{\geq 0})^d$ with $i_1+2i_2+\cdots+di_d=d$. Then Lemma 2.1 shows that

$$a_{i_1,\dots,i_d}=\sum_{j=1}^{d}(-1)^{j-1}(H_{d-j})_{i_1,\dots,i_j-1,\dots,i_d},$$

where $(H_{d-j})_{i_1,\dots,i_j-1,\dots,i_d}$ is the coefficient of the monomial $\Pi_1^{i_1}\cdots\Pi_j^{i_j-1}\cdots\Pi_d^{i_d}$ in the expression of H_{d-j} as a polynomial of $\mathbb{F}_q[\Pi_1,\dots,\Pi_d]$.

Therefore, applying the inductive hypothesis, we obtain:

$$a_{i_1,\dots,i_d}=\sum_{j=1}^{d}(-1)^{j-1}(-1)^{\Delta(i_1,\dots,i_j-1,\dots,i_d)}\frac{(i_1+\cdots+i_d-1)!}{i_1!\cdots(i_j-1)!\cdots i_d!}.$$

If j is an odd number, then $\Delta(i_1,\dots,i_j-1,\dots,i_d)=\Delta(i_1,\dots,i_j,\dots,i_d)$ and $(-1)^{j-1}=1$ hold, which implies $(-1)^{j-1+\Delta(i_1,\dots,i_j-1,\dots,i_d)}=(-1)^{\Delta(i_1,\dots,i_j,\dots,i_d)}$. On the other hand, if j is an even number then we have $(-1)^{j-1}=-1$ and $(-1)^{\Delta(i_1,\dots,i_j,\dots,i_d)}=(-1)^{j-1}(-1)^{\Delta(i_1,\dots,i_j-1,\dots,i_d)}$. Therefore

$$\begin{aligned}a_{i_1,\dots,i_d}&=(-1)^{\Delta(i_1,\dots,i_d)}(i_1+\cdots+i_d-1)!\frac{(i_1+\cdots+i_d)}{i_1!\dots i_d!}\\&=(-1)^{\Delta(i_1,\dots,i_d)}\frac{(i_1+\cdots+i_d)!}{i_1!\dots i_d!}.\end{aligned}$$

This concludes the proof of the proposition. □

It is interesting to remark the similarity of the expression for H_d with Waring's formula expressing the power sums in terms of the elementary symmetric polynomials (see, e.g., [17, Theorem 1.76]).

Finally we obtain an expression of the polynomial $H_f\in\mathbb{F}_q[X_1,\dots,X_{k+1}]$ associated to an arbitrary polynomial $f\in\mathbb{F}_q[T]$ of degree $k+d$ in terms of the polynomials H_d.

Proposition 2.3. *Let $f:=T^{k+d}+f_{d-1}T^{k+d-1}+\cdots+f_0T^k$ be a polynomial of $\mathbb{F}_q[T]$ and let $H_f\in\mathbb{F}_q[X_1,\dots,X_{k+1}]$ be the polynomial associated to f. Then the following identity holds:*

$$H_f=H_d+f_{d-1}H_{d-1}+\cdots+f_1H_1+f_0. \tag{6}$$

Proof. In the proof of Lemma 2.1 we obtain the following congruence relation:

$$T^{k+d}\equiv\Pi_1T^{k+d-1}-\Pi_2T^{k+d-2}+\cdots+(-1)^{d-1}\Pi_dT^k+\mathcal{O}(T^{k-1})\mod Q.$$

Hence we have

$$T^{k+d}+\sum_{j=0}^{d-1}f_jT^{k+j}\equiv\sum_{j=0}^{d-1}\big((-1)^{d-1+j}\Pi_{d-j}+f_j\big)T^{k+j}+\mathcal{O}(T^{k-1})\mod Q.$$

Therefore, taking into account that $T^{k+j} \equiv H_jT^k + \mathcal{O}(T^{k-1}) \mod Q$ holds for $1 \le j \le d-1$, we obtain

$$\begin{aligned} f := T^{k+d} + \sum_{j=0}^{d-1} f_jT^{k+j} &\equiv \sum_{j=0}^{d-1} \big((-1)^{d-1+j}\Pi_{d-j} + f_j\big)H_jT^k + \mathcal{O}(T^{k-1}) \mod Q \\ &= \left(\sum_{j=0}^{d-1}(-1)^{d-1+j}\Pi_{d-j}H_j + \sum_{j=0}^{d-1} f_jH_j\right)T^k + \mathcal{O}(T^{k-1}) \\ &= \left(H_d + \sum_{j=0}^{d-1} f_jH_j\right)T^k + \mathcal{O}(T^{k-1}), \end{aligned}$$

where the last equality is a consequence of Lemma 2.1. This shows that (6) is valid and finishes the proof. □

Remark 2.4. From Lemma 2.1 and Proposition 2.2 we easily conclude that H_d is a homogeneous polynomial of $\mathbb{F}_q[X_1,\dots,X_{k+1}]$ of degree d and can be expressed as a polynomial in the elementary symmetric polynomials $\Pi_1,\dots,\Pi_d$. In this sense, we observe that H_d is a monic element of $\mathbb{F}_q[\Pi_1,\dots,\Pi_{d-1}][\Pi_d]$, up to a nonzero constant of $\mathbb{F}_q$. Combining these remarks and Proposition 2.3 we see that, for an arbitrary polynomial $f := T^{k+d} + f_{d-1}T^{k+d-1} + \cdots + f_0T^k \in \mathbb{F}_q[T]$, the corresponding polynomial $H_f \in \mathbb{F}_q[X_1,\dots,X_{k+1}]$ has degree d and is also a monic element of $\mathbb{F}_q[\Pi_1,\dots,\Pi_{d-1}][\Pi_d]$.

3. The geometry of the set of zeros of H_f

For positive integers d and k with $k > d$, let be given $f := T^{k+d} + f_{d-1}T^{k+d-1} + \cdots + f_0T^k \in \mathbb{F}_q[T]$ and consider the corresponding polynomial $H_f \in \mathbb{F}_q[X_1,\dots,X_{k+1}]$. According to Remark 2.4, we may express H_f as a polynomial in the first d elementary symmetric polynomials $\Pi_1,\dots,\Pi_d$ of $\mathbb{F}_q[X_1,\dots,X_{k+1}]$, namely $H_f = G_f(\Pi_1,\dots,\Pi_d)$, where $G_f \in \mathbb{F}_q[Y_1,\dots,Y_d]$ is a monic element of $\mathbb{F}_q[Y_1,\dots,Y_{d-1}][Y_d]$ of degree 1 in Y_d.

In this section we obtain critical information on the geometry of the set of zeros of H_f that will allow us to establish upper bounds on the number q–rational zeros of H_f.

3.1. Notions of algebraic geometry.

Since our approach relies heavily on tools of algebraic geometry, we briefly collect the basic definitions and facts that we need in the sequel. We use standard notions and notations of algebraic geometry, which can be found in, e.g., [13], [19].

We denote by $\mathbb{A}^n$ the affine n–dimensional space $\overline{\mathbb{F}}_q^n$ and by $\mathbb{P}^n$ the projective n–dimensional space over $\overline{\mathbb{F}}_q^{n+1}$. Both spaces are endowed with their respective Zariski topologies, for which a closed set is the zero locus of polynomials of $\overline{\mathbb{F}}_q[X_1,\dots,X_n]$ or of homogeneous polynomials of $\overline{\mathbb{F}}_q[X_0,\dots,X_n]$. For $\mathsf{K} := \mathbb{F}_q$ or $\mathsf{K} := \overline{\mathbb{F}}_q$, we say that a subset $V \subset \mathbb{A}^n$ is an affine K–variety if it is the set of common zeros in $\mathbb{A}^n$ of polynomials $F_1,\dots,F_m \in \mathsf{K}[X_1,\dots,X_n]$. Correspondingly, a projective K–variety is the set of common zeros in $\mathbb{P}^n$ of homogeneous polynomials $F_1,\dots,F_m \in \mathsf{K}[X_0,\dots,X_n]$. An affine or projective K–variety is sometimes called simply a variety. When V is the set of zeros of a single polynomial of $\mathsf{K}[X_1,\dots,X_n]$, or a single homogeneous polynomial of $\mathsf{K}[X_0,\dots,X_n]$, we say that V is an (affine or projective) $\mathbb{F}_q$–hypersurface.

A K–variety V is K–irreducible if it cannot be expressed as a finite union of proper K–subvarieties of V. Further, V is absolutely irreducible if it is irreducible as a $\overline{\mathbb{F}}_q$–variety. An $\mathbb{F}_q$–hypersurface V is absolutely irreducible if and only if any polynomial of $\mathbb{F}_q[X_1,\dots,X_n]$, or any homogeneous polynomial of $\mathbb{F}_q[X_0,\dots,X_n]$, of minimal degree defining V is absolutely irreducible, namely is an irreducible element of the ring $\overline{\mathbb{F}}_q[X_1,\dots,X_n]$ or $\overline{\mathbb{F}}_q[X_0,\dots,X_n]$. Any K–variety V can be expressed as an irredundant union $V=\mathcal{C}_1\cup\cdots\cup\mathcal{C}_s$ of absolutely irreducible K–varieties, unique up to reordering, which are called the absolutely irreducible K–components of V.

The set $V(\mathbb{F}_q):=V\cap\mathbb{F}_q^n$ is the set of q–rational points of V. Studying the number of elements of $V(\mathbb{F}_q)$ is a classical problem. The existence of q–rational points depends upon many circumstances concerning the geometry of the underlying variety.

For a K-variety V contained in $\mathbb{A}^n$ or $\mathbb{P}^n$, we denote by $I(V)$ its defining ideal, namely the set of polynomials of $\mathsf{K}[X_1,\dots,X_n]$, or of $\mathsf{K}[X_0,\dots,X_n]$, vanishing on V. The coordinate ring $\mathsf{K}[V]$ of V is the quotient ring $\mathsf{K}[X_1,\dots,X_n]/I(V)$ or $\mathsf{K}[X_0,\dots,X_n]/I(V)$. The dimension $\dim V$ of a K-variety V is the length r of the longest chain $V_0\subsetneq V_1\subsetneq\cdots\subsetneq V_r$ of nonempty irreducible K-varieties contained in V. The degree $\deg V$ of an irreducible K-variety V is the maximum number of points lying in the intersection of V with a generic linear space L of codimension $\dim V$, for which $V\cap L$ is a finite set. More generally, following [11], if $V=V_1\cup\cdots\cup V_s$ is the decomposition of V into irreducible K–components, we define the degree of V as

$$\deg V:=\sum_{i=1}^{s}\deg V_i.$$

Let V be a variety contained in $\mathbb{A}^n$ and let $I(V)\subset\overline{\mathbb{F}}_q[X_1,\dots,X_n]$ be the defining ideal of V. Let $\mathbf{x}$ be a point of V. The dimension $\dim_{\mathbf{x}}V$ of V at $\mathbf{x}$ is the maximum of the dimensions of the irreducible components of V that contain $\mathbf{x}$. If $I(V)=(F_1,\dots,F_m)$, the tangent space $\mathcal{T}_{\mathbf{x}}V$ to V at $\mathbf{x}$ is the kernel of the Jacobian matrix $(\partial F_i/\partial X_j)_{1\le i\le m,1\le j\le n}(\mathbf{x})$ of the polynomials $F_1,\dots,F_m$ with respect to $X_1,\dots,X_n$ at $\mathbf{x}$. The point $\mathbf{x}$ is regular if $\dim\mathcal{T}_{\mathbf{x}}V=\dim_{\mathbf{x}}V$ holds. Otherwise, the point $\mathbf{x}$ is called singular. The set of singular points of V is the singular locus $\mathrm{Sing}(V)$ of V. For a projective variety, the concepts of tangent space, regular and singular point can be defined by considering an affine neighborhood of the point under consideration.

3.2. The singular locus of symmetric hypersurfaces.

With the notations of the beginning of Section 3, let $V_f\subset\mathbb{A}^{k+1}$ denote the $\mathbb{F}_q$–hypersurface defined by H_f. Our main concern in this section is the study of the singular locus of V_f. For this purpose, we consider the somewhat more general framework that we now introduce. This will allow us to make more transparent the facts concerning the algebraic structure of the family of polynomials H_f which are important at this point.

Let $Y_1,\dots,Y_d$ be new indeterminates over $\overline{\mathbb{F}}_q$, let $G\in\mathbb{F}_q[Y_1,\dots,Y_d]$ be a given polynomial and let $\nabla G\in\mathbb{F}_q[Y_1,\dots,Y_d]^d$ denote the vector consisting of the first partial derivatives of G. Suppose that $\nabla G(\mathbf{y})$ is a nonzero vector of $\mathbb{A}^d$ for every $\mathbf{y}\in\mathbb{A}^d$. Hence G is square–free and defines a nonsingular hypersurface $W\subset\mathbb{A}^d$.

Let $\Pi_1,\dots,\Pi_d$ be the first d elementary symmetric polynomials of $\mathbb{F}_q[X_1,\dots,X_{k+1}]$ and let $H:=G(\Pi_1,\dots,\Pi_d)$. We denote by $V\subset\mathbb{A}^{k+1}$ the hypersurface defined by H. The main result of this section will be an upper bound on the dimension of the singular locus of V. For this purpose, we consider the following surjective morphism of $\mathbb{F}_q$–hypersurfaces:

$$\begin{array}{rcl} \Pi : V & \rightarrow & W \\ \mathbf{x} & \mapsto & (\Pi_1(\mathbf{x}), \ldots, \Pi_d(\mathbf{x})). \end{array}$$

For $\mathbf{x} \in V$ and $\mathbf{y} := \Pi(\mathbf{x})$, we denote by $\mathcal{T}_{\mathbf{x}}V$ and $\mathcal{T}_{\mathbf{y}}W$ the tangent spaces to V at $\mathbf{x}$ and to W at $\mathbf{y}$. We also consider the differential map of Π at $\mathbf{x}$, namely

$$\begin{array}{rcl} \mathrm{d}_{\mathbf{x}}\Pi : \mathcal{T}_{\mathbf{x}}V & \rightarrow & \mathcal{T}_{\mathbf{y}}W \\ \mathbf{v} & \mapsto & A(\mathbf{x}) \cdot \mathbf{v}, \end{array}$$

where $A(\mathbf{x})$ stands for the $d \times (k+1)$ matrix

$$A(\mathbf{x}) := \begin{pmatrix} \dfrac{\partial \Pi_1}{\partial X_1}(\mathbf{x}) & \cdots & \dfrac{\partial \Pi_1}{\partial X_{k+1}}(\mathbf{x}) \\ \vdots & & \vdots \\ \dfrac{\partial \Pi_d}{\partial X_1}(\mathbf{x}) & \cdots & \dfrac{\partial \Pi_d}{\partial X_{k+1}}(\mathbf{x}) \end{pmatrix}. \tag{7}$$

In order to prove our result about the singular locus of V, we first make a few remarks concerning the Jacobian matrix of the elementary symmetric polynomials that will be useful in the sequel.

It is well known that the first partial derivatives of the elementary symmetric polynomials Π_i satisfy the following equalities (see, e.g., [14]) for $1 \leq i, j \leq k+1$:

$$\frac{\partial \Pi_i}{\partial X_j} = \Pi_{i-1} - X_j \Pi_{i-2} + X_j^2 \Pi_{i-3} + \cdots + (-1)^{i-1} X_j^{i-1}. \tag{8}$$

As a consequence, denoting by A_{k+1} the $(k+1) \times (k+1)$ Vandermonde matrix

$$A_{k+1} := \begin{pmatrix} 1 & 1 & \cdots & 1 \\ X_1 & X_2 & \cdots & X_{k+1} \\ \vdots & \vdots & & \vdots \\ X_1^k & X_2^k & \cdots & X_{k+1}^k, \end{pmatrix}, \tag{9}$$

we deduce that the Jacobian matrix of $\Pi_1, \ldots, \Pi_{k+1}$ with respect to $X_1, \ldots, X_{k+1}$ can be factored as follows:

$$\left(\frac{\partial \Pi_i}{\partial X_j} \right)_{1 \leq i,j \leq k+1} := B_{k+1} \cdot A_{k+1} := \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 \\ \Pi_1 & -1 & 0 & & \\ \Pi_2 & -\Pi_1 & 1 & \ddots & \vdots \\ \vdots & \vdots & \vdots & \ddots & 0 \\ \Pi_k & -\Pi_{k-1} & \Pi_{k-2} & \cdots & (-1)^k \end{pmatrix} \cdot A_{k+1} \tag{10}$$

We observe that the left factor B_{k+1} is a square, lower–triangular matrix whose determinant is equal to $(-1)^{k(k+1)/2}$. This implies that the determinant of the matrix $(\partial \Pi_i / \partial X_j)_{1 \leq i,j \leq k+1}$ is equal, up to a sign, to the determinant of A_{k+1}, i.e.,

$$\det \left(\frac{\partial \Pi_i}{\partial X_j} \right)_{1 \leq i,j \leq k+1} = (-1)^{k(k+1)/2} \prod_{1 \leq i < j \leq k+1} (X_i - X_j).$$

An interesting fact, which will not be used in what follows, is that the inverse matrix of the matrix B_{k+1} of (10) is given by

$$B_{k+1}^{-1} = \begin{pmatrix} H_0 & 0 & 0 & \dots & 0 \\ H_1 & -H_0 & 0 & & \\ H_2 & -H_1 & H_0 & \ddots & \vdots \\ \vdots & \vdots & \vdots & \ddots & 0 \\ H_k & -H_{k-1} & H_{k-2} & \cdots & (-1)^k H_0 \end{pmatrix}.$$

Theorem 3.1. *The singular locus Σ of V has dimension at most $d-1$. Moreover, the elements of Σ have at most $d-1$ pairwise–distinct coordinates.*

Proof. By the chain rule we deduce that the partial derivatives of H satisfy the following equality for $1 \leq j \leq k+1$:

$$\frac{\partial H}{\partial X_j} = \left(\frac{\partial G}{\partial Y_1} \circ \Pi\right) \cdot \frac{\partial \Pi_1}{\partial X_j} + \cdots + \left(\frac{\partial G}{\partial Y_d} \circ \Pi\right) \cdot \frac{\partial \Pi_d}{\partial X_j}.$$

If $\mathbf{x}$ is any point of Σ, then we have

$$\nabla H(\mathbf{x}) = \nabla G(\Pi(\mathbf{x})) \cdot A(\mathbf{x}) = \mathbf{0},$$

where $A(\mathbf{x})$ is the matrix defined in (7). Fix $\mathbf{x} \in \Sigma$ and let $\mathbf{v} := \nabla G\big(\Pi(\mathbf{x})\big)$. By hypothesis we have that $\mathbf{v} \in \mathbb{A}^d$ is a nonzero vector satisfying

$$\mathbf{v} \cdot A(\mathbf{x}) = \mathbf{0}.$$

Hence, all the maximal minors of $A(\mathbf{x})$ must be zero.

The matrix $A(\mathbf{x})$ is the $d \times (k+1)$–submatrix of $(\partial \Pi_i / \partial X_j)_{1 \leq i,j \leq k+1}(\mathbf{x})$ consisting of the first d rows of the latter. Therefore, from (10) we conclude that

$$A(\mathbf{x}) = B_{d,k+1}(\mathbf{x}) \cdot A_{k+1}(\mathbf{x}),$$

where $B_{d,k+1}(\mathbf{x})$ is the $d \times (k+1)$–submatrix of $B_{k+1}(\mathbf{x})$ consisting of the first d rows of $B_{k+1}(\mathbf{x})$. Furthermore, since the last $k+1-d$ columns of $B_{d,k+1}(\mathbf{x})$ are zero, we may rewrite this identity in the following way:

$$A(\mathbf{x}) = B_d(\mathbf{x}) \cdot \begin{pmatrix} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_{k+1} \\ \vdots & \vdots & & \vdots \\ x_1^{d-1} & x_2^{d-1} & \dots & x_{k+1}^{d-1}, \end{pmatrix}, \tag{11}$$

where $B_d(\mathbf{x})$ is the $(d \times d)$–submatrix of $B_{k+1}(\mathbf{x})$ consisting on the first d rows and the first d columns of $B_{k+1}(\mathbf{x})$.

Fix $1 \leq l_1 < \cdots < l_d \leq k+1$, set $I := (l_1, \dots, l_d)$ and consider the $(d \times d)$–submatrix $M_I(\mathbf{x})$ of $A(\mathbf{x})$ consisting of the columns $l_1, \dots, l_d$ of $A(\mathbf{x})$, namely $M_I(\mathbf{x}) := (\partial \Pi_i / \partial X_{l_j})_{1 \leq i,j \leq d}(\mathbf{x})$.

From (10) and (11) we easily see that $M_I(\mathbf{x}) = B_d(\mathbf{x}) \cdot A_{d,I}(\mathbf{x})$, where $A_{d,I}(\mathbf{x})$ is the Vandermonde matrix $A_{d,I}(\mathbf{x}) := (x_{l_j}^{i-1})_{1 \leq i,j \leq d}$. Therefore, we obtain

$$\det\big(M_I(\mathbf{x})\big) = (-1)^{(d-1)d/2} \det A_{d,I}(\mathbf{x}) = (-1)^{(d-1)d/2} \prod_{1 \leq r < s \leq d} (x_{l_r} - x_{l_s}) = 0. \tag{12}$$

Since (12) holds for every $I := (l_1, \dots, l_d)$ as above, we conclude that every point $\mathbf{x} \in \Sigma$ has at most $d-1$ pairwise–distinct coordinates. In particular, Σ is contained in a finite union of linear varieties of $\mathbb{A}^{k+1}$ of dimension $d-1$, and thus its dimension is at most $d-1$. □

We observe that the proof of Theorem 3.1 provides a more precise description of the singular locus Σ of V, which is the subject of the following remark.

Remark 3.2. Let notations and assumptions be as in Theorem 3.1. From the proof of Theorem 3.1 we obtain the following inclusion:

$$\Sigma \subset \bigcup_{\mathcal{I}} \mathcal{L}_{\mathcal{I}},$$

where $\mathcal{I} := \{I_1, \dots, I_{d-1}\}$ runs over all the partitions of $\{1, \dots, k+1\}$ into $d-1$ nonempty subsets $I_j \subset \{1, \dots, k+1\}$ and $\mathcal{L}_{\mathcal{I}}$ is the linear variety

$$\mathcal{L}_{\mathcal{I}} := \operatorname{span}(\mathbf{v}^{(I_1)}, \dots, \mathbf{v}^{(I_{d-1})})$$

spanned by the vectors $\mathbf{v}^{(I_j)} := (v_1^{(I_j)}, \dots, v_{k+1}^{(I_j)})$ defined by $v_m^{(I_j)} := 1$ for $m \in I_j$ and $v_m^{(I_j)} := 0$ for $m \notin I_j$. In particular, it follows that if Σ has dimension $d-1$, then it contains a linear variety $\mathcal{L}_{\mathcal{I}}$ as above.

3.3. The dimension of the singular locus of V_f. Now we consider the hypersurface V_f defined by the polynomial $H_f \in \mathbb{F}_q[X_1, \dots X_{k+1}]$ associated to the polynomial $f := T^{k+d} + f_{d-1}T^{k+d-1} + \cdots + f_0T^k$. According to Remark 2.4, we may express H_f in the form $H_f = G_f(\Pi_1, \dots, \Pi_d)$, where $G_f \in \mathbb{F}_q[Y_1, \dots, Y_d]$ is a polynomial of degree d which is monic in Y_d, up to a nonzero constant. Moreover, since

$$\nabla G_f(\mathbf{y}) = \left(\frac{\partial G_f}{\partial Y_1}(\mathbf{y}), \dots, \frac{\partial G_f}{\partial Y_{d-1}}(\mathbf{y}), (-1)^{d-1}\right)$$

holds for every $\mathbf{y} \in \mathbb{A}^d$, we see that $\nabla G_f(\mathbf{y}) \neq \mathbf{0}$ for every $\mathbf{y} \in \mathbb{A}^d$; in other words, G_f defines a nonsingular hypersurface $W \subset \mathbb{A}^d$. Then the results of Section 3.2 can be applied to H_f. In particular, we have the following immediate consequence of Theorem 3.1.

Corollary 3.3. *The singular locus $\Sigma_f \subset \mathbb{A}^{k+1}$ of V_f has dimension at most $d-1$.*

In order to obtain estimates on the number of q–rational points of V_f we also need information concerning the behavior of V_f "at infinity". For this purpose, we consider the projective closure $\operatorname{pcl}(V_f) \subset \mathbb{P}^{k+1}$ of V_f, whose definition we now recall. Consider the embedding of $\mathbb{A}^{k+1}$ into the projective space $\mathbb{P}^{k+1}$ which assigns to any $\mathbf{x} := (x_1, \dots, x_{k+1}) \in \mathbb{A}^{k+1}$ the point $(1 : x_1 : \cdots : x_{k+1}) \in \mathbb{P}^{k+1}$. The closure $\operatorname{pcl}(V_f) \subset \mathbb{P}^{k+1}$ of the image of V_f under this embedding in the Zariski topology of $\mathbb{P}^{k+1}$ is called the projective closure of V_f. The points of $\operatorname{pcl}(V_f)$ lying in the hyperplane $\{X_0 = 0\}$ are called the points of $\operatorname{pcl}(V_f)$ at infinity.

It is well–known that $\operatorname{pcl}(V_f)$ is the $\mathbb{F}_q$–hypersurface of $\mathbb{P}^{k+1}$ defined by the homogenization $H_f^h \in \mathbb{F}_q[X_0, \dots, X_{k+1}]$ of the polynomial H_f (see, e.g., [13, §I.5, Exercise 6]). We have the following result.

Proposition 3.4. $\operatorname{pcl}(V_f)$ *has singular locus at infinity of dimension at most $d-2$.*

Proof. By Proposition 2.3, we have

$$H_f = H_d + f_{d-1}H_{d-1} + \cdots + f_1H_1 + f_0,$$

where each H_j is a homogeneous polynomial of degree j for $1 \le j \le d$. Hence, the homogenization of H_f is the following polynomial of $\mathbb{F}_q[X_0, \ldots, X_{k+1}]$:

$$H_f^h = H_d + f_{d-1} H_{d-1} X_0 + \cdots + f_1 H_1 X_0^{d-1} + f_0 X_0^d. \tag{13}$$

Let $\Sigma_f^\infty \subset \mathbb{P}^{k+1}$ denote the singular locus of $\mathrm{pcl}(V_f)$ at infinity, namely the set of singular points of $\mathrm{pcl}(V_f)$ lying in the hyperplane $\{X_0 = 0\}$. We have that any point $\mathbf{x} \in \Sigma_f^\infty$ satisfies the identities $H_f^h(\mathbf{x}) = 0$ and $\partial H_f^h / \partial X_i(\mathbf{x}) = 0$ for $0 \le i \le k+1$. From (13) we see that any point $\mathbf{x} := (0 : x_1 : \cdots : x_{k+1}) \in \Sigma_f^\infty$ satisfies the identities

$$\left\{ \begin{array}{rcll} H_d(x_1, \ldots, x_{k+1}) & = & 0, & \\ f_{d-1} H_{d-1}(x_1, \ldots, x_{k+1}) & = & 0, & \\ \dfrac{\partial H_d}{\partial X_i}(x_1, \ldots, x_{k+1}) & = & 0 & (1 \le i \le k+1). \end{array} \right. \tag{14}$$

From Proposition 2.2 and Remark 2.4 we have that $H_d \in \mathbb{F}_q[X_1, \ldots, X_{k+1}]$ is a homogeneous polynomial of degree d which can be expressed in the form $H_d = G_d(\Pi_1, \ldots, \Pi_d)$, where $G_d \in \mathbb{F}_q[Y_1, \ldots, Y_d]$ has degree d and is monic in Y_d. Combining these remarks with Theorem 3.1 we conclude that the set of solutions of (14) is an affine cone of $\mathbb{A}^{k+1}$ of dimension at most $d-1$, and hence, a projective variety of $\mathbb{P}^k$ of dimension at most $d-2$. This finishes the proof of the proposition. □

We end this section with a useful consequence of our bound on the dimension of the singular locus of $\mathrm{pcl}(V_f)$, namely that V_f is absolutely irreducible. This result, which has been proved in [4, Section 4], is obtained here as an easy consequence of Proposition 3.4.

Corollary 3.5. *The hypersurface V_f is absolutely irreducible.*

Proof. We observe that V_f is absolutely irreducible if and only if $\mathrm{pcl}(V_f)$ is absolutely irreducible (see, e.g., [13, Chapter I, Proposition 5.17]). If $\mathrm{pcl}(V_f)$ is not absolutely irreducible, then it has a nontrivial decomposition into absolutely irreducible components

$$\mathrm{pcl}(V_f) = \mathcal{C}_1 \cup \cdots \cup \mathcal{C}_s,$$

where $\mathcal{C}_1, \ldots, \mathcal{C}_s$ are projective hypersurfaces of $\mathbb{P}^{k+1}$. Since $\mathcal{C}_i \cap \mathcal{C}_j \neq \emptyset$ and $\mathcal{C}_i$, $\mathcal{C}_j$ are absolutely irreducible, we conclude that $\dim(\mathcal{C}_i \cap \mathcal{C}_j) = k-1$ holds.

Denote by Σ_f^h the singular locus of $\mathrm{pcl}(V_f)$. Corollary 3.3 and Proposition 3.4 imply $\dim \Sigma_f^h \le d-1$. On the other hand, we have $\mathcal{C}_i \cap \mathcal{C}_j \subset \Sigma_f^h$ for any $i \neq j$, which implies $\dim \Sigma_f^h \ge k-1$. This contradicts the assertion $\dim \Sigma_f^h \le d-1$, since we have $d < k$ by hypothesis. It follows that V_f is absolutely irreducible. □

4. The singular locus of V_f for fields of large characteristic

In this section we characterize the set of polynomials $f \in \mathbb{F}_q[T]$ for which the associated hypersurface $V_f \subset \mathbb{A}^{k+1}$ has a singular locus of dimension $d-1$. This characterization enables us to give conditions under which such polynomials do not generate deep holes of the standard Reed–Solomon code of dimension k over $\mathbb{F}_q$.

The first step is to obtain a suitable expression of the derivatives of the polynomial H_d associated to T^{k+d}.

Lemma 4.1. *If $j \geq 2$, then the partial derivatives of the polynomials H_j satisfy the following identity for $1 \leq i \leq k+1$:*

$$\frac{\partial H_j}{\partial X_i} = H_{j-1} + H_{j-2}X_i + H_{j-3}X_i^2 + \cdots + X_i^{j-1}.$$

Proof. The proof is by induction on j. By Lemma 2.1 we have $H_1 = \Pi_1$ and $H_2 = \Pi_1 H_1 - \Pi_2$. Combining this with (8) we easily see the assertion for $j = 2$. Next assume that the statement of the lemma holds for $2 \leq j \leq l-1$; we are going to show that it also holds for $j = l$. According to Lemma 2.1, we have

$$\frac{\partial H_l}{\partial X_i} = \sum_{m=1}^{l} (-1)^{m-1} \frac{\partial(\Pi_m H_{l-m})}{\partial X_i}. \tag{15}$$

By the inductive hypothesis and the expression (8) for the first partial derivatives of the elementary symmetric polynomials, each term in the right–hand side of (15) can be expressed as follows:

$$\frac{\partial(\Pi_m H_{l-m})}{\partial X_i} = H_{l-m} \sum_{n=1}^{m} (-1)^{n-1} \Pi_{m-n} X_i^{n-1} + \Pi_m \sum_{n=1}^{l-m} H_{l-(m+n)} X_i^{n-1}. \tag{16}$$

Now we determine the coefficient of H_{l-m} in the right–hand side of (15). From (16) we see that the only terms having a nonzero contribution to the coefficient of H_{l-m} are $\partial(\Pi_n H_{l-n})/\partial X_i$ for $1 \leq n \leq m$. In particular, we easily deduce that the coefficient of H_{l-1} is 1. For $1 \leq n < m$, the summand $(-1)^{n-1}\partial(\Pi_n H_{l-n})/\partial X_i$ contributes with the term $(-1)^{n-1}X_i^{m-n-1}\Pi_n$. On the other hand, the summand $(-1)^{m-1}\partial(\Pi_m H_{l-m})/\partial X_i$ in the right–hand side of (15) contributes with the sum $(-1)^{m-1}\sum_{n=0}^{m-1}(-1)^{m-n-1}\Pi_n X_i^{m-n-1}$. Putting all these terms together, we conclude that the term H_{l-m} occurs in (15) multiplied by

$$(-1)^{m-1} \sum_{n=0}^{m-1} (-1)^{m-n-1} \Pi_n X_i^{m-n-1} + \sum_{n=1}^{m-1} (-1)^{n-1} \Pi_n X_i^{m-n-1} = X_i^{m-1}.$$

This finishes the proof of the lemma. □

Observe that, similarly to the factorization (10) of the Jacobian matrix of the elementary symmetric polynomials of Section 3.2, Lemma 4.1 allows us to express the Jacobian matrix of $H_1, \ldots, H_{k+1}$ with respect to $X_1, \ldots, X_{k+1}$ as the following matrix product:

$$\left(\frac{\partial H_i}{\partial X_j}\right)_{1 \leq i,j \leq k+1} := \begin{pmatrix} H_0 & 0 & \cdots & 0 \\ H_1 & H_0 & \ddots & \vdots \\ \vdots & \vdots & \ddots & 0 \\ H_k & H_{k-1} & \ldots & H_0 \end{pmatrix} \cdot A_{k+1}, \tag{17}$$

where A_{k+1} is the Vandermonde matrix defined in (9).

Let $f \in \mathbb{F}_q[T]$ be a polynomial of the form

$$f := T^{k+d} + f_{d-1}T^{k+d-1} + \cdots + f_1 T^{k+1} + f_0 T^k,$$

and let $V_f \subset \mathbb{A}^{k+1}$ be the hypersurface associated to f. By Proposition 2.3, we have that V_f is the hypersurface defined by the polynomial

$$H_f = H_d + f_{d-1}H_{d-1} + \cdots + f_1 H_1 + f_0 H_0,$$

where the polynomials $H_j \in \mathbb{F}_q[X_1, \ldots, X_{k+1}]$ $(0 \le j \le d)$ are defined in Section 2. We recall that each H_j is homogeneous and symmetric of degree j (Remark 2.4).

Corollary 3.3 asserts that the singular locus Σ_f of V_f has dimension at most $d-1$. Suppose now that the dimension of Σ_f is equal to $d-1$. From Remark 3.2 we see that there exists a partition $\mathcal{I} := \{I_1, \ldots, I_{d-1}\}$ of the set $\{1, \ldots, k+1\}$ into $d-1$ nonempty sets $I_j \subset \{1, \ldots, k+1\}$ with the following property: let $\mathcal{L}_{\mathcal{I}} \subset \mathbb{A}^{k+1}$ denote the linear variety

$$\mathcal{L}_{\mathcal{I}} := \mathrm{span}(\mathbf{v}^{(I_1)}, \ldots, \mathbf{v}^{(I_{d-1})})$$

spanned by the vectors $\mathbf{v}^{(I_j)} := (v_1^{(I_j)}, \ldots, v_{k+1}^{(I_j)})$ defined by $v_l^{(I_j)} := 1$ for $l \in I_j$ and $v_l^{(I_j)} := 0$ for $l \notin I_j$ $(1 \le j \le d-1)$. Then $\mathcal{L}_{\mathcal{I}} \subset \Sigma_f$ holds. Let $\lambda := (\lambda_1, \ldots, \lambda_{d-1}) \in \mathbb{A}^{d-1}$ and let $\mathbf{x} := \sum_{j=1}^{d-1} \lambda_j \mathbf{v}^{(I_j)}$ be an arbitrary point of $\mathcal{L}_{\mathcal{I}}$. Since $\mathbf{x}$ is a singular point of V_f we have

$$0 = \frac{\partial H_f}{\partial X_i}(\mathbf{x}) = \frac{\partial H_d}{\partial X_i}(\mathbf{x}) + \sum_{j=1}^{d-1} f_{d-j} \frac{\partial H_{d-j}}{\partial X_i}(\mathbf{x})$$

for $1 \le i \le k+1$. This shows that the following matrix identity holds:

$$(18) \qquad -\begin{pmatrix} \dfrac{\partial H_1}{\partial X_1}(\mathbf{x}) & \cdots & \dfrac{\partial H_{d-1}}{\partial X_1}(\mathbf{x}) \\ \vdots & & \vdots \\ \dfrac{\partial H_1}{\partial X_{k+1}}(\mathbf{x}) & \cdots & \dfrac{\partial H_{d-1}}{\partial X_{k+1}}(\mathbf{x}) \end{pmatrix} \begin{pmatrix} f_1 \\ \vdots \\ f_{d-1} \end{pmatrix} = \begin{pmatrix} \dfrac{\partial H_d}{\partial X_1}(\mathbf{x}) \\ \vdots \\ \dfrac{\partial H_d}{\partial X_{k+1}}(\mathbf{x}) \end{pmatrix}.$$

By symmetry, we may assume that $x_i = \lambda_i$ holds for $1 \le i \le d-1$. We further assume that $\lambda_i \ne \lambda_j$ for $i \ne j$. Considering the first $d-1$ equations of (18) we obtain the square system

$$(19) \qquad -B(\mathbf{x}) \cdot \begin{pmatrix} f_1 \\ \vdots \\ f_{d-1} \end{pmatrix} = \begin{pmatrix} \dfrac{\partial H_d}{\partial X_1}(\mathbf{x}) \\ \vdots \\ \dfrac{\partial H_d}{\partial X_{d-1}}(\mathbf{x}) \end{pmatrix},$$

where $B(\mathbf{x}) \in \mathbb{A}^{(d-1)\times(d-1)}$ is the matrix

$$B(\mathbf{x}) := \begin{pmatrix} \dfrac{\partial H_1}{\partial X_1}(\mathbf{x}) & \cdots & \dfrac{\partial H_{d-1}}{\partial X_1}(\mathbf{x}) \\ \vdots & & \vdots \\ \dfrac{\partial H_1}{\partial X_{d-1}}(\mathbf{x}) & \cdots & \dfrac{\partial H_{d-1}}{\partial X_{d-1}}(\mathbf{x}) \end{pmatrix}.$$

From (17) we see that $B(\mathbf{x})$ can be factored as follows:

$$(20) \qquad B(\mathbf{x}) = A_{d-1}(\mathbf{x})^t \cdot \begin{pmatrix} H_0 & H_1(\mathbf{x}) \ldots & & H_{d-2}(\mathbf{x}) \\ 0 & H_0 & \ldots & H_{d-3}(\mathbf{x}) \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & H_0 \end{pmatrix},$$

where $A_{d-1}(\mathbf{x})$ is the Vandermonde matrix $A_{d-1}(\mathbf{x}) := (x_j^{i-1})_{1\le i,j\le d-1}$. As a consequence, we have that $B(\mathbf{x})$ is nonsingular and its determinant is equal to

$$\det B(\mathbf{x}) = \prod_{1\le i<j\le d-1} (x_i - x_j). \tag{21}$$

Hence $(f_1,\dots,f_{d-1})$ is the unique solution of the linear system (19). Furthermore, by the Cramer rule we obtain

$$f_j = \frac{\det B^{(j)}(\mathbf{x})}{\det B(\mathbf{x})} \quad (1\le j\le d-1),$$

where $B^{(j)}(\mathbf{x}) \in \mathbb{A}^{(d-1)\times(d-1)}$ is the matrix obtained by replacing the jth column of $B(\mathbf{x})$ by the vector $b(\mathbf{x}) := \big((\partial H_d/\partial X_1)(\mathbf{x}),\dots,(\partial H_d/\partial X_{d-1})(\mathbf{x})\big)$.

Let $B, B^{(j)} \in \mathbb{F}_q[X_1,\dots,X_{k+1}]^{(d-1)\times(d-1)}$ be the "generic" versions of the matrices $B(\mathbf{x}), B^{(j)}(\mathbf{x})$ for $1\le j\le d-1$. We claim that $\det B = \prod_{1\le i<j\le d-1}(X_i - X_j)$ divides $\det B^{(j)}$ in $\mathbb{F}_q[X_1,\dots,X_{k+1}]$.

In order to show this claim, let $C \in \mathbb{F}_q[X_1,\dots,X_{d-1}]^{(d-1)\times d}$ be the following matrix:

$$C := \begin{pmatrix} 1 & X_1 & \cdots & X_1^{d-2} & X_1^{d-1} \\ 1 & X_2 & \cdots & X_2^{d-2} & X_2^{d-1} \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & X_{d-1} & \cdots & X_{d-1}^{d-2} & X_{d-1}^{d-1} \end{pmatrix}. \tag{22}$$

Observe that this matrix is obtained by appending the vector column $(X_j^{d-1})_{1\le j\le d-1}$ to the transpose A_{d-1}^t of the generic matrix $A_{d-1} \in \mathbb{F}_q[X_1,\dots,X_{d-1}]^{(d-1)\times(d-1)}$. Further, for $1\le j\le d-1$ we define a matrix $H^{(j)} \in \mathbb{F}_q[X_1,\dots,X_{k+1}]^{d\times(d-1)}$ as

$$H^{(j)} := \begin{pmatrix} H_0 & H_1 & \cdots & H_{j-2} & H_{d-1} & H_j & \cdots & H_{d-2} \\ 0 & H_0 & \cdots & H_{j-1} & H_{d-2} & H_{j-1} & \cdots & H_{d-3} \\ \vdots & 0 & \ddots & \vdots & \vdots & \vdots & & \vdots \\ & & \ddots & H_0 & H_{d-j+1} & H_2 & \cdots & H_{j-1} \\ \vdots & \vdots & & 0 & H_{d-j} & H_1 & & \vdots \\ & & & & H_{d-j-1} & H_0 & \ddots & \\ \vdots & \vdots & & \vdots & \vdots & 0 & \ddots & H_1 \\ & & & & H_1 & \vdots & \ddots & H_0 \\ 0 & 0 & \cdots & 0 & H_0 & 0 & \cdots & 0 \end{pmatrix},$$

namely $H^{(j)}$ is obtained by appending a zero dth row to the second factor in the right–hand side of (20) and replacing the resulting jth column by the column vector $(H_{d-j} : 1\le j\le d) \in \mathbb{F}_q[X_1,\dots,X_{k+1}]^{d\times 1}$.

It turns out that the matrix $B^{(j)}$ can be factored as follows:

$$B^{(j)} = C\cdot H^{(j)}. \tag{23}$$

Indeed, for $l\ne j$, the lth columns of B and $B^{(j)}$ agree, and the fact that the lth columns of both sides of (23) are equal is easily deduced from (20). On the other hand, from Lemma 4.1 we immediately conclude that the jth columns of $B^{(j)}$ and $C\cdot H^{(j)}$ are equal.

In particular, the determinant of $B^{(j)}$ can be obtained from (23) by means of the Cauchy–Binet formula. Since any maximal minor of C is a multiple of $\det B$ (see, e.g., [6, Lemma 2.1] or [7, Exercise 281]), we immediately deduce that $\det B$ divides $\det B^{(j)}$ in $\mathbb{F}_q[X_1,\dots,X_{k+1}]$.

As a consequence of our claim, we see that for $1\le j\le d-1$ there exists a homogeneous polynomial $P^{(j)}\in\mathbb{F}_q[X_1,\dots,X_{d-1}]$ of degree $d-j$ or zero such that

$$f_{d-j}=P^{(j)}(\lambda_1,\dots,\lambda_{d-1}) \tag{24}$$

holds for $1\le j\le d-1$ and for any $(\lambda_1,\dots,\lambda_{d-1})\in\mathbb{A}^{d-1}$ with $\lambda_i\neq\lambda_j$ for $i\neq j$. Since (24) holds in a Zariski open dense subset of $\mathbb{A}^{d-1}$, we conclude that (24) holds for every $(\lambda_1,\dots,\lambda_{d-1})\in\mathbb{A}^{d-1}$. By substituting 0 for λ_i in (24) we deduce that $f_{d-j}=0$ holds for $1\le j\le d-1$. Finally taking into account that $(0,\dots,0)$ belongs to $\mathcal{L}_{\mathcal{I}}\subset\Sigma_f\subset V_f$ we obtain $f_0=0$. Therefore, we have the following result.

Theorem 4.2. *With notations as above, if the singular locus Σ_f of V_f has dimension $d-1$, then $f_0=\cdots=f_{d-1}=0$ holds.*

4.1. The monomial case. Fix a polynomial $f\in\mathbb{F}_q[T]$ of degree $k+d<q-1$ with $k>d$ as in (1) and consider the corresponding hypersurface $V_f\subset\mathbb{A}^{k+1}$. Corollary 3.3 shows that the dimension of the singular locus of V_f is at most $d-1$. Furthermore, Theorem 4.2 asserts that, if the dimension of the singular locus of V_f is $d-1$, then the polynomial f is necessarily the monomial $f=T^{k+d}$. Our purpose in this section is to show that, if the characteristic p of $\mathbb{F}_q$ satisfies the inequality $p>d+1$, then this monomial does not generate a deep hole of the standard Reed–Solomon code of dimension k over $\mathbb{F}_q$. This implies that, for the sake of deciding the existence of deep holes, we may assume without loss of generality that the singular locus of V_f has dimension at most $d-2$ when $p>d+1$ holds. As a first step in this direction, we prove that, if the dimension of the singular locus of V_f is $d-1$, then p divides $k+d$.

Lemma 4.3. *Fix positive integers k and d with $k>d$. If the hypersurface $V_d\subset\mathbb{A}^{k+1}$ associated to T^{k+d} has a singular locus of dimension $d-1$, then $p|(k+d)$.*

Proof. We use the notations of the proof of Theorem 4.2. In such a proof we show that, if the singular locus Σ_d of V_d has dimension $d-1$, then there exists a linear variety

$$\mathcal{L}_{\mathcal{I}}:=\operatorname{span}(\mathbf{v}^{(I_1)},\dots,\mathbf{v}^{(I_{d-1})})$$

of dimension $d-1$ contained in Σ_d, where $v_i^{I_j}\in\{0,1\}$ for $1\le i\le k+1$ and $1\le j\le d-1$, and $\mathbf{v}^{(I_1)}+\cdots+\mathbf{v}^{(I_{d-1})}=(1,\dots,1)$. Let $\lambda:=(\lambda_1,\dots,\lambda_{d-1})\in\mathbb{A}^{d-1}$ and let $\mathbf{x}:=\sum_{j=1}^{d-1}\lambda_j\mathbf{v}^{(I_j)}$ be and arbitrary point of $\mathcal{L}_{\mathcal{I}}$. As in the proof of Theorem 4.2, we assume that $x_i=\lambda_i$ $(1\le i\le d-1)$ and $\lambda_i\neq\lambda_j$ $(1\le i<j\le k+1)$ holds. By (21) we have that the matrix $B(\mathbf{x})$ is nonsingular and hence $\mathbf{0}\in\mathbb{A}^d$ is the unique solution of the linear square system (19), namely

$$-B(\mathbf{x})\cdot\begin{pmatrix} f_1\\ \vdots\\ f_{d-1}\end{pmatrix}=\begin{pmatrix}\dfrac{\partial H_d}{\partial X_1}(\mathbf{x})\\ \vdots\\ \dfrac{\partial H_d}{\partial X_{d-1}}(\mathbf{x})\end{pmatrix}.$$

In particular, the Cramer rule implies

$$\det B^{(d-1)}(\mathbf{x})=0, \tag{25}$$

where $B^{(d-1)}(\mathbf{x}) \in \mathbb{A}^{(d-1)\times(d-1)}$ is the matrix obtained by replacing the $(d-1)$th column of $B(\mathbf{x})$ by the vector $b(\mathbf{x}) := \big((\partial H_d/\partial X_j)(\mathbf{x}) : 1 \le j \le d-1\big)$. We also recall that the matrix $B^{(d-1)}(\mathbf{x})$ can be factored as in (23), namely $B^{(d-1)}(\mathbf{x}) = C(\mathbf{x}) \cdot H^{(d-1)}(\mathbf{x})$, where $C(\mathbf{x})$ is defined as in (22) and $H^{(d-1)}(\mathbf{x}) \in \mathbb{A}^{d\times(d-1)}$ is the following matrix:

$$H^{(d-1)}(\mathbf{x}) := \begin{pmatrix} 1 & H_1(\mathbf{x}) & \cdots & H_{d-3}(\mathbf{x}) & H_{d-1}(\mathbf{x}) \\ 0 & 1 & \cdots & H_{d-4}(\mathbf{x}) & H_{d-2}(\mathbf{x}) \\ & 0 & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & 1 & H_2(\mathbf{x}) \\ & & & 0 & H_1(\mathbf{x}) \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

We shall obtain an explicit expression of $\det B^{(d-1)}(\mathbf{x})$ by applying the Cauchy–Binet formula to such a factorization of $B^{(d-1)}(\mathbf{x})$. For this purpose, we observe that $H^{(d-1)}(\mathbf{x})$ has only two nonzero $(d-1)\times(d-1)$ minors: the one corresponding to the submatrix consisting of the first $d-1$ rows of $H^{(d-1)}(\mathbf{x})$, whose value is equal to $H_1(\mathbf{x})$, and the one determined by the rows $\{1,\dots,d-2,d\}$ of $H^{(d-1)}(\mathbf{x})$, which is equal to 1. Therefore, by the Cauchy-Binet formula we have

$$\det B^{(d-1)}(\mathbf{x}) = H_1(\mathbf{x}) \cdot \det B(\mathbf{x}) + \det \begin{pmatrix} 1 & x_1 & \cdots & x_1^{d-3} & x_1^{d-1} \\ 1 & x_2 & \cdots & x_2^{d-3} & x_2^{d-1} \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & x_{d-1} & \cdots & x_{d-1}^{d-3} & x_{d-1}^{d-1} \end{pmatrix}.$$

Combining (25) with, e.g., [6, Lemma 2.1] or [7, Exercise 280], we obtain the following identity:

$$\begin{aligned} 0 &= H_1(\mathbf{x}) \cdot \det B(\mathbf{x}) + (x_1 + \cdots + x_{d-1}) \det B(\mathbf{x}) \\ &= \det B(\mathbf{x}) \cdot \big((\#I_1+1)\lambda_1 + \cdots + (\#I_{d-1}+1)\lambda_{d-1}\big). \end{aligned}$$

From (21) we see that $B(\mathbf{x})$ is a nonsingular matrix. Hence we conclude that

$$(\#I_1+1)\lambda_1 + \cdots + (\#I_{d-1}+1)\lambda_{d-1} = 0 \tag{26}$$

holds for every $\lambda \in \mathbb{A}^{d-1}$ with $\lambda_i \neq \lambda_j$ for $i \neq j$, and thus for every $\lambda \in \mathbb{A}^{d-1}$. Substituting 1 for λ_i in (26), the statement of the lemma follows. □

Remark 4.4. The conclusion in the statement of Lemma 4.3, namely that $p|(k+d)$, is actually a rather weak consequence of (26). In addition to such a conclusion, (26) establishes strong restrictions on the partitions $\mathcal{I}$ of the linear varieties $\mathcal{L}_{\mathcal{I}}$ contained in the singular locus Σ_d of a hypersurface V_d with $\dim \Sigma_d = d-1$. In particular, fix $i \in \{1,\dots,d-1\}$ and substitute 1 for λ_i and 0 for any λ_j with $j \neq i$. Then (26) implies $\#I_i \equiv -1 \mod p$.

Now we are ready to prove the main result of this section, namely that the assumption $p > d+1$ implies that any member V_f of the family of hypersurfaces which are relevant for the nonexistence of deep holes has singular locus of dimension at most $d-2$.

Proposition 4.5. *Let be given positive integers k and d with $k > d$, $p > d+1$, and $q-1 > k+d$. Assume further that $p|(k+d)$ holds. Let $\mathbf{w}_d \in \mathbb{F}_q^{q-1}$ be the* *word generated by the polynomial $T^{k+d} \in \mathbb{F}_q[T]$. Then $\mathbf{w}_d$ is not a deep hole of the standard Reed–Solomon code C of dimension k over $\mathbb{F}_q$.*

Proof. Write $q := p^s$. The inequality $q - 1 > k + d \geq p$ implies $s > 1$. Consider the trace mapping $\mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p} : \mathbb{F}_q \to \mathbb{F}_p$ defined by $\mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha) = \sum_{i=0}^{s-1} \alpha^{p^i}$. It is well–known that $\mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}$ is a surjective $\mathbb{F}_p$–linear morphism. This in particular implies that there exist p^{s-1} elements in $\mathbb{F}_q$ whose trace equals zero. Write $k + d = p\,l$. Then the condition $q - 1 > k + d$ implies $p^{s-1} > l$, which in turn shows that there exist l pairwise–distinct elements $b_1 \ldots , b_l \in \mathbb{F}_q^*$ with $\mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(b_i) = 0$.

Since $\mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(b_i) = 0$ holds for $1 \leq i \leq l$, by [5, Theorem 3] it follows that the Artin–Schreier polynomial $g_{b_i} := T^p - T - b_i \in \mathbb{F}_q[T]$ has p distinct roots in $\mathbb{F}_q^*$ for $1 \leq i \leq l$. Furthermore, since $b_i \neq b_j$ holds for $i \neq j$, we easily deduce that g_{b_i} and g_{b_j} have no common roots. Therefore, the polynomial

$$g := \prod_{i=1}^{l} g_{b_i} = \prod_{i=1}^{l} (T^p - T - b_i) \tag{27}$$

has $p\,l$ distinct roots in $\mathbb{F}_q^*$. On the other hand,

$$g = T^{k+d} - lT^{p(l-1)+1} + \mathcal{O}(T^{p(l-1)}) = T^{k+d} + h(T),$$

where $h := lT^{p(l-1)+1} + \mathcal{O}(T^{p(l-1)})$ has degree at most $p(l - 1) + 1$. Denote by $\mathbf{w}_h \in \mathbb{F}_q^{q-1}$ the word generated by the polynomial h. Since

$$p(l - 1) + 1 = k + d - p + 1 \leq k + d - (d + 2) + 1 = k - 1$$

holds, we have that $\mathbf{w}_h$ is a codeword. The fact that the polynomial g of (27) has $p\,l > k$ distinct roots in $\mathbb{F}_q^*$ implies $\mathsf{d}(\mathbf{w}_d, \mathbf{w}_h) < q - 1 - k$ holds, where d denotes the Hamming distance of $\mathbb{F}_q^{q-1}$. We conclude that $\mathbf{w}_d$ is not a deep hole of the code C. This finishes the proof of the proposition. □

5. Main results

We have shown that, if a given hypersurface V_f has a q–rational point with nonzero, pairwise–distinct coordinates, then there are no deep holes of the standard Reed–Solomon code C of dimension k over $\mathbb{F}_q$. Combining the results of Sections 3 and 4, we will obtain a lower bound for the number of q–rational points of V_f and an upper bound for the number of q–rational points of V_f with a zero coordinate or at least two equal coordinates. From these results we will establish a lower bound for the number of q–rational points of V_f as required. This will allow us to obtain conditions on q, d and k which imply the nonexistence of deep holes of the standard Reed–Solomon code C.

As before, let be given positive integers d and k with $k > d$ and $q - 1 > k + d$ and a polynomial $f := T^{k+d} + f_{d-1}T^{k+d-1} + \cdots + f_0T^k \in \mathbb{F}_q[T]$. Consider the hypersurface $V_f \subset \mathbb{A}^{k+1}$ defined by the polynomial $H_f \in \mathbb{F}_q[X_1, \ldots X_{k+1}]$ associated to f. According to Corollaries 3.3 and 3.5, the hypersurface V_f has a singular locus of dimension at most $d - 1$ and is absolutely irreducible.

5.1. Estimates on the number of q–rational points of hypersurfaces.

In what follows, we shall use an estimate on the number of q–rational points of a projective $\mathbb{F}_q$–hypersurface due to S. Ghorpade and G. Lachaud ([8]; see also

[9]). In [8, Theorem 6.1] the authors prove that, for an absolutely irreducible $\mathbb{F}_q$–hypersurface $V \subset \mathbb{P}^{m+1}$ of degree $d \geq 2$ and singular locus of dimension at most $s \geq 0$, the number $\#V(\mathbb{F}_q)$ of q–rational points of V satisfies the estimate

$$|\#V(\mathbb{F}_q) - p_m| \leq b_{m-s-1,d}\, q^{\frac{m+s+1}{2}} + C_{s,m}(V) q^{\frac{m+s}{2}}, \tag{28}$$

where $p_m := q^m + q^{m-1} + \cdots + q + 1$ is the cardinality of $\mathbb{P}^m(\mathbb{F}_q)$. Here $b_{m-s-1,d}$ is the $(m-s-1)$th primitive Betti number of any nonsingular hypersurface in $\mathbb{P}^{m-s}$ of degree d, which is upper bounded by

$$b_{m-s-1,d} \leq \frac{d-1}{d}\big((d-1)^{m-s} - (-1)^{m-s}\big) \leq (d-1)^{m-s}, \tag{29}$$

while $C_{s,m}(V)$ is the sum

$$C_{s,m}(V) := \sum_{i=m}^{m+s} b_{i,\ell}(V) + \varepsilon_i,$$

where $b_{i,\ell}(V)$ denotes the ith ℓ–adic Betti number of V for a prime ℓ different from $p := \mathrm{char}(\mathbb{F}_q)$ and $\varepsilon_i := 1$ for even i and $\varepsilon_i := 0$ for odd i. In [8, Proposition 5.1] it is shown that

$$C_{s,m}(V) \leq 18(d+3)^{m+2}. \tag{30}$$

This bound is a particular case of a bound for singular projective complete intersections. Nevertheless, in our case it is possible to slightly improve (30).

Lemma 5.1. *If $V \subset \mathbb{P}^{m+1}$ is an absolutely irreducible hypersurface of degree $d \geq 2$ and singular locus of dimension at most $s \geq 0$, then we have the following bound:*

$$C_{s,m}(V) \leq 6(d+2)^{m+2}. \tag{31}$$

Proof. Let $E(n,d)$ be a universal upper bound for the Euler characteristic of any affine hypersurface $\mathcal{V} \subset \mathbb{A}^n$ defined by the vanishing of a polynomial $F_{\mathcal{V}} \in \overline{\mathbb{F}}_q[X_1, \ldots, X_n]$ of degree at most d, and let $A(n,d)$ be the number

$$A(n,d) := E(n,d) + 2 + 2\sum_{j=1}^{n-1} E(j,d).$$

Then the Katz inequality [12, Theorem 3] implies that

$$C_{s,m}(V) \leq s + 2 + \sum_{n=1}^{m+1} \big(1 + A(n+1, d+1)\big). \tag{32}$$

As a consequence of [1, Theorem 5.27] it follows that an admissible choice for $E(n,d)$ is the following:

$$E(n,d) := \frac{2}{d}\big((d+1)^{n+1} - 1\big).$$

Elementary calculations show that, for such a choice of $E(n,d)$, we have

$$\begin{aligned} A(n,d) &= 2 + \frac{2}{d^2}\big((d+1)^{n+1}(d+2) - (2d^2 + d(2n+3) + 2)\big) \\ &\leq 2 + 2\frac{(d+2)}{d^2}\big((d+1)^{n+1} - 2d\big). \end{aligned}$$

Combining this inequality with (32) we obtain

$$C_{s,m}(V) \leq m + 1 + \sum_{n=1}^{m+1} \Big(3 + 2\frac{(d+3)}{(d+1)^2}\big((d+2)^{n+2} - 2d - 2\big)\Big) \leq 6(d+2)^{m+2}.$$

This finishes the proof of the lemma. □

Combining (28) with (29) and Lemma 5.1 we obtain an explicit upper bound for the number of q–rational points of singular projective $\mathbb{F}_q$–hypersurfaces. More precisely, if $V\subset\mathbb{P}^{m+1}$ is an absolutely irreducible $\mathbb{F}_q$–hypersurface of degree $d\geq 2$ and singular locus of dimension at most $s\geq 0$, then the number of q–rational points of V satisfies the estimate

$$|\#V(\mathbb{F}_q)-p_m|\leq(d-1)^{m-s}\,q^{\frac{m+s+1}{2}}+6(d+2)^{m+2}q^{\frac{m+s}{2}}. \tag{33}$$

The first step towards our main result is to obtain a lower bound on the number of q–rational points of the hypersurface V_f. For this purpose, combining Corollary 3.5 and [13, Chapter I, Proposition 5.17] we conclude that the projective closure $\mathrm{pcl}(V_f)\subset\mathbb{P}^{k+1}$ of V_f is an absolutely irreducible hypersurface which is defined over $\mathbb{F}_q$. Furthermore, from Corollary 3.3 and Proposition 3.4 we deduce that the singular locus of $\mathrm{pcl}(V_f)$ has dimension at most $d-1$. Therefore from (33) we deduce the following estimate:

$$|\#\mathrm{pcl}(V_f)(\mathbb{F}_q)-p_k|\leq(d-1)^{k-d+1}\,q^{\frac{k+d}{2}}+6(d+2)^{k+2}q^{\frac{k+d-1}{2}}. \tag{34}$$

Our next result provides a lower bound on the number of q–rational zeros of the affine hypersurface V_f.

Proposition 5.2. *Let be given positive integers d and k with $k>d\geq 2$ and $q-1>k+d$. Then the number of q–rational points of the hypersurface V_f satisfies the following inequality:*

$$\#V_f(\mathbb{F}_q)\geq q^k-2(d-1)^{k-d+1}q^{\frac{k+d}{2}}-7(d+2)^{k+2}q^{\frac{k+d-1}{2}}.$$

Proof. Since we are interested in the q–rational points of V_f, we discard the points of $\mathrm{pcl}(V_f)(\mathbb{F}_q)$ lying in the hyperplane at infinity $\{X_0=0\}$. Since $\mathrm{pcl}(V_f)$ is the zero locus of the polynomial $H_f^h=H_d+f_{d-1}H_{d-1}X_0+\cdots+f_0X_0^d\in\mathbb{F}_q[X_0,\ldots,X_{k+1}]$, we conclude

$$\#\big(\mathrm{pcl}(V_f)(\mathbb{F}_q)\cap\{X_0=0\}\big)=\#\{\mathbf{x}\in\mathbb{P}^k(\mathbb{F}_q):H_d(\mathbf{x})=0\}.$$

According to Proposition 3.4, the projective $\mathbb{F}_q$–hypersurface $V_f^\infty\subset\mathbb{P}^k$ defined by H_d has a singular locus of dimension at most $d-2$. Applying (33) we obtain

$$|\#V_f^\infty(\mathbb{F}_q)-p_{k-1}|\leq(d-1)^{k-d+1}\,q^{\frac{k+d-2}{2}}+6(d+2)^{k+1}\,q^{\frac{k+d-3}{2}}. \tag{35}$$

Combining (34) and (35) we have:

$$\begin{aligned}\#V_f(\mathbb{F}_q)-q^k&=\big(\#\mathrm{pcl}(V_f)(\mathbb{F}_q)-p_k\big)-\big(\#V_f^\infty(\mathbb{F}_q)-p_{k-1}\big)\\&\geq-(d-1)^{k-d+1}q^{\frac{k+d}{2}}(1+q^{-1})-6(d+2)^{k+2}q^{\frac{k+d-1}{2}}\big(1+(q(d+2))^{-1}\big).\end{aligned}$$

From this lower bound the inequality of the statement easily follows. □

Next we obtain an upper bound on the number of q–rational points of the hypersurface V_f which are not useful in connection with the existence of deep holes, namely those with a zero coordinate or at least two equal coordinates. We begin with the case of the points with a zero coordinate.

Proposition 5.3. *With hypotheses as in Proposition 5.2, the number N_1 of q–rational points of V_f with a zero coordinate satisfies the following inequality:*

$$N_1\leq(k+1)\left(q^{k-1}+2(d-1)^{k-d}q^{\frac{k+d-1}{2}}+7(d+2)^{k+1}q^{\frac{k+d-2}{2}}\right).$$

Proof. Let $\mathbf{x} := (x_1, \dots, x_{k+1})$ be a point of V_f with a zero coordinate. Without loss of generality we may assume $x_{k+1} = 0$. Hence, $\mathbf{x}$ is a q–rational point of the intersection $W_{k+1} := V_f \cap \{X_{k+1} = 0\}$. Observe that W_{k+1} is the $\mathbb{F}_q$–hypersurface of the linear space $\{X_{k+1} = 0\}$ defined by the polynomial $G_f(\Pi_1^k, \dots, \Pi_d^k)$, where $\Pi_1^k, \dots, \Pi_d^k$ are the first d elementary symmetric polynomials of the ring $\mathbb{F}_q[X_1, \dots, X_k]$. Then Theorem 3.1 shows that W_{k+1} has a singular locus of dimension at most $d - 1$. Furthermore, Proposition 3.4 implies that the singular locus of W_{k+1} at infinity has dimension at most $d - 2$. As a consequence, arguing as in the proof of Proposition 5.2 we obtain

$$\begin{aligned}\#W_{k+1}(\mathbb{F}_q) - q^{k-1} &= \big(\#\mathrm{pcl}(W_{k+1})(\mathbb{F}_q) - p_{k-1}\big) - \big(\#W_{k+1}^{\infty}(\mathbb{F}_q) - p_{k-2}\big) \\ &\leq (d-1)^{k-d} q^{\frac{k+d-1}{2}} + 6(d+2)^{k+1} q^{\frac{k+d-2}{2}} \\ &\quad + (d-1)^{k-d} q^{\frac{k+d-3}{2}} + 6(d+2)^{k} q^{\frac{k+d-4}{2}}.\end{aligned}$$

Therefore, we have the upper bound

$$\#W_{k+1}(\mathbb{F}_q) \leq q^{k-1} + 2(d-1)^{k-d} q^{\frac{k+d-1}{2}} + 7(d+2)^{k+1} q^{\frac{k+d-2}{2}}. \tag{36}$$

Adding the upper bounds of the q–rational points of the varieties $W_i := V_f \cap \{X_i = 0\}$ for $1 \leq i \leq k+1$, the proposition follows. □

Next we consider the number of q–rational points of V_f with two equal coordinates.

Proposition 5.4. *With hypotheses as in Proposition 5.2, the number N_2 of q–rational points of V_f with at least two equal coordinates satisfies the following inequality:*

$$N_2 \leq \frac{(k+1)k}{2} \Big(q^{k-1} + 2(d-1)^{k-d} q^{\frac{k+d-1}{2}} + 7(d+2)^{k+1} q^{\frac{k+d-2}{2}} \Big).$$

Proof. Let $\mathbf{x} := (x_1, \dots, x_{k+1}) \in V_f(\mathbb{F}_q)$ be a point having two distinct coordinates with the same value. Without loss of generality we may assume that $x_k = x_{k+1}$ holds. Then $\mathbf{x}$ is a q–rational point of the hypersurface $W_{k,k+1} \subset \{X_k = X_{k+1}\}$ defined by the polynomial $G_f(\Pi_1^*, \dots, \Pi_d^*) \in \mathbb{F}_q[X_1, \dots, X_k]$, where $\Pi_i^* := \Pi_i(X_1, \dots, X_k, X_k)$ is the polynomial of $\mathbb{F}_q[X_1, \dots, X_k]$ obtained by substituting X_k for X_{k+1} in the ith elementary symmetric polynomial of $\mathbb{F}_q[X_1, \dots, X_{k+1}]$. Observe that

$$\Pi_i^* = \Pi_i^{k-1} + 2X_k \cdot \Pi_{i-1}^{k-1} + X_k^2 \cdot \Pi_{i-2}^{k-1} \tag{37}$$

where Π_j^l denotes the jth elementary symmetric polynomial of $\mathbb{F}_q[X_1, \dots, X_l]$ for $1 \leq j \leq d$ and $1 \leq l \leq k+1$.

We claim that the singular locus of $\mathrm{pcl}(W_{k,k+1})$ and the singular locus of $W_{k,k+1}$ at infinity have dimension at most $d-1$ and $d-2$, respectively. In order to show this claim, we first assume that the characteristic p of $\mathbb{F}_q$ is greater than 2. Then, using (37) it can be proved that all the maximal minors of the Jacobian matrix $(\partial \Pi_i^* / \partial X_j)_{1 \leq i \leq d, 1 \leq j \leq k}$ are equal, up to multiplication by a nonzero constant, to the corresponding minors of the Jacobian matrix $(\partial \Pi_i^k / \partial X_j)_{1 \leq i \leq d, 1 \leq j \leq k}$. Then the proofs of Theorem 3.1 and Proposition 3.4 go through with minor corrections and show our claim.

Now assume $p = 2$. From (37) we see that the first partial derivative of Π_j^* with respect to X_k is equal to zero. Furthermore, it is easy to see that the nonzero $(d \times d)$–minor of the Jacobian matrix $(\partial \Pi_i^* / \partial X_j)_{1 \leq i \leq d, 1 \leq j \leq k}$ determined by the columns $1 \leq i_1 < i_2 < \cdots < i_d \leq k-1$ equals the corresponding nonzero minor of $(\partial \Pi_i^{k-1}/\partial X_j)_{1\leq i\leq d, 1\leq j\leq k}$. This shows that each nonzero maximal minor of $(\partial \Pi_i^*/\partial X_j)_{1\leq i\leq d,1\leq j\leq k}$ is a Vandermonde determinant depending on d of the indeterminates $X_1,\dots,X_{k-1}$. In particular, the vanishing of all these minors does not impose any condition on the variable X_k.

Let $\Sigma_{k,k+1}$ denote the singular locus of $W_{k,k+1}$. Arguing as in the proof of Theorem 3.1, we have the following inclusion (see Remark 3.2):

$$\Sigma_{k,k+1} \subset \bigcup_{\mathcal{I}} \mathcal{L}_{\mathcal{I}}, \tag{38}$$

where $\mathcal{I} := \{I_1,\dots,I_d\}$ runs over all the partitions of $\{1,\dots,k+1\}$ into d nonempty subsets $I_j \subset \{1,\dots,k+1\}$ such that $I_j \subset \{1,\dots,k-1\}$ for $1 \leq j \leq d-1$ and $I_d := \{k,k+1\}$, and $\mathcal{L}_{\mathcal{I}}$ is the linear variety

$$\mathcal{L}_{\mathcal{I}} := \mathrm{span}(\mathbf{v}^{(I_1)},\dots,\mathbf{v}^{(I_d)})$$

spanned by the vectors $\mathbf{v}^{(I_j)} := (v_1^{(I_j)},\dots,v_{k+1}^{(I_j)})$ defined by $v_m^{(I_j)} := 1$ for $m \in I_j$ and $v_m^{(I_j)} := 0$ for $m \notin I_j$. It follows that $\Sigma_{k,k+1}$ has dimension at most d, and if $\dim \Sigma_{k,k+1} = d$ holds, then it contains a linear variety $\mathcal{L}_{\mathcal{I}}$ as above.

Now we show that $\Sigma_{k,k+1}$ has dimension at most $d-1$. Arguing by contradiction, suppose that $\Sigma_{k,k+1}$ has dimension d. Following the proof of Theorem 4.2 we conclude that f is the monomial T^{k+d}, and thus $H_f = H_d$ holds. Fix $\mathcal{I} := \{I_1,\dots,I_d\}$ as above and consider the corresponding d–dimensional linear variety $\mathcal{L}_{\mathcal{I}}$. We claim that $\mathcal{L}_{\mathcal{I}}$ intersects $\Sigma_{k,k+1}$ properly. Observe that, combining this claim with (38), we easily deduce that $\dim \Sigma_{k,k+1} \leq d-1$, since each variety $\mathcal{L}_{\mathcal{I}}$ is absolutely irreducible and each irreducible component of $\Sigma_{k,k+1}$ is a proper subvariety of a suitable $\mathcal{L}_{\mathcal{I}}$. This contradicts our supposition $\dim \Sigma_{k,k+1} = d$, showing thus that $\dim \Sigma_{k,k+1} \leq d-1$ holds.

In order to prove our claim, consider the line $\ell_\lambda := \{\mathbf{v}_\lambda := (0,\dots,0,\lambda,\lambda) \in \mathbb{A}^{k+1} : \lambda \in \mathbb{A}^1\} \subset \mathcal{L}_{\mathcal{I}}$. Observe that $\ell_\lambda \cap \Sigma_{k,k+1} = \{\mathbf{v}_\lambda \in \mathbb{A}^{k+1} : H_d(\mathbf{v}_\lambda) = 0, \nabla H_d(\mathbf{v}_\lambda) = \mathbf{0}\}$. From the identities $\Pi_j(\mathbf{v}_\lambda) = 0$ $(j \notin \{0,2\})$ and $\Pi_2(\mathbf{v}_\lambda) = \lambda^2$ and Proposition 2.2, we conclude that $H_d(\mathbf{v}_\lambda) = \pm\lambda^d$ for even d and $H_{d-1}(\mathbf{v}_\lambda) = \pm\lambda^{d-1}$ for odd d. Furthermore, from Lemma 4.1 we obtain $(\partial H_d/\partial X_1)(\mathbf{v}_\lambda) = H_{d-1}(\mathbf{v}_\lambda) = \pm\lambda^{d-1}$ for odd d. In both cases, the identities $H_d(\mathbf{v}_\lambda) = (\partial H_d/\partial X_1)(\mathbf{v}_\lambda) = 0$ imply $\lambda = 0$. This shows that $\ell_\lambda \subset \mathcal{L}_{\mathcal{I}}$ intersects properly $\Sigma_{k,k+1}$ and shows our claim.

Finally, arguing as in Proposition 3.4 we conclude that the singular locus of $W_{k,k+1}$ at infinity has dimension at most $d-2$.

Summarizing, we have that, independently of the characteristic p of $\mathbb{F}_q$, the singular locus of $\mathrm{pcl}(W_{k,k+1})$ and the singular locus of $W_{k,k+1}$ at infinity have dimension at most $d-1$ and $d-2$. Then, following the proof of Proposition 5.3 we obtain:

$$\#W_{k,k+1}(\mathbb{F}_q) \leq q^{k-1} + 2(d-1)^{k-d} q^{\frac{k+d-1}{2}} + 7(d+2)^{k+1} q^{\frac{k+d-2}{2}}. \tag{39}$$

From (39) we deduce the statement of the proposition. □

5.2. Results of nonexistence of deep holes. Now we are ready to prove the main results of this paper. Fix q, k and $d \geq 3$ with $q-1 > k+d$ and consider the standard Reed–Solomon code C of dimension k over $\mathbb{F}_q$. From Section 1 we have that a polynomial $f := T^{k+d} + f_{d-1}T^{k+d-1} + \cdots + f_0 T^k$ does not generate a deep hole of the code C if and only if the corresponding hypersurface $V_f \subset \mathbb{A}^{k+1}$ has a q–rational point with nonzero, pairwise–distinct coordinates. Combining Propositions

5.2, 5.3 and 5.4 we conclude that the number N of such points satisfies the following inequality:

$$\begin{aligned}N \geq q^k - \frac{(k+1)(k+2)}{2}q^{k-1} - 2(d-1)^{k-d}q^{\frac{k+d}{2}}\left(d-1+\frac{(k+1)(k+2)}{2q^{\frac{1}{2}}}\right)\\ -7(d+2)^{k+1}q^{\frac{k+d-1}{2}}\left(d+2+\frac{(k+1)(k+2)}{2q^{\frac{1}{2}}}\right).\end{aligned} \tag{40}$$

Therefore, the polynomial f does not generate a deep hole of the code C if the right–hand side of (40) is a positive number.

Suppose that q, k and $d \geq 3$ satisfy the following conditions:

$$q > (k+1)^2, \quad k > 3d. \tag{41}$$

Since $k \geq 10$, it follows that $\frac{3}{4}(k+1)(k+2) \leq (k+1)^2 < q$ holds. Therefore, we have $q - \frac{1}{2}(k+1)(k+2) > q/3$, which implies

$$q^k - \frac{(k+1)(k+2)}{2}q^{k-1} = q^{k-1}\left(q - \frac{(k+1)(k+2)}{2}\right) > \frac{q^k}{3}.$$

Hence, the right–hand side of (40) is positive if the following condition holds:

$$\begin{aligned}\frac{q^k}{3} \quad \geq \quad & 2(d-1)^{k-d}q^{\frac{k+d}{2}}\left(d-1+\frac{(k+1)(k+2)}{2q^{\frac{1}{2}}}\right)\\ & +7(d+2)^{k+1}q^{\frac{k+d-1}{2}}\left(d+2+\frac{(k+1)(k+2)}{2q^{\frac{1}{2}}}\right).\end{aligned} \tag{42}$$

Taking into account that $k+1 < q^{\frac{1}{2}}$, we conclude that (42) can be replaced by the following condition:

$$\frac{q^k}{3} \geq 2(d-1)^{k-d}q^{\frac{k+d}{2}}\left(d-1+\tfrac{k+2}{2}\right) + 7(d+2)^{k+1}q^{\frac{k+d-1}{2}}\left(d+2+\tfrac{k+2}{2}\right).$$

From $d \leq \frac{k-1}{3}$ we obtain $d+2+\frac{k+2}{2} \leq k+1$, and therefore we conclude that the right–hand side of (40) is positive if

$$\frac{q^k}{3} \geq 2(d-1)^{k-d}(k-2)q^{\frac{k+d}{2}} + 7(d+2)^{k+1}(k+1)q^{\frac{k+d-1}{2}},$$

or equivalently if

$$q^k \geq 6(d-1)^{k-d}(k-2)q^{\frac{k+d}{2}} + 21(d+2)^{k+1}(k+1)q^{\frac{k+d-1}{2}}, \tag{43}$$

holds. Furthermore, this condition is in turn implied by the following conditions:

$$\frac{q^k}{8} \geq 6(d-1)^{k-d}(k-2)q^{\frac{k+d}{2}}, \quad \frac{7q^k}{8} \geq 21(d+2)^{k+1}(k+1)q^{\frac{k+d-1}{2}},$$

which can be rewritten as

$$q^k \geq 48(d-1)^{k-d}(k-2)q^{\frac{k+d}{2}}, \quad q^k \geq 24(d+2)^{k+1}(k+1)q^{\frac{k+d-1}{2}}. \tag{44}$$

The first inequality is equivalent to the following inequality:

$$q \geq (48(k-2))^{\frac{2}{k-d}}(d-1)^2.$$

From (41) one easily concludes that $3(k-d) \geq 2k+1$ holds. Since the function $k \mapsto \big(48(k-2)\big)^{6/(2k+1)}$ is decreasing, taking into account that $k \geq 10$ holds we deduce that a sufficient condition for the fulfillment of the inequality above is

$$q > 6d^2. \tag{45}$$

Next we consider the second inequality of (44). First, we observe that this inequality can be expressed as follows:

$$q > (24(k+1))^{\frac{2}{k-d+1}} \left(\frac{d+2}{d}\right)^{2+\frac{2d}{k-d+1}} d^{2+\frac{2d}{k-d+1}}. \tag{46}$$

From (41) we deduce $3(k-d+1) \geq 2k+4$. Taking into account that the function $k \mapsto \big(24(k+1)\big)^{3/(k+2)}$ is decreasing, in particular for $k \geq 12$ (and thus for $d \geq 4$), we see that (46) is satisfied if the following condition holds:

$$q > 14\, d^{2+2d/(k-d)}. \tag{47}$$

Combining (41), (45) and (47) we conclude that (41) and (47) yield a sufficient condition for the nonexistence of deep holes. Finally, starting from (40) one easily sees that (41) and (47) yield a sufficient condition for the nonexistence of deep holes for $d = 3$. As a consequence, we have the following result.

Theorem 5.5. *Let k and d be integers with $k > d \geq 3$ and $q - 1 > k + d$, and let C be the standard Reed–Solomon code of dimension k over $\mathbb{F}_q$. Let be given a real number ϵ with $0 < \epsilon < 1$ and let $\mathbf{w}$ be a word generated by a polynomial $f \in \mathbb{F}_q[T]$ of degree $k + d$. If the conditions*

$$q > \max\{(k+1)^2, 14\, d^{2+\epsilon}\}, \quad k \geq d\Big(\frac{2}{\epsilon} + 1\Big)$$

hold, then $\mathbf{w}$ is not a deep hole of C.

We remark that in [15] it is shown that, for $d = 1$, $k > 2$ and $q > k+3$, polynomials of degree $k+1$ do not generate deep holes of the standard Reed–Solomon code C. On the other hand, a similar result as in Theorem 5.5 can be obtained for $d = 2$ with our approach, namely that for a suitable constant $M_1 > 14$, if the conditions $q > \max\{(k+1)^2, M_1\, 2^{2+\epsilon}\}$ and $k \geq 2(2/\epsilon + 1)$ hold, then no polynomial of degree $k+2$ generates a deep hole of C.

5.3. NONEXISTENCE OF DEEP HOLES FOR $\mathrm{char}(\mathbb{F}_q) > d + 1$.

Finally, we briefly indicate what we obtain under the assumption that the characteristic p of $\mathbb{F}_q$ satisfies the inequality $p > d+1$. Fix q, k and $d \geq 3$ with $q-1 > k+d$, $k > d$ and $p > d+1$ and consider the standard Reed–Solomon code C of dimension k over $\mathbb{F}_q$.

Fix $f := T^{k+d} + f_{d-1}T^{k+d-1} + \cdots + f_0T^k \in \mathbb{F}_q[T]$. First suppose that the singular locus of the hypersurface V_f associated to f has dimension $d-1$. By Theorem 4.2 we have that f is the monomial T^{k+d}. Furthermore, from Lemma 4.3 it follows that $p|(k+d)$. Then Proposition 4.5 shows that the monomial T^{k+d} does not generate a deep hole of C. Therefore, we may assume without loss of generality that V_f has a singular locus of dimension at most $d-2$. As a consequence, arguing as in the proofs of Propositions 5.2, 5.3 and 5.4 we obtain the following bounds:

$$\begin{aligned}
\#V_f(\mathbb{F}_q) &\geq q^k - 2(d-1)^{k-d+2} q^{\frac{k+d-1}{2}} - 7(d+2)^{k+2} q^{\frac{k+d-2}{2}}, \\
N_1 &\leq \frac{(k+1)(k+2)}{2}\Big(q^{k-1} + 2(d-1)^{k-d+1} q^{\frac{k+d-2}{2}} + 7(d+2)^{k+1} q^{\frac{k+d-3}{2}}\Big),
\end{aligned}$$

where N_1 denotes the number of q–rational points of V_f having a zero coordinate or at least two equal coordinates. Hence we have that the number N of q–rational points of V_f with nonzero, pairwise–distinct coordinates satisfies the following inequality:

$$
\begin{aligned}
N \geq q^k - \frac{(k+1)(k+2)}{2}q^{k-1} - 2(d-1)^{k-d+1}q^{\frac{k+d-1}{2}}\left(d-1+\frac{(k+1)(k+2)}{2q^{\frac{1}{2}}}\right)\\
-7(d+2)^{k+1}q^{\frac{k+d-2}{2}}\left(d+2+\frac{(k+1)(k+2)}{2q^{\frac{1}{2}}}\right).
\end{aligned}
\tag{48}
$$

Suppose that q, k and $d \geq 4$ satisfy the following conditions:

$$q > (k+1)^2, \quad k > 3(d-1). \tag{49}$$

Then the right–hand side of (48) is positive if

$$q^k \geq \max\left\{48(d-1)^{k-d+1}(k-1)q^{\frac{k+d-1}{2}},\, 24(d+2)^{k+1}(k+2)q^{\frac{k+d-2}{2}}\right\}. \tag{50}$$

With similar arguments as in the proof of Theorem 5.5 we conclude that (50) is satisfied if the following condition holds:

$$q > 14\, d^{2+(2d-2)/(k-d+2)}. \tag{51}$$

On the other hand, starting from (48) one easily sees that (51) yields a sufficient condition for the nonexistence of deep holes for $d = 3$. Summarizing, we have the following result.

Theorem 5.6. *Let k and d be integers with $k > d \geq 3$ and $q-1 > k+d$, and let C be the standard Reed–Solomon code of dimension k over $\mathbb{F}_q$. Let be given a real number ϵ with $0 < \epsilon < 1$ and let $\mathbf{w}$ be a word generated by a polynomial $f \in \mathbb{F}_q[T]$ of degree $k+d$. If $\mathrm{char}(\mathbb{F}_q) > d+1$ and the conditions*

$$q > \max\{(k+1)^2, 14\, d^{2+\epsilon}\}, \quad k \geq (d-1)\Big(\frac{2}{\epsilon}+1\Big)$$

hold, then $\mathbf{w}$ is not a deep hole of C.

Acknowledgments

The authors are pleased to thank an anonymous referee for his/her careful and constructive report, which helped to significantly improve the presentation of the results of this paper.

References

[1] A. Adolphson and S. Sperber, *On the degree of the L-function associated with an exponential sum*, Compos. Math., **68** (1988), 125–159.

[2] Y. Aubry and F. Rodier, *Differentially 4-uniform functions*, in "Arithmetic, Geometry, Cryptography and Coding Theory 2009" (eds. D. Kohel and R. Rolland), Amer. Math. Soc., (2010), 1–8.

[3] A. Cafure and G. Matera, *Improved explicit estimates on the number of solutions of equations over a finite field*, Finite Fields Appl., **12** (2006), 155–185.

[4] Q. Cheng and E. Murray, *On deciding deep holes of Reed-Solomon codes*, in "Theory and Applications of Models of Computation," Springer, Berlin, (2007), 296–305.

[5] R. Coulter and M. Henderson, *A note on the roots of trinomials over a finite field*, Bull. Austral. Math. Soc., **69** (2004), 429–432.

[6] T. Ernst, *Generalized Vandermonde determinants*, report 2000: 6 Matematiska Institutionen, Uppsala Universitet, 2000; available online at http://www2.math.uu.se/research/pub/Ernst1.pdf

[7] D. K. Faddeev and I. S. Sominskii, "Problems in Higher Algebra," Freeman, San Francisco, 1965.

[8] S. Ghorpade and G. Lachaud, *Étale cohomology, Lefschetz theorems and number of points of singular varieties over finite fields*, Mosc. Math. J., **2** (2002), 589–631.

[9] S. Ghorpade and G. Lachaud, *Number of solutions of equations over finite fields and a conjecture of Lang and Weil*, in "Number Theory and Discrete Mathematics" (eds. A.K. Agarwal et al.), Hindustan Book Agency, (2002), 269–291.

[10] V. Guruswami and A. Vardy, *Maximum-likelihood decoding of Reed-Solomon codes is NP-hard*, IEEE Trans. Inform. Theory, **51** (2005), 2249–2256.

[11] J. Heintz, *Definability and fast quantifier elimination in algebraically closed fields*, Theoret. Comput. Sci., **24** (1983), 239–277.

[12] N. Katz, *Sums of Betti numbers in arbitrary characteristic*, Finite Fields Appl., **7** (2001), 29–44.

[13] E. Kunz, "Introduction to Commutative Algebra and Algebraic Geometry," Birkhäuser, Boston, 1985.

[14] A. Lascoux and P. Pragracz, *Jacobian of symmetric polynomials*, Ann. Comb., **6** (2002), 169–172.

[15] J. Li and D. Wan, *On the subset sum problem over finite fields*, Finite Fields Appl., **14** (2008), 911–929.

[16] Y.-J. Li and D. Wan, *On error distance of Reed-Solomon codes*, Sci. China Ser. A, **51** (2008), 1982–1988.

[17] R. Lidl and H. Niederreiter, "Finite Fields," 2^{nd} edition, Addison-Wesley, Massachusetts, 1997.

[18] F. Rodier, *Borne sur le degré des polynômes presque parfaitement non-linéaires*, in "Arithmetic, Geometry, Cryptography and Coding Theory," Amer. Math. Soc., (2009), 169–181.

[19] I. R. Shafarevich, "Basic Algebraic Geometry: Varieties in projective space," Springer, Berlin, 1994.

[20] D. Wan, *Generators and irreducible polynomials over finite fields*, Math. Comp., **66** (1997), 1195–1212.

Received October 2010; revised December 2011.

E-mail address: acafure@ungs.edu.ar
E-mail address: gmatera@ungs.edu.ar
E-mail address: mprivitelli@conicet.gov.ar