DTU Library

A combinatorial approach to the number of solutions of systems of homogeneous polynomial equations over finite fields

Beelen, Peter; Datta, Mrinmoy; Ghorpade, Sudhir R.

[Link back to DTU Orbit](#)

A COMBINATORIAL APPROACH TO THE NUMBER OF SOLUTIONS OF SYSTEMS OF HOMOGENEOUS POLYNOMIAL EQUATIONS OVER FINITE FIELDS

PETER BEELEN, MRINMOY DATTA, AND SUDHIR R. GHORPADE

ABSTRACT. We give a complete conjectural formula for the number $e_r(d, m)$ of maximum possible $\mathbb{F}_q$-rational points on a projective algebraic variety defined by r linearly independent homogeneous polynomial equations of degree d in $m + 1$ variables with coefficients in the finite field $\mathbb{F}_q$ with q elements, when $d < q$. It is shown that this formula holds in the affirmative for several values of r. In the general case, we give explicit lower and upper bounds for $e_r(d, m)$ and show that they are sometimes attained. Our approach uses a relatively recent result, called the projective footprint bound, together with results from extremal combinatorics such as the Clements–Lindström Theorem and its variants. Applications to the problem of determining the generalized Hamming weights of projective Reed–Muller codes are also included.

2020 MATH. SUBJ. CLASS. Primary: 14G15, 11G25, 14G05; Secondary: 11T71, 94B27, 51E20.

KEY WORDS AND PHRASES. Finite field, projective algebraic variety, footprint bound, projective Reed–Muller code, generalzed Hamming weight.

1. INTRODUCTION

Fix a prime power q and positive integers r, d, m. Let $\mathbb{F}_q$ denote the finite field with q elements and $\mathbb{F}_q[x_0, \ldots, x_m]$ the polynomial ring in $m + 1$ variables $x_0, x_1, \ldots, x_m$ with coefficients in $\mathbb{F}_q$. For any homogeneous polynomials $F_1, \ldots, F_r$ in $\mathbb{F}_q[x_0, \ldots, x_m]$, let $V(F_1, \ldots, F_r)$ denote the closed subvariety of the projective m-space $\mathbb{P}^m$ (over an algebraic closure of $\mathbb{F}_q$) given by the vanishing of $F_1, \ldots, F_r$,

and let $V(F_1, \ldots, F_r)(\mathbb{F}_q)$ be the set of its $\mathbb{F}_q$-rational points, i.e., the set of all $\mathbb{F}_q$-rational common zeros in $\mathbb{P}^m$ of $F_1, \ldots, F_r$. Define

$$e_r(d, m) := \max_{F_1, \ldots, F_r} |V(F_1, \ldots, F_r)(\mathbb{F}_q)|, \tag{1}$$

where the maximum is over all possible families $\{F_1, \ldots, F_r\}$ of r linearly independent homogeneous polynomials of degree d in $\mathbb{F}_q[x_0, \ldots, x_m]$. Note that the condition on linear independence implies that r can be at most $\binom{m+d}{d}$. Note also that an obvious upper bound for $e_r(d, m)$ is p_m, where for $j \in \mathbb{Z}$, by p_j we denote $|\mathbb{P}^j(\mathbb{F}_q)|$, i.e., $\mathsf{p}_j := q^j + q^{j-1} + \cdots + q + 1$ if $j \geqslant 0$, and $\mathsf{p}_j := 0$ if $j < 0$.

Explicit determination of $e_r(d, m)$ is an open problem, in general, and it has been of some interest for about two decades. While it is easy to see that $e_r(1, m) = \mathsf{p}_{m-r}$ for $r \leqslant m + 1$ and $e_r(d, 1) = d - r + 1$ for $r \leqslant d + 1 \leqslant q$ (see for example [9, § 2.1]), the case of $r = 1$ is rather nontrivial. Here it was conjectured by M. Tsfasman that

$$e_1(d, m) = dq^{m-1} + \mathsf{p}_{m-2} \quad \text{for } d \leqslant q. \tag{2}$$

This was subsequently proved by Serre [18] and, independently, by Sørensen [19] in 1991. In the general case, an intricate formula for $e_r(d, m)$ for $d < q - 1$ was conjectured by Tsfasman and Boguslavsky (cf. [6], [10]), and this was proved in the affirmative by Boguslavsky [6] in 1997 for $r = 2$. The case of $r > 2$ remained open for a considerable time. Eventually, it was proved in [9] and [10] that the conjectural formula of Tsfasman and Boguslavsky is true if $r \leqslant m + 1$, and it can be false if $r > m + 1$. In [9], a new conjectural formula for $e_r(d, m)$ was proposed for many (but not all) values of r, namely for $r \leqslant \binom{m+d-1}{d-1}$. We will refer to this as the *incomplete conjecture*. To state it, let us first define an important combinatorial quantity whose genesis lies in the work of Heijnen and Pellikaan [12] related to an affine counterpart of the problem of finding $e_r(d, m)$. For $1 \leqslant r \leqslant \binom{m+d}{d}$, we define

$$H_r(d, m) := \sum_{i=1}^m \alpha_i q^{m-i}, \quad \text{where } (\alpha_1, \ldots, \alpha_m) \text{ is the } r^{\text{th}} \text{ element of } Q_{\leqslant d}^m,$$

and where $Q_{\leqslant d}^m$ denotes the collection, ordered in descending lexicographic order, of all m-tuples $(\beta_1, \ldots, \beta_m)$ of integers satisfying $0 \leqslant \beta_i < q$ for $i = 1, \ldots, m$ and $\beta_1 + \cdots + \beta_m \leqslant d$. For example, if $d < q$, then $H_1(d, m) = dq^{m-1}$ and $H_{\binom{m+d}{d}}(d, m) = 0$, since $(d, 0, \ldots, 0)$ and $(0, 0, \ldots, 0)$ are clearly the first and the last m-tuples of $Q_{\leqslant d}^m$ in descending lexicographic order. As a convention, we set

$$H_0(d, m) := q^m \text{ for } d, m \geqslant 0 \quad \text{and} \quad H_1(d, m) := 0 \text{ if } d = 0 \text{ or } m = 0. \tag{3}$$

In this way, $H_r(d, m)$ is defined for all nonnegative integers r, d, m with $r \leqslant \binom{m+d}{d}$. The "incomplete conjecture" of [9] can now be stated as follows.

$$e_r(d, m) = H_r(d-1, m) + \mathsf{p}_{m-1} \quad \text{for } 1 \leqslant r \leqslant \binom{m+d-1}{d-1} \text{ and } 1 \leqslant d < q. \tag{4}$$

For example, if $r = 1$, then this says that $e_1(d, m) = (d-1)q^{m-1} + \mathsf{p}_{m-1}$, which agrees with the Serre–Sørensen formula (2). Note also that (4) holds trivially when $d = 1$ or $m = 1$. Results of [9] prove (4) in the affirmative if $r \leqslant m+1$ and $d < q-1$. The validity of (4) was extended further in [4] to $r \leqslant \binom{m+2}{2}$ and $1 < d < q$. This,

then, is currently the best known general result as far as an explicit determination of $e_r(d, m)$ is concerned. Apart from this, the last few values of $e_r(d, m)$ were determined in [8] using the connection with coding theory (explained in Section 7) and the work of Sørensen [19]; more precisely, it was shown in [8, Thm. 4.7] that

$$e_{\binom{m+d}{d}-t}(d, m) = t \quad \text{for } t = 0, 1, \ldots, d. \tag{5}$$

We are now ready to describe the main results of this paper. First, we extend (4) to a conjectural formula for $e_r(d, m)$ for all permissible values of r, d, m with $d < q$. To state this "complete conjecture", let us first observe that

$$\binom{m+d}{d} = \binom{m+d-1}{d-1} + \binom{m+d-2}{d-1} + \cdots + \binom{d-1}{d-1} \tag{6}$$

and that for any positive integer $r < \binom{m+d}{d}$, there are unique integers i, j such that

$$r = \binom{m+d-1}{d-1} + \cdots + \binom{m+d-i}{d-1} + j, \ \ 0 \leqslant i \leqslant m, \text{ and } 0 \leqslant j < \binom{m+d-i-1}{d-1}.$$

By convention, and in accordance with (6), we set $i := m$ and $j := \binom{m+d-i-1}{d-1} = 1$ when $r = \binom{m+d}{d}$. With i and j thus defined (for a given value of r), the "complete conjecture" states that

$$e_r(d, m) = H_j(d-1, m-i) + \mathsf{p}_{m-i-1} \quad \text{for } 1 \leqslant r \leqslant \binom{m+d}{d} \text{ and } 1 \leqslant d < q. \tag{7}$$

Note that if $r < \binom{m+d-1}{d-1}$, then $i = 0$ and $j = r$, whereas if $r = \binom{m+d-1}{d-1}$, then $i = 1$ and $j = 0$. Thus (7) reduces to (4) in this case, thanks to our conventions. In particular, from [4, Thm. 5.3], we see that (7) holds in the affirmative if $r \leqslant \binom{m+2}{2}$. We provide further evidence for the "complete conjecture" in this paper by showing that it holds in the affirmative for an additional md values of r, namely for

$$r = \binom{m+d-1}{d-1} + \cdots + \binom{m+d-i}{d-1} - t, \quad \text{where } 1 \leqslant i \leqslant m \text{ and } 0 \leqslant t \leqslant d-1;$$

in fact, for r as above, we obtain $e_r(d, m) = \mathsf{p}_{m-i} + t$. These results are also valid when $i = m + 1$, but in view of (6), this case is already covered by (5). In the general case, we show that the conjectural formula is always a lower bound even when $d = q$, that is,

$$e_r(d, m) \geqslant H_j(d-1, m-i) + \mathsf{p}_{m-i-1} \quad \text{for } 1 \leqslant r \leqslant \binom{m+d}{d} \text{ and } 1 \leqslant d \leqslant q. \tag{8}$$

The conjectural formula (7) as well as the lower bound (8) for $e_r(d, m)$ can be described by the alternative formula

$$\mathsf{p}_{s_d-d} + \lfloor q^{s_{d-1}-d+1} \rfloor + \lfloor q^{s_{d-2}-d+2} \rfloor + \cdots + \lfloor q^{s_1-1} \rfloor,$$

where $s_1, \ldots, s_d$ are unique integers satisfying the d-binomial expansion

$$\binom{m+d}{d} - r = \binom{s_d}{d} + \binom{s_{d-1}}{d-1} + \cdots + \binom{s_1}{1} \quad \text{and} \quad s_d > s_{d-1} > \cdots > s_1 \geqslant 0.$$

We also find in this paper an explicit upper bound for $e_r(d, m)$ using methods from extremal combinatorics and a projective counterpart of $H_r(d, m)$, which we denote by $K_r(d, m)$. More precisely, we show that for $1 \leqslant r \leqslant \binom{m+d}{d}$ and $1 \leqslant d \leqslant q$,

$$e_r(d, m) \leqslant K_r(d, m), \quad \text{where} \quad K_r(d, m) := \sum_{i=0}^{m} a_i \mathsf{p}_{m-i-1}, \qquad (9)$$

and where $(a_0, a_1, \ldots, a_m)$ is the r-th element, in descending lexicographic order, of the set of all $(m + 1)$-tuples $(b_0, b_1, \ldots, b_m)$ of nonnegative integers satisfying $b_0 + b_1 + \cdots + b_m = d$. It is also shown that this upper bound is attained for several values of r. In turn, this plays a crucial role in ascertaining the validity of (7) for the additional md values of r mentioned earlier.

The determination of $e_r(d, m)$ is directly related to the determination of the generalized Hamming weights (also known as higher weights) of the projective Reed–Muller codes $\mathrm{PRM}_q(d, m)$, which go back to Lachaud [15]. This connection was explained in [8, §4] when $d \leqslant q$. We elucidate it further in Section 7 by noting that in general (when d can be larger than q), it is more natural to consider a variant of $e_r(d, m)$, called $\bar{e}_r(d, m)$, wherein one takes into account the vanishing ideal of $\mathbb{P}^m(\mathbb{F}_q)$. This also brings to the fore a basic notion of projective reduction, which was enunciated in [5]. We remark that the affine counterpart of the problem of determining $\bar{e}_r(d, m)$ corresponds to determining the generalized Hamming weights of Reed–Muller codes $\mathrm{RM}_q(d, m)$, and this has been solved by V. Wei [20] when $q = 2$, and by Heijnen and Pellikaan [12], in general. (See also [3].)

The methods used in proving the main results of this paper differ significantly from those in our earlier works such as [9] and [4]. Here we adopt a combinatorial approach and the groundwork for this has been laid in [5], where a *projective footprint bound* for the number of $\mathbb{F}_q$-rational points of arbitrary projective algebraic varieties defined over $\mathbb{F}_q$ was obtained. This groundwork is combined in this paper with methods from extremal combinatorics and a culmination of ideas such as the Kruskal–Katona Theorem, a lemma of Wei [20, Lem. 6], the Clements–Lindström Theorem, and a theorem of Heijnen [13, Appendix A] (see also [12, Thm. 5.7] and [3, Thm. 3.8]). These feed into the results in Sections 4, 5 and 6, which form the technical core of this paper. For a leisurely introduction to extremal combinatorics and some of the classical results mentioned above, one may refer to the book of Anderson [1].

2. A Lower Bound and a Conjecture

In this section, we shall prove the lower bound (8) and formally state our "complete conjecture" concerning $e_r(d, m)$. Recall that $e_r(d, m)$ is defined by (1) for positive numbers r, d, m with $r \leqslant \binom{m+d}{d}$. One can extend the definition to include the trivial cases when r or d or m is zero, or simply, set the following convention.

$$e_0(d, m) := \mathsf{p}_m \text{ for } d, m \geqslant 0 \quad \text{and} \quad e_1(d, m) := 0 \text{ if } d = 0 \text{ or } m = 0. \qquad (10)$$

Thus $e_r(d, m)$ is defined for all nonnegative integers r, d, m satisfying $r \leqslant \binom{m+d}{d}$.

In the remainder of this section, m denotes a positive integer and, as usual, $\mathbb{F}_q$ denotes the finite field with q elements.

2.1. Zeros of affine varieties over finite fields. Let r, d be any nonnegative integers. Given any polynomials $f_1, \ldots, f_r \in \mathbb{F}_q[x_1, \ldots, x_m]$, we shall denote by $Z(f_1, \ldots, f_r)(\mathbb{F}_q)$ the set of all $\mathbb{F}_q$-rational points of the affine algebraic variety in $\mathbb{A}^m$ (over an algebraic closure of $\mathbb{F}_q$) defined by $f_1, \ldots, f_r$; in other words,

$$Z(f_1, \ldots, f_r)(\mathbb{F}_q) = \{(a_1, \ldots, a_m) \in \mathbb{F}_q^m : f_j(a_1, \ldots, a_m) = 0 \text{ for all } j = 1, \ldots, r\}.$$

Note that if $r = 0$, then $Z(f_1, \ldots, f_r)(\mathbb{F}_q) = \mathbb{F}_q^m$. We shall now define a natural affine analogue of $e_r(d, m)$. For $0 \leqslant r \leqslant \binom{m+d}{d}$, we define

$$e_r^{\mathbb{A}}(d, m) := \max_{f_1, \ldots, f_r} |Z(f_1, \ldots, f_r)(\mathbb{F}_q)|,$$

where the maximum is taken over families of r linearly independent polynomials $f_1, \ldots, f_r$ of degree $\leqslant d$ in $\mathbb{F}_q[x_1, \ldots, x_m]$.

As explained in [4, §2.1], the result of Heijnen and Pellikaan [12, Thm. 5.10] in the case $d < q$ can be stated as follows. Here $H_r(d, m)$ is as defined in the introduction, including the conventions given in (3).

Theorem 2.1 (Heijnen–Pellikaan)**.** *If $0 \leqslant d < q$ and $0 \leqslant r \leqslant \binom{m+d}{d}$, then*

$$e_r^{\mathbb{A}}(d, m) = H_r(d, m).$$

A more general version of this result will be discussed later (in § 6.1).

2.2. A lower bound for $e_r(d, m)$. We begin by noting a simple and well-known fact whose proof is outlined for the sake of completeness.

Lemma 2.2. *Let d be a positive integer. Then*

$$\binom{m + d}{d} = \sum_{a=1}^{m+1} \binom{m + d - a}{d - 1}. \tag{11}$$

Moreover, for any nonnegative integer $r < \binom{m+d}{d}$, there are unique integers i, j with

$$r = j + \sum_{a=1}^{i} \binom{m + d - a}{d - 1}, \quad 0 \leqslant i \leqslant m, \quad \text{and} \quad 0 \leqslant j < \binom{m + d - i - 1}{d - 1}. \tag{12}$$

Proof. The identity in (11) follows easily from induction on m. If $0 \leqslant r < \binom{m+d}{d}$, then the largest nonnegative integer i such that $\sum_{a=1}^{i} \binom{m+d-a}{d-1} \leqslant r$ clearly satisfies $0 \leqslant i \leqslant m$, thanks to (11). Thus (12) holds with $j := r - \sum_{a=1}^{i} \binom{m+d-a}{d-1}$. $\square$

We remark that although m is assumed to be a fixed positive integer, the identity in (11) holds trivially also when $m = 0$, and this fact may be tacitly assumed in the sequel. Our next result is a general lower bound for $e_r(d, m)$ when $d \leqslant q$.

Theorem 2.3. *Let d, r be positive integers with $d \leqslant q$ and $r \leqslant \binom{m+d}{d}$, and let i, j be as in (12) if $r < \binom{m+d}{d}$, while $i := m$ and $j := \binom{m+d-i-1}{d-1} = 1$ if $r = \binom{m+d}{d}$. Then*

$$e_r(d, m) \geqslant H_j(d - 1, m - i) + \mathsf{p}_{m-i-1}.$$

Proof. If $r = \binom{m+d}{d}$, then clearly, $e_r(d, m) = 0$ and $H_1(d-1, m-m) + \mathsf{p}_{m-m-1} = 0$, as per the conventions in equation (3). Now assume that $r < \binom{m+d}{d}$, and let i, j be as in (12). We shall prove the desired inequality by producing a set B of r linearly independent polynomials in $\mathbb{F}_q[x_0, \ldots, x_m]_d$ with the property that $|V(B)(\mathbb{F}_q)| = H_j(d-1, m-i) + \mathsf{p}_{m-i-1}$.

First, for each positive integer $a \leqslant i$, let $\mathcal{B}_a$ be a basis of the $\mathbb{F}_q$-vector space $x_{m-a+1}\mathbb{F}_q[x_0, \ldots, x_{m-a+1}]_{d-1}$; for instance, $\mathcal{B}_a$ can be the set of monomials of degree d in $x_0, \ldots, x_{m-a+1}$ that are divisible by x_{m-a+1}. Clearly, the sets $\mathcal{B}_a$ are disjoint and $|\mathcal{B}_a| = \binom{m+d-a}{d-1}$ for $1 \leqslant a \leqslant i$. Note that

$$V\Big(\bigcup_{a=1}^{i} \mathcal{B}_a\Big)(\mathbb{F}_q) = \{[a_0 : \cdots : a_m] \in \mathbb{P}^m(\mathbb{F}_q) \colon a_m = \cdots = a_{m-i+1} = 0\},$$

Next, since $d-1 < q$, by Theorem 2.1, we obtain j linearly independent polynomials $f_1, \ldots, f_j$ each of degree at most $d-1$ in the polynomial ring $\mathbb{F}_q[x_0, \ldots, x_{m-i-1}]$ such that $|Z_{m-i}(f_1, \ldots, f_j)(\mathbb{F}_q)| = H_j(d-1, m-i)$, where $Z_{m-i}(f_1, \ldots, f_j)$ denotes the set of common zeroes of $f_1, \ldots, f_j$ in the $(m-i)$ dimensional affine subspace of $\mathbb{P}^m$ given by $\{[a_0 : \cdots : a_m] \colon a_{m-i} = 1, a_s = 0 \text{ for } m-i < s \leqslant m\}$. Let $F_1, \ldots, F_j$ be the polynomials obtained, respectively, by homogenizing $f_1, \ldots, f_j$ to degree d with respect to the variable x_{m-i}. Clearly, the polynomials $F_1, \ldots, F_j$ lie in $\mathbb{F}_q[x_0, \ldots, x_{m-i}]_d$ and they are linearly independent. Also, it is clear that $\mathbb{F}_q[x_0, \ldots, x_{m-i}] \cap \mathcal{B}_a$ is empty for each $a = 1, \ldots, i$. Consequently, B is a linearly independent subset of $\mathbb{F}_q[x_0, \ldots, x_m]_d$ and

$$|B| = j + \sum_{a=1}^{i} \binom{m+d-a}{d-1} = r, \quad \text{where} \quad B := \{F_1, \ldots, F_j\} \cup \Big(\bigcup_{a=1}^{i} \mathcal{B}_a\Big),$$

with the convention that the relevant sets are empty if $j = 0$ or $i = 0$. Further, by intersecting $V(B) = V(F_1, \ldots, F_j) \cap V(\bigcup_{a=1}^{i} \mathcal{B}_a)$ with the affine patch $\{x_{m-i} = 1\}$ and the hyperplane $\{x_{m-i} = 0\}$ of $\mathbb{P}^m$, we see that $|V(B)(\mathbb{F}_q)|$ equals

$$|Z_{m-i}(f_1, \ldots, f_j)(\mathbb{F}_q)| + |\{[a_0 : \cdots : a_m] \in \mathbb{P}^m(\mathbb{F}_q) \colon a_m = \cdots = a_{m-i} = 0\}|,$$

which is $H_j(d-1, m-i) + \mathsf{p}_{m-i-1}$, as desired. $\square$

We remark that when $d = q$, the lower bound in Theorem 2.3 is not attained, in general. This is shown in [4, § 6], where the exact values of $e_r(q, m)$ are obtained for $1 \leqslant r \leqslant m+1$.

2.3. The "complete conjecture". It appears plausible that the lower bound in Theorem 2.3 is attained when $d < q$. More precisely, we conjecture the following.

Conjecture 2.4. *Let d, r be integers with $1 \leqslant d < q$ and $1 \leqslant r \leqslant \binom{m+d}{d}$, and let i, j be as in (12) if $r < \binom{m+d}{d}$, while $i := m$ and $j := \binom{m+d-i-1}{d-1}$ if $r = \binom{m+d}{d}$. Then*

$$e_r(d, m) = H_j(d-1, m-i) + \mathsf{p}_{m-i-1}.$$

As noted in the introduction, if $1 \leqslant r \leqslant \binom{m+d-1}{d-1}$, then Conjecture 2.4 reduces to [9, Conjecture 6.6]. The case $d = 1$ of Conjecture 2.4 holds trivially, while the

case $d = 2$ follows from the work of Zanella [21]. Further, it was shown in [4] that Conjecture 2.4 holds when $2 \leqslant d < q$ and $r \leqslant \binom{m+2}{2}$.

We will now describe an alternative formulation of Conjecture 2.4 deduced from the alternative description of $H_r(d, m)$ given in [2]. Before stating it, let us recall that given any positive integer d, we can express every nonnegative integer N as

$$N = \sum_{a=1}^{d} \binom{s_a}{a} \quad \text{for unique } s_a \in \mathbb{Z} \text{ with } s_d > s_{d-1} > \cdots > s_1 \geqslant 0.$$

This is called the *d-binomial representation* of N or the *d-th Macaulay representation* of N. We will find it convenient to consider $m_a := s_a - a$ for $1 \leqslant a \leqslant d$ so as to write the above expansion for N as

$$N = \sum_{a=1}^{d} \binom{m_a + a}{a} \quad \text{for unique } m_a \in \mathbb{Z} \text{ with } m_d \geqslant m_{d-1} \geqslant \cdots \geqslant m_1 \geqslant -1. \quad (13)$$

We may refer to $(m_d, \ldots, m_1)$ as the *Macaulay d-tuple* corresponding to N. Observe that if M is any nonnegative integer, then

$$0 \leqslant N < \binom{M + d}{d} \implies M - 1 \geqslant m_d \geqslant m_{d-1} \geqslant \cdots \geqslant m_1 \geqslant -1. \quad (14)$$

The following result is a direct consequence of the proof of [2, Thm. 3.1] and we remark that its proof does not use the theorem of Heijnen–Pellikaan (Theorem 6.4).

Lemma 2.5. *Assume that $1 \leqslant d < q$ and $0 \leqslant r \leqslant \binom{m+d}{d}$. Suppose the Macaulay d-tuple corresponding to $\binom{m+d}{d} - r$ is $(m_d, \ldots, m_1)$. Then*

$$H_r(d, m) = \sum_{a=1}^{d} \lfloor q^{m_a} \rfloor.$$

Proof. If $r = 0$, then $H_r(d, m) = q^m$, in accordance with our convention (3). On the other hand, the Macaulay d-tuple corresponding to $\binom{m+d}{d}$ is clearly $(m, -1, \ldots, -1)$. So the desired equality holds when $r = 0$. For $1 \leqslant r \leqslant \binom{m+d}{d}$, the desired equality is a special case of [2, Thm. 3.1] and its proof, since for $d < q$, the dimension $\rho_q(d, m)$ of the Reed–Muller code $\mathrm{RM}_q(d, m)$ is $\binom{m+d}{d}$. $\square$

Corollary 2.6. *Assume that $1 \leqslant d \leqslant q$ and $1 \leqslant r \leqslant \binom{m+d}{d}$. Let i, j be as in (12) if $r < \binom{m+d}{d}$, while $i := m$ and $j := \binom{m+d-i-1}{d-1}$ if $r = \binom{m+d}{d}$. Also let $(m_d, \ldots, m_1)$ be the Macaulay d-tuple corresponding to $\binom{m+d}{d} - r$. Then*

$$H_j(d - 1, m - i) + \mathsf{p}_{m-i-1} = \mathsf{p}_{m_d} + \sum_{a=1}^{d-1} \lfloor q^{m_a} \rfloor.$$

Proof. First, note that if $d = 1$, then $i = r$ and $j = 0$, and so in view of (3), $H_j(d-1, m-i) + \mathsf{p}_{m-i-1} = q^{m-r} + \mathsf{p}_{m-r-1} = \mathsf{p}_{m-r}$. Also, the Macaulay 1-tuple corresponding to $m + 1 - r$ is clearly $(m - r)$. Thus the desired equality holds when $d = 1$. Likewise, if $i = m$, then clearly j is 0 or 1 and $\binom{m+d}{d} - r$ is 1 or 0, thanks

to (11); in this case, $m_a = -1$ for $1 \leqslant a < d$, whereas m_d is 0 or -1 according as j is 0 or 1. Hence, in view of (3), the desired equality also holds when $i = m$.

Now suppose $d > 1$ and $0 \leqslant i < m$. Then $1 \leqslant d - 1 < q$ and $1 \leqslant r < \binom{m+d}{d}$. Using the equality in (12) together with (11), we can write

$$\binom{m+d}{d} - r = \binom{m+d-i-1}{d-1} - j + \sum_{a=1}^{m-i} \binom{m+d-i-a-1}{d-1}$$

$$= \binom{m+d-i-1}{d} + \binom{m+d-i-1}{d-1} - j,$$

where the last equality follows from (11) with m replaced by $m - i - 1$. In case $j = 0$, the last expression is simply $\binom{m+d-i}{d}$, and in this case $m_d = m - i$ while $m_a = -1$ for $1 \leqslant a < d$. Thus, in view of (3), we see that when $j = 0$,

$$H_j(d-1, m-i) + \mathsf{p}_{m-i-1} = q^{m-i} + \mathsf{p}_{m-i-1} = \mathsf{p}_{m-i} = \mathsf{p}_{m_d} + \sum_{a=1}^{d-1} \lfloor q^{m_a} \rfloor,$$

as desired. Now suppose $0 < j < \binom{m+d-i-1}{d-1}$. By (14) and Lemma 2.5, it follows that if $(\mu_{d-1}, \ldots, \mu_1)$ is the Macaulay $(d-1)$-tuple corresponding to $\binom{m+d-i-1}{d-1} - j$, then $m - i - 1 \geqslant \mu_{d-1} \geqslant \cdots \geqslant \mu_1$, and further,

$$\binom{m+d-i-1}{d-1} - j = \sum_{a=1}^{d-1} \binom{\mu_a + a}{a} \quad \text{and} \quad H_j(d-1, m-i) = \sum_{a=1}^{d-1} \lfloor q^{\mu_a} \rfloor. \quad (15)$$

Substituting this in the expression obtained earlier for $\binom{m+d}{d} - r$, we see that

$$\binom{m+d}{d} - r = \binom{m+d-i-1}{d} + \sum_{a=1}^{d-1} \lfloor q^{\mu_a} \rfloor.$$

This together with the uniqueness of Macaulay d-tuples implies that $m_d = m - i - 1$ and $m_a = \mu_a$ for $1 \leqslant a < d$. Consequently, (15) yields the desired equality $\qquad \square$

In view of Corollary 2.6, the lower bound in Theorem 2.3 and the conjectural formula for $e_r(d, m)$ in Conjecture 2.4 can be written as

$$\mathsf{p}_{m_d} + \sum_{a=1}^{d-1} \lfloor q^{m_a} \rfloor,$$

where $(m_d, \ldots, m_1)$ is the Macaulay d-tuple corresponding to $\binom{m+d}{d} - r$.

3. Projective Reduction, Shadows and Footprints

In this section, we review some preliminary notions and results, which will be useful to us in the remainder of the paper. Throughout this section, m denotes a positive integer and $\mathbb{F}_q$ the finite field with q elements.

3.1. Projective reduction. Recall that a monomial $\mu \in \mathbb{F}_q[x_1, \ldots, x_m]$ given by $\mu = x_1^{\alpha_1} \cdots x_m^{\alpha_m}$ is said to be *reduced* if $0 \leqslant \alpha_i \leqslant q - 1$ for all $i = 1, \ldots, m$ and a polynomial $F \in \mathbb{F}_q[x_1, \ldots, x_m]$ is said to be reduced if it is an $\mathbb{F}_q$-linear combination of reduced monomials. It is well-known (see for example [14, Ch. 2] or [11]) that the set of all reduced monomials gives rise to a basis of the $\mathbb{F}_q$-vector space $\mathbb{F}_q[x_1, \ldots, x_m]/I(\mathbb{A}^m(\mathbb{F}_q))$, where $I(\mathbb{A}^m(\mathbb{F}_q))$ denotes the ideal consisting of all polynomials in $\mathbb{F}_q[x_1, \ldots, x_m]$ vanishing at every point of $\mathbb{A}^m(\mathbb{F}_q)$. More precisely, any element of $\mathbb{F}_q[x_1, \ldots, x_m]/I(\mathbb{A}^m(\mathbb{F}_q))$ can be written uniquely as $\tilde{f} + I(\mathbb{A}^m(\mathbb{F}_q))$ for some reduced polynomial $\tilde{f}$.

A projective analogue of the above notion and result is given in [5, §2]. We recall this below. Here, and hereafter, we denote by $\mathbb{M}$ the set of all monomials in the $m + 1$ variables $x_0, \ldots, x_m$.

Definition 3.1. For a nonnegative integer a, let $\overline{a}$ be the unique integer satisfying

$$0 \leqslant \overline{a} < q \quad \text{and} \quad \overline{a} = \begin{cases} 0 & \text{if } a = 0, \\ \tilde{a} & \text{if } a > 0 \text{ and } \tilde{a} \equiv a \,(\text{mod } q - 1), \text{ where } 0 < \tilde{a} \leqslant q - 1. \end{cases}$$

Let $\mu \in \mathbb{M}$. If $\mu \neq 1$, then we may write $\mu = x_0^{a_0} \cdots x_\ell^{a_\ell}$, where $0 \leqslant \ell \leqslant m$ and $a_0, \ldots, a_\ell$ are nonnegative integers with $a_\ell > 0$. Define

$$\overline{\mu} := x_0^{\overline{a_0}} \cdots x_{\ell-1}^{\overline{a_{\ell-1}}} x_\ell^{a_\ell + \sum_{j=0}^{\ell-1}(a_j - \overline{a_j})}.$$

If $\mu = 1$, then we define $\overline{\mu} = 1$. Note that $\overline{\mu} \in \mathbb{M}$ with $\deg \overline{\mu} = \deg \mu$. We call $\overline{\mu}$ the *projective reduction* of μ. Any polynomial $F \in \mathbb{F}_q[x_0, \ldots, x_m]$ can be written uniquely as $F = \sum_{i=1}^n c_i \mu_i$, where $c_i \in \mathbb{F}_q \setminus \{0\}$ and $\mu_i \in \mathbb{M}$. We define $\overline{F}$, the *projective reduction* of F, as $\overline{F} = \sum_{i=1}^n c_i \overline{\mu_i}$. A monomial $\mu \in \mathbb{M}$ (resp. polynomial $F \in \mathbb{F}_q[x_0, \ldots, x_m]$) is said to be *projectively reduced* if $\overline{\mu} = \mu$ (resp. $\overline{F} = F$).

It is easy to see from the definition that a reduced polynomial is projectively reduced. In particular, a polynomial of degree $d \leqslant q - 1$ is necessarily reduced and hence projectively reduced. A polynomial of degree q is not necessarily reduced but is always projectively reduced. Clearly, a polynomial of degree $d > q$ may not even be projectively reduced. It is easy to see that if $F \in \mathbb{F}_q[x_0, \ldots, x_m]$, then

$$F(c_0, \ldots, c_m) = \overline{F}(c_0, \ldots, c_m) \quad \text{for all } (c_0, \ldots, c_m) \in \mathbb{F}_q^{m+1}. \tag{16}$$

For further properties of projective reduction and projectively reduced polynomials we refer to [5, Proposition 2.2].

Throughout this article, we denote by $\overline{\mathbb{M}}$ the set of projectively reduced monomials in $m+1$ variables $x_0, \ldots, x_m$. Further, for any nonnegative integer e, we denote by $\overline{\mathbb{M}}_e$ the set of all projectively reduced monomials in $\overline{\mathbb{M}}$ of degree e. Clearly, $\overline{\mathbb{M}}$ equals the disjoint union $\coprod_{e \geqslant 0} \overline{\mathbb{M}}_e$.

Let $I(\mathbb{P}^m(\mathbb{F}_q))$ denote the ideal of $\mathbb{F}_q[x_0, \ldots, x_m]$ generated by the homogeneous polynomials that vanish at all points of $\mathbb{P}^m(\mathbb{F}_q)$. It was shown by Mercier and Rolland [16] that this ideal is equal to the ideal $\Gamma_q(\mathbb{F}_q)$ of $\mathbb{F}_q[x_0, \ldots, x_m]$ generated by $\{x_i^q x_j - x_i x_j^q : 0 \leqslant i < j \leqslant m\}$. It was further proved in [5, Theorem 2.8] that the set $\{x_i^q x_j - x_i x_j^q : 0 \leqslant i < j \leqslant m\}$ forms a universal Gröbner basis for $\Gamma_q(\mathbb{F}_q)$. To conclude this subsection, we note that the projectively reduced monomials give rise

to a basis of the $\mathbb{F}_q$-vector space $\mathbb{F}_q[x_0, \ldots, x_m]/I(\mathbb{P}^m(\mathbb{F}_q))$. More precisely, any element of $\mathbb{F}_q[x_0, \ldots, x_m]/I(\mathbb{P}^m(\mathbb{F}_q))$ can be written uniquely as $f + I(\mathbb{P}^m(\mathbb{F}_q))$, where f is a projectively reduced polynomial. For a proof, see [5, Corollary 2.10].

3.2. Shadows and footprints. Given $\mathcal{S} \subseteq \mathbb{M}$ and a nonnegative integer e, define

$$\nabla_e(\mathcal{S}) := \{\mu \in \overline{\mathbb{M}}_e : \nu \mid \mu \text{ for some } \nu \in \mathcal{S}\} \quad \text{and} \quad \Delta_e(\mathcal{S}) := \overline{\mathbb{M}}_e \setminus \nabla_e(\mathcal{S}).$$

The set $\nabla_e(\mathcal{S})$ is called the *shadow* of $\mathcal{S}$ in $\overline{\mathbb{M}}_e$, while the set $\Delta_e(\mathcal{S})$ is known as the *footprint* of $\mathcal{S}$ in $\overline{\mathbb{M}}_e$.

Recall that by a *term order* on $\mathbb{M}$, one means a total order $\prec$ on the set $\mathbb{M}$ of all monomials in $x_0, \ldots, x_m$ such that (i) $1 \preccurlyeq \mu$ for all $\mu \in \mathbb{M}$, and (ii) $\mu\nu \preccurlyeq \mu'\nu$ whenever $\mu, \mu', \nu \in \mathbb{M}$ are such that $\mu \preccurlyeq \mu'$. Let $\prec$ be any term order on $\mathbb{M}$ for which $x_0 \succ x_1 \succ \ldots \succ x_m$. For example, we can take $\prec$ to be the lexicographic order $\prec_{\text{lex}}$ defined by

$$x_0^{a_0} \cdots x_m^{a_m} \prec_{\text{lex}} x_0^{b_0} \cdots x_m^{b_m} \iff \text{the first nonzero entry of b} - \text{a is positive}, \quad (17)$$

where b $-$ a denotes the difference tuple $(b_0 - a_0, \ldots, b_m - a_m)$. Other examples of such term orders are also possible. For now, we just fix a term order $\prec$ on $\mathbb{M}$ for which $x_0 \succ x_1 \succ \ldots \succ x_m$. For a nonzero polynomial $F \in \mathbb{F}_q[x_0, \ldots, x_m]$, we denote by $\text{lm}_\prec(F)$ or simply $\text{lm}(F)$, the *leading monomial* of F, i.e., the largest monomial (w.r.t $\prec$) appearing in F with a nonzero coefficient. For any set $\mathcal{S}$ of nonzero polynomials in $\mathbb{F}_q[x_0, \ldots, x_m]$ and any nonnegative integer e, we define

$$\text{lm}(\mathcal{S}) := \{\text{lm}(F) : F \in \mathcal{S}\}, \quad \nabla_e(\mathcal{S}) := \nabla_e(\text{lm}(\mathcal{S})) \quad \text{and} \quad \Delta_e(\mathcal{S}) := \Delta_e(\text{lm}(\mathcal{S})).$$

The following important result from [5] relates footprints in $\overline{\mathbb{M}}_e$ to the number of $\mathbb{F}_q$-rational points of projective algebraic varieties defined over $\mathbb{F}_q$. Here, and hereafter, for an assertion depending on a nonnegative integer e, the expression "for all $e \gg 0$" means that the assertion holds for all large enough values of e, i.e., there is a nonnegative integer e_0 such that the assertion holds for all $e \geqslant e_0$.

Theorem 3.2 (projective $\mathbb{F}_q$-footprint bound). *Let $\mathcal{S} = \{F_1, \ldots, F_r\}$ be a set of nonzero, projectively reduced homogeneous polynomials in $\mathbb{F}_q[x_0, \ldots, x_m]$. Write $\mathcal{X} = V(\mathcal{S})$ for the corresponding algebraic variety in $\mathbb{P}^m$. Then*

$$|\mathcal{X}(\mathbb{F}_q)| \leqslant |\Delta_e(\mathcal{S})| \quad \text{for all } e \gg 0.$$

Proof. Since $F_1, \ldots, F_r$ are projectively reduced, $\text{lm}(\mathcal{S}) \subseteq \overline{\mathbb{M}}$. Thus the notion of footprint $\Delta_e(\mathcal{S})$ defined above coincides with that of projective $\mathbb{F}_q$-footprint $\overline{\Delta}_e(\mathcal{S})$ defined in [5, Def. 3.10]. So the desired result follows from [5, Thm. 3.12]. $\square$

We can decompose $\overline{\mathbb{M}}$ into disjoint subsets by considering the last variable appearing in a given monomial. Thus, following [5], we define

$$\overline{\mathbb{M}}^{(0)} = \{x_0^a : a \geqslant 0\} \quad \text{and for } 1 \leqslant \ell \leqslant m, \quad \overline{\mathbb{M}}^{(\ell)} := \{x_0^{a_0} \cdots x_\ell^{a_\ell} \in \overline{\mathbb{M}} : a_\ell > 0\}.$$

Further, for any integers e, ℓ with $e \geqslant 0$ and $0 \leqslant \ell \leqslant m$, define $\overline{\mathbb{M}}_e^{(\ell)} := \overline{\mathbb{M}}^{(\ell)} \cap \overline{\mathbb{M}}_e$. Evidently, $\overline{\mathbb{M}} = \coprod_{\ell=0}^m \overline{\mathbb{M}}^{(\ell)}$ and $\overline{\mathbb{M}}_e = \coprod_{\ell=0}^m \overline{\mathbb{M}}_e^{(\ell)}$. It is easy to see that

$$|\overline{\mathbb{M}}_e^{(\ell)}| = q^\ell \text{ for } e \geqslant \ell(q-1) + 1 \quad \text{and hence} \quad |\overline{\mathbb{M}}_e| = \mathsf{p}_m \text{ for } e \geqslant m(q-1) + 1.$$

We refer to [5, Section 2.1] for more details.

The sets $\overline{\mathbb{M}}_e^{(\ell)}$ help us in decomposing the shadows or footprints into several disjoint components. To this end, we define

$$\nabla_e^{(\ell)}(\mathcal{S}) := \nabla_e(\mathcal{S}) \cap \overline{\mathbb{M}}_e^{(\ell)} \quad \text{and} \quad \Delta_e^{(\ell)}(\mathcal{S}) := \Delta_e(\mathcal{S}) \cap \overline{\mathbb{M}}_e^{(\ell)}. \tag{18}$$

For any $\mathcal{S} \subseteq \overline{\mathbb{M}}$ and any nonnegative integer e, it is clear that

$$|\nabla_e(\mathcal{S})| = \sum_{\ell=0}^{m} |\nabla_e^{(\ell)}(\mathcal{S})| \quad \text{and} \quad |\Delta_e(\mathcal{S})| = \sum_{\ell=0}^{m} |\Delta_e^{(\ell)}(\mathcal{S})|. \tag{19}$$

Given a nonnegative integer $\ell \leqslant m$, by specializing the variables $x_{\ell+1}, \ldots, x_m$ to 1, we can associate to a subset of $\overline{\mathbb{M}}$, a set of projectively reduced monomials in $x_0, \ldots, x_\ell$ as follows.

Definition 3.3. Let $\mathcal{S} \subset \overline{\mathbb{M}}$. For $0 \leqslant \ell \leqslant m$, we define

$$\mathcal{S}^{\langle \ell \rangle} := \{x_0^{a_0} \cdots x_\ell^{a_\ell} \in \mathcal{S} \colon 0 \leqslant a_j < q \text{ for all } j < \ell\}.$$

Note that if $0 \leqslant \ell \leqslant m$ and if $\mu \in \mathcal{S} \setminus \mathcal{S}^{\langle \ell \rangle}$, then either (i) $x_i \,|\, \mu$ for some $i > \ell$, or (ii) $\mu = x_0^{a_0} \cdots x_j^{a_j}$ with $a_j > q$ for some $j < \ell$. In either case, it is easily seen that $\nabla_e^{(\ell)}(\mu) = \varnothing$. This shows that

$$\nabla_e^{(\ell)}(\mathcal{S}) = \nabla_e^{(\ell)}(\mathcal{S}^{\langle \ell \rangle}) \quad \text{and hence} \quad \Delta_e^{(\ell)}(\mathcal{S}) = \Delta_e^{(\ell)}(\mathcal{S}^{\langle \ell \rangle}) \quad \text{for any } e \geqslant 0. \tag{20}$$

The following reformulation of Theorem 3.2 will be useful to us later.

Corollary 3.4. *Let* $F_1, \ldots, F_r$ *be any nonzero projectively reduced homogeneous polynomials in* $\mathbb{F}_q[x_0, \ldots, x_m]$, *and let* $\mathcal{X} = V(F_1, \ldots, F_r)$ *be the corresponding projective variety in* $\mathbb{P}^m$. *Also, let* $\mathcal{S} = \{\mathrm{lm}(F_1), \ldots, \mathrm{lm}(F_r)\}$. *Then*

$$|\mathcal{X}(\mathbb{F}_q)| \leqslant \sum_{\ell=0}^{m} |\Delta_e^{(\ell)}(\mathcal{S}^{\langle \ell \rangle})| \quad \text{for all } e \gg 0.$$

Proof. From equation (20) and the second part of equation (19), we see that

$$|\Delta_e(\mathcal{S})| = \sum_{\ell=0}^{m} |\Delta_e^{(\ell)}(\mathcal{S}^{\langle \ell \rangle})|. \tag{21}$$

Thus the desired result follows from Theorem 3.2. $\qquad\square$

4. Affine Combinatorics

In this section, we will consider some results from extremal combinatorics together with their generalizations and variants that will be useful for us later. These results are mainly concerned with sets of monomials in ℓ variables that are reduced in the usual (or the affine) sense. Throughout this section, m will be a fixed positive integer and ℓ, d as well as a_i, b_i denote nonnegative integers with $\ell \leqslant m$.

4.1. Shadows and footprints in the hypercube. For $0 \leqslant \ell \leqslant m$, define

$$\mathbb{H}^{(\ell)} := \{x_0^{a_0} \cdots x_{\ell-1}^{a_{\ell-1}} : 0 \leqslant a_j \leqslant q - 1 \text{ for all } j = 0, \ldots \ell - 1\}.$$

Note that the "exponent map" given by $x_0^{a_0} \cdots x_{\ell-1}^{a_{\ell-1}} \mapsto (a_0, \ldots, a_{\ell-1})$ lets us identify the set $\mathbb{H}^{(\ell)}$ with Q^ℓ, where $Q := \{0, 1, \ldots, q - 1\}$, and thus we may refer to $\mathbb{H}^{(\ell)}$ as the (ℓ-dimensional) *hypercube*. We remark that when $q = 2$, elements of $\mathbb{H}^{(\ell)}$ can be identified with subsets of $\{0, \ldots, \ell - 1\}$, whereas in general, they may be viewed as multisets formed by the elements of $\{0, \ldots, \ell - 1\}$. We will, however, stick to viewing $\mathbb{H}^{(\ell)}$ as the set of reduced monomials in ℓ variables $x_0, \ldots, x_{\ell-1}$.

Divisibility of monomials gives a natural partial order on $\mathbb{H}^{(\ell)}$, which corresponds, via the exponent map, to the "product order" $\leqslant_P$ on Q^ℓ defined by $(a_0, \ldots, a_{\ell-1}) \leqslant_P (b_0, \ldots, b_{\ell-1})$ if and only if $a_i \leqslant b_i$ for all $i = 0, \ldots, \ell - 1$. On the other hand, the usual lexicographic order on Q^ℓ corresponds to the total order on $\mathbb{H}^{(\ell)}$, which we denote, as in (17), by $\prec_{\text{lex}}$. Note that if $\mu, \nu \in \mathbb{H}^{(\ell)}$ are such that $\nu \,|\, \mu$, i.e., ν divides μ, then $\nu \preccurlyeq_{\text{lex}} \mu$.

As before, for a nonnegative integer d, we define

$$\mathbb{H}_d^{(\ell)} := \{\mu \in \mathbb{H}^{(\ell)} : \deg \mu = d\} \quad \text{and} \quad \mathbb{H}_{\leqslant d}^{(\ell)} := \{\mu \in \mathbb{H}^{(\ell)} : \deg \mu \leqslant d\}.$$

The sets $\mathbb{H}_{<d}^{(\ell)}$, $\mathbb{H}_{\geqslant d}^{(\ell)}$ and $\mathbb{H}_{>d}^{(\ell)}$ are defined analogously.

We will now define shadow and footprint in the context of the hypercube $\mathbb{H}^{(\ell)}$. To avoid confusion with the notions defined in Section 3.2, we will use a different notation.

For any $\mathcal{T} \subseteq \mathbb{H}^{(\ell)}$, the *shadow* and *footprint* of $\mathcal{T}$ in $\mathbb{H}^{(\ell)}$ are denoted by $\mathsf{SH}^{(\ell)}(\mathcal{T})$ and $\mathsf{FP}^{(\ell)}(\mathcal{T})$, respectively, and defined by

$$\mathsf{SH}^{(\ell)}(\mathcal{T}) := \{\mu \in \mathbb{H}^{(\ell)} : \nu \,|\, \mu \text{ for some } \nu \in \mathcal{T}\} \quad \text{and} \quad \mathsf{FP}^{(\ell)}(\mathcal{T}) := \mathbb{H}^{(\ell)} \setminus \mathsf{SH}^{(\ell)}(\mathcal{T}).$$

For a nonnegative integer d, we also define,

$$\mathsf{FP}_d^{(\ell)}(\mathcal{T}) := \mathsf{FP}^{(\ell)}(\mathcal{T}) \cap \mathbb{H}_d^{(\ell)} \quad \text{and} \quad \mathsf{FP}_{\leqslant d}^{(\ell)}(\mathcal{T}) := \mathsf{FP}^{(\ell)}(\mathcal{T}) \cap \mathbb{H}_{\leqslant d}^{(\ell)}.$$

The sets $\mathsf{FP}_{<d}^{(\ell)}(\mathcal{T})$, $\mathsf{FP}_{\geqslant d}^{(\ell)}(\mathcal{T})$ and $\mathsf{FP}_{>d}^{(\ell)}(\mathcal{T})$ are defined analogously. Moreover, the corresponding subsets of $\mathsf{SH}^{(\ell)}(\mathcal{T})$ are also defined in a similar manner.

Definition 4.1. Let ℓ, d, ρ, ρ' be integers satisfying $0 \leqslant d \leqslant \ell(q-1)$, $0 \leqslant \ell \leqslant m$, $0 \leqslant \rho \leqslant |\mathbb{H}_{\leqslant d}^{(\ell)}|$, and $0 \leqslant \rho' \leqslant |\mathbb{H}_d^{(\ell)}|$. Define

$\mathcal{M}_d^{(\ell)}(\rho) :=$ the set of first ρ elements of $\mathbb{H}_{\leqslant d}^{(\ell)}$ in descending lexicographic order,

$\mathcal{L}_d^{(\ell)}(\rho') :=$ the set of first ρ' elements of $\mathbb{H}_d^{(\ell)}$ in descending lexicographic order.

Note that if ℓ, ρ, ρ' are positive and $d < q$, then both $\mathcal{M}_d^{(\ell)}(\rho)$ and $\mathcal{L}_d^{(\ell)}(\rho')$ contain x_0^d, which is the largest element of $\mathbb{H}_{\leqslant d}^{(\ell)}$ as well as $\mathbb{H}_d^{(\ell)}$ in lexicographic order. Also, for a fixed $d \geqslant 0$, the set $\mathbb{H}_{\leqslant d}^{(\ell)}$ is finite and $\prec_{\text{lex}}$ is a total order on it. Consequently, a set of the form $\mathcal{M}_d^{(\ell)}(\rho)$ can be characterized as a subset $\mathcal{T}$ of $\mathbb{H}_{\leqslant d}^{(\ell)}$ that is *upwards closed*, which means that $\mu \in \mathcal{T}$ whenever $\mu, \mu' \in \mathbb{H}_{\leqslant d}^{(\ell)}$ with

$\mu' \prec_{\mathrm{lex}} \mu$ and $\mu' \in \mathcal{T}$. Similarly, sets of the form $\mathcal{L}_d^{(\ell)}(\rho')$ can be characterized as upwards closed subsets of $\mathbb{H}_d^{(\ell)}$.

4.2. Extremal combinatorics. We will now discuss some combinatorial results that help us determine the subsets of $\mathbb{H}_d^{(\ell)}$ (resp. $\mathbb{H}_{\leqslant d}^{(\ell)}$) of a given cardinality that have footprint of the maximum possible size. We begin with a result due to Heijnen and Pellikaan [12, Prop. 5.9]. Its formulation below is as in [3, Lem. 4.2], where the result is proved in a more general setting.

Proposition 4.2. *Let ℓ, d, ρ be integers satisfying $1 \leqslant \ell \leqslant m$, $0 \leqslant d \leqslant \ell(q-1)$, and $1 \leqslant \rho \leqslant |\mathbb{H}_{\leqslant d}^{(\ell)}|$. Also, let α be the ρth element of $\mathbb{H}_{\leqslant d}^{(\ell)}$, i.e., the smallest element of $\mathcal{M}_d^{(\ell)}(\rho)$ in lexicographic order. Then*

$$\mathsf{SH}^{(\ell)}(\mathcal{M}_d^{(\ell)}(\rho)) = \{\mu \in \mathbb{H}^{(\ell)} \,:\, \alpha \preccurlyeq_{\mathrm{lex}} \mu\}.$$

Consequently, $\mathsf{SH}^{(\ell)}(\mathcal{M}_d^{(\ell)}(\rho)) \cap \mathbb{H}_{\leqslant d}^{(\ell)} = \mathcal{M}_d^{(\ell)}(\rho)$.

Corollary 4.3. *Let ℓ, d, ρ be integers satisfying $1 \leqslant \ell \leqslant m$, $1 \leqslant d \leqslant \ell(q-1)$, and $0 \leqslant \rho \leqslant |\mathbb{H}_{\leqslant d}^{(\ell)}|$. Then $\mathsf{SH}_d^{(\ell)}(\mathcal{M}_{d-1}^{(\ell)}(\rho)) = \mathcal{L}_d^{(\ell)}(\rho')$ for some nonnegative integer ρ'. Moreover, if ρ is positive, then so is ρ'.*

Proof. If $\rho = 0$, then $\mathcal{M}_{d-1}^{(\ell)}(\rho)$ is empty, and hence so is its shadow in $\mathbb{H}^{(\ell)}$. Thus we can take $\rho' = 0$ in this case. Now suppose $\rho \geqslant 1$. First, note that $\mathsf{SH}_d^{(\ell)}(\mathcal{M}_{d-1}^{(\ell)}(\rho))$ is nonempty. Indeed, $d - 1 < \ell(q-1)$ and so we can write $d - 1 = j(q-1) + a_j$ for unique integers j, a_j with $0 \leqslant j \leqslant \ell - 1$ and $0 \leqslant a_j < q - 1$. Since $\rho \geqslant 1$, the set $\mathcal{M}_{d-1}^{(\ell)}(\rho)$ contains $\nu := x_0^{q-1} \cdots x_{j-1}^{q-1} x_j^{a_j}$, being the largest element of this set in lexicographic order. Now $\mu := \nu x_{\ell-1}$ is clearly in $\mathsf{SH}_d^{(\ell)}(\mathcal{M}_{d-1}^{(\ell)}(\rho))$.

To complete the proof, it suffices to show that $\mathsf{SH}_d^{(\ell)}(\mathcal{M}_{d-1}^{(\ell)}(\rho))$ is upwards closed. Assume the contrary. Then there exist μ, $\mu' \in \mathbb{H}_d^{(\ell)}$ such that $\mu' \in \mathsf{SH}_d^{(\ell)}(\mathcal{M}_{d-1}^{(\ell)}(\rho))$ and $\mu' \prec_{\mathrm{lex}} \mu$, but $\mu \notin \mathsf{SH}_d^{(\ell)}(\mathcal{M}_{d-1}^{(\ell)}(\rho))$. Let $\nu \in \mathcal{M}_{d-1}^{(\ell)}(\rho)$ be such that $\nu \,|\, \mu'$. Then $\nu \preccurlyeq_{\mathrm{lex}} \mu'$. Also, let ν' be the least element of $\mathcal{M}_{d-1}^{(\ell)}(\rho)$ in lexicographic order. Then $\nu' \preccurlyeq_{\mathrm{lex}} \nu$ and $\nu \preccurlyeq_{\mathrm{lex}} \mu'$, since $\nu \,|\, \mu'$. Consequently, $\nu' \prec_{\mathrm{lex}} \mu$. By the previous proposition, $\mu \in \mathsf{SH}_d^{(\ell)}(\mathcal{M}_{d-1}^{(\ell)}(\rho))$, which is a contradiction. $\qquad\square$

The following result is due to Clements and Lindström [7, Cor. 1] (see also [3, Thm. 3.1]). The case $q = 2$ of it is equivalent to the Kruskal–Katona theorem.

Theorem 4.4 (Clements–Lindström)**.** *Let $\mathcal{T} \subseteq \mathbb{H}_d^{(\ell)}$ with $|\mathcal{T}| = \rho'$. Then*

$$\mathsf{SH}_{d+1}^{(\ell)}(\mathcal{L}_d^{(\ell)}(\rho')) \subseteq \mathcal{L}_{d+1}^{(\ell)}(|\mathsf{SH}_{d+1}^{(\ell)}(\mathcal{T})|) \text{ and hence } |\mathsf{FP}_{d+1}^{(\ell)}(\mathcal{T})| \leqslant |\mathsf{FP}_{d+1}^{(\ell)}(\mathcal{L}_d^{(\ell)}(\rho'))|.$$

As in [3, Cor. 3.2], the following corollary can be deduced easily from the above theorem by using induction on e.

Corollary 4.5. *Let $\mathcal{T} \subseteq \mathbb{H}_d^{(\ell)}$ with $|\mathcal{T}| = \rho'$, and let e be an integer $\geqslant d$. Then*

$$\mathsf{SH}_e^{(\ell)}(\mathcal{L}_d^{(\ell)}(\rho')) \subseteq \mathcal{L}_e^{(\ell)}(|\mathsf{SH}_e^{(\ell)}(\mathcal{T})|); \quad \text{in particular,} \quad |\mathsf{SH}_e^{(\ell)}(\mathcal{L}_d^{(\ell)}(\rho'))| \leqslant |\mathsf{SH}_e^{(\ell)}(\mathcal{T})|.$$

Consequently, $|\mathsf{FP}_e^{(\ell)}(\mathcal{T})| \leqslant |\mathsf{FP}_e^{(\ell)}(\mathcal{L}_d^{(\ell)}(\rho'))|$ and hence $|\mathsf{FP}^{(\ell)}(\mathcal{T})| \leqslant |\mathsf{FP}^{(\ell)}(\mathcal{L}_d^{(\ell)}(\rho'))|$.

The following theorem can be traced back to Wei [20, Lemma 6] and it gives an analogue of the last inequality for subsets of $\mathbb{H}_{\leqslant d}^{(\ell)}$.

Theorem 4.6 (Wei). *Let $\mathcal{T} \subset \mathbb{H}_{\leqslant d}^{(\ell)}$ be a subset with $|\mathcal{T}| = \rho$. Then*

$$|\mathsf{FP}^{(\ell)}(\mathcal{T})| \leqslant |\mathsf{FP}^{(\ell)}(\mathcal{M}_d^{(\ell)}(\rho))|.$$

Strictly speaking, Lemma 6 of Wei [20] proves the above theorem for the special case when $q = 2$. A general version is stated in Heijnen and Pellikaan [12, Thm. 5.7], although in a slightly different way. A detailed proof appears in Appendix A of Heijnen's thesis [13]. We refer to [3, Thm. 3.8] for a similar result in a more general setting. We conclude this subsection by proving the following common generalization of the results of Clements–Lindström (Corollary 4.5) and of Wei and Heijnen–Pellikaan (Theorem 4.6). Indeed, Corollary 4.5 corresponds to the case $\rho' = \rho$, while Theorem 4.6 corresponds to the case $\rho' = 0$.

Theorem 4.7. *Assume that ℓ, d, ρ are positive integers with $\ell \leqslant m$, $d \leqslant \ell(q-1)$, and $\rho \leqslant |\mathbb{H}_{\leqslant d}^{(\ell)}|$. Let $\mathcal{T} \subseteq \mathbb{H}_{\leqslant d}^{(\ell)}$ with $|\mathcal{T}| = \rho$. If $\rho' := |\mathcal{T} \cap \mathbb{H}_d^{(\ell)}|$, then*

$$|\mathsf{FP}^{(\ell)}(\mathcal{T})| \leqslant |\mathsf{FP}^{(\ell)}(\mathcal{U})|, \quad where \quad \mathcal{U} := \mathcal{L}_d^{(\ell)}(\rho') \cup \mathcal{M}_{d-1}^{(\ell)}(\rho - \rho').$$

Proof. Let $\rho' := |\mathcal{T} \cap \mathbb{H}_d^{(\ell)}|$ and $\mathcal{U} := \mathcal{L}_d^{(\ell)}(\rho') \cup \mathcal{M}_{d-1}^{(\ell)}(\rho - \rho')$. It suffices to show that $|\mathsf{SH}^{(\ell)}(\mathcal{U})| \leqslant |\mathsf{SH}^{(\ell)}(\mathcal{T})|$. We will do this by distinguishing two cases.

CASE 1: $\mathcal{L}_d^{(\ell)}(\rho') \subseteq \mathsf{SH}_d^{(\ell)}(\mathcal{M}_{d-1}^{(\ell)}(\rho - \rho'))$.

Let $\mu \in \mathsf{SH}^{(\ell)}(\mathcal{U})$. Then there is $\nu \in \mathcal{U}$ such that $\nu \mid \mu$. Suppose $\nu \in \mathcal{L}_d^{(\ell)}(\rho')$. Since $\mathcal{L}_d^{(\ell)}(\rho') \subseteq \mathsf{SH}_d^{(\ell)}(\mathcal{M}_{d-1}^{(\ell)}(\rho - \rho'))$, there is $\nu' \in \mathcal{M}_{d-1}^{(\ell)}(\rho - \rho')$ such that $\nu' \mid \nu$, and hence $\nu' \mid \mu$. This shows that $\mathsf{SH}^{(\ell)}(\mathcal{U}) = \mathsf{SH}^{(\ell)}(\mathcal{M}_{d-1}^{(\ell)}(\rho - \rho'))$. Consequently,

$$\left|\mathsf{SH}^{(\ell)}(\mathcal{U})\right| = \left|\mathsf{SH}^{(\ell)}(\mathcal{M}_{d-1}^{(\ell)}(\rho - \rho'))\right| \leqslant \left|\mathsf{SH}^{(\ell)}(\mathcal{T} \cap \mathbb{H}_{\leqslant d-1}^{(\ell)})\right| \leqslant \left|\mathsf{SH}^{(\ell)}(\mathcal{T})\right|,$$

where the penultimate inequality is a consequence of Theorem 4.6 (applied to shadows instead of footprints), while the last inequality follows since $\mathcal{T} \cap \mathbb{H}_{\leqslant d-1}^{(\ell)} \subseteq \mathcal{T}$.

CASE 2: $\mathcal{L}_d^{(\ell)}(\rho') \not\subseteq \mathsf{SH}_d^{(\ell)}(\mathcal{M}_{d-1}^{(\ell)}(\rho - \rho'))$.

By Corollary 4.3, $\mathsf{SH}_d^{(\ell)}(\mathcal{M}_{d-1}^{(\ell)}(\rho - \rho')) = \mathcal{L}_d^{(\ell)}(\rho'')$ for some nonnegative integer ρ''. Hence $\mathcal{L}_d^{(\ell)}(\rho') \not\subseteq \mathcal{L}_d^{(\ell)}(\rho'')$ and this implies that $\rho' \not\leqslant \rho''$, i.e., $\rho'' < \rho'$. It follows that $\mathsf{SH}_d^{(\ell)}(\mathcal{M}_{d-1}^{(\ell)}(\rho - \rho')) \subseteq \mathcal{L}_d^{(\ell)}(\rho')$. Consequently,

$$\mathsf{SH}_{\geqslant d}^{(\ell)}(\mathcal{U}) = \mathsf{SH}_{\geqslant d}^{(\ell)}(\mathcal{L}_d^{(\ell)}(\rho')) \cup \mathsf{SH}_{\geqslant d}^{(\ell)}(\mathcal{M}_{d-1}^{(\ell)}(\rho - \rho')) = \mathsf{SH}_{\geqslant d}^{(\ell)}(\mathcal{L}_d^{(\ell)}(\rho')). \tag{22}$$

On the other hand, $\mathsf{SH}_{<d}^{(\ell)}(\mathcal{U}) = \mathsf{SH}_{<d}^{(\ell)}(\mathcal{M}_{d-1}^{(\ell)}(\rho - \rho')) = \mathsf{SH}^{(\ell)}(\mathcal{M}_{d-1}^{(\ell)}(\rho - \rho')) \cap \mathbb{H}_{<d}^{(\ell)}$, and so by Proposition 4.2. we see that

$$\mathsf{SH}_{<d}^{(\ell)}(\mathcal{U}) = \mathcal{M}_{d-1}^{(\ell)}(\rho - \rho'). \tag{23}$$

Using equations (22) and (23), we obtain

$$|\mathsf{SH}^{(\ell)}(\mathcal{U})| = \rho - \rho' + |\mathsf{SH}_{\geqslant d}^{(\ell)}(\mathcal{L}_d^{(\ell)}(\rho'))| \leqslant \rho - \rho' + |\mathsf{SH}_{\geqslant d}^{(\ell)}(\mathcal{T} \cap \mathbb{H}_d^{(\ell)})|,$$

where the last inequality follows from Corollary 4.5. Now since $|\mathcal{T} \cap \mathbb{H}_{<d}^{(\ell)}| = \rho - \rho'$,

$$\left|\mathsf{SH}^{(\ell)}(\mathcal{U})\right| \leqslant \left|\mathsf{SH}_{<d}^{(\ell)}(\mathcal{T} \cap \mathbb{H}_{<d}^{(\ell)})\right| + \left|\mathsf{SH}_{\geqslant d}^{(\ell)}(\mathcal{T} \cap \mathbb{H}_d^{(\ell)})\right|.$$

Hence $|\mathsf{SH}^{(\ell)}(\mathcal{U})| \leqslant |\mathsf{SH}_{<d}^{(\ell)}(\mathcal{T})| + |\mathsf{SH}_{\geqslant d}^{(\ell)}(\mathcal{T})| = |\mathsf{SH}^{(\ell)}(\mathcal{T})|$, as desired. $\qquad\square$

5. Specializations and Expanders

In order to effectively relate the two notions Δ_e and FP of footprint considered in the previous two sections, we will introduce two maps, denoted $\sigma^{(\ell)}$ and ϕ, on the space of projectively reduced monomials in $x_0, \ldots, x_m$ and prove some of their properties. Throughout this section, m is a fixed positive integer, while ℓ, d, e denote nonnegative integers satisfying $\ell \leqslant m$.

5.1. Specialization. For any nonnegative integer $\ell \leqslant m$, we define

$$\sigma^{(\ell)} \colon \overline{\mathbb{M}} \to \overline{\mathbb{M}} \cup \{0\} \quad \text{by} \quad \sigma^{(\ell)}(\mu) := \begin{cases} x_0^{a_0} \cdots x_{\ell-1}^{a_{\ell-1}} & \text{if } \mu = x_0^{a_0} \cdots x_{\ell-1}^{a_{\ell-1}} x_\ell^{a_\ell}, \\ 0 & \text{if } \mu \notin \mathbb{F}_q[x_0, \ldots, x_\ell], \end{cases}$$

with the usual convention that an empty product equals 1. We may refer to $\sigma^{(\ell)}$ as the *specialization map* at level ℓ, since it corresponds to specializing the variables $(x_\ell, x_{\ell+1}, \ldots, x_m)$ to $(1, 0, \ldots, 0)$.

Proposition 5.1. *Let ℓ, d, e be nonnegative integers such that $e \geqslant d + m(q-1)$ and $\ell \leqslant m$. Suppose $\mu \in \overline{\mathbb{M}}_d \cap \mathbb{F}_q[x_0, \ldots, x_\ell]$ and $\nu \in \overline{\mathbb{M}}_e^{(\ell)}$. Then*

$$\mu \,|\, \nu \;\Leftrightarrow\; \sigma^{(\ell)}(\mu) \,|\, \sigma^{(\ell)}(\nu).$$

Proof. We can write $\mu = x_0^{a_0} \cdots x_\ell^{a_\ell}$ and $\nu = x_0^{b_0} \cdots x_{\ell-1}^{b_{\ell-1}} x_\ell^{b_\ell}$ for some nonnegative integers a_j, b_j for $0 \leqslant j \leqslant \ell$ such that $b_j \leqslant q - 1$ for all $j \leqslant \ell - 1$ and $b_\ell > 0$. Note that $\sigma^{(\ell)}(\mu) = x_0^{a_0} \cdots x_{\ell-1}^{a_{\ell-1}}$ and $\sigma^{(\ell)}(\nu) = x_0^{b_0} \cdots x_{\ell-1}^{b_{\ell-1}}$.

If $\mu \,|\, \nu$, then $a_i \leqslant b_i$ for $0 \leqslant i \leqslant \ell$, and this readily implies that $\sigma^{(\ell)}(\mu) \,|\, \sigma^{(\ell)}(\nu)$. To prove the converse, suppose $\sigma^{(\ell)}(\mu) \,|\, \sigma^{(\ell)}(\nu)$. Then $a_i \leqslant b_i \leqslant q - 1$ for $0 \leqslant i \leqslant \ell - 1$. Since $\sum_{i=0}^{\ell} a_i = d$ and $\sum_{i=0}^{\ell} b_i = e$, we obtain

$$b_\ell - a_\ell = e - d + \sum_{i=0}^{\ell-1}(a_i - b_i) \geqslant m(q-1) - \ell(q-1) \geqslant 0.$$

This shows that $\mu \,|\, \nu$. $\qquad\square$

Remark 5.2. Suppose $0 \leqslant d < q$. Then $\sigma^{(m)}$ gives a bijection of $\overline{\mathbb{M}}_d = \mathbb{M}_d$ onto $\mathbb{H}_{\leqslant d}^{(m)}$. Indeed, if $\mu = x_0^{a_0} \cdots x_m^{a_m} \in \overline{\mathbb{M}}_d$, then clearly, $0 \leqslant a_i \leqslant d \leqslant q - 1$ for $0 \leqslant i \leqslant m$; also $a_0 + \cdots + a_{m-1} \leqslant d$. Moreover, $a_m = d - a_0 - \cdots - a_{m-1}$, and so μ is determined by $\sigma^{(m)}(\mu) = x_0^{a_0} \cdots x_{m-1}^{a_{m-1}} \in \mathbb{H}_{\leqslant d}^{(m)}$. A similar reasoning shows that $\sigma^{(m)}$ preserves lexicographic order, i.e., for any $\mu, \nu \in \overline{\mathbb{M}}_d$, we have $\mu \prec_{\text{lex}} \nu \Leftrightarrow \sigma^{(m)}(\mu) \prec_{\text{lex}} \sigma^{(m)}(\nu)$.

The following result gives a useful relation between the two notions of footprint.

Theorem 5.3. *Let d, e be any nonnegative integers such that $e \geqslant d + m(q-1)$ and let $\mathcal{S} \subset \overline{\mathbb{M}}_d$. Then*

$$|\Delta_e^{(\ell)}(\mathcal{S}^{\langle \ell \rangle})| = |\mathsf{FP}^{(\ell)}(\sigma^{(\ell)}(\mathcal{S}^{\langle \ell \rangle}))| \quad \text{for all nonnegative integers } \ell \leqslant m,$$

and consequently,

$$|\Delta_e(\mathcal{S})| = \sum_{\ell=0}^{m} |\mathsf{FP}^{(\ell)}(\sigma^{(\ell)}(\mathcal{S}^{\langle \ell \rangle}))|.$$

Proof. Fix a nonnegative integer $\ell \leqslant m$. It is clear from Definition 3.3 that $\sigma^{(\ell)}(\mathcal{S}^{\langle \ell \rangle}) \subseteq \mathbb{H}^{(\ell)}$. From Proposition 5.1, we see that the map

$$\Delta_e^{(\ell)}(\mathcal{S}^{\langle \ell \rangle}) \to \mathsf{FP}^{(\ell)}(\sigma^{(\ell)}(\mathcal{S}^{\langle \ell \rangle})) \quad \text{defined by} \quad \mu \mapsto \sigma^{(\ell)}(\mu)$$

is well-defined. Moreover, since $e \geqslant d + m(q-1)$, this map is easily seen to be a bijection. This yields the first assertion in the theorem. Consequently, we obtain the last assertion from equation (21). $\square$

5.2. Footprint expander. In this subsection, we consider a degree-preserving map ϕ on sets of projectively reduced monomials in $x_0, \ldots, x_m$ such that ϕ is injective and has the property that $|\Delta_e(\mathcal{S})| \leqslant |\Delta_e(\phi(\mathcal{S}))|$ for any $\mathcal{S} \subseteq \overline{\mathbb{M}}$ and $e \gg 0$. For this reason, ϕ may be referred to as an *expander* map.

Definition 5.4. Let $\mathcal{S} \subseteq \overline{\mathbb{M}}$. If $\mu = x_0^{i_0} \cdots x_m^{i_m} \in \mathcal{S}$, then define

$$\phi(\mu) := \begin{cases} \mu \frac{x_{m-1}}{x_m} & \text{if } x_0^{i_0} \cdots x_{m-2}^{i_{m-2}} x_{m-1}^{i_{m-1}+i_m} \notin \mathcal{S} \text{ and } i_{m-1} + 1 < q, \\ \mu & \text{otherwise.} \end{cases}$$

Note that if $i_m = 0$, then $x_0^{i_0} \cdots x_{m-2}^{i_{m-2}} x_{m-1}^{i_{m-1}+i_m} = \mu \in \mathcal{S}$. Hence, in the first case of the definition, we must have $i_m > 0$. In particular, $\phi(\mu)$ is always a monomial, and we obtain a well-defined map $\phi \colon \mathcal{S} \to \overline{\mathbb{M}}$ which preserves degrees.

Proposition 5.5. *Let $\mathcal{S} \subseteq \overline{\mathbb{M}}$. Then the map $\phi \colon \mathcal{S} \to \overline{\mathbb{M}}$ is injective and it satisfies*

$$\mathcal{S}^{\langle m-1 \rangle} = \phi(\mathcal{S}^{\langle m-1 \rangle}) \subseteq \phi(\mathcal{S})^{\langle m-1 \rangle} \quad \text{and} \quad \phi(\mathcal{S}^{\langle m \rangle}) = \phi(\mathcal{S})^{\langle m \rangle}.$$

Proof. It is easy to see that ϕ is injective. Also, as noted earlier, $\phi(\mu) = \mu$ in case $\mu \in \mathcal{S}^{\langle m-1 \rangle}$. This implies that $\mathcal{S}^{\langle m-1 \rangle} = \phi(\mathcal{S}^{\langle m-1 \rangle}) \subseteq \phi(\mathcal{S})^{\langle m-1 \rangle}$. To prove that $\phi(\mathcal{S}^{\langle m \rangle}) = \phi(\mathcal{S})^{\langle m \rangle}$, suppose $\mu = x_0^{i_0} \cdots x_m^{i_m} \in \mathcal{S}^{\langle m \rangle}$. Then $i_j < q$ for $0 \leqslant j \leqslant m-1$. In case $\phi(\mu) = \mu$, then clearly, $\phi(\mu) \in \phi(\mathcal{S})^{\langle m \rangle}$. In particular, if $i_{m-1} = q-1$, then $\phi(\mu) \in \phi(\mathcal{S})^{\langle m \rangle}$ because in this case, $i_{m-1} + 1 = q$ and so $\phi(\mu) = \mu$. On the other hand, if $i_{m-1} < q-1$ and $\phi(\mu) \neq \mu$, then $\phi(\mu) = x_0^{i_0} \cdots x_{m-1}^{i_{m-1}+1} x_m^{i_m-1}$. Since $i_{m-1} + 1 < q$, we obtain $\phi(\mu) \in \phi(\mathcal{S})^{\langle m \rangle}$. This shows that $\phi(\mathcal{S}^{\langle m \rangle}) \subseteq \phi(\mathcal{S})^{\langle m \rangle}$. In order to prove the reverse inclusion, we take $\mu \in \phi(\mathcal{S})^{\langle m \rangle}$. Since $\mu \in \phi(\mathcal{S})$, there exists $\mu' \in \mathcal{S}$ such that $\phi(\mu') = \mu$. It is trivial to see that $\mu' \in \mathcal{S}^{\langle m \rangle}$. $\square$

We now give a series of lemmas and a proposition leading to the result that ϕ does not decrease footprints in $\overline{\mathbb{M}}_e$ for all large enough e.

Lemma 5.6. *Let $\mathcal{S}$ be a finite subset of $\overline{\mathbb{M}}$. Then $\Delta_e^{(m)}(\mathcal{S}) \subseteq \Delta_e^{(m)}(\phi(\mathcal{S}))$ for all $e \gg 0$.*

Proof. It suffices to show that $\nabla_e^{(m)}(\phi(\mathcal{S})) \subseteq \nabla_e^{(m)}(\mathcal{S})$ for all $e \gg 0$. To this end, let $\nu \in \nabla_e^{(m)}(\phi(\mathcal{S}))$. Then $\nu \in \overline{\mathbb{M}}_e^{(m)}$ and there exists $\mu \in \phi(\mathcal{S})$ such that $\mu \,|\, \nu$. If $\mu \in \mathcal{S}$, then $\nu \in \nabla_e^{(m)}(\mathcal{S})$. Suppose $\mu \notin \mathcal{S}$. Since $\mu \in \phi(\mathcal{S})$, it follows from Definition 5.4 that $\mu x_m/x_{m-1} \in \mathcal{S}$. In particular, $x_{m-1} \,|\, \mu$ and $(\mu/x_{m-1}) \,|\, \nu$. Further, since $\nu \in \overline{\mathbb{M}}_e^{(m)}$, we see that $\deg_{x_m} \nu \gg 0$ for all $e \gg 0$, whereas $\deg_{x_m} \mu$ is bounded since $\mathcal{S}$ is finite. Consequently, $(\mu x_m/x_{m-1}) \,|\, \nu$, and so $\nu \in \nabla_e^{(m)}(\mathcal{S})$ for $e \gg 0$. $\qquad\square$

Lemma 5.7. *Let $\mathcal{S} \subseteq \overline{\mathbb{M}}$. Then $\Delta_e^{(m-1)}(\phi(\mathcal{S})) \subseteq \Delta_e^{(m-1)}(\mathcal{S})$ for all $e \geqslant 0$.*

Proof. Fix a nonnegative integer e. We will show that $\nabla_e^{(m-1)}(\mathcal{S}) \subseteq \nabla_e^{(m-1)}(\phi(\mathcal{S}))$. Let $\nu \in \nabla_e^{(m-1)}(\mathcal{S})$. Then $\nu \in \overline{\mathbb{M}}_e^{(m-1)}$ and there exists $\mu \in \mathcal{S}$ such that $\mu \,|\, \nu$. In particular, $\deg_{x_m} \mu \leqslant \deg_{x_m} \nu = 0$, and so $\phi(\mu) = \mu$. It follows that $\mu \in \phi(\mathcal{S})$ and so $\nu \in \nabla_e^{(m-1)}(\phi(\mathcal{S}))$. $\qquad\square$

Lemma 5.8. *Let $\mathcal{S} \subseteq \overline{\mathbb{M}}$ and let e be a nonnegative integer. Suppose $\nu \in \Delta_e^{(m-1)}(\mathcal{S})$ and $\mu \in \overline{\mathbb{M}}$ satisfy $\mu \,|\, \nu$. Then $\mu \notin \mathcal{S}^{\langle m-1 \rangle}$.*

Proof. Since $\Delta_e^{(m-1)}(\mathcal{S}) = \Delta_e^{(m-1)}(\mathcal{S}^{\langle m-1 \rangle})$, this follows directly. $\qquad\square$

Lemma 5.9. *Let $\mathcal{S} \subseteq \overline{\mathbb{M}}$ and let e be a nonnegative integer. Suppose there exists $\nu \in \Delta_e^{(m-1)}(\mathcal{S}) \setminus \Delta_e^{(m-1)}(\phi(\mathcal{S}))$, i.e., $\nu \in \nabla_e^{(m-1)}(\phi(\mathcal{S})) \setminus \nabla_e^{(m-1)}(\mathcal{S})$. Then the set $\{\mu \in \mathcal{S} \colon \deg_{x_{m-1}} \mu < q$ and $\mu \,|\, (\nu x_m)\}$ is nonempty.*

Proof. Since $\nu \in \nabla_e^{(m-1)}(\phi(\mathcal{S})) = \nabla_e^{(m-1)}(\phi(\mathcal{S})^{\langle m-1 \rangle})$, there exists $\tilde{\mu} \in \phi(\mathcal{S})^{\langle m-1 \rangle}$ such that $\tilde{\mu} \,|\, \nu$. Moreover, $\nu \notin \nabla_e^{(m-1)}(\mathcal{S})$ implies $\tilde{\mu} \notin \mathcal{S}$. Hence $x_{m-1} \,|\, \tilde{\mu}$ and $\tilde{\mu} x_m/x_{m-1} \in \mathcal{S}$. Let $\mu := \tilde{\mu} x_m/x_{m-1}$. Note that μ is projectively reduced since $\mu \in \mathcal{S}$. Further, $\deg_{x_m} \mu > 0$ since $\phi(\mu) \neq \mu$. This implies that $\deg_{x_{m-1}} \mu < q$. Also, since $\tilde{\mu} \,|\, \nu$, we see that $\tilde{\mu}/x_{m-1}$ divides ν and so $\mu \,|\, (\nu x_m)$. $\qquad\square$

Proposition 5.10. *Let $\mathcal{S} \subset \overline{\mathbb{M}}$ be a finite set. Then*

$$\left| \Delta_e^{(m-1)}(\mathcal{S}) \setminus \Delta_e^{(m-1)}(\phi(\mathcal{S})) \right| \leqslant \left| \Delta_e^{(m)}(\phi(\mathcal{S})) \setminus \Delta_e^{(m)}(\mathcal{S}) \right| \quad \text{for all } e \gg 0.$$

Proof. For a nonnegative integer e and $\nu \in \Delta_e^{(m-1)}(\mathcal{S}) \setminus \Delta_e^{(m-1)}(\phi(\mathcal{S}))$, define

$$S_\nu := \{\mu \in \mathcal{S} \colon \deg_{x_{m-1}} \mu < q \text{ and } \mu \,|\, (\nu x_m^j) \text{ for some } j > 0\}.$$

By Lemma 5.9, the set S_ν is nonempty. Moreover, since $\mathcal{S}$ is a finite set, we see that

$$k_\nu := \min\{\deg_{x_{m-1}} \mu \colon \mu \in S_\nu\} \quad \text{and} \quad E := \max\{\deg_{x_m} \mu \colon \mu \in \mathcal{S}\}$$

are well-defined, and

$$S_\nu = \{\mu \in \mathcal{S} \colon \deg_{x_{m-1}} \mu < q \text{ and } \mu \,|\, (\nu x_m^E)\}.$$

For $e \geqslant 0$, consider the map $\psi \colon \Delta_e^{(m-1)}(\mathcal{S}) \setminus \Delta_e^{(m-1)}(\phi(\mathcal{S})) \to \overline{\mathbb{M}}_e$ given by

$$\nu = x_0^{i_0} \cdots x_{m-1}^{i_{m-1}} \mapsto x_0^{i_0} \cdots x_{m-2}^{i_{m-2}} x_{m-1}^{k_\nu} x_m^{i_{m-1}-k_\nu}.$$

Clearly, the map ψ is injective and to prove the proposition, it is enough to show that the image of ψ is contained in $\Delta_e^{(m)}(\phi(\mathcal{S})) \setminus \Delta_e^{(m)}(\mathcal{S})$, provided $e \gg 0$.

Let us fix $e \geqslant 0$ and $\nu = x_0^{i_0} \cdots x_{m-1}^{i_{m-1}} \in \Delta_e^{(m-1)}(\mathcal{S}) \setminus \Delta_e^{(m-1)}(\phi(\mathcal{S}))$. Also, for simplicity, let us write $k = k_\nu$. From Lemma 5.9, we see that $k < q$. By the definition of k, there exists $\mu^* \in \mathcal{S}$ with $\deg_{x_{m-1}} \mu^* = k$ such that $\mu^* \mid (\nu x_m^E)$. Now since $\nu \in \overline{\mathbb{M}}_e^{(m-1)}$, we see that $i_j < q$ for $0 \leqslant j < m-1$, whereas $i_{m-1} \gg 0$ if $e \gg 0$. Hence $E \leqslant i_{m-1} - k$ if $e \gg 0$. This implies that $\mu^* \mid \psi(\nu)$ whenever $e \gg 0$. Since $\mu^* \in \mathcal{S}$, we conclude that $\psi(\nu) \notin \Delta_e^{(m)}(\mathcal{S})$. We now prove that $\psi(\nu) \in \Delta_e^{(m)}(\phi(\mathcal{S}))$ for $e \gg 0$ by distinguishing two cases.

CASE 1: $k = q - 1$.

Since $\nu \in \nabla_e^{(m-1)}(\phi(\mathcal{S}))$, there exists $\mu \in \phi(\mathcal{S})$ such that $\mu \mid \nu$. Let $\tilde{\mu} \in \mathcal{S}$ be such that $\mu = \phi(\tilde{\mu})$. Then either $\tilde{\mu} = \mu$ or $\tilde{\mu} = \mu x_m / x_{m-1}$. If $\tilde{\mu} = \mu$, then $\nu \in \nabla_e^{(m-1)}(\mathcal{S})$, which is a contradiction. Thus $\tilde{\mu} = \mu x_m / x_{m-1}$. Since $\mu \mid \nu$, clearly $\tilde{\mu} \mid (\nu x_m)$. Hence $\tilde{\mu} \in S_\nu$. From the assumption that $k = q - 1$, we conclude that $\deg_{x_{m-1}}(\tilde{\mu}) = q - 1$. But then $\mu = \phi(\tilde{\mu}) = \tilde{\mu}$, which is again a contradiction. Therefore, the case $k = q - 1$ can not occur.

CASE 2: $k < q - 1$.

Suppose, if possible, $\psi(\nu) \in \nabla_e^{(m)}(\phi(\mathcal{S}))$. Then there exists $\mu \in \phi(\mathcal{S})$ such that $\mu \mid \psi(\nu)$. Write $\mu = x_0^{j_0} \cdots x_m^{j_m}$. Then $j_0 \leqslant i_0, \ldots, j_{m-2} \leqslant i_{m-2}$ and $j_{m-1} \leqslant k < q - 1$. Note that $x_0^{j_0} \cdots x_{m-2}^{j_{m-2}} x_{m-1}^{j_{m-1}+j_m} \mid \nu$ whenever $e \gg 0$. This implies that $x_0^{j_0} \cdots x_{m-2}^{j_{m-2}} x_{m-1}^{j_{m-1}+j_m} \notin \mathcal{S}$, since $\nu \in \Delta_e^{(m-1)}(\mathcal{S})$. Choose $\tilde{\mu} \in \mathcal{S}$ such that $\phi(\tilde{\mu}) = \mu$. If $\tilde{\mu} = \mu$, then by the definition of ϕ and the fact that $x_0^{j_0} \cdots x_{m-2}^{j_{m-2}} x_{m-1}^{j_{m-1}+j_m} \notin \mathcal{S}$, we conclude that $j_{m-1} \geqslant q - 1$, which is a contradiction. Therefore $\tilde{\mu} \neq \mu$. This implies that $\tilde{\mu} = x_0^{j_0} \cdots x_{m-1}^{j_{m-1}-1} x_m^{j_m+1} \in \mathcal{S}$. Furthermore, $\tilde{\mu} \mid \nu x_m^j$ whenever $j \geqslant j_m + 1$ and $e \gg 0$. Thus $\tilde{\mu} \in S_\nu$. But then $\deg_{x_{m-1}} \tilde{\mu} = j_{m-1} - 1 < j_{m-1} \leqslant k$, and this contradicts the minimality of k if $e \gg 0$. Hence $\psi(\nu) \in \Delta_e^{(m)}(\phi(\mathcal{S}))$ for $e \gg 0$. $\qquad\square$

Theorem 5.11. *Let $\mathcal{S} \subset \overline{\mathbb{M}}$ be a finite set. Then $|\Delta_e(\mathcal{S})| \leqslant |\Delta_e(\phi(\mathcal{S}))|$ for $e \gg 0$.*

Proof. Since $\phi(\mu) = \mu$ for all $\mu \in \mathcal{S}$ with $\deg_{x_m} \mu = 0$ and since $\deg_{x_{m-1}} \phi(\mu) > 0$ if $\phi(\mu) \neq \mu$, it is clear that $\mathcal{S}^{\langle j \rangle} = \phi(\mathcal{S})^{\langle j \rangle}$ for $j = 0, \ldots, m - 2$. Hence

$$\Delta_e^{(j)}(\mathcal{S}) = \Delta_e^{(j)}(\mathcal{S}^{\langle j \rangle}) = \Delta_e^{(j)}(\phi(\mathcal{S})^{\langle j \rangle}) = \Delta_e^{(j)}(\phi(\mathcal{S})) \quad \text{for all } j = 0, \ldots, m - 2.$$

Thus it is enough to show that

$$|\Delta_e^{(m)}(\mathcal{S})| + |\Delta_e^{(m-1)}(\mathcal{S})| \leqslant |\Delta_e^{(m)}(\phi(\mathcal{S}))| + |\Delta_e^{(m-1)}(\phi(\mathcal{S}))|.$$

This follows directly from Proposition 5.10 in view of Lemmas 5.6 and 5.7. $\qquad\square$

6. Number of Solutions of Equations over Finite Fields

Throughout this section, m denotes a fixed positive integer, while d, r are non-negative integers. Recall that $e_r(d, m)$ has been defined by (1) and the conventions (10) whenever $r \leqslant \binom{m+d}{d}$. In this section, we shall prove our main results concerning $e_r(d, m)$ and a related quantity, called $\bar{e}_r(d, m)$, that we shall define shortly.

6.1. Projectively reduced equations. As in Section 3.1, let $\Gamma_q(\mathbb{F}_q)$ denote the ideal of $\mathbb{F}_q[x_0, \ldots, x_m]$ generated by $\{x_i^q x_j - x_i x_j^q : 0 \leqslant i < j \leqslant m\}$. Evidently, $\Gamma_q(\mathbb{F}_q)$ is a homogeneous ideal and if we let $\Gamma_q(\mathbb{F}_q)_d$ denote its dth homogeneous component, then its vector space dimension is known, e.g., from [16, Thm. 5.2], namely

$$r_d := \dim_{\mathbb{F}_q} \Gamma_q(\mathbb{F}_q)_d = \sum_{j=2}^{m+1} (-1)^j \binom{m+1}{j} \sum_{i=0}^{j-2} \binom{d + (i+1)(q-1) - jq + m}{d + (i+1)(q-1) - jq} \quad (24)$$

for any $d \geqslant 0$. As noted in Section 3.1, the space of projectively reduced polynomials in $\mathbb{F}_q[x_0, \ldots, x_m]$ can be identified with $\mathbb{F}_q[x_0, \ldots, x_m]/\Gamma_q(\mathbb{F}_q)$. In particular, $r_d \leqslant \binom{m+d}{d}$ and the dimension of this space of projectively reduced polynomials in $\mathbb{F}_q[x_0, \ldots, x_m]_d$ is $\binom{m+d}{d} - r_d$ for any nonnegative integer d. This also shows that

$$|\overline{\mathbb{M}}_d| = \binom{m+d}{d} - r_d \quad \text{for any } d \geqslant 0. \quad (25)$$

Using this or otherwise (see for example [16, p. 237]), we readily see that

$$r_d = 0 \text{ if } d \leqslant q, \quad r_{q+1} = \binom{m+1}{2}, \quad \text{and} \quad r_d = \binom{m+d}{d} - \mathsf{p}_m \text{ if } d > m(q-1). \quad (26)$$

Definition 6.1. For any $d \geqslant 0$ and $1 \leqslant r \leqslant \binom{m+d}{d} - r_d$, we define

$$\overline{e}_r(d, m) := \max_{G_1, \ldots, G_r} |V(G_1, \ldots, G_r)(\mathbb{F}_q)|, \quad (27)$$

where the maximum is taken over all possible sets $\{G_1, \ldots, G_r\}$ of r linearly independent, projectively reduced polynomials in $\mathbb{F}_q[x_0, \ldots, x_m]_d$. As a natural convention, we set $\overline{e}_0(d, m) := 0$.

It is clear that $\overline{e}_r(d, m) \leqslant e_r(d, m)$ for all $d \geqslant 0$ and $1 \leqslant r \leqslant \binom{m+d}{d} - r_d$. A more precise relationship is given by the following.

Theorem 6.2. *Let d, r be nonnegative integers such that $r \leqslant \binom{m+d}{d} - r_d$. Then*

$$e_{r+r_d}(d, m) = \overline{e}_r(d, m).$$

In particular, $e_r(d, m) = \overline{e}_r(d, m)$ if $d \leqslant q$.

Proof. Fix a basis $\{\Phi_1, \ldots, \Phi_{r_d}\}$ of the $\mathbb{F}_q$-vector space $\Gamma_q(\mathbb{F}_q)_d$. We will show that $e_{r+r_d}(d, m) \geqslant \overline{e}_r(d, m)$ and $e_{r+r_d}(d, m) \leqslant \overline{e}_r(d, m)$.

Let $G_1, \ldots, G_r \in \mathbb{F}_q[x_0, \ldots, x_m]_d$ be linearly independent and projectively reduced polynomials such that $|V(G_1, \ldots, G_r)(\mathbb{F}_q)| = \overline{e}_r(d, m)$. Then every nontrivial linear combination of $G_1, \ldots, G_r$ is projectively reduced and therefore it does not belong to $\Gamma_q(\mathbb{F}_q)_d$. Consequently, the polynomials $G_1, \ldots, G_r, \Phi_1, \ldots, \Phi_{r_d}$ are linearly independent. Since $\Phi_1, \ldots, \Phi_{r_d}$ vanish everywhere on $\mathbb{P}^m(\mathbb{F}_q)$, we see that $V(G_1, \ldots, G_r)(\mathbb{F}_q) = V(G_1, \ldots, G_r, \Phi_1, \ldots, \Phi_{r_d})(\mathbb{F}_q)$. It follows that

$$e_{r+r_d}(d, m) \geqslant |V(G_1, \ldots, G_r, \Phi_1, \ldots, \Phi_{r_d})(\mathbb{F}_q)|$$
$$= |V(G_1, \ldots, G_r)(\mathbb{F}_q)|$$
$$= \overline{e}_r(d, m).$$

To prove the other inequality, suppose $F_1, \ldots, F_{r+r_d}$ are linearly independent polynomials in $\mathbb{F}_q[x_0, \ldots, x_m]_d$ such that $|V(F_1, \ldots, F_{r+r_d})(\mathbb{F}_q)| = e_{r+r_d}(d, m)$. Let V_{r+r_d} denote the $\mathbb{F}_q$-linear span of $F_1, \ldots, F_{r+r_d}$. Then

$$\dim_{\mathbb{F}_q} \frac{V_{r+r_d} + \Gamma_q(\mathbb{F}_q)_d}{\Gamma_q(\mathbb{F}_q)_d} \geqslant \dim_{\mathbb{F}_q} V_{r+r_d} - \dim_{\mathbb{F}_q} \Gamma_q(\mathbb{F}_q)_d = (r + r_d) - r_d = r.$$

So we can find $F_1', \ldots, F_r' \in V_{r+r_d} + \Gamma_q(\mathbb{F}_q)_d$ that are linearly independent (mod $\Gamma_q(\mathbb{F}_q)_d$). Let $G_i' = \overline{F_i'}$ denote the projective reduction of F_i'. Then $G_1', \ldots, G_r'$ are linearly independent and projectively reduced polynomials in $\mathbb{F}_q[x_0, \ldots, x_m]_d$. Hence as in the previous paragraph, we see that $G_1', \ldots, G_r', \Phi_1, \ldots, \Phi_{r_d}$ are linearly independent. Also, $F_i' - G_i' \in \Gamma_q(\mathbb{F}_q)$ for all $i = 1, \ldots, r$. It follows that

$$\begin{aligned}
e_{r+r_d}(d, m) &\geqslant |V(G_1', \ldots, G_r', \Phi_1, \ldots, \Phi_{r_d})(\mathbb{F}_q)| \\
&= |V(G_1', \ldots, G_r')(\mathbb{F}_q)| \\
&= |V(F_1', \ldots, F_r')(\mathbb{F}_q)| \\
&\geqslant |V(F_1, \ldots, F_{r+r_d})(\mathbb{F}_q)| \\
&= e_{r+r_d}(d, m).
\end{aligned}$$

Consequently, equality holds throughout, and in particular,

$$\overline{e}_r(d, m) \geqslant |V(G_1', \ldots, G_r')(\mathbb{F}_q)| = e_{r+r_d}(d, m).$$

This proves that $e_{r+r_d}(d, m) = \overline{e}_r(d, m)$. Finally, if $d \leqslant q$, then $r_d = 0$, and therefore $e_r(d, m) = \overline{e}_r(d, m)$ in this case. $\qquad\square$

Remark 6.3. As noted in [9, Rem. 6.2], one has $e_r(d, m) = \mathsf{p}_m$ if $0 \leqslant r \leqslant r_d$. Indeed, it is clear that for any $r \geqslant 0$ one has $e_r(d, m) \leqslant |\mathbb{P}^m(\mathbb{F}_q)| = \mathsf{p}_m$, while for $r \leqslant r_d$, one may choose linearly independent polynomials $G_1, \ldots, G_r \in \Gamma_q(\mathbb{F}_q)_d$ and deduce that $e_r(d, m) \geqslant |V(G_1, \ldots, G_r)(\mathbb{F}_q)| = \mathsf{p}_m$.

The vanishing ideal of $\mathbb{A}^m(\mathbb{F}_q)$ is easy to determine; it is precisely the ideal of $\mathbb{F}_q[x_1, \ldots, x_m]$ generated by $\{x_i^q - x_i : 1 \leqslant i \leqslant m\}$. It is not difficult to see (using, e.g., the principle of inclusion-exclusion) that the dimension of the $\mathbb{F}_q$-vector space of polynomials of degree $\leqslant d$ in this vanishing ideal is given by

$$\rho_d := \sum_{j=1}^m (-1)^{j-1} \binom{m}{j} \binom{m+d-jq}{d-jq} \quad \text{for all } d \geqslant 0.$$

In case $d < q$, one can directly see that $\rho_d = 0$. Since the dimension of the $\mathbb{F}_q$-vector space of polynomials of degree $\leqslant d$ in $\mathbb{F}_q[x_1, \ldots, x_m]$ is clearly $\binom{m+d}{d}$, we see that $\rho_d \leqslant \binom{m+d}{d}$ for all $d \geqslant 0$.

We have seen in Section 2.1 an affine analogue of $e_r(d, m)$, namely, $e_r^{\mathbb{A}}(d, m)$. Here is a natural affine analogue of $\overline{e}_r(d, m)$. For $0 \leqslant r \leqslant \binom{m+d}{d} - \rho_d$, we define

$$\overline{e}_r^{\mathbb{A}}(d, m) := \max_{g_1, \ldots, g_r} |Z(g_1, \ldots, g_r)(\mathbb{F}_q)|,$$

where the maximum is taken over r linearly independent and reduced polynomials $g_1, \ldots, g_r$ of degree $\leqslant d$ in $\mathbb{F}_q[x_1, \ldots, x_m]$. Arguing similarly as in the proof of

Theorem 6.2, we see that

$$e_{r+\rho_d}^{\mathbb{A}}(d,\, m) = \overline{e}_r^{\mathbb{A}}(d,\, m) \quad \text{for } 1 \leqslant r \leqslant \binom{m+d}{d} - \rho_d.$$

Moreover, $e_r^{\mathbb{A}}(d,\, m) = \overline{e}_r^{\mathbb{A}}(d,\, m)$ if $d < q$, whereas $e_r^{\mathbb{A}}(d,\, m) = q^m$ if $r \leqslant \rho_d$.

The result of Heijnen and Pellikaan [12] that was alluded to in the introduction solves the problem of determining $\overline{e}_r^{\mathbb{A}}(d,\, m)$. A special case of this (when $d < q$) was stated earlier (Theorem 2.1). Here is the general version.

Theorem 6.4 (Heijnen–Pellikaan). *Let d be a nonnegative integer. Then*

$$\overline{e}_r^{\mathbb{A}}(d,\, m) = H_r(d,\, m) \quad \text{for } 1 \leqslant r \leqslant \binom{m+d}{d} - \rho_d.$$

6.2. An upper bound. In this subsection we will use the combinatorial results in Sections 4 and 5 to obtain an upper bound for $e_r(d,\, m)$ when $d < q$. As we have seen in the last subsection, when $d \leqslant q$, the quantities $e_r(d,\, m)$ and $\overline{e}_r(d,\, m)$ coincide. Thus, we will work with $\overline{e}_r(d,\, m)$, and we begin by relating it with the "maximal footprint" defined as follows.

Definition 6.5. Given any nonnegative integers d, r and e with $1 \leqslant r \leqslant |\overline{\mathbb{M}}_d|$, i.e., $1 \leqslant r \leqslant \binom{m+d}{d} - r_d$, define

$$A_r(d,\, m;\, e) := \max\{|\Delta_e(\mathcal{S})| : \mathcal{S} \subseteq \overline{\mathbb{M}}_d \text{ with } |\mathcal{S}| = r\}.$$

The relation between $A_r(d,\, m;\, e)$ and $\overline{e}_r(d,\, m)$ is given by the lemma below. In the remainder of this section, we consider the lexicographic order $\prec_{\text{lex}}$ on the set $\mathbb{M}$ of all monomials in $x_0,\, \ldots,\, x_m$. For $0 \neq F \in \mathbb{F}_q[x_0,\, \ldots,\, x_m]$, the largest monomial (w.r.t. $\prec_{\text{lex}}$) appearing in F (with a nonzero coefficient) will be denoted by $\text{lm}(F)$.

Lemma 6.6. *Let d, r be nonnegative integers with $1 \leqslant r \leqslant \binom{m+d}{d} - r_d$. Then*

$$\overline{e}_r(d,\, m) = \max_{F_1, \ldots, F_r} |V(F_1,\, \ldots,\, F_r)(\mathbb{F}_q)|,$$

where the maximum is over all possible sets $\{F_1,\, \ldots,\, F_r\}$ of linearly independent and projectively reduced polynomials in $\mathbb{F}_q[x_0,\, \ldots,\, x_m]_d$ such that their leading monimials $\text{lm}(F_1),\, \ldots,\, \text{lm}(F_r)$ are distinct. Consequently,

$$\overline{e}_r(d,\, m) \leqslant A_r(d,\, m;\, e) \quad \text{for all } e \gg 0.$$

Proof. If $G_1,\, \ldots,\, G_r \in \mathbb{F}_q[x_0,\, \ldots,\, x_m]_d$ are linearly independent and projectively reduced, then we can easily obtain $F_1,\, \ldots,\, F_r \in \mathbb{F}_q[x_0,\, \ldots,\, x_m]_d$ that are linearly independent and projectively reduced such that $\text{lm}(F_1),\, \ldots,\, \text{lm}(F_r)$ are distinct and $V(F_1,\, \ldots,\, F_r) = V(G_1,\, \ldots,\, G_r)$. For example, we can obtain them recursively by taking $F_1 := G_1$ and for $1 < i \leqslant r$, taking $F_i := G_i - c_1 F_1 - \cdots - c_{i-1} F_{i-1}$, where $c_1,\, \ldots,\, c_{i-1} \in \mathbb{F}_q$ are chosen in such a way that none among $\text{lm}(F_1),\, \ldots,\, \text{lm}(F_{i-1})$ appear in F_i. This proves the first assertion. The second assertion follows from the first using the projective $\mathbb{F}_q$-footprint bound (Theorem 3.2). $\qquad\square$

The following result could be viewed as a projective analogue of Theorem 4.6, which in turn arose from the works of Clements–Lindström [7], Wei [20] and Heijnen–Pellikaan [12], [13]. For any integers d, r with $d \geqslant 0$ and $1 \leqslant r \leqslant$

$\binom{m+d}{d} - r_d$, we denote by $\mathcal{M}_d(r)$ the set of first r elements of $\overline{\mathbb{M}}_d$ in descending lexicographic order, and for any $d \geqslant 0$, we set $\mathcal{M}_d(r)$ to be the empty set if $r = 0$.

Theorem 6.7. *Let d, r be integers with $1 \leqslant d < q$ and $1 \leqslant r \leqslant \binom{m+d}{d} - r_d$. Then*

$$|\Delta_e(\mathcal{S})| \leqslant \left|\Delta_e(\mathcal{M}_d(r))\right| \quad \text{for all } e \gg 0 \text{ and } \mathcal{S} \subseteq \overline{\mathbb{M}}_d \text{ with } |\mathcal{S}| = r. \quad (28)$$

Consequently, $A_r(d, m; e) = |\Delta_e(\mathcal{M}_d(r))|$ and $\overline{e}_r(d, m) \leqslant |\Delta_e(\mathcal{M}_d(r))|$ for $e \gg 0$.

Proof. We prove (28) by induction on m. Suppose $m = 1$ and $\mathcal{S} = \{\mu_1, \ldots, \mu_r\} \subseteq \overline{\mathbb{M}}_d$. We may assume, without loss of generality, that $\mu_1 \succ_{\text{lex}} \ldots \succ_{\text{lex}} \mu_r$. Since the set $\overline{\mathbb{M}}_d$ consists of $x_0^d \succ_{\text{lex}} x_0^{d-1}x_1 \succ_{\text{lex}} \ldots \succ_{\text{lex}} x_1^d$, we obtain $\deg_{x_0} \mu_r < \cdots < \deg_{x_0} \mu_1$.

Now observe that if $e \gg 0$, then $\Delta_e^{(0)}(\mathcal{S}) = \varnothing$ if $x_0^d \in \mathcal{S}$, whereas $\Delta_e^{(0)}(\mathcal{S}) = \{x_0^e\}$ if $x_0^d \notin \mathcal{S}$. Also, if $i := \deg_{x_0} \mu_r$ and $e \geqslant i-1$, then $\Delta_e^{(1)}(\mathcal{S}) = \{x_0^{i-1}x_1^{e-i+1}, \ldots, x_1^e\}$, and so $|\Delta_e^{(1)}(\mathcal{S})| = \deg_{x_0} \mu_r$. Consequently, if $x_0^d \in \mathcal{S}$, then $\deg_{x_0} \mu_r \leqslant d-r+1$ and

$$|\Delta_e(\mathcal{S})| = |\Delta_e^{(0)}(\mathcal{S})| + |\Delta_e^{(1)}(\mathcal{S})| = 0 + \deg_{x_0} \mu_r \leqslant d - r + 1 \quad \text{for all } e \gg 0,$$

whereas if $x_0^d \notin \mathcal{S}$, then $\deg_{x_0} \mu_r \leqslant d - r$ and

$$|\Delta_e(\mathcal{S})| = |\Delta_e^{(0)}(\mathcal{S})| + |\Delta_e^{(1)}(\mathcal{S})| = 1 + \deg_{x_0} \mu_r \leqslant d - r + 1 \quad \text{for all } e \gg 0.$$

On the other hand, $\mathcal{M}_d(r) = \{x_0^d, x_0^{d-1}x_1, \ldots, x_0^{d-r+1}x_1^{r-1}\}$ and a similar reasoning shows that $|\Delta_e(\mathcal{M}_d(r))| = d - r + 1$ for all $e \gg 0$.

Next suppose $m > 1$ and (28) holds for all values of m smaller than the given one. Consider any $\mathcal{S} \subseteq \overline{\mathbb{M}}_d$ with $|\mathcal{S}| = r$ and let $r' := |\mathcal{S}^{\langle m-1 \rangle}|$. By Theorem 5.3,

$$|\Delta_e(\mathcal{S})| = \sum_{\ell=0}^m |\Delta_e^{(\ell)}(\mathcal{S})| = \sum_{\ell=0}^m |\mathsf{FP}^{(\ell)}(\sigma^{(\ell)}(\mathcal{S}^{\langle \ell \rangle}))|.$$

Moreover $\mathcal{S}^{\langle m \rangle} = \mathcal{S}$, since $d < q$. This implies that $|\mathcal{S}| = |\sigma^{(m)}(\mathcal{S}^{\langle m \rangle})| = r$ and $\sigma^{(m)}(\mathcal{S}^{\langle m \rangle}) \subset \mathbb{H}_{\leqslant d}^{(m)}$. Hence by Theorem 4.7,

$$|\Delta_e^{(m)}(\mathcal{S})| = |\mathsf{FP}^{(m)}(\sigma^{(m)}(\mathcal{S}^{\langle m \rangle}))| \leqslant |\mathsf{FP}^{(m)}(T)|,$$

where $T = \mathcal{L}_d^{(m)}(r') \cup \mathcal{M}_{d-1}^{(m)}(r - r')$. Now define

$$\mathcal{T} := \mathcal{L}_d^{(m)}(r') \cup x_m \mathcal{M}_{d-1}(r - r'),$$

where $x_m \mathcal{M}_{d-1}(r - r') = \{x_m \mu : \mu \in \mathcal{M}_{d-1}(r - r')\}$. Since $d < q$, we readily see that $\mathcal{T} \subset \overline{\mathbb{M}}_d$, $|\mathcal{T}| = r$, and $\sigma^{(m)}(\mathcal{T}) = T$. Therefore by Theorem 5.3,

$$|\Delta_e^{(m)}(\mathcal{S})| \leqslant |\mathsf{FP}^{(m)}(\sigma^{(m)}(\mathcal{T}))| = |\Delta_e^{(m)}(\mathcal{T})|.$$

On the other hand, by the induction hypothesis,

$$\sum_{\ell=0}^{m-1} |\Delta_e^{(\ell)}(\mathcal{S})| \leqslant \sum_{\ell=0}^{m-1} |\Delta_e^{(\ell)}(\mathcal{T})|.$$

Consequently, from equation (19) and the definition of $\mathcal{T}$, it follows that

$$|\Delta_e(\mathcal{S})| = \sum_{\ell=0}^{m} |\Delta_e^{(\ell)}(\mathcal{S})| \leqslant \sum_{\ell=0}^{m} |\Delta_e^{(\ell)}(\mathcal{T})| = |\Delta_e(\mathcal{L}_d^{(m)}(r') \cup x_m \mathcal{M}_{d-1}(r - r'))|. \quad (29)$$

With this in view, we can replace $\mathcal{S}$ by $\mathcal{L}_d^{(m)}(r') \cup x_m \mathcal{M}_{d-1}(r - r')$. Thus, to prove (28), it suffices to show that $|\Delta_e(\mathcal{S})| \leqslant |\Delta_e(\mathcal{T})|$ for all $e \gg 0$, where we now take

$$\mathcal{S} := \mathcal{L}_d^{(m)}(r') \cup x_m \mathcal{M}_{d-1}(r - r') \quad \text{and} \quad \mathcal{T} := \mathcal{M}_d(r).$$

In view of Remark 5.2, $\sigma^{(m)}(\mathcal{T}) = \mathcal{M}_d^{(m)}(r)$. Also clearly, $\mathcal{T}^{\langle m-1 \rangle} = \mathcal{L}_d^{(m)}(s')$ and $\mathcal{T} \setminus \mathcal{T}^{\langle m-1 \rangle} = x_m \mathcal{M}_{d-1}(r - s')$ for some $s' \geqslant 0$. Now we distinguish two cases.

CASE 1: $r' < s'$.

Let α be the $(r'+1)^{\text{th}}$ element of $\mathbb{H}_d^{(m)}$. Since $r' < s'$, we see that $\alpha \in \mathcal{L}_d^{(m)}(s')$ and $\alpha \notin \mathcal{L}_d^{(m)}(r')$. In particular, $\alpha \in \mathcal{T} \setminus \mathcal{S}$. We claim that there exists $\beta \in \mathcal{S}$ such that $\beta \prec_{\text{lex}} \alpha$. Suppose, if possible, the claim is false. Then $\alpha \preccurlyeq_{\text{lex}} \beta$ for every $\beta \in \mathcal{S}$. Since $\alpha \in \mathcal{T}$ and $\mathcal{T} = \mathcal{M}_d(r)$, this will imply that $\beta \in \mathcal{T}$ for all $\beta \in \mathcal{S}$. Thus, $\mathcal{S} \subset \mathcal{T}$. Further, the fact that $|\mathcal{S}| = |\mathcal{T}| = r$ implies that $\mathcal{S} = \mathcal{T}$. But this is a contradiction since $\alpha \in \mathcal{T} \setminus \mathcal{S}$. Hence the claim is true. Note that if $\beta \in \mathcal{S}$ is such that $\beta \prec_{\text{lex}} \alpha$, then $\alpha \notin \mathcal{L}_d^{(m)}(r')$ implies that $\beta \notin \mathcal{L}_d^{(m)}(r')$, and so $\beta \in x_m \mathcal{M}_{d-1}(r - r')$. Now choose $\gamma = x_0^{i_0} \cdots x_m^{i_m}$ to be the largest (in lexicographical order) element of $\mathcal{S}$ such that $\gamma \prec_{\text{lex}} \alpha$. Then, as noted above, $\gamma \in x_m \mathcal{M}_{d-1}(r - r')$. Consider $\mu := \gamma x_{m-1}/x_m$. Since $\gamma \in x_m \mathcal{M}_{d-1}(r - r')$ and $d < q$, we see that $\mu \in \overline{\mathbb{M}}_d$. Moreover, $\mu \succ_{\text{lex}} \gamma$ and in fact, μ is the immediate successor of γ in $\overline{\mathbb{M}}_d$ in the lexicographic order. Hence $\gamma \prec_{\text{lex}} \alpha$ implies that $\mu \preccurlyeq_{\text{lex}} \alpha$. In case $x_m \mid \mu$, then $\mu \in x_m \mathcal{M}_{d-1}(r - r')$ because $\mu \succ_{\text{lex}} \gamma$ and $x_m \mathcal{M}_{d-1}(r - r')$ is upwards closed in $x_m \overline{\mathbb{M}}_{d-1}$. But then $\mu \in \mathcal{S}$, and this contradicts the maximality of γ. Thus $x_m \nmid \mu$, i.e., $i_m = 1$ and $\mu \notin \mathcal{S}$. In particular, since $d < q$, we see that $i_{m-1} + 1 < q$ and $x_0^{i_0} \cdots x_{m-2}^{i_{m-2}} x_{m-1}^{i_{m-1}+i_m} = \mu \notin \mathcal{S}$. Hence by Definition 5.4, $\mu = \phi(\gamma) \in \phi(\mathcal{S})^{\langle m-1 \rangle}$, even though $\gamma \notin \mathcal{S}^{\langle m-1 \rangle}$. On the other hand, if $\nu \in \mathcal{S}^{\langle m-1 \rangle}$, then clearly, $\phi(\nu) = \nu$, and so $\nu \in \phi(\mathcal{S})^{\langle m-1 \rangle}$. This shows that $r'' := |\phi(\mathcal{S})^{\langle m-1 \rangle}| > |\mathcal{S}^{\langle m-1 \rangle}| = r'$. Moreover, by Theorem 5.11, $|\Delta_e(\mathcal{S})| \leqslant |\Delta_e(\phi(\mathcal{S}))|$. Now, if $r'' < s'$, then we iterate the procedure by replacing $\mathcal{S}$ with $\phi(\mathcal{S})$. Else we proceed to the next case.

CASE 2: $r' \geqslant s'$.

In this case, for $\ell = 0, \ldots, m-1$,

$$\Delta_e^{(\ell)}(\mathcal{S}) = \Delta_e^{(\ell)}(\mathcal{L}_d^{(m)}(r')) \subseteq \Delta_e^{(\ell)}(\mathcal{L}_d^{(m)}(s')) = \Delta_e^{(\ell)}(\mathcal{T}) \quad \text{for all } e \gg 0.$$

Moreover, $\sigma^{(m)}(\mathcal{T}) = \mathcal{M}_d^{(m)}(r)$ and so by Theorem 4.6,

$$|\Delta_e^{(m)}(\mathcal{S})| = |\mathsf{FP}^{(m)}(\sigma^{(m)}(\mathcal{S}^{\langle m \rangle}))| \leqslant |\mathsf{FP}^{(m)}(\sigma^{(m)}(\mathcal{T}))| = |\Delta_e^{(m)}(\mathcal{T})| \quad \text{for all } e \gg 0.$$

Hence from equation (19), we obtain $|\Delta_e(\mathcal{S})| \leqslant |\Delta_e(\mathcal{T})|$ for all $e \gg 0$, as desired. $\qquad\square$

We are now ready to obtain an upper bound for $e_r(d, m)$ mentioned in the introduction. For any integers d, r with $d \geqslant 0$ and $1 \leqslant r \leqslant \binom{m+d}{d} - r_d$, let us define

$$K_r(d, m) := \sum_{j=0}^{m-1} a_j \mathsf{p}_{m-1-j},$$

where $(a_0, \ldots, a_m)$ denotes the rth element, in lexicographic order, of the set of $(m + 1)$-tuple $(b_0, \ldots, b_m)$ of nonnegative integers such that $b_0 + \cdots + b_m = d$, or in other words, $a_0, \ldots, a_m$ are unique nonnegative integers such that $x_0^{a_0} \cdots x_m^{a_m}$ is the smallest monomial in $\mathcal{M}_d(r)$ in lexicographic order.

Theorem 6.8. *Let d, r be integers such that $1 \leqslant d < q$ and $1 \leqslant r \leqslant \binom{m+d}{d}$. Then $A_r(d, m; e) = K_r(d, m)$ for all $e \gg 0$. Consequently,*

$$e_r(d, m) \leqslant K_r(d, m).$$

Proof. Let $x_0^{a_0} \cdots x_m^{a_m}$ be the smallest monomial in $\mathcal{M}_d(r)$ in lexicographic order. In view of Theorem 6.7, it suffices to show that

$$|\Delta_e(\mathcal{M}_d(r))| = \sum_{j=0}^{m-1} a_j \mathsf{p}_{m-1-j} \quad \text{for all } e \gg 0.$$

We will prove this by induction on m. The case $m = 1$ is easy, since we have already noted in the proof of Theorem 6.7 that $|\Delta_e(\mathcal{M}_d(r))| = d - r + 1 = (d - r + 1)\mathsf{p}_0$ and $x_0^{d-r+1} x_1^{r-1}$ is the smallest monomial in $\mathcal{M}_d(r)$ in lexicographic order if $m = 1$.

Now suppose that $m > 1$ and the result holds for all values of m smaller than the given one. In view of Remark 5.2, $\sigma^{(m)}(\mathcal{M}_d(r)) = \mathcal{M}_d^{(m)}(r)$ and therefore from equation (20) and Theorem 5.3, we see that

$$|\Delta_e^{(m)}(\mathcal{M}_d(r))| = |\mathsf{FP}^{(m)}(\mathcal{M}_d^{(m)}(r))| = \sum_{j=0}^{m-1} a_j q^{m-1-j} \quad \text{for all } e \gg 0,$$

where the last equality follows from [12, Prop. 5.9] (see also [3, Lem. 4.2]). On the other hand, from equations (19) and (20), we see that

$$
\begin{aligned}
|\Delta_e(\mathcal{M}_d(r))| &= |\Delta_e^{(m)}(\mathcal{M}_d(r))| + \sum_{j=0}^{m-1} |\Delta_e^{(j)}(\mathcal{M}_d(r)^{\langle j \rangle})| \\
&= |\Delta_e^{(m)}(\mathcal{M}_d(r))| + |\Delta_e(\mathcal{M}_d(r)^{\langle m-1 \rangle})| \quad \text{for all } e \geqslant 0,
\end{aligned}
$$

Note that the smallest monomial in $\mathcal{M}_d(r)^{\langle m-1 \rangle}$ equals $x_0^{a_0} \cdots x_{m-2}^{a_{m-2}} x_{m-1}^{a_{m-1}+a_m}$. Hence using the induction hypothesis, we obtain

$$|\Delta_e(\mathcal{M}_d(r))| = \sum_{j=0}^{m-1} a_j q^{m-1-j} + \sum_{j=0}^{m-2} a_j \mathsf{p}_{m-2-j} = \sum_{j=0}^{m-1} a_j \mathsf{p}_{m-1-j} \quad \text{for all } e \gg 0.$$

This completes the proof. $\qquad \square$

As an application of Theorem 6.8, we show below that Conjecture 2.4 holds (in the affirmative) for some "large" values of r.

Lemma 6.9. *Let d be a positive integer with $d < q$ and let $r = \sum_{a=1}^{i} \binom{m+d-a}{d-1}$ for some positive integer $i \leqslant m + 1$. Then Conjecture 2.4 holds and*

$$e_r(d,\, m) = \mathsf{p}_{m-i}.$$

Proof. If $i = m + 1$, then by equation (11), $r = \binom{m+d}{d}$, and in this case it is clear that $e_r(d,\, m) = 0 = \mathsf{p}_{m-i}$. Now suppose $i \leqslant m$ so that $r < \binom{m+d}{d}$. We claim that the $(r+1)^{\text{th}}$ monomial of $\overline{\mathbb{M}}_d$ in descending lexicographical order is given by x_i^d. This is clear if $i = m$, and the general case follows by decreasing induction on i if we note that for $i < m$, the monomials $\mu \in \overline{\mathbb{M}}_d$ that satisfy $x_i^d \succcurlyeq_{\text{lex}} \mu \succ_{\text{lex}} x_{i+1}^d$ are precisely the monomials of degree d in the $m - i + 1$ variables $x_i, \ldots, x_m$ that are divisible by x_i, and the number of such monomials is clearly $\binom{m-i+d-1}{d-1}$, i.e., $\binom{m+d-(i+1)}{d-1}$. From the above claim, it follows that the rth monomial of $\overline{\mathbb{M}}_d$ in descending lexicographical order is given by $x_{i-1}x_m^{d-1}$. Hence Theorem 6.8 implies that $e_r(d,\, m) \leqslant \mathsf{p}_{m-1-(i-1)} = \mathsf{p}_{m-i}$, while Theorem 2.3 shows that

$$e_r(d,\, m) \geqslant \mathsf{p}_{m-i-1} + H_0(d-1,\, m-i) = \mathsf{p}_{m-i-1} + q^{m-i} = \mathsf{p}_{m-i}.$$

This proves the lemma. $\qquad\square$

In the next section, we use a little trick from coding theory and results proved in this section to prove the validity of Conjecture 2.4 for some more values of r.

7. Connection with Projective Reed–Muller Codes

We begin by recalling some basics about linear codes and the notion of generalized Hamming weight that is relevant for us. We will then consider the projective Reed–Muller codes, and show that the determination of their generalized Hamming weights is intimately related to the problem considered in this paper. As before, m will denote a fixed positive integer. Moreover, n, k are positive integers with $k \leqslant n$.

7.1. Generalized Hamming weights and projective Reed–Muller codes.
Recall that a *q-ary $[n,\, k]$ (error-correcting linear) code* is defined as a k-dimensional $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$. If C is a q-ary $[n,\, k]$ code, then the parameters n and k are known, respectively, as the *length* and the *dimension* of C. For any $D \subseteq \mathbb{F}_q^n$, we define the *support* of D to be the subset

$$\mathrm{Supp}(D) = \{i \in \{1, \ldots, n\} \colon c_i \neq 0 \text{ for some } (c_1, \ldots, c_n) \in D\}$$

and the *support weight* of D, denoted $\mathrm{w}_H(D)$, to be the cardinality of $\mathrm{Supp}(D)$.

Let C be a q-ary $[n,\, k]$ code. For $1 \leqslant r \leqslant k$, the rth *generalized Hamming weight* (also known as the rth *higher weight*) of C is defined to be

$$d_r(C) := \min\{\mathrm{w}_H(D) \colon D \text{ subspace of } C \text{ with } \dim D = r\}.$$

Note that $d_1(C)$ is the minimum distance of C. The notion of generalized Hamming weights was introduced by Wei [20] and he showed that for any q-ary $[n,\, k]$ code C,

$$1 \leqslant d_1(C) < d_2(C) \cdots < d_k(C) \leqslant n. \tag{30}$$

Also, it is clear that $d_k(C) = n$ if C is *nondegenerate*, i.e., C is not contained in a coordinate hyperplane of $\mathbb{F}_q^n$.

We now recall the projective Reed–Muller codes, introduced by Lachaud [15]. Let $P_1, \ldots, P_{\mathsf{p}_m}$ be some fixed representatives in $\mathbb{F}_q^{m+1}$ for the p_m points of $\mathbb{P}^m(\mathbb{F}_q)$, e.g., we could represent each point of $\mathbb{P}^m(\mathbb{F}_q)$ by an $(m+1)$-tuple of elements of $\mathbb{F}_q$, not all zero, such that the last nonzero coordinate is 1. Consider the linear map

$$\mathrm{ev}\colon \mathbb{F}_q[x_0, \ldots, x_m] \to \mathbb{F}_q^{\mathsf{p}_m} \quad \text{given by} \quad \mathrm{ev}(F) = (F(P_1), \ldots, F(P_{\mathsf{p}_m})).$$

The dth order *projective Reed–Muller code*, denoted by $\mathrm{PRM}_q(d, m)$, is defined as the image of the space of homogeneous polynomials of degree d in $x_0, \ldots, x_m$ with coefficients in $\mathbb{F}_q$, under the map ev, i.e., $\mathrm{PRM}_q(d, m) := \mathrm{ev}(\mathbb{F}_q[x_0, \ldots, x_m]_d)$. Note that $\mathrm{PRM}_q(d, m)$ is a nondegenerate linear code of length p_m. A formula for the dimension of $\mathrm{PRM}_q(d, m)$ can be deduced from the observations in Sections 3.1 and 6.1. Indeed, these observations show that the kernel of the map ev restricted to $\mathbb{F}_q[x_0, \ldots, x_m]_d$ is precisely $\Gamma_q(\mathbb{F}_q)_d$; consequently, in view of equations (24) and (25), and with r_d as in (24), we see that

$$\mathrm{PRM}_q(d, m) \cong \frac{\mathbb{F}_q[x_0, \ldots, x_m]_d}{\Gamma_q(\mathbb{F}_q)_d} \quad \text{and} \quad \dim \mathrm{PRM}_q(d, m) = |\overline{\mathbb{M}}_d| = \binom{m+d}{d} - r_d.$$

Thus we see that the dimension, say $k_q(d, m)$, of $\mathrm{PRM}_q(d, m)$ is given by

$$k_q(d, m) = \binom{m+d}{d} - \sum_{j=2}^{m+1}(-1)^j\binom{m+1}{j}\sum_{i=0}^{j-2}\binom{d+(i+1)(q-1)-jq+m}{d+(i+1)(q-1)-jq}.$$

In view of (26), this formula simplifies to $\binom{m+d}{d}$ if $d \leqslant q$ and to p_m if $d \geqslant m(q-1)+1$. In fact, if $d \geqslant m(q-1)+1$, then $\mathrm{PRM}_q(d, m) = \mathbb{F}_q^{\mathsf{p}_m}$. Thus projective Reed–Muller codes are of interest only when $d \leqslant m(q-1)$. The following result of Sørensen [19, Thm. 1] gives an alternative formula for the dimension and an explicit formula for the minimum distance of projective Reed–Muller codes of an arbitrary order.

Theorem 7.1 (Sørensen). *Suppose $1 \leqslant d \leqslant m(q-1)$. Then the projective Reed–Muller code $\mathrm{PRM}_q(d, m)$ is a nondegenerate linear code with*

$\quad$ (i) $\dim \mathrm{PRM}_q(d, m) = \displaystyle\sum_{\substack{t=1 \\ t \equiv d \pmod{q-1}}}^{d}\left(\sum_{j=0}^{m+1}(-1)^j\binom{m+1}{j}\binom{t-jq+m}{t-jq}\right),$

$\quad$ (ii) $d_1(\mathrm{PRM}_q(d, m)) = (q-s)q^{m-t-1}$, *where s and t are unique integers such that $d-1 = t(q-1)+s$ and $0 \leqslant s < q-1$.*

7.2. Connection with homogeneous equations over finite fields. It was noted in [10, §4.2] that if $d \leqslant q$, then $d_r(\mathrm{PRM}_q(d, m)) = \mathsf{p}_m - e_r(d, m)$ for each positive integer $r \leqslant \binom{m+d}{d}$. We observe that there is a more general relation.

Lemma 7.2. *Let d, r be any integers with $d \geqslant 1$ and $1 \leqslant r \leqslant \binom{m+d}{d} - r_d$. Then*

$$d_r(\mathrm{PRM}_q(d, m)) = \mathsf{p}_m - \bar{e}_r(d, m). \tag{31}$$

Proof. Clearly, for any r-dimensional subspace D of $\mathrm{PRM}_q(d, m)$, there exist r linearly independent, projectively reduced polynomials $F_1, \ldots, F_r \in \mathbb{F}_q[x_0, \ldots, x_m]_d$ such that D is the $\mathbb{F}_q$-linear span of $\mathrm{ev}(F_1), \ldots, \mathrm{ev}(F_r)$, and moreover,

$$\mathrm{w}_H(D) = \mathsf{p}_m - |\{i\colon F_j(P_i) = 0 \text{ for all } 1 \leqslant j \leqslant r\}| = \mathsf{p}_m - |V(F_1, \ldots, F_r)(\mathbb{F}_q)|.$$

This yields the desired equality. □

Corollary 7.3. *Let d be an integer satisfying $1 \leqslant d \leqslant q$. Then*

$$e_1(d, m) > e_2(d, m) > \cdots > e_{\binom{m+d}{d}}(d, m) = 0.$$

Proof. By Theorem 6.2, if $d \leqslant q$, then $\overline{e}_r(d, m) = e_r(d, m)$ for $1 \leqslant r \leqslant \binom{m+d}{d}$. So the desired inequalities follow from equation (30) and Lemma 7.2. It is obvious from the definition that $e_{\binom{m+d}{d}}(d, m) = 0$, or alternatively, it follows from noting that $\mathrm{PRM}_q(d, m)$ is always a nondegenerate code. □

The following result generalizes Lemma 6.9 as well as [10, Thm. 4.7], and extends the validity of Conjecture 2.4 for some additional values of r.

Theorem 7.4. *Suppose $1 \leqslant d < q$ and $r = \sum_{a=1}^{i} \binom{m+d-a}{d-1} - t$ for some positive integer $i \leqslant m + 1$. and nonnegative integer $t < d$. Then*

$$e_r(d, m) = \mathsf{p}_{m-i} + t \quad \text{and consequently,} \quad d_r(\mathrm{PRM}_q(d, m)) = \mathsf{p}_m - \mathsf{p}_{m-i} - t.$$

Proof. By Lemma 6.9, $e_{r+t}(d, m) = \mathsf{p}_{m-i}$. In particular, the result holds if $t = 0$. Now assume that $1 \leqslant t < d$. As in the proof of Lemma 6.9, we observe that the rth monomial of $\overline{\mathbb{M}}_d$ in descending lexicographical order is given by $x_{i-1}x_{m-1}^t x_m^{d-1-t}$. Hence Theorem 6.8 implies that $e_r(d, m) \leqslant \mathsf{p}_{m-i} + t$, whereas Corollary 7.3 implies that $e_r(d, m) \geqslant t + e_{r+t}(d, m) = t + \mathsf{p}_{m-i}$. This yields the desired results. □

Example 7.5. Suppose $m = 2$ and $d = 4$. Assume that $q > 4$. First, we know from [4, Thm. 5.3] that equation (4) is valid for all $r \leqslant \binom{m+2}{2}$. Thus we know $e_r(d, m)$ for $1 \leqslant r \leqslant 6$. Next, Lemma 6.9 covers the values $r = 10$, 14 and $15 = \binom{2+4}{4}$, since $10 = \binom{5}{3}$, while $14 = \binom{5}{3} + \binom{4}{3}$ and $15 = \binom{5}{3} + \binom{4}{3} + \binom{3}{3}$. The remaining values are taken care of by Theorem 7.4. Consequently, we can write down the complete set of generalized Hamming weights of $\mathrm{PRM}_q(4, 2)$ for $q \geqslant 5$. A similar conclusion holds when $(m, d) = (2, 3)$ and $q \geqslant 4$.

Finally, we remark that since $\overline{e}_r(d, m) = e_r(d, m)$ when $d \leqslant q$, it is clear from (31) that the results and conjectures about $e_r(d, m)$ in Section 6 can be easily reformulated in terms of $d_r(\mathrm{PRM}_q(d, m))$. As a sampling of one such result, we give below a reformulation of Theorem 6.8 in the spirit of that in [12, Thm. 5.10].

Proposition 7.6. *Let r, d be positive integers with $d < q$ and $r \leqslant \binom{m+d}{d}$. Further, let $\mathcal{Q}_d^m := \{(\alpha_0, \ldots, \alpha_m) \in Q^{m+1} \colon \sum_{i=0}^{m} \alpha_i = (m + 1)(q - 1) - d\}$, where as in Section 4.1, $Q := \{0, 1, \ldots, q-1\}$. If $(\beta_0, \ldots, \beta_m)$ is the rth element of $\mathcal{Q}_d^m$ in ascending lexicographic order, then*

$$d_r(\mathrm{PRM}_q(d, m)) \geqslant m + 1 + \sum_{j=0}^{m-1} \beta_j \mathsf{p}_{m-1-j}.$$

Proof. Let $x_0^{a_0} \cdots x_m^{a_m}$ be the smallest monomial in $\mathcal{M}_d(r)$ in lexicographic order. Then Lemma 7.2 and Theorem 6.8 imply that

$$d_r(\mathrm{PRM}_q(d,\,m)) \geqslant \mathsf{p}_m - \sum_{j=0}^{m-1} a_j \mathsf{p}_{m-1-j}$$

$$= m + 1 + \sum_{j=0}^{m-1}(q-1)\mathsf{p}_{m-1-j} - \sum_{j=0}^{m-1} a_j \mathsf{p}_{m-1-j}$$

$$= m + 1 + \sum_{j=0}^{m-1}(q-1-a_j)\mathsf{p}_{m-1-j}.$$

The result now follows by noting that the $(m+1)$-tuple $(q-1-a_0,\,\ldots,\,q-1-a_m)$ is the rth element of $\mathcal{Q}_d^m$ in ascending lexicographic order. $\square$

Remark 7.7. In a recent work, Ramkumar, Vajha, and Vijay Kumar [17] have determined all the generalized Hamming weights of what they call the "binary projective Reed–Muller code". However, the code they consider is not $\mathrm{PRM}_2(d,\,m)$ as defined above (and studied by Lachaud [15], Sørensen [19], and others), but, in fact, a puncturing of a subcode of $\mathrm{PRM}_2(d,\,m)$. Indeed, they consider evaluations at points of $\mathbb{P}^m(\mathbb{F}_2)$ (which, in this case, is just $\mathbb{F}_2^{m+1} \setminus \{(0,\,\ldots,\,0)\}$) of polynomials in $\mathbb{F}_2[x_0,\,\ldots,\,x_m]_d$ that are reduced in the affine sense. The resulting code is degenerate, in general, and so they puncture it suitably so as to obtain a nondegenerate code, say $C_2(d,\,m)$ for $1 \leqslant d \leqslant m$. The length of $\mathrm{PRM}_2(d,\,m)$ is $2^{m+1} - 1$, while that of $C_2(d,\,m)$ is $2^{m+1} - \sum_{i=0}^{d-1}\binom{m}{i}$. Likewise, the dimension of $\mathrm{PRM}_2(d,\,m)$ is $\binom{m+2}{2}$, while that of $C_2(d,\,m)$ is $\binom{m+1}{2}$. Evidently, the generalized Hamming weight $d_r(C_2(d,\,m))$, for which a formula is given in [17], provides an upper bound for $d_r(\mathrm{PRM}_2(d,\,m))$ when $1 \leqslant r \leqslant \binom{m+1}{2}$, but the equality does not hold, in general.

Acknowledgements

References

[1] I. Anderson, *Combinatorics of finite sets*, Dover Publications, Inc., Mineola, NY, 2002. MR 1902962

[2] P. Beelen, *A note on the generalized Hamming weights of Reed–Muller codes*, Appl. Algebra Engrg. Comm. Comput. **30** (2019), no. 3, 233–242. MR 3948262

[3] P. Beelen and M. Datta, *Generalized Hamming weights of affine Cartesian codes*, Finite Fields Appl. **51** (2018), 130–145. MR 3781399

[4] P. Beelen, M. Datta, and S. R. Ghorpade, *Maximum number of common zeros of homogeneous polynomials over finite fields*, Proc. Amer. Math. Soc. **146** (2018), no. 4, 1451–1468. MR 3754333

[5] P. Beelen, M. Datta, and S. R. Ghorpade, *Vanishing ideals of projective spaces over finite fields and a projective footprint bound*, Acta Math. Sin. (Engl. Ser.) **35** (2019), no. 1, 47–63. MR 3917991

[6] M. Boguslavsky, *On the number of solutions of polynomial systems*, Finite Fields Appl. **3** (1997), no. 4, 287–299. MR 1478830

[7] G. F. Clements and B. Lindström, *A generalization of a combinatorial theorem of Macaulay*, J. Combinatorial Theory **7** (1969), 230–238. MR 246781

[8] M. Datta and S. R. Ghorpade, *On a conjecture of Tsfasman and an inequality of Serre for the number of points of hypersurfaces over finite fields*, Mosc. Math. J. **15** (2015), no. 4, 715–725. MR 3438829

[9] M. Datta and S. R. Ghorpade, *Number of solutions of systems of homogeneous polynomial equations over finite fields*, Proc. Amer. Math. Soc. **145** (2017), no. 2, 525–541. MR 3577858

[10] M. Datta and S. R. Ghorpade, *Remarks on the Tsfasman–Boguslavsky Conjecture and higher weights of projective Reed–Muller codes*, Arithmetic, geometry, cryptography and coding theory, Contemp. Math., vol. 686, Amer. Math. Soc., Providence, RI, 2017, pp. 157–169. MR 3630614

[11] S. R. Ghorpade, *A note on Nullstellensatz over finite fields*, Contributions in algebra and algebraic geometry, Contemp. Math., vol. 738, Amer. Math. Soc., Providence, RI, 2019, pp. 23–32. MR 4014962

[12] P. Heijnen and R. Pellikaan, *Generalized Hamming weights of q-ary Reed–Muller codes*, IEEE Trans. Inform. Theory **44** (1998), no. 1, 181–196. MR 1486657

[13] P. W. Heijnen, *Some classes of linear codes*, Ph.D. thesis, Eindhoven University of Technology, Eindhoven, 1999. MR 1707274.

[14] J.-R. Joly, *Équations et variétés algébriques sur un corps fini*, Enseign. Math. (2) **19** (1973), 1–117. MR 327723

[15] G. Lachaud, *Projective Reed–Muller codes*, Coding theory and applications (Cachan, 1986), Lecture Notes in Comput. Sci., vol. 311, Springer, Berlin, 1988, pp. 125–129. MR 960714

[16] D.-J. Mercier and R. Rolland, *Polynômes homogènes qui s'annulent sur l'espace projectif $\mathbb{P}^m(\mathbb{F}_q)$*, J. Pure Appl. Algebra **124** (1998), no. 1-3, 227–240. MR 1600301

[17] V. Ramkumar, M. Vajha, and P. V. Kumar, *Determining the generalized Hamming weight hierarchy of the binary projective Reed–Muller code*, preprint arXiv:1806.02028 [cs.IT].

[18] J.-P. Serre, *Lettre à M. Tsfasman*, Journées Arithmétiques (Luminy, 1989), Astérisque **198–200** (1991), 351–353. MR 1144337

[19] A. B. Sørensen, *Projective Reed–Muller codes*, IEEE Trans. Inform. Theory **37** (1991), no. 6, 1567–1576. MR 1134296

[20] V. K. Wei, *Generalized Hamming weights for linear codes*, IEEE Trans. Inform. Theory **37** (1991), no. 5, 1412–1418. MR 1136673

[21] C. Zanella, *Linear sections of the finite Veronese varieties and authentication systems defined using geometry*, Des. Codes Cryptogr. **13** (1998), no. 2, 199–212. MR 1600208

P. B.: DEPARTMENT OF APPLIED MATHEMATICS AND COMPUTER SCIENCE, TECHNICAL UNIVERSITY OF DENMARK, 2800 KGS. LYNGBY, DENMARK
E-mail address: `pabe@dtu.dk`

M. D.: DEPARTMENT OF MATHEMATICS, INDIAN INSTITUTE OF TECHNOLOGY HYDERABAD, KANDI, SANGAREDDY, TELANAGANA, 502285, INDIA
E-mail address: `mrinmoy.datta@math.iith.ac.in`

S. R. G.: DEPARTMENT OF MATHEMATICS, INDIAN INSTITUTE OF TECHNOLOGY BOMBAY, POWAI, MUMBAI 400076, INDIA
E-mail address: `srg@math.iitb.ac.in`