ON THE MINIMUM DISTANCE, MINIMUM WEIGHT CODEWORDS, AND THE DIMENSION OF PROJECTIVE REED-MULLER CODES

Sudhir R. Ghorpade✉* and Rati Ludhani✉

Department of Mathematics, Indian Institute of Technology Bombay,
Powai, Mumbai 400076, India

Abstract. We give an alternative proof of the formula for the minimum distance of a projective Reed-Muller code of an arbitrary order. It leads to a complete characterization of the minimum weight codewords of a projective Reed-Muller code. This is then used to determine the number of minimum weight codewords of a projective Reed-Muller code. Various formulas for the dimension of a projective Reed-Muller code, and their equivalences are also discussed.

1. **Introduction.** Reed-Muller codes constitute a widely studied and fairly well-understood class of linear codes. These codes were introduced, in the binary case, by Muller [21], and further studied by Reed [22] in 1954. (See [23] for an account of the early history.) Generalizations of Reed-Muller codes to the q-ary case were considered and extensively studied in the following decade by Kasami, Lin, and Peterson [16] and by Delsarte, Goethals, and MacWilliams [10]. As a result of this, and also subsequent work, notably by Berger and Charpin [7] and by Heijnen and Pellikaan [14], we know a great deal about q-ary Reed-Muller codes of an arbitrary order. For instance, the length, dimension, minimum distance, characterization and enumeration of minimum weight codewords, duals, automorphisms, and generalized Hamming weights, are completely known. For convenience of reader and ease of reference, a brief summary of several of the known results is given in §2.1.

Projective Reed-Muller (PRM) codes in the general q-ary case, but of order $d < q$, were introduced by Lachaud [17] in 1986. (See Section 3 of [13] for an account of the history.) The length and dimension as well as bounds for the minimum distance of PRM codes of order $d < q$, and the exact minimum distance in the case $d = 2$ and $q = 2^e$, $e \geq 2$, were obtained by Lachaud [17]. Some of these ideas and results go

---

back to Manin's course of lectures during 1981-82 at Moscow State University, and are sketched in Chapter I, Section 3, Example 2 b) of [28]. Tsfasman conjectured a sharp bound for the number of $\mathbb{F}_q$-rational points of a projective hypersurface of a given degree $d \leq q$. This bound was proved in the affirmative by Serre [26], and it was then shown by Lachaud [18] how the minimum distance of PRM codes of order $d \leq q$ can be obtained as a consequence of Serre's inequality. Independently, Sørensen [27] gave explicit formulas for the length, dimension, and the minimum distance of PRM codes not just of order $d \leq q$, but of an arbitrary order. Further, he determined the duals of PRM codes as well. Sørensen's work has had a considerable impact as is indicated by the number of citations to [27]. Moreover, PRM codes continue to be of considerable current interest, and while the automorphism group is known (cf. [6]), the question about the determination of their generalized Hamming weights is still open in general even though there has been significant progress lately (see, e.g., [5] and references therein for the current state of the art).

Recently, while revisiting Sørensen's proof for the minimum distance of PRM codes of an arbitrary order, we noticed that there was a gap in the argument. While we realized later that the gap can be fixed and the result is correct as stated, we were able to obtain an alternative proof of Sørensen's result by suitably adapting the arguments of Serre [26]. An additional dividend of this alternative proof is that it leads to a characterization of the minimum weight codewords of a projective Reed-Muller code. Since such a characterization is not given in Sørensen's paper [27] and it did not seem to be readily available in the literature, we initially thought that it was new. However, we later found that Rolland [25, Lemma 2.3] has already given a characterization of the minimum weight codewords of a PRM code using different methods; see also Ballet and Rolland [2, Theorem 8] for a detailed proof of Rolland's result. Nonetheless, we believe that the alternative proof given here and the resulting characterization is of some interest. Another noteworthy feature of our proof is the use of the notion of projective reduction that was developed and systematically used in [4], and this seems quite natural in the context of PRM codes. We also give an explicit formula for the number of minimum weight codewords of a PRM code of an arbitrary order. As far as we know, this appears to be new and somewhat nontrivial, even after knowing a characterization of the minimum weight codewords. Finally, we review various formulas for the dimension of a PRM code of an arbitrary order and make some remarks on their equivalence. We also include a direct proof of one of the dimension formulas using the notion of projective reduction. An appendix reproduces a hitherto unpublished proof of M. Quercia about the equivalence of two classical formulas for the dimension of a PRM code.

2. **Basics of Reed-Muller and projective Reed-Muller codes.** Fix, throughout this paper, a prime power q and a positive integer m. As usual, $\mathbb{Z}$ denotes the set of integers and $\mathbb{F}_q$ the finite field with q elements. Given any $b \in \mathbb{Z}$ and a in an integral domain R containing $\mathbb{Z}$ as a subring, the corresponding binomial coefficient is defined by

$$\binom{a}{b} := \begin{cases} \dfrac{a(a-1)\cdots(a-b+1)}{b!} & \text{if } b \geq 0, \\ 0 & \text{if } b < 0. \end{cases}$$

This is, in general, an element of the quotient field of R. In case $\mathsf{R} = \mathbb{Z}$, it is in $\mathbb{Z}$.

2.1. **Reed-Muller codes.** Let $\nu \in \mathbb{Z}$ with $\nu \geq 0$, and let $\mathbb{F}_q[X_1, \ldots, X_m]_{\leq \nu}$ denote the space of all polynomials in m variables with coefficients in $\mathbb{F}_q$ of (total) degree $\leq \nu$. Write $\mathbb{F}_q^m = \{P_1, \ldots, P_{q^m}\}$. Consider the evaluation map

$$\mathrm{ev} : \mathbb{F}_q[X_1, \ldots, X_m]_{\leq \nu} \to \mathbb{F}_q^{q^m} \quad \text{defined by} \quad f \mapsto c_f := (f(P_1), \ldots, f(P_{q^m})).$$

Clearly ev is a linear map and its image is a nondegenerate linear code of length q^m; this code is called the *(generalized) Reed-Muller code* of order ν, and it is denoted by $\mathrm{RM}_q(\nu, m)$.

It is easy to see that if $\nu < q$, then the map ev is injective and so dim $\mathrm{RM}_q(\nu, m) = \binom{m+\nu}{\nu}$; see, e.g., [11, Lemma 2.1]. Also, if $\nu < q$, then it follows from Ore's inequality (see, e.g., [11, Corollary 2.7]) that the minimum distance of $\mathrm{RM}_q(\nu, m)$ is $(q - \nu)q^{m-1}$. On the other hand, if $\nu \geq m(q-1)$, then it is not difficult to see (using, for instance, a slight modification of the argument in [12, Remark 2]) that the map ev is surjective and so $\mathrm{RM}_q(\nu, m) = \mathbb{F}_q^{q^m}$. With this in view, we shall assume that $0 \leq \nu \leq m(q-1)$. In this general case, the restriction of ev to the space of all *reduced*[1] polynomials in $\mathbb{F}_q[X_1, \ldots, X_m]_{\leq \nu}$ is injective (see, e.g., [11, Lemma 2.1]); consequently, the dimension, say $\rho_q(\nu, m)$, of $\mathrm{RM}_q(\nu, m)$ is given by the number of reduced monomials in m variables of degree ν, and it is explicitly given by either of the following formulas.

$$\sum_{s=0}^{\nu} \sum_{i=0}^{m} (-1)^i \binom{m}{i} \binom{s - iq + m - 1}{s - iq} = \sum_{i=0}^{m} (-1)^i \binom{m}{i} \binom{m + \nu - iq}{m}. \quad (1)$$

One may refer to [1, Theorem 5.4.1] for a proof of the first formula, and to [24, Proposition 5] or [12, Lemma 1] for a direct proof of the second formula.

Kasami-Lin-Peterson [16] showed that if $\nu \in \mathbb{Z}$ with $0 \leq \nu \leq m(q-1)$ is written as $\nu = t(q-1) + s$ for unique $t, s \in \mathbb{Z}$ such that $t \geq 0$ and $0 \leq s < q-1$, then the minimum distance of $\mathrm{RM}_q(\nu, m)$ is $(q - s)q^{m-t-1}$. Furthermore, with t, s as above, Delsarte-Goethals-MacWilliams [10] showed that $c \in \mathrm{RM}_q(\nu, m)$ is a minimum weight codeword if and only if $c = \mathrm{ev}(f)$, where

$$f = \omega_0 \left(\prod_{i=1}^{t} (1 - \ell_i^{q-1}) \right) \prod_{j=1}^{s} (\ell_{t+1} - \omega_j) \quad (2)$$

for some linearly independent polynomials $\ell_1, \ldots, \ell_{t+1} \in \mathbb{F}_q[X_1, \ldots, X_m]$ of degree 1, and some $\omega_0, \omega_1, \ldots, \omega_s \in \mathbb{F}_q$ with $\omega_0 \neq 0$ and $\omega_1, \ldots, \omega_s$ distinct. For an alternative proof of this characterization, see [19]. Here it should be understood that when $s = 0$, the second product in (2) is empty (and hence equal to 1) and in this case only the existence and linear independence of t polynomials $\ell_1, \ldots, \ell_t \in \mathbb{F}_q[X_1, \ldots, X_m]$ of degree 1 is asserted in the characterization. Delsarte-Goethals-MacWilliams [10] further observed that the number of minimum weight codewords of $\mathrm{RM}_q(\nu, m)$ is given by

$$(q-1)q^t \begin{bmatrix} m \\ t \end{bmatrix}_q M_s, \quad \text{where} \quad M_s := \begin{cases} \binom{q}{s} \begin{bmatrix} m - t \\ 1 \end{bmatrix}_q & \text{if } s > 0, \\ 1 & \text{if } s = 0. \end{cases} \quad (3)$$

---

[1] A polynomial $f \in \mathbb{F}_q[X_1, \ldots, X_m]$ is said to be *reduced* if $\deg_{X_i} f \leq q-1$ for each $i = 1, \ldots, m$.

Here, and hereafter, for any $a, b \in \mathbb{Z}$, we denote, as usual, by $\begin{bmatrix} a \\ b \end{bmatrix}_q$ the Gaussian binomial coefficient given by

$$\begin{bmatrix} a \\ b \end{bmatrix}_q := \begin{cases} \dfrac{(q^a - 1)(q^a - q) \cdots (q^a - q^{b-1})}{(q^b - 1)(q^b - q) \cdots (q^b - q^{b-1})} & \text{if } 0 \le b \le a, \\ 0 & \text{otherwise.} \end{cases}$$

Delsarte-Goethals-MacWilliams [10] also showed that the dual of $\mathrm{RM}_q(\nu, m)$ is given by $\mathrm{RM}_q(m(q-1) - \nu - 1, m)$, where by convention, $\mathrm{RM}_q(-1, m)$ is the trivial code $\{\mathbf{0}\}$. As indicated in the Introduction, the automorphism group as well as the generalized Hamming weights of $\mathrm{RM}_q(\nu, m)$ are known, and for these, we refer to the papers of Berger and Charpin [7] and of Heijnen and Pellikaan [14] as well as Beelen and Datta [3].

2.2. **Projective Reed-Muller codes.** Fix, in the remainder of this paper, a positive integer d. Given any $k \in \mathbb{Z}$, let

$$p_k := \begin{cases} 1 + q + q^2 + \cdots + q^k & \text{if } k \ge 0, \\ 0 & \text{if } k < 0. \end{cases}$$

Each point of the m-dimensional projective space $\mathbb{P}^m(\mathbb{F}_q)$ over $\mathbb{F}_q$ admits a unique representative in $\mathbb{F}_q^{m+1}$ in which the last nonzero coordinate is 1. Let $\mathsf{P}_1, \ldots, \mathsf{P}_{p_m}$ be an ordered listing of such representatives in $\mathbb{F}_q^{m+1}$ of points of $\mathbb{P}^m(\mathbb{F}_q)$. Let $\mathbb{F}_q[X_0, \ldots, X_m]_d$ denote the space of homogeneous polynomials in $\mathbb{F}_q[X_0, \ldots, X_m]$ of degree d together with the zero polynomial. Consider the evaluation map

$$\mathrm{Ev} : \mathbb{F}_q[X_0, \ldots, X_m]_d \to \mathbb{F}_q^{p_m} \quad \text{defined by} \quad F \mapsto c_F := (F(\mathsf{P}_1), \ldots, F(\mathsf{P}_{p_m})). \tag{4}$$

Note that Ev is a linear map and its image is a nondegenerate linear code of length p_m. This code is said to be the *projective Reed-Muller code* of order d and length p_m, and it is denoted by $\mathsf{PRM}_q(d, m)$.

A convenient way to study the projective Reed-Muller code is to use the notion of projective reduction, which was introduced in [4] and employed in [11] to determine the vanishing ideal of $\mathbb{P}^m(\mathbb{F}_q)$. Let us recall that the projective reduction $\overline{\mu}$ of a monomial $\mu \in \mathbb{F}_q[X_0, \ldots, X_m]$ of positive degree is defined as follows. Write $\mu = X_0^{a_0} \cdots X_\ell^{a_\ell}$ for unique nonnegative integers $a_0, \ldots, a_\ell$ with $a_\ell > 0$ so that X_ℓ is the last variable in μ. For $0 \le i \le \ell - 1$, let $\overline{a}_i = a_i$ if $0 \le a_i \le q - 1$, whereas if $a_i \ge q$, then let $\overline{a}_i$ be the unique integer such that $\overline{a}_i \equiv a_i \pmod{q - 1}$ and $1 \le \overline{a}_i \le q - 1$. We then define

$$\overline{\mu} := X_0^{\overline{a}_0} \cdots X_{\ell-1}^{\overline{a}_{\ell-1}} X_\ell^{a_\ell + \sum_{i=0}^{\ell-1}(a_i - \overline{a}_i)}.$$

The monomial $\overline{\mu}$ is uniquely determined by μ and it has the same degree as μ. In case $\mu = 1$, we set $\overline{\mu} := 1$. Observe that $\overline{\mu}(\mathsf{P}) = \mu(\mathsf{P})$ for all $\mathsf{P} \in \mathbb{F}_q^{m+1}$. We say that a monomial μ is *projectively reduced* if $\overline{\mu} = \mu$. These notions extend by $\mathbb{F}_q$-linearity to arbitrary polynomials in $\mathbb{F}_q[X_0, \ldots, X_m]$. Now let

$$C_q(d, m) := \{ f \in \mathbb{F}_q[X_0, \ldots, X_m]_d : f \text{ is projectively reduced} \}.$$

Note that $C_q(d, m)$ is a $\mathbb{F}_q$-linear subspace of the polynomial ring $\mathbb{F}_q[X_0, \ldots, X_m]$.

Lemma 2.1. *The restriction* $\mathrm{Ev}|_{C_q(d,m)}$ *of the evaluation map defined in* (4)*, to* $C_q(d, m)$*, is injective. Moreover,* $\mathsf{PRM}_q(d, m) = \mathrm{Ev}(C_q(d, m))$.

Proof. The first assertion follows from Lemma 3.1 of [11], and the second assertion follows from Lemma 3.2 and Theorem 3.3 of [11]. $\qquad \square$

Corollary 2.2. *If F is a nonzero polynomial in $C_q(d,m)$, then $|V(F)| \leq p_m - 1$.*

Proof. This is an immediate consequence of Lemma 2.1. □

Lemma 2.3. *If $d \geq m(q-1)+1$, then $\mathsf{PRM}_q(d,m) = \mathsf{PRM}_q(m(q-1)+1,m) = \mathbb{F}_q^{p_m}$.*

Proof. Let $\nu \in \{1,\ldots,p_m\}$. Write $\mathsf{P}_\nu \in \mathbb{F}_q^{m+1}$ as $\mathsf{P}_\nu = (a_0,\ldots,a_{j_\nu-1},1,0,\ldots,0)$ for unique $j_\nu \in \{0,1,\ldots,m\}$ and $a_0,\ldots,a_{j_\nu-1} \in \mathbb{F}_q$. Now assume that $d \geq m(q-1)+1$. Define the polynomial $F_\nu = F_\nu(X_0,\ldots,X_m)$ by

$$F_\nu := X_{j_\nu}^{d-m(q-1)} \prod_{i=0}^{j_\nu-1} \left(X_{j_\nu}^{q-1} - (X_i - a_i X_{j_\nu})^{q-1} \right) \prod_{k=j_\nu+1}^{m} (X_{j_\nu}^{q-1} - X_k^{q-1}). \qquad (5)$$

Clearly, $F_\nu \in \mathbb{F}_q[X_0,\ldots,X_m]_d$. Observe that $F_\nu(\mathsf{P}_\nu) = 1$ and $F_\nu(\mathsf{P}_\mu) = 0$ for any $\mu \in \{1,\ldots,p_m\}$ with $\mu \neq \nu$. Hence any $\lambda = (\lambda_1,\ldots,\lambda_{p_m}) \in \mathbb{F}_q^{p_m}$ can be written as $\lambda = \mathrm{Ev}(F)$, where $F = \lambda_1 F_1 + \cdots + \lambda_{p_m} F_{p_m}$. It follows that $\mathsf{PRM}_q(d,m) = \mathbb{F}_q^{p_m}$. □

We remark that the polynomial (5) was used by Sørensen in [27, Lemma 3].

3. Minimum distance of projective Reed-Muller codes.

In view of the results of the previous section, every codeword of $\mathsf{PRM}_q(d,m)$ is of the form $\mathrm{Ev}(F)$ for a unique $F \in C_q(d,m)$, and determining the Hamming weight of this codeword corresponds to finding the number of zeros in $\mathbb{P}^m(\mathbb{F}_q)$ of F.

For any $f_1,\ldots,f_r \in \mathbb{F}_q[X_1,\ldots,X_m]_{\leq d}$, we denote by $Z(f_1,\ldots,f_r)$ the set of common zeros of $f_1,\ldots,f_r$ in $\mathbb{A}^m(\mathbb{F}_q)$, whereas for $F_1,\ldots,F_r \in \mathbb{F}_q[X_0,\ldots,X_m]_d$, we denote by $V(F_1,\ldots,F_r)$ the set of common zeros of $F_1,\ldots,F_r$ in $\mathbb{P}^m(\mathbb{F}_q)$. By a *hyperplane* in $\mathbb{P}^m(\mathbb{F}_q)$ we shall mean a subset of the form $V(L)$, where L is a nonzero homogeneous linear polynomial in $\mathbb{F}_q[X_0,\ldots,X_m]$. We shall denote by $\widehat{\mathbb{P}^m}$ the set of all hyperplanes in $\mathbb{P}^m(\mathbb{F}_q)$. Note that the cardinality of $\widehat{\mathbb{P}^m}$ is p_m. Also note that if P, P' are distinct points of $\mathbb{P}^m(\mathbb{F}_q)$, then $|\{H \in \widehat{\mathbb{P}^m} : P \in H\}| = p_{m-1}$ and $|\{H \in \widehat{\mathbb{P}^m} : P, P' \in H\}| = p_{m-2}$.

Lemma 3.1. *Let F be a nonzero projectively reduced polynomial in $\mathbb{F}_q[X_0,\ldots,X_m]_d$. Suppose L is a nonzero homogeneous linear polynomial in $\mathbb{F}_q[X_0,\ldots,X_m]$ such that the hyperplane $V(L)$ is contained in $V(F)$. Then L divides F.*

Proof. By a linear change of coordinates, we may assume that $L = X_m$. Separating the monomials in F that are divisible by X_m, we can write $F = X_m G + R$ for some homogeneous and projectively reduced polynomials $G \in \mathbb{F}_q[X_0,\ldots,X_m]_{d-1}$ and $R \in \mathbb{F}_q[X_0,\ldots,X_{m-1}]_d$. Since $V(X_m) \subseteq V(F)$, we see that $R(\mathsf{P}) = 0$ for all $\mathsf{P} \in \mathbb{P}^{m-1}(\mathbb{F}_q)$. But R is projectively reduced, and so it follows from Lemma 2.1 that R is the zero polynomial. Thus, X_m divides F. □

Theorem 3.2. *Let F be a nonzero polynomial in $C_q(d,m)$. Then*

$$|V(F)| \leq p_m - \lceil (q-s)q^{m-t-1} \rceil, \qquad (6)$$

where t,s are unique integers such that $d - 1 = t(q-1) + s$ with $t \geq 0$ and $0 \leq s < q-1$. Moreover, if $1 \leq d \leq m(q-1)$ and if the equality holds in (6), then $V(F)$ is a union of at most d distinct hyperplanes in $\mathbb{P}^m(\mathbb{F}_q)$.

Proof. In case $d \geq m(q-1)+1$, or equivalently, $t > m-1$, then $\lceil (q-s)q^{m-t-1} \rceil = 1$, and so (6) is a consequence of Corollary 2.2.

Now assume that $1 \le d \le m(q-1)$. Then $t \le m-1$ and therefore

$$p_m - \lceil (q-s)q^{m-t-1} \rceil \ge p_m - q^m > 0.$$

In particular, (6) holds trivially if $V(F)$ is empty. Thus we shall assume that $V(F)$ is nonempty.

We will use induction on m. First, suppose $m = 1$. Then, $d \le q-1$, and hence $t = 0$. Consequently, $p_m - \lceil (q-s)q^{m-t-1} \rceil = p_1 - (q-s)q^{1-0-1} = s+1 = d$. Thus (6) is a consequence of the elementary fact that a nonzero homogeneous polynomial of degree d in two variables over a field F has at most d non-proportional zeros in $F^2 \setminus \{(0,0)\}$. Moreover since hyperplanes in $\mathbb{P}^1(\mathbb{F}_q)$ are given by points, we also see that if $m = 1$ and if the equality holds in (6), then $V(F)$ is a union of exactly d distinct hyperplanes in $\mathbb{P}^m(\mathbb{F}_q)$.

Next, suppose $m > 1$ and the result holds for smaller values of m. Define

$$\Gamma := \{ H \in \widehat{\mathbb{P}^m} : H \subseteq V(F) \}.$$

In view of Lemma 3.1, we see that Γ can contain at most d distinct hyperplanes in $\mathbb{P}^m(\mathbb{F}_q)$. Write

$$\Gamma = \{H_1, \ldots, H_\ell\} \quad \text{and} \quad \mathcal{L} = \bigcup_{i=1}^{\ell} H_i$$

for some nonnegative integer $\ell \le d$. We shall now divide the proof in two mutually exclusive and exhaustive cases.

Case 1. $\mathcal{L} = V(F)$.

In this case, we must have $\ell \ge 1$ since $V(F)$ is nonempty. By a linear change of coordinates, we may assume that $H_1 = V(X_m)$. In view of Lemma 3.1, we see that $F(X_0, \ldots, X_{m-1}, 0) = 0$ and $f(X_0, \ldots, X_{m-1}) := F(X_0, \ldots, X_{m-1}, 1)$ is a nonzero reduced polynomial in $\mathbb{F}_q[X_0, \ldots, X_{m-1}]_{\le d-1}$. Thus

$$
\begin{aligned}
|V(F)| &= |V(F(X_0, \ldots, X_{m-1}, 0))| + |Z(f)| \\
&\le p_{m-1} + q^m - \lceil (q-s)q^{m-t-1} \rceil \\
&= p_m - \lceil (q-s)q^{m-t-1} \rceil,
\end{aligned}
\tag{7}
$$

where the second step uses the formula (recalled in § 2.1) for the minimum distance of Reed-Muller code $\mathrm{RM}_q(d-1, m)$ and the fact that $\mathrm{ev}(f)$ is a nonzero codeword of this code since f is nonzero reduced polynomial. Thus (6) is proved in Case 1.

Case 2. $\mathcal{L} \ne V(F)$.

In this case, there exists some $P \in V(F) \setminus \mathcal{L}$. In particular, a hyperplane in $\mathbb{P}^m(\mathbb{F}_q)$ passing through P can not be contained in $V(F)$. For sections of $V(F)$ by such hyperplanes, we make the following

Claim: If H is any hyperplane in $\mathbb{P}^m(\mathbb{F}_q)$ such that $H \not\subseteq V(F)$, then

$$|V(F) \cap H| \le p_{m-1} - \lceil (q-s)q^{m-t-2} \rceil.$$

To prove this, fix a hyperplane H in $\mathbb{P}^m(\mathbb{F}_q)$ such that $H \not\subseteq V(F)$. By a linear change of coordinates, we may assume that $H = V(X_m)$. As in the proof of Lemma 3.1, we can write $F = X_m G + R$ for some homogeneous and projectively reduced polynomials $G \in \mathbb{F}_q[X_0, \ldots, X_m]_{d-1}$ and $R \in \mathbb{F}_q[X_0, \ldots, X_{m-1}]_d$. Since $V(X_m) \not\subseteq V(F)$, we see that R is a nonzero polynomial in $C_q(d, m-1)$. Also, $V(F) \cap H = V(R) \cap H$ is the zero set of R in $\mathbb{P}^{m-1}(\mathbb{F}_q)$. Hence by the induction

hypothesis, $|V(F) \cap H| \leq p_{m-1} - \lceil (q-s)q^{m-t-2} \rceil$. This proves the chaim.

Recall that we had chosen $P \in V(F) \setminus \mathcal{L}$. Following Serre [26], we consider the incidence set

$$\mathcal{I} := \{(P', H) : P' \in V(F) \setminus \{P\} \text{ and } H \in \widehat{\mathbb{P}^m} \text{ with } P, P' \in H\}.$$

This set can be counted in two different ways as follows. On the one hand,

$$|\mathcal{I}| = \sum_{\substack{P' \in V(F) \setminus \{P\}}} \sum_{\substack{H \in \widehat{\mathbb{P}^m} \\ P,P' \in H}} 1 = \sum_{\substack{P' \in V(F) \setminus \{P\}}} p_{m-2} = p_{m-2}(|V(F)| - 1).$$

On the other hand,

$$\begin{aligned} |\mathcal{I}| &= \sum_{\substack{H \in \widehat{\mathbb{P}^m} \\ P \in H}} \sum_{\substack{P' \in V(F) \setminus \{P\} \\ P' \in H}} 1 \\ &= \sum_{\substack{H \in \widehat{\mathbb{P}^m} \\ P \in H}} (|V(F) \cap H| - 1) \\ &\leq \sum_{\substack{H \in \widehat{\mathbb{P}^m} \\ P \in H}} \left(p_{m-1} - \lceil (q-s)q^{m-t-2} \rceil - 1 \right) \\ &= p_{m-1} \left(p_{m-1} - \lceil (q-s)q^{m-t-2} \rceil - 1 \right) \end{aligned}$$

where the inequality in Step 3 follows from the claim above. On comparing both these values of $|\mathcal{I}|$, we obtain

$$\begin{aligned} |V(F)| &\leq \frac{p_{m-1}(p_{m-1} - \lceil (q-s)q^{m-t-2} \rceil - 1)}{p_{m-2}} + 1 \\ &= \frac{(p_{m-1})^2 - p_{m-1} + p_{m-2}}{p_{m-2}} - \frac{p_{m-1} \lceil (q-s)q^{m-t-2} \rceil}{p_{m-2}} \\ &= \frac{(p_{m-1})^2 - q^{m-1}}{p_{m-2}} - \frac{p_{m-1}}{p_{m-2}} \lceil (q-s)q^{m-t-2} \rceil \\ &= \frac{(q^m - 1)^2 - q^{m-1}(q-1)^2}{(q^{m-1} - 1)(q-1)} - \left(\frac{q^m - 1}{q^{m-1} - 1} \right) \lceil (q-s)q^{m-t-2} \rceil \\ &= \frac{q^{m+1} - 1}{q - 1} - \left(\frac{q^m - 1}{q^{m-1} - 1} \right) \lceil (q-s)q^{m-t-2} \rceil \\ &< p_m - q \lceil (q-s)q^{m-t-2} \rceil, \end{aligned}$$

where the last inequality follows since $q^m - 1 > q^m - q$. Thus,

$$|V(F)| < \begin{cases} p_m - (q-s)q^{m-t-1} & \text{if } t < m-1, \\ p_m - q & \text{if } t = m-1 \end{cases}$$

$$\leq \begin{cases} p_m - (q-s)q^{m-t-1} & \text{if } t < m-1, \\ p_m - (q-s) & \text{if } t = m-1 \end{cases}$$

$$= p_m - \lceil (q-s)q^{m-t-1} \rceil.$$

This yields (6). Moreover, since the inequality in (6) is strict in Case 2, the second assertion is proved as well. □

Corollary 3.3. *Assume that $1 \le d \le m(q-1) + 1$. Then the minimum distance of projective Reed-Muller code $\mathsf{PRM}_q(d, m)$ is*

$$(q - s)q^{m-t-1},$$

where t, s are unique integers such that $d - 1 = t(q - 1) + s$ with $t \ge 0$ and $0 \le s < q - 1$. Moreover, if $\omega_1, \ldots, \omega_s$ are any distinct elements of $\mathbb{F}_q$ and if

$$G := X_t \prod_{i=0}^{t-1} (X_i^{q-1} - X_t^{q-1}) \prod_{j=1}^{s} (X_{t+1} - \omega_j X_t), \tag{8}$$

then $c_G = \mathrm{Ev}(G)$ is a minimum weight codeword of $\mathsf{PRM}_q(d, m)$.

Proof. Since $d \le m(q - 1) + 1$, we see that $t \le m$ and moreover, if $t = m$, then $s = 0$. Thus, $\lceil (q - s)q^{m-t-1} \rceil = (q - s)q^{m-t-1}$. Hence Theorem 3.2 shows that

$$d(\mathsf{PRM}_q(d, m)) \ge (q - s)q^{m-t-1}. \tag{9}$$

Next, suppose $\lambda_1, \ldots, \lambda_s$ are distinct elements of $\mathbb{F}_q$ and G is the polynomial given by (8). Clearly, $G \in \mathbb{F}_q[X_0, \ldots, X_m]_d$ and G has zeros at all points of $\mathbb{P}^m(\mathbb{F}_q)$ except those of the form $(0 : \cdots : 0 : 1 : a_{t+1} : a_{t+2} : \cdots : a_m)$, where $a_{t+1} \ne \omega_j$ for $j = 1, \ldots, s$ and $a_r \in \mathbb{F}_q$ for $r = t+2, \ldots, m$. Thus $|V(G)| = p_m - (q - s)q^{m-t-1}$. This, together with (9) shows that the minimum distance of $\mathsf{PRM}_q(d, m)$ is $(q - s)q^{m-t-1}$ and moreover, $c_G = \mathrm{Ev}(G)$ is a minimum weight codeword of $\mathsf{PRM}_q(d, m)$. □

Remark 3.4. The proof of minimum distance given by Sørensen [27, Theorem 1] has a mistake in the case $t = m-1$, i.e., when $d-1 = (m-1)(q-1)+s$, $0 \le s < q-1$. According to the argument in [27, p. 1569], if $\mathbb{P}^m(\mathbb{F}_q) \setminus V(F) = \{P_1, \ldots, P_e\}$, then we can find linear homogeneous polynomials $G_i(X), i = 1, \ldots, e - 1$ such that $G_i(P_j) = \delta_{ij}$ for $i = 1, \ldots, e - 1$, $j = 1, \ldots, e$.[2] However, this does not seem correct, since it is possible that some P_j is a linear combination of the other points P_i. Also, $H(X) = F(X) \prod_{i=1}^{e-1} G_i(X)$ does not imply that $V(H) = \mathbb{P}^m(\mathbb{F}_q) \setminus \{P_e\}$. To correct this, we may use a weaker condition. Namely, for each positive integer $i \le e - 1$, take $G_i(X)$ to be a linear homogeneous polynomial such that $V(G_i)$ is a hyperplane which passes through P_i but not through P_e. This is possible since P_i, P_e are distinct points of $\mathbb{P}^m(\mathbb{F}_q)$. [See, for example, Lemma 4.1 below.] Then $H(X) := F(X) \prod_{i=1}^{e-1} G_i(X)$ does have the property that $V(H) = \mathbb{P}^m(\mathbb{F}_q) \setminus \{P_e\}$.

Remark 3.5. An alternative proof of the formula for the minimum distance of $\mathsf{PRM}_q(d, m)$ is given by Carvalho, Neumann, and Lopez [9, Corollary 3.9 (c)], where they derive it from a more general result on projective nested cartesian codes.

4. **Minimum weight codewords of projective Reed-Muller codes.** In this section, we characterize the minimum weight codewords of projective Reed-Muller codes in terms of homogeneous polynomials whose images under the evaluation map (4) are these codewords. We begin with a simple observation.

---

[2]If one is writing equalities such as $G_1(P_1) = 1$, then one should take $P_1, \ldots, P_e$ to be certain fixed representatives in $\mathbb{F}_q^{m+1}$ of points of $\mathbb{P}^m(\mathbb{F}_q) \setminus V(F)$, but this is tacitly understood in [27] and stated explicitly in Section II of [27]. Also, unlike in [27], we have denoted $|\mathbb{P}^m(\mathbb{F}_q) \setminus V(F)|$ by e (rather than t) so as to avoid a conflict with the notation used in this paper.

Lemma 4.1. *Given any $A, B \in \mathbb{P}^m(\mathbb{F}_q)$ with $A \neq B$, there is a homogeneous linear polynomial $L \in \mathbb{F}_q[X_0, \ldots, X_m]$ such that $L(A) = 0$ and $L(B) \neq 0$.*

Proof. Let $A = (a_0 : a_1 : \cdots : a_m)$ and $B = (b_0 : b_1 : \cdots : b_m)$ be distinct elements of $\mathbb{P}^m(\mathbb{F}_q)$. Since $A \neq B$, there are integers i, j with $0 \leq i < j \leq m$ such that $a_i b_j - a_j b_i \neq 0$. Now $L = a_i X_j - a_j X_i$ has the desired properties. $\square$

Let us recall that the codewords of $\mathsf{PRM}_q(d, m)$ are of the form c_F, defined as in (4), where F varies over the elements of $\mathbb{F}_q[X_0, \ldots, X_m]_d$. The *support* of such a codeword is given by the set

$$\mathrm{Supp}\,(c_F) = \left\{ \mathsf{P} \in \{\mathsf{P}_1, , \ldots, \mathsf{P}_{p_m}\} : F(\mathsf{P}) \neq 0 \right\},$$

where $\mathsf{P}_1, \ldots, \mathsf{P}_{p_m}$ are as in §2.2. For any $F \in \mathbb{F}_q[X_0, \ldots, X_m]_d$, we can clearly identify $\mathrm{Supp}\,(c_F)$ with $\mathbb{P}^m(\mathbb{F}_q) \setminus V(F)$. In case c_F is a minimum weight codeword, i.e., a nonzero codeword of least Hamming weight, we can say a little more.

Lemma 4.2. *Let $F \in \mathbb{F}_q[X_0, \ldots, X_m]_d$ be such that c_F is a minimum weight codeword of $\mathsf{PRM}_q(d, m)$. Then for any $G \in \mathbb{F}_q[X_0, \ldots, X_m]_d$,*

$$V(F) = V(G) \Longleftrightarrow \mathrm{Supp}\,(c_F) = \mathrm{Supp}\,(c_G) \Longleftrightarrow c_F = c_{\lambda G} \text{ for some nonzero } \lambda \in \mathbb{F}_q.$$

Proof. The first equivalence as well as the reverse implication in the second equivalence is obvious. Suppose $\mathrm{Supp}\,(c_F) = \mathrm{Supp}\,(c_G)$. Pick any $\mathsf{P}_\nu \in \mathrm{Supp}\,(c_F)$. Then $F(\mathsf{P}_\nu) \neq 0 \neq G(\mathsf{P}_\nu)$, and so there is $\lambda \in \mathbb{F}_q$ with $\lambda \neq 0$ such that $F(\mathsf{P}_\nu) = \lambda\, G(\mathsf{P}_\nu)$. Consequently, $\mathrm{Supp}(c_{F - \lambda G}) \subseteq \mathrm{Supp}(c_F) \setminus \{\mathsf{P}_\nu\}$. Since c_F is a minimum weight codeword, it follows that $c_{F - \lambda G} = 0$, that is, $c_F = c_{\lambda G}$. $\square$

We are now ready to prove the main result of this section.

Theorem 4.3. *Assume that $1 \leq d \leq m(q-1)+1$ and let t, s be unique integers such that $d - 1 = t(q - 1) + s$ with $t \geq 0$ and $0 \leq s < q - 1$. Then $c \in \mathbb{F}_q^{p_m}$ is a minimum weight codeword of $\mathsf{PRM}_q(d, m)$ if and only if $c = c_Q$ for some $Q \in \mathbb{F}_q[X_0, \ldots, X_m]_d$ of the form*

$$Q = L_t \prod_{i=0}^{t-1} \left(L_t^{q-1} - L_i^{q-1} \right) \prod_{j=1}^{s} (L_{t+1} - \omega_j L_t) \tag{10}$$

where $L_0, \ldots, L_t, L_{t+1}$ are linearly independent homogeneous linear polynomials in $\mathbb{F}_q[X_0, \ldots, X_m]$ and $\omega_1, \ldots, \omega_s$ are distinct elements of $\mathbb{F}_q$. [Here it is understood that if $s = 0$, then the second product in (10) is empty (and hence equal to 1) and in this case only the existence and linear independence of $L_0, \ldots, L_t$ is asserted.]

Proof. If Q is as in (10), then it is clear that $Q \in \mathbb{F}_q[X_0, \ldots, X_m]_d$ and moreover, by a linear change of coordinates, we see that $|V(Q)| = |V(G)|$, where G is as in (8). Thus Corollary 3.3 implies that c_Q is a minimum weight codeword of $\mathsf{PRM}_q(d, m)$.

To prove the converse, let $F \in \mathbb{F}_q[X_0, \ldots, X_m]_d$ be a nonzero polynomial such that $|V(F)| = p_m - (q - s)q^{m-t-1}$. We need to show that there exists some $Q \in \mathbb{F}_q[X_0, \ldots, X_m]_d$ of the form (10) such that $c_F = c_Q$. To this end, let us first consider the extreme case when $d = m(q - 1) + 1$ so that $t = m$ and $s = 0$. In this case $|V(F)| = p_m - 1$ and so there is unique $\nu \in \{1, \ldots, p_m\}$ such that $F(\mathsf{P}_\nu) \neq 0$ and $F(\mathsf{P}_\mu) = 0$ for all $\mu \in \{1, \ldots, p_m\}$ with $\mu \neq \nu$. Thus if F_ν is as in (5), then by Lemma 4.2, $c_F = c_{\omega_0 F_\nu}$ for some $\omega_0 \in \mathbb{F}_q$ with $\omega_0 \neq 0$. Now, if as in

the proof of Lemma 2.1, we write $\mathsf{P}_\nu = (a_0, \ldots, a_{j_\nu - 1}, 1, 0, \ldots, 0)$, and we let

$$L_t = L_m = \omega_0 X_{j_\nu} \quad \text{and} \quad L_i = \begin{cases} (X_i - a_i X_{j_\nu}) & \text{if } 0 \le i < j_\nu, \\ X_{i+1} & \text{if } j_\nu \le i \le m-1, \end{cases}$$

then $L_0, \ldots, L_t$ are linearly independent and it is clear from (5) that F is as in (10).

Thus, we will now assume that $1 \le d \le m(q-1)$. Then $0 \le t \le m-1$ and $0 \le s \le q-2$. This implies that

$$p_m - |V(F)| = (q-s)q^{m-t-1} \ge 2. \tag{11}$$

Further, since $|V(F)|$ attains the bound in (6), we see from Theorem 3.2 that there is a positive integer $r \le d$ and homogeneous linear polynomials $G_1, \ldots, G_r$ in $\mathbb{F}_q[X_0, \ldots, X_m]$ such that the corresponding hyperplanes $V(G_1), \ldots, V(G_r)$ are distinct (i.e., $G_1, \ldots, G_r$ are pairwise linearly independent) and

$$V(F) = \bigcup_{i=1}^{r} V(G_i).$$

We claim that $r = d$. To see this, assume the contrary, i.e., suppose $1 \le r < d$. In view of (11), there are $A, B \in \mathbb{P}^m(\mathbb{F}_q) \setminus V(F)$ such that $A \ne B$. Hence by Lemma 4.1, there is a homogeneous linear polynomial L in $\mathbb{F}_q[X_0, \ldots, X_m]$ such that $L(A) = 0$ and $L(B) \ne 0$. Now consider $G := L^{d-r} G_1 \cdots G_r$. Then $G \in \mathbb{F}_q[X_0, \ldots, X_m]_d$ and $G(P) = 0$ for all $P \in V(F) \cup \{A\}$. Also c_G is a nonzero codeword of $\mathsf{PRM}_q(d, m)$ since $G(B) \ne 0$. But the Hamming weight of c_G is smaller than that of c_F since $|V(G)| > |V(F)|$. This contradicts the assumption that c_F is a minimum weight codeword. Hence the claim that $r = d$ is proved.

Now let $G := G_1 \cdots G_d$. Then $V(F) = V(G)$. Hence by Lemma 4.2, there is $\lambda \in \mathbb{F}_q$ with $\lambda \ne 0$ such that $c_F = c_{\lambda G}$. We can thus assume without loss of generality that F is a product of d pairwise linearly independent homogeneous linear factors, and moreover by a linear change of coordinates, we may assume that one of the linear factors is X_m. Consequently, we can write $F = X_m F_1$ for some $F_1 \in \mathbb{F}_q[X_0, \ldots, X_m]_{d-1}$ such that F_1 is not divisible by X_m. Thus, if we let $f_1(X_0, \ldots, X_{m-1}) = F_1(X_0, \ldots, X_{m-1}, 1)$, then f_1 is a polynomial in $\mathbb{F}_q[X_0, \ldots, X_{m-1}]$ of degree $d-1$. Moreover, by intersecting $V(F)$ with the hyperplane $V(X_m)$ and its complement in $\mathbb{P}^m(\mathbb{F}_q)$, we see that

$$p_m - (q-s)q^{m-t-1} = |V(F)| = p_{m-1} + |Z(f_1)| \text{ and so } |Z(f_1)| = q^m - (q-s)q^{m-t-1}.$$

It follows that $\mathrm{ev}(f_1)$ can be viewed as a minimum weight codeword of the Reed-Muller code $\mathrm{RM}_q(d-1, m)$. Hence by [10, Theorem 2.6.3], $\mathrm{ev}(f_1) = \mathrm{ev}(f)$ for some $f \in \mathbb{F}_q[X_0, \ldots, X_{m-1}]$ of the form (2), i.e.,

$$f = \omega_0 \left(\prod_{i=1}^{t} (1 - \ell_i^{q-1}) \right) \prod_{j=1}^{s} (\ell_{t+1} - \omega_j')$$

for some linearly independent polynomials $\ell_1, \ldots, \ell_{t+1} \in \mathbb{F}_q[X_0, \ldots, X_{m-1}]$ of degree 1, and some $\omega_0, \omega_1', \ldots, \omega_s' \in \mathbb{F}_q$ with $\omega_0 \ne 0$ and $\omega_1', \ldots, \omega_s'$ distinct. Now

$$F(X_0, \ldots, X_m) = X_m^d F_1\left(\frac{X_0}{X_m}, \ldots, \frac{X_{m-1}}{X_m}, 1 \right) = X_m\left(X_m^{d-1} f_1\left(\frac{X_0}{X_m}, \ldots, \frac{X_{m-1}}{X_m} \right) \right)$$

and so if we let

$$Q(X_0, \ldots, X_m) := X_m\left(X_m^{d-1} f\left(\frac{X_0}{X_m}, \ldots, \frac{X_{m-1}}{X_m} \right) \right),$$

then we see that $Q \in \mathbb{F}_q[X_0, \ldots, X_m]_d$ and $F(\mathsf{P}_\nu) = Q(\mathsf{P}_\nu)$ for each $\nu = 1, \ldots, p_m$, and hence $c_F = c_Q$. Moreover if we let

$$L_i(X_0, \ldots, X_m) := X_m \left(\ell_{i+1} \left(\frac{X_0}{X_m}, \ldots, \frac{X_{m-1}}{X_m} \right) \right) \quad \text{for } i = 0, 1, \ldots, t-1,$$

and also let $L_t := \omega_0 X_m$ and in case $s > 0$, we further let

$$L_{t+1}(X_0, \ldots, X_m) := X_m \left(\ell_{t+1} \left(\frac{X_0}{X_m}, \ldots, \frac{X_{m-1}}{X_m} \right) \right),$$

then we see that $L_1, \ldots, L_t, L_{t+1}$ are nonzero homogeneous linear polynomials in $\mathbb{F}_q[X_0, \ldots, X_m]$ and moreover

$$Q = L_t \prod_{i=0}^{t-1} \left(L_t^{q-1} - L_i^{q-1} \right) \prod_{j=1}^{s} (L_{t+1} - \omega_j L_t) \quad \text{where} \quad \omega_j := \frac{\omega_j'}{\omega_0} \text{ for } j = 1, \ldots, s.$$

It remains to show that $L_0, \ldots, L_{t+1}$ are linearly independent, or more precisely, if $s = 0$, then $L_0, \ldots, L_t$ are linearly independent, whereas if $s > 0$, then $L_0, \ldots, L_{t+1}$ are linearly independent. To this end, first suppose $s = 0$. Since $\ell_1, \ldots, \ell_t$ are linearly independent, it is clear that $L_0, \ldots, L_{t-1}$ are linearly independent. Now if $L_0, \ldots, L_t$ were linearly dependent, then X_m would be a $\mathbb{F}_q$-linear combination of $L_0, \ldots, L_{t-1}$. On the other hand, since $|V(Q)| = |V(F)| = p_m - q^{m-t} < p_m$, there is some $A \in \mathbb{P}^m(\mathbb{F}_q)$ such that $Q(A) \neq 0$. In particular, $L_t(A) \neq 0$, but $L_i(A) = 0$ for $i = 0, 1, \ldots, t-1$, which shows that X_m cannot be a $\mathbb{F}_q$-linear combination of $L_0, \ldots, L_{t-1}$.

Next, suppose $s > 0$. As before, the linear independence of $\ell_1, \ldots, \ell_{t+1}$ shows that $L_0, \ldots, L_{t-1}, L_{t+1}$ are linearly independent. Fix an arbitrary element A of $\mathbb{P}^m(\mathbb{F}_q) \setminus V(Q)$. Since $Q(A) \neq 0$, we must have $L_t(A) \neq 0$ and $L_i(A) = 0$ for $i = 0, 1, \ldots, t-1$. In particular, we can find a unique representative of A in $\mathbb{F}_q^{m+1}$, say $\mathsf{A} = (\mathsf{a}_0, \mathsf{a}_1, \ldots, \mathsf{a}_m)$, such that $\mathsf{a}_m = 1$. Suppose, if possible, X_m is a $\mathbb{F}_q$-linear combination of $L_0, \ldots, L_{t-1}, L_{t+1}$. Then $L_{t+1}(\mathsf{A})$ is necessarily equal to a fixed nonzero scalar in $\mathbb{F}_q$, say λ, which is independent of the choice of A in $\mathbb{P}^m(\mathbb{F}_q) \setminus V(Q)$. It follows that $|\mathbb{P}^m(\mathbb{F}_q) \setminus V(Q)|$ is at most

$$|\{\mathbf{a} = (a_0, \ldots, a_{m-1}) \in \mathbb{F}_q^m : \ell_i(\mathbf{a}) = 0 \text{ for } i = 1, \ldots, t \text{ and } \ell_{t+1}(\mathbf{a}) = \lambda\}| = q^{m-t-1},$$

where the last equality follows since $\ell_1, \ldots, \ell_{t+1}$ are linearly independent polynomials of degree 1. But then

$$(q - s)q^{m-t-1} = |\mathbb{P}^m(\mathbb{F}_q) \setminus V(Q)| \leq q^{m-t-1},$$

which is a contradiction since $s < q - 1$. This shows that $L_0, \ldots, L_{t+1}$ are linearly independent. $\qquad\square$

5. **Enumeration of minimum weight codewords.** In this section, we will use Theorem 4.3 to prove the following.

Theorem 5.1. *Assume that $1 \leq d \leq m(q - 1) + 1$ and let t, s be unique integers such that $d - 1 = t(q - 1) + s$ with $t \geq 0$ and $0 \leq s < q - 1$. Then the number of minimum weight codewords of $\mathsf{PRM}_q(d, m)$ is equal to*

$$\left(q^{m+1} - 1 \right) \begin{bmatrix} m \\ t \end{bmatrix}_q N_s, \quad \text{where} \quad N_s = \begin{cases} 1 & \text{if } s = 0, \\ \dfrac{1}{s+1} \dbinom{q}{s} \begin{bmatrix} m-t \\ 1 \end{bmatrix}_q & \text{if } s \neq 0. \end{cases} \tag{12}$$

Before giving a proof of this result, it will be convenient to set some notation and terminology, and also some preliminary results which will be useful to us in the sequel. First, let us fix d, t and s as in the statement of Theorem 5.1. We shall denote by $\mathcal{M}_q(d, m)$, and often simply by $\mathcal{M}$, the set of all minimum weight codewords of $\mathsf{PRM}_q(d, m)$. The polynomial ring $\mathbb{F}_q[x_0, \ldots, x_m]$ in $m + 1$ variables with coefficients in $\mathbb{F}_q$ will be denoted by R, and for any nonnegative integer e, we denote by R_e the space of homogeneous polynomials in R of degree e, including the zero polynomial. In particular, R_1 is the $(m + 1)$-dimensional $\mathbb{F}_q$-vector space of homogeneous linear polynomials in R. We shall use a slight variant of the notion of support of a codeword of $\mathsf{PRM}_q(d, m)$. Namely, given any $F \in R_d$, we let

$$\mathrm{supp}(c_F) = \{P \in \mathbb{P}^m(\mathbb{F}_q) : F(P) \neq 0\} = \mathbb{P}^m(\mathbb{F}_q) \setminus V(F).$$

Thus, the only difference between $\mathrm{supp}(c_F)$ and $\mathrm{Supp}(c_F)$ is that the former comprises of points of $\mathbb{P}^m(\mathbb{F}_q)$ rather than their chosen representatives in $\mathbb{F}_q^{m+1}$. Let $\mathcal{P}(\mathbb{P}^m)$ denote the set of all subsets of $\mathbb{P}^m(\mathbb{F}_q)$. In view of Lemma 4.2, we see that the map $\Phi : \mathcal{M} \to \mathcal{P}(\mathbb{P}^m)$ defined by $\Phi(c) := \mathrm{supp}(c)$ has the property that

$$|\mathcal{M}| = (q - 1)|\Phi(\mathcal{M})|. \tag{13}$$

Continuing with notations, for any $e \in \mathbb{Z}$ with $-1 \leq e \leq m$, we denote by $\mathcal{G}_e(\mathbb{P}^m)$ the Grassmannian consisting of all e-dimensional projective linear subspaces[3] of $\mathbb{P}^m(\mathbb{F}_q)$. It is elementary and well-known that the cardinality of $\mathcal{G}_e(\mathbb{P}^m)$ is the Gaussian binomial coefficient $\begin{bmatrix} m+1 \\ e+1 \end{bmatrix}_q$. Here is a useful preliminary result.

Lemma 5.2. *Let* $K_0, \ldots, K_r \in R_1$ *be linearly independent. Then the map*

$$\theta : \mathbb{F}_q^{m+1} \to \mathbb{F}_q^{r+1} \quad \text{defined by} \quad \theta(\mathbf{a}) := (K_0(\mathbf{a}), \ldots, K_r(\mathbf{a}))$$

is surjective.

Proof. Extend $\{K_0, \ldots, K_r\}$ to a $\mathbb{F}_q$-vector space basis $\{K_0, \ldots, K_m\}$ of R_1. Then the map $\widehat{\theta} : \mathbb{F}_q^{m+1} \to \mathbb{F}_q^{m+1}$ defined by $\widehat{\theta}(\mathbf{a}) := (K_0(\mathbf{a}), \ldots, K_m(\mathbf{a}))$ is an $\mathbb{F}_q$-vector space isomorphism. In particular, $\widehat{\theta}$ is surjective, and hence so is θ. $\square$

The following lemma will prove Theorem 5.1 in the special case when $s = 0$.

Lemma 5.3. *Assume that $s = 0$ so that $d = t(q - 1) + 1$ with $0 \leq t \leq m$. Then*

$$|\mathcal{M}_q(d, m)| = (q^{m+1} - 1) \begin{bmatrix} m \\ t \end{bmatrix}_q.$$

Proof. If $t = 0 = s$, then $\mathsf{PRM}_q(d, m)$ is the simplex code of length p_m, dimension $m+1$ and minimum distance q^m. In this case, every nonzero codeword is a minimum weight codeword and so the desired formula clearly holds. We now assume that $t \geq 1$. Consider the incidence set $\mathcal{I}$ and the map $\tau : \mathcal{I} \to \Phi(\mathcal{M})$ defined by

$$\mathcal{I} := \{(E, H) \in \mathcal{G}_{m-t}(\mathbb{P}^m) \times \mathcal{G}_{m-t-1}(\mathbb{P}^m) : H \subseteq E\} \quad \text{and} \quad \tau(E, H) := E \cap H^c,$$

where by H^c we denote the complement of H in $\mathbb{P}^m(\mathbb{F}_q)$, i.e., $H^c := \mathbb{P}^m(\mathbb{F}_q) \setminus H$. Note that if $(E, H) \in \mathcal{I}$, then there are linearly independent $L_0, \ldots, L_t \in R_1$ such that $E = V(L_0, \ldots, L_{t-1})$ and $H = V(L_0, \ldots, L_t)$. Consequently,

$$E \cap H^c = \mathrm{supp}(c_F) \quad \text{where} \quad F := L_t \prod_{i=0}^{t-1} \left(L_t^{q-1} - L_i^{q-1} \right).$$

---

[3] As per the standard conventions, the empty subset of $\mathbb{P}^m(\mathbb{F}_q)$, which corresponds to the zero subspace of $\mathbb{F}_q^{m+1}$, is the only projective linear subspace of $\mathbb{P}^m(\mathbb{F}_q)$ of dimension -1.

Thus τ is well-defined. Moreover, Theorem 4.3 shows that τ is surjective. We claim that τ is also injective. To see this, let (E, H), $(E', H') \in \mathcal{I}$ be such that $\tau(E, H) = \tau(E', H')$. Suppose, if possible, $H \neq H'$. Then there are linearly independent $L_0, \ldots, L_t \in R_1$ and linearly independent $L'_0, \ldots, L'_t$ in R_1 such that $E = V(L_0, \ldots, L_{t-1})$, $H = V(L_0, \ldots, L_t)$, $E' = V(L'_0, \ldots, L'_{t-1})$, and $H' = V(L'_0, \ldots, L'_t)$. Since H, H' have the same dimension and $H \neq H'$, we must have $H \nsubseteq H'$. Hence there is some $j \in \{0, \ldots, t\}$ such that L'_j does not vanish on H. This implies that $L_0, \ldots, L_t, L'_j$ are linearly independent. First, suppose $0 \leq j \leq t-1$. By Lemma 5.2, there exists $\mathbf{a} \in \mathbb{F}_q^{m+1}$ such that $L_0(\mathbf{a}) = \cdots = L_{t-1}(\mathbf{a}) = 0$ and $L_t(\mathbf{a}) = 1 = L'_j(\mathbf{a})$. Next, suppose $j = t$. Again, by Lemma 5.2, there exists $\mathbf{b} \in \mathbb{F}_q^{m+1}$ such that $L_0(\mathbf{b}) = \cdots = L_{t-1}(\mathbf{b}) = 0$ and $L_t(\mathbf{b}) = 1$, but $L'_t(\mathbf{b}) = 0$. Note that these $\mathbf{a}$ and $\mathbf{b}$, when they exist, are necessarily nonzero. Thus, in either case, if P is the point of $\mathbb{P}^m(\mathbb{F}_q)$ corresponding to $\mathbf{a}$ or $\mathbf{b}$ (according as $0 \leq j < t$ or $j = t$), then $P \in E \cap H^c$, but $P \notin E' \cap H'^c$. But this contradicts the assumption that $\tau(E, H) = \tau(E', H')$. So we must have $H = H'$, and therefore $E = E'$. Thus we have shown that τ is bijective. Consequently, in view of (13), we obtain

$$|\mathcal{M}_q(d, m)| = (q-1)|\mathcal{I}| = (q-1)\begin{bmatrix} m+1 \\ m-t+1 \end{bmatrix}_q \begin{bmatrix} m-t+1 \\ 1 \end{bmatrix}_q = (q^{m+1}-1)\begin{bmatrix} m \\ t \end{bmatrix}_q,$$

as desired. □

Next, we consider the case when $s \neq 0$. By Theorem 4.3, we know that a minimum weight codeword of $\mathsf{PRM}_q(d, m)$ is of the form c_F, where

$$F = L_t \prod_{i=0}^{t-1} \left(L_t^{q-1} - L_i^{q-1} \right) \prod_{j=1}^{s} (L_{t+1} - \omega_j L_t) \tag{14}$$

for some linearly independent $L_0, \ldots, L_{t+1} \in R_1$ and some distinct $\omega_1, \ldots, \omega_s \in \mathbb{F}_q$. The support of such a codeword is given by $V(L_t)^c \cap V(L_0, \ldots, L_{t-1}) \cap W$, where

$$W = \bigcap_{j=1}^{s} V(L_{t+1} - \omega_j L_t)^c = \bigcup_{\mu} V(L_{t+1} - \mu L_t),$$

where μ varies over elements of $\mathbb{F}_q \setminus \{\omega_1, \ldots, \omega_s\}$. It is, however, possible that a different choice $L'_0, \ldots, L'_{t+1} \in R_1$ could give rise to the same support. In effect, one can replace L_t by a linear combination of the form $L_t + \sum_{i=0}^{t-1} c_i L_i$ or one can even swap it with a factor of the form $(L_{t+1} - \omega_j L_t)$. Thus one has to be a little more careful while counting the possible supports of minimum weight codewords. To do it systematically, we consider a set $\mathcal{J}$ and a map Ψ defined as follows.

Let $\mathcal{P}_s(\mathbb{F}_q)$ denote the set of all subsets of $\mathbb{F}_q$ containing s elements, and let

$$\mathcal{J} := \{(E, L_t, L_{t+1}, S) \in \Lambda : E \nsubseteq V(L_t) \text{ and } E \cap V(L_t) \nsubseteq V(L_{t+1})\},$$

where $\Lambda := \mathcal{G}_{m-t}(\mathbb{P}^m) \times R_1 \times R_1 \times \mathcal{P}_s(\mathbb{F}_q)$. Define $\Psi : \mathcal{J} \longrightarrow \Phi(\mathcal{M})$ by

$$\Psi(E, L_t, L_{t+1}, S) := (E \setminus V(L_t)) \cap \left(\bigcup_{\mu \in \mathbb{F}_q \setminus S} V(L_{t+1} - \mu L_t) \right) \text{ for } (E, L_t, L_{t+1}, S) \in \mathcal{J}.$$

Note that if $(E, L_t, L_{t+1}, S) \in \mathcal{J}$, then there are polynomials $L_0, \ldots, L_{t-1} \in R_1$ such that $E = V(L_0, \ldots, L_{t-1})$ and $L_0, \ldots, L_{t+1}$ are linearly independent, and moreover, $\Psi(E, L_t, L_{t+1}, S) = \mathrm{supp}(c_F)$, where F is given by (14). This shows that Ψ is well-defined. Furthermore, Theorem 4.3 shows that Ψ is surjective. The next few lemmas will help us analyze the fibres of Ψ.

Lemma 5.4. *Let* (E, L_t, L_{t+1}, S) *and* (E', L'_t, L'_{t+1}, S') *be elements of* $\mathcal{J}$ *such that* $\Psi(E, L_t, L_{t+1}, S) = \Psi(E', L'_t, L'_{t+1}, S')$. *Then* $E = E'$.

Proof. By our hypothesis, we can find $L_0, \ldots, L_{t-1}, L'_0, \ldots, L'_{t-1} \in R_1$ such that $E = V(L_0, \ldots, L_{t-1})$, $E' = V(L'_0, \ldots, L'_{t-1})$, and the subsets $\{L_0, \ldots, L_{t+1}\}$ and $\{L'_0, \ldots, L'_{t+1}\}$ of R_1 are linearly independent; moreover, if F is given by (14) and F' is given by (14) with L_i replaced by L'_i for $0 \le i \le t+1$ and S by S', then

$$\Psi(E, L_t, L_{t+1}, S) = \operatorname{supp}(c_F) = \operatorname{supp}(c_{F'}) = \Psi(E', L'_t, L'_{t+1}, S'). \qquad (15)$$

Now suppose, if possible, $E \ne E'$. Then one among $L'_0, \ldots, L'_{t-1}$, say L'_0, must be such that $L_0, \ldots, L_{t-1}, L'_0$ are linearly independent. In case $L_0, \ldots, L_{t+1}, L'_0$ are also linearly independent, then by Lemma 5.2, we can find $P \in E$ such that $L_t(P) \ne 0$ and $L_{t+1}(P) = \mu L_t(P)$ for some $\mu \in \mathbb{F}_q \setminus S$ and moreover, $L'_0(P) \ne 0$. But then $P \in \operatorname{supp}(c_F) \setminus \operatorname{supp}(c_{F'})$, which contradicts (15). Thus $L_0, \ldots, L_{t+1}, L'_0$ are linearly dependent, and so we can find $c_0, \ldots, c_{t+1} \in \mathbb{F}_q$ such that

$$L'_0 = c_0 L_0 + \ldots + c_{t-1} L_{t-1} + c_t L_t + c_{t+1} L_{t+1} \quad \text{and} \quad c_t, c_{t+1} \text{ are not both zero.}$$

Now since $|S| = s \le q - 2$, there exist distinct $\mu_1, \mu_2 \in \mathbb{F}_q \setminus S$. By Lemma 5.2, we can find $P_1, P_2 \in E$ such that $L_t(P_i) \ne 0$ and $L_{t+1}(P_i) = \mu_i L_t(P_i)$ for $i = 1, 2$. It follows that $P_1, P_2 \in \operatorname{supp}(c_F) = \operatorname{supp}(c_{F'})$, and hence $L'_0(P_i) = 0$ for $i = 1, 2$. On the other hand, $L'_0(P_i) = (c_t + c_{t+1}\mu_i)L_t(P_i)$ for $i = 1, 2$. But then $c_t + c_{t+1}\mu_1 = 0 = c_t + c_{t+1}\mu_2$, which implies that $c_{t+1} = 0$ (since $\mu_1 \ne \mu_2$), and hence $c_t = 0$. Thus we obtain a contradiction. This proves that $E = E'$. $\qquad \square$

Lemma 5.5. *Suppose* $(E, L_t, L_{t+1}, S) \in \mathcal{J}$ *and* $S' \in \mathcal{P}_s(\mathbb{F}_q)$ *have the property that* $\Psi(E, L_t, L_{t+1}, S) = \Psi(E, L_t, L_{t+1}, S')$. *Then* $S = S'$.

Proof. Suppose, on the contrary, $S \ne S'$. Pick some $\omega \in S$ such that $\omega \notin S'$. By Lemma 5.2, we can find $P \in E$ such that $L_t(P) \ne 0$ and $L_{t+1}(P) = \omega L_t(P)$. Then $P \in \Psi(E, L_t, L_{t+1}, S')$, while $P \notin \Psi(E, L_t, L_{t+1}, S)$, which is a contradiction. $\qquad \square$

Lemma 5.6. *Let* $(E, L_t, L_{t+1}, S) \in \mathcal{J}$. *Then there are exactly* $q^{t+1}(q-1)$ *elements in* $\mathcal{J}$ *of the form* (E, L_t, L'_{t+1}, S') *such that* $\Psi(E, L_t, L_{t+1}, S) = \Psi(E, L_t, L'_{t+1}, S')$.

Proof. Suppose $L'_{t+1} \in R_1$ and $S' \in \mathcal{P}_s(\mathbb{F}_q)$ are such that $\Psi(E, L_t, L_{t+1}, S) = \Psi(E, L_t, L'_{t+1}, S')$. Choose $L_0, \ldots, L_{t-1} \in R_1$ such that $E = V(L_0, \ldots, L_{t-1})$ and $\{L_0, \ldots, L_{t+1}\}$ as well as $\{L_0, \ldots, L_t, L'_{t+1}\}$ are linearly independent. In case $\{L_0, \ldots, L_{t+1}, L'_{t+1}\}$ is also linearly independent, then by Lemma 5.2, we can find $P \in E$ such that $L_t(P) \ne 0$, $L_{t+1}(P) = \mu L_t(P)$, and $L'_{t+1}(P) = \omega L_t(P)$ for some $\mu \in \mathbb{F}_q \setminus S$ and $\omega \in S$. But then $P \in \Psi(E, L_t, L_{t+1}, S') \setminus \Psi(E, L_t, L'_{t+1}, S')$, which is a contradiction. Thus there are $c_0, \ldots, c_{t+1} \in \mathbb{F}_q$ such that

$$L'_{t+1} = c_0 L_0 + \ldots + c_{t-1} L_{t-1} + c_t L_t + c_{t+1} L_{t+1}. \qquad (16)$$

Note that $c_0, \ldots, c_{t+1}$ are uniquely determined by L'_{t+1} since $\{L_0, \ldots, L_{t+1}\}$ is linearly independent. Moreover, $c_{t+1} \ne 0$ since $\{L_0, \ldots, L_t, L'_{t+1}\}$ is also linearly independent. On the other hand, if $c_0, \ldots, c_{t+1} \in \mathbb{F}_q$ are picked arbitrarily with $c_{t+1} \ne 0$, and if L'_{t+1} is given by (16), then we will show that there exists unique S' in $\mathcal{P}_s(\mathbb{F}_q)$ such that $\Psi(E, L_t, L_{t+1}, S) = \Psi(E, L_t, L'_{t+1}, S')$. To prove the existence, note that for any $\lambda \in \mathbb{F}_q$,

$$L'_{t+1} - \lambda L_t = c_t L_t + c_{t+1} L_{t+1} - \lambda L_t = c_{t+1}\left(L_{t+1} - \frac{\lambda - c_t}{c_{t+1}} L_t\right) \quad \text{on points of } E.$$

Thus if we take $S' \in \mathcal{P}_s(\mathbb{F}_q)$ such that $\mathbb{F}_q \setminus S' = \{\mu c_{t+1} + c_t : \mu \in \mathbb{F}_q \setminus S\}$, then

$$E \cap \Big(\bigcup_{\mu' \in \mathbb{F}_q \setminus S'} V(L'_{t+1} - \mu' L_t) \Big) = E \cap \Big(\bigcup_{\mu \in \mathbb{F}_q \setminus S} V(L_{t+1} - \mu L_t) \Big).$$

This implies that $\Psi(E, L_t, L_{t+1}, S) = \Psi(E, L_t, L'_{t+1}, S')$. The uniqueness of S' (for the given choice of L'_{t+1}) is an immediate consequence of Lemma 5.5. Since L'_{t+1} of the form (16) can be chosen in exactly $q^{t+1}(q-1)$ ways, the lemma is proved. $\square$

Lemma 5.7. *Let* $(E, L_t, L_{t+1}, S) \in \mathcal{J}$. *Then there are exactly* $(s+1)(q-1)^2 q^{2t+1}$ *elements* (E', L'_t, L'_{t+1}, S') *in* $\mathcal{J}$ *such that* $\Psi(E, L_t, L_{t+1}, S) = \Psi(E', L'_t, L'_{t+1}, S')$.

Proof. Write $\sigma := \Psi(E, L_t, L_{t+1}, S)$. Choose $L_0, \ldots, L_{t-1} \in R_1$ such that $E = V(L_0, \ldots, L_{t-1})$ and $\{L_0, \ldots, L_{t+1}\}$ is linearly independent. Now if (E', L'_t, L'_{t+1}, S') is in $\Psi^{-1}(\sigma)$, i.e., it is an element of $\mathcal{J}$ such that $\Psi(E', L'_t, L'_{t+1}, S') = \sigma$, then by Lemma 5.4, $E' = E$, and therefore, $\{L_0, \ldots, L_{t-1}, L'_t, L'_{t+1}\}$ is also linearly independent. Further, as before, we can use Lemma 5.2 to show that $\{L_0, \ldots, L_{t+1}, L'_t\}$ is linearly dependent. Thus exactly one of the following two cases are possible.

Case 1. $L'_t := b_0 L_0 + \cdots + b_t L_t$ for some $b_0, \ldots, b_t \in \mathbb{F}_q$.

In this case, we must have $b_t \neq 0$. Further, given any $b_0, \ldots, b_t \in \mathbb{F}_q$ with $b_t \neq 0$, if we take $L'_t := b_0 L_0 + \cdots + b_t L_t$, then we can show that there is a unique $S^* \in \mathcal{P}_s(\mathbb{F}_q)$ for which $\Psi(E, L_t, L_{t+1}, S) = \Psi(E', L'_t, L_{t+1}, S^*)$. Indeed, the uniqueness of S^* is clear from Lemma 5.5, whereas for the existence, it suffices to observe that for any $\lambda \in \mathbb{F}_q$,

$$L_{t+1} - \lambda L'_t = L_{t+1} - \lambda b_t L_t \quad \text{on points of } E,$$

and so we can take $S^* = \{\mu/b_t : \mu \in \mathbb{F}_q \setminus S\}$. It follows that there are exactly $q^t(q-1)$ choices of $b_0, \ldots, b_t \in \mathbb{F}_q$ with $b_t \neq 0$ and a corresponding unique choice of S^* for which $L'_t := b_0 L_0 + \ldots + b_t L_t$ satisfies $\Psi(E, L_t, L_{t+1}, S) = \Psi(E', L'_t, L_{t+1}, S^*)$. Furthermore, for any such choice of L'_t and $S^* \in \mathcal{P}_s(\mathbb{F}_q)$, by Lemma 5.6, there are exactly $q^{t+1}(q-1)$ choices of L'_{t+1} and corresponding unique choice of $S' \in \mathcal{P}_s(\mathbb{F}_q)$ for which $\Psi(E', L'_t, L_{t+1}, S^*) = \Psi(E', L'_t, L'_{t+1}, S')$. It follows that there are exactly $q^t(q-1) \times q^{t+1}(q-1) = q^{2t+1}(q-1)^2$ elements (E', L'_t, L'_{t+1}, S') in $\Psi^{-1}(\sigma)$ for which $L'_t := b_0 L_0 + \ldots + b_t L_t$ for some $b_0, \ldots, b_t \in \mathbb{F}_q$ with $b_t \neq 0$.

Case 2. $L'_t = b_0 L_0 + \cdots + b_{t+1} L_{t+1}$ for some $b_0, \ldots, b_{t+1} \in \mathbb{F}_q$ with $b_{t+1} \neq 0$.

In this case, we claim that $-b_t/b_{t+1} \in S$. To prove this, assume the contrary. Use Lemma 5.2 to choose $P \in E$ such that $L_t(P) \neq 0$ and $L_{t+1}(P) = (-b_t/b_{t+1}) L_t(P)$. Then $P \in \sigma$, since $-b_t/b_{t+1} \notin S$. On the other hand, our choice of P implies that

$$L'_t(P) = b_t L_t(P) + b_{t+1} L_{t+1}(P) = 0$$

and therefore $P \notin \Psi(E', L'_t, L'_{t+1}, S') = \sigma$, which is a contradiction. Thus the claim is proved. We shall now show that for any fixed choice of $b_0, \ldots, b_{t+1} \in \mathbb{F}_q$ with $b_{t+1} \neq 0$ and $-b_t/b_{t+1} \in S$, if we take $L'_t = b_0 L_0 + \cdots + b_{t+1} L_{t+1}$, and $L^*_{t+1} := L_t$, then there is a unique $S^* \in \mathcal{P}_s(\mathbb{F}_q)$ such that $(E, L'_t, L^*_{t+1}, S^*) \in \mathcal{J}$ and $\Psi(E, L'_t, L^*_{t+1}, S^*) = \sigma$. To see this, first note that $\{L_0, \ldots, L_{t-1}, L'_t, L^*_{t+1}\}$ is linearly independent. Further, if we take $S^* \in \mathcal{P}_s(\mathbb{F}_q)$ such that

$$\mathbb{F}_q \setminus S^* = \left\{ \frac{1}{b_t + \mu b_{t+1}} : \mu \in \mathbb{F}_q \setminus S \right\}.$$

then S^* is well-defined since $-b_t/b_{t+1} \in S$. Moreover, if for any $\mu^* \in \mathbb{F}_q \setminus S^*$, we write $\mu^* = 1/(b_t + \mu b_{t+1})$ for some $\mu \in \mathbb{F}_q \setminus S$, then on points of E, we have

$$L_{t+1}^* - \mu^* L_t' = L_t - \frac{1}{b_t + \mu b_{t+1}}(b_t L_t + b_{t+1} L_{t+1}) = \frac{-b_{t+1}}{b_t + \mu b_{t+1}}(L_{t+1} - \mu L_t).$$

Consequently,

$$(E \setminus V(L_t')) \cap \Big(\bigcup_{\mu^* \in \mathbb{F}_q \setminus S^*} V(L_{t+1}^* - \mu^* L_t') \Big) = (E \setminus V(L_t)) \cap \Big(\bigcup_{\mu \in \mathbb{F}_q \setminus S} V(L_{t+1} - \mu L_t) \Big) = \sigma.$$

This shows the existence of a polynomial $L_{t+1}^* \in R_1$ and a set $S^* \in \mathcal{P}_s(\mathbb{F}_q)$ such that $(E, L_t', L_{t+1}^*, S^*) \in \mathcal{J}$ and $\Psi(E, L_t', L_{t+1}^*, S^*) = \sigma$. The uniqueness of S^* for the given choice of L_{t+1}^* is clear from Lemma 5.5. Moreover, by Lemma 5.6, there are exactly $q^{t+1}(q-1)$ choices of L_{t+1}' and corresponding unique choice of $S' \in \mathcal{P}_s(\mathbb{F}_q)$ for which $\Psi(E', L_t', L_{t+1}^*, S^*) = \Psi(E', L_t', L_{t+1}', S')$. Since $b_0, \ldots, b_{t+1} \in \mathbb{F}_q$ such that $b_{t+1} \neq 0$ and $-b_t/b_{t+1} \in S$ can be chosen in $s(q-1)q^t$ ways, we see that there are exactly $q^{t+1}(q-1) \times s(q-1)q^t = sq^{2t+1}(q-1)^2$ elements (E', L_t', L_{t+1}', S') in $\Psi^{-1}(\sigma)$ for which L_t' is as in Case 2.

By combining the counts in Case 1 and Case 2, we obtain the desired result. $\square$

We are now ready to prove the main result of this section.

Proof of Theorem 5.1. If $s = 0$, then the desired formula (12) follows from Lemma 5.3. If $s \neq 0$, then by Lemma 5.7,

$$|\Psi^{-1}(\sigma)| = (s+1)(q-1)^2 q^{2t+1} \quad \text{for all } \sigma \in \Phi(\mathcal{M}). \tag{17}$$

It follows that

$$
\begin{aligned}
|\Phi(\mathcal{M})| &= \frac{|\mathcal{J}|}{(s+1)(q-1)^2 q^{2t+1}} \\
&= \frac{1}{(s+1)(q-1)^2 q^{2t+1}} \begin{bmatrix} m+1 \\ m-t+1 \end{bmatrix}_q \left(q^{m+1} - q^t\right)\left(q^{m+1} - q^{t+1}\right)\binom{q}{s} \\
&= \frac{1}{s+1} \begin{bmatrix} m+1 \\ t \end{bmatrix}_q \begin{bmatrix} m-t+1 \\ 1 \end{bmatrix}_q \begin{bmatrix} m-t \\ 1 \end{bmatrix}_q \binom{q}{s} \\
&= \frac{(q^{m+1} - 1)}{(s+1)(q-1)} \begin{bmatrix} m \\ t \end{bmatrix}_q \begin{bmatrix} m-t \\ 1 \end{bmatrix}_q \binom{q}{s}.
\end{aligned}
$$

By combining this with (13), we obtain the desired formula. $\square$

Remark 5.8. The formula (12) for the number of minimum weight codewords of the projective Reed-Muller code $\mathsf{PRM}_q(d, m)$ is evidently a positive integer when $s = 0$. In case $s \neq 0$, we can easily rewrite (12) as

$$\frac{\left(q^{m+1} - 1\right)\left(q^m - 1\right)}{(q+1)(q-1)} \begin{bmatrix} m-1 \\ t \end{bmatrix}_q \binom{q+1}{s+1},$$

and this readily shows that it is a positive integer. In the special case when $t = m-1$ and $s = q - k$, where $2 \leq k \leq q - 1$, the formula reduces to

$$\frac{(q-1)}{(q+1)} p_m p_{m-1} \binom{q+1}{k}.$$

It may be interesting to note that this is precisely equal to $(q-1)$ times the number of collections of k collinear points in $\mathbb{P}^m(\mathbb{F}_q)$. For geometric interpretations such as this, and more, we refer to Kaplan and Matei [15], especially §3.3 of their paper.

6. **Dimension formulas for projective Reed-Muller codes.** Fix throughout this section $m, d \in \mathbb{Z}$ such that $m \geq 1$ and $1 \leq d \leq m(q-1)+1$. As before, let t, s be unique integers such that $d - 1 = t(q-1) + s$ with $t \geq 0$ and $0 \leq s < q - 1$. An explicit formula for the dimension of a PRM code of an arbitrary order d was first given by Sørensen [27]. It is as follows.

$$\alpha_q(d, m) := \sum_{\substack{e=1 \\ e \equiv d \pmod{q-1}}}^{d} \left(\sum_{j=0}^{m+1} (-1)^j \binom{m+1}{j} \binom{e - jq + m}{e - jq} \right). \tag{18}$$

Later Mercier-Rolland [20] gave another formula for the dimension of PRM codes of order d using the dimension of vanishing ideal of $\mathbb{P}^m(\mathbb{F}_q)$. This one is as follows.

$$\beta_q(d, m) := \binom{m + d}{d} - \sum_{j=2}^{m+1} (-1)^j \binom{m+1}{j} \sum_{i=0}^{j-2} \binom{d + (i+1)(q-1) - jq + m}{d + (i+1)(q-1) - jq}. \tag{19}$$

Around the same time[4], Rentería and Tapia-Recillas [24, Proposition 12] gave the following nice formula for the dimension of $\mathsf{PRM}_q(d, m)$:

$$\gamma_q(d, m) := \sum_{i=0}^{m} \sum_{j=0}^{i} (-1)^j \binom{i}{j} \binom{i + d - 1 - jq}{i}. \tag{20}$$

More recently, Can, Joshua and Ravindra [8, Proposition 3.5] have proposed another formula for the dimension of PRM codes of order d, which is as follows.

$$\delta_q(d, m) := \sum_{\substack{e=1 \\ e \equiv d \pmod{q-1}}}^{d} \left(\sum_{j=0}^{\lfloor e/q \rfloor} (-1)^j \binom{m+1}{j} \binom{e - jq + m}{m} \right). \tag{21}$$

Can, Joshua and Ravindra [8] further alleged that the formula of Sørensen [27] is wrong and wrote that the expression on the right in (18) is equal to 0. This is, in fact, not correct. To clear the confusion, let us first note that the binomial coefficients are (and always should be!) defined as in the beginning of Section 2. In particular, $\binom{a}{b}$ is zero when $b < 0$. In fact, if $a, b \in \mathbb{Z}$, then

$$\binom{a}{b} = 0 \iff \text{either } b < 0 \text{ or } b > a \geq 0. \tag{22}$$

Furthermore, the identity $\binom{a}{b} = \binom{a}{a-b}$ is not absolute, but conditional. In the first place it requires that $a \in \mathbb{Z}$ and in fact, for any $a, b \in \mathbb{Z}$

$$\binom{a}{b} = \binom{a}{a - b} \iff \text{either } a \geq 0 \text{ or } a < b < 0. \tag{23}$$

We remark in passing that on the other hand, the Pascal triangle identity, viz.,

$$\binom{a}{b - 1} + \binom{a}{b} = \binom{a + 1}{b} \tag{24}$$

is an absolute identity in the sense that it is valid for all $b \in \mathbb{Z}$ and all a in any integral domain containing $\mathbb{Z}$ as a subring. At any rate, in view of (22), the summation over j in (18) is, in effect, over $0 \leq j \leq \min\{m + 1, \lfloor e/q \rfloor\} = \lfloor e/q \rfloor$ for any positive integer $e \leq d$, where the last equality follows since $e \leq d \leq m(q-1) + 1 \leq mq$. Moreover, for $0 \leq j \leq \lfloor e/q \rfloor$, by (23), we obtain $\binom{e - jq + m}{e - jq} = \binom{e - jq + m}{m}$. Thus it

---

is clear that $\alpha_q(d,m) = \delta_q(d,m)$. In other words, the formulas of Sørensen and of Can, Joshua and Ravindra are, in fact, the same! The argument in Section 3 of [8] to conclude that $\alpha_q(d,m) = 0$ uses their Lemma 3.3, which is perfectly fine, but then it also uses the "identity" $\binom{e-jq+m}{e-jq} = \binom{e-jq+m}{m}$ for an arbitrary nonnegative integer j, which as we have noted in (23), is not always true. [There is also a typo in the definition given in [8, p. 6] of the polynomial $P(x)$; namely, t should be replaced throughout by $t+m$ in the expression on the right, but this is minor].

The equivalence of (18) and (19) is rather nontrivial. As mentioned in [20], a direct proof of this was given by Michel Quercia, but to the best of our knowledge, this has not been published. The argument of Michel Quercia was made available to us by Robert Rolland, and we have reproduced it in the appendix to this paper. We give below an alternative argument to prove the equivalence of these formulas. This alternative argument uses the following simple combinatorial lemma, which has been given, for instance, by Sørensen [27].

Lemma 6.1. *Let n, a, b be any nonnegative integers and let $N(a, n, b)$ denote the number of ways in which one can place a objects in n blocks such that no block contains more than b objects. Then*

$$N(a, n, b) = \sum_{j=0}^{n} (-1)^j \binom{n}{j} \binom{a - j(b+1) + n - 1}{a - j(b+1)}. \qquad (25)$$

Proof. See [27, Lemma 5]. Or use an argument as in the proof of [12, Lemma 1]. □

Remark 6.2. Given any nonnegative integers n, a, b, it is clear from the description of $N(a, n, b)$ that it is the number of monomials in n variables of degree a such that the degree in each variable is at most b. In particular, if $0 \le \nu \le n(q-1)$, then $N(\nu, n, q-1)$ is the number of reduced monomials of degree ν in n variables, and so we see that $N(\nu, n, q-1) = \rho_q(\nu, n) - \rho_q(\nu - 1, n)$, where $\rho_q(\nu, n)$ is given by (1) if $n \ge 1$ and where by convention, $\rho_q(0, 0) := 1$ and $\rho_q(k, n) := 0$ if $k \in \mathbb{Z}$ with $k < 0$. This can also be seen directly by comparing (1) with the formula in Lemma 6.1 and using the Pascal triangle identity (24). Note also that the degree of a reduced monomial in n variables is always $\le n(q-1)$ and so

$$\rho_q(\nu, n) = \rho_q\left(\min\{\nu,\, n(q-1)\},\, n\right) \quad \text{for any nonnegative integers } \nu, n. \qquad (26)$$

This is clear from the description of $\rho_q(\nu, n)$ as the number of reduced monomials in n variables of degree $\le \nu$, and also from the formula (1) because if $\nu > n(q-1)$, then using (1), (25), and successive applications of (24), we see that

$$\rho_q(\nu, n) = \rho_q(n(q-1), n) + \sum_{a=n(q-1)+1}^{\nu} N(a,\, n,\, q-1) \;=\; \rho_q(n(q-1),\, n),$$

where the last equality follows since any distribution of $n(q-1)+1$ or more objects in n blocks will result in at least one block containing q or more objects.

We are now ready to prove that the two dimension formulas $\alpha_q(d,m)$ and $\beta_q(d,m)$ given by (18) and (19) are equal.

Proposition 6.3. $\alpha_q(d,m) = \beta_q(d,m)$.

Proof. First note that we may rewrite (19) as

$$\beta_q(d,m) = \binom{m+d}{d} - \sum_{j=0}^{m+1}(-1)^j\binom{m+1}{j}\sum_{\substack{e=d+(q-1) \\ e\equiv d \ (\mathrm{mod}\ q-1)}}^{d+(j-1)(q-1)}\binom{e-jq+m}{e-jq}.$$

Also note that by separating terms in (18) corresponding to $e = d$ and $j = 0$ as well as $e = d$ and $j \geq 1$, we can write

$$\alpha_q(d,m) \quad = \quad \sum_{\substack{1\leq e<d \\ e\equiv d \ (\mathrm{mod}\ q-1)}}\sum_{j=0}^{m+1}(-1)^j\binom{m+1}{j}\binom{e-jq+m}{e-jq}$$

$$+\binom{m+d}{d} + \sum_{j=1}^{m+1}(-1)^j\binom{m+1}{j}\binom{d-jq+m}{d-jq}$$

Thus $\alpha_q(d,m) = \beta_q(d,m)$ is equivalent to the equality

$$\sum_{j=0}^{m+1}(-1)^j\binom{m+1}{j}\sum_{\substack{e=1 \\ e\equiv d \ (\mathrm{mod}\ q-1)}}^{d+(j-1)(q-1)}\binom{e-jq+m}{e-jq} = 0, \tag{27}$$

Define

$$c := \sum_{j=0}^{m+1}(-1)^j\binom{m+1}{j}\sum_{\substack{e\equiv d \ (\mathrm{mod}\ q-1) \\ -\infty<e\leq d+(j-1)(q-1)}}\binom{e-jq+m}{e-jq}.$$

Then the expression on the left in (27) is equal to $c - 1$ if d is a multiple of $q - 1$, and is equal to c otherwise. Thus it is enough to show that $c = 1$ if d is a multiple of $q - 1$ and $c = 0$ if d is not a multiple of $q - 1$. Now

$$c \quad = \quad \sum_{j=0}^{m+1}\sum_{k=0}^{\infty}(-1)^j\binom{m+1}{j}\binom{d+(j-1)(q-1)-k(q-1)-jq+m}{d+(j-1)(q-1)-k(q-1)-jq}$$

$$= \quad \sum_{k=0}^{\infty}\sum_{j=0}^{m+1}(-1)^j\binom{m+1}{j}\binom{d+(j-1)(q-1)-k(q-1)-jq+m}{d+(j-1)(q-1)-k(q-1)-jq}$$

$$= \quad \sum_{k=0}^{\infty}\sum_{j=0}^{m+1}(-1)^j\binom{m+1}{j}\binom{d-(k+1)(q-1)-j+m}{d-(k+1)(q-1)-j}$$

$$= \quad \sum_{k=0}^{\infty}N(d-(k+1)(q-1),\ m+1,\ 0)$$

where the last equality uses Lemma 6.1 and the notation therein. But evidently,

$$N(d-(k+1)(q-1),\ m+1,\ 0) = \begin{cases} 1 & \text{if } d = (k+1)(q-1), \\ 0 & \text{if } d \neq (k+1)(q-1). \end{cases}$$

This implies that $c = 1$ if d is a multiple of $q - 1$, and 0 otherwise. $\square$

We will now consider the formula $\gamma_q(d,m)$ of Rentería and Tapia-Recillas [24, Proposition 12]. They proved it using an ideal-theoretic approach and the notion of Hilbert functions. (See also [9, Corollary 3.9 (b)], where Carvalho, Neumann, and Lopez derive the same formula from a more general result on projective nested

cartesian codes.) Moreover, [24, Lemma 9] implies that $\gamma_q(d, m)$ can be related to the dimensions of certain Reed-Muller codes. We show below that the notion of projective reduction can also be used to give a short direct proof of the formula of Rentería and Tapia-Recillas for the dimension of $\mathsf{PRM}_q(d, m)$.

Recall that we had defined the Reed-Muller code $\mathrm{RM}_q(\nu, m)$ for any $\nu \in \mathbb{Z}$ with $0 \le \nu \le m(q-1)$. We shall find it convenient to extend this definition a bit so as to set $\mathrm{RM}_q(0,0)$ to be the 1-dimensional code of length 1, namely, $\mathbb{F}_q$. This is consistent with the formula (1) given earlier, namely,

$$\rho_q(\nu, m) := \dim \mathrm{RM}_q(\nu, m) = \sum_{j=0}^{m} (-1)^j \binom{m}{j} \binom{m + \nu - jq}{m}$$

and also with convention $\rho_q(0,0) := 1$, which was stated earlier.

Theorem 6.4. *The dimension of the code* $\mathsf{PRM}_q(d, m)$ *is given by*

$$\sum_{i=0}^{m} \rho_q(d-1, i) = \sum_{i=0}^{m} \sum_{j=0}^{i} (-1)^j \binom{i}{j} \binom{i + d - 1 - jq}{i} = \gamma_q(d, m). \qquad (28)$$

Proof. Let E be the set of all $(m+1)$-tuples of nonnegative integers whose sum is equal to d. For $\mathbf{a} = (a_0, \dots, a_m) \in E$, let $\ell(\mathbf{a}) := \max\{j \in \{0, 1, \dots, m\} : a_j > 0\}$. Note that this is well-defined since $d \ge 1$. Define

$$B := \{\mathbf{a} = (a_0, \dots, a_m) \in E : a_j < q \text{ for } 0 \le j < \ell(\mathbf{a})\}.$$

It is clear from Lemma 2.1 that $\dim \mathsf{PRM}_q(d, m) = |B|$. Now observe that

$$B = \coprod_{i=0}^{m} B_i \quad \text{where for } 0 \le i \le m, \quad B_i := \{\mathbf{a} \in B : \ell(\mathbf{a}) = i\}.$$

For $i \in \{0, 1, \dots, m\}$, the map $\mathbf{a} \mapsto (a_0, \dots, a_{i-1})$ is readily seen to be a bijection of B_i onto the set of exponent vectors of reduced monomials in i variables of degree $\le d - 1$; consequently, $|B_i| = \rho_q(d-1, i)$. This yields the desired formula. $\qquad \square$

Finally, we give a direct proof of the equivalence of the dimension formulas of Sørensen and Rentería–Tapia-Recillas.

Proposition 6.5. $\alpha_q(d, m) = \gamma_q(d, m)$.

Proof. First, note that (18) can be written in the notation of Lemma 6.1 as

$$\alpha_q(d, m) = \sum_{\substack{e=1 \\ e \equiv d \pmod{q-1}}}^{d} N(e, m+1, q-1). \qquad (29)$$

Fix any $e \in \{1, \dots, d\}$. Then $N(e, m+1, q-1)$ is the number of reduced monomials of degree e in $m+1$ variables $x_0, \dots, x_m$. Given such a reduced monomial, if x_i is the last variable appearing in it, then it must be of the form $\mu\, x_i^{j_i}$, where $1 \le j_i \le q-1$ and μ is a reduced monomial in $x_0, \dots, x_{i-1}$ of degree $e - j_i$. Note that the degree $e - j_i$ of μ satisfies $e - q + 1 \le e - j_i \le e - 1$. Conversely, any reduced monomial in $x_0, \dots, x_{i-1}$ of degree a, where $e - q + 1 \le a \le e - 1$, would give rise (upon multiplication by x_i^{e-a}) to a unique reduced monomial of degree e in $x_0, \dots, x_i$

with a positive exponent for x_i. Thus partitioning reduced monomials of degree e in $x_0, \ldots, x_m$ by the last variable appearing in them, we see that

$$N(e, m+1, q-1) = \sum_{i=0}^{m} \left(\rho_q(e-1, i) - \rho_q(e-q, i) \right).$$

On the other hand, since $d = t(q-1) + s + 1$ with $0 \leq t \leq m$ and $0 \leq s < q-1$, the parameter e in the summation in (29) takes values of the form $r(q-1) + s + 1$, where r ranges from 0 to t. Thus, we see that

$$\alpha_q(d, m) = \sum_{r=0}^{t} N(r(q-1) + s + 1, m+1, q-1) = \sum_{r=0}^{t} \sum_{i=0}^{m} \left(A(r, i) - A(r-1, i) \right),$$

where $A(k, i) := \rho_q(k(q-1) + s, i)$ for $-1 \leq k \leq t$ and $0 \leq i \leq m$. Now, by interchanging the summations over i and r, and then observing that the inner sum is telescoping, and moreover, $A(-1, i) = 0$, we obtain

$$\alpha_q(d, m) = \sum_{i=0}^{m} A(t, i) = \sum_{i=0}^{m} \rho_q(d-1, i).$$

This proves that $\alpha_q(d, m) = \gamma_q(d, m)$. $\qquad\square$

Appendix A. Quercia's proof of equivalence of dimension formulas. Here we reproduce Michel Quercia's original proof of the equivalence of the formulas, due to Sørensen and Mercier-Rolland, for the dimension of projective Reed-Muller codes. We use notations consistent with this article.

Proposition A.1 (Quercia). *Let q be a prime power and let d, m be positive integers such that $d \leq m(q-1) + 1$. Also, let $\alpha_q(d, m)$ and $\beta_q(d, m)$ be given by (18) and (19), respectively. Then $\alpha_q(d, m) = \beta_q(d, m)$.*

Proof. As in the proof of Proposition 6.3, the assertion $\alpha_q(d, m) = \beta_q(d, m)$ is equivalent to the equality

$$\sum_{j=0}^{m+1} (-1)^j \binom{m+1}{j} \sum_{\substack{e \equiv d \pmod{q-1} \\ 0 < e \leq d + (j-1)(q-1)}} \binom{e - jq + m}{e - jq} = 0. \tag{30}$$

Define

$$c := \sum_{j=0}^{m+1} (-1)^j \binom{m+1}{j} \sum_{\substack{e \equiv d \pmod{q-1} \\ -\infty < e \leq d + (j-1)(q-1)}} \binom{e - jq + m}{e - jq}. \tag{31}$$

Observe that the expression on the left in (30) is equal to $c - 1$ if d is a multiple of $q - 1$, and is equal to c otherwise. Thus it is enough to show that $c = 1$ if d is

a multiple of $q - 1$ and $c = 0$ if d is not a multiple of $q - 1$. We use a functional approach to prove this.

Let $\mathcal{E}$ be the $\mathbb{Z}$-module of the sequences $u = (u_n)_{n \in \mathbb{Z}}$ which take integer values and vanish in the vicinity of $-\infty$ (i.e., for each $u = (u_n)_{n \in \mathbb{Z}} \in \mathcal{E}$, there is $n_0 \in \mathbb{Z}$ such that $u_n = 0$ for all $n \in \mathbb{Z}$ with $n < n_0$). Denote by I the identity mapping of $\mathcal{E}$ and T the transfer operator defined by

$$(Tu)_n = u_{n+1} \quad \text{for } n \in \mathbb{Z}.$$

The sequence $u^{(m)}$, defined by

$$(u^{(m)})_n = \binom{n + m}{n} \quad \text{for } n \in \mathbb{Z},$$

belongs to $\mathcal{E}$ and the number c as defined in (31) is the term with index 0 of the sequence $x = Lu^{(m)}$ where

$$L = \sum_{j=0}^{m+1} (-1)^j \binom{m+1}{j} \sum_{\substack{e \equiv d \pmod{q-1} \\ -\infty < e \leq d+(j-1)(q-1)}} T^{e-jq}.$$

Note that the above series has a value as an $\mathcal{E}$-endomorphism. Define

$$\Delta := \sum_{k \leq 0} T^{k(q-1)} = (I - T^{-q+1})^{-1}.$$

Then

$$\begin{aligned}
L &= \sum_{j=0}^{m+1} (-1)^j \binom{m+1}{j} T^{d+(j-1)(q-1)-jq} \Delta \\
&= \sum_{j=0}^{m+1} (-1)^j \binom{m+1}{j} T^{d-j-q+1} \Delta \\
&= T^{d-q+1} \Delta (I - T^{-1})^{m+1}
\end{aligned}$$

On the other hand, $(I - T^{-1})u^{(m)} = u^{(m-1)}$. This implies that

$$(I - T^{-1})^{m+1} u^{(m)} = u^{(-1)},$$

where $u^{(-1)}$ is the sequence belonging to $\mathcal{E}$ defined by

$$(u^{(-1)})_0 = 1 \quad \text{and} \quad (u^{(-1)})_n = 0 \text{ if } n \in \mathbb{Z} \text{ with } n \neq 0.$$

Thus $x = Lu^{(m)} = T^{d-q+1} \Delta u^{(-1)}$ is given by

$$x_n = \begin{cases} 1 & \text{if } n \equiv -d \pmod{q-1} \text{ and } n > -d, \\ 0 & \text{otherwise.} \end{cases}$$

Considering x_0, we obtain the desired result. $\qquad\qquad\square$

REFERENCES

[1] E. F. Assmus Jr. and J. D. Key, *Designs and their Codes*, Cambridge Tracts in Math., **103**, Cambridge Univ. Press, 1992.

[2] S. Ballet and R. Rolland, On low weight codewords of generalized affine and projective Reed-Muller codes, *Des. Codes Cryptogr.*, **73** (2014), 271-297.

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

[4] 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), 47-63.

[5] P. Beelen, M. Datta and S. R. Ghorpade, A combinatorial approach to the number of solutions of systems of homogeneous polynomial equations over finite fields, *Moscow Math J.*, **22** (2022), 565-593.

[6] T. Berger, Automorphism groups of homogeneous and projective Reed-Muller codes, *IEEE Trans. Inform. Theory*, **48** (2002), 1035-1045.

[7] T. Berger and P. Charpin, The automorphism group of generalized Reed-Muller codes, *Discrete Math.*, **117** (1993), 1-17.

[8] M. B. Can, R. Joshua and G. V. Ravindra, Higher Grassmann codes II, *Finite Fields Appl.*, **89** (2023), Art. 102211, 21 pp.

[9] C. Carvalho, V. G. L. Neumann and H. H. Lopez, Projective nested cartesian codes, *Bull. Braz. Math. Soc.*, **48** (2017), 283-302.

[10] P. Delsarte, J. M. Goethals and F. J. MacWilliams, On generalized Reed-Muller codes and their relatives, *Information and Control*, **16** (1970), 403-442.

[11] S. R. Ghorpade, A note on Nullstellensatz over finite fields, in *Contributions in Algebra and Algebraic Geometry* (Aurangabad, 2017), *Contemp. Math.*, **738**, Amer. Math. Soc., Providence, 2019, 23-32.

[12] S. R. Ghorpade and R. Ludhani, On the purity of resolutions of Stanley-Reisner rings associated to Reed-Muller codes, in: *Algebra and Related Topics with Applications* (Aligarh, 2019), *Springer Proc. Math. Stat.*, **392**, Springer, Singapore, 2022, 325-335.

[13] S. R. Ghorpade, C. Ritzenthaler, F. Rodier and M. A. Tsfasman, Arithmetic, geometry, and coding theory: Homage to Gilles Lachaud, *Arithmetic, Geometry, Cryptography and Coding Theory, Contemp. Math.*, **770**, Amer. Math. Soc., Providence, 2021, 131-150.

[14] P. Heijnen and R. Pellikaan, Generalized Hamming weights of q-ary Reed-Muller codes, *IEEE Trans. Inform. Theory*, **44** (1998), 181-196.

[15] N. Kaplan and V. Matei, Counting plane cubic curves over finite fields with a prescribed number of rational intersection points, *Eur. J. Math.*, **7** (2021), 1137-1181.

[16] T. Kasami, S. Lin and W. W. Peterson, New generalization of the Reed-Muller codes–Part I: Primitive Codes, *IEEE Trans. Inform. Theory*, **IT-14** (1968), 189-199.

[17] G. Lachaud, Projective Reed-Muller codes, in *Coding Theory and Applications* (Cachan, 1986), Lecture Notes in Comput. Sci., **311**, Springer, Berlin, 1988, 125-129.

[18] G. Lachaud, The parameters of projective Reed-Muller codes, *Discrete Math.*, **81** (1990), 217-221.

[19] E. Leducq, A new proof of Delsarte, Goethals and MacWilliams theorem on minimal weight codewords of generalized Reed-Muller codes, *Finite Fields Appl.*, **18** (2012), 581-586.

[20] 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), 227-240.

[21] D. E. Muller, Application of Boolean algebra to switching circuit design and to error detection, *IRE Trans. Electron. Comput.*, **EC-3** (1954), 6-12.

[22] I. S. Reed, A class of multiple-error-correcting codes and the decoding scheme, *Trans. IRE*, (1954), 38-49.

[23] I. S. Reed, A brief history of the development of error correcting codes, *Comput. Math. Appl.*, **39** (2000), 89-93.

[24] C. Rentería and H. Tapia-Recillas, Reed-muller codes: An ideal theory approach, *Comm. Algebra*, **25** (1997), 401-413.

[25] R. Rolland, Number of points of non-absolutely irreducible hypersurfaces, in *Algebraic Geometry and its Applications* (Papette, 2007), Ser. Number Theory Appl., **5**, World Scientific, Singapore, 2008, 481-487.

[26] J.-P. Serre, Lettre à M. Tsfasman, in *Journées Arithmétiques* (Luminy, 1989), *Astérisque*, **198-199-200** (1991), 351-353.

[27] A. B. Sørensen, Projective Reed-Muller codes, *IEEE Trans. Inform. Theory*, **37** (1991), 1567-1576.

[28] S. G. Vlèduts and Yu. I. Manin, Linear codes and modular curves, *J. Sov. Math.*, **30** (1985), 2611-2643.