Generalized Hamming weights of q -ary Reed-Muller codes

Petra Heijnen and Ruud Pellikaan *

Appeared in *IEEE Trans. Inform. Theory*,
vol. 44, pp. 181-196, Jan. 1998.

Abstract The order bound on generalized Hamming weights is introduced in a general setting of codes on varieties which comprises both the one point geometric Goppa codes as the q -ary Reed-Muller codes. For the latter codes it is shown that this bound is sharp and that they satisfy the double chain condition.

1 Introduction

In terms of polynomials the problem of finding the generalized Hamming weights of q -ary Reed-Muller codes is equivalent to Problem 7.1 of [39]:

Let $f_1, \dots, f_r$ be linearly independent polynomials in m variables of degree u or less with coefficients in $\mathbb{F}_q$, the finite field of q elements.

What is the maximum possible number of solutions in $\mathbb{F}_q^m$ of the system $f_1 = \dots = f_r = 0$?

Let $n = q^m$. Let $P_1, \dots, P_n$ be an enumeration of the points of $\mathbb{F}_q^m$. The ring of polynomials in m variables with coefficients in $\mathbb{F}_q$ is denoted by $\mathbb{F}_q[X_1, \dots, X_m]$. Consider the evaluation map

$$ev : \mathbb{F}_q[X_1, \dots, X_m] \longrightarrow \mathbb{F}_q^n$$

---

*Both authors are from the Department of Mathematics and Computing Science, Eindhoven University of Technology, P.O. Box 513, 5600 MB Eindhoven, The Netherlands.

defined by $ev(f) = (f(P_1), \dots, f(P_n))$. The q -ary Reed-Muller (RM) code $\mathcal{RM}_q(u, m)$ of order u in m variables is the image of this evaluation map of all polynomials of degree u or less. The polynomials which evaluate to the zero word form the ideal generated by $X_i^q - X_i$ for $i = 1, \dots, m$. If the polynomial f is evaluated to the word $\mathbf{c}$, then the number of zeros of f in $\mathbb{F}_q^m$ is equal to $n - wt(\mathbf{c})$. If the polynomials $f_1, \dots, f_r$ are evaluated to the words $\mathbf{c}_1, \dots, \mathbf{c}_r$, then the number of common zeros of these polynomials is equal to n minus the size of the support of the linear code generated by $\mathbf{c}_1, \dots, \mathbf{c}_r$. The *support* of a code C is defined by

$$\text{supp}(C) = \{i : c_i \neq 0 \text{ for some } \mathbf{c} \in C\}.$$

The *support weight* or *effective length* of C is the number of elements of its support.

The r th *generalized Hamming weight* (GHW) or r th *minimum support weight* of a linear code C is defined by

$$d_r(C) = \min\{|\text{supp}(D)| : D \text{ is a linear subcode of } C \text{ and } \dim(D) = r\}.$$

The RM codes were defined in [32, 28] for the binary case and this was generalized to arbitrary q in [7, 18, 43].

Generalized Hamming weights were introduced in the study [15, 24] on the weight distribution of codes over extensions of $\mathbb{F}_q$. The concept was rediscovered in [41] where the problem of the GHW's of the binary RM codes was solved. In [1] the GHW's of the ternary RM codes was computed. An equivalent definition was found for projective systems in projective space in [38, 39]. The generalized weight enumerator was defined in [25] and a Macwilliams identity was proved in [34].

The connection between the trellis or state complexity of a code and its GHW's was made in [20, 21]. The sequence of GHW's is called the *length/dimension profile* (LDP) in [13]. The inverse function is called the *dimension/length profile* (DLP). The DLP bound on the state complexity becomes an equality if the code satisfies the double chain condition [8, 14, 20, 42].

A code C satisfies the *chain condition* if there is an increasing sequence (D_r) of subcodes of C such that $D_r \subset D_{r+1}$, $\dim(D_r) = r$ and the effective length of D_r is $d_r(C)$ for all r . Or equivalently, there exists a permutation of the coordinates and there is an increasing sequence (D_r) of subcodes of C such that $D_r \subset D_{r+1}$, $\dim(D_r) = r$ and $\text{supp}(D_r) = \{1, 2, \dots, d_r\}$ for all r .

A code C satisfies the *two way* or *double chain condition* if there exists a permutation of the coordinates and there are increasing sequences (D_r^L) and (D_r^R) of subcodes of C such that $D_r^L \subset D_{r+1}^L$, $\dim(D_r^L) = r$ and such that $D_r^R \subset D_{r+1}^R$, $\dim(D_r^R) = r$ and $\text{supp}(D_r^L) = \{1, 2, \dots, d_r\}$ and $\text{supp}(D_r^R) = \{n+1-d_r, n+2-d_r, \dots, n\}$ for all r .

A general setting will be given where our method applies. This is taken from [16] and originates from [11, 12]. Consider a geometric object $\mathcal{X}$ with a subset $\mathcal{P}$ consisting of n points which are enumerated by $P_1, \dots, P_n$. Suppose that we have a vector space L over $\mathbb{F}_q$ of functions on $\mathcal{X}$ such that $f(P_i) \in \mathbb{F}_q$ for all i and $f \in L$. In this way one has an evaluation map

$$ev_{\mathcal{P}} : L \longrightarrow \mathbb{F}_q^n$$

which is defined by $ev_{\mathcal{P}}(f) = (f(P_1), \dots, f(P_n))$. If this evaluation map is linear, then its image E and its dual C are linear codes. The notion of an order function on the space of functions on $\mathcal{X}$ gives sequences of vector spaces $L(l)$, evaluation codes $E(l)$ and their duals $C(l)$, where l is a parameter denoting the dimension of $L(l)$. These codes comprise the one point geometric Goppa codes and the RM codes. In the first case $\mathcal{X}$ is an algebraic curve defined over $\mathbb{F}_q$, $\mathcal{P}$ is a set of rational points on $\mathcal{X}$ and L is a vector space of rational functions which have only poles at a fixed point P with an upper bound on the pole order at P . In the second case $\mathcal{X}$ is the affine space of dimension m , $\mathcal{P}$ is the set of all q^m rational points of $\mathcal{X}$ and L is the vector space of all polynomials in m variables with coefficients in $\mathbb{F}_q$ of degree at most u .

The decoding of these codes can be done by majority voting of unknown syndromes [10, 12, 16, 17, 30].

In this paper the order bound on the generalized Hamming weights is defined and in detail studied for the RM codes over all finite fields. It turns out that the order bound is sharp in this case. The shift bound as defined in [30] is tight for the minimum distance of RM codes but does not give the right answer for the higher Hamming weights.

A direct consequence of our methods is that the RM codes satisfy the double chain condition. This gives the state complexity of these codes as done in the binary case by [20, 21].

In Section 2 the definition of an order function is given. The order bound on the generalized Hamming weights is given in Section 3. The theory is applied to Reed-Muller codes in Section 4. Some combinatorics of extremal poset theory is applied to get a formula for the higher weights of RM codes in Section 5. Another formula is derived in Section 6. We conclude with some remarks and open problems.

2 Order functions and higher weights

In this section the notion of an order function will be defined. It has its origin in valuation theory [9] and the theory of *Gröbner bases* [4, 6].

In this paper $\mathbb{F}$ denotes a field, $\mathbb{F}_q$ the finite field with q elements. An $\mathbb{F}$ -algebra will be a commutative ring with a unit that contains $\mathbb{F}$ as a unitary subring. $\mathbb{N}$ denotes the positive integers and $\mathbb{N}_0$ the nonnegative integers.

The dimension of polynomials in one variable of degree at most d is equal to $d + 1$. This is no longer the case for polynomials in several variables. Decreasing sequences of codes $(C(l) \mid l \in \mathbb{N})$ will be introduced. The code $C(l)$ is defined by parity checks with words that are evaluations of functions in a certain $\mathbb{F}_q$ -algebra of a given order. For inductive arguments for bounds on the generalized Hamming weights it is necessary that the dimension of $C(l)$ is at most one more than the dimension of $C(l + 1)$.

A way to obtain this objective for the ring of polynomials in two variables is to define the order by looking at the degree firstly and the lexicographic order on the exponents (i, j) of the monomial $X^i Y^j$ secondly. This order $\prec$ looks like

$$1 \prec Y \prec X \prec Y^2 \prec XY \prec X^2 \prec Y^3 \prec XY^2 \dots$$

Notice that this order respects multiplication of monomials. This is formalized as follows.

Definition 2.1 Let $R = \mathbb{F}[X_1, \dots, X_m]$. Suppose that $\prec$ is a total order on the set of monomials in the variables $X_1, \dots, X_m$ such that for all monomials M_1, M_2 , and M the following holds

- (R.1) If $M \neq 1$, then $1 \prec M$,
- (R.2) If $M_1 \prec M_2$, then $MM_1 \prec MM_2$.

Then $\prec$ is called a *reduction, term* or *admissible* order on the monomials [4, 6].

The multi-index notation is used for monomials. That means $X^\alpha = \prod_{s=1}^m X_s^{\alpha_s}$ if $\alpha = (\alpha_1, \dots, \alpha_m)$. The degree of X^α and α is defined by

$$\deg(X^\alpha) = \deg(\alpha) = \sum_{s=1}^m \alpha_s.$$

Giving a reduction order on monomials in m variables is the same as giving a total order on $\mathbb{N}_0^m$ such that, for all α_1, α_2 , and α in $\mathbb{N}_0^m$, the following holds

- (E.1) If $\alpha \neq 0$, then $0 \prec \alpha$,
- (E.2) If $\alpha_1 \prec \alpha_2$, then $\alpha + \alpha_1 \prec \alpha + \alpha_2$.

We use $\prec$ both for monomials and exponents.

Example 2.2 The *lexicographic order* $\prec_L$ is defined by

$$X^\alpha \prec_L X^\beta \Leftrightarrow \alpha_1 = \beta_1, \dots, \alpha_{l-1} = \beta_{l-1} \text{ and } \alpha_l < \beta_l \text{ for some } l.$$

The lexicographic order is a reduction order. See [6]. For $m = 2$ with $X = X_1$ and $Y = X_2$ the start of the lexicographic order looks like

$$\begin{array}{cccccccccccccccc} 1 & \prec & Y & \prec & Y^2 & \prec & \dots & \prec & Y^j & \prec & Y^{j+1} & \prec & \dots \\ X & \prec & XY & \prec & XY^2 & \prec & \dots & \prec & XY^j & \prec & XY^{j+1} & \prec & \dots \\ X^2 & \prec & \dots & & & & & & & & & & \end{array}$$

Hence X^{i+1} is the supremum of the set $\{X^i Y^j \mid j \in \mathbb{N}_0\}$. If $m \geq 2$, then the lexicographic order is not isomorphic with the positive integers.

Example 2.3 The *graded lexicographic order* $\prec_D$ is defined by

$$X^\alpha \prec_D X^\beta \Leftrightarrow \deg(X^\alpha) < \deg(X^\beta) \text{ or } \deg(X^\alpha) = \deg(X^\beta), X^\alpha \prec_L X^\beta.$$

The graded lexicographic order is a reduction order [6] which is isomorphic with the positive integers. This section started with the two variable case as an example.

The order is extended to a function on all polynomials in the following way. Let $\prec$ be a reduction order which is isomorphic with the positive integers.

Let $f_1, f_2, \dots$ be an enumeration of the set of monomials such that $f_i \prec f_{i+1}$ for all i . The monomials are a basis of $\mathbb{F}[X_1, \dots, X_m]$ over $\mathbb{F}$. Hence every nonzero polynomial f can be written in a unique way as

$$f = \sum_{i=1}^j \lambda_i f_i,$$

where $\lambda_i \in \mathbb{F}$ for all i , and $\lambda_j \neq 0$. Then f_j is called the *leading monomial* of f . Define a function

$$\rho : \mathbb{F}[X_1, \dots, X_m] \longrightarrow \mathbb{N}_0 \cup \{-\infty\},$$

by $\rho(0) = -\infty$ and $\rho(f) = j - 1$ where j is the smallest positive integer such that f can be written as a linear combination of the first j monomials. It is not difficult to show that ρ satisfies the following conditions

- (O.0) $\rho(f) = -\infty$ if and only if $f = 0$
- (O.1) $\rho(\lambda f) = \rho(f)$ for all nonzero $\lambda \in \mathbb{F}$
- (O.2) $\rho(f + g) \leq \max\{\rho(f), \rho(g)\}$
and equality holds when $\rho(f) < \rho(g)$.
- (O.3) If $\rho(f) < \rho(g)$ and $h \neq 0$, then $\rho(fh) < \rho(gh)$
- (O.4) If $\rho(f) = \rho(g)$, then there exists a nonzero $\lambda \in \mathbb{F}$ such that $\rho(f - \lambda g) < \rho(g)$.

for all $f, g, h \in R$. Here $-\infty < n$ for all $n \in \mathbb{N}_0$. The properties of the function ρ are captured in the following definition.

Definition 2.4 Let R be an $\mathbb{F}$ -algebra. An *order function* on R is a map

$$\rho : R \longrightarrow \mathbb{N}_0 \cup \{-\infty\},$$

that satisfies conditions (O.0), $\dots$, (O.4).

3 The order bound on the generalized weights

In this section a sequence $(C(l) : l \in \mathbb{N})$ of codes is defined by means of an $\mathbb{F}_q$ -algebra R together with an order function ρ on R and a morphism of $\mathbb{F}_q$ -algebras $\varphi : R \rightarrow \mathbb{F}_q^n$. The order bound $d_r(l)$ is defined and it is shown

that it is a lower bound on the r th generalized Hamming weight of $C(l)$.

Let R be an $\mathbb{F}_q$ -algebra with an order function ρ . So let $\{f_i : i \in \mathbb{N}\}$ be a basis of R over $\mathbb{F}_q$ such that $\rho(f_i) < \rho(f_{i+1})$ for all $i \in \mathbb{N}$, and for all nonzero $f \in R$ there exists a j with $\rho(f) = \rho(f_j)$. The existence of such a basis can be shown in general [16, 30], but this fact is not needed in this paper since we specialize to the ring $R = \mathbb{F}_q[X_1, \dots, X_m]$ which has a basis of monomials with the above mentioned property. Let $L(l)$ be the vector space generated by $f_1, \dots, f_l$. Hence for all nonzero $f \in R$ we have that $\rho(f) = \rho(f_l)$ if and only if l is the smallest integer such that $f \in L(l)$. Let $l(i, j)$ be the smallest positive integer l such that $f_i f_j \in L(l)$. So $l(i, j) < l(i+1, j)$ for all $i, j \in \mathbb{N}$.

The standard innerproduct is defined by $\mathbf{a} \cdot \mathbf{b} = \sum a_i b_i$ for $\mathbf{a} = (a_1, \dots, a_n)$ and $\mathbf{b} = (b_1, \dots, b_n)$. The coordinatewise multiplication $*$ on $\mathbb{F}_q^n$ is defined by $\mathbf{a} * \mathbf{b} = (a_1 b_1, \dots, a_n b_n)$. The vector space $\mathbb{F}_q^n$ becomes an $\mathbb{F}_q$ -algebra with this multiplication.

Let

$$\varphi : R \longrightarrow \mathbb{F}_q^n,$$

be a morphism of $\mathbb{F}_q$ -algebras, that means φ is $\mathbb{F}$ -linear and

$$\varphi(fg) = \varphi(f) * \varphi(g).$$

Let $\mathbf{h}_i = \varphi(f_i)$. Define

$$C(l) = \{\mathbf{c} \in \mathbb{F}_q^n : \mathbf{c} \cdot \mathbf{h}_i = 0 \text{ for all } i \leq l\}.$$

In this paper only those algebra morphisms φ will be considered that are *surjective*. Then there exists an N such that $\mathbf{h}_1, \dots, \mathbf{h}_N$ generate $\mathbb{F}_q^n$. Hence $C(l) = 0$ for all $l \geq N$.

Definition 3.1 Let $\mathbf{y} \in \mathbb{F}_q^n$. Consider the *syndromes*

$$s_i(\mathbf{y}) = \mathbf{y} \cdot \mathbf{h}_i \quad \text{and} \quad s_{ij}(\mathbf{y}) = \mathbf{y} \cdot (\mathbf{h}_i * \mathbf{h}_j).$$

Then $S(\mathbf{y}) = (s_{ij}(\mathbf{y}) : 1 \leq i, j \leq N)$ is the *matrix of syndromes* of $\mathbf{y}$.

Lemma 3.2 Let $\mathbf{y} \in \mathbb{F}_q^n$. Let $D(\mathbf{y})$ be the $n \times n$ diagonal matrix with $\mathbf{y}$ on the diagonal. Let H be the $N \times n$ matrix with $\mathbf{h}_i$ on the i th row. Then

$$S(\mathbf{y}) = HD(\mathbf{y})H^T,$$

Proof. The matrix of syndromes $S(\mathbf{y})$ is equal to $HD(\mathbf{y})H^T$, since

$$s_{ij}(\mathbf{y}) = \mathbf{y} \cdot (\mathbf{h}_i * \mathbf{h}_j) = \sum_{l=1}^n y_l h_{il} h_{jl},$$

where h_{il} is the l th entry of $\mathbf{h}_i$. □

Definition 3.3 We define the *image of S* with respect to U as

$$Im(S, U) = \{\mathbf{y} \in \mathbb{F}_q^N : \text{there exist } \mathbf{u} \in U \text{ and } \mathbf{x} \in \mathbb{F}_q^N \text{ such that } \mathbf{x}S(\mathbf{u}) = \mathbf{y}\}$$

and its linear span is denoted by $Im^*(S, U)$. The *image of D* with respect to U is defined by

$$Im(D, U) = \{\mathbf{w} \in \mathbb{F}_q^n : \text{there exist } \mathbf{u} \in U \text{ and } \mathbf{v} \in \mathbb{F}_q^n \text{ such that } \mathbf{v}D(\mathbf{u}) = \mathbf{w}\}$$

and its linear span is denoted by $Im^*(D, U)$.

Remark 3.4 The images $Im(S, U)$ and $Im(D, U)$ are in general not linear spaces. Take for instance $q = 2$ and $U = \langle (1, 1, 0), (0, 1, 1) \rangle$. Then $Im(D, U) = \mathbb{F}_2^3 \setminus \{(1, 1, 1)\}$.

Lemma 3.5

- 1) $Im^*(S, U) \cong Im^*(D, U)$,
- 2) $Im^*(D, U) = \langle \mathbf{e}_j : j \in \text{supp}(U) \rangle$,
- 3) $\dim(Im^*(S, U)) = |\text{supp}(U)|$.

Proof.

1) Consider the linear map $\eta : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^N$ with matrix H^T , so $\eta(\mathbf{w}) = \mathbf{w}H^T$. We claim that $\eta(Im(D, U)) = Im(S, U)$.

Let $\mathbf{w} \in Im(D, U)$, then there exists a $\mathbf{v} \in \mathbb{F}_q^n$ such that $\mathbf{w} = \mathbf{v}D(\mathbf{u})$. The rows of H generate $\mathbb{F}_q^n$, since φ is surjective. So $\mathbf{v} = \mathbf{x}H$ for some $\mathbf{x} \in \mathbb{F}_q^N$. Hence $\eta(\mathbf{w}) = \mathbf{w}H^T = \mathbf{v}D(\mathbf{u})H^T = \mathbf{x}HD(\mathbf{u})H^T = \mathbf{x}S(\mathbf{u}) \in Im(S, U)$, where the last equality is stated in Lemma 3.2.

Suppose $\mathbf{y} \in Im(S, U)$. Then there exists an $\mathbf{x} \in \mathbb{F}_q^N$ and a $\mathbf{u} \in U$ such that $\mathbf{y} = \mathbf{x}S(\mathbf{u})$. We can write $S(\mathbf{u}) = HD(\mathbf{u})H^T$, so $\mathbf{y} = \mathbf{x}HD(\mathbf{u})H^T$. Let $\mathbf{v} = \mathbf{x}H$, then $\mathbf{v} \in \mathbb{F}_q^n$. Let $\mathbf{w} = \mathbf{v}D(\mathbf{u})$, then $\mathbf{w} \in Im(D, U)$ and $\eta(\mathbf{w}) = \mathbf{w}H^T = \mathbf{y}$. This proves the claim.

The map η is injective, since H has rank n . Therefore $Im^*(S, U) \cong Im^*(D, U)$ under η .

2) Let $\mathbf{y} \in \text{Im}(D, U)$. Then there is a $\mathbf{u} \in U$ and an $\mathbf{x} \in \mathbb{F}_q^n$, such that $\mathbf{y} = D(\mathbf{u})\mathbf{x} = \mathbf{u} * \mathbf{x}$. So $y_j = u_j x_j$, and $y_j = 0$ if $j \notin \text{supp}(U)$. Hence $\langle \mathbf{e}_j : j \in \text{supp}(U) \rangle$ is a basis of $\text{Im}^*(D, U)$, where $\mathbf{e}_j$ is the j th standard basis vector of length n , that is to say the i th coordinate of $\mathbf{e}_j$ is one if $i = j$ and zero otherwise.

3) This follows directly from 1) and 2). $\square$

Remark 3.6 One can show that $\text{Im}(D, U) = \text{Im}^*(D, U)$ and $\text{Im}(S, U) = \text{Im}^*(S, U)$ if $q > |\text{supp}(U)|$.

Lemma 3.7 Let U be a linear subspace of $C(l)$ of dimension r with $r > 0$. Then there exists a unique r -tuple $(l_1, \dots, l_r)$ such that $l \leq l_1 < \dots < l_r < N$ and $\dim(U \cap C(l_i + 1)) = \dim(U \cap C(l_i)) - 1$ for $i = 1, \dots, r$.

Proof. Let $U(m) = U \cap C(m)$. Then $(U(m) : m \in \mathbb{N})$ is a decreasing chain of subspaces of U . Furthermore $U(l) = U$ has dimension $r > 0$, $U(m) = 0$ for $m \geq N$ and

$$\dim U(m) - 1 \leq \dim U(m + 1) \leq \dim U(m).$$

So there are exactly r values for m such that $l \leq m < N$ and $\dim U(m + 1) = \dim U(m) - 1$, which are denoted by $l_1 < \dots < l_r$. $\square$

Definition 3.8 The $(l_1, \dots, l_r)$ is called the *associated r -tuple* of the subspace U of $C(l)$ of dimension r .

Definition 3.9 Define the sets $N(l)$ and $A(l)$ by

$$\begin{aligned} N(l) &= \{(i, j) \in \mathbb{N}^2 : l(i, j) = l + 1\}, \\ A(l) &= \{i \in \mathbb{N} : l(i, j) = l + 1 \text{ for some } j\}. \end{aligned}$$

Define for $l_1 < \dots < l_r$ the set $A(l_1, \dots, l_r)$ by

$$A(l_1, \dots, l_r) = \cup_{t=1}^r A(l_t).$$

Let $a(l_1, \dots, l_r)$ denote the number of elements of $A(l_1, \dots, l_r)$.

Lemma 3.10

- 1) If $\mathbf{y} \in C(l)$ and $l(i, j) \leq l$, then $s_{ij}(\mathbf{y}) = 0$.
- 2) If $\mathbf{y} \in C(l) \setminus C(l + 1)$ and $l(i, j) = l + 1$, then $s_{ij}(\mathbf{y}) \neq 0$.

Proof.

1) Let $\mathbf{y} \in C(l)$. If $l(i, j) \leq l$, then $f_i f_j \in L(l)$. So $\mathbf{h}_i * \mathbf{h}_j = \varphi(f_i f_j)$ is an element of $\varphi(L(l))$, which is the dual of $C(l)$. Hence $s_{ij}(\mathbf{y}) = \mathbf{y} \cdot (\mathbf{h}_i * \mathbf{h}_j) = 0$.
2) Let $\mathbf{y} \in C(l) \setminus C(l+1)$. If $l(i, j) = l+1$, then $f_i f_j \in L(l+1) \setminus L(l)$. So $f_i f_j \equiv \mu f_{l+1}$ modulo $L(l)$ for some nonzero $\mu \in \mathbb{F}_q$. Hence $\mathbf{h}_i * \mathbf{h}_j \equiv \mu \mathbf{h}_{l+1}$ modulo $\varphi(L(l))$. Now $\mathbf{y} \notin C(l+1)$, so $s_{l+1}(\mathbf{y}) \neq 0$. Therefore $s_{ij}(\mathbf{y}) \neq 0$ $\square$

Lemma 3.11 *If $t = |N(l)|$ and $(i_1, j_1), \dots, (i_t, j_t)$ is an enumeration of the elements of $N(l)$ in increasing order with respect to the lexicographic order on $\mathbb{N}^2$, then $i_1 < \dots < i_t$ and $j_t < \dots < j_1$. In particular $N(l)$ and $A(l)$ have the same number of elements. If moreover $\mathbf{y} \in C(l) \setminus C(l+1)$, then*

$$s_{i_r j_s}(\mathbf{y}) = \begin{cases} 0 & \text{if } r < s \\ \text{not zero} & \text{if } r = s. \end{cases}$$

Proof. The sequence $(i_1, j_1), \dots, (i_t, j_t)$ is ordered in such a way that $i_1 \leq \dots \leq i_t$ and $j_r < j_{r+1}$ if $i_r = i_{r+1}$. If $i_r = i_{r+1}$, then $j_r < j_{r+1}$. So

$$l+1 = l(i_r, j_r) < l(i_r, j_{r+1}) = l(i_{r+1}, j_{r+1}) = l+1,$$

which is a contradiction. Hence the sequence $i_1, \dots, i_t$ is strictly increasing. A similar argument shows that $j_{s+1} < j_s$ for all $s < t$.

Let $\mathbf{y} \in C(l)$. If $r < s$, then $l(i_r, j_s) < l(i_s, j_s) = l+1$. Lemma 3.10 implies that $s_{i_r j_s}(\mathbf{y}) = 0$.

Moreover, let $\mathbf{y} \notin C(l+1)$. If $r = s$, then $l(i_r, j_s) = l+1$. Lemma 3.10 implies that $s_{i_r j_s}(\mathbf{y}) \neq 0$. $\square$

Proposition 3.12 *Let U be a linear subspace of $C(l)$ of dimension r with associated r -tuple $(l_1, \dots, l_r)$. Then*

$$|\text{supp}(U)| \geq a(l_1, \dots, l_r).$$

Proof. Let U be a linear subspace of $C(l)$ of dimension r . Let $\mathbf{u}_1, \dots, \mathbf{u}_r$ be a basis of U with indices $l \leq l_1 < \dots < l_r \leq N$ such that $\mathbf{u}_i \in C(l_i)$ and $\mathbf{u}_i \notin C(l_i + 1)$ for all $i = 1, \dots, r$.

Let M_k be the $a(l_k) \times N$ submatrix of $S(\mathbf{u}_k)$ with the $a(l_k)$ rows corresponding to the indices of $A(l_k)$. The matrix M_k has rank $a(l_k)$, since it has an $a(l_k) \times a(l_k)$ submatrix with nonzeros on the backdiagonal and zeros above the backdiagonal, according to Lemma 3.11.

Let M be the $\sum a(l_k) \times N$ matrix defined by

$$M = \begin{pmatrix} M_1 \\ \vdots \\ M_r \end{pmatrix}.$$

The rank of M is a lower bound of the dimension of $Im^*(S, U)$.

Apply Gaussian elimination to M with the $a(l_1)$ pivots in the rows of M_1 and the columns corresponding to $A(l_1)$. Suppose that we have found a matrix with pivots in the rows of $M_1, \dots, M_k$ and the columns corresponding to $\cup_{i=1}^k A(l_i)$. Apply Gaussian elimination with the pivots in the rows of M_{k+1} and the columns corresponding to

$$A(l_{k+1}) \setminus (\cup_{i=1}^k A(l_i)).$$

So with induction and Gaussian elimination a matrix M' is obtained from M with pivots in the columns corresponding with $\cup_{k=1}^r A(l_k)$. So M , and therefore $Im^*(S, U)$, has rank at least $a(l_1, \dots, l_r)$.

The proof is completed with Lemma 3.5. $\square$

Definition 3.13 Let $d_{ORD, \varphi, r}(l)$ be the minimal $a(l_1, \dots, l_r)$ such that $l \leq l_1 < \dots < l_r \leq N$ and $C(l_i) \neq C(l_i + 1)$ for all $i = 1, \dots, r$. It is called the *order bound* on the r th generalized Hamming weight and will be abbreviated by $d_r(l)$.

Theorem 3.14

$$d_r(C(l)) \geq d_r(l).$$

Proof. This is a direct consequence of Proposition 3.12, the definition of GHW's and Definition 3.13. $\square$

Remark 3.15 The codes $C(l)$ can be decoded by means of the scheme of majority voting of unknown syndromes which corrects $\lfloor (d_1(l) - 1)/2 \rfloor$ errors. See [10, 17, 30].

4 Reed-Muller codes

The theory of the previous section will be applied to RM codes.

Order the monomials by the graded lexicographic order. Let $\mathcal{P}$ be the set of all distinct points of $\mathbb{F}_q^m$. So, $n = q^m$ and $\mathcal{P} = \{P_1, \dots, P_n\}$. Let $\varphi(f) = (f(P_1), \dots, f(P_n))$. The map φ is a surjective morphism of $\mathbb{F}_q$ -algebras by [7, 16]. Define $\mathbf{h}_i = \varphi(f_i)$ and $C(l) = \{\mathbf{c} \in \mathbb{F}_q^n : \mathbf{c} \cdot \mathbf{h}_i = 0 \text{ for all } i \leq l\}$.

Since $\varphi(f^q) = \varphi(f)$ many of the parity checks $\mathbf{h}_i$ will be the same and therefore adding an extra parity check will not always lead to a different code. A monomial X^α is called *reduced* if $0 \leq \alpha_j \leq q-1$ for all $j, 1 \leq j \leq m$. There are exactly $q^m = n$ of these monomials. The set $\{\varphi(X^\alpha) : X^\alpha \text{ is reduced}\}$ is a basis for $\mathbb{F}_q^n$. A polynomial is called reduced if it is a linear combination of reduced monomials. For every polynomial f there exists a unique reduced polynomial $\bar{f}$ such that $\varphi(f) = \varphi(\bar{f})$.

Lemma 4.1 *Let $f \in \mathbb{F}_q[X_1, \dots, X_m]$ be reduced. Then*

$$\sum_{i=1}^n f(P_i) = \begin{cases} 0 & \text{if } \deg(f) < (q-1)m \\ \text{not zero} & \text{if } \deg(f) = (q-1)m \end{cases}$$

Proof. The proof can be found in [7, 16]. □

Consider the sequence of codes $(C(l) : l \in \mathbb{N})$. Then $C(l+1) \subseteq C(l)$, and $\dim(C(l+1)) \geq \dim(C(l)) - 1$ and $C(l) = 0$ for all $l > N$. So $\{C(l) : l \in \mathbb{N}\}$ consists of n distinct codes. Define a new sequence $(C_r)_{r=1}^n$ such that C_r has dimension $n - r$ and $C_r = C(l) \neq C(l-1)$ for some l .

Proposition 4.2

$$C_r^\perp = C_{n-r}$$

Proof. Consider the subsequence of the infinite sequence of monomials $(f_i : i \in \mathbb{N})$ consisting of all reduced monomials X^α . This new sequence is also ordered by the graded lexicographic order. Let $g_i, 1 \leq i \leq n$, be the i -th monomial within this new sequence. Then the code C_r is, by definition, equal to

$$C_r = \{\mathbf{c} \in \mathbb{F}_q^n : \mathbf{c} \cdot \varphi(g_i) = 0 \text{ for all } i \leq r\}.$$

Therefore $\varphi(g_i)$ is an element of the dual of the code C_r . We have to prove that $\varphi(g_i)$ is in C_{n-r} for all $i \leq r$. Since

$$C_{n-r} = \{ \mathbf{c} \in \mathbb{F}_q^n : \mathbf{c} \cdot \varphi(g_j) = 0 \text{ for all } j \leq n-r \}$$

this is the same as to prove that

$$\varphi(g_i) \cdot \varphi(g_j) = 0$$

for all $i \leq r$ and all $j \leq n-r$. Now

$$\varphi(g_i) \cdot \varphi(g_j) = \sum_{l=1}^n (g_i g_j)(P_l)$$

and Lemma 4.1 implies that this equals zero if the degree of $g_i g_j$ is smaller than $m(q-1)$.

Let $g_n = X^\mu = X_1^{q-1} \cdots X_m^{q-1}$. If $X^\alpha \prec X^\beta$, then $X^{\mu-\beta} \prec X^{\mu-\alpha}$ since the graded lexicographic order is a reduction order. So the sequence $g_1, g_2, \dots, g_n$ transforms into the sequence $g_n, g_{n-1}, \dots, g_1$ under the operation $X^\alpha \mapsto X^{\mu-\alpha}$ and hence $g_i g_j = g_n$ if $i+j = n+1$.

If $i \leq r$ and $j \leq n-r$ then $i+j \leq n$. Let $i' = n+1-j$. Then $i < i'$, so $g_i g_j < g_{i'} g_j = g_n$ and $\deg(g_i g_j) < \deg(g_n) = m(q-1)$. $\square$

Definition 4.3 Let $Q = \{0, 1, \dots, q-1\}$. Let $\mu = (q-1, \dots, q-1)$. Define $\alpha^\perp = \mu - \alpha$ for $\alpha \in Q^m$. Let $f_l = X^\alpha$ be reduced. Define $f_l^\perp = X^{\alpha^\perp}$.

Remark 4.4 The mapping on Q^m which sends α to $\alpha^\perp$ is a bijection which reverses the lexicographic order.

Corollary 4.5 Let $f \in \mathbb{F}_q[X_1, \dots, X_m]$ be reduced. If $f_{l+1}^\perp$ is the leading monomial of f , then $\varphi(f) \in C(l) \setminus C(l+1)$.

Proof. This is a consequence of Proposition 4.2. $\square$

Definition 4.6 The q -ary Reed-Muller code of order u and in m variables is defined by

$$\mathcal{RM}_q(u, m) = \{ \varphi(f) : f \in R, \deg(f) \leq u \}.$$

Remark 4.7 Define $u^\perp = (q-1)m - u - 1$. The dual of the code $\mathcal{RM}_q(u, m)$ is $\mathcal{RM}_q(u^\perp, m)$ by Proposition 4.2. See also [7]. So

$$\mathcal{RM}_q(u, m) = \{\mathbf{c} \in \mathbb{F}_q^m : \mathbf{c} \cdot \mathbf{h} = 0 \text{ for } \mathbf{h} = \varphi(f) \text{ and } \deg(f) \leq u^\perp\}.$$

Let l be the integer such that $f_l = X_1^{u^\perp}$. Then $f_{l+1} = X_m^{u^\perp+1}$ and $C(l) = \mathcal{RM}_q(u, m)$, since the monomials are ordered by the graded lexicographic order. It will be shown that there exists a subspace U of $\mathcal{RM}_q(u, m)$ of dimension r such that the support of U reaches the bound $d_r(l)$.

Definition 4.8 Let $Q = \{0, \dots, q-1\}$. Enumerate the elements of $\mathbb{F}_q$ by Q . So $\mathbb{F}_q = \{a_0, \dots, a_{q-1}\}$. If q is prime, then we take for a_i the residue of i modulo q . Let $\alpha \in Q^m$. Then P_α is defined by $P_\alpha = (a_{\alpha_1}, \dots, a_{\alpha_m})$.

Remark 4.9 From now on the $n = q^m$ points $P_1, \dots, P_n$ of $\mathbb{F}_q^m$ are ordered by taking the P_α with the lexicographic order on the $\alpha \in Q^m$. In this way we have identified the set $\{1, \dots, n\}$ with Q^m . Thus supports of codes in $\mathbb{F}_q^n$ will be subsets of Q^m .

Definition 4.10 Let $\alpha \in Q^m$. Define the polynomial f_α by

$$f_\alpha = \prod_{s=1}^m \prod_{\alpha_s < t \leq q-1} (X_s - a_t).$$

and the corresponding word $\mathbf{h}_\alpha = \varphi(f_\alpha)$.

Remark 4.11 For the degree of f_α we find

$$\deg(f_\alpha) = \sum_{s=1}^m (q-1 - \alpha_s) = (q-1)m - \sum_{s=1}^m \alpha_s = (q-1)m - \deg(X^\alpha).$$

So, if the degree of the monomial X^α is greater than $u^\perp$, then the degree of f_α is smaller than or equal to u and therefore $\mathbf{h}_\alpha$ is a codeword of $\mathcal{RM}_q(u, m)$.

Definition 4.12 The *partial order* $\preceq_P$ on Q^m is defined by $\alpha \preceq_P \beta$ if and only if $\alpha_s \leq \beta_s$ for all $s = 1, \dots, m$. Define the *downward shadow* or the *ideal* generated by an element $\alpha \in Q^m$ by

$$\Delta\alpha = \{\beta \in Q^m : \beta \preceq_P \alpha\}.$$

Define the *ideal* generated by a subset $A \subseteq Q^m$ by

$$\Delta A = \bigcup_{\alpha \in A} \Delta \alpha.$$

Define the *upward shadow* of $\alpha \in Q^m$ by

$$\nabla \alpha = \{\beta \in Q^m : \alpha \preceq_P \beta\}.$$

Lemma 4.13 *Let $\alpha \in Q^m$ such that $f_{l+1} = X^\alpha$. Then there is a bijection between $A(l)$ and $\Delta \alpha = \text{supp}(\mathbf{h}_\alpha)$. The number of elements of $A(l)$ is $\prod_{s=1}^m (\alpha_s + 1) = \text{wt}(\mathbf{h}_\alpha)$.*

Proof. The set $N(l)$ exists of all pairs (i, j) such that $f_i f_j = f_{l+1}$. The integer i , with $f_i = X^\beta$, is an element of the set $A(l)$ if and only if $\beta \preceq_P \alpha$. So there is a bijection between $A(l)$ and $\Delta \alpha$. Hence $|A(l)| = |\Delta \alpha| = \prod_{s=1}^m (\alpha_s + 1)$.

If $\beta \in Q^m$, then

$$f_\alpha(P_\beta) \neq 0 \text{ if and only if } \beta \preceq_P \alpha.$$

Hence $\Delta \alpha = \text{supp}(\mathbf{h}_\alpha)$. □

Lemma 4.14 *Let l be a positive integer. Let $l \leq l_1 < \dots < l_r$ such that $C(l_i) \neq C(l_i + 1)$. Then there exists a subspace U of $C(l)$ of dimension r , such that $(l_1, \dots, l_r)$ is its associated r -tuple and it has effective length $a(l_1, \dots, l_r)$.*

Proof. Define $\alpha(i)$, for $1 \leq i \leq r$, by $f_{l_i+1} = X^{\alpha(i)}$. Then $f_{l_i+1}^\perp$ is the leading monomial of $f_{\alpha(i)}$. Hence

$$\mathbf{h}_{\alpha(i)} = \varphi(f_{\alpha(i)}) \in C(l_i) \setminus C(l_i + 1),$$

by Corollary 4.5. Let U be the space generated by $\mathbf{h}_{\alpha(1)}, \dots, \mathbf{h}_{\alpha(r)}$, then the dimension of U is r and its associated r -tuple is $(l_1, \dots, l_r)$.

Furthermore

$$\text{supp}(U) = \cup_{i=1}^r \text{supp}(h_{\alpha(i)}) = \cup_{i=1}^r \Delta \alpha(i)$$

by Lemma 4.13. There is a bijection between $A(l_1, \dots, l_r) = \cup_{i=1}^r A(l_i)$ and $\cup_{i=1}^r \Delta \alpha(i)$ by Lemma 4.13. Therefore the effective length of U is $a(l_1, \dots, l_r)$. □

Remark 4.15 The subcode U of Lemma 4.14 depends on the choice of the order of the q^m points of $\mathbb{F}_q^m$. Any permutation σ of $\{1, \dots, m\}$ and any permutation τ of Q induce a permutation of Q^m and give another subcode U' of the same code $C(l)$ with the same associated r -tuple and effective length.

Proposition 4.16 Let $u^\perp = (q-1)m - u - 1$. Let l be the positive integer such that $f_l = X_1^{u^\perp}$. Then $C(l) = \mathcal{RM}_q(u, m)$ and $d_r(C(l)) = d_r(l)$.

Proof. This follows directly from Lemma 4.14 and Definition 3.13. $\square$

Example 4.17 Let $R = \mathbb{F}_3[X_1, X_2, X_3]$. Consider the graded lexicographic order on the monomials in the variables X_1, X_2, X_3 . Let f_i be the i th monomial in this order.

$f_1 = 1$	$f_{19} = X_1^2 X_2$	$f_{37} = X_2 X_3^4$	$f_{55} = X_1^4 X_2$
$f_2 = X_3$	$f_{20} = X_1^3$	$f_{38} = X_2^2 X_3^3$	$f_{56} = X_1^5$
$f_3 = X_2$	$f_{21} = X_3^4$	$f_{39} = X_2^3 X_3^2$	$f_{57} = X_3^6$
$f_4 = X_1$	$f_{22} = X_2 X_3^3$	$f_{40} = X_2^4 X_3$	$f_{58} = X_1 X_3^5$
$f_5 = X_3^2$	$f_{23} = X_2^2 X_3^2$	$f_{41} = X_2^5$	$f_{59} = X_2^2 X_3^4$
$f_6 = X_2 X_3$	$f_{24} = X_2^3 X_3$	$f_{42} = X_1 X_3^4$	$f_{60} = X_2^3 X_3^3$
$f_7 = X_2^2$	$f_{25} = X_2^4$	$f_{43} = X_1 X_2 X_3^3$	$f_{61} = X_2^4 X_3^2$
$f_8 = X_1 X_3$	$f_{26} = X_1 X_3^3$	$f_{44} = X_1 X_2^2 X_3^2$	$f_{62} = X_2^5 X_3^1$
$f_9 = X_1 X_2$	$f_{27} = X_1 X_2 X_3^2$	$f_{45} = X_1 X_2^3 X_3$	$f_{63} = X_2^6$
$f_{10} = X_1^2$	$f_{28} = X_1 X_2^2 X_3$	$f_{46} = X_1 X_2^4$	$f_{64} = X_1 X_3^5$
$f_{11} = X_3^3$	$f_{29} = X_1 X_2^3$	$f_{47} = X_1^2 X_3^3$	$f_{65} = X_1 X_2 X_3^4$
$f_{12} = X_2 X_3^2$	$f_{30} = X_1^2 X_3^2$	$f_{48} = X_1^2 X_2 X_3^2$	$f_{66} = X_1 X_2^2 X_3^3$
$f_{13} = X_2^2 X_3$	$f_{31} = X_1^2 X_2 X_3$	$f_{49} = X_1^2 X_2^2 X_3$	$f_{67} = X_1 X_2^3 X_3^2$
$f_{14} = X_2^3$	$f_{32} = X_1^2 X_2^2$	$f_{50} = X_1^2 X_2^3$	$f_{68} = X_1 X_2^4 X_3$
$f_{15} = X_1 X_3^2$	$f_{33} = X_1^3 X_3$	$f_{51} = X_1^3 X_3^2$	$f_{69} = X_1 X_2^5$
$f_{16} = X_1 X_2 X_3$	$f_{34} = X_1^3 X_2$	$f_{52} = X_1^3 X_2 X_3$	$f_{70} = X_1^2 X_3^4$
$f_{17} = X_1 X_2^2$	$f_{35} = X_1^4$	$f_{53} = X_1^3 X_2^2$	$f_{71} = X_1^2 X_2 X_3^3$
$f_{18} = X_1^2 X_3$	$f_{36} = X_3^5$	$f_{54} = X_1^4 X_3$	$f_{72} = X_1^2 X_2^2 X_3^2$

and so on. Let $\mathcal{P}$ be the set of all 27 distinct points in $\mathbb{F}_3^3$. Let φ be the evaluation map from R to $\mathbb{F}_3^{27}$ defined by $\varphi(f) = (f(P_1), \dots, f(P_{27}))$. The points $P_1, \dots, P_{27}$ ordered in the lexicographic order are tabulated below

in the columns. In the tables below a word $(x_1, x_2, \dots, x_n)$ is denoted by $x_1x_2 \cdots x_n$.

$$\begin{aligned}\varphi(X_1) &= 00000000011111111222222222 \\ \varphi(X_2) &= 000111222000111222000111222 \\ \varphi(X_3) &= 012012012012012012012012\end{aligned}$$

The word $\mathbf{h}_i$ is defined by $\mathbf{h}_i = \varphi(f_i)$ for all $i \in \mathbb{N}$. The codes $C(l)$ are defined by

$$C(l) = \{\mathbf{c} \in \mathbb{F}_3^{27} : \mathbf{c} \cdot \mathbf{h}_i = 0 \text{ for all } i \leq l\}.$$

Then $C(l) = 0$ for all $l > 72$. Consider for instance the code

$$C(10) = \mathcal{RM}_3(2, 3)^\perp = \mathcal{RM}_3(3, 3).$$

Let U be a subspace of the code $C(10)$ of dimension 4, for instance

$$U = \langle \mathbf{h}_5, \mathbf{h}_6, \mathbf{h}_{13}, \mathbf{h}_{19} \rangle.$$

Then $f_{19}^\perp = f_{12}$, $f_{13}^\perp = f_{18}$, $f_6^\perp = f_{31}$ and $f_5^\perp = f_{32}$. So the unique 4-tuple associated with U is $(11, 17, 30, 31)$ by Corollary 4.5.

The sets $A(11)$, $A(17)$, $A(30)$ and $A(31)$ will be computed.

- $f_{12} = X_3^2 X_2$ which can be factorized in

$$1 \cdot X_2 X_3^2 = X_2 \cdot X_3^2 = X_2 X_3 \cdot X_3,$$

so the set

$$A(11) = \{1, 2, 3, 5, 6, 12\}.$$

- $f_{18} = X_3 X_1^2$ which can be factorized in

$$1 \cdot X_1^2 X_3 = X_1 \cdot X_1 X_3 = X_1^2 \cdot X_3,$$

so the set

$$A(17) = \{1, 2, 4, 8, 10, 18\}.$$

- $f_{31} = X_3 X_2 X_1^2$ which can be factorized in

$$\begin{aligned}1 \cdot X_1^2 X_2 X_3 &= X_1 \cdot X_1 X_2 X_3 = X_1^2 X_3 \cdot X_2 = \\ &X_1^2 X_2 \cdot X_3 = X_1^2 \cdot X_2 X_3 = X_1 X_2 \cdot X_1 X_3,\end{aligned}$$

so the set

$$A(30) = \{1, 2, 3, 4, 6, 8, 9, 10, 16, 18, 19, 31\}.$$

- $f_{32} = X_2^2 X_1^2$ which can be factorized in

$$1 \cdot X_1^2 X_2^2 = X_1 \cdot X_1 X_2^2 = X_2 \cdot X_1^2 X_2 = X_1^2 \cdot X_2^2 = X_1 X_2 \cdot X_1 X_2$$

so the set

$$A(31) = \{1, 3, 4, 7, 9, 10, 17, 19, 32\}$$

Hence $A(11) \cup A(17) \cup A(30) \cup A(31)$ is equal to

$$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 16, 17, 18, 19, 31, 32\}$$

and the number of elements is

$$a(11, 17, 30, 31) = 17.$$

Consider the basis of U .

$$\begin{aligned} \mathbf{h}_5 &= \varphi(X_3^2) &= 011011011011011011011011 \\ \mathbf{h}_6 &= \varphi(X_2 X_3) &= 000012021000012021000012021 \\ \mathbf{h}_{13} &= \varphi(X_2^2 X_3) &= 000012012000012012000012012 \\ \mathbf{h}_{19} &= \varphi(X_1^2 X_2) &= 000000000000111222000111222 \end{aligned}$$

The value $a(11, 17, 30, 31) = 17$ is smaller than 22, the effective length of U . In Example 5.14 it will be shown that the minimal value $d_4(10)$ will be attained for $a(11, 12, 14, 22) = 12$.

Example 4.18 Consider the code $C(20) = \mathcal{RM}_3(3, 3)^\perp = \mathcal{RM}_3(2, 3)$. Take

$$\begin{aligned} \alpha(1) &= (1, 2, 1) \\ \alpha(2) &= (2, 0, 2) \\ \alpha(3) &= (2, 2, 0) \\ \alpha(4) &= (2, 1, 2) \end{aligned}$$

Since $q = 3$ is prime, the elements of $\mathbb{F}_q$ can be represented by $\{0, 1, 2\}$. So

$$\begin{aligned} f_{\alpha(1)} &= (X_1 - 2)(X_3 - 2) &= X_1 X_3 + X_1 + X_3 + 1 \\ f_{\alpha(2)} &= (X_2 - 1)(X_2 - 2) &= X_2^2 + 2 \\ f_{\alpha(3)} &= (X_3 - 1)(X_3 - 2) &= X_3^2 + 2 \\ f_{\alpha(4)} &= X_2 - 2 &= X_2 + 1 \end{aligned}$$

Since the sum of the entries of the $\alpha(i)$ is greater than 3, the $\mathbf{h}_{\alpha(i)}$ is an element of $\mathcal{RM}_3(2, 3)$, for all $i, 1 \leq i \leq 4$. So, $U = \langle \mathbf{h}_{\alpha(1)}, \mathbf{h}_{\alpha(2)}, \mathbf{h}_{\alpha(3)}, \mathbf{h}_{\alpha(4)} \rangle$ is a subspace of dimension 4 of $\mathcal{RM}_3(2, 3)$.

First the number of elements in the support of U will be computed.

$$\begin{aligned}
\mathbf{h}_{\alpha(1)} &= \varphi(X_1 X_3 + X_1 + X_3 + 1) = 1201201202102102100000000000 \\
\mathbf{h}_{\alpha(2)} &= \varphi(X_2^2 + 2) = 2220000002220000002220000000 \\
\mathbf{h}_{\alpha(3)} &= \varphi(X_3^2 + 2) = 200200200200200200200200200 \\
\mathbf{h}_{\alpha(4)} &= \varphi(X_2 + 1) = 111222000111222000111222000
\end{aligned}$$

The effective length of U is 23.

The leading monomials of $f_{\alpha(1)}$, $f_{\alpha(2)}$, $f_{\alpha(3)}$, and $f_{\alpha(4)}$ are $f_{28}^\perp$, $f_{30}^\perp$, $f_{32}^\perp$ and $f_{48}^\perp$, respectively. So the unique 4-tuple associated with U is $(27, 29, 31, 47)$ by Lemma 4.14.

Next the sets $A(27)$, $A(29)$, $A(31)$ and $A(47)$ will be calculated.

$$\begin{aligned}
A(27) &= \{1, 2, 3, 4, 6, 7, 8, 9, 13, 16, 17, 28\} \\
A(29) &= \{1, 2, 4, 5, 8, 10, 15, 18, 30\} \\
A(31) &= \{1, 3, 4, 7, 9, 10, 17, 19, 32\} \\
A(47) &= \{1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 16, 18, 19, 27, 30, 31, 48\}
\end{aligned}$$

So $A(27) \cup A(29) \cup A(31) \cup A(47)$ is equal to

$$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 15, 16, 17, 18, 19, 27, 28, 30, 31, 32, 48\}$$

and therefore $a(27, 29, 31, 47) = 23$ which equals the effective length of U . In Example 5.13 it will be shown that the minimal value $d_4(20)$ will be attained for $a(22, 26, 27, 43) = 18$.

5 Some combinatorics

It seems that we have translated the problem of the computation of the GHW's of RM codes in an equally difficult question. The aim of this section is to give an explicit description of an r -tuple that gives the minimum $a(l_1, \dots, l_r)$ in Definition 3.13 of the order bound $d_r(l)$ with the help of results from extremal poset theory.

Remark 5.1 Let $Q = \{0, \dots, q-1\}$. Consider the set Q^m with the lexicographic order $\prec_L$. Define $\bar{\alpha} = (\alpha_m, \dots, \alpha_1)$ if $\alpha = (\alpha_1, \dots, \alpha_m)$. Let $\mu = (q-1, \dots, q-1)$. Then the mapping from Q^m to itself defined by $\alpha \mapsto \mu - \alpha$ is a bijection. The *antilexicographic order* $\prec_A$ on Q^m is defined by $\alpha \prec_A \beta$ if and only if there exists a t such that $\alpha_i = \beta_i$ for all $i > t$

and $\alpha_t > \beta_t$. Hence $\alpha \prec_A \beta$ if and only if $\mu - \bar{\alpha} \prec_L \mu - \bar{\beta}$. So apart from the duality $\alpha \mapsto \alpha^\perp$ discussed in Remark 4.4, there is a second duality $\alpha \mapsto \bar{\alpha}^\perp = \mu - \bar{\alpha}$ on Q^m which is an isomorphism of linear orders between $(Q^m, \prec_L)$ and $(Q^m, \prec_A)$, and which induces an isomorphism between $\Delta\alpha$ and $\nabla\bar{\alpha}^\perp$. Everything which will be said about the lexicographic order can equally well be said dually for the antilexicographic order, as done in [41] and the next section.

Recall the definitions from 4.12. The partial order $\preceq_P$ on Q^m is defined by $\alpha \preceq_P \beta$ if and only if $\alpha_i \leq \beta_i$ for all i , $i = 1, \dots, m$. The ideal generated by element $\alpha \in Q^m$ is defined by $\Delta\alpha = \{\beta \in Q^m : \beta \preceq_P \alpha\}$. The ideal generated by a subset $A \subseteq Q^m$ is defined by $\Delta A = \bigcup_{\alpha \in A} \Delta\alpha$.

Definition 5.2 Let v be a fixed integer, $0 \leq v \leq m(q-1)$. Define the sets F_v and $F_{>v}$ by

$$\begin{aligned} F_v &= \{\alpha \in Q^m : \deg(\alpha) = v\}, \\ F_{>v} &= \{\alpha \in Q^m : \deg(\alpha) > v\}. \end{aligned}$$

Remark 5.3 The second duality $\alpha \mapsto \bar{\alpha}^\perp$ on Q^m induces also an isomorphism between $F_{>u}^\perp$ with respect to the lexicographic order and the set of all $\alpha \in Q^m$ such that $\deg(\alpha) \leq u$ with respect to the antilexicographic order, where $u^\perp = m(q-1) - u - 1$.

Definition 5.4 The *initial segment* of length r of a subset of Q^m consists of the first r elements of this subset with respect to the lexicographic order. Let $L_v(r)$ be the initial segment of length r of F_v . Let $L_{>v}(r)$ be the initial segment of length r of $F_{>v}$.

Theorem 5.5 Let A be a subset of F_v consisting of r elements. Then

$$|(\Delta L_v(r)) \cap F_{v-1}| \leq |(\Delta A) \cap F_{v-1}|.$$

Proof. This theorem is due to [27] when $Q = \mathbb{N}_0$, [22, 26] when $Q = \{0, 1\}$, and [5] when $Q = \{0, \dots, q-1\}$. $\square$

Corollary 5.6 Let A be a subset of F_v consisting of r elements. Then

$$|\Delta L_v(r)| \leq |\Delta A|.$$

Proof. Apply Theorem 5.5 iteratively to each layer F_{i-1} and $(\Delta A) \cap F_i$. See the remark after [41, Theorem 6]. $\square$

Theorem 5.7 *Let A be a subset of $F_{>v}$ consisting of r elements. Then*

$$|\Delta L_{>v}(r)| \leq |\Delta A|.$$

Proof. This theorem is proved in the binary case in [41, Lemma 6] as a consequence of Theorem 5.5 for $q = 2$. But since this argument is valid for any q and Theorem 5.5 is true for any q , this theorem is also valid for any q . See also [2] where this theorem is proved in the more general setting of so called *Macaulay posets*. $\square$

Lemma 5.8 *Let r be an integer such that $0 \leq r < q^m$. Write*

$$r = \sum_{i=1}^m \alpha_{m-i+1} q^{i-1}.$$

Then $(\alpha_1, \dots, \alpha_m)$ is the $(r+1)$ st element of Q^m with respect to the lexicographic order.

Proof. Suppose $\alpha, \beta \in Q^m$ and $\alpha \prec_L \beta$. Then there exists a t such that $\alpha_i = \beta_i$ for all $i < t$ and $\alpha_t < \beta_t$. A straight forward calculation shows that $\sum_{i=1}^m \alpha_{m-i+1} q^{i-1} < \sum_{i=1}^m \beta_{m-i+1} q^{i-1}$. Consider the map

$$\sigma : Q^m \longrightarrow \{0, 1, \dots, q^m - 1\}$$

defined by $\sigma(\alpha_1, \dots, \alpha_m) = \sum_{i=1}^m \alpha_{m-i+1} q^{i-1}$. Then σ is well defined. So σ is a strictly monotone map between two linear orders with the same number of elements. Hence it is an isomorphism of linear orders. $\square$

Proposition 5.9 *Let α be the r th element in $F_{>v}$ with respect to the lexicographic order $\prec_L$. Then*

$$\Delta L_{>v}(r) = \{\beta \in Q^m : \beta \prec_L \alpha \text{ or } \beta = \alpha\}$$

and it has $\sum_{i=1}^m \alpha_{m-i+1} q^{i-1} + 1$ elements.

Proof. Define $\preceq_L$ by $\beta \preceq_L \alpha$ if and only if $\beta \prec_L \alpha$ or $\beta = \alpha$. Then the partial order $\preceq_P$ is coarser than $\preceq_L$, that is to say, if $\beta \preceq_P \alpha$, then $\beta \preceq_L \alpha$. So $\Delta L_{>v}(r) \subseteq \{\beta \in Q^m : \beta \preceq_L \alpha\}$.

If $\beta \preceq_L \alpha$, then there exists a t such that $\beta_i = \alpha_i$ for all $i < t$ and $\beta_t < \alpha_t$. Define γ by $\gamma_i = \alpha_i$ for all $i < t$, $\gamma_t = \alpha_t - 1$ and $\gamma_i = q - 1$ for all $i > t$. Then $\beta \in \Delta\gamma$, $\gamma \prec_L \alpha$ and $\deg(\gamma) \geq \deg(\alpha) - 1 \geq v$. If $\deg(\gamma) = v$, then $\alpha_i = q - 1$ for all $i \geq t$, so $\beta \in \Delta\alpha$. If $\deg(\gamma) > v$, then $\gamma \in L_{>v}(r)$. Hence $\beta \in \Delta L_{>v}(r)$. This proves the converse inclusion. The statement about the number of elements follows from Lemma 5.8. $\square$

Theorem 5.10 *Let α be the r th element in Q^m in the lexicographic order with the property that $\deg(\alpha) > u^\perp = (q - 1)m - u - 1$. Then*

$$d_r(\mathcal{RM}_q(u, m)) = \sum_{i=1}^m \alpha_{m-i+1} q^{i-1} + 1.$$

Proof. Let $v = u^\perp$. Let l be the positive integer such that $f_l = X_1^v$. Then $C(l) = \mathcal{RM}_q(u, m)$ and $d_r(C(l)) = d_r(l)$ by Proposition 4.16. Let $l \leq l_1 < \dots < l_r$ such that $C(l_i) \neq C(l_i + 1)$ for all $i = 1, \dots, r$. Let $\alpha(i)$ be the exponent of f_{l_i+1} , so $f_{l_i+1} = X^{\alpha(i)}$. Then $\deg(\alpha(i)) > v$ and $\text{supp}(U) = \cup_{i=1}^r \Delta\alpha(i)$ and the effective length of U is $a(l_1, \dots, l_r)$ by Lemma 4.14. The minimal value of these $a(l_1, \dots, l_r)$ is by definition $d_r(l)$ and is obtained for $(l_1, \dots, l_r)$ the r -tuple such that $\alpha(1), \dots, \alpha(r)$ are the first r elements of $F_{>v}$ with respect to the lexicographic order, that is to say the elements of $L_{>v}(r)$ by Theorem 5.7. Moreover if $\alpha(r) = \alpha = (\alpha_1, \dots, \alpha_m)$ is the r th element of $F_{>v}$, then

$$|\cup_{i=1}^r \Delta\alpha(i)| = |\Delta L_{>v}(r)| = \sum_{i=1}^m \alpha_{m-i+1} q^{i-1} + 1.$$

$\square$

Corollary 5.11 *For given m, q and u , $0 \leq u < (q - 1)m$. Write $u^\perp + 1 = \theta(q - 1) + \mu$ for some $\theta, \mu \in \mathbb{N}_0$ with $\mu < q - 1$. Then the minimum distance of $\mathcal{RM}_q(u, m)$ is equal to $(\mu + 1)q^\theta$.*

Proof. This statement is well-known [7, 18], but it follows also from Theorem 5.10. Let $\alpha_i = 0$ for all $i < m - \theta$, $\alpha_{m-\theta} = \mu$, and $\alpha_i = q - 1$ for all

$i > m - \theta$. Then $\deg(\alpha) = u^\perp + 1$. The m -tuple α is the first element of $F_{>u^\perp}$. Hence

$$d_1(\mathcal{RM}_q(u, m)) = \sum_{i=1}^{\theta} (q-1)q^{i-1} + \mu q^\theta + 1 = (\mu+1)q^\theta.$$

□

Corollary 5.12 *The Reed-Muller codes satisfy the double chain condition.*

Proof. This is proved in the binary case in [20]. Let $d_r = d_r(\mathcal{RM}_q(u, m))$. We have shown in Proposition 5.9 and Theorem 5.10 that $\{1, 2, \dots, d_r\}$ is the support of a subcode of $\mathcal{RM}_q(u, m)$ of dimension r . So it satisfies the chain condition. Let $\tau(j) = q-1-j$ for all $j \in Q$. Then τ is a permutation of Q . The induced permutation on Q^m reverses the lexicographic order on Q^m , see Remark 4.4. So it transforms the first t coordinates to the last t , for any t . Hence the last d_r coordinates form also the support of a subcode of dimension r , by Remark 4.15. □

Example 5.13 Consider the code $C(20) = \mathcal{RM}_3(2, 3)$. This is a continuation of Example 4.18. Enumerate all the points $P_1, \dots, P_{27}$ of $\mathbb{F}_3^3$ in lexicographic order.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1
0	0	0	1	1	1	2	2	2	0	0	0	1	1	1	2	2	2
0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2

19	20	21	22	23	24	25	26	27
2	2	2	2	2	2	2	2	2
0	0	0	1	1	1	2	2	2
0	1	2	0	1	2	0	1	2

In this enumeration those points for which the sum of their entries is greater than 3 are printed boldface. Their labels in the lexicographic order gives us the generalized weights of $C(20)$.

r	1	2	3	4	5	6	7	8	9	10
$d_r(C)$	9	15	17	18	21	23	24	25	26	27

The value for $d_4(20)$ is attained for $a(22, 26, 27, 43) = 18$, since $f_{23} = X_2^2 X_3^2$, $f_{27} = X_1 X_2 X_3^2$, $f_{28} = X_1 X_2^2 X_3$ and $f_{44} = X_1 X_2^2 X_3^2$, respectively, corresponding to $(0, 2, 2)$, $(1, 1, 2)$, $(1, 2, 1)$ and $(1, 2, 2)$, respectively.

Example 5.14 Now consider the code $C(10) = \mathcal{RM}_3(3, 3)$. This is a continuation of Example 4.17. In the enumeration of points of $\mathbb{F}_3^3$ we consider now all points for which the sum of their entries is greater than 2. Their labels in the lexicographic order gives us the generalized weights of $C(10)$.

r	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$d_r(C)$	6	8	9	12	14	15	16	17	18	20	21	22	23	24	25	26	27

The value for $d_4(10)$ is attained by $a(11, 12, 14, 22)$.

6 A recursive formula

In this section a recursive formula for the determination of the GHW's of RM codes will be derived.

Definition 6.1 Let u, v and m be nonnegative integers. Define

$$\begin{aligned} M_q(u, m) &= \{X^\alpha : \alpha \in Q^m, \deg(\alpha) \leq u\}, \\ M_q(u, v, m) &= \{X^\alpha : \alpha \in Q^m, \deg(\alpha) \leq u, \alpha_m \leq v\}. \end{aligned}$$

Definition 6.2 Let $\rho_q(u, m)$ and $\rho_q(u, v, m)$ denote the number of elements of $M_q(u, m)$ and $M_q(u, v, m)$, respectively. Most of the time the index q will be deleted.

Remark 6.3 It is clear that $M(u, 0, m) = M(u, m-1) = M(u, q-1, m-1)$ and that $M(u, v, m) = M(u, u, m)$ if $u < v$.

The following lemma is basic to the recursive procedure later in this section.

Lemma 6.4 If $0 < v \leq u$, then

$$\begin{aligned} M(u, v, m) &= M(u, v-1, m) \cup M(u-v, m-1)X_m^v \\ \rho(u, v, m) &= \rho(u, v-1, m) + \rho(u-v, m-1). \end{aligned}$$

Proof. If $X^\alpha \in M(u, v, m)$, then either $\alpha_m \leq v - 1$ or $\alpha_m = v$. So $M(u, v, m)$ is the disjoint union of $M(u, v - 1, m)$ and $M(u - v, m - 1)X_m^v$. $\square$

Lemma 6.5

$$\rho_q(u, m) = \dim(\mathcal{RM}_q(u, m)) = \sum_{i=0}^u \sum_{j=0}^{\lfloor i/q \rfloor} (-1)^j \binom{m}{j} \binom{m-1+i-qj}{m-1}$$

Proof. See [35] or [38, Exercise 1.2.8]. $\square$

Proposition 6.6 *Let u, v and m be nonnegative integers such that $v \leq q - 1$. Let r be an integer such that $0 \leq r < \rho(u, v, m)$, then r has a canonical representation with respect to (u, v, m) , that is to say, there exist a positive integer t and sequences of nonnegative integers $u_0, u_1, \dots, u_t$ and $m_0, m_1, \dots, m_t$, and sets $N(u_i, m_i)$ of $\rho(u_i, m_i)$ monomials such that $\cup_{i=1}^t N(u_i, m_i)$ is a disjoint union and consists of the first r elements of $M(u, v, m)$ with respect to the antilexicographic order. So*

$$r = \sum_{i=1}^t \rho(u_i, m_i).$$

Furthermore

$$u_i = \max\{0, u_{i-1} + 1 - (q - 1)(m_{i-1} - m_i)\}$$

for all i , $1 \leq i \leq t$, where $u_0 = u + (q - 1) - (v + 1)$ and $m_0 = m$. The canonical representation of r with respect to (u, v, m) is unique.

Proof. See [41, Lemma 2] for the binary case and [1] for arbitrary q . The idea of the representation is to use by induction Lemma 6.4

$$M(u', v', m') = M(u', v' - 1, m') \cup M(u' - v', m' - 1)X_{m'}^{v'}.$$

All elements of $M(u' - v', m' - 1)X_{m'}^{v'}$ are smaller than the elements of $M(u', v' - 1, m')$ with respect to the antilexicographic order.

The sequences (u_i) , (m_i) and the sets $N(u_i, m_i)$ are defined and their properties are proved by induction on the quadruples (r, u, v, m) that are ordered

with respect to the lexicographic order. If $r = 0$, then there is nothing to prove. Assume that the sequences and the sets are defined and have the desired properties for all r' , $0 \leq r' < r$.

(i) If $v = 0$, then $M(u, v, m) = M(u, q - 1, m - 1)$ by Remark 6.3. So we may assume $v > 0$.

(ii) If $u < v$, then $M(u, v, m) = M(u, u, m)$ by Remark 6.3. So we may assume $v \leq u$.

(iii) Suppose $0 < v \leq u$ and $r \geq \rho(u - v, m - 1)$. Let $r' = r - \rho(u - v, m - 1)$. Then $0 \leq r' < \rho(u, v - 1, m)$, since $\rho(u, v, m) = \rho(u, v - 1, m) + \rho(u - v, m - 1)$ by Lemma 6.4. By induction r' has a canonical representation with respect to $(u, v - 1, m)$, so there exists a t' and sequences $u'_0, u'_1, \dots, u'_{t'}$ and $m'_0, m'_1, \dots, m'_{t'}$, and sets $N'(u'_i, m'_i)$ consisting of $\rho(u'_i, m'_i)$ elements, with the stated properties. Let $u_0 = u + (q - 1) - (v + 1)$ and $m_0 = m$. Let $u_1 = u - v$, $m_1 = m - 1$ and $N(u_1, m_1) = M(u_1, m_1)X_m^v$. Let $t = t' + 1$. Let $u_i = u'_{i-1}$, $m_i = m'_{i-1}$ and $N(u_i, m_i) = N'(u'_{i-1}, m'_{i-1})$ for all $2 \leq i \leq t$. In this way a canonical representation of r with respect to (u, v, m) is obtained.

(iv) If $0 < v \leq u$ and $0 \leq r < \rho(u - v, m - 1) = \rho(u - v, q - 1, m - 1)$, then by induction r has a canonical representation with respect to $(u - v, q - 1, m - 1)$. So there exist a positive integer t' and sequences of nonnegative integers $u'_0, u'_1, \dots, u'_{t'}$ and $m'_0, m'_1, \dots, m'_{t'}$, and sets $N'(u'_i, m'_i)$ of $\rho(u'_i, m'_i)$ monomials such that $\cup_{i=1}^{t'} N'(u'_i, m'_i)$ is a disjoint union and consists of the first r elements of $M(u - v, q - 1, m - 1)$ with respect to the antilexicographic order. Let $t = t'$. Let $u_0 = u + (q - 1) - (v + 1)$ and $m_0 = m$. Let $u_i = u'_i$ and $m_i = m'_i$ for all $1 \leq i \leq t$. Let $N(u_i, m_i) = N'(u_i, m'_i)X_m^v$. Hence a canonical representation of r with respect to (u, v, m) is obtained.

The proof of the statement about the u_i and of the uniqueness of the canonical representation is left to the reader. $\square$

Proposition 6.7 *Let $u_0, u_1, \dots, u_t$ and $m_0, m_1, \dots, m_t$ be the sequences in the canonical representation of r with respect to (u, v, m) . Let*

$$\beta_i = u_i - [u_{i-1} + 1 - (q - 1)(m_{i-1} - m_i)] + 1,$$

for $i = 1, \dots, t$. Let U be the code generated by the $\mathbf{h}_{\alpha^\perp}$ for the first r elements $X^\alpha \in M(u, v, m)$ with respect to the antilexicographic order. Let $R = \rho_q(u - v, m - 1)$. Then

$$|supp(U)| = \begin{cases} (q - v) \sum_{i=1}^t \beta_i q^{m_i} & \text{if } r \leq R, \\ (q - v) \beta_1 q^{m_1} + \sum_{i=2}^t \beta_i q^{m_i} & \text{if } r > R. \end{cases}$$

Proof. See [1] in case $v = q - 1$. The general case is treated in the Appendix. $\square$

Theorem 6.8 *Let the sequence (β_i) be associated to the canonical representation of r with respect to $(u, q - 1, m)$ as in Proposition 6.7. Then*

$$d_r(\mathcal{RM}_q(u, m)) = \sum_{i=1}^t \beta_i q^{m_i}.$$

Proof. See [41, Corollary 6] for the binary case and [1] for $q = 3$. It is a consequence of Theorem 5.10, Remark 5.1 and Proposition 6.7 with $v = q - 1$. $\square$

Remark 6.9 The inductive procedure to obtain the sequences (u_i) and (m_i) and the sets $N(u_i, m_i)$ in the proof of Proposition 6.6 can be depicted by a labeled directed graph. The nodes consist of quadruples of the form (r, u, v, m) and the leaves are the pairs (u_i, m_i) .

Suppose that (r, u, v, m) is the quadruple that corresponds to the state in the proof where the first r monomials are looked for in $M(u, v, m)$.

(i) If $v = 0$, then a vertical arrow is drawn from $(r, u, 0, m)$ to $(r, u, q - 1, m - 1)$ as follows:

$$\begin{array}{c} (r, u, 0, m) \\ \downarrow \\ (r, u, q - 1, m - 1) \end{array}$$

(ii) If $u < v$, then a vertical arrow is drawn from (r, u, v, m) to (r, u, u, m) as follows:

$$\begin{array}{c} (r, u, v, m) \\ \downarrow \\ (r, u, u, m) \end{array}$$

(iii) If $0 < v \leq u$ and $r \geq \rho(u - v, m - 1)$, then two diagonal arrows are drawn from (r, u, v, m) . The first down to the left to $(r', u, v - 1, m)$ with $r' = r - \rho(u - v, m - 1)$. The second down to the right to $(u - v, m - 1)$ with the label X_m^v as follows:

$$\begin{array}{ccc} & (r, u, v, m) & \\ \swarrow & & \searrow^{X_m^v} \\ (r', u, v - 1, m) & & (u - v, m - 1) \end{array}$$

(iv) If $0 < v \leq u$ and $0 \leq r < \rho(u - v, m - 1)$, then a diagonal arrow is drawn from (r, u, v, m) down to the right to $(r, u - v, q - 1, m - 1)$ with the label X_m^v as follows:

$$\begin{array}{ccc} (r, u, v, m) & & \\ & \searrow^{X_m^v} & \\ & & (r, u - v, q - 1, m - 1) \end{array}$$

The leaves of the tree are pairs of the form (u_i, m_i) where the index i increases with the distance to the node at the top. The set $N(u_i, m_i)$ is obtained by multiplying $M(u_i, m_i)$ by the monomials that stand as labels of the edges of the unique path from the top node to the leaf (u_i, m_i) .

Example 6.10 Let $q = 4$, $r = 8$ and $u = v = m = 3$. Then the tree looks like:

The pairs (u_i, m_i) , the sets $N(u_i, m_i)$ and the β_i are given in the following

table.

i	(u_i, m_i)	$N(u_i, m_i)$	β_i
0	(2, 3)		
1	(0, 2)	$\{1\} \cdot X_3^3$	1
2	(1, 2)	$\{1, X_1, X_2\} \cdot X_3^2$	1
3	(0, 1)	$\{1\} \cdot X_2^2 \cdot X_3$	2
4	(1, 1)	$\{1, X_1\} \cdot X_2 \cdot X_3$	1
5	(0, 0)	$\{1\} \cdot X_1^2 \cdot X_3$	2

Hence $d_8 = 1 \cdot 4^2 + 1 \cdot 4^2 + 2 \cdot 4^1 + 1 \cdot 4^1 + 2 \cdot 4^0 = 46$ by Theorem 6.8.

Now $u^\perp = (4 - 1) \cdot 3 - 3 - 1 = 5$. The first 8 elements of $F_{>5}$ are tabulated below.

α_1	0	1	1	1	2	2	2	2
α_2	3	2	3	3	1	2	2	3
α_3	3	3	2	3	3	2	3	1

Hence $d_8 = 1 \cdot 4^0 + 3 \cdot 4^1 + 2 \cdot 4^2 + 1 = 46$ by Theorem 5.10.

Remark 6.11 Notice that in the binary case $v = 0$ or $v = 1$. The only occurrence of $v = 0$ in the tree is directly after case (iii). Hence the index for v is superfluous and can be deleted. Case (iii) gives rise to the diagram:

$$\begin{array}{ccc}
 & (r, u, m) & \\
 \swarrow & & \searrow^{X_m} \\
 (r', u, m - 1) & & (u - 1, m - 1)
 \end{array}$$

Furthermore $u_i = u_{i-1} + 1 - (m_{i-1} - m_i)$, so $\beta_i = 1$ for all $i = 1, \dots, t$ when $q = 2$.

Example 6.12 Let $q = 2$, $r = 10$, $u = 3$, and $m = 5$. Then the tree looks

like:

The pairs (u_i, m_i) and sets $N(u_i, m_i)$ are given in the following table.

i	(u_i, m_i)	$N(u_i, m_i)$
0	(2, 5)	
1	(1, 3)	$\{1, X_1, X_2, X_3\} \cdot X_4 \cdot X_5$
2	(1, 2)	$\{1, X_1, X_2\} \cdot X_3 \cdot X_5$
3	(1, 1)	$\{1, X_1\} \cdot X_2 \cdot X_5$
4	(1, 0)	$\{1\} \cdot X_1 \cdot X_5$

Hence $d_{10} = 2^3 + 2^2 + 2^1 + 2^0 = 15$ by Theorem 6.8.

Now $u^\perp = (2 - 1) \cdot 5 - 3 - 1 = 1$. The 10th element of $F_{>1}$ is $(0, 1, 1, 1, 0)$.

So $d_{10} = 0 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^3 + 0 \cdot 2^4 + 1 = 15$ by Theorem 5.10.

The sets $N(u_i, m_i)$ are not always of the form $M(u_i, m_i) \prod_{j=m_i+1}^{m_i+u-u_i} X_j$ as claimed in the proof of [41, Corollary 6].

7 Concluding remarks and questions

The above methods readily apply to the case where $\mathcal{P}$ corresponds to a multidimensional block of the form $\{\alpha \in Q^m : 0 \leq \alpha_i \leq q_i - 1 \text{ for all } i\}$, where the q_i are positive integers such that $q_i \leq q$ for all i .

Also the weighted (affine) RM codes [36] can be treated by our methods by considering the weighted graded lexicographic order where the degree of the monomials is weighted.

Problem 7.1' of [39] is still an open question, that is to say what the GHW's of the projective or nonprimitive RM codes [35, 43] are and whether the above methods also apply to these codes. In [3] and [44] the GHW's of the first and second order projective RM codes are computed. In [3] a conjecture is formulated for the GHW's of projective RM codes which is quite similar in spirit to the answer given in Theorem 5.10 for the ordinary RM codes. The fundamental problem of the determination of the (generalized) weight distribution [25, 34] of RM codes seems still far out of reach, but Remark 4.15 gives a lot of subcodes with a known effective length.

Let R be an $\mathbb{F}$ -algebra. A *weight function* on R is an order function on R that satisfies furthermore

$$(O.5) \quad \rho(fg) = \rho(f) + \rho(g)$$

for all $f, g \in R$. Here $-\infty + n = -\infty$ for all $n \in \mathbb{N}_0$.

The standard example of an $\mathbb{F}$ -algebra R with a degree function ρ is obtained by taking $R = \mathbb{F}[X_1, \dots, X_m]$ and $\rho(f) = \deg(f)$, the degree of $f \in R$. It is a weight function if and only if $m = 1$. More generally, let $\mathcal{X}$ be an algebraic curve defined over the field $\mathbb{F}$. Let P be a rational point of $\mathcal{X}$. Let R be the ring of rational functions on $\mathcal{X}$ which have only poles at the point P . Let v_P be the discrete valuation at P on R . Let $\rho(f) = -v_P(f)$, so it is the pole order of f at P . Then ρ is a weight function on R . See [16, 31, 37, 38].

In [40, 29] bounds are given for the GHW's of algebraic geometry codes involving the gonality sequence. Good bounds are obtained [16, 23] for the minimum distance of the one point AG codes in terms of the Weierstrass semigroup of the point at infinity, or what amounts to the same, the semigroup of the weight function ρ . This is generalized with the theory of Gröbner bases for affine algebraic sets in [33].

A Proof of Proposition 6.7

Let $\alpha(1), \dots, \alpha(r)$ be such that $X^{\alpha(i)}$ is the i th element of $M_q(u, v, m)$ with respect to the antilexicographic order, for $i = 1, \dots, r$.

Let $r = 1$. The first element $X^{\alpha(1)}$ in $M_q(u, v, m)$ with respect to the antilex-

icographic order is

$$\alpha(1) = (\underbrace{0, \dots, 0}_{m-\theta-2}, \mu, \underbrace{q-1, \dots, q-1}_{\theta}, v),$$

where $u - v = \theta(q - 1) + \mu$, $\mu < q - 1$.

The size of the support of U if $r = 1$, is

$$|\nabla \alpha(1)| = q^{m-\theta-2}(q - \mu)(q - v),$$

by Lemma 4.13 and Remark 5.1. For the canonical representation of $r = 1$, we find $u_0 = u + (q - 1) - (v + 1)$, $m_0 = m$, $u_1 = 0$ and

$$m_1 = \begin{cases} m - 1 & \text{if } v = u, \\ m - 2 - \theta & \text{if } v < u. \end{cases}$$

Then

$$\beta_1 = u_1 - [u_0 + 1 - (q - 1)(m_0 - m_1)] + 1 = \begin{cases} 1 & \text{if } u = v, \\ q - \mu & \text{if } u > v. \end{cases}$$

So

$$(q - v)\beta_1 q^{m_1} = (q - v)(q - \mu)q^{m-\theta-2}$$

in both cases $u = v$ and $u > v$, and it is equal to the effective length of U . Hence the proposition is proved for $r = 1$.

Assume from now on that $r > 1$. Let $j + 1$ be the first nonzero position of $\alpha(r - 1)$. So

$$\alpha(r - 1) = (\alpha_1, \alpha_2, \dots, \alpha_m) = (\underbrace{0, \dots, 0}_j, \alpha_{j+1}, \dots, \alpha_m),$$

with $\alpha_{j+1} \neq 0$.

We want to express $\alpha(r)$ in terms of $\alpha(r - 1)$. Four cases 1(a)i, 1(a)ii, 1(b) and 2 will be considered. Later case 2 will be subdivided in 2(a), 2(b)i and 2(b)ii. Define

$$\begin{aligned} M &= u + 1 - \sum_{l=j+1}^m \alpha_l, \\ F &= \lfloor \frac{M}{q-1} \rfloor. \end{aligned}$$

Case 1(a)i If $j > 0$, $r > 2$ and $\alpha_1(r-2) = 1$, and $F < j$, then

$$\alpha(r) = (\underbrace{0, \dots, 0}_{j-F-1}, M - F(q-1), \underbrace{q-1, \dots, q-1}_F, \alpha_{j+1} - 1, \alpha_{j+2}, \dots, \alpha_m).$$

Case 1(a)ii If $j > 0$, $r > 2$ and $\alpha_1(r-2) = 1$, and $F \geq j$, then

$$\alpha(r) = (\underbrace{q-1, \dots, q-1}_j, \alpha_{j+1} - 1, \alpha_{j+2}, \dots, \alpha_m).$$

Case 1(b) If $j > 0$ and $r = 2$ or $\alpha_1(r-2) \neq 1$, then

$$\alpha(r) = (\underbrace{0, \dots, 0}_{j-1}, 1, \alpha_{j+1} - 1, \alpha_{j+2}, \dots, \alpha_m).$$

Case 2 If $j = 0$, that is to say $\alpha_1 \neq 0$, then

$$\alpha(r) = (\alpha_1 - 1, \alpha_2, \dots, \alpha_m).$$

In all four cases it is easy to verify that

$$\alpha(r-1) \prec_A \alpha(r),$$

and that there exists no β such that $X^\beta \in M_q(u, v, m)$ and

$$\alpha(r-1) \prec_A \beta \prec_A \alpha(r),$$

since $\deg(\beta) > u$ otherwise.

Hence $\alpha(r)$ can be determined from $\alpha(r-1)$ and $\alpha(r-2)$.

Let $U(r) = \langle \mathbf{h}_{\alpha^\perp(1)}, \dots, \mathbf{h}_{\alpha^\perp(r)} \rangle$. Let $SU(r)$ be the effective length of $U(r)$.

We want to express $SU(r)$ in terms of $SU(r-1)$. Now

$$SU(r) = |\cup_{i=1}^r \nabla \alpha(i)|$$

by the dual version of Lemma 4.14 and Remark 5.1. Hence

$$SU(r) = SU(r-1) + |\nabla \alpha(r) \setminus \cup_{i=1}^{r-1} \nabla \alpha(i)|$$

The second term at the right is described by the following lemma.

Lemma A.1 Let $\gamma = (\gamma_1, \dots, \gamma_m)$, then

$$\gamma \in \nabla\alpha(r) \setminus \bigcup_{i=1}^{r-1} \nabla\alpha(i)$$

if and only if

$$\begin{cases} \alpha(r-1) \prec_A (\gamma_1, \dots, \gamma_{m-1}, v) \preceq_A \alpha(r), \gamma_m \leq v, & \text{if } r \leq R, \\ \alpha(r-1) \prec_A \gamma \preceq_A \alpha(r), & \text{if } r > R. \end{cases}$$

Proof. This lemma is the dual version of Proposition 5.9, see Remark 5.1. $\square$

Case 1(a)i

$$SU(r) = \begin{cases} SU(r-1) + q^{j-F-1}(q-M+F(q-1))(q-v) & \text{if } r \leq R, \\ SU(r-1) + q^{j-F-1}(q-M+F(q-1)) & \text{if } r < R. \end{cases}$$

Proof. Let $\gamma \in \nabla\alpha(r)$, then

$$\gamma = (\geq 0, \dots, \geq 0, \geq M-F(q-1), q-1, \dots, q-1, \geq \alpha_{j+1}-1, \geq \alpha_{j+2}, \dots, \geq \alpha_m).$$

And if $\alpha(r-1) \prec_A \gamma$, then

$$\gamma = (\geq 0, \dots, \geq 0, \geq M-F(q-1), q-1, \dots, q-1, \alpha_{j+1}-1, \alpha_{j+2}, \dots, \alpha_m).$$

Hence by Lemma A.1

$$\gamma \in \nabla\alpha(r) \setminus \bigcup_{i=1}^{r-1} \nabla\alpha(i)$$

and there are

$$q^{j-F-1}(q-M+F(q-1))(q-v)$$

of these distinct γ 's if $r \leq R$, and

$$q^{j-F-1}(q-M+F(q-1))$$

if $r > R$. $\square$

Case 1(a)ii

$$SU(r) = \begin{cases} SU(r-1) + (q-v) & \text{if } r \leq R, \\ SU(r-1) + 1 & \text{if } r > R. \end{cases}$$

Proof. If

$$\gamma = (q-1, \dots, q-1, \alpha_{j+1}+1, \alpha_{j+2}, \dots, \alpha_{m-1}, \alpha_m),$$

then $\alpha(r-1) \prec_A \gamma \leq_A \alpha(r)$ and there are $(q-v)$ of these distinct γ 's if $r \leq R$, and 1 if $r > R$. $\square$

Case 1(b)

$$SU(r) = \begin{cases} SU(r-1) + q^{j-1}(q-1)(q-v) & \text{if } r \leq R, \\ SU(r-1) + q^{j-1}(q-1) & \text{if } r < R. \end{cases}$$

Proof. If

$$\gamma = (\geq 0, \dots, \geq 0, \geq 1, \alpha_{j+1} + 1, \alpha_{j+2}, \dots, \alpha_{m-1}, \alpha_m),$$

then $\alpha(r-1) \prec_A \gamma \leq_A \alpha(r)$ and there are $q^{j-1}(q-1)(q-v)$ of these distinct γ 's if $r \leq R$, and $q^{j-1}(q-1)$ if $r > R$. $\square$

Case 2

$$SU(r) = \begin{cases} SU(r-1) + (q-v) & \text{if } r \leq R, \\ SU(r-1) + 1 & \text{if } r > R. \end{cases}$$

Proof. If

$$\gamma = (\alpha_1 + 1, \alpha_2, \dots, \alpha_{m-1}, \alpha_m),$$

then $\alpha(r-1) \prec_A \gamma \leq_A \alpha(r)$ and there are $(q-v)$ of these distinct γ 's if $r \leq R$, and 1 if $r > R$. $\square$

Let $u(r-1) = (u_0, \dots, u_t)$ and $m(r-1) = (m_0, \dots, m_t)$ be the sequences in the canonical representation of $r-1$. Let $\beta(r-1) = (\beta_1, \dots, \beta_t)$. Let $u(r) = (\bar{u}_1, \dots, \bar{u}_\tau)$ and $m(r) = (\bar{m}_1, \dots, \bar{m}_\tau)$ be the sequences in the canonical representation of r .

In the following six cases the $u(r)$ and $m(r)$ are expressed in terms of $u(r-1)$ and $m(r-1)$. The reader is advised to draw the corresponding directed labeled graphs as explained in Remark 6.9.

Note that if $\gamma = (0, \dots, 0, \alpha_{j+2}, \dots, \alpha_m)$, then

$$X^{\alpha(r-1)} = X_{j+1}^{\alpha_{j+1}} \cdot X^\gamma.$$

1. (a) i. In this case

$$X^{\alpha(r)} = X_{j-F}^{M-F(q-1)} \cdot X_{j-F+1}^{q-1} \cdots X_j^{q-1} \cdot X_{j+1}^{\alpha_{j+1}-1} \cdot X^\gamma.$$

$\bar{u}_i = u_i$ and $\bar{m}_i = m_i$ for $1 \leq i \leq t$ and $\tau = t+1$. Then the tree to obtain the canonical representation of r is an extension of the tree of the canonical representation of $r-1$.

Hence $m_t = j$, $u_t = M-1$, $\bar{u}_\tau = 0$ and $\bar{m}_\tau = j-F-1$. And

$$\beta(r) = (\beta_1, \dots, \beta_t, M-1+(q-1)(F-1)).$$

ii. Now

$$X^{\alpha(r)} = X_1^{q-1} \cdots X_j^{q-1} \cdot X_{j+1}^{\alpha_{j+1}-1} \cdot X^\gamma$$

$\bar{u}_i = u_i$ and $\bar{m}_i = m_i$ for $1 \leq i \leq t$ and $\tau = t + 1$. Then the tree to obtain the canonical representation of r is an extension of the tree of the canonical representation of $r - 1$.

Hence $m_t = j$, $\bar{u}_\tau = u_t + 1 - j(q - 1)$ and $\bar{m}_\tau = 0$. And

$$\beta(r) = (\beta_1, \dots, \beta_t, 1).$$

(b) In this case

$$X^{\alpha(r)} = X_j \cdot X_{j+1}^{\alpha_{j+1}-1} \cdot X^\gamma.$$

$\bar{u}_i = u_i$ and $\bar{m}_i = m_i$ for $1 \leq i \leq t$ and $\tau = t + 1$. Then the tree to obtain the canonical representation of r is an extension of the tree of the canonical representation of $r - 1$.

Hence $u_t = 0$, $m_t = j$, $\bar{u}_\tau = 0$ and $\bar{m}_\tau = j - 1$. And

$$\beta(r) = (\beta_1, \dots, \beta_t, q - 1).$$

2. Now

$$X^{\alpha(r)} = X^{\alpha_1-1} \cdot X^\gamma.$$

(a) If $\alpha_1 > 1$, then $\bar{u}_i = u_i$ and $\bar{m}_i = m_i$ for $1 \leq i \leq t$ and $\tau = t + 1$. Then the tree to obtain the canonical representation of r is an extension of the tree of the canonical representation of $r - 1$. Hence $m_t = 0$, $\bar{m}_\tau = 0$ and $\bar{u}_\tau = u_t + 1$. And

$$\beta(r) = (\beta_1, \dots, \beta_t, 1).$$

(b) If $\alpha_1 = 1$, then let $\alpha(r) = (0, \dots, 0, \alpha_s, \dots, \alpha_m)$, $\alpha_s \neq 0$.

Then

$$N(\bar{u}_\tau, \bar{m}_\tau) = X^{\alpha(r)} \cdot M(\bar{u}_\tau, \bar{m}_\tau).$$

Therefore $\bar{m}_\tau = s - 1$ and $\bar{u}_\tau = u - \sum_{i=s}^m \alpha_i$ and τ is defined by

$$\sum_{i=\tau}^t \rho(u_i, m_i) + 1 = \rho(\bar{u}_\tau, \bar{m}_\tau).$$

Furthermore $\bar{u}_i = u_i$ and $\bar{m}_i = m_i$ for $i < \tau$.

- i. If $\alpha_s \leq q - 2$, then let $\gamma = (0, \dots, 0, \alpha_{s+1}, \dots, \alpha_m)$.
Then $X^{\alpha(r)} = X_s^{\alpha_s} \cdot X^\gamma$ and $u_{\tau-1} = u - \sum_{i=s}^m \alpha_i - 1$ and $m_{\tau-1} = s - 1$. Hence $\beta(r) = (\beta_1, \dots, \beta_{\tau-1}, 1)$.
- ii. If $\alpha_s = q - 1$, then let $\gamma = (0, \dots, 0, \alpha_{s+2}, \dots, \alpha_m)$.
Then $X^{\alpha(r)} = X_s^{q-1} \cdot X^\gamma$ and $u_{\tau-1} = u - \sum_{i=s+1}^m \alpha_i - 1$ and $m_{\tau-1} = s$. Hence $\beta(r) = (\beta_1, \dots, \beta_{\tau-1}, 1)$.

This ends the treatment of the six cases.

Let $r \leq R$ and assume that

$$SU(r-1) = (q-v) \sum_{i=1}^t \beta_i(r-1) q^{m_i}.$$

Define $BS(r)$ as

$$BS(r) = (q-v) \sum_{i=1}^{\tau} \beta_i(r) q^{\overline{m}_i}.$$

Hence $BS(r-1) = SU(r-1)$ by the induction hypothesis. It remains to prove that in that case $BS(r) = SU(r)$.

Case 1(a)i

$$\begin{aligned} SU(r) - SU(r-1) &= q^{j-F-1} (q - M + F(q-1))(q-v) \\ BS(r) - BS(r-1) &= (q-v)(M-1 + (q-1)(F-1))q^{j-F-1} \end{aligned}$$

The other cases are left to the reader.

For $r > R$ the proof is the same, since in $SU(r)$ only the factor $(q-v)$ has disappeared, just as in the Proposition.

References

- [1] A. Ashikhmin, "Generalized Hamming weights of Reed-Muller codes over $GF(3)$," (in Russian) *Chapter of Ph.D. Thesis*, Institute for Problems of Information Transmission, Moscow, 1994.
- [2] S. Bezrukov and P. Heijnen, "On minimal ideals in Macaulay posets," preprint Feb. 1996.

- [3] M. Boguslavsky, "On the number of solutions of polynomial systems," to appear in *Finite Fields and their Applications*.
- [4] B. Buchberger, "Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal," *Ph.D. Thesis*, Univ. of Innsbruck, Austria, 1965.
- [5] G.F. Clements and B. Lindström, "A generalization of a combinatorial theorem of Macaulay," *Journ. Combinatorial Theory*, vol. 7, pp. 230-238, 1969.
- [6] D. Cox, J. Little and D. O'Shea, *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry*, Springer-Verlag, Berlin, 1992.
- [7] P. Delsarte, J.M. Goethals and F.J. MacWilliams, "On generalized Reed-Muller codes and their relatives," *Information and Control*, vol. 16, pp. 403-442, 1970.
- [8] S.B. Encheva, "On binary linear codes which satisfy the two-way chain condition," *IEEE Trans. Inform. Theory*, vol. IT-42, pp. 1038-1047, May 1996.
- [9] O. Endler, *Valuation theory*, Universitext, Springer-Verlag, Berlin, 1972
- [10] G.-L. Feng and T.R.N. Rao, "Decoding of algebraic geometric codes up to the designed minimum distance," *IEEE Trans. Inform. Theory*, vol. IT-39, pp. 37-45, Jan. 1993.
- [11] G.-L. Feng and T.R.N. Rao, "A simple approach for construction of algebraic-geometric codes from affine plane curves," *IEEE Trans. Inform. Theory*, vol. IT-40, pp. 1003-1012, July 1994.
- [12] G.-L. Feng, V. Wei, T.R.N. Rao and K.K. Tzeng, "Simplified understanding and efficient decoding of a class of algebraic-geometric codes," *IEEE Trans. Inform. Theory*, vol. IT-40, pp. 981-1002, July 1994.
- [13] G.D. Forney Jr., "Dimension/length profiles and trellis complexity of linear block codes," *IEEE Trans. Inform. Theory*, vol. IT-40, pp. 1741-1752, Nov. 1994.

- [14] G.D. Forney Jr., "Dimension/length profiles and trellis complexity of lattices," *IEEE Trans. Inform. Theory*, vol. IT-40, pp. 1753-1772, Nov.1994.
- [15] T. Helleseeth, T. Kløve and J. Mykkelveit, "The weight distribution of irreducible cyclic codes with block lengths $n_1((q^l - 1)/N)$," *Discrete Math.*, vol. 18, pp. 179-211, 1977.
- [16] T. Høholdt, J.H. van Lint and R. Pellikaan, "Algebraic geometry codes", to appear in *Handbook of Coding Theory*, R.A. Brualdi, W.C. Huffman and V. Pless (Eds.), Elsevier, Amsterdam.
- [17] T. Høholdt and R. Pellikaan, "On decoding algebraic-geometric codes," *IEEE Trans. Inform. Theory*, vol. IT-41, pp. 1589-1614, Nov. 1995.
- [18] T. Kasami, S. Lin and W.W. Peterson, "New generalization of Reed-Muller codes. Part 1: Primitive codes," *IEEE Trans. Inform. Theory*, vol. IT-14, pp. 189-199, 1968.
- [19] T. Kasami, S. Lin and W.W. Peterson, "Polynomial codes," *IEEE Trans. Inform. Theory*, vol. IT-14, pp. 807-814, 1968.
- [20] T. Kasami, T. Takata, T. Fujiwara and S. Lin, "On the optimum bit orders with respect to the state complexity of trellis diagrams for linear binary codes," *IEEE Trans. Inform. Theory*, vol. IT-39, pp. 242-245, Jan. 1993.
- [21] T. Kasami, T. Takata, T. Fujiwara and S. Lin, "On complexity of trellis structure of linear block codes," *IEEE Trans. Inform. Theory*, vol. IT-39, pp. 1057-1064, May 1993.
- [22] G.O.H. Katona, "A theorem of finite sets," in *Theory of Graphs, Proceedings of the Colloquium held at Tihany, Hungary, September 1966*, ed. by P. Erdős and G. Katona, Academic Press, New York; Akademia Kiado, Budapest 1968, pp. 187-207.
- [23] C. Kirfel and R. Pellikaan, "The minimum distance of codes in an array coming from telescopic semigroups," *IEEE Trans. Inform. Theory*, vol. IT-41, pp. 1720-1732, Nov. 1995.
- [24] T. Kløve, "The weight distribution of linear codes over $GF(q^l)$ having generator matrix over $GF(q)$," *Discrete Math.*, vol. 23, pp. 159-168, 1978.

- [25] T. Kløve, "Support weight distribution of linear codes," *Discrete Math.*, vol. 106/107, pp. 311-316, 1992.
- [26] J.B. Kruskal, "The optimal number of simplices in a complex," in *Math. Optimization Techniques*, Univ. Calif. Press, Berkeley, California, 1963, pp. 251-268.
- [27] F.S. Macaulay, "Some properties of enumeration in the theory of modular systems," *Proc. London Math. Soc.*, vol. 26, pp. 531-555, 1927.
- [28] R.E. Muller, "Application of Boolean algebra to switching circuit design and to error detection," *IRE Trans. Electronic Comput.*, vol. EC-3, pp. 6-12, 1954.
- [29] C. Munuera, "On the generalized Hamming weights of geometric Goppa codes," *IEEE Trans. Inform. Theory*, vol. IT-40, pp. 2092-2099, Nov. 1994.
- [30] R. Pellikaan, "The shift bound for cyclic, Reed-Muller and geometric Goppa codes," in *Arithmetic, Geometry and Coding Theory*, ed. by R. Pellikaan, M. Perret and S.G. Vlăduț, Walter de Gruyter, Berlin 1996, pp. 155-175.
- [31] R. Pellikaan, "On the existence of order and weight functions," to appear in *Journ. Statistical Planning and Inference*.
- [32] I.S. Reed, "A class of multiple-error-correcting codes and the decoding scheme," *IRE Trans. Inform. Theory*, vol. PGIT-4, pp. 38-49, 1954.
- [33] T. Shibuya, J. Mizutani and K. Sakaniwa, "On generalized Hamming weights of codes constructed on affine algebraic sets," in *Proc. of AAECC-12, Lect. Notes Comp. Science*, vol. 1255, pp. 311-320, 1997.
- [34] J. Simonis, "The effective length of subcodes," *AAECC*, vol. 5, pp. 371-377, 1994.
- [35] A.B. Sørensen, "Projective Reed-Muller codes," *IEEE Trans. Inform. Theory*, vol. IT-37, pp. 1567-1576, Nov. 1991.
- [36] A.B. Sørensen, "Weighted projective Reed-Muller codes and algebraic geometric codes," *IEEE Trans. Inform. Theory*, vol. IT-38, pp. 1821-1826, 1992.

- [37] H. Stichtenoth, *Algebraic function fields and codes*, Universitext, Springer-Verlag, Berlin 1993.
- [38] M.A. Tsfasman and S.G. Vlăduț, *Algebraic geometric codes*, Mathematics and its Applications, vol. 58, Kluwer Acad, Publ., Dordrecht 1991.
- [39] M.A. Tsfasman and S.G. Vlăduț, “Survey on generalized Hamming weights,” *IEEE Trans. Inform. Theory*, vol. IT-41, pp. 1564-1588, Nov. 1995.
- [40] K. Yang, P.V. Kumar and H. Stichtenoth, “On the weight hierarchy of geometric Goppa codes,” *IEEE Trans. Inform. Theory*, vol. IT-40, pp. 913-920, May 1994.
- [41] V.K. Wei, “Generalized Hamming weights for linear codes,” *IEEE Trans. Inform. Theory*, vol. IT-37, pp. 1412-1418, Sept. 1991.
- [42] V.K. Wei and K. Yang, “On the generalized Hamming weights of product codes,” *IEEE Trans. Inform. Theory*, vol. IT-39, pp. 1709-1713, Sept. 1993.
- [43] E.J. Weldon, “New generalizations of the Reed-Muller codes. Part II: nonprimitive codes,” *IEEE Trans. Inform. Theory*, vol. IT-14, pp. 199-205, 1968.
- [44] X.-W. Wu, “Generalized Hamming weights of some classes of projective codes,” *Ph.D. Thesis*, Institute of System Sciences, Beijing, May 1995.