AAECC (2019) 30:233–242
https://doi.org/10.1007/s00200-018-0369-8

ORIGINAL PAPER

A note on the generalized Hamming weights of Reed–Muller codes

Peter Beelen[1]

Received: 3 July 2018 / Revised: 8 August 2018 / Accepted: 8 August 2018 / Published online: 18 August 2018

Abstract
In this note, we give a very simple description of the generalized Hamming weights of Reed–Muller codes. For this purpose, we generalize the well-known Macaulay representation of a nonnegative integer and state some of its basic properties.

Keywords Reed–Muller code · Macaulay decomposition · Generalized Hamming weight

Mathematics Subject Classification 11H71 · 94B27

1 Preliminaries

Let $\mathbb{F}_q$ be the finite field with q elements and denote by $\mathbb{A}^m := \mathbb{A}^m(\mathbb{F}_q)$ the m-dimensional affine space defined over $\mathbb{F}_q$. This space consists of q^m points $(a_1, \ldots, a_m)$ with $a_1, \ldots, a_m \in \mathbb{F}_q$. Let $T(m) := \mathbb{F}_q[x_1, \ldots, x_m]$ denote the ring of polynomials in m variables and coefficients in $\mathbb{F}_q$. Further let $T_{\le d}(m)$ be the set of polynomials in $T(m)$ of total degree at most d. A monomial $X_1^{\alpha_1} \cdots X_m^{\alpha_m}$ is called reduced if $(\alpha_1, \ldots, \alpha_m) \in \{0, 1, \ldots, q-1\}^m$. Similarly a polynomial $f \in T(m)$ is called reduced if it is an $\mathbb{F}_q$-linear combination of reduced monomials. We denote the set of reduced polynomials by $T^{\text{red}}(m)$ and define $T^{\text{red}}_{\le d}(m) := T_{\le d}(m) \cap T^{\text{red}}(m)$.

One reason for considering reduced polynomials comes from coding theory. Indeed, Reed–Muller codes are obtained by evaluating certain polynomials in the points of $\mathbb{A}^m$, but the evaluation map

$$\text{Ev} : T(m) \to \mathbb{F}_q^{q^m}, \quad \text{defined by } \text{Ev}(f) = (f(P))_{P \in \mathbb{A}^m}$$

✉ Peter Beelen
pabe@dtu.dk

1 Department of Applied Mathematics and Computer Science, Technical University of Denmark, 2800 Kongens Lyngby, Denmark

is not injective. However, its restriction to $T^{\text{red}}(m)$ is. In fact, the kernel of Ev consists precisely of the ideal $I \subset T(m)$ generated by the polynomials $x_i^q - x_i$ $(1 \le i \le m)$. Working with reduced polynomials is simply a convenient way to take this into account, since for two reduced polynomials $f_1, f_2 \in T(m)$ the equality $f_1 + I = f_2 + I$ holds if and only if $f_1 = f_2$.

The Reed–Muller code $\text{RM}_q(d, m)$ is the set of vectors from $\mathbb{F}_q^{q^m}$ obtained by evaluating polynomials of total degree up to d in the q^m points of $\mathbb{A}^m$, that is to say:

$$\text{RM}_q(d, m) := \{(f(P))_{P \in \mathbb{A}^m} \; : \; f \in T_{\le d}(m)\}.$$

By the above, we also have $\text{RM}_q(d, m) := \{(f(P))_{P \in \mathbb{A}^m} \; : \; f \in T^{\text{red}}_{\le d}(m)\}$ and moreover, we have

$$\dim \text{RM}_q(d, m) = \dim T^{\text{red}}_{\le d}(m). \tag{1}$$

Reed–Muller codes $\text{RM}_q(d, m)$ have been studied extensively for their elegant algebraic properties. Their generalized Hamming weights $d_r(\text{RM}_q(d, m))$ have been determined in [4] by Heijnen and Pellikaan. For a general linear code $C \subseteq \mathbb{F}_q^n$ these are defined as follows:

$$d_r(C) := \min_{D \subseteq C : \dim D = r} |\text{supp}(D)|,$$

where the minimum is taken over all r-dimensional $\mathbb{F}_q$-linear subspaces D of C and where $\text{supp}(D)$ denotes the support of D, that is to say

$$\text{supp}(D) := \{i \; : \; \exists\, (c_1, \dots, c_n) \in D,\; c_i \ne 0\}.$$

In case of Reed–Muller codes, there is a direct relation between generalized Hamming weights and the number of common solutions to systems of polynomial equations. Indeed, if $D \subset \text{RM}_q(d, m)$ is spanned by $(f_i(P))_{P \in \mathbb{A}^m}$ for $f_1, \dots, f_r \in T^{\text{red}}_{\le d}(m)$, then $|\text{supp}(D)| = q^m - |\mathsf{Z}(f_1, \dots, f_r)|$ where $\mathsf{Z}(f_1, \dots, f_r) := \{P \in \mathbb{A}^m \; : \; f_1(P) = \cdots = f_r(P) = 0\}$ denotes the set of common zeros of $f_1, \dots, f_r$ in the m-dimensional affine space $\mathbb{A}^m$ over $\mathbb{F}_q$. Therefore, if we define

$$\bar{e}_r^{\mathbb{A}}(d, m) := \max \left\{ |\mathsf{Z}(f_1, \dots, f_r)| \; : \; f_1, \dots, f_r \in T^{\text{red}}_{\le d}(m) \;\; \text{linearly independent} \right\}, \tag{2}$$

then $d_r(\text{RM}_q(d, m)) = q^m - \bar{e}_r^{\mathbb{A}}(d, m)$. Note that $T^{\text{red}}(m)$ is a vector space over $\mathbb{F}_q$ of dimension q^m and that a reduced polynomial has total degree at most $m(q-1)$. Therefore $T^{\text{red}}(m) = T^{\text{red}}_{\le m(q-1)}(m)$. This implies in particular that $\text{RM}_q(d, m) = \mathbb{F}_q^{q^m}$ for $d \ge m(q-1)$. Therefore, we will always assume that $d \le m(q-1)$.

The result of Heijnen–Pellikaan in [4] on the value of $d_r(\text{RM}_q(d, m))$ can now be restated as follows, see for example [2].

$$\bar{e}_r^{\mathbb{A}}(d, m) = \sum_{i=1}^{m} \mu_i q^{m-i}, \tag{3}$$

where $(\mu_1, \ldots, \mu_m)$ is the r-th m-tuple in descending lexicographic order among all m-tuples $(\beta_1, \ldots, \beta_m) \in \{0, 1, \ldots, q-1\}^m$ satisfying $\beta_1 + \cdots + \beta_m \leq d$.

Following the notation in [4], we denote with $\rho_q(d, m)$ the dimension of $\mathrm{RM}_q(d, m)$. Equation (1) implies that $\rho_q(d, m) = \dim(T^{\mathrm{red}}_{\leq d}(m))$. In particular, we have

$$\rho_q(d, m) = \dim(T_{\leq d}(m)) = \binom{m+d}{d}, \quad \text{if } d \leq q-1, \tag{4}$$

since $T_{\leq d}(m) = T^{\mathrm{red}}_{\leq d}(m)$ if $d < q$. Here as well as later on we use the convention that $\binom{a}{b} = 0$ if $a < b$. In particular we have $\rho_q(d, m) = 0$ if $d < 0$. As shown in [1, §5.4], for the general case $d \leq m(q-1)$, we have

$$\rho_q(d, m) = \dim\left(T^{\mathrm{red}}_{\leq d}(m)\right) = \sum_{i=0}^{d}\sum_{j=0}^{m}(-1)^j\binom{m}{j}\binom{m-1+i-qj}{m-1}. \tag{5}$$

In this note, we will present an easy-to-obtain expression for $\bar{e}^{\mathbb{A}}_r(d, m)$ involving a certain representation of the number $\rho_q(d, m) - r$ that we introduce in the next section.

2 The *d*-th Macaulay representation with respect to *q*

Let d be a positive integer. The d-th Macaulay (or d-binomial) representation, of a nonnegative integer N is a way to write N as sum as certain binomial coefficients. To be precise

$$N = \sum_{i=1}^{d}\binom{s_i}{i},$$

where the s_i integers satisfying $s_d > s_{d-1} > \cdots > s_1 \geq 0$. The usual convention that $\binom{a}{b} = 0$ if $a < b$, is used. For example, the d-th Macaulay representation of 0 is given by $0 = \sum_{i=1}^{d}\binom{i-1}{i}$. Given d and N the integers s_i exist and are unique. The Macaulay representation is among other things used for the study of Hilbert functions of graded modules, see for example [3]. It is well known (see for example [3]) that if N and M are two nonnegative integers with Macaulay representations given by $(k_d, \ldots, k_1)$ and $(\ell_d, \ldots, \ell_1)$ then $N \leq M$ if and only if $(k_d, \ldots, k_1) \preccurlyeq (\ell_d, \ldots, \ell_1)$, where $\preccurlyeq$ denotes the lexicographic order.

For our purposes it is more convenient to define $m_i := s_i - i$. We then obtain

$$N = \sum_{i=1}^{d}\binom{m_i+i}{i}, \tag{6}$$

where m_i are integers satisfying $m_d \geq m_{d-1} \geq \cdots \geq m_1 \geq -1$. The reason for this is that for $d \leq q-1$ we have $\rho_q(d, m) = \binom{m+d}{d}$. Therefore, we can interpret Eq. (6) as a statement concerning dimensions of the Reed–Muller codes $\mathrm{RM}_q(i, m_i)$. For a suitable choice of N, it turns out that the m_i completely determine the value of $\bar{e}^{\mathbb{A}}_r(d, m)$ if $d \leq q-1$. For $d \geq q$, even though the dimension $\rho_q(d, m)$ is not longer given by

$\binom{m+d}{d}$, there exists a variant of the usual d-th Macaulay representation that turns out to be equally meaningful for Reed–Muller codes. Before stating this representation, we give a lemma.

Lemma 2.1 *Let $m \geq 1$ be an integer. We have*

$$\rho_q(d, m) = \sum_{i=0}^{\min\{d,q-1\}} \rho_q(d-i, m-1).$$

Proof Any polynomial $f \in T(m)$ can be seen as a polynomial in the variable X_m with coefficients in $T(m-1)$. This implies that $T(m) = \sum_{i \geq 0} X_m^i T(m)$, where the sum is a direct sum. Similarly we can write

$$T_{\leq d}^{\mathrm{red}}(m) = \sum_{i=0}^{\min\{d,q-1\}} X_m^i T_{\leq d-i}^{\mathrm{red}}(m-1).$$

The result now follows. □

A consequence of this lemma is the following.

Corollary 2.2 *Let $d = a(q-1) + b$ for integers a and b satisfying $a \geq 0$ and $1 \leq b \leq q-1$. Further suppose that $m \geq a$. Then*

$$\rho_q(d, m) - 1 = \sum_{j=0}^{a-1} \sum_{\ell=0}^{q-2} \rho_q(d - j(q-1) - \ell, m - j - 1) + \sum_{i=1}^{b} \rho_q(i, m - a - 1).$$

Proof This follows using Lemma 2.1 repeatedly. First applying the lemma to each sum within the double summation on the right-hand side, we see that

$$\begin{aligned}
&\sum_{j=0}^{a-1} \sum_{\ell=0}^{q-2} \rho_q(d - j(q-1) - \ell, m - j - 1) \\
&\quad = \sum_{j=0}^{a-1} \big(\rho_q(d - j(q-1), m - j) - \rho_q(d - (j+1)(q-1), m - j - 1)\big) \\
&\quad = \rho_q(d, m) - \rho_q(d - a(q-1), m - a) = \rho_q(d, m) - \rho_q(b, m - a).
\end{aligned}$$

Using the same lemma to rewrite the single summation on the right-hand side in Eq. (9) we see that if $m > a$

$$\sum_{i=1}^{b} \rho_q(i, m-a-1) = \rho_q(b, m-a) - \rho_q(0, m-a-1) = \rho_q(b, m-a) - 1,$$

while if $m = a$, the single summation equals 0 and the double summation simplifies to $\rho_q(d, m) - 1$. In either case, we obtain the desired result □

We can now show the following.

Theorem 2.3 *Let $N \geq 0$ and $d \geq 1$ be integers and q a prime power. Then there exist uniquely determined integers $m_1, \dots, m_d$ satisfying*

1. $N = \sum_{i=1}^{d} \rho_q(i, m_i)$,
2. $-1 \leq m_1 \leq \cdots \leq m_d$,
3. *for all i satisfying $1 \leq i \leq d-q+1$, either $m_{i+q-1} > m_i$ or $m_{i+q-1} = m_i = -1$.*

Proof We start by showing uniqueness. Suppose that

$$N = \sum_{i=1}^{d} \rho_q(i, m_i) = \sum_{i=1}^{d} \rho_q(i, n_i) \tag{7}$$

and the integers $n_1, \dots, n_d$ and $m_1, \dots m_d$ satisfy the conditions from the theorem. First of all, if $m_d = -1$ or $n_d = -1$ then $N = 0$. Either assumption implies that $(m_d, \dots, m_1) = (-1, \dots, -1) = (n_d, \dots, n_1)$. Indeed $n_i \geq 0$ or $m_i \geq 0$ for some i directly implies that $N > 0$. Therefore we from now on assume that $m_d \geq 0$ and $n_d \geq 0$. To arrive at a contradiction, we may assume without loss of generality that $n_d \leq m_d - 1$.

Define e to be the smallest integer such that $n_e \geq 0$. Equation (7) can then be rewritten as

$$N = \sum_{i=1}^{d} \rho_q(i, m_i) = \sum_{i=e}^{d} \rho_q(i, n_i) \tag{8}$$

Condition 3 from the theorem implies that $n_{i-q+1} < n_i$ for all i satisfying $e \leq i \leq d$. Now write $d - e + 1 = a(q-1) + b$ for integers a and b satisfying $a \geq 0$ and $1 \leq b \leq q-1$. With this notation, we obtain that for any $0 \leq j \leq a-1$ and $0 \leq \ell \leq q-2$ we have that

$$n_{d-j(q-1)-\ell} \leq n_d - j \leq m_d - j - 1.$$

In particular choosing $j = a-1$ and $\ell = 0$, this implies that $m_d \geq a + n_{q-1+b} \geq a + 1 + n_b \geq a$. Using these observations, we obtain from Eq. (7) that

$$\begin{aligned}
\rho_q(d, m_d) \leq N = \sum_{i=e}^{d} \rho_q(i, n_i) \\
&\leq \sum_{j=0}^{a-1} \sum_{\ell=0}^{q-2} \rho_q(d - j(q-1) - \ell, m_d - j - 1) \\
&\quad + \sum_{i=1}^{b} \rho_q(e + i - 1, m_d - a - 1).
\end{aligned} \tag{9}$$

Applying the same technique as in the proof of Corollary 2.2, we derive that

$$\sum_{j=0}^{a-1}\sum_{\ell=0}^{q-2}\rho_q(d-j(q-1)-\ell,m_d-j-1)=\rho_q(d,m_d)-\rho_q(b+e-1,m_d-a)$$

and Eq. (9) can be simplified to

$$\rho_q(d,m_d)\leq\rho_q(d,m_d)-\rho_q(b+e-1,m_d-a)+\sum_{i=1}^{b}\rho_q(e+i-1,m_d-a-1). \quad (10)$$

For $m_d=a$ the right-hand side equals $\rho_q(d,m_d)-1$, leading to a contradiction. If $m_d>q$, Eq. (10) implies

$$\begin{aligned}\rho_q(b+e-1,m_d-a)&\leq\sum_{i=1}^{b}\rho_q(e+i-1,m_d-a-1)\\&=\sum_{j=0}^{b-1}\rho_q(e+b-1-j,m_d-a-1)\\&<\sum_{j=0}^{\min\{e+b-1,q-1\}}\rho_q(e+b-1-j,m_d-a-1)\\&=\rho_q(b+e-1,m_d-a),\end{aligned}$$

where in the last equality we used Lemma 2.1. Again we arrive at a contradiction. This completes the proof of uniqueness of the d-th Macaulay representation with respect to q.

Now we show existence. Let d, N and q be given. We will proceed with induction on d. For $d=1$, note that $\rho_q(1,m)=m+1$ for any $m\geq-1$. Therefore, for a given $N\geq0$, we can write $N=\rho_q(1,N-1)$.

Now assume the theorem for $d-1$. There exists $m_d\geq-1$ such that

$$\rho_q(d,m_d)\leq N<\rho_q(d,m_d+1). \quad (11)$$

Applying the induction hypothesis on $N-\rho_q(d,m_d)$, we can find $m_{d-1},\ldots,m_1$ satisfying the conditions of the theorem for $d-1$. In particular we have that

1. $N-\rho_q(d,m_d)=\sum_{i=1}^{d-1}\rho_q(i,m_i)$,
2. $-1\leq m_1\leq\cdots\leq m_{d-1}$,
3. $m_{i+(q-1)}>m_i$ for all $1\leq i\leq d-q$.

Clearly this implies that $N=\sum_{i=1}^{d}\rho_q(i,m_i)$, but it is not clear a priori that $m_1,\ldots,m_d$ satisfy conditions 2 and 3 as well. Conditions 2 and 3 would follow once we show that $m_d\geq m_{d-1}$ and either $m_d>m_{d-q+1}$ or $m_d=m_{d-q+1}=-1$. First of all, if $m_d=-1$, then $N=0$ and $(m_d,\ldots,m_1)=(-1,\ldots,-1)$. Hence there is nothing to prove in that case. Assume $m_d \geq 0$. From Eq. (11) and Lemma 2.1 we see that

$$N - \rho_q(d, m_d) < \rho_q(d, m_d + 1) - \rho_q(d, m_d) = \sum_{i=1}^{\min\{d,q-1\}} \rho_q(d - i, m_d). \quad (12)$$

First suppose that $d \leq q - 1$. First of all, Condition 3 is empty in that setting. Further, Eq. (12) implies

$$N - \rho_q(d, m_d) < \sum_{i=1}^{d} \rho_q(d - i, m_d) = \sum_{i=1}^{d-1} \rho_q(d - i, m_d) + 1$$

and hence

$$N - \rho_q(d, m_d) \leq \sum_{i=1}^{d-1} \rho_q(d - i, m_d) = \sum_{j=0}^{d-2} \rho_q(d - 1 - j, m_d) < \rho_q(d - 1, m_d + 1).$$

This shows that $m_{d-1} \leq m_d$ as desired.

Now suppose that $d \geq q$. In this situation Eq. (12) implies

$$N - \rho_q(d, m_d) < \sum_{i=1}^{q-1} \rho_q(d - i, m_d) = \sum_{j=0}^{q-2} \rho_q(d - 1 - j, m_d) < \rho_q(d - 1, m_d + 1).$$

Hence $m_{d-1} \leq m_d$ as before. Finally assume that $m_d \leq m_{d-q+1}$. Then by the previous and Condition 2, we have $m_d = m_{d-1} = \cdots = m_{d-q+1}$. Hence $N \geq \sum_{i=0}^{q-1} \rho_q(d - i, m_d) = \rho_q(d, m_d + 1)$ which is in contradiction with Eq. (11). This concludes the induction step and hence the proof of existence. □

We call the representation of N in the above theorem the d-th Macaulay representation of N with respect to q. One retrieves the usual d-th Macaulay representation letting q tend to infinity. We refer to $(m_d, \ldots, m_1)$ as the coefficient tuple of this representation. A direct corollary of the above is the following.

Corollary 2.4 *The coefficient tuple $(m_d, \ldots, m_1)$ of the d-th Macaulay representation with respect to q of a nonnegative integer N can be computed using the following greedy algorithm: The coefficient m_{d-i} can be computed recursively (starting with $i = 0$) as the unique integer $m_{d-i} \geq -1$ such that*

$$\rho_q(d - i, m_{d-i}) \leq N - \sum_{j=d-i+1}^{d} \rho_q(j, m_j) < \rho_q(d - i, m_{d-i} + 1).$$

Proof From the existence-part of the proof of Theorem 2.3 it follows directly that the given greedy algorithm finds the desired coefficients. □

A further corollary is the following. As before $\preceq$ denotes the lexicographic order.

Corollary 2.5 *Suppose the N and M are two nonnegative integers whose respective coefficient tuples are $(n_d, \ldots, n_1)$ and $(m_d, \ldots, m_1)$. Then*

$$N \leq M \quad \textit{if and only if } (n_d, \ldots, n_1) \preceq (m_d, \ldots, m_1).$$

Proof Assume $(n_d, \ldots, n_1) \preceq (m_d, \ldots, m_1)$. It is enough to show the corollary in case $n_d < m_d$. We know from the previous corollary that n_d and m_d may be determined using the given greedy algorithm. In particular this implies that $n_d < m_d$ implies

$$N < \rho_q(d, n_d + 1) \leq \rho_q(d, m_d) \leq M.$$

Assume that $N \leq M$. We use induction on d. The induction basis is trivial: If $d = 1$, then $m_1 = M - 1$ and $n_1 = N - 1$. For the induction step, note that $N \leq M < \rho_q(d, m_d + 1)$ implies by the greedy algorithm that $n_d \leq m_d$. If $n_d < m_d$, we are done. If $n_d = m_d$, we replace N with $N - \rho_q(d, m_d)$ and M with $M - \rho_q(d, m_d)$ and use the induction hypothesis to conclude that $(n_d, \ldots, n_1) \preceq (m_d, \ldots, m_1)$. □

3 A simple expression for $\bar{e}_r^{\mathbb{A}}(d, m)$

We are now ready to state and prove the relation between the Macaulay representation with respect to q and $\bar{e}_r^{\mathbb{A}}(d, m)$.

Theorem 3.1 *For $1 \leq r \leq \rho_q(d, m)$, let the d-th Macaulay representation of $\rho_q(d, m) - r$ with respect to q be given by*

$$\rho_q(d, m) - r = \sum_{i=1}^{d} \rho_q(i, m_i).$$

Denoting the floor function as $\lfloor \cdot \rfloor$, we have

$$\bar{e}_r^{\mathbb{A}}(d, m) = \sum_{i=1}^{d} \lfloor q^{m_i} \rfloor.$$

Proof We know from Eq. (3) that we need to show that

$$\sum_{i=1}^{d} \lfloor q^{m_i} \rfloor = \sum_{i=1}^{m} \mu_i q^{m-i},$$

with $(\mu_1, \ldots, \mu_m)$ is the r-th element in descending lexicographic order among all m-tuples $(\beta_1, \ldots, \beta_m)$ in $\{0, 1, \ldots, q - 1\}^m$ satisfying $\beta_1 + \cdots + \beta_m \leq d$. First of all note that since $r \geq 1$, we have $\rho_q(d, m) - r < \rho_q(d, m)$. In particular this implies that $m_d \leq m - 1$. Therefore the coefficients of the d-tuple $(m_d, \ldots, m_1)$ are in $\{-1, 0, \ldots, m-1\}$. Now for $1 \leq i \leq m+1$ define $\mu_i := |\{j : m_j = m - i\}|$. Since the d-tuple $(m_d, \ldots, m_1)$ is nonincreasing by Condition 2 from Theorem 2.3, we can reconstruct it uniquely from the $(m+1)$-tuple $(\mu_1, \mu_2, \ldots, \mu_{m+1})$. Moreover, Condition 3 from Theorem2.3, implies that $(\mu_1, \ldots, \mu_m) \in \{0, 1, \ldots, q-1\}^m$, but note that μ_{m+1} could be strictly larger than $q-1$. Further by construction we have $\mu_1 + \cdots + \mu_m + \mu_{m+1} = d$, implying that $\mu_1 + \cdots + \mu_m \leq d$. Note that μ_{m+1} is determined uniquely by $(\mu_1, \ldots, \mu_m)$, since $\mu_0 = d - \mu_1 - \cdots - \mu_m$. Therefore the correspondence between the d-tuples $(m_d, \ldots, m_1)$ of coefficients of the d-th Macaulay representations with respect to q of integers $0 \leq N < \rho_q(d, m)$ and the m-tuples $(\mu_1, \ldots, \mu_m) \in \{0, 1, \ldots, q-1\}^m$ satisfying $\mu_1 + \cdots + \mu_m \leq d$, is a bijection. Moreover by construction we have

$$\sum_{i=1}^{d} \lfloor q^{m_i} \rfloor = \sum_{j=1}^{m+1} \mu_j \lfloor q^{m-j} \rfloor = \sum_{j=1}^{m} \mu_j q^{m-j}.$$

What remains to be shown is that the constructed m-tuple coming from the integer $\rho_q(d, m) - r$ is in fact the r-th in descending lexicographic order. First of all, by Corollary 2.2 we see that for $r = 1$ and $d = aq + b$ that the m-tuple associated to $\rho_q(d, m) - 1$ equals $(q-1, \ldots, q-1, b, 0, \ldots, 0)$, which under the lexicographic order is the maximal m-tuple among all m-tuples $(\beta_1, \ldots, \beta_m) \in \{0, 1, \ldots, q-1\}^m$ satisfying $\beta_1 + \cdots + \beta_m \leq d$. Next we show that the conversion between d-tuples $(m_d, \ldots, m_1)$ to m-tuples $(\mu_1, \ldots, \mu_m)$ preserves the lexicographic order. Suppose therefore that $1 \leq r \leq s \leq \rho_q(d, m)$. We write $N := \rho_q(d, m) - s$ and $M := \rho_q(d, m) - r$. and denote their Macaulay coefficient tuples with $(n_d, \ldots, n_1)$ and $(m_d, \ldots, m_1)$. Since $N \leq M$, Corollary 2.5 implies that $(n_d, \ldots, n_1) \preceq (m_d, \ldots, m_1)$. Also, since these d-tuples are nonincreasing, this implies that their associated m-tuples $(\nu_1, \ldots, \nu_m)$ and $(\mu_1, \ldots, \mu_m)$ satisfy $(\nu_1, \ldots, \nu_m) \preceq (\mu_1, \ldots, \mu_m)$. Indeed assuming without loss of generality that $\nu_1 < \mu_1$ we see that $m_i = n_i = m - 1$ for $d - \nu_1 \leq i \leq d$ but $n_i < m_i = m - 1$ for $i = \nu_1 + 1$. Now the desired result follows immediately. □

Combining this theorem with the greedy algorithm in Corollary 2.4, it is very simple to compute values of $\bar{e}_r^{\mathbb{A}}(d, m)$ or equivalently of $d_r(\mathrm{RM}_q(d, m))$. We illustrate this in the two following examples. The parameters in these example also occur in examples from [4].

Example 3.2 Let $q = 4$, $r = 8$, $d = m = 3$. Since $d \leq q - 1$, we may work with the usual Macaulay representation when applying Theorem 3.1. We have $\rho_q(d, m) = \binom{6}{3} = 20$ and hence

$$\rho_q(d, m) - r = 12 = \binom{5}{3} + \binom{2}{2} + \binom{1}{1} = \rho_4(3, 2) + \rho_4(2, 0) + \rho_4(1, 0)$$

is the 3-rd Macaulay representation of 12. Theorem 3.1 implies that $\bar{e}_8^{\mathbb{A}}(3, 3) = 4^2 + 4^0 + 4^0 = 18$ and hence $d_8(\mathrm{RM}_4(3, 3)) = 64 - 18 = 46$ in accordance with Example 6.10 in [4].

Example 3.3 Let $q = 2$, $r = 10$, $d = 3$ and $m = 5$. We have $\rho_2(3, 5) = 26$ by Eq. (5) and hence applying the greedy algorithm from Corollary 2.4, we compute that

$$\rho_q(d, m) - r = 16 = 15 + 1 + 0 = \rho_2(3, 4) + \rho_2(2, 0) + \rho_2(1, -1)$$

is the 3rd Macaulay representation of 16 with respect to 2. Theorem 3.1 implies that $\bar{e}_{10}^{\mathbb{A}}(3, 3) = 2^4 + 2^0 = 17$ and hence $d_8(\mathrm{RM}_2(3, 5)) = 32 - 17 = 15$ in accordance with Example 6.12 in [4].

Remark 3.4 Theorem 3.1 is somewhat similar in spirit as Theorem 6.8 from [4] in the sense that in both theorems a certain representation in terms of dimensions of Reed–Muller codes is used to give an expression for $d_r(\mathrm{RM}_q(d, m))$. Where we studied decompositions of $\rho_q(d, m) - r$, in [4] the focus was on r itself. This suggest there may exist a duality between the two approaches, but the similarities seem to stop there. The representation in [4] is not the Macaulay representation with respect to q that we have used here. For us it is for example very important that each degree i between 1 and d occurs once in Theorem 2.3 (implying that the greedy algorithm terminates after at most d iterations), while this is not the case in Theorem 6.8 [4]. It could be interesting future work to determine if a deeper lying relationship between the two approaches exists.

References

1. Assmus Jr., E.F., Key, J.D.: Designs and Their Codes. Cambridge University Press, Cambridge (1992)
2. Beelen, P., Datta, M.: Generalized Hamming weights of affine Cartesian codes. Finite Fields Appl. **51**, 130–145 (2018)
3. Green, M.: Restrictions of linear series to hyperplanes, and some results of Macaulay and Gotzmann. In: Ballico, E., Ciliberto, C. (eds.) Algebraic Curves and Projective Geometry. Lecture Notes in Mathematics, vol 1389, pp. 76–86. Springer, Berlin (1989)
4. Heijnen, P., Pellikaan, R.: Generalized Hamming weights of q-ary Reed–Muller codes. IEEE Trans. Inf. Theory **44**(1), 181–196 (1998)