Journal of Pure and Applied Algebra 224 (2020) 106385

Contents lists available at ScienceDirect

Journal of Pure and Applied Algebra

www.elsevier.com/locate/jpaa

Pure resolutions, linear codes, and Betti numbers

Sudhir R. Ghorpade [a,*,1], Prasant Singh [b,2]

[a] *Department of Mathematics, Indian Institute of Technology Bombay, Powai, Mumbai 400076, India*
[b] *Department of Mathematics and Statistics, UiT The Arctic University of Norway, N-9037 Tromsø, Norway*

A R T I C L E I N F O

Article history:
Received 25 October 2019
Received in revised form 23 March 2020
Available online 3 April 2020
Communicated by S. Iyengar

MSC:
13D02; 94B05; 05B25; 51E20

A B S T R A C T

We consider the minimal free resolutions of Stanley-Reisner rings associated to linear codes and give an intrinsic characterization of linear codes having a pure resolution. We use this characterization to quickly deduce the minimal free resolutions of Stanley-Reisner rings associated to MDS codes as well as constant weight codes. We also deduce that the minimal free resolutions of Stanley-Reisner rings of first order Reed-Muller codes are pure, and explicitly describe the Betti numbers. Further, we show that in the case of higher order Reed-Muller codes, the minimal free resolutions are almost always not pure. The nature of the minimal free resolution of Stanley-Reisner rings corresponding to several classes of two-weight codes, besides the first order Reed-Muller codes, is also determined.

1. Introduction

One of the interesting developments in algebraic coding theory in the recent past is the association of a fine set of invariants, called *Betti numbers*, to linear error correcting codes. This is due to Johnsen and Verdure [16] and their idea is as follows. Some basic terminology used below is reviewed in the next section.

Let C be a q-ary linear code of length n and dimension k and let H be a parity check matrix of C. The vector matroid corresponding to H is a pure simplicial complex, say Δ, and its Stanley-Reisner ring R_Δ over $\mathbb{F}_q$ is a finitely generated standard graded $\mathbb{F}_q$-algebra of dimension $n-k$. As such it has a minimal graded free resolution. Moreover, Δ is shellable, thanks to a classical result that goes back to Provan [22] (see also Björner [4, §7.3]). Hence R_Δ is Cohen-Macaulay. (See, for example, [13, Ch. 6, §2].) So by the

* Corresponding author.
E-mail addresses: srg@math.iitb.ac.in (S.R. Ghorpade), psinghprasant@gmail.com (P. Singh).

[1] Sudhir Ghorpade is partially supported by DST-RCN grant INT/NOR/RCN/ICT/P-03/2018 from the Dept. of Science & Technology, Govt. of India, MATRICS grant MTR/2018/000369 from the Science & Engg. Research Board, and IRCC award grant 12IRAWD009 from IIT Bombay.
[2] Prasant Singh is supported by a postdoctoral fellowship from grant 280731 from the Research Council of Norway.

https://doi.org/10.1016/j.jpaa.2020.106385
0022-4049/

Auslander-Buchsbaum formula, the length of any minimal free resolution of R_Δ is $n-(n-k)=k$, and it looks like

$$F_k \longrightarrow F_{k-1} \longrightarrow \cdots \longrightarrow F_1 \longrightarrow F_0 \longrightarrow R_\Delta \longrightarrow 0 \tag{1}$$

where $F_0 = R := \mathbb{F}_q[X_1, \ldots, X_n]$ and each F_i is a graded free R-module of the form

$$F_i = \bigoplus_{j \in \mathbb{Z}} R(-j)^{\beta_{i,j}} \quad \text{for } i = 0, 1, \ldots, k. \tag{2}$$

The nonnegative integers $\beta_{i,j}$ thus obtained depend only on C (and not on the choice of H or the minimal free resolution of R_Δ), and are the *Betti numbers* of C. Thus we may refer to (1) as a (graded minimal free) *resolution* of C. Such a resolution is said to be *pure* of type $(d_0, d_1, \ldots, d_k)$ if for each $i = 0, 1, \ldots, k$, the Betti number $\beta_{i,j}$ is nonzero if and only if $j = d_i$. If, in addition, $d_0, d_1, \ldots, d_k$ are consecutive, then the resolution is said to be *linear*. Johnsen and Verdure [16] showed that the Betti numbers of a code C contain information about all the generalized Hamming weights $d_i(C)$ of C. In fact, they showed that

$$d_i(C) = \min\{j : \beta_{i,j} \neq 0\} \quad \text{for } i = 1, \ldots, k. \tag{3}$$

More recent work of Johnsen, Roksvold and Verdure [18] shows that the Betti numbers of C and its elongations determine the so-called generalized weight polynomial of C. Thus, if we combine this with the results of Jurrius and Pellikaan [19], then we obtain a direct relation between the generalized weight enumerator of C and the Betti numbers of C and of its elongations.

It is clear therefore that explicit determination of Betti numbers of codes would be useful and interesting. On the other hand, it is usually a hard problem, except in some special cases. The simplest class of codes for which Betti numbers are completely determined is that of MDS codes where the minimal free resolution is linear. The next case is that of simplex codes or dual Hamming codes, which are essentially the prototype of constant weight codes (indeed, by a classical result of Bonisoli [6], every constant weight code is a concatenation of simplex codes, possibly with added 0-coordinates). For such codes, the Betti numbers were explicitly determined by Johnsen and Verdure in another paper [17]. In this case, it turns out that the resolution is pure, although not necessarily linear.

In general, Betti numbers of pure resolutions are relatively easy to determine, thanks to a formula of Herzog and Kühl [14], which in the case of linear codes provides an expression for the Betti numbers in terms of the generalized Hamming weights. So the result for simplex codes can be deduced from it if one knows that their (minimal free) resolutions are necessarily pure. Partly with this in view, we consider the question of obtaining an intrinsic characterization for a linear code to have a pure resolution. A complete characterization is given in Theorem 3.6. This is then applied to show that the first order Reed-Muller codes have a pure resolution and all their Betti numbers can be described explicitly. On the other hand, we show that Reed-Muller codes of order 2 or more do not, in general, have a pure resolution. As a corollary, it is seen that the property of admitting a pure resolution is not preserved when passing to the dual.

The first order Reed-Muller codes are examples of two-weight codes, and it is natural to ask if a similar result holds for every two-weight code. However, unlike constant weight codes, the structure of two-weight codes is far more complicated and it is a topic of considerable research in coding theory and finite projective geometry. We refer to the survey of Calderbank and Kantor [8] and the references therein for a variety of examples of two-weight codes. We also take up the question of determining the Betti numbers of many of these codes. It is seen that the resolution is not always pure and thus we can not appeal to the Herzog-Kühl formula. Nonetheless, we succeed in determining the Betti numbers of many two-weight codes, partly by using a set of equations due to Boij and Söderberg [5]. It appears that the technique of Boij-Söderberg equations used here could be fruitful in the determination of Betti numbers of many important classes of linear codes.

We remark that although our results on the Betti numbers of simplex and first order Reed-Muller codes using the Herzog-Kühl formula were obtained independently in early 2015, Trygve Johnsen [15] has informed us that similar formulas are obtained in the Ph.D. thesis of Armenoff [1] and the Master's thesis of Karpova [21]. In any case, our emphasis here is on the general characterization of purity, applications to Reed-Muller codes that are not only of first order, but also of higher order, and the determination of Betti numbers of many two-weight codes.

2. Preliminaries

Fix, throughout this paper, positive integers n, k with $k \leq n$ and a finite field $\mathbb{F}_q$ with q elements. We denote by $[n]$ the set $\{1, \ldots, n\}$ of first n positive integers. Also, $2^{[n]}$ denotes the set of all subsets of $[n]$. For any finite set σ, we denote by $|\sigma|$ the cardinality of σ. By a $[n, k]_q$-code, we shall mean a q-ary linear code of length n and dimension k, i.e., a k-dimensional subspace of $\mathbb{F}_q^n$.

2.1. Codes and matroids

Let C be a $[n, k]_q$-code and let H be a parity check matrix of C. For $i \in [n]$, let H_i denote the i-th column of H. Define

$$\Delta := \{\sigma \in 2^{[n]} : \{H_i : i \in \sigma\} \text{ is linearly independent over } \mathbb{F}_q\}.$$

The ordered pair $([n], \Delta)$ is a matroid, and we call it the *matroid associated to the code* C. Elements of Δ are called *independent sets* of this matroid. A maximal independent set in Δ is called a *basis* of the matroid. It is well-known that every basis of a matroid has the same cardinality and this number is called the *rank* of the matroid. If $\sigma \subseteq [n]$ and if we let $\Delta|\sigma := \{\tau \in \Delta : \tau \subseteq \sigma\}$, then $(\sigma, \Delta|\sigma)$ is a matroid, called the *restriction* of the matroid $([n], \Delta)$ to σ; the rank of this restricted matroid is called the *rank* of σ and denoted by $r(\sigma)$; the difference $|\sigma| - r(\sigma)$ is denoted by $\eta(\sigma)$ and called the *nullity* of σ. Evidently, the rank of the matroid $([n], \Delta)$ is the rank of H, which is $n - k$, and so the nullity of any $\sigma \subseteq [n]$ ranges from 0 to k. For $0 \leq i \leq k$, we define

$$N_i := \{\sigma \subseteq [n] : \eta(\sigma) = i\}.$$

2.2. Stanley-Reisner rings and Betti numbers

Suppose $([n], \Delta)$ is as in the previous subsection. Then Δ is a simplicial complex. We denote by I_Δ the ideal of the polynomial ring $R := \mathbb{F}_q[X_1, \ldots, X_n]$ generated by all monomials of the form $\prod_{i \in \tau} X_i$, where $\tau \in 2^{[n]} \setminus \Delta$. The quotient $R_\Delta = R/I_\Delta$ is called the *Stanley-Reisner ring* or the *face ring* associated to Δ. As noted in the Introduction, R_Δ has a minimal free resolution of the form (1). Furthermore, since I_Δ is a monomial ideal generated by squarefree monomials, we can choose the free R-modules F_i in (1) to be not only $\mathbb{Z}$-graded as in (2), but also $\mathbb{Z}^n$-graded so as to write

$$F_i = \bigoplus_{\sigma \in \mathbb{Z}^n} R(-\sigma)^{\beta_{i,\sigma}} \quad \text{for } i = 1, \ldots, k. \tag{4}$$

In fact, the $\mathbb{Z}^n$-graded Betti numbers $\beta_{i,\sigma}$ have the property that $\beta_{i,\sigma} = 0$ unless the n-tuple $\sigma = (\sigma_1, \ldots, \sigma_n)$ has all its coordinates in $\{0, 1\}$. Such n-tuples in $\{0, 1\}^n$ can be naturally identified with subsets of $[n]$ where $(\sigma_1, \ldots, \sigma_n)$ corresponds to the subset $\{i \in [n] : \sigma_i = 1\}$ of $[n]$ that we shall also denote by σ. Thus, we may index the direct sum in (4) by $\sigma \in 2^{[n]}$. The relation between the $\mathbb{Z}$-graded and $\mathbb{Z}^n$-graded Betti numbers is simply that

$$\beta_{i,j} = \sum_{|\sigma|=j} \beta_{i,\sigma} \quad \text{for } i = 1, \ldots, k. \tag{5}$$

Johnsen and Verdure [16] proved an important relationship between the $\mathbb{Z}^n$-graded Betti numbers and subsets of a given nullity. Namely, for $1 \le i \le k$ and $\sigma \subseteq [n]$,

$$\beta_{i,\sigma} \neq 0 \iff \sigma \in N_i \text{ and } \sigma \text{ is a minimal element of } N_i. \tag{6}$$

This result, which can perhaps be traced back to Stanley [23, p. 59], will be very useful for us in the sequel. Note also that if $\mu_1, \ldots, \mu_t$ are squarefree monomials in R which constitute a minimal set of generators of I_Δ and if $\sigma_j \in 2^{[n]}$ denotes the support of μ_j (so that $\mu_j = \prod_{i \in \sigma_j} X_i$) for $1 \le j \le t$, then without loss of generality, we can take the first free R-module in (4) to be

$$F_1 = \bigoplus_{j=1}^{t} R(-\sigma_j). \tag{7}$$

Finally, we recall the following general result, which was alluded to in the Introduction. A proof can be found in [5]. We note that a graded module M over a polynomial ring R having projective dimension k will have a minimal free resolution such as (1) with R_Δ replaced by M, except in this case F_0 may not be equal to R. In general, we let $\beta_i := \mathrm{rank}_R(F_i) = \sum_j \beta_{i,j}$. Note that if M has a pure resolution of type $(d_0, d_1, \ldots, d_k)$, then $\beta_i := \beta_{i,d_i}$ for $i = 0, 1, \ldots, k$.

Theorem 2.1 *(Boij-Söderberg). Let R be the polynomial ring over a field and let M be a graded R-module of finite projective dimension k. Then M is Cohen-Macaulay if and only if its graded Betti numbers satisfy the equations*

$$\sum_{i=0}^{k} \sum_{j \in \mathbb{Z}} (-1)^i j^\ell \beta_{i,j} = 0 \quad \textit{for } \ell = 0, \ldots, k-1. \tag{8}$$

In particular, if the minimal free resolution of M is pure of type $(d_0, d_1, \ldots, d_k)$, then (8) implies the Herzog-Kühl formula [14]:

$$\beta_i = \beta_0 \left| \prod_{j \neq i} \frac{d_j}{(d_j - d_i)} \right| \quad \textit{for } i = 1, \ldots, k, \tag{9}$$

As noted in the Introduction, Stanley-Reisner rings associated to linear codes (or more generally, simplicial complexes corresponding to matroids) are Cohen-Macaulay, and hence the above theorem is applicable; moreover, in this case, $\beta_0 = 1$. If a $[n,k]_q$-code C has a pure resolution of type $(d_0, \ldots, d_k)$, then $d_0 = 0$ and for $1 \le i \le k$, d_i is precisely the i-th generalized Hamming weight of C, thanks to (3); we will refer to $\beta_i = \beta_{i,d_i}$ as the *Betti numbers of* C in this case.

3. Pure resolution of linear codes

In this section we will give a characterization of the purity of the resolution of the Stanley-Reisner ring associated to a linear code in terms of the support weight of certain subcodes of the code. We will then outline some simple applications.

Let C be a $[n,k]_q$-code and let $H = [H_1 \dots H_n]$ be a parity check matrix of C, where, as before, H_i denotes the ith column of H. For any subset σ of $[n]$, define $S(\sigma)$ to be the subspace $\langle H_i : i \in \sigma \rangle$ of $\mathbb{F}_q^{n-k}$ spanned by the columns of H indexed by σ. Note that $r(\sigma) = \dim S(\sigma)$. Let us also define a related subspace of $\mathbb{F}_q^n$ by

$$\widehat{S}(\sigma) := \{x = (x_1, \dots, x_n) \in \mathbb{F}_q^n : x_i = 0 \text{ for } i \notin \sigma \text{ and } \sum_{i \in \sigma} x_i H_i = 0\}.$$

Recall that for any subcode D of C, i.e., a subspace D of C, the *support* of D is the set $\mathrm{Supp}(D)$ of all $i \in [n]$ for which there is $x = (x_1, \dots, x_n) \in D$ with $x_i \neq 0$; further, we let $\mathrm{wt}(D) := |\mathrm{Supp}(D)|$, and call this the *weight* of D.

Lemma 3.1. *Let $\sigma \subseteq [n]$. Then $\widehat{S}(\sigma)$ is a subcode of C and $\mathrm{Supp}(\widehat{S}(\sigma)) \subseteq \sigma$.*

Proof. Since $C = \{x = (x_1, \dots, x_n) \in \mathbb{F}_q^n : \sum_{i=1}^n x_i H_i = 0\}$, it is clear that $\widehat{S}(\sigma)$ is a subcode of C. The inclusion $\mathrm{Supp}(\widehat{S}(\sigma)) \subseteq \sigma$ is obvious. □

For any $\sigma \subseteq [n]$, let $\mathbb{F}_q^\sigma$ denote the set of all ordered $|\sigma|$-tuples $(x_i)_{i \in \sigma}$ of elements of $\mathbb{F}_q$ indexed by σ. Consider the map

$$\phi_\sigma : \mathbb{F}_q^\sigma \to S(\sigma) \quad \text{defined by} \quad \phi_\sigma(x) = \sum_{i \in \sigma} x_i H_i. \tag{10}$$

Clearly ϕ_σ is a surjective $\mathbb{F}_q$-linear map.

Lemma 3.2. *Let $\sigma \subseteq [n]$ and let ϕ_σ be as in (10). Then $\ker \phi_\sigma$ is isomorphic (as a $\mathbb{F}_q$-vector space) to $\widehat{S}(\sigma)$. Consequently,*

$$\dim S(\sigma) = |\sigma| - \dim \widehat{S}(\sigma). \tag{11}$$

Proof. Consider the map $\psi : \mathbb{F}_q^\sigma \longrightarrow \mathbb{F}_q^n$ given by $\psi(x) = (v_1, v_2, \dots, v_n)$, where

$$v_i = \begin{cases} x_i & \text{if } i \in \sigma, \\ 0 & \text{otherwise.} \end{cases}$$

It is easily seen that the restriction of ψ to $\ker \phi_\sigma$ gives an isomorphism of $\ker \phi_\sigma$ onto $\widehat{S}(\sigma)$. The second assertion follows from the Rank-Nullity theorem. □

For $0 \le i \le k$, let $\mathbb{G}_i(C)$ denote the Grassmannian of all i-dimensional subspaces of C. We call $D \in \mathbb{G}_i(C)$ an *i-minimal subcode* of C if $\mathrm{Supp}(D)$ is minimal among the supports of all i-dimensional subcodes of C, i.e., $\mathrm{Supp}(D') \nsubseteq \mathrm{Supp}(D)$ for any $D' \in \mathbb{G}_i(C)$ with $D' \neq D$. We let

$$\mathcal{D}_i = \text{the set of all } i\text{-minimal subcodes of } C.$$

Note that if $i = 0$, then the only element of $\mathbb{G}_i(C)$ is $\{0\}$, and its support is $\emptyset$, which is clearly i-minimal. Moreover, $r(\emptyset) = 0 = |\emptyset|$, and thus $\mathrm{Supp}(\{0\}) \in N_0$. In fact, a more general result holds. Recall (from § 2.1) that N_i denotes the set of all subsets of $[n]$ of nullity i.

Proposition 3.3. *Suppose $0 \le i \le k$ and $D \in \mathcal{D}_i$. Then $\mathrm{Supp}(D) \in N_i$.*

Proof. Let $\sigma := \mathrm{Supp}(D)$. Then for any $x \in D$, clearly $x_i = 0$ for all $i \in [n]$ with $i \notin \sigma$. Also, since $D \subseteq C$, we see that $\sum x_i H_i = 0$ for each $x = (x_1, \dots, x_n) \in D$. It follows that $D \subseteq \widehat{S}(\sigma)$. In particular, $\dim \widehat{S}(\sigma) \geq i$. Further, by Lemma 3.1,

$$\sigma = \mathrm{supp}(D) \subseteq \mathrm{supp}(\widehat{S}(\sigma)) \subseteq \sigma.$$

Therefore $\mathrm{supp}(\widehat{S}(\sigma)) = \sigma$. In case $\dim(\widehat{S}(\sigma)) > i$, we can choose some $j \in \sigma$ and observe that $\{x \in \widehat{S}(\sigma) : x_j = 0\}$ is a subspace of dimension $\dim \widehat{S}(\sigma) - 1$, and its support is contained in $\sigma \setminus \{j\}$. This can be used to construct an i-dimensional subcode D' of $\widehat{S}(\sigma)$ with support a proper subset of σ. But then the minimality of the support of D is contradicted. It follows that $\dim \widehat{S}(\sigma) = i$, and hence $D = \widehat{S}(\sigma)$. Now equation (11) shows that $r(\sigma) = |\sigma| - i$, that is, $\sigma \in N_i$. $\square$

It turns out that a partial converse of the above proposition is also true.

Proposition 3.4. *Suppose $0 \leq i \leq k$ and σ is a minimal element of N_i (with respect to inclusion). Then there exists $D \in \mathcal{D}_i$ such that $\sigma = \mathrm{Supp}(D)$.*

Proof. Since $\sigma \in N_i$, we see that $\dim S(\sigma) = r(\sigma) = |\sigma| - i$. Hence, equation (11) implies that $\dim \widehat{S}(\sigma) = i$. Let $D := \widehat{S}(\sigma)$ and $\sigma' := \mathrm{Supp}(D)$. Then D is an i-dimensional subcode of C and by Lemma 3.1, $\sigma' \subseteq \sigma$. We claim that $D \in \mathcal{D}_i$. To see this, assume the contrary. Then there exists $D' \in \mathbb{G}_i(C)$ with $D' \neq D$ such that $\mathrm{Supp}(D') \subsetneq \sigma'$. Replacing D' by an i-dimensional subcode with smaller support, if necessary, we may assume that D' is i-minimal. But then by Proposition 3.3, $\mathrm{Supp}(D') \in N_i$, which contradicts the minimality of σ in N_i. Thus, $D \in \mathcal{D}_i$. $\square$

Corollary 3.5. *Suppose $0 \leq i \leq k$ and $\sigma \subseteq [n]$. Then σ is a minimal element of N_i if and only if there exists an i-minimal subcode D of C with $\mathrm{Supp}(D) = \sigma$.*

Proof. Follows from Propositions 3.3 and 3.4. $\square$

Theorem 3.6. *Let C be an $[n, k]_q$ code and $d_1 < \cdots < d_k$ its generalized Hamming weights. Then any $\mathbb{N}$-graded minimal free resolution of C is pure if and only if for each $i = 1, \dots, k$, all the i-minimal subcodes of C have support weight d_i.*

Proof. From (6) and Corollary 3.5, we see that for $1 \leq i \leq k$ and $\sigma \subseteq [n]$,

$$\beta_{i,\sigma} \neq 0 \iff \sigma = \mathrm{Supp}(D) \text{ for some } D \in \mathcal{D}_i. \tag{12}$$

Thus, the desired result follows from (3) and (5). $\square$

Corollary 3.7. *The Betti numbers at the first step of a $[n, k]_q$-code C are given by*

$$\beta_{1,j} = |\{D \in \mathcal{D}_1 : \mathrm{wt}(D) = j\}| \text{ for any nonnegative integer } j.$$

Proof. Follows from (7) and (12). $\square$

Remark 3.8. Let C be an $[n, k]_q$ code and h a positive integer $\leq k$. Given a resolution of C, say (1), by its *left part after h steps*, we mean the exact sequence

$$F_k \longrightarrow F_{k-1} \longrightarrow \cdots \longrightarrow F_h$$

which is a minimal free resolution of the cokernel of the last map $F_{h+1} \longrightarrow F_h$. Now let $d_1 < \cdots < d_k$ be the generalized Hamming weights of C. It is clear that the proof of Theorem 3.6 also shows that the left part after h steps of any $\mathbb{N}$-graded minimal free resolution of C is pure if and only if for each $i = h, \ldots, k$, all the i-minimal subcodes of C have support weight d_i.

We now show how a characterization due to Johnsen and Verdure [16] of MDS codes can be deduced from our characterization of purity, and moreover, how the minimal free resolution of an MDS code can then be readily determined using the Herzog-Kühl formula.

Corollary 3.9. *Let C be a nondegenerate $[n,k]_q$-code and h a positive integer $\leq k$. Then C is h-MDS if and only if the left part of its resolution after h steps is linear. In particular, C is an MDS code if and only if its resolution is linear. Moreover, if C is MDS, then its Betti numbers are given by*

$$\beta_i = \binom{n-k+i-1}{i-1}\binom{n}{k-i} \quad \textit{for } i = 1, \ldots, k.$$

Proof. Suppose the left part after h steps of a resolution of C is linear. Since C is nondegenerate, $d_k = n$, and so from the linearity together with equation (3), we obtain $d_i = n - k + i$ for $h \leq i \leq k$. Taking $i = h$, we see that C is h-MDS.

Conversely, suppose C is h-MDS. Then from the strict monotonicity of generalized Hamming weights [25, Thm. 1], we see that $d_i = n - k + i$ for $h \leq i \leq k$. Now fix $i \in \{h, \ldots, k\}$ and let D be an i-minimal subcode of C. Let $\sigma := \mathrm{Supp}(D)$. By Proposition 3.3, $\sigma \in N_i$. Also, $n - k + i = d_i \leq |\sigma|$. Consequently, $n - k \leq |\sigma| - i = r(\sigma) \leq n - k$. It follows that $|\mathrm{Supp}(D)| = d_i$. Thus, in view of Remark 3.8, we conclude that the left part after h steps of any resolution of C is linear.

Now assume that C is MDS. Then, in view of (9), we see that for $1 \leq i \leq k$,

$$\beta_i = \prod_{j \neq i} \frac{d_j}{|d_j - d_i|} = \prod_{j \neq i} \frac{n-k+j}{|j-i|} = \left(\prod_{j=1}^{i-1} \frac{n-k+j}{i-j}\right)\left(\prod_{j=i+1}^{k} \frac{n-k+j}{j-i}\right),$$

and an easy calculation shows that this is equal to $\binom{n-k+i-1}{i-1}\binom{n}{k-i}$. $\square$

Let us also show how the result of Johnsen and Verdure [17] about the minimal free resolution of constant weight codes can be deduced from Theorem 3.6.

Corollary 3.10. *Let C be an $[n,k]_q$-code in which each nonzero codeword has constant weight d. Then the $\mathbb{N}$-graded resolution of C is pure. Moreover, the generalized Hamming weights (or the shifts) and the Betti numbers of C are given by*

$$d_i = \frac{q^{k-1}(q^i - 1)}{q^{i-1}(q-1)} \quad \textit{and} \quad \beta_i = \begin{bmatrix} k \\ i \end{bmatrix}_q q^{\frac{i(i-1)}{2}}, \quad \textit{for } i = 1, \ldots, k,$$

where $\begin{bmatrix} k \\ i \end{bmatrix}_q$ denotes the Gaussian binomial coefficient.

Proof. It is well-known (see, e.g., [20, Thm. 1]) that every j-dimensional subcode of the constant weight code C has support weight d_j, where

$$d_j = \frac{d(q^j - 1)}{q^{j-1}(q-1)} \quad \text{for } j = 1, \ldots, k.$$

Hence, by Theorem 3.6, C has a pure resolution. Evidently, the numbers d_i defined above are the generalized Hamming weights of C. Moreover, for $i, j = 1, \dots, k$,

$$d_i - d_j = \frac{d(q^{i-j}-1)}{q^{i-1}(q-1)}, \quad \text{if } j < i, \text{ whereas} \quad d_j - d_i = \frac{d(q^{j-i}-1)}{q^{j-1}(q-1)}, \quad \text{if } j > i.$$

Hence, the Herzog-Kühl formula (9) implies that for $i = 1, \dots, k$,

$$\beta_i = \prod_{j \neq i} \frac{d_j}{|d_j - d_i|} = \left(\prod_{j=1}^{i-1} \frac{q^{i-j}(q^j-1)}{q^{i-j}-1} \right) \left(\prod_{j=i+1}^{k} \frac{q^j-1}{q^{j-i}-1} \right) = q^{\frac{i(i-1)}{2}} \begin{bmatrix} k \\ i \end{bmatrix}_q,$$

where the last equality follows by noting that for $i = 1, \dots, k$,

$$\begin{bmatrix} k \\ i \end{bmatrix}_q = \begin{bmatrix} k \\ k-i \end{bmatrix}_q = \frac{(q^k-1)(q^{k-1}-1)\cdots(q^{i+1}-1)}{(q^{k-i}-1)(q^{k-i-1}-1)\cdots(q-1)} = \prod_{j=i+1}^{k} \frac{q^j-1}{q^{j-i}-1}.$$

This proves the desired result. □

4. Reed-Muller codes

In this section we consider generalized Reed-Muller codes and prove that the resolution of the first order Reed-Muller code is pure, whereas for other Reed-Muller codes, it is non-pure. Let us begin by recalling the construction of (generalized) Reed-Muller codes. Fix integers r, m such that $m \geq 1$ and $0 \leq r \leq m(q-1)$. Define

$$V_q(r,m) = \{f \in \mathbb{F}_q[X_1, \dots, X_m] : \deg f \leq r \text{ and } \deg_{X_i} f < q \text{ for } i = 1, \dots, m\}.$$

Fix an ordering $P_1, \dots, P_{q^m}$ of the elements of $\mathbb{F}_q^m$. Consider the evaluation map

$$\mathrm{Ev} : V_q(r,m) \to \mathbb{F}_q^{q^m} \quad \text{defined by} \quad f \mapsto c_f := (f(P_1), \dots, f(P_{q^m})).$$

The image of Ev is called the *generalized Reed-Muller code of order* r, and we denote it by $\mathcal{RM}_q(r,m)$. It is well-known that $\mathcal{RM}_q(r,m)$ is an $[n,k,d]_q$-code, with

$$n = q^m, \quad k = \sum_{i=0}^{m} (-1)^i \binom{m}{i} \binom{m+r-iq}{m}, \quad \text{and} \quad d = (q-s)q^{m-t-1}, \tag{13}$$

where t, s are unique integers satisfying $r = t(q-1)+s$ and $0 \leq s \leq q-2$. Further, for any $\omega_0, \omega_1, \dots, \omega_t \in \mathbb{F}_q$ with $\omega_0 \neq 0$ and any distinct $\omega'_1, \dots, \omega'_s \in \mathbb{F}_q$, the polynomial

$$f(X_1 \dots, X_m) = \omega_0 \prod_{i=1}^{t} (1 - (X_i - \omega_i)^{q-1}) \prod_{j=1}^{s} (X_{t+1} - \omega'_j)$$

is in $V_q(r,m)$ and $\mathrm{Ev}(f)$ is a minimum weight codeword of $\mathcal{RM}_q(r,m)$. Moreover, up to a (nonhomogeneous) linear substitution in $X_1, \dots, X_m$, every minimum weight codeword of $\mathcal{RM}_q(r,m)$ is of this form; see, e.g., Theorems 2.6.2 and 2.6.3 of [10]. It is also well-known (see, e.g., [2, §5.4]) that the dual of $\mathcal{RM}_q(r,m)$ is given by[3]

[3] Strictly speaking, for the formula (14) to be valid, we should note that the definition of $\mathcal{RM}_q(r,m)$ is meaningful also when $r = -1$ in which case it is the zero code of length q^m.

$$\mathcal{RM}_q(r,m)^\perp = \mathcal{RM}_q(r^\perp, m) \quad \text{where} \quad r^\perp + r + 1 = m(q-1). \tag{14}$$

In particular, if $r = m(q-1)-1$, then $\mathcal{RM}_q(r,m)$ is a MDS code (being the dual of $\mathcal{RM}_q(0,m)$, which is the 1-dimensional code of length q^m generated by the all-1 vector). Also if $r = m(q-1)$, then $\mathcal{RM}_q(r,m)$ is a MDS code, being the full space $\mathbb{F}_q^m$. Finally, if $m = 1$, then $\mathcal{RM}_q(r,m)$ is a Reed-Solomon code, and in particular, a MDS code. Thus, in all these "trivial cases", $\mathcal{RM}_q(r,m)$ has a pure, and in fact, linear, resolution. The following result deals with the first nontrivial case of $r = 1$.

Theorem 4.1. *The $\mathbb{N}$-graded minimal free resolution of the first order Reed-Muller code $\mathcal{RM}_q(1,m)$ is pure and is given by*

$$R(-d_{m+1})^{\beta_{m+1}} \longrightarrow R(-d_m)^{\beta_m} \longrightarrow \cdots \longrightarrow R(-d_1)^{\beta_1} \longrightarrow R$$

where $d_i = q^m - \lfloor q^{m-i} \rfloor$ for $1 \le i \le m+1$, and

$$\beta_i = \begin{cases} q^{\binom{i+1}{2}} \displaystyle\prod_{j=1}^{m-i} \frac{q^{m+1-j}-1}{q^{m+1-i-j}-1} & \text{if } 1 \le i \le m, \\ \displaystyle\prod_{j=1}^{m} (q^j - 1) & \text{if } i = m+1. \end{cases}$$

Proof. First, note that $\dim \mathcal{RM}_q(1,m) = m+1$. Let i be a positive integer $\le m+1$. If $i = m+1$, then the only i-dimensional subcode of $\mathcal{RM}_q(1,m)$ is $\mathcal{RM}_q(1,m)$ itself, and this has support weight q^m. Now suppose $1 \le i \le m$. Let D be a subcode of $\mathcal{RM}_q(1,m)$ of dimension i. Then the support weight of D is clearly

$$q^m - |Z(f_1, \dots, f_i)|,$$

where $f_1, \dots, f_i \in V_q(1,m)$ are linearly independent polynomials whose images under Ev form a basis of D, and where $Z(f_1, \dots, f_i)$ denotes the set of common zeros in $\mathbb{F}_q^m$ of $f_1, \dots, f_i$. Now $f_1 = \cdots = f_i = 0$ is a system of i linearly independent (not necessarily homogeneous) linear equations in m variables, and thus it has either no solutions (when the system is inconsistent) or exactly q^{m-i} solutions (when the system is consistent). Accordingly, the support weight of D is either q^m or $q^m - q^{m-i}$. Moreover, if the former holds, then $\mathrm{Supp}(D) = \{1, \dots, q^m\}$, and so D cannot be an i-minimal subcode of $\mathcal{RM}_q(1,m)$. It follows that all i-minimal subcodes of $\mathcal{RM}_q(1,m)$ have the same support weight $d_i = q^m - \lfloor q^{m-i} \rfloor$ for $1 \le i \le m+1$. Thus, by Theorem 3.6, $\mathcal{RM}_q(1,m)$ has a pure resolution. Consequently, the Betti numbers of $\mathcal{RM}_q(1,m)$ can be determined using the Herzog-Kühl formula (9) as follows.

$$\beta_{m+1} = \prod_{j=1}^{m} \frac{d_j}{d_{m+1} - d_j} = \prod_{j=1}^{m} \frac{q^m - q^{m-j}}{q^{m-j}} = \prod_{j=1}^{m} (q^j - 1),$$

whereas for $1 \le i \le m$,

$$\begin{aligned} \beta_i &= \frac{d_{m+1}}{d_{m+1} - d_i} \prod_{m+1 > j > i} \frac{d_j}{d_j - d_i} \prod_{j<i} \frac{d_j}{d_j - d_i} \\ &= q^i \prod_{j=i+1}^{m} \frac{q^{m-j}(q^j - 1)}{q^{m-j}(q^{j-i} - 1)} \prod_{j=1}^{i-1} \frac{q^{m-j}(q^j - 1)}{q^{m-i}(q^{i-j} - 1)} \end{aligned}$$

$$= q^{\frac{i(i+1)}{2}} \prod_{j=i+1}^{m} \frac{(q^j - 1)}{(q^{j-i} - 1)} = q^{\binom{i+1}{2}} \prod_{j=1}^{m-i} \frac{(q^{m+1-j} - 1)}{(q^{m+1-i-j} - 1)}.$$

This proves the theorem. □

Remark 4.2. Observe that the pure resolution of $\mathcal{RM}_q(1,m)$ in Theorem 4.1 is linear only when either $m = 1$ or $m = 2 = q$. As noted earlier, $\mathcal{RM}_q(1,m)$ is a MDS code in this case.

Next, we shall show that the minimal free $\mathbb{N}$-resolutions of many generalized Reed-Muller codes of order higher than one are not pure. It will be convenient to consider various cases separately. As usual, we shall say that an element c of a linear code C is a *minimal codeword* if either $c = 0$, or if $c \neq 0$ and the support of the 1-dimensional subspace $\langle c \rangle$ of C spanned by c is minimal among the supports of all 1-dimensional subcodes of C. Evidently, a codeword of minimum weight is minimal, but the converse may not be true.

4.1. Binary case

In this subsection we consider the binary case, i.e., when $q = 2$. We will use the following simple, but useful, observation. It is stated, for instance, in Ashikhmin and Barg [3, Lemma 2.1]. The proof is obvious and is omitted.

Lemma 4.3. *Let C be a binary linear code and let $d = d(C)$ be its minimum distance. If $c \in C$ is not a minimal weight codeword, then $c = c_1 + c_2$ for some nonzero $c_1, c_2 \in C$ such that* $\mathrm{Supp}(\langle c_1 \rangle)$ *and* $\mathrm{Supp}(\langle c_2 \rangle)$ *are disjoint and* $\mathrm{Supp}(\langle c_i \rangle) \subsetneq \mathrm{Supp}(\langle c \rangle)$ *for $i = 1, 2$. In particular, if $c \in C$ has* $\mathrm{wt}(c) < 2d$*, then c is a minimal codeword of C.*

The following result shows that all "nontrivial" binary Reed-Muller codes of order greater than 1 have a non-pure resolution.

Proposition 4.4. *Assume that $m \geq 4$ and $1 < r \leq m - 2$. Then any minimal free $\mathbb{N}$-resolution of the binary Reed-Muller code $\mathcal{RM}_2(r,m)$ is not pure.*

Proof. The minimum distance of $\mathcal{RM}_2(r,m)$ is $d := 2^{m-r}$ and if we let

$$Q(X_1, \ldots, X_m) = X_1 X_2 \cdots X_{r-2}(X_{r-1}X_r + X_{r+1}X_{r+2}),$$

then clearly, $Q \in V_2(r,m)$. Moreover, the corresponding codeword $c_Q = \mathrm{Ev}(Q)$ has weight $6 \times 2^{m-r-2} = 3d/2$. Indeed, $Q(a_1, \ldots, a_m) \neq 0$ for $(a_1, \ldots, a_m) \in \mathbb{F}_2^m$ precisely when $a_1 = \cdots = a_{r-2} = 1$, $(a_{r-1}, a_r, a_{r+1}, a_{r+2})$ is one among $(0,1,1,1)$, $(1,0,1,1)$, $(0,0,1,1)$, $(1,1,0,1)$, $(1,1,1,0)$, and $(1,1,0,0)$, while $a_{r+3}, \ldots, a_m \in \mathbb{F}_2$ are arbitrary. Hence, by Lemma 4.3, c_Q is a minimal codeword, but it is clearly not of minimum weight. Thus, the desired result follows from Theorem 3.6. □

Remark 4.5. As Alexander Barg has pointed out to one of us, the last assertion in Lemma 4.3 can be extended to the q-ary case to show that codewords of weight less than $dq/(q-1)$ are minimal in C, where C is a q-ary linear code with minimum distance d. However, for $q > 2$, this is often a restrictive hypothesis, and in the next subsections, we will deal with q-ary Reed-Muller codes using a different strategy.

4.2. The case of $t = 0$

Let t, s be as in (13) so that $r = t(q-1) + s$ and $0 \leq s < q - 1$. We will consider the case of Reed-Muller codes of order $r > 1$ for which $t = 0$ (so that $r = s$). Note that such codes are necessarily non-binary, and in fact, $q \geq 4$. We shall also exclude the case when $m = 1$, since $\mathcal{RM}_q(r, 1)$ is a Reed-Solomon (and hence MDS) code for $1 \leq r \leq (q-1)$.

Proposition 4.6. *Assume that $m \geq 2$ and $1 < r < q-1$. Then any minimal free $\mathbb{N}$-resolution of the Reed-Muller code $\mathcal{RM}_q(r, m)$ is not pure.*

Proof. Choose distinct elements $\omega_1, \ldots, \omega_{r-1} \in \mathbb{F}_q$ and an arbitrary $\omega \in \mathbb{F}_q$. Define

$$Q(X_1, \ldots, X_m) = (X_2 - \omega) \prod_{i=1}^{r-1} (X_1 - \omega_i).$$

Clearly, $Q \in V_q(r, m)$ and the corresponding codeword $c_Q = \mathrm{Ev}(Q)$ has weight $(q - r + 1)(q - 1)q^{m-2}$. On the other hand, by (13), the minimum distance of $\mathcal{RM}_q(r, m)$ is $(q - r)q^{m-1}$. Observe that

$$(q - r + 1)(q - 1)q^{m-2} - (q - r)q^{m-1} = (r - 1)q^{m-2} > 0 \quad \text{since } r > 1.$$

It follows that c_Q is not a minimum weight codeword. If c_Q is a minimal codeword, then Theorem 3.6 implies the desired result. Now suppose c_Q is not a minimal codeword of $\mathcal{RM}_q(r, m)$. Then we can find $F \in V_q(r, m)$ such that c_F is a minimal codeword of $\mathcal{RM}_q(r, m)$ and $\mathrm{Supp}(c_F) \subset \mathrm{Supp}(c_Q)$. Again, if c_F is not a minimal codeword of $\mathcal{RM}_q(r, m)$, then we are done. Otherwise, by the characterization of minimum weight codewords of $\mathcal{RM}_q(r, m)$, we must have

$$F(X_1, \ldots, X_m) = \prod_{j=1}^{r} (L - \omega'_j)$$

for some distinct elements $\omega'_1, \ldots, \omega'_r \in \mathbb{F}_q$ and some nonzero linear polynomial L in $\mathbb{F}_q[X_1, \ldots, X_m]$ that we can assume to be homogeneous (by adjusting ω'_j, if necessary). Write $L = a_1X_1 + \cdots + a_mX_m$. Since $\mathrm{Supp}(c_F) \subset \mathrm{Supp}(c_Q)$, it follows that L vanishes whenever we substitute $X_1 = \omega_i$ for some $i \in \{1, \ldots, r\}$ or we substitute $X_2 = \omega$. In particular, $a_1\omega_1 + a_2X_2 + \cdots + a_mX_m = \omega'_j$ for some $j \in \{1, \ldots, r\}$. Comparing the degree in each of the variables $X_2, \ldots, X_m$, we obtain $a_2 = \cdots = a_m = 0$ so that $L = a_1X_1$. But then L does not vanish when we substitute $X_2 = \omega$, and we obtain a contradiction. This proves the proposition. □

4.3. The case of $0 < t < m-1$ *and* $1 < s < q-1$

The arguments here will be similar to those in the previous subsection, except that we have to deal with an additional factor of degree $t(q - 1)$. Note that $1 < s < q - 1$ implies that $q \geq 4$.

Proposition 4.7. *Assume that $1 < r < m(q-1)$ and moreover, $r = t(q-1) + s$ with $0 < t < m-1$ and $1 < s < q-1$. Then any minimal free $\mathbb{N}$-resolution of the Reed-Muller code $\mathcal{RM}_q(r, m)$ is not pure.*

Proof. Choose distinct elements $\omega_1, \ldots, \omega_{s-1} \in \mathbb{F}_q$ and an arbitrary $\omega \in \mathbb{F}_q$. Define

$$Q(X_1, \ldots, X_m) = \left(\prod_{i=1}^{t} (X_i^{q-1} - 1)\right) \left(\prod_{j=1}^{s-1} (X_{t+1} - \omega_j)\right) (X_{t+2} - \omega)$$

Clearly, $Q \in V_q(r,m)$ and the corresponding codeword $c_Q = \mathrm{Ev}(Q)$ has weight $(q-s+1)(q-1)q^{m-t-2}$. On the other hand, by (13), the minimum distance of $\mathcal{RM}_q(r,m)$ is $(q-s)q^{m-t-1}$. Observe that

$$(q-s+1)(q-1)q^{m-t-2} - (q-s)q^{m-t-1} = (s-1)q^{m-t-2} > 0 \quad \text{since } s > 1.$$

Thus, as in the proof of Proposition 4.6, it suffices to show that if there exists F in $V_q(r,m)$ such that c_F is a minimum weight codeword with $\mathrm{Supp}(c_F) \subset \mathrm{Supp}(c_Q)$, then we arrive at a contradiction. Again, any such F has to be of the form

$$F(X_1,\dots,X_m) = \left(\prod_{i=1}^{t}(L_i^{q-1}-1)\right)\left(\prod_{j=1}^{s}(L_{t+1}-\omega'_j)\right)$$

for some distinct $\omega'_1,\dots,\omega'_s \in \mathbb{F}_q$, and linearly independent linear polynomials $L_1,\dots,L_{t+1} \in \mathbb{F}_q[X_1,\dots,X_m]$ with L_{t+1} homogeneous. Note that $\mathrm{Supp}(c_Q)$ is contained in the linear space $A = \{(a_1,\dots,a_m) \in \mathbb{F}_q^m : a_i = 0 \text{ for } i = 1,\dots,t\}$, which can be identified with $\mathbb{A}^{m-t}$, while $\mathrm{Supp}(c_F)$ is contained in the affine space $A' := \{\mathbf{a} \in \mathbb{F}_q^m : L_i(\mathbf{a}) = 0 \text{ for } i = 1,\dots,t\}$ of dimension $m-t$. Further, since $\mathrm{Supp}(c_F) \subset \mathrm{Supp}(c_Q)$, we obtain $\mathrm{Supp}(c_F) \subseteq A \cap A'$. Now if $A \neq A'$, then $\dim(A \cap A') \le m-t-1$, and so $(q-s)q^{m-t-1} \le q^{m-t-1}$, which is impossible because $s < q-1$. This shows that $A = A'$. Consequently,

$$F(0,\dots,0,X_{t+1},\dots,X_m) = \prod_{j=1}^{s}\left(L_{t+1}(0,\dots,0,X_{t+1},\dots,X_m) - \omega'_j\right)$$

gives a minimum weight codeword in $\mathcal{RM}_q(s,m-t)$ whose support contains the support of the codeword of $\mathcal{RM}_q(s,m-t)$ associated to $Q(0,\dots,0,X_{t+1},\dots,X_m)$. But then this leads to a contradiction exactly as in the proof of Proposition 4.6. $\square$

4.4. The case of $s = 0$

Since the binary case and the case $t = 0$ have already been dealt with in subsections 4.1 and 4.2, we shall assume that $q \ge 3$ and $1 \le t \le m-1$. Then $s = 0$ implies that $r = t(q-1) > 1$.

Proposition 4.8. *Assume that $q \ge 3$ and $r = t(q-1)$ with $1 \le t \le m-1$. Then any minimal free $\mathbb{N}$-resolution of the Reed-Muller code $\mathcal{RM}_q(r,m)$ is not pure.*

Proof. Write $\mathbb{F}_q = \{\omega_1,\dots,\omega_q\}$ and pick any $\omega \in \mathbb{F}_q$. Consider

$$Q(X_1,\dots,X_m) = \left(\prod_{i=1}^{t-1}(X_i^{q-1}-1)\right)\left(\prod_{j=3}^{q}(X_{t+1}-\omega_j)\right)(X_{t+2}-\omega)$$

Then $\deg Q = (t-1)(q-1) + (q-2) + 1 = t(q-1) = r$ and so $Q \in V_q(r,m)$. Also, we can write $\mathrm{Supp}(c_Q) = A_1 \cup A_2$, where for $i = 1,2$,

$$A_i := \{\mathbf{a} = (a_1,\dots,a_m) \in \mathbb{F}_q^m : a_1 = \cdots = a_t = 0,\ a_{t+1} = \omega_i,\ \text{and } a_{t+2} \neq \omega\}.$$

Clearly, A_1, A_2 are disjoint and so $\mathrm{wt}(c_Q) = 2(q-1)q^{m-t-1}$. The minimum distance of $\mathcal{RM}_q(r,m)$ in this case is q^{m-t}, and $2(q-1)q^{m-t-1} > q^{m-t}$, since $q \ge 3$. Thus, c_Q is not a minimum weight codeword. As in the proof of Proposition 4.6, it suffices to show that the existence of $F \in V_q(r,m)$ such that c_F is a minimum weight codeword with $\mathrm{Supp}(c_F) \subset \mathrm{Supp}(c_Q)$ leads to a contradiction. By the characterization of minimum weight codewords of $\mathcal{RM}_q(r,m)$, any such F has to be of the form $F(X_1,\dots,X_m) = \prod_{i=1}^{t}(L_i^{q-1}-1)$ for some linearly independent linear polynomials $L_1,\dots,L_t$ in $\mathbb{F}_q[X_1,\dots,X_m]$. Hence, $\mathrm{Supp}(c_F)$ is the affine space $A' := \{\mathbf{a} \in \mathbb{F}_q^m : L_i(\mathbf{a}) = 0 \text{ for } i = 1,\dots,t\}$. Since $\mathrm{Supp}(c_F) \subset \mathrm{Supp}(c_Q)$, we can argue as in the proof of Proposition 4.7 to deduce that A' is in fact, the linear space $\{\mathbf{a} \in \mathbb{F}_q^m : a_1 = \cdots = a_t = 0\}$. We now claim that $\mathrm{Supp}(c_F)$ is either disjoint from A_1 or from A_2. Indeed, if this is not the case then there are $P_i \in \mathrm{Supp}(c_F) \cap A_i$ for $i = 1, 2$. But then $P_\lambda := P_1 + \lambda(P_2 - P_1) \in \mathrm{Supp}(c_F)$ for any $\lambda \in \mathbb{F}_q$, since $\mathrm{Supp}(c_F) = A'$ is linear. Also since $q \neq 3$, we can pick $\lambda \in \mathbb{F}_q$ such that $\lambda \neq 0$ and $\lambda \neq 1$. Now $\mathrm{Supp}(c_F) \subset \mathrm{Supp}(c_Q) = A_1 \cup A_2$ leads to a contradiction since the t^{th} coordinate of P_λ is neither ω_1 nor ω_2. This proves the claim. It follows that $A' = \mathrm{Supp}(c_F) \subset A_i$ for some $i \in \{1,2\}$. But then $q^{m-t} \le (q-1)q^{m-t-1}$, which is a contradiction. This proves the proposition. □

4.5. The case of $t = m-1$ and $1 < s < q-2$

We will now consider the last case of nontrivial Reed-Muller codes $\mathcal{RM}_q(r,m)$ of order $r = t(q-1)+s$, where $r > 1$ and $s \neq 1$, namely, when $t = m-1$ and $s > 1$. Note that if we allow $s = q-2$, then $\mathcal{RM}_q(r,m)$ becomes a MDS code, and so we shall assume that $1 < s < q-2$. In particular, this implies that $q \ge 5$.

Proposition 4.9. *Assume that $r = (m-1)(q-1)+s$ with $1 < s < q-2$. Then any minimal free $\mathbb{N}$-resolution of the Reed-Muller code $\mathcal{RM}_q(r,m)$ is not pure.*

Proof. As in the proof of Proposition 4.8, write $\mathbb{F}_q = \{\omega_1,\dots,\omega_q\}$ and pick any $\omega \in \mathbb{F}_q$. Also let $\nu_1,\dots,\nu_{s+1}$ be any distinct elements of $\mathbb{F}_q$. Consider

$$Q(X_1,\dots,X_m) = \left(\prod_{i=1}^{m-2}(X_i^{q-1}-1)\right)\left(\prod_{j=3}^{q}(X_{m-1}-\omega_j)\right)\left(\prod_{j=1}^{s+1}(X_m-\nu_j)\right).$$

Then $\deg Q = (m-2)(q-1) + (q-2) + (s+1) = (m-1)(q-1) + s = r$ and so $Q \in V_q(r,m)$. Also, $\mathrm{wt}(c_Q) = 2(q-s-1)$ and $\mathrm{Supp}(c_Q) \subset A_1 \cup A_2$, where A_i denotes the affine line $\{\mathbf{a} = (a_1,\dots,a_m) \in \mathbb{F}_q^m : a_1 = \cdots = a_{m-2} = 0,\ a_{m-1} = \omega_i\}$ for $i = 1, 2$. The minimum distance of $\mathcal{RM}_q(r,m)$ in this case is $q-s$ and it is less than $2(q-s-1)$, since $s < q-2$. As in the proof of Proposition 4.6, it suffices to show that the existence of $F \in V_q(r,m)$ such that c_F is a minimum weight codeword with $\mathrm{Supp}(c_F) \subset \mathrm{Supp}(c_Q)$ leads to a contradiction. By the characterization of minimum weight codewords of $\mathcal{RM}_q(r,m)$, any such F has to be of the form

$$F(X_1,\dots,X_m) = \prod_{i=1}^{m-1}(L_i^{q-1}-1)\prod_{j=1}^{s}(L_m-\omega_j')$$

for some linearly independent linear polynomials $L_1,\dots,L_m$ in $\mathbb{F}_q[X_1,\dots,X_m]$ and distinct $\omega_1',\dots,\omega_s' \in \mathbb{F}_q$. Also, arguing as in the proof of Theorem 4.8, we see that $\mathrm{Supp}(c_F)$ is contained in the affine line $A' := \{\mathbf{a} \in \mathbb{F}_q^m : L_i(\mathbf{a}) = 0 \text{ for } i = 1,\dots,m-1\}$. Now if any two points of $\mathrm{Supp}(c_F)$ belong to different affine lines A_1 and A_2, then $A_i \cap A'$ is nonempty for $i = 1, 2$ and dimension considerations imply that $A_1 = A_2 = A'$, which is a contradiction. Hence, the $(q-s)$ points of $\mathrm{Supp}(c_F)$ are contained in $\mathrm{Supp}(c_Q) \cap A_i$ for a unique $i \in \{1,2\}$. But then $q-s \le q-s-1$, which is a contradiction. This proves the proposition. □

An easy consequence of the above result is that unlike linear resolutions (which correspond to MDS codes), purity of a resolution is not preserved when passing to the dual.

Corollary 4.10. *There exist linear codes C with a pure resolution such that $C^{\perp}$ does not have a pure resolution.*

Proof. By Theorem 4.1, the first order Reed-Muller code $\mathcal{RM}_q(1,m)$ has a pure resolution. But the dual of $\mathcal{RM}_q(1,m)$ is $\mathcal{RM}_q((m-1)(q-1)+(q-3),m)$ and it does not have a pure resolution, thanks to Proposition 4.9. □

We can consolidate the results in subsections 4.1–4.5 to obtain the following.

Theorem 4.11. *Assume that $m \geq 2$ and $1 < r < m(q-1)-1$. Write $r = t(q-1)+s$, where $0 \leq t \leq m-1$ and $0 \leq s < q-1$. Suppose $s \neq 1$. Then any minimal free $\mathbb{N}$-resolution of the Reed-Muller code $\mathcal{RM}_q(r,m)$ is not pure.*

Proof. Follows from Propositions 4.4, 4.6, 4.7, 4.8, and 4.9. □

5. On the purity and resolutions of some two-weight codes

This section is devoted to two-weight codes. A linear code C is said to be a *two-weight code* if there are two distinct positive integers w_1 and w_2 such that every nonzero codeword of C has weight either w_1 or w_2. We will usually take $w_1 < w_2$ so that $w_1 = d_1(C)$. We have seen in Corollary 3.10 that the resolution of constant weight codes are pure and their Betti numbers are explicitly known. The first order Reed-Muller codes are examples of two-weight codes, and Theorem 4.1 shows that their resolutions are pure and the Betti numbers can be explicitly determined. Thus, it is natural to ask if every two-weight code has pure resolution. In this section we will choose several examples of two-weight codes given by Calderbank and Kantor [8] and see that some of them have pure resolution and others do not. In [8], these codes are referred to by a nomenclature such as RT1, TF1, TF1^d, etc., and this is indicated in parenthesis at the beginning of each of the examples considered here. We also compute the Betti numbers of some of the two-weight codes irrespective of whether or not their resolution is pure. The examples of two-weight codes given in [8] are defined geometrically. So before considering them here, we recall a geometric language for codes and translate our characterization of purity (Theorem 3.6) in this language.

As before, fix positive integers n, k with $k \leq n$ and a prime power q. We denote by $\mathbb{P}^{k-1}$ the $(k-1)$-dimensional projective space over the finite field $\mathbb{F}_q$. A (nondegenerate) $[n,k]_q$ *projective system* is a multiset of n points in $\mathbb{P}^{k-1}$ that do not lie on a hyperplane of $\mathbb{P}^{k-1}$. Let $\mathcal{P}$ be a $[n,k]_q$ projective system. For $r = 1, \dots, k$, the r^{th} *generalized Hamming weight*, or the r^{th} *higher weight* of $\mathcal{P}$ is defined by

$$d_r(\mathcal{P}) = n - \max\{|\mathcal{P} \cap \Pi_r| : \ \Pi_r \ \text{ linear subspace of } \mathbb{P}^{k-1} \text{ with } \operatorname{codim} \Pi_r = r\}.$$

Here the "cardinality" $|\mathcal{P} \cap \Pi_r|$ is understood as the sum of multiplicities of points of $\mathcal{P}$ that are in Π_r. Note that the only linear subspace of codimension k in $\mathbb{P}^{k-1}$ is the empty set, whereas those of codimension $k-1$ consist of a single point. Thus,

$$d_k(\mathcal{P}) = n \quad \text{and} \quad d_{k-1}(\mathcal{P}) = n-1. \tag{15}$$

We can naturally associate a nondegenerate $[n,k]_q$-linear code to $\mathcal{P}$ as follows. Choose representatives $P_1, \dots, P_n$ in $\mathbb{F}_q^k$ corresponding to the n points of $\mathcal{P}$. Let $(\mathbb{F}_q^k)^*$ be the dual space of the vector space $\mathbb{F}_q^k$. Consider the evaluation map

$$\operatorname{Ev} : (\mathbb{F}_q^k)^* \to \mathbb{F}_q^n \text{ defined by } \operatorname{Ev}(f) = (f(P_1), \dots, f(P_n)).$$

The image of Ev is a linear subspace C of $\mathbb{F}_q^n$ such that $\dim C = k$ and C is not contained in a coordinate hyperplane of $\mathbb{F}_q^n$. This, then, is the $[n,k]_q$-linear code associated to $\mathcal{P}$. We refer to Tsfasman, Vlăduţ and Nogin [24] for more on projective systems and simply remark that the above association gives rise to a one-to-one correspondence between the equivalence classes of $[n,k]_q$ projective systems and nondegenerate $[n,k]_q$-linear codes, which preserves generalized Hamming weights. Also, subcodes of C of dimension r correspond to linear subspaces of $\mathbb{P}^{k-1}$ of codimension r. Thus, we define the *support* of a linear subspace Π_r of $\mathbb{P}^{k-1}$ with $\operatorname{codim}\Pi_r = r$, to be the multiset $\mathcal{P} \setminus \mathcal{P} \cap \Pi_r$. This corresponds precisely to the support of the corresponding subcode of C. As a consequence, we obtain the following geometric translation of our characterization of purity.

Theorem 5.1. *Let $\mathcal{P} \subseteq \mathbb{P}^{k-1}$ be an $[n,k]_q$ projective system and let C be the corresponding $[n,k]_q$-code. The $\mathbb{N}$-graded minimal free resolution of C is pure if and only if for every $1 \le r \le k-1$ and every linear subspace $\Pi_r \subset \mathbb{P}^{k-1}$ of codimension r, there exists a linear subspace $H(\Pi_r) \subset \mathbb{P}^{k-1}$ of codimension r with $\Pi_r \cap \mathcal{P} \subseteq H(\Pi_r) \cap \mathcal{P}$ and $|H(\Pi_r) \cap \mathcal{P}| = n - d_r(\mathcal{P})$.*

Proof. Follows from Theorem 3.6. □

Corollary 5.2. *$\mathcal{P} \subseteq \mathbb{P}^{k-1}$ be an $[n,k]_q$ projective system and let C be the corresponding linear code. Then the $\mathbb{N}$-graded resolution of C is always pure at the $(k-1)^{th}$ and k^{th} step.*

Proof. From (15), we see that C is $(k-1)$-MDS. Thus the desired result follows from Corollary 3.9 and Theorem 5.1. □

The following definition from [8] is a geometric counterpart of two-weight codes.

Definition 5.3. Let h_1, h_2 be distinct nonnegative integers. An $[n,k]_q$ projective system $\mathcal{P}$ is said to be a *projective $(n,k,h_1,h_2)_q$ system* if every hyperplane of $\mathbb{P}^{k-1}$ intersects $\mathcal{P}$ either at h_1 points or at h_2 points (counting multiplicities).

Note that if $\mathcal{P}$ is a projective $(n,k,h_1,h_2)_q$ system, then every nonzero codeword of the corresponding $[n,k]_q$ code C is of Hamming weight w_1 or w_2, where $w_i = n - h_i$ for $i = 1,2$. Also note that for $i = 1,2$, if A_{w_i} denotes the number of codewords of C of weight w_i, then

$$A_{w_i} = (q-1)\nu_i, \tag{16}$$

where ν_i denotes the number of hyperplanes Π of $\mathbb{P}^{k-1}$ such that $|\Pi \cap \mathcal{P}| = h_i$. The factor $(q-1)$ is due to the fact that the codewords $\mathrm{Ev}(f)$ and $\mathrm{Ev}(\lambda f)$ of C correspond to the same hyperplane in $\mathbb{P}^{k-1}$ for any $\lambda \in \mathbb{F}_q$ with $\lambda \neq 0$.

We are now ready to discuss several examples from [8] of two-weight codes, and investigate their purity and minimal free resolutions. We use the following notation.

$$p_j = p_j(q) := |\mathbb{P}^j(\mathbb{F}_q)| = \begin{cases} q^j + q^{j-1} + \cdots + q + 1 & \text{if } j \ge 0, \\ 0 & \text{if } j < 0. \end{cases}$$

Example 5.4 *(RT1).* Take the base field as $\mathbb{F}_{q^2}$ and let $\mathbb{P} = \mathbb{P}^{k-1}(\mathbb{F}_{q^2})$. Consider $\mathcal{P} = \mathbb{P}^{k-1}(\mathbb{F}_q)$ as a projective system in $\mathbb{P}$. If Π is a hyperplane in $\mathbb{P}$, then it is given by an equation of the form $\sum_{i=1}^k z_i X_i = 0$, where $z_1, \ldots, z_k \in \mathbb{F}_{q^2}$, not all zero. Fix a $\mathbb{F}_q$-basis $\{1, \theta\}$ of $\mathbb{F}_{q^2}$ and write $z_i = a_i + \theta b_i$, where $a_i, b_i \in \mathbb{F}_q$ for $i = 1, \ldots, k$. Then $\mathcal{P} \cap \Pi$ consists of points $(c_1 : \cdots : c_k) \in \mathbb{P}^{k-1}(\mathbb{F}_q)$ satisfying $\sum a_i c_i = 0$ and $\sum b_i c_i = 0$. Now if there is $\lambda \in \mathbb{F}_q$ such that $a_i = \lambda b_i$ for all $i = 1, \ldots, k$, or such that $b_i = \lambda a_i$ for all $i = 1, \ldots, k$, then $\mathcal{P} \cap \Pi$ corresponds to a $\mathbb{F}_q$-rational hyperplane in $\mathbb{P}^{k-1}(\mathbb{F}_q)$. Otherwise, it corresponds to a linear subspace of codimension 2 in $\mathbb{P}^{k-1}(\mathbb{F}_q)$. Thus, $|\mathcal{P} \cap \Pi| = p_{k-2}(q)$ or $p_{k-3}(q)$. It follows that the linear code corresponding to $\mathcal{P}$, say C, is a two-weight code of length $p_{k-1}(q)$ and dimension k over $\mathbb{F}_{q^2}$. Also, it is clear that as Π_r varies over $\mathbb{F}_{q^2}$-linear subspaces of codimension r in $\mathbb{P}$, the maximum possible value of $|\mathcal{P} \cap \Pi_r|$ is attained when Π_r is $\mathbb{F}_q$-rational, and in that case $|\mathcal{P} \cap \Pi_r| = p_{k-1-r}(q)$ for $r = 1, \dots, k$. It follows that the higher weights of $\mathcal{P}$ are given by $d_r = p_{k-1}(q) - p_{k-1-r}(q)$ for $r = 1, \dots, k$.

To determine the purity of the minimal free resolution of C, fix a $\mathbb{F}_{q^2}$-linear subspace Π of codimension r in $\mathbb{P}$. Let $t := \dim_{\mathbb{F}_q}(\Pi \cap \mathcal{P})$. If Π is not $\mathbb{F}_q$-rational, then $t < k - 1 - r$. Let $\{f_1, \dots, f_{t+1}\}$ be a $\mathbb{F}_q$-basis of $\Pi \cap \mathcal{P}$. Extend this to a linearly independent set $\{f_1, \dots, f_{t+1}, \dots, f_{k-r}\} \subset \mathcal{P}$. Note that the set $\{f_1, \dots, f_{k-r}\}$ is linearly independent over $\mathbb{F}_{q^2}$. (This can be seen, as before, by expressing the coefficients in a linear dependence relation in terms of $1, \theta$.) Now if $H = H(\Pi_r)$ is the linear subspace of $\mathbb{P}$ spanned by $\{f_1, \dots, f_{k-r}\}$, then $\Pi \cap \mathcal{P} \subset H \cap \mathcal{P}$ and $|H \cap \mathcal{P}| = n - d_r(\mathcal{P})$. Thus, Theorem 5.1 shows that the $\mathbb{N}$-graded minimal free resolution of C is pure. Moreover, it is of the form

$$0 \to R(-d_k)^{\beta_k} \to \cdots \to R(-d_2)^{\beta_2} \to R(-d_1)^{\beta_1} \to R$$

where $d_r = p_{k-1}(q) - p_{k-1-r}(q)$ and β_r's are given by Herzog-Kühl equation for $r = 1, \dots, k$. In fact, this is precisely the resolution for constant weight codes given in Corollary 3.10. It may be noted that even though constant weight codes have been characterized by Johnsen and Verdure [17, Thm. 2 and Prop. 4] as those having a resolution as in Corollary 3.10, the code C is not a constant weight code because it is a code over $\mathbb{F}_{q^2}$, whereas the characterization is for q-ary codes.

Remark 5.5. One can similarly consider $\mathcal{P} = \mathbb{P}^{k-1}(\mathbb{F}_q) \subseteq \mathbb{P}^{k-1}(\mathbb{F}_{q^m})$ for any $m \geq 2$, and show that the resolution of the linear code corresponding to this projective system is pure and of the form similar to that in Example 5.4 even though this code is not a two-weight code when $m > 2$.

Example 5.6 *(TF1).* Assume that q is even and consider the projective plane $\mathbb{P}^2$ over $\mathbb{F}_q$. Let $\mathcal{P} \subseteq \mathbb{P}^2$ be a *hyperoval*, i.e., a set of $q + 2$ distinct points, no three collinear, with the property that if L is a line in $\mathbb{P}^2$, then $|L \cap \mathcal{P}| = 0$ or 2. In this case, the corresponding code is an MDS $[q + 2, 3]_q$-code and the resolution of this code is given by Corollary 3.9.

Example 5.7 *(TF1^d).* Suppose q is even and $\mathcal{P}$ is the hyperoval in the projective plane $\mathbb{P}^2$ over $\mathbb{F}_q$ as in Example 5.6. Let $\widehat{\mathbb{P}^2}$ be the dual projective plane. Consider

$$\widehat{\mathcal{P}} = \{L : L \text{ is a line in } \mathbb{P}^2 \text{ with } |L \cap \mathcal{P}| = 2\}.$$

Note that $\widehat{\mathcal{P}} \subseteq \widehat{\mathbb{P}^2}$ and the points of the projective plane $\mathbb{P}^2$ are lines in $\widehat{\mathbb{P}^2}$. Note also that any two points of $\mathcal{P}$ correspond to a unique line L in $\mathbb{P}^2$ such that $L \in \widehat{\mathcal{P}}$. Consequently, $|\widehat{\mathcal{P}}| = \binom{q+2}{2}$. Now consider a line in $\widehat{\mathbb{P}^2}$, i.e., a point P of $\mathbb{P}^2$. Counting the intersection of this line with $\widehat{\mathcal{P}}$ corresponds to counting lines $L \subseteq \mathbb{P}^2$ that pass through P and intersect the hyperoval $\mathcal{P}$ in exactly two points. The cardinality of this intersection depends only on whether or not the chosen point P lies on $\mathcal{P}$. More precisely, if $P \in \mathcal{P}$, then any line passing through P will intersect the hyperoval $\mathcal{P}$ in two points, and there are exactly $(q + 1)$ such lines. On the other hand, if $P \notin \mathcal{P}$, then choosing any point Q on $\mathcal{P}$ will correspond to a unique line L_Q passing through P and Q such that L_Q intersects $\mathcal{P}$ in another point $Q' \neq Q$. Further, since each L_Q passes through P, the points $Q' \in \mathcal{P}$ corresponding to $Q \in \mathcal{P}$ are distinct. Since $|\mathcal{P}| = q + 2$, it follows that there are exactly

$(q+2)/2$ lines of the form L_Q. This shows that $\mathcal{P}$ is a $\left(\binom{q+2}{2}, 3, (q+1), \frac{q+2}{2}\right)_q$ projective system, and it corresponds to an $[\binom{q+2}{2}, 3]_q$ two-weight code with distinct nonzero weights

$$w_1 = \binom{q+2}{2} - (q+1) = \frac{q(q+1)}{2} \quad \text{and} \quad w_2 = \binom{q+2}{2} - \frac{q+2}{2} = \frac{q(q+2)}{2}.$$

Also, the number of lines in $\widehat{\mathbb{P}^2}$ that intersect $\widehat{P}$ in $(q+1)$ points is $|\mathcal{P}| = q+2$, whereas the number of lines in $\widehat{\mathbb{P}^2}$ that intersect $\widehat{P}$ in $\frac{q+2}{2}$ points is $|\mathbb{P}^2 \setminus \mathcal{P}| = q^2 - 1$. Thus, in view of (16), we see that the weight spectrum of the two-weight code corresponding to $\widehat{\mathcal{P}}$ is given by

$$A_{w_1} = (q+2)(q-1) \quad \text{and} \quad A_{w_2} = (q^2-1)(q-1).$$

Furthermore, any hyperplane section of $\widehat{P}$ has to be either of the following two types: (i) a set consisting of lines passing through a fixed $P \in \mathcal{P}$ and a varying point of $\mathcal{P} \setminus \{P\}$, or (ii) a set consisting of lines of the form L_Q where Q varies over a suitable subset of $\mathcal{P}$ having $(q+2)/2$ elements. Now a set of type (ii) has at least two lines and no two lines in this set can intersect in a point of $\mathcal{P}$. Hence a set of type (ii) can never be contained in any set of type (i). It follows that the purity criterion in Theorem 5.1 is violated (for $r = 1$). Equivalently, every 1-dimensional subcode of C has minimal support, and since C has two distinct nonzero weights $d_1 = w_1 < w_2$, we see that the criterion in Theorem 3.6 is violated (for $i = 1$). Thus, the resolution of C is not pure. Moreover, in view of (5) and (12), we see that the resolution has two twists at the first step, whereas it is pure at the second and third step, thanks to Corollary 5.2. Hence, the resolution of C is of the form

$$R(-d_3)^{\beta_{3,d_3}} \to R(-d_2)^{\beta_{2,d_2}} \to R(-w_2)^{\beta_{1,w_2}} \oplus R(-w_1)^{\beta_{1,w_1}}$$

where w_1, w_2 are as before and

$$d_2 = \binom{q+2}{2} - 3 + 2 = \frac{q(q+3)}{2} \quad \text{and} \quad d_3 = \binom{q+2}{2} - 3 + 3 = \frac{(q+1)(q+2)}{2}.$$

Moreover, from Corollary 3.7, we see that

$$\beta_{1,w_1} = (q+2) \quad \text{and} \quad \beta_{1,w_2} = (q^2-1).$$

To determine the remaining Betti numbers, let us write $X_1 = \beta_{1,w_1}$, $X_2 = \beta_{1,w_2}$, $Y = \beta_{2,d_2}$, and $Z = \beta_{3,d_3}$. Then the Boij-Söderberg equations (8) give the following system of linear equations

$$\begin{aligned} 1 - (X_1 + X_2) + Y - Z &= 0 \\ -w_1 X_1 - w_2 X_2 + d_2 Y - d_3 Z &= 0 \\ -w_1^2 X_1 - w_2^2 X_2 + d_2^2 Y - d_3^2 Z &= 0 \end{aligned}$$

Putting the values of w_1, w_2, d_2, d_3, X_1 and X_2, we obtain $Y = \frac{q(q+1)(q+2)}{2}$ and $Z = \frac{q^2(q+1)}{2}$. This determines the resolution of the code C corresponding to $\widehat{\mathcal{P}}$.

Example 5.8 *(TF2).* Assume that q is even with $q > 2$. Suppose h is an integer such that $1 < h < q$ and h divides q. Following Denniston [12], a *maximal arc* in the projective plane $\mathbb{P}^2$ may be defined as a set of points meeting every line in h points or none at all. Let $\mathcal{P} \subseteq \mathbb{P}^2$ be a maximal arc consisting of $n = 1 + (q+1)(h-1)$ points. It has been shown by Denniston [12] that such maximal arcs exist. Since $|L \cap \mathcal{P}| = 0$ or h, for any line L in $\mathbb{P}^2$, we see that the $[n, 3]_q$-code C corresponding to $\mathcal{P}$ is a two-weight code (cf. [8]) whose nonzero weights are $q(h-1)$ and n. Since the second weight of C is the length of C, a minimal 1-dimensional subcode of C must be of minimum weight. Hence, by Theorem 3.6, the minimal free resolution of the code C is pure. Thus, in view of Corollary 5.2, we see that the resolution of C is of the form:

$$R(-d_3)^{\beta_{3,d_3}} \to R(-d_2)^{\beta_{2,d_2}} \to R(-d_1)^{\beta_{1,d_1}}$$

where $d_1 = q(h-1)$, $d_2 = (q+1)(h-1)$ and $d_3 = 1 + (q+1)(h-1)$. Using the Herzog-Kühl formula, one can compute the Betti numbers, and they are

$$\beta_{1,d_1} = (q+1)^2 - \frac{q}{h}, \quad \beta_{2,d_2} = qn, \quad \text{and} \quad \beta_{3,d_3} = (h-1)^2(q+1)\frac{q}{h}.$$

Example 5.9 *(TF2^d).* Let q, h, n and $\mathcal{P}$ be as in Example 5.8. Consider the dual projective plane $\widehat{\mathbb{P}^2}$ of $\mathbb{P}^2$, and let $\widehat{\mathcal{P}} = \{L \in \widehat{\mathbb{P}^2} : |L \cap \mathcal{P}| = h\}$. Now there are exactly $(q+1)$ lines passing through a point of $\mathbb{P}^2$, and in case this point is in $\mathcal{P}$, then such a line intersects $\mathcal{P}$ in exactly h points. Since $|\mathcal{P}| = n$, it follows that

$$\hat{n} := |\widehat{\mathcal{P}}| = \frac{(q+1)n}{h} = \frac{(q+1)\,(1+(q+1)(h-1))}{h}.$$

Next we want to understand the intersection of $\widehat{\mathcal{P}}$ with a hyperplane of $\widehat{\mathbb{P}^2}$. Note that a hyperplane, say H, of $\widehat{\mathbb{P}^2}$ corresponds to a point, say P, of $\mathbb{P}^2$, and

$$H \cap \widehat{\mathcal{P}} = \{L \subset \mathbb{P}^2 : \ L \text{ is a line passing through } P \text{ and } |L \cap \mathcal{P}| = h\}.$$

Therefore $|H \cap \widehat{\mathcal{P}}|$ is $(q+1)$ or n/h, according as $P \in \mathcal{P}$ or $P \notin \mathcal{P}$. Thus $\widehat{\mathcal{P}}$ is an $(\hat{n},\ 3,\ (q+1),\ \frac{n}{h})_q$ projective system and the corresponding $[\hat{n},\ 3]_q$-code is a two-weight code with distinct nonzero weights given by

$$w_1 = \hat{n} - (q+1) = \frac{q(q+1)(h-1)}{h} \quad \text{and} \quad w_2 = \hat{n} - \frac{n}{h} = \frac{qn}{h}.$$

Using similar arguments as in Example 5.7, we see that the weight spectrum of this code is given by

$$A_{w_1} = (q-1)n \quad \text{and} \quad A_{w_2} = (q-1)(q+1)(q-h+1),$$

and also that the resolution of this code is of the form

$$R(-d_3)^{\beta_{3,d_3}} \to R(-d_2)^{\beta_{2,d_2}} \to R(-w_2)^{\beta_{1,w_2}} \oplus R(-w_1)^{\beta_{1,w_1}}$$

where $\beta_{1,w_1} = n = 1 + (q+1)(h-1)$ and $\beta_{1,w_2} = (q+1)(q-h+1)$, and in view of Corollary 5.2, $d_2 = \hat{n} - 1$ and $d_3 = \hat{n}$. As in Example 5.7, using the Boij-Söderberg equations (8) and putting all known values, we obtain

$$\beta_{2,d_2} = \frac{q(q+1)(qh+h-q)}{h} \quad \text{and} \quad \beta_{3,d_3} = \frac{q^2(q+1)(h-1)}{2}.$$

We remark that when $q > 2$, Examples 5.6 and 5.7 are special cases of Examples 5.8 and 5.9, respectively, with $h = 2$.

Example 5.10 *(TF3).* Assume that $q > 2$. In the finite projective 3-space $\mathbb{P}^3$ over $\mathbb{F}_q$, an *ovoid* may be defined as a set of $q^2 + 1$ points, no three of which are collinear (see, e.g., Dembowski [11, p. 48]). Suppose $\mathcal{P}$ is an ovoid in $\mathbb{P}^3$. Then for any hyperplane H of $\mathbb{P}^3$, the intersection $\mathcal{P} \cap H$ is an ovoid in $H \simeq \mathbb{P}^2$, and hence using [11, p. 48, §49], we see that $|H \cap \mathcal{P}| = 1$ or $q+1$. Let C be the corresponding linear code. Then C is a two-weight code of length $n = q^2+1$, dimension $k = 4$, and weights $w_1 = q(q-1)$ and $w_2 = q^2$. The resolution of this code C is pure. To see this, note that if Π is a hyperplane in $\mathbb{P}^3$ intersecting $\mathcal{P}$ at only one point, then there is another hyperplane H with $|H \cap \mathcal{P}| = q+1$ and $\Pi \cap \mathcal{P} \subset H \cap \mathcal{P}$. More precisely, let $\Pi \cap \mathcal{P} = \{P\}$ and let $Q \in \mathcal{P}$ be any point other than P. Take any hyperplane H passing through P and Q. Since $|H \cap \mathcal{P}| > 1$, we must have $|H \cap \mathcal{P}| = q+1$. Further, $\Pi \cap \mathcal{P} \subset H \cap \mathcal{P}$. It follows that all minimal codewords of C are of minimum weight. Hence, by Corollary 3.7, we see that $\beta_{1,j} = 0$ for all $j \neq w_1$, i.e., the resolution of C is "pure at the first step". Next, observe that the maximum possible cardinality of $L \cap \mathcal{P}$ is 2 for any line L in $\mathbb{P}^3$, and there do exist lines L for which $|L \cap \mathcal{P}| = 2$. Hence, $d_2(C) = n-2 = q^2-1$. Consequently, C is a 2-MDS code, and hence by Corollary 3.9, the resolution is linear after the second step. This proves that the resolution of C is pure and is of the form

$$R(-(q^2+1))^{\beta_{4,q^2+1}} \to R(-q^2)^{\beta_{3,q^2}} \to R(-(q^2-1))^{\beta_{2,q^2-1}} \to R(-q(q-1))^{\beta_{1,q(q-1)}}$$

where the Betti numbers can be obtained from Herzog-Kühl formula (9) as follows.

$$\beta_{4,q^2+1} = \tfrac{q^3(q-1)^2}{2}, \qquad \beta_{3,q^2} = (q-1)(q^2-1)(q^2+1),$$
$$\beta_{2,q^2-1} = \tfrac{q^3(q^2+1)}{2}, \quad \text{and} \quad \beta_{1,q(q-1)} = q(q^2+1).$$

Example 5.11 *(RT3).* Assume that $k \geq 3$. Consider the quadratic extension $\mathbb{F}_{q^2}$ of $\mathbb{F}_q$ and the projective variety $\mathcal{P}_{k-2} \subset \mathbb{P}^{k-1}(\mathbb{F}_{q^2})$ defined by the equation

$$X_1^{q+1} + \cdots + X_k^{q+1} = 0.$$

Following Bose and Chakravarti [7], we may refer to $\mathcal{P}_{k-2}$ as the (nondegenerate) Hermitian variety of dimension $k-2$. Let C_{k-2} be the $[n_k, k]_{q^2}$-code corresponding to $\mathcal{P}_{k-2}$, where $n_k := |\mathcal{P}_{k-2}|$. We know from [7, Theorem 8.1] that

$$n_k = \frac{\left(q^k - (-1)^k\right)\left(q^{k-1} - (-1)^{k-1}\right)}{q^2-1}. \tag{17}$$

To understand the weights of C_{k-2}, first note that since $x \mapsto x^q$ is an involutory automorphism of $\mathbb{F}_{q^2}$, every hyperplane of $\mathbb{P}^{k-1}(\mathbb{F}_{q^2})$ is given by an equation of the form $c_1^q X_1 + \cdots + c_k^q X_k = 0$ for some $\mathbf{c} = (c_1 : \cdots : c_k) \in \mathbb{P}^{k-1}(\mathbb{F}_{q^2})$; we denote this hyperplane by $H_{\mathbf{c}}$ and call it a *tangent hyperplane* in case $\mathbf{c} \in \mathcal{P}_{k-2}$ (see, e.g., Chakravarti [9, §2]). We remark that $H_{\mathbf{c}}$ and $\mathbf{c}$ determine each other. In other words, if $\mathbf{c}, \mathbf{d} \in \mathbb{P}^{k-1}(\mathbb{F}_{q^2})$, then: $H_{\mathbf{c}} = H_{\mathbf{d}} \Leftrightarrow \mathbf{c} = \mathbf{d}$. Now from [9, Theorem 3.1] and from Theorem 7.4 as well as Theorem 8.1 (and its corollary) of [7], we see that

$$|H_{\mathbf{c}} \cap \mathcal{P}_{k-2}| = \begin{cases} n_{k-1} & \text{if } H_{\mathbf{c}} \text{ is not a tangent hyperplane,} \\ 1 + q^2 n_{k-2} & \text{if } H_{\mathbf{c}} \text{ is a tangent hyperplane,} \end{cases} \tag{18}$$

where n_{k-1} and n_{k-2} are given by expressions similar to that in (17) with appropriate substitution. Thus, it follows that C_{k-2} is a two-weight code. We will now discuss the nature of the resolution of this code when $k = 3$ and $k = 4$.

First, suppose $k = 3$. Then $\mathcal{P}_1$ is the Hermitian curve consisting of q^3+1 points. If L is a line in $\mathbb{P}^2(\mathbb{F}_{q^2})$, then by (18), $|L \cap \mathcal{P}_1|$ is either $q+1$ or 1, and thus the two nonzero weights of C_1 are given by $w_1 = q(q^2-1)$ and $w_2 = q^3$. Moreover, if L_1 is a tangent line to $\mathcal{P}_1$ so that $L_1 \cap \mathcal{P}_1$ consists of a single point, say P, then by choosing another point Q of $\mathcal{P}_1$ and a line L_2 passing through P and Q, we find

$$|L_2 \cap \mathcal{P}_1| = q + 1 \quad \text{and} \quad L_1 \cap \mathcal{P}_1 \subset L_2 \cap \mathcal{P}_1.$$

Consequently, every 1-minimal subcode of C_1 has support weight $w_1 = d_1(C_1)$. Thus, as in Example 5.10, we can deduce from Corollary 3.7 that the resolution of C_1 is "pure at the first step". This together with Corollary 5.2 shows that the resolution of C_1 is pure and it looks like

$$R(-(q^3+1))^{\beta_{3,q^3+1}} \to R(-q^3)^{\beta_{2,q^3}} \to R(-q(q^2-1))^{\beta_{1,q(q^2-1)}}$$

where the Betti numbers can be obtained from Herzog-Kühl formula (9) as follows.

$$\beta_{1,q(q^2-1)} = q^2(q^2-q+1),\ \beta_{2,q^3} = (q^3+1)(q^2-1) \text{ and } \beta_{3,q^3+1} = q(q^2-1)(q^2-q+1).$$

Next, suppose $k = 4$. Here $\mathcal{P}_2$ is the Hermitian surface with $(q^2+1)(q^3+1)$ points. Further, by (18), a section $\mathcal{P}_2 \cap H_{\mathbf{c}}$ of the Hermitian surface by a tangent hyperplane has q^3+q^2+1 points, while a section $\mathcal{P}_2 \cap H_{\mathbf{d}}$ by a non-tangent hyperplane has q^3+1 points. Moreover, $\mathcal{P}_2 \cap H_{\mathbf{d}} \nsubseteq \mathcal{P}_2 \cap H_{\mathbf{c}}$ for any $\mathbf{c} \in \mathcal{P}_2$ and $\mathbf{d} \in \mathbb{P}^3(\mathbb{F}_{q^2}) \setminus \mathcal{P}_2$. Indeed, by [9, Theorem 3.1], $\mathcal{P}_2 \cap H_{\mathbf{d}}$ is nondegenerate in $H_{\mathbf{d}} \simeq \mathbb{P}^2$ and so the linear span of points in $\mathcal{P}_2 \cap H_{\mathbf{d}}$ is $H_{\mathbf{d}}$. But then $\mathcal{P}_2 \cap H_{\mathbf{d}} \subseteq \mathcal{P}_2 \cap H_{\mathbf{c}}$ would imply that $H_{\mathbf{d}} \subseteq H_{\mathbf{c}}$ and hence $H_{\mathbf{d}} = H_{\mathbf{c}}$, which is a contradiction. (Alternatively, if $\mathcal{P}_2 \cap H_{\mathbf{d}} \subseteq \mathcal{P}_2 \cap H_{\mathbf{c}}$, then $q^3+q^2+1 = |\mathcal{P}_2 \cap H_{\mathbf{d}}| = |\mathcal{P}_2 \cap H_{\mathbf{d}} \cap H_{\mathbf{c}}| \leq |H_{\mathbf{d}} \cap H_{\mathbf{c}}| = q^2+1$, which is a contradiction.) At any rate, it follows that C_2 is a two-weight code with the nonzero weights $w_1 = q^5$ and $w_2 = q^5+q^2$, and moreover, every 1-dimensional subcode of C_2 is minimal. Thus, the resolution of C_2 has two twists at the first level and by Corollary 3.7, the corresponding Betti numbers are as follows.

$$\beta_{1,w_1} = |\mathcal{P}_2| = (q^2+1)(q^3+1) \quad \text{and} \quad \beta_{1,w_2} = |\mathbb{P}^3(\mathbb{F}_{q^2}) \setminus \mathcal{P}_2| = q^3(q^2+1)(q-1).$$

To understand the behavior of the resolution at the second step, we consider 2-dimensional subcodes of C_2 and determine which of these are minimal. Equivalently, we consider the sections $\mathcal{P}_2 \cap L$ of the Hermitian surface with a line L in $\mathbb{P}^3(\mathbb{F}_{q^2})$. It is shown in [7, §10] (see also [9, §5.2]) that $|\mathcal{P}_2 \cap L|$ can only take 3 possible values, namely, q^2+1, $q+1$, or 1. Accordingly, the line L is referred to as a generator, secant line, or tangent line, respectively. It is clear that if L is a tangent line, then there is a non-tangent line L' such that $\mathcal{P}_2 \cap L \subset \mathcal{P}_2 \cap L'$. On the other hand, if L is a secant line, then $\mathcal{P}_2 \cap L \not\subset \mathcal{P}_2 \cap L'$ for any generator L', because there is a unique line passing through any two points of $\mathbb{P}^3(\mathbb{F}_{q^2})$. It follows that there are two types of 2-minimal subcodes of C_2, one with support weight $d_2 = |\mathcal{P}_2| - (q^2+1) = q^3(q^2+1)$ and another with support weight $d_2' = |\mathcal{P}| - (q+1) = q(q^4+q^2+q-1)$. Thus, it follows from (5) and (12) that the resolution of C_2 has two twists at level 2, and these correspond to the above values of d_2 and d_2'. Finally, we note that C_2 is 3-MDS and by Corollary 5.2, the resolution of C_2 is pure at the third and fourth steps. Thus, we can conclude that the minimal free resolution of C_2 has the form

$$R(-d_4)^z \to R(-d_3)^y \to R(-d_2')^{x_1} \oplus R(-d_2)^{x_2} \to R(-w_2)^{\beta_{1,w_2}} \oplus R(-w_1)^{\beta_{1,w_1}}$$

where w_1, w_2, d_2, d_2' are as before, $d_3 = (q^2+1)(q^3+1) - 1$, $d_4 = (q^2+1)(q^3+1)$, and x_1, x_2, y, z denote the undetermined Betti numbers, namely,

$$x_1 = \beta_{2,d_2'}, \quad x_2 = \beta_{2,d_2}, \quad y = \beta_{3,d_3}, \quad z = \beta_{4,d_4}.$$

To determine these, we note that the Boij-Söderberg equations (8) give rise to

$$\begin{aligned} 1 - (\beta_{1,w_1} + \beta_{1,w_1}) + (\beta_{2,d_2} + \beta_{2,d_2'}) - \beta_{3,d_3} + \beta_{4,d_4} &= 0 \\ -(w_1\beta_{1,w_1} + w_2\beta_{1,w_1}) + (d_2\beta_{2,d_2} + d_2'\beta_{2,d_2'}) - d_3\beta_{3,d_3} + d_4\beta_{4,d_4} &= 0 \end{aligned}$$

$$-(w_1^2\beta_{1,w_1} + w_2^2\beta_{1,w_1}) + (d_2^2\beta_{2,d_2} + {d'_2}^2\beta_{2,d'_2}) - d_3^2\beta_{3,d_3} + d_4^2\beta_{4,d_4} = 0$$
$$-(w_1^3\beta_{1,w_1} + w_2^3\beta_{1,w_1}) + (d_2^3\beta_{2,d_2} + {d'_2}^3\beta_{2,d'_2}) - d_3^3\beta_{3,d_3} + d_4^3\beta_{4,d_4} = 0$$

and this is a system of four linear equation in four unknowns. Substituting the values of the known quantities and solving, we obtain

$$\beta_{2,d_2} = q^2(q^3+1)(q+1), \qquad \beta_{2,d'_2} = q^6(q^2+1)(q^2-q+1),$$
$$\beta_{3,d_3} = q^3(q^2+1)(q^3+1)(q^3-q+1), \quad \text{and} \quad \beta_{2,d_4} = q^9(q^2-q+1).$$

Thus, the resolution of C_2 is completely determined.

We remark that when $k \geq 5$, the minimum weight of C_{k-2} will be $n_k - n_{k-1}$ or $n_k - 1 - q^2 n_{k-2}$ according as k is odd or even. Moreover, a cardinality argument similar to the one in the case of $k = 4$ will show that all 1-dimensional subcodes of C_{k-2} are minimal, and hence the resolution is not pure (at the first step). It would be interesting to completely determine the resolution of C_{k-2}, in general.

Acknowledgements

We are grateful to Trygve Johnsen for helpful discussions and encouragement. The authors are also grateful to the Indo-Norwegian project MAIT: EECC, supported by the Research Council of Norway and the Dept. of Science and Technology of Govt. of India, which facilitated mutual visits that were helpful to complete this work. The second named author would like to acknowledge past funding, during earlier stages of this work, from the Council of Scientific and Industrial Research, India for a doctoral fellowship at IIT Bombay, and from H.C. Ørsted cofund postdoctoral fellowship at the Technical University of Denmark.

References

[1] N. Armenoff, Free Resolutions Associated to Representable Matroids, Ph.D. Thesis, Univ. Kentucky, Lexington, KY, 2015.
[2] E.F. Assmus Jr., J.D. Key, Designs and Their Codes, Cambridge Tracts in Math., vol. 103, Cambridge Univ. Press, 1992.
[3] A. Ashikhmin, A. Barg, Minimal vectors in linear codes, IEEE Trans. Inf. Theory 44 (1998) 2010–2017.
[4] A. Björner, The homology and shellability of matroids and geometric lattices, in: Matroid Applications, in: Encyclopedia Math. Appl., vol. 40, Cambridge Univ. Press, 1992, pp. 226–283.
[5] M. Boij, J. Söderberg, Graded Betti numbers of Cohen-Macaulay modules and the multiplicity conjecture, J. Lond. Math. Soc. 78 (2008) 85–106.
[6] A. Bonisoli, Every equidistant linear code is a sequence of dual Hamming codes, Ars Comb. 18 (1984) 181–186.
[7] R.C. Bose, I.M. Chakravarti, Hermitian varieties in a finite projective space $\mathrm{PG}(N, q^2)$, Can. J. Math. 18 (1966) 1161–1182.
[8] R. Calderbank, W.M. Kantor, The geometry of two-weight codes, Bull. Lond. Math. Soc. 18 (2) (1986) 97–122.
[9] I.M. Chakravarti, Some properties and applications of Hermitian varieties in a finite projective space $\mathrm{PG}(N, q^2)$ in the construction of strongly regular graphs (two-class association schemes) and block designs, J. Comb. Theory, Ser. B 11 (1971) 268–283.
[10] P. Delsarte, J.M. Goethals, F.J. Mac Williams, On generalized Reed-Muller codes and their relatives, Inf. Control 16 (1970) 403–442.
[11] P. Dembowski, Finite Geometries, Ergeb. Math. Grenzgeb., vol. 44, Springer-Verlag, Berlin-Heidelbeg-New York, 1968.
[12] R.H.F. Denniston, Some maximal arcs in finite projective planes, J. Comb. Theory 6 (1969) 317–319.
[13] S.R. Ghorpade, A.R. Shastri, M.K. Srinivasan, J.K. Verma (Eds.), Combinatorial Topology and Algebra, RMS Lec. Notes Ser., vol. 18, Ramanujan Math. Soc., Mysore, 2013.
[14] J. Herzog, M. Kühl, On the Betti numbers of finite pure and linear resolutions, Commun. Algebra 12 (1984) 1627–1646.
[15] T. Johnsen, Private Communication, April 2015.
[16] T. Johnsen, H. Verdure, Hamming weights and Betti numbers of Stanley-Reisner rings associated to matroids, Appl. Algebra Eng. Commun. Comput. 24 (2013) 73–93.
[17] T. Johnsen, H. Verdure, Stanley-Reisner resolution of constant weight codes, Des. Codes Cryptogr. 72 (2014) 471–481.
[18] T. Johnsen, J. Roksvold, H. Verdure, A generalization of weight polynomials to matroids, Discrete Math. 339 (2016) 632–645.
[19] R. Jurrius, R. Pellikaan, Extended and generalized weight enumerators, in: Proc. Int. Workshop on Coding and Cryptography WCC 2009, Selmer Center, Univ. Bergen, Norway, 2009, pp. 76–91, https://www.relindejurrius.nl/publications/2009_WCC.pdf.
[20] Z. Liu, W. Chen, Notes on the value function, Des. Codes Cryptogr. 54 (2010) 11–19.

[21] A. Karpova, Homological Methods Applied to Theory of Codes and Matroids, Master's Thesis, The Arctic Univ. Norway, Tromsø, Norway, 2015.
[22] J.S. Provan, Decompositions, Shellings, and Diameters of Simplicial Complexes and Convex Polyhedra, Ph.D. Thesis, Cornell Univ., Ithaca, NY, 1977.
[23] R.P. Stanley, Cohen-Macaulay complexes, in: Higher Combinatorics, Proc. NATO Advanced Study Inst., Berlin, 1976, Reidel, Dordrecht, 1977, pp. 51–62.
[24] M. Tsfasman, S. Vlăduţ, D. Nogin, Algebraic Geometric Codes: Basic Notions, Math. Surv. Monogr., vol. 139, Amer. Math. Soc., Providence, 2007.
[25] V.K. Wei, Generalized Hamming weights for linear codes, IEEE Trans. Inf. Theory 37 (1991) 1412–1418.