ON THE PURITY OF RESOLUTIONS OF STANLEY-REISNER RINGS ASSOCIATED TO REED-MULLER CODES

SUDHIR R. GHORPADE AND RATI LUDHANI

Abstract. Following Johnsen and Verdure (2013), we can associate to any linear code C an abstract simplicial complex and in turn, a Stanley-Reisner ring R_C. The ring R_C is a standard graded algebra over a field and its projective dimension is precisely the dimension of C. Thus R_C admits a graded minimal free resolution and the resulting graded Betti numbers are known to determine the generalized Hamming weights of C. The question of purity of the minimal free resolution of R_C was considered by Ghorpade and Singh (2020) when C is the generalized Reed-Muller code. They showed that the resolution is pure in some cases and it is not pure in many other cases. Here we give a complete characterization of the purity of graded minimal free resolutions of Stanley-Reisner rings associated to generalized Reed-Muller codes of an arbitrary order.

1. introduction

This article concerns a topic that is at the interface of homological aspects of commutative algebra and the theory of linear error correcting codes. Our motivation comes from the work of Johnsen and Verdure [11] and the more recent work [8]. In [11], the notion of *Betti numbers* of a linear code is introduced. The Betti numbers of a linear code C of length n are, in fact, the graded Betti numbers of the Stanley-Reisner ring R_C of the simplicial complex Δ_C on $[n] := \{1, \dots, n\}$ whose faces are precisely the subsets $\{i_1, \dots, i_t\}$ of $[n]$ for which the columns $H_{i_1}, \dots, H_{i_t}$ of a parity check matrix H of C are linearly independent. In [11], it was shown that the Betti numbers of a linear code determine its generalized Hamming weights. Further, Johnsen, Roksvold and Verdure [13] showed that the Betti numbers of a linear code (and its elongations) determine its generalized weight polynomials and hence the extended weight enumerators. On the other hand, the work of Jurrius and Pellikaan [14] shows that the extended weight enumerators of a linear code determine its generalized weight enumerator. So it is clear that the Betti numbers of a linear code (and its elongations) are also closely related to several classical parameters of that code. Thus it is useful to know them explicitly. Computation of these Betti numbers is in general, a difficult problem, but it becomes easy, by a formula of Herzog and Kühl [10], when the corresponding minimal free resolutions are pure. An intrinsic characterization of purity of the graded minimal free resolutions of Stanley-Reisner rings associated to arbitrary linear codes was obtained in

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.

Rati Ludhani is supported by Prime Minister's Research Fellowship PMRF-192002-256 at IIT Bombay.

[8]. As a consequence, known results about the Betti numbers of MDS codes (cf. [11]) and constant weight codes (cf. [12]) were easily deduced.

One of the most important and widely studied class of linear codes is that of Reed-Muller codes. These codes were introduced by Reed [18] in the binary case and several of their properties were established by Muller [17]; see also [4, pp. 20–38]. We shall consider Reed-Muller codes in the most general sense, as given by Kasami, Lin and Peterson [15] and by Delsarte, Goethals, and MacWilliams [6]. Generalized Hamming weights of (generalized) Reed-Muller codes are explicitly known, thanks to the work of Heijnen and Pellikaan [9] (see also [2] and [3]). It is, therefore, natural, to ask for an explicit determination of the Betti numbers of Reed-Muller codes. The problem would be tractable if we know when the graded minimal free resolutions of Stanley-Reisner rings of simplicial complexes corresponding to Reed-Muller codes are pure. This question about purity was considered in [8] and an answer was provided in many, but not all, cases. In this article we build upon the work in [8] and complete it to give a characterization of purity of graded minimal free resolutions of Stanley-Reisner rings associated to arbitrary Reed-Muller codes.

This paper is organized as follows. In Section 2, we review (generalized) Reed-Muller codes and discuss their properties that are relevant for us. Next, in Section 3, the notion of purity of a minimal free resolution is recalled and some key results in [8], such as the intrinsic characterization mentioned above and results about the purity or non-purity of resolutions corresponding to Reed-Muller codes, are stated. Our main result on a characterization of purity of free resolutions of Stanley-Reisner rings associated to Reed-Muller codes is also proved here. As a corollary, we give a characterization of Reed-Muller codes that are MDS codes.

2. Reed-Muller codes

Standard references for (generalized) Reed-Muller codes are the book of Assmus and Key [1] (especially, Chapter 5) and the seminal paper of Delsarte, Goethals, and MacWilliams [6]. Let us begin by setting some basic notation and terminology.

Fix throughout this paper a prime power q and a finite field $\mathbb{F}_q$ with q elements. Let n, k be integers with $1 \le k \le n$. We write $[n,k]_q$*-code* to mean a q-ary linear code of length n and dimension k, i.e., a k-dimensional $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$. Recall that the *Hamming weight* of an element $c = (c_1, \dots, c_n) \in \mathbb{F}_q^n$ is defined by

$$\mathrm{wt}(c) := |\{i \in \{1, \dots, n\} : c_i \neq 0\}|.$$

The *minimum distance* of an $[n,k]_q$-code C can be defined by

$$d(C) := \min\{\mathrm{wt}(c) : c \in C\}$$

and if $d(C) = d$, then C may be referred to as an $[n,k,d]_q$-code. In this case, the elements of C of Hamming weight d will be referred to as the *minimum weight codewords* of C. An $[n,k]_q$-code is said to be *nondegenerate* if it is not contained in a coordinate hyperplane of $\mathbb{F}_q^n$. We denote by $\mathbb{N}$ the set of nonnegative integers.

Let m, r be integers such that $m \ge 1$ and $0 \le r \le m(q-1)$. Define

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

Note that $V_q(r,m)$ is a $\mathbb{F}_q$-linear subspace of the polynomial ring $\mathbb{F}_q[X_1, \dots, X_m]$. Fix an ordering $\mathsf{P}_1, \dots, \mathsf{P}_{q^m}$ of the elements of $\mathbb{F}_q^m$ and consider the evaluation map

$$(1) \quad \mathrm{Ev} : V_q(r,m) \to \mathbb{F}_q^{q^m} \quad \text{defined by} \quad f \mapsto c_f := (f(\mathsf{P}_1), \dots, f(\mathsf{P}_{q^m})).$$

Clearly, Ev is a linear map and its image is a nondegenerate linear code of length q^m; this code is called the *(generalized) Reed-Muller code of order* r, and it is denoted by $\mathsf{RM}_q(r,m)$. The dimension of $\mathsf{RM}_q(r,m)$ is given by the following formula that can be found in Assmus and Key [1, Theorem 5.4.1]:

$$\dim \mathsf{RM}_q(r,m) = \sum_{s=0}^{r}\sum_{i=0}^{m}(-1)^i\binom{m}{i}\binom{s-iq+m-1}{s-iq}. \tag{2}$$

In [8, eq. (13)], a somewhat simpler formula for the dimension is stated (without proof). It is not difficult to derive it from (2). However, we give an independent and direct proof of the simpler formula below.

Lemma 1. *Let m, r be integers such that $m \geq 1$ and $0 \leq r \leq m(q-1)$. Then*

$$\dim \mathsf{RM}_q(r,m) = \sum_{i=0}^{m}(-1)^i\binom{m}{i}\binom{m+r-iq}{m}. \tag{3}$$

Proof. It is well-known that the map Ev given by (1) is injective. This follows, for instance, from [7, Lemma 2.1]. Also, if $E := \{(v_1,\dots,v_m)\in\mathbb{N}^m : v_1+\dots+v_m \leq r\}$, then it is easily seen that a basis of $V_q(r,m)$ is given by

$$B := \{X_1^{v_1}\cdots X_m^{v_m} : (v_1,\dots,v_m)\in E \text{ and } 0\leq v_j<q \text{ for } 1\leq j\leq m\}.$$

Let $E_j := \{(v_1,\dots,v_m)\in E : v_j \geq q\}$ for $1\leq j\leq m$. The set B is clearly in bijection with $E\setminus(E_1\cup\dots\cup E_m)$. It is elementary and well-known that $|E| = \binom{m+r}{m}$. By changing v_j to $v_j' = v_j - q$, we also see that $|E_j| = \binom{m+r-q}{m}$ for $1\leq j\leq m$, and more generally, $|E_{j_1}\cap\dots\cap E_{j_i}| = \binom{m+r-iq}{m}$ for $1\leq j_1<\dots<j_i\leq m$. It follows that $\dim\mathsf{RM}_q(r,m) = \dim V_q(r,m) = |B|$, and this is equal to

$$\begin{aligned}|E| - |E_1\cup\dots\cup E_m| &= \binom{m+r}{m} - \sum_{i=1}^{m}(-1)^{i-1}\sum_{1\leq j_1<\dots<j_i\leq m}|E_{j_1}\cap\dots\cap E_{j_i}|\\ &= \binom{m+r}{m} - \sum_{i=1}^{m}(-1)^{i-1}\binom{m}{i}\binom{m+r-iq}{m}.\end{aligned}$$

The last expression is clearly equal to the desired formula in (3). □

Remark 2. In case $0\leq r<q$, formula (3) simplifies to $\dim\mathsf{RM}_q(r,m) = \binom{m+r}{m}$. This can also be seen by noting that the set E_j in the proof above is empty for each $j = 1,\dots,m$ when $r<q$. On the other hand, if $r = m(q-1)$, then the map Ev given by (1) is also surjective. To see this, write $\mathsf{P}_\nu = (a_{\nu 1},\dots,a_{\nu m})$ and consider

$$F_\nu(X_1,\dots,X_m) := \prod_{j=1}^{m}\left(1-(X_j-a_{\nu j})^{q-1}\right) \quad \text{for } \nu = 1,\dots,q^m. \tag{4}$$

Note that for any $\nu\in\{1,\dots,q^m\}$, the polynomial F_ν is in $V_q(m(q-1),m)$ and it has the property that $F_\nu(\mathsf{P}_\nu) = 1$ and $F_\nu(\mathsf{P}_\mu) = 0$ for any $\mu\in\{1,\dots,q^m\}$ with $\mu\neq\nu$. Hence any $\lambda = (\lambda_1,\dots,\lambda_{q^m})\in\mathbb{F}_q^{q^m}$ can be written as $\lambda = \mathrm{Ev}(F)$, where $F = \lambda_1F_1+\dots+\lambda_{q^m}F_{q^m}$. It follows that $\mathsf{RM}_q(m(q-1),m) = \mathbb{F}_q^{q^m}$. In particular, Lemma 1 yields the following curious identity:

$$\sum_{i=0}^{m}(-1)^i\binom{m}{i}\binom{(m-i)q}{m} = q^m \quad \text{or equivalently,} \quad \sum_{i=0}^{m}(-1)^i\binom{m}{i}\binom{iq}{m} = (-q)^m.$$

It may be interesting to obtain a direct proof of the above identity.

We now recall the following important result about the minimum distance and the minimum weight codewords of Reed-Muller codes.

Proposition 3. *Let m, r be integers such that $m \geq 1$ and $0 \leq r \leq m(q-1)$. Then there are unique $t, s \in \mathbb{N}$ such that*

$$r = t(q-1) + s \quad \text{and} \quad 0 \leq s \leq q-2. \tag{5}$$

With t, s as above, the minimum distance of $\mathsf{RM}_q(r,m)$ is given by

$$d = (q-s)q^{m-t-1}. \tag{6}$$

Further, if $f \in V_q(r,m)$ is given by

$$f(X_1, \ldots, X_m) = \omega_0 \prod_{i=1}^{t} \left(1 - (X_i - \omega_i)^{q-1}\right) \prod_{j=1}^{s} (X_{t+1} - \omega'_j) \tag{7}$$

where $\omega_0, \omega_1, \ldots, \omega_t \in \mathbb{F}_q$ with $\omega_0 \neq 0$ and $\omega'_1, \ldots, \omega'_s$ are any distinct elements of $\mathbb{F}_q$, then $\mathrm{Ev}(f)$ is a minimum weight codeword of $\mathsf{RM}_q(r,m)$. Moreover, every minimum weight codeword of $\mathsf{RM}_q(r,m)$ is of the form $\mathrm{Ev}(g)$, where g is obtained from a polynomial of the form (7) by substituting for $X_1, \ldots, X_{t+1}$ any $(t+1)$ linearly independent linear forms in $\mathbb{F}_q[X_1, \ldots, X_m]$.

Proof. The formula in (6) follows from [6, Theorem 2.6.1] and [15, Theorem 5]. The assertion about the minimum weight codewords is proved in [6, Theorem 2.6.3] (see also [16, Theorem 1]). □

We end this section by observing that the Reed-Muller code $\mathsf{RM}_q(r,m)$ is a particularly nice code when m is small or when r is either very small or very large.

Lemma 4. *Let m, r be integers such that $m \geq 1$ and $0 \leq r \leq m(q-1)$. Then $\mathsf{RM}_q(r,m)$ is an MDS code in each of the following cases: (i) $m = 1$, (ii) $r = 0$, (iii) $r = m(q-1)$, and (iv) $r = m(q-1) - 1$.*

Proof. (i) If $0 \leq r < q$, then in view of Remark 2 and Proposition 3, we see that $\mathsf{RM}_q(r,1)$ is a $[q,\, r+1,\, q-r]_q$-code, and hence it is an MDS code.

(ii) Clearly, $\mathsf{RM}_q(0,m)$ is the 1-dimensional code of length q^m spanned by the all-1 vector, and this is evidently an MDS code.

(iii) From Remark 2, $\mathsf{RM}_q(m(q-1),m) = \mathbb{F}_q^{q^m}$, which is obviously an MDS code.

(iv) Suppose $r = m(q-1) - 1$. We will show that

$$\mathsf{RM}_q(r,m) = \Lambda, \quad \text{where} \quad \Lambda := \left\{ (\lambda_1, \ldots, \lambda_{q^m}) \in \mathbb{F}_q^{q^m} : \lambda_1 + \cdots + \lambda_{q^m} = 0 \right\}. \tag{8}$$

This would imply that $\mathsf{RM}_q(r,m)$ is a $[q^m, q^m - 1, 2]_q$-code, and hence an MDS code. To prove (8), first note that the monomial $X_1^{q-1} \cdots X_m^{q-1}$ is in $V_q(m(q-1),m)$, but not in the subspace $V_q(r,m)$. Since we have seen in Remark 2 that Ev gives an isomorphism of $V_q(m(q-1),m)$ onto $\mathbb{F}_q^{q^m}$, it follows that $\dim_{\mathbb{F}_q} V_q(r,m) \leq q^m - 1$. Hence it suffices to show that $\Lambda \subseteq \mathsf{RM}_q(r,m)$. To this end, we assume without loss of generality that the ordering $\mathsf{P}_1, \ldots, \mathsf{P}_{q^m}$ of points of $\mathbb{F}_q^m$ is such that P_1 is the origin. For $1 \leq \nu \leq q^m$, consider the polynomial F_ν given by (4), and write

$$F_\nu = F_1 + G_\nu, \quad \text{where} \quad F_1 = \prod_{j=1}^{m} \left(1 - X_j^{q-1}\right) \quad \text{and} \quad G_\nu := F_\nu - F_1.$$

Note that $G_\nu \in V_q(r,m)$ for each $\nu = 1, \ldots, q^m$. Also, $F_1(\mathsf{P}_1) = 1$ and $F_1(\mathsf{P}_\mu) = 0$ for $2 \leq \mu \leq q^m$. So in view of the properties of F_ν noted in Remark 2, we see that

$G_1(\mathsf{P}_1) = 0$ while $G_\nu(\mathsf{P}_1) = -1$ and $G_\nu(\mathsf{P}_\nu) = 1$ for $2 \le \nu \le q^m$, and moreover, $G_\nu(\mathsf{P}_\mu) = 0$ for $2 \le \nu, \mu \le q^m$ with $\nu \ne \mu$. Thus given any $\lambda = (\lambda_1, \dots, \lambda_{q^m}) \in \Lambda$, the polynomial $G := \sum_{\nu=1}^{q^m} \lambda_\nu G_\nu \in V_q(r, m)$ and $\mathrm{Ev}(G) = \lambda$. This proves (8). □

Remark 5. In [8, pp. 8–9], the results in Lemma 4, especially (iv), were deduced by appealing to the structure of duals of Reed-Muller codes. Here we have chosen to give a more direct and elementary proof. We remark also that the converse of the result in Lemma 4 is true. An indirect proof of this is given later; see Corollary 11.

3. Characterizations of Purity

Let $n, k \in \mathbb{N}$ with $1 \le k \le n$ and let C be an $[n, k]_q$-code. We have explained in the introduction how one can associate an abstract simplicial complex Δ_C to C. Note that this complex is independent of the choice of a parity check matrix of C. Let $R := \mathbb{F}_q[x_1, \dots, x_n]$ denote the polynomial ring in n variables over $\mathbb{F}_q$ and let I_C denote the ideal of R generated by the monomials $x_{i_1} \cdots x_{i_t}$ where $\{i_1, \dots, i_t\}$ vary over non-faces, i.e., over subsets of $[n] := \{1, \dots, n\}$ that are not in Δ_C. The Stanley-Reisner ring R_C corresponding to Δ_C (with the base field[1] $\mathbb{F}_q$) is, by definition, the quotient R/I_C. We call R_C the *Stanley-Reisner ring* associated to C. Clearly, R_C is a finitely generated standard graded $\mathbb{F}_q$-algebra and as noted in [8, §1], R_C is Cohen-Macaulay and it admits an $\mathbb{N}$-graded minimal free resolution of the form

$$F_k \longrightarrow F_{k-1} \longrightarrow \cdots \longrightarrow F_1 \longrightarrow F_0 \longrightarrow R_\Delta \longrightarrow 0 \tag{9}$$

where $F_0 = R$ and each F_i is a graded free R-module of the form

$$F_i = \bigoplus_{j \in \mathbb{Z}} R(-j)^{\beta_{i,j}} \quad \text{for } i = 0, 1, \dots, k. \tag{10}$$

The nonnegative integers $\beta_{i,j}$ thus obtained are called the *Betti numbers* of C. The resolution (9) is said to be *pure* of type $(d_0, d_1, \dots, d_k)$ if for each $i = 0, 1, \dots, k$, the Betti number $\beta_{i,j}$ is nonzero if and only if $j = d_i$. If, in addition, $d_1, \dots, d_k$ are consecutive, then the resolution is said to be *linear*. We remark that the Betti numbers $\beta_{i,j}$ as well as the properties of purity and linearity depend only on C and they are independent of the choice of a minimal free resolution of R_C.

The result below is due to Johnsen and Verdure [11]; see also [8, Corollary 3.9].

Proposition 6. *Let C be an $[n, k]_q$-code. Then C is an MDS code if and only if C is nondegenerate and every $\mathbb{N}$-graded minimal free resolution of R_C is linear.*

We will now recall the intrinsic characterization of purity given in [8] and alluded to in the Introduction. But first, we review some relevant terminology about codes.

Let n, k and C be as above. By a *subcode* of C we mean a $\mathbb{F}_q$-linear subspace of C. Given a subcode D of C, the *support* of D and the *weight* of D are defined by

$$\mathrm{Supp}(D) := \{i \in [n] : \exists\ (c_1, \dots, c_n) \in D \text{ with } c_i \ne 0\} \quad \text{and} \quad \mathrm{wt}(D) := |\mathrm{Supp}(D)|.$$

[1] It is only for the sake of definitiveness that we take the base field to be $\mathbb{F}_q$. We could in fact replace $\mathbb{F}_q$ by an arbitrary field, Indeed, it is known that for Stanely-Reisner rings associated to linear codes, and more generally, matroids, the Betti numbers are independent of the choice of a base field; see, e.g., [11, Renark 1]. On the other hand, there are examples of simplicial complexes for which the Betti numbers of their Stanely-Reisner rings do depend on the choice of the base field even when the complex is shellable (see, e.g., [19, Examples 3.3, 3.4]) or stronger still, vertex decomposable (see, e.g., [5, p. 567]).

Given any $c \in C$, we often denote by $\mathrm{Supp}(c)$ and $\mathrm{wt}(c)$ the support of $\langle c\rangle$ and the weight of $\langle c\rangle$, respectively, where $\langle c\rangle$ denotes the subcode of C spanned by c. For $1 \le i \le k$, the i^{th} *generalized Hamming weight* of C is defined by

$$d_i(C) := \min\{\mathrm{wt}(D) : D \text{ a subcode of } C \text{ with } \dim D = i\}.$$

It is obvious that $d_1(C) = d(C)$ and it is well-known $d_i(C) < d_{i+1}(C)$ for $1 \le i \le k-1$; see, e.g., [20, Theorem 1]. Note that C is nondegenerate if and only if $d_k(C) = n$. An i-dimensional subcode D of C is said to be *i-minimal* if its support is minimal among the supports of all i-dimensional subcodes of C, i.e., $\mathrm{Supp}(D') \nsubseteq \mathrm{Supp}(D)$ for any i-dimensional subcode D' of C, with $D' \neq D$.

We are now ready to state (an equivalent version of) the intrinsic characterization of purity given in [8, Theorem 3.6].

Proposition 7. *Let C be an $[n,k]_q$-code and let $d_1 < \cdots < d_k$ be its generalized Hamming weights. Also, let R_C be the Stanley-Reisner ring associated to C. Then every $\mathbb{N}$-graded minimal free resolution of R_C is not pure if and only if for some $i \in \{1,\dots,k\}$, there exists an i-minimal subcode D_i of C such that $\mathrm{wt}(D_i) > d_i$.*

We summarize below the results in [8] about the purity and non-purity of graded minimal free resolutions of Stanley-Reisner ring associated to Reed-Muller codes.

Proposition 8. *Let m, r be integers such that $m \ge 1$ and $0 \le r \le m(q-1)$. Also, let t, s be unique nonnegative integers satisfying (5). Then every $\mathbb{N}$-graded minimal free resolution of the Stanley-Reisner ring associated to $\mathsf{RM}_q(r,m)$ is*

(i) *pure if $r = 1$,*
(ii) *not pure if $q = 2$, $m \ge 4$, and $1 < r \le m-2$, and*
(iii) *not pure if $m \ge 2$, $1 < r < m(q-1)-1$, and $s \neq 1$.*

Proof. The assertion in (i) is proved in [8, Theorem 4.1], while the assertions in (ii) and (iii) are proved in [8, Proposition 4.4] and [8, Theorem 4.11], respectively. □

The values of q, m, r not covered by (i)–(iv) in Lemma 4 and (i)–(iii) in Proposition 8 are precisely $q \ge 3$, $m \ge 2$, and $r = q,\ 2q-1, \dots, (m-1)q-(m-2)$, except that $(m-1)q-(m-2)$ is excluded if $q = 3$. This is taken care of by the following.

Lemma 9. *Let m, r be integers such that $m \ge 2$ and $1 < r < m(q-1)-1$. Also let t, s be unique integers satisfying (5). Assume that $q \ge 3$ and also that $s = 1$. Then every $\mathbb{N}$-graded minimal free resolution of the Stanley-Reisner ring associated to the Reed-Muller code $\mathsf{RM}_q(r,m)$ is not pure.*

Proof. The conditions on m, r and our assumptions imply that $1 \le t \le m-1$ and moreover if $q = 3$, then $1 \le t \le m-2$. Also note that by Proposition 3, the minimum distance of $\mathsf{RM}_q(r,m)$ is given by $d = (q-1)q^{m-t-1}$. We will divide the proof in two cases according as $q > 3$ and $q = 3$.

Case 1. $q > 3$.

Write $\mathbb{F}_q = \{\omega_1, \dots, \omega_q\}$, and let ω_1', ω_2' be two distinct elements of $\mathbb{F}_q$. Define

$$Q(X_1,\dots,X_m) := \left(\prod_{i=1}^{t-1}(X_i^{q-1}-1)\right)\left(\prod_{j=3}^{q}(X_t-\omega_j)\right)\left(\prod_{k=1}^{2}(X_{t+1}-\omega_k')\right).$$

Then $\deg(Q) = (t-1)(q-1)+(q-2)+2 = (t-1)(q-1)+q = t(q-1)+1 = r$, and thus $Q \in V_q(r,m)$. For $i = 1, 2$, let

$$A_i := \left\{\mathbf{a} = (a_1,\dots,a_m) \in \mathbb{F}_q^m : a_1 = \cdots = a_{t-1} = 0,\ a_t = \omega_i \text{ and } a_{t+1} \notin \{\omega_1', \omega_2'\}\right\}.$$

Then $\mathrm{Supp}(c_Q) = A_1 \cup A_2$. Observe that A_1 and A_2 are disjoint. Consequently,

$$\mathrm{wt}(c_Q) = 2(q-2)q^{m-t-1} \quad \text{and therefore} \quad \mathrm{wt}(c_Q) > d = (q-1)q^{m-t-1},$$

where the last inequality follows since $q > 3$. Thus c_Q is not a minimum weight codeword. We claim that the 1-dimensional subcode $\langle c_Q \rangle$ is 1-minimal. This claim together with Proposition 7 would imply the desired result. To prove the claim, assume the contrary. Thus, suppose there is $F \in V_q(r, m)$, such that c_F is a minimum weight codeword of $\mathsf{RM}_q(r, m)$ and $\mathrm{Supp}(c_F) \subsetneq \mathrm{Supp}(c_Q)$. By Proposition 3, F must be of the form

$$F(X_1, \dots, X_m) = \omega_0 \left(\prod_{i=1}^{t} (1 - L_i^{q-1}) \right) (L_{t+1} - \omega) \tag{11}$$

for some $\omega_0, \omega \in \mathbb{F}_q$ with $\omega_0 \neq 0$ and some linearly independent linear polynomials $L_1, \dots, L_{t+1}$ in $\mathbb{F}_q[X_1, \dots, X_m]$, with L_{t+1} homogeneous (while $L_1, \dots, L_t$ are not necessarily homogeneous). Note that $\mathrm{Supp}(c_F) = A'$, where

$$A' := \left\{ \mathbf{a} = (a_1, \dots, a_m) \in \mathbb{F}_q^m : L_i(\mathbf{a}) = 0 \text{ for } 1 \leq i \leq t \text{ and } L_{t+1}(\mathbf{a}) \neq \omega \right\}. \tag{12}$$

Since $\mathrm{Supp}(c_F) \subset \mathrm{Supp}(c_Q)$, we obtain $A' \subset A_1 \cup A_2$. We now assert that A' is disjoint from one of the A_i. Indeed, if the assertion is not true, then we can choose $P_i \in A' \cap A_i$ for $i = 1, 2$. Write $b_i := L_{t+1}(P_i)$ for $i = 1, 2$. Since $P_i \in A'$, we see that $b_i \neq \omega$ for $i = 1, 2$. Now pick $\lambda \in \mathbb{F}_q$ such that $\lambda \neq 0, 1$ and $(1-\lambda)b_1 + \lambda b_2 \neq \omega$, which is possible because $q \geq 4$.[1] Define $P_\lambda := (1-\lambda)P_1 + \lambda P_2$. Then $P_\lambda \in A'$, and this contradicts the inclusion $A' \subset A_1 \cup A_2$ because the t^{th} coordinate of P_λ is neither ω_1 nor ω_2. This proves the above assertion. Thus $\mathrm{Supp}(c_F) = A' \subseteq A_i$ for some i. But then $(q-1)q^{m-t-1} \leq (q-2)q^{m-t-1}$, which is a contradiction. This proves the claim and hence the desired result when $q > 3$.

Case 2. $q = 3$.

In this case $1 \leq t \leq m-2$, as noted earlier. Write $\mathbb{F}_q = \{\omega_1, \omega_2, \omega_3\}$. Define

$$Q(X_1, \dots, X_m) := \left(\prod_{i=1}^{t-1} (X_i^{q-1} - 1) \right) (X_t - \omega_3)(X_{t+1} - \omega_3)(X_{t+2} - \omega_3).$$

Then $\deg(Q) = (t-1)(q-1) + 3 = t(q-1) + 1 = r$, since $q = 3$, and so $Q \in V_q(r, m)$. Let $E := \left\{ \mathbf{a} = (a_1, \dots, a_m) \in \mathbb{F}_q^m : a_1 = \dots = a_{t-1} = 0 \right\}$, and for $i = 1, 2$, let

$$\begin{aligned} A_i &:= \{\mathbf{a} = (a_1, \dots, a_m) \in E : a_t = \omega_i \text{ and } a_{t+1}, a_{t+2} \in \{\omega_1, \omega_2\}\}, \\ A_i' &:= \{\mathbf{a} = (a_1, \dots, a_m) \in E : a_{t+1} = \omega_i \text{ and } a_t, a_{t+2} \in \{\omega_1, \omega_2\}\}, \text{ and} \\ A_i'' &:= \{\mathbf{a} = (a_1, \dots, a_m) \in E : a_{t+2} = \omega_i \text{ and } a_t, a_{t+1} \in \{\omega_1, \omega_2\}\}. \end{aligned}$$

Then $\mathrm{Supp}(c_Q) = A_1 \cup A_2 = A_1' \cup A_2' = A_1'' \cup A_2''$ and $\mathrm{wt}(c_Q) = 2^3 q^{m-t-2}$. Note that $\mathrm{wt}(c_Q) > (q-1)q^{m-t-1}$, since $q = 3$. Thus, as in Case 1, it suffices to show that there does not exist any $F \in V_q(r, m)$ such that c_F is a minimum weight codeword and $\mathrm{Supp}(c_F) \subsetneq \mathrm{Supp}(c_Q)$. Suppose, if possible, there is such F. Then it must be of the form (11), and its support is given by the set A' in (12). Now write $\mathbb{F}_q \setminus \{\omega\} = \{u_1, u_2\}$, and for $i = 1, 2$, let

$$B_i := \left\{ \mathbf{a} = (a_1, \dots, a_m) \in \mathbb{F}_q^m : L_i(\mathbf{a}) = 0 \text{ for } 1 \leq i \leq t \text{ and } L_{t+1}(\mathbf{a}) = u_i \right\}.$$

[1] If $b_1 = b_2$, then the only condition on λ is that $\lambda \neq 0, 1$, whereas if $b_1 \neq b_2$, then it suffices to choose $\lambda \in \mathbb{F}_q$ such that $\lambda \neq 0, 1$ and $\lambda \neq (\omega - b_1)/(b_2 - b_1)$.

Note that each B_i is an affine space (i.e., a translate of a linear subspace) in $\mathbb{F}_q^m$ and $\mathrm{Supp}(c_F) = B_1 \cup B_2$. Thus $B_1 \cup B_2 \subset A_1 \cup A_2$. We claim that $B_1 \subseteq A_i$ for some $i \in \{1, 2\}$. Indeed, if this is not true, then we can find $P_i \in B_1 \cap A_i$ for each $i = 1, 2$. Since $q = 3$, we can choose $\lambda \in \mathbb{F}_q$ such that $\lambda \neq 0, 1$. Consider $P_\lambda := (1 - \lambda)P_1 + \lambda P_2$. Since B_1 is an affine space, $P_\lambda \in B_1$. On the other hand, the t^{th} coordinate of P_λ is neither ω_1 nor ω_2, and hence $P_\lambda \notin A_1 \cup A_2$. This contradicts the inclusion $B_1 \subset A_1 \cup A_2$, and so the claim is proved. In a similar manner, we see that $B_1 \subseteq A'_j$ and $B_1 \subseteq A''_k$ for some $j, k \in \{1, 2\}$. It follows that $B_1 \subseteq A_i \cap A'_j \cap A''_k$. But clearly, $|B_1| = q^{m-t-1}$ and $|A_i \cap A'_j \cap A''_k| = q^{m-t-2}$. So we obtain $q^{m-t-1} \leq q^{m-t-2}$, which is a contradiction. This completes the proof. □

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

Theorem 10. *Let $m, r \in \mathbb{N}$ be such that $m \geq 1$ and $0 \leq r \leq m(q-1)$. Then every $\mathbb{N}$-graded minimal free resolution of the Stanley-Reisner ring associated to the Reed-Muller code $\mathsf{RM}_q(r, m)$ is pure if and only if $m = 1$ or $r \leq 1$ or $r \geq m(q-1) - 1$.*

Proof. Follows from Lemma 4, Proposition 6, Proposition 8, and Lemma 9. □

As an application, we show that the converse of the result in Lemma 4 is true.

Corollary 11. *Let $m, r \in \mathbb{N}$ be such that $m \geq 1$ and $0 \leq r \leq m(q-1)$. Then the Reed-Muller code $\mathsf{RM}_q(r, m)$ is an MDS code if and only if $m = 1$ or $r = 0$ or $r \geq m(q-1) - 1$.*

Proof. If $m = 1$ or $r = 0$ or $r \geq m(q-1) - 1$, then by Lemma 4, $\mathsf{RM}_q(r, m)$ is an MDS code. Conversely, suppose $\mathsf{RM}_q(r, m)$ is an MDS code. Then by Proposition 6, every $\mathbb{N}$-graded minimal free resolution of its Stanley-Reisner ring is pure. So by Theorem 10, we must have $m = 1$ or $r \leq 1$ or $r \geq m(q-1) - 1$. If $m \geq 2$, then the case $r = 1$ is ruled out because by [8, Theorem 4.1], the generalized Hamming weights (which coincide with the "shifts" in the resolution) of $\mathsf{RM}_q(1, m)$ are given by $d_i = q^m - \lfloor q^{m-i} \rfloor$ for $1 \leq i \leq m + 1$, and these are clearly non-consecutive if $m \geq 2$, and so by Proposition 6, $\mathsf{RM}_q(1, m)$ cannot be an MDS code if $m \geq 2$. Thus we must have $m = 1$ or $r = 0$ or $r \geq m(q-1) - 1$. □

References

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

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

[3] P. Beelen, A note on the generalized Hamming weights of Reed-Muller codes, *Appl. Algebra Engrg. Comm. Comput.* **30** (2019), 233–242.

[4] E. R. Berlekamp (Ed.), *Key Papers in the Development of Coding Theory*, IEEE Press, New York, 1974.

[5] K. Dalili and M. Kummini, Dependence of Betti numbers on characteristic, *Comm. Algebra* **42** (2014), 563–570.

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

[7] S. R. Ghorpade, A note on Nullstellensatz over finite fields, in: *Contributions in Algebra and Algebraic Geometry*, pp. 23–32, *Contemp. Math.*, **738**, Amer. Math. Soc., Providence, 2019.

[8] S. R. Ghorpade and P. Singh, Pure Resolutions, linear codes, and Betti numbers. *J. Pure Appl. Algebra* **224** (2020), no. 10, Art. 106385, 22 pp.

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

[10] J. Herzog and M. Kühl, On the Betti numbers of finite pure and linear resolutions, *Comm. Algebra* **12** (1984), 1627–1646.

[11] T. Johnsen and H. Verdure, Hamming weights and Betti numbers of Stanley-Reisner rings associated to matroids, *Appl. Algebra Engrg. Comm. Comput.* **24** (2013), 73–93.

[12] T. Johnsen and H. Verdure, Stanley-Reisner resolution of constant weight codes, *Des. Codes Cryptogr.*, **72** (2014), 471–481.

[13] T. Johnsen, J. Roksvold, and H. Verdure, A generalization of weight polynomials to matroids, *Discrete Math.*, **339** (2016), 632–645.

[14] R. Jurrius and 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

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

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

[17] D. E. Muller, Application of Boolean algebra to switching circuit design and to error detection, *IRE Trans. Electron. Comput.* **EC-3** (1954), no. 3, 6–12.

[18] I. S. Reed, A class of multiple-error-correcting codes and the decoding scheme, *IRE Trans. Inform. Theory* **PGIT-4** (1954), 38–49.

[19] N. Terai and T. Hibi, Some results on Betti numbers of Stanley-Reisner rings, *Discrete Math.*, **157** (1996), 311–320.

[20] V. K. Wei, Generalized Hamming weights for linear codes, *IEEE Trans. Inform. Theory* **37** (1991), 1412–1418.

Department of Mathematics, Indian Institute of Technology Bombay,
Powai, Mumbai 400076, India
E-mail address: srg@math.iitb.ac.in

Department of Mathematics, Indian Institute of Technology Bombay,
Powai, Mumbai 400076, India
E-mail address: lrati@math.iitb.ac.in