HIGHER WEIGHT SPECTRA OF VERONESE CODES

TRYGVE JOHNSEN AND HUGUES VERDURE

Abstract. We study q-ary linear codes C obtained from Veronese surfaces over finite fields. We show how one can find the higher weight spectra of these codes, or equivalently, the weight distribution of all extension codes of C over all field extensions of $\mathbb{F}_q$. Our methods will be a study of the Stanley-Reisner rings of a series of matroids associated to each code C.

1. Introduction

Projective Reed-Müller codes is a class of error-correcting codes that has attracted much attention over the last decades. To find the code parameters, including the generalized Hamming weights, has been a difficult task, and some important results concerning this have appeared quite recently. See for example [15], [19], [18], [4], [5], [6], [2] for results on code parameters, and generalized Hamming weights. To find the higher weight spectra of such codes is more difficult, when the order of the projective Reed-Müller codes is higher than one, and to our knowledge there are few results about this. Therefore it is natural to start with the simplest projective Reed-Müller codes of order at least 2, namely the so-called Veronese codes C_q over any finite field $\mathbb{F}_q$, where the $n = q^2 + q + 1$ columns of the generator matrix G_q correspond to the points of $\mathbb{P}^2$. Moreover each row is obtained by taking an element of a basis for the vector space of all homogeneous polynomials of degree 2 in 3 variables, and evaluating it at the points of $\mathbb{P}^2$ (in some fixed order). Since this vector space has dimension 6, there will be 6 such rows. Alternatively one could think of the columns of G_q as the point of the 2-uple Veronese embedding of $\mathbb{P}^2$ in $\mathbb{P}^5$. This is why we call these codes Veronese codes; since they in the way described correspond to the projective system of points of the mentioned Veronese surface (of degree 4 in $\mathbb{P}^5$).

In this article, we are interested in computing the higher weight spectra, that is the number of subcodes of given dimension and weight of C_q.

The code C_2 is MDS and of dimension 6 and length 7, while the code C_3 of dimension 6 and length 13 is more interesting, and it differs both from C_2, and from the codes C_q, for $q \geq 4$, concerning the aspects we study here. We determine

Date: 22/06/2020.

2000 *Mathematics Subject Classification.* 05E45, 94B05, 05B35, 13F55.

T. Johnsen and H. Verdure are with the Department of Mathematics and Statistics, UiT The Arctic University of Norway, 9037 Tromsø, Norway. The authors are grateful to Sudhir Ghorpade, IIT-Bombay for being a valuable discussion partner as the work proceeded, and for the great hospitality, which provided optimal conditions for making the this article possible.

This work was partially supported with a joint grant from RCN, Norway (Project number 280731), and DST, India.

This work was also partially supported by the project Pure Mathematics in Norway, funded by Bergen Research Foundation and Tromsø Research Foundation.

the higher weight spectra and the generalized weight polynomials for both codes in Section 4. For the codes C_q, with $q \geqslant 4$, we give a unified treatment, and determine both their higher weight spectra and their generalized weight polynomials. All elements of the weight spectra, and all coefficients of the generalized weight polynomials, turn out to be polynomials in q, with coefficients $\frac{a}{b}$, where a is an integer, and b an integer dividing 24.

Our methods will consist of finding the $\mathbb{N}$-graded resolutions of the Stanley-Reisner rings of a series of matroids derived from the parity check matroid M_q of each code. The $\mathbb{N}$-graded Betti numbers of these resolutions will give us the generalized weight polynomials $P_j(Z)$ that calculate the usual weight distribution of all extension codes of the C_q over field extensions of $\mathbb{F}_q$. Finally a straightforward and well known conversion formula will, from the knowledge of the $P_j(Z)$, give us the higher weight spectra of the original codes C_q that we study.

In Section 5, we present an alternative method to compute the higher weight polynomials, suggested by one of the referees. It consists of finding directly the higher weight polynomials by computing the number of $\mathbb{F}_q$-rational points on conics defined over field extensions. At the end of the section, we discuss briefly advantages/inconveniences of the two methods.

2. Definitions and notation

Let q be a prime power and let ν_q be the Veronese map that maps $\mathbb{P}^2$ into $\mathbb{P}^5$ over $\mathbb{F}_q$, i.e. (x, y, z) is mapped to $(x^2, xy, xz, y^2, yz, z^2)$, and let V_q be the image, a non-degenerate smooth surface of degree 4. The cardinality $|V|$ of V is $|\mathbb{P}^2| = q^2+q+1$. Fix some order for the points of V, and for each such point, fix a coordinate 6-tuple that represents it. Let G_q be the $(6 \times (q^2 + q + 1))-$ matrix, whose columns are the coordinate 6-tuples of the points of V, taken in the order fixed.

Definition 1. *The Veronese code C_q is the linear $[q^2+q+1, 6]_q$-code with generator matrix G_q.*

For $q = 2$ we thus get a $[7, 6]$-code C_2, and it is well known, for example by looking at its dual code, which is generated by a single code word with no zeroes ([19]), that this is an MDS-code, and then all we are interested to know about this code is well known (A more straightforward method is of course just to calculate all 64 codewords, and check that there is no such word with weight 1). From now on we will assume that $q \geq 4$, and we will give a common description of the C_q for all these q. We will return to the cases $q = 2$ and 3 first in Section 4, where we will comment on, and give the relevant results for these two cases.

2.1. Hamming weights, spectra and generalized weight polynomials.

Definition 2. *Let C be a $[n, k]$ linear code over $\mathbb{F}_q$. Let $\boldsymbol{c} = (c_1, \cdots, c_n) \in C$. The Support of $\boldsymbol{c}$ is the set*

$$Supp(\boldsymbol{c}) = \{i \in \{1, \cdots, n\} : c_i \neq 0\}.$$

Its weight is

$$wt(\boldsymbol{c}) = |Supp(\boldsymbol{c})|.$$

Similarly, if $T \subset C$, then its support and weight are

$$Supp(T) = \bigcup_{\boldsymbol{c} \in T} Supp(\boldsymbol{c}) \text{ and } wt(T) = |Supp(T)|.$$

Important invariants of a code are the generalized Hamming weights, introduced by Wei in [20]:

Definition 3. *Let C be a $[n,k]$ linear code over $\mathbb{F}_q$. Its generalized Hamming weights are*

$$d_i = \min\{wt(D) : D \subset C \text{ is a subcode of dimension } i\}$$

for $1 \leqslant i \leqslant k$.

We also have

Definition 4. *Let C be a $[n,k]$ linear code over $\mathbb{F}_q$. For $1 \leqslant w \leqslant n$ and $1 \leqslant r \leqslant k$, the higher weight spectra of C are*

$$A_w^{(r)} = \left|\{D : D \text{ subcode of } C \text{ of dim. } r \text{ and weight } w\}\right|.$$

In particular, we have

$$d_r = \min\{w : \ A_w^{(r)} \neq 0\}.$$

In [14], Jurrius and Pellikaan show that the number of codewords of a given code extended to a field extension of a given weight can be expressed by polynomials (the generalized weight polynomials). More precisely, if C is a $[n,k]$-code over $\mathbb{F}_q$, then the code $C^{(i)} = C \otimes_{\mathbb{F}_q} \mathsf{F}q^i$ for $i \geqslant 1$ is a $[n,k]$ code over $\mathsf{F}q^i$. Any generator/parity check matrix of C is a generator/parity check matrix of $C^{(i)}$. Then

Theorem 5. *Let C be a (n,k)-code over $\mathbb{F}_q$. Then, there exists polynomials $P_w \in \mathbb{Z}[Z]$ for $0 \leqslant w \leqslant n$ such that*

$$\forall i \geqslant 1, P_w(q^i) = \left|\left\{\boldsymbol{c} \in C^{(i)} : wt(\boldsymbol{c}) = w\right\}\right|.$$

In [13], Jurrius gives a relation between the higher weight spectra and the polynomials defined above, namely

Theorem 6. *Let C be a $[n,k]$ code over $\mathbb{F}_q$. Let $0 \leqslant w \leqslant n$. Then*

$$P_w(q^m) = \sum_{r=0}^{m} A_w^{(r)} \prod_{i=0}^{r-1} (q^m - q^i).$$

2.2. **Matroids, resolutions and elongations.** Our goal in this paper is to find the higher weight spectra for the Veronese codes C_q for $q \geqslant 3$. In order to do this, we will compute the higher weight polynomials of the code, making use of some machinery related to matroids associated to the code and their Stanley-Reisner resolutions.

There are many equivalent definitions of a matroid. We refer to [16] for a deeper study of the theory of matroids.

Definition 7. *A matroid is a pair $(E, \mathcal{I})$ where E is a finite set and $\mathcal{I}$ is a set of subsets of E satisfying*

(R_1) $\emptyset \in \mathcal{I}$
(R_2) *If $I \in \mathcal{I}$ and $J \subset I$, then $J \in \mathcal{I}$*
(R_3) *If $I, J \in \mathcal{I}$ and $|I| < |J|$, then $\exists j \in J \backslash I$ such that $I \cup \{j\} \in \mathcal{I}$.*

The elements of $\mathcal{I}$ are called independent sets. The subsets of E that are not independent are called dependent sets, and inclusion minimal dependent sets are called circuits.

For any $X \subset E$, its rank is

$$r(X) = \max\{|I| : I \in \mathcal{I},\ I \subset X\}$$

and its nullity is $n(X) = |X| - r(X)$. The rank of the matroid is $r(M) = r(E)$. Finally, for any $0 \leqslant i \leqslant |E| - r(M)$,

$$N_i = \{X \subset E :\ n(X) = i\}.$$

Note that N_1 is the set of circuits of the matroid.

If C is a $[n, k]$-linear code given by a $(n-k) \times k$ parity check matrix H, then we can associate to it a matroid $M_C = (E, \mathcal{I})$, where $E = \{1, \cdots, n\}$ and $X \in \mathcal{I}$ if and only if the columns of H indexed by X are linearly independent over $\mathbb{F}_q$. It can be shown that this matroid is independent of the choice of the parity check matrix of the code. In the sequel, we denote by M_q the matroid associated to the Veronese code C_q.

By axioms (R_1) and (R_2), any matroid $M = (E, \mathcal{I})$ is also a simplicial complex on E. Let $\mathbb{K}$ be a field. We can associate to M a monomial ideal I_M in $R = K[\{X_e\}_{e \in E}]$ defined by

$$I_M = < \boldsymbol{X}^\sigma : \sigma \notin \mathcal{I} >$$

where $\boldsymbol{X}^\sigma$ is the monomial product of all X_e for $e \in \sigma$. This ideal is called the Stanley-Reisner ideal of M and the quotient $R_M = R/I_M$ the Stanley-Reisner ring associated to M. We refer to [7] for the study of such objects. As described in [11] the Stanley-Reisner ring has minimal $\mathbb{N}$ and $\mathbb{N}^n$-graded free resolutions

$$0 \leftarrow R_M \leftarrow R \leftarrow \bigoplus_{j \in \mathbb{N}} R(-j)^{\beta_{1,j}} \leftarrow \bigoplus_{j \in \mathbb{N}} R(-j)^{\beta_{2,j}} \leftarrow \cdots \leftarrow \bigoplus_{j \in \mathbb{N}} R(-j)^{\beta_{|E|-r(M),j}} \leftarrow 0$$

and

$$c0 \leftarrow R_M \leftarrow R \leftarrow \bigoplus_{\alpha \in \mathbb{N}^n} R(-\alpha)^{\beta_{1,\alpha}} \leftarrow \bigoplus_{\alpha \in \mathbb{N}^n} R(-\alpha)^{\beta_{2,\alpha}} \leftarrow \cdots \leftarrow \bigoplus_{\alpha \in \mathbb{N}^n} R(-\alpha)^{\beta_{|E|-r(M),\alpha}} \leftarrow 0.$$

In particular the numbers $\beta_{i,j}$ and $\beta_{i,\alpha}$ are independent of the minimal free resolution, (and for a matroid also of the field $\mathbb{K}$) and are called respectively the $\mathbb{N}$-graded and $\mathbb{N}^n$-graded Betti numbers of the matroid. We have

$$\beta_{i,j} = \sum_{wt(\alpha)=j} \beta_{i,\alpha}.$$

We also note that $\beta_{0,0} = 1$.

It is well known that the independent sets of a matroid constitute a shellable simplicial complex. Hence the ring R_M is Cohen-Macaulay, and the length $\min\{i : \beta_{i,j} \neq 0$, for some $j\}$ is $n - r(M)$ by the Auslander-Buchsbaum formula ([1]). When $M = M_C$ is associated to the parity check matroid of a linear code of dimension k, this length is then $n-(n-k)=k$. Moreover, we then have, as a consequence of a more general result by Peskine and Szpiro ([17, Lemma on p. 1422]):

Theorem 8. *Let M be a matroid on a set of cardinality n and of rank $r=n-k$. Then the $\mathbb{N}$-graded Betti numbers of R_M satisfy the equations*

$$\sum_{i=0}^{k}\sum_{j=0}^{n}(-1)^i j^s \beta_{i,j}=0, \tag{1}$$

for $0\leqslant s\leqslant k-1$, where by convention, $0^0=1$.

The k equations (2) from Theorem 8 are often called the Herzog-Kühl equations, and have a particularly nice form and solution when the resolution is pure. See also [3, Equation (2.1)] and [8] for more on this topic.

Remark 9. *For a matroid M of rank r on a set of cardinality n, we define $\phi_j(M)=\sum_{i=0}^{n-r}(-1)^i\beta_{i,j}$. Then the Herzog-Kühl equations can be written:*

$$\sum_{j=0}^{n} j^s\phi_j(M)=0,$$

and it is clear that these equations are independent in the variables $\phi_j(M)$ with a Vandermonde coefficient matrix.

Also, as explained in [11, Theorem 1], we can compute the $\mathbb{N}^n$-graded Betti number $\beta_{i,\alpha}$ as the Euler characteristic of a certain matroid. If M is a matroid and σ is a subset of the ground set E, then M_σ , the restriction of M to σ, is the matroid with independent sets

$$\mathcal{I}(M_\sigma)=\{\tau\in\mathcal{I}(M):\tau\subset\sigma\}\,.$$

Moreover, the Euler characteristic of M is

$$\begin{aligned}\chi(M) &= \sum_{i=0}^{|E|}(-1)^i\left|\{\tau\subset E:|\tau|=i \text{ and } \tau\notin\mathcal{I}\}\right| \\ &= \sum_{i=0}^{|E|}(-1)^{i-1}\left|\{\tau\subset E:|\tau|=i \text{ and } \tau\in\mathcal{I}\}\right|\end{aligned}$$

Theorem 10. *Let M be a matroid on the ground set E. Let $\sigma\subset E$. Then*

$$\beta_{n(\sigma),\sigma}=(-1)^{r(\sigma)-1}\chi(M_\sigma).$$

In particular, for any circuit σ, $\beta_{1,\sigma}=1$.

In [11] generally for matroids, and particularly for matroids associated to codes, we show that:

Theorem 11. *Let C be a $[n,k]$-code over $\mathbb{F}_q$. The $\mathbb{N}$-graded Betti numbers of the matroid M_C satisfy: $\beta_{i,j}\neq 0$ if and only if there exists an inclusion minimal set in N_i of cardinality j. In particular, $d_i=\min\{j:\beta_{i,j}\neq 0\}$.*

Definition 12. *Let $M=(E,\mathcal{I})$ be a matroid, with $|E|=n$, and let $l\geqslant 0$. Then, the l-th elongation of M is the matroid $M^{(l)}=(E,\mathcal{I}^{(l)})$ with*

$$\mathcal{I}^{(l)}=\{I\cup X: I\in\mathcal{I}, X\subset E,\ |X|\leqslant l\}.$$

The l-th elongation of M is a matroid of rank $\min\{n,r(M)+l\}$.

Remark 13. *Another, equivalent, way of defining $M^{(l)}$, is: $M^{(l)}$ is the matroid with the same ground set E as M, and with nullity function $n^{(l)}(X) = \max\{0, n(X) - l\}$, for each $X \subset E$.*

Definition 14. *Let $N_i^{(l)}$ be the set of subsets X of E with $n^{(l)}(X) = i$.*

The following result is trivial, but useful:

Proposition 15. *$N_i^{(l)} = N_{i+l}$, for $i = 0, \cdots, n - r(M) - l$. In particular the inclusion minimal elements of $N_i^{(l)}$ are the same as the inclusion minimal elements of N_{i+l}.*

The main theorem of [12] gives an expression of the generalized weight polynomials of a code in term of the Betti numbers of its associated matroid and its elongations, namely:

Theorem 16. *Let C be a $[n, k]$ code over $\mathbb{F}_q$. We denote by $\beta_{i,j}^{(l)}$ the Betti numbers of the matroids $M_C^{(l)}$. Then, for every $0 \leqslant w \leqslant n$,*

$$P_w(Z) = \sum_{0 \leqslant l \leqslant k-1} \sum_{i \geqslant 0} (-1)^{i+1} \beta_{i,w}^{(l)} Z^l (Z - 1).$$

Remark 17. *The formula in Theorem 16 can also be written as*

$$P_w(Z) = \sum_{l \geqslant 0} \sum_{i \geqslant 0} (-1)^{i+1} (\beta_{i,w}^{(l-1)} - \beta_{i,w}^{(l)}) Z^l.$$

Using Remark 9 we see that this can be written as:

$$P_w(Z) = \sum_{l \geqslant 0} (\phi_w(M^{(l)}) - \phi_w(M^{(l-1)})) Z^l.$$

In any case the input in the formula of Theorem 16 contains the output of the Herzog-Kühl equations for the various $M^{(l)}$ (when those equations are combined with sufficient other information to be solvable). Whether we want to use the set of all $\beta_{i,w}^l$ as this output/input, or are happy to use just the $\phi_w(M^{(l)})$, is a matter of taste or opportunity. It is clear that if one knows all the $\beta_{i.w}^l$ for a fixed w, then one can derive all the $\phi_w(M^{(l)})$, but the converse is not necessarily true. In this paper we choose to find all the $\beta_{i,w}^l$ in order to find all the $P_w(Z)$ since it is not significantly more difficult than to find the weaker, but sufficient, information obtained from all the $\phi_w(M^{(l)})$.

3. Main theorem

We are now able to give our main theorem, namely the higher weight spectra of the Veronese codes. We give here the result for $q \geqslant 4$, as well as the steps of the proof. Later, we will give the results for the degenerate cases $q = 2, 3$.

Theorem 18. *Let $q \geqslant 4$ and consider the Veronese code C_q. Then all the $A_w^{(r)}$ are 0, with the following exceptions:*

$$
\begin{aligned}
A^{(1)}_{q^2-q} &= \tfrac{1}{2}(q^4+2q^3+2q^2+q)\\
A^{(1)}_{q^2} &= q^5+q+1\\
A^{(1)}_{q^2+q} &= \tfrac{1}{2}(q^4-q)\\
A^{(2)}_{q^2-1} &= q^4+q^3+q^2\\
A^{(2)}_{q^2} &= q^3+2q^2+2q+1\\
A^{(2)}_{q^2+q-3} &= \tfrac{1}{24}(q^8-q^6-q^5+q^3)\\
A^{(2)}_{q^2+q-2} &= \tfrac{1}{2}(q^7+q^6-q^4-q^3)\\
A^{(2)}_{q^2+q-1} &= \tfrac{1}{4}(q^8+5q^6+7q^5+4q^4-q^3-4q^2)\\
A^{(2)}_{q^2+q} &= \tfrac{1}{6}(2q^8+3q^7+q^6+4q^5+9q^4+5q^3-6q)\\
A^{(2)}_{q^2+q+1} &= \tfrac{1}{8}(3q^8+q^6-3q^5-q^3)\\
A^{(3)}_{q^2} &= q^2+q+1\\
A^{(3)}_{q^2+q-2} &= \tfrac{1}{6}(q^6+2q^5+2q^4+q^3)\\
A^{(3)}_{q^2+q-1} &= \tfrac{1}{2}(q^7+2q^6+3q^5+3q^4+2q^3+q^2)\\
A^{(3)}_{q^2+q} &= \tfrac{1}{2}(2q^8+2q^7+3q^6+2q^5+4q^4+3q^3+2q^2)\\
A^{(3)}_{q^2+q+1} &= \tfrac{1}{6}(6q^9+3q^7+2q^6+q^5-5q^4+2q^3-3q^2)\\
A^{(4)}_{q^2+q-1} &= \tfrac{1}{2}(q^4+2q^3+2q^2+q)\\
A^{(4)}_{q^2+q} &= q^6+2q^5+2q^4+q^3+q^2+q+1\\
A^{(4)}_{q^2+q+1} &= \tfrac{1}{2}(2q^8+2q^7+2q^6+q^4-q)\\
A^{(5)}_{q^2+q} &= q^2+q+1\\
A^{(5)}_{q^2+q+1} &= q^5+q^4+q^3\\
A^{(6)}_{q^2+q+1} &= 1
\end{aligned}
$$

In order to prove this theorem, we will compute the Stanley-Reisner resolutions of the matroid M_q and its elongations. We first will find which subsets of $\{1, \cdots, q^2+q+1\}$ are minimal in the different N_i. In particular this will give us which Betti numbers $\beta^{(l)}_{1,j}$ are non-zero (Corollary 22). When this is done, it turns out that for every elongation $M_q^{(l)}$, for $l \geq 1$, the number of unknowns is equal to the number of Herzog-Kühl equations from Formula (1), and that all these equations are independent. For the matroid M_q itself, however, there will be one unknown more than the number of equations. We will then, in Proposition 25, compute one of the missing Betti numbers $\beta^{(0)}_{2,q^2-1}$. After that we will be in a situation where we can find all the Betti numbers with the Herzog-Kühl equations from Formula (1). Thereafter we will compute the generalized weight polynomials $P(Z)$ using Theorem 16. Finally we will find the the higher weight spectra, using Theorem 6 repeatedly.

3.1. **Stanley-Reisner resolutions.** We will use the following result by Hirschfeld [10]

Proposition 19. *In $\mathbb{P}^2_q$ the $\frac{q^6-1}{q-1}$ conics are as follows.*

- *There are q^2+q+1 double lines,*
- *There are $\frac{1}{2}q(q+1)(q^2+q+1)$ pairs of two distinct lines*
- *There are q^5-q^2 irreducible conics*

- *There are $\frac{1}{2}q(q-1)(q^2+q+1)$ conics that just possess a single $\mathbb{F}_q$-rational point each.*

There is a one-to-one correspondence between words of C_q and affine equations for conics, and under this correspondence, the support of a codeword correspond to points of $\mathbb{P}_q^2$ that are not on the conic. Thus, the circuits of M_q correspond to conics with maximal set of points (under inclusion). By Proposition 19, it is thus easy to see that we have two types of circuits, namely the one corresponding to pairs of lines, and the one corresponding to irreducible conics. This shows that

$$\beta^{(0)}_{1,q^2+q+1-(2q+1)} = \frac{1}{2}q(q+1)(q^2+q+1)$$

and

$$\beta^{(0)}_{1,q^2+q+1-(q+1)} = q^5 - q^2,$$

the other $\beta^{(0)}_{1,j}$ being 0. In order to compute the other Betti numbers of M_q, we will need the following lemma:

Lemma 20. *For any $X \subset E = \{1, \cdots, q^2+q+1\}$ the nullity $n(X)$ is equal to the dimension over $\mathbb{F}_q$ of the affine set of polynomial expressions that define conics that pass through all the points of $E \backslash X$.*

Proof. The matroid derived from any generator matrix of C_q, is the dual matroid of M_q. Its rank function r^* therefore satisfies

$$r(X) = |X| + r^*(E\backslash X) - r^*(E)$$

for $X \subset E$, and hence $n(X) = r^*(E) - r^*(E\backslash X)$. The last expression is equal to the dimension of the kernel of the projection map when projecting all the codewords, each of which corresponds to the affine equation of a conic, on to the space $\mathbb{F}_q^{E\backslash X}$ in a natural way. This kernel is precisely the polynomials that define conics passing through the points of $E\backslash X$, or alternatively, the codewords, whose support lie inside X. □

We can therefore find when the Betti numbers of M_q and its elongations are non-zero. This comes as a corollary of the following theorem:

Theorem 21. *We have the following.*

- *The minimal elements of N_1 are the complements of the $\frac{1}{2}q(q+1)(q^2+q+1)$ pairs of distinct lines and of the q^5-q^2 irreducible conics.*
- *The minimal subsets of N_2 are the $q^2(q^2+q+1)$ complements of $q+1$ points on a line and a point outside of the line, and the $\frac{1}{24}(q^2+q+1)q^2(q^2+q)(q-1)^2$ complements of quadrilateral configurations of 4 points such that no 3 points lie on a line.*
- *The minimal elements of N_3 are the q^2+q+1 complements of $q+1$ points on a line, and the $\frac{1}{6}(q^2+q+1)q^2(q^2+q)$ complements of triangle configurations of 3 non-aligned points.*
- *The minimal elements of N_4 are the $\frac{1}{2}(q^2+q+1)(q^2+q)$ complements of pairs of points.*
- *The minimal elements of N_5 are the q^2+q+1 complements of a single point.*
- *The only element of N_6 is E.*

Proof. In the text following Proposition 19, we have already treated the case with determining minimal elements of N_1. The complement of any set of points, such that no conic contains all of them, has nullity 0 and is not considered here.
We will now determine the minimal elements of N_2. A subset of cardinality at least $q+3$ lying on a conic necessarily lies on a pair of lines, and defines these two lines uniquely. Therefore, its complement has nullity 1, and does not need to be considered here. Any subset of cardinality $q+2$ lying on a conic necessarily lies on a pair of distinct lines. If not $q+1$ of the points lie on the same line, then both lines are uniquely defined, and the nullity of the complement is 1 again. If $q+1$ points lie on the same line, then there is an (exactly) 2-dimensional affine family of quadric polynomials which define conics going through these points (a fixed line and a variable line), and the nullity of the complement is 2 by Lemma 20. Obviously, the complement of these configurations are minimal in N_2. Moreover there are exactly $q^2(q^2+q+1)$ such configurations. Consider now $X \subset E$ with $5 \leqslant |X| \leqslant q+1$ that lie on a conic. If the points of X lie on the same line, then $n(E \backslash X) = 3$ and it doesn't have to be considered here. If they lie on a pair of lines (but not a single line), then either $n(E \backslash X) = 1$ if the two lines are uniquely defined, or $n(E \backslash X) = 2$, but $E \backslash X$ is not minimal in N_2 (we could complete X with the remaining points on the line that is uniquely defined). If they lie on an irreducible conic, then $n(E \backslash X) = 1$ since an irreducible conic is uniquely defined by 5 of its points. Consider now $X \subset E$ with $|X| = 4$ and (then) lying on a conic. If 3 of them are aligned, then we can argue in the same way as before for lines and pair of lines (so $E \backslash X$ is not minimal in any N_i). If no 3 of them are aligned, then there is a 2-(and not 3-)dimensional affine family of quadric polynomials defining conics passing through X, and therefore $n(E \backslash X) = 2$. Obviously, these configurations are minimal in N_2, since adding a point reduces the nullity (either being on a unique irreducible conic, or uniquely determined pairs of lines). There are exactly $\frac{1}{24}(q^2+q+1)q^2(q^2+q)(q-1)^2$ such configurations. Finally, since the rank of the code is 6, all subsets of cardinality at most 3 have nullity at least 3, and this completes the analysis of the minimal sets of N_2. .

The other cases are done in a similar way. Let us determine the minimal elements of N_3: The nullity of the complement of any subset of cardinality at least $q+2$ is at most 2, as we have seen. The complement of $q+1$ points on a line, on the other hand, are then minimal in N_3, and there are exactly q^2+q+1 lines in $\mathbb{P}^2_q$. The complements of any subset of cardinality between q and 4 has either nullity different from 3 or are not minimal in N_3. Three non-aligned points give a 3-dimensional affine family of quadric polynomials defining conics passing through X, and the complement of the set of these points are minimal in N_3. There are $\frac{1}{6}(q^2+q+1)q^2(q^2+q)$ such configurations. Finally, the complements of 2 or less points have nullity at least 4 since the rank of the code is 6.
For nullity $4, 5, 6$, then we can see that 3 points or more have complements with nullity at most 3. And i points give a $(6-i)$-dimensional affine family of quadric polynomials defining conics passing through the i points, for $i = 2, 1, 0$, Moreover there are $\frac{1}{2}(q^2+q+1)(q^2+q)$ pairs of points, q^2+q+1 single points and 1 empty set in $\mathbb{P}^2_q$, corresponding to $i = 2, 1, 0$, respectively. These observations settles the cases of finding the minimal elements of N_4, N_5, N_6. □

We recall that the length of the resolution of R_{M_q} is $\dim C_q = 6$, and the lengths of the resolutions of $R_{M_q^{(i)}}$ then are $6-i$, for $i = 1, \cdots, 5$.

Corollary 22. *The only non-zero Betti numbers of $M_q^{(i)}$ for $0 \leqslant i \leqslant 5$ are $\beta_{0,0}^{(i)} = 1$ and*

$$\beta^{(i)}_{1-i,q^2-q}, \beta^{(i)}_{1-i,q^2}, \beta^{(i)}_{2-i,q^2-1}, \beta^{(i)}_{2-i,q^2+q-3}, \beta^{(i)}_{3-i,q^2},$$
$$\beta^{(i)}_{3-i,q^2+q-2}, \beta^{(i)}_{4-i,q^2+q-1}, \beta^{(i)}_{5-i,q^2+q}, \beta^{(i)}_{6-i,q^2+q+1}$$

when these quantities make sense. Moreover, we have

$$\begin{array}{l}
\beta^{(0)}_{1,q^2-q} = \frac{1}{2}q(q+1)(q^2+q+1) \\
\beta^{(0)}_{1,q^2} = q^5 - q^2 \\
\beta^{(1)}_{1,q^2-1} = q^2(q^2+q+1) \\
\beta^{(1)}_{1,q^2+q-3} = \frac{1}{24}(q^2+q+1)q^2(q^2+q)(q-1)^2 \\
\beta^{(2)}_{1,q^2} = q^2+q+1 \\
\beta^{(2)}_{1,q^2+q-2} = \frac{1}{6}(q^2+q+1)q^2(q^2+q) \\
\beta^{(3)}_{1,q^2+q-1} = \frac{1}{2}(q^2+q+1)(q^2+q) \\
\beta^{(4)}_{1,q^2+q} = q^2+q+1 \\
\beta^{(5)}_{1,q^2+q+1} = 1
\end{array}$$

Proof. This is an immediate consequence of Theorems 10, 11 and 21 and Proposition 15. □

As a corollary, we can find the generalized Hamming weights of the Veronese codes, already given in [21]:

Corollary 23. *The generalized Hamming weights of the code C_q are*

$$d_1 = q^2 - q, \quad d_2 = q^2 - 1, \quad d_3 = q^2,$$
$$d_4 = q^2 + q - 1, \quad d_5 = q^2 + q, \quad d_6 = q^2 + q + 1.$$

Proof. This is a direct consequence of Theorem 11. □

After using Corollary 22 we have 7 unknown remaining Betti number in the 6 (Herzog-Kühl) equations described in Formula (1) for the matroid M_q, We have 5 equations for $M_q^{(1)}$, with 5 unknown Betti numbers, and for $2 \leqslant l \leqslant 5$, we have $6-l$ equations for $M_q^{(l)}$ for $5-l$ unknown Betti numbers. We will now find $\beta^{(0)}_{2,q^2-1}$, and thus reduce the number of unknown Betti numbers $\beta^{(0)}_{i,j}$ from 7 to 6. Thereafter, it turns out that all the Herzog-Kühl equation sets from Formula (1) will be independent, and we will find all the remaining unknown $\beta^{(l)}_{i,j}$, for $l = 0, \cdots, 5$.

Proposition 24. *Let $X \subset E$ be a set of $q+1$ points on a line together with a point outside of this line. Then*

$$\beta^{(0)}_{2,E \backslash X} = q.$$

Proof. Write $X = D \cup \{P_0\}$ where D is the line and P_0 the point outside. For ease of notation we denote M_q by M. We consider the restricted matroid $M_{E\backslash X}$ and will compute its Euler characteristic, and conclude by Theorem 10. We will denote, for $0 \leqslant z \leqslant q^2 - 1$,

$$D_z = |\{Y \subset E\backslash X : \ |Y| = z \text{ and } Y \notin \mathcal{I}\}|.$$

For $Z \supset X$ we have that $E\backslash Z \notin \mathcal{I}$ if and only if Z is contained in a conic, and necessarily this conic has to be a pair of lines containing D and P_0. Thus, if $0 \leqslant z < q^2 - q$, then $D_z = 0$. Also, $D_{q-1} = 1$. Now, consider $q^2 - q \leqslant z \leqslant q^2 - 2$. The pair of lines containing X are parametrized by the points of D. And if Z is a subset of such a parametrized conic of cardinality t, then we have $\binom{q-1}{t-(q+2)}$ choices for Z. Thus we find that

$$D_z = (q+1)\binom{q-1}{q^2-1-z}.$$

Using the fact that the alternate sums of binomial coefficients is 0, we get that

$$\chi(M_{E\backslash X}) = \sum_{z=0}^{q^2-1} (-1)^z D_z = (-1)^{q^2} q.$$

□

Corollary 25. *We have*

$$\beta^{(0)}_{2,q^2-1} = q^3(q^2+q+1).$$

Proof. This is a direct consequence of Theorem 21: $\beta^{(0)}_{2,q^2-1}$ is the product of the number $q^2(q^2+q+1)$ of minimal elements of N_2 of degree q^2-1, and the "local" contribution $\beta_{2,E\backslash X} = |\chi(M_{E\backslash X})| = |(-1)^{q^2} q| = q$ which we calculated in Proposition 24. □

Theorem 26. *With the previous notation, the Betti numbers of the matroid M_q and its elongations are*

$$\beta^{(0)}_{1,q^2-q} = \frac{1}{2}(q^4 + 2q^3 + 2q^2 + q),$$
$$\beta^{(0)}_{1,q^2} = q^5 - q^2$$
$$\beta^{(0)}_{2,q^2-1} = q^5 + q^4 + q^3,$$
$$\beta^{(0)}_{2,q^2+q-3} = \frac{1}{24}(q^9 - q^7 - q^6 + q^4)$$
$$\beta^{(0)}_{3,q^2} = q^5 - q^3 - q^2 + 1,$$
$$\beta^{(0)}_{3,q^2+q-2} = \frac{1}{6}(q^9 - q^8 - q^7 + q^6 + 3q^5 + 3q^4)$$
$$\beta^{(0)}_{4,q^2+q-1} = \frac{1}{4}(q^9 - 2q^8 + q^7 + 3q^6 + 2q^5 - q^4 - 4q^3),$$
$$\beta^{(0)}_{5,q^2+q} = \frac{1}{6}(q^9 - 3q^8 + 5q^7 - q^6 - 3q^5 - 2q^4 + 6q^2 - 3q)$$
$$\beta^{(0)}_{6,q^2+q+1} = \frac{1}{24}(q^9 - 4q^8 + 11q^7 - 17q^6 + 12q^5 - 3q^4)$$
$$\beta^{(1)}_{1,q^2-1} = q^4 + q^3 + q^2$$
$$\beta^{(1)}_{1,q^2+q-3} = \frac{1}{24}(q^8 - q^6 - q^5 + q^3)$$
$$\beta^{(1)}_{2,q^2} = q^4 + q^3 - q - 1$$
$$\beta^{(1)}_{2,q^2+q-2} = \frac{1}{6}(q^8 + q^6 + 3q^5 + 4q^4 + 3q^3)$$
$$\beta^{(1)}_{3,q^2+q-1} = \frac{1}{4}(q^8 + 3q^6 + 3q^5 - 3q^3 - 4q^2),$$
$$\beta^{(1)}_{4,q^2+q} = \frac{1}{6}(q^8 + 5q^6 - q^5 - 6q^4 - 5q^3 + 6q)$$
$$\beta^{(1)}_{5,q^2+q+1} = \frac{1}{24}(q^8 + 7q^6 - 9q^5 - 8q^4 + 9q^3)$$
$$\beta^{(2)}_{1,q^2} = q^2 + q + 1$$
$$\beta^{(2)}_{1,q^2+q-2} = \frac{1}{6}(q^6 + 2q^5 + 2q^4 + q^3)$$
$$\beta^{(2)}_{2,q^2+q-1} = \frac{1}{2}(q^6 + 2q^5 + 2q^4 + q^3)$$
$$\beta^{(2)}_{3,q^2+q} = \frac{1}{2}(q^6 + 2q^5 + 2q^4 - q^3 - 2q^2 - 2q)$$
$$\beta^{(2)}_{4,q^2+q+1} = \frac{1}{6}(q^6 + 2q^5 + 2q^4 - 5q^3)$$
$$\beta^{(3)}_{1,q^2+q-1} = \frac{1}{2}(q^4 + 2q^3 + 2q^2 + q)$$
$$\beta^{(3)}_{2,q^2+q} = q^4 + 2q^3 + q^2 - 1$$
$$\beta^{(3)}_{3,q^2+q+1} = \frac{1}{2}(q^4 + 2q^3 - q)$$
$$\beta^{(4)}_{1,q^2+q} = q^2 + q + 1$$
$$\beta^{(4)}_{2,q^2+q+1} = q^2 + q$$
$$\beta^{(5)}_{1,q^2+q+1} = 1$$

Proof. This follows immediately from Corollary 22, Proposition 24 and Theorem 8, after using the computer program Mathematica to solve the Herzog-Kühl equations (1) from Theorem 8 for the Betti numbers appearing in each of the the $\mathbb{N}$-graded resolutions of the Stanley-Reisner rings of the matroids $M_q^{(l)}$, for $l = 0, 1, \cdots, 5$. (After usage of Corollary 22 which assigns integer values to a sufficient set of Betti numbers, the coefficient matrices of the Herzog-Kühl equations for each of the matroids in question, in terms of those Betti numbers that are still unknown, are now of Vandermonde type). □

Remark 27. It is also possible to find all these Betti numbers without using the Herzog-Kühl equations: First Proposition 15 gives, for each l and i in question, that a subset Y of E is minimal among those sets that have nullity i for the matroid $M_q^{(l)}$ if and only if Y is minimal among those sets that have nullity $i + l$ for the matroid $M_q^{(l)}$. Furthermore one can find the local contributions $\beta_{i,Y}^{(l)}$, for each Y minimal among those sets that have nullity i for the matroid $M_q^{(l)}$, by performing arguments and calculations analogous to those in the proof of Proposition 24. The result, $\beta_{i,j}^{(l)}$, is then computed as the product of the number (given in Theorem 21) of subsets Y of E that have cardinality j and are minimal in N_{i+l}, and the common number $\beta_{i,Y}^{(l)}$ for all these sets Y. We have done this for all the Betti numbers given in Theorem 26, but see no reason to present the calculations here, since usage of a computer program like Mathematica gives the solution for the $\beta_{i,j}^{(l)}$ directly. If, on the other hand, for some reason, one would be interested in knowing the values of the"local" contributions $\beta_{i,Y}^{(l)}$, one can just divide the values of the $\beta_{i,j}^{(l)}$ appearing in Theorem 26 by the corresponding numbers appearing in Theorem 21.

3.2. **Higher weight polynomials and weight spectra.**

Theorem 28. *Let $q \geqslant 4$ be a prime power. Then the Veronese code C_q has 9 non-zero generalized weight polynomials, namely*

$$
\begin{array}{lcl}
P_0(Z) & = & 1 \\
P_{q^2-q}(Z) & = & \binom{q^2+q+1}{2}(Z-1) \\
P_{q^2-1}(Z) & = & (q^2+q+1)q^2(Z-q)(Z-1) \\
P_{q^2}(Z) & = & (q^2+q+1)(Z-1) \\
 & & (Z^2-(q^2-1)Z+2q^3-2q^2-q+1) \\
P_{q^2+q-3}(Z) & = & \frac{1}{24}(q^2+q+1)(q+1)q^3 \\
 & & (q-1)^2(Z-q)(Z-1) \\
P_{q^2+q-2}(Z) & = & \frac{1}{6}(q^2+q+1)(q+1)q^3(Z-1) \\
 & & (Z-q)(Z-(q^2-3q+3)) \\
P_{q^2+q-1}(Z) & = & \frac{1}{4}(q^2+q+1)(q+1)q(Z-1)(Z-q) \\
 & & [2Z^2-2(q^2-q)Z \\
 & & +(q^4-4q^3+7q^2-4q)] \\
\frac{6P_{q^2+q}(Z)}{(q^2+q+1)(Z-1)} & = & 6Z^4-(6q^2+6q-6)Z^3 \\
 & & +(3q^4+3q^3-6q)Z^2 \\
 & & -(q^6-q^5+5q^4-5q^3-6q^2+6q)Z \\
 & & +q^7-4q^6+8q^5-5q^4 \\
 & & -6q^3+9q^2-3q \\
\frac{24P_{q^2+q+1}}{(Z-1)(Z-q)} & = & 24Z^4-24q^2Z^3+(12q^4-12q)Z^2 \\
 & & -(4q^6-4q^5+8q^4-20q^3+12q^2)Z \\
 & & +q^8-4q^7+11q^6 \\
 & & -17q^5+12q^4-3q^3
\end{array}
$$

Proof. This is a direct consequence of Theorems 16 and 26. □

Proof of Theorem 18. This is a direct consequence of Theorem 28 and repeated usage of Theorem 6. □

4. The cases $q = 2$ and $q = 3$

The cases $q = 2$ and $q = 3$ are very similar to the "general" case $q \geq 4$, except that some degeneracies appear. It can be shown that in the case $q = 2$, where $q^2 - 1 = q^2 + q - 3$ and $q^2 = q^2 + q - 2$, we have $\beta^{(0)}_{1,4} = 0$, and all the resolutions in question are linear, and easy to cope with (The code is MDS for $q = 2$, and then both M and all its elongation matroids are uniform, and their associated Betti numbers then follow directly from the Herzog-Kühl equations). In general, the higher weights of MDS codes are known, and only depend on the parameters of the code (see [14, Theorem 5.8]). Our method confirms their result.

In the case $q = 3$, we have $\beta^{(0)}_{1,9} = 0$. This constitutes a difference with the cases $q \geq 4$, where the coefficient $\beta^{(0)}_{1,q^2}$ is non-zero. The non-zero value is due to the complement X of the irreducible conic (with $q + 1$ points). For $q \geqslant 4$, these complements are minimal sets in N_1. But for $q = 3$ an irreducible conic has 4 points, and is always included in a pair of distinct lines, and therefore would not lead to a minimal element in N_1. Apart from this difference from the cases $q \geq 4$ the arguments for establishing the Betti numbers, generalized weight polynomials, and higher weight spectra are almost identical for $q = 3$ to those in the cases $q \geq 4$.

We now give just the main result about these 2 cases, without going more into the details concerning the computation of the Betti numbers and the general weight polynomials:

Theorem 29. *The higher weight spectra of the Veronese code C_3 is*

$$\begin{array}{lll} A_6^{(1)} = 78, & A_9^{(1)} = 247, & A_{12}^{(1)} = 39, \\ A_8^{(2)} = 117 & A_9^{(2)} = 286, & A_{10}^{(2)} = 1404, \\ A_{11}^{(2)} = 3042, & A_{12}^{(2)} = 3705, & A_{13}^{(2)} = 2457, \\ A_9^{(3)} = 13, & A_{10}^{(3)} = 234, & A_{11}^{(3)} = 2340, \\ A_{12}^{(3)} = 10296, & A_{13}^{(3)} = 20997, & A_{11}^{(4)} = 78, \\ A_{12}^{(4)} = 1417, & A_{13}^{(4)} = 9516, & A_{12}^{(5)} = 13, \\ A_{13}^{(5)} = 351, & A_{13}^{(6)} = 1, & \end{array}$$

all the other being 0*.*

Theorem 30. *The higher weight spectra of the Veronese code C_2 is*

$$\begin{array}{llll} A_2^{(1)} = 21, & A_4^{(1)} = 35, & A_6^{(1)} = 7, & A_3^{(2)} = 35, \\ A_4^{(2)} = 105, & A_5^{(2)} = 210, & A_6^{(2)} = 210, & A_7^{(2)} = 91, \\ A_4^{(3)} = 35, & A_5^{(3)} = 210, & A_6^{(3)} = 560, & A_7^{(3)} = 590, \\ A_5^{(4)} = 21, & A_6^{(4)} = 175, & A_7^{(4)} = 455, & A_6^{(5)} = 7, \\ & A_7^{(5)} = 56, & A_7^{(6)} = 1, & \end{array}$$

all the other being 0*.*

5. An alternative method

During the reviewing process of this paper, one of the anonymous referees suggested an alternative way of computing the higher weight spectra of the Veronese codes. We thank him/her for this nice method, which we will briefly present here, and we will discuss the differences, advantages and drawbacks of the two methods. As mentioned in [13] and earlier in this paper in Theorems 5 and 6, the higher weight spectra are equivalent to the generalized weight polynomials. We can compute them directly, if we can compute the number of codewords in $C^{(i)} = C \otimes_{\mathbb{F}_q} \mathbb{F}_{q^i}$ of a given support. For the rest of this section, we write $Q = q^i$.

A result somewhat similar to that of Lemma 20 is the following:

Lemma 31. *For any $0 \leqslant w \leqslant n$, the number of codewords of $C^{(i)}$ of weight $n - w$ is equal to the number of quadratic equations in* 3 *variables over $\mathsf{F}Q$, with exactly w rational points over $\mathbb{F}_q$.*

We assume that $q \geqslant 4$. From [10], we know how the decomposition of the set of conics defined over $\mathsf{F}Q$ into different types looks like (double lines, pairs of lines, conics with just 1 rational point, irreducible conics). It is rather easy to find out how many different $\mathbb{F}_q$-rational points the 3 first kinds of conics have, but the latter kind (irreducible conics) requires more work. One remarks that if a conic has 5 or more $\mathbb{F}_q$-rational points, then the conic is defined over $\mathbb{F}_q$. So one has to focus on conics with 4 or less $\mathbb{F}_q$-rational points. Moreover, using MacWilliams identities ([14]) that relate the higher weight polynomials of the code to those of its dual, and knowing that there are no codewords of weight 1,2 and 3 in the dual, it is just necessary to compute the number of conics with exactly 4 rational points over $\mathbb{F}_q$.

Let $\mathfrak{C}$ be the set of irreducible conics over $\mathsf{F}Q$. The group $PGL_3(\mathsf{F}Q)$ acts transitively on $\mathfrak{C}$ in the obvious way. The conic $\mathcal{C}_0$ with equation $Y^2 - XZ = 0$ is parametrized by

$$\begin{array}{cccc} \gamma: & \mathbb{P}^1(\mathsf{F}Q) & \longrightarrow & \mathcal{C}(\mathsf{F}Q) \\ & (t:1) & \longmapsto & (t^2:t:1) \\ & \infty=(1:0) & \longmapsto & (1:0:0) \end{array}$$

From [10, Corollary 7.14], it is known that the stabiliser of $\mathcal{C}_0$ under the group action is the image H of the group monomorphism

$$\begin{array}{cccc} \theta: & PGL_2(\mathsf{F}Q) & \longrightarrow & PGL_3(\mathsf{F}Q) \\ & \begin{bmatrix} a & b \\ c & d \end{bmatrix} & \longmapsto & \begin{bmatrix} a^2 & 2ab & b^2 \\ ac & ad+bc & bd \\ c^2 & 2cd & d^2 \end{bmatrix}. \end{array}$$

Thus, $\mathfrak{C} \approx PGL_3(\mathsf{F}Q)/H$, and with this bijection, the set of points of $G\mathcal{C}_0$ for $G \in PGL_3(\mathsf{F}Q)$ is $\{G\gamma(t) : t \in \mathbb{P}^1(\mathsf{F}Q)\}$.

So let $\mathcal{C} \in \mathfrak{C}$ be a curve with exactly 4 rational points over $\mathbb{F}_q$. Choose 3 of them, say P_1, P_2 and P_3. If we write $P_j = (x_j : y_j : z_j)$, we may assume that the first non-zero coordinate of each of the P_j's is 1, and consequently, all the other coordinates are in $\mathbb{F}_q$. From the parametrization, there exists $G \in PGL_3(\mathsf{F}Q)$ such that $G\gamma(t_j) = P_j$ for some $t_j \in \mathsf{F}Q$. Since $PGL_2(\mathsf{F}Q)$ acts triply transitively on $\mathbb{P}^1(\mathsf{F}Q)$ ([10, Corollary 7.15]), there exists a unique $G' \in H$ that sends the triple $(\gamma(t_1), \gamma(t_2), \gamma(t_3))$ to $(\gamma(\infty), \gamma(1), \gamma(0))$. Replacing G by GG'^{-1}, we have thus that

$$G\gamma(\infty) = P_1,\ G\gamma(1) = P_2,\ G\gamma(0) = P_3.$$

This means that

$$G \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} = AD$$

with

$$A = \begin{bmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \\ z_1 & z_2 & z_3 \end{bmatrix} \in GL_3(\mathbb{F}_q)$$

and $D = diag(1, \alpha, \beta) \in GL_3(\mathsf{F}Q)$. This decomposition is unique as soon as we demand that the matrix $A \in GL_3(\mathbb{F}_q)$ is such that the first non-zero entry in each column is 1, and D is a diagonal matrix with top left corner equal to 1 in $GL_3(\mathsf{F}Q)$. The conditions on $\alpha, \beta \in \mathsf{F}Q^*$ is that the curve should have exactly a fourth $\mathbb{F}_q$-rational point, that is, that there exists exactly one $s \in \mathsf{F}Q \backslash \{0, 1\}$ such that $G\gamma((s:1))$ is $\mathbb{F}_q$-rational. But

$$G \begin{bmatrix} s^2 \\ s \\ 1 \end{bmatrix} = AD \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}^{-1} \begin{bmatrix} s^2 \\ s \\ 1 \end{bmatrix} = A \begin{bmatrix} 1-s \\ \alpha s \\ \beta(s^2-s) \end{bmatrix}$$

is $\mathbb{F}_q$-rational if and only if $(1-s : \alpha s : \beta(s^2-s))$ is defined over $\mathbb{F}_q$, that is $\frac{\alpha s}{1-s} \in \mathbb{F}_q^*$ and $-\beta s \in \mathbb{F}_q^*$. Thus, saying that the curve has exactly one extra $\mathbb{F}_q$ rational point is equivalent to say that the equation

$$\beta x + \alpha y + xy = 0$$

has a unique solution $(x, y) \in (\mathbb{F}_q^*)^2$. This is true if and only if $\alpha \in \mathsf{F}Q - \mathbb{F}_q$ and $\beta = \beta_0 + \beta_1 \alpha$ for $\beta_0, \beta_1 \in \mathbb{F}_q^*$. We have thus showed that, with these conditions on α

and β, there is a bijection between 4-tuples $(\mathcal{C}, P_1, P_2, P_3)$, where $\mathcal{C}$ is an irreducible conic with exactly 4 rational points over $\mathbb{F}_q$, and the P_j's are 3 distinct F_q-rational points, and the set of pairs (A, D) with the restrictions above. This gives that the number of irreducible conics with exactly $\mathbb{F}_q$ rational points over $\mathbb{F}_q$ is

$$\frac{1}{4 \cdot 3 \cdot 2} \frac{\#GL_3(\mathbb{F}_q)}{(q-1)^3}(Q-q)(q-1)^2.$$

This gives the fifth polynomial of Theorem 28 (up to a factor $(Q-1)$ since in the theorem we compute the number of equations, while we compute the number of conics in this section).

If one compares the two approaches, there are obvious advantages (and corresponding disadvantages) with both of them. Basically, our method consists of computing the number of different conics passing through some configurations of points, while the second method consists of finding the number of $\mathbb{F}_q$-rational points on conics defined over an extension. An advantage of the second method is its directness, and it does not require any homological/topological algebra. The advantage of our method is that we just need to understand the geometry of conics defined over a single field. This pre-assumes of course that one already possesses the techniques and results described in [11] and [12], which restricts dramatically the number of point configurations to look at.

It is not obvious to us which of the approaches that would be best fit for generalizations. A natural example is to find the analogue of Theorem 28 for, say, the code obtained from mapping $\mathbb{P}^3$ into $\mathbb{P}^9$ by the quadratic Veronese embedding, and taking coordinate representatives of the q^3+q^2+q+1 embedded points as columns of a $10 \times (q^3+q^2+q+1)$ generator matrix of a code over F_q, then one has [10, Section 15.3] at hand. There, one finds a higher dimensional analogue of Proposition 19, and one classifies the quadrics in $\mathbb{P}^3$ over a finite field (six different types: double planes, plane pairs, hyperbolic quadrics, elliptic quadrics, cones, lines).

Should one view this result over $\mathbb{F}_Q$, and do like the referee suggests, and find some way to count the $\mathbb{F}_q$-rational points of the quadrics? Or should one view everything over a single F_q and use the analogues of Theorem 21, Lemma 20, Theorem 10, and the Herzog-Kühl equations? This is not clear to us, and we think it is good to have several methods available for future use concerning this or related problems.

References

[1] Auslander, M., Buchsbaum, D. A., *Homological dimension in local rings*, Trans. Amer. Math. Soc., 85, p. 390–405, 1957.

[2] Beelen, Peter; Datta, Mrinmoy; Ghorpade, Sudhir R. *Maximum number of common zeros of homogeneous polynomials over finite fields.* Proc. Amer. Math. Soc. 146, no. 4, p. 1451-1468, 2018.

[3] Boij, M., Søderberg, J. *Graded Betti numbers of Cohen-Macaulay modules and the multiplicity conjectures*, J. Lond. Math. Soc. (2), 78,no. 1, p. 85–106, 2008.

[4] Datta, M., Ghorpade, S.R., *Remarks on Tsfasman-Boguslavsky conjecture and higher weights of projective Reed-Müller codes.* In: Arithmetic, Geometry, Cryptography and Coding Theor. Contemp. Math. 686, p. 157–169, 2017.

[5] Datta, M.; Ghorpade, S. R. *Number of solutions of systems of homogeneous polynomial equations over finite fields.* Proc. Amer. Math. Soc., 145, no. 2, p. 525-541, 2017

[6] Datta, M.; Ghorpade, S. R. *On a conjecture of Tsfasman and an inequality of Serre for the number of points of hypersurfaces over finite fields.* Mosc. Math. J., 15, no. 4, p. 715-725, 2015

[7] Herzog, J., Hibi, T., *Monomial Ideals*, Graduate Texts in Mathematics, 260, Springer-Verlag, 2011.

[8] Herzog, J., Kühl, M., *On the Betti numbers of finite pure and linear resolutions.* Comm. Algebra, 12, no. 13-14, p.1627–1646, 1984.

[9] Hirschfeld, J., *Finite projective spaces of three dimensions*, Oxford University Press, 1985.

[10] Hirschfeld, J., *Projective geometries over finite fields*, Second edition, Oxford University Press, 1998.

[11] Johnsen, T., Verdure, H. *Hamming weights and Betti numbers of Stanley-Reisner rings associated to matroids*, Appl. Algebra Engrg. Comm. Comput., 201, p. 73–93, 2013.

[12] Johnsen, T., Roksvold, J.N., Verdure, H. *A generalization of weight polynomials to matroids*, Discrete Math., 339, p. 632–45, 2013.

[13] Jurrius, R. *Weight enumeration of codes from finite spaces*, Des. Codes Cryptogr., 63, p. 321–330, 2012.

[14] Jurrius, R., Pellikaan, G. R. *Codes, arrangements and matroids.* In: Algebraic geometric modeling in information theory. Ser. Coding Theory Cryptol., 8, p. 219–325, 2013.

[15] Lachaud G. R., *The parameters of projective Reed-Müller codes*, Discrete Math., 81, no. 2, p. 217–221, 1990

[16] J.G. Oxley, *Matroid theory*, Oxford University Press, 1992.

[17] Peskine, C., Szpiro, L., *Syzygies et multiplicités*, C. R. Acad. Sci. Paris Sr. A, 278, p. 1421–1424, 1974.

[18] Serre, J.-P. *Lettre a M. Tsfasman.* Astérisque, 11, p. 351–353, 1992.

[19] Sørensen, A.B., *Projective Reed-Muller codes*, IEEE Trans. Inform. Theory, 37, no. 6, p. 1567–1576, 1991.

[20] V.K. Wei, *Generalized Hamming weights for linear codes*, IEEE Trans. Inform. Theory, 37, no. 5, p. 1412–1418, 1991.

[21] Zanella, C. *Linear Sections of the finite Veronese Varieties and Authentication Systems Defined Using Geometry*, Des. Codes Cryptogr., 13, p. 199–212, 1998.

Department of Mathematics and Statistics, UiT-The Arctic University of Norway N-9037 Tromsø, Norway

E-mail address: trygve.johnsen@uit.no

Department of Mathematics and Statistics, UiT-The Arctic University of Norway N-9037 Tromsø, Norway

E-mail address: hugues.verdure@uit.no