A generalization of weight polynomials to matroids*

Trygve Johnsen, Jan Roksvold[†], Hugues Verdure

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

November 13, 2015

Abstract

Generalizing polynomials previously studied in the context of linear codes, we define weight polynomials and an enumerator for a matroid M. Our main result is that these polynomials are determined by Betti numbers associated with $\mathbb{N}_0$-graded minimal free resolutions of the Stanley-Reisner ideals of M and so-called elongations of M. Generalizing Greene's theorem from coding theory, we show that the enumerator of a matroid is equivalent to its Tutte polynomial.

1 Introduction

For a linear $[n,k]$-code C over $\mathbb{F}_q$, let $A_{C,j}$ denote the number of words of weight j in C. The Hamming weight enumerator

$$W_C(X,Y) = \sum_{j=0}^{n} A_{C,j} X^{n-j} Y^j$$

has important applications in the theory of error-correcting codes, where it amongst other things determines the probability of having an undetected error (see [12, Proposition 1.12]).

Let $M(H)$ denote the vector matroid associated to a parity-check matrix H of C. The connection

$$W_C(X,Y) = (X-Y)^{n-k} Y^k t_{M(H)} \left(\frac{X}{Y}, \frac{X+(q-1)Y}{X-Y} \right) \qquad (1)$$

---

between the Hamming weight enumerator of an $\mathbb{F}_q$-code and the specialization of its associated Tutte polynomial on the hyperbola $(x-1)(y-1) = q$ was first established in Greene's paper [7], and we shall therefore refer to equation (1) as *Greene's theorem*.

For Q a power of q, the set of all $\mathbb{F}_Q$-linear combinations of words of C is itself a linear code. This code is commonly referred to as the extension of C to $\mathbb{F}_Q$, and is denoted by $C \otimes_{\mathbb{F}_q} \mathbb{F}_Q$. In [12], it is found that the number $A_{C,j}(Q)$ of words of weight j in $C \otimes_{\mathbb{F}_q} \mathbb{F}_Q$ can be expressed in terms of the initial code C, as a polynomial in Q. This leads the authors to the definition of an *extended* weight enumerator $W_C(X, Y, Q)$ for C, with the desired property that

$$W_C(X, Y, Q) = W_{C \otimes_{\mathbb{F}_q} \mathbb{F}_Q}(X, Y).$$

The polynomial $W_C(X, Y, Q)$ is then, in turn, shown to be equivalent to the Tutte polynomial of $M(H)$ – thereby extending Greene's theorem.

Our primary objective in this article is to demonstrate that the polynomial $A_{C,j}(Q)$ is determined by the Betti numbers associated to $\mathbb{N}_0$-graded minimal free resolutions of the Stanley-Reisner ideals of $M(H)$ and its so-called *elongations*. This is intended to serve as one brick in the bridge being built between commutative combinatorial algebra and the theory of linear codes. The result can also be seen as a continuation of the work done in [9], where it is demonstrated that the Betti numbers associated to an $\mathbb{N}_0$-graded minimal free resolution of the Stanley-Reisner ideal of $M(H)$ determine the higher Hamming weight hierarchy of C.

It seemed natural to begin the pursuit of the above-stated objective by generalizing the polynomial $A_{C,j}(Q)$ to a polynomial $P_{M,j}(Z)$ defined for all matroids, not only those stemming from a linear code, but of course with the property that $A_{C,j}(Q) = P_{M(H),j}(Q)$. Having defined such a polynomial $P_{M,j}(Z)$, it is equally natural to define and investigate a more general *matroidal* enumerator

$$W_M(X, Y, Z) = \sum_{j=0}^{n} P_{M,j}(Z) X^{n-j} Y^j.$$

Our second objective is to extend Greene's theorem from codes to matroids by way of this matroidal weight enumerator. Since its discovery, Greene's theorem has been generalized, specialized, and extended in several ways. For example, in addition to the already mentioned equivalence between the Tutte polynomial and the extended weight enumerator of a linear code, it was demonstrated in [3, Theorems 4 and 5] and (independently) in [11, Theorem 3.3.5] that the Tutte polynomial and the set of so-called higher weight enumerators of a linear code determine each other as well. Related results and methods can also be found in [2], where the connection between the weight enumerator and the Tutte polynomial is used to establish bounds on all-terminal reliability of vectorial matroids. In addition, [2] provides new proofs of Greene's theorem itself, and shows how the weight polynomial and the partition polynomial of the Potts model are related. The connection between the weight enumerator and

the Tutte polynomial is also used in [16, Corollaries 10, 11 and 12] when looking at two-variable coloring formulas for graphs. A generalization of Greene's theorem is given in [17, Theorem 9.4] to latroids, which are useful for studying codes over rings.

As can be seen in [6, p. 131], the Tutte polynomial of a matroid determines its higher weights. Thus we already know that the polynomials $P_{M,j}$, being equivalent to the Tutte polynomial, must determine the higher weights of M as well – at least indirectly. We shall see that they do so in a very simple and accessible way.

1.1 Structure of this paper

- Section 2 contains definitions and results used later on.

- In Section 3 we look at the number of codewords in the extension of a linear code C over $\mathbb{F}_q$ – as a polynomial in q^r.

- In Section 4, we generalize the polynomial from Section 3 to matroids, and use these generalized weight polynomials to define a matroidal enumerator. We proceed to demonstrate that this enumerator is *equivalent* to the Tutte polynomial of M.

- In Section 5 we prove our main result: The generalized weight polynomials are determined by the Betti numbers associated to $\mathbb{N}_0$-graded minimal free resolutions of the Stanley-Reisner ideal of M and the elongations of M.

- In Section 6 we shall see a counterexample showing that the converse of our main result is not true; the generalized weight enumerators do not determine the $\mathbb{N}_0$-graded Betti numbers of the Stanley-Reisner ideal of M.

2 Preliminaries

2.1 Linear codes and weight enumerators

A linear $[n, k]$-code C over $\mathbb{F}_q$ is, by definition, a k-dimensional subspace of $\mathbb{F}_q^n$. The elements of this subspace are commonly referred to as *words*, and any $k \times n$ matrix whose rows form a basis for C is referred to as a *generator matrix*. Thus a linear code typically has several generator matrices.

The *dual code* is the orthogonal complement of C, and is denoted by $C^\perp$. A *parity-check matrix* of C is a $(n - k) \times n$-matrix with the property that

$$Hx^T = 0 \Leftrightarrow x \in C.$$

It is easy to see that H is a parity check matrix for C if and only if H is a generator matrix for $C^\perp$.

2.2 Puncturing and shortening a linear code

Let C be a linear code of length n, and let $J \subseteq \{1 \ldots n\}$.

Definition 2.1. The *puncturing of C in J* is the linear code obtained by eliminating the coordinates indexed by J from the words of C.

Definition 2.2.

$$C(J) = \{w \in C : w_j = 0 \text{ for all } j \in J\}.$$

Clearly, $C(J)$ is itself a linear code.

Definition 2.3. The *shortening of C in J* is the puncturing of $C(J)$ in J.

2.3 Matroids

There are numerous equivalent ways of defining a matroid. We choose to give here the definition in terms of independent sets. For an introduction to matroid theory in general, we recommend e.g. [15].

Definition 2.4. A *matroid M* consists of a finite set E and a set $I(M)$ of subsets of E such that:

- $\emptyset \in I(M)$.

- If $I_1 \in I(M)$ and $I_2 \subseteq I_1$, then $I_2 \in I(M)$.

- If $I_1, I_2 \in I(M)$ and $|I_1| > |I_2|$, then there is a $x \in I_1 \smallsetminus I_2$ such that $I_2 \cup x \in I(M)$.

The elements of $I(M)$ are referred to as the *independent sets* (of M). The *bases* of M are the independent sets that are not contained in any other independent set. In other words, the *maximal independent sets*. Conversely, given the bases of a matroid, we find the independent sets to be those sets that are contained in a basis. We denote the bases of M by $B(M)$. It is a fundamental result that all bases of a matroid have the same cardinality.

The dual matroid $\overline{M}$ is the matroid on E whose bases are the complements of the bases of M. Thus

$$B(\overline{M}) = \{E \smallsetminus B : B \in B(M)\}.$$

Definition 2.5. For $\sigma \subseteq E$, the rank function r_M and nullity function n_M are defined by

$$r_M(\sigma) = \max\{|I| : I \in I(M), I \subseteq \sigma\},$$

and

$$n_M(\sigma) = |\sigma| - r_M(\sigma).$$

Whenever the matroid M is clear from the context, we omit the subscript and write simply r and n. Note that a subset σ of E is independent if and only if $n(\sigma) = 0$. The rank $r(M)$ of M itself is defined as $r(M) = r_M(E)$.

We let $\overline{r}$ and $\overline{n}$, respectively, denote the rank- and nullity function of $\overline{M}$, and point out that

$$\overline{r}(\sigma) = |\sigma| + r(E \smallsetminus \sigma) - r(E). \tag{2}$$

Definition 2.6. If $\sigma \subseteq E$, then $\{I \subseteq \sigma : I \in I(M)\}$ form the set of independent sets of a matroid $M_{|\sigma}$ on σ. We refer to $M_{|\sigma}$ as the *restriction of M to σ*.

Definition 2.7. The *higher weights* $\{d_i\}$ of M are defined by

$$d_i = \min\{|\sigma| : \sigma \subseteq E(M) \text{ and } n(\sigma) = i\}.$$

Definition 2.8. The *Tutte polynomial* of M is defined by

$$t_M(X, Y) = \sum_{\sigma \subseteq E} (X - 1)^{r(E) - r(\sigma)} (Y - 1)^{|\sigma| - r(\sigma)}.$$

It carries information on several invariants of M. For example $t_M(1, 1)$ counts the number of bases of M, while $t_M(2, 1)$ is the number of independent sets.

Definition 2.9. Let f_i denote the number of independent sets of cardinality i. The *reduced Euler characteristic* $\chi(M)$ of M is defined by

$$\chi(M) = -1 + f_1 - f_2 + \cdots + (-1)^{r(M)-1} f_{r(M)}.$$

It is straightforward to verify that $\chi(M) = (-1)^{r(M)-1} t_M(0, 1)$.

Without any loss of generality we shall throughout this article assume that

$$E = \{1, \ldots, n\}.$$

Furthermore, we shall frequently identify $\sigma \subseteq E$ with its indicator vector in $\{0, 1\}^n$ whose i^{th} coordinate is 1 if and only if $i \in \sigma$. The expression $|\sigma|$ should, however, always be interpreted as the number of elements in σ, or, equivalently, as the number of elements in the support of the corresponding indicator vector.

Example 2.1 $(U(r, n))$**.** The set of all cardinality-r subsets of E form the set of bases for a matroid $U(r, n)$ on E. We refer to $U(r, n)$ as the *uniform matroid of rank r on an n-element set*. Observe that $I \subseteq E$ is independent in $U(r, n)$ if and only if $|I| \leq r$.

Clearly, we have $d_i(U(r, n)) = r + i$, for $1 \leq i \leq n - r$. And it is equally clear that

$$\chi(U(r, n)) = \sum_{i=0}^{r} (-1)^{i+1} \binom{n}{i}.$$

As for the Tutte polynomial, note that for $\sigma \subseteq E$ with $|\sigma| < r$ we have $|\sigma| - r(\sigma) = 0$. While for those σ with $|\sigma| > r$ we have $r(E) - r(\sigma) = 0$. For the $\binom{n}{r}$ subsets σ with $|\sigma| = r$, both $|\sigma| - r(\sigma)$ and $r(E) - r(\sigma)$ are equal to 0. Thus

$$t_{U(r,n)}(X, Y) = \sum_{i=0}^{r-1} \binom{n}{i} (X - 1)^{r-i} + \binom{n}{r} + \sum_{i=r+1}^{n} \binom{n}{i} (Y - 1)^{i-r}.$$

2.4 From linear code to matroid

Let A be an $m \times n$ matrix over some field $\Bbbk$. Let E be the set of column labels of A. It is easy to verify that if we take as independent sets those subsets of E that correspond to a set of $\Bbbk$-linearly independent columns, this constitutes a matroid on E. We refer to this as the *vector matroid* of A and denote it $M(A)$.

Note that if G and G' are two generator matrices for the linear code C, then $M(G) = M(G')$. The same goes for parity-check matrices, of course. It therefore makes sense to speak of *the* matroid corresponding to a generator (or parity-check) matrix of C, and to write $M(G)$ and $M(H)$ without specifying G or H. Thus to a linear code C, with generator matrix G and parity-check matrix H, there naturally correspond two matroids: $M(G)$ and $M(H)$. We shall mostly consider $\underline{M(H)}$, but this is not very crucial since duality results abound and $M(H) = \overline{M(G)}$.

Note that $r(M(G)) = \dim(C)$, while $r(M(H)) = \dim(C^\perp)$, and that $d_1(M(H))$ is equal to the minimum distance of C.

Example 2.2. Let C be the $[7, 4]$-code over $\mathbb{F}_5$ with parity-check matrix

$$H = \begin{pmatrix} 1 & 0 & 0 & 3 & 3 & 3 & 4 \\ 0 & 1 & 0 & 0 & 2 & 2 & 0 \\ 0 & 0 & 1 & 4 & 4 & 4 & 4 \end{pmatrix}.$$

Then $M(H)$ will be a matroid on $E = \{1, \ldots, 7\}$. The columns $\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$

and $\begin{bmatrix} 3 \\ 2 \\ 4 \end{bmatrix}$ form a *maximal* linearly independent set of columns, so $\{1, 3, 6\}$ is

a basis for $M(H)$, and $r(M(H)) = 3$. The full set of bases is

$$B(M(H)) = \{\{1, 3, 6\}, \{1, 3, 5\}, \{1, 2, 6\}, \{2, 3, 6\}, \{1, 2, 5\}, \{1, 5, 7\}, \{3, 6, 7\}, \{2, 4, 7\},$$
$$\{1, 4, 6\}, \{2, 3, 4\}, \{4, 6, 7\}, \{1, 2, 3\}, \{1, 2, 7\}, \{3, 4, 5\}, \{1, 6, 7\}, \{1, 4, 5\},$$
$$\{1, 2, 4\}, \{2, 3, 7\}, \{4, 5, 7\}, \{3, 5, 7\}, \{2, 6, 7\}, \{2, 5, 7\}, \{2, 3, 5\}, \{3, 4, 6\}\}.$$

2.5 The elongation of M to rank $r(M) + i$

Let M be a matroid on $E = \{1, \ldots, n\}$.

Definition 2.10. For $0 \leq i \leq n - r(M)$, let $M_{(i)}$ be the matroid whose independent sets are given by $I(M_{(i)}) = \{\sigma \in E : n(\sigma) \leq i\}$.

It is not difficult to verify that $M_{(i)}$ is indeed a matroid [15, Section 1.3, ex.6]. Note that $M_{(0)} = M$, and that $B(M_{(n-r(M))}) = \{E\}$.

The following is straightforward:

Proposition 2.1. *For $\sigma \subseteq E$, we have*

$$r_{M_{(i)}}(\sigma) = \begin{cases} r(\sigma) + i, & n(\sigma) > i. \\ |\sigma|, & n(\sigma) \leq i. \end{cases} \tag{3}$$

And

$$n_{M_{(i)}}(\sigma) = \begin{cases} n(\sigma) - i, & n(\sigma) > i. \\ 0, & n(\sigma) \leq i. \end{cases} \tag{4}$$

By definition we have $r_i(M_{(i)}) = r_i(E)$. It thus follows from Proposition 2.1 that

$$r_i(M_{(i)}) = r(M) + i. \tag{5}$$

The matroid $M_{(i)}$ is commonly referred to as the *elongation* of M to rank $r(M) + i$.

If $\sigma \subseteq E$ then the rank function of $M_{|\sigma}$ is the restriction of r_M to subsets of σ. We point out, for later use, that this implies

$$(M_{(i)})_{|\sigma} = (M_{|\sigma})_{(i)}. \tag{6}$$

2.6 The Stanley-Reisner ideal, Betti numbers, and the reduced chain complex

Let M be a matroid on $E = \{1, \ldots, n\}$. Let $\Bbbk$ be a field.

Definition 2.11. A *circuit* of M is a subset C of E with the property that C is not itself independent, but $C \smallsetminus x$ is independent for every $x \in C$.

In other words, the circuits of a matroid are the minimal dependent sets, while the independent sets are precisely those that do not contain a circuit.

Let $S = \Bbbk[x_1, \ldots, x_n]$.

Definition 2.12 (Stanley-Reisner ideal). Let I_M be the ideal in S generated by monomials corresponding to circuits of M. That is, let

$$I_M = \langle x_{j_1} x_{j_2} \cdots x_{j_s} : \{j_1 j_2, \ldots, j_s\} \text{ is a circuit of } M \rangle.$$

We refer to I_M as the *Stanley-Reisner ideal* of M.

It is clear that, viewed as an S-module, the Stanley-Reisner ideal permits both the standard $\mathbb{N}_0$-grading and the standard $\mathbb{N}_0^n$-grading [4, Section 6.3].

Definition 2.13. For $\mathbf{a} \in \mathbb{N}_0^n$, let $S(-\mathbf{a})$ denote the S-module obtained by shifting the gradation of S, seen as an $\mathbb{N}_0^n$-graded module, by $\mathbf{a}$.

Definition 2.14. For $j \in \mathbb{N}_0$, let $S(-j)$ denote the S-module obtained by shifting the gradation of S, seen as an $\mathbb{N}_0$-graded module, by j.

Note that $S(-\mathbf{a})$ is isomorphic to $S\mathbf{x}^{\mathbf{a}}$ as an $\mathbb{N}_0^n$-graded S-module, while $S(-j)$ is isomorphic to $\langle x^j \rangle_S$ as an $\mathbb{N}_0$-graded S-module.

Definition 2.15. An $\mathbb{N}_0^n$-graded S-module F is said to be *free* if it is of the form

$$F = S(-\mathbf{a_1}) \oplus S(-\mathbf{a_2}) \cdots \oplus S(-\mathbf{a_r}),$$

for some $\mathbf{a_1}, \mathbf{a_2}, \ldots, \mathbf{a_r} \in \mathbb{N}_0^n$.

And likewise:

Definition 2.16. An $\mathbb{N}_0$-graded S-module F is said to be *free* if it is of the form

$$F = S(-j_1) \oplus S(-j_2) \cdots \oplus S(-j_r),$$

for some $j_1, j_2, \ldots, j_r \in \mathbb{N}_0$.

Definition 2.17. A chain of S-modules and S-homomorphisms

$$\cdots \longleftarrow X_{i-1} \xleftarrow{\phi_i} X_i \longleftarrow \cdots$$

is said to be a *complex* if $\operatorname{im} \phi_i \subseteq \ker \phi_{i-1}$ for each i. Furthermore, the complex is said to be *minimal* whenever $\operatorname{im} \phi_i \subseteq \langle x_1, x_2, \ldots, x_n \rangle X_{i-1}$.

A complex is said to be *exact at homological degree i* if $\operatorname{im} \phi_i = \ker \phi_{i-1}$. Bringing these concepts together, we have:

Definition 2.18. An $\mathbb{N}_0^n$-*graded minimal free resolution* of an $\mathbb{N}_0^n$-graded S-module N is a minimal left complex

$$0 \longleftarrow F_0 \xleftarrow{\phi_1} F_1 \xleftarrow{\phi_2} F_2 \longleftarrow \cdots \xleftarrow{\phi_l} F_l \longleftarrow 0 \qquad (7)$$

where

$$F_i = \bigoplus_{\mathbf{a} \in \mathbb{N}_0^n} S(-\mathbf{a})^{\beta_{i,\mathbf{a}}},$$

which is exact everywhere except for in F_0, where $F_0 / \operatorname{im} \phi_1 \cong N$. We also require the homomorphisms ϕ_i to be degree-preserving, in that degree $\mathbf{a}$ elements of F_i are sent to degree $\mathbf{a}$ elements of F_{i-1}.

It is straightforward to verify that the resolution being *minimal* implies $\mathbf{a} \in \{0,1\}^n$ for each $\mathbf{a}$ appearing in (7).

Replacing "$\mathbb{N}_0^n$-graded" with "$\mathbb{N}_0$-graded" and setting

$$F_i = \bigoplus_{j \in \mathbb{N}_0} S(-j)^{\beta_{i,j}}$$

in Definition 2.18 gives us the definition of an $\mathbb{N}_0$-*graded minimal free resolution* of N.

The $\beta_{i,\mathbf{a}}$ and $\beta_{i,j}$ are referred to as the $\mathbb{N}_0^n$-graded and $\mathbb{N}_0$-graded *Betti numbers* of N, respectively. Sometimes we want to emphasize the module N, and write $\beta_{i,\mathbf{a}}(N)$ or $\beta_{i,j}(N)$. Hilbert's Syzygy Theorem states that the *length* l of (7) is less than or equal to n. We shall here only be looking at minimal

free resolutions of the Stanley-Reisner ideal I_M. Since M is a matroid, these all have length $n - r(M) - 1$ (see e.g. [9, Corollary 3(b)]).

It follows from [8, Theroem A.2.2] that *the Betti numbers associated with a ($\mathbb{N}_0$- or $\mathbb{N}_0^n$-graded) minimal free resolution are unique*, in that any other minimal free resolution must have the same Betti numbers. We may therefore, without ambiguity, write

$$\beta_{i,j} = \sum_{|\operatorname{Supp}(\mathbf{a})|=j} \beta_{i,\mathbf{a}}.$$

Note that for an empty ideal all the (graded or ungraded) Betti numbers are zero. This is for example always the case with $I_{M_{(n-r(M))}}$ since $M_{(n-r(M))}$ has no circuits.

Definition 2.19. Let $I_i(M)$ denote the set consisting of those independent sets of M that have cardinality i, and let $\Bbbk^{I_i(M)}$ be the free $\Bbbk$-vector space on $I_i(M)$. The *(reduced) chain complex* of M over $\Bbbk$ is the complex

$$0 \longleftarrow \Bbbk^{I_0(M)} \xleftarrow{\delta_1} \cdots \longleftarrow \Bbbk^{I_{i-1}(M)} \xleftarrow{\delta_i} \Bbbk^{I_i(M)} \longleftarrow \cdots \xleftarrow{\delta_{r(M)}} \Bbbk^{I_{r(M)}(M)} \longleftarrow 0,$$

where the boundary maps δ_i are defined on independent sets of M of size i as follows: With the natural ordering on E, set $\operatorname{sign}(j,\sigma) = (-1)^{r-1}$ if j is the rth element of $\sigma \subseteq E$, and let

$$\delta_i(\sigma) = \sum_{j \in \sigma} \operatorname{sign}(j,\sigma)\, \sigma \smallsetminus j.$$

Extending δ_i $\Bbbk$-linearly, we obtain a $\Bbbk$-linear map from $I_i(M)$ to $I_{i-1}(M)$.

Definition 2.20. The ith *reduced homology* of M over $\Bbbk$ is the vector space

$$H_i(M;\Bbbk) = \ker(\delta_i)/\operatorname{im}(\delta_{i+1}).$$

In proving our main result (Theorem 5.1), we shall draw upon the following two results, the first of which is a concatenation of [1, Proposition 7.4.7 (i) and Proposition 7.8.1].

Theorem 2.1. *Let $H_i(M;\Bbbk)$ denote the i-th homology of M over $\Bbbk$. Then*

$$H_i(M;\Bbbk) = \begin{cases} \Bbbk^{(-1)^{i-1}\chi(M)}, & i = r(M) \\ 0, & i \neq r(M). \end{cases}$$

Theorem 2.2 (Hochster's formula)**.**

$$\beta_{i,\sigma}(I_M) = \dim_{\Bbbk} H_{|\sigma|-i-1}(M_{|\sigma};\Bbbk).$$

We would like to point out, for later use, that Theorems 2.1 and 2.2 combined imply

$$\sum_{i=0}^{n} (-1)^i \beta_{i,\sigma} = (-1)^{n_M(\sigma)-1} \beta_{n_M(\sigma)-1,\sigma}. \tag{8}$$

It is established in [1] that for a matroid M the dimension of $H_i(M; \Bbbk)$ is in fact independent of $\Bbbk$. Thus *for matroids, the ($\mathbb{N}_0$- or $\mathbb{N}_0^n$-graded) Betti numbers are not only unique, but independent of the choice of field.* We shall therefore omit referring to or specifying a particular field $\Bbbk$ throughout.

Example 2.3 (Continuation of Ex. 2.2). Since $M(H)$ has set of circuits

$$\big\{\{1,2,6,7\}, \{5,6\}, \{2,3,6,7\}, \{1,2,3,5\}, \{1,3,7\}, \{1,4,7\}, \{1,2,3,6\},$$
$$\{2,4,6\}, \{2,3,5,7\}, \{3,4,7\}, \{1,2,5,7\}, \{1,3,4\}, \{2,4,5\}\big\}$$

its Stanley-Reisner ideal is

$$I_{M(H)} = \langle x_1 x_2 x_6 x_7, x_5 x_6, x_2 x_3 x_6 x_7, x_1 x_2 x_3 x_5, x_1 x_3 x_7, x_1 x_4 x_7, x_1 x_2 x_3 x_6,$$
$$x_2 x_4 x_6, x_2 x_3 x_5 x_7, x_3 x_4 x_7, x_1 x_2 x_5 x_7, x_1 x_3 x_4, x_2 x_4 x_5 \rangle.$$

Using MAGMA ([5]), we find the $\mathbb{N}_0$-graded minimal free resolution of $I_{M(H)}$ to be

$$0 \leftarrow S(-2) \oplus S(-3)^6 \oplus S(-4)^6 \leftarrow S(-4)^5 \oplus S(-5)^{28} \leftarrow S(-6)^{31} \leftarrow S(-7)^{10} \leftarrow 0.$$

Similarly, we find the $\mathbb{N}_0$-graded minimal free resolutions corresponding to the elongations of M to be

$$I_{M(H)_{(1)}} :$$
$$0 \longleftarrow S(-4)^2 \oplus S(-5)^{15} \longleftarrow S(-6)^{29} \longleftarrow S(-7)^{13} \longleftarrow 0,$$

$$I_{M(H)_{(2)}} :$$
$$0 \longleftarrow S(-6)^7 \longleftarrow S(-7)^6 \longleftarrow 0,$$

$$I_{M(H)_{(3)}} :$$
$$0 \longleftarrow S(-7) \longleftarrow 0.$$

3 Number of codewords of weight j

Let C be a linear $[n, k]$-code over $\mathbb{F}_q$, with a generator matrix $G = [g_{i,j}]$ for $1 \le i \le k$, $1 \le j \le n$. Let $Q = q^r$ for some $r \in \mathbb{N}$.

Definition 3.1. For $0 \le m \le n$, let $A_{C,m}(Q)$ denote the number of words of weight m in $C \otimes_{\mathbb{F}_q} \mathbb{F}_Q$.

Let $\mathbf{c}_j$ denote column j of G. If $\mathbf{a} = (a_1, a_2, \ldots, a_k) \in \mathbb{F}_Q{}^k$, the codeword $\mathbf{a} \cdot G$ has weight n if and only if

$$\mathbf{c}_j{}^T \cdot \mathbf{a} \ne 0$$

for all $1 \le j \le n$. In other words, if we let $S_j(Q) = \{\mathbf{x} \in \mathbb{F}_Q^k : \mathbf{c}_j{}^T \cdot \mathbf{x} = 0\}$, corresponding to column j, we have that $\mathbf{a} \cdot G$ has weight n if and only if

$$\mathbf{a} \in \mathbb{F}_Q^k \smallsetminus (S_1(Q) \cup S_2(Q) \cup \cdots \cup S_n(Q)). \tag{9}$$

Definition 3.2. For $U = \{u_1, u_2, \ldots, u_s\} \subseteq \{1, \ldots, n\}$, let

$$S_U(Q) = S_{u_1}(Q) \cap S_{u_2}(Q) \cap \cdots \cap S_{u_s}(Q).$$

By the inclusion/exclusion-principle then, we see from (9) that

$$A_{C,n}(Q) = Q^k - \sum_{|U|=1} |S_U(Q)| + \sum_{|U|=2} |S_U(Q)| + \cdots + (-1)^n \sum_{|U|=n} |S_U(Q)|.$$

If $B_U = \begin{pmatrix} \mathbf{c}_{u_1}^T \\ \mathbf{c}_{u_2}^T \\ \vdots \\ \mathbf{c}_{u_s}^T \end{pmatrix}$, then $|S_U(Q)| = Q^{\dim(\ker B_U)} = Q^{k-\dim(\operatorname{col} B_U)} = Q^{k - r_{M(G)}(U)}$,

which according to (2) is equal to $Q^{n_{M(H)}(E \smallsetminus U)}$. Since $Q^k = |S_\emptyset(Q)|$, we conclude that

$$A_{C,n}(Q) = \sum_{U \subseteq E} (-1)^{|U|} Q^{n_{M(H)}(E \smallsetminus U)} = (-1)^n \sum_{\gamma \subseteq E} (-1)^{|\gamma|} Q^{n_{M(H)}(\gamma)}. \qquad (10)$$

Definition 3.3.

$$a_{C,\sigma}(Q) = |\{w \in C \otimes_{\mathbb{F}_q} \mathbb{F}_Q : \operatorname{Supp}(w) = \sigma\}|.$$

Lemma 3.1.

$$a_{C,\sigma}(Q) = (-1)^{|\sigma|} \sum_{\gamma \subseteq \sigma} (-1)^{|\gamma|} Q^{n_M(\gamma)}.$$

Proof. Let $C_\sigma(Q)$ denote the shortening of $C \otimes_{\mathbb{F}_q} \mathbb{F}_Q$ in $\{1 \ldots n\} \smallsetminus \sigma$, and let $H_{|\sigma}$ be the restriction of H to columns indexed by σ. Then $H_{|\sigma}$ is a parity-check matrix for $C_\sigma(Q)$.

Clearly $a_{C,\sigma}(Q) = a_{C_\sigma,\sigma}(Q)$, and since $M(H)_{|\sigma} \cong M(H_{|\sigma})$ it follows by an argument similar to the one leading to (10) that

$$a_{C,\sigma}(Q) = (-1)^{|\sigma|} \sum_{\gamma \subseteq \sigma} (-1)^{|\gamma|} Q^{n_{M(H)_{|\sigma}}(\gamma)}.$$

The result follows, since $n_{M(H)_{|\sigma}}(\gamma) = n_{M(H)}(\gamma)$ for all $\gamma \subseteq \sigma$. $\qquad \square$

Proposition 3.1. *For* $1 \leq m \leq n$,

$$A_{C,m}(Q) = (-1)^m \sum_{|\sigma|=m} \sum_{\gamma \subseteq \sigma} (-1)^{|\gamma|} Q^{n_{M(H)}(\gamma)}$$

Proof. This is clear from Lemma 3.1, since $A_{C,m}(Q) = \sum_{|\sigma|=m} a_{C,\sigma}(Q)$. $\qquad \square$

In the following sections we shall see what comes from generalizing the *weight polynomials* $A_{C,m}(Q)$ to matroids.

4 Generalized weight polynomials and a generalized enumerator

Looking back at Proposition 3.1, it is clear that the polynomial $A_C(Q)$ appearing there may equally well be defined for matroids in general – not only for those derived from a linear code.

For the remainder of this section, let M be a matroid on $E = \{1, \ldots, n\}$.

4.1 GWP and the enumerator

Definition 4.1 (GWP). We define the polynomial $P_{M,j}(Z)$ by letting $P_{M,0}(Z) = 1$ and
$$P_{M,j}(Z) = (-1)^j \sum_{|\sigma|=j} \sum_{\gamma \subseteq \sigma} (-1)^{|\gamma|} Z^{n_M(\gamma)} \text{ for } 1 \leq j \leq n.$$

We shall refer to $P_{M,j}$ as the jth *generalized weight polynomial*, or just *GWP*, of M.

In light of Proposition 3.1, we see that $A_{C,j}(q^r) = P_{M(H),j}(q^r)$ for any linear $\mathbb{F}_q$-code C with parity check matrix H.

Comparing Definition 4.1 with the definition of $d_i(M)$, it is immediately clear that the generalized weight polynomials together determine the higher weights:

Proposition 4.1.
$$d_i(M) = \min\{j : \deg P_{M,j} = i\}.$$

Also, we would like to point out that the nth generalized weight polynomial of M is equal to the *characteristic polynomial* (see [13]) of $\overline{M}$.

Analogous to how $A_{C,j}(Q)$ is used to define the *extended weight enumerator* $W_C(X, Y, Q)$ of a code C (see [12]), we use the GWP to define the *enumerator* of M:

Definition 4.2 (Matroid enumerator). The *enumerator* W_M of M is

$$W_M(X, Y, Z) = \sum_{i=0}^{n} P_{M,i}(Z) X^{n-i} Y^i.$$

Example 4.1. Let $\mathcal{V}^8$ be the matroid on $E = \{1, \ldots, 8\}$ with bases

$$\{\sigma \subseteq E : |\sigma| = 4\} \smallsetminus \{\{1,2,3,4\}, \{1,2,7,8\}, \{3,4,5,6\}, \{3,4,7,8\}, \{5,6,7,8\}\}.$$

This is the well-known *Vámos matroid*. It is non-representable; that is, it is not the vector matroid of any matrix (and thus does not come from any code). Using MAGMA, we find the enumerator of $\mathcal{V}^8$ to be

$$
\begin{aligned}
W_{\mathcal{V}^8}(X, Y, Z) = & X^8 + 5X^4Y^4Z - 5X^4Y^4 + 36X^3Y^5Z - 36X^3Y^5 + 28X^2Y^6Z^2 \\
& - 138X^2Y^6Z + 110X^2Y^6 + 8XY^7Z^3 - 56XY^7Z^2 + 148XY^7Z \\
& - 100XY^7 + Y^8Z^4 - 8Y^8Z^3 + 28Y^8Z^2 - 51Y^8Z + 30Y^8.
\end{aligned}
$$

Observe that if C is a linear code with parity-check matrix H and extended weight enumerator $W_C(X, Y, Q)$ (see e.g. [12]), then

$$W_C(X, Y, Q) = W_{M(H)}(X, Y, Q).$$

4.2 Equivalence to the Tutte polynomial

It was shown in [12] that the extended weight enumerator of a linear code is equivalent to the Tutte polynomial of its associated matroid. We shall see that this is still true when it comes to matroids and their enumerators, in general. After a small leap (Proposition 4.2), an analogous proof to the one found in [12] for linear codes went through.

Proposition 4.2.

$$P_{M,i}(Z) = \sum_{j=n-i}^{n} (-1)^{i+j+n} \binom{j}{n-i} \sum_{|\gamma|=j} Z^{n_M(E \smallsetminus \gamma)}.$$

Proof.

$$
\begin{aligned}
P_{M,i}(Z) &= (-1)^i \sum_{|\sigma|=i} \sum_{\gamma \subseteq \sigma} (-1)^{|\gamma|} Z^{n_M(\gamma)} \\
&= (-1)^i \sum_{|\sigma|=i} \sum_{E \smallsetminus \gamma \subseteq \sigma} (-1)^{|E \smallsetminus \gamma|} Z^{n_M(E \smallsetminus \gamma)} \\
&= (-1)^i \sum_{|\sigma|=i} \sum_{E \smallsetminus \sigma \subseteq \gamma} (-1)^{|E \smallsetminus \gamma|} Z^{n_M(E \smallsetminus \gamma)} \\
&= (-1)^i \sum_{|\gamma| \geq n-i} \sum_{\left\{\substack{E \smallsetminus \sigma: \\ E \smallsetminus \sigma \subseteq \gamma, \\ |\sigma|=i}\right\}} (-1)^{|E \smallsetminus \gamma|} Z^{n_M(E \smallsetminus \gamma)} \\
&= (-1)^i \sum_{|\gamma| \geq n-i} \binom{j}{n-i} (-1)^{|E \smallsetminus \gamma|} Z^{n_M(E \smallsetminus \gamma)} \\
&= \sum_{j=n-i}^{n} \sum_{|\gamma|=j} \binom{j}{n-i} (-1)^{i+j+n} Z^{n_M(E \smallsetminus \gamma)}.
\end{aligned}
$$

$\square$

Proposition 4.2 above is what enables us to use basically the same technique as that employed in [12] for the proofs of Theorems 4.1 and 4.2.

Lemma 4.1.

$$W_M(X, Y, Z) = \sum_{j=0}^{n} \sum_{|\gamma|=j} Z^{n_M(E \smallsetminus \gamma)} (X - Y)^j Y^{n-j}.$$

Proof.

$$W_M(X,Y,Z) = \sum_{i=0}^{n} \sum_{j=n-i}^{n} (-1)^{i+j+n} \binom{j}{n-i} \sum_{|\gamma|=j} Z^{n_M(E \smallsetminus \gamma)} X^{n-i} Y^i$$

$$= \sum_{j=0}^{n} \sum_{i=n-j}^{n} (-1)^{j-n+i} \binom{j}{j-n+i} \sum_{|\gamma|=j} Z^{n_M(E \smallsetminus \gamma)} X^{n-i} Y^i$$

$$= \sum_{j=0}^{n} \sum_{k=0}^{j} (-1)^k \binom{j}{k} \sum_{|\gamma|=j} Z^{n_M(E \smallsetminus \gamma)} X^{j-k} Y^{n-j+k}$$

$$= \sum_{j=0}^{n} \sum_{|\gamma|=j} Z^{n_M(E \smallsetminus \gamma)} \left(\sum_{k=0}^{j} (-1)^k \binom{j}{k} X^{j-k} Y^k \right) Y^{n-j}$$

$$= \sum_{j=0}^{n} \sum_{|\gamma|=j} Z^{n_M(E \smallsetminus \gamma)} (X - Y)^j Y^{n-j}.$$

$\square$

We shall also need a slight reformulation of the Tutte polynomial.

Lemma 4.2.

$$t_M(X,Y) = \sum_{j=0}^{n} \sum_{|\gamma|=j} (X-1)^{n_M(E \smallsetminus \gamma)-(n-r(M)-j)} (Y-1)^{n_M(E \smallsetminus \gamma)}.$$

Proof. Follows by rewriting the $t_M(X,Y)$ from Definition 2.8 as

$$t_M(X,Y) = \sum_{\gamma \subseteq E} (X-1)^{\overline{n}(\gamma)} (Y-1)^{n(E \smallsetminus \gamma)}$$

and noting that $\overline{n}(\gamma) = n(E \smallsetminus \gamma) - (\overline{r}(E) - |\gamma|)$.

$\square$

Using Lemmas 4.1 and 4.2 it is now routine to verify the following two identities:

Theorem 4.1.

$$W_M(X,Y,Z) = (X-Y)^{n-r(M)} Y^{r(M)} t_M \left(\frac{X}{Y}, \frac{X+(Z-1)Y}{X-Y} \right).$$

Theorem 4.2.

$$t_M(X,Y) = (X-1)^{-(n-r(M))} X^n W_M(1, X^{-1}, (X-1)(Y-1)).$$

Example 4.2 (Continuation of Ex. 4.1)**.** Having already found the weight enumerator of $\mathcal{V}^8$, we infer from Theorem 4.2 that

$$t_{\mathcal{V}^8}(X,Y) = X^4 + 4X^3 + 10X^2 + 5XY + 15X + Y^4 + 4Y^3 + 10Y^2 + 15Y.$$

14

5 The GWP is determined by $\mathbb{N}_0$-graded Betti numbers

As before, let M be a matroid on $E = \{1, \ldots, n\}$. Recall from Section 2 that the $\mathbb{N}_0$- and $\mathbb{N}_0^n$-graded Betti numbers corresponding to the Stanley-Reisner ideal I_M are independent of the choice of the underlying field $\Bbbk$. The only thing of importance, and thus our only assumption, is that the $\mathbb{N}_0$-graded (or $\mathbb{N}_0^n$-graded) minimal free resolution of I_M is constructed with respect to the same field as the reduced chain complex over M. We may therefore omit specifying a field. Recall also that $M_{(l)}$ denotes the elongation of M to rank $r(M) + l$.

Throughout the rest of this article we shall employ the convention that $\beta_{i,j}(I_{M_{(l)}}) = 0$ whenever $l \notin [0, n - r(M)]$.

Theorem 5.1 (Main result). *For each $1 \leq j \leq n$ the coefficient of Z^l in $P_{M,j}$ is equal to*

$$\sum_{i=0}^{n} (-1)^i \Big(\beta_{i,j}(I_{M_{(l-1)}}) - \beta_{i,j}(I_{M_{(l)}}) \Big).$$

Proof. Let $s_{\sigma,l}$ denote the coefficient of Z^l in $P_{M_{|\sigma},|\sigma|}$. Since

$$P_{M,j}(Z) = \sum_{|\sigma|=j} P_{M_{|\sigma},|\sigma|}(Z),$$

the coefficient of Z^l in $P_{M,j}(Z)$ is $\sum_{|\sigma|=j} s_{\sigma,l}$. On the other hand, we have

$$s_{\sigma,l} = (-1)^{|\sigma|} \sum_{\substack{\gamma \subseteq \sigma \\ n_M(\gamma)=l}} (-1)^{|\gamma|} = (-1)^{|\sigma|} \Bigg[\sum_{\substack{\gamma \subseteq \sigma \\ n_{M_{(l)}}(\gamma)=0}} (-1)^{|\gamma|} - \sum_{\substack{\gamma \subseteq \sigma \\ n_{M_{(l-1)}}(\gamma)=0}} (-1)^{|\gamma|} \Bigg].$$

Applying Theorems 2.1 and 2.2, in combination with (6), we see that

$$(-1)^{|\sigma|} \sum_{\gamma \subseteq \sigma, n_{M_{(l)}}(\gamma)=0} (-1)^{|\gamma|} = (-1)^{n_{M_{(l)}}(\sigma)} \dim H_{r_{M_{(l)}}(\sigma)}(M_{(l)|\sigma})$$

$$= (-1)^{n_{M_{(l)}}(\sigma)} \beta_{n_{M_{(l)}}(\sigma)-1,\sigma}(I_{M_{(l)|\sigma}}),$$

which is equal to $(-1)^{n_{M_{(l)}}(\sigma)} \beta_{n_{M_{(l)}}(\sigma)-1,\sigma}(I_{M_{(l)}})$ – since, in general, $\beta_{i,\sigma}(\Delta) = \beta_{i,\sigma}(\Delta_{|\sigma})$.

Thus

$$s_{\sigma,l} = (-1)^{n_{M_{(l)}}(\sigma)} \beta_{n_{M_{(l)}}(\sigma)-1,\sigma}(I_{M_{(l)}}) - (-1)^{n_{M_{(l-1)}}(\sigma)} \beta_{n_{M_{(l-1)}}(\sigma)-1,\sigma}(I_{M_{(l-1)}})$$

$$= (-1)^{n_{M_{(l-1)}}(\sigma)-1} \beta_{n_{M_{(l-1)}}(\sigma)-1,\sigma}(I_{M_{(l-1)}}) - (-1)^{n_{M_{(l)}}(\sigma)-1} \beta_{n_{M_{(l)}}(\sigma)-1,\sigma}(I_{M_{(l)}}),$$

which by (8) is equal to

$$\sum_{i=0}^{n} (-1)^i \beta_{i,\sigma}(I_{M_{(l-1)}}) - \sum_{i=0}^{n} (-1)^i \beta_{i,\sigma}(I_{M_{(l)}}).$$

Consequently, the coefficient of Z^l in $P_{M,j}(Z)$ is

$$\sum_{|\sigma|=j}\left(\sum_{i=0}^{n}(-1)^i\Big(\beta_{i,\sigma}(I_{M_{(l-1)}})-\beta_{i,\sigma}(I_{M_{(l)}})\Big)\right)=\sum_{i=0}^{n}(-1)^i\left(\sum_{|\sigma|=j}\beta_{i,\sigma}(I_{M_{(l-1)}})-\sum_{|\sigma|=j}\beta_{i,\sigma}(I_{M_{(l)}})\right)$$
$$=\sum_{i=0}^{n}(-1)^i\Big(\beta_{i,j}(I_{M_{(l-1)}})-\beta_{i,j}(I_{M_{(l)}})\Big).$$

$\square$

Example 5.1 (Continuation of Ex. 2.3). Let us calculate $P_{M(H),5}(Z)$ using Theorem 5.1. Having already found the $\mathbb{N}_0$-graded Betti numbers of $M(H)$ and its elongations, we easily calculate

$$P_{M(H),5}(Z)=\beta_{0,5}(I_{M(H)_{(1)}})Z^2$$
$$+\Big(\big(-\beta_{1,5}(I_{M(H)})\big)-\big(\beta_{0,5}(I_{M(H)_{(1)}})\big)\Big)Z$$
$$-\big(-\beta_{1,5}(I_{M(H)})\big)$$
$$=15Z^2+\big((-28)-15\big)Z-(-28).$$

Continuing like this, we find the complete set of weight polynomials:

$P_{M(H),0}(Z)=1$
$P_{M(H),1}(Z)=0$
$P_{M(H),2}(Z)=Z-1$
$P_{M(H),3}(Z)=6Z-6$
$P_{M(H)4}(Z)=2Z^2-Z-1$
$P_{M(H),5}(Z)=15Z^2-43Z+28$
$P_{M(H),6}(Z)=7Z^3-36Z^2+60Z-31$
$P_{M(H),7}(Z)=Z^4-7Z^3+19Z^2-23Z+10.$

Corollary 5.1. *Let C be a linear code over $\mathbb{F}_q$ of length n, with parity check matrix H. For $1\leq m\leq n$ and Q a power of q, we have*

$$A_{C,m}(Q)=\sum_{l=0}^{n}\left(\sum_{i=0}^{n}(-1)^i\Big(\beta_{i,m}(I_{M(H)_{(l-1)}})-\beta_{i,m}(I_{M(H)_{(l)}})\Big)\right)Q^l.$$

Proof. This is immediate from Theorem 5.1, since $A_{C,m}(Q)=P_{M(H),m}(Q)$ by Proposition 3.1. $\square$

In light of Corollary 5.1, the polynomials found in Example 5.1, when evaluated at q^r, determine the number of codewords of a given weight in $C\otimes_{\mathbb{F}_q}\mathbb{F}_{q^r}$.

Occasionally, the result of Corollary 5.1 can greatly simplify the task of calculating weight polynomials $A_{C,m}(Q)$ for a linear code C. This is for instance the case with MDS-codes:

Example 5.2. Let C be an MDS $[n, k]$-code over $\mathbb{F}_q$, with parity check matrix H. It is well known that $M(H)$ is the uniform matroid $U(s, n)$, where $s = n - k$; which of course implies that

$$M(H)_{(l)} = U(s + l, n).$$

From e.g. [9, Example 3], we see that

$$\beta_{i,j}(I_{M(H)_{(l)}}) = \begin{cases} \binom{j-1}{s+l}\binom{n}{j}, & i = j - l - s - 1. \\ 0, & \text{otherwise.} \end{cases}$$

We conclude from Corollary 5.1 that for $1 \le m \le n$, and $Q = q^r$, we have

$$A_{C,m}(Q) = \sum_{l=1}^{n}(-1)^{m+l+s}\binom{n}{m}\left(\binom{m-1}{s+l-1} + \binom{m-1}{s+l}\right)Q^l + (-1)^{m+s}\binom{n}{m}\binom{m-1}{s}$$

$$= (-1)^{m+s}\binom{n}{m}\left(\sum_{l=1}^{n}(-1)^l\binom{m}{s+l}Q^l + \binom{m-1}{s}\right).$$

5.1 Further results

The generalized weight polynomials of $M_{(k-1)}$ determine those of $M_{(k)}$ for all $1 \le k \le n - r(M)$.

Proposition 5.1. Let $k \ge 1$. If

$$P_{M_{(k-1)},j}(Z) = a_n Z^n + a_{n-1}Z^{n-1} + \cdots + a_1 Z + a_o,$$

then

$$P_{M_{(k)},j}(Z) = a_n Z^{n-1} + a_{n-1}Z^{n-2} + \cdots + a_2 Z + (a_1 + a_o).$$

Proof. Let $s_{\sigma,l}^{(k)}$ denote the coefficient of Z^l in $P_{M_{(k)}|\sigma,|\sigma|}$. As noted in the proof of Theorem 5.1, the coefficient of Z^l in $P_{M_{(k)},j}$ is $\sum_{|\sigma|=j} s_{\sigma,l}^{(k)}$, and

$$s_{\sigma,l}^{(k)} = (-1)^{|\sigma|}\sum_{\substack{\gamma \subseteq \sigma \\ n_{M_{(k)}}(\gamma)=l}}(-1)^{|\gamma|}.$$

Assume first that $l \ge 1$. By Proposition 2.1 we have,

$$s_{\sigma,l}^{(k)} = (-1)^{|\sigma|}\sum_{\substack{\gamma \subseteq \sigma \\ n_{M_{(k)}}(\gamma)=l}}(-1)^{|\gamma|}$$

$$= (-1)^{|\sigma|}\sum_{\substack{\gamma \subseteq \sigma \\ n_{M_{(k-1)}}(\gamma)=l+1}}(-1)^{|\gamma|}$$

$$= s_{\sigma,l+1}^{(k-1)}.$$

Finally, by Proposition 2.1 again, we see that

$$
\begin{aligned}
s_{\sigma,0}^{(k)} &= (-1)^{|\sigma|} \sum_{\substack{\gamma \subseteq \sigma \\ n(\gamma) \leq k}} (-1)^{|\gamma|} \\
&= (-1)^{|\sigma|} \sum_{\substack{\gamma \subseteq \sigma \\ n(\gamma) = k}} (-1)^{|\gamma|} + (-1)^{|\sigma|} \sum_{\substack{\gamma \subseteq \sigma \\ n(\gamma) \leq k-1}} (-1)^{|\gamma|} \\
&= (-1)^{|\sigma|} \sum_{\substack{\gamma \subseteq \sigma \\ n_{M_{(k-1)}}(\gamma) = 1}} (-1)^{|\gamma|} + (-1)^{|\sigma|} \sum_{\substack{\gamma \subseteq \sigma \\ n_{M_{(k)}}(\gamma) = 0}} (-1)^{|\gamma|} \\
&= s_{\sigma,1}^{(k-1)} + s_{\sigma,0}^{(k-1)},
\end{aligned}
$$

and this concludes our proof. $\qquad\square$

Combining Propositions 5.1 and 4.1, we see that

Corollary 5.2.
$$
d_i(M_{(l+1)}) = d_{i+1}(M_{(l)}).
$$

Example 5.3 (The simplex code $\mathcal{S}_2(3)$). Let $\mathcal{S}_2(3)$ be the simplex code of dimension 3 over $\mathbb{F}_2$. This code has length $n = 7$. Let H be a parity-check matrix of $\mathcal{S}_2(3)$.

The higher weights of $\mathcal{S}_2(3)$ are $(d_1, d_2, d_3) = (4, 6, 7)$, from which it follows by way of [10, Theorem 2] that the non-zero Betti numbers of $I_{M(H)}$ are

$$
(\beta_{0,4}, \beta_{1,6}, \beta_{2,7}) = (7, 14, 8).
$$

By Proposition 5.2, the higher weights of $M_{(1)}$ are $(d_1, d_2) = (6, 7)$, which implies that $M(H)_{(1)}$ must be the uniform matroid $U(5, 7)$. From [9, Example 3] then, we see that the only non-zero Betti numbers of $I_{M(H)_{(1)}}$ are $\beta_{0,6}(I_{M(H)_{(1)}}) = 7$ and $\beta_{1,7}(I_{M(H)_{(1)}}) = 6$. As always, the $(n-r(M(H))-1)^{th}$ elongation $M(H)_{(2)}$ has $\{1,\ldots,7\}$ as its only circuit, such that the only non-zero Betti number associated with $I_{M(H)_{(2)}}$ is $\beta_{0,7}(I_{M(H)_{(2)}}) = 1$.

Having found all $\mathbb{N}_0$-graded Betti numbers from all elongations, we easily calculate the weight polynomials using Corollary 5.1:

$$
\begin{aligned}
A_{\mathcal{S}_2(3),0}(Q) &= 1 \\
A_{\mathcal{S}_2(3),1}(Q) &= 0 \\
A_{\mathcal{S}_2(3),2}(Q) &= 0 \\
A_{\mathcal{S}_2(3),3}(Q) &= 0 \\
A_{\mathcal{S}_2(3),4}(Q) &= 7Q - 7 \\
A_{\mathcal{S}_2(3),5}(Q) &= 0 \\
A_{\mathcal{S}_2(3),6}(Q) &= 7Q^2 - 21Q + 14 \\
A_{\mathcal{S}_2(3),7}(Q) &= Q^3 - 7Q^2 + 14Q - 8
\end{aligned}
$$

6 Concerning the converse

Having seen that the Betti numbers associated with the elongations $M_{(i)}, 0 \leq i \leq n - r(M)$, determine the polynomials $P_{M,j}(Z), 1 \leq j \leq n$, it is natural to ask whether the opposite is true. The answer to this is negative, as the following counterexample shows:

Example 6.1 (Continuation of Ex. 5.1)**.** Let N be the matroid on $\{1, \ldots, 7\}$ with bases

$$B(N) = \{\{1, 4, 7\}, \{1, 3, 6\}, \{1, 3, 5\}, \{1, 3, 4\}, \{2, 3, 6\}, \{3, 4, 7\}, \{1, 2, 5\}, \{1, 5, 7\},$$
$$\{3, 6, 7\}, \{2, 4, 7\}, \{3, 5, 6\}, \{2, 3, 4\}, \{1, 2, 3\}, \{1, 2, 7\}, \{1, 5, 6\}, \{3, 4, 5\},$$
$$\{1, 6, 7\}, \{1, 4, 5\}, \{2, 3, 7\}, \{2, 5, 6\}, \{2, 4, 5\}, \{3, 5, 7\}, \{2, 6, 7\}, \{2, 5, 7\}\}.$$

The Stanley-Reisner ideal of N has minimal free resolution

$$0 \leftarrow S(-2) \oplus S(-3)^6 \oplus S(-4)^5 \leftarrow S(-4)^4 \oplus S(-5)^{28} \leftarrow S(-6)^{31} \leftarrow S(-7)^{10} \leftarrow 0.$$

Comparing to the minimal free resolution of $I_{M(H)}$, we see that the Betti numbers are not the same. However, it is easy to see, using Proposition 5.1, that N has the same generalized weight polynomials as $M(H)$.

Note that this is the "smallest" counterexample, in that there are no counterexamples for $n < 7$.

Moreover, knowing the Betti numbers of M is in itself *not* enough to calculate $P_{M,j}$ – in general we need the Betti numbers derived from the elongations $M_{(i)}$ as well:

Example 6.2. The matroids M and N on $\{1, \ldots, 8\}$ with bases

$$B(M) = \{\{1, 3, 4, 6, 7\}, \{1, 2, 3, 6, 8\}, \{1, 2, 3, 4, 8\}, \{1, 2, 3, 5, 8\}, \{1, 2, 5, 6, 8\}, \{1, 2, 3, 4, 7\},$$
$$\{1, 2, 3, 5, 7\}, \{1, 2, 5, 6, 7\}, \{1, 3, 4, 5, 7\}, \{1, 3, 4, 6, 8\}, \{1, 2, 4, 6, 8\}, \{1, 2, 4, 6, 7\},$$
$$\{1, 3, 4, 5, 8\}, \{1, 2, 4, 5, 7\}, \{1, 4, 5, 6, 7\}, \{1, 2, 3, 6, 7\}, \{1, 3, 5, 6, 7\}, \{1, 4, 5, 6, 8\},$$
$$\{1, 3, 5, 6, 8\}, \{1, 2, 4, 5, 8\}\}$$

and

$$B(N) = \{\{1, 3, 4, 6, 7\}, \{1, 2, 3, 4, 8\}, \{1, 2, 3, 5, 8\}, \{1, 2, 5, 6, 8\}, \{1, 2, 3, 4, 7\}, \{1, 2, 3, 5, 7\},$$
$$\{1, 2, 5, 6, 7\}, \{1, 3, 4, 5, 7\}, \{1, 3, 4, 6, 8\}, \{1, 2, 4, 6, 8\}, \{1, 2, 4, 6, 7\}, \{1, 3, 4, 5, 8\},$$
$$\{1, 2, 4, 5, 7\}, \{1, 3, 4, 5, 6\}, \{1, 2, 4, 5, 6\}, \{1, 3, 5, 6, 7\}, \{1, 2, 3, 5, 6\}, \{1, 2, 3, 4, 6\},$$
$$\{1, 3, 5, 6, 8\}, \{1, 2, 4, 5, 8\}\},$$

respectively, both have

$$0 \leftarrow S(-2) \oplus S(-4)^5 \leftarrow S(-5)^4 \oplus S(-6)^5 \leftarrow S(-7)^4 \leftarrow 0$$

as the minimal free resolution of their associated Stanley-Reisner ideal, while

$$P_{M,4}(Z) = Z^2 - 5Z + 4 \neq 2Z^2 - 6Z + 4 = P_{N,4}(Z).$$

Again this is the "smallest" counterexample.

It is however possible for two non-isomorphic matroids to have identical $\mathbb{N}_0$-graded Betti numbers in all elongation levels (the smallest example of which is given by a pair of rank 3 on $\{1, \ldots, 6\}$).

References

[1] A. Bjoerner, *Homology and shellability*, 1992, pp. 226-283.

[2] A. Barg, *On some polynomials related to weight enumerators of linear codes*, SIAM J. Discrete Math. **15**(2) (2002) 155-164.

[3] T. Britz, *Code enumerators and Tutte polynomials*, IEEE Trans. Inform. Theory **55**(9) (2010) 4350-4358.

[4] D. Cox, J. Little, D. O'Shea, *Using Algebraic Geometry*, Graduate Texts in Mathematics **185**, Springer, 2000.

[5] W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997) 235-265.

[6] I. Duursma, *Combinatorics of the Two-Variable Zeta Function*, Finite Fields and Applications, Lecture Notes in Comput. Sci. **2948** (2004) 109-136.

[7] C. Greene, *Weight enumeration and the geometry of linear codes*, St. Appl. Math. **55** (1976) 119-128.

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

[9] T. Johnsen, H. Verdure, *Hamming weights and Betti numbers of Stanley-Reisner rings associated to matroids*, AAECC **24** no. 1 (2013) 73-93.

[10] T. Johnsen, H. Verdure, *Stanley-Reisner resolution of constant-weight linear codes*, Des. Codes Cryptogr. **72**(2) (2014) 471-481.

[11] R. Jurrius. *Classifying polynomials of linear codes*, Masters thesis, Leiden University, 2008

[12] R. Jurrius, R. Pellikaan *Codes, arrangements and matroids*. In: E. Martinez-Moro (Ed.), Algebraic geometry modeling in information theory (pp. 219-325). London: World Scientific, 2013.

[13] J. Kung, *Critical problems*, Contemporary Mathematics **197** (1996).

[14] E. Miller, B. Sturmfels, *Combinatorial Commutative Algebra*, Graduate Texts in Mathematics **227**, Springer, 2005.

[15] J. Oxley, *Matroid Theory*, 2nd Edition, Oxford University Press Inc., New York, 1992.

[16] V. Reiner, *An interpretation for the Tutte polynomial*, European J. Combin. **20**(2) (1999) 149-161.

[17] D. Vertigan, *Latroids and their representation by codes over modules*, Trans. Amer. Math. Soc. **356**(10) (2004) 3841-3868.