Discrete Mathematics 339 (2016) 632–645

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

A generalization of weight polynomials to matroids

Trygve Johnsen, Jan Roksvold *, Hugues Verdure

Department of Mathematics and Statistics, UiT The Arctic University of Norway, P.O. Box 6050 Langnes, 9037 Tromsø, Norway

ARTICLE INFO

Article history:
Received 2 January 2014
Received in revised form 1 October 2015
Accepted 4 October 2015
Available online 11 November 2015

Keywords:
Matroid
Weight enumerator
Linear code
Stanley–Reisner ideal
Higher weights
Tutte polynomial

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

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

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 Eq. (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

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

* Corresponding author.
E-mail addresses: trygve.johnsen@uit.no (T. Johnsen), jan.n.roksvold@uit.no (J. Roksvold), hugues.verdure@uit.no (H. Verdure).

http://dx.doi.org/10.1016/j.disc.2015.10.005
0012-365X/

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 [4, 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 [1], 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, [1] 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 [15, Corollaries 10, 11 and 12] when looking at two-variable coloring formulas for graphs. A generalization of Greene's theorem is given in [16, 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 $J \subseteq \{1 \dots n\}$.

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.