DIMACS Technical Report 99-54

On some polynomials related to weight enumerators of linear codes

by

Alexander Barg[1]
Math. Research
Bell Labs, Lucent Technologies
700 Mountain Ave.,
Murray Hill. NJ 07974

[1]Permanent Member

DIMACS is a partnership of Rutgers University, Princeton University, AT&T Labs-Research, Bell Labs, NEC Research Institute and Telcordia Technologies (formerly Bellcore).

DIMACS was founded as an NSF Science and Technology Center, and also receives support from the New Jersey Commission on Science and Technology.

ABSTRACT

A linear code can be thought of as a vector matroid represented by the columns of code's generator matrix; a well-known result in this context is Greene's theorem on a connection of the weight polynomial of the code and the Tutte polynomial of the matroid. We examine this connection from the coding-theoretic viewpoint, building upon the rank polynomial of the code. This enables us to obtain bounds on all-terminal reliability of linear matroids and new proofs of two known results: Greene's theorem and a connection between the weight polynomial and the partition polynomial of the Potts model. First version posted in December 1999, revised in December 2001.

1 Introduction

A linear matroid M together with a chosen representation over a finite field $\mathbb{F}_q$ is the same object as a linear code. The most well-known result underlining this connection is Greene's theorem on the relation of the weight polynomial of the code and the Tutte polynomial of the matroid. In this paper we further examine the relation between the polynomial invariants of codes, matroids and some other combinatorial objects. Our point of view is coding-theoretic. We begin with listing basic definitions for linear codes and some very simple linear-algebraic properties of subcodes. These properties lead almost immediately to a relation between the weight polynomial of a linear code and the rank polynomial of the corresponding matroid. This relation is of course nothing else than Greene's theorem; as we will show, this theorem is a purely linear-algebraic fact. An advantage of the coding-theoretic point of view is determined by the fact that the weight polynomial enjoys more structural properties than more general matroid invariants; when this structure translates to other problems, it sometimes produces interesting insights.

As an example, we relate the reliability polynomial of a linear matroid to an evaluation of the weight polynomial of the code. The corresponding functional on linear codes turns out to be well-studied under the name of the probability of undetected error of the code. Together with some related ideas this enables us to derive upper and lower bounds on the matroid reliability. As another application of the weight-rank connection, we give a direct proof of the link between the partition function of the Potts model and the weight polynomial of the cocycle code of the graph.

General sources for coding theory are the books [17], [19]. Relevant applications of the Tutte polynomial are covered in [6], [24]. All the necessary information on interaction models is contained in [24].

2 The rank polynomial of the code

2.1 Definitions

A *linear code* C of length n is a linear subspace of $\mathbb{F}_q^n$. Let $\mathcal{A}_i$ be the number of vectors of Hamming weight i in it, $0 \leq i \leq n$. Clearly, $\mathcal{A}_0 = 1$. The minimal $i \geq 1$ such that $\mathcal{A}_i \neq 0$ is called the *minimum distance* of the code, denoted $d(C)$. The polynomial

$$\mathcal{A}(x,y) = \sum_{i=0}^{n} \mathcal{A}_i x^{n-i} y^i$$

is called the *weight polynomial* of C. The matrix $\mathbf{G}$ whose rows form a basis of C as an $\mathbb{F}_q$-linear space is called a *generator matrix* of the code.

Let $E = \{1, 2, \ldots, n\}$ be the set of code coordinates. For any subset $F \subset E$ denote by $\mathbf{G}(F)$ the submatrix of $\mathbf{G}$ formed by columns with numbers in F. Let $\bar{F} = E \setminus F$.

Let $Z \subset E$ be the set of all-zero columns in G. The number $n - |Z|$ is called the *effective length* of C, denoted $\mathrm{el}(C)$.

By $(\mathbf{a}, \mathbf{b}) = \sum_{i=1}^{n} a_i b_i$ we denote the standard dot product in $\mathbb{F}_q^n$. The *dual code* of C is defined as $C^\perp := \{\mathbf{c} \in \mathbb{F}_q \mid (\mathbf{c}, \mathbf{c}') = 0 \text{ for all } \mathbf{c}' \in C\}$. Denote by $\mathbf{H}$ the generator matrix of $C^\perp$ (this matrix is also called the *parity-check matrix* of C). Let $k := \dim C$, so $\dim C^\perp = n - k$. The weight polynomial of $C^\perp$ is denoted by $\mathcal{A}^\perp(x,y)$. The minimum distance of $C^\perp$ is also called the *dual distance* of C.

Let $C_F := \mathrm{proj}_F\, C,\ C^F := \{\mathbf{c} \in C \mid c_e = 0\ \forall e \in \bar{F}\}$. In coding literature the subcode C^F is called the *shortening* of C and the subcode C_F the *puncturing* of C, both with respect to $\bar{F}$. Clearly, $\dim C_F = \mathrm{rk}(\mathbf{G}(F))$. Standard properties of these subcodes are given in the following obvious lemma.

Lemma 1 (i) $C_F \cong C/C^{\bar{F}};\quad \dim C_F = k - \dim C^{\bar{F}}$
(ii) $\dim C^F = |F| - \mathrm{rk}(\mathbf{H}(F))$.

The *rank polynomial* of C is defined as $\mathcal{U}(x,y) = \sum_{u=0}^{n}\sum_{v=0}^{k}\mathcal{U}_u^v x^u y^v$, where

$$\mathcal{U}_u^v = |\{F \subseteq E \mid |F| = u, \mathrm{rk}(\mathbf{G}(F)) = v\}|.$$

The code C can be also thought of as a (vector) matroid M represented by the column space of $\mathbf{G}$; so given C we speak of a matroid of the code, denoted $M(C)$, and vice versa, given M, we call C the code of M, denoted $C(M)$. If $\mathrm{el}(C) = n$ then $M(C)$ is loopless. The interest for us in pursuing this connection, besides establishing new links between linear codes and combinatorics, is that methods of coding theory enable one to derive absolute bounds on evaluations of $\mathcal{A}(x,y)$ which can be useful in other areas.

2.2 Greene's theorem

The rank polynomial of C, essentially, is an invariant of $M(C)$. Another matroid invariant that appears in numerous contexts in combinatorics, is the *Tutte polynomial* of M, defined as follows:

$$\mathcal{T}(M;x,y) = \sum_{u=0}^{n}\sum_{v=0}^{k}\mathcal{U}_u^v(x-1)^{k-v}(y-1)^{u-v},$$

where $k = \dim C$ is the rank of M. The following theorem relates $\mathcal{A}(x,y)$ and $\mathcal{T}(M;x,y)$.

Theorem 1 (Greene [8])

$$\mathcal{A}(x,y) = y^{n-k}(x-y)^k\mathcal{T}\Big(M;\frac{x+(q-1)y}{x-y},\frac{x}{y}\Big). \tag{1}$$

The proof, as given in [8] and reproduced in [23], [6], first shows that a certain polynomial related to $\mathcal{A}(x,y)$ is a (Tutte-Grothendieck) invariant of M, and then invokes Brylawski's theorem that states that every invariant is an evaluation of the Tutte polynomial, defined completely by its values on loops and isthmuses. We shall show that this theorem follows from Lemma 1.

The polynomials $\mathcal{A}(x,y)$ and $\mathcal{U}(x,y)$ are connected by the following relation.

Theorem 2

$$\mathcal{A}(x,y) = y^n|C|\mathcal{U}\Big(\frac{x-y}{y},\frac{1}{q}\Big). \tag{2}$$

Proof : Let us count in two ways the size of the set

$$\Big\{(F,\mathbf{c})|F \subseteq E,\ |F| = w \text{ and } \mathbf{c} \in C^F,\ 0 \le \mathrm{wt}(\mathbf{c}) \le w\Big\}.$$

Taking into account Lemma 1, we obtain

$$\sum_{i=0}^{w} \binom{n-i}{n-w} \mathcal{A}_i = \sum_{|F|=w} |C^F| = \sum_{|F|=w} q^{k-\mathrm{rk}(\mathbf{G}(\bar{F}))} \tag{3}$$

$$= \sum_{u=0}^{k} q^{k-u} \mathcal{U}_{n-w}^{u} \quad (0 \le w \le n). \tag{4}$$

Now let $\mathcal{B}_w = \sum_{j=0}^{w} \binom{n-j}{n-w} \mathcal{A}_j$. We then have

$$\mathcal{A}(x,y) = \sum_{w=0}^{n} \mathcal{B}_w (x-y)^{n-w} y^w = \sum_{w=0}^{n} \sum_{u=0}^{k} q^{k-u} \mathcal{U}_{n-w}^{u} (x-y)^{n-w} y^w \tag{5}$$

$$= \sum_{\alpha=0}^{n} \sum_{u=0}^{k} q^{k-u} \mathcal{U}_{\alpha}^{u} (x-y)^{\alpha} y^{n-\alpha} = y^n q^k \mathcal{U}\Big(\frac{x-y}{y}, \frac{1}{q}\Big).$$

∎

Note that Theorem 2 already relates $\mathcal{A}(x,y)$ to a polynomial with coefficients $\mathcal{U}_u^v$. Therefore, Theorem 1 should be a mere reformulation of (2), which it is.

Proof : (OF THEOREM 1) Starting with the definition of $\mathcal{T}$, we obtain

$$y^{n-k}(x-y)^k \mathcal{T}\Big(M; \frac{x+(q-1)y}{x-y}, \frac{x}{y}\Big)$$

$$= y^{n-k}(x-y)^k \sum_{u=0}^{n} \sum_{v=0}^{k} \mathcal{U}_u^v \Big(\frac{qy}{x-y}\Big)^{k-v} \Big(\frac{x-y}{y}\Big)^{u-v}$$

$$= y^n q^k \mathcal{U}\Big(\frac{x-y}{y}, \frac{1}{q}\Big).$$

∎

Eq.(3) together with Lemma 1(ii) also enables us to relate the weight polynomial of C and the rank polynomial of $C^\perp$, denoted $\mathcal{U}^\perp(x,y)$.

Theorem 3 [4]

$$\mathcal{A}(x,y) = (x-y)^n \mathcal{U}^\perp\Big(\frac{qy}{x-y}, \frac{1}{q}\Big) \tag{6}$$

$$\mathcal{U}^\perp(x,y) = x^n y^{\dim C^\perp} \mathcal{U}\Big(\frac{1}{xy}, y\Big) \tag{7}$$

The only known application of Theorem 1 in coding theory [8],[23], [6] is to derive MacWilliams-type theorems on the relation of $\mathcal{A}$ and $\mathcal{A}^\perp$. The classical MacWilliams equation has the form

$$\mathcal{A}^\perp(x,y) = \frac{1}{|C|} \mathcal{A}(x+(q-1)y, x-y). \tag{8}$$

This was proved in [8] by using (1) together with the relation $T(M(C);x,y) = T(M(C^\perp);y,x)$, which is implied by the definition of the Tutte polynomial. We have shown that this argument is the same as one of the two proof in the original paper [16].

2.3 Support weight distributions

Let us also mention a generalization of Theorem 1 observed in [3]. It is related to the notion of support weight distributions of linear codes.

The *support* of a subset $A \subset C$ is defined as $\operatorname{supp} A = \bigcup_{\mathbf{c}\in A} \operatorname{supp}(\mathbf{c})$, where $\operatorname{supp}(\mathbf{c}) = \{e \in \{1, 2, \ldots, n\} : \mathbf{c}_e \neq 0\}$.

Definition. The *rth support weight distribution* of a code C is the set of n numbers $\mathcal{A}_i^r$, $0 \le i \le n$, where

$$\mathcal{A}_i^r = \big|\{A \ : \ A \text{ a linear subcode of } C, \dim A = r, |\operatorname{supp} A| = i\}\big|.$$

In particular, for $r = 1$ we obtain the "support distribution" of the projective code $\mathbf{P}C$. So $\mathcal{A}_i = \mathcal{A}_i^0 + (q-1)\mathcal{A}_i^1, 0 \le i \le n$. The following theorem relates the support weight distributions of C to its Tutte polynomial.

Theorem 4 [3]

$$\sum_{i=0}^{n} \Big(\sum_{m=0}^{r} [r]_m \mathcal{A}_i^m \Big) x^{n-i} y^i = (x-y)^k y^{n-k} \mathcal{T}\Big(M, \frac{x + (q^r-1)y}{x-y}, \frac{x}{y}\Big),$$

where $k = \dim C$ *and* $[r]_m := \prod_{j=0}^{m-1}(q^r - q^j)$.

The proof method of [3] parallels that of [8]. Without going into details we remark that it is possible to give a proof of Theorem 4 similar to that of the previous section. The proof is based on the following generalization of Lemma 4.

Lemma 2 [21]

$$\sum_{i=0}^{w} \binom{n-i}{n-w} \mathcal{A}_i^r = \sum_{v=0}^{n-k} \begin{bmatrix} w-v \\ r \end{bmatrix} (\mathcal{U}^\perp)_w^v \quad (0 \le w \le n, 0 \le r \le k)$$

Another proof of Theorem 4 is given in [20].

3 The reliability polynomial of linear matroids

3.1 Definitions

Let M be a linear matroid of rank k on the ground set E of size n defined by its representation over $\mathbb{F}_q$ and let $f_i := \mathcal{U}_i^i$ be its number of independent sets of size i. The (*all-terminal*) *reliability polynomial* of M, by definition, is

$$\mathcal{R}(M; x, y) := \sum_{i=0}^{k} f_i x^{n-i} y^i \tag{9}$$

The terminology is motivated by the special case of cographic matroids. Namely, let $G(V, E)$ be a connected graph and let M be a matroid whose independent sets are given by subsets of edges whose removal does not make G disconnected. The rank k of M equals $|E| - |V| + 1$. Further,

suppose that G is subjected to an edge removal process under which each edge in E is independently left intact with probability p and removed with probability $1-p$. Then the probability that upon completion of this process the graph remains connected is given by $\mathcal{R}(M;p,1-p)$. If G is thought of as a network in which each link is operational with probability p then $\mathcal{R}(M;p,1-p)$ gives the probability for G to be operational. Below we use the notation $\mathrm{Rel}(M,p) := \mathcal{R}(M;p,1-p)$.

One of the main problems related to the reliability polynomial in the general case is deriving bounds on $\mathrm{Rel}(M,p)$ in terms of other numerical parameters of M. The aim of this section is to use results from coding theory to derive bounds on $\mathrm{Rel}(M,p)$.

3.2 Upper bounds

Let $(\mathcal{A}_0, \mathcal{A}_1, \ldots, \mathcal{A}_n)$ be the weight distribution of a linear k-dimensional code $C(M)$. The reliability $\mathrm{Rel}(M,p)$ is related to the weight polynomial $\mathcal{A}(\cdot,\cdot)$ of $C(M)$, via the following inequalities.

Theorem 5

$$\mathrm{Rel}(M,p) \leq \sum_{w=n-k+1}^{n} p^w (1-p)^{n-w} \sum_{j=1}^{w} \binom{n-j}{n-w} \mathcal{A}_j + f_k p^{n-k}(1-p)^k \tag{10}$$

$$\mathrm{Rel}(M,p) \leq \mathcal{A}(1,p) - 1 + f_k p^{n-k}(1-p)^k. \tag{11}$$

Proof : We have

$$\begin{aligned}
\mathrm{Rel}(M,p) - f_k p^{n-k}(1-p)^k &= \sum_{i=0}^{k-1} \mathcal{U}_i^i p^{n-i}(1-p)^i \\
&\leq \sum_{i=0}^{k-1} p^{n-i}(1-p)^i \sum_{u=0}^{i} (q^{k-u}-1)\mathcal{U}_i^u \\
&= \sum_{w=n-k+1}^{n} p^w (1-p)^{n-w} \sum_{u=0}^{k} (q^{k-u}-1)\mathcal{U}_{n-w}^u.
\end{aligned}$$

Now proceeding as in (3), (5) we see that

$$\mathcal{C}_w := \sum_{u=0}^{k} (q^{k-u}-1)\mathcal{U}_{n-w}^u = \sum_{j=1}^{w} \binom{n-j}{n-w} \mathcal{A}_j$$

Substituting this proves (10). To prove (11), we extend the summation on w on the right-hand side of (10) to the range $1 \leq w \leq n$ and note that

$$\sum_{i=1}^{n} \mathcal{A}_i x^{n-i} y^i = \sum_{w=1}^{n} \mathcal{C}_w (x-y)^{n-w} y^w.$$

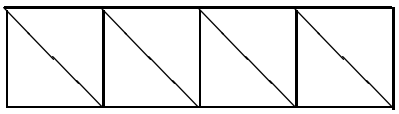
Thus

$$\sum_{w=1}^{n} p^w (1-p)^{n-w} \sum_{j=1}^{w} \binom{n-j}{n-w} \mathcal{A}_j = \sum_{i=1}^{n} \mathcal{A}_i p^i.$$

This completes the proof. ∎

In general bounds (10)-(11) are good only for small values of p. We give one simple example.

EXAMPLE. Consider the "ladder" graph Γ from [7].



Its cocycle matroid M has rank 8 and can be represented over $\mathbb{F}_2$ by the columns of the matrix $\mathbf{G}$ whose rows are $(1^3 0^{14})$, $(1^2 0 1^2 0^{12})$, and their three right shifts by four positions. The code C generated by $\mathbf{G}$ has parameters $[n = 17, k = 8, d = 3]$ and weight distribution $\mathcal{A}_0 = 1, \mathcal{A}_3 = 8, \mathcal{A}_4 = 7, \mathcal{A}_5 = 6, \ldots$. Its dual code $C^\perp$ (the cycle code of Γ) has parameters $[17, 9, 2]$. We have [7] $f_0 = 1, f_1 = 17, f_2 = 134, f_3 = 641, f_4 = 2041, f_5 = 4447, \ldots$. On the other hand, estimate (10) gives $f_0 = 1, f_1 \le 17, f_2 \le 136, f_3 \le 688, f_4 \le 2499, f_5 \le 7013 \ldots$. For small p this results in reasonably good estimates of $\mathrm{Rel}(M, p)$. We note that the well-known Ball-Provan bounds give in this case better results: $f_0 = 1, f_1 \le 17, f_2 \le 134, f_3 \le 651, f_4 \le 2184, f_5 \le 5369, \ldots$ and hence better estimates of $\mathrm{Rel}(M, p)$.

An advantage of the estimate (10) is that the weight coefficients of any linear code satisfy a set of Delsarte inequalities, i.e., linear inequalities of the form

$$\sum_{u=0}^{n} (-1)^{j-u} \binom{n-u}{n-j} q^u \sum_{i=0}^{n-u} \binom{n-i}{u} A_i \ge 0 \quad (0 \le j \le n).$$

This enables one to upper-bound the right-hand side of (10) using the methods of [1], [2]. Note that absolute bounds on the reliability $\mathrm{Rel}(M(C), p)$ that are obtainable under this approach involve the minimum distance of the code C as a parameter.

Another way to bound above the right-hand side of (11) is by estimating evaluations of $\mathcal{A}(x, y)$. For them, let us look at the problem of error detection in coding theory. More specifically, given a linear code C, its *probability of undetected error* is

$$P_{ue}(C, \epsilon) := \sum_{i=1}^{n} \mathcal{A}_i \Big(\frac{\epsilon}{q-1}\Big)^i (1-\epsilon)^{n-i} = \mathcal{A}\Big(1-\epsilon, \frac{\epsilon}{q-1}\Big) - (1-\epsilon)^n.$$

The motivation for this definition is the following scenario of information transmission. Suppose a q-ary code C is used to send messages over the q-ary symmetric channel. The channel is memoryless, and if a is a q-ary letter on the input then the probability of getting a letter b on the output is given by

$$P(b|a) = \frac{\epsilon}{q-1}(1 - \delta_{a,b}) + (1-\epsilon)\delta_{a,b}$$

for some fixed $\epsilon \in [0, (q-1)/q]$. Suppose that at the receiving end the code is used for error detection. Namely, the received vector $\mathbf{y}$ is tested for containment in C, and if the test fails, the decoder "detects an error." The probability that the error will be missed (not detected) is then given by $P_{ue}(C, \epsilon)$.

Therefore, we can formulate the following proposition.

Proposition 1

$$\mathrm{Rel}(M,p) \le (1+p(q-1))^n P_{ue}\Big(C(M), \frac{p(q-1)}{1+p(q-1)}\Big) + f_k p^{n-k}(1-p)^k. \tag{12}$$

Proof : By Theorem 5 we have

$$P_{ue}(C(M),\epsilon) = (1-\epsilon)^n \sum_{i=1}^{n} \mathcal{A}_i p^i \ge (1-\epsilon)^n [\mathrm{Rel}(M,p) - f_k p^{n-k}(1-p)^k],$$

where $p = \epsilon/(q-1)(1-\epsilon)$. ∎

In the context of information transmission one assumes that $\epsilon \in [0,(q-1)/q]$ since for greater ϵ the probability of undetected error is usually close to 0. Then p varies in the entire segment $[0,1]$; so inequality (12) covers all the interval of values of p.

Among the problems that present interest in coding theory are the behavior of $P_{ue}(C,p)$ for a given code (for instance, the question whether $P_{ue}(C,p)$ is monotone in p, and if not, what is the number of its maxima), and absolute bounds on P_{ue}. More specifically, let

$$P_{ue}(n,R,p) = \min_{C\in\mathbb{F}_q^n, |C|=q^{nR}} P_{ue}(C,p)$$

be the smallest possible probability of undetected error over linear codes of fixed length n and size q^{nR}. A number of lower and upper bounds on $P_{ue}(n,R,p)$ are known in the literature; see [12]. Together with Proposition 1 and the obvious $U_k^k \le \binom{n}{k}$ this enables us to formulate bounds on the reliability polynomial. For simplicity let us put $q=2$. Let

$$\mathrm{Rel}(n,k,p) = \min_{\substack{M \text{ is a linear matroid on } E \\ |E|=n, \mathrm{rk}\, E=k}} \mathrm{Rel}(M,p).$$

Proposition 2

$$\mathrm{Rel}(n,k,p) \le 2^{k-n}((1+p)^n - 1) + \binom{n}{k} p^{n-k}(1-p)^k \tag{13}$$

$$\mathrm{Rel}(n,k,p) \le (1+p)^n \Big(\frac{2^k-1}{2^n-1}\Big[\frac{(p^u+(1+p)^u)^n}{(1+p)^{nu}} - (1+p)^{-un}\Big]\Big)^{\frac{1}{u}} + \binom{n}{k} p^{n-k}(1-p)^k \quad (0<u\le 1). \tag{14}$$

Proof : Follows upon substituting in (12) known bounds on P_{ue}, those of [13] and [14], respectively. ∎

Note that (13) is the special case of (14) for $u=1$. Although the quantity $\mathcal{A}(1,p)$ includes many more (nonnegative) terms than $\mathrm{Rel}(M,p)$, the estimates of the last proposition are nontrivial for some values of the rank k and of p. To see this, let $n\to\infty, k=Rn$, $0<R<1$. Let us rewrite (13) as follows:

$$\mathrm{Rel}(n,nR,p) \lesssim 2^{-n\min[1-R-\log_2(1+p), D(R\|1-p)]}$$

where

$$D(x\|y) = x\log_2(x/y) + (1-x)\log_2(1-x)/(1-y).$$

Thus for large n the estimate (13) is nontrivial if $p < 2^{1-R} - 1$, and roughly the same holds true for (14).

Because of the connection to linear codes the problem of bounding $P_{ue}(n, R, p)$ generally seems easier than that of bounding $\mathrm{Rel}(n, k, p)$. However, the exact asymptotic behavior of $P_{ue}(n, R, p)$ is also not known, let alone the exact value of P_{ue} for finite n, k.

3.3 Lower bounds

Results from coding theory can be also used to derive lower bounds on $\mathrm{Rel}(M, p)$. Let us quote a result from [10].

Proposition 3 *Let M be a binary matroid of rank k on the ground set of size n and suppose that the distance of the code $C(M)$ is d. Then $f_k \geq 2^{\dim(k,d)}$, where $\dim(k, d)$ is the minimum dimension of a binary linear code of length k and dual distance d.*

Together with known bounds on the minimal dimension of linear codes of given length and dual distance [15] this gives lower bounds on f_k and hence also on $\mathrm{Rel}(M, p)$ since $\mathrm{Rel}(M, p) \geq f_k p^{n-k}(1-p)^k$.

Note that it is easy to understand the average behavior of the coefficients f_i if the code is chosen randomly with uniform probability from the ensemble of linear codes. This amounts to a study of coranks of submatrices of a random matrix, which is a fairly standard subject in the study of linear codes; see, e.g., [10]. A similar technique was used in the study of the average, over the ensemble of linear codes of given length and dimension, probability of undetected error [12, Sect 3.2].

4 The partition function of the Potts model

Let $\Gamma = (V, E)$ be a finite graph with $|E(\Gamma)| = n$ edges and $c(E)$ connected components. Consider the Potts model of interaction for a physical system represented by Γ [5], [24]. Under this model each vertex in $V(\Gamma)$ can be in one of q possible states; an allocation of states to all the vertices defines a state σ of the system or a coloring of $V(\Gamma)$ with q colors. Two adjacent vertices interact with nonzero energy when they have the same color; the interaction energy is equal to a constant $-J$ independent of the specific pair of vertices. Thus, the Hamiltonian of a state σ, or its total energy, equals $H(\sigma) = -J|U(\sigma)|$, where $U(\sigma)$ is the subset of edges with both ends of the same color. The *partition function* of the model is defined as $Z = \sum_\sigma e^{-H(\sigma)/kT}$, where k is the Boltzmann constant and T is the temperature. Under random interaction, the probability of finding the system in a state σ equals $\exp(-H(\sigma)/kT)/Z$.

Letting $y = e^{-J/kT}$, we can rewrite Z as a rational function of y as follows:

$$Z(y) := \sum_\sigma y^{-|U(\sigma)|}.$$

We intend to relate $Z(y)$ to the cocycle code of Γ. Let q be a prime power, and consider the representation of the cycle matroid $M(\Gamma)$ over the field $\mathbb{F}_q$ by the columns of a matrix $\mathbf{G}$. The *cocycle code* $C(\Gamma)$ [9] is the row space of $\mathbf{G}$. The length of $C(\Gamma)$ equals n, the dimension is $|V| - c(E)$.

The main result of this section is given in the following theorem.

Theorem 6 *Let $\mathcal{A}(x,y)$ be the weight polynomial of $C(\Gamma)$. Then*

$$\mathcal{A}(1,y) = q^{-c(E)} y^n Z(y)$$

Proof : We have the following chain of equalities:

$$\begin{aligned}
Z(y) = \sum_{\sigma} y^{-|U(\sigma)|} = \sum_{\sigma} \Big(1 + \frac{1-y}{y}\Big)^{|U(\sigma)|} &= \sum_{\sigma} \sum_{F \subseteq U(\sigma)} (1-y)^{|F|} y^{-|F|} \\
&\stackrel{(a)}{=} \sum_{F \subseteq E} (1-y)^{|F|} y^{-|F|} q^{c(F)} = \sum_{i=0}^{n} (1-y)^i y^{-i} \sum_{|F|=i} q^{c(F)} \\
&\stackrel{(b)}{=} \sum_{i=0}^{n} (1-y)^i y^{-i} \sum_{|F|=i} q^{|V|-\mathrm{rk}(\mathbf{G}(F))} \\
&\stackrel{(c)}{=} q^{c(E)} \sum_{i=0}^{n} (1-y)^i y^{-i} \sum_{|F|=i} |C^F| \\
&\stackrel{(d)}{=} q^{c(E)} \sum_{j=0}^{n} (1-y)^{n-j} y^{-(n-j)} \mathcal{B}_j \\
&\stackrel{(e)}{=} q^{c(E)} y^{-n} \mathcal{A}(1,y),
\end{aligned}$$

where $c(F)$ is the number of connected components in the subgraph (V,F) formed on the vertices of Γ by the edges in F. Here (a) follows by counting in two ways the size of the set

$$\big\{(F,\sigma) \mid F \subseteq E, \text{ connected components of } (V,F) \text{ are monochromatic}\big\};$$

in (b) we use the fact that the cocycle rank of the graph (V,F) equals $\mathrm{rk}(\mathbf{G}(F)) = |V| - c(F)$; (c) follows by Lemma 1(i); (d) relies on (3), and (e) is implied by the first equality in (5). ∎

Together with Theorem 1 this theorem implies the relation between the Tutte polynomial and the function Z, which is, of course, a well-known fact [11], [24, p.64]. Therefore, although Theorem 6 was not explicitly stated in the literature, it can be deduced from Greene's theorem.

Theorem 2 enables us relate $Z(y)$ to the rank polynomial of $C(M)$ as follows:

$$Z(y) = q^{|V|} \mathcal{U}\Big(\frac{1-y}{y}, \frac{1}{q}\Big).$$

This implies an interpretation of the coefficients of $Z(y)$ in terms of the number of subsets of E of a given size and rank, and, in particular, of the number f_i of independent subsets of size i.

Further connections between spin models and combinatorial theory of codes (theory of association schemes) are covered in the survey [18].

5 Concluding remark

The results of this paper can be extended from linear matroids to a somewhat broader class of almost affine matroids introduced in [22]. To define almost affine representability of a matroid M

with the rank function ρ on the ground set E of size n, consider a $N \times n$ matrix D with entries from a finite set of size q. As above, for $F \subseteq E$ let $D(F)$ be the submatrix of D formed by columns with numbers in F. Let

$$r(F) = \log_q |\{\text{number of different rows in } D(F)\}|.$$

We say that M is almost affinely represented by D if $r(F)$ is integer for every $F \subseteq E$ and $\rho F = r(F)$ for every $F \subseteq E$. A matroid is called *almost affine* if it allows of an almost affine representation. Linear matroids form a subset of the class of almost affine matroids; as proved in [22], this inclusion is proper.

References

[1] A. Ashikhmin, A. Barg, and S. Litsyn, *Estimates of the distance distribution of codes and designs*, IEEE Trans. Inform. Theory **47** (2001), no. 3, 1050–1061.

[2] ———, *Estimates of the distance distribution of nonbinary codes, with applications*, Codes and Association Schemes (A. Barg and S. Litsyn, eds.), Providence, R.I.: AMS, 2001, pp. 287–303.

[3] A. Barg, *The matroid of supports of a linear code*, Appl. Alg. Engrg. Commun. Comput. **8** (1997), 165–172.

[4] A. Barg and A. Ashikhmin, *Binomial moments of the distance distribution and the probability of undetected error*, Des. Codes Cryptogr. **16** (1999), no. 2, 103–116.

[5] N. L. Biggs, *Interaction models*, London Math. Soc. Lect. Notes, vol. 30, Cambr. Univ. Press, 1977.

[6] T. H. Brylawski and J. G. Oxley, *The Tutte polynomial and its applications*, Matroid Applications (N. White, ed.), Encyclopedia of Mathematics and its Applications, vol. 40, Cambridge Univ. Press, Cambridge, 1992, pp. 123–225.

[7] C. J. Colbourn and D. D. Harms, *Bounding all-terminal reliability in computer networks*, Networks **18** (1988), 1–12.

[8] C. Greene, *Weight enumeration and the geometry of linear codes*, Stud. Appl. Math. **55** (1976), 119–128.

[9] S. L. Hakimi and J. G. Bredeson, *Graph theoretic error-correcting codes*, IEEE Trans. Inform. Theory **14** (1968), 584–591.

[10] T. Helleseth, T. Kløve, and V. I. Levenshtein, *On the information function of an error-correcting code*, IEEE Trans. Inform. Theory **43** (1997), no. 2, 549–557.

[11] F. Jaeger, *Tutte polynomial and link polynomials*, Proc. Amer. Math. Soc. **103** (1988), no. 2, 647–654.

[12] T. Kløve and V. I. Korzhik, *Error detecting codes*, Kluwer, Boston e. a., 1995.

[13] V. I. Korzhik, *Bounds on the probability of undetected error and optimum group codes in a channel with feedback*, Radiotechnika **20** (1965), no. 1, 27–33, (In Russian). English translation in *Telecommun. Radio Eng.*, **20** (1, pt.2) (1965), 87–92.

[14] V. I. Levenshtein, *Bounds on the probability of undetected error*, Problemy Peredachi Informatsii **13** (1977), no. 1, 3–18.

[15] ———, *Krawtchouk polynomials and universal bounds for codes and designs in Hamming spaces*, IEEE Trans. Inform. Theory **41** (1995), no. 5, 1303–1321.

[16] F. J. MacWilliams, *A theorem in the distribution of weights in a systematic code*, Bell Syst. Techn. Journ. **42** (1963), 79–94.

[17] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, 3 ed., North-Holland, Amsterdam, 1991.

[18] K. Nomura, *Spin models and Bose-Mesner algebra*, Europ. J. Combinatorics **20** (1999), 691–700.

[19] V. Pless and W. C. Huffman (eds.), *Handbook of coding theory, vol. 1,2*, Elsevier Science, Amsterdam, 1998, 2169pp.

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

[21] J. Simonis, *The effective length of subcodes*, Appl. Alg. Engrg. Commun. Comput. **5** (1994), 371–377.

[22] J. Simonis and A. Ashikhmin, *Almost affine codes*, Des. Codes Cryptogr. **14** (1998), no. 2, 179–197.

[23] D. J. A. Welsh, *Matroid theory*, Academic Press, London, 1976.

[24] ———, *Complexity: knots, colourings and counting*, LMS Lect. Notes Series, vol. 186, Cambridge Univ. Press, 1993.