DIMACS Technical Report 99-54

On polynomial invariants of linear codes, matroids, and finite interaction models

by

Alexander Barg [1]

[1]Bell Labs, Lucent Technologies, 600 Mountain Ave., Murray Hill, NJ 07974.

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 relate the weight polynomial of codes and the reliability polynomial of linear matroids and to prove new bounds on the latter;
- to prove that the partition polynomial of the Potts model equals the weight polynomial of the cocycle code of the underlying graph, and
- to give a simple proof of Greene's theorem and its generalization.

1 Introduction

A linear matroid M together with a chosen representation 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 underlie all the results in the paper, including the main results mentioned in the abstract. In particular, they 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; we show that this theorem does not require any of the standard tools such as Tutte-Grothendieck invariants or recursive computation of the Tutte polynomial. An advantage of the coding-theoretic point of view is determined by the fact that the weight polynomial enjoys more structural properties than 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. This enables us to derive upper and lower bounds on the matroid reliability. As another application of the weight-rank connection, we prove, somewhat surprisingly, that the partition function of the Potts model is equal to the weight polynomial of the cocycle code of the graph. We conclude by returning to codes and showing that certain generalizations of the weight polynomial fall naturally in the general pattern of the paper.

Coding-theoretic concepts are perhaps the least standard of all the material in the paper. General sources for coding theory are the books [37], [39]. Graph-theoretic codes were introduced in [23], [22]. They are relatively well understood from the coding point of view; see a summary in [29]. Relevant applications of the Tutte polynomial are covered in [13], [47]. All the necessary information on interaction models is contained in [47] or, on a more general level, in [9]. Coding-theoretic part of this paper is a development of ideas in [2], [5], [7], [40]. Specific references for other parts are given below.

2 The rank polynomial of the code

We begin with some definitions and simple properties of linear codes. A *linear code* C is an arbitrary linear subspace of $\mathbb{F}_q^n$. The number n is called the length of C. Let $\mathcal{A}_i$ be the number of vectors of Hamming weight i in it, $0 \le i \le n$. Clearly, $\mathcal{A}_0 = 1$. Minimal $i \ge 1$ 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 the *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, $\dim C_F = \mathrm{rk}(\mathbf{G}(F))$. The following lemma collects some basic linear-algebraic facts on these subcodes.

Lemma 1:

(i) $\quad C_F \cong C/C^{\bar{F}}$; $\quad \dim C_F = k - \dim C^{\bar{F}}$

(ii) $\quad \dim C^F = |F| - \mathrm{rk}(\mathbf{H}(F))$

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

Theorem 2:

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

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

$$\sum_{i=0}^{w} \binom{n-i}{n-w} \mathcal{A}_i = \sum_{|F|=w} |C^F| = \sum_{|F|=w} q^{k-\mathrm{rk}(\mathbf{G}(\bar{F}))} \tag{2}$$

$$= \sum_{u=0}^{k} q^{k-u} \mathcal{U}_{n-w}^{u} \quad (0 \le w \le n). \tag{3}$$

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

$$\mathcal{A}(x,y) = \sum_{w=0}^{n} \mathcal{C}_w (x-y)^{n-w} y^w = \sum_{w=0}^{n} \sum_{u=0}^{k} q^{k-u} \mathcal{U}_{n-w}^{u} (x-y)^{n-w} y^w \tag{4}$$

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

∎

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 motivation of the present study lies in the fact that polynomial invariants of matroids generally capture a finer combinatorial structure than the weight polynomial of codes and enable us to connect the latter to polynomial invariants of other objects. 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 (see, e.g., the next section).

The rank polynomial of C, essentially, is an invariant of M. Another matroid invariant that appears in numerous contexts in combinatorics, is the *Tutte polynomial* of M, defined as follows[1]:

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

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

Theorem 3: (Greene [21])

$$\mathcal{A}(x,y) = y^{n-k}(x-y)^k \mathcal{T}\Big(M; \frac{x+(q-1)y}{x-y}, \frac{x}{y}\Big). \tag{5}$$

[1]The matroid M is usually listed as one of the arguments of $\mathcal{T}$. To be consistent, one should write the weight polynomial as $\mathcal{A}(C;x,y)$, but the tradition rules otherwise.

The proof, as given in [21] and reproduced in [46], [13], 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. The same line of thought is addressed again in [14].

To give a more direct proof note that Theorem 2 already relates $\mathcal{A}(x,y)$ to a polynomial with coefficients $\mathcal{U}_u^v$. Therefore, Theorem 3 should be a mere reformulation of (1), which it is.

Proof of Theorem 3: Starting with the definition of $\mathcal{T}$, we obtain

$$\begin{aligned} y^{n-k}(x-y)^k\mathcal{T}\Big(M;\frac{x+(q-1)y}{x-y},\frac{x}{y}\Big) \\ &= y^{n-k}(x-y)^k\sum_{u=0}^{n}\sum_{v=0}^{k}\mathcal{U}_u^v\Big(\frac{qy}{x-y}\Big)^{k-v}\Big(\frac{x-y}{y}\Big)^{u-v} \\ &= y^nq^k\mathcal{U}\Big(\frac{x-y}{y},\frac{1}{q}\Big). \end{aligned}$$

∎

Eq.(2) together with Lemma 1(ii) also enables us to relate the weight polynomial of C and the rank polynomial of $C^\perp$, denoted $\mathcal{U}^\perp(x,y)$. The following identities are implicit in [36], [40], and explicit in [7].

Theorem 4:

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

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

Both Greene [21] and references [46], [13], [14] then go on to use Theorem 3 together with the duality for Tutte polynomials to derive the MacWilliams theorem on the relation of $\mathcal{A}(\cdot,\cdot)$ and $\mathcal{A}^\perp(\cdot,\cdot)$. The MacWilliams equation has the form [36]

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

Under the approach of this section, the last equation, Theorem 3, and Tutte's duality are all contained in Theorem 2.

Equating coefficients in (8) we obtain the following set of MacWilliams identities:

$$\mathcal{A}_i^\perp = \frac{1}{|C|}\sum_{j=0}^{n}\mathcal{A}_jK_i(j), \quad (0\le i\le n)$$

where $K_i(j) := \sum_{\alpha=0}^{n}(-1)^{\alpha}(q-1)^{i-\alpha}\binom{j}{\alpha}\binom{n-j}{i-\alpha}$ is the *Krawtchouk number.* Since $\mathcal{A}_i^{\perp} \geq 0$, this gives a set of nonnegativity conditions on the weight coefficients of C, known in coding theory as the Delsarte inequalities [19], which prove surprisingly useful in many coding-theoretic problems. One of the most far-reaching applications is using them as a part of the linear programming problem

$$\{ \max \sum_{i=1}^{n} \mathcal{A}_i \mid \sum_{j=1}^{n} \mathcal{A}_j K_i(j) \geq -1,\ 0 \leq j \leq n \} \tag{9}$$

with respect to n nonnegative integer variables $\mathcal{A}_i$ to bound the maximum possible size of the linear code $|C| = 1 + \sum_{i=1}^{n} \mathcal{A}_i$ or to prove nonexistence of codes [10]. Therefore, it seems worthwhile to remark that (3) implies the following nonnegativity conditions for the rank coefficients of M:

$$\sum_{w=0}^{i}(-1)^{n-w}\binom{n-w}{n-i}\sum_{u=0}^{k} q^{k-u}\mathcal{U}_{n-w}^{u} \geq 0, \quad 0 \leq i \leq n. \tag{10}$$

3 The reliability polynomial of matroids

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

$$\mathcal{R}(M; x, y) := \sum_{i=0}^{k} f_i x^{n-i} y^i \tag{11}$$

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 $\mathrm{Rel}(M, p) := \mathcal{R}(M; p, 1-p)$.

The polynomial $\mathcal{R}(M; x, y)$ can be written in a number of different forms [17], [12] which involve coefficients of generating functions of the number of various objects in M, connected by relations similar to those of the previous section. For instance, the reliability polynomial is related to the Tutte polynomial by the following obvious identity: $\mathcal{R}(M; x-1, 1) = \mathcal{T}(M; x, 1)$. So we obtain

$$\mathrm{Rel}(M, p) = p^{n-k}\sum_{i=0}^{k} h_i (1-p)^i,$$

where the coefficients $\left(h_i = \sum_{v=0}^{i}(-1)^{i-v}\binom{k-v}{k-i}f_v,\ 0 \le i \le k\right)$ form the so-called *h-vector* of M. Below we work with the form (11) (called the *f-form* of $\mathrm{Rel}(M,p)$) since it fits in with the framework introduced above.

The reliability polynomial of networks was introduced in [38] and has been a subject of study in combinatorics ever since. A survey of its properties is given in [17]; its connections to matroid invariants are examined in [11],[44], among others. 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 such as the size of fundamental cocircuits, etc. The aim of this section is to use results from coding theory to derive absolute bounds on $\mathrm{Rel}(M,p)$. Let us introduce the quantity

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

Let $\mathcal{A}(x,y)$ be the weight polynomial of the linear code $C(M)$. Unfortunately, $\mathrm{Rel}(M,p)$ is not directly expressible via $\mathcal{A}(\cdot,\cdot)$, but one can relate them by the following inequality.

Theorem 5:

$$\mathrm{Rel}(M,p) \le \mathcal{U}_k^k p^{n-k}(1-p)^k + \mathcal{A}(1,p) - 1. \tag{12}$$

Proof. We have

$$\begin{aligned} -\mathcal{U}_k^k p^{n-k}(1-p)^k + \mathrm{Rel}(M,p) &= \sum_{i=0}^{k-1} \mathcal{U}_i^i p^{n-i}(1-p)^i \\ &\le \sum_{i=0}^{k-1} p^{n-i}(1-p)^i \sum_{u=0}^{k}(q^{k-u}-1)\mathcal{U}_u^i \\ &= \sum_{w=n-k+1}^{n} p^w(1-p)^{n-w}\sum_{u=0}^{k}(q^{k-u}-1)\mathcal{U}_{n-w}^u \\ &\le \sum_{w=1}^{n} p^w(1-p)^{n-w}\sum_{u=0}^{k}(q^{k-u}-1)\mathcal{U}_{n-w}^u, \end{aligned} \tag{13}$$

where the first inequality holds true because $\mathcal{U}_s^s \le \sum_{u=0}^{k}(q^{k-u}-1)\mathcal{U}_s^u$ for any $0 \le s \le k-1$[2].

[2] For $s = k$ this fails, for instance, for the uniform matroid of rank k.

Now proceeding as in (2), (4) we see that

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

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

(see also [7]). Therefore, continuing from (13), we obtain

$$\mathrm{Rel}(M,p) \le \mathcal{U}_k^k p^{n-k}(1-p)^k + \sum_{i=1}^{n}\mathcal{A}_i p^i.$$

This completes the proof. ∎

To derive specific bounds on the reliability of linear matroids, we thus need bounds on evaluations of $\mathcal{A}(x,y)$. These were studied in coding theory in the context of error detection. More specifically, given a 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 problem related to information transmission. Suppose a q-ary code C is used to send messages over a symmetric channel with crossover probability ϵ. This means that each transmitted symbol is independently subjected to the following error process: it is received error-free with probability $1-\epsilon$ and changed in the channel to another symbol with probability $\epsilon/(q-1)$. 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." Such a decoding may be weak in the sense that it does not use the full correcting power of the code. On the other hand, it is computationally very simple; indeed, it can be accomplished by multiplying $\mathbf{y}$ by the parity-check matrix $\mathbf{H}$.

Under these assumptions the probability that for a given code C an error in the channel is not detected at the receiving end equals $P_{ue}(C,\epsilon)$. Therefore, we can formulate the following proposition.

Proposition 6:

$$\mathrm{Rel}(M,p) \le (1+p(q-1))^n\Big[P_{ue}\Big(C(M),\frac{p(q-1)}{1+p(q-1)}\Big) + \mathcal{U}_k^k p^{n-k}(1-p)^k\Big]. \tag{14}$$

PROOF. By Theorem 5 we have

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

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 close to 0. Then p varies in the entire segment $[0,1]$; so inequality (14) 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 best 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 [30]. Together with Proposition 6 and the obvious $U_k^k\le\binom{n}{k}$ this enables us to formulate bounds on $\mathrm{Rel}(n,k,p)$, both finite and asymptotic. For simplicity we put $q=2$.

Proposition 7:

$$\mathrm{Rel}(n,k,p)\le(1+p)^n\Big[2^{k-n}(1-(1+p)^{-n})+\binom{n}{k}p^{n-k}(1-p)^k\Big] \qquad (15)$$

$$\mathrm{Rel}(n,k,p)\le(1+p)^n\Big[\Big(\frac{2^k-1}{2^n-1}\Big[\frac{(p^u+(1+p)^u)^n}{(1+p)^{nu}}-(1+p)^{-un}\Big]\Big)^{\frac{1}{u}} + \binom{n}{k}p^{n-k}(1-p)^k\Big] \quad (0<u\le 1) \qquad (16)$$

Further, let $n\to\infty$, $0<R<1$. Then

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

where

$$E(R,p)=\begin{cases} T\big(H^{-1}(1-R),\frac{p}{1+p}\big) & 0\le R\le 1-H\big(1-R,\frac{p}{1+p}\big) \quad \text{(I)}\\ 1-R & 1-H\big(1-R,\frac{p}{1+p}\big)\le R\le 1, \quad \text{(II)}\end{cases} \qquad (17)$$

where $H(u)=-u\log_2 u-(1-u)\log_2(1-u)$ and $T(u,v)=-u\log_2 v-(1-u)\log_2(1-v)$.

PROOF. Parts (15) and (16) follow upon substituting in (14) known bounds on P_{ue}, those of [31] and [33], respectively. The remaining parts follow by a standard asymptotic argument. For instance, for (17.II), computing logarithms in (15), we obtain

$$\log_2 \mathrm{Rel}(n,k,p) \lesssim n\Big\{ \log_2(1+p) + \max\Big[R-1, \log_2\binom{n}{k} \\ + (1-R)\log_2 p + R\log_2(1-p)\Big]\Big\}$$

∎

A few comments on these bounds may be in order. Generally, they should be fairly weak since the functional $\mathcal{A}(1,p)$ includes many more (nonnegative) terms than $\mathrm{Rel}(M,p)$. However for some parameters (R,p) they are nontrivial (for instance, (17.II) trivializes only for $p \ge 2^{1-R}-1$, and roughly the same holds true for (15)). It can be checked, for instance by calculating the bounds, that both terms in the minimum in the exponent are essential.

Finally, note that (15) is the special case of (16) for $u=1$.

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 (the best results to-date are given in [2],[35]), let alone the exact value of $P_{ue}(n,k/n,p)$ for finite n,k.

Turning to lower bounds, let us quote a result from [24].

Proposition 8: *Let M be a binary matroid of rank k and suppose that the dual distance of the code $C(M)$ is $d^\perp$. Then $f_k \ge 2^{\dim(k,d^\perp)}$, where the exponent is the minimum dimension of a binary linear code of length k and dual distance $d^\perp$.*

Together with known bounds on the minimal dimension of linear codes of given length and dual distance [34] this gives absolute lower bounds on f_k and hence also on $\mathrm{Rel}(M,p)$ since $\mathrm{Rel}(M,p) \ge f_k p^{n-k}(1-p)^k$.

For some special classes of codes information on the f-numbers can be derived from their structural properties. Let C be a binary code of minimum distance $d(C) \ge 3$. Let

$$\mathcal{M}_i := \big\{\mathbf{c} \in C \mid \mathrm{wt}(\mathbf{c}) = i,\ \mathrm{supp}(\mathbf{c}) \text{ is a circuit in } M(C^\perp)\big\}.$$

A code vector $\mathbf{c} \in C$ whose support is a circuit in $M(C^\perp)$ is called a *minimal vector* of C. Thus, the support of a minimal vector $\mathbf{c}$ gives rise to an independent subset of $M(C^\perp)$ of size $|\mathrm{supp}(\mathbf{c})|-1$; the converse is generally not true – many independent subsets correspond to no minimal vectors of C. However because of the condition on the distance of C no independent subset gives rise to more that one minimal vector. Thus $f_i(M(C^\perp)) \ge \mathcal{M}_{i+1}$; this gives lower bounds on $\mathrm{Rel}(M(C^\perp),p)$.

Example. Let $n = 2^m, m \geq 4$, and consider the matrix G with rows given by incidence vectors of all $(m-2)$-flats in the affine geometry $A_m(\mathbb{F}_2)$. The row space of this matrix forms the Reed–Muller code of the 2nd order, denoted $R(2,m)$ [3]. The dimension of this code equals $1 + m + \binom{m}{2}$; its distance is 2^{m-2}. Its dual code $C^\perp$ is a Reed–Muller code of order $m-3$ with $D^\perp = 8$ [3]. The distribution of minimal vectors in C for $1 \leq i \leq \dim(C^\perp) + 1$ was computed in [1] (the formulas are too cumbersome to be reproduced here). This gives a lower bound on the reliability of $M(C^\perp)$.

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 [1], [6]. 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 [32], [30, Sect 3.2].

An interesting recent result in the frame of network reliability is the following set of positivity conditions discovered in [11]; see also [15], [16].

Theorem 9: *Let* $\operatorname{el} C^\perp = n$. *Then*

$$\sum_{i=0}^{j} \sum_{v=0}^{i} (-1)^v b^i \binom{k-v}{k-i} U_v^v \geq 0, \quad (0 \leq j \leq k) \tag{18}$$

where $b \geq 1$ *is an arbitrary real number.*

It seems that the set of inequalities (18) is independent of the Delsarte inequalities (10). In conjunction with the linear-programming problem (9) this should in principle lead to new coding-theoretic results. Indeed, it is easy to rewrite problem (9) in terms of the rank coefficients. The objective function (the size of a $q-ary$ code of length n and dimension k with $\operatorname{el} C^\perp = n$) has the form

$$\max \sum_{w=0}^{n} (-2)^{n-w} \sum_{u=0}^{k} q^{k-u} \mathcal{U}_{n-w}^u \qquad (\mathcal{U}_w^u \geq 0, 0 \leq u \leq w \leq n,\ \mathcal{U}_w^0 = \delta_{w,0})$$

subject to resrictions (10), (18). If we assume that $\operatorname{el}(C) = n$, then $\mathcal{U}_0^u = \delta_{u,0}$, and the total number of nonzero variables equals $1 + k(k+1)/2 + (n-k)k$. On the other hand, (18) can obviously be used as a set of restrictions in a linear program with the objective function $\operatorname{Rel}(n,k,p)$.

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 [9], [47].

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. The importance of this function is determined by the fact that, under random interaction, it plays a role of the normalizing factor; namely, 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 G. The *cocycle code* $C(\Gamma)$ [22] is the row space of G. The matrix G has n columns; assuming that its rows are linearly independent, their number is $|V| - c(E)$.

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

Theorem 10: *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:

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

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 (2), and (e) is implied by the first equality in (4). ∎

Together with Theorem 3 this theorem implies the relation between the Tutte polynomial and the function Z, which is, of course, a well-known fact [26], [47, p.64]. This relation enables one to define the partition function for matroids [43]; in the linear case the preceding argument would imply, if somewhat tautologically, that this function is again the weight enumerator of the code.

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, which is a result in [43].

Developing the motif of this section further, one could look at the relation of the weight polynomial and link invariants since the latter are strongly related to the partition function. Particularly appealing in this context are the works of F. Jaeger ([27], [28]; see also [18]) uncovering a general relation of interaction (spin) models and the theory of association schemes, which also serves a general framework for the combinatorial theory of codes [20]. In particular, a relation of the Potts model to the Hamming scheme was examined in [4], where it was shown that spin models found in the Hamming scheme in essence cannot be anything else than the Potts model. So in retrospect something like Theorem 10 is not completely unexpected. Another parallel is Biggs's algebraic duality theorem for interaction models [8] which looks very much like a version of the Delsarte-MacWilliams duality in association schemes [20].

5 Odds and ends

Let us also mention a generalization of Theorem 3 observed in [5]. It is related to the notion of support weight distributions of linear codes introduced in [25] (it was studied widely in the 90-s following rediscovery in [45]; see a survey in [42]).

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

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

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

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, proved in [5] following the approach of [21], relates the support weight distributions of C to its Tutte polynomial.

Theorem 11:

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

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

This theorem can be derived along the lines of the present paper relying on a lemma in [40], which generalizes Lemma 3.

Lemma 12: [40]

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

Yet another way of proving Theorem 11 relies on considering the Hamming weight distribution $(\mathcal{A}_i^{C^{(r)}}, 0 \le i \le n)$ of the code $C^{(r)} := \mathbb{F}_{q^r} \otimes C$ (as $\mathbb{F}_q$-modules). By a result in [25], $\mathcal{A}_i^{C^{(r)}} = \sum_{m=0}^{r} [r]_m \mathcal{A}_i^m$, and so Theorem 11 is implied by Theorem 3.

Note that the results of this paper can be extended from linear matroids to a somewhat broader class of almost affine matroids introduced in [41]. 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 [41], this inclusion is proper.

Let D be the matrix that represents, almost affinely, a given matroid M. The rows of D form a subset of $\{1, \dots, q\}^n$ called an almost affine code C. As usual in coding theory, one can introduce the set of local distance polynomials of this code as follows:

$$A_{\mathbf{c}}(x, y) = \sum_{i=0}^{n} A_{i,\mathbf{c}} x^{n-i} y^i \quad (\mathbf{c} \in C),$$

where $A_{i,\mathbf{c}} = |\{\mathbf{c}' \in C \,:\, \mathrm{dist}(\mathbf{c}, \mathbf{c}') = i\}|$. One of the results in [41] shows that the $A_{\mathbf{c}}(x, y)$ does not depend on $\mathbf{c}$ and satisfies the same properties as the weight polynomial of linear codes. Consequently, it is also connected to the Tutte and reliability polynomials of M by the same relations as above.

References

[1] A. Ashikhmin and A. Barg, *Minimal vectors in linear codes*, IEEE Trans. Inform. Theory **44** (1998), no. 5, 2010–2017.

[2] ———, *Binomial moments of the distance distribution: Bounds and applications*, IEEE Trans. Inform. Theory **45** (1999), no. 2, 438–452.

[3] E. F. Assmus, Jr. and J. D. Key, *Designs and their codes*, Cambridge Tracts in Mathematics, vol. 103, Cambr. Univ. Press, Cambridge, 1992.

[4] E. Bannai, E. Bannai, T. Ikuta, and K. Kawagoe, *Spin models constructed from the Hamming association schemes*, Proc. 10th Algebraic Combin. Sympos., Gifu Univ., 1982, pp. 91–106.

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

[6] ———, *Complexity issues in coding theory*, Handbook of Coding Theory (V. Pless and W. C. Huffman, eds.), vol. 1, Elsevier Science, Amsterdam, 1998, pp. 649–754.

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

[8] N. L. Biggs, *On the duality of interaction models*, Math. Proc. Cambridge Philos. Soc. **80** (1976), 429–436.

[9] ———, *Interaction models*, London Math. Soc. Lect. Notes, vol. 30, Cambr. Univ. Press, 1977.

[10] A. E. Brouwer, *The linear programming bound for binary linear codes*, IEEE Trans. Inform. Theory **39** (1993), no. 2, 677–680.

[11] J. I. Brown and C. J. Colbourn, *Roots of the reliability polynomial*, SIAM J. Discrete Math. **5** (1992), no. 4, 571–585.

[12] ———, *Non-Stanley bounds for network reliability*, J. Alg. Combin. **5** (1996), 13–36.

[13] 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.

[14] P. J. Cameron, *Notes on matroids and codes*, unpublished, 1998.

[15] M. K. Chari, *Matroid inequalities*, Discrete Mathematics **147** (1995), 283–286.

[16] ———, *Two decompositions in topological combinatorics with applications to matroid complexes*, Trans. Amer. Math. Soc. **349** (1997), no. 10, 3925–3943.

[17] C. J. Colbourn, *The combinatorics of network reliability*, Oxford Univ. Press, New York, 1987.

[18] P. de la Harpe, *Spin models for link polynomials, strongly regular graphs and Jaeger's Higman-Sims model*, Pacific J. Math. **187** (1994), no. 1, 57–96.

[19] P. Delsarte, *Bounds for unrestricted codes, by linear programming*, Philips Res. Rep. **27** (1972), 272–289.

[20] P Delsarte, *An algebraic approach to the association schemes of coding theory*, Philips Research Repts Suppl. **10** (1973), 1–97.

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

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

[23] S. L. Hakimi and H. Frank, *Cut set matrices and linear codes*, IEEE Trans. Inform. Theory **11** (1965), 457–458.

[24] 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.

[25] T. Helleseth, T Kløve, and J. Mykkeltveit, *The weight distribution of irreducible cyclic codes with block lengths* $n_1((q^l-1)/n)$, Discrete Mathematics **18** (1977), 179–211.

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

[27] ———, *On spin models, triply regular association schemes, and duality*, J. Algebraic Combin. **4** (1995), 103–144.

[28] ———, *Spin modesl for link invariants*, Surveys in Combinatorics (P. Rowlinson, ed.), London Math. Soc. Lect. Notes, vol. 218, Cambr. Univ. Press, 1995, pp. 71–101.

[29] D. Jungnickel and S. A. Vanstone, *Graphical codes revisited*, IEEE Trans. Inform. Theory **43** (1997), no. 1, 136 – 146.

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

[31] 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.

[32] V. K. Leontiev, *Error detecting encoding*, Problemy Peredachi Informatsii **3** (1972), no. 1, 6–14.

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

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

[35] S. Litsyn, *New upper bounds on error exponents*, IEEE Trans. Inform. Theory **45** (1999), no. 2, 385–398.

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

[37] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland, Amsterdam, 1993.

[38] E. F. Moore and Shannon C. E., *Reliable circuits using less reliable components*, Journ. Franklin Instit. **262** (1956), 191–208 and 281–297.

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

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

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

[42] M. A. Tsfasman and S. G. Vlăduţ, *Geometric approach to higher weights*, IEEE Trans. Inform. Theory **41** (1995), 1564–1588.

[43] D. G. Wagner, *The Tutte dichromate and Whitney homology of matroids*, preprint.

[44] ———, *Zeros of reliability polynomials and f-vectors of matroids*, preprint.

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

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

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