The Tutte Polynomial and Linear Codes

Linear Codes

A **linear code** over $GF(q)$ is a k-dimensional subspace of the vectorspace $GF(q)^n$. We call k the **dimension** of the code and n the **length** of the code. Codes are normally denoted C.

A linear code of length n and dimension k is called a $[n, k]$-code.

If G is a $r \times n$ matrix over $GF(q)$, whose rows form a basis for C, then G is a **generator matrix** for C. As with every matrix, there is an associated matroid, which in this case depends only on C. Hence the matroid is $M(C)$.

The **dual code**, C^*, of C, is defined by $C^* = \{\mathbf{v} \in GF(q)^n | \mathbf{v} \cdot \mathbf{w} = 0 \ \forall \mathbf{w} \in C\}$. If C is a $[n, k]$-code, then C^* is a $[n, n-k]$-code. Furthermore, $M(C^*) \cong M^*(C)$ [White (1986)]

The members of a linear code are called **codewords**. If $\mathbf{v}$ is the codeword $(v_1, \ldots, v_n)$, then the **weight** of $\mathbf{v}$ is $w(\mathbf{v}) = |\{i | v_i \neq 0\}|$.

The **distance** of C, denoted $d(C)$, is $\inf_{\mathbf{v} \in C - 0} \{w(\mathbf{v})\}$. It should be obvious that d is the size of a smallest bond in $M(C)$, or the size of a smallest circuit in $M^*(C)$.

The Codeweight Polynomial

If W is a subspace of $GF(q)^n$, then W_0 will denote the subspace consisting of those vectors in W whose first entry is 0. $\widehat{W}$ will denote the vectorspace obtained from W by removing the first entry of every vector. By convention, $\widehat{W_0} = \widehat{W}$ where $W = W_0$.

For a linear code C, the **codeweight polynomial** $A(C; q, z)$ of C is defined by

$$A(C; q, z) = \sum_{\mathbf{v} \in C} z^{w(\mathbf{v})}$$

Thus, if a_i is the number of codewords in C having weight i, then

$$A(C; q, z) = \sum_{i=0}^{n} a_i z^i.$$

Theorem 1 (Greene, 1976)**.**

$$A(C; q, z) = (1-z)^k z^{n-k} T\left(M(C); \frac{1 + z(q-1)}{1-z}, \frac{1}{z}\right).$$

Proof. Let $f(M(C)) = A(C; q, z)$. We will show that f is well defined and that it is a TG-invariant, for which $a = z$ and $b = 1 - z$. Firstly, f is well defined if C has length 1, as then

$$f(M(C)) = \begin{cases} 1, & \text{if } M(C) \text{ is a loop,} \\ 1 + z(q-1), & \text{if } M(C) \text{ is a coloop.} \end{cases}$$

Assume that f is well-defined if C has length strictly less than m, and suppose that C has length m, where $m \geq 2$.

Let G be a generator matrix for C and suppose that $e \in M(C)$ is not a loop or a coloop. WOLOG, we may assume that e corresponds to the first column of G. Let G' be the matrix obtained by applying standard row operations to G so that $G'_{1,1} = 1$ and $G'_{i,1} = 0$, for all $i \neq 1$. Clearly, G' is also a generator matrix for C. From the matrix G', we can deduce that

$$M(\widehat{C}_0) = M(C)/e \qquad \text{and} \qquad M(\widehat{C}) = M(C)\backslash e \tag{1}$$

Now consider the map $g : C - C_0 \longrightarrow \widehat{C} - \widehat{C}_0$, that removes the first entry of each codeword, that is, $g((v_1, \mathbf{v}')) = \mathbf{v}'$. If $(v_1, \mathbf{v}')$ and $(u_1, \mathbf{v}')$ are both in C, for $v_1 \neq u_1$, then $(v_1 - u_1, \mathbf{v}') \in C$. But then e is a coloop of $M(C)$, a contradiction. Hence the image of g is $\widehat{C} - \widehat{C}_0$, and g is a bijection.

By definition, $A(C) = \sum_{\mathbf{v} \in C} z^{w(\mathbf{v})}$. Therefore

$$\begin{aligned}
A(C) &= \sum_{(v_1,\mathbf{v}') \in C_0} z^{w((v_1,\mathbf{v}'))} + \sum_{(v_1,\mathbf{v}') \in C - C_0} z^{w((v_1,\mathbf{v}'))} \\
&= \sum_{\mathbf{v}' \in C_0} z^{w(\mathbf{v}')} + z \sum_{(v_1,\mathbf{v}') \in C - C_0} z^{w(\mathbf{v}')} \\
&= \sum_{\mathbf{v}' \in \widehat{C}_0} z^{w(\mathbf{v}')} + z \sum_{(v_1,\mathbf{v}') \in \widehat{C} - \widehat{C}_0} z^{w(\mathbf{v}')} \\
&= z \sum_{\mathbf{v}' \in \widehat{C}} z^{w(\mathbf{v}')} + (1-z) \sum_{\mathbf{v}' \in \widehat{C}_0} z^{w(\mathbf{v}')} \\
&= zA(\widehat{C}) + (1-z)A(\widehat{C}_0).
\end{aligned}$$

Hence, by Equation 1 and the induction assumption, if e is not a loop or a coloop of $M(C)$, then

$$A(C) = zf(M(C)\backslash e) + (1-z)(f(M(C)/e). \tag{2}$$

Now suppose that e is a loop of $M(C)$. Then $A(C) = A(\widehat{C}_0)$, so, by the induction assumption,

$$A(C) = f(\text{loop})f(M(C)/e). \tag{3}$$

Finally, suppose that e is a coloop of $M(C)$. Then C is the direct sum of $\widehat{C}$ with a one-dimensional space. Hence $A(C) = (1 + (q-1)z)A(\widehat{C})$ and so, by the induction assumption,

$$A(C) = f(\text{coloop})f(M(C)\backslash e). \tag{4}$$

Combining Equations 2 to 4, we conclude by induction that f is well defined, and is a TG-invariant. The result follows from the recipe theorem. □

Critical Exponents

The other pioneering work in matroid invariants of linear codes was by Dowling in 1971. He showed that one of the fundamental problems of coding theory – that of finding the maximum dimension for a code of fixed length and minimum distance.

The **punctured Hamming ball**, $H_q(n, d-1)$, consists of all non-zero vectors of $GF(q)^n$ with weight less than d.

It follows that C is a maximum dimension length n linear code having distance at least d if and only if C is a maximum dimension subspace of $GF(q)^n$ containing no member of $H_q(n, d-1)$. Thus the problem of maximising the dimension of a code of distance at least d is equivalent to the problem of finding the critical exponent of the vector matroid on $H_q(n, d-1)$.

Theorem 2 (Dowling, 1971)**.** *If k is the maximum dimension of a linear code over $GF(q)$ having length n and distance at least d, and c is the critical exponent of the vector matroid on $H_q(n, d-1)$, then $k = n - c$.*

Proof. Follows directly from the definition of the critical exponent – listen to Ben's talk. □

Binary Codes

This TG-invariant was discovered for graphs by Rosenstiehl & Read in 1978, and Jaeger noticed that their result could be extended to binary matroids in 1989.

Theorem 3. *Let C be a binary code of length n. Then*

$$T(M(C); -1, -1) = (-1)^n 2^{\dim(C \cap C^*)}$$

Hence

$$|T(M(C); -1, -1)| = |C \cap C^*|.$$

Proof. Let $h(M(C)) = (-1)^{n(C)} 2^{\dim(C \cap C^*)}$ where $n(C)$ is the length of C. We shall show that h is a well defined TG-invariant. First note that h is well defined if $n(C) = 1$ for, in this case, $C \cap C^* = \{\mathbf{0}\}$ and so $h(M(C)) = -1$. Assume that h is well defined if $n(C) < m$ and let $n(C) = m \geq 2$.

Let $B = B(C) = C \cap C^*$, and suppose that $e \in M(C)$ is neither a loop nor a coloop. WOLOG, e corresponds to the first column of G, a generator matrix for C. If $\mathbf{x} \in \widehat{C}$, then either $(1, \mathbf{x})$ or $(0, \mathbf{x})$ is in C, but not both (as then $(1, \mathbf{0}) \in C$, making e a coloop of $M(C)$). Now note that

$$\text{either } B = B_0, \text{ or, for some vector } \mathbf{x} \text{ having first entry 1, } B = B_0 + \langle \mathbf{x} \rangle. \tag{5}$$

In view of Equation 1, we shall write $C\backslash e$ for $\widehat{C}$, and C/e for $\widehat{C}_0$. Also, one can easily check that $(C\backslash e)^* = C^*/e$. In different notation, $(C\backslash e)^* = \widehat{C^*}_0$. Thus if $\mathbf{x} \in B(C\backslash e) = (C\backslash e) \cap (C\backslash e)^*$, then $(0, \mathbf{x}) \in C^*$, while either $(0, \mathbf{x}) \in C$ or $(1, \mathbf{x}) \in C$ (but not both). Dually, if $\mathbf{y} \in B(C/e)$, then $(0, \mathbf{y}) \in C$, while either $(0, \mathbf{y})$ or $(1, \mathbf{y})$ is in C^*, but not both.

The proof of the following lemma is left as an exercise for the reader.

Lemma 4. *Either*

(i) for some $\boldsymbol{x}$ in $B(C\backslash e)$, $(1, \boldsymbol{x}) \in C$ and so $B(C\backslash e) = \widehat{B}_0 + \langle \boldsymbol{x} \rangle$; or

(ii) for all $\boldsymbol{x}$ in $B(C\backslash e)$, $(0, \boldsymbol{x}) \in C$ and so $B(C\backslash e) = \widehat{B}_0$. □

Now suppose that $\dim B = k$. We will show that one of the following three posibilities must happen:

$$\dim B(C\backslash e) = k - 1 = \dim B(C/e) \tag{6}$$

$$\dim B(C\backslash e) = k + 1, \ \dim B(C/e) = k \tag{7}$$

$$\dim B(C\backslash e) = k, \ \dim B(C/e) = k + 1. \tag{8}$$

First we note that the following are equivalent:

(1) $B = B_0$

(2) $(1, \mathbf{0}) \in B^*$

(3) $(1, \mathbf{0}) \in (C \cap C^*)^* = C + C^*$

(4) For some $\mathbf{z}$,

  (a) $(1, \mathbf{z}) \in C$ and $(0, \mathbf{z}) \in C^*$; or

  (b) $(1, \mathbf{z}) \in C^*$ and $(1, \mathbf{z}) \in C$.

Suppose that $B \neq B_0$. Then (i) cannot occur, otherwise $(1, \mathbf{x}) \in C$ and $(0, \mathbf{x}) \in C^*$, meaning that $(1, \mathbf{0}) \in C + C^*$, which is a contradiction. Therefore $B(C\backslash e) = \widehat{B}_0$ and, dually, $B(C/e) = \widehat{B}_0$. So $\dim B(C\backslash e) = \dim \widehat{B} = \dim B(C/e)$. But, by Equation 5, as $B \neq B_0$, $\dim B = \dim B_0 + 1 = \dim \widehat{B}_0 + 1$. Thus, if $B \neq B_0$, then Equation 6 occurs.

Now suppose that $B = B_0$. Then, from above, either (4a) or (4b) occurs. If (4a) occurs, then, for some $\mathbf{z}_1$, $(1, \mathbf{z}_1) \in C$ and $(0, \mathbf{z}_1) \in C^*$, so $\mathbf{z}_1 \in B(C\backslash e)$. If (4b) occurs, then, for some $\mathbf{z}_2$, $(0, \mathbf{z}_2) \in C$ and $(1, \mathbf{z}_2) \in C^*$, so $\mathbf{z}_2 \in B(C/e)$. However, only one of (4a) and (4b) can occur. Otherwise, for some $\mathbf{z}_1$ and $\mathbf{z}_2$, both $(1, \mathbf{z}_1)$ and $(0, \mathbf{z}_2)$ are in C, and $(0, \mathbf{z}_1)$ and $(1, \mathbf{z}_2)$ are in C^*. Hence $(1, \mathbf{z}_1) \cdot (1, \mathbf{z}_2) = 0$ and $(0, \mathbf{z}_1) \cdot (0, \mathbf{z}_2) = 0$, so $1 = 0$; which is a contradiction.

Suppose that (4a) occurs. Then, as $\mathbf{z}_1 \in B(C\backslash e)$, we have, by Lemma 4i, that $\dim B(C\backslash e) = \dim \widehat{B}_0 + 1 = \dim B_0 + 1 = \dim B + 1$. Moreover, as (4b) does not occur, the dual of Lemma 4 implies that $B(C/e) = \widehat{B}_0$, so $\dim B(C/e) = \dim \widehat{B}_0 = \dim B_0 = \dim B$. Hence, if (4a) occurs, then so does Equation 7 and, by duality, if (4b) occurs, so does Equation 8. We conclude that one of Equations 6, 7 and 8 must occur. In each case, it is routine to check that

$$(-1)^n 2^{\dim B} = (-1)^{n(C\backslash e)} 2^{\dim B(C\backslash e)} + (-1)^{n(C/e)} 2^{\dim B(C/e)}.$$

Hence, by Equation 1 and the induction assumption, if e is neither a loop nor a coloop of $M(C)$, then

$$(-1)^{n(C)} 2^{\dim B} = h(M(C)\backslash e) + h(M(C)/e).$$

Also, if e is a loop or a coloop, then

$$(-1)^{n(C)} 2^{\dim B} = \begin{cases} h(\text{loop})h(M(C)\backslash e) & \text{if } e \text{ is a loop,} \\ h(\text{coloop})h(M(C)\backslash e) & \text{if } e \text{ is a coloop.} \end{cases}$$

From the last two equations, we deduce by induction that h is a well defined TG-invariant. As $h(\text{loop}) = h(\text{coloop}) = -1$, it follows by the Recipe Theorem that $h(M(C)) = T(M(C); -1, -1)$. □

Corollary 5. *Let C be a binary code. Then $C \cap C^*$ is trivial if and only if $M(C)$ has an odd number of bases*

Proof. As we're working in $GF(2)$, $-1 = 1$, so $T(M; 1, 1) = T(M; -1, -1)$, for some matroid M. But $T(M; 1, 1)$ is the number of bases of M. The result follows from Theorem 3. □

In contrast to the binary case, if C is a linear code over $GF(q)$ for $q \geq 4$ then $\dim(C \cap C^*)$ is not, in general, a matroid invariant. For example, consider the following representation of $U_{2,4}$ over $GF(13)$, where $\varpi \notin \{0, 1\}$.

$$\begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & \varpi \end{bmatrix}$$

In this case,

$$\dim(C \cap C^*) = \begin{cases} 1 & \text{if } a \in \{6, 8\}, \\ 0 & \text{otherwise.} \end{cases}$$

When $q = 3$, Jaeger showed in 1989 that $(\sqrt{3})^{\dim(C \cap C^*)}$ is the modulus of the complex number $T(M(C); j, j^2)$, where $j = e^{\frac{2\pi i}{3}}$.