Resumo

Neste trabalho apresentamos algumas relações entre matróides e códigos lineares. Estudamos vários invariantes numéricos de matróides e vemos que estes é um dos muitos aspectos de teoria das matróides que tiveram origem em teoria dos grafos. Analisamos uma classe especial de tais invariantes: os invariantes Tutte-Grothendieck. Mostramos que o polinômio de Tutte é o invariante T-G universal (Brilawski,1972) e o relacionamos a teoria dos códigos mostrando que a distribuição de pesos de palavras-código em um código linear é um invariante T-G generalizado (Greene,1976).

Abstract

In this work we present a relation between matroid and linear codes. Numericals invariants for matroids is one the many topics of matroid theory having its origins graph theory. The Tutte Polynomial of the matroid play a role very important in various problems concerned with such invariants. In 1972 Brylawski showed that the Tutte Polynomial is a T-G invariant. In 1976, Greene established a relation among linear codes and the Tutte Polynomial showing that the distribuition of codeweigths in a linear codes is a generalized T-G invariant.

Universidade Federal de Campina Grande
Centro de Ciências e Teconologia
Programa de Pós-Graduação em Matemática
Curso de Mestrado em Matemática

Aplicações do Polinômio de Tutte aos Códigos lineares

por

Lino Marcos da Silva

sob orientação do

Prof. Dr. Braulio Maia Junior

Dissertação apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCT - UFCG, como requisito parcial para obtenção do título de Mestre em Matemática.

Campina Grande - PB

03/2006

Aplicações do Polinômio de Tutte aos Códigos Lineares

por

Lino Marcos da Silva

Dissertação apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCT - UFCG, como requisito parcial para obtenção do título de Mestre em Matemática.

Área de Concentração: Matemática.

Aprovada por:

Prof. Dr. Manoel Lemos

Prof. Dr. Francisco Marcos de Assis

Prof. Dr. Braulio Maia Junior

Orientador

Universidade Federal de Campina Grande
Centro de Ciências e Tecnologia
Programa de Pós-Graduação em Matemática
Curso de Mestrado em Matemática

03/2006

Agradecimentos

01. Primeiramente, agradeço à Deus pela vida e pelo livre arbítrio que deu aos homens para que pudessem desafiar os limites da compreensão de sua própria existência e desencandeasse uma busca interminável pelo conhecimento.

02. Aos meus pais pelos valores éticos, morais e espirituais com que educaram a mim e a meus irmãos. Aos quais também agradeço, pelo afeto.

03. Ao professor Bráulio Maia Júnior pela orientação deste trabalho e também pelos conselhos e lições que tanto estão sendo úteis na minha vida profissional, pessoal e acadêmica.

04. Aos queridos amigos-irmãos Marta Élid e Aluizio pelos incontáveis encontros que realizamos para discutir, entender e compreender os fundamentos das Teorias dos Grafos e das Matróides.

05. Aos professores do DME. Em especial: Marco Aurélio, Daniel Pellegrino, Vânio Fragoso e Francisco Morais.

06. Aos funcionários técnicos-administrativos do DME. Em especial a Dona Salete e Dona Argentina pela sempre disponibilidade em nos ajudar.

07. Aos alunos e amigos do Programa de Pós-Graduação em Matemática do DME/UFCG, pela companhia.

08. A CAPES, pela ajuda financeira.

09. A FACAPE, pela compreensão de seus coordenadores.

10. Aos Professores do departamento de Matemática da FFPP/UPE. Em especial aos professores Sebastião Rildo, Valdir Veneziani e José Petrúcio de Queiroz, pelo incentivo.

11. A todos os amigos que me incentivaram para enfrentar este desafio. Em especial aos amigos Antônio Ronaldo Garcia e Michael Rolim.

12. Aos meus alunos pela torcida.

Dedicatória

Conta-se que numa certa guerra, um soldado dirigiu-se ao seu superior e lhe solicitou permissão para ir buscar um amigo que não voltou do campo de batalha. Permissão negada, respondeu o tenente. Mas o soldado, sabendo que o amigo estava em apuros, ignorou a proibição e foi a sua procura. Algum tempo depois retornou, mortalmente ferido, transportando o cadáver do seu amigo nos braços. O seu superior estava furioso e o repreendeu: - Não disse para você não se arriscar? Eu sabia que a viagem seria inútil! Agora eu perdi dois homens ao invés de um. Diga-me: valeu a pena ir lá para trazer um cadáver? E o soldado, com o pouco de força que lhe restava, respondeu:-Claro que sim, senhor! Quando eu o encontrei ele ainda estava vivo e pôde me dizer: - "Tinha certeza que você viria"!

À José Dantas de Amorim

À Anete Rolim de Albuquerque Gomes (In Memorian)

Conteúdo

Introdução

O Polinômio de Tutte de uma matróide é um polinômio de duas variáveis com coeficientes inteiros não negativos. Este polinômio é relevante em muitos problemas envolvendo invariantes numéricos de matróides. Por exemplo, podemos facilmente determinar para uma dada matróide, a partir do seu Polinômio de Tutte: o posto, a nulidade, o número de bases e o número de conjuntos independentes, entre outros. O objetivo principal deste trabalho é apresentar uma relação entre o polinômio de Tutte de uma matróide vetorial associada a um código linear C e o seu polinômio enumerador de pesos. Este resultado foi obtido por Greene em 1976.

Esta dissertação está estruturada da seguinte maneira. No capítulo 1 fazemos uma introdução à teoria das matróides dando algumas classes de exemplos, definições e resultados que serão necessários a este trabalho. Neste capítulo ainda definimos a Função de Möbius de um reticulado de conjuntos fechados e o polinômio característico de uma matróide. No capítulo 2, definimos e damos exemplos de invariantes de matróides, invariantes Tutte-Grothendieck e mostramos que o polinômio de Tutte é o invariante Tutte-Grothendieck universal. No capítulo 3, damos as noções de teoria dos códigos necessárias ao nosso trabalho; definimos o polinômio enumerador de pesos de um código linear C e mostramos que o mesmo é um invariante Tutte-Grothendieck generalizado. Vemos ainda que um dos problemas fundamentais da Teoria do Códigos é na verdade um caso particular do problema crítico para matróides.

Capítulo 1

Preliminares

1.1 Notação

As notações utilizadas aqui são, basicamente, as mesmas utilizadas por Oxley [3]. Se E é um conjunto finito, denotaremos por 2^E sua coleção de subconjuntos e por $|E|$ sua cardinalidade. O conjunto dos números inteiros, números inteiros positivos, números racionais, números reais e números complexos serão denotados por $\mathbb{Z}, \mathbb{Z}^+, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$, respectivamente. Se X e Y são conjuntos, então $X - Y$ denotará o conjunto

$$\{x \in X : x \notin Y\}.$$

Frequentemente desejaremos adicionar ou remover um único elemento de um conjunto X. Em tais casos, abreviaremos $X \cup \{e\}$ e $X - \{e\}$ por $X \cup e$ e $X - e$, respectivamente. Usaremos o termo *multiconjunto* em vez de conjunto quando houver a possibilidade deste conjunto possuir elementos repetidos. Se Denotarmos um corpo arbitrário por K então K^n denotará o espaço vetorial sobre K. No entanto , quando o corpo considerado for um corpo de Galois com q elementos, onde q é a potência de um primo, denotaremos este corpo por $GF(q)$. Neste caso, o espaço vetorial de dimensão n sobre $GF(q)$ será denotado por $V(n, q)$. A notação para matriz utilizada aqui será a usual onde a matriz I_r é a matriz identidade com r linhas e r colunas; e a transposta de uma matriz A será denotada por A^T. Se v é um vetor de um espaço vetorial V sobre um corpo K então $\langle v \rangle$ denota o supespaço de V gerado por v. A dimensão de V é denotada

por $dimV$. Daremos a seguir algumas noções de Teoria dos Grafos. A figura 1.1 é uma representação de um grafo G particular. O conjunto de *vértices* deste grafo é

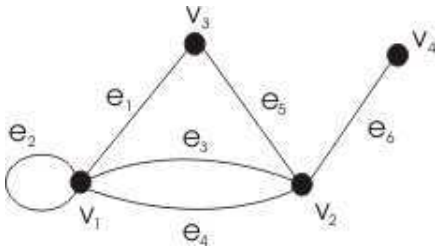

Figura 1.1: Exemplo de um Grafo

$V(G) = \{v_1, v_2, v_3, v_4\}$ e o seu conjunto de *arestas* é $E(G) = \{e_1, e_2, e_3, e_4, e_5, e_6\}$. Uma aresta do tipo de e_2, que é incidente em um único vértice, é denominada de *laço*. Já arestas como e_3 e e_4 que incidem no mesmo par de vértices, são chamadas de *arestas paralelas* ou *arestas múltiplas*. Os conjuntos $\{e_2\}$, $\{e_3, e_4\}$, $\{e_1, e_3, e_5\}$ e $\{e_1, e_4, e_5\}$ são chamados de *ciclos* do grafo G. Uma aresta como e_6 que não pertence a nenhum ciclo é chamada de *ponte* ou *istmo* de G. Em um grafo podemos realizar as operações de *remoção* e *contração* de arestas. A primeira consiste em apagar a aresta do grafo; e a segunda, consiste encolher a aresta até que os vértices ligados por ela coincidam.

1.2 Matróides

1.2.1 Definições e exemplos

Nesta secção apresentaremos um resumo da Teoria das Matróides que será necessária para esta dissertação. Daremos algumas definições básicas e algumas operações sobre matróides , tais como: dualidade, remoção , contração e soma direta. Veremos também como obter uma nova matróide a partir de uma dada, usando as operações citadas anteriormente. Para maiores detalhes e provas dos resultados desta seção indicamos como referência o livro do Oxley [3].

Matróides foram introduzidas por Whitney em 1935 como uma abstração da independência linear em espaços vetoriais e das propriedades de ciclos em Grafos. Essas duas abordagens de Whitney renderam duas importantes classes de matróides: as vetoriais e as gráficas. Além disso grande parte da terminologia de objetos em

teoria das matróides tem sua origem em uma dessas classes de matróides. Uma das principais características dessas estruturas é que existem várias maneiras de definí-las. Aqui definiremos uma matróide em termo de seus conjuntos independentes. Mais adiante, porém, daremos outras formas alternativas de definições para matróides.

Uma *Matróide* M é um par ordenado $(E, \mathcal{I})$, consistindo de um conjunto finito E e uma coleção $\mathcal{I}$ de subconjuntos de E satisfazendo as seguintes propriedades:

(I1) $\varnothing \in \mathcal{I}$

(I2) Se $I \in \mathcal{I}$ e $J \subseteq I$, então $J \in \mathcal{I}$

(I3) Se $I, J \in \mathcal{I}$ e $|J| < |I|$, então existe um elemento $\boldsymbol{e}$ de $I - J$ tal que, $J \cup e \in \mathcal{I}$.

Se M é a matróide $(E, \mathcal{I})$, então dizemos que M é uma matróide sobre E. Os membros de $\mathcal{I}$ são chamados de conjuntos *independentes* de M e E é chamado o *conjunto básico* de M. Frequentemente escrevemos $\mathcal{I}\ (M)$ para denotarmos $\mathcal{I}$ e $E(M)$ para E, particularmente quando muitas matróides estão sendo consideradas, e assim evitarmos alguma confusão nas notações. Um subconjunto de E que não está em $\mathcal{I}$ é chamado de *dependente*. Dizemos que duas matróides M e N são *isomorfas*, e escrevemos $M \cong N$, se existe uma bijeção $\Psi : E(M) \to E(N)$ tal que para todo $X \subseteq E(M)$, $\Psi(X)$ é independente em N se e somente se X é independente em M.
Como dissemos anteriormente o termo matróide foi cunhado por Whitney (1935) por causa de uma classe fundamental de exemplos dessas estruturas que têm origem em matrizes do seguinte modo:

Proposição 1.1 *Seja A uma matriz do tipo $m \times n$ com entradas em um corpo K. Sejam E o conjunto que rotula as colunas de A e $\mathcal{I}$ a coleção de subconjuntos I de E para os quais o multiconjunto de colunas rotuladas por I são linearmente independentes sobre K. Então $(E, \mathcal{I})$ é uma matróide.*

Uma matróide obtida de uma matriz A, como acima, será denotada por $M[A]$ e chamada de *matróide vetorial* de A. Se M é uma matróide isomorfa a $M[A]$ para alguma matriz A sobre um corpo F, então M é dita ser uma matróide *representável* sobre F e A é chamada de uma *representação* de M. Dizemos ainda que $M[A]$ é representável sobre F. Matróides representáveis sobre $GF(2)$ são chamadas de *binárias*.

Matróides vetoriais serão bastantes consideradas no decorrer deste trabalho. Como um exemplo particular de tais matróides, considere o seguinte:

Exemplo 1.2 *Seja A a matriz*

$$\begin{matrix} 1 & 2 & 3 & 4 & 5 \end{matrix}$$
$$\begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

com entradas em $\mathbb{R}$.

Então $E = \{1, 2, 3, 4, 5\}$ e

$\mathcal{I} = \{\varnothing, \{1\}, \{2\}, \{4\}, \{5\}, \{1, 2\}, \{1, 5\}, \{2, 4\}, \{2, 5\}, \{4, 5\}\}$.

O conjunto de conjuntos dependentes desta matróide é

$\{\{3\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{3, 4\}, \{3, 5\}\} \cup \{X \subseteq E; |X| \geq 3\}$.

Uma outra família importante de matróides é dada pela proposição a seguir.

Proposição 1.3 *Sejam m e n inteiros não negativos tais que $m \leq n$. Seja E um conjunto com n elementos. Se $\mathcal{I} = \{X \subseteq E : |X| \leq m\}$, então $(E, \mathcal{I})$ é uma matróide. Denotamos esta matróide por $U_{m,n}$ e chamamos de matróide uniforme .*

Como um exemplo particular de matróides uniformes considere o seguinte:

Exemplo 1.4 *A matróide uniforme $U_{2,4}$ é a matróide uniforme que tem como conjunto básico o conjunto $E = \{1, 2, 3, 4\}$ e cuja coleção de conjuntos independentes é formada pelos subconjuntos de E que tem 2 ou menos elementos. Ou seja*

$\mathcal{I}\ (U_{2,4}) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}\}$

Um conjunto dependente minimal em uma matróide arbitrária M é chamado de *circuito* de M e um conjunto independente maximal é chamado de *base*. Denotamos por $\mathcal{C}\ (M)$ e $\mathcal{B}\ (M)$ o conjunto de circuitos e de bases, respectivamente, da matróide M. Um subconjunto de $E(M)$ que contém uma base recebe o nome de *conjunto gerador*.

Dos axiomas de independência e da maximilidade de uma base, segue que todas as bases de uma matróide M têm a mesma cardinalidade; esta cardinalidade é denotada por $r(M)$ e é chamada de o *posto* de M. Para qualquer conjunto $X \subseteq E$, o posto de X é a cardinalidade do maior conjunto independente em X e é denotado por $r(X)$ ou $r_M(X)$. A nulidade de X é dada por $n(X) = |X| - r(X)$. Se x e y são elementos de

E tais que $r(\{x\}) = r(\{y\}) = r(\{x, y\}) = 1$,então dizemos que x e y são *elementos paralelos*. Numa matróide vetorial, dois elementos são paralelos se rotulam colunas iguais ou colunas proporcionais. No **Exemplo 1.2** os elementos 1 e 4 são elementos paralelos.

Seja M uma matróide arbitrária sobre E e com função posto r. Definimos o *operador fecho* de M como sendo a função $Cl : 2^E \to 2^E$ definida, para todo $X \subseteq E$, por

$$Cl(X) = \{x \in E : r(X \cup x) = r(X)\}.$$

No **Exemplo 1.2** $Cl(\varnothing) = \{3\}$, $Cl(\{1, 2\}) = \{1, 2, 3, 4, 5\}$ e $Cl(\{1\}) = \{1, 3, 4\}$.

Dizemos que um conjunto $X \subseteq E$ é *fechado* se $Cl(X) = X$. Alternativamente, dizemos que um conjunto $X \subseteq E$ é um *conjunto fechado* se $r(X \cup x) = r(X) + 1$ para todo $x \in E - X$. Os conjuntos $\{1, 3, 4\}$, $\{2, 3\}$, $\{3, 4\}$ e $\{5, 6\}$ no **Exemplo 1.2** são conjuntos fechados. Um conjunto fechado que tem posto $r(M) - 1$ é chamado de *hiperplano*.

Os conjuntos de bases, circuitos e conjuntos fechados; a função posto e o operador fecho são suficientes para determinar uma matróide M a menos de isormorfismo. Para cada um deles existe um resultado análogo ao seguinte teorema.

Teorema 1.5 *Seja $\mathcal{C}$ uma coleção de subconjuntos de um conjunto E tal que:*

(C1) $\varnothing \notin \mathcal{C}$

(C2) Se $C_1, C_2 \in \mathcal{C}$ e $C_1 \subseteq C_2$, então $C_1 = C_2$.

(C3) Se $C_1, C_2 \in \mathcal{C}$ com $e \in C_1 \cap C_2$, então existe $C \in \mathcal{C}$ tal que $C \subseteq (C_1 \cup C_2) - e$.

Então existe uma única matróide M sobre o conjunto E que tem $\mathcal{C}$ como seu conjunto de circuitos.

A propriedade (C3) é chamada de *axioma da eliminação do circuito*.

O terceiro exemplo de matróides que daremos são as matróides derivadas de grafos.

Proposição 1.6 *Seja E o conjunto de arestas de um grafo G e $\mathcal{C}$ o conjunto de ciclos de G. Então $\mathcal{C}$ é o conjunto de circuitos de uma matróide sobre E.*

A matróide derivada do grafo G como acima é chamada de *matróide ciclo* ou *matróide poligonal* de G e é denotada por $M(G)$. Uma matróide que é isomorfa a matróide ciclo

de um grafo é chamada de *matróide gráfica*. A matróide ciclo $M(G)$ do grafo G da Figura 1.1 tem como seu conjunto de circuitos o conjunto

$$\mathcal{C} = \{\{e_2\}, \{e_3, e_4\}, \{e_1, e_3, e_5\}\, e\, \{e_1, e_4, e_5\}\}$$

enquanto seu conjunto de bases é

$$\{\{e_1, e_5, e_6\}, \{e_1, e_3, e_6\}, \{e_1, e_4, e_6\}, \{e_3, e_5, e_6\}\, e\, \{e_4, e_5, e_6\}\}$$

1.2.2 Dualidade

Um dos principais atrativos na teoria da matróides é a existência da teoria da dualidade. Pois ao contrário do que acontece com os grafos, toda matróide possui uma dual. Como principal resultado desta secção temos o seguinte

Teorema 1.7 *Seja $\mathcal{B}$ o conjunto de bases de uma matróide M sobre E, então*

$$\mathcal{B}^*(M) = \{E - B; B \in \mathcal{B}(M)\}$$

é o conjunto de bases de uma matróide sobre E, chamada matróide dual de M.

Denotamos a matróide dual de M por M^*. Por definição, a matróide M e sua dual M^* estão relacionadas por

$$(M^*)^* = M.$$

A partir da definição da matróide dual de M podemos deduzir as seguintes propriedades para M:

- Um subconjunto $X \subseteq E$ é independente em M^* se e somente se $E - X$ é um conjunto gerador de M.
- O posto de M^* é dado por $|E| - r(M)$

Este último resultado é um caso especial da relação entre as funções posto r e r^* de M e M^*, respectivamente, que é dada por

$$r^*(X) = |X| - r(E) + r(E - X)$$

para qualquer $X \subseteq E$. A função $r^* : E \to \mathbb{Z}$ é também chamada de *função coposto* de M. Seguindo esta mesma notação: uma *cobase* de M é uma base de M^*, um *cocircuito*

de M é um circuito de M^* e assim por diante. Dizemos que uma matróide M é *auto-dual* se $M = M^*$.

Agora, vamos ver o efeito da dualidade sobre a matróide vetorial $M[A]$ da matriz A do tipo $m \times n$. Sabemos que $M[A]$ tem como seu conjunto básico E o conjunto dos rótulos das colunas de A. Vejamos agora, como podemos alterar uma matriz A sem afetar a matróide vetorial $M[A]$. O resultado a seguir é muito comum em textos básicos de álgebra linear e não o provaremos aqui.

Lema 1.1 *Seja A uma matriz com entradas em um corpo F. Então $M[A]$ não se altera quando efetuamos qualquer uma das seguintes operações em A.*

(i) permutação de duas linhas.

(ii) multiplicação de uma linha por um escalar não nulo.

(iii) Adição de um múltiplo escalar de uma linha a outra.

(iv) remoção de uma linha nula (a menos que ela seja a única)

(v) permutação de duas colunas (acompanhadas de seus respectivos rótulos)

(vi) multiplicação de uma coluna por um escalar não nulo.

Comumente as operações do lema anterior são chamadas de *operações elementares linha* da matriz A.

Podemos notar que se A é uma matriz nula com n colunas, então $M[A] \cong U_{0,n}$. Com efeito, cada uma dessas duas matróides são formadas apenas por n laços. Agora se A é uma matriz não nula com posto r, das operações *(i)* até *(v)* do **Lema 1.1** podemos transformar A em uma matriz da forma $[I_r|D]$ onde I_r é a matriz identidade $r \times r$ e D é alguma matriz $r \times (n-r)$ sobre F. Dizemos que $[I_r|D]$ é a *forma padrão* da matriz A. O teorema a seguir nos dá a dual de uma matróide vetorial M.

Teorema 1.8 *Se M é a matróide vetorial de $[I_r|D]$, então M^* é a matróide vetorial de $[-D^T|I_{n-r}]$.*

Este último resultado nos dá uma interessante conexão entre dualidade em matróides e ortogonalidade em espaços vetoriais. De fato dado um subespaço W de um espaço

vetorial V, o conjunto W^T de vetores de V que são ortogonais a cada vetor de W forma um subespaço de V chamado de *complemento ortogonal* de W. Mostra-se em álgebra linear que se W é o espaço vetorial gerado pelas linhas da matriz $[I_r|D]$, então W^T é o espaço vetorial gerado pelas linhas de $[-D^T|I_{n-r}]$.

Exemplo 1.9 *Voltemos ao* **Exemplo 1.2** *onde a matróide vetorial M tinha como representação a seguinte matriz*

$$\begin{matrix} & 1 & 2 & 3 & 4 & 5 \end{matrix}$$
$$\begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

então pelo desenvolvido acima a matróide dual M^* será representada pela seguinte matriz

$$\begin{matrix} 1 & 2 & 3 & 4 & 5 \end{matrix}$$
$$\begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 1 & 0 \\ -1 & -1 & 0 & 0 & 1 \end{bmatrix}$$

1.2.3 Laços e Pontes

Um *laço* é um elemento da matróide cujo posto é zero. Este nome foi herdada da teoria dos grafos onde um laço corresponde a uma aresta que incide em um único vértice. Em uma matróide vetorial um laço corresponde a uma coluna nula e na matróide uniforme $U_{m,n}$ existem laços se e somente se $m = 0$. Na matróide vetorial sobre a matriz do **Exemplo 1.2** o elemento cujo rótulo é 3, ou seja a terceira coluna, é um laço.

Proposição 1.10 *Para um elemento x de uma matróide M que é um laço são equivalentes as seguintes afirmações:*

(a) x é um circuito;

(b) $r_M(x) = 0$;

(c) x pertence a $Cl(\varnothing)$;

(d) x pertence a cada conjunto fechado de M;

Um elemento x é uma *ponte* ou um *istmo* de M se x é um laço de M^*. Assim, de acordo com a notação introduzida na **Secção 1.2.2** dizer que um elemento x de uma matróide M é uma ponte é equivalente a dizer que x é um *colaço* de M.
Veremos a seguir como identificarmos uma ponte em uma matróide vetorial M. Um elemento x é uma ponte de M, se não é um laço e se sempre podemos obter por meio das operações elementares linhas *(i)* à *(v)* do **Lema 1.1** uma matriz A' na qual a coluna c_j rotulada por x é um vetor com uma única entrada não nula e a_{ij} é a única entrada não nula na i-ésima linha de A. Em outras palavras, um elemento x de uma matróide vetorial é uma ponte, se pudermos obter por meio de uma sequência de operações elementares linha, na coluna rotulada por esse elemento, uma única entrada a_{ij} não nula, a qual é também a única entrada não nula da i-ésima linha dessa matriz. O elemento rotulada pelo número 3 da matróide do **Exemplo 1.9** é uma ponte.

Proposição 1.11 *Um elemento $x \in E$ é uma ponte de $M(E)$ se e somente se satisfaz qualquer uma das seguintes afirmativas:*

(a) $r_M(X \cup x) = r(X) + 1$, *para todo* $X \subseteq E - x$;

(b) x *está em cada base;*

(c) x *não está em nenhum circuito;*

(d) $I \cup x$ *é independente para cada conjunto independente* I.

Uma matróide sem laços e sem elementos paralelos é chamada de *matróide simples* ou uma *geometria*.

1.2.4 Remoção, Contração e Menores

Nesta seção introduziremos as operações de remoção e contração sobre uma matróide M. Examinaremos seus efeitos sobre matróides vetoriais e veremos como estas operações se relacionam com a dualidade.
Sejam M uma matróide $(E, \mathcal{I})$, e um elemento de E e

$$\mathcal{I}' = \{I \subseteq E - e : I \in \mathcal{I}\}.$$

Então $(E-e, \mathcal{I}')$ é uma matróide chamada de *remoção* e de M e é denotada por $M\backslash e$
Sejam M uma matróide $(E, \mathcal{I})$ e e um elemento de E que não é um laço. Seja

$$\mathcal{I}'' = \{I \subseteq E - e : I \cup e \in \mathcal{I}\}.$$

Então $(E-e, \mathcal{I}'')$ é uma matróide chamada de *contração* e de M e é denotada por M/e. Se e é um laço definimos $M/e = M\backslash e$. Alternativamente, podemos definir a operação de contração como sendo a dual da remoção. Ou seja, se M/e é a contração e de M então

$$M/e = (M^*\backslash e)^*.$$

Se e e f são elementos distintos de uma matróide M, então

$$(M\backslash e)\backslash f = (M\backslash f)\backslash e; (M/e)/f = (M/f)/e \quad \text{e} \quad (M\backslash e)/f = (M/f)\backslash e.$$

Isto significa que, para subonjuntos disjuntos X e Y do conjunto E, a matróide $M\backslash X$, M/Y e $M\backslash X/Y$ estão bem definidas. Uma *menor* N de M é qualquer matróide que pode ser obtida de M por meio de uma sequência de remoções e contrações, isto é, qualquer matróide N arbitrária da forma $N = M\backslash X/Y$, ou equivalentemente, da forma $N = M/X\backslash Y$. Em particular, para $N = M\backslash(E\backslash X)$, escrevemos $N = M(X)$ e dizemos que N é *restrição* de M a X ou que N é uma *submatróide* de M.
De maneira mais geral, se M é uma matróide que tem conjunto básico E e $T \subseteq E$ então $M\backslash T$ e M/T são matróides sobre $E - T$. Além disso, se r é a função posto de M então para todo $X \subseteq E - T$

$$r_{M\backslash T}(X) = r_M(X) \tag{1.1}$$

$$r_{M/T}(X) = r_M(X \cup T) - r_M(T) \tag{1.2}$$

Ainda para uma matróide M sobre E e $T \subseteq E$ podemos relacionar dualidade, remoção e contração do seguinte modo $M^*/T = (M\backslash T)^*$ e $M^*\backslash T = (M/T)^*$.
Se $\mathcal{M}$ é uma classe de matróides tal que para cada $M \in \mathcal{M}$ todos os menores de M pertencem a $\mathcal{M}$, então dizemos que $\mathcal{M}$ é *menor-fechada* ou que $\mathcal{M}$ é *fechada em relação a tomada de menores.* As classes de matróides representáveis sobre um corpo F, matróides gráficas e matróides uniformes são menores fechadas.
No decorrer deste trabalho necessitaremos efetuar remoções e contrações em matróides vetoriais. Remover um elemento e de uma matróide vetorial $M = M[A]$ equivale a

remover a coluna de A que está rotulada por e.

Já a contração de e poderá ser feita do seguinte modo: se e é um laço de M, então e rotula uma coluna nula de A e neste caso $M/e = M\backslash e$. Agora, assumamos que e não é um laço de M, ou seja e rotula uma coluna não nula de A. Suponhamos primeiro que e rotula uma coluna com apenas uma entrada diferente de zero. Observemos que e determina a única linha de A na qual e tem sua única entrada não nula. Removendo-se de A esta linha e a coluna rotulada por e, obtemos uma representação para M/e.

Por fim quando e rotula uma coluna que é um vetor com mais de uma entrada não nula, efetuando-se operações elementares do tipo *(i)* até *(v)* do **Lema 1.1**, transformamos A em uma matriz A' na qual e rotula um vetor unitário. Sabemos que $M[A] = M[A']$ e então podemos proceder como antes para obter uma representação para M/e.

Exemplo 1.12 *Seja M a matróide vetorial do **Exemplo 1.2** então $M\backslash 2$ é a matróide vetorial da seguinte matriz*

$$\begin{array}{c} \begin{array}{cccc} 1 & 3 & 4 & 5 \end{array} \\ \left[\begin{array}{cccc} 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{array}\right] \end{array}$$

enquanto $M/2$ é representada por

$$\begin{array}{c} \begin{array}{cccc} 1 & 3 & 4 & 5 \end{array} \\ \left[\begin{array}{cccc} 1 & 0 & 1 & 1 \end{array}\right] \end{array}$$

1.2.5 Soma Direta

Uma outra operação sobre matróides tão importante quanto remoção e contração é a soma direta. Dadas duas matróides M_1 e M_2 com conjuntos básicos disjuntos E_1 e E_2, definimos a *soma direta*, $M_1 \oplus M_2$, como sendo a matróide que tem conjunto básico $E = E_1 \cup E_2$ e coleção de conjuntos independentes

$$\mathcal{I} = \{I_1 \cup I_2; I_1 \in \mathcal{I}(M_1)\, e\, I_2 \in \mathcal{I}(M_2)\}.$$

Para todos subconjuntos, $X_1 \subseteq E_1$ e $X_2 \subseteq E_2$ temos

$$r_{M_1 \oplus M_2}(X_1 \cup X_2) = r_{M_1}(X_1) + r_{M_2}(X_2).$$

Uma característica de soma direta é que ela é uma operação auto-dual, ou seja,

$$(M_1 \oplus M_2)^* = M_1^* \oplus M_2^*.$$

1.3 A Função de Möbius e o Polinômio Característico de uma Matróide

1.3.1 O reticulado de conjuntos fechados

Um *conjunto parcialmente ordenado* é um conjunto P munido de uma relação binária, $\leq$, tais que para todo x, y e $z \in P$, as seguintes condições valem

(P1) $x \leq x$

(P2) se $x \leq y$ e $y \leq x$, então $x = y$

(P3) Se $x \leq y$ e $y \leq z$, então $x \leq z$

Dizemos que um conjunto parcialmente ordenado $\mathcal{L}$ é um *reticulado* se para cada dois elementos $x, y \in \mathcal{L}$, o conjunto parcialmente ordenado $\{z \in \mathcal{L}; z \geq x, z \geq y\}$ tem um elemento mínimo em $\mathcal{L}$ denotado por $x \vee y$; e o conjunto parcialmente ordenado $\{z \in \mathcal{L}; z \leq x, z \leq y\}$ tem um elemento máximo em $\mathcal{L}$ denotado por $x \wedge y$.
Para uma matróide M denotaremos por $\mathcal{L}(M)$ a coleção de conjuntos fechados de M ordenados por inclusão.

Proposição 1.13 *$\mathcal{L}(M)$ é um reticulado e, para conjuntos fechados quaisquer X e Y de M*

$$X \wedge Y = X \cap Y \, e \, X \vee Y = Cl(X \cup Y).$$

Se o conjunto parcialmente ordenado P tem um elemento z tal que $z \leq x$ para todo $x \in P$, então chamamos z de *o zero* de P e denotamos ele por $\hat{0}$ ou simplesmente por 0. Analogamente, se P tem um elemento w tal que $w \geq x$ para todo $x \in P$, então w é chamado de o *um* de P e é frequentemente denotado por $\hat{1}$. Podemos percerber que todo reticulado finito tem um elemento *zero* e um elemento *um*. Em particular, para uma matróide M, o *zero* de $\mathcal{L}(M)$ é $Cl(\varnothing)$ e o *um* é $E(M)$. Podemos representar um conjunto parcialmente ordenado P por um *Diagrama de Hasse*. Um tal diagrama é um grafo simples, onde os seus vértices correspondem aos elementos de P. Neste grafo, se $x > y$, então o vértice correspondente a x é desenhado acima do correspondente a y. Dois vértices x e y são ligados por uma aresta, sempre que x cobre y. Em um conjunto

parcialmente ordenado, dizemos que x cobre y se $y < x$ e não existe $z \in P$ tal que $y < z < x$.

Exemplo 1.14 *O reticulado de conjuntos fechados de* $M = U_{2,4}$ *onde* $E(M) = \{a, b, c, d\}$ *é o conjunto*

$$\mathcal{L}(M) = \{\varnothing, \{a\,\{b\}, \{c\}, \{d\}, \{a, b, c, d\}\}$$

e o diagrama de Hasse *que representa* $\mathcal{L}(M)$ *é o da figura abaixo*

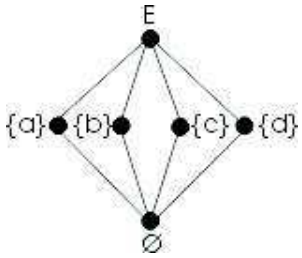

Figura 1.2: Diagrama de Hasse

1.3.2 A Função de Möbius

Seja P um conjunto parcialmente ordenado e considere as funções inteiras $P \times P$ em $\mathbb{Z}$. A função $\mu_P : P \times P \to \mathbb{Z}$ que satisfaz
$\mu(x, x) = 1, \forall x \in P$
$\mu(x, z) = -\sum_{x \leq y < z} \mu(x, y), x < y$ em P. É chamada de *Função de Möbius* de P.
O próximo resultado é uma importante propriedade da Função de Möbius conhecida como a *inversão de Möbius*.

Proposição 1.15 *Seja* P *um conjunto parcialmente ordenado. Sejam* f *e* g *funções sobre* P *com valores em um anel qualquer. Então*

$$g(x) = \sum_{y \geq x} f(y)$$

implica

$$f(x) = \sum_{y \geq x} \mu_P(x, y) g(y),$$

e vice-versa.

Seja M uma matróide e $\mathcal{L}$ o seu reticulado de conjuntos fechados. Denotaremos por $\mu_{\mathcal{L}}$ a Função de Möbius de $\mathcal{L}$.

A Função de Möbius da matróide M é definida por

$$\begin{aligned} \mu_M(X,F) &= \mu_{\mathcal{L}}(X,F), \quad \text{se } X,F \in \mathcal{L}, \\ \mu_M(X,F) &= 0, \qquad\qquad \text{se } X \notin \mathcal{L}, F \in \mathcal{L}; \end{aligned}$$

$\mu_M(X,F)$ não está definida se $F \notin \mathcal{L}$.

Exemplo 1.16 *A Função de Möbius de $M = U_{2,4}$ com $E(M) = \{a,b,c,d\}$ é dada por*

$$\begin{aligned} \mu_M(\varnothing, E) &= \mu_{\mathcal{L}}(\varnothing, E) \\ &= -\big[\mu_{\mathcal{L}}(\varnothing,\varnothing) + \mu_{\mathcal{L}}(\varnothing,\{a\}) + \mu_{\mathcal{L}}(\varnothing,\{b\}) + \mu_{\mathcal{L}}(\varnothing,\{c\}) + \mu_{\mathcal{L}}(\varnothing,\{d\})\big] \\ &= -\big[1-1-1-1-1\big] \\ &= 3. \end{aligned}$$

1.3.3 O Polinômio Característico

O polinômio característico é uma analogia para matróides do polinômio cromático para grafos. Para uma matróide M, este polinômio é definido por

$$p(M,\lambda) = \sum_{F \in \mathcal{L}} \mu_M(\varnothing, F)\lambda^{r(M)-r(F)}$$

Onde $\mathcal{L}$ denota o reticulado de conjuntos fechados de M.

Exemplo 1.17 *O polinômio característico de $M = U_{2,4}$ é calculado a seguir:*

$$\begin{aligned} p(M,\lambda) &= \mu_M(\varnothing,\varnothing)\lambda^{2-0} + \mu_M(\varnothing,\{a\})\lambda^{2-1} + \mu_M(\varnothing,\{b\})\lambda^{2-1} + \mu_M(\varnothing,\{c\})\lambda^{2-1} + \\ &\quad + \mu_M(\varnothing,\{d\})\lambda^{2-1} + \mu_(\varnothing, E)\lambda^{2-2} \\ &= 1\lambda^2 + (-1)\lambda^1 + (-1)\lambda^1 + (-1)\lambda^1 + (-1)\lambda^1 + 3\lambda^0 \\ &= \lambda^2 - 4\lambda + 3. \end{aligned}$$

Proposição 1.18 *O polinômio característico de uma matróide $M = M(E)$ satisfaz:*

(i) A regra de remoção-contração: se $e \in E$ não é ponte nem laço.

$$p(M, \diagdown) = p(M-e,\lambda) - p(M/e,\lambda)$$

(ii) A regra da soma direta: se $M = M_1 \oplus M_2$

$$p(M,\lambda) = p(M_1,\lambda)p(M_2,\lambda).$$

Capítulo 2

O Polinômio de Tutte

2.1 Introdução

A teoria de invariantes numéricos para matróides é um dos muitos aspectos da teoria das matróides que tiveram origem na teoria dos grafos. De fato, muitas idéias na teoria desses invariantes foram desenvolvidas por Veblen(1912), Birkhoff(1912-13), Whitney(1932) e Tutte(1947;1954) quando consideraram coloração e fluxos em grafos. As aplicações desta teoria, extrapola os limites da teoria dos grafos e atinge campos como: a teoria dos códigos, a teoria da percolação, teoria dos sistemas elétricos e mecânica estatística. Além disso, muitas novas aplicações à teoria dos grafos tem sido encontradas. Neste capítulo definiremos e daremos alguns exemplos fundamentais desses invariantes. Consideraremos, em particular, os invariantes T-G. Como principal resultado deste capítulo, provaremos que o polinômio de Tutte é o invariante T-G universal.

Seja $\mathcal{K}$ o conjunto formado por todas as matróides. Dizemos que uma função f definida em $\mathcal{K}$ é um *invariante sob isomorfismo* de matróides, ou simplesmente um *invariante de matróides*, se

$$f(M) = f(N) \tag{2.1}$$

sempre que $M \cong N$.

Como exemplo de um invariante de matróides podemos citar a função $i(M) : \mathcal{K} \longrightarrow \mathbb{Z}^+$

que dá o número de conjuntos independentes de cada matróide $M \in \mathcal{K}$. De fato, se as matróides M e N são isomorfas existe uma bijeção entre M e N que preserva conjuntos independentes. Logo $i(M) = i(N)$.

Sejam $\mathcal{K}$, uma classe de matróides fechada sob isomorfismo e a tomada de menores e f uma função definida em $\mathcal{K}$. Dizemos que f é um *invariante Tutte-Grothendieck* ou, abreviadamente, um *invariante T-G* se f satisfaz as seguintes condições:

$$f(M) = f(M\backslash e) + f(M/e) \text{ se e não é um laço nem uma ponte} \tag{2.2}$$

$$f(M) = f(M(e))f(M\backslash e) \text{ caso contrário.} \tag{2.3}$$

Se a função f é um invariante de matróide que satisfaz (2.3) e a seguinte generalização de (2.2)

$$f(M) = \sigma f(M\backslash e) + \tau f(M/e) \tag{2.4}$$

para σ e τ números não nulos fixos . Então f é chamada de *invariante T-G generalizado*. Daqui por diante utilizaremos as letras P e L para denotarmos uma matróide com um único elemento, o qual é uma ponte e um laço, respectivamente. Um resultado muito interessante da teoria desses invariantes, é que cada invariante T-G é uma avaliação de um certo polinômio de duas variáveis $t(M; x, y)$ tal que

$$f(P) = x \quad e \quad f(L) = y \tag{2.5}$$

A partir destes resultados, deduziremos uma caracterização de todos os invariantes T-G generalizados. Um desenvolvimento mais detalhado desta teoria aparece em Brylawski(1982). Aqui estabeleceremos apenas os resultados necessários à aplicações desta teoria aos códigos lineares.

2.2 O Polinômio de Tutte

Nesta seção estabeleceremos o resultado fundamental que caracteriza todos os invariantes T-G e invariantes T-G generalizados. Seja $M = M(E)$ uma matróide arbitrária com função posto r e função nulidade n. Definimos o *Polinômio Gerador Associado ao Posto* $S(M; x, y)$ de M por

$$S(M; x, y) = \sum_{X \subseteq E} x^{r(E)-r(X)} y^{n(X)} = \sum_{X \subseteq E} x^{r(E)-r(X)} y^{|X|-r(X)} \tag{2.6}$$

Se denotarmos por a_{ij} o número de submatróides que têm posto $r(M)-i$ e nulidade j então temos que

$$S(M;x,y)=\sum_{i}\sum_{j}a_{ij}x^{i}y^{j}. \tag{2.7}$$

Lema 2.1 *S(M;x,y) é um invariante de matróide para a classe de todas as matróides $\mathcal{K}$.*

Prova. Sejam $M,N\in\mathcal{K}$ tais que $M\cong N$. Pela definição de isomorfismo de matróides, existe uma bijeção $\Psi:E(M)\longrightarrow E(N)$ tal que $\Psi(X)\in\mathcal{I}(N)$ se e somente $X\in\mathcal{I}(M)$. Além disso $|\Psi(X)|=|X|$, para todo $X\subseteq E(M)$. Daí $r_N(\Psi(X))=r_M(X)$. Logo

$$\begin{aligned}S(M;x,y) &= \sum_{X\subseteq E(M)}x^{r(E(M))-r_M(X)}y^{n(X)}\\ &= \sum_{\Psi(X)\subseteq E(N)}x^{r(\Psi(E(M)))-r_N(\Psi(X))}y^{n(\Psi(X))}\\ &= S(N;x,y).\end{aligned}$$

■

Lema 2.2

$$S(P;x,y)=x+1\quad e\quad S(L;x,y)=y+1 \tag{2.8}$$

Prova. Note que P e $\varnothing$ são as únicas submatróides de P e que $r(P)=1$ e $n(P)=|P|-r(P)=1-1=0$. Logo $S(P;x,y)=x^{1-1}y^{0}+x^{1-0}y^{0}=1+x$. Da mesma forma L e $\varnothing$ são as únicas submatróides de L e $r(L)=0$ enquanto $n(L)=|L|-r(L)=1-0=1$. Então $S(L;x,y)=x^{0-0}y^{1}+x^{0-0}y^{0}=y+1$ ■

Proposição 2.1 *$S(M;x,y)$ é um invariante $T-G$ para a classe de todas as matróides.*

Prova. Sejam $M=M(E)$, $X\subseteq E$ e $e\in E$. Percebamos que

$$S(M;x,y)=\sum_{X\subseteq E}x^{r(E)-r(X)}y^{n(X)}=\underbrace{\sum_{\substack{X\subseteq E\\ e\notin X}}x^{r(E)-r(X)}y^{n(X)}}_{I}+\underbrace{\sum_{\substack{X\subseteq E\\ e\in X}}x^{r(E)-r(X)}y^{n(X)}}_{II} \tag{2.9}$$

Para maior clareza vamos analisar as expressões I e II separadamente.

$$I=\sum_{\substack{X\subseteq E\\ e\notin X}}x^{r(E)-r(X)}y^{n(X)}=\sum_{X\subseteq E-e}x^{r(E)-r(X)}y^{n(X)}.$$

Além disso,

$$r(E) = \begin{cases} r(E-e)+1 & \text{se e é uma ponte} \\ r(E-e) & \text{caso contrário} \end{cases}$$

Observemos que

$$\sum_{X\subseteq E-e} x^{r(E-e)+1-r(X)}y^{n(X)} = \sum_{X\subseteq E-e} x^{r(E-e)-r(X)}x^1y^{n(X)} = x\sum_{X\subseteq E-e} x^{r(E-e)-r(X)}y^{n(X)}$$

Então

$$I = \begin{cases} x\displaystyle\sum_{X\subseteq E-e} x^{r(E-e)-r(X)}y^{n(X)} & \text{se } e \text{ é uma ponte;} \\ \displaystyle\sum_{X\subseteq E-e} x^{r(E-e)-r(X)}y^{n(X)} & \text{caso contrário.} \end{cases}$$

Portanto

$$I = \begin{cases} xS(M\backslash e; x, y) & \text{se } e \text{ é uma ponte} \\ S(M\backslash e; x, y) & \text{caso contrário} \end{cases} \tag{2.10}$$

Agora analisaremos a expressão II de (2.9). Note que se $Y \subseteq E-e$ então $Y\cup e \subseteq E$. Assim podemos fazer $X = Y\cup e$ para todo $Y \subseteq E-e$. E então

$$II = \sum_{\substack{X\subseteq E \\ e\in X}} x^{r(E)-r(X)}y^{n(X)} = \sum_{Y\subseteq E-e} x^{r((E-e)\cup e)-r(Y\cup e)}y^{n(Y\cup e)}.$$

Agora, denotemos por r' e n' as funções posto e nulidade, respectivamente, de M/e. Então, para todo $Y \subseteq E-e$, temos pela definição da função posto de M/e que $r'(Y) = r(Y\cup e) - r(\{e\})$.

Logo,

$$r'(Y) = \begin{cases} r(Y\cup e) & \text{se e é um laço,} \\ r(Y\cup e)-1 & \text{caso contrário.} \end{cases}$$

Por definição temos que

$$n(Y\cup e) = |Y\cup e| - r(Y\cup e) = |Y| + 1 - r(Y\cup e).$$

Portanto, se e é um laço $n(Y\cup e) = \underbrace{|Y| - r'(Y)}_{n'(Y)} + 1$ e então $n'(Y) = n(Y\cup e) - 1$.

Por outro lado, se e não é um laço

$$n(Y\cup e) = |Y| - \underbrace{(r(Y\cup e)-1)}_{r'(Y)} = |Y| - r'(Y) = n'(Y).$$

Ou seja, $n'(Y) = n(Y \cup e)$.

Resumindo temos

$$n'(Y) = \begin{cases} n(Y \cup e) - 1 & \text{se } e \text{ é um laço,} \\ n(Y \cup e) & \text{caso contrário.} \end{cases}$$

Além disso, temos que

$$r'(E-e) = \begin{cases} r(E-e) & = & r((E-e) \cup e) = r(E) & \text{se } e \text{ é um laço,} \\ r(E) - 1 & = & r((E-e) \cup e) - 1 & \text{caso contrário.} \end{cases}$$

Retornando a II e fazendo as substituições necessárias temos

$$II = \begin{cases} \displaystyle\sum_{Y \subseteq E-e} x^{r'(E-e)-r'(Y)} y^{n'(Y)+1} & \text{se } e \text{ é um laço,} \\ \displaystyle\sum_{Y \subseteq E-e} x^{r'(E-e)+1-(r'(Y)+1)} y^{n'(Y)} & \text{caso contrário.} \end{cases}$$

$$II = \begin{cases} y \displaystyle\sum_{Y \subseteq E-e} x^{r'(E-e)-r'(Y)} y^{n'(Y)} & \text{se } e \text{ é um laço,} \\ \displaystyle\sum_{Y \subseteq E-e} x^{r'(E-e)-r'(Y)} y^{n'(Y)} & \text{caso contrário.} \end{cases}$$

Assim,

$$II = \begin{cases} yS(M/e; x, y) & \text{se } e \text{ é um laço,} \\ S(M/e; x, y) & \text{caso contrário.} \end{cases} \tag{2.11}$$

Finalmente, substituindo as equações I e II na equação (2.9) temos

$$S(M; x, y) = \begin{cases} S(M\backslash e; x, y) & + & S(M/e; x, y) & \text{se } e \text{ não é ponte nem laço,} \\ xS(M/e; x, y) & + & S(M/e; x, y) & \text{se } e \text{ é uma ponte,} \\ S(M\backslash e; x, y) & + & yS(M/e; x, y) & \text{se } e \text{ é um laço.} \end{cases}$$

Como $M\backslash e = M/e$ se e é um laço ou uma ponte, então

$$S(M; x, y) = \begin{cases} S(M\backslash e; x, y) + S(M/e; x, y) & \text{se } e \text{ não é ponte nem laço,} \\ (x+1)S(M\backslash e; x, y) & \text{se } e \text{ é uma ponte,} \\ (y+1)S(M/e; x, y) & \text{se } e \text{ é um laço.} \end{cases}$$

Pelo **Lema 2.2**

$$S(M;x,y) = \begin{cases} S(M\backslash e;x,y) + S(M/e;x,y) & \text{se } e \text{ não é ponte nem laço,} \\ S(P;x,y)S(M\backslash e;x,y) & \text{se } e \text{ é uma ponte,} \\ S(L;x,y)S(M/e;x,y) & \text{se } e \text{ é um laço.} \end{cases}$$

Usando novamente o fato de que $M\backslash e = M/e$ quando e é um laço ou uma ponte, temos

$$S(M;x,y) = \begin{cases} S(M\backslash e;x,y) + S(M/e;x,y) & \text{se } e \text{ não é ponte nem laço,} \\ S(M(e);x,y)S(M/e;x,y) & \text{caso contrário.} \end{cases}$$

Logo $S(M;x,y)$ satisfaz as equações (2.2) e (2.3). Mas, pelo **Lema 2.1** $S(M;x,y)$ é um invariante de matróide, portanto concluimos que é um invariante T-G. ■

O próximo teorema, o principal desta secção, é um resultado de Brylawski, obtido em 1972. Ele mostra que $S(M;x,y)$ não é apenas um invariante T-G. É o invariante T-G universal. Denotaremos por $\mathcal{M}$ o conjunto de todas as matróides isomorfas e por $\mathcal{M}'$ o conjunto formado por todas as matróides não vazias.

Teorema 2.2 *Existe uma única função $t : \mathcal{M} \to \mathbb{Z}[x,y]$ com as seguintes propriedades:*

(i) $t(P;x,y) = x \quad e \quad t(L;x,y) = y$;

(ii) Se $e \in M(E)$ não é laço nem ponte, então $t(M;x,y) = t(M\backslash e;x,y) + t(M/e;x,y)$;

(iii) Se $e \in M(E)$ é um laço ou uma ponte, então $t(M;x,y) = t(M(e);x,y)t(M/e;x,y)$.

Além disso, seja R um anel comutativo e suponha que f seja uma função qualquer de $\mathcal{M}'$ em R. Se f satisfaz (2.2) *e* (2.3) *da definição de invariante T-G sempre que $|E| \geq 2$, então,*

$$f(M) = t(M; f(P), f(L))$$

para toda matróide $M \in \mathcal{M}'$.

Prova. Observe que para uma matróide $M \in \mathcal{M}$, o polinômio gerador S é uma função de $\mathcal{M}$ em $\mathbb{Z}[x,y]$. Agora, note que se fizermos $t(M;x,y) = S(M;x-1,y-1)$. Então os itens *(i),(ii)* e *(iii)* valem. De fato,
$t(P;x,y) = S(P;x-1,y-1) = x-1+1 = x$, e

$t(L;x,y) = S(L;x-1,y-1) = y-1+1 = y$.

Agora, se e não é um laço nem uma ponte de M, então

$$\begin{aligned} t(M;x,y) &= S(M;x-1,y-1) \\ &= S(M\backslash e;x-1,y-1) + S(M/e;x-1,y-1) \\ &= t(M\backslash e;x,y) + t(M/e;x,y). \end{aligned}$$

Por fim se e é um laço ou uma ponte de M

$$\begin{aligned} t(M;x,y) &= S(M;x-1,y-1) \\ &= S(M(e);x-1,y-1)S(M\backslash e;x-1,y-1) \\ &= t(M(e);x,y)t(M\backslash e;x,y). \end{aligned}$$

Agora, para mostrar a unicidade de t suponhamos que existe $t' : \mathcal{M} \longrightarrow \mathbb{Z}[x,y]$ satisfazendo as propriedades *(i),(ii)* e *(iii)* e vamos mostrar, usando indução sobre a $|E(M)|$, que $t = t'$. Para $|E(M)| = 1$ temos que M é uma ponte ou um laço. Como por hipótese t' satisfaz *(i)* temos que $t'(P;x,y) = x = t(P;x,y)$ se $M = P$; ou $t'(L;x,y) = y = t(L;x,y)$ se $M = L$. Logo, para $|E(M)| = 1$ temos $t' = t$. Suponhamos que para $1 \leq |E(M)| \leq n-1$ a igualdade seja verdadeira e seja $|E(M)| = n$. Como t' satisfaz *(ii)*, então se e não é um laço nem uma ponte temos

$$t'(M;x,y) = t'(M\backslash e;x,y) + t'(M/e;x,y).$$

Como, $|E(M\backslash e)| = n-1$. Temos, pela hipótese de indução, as seguintes igualdades

$$t'(M\backslash e;x,y) = t(M\backslash e;x,y) \quad \text{e} \quad t'(M/e);x,y) = t(M/e;x,y).$$

Portanto, $t'(M;x,y) = t(M\backslash e;x,y) + t(M/e;x,y) = t(M;x,y)$.

Por fim, se e é um laço ou uma ponte então $t'(M;x,y) = t'(M(e);x,y)t'(M\backslash e;x,y)$ pois t' satisfaz *(iii)*. Como a cardinalidade da matróide $M(e)$ é 1 e a cardinalidade de $M\backslash e$ satisfaz a hipótese de indução temos que

$$t'(M;x,y) = t(M(e);x,y)t(M;x,y) = t(M;x,y).$$

Concluimos, portanto, que $t = t'$.

Para completarmos a prova, considere $f : \mathcal{M}' \longrightarrow R$ uma função qualquer tal que sempre que $|E(M)| \geq 2$, f satisfaz as equações (2.2) e (2.3) da definição de invariantes T-G

para toda matróide $M \in \mathcal{M}$. Novamente usando indução sobre $|E(M)|$ mostraremos que $f(M) = t(M; f(P), f(L))$. Primeiro suponhamos que $|E(M)| = 2$ e que $e \in E$ não é laço nem ponte. Então $M\backslash e$ é uma ponte e M/e é um laço. Assim, $f(M\backslash e) = f(P)$ e $f(M/e) = f(L)$. Fazendo a avaliação desses valores em t, temos

$$\begin{aligned} t(M; f(P), f(L)) &= t(M; f(M\backslash e), f(M/e)) \\ &= t(M\backslash e; f(M\backslash e), f(M/e)) + t(M/e; f(M\backslash e), f(M/e)) \\ &= f(M\backslash e) + f(M/e), \text{ pois } M\backslash e \text{ é uma ponte e } M/e \text{ é um laço} \\ &= f(M), \text{pois } f \text{ satisfaz a equação (2.2).} \end{aligned}$$

Suponhamos que a igualdade se verifique para todos os valores $2 \leq |E(M)| \leq n-1$ e considere $|E(M)| = n$. Como $|E(M\backslash e)| = |E(M/e)| = n-1$ e f satisfaz (2.2) temos que

$$\begin{aligned} f(M) &= f(M\backslash e) + f(M/e) \\ &= t(M\backslash e; f(P), f(L)) + t(M/e; f(P), f(L)) \\ &= t(M, f(P), f(L)). \end{aligned}$$

Procedendo de modo análogo, mostramos que a igualdade vale também quando e é um laço ou uma ponte. ■

A função $t(M; x, y)$ é chamada de *Polinômio de Tutte* da matróide M. E da mesma forma que o polinômio gerador S, podemos escrever $t(M; x, y)$ como $\sum_i \sum_j b_{ij} x^i y^j$ onde $b_{ij} \geq 0$. Frequentemente abreviaremos esse somatório duplo por $\sum b_{ij} x^i y^j$. Além disso, segue imediatamente da prova do teorema anteiror que

$$t(M; x, y) = S(M; x-1, y-1). \tag{2.12}$$

Portanto,

$$t(M; x, y) = \sum_{X \subseteq E} (x-1)^{r(E)-r(X)} (y-1)^{n(X)}. \tag{2.13}$$

Podemos calcular o polinômio de Tutte utilizando este somatório, ou alternativamente, de forma recursiva usando os o **Teorema 2.2**. Ilustraremos esta segunda técnica no próximo exemplo.

Exemplo 2.3 *Considere a matriz A abaixo com entradas em $GF(3)$ e seja $M = M[A]$ a matróide vetorial de A.*

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

Rotulemos por $1, 2, 3, 4$ *as colunas de* A. *Dessa forma* $E(M) = \{1, 2, 3, 4\}$. *Nos cálculos a seguir abreviaremos* $t(N; x, y)$ *para* $t(N)$.

Como o elemento 1 *de* M *não é um laço nem uma ponte podemos aplicar o item (ii) do* **Teorema 2.2**. *Assim*

$$\begin{aligned}
t\left(\begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & -1 \end{bmatrix}\right) &= \underbrace{t\left(\begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & -1 \end{bmatrix}\right)}_{t(M-1)} + \underbrace{t\left(\begin{bmatrix} 1 & 1 & -1 \end{bmatrix}\right)}_{t(M/1)} \\
&= \underbrace{t\left(\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\right)}_{t(\{M-1\})-2)} + \underbrace{t([11])}_{t(\{M-1\}/2)} + \underbrace{t([1-1])}_{t(\{M/1\}-2)} + \underbrace{t([00])}_{t(\{M/1\}/2)} \\
&= t\left(\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}\right) + t([11]) + t([1-1]) + t([00]) \\
&= xt\left(\begin{bmatrix} 1 \\ 0 \end{bmatrix}\right) + \underbrace{t([-1])}_{t(\{M-1-2\}-3)} + \underbrace{t([0])}_{t(\{M-1-2\}/3)} + \underbrace{t([-1])}_{t(\{M/1-2\}-3)} + \\
&+ \underbrace{t([0])}_{t(\{M/1-2\}/3)} + yt([0]) \\
&= xx + x + y + x + y + yy \\
&= x^2 + 2x + 2y + y^2.
\end{aligned}$$

O próximo resultado relaciona o polinômio de Tutte de uma matróide M com o de sua dual M^*. Lembramos que se $X \subseteq E$, o posto de X em M^* é dado por

$$r^*(X) = |X| - r(E) + r(E - X),$$

onde r é a função posto de $M(E)$.

Proposição 2.4 *Para todas as matróides* M, $t(M^*; x, y) = t(M; y, x)$

Prova.

$$\begin{aligned}
t(M^*;x,y) &= \sum_{X\subseteq E}(x-1)^{r^*(E)-r^*(X)}(y-1)^{n^*(X)} \\
&= \sum_{X\subseteq E}(x-1)^{|E|-r(E)-(|X|-r(E)+r(E-X)}(y-1)^{|X|-r^*(X)} \\
&= \sum_{X\subseteq E}(x-1)^{|E|-|X|-r(E-X)}(y-1)^{|X|-(|X|-r(E)+r(E-X)} \\
&= \sum_{X\subseteq E}(x-1)^{|E-X|-r(E-X)}(y-1)^{r(E)+r(E-X)} \\
&= \sum_{X\subseteq E}(x-1)^{n(E-X)}(y-1)^{r(E)+r(E-X)} \\
&= \sum_{E-X\subseteq E}(y-1)^{r(E)+r(E-X)}(x-1)^{n(E-X)} \\
&= t(M;y,x)
\end{aligned}$$

■

O próximo resultado estabelece como encontrar o polinômio de Tutte de uma matróide que é a soma direta de duas matróides, sendo conhecidos os polinômios das parcelas envolvidas na decomposição.

Proposição 2.5 *Sejam $M_1(E_1)$ e $M_2(E_2)$ matróides com conjuntos básicos E_1 e E_2 disjuntos. Se $M = M_1 \oplus M_2$. Então $t(M;x,y) = t(M_1;x,y)t(M_2;x,y)$*

Prova. Sejam $E = E(M_1 \oplus M_2)$, r_1 a função posto de M_1 e r_2 a função posto de M_2. Sabemos que $r_{M_1\oplus M_2}(E) = r_1(E_1) + r_2(E_2)$ e para todo $X \subseteq E$,

$$r_{M_1\oplus M_2}(X) = r_1(X \cap E_1) + r_2(X \cap E_2).$$

Pela equação (2.13) temos que

$$t(M_1 \oplus M_2;x,y) = \sum_{X\subseteq E}(x-1)^{r_{M_1\oplus M_2}(E)-r_{M_1\oplus M_2}(X)}(y-1)^{|X|-r_{M_1\oplus M_2}(X)}$$

Calculando as expressões dos expoentes de $(x-1)$ e $(y-1)$ temos,

$$\begin{aligned}
r_{M_1\oplus M_2}(E) - r_{M_1\oplus M_2}(X) &= [r_1(E_1) + r_2(E_2)] - [r_1(X \cap E_1) + r_2(X \cap 2)] \\
&= [r_1(E_1) - r_1(X \cap E_1)] + [r_2(E_2) - r_2(X \cap E_2)].
\end{aligned}$$

Como $X = X \cap E_1 \cup X \cap E_2$ temos que $|X| = |X \cap E_1| + |X \cap E_2|$. Logo

$$\begin{aligned} |X| - r_{M_1 \oplus M_2}(X) &= |X| - [r_1(X \cap E_1) + r_2(X \cap E_2)] \\ &= |X \cap E_1| + |X \cap E_2| - r_1(X \cap E_1) - r_2(X \cap E_2) \\ &= |X \cap E_1| - r_1(X \cap E_1) + |X \cap E_2| - r_2(X \cap E_2) \end{aligned}$$

Fazendo $X_1 = X \cap E_1$ e $X_2 = X \cap E_2$, para cada $X \subseteq E$ e substituindo estes valores em t obtemos

$t(M_1 \oplus M_2; x, y) =$

$$= \sum_{X \subseteq E} (x-1)^{r_1(E_1) - r_1(X \cap E_1)} (x-1)^{r_2(E_2) - r_2(X \cap E_2)} (y-1)^{|X \cap E_1| - r_1(X \cap E_1)} (y-1)^{|X \cap E_2| - r_2(X \cap E_2)}$$

$$= \sum_{X \subseteq E} (x-1)^{r_1(E_1) - r_1(X \cap E_1)} (y-1)^{|X \cap E_1| - r_1(X \cap E_1)} (x-1)^{r_2(E_2) - r_2(X \cap E_2)} (y-1)^{|X \cap E_2| - r_2(X \cap E_2)}$$

$$= \sum_{X_1 \subseteq E_1} (x-1)^{r_1(E_1) - r_1(X \cap E_1)} (y-1)^{|X \cap E_1| - r_1(X \cap E_1)} \sum_{X_2 \subseteq E_2} (x-1)^{r_2(E_2) - r_2(X \cap E_2)} (y-1)^{|X \cap E_2| - r_2(X \cap E_2)}$$

$$= \sum_{X_1 \subseteq E_1} (x-1)^{r_1(E_1) - r_1(X_1)} (y-1)^{|X_1| - r_1(X_1)} \sum_{X_2 \subseteq E_2} (x-1)^{r_2(E_2) - r_2(X_2)} (y-1)^{|X_2| - r_2(X_2)}$$

$$= t(M_1; , x, y) t(M_2; x, y).$$

■

Podemos observar que o item *(iii)* do **Teorema 2.2** é um caso especial desta última proposição. De fato, se $e \in E(M)$ então $(E - e) \cap e = \varnothing$. Logo se e não é laço nem ponte podemos fazer $M = (E - e) \oplus e$ e daí

$$t(M; x, y) = t(M(E-e) \oplus e; x, y) = t(M \backslash e; x, y) t(M(e); x, y) = t(M \backslash e; x, y) t(M(e); x, y).$$

Como consequência desta observação, temos que o referido item pode ser substituido pela proposição anterior no enunciado do **Teorema 2.2**.
O resultado seguinte caracteriza todos os invariantes T-G generalizados e é uma extensão do **Teorema 2.2**.

Corolário 2.6 *Sejam σ e τ elementos não nulos de um corpo F. Existe uma única função t' de $\mathcal{M}$ no anel de polinômios $\mathbb{F}[x, y]$ com as seguintes propriedades.*

(i) $t'(P;x.y) = x$ *e* $t'(L;x,y) = y$;

(ii) Se $e \in M$ *não é laço nem ponte, então* $t'(M;x,y) = \sigma t'(M\backslash e;x,y)+\tau t'(M/e;x,y)$;

(iii) Se $e \in M$ *é laço ou ponte, então* $t'(M;x,y) = t'(M(e);x,y)t'(M\backslash e;x,y)$.

Além disso, t' *é dada por*

$$t'(M;x,y) = \sigma^{|E|-r(E)}\tau^{r(E)}t\Big(M;\frac{x}{\tau},\frac{y}{\sigma}\Big).$$

Prova. Primeiro vamos mostrar que para toda matróide $M \in \mathcal{M}$

$$t'(M;x,y) = \sigma^{|E|-r(E)}\tau^{r(E)}t\Big(M;\frac{x}{\tau},\frac{y}{\sigma}\Big)$$

satisfaz as propriedades de *(i)* a *(iii)*. Com efeito, para as matróides P e L temos

$$t'(P;x,y) = \sigma^{|P|-r(P)}\tau^{r(P)}t\Big(P;\frac{x}{\tau},\frac{y}{\sigma}\Big) = \sigma^0\tau^1\frac{x}{\tau} = x$$

e

$$t'(L;x,y) = \sigma^{|L|-r(L)}\tau^{r(L)}t\Big(L;\frac{x}{\tau},\frac{y}{\sigma}\Big) = \sigma^1\tau^0\frac{y}{\sigma} = y$$

Portanto *(i)* é satisfeita. Agora, se $e \in E(M)$ não é um laço nem uma ponte, temos

$$\begin{aligned} t'(M\backslash e;x,y) &= \sigma^{|E-e|-r(E-e)}\tau^{r(E-e)}t\Big(M\backslash e;\frac{x}{\tau},\frac{y}{\sigma}\Big) \\ &= \sigma^{|E|-1-r(E)}\tau^{r(E)}t\Big(M\backslash e;\frac{x}{\tau},\frac{y}{\sigma}\Big) \end{aligned}$$

Logo,

$$t(M\backslash e;\frac{x}{\tau},\frac{y}{\sigma}) = \frac{1}{\sigma^{|E|-1-r(E)}\tau^{r(E)}}t'(M\backslash e;x,y) \tag{2.14}$$

Analogamente

$$t(M/e;\frac{x}{\tau},\frac{y}{\sigma}) = \frac{1}{\sigma^{|E|-r(E)}\tau^{r(E)-1}}t'(M/e;x,y). \tag{2.15}$$

Sabemos que quando e não é laço nem ponte

$$t(M;x,y) = t(M\backslash e;x,y) + t(M/e;x,y).$$

Então

$$t'(M;x,y) = \sigma^{|E|-r(E)}\tau^{r(E)}\Big[t(M-e;\frac{x}{\tau},\frac{y}{\sigma}) + t(M/e;\frac{x}{\tau},\frac{y}{\sigma})\Big]$$

Substituindo as igualdades (2.14) e (2.15) obtemos

$$t'(M;x,y) = \frac{1}{\sigma^{-1}} t\Big(M-e;\frac{x}{\tau},\frac{y}{\sigma}\Big) + \frac{1}{\tau^{-1}} t\Big(M/e;\frac{x}{\tau},\frac{y}{\sigma}\Big)$$

Portanto

$$t'(M;x,y) = \sigma t'(M\backslash e;x,y) + \tau t'(M/e;x,y)$$

e então t' satisfaz *(ii)*. Finalmente consideremos o caso em que $e \in M$ é um laço ou uma ponte. Neste caso temos,

$$t'(M;x,y) = \sigma^{|E|-r(E)}\tau^{r(E)}\Big[t\Big(M(e);\frac{x}{\tau},\frac{y}{\sigma}\Big)t\Big(M\backslash e;\frac{x}{\tau},\frac{y}{\sigma}\Big)\Big]$$

Agora observemos que

$$|E|-r(E) = \begin{cases} |E-e|+1-r(E-e) &= 1+[|E-e|-r(E-e)] & \text{se } e \text{ é um laço} \\ |E-e|+1-[r(E-e)-1] &= |E-e|-r(E-e) & \text{se } e \text{ é uma ponte} \end{cases}$$

Assim

$$t'(M;x,y) = \begin{cases} \dfrac{y}{\sigma}\sigma^{1+[|E-e|-r(E-e)]}\tau^{r(E-e)}t(M-e;\dfrac{x}{\tau},\dfrac{y}{\sigma}) & \text{se } e \text{ é laço} \\ \dfrac{x}{\tau}\sigma^{|E-e|-r(E-e)}\tau^{r(E-e)+1}t(M\backslash e;\dfrac{x}{\tau},\dfrac{y}{\sigma}) & \text{se } e \text{ é ponte} \end{cases}$$

$$t'(M;x,y) = \begin{cases} yt'(M\backslash e;x,y) & \text{se } e \text{ é laço} \\ xt'(M\backslash e;x,y) & \text{se } e \text{ é ponte} \end{cases}$$

Logo $t'(M;x,y) = t'(M(e);x,y)t'(M\backslash e;x,y)$ e portanto (iii) é satisfeita. Resta então mostrar a unicidade de t'. Mas esta segue direto da unicidade de t. ■

O **Teorema 2.2** e o **Colorário 2.6** caracterizam invariantes T-G que são determinados simplesmente a partir do polinômio de Tutte. Os invariantes de matróides que podem ser determinados a partir deste polinômio, são especificamente aquelas funções $f : \mathcal{M} \longrightarrow \Omega$, onde Ω é um conjunto arbitrário, tais que $f(M) = f(N)$ sempre que M e N têm o mesmo polinômio de Tutte. Tais funções são chamadas *invariantes de Tutte*. Portanto, todos os invariantes T-G e invariantes T-G generalizados são exemplo de invariantes de Tutte. Outros exemplos de invariantes de Tutte são o posto e a nulidade

de uma matróide M. De fato,

$$t(M;x,y) = S(M;x-1,y-1) = \sum_{X\subseteq E}(x-1)^{r(E)-r(X)}(y-1)^{n(X)}.$$

Logo,

$$r(M) \text{ é a maior potência de } x \text{ em } t(M;x,y) \tag{2.16}$$

$$n(M) \text{ é a maior potência de } y \text{ em } t(M;x,y) \tag{2.17}$$

Portanto, se M e N são matróides que possuem o mesmo polinômio de Tutte então $r(M) = r(N)$ e $n(M) = n(N)$. Além do mais, como $|E| = r(M) + n(M)$, temos que a cardinalidade do conjunto básico também é um invariante de Tutte.

2.3 Algumas Aplicações Básicas

O próximo resultado contém algumas aplicações básicas de invariantes T-G generalizados e invariantes de Tutte. Dada uma matróide M, denotaremos por $b(M)$, $i(M)$ e $s(M)$ o número de bases, conjuntos independentes e conjuntos geradores, respectivamente, de M.

Proposição 2.7 *Seja M uma matróide com polinômio de Tutte $t(M;x,y)$. Então:*

(i) $b(M) = t(M;1,1) = S(M;0,0)$;

(ii) $i(M) = t(M;2,1) = S(M;1,0)$;

(iii) $s(M) = t(M;1,2) = S(M;0,1)$;

(iv) $2^{|E|} = t(M;2,2) = S(M;1,1)$.

Prova. Seja e um elemento da matróide M e suponha que $e \in E(M)$ não é laço nem ponte. Particionemos o conjunto $\mathcal{B}$ de bases de M nos subconjuntos $\mathcal{B}'$ e $\mathcal{B}''$ cada um com a seguinte propriedade:

$\mathcal{B}' = \{B \in \mathcal{B} : e \notin B\}$

$\mathcal{B}'' = \{B \in \mathcal{B} : e \in B\}$.

Definido desta forma $\mathcal{B}' = \mathcal{B}(M\backslash e)$ o que implica $|\mathcal{B}'| = b(M\backslash e)$. E como por definição $\mathcal{B}(M/e) = \{B - e : B \in \mathcal{B}''\}$ temos então que $|\mathcal{B}''| = |\mathcal{B}(M/e)| = b(M/e)$. Logo, se e não é laço nem ponte

$$b(M) = |\mathcal{B}'| + |\mathcal{B}''| = b(M\backslash e) + b(M/e).$$

Por outro lado, se e é um laço ou uma ponte, como $M\backslash e = M/e$ temos que $b(M\backslash e) = b(M/e)$ e então $b(M) = b(M(e))b(M\backslash e)$, já que $b(M(e)) = 1$. Logo, $b(M)$ satisfaz os itens (2.2) e (2.3) da definição de invariantes T-G e pelo **Teorema 2.2**

$$b(M) = t(M; b(P), b(L)) = t(M; 1, 1) = S(M; 0, 0).$$

Portanto *(i)* vale.

Usando o mesmo raciocínio anterior para $e \in E(M)$ que não é laço nem ponte mostramos que $i(M) = i(M\backslash e)+i(M/e)$. Agora se $e \in E(M)$ é um laço temos que $i(M) = i(M\backslash e)$ pois e não pertence a nenhum independente de M. Além disso, como o $\varnothing$ é o único conjunto independente de L, temos que $i(L) = 1$. Já se e é uma ponte então $I - e$ é independente para cada independente I de M. Logo $i(M) = 2i(M\backslash e)$. Além do mais $i(P) = 2$ pois o $\varnothing$ e $\{e\}$ são os conjuntos independentes de P. Portanto se e é laço ou ponte $i(M) = i(M(e))i(M\backslash e)$. Logo $i(M)$ é um invariante T-G. Pelo **Teorema 2.2**, temos que

$$i(M) = t(M; i(P), i(L)) = t(M, 2, 1) = S(M, 1, 0).$$

Para provar *(iii)* observemos primeiro que $S(M) = i(M^*)$. Com efeito, dado $X \subseteq E(M)$, X é um gerador de $E(M)$ se e somente se $E - X$ é independente em M^*. Logo existe uma correspondência biunívoca entre $\mathcal{S}(M)$, o conjunto dos geradores de M, e $\mathcal{I}(M^*)$. Deste modo $|\mathcal{S}(M)| = |\mathcal{I}(M^*)|$ e portanto $s(M) = i(M^*)$. Agora por *(ii)* e pela **Proposição 2.4** temos

$$\begin{aligned} s(M) = i(M^*) &= t(M^*; 2, 1) \\ &= t(M; 1, 2) \\ &= S(M; 0, 1). \end{aligned}$$

Finalmente, para provar *(iv)* usaremos o fato que $t(M; x, y) = S(M; x, y)$ e avaliaremos t em $x = y = 2$. Ou seja

$$\begin{aligned} t(M; 2, 2) &= S(M; 1, 1) \\ &= \sum_{X \subseteq E} 1^{r(E)-r(X)} 1^{n(X)} \\ &= \sum_{X \subseteq E} 1, \forall X \subseteq E \\ &= 2^{|E|}. \end{aligned}$$

■

Podemos observar do item *(i)* dessa última proposição que o número de bases de uma matróide M é dado pela soma dos coeficientes de seu polinômio de Tutte. De fato, $b(M) = t(M;1,1) = \sum_i \sum_j b_{ij}$.

Considere o M a matróide ciclo do grafo da Figura 1.2, o polinômio de Tutte dessa matróide é

$$t(M;x,y) = x^3y + x^2y + x^2y^2 + xy^2 + xy^3.$$

Calculando $t(M;1,1)$ e $t(M;2,2)$ obtemos

$$t(M;1,1) = 1 + 1 + 1 + 1 + 1 = 5$$

que é o número de bases de M e

$$t(M;2,2) = 16 + 16 + 8 + 8 + 16 = 64$$

que é igual a $2^6 = 2^{|E|}$.

Capítulo 3

Aplicações aos Códigos Lineares

Neste capítulo, abordaremos os trabalhos de Greene, Dowling, Jaeger & Rosenstiehl e Read que aplicaram técnicas Tutte-Grothendieck à vários problemas relacionados aos códigos lineares. Nas primeiras seções daremos algumas definições e resultados básicos de Teoria dos Códigos, observamos como podemos associar uma matróide a um dado código linear e por fim apresentamos algumas aplicações do Polinômio de Tutte aos Códigos Lineares e a relação entre estes e o problema crítico para matróides.

3.1 Códigos Lineares

Nesta secção faremos uma breve introdução aos códigos lineares dando algumas definições básicas e apresentando alguns resultados importantes para este trabalho. As definições e resultados enunciados nesta seção podem ser encontrados em Hefez[4] e Berlekamp[6]. Durante o processo de armazenamento ou transmissão de dados por um canal de comunicação, ocorrem erros que não podemos prever. Isso ocorre devido a própria natureza do canal de comunicação. A Teoria dos Códigos se preocupa em detectar e até corrigir esses erros. Logo se faz necessário a construção de códigos que possam corrigir erros aleatórios. Esses tipos de códigos são chamados de *códigos corretores de erros*. Os códigos desse tipo mais utilizados na prática são os códigos lineares.

3.1.1 Definições e resultados elementares

Denotaremos por K um corpo finito com q elementos, o qual chamaremos *alfabeto*. Assim, para cada número natural n, temos um espaço vetorial K^n de dimensão n. Tomaremos q como sendo a potência de um número primo p, ou seja, $q = p^s$, para algum $s \in \mathbb{Z}^+$. Assim obtemos $K = GF(q)$, o corpo de Galois de q elementos.

Um *código linear* C ou um $[n, r]-$código linear sobre K é um subespaço vetorial de dimensão r do espaço vetorial K^n.

Chamamos r e n de *dimensão* e *comprimento* de C, respectivamente. Cada vetor $x \in C$, é chamado de *palavra-código* ou simplesmente de palavra. Desse modo, como $C \subseteq K^n$ temos que cada palavra-código de C é uma n-upla. A quantidade de palavras que um $[n, r]-$código linear C sobre K possui é dada por $|C| = q^r$. Com efeito, se $\{v_1, v_2, ..., v_r\}$ é uma base de C, então todo elemento de C se escreve de modo único na forma

$$\lambda_1 v_1 + \lambda_2 v_2 + ... + \lambda_r v_r,$$

onde cada λ_i, $i = 1, 2, ..., r$ é um dos q elementos de K.

Uma matriz G do tipo $r \times n$ com entradas em K e cujas linhas formam uma base de C é chamada uma *matriz geradora* de C.

Exemplo 3.1 *A matriz abaixo é uma matriz geradora de um* [7,4]*-código linear sobre* $GF(2)$.

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

Uma das vantagens de definirmos um código linear C em termos de sua matriz geradora é que com esta matriz precisamos guardar apenas k palavras-código, ao contrário das q^k palavras que compõem o código C.

Dizemos que dois códigos de comprimento n são *linearmente equivalentes* se e somente se, cada um deles pode ser obtido do outro mediante uma sequência de operações do tipo:

(i) multiplicação dos elementos numa dada posição fixa por um escalar não nulo em todas as palavras-código.

(ii) Permutações das posições coordenadas de todas as palavras-código, mediante uma permutação fixa de $\{1, 2, ..., n\}$.

Assim, para cada código linear C existe um código equivalente C' que tem uma matriz geradora na forma

$$G = [I_r|A]$$

sendo I_r é a $r \times r$ matriz identidade e A é uma $r \times (n-r)$ matriz.
Definimos o *código dual* C^* de C, por

$$C^* = \{v \in K^n; v \cdot u = 0, \text{ para todo } u \in C\}$$

onde $v \cdot u$ representa o produto interno canônico em K^n. Ou seja, $v \cdot u = \sum_{i=1}^{n} v_i u_i$. Sabemos da Àlgebra Linear que o conjunto C^* é um subespaço vetorial de dimensão $n-r$ de K^n. Portanto, C^* é um [n,n-r]-código linear. Além disso, se $G = [I_r|A]$ é uma matriz geradora de C então

$$H = [-A^T|I_{n-r}] \tag{3.1}$$

é uma matriz geradora para C^* e é chamada de *matriz teste de paridade* de C. A proposição a seguir nos permite caracterizar os elementos de um código linear C por uma condição de anulamento.

Proposição 3.2 *Seja C um código linear e suponhamos que H seja uma matriz geradora de C^*. Temos que*

$$v \in C \text{ se e somente se } Hv^T = 0.$$

Dados um código C com matriz teste de paridade H e um vetor $v \in K^n$, chamamos o vetor Hv^T de *síndrome* de v. A síndrome de um vetor Hv^T é muito importante na *decodificação*, que é o procedimento de detecção e correção de erros num determinado código. Dado o código C que tem como matriz geradora a matriz G do exemplo anterior podemos obter sua matriz teste de paridade H, usando a expressão (3.1). Assim,

$$H = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

Seja $v = (v_1, v_2, ..., v_n)$ uma palavra-código de C. Definimos o *suporte* $S(v)$ de v como sendo

$$S(v) = \{i : v_i \neq 0\}.$$

O *peso de Hamming*, $w(v)$, de v é a cardinalidade de seu suporte. Ou seja,

$$w(v) = |\{i : v_i \neq 0\}|.$$

Em outras palavras podemos dizer que $w(v)$ é igual ao número de coordenadas não nulas de v.

Dimensão e comprimento são dois dos três parâmetros fundamentais associados a um código linear C. O terceiro desses parâmetros é a *distância mínima* d de C, a qual chamaremos apenas de *distância* de C. Definimos a distância d de um código linear C como sendo

$$d = min\{w(v) : v \in C - 0\}.$$

A matriz teste paridade de um código linear contém, de um maneira bastante simples, informações sobre o valor de sua distância d.

Lema 3.1 *Seja C um código linear com matriz teste de paridade H. Temos que a distância d de C é maior ou igual a s, se e somente se, quaisquer $s-1$ colunas de H são linearmente independentes.*

Proposição 3.3 *Seja H a matriz teste de paridade de um código C. Temos que a distância de C é igual a s se, e somente se quaisquer $s-1$ colunas de H são linearmente independentes e existem s colunas de H linearmente dependentes.*

Corolário 3.4 *Os parâmetros $[n, r, d]$ de um código linear satisfazem a desigualdade*

$$d \leq n - r + 1.$$

Prova. Se H é uma matriz teste de paridade de C, ela tem posto $n - r$. Como, pela proposição anterior $d - 1$ é menor ou igual ao posto de H, segue

$$d - 1 \leq n - r \Rightarrow d \leq n - r + 1$$

■

Como consequência do **Corolário 3.4** temos que dados três inteiros positivos arbitrários n, r e d, nem sempre existe um código linear que tenha parâmetros $[n, r, d]$, pois

existe uma interdependência entre eles, e um dos problemas fundamentais da teoria dos códigos é estudá-la.

3.1.2 Operações sobre Códigos

Sejam $u = (u_1, u_2, ..., u_n)$ e $v = (v_1, v_2, ..., v_n)$ palavras de um código C. Definimos a *concatenação* $u * v$ de u com v como sendo

$$u * v = (u_1, u_2, ..., u_n, v_1, v_2, ..., v_n).$$

Se C_1 e C_2 são códigos sobre o mesmo corpo $GF(q)$, então a *soma direta* $C_1 \oplus C_2$ consiste do conjunto de todas as palavras da forma $c_1 * c_2$, em que $c_1 \in C_1$ e $c_2 \in C_2$. O comprimento e a dimensão de $C_1 \oplus C_2$ são respectivamente, o comprimento de C_1 mais o de C_2 e a dimensão de C_1 mais a de C_2. Já a distância de $C_1 \oplus C_2$ é a menor entre as distâncias de C_1 e C_2.

Podemos, ainda, modificar um [n,r]-código linear C sobre K por de meio das operações *perfuração* e *encurtamento*. A operação perfuração atua no código C removendo a i-ésima coordenada de cada palavra-código de C. Como resultado obtemos um [n-1,r]-código C' sobre K. A operação encurtamento toma todas as palavras de C que têm zero na i-ésima coordenada e remove esta coordenada em cada uma dessas palavras, obtendo assim um [n-1,r-1]-código C'' sobre K. Observemos que essas operações são análogas as operações de remoção e contração de em uma matróide M.

3.1.3 O Polinômio enumerador de pesos

Seja C um código linear sobre $GF(q)$. O *Polinômio enumerador de pesos* $A(C; q, z)$ de C é definido por

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

Se denotarmos por a_i, $i = 0, 1, 2, ..., n$, o número de palavras código $v \in C$ que tem peso i, então

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

3.1.4 Exemplos de Códigos

Um dos exemplos mais simples de um código linear é um código binário, chamado de *Código de Repetição*. Este código é construido do seguinte modo. Começamos com um dígito, (0 ou 1), que são chamados de *dígitos mensagens*; e anexamos r dígitos arbitrários, que são chamados de *dígitos testes*. Assim, obtemos um código dee comprimento $n = r + 1$. Como o valor de cada dígito teste é igual ao valor do dígito mensagem, este código possue apenas duas palavras-código, que são as palavras: $(0, 0, ..., 0)$ e $(1, 1, ..., 1)$. Portanto, se denotarmos este código por C, o seu o polînômio enumerador de pesos é

$$A(z) = 1 + z^{r+1};$$

enquanto polinômio de Tutte da matriz associada $M(C)$ é dado por

$$t(M(C); x, y) = x + y + y^2 + y^3 + ... + y^{r-1} + y^r.$$

Um outro tipo de código binário muito conhecido são os *Códigos de Hamming* . Eles foram a primeira classe de códigos criados para correção de erros. Esses códigos e suas variações têm sido bastante utilizados para o controle de erros em comunicação digital e sistemas de armazenamentos de dados. Formalmente, definimos um Código de Hamming de ordem m sobre $K = GF(2)$ como sendo um código com matriz teste de paridade H_m do tipo $m \times n$, cujas colunas são os elementos de $K^n - 0$. Note, que o comprimento n de um Código de Hamming é é igual a $2^m - 1$ e sua dimensão k é igual a $2^m - m - 1$. Comumente denota-se um Código de Hamming de ordem m por $[2^m - 1, 2^m - m - 1]$-código de Hamming. A matriz do **Exemplo 3.1** é a matriz geradora de um $[7, 4]-$código de Hamming. Este código tem como polinômio enumerador de pesos, o seguinte polinômio:

$$A(z) = 1 + 7z^3 + 7z^4 + z^7.$$

Já o polinômio de Tutte da matróide associada $M(C)$ é

$$t(M(C); x, y) = x^4 + 3x^3 + 6x^2 + 3x + 7xy + 3y + 4y^2 + y^3.$$

3.2 Matróides e Códigos

Nesta secção veremos como podemos associar uma matróide vetorial a um código linear. Sejam C um [n,r]-código linear sobre $GF(q)$ e G uma matriz geradora de C. Sabemos que os conjuntos de colunas linearmente independentes de G são os conjuntos independentes de uma matróide representável, a matróide vetorial $M[G]$ de G. Podemos notar que que a matróide $M[G]$ não depende da matriz G e sim do código C. Com efeito, sendo G uma matriz geradora de C, efetuando-se operações elementares linha sobre G obtemos uma certa relação de equivalência sobre o conjunto das matrizes $r \times n$ com entradas em $GF(q)$; onde cada uma dessas classes de matrizes corresponde à um único código linear (a menos de uma equivalência entre códigos) e a uma única matróide vetorial (a menos de isomorfismo) já que essas transformações, como vimos no capítulo 1, não afetam a independência linear das colunas de G. Dessa forma, dado um código linear C com matriz geradora G, podemos associar-lhe uma matróide, que é a matróide vetorial $M[G]$ a qual denotaremos por $M(C)$ e chamaremos de *matróide associada* ao código C.

Sabemos da teoria das matróides, que para uma matróide vetorial de uma matriz do tipo $k \times n$ na forma $[I_k|A]$ temos $M^*[I_k|A] \cong M[-A^T|I_{n-k}]$. Daí podemos concluir que a matróide associada a C^* é isomorfa a matróide $M^*(C)$, a dual de $M(C)$. Ou seja

$$M(C^*) \cong M^*(C).$$

Com efeito, para um [n,k]-código linear temos

$$M^*(C) = M^*[G] = M^*[I_k|A] = M[-A^T|I_{n-k}].$$

Por outro lado,

$$M(C^*) = M[H] = M[-A^T|I_{n-k}].$$

Proposição 3.5 *seja $M(C)$ a matróide associada a um código linear C com distância d. Então, $M(C)$ tem um cocircuito minimal de cardinalidade d.*

Prova. Pela **Proposição 3.3**, dado um código linear C com distância d, quaisquer conjunto com $d-1$ colunas da matriz teste de paridade é linearmente independente e existem d colunas linearmente dependentes. Segue que $M(C^*)$ tem um circuito de

cardinalidade d e portanto $M(C)$ tem um corcircuito de cardinalidade d. Além disso, não existem em H conjuntos com menos de $d-1$ colunas linearmente dependentes. Logo $M(C^*)$ não possui circuitos com menos de d elementos e o resultado segue. ■

Proposição 3.6 *Seja C um $[n,k,d]$-código linear e seja $M(C)$ sua matróide associada com polinômio de Tutte $t(M(C))$. Então*

$$d = n - k + 1 - \textit{máx}\{j; b_{ij} > 0 \textit{ para algum } i > 0\}.$$

Onde b_{ij} é um coeficiente do polinômio de Tutte de $M(C)$.

Prova. Sejam M uma matróide arbitrária e X um circuito minimal de M. Sabemos que o polinômio gerador associado ao posto de M é

$$S(M(C); x, y) = \sum_{X \subseteq E} x^{r(E)-r(X)} y^{|X|-r(X)} = \sum_i \sum_j a_{ij} x^i y^j.$$

Como X é um circuito, então $n(X) = 1 > 0$. Do fato de X ser minimal obtemos que

$$r(E) - r(X) = \text{máx}\{r(E) - r(X); \exists X \subseteq E \quad e \quad n(X) > 0\}.$$

Observemos que as expressões $\exists X \subseteq E$ e $n(X) > 0$ podem ser substituídas por $a_{ij} > 0$ e $j > 0$, respectivamente. Assim, obtemos a seguinte expressão:

$$r(E) - r(X) = \text{máx}\{i; a_{ij} > 0 \,\text{para algum}\, j > 0\}$$

Como $t(M; x, y) = S(M; x-1, y-1)$, podemos reescrever esta expressão do seguinte modo:

$$r(E) - r(X) = \text{máx}\{i; b_{ij} > 0 \,\text{para algum}\, j > 0\}.$$

Usando a **Proposição 2.4** obtemos para a matróide dual de M, na qual X é um corcircuito minimal de M, a seguinte expressão:

$$r^*(E) - r^*(X) = \text{máx}\{j; b_{ij} > 0 \,\text{para algum}\, i > 0\}$$

Mas, $r^*(E) = n - k$ e $r^*(X) = d - 1$. Logo,

$$n - k - (d-1) = \text{máx}\{j; b_{ij} > 0 \,\text{para algum}\, i > 0\}$$

e então,

$$d = n - k + 1 - \text{máx}\{j; b_{ij} > 0 \,\text{para algum}\, i > 0\}.$$

■

Já vimos que o polinômio de Tutte da matróide M associada ao $[7,4]-$código de Hamming é $t(M(C);x,y) = x^4+3x^3+6x^2+3x+7xy+3y+4y^2+y^3$. Como neste polinômio o único termo não nulo envolvendo as inderterminadas x e y simultaneamente é $7xy$ então, máx$\{j; b_{ij} > 0 \,\text{para algum}\, i > 0\} = 1$. Logo, pela **Proposição 3.6**, obtemos $d = 7-4+1-1 = 3$. Portanto, a distância mínima do $[7,4]-$código de Hamming é 3.

3.3 Aplicações

Nesta secção faremos algumas aplicações das técnicas T-G aos códigos lineares. A partir de agora convencionaremos que se W é um susbespaço vetorial de K^n, então denotaremos por W_0 o subespaço consistindo de todos os vetores em W que têm a primeira coordenada nula; $\widehat{W}$ denotará o espaço vetorial obtido de W removendo-se a primeira coordenada de cada vetor. Assim, quando $W_0 = W$ teremos $\widehat{W_0} = \widehat{W}$.

3.3.1 A relação entre A(C;q,z) e t(M(C))

O resultado seguinte, o qual segundo Brylawski & Oxley[1], é uma das mais profundas aplicações de técnicas T-G, foi obtido por Greene[10] em 1976 e mostra que a distribuição de pesos das palavras-código de um código linear é um invariante T-G generalizado.

Teorema 3.7 *Seja $A(C;q,z)$ o polinômio enumerador de pesos de um [n,r]- código linear C sobre $GF(q)$, cuja matróide associada é $M(C)$. Então:*

$$A(C;q,z) = (1-z)^r z^{n-r} t\Big(M(C); \frac{1+(q-1)z}{1-z}, \frac{1}{z}\Big).$$

Prova. Seja $f(M(C)) = A(C;q,z)$. Usaremos a indução sobre o comprimento de C para mostrar que f está bem definida e é um invariante T-G generalizado para o qual $\sigma = z$ e $\tau = 1-z$. Primeiro vamos mostrar que f está bem definida quando C tem comprimento $n = 1$. Neste caso a matróide $M(C)$ é composta de um único elemento e. Logo $M(C)$ é um laço ou uma ponte. Seja e um laço, então C tem uma única palavra código, que é o zero. Daí

$$A(C;q,z) = a_0 z^0 = 1.$$

Agora, suponha que e é uma ponte. Então C possui $q-1$ palavras-código não nulas de peso 1 mais a palavra nula. Assim, temos

$$A(C;q,z) = a_0 z^0 + a_1 z^1 = 1 + (q-1)z.$$

Portanto, concluimos que se C tem comprimento $n = 1$ então

$$f(M(C)) = \begin{cases} 1, & \text{se M(C) é um laço,} \\ 1 + (q-1)z, & \text{se M(C) é uma ponte.} \end{cases}$$

Suponhamos que f está bem definida para todo C com comprimento menor que n e suponha que C tem comprimento n, onde $n \geq 2$. Sejam G uma matriz geradora de C e $e \in E(M(C))$ tal que e não é um laço nem uma ponte. Sem perda de generalidade, podemos assumir que e corresponde a primeira coluna de G e que G seja uma matriz da forma $[I_r|A]$. Considere $\widehat{G}_0$ a matriz obtida de G removendo a primeira linha e a primeira coluna de G. Notemos que $M[\widehat{G}_0] = M[G]/e$. Considere ainda $\widehat{G}$ a matriz obtida de G removendo-se a primeira coluna de G. Temos que $M[\widehat{G}] = M[G]\backslash e$. Note ainda que $\widehat{G}_0$ e $\widehat{G}$ são matrizes geradoras de $\widehat{C}_0$ e $\widehat{C}$, respectivamente. Daí, temos que

$$M(\widehat{C}_0) = M(C)/e \quad e \quad M(\widehat{C}) = M(C)\backslash e \tag{3.2}$$

Afirmamos que

$$|C - C_0| = |\widehat{C} - \widehat{C}_0|. \tag{3.3}$$

Com efeito, considere agora a aplicação

$$g : C - C_0 \to \widehat{C} - \widehat{C}_0$$

definida por $g((v_1, v')) = v'$, ou seja g remove a primeira coordenada de cada palavra-código de $C - C_0$. Vamos mostrar que g é uma bijeção. Primeiro note que dado $v' \in \widehat{C} - \widehat{C}_0$, existe $v \in GF(q)$ tal que $(v, v') \in C - C_0$. Logo g é sobrejetora. Além, disso dados $u_1, v_1 \in GF(q)$, não nulos, com $u_1 \neq v_1$, temos que $(u_1, v'), (v_1, v') \in C - C_0$ são tais que $(u_1, v') \neq (v_1, v')$ e no entanto $g((u_1, v')) = v' = g((v_1, v'))$. Mas, neste caso $u_1 \neq v_1$ implica em $(u_1 - v_1, 0) \in C$. O que é um absurdo. Pois, deste modo, e seria uma ponte em $M(C)$. Logo g é injetora e portanto bijetora. Por definição,

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

$$\begin{aligned}
A(C) &= \sum_{(v_1,v')\in C_0} z^{w((v_1,v'))} + \sum_{(v_1,v')\in C-C_0} z^{w((v_1,v'))} \\
&= \sum_{v'\in \widehat{C}_0} z^{w(v')} + \sum_{(v_1,v')\in C-C_0} z^{w(v')+1} \\
&= \sum_{v'\in \widehat{C}_0} z^{w(v')} + z \sum_{(v_1,v')\in C-C_0} z^{w(v')} \quad \text{por (3.3) temos,} \\
&= \sum_{v'\in \widehat{C}_0} z^{w(v')} + z \sum_{v'\in \widehat{C}-\widehat{C}_0} z^{w(v')} \\
&= \sum_{v'\in \widehat{C}_0} z^{w(v')} + z\Big[\sum_{v'\in \widehat{C}} z^{w(v')} - \sum_{v'\in \widehat{C}_0} z^{w(v')}\Big] \\
&= z\sum_{v'\in \widehat{C}} z^{w(v')} + (1-z)\sum_{v'\in \widehat{C}_0} z^{w(v')}.
\end{aligned}$$

Portanto,

$$A(C) = zA(\widehat{C}) + (1-z)A(\widehat{C}_0). \tag{3.4}$$

Como $\widehat{C}$ e $\widehat{C}_0$ têm ambos comprimento $n-1$, segue da hipótese de indução e da equação (3.2) que

$$A(\widehat{C}) = f(M(\widehat{C})) = f(M(C)\backslash e).$$

e

$$A(\widehat{C}_0) = f(M(\widehat{C}_0)) = f(M(C)/e).$$

Então pela equação (3.4) segue que se e não é um laço nem uma ponte

$$A(C) = zf(M(C)-e) + (1-z)f(M(C)/e). \tag{3.5}$$

Agora, suponha que e é um laço de $M(C)$. Então a primeira coordenada de cada palavra-código de C é nula. Logo, $A(C) = A(\widehat{C}_0)$. Como $\widehat{C}_0$ tem comprimento $n-1$ segue da expressão (3.2),da hipótese de indução e do fato que $f(L) = 1$ que

$$A(C) = f(M(C)/e) = 1.f(M(C)/e) = f(L).f(M(C)/e) \tag{3.6}$$

Finalmente, se e é uma ponte de $M(C)$, então C é a soma direta de $\widehat{C}$ com um espaço vetorial unidimensional. Assim, se c é uma palavra código de C, então podemos escrever

$c = (v_1, v')$ onde $v' \in \widehat{C}$. Além disso, temos que $c = (0, v')$ ou $c = (v_1, v')$ onde para cada $v' \in \widehat{C}$ existem $q-1$ letras, não nulas, distintas para ocupar o lugar de v_1 em c. Assim,

$$\begin{aligned} A(C) &= \sum_{(0,v')\in C} z^{w((0,v'))} + \sum_{(v_1,v')\in C} z^{w((v_1,v'))} \\ &= \sum_{v'\in\widehat{C}} z^{w(v')} + (q-1)\sum_{v'\in\widehat{C}} z^{w(v')+1} \\ &= \sum_{v'\in\widehat{C}} z^{w(v')} + (q-1)z\sum_{v'\in\widehat{C}} z^{w(v')} \\ &= [1+(q-1)z]\sum_{v'\in\widehat{C}} z^{w(v')} \\ &= [1+(q-1)z]A(\widehat{C}). \end{aligned}$$

Como $\widehat{C}$ tem comprimento $n-1$ e $1+(q-1)z = f(P)$, segue da expressão (3.2) e da pela hipótese de indução que

$$A(C) = f(P)f(M(C)-e). \tag{3.7}$$

Combinando as equações (3.5), (3.6) e (3.7) concluimos pela hipótese de indução sobre o comprimento de C que f está bem definida. Além disso, as mesmas equações implicam que f é um invariante T-G generalizado. Portanto,segue do **Corolário 2.6** que

$$A(C;q,z) = (1-z)^r z^{n-r} t\Big(M(C); \frac{1+(q-1)z}{1-z}, \frac{1}{z}\Big)$$

■

3.3.2 A Identidade de MacWillians

O próximo resultado é conhecido como a *Identidade de MacWilliams* para códigos lineares. Ela é fundamental para a Teoria dos Códigos por relacionar o polinômio enumerador de pesos $A(C;q,z)$ de um código linear C e o polinômio do seu dual, $A(C^*;q,z)$. Uma prova deste teorema, como a feita por MacWillians, pode ser encontrado em [6] e [14], porém utilizando o **Teorema 3.7**, faremos aqui uma prova mais simples.

Teorema 3.8 *Sejam $A(C;q,z)$ e $A(C^*;q,z)$ os polinômios enumeradores de pesos de um [n,k]-código linear sobre $GF(q)$ e do seu dual C^*, respectivamente. Então,*

$$A(C^*;q,z) = \frac{[1+(q-1)z]^n}{q^r} A\Big(C;q,\frac{1-z}{1+(q-1)z}\Big).$$

Prova. Sabemos que $dim(C^*) = n-r$ e que $M^*(C) \cong M(C^*)$. Agora, usando o **Teorema 3.7** e a **Proposição 2.4** para calcularmos $A(C^*;q,z)$ obtemos:

$$A(C^*;q,z) = (1-z)^{n-r} z^r t\Big(M(C);\frac{1}{z},\frac{1+(q-1)z}{1-z}\Big). \tag{3.8}$$

Agora façamos

$$X = \frac{[1+(q-1)z]^n}{q^r} A\Big(C;q,\frac{1-z}{1+(q-1)z}\Big) \tag{3.9}$$

Façamos também

$$\frac{1-z}{1+(q-1)z} = \lambda \Rightarrow 1+(q-1)z = \frac{1-z}{\lambda}$$

e calculemos $A(C;q,\lambda)$ usando o **teorema 3.7** novamente. Daí obtemos

$$A(C;q,\lambda) = (1-\lambda)^r \lambda^{n-r} t\Big(M(C);\frac{1+(q-1)\lambda}{1-\lambda},\frac{1}{\lambda}\Big).$$

substituindo na igualdade (3.9) temos

$$\begin{aligned} X &= \frac{\Big(\frac{1-z}{\lambda}\Big)^n}{q^r}(1-\lambda)^r\lambda^{n-r}t\Big(M(C);\frac{1+(q-1)\lambda}{1-\lambda},\frac{1}{\lambda}\Big) \\ X &= \Big(\frac{1}{\lambda}\Big)^n\frac{(1-z)^n}{q^r}(1-\lambda)^r\lambda^{n-r}t\Big(M(C);\frac{1+(q-1)\lambda}{1-\lambda},\frac{1}{\lambda}\Big) \end{aligned} \tag{3.10}$$

Agora, para facilitar nossos cálculos iremos determinar separadamente as expressões

$1-\lambda$, $\frac{1}{\lambda}$ e $\frac{1+(q-1)\lambda}{1-\lambda}$. Assim, obtemos:

$$1-\lambda = 1-\frac{1-z}{1+(q-1)z} = \frac{qz}{1+(q-1)z};$$

$$\frac{1}{\lambda} = \frac{1+(q-1)z}{1-z};$$

$$\frac{1+(q-1)\lambda}{1-\lambda} = \frac{1}{z}.$$

Substituindo os resultados obtidos na igualdade (3.10) obtemos

$$X = \Big(\frac{1+(q-1)z}{1-z}\Big)^n \frac{(1-z)^n}{q^r}\Big(\frac{qz}{1+(q-1)z}\Big)^r \Big(\frac{1-z}{1+(q-1)z}\Big)^{n-r} t\Big(M(C); \frac{1}{z}, \frac{1+(q-1)z}{1-z}\Big)$$

$$X = \frac{(1-z)^n}{[1+(q-1)z]^r} z^r \Big(\frac{1+(q-1)z}{1-z}\Big)^r t\Big(M(C); \frac{1}{z}, \frac{1+(q-1)z}{1-z}\Big)$$

$$X = (1-z)^{n-r} z^r t\Big(M(C); \frac{1}{z}, \frac{1+(q-1)z}{1-z}\Big).$$

Finalmente, combinando esta última equação com as equações (3.8) e (3.9) chegamos ao resultado desejado. Ou seja

$$A(C^*; q, z) = \frac{[1+(q-1)z]^n}{q^r} A\Big(C; q, \frac{1-z}{1+(q-1)z}\Big).$$

■

Usaremos o Código de Repetição Binário C de comprimento $n = 5$ para exemplificarmos os teoremas 3.7 e 3.8. Sabemos que neste código $q = 2$ e $r = 1$. Logo, pelo **Teorema 3.7**, temos

$$A(C; 2, z) = (1-z)^1 z^4 t\Big(M(C); \frac{1+z}{1-z}, \frac{1}{z}\Big)$$

Sabemos também, que o polinômio de Tutte da matróide associada a este código é

$$t(M(C); x, y) = x + y + y^2 + y^3 + y^4.$$

Logo,

$$\begin{aligned} A(C, 2, z) &= (1-z)^1 z^4 t\Big(M(C); \frac{1+z}{1-z}, \frac{1}{z}\Big) \\ &= (1-z)z^4\Big(\frac{1+z}{1-z} + \frac{1}{z} + \frac{1}{z^2} + \frac{1}{z^3} + \frac{1}{z^4}\Big) \\ &= (1+z)z^4 + (1-z)\Big(z^3 + z^2 + z + 1\Big) \\ &= 1 + z^5. \end{aligned}$$

Embora o Código de Repetição Binária tenha apenas duas palavras-código e portanto tenha um polinômio enumerador de pesos simples, o mesmo não ocorre com o seu dual C^*. De fato, C^* é um $[5, 4]-$código linear e portanto tem $2^4 = 16$ palavras-código. Uma

maneira de fazer a distribuição de pesos de C^* é encontrar as suas 16 palavras-código e calcular o peso de cada uma delas. No entanto, como já dispomos do polinômio enumerador de pesos do C, usaremos a Identidade de MacWillians para obtermos, de forma mais simples, o polinômio enumerador de pesos de C^*. Deste modo, usando o **Teorema 3.8**, obtemos

$$\begin{aligned} A(C^*;2,z) &= \frac{(1+z)^5}{2}A\Big(C;2,\frac{1-z}{1+z}\Big) \\ &= \frac{(1+z)^5}{2}\Big[1+(\frac{1-z}{1+z})^5\Big] \\ &= \frac{1}{2}\Big[(1+z)^5+(1-z)^5\Big] \\ &= 1+10z^2+5z^4 \end{aligned}$$

3.3.3 Relação entre o problema crítico e códigos lineares

Outro trabalho pioneiro na teoria dos invariantes de matróides de códigos lineares foi desenvolvido por Dowling [10] em 1971. Ele mostrou que um problema fundamental em Teoria dos Códigos, o de *encontrar a maior dimensão r possível para um código linear sobre $GF(q)$ de comprimento n e distância pelo menos d*, é um caso especial do problema crítico para matróides.

O problema crítico foi desenvolvido inicialmente para Teoria dos Grafos como sendo o seguinte: *encontrar o menor inteiro positivo tal que $\chi_\Gamma(\lambda) > 0$, onde $\chi_\Gamma(\lambda)$ é o polinômio cromático de um grafo Γ na indeterminada λ.* Este problema foi adaptado para matróides por Crapo e Rota[11], onde as cores foram substituídas por vetores sobre um corpo finito de ordem q e, o problema passou a ser o seguinte: *dada uma matróide vetorial M sobre $GF(q)$ encontrar o menor expoente inteiro positivo d para o qual $p(M;q^d) > 0$, onde p é o polinômio característico de M.* Seja uma E um conjunto de vetores sobre o espaço vetorial $V(n,q)$, o qual denotaremos apenas por K^n, e sejam $M(E)$ a matróide vetorial de E. Considere uma k-upla $(f_1,...,f_k)$ de funcionais lineares sobre K, ou seja

$$f_i : K^n \to K.$$

onde $i = 1, 2, ..., k$. Dizemos que uma k-upla $(f_1, ..., f_k)$ de funcionais lineares distingue E se

$$\{v \in K^n; f_i(v) = 0, \forall \quad 1 \leq i \leq k\} \cap E = \varnothing.$$

Sabemos da álgebra linear que o conjunto $\{v \in K^n; f(v) = 0\}$ é o núcleo de f o qual é denotado por $kerf$. Assim, temos que $\{v \in K^n; f_i(v) = 0, \forall \quad 1 \leq i \leq k\} = \bigcap_{i=1}^{k} kerf_i$. Logo, podemos dizer que $(f_1, ..., f_k)$ distingue E se

$$(\bigcap_{i=1}^{k} kerf_i) \cap E = \varnothing. \tag{3.11}$$

O próximo resultado fundamental é conhecido como o *Teorema Crítico* e foi obtido por Crapo e Rota em 1970. Denotaremos por $\mathcal{L}(M)$ o reticulado de conjuntos fechados da matróide $M(E)$ citada anteriorente.

Teorema 3.9 *Seja E um subespaço de dimensão m do espaço vetorial K^n, e seja d um inteiro positivo. O número de d-uplas de funcionais lineares que distinguem E é igual a $(q^d)^{n-m}p(M(E), q^d)$.*

Prova. Primeiro observemos que, dado $X \subseteq K^n$ com $dimX = s$, o número de aplicações lineares $f : K^n \to K^d$ cujo núcleo contém X é $q^{d(n-s)}$. Com efeito, dada $\{p_1, ..., p_s\}$ uma base de X podemos completá-la até obter uma base de K^n , digamos

$$\{p_1, ..., p_s, p_{s+1}, ..., p_n\}.$$

Definamos $f : K^n \to K^d$ tal que $f|_X = 0$. Assim, temos que X está contido no núcleo de f, ou seja $X \subseteq kerf$. Agora contemos quantas são as aplicações f de $K^n - X$ em K^d. Note que para cada $p_i, i = s+1, ..., n$ temos q^d possíveis valores para $f(p_i)$. Assim , pelo principio fundamental da contagem temos

$$\underbrace{q^d \times q^d \times ... \times q^d}_{n-s\, vezes} = q^{d(n-s)}.$$

Agora, para cada subconjunto F de K^n, denotemos por $v(F)$ o número de aplicações lineares $f : K^n \to K^d$ tais que $E \cap Kerf = F$. Note que $E \cap Kerf = F$ é fechado em $M(E)$. Ou seja F pertence ao reticulado de conjuntos fechados $\mathcal{L}(E)$ de $M(E)$. Temos portanto, que para cada $X \in \mathcal{L}(E)$

$$\sum_{F \geq X} v(F) = (q^d)^{n-s}$$

Fazendo a inversão de Möbius, temos que

$$v(X) = \sum_{F \geq X} \mu_E(X, F)(q^d)^{n-dimF}.$$

Fazendo $X = 0 = Cl(\varnothing)$, temos

$$v(0) = \sum_{F \in L(E)} \mu_E(0, F)(q^d)^{n-dimF}$$

$$v(0) = \sum_{F \in L(E)} \mu_E(0, F)(q^{d(n-dimF)}$$

Como $dimF = m + (-m + dimF)$, temos que

$$q^{d.n}q^{-d.dimF} = q^{d.n}q^{-d.m}q^{d.m}q^{-d.dimF} = (q^d)^{n-m}(q^d)^{m-dimF}.$$

E daí,

$$v(0) = \sum_{F \in L(E)} \mu_E(0, F)(q^d)^{n-m}(q^d)^{m-dimF}$$

Como, m,n e d são constantes, segue que

$$v(0) = (q^d)^{n-m} \sum_{F \in L(E)} \mu_E(0, F)(q^d)^{m-dimF}$$

$$v(0) = (q^d)^{n-m} \sum_{F \in L(E)} \mu_E(0, F)(q^d)^{dimE-dimF}.$$

Logo,

$$v(0) = (q^d)^{n-m} p(M(E), q^d).$$

Portanto, concluimos que o número de funcionais lineares f tais que $E \cap Kerf = \varnothing$ é igual a $(q^d)^{n-m}p(M(E), q^d)$. No caso em que o vazio não é fechado, ou seja, $M(E)$ tem um laço, temos que $E \cap Kerf \neq \varnothing$, e portanto não existe um conjunto de funcionais distinguindo E. ■

Segue do teorema crítico que para uma matróide $M(E)$, $p(M(E), q^k) \geq 0, \forall \quad k \in \mathbb{Z}^+$.

Seja M uma matróide vetorial. O expoente crítico $c(M; q)$ de M é definido por

$$c(M; q) = \begin{cases} \infty & \text{se M tem um laço} \\ \text{mín}\{j \in \mathbb{N}; p(M; q^j) > 0\} & \text{do contrário} \end{cases}$$

Segue do teorema crítico que

$$c(M; q) = \text{mín}\{j \in \mathbb{N}; p(M; q^k) > 0, \text{para todo inteiro}\, k \geq j\}.$$

Sabemos da Álgebra Linear que o núcleo de um funcional linear é um hiperplano. Logo temos o seguinte

Corolário 3.10 *Seja $E - \{0\}$ um subconjunto não vazio de um espaço vetorial K^n. Então,*

$$\begin{aligned} c(M;q) &= \textit{mín}\{j \in \mathbb{N}; K^n \textit{tem hiperplanos } H_1, H_2, ..., H_n \textit{ tais que } \left(\bigcap_{i=1}^{j} H_i\right) \cap E = \varnothing\}. \\ &= \textit{mín}\{j \in \mathbb{N}; K^n \textit{ tem um subespaço de dimensão } \ n-j \textit{ que tem intersecção} \\ &\quad \textit{vazia com } E\}. \end{aligned}$$

Chamamos de bola perfurada de Hamming, $H_q(n, d-1)$, ao conjunto de todos os vetores não nulos de $V(n,q)$, tais que o número de coordenadas não nulas é menor ou igual a d. Ou seja,

$$H_q(n, d-1) = \{v \in V(n,q); 0 < w(v) \leq d\}.$$

Proposição 3.11 *C é um código linear de comprimento n e dimensão máxima, com distância pelo menos d, se e somente se, C é um subespaço de $V(n,q)$ de dimensão máxima que não contém nenhum membro de $H_q(n, d-1)$.*

Prova. $C = \{v \in V(n,q); w(v) \geq d\} \cup \{0\} \Longleftrightarrow C \cap H_q(n, d-1) = \varnothing$. ■

A proposição acima nos permite concluir que o problema de encontrar a dimensão máxima de um código linear com distância maior ou igual a d é equivalente ao problema de encontrar o expoente crítico da matróide vetorial sobre $H_q(n, d-1)$. Enunciamos este fato no seguinte teorema:

Teorema 3.12 *Seja r a dimensão máxima de um código linear sobre $GF(q)$ de comprimento n e distância maior ou igual a d e seja c o expoente crítico da matróide vetorial sobre $H_q(n, d-1)$. Então $r = n - c$.*

Prova. Seja M a matróide vetorial sobre $H_q(n, d-1)$ e c o seu expoente crítico. Pelo **Corolário 3.10**

$$c = \text{mín}\{j \in \mathbb{N}; V(n,q) \text{ tem um subespaço } W \text{ de dimensão } n-j \text{ tal que } W \cap H_q(n, d-1) = \varnothing\}.$$

Como $C \cap H_q(n, d-1) = \varnothing$. Segue que $r = n - c$. ■

Seja $\{v_1, v_2, ..., v_n\}$ uma base do espaço vetorial $V(n,q)$ e denote por $GF(q)^*$ o grupo

multiplicativo de $GF(q)$, ou seja, $GF(q) - \{0\}$. Chamamos de geometria de Dowling, e denotamos, por $Q_n(GF(q)^*)$, a matróide simples de posto n , obtida restringindo-se a matróide sobre $V(n,q)$ ao conjunto

$$\{v_1, v_2, ..., v_n\} \cup \{v_i + \alpha v_j; 1 \leq i < j \leq n \,\mathrm{e}\, \alpha \in GF(q)^*\}.$$

Proposição 3.13 *Seja $G_q(n, d-1)$ a simplificação da matróide sobre $H_q(n, d-1)$. Então $G_q(n,2) = Q_n(GF(q)^*)$.*

Prova. De fato,

$$\begin{aligned} G_q(n,2) &= \{v \in V(n,q); 0 < w(v) \leq 2\} \\ &= \{v_1, v_2, ..., v_n\} \cup \{v_i + \alpha v_j \,; 1 \leq i < j \leq n \, e \, \alpha \in GF(q)^*\} \\ &= Q_n(GF(q)^*). \end{aligned}$$

■

Uma maneira de resolver o problema crítico para códigos lineares é calcular explicitamente o polinômio característico da matróide de Dowling. $G(m,n)$. Mas, em geral isso não é fácil, exceto nos casos onde $m = 1, 2, n-1$. Como referência para um estudo mais aprofundado dos resultados originados do trabalho de Dowling, indicamos [7] e [10].

3.3.4 Uma aplicação aos códigos binários

O Próximo resultado é um invariante T-G para códigos binários. Este invariante foi descoberto para grafos por Rosenstiehl e Read [13] em 1978, e Jaeger [12] em 1989 notou que poderia ser extendido para matróides binárias.

Teorema 3.14 *Seja C um código binário de comprimento n. Então,*

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

Além disso, $|tM(C); -1, -1)| = |C \cap C^*|$.

Prova. Seja $h(M(C)) = (-1)^{n(C)}(-2)^{dim(C \cap C^*)}$. Usaremos a indução sobre o comprimento $n(C)$ de C para mostrar que h é um invariante T-G bem definido. No caso $n(C) = 1$, temos que a matriz geradora de C possui uma única coluna e portanto a matróide $M(C)$ é um laço ou uma ponte. Se $M(C)$ é um laço, então o código C é

formado apenas pela palavra-código nula. Logo $C \cap C^* = \{0\}$. Agora, se $M(C)$ é uma ponte, então $M^*(C)$ é uma laço e neste caso o código dual de C é quem é formado apenas da palavra-código nula; e novamente temos $C \cap C^* = \{0\}$. Logo se $M(C)$ é um laço ou uma ponte, temos $C \cap C^* = \{0\}$ e portanto $dim C \cap C^* = \{0\}$ e

$$h(M(C)) = (-1)^1(-2)^0 = -1.$$

Por outro lado, sabemos que para as matróides L e P que são formadas apenas por um laço e uma ponte, respectivamente; temos:

$$t(L; -1, -1) = t(P; -1, -1) = -1.$$

Logo, concluimos que para h está bem definida para $n(C) = 1$.
Vamos assumir, que h está bem definida para $n(C) < m$ e consideremos $n(C) = m \geq 2$. Daqui por diante denotaremos o conjunto $C \cap C^*$ por $B = B(C)$. Lembramos ao leitor que $\widehat{C}$ denota o código obtido removendo a primeira coordenada em cada palavra-código de C e C_0 denota o código formado pelas palavras-código de C que tem primeira coordenada nula.
Seja e um elemento da matróide associada a C que não seja um laço nem uma ponte. Vamos assumir, sem perda de generalidade, que e corresponde a primeira coluna de uma matriz geradora de C. Note que que se $v \in \widehat{C}$, então

$$(1, v) \text{ e } (0, v) \text{ não pertencem simultaneamente a } C. \tag{3.12}$$

Pois, do contrário $(1, v) + (0, v) = (1, 0) \in C$. Assim, e seria uma ponte de $M(C)$. O que seria uma contradição. Agora observe que

$$B = B_0 \text{ ou para algum vetor } x \text{ com primeira coordenada 1, } B = B_0 + \langle x \rangle. \tag{3.13}$$

De fato, se para todo $x \in \widehat{B}$ tivermos $(0, x) \in C$ então todos os vetores de B devem ter a primeira coordenada nula e portanto $B = B_0$. Caso seja $B \neq B_0$ então deve existir um vetor $x = (1, y)$ com primeira coordenada 1 tal que $(0, y) \notin C$ e portanto $B = B_0 + \langle x \rangle$.
Daqui por diante adotaremos a seguinte notação

$$C - e = \widehat{C} \, e \, C/e = \widehat{C}_0.$$

Afirmamos que

$$(\widehat{C})^* = \widehat{(C^*)}_0. \tag{3.14}$$

Com efeito, se $x \in \widehat{(C^*)}_0$ então para todo $(y_1, y') \in C$, efuando o produto interno canônico, obtemos

$$(y_1, y').(0, x) = 0 \Rightarrow y'x = 0.$$

Como $y' \in \widehat{C}$ concluimos que $x \in (\widehat{C})^*$. Logo $\widehat{(C^*)}_0 \subseteq (\widehat{C})^*$. Por outro lado, se $x \in (\widehat{C})^*$ então para todo $y \in \widehat{C}$ obtemos $x.y = 0$. Como $y \in \widehat{C}$, temos que $(1, y) \in C$ ou $(0, y) \in C$. Afirmamos que $(1, x) \notin C^*$. De fato, suponha que $(1, x) \in C^*$ e considere $(1, y) \in C$. Assim, efetuando o produto interno $(1, x) \cdot (1, y)$ obtemos $1 + xy = 0$. Como $xy = 0$, obtemos $1 = 0$. Um absurdo. Logo a primeira coordenada de x é o 0 e portanto $x \in \widehat{(C^*)}_0$. Logo, $(\widehat{C})^* \subseteq \widehat{(C^*)}_0$. E então $(\widehat{C})^* = \widehat{(C^*)}_0$.
As expressões (3.12) e (3.14) nos possibilita fazer a seguinte análise:
Se $x \in B(C - e) = (C - e) \cap (C - e)^* = \widehat{C} \cap \widehat{(C^*)}_0$, então $(0, x) \in C^*$ enquanto que ou $(0, x) \in C$ ou $(1, x) \in C$. Dualmente, se $y \in B(C/e) = (C/e) \cap (C/e)^* = \widehat{C}_0 \cap (\widehat{C}_0)^*$, então $y \in \widehat{C}_0$ e $(0, y) \in C$, enquanto que ou $(0, y) \in C^*$ ou $(1, y) \in C^*$, mas não ambos. Pois do contrário $(0, y) + (1, y) = (1, 0) \in C^*$. Logo e seria uma ponte de $M(C^*)$ e portanto um laço de $M(C)$. Uma contradição.

Lema 3.2 *Os itens (i) e (ii) abaixo são mutualmente exclusivos.*

(i) para algum $x \in B(C - e), (1, x) \in C$ e então $B(C - e) = \widehat{B}_0 + \langle x \rangle$;

(ii) para todo $x \in B(C - e), (0, x) \in C$ e $B(C - e) = \widehat{B}_0$.

Prova. Suponha que para todo $x \in B(C - e)$ $(0, x) \in C$ logo, por (3.12) $(1, x) \notin C$ e $B(C)$ é formado apenas por vetores com primeira coordenada nula. Ou seja, $B(C) = B_0$ e Portanto $B(C-e) = \widehat{B}_0$. Por outro lado, se para algum vetor $x \in B(C-e)$, $(1, x) \in C$ então por (3.12) $(0, x) \notin C$, logo, $x \notin \widehat{B}_0$ o que implica $B(C - e) \neq \widehat{B}_0$. Portanto, $B(C - e) = \widehat{B}_0 + \langle x \rangle$. ■

Por dualidade, provamos o seguinte:

Lema 3.3 *Os itens (i) e (ii) abaixo são mutualmente exclusivos.*

(i) para todo $y \in B(C/e), (0, y) \in C^*$ e $B(C/e) = \widehat{B}_0$; ou

(ii) para algum $y \in B(C/e) talque (1, y) \in C^*$ *e* $B(C/e) = \widehat{B}_0 + \langle y \rangle$.

Lema 3.4 *São equivalentes as afirmações:*

(1) $B = B_0$

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

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

(4) para algum z

(a) $(1, z) \in C$ *e* $(0, z) \in C^*$*; ou*

(b) $(1, z) \in C^*$ *e* $(0, z) \in C$.

Além disso afirmamos que (4-a) e (4-b) não ocorrem simultaneamente.

Prova. *(1)*$\Rightarrow$ *(2)* $B = B_0 \Rightarrow \forall x \in B, x = (0, v)$ para algum $v \in \hat{B}$. Logo $(1, 0) \in B^*$.
(2)$\Rightarrow$ *(3)* $(1, 0) \in B^* \Rightarrow (1, 0) \in (C \cap C^*)^* = C + C^*$.
(3)$\Rightarrow$ *(4)*Por hipótese $(1, 0) \notin C^*$, pois do contrário e seria um laço de $M^*(C)$. Além disso se para algum $z \in \hat{C}$, $(1, z) \in C$; então $(0, z) \notin C$. Como $(1, 0) \in C + C^*$. Logo $(0, z) \in C^*$ e (a) ocorre. Analogamente, se $(0, z) \in C$ então $(1, z) \in C^*$ e (b) ocorre.
(4)$\Rightarrow$ *(1)*Suponhamos que $B \neq B_0$, então existe $x \in \widehat{B}$ tal que $(1, x) \in B$. Como *(4)* vale temos que $(1, 0) \in B^*$. Daí, $(1, x).(1, 0) = 0 \Rightarrow 1 + 0 = 0 \Rightarrow 1 = 0$. Um absurdo.
Por fim, para mostrarmos que *(4-a)* e *(4-b)* não ocorrem ao mesmo tempo, suponha que para algum z_1 e z_2 quaisquer tivermos $(1, z_1)$ e $(0, z_2) \in C$; e $(0, z_1)$ e $(1, z_2) \in C^*$ então

$$(1, z_1).(1, z_2) = 0 \Rightarrow 1 + z_1 z_2 = 0 \Rightarrow z_1 z_2 = 1$$

$$(0, z_1).(0, z_2) = 0 \Rightarrow 0 + z_1 z_2 = 0 \Rightarrow z_1 z_2 = 0$$

Donde obtemos $1 = 0$. Um absurdo. Portanto, *(4-a)* e *(4-b)* são mutualmente exclusivos. ■

Lema 3.5 *Suponha que* $dim B = k$*, então um dos itens (i), (ii) e (iii) abaixo deve ocorrer.*

(i) dim B(C-e) = dim B(C/e)

(ii) dim B(C-e) = k+1 = dim B(C/e) = k

(iii) dim B(C-e) = dim B(C/e) = k+1

Prova. Suponha que $B \neq B_0$. Afirmamos que (i) no **Lema 3.2** não pode ocorrer. Do contrário, $(1,x) \in C$ e $(0,x) \in C^*$ o que implica $(1,x)+(0,x) = (1,0) \in C + C^*$ e pelo **Lema 3.4**, $B = B_0$. Contradição. Logo, se $B \neq B_0$, ocorre (ii) no **Lema 3.2** e portanto $B(C-e) = \hat{B}_0$. Dualmente, $B(C/e) = \hat{B}_0$. Portanto

$$dim(B(C-e)) = dim(\hat{B}_0) = dim(B(C/e)).$$

Como $B \neq B_0$, pela expressão (3.13)

$$dimB = dimB_0 + 1 = dim\hat{B}_0 + 1.$$

Logo

$$k = dim\hat{B}_0 + 1 \Rightarrow dim\hat{B}_0 = k - 1.$$

Portanto,

$$dimB(C-e) = dimB(C/e) = k - 1$$

e o item *(i)* deste lema ocorre.
Agora vamos assumir que $B = B_0$. Então, *(4-a)* ou *(4-b)* ocorre. Suponha que *(4-a)* ocorre. Daí, temos que para algum z, $(0,z) \in C$ e $(1,z) \in C^*$. Logo, $z \in B(C-e)$. Então, pelo item *(i)* do **Lema 3.2** temos que $B(C-e) = \widehat{B}_0 + \langle x \rangle$. Logo,

$$dimB(C-e) = dim\hat{B}_0 + 1 = dimB_0 + 1 = dimB + 1.$$

Ou seja

$$dimB(C-e) = dimB + 1 = k + 1.$$

Além disso como *(4-b)* não ocorre, o **Lema 3.3** implica que

$$B(C/e) = \hat{B}_0.$$

Logo $dimB(C/e) = dim\hat{B}_0 = dimB_0 = dimB$ ou seja

$$dimB(C/e) = dimB = k.$$

Portanto, se *(4-a)* ocorre, então o item *(ii)* deste lema vale. Por dualidade, se *(4-b)* ocorre, então vale o item *(iii)*. Concluimos assim que um dos itens *(i)*, *(ii)* e *(iii)* deste

lema deve ocorrer. ■

Em cada caso, podemos facilmente verificar que

$$(-1)^n(-2)^{dimB} = (-1)^{n(C-e)}(-2)^{dimB(C-e)} + (-1)^{n(C/e)}(-2)^{dimB(C/e)}.$$

Logo, como $n(C-e) = n(C) - 1 < m$ segue da hipótese de indução, que se e não é um laço nem uma ponte de $M(C)$, então

$$(-1)^{n(C)}(-2)^{dimB} = h(M(C-e)) + h(M(C/e)) \tag{3.15}$$

Agora suponha que e seja um laço ou uma ponte de $M(C)$. Então

$$\widehat{C} = \widehat{C}_0 \Rightarrow C - e = C/e$$

e deste modo cada palavra-código em $C \cap C^*$ tem a primeira coordenada nula. De fato, se e é um laço ou uma ponte; ou a matriz geradora de C ou a matriz geradora de C^* têm a primeira coluna nula. Considere então, $(0, x) \in C \cap C^*$. Afirmamos que

$$x \in B(C-e) = (C-e) \cap (C-e)^* = \widehat{C} \cap \widehat{C^*}_0.$$

Suponha, por absurdo, que $x \notin \widehat{C} \cap \widehat{C^*}_0$. Então, $(0, x) \notin C^*$. O que é uma contradição. Logo, $|(C-e) \cap (C-e)^*| = |C \cap C^*|$ e portanto,

$$dimB(C-e) = dimB(C).$$

Assim,

$$(-1)^{n(C)}(-2)^{dimB(C)} = (-1)^{n(C)}(-2)^{dimB(C-e)} = (-1)(-1)^{n+1}(-2)^{dimB(C-e)}.$$

Como $n(C-e) = n(C) - 1 < m$, segue da hipótese de indução que

$$(-1)^{n(C-e)}(-2)^{dimB(C-e)} = h(M(C) - e).$$

Logo,

$$(-1)^{n(C)-1}(-2)^{dimB(C)} = h(M(C) - e),$$

$$(-1)(-1)^{n(C)}(-2)^{dimB(C)} = h(M(C) - e),$$

$$(-1)^{n(C)}(-2)^{dimB(C)} = (-1)h(M(C) - e).$$

Como $(-1) = h(P) = h(L)$, temos que

$$(-1)^n(-2)^{dimB(C)} = \begin{cases} h(P)h(M(C)-e), & \text{se } e \text{ é uma ponte} \\ h(L)h(M(C)-e), & \text{se } e \text{ é um laço.} \end{cases}$$

Da equação anterior juntamente com a (3.15) concluimos que h é um invariante T-G bem definido com $h(I) = h(L) = -1$. Segue do **Teorema 2.2** que

$$h(M(C)) = t(M(C); h(P), h(L)) = t(M(C); -1, -1).$$

Portanto,

$$(-1)^n(-2)^{dimC\cap C^*} = t(M(C); -1, -1).$$

■

Corolário 3.15 *Seja C um código binário. Então $C \cap C^*$ é trivial se e somente se $M(C)$ tem um número impar de bases.*

Prova. Seja M uma matróide qualquer. Note que se avaliarmos $t(M; 1, 1)$ e $t(M; -1, -1)$ módulo 2, obtemos o mesmo resultado. Lembramos também que pelo item *(i)* do **Teorema 2.7** $t(M; 1, 1)$ é o número de bases de M. Agora, suponha primeiro que $C \cap C^* = 0$. Então, pelo **Teorema 3.14** $|t(M; -1, -1) = |C \cap C^*| = 1$. Reciprocramente se $M(C)$ tem um número impar k de bases, então avaliando $t(M; -1, -1)$ módulo2, obtemos

$$t(M; 1, 1) = kmod2 = 1.$$

Logo,$|t(M; -1, -1) = 1 \Rightarrow |C \cap C^*| = 1$ e portanto $C \cap C^* = \{0\}$. ■

Considere um código binário C de dimensão r. Fazendo $(q, z) = (4, 1)$ no **Teorema 3.7** e usando o **Teorema 3.14**, obtemos

$$2^{r+dim(C\cap C^*)} = |c_p - c_i| \tag{3.16}$$

Onde c_p e c_i são os números de palavras códigos que têm peso par e ímpar, respectivamente, no código linear sobre $GF(4)$ que é gerado por C. De fato, avaliando o

polinômio enumerador de pesos em $z = 1$

$$\begin{aligned} A(z) &= \sum_{i=0}^{n} a_i (z)^i \\ A(1) &= \sum_{i=0}^{n} a_i (-1)^i \\ &= \sum_{i \text{ é } par} a_i (-1)^i + \sum_{i \text{ é } mpar} a_i (-1)^i \\ &= c_p - c_i. \end{aligned} \tag{3.17}$$

Por outro lado, usando o **Teorema 3.7**, obtemos

$$A(C; 4, 1) = 2^r (-1)^{n-r} t(M(C), -1, -1) \tag{3.18}$$

Logo, igualando as expressões (3.17) e (3.18), obtemos

$$2^r (-1)^{n-r} t(M(C), -1, -1) = c_p - c_i.$$

Calculando o módulo desta expressão, e usando o **teorema 3.14**, obtemos

$$2^r |t(M(C), -1, -1)| = |c_p - c_i| \Rightarrow 2^r |C \cap C^*| = |c_p - c_i|$$

Como $|C \cap C^*| = 2^d im(C \cap C^*)$. Então

$$2^r 2^{dim(C \cap C^*)} = |c_p - c_i|$$

e portanto

$$2^{r + dim(C \cap C^*)} = |c_p - c_i|.$$

Uma consequência da igualdade (3.16) é que $C \subseteq C^*$ se e somente se, no código sobre $GF(4)$ que é gerado por C, todas as palavras-código têm peso par. Com efeito, se $C \subseteq C^* \Longrightarrow C \cap C^* = C \Longrightarrow dim(C \cap C^*) = dimC = r$. Logo, usando a igualdade (3.16), $2^{r+r} = |c_p - c_i| \Longrightarrow 4^r = |c_p - c_i|$. Mas, $4^r = |C| \Longrightarrow |C| = |c_p - c_i| \Longrightarrow c_i = 0 \Longrightarrow |C| = c_p$. Reciprocramente, se $|C| = c_p$.Como $|c_p - c_i| = 2^{r + dim(C \cap C^*)}$ e $_i = 0$ temos $|c_p| = 2^{r + dim(C \cap C^*)} \Longrightarrow 4^r = 2^{r + dim(C \cap C^*)} \Longrightarrow 2r = r + dim(C \cap C^*) \Longrightarrow r = dim(C \cap C^*)$. Como $dimC = r$ e $C \cap C^* \subseteq C$ então $C \subseteq C^*$ e portanto $C \subseteq C^*$.

Em contraposição aos códigos binários, se C é um código linear sobre $GF(q)$ para $q \geq 4$ então $dim(C \cap C^*)$ não é, em geral, um invariante de matróides. Por exemplo, considere a seguinte representação de $U_{2,4}$ sobre $GF(13)$ onde a não pertence a $\{0, 1\}$.

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

Podemos checar que

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

Bibliografia

[1] BRYLAWSKI, T & OXLEY, J. The Tutte Polynomial, in White, Neil(ed),*Matroid Aplications*, Encyclopedia of Mathematics and its applications;v.40,pp.123-225. Cambridge University Press,1992.

[2] ZASLAVSKY, T. The Möbius Function and the Characteristic Polynomial, in White Neil (ed), *Combinatorial Geometries*, Encyclopedia of mathematics and its applications; v.29,pp.114-138. Cambridge University Press,1987.

[3] OXLEY, James. *Matroid Theory*. Oxford University Press, 1992.

[4] HEFEZ, A & VILLELA, Maria Lúcia T., *Códigos corretores de erros*.IMPA,2002.

[5] WHITE, Neil. *Theory of Matroids*. Encyclopedia of mathematics and its applications;v.26. Cambridge University Press,1986.

[6] BERLEKAMP, Elwyn R. *Algebraic Coding Theory*. MaGraw-Hill Book Company, 1968.

[7] LIN, Shu & COSTELLO, Daniel Jr. *Error Control Coding: Fundamentals and Applications*. Prentece-Hall seres in computer appications in eletrical engineering. 1983

[8] KUNG, Joseph P. S. Critical Problems in *Matroid Theory*. AMS-INMS-SIAM joint Summer Research Conference on Matroid Theory, July 2-6, 1995, University of Washington, Seatlle. joseph E. Bonin, James G. Oxleym Brigite Servatius, editors.

[9] GREENE, C. Wheigt enumeration and the geometry of linear codes, *stud.Appl.Math*. **55**, 119-28.

[10] DOWLING, T.A. Codes, packing and critical problem,*Atti del Convegno di Geometria combinatoria e sue Applicazioni*, pp.209-24. Institute of Mathematics, University of Perugia, Perugia. 1971.

[11] CRAPO, H. H & ROTA, G-C. On the Foundations of Combinatorial Theory: Combinatorial Geometries, preliminary edition, M.I.T. Press, Cambridge, Mass.1970.

[12] JAEGER,F. On Tutte Polynomials of matroids representable over GF(q), *Europ. J. Comb.* **10**, 247-55.

[13] ROSENSTHIEHL, P. & READ, R. C. On the principal edge tripartition of a graph, in B. Bollobás(ed), *Advances in Graph Theory*, Ann. Discrete Math. 3, pp. 195-226. North-Holland, Amsterdam.

[14] MACWILLIANS, Florence jessie. *The Theory of error-correting codes*. North-Holland Publishing company, 1917.

Índice