



Universidade Federal de Pernambuco
Centro de Ciências Exatas e da Natureza
Departamento de Matemática

Pós-graduação em Matemática

**O POLINÔMIO DE TUTTE E DUAS
GENERALIZAÇÕES**

Gabriel de Moraes Coutinho

DISSERTAÇÃO DE MESTRADO

Recife
2010

Universidade Federal de Pernambuco
Centro de Ciências Exatas e da Natureza
Departamento de Matemática

Gabriel de Moraes Coutinho

O POLINÔMIO DE TUTTE E DUAS GENERALIZAÇÕES

Trabalho apresentado ao Programa de Pós-graduação em Matemática do Departamento de Matemática da Universidade Federal de Pernambuco como requisito parcial para obtenção do grau de Mestre em Matemática.

Orientador: *Prof. Manoel J. M. S. Lemos*

Recife
2010

Coutinho, Gabriel de Moraes

O polimônio de Tutte e duas generalizações / Gabriel de Moraes Coutinho. - Recife: O Autor, 2010.

xi, 87 folhas

Dissertação (mestrado) – Universidade Federal de Pernambuco. CCEN. Matemática, 2010.

Inclui bibliografia.

**1. Matemática. 2. Matemática discreta. 3. Teoria dos Grafos.
I. Título.**

510

CDD (22. ed.)

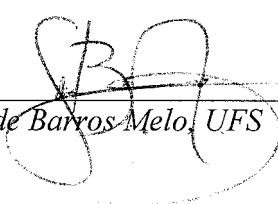
MEI2010 – 0101

Dissertação submetida ao Corpo Docente do Programa de Pós-graduação do Departamento de Matemática da Universidade Federal de Pernambuco como parte dos requisitos necessários para a obtenção do Grau de Mestrado em Matemática.

Aprovado:


Manoel José Machado Soares Lemos, UFPE
Orientador


Sóstenes Luiz Soares Lins, UFPE


Silvio de Barros Melo, UFS

O POLINÔMIO DE TUTTE E DUAS GENERALIZAÇÕES

Por

Gabriel de Moraes Coutinho

UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE CIÊNCIAS EXATAS E DA NATUREZA
DEPARTAMENTO DE MATEMÁTICA
Cidade Universitária – Tels. (081) 2126 - 8414 – Fax: (081) 2126 - 8410
RECIFE – BRASIL

Julho – 2010

O autor autoriza a reprodução parcial ou total deste texto desde que a fonte seja devidamente identificada. O autor também agradece qualquer correção, crítica, sugestão ou elogio, e pede para que sejam enviados para gmcout@gmail.com ou gabriel@dmate.ufpe.br.

Wir dürfen nicht denen glauben, die heute mit philosophischer Miene und überlegenem Tone den Kulturuntergang prophezeien und sich in dem Ignorabimus gefallen. Für uns gibt es kein Ignorabimus, und meiner Meinung nach auch für die Naturwissenschaft überhaupt nicht. Statt des törichten Ignorabimus heiÙe im Gegenteil unsere Losung: Wir müssen wissen - wir werden wissen!

Não podemos acreditar naqueles, que hoje, com atitude filosófica e tom ponderado, profetizam o fim da cultura e aceitam o ignorabimus. Para nós não existe ignorabimus, e em minha opinião em lugar algum da ciência natural. Em oposição ao estúpido ignorabimus, nosso lema deverá ser: Temos que saber - Saberemos!

—DAVID HILBERT (Para a Sociedade de Cientistas e Médicos Alemães, 1930)

RESUMO

O Polinômio de Tutte generaliza alguns polinômios usados para contar estruturas em grafos, tais como colorações e fluxos. Não obstante, é mais naturalmente definido para matróides. Em termos mais formais, é essencialmente o único invariante polinomial com comportamento multiplicativo para soma direta de matróides ou uniões disjuntas de grafos conexos. Adicionando alguma complexidade em sua formulação, é possível capturar nele as simetrias de um grafo por um argumento de contagem de órbitas de grupos. Com outro viés, é possível codificar algebricamente uma matróide atribuindo pesos para os seus elementos ao construirmos uma variação do Polinômio de Tutte, o que resulta praticamente na função de partição do modelo de Potts.

Ambas as generalizações possuem motivação prática e propriedades estruturais. Nesta dissertação, abordaremos todos estes temas e as relações entre eles.

Palavras-chave: Polinômio de Tutte; Polinômio Orbital de Tutte; Modelo de Potts; Grafos; Matróides

ABSTRACT

The Tutte Polynomial generalizes some counting polynomials defined on graphs. Notwithstanding, it's naturally defined for matroids. Formalizing its construction, it is essentially the only polynomial invariant which is multiplicative on direct sums of matroids and on disjoint union of graphs. With an argument for counting orbits of a group, one may formulate a version of the polynomial that captures the symmetries of a graph. In another direction, matroid can be completely described in algebraic terms if weights are assigned to its elements while defining a variation of the Tutte Polynomial. The resulting polynomial is essentially the partition function of the Potts model.

Both generalizations are well motivated and have good structural properties. At the present text, we shall study these subjects and the interconnections among them.

Keywords: Tutte Polynomial; Orbital Tutte Polynomial; Potts Model; Graphs; Matroids

SUMÁRIO

Apresentação	1
Capítulo 1—Introdução - grafos, matróides e um pouco de álgebra	3
1.1 Grafos	3
1.2 Matróides	5
1.2.1 Introdução	5
1.2.2 Dualidade, laço, colaços, circuitos e cocircuitos	6
1.3 Matróides gráficas, a função posto e menores	7
1.4 Planaridade e dualidade	8
1.4.1 Planaridade	8
1.4.2 Dualidade	9
1.4.3 Dualidade em matróides gráficas	11
1.5 Um pouco de álgebra abstrata	13
1.5.1 Grupos	13
1.5.2 Anéis e domínios	15
1.5.3 Ideais e Módulos	16
1.5.4 Primeiro teorema de homomorfismos para módulos	17
Capítulo 2—Polinômios em grafos e matróides	19
2.1 Colorações, tensões, fluxos e confiabilidade	19
2.1.1 Colorações	19
2.1.2 Tensões	21
2.1.3 Fluxos	22
2.1.4 Confiabilidade	24
2.2 Polinômio de Tutte	24
2.2.1 Definições para grafos	24
2.2.2 Matróides	29
2.2.3 Avaliações do polinômio de Tutte	30
2.3 Invariante de Tutte-Grothendick	31
2.3.1 Grafos	31
2.3.2 Revisitando os polinômios cromático, de tensão, de fluxo e de confiabilidade	34
2.3.3 Formalização da idéia de invariante de Tutte-Grothendick	34
2.3.4 O polinômio universal para matróides	36

Capítulo 3—Matrizes	38
3.1 Alguma álgebra linear	38
3.1.1 Forma Normal de Smith	38
3.1.2 Dualidade de matrizes	42
3.2 Aplicação à combinatória	44
3.2.1 Matrizes e grafos	44
3.2.2 Matrizes e matróides	46
3.2.3 Matrizes, grafos e matróides	49
Fluxos e tensões - dualidade	50
Capítulo 4—Contando órbitas de ações de grupos	53
4.1 Polinômio cromático orbital	53
4.2 Polinômios orbitais de fluxo e de tensão	54
4.3 O polinômio orbital de Tutte	55
4.3.1 Variáveis no polinômio de Tutte	61
Mais alguma álgebra linear	61
De volta às variáveis	63
4.4 Conclusão	63
Capítulo 5—Polinômio de Tutte em várias variáveis	64
5.1 O polinômio dicromático	64
5.2 Motivação física - o modelo de Potts	65
5.2.1 (Re)-definições, nomenclaturas e convenções	68
5.3 Multi-variáveis - abordagem em grafos	69
5.3.1 E quando $q \rightarrow 0$?	71
Subgrafos geradores maximalmente conexos	71
Florestas geradoras	72
Florestas geradoras maximais	72
5.3.2 O polinômio de fluxo em multi-variáveis	72
5.4 Versão para matróides	73
5.4.1 Matróides e grafos	74
5.4.2 Recorrência	74
5.4.3 Soma direta	75
5.4.4 Limites $q \rightarrow 0$	76
Conjuntos geradores da matróide	77
Conjuntos independentes	77
Bases	77
Relação com grafos	77
5.4.5 Arestas em paralelo e em série	78
5.5 Dualidade	80
5.5.1 Dualidade em $q \rightarrow 0$	82

5.5.2	Dualidade no polinômio de fluxo - onde alguns tópicos de todo o texto são revisitados	84
5.6	O polinômio de confiabilidade revisitado	84
5.7	Comentário final	86
	Considerações finais	87
	Conclusões	87
	Daqui, para onde?	87
	Referências	89

APRESENTAÇÃO

Esta é uma dissertação sobre o polinômio de Tutte. Trata-se de um polinômio em duas variáveis associado a um grafo que se especializa através de algumas atribuições às variáveis para contar certas estruturas do grafo. É uma ferramenta extremamente poderosa em combinatória enumerativa, pois, por exemplo, possui definições alternativas que nos permitem abordar problemas por diferentes pontos de vista.

Motivados pela beleza desta teoria, pela importância de alguns resultados e pela relação com outras áreas da combinatória, partimos em busca de definições mais gerais deste polinômio. Naturalmente, trabalharemos com construções de maior complexidade, mas que também nos fornecerão mais informações.

Decidimos também que os resultados e os polinômios deveriam ser apresentados para uma estrutura mais geral que um grafo - uma matróide. Em parte, ganhamos generalidade nos resultados a um custo muito baixo, pois o polinômio de Tutte, em certo sentido, habita mais naturalmente no espaço das matróides. Por outro lado, ganharemos também facilidade e clareza em alguns argumentos, principalmente naqueles associados a dualidade.

Ao falarmos de grafos e matróides, a motivação para falarmos de matrizes surgiu naturalmente. *Mutatis mutandi*, uma mesma estrutura abstrata pode ser codificada como um grafo, uma matróide ou uma matriz. A abordagem escolhida dependerá do contexto, no sentido em que buscaremos sempre o argumento mais vantajoso, seja no sentido da clareza, seja no sentido da generalidade, seja no sentido de aproveitar uma teoria já estabelecida.

No primeiro capítulo, vamos apresentar nossos principais objetos de estudos. Definiremos um grafo e uma matróide, e falaremos brevemente sobre alguns resultados básicos acerca dessas estruturas. Teremos uma seção sobre planaridade e dualidade de grafos, culminando num resultado importante que será acessado ao longo do texto. Falaremos também neste primeiro capítulo de grupos, anéis, domínios e módulos: estruturas algébricas que serão utilizadas ao longo do texto.

No capítulo 2, apresentaremos *counting polynomials*, e logo após o Polinômio de Tutte. Exporemos três definições alternativas para este e demonstraremos que todas são equivalentes. Mostraremos que todos esses polinômios são na verdade invariantes de Tutte-Grothendick (TG-invariantes). Por fim, mostraremos que um polinômio TG-invariante é uma re-apresentação do Polinômio de Tutte.

No terceiro capítulo, falaremos da relação que grafos e matróides estabelecem com matrizes. Originalmente, estes comentários viriam como uma seção no capítulo 4, pois é lá que eles serão úteis. Mas resolvemos estabelecer vários resultados, um pouco mais do que o que seria necessário. Ao final deste capítulo, apresentaremos uma bela aplicação desta teoria.

No capítulo 4 vamos generalizar os polinômios apresentados no capítulo 2, levando em consideração a ação de um grupo de automorfismos na estrutura em questão. Nossas principais ferramentas serão o *lema de contagem de órbitas* e a teoria de matrizes apresentada no capítulo 3. Seguiremos basicamente o trabalho de Cameron [CJR08]. Este capítulo é basicamente dedicado a apresentar uma definição e mostrar que ela é efetivamente uma generalização de casos particulares com significado combinatório.

No quinto capítulo, apresentaremos uma variação do polinômio de Tutte chamado *polinômio dicromático*. Mostraremos que este polinômio dicromático aparece naturalmente na física como a função de partição do modelo de Potts com q estados. A seguir, generalizaremos este polinômio atribuindo pesos nas arestas (do grafo ou da matróide), o que é de fato a apresentação correta para o modelo de Potts. Veremos que este polinômio habita naturalmente o espaço de matróides - ele é de fato a codificação algébrica de uma matróide. A literatura sobre este tema é vasta, porém, dispersa. Por este motivo, escolhemos apresentar as propriedades básicas. Seguiremos basicamente o que está em Sokal [Sok05].

O estudo das raízes do polinômio de Tutte (e de todas as suas variações) é um tópico clássico que não será abordado neste texto. Para ambas as generalizações que apresentaremos nos capítulos 4 e 5, já existem resultados estabelecidos acerca da localização das raízes de ambos os polinômios, como também existem resultados sobre a localização das raízes em casos particulares do polinômio de Tutte. Um tratamento adequado deste tópico entraria em resultados técnicos e específicos e tornaria este texto demasiado longo para os seus propósitos. Seria uma possível continuação deste trabalho. Ainda assim, para o leitor interessado, sugerimos, acerca do polinômio de Tutte, as referências Jackson [Jac03], Cameron [CK07] e Sokal [Sok04].

Nossa tentativa será de fazer um texto absolutamente compreensível para quem possuir um conhecimento básico em combinatória, álgebra linear e teoria de grupos. Mais que isso, como apresentaremos todas as definições, enunciaremos todos os teoremas usados e praticamente faremos todas as demonstrações, o texto deverá ser compreensível para qualquer leitor com experiência em matemática.

CAPÍTULO 1

INTRODUÇÃO - GRAFOS, MATRÓIDES E UM POUCO DE ÁLGEBRA

Neste capítulo apresentamos nossos objetos de estudo. Na primeira seção, falaremos de grafos. Usaremos uma definição geral que nos permite falar de multigrafos, mas seguiremos em uma notação mais convencional. Mencionaremos brevemente subgrafos e conectividade.

A segunda seção apresentará matróides. Um leitor não familiarizado pode encontrar dificuldades para se acostumar com as idéias, pois não apresentaremos exemplos. Falaremos das definições alternativas, da função posto, de menores e de dualidade.

Na terceira seção, estabeleceremos a relação entre grafos e matróides.

Na quarta seção, vamos falar de planaridade e de dualidade em grafos, mas também em matróides no momento final do capítulo, ao apresentarmos um resultado fundamental.

1.1 GRAFOS

Apresentamos as definições básicas a serem usadas ao longo do texto a seguir.

Definição 1.1. Um *grafo* G é uma tripla ordenada (V, E, \mathcal{I}) de conjuntos disjuntos onde $\mathcal{I} \subset (V \times E)$ satisfazendo:

$$1 \leq |\{v \in V : (v, e) \in \mathcal{I}\}| \leq 2 \text{ para cada } e \in E$$

Dizemos que os elementos de V são *vértices* e os de E são *arestas*. O conjunto \mathcal{I} simplesmente relaciona vértices a arestas, de modo que cada aresta se relacione a no mínimo um e a no máximo dois vértices.

A seguir, apresentamos parte da nomenclatura introduzida por Bollobás [Bol98]. O leitor familiarizado não encontrará surpresas.

Uma aresta e é *incidente* a um vértice v (ou v incidente a e) se $(v, e) \in \mathcal{I}$.

Uma aresta é um *laço* se for incidente a somente um vértice.

Dois vértices são *vizinhos* ou *adjacentes* se há uma aresta incidente a ambos.

Estamos utilizando esta definição de grafo, ao invés da tradicional com $G = (V, E)$, $E \subset V^2$, para permitirmos a existência de laços e arestas paralelas entre vértices.

Um grafo sem laços e sem arestas paralelas é um *grafo simples*.

Contudo, em certos momentos, vamos abusar da notação, e nos referiremos a grafos que não sejam simples (multigrafos) simplesmente por $G = (V, E)$, e uma aresta e incidente a u e v como $e = uv$, mesmo que *a priori* ela possa não ser a única.

Um grafo simples em que cada par de vértices distintos é adjacente é um *grafo completo*, denotado por K_n se tem n vértices.

Um grafo de n vértices e nenhuma aresta é o *grafo nulo*, denotado por E_n .

O número de arestas incidentes a um vértice v é chamado grau do vértice, denotado por $d(v)$. Cada laço incidente a um vértice contribui com 2 em seu grau.

Um grafo simples conexo de n vértices em que todos os vértices tem grau 2 é denotado por C_n .

A seguir algumas estruturas definidas em grafos:

Um *passeio* é uma seqüência alternada de vértices e arestas incidentes aos seus vizinhos na seqüência, sem restrições, usualmente denotado por $v_0, e_1, v_1, e_2, \dots, e_n, v_n$. Um passeio deve sempre começar e se encerrar em um vértice.

Um *caminho* é um passeio no qual não há vértice visitado mais de uma vez.

Um *ciclo* é um caminho fechado.

Uma *trilha* T é um passeio no qual não há aresta visitada mais de uma vez, entretanto não há restrição quanto aos vértices.

Um *circuito*¹ é uma trilha fechada.

Algumas definições sobre conectividade:

Fixado um vértice v , a *componente conexa* do grafo contendo v é o conjunto de todos os vértices w para os quais existe um passeio iniciado em v e encerrando em w .

Um grafo é *conexo* se contiver apenas uma componente conexa.

O número de componentes conexas em um grafo G é denotado por $\kappa(G)$.

Uma *floresta* é um grafo sem ciclos.

Uma *árvore* é uma floresta conexa.

Um *corte* é um conjunto minimal de arestas com respeito à propriedade que a remoção destas arestas aumenta o número de componentes conexas do grafo.

Agora introduzimos definições acerca de subgrafos:

Um grafo $G' = (V', E', \mathcal{I}')$ é um *subgrafo* de $G = (V, E, \mathcal{I})$ se for tal que $V' \subset V$, $E' \subset E$ e $\mathcal{I}' \subset \mathcal{I}$.

¹Infelizmente há um choque entre a nomenclatura usual de Teoria de Grafos e a de Teoria de Matróides. Como veremos, chamaremos de circuito de uma matróide o que corresponde a um ciclo no grafo.

Dizemos que é *induzido* por um conjunto E' de arestas se $\mathcal{I}' = \mathcal{I}|_{E'}$.

Dizemos que é *gerador* se $V = V'$.

Em geral nos referimos ao conjunto de vértices de um grafo G específico por $V(G)$ e nos referiremos ao subgrafo gerador de G induzido por $A \subset E$ por G_A .

Nosso primeiro resultado:

Proposição 1.1. Todo grafo conexo em n vértices possui uma árvore geradora. Qualquer árvore geradora possui exatamente $n-1$ arestas. E mais, se um grafo conexo em n vértices possui $n-1$ arestas, então ele é uma árvore.

As duas primeiras afirmações seguem por indução no número de vértices. A terceira por contradição ao supormos que ele possui um ciclo, logo de onde podemos eliminar uma aresta sem desconectá-lo, e assim poderemos obter árvore geradora com menos que $n-1$ arestas.

1.2 MATRÓIDES

1.2.1 Introdução

Definição 1.2. Uma *matróide* M é um par ordenado (E, r) onde E é um conjunto e r é uma função inteira não negativa definida no conjunto das partes de E , $r : \mathcal{P}(E) \rightarrow \mathbb{N}$, satisfazendo as seguintes propriedades:

- (i) $0 \leq r(A) \leq |A|$ para todo $A \subset E$
- (ii) Se $A \subset B$, então $r(A) \leq r(B)$
- (iii) $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$

Dizemos que E é o conjunto base e que esta função r é a *função posto* da matróide M .

Quando não ficar claro de qual matróide estamos falando, escreveremos $E(M)$ e r_M para nos referirmos ao conjunto base e à função posto da matróide M .

Os comentários a seguir seguem Oxley [Oxl92].

Se $r(A) = |A|$, dizemos que A é um conjunto *independente*.

Proposição 1.2. Todo subconjunto de um conjunto independente também é um conjunto independente.

Demonstração. Seja A independente, $B \subset A$ e B_A o complementar de B em A . Teremos:

$$r(B \cup B_A) + r(B \cap B_A) \leq r(B) + r(B_A)$$

ou seja:

$$|A| = r(A) \leq r(B) + r(B_A) \leq |B| + |B_A| = |A|$$

Donde ocorre a igualdade, e ela só pode ocorrer quando $r(B) = |B|$ e $r(B_A) = |B_A|$.

Proposição 1.3. O posto de um conjunto X é igual à cardinalidade do maior subconjunto independente, digamos A , contido em X .

Demonstração. A demonstração segue por indução na cardinalidade de $X \setminus A$. Se $X = A$, não há nada a mostrar. Seja então $x \in X \setminus A$. Então A também é o maior independente de $X \setminus x$. Por hipótese de indução, teremos $r(X \setminus x) = |A|$. Agora $|A| \leq r(X) + 0 \leq r(X \setminus x) + r(x) \leq |A| + 1$. Se $r(X) = |A| + 1$, então $r(A \cup x) = |A| + 1$. De fato, seja $B = (X \setminus x) \setminus A$. Teremos:

$$r(A \cup x \cup B) + r(A) \leq r(A \cup x) + r(A \cup B) = r(A \cup x) + r(A)$$

pois $|A| = r(X \setminus x) = r(A \cup B)$. Logo $r(X) \leq r(A \cup x) \leq r(X)$. Mas A é um independente maximal, portanto $r(A \cup x) = |A| + 1$ é uma contradição. Portanto $r(X) = |A|$, como queríamos. ■

Um independente maximal com respeito a inclusão é dito uma *base*.

Note que se ao invés de começarmos com a função posto tivéssemos apresentado todos os conjunto independentes, a matróide estaria definida - bastaria definirmos o posto de um subconjunto como a cardinalidade do maior independente nele contido. O mesmo poderia ser dito acerca das bases, já que os independentes são exatamente os subconjuntos de bases.

Um conjunto que não é independente é dito um *dependente*.

Note em particular que uma matróide também está definida a partir de seus dependentes ou de seus circuitos. Há axiomas que definem independentes, bases e circuitos, que podem ser encontrados em Oxley [Oxl92].

1.2.2 Dualidade, laço, colaços, circuitos e cocircuitos

A matróide *dual* M^* de uma matróide M é obtida sobre o mesmo conjunto E tomando o complementar das bases originais para serem as bases da dual.

Proposição 1.4. Em termos da função posto para dual r^* , isto significa que, para todo $A \subset E$:

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

Demonstração. De fato, um independente maximal da dual I contido em A é exatamente um subconjunto maximal de A da forma $B^* \cap A$, B^* base da dual. Mas isso é exatamente o mesmo que dizer que $A - I$ um subconjunto minimal de A da forma $B \cap A$, B base de M . Agora note que:

$$|B \cap A| = |B| - |B - A|$$

Mas $B - A$ é independente e maximal em $E - A$ pois $B \cap A$ é minimal em A . Logo:

$$|B \cap A| = r(E) - r(E - A)$$

Agora: $r^*(A) = |I| = |A - B| = |A| - |A \cap B| = |A| + r(E - A) - r(E)$

Vamos introduzir algumas definições.

Um elemento e de uma matróide é dito um *laço* quando:

$$r(e) = 0$$

Um elemento e de uma matróide é dito um *colação* quando for um laço na dual, ou seja:

$$r^*(e) = 0$$

Isto é equivalente a: $r(E \setminus e) = r(E) - 1$.

Um dependente minimal na matróide é chamado de *circuito*.

Um conjunto que é dependente minimal na matróide dual é chamado de *cocircuito*.

1.3 MATRÓIDES GRÁFICAS, A FUNÇÃO POSTO E MENORES

Um grafo G induz uma matróide M , denotada por $M(G)$, definida sobre o conjunto de arestas E quando tomamos o posto de um conjunto $A \subset E$ por:

$$r(A) = \text{número de arestas de uma floresta maximal do subgrafo induzido por } A$$

Note que as bases desta matróide são as florestas geradoras maximais do grafo, e que os circuitos da matróide são os ciclos do grafo. Uma aresta que incide somente em um vértice é considerada um ciclo no grafo, portanto um circuito da matróide, e será chamada de laço.

Uma matróide é *gráfica* se existir um grafo que a induza.

O posto definido na forma acima para matróides possui uma interpretação gráfica. A generalização do fato que toda árvore em n vértices tem $n - 1$ arestas é que toda floresta em um grafo de n vértices possui exatamente $n - \kappa(G)$ arestas, onde $\kappa(G)$ é o número de componentes conexas do grafo G . Desta forma, define-se:

$$r(A) = |V| - \kappa(G_A)$$

como o posto de um conjunto A de arestas em um grafo.

Define-se também a *nulidade* de um conjunto A (num grafo ou numa matróide) como sendo:

$$n(A) = |A| - r(A)$$

Introduzimos ainda duas definições importantes.

A *remoção* de uma aresta e em um grafo G é denotada por $G \setminus e$ e trata-se simplesmente de tomar o mesmo grafo que G sem a aresta e , isto é, o grafo $G_{E \setminus e}$.

A *contração* de uma aresta e ocorre quando remove-se a aresta e identificam-se os dois vértices a ela incidentes como um só, que passa a ser incidente a todas as arestas incidentes aos dois originais. Esta operação é denotada por G/e .

Uma *ponte* é uma aresta cuja remoção aumenta o número de componentes conexas em um grafo.

A generalização destas operações para matróides pode ser expressa através das alterações que causam na função posto. Com efeito, se $e \notin A$, temos:

$$r_{M \setminus e}(A) = r(A) \text{ e } r_{M/e}(A) = r(A \cup e) - r(e)$$

Olhando para estas equações, é possível observar que estas operações são associativas e comutativas.

Um grafo ou uma matróide obtido após uma dessas operações é chamado de *menor*.

Por fim, observe que:

Os laços de um grafo tornam-se laços na matróide gráfica associada, pois $r(e) = |V| - \kappa(G_e) = 0$.

As pontes de um grafo tornam-se colaços na matróide gráfica associada, pois $r(E \setminus e) = |V| - \kappa(G_{E \setminus e}) = |V| - (\kappa(G) + 1) = r(E) - 1$.

1.4 PLANARIDADE E DUALIDADE

O leitor com experiência nos tópicos mencionados no título poderá evitar esta seção sem prejuízo algum para o entendimento do texto. Possivelmente, somente no quinto capítulo, será importante revisar alguns comentários feitos na subseção *dualidade*.

Apesar de nossa intuição nos guiar sem tormentos nos fatos básicos acerca deste tema, uma mente cética pode encontrar inúmeras questões não respondidas em comentários informais. Não faremos uma introdução absolutamente formal; para tal, indicamos Diestel [Die05]. Procuraremos, contudo, não omitir os detalhes mais importantes.

1.4.1 Planaridade

Um grafo *desenhado*² no plano é dito um *grafo plano* se, neste *desenho*, duas arestas não se tocam onde não existem vértices. Observe que um tal desenho induz uma partição do plano em regiões simplesmente conexas, ao que chamaremos de *faces* do grafo plano. Denotaremos um desenho d de um grafo G por $G_d = (V_d, E_d, F_d)$, cada um dos conjuntos sendo os vértices, as arestas e as faces do desenho, respectivamente³. Um grafo abstrato é dito *planar* quando é possível desenhá-lo como um grafo plano.

²“Desenhado” aqui significa que os vértices do grafo são pontos no plano, e as arestas são curvas contínuas sem auto-interseções, cujos pontos terminais são os vértices a ela incidentes no grafo.

³Um grafo abstrato pode ser desenhado de infinitas maneiras. O conjunto de faces *depende* de como o grafo está desenhado, i.e., é uma característica do desenho, não do grafo.

Proposição 1.5. Seja um grafo $G_d = (V_d, E_d, F_d)$ grafo plano, então:

$$|V_d| + |F_d| - |E_d| = 2$$

Esta relação é devida a Euler, e o número que aparece ao lado direito é chamado *característica de Euler* da superfície sobre a qual estamos desenhando o grafo, no caso, o plano.

Omitiremos temporariamente o índice d por limpeza de notação.

Demonstração. Faremos por indução. Para $|V| = 1$, $|E| = 0$ e $|F| = 1$, ou seja, o grafo formado por um vértice e sem arestas, é imediato. Seja então G um grafo qualquer com m arestas. Se toda aresta for uma ponte, então G é uma árvore, e o resultado segue trivialmente ao observarmos que $|E| = m$, $|V| = m + 1$ e $|F| = 1$. Se G não é uma árvore, escolhamos uma aresta e que não seja ponte e vamos removê-la, gerando o grafo $G' = G \setminus e$. Esta remoção não altera o número de vértices, mas diminui em 1 o número de faces, já os os vértices terminais desta aresta se ligam por um outro caminho. Aplicamos a indução. Ou seja: $|V'| + |F'| - |E'| = 2$. Mas como $|F'| = |F| - 1$ e $|E'| = |E| - 1$, temos o resultado. ■

Como $|V|$ e $|E|$ são constantes para qualquer desenho de G , vemos que $|F|$ é um invariante para qualquer desenho de um grafo planar. Este fato nos permitirá falar de dualidade em grafos planares.

1.4.2 Dualidade

Seja G um grafo planar, não necessariamente conexo. Consideramos um desenho G_d plano de G . Desenhemos o grafo plano⁴ $G_d^* = (V_d^*, E_d^*, F_d^*)$ colocando um vértice de V_d^* no interior de cada face de F_d e ligando dois vértices se as faces são vizinhas. Se por acaso a face for vizinha a si própria, ou seja, se existirem arestas tais que ambos os lados tenham a mesma face (serão as pontes), então construímos um laço incidente ao vértice correspondente para cada uma das arestas, e de modo que este laço cruze a ponte somente uma vez. Chamaremos este de *desenho dual*.

É imediato observar que $|E_d| = |E_d^*|$, e mais, olhando para os desenhos de G_d e G_d^* , cada aresta de E_d cruzará com uma única aresta de E_d^* , o que nos permite identificar os conjuntos E_d e E_d^* como essencialmente os mesmos. Temos também $V_d \sim F_d^*$ e $F_d \sim V_d^*$. Seja $\varphi_{G_d \rightarrow G_d^*}$ a notação para a função $G_d \rightarrow G_d^*$ que identifica $(V_d, E_d, F_d) \sim (F_d^*, E_d^*, V_d^*)$.

Em geral, dado um grafo planar abstrato G , denotaremos por G^* um grafo abstrato cujo desenho seja dual de um desenho de G . É um fato triste não existir unicidade⁵ em geral para G^* .

Nas argumentações a seguir, quando escrevemos G^* , queremos dizer “qualquer grafo abstrato dual *arbitrário*” de G .

⁴Por enquanto visto apenas como desenho.

⁵Mesmo considerando “a menos de isomorfismos”.

Proposição 1.6. Seja G um grafo planar qualquer. Então G^* é conexo.

Em particular, se G é desconexo, com componentes G_1, \dots, G_n , então G^* é o grafo formado pelos blocos G_1^*, \dots, G_n^* , onde n vértices,⁶ um em cada bloco, são identificados como o mesmo em G^* .

Demonstração. De fato, basta observar que qualquer curva no plano ligando um ponto no interior de uma face F_1 e outro no interior de F_2 pode ser ajustado para cruzar somente arestas do desenho do grafo. As arestas que forem cruzadas induzirão um caminho no desenho dual, portanto no pseudo-dual. Mas isso para qualquer par de faces, logo um caminho entre qualquer par de vértices no pseudo-dual.

Para ver a segunda parte, basta observarmos que um vértice em cada G_k^* é referente à face ilimitada de G , mas esta face é a mesma para cada G_k , portanto este vértice deve ser o mesmo em G^* . ■

Proposição 1.7. Um grafo planar G é conexo se, e somente se,

$$G^{**} = G$$

e por este motivo, diremos que somente os grafos planares conexos possuem *duais verdadeiros*.

Demonstração. Pela proposição anterior, é óbvio que se G não for conexo, então não possui um dual verdadeiro.

Seja G conexo, precisamos mostrar que a função $\varphi_{G_d^* \rightarrow G_d^{**}} \circ \varphi_{G_d \rightarrow G_d^*}$ é essencialmente a identidade de G . Ela já é a identidade em E . Observamos agora que:

$$|V_d| - |E_d| + |F_d| = |V_d^*| - |E_d^*| + |F_d^*| = |V_d^{**}| - |E_d^{**}| + |F_d^{**}| = 2$$

Obviamente $|E_d| = |E_d^*| = |E_d^{**}|$. Também vale $|F_d| = |V_d^*|$ e $|F_d^*| = |V_d^{**}|$ por definição. Mas então:

$$|V_d| + |F_d| = |V_d^*| + |F_d^*| \Rightarrow |V_d| = |F_d^*|$$

E também:

$$|V_d^*| + |F_d^*| = |V_d^{**}| + |F_d^{**}| \Rightarrow |V_d^*| = |F_d^{**}|$$

Em geral, dado um vértice v em V_d , ao aplicarmos $\varphi_{G_d \rightarrow G_d^*}$, este vértice se identifica a uma face de modo canônico - é a face que será incidente às arestas que são imagens por meio de φ das arestas que eram incidentes em v . O que pode ocorrer é que dois vértices tornem-se uma mesma face, mas as igualdades acima garantem que isso jamais ocorrerá. Neste sentido, cada vértice será associado a uma face que é incidente exatamente às arestas que são imagens das arestas que eram incidentes ao vértice. Ou seja, se e_1, \dots, e_m eram incidentes a v , então a face $f^* = \varphi_{G_d \rightarrow G_d^*}(v)$ terá exatamente as arestas $\varphi_{G_d \rightarrow G_d^*}(e_1), \dots, \varphi_{G_d \rightarrow G_d^*}(e_m)$ como borda. Mas então, por definição, o vértice $\varphi_{G_d^* \rightarrow G_d^{**}}(f^*)$ será incidente exatamente às arestas $\varphi_{G_d^* \rightarrow G_d^{**}} \circ \varphi_{G_d \rightarrow G_d^*}(e_1) = e_1, \dots, \varphi_{G_d^* \rightarrow G_d^{**}} \circ \varphi_{G_d \rightarrow G_d^*}(e_m) = e_m$, que eram as arestas incidentes a v . ■

⁶Não são arbitrários.

Proposição 1.8. Seja G um grafo planar qualquer, digamos com componentes conexas G_1, \dots, G_n ($n = 1$ se G conexo). Então G^{**} é exatamente igual ao grafo obtido quando um vértice, não arbitrário, de cada G_k , são identificados como o mesmo.

Demonstração. Imediata após as duas proposições acima, basta considerar o dual do grafo formado pela união disjunta de G_1^*, \dots, G_n^* . ■

Ao longo do texto a seguir, quando escrevermos G^* , estaremos nos referindo ao grafo obtido a partir G pela operação de dualidade. Se quisermos nos referir ao grafo cuja operação de dualidade resulta em G , escreveremos *G . Ou seja, com G qualquer, por definição:

$$G = ({}^*G)^*$$

Mas vimos que se G não é conexo, então a igualdade a seguir não vale em geral:

$$G = {}^*(G^*)$$

valendo sempre somente se G for conexo. Na proposição a seguir, novamente omitiremos o índice d .

Proposição 1.9 (Relação de Euler revisitada). Se o grafo G é planar, vale:

$$|V| - |E| + |F| = \kappa(G) + \kappa(G^*)$$

Se G é conexo, *G qualquer grafo cuja dualização resulte em G , então:

$$|{}^*V| - |{}^*E| + |{}^*F| = \kappa({}^*G) + \kappa(G)$$

Demonstração. Para a primeira, basta repetirmos a demonstração original, observando que $\kappa(G^*) = 1$ para todo G , e trocando a frase “Se toda aresta for uma ponte, então G é uma árvore, e o resultado segue trivialmente ao observarmos que $|E| = m$, $|V| = m + 1$ ” pela frase: “Se toda aresta for uma ponte, então G é uma floresta, e o resultado segue trivialmente ao observarmos que $|E| = m$, $|V| = m + \kappa(G)$.” Para a segunda, basta trocar G por *G acima. ■

Ao longo do texto, em geral, não será propriamente relevante se o grafo planar considerado é ou não conexo, salvo quando mencionado o contrário.

1.4.3 Dualidade em matróides gráficas

Lembramos que $M(G)$ é a matróide associada ao grafo G , definida no conjunto de arestas do grafo, de modo que o posto de um conjunto de arestas é a cardinalidade (em arestas) da maior floresta contida no conjunto. Ou seja:

$$r(A) = |V(G)| - \kappa(G_A)$$

Lembramos que M^* é a matróide dual associada a M , definida sobre o mesmo conjunto E , de modo que:

$$r^*(A) = |A| + r(E \setminus A) - r(E)$$

Teremos essencialmente um resultado fundamental.

Teorema 1.1. Seja G um grafo planar e G^* um dual seu. Então:

$$M(G^*) \simeq M(G)^*$$

Seja A um conjunto de arestas em G , \bar{A} seu complementar.

Lema 1.1. Seja G um grafo e G^* um dual seu. Seja $A \subset E$. Denotaremos por $G_{A^*}^*$ o subgrafo gerador de G^* induzido por A^* , i.e., as arestas canonicamente associadas a A . Então:

$$\kappa(G_{A^*}^*) = |F(G_{\bar{A}})|$$

Demonstração. Não há dificuldades. Olhando para o desenho sobreposto do grafo e seu dual, notamos que uma face em $F(G_{\bar{A}})$ vai separar dois componentes em $G_{A^*}^*$, um que ficará dentro da face, e outro que ficará fora. Por outro lado, olhamos para um componente de $G_{A^*}^*$ e seu complementar. O conjunto de arestas que incide nesta componente e no complementar (corte) induz um ciclo em G . Mas o lado deste ciclo voltado para a componente conexa será uma face, caso contrário poderia ser decomposto em faces, induzindo uma decomposição em componentes desconexas de uma componente conexa de $G_{A^*}^*$, uma contradição. ■

Demonstração do teorema. Começamos observando que a matróide gráfica associada a um grafo não distingue um grafo desconexo e o grafo conexo obtido unindo as componentes desconexas ao identificarmos um vértice. Por este motivo, vamos supor sem perda de generalidade que G é conexo.

Temos que:

$$r^*(A) = |A| + r(\bar{A}) - r(E)$$

Em termos de grafos, isso quer dizer:

$$r^*(A) = |E| - |\bar{A}| + (|V| - \kappa(G_{\bar{A}})) - (|V| - \kappa(G)) = |E| - |\bar{A}| + 1 - \kappa(G_{\bar{A}})$$

Agora o posto de A^* é:

$$r(A^*) = |V^*| - \kappa(G_{A^*}^*)$$

Pela fórmula de Euler, temos que:

$$|V^*| = 2 - |V| + |E|$$

Ou seja:

$$r(A^*) = 2 - |V| + |E| - \kappa(G_{A^*}^*)$$

Lembramos que o objetivo é mostrar que:

$$r(A^*) = r^*(A)$$

Mas, cancelando o termo $|E|$, isto se resume a mostrar que:

$$2 - |V| - \kappa(G_{A^*}^*) = -|\bar{A}| + 1 - \kappa(G_{\bar{A}})$$

O resultado é portanto equivalente à seguinte igualdade:

$$\kappa(G_{A^*}^*) = 1 - |V| + |\bar{A}| + \kappa(G_{\bar{A}})$$

Lembramos que $|V| = |V(G_{\bar{A}})|$ por definição de subgrafo gerador. A fórmula de Euler aplicada ao grafo $G_{\bar{A}}$ nos diz que:

$$|F(G_{\bar{A}})| = 1 - |V(G_{\bar{A}})| + |\bar{A}| + \kappa(G_{\bar{A}})$$

Nossa conclusão é que:

$$r^*(A) = r(A^*) \text{ se, somente se, } \kappa(G_{A^*}^*) = |F(G_{\bar{A}})|$$

mas a condição da direita foi exatamente o lema anterior. ■

1.5 UM POUCO DE ÁLGEBRA ABSTRATA

1.5.1 Grupos

Nesta subseção, usaremos G para denotar um conjunto qualquer. Falaremos brevemente de grupos, com o objetivo de demonstrar um resultado que será usado no capítulo 4.

Definição 1.3. Um *grupo* $(G, *)$ é um par ordenado de um conjunto G e uma operação binária $*$ fechada neste conjunto satisfazendo:

- (1) Associatividade: $(a * b) * c = a * (b * c)$ para todos $a, b, c \in G$.
- (2) Existência de elemento neutro: Existe um $e \in G$ tal que $e * a = a * e = a$ para todo $a \in G$.
- (3) Existência de inverso: Para todo $a \in G$, existe um $b \in G$ tal que $a * b = b * a = e$. Este b é usualmente denotado por a^{-1} .

Será comum nos referirmos a um grupo $(G, *)$ simplesmente por G quando a operação em questão for óbvia. Será comum também omitirmos o sinal desta operação, ou seja, $a * b = ab$.

Um grupo G satisfazendo $ab = ba$ para quaisquer $a, b \in G$ é chamado grupo *comutativo* ou *abeliano*.

Um *subgrupo* de $(G, *)$ é um grupo $(G', *)$ satisfazendo $G' \subset G$.

Um *homomorfismo* de um grupo $(G, *)$ para um grupo (H, \star) é uma função $\varphi : G \rightarrow H$ satisfazendo:

$$\varphi(a * b) = \varphi(a) \star \varphi(b)$$

para todos $a, b \in G$.

Um homomorfismo é chamado de *isomorfismo* se for uma bijeção.

Sugerimos Meier [Mei08] para melhores referências acerca do que segue.

Um grupo G age sobre um conjunto X se as seguintes condições se verificam:

1. $g : X \rightarrow X$ para todo $g \in G$
2. Se $e \in G$ é a identidade, então $e(x) = x$ para todo $x \in X$
3. Para todos $g, h \in G$, temos $g(h(x)) = gh(x)$ para todo $x \in X$

É trivial observar que todo elemento g induz uma permutação no conjunto. Por este mesmo motivo, grupos são identificados com permutações em um conjunto, e as permutações de um conjunto formam um grupo natural cuja operação é a composição. De fato, todo grupo abstrato é isomorfo a um grupo de permutações (Cayley).

A *órbita* de um elemento $x \in X$ é definida por:

$$x^G = \{g(x) : g \in G\}$$

O estabilizador de um elemento $x \in X$ é definido por:

$$G_x = \{g \in G : g(x) = x\}$$

Denotamos os elementos fixados por g como $\text{fix}(g)$, ou seja:

$$\text{fix}(g) = \{x \in X : g(x) = x\}$$

Lema 1.2. O estabilizador de qualquer elemento é um subgrupo.

Demonstração. Notamos que $G_x \subset G$. Vamos mostrar que é um grupo com a mesma operação que G . A associatividade é natural a partir da definição de ação de um grupo em um conjunto. O elemento neutro pertence a G_x pelo mesmo motivo. Resta ver que, se $g \in G_x$, então g^{-1} também estará em G_x . Mas então se $g(x) = x$, aplicando g^{-1} em ambos os lados, teremos $x = g^{-1}(x)$, como queríamos. ■

Lema 1.3. As órbitas particionam o conjunto.

Demonstração. Basta notar que $g(y) \in x^G \Rightarrow g(y) = h(x) \Rightarrow y = g^{-1}h(x) \Rightarrow y \in x^G$. Ou seja, se há uma interseção entre y^G e x^G , então $y^G \subset x^G$. Por simetria, teremos a igualdade. ■

Agora seja H um subgrupo de G . Uma *classe lateral a esquerda* de H é um conjunto do tipo aH , onde $a \in G$.

Lema 1.4. As classes laterais particionam o grupo e são equicardinais.

Demonstração. Note que:

$$ah_1 = bh_2 \Rightarrow a = b(h_2h_1^{-1}) \in bH$$

Logo $aH \subset bH$. A mesma argumentação funciona trocando a por b , donde concluímos a igualdade. Ou seja, se há uma interseção, automaticamente temos a igualdade. É trivial observar que $|aH| = |H|$, pois $ah_1 \neq ah_2 \Leftrightarrow h_1 \neq h_2$.

Lema 1.5. As classes laterais a esquerda do estabilizador de x correspondem exatamente aos elementos da órbita de x .

Demonstração. Basta observar que:

$$aG_x = bG_x \Leftrightarrow b^{-1}aG_x = G_x \Leftrightarrow b^{-1}a \in G_x \Leftrightarrow b^{-1}a(x) = x \Leftrightarrow a(x) = b(x)$$

Lema 1.6. Para qualquer grupo G agindo sobre qualquer conjunto X , vale que:

$$|G| = |G_x||x^G| \text{ para qualquer } x \in X$$

Demonstração. Lembre-se que as classes laterais de um subgrupo são equicardinais e particionam o grupo, ie, o tamanho do grupo é o tamanho do subgrupo vezes a quantidade de classes. Mas cada classe de x corresponde a um elemento da órbita.

Teorema 1.2 (Lema de contagem de órbitas). O número de órbitas na ação de G sobre X é dado por:

$$\frac{1}{|G|} \sum_{g \in G} |\text{fix}(g)|$$

Demonstração. Obtemos este resultado fazendo dupla contagem nos pares (g, x) em que $g(x) = x$. Teremos:

$$\sum_{g \in G} |\text{fix}(g)| = \sum_{x \in X} |G_x| = \sum_{x \in X} \frac{|G|}{|x^G|}$$

Ou seja:

$$\sum_{x \in X} \frac{1}{|x^G|} = \frac{1}{|G|} \sum_{g \in G} |\text{fix}(g)|$$

Mas o que está no lado esquerdo é justamente o número de órbitas, pois cada órbita irá contribuir ao somatório com $|x^G| \cdot \frac{1}{|x^G|} = 1$, já que elas particionam o conjunto.

1.5.2 Anéis e domínios

Adicionando uma segunda operação, teremos os anéis.

Definição 1.4. Um *anel* $(A, +, *)$ é uma tripla ordenada de conjunto A e de duas operações, de modo que $(A, +)$ é um grupo abeliano, e que:

* é associativa.

* é distributiva com respeito a $+$, ou seja, $a * (b + c) = a * b + a * c$, e também $(b + c) * a = b * a + c * a$.

Em geral, chamamos a operação $+$ de soma no anel, e $*$ de produto no anel, que usualmente poderá ter o sinal omitido.

Um anel ainda *pode* satisfazer as seguintes propriedades:

- (1) $\exists u \in A : au = a = ua \forall a \in A$ (existência de unidade multiplicativa).
- (2) $ab = ba \forall a, b \in A$ (comutatividade do produto).
- (3) Seja 0 o elemento neutro da $+$. Vale então que $ab = 0 \Rightarrow a = 0$ ou $b = 0$ (não existem *divisores de zero*).
- (4) Vale (1) e para cada $a \in A$ tal que $a \neq 0$, existe um $b \in A$ tal que $a \cdot b = b \cdot a = u$ (existência de inverso multiplicativo).

Definição 1.5. Um anel satisfazendo (1) é um anel com unidade.

Um anel satisfazendo (2) é um anel comutativo.

Um anel satisfazendo (1),(2) e (3) é um domínio de integridade.

Um anel satisfazendo (2) e (4) é um corpo.

Um anel satisfazendo (4), mas que não satisfaça (2), é um anel de divisão.

Exemplos típicos de anéis com unidade são os conjuntos de matrizes quadradas de tamanho fixo sobre um corpo. Para anéis comutativos, temos os inteiros módulo n , denotados por \mathbb{Z}_n . Para domínios de integridade, temos os inteiros \mathbb{Z} . Os corpos mais comuns são \mathbb{Q} , \mathbb{R} e \mathbb{C} . O exemplo típico para anéis de divisão são os quatérnios.

Proposição 1.10. Um corpo é um domínio de integridade. Um anel de divisão é um domínio de integridade. Em geral, um divisor de zero não pode ser invertível.

Demonstração. Basta mostrarmos que (4) implica que não existem divisores de zero. Se $ab = 0$, supondo sem perda de generalidade que $a \neq 0$, multiplicamos por a^{-1} pela esquerda e temos $b = 0$. Logo a não é um divisor de zero. Por simetria, o mesmo vale para b . Mas isto é para quaisquer elementos do anel, logo A é domínio de integridade. ■

Alguns resultados são fáceis a partir do que falamos, por exemplo, o fato que todo domínio finito é um corpo. Nesta mesma linha, temos um dos resultados mais surpreendentes que pode ser obtido apenas a partir de definições simples: o fato que todo anel de divisão finito também é um corpo. Infelizmente, esses temas não fazem parte do escopo deste texto, e não apresentaremos suas demonstrações. Sugerimos [Her75] para elas.

1.5.3 Ideais e Módulos

Definição 1.6. Definimos um subconjunto $I \subset A$ como sendo um *ideal* se as seguintes propriedades se verificam:

1. Se $a \in I$ e $b \in I$, então $a + b \in I$.
2. Se $a \in I$ e $x \in A$ é um elemento qualquer, então $ax \in I$.

O subconjunto dos números pares é um ideal de \mathbb{Z} . Aliás, $n \cdot \mathbb{Z}$ é um ideal para todo n .

Definição 1.7. Um ideal é dito *principal* se for gerado por um único elemento, ou seja, se todo elemento do ideal for o produto deste elemento por outro qualquer. Denotamos o ideal I gerado por a por $I = (a)$. Daí $y \in (a) \Leftrightarrow y = ax$ para algum x .

Definição 1.8. Um domínio A é de *ideais principais* (DIP) se todo ideal é principal.

É fácil mostrar que \mathbb{Z} é um DIP, em particular, dado um ideal em \mathbb{Z} gerado por alguns elementos, o MDC desses elementos será um gerador único deste ideal.

Introduzimos ainda a definição de módulo. Com exceção do teorema da próxima subseção, as propriedades de módulos serão apresentadas somente quando necessário, e a maior parte delas no final do capítulo 4.

Definição 1.9. Dado um anel A , dizemos que M é um *A -módulo à esquerda* se $(M, +)$ for um grupo abeliano e se existir a operação $\bullet : (A, M) \rightarrow M$ satisfazendo:

$$a \bullet (r + s) = a \bullet r + a \bullet s$$

$$(a + b) \bullet r = a \bullet r + b \bullet r$$

$$a \bullet (b \bullet r) = (ab) \bullet r$$

para todos $a, b \in A$ e $r, s \in M$.

Um A -módulo à direita é definido de forma análoga. Diremos simplesmente um A -módulo se a operação \bullet for comutativa. Observe que trata-se apenas de uma generalização da noção de espaço vetorial para quando temos um anel qualquer como conjunto de escalares ao invés de um corpo.

1.5.4 Primeiro teorema de homomorfismos para módulos

Sejam M e N módulos sobre um anel A . Um *homomorfismo* entre módulos, assim como definimos para grupos, é uma função que preserva as operações nos módulos. De certa forma, é como se a função fosse distributiva com respeito à operação do seu domínio.

Um *sub-módulo* de M é um subconjunto $M' \subset M$ que seja também um A -módulo com as mesmas operações de M .

Seja $M' \subset M$ um sub-módulo. Definimos a relação \sim em M por:

$$r \sim s \Leftrightarrow r - s \in M'$$

Trata-se de uma *relação de equivalência*.

A *classe de equivalência* de um elemento $r \in M$ é definida como sendo o conjunto de todos os $s \in M$ tais que $r \sim s$. Mostra-se com facilidade que as classes de equivalência particionam M . O conjunto de todas as classes de equivalência é denotado por M/M' , e é chamado de *quociente* de M por M' . É fácil mostrar que M/M' é um A -módulo. Denotaremos em geral a classe de um elemento r por \bar{r} .

O *núcleo* de um homomorfismo $\varphi : M \rightarrow N$ é definido por:

$$\text{Nuc}(\varphi) = \{r \in M : \varphi(r) = 0\}$$

onde este 0 representa o elemento neutro da soma no módulo.

É trivial mostrar que $\text{Nuc}(\varphi)$ é um sub-módulo de M e que $\text{Im}(\varphi)$, a imagem de φ , é um sub-módulo de N .

Teremos então:

Teorema 1.3. Seja $\varphi : M \rightarrow N$ um homomorfismo. Então:

$$M/\text{Nuc}(\varphi) \simeq \text{Im}(\varphi)$$

Este símbolo \simeq significa que os dois módulos são isomorfos.

Demonstração. Considere a função:

$$\phi : M/\text{Nuc}(\varphi) \rightarrow \text{Im}(\varphi)$$

definida por:

$$\phi(\bar{r}) = \varphi(r)$$

Trata-se de um homomorfismo, pois:

$$\phi(\bar{r} + \bar{s}) = \phi(\overline{r+s}) = \varphi(r+s) = \varphi(r) + \varphi(s) = \phi(\bar{r}) + \phi(\bar{s})$$

É obviamente sobrejetiva. Para mostrar simultaneamente que está bem definida e que é injetiva, observe que:

$$\begin{aligned} \phi(\bar{r}) = \phi(\bar{s}) &\Leftrightarrow \phi(\bar{r}) - \phi(\bar{s}) = 0 \Leftrightarrow \phi(\overline{r-s}) = 0 \Leftrightarrow \\ &\Leftrightarrow \varphi(r-s) = 0 \Leftrightarrow r-s \in \text{Nuc}(\varphi) \Leftrightarrow \bar{r} = \bar{s} \end{aligned}$$

o que conclui a demonstração. ■

Observe que todo grupo G possui uma estrutura de \mathbb{Z} -módulo. De fato, a operação natural $\bullet : (\mathbb{Z}, G) \rightarrow G$ é simplesmente $n \bullet g = \underbrace{ggg\dots g}_{n \text{ vezes}}$ se n for positivo, ou $n \bullet g = (ggg\dots g)^{-1}$ se n negativo.

Um anel A por sua vez é um módulo sobre si próprio, e um homomorfismo $A \rightarrow B$ induz uma estrutura de A -módulo em B .

Com alguns ajustes, é possível mostrar *mutatis mutandis* que o teorema de homomorfismos apresentado vale para grupos e para anéis.

CAPÍTULO 2

POLINÔMIOS EM GRAFOS E MATRÓIDES

Este é o capítulo que introduz o assunto desta dissertação.

Primeiramente, vamos falar de polinômios que contam certas estruturas em um grafo. São essencialmente polinômios em uma variável.

Na segunda seção, apresentaremos o polinômio de Tutte. Falaremos de definições alternativas e aplicações.

Na última seção, mostraremos que todos estes polinômios são na verdade casos particulares de um polinômio universal. O belo resultado a ser mostrado é que este polinômio universal é essencialmente igual ao polinômio de Tutte.

2.1 COLORAÇÕES, TENSÕES, FLUXOS E CONFIABILIDADE

Nesta seção, vamos falar de colorações, tensões, fluxos e confiabilidade em grafos, introduzindo *counting polynomials*. Nossa principal ferramenta serão as operações de remoção e contração de arestas. O objetivo será introduzir exemplos de uma idéia a ser generalizada na próxima seção. Começaremos falando de colorações.

2.1.1 Colorações

Uma n -coloração no conjunto de vértices de um grafo G é uma função

$$c : V(G) \rightarrow S, \quad |S| = n$$

Dizemos que é *própria* se $c(v) \neq c(w)$ sempre que v e w sejam vizinhos. Como quase todas as colorações que nos interessam são as próprias, vamos simplesmente omitir este adjetivo, convencionando que ele estará sempre implícito, salvo se dito o contrário. Chamamos os elementos de S de cores. Dizemos que G é n -colorável se existir alguma coloração em n cores. Dizemos que é k -cromático se k é o menor n tal que G é n -colorável. Denotamos tal k por $\chi(G)$. Muitos resultados existem a respeito da existência de colorações e das condições necessárias para elas, e o leitor interessado pode consultar Bollobás [Bol98] ou Diestel [Die05], mas nosso objetivo agora será contar quantas colorações um grafo possui. Seguiremos basicamente Aigner [Aig07].

Seja $\chi_G(\lambda)$ uma função que determina o número de λ -colorações que um grafo possui. Algumas observações são imediatas:

$$\chi_G(\lambda) = 0 \text{ para todo } \lambda \text{ se } G \text{ possui um laço.}$$

$$\chi_{E_n}(\lambda) = \lambda^n$$

$$\chi_{G_1 \sqcup G_2}(\lambda) = \chi_{G_1}(\lambda) \cdot \chi_{G_2}(\lambda) \text{ onde } \sqcup \text{ denota a união disjunta dos grafos.}$$

Vamos introduzir uma relação de recorrência que permita calcular $\chi_G(\lambda)$ a partir do valor da função nos menores de G .

Proposição 2.1. Seja $e = vw$ aresta que não seja laço. Então:

$$\chi_G(\lambda) = \chi_{G \setminus e}(\lambda) - \chi_{G/e}(\lambda)$$

Demonstração. Considere uma coloração c de $G \setminus e$. Temos que $c(v) = c(w)$ se, e somente se, esta coloração também é de G/e . Por outro lado, $c(v) \neq c(w)$ se, e somente se, esta é uma coloração para G . ■

A proposição acima nos fornece um método iterativo para calcular $\chi_G(\lambda)$, ao que mostraremos tratar-se de um polinômio. Vamos passar por cima do fato que não sabemos *a priori* se este processo iterativo resultará necessariamente em um único polinômio, mesmo que mudemos a ordem de remover/contrair as arestas. De fato há a unicidade, e assumimos isto tacitamente, mesmo que pudéssemos demonstrar facilmente por indução. Ocorre que obteremos este resultado como consequência de um resultado mais geral logo a seguir. Por ora, a seguinte proposição estabelece algumas propriedades.

Proposição 2.2. Seja G um grafo sem laços. Então:

- (i) $\chi_G(\lambda) = a_n \lambda^n + a_{n-1} \lambda^{n-1} + \dots + a_1 \lambda + a_0$ polinômio em λ com coeficientes em \mathbb{Z} .
- (ii) O grau de $\chi_G(\lambda)$ é $n = |V|$.
- (iii) $a_n = 1$, os coeficientes $a_n, \dots, a_{\kappa(G)}$ são não nulos com sinais alternantes, e $a_i = 0$ para todo $i < \kappa(G)$.
- (iv) Se $G = K_n$, então $\chi(K_n; \lambda) = \lambda(\lambda - 1) \dots (\lambda - n)$.

Demonstração. A demonstração de (i) e (ii) segue por indução em $|E|$. Primeiro, se $G = E_n$ não possui arestas, então $\chi(E_n; \lambda) = \lambda^n$. Agora sejam:

$$\chi_{G \setminus e}(\lambda) = b_n \lambda^n + \dots + b_0$$

$$\chi_{G/e}(\lambda) = c_{n-1} \lambda^{n-1} + \dots + c_0$$

Temos que $\text{grau}[\chi_G(\lambda)] = \text{grau}[\chi_{G \setminus e}(\lambda)] = n$. Ainda, $a_i = b_i - c_i$, mas b_i e c_i tem sinais opostos. Logo o sinal de a_i será igual ao de b_i . Para ver (iii), basta observar então que a_i será 0 quando $b_i = c_i = 0$, mas isto segue do fato que $\kappa(G) = \kappa(G/e) \leq \kappa(G \setminus e)$. Para (iv), note que não existe coloração definida para n cores ou menos, e que para mais cores trata-se apenas de fazer um arranjo simples nos vértices. ■

Chamamos então de $\chi_G(\lambda)$ de *polinômio cromático* de G . A pergunta natural que segue é se existe uma fórmula fechada para $\chi_G(\lambda)$, ou seja, se é possível calcular o polinômio cromático sem precisar efetuar as reduções. Tal fórmula existe, mas infelizmente ela não é facilmente computável.

Proposição 2.3. Seja G um grafo sem laços. Então:

$$\chi_G(\lambda) = (-1)^{|V|-\kappa(G)} \lambda^{\kappa(G)} \sum_{AC E} (-\lambda)^{r(E)-r(A)} (-1)^{n(A)}$$

A prova segue de uma aplicação do princípio da inclusão e exclusão. Não a apresentaremos, pois este resultado é corolário de um resultado mais geral apresentado na terceira seção deste capítulo.

2.1.2 Tensões

Dado um multigrafo $G = (V, E)$, tornamos este um grafo dirigido $G = (V, \vec{E})$ se a cada aresta $e = uv$, identificarmos um dos dois vértices como inicial, e o outro como final. Seja A um grupo abeliano escrito aditivamente. Uma A -tensão f em um multigrafo $G = (V, E)$ é uma função $f : \vec{E} \rightarrow A$ satisfazendo:

- (i) Para cada ciclo do grafo, a soma das tensões nas aresta de mesmo sentido que o ciclo é igual à soma das tensões nas arestas de sentido oposto.
- (ii) $f(e) \neq 0$ para toda $e \in \vec{E}$.

Esta segunda condição poderia ser excluída da definição original, e então teríamos que falar de *tensões que nunca se anulam*. Note que o número de tensões de um grafo não depende da orientação escolhida. Para ver isso, note que existe uma bijeção entre as tensões de uma determinada orientação e as tensões de outra. Basta que cada vez que se inverta o sentido de uma aresta, tomemos o inverso (no grupo) da tensão original na aresta para ser a tensão na aresta invertida.

Proposição 2.4. O número de A -tensões em um grafo, onde $|A| = k$, é dado por um polinômio $\tau_G(k)$ que não depende da estrutura do grupo, mas só da sua cardinalidade. E mais:

$$\tau_G(k) = \frac{\chi_G(k)}{k^{\kappa(G)}}$$

Duas demonstrações são possíveis neste momento. Uma é verificando que tensões satisfazem as mesmas relações de recorrência que colorações, com exceção do fato que $\tau_{E_n}(k) = 1 \neq k^n$. A outra demonstração consiste em mostrar de fato como obter uma tensão a partir de uma k -coloração, e faremos esta.

Demonstração. Seja $G = (V, \vec{E})$ grafo dirigido e A , onde $|A| = k$, grupo abeliano. Seja $f : V \rightarrow A$ uma coloração nos vértices. Seja $\partial f : E \rightarrow A$ tal que $\partial f(u \rightarrow v) = f(v) - f(u)$. Observe que trata-se de uma tensão. Com efeito, seja C ciclo, e $C^+ \subset C$ as arestas cuja orientação combina com a de C , sendo C^- seu complementar. Olhando para:

$$\sum_{e \in C^+} \partial f(e)$$

cada vértice vai aparecer nenhuma, uma vez ou duas vezes. Se aparecer duas vezes, significa que ele é final de uma aresta e inicial de outra, logo os termos se cancelam. Mas esta é a situação em que este mesmo vértice não aparece em

$$\sum_{e \in C^-} \partial f(e)$$

Equivalentemente se um vértice aparecer duas vezes na soma acima.

Os vértice que aparecem uma vez em uma das somas, também aparecem uma vez na outra. Se ele aparece como final em uma, também será final em outra, equivalentemente se for inicial. Concluímos então que:

$$\sum_{e \in C^+} \partial f(e) = \sum_{e \in C^-} \partial f(e)$$

Vimos que toda coloração induz uma tensão. Agora, uma tensão também induz uma coloração. Induz, na verdade, $k^{\kappa(G)}$ colorações. Basta que em cada componente conexa, escolhamos um valor para um dos vértices, e há k maneiras de fazermos isso. O restante dos valores será determinado pela tensão. ■

2.1.3 Fluxos

Consideramos um multigrafo $G = (V, \vec{E})$ dirigido. Denotaremos uma aresta e dirigida com início em u e término em v por $e = u \rightarrow v$, e diremos que $u = e^-$ e que $v = e^+$. Seja A um grupo abeliano escrito aditivamente. Um A -fluxo f em um multigrafo $G = (V, E)$ é uma função $f : \vec{E} \rightarrow A$ satisfazendo:

- (i) Para todo $u \in V(G)$, $\sum_{e^- = u} f(e) = \sum_{e^+ = u} f(e)$, em outras palavras, a quantidade de fluxo que entra em um vértice é igual à quantidade de fluxo que sai dele.
- (ii) $f(e) \neq 0$ para toda $e \in \vec{E}$.

Também esta segunda condição poderia ser excluída da definição original, e então teríamos que falar de *fluxos que nunca se anulam*. Observemos novamente que o número de fluxos de um grafo não depende da orientação escolhida. Para ver isso, note que existe uma bijeção entre os fluxos de uma determinada orientação e os fluxos de outra. Basta que cada vez que se inverta o sentido de uma aresta, tomemos o inverso (no grupo) do fluxo original na aresta para ser o fluxo na aresta invertida. Veremos futuramente que o número de fluxos também não depende da estrutura do grupo, somente da sua cardinalidade.

Definimos, a título de notação, $\partial(v) = \sum_{e^+ = v} f(e) - \sum_{e^- = v} f(e)$. O item (i) diz que $\partial(v) = 0$ para todo v .

Um primeiro fato a ser observado é que se um grafo possui uma ponte, então ele não pode possuir um fluxo. Para ver isso, suponha que uma ponte $b = u \rightarrow v$, onde $u \in X$

e $v \in Y$, X e Y componentes conexas do grafo $G \setminus b$. Suponha que exista um fluxo f . Vamos olhar para a componente X :

$$\sum_{v \in V(X)} \partial(v) = 0$$

pois cada um dos termos $\partial(v)$ é zero por hipótese. Rearrmando esta soma, teremos que o fluxo em cada aresta cujos extremos estejam contidos em X aparece duas vezes, uma vez positivamente como fluxo de chegada e uma vez negativamente como fluxo de saída. Logo o somatório nestas arestas será 0. A única aresta que é incidente a X mas não aparece neste conjunto é justamente a ponte b . Comparando os dois somatórios, teremos que:

$$f(b) = 0$$

contrariando a segunda hipótese acerca de fluxos.

Denotaremos agora $\varphi_G(A)$ o número de A -fluxos num grafo G . Um segundo fato a ser observado é que se e é um laço (dirigido), então ele pode receber qualquer valor não nulo em um fluxo. Ou seja:

$$\varphi_G(A) = (|A| - 1)\varphi_{G \setminus e}(A)$$

A seguir, teremos o seguinte:

Proposição 2.5. Seja $\varphi_G(A)$ como definido acima. Seja e uma aresta que não é nem um laço nem uma ponte. Então:

$$\varphi_G(A) = \varphi_{G/e}(A) - \varphi_{G \setminus e}(A)$$

Demonstração. Seja f um fluxo em $\varphi_{G/e}(A)$, onde $e = u \rightarrow v$. Seja x o vértice de G/e correspondente a u e v . Seja E_u^+ o conjunto das arestas de G/e que terminam em x mas que terminavam em u , o mesmo para E_v^+ , E_u^- e E_v^- . Note que um A -fluxo em G corresponde exatamente a um A -fluxo em G/e quando:

$$\sum_{w \in E_u^+} f(w) \neq \sum_{w \in E_u^-} f(w)$$

Nesta circunstância, temos que $\sum_{w \in E_u^+} f(w) - \sum_{w \in E_u^-} f(w) \neq 0$, e então $f(e)$ era igual a esta diferença. Por outro lado, um A -fluxo em $G \setminus e$ corresponde exatamente a um A -fluxo em G/e quando:

$$\sum_{w \in E_u^+} f(w) = \sum_{w \in E_u^-} f(w)$$

por motivos agora claros. █

De posse desses resultados, e observando fatos óbvios como que o número de fluxos em um ciclo C_n qualquer é exatamente $(|A| - 1)$ (um fluxo para cada elemento do grupo), é possível obter $\varphi_G(A)$ como um polinômio (e único!) a partir de iterações. Novamente não daremos muita atenção a este fato, ele seguirá como um corolário imediato de um resultado vindouro.

2.1.4 Confiabilidade

Citamos Godsil [GR04] a respeito desta seção. Consideramos agora um grafo $G = (V, E)$. Suponha que exista uma probabilidade fixa p , $0 \leq p \leq 1$, para que cada aresta seja independentemente removida. Vamos denotar por $C_G(p)$ a probabilidade do número de componentes conexas de G não aumentar. Esta é uma medida de quão confiável uma rede pode ser.

Alguns fatos são imediatos:

$$C_G(p) = C_{G \setminus e}(p) \text{ se } e \text{ é um laço}$$

e também

$$C_G(p) = (1 - p) \cdot C_{G/e}(p) = (1 - p) \cdot C_{G \setminus e}(p) \text{ se } e \text{ é uma ponte}$$

Note agora que:

Proposição 2.6. Se e não é laço nem ponte, então:

$$C_G(p) = pC_{G \setminus e}(p) + (1 - p)C_{G/e}(p)$$

Demonstração. Observe que a remoção da aresta e não irá alterar o número de componentes conexas de G . Com probabilidade p , o grafo G se tornará $G \setminus e$. Com probabilidade $(1 - p)$, teremos que G se tornará essencialmente a mesma coisa que G/e no que diz respeito à conectividade por arestas. ■

As informação acima nos permitem concluir trivialmente que $C_G(p)$ de fato trata-se de um polinômio, a ser chamada *polinômio de confiabilidade* do grafo G . Por mais uma vez, desta vez a última, postergaremos a demonstração detalhada deste fato para a terceira seção deste capítulo.

2.2 POLINÔMIO DE TUTTE

2.2.1 Definições para grafos

As quatro subseções anteriores nos levam a crer que determinadas características de um grafo são obtidas através da avaliação de certos polinômios. A pergunta natural que cabe neste momento é se é possível generalizar o que foi dito até agora.

O polinômio cromático zerava quando um grafo possuía um laço, e o polinômio de fluxo zerava se houvesse uma ponte. Em certo sentido, são colapsos que nos fazem perder muita informação a respeito do grafo. O polinômio de confiabilidade não nos permite distinguir exatamente a quantidade de laços do grafo. Veremos que, essencialmente, todos esses problemas podem ser superados se definirmos um polinômio em duas variáveis pelas relações a seguir.

Definição 2.1 (Definição indutiva). Seja $G = (V, E)$ um multigrafo. Seja $e \in E$. Definimos então:

$$T_{E_n}(x, y) = 1 \text{ para todo } n$$

e a recorrência:

$$T_G(x, y) = \begin{cases} xT_{G \setminus e}(x, y) & \text{se } e \text{ é ponte} \\ yT_{G \setminus e}(x, y) & \text{se } e \text{ é laço} \\ T_{G/e}(x, y) + T_{G \setminus e}(x, y) & \text{se } e \text{ não é ponte nem laço} \end{cases}$$

É claro que trata-se de um polinômio, e a unicidade para diferentes ordens na decomposição será verificada no próximo teorema. E mais, esta definição pode ser trivialmente generalizada para matróides. Vamos agora mostrar duas definições equivalentes para este mesmo polinômio. Lembramos que o posto de um conjunto A de arestas é a cardinalidade do maior independente nele contido (se estamos falando de matróides), ou simplesmente o tamanho de uma floresta geradora maximal para o subgrafo gerador G_A induzido por A . Em outras palavras:

$$r(A) = |V| - \kappa(G_A)$$

A nulidade é o complemento do posto:

$$n(A) = |A| - r(A)$$

Nestas condições:

Teorema 2.1 (Definição por meio de função geradora posto-nulidade). Seja $G = (V, E)$ multigrafo. Então:

$$T_G(x, y) = \sum_{A \subseteq E} (x-1)^{r(E)-r(A)} (y-1)^{n(A)}$$

Demonstração. Vamos mostrar por indução no número de arestas que $T_G(x, y)$ satisfaz a fórmula acima. Primeiro observemos que se $E = \emptyset$, então

$$T_{E_n}(x, y) = 1 = \sum_{A \subseteq \emptyset} (x-1)^{r(E)-r(A)} (y-1)^{n(A)}$$

Considere um grafo $G = (V, E)$ e fixe uma aresta qualquer e . Existe uma partição do conjunto das partes de E entre os subconjuntos que contém e , e os expressaremos por $A \cup e$, e subconjuntos que não contém, que expressaremos por $A \not\supset e$. Agora:

- (1) Se e é uma ponte, então $r_{G \setminus e}(E) = r(E) - 1$. Por outro lado, supondo que $e \notin A$, então $r_{G \setminus e}(A) = r(A)$ e logo $n_{G \setminus e}(A) = n(A)$. E ainda, $r(A \cup e) = r(A) + 1$ e $n(A \cup e) = n(A)$. Temos por hipótese indutiva que:

$$T_{G \setminus e}(x, y) = \sum_{A \not\supset e} (x-1)^{r(E)-r(A)-1} (y-1)^{n(A)}$$

E sabemos por definição de T_G que:

$$T_G(x, y) = xT_{G \setminus e}(x, y)$$

Logo:

$$\begin{aligned}
T_G(x, y) &= xT_{G \setminus e}(x, y) = T_{G \setminus e}(x, y) + (x-1)T_{G \setminus e}(x, y) \\
&= \sum_{A \not\ni e} (x-1)^{r(E)-r(A)-1} (y-1)^{n(A)} + (x-1) \sum_{A \not\ni e} (x-1)^{r(E)-r(A)-1} (y-1)^{n(A)} = \\
&= \sum_{A \cup e} (x-1)^{r(E)-r(A \cup e)} (y-1)^{n(A \cup e)} + \sum_{A \not\ni e} (x-1)^{r(E)-r(A)} (y-1)^{n(A)} = \\
&= \sum_{A \subset E} (x-1)^{r(E)-r(A)} (y-1)^{n(A)}
\end{aligned}$$

como queríamos.

- (2) Se e é um laço, então $r_{G \setminus e}(E) = r(E)$. Por outro lado, supondo que $e \notin A$, então $r_{G \setminus e}(A) = r(A)$ e logo $n_{G \setminus e}(A) = n(A)$. E ainda, $r(A \cup e) = r(A)$ e $n(A \cup e) = n(A) + 1$. Temos por hipótese indutiva que:

$$T_{G \setminus e}(x, y) = \sum_{A \not\ni e} (x-1)^{r(E)-r(A)} (y-1)^{n(A)}$$

E sabemos por definição de T_G que:

$$T_G(x, y) = yT_{G \setminus e}(x, y)$$

Logo:

$$\begin{aligned}
T_G(x, y) &= yT_{G \setminus e}(x, y) = (y-1)T_{G \setminus e}(x, y) + T_{G \setminus e}(x, y) = \\
&= (y-1) \sum_{A \not\ni e} (x-1)^{r(E)-r(A)} (y-1)^{n(A)} + \sum_{A \not\ni e} (x-1)^{r(E)-r(A)} (y-1)^{n(A)} = \\
&= \sum_{A \cup e} (x-1)^{r(E)-r(A \cup e)} (y-1)^{n(A \cup e)} + \sum_{A \not\ni e} (x-1)^{r(E)-r(A)} (y-1)^{n(A)} = \\
&= \sum_{A \subset E} (x-1)^{r(E)-r(A)} (y-1)^{n(A)}
\end{aligned}$$

como queríamos.

- (3) Se e não é laço nem ponte, e considerando $e \notin A \subset E$, então:

- $r(E) = r_{G \setminus e}(E) = r_{G/e}(E) + 1$
- $r(A \cup e) = \begin{cases} r(A) + 1 & \text{se } e \text{ é ponte em } G_{A \cup e} \\ r(A) & \text{caso contrário} \end{cases}$
- $n(A \cup e) = \begin{cases} n(A) & \text{se } e \text{ é ponte em } G_{A \cup e} \\ n(A) + 1 & \text{caso contrário} \end{cases}$
- $r(A) = r_{G \setminus e}(A) = \begin{cases} r_{G/e}(A) & \text{se } e \text{ é ponte em } G_{A \cup e} \\ r_{G/e}(A) + 1 & \text{caso contrário} \end{cases}$

$$\bullet n(A) = n_{G \setminus e}(A) = \begin{cases} n_{G/e}(A) & \text{se } e \text{ é ponte em } G_{A \cup e} \\ n_{G/e}(A) - 1 & \text{caso contrário} \end{cases}$$

Por hipótese indutiva em $G \setminus e$ e G/e , teremos:

$$\begin{aligned} T_{G \setminus e}(x, y) &= \sum_{A \not\ni e} (x-1)^{r(E)-r(A)} (y-1)^{n(A)} \\ T_{G/e}(x, y) &= \sum_{\substack{A \cup e \\ e \text{ ponte}}} (x-1)^{r(E)-1-r(A)} (y-1)^{n(A)} \\ &\quad + \sum_{\substack{A \cup e \\ e \text{ ã ponte}}} (x-1)^{r(E)-1-(r(A)-1)} (y-1)^{n(A)+1} \end{aligned}$$

Por definição de T_G , teremos:

$$T_G(x, y) = T_{G \setminus e}(x, y) + T_{G/e}(x, y)$$

Logo o polinômio de Tutte em G será dado por:

$$\begin{aligned} T_G(x, y) &= \sum_{\substack{A \cup e \\ e \text{ ponte}}} (x-1)^{r(E)-r(A)-1} (y-1)^{n(A)} + \sum_{\substack{A \cup e \\ e \text{ ã ponte}}} (x-1)^{r(E)-r(A)} (y-1)^{n(A)+1} \\ &\quad + \sum_{A \not\ni e} (x-1)^{r(E)-r(A)} (y-1)^{n(A)} = \sum_{\substack{A \cup e \\ e \text{ ponte}}} (x-1)^{r(E)-r(A \cup e)} (y-1)^{n(A \cup e)} \\ &\quad + \sum_{\substack{A \cup e \\ e \text{ ã ponte}}} (x-1)^{r(E)-r(A \cup e)} (y-1)^{n(A \cup e)} + \sum_{A \not\ni e} (x-1)^{r(E)-r(A)} (y-1)^{n(A)} \\ &= \sum_{A \subseteq E} (x-1)^{r(E)-r(A)} (y-1)^{n(A)} \end{aligned}$$

concluindo como queríamos. ■

Corolário 2.1.1. O polinômio de Tutte, como foi definido, é único! Ele independe da ordem de remoção/contração de arestas.

Para tal, basta notar que não há qualquer menção à ordem na fórmula obtida no teorema.

Apresentaremos agora uma terceira definição para o polinômio de Tutte. Antes disso, introduzimos alguma nomenclatura. Primeiro, dada uma floresta geradora maximal S e uma aresta $e \notin S$, existe um ciclo definido por e , o único ciclo em $S \cup e$. Da mesma forma, dada $f \in S$, existe um corte no grafo definido por f , o conjunto de arestas C tal que se $f' \in C$, então $(S - f) \cup f'$ é floresta geradora maximal. Digamos agora que exista uma ordem \prec nas arestas de G , digamos $E = \{e_1, \dots, e_m\}$, com $e_i \prec e_j \Leftrightarrow i < j$. Dada uma floresta fixa S , uma aresta f é chamada de *internamente ativa* se $f \in S$ e f é a menor aresta no corte definido por si. De modo dual, uma aresta e é *externamente ativa* se $e \notin S$ e e é a menor aresta no ciclo definido por e .

A *atividade interna* de S é o número de arestas internamente ativas que existem em S , e a *atividade externa* de S é o número de arestas externamente ativas em S .

Teorema 2.2 (Definição por meio da expansão em florestas geradoras maximais). Seja $G = (V, E)$ grafo com uma ordem total \prec em suas arestas. Então

$$T_G(x, y) = \sum_{i,j} t_{ij} x^i y^j$$

onde t_{ij} é o número de florestas geradoras maximais com atividade interna i e atividade externa j .

De fato este teorema parece muito diferente das definições anteriores, mas esperamos que a demonstração seja esclarecedora. Novamente será mais fácil mostrar que esta definição satisfaz as recorrências da definição indutiva, mas desta vez, vamos fazer uso da unicidade, escolhendo especificamente uma aresta para iniciarmos a decomposição.

Demonstração. Definimos $P_G(x, y) = \sum_{i,j} t_{ij} x^i y^j$ e vamos mostrar que esta definição satisfaz as recorrências. A unicidade do polinômio de Tutte obtido por meio delas irá nos garantir a igualdade $P_G(x, y) = T_G(x, y)$. Primeiro começamos notando que, trivialmente, $P_{E_n}(x, y) = 1$ pois \emptyset é uma (e única) floresta geradora sem atividades. Agora teremos que:

- (1) Se e é uma ponte, então $e \in S$ para toda floresta geradora maximal S . E mais, e é a única aresta no corte definido por si, portanto é internamente ativa em todas as florestas. Agora seja s_{ij} o número de florestas geradoras maximais em $G \setminus e$ com atividade interna i e atividade externa j . Fica claro portanto que:

$$s_{ij} = t_{(i+1)j}$$

onde t_{ij} é referente a G . Logo:

$$xP_{G \setminus e}(x, y) = x \sum_{i,j} s_{ij} x^i y^j = \sum_{i,j} t_{(i+1)j} x^{i+1} y^j = P_G(x, y)$$

- (2) Se e é um laço, então $e \notin S$ para toda floresta geradora maximal S . E mais, e é a única aresta no ciclo definido por si, portanto é externamente ativa em todas as florestas. Agora seja s_{ij} como acima. Fica claro portanto que:

$$s_{ij} = t_{i(j+1)}$$

Logo:

$$yP_{G \setminus e}(x, y) = y \sum_{i,j} s_{ij} x^i y^j = \sum_{i,j} t_{i(j+1)} x^i y^{j+1} = P_G(x, y)$$

- (3) Seja agora e a maior aresta por meio de \prec que não é laço nem ponte. Seja s_{ij} referente a $G \setminus e$ e r_{ij} referente a G/e . Vamos mostrar que $s_{ij} + r_{ij} = t_{ij}$. Para isto, considere S uma floresta geradora maximal em G com atividade interna i e atividade externa j .

Se $e \in S$, então $S - e$ é floresta em $G \setminus e$ se, e somente se, e é ponte. Logo $S - e$ não é floresta em $G \setminus e$, e não contribui em nada com s_{ij} . Por outro lado, $S - e$ é floresta em G/e , e uma aresta é internamente ativa em S se, e só se, o é em $S - e$, pois a e não pode ser já que é máxima. Uma aresta também será externamente ativa em S se, e só se, o for em $S - e$, pois e é máxima. Daí toda floresta S contendo e contribui igualmente na contagem de t_{ij} e de r_{ij} , sem alterar s_{ij} .

Se $e \notin S$, então $S - e$ é floresta em G/e se, e somente se, e é laço. Logo $S - e$ não é floresta em G/e , e não contribui em nada com r_{ij} . Por outro lado, $S - e$ é floresta em $G \setminus e$, e uma aresta é internamente ativa em S se, e só se, o é em $S - e$, pois e é máxima. Uma aresta também será externamente ativa em S se, e só se, o for em $S - e$, pois a e é máxima e não pode ser. Daí toda floresta S não contendo e contribui igualmente na contagem de t_{ij} e de s_{ij} , sem alterar r_{ij} .

Mais ainda, não há outra maneira de realizar estas contribuições, pois, fixada a aresta e , uma floresta ou a contém ou não a contém. ■

Corolário 2.2.1. O número t_{ij} independe da ordem \prec introduzida nas arestas do grafo.

De fato, não há qualquer menção a esta ordem na definição do Teorema 2.1.

Corolário 2.2.2. Os coeficientes em $T_G(x, y) = \sum_{A \subseteq E} (x - 1)^{r(E) - r(A)} (y - 1)^{n(A)}$ são todos positivos.

Pois assim claramente o são na expressão do Teorema 2.2.

2.2.2 Matróides

As considerações realizadas sobre polinômio de Tutte se estendem trivialmente para matróides, pois os conceitos de *remoção e contração de arestas* e de *posto e nulidade* são trivialmente generalizados para matróides. Temos então:

Definição 2.2. Seja M uma matróide sobre um conjunto E com posto r . Então definimos o polinômio de Tutte desta matróide por:

$$T_M(x, y) = \sum_{A \subseteq E} (x - 1)^{r(E) - r(A)} (y - 1)^{n(A)}$$

Observe que, obviamente, se $M(G)$ é a matróide gráfica associada ao grafo G , então:

$$T_{M(G)}(x, y) = T_G(x, y)$$

Proposição 2.7. Em geral, vale que:

$$T_M(x, y) = T_{M^*}(y, x)$$

Se G é planar, com dual G^* , então:

$$T_G(x, y) = T_{G^*}(y, x)$$

Demonstração. Lembramos que:

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

Logo:

$$r^*(E) - r^*(A) = |E| - r(E) - |A| - r(E - A) + r(E) = |E - A| - r(E - A) = n(E - A)$$

Por outro lado:

$$n^*(A) = |A| - r^*(A) = r(E) - r(E - A)$$

Teremos então que:

$$T_{M^*}(y, x) = \sum_{A \subseteq E} (y-1)^{r^*(E)-r^*(A)} (x-1)^{n^*(A)} = \sum_{A \subseteq E} (y-1)^{n(E-A)} (x-1)^{r(E)-r(E-A)} = T_M(x, y)$$

A última igualdade pois quando A percorre todos os subconjuntos de E , o mesmo ocorre com $E - A$.

Para ver a segunda afirmação, basta lembrarmos do Teorema 1.1, que dizia que:

$$M(G)^* = M(G^*)$$

■

O leitor deve ter notado que ainda não é possível explicitar os polinômios cromático, de fluxo e de confiabilidade a partir do polinômio de Tutte. Este será o objetivo da próxima seção, mas antes apresentamos algumas avaliações do polinômio de Tutte.

2.2.3 Avaliações do polinômio de Tutte

A seguir, apresentamos alguns exemplos de avaliações do polinômio de Tutte. Nos momentos em que aparecem termos 0^0 , estamos querendo dizer $x^0 \Big|_{x=0}$, daí $1 \Big|_{x=0} = 1$ (também com y no lugar de x).

Exemplo 2.1. Seja $\tau(G)$ número de florestas geradoras maximais de G . Então:

$$T_G(1, 1) = \tau(G)$$

De fato, teremos que:

$$T_G(1, 1) = \sum_{A \subseteq E} 0^{r(E)-r(A)} \cdot 0^{n(A)}$$

Logo só sobrevivem os termos em subconjuntos que $r(E) = r(A) = |A|$. Mas esses serão justamente as bases da matróide, ou florestas geradoras maximais do grafo. O somatório vai contar 1 para cada um desses conjuntos, o que conclui.

Exemplo 2.2. Seja $\tilde{\tau}(G)$ número de florestas de G . Então:

$$T_G(2, 1) = \tilde{\tau}(G)$$

De fato, teremos que:

$$T_G(2, 1) = \sum_{A \subseteq E} 1^{r(E)-r(A)} \cdot 0^{n(A)}$$

Logo sobrevivem todos os termos em subconjuntos que $r(A) = |A|$. Mas esses serão justamente os independentes da matróide, ou florestas do grafo.

Exemplo 2.3. $G = (V, E)$ grafo qualquer, então:

$$T_G(1, 2) = \text{número de subgrafos com mesmo posto que } G$$

Se G for conexo, este é o número de subgrafos geradores conexos. De fato, teremos que:

$$T_G(1, 2) = \sum_{A \subseteq E} 0^{r(E)-r(A)} \cdot 1^{n(A)}$$

Logo sobrevivem todos os termos em subconjuntos que $r(E) = r(A)$.

Exemplo 2.4. $G = (V, E)$ grafo qualquer, então:

$$T_G(2, 2) = 2^{|E|}$$

De fato, teremos que:

$$T_G(2, 2) = \sum_{A \subseteq E} 1^{r(E)-r(A)} \cdot 1^{n(A)}$$

O somatório vai contar 1 para cada subconjunto $A \subseteq E$, o que conclui.

2.3 INVARIANTE DE TUTTE-GROTHENDICK

2.3.1 Grafos

Nosso objetivo agora é apresentar uma definição bastante geral que nos permita obter os polinômios apresentados como casos particulares. Sempre utilizando a idéia da recorrência na construção do polinômio, vamos adicionar parâmetros. Observe:

Definição 2.3. Seja $U : \mathcal{G} \rightarrow \mathbb{Z}[x, y, \alpha, \sigma, \tau]$ denotado por $U_G(x, y, \alpha, \sigma, \tau)$ o *polinômio universal* de um grafo G numa classe de grafos \mathcal{G} fechada com respeito a tomada de menores, definido por meio dos fatos:

$$(i) \ U_{E_n}(x, y, \alpha, \sigma, \tau) = \alpha^n$$

$$(ii) \ U_G = \begin{cases} xU_{G \setminus e} & \text{se } e \text{ é uma ponte} \\ yU_{G \setminus e} & \text{se } e \text{ é um laço} \\ \sigma U_{G \setminus e} + \tau U_{G/e} & \text{se } e \text{ não é laço nem ponte} \end{cases}$$

A priori, não sabemos (1) nem se o resultado será mesmo um polinômio (2) nem se ele será único, pois a ordem para desconstruir do grafo pode ser relevante. É claro que por uma analogia ao polinômio de Tutte, somos levados a crer que estes temores são vãos. Mais que isso, vamos mostrar como obter $U_G(x, y, \alpha, \sigma, \tau)$ a partir de $T_G(x, y)$.

Teorema 2.3. Seja G grafo, T_G seu polinômio de Tutte, U_G seu polinômio universal como acima. Então, se $\sigma \neq 0$ e $\tau \neq 0$, teremos:

$$U_G(x, y, \alpha, \sigma, \tau) = \alpha^{\kappa(G)} \sigma^{n(E)} \tau^{r(E)} T_G\left(\frac{\alpha x}{\tau}, \frac{y}{\sigma}\right)$$

E mais, se $l(G)$ denota o número de laços e $p(G)$ o número de pontes, então:

$$(A) \quad U_G(x, y, \alpha, \sigma, 0) = \alpha^{|V(G)|} \sigma^{n(E)-l(G)} x^{r(E)} y^{l(G)}$$

$$(B) \quad U_G(x, y, \alpha, 0, \tau) = \alpha^{\kappa(G)+p(G)} \tau^{r(E)-p(G)} x^{p(G)} y^{n(E)}$$

$$(C) \quad U_G(x, y, \alpha, 0, 0) = \begin{cases} \alpha^{|V(G)|} x^{p(G)} y^{l(G)} & \text{se } E(G) \text{ consiste apenas de pontes e laços} \\ 0 & \text{caso contrário} \end{cases}$$

Observe que estamos encarando σ e τ como variáveis. A divisão efetuada é em certo sentido simbólica, ou então podemos imergir $\mathbb{Z}[x, y, \alpha, \sigma, \tau]$ em seu corpo de frações. Lembramos ao leitor que $\kappa(G)$ é o número de componentes conexas de G , $r(E)$ é o seu posto, ou seja, $|V(G)| - \kappa(G)$, e $n(E)$ sua nulidade, i.e., $|E| - r(E)$.

Demonstração. Vamos mostrar por indução no número de arestas de G . Se G não tem arestas, então:

$$\kappa(G) = n \quad r(E) = n(E) = 0$$

Daí

$$U_{E_n}(x, y, \alpha, \sigma, \tau) = \alpha^n = \alpha^n \sigma^0 \tau^0 T_{E_n}\left(\frac{\alpha x}{\tau}, \frac{y}{\sigma}\right)$$

por definição em T_{E_n} .

Agora fixamos uma aresta e qualquer em G . Por definição:

$$U_G = \begin{cases} xU_{G \setminus e} & \text{se } e \text{ é uma ponte} \\ yU_{G \setminus e} & \text{se } e \text{ é um laço} \\ \sigma U_{G \setminus e} + \tau U_{G/e} & \text{se } e \text{ não é laço nem ponte} \end{cases}$$

(i) Seja e uma ponte. Lembramos que neste caso:

$$T_G(\mathfrak{x}, \mathfrak{y}) = \mathfrak{x} T_{G \setminus e}(\mathfrak{x}, \mathfrak{y}) \text{ implicando que } T_{G \setminus e}(\mathfrak{x}, \mathfrak{y}) = \frac{T_G(\mathfrak{x}, \mathfrak{y})}{\mathfrak{x}}$$

então, por hipótese indutiva:

$$\begin{aligned} U_G &= xU_{G \setminus e} = x \cdot \alpha^{\kappa(G \setminus e)} \sigma^{n(G \setminus e)} \tau^{r(G \setminus e)} T_{G \setminus e}\left(\frac{\alpha x}{\tau}, \frac{y}{\sigma}\right) \\ &= x \alpha^{\kappa(G)+1} \sigma^{n(E)} \tau^{r(E)-1} \frac{T_G\left(\frac{\alpha x}{\tau}, \frac{y}{\sigma}\right)}{\alpha x / \tau} = \alpha^{\kappa(G)} \sigma^{n(E)} \tau^{r(E)} T_G\left(\frac{\alpha x}{\tau}, \frac{y}{\sigma}\right) \end{aligned}$$

como queríamos.

(ii) Seja e um laço. Lembramos que neste caso:

$$T_G(\mathbf{x}, \mathbf{y}) = \eta T_{G \setminus e}(\mathbf{x}, \mathbf{y}) \text{ implicando que } T_{G \setminus e}(\mathbf{x}, \mathbf{y}) = \frac{T_G(\mathbf{x}, \mathbf{y})}{\eta}$$

então, por hipótese indutiva:

$$\begin{aligned} U_G &= y U_{G \setminus e} = y \cdot \alpha^{\kappa(G \setminus e)} \sigma^{n(G \setminus e)} \tau^{r(G \setminus e)} T_{G \setminus e} \left(\frac{\alpha x}{\tau}, \frac{y}{\sigma} \right) \\ &= y \alpha^{\kappa(G)} \sigma^{n(E)-1} \tau^{r(E)} \frac{T_G \left(\frac{\alpha x}{\tau}, \frac{y}{\sigma} \right)}{y/\sigma} = \alpha^{\kappa(G)} \sigma^{n(E)} \tau^{r(E)} T_G \left(\frac{\alpha x}{\tau}, \frac{y}{\sigma} \right) \end{aligned}$$

como queríamos.

(iii) Seja e nem laço nem ponte. Lembramos que neste caso:

$$T_G(\mathbf{x}, \mathbf{y}) = T_{G \setminus e}(\mathbf{x}, \mathbf{y}) + T_{G/e}(\mathbf{x}, \mathbf{y})$$

então, por hipótese indutiva:

$$\begin{aligned} U_G &= \sigma U_{G \setminus e} + \tau U_{G/e} = \\ &= \sigma \alpha^{\kappa(G \setminus e)} \sigma^{n(G \setminus e)} \tau^{r(G \setminus e)} T_{G \setminus e} \left(\frac{\alpha x}{\tau}, \frac{y}{\sigma} \right) + \tau \alpha^{\kappa(G/e)} \sigma^{n(G/e)} \tau^{r(G/e)} T_{G/e} \left(\frac{\alpha x}{\tau}, \frac{y}{\sigma} \right) \\ &= \sigma \alpha^{\kappa(G)} \sigma^{n(E)-1} \tau^{r(E)} T_{G \setminus e} \left(\frac{\alpha x}{\tau}, \frac{y}{\sigma} \right) \\ &+ \tau \alpha^{\kappa(G)} \sigma^{n(E)} \tau^{r(E)-1} \left[T_G \left(\frac{\alpha x}{\tau}, \frac{y}{\sigma} \right) - T_{G \setminus e} \left(\frac{\alpha x}{\tau}, \frac{y}{\sigma} \right) \right] = \\ &= \alpha^{\kappa(G)} \sigma^{n(E)} \tau^{r(E)} T_G \left(\frac{\alpha x}{\tau}, \frac{y}{\sigma} \right) \end{aligned}$$

como queríamos.

Agora vamos mostrar (A), (B) e (C). Uma demonstração que garantisse a unicidade das expressões teria que utilizar o princípio da indução no número de arestas. Notamos que não haveria qualquer dificuldade em fazê-lo, mas seria longo pois haveria três casos (aresta sendo laço, ponte, ou nem um nem outro) para cada letra. A maneira que faremos, por desconstrução do grafo, não garante a unicidade, pois desconstruiremos o grafo em uma ordem específica. Todavia, é uma forma que esclarece muito mais como tais expressões foram obtidas.

Começamos observando que o formato terá que ser necessariamente monomial, pois nunca haverá uma soma, por definição.

(A) Seja T floresta geradora maximal do grafo. Removendo todas as arestas que não são laços e que não estão em T , aparecerá o termo $\sigma^{n(E)-l(G)}$. Agora removemos as arestas da floresta, todas pontes. Então teremos o termo $x^{r(E)}$. Removendo todos os laços, teremos $y^{l(G)}$. Sobrará justamente os vértices do grafo, daí teremos $\alpha^{|V(G)|}$.

- (B) Seja T floresta geradora maximal do grafo. Removendo todas as pontes do grafo G (obviamente contidas em T), e teremos o termo $x^{p(G)}$. Nosso grafo agora é formado por várias componentes conexas. Agora contraímos o restante das arestas de T , logo aparecendo o termo $\tau^{r(E)-p(G)}$. Este processo transformou cada componente conexa em um único vértice, possivelmente com laços. São exatamente todas as arestas que não faziam parte de T . Daí teremos o termo $y^{n(E)}$. O número de vértices é exatamente o número de componentes conexas após a remoção das pontes, ou seja, teremos $\alpha^{\kappa(G)+p(G)}$.
- (C) Se alguma aresta não é laço nem ponte, então $U_G = 0.U_{G \setminus e} + 0.U_{G/e}$. Se todas são laços ou pontes, então a remoção dos laços gerará o termo $y^{l(G)}$, a remoção das pontes o termo $x^{p(G)}$, e os vértices o termo $\alpha^{|V(G)|}$. ■

Este teorema faz com que o polinômio universal herde as propriedades do polinômio de Tutte.

2.3.2 Revisitando os polinômios cromático, de tensão, de fluxo e de confiabilidade

E mais: com este resultado, o polinômio de Tutte é (quase) tudo que precisamos saber para que obtenhamos os três polinômios mencionados na primeira seção. Observe:

Exemplo 2.5. O polinômio cromático é obtido a partir do polinômio universal fazendo $\alpha = \lambda$, $x = \frac{\lambda-1}{\lambda}$, $y = 0$, $\sigma = 1$ e $\tau = -1$.

Exemplo 2.6. O polinômio de tensão é obtido a partir do polinômio universal fazendo $\alpha = -1$, $x = \frac{\lambda-1}{\lambda}$, $y = 0$, $\sigma = 1$ e $\tau = -1$.

Exemplo 2.7. O polinômio de fluxo (sobre um grupo abeliano H) é obtido a partir do polinômio universal fazendo $\alpha = 1$ (por vacuidade), $x = 0$, $y = |H| - 1$, $\sigma = -1$ e $\tau = 1$. Em particular, o polinômio de fluxo só depende da cardinalidade do grupo, e não da sua estrutura. Por este motivo, se $|H| = q$, será comum nos referirmos ao polinômio não por $\varphi_G(H)$, e sim por $\varphi_G(q)$.

Exemplo 2.8. O polinômio de confiabilidade é obtido a partir do polinômio universal fazendo $\alpha = 1$ (por vacuidade), $x = (1 - p)$, $y = 1$, $\sigma = p$ e $\tau = (1 - p)$.

Exemplo 2.9. Naturalmente, o próprio polinômio de Tutte é um caso particular. Obtido com $\alpha = \sigma = \tau = 1$, x e y variáveis.

2.3.3 Formalização da idéia de invariante de Tutte-Grothendick

Introduzimos agora uma definição com o objetivo de formalizar o que vimos à vista de funções multiplicativas.

Definição 2.4. Seja \mathcal{G} uma classe de grafos fechada com respeito à tomada de menores. Um invariante gráfico f de \mathcal{G} para um anel comutativo R com unidade é chamado de *invariante generalizado de Tutte-Grothendick* ou *T-G invariante* se:

- (1) $f(E_1) = r$, r elemento do anel.
- (2) Existem a e b em R tais que para todo grafo G em \mathcal{G} e toda aresta ordinária (nem ponte nem laço) e vale que:

$$f(G) = af(G \setminus e) + bf(G/e)$$

- (3) Para quaisquer $G, H \in \mathcal{G}$, se $G \sqcup H \in \mathcal{G}$ e/ou $G * H \in \mathcal{G}$, então:

$$f(G \sqcup H) = f(G)f(H) \text{ e/ou } f(G * H) = \frac{f(G)f(H)}{r}$$

onde \sqcup denota a união disjunta, e $*$ denota a união disjunta de dois grafos fazendo com que um par determinado de vértices, um de cada grafo, se torne o mesmo na união. A esta união $*$, daremos o nome de união concatenada.

Dizemos que (r, a, b) são os parâmetros do T-G invariante.

O teorema abaixo diz que o polinômio universal apresentado é essencialmente o único invariante de Tutte-Grothendick para parâmetros dados.

Teorema 2.4. Seja \mathcal{G} classe de grafos fechada com respeito à tomada de menores. Seja R anel comutativo com identidade. Seja $f : \mathcal{G} \rightarrow R$. Se existirem $(r, a, b) \in R$ tais que f é um T-G invariante com tais parâmetros, então:

$$f(G) = r^{\kappa(G)} a^{n(E)} b^{r(E)} T_G \left(\frac{rx}{b}, \frac{y}{a} \right)$$

onde $f(P) = r^2x$ e $f(L) = ry$, $P = K_2$ e L grafo formado por um vértice e um laço.

E mais, sejam $r, a, b, x_0, y_0 \in R$. Então existe um único T-G invariante com parâmetros (r, a, b) satisfazendo $f(P) = r^2x_0$ e $f(L) = ry_0$, e é dado pela expressão acima.

Demonstração. Praticamente já mostramos este teorema. Essencialmente, o que devemos fazer é mostrar que esta definição de invariante de Tutte-Grothendick é a mesma do polinômio universal. Para tal, observe que:

$$f(E_n) = f(\underbrace{E_1 \sqcup \dots \sqcup E_1}_{n \text{ vezes}}) = f(E_1)^n = r^n$$

Seja agora $P = K_2$. Temos que se e é uma ponte em G , com G_1 e G_2 as componentes conexas separadas por e , então:

$$\begin{aligned} f(G) &= f(G_1 * P * G_2) = \\ &= \frac{1}{r^2} f(G_1) f(P) f(G_2) = \frac{1}{r^2} f(P) f(G_1 \sqcup G_2) = \frac{1}{r^2} f(P) f(G \setminus e) = x f(G \setminus e) \end{aligned}$$

e também, se e é um laço de G e L o grafo formado unicamente por um laço, então:

$$f(G) = f(G \setminus e * L) = \frac{1}{r} f(L) f(G \setminus e) = y f(G \setminus e)$$

■

2.3.4 O polinômio universal para matróides

De modo bastante análogo ao que fizemos até agora, poderíamos ter definido o polinômio universal para matróides, obviamente ignorando as considerações sobre número de vértices, e usando a analogia entre as pontes e os laços de um grafo com os colaços e os laços de uma matróide. Então teríamos:

Definição 2.5. Seja $U : \mathcal{M} \rightarrow \mathbb{Z}[x, y, \alpha, \sigma, \tau]$ denotado por $U_M(x, y, \alpha, \sigma, \tau)$ o *polinômio universal* de uma matróide M numa classe de matróides \mathcal{M} fechada com respeito a tomada de menores, definido por meio dos fatos:

$U_{M_\emptyset} = \alpha$ se M_\emptyset é a matróide definida no conjunto vazio.

$$U_M = \begin{cases} xU_{M \setminus e} & \text{se } e \text{ é um colaço} \\ yU_{M \setminus e} & \text{se } e \text{ é um laço} \\ \sigma U_{M \setminus e} + \tau U_{M/e} & \text{se } e \text{ não é laço nem colaço} \end{cases}$$

Teorema 2.5. Seja M matróide, T_M seu polinômio de Tutte, U_M seu polinômio universal como acima. Então, se $\sigma \neq 0$ e $\tau \neq 0$, teremos:

$$U_M(x, y, \alpha, \sigma, \tau) = \alpha \sigma^{n(E)} \tau^{r(E)} T_M \left(\frac{x}{\tau}, \frac{y}{\sigma} \right)$$

E mais, se $l(M)$ denota o número de laços e $c(M)$ o número de colaços, então:

- (A) $U_M(x, y, \alpha, \sigma, 0) = \alpha \sigma^{n(E) - l(M)} x^{r(E)} y^{l(M)}$
- (B) $U_M(x, y, \alpha, 0, \tau) = \alpha \tau^{r(E) - c(M)} x^{c(M)} y^{n(E)}$
- (C) $U_M(x, y, \alpha, 0, 0) = \begin{cases} \alpha x^{c(M)} y^{l(M)} & \text{se } E(M) \text{ consiste apenas de colaços e laços} \\ 0 & \text{caso contrário} \end{cases}$

Definição 2.6. Seja \mathcal{M} uma classe de matróides fechada com respeito à tomada de menores. Um invariante matroidal f de \mathcal{M} para um anel comutativo R com unidade é chamado de *invariante generalizado de Tutte-Grothendick* ou *T-G invariante* se:

- (1) $f(M_\emptyset) = r$, r elemento do anel.
- (2) Existem a e b em R tais que para todo grafo M em \mathcal{M} e toda aresta ordinária (nem ponte nem laço) e vale que:

$$f(M) = af(M \setminus e) + bf(M/e)$$

- (3) Para quaisquer $M, N \in \mathcal{M}$, se $M \sqcup N \in \mathcal{M}$, então:

$$f(M \sqcup N) = f(M)f(N)$$

Dizemos que (r, a, b) são os parâmetros do T-G invariante.

Teorema 2.6. Seja \mathcal{M} classe de matróides fechada com respeito à tomada de menores. Seja R anel comutativo com identidade. Seja $f : \mathcal{M} \rightarrow R$. Se existirem $(r, a, b) \in R$ tais que f é um T-G invariante com tais parâmetros, então:

$$f(M) = r a^{n(E)} b^{r(E)} T_M \left(\frac{x}{b}, \frac{y}{a} \right)$$

onde $f(C) = rx$ e $f(L) = ry$, C matróide composta por um colaço e L matróide formada por um laço.

E mais, sejam $r, a, b, x_0, y_0 \in R$. Então existe um único T-G invariante com parâmetros (r, a, b) satisfazendo $f(C) = rx_0$ e $f(L) = ry_0$, e é dado pela expressão acima.

CAPÍTULO 3

MATRIZES

Este breve capítulo será dedicado a estabelecer alguns fundamentos da teoria de matrizes sobre domínios de ideais principais, e em seguida apresentar a relação entre matrizes, grafos e matróides.

De fato, podemos olhar para um grafo, para a matróide gráfica associada, ou para a matriz de incidência do grafo. Muitas propriedades podem ser observadas em todos os três pontos de vista. Ocorre que certas argumentações podem ser mais fáceis, a depender da abordagem.

No final deste capítulo, vamos apresentar a demonstração de um resultado clássico acerca da dualidade entre fluxos e tensões (ou colorações) como aplicação dos resultados do capítulo.

3.1 ALGUMA ÁLGEBRA LINEAR

Esta seção pode ser evitada por um leitor familiarizado com as noções de fatores invariantes e dualidade em matrizes sobre anéis.

3.1.1 Forma Normal de Smith

Seja R um domínio de ideais principais (DIP). Denotaremos por R^* o conjunto dos elementos invertíveis de R . Seja $M \in \mathcal{M}_{m \times n}(R)$. Definimos o *espaço de linhas* e o *espaço nulo (de colunas)* respectivamente por:

$$\rho(M) = \{yM : y \in R^m\}$$

$$\nu(M) = \{x \in R^n : Mx^T = 0\}$$

Lembramos que as operações elementares em uma matriz são:

- (i) Multiplicação de linha ou coluna por elemento invertível do anel.
- (ii) Troca de posição entre duas linhas ou duas colunas.
- (iii) Somar a uma linha (coluna) um múltiplo de outra linha (coluna).

São fatos notórios que:

Realizar um conjunto de tais operações em A é o mesmo que fazer $P \cdot A \cdot Q$, onde $P \in \mathcal{M}_{m \times m}(R)$ e $Q \in \mathcal{M}_{n \times n}(R)$ são certas matrizes invertíveis.

Da mesma forma, qualquer matriz do tipo $P \cdot A \cdot Q$, P e Q invertíveis, pode ser obtida a partir de A por meio de tais operações.

Estas operações não alteram o posto de uma matriz, e mais, qualquer matriz B obtida de uma matriz A por meio de tais operações é dita *equivalente* a A , e denotamos este fato por $A \approx B$. Ou seja:

$$A \approx B \Leftrightarrow \text{Existem } P \text{ e } Q \text{ invertíveis tais que } PAQ = B$$

Uma matriz é invertível se, e somente se, o seu determinante é um invertível do anel.

A demonstração destes fatos acima pode ser encontrada em qualquer bom texto de álgebra linear, mas sugerimos Eves [Eve66].

Lema. Se $A \approx B$, então $\rho(A) \simeq \rho(B)$.

Demonstração. De fato, note que:

$$\{x \cdot P \cdot A \cdot Q : x \in R^m\} = \{y \cdot A \cdot Q : y \in R^m\}$$

Basta que $x = yP^{-1}$. Agora:

$$\{y \cdot A \cdot Q : y \in R^m\} \rightarrow \{y \cdot A : y \in R^m\}$$

onde $y \cdot A \cdot Q \mapsto (y \cdot A \cdot Q)Q^{-1}$ é um isomorfismo natural de submódulos de R^n , porque em particular o é no próprio R^n . ■

Teorema 3.1 (Forma Normal de Smith). Por meio de operações elementares em linhas e colunas, qualquer matriz M pode ser transformada em uma matriz composta por zeros a menos de sua diagonal, onde aparecem os elementos d_1, \dots, d_r tais que d_i divide d_{i+1} . Estes elementos são denominados *fatores invariantes* e são únicos a menos de multiplicação por invertíveis. Convencionando que 0 é fator invariante de multiplicidade $n - r$, então considerando os n fatores invariantes d_1, \dots, d_n , teremos a relação entre os R -módulos:

$$R^n / \rho(M) \simeq \bigoplus_{i=1}^n R/d_i R$$

Demonstração. Vamos mostrar a primeira parte por indução. Se o posto é 0, não há nada a mostrar. Suponha portanto que o resultado é válido para todas as matrizes de posto $r - 1$, e seja $M = ((a_{ij}))$ matriz qualquer de posto r , com m linhas e n colunas.

Suponha sem perda de generalidade que $a_{11} \neq 0$, caso contrário, façamos operações do tipo (ii) para que seja.

Se a_{11} divide a_{12} , use operações do tipo (iii) para zerar a posição de a_{12}

Caso contrário, seja d o gerador do ideal gerado por eles. Então existem σ e τ tais que:

$$a_{11}\sigma + a_{12}\tau = d$$

Se $a_{1i} = d\alpha_i$, $i = 1, 2$, teremos $a_{12}\alpha_1 - a_{11}\alpha_2 = 0$. Observe então que:

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots \\ \vdots & & \ddots & \end{pmatrix} \begin{pmatrix} \sigma & -\alpha_2 & 0 & 0 & \dots \\ \tau & \alpha_1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & & 1 \\ \vdots & & & & \ddots \end{pmatrix} = \begin{pmatrix} d & 0 & a_{13} & \dots \\ \vdots & & \ddots & \end{pmatrix}$$

Note também que $\alpha_1\sigma + \alpha_2\tau = 1$, portanto o determinante da matriz usada para multiplicar M é 1, logo é uma matriz invertível, daí obtida por meio de operações elementares.

Repetimos o processo acima para os outros elementos da primeira linha, até que só tenhamos o primeiro elemento não nulo. Digamos, e_1 . Note que e_1 é gerador do ideal gerado pelos elementos originais da primeira linha. Seja M_1 a matriz obtida. Observe que M_1 é da forma:

$$M_1 = \left(\begin{array}{c|ccc} e_1 & 0 & \dots & 0 \\ * & & & \\ \vdots & & A_1 & \\ * & & & \end{array} \right) \approx M$$

Seja agora e_2 o gerador do ideal gerado pelos elementos da primeira coluna de M_1 . Repetimos o processo, obtendo uma matriz M_2 como abaixo:

$$M_2 = \left(\begin{array}{c|ccc} e_2 & * & \dots & * \\ 0 & & & \\ \vdots & & A_2 & \\ 0 & & & \end{array} \right) \approx M$$

Iterando este procedimento, vamos gerar uma sequência de e_i s satisfazendo

$$(e_1) \subset (e_2) \subset (e_3) \subset \dots$$

Mas esta sequência estabiliza, uma vez que:

$$\bigcup_{i \geq 0} (e_i) \text{ é um ideal, logo } = (b)$$

pois estamos em um DIP. Mas então é óbvio que $(b) = (e_s)$ para algum s , implicando que:

$$(e_1) \subset (e_2) \subset (e_3) \subset \dots \subset (e_s) = (e_{s+1}) = \dots$$

Consideramos então a matriz (supondo sem perda de generalidade s ímpar):

$$M_s = \left(\begin{array}{c|ccc} e_s & 0 & \dots & 0 \\ z_2 & & & \\ \vdots & & & \\ z_m & & & \end{array} \begin{array}{c} \\ \\ A_s \\ \end{array} \right) \approx M$$

Mas vimos que e_s divide todos os elementos z_i s, daí por meio de operações elementares do tipo (iii), obtemos a matriz:

$$M' = \left(\begin{array}{c|ccc} e_s & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & & \\ 0 & & & \end{array} \begin{array}{c} \\ A \\ \end{array} \right) \approx M$$

Agora observe que a matriz A tem posto $r - 1$. Em A , aplicamos a hipótese indutiva, obtendo a matriz:

$$M'' = \left(\begin{array}{c|cccc} e_s & 0 & \dots & & 0 \\ 0 & g_2 & & & \\ & & \ddots & & \\ \vdots & & & g_{r-1} & \\ 0 & & & & 0 \\ & & & & & \ddots \end{array} \right) \approx M$$

Ainda não acabou, pois não sabemos se $e_s | g_2$. Seja d gerador do ideal gerado por e_s e g_2 e seja $e_s = \epsilon d$. Então (olhando somente para as duas primeiras linhas e colunas), teremos:

$$\begin{pmatrix} e_s & 0 \\ 0 & g_2 \end{pmatrix} \approx \begin{pmatrix} e_s & 0 \\ d & g_2 \end{pmatrix} \approx \begin{pmatrix} 0 & g_2(-\epsilon) \\ d & 0 \end{pmatrix} \approx \begin{pmatrix} d & 0 \\ 0 & g_2(-\epsilon) \end{pmatrix}$$

Fazemos então $d_1 = d$. Se $g_2(\epsilon) | g_3$, acabou - fazemos $d_2 = g_2(\epsilon)$ e $d_i = g_i$ com $i \geq 3$. Caso contrário, repetimos o processo acima, definindo por d_2 o gerador do ideal gerado por $g_2(\epsilon)$ e g_3 . Assim por diante, e teremos finalmente:

$$M''' = \left(\begin{array}{cccc} d_1 & 0 & \dots & 0 \\ 0 & d_2 & & \\ & & \ddots & \\ \vdots & & & d_r \\ & & & & 0 \\ 0 & & & & & \ddots \end{array} \right) \approx M$$

Para ver a unicidade, suponha agora que $A \approx B$. Seja M_j o ideal gerado pelos menores $j \times j$ de uma matriz M . Seja a_j o gerador de A_j e b_j o de B_j . Lembramos que o

determinante é uma função n -linear em linhas ou colunas, logo $A_j \subset B_j$ e vice versa, implicando $a_j = u \cdot b_j$, $u \in R^*$. Olhando então para A e uma matriz na forma de Smith que seja equivalente a A , digamos S , onde s_j é o gerador de S_j , sendo d_1, \dots, d_r os fatores invariantes de S , então:

$$\frac{a_j}{a_{j-1}} = \frac{u \cdot s_j}{v \cdot s_{j-1}} = u' \cdot d_j$$

isto para qualquer S na forma de Smith e equivalente a A . Concluimos a demonstração da unicidade. Para uma matriz M , nos referiremos à sua Forma Normal de Smith por $\text{FNS}(M)$.

Por fim, considere o homomorfismo:

$$R^n \rightarrow R/(d_1) \oplus \dots \oplus R/(d_n)$$

tal que $(r_1, \dots, r_n) \rightarrow (r_1 + (d_1), \dots, r_n + (d_n))$. O núcleo deste homomorfismo serão justamente os (r_1, \dots, r_n) tais que $r_i \in (d_i)$, mas isto nada mais é do que o conjunto $\{y \cdot \text{FNS}(M) : y \in R^m\} = \rho(\text{FNS}(M)) \simeq \rho(M)$. Finalmente:

$$R^n / \rho(\text{FNS}(M)) \simeq R^n / \rho(M) \simeq R/(d_1) \oplus \dots \oplus R/(d_n)$$

■

Se por acaso $R = \mathbb{Z}$, escolheremos os fatores invariantes para serem não negativos. Se $R = \mathbb{R}$, então tomaremos somente 0 e 1 como fatores invariantes.

A forma normal de Smith terá um papel fundamental para relacionar as definições abaixo.

3.1.2 Dualidade de matrizes

Definição 3.1. Duas matrizes M e M^* são duais se o espaço de linhas de uma delas for igual ao espaço nulo da outra, e vice-versa.

Definição 3.2. Uma matriz é *totalmente unimodular* se todo subdeterminante for 0 ou um invertível do anel.

Dois comentários acerca das definições acima. Nem toda matriz possui uma dual, e ser totalmente unimodular não é uma característica invariante por operações elementares. O teorema a seguir esclarecerá estes fatos.

Lema. Seja M matriz sobre R . (1) Então $\rho(M)^\perp = \nu(M)$, onde \perp indica o espaço ortogonal com respeito ao produto interno usual. (2) Uma matriz M possui uma dual se, e somente se, $\rho(M)^{\perp\perp} = \rho(M)$.

Demonstração. Para (1), se $\langle x, yM \rangle = 0$ para todo $y \in R^m$, então em particular vale para

$$e_i = (0, 0, \dots, 0, 1, 0, \dots, 0) \text{ o } 1 \text{ na } i\text{-ésima posição, para todo } i$$

Isso diz que x é ortogonal a todas as linhas de M , mas então $M \cdot x^T = 0$, concluindo que $\rho(M)^\perp \subset \nu(M)$. Por outro lado, se x é ortogonal a todas as linhas de $M = ((a_{ij}))$, com $y = (y_1, \dots, y_m)$, então aplicamos a linearidade do produto interno para obtermos:

$$\langle x, yM \rangle = \sum_{i=1}^m y_i \langle x, (a_{i1}, \dots, a_{in}) \rangle = 0$$

concluindo que $x \in \rho(M)^\perp$, logo $\nu(M) \subset \rho(M)^\perp$, e temos (1). Para a volta de (2), observe que sempre podemos tomar uma matriz cujo espaço de linhas seja um dado espaço qualquer, no caso M^* tal que $\rho(M^*) = \rho(M)^\perp = \nu(M)$. Daí:

$$\rho(M)^{\perp\perp} = \rho(M) \Rightarrow \nu(M)^\perp = \rho(M) \Rightarrow \rho(M^*)^\perp = \rho(M) \Rightarrow \nu(M^*) = \rho(M)$$

Para a ida; se M possui uma dual, digamos M^* , então:

$$\rho(M^*) = \nu(M) \quad \text{e} \quad \nu(M^*) = \rho(M)$$

Mas então:

$$\rho(M)^{\perp\perp} = \nu(M)^\perp = \rho(M^*)^\perp = \nu(M^*) = \rho(M) \quad \blacksquare$$

Lema 3.1. Se M e M^* são duais, então podemos efetuar operações nas linhas de ambas sem que este fato se altere. E mais, podemos conservar a dualidade ao efetuarmos operações nas colunas de uma, desde que façamos as operações duais na outra.

Por operações duais, queremos dizer que: (1) ao somarmos α vezes a i -ésima coluna na j -ésima coluna de M , deveremos somar $-\alpha$ vezes a j -ésima coluna na i -ésima coluna de M^* (2) só podemos multiplicar colunas por elemento invertível, e ao multiplicarmos a i -ésima coluna de M por α , deveremos multiplicar a j -ésima coluna de M^* por α^{-1} (3) se trocarmos duas colunas de lugar em M , deveremos trocar as mesmas duas colunas em M^* .

Demonstração. De fato, as operações nas linhas não alteram nem o espaço de linhas nem o espaço nulo. Já as operações duais em colunas não alteram a ortogonalidade das linhas de M e M^* , pelo lema acima, isso conserva a dualidade. \blacksquare

Teorema 3.2. Seja M uma matriz sobre R , domínio de ideais principais. Então as seguintes condições são equivalentes:

- (1) M possui uma matriz dual.
- (2) Os fatores invariantes de M são 0 ou invertíveis do anel.
- (3) M é equivalente a uma matriz totalmente unimodular.

Demonstração. (1) \Leftrightarrow (2) Pelas operações elementares, coloquemos M na Forma Normal de Smith. Suponhamos r fatores invariantes não nulos. Observe então que $\rho(M)^{\perp\perp}$ é exatamente o conjunto de todos os vetores cujas primeiras r coordenadas são arbitrárias, e as demais são nulas. Mas então $\rho(M)^{\perp\perp} = \rho(M)$ se, e somente se, os r fatores invariantes são invertíveis do anel.

(2) \Rightarrow (3) Basta considerar a Forma Normal de Smith de M .

(3) \Rightarrow (2) Pelo que vimos, os fatores invariantes d_i de uma matriz M são justamente $d_i = f_i/f_{i-1}$, onde os f_i são os geradores do ideal gerado pelos menores $i \times i$ da matriz. Se a matriz é totalmente unimodular, então os fatores invariantes não nulos serão invertíveis do anel. ■

Corolário 3.2.1. Dada uma matriz qualquer M , se M' é uma matriz cujo espaço nulo seja o espaço de linhas de M , e M'' é uma matriz cujo espaço nulo seja o espaço de linhas de M' , então M' e M'' são matrizes duais.

3.2 APLICAÇÃO À COMBINATÓRIA

Nesta seção, vamos usar as ferramentas da seção anterior para estabelecermos relações importantes entre matrizes, grafos e matróides.

3.2.1 Matrizes e grafos

Seja $X = (V, E)$ um grafo dirigido. Seja C a família dos ciclos (orientados) de X . Introduzimos duas definições.

Definição 3.3. A *matriz de incidência vértice-aresta com sinal* é uma matriz cujas linhas são indexadas pelos vértices de X e as colunas pelas arestas. Uma entrada da matriz é -1 se o vértice for inicial da aresta, 1 se o vértice for final, e 0 caso não haja incidência. Denotaremos essa matriz por M_E^V .

Definição 3.4. A *matriz de incidência ciclo-aresta com sinal* é uma matriz cujas linhas são indexadas pelos ciclos, com orientação, de X , e as colunas pelas arestas. Uma entrada da matriz é -1 se os sentidos da aresta e do ciclo forem diferentes, 1 se forem iguais, e 0 se a aresta não pertencer ao ciclo. Denotaremos essa matriz por M_E^C .

Teorema 3.3. Dado $X = (V, E)$ grafo dirigido, C família de ciclos, então M_E^V é totalmente unimodular. E mais:

$$M_E^V \text{ e } M_E^C \text{ formam um par dual.}$$

Demonstração. Começaremos mostrando que M_E^V é totalmente unimodular por indução. Se só existe um vértice, o resultado segue. Agora suponhamos que ele seja válido para todas as matrizes quadradas de ordem $n-1$. Considere então um grafo X com n vértices ou mais. Tomamos uma submatriz quadrada de ordem n . Se alguma coluna é toda nula, então o determinante é 0 . Se alguma coluna possui apenas um elemento, ele é 1 ou -1 , e o determinante será \pm o determinante de uma matriz de ordem $n-1$, e o resultado segue. Se, por fim, todas as colunas tem dois elementos, então somamos todas elas a alguma coluna fixada, e teremos então uma coluna nula, resultando num determinante igual a 0 . Logo M_E^V é totalmente unimodular para qualquer grafo.

Sabemos então que M_E^V possui um dual. Vamos mostrar que $\rho(M_E^C) = \nu(M_E^V)$. Isto acabará sendo suficiente. Seja inicialmente:

$$x = y \cdot M_E^C \in \rho(M_E^C)$$

Vamos ver que $M_E^V \cdot x^T = 0$, o que é equivalente a mostrar que:

$$\langle x, \mathbf{v} \rangle = 0$$

para cada \mathbf{v} fixado, onde \mathbf{v} representa o vetor linha da matriz M_E^V referente ao vértice v . Consideremos então \mathcal{C} a família de todos os ciclos do grafo X que passam pelo vértice v . Seja $x(e)$ a coordenada de x referente à coluna da aresta e e $y(C)$ a coordenada do vetor y referente ao ciclo C . Sejam e_v e e_C as coordenadas em M_E^V e M_E^C referentes à aresta e e respectivamente aos vértice v e ciclo C . Observe então que:

$$\langle x, \mathbf{v} \rangle = \sum_{e \in E} x(e) \cdot e_v$$

Daí

$$\langle x, \mathbf{v} \rangle = \sum_{e \in E} \left(\sum_{C \in \mathcal{C}} y(C) \cdot e_C \right) e_v$$

Ou simplesmente:

$$\langle x, \mathbf{v} \rangle = \sum_{e \in E} \sum_{C \in \mathcal{C}} y(C) \cdot e_C \cdot e_v = \sum_{\substack{e \in E \\ C \in \mathcal{C}}} y(C) \cdot e_C \cdot e_v$$

Neste grande somatório, cada termo $y(C)$ aparecerá exatamente duas vezes, uma para cada aresta contida em C e incidente a v , digamos e e f . Mas se $e_C = f_C = 1$ ou $e_C = f_C = -1$, então ambas estão no mesmo sentido, logo $e_v = -f_v$, pois uma terá v como final e a outra como inicial. Da mesma forma, se $e_C = -f_C$, então elas estão em sentido opostos, e $e_v = f_v$. Em qualquer caso, $y(C)$ aparecerá com sinais opostos. Concluimos então que:

$$\langle x, \mathbf{v} \rangle = 0 \text{ para todo } \mathbf{v} \quad \Rightarrow \quad M_E^V \cdot x^T = 0$$

Agora suponha $M_E^V \cdot x^T = 0$. Observe que x é um fluxo¹ em X (possivelmente nulo em algumas arestas). Vamos mostrar que este fluxo pode ser decomposto em uma soma de funções que são localmente tensões² em cada ciclo. Ou seja, elementos de $\rho(M_E^C)$. Faremos por indução.

Primeiro: se o grafo só possui um ciclo, então cada fluxo possível no grafo é uma tensão neste ciclo, nulo nas demais arestas. Suponha que o resultado é válido para todo grafo com m ciclos ou menos. Seja um grafo com $m + 1$ ciclos, φ fluxo dele. Nosso

¹Definido no grupo abeliano identificado com o anel em qual está definida M_E^V .

²Mesma observação feita acima.

objetivo é mostrar que existem funções $f_1, \dots, f_{m+1} : E \rightarrow R$ tais que f_i é tensão do ciclo C_i e constante nula nas demais arestas, de modo que:

$$\varphi = \sum_{i=1}^{m+1} f_i$$

Consideramos então $e \in E$ incidente a um ciclo C_k . Definamos f_k de modo que $f_k(f) = \varphi(e)$ para todo $f \in C_k$. Afirmamos que $\varphi - f_k$ é ainda um fluxo. Com efeito, todo vértice do ciclo perdeu e ganhou um fluxo de $\varphi(e)$, e nada aconteceu aos demais. Removemos portanto todas as arestas do ciclo C_k . Nosso novo grafo terá então m ou menos ciclos, e portanto vale a hipótese indutiva. Se forem m , digamos que sejam $f_1, \dots, f_{k-1}, f_{k+1}, \dots, f_m$, e o resultado segue ao adicionarmos f_k . Se forem menos que m , então definimos $f_l \equiv 0$ para todo ciclo C_l que tenha sido destruído acidentalmente ao removermos as arestas de C_k , e repetimos o argumento para o caso de m ciclos, encerrando.

Concluimos então que $\rho(M_E^C) = \nu(M_E^V)$. Para mostrarmos que $\rho(M_E^V) = \nu(M_E^C)$, basta utilizarmos o fato que M_E^V tem dual, ou seja $\rho(M_E^V)^{\perp\perp} = \rho(M_E^V)$. Observe:

$$\rho(M_E^V) = \rho(M_E^V)^{\perp\perp} = \nu(M_E^V)^{\perp} = \rho(M_E^C)^{\perp} = \nu(M_E^C)$$

concluindo a demonstração. ■

3.2.2 Matrizes e matróides

O teorema a seguir associa dualidade em matrizes e em matróides da maneira esperada. Lembre-se que, dada uma matriz A sobre um domínio de ideais principais R , podemos indexar as colunas da matriz, e os conjuntos de colunas dessa matriz que são linearmente independentes induzem os conjuntos independentes de uma matróide sobre os índices das colunas. Dizemos que é uma matróide *representável* sobre o corpo de frações de R , a ser denotado por \mathbb{F} , e denotaremos a matróide associada à matriz A por $\mathcal{M}(A)$.

Teorema 3.4. Sejam A, A^* matrizes duais sobre R , um domínio de ideais principais. Então $\mathcal{M}(A)^*$ (dual da matróide $\mathcal{M}(A)$) é igual a $\mathcal{M}(A^*)$.

Lema 3.2. (1) Se A e B são equivalentes por meio de operações elementares em linhas, então $\mathcal{M}(A) = \mathcal{M}(B)$. Se for possível trocar duas colunas de posição, então convençionalmente que o rótulo da coluna move-se com ela, e continuamos com $\mathcal{M}(A) = \mathcal{M}(B)$. (2) E mais, $\mathcal{M}(A) = \mathcal{M}(X)$, onde X é uma matriz equivalente a A por meio de operações elementares em linhas e troca de colunas, e é do tipo:

$$X = \left(\begin{array}{c|c} I_r & D \end{array} \right) = [I_r | D]$$

onde r é o posto da matróide, I_r a identidade de ordem r , e D uma matriz de tamanho $r \times (n - r)$, onde n é o número de elementos da matróide.

Observe que a volta do ítem (1) em geral é falsa, mas vale para certos casos particulares, o que veremos no final desta seção.

Demonstração. Para (1), notamos que operações elementares de linha não alteram as relações de dependência entre as colunas. Para (2), basta observar que as operações de linha mais a troca de colunas pode deixar qualquer matriz neste formato, com possivelmente algumas linhas nulas abaixo. Mas remoção de linhas nulas não altera a matrôide definida nas colunas (desde que não se trate da única linha, e neste caso $I_r = I_0$ e D é a linha nula). ■

Lema 3.3. Temos que $\mathcal{M}([I_r|D])^* = \mathcal{M}([-D^T|I_{n-r}])$.

A demonstração do resultado é incluída por completude, mas encontra-se em Oxley [Oxl92].

Demonstração. Seja $M = \mathcal{M}([I_r|D])$. Seja $E = \{e_1, \dots, e_r, e_{r+1}, \dots, e_n\}$ o conjunto de índices sobre o qual M está definida. Seja B base de M . Vamos mostrar inicialmente que $E - B$ é base para $\mathcal{M}([-D^T|I_{n-r}])$. Note que rearranjar linhas e colunas de $[I_r|D]$ provoca somente o efeito de rearranjar colunas e linhas em $[-D^T|I_{n-r}]$. Portanto, sem perda de generalidade, assumimos que $B = \{e_{r-t+1}, e_{r-t+2}, \dots, e_r, e_{r+1}, \dots, e_{2r-t}\}$. Escrevemos então:

$$[I_r|D] = \left(\begin{array}{c|c|c|c} e_1 \dots e_{r-t} & e_{r-t+1} \dots e_r & e_{r+1} \dots e_{2r-t} & e_{2r-t+1} \dots e_n \\ \hline I_{r-1} & 0 & D_1 & D_2 \\ \hline 0 & I_t & D_3 & D_4 \end{array} \right)$$

A matriz:

$$\left(\begin{array}{c|c} 0 & D_1 \\ \hline I_t & D_3 \end{array} \right)$$

tem posto r pois B é base. Logo D_1 , e então $-D_1^T$, têm posto $r - t$. A partição de $[I_r|D]$ induz a partição a seguir:

$$[-D^T|I_{n-r}] = \left(\begin{array}{c|c|c|c} e_1 \dots e_{r-t} & e_{r-t+1} \dots e_r & e_{r+1} \dots e_{2r-t} & e_{2r-t+1} \dots e_n \\ \hline -D_1^T & -D_3^T & I_{r-t} & 0 \\ \hline -D_2^T & -D_4^T & 0 & I_{n-(2r-t)} \end{array} \right)$$

Onde a submatriz correspondente a $E - B$ é:

$$\left(\begin{array}{c|c} -D_1^T & 0 \\ \hline -D_2^T & I_{n-(2r-t)} \end{array} \right)$$

Cujo posto é exatamente a soma dos postos de $I_{n-(2r-t)}$ e $-D_1^T$, ou seja:

$$n - (2r - t) + (r - t) = n - r$$

Logo $E - B$ é base de $\mathcal{M}([-D^T, I_{n-r}])$. É fácil ver que toda base é obtida desta forma, concluindo que de fato $\mathcal{M}([-D^T, I_{n-r}]) = M^*$. \blacksquare

Lema 3.4. Temos que $[-D^T|I_{n-r}]$ é uma dual para $[I_r|D]$.

Demonstração. Lembramos que estamos trabalhando sobre \mathbb{F} , ou seja, todas as matrizes possuem dual pois os fatores invariantes de todas as matrizes são invertíveis. Seja $y = (y_1, \dots, y_r)$. Seja $D = [d_1|d_2|\dots|d_{n-r}]$. Então

$$y[I_r|D] = (y_1, \dots, y_r, (y \cdot d_1), \dots, (y \cdot d_{n-r}))$$

Agora:

$$\begin{aligned} & [-D^T|I_{n-r}] \cdot (y_1, \dots, y_r, (y \cdot d_1), \dots, (y \cdot d_{n-r}))^T = \\ & = ((-d_1 \cdot y) + (y \cdot d_1), (-d_2 \cdot y) + (y \cdot d_2), \dots, (-d_{n-r} \cdot y) + (y \cdot d_{n-r})) = 0 \end{aligned}$$

Isto mostra que $\rho([I_r|D]) \subset \nu([-D^T|I_{n-r}])$. Equivalentemente, se

$$[-D^T|I_{n-r}] \cdot x^T = 0 \quad \text{onde } x = (x_1, \dots, x_n),$$

então

$$(-d_i \cdot (x_1, \dots, x_r)) + x_{r+i} = 0 \Rightarrow x_{r+i} = (d_i \cdot (x_1, \dots, x_r)) \quad \forall i$$

Ou seja,

$$(x_1, \dots, x_n) = (x_1, \dots, x_r)[I_r|D]$$

Temos então que $\rho([I_r|D]) = \nu([-D^T|I_{n-r}])$. Por um argumento que já vimos anteriormente, ao sabermos que estas matrizes já possuem duais, teremos que:

$$\rho([-D^T|I_{n-r}]) = \rho([-D^T|I_{n-r}])^{\perp\perp} = \nu([-D^T|I_{n-r}])^{\perp} = \rho([I_r|D])^{\perp} = \nu([I_r|D]) \quad \blacksquare$$

Demonstração do teorema. Consideramos os lemas acima. Começamos então com o par dual A e A^* . Observe que:

$$\mathcal{M}(A)^* = \mathcal{M}([I_r|D])^* = \mathcal{M}([-D^T|I_{n-r}])$$

Queremos mostrar que $\mathcal{M}([-D^T|I_{n-r}]) = \mathcal{M}(A^*)$, e para isso, é suficiente ver que $A^* \approx [-D^T|I_{n-r}]$.

Consideramos agora o lema 3.1, que diz que se tínhamos um par dual (A, A^*) e efetuamos operações elementares nas linhas e trocamos colunas de A para obtermos, digamos, J , igual a $[I_r|D]$ a menos de remoção de linhas nulas, então as mesmas operações levaram A^* a uma B , digamos, de modo que (J, B) é um par dual. Agora:

$$\mathcal{M}(A^*) = \mathcal{M}(B) \text{ pois } A^* \approx B$$

Considere então J' igual a $[-D^T|I_{n-r}]$. Observe trivialmente que J' é dual de J . Resta mostrar que as duas matrizes B e J' , que são duais da matriz J , são equivalentes por operações elementares de linhas e troca de colunas. Primeiro notemos que B e J' tem mesmo posto $n - r$. Seja B com dimensão $m \times n$. É claro que $m \geq n - r$.

Por operações elementares nas linhas de B , zeremos $m - (n - r)$ linhas e as removamos.

Organizemos as colunas de B de modo que $B = [B'|B_{n-r}]$, onde B' tem dimensão $(n - r) \times r$ e B_{n-r} tem dimensão $(n - r) \times (n - r)$, mas de modo que B_{n-r} tenha posto $n - r$, logo seja invertível.

Por um abuso de notação, continuamos chamando de B a matriz oriunda das operações acima. Seja $t = n - r$. Agora, sabemos que $\rho(B) = \rho(J')$. Seja $\{e_1, \dots, e_t\}$ a base canônica do \mathbb{F}^t . Considere a família de vetores:

$$e_1B, \dots, e_tB$$

São exatamente as linhas de B . Eles pertencem a $\rho(J')$. O que sabemos a respeito da matriz J' é que, se $v \in \mathbb{F}^t$, então vJ' possui n coordenadas, as últimas t são exatamente uma cópia v . Sejam b_1, \dots, b_t as linhas de B_t . Temos então que:

$$(e_1B, \dots, e_tB) = (b_1J', \dots, b_tJ')$$

Portanto:

$$B = B_{n-r} \cdot J'$$

mas a multiplicação a esquerda por uma matriz invertível são operações elementares em linhas, o que conclui a demonstração. ■

3.2.3 Matrizes, grafos e matróides

Seja $X = (V, E)$ multi-grafo não dirigido. Introduzimos uma orientação completamente arbitrária em X . O último resultado desta seção associa a matróide definida na matriz M_E^V , $\mathcal{M}(M_E^V)$, com a matróide gráfica associada ao grafo X , $M(X)$. Note em particular que no caso de um multigrafo-dirigido, se e é um laço no vértice v , a entrada na matriz M_E^V correspondente a e e a v é definida como sendo 0.

Teorema 3.5. Temos simplesmente que:

$$M(X) = \mathcal{M}(M_E^V)$$

para qualquer orientação escolhida para X .

Demonstração. Mostraremos que os circuitos das matróides são exatamente os mesmos. Considere um circuito em $M(X)$, ou seja, um ciclo C no grafo X , digamos determinado pelas arestas $\{e_1, \dots, e_k\}$. Sejam $\{c_1, \dots, c_k\}$ as colunas associadas a estas arestas na matriz M_E^V . Seja $a_i = 1$ se e_i está no sentido de C , $a_i = -1$ caso contrário. Então:

$$\sum_{i=1}^k a_i c_i = 0$$

Logo $\{c_1, \dots, c_k\}$ indexam vetores linearmente dependentes, portanto este é um conjunto dependente na matróide.

Agora seja $\{c_1, \dots, c_k\}$ um circuito em $\mathcal{M}(M_E^V)$. Temos então que:

$$\sum_{i=1}^k a_i c_i = 0$$

para a_i s todos não nulos (é um dependente minimal). Portanto se alguma entrada de um c_i é não nula, existe pelo menos um outro c_j tal que a entrada na mesma posição é não nula. No subgrafo induzido pelas arestas associadas $\{e_1, \dots, e_k\}$, portanto, todo vértice terá grau pelo menos 2, donde garantimos a existência de pelo menos um ciclo. Logo o conjunto de arestas $\{e_1, \dots, e_k\}$ é um dependente em $M(X)$.

Temos portanto duas matróides em que todo circuito de uma é dependente na outra. Em geral, quando isto ocorre, temos que elas são a mesma matróide. Com efeito, suponha que C , circuito de M , é igual a D' , dependente de M' . Seja $C' \subset D'$ igual a D , dependente de M . Então:

$$C = D' \supseteq C' = D$$

Logo só pode valer a igualdade, pois um dependente contido num circuito é o próprio circuito. Mas então os circuitos das matróides são os mesmos, implicando a igualdade entre as matróides. ■

Fluxos e tensões - dualidade Neste momento, os fluxos e tensões considerados poderão ser nulos nas arestas.

Todas as observações feitas até agora nos permitirão deduzir, a título de aplicação, uma bela consequência acerca da estrutura de um grafo planar e seu dual. Ao longo das argumentações abaixo, até o final desta seção, vamos supor que o anel R é o corpo $\mathbb{Z}_3 = \{0, 1, -1\}$. Certamente, não haverá qualquer prejuízo na conclusão, e os resultados anteriores permanecem, já que todo corpo é um domínio de ideais principais.

O lema a seguir é a essência do que iremos mostrar. Ele será re-utilizado no capítulo 5.

Lema 3.5. Um A -fluxo é exatamente uma escolha em A para cada elemento de uma base fixada em $\nu(M_E^V)$. Uma A -tensão é uma escolha em A para cada elemento em uma base fixada em $\nu(M_E^C)$.

Observe que existe uma operação natural entre um elemento de um grupo abeliano A e um elemento de $\mathbb{Z}_3 = \{0, 1, -1\}$, com resultado no grupo em questão. É exatamente:

$$o : \mathbb{Z}_3 \times A \rightarrow A$$

tal que $o(1, a) = a$, $o(-1, a) = a^{-1}$ e $o(0, a) = e$.

Demonstração. Consideramos uma base de $\nu(M_E^V)$, e operamos cada elemento da base com um elemento em A . É óbvio que a “soma” em A dos novos vetores ainda será um A -fluxo. E mais, todo fluxo poderá ser escrito, e de maneira única.

Mostraremos brevemente por indução, porque essencialmente é uma repetição de um argumento já utilizado. Se só há um vetor na base, só haverá um ciclo no grafo, e portanto todo fluxo no grafo será uma escolha de um valor para este ciclo (que pode mudar de sinal a cada aresta a depender da orientação delas). Se existem m vetores na base, fixamos um vetor e uma entrada deste vetor referente a uma aresta, e operamos este vetor com os outros da base de modo que este passe a ser o único vetor que tenha esta entrada não nula. Estabelecemos que este vetor está associado ao valor do fluxo nesta aresta, e pensaremos no fluxo ao longo do ciclo (com sinal) induzido pelo vetor como sendo constante igual ao valor na aresta. Então removemos as arestas incidentes somente a este vetor, e subtraímos do fluxo das outras arestas do grafo o fluxo no ciclo associado ao vetor removido. Aplicamos a hipótese indutiva e voltamos ao grafo original, concluindo a argumentação.

Para ver a segunda parte do lema, vamos considerar a identificação natural entre tensões e colorações. Uma base de $\nu(M_E^C)$ é uma base de $\rho(M_E^V)$. Os vetores de $\rho(M_E^V)$ tem uma entrada para cada aresta, e cada entrada é o gradiente de uma \mathbb{Z}_3 -coloração (0, 1 ou -1) nos vértices incidentes à aresta. Se só existe um vetor na base, então toda coloração gerará essencialmente uma única tensão (em \mathbb{Z}_3), daí poderemos escolher um valor em A para esta tensão. Como toda tensão é oriunda de uma coloração, temos o caso base. Suponha agora m vetores na base e m \mathbb{Z}_3 -colorações que geram estes vetores. Escolhemos uma, c , e façamos com que possua um vértice colorido somente por ela. Removemos os vértices coloridos somente por esta, gerando o grafo $X \setminus c$. Aplicamos a hipótese indutiva. Voltando a X , seja uma A -tensão qualquer. Será a soma de uma A -tensão em $X \setminus c$ e uma em X que obedeça às cores de c . Mas temos $|A|$ possibilidades para esta última, pois certamente existe uma aresta em X que não está em $X \setminus c$. ■

Corolário 3.5.1. O número de A -fluxos é $|A|^{\dim \nu(M_E^V)}$. O número de A -tensões é $|A|^{\dim \nu(M_E^C)}$.

Infelizmente, omitiremos a demonstração do lema a seguir, crucial para a argumentação, pois depende de certa teoria acerca da representabilidade de matróides, o que foge ao objetivo deste texto. Sugerimos Oxley [Oxl92] para a demonstração deste resultado.

Lema. Sejam A e B matrizes sobre \mathbb{Z}_3 . Se $\mathcal{M}(A) = \mathcal{M}(B)$, então A e B são equivalentes por meio de operações elementares em linhas e troca de colunas.

Teremos então este resultado.

Teorema 3.6. Fixado um grupo abeliano A , existe uma identificação natural biunívoca entre os A -fluxos em um grafo planar e as A -tensões no dual, e vice versa.³

Demonstração. Sejam agora $X = (V, E)$ e $X^* = (V^*, E^*)$ grafos duais (há uma identificação canônica entre os elementos de E e E^*). Sejam $M(X)$ e $M(X^*)$ as matróides

³Obviamente não é preciso fazer toda esta teoria para mostrar este resultado. Mas já que o Corolário 3.5.1 nos será útil futuramente, achamos que seria interessante mostrar esta aplicação.

gráficas associadas. Temos que:

$$\mathcal{M}(M_{E^*}^{V^*}) = M(X^*) = M(X)^* = \mathcal{M}(M_E^V)^* = \mathcal{M}((M_E^V)^*)$$

Se as matrôides são iguais, e como as matrizes $M_{E^*}^{V^*}$ e $(M_E^V)^*$ tem entradas em \mathbb{Z}_3 , temos que essas matrizes são equivalentes. Agora observe que $(M_E^V)^* = M_E^C$.

Sendo equivalentes, elas possuem o mesmo espaço de linhas e principalmente o mesmo espaço nulo, donde concluímos:

$$\nu(M_{E^*}^{V^*}) = \nu(M_E^C)$$

Então, fixando uma base para este subespaço, uma escolha⁴ em A para cada elemento desta base vai identificar as tensões por um lado com os fluxos pelo outro. Por questões de dualidade na argumentação, concluímos também o “vice versa”. ■

⁴Usando o Lema 3.5.

CAPÍTULO 4

CONTANDO ÓRBITAS DE AÇÕES DE GRUPOS

Neste capítulo, vamos introduzir polinômios para contar o número de órbitas na ação de um grupo sobre um grafo e uma estrutura adicional, como uma coloração, um fluxo, ou uma tensão. Vamos nos basear essencialmente em Cameron [CJR08] e Rudd [Rud10]. A ferramenta fundamental a ser utilizada neste capítulo será o *lema de contagem de órbitas*, resultado clássico em Teoria de Grupos. Também usaremos fortemente a teoria de matrizes apresentada no capítulo anterior. O ponto alto deste capítulo é a introdução de uma definição apropriada para um polinômio de Tutte que capture as simetrias do grupo, o que ocorrerá por meio da adição de novas variáveis. Mostraremos que esta definição se especializa corretamente para um polinômio cromático orbital ou um polinômio orbital de fluxo.

Não abordaremos neste capítulo aspectos relacionados ao *Índice Cíclico de um Grupo*, tipo de polinômio definido em grupos. Em particular não estaremos interessados na teoria de Polya, que também diz respeito à enumeração de simetrias. Para mais informações a respeito deste tema, sugerimos [Lin81]. Como aponta Cameron em [CJR08], apesar de existir uma definição sugerida por ele próprio que generaliza simultaneamente o polinômio de Tutte convencional e o índice cíclico de um grupo, não é conhecida relação entre o polinômio que apresentaremos neste capítulo e este polinômio definido em grupos.

Neste capítulo, utilizaremos G para denotar um grupo e X para um grafo.

4.1 POLINÔMIO CROMÁTICO ORBITAL

Seja G um grupo de automorfismos de um grafo X , e seja k um inteiro positivo. Nosso objetivo é contar o número de órbitas da ação do grupo G nas k -colorações de X . Ou seja, sempre que uma coloração puder ser obtida de outra por meio de um automorfismo do grafo, elas estarão na mesma órbita, e as contaremos somente uma vez.

Para usar o Lema de contagem de órbitas apresentado no capítulo 1, precisamos obter $\text{fix}(g)$ para cada g . Ora, uma coloração f é fixada por g se, e somente se, todos os vértices em cada órbita de g (visto como automorfismo do grafo) tiverem a mesma cor. Agora, se alguma órbita de g possui vértices vizinhos, então não existe coloração possível fixada por g . Caso contrário, denotaremos por X_g o (multi-)grafo em que cada órbita de g foi contraída a um único ponto. É imediato observar que o número de k -colorações fixadas por g é exatamente o número de k -colorações em X_g , que já sabemos ser igual a $\chi_{X_g}(k)$, o polinômio cromático do grafo X_g .

Teorema 4.1. O número de órbitas de um grupo G em k -colorações de um grafo X é denotado por:

$$O_{X,G}^x(k)$$

Isto é um polinômio de grau n e coeficiente dominante $1/|G|$.

Demonstração. Temos, pelo Lema de contagem de órbitas, que:

$$O_{X,G}^{\chi}(k) = \frac{1}{|G|} \sum_{g \in G} \chi_{X_g}(k)$$

Daí obviamente temos que trata-se de um polinômio. O grau desse polinômio é o maior dentre os graus dos $\chi_{X_g}(k)$, mas o grau de cada um desses é o número de vértices em X_g . Ora, este número é maximal quando g é a identidade, ou seja, quando não há qualquer contração. Será exatamente n . Isto conclui a demonstração. ■

Exemplo 4.1. Por argumentos simples de contagem, mostra-se que:

$$O_{X,\{\text{id}\}}^{\chi}(k) = \chi_X(k)$$

$$O_{K_n, S_n}^{\chi}(k) = \binom{k}{n}$$

$$O_{K_n, G}^{\chi}(k) = \frac{k(k-1)\dots(k-n+1)}{|G|}$$

$$O_{E_n, S_n}^{\chi}(k) = \binom{k+n-1}{n} = (-1)^n \binom{-k}{n}$$

4.2 POLINÔMIOS ORBITAIS DE FLUXO E DE TENSÃO

Para simplificar a notação, vamos denotar a ação de um elemento g sobre um elemento x por:

$$g(x) = x^g$$

Seja G um grupo de automorfismos agindo em um grafo X . Seja $g \in G$. Seja $f : E \rightarrow A$, grupo abeliano. Então definimos que g age sobre f da seguinte forma:

$$f(v \rightarrow w)^g = f(v^{g^{-1}} \rightarrow w^{g^{-1}}) \text{ ou } -f(w^{g^{-1}} \rightarrow v^{g^{-1}})$$

a depender de qual a orientação da aresta entre os vértices $v^{g^{-1}}$ e $w^{g^{-1}}$.

Observe que esta função f pode tanto ser uma tensão como um fluxo. A contagem das órbitas dessas estruturas, fluxos e tensões, não é simples. Apesar de haver uma estreita relação entre tensões e colorações, como vimos no capítulo anterior, uma tensão fixada por um automorfismo g pode não ser o gradiente de uma coloração fixada por este mesmo automorfismo. Por exemplo, considere o grafo cíclico C_n e g uma rotação que manda cada vértice num vizinho. Suponha que $a \in A$ é tal que $n \cdot a = 0$. Agora orientemos todas as arestas de C_n no sentido da rotação, e atribuamos o valor $f(e) = a$ para toda $e \in E(C_n)$. Observe que f é uma tensão, fixada por g . Por outro lado, a coloração associada a f será fixada por g se, e somente se, $a = 0$ (o que, em particular, nem faz parte da nossa definição de tensão - e a coloração associada nem própria seria).

O teorema a seguir caracteriza o número de órbitas de G em fluxos e tensões.

Teorema 4.2. O número de órbitas de G em fluxos e tensões de um grafo X com valores num grupo abeliano finito A são dados respectivamente por:

$$O_{X,G}^{\varphi}(\alpha_1, \dots, \alpha_n) \text{ e } O_{X,G}^{\tau}(\alpha_1, \dots, \alpha_n)$$

onde $O_{X,G}^{\varphi}$ e $O_{X,G}^{\tau}$ são polinômios em n variáveis x_1, \dots, x_n , e os α_i são o número de soluções da equação $i.a = 0$ no grupo abeliano A .

A demonstração deste teorema seguirá mais adiante, após falarmos do polinômio orbital de Tutte.

4.3 O POLINÔMIO ORBITAL DE TUTTE

Nesta seção abordaremos um dos pontos altos desta monografia. Nosso objetivo será apresentar uma versão generalizada do polinômio de Tutte, na tentativa de capturar as simetrias do grafo descritas por um grupo de automorfismos no próprio polinômio. Seguiremos basicamente Cameron [CJR08].

Dada uma matriz M com n colunas, definimos um automorfismo de M como sendo um automorfismo do módulo livre R^n que preserva os espaços de linhas e de nulidade de M . Obviamente, se M possui dual M^* , elas terão os mesmos automorfismos. Todo automorfismo g portanto pode ser representado por uma matriz $n \times n$, que chamaremos naturalmente por g . Definindo 1_n a matriz identidade de tamanho n , introduzimos as seguintes notações:

$$M_g = \begin{pmatrix} M \\ g - 1_n \end{pmatrix} \quad M_g^* = \begin{pmatrix} M^* \\ g - 1_n \end{pmatrix}$$

Introduzimos ainda mais notações. Para $S \subset E = [1, \dots, n]$, N matriz com n colunas indexadas por E , $N[S]$ será a submatriz de N composta pelas colunas de índice em S .

Fixado um elemento $r \in R$, a classe de associados de r é o conjunto $\{ru : u \in R^*\}$, onde R^* são os invertíveis do anel. Observe que as classes de associados particionam o anel R . Definimos por I o conjunto das classes de associados. Definimos então dois conjuntos de variáveis, que tomam por conjunto de índices o conjunto I :

$$\{x_{\iota} : \iota \in I\} \text{ e } \{x_{\iota}^* : \iota \in I\}$$

Observe que os ι s são subconjuntos de R . Convencionamos que $x_r = x_{\iota}$ se $r \in \iota$, classe de associados de r .

Para uma matriz N , sejam d_1, \dots, d_n seus fatores invariantes, inclusive com os zeros. Definimos:

$$x(N) = \prod_{j=1}^n x_{d_j} \text{ e } x^*(N) = \prod_{j=1}^n x_{d_j}^*$$

Finalmente podemos definir o polinômio orbital de Tutte. Vamos assumir que M e M^* é um par dual a partir de agora.

Definição 4.1. Seja G grupo de automorfismos finito da matriz M . Então o *polinômio orbital de Tutte* da matriz é:

$$\text{OT}(M; G) = \frac{1}{|G|} \sum_{g \in G} \sum_{S \subset E} x(M_g[S]) x^*(M_g^*[E \setminus S])$$

Observe naturalmente que o polinômio orbital de Tutte de um grafo $X = (V, E)$ será o polinômio orbital da matriz M_E^V . Para motivar a definição acima, observe os teoremas abaixo.

Teorema 4.3. Se G é o grupo trivial, então $\text{OT}(M; G)$ envolve somente x_0, x_1, x_0^* e x_1^* . Fazendo $x_1 = x_1^* = 1$, $x_0 = y - 1$ e $x_0 = x - 1$, então temos o polinômio de Tutte da matróide associada a M .

Demonstração. Se G é trivial, as matrizes M e M^* possuem como fatores invariantes 0 e 1 (pois são dualizáveis). Por outro lado, $r(S)$, posto de S , é exatamente a multiplicidade do fator invariante 1 em S . Teremos:

$$\text{OT}(M; G) = \sum_{S \subset E} x(M[S])x^*(M^*[E \setminus S])$$

Mas

$$x(M[S]) = x_0^{\text{mult. de } 0} x_1^{\text{mult. de } 1} = (y - 1)^{n(S)}$$

e também:

$$x^*(M^*[E \setminus S]) = (x_0^*)^{\text{mult. de } 0} (x_1^*)^{\text{mult. de } 1} = (x - 1)^{n^*(E \setminus S)}$$

Mas $n^*(E - S) = |E - S| - r^*(E - S) = |E - S| - [r(E - (E - S)) - r(E) + |E - S|] = r(E) - r(S)$ concluindo a demonstração. ■

Consideramos agora o grafo dirigido X com n arestas, e sua matriz de incidência vértice-aresta M_E^V . Um automorfismo de X é representado por uma matriz g de dimensão $n \times n$ em que a entrada (e, e') é 1 se o automorfismo manda e em e' sem inverter orientação, -1 se inverte, 0 no caso em que e não vai para e' . Lembramos que fixado nosso grupo abeliano A , α_i é o número de soluções da equação $ix = 0$ em A , onde i é um inteiro.

Teorema 4.4. Seja $X = (V, E)$, $M = M_E^V$ sobre \mathbb{Z} , G grupo de automorfismos de X . O polinômio orbital de Tutte $\text{OT}(M; G)$, ao fazermos as substituições $x_i = \alpha_i$ e $x_i^* = -1$ para todo i , é o número de G -órbitas em A -fluxos de X . A substituição $x_i = -1$ e $x_i^* = \alpha_i$ é o número de órbitas em A -tensões.

Demonstração. Observamos inicialmente que $x(M_g[E])$ é o número total de A -fluxos (possivelmente nulos em algumas arestas) fixados por g . Temos que $x \in A^n$ é fluxo se, e somente se, $M \cdot x^T = 0$. É fixada por g se, e somente se, $g \cdot x^T = x^T$. Logo x é um fluxo, e fixado por g , se, e somente se:

$$M_g \cdot x^T = \begin{pmatrix} M \cdot x^T \\ g \cdot x^T - I \cdot x^T \end{pmatrix} = \begin{pmatrix} 0 \\ x^T - x^T \end{pmatrix} = 0$$

Operações elementares em linhas e colunas de M_g não alteram o número de soluções. Com efeito, as operações em linha nem alteram as soluções, ao passo que uma operação o em colunas transforma a solução x em $x \cdot o^{-1}$.

Considere então a matriz M_g na forma normal de Smith, com fatores invariantes $\{d_1, \dots, d_r\}$ e 0 com multiplicidade $n - r$. Então o número de A -fluxos fixados por M_g é

o número de soluções de $\text{FNS}(M_g) \cdot x^T = 0$. Mas $x = (x_1, \dots, x_n)$ é solução desta equação se, e somente se, $d_j x_j = 0$ para $j = 1, \dots, r$, com x_{r+1} até x_n livres. Ou seja, o número de soluções será:

$$\alpha_{d_1} \alpha_{d_2} \dots \alpha_{d_r} \alpha_0^{n-r} = x(M_g[E])$$

Agora vamos olhar para o que ocorre quando temos $S \subset E$. Seja $\theta(S)$ o número de fluxos fixados por g que se anulam em todas as arestas fora de S , e $\phi(S)$ o número de fluxos fixados por g que se anulam exatamente nas arestas fora de S . Temos que:

$$\theta(S) = x(M_g[S])$$

por um argumento igual ao do parágrafo anterior, apenas restringindo para a matriz $M_g[S]$, fazendo com que os fluxos x recebam 0 nas entradas correspondentes as arestas em $E - S$. Pelo princípio da Inclusão e Exclusão, teremos que:

$$\phi(E) = \sum_{S \subset E} (-1)^{n-|S|} \theta(S)$$

Mas $(-1)^{n-|S|} = x^*(M_g^*[S])$ se $x_i^* = -1$ para todo i .

Pelo lema de contagem de órbitas, o número total de órbitas da ação de um grupo em uma estrutura é:

$$\frac{1}{|G|} \sum_{g \in G} |\text{fix}(g)|$$

Teremos então:

$$\frac{1}{|G|} \sum_{g \in G} \sum_{S \subset E} (-1)^{n-|S|} \theta(S) = \frac{1}{|G|} \sum_{g \in G} \sum_{S \subset E} x(M_g[S]) x^*(M_g^*[S])$$

Para ver a parte da tensão, lembre-se que $(M_E^V)^* = M_E^C$, e que $M_E^C \cdot x^T = 0$ se, e somente se, x é uma tensão (possivelmente nula). O restante do argumento é basicamente o mesmo. █

Generalizando o teorema acima, teremos:

Teorema 4.5. Dado grafo X , grupo de automorfismos G . Seja φ_m o número de órbitas na ação de G sobre A -fluxos não nulos em exatamente $n - m$ arestas de X . Seja τ_m o número de órbitas na ação de G sobre A -tensões não nulas em exatamente $n - m$ arestas de X . Então:

- (a) $\sum_{m=0}^n \varphi_m x^m = \text{OT}(M; G)$, com $x_i = \alpha_i$ e $x_i^* = x - 1$.
- (b) $\sum_{m=0}^n \tau_m x^m = \text{OT}(M; G)$, com $x_i = x - 1$ e $x_i^* = \alpha_i$.

Demonstração. Para mostrar (a), observe que o papel das variáveis x_i^* foi considerado na equação:

$$\phi(E) = \sum_{S \subset E} (-1)^{n-|S|} \theta(S)$$

Só que agora queremos determinar fluxos não nulos em um conjunto T fixo, então este T entra no lugar de E . Teremos então:

$$\phi(T) = \sum_{S \subset T} (-1)^{|T|-|S|} \theta(S)$$

Teremos então:

$$\begin{aligned} \sum_{m=0}^n \varphi_m x^m &= \frac{1}{|G|} \sum_{g \in G} \sum_{T \subset E} \phi(T) x^{n-|T|} = \frac{1}{|G|} \sum_{g \in G} \sum_{T \subset E} \sum_{S \subset T} (-1)^{|T|-|S|} \theta(S) x^{n-|T|} = \\ &= \frac{1}{|G|} \sum_{g \in G} \sum_{S \subset E} \theta(S) \sum_{T \supset S} (-1)^{|T|-|S|} x^{n-|T|} = \\ &= \frac{1}{|G|} \sum_{g \in G} \sum_{S \subset E} \theta(S) \sum_{k=0}^{n-|S|} \binom{n-|S|}{|T|-|S|} (-1)^{|T|-|S|} x^{n-|T|} = \\ &= \frac{1}{|G|} \sum_{g \in G} \sum_{S \subset E} \theta(S) (x-1)^{n-|S|} = \frac{1}{|G|} \sum_{g \in G} \sum_{S \subset E} x(M_g[S]) x^*(M_g^*[S]) \end{aligned}$$

A demonstração de (b) segue exatamente da mesma forma, a partir da observação que já fizemos quanto à dualidade entre M_E^V e M_E^C . ■

Sobre as colorações, infelizmente o polinômio de Tutte apresentado neste formato não nos permite considerar colorações em grafos não conexos. Observe o teorema abaixo.

Teorema 4.6. Seja $X = (V, E)$ e denotamos $M_E^V = M$. O número de k -colorações em um grafo qualquer X fixadas por um automorfismo g é:

$$k^{c'(g)} \sum_{S \subset E} x(M_g[S]) x^*(M_g^*[S])$$

fazendo $x_i = -1$, $x_0^* = k$, $x_i^* = 1$ se $i > 0$. O termo $c'(g)$ indica o número de ciclos de g no conjunto dos componentes conexos de X .

Para a demonstração, será necessário que nenhum elemento do domínio R seja aditivamente cíclico. De fato, não há nenhuma perda de generalidade em supor que $R = \mathbb{Z}$. O lema a seguir é de fundamental importância.

Lema. Para qualquer $S \subset E$, fixado um automorfismo g , vale que:

$$c'(g) + n(M_g^*[S]) = c(g)$$

onde $c(g)$ é o número de ciclos de g nos vértices do grafo.

Demonstração do lema. Vamos omitir os argumentos $[S]$, indicando que as considerações valem para qualquer S . Seja g^E a matriz (com sinais) que representa a permutação das arestas de E induzidas por g , que nesta notação será visto somente como automorfismo, e seja g^V a matriz que representa a permutação nos vértices em V . Como g é automorfismo do grafo, é trivial observar que:

$$g^V \cdot M = M \cdot g^E \Leftrightarrow (g^V - I) \cdot M = M \cdot (g^E - I)$$

Também é fácil ver que $(g^V)^T = (g^{-1})^V$, e que $(g^E)^T = (g^{-1})^E$, portanto as igualdades acima valem com matrizes transpostas. Agora observemos que cada ciclo da ação de g corresponde a um bloco quadrado na matriz $(g^V - I)$, onde a diagonal é composta por -1 s e cada linha e cada coluna possui exatamente um número 1, o restante sendo 0. Observe que a soma de todas as linhas é a linha nula, mas que a remoção de qualquer uma delas gerará um conjunto linearmente independente. Portanto estes blocos tem co-posto 1. Rearrumando a matriz, é fácil ver que o co-posto de $(g^V - I)$ é a soma dos co-postos destes blocos, em outras palavras:

$$c(g) = n(g^V - I)$$

Observe que o espaço nulo de linhas (e não de colunas, como até agora) de $(g^V - I)$, denotado por $\mu(g^V - I)$, é gerado por vetores que são constantes em cada ciclo de g , e que $\mu(M)$ é gerado por vetores que são constantes em cada componente conexa do grafo. Sejam $\{q_1, \dots, q_\kappa\}$ os geradores de $\mu(M)$, onde $\kappa = \kappa(G)$, digamos com entradas iguais a 1 em uma componente conexa e nulas nas demais. Daí:

$$\text{Se } x \cdot (g^V - I)M = 0, \text{ então } x \cdot (g^V - I) = \sum_{i=1}^{\kappa} a_i q_i \in \mu(M)$$

Mas a soma das coordenadas de $x \cdot g^V$ e x é a mesma em cada componente conexa, implicando que $a_i = 0$ para todo i (para toda componente conexa). Isto nos diz que $\mu[(g^V - I)M] \subset \mu(g^V - I)$. Por outro lado, é trivial observar $\mu(g^V - I) \subset \mu[(g^V - I)M]$. Portanto:

$$\mu[(g^V - I)M] = \mu(g^V - I)$$

Agora $(g^V - I)M = M(g^E - I)$, como já foi observado. Voltando a tratar do espaço de nulidade em colunas, temos:

$$\begin{aligned} \nu(M_g^*) &= \nu(M^*) \cap \nu(g^E - I) = \rho(M) \cap \nu(g^E - I) = \\ &= \{xM : xM((g^E)^T - I) = 0\} = \{xM : x \in \mu[M((g^E)^T - I)]\} = \\ &= \{xM : x \in \mu[((g^V)^T - I)M]\} = \{xM : x \in \mu((g^V)^T - I)\} \end{aligned}$$

Considere então:

$$\pi : \mu((g^V)^T - I) \rightarrow \rho(M)$$

tal que $\pi(x) = xM$. O domínio é $\mu((g^V)^T - I)$, o conjunto dos x tais que x é constante em cada ciclo (em vértices) de g . O núcleo é $\mu(M) \cup \mu((g^V)^T - I)$, o conjunto dos x

que são constantes em cada ciclo e em cada componente conexa, ou seja, em cada ciclo no conjunto das componentes conexas. Pelo teorema do núcleo e imagem, teremos:

$$\dim(\text{im}(\pi)) = \dim(\mu((g^V)^T - I)) - c'(g) = n(g^V - I) - c'(g) = c(g) - c'(g)$$

E portanto:

$$c(g) - c'(g) = \dim(\text{im}(\pi)) = \dim(\nu(M_g^*)) = n(M_g^*)$$

Agora vamos mostrar o teorema.

Demonstração do teorema. Observaremos que o número de colorações (não necessariamente próprias) fixadas por g é igual a $k^{c'(g)}x^*(M_g^*[S])$ com as substituições do teorema. Novamente, vamos omitir os argumentos $[S]$.

Começamos observando que, fazendo $x_0^* = k$, $x_i^* = 1$ se $i > 0$, então:

$$x^*(M_g^*) = k^{n(M_g^*)}$$

Por outro lado, o número de colorações fixadas por g é $k^{c(g)}$, onde $c(g)$ é o número de ciclos de g nos vértices do grafo (pois temos k opções para cada ciclo). Queremos mostrar então que:

$$k^{c'(g)}k^{n(M_g^*)} = k^{c(g)}$$

Mas isto é equivalente a $c'(g) + n(M_g^*) = c(g)$, que já vimos no lema.

Agora pelo princípio da inclusão e exclusão, o número de colorações próprias fixadas por g em E será:

$$\sum_{S \subset E} (-1)^{n-|S|} k^{c'(g)} x^*(M_g^*[S])$$

Mas $(-1)^{n-|S|} = x(M_g[S])$ se $x_i = -1$ para todo i . Teremos portanto que o número de colorações fixadas por g será:

$$k^{c'(g)} \sum_{S \subset E} x(M_g[S]) x^*(M_g^*[S])$$

como queríamos. █

Podemos particularizar o teorema sem dificuldades para quando X for conexo:

Corolário 4.6.1. Se X é grafo conexo, então o número de órbitas de um grupo de automorfismos G em k -colorações de X é:

$$k \cdot \text{OT}(M; G)$$

fazendo $x_i = -1$ para todo i , $x_0^* = k$, $x_i^* = 1$ se $i > 0$.

Demonstração. Basta notar que $c'(g) = 1$ para todo g (aliás, esta é uma hipótese mais fraca), e portanto pode ser posto em evidência ao aplicarmos o lema de contagem de órbitas. O número total de órbitas da ação de um grupo em uma estrutura é:

$$\frac{1}{|G|} \sum_{g \in G} |\text{fix}(g)|$$

Teremos então para as colorações:

$$\frac{1}{|G|} \sum_{g \in G} k \cdot \sum_{S \subset E} x(M_g[S]) x^*(M_g^*[S])$$

Ou seja:

$$k \cdot \text{OT}(M; G)$$

com as substituições do teorema. ■

Observamos que no caso do grafo não ser conexo, não é conhecida uma maneira de associar o número de k -colorações com o Polinômio Orbital de Tutte.

4.3.1 Variáveis no polinômio de Tutte

Nesta seção, vamos mostrar qual condição necessária para que uma variável apareça em nosso polinômio de Tutte. Será novamente necessário o uso de álgebra linear.

Mais alguma álgebra linear Se M , F_0 e F_1 são R -módulos, então denotamos uma *sequência exata à direita de homomorfismos* por:

$$F_1 \xrightarrow{\varphi} F_0 \xrightarrow{\pi} M \rightarrow 0$$

e isto quer dizer que π é sobrejetora, e que $\text{im}(\varphi) = \text{nuc}(\pi)$. Esta sequência é uma *apresentação* de M se F_0 e F_1 forem livres (possuírem base). Observe que neste caso, o homomorfismo φ pode ser representado por uma matriz \mathbf{m} , e que $\text{im}(\varphi) = \rho(\mathbf{m})$. Mas usando a propriedade universal de homomorfismos, teremos que:

$$M \simeq F_0 / \text{nuc}(\pi) = F_0 / \text{im}(\varphi) = F_0 / \rho(\mathbf{m})$$

Também costuma-se dizer que a matriz \mathbf{m} é uma apresentação (livre) do módulo.

Por um fator invariante de um R -módulo M finitamente gerado, estamos nos referindo aos fatores invariantes da matriz que é a apresentação a seguir deste módulo:

$$R^m \xrightarrow{\varphi} R^n \xrightarrow{\pi} M \rightarrow 0$$

onde n é a cardinalidade de um menor número de geradores de M , e m é a cardinalidade do menor número de geradores de $\text{nuc}(\pi)$. Isto significa, em particular, que:

$$M \simeq R^n / \rho(\mathbf{m}) \simeq \bigoplus_{i=1}^n R / (d_i)$$

pelo teorema da forma normal de Smith. Em outras palavras, existe um isomorfismo entre o módulo e a soma direta dos quocientes deste módulo por seus fatores invariantes.

Observe que podemos extrair os fatores invariantes nulos, e teremos:

$$M \simeq R^{n-r} \oplus \bigoplus_{i=1}^r R/(d_i)$$

Ou seja, todo módulo M se expressa como soma direta de um R -módulo livre com um módulo de torção¹.

Observe ainda que sobre um anel de ideais principais, todo módulo sem torção e finitamente gerado é um módulo livre. De fato, a decomposição deste módulo como acima não poderá conter elementos do tipo $R/(d_i)$. Só restará portanto a parte livre.

Lema 4.1. Seja W um \mathbb{Z} -módulo livre finitamente gerado, g um automorfismo de W de ordem i . Seja I a matriz identidade de tamanho conveniente. Então os fatores invariantes de $W/(g - I)W$ são 0 ou um divisor de i .

Demonstração. Seja

$$W/(g - I)W = U_0 \oplus U_1 ; \quad \text{onde } U_0 \text{ é livre, e } U_1 \text{ é de torção}$$

Os fatores invariantes do módulo livre são todos nulos, então vamos olhar para U_1 . Seja W_1 tal que $\pi(W_1) = U_1$, onde π é a projeção $W \rightarrow W/(g - I)W$. Seja

$$V_1 = W_1 \otimes \mathbb{Q}$$

ou seja, W_1 com coeficientes em \mathbb{Q} . Observe que um autovalor de g em V_1 é necessariamente uma i -ésima raiz da unidade, pois:

$$g(v) = k.v \Rightarrow g^i(v) = k^i.v = v \Rightarrow k^i = 1$$

Suponha para efeito de derivar contradição que 1 é autovalor, digamos com autovetor v . Sabemos que um múltiplo inteiro de v está em W_1 . Seja w este múltiplo. Suponha que:

$$kw = \bar{0}, \text{ ou seja, } kw \in (g - I)W, \text{ digamos } kw = (g - I)x$$

onde $g \cdot w = w$. Então teremos que:

$$kw = (g^2 - g)x, kw = (g^3 - g^2)x, \dots, kw = (1 - g^{i-1})x$$

Somando as equações, teremos:

$$ikw = 0$$

contrariando o fato que w pertence a um módulo livre, no caso W_1 . Então não existe k tal que $kw = \bar{0}$, implicando que w gera um sub-módulo livre de torção em $W_1/(g - I)W_1$,

¹Um elemento v de um R -módulo M é dito de *torção* quando existe um $r \in R$, não divisor de zero, tal que $r.v = 0$. É fácil verificar que um R -módulo do tipo $R/(d_i)$ é todo de torção, em particular, $d_i.\bar{r} = \bar{0}$ para todo $\bar{r} \in R/(d_i)$.

contrariando a hipótese sobre este módulo. Da igualdade $g^i - I = (g - I)(g^{i-1} + \dots + I)$, temos que este segundo fator zera em V_1 , e logo em W_1 .

Agora considere o polinômio de coeficientes inteiros $f(x)$ tal que:

$$f(y + 1) = \frac{((y + 1)^{i-1} + \dots + 1) - i}{y}$$

Chamando $x = y + 1$, teremos:

$$f(x)(x - 1) = (x^i + \dots + 1) - i$$

Mas tanto $g^i + \dots + I$ como $g - I$ anulam o módulo $W_1/(g - I)W_1$, logo i também anula este módulo, portanto os fatores invariantes do módulo são divisores de i , conforme queríamos. ■

De volta às variáveis

Teorema 4.7. Se a variável x_i aparece no polinômio orbital de Tutte, então $i = 0$ ou i é a ordem de um elemento de G .

Lembre-se que a variável x_i vai aparecer exatamente quando i for um fator invariante da matriz $M_g[S]$ para algum $S \subset E$, pois $x(M_g[S]) = \prod x_{d_j}$, onde d_1, \dots, d_s são os fatores invariantes de $M_g[S]$.

Demonstração. Se $k|i$, e i é ordem de g , então $g^{i/k}$ tem ordem k . Daí precisamos mostrar que ou 0 ou os divisores da ordem i de um automorfismo g são fatores invariantes das matrizes M_g e M_g^* . Em outras palavras, isto significa dizer que:

$$\mathbb{Z}^{|E|}/\rho(M_g) \text{ e } \mathbb{Z}^{|E|}/\rho(M_g^*)$$

são somas diretas de um módulos livre com um módulo anulado por i . Olhando para o primeiro, teremos:

$$\mathbb{Z}^{|E|}/\rho(M_g) \simeq \mathbb{Z}^{|E|}/\rho(M) \oplus \mathbb{Z}^{|E|}/\rho(g - I)$$

onde $\rho(g - I) = \mathbb{Z}^{|E|}(g - I) = (g^T - I)\mathbb{Z}^{|E|}$, lembrando $g^T = g^{-1}$ (logo mesma ordem). Mas $\mathbb{Z}^{|E|}/\rho(M)$ só tem 0s e 1s como fatores invariantes (pois M é dualizável), e:

$$\mathbb{Z}^{|E|}/(g^T - I)\mathbb{Z}^{|E|}$$

está no formato do lema da seção anterior. ■

4.4 CONCLUSÃO

De fato ainda não há muita literatura sobre este tema. O natural daqui seria apresentar o que consta em Cameron [CK07] sobre raízes dos polinômios orbitais. Não acreditamos, todavia, que isso nos seria de grande acréscimo, uma vez que ainda não há uma teoria bem estabelecida.

Acreditamos que é mais vantajoso apresentar uma segunda generalização do polinômio de Tutte, e que segue em um caminho absolutamente diferente. Ampliaremos nossa compreensão sobre o tema, e abriremos possibilidades para, no futuro, buscarmos uma relação entre os dois polinômios.

CAPÍTULO 5

POLINÔMIO DE TUTTE EM VÁRIAS VARIÁVEIS

Neste capítulo, vamos falar do polinômio de Tutte em multi-variáveis tratado por Sokal [Sok05], e estudar as relações entre o polinômio de Tutte e modelos provenientes da Mecânica Estatística (obviamente muito mais interessados no polinômio de Tutte). Seguiremos em linhas gerais o que consta em Sokal [Sok05] e Bollobás [Bol98]. Não é claro, como aponta Cameron [CJR08], se existe alguma relação entre o polinômio de Tutte em várias variáveis introduzido por Sokal e o polinômio orbital de Tutte apresentado no capítulo anterior.

Neste capítulo, voltaremos a utilizar G para denotar um grafo.

5.1 O POLINÔMIO DICROMÁTICO

Seja $G = (V, E)$ um multigrafo. Começamos introduzindo o *polinômio dicromático* $Z_G(q, v)$ pelas relações abaixo:

- (i) $Z_{E_n} = q^n, \forall n \geq 1$
- (ii) $Z_{G \setminus e} + vZ_{G/e}, \forall e \in E(G)$ (ponte, laço ou qualquer)

Veremos que trata-se de uma boa definição. Com efeito, lembramos a Definição 2.3, do capítulo 2 desta monografia.

Proposição 5.1. Este polinômio dicromático nada mais é do que o polinômio universal calculado em: $\alpha = q, \sigma = 1, \tau = v, x = (q + v)/q$ e $y = 1 + v$.

Demonstração. Quanto a α, σ e τ , é óbvio. Quanto a y , basta observar que se e é laço, então $G \setminus e = G/e$. Precisamos mostrar portanto que, se e é uma ponte, então:

$$\frac{q + v}{q} U_{G \setminus e} = U_{G \setminus e} + vU_{G/e}$$

Ou seja, que $U_{G \setminus e} = qU_{G/e}$. De fato, sejam G_1 e G_2 as componentes separadas por e . Então relembremos as considerações sobre invariantes de Tutte-Grothendick no Teorema 2.6. Teremos que

$$U_{G \setminus e} = U_{G_1} U_{G_2}$$

e que

$$U_{G/e} = \frac{U_{G_1} U_{G_2}}{q}$$

concluindo. |

Com a unicidade do polinômio universal, sabemos que qualquer polinômio que satisfaça as relações na definição do polinômio dicromático só pode ser o próprio.

O polinômio dicromático relaciona-se com o polinômio de Tutte da seguinte forma:

$$Z_G(q, v) = q^{\kappa(G)} v^{r(E)} T_G \left(\frac{q+v}{v}, 1+v \right)$$

consequência imediata da proposição anterior e do Teorema 2.3.

Equivalentemente, podemos escrever:

$$T_G(x, y) = (x-1)^{-\kappa(G)} (y-1)^{-|V|} Z_G((x-1)(y-1), (y-1))$$

Ressaltamos que o polinômio cromático apresentado no segundo capítulo desta monografia nada mais é do que este polinômio dicromático calculado com $v = -1$ (o grafo não pode ter laços).

Teorema 5.1 (Definição alternativa).

$$Z_G(q, v) = \sum_{A \subseteq E} v^{|A|} q^{\kappa(G_A)}$$

Demonstração. Para efeitos de notação, seja temporariamente

$$\widehat{Z}_G(q, v) \stackrel{\text{def}}{=} \sum_{A \subseteq E} v^{|A|} q^{\kappa(G_A)}$$

Observe:

(i) Trivialmente $\widehat{Z}_{E_n}(q, v) = q^n$.

(ii) Observe:

$$\sum_{A \subseteq E} v^{|A|} q^{\kappa(G_A)} = \sum_{A \subseteq E \setminus e} v^{|A|} q^{\kappa(G_A)} + \sum_{\substack{A \cup e \\ A \subseteq E \setminus e}} v^{|A|} q^{\kappa(G_A)}$$

O primeiro termo do lado direito é exatamente igual a $\widehat{Z}_{G \setminus e}(q, v)$, pois $\kappa(G_A) = \kappa((G \setminus e)_A)$ se $e \notin A$. O segundo termo será exatamente $v \widehat{Z}_{G/e}(q, v)$, pois $\kappa(G_A) = \kappa((G/e)_A)$ se $e \in A$. ■

5.2 MOTIVAÇÃO FÍSICA - O MODELO DE POTTS

Seja $G = (V, E)$ multigrafo e seja $q \geq 1$ inteiro. Denotaremos o conjunto $\{1, \dots, q\} \subset \mathbb{N}$ por $[q]$. Definimos uma função:

$$\omega : V \rightarrow [q]$$

como um *estado* do *modelo de Potts* com q estados em G . Denotamos $\omega(x) = \omega_x$.

Definimos a *energia* de uma aresta como sendo 0 se os estados nos vértices são os mesmos, e 1 se são diferentes. Definimos o *hamiltoniano*, ou energia, de um estado ω por:

$$H(\omega) = \sum_{xy \in E} (1 - \delta(\omega_x, \omega_y))$$

onde δ é a função delta de Kronecker.

Fixado V e q , consideramos então o conjunto de todos os possíveis estados, a ser denotado por Ω , e que é exatamente o conjunto de todas as possíveis funções $V \rightarrow [q]$, ou seja, $\Omega = [q]^V$. A *medida boltzmanniana* $\mu : \Omega \rightarrow \mathbb{R}$ é dada por:

$$\mu_G^{q,\beta}(\omega) = e^{-H(\omega)/k_B T} = e^{-\beta H(\omega)}$$

onde k_B é a *constante de Boltzmann*, T a *temperatura absoluta* do sistema e β a *temperatura inversa*, $\beta = 1/k_B T$. A probabilidade do estado ω é, portanto:

$$\frac{\mu_G^{q,\beta}(\omega)}{P_G(q,\beta)}$$

onde P_G é a *função de partição*, ou somatório das medidas, e portanto:

$$P_G(q,\beta) = \mu_G^{q,\beta}(\Omega) = \sum_{\omega \in \Omega} \mu_G^{q,\beta}(\omega)$$

Nosso próximo resultado associa a função de partição acima com o polinômio dicromático.

Teorema 5.2. Seja $G = (V, E)$ multigrafo, $q \in \mathbb{Z}^+$, $\beta \in \mathbb{R}$. Então:

$$P_G(q,\beta) = e^{-\beta|E|} Z_G(q, v)$$

calculado com $v = e^\beta - 1$.

Demonstração. Seja $\tilde{P}(q,\beta) = e^{\beta|E|} P_G(q,\beta)$. Nesta notação, queremos mostrar que:

$$\tilde{P}(q,\beta) = Z_G(q, v) \text{ com } v = e^\beta - 1$$

Isto significa mostrar que $\tilde{P}(q,\beta)$ satisfaz (i) e (ii) da definição do polinômio dicromático. Observe:

(i) Se $G = E_n$, então $H(\omega) = 0$, e daí:

$$\tilde{P}(q,\beta) = e^{\beta|E|} P_G(q,\beta) = e^{\beta|E|} \sum_{\omega \in \Omega} e^{-\beta H(\omega)} = e^0 \sum_{\omega \in \Omega} e^0 = q^n = Z_{E_n}(q, v)$$

(ii)

$$\begin{aligned}
\tilde{P}(q, \beta) &= e^{\beta|E|} \sum_{\omega \in \Omega} e^{-\beta H(\omega)} = e^{\beta|E|} \sum_{\omega \in \Omega} e^{(-\beta \sum_{xy \in E} (1 - \delta(\omega_x, \omega_y)))} = \\
&= \sum_{\omega \in \Omega} e^{\beta|E| + \beta(\sum_{xy \in E} \delta(\omega_x, \omega_y)) - \beta|E|} = \sum_{\omega \in \Omega} \prod_{xy \in E} e^{\beta \delta(\omega_x, \omega_y)} \\
&= \sum_{\omega \in \Omega} \prod_{xy \in E} (v + 1)^{\delta(\omega_x, \omega_y)} = \sum_{\omega \in \Omega} \prod_{xy \in E} (1 + v \delta(\omega_x, \omega_y))
\end{aligned}$$

Seja e uma aresta entre a e b , que podem ser o mesmo vértice. Vamos dividir a soma entre os estados ω tais que $\omega_a = \omega_b$ e os que ocorre a diferença. Teremos então:

$$\begin{aligned}
\tilde{P}(q, \beta) &= (1 + v) \sum_{\omega \in \Omega} \prod_{xy \in E \setminus e} (1 + v \delta(\omega_x, \omega_y)) + \sum_{\omega \in \Omega} \prod_{xy \in E \setminus e} (1 + v \delta(\omega_x, \omega_y)) = \\
&= \sum_{\omega \in \Omega} \prod_{xy \in E \setminus e} (1 + v \delta(\omega_x, \omega_y)) + \sum_{\omega \in \Omega} \prod_{xy \in E \setminus e} (1 + v \delta(\omega_x, \omega_y)) + \\
&+ v \sum_{\omega \in \Omega} \prod_{xy \in E \setminus e} (1 + v \delta(\omega_x, \omega_y)) = \\
&= \tilde{P}_{G \setminus e}(q, \beta) + v \tilde{P}_{G/e}(q, \beta)
\end{aligned}$$

pois quando contraímos a aresta e , é exatamente a mesma coisa que considerar o produto nas outras arestas dos estados que igualam nos vértices incidentes a e . ■

O que acontece se a energia nas arestas não for somente 0 ou 1 mas puder assumir qualquer valor? Seja J_e a energia na aresta e se os estados nas extremidades forem diferentes, e 0 se forem iguais. O hamiltoniano é portanto:

$$H(\omega) = \sum_{xy=e \in E} (J_e - J_e \delta(\omega_x, \omega_y))$$

onde $\omega : V \rightarrow [q]$. E como antes, consideramos a medida boltzmanniana:

$$\mu_G^{q, \beta, J}(\omega) = e^{-\beta H(\omega)}$$

onde J é a nossa notação para o conjunto (ordenado) composto por todos os J_e . A função de partição, portanto, será:

$$P_G(q, \beta, J) = \sum_{\omega \in \Omega} \mu_G^{q, \beta, J}(\omega)$$

Teorema 5.3. Para um inteiro $q \geq 1$, teremos:

$$P_G(q, \beta, J) = e^{-\beta(\sum_{e \in E} J_e)} \sum_{\omega \in \Omega} \prod_{xy=e \in E} (1 + v_e \delta(\omega_x, \omega_y))$$

onde $v_e = e^{\beta J_e} - 1$.

Demonstração. Argumentaremos como já foi feito na demonstração do teorema anterior. Ao longo destes cálculos, x e y representarão os vértices incidentes a uma aresta e .

$$\begin{aligned} e^{\beta(\sum_{e \in E} J_e)} \sum_{\omega \in \Omega} e^{-\beta H(\omega)} &= e^{\beta(\sum_{e \in E} J_e)} \sum_{\omega \in \Omega} e^{-\beta(\sum_{e \in E} (J_e - J_e \delta(\omega_x, \omega_y)))} = \\ &= e^{\beta(\sum_{e \in E} J_e)} \sum_{\omega \in \Omega} e^{-\beta(\sum_{e \in E} J_e) + \beta(\sum_{e \in E} J_e \delta(\omega_x, \omega_y))} = \\ &= \sum_{\omega \in \Omega} e^{\beta(\sum_{e \in E} J_e \delta(\omega_x, \omega_y))} = \sum_{\omega \in \Omega} \prod_{e \in E} e^{\beta J_e \delta(\omega_x, \omega_y)} = \\ &= \sum_{\omega \in \Omega} \prod_{e \in E} (1 + v_e)^{\delta(\omega_x, \omega_y)} = \sum_{\omega \in \Omega} \prod_{e \in E} (1 + v_e \delta(\omega_x, \omega_y)) \end{aligned}$$

Essa igualdade nos motiva a estender a definição de polinômio dicromático, o que faremos na próxima seção. Por ora, um breve comentário acerca de convenções utilizadas.

5.2.1 (Re)-definições, nomenclaturas e convenções

Sokal [Sok05], e o que parece ser a convenção adotada na física, exhibe as definições trabalhadas até agora com uma mudança de referencial. A energia em uma aresta é considerada 0 se os estados são diferentes, e $-J_e$ se são iguais. Permanece a definição da medida boltzmanniana, mas observe que o novo aspecto do hamiltoniano será:

$$H(\omega) = \sum_{xy=e \in E} (-J_e \delta(\omega_x, \omega_y))$$

Neste sentido, o Teorema 5.3 toma o seguinte aspecto:

Teorema 5.4.

$$P_G(q, \beta, J) = \sum_{\omega \in \Omega} \mu_G^{q, \beta, J}(\omega) = \sum_{\omega \in \Omega} \prod_{xy=e \in E} (1 + v_e \delta(\omega_x, \omega_y))$$

Também introduzimos a nomenclatura convencional por questões de completude. Uma energização nas arestas é chamada de *ferromagnética* se os J_e são todos iguais e positivos. Neste caso, ela favorece estados iguais nos vértices, no sentido em que a probabilidade:

$$\frac{\mu_G^{q, \beta, J}(\omega)}{P_G(q, \beta, J)}$$

é maior quando os estados ω são tais que vértices vizinhos assumem mesmos valores (portanto energia mínima nas arestas, já que $-J_e < 0$). Neste caso, teremos $v_e \geq 0$.

A energização é chamada *anti-ferromagnética* se os J_e forem todos iguais e negativos, e então teremos $v_e \in [-1, 0]$. Por fim, a energização é *não-física* se os $v_e < -1$, pois neste caso os pesos podem ser negativos.

Doravante, vamos considerar as definições apresentadas nesta subseção, salvo mencionado o contrário. Observe que o polinômio cromático, já mencionado no capítulo 2, e revisitado ao final da seção anterior, ocorre quando $v_e = -1$ para todo e . Isto ocorre para qualquer $J_e < 0$ com $\beta \rightarrow \infty$, ou seja, é o limite da temperatura absoluta zero do modelo de Potts *anti-ferromagnético*.

5.3 MULTI-VARIÁVEIS - ABORDAGEM EM GRAFOS

Estenderemos a definição alternativa apresentada no Teorema 5.1 atribuindo um peso v_e para cada aresta.

Definição 5.1. Seja $G = (V, E)$. O *Polinômio de Tutte em multi-variáveis* é definido por:

$$Z_G(q, \mathbf{v}) = \sum_{A \subseteq E} q^{\kappa(G_A)} \prod_{e \in A} v_e$$

onde $\mathbf{v} = \{v_e\}_{e \in E}$.

O Teorema a seguir associa esse polinômio em várias variáveis à função de partição do modelo de Potts com energia qualquer.

Teorema 5.5 (Devido a Fortuin-Kasteleyn). Considerando $\omega : V \rightarrow [q]$, e $\Omega = [q]^V$, temos:

$$\sum_{\omega \in \Omega} \prod_{e \in E} (1 + v_e \delta(\omega_x, \omega_y)) = \sum_{A \subseteq E} q^{\kappa(G_A)} \prod_{e \in A} v_e$$

Demonstração. A demonstração será por indução no número de arestas. Seja $f \in E$ aresta fixada, digamos que u e v sejam suas extremidades. Como sempre, $e \in E$ aresta qualquer, x e y suas extremidades (a variarem de acordo com a variação de e). Sejam agora:

$$\Omega^f = \{\omega \in \Omega : \delta(\omega_u, \omega_v) = 1\} \text{ e } \Omega_f = \{\omega \in \Omega : \delta(\omega_u, \omega_v) = 0\}$$

Teremos então:

$$\begin{aligned} \sum_{\omega \in \Omega} \prod_{e \in E} (1 + v_e \delta(\omega_x, \omega_y)) &= \sum_{\omega \in \Omega^f} \prod_{e \in E} (1 + v_e \delta(\omega_x, \omega_y)) + \sum_{\omega \in \Omega_f} \prod_{e \in E} (1 + v_e \delta(\omega_x, \omega_y)) = \\ &= (1 + v_f) \sum_{\omega \in \Omega^f} \prod_{e \in E \setminus f} (1 + v_e \delta(\omega_x, \omega_y)) + \sum_{\omega \in \Omega_f} \prod_{e \in E \setminus f} (1 + v_e \delta(\omega_x, \omega_y)) = \\ &= \sum_{\omega \in \Omega^f} \prod_{e \in E \setminus f} (1 + v_e \delta(\omega_x, \omega_y)) + v_f \sum_{\omega \in \Omega^f} \prod_{e \in E \setminus f} (1 + v_e \delta(\omega_x, \omega_y)) + \\ &\quad + \sum_{\omega \in \Omega_f} \prod_{e \in E \setminus f} (1 + v_e \delta(\omega_x, \omega_y)) \end{aligned}$$

Mas o primeiro termo e o terceiro termo da soma acima, combinados, formam:

$$\sum_{\omega \in \Omega^f} \prod_{e \in E \setminus f} (1 + v_e \delta(\omega_x, \omega_y)) + \sum_{\omega \in \Omega_f} \prod_{e \in E \setminus f} (1 + v_e \delta(\omega_x, \omega_y)) = \sum_{\omega \in \Omega} \prod_{e \in E \setminus f} (1 + v_e \delta(\omega_x, \omega_y)) \text{ em } G \setminus f$$

e o segundo termo é exatamente:

$$v_f \sum_{\omega \in \Omega^f} \prod_{e \in E \setminus f} (1 + v_e \delta(\omega_x, \omega_y)) = v_f \sum_{\omega \in \Omega} \prod_{e \in E \setminus f} (1 + v_e \delta(\omega_x, \omega_y)) \text{ em } G/f$$

Aplicamos, portanto, a hipótese indutiva em $G \setminus f$ e G/f , obtendo:

$$\sum_{\omega \in \Omega} \prod_{e \in E} (1 + v_e \delta(\omega_x, \omega_y)) = \sum_{A \subset E \setminus f} q^{\kappa((G \setminus f)_A)} \prod_{e \in A} v_e + v_f \sum_{A \subset E \setminus f} q^{\kappa((G/f)_A)} \prod_{e \in A} v_e$$

Mas o número de componentes conexas de $(G \setminus f)_A$ é o mesmo que o de G_A para todo A que não contém f , e o de $(G/f)_A$ é o mesmo que o de G_A para todo A que contém f . Sejam então $A \subset E \setminus f$. Teremos:

$$\sum_{\omega \in \Omega} \prod_{e \in E} (1 + v_e \delta(\omega_x, \omega_y)) = \sum_A q^{\kappa(G_A)} \prod_{e \in A} v_e + v_f \sum_{f \cup A} q^{\kappa(G_A)} \prod_{e \in A} v_e = \sum_{A \subset E} q^{\kappa(G_A)} \prod_{e \in A} v_e$$

encerrando a demonstração. |

Uma maneira de reescrever o polinômio de Tutte em várias variáveis nos ajudará a obter dois exemplos interessantes deste polinômio em tipos especiais de grafos.

Proposição 5.2.

$$Z_G(q, \mathbf{v}) = q^{|V|} \sum_{A \subset E} q^{c(G_A)} \prod_{e \in A} \frac{v_e}{q}$$

onde $c(G_A)$ é o *número ciclomático*, i.e., o número de ciclos linearmente independentes no subgrafo gerador induzido por A .

Demonstração. Obviamente é bem mais natural pensarmos nessa relação de dependência entre ciclos se os olharmos como linhas na matriz M_A^C . Lembramos que foi mostrado que:

$$M_A^V \text{ e } M_A^C \text{ formam um par dual!}$$

Neste sentido, teremos $\dim[\rho(M_A^C)] = \dim[\nu(M_A^V)] = n(A)$, ou seja, o número de ciclos linearmente independentes é igual à nulidade de um conjunto de arestas, ou simplesmente $|A| - r(A)$. Então temos a relação fundamental abaixo:

$$k(G_A) = |V| - r(A) = |V| - |A| + c(G_A)$$

o resultado segue, portanto, trivialmente. |

Dois exemplos:

Exemplo 5.1. Seja T uma árvore. Então:

$$Z_T(q, \mathbf{v}) = q \prod_{e \in E} (q + v_e)$$

pois $c(G_A) = 0$ para todo $A \subset E$.

Exemplo 5.2. Seja C_n o ciclo de ordem n . Então:

$$Z_{C_n}(q, \mathbf{v}) = \prod_{e \in E} (q + v_e) + (q - 1) \prod_{e \in E} v_e$$

pois $c(G_A) = 0$ para todo $A \subset E$ e $c(G) = 1$.

5.3.1 E quando $q \rightarrow 0$?

Consideramos a definição:

$$Z_G(q, \mathbf{v}) = \sum_{A \subset E} q^{\kappa(G_A)} \prod_{e \in E} v_e$$

E lembramos que:

$$T_G(x, y) = \sum_{A \subset E} (x - 1)^{r(E) - r(A)} (y - 1)^{n(A)}$$

Implicando a equivalência:

$$Z_G(q, v) = q^{\kappa(G)} v^{r(E)} T_G\left(1 + \frac{q}{v}, 1 + v\right)$$

já vista anteriormente.

Subgrafos geradores maximalmente conexos Se consideramos q cada vez menor, \mathbf{v} fixo, vão se sobressair no somatório os termos em que $\kappa(G_A)$ for cada vez menor. Certamente, o menor valor possível ocorrerá quando tivermos $\kappa(G)$ ao invés de $\kappa(G_A)$ para qualquer A (lembre-se que G_A tem todos os vértices de G , mas somente as arestas de A). Neste caso, consideramos:

$$\lim_{q \rightarrow 0} q^{-\kappa(G)} Z_G(q, \mathbf{v}) = \sum_{\substack{A \subset E \\ \kappa(G_A) = \kappa(G)}} \prod_{e \in A} v_e \stackrel{\text{def}}{=} \text{SGMC}_G(\mathbf{v})$$

Observe que se $v_e = 1$ para todo e , teremos o número de subgrafos geradores maximalmente conexos. Este polinômio SGMC_G é o polinômio gerador dos *subgrafos geradores maximalmente conexos*.

Se considerarmos $v_e = v$ para toda $e \in E$, e observando que fazer $q \rightarrow 0$ em $q^{-\kappa(G)} Z_G(q, \mathbf{v})$ é exatamente o mesmo que fazer $q = 0$ em $v^{r(E)} T_G\left(1 + \frac{q}{v}, 1 + v\right)$, teremos:

$$\text{SGMC}_G(v) = v^{r(E)} T_G(1, 1 + v)$$

polinômio em uma variável.

Florestas geradoras Agora faremos $q \rightarrow 0$, deixando fixo $\mathbf{w} = \mathbf{v}/q$. Da expressão obtida na Proposição 5.2, ou seja, da igualdade:

$$Z_G(q, \mathbf{v}) = q^{|V|} \sum_{A \subseteq E} q^{c(G_A)} \prod_{e \in A} \frac{v_e}{q}$$

temos que vão se sobressair no somatório os termos em que $c(G_A)$ for cada vez menor, onde o mínimo possível é claramente 0. Teremos portanto:

$$\lim_{q \rightarrow 0} q^{-|V|} Z_G(q, q\mathbf{w}) = \sum_{\substack{A \subseteq E \\ c(G_A)=0}} \prod_{e \in A} w_e \stackrel{\text{def}}{=} \text{FG}_G(\mathbf{w})$$

onde $\text{FG}_G(\mathbf{w})$ é o polinômio gerador das *florestas geradoras* do grafo G . É trivial observar que se $w_e = 1$ para toda $e \in E$, teremos exatamente o número de florestas geradoras do grafo.

Novamente tomando $v_e = v$, e observando $v/q = w$, temos que fazer $q \rightarrow 0$ em $q^{-|V|} Z_G(q, \mathbf{v})$ é exatamente o mesmo que fazer $q = 0$ em $w^{r(E)} T_G(1 + \frac{1}{w}, 1 + qw)$. Logo:

$$\text{FG}_G(w) = w^{r(E)} T_G\left(1 + \frac{1}{w}, 1\right)$$

polinômio em uma variável...

Florestas geradoras maximais Podemos tanto começar de SGMC_G como de $\text{FG}_G(\mathbf{w})$.

Em SGMC_G , fazemos $v_e \rightarrow \lambda v_e$ e tomamos o limite $\lambda \rightarrow 0$, o que claramente fará se sobressair os subgrafos geradores maximalmente conexos com menos arestas, ou seja, florestas geradoras maximais, e estas possuem exatamente $|V| - \kappa(G)$ arestas.

Por outro lado, em $\text{FG}_G(\mathbf{v})$, trocamos v_e por λv_e e faremos $\lambda \rightarrow \infty$, o que claramente fará se sobressair entre todas as florestas geradoras, aquelas com mais arestas, ou seja, as maximais.

Juntando as argumentações nos dois parágrafos acima, teremos:

$$\lim_{\lambda \rightarrow 0} \lambda^{-(|V| - \kappa(G))} \text{SGMC}_G(\lambda \mathbf{v}) = \lim_{\lambda \rightarrow \infty} \lambda^{-(|V| - \kappa(G))} \text{FG}_G(\lambda \mathbf{v}) = \sum_{\substack{A \subseteq E \\ \kappa(G_A) = \kappa(G) \\ c(G_A) = c(G)}} \prod_{e \in E} v_e$$

Ao que denotaremos por $\text{FGM}_G(\mathbf{v})$

5.3.2 O polinômio de fluxo em multi-variáveis

Vamos generalizar o polinômio de fluxo para situações em que cada aresta recebe um peso qualquer, ou seja, vamos definir um polinômio de fluxo em várias variáveis. Seja como antes $\mathbf{v} = \{v_e\}_{e \in E}$. Definimos então, para um grupo abeliano A e um grafo G , este polinômio:

$$\Phi_G(A, \mathbf{v}) = \sum_{A\text{-fluxos } \varphi} \prod_{e \in E} (1 + v_e \delta(\varphi(e), 0))$$

onde, lembramos, este é o delta de Kronecker. Obviamente, se $v_e = -1$ para toda $e \in E$, teremos simplesmente a quantidade de fluxos não nulos no grafo.

Teorema 5.6. Seja G grafo e A grupo abeliano finito tal que $|A| = q$. Então:

$$\Phi_G(A, \mathbf{v}) = q^{-|V|} \left(\prod_{e \in E} v_e \right) Z_G(q, q/\mathbf{v})$$

onde $q/\mathbf{v} = \{q/v_e\}_{e \in E}$. E mais, $\Phi_G(A, \mathbf{v})$ só depende de q , e não da estrutura do grupo.

Demonstração. Lembramos que o número total de fluxos é:

$$q^{\dim \nu(M_E^V)}$$

pelo Corolário 3.5.1. Mas $\dim \nu(M_E^V) = \dim \rho(M_E^C) = c(G)$. Agora, os fluxos que se anulam em $F \subset E$ estão em correspondência biunívoca com os fluxos em $G_{E \setminus F}$, logo a quantidade de tais fluxos é $q^{c(G_{E \setminus F})}$. Teremos então:

$$\Phi_G(A, \mathbf{v}) = \sum_{A\text{-fluxos } \varphi} \prod_{e \in E} (1 + v_e \delta(\varphi(e), 0)) = \sum_{F \subset E} q^{c(G_{E \setminus F})} \prod_{e \in F} v_e$$

Pois o termo $\prod_{e \in F} v_e$ vai aparecer na expansão do produtório em $\Phi_G(A, \mathbf{v})$ exatamente uma vez para cada A -fluxo que se anular em F ou em algum conjunto maior, ou seja, em $q^{c(G_{E \setminus F})}$ fluxos. Agora:

$$\sum_{F \subset E} q^{c(G_{E \setminus F})} \prod_{e \in F} v_e = \left(\prod_{e \in E} v_e \right) \sum_{\bar{F} \subset E} q^{c(G_{\bar{F}})} \prod_{e \in \bar{F}} \frac{1}{v_e}$$

onde $\bar{F} = E \setminus F$. Mas lembramos ao leitor a expressão obtida na Proposição 5.2:

$$Z_G(q, \mathbf{v}) = q^{|V|} \sum_{A \subset E} q^{c(G_A)} \prod_{e \in A} \frac{v_e}{q}$$

Logo teremos:

$$\left(\prod_{e \in E} v_e \right) \sum_{\bar{F} \subset E} q^{c(G_{\bar{F}})} \prod_{e \in \bar{F}} \frac{1}{v_e} = q^{-|V|} \left(\prod_{e \in E} v_e \right) Z_G(q, q/\mathbf{v})$$

5.4 VERSÃO PARA MATRÓIDES

Qual a versão do polinômio de Tutte em várias variáveis para matróides? Certamente não faz sentido falar em componentes conexas do grafo induzido por conjunto de arestas. Por outro lado, temos que estender de modo que a restrição para matróides gráficas coincida com a do grafo associado. Temos a relação:

$$r(A) = |V| - \kappa(G_A)$$

Considere então:

$$\tilde{Z}_G(q, \mathbf{v}) = q^{-|V|} Z_G(q, \mathbf{v}) = \sum_{A \in E} q^{\kappa(G_A) - |V|} \prod_{e \in A} v_e$$

Daí definimos:

$$Z_M(q, \mathbf{v}) = \sum_{A \in E} q^{-r(A)} \prod_{e \in A} v_e$$

Apresentamos um teorema conceitual interessante.

Teorema 5.7. O polinômio de Tutte em várias variáveis, na versão para matróides, é a codificação algébrica de toda informação sobre uma matróide M .

Demonstração. Como uma matróide é completamente determinada por sua função posto, temos o resultado. ■

5.4.1 Matróides e grafos

Ao longo desta seção inteira, vamos definitivamente encarar o polinômio de Tutte em várias variáveis como um polinômio definido para matróides. Ganharemos generalidade e facilidade nas demonstrações. Então lembramos que:

$$Z_{M(G)}(q, \mathbf{v}) = q^{-|V|} Z_G(q, \mathbf{v})$$

Com essa relação, estenderemos os resultados para grafos.

5.4.2 Recorrência

Lembramos que a definição original do polinômio dicromático em duas variáveis foi feita a partir de uma relação de recorrência. Por outro lado, para definirmos o polinômio dicromático em várias variáveis, utilizamos como definição uma expressão fechada 5.1, cuja análoga para o caso bi-dimensional havia sido concluída como o Teorema 5.1. Agora, faremos o inverso. Vamos mostrar que este polinômio em várias variáveis como foi definido, também satisfaz uma relação de recorrência essencialmente igual à da definição original. Esta proposição será bastante útil para as demonstrações futuras.

Proposição 5.3. Para qualquer aresta e que não seja um laço, vale que:

$$Z_M(q, \mathbf{v}) = Z_{M \setminus e}(q, \mathbf{v}_{\neq e}) + \frac{v_e}{q} Z_{M/e}(q, \mathbf{v}_{\neq e})$$

Se e for um laço, então:

$$Z_M(q, \mathbf{v}) = Z_{M \setminus e}(q, \mathbf{v}_{\neq e}) + v_e Z_{M/e}(q, \mathbf{v}_{\neq e})$$

Demonstração. Seja $A \subset E \setminus e$ para o resto da demonstração. Então:

$$\begin{aligned} \sum_{F \subset E} \left(q^{-r(F)} \prod_{f \in F} v_f \right) &= \sum_A \left(q^{-r(A)} \prod_{f \in A} v_f \right) + \sum_{A \cup e} \left(q^{-r(A \cup e)} \prod_{f \in A \cup e} v_f \right) = \\ &= \sum_A \left(q^{-r(A)} \prod_{f \in A} v_f \right) + v_e \sum_{A \cup e} \left(q^{-r(A \cup e)} \prod_{f \in A} v_f \right) \end{aligned}$$

Então, observe que:

$$r_M(A) = r_{M \setminus e}(A) \text{ e que } r_M(A \cup e) = \begin{cases} r_{M/e}(A) + 1 & \text{se } e \text{ não é laço} \\ r_{M/e}(A) & \text{se } e \text{ é laço} \end{cases}$$

o que certamente conclui. ■

Corolário 5.7.1. No caso de grafos, vale simplesmente para toda aresta e :

$$Z_G(q, \mathbf{v}) = Z_{G \setminus e}(q, \mathbf{v}_{\neq e}) + v_e Z_{G/e}(q, \mathbf{v}_{\neq e})$$

Demonstração. Basta observar que quando e é um laço não há diminuição do número de vértices em G/e , e quando que e não é laço, a diminuição afeta o termo $q^{-|V|}$, mas isso se cancela com a alteração causada em $q^{-r(A \cup e)}$. ■

5.4.3 Soma direta

Conseguimos generalizar também as expressões para soma direta de duas matróides.

Definição 5.2. Dadas duas matróides M_1 e M_2 , sobre conjuntos E_1 e E_2 , com funções posto r_1 e r_2 , definimos a matróide $M_1 \oplus M_2 = M$ com posto r de modo que:

- (i) $E(M) = E_1 \cup E_2$
- (ii) $r(A) = r_1(A)$ se $A \in E_1$ ou $r(A) = r_2(A)$ se $A \in E_2$.
- (iii) Se $A = A_1 \cup A_2$, então $r(A) = r_1(A_1) + r_2(A_2)$.

Se G_1 e G_2 são grafos, é trivial observar que:

- (i) $M(G_1 \sqcup G_2) = M(G_1) \oplus M(G_2)$
- (ii) $M(G_1 * G_2) = M(G_1) \oplus M(G_2)$

onde, lembramos, \sqcup denota a união disjunta de grafos e $*$ denota a união concatenada, ou seja, a união disjunta identificando um vértice de cada grafo como sendo o mesmo. Uma breve explicação é que uma floresta em ambas as uniões dos grafos é a união de uma floresta em cada um deles.

Desta forma, o que mostrarmos abaixo para os polinômios de Tutte de $M(G_1) \oplus M(G_2)$, estará valendo para os polinômio de Tutte de $G_1 \sqcup G_2$ e $G_1 * G_2$, possivelmente com uma correção na variável q associada ao número de vértices, uma vez que $|V(G_1 \sqcup G_2)| = |V(G_1 * G_2)| + 1$.

Proposição 5.4. Seja $M = M_1 \oplus M_2$. Então:

$$Z_M(q, \mathbf{v}) = Z_{M_1}(q, \mathbf{v}) \cdot Z_{M_2}(q, \mathbf{v})$$

Demonstração. Utilizaremos a decomposição do polinômio de Tutte e indução. Suponha que este resultado é válido para qualquer matróide com $m - 1$ arestas decomposta como soma direta. Suponha que $|E(M)| = m$. Seja $e \in M$, digamos que não seja laço, suponha sem perda de generalidade que $e \in M_1$. Teremos então:

$$Z_M = Z_{M \setminus e} + \frac{v_e}{q} Z_{M/e}$$

Mas $M \setminus e = M_1 \setminus e \oplus M_2$ e $M/e = M_1/e \oplus M_2$. Então:

$$Z_M = Z_{M \setminus e} + \frac{v_e}{q} Z_{M/e} = Z_{M_1 \setminus e} Z_{M_2} + \frac{v_e}{q} Z_{M_1/e} Z_{M_2} = \left(Z_{M_1 \setminus e} + \frac{v_e}{q} Z_{M_1/e} \right) Z_{M_2} = Z_{M_1} Z_{M_2}$$

e obviamente a mesma argumentação vale se e for um laço. |

Corolário 5.7.2. No caso gráfico, temos que se $G = G_1 \sqcup G_2$, então:

$$Z_G(q, \mathbf{v}) = Z_{G_1}(q, \mathbf{v}) \cdot Z_{G_2}(q, \mathbf{v})$$

Se $G = G_1 * G_2$, então:

$$Z_G(q, \mathbf{v}) = \frac{Z_{G_1}(q, \mathbf{v}) \cdot Z_{G_2}(q, \mathbf{v})}{q}$$

Demonstração. Temos que:

$$Z_G(q, \mathbf{v}) = q^{|V|} Z_M(q, \mathbf{v}) = q^{|V|} (Z_{M_1}(q, \mathbf{v}) \cdot Z_{M_2}(q, \mathbf{v}))$$

Se $G = G_1 \sqcup G_2$, então $|V| = |V_1| + |V_2|$. Daí:

$$q^{|V|} (Z_{M_1}(q, \mathbf{v}) \cdot Z_{M_2}(q, \mathbf{v})) = q^{|V_1|} Z_{M_1}(q, \mathbf{v}) \cdot q^{|V_2|} Z_{M_2}(q, \mathbf{v}) = Z_{G_1}(q, \mathbf{v}) \cdot Z_{G_2}(q, \mathbf{v})$$

Se $G = G_1 * G_2$, então $|V| = |V_1| + |V_2| - 1$. Daí:

$$q^{|V|} (Z_{M_1}(q, \mathbf{v}) \cdot Z_{M_2}(q, \mathbf{v})) = q^{-1} (q^{|V_1|} Z_{M_1}(q, \mathbf{v}) \cdot q^{|V_2|} Z_{M_2}(q, \mathbf{v})) = \frac{Z_{G_1}(q, \mathbf{v}) \cdot Z_{G_2}(q, \mathbf{v})}{q}$$
|

5.4.4 Limites $q \rightarrow 0$

Chamamos atenção do leitor para a correspondência entre conceitos de grafos e matróides.

Subgrafos geradores maximalmente conexos	\longleftrightarrow	Conjuntos geradores da matróide
Florestas geradoras	\longleftrightarrow	Conjuntos independentes
Florestas geradoras maximais	\longleftrightarrow	Bases

Neste sentido, consideraremos novamente os limites $q \rightarrow 0$.

Conjuntos geradores da matróide Vamos considerar o seguinte limite:

$$\lim_{q \rightarrow 0} q^{r(E)} Z_M(q, \mathbf{v})$$

certamente, ele vai selecionar somente aqueles conjuntos A tais que $r(A) = r(E)$, ou seja, os geradores da matróide. Então definimos o polinômio gerador dos conjuntos geradores por:

$$\mathbf{G}_M(\mathbf{v}) = \lim_{q \rightarrow 0} q^{r(E)} Z_M(q, \mathbf{v}) = \sum_{\substack{A \subseteq E \\ r(A)=r(E)}} \prod_{e \in A} v_e$$

Conjuntos independentes Vamos considerar o seguinte limite:

$$\lim_{q \rightarrow 0} Z_M(q, q\mathbf{w})$$

onde $\mathbf{v} = q\mathbf{w}$. Certamente, ele vai selecionar somente aqueles conjuntos A tais que $|A| = r(A)$, ou seja, os independentes. Então definimos o polinômio gerador dos conjuntos independentes por:

$$\mathbf{I}_M(\mathbf{w}) = \lim_{q \rightarrow 0} Z_M(q, q\mathbf{w}) = \sum_{\substack{A \subseteq E \\ r(A)=|A|}} \prod_{e \in A} w_e$$

Bases Vamos considerar o seguintes limites:

$$\lim_{\lambda \rightarrow 0} \lambda^{-r(E)} \mathbf{G}_M(\lambda \mathbf{v})$$

$$\lim_{\lambda \rightarrow \infty} \lambda^{-r(E)} \mathbf{I}_M(\lambda \mathbf{w})$$

O primeiro vai selecionar, dentre os conjuntos A tais que $r(A) = r(E)$, aquele que $|A| = r(E) = r(A)$, *id est*, os geradores independentes.

O segundo seleciona, dentre os que $|A| = r(A)$, aqueles em que $r(A) = |A| = r(E)$, ou seja, os independentes geradores.

Em ambos os casos, estamos falando das bases da matróide, e portanto definimos:

$$\mathbf{B}_M(\mathbf{v}) = \lim_{\lambda \rightarrow 0} \lambda^{-r(E)} \mathbf{G}_M(\lambda \mathbf{v}) = \lim_{\lambda \rightarrow \infty} \lambda^{-r(E)} \mathbf{I}_M(\lambda \mathbf{w}) = \sum_{\substack{A \subseteq E \\ r(A)=r(E) \\ |A|=r(A)}} \prod_{e \in A} v_e$$

Relação com grafos Os três polinômios apresentados acima são exatamente iguais ao caso gráfico. Em outras palavras:

Proposição 5.5.

- (1) $\mathbf{G}_M(G)(\mathbf{v}) = \text{SGM}_G(\mathbf{v})$
- (2) $\mathbf{I}_M(G)(\mathbf{w}) = \text{FG}_G(\mathbf{w})$
- (3) $\mathbf{B}_M(G)(\mathbf{v}) = \text{FGM}_G(\mathbf{v})$

Demonstração. Basta observar que as somas em cada polinômio são efetuadas exatamente sobre os mesmos conjuntos. ■

5.4.5 Arestas em paralelo e em série

O conceito de arestas em paralelo e arestas em série aparece naturalmente em Teoria de Matróides.

Definição 5.3. Dizemos que duas arestas e e f estão em *paralelo* se:

$$r(e) = r(f) = r(e, f) = 1$$

Ou seja, se elas são um circuito.

Dizemos que estão em *série* se elas estão em paralelo na matróide dual, ou seja, se são um cocircuito.

Lema 5.1.

(P) Para qualquer conjunto $A \subset E$, teremos que se e e f são um circuito, então:

$$r(A \cup e) = r(A \cup f) = r(A \cup e \cup f)$$

(S) Para qualquer conjunto $A \subset E \setminus \{e, f\}$, teremos que se e e f são um cocircuito, então:

$$r(A \cup e) = r(A \cup f) = r(A) + 1$$

Demonstração.

(P) Pelo terceiro axioma da função posto, teremos:

$$r(\{A \cup e\} \cup \{e, f\}) + r(\{A \cup e\} \cap \{e, f\}) \leq r(A \cup e) + r(e, f)$$

Ou seja:

$$r(A \cup e \cup f) + 1 \leq r(A \cup e) + 1$$

A desigualdade no sentido oposto vale trivialmente, daí temos a igualdade, e por simetria também para $r(A \cup f)$.

(S) Seja \tilde{A} o complementar de A em $E \setminus \{e, f\}$. Então:

$$r^*(\tilde{A} \cup e \cup f) = |\tilde{A}| + 2 + r(A) - r(E) \quad \text{e} \quad r^*(\tilde{A} \cup f) = |\tilde{A}| + 1 + r(A \cup e) - r(E)$$

Suponha, para efeito de contradição, que $r(A \cup e) = r(A)$. Então:

$$r^*(\tilde{A} \cup e \cup f) = r^*(\tilde{A} \cup f) + 1$$

Contradição pelo item anterior, já que e e f estão em paralelo na matróide dual. ■

Proposição 5.6 (Paralelo (P)). Seja M matróide, e e f em paralelo. Então o polinômio de Tutte em várias variáveis de M , com pesos v_e e v_f para as arestas em questão, coincide com o de $M \setminus f$ se mudarmos o peso de e para $v_e + v_f + v_e v_f$. A tese também vale se supusermos que e e f são ambos laços.

Demonstração. Particionamos o conjunto das partes de E entre os conjuntos A que não contém e nem f , os $A_e = A \cup e$, os $A_f = A \cup f$ e os $A_{ef} = A \cup e \cup f$. Então, obviamente:

$$\begin{aligned} Z_M(q, \mathbf{v}) &= \sum_{A \subset E \setminus \{e, f\}} \left(q^{-r(A)} \prod_{d \in A} v_d \right) + \sum_{A \subset E \setminus \{e, f\}} \left(q^{-r(A_e)} \prod_{d \in A_e} v_d \right) + \\ &+ \sum_{A \subset E \setminus \{e, f\}} \left(q^{-r(A_f)} \prod_{d \in A_f} v_d \right) + \sum_{A \subset E \setminus \{e, f\}} \left(q^{-r(A_{ef})} \prod_{d \in A_{ef}} v_d \right) = \\ &= \sum_{A \subset E \setminus \{e, f\}} \left(q^{-r(A)} \prod_{d \in A} v_d \right) + v_e \sum_{A \subset E \setminus \{e, f\}} \left(q^{-r(A_e)} \prod_{d \in A} v_d \right) + \\ &+ v_f \sum_{A \subset E \setminus \{e, f\}} \left(q^{-r(A_e)} \prod_{d \in A} v_d \right) + v_e v_f \sum_{A \subset E \setminus \{e, f\}} \left(q^{-r(A_e)} \prod_{d \in A} v_d \right) \end{aligned}$$

pois $r(A \cup e) = r(A \cup f) = r(A \cup e \cup f)$ (se forem laços, é óbvio. Se forem um circuito, usamos a parte (P) do lema). Mas então:

$$Z_M(q, \mathbf{v}) = \sum_{A \subset E \setminus \{e, f\}} \left(q^{-r(A)} \prod_{d \in A} v_d \right) + (v_e + v_f + v_e v_f) \sum_{A \subset E \setminus \{e, f\}} \left(q^{-r(A_e)} \prod_{d \in A} v_d \right)$$

onde os postos são na matróide $M \setminus f$, o que não faz diferença. ■

Denotaremos a tese desta proposição pela seguinte expressão:

$$Z_M(q, \mathbf{v}_{\neq e, f}, v_e, v_f) = Z_{M \setminus f}(q, \mathbf{v}_{\neq e, f}, v_e + v_f + v_e v_f)$$

Proposição 5.7 (Série (S)). Seja M matróide, e e f em série. Então o polinômio de Tutte em várias variáveis de M , com pesos v_e e v_f para as arestas em questão, coincide com o de M/f se o multiplicarmos por $\frac{q + v_e + v_f}{q}$ e se mudarmos o peso de e para $\frac{v_e v_f}{q + v_e + v_f}$. A tese também vale se e ou f (ou ambos) for(em) colaço(s).

Demonstração. Consideramos novamente a partição do conjunto das partes de E entre os conjuntos A , os A_e , os A_f e os A_{ef} . Teremos então, procedendo como antes:

$$\begin{aligned} Z_M(q, \mathbf{v}) &= \sum_{A \subset E \setminus \{e, f\}} \left(q^{-r(A)} \prod_{d \in A} v_d \right) + v_e \sum_{A \subset E \setminus \{e, f\}} \left(q^{-r(A)-1} \prod_{d \in A} v_d \right) + \\ &+ v_f \sum_{A \subset E \setminus \{e, f\}} \left(q^{-r(A_f)} \prod_{d \in A} v_d \right) + v_e v_f \sum_{A \subset E \setminus \{e, f\}} \left(q^{-r(A_{ef})} \prod_{d \in A} v_d \right) \end{aligned}$$

pois $r(A \cup e) = r(A) + 1$ (se e for um colaço, é óbvio. Se $\{e, f\}$ forem um cocircuito, usamos a parte (S) do lema). Agora vamos pensar na matróide M/f . Lembramos então neste caso que,

$r_{M/f}(C) = r_M(C \cup f) - 1$, desde que f não seja laço. Então:

$$\begin{aligned} Z_M(q, \mathbf{v}) &= \sum_{A \subset E \setminus \{e, f\}} \left(q^{-r(A)} \prod_{d \in A} v_d \right) + v_e \sum_{A \subset E \setminus \{e, f\}} \left(q^{-r(A)-1} \prod_{d \in A} v_d \right) + \\ &+ v_f \sum_{A \subset E \setminus \{e, f\}} \left(q^{-r(A)-1} \prod_{d \in A} v_d \right) + \frac{v_e v_f}{q} \sum_{A \subset E \setminus \{e, f\}} \left(q^{-r(A_e)-1} \prod_{d \in A} v_d \right) = \\ &= \left(1 + \frac{v_e}{q} + \frac{v_f}{q} \right) \sum_{A \subset E \setminus \{e, f\}} \left(q^{-r(A)} \prod_{d \in A} v_d \right) + \frac{v_e v_f}{q} \sum_{A \subset E \setminus \{e, f\}} \left(q^{-r(A_e)} \prod_{d \in A} v_d \right) \end{aligned}$$

concluindo. ■

Denotaremos a tese desta proposição pela seguinte expressão:

$$Z_M(q, \mathbf{v}_{\neq e, f}, v_e, v_f) = \frac{q + v_e + v_f}{q} Z_{M/f} \left(q, \mathbf{v}_{\neq e, f}, \frac{v_e v_f}{q + v_e + v_f} \right)$$

Corolário 5.7.3. No caso gráfico:

(P) Mesma relação da Proposição 5.6

(S) Considerando o enunciado da Proposição 5.7, multiplicamos o polinômio inteiro por $q + v_e + v_f$, e não por $\frac{q + v_e + v_f}{q}$.

Demonstração. No caso em paralelo, como G e $G \setminus f$ tem mesmo número de vértices, multiplicaremos ambos os lados por $q^{|V|}$, e a igualdade permanece. No caso em série, como G/f tem um vértice a menos que G , ao multiplicarmos ambos os lados por $q^{|V|}$, teremos que cancelar o q no denominador para que fique $q^{|V|-1}$ no lado de $Z_{M/f}$. ■

Como aplicação desta subseção, vamos mostrar um teorema sobre o polinômio de confiabilidade em várias variáveis. Mas antes disso, uma seção sobre dualidade.

5.5 DUALIDADE

Nesta seção, vamos mostrar como o comportamento do polinômio de Tutte em várias variáveis é excelente no que diz respeito à dualidade, não somente quando olhamos para as matróides, mas também no que diz respeito aos grafos planares.

Proposição 5.8. Se M é matróide, $Z_M(q, \mathbf{v})$ seu polinômio de Tutte em várias variáveis, então:

$$Z_{M^*}(q, \mathbf{v}) = q^{r(E)} \prod_{e \in E} \frac{v_e}{q} Z_M \left(q, \frac{q}{\mathbf{v}} \right)$$

onde $q/\mathbf{v} = \{q/v_e\}_{e \in E}$

Demonstração. Denotaremos $E \setminus A = \bar{A}$. Lembramos a expressão que associa a função posto r da matróide com a função posto r^* da dual:

$$r^*(A) = |A| + r(\bar{A}) - r(E)$$

Então teremos que:

$$Z_{M^*}(q, \mathbf{v}) = \sum_{A \subseteq E} \left(q^{-r^*(A)} \prod_{e \in A} v_e \right) = \sum_{A \subseteq E} \left(q^{-|A| - r(\bar{A}) + r(E)} \prod_{e \in A} v_e \right)$$

Colocaremos $q^{r(E)}$ em evidência. E mais, observando que:

$$q^{-|A|} \prod_{e \in A} v_e = \prod_{e \in E} \frac{v_e}{q} \prod_{e \in \bar{A}} \frac{q}{v_e}$$

Teremos então:

$$Z_{M^*}(q, \mathbf{v}) = q^{r(E)} \sum_{A \subseteq E} \left(q^{-r(\bar{A})} \prod_{e \in E} \frac{v_e}{q} \prod_{e \in \bar{A}} \frac{q}{v_e} \right)$$

Mas podemos indexar a soma simplesmente em \bar{A} , e então não fará mais diferença se é o complementar ou não pois no fundo estaremos percorrendo todos os subconjuntos de A . Logo:

$$Z_{M^*}(q, \mathbf{v}) = q^{r(E)} \prod_{e \in E} \frac{v_e}{q} \sum_{A \subseteq E} \left(q^{-r(A)} \prod_{e \in A} \frac{q}{v_e} \right)$$

como queríamos. ■

Para falarmos de grafos planares, vamos precisar tomar um cuidado importante. Lembramos que para matróides, certamente é válido que:

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

Ocorre que esta relação não é válida em geral para grafos, como pode ser esclarecido pela Proposição 1.8. Sugerimos também que o leitor revise toda seção sobre dualidade em grafos, em particular a Proposição 1.9.

Corolário 5.7.4. Seja G um grafo planar qualquer. Então:

$$Z_{G^*}(q, \mathbf{v}) = q^{\kappa(G^*) - |V|} \prod_{e \in E} v_e Z_G \left(q, \frac{q}{\mathbf{v}} \right)$$

e também:

$$Z_G(q, \mathbf{v}) = q^{\kappa(G) - |V^*|} \prod_{e \in E} v_e Z_{G^*} \left(q, \frac{q}{\mathbf{v}} \right)$$

para qualquer G^* dual de G .

Demonstração. Temos por definição:

$$Z_{G^*}(q, \mathbf{v}) = q^{|V^*|} Z_{M(G^*)}(q, \mathbf{v})$$

Mas:

$$\begin{aligned} q^{|V^*|} Z_{M(G^*)}(q, \mathbf{v}) &= q^{|V^*|} Z_{M(G)^*}(q, \mathbf{v}) = q^{|V^*|} q^{r(E)} \prod_{e \in E} \frac{v_e}{q} Z_{M(G)}\left(q, \frac{q}{\mathbf{v}}\right) = \\ &= q^{|V^*|} q^{r(E)} \prod_{e \in E} \frac{v_e}{q} q^{-|V|} Z_G\left(q, \frac{q}{\mathbf{v}}\right) \end{aligned}$$

Mas $r(E) = |V| - \kappa(G)$, daí:

$$Z_{G^*}(q, \mathbf{v}) = q^{|V^*| - \kappa(G)} \prod_{e \in E} \frac{v_e}{q} Z_G\left(q, \frac{q}{\mathbf{v}}\right)$$

Donde concluiremos, ao observar a relação de Euler generalizada, Proposição 1.9:

$$|V| - |E| + |V^*| = \kappa(G^*) + \kappa(G) \Rightarrow |V^*| - \kappa(G) = \kappa(G^*) - |V| + |E|$$

Para ver a segunda parte, lembramos que na notação da Proposição 1.9, basta considerar H grafo planar conexo, e fazer $G = {}^*H$. A relação de Euler permanece, assim como o restante da argumentação. ■

Esta proposição nos diz que, olhando para o polinômio de Tutte para várias variáveis, todo grafo planar possui um dual verdadeiro!!¹ Por este motivo, a partir de agora, G^* representará qualquer grafo cuja operação de dualidade resulte em G , ou qualquer grafo obtido a partir de G por meio da operação de dualidade (na notação do capítulo 1, vamos identificar *G e G^* como os mesmos).

5.5.1 Dualidade em $q \rightarrow 0$

Vamos revisitar o tópico dos limites $q \rightarrow 0$ à luz da expressão para dualidade.

Proposição 5.9. Seja M matróide. Então:

$$(1) \mathbf{G}_{M^*}(\mathbf{v}) = \prod_{e \in E} v_e \mathbf{I}_M\left(\frac{1}{\mathbf{v}}\right)$$

$$(2) \mathbf{I}_{M^*}\left(\frac{\mathbf{v}}{q}\right) = \prod_{e \in E} \frac{v_e}{q} \mathbf{G}_M\left(\frac{q}{\mathbf{v}}\right)$$

$$(3) \mathbf{B}_{M^*}(\mathbf{v}) = \prod_{e \in E} v_e \mathbf{B}_M\left(\frac{1}{\mathbf{v}}\right)$$

A demonstração será direta.

¹Esse seria o caso em geral se na definição de dualidade para grafos planares, tivéssemos estipulado que o dual de um grafo desconexo seria a união disjunta dos duais das componentes conexas. Esta definição parece muito mais vantajosa para esta dissertação, contudo preferimos não ir de encontro à convenção.

Demonstração. Lembramos que:

$$\mathbf{G}_M(\mathbf{v}) = \lim_{q \rightarrow 0} q^{r(E)} Z_M(q, \mathbf{v})$$

$$\mathbf{I}_M\left(\frac{\mathbf{v}}{q}\right) = \lim_{q \rightarrow 0} Z_M(q, \mathbf{v})$$

$$\mathbf{B}_M(\mathbf{v}) = \lim_{\lambda \rightarrow 0} \lambda^{-r(E)} \mathbf{G}_M(\lambda \mathbf{v}) = \lim_{\lambda \rightarrow \infty} \lambda^{-r(E)} \mathbf{F}\mathbf{G}_G(\lambda \mathbf{v})$$

Para (1), teremos:

$$\begin{aligned} \mathbf{G}_{M^*}(\mathbf{v}) &= \lim_{q \rightarrow 0} q^{r^*(E)} Z_{M^*}(q, \mathbf{v}) = \lim_{q \rightarrow 0} q^{|E|-r(E)} q^{r(E)} \prod_{e \in E} \frac{v_e}{q} Z_M\left(q, \frac{q}{\mathbf{v}}\right) = \\ &= \prod_{e \in E} v_e \lim_{q \rightarrow 0} Z_M\left(q, \frac{q}{\mathbf{v}}\right) = \prod_{e \in E} v_e \mathbf{I}_M\left(\frac{1}{\mathbf{v}}\right) \end{aligned}$$

Para (2), teremos:

$$\mathbf{I}_{M^*}\left(\frac{\mathbf{v}}{q}\right) = \lim_{q \rightarrow 0} Z_{M^*}(q, \mathbf{v}) = \lim_{q \rightarrow 0} q^{r(E)} \prod_{e \in E} \frac{v_e}{q} Z_M\left(q, \frac{q}{\mathbf{v}}\right) = \prod_{e \in E} \frac{v_e}{q} \mathbf{G}_M\left(\frac{q}{\mathbf{v}}\right)$$

Para (3), finalmente:

$$\begin{aligned} \mathbf{B}_{M^*}(\mathbf{v}) &= \lim_{\lambda \rightarrow 0} \lambda^{-r^*(E)} \mathbf{G}_{M^*}(\lambda \mathbf{v}) = \lim_{\lambda \rightarrow 0} \lambda^{-|E|+r(E)} \prod_{e \in E} \lambda v_e \mathbf{I}_M\left(\frac{1}{\lambda \mathbf{v}}\right) \stackrel{\lambda=1/\mu}{=} \\ &= \lim_{\mu \rightarrow \infty} \mu^{-r(E)} \prod_{e \in E} v_e \mathbf{I}_M\left(\frac{\mu}{\mathbf{v}}\right) = \prod_{e \in E} v_e \mathbf{B}_M\left(\frac{1}{\mathbf{v}}\right) \end{aligned}$$

Proposição 5.10. Para grafos G planares, valem as seguintes relações:

$$(1) \quad \mathbf{S}\mathbf{G}\mathbf{M}\mathbf{C}_{G^*}(\mathbf{v}) = \prod_{e \in E} v_e \mathbf{F}\mathbf{G}_G\left(\frac{1}{\mathbf{v}}\right)$$

$$(2) \quad \mathbf{F}\mathbf{G}_{G^*}\left(\frac{\mathbf{v}}{q}\right) = \prod_{e \in E} \frac{v_e}{q} \mathbf{S}\mathbf{G}\mathbf{M}\mathbf{C}_G\left(\frac{q}{\mathbf{v}}\right)$$

$$(3) \quad \mathbf{F}\mathbf{G}\mathbf{M}_{G^*}(\mathbf{v}) = \prod_{e \in E} v_e \mathbf{F}\mathbf{G}\mathbf{M}_G\left(\frac{1}{\mathbf{v}}\right)$$

Demonstração. Imediato após a Proposição 5.5.

Na seção abaixo, falaremos apenas de grafos.

5.5.2 Dualidade no polinômio de fluxo - onde alguns tópicos de todo o texto são revisitados

Observando a fórmula para o polinômio de fluxo em várias variáveis obtida no Teorema 5.6:

$$\Phi_G(A, \mathbf{v}) = \Phi_G(q, \mathbf{v}) = q^{-|V|} \left(\prod_{e \in E} v_e \right) Z_G(q, q/\mathbf{v})$$

Vemos claramente que:

$$Z_{G^*}(q, \mathbf{v}) = q^{\kappa(G^*)} \Phi_G(A, \mathbf{v})$$

Lembramos ao leitor mais uma vez que o polinômio cromático é o polinômio dicromático avaliado em $v = -1$, ou o polinômio em várias variáveis avaliado com $v_e = -1$ para toda $e \in E$:

$$\chi_G(q) = Z_G(q, -1)$$

Lembramos também o comentário feito a partir da definição do polinômio de fluxo em várias variáveis: se $v_e = -1$ para toda aresta, então teremos exatamente o polinômio de fluxo introduzido no capítulo 2, aquele que conta os fluxos não nulos no grafo.

$$\varphi_G(q) = \Phi_G(q, -1)$$

Salta aos olhos, portanto, a profunda relação:²

$$\chi_{G^*}(q) = q^{\kappa(G^*)} \varphi_G(q)$$

Essencialmente, estamos vendo que os polinômio cromático e de fluxo são objetos duais. Desta igualdade, é corolário imediato o Teorema devido a Tutte 1954:

$$\chi(G^*) = \varphi(G)$$

Ou seja, o menor k tal que G^* possui uma k -coloração também é o menor k tal que G possui um k -fluxo (fluxo num grupo de ordem k). Observe ainda que $\tau_G(q) = \frac{\chi_G(q)}{q^{\kappa(G)}}$, ou seja:

$$\tau_{G^*}(q) = \varphi_G(q)$$

De fato, já tínhamos feito mais que isso no Teorema 3.6, mostrando que é possível identificar canonicamente um fluxo no grafo com uma tensão no dual.

5.6 O POLINÔMIO DE CONFIABILIDADE REVISITADO

Seja G um grafo. Suponhamos que cada aresta e tenha uma probabilidade p_e de ser removida após determinado momento, probabilidades estas consideradas de forma independente. Vamos denotar por $\mathbf{C}_G(\mathbf{p})$, $\mathbf{p} = \{p_e\}_{e \in E}$, a probabilidade do número de componentes conexas do grafo não aumentar. É uma medida de quão confiável uma rede pode ser, como já observáramos no capítulo 2. Agora, entretanto, seguiremos uma abordagem diferente. Claramente, teremos que:

$$\mathbf{C}_G(\mathbf{p}) = \sum_{\substack{A \subseteq E \\ \kappa(G_A) = \kappa(G)}} \prod_{e \in A} (1 - p_e) \prod_{e \in A} p_e$$

²Obviamente, esta relação já poderia ter aparecido muito antes, mas este pareceu o momento mais apropriado

É a soma das probabilidades de sobrar exatamente cada um dos subgrafos geradores maximalmente conexos.

Pelo fato deste polinômio destacar exatamente os subgrafos geradores maximalmente conexos, podemos reescrevê-lo usando SGMC_G , como introduzido anteriormente. De fato, teremos que essencialmente são a mesma coisa:

$$\mathbf{C}_G(\mathbf{p}) = \prod_{e \in E} p_e \text{SGMC}_G \left(\frac{1 - \mathbf{p}}{\mathbf{p}} \right)$$

$$\text{SGMC}_G(\mathbf{v}) = \prod_{e \in E} (v_e + 1) \mathbf{C}_G \left(\frac{1}{\mathbf{v} + 1} \right)$$

Apresentamos então um teorema devido a Sokal, como aplicação das considerações sobre arestas em paralelo e em série. Introduzimos antes uma definição:

Definição 5.4. Um grafo *série-paralelo* é um grafo obtido a partir de uma floresta por meio das seguintes operações:

Trocar aresta por par em paralelo.

Trocar aresta por par em série.

Teorema 5.8. Seja G um grafo série-paralelo sem laços e conexo. Se $|1 + v_e| < 1$ para toda aresta e , então $\text{SGMC}_G(\mathbf{v}) \neq 0$.

Demonstração. Vamos mostrar por indução. Se o grafo série-paralelo sem laços e conexo tem duas arestas, então:

Trata-se do 2-ciclo. O polinômio $\text{SGMC}_G(\mathbf{v})$ será:

$$\text{SGMC}_G(\mathbf{v}) = \sum_{\substack{ACE \\ \kappa(G_A) = \kappa(G)}} \prod_{e \in A} v_e = v_1 + v_2 + v_1 v_2 = (1 + v_1)(1 + v_2) - 1$$

Mas $(1 + v_1)(1 + v_2) - 1 = 0 \Leftrightarrow (1 + v_1)(1 + v_2) = 1$, claramente impossível.

Trata-se da 2-árvore. O polinômio $\text{SGMC}_G(\mathbf{v})$ será:

$$\text{SGMC}_G(\mathbf{v}) = \sum_{\substack{ACE \\ \kappa(G_A) = \kappa(G)}} \prod_{e \in A} v_e = v_1 v_2$$

Mas $v_1 v_2 = 0 \Leftrightarrow v_1 = 0$ ou $v_2 = 0$, o que não ocorre por hipótese.

Agora suponha que o resultado vale para qualquer grafo série-paralelo sem laços e conexo com $m - 1$ arestas. Seja G um grafo com m arestas. Tomamos as arestas e e f pareadas. Usaremos os resultados da Subseção 5.4.5.

Se estão em paralelo, então elas podem ser substituídas por uma aresta d com peso $1 + v_e + v_f + v_e v_f = (1 + v_e)(1 + v_f)$ sem alterar o polinômio de Tutte em várias variáveis. Mas este novo grafo satisfaz a hipótese de indução.

Se estão em série, chamamos atenção para o fato que o polinômio é considerado com $q \rightarrow 0$. Então substituímos as arestas e e f pela aresta d com peso $v_d = \frac{v_e v_f}{v_e + v_f}$ e multiplicamos o grafo inteiro por $v_e + v_f$. Primeiro note que $v_e + v_f < 0$. Agora note que:

$$v_d = \frac{v_e v_f}{v_e + v_f} \Leftrightarrow \frac{1}{v_d} = \frac{1}{v_e} + \frac{1}{v_f}$$

Observe também:

$$|1 + x| < 1 \Leftrightarrow -1 < 1 + x < 1 \Leftrightarrow -2 < x < 0 \Leftrightarrow \frac{-1}{2} > \frac{1}{x}$$

Daí teremos simplesmente que:

$$\frac{1}{v_d} = \frac{1}{v_e} + \frac{1}{v_f} < -1 < \frac{-1}{2}$$

Concluindo que $|1 + v_d| < 1$. Isto quer dizer que o novo grafo, obtido com d no lugar de e e f , satisfaz a hipótese indutiva. ■

Em termos do polinômio de confiabilidade, fazendo $\frac{1 - p_e}{p_e} = v_e \Leftrightarrow p_e = \frac{1}{v_e + 1}$ e olhando para a igualdade:

$$\mathbf{C}_G(\mathbf{p}) = \prod_{e \in E} \left(\frac{1}{v_e + 1} \right) \text{SGMC}_G(\mathbf{v})$$

Teremos que $|v_e + 1| < 1 \Rightarrow \mathbf{C}_G(\mathbf{p}) \neq 0$. Mas a condição $|v_e + 1| < 1$ é a mesma que:

$$\frac{1}{|p_e|} < 1 \text{ ou simplesmente } |p_e| > 1$$

Obviamente este resultado só faz sentido se deixarmos de pensar nos p_e s como probabilidades.

5.7 COMENTÁRIO FINAL

Já sobre este tema, a literatura é bem mais vasta, certamente pelo interesse físico envolvido. Boa parte desta literatura é sobre a localização das raízes, e um trabalho do próprio Sokal [Sok04], por exemplo, aborda este tema. Não há contudo, uma teoria completa ou tampouco um resultado fundamental sobre o tema. Acreditamos então que novamente estaríamos entrando em especificidades que estão fora do foco da presente dissertação.

CONSIDERAÇÕES FINAIS

CONCLUSÕES

O Polinômio de Tutte é uma ferramenta enumerativa extremamente poderosa, que pode ser usada em várias situações ao trabalharmos com grafos e matróides. O fato de possuir definições distintas nos fornece uma flexibilidade interessante para abordar problemas e para fazer avaliações do próprio polinômio em certos valores.

Consideramos que foi extremamente proveitoso observar a relação entre grafos, matrizes e matróides. Muitas vezes, um problema para uma estrutura expresso em um desses formatos pode se tornar bem mais simples ao olharmos no outro formato, seja por questões de notação, da presença de resultados auxiliares, ou até mesmo por facilidade na nossa intuição. O fato de que a *dualidade* é preservada quando alternamos entre essas diferentes abordagens foi muito importante para estabelecermos nossos resultados.

Ser capaz de capturar no Polinômio de Tutte as simetrias de um grafo é uma generalização importante. Apesar de esta ser uma teoria recente e ainda pouco desenvolvida, são promissoras as perspectivas de pensarmos no polinômio de Tutte como uma ferramenta para entendermos como certas estruturas definidas em um grafo se comportam na presença dos automorfismos dele.

Observamos também que muitas propriedades de grafos são conhecidas ao olharmos para certas matrizes associadas a ele, não somente a de incidência, mas também a de adjacência, o laplaciano, etc. Trata-se de um ramo bem estabelecido de Teoria Algébrica de Grafos. Tentar obter muitas propriedades a respeito de um grafo olhando para o polinômio de Tutte convencional esbarra no fato de que este polinômio não distingue uma aresta de outra (a não ser pontes e laços), mesmo que elas tenham papéis bem diferentes. Atribuir um peso para cada aresta é o caminho para codificarmos mais propriamente um grafo em um polinômio, e de fato, toda informação a respeito de um grafo relacionada ao número de vértices e à matróide gráfica associada estão contidas no polinômio de Tutte em várias variáveis. Este é essencialmente a função de partição do modelo de Potts com q estados.

Por fim, como o polinômio de Tutte e suas especializações guardam tantas informações a respeito do grafo ou de uma matróide, o seu cálculo é capaz de resolver inúmeros problemas em teoria dos grafos. Calcular o polinômio cromático é, observamos, suficiente para resolvermos o problema do cálculo do número cromático de um grafo - em particular será o menor inteiro positivo que não seja raiz deste polinômio. Obviamente, como este problema já é NP completo, o cálculo do polinômio de Tutte não pode ser menos fácil. As próprias definições que apresentamos já mostram por si só esta dificuldade: ou precisávamos desconstruir o grafo inteiro, ou considerar vários subconjuntos de arestas, ou as florestas geradoras.

DAQUI, PARA ONDE?

De fato não salta aos olhos uma maneira de generalizar ambos os polinômios numa mesma direção, o que pode ser observado em parte pela natureza absolutamente distinta de suas

variáveis, e em parte pela diferença conceitual na maneira como foram definidos. Contudo, acreditamos que isto pode ser um tema para uma pesquisa futura na área.

Também despertamos o interesse em considerar outros polinômios que aparecem em combinatória enumerativa, combinatória algébrica e topologia combinatória. Para citar: Polinômio de Jones, Polinômio de Entrelace, Polinômio de Transição e o Índice Cíclico de um Grupo e sua generalização proposta por Cameron, os dois últimos já mencionados no começo do capítulo 4. Em particular, poderemos investigar possíveis generalizações da Teoria de Polyá.

O próprio uso de matrizes nos motivou também a pesquisar mais a fundo o uso da álgebra de matrizes em combinatória, tema este extremamente vasto. Ser capaz de observar o polinômio de Tutte em várias variáveis e extrair dele informações do tipo que se obtém ao olharmos para os autovalores da matriz de adjacência pode ser um caminho interessante.

A discussão sobre complexidade nos levou a pesquisar o tema, por exemplo em Welsh [WM00]. Apesar de ser um tema interessante, não achamos que havia espaço nesta dissertação para ele. Por fim, observamos apenas que certamente se alguém pretende obter muitas informações a respeito de um grafo, calcular o polinômio de Tutte é uma boa estratégia.

REFERÊNCIAS BIBLIOGRÁFICAS

- [Aig07] Martin Aigner. *A Course in Enumeration*. Springer Verlag, New York, 2007.
- [BO92] T. Brylawski and J. Oxley. The Tutte polynomial and its applications. In N. White, editor, *Encyclopedia of Mathematics and its Applications*, volume 40, chapter Matroid Applications. Cambridge University Press, Cambridge, 1992.
- [Bol98] Béla Bollobás. *Modern Graph Theory*. Springer Verlag, New York, 1998.
- [CJR08] Peter Cameron, Bill Jackson, and Jason Rudd. Orbit-counting polynomials for graphs and codes. *Discrete Mathematics*, 308:920–930, 2008.
- [CK07] Peter Cameron and Koko Kayibi. Orbit chromatic and flow roots. *Combinatorics, Probability and Computing*, 16:401–407, 2007.
- [Die05] Richard Diestel. *Graph Theory*. Springer Verlag, New York, 2005.
- [EMM08] J. A. Ellis-Monaghan and C. Merino. Graph Polynomials and Their Applications i: The Tutte Polynomial. *arXiv:math*, 0803.3079v2, 2008.
- [Eve66] Howard Eves. *Elementary Matrix Theory*. Dover Publications, New York, 1966.
- [GR04] C. Godsil and G. Royle. *Algebraic Graph Theory*. Springer Verlag, New York, 2004.
- [Her75] Israel Nathan Herstein. *Topics in Algebra*. John Wiley & Sons, 1975.
- [HH70] B. Hartley and T. Hawkes. *Rings, Modules and Linear Algebra*. Chapman and Hall, 1970.
- [Jac03] Bill Jackson. Zeros of chromatic and flow polynomials of graphs. *Journal of Geometry*, 76:95–109, 2003.
- [Lan02] Serge Lang. *Algebra*. Springer Verlag, New York, 2002.
- [Lin81] Sóstenes Lins. *Princípios de Enumeração*. Instituto de Matemática Pura e Aplicada, 1981.
- [Mei08] John Meier. *Groups, Graphs and Trees*. Cambridge University Press, Cambridge, 2008.
- [Oxl92] James Oxley. *Matroid Theory*. Oxford University Press, Oxford, 1992.
- [Rud10] Jason Rudd. Tutte polynomials for counting and classifying orbits. *Discrete Mathematics*, 310:206–222, 2010.
- [Sok04] Alan Sokal. Bounds on the complex zeros of (di)chromatic polynomials and Potts-model partition functions. *Combinatorics, Probability and Computing*, 10:221–26141–77, 2004.

- [Sok05] Alan Sokal. The multivariate Tutte polynomial (alias Potts model) for graphs and matroids. In Bridget S. Webb, editor, *Surveys in Combinatorics*, pages 173–226. Cambridge University Press, 2005.
- [Tut54] William Tutte. A contribution to the theory of chromatic polynomials. *Canadian Journal of Mathematics*, 6:80–91, 1954.
- [Tut04] William Tutte. Graph-polynomial. *Advances in Applied Mathematics*, 32:5–9, 2004.
- [WM00] D. Welsh and C. Merino. The Potts model and the Tutte polynomial. *Journal of Mathematical Physics*, 41(3):1127–1152, 2000.

Este volume foi tipografado em L^AT_EX na classe UFPETthesis (www.cin.ufpe.br/~paguso/ufpethesis).
Para detalhes sobre este documento, clique [aqui](#).