

Bachelorarbeit

The Tutte Polynomial for Graphs and Matroids

Nelli Funk

22.02.2024

Betreuung:

Erstprüfer: Prof. Dr. André Uschmajew

Zweitprüfer: Prof. Dr. Dirk Hachenberger

Fakultät für Mathematik
Lehrstuhl Mathematical Data Science

Universität Augsburg

Contents

1	Introduction	4
2	Graphs	6
2.1	Preliminaries in Graph Theory	6
2.2	The Geometric Dual of a Planar Graph	9
2.3	The Deletion-Contraction Algorithm for Graphs	11
2.4	Graph Polynomials	14
2.4.1	Colorings and the Chromatic Polynomial	14
2.4.2	Flows and the Flow Polynomial	18
2.4.3	Network-Reliability and the Reliability Polynomial	22
3	Matroids	25
3.1	Preliminaries in Matroid Theory	25
3.2	The Dual Matroid	30
3.3	The Deletion-Contraction Algorithm for Matroids	33
3.4	The Tutte Polynomial for Matroids	38
3.5	The Tutte Polynomial as a Matroid Invariant	43
4	Graphs as Matroids	48
4.1	The Cycle Matroid	48
4.2	The Bond Matroid	51
4.3	The Tutte Polynomial for Graphs	53
4.4	The Tutte Polynomial as a Graph Invariant	57
5	Complexity and Applications	62
5.1	Computational Complexity of the Tutte Polynomial	62
5.2	Applications of the Tutte Polynomial	63
5.2.1	Knot Theory	64
5.2.2	Coding Theory	64

1 Introduction

Algebraic graph theory is a fascinating subject. It offers the pleasure of seeing many surprising and useful connections between two beautiful parts of mathematics: algebra and graph theory. We will see many of those throughout this thesis. We start in section 2.1 by defining a graph as a tuple of a vertex set and an edge set, where an edge is a connection between two vertices. In section 2.2 we will define the geometric dual of a graph before we introduce the deletion-contraction algorithm in section 2.3. This algorithm uses recursive formulas to compute several graph invariants, such as the number of spanning trees or the number of acyclic orientations. The recursive formulas hold for the actions of deleting or contracting an edge, depending on its kind. We differentiate between loops, bridges and ordinary edges. But it is also possible to compute several graph polynomials with this algorithm. We will introduce the *chromatic polynomial*, the *flow polynomial* and the *reliability polynomial*.

The chromatic polynomial was introduced by George Birkhoff who aimed to prove the four color conjecture (now theorem). In general we will consider vertex colorings of a graph, where no two connected vertices have the same color. The chromatic polynomial takes the number of colors as an input and returns the number of different vertex colorings of such kind. The flow polynomial counts the number of nowhere-zero A -flows for a graph with an orientation and an additive abelian group A with order k . Hence it takes the order of the group as an input and returns the number of nowhere-zero flows. For the reliability polynomial we consider a graph as a network and delete each edge with some probability $(1 - p)$. The reliability polynomial takes p as an input and returns the probability that the network survives.

Thomas William Tutte [Tut47] was motivated by the first two polynomials to find a universal polynomial in such way, that any graph polynomial that satisfies some deletion-contraction recursion is in fact a specialization of the universal polynomial. He named it the *dichromate*, nowadays it is known as the *Tutte polynomial* in his honor. Before defining this two variable polynomial on graphs, we want to define it on a more general construction called matroid.

Chapter 3 is dedicated to give a short introduction into matroids, where we follow the same concept as for graphs in chapter 2. We start by defining a matroid through its ground set and its collection of independent sets. We then define the deletion and contraction action of subsets of matroids and use it to define the rank function of a matroid. We can also define a rank function on the dual of a matroid. These two rank functions are important for the definition of the Tutte polynomial on matroids. We will show that the Tutte polynomial satisfies some recursive deletion-contraction algorithm before we prove the recipe theorem from Dominic James Welsh [Wel99]. This theorem states that any matroid polynomial that satisfies a recursive deletion-contraction relation on ordinary edges and is multiplicative on direct sums, is in fact a specialization of the Tutte Polynomial for matroids.

We will discuss how a graph can always be expressed as a matroid, but not every matroid can be expressed as a graph. The matroid for a graph $G = (V, E)$ has groundset E . We can compute the incidence matrix belonging to G and consider the columns of the matrix as vectors in a vector space. The collection of independent

sets for the matroid are the sets of edges whose corresponding vectors are linear independent. Hence the Tutte Polynomial can be defined on graphs. When proving that the graph polynomials from chapter 2 are specializations of the Tutte Polynomial, a particular problem arises. The recipe theorem can not be applied the way it was stated. Because there are two graph constructions that correspond to the direct sum of matroids, the one point join and the distinct union of graphs. Also when we construct a matroid for some graph, we loose a lot of information about the vertices of the graph. For example, isolated vertices are no longer observed. But this information is quite important for many graph polynomials. In section 4.4 we prove a recipe theorem for graph polynomials, that fixes this problem.

The last chapter scratches the surface of complexity of the Tutte polynomial and its applications. In fact Francois Jaeger, Dominic Vertigan and Dominic Welsh proved in their paper "On the computational complexity of the Jones and Tutte polynomials" [JWV90] that the problem of evaluating the Tutte Polynomial at a point in the (x, y) -plane is $\#P$ hard, except at the hyperbola $(x - 1)(y - 1) = 1$ and for 8 specific points in the plane. We will also discuss what graph invariant needs to be bounded such that this problem is in P . We finish the thesis with connections between topological knot theory and the Tutte polynomial and coding theory and the Tutte polynomial. A more detailed overview of all applications of the Tutte Polynomial surely gives "The Handbook of the Tutte Polynomial and Related Topics" edited by Joanna Ellis-Monaghan and Ian Moffatt [EMM22]. The interested reader may also find an overview of approximation results for the Tutte Polynomial in [EMM22].

2 Graphs

Even though graph theory is a very interesting part of mathematics, it is not part of the undergraduate studies of every mathematician. Thus we are going to introduce in Section 2.1 the definitions used throughout this thesis in as little detail as needed. We mostly follow [GR01]. We introduce the notions of *spanning forests*, *bridges* and *loops* with regard to the definition of *bases*, *coloops* and *loops* for matroids in Chapter 3 and Chapter 4. In section 2.2 we will discuss *planar graphs* and explain the construction of the *geometric dual* of a planar graph. We also define the operations of *deleting* and *contracting* an edge in Section 2.1, so that we can define the *deletion-contraction algorithm* in Section 2.3. We use the deletion-contraction algorithm to compute the number of *spanning trees* and the number of *acyclic orientations* of a graph. Moreover, this algorithm can also be used to compute specific *graph polynomials* belonging to a graph. In this thesis, we focus on the *chromatic polynomial*, the *flow polynomial* and the *reliability polynomial*. Subsections 2.4.1 - 2.4.3 give a detailed introduction into each problem statement and show how each polynomial can be computed using the algorithm. We illustrate with different small examples throughout Section 2.4.

2.1 Preliminaries in Graph Theory

This section focuses on the introduction into graph theory. We start by defining a *graph* through an ordered tuple of *vertices* and *edges* and characterize relationships between those. The goal of this chapter is to get the reader familiarized with graphs and different graph theoretic definitions. To achieve this, we give different figurative examples.

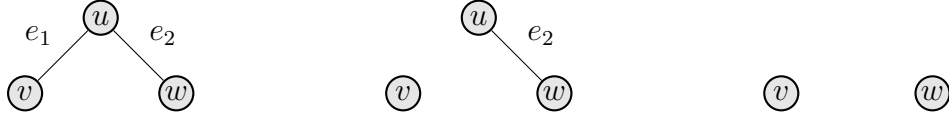
Definition 2.1. A *graph* $G = (V(G), E(G))$ consists of a *vertex set* $V(G)$ and an *edge set* $E(G)$, where an edge $e \in E(G)$ is an unordered pair $e = (u, v)$ of, not necessarily distinct, vertices $u, v \in V(G)$. We call u and v the *end-vertices* of e . We call two edges e_1, e_2 *multiple* or *parallel*, if the end-vertices of e_1 are also the end-vertices of e_2 .

We will usually use V, E for the vertex- and edgeset if the graph follows from the context.

Definition 2.2. If $e = (u, v) \in E$, then u and v are called *adjacent* or *neighbours* and u and v are called *incident* to the edge e . Two edges e_1, e_2 are called *incident* if e_1 is incident to an end-vertex of e_2 .

Definition 2.3. Let $G = (V, E)$ be a graph and $e \in E$ an edge. Then the graph $G - e = (V, E - e)$ is obtained by deleting the edge e from E . Let $v \in V$ be a vertex, then the graph $G - v = (V - v, \tilde{E})$ with $\tilde{E} = \{e \in E \mid e \text{ not incident to } v\}$ is obtained by deleting v and all edges incident to v .

Example 2.4. One way to represent graphs are diagrams. Consider the graph $G = (V, E)$ with $V = \{u, v, w\}$ and $E = \{e_1 = (u, v), e_2 = (u, w)\}$. Figure 1 shows one representation of the graphs G , $G - e_1$ and $G - u$.

Figure 1: Representation of the graphs G , $G - e_1$ and $G - u$.

Definition 2.5. A graph G is called *complete* if there exists an edge $e = (u, v) \in E(G)$ for every distinct pair $u, v \in V(G)$. For some $n \in \mathbb{N}$, we denote the complete graph on n vertices by K_n . A graph with at least one vertex but no edges is called *empty*. We call a graph G *bipartite*, if there exists a bipartition A, B of the vertexset, such the vertices in A, B respectively, are pairwise non-adjacent. We denote such graphs by $K_{|A|,|B|}$.

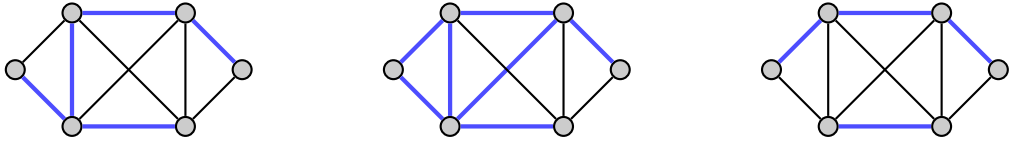
Definition 2.6. Let G be a graph, we call H a *subgraph* of G if

$$V(H) \subseteq V(G), \quad E(H) \subseteq E(G).$$

If $V(H) = V(G)$, we call H a *spanning subgraph* of G . We call H an *induced subgraph* of G if the following holds for all vertices $u, v \in V(H)$:

$$(u, v) \in E(H) \iff (u, v) \in E(G).$$

Example 2.7. The following figure shows some spanning subgraphs of a graph G .

Figure 2: Three spanning subgraphs (in blue) of G .

The graph has the complete graphs K_3 and K_4 as induced subgraphs.

Figure 3: K_3 and K_4 (in blue) as induced subgraphs.

Definition 2.8. Let G be a graph and consider a sequence $W = v_0 e_1 v_1 \dots v_{k-1} e_k v_k$ of vertices and edges $e_i \in E$ such that $e_i = (v_{i-1}, v_i)$ for each i . This sequence is called a $v_0 v_k$ -*walk*. If W is a sequence of distinct vertices and edges, we call W a *path*. If W is a sequence of distinct vertices and edges, except $v_0 = v_k$, we call W a *cycle*. A graph that doesn't contain any cycles is called *acyclic*.

Definition 2.9. A graph G is called *connected* if it contains a path between any two vertices, otherwise it is *disconnected*. An induced and connected subgraph H , where for every $v \in V(H)$ there does not exist a path to any $u \notin V(H)$, is called a *connected component*. The *number of connected components* of a graph H is denoted by $c(H)$ and often referred to as the *number of components*.

Definition 2.10. An acyclic graph is called a *forest*. If it is also connected, it is called a *tree*. A spanning subgraph that is acyclic and connected is called a *spanning tree*.

Theorem 2.11. Let $G = (V(G), E(G))$ be a connected graph. Then

$$|E(G)| = |V(G)| - 1$$

holds if and only if G is a tree.

Proof. Let G be an arbitrary connected graph on n vertices and $m = n - 1$ edges. For a graph on n vertices to be connected, it has to have at least $n - 1$ edges. Hence deleting an edge will result in a disconnected graph, such that G is acyclic, thus a tree.

Now let G be a tree. We are going to use induction on the number of vertices. First let $V(G) = 1$. Then for G to be a tree it needs $m = 0 = 1 - 1$ edges. Now suppose the statement holds for any tree on n vertices and consider a graph G with $V(G) = n + 1$. Deleting any edge from G will result in a disconnected graph with connected components G_1 and G_2 which are acyclic because G was acyclic. Therefore G_1 and G_2 are trees. Since $V(G_1) \leq n$ and $V(G_2) \leq n$ the induction hypothesis holds for these trees and we get $E(G_1) = V(G_1) - 1$, $E(G_2) = V(G_2) - 1$. But from $E(G) = E(G_1) + E(G_2) + 1$ it follows that

$$E(G) = V(G_1) + V(G_2) - 1 = V(G) - 1. \quad \square$$

Definition 2.12. Let G be a graph. An edge $e = (v, v)$ from a vertex v to itself is called a *loop*. If for some edge f we have $c(G) < c(G - f)$, then f is called a *bridge*. An edge that is neither a loop nor a bridge is called *ordinary*.

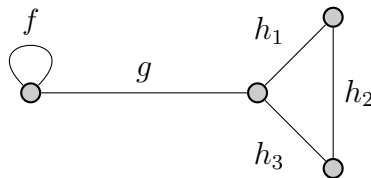


Figure 4: Graph with loop f , bridge g and ordinary edges h_1, h_2, h_3 .

Two representations of a graph can look very differently. Therefore we need to quantify if two representations come from the same graph.

Definition 2.13. Two graphs G, H are called *isomorphic*, if there exists a bijection

$$\varphi : V(G) \rightarrow V(H)$$

such that $(x, y) \in E(G)$ if and only if $(\varphi(x), \varphi(y)) \in E(H)$. We call φ an *isomorphism* from G to H , and write $G \cong H$ if such a φ exists.

Example 2.14. Figure 5 shows the graphs G and H , whose chosen representations look quite different, but G and H are actually isomorphic.

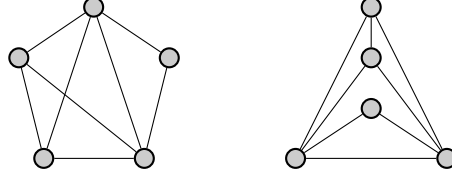


Figure 5: Two isomorphic graphs on five vertices.

2.2 The Geometric Dual of a Planar Graph

So far we have been using the convenient representation of graphs through diagrams, where vertices are represented by points and edges by lines or curves. Now we are interested in drawing graphs in such a way, that no two edges intersect. Such a drawing is not always possible in the plane. If there exists such a drawing, the graph is called *planar*. We will look at planar graphs following the definitions in chapter 4 of [GR01]. We are then going to give a detailed description of the construction of a dual graph. The concept of duality plays an important role in defining the Tutte Polynomial in Section 3.4. Later we are going to generalize duality to arbitrary graphs, when we introduce the dual to the cycle matroid in Section 4.2.

To define planar graphs, we need to formalize the process of drawing a graph on the plane. To do this, we recall that a *Jordan curve* in the plane is a continuous curve which does not intersect itself.

Definition 2.15. Consider a function $\vartheta : V \rightarrow \mathbb{R}^2$ that maps each vertex v of a graph G to a distinct point $\vartheta(v)$ of the plane and each edge e of G to a Jordan curve γ_e mapping $[0, 1]$ to the plane joining its endpoints. Thus for an edge $e = (u, v)$, the corresponding curve satisfies $\gamma_e(0) = \vartheta(u)$ and $\gamma_e(1) = \vartheta(v)$. We call such a function a *planar embedding* if the following two conditions are satisfied

- i) for two nonincident edges e_1 and e_2 and their corresponding curves $\gamma_{e_1}, \gamma_{e_2}$:

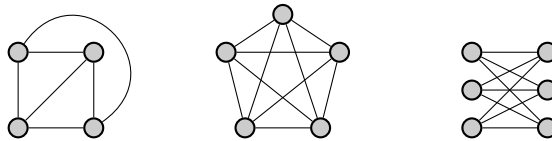
$$\gamma_{e_1}(x) \neq \gamma_{e_2}(y) \quad \forall x, y \in [0, 1].$$

- ii) for two incident edges $f_1 = (u, v)$ and $f_2 = (v, w)$ and their corresponding curves $\gamma_{f_1}, \gamma_{f_2}$:

$$\gamma_{f_1}(1) = \gamma_{f_2}(0) \text{ and } \gamma_{f_1}(x) \neq \gamma_{f_2}(y) \quad \forall x \in [0, 1[\text{ and } \forall y \in]0, 1].$$

Definition 2.16. A graph is called *planar* if it has a planar embedding. We call a planar graph together with its planar embedding a *plane graph*.

Example 2.17. The complete graph on 4 vertices K_4 is planar, Figure 5 shows a planar embedding of K_4 and two nonplanar graphs.

Figure 6: The plane graph K_4 and the nonplanar graphs K_5 and $K_{3,3}$.

The graphs K_5 and $K_{3,3}$ are quite interesting for the studies of planar graphs. There is a well-known theorem due to Kuratowski, which states that a graph is planar if and only if it does not contain K_5 or $K_{3,3}$ as subgraphs. More discussions on this can be found in [Wel76].

To be able to construct the geometric dual of a plane graph, we need to define the area in the plane enclosed by the edges of the plane graph. The edges of a planar graph together with a fixed embedding divide the plane into regions, which we call the *faces* of the graph. For a given connected graph G , we can now construct a new graph. Firstly, the vertices of the new graph correspond to the faces of G , where each vertex is being placed in the planar embedding of the corresponding face. Secondly, every edge e of G gives rise to an edge of the new graph connecting the two faces of G , whose boundaries both contain e .

Definition 2.18. Let G and H be two graphs, their *disjoint union* is denoted by $G \sqcup H$ with vertex set $V(G \sqcup H) = V(G) \sqcup V(H)$ and edge set $E(G \sqcup H) = E(G) \sqcup E(H)$.

If G is disconnected and has connected components G_1, \dots, G_k , then G^* is the disjoint union of the dual graphs for each connected component: $G^* = G_1^* \sqcup \dots \sqcup G_k^*$.

Definition 2.19. We call the resulting graph from this construction the dual graph and denote it by G^* .

We are going to use the following example to describe the construction of a dual graph.

Example 2.20. Let us consider the following graph:

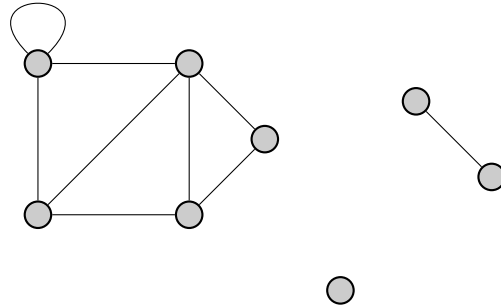
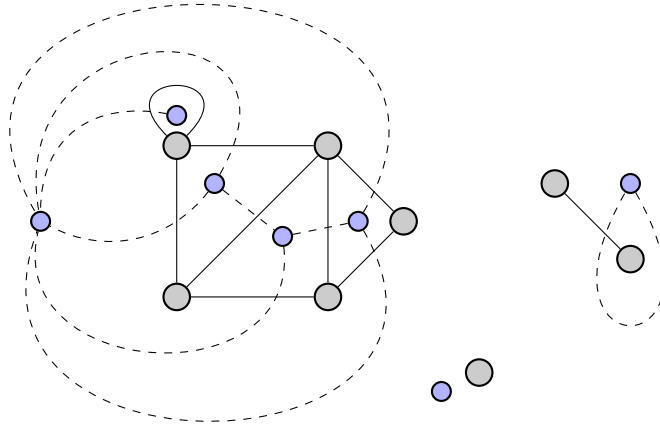


Figure 7: Graph G .

To construct the dual graph G^* of G , place a blue vertex on each face of G and connect each of them with a dashed edge \hat{e} , whenever the corresponding faces touch the same edge e of G . We say the edges $\hat{e} \in G^*$ and $e \in G$ are corresponding. This results in the graph shown in Figure 8.

Figure 8: Graph G with dual graph G^* .

In the previous example, the constructed dual graph is a planar graph. Indeed, the geometric dual of any plane graph is planar again. Moreover, constructing the dual graph G^{**} of some dual graph G^* will result in G again. For a detailed discussion on these concepts see [Oxl11].

2.3 The Deletion-Contraction Algorithm for Graphs

In this section we will consider graph invariants which can be computed through a recursive algorithm, called the *deletion-contraction algorithm*. The delete operation is defined in Definition 2.3. We start by defining the operation of contraction of an edge $e \in G$. We are going to follow the results from chapter 15 of [GR01].

Definition 2.21. A *graph invariant* is a function f on a specified class of graphs such that for all G and H in the class the following holds:

$$G \cong H \implies f(G) = f(H).$$

A graph invariant whose image lies in some polynomial ring is called a *graph polynomial*.

Definition 2.22. Let G be a graph and for $e = (u, v) \in E(G)$ consider the set

$$E_1 := \{(x, y) \mid y \text{ is adjacent to } u\} \cup \{(x, y) \mid y \text{ is adjacent to } v\}.$$

We construct

$$G/e = ((V(G) - \{u, v\}) \cup \{x\}, \hat{E}),$$

with

$$\hat{E} = (E - \{e \in E \mid e \text{ incident to } u \text{ or } v\}) \cup E_1,$$

by deleting the edge e from the edgeset and identifying the vertices u, v as the vertex x . We say G/e is obtained by *contracting* e .

It is possible that the contracting action results in G having loops or multiple edges, which is illustrated in Figure 9. For the computation of the number of spanning trees or the number of acyclic orientations for example, these can not just be ignored.

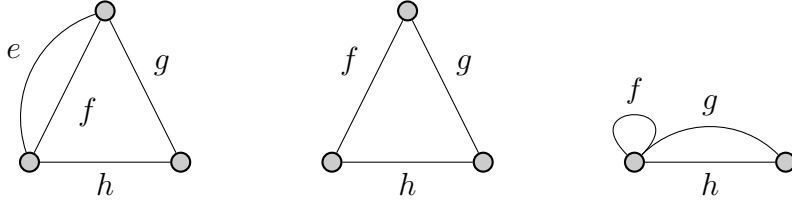


Figure 9: Graph G , deletion $G - e$, and contraction G/e .

The operations of deleting and contracting edges are dual to each other, which the following theorem illustrates.

Theorem 2.23. *Let G be a plane graph and $e \in E(G)$ an ordinary edge. Let G^* be the geometric dual of G and denote by \hat{e} the edge in G^* corresponding to e . Then*

$$(G - e)^* = G^* / \hat{e} \quad \text{and} \quad (G/e)^* = G^* - \hat{e}.$$

Proof. Let $e = (u, v) \in G$ and $\hat{e} = (x, y) \in G^*$ be the corresponding edge in the dual graph induced by e . Firstly, the connected component of $G - e$ containing e has exactly one face less than G , hence the corresponding connected component of $(G - e)^*$ has one vertex less than G^* . The missing vertex was incident to the corresponding edge \hat{e} , so without loss of generality $x \notin V((G - e)^*)$. Since $e \notin G - e$, the corresponding edge \hat{e} is missing in the corresponding connected component of $(G - e)^*$. Deleting e from G does not change the other faces of the planar embedding or the edges of G . Thus, the only differences are the missing vertex x and edge \hat{e} , so that $(G - e)^* = G^* / \hat{e}$ holds.

Now for the other equality we consider again $e = (u, v) \in G$ and $\hat{e} = (x, y) \in G^*$. The action of contracting e will result in the same number of faces, but one edge less. Hence the dual graph $(G/e)^*$ has the same number of vertices as G^* , but the corresponding edge \hat{e} is missing, so that $(G/e)^* = G^* - \hat{e}$ holds. \square

Definition 2.24. Let G and H be graphs. We call H a *minor* of G if it results from deleting edges, deleting vertices, or contracting edges of G . We call a class \mathcal{G} of graphs *minor-closed* if, whenever G is in \mathcal{G} , then every minor of G is also in \mathcal{G} .

Definition 2.25. Let \mathcal{G} be a minor-closed class of graphs and

$$f : \mathcal{G} \rightarrow \mathbb{R}, G \mapsto f(G)$$

a function. We call a recursive algorithm for f a *deletion-contraction algorithm* if there are numbers $a_1, a_2, a_3, b_1, b_2, b_3, c \in \mathbb{R}$, such that the following equality holds for every edge $e \in E$.

$$f(G) = \begin{cases} a_1 f(G - e) + b_1 f(G/e), & \text{if } e \text{ is a loop;} \\ a_2 f(G - e) + b_2 f(G/e), & \text{if } e \text{ is a bridge;} \\ a_3 f(G - e) + b_3 f(G/e), & \text{if } e \text{ is ordinary;} \\ c, & \text{if } E(G) = \emptyset. \end{cases}$$

One example of a graph parameter, which can be computed through a deletion-contraction algorithm is the number of spanning trees of a graph G .

Theorem 2.26. *Let $\tau(G)$ denote the number of spanning trees of a graph G , then*

$$\tau(G) = \begin{cases} \tau(G - e), & \text{if } e \text{ is a loop;} \\ \tau(G/e), & \text{if } e \text{ is a bridge;} \\ \tau(G - e) + \tau(G/e), & \text{otherwise.} \end{cases}$$

Proof. Let G be a graph, $e \in E(G)$. First, if e is a loop in G , then no spanning tree T of G contains e , thus we can delete e and the spanning trees of $G - e$ are exactly the ones of G . Now, if e is not a loop, then every spanning tree T either contains e or not, thus we can count them according to this distinction. The spanning trees that do not contain e are exactly the spanning trees of $G - e$. Moreover if $e \in T$, then the trees T/e are exactly the spanning trees of G/e . Therefore,

$$\tau(G) = \tau(G - e) + \tau(G/e)$$

However, if e is a bridge in G , then $\tau(G - e) = 0$, since the graph $G - e$ is not connected, leaving us with $\tau(G) = \tau(G/e)$. \square

This in fact yields a recursive algorithm, since $G - e$ and G/e are smaller graphs than G compared to their number of edges, by applying these equations until there are only trees left. Deletion-contraction algorithms play a quite important role in the study of graph parameters. We now want to introduce another graph parameter that can be computed with such an algorithm.

Definition 2.27. We call a graph $G = (V, E)$ a *directed graph* if E is the set of ordered pairs of vertices. Each edge $e \in E$ is directed by the order (head, tail) of its end-vertices, we write head \rightarrow tail. An *orientation* ω is an assignment of a direction to each edge $e = (u, v) \in E$, either $u \xrightarrow{\omega} v$ or $u \xleftarrow{\omega} v$. We denote G^ω for a graph G with a fixed orientation ω .

Definition 2.28. For a directed graph G , we call a walk a *directed walk*, if consecutive edges $e = (u, v), f = (v, w)$ are directed as $u \rightarrow v, v \rightarrow w$. A cycle that is directed in this way, is called a *directed cycle*. If ω is an orientation on a graph G such that no directed cycles exist, we call ω an *acyclic orientation*.

Since we can assign one of two possible directions to each edge, there are $2^{|E(G)|}$ possible orientations. However, some of them might include oriented cycles. But the number of acyclic orientations can be computed similarly to the number of spanning trees by a deletion-contraction algorithm.

Theorem 2.29. *Let G be a graph, and let $\kappa(G)$ denote the number of its acyclic orientations. Then*

$$\kappa(G) = \begin{cases} 0, & \text{if } G \text{ contains a loop;} \\ 2\kappa(G/e), & \text{if } e \text{ is a bridge;} \\ \kappa(G - e) + \kappa(G/e), & \text{if } e \text{ is ordinary.} \end{cases}$$

Proof. Any loop of the graph G forms a cycle by itself, thus there are no acyclic orientations if G contains a loop. Let $e = (u, v) \in G$ be a bridge. Then any acyclic orientation of G can be formed by taking an orientation of G/e and orienting e either $u \rightarrow v$ or $u \leftarrow v$. Now let $e = (u, v)$ be ordinary. An orientation of G is acyclic if and only if the orientation restricted to $G - e$ is acyclic. Or similarly, the acyclic orientations of $G - e$ with e oriented such that no cycle emerges, are exactly the acyclic orientations of G . If there is a path from u to v respecting the orientation, then clearly there can not be one from v to u . Any acyclic orientation of $G - e$ either has such a path, or not, thus we can partition them in this way.

If there is no path joining the end-vertices of e , then these orientations are exactly the ones from G/e , so there are $\kappa(G/e)$ such orientations. Adding e oriented in either way will not make the orientation cyclic, thus we have $2\kappa(G/e)$ acyclic orientations of G where there is no path in $G - e$ joining the end-vertices of e .

Now we have already considered the number of acyclic orientations of $G - e$ having no path joining u and v , leaving us with $\kappa(G - e) - \kappa(G/e)$ for the number of acyclic orientations of $G - e$ with a path joining u and v . In this case, there is only one way the edge e can be oriented, such that G is still acyclic with this orientation: $u \rightarrow v$ if there is a path from u to v and $u \leftarrow v$ if there is a path from v to u .

Hence,

$$\kappa(G) = 2\kappa(G/e) + \kappa(G - e) - \kappa(G/e) = \kappa(G/e) + \kappa(G - e). \quad \square$$

2.4 Graph Polynomials

William Thomas Tutte developed the Tutte polynomial for graphs by looking at two specific graph polynomials which are computable through a deletion-contraction recursion: the chromatic polynomial and the flow polynomial. Chris Godsil and Gordon Royle used the chromatic polynomial and the reliability polynomial in Chapter 15 of [GR01] to give examples of graph polynomials that are computable through a deletion-contraction algorithm. The goal of this chapter is to give a short overview of the basic concepts in vertex coloring, network flows and network reliability. We will be able to prove the deletion-contraction recursion formulas for each polynomial. In Section 4.4 we will show the connection between these polynomials and the Tutte polynomial. But for now we will only consider them as graph invariants. However, we will refrain from proving that each polynomial is indeed an invariant, which is going to follow immediately from the recursive formulas.

2.4.1 Colorings and the Chromatic Polynomial

This subsection gives a detailed overview of the most important concepts in vertex coloring. We are going to start by defining a proper λ -coloring and the chromatic number $\chi(G)$ for an arbitrary graph G . We will then use combinatorial techniques to compute the chromatic number for complete graphs and trees, before finally proving the computation of the chromatic polynomial through a deletion-contraction algorithm. We will follow the definitions of Chapters 1 and 15 in [GR01] and fill in some details from Chapter 11 in [EMM22].

Definition 2.30. Let G be a graph. Given a positive integer λ we call a map

$$\varphi : V(G) \rightarrow \{1, 2, \dots, \lambda\}$$

such that

$$(u, v) \in E(G) \implies \varphi(u) \neq \varphi(v)$$

a *proper λ -coloring* of G . Two proper λ -colorings φ, φ' of G are *distinct* if $\varphi(v) \neq \varphi'(v)$ for some $v \in V(G)$.

Definition 2.31. We call

$$\chi(G) := \min\{\lambda \mid G \text{ has a proper } \lambda \text{-coloring}\}$$

the *chromatic number* of G .

In combinatorics it is of interest to deduce the number of proper λ -colorings of a graph G , which we will denote by $P(G, \lambda)$. For some graphs it is quite easy to determine this number using combinatorial techniques.

Proposition 2.32. Let $G = K_n$ be the complete graph on n vertices, then

$$P(K_n, \lambda) = \lambda(\lambda - 1) \cdots (\lambda - n + 1).$$

Proof. We start with an arbitrary vertex v_1 and choose one of the λ colors and assign this color to the vertex. Since our graph is complete, any other vertex v_2 is adjacent to v_1 . Thus we are left with $(\lambda - 1)$ colors to choose from and we assign v_2 any of those. We continue until we are at the last uncolored vertex v_n , which is adjacent to all vertices that are already colored. Thus we are left with $(\lambda - (n - 1))$ colors to choose from. By the rule of product from combinatorial theory, the number of choices we have to color the whole graph is the product of the choices for each single vertex. \square

Proposition 2.33. Let T be a tree with $V(T) = n$. Then

$$P(T, \lambda) = \lambda(\lambda - 1)^{n-1}.$$

Proof. We start by coloring an arbitrary vertex v_1 of the tree, for which we can choose any of the λ colors. For every vertex connected to v_1 , we are left with $(\lambda - 1)$ colors to choose from. We choose a vertex v_2 and assign a color to v_2 . If we continue choosing a vertex that is adjacent to a colored vertex, it will always be adjacent to exactly one colored vertex, otherwise T would contain a cycle. For each such vertex there are $(\lambda - 1)$ colors to choose from. By the rule of product, we get $P(T, \lambda) = \lambda(\lambda - 1)^{n-1}$. \square

In the last two propositions we used combinatorics to give a formula on how to compute the number of proper λ -colorings for complete graphs and trees. The following theorem provides a recursive formula for the computation of the number of proper λ -colorings of an arbitrary graph G . It also shows that $P(G, \lambda)$ is actually a polynomial in λ and can be computed through a deletion-contraction algorithm.

Theorem 2.34. Let G be a graph and $P(G, \lambda)$ the number of its proper λ -colorings, then

$$P(G, \lambda) = \begin{cases} \lambda^{|V|}, & \text{if } E = \emptyset; \\ 0, & \text{if } G \text{ contains a loop}; \\ P(G - e, \lambda) - P(G/e, \lambda), & \text{if } e \text{ is not a loop.} \end{cases}$$

Thus, it is actually a polynomial in λ .

Proof. If the graph G does not have any edges, we have λ colors to choose from for each vertex, so by the rule of product we get $\lambda^{|V|}$. Now let $e \in E$ be an edge. Obviously, if e is a loop, the graph does not admit any proper colorings, so suppose e is not a loop. We want to show

$$P(G - e, \lambda) = P(G, \lambda) + P(G/e, \lambda).$$

Now let φ be a proper λ -coloring of $G - e$. Then φ either satisfies $\varphi(u) \neq \varphi(v)$ or $\varphi(u) = \varphi(v)$. There is a bijection between the proper colorings of G and those of $G - e$ satisfying $\varphi(u) \neq \varphi(v)$. Similarly, the proper colorings of G/e correspond bijectively with those of $G - e$ satisfying $\varphi(u) = \varphi(v)$. \square

Definition 2.35. Let G be a graph. We call $P(G, \lambda)$ the *chromatic polynomial* of G .

From the definition of the chromatic polynomial it is clear that it is monotonically increasing, $P(G; \lambda) = 0$ if $\lambda < \chi(G)$ and $P(G; \lambda) > 0$ else.

Example 2.36. We want to use Theorem 2.34. to compute the chromatic polynomial for the graph in Figure 10.

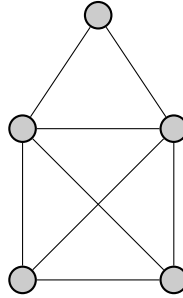


Figure 10: Graph from Example 2.36.

We can start with the graph itself and apply Theorem 2.34 until we are left with either complete graphs, graphs with loops or trees. But we choose to start with K_5 and delete two edges from one vertex:

$$P\left(\begin{array}{c} \text{Graph in Figure 10} \end{array}\right) = P\left(\begin{array}{c} \text{Graph with 4 vertices, top vertex connected to 3 others} \end{array}\right) - P\left(\begin{array}{c} \text{Graph with 4 vertices, top vertex connected to 2 others} \end{array}\right) = P\left(\begin{array}{c} \text{Graph with 4 vertices, top vertex connected to 3 others} \end{array}\right) - 2 \cdot P\left(\begin{array}{c} \text{Graph with 4 vertices, top vertex connected to 2 others} \end{array}\right).$$

With

$$\begin{aligned} P(K_5, \lambda) &= \lambda(\lambda - 1)(\lambda - 2)(\lambda - 3)(\lambda - 4), \\ P(K_4, \lambda) &= \lambda(\lambda - 1)(\lambda - 2)(\lambda - 3), \end{aligned}$$

we get

$$\begin{aligned} P\left(\begin{array}{c} \text{Graph with 5 vertices and 7 edges} \end{array}\right) &= P\left(\begin{array}{c} \text{Graph with 5 vertices and 8 edges} \end{array}\right) + 2 \cdot P\left(\begin{array}{c} \text{Graph with 4 vertices and 4 edges} \end{array}\right) \\ &= \lambda(\lambda - 1)(\lambda - 2)(\lambda - 3)(\lambda - 4) + 2 \cdot \lambda(\lambda - 1)(\lambda - 2)(\lambda - 3) \\ &= \lambda(\lambda - 1)(\lambda - 2)^2(\lambda - 3). \end{aligned}$$

Just from one look at the chromatic polynomial of our graph, we see that there are at least 4 colors needed to color the graph properly. Indeed $P(G, 4) = 48$, so we have 48 different assignments of the 4 colors. The attentive reader might have noticed that while contracting an edge, we dismissed an edge that would form a parallel edge. We did this because we only needed to know whether two vertices are connected, not by how many edges.

Theorem 2.34 is the frequently used deletion-contraction algorithm for the chromatic polynomial. But it is possible to differentiate a bridge from an ordinary edge and give a more detailed form of the deletion-contraction algorithm. We will use it in the next section to compare the flow polynomial to the chromatic polynomial.

Theorem 2.37. *Let G be a graph and $P(G, \lambda)$ its chromatic polynomial. Then*

$$P(G, \lambda) = \begin{cases} \frac{\lambda-1}{\lambda} P(G - e, \lambda), & \text{if } e \text{ is a bridge;} \\ 0, & \text{if } e \text{ is a loop;} \\ P(G - e, \lambda) - P(G/e, \lambda), & \text{if } e \text{ is ordinary;} \\ \lambda^{|V|}, & \text{if } E = \emptyset. \end{cases}$$

Proof. We only need to prove the first case, which we will do by induction on the number of edges. For the base case let $|E(G)| = 1$ and $|V(G)| = n$ and $e \in E(G)$ a bridge. Since $G - e$ and G/e are empty graphs on n and $n - 1$ vertices respectively, we have

$$P(G, \lambda) = P(G - e, \lambda) - P(G/e, \lambda) = \lambda^n - \lambda^{n-1} = \lambda^n \left(1 - \frac{1}{\lambda}\right) = P(G - e) \cdot \frac{\lambda - 1}{\lambda}.$$

Suppose the statement holds for all graphs with m edges and let G be a graph on $m + 1$ edges. If G does not contain a bridge, there is nothing to show. So let $e \in G$ be a bridge. Then, for any ordinary edge f , we know

$$P(G, \lambda) = P(G - f, \lambda) - P(G/f, \lambda)$$

from Theorem 2.34. Both graphs on the right hand side of this equation have exactly m edges. Hence we can use the induction hypothesis on these to get

$$P(G - f, \lambda) - P(G/f, \lambda) = \frac{\lambda - 1}{\lambda} P((G - f) - e, \lambda) - \frac{\lambda - 1}{\lambda} P((G/f) - e, \lambda).$$

But the resulting graph does not depend on the order of the operations delete and contract, thus the right hand side of this equation is equal to

$$\frac{\lambda - 1}{\lambda} (P((G - e) - f, \lambda) - P((G - e)/f, \lambda)).$$

Using Theorem 2.34 once more will end the proof:

$$P(G, \lambda) = \frac{\lambda - 1}{\lambda} P(G - e, \lambda). \quad \square$$

Remark 2.38. The chromatic polynomial of a graph G has a subgraph expansion. If $c(A)$ denotes the number of connected components of the spanning subgraph (V, A) , then

$$P(G, \lambda) = \sum_{A \subseteq E(G)} (-1)^{|A|} \lambda^{c(A)}.$$

For further context see Chapter 11 of [EMM22].

George David Birkhoff introduced the chromatic polynomial for planar graphs in 1912 in order to prove the long-standing four color conjecture, stating that a loopfree planar graph G has chromatic number $\chi(G) \leq 4$. Thus $P(G; 4) > 0$ for any loopfree planar graph G . The chromatic polynomial was later extended to general graphs by Whitney in 1932. The four color problem was proven in 2002, but many mathematicians still seek to prove it using the chromatic polynomial.

2.4.2 Flows and the Flow Polynomial

In the previous section we have already introduced the chromatic polynomial and proved some important properties. In this section we are going to introduce A -flows for an abelian group A and the flow polynomial for graphs. We are going to prove its deletion-contraction formula and give a connection to the chromatic polynomial. In particular, the four color problem is equivalent to the problem of every bridgeless planar graph having a nowhere-zero $\mathbb{Z}/k\mathbb{Z}$ -flow.

At first we have to define an important matrix, whose entries are determined by the characteristics of the graph it belongs to.

Definition 2.39. Let G^ω be a graph with a fixed orientation ω of its edges. The *incidence matrix* of the oriented graph G^ω is the matrix $D \in \{0, \pm 1\}^{V \times E}$ whose (v, e) -entry is defined by

$$D_{v,e} = \begin{cases} 1, & \text{if } e \text{ is directed out of } v \text{ by } \omega \\ -1, & \text{if } e \text{ is directed into } v \text{ by } \omega \\ 0, & \text{if } e \text{ is not incident with } v, \text{ or } e \text{ is a loop on } v. \end{cases}$$

Definition 2.40. Let G^ω be a graph with a fixed orientation ω , A be an additive abelian group and D be the incidence matrix of G^ω . We call an element of the kernel of D an A -flow.

This definition can be expressed in a more graphic way: For a vertex $v \in V$ the set $\omega^+(v)$ consists of those edges directed out of v by the orientation ω and $\omega^-(v)$ is the set of edges directed into v . Thus an A -flow of G^ω can be viewed as a mapping $\phi : E(G) \rightarrow A$ such that Kirchhoff's current law is satisfied at each vertex of G :

$$\sum_{e \in \omega^+(v)} \phi(e) - \sum_{e \in \omega^-(v)} \phi(e) = 0, \quad \text{for each } v \in V.$$

Definition 2.41. A *nowhere-zero* A -flow of G^ω is an A -flow $\phi : E(G) \rightarrow A$ with the additional property that $\phi(e) \neq 0$ for every $e \in E(G)$.

Example 2.42. Figure 11 shows the Petersen graph with a nowhere-zero $\mathbb{Z}/5\mathbb{Z}$ -flow.

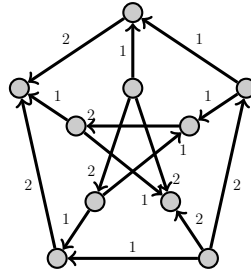


Figure 11: The Petersen graph with a nowhere-zero $\mathbb{Z}/5\mathbb{Z}$ -flow.

If we are interested in counting the different nowhere-zero A -flows for an abelian group A an interesting phenomenon arises: The number of nowhere-zero A -flows of G^ω depends only on the order of A and not on its structure. To see this, we will define the flow polynomial and show that it has a recursive deletion-contraction relation.

Definition 2.43. The *flow polynomial* of G^ω is defined by its evaluations at a positive integer k by

$$F(G^\omega; k) = \#\{\phi : E(G) \rightarrow A : \phi \text{ is a nowhere zero } A\text{-flow of } G, \text{ with } |A| = k\}.$$

Example 2.44. Let us consider the graph G in Figure 12, and find the number of nowhere-zero $\mathbb{Z}/k\mathbb{Z}$ -flows for G .

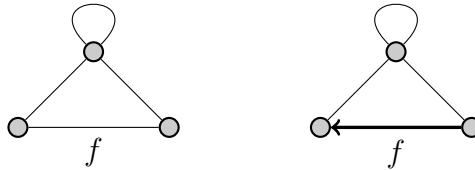


Figure 12: Graph G and Graph G with oriented edge f .

For that we need to consider possible orientations of G . Orienting the loop in either way will result in the same flow polynomial, hence we have 2^3 different orientations, giving us 8 different oriented graphs. Let us first consider the four graphs, where f is oriented as in Figure 12. The flow on the edges incident to the end-vertices of f is uniquely determined.

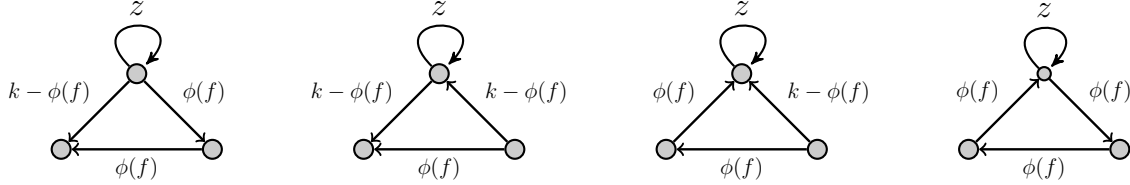


Figure 13: Four different orientations of G with flows.

Any flow on some loop can be neglected in the formula of Kirchhoff's current law, since it flows into and out of the vertex. Hence the flow on the loop can be any nonzero element $z \in \mathbb{Z}/k\mathbb{Z}$. Thus there are $(k-1)$ possibilities to choose $\phi(f)$ and $(k-1)$ possibilities to choose z . From this we obtain $(k-1)^2$ different flows for G with f oriented as in Figure 12. Orienting f the other way will result in flows that were already considered. Hence $F(G^\omega; k) = (k-1)^2$ for any orientation of G . For example, if $k = 3$, there are exactly 4 different flows the graph G^ω with fixed orientation ω can have.

The last example suggests that the number of nowhere-zero A -flows only depends on the order of the group A . Similar to the chromatic polynomial, we can prove that the number of nowhere-zero \mathbb{Z}_k -flows is indeed a polynomial in k by using the following recurrence relation:

Theorem 2.45. *The flow polynomial of a graph G^ω satisfies*

$$F(G^\omega; k) = \begin{cases} 0, & \text{if } G \text{ contains a bridge;} \\ (k-1)F(G^\omega - e; k), & \text{if } e \text{ is a loop;} \\ F(G^\omega/e; k) - F(G^\omega - e; k), & \text{if } e \text{ is ordinary;} \\ 1, & \text{if } E(G) = \emptyset. \end{cases}$$

Proof. Firstly, if $E(G) = \emptyset$, there is exactly one map from the empty set to A , namely the empty map, hence $F(G; k) = 1$. Secondly, if G^ω has a bridge e , it does not have any nowhere-zero A -flow. Indeed, suppose e is the only edge from V_1 to $V_2 = V(G) - V_1$. An A -flow must satisfy for a disjoint partition of the vertex set of a graph, that the total flow into V_1 must equal the total flow into V_2 . Since e is a bridge between V_1 and V_2 , there is no nowhere-zero A -flow. If e is a loop, then we can freely assign any of the non-zero values of A . Then any nowhere-zero A -flow of $G^\omega - e$ together with any of the $(k-1)$ assignments of e is a nowhere-zero A -flow of G^ω .

Now let e be an edge in G^ω that is ordinary. Consider a nowhere-zero A -flow ϕ of G^ω/e . For an edge incident to e consider its corresponding edge in G/e after contracting e . Then we have a bijection between $E(G^\omega - e)$ and $E(G^\omega/e)$ that maps

each edge to its corresponding edge in the contraction. Therefore ϕ can be regarded as a flow ϕ' on $G^\omega - e$. Now ϕ' is either a nowhere-zero A -flow on $G^\omega - e$, or Kirchhoffs current law is failed at both end-vertices of e and nowhere else. If the latter case is true, there is a unique extension of ϕ' to a nowhere-zero A -flow ϕ'' on G^ω . Let u, v denote the end-vertices of e . If

$$\sum_{f \in \omega^+(u)} \phi'(f) - \sum_{f \in \omega^-(u)} \phi'(f) = c,$$

then

$$\sum_{f \in \omega^+(v)} \phi'(f) - \sum_{f \in \omega^-(v)} \phi'(f) = c$$

must also hold. Thus $\phi''(e) = c$. Consequently,

$$F(G^\omega / e; k) = F(G^\omega - e; k) + F(G^\omega; k). \quad \square$$

As an easy consequence of this theorem, we see that the flow polynomial depends only on the order of A and not on its structure. Furthermore, it is indeed a polynomial in k .

Remark 2.46. Similarly to the chromatic polynomial, the flow polynomial has a subgraph expansion, see [EMM22]: For a finite Abelian group A with order k the graph $G^\omega = (V, E)$ with orientation ω has flow polynomial

$$F(G^\omega; k) = \sum_{F \subseteq E(G)} (-1)^{|E(G)| - |F|} k^{|F| - |V| + c(F)}.$$

Example 2.47. Let us compute the flow polynomial of the graph in Example 2.43 through the recursive algorithm:

$$\begin{aligned} F\left(\begin{array}{c} \text{graph with 3 vertices and 3 edges, one loop} \end{array}\right) &= (k-1) \cdot F\left(\begin{array}{c} \text{triangle graph} \end{array}\right) \\ &= (k-1) \cdot \left[F\left(\begin{array}{c} \text{graph with 2 vertices and 2 edges, one loop} \end{array}\right) - F\left(\begin{array}{c} \text{path graph with 2 vertices} \end{array}\right) \right] \\ &= (k-1) \cdot F\left(\begin{array}{c} \text{graph with 2 vertices and 2 edges, one loop} \end{array}\right) \\ &= (k-1) \cdot \left[F\left(\begin{array}{c} \text{graph with 1 vertex and 1 loop} \end{array}\right) - F\left(\begin{array}{c} \text{path graph with 1 vertex} \end{array}\right) \right] \\ &= (k-1) \cdot F\left(\begin{array}{c} \text{graph with 1 vertex and 1 loop} \end{array}\right) = (k-1)^2. \end{aligned}$$

This matches with our earlier result from Example 2.44.

It is natural to consider the flow polynomial for a graph G , as the dual of the chromatic polynomial for G , as the following theorem shows.

Theorem 2.48. *The chromatic polynomial and the flow polynomial are related by duality:*

$$P(G; k) = F(G^*; k)k^{c(G)}$$

whenever G is a plane graph with dual G^* .

Proof. We will mainly use the deletion-contraction recursion of the polynomials from Theorem 2.37 and Theorem 2.45. The flow polynomial is defined for a graph G with given orientation ω . Since the orientation is negligible, we write G for the oriented as well as the unoriented graph. Firstly, let $E(G) = \emptyset$, then $c(G) = |V|$ and $E(G^*) = \emptyset$. Hence

$$P(G; k) = 1 \cdot k^{|V|} = F(G^*; k)k^{c(G)}.$$

Secondly, let e be a loop in G . Then the corresponding edge \hat{e} in G^* is a bridge. Hence

$$P(G; k) = 0 = F(G^*; k)k^{c(G)}.$$

We are using an induction on the number of edges in G . We have already covered the base case of $E(G) = \emptyset$. Suppose the statement holds for all graphs with m edges and consider a graph G with $m+1$ edges. Now let $e \in G$ be a bridge, then with the induction hypothesis it follows that

$$P(G; k) = \frac{k-1}{k} P(G-e; k) \stackrel{IH}{=} \frac{k-1}{k} \cdot k^{c(G-e)} F((G-e)^*; k).$$

We can now use that $c(G-e) = c(G) + 1$ and Theorem 2.23 with \hat{e} being a loop in G^* , which results in

$$\frac{k-1}{k} \cdot k^{c(G-e)} F(G^* - \hat{e}; k) = k^{c(G)} F(G^*; k).$$

Lastly, let $e \in G$ be an ordinary edge, then $\hat{e} \in G^*$ is also ordinary. We start by using the induction hypothesis

$$P(G; k) = P(G-e; k) - P(G/e; k) \stackrel{IH}{=} k^{c(G-e)} F((G-e)^*; k) - k^{c(G/e)} F((G/e)^*; k).$$

In Theorem 2.23 we proved that $(G-e)^* = G^*/\hat{e}$ and $(G/e)^* = G^* - \hat{e}$ if e is ordinary in G . Using that $c(G-e) = c(G) = c(G/e)$ we get

$$P(G; k) = k^{c(G)} (F(G^*/\hat{e}; k) - F(G^* - \hat{e}; k)) = k^{c(G)} F(G^*; k). \quad \square$$

2.4.3 Network-Reliability and the Reliability Polynomial

Our next example comes from network-reliability theory. It is based on the idea of using a graph to represent a computer network where the edges represent links. These links are possibly unreliable and may fail with some probability.

Let G be a graph representing some network. Then each edge is operating with some probability p , where $0 \leq p \leq 1$, hence it is failing with probability $(1-p)$. We

can think of deleting the edges of G with fixed probability $(1 - p)$. Now let $C(G, p)$ denote the probability that no connected component of G is disconnected as a result. Thus $C(G; p)$ is basically the probability that the network survives. Obviously, if T is a tree on n vertices, then it remains connected if and only if every edge of G survives. Hence $C(T; p) = p^{n-1}$.

Definition 2.49. We call the function $C(G; p)$ the *reliability polynomial* of G .

As with the chromatic polynomial and the flow polynomial, we will show that the reliability polynomial is computable through a deletion-contraction algorithm and justify the name by showing that it is actually a polynomial.

Theorem 2.50. Let $C(G, p)$ denote the probability that no component of G is disconnected when each edge of G is deleted independently with probability $(1 - p)$. Then

$$C(G; p) = \begin{cases} C(G - e; p), & \text{if } e \text{ is a loop;} \\ p \cdot C(G/e; p), & \text{if } e \text{ is a bridge;} \\ (1 - p) \cdot C(G - e; p) + p \cdot C(G/e; p), & \text{if } e \text{ is ordinary;} \\ 1, & \text{if } E(G) = \emptyset. \end{cases}$$

Proof. First, let $E(G) = \emptyset$. Then there are no edges that could be deleted. Hence the probability that the network survives is 1. Next, let $e \in E(G)$ be a loop. Deleting e will not increase the number of connected components of G , so we can freely delete e which results in $C(G; p) = C(G - e; p)$. Next, let $e \in E(G)$ be a bridge. Deleting e will always result in an increase of connected components of G . Thus, the network survives if and only if e is not deleted and G/e survives, hence $C(G; p) = p \cdot C(G/e; p)$. Lastly, let $e \in E(G)$ be ordinary. If e is deleted, then the network G survives if and only if $G - e$ survives. If e is not deleted, then the network survives if and only if G/e survives. Together this results in

$$C(G; p) = (1 - p)C(G - e; p) + pC(G/e; p). \quad \square$$

Example 2.51. Let us compute the reliability polynomial for the graph from ex-

ample 2.47.

$$\begin{aligned}
C\left(\begin{array}{c} \text{graph with 3 nodes and a loop on the top node} \end{array}\right) &= C\left(\begin{array}{c} \text{triangle graph} \end{array}\right) \\
&= (1-p) \cdot C\left(\begin{array}{c} \text{V-shaped graph} \end{array}\right) + p \cdot C\left(\begin{array}{c} \text{graph with two nodes and a loop on both} \end{array}\right) \\
&= (1-p) \cdot p \cdot C\left(\begin{array}{c} \text{edge graph} \end{array}\right) \\
&\quad + p \cdot \left[(1-p) \cdot C\left(\begin{array}{c} \text{edge graph} \end{array}\right) + p \cdot C\left(\begin{array}{c} \text{graph with one node and a loop} \end{array}\right) \right] \\
&= p \cdot (1-p) \cdot p + p \cdot [(1-p) \cdot p + p \cdot 1] \\
&= p^2 - p^3 + p^2 - p^3 + p^2 \\
&= -2p^3 + 3p^2
\end{aligned}$$

If $p = 0.5$, then $C(G, 0.5) = 0.5$. Hence deleting each edge with a probability of 0.5 results in a 0.5 probability that the network survives. This result is not surprising. If we consider the graph without the loop, then we are left with an edgeset which has cardinality 3. The power set of the edgeset has cardinality $2^3 = 8$. For the graph to stay connected, at least 2 edges need to survive. We have

$$\binom{3}{2} + \binom{3}{3} = 4$$

possibilities, such that the graph survives. Since each subset has equal probability, the probability that the graph survives is $\frac{4}{8} = 0.5$.

3 Matroids

Matroids were first introduced to give a framework for the notions of dependence, that was found both in graphs and linear algebra. Some undergraduate students may have encountered matroids in a course on computer science when studying greedy algorithms on graphs. A problem for which greedy algorithms are used, is to find a minimal spanning tree on a weighted graph. A greedy algorithm starts by sorting the values to be compared by size. It is a fascinating fact that a greedy algorithm returns an optimal solution if the underlying problem has a matroid structure. The proof for this statement can be found in [Oxl11]. However, we are going to focus on the structure of matroids. The goal of this chapter is to introduce the *Tutte Polynomial* for matroids and prove the *Recipe Theorem* from Dominic Welsh. We use the definition of a *Tutte-Grothendieck Invariant* for matroids, which are functions on classes of matroids, that satisfy a deletion-contraction relation on ordinary elements and are multiplicative on direct sums. The recipe theorem states that all Tutte-Grothendieck invariants are in fact specializations of the Tutte polynomial.

Section 3.1 is fully dedicated to give a detailed introduction into matroid theory. We will start by defining a matroid as a finite ground set together with a collection of subsets of the ground set, which we call *independent sets*. Later we are going to show that a matroid can also be defined through its groundset and a so-called rank function. Our main examples are matrices, vector spaces and uniform matroids. Just like in Chapter 2, we will then define the dual matroid in Section 3.2 before we continue with the deletion and contraction actions in Section 3.3. In Section 3.4 we define the Tutte polynomial through its subset expansion, which uses the rank functions of the matroid and the dual matroid. Theorem 3.50 gives the formulas of the recursive deletion-contraction computation of the Tutte polynomial for a matroid. In Section 3.5 we introduce *matroid isomorphism invariants*, show that the Tutte Polynomial itself is a Tutte-Grothendieck invariant and finally prove the recipe theorem. As an example of a matroid isomorphism invariant, that specializes to the Tutte polynomial, we will use the *characteristic polynomial* of a matroid.

Chris Godsil and Gordon Royle chose in [GR01] to directly introduce matroids through their rank function. However, we want to point out the many analogies to concepts from linear algebra, which is why we chose the introduction through independent sets. For this we mainly use the two works of James Oxley [Oxl11] and Dominic Welsh [Wel76], which both had a big impact on the research in matroid theory. As in Chapter 2, we will use "Handbook of the Tutte Polynomial and Related Topics" [EMM22] as an overview of the most important concepts needed for a complete discussion of the Tutte polynomial on matroids.

3.1 Preliminaries in Matroid Theory

There are many different but equivalent ways to define matroids. We choose to start with the definition through a groundset and a collection of subsets, called *independent sets*. As in linear algebra, we call the inclusion-maximal independent sets the *bases*. It is also possible to define a matroid through its groundset and collection of bases. We are going to show how any matrix gives rise to a matroid and prove that

any two bases of a matroid have the same cardinality. But most importantly we are going to prove that we can define any matroid through its groundset and rank function.

Definition 3.1. Let Ω be a finite set and \mathcal{I} be a collection of subsets of Ω having the following three properties:

- (I1) $\emptyset \in \mathcal{I}$.
- (I2) If $I \in \mathcal{I}$ and $J \subseteq I$, then $J \in \mathcal{I}$.
- (I3) If I_1 and I_2 are in \mathcal{I} and $|I_1| < |I_2|$, then there is an element e of $I_2 - I_1$ such that $I_1 \cup e \in \mathcal{I}$.

We call the ordered pair (Ω, \mathcal{I}) a *matroid* \mathcal{M} , Ω the *ground set* of \mathcal{M} and the members of \mathcal{I} the *independent sets* of \mathcal{M} . A subset of Ω that is not in \mathcal{I} is called *dependent*.

Lemma 3.2. Let $\mathcal{M} = (\Omega, \mathcal{I})$ be a matroid and $T \subseteq \Omega$ a subset. Consider the set $\mathcal{I}|T := \{I \subseteq T : I \in \mathcal{I}\}$, then $(T, \mathcal{I}|T)$ is a matroid.

Proof. We need to prove whether $(T, \mathcal{I}|T)$ satisfies (I1), (I2) and (I3). Since $\emptyset \subseteq T$ and $\emptyset \in \mathcal{I}$ the empty set is also contained in $\mathcal{I}|T$.

Now let $I \in \mathcal{I}|T$ and $J \subseteq I$. Then by the definition of $\mathcal{I}|T$ we have $I \subseteq T$ and $I \in \mathcal{I}$. Since \mathcal{I} satisfies (I2) itself, $J \in \mathcal{I}$, with $J \subseteq I \subseteq T$ the set J is also contained in $\mathcal{I}|T$.

Now consider $I_1, I_2 \in \mathcal{I}|T$ with $|I_1| < |I_2|$. By the definition of $\mathcal{I}|T$, $I_1, I_2 \in \mathcal{I}$ and since \mathcal{I} satisfies (I3), there is an element $e \in I_2 - I_1$, such that $I_1 \cup e \in \mathcal{I}$. Since $I_2, I_1 \subseteq T$, $I_1 \cup e \subseteq T$ and therefore $I_1 \cup e \in \mathcal{I}|T$. \square

Definition 3.3. Let $\mathcal{M} = (\Omega, \mathcal{I})$ be a matroid and $T \subseteq \Omega$ a subset. We call the matroid $(T, \mathcal{I}|T)$ with

$$\mathcal{I}|T = \{I \in \mathcal{I} : I \subseteq T\}$$

the *restriction* of \mathcal{M} to T . We denote the matroid by $\mathcal{M}|T$. If we want to emphasize which set is deleted from the ground set, we write $\mathcal{M} - \bar{T}$ for $\mathcal{M}|T$ and call it the *deletion* of \bar{T} from \mathcal{M} .

Proposition 3.4. Let Ω be the set of column labels of an $n \times m$ -matrix A over a field \mathbb{F} . Let \mathcal{I} be the set of subsets E of Ω for which the multiset of columns labelled by E is a set and is linearly independent in the vector space $V(n, \mathbb{F})$. Then (Ω, \mathcal{I}) is a matroid.

Proof. It is clear, that \mathcal{I} satisfies (I1) and (I2). For property (I3), let $I, J \in \mathcal{I}$ with $|I| < |J|$. Now consider the span of the union $\text{span}(I \cup J)$, then $\dim(\text{span}(I \cup J)) \geq |J|$. Suppose there is no element $e \in J - I$ such that $I \cup e \in \mathcal{I}$, then $I \cup e$ is linearly dependent for every element $e \in J - I$. Therefore $\text{span}(I \cup J) \subseteq \text{span}(I)$ and for their dimensions the following inequality must hold:

$$|J| \leq \dim(\text{span}(I \cup J)) \leq |I|.$$

But this is a contradiction to $|J| > |I|$, hence (I3) holds. \square

Example 3.5. Consider the following matrix over the field \mathbb{R}

$$A = \begin{matrix} & \begin{matrix} \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{4} & \mathbf{5} \end{matrix} \\ \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix} \end{matrix}$$

Then with the previous proposition $\Omega = \{1, 2, 3, 4, 5\}$ and

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

In linear algebra, an inclusion maximal subset U of a vector space V is called a basis if U consists of linearly independent vectors. Adding any vector to U from $V - U$ returns linearly dependent vectors. Similarly to vector spaces, we can define the *bases* of a matroid.

Definition 3.6. Let $\mathcal{M} = (\Omega, \mathcal{I})$ be a finite set, we call an inclusion-maximal independent set of \mathcal{M} a *basis* and an inclusion-minimal dependent set of \mathcal{M} a *circuit*.

In Chapter 4 we are going to show how the spanning forests, cycles respectively, of a graph correspond to the bases, circuits respectively, of the matroid belonging to the graph.

Lemma 3.7. All bases of a matroid $\mathcal{M} = (\Omega, \mathcal{I})$ have the same size.

Proof. Let B_1 and B_2 be inclusion-maximal independent sets, and assume $|B_1| > |B_2|$. Then by (I3) there must be an element $e \in B_1$ such that $B_2 \cup B_1$ is itself independent. But $B_2 \subset B_2 \cup e$, thus B_2 was not an inclusion-maximal independent set, hence not a basis. \square

Definition 3.8. Let Ω be a finite set, and let $\text{rkf} : \mathcal{P}(\Omega) \rightarrow \mathbb{Z}^+ \cup \{0\}$ be a function that satisfies the following properties.

(R1) If $A \subseteq B \subseteq \Omega$, then $\text{rkf}(A) \leq \text{rkf}(B)$.

(R2) If $A, B \subseteq \Omega$, then $\text{rkf}(A \cup B) + \text{rkf}(A \cap B) \leq \text{rkf}(A) + \text{rkf}(B)$.

(R3) If $A \subseteq \Omega$, then $0 \leq \text{rkf}(A) \leq |A|$.

We call such a function a *rank function*.

(R3) is reminiscent of the identity

$$\dim(U + W) + \dim(U \cap W) = \dim(U) + \dim(W),$$

where U and W are subspaces of a finite-dimensional vector space V and

$$U + W = \{v \in V \mid v = u + w \text{ for } u \in U \text{ and } w \in W\}.$$

The most obvious example for a rank function, is the one that maps each set to its cardinality, the following example is more interesting.

Example 3.9. Let G be a graph with some orientation σ and D be the $m \times n$ incidence matrix of the oriented graph G^σ . Let Ω be the set of the columns of D and for $A \subseteq \Omega$ let

$$\text{rank}(A) = \dim(\text{span}(A)).$$

Then rank is a rank function, where (R1), (R2), (R3) follow directly from linear algebra. Moreover, it is independent of the orientation, since reversing the orientation of an edge is only multiplying the corresponding column in the matrix by (-1) .

Definition 3.10. Let $\mathcal{M} = (\Omega, \mathcal{I})$ be a matroid and $A \subseteq \Omega$. We call the cardinality of a basis \mathcal{B} of the restriction $\mathcal{M}|A$ the *rank* of A and denote it by $\text{rk}(A)$.

The following lemma, shows that rk is indeed a rank function, so that it deserves its name.

Lemma 3.11. *Let $\mathcal{M} = (\Omega, \mathcal{I})$ be a matroid, then rk , as defined in Definition 3.10, maps $\mathcal{P}(\Omega)$ to nonnegative integers and is a rank function.*

Proof. Let $\mathcal{M} = (\Omega, \mathcal{I})$ and $A, B \subseteq \Omega$ be subsets such that $A \subseteq B$. Let \mathcal{B} be a basis of $\mathcal{M}|B$. Then $\mathcal{B} \cap A$ is a basis of $\mathcal{M}|A$. Therefore $\text{rk}(A) \leq \text{rk}(B)$. Moreover, for a subset A its rank $\text{rk}(A)$ equals the cardinality of a basis \mathcal{B} of $\mathcal{M}|A$. From $|\mathcal{B}| \leq |A|$, it follows that $0 \leq \text{rk}(A) \leq |A|$. Now let $A, B \subseteq \Omega$ be arbitrary subsets. Let $\mathcal{B}^{A \cap B}$ be a basis of the matroid $\mathcal{M}|(A \cap B) = (A \cap B, \mathcal{I}|(A \cap B))$ with $\mathcal{I}|(A \cap B) = \{I \in \mathcal{I} : I \subseteq A \cap B\}$ and consider the matroid $\mathcal{M}|(A \cup B) = (A \cup B, \mathcal{I}|(A \cup B))$ with $\mathcal{I}|(A \cup B) = \{I \in \mathcal{I} : I \subseteq A \cup B\}$. In addition let $\mathcal{B}^{A \cap B}$ be a basis of $\mathcal{M}|(A \cap B)$. Then $\mathcal{B}^{A \cap B} \in \mathcal{I}|(A \cup B)$, hence $\mathcal{B}^{A \cap B} \subseteq \mathcal{B}^{A \cup B}$ for some basis $\mathcal{B}^{A \cup B}$ of $\mathcal{M}|(A \cup B)$. Now since $\mathcal{B}^{A \cup B} \cap A \subseteq \mathcal{B}^{A \cup B}$ and $\mathcal{B}^{A \cup B} \cap B \subseteq \mathcal{B}^{A \cup B}$ are independent in \mathcal{M} and fully contained in A, B respectively, they are also independent in $\mathcal{M}|A, \mathcal{M}|B$ respectively. Therefore

$$\text{rk}(A) \geq \text{rk}(\mathcal{B}^{A \cup B} \cap A) = |\mathcal{B}^{A \cup B} \cap A| \text{ and } \text{rk}(B) \geq \text{rk}(\mathcal{B}^{A \cup B} \cap B) = |\mathcal{B}^{A \cup B} \cap B|,$$

which shows

$$\text{rk}(A) + \text{rk}(B) \geq |\mathcal{B}^{A \cup B} \cap A| + |\mathcal{B}^{A \cup B} \cap B|.$$

For two arbitrary finite sets X and Y the sum of their cardinalities equals the sum of the cardinalities of their union and intersection, hence

$$|\mathcal{B}^{A \cup B} \cap A| + |\mathcal{B}^{A \cup B} \cap B| = |(\mathcal{B}^{A \cup B} \cap A) \cup (\mathcal{B}^{A \cup B} \cap B)| + |(\mathcal{B}^{A \cup B} \cap A) \cap (\mathcal{B}^{A \cup B} \cap B)|.$$

Together we can conclude

$$\text{rk}(A) + \text{rk}(B) \geq |\mathcal{B}^{A \cup B} \cap (A \cup B)| + |\mathcal{B}^{A \cup B} \cap A \cap B|,$$

and with $\mathcal{B}^{A \cup B} \cap (A \cup B) = \mathcal{B}^{A \cup B}$ and $\mathcal{B}^{A \cup B} \cap A \cap B = \mathcal{B}^{A \cap B}$, we finish the proof

$$\text{rk}(A) + \text{rk}(B) \geq |\mathcal{B}^{A \cup B}| + |\mathcal{B}^{A \cap B}| = \text{rk}(A \cup B) + \text{rk}(A \cap B). \quad \square$$

We chose to introduce a matroid through its set of independent sets, but [GR01] characterize a matroid through its rank function. Theorem 3.13 shows the equivalence of these two approaches. We will need the following lemma for its proof.

Lemma 3.12. *Let Ω be a set and rk be a function on $\mathcal{P}(\Omega)$ satisfying (R2) and (R3). If A and B are subsets of Ω such that $\text{rk}(A \cup e) = \text{rk}(A)$ for all $e \in B - A$, then $\text{rk}(A \cup B) = \text{rk}(A)$.*

Proof. We will argue by induction on $|B - A| = |\{e_1, \dots, e_k\}| = k$. If $k = 1$ and $\text{rk}(A \cup e_1) = \text{rk}(A)$, then $\text{rk}(A) = \text{rk}(A \cup e_1) = \text{rk}(A \cup B)$. Assume the statement holds for all sets A and B where $|B - A| = m$ and let $k = m + 1$. Then by the induction assumption

$$\text{rk}(A) + \text{rk}(A) = \text{rk}(A \cup \{e_1, e_2, \dots, e_m\}) + \text{rk}(A \cup e_{m+1}),$$

and with (R2) we have

$$\begin{aligned} \text{rk}(A) + \text{rk}(A) &\geq \text{rk}((A \cup \{e_1, e_2, \dots, e_m\}) \cup (A \cup e_{m+1})) \\ &\quad + \text{rk}((A \cup \{e_1, e_2, \dots, e_m\}) \cap (A \cup e_{m+1})) \\ &= \text{rk}(A \cup \{e_1, \dots, e_{m+1}\}) + \text{rk}(A) \\ &\geq \text{rk}(A) + \text{rk}(\emptyset) + \text{rk}(A). \end{aligned}$$

Equality must hold throughout, therefore

$$\text{rk}(A \cup \{e_1, \dots, e_{m+1}\}) = \text{rk}(A). \quad \square$$

Theorem 3.13. *Let Ω be a set and rkf a function that maps $\mathcal{P}(\Omega)$ into the set of non-negative integers and satisfies (R1) - (R3). Let \mathcal{I} be the collection of subsets I such that $\text{rkf}(I) = |I|$. Then (Ω, \mathcal{I}) is a matroid with rank function rkf .*

Proof. We will prove that \mathcal{I} satisfies (I1) - (I3) and that the rank function rk on \mathcal{M} determined by \mathcal{I} is indeed the rank function rkf . First let us prove (I1). From the definition of rkf , it satisfies $0 \leq \text{rkf}(\emptyset) \leq |\emptyset| = 0$. Thus equality must hold throughout and $\text{rkf}(\emptyset) = |\emptyset|$, hence $\emptyset \in \mathcal{I}$ and $\mathcal{I} \neq \emptyset$. For (I2) suppose that $I \in \mathcal{I}$ and $J \subseteq I$. Now consider the complement of J in I , with (R2) we receive

$$\begin{aligned} \text{rkf}(J \cup (I - J)) + \text{rkf}(J \cap (I - J)) &\leq \text{rkf}(J) + \text{rkf}(I - J) \\ \iff \text{rkf}(I) + \text{rkf}(\emptyset) &\leq \text{rkf}(J) + \text{rkf}(I - J) \end{aligned} \quad (3.1)$$

But since $I \in \mathcal{I}$, $\text{rkf}(I) = |I|$ and with (R3) $\text{rkf}(J) \leq |J|$ and $\text{rkf}(I - J) \leq |I - J|$ hold. Thus by Equation (3.1) we have

$$|I| \leq \text{rkf}(J) + \text{rkf}(I - J) \leq |J| + |I - J| = |I|,$$

where equality must hold throughout. Hence $\text{rkf}(J) = |J|$ and by the definition $J \in \mathcal{I}$ follows. Now assume that $I_1, I_2 \in \mathcal{I}$, such that $|I_2| > |I_1|$ but for all elements $e \in I_2 - I_1$ the union $I_1 \cup e$ is not an element of \mathcal{I} . If $I_1 \cup e \notin \mathcal{I}$, then $\text{rkf}(I_1 \cup e) \neq |I_1 \cup e| = |I_1| + 1$. By (R3) we also know that $\text{rkf}(I_1 \cup e) \leq |I_1 \cup e|$. Furthermore, since $I_1 \subset (I_1 \cup e)$, $\text{rkf}(I_1) \leq \text{rkf}(I_1 \cup e)$ follows by (R1). Hence

$$|I_1| = \text{rkf}(I_1) \leq \text{rkf}(I_1 \cup e) < |I_1| + 1 \implies \text{rkf}(I_1 \cup e) = |I_1|.$$

Now by applying Lemma 3.12 on I_1 and I_2 this tells us

$$|I_1| = \text{rkf}(I_1) = \text{rkf}(I_1 \cup I_2) \stackrel{R1}{\geq} \text{rkf}(I_2) = |I_2|,$$

which is a contradiction to $|I_2| > |I_1|$. So \mathcal{I} satisfies (I3). Since \mathcal{I} satisfies (I1) - (I3), $\mathcal{M} = (\Omega, \mathcal{I})$ is a matroid. It is left to prove that $\text{rkf}(A) = \text{rk}(A)$ for all $A \subseteq \Omega$. First, let $A \in \mathcal{I}$, then $\text{rkf}(A) = |A|$ and $\text{rk}(A) = |A|$, since A is a basis of $\mathcal{M}|A$. Now let $A \notin \mathcal{I}$ and let \mathcal{B} be a basis for $\mathcal{M}|A$, then $\text{rk}(A) = |\mathcal{B}|$. Additionally, $\mathcal{B} \cup x \notin \mathcal{I}$ for all $x \in A - \mathcal{B}$. Hence,

$$|\mathcal{B}| = \text{rkf}(\mathcal{B}) \leq \text{rkf}(\mathcal{B} \cup x) < |\mathcal{B} \cup x|,$$

so $\text{rkf}(\mathcal{B} \cup x) = \text{rkf}(\mathcal{B})$. By Lemma 3.12, we conclude

$$\text{rkf}(A) = \text{rkf}(\mathcal{B} \cup A) = \text{rkf}(\mathcal{B}) = |\mathcal{B}| = \text{rk}(A). \quad \square$$

Corollary 3.14. *Let Ω be a finite set. A function $\text{rkf} : \mathcal{P}(\Omega) \rightarrow \mathbb{Z}^+ \cup \{0\}$ is the rank function of a matroid in Ω if and only if rkf satisfies properties (R1), (R2) and (R3).*

Remark 3.15. The last corollary follows from the preceding theorem and lemma. With this corollary, we can now define a matroid through its ground set Ω and a rank function on Ω satisfying (R1) - (R3). We write $\mathcal{M} = (\Omega, \text{rk})$. If we want to emphasize that a rank function rk belongs to a matroid \mathcal{M} we write $\text{rk}_{\mathcal{M}}$.

Definition 3.16. For a matroid \mathcal{M} we call $\text{rk}(\Omega)$ the *rank* of \mathcal{M} and denote it by $\text{rk}(\mathcal{M})$.

Example 3.17. Let Ω be an n -element set and r be an integer with $0 \leq r \leq n$. We define the Matroid \mathcal{U}_n^r with ground set Ω through the rank function $\text{rk}(A) := \min\{|A|, r\}$ for a subset $A \subseteq \Omega$. This matroid is called the *uniform matroid* of rank r on an n -element set. It is easy to see that the independent sets of a uniform matroid \mathcal{U}_n^r are the subsets of Ω with cardinality at most r and a subset is a basis if and only if its cardinality is exactly r . The rank of the uniform Matroid is

$$\text{rk}(\mathcal{U}_n^r) = r.$$

Definition 3.18. Let $\mathcal{M} = (\Omega, \text{rk})$ be a matroid. We call a subset $A \subseteq \Omega$ that satisfies $\text{rk}(A) = \text{rk}(\Omega)$ a *spanning* set of \mathcal{M} .

Remark 3.19. With Lemma 3.7 we can easily see that a subset $A \subseteq \Omega$ is a basis of a matroid if and only if it is an inclusion-minimal spanning set.

3.2 The Dual Matroid

In this section, we will introduce the dual matroid \mathcal{M}^\perp by defining a dual rank function for a given matroid \mathcal{M} . We will show that the bases of \mathcal{M}^\perp are the set theoretic complements of the bases of \mathcal{M} . We will also point out analogies to linear algebra, concerning the concept of orthogonality of vector spaces.

We denote for a subset $A \subseteq \Omega$, the set theoretic complement $\Omega - A$ by \overline{A} .

Definition 3.20. Let f be a function on the subsets of Ω . We define

$$f^\perp(A) := |A| + f(\overline{A}) - f(\Omega)$$

to be the dual of f on the subsets $A \subseteq \Omega$.

Remark 3.21. We want to justify the notation above. Let $\mathcal{M} = (\Omega, \mathcal{I})$ be a matroid and f be a function on the subsets of Ω that satisfies $f(\emptyset) = 0$. For a subset $A \subseteq \Omega$, using the definition of the dual rank function once returns

$$f^{\perp\perp}(A) = |A| + f^{\perp}(\overline{A}) - f^{\perp}(\Omega) + f^{\perp}(\Omega) - f^{\perp}(\Omega).$$

Substituting the definition of the dual rank function a second time returns

$$f^{\perp\perp}(A) = |A| - (|\overline{A}| + f(A) - f(\Omega)) - (|\Omega| + f(\emptyset) - f(\Omega)) = f(A).$$

Lemma 3.22. *If \mathbf{rk} is a rank function on Ω , then \mathbf{rk}^{\perp} is also a rank function on Ω .*

Proof. We will start by proving the condition (R2) for \mathbf{rk}^{\perp} . For this we have to remember that the cardinality function satisfies (R2) itself. Now since

$$\begin{aligned} \mathbf{rk}^{\perp}(A \cup B) &= |A \cup B| + \mathbf{rk}(\overline{A \cup B}) - \mathbf{rk}(\Omega) \\ \text{and } \mathbf{rk}^{\perp}(A \cap B) &= |A \cap B| + \mathbf{rk}(\overline{A \cap B}) - \mathbf{rk}(\Omega), \end{aligned}$$

the right side of (R2) for \mathbf{rk}^{\perp} equals

$$\mathbf{rk}^{\perp}(A \cup B) + \mathbf{rk}^{\perp}(A \cap B) = |A \cup B| + |A \cap B| + \mathbf{rk}(\overline{A \cap B}) + \mathbf{rk}(\overline{A \cup B}) - 2\mathbf{rk}(\Omega).$$

Whereas with

$$\begin{aligned} \mathbf{rk}^{\perp}(A) &= |A| + \mathbf{rk}(\overline{A}) - \mathbf{rk}(\Omega) \\ \mathbf{rk}^{\perp}(B) &= |B| + \mathbf{rk}(\overline{B}) - \mathbf{rk}(\Omega) \end{aligned}$$

the left side of the inequality equals

$$\mathbf{rk}^{\perp}(A) + \mathbf{rk}^{\perp}(B) = |A| + |B| + \mathbf{rk}(\overline{A}) + \mathbf{rk}(\overline{B}) - 2\mathbf{rk}(\Omega).$$

Since $|A \cup B| + |A \cap B| = |A| + |B|$ for any two sets, we only need to show that

$$\mathbf{rk}(\overline{A \cap B}) + \mathbf{rk}(\overline{A \cup B}) \leq \mathbf{rk}(\overline{A}) + \mathbf{rk}(\overline{B}).$$

But as we already noted before, \mathbf{rk} is itself a function that satisfies (R2), hence this inequality is satisfied.

We will now show that \mathbf{rk}^{\perp} is nonnegative and satisfies $\mathbf{rk}^{\perp}(A) \leq |A|$. First we rewrite \mathbf{rk}^{\perp} as

$$\mathbf{rk}^{\perp}(A) = |A| - (\mathbf{rk}(\Omega) - \mathbf{rk}(\overline{A}))$$

and remember that $|A| \geq 0$ holds.

For \mathbf{rk}^{\perp} to be nonnegative, we only need to show that $\mathbf{rk}(\Omega) - \mathbf{rk}(\overline{A}) \leq |A|$. First, $\mathbf{rk}(\Omega) = \mathbf{rk}(\Omega) + \mathbf{rk}(\emptyset) = \mathbf{rk}(A \cup \overline{A}) + \mathbf{rk}(A \cap \overline{A})$. Applying (R2) for \mathbf{rk} yields

$$\mathbf{rk}(\Omega) \leq \mathbf{rk}(A) + \mathbf{rk}(\overline{A}).$$

Now \mathbf{rk} satisfies (R3), hence

$$\mathbf{rk}(\Omega) - \mathbf{rk}(\overline{A}) \leq |A|.$$

For rk^\perp to satisfy (R3), we only need to show that $\text{rk}(\Omega) - \text{rk}(\overline{A}) \geq 0$. For this we use that rk satisfies (R1), and with $\overline{A} \subseteq \Omega$ this implies $\text{rk}(\overline{A}) \leq \text{rk}(\Omega)$.

We will now show that rk^\perp satisfies (R1). Let $A \subseteq B$. We can write $\overline{A} = \overline{B} \cup (B - A)$. Furthermore, since $A \subseteq B$ the intersection $\overline{B} \cap (B - A)$ is empty, hence $\text{rk}(\overline{B} \cap (B - A)) = 0$. With this information we get

$$\text{rk}^\perp(A) = |A| + \text{rk}(\overline{A}) - \text{rk}(\Omega) = |A| + \text{rk}(\overline{B} \cup (B - A)) + \text{rk}(\overline{B} \cap (B - A)) - \text{rk}(\Omega).$$

Now we can use (R2) and (R3) to get

$$\text{rk}(\overline{B} \cup (B - A)) + \text{rk}(\overline{B} \cap (B - A)) \leq \text{rk}(\overline{B}) + \text{rk}(B - A) \leq \text{rk}(\overline{B}) + |B - A|.$$

Together this results in

$$\text{rk}^\perp(A) \leq |A| + \text{rk}(\overline{B}) + |B - A| - \text{rk}(\Omega) = |B| + \text{rk}(\overline{B}) - \text{rk}(\Omega) = \text{rk}^\perp(B). \quad \square$$

Remark 3.23. With $\text{rk}(\emptyset) \leq |\emptyset| = 0$ we get $\text{rk}^{\perp\perp} = \text{rk}$.

Definition 3.24. If $\mathcal{M} = (\Omega, \text{rk})$ is a matroid, then $\mathcal{M}^\perp := (\Omega, \text{rk}^\perp)$ is called the *dual* of \mathcal{M} .

Lemma 3.25. The rank of the dual Matroid is $\text{rk}(\mathcal{M}^\perp) = |\Omega| - \text{rk}(\Omega)$.

Proof. Firstly, $\text{rk}(\mathcal{M}^\perp) = \text{rk}^\perp(\Omega)$ by definition of the rank of a matroid. Secondly,

$$\text{rk}^\perp(\Omega) = |\Omega| + \text{rk}(\emptyset) - \text{rk}(\Omega) = |\Omega| - \text{rk}(\Omega). \quad \square$$

Theorem 3.26. The bases of \mathcal{M}^\perp are the complements of the bases of \mathcal{M} .

Proof. Let $A \subset \Omega$ be independent in \mathcal{M} , then

$$\text{rk}^\perp(\overline{A}) = |\overline{A}| + \text{rk}(A) - \text{rk}(\Omega) = |\overline{A}| + |A| - \text{rk}(\Omega) = |\Omega| - \text{rk}(\Omega)$$

and

$$\text{rk}^\perp(\Omega) = |\Omega| + \text{rk}(\emptyset) - \text{rk}(\Omega) = |\Omega| - \text{rk}(\Omega).$$

Thus $\text{rk}^\perp(\Omega) = \text{rk}^\perp(\overline{A})$ holds if and only if A is independent in \mathcal{M} , and $\text{rk}^\perp(\Omega) = \text{rk}^\perp(\overline{A})$ means that \overline{A} is spanning in \mathcal{M}^\perp . Consequently A is independent in \mathcal{M} if and only if \overline{A} is spanning in \mathcal{M}^\perp . By duality, A is spanning in \mathcal{M} if and only if \overline{A} is independent in \mathcal{M}^\perp .

Now let B be a basis, hence for all $A \in \Omega$ with $B \subset A$, $\text{rk}(A) < |A|$ holds. Their complements satisfy $\overline{A} \subset \overline{B}$ and since B is independent in \mathcal{M} , it is spanning in \mathcal{M}^\perp , thus $\text{rk}^\perp(\overline{B}) = \text{rk}(\Omega)$. However A is dependent in \mathcal{M} , so its complement is spanning in \mathcal{M}^\perp , thus $\text{rk}^\perp(\overline{A}) < \text{rk}(\Omega)$. Leaving us with B being an inclusion minimal spanning set in \mathcal{M}^\perp , therefore a basis in \mathcal{M}^\perp . \square

We are now going to introduce the notions of *loops* and *coloops* of a matroid. In Chapter 4, we are going to explain the connection between these and the notions *loops*, *bridges* for graphs.

Definition 3.27. Let \mathcal{M} be a matroid. We call an element $e \in \Omega$ a *loop* if $\text{rk}(\{e\}) = 0$. If an element e of the matroid \mathcal{M} is a loop in \mathcal{M}^\perp , then we call e a *coloop* in \mathcal{M} .

Lemma 3.28. *Let $\mathcal{M} = (\Omega, \mathbf{rk})$ be a matroid and \mathcal{M}^\perp be its dual and let e be an element in \mathcal{M} . Then e is a coloop in \mathcal{M} if and only if $\mathbf{rk}(\Omega - \{e\}) = \mathbf{rk}(\Omega) - 1$.*

Proof. We only need to look at the definition of the dual rank function:

$$\begin{aligned} \mathbf{rk}^\perp(e) = |e| + \mathbf{rk}(\Omega - e) - \mathbf{rk}(\Omega) &\iff \mathbf{rk}^\perp(e) = 1 + \mathbf{rk}(\Omega - e) - \mathbf{rk}(\Omega) \\ &\iff \mathbf{rk}(\Omega - e) - \mathbf{rk}^\perp(e) = \mathbf{rk}(\Omega) - 1 \end{aligned}$$

Thus, $\mathbf{rk}(\Omega - e) = \mathbf{rk}(\Omega) - 1$ if and only if $\mathbf{rk}^\perp(e) = 0$. \square

In linear algebra the bidual space of a finite dimensional vector space V is isomorphic to V . The analogous result for matroids, is that taking the dual of a matroid twice results in the original matroid.

Corollary 3.29. *If \mathcal{M} is a matroid, then $\mathcal{M}^{\perp\perp} = \mathcal{M}$.*

Proof. Let $\mathcal{M} = (\Omega, \mathbf{rk})$ be a matroid. We've already showed that $f^{\perp\perp} = f$ for any function f . Thus with $\mathbf{rk}^{\perp\perp} = \mathbf{rk}$ and $\mathcal{M}^\perp = (\Omega, \mathbf{rk}^\perp)$, we get

$$\mathcal{M}^{\perp\perp} = (\Omega, \mathbf{rk}^{\perp\perp}) = (\Omega, \mathbf{rk}) = \mathcal{M}. \quad \square$$

Example 3.30. We have already noted that the bases of the rank- r uniform matroid \mathcal{U}_n^r are the r -element subsets of an n -element set Ω . Thus the bases of the dual matroid are the $(n - r)$ -element subsets of Ω . Hence,

$$(\mathcal{U}_n^r)^\perp = \mathcal{U}_n^{n-r}.$$

3.3 The Deletion-Contraction Algorithm for Matroids

We have introduced the operations of deletion and contraction in the context of graph theory. We will now introduce these operations for matroids and prove that they are dual actions. Then we will consider a way of glueing two matroids.

Let $\mathcal{M} = (\Omega, \mathbf{rk})$ be a matroid. In Definition 3.3 we defined the restriction $\mathcal{M}|T$. We already noted that restricting a matroid to a subset T can also be called the deletion of a subset \overline{T} .

We begin by noting that for a subset $T \subseteq \Omega$ and $A \subseteq \overline{T}$ the function

$$\begin{aligned} \mathbf{rk}_{\mathcal{M}-T} : \mathcal{P}(\Omega - T) &\rightarrow \mathbb{Z}^+ \cup \{0\} \\ A &\mapsto \mathbf{rk}(A) \end{aligned}$$

is the rank function on $\Omega - T$ of the matroid $\mathcal{M} - T$. Now consider the function

$$\begin{aligned} \mathbf{rk}_{\mathcal{M}/T} : \mathcal{P}(\Omega - T) &\rightarrow \mathbb{Z}^+ \cup \{0\} \\ A &\mapsto \mathbf{rk}(A \cup T) - \mathbf{rk}(T) \end{aligned}$$

defined on the subsets of $\Omega - T$.

Lemma 3.31. *Let $\mathcal{M} = (\Omega, \mathbf{rk})$ be a matroid. Then $\mathbf{rk}_{\mathcal{M}/T}$ defines a rank function on $\Omega - T$ for any subset $T \subseteq \Omega$.*

Proof. We need to prove (R1), (R2) and (R3). For (R1), let $A \subseteq B$ be subsets of $\Omega - T$. Then $\text{rk}_{\mathcal{M}/T}(A) = \text{rk}(A \cup T) - \text{rk}(T)$ and $\text{rk}_{\mathcal{M}/T}(B) = \text{rk}(B \cup T) - \text{rk}(T)$, such that

$$\text{rk}_{\mathcal{M}/T}(A) \leq \text{rk}_{\mathcal{M}/T}(B) \iff \text{rk}(A \cup T) \leq \text{rk}(B \cup T),$$

which is always true, since from $A \subseteq B$ follows $A \cup T \subseteq B \cup T$.

Next we will show (R2), let A, B be arbitrary subsets of $\Omega - T$. Then,

$$\text{rk}_{\mathcal{M}/T}(A \cup B) + \text{rk}_{\mathcal{M}/T}(A \cap B) = \text{rk}(A \cup B \cup T) - 2\text{rk}(T) + \text{rk}((A \cap B) \cup T),$$

but $A \cup B \cup T = (A \cup T) \cup (B \cup T)$ and $(A \cap B) \cup T = (A \cup T) \cap (B \cup T)$, hence

$$\text{rk}_{\mathcal{M}/T}(A \cup B) + \text{rk}_{\mathcal{M}/T}(A \cap B) = \text{rk}((A \cup T) \cup (B \cup T)) - 2\text{rk}(T) + \text{rk}((A \cup T) \cap (B \cup T)).$$

Now we can use that rk satisfies (R2), thus

$$\text{rk}_{\mathcal{M}/T}(A \cup B) + \text{rk}_{\mathcal{M}/T}(A \cap B) \leq \text{rk}(A \cup T) + \text{rk}(B \cup T) - 2\text{rk}(T) = \text{rk}_{\mathcal{M}/T}(A) + \text{rk}_{\mathcal{M}/T}(B).$$

Now let's prove the last condition (R3). We can use (R2) and (R3) for rk and that rk maps into the natural numbers, then

$$\begin{aligned} \text{rk}_{\mathcal{M}/T}(A) &= \text{rk}(A \cup T) - \text{rk}(T) \leq \text{rk}(A) + \text{rk}(T) - \text{rk}(A \cap T) - \text{rk}(T) \\ &= \text{rk}(A) - \text{rk}(A \cap T) \leq |A| - \text{rk}(A \cap T) \leq |A|. \square \end{aligned}$$

Definition 3.32. For a matroid $\mathcal{M} = (\Omega, \text{rk})$ and a subset $T \subseteq \Omega$ we call the matroid $\mathcal{M}/T = (\Omega - T, \text{rk}_{\mathcal{M}/T})$ the *contraction* of T .

Remark 3.33. Let $\mathcal{M} = (\Omega, \text{rk})$ be a matroid. If e is a loop in \mathcal{M} then for any subset $A \subseteq \Omega$ we have

$$\text{rk}_{\mathcal{M}/e}(A) = \text{rk}(A \cup \{e\}).$$

Proposition 3.34. Let $\mathcal{M} = (\Omega, \mathcal{I})$ be a matroid and for some $T \subseteq \Omega$ let \mathcal{M}/T be the contraction of T . Then $\mathcal{M}/T = (\Omega - T, \hat{\mathcal{I}})$ where

$$\hat{\mathcal{I}} = \{I \subseteq \Omega - T : \mathcal{M}|T \text{ has a basis } B \text{ such that } B \cup I \in \mathcal{I}\}.$$

Proof. Denote by $\mathcal{I}_{\mathcal{M}/T}$ the set of subsets $I \subseteq \Omega - T$, which satisfy $\text{rk}_{\mathcal{M}/T}(I) = |I|$. Let \mathcal{B}_T be a basis of $\mathcal{M}|T$. We will prove the following equalities:

$$\begin{aligned} \hat{\mathcal{I}} &= \{I \subseteq \Omega - T : I \cup \mathcal{B}_T \in \mathcal{I}\} \\ &= \{I \subseteq \Omega - T : \mathcal{M}|T \text{ has a basis } \mathcal{B} \text{ such that } \mathcal{B} \cup I \in \mathcal{I}\}. \end{aligned}$$

By definition of the two sets $\{I \subseteq \Omega - T : \mathcal{M}|T \text{ has a basis } \mathcal{B} \text{ such that } \mathcal{B} \cup I \in \mathcal{I}\}$ contains $\{I \subseteq \Omega - T : I \cup \mathcal{B}_T \in \mathcal{I}\}$. Now let $I \subseteq \Omega - T$ and $\mathcal{B} \cup I \in \mathcal{I}$ for some basis \mathcal{B} of $\mathcal{M}|T$, we will show that $I \in \hat{\mathcal{I}}$. Since \mathcal{B} is an inclusion-maximal independent set in T , the set $I \cup \mathcal{B}$ is an inclusion-maximal independent set in $I \cup T$, hence $I \cup \mathcal{B}$ is a basis of $I \cup T$. Thus $\text{rk}_{\mathcal{M}}(I \cup \mathcal{B}) = \text{rk}_{\mathcal{M}}(I \cup T)$ and with $\text{rk}_{\mathcal{M}/T}(I) = \text{rk}_{\mathcal{M}}(I \cup T) - \text{rk}_{\mathcal{M}}(T)$, we get

$$\text{rk}_{\mathcal{M}/T}(I) = \text{rk}_{\mathcal{M}}(I \cup \mathcal{B}) - \text{rk}_{\mathcal{M}}(T).$$

Now since $I \cup \mathcal{B} \in \mathcal{I}$ and B is a basis of T ,

$$\text{rk}_{\mathcal{M}/T}(I) = |I \cup \mathcal{B}| - |\mathcal{B}| = |I|,$$

thus, $I \in \mathcal{I}_{\mathcal{M}/T}$.

To complete the proof, we now have to show that $\hat{\mathcal{I}} \subseteq \{I \subseteq \Omega - T : I \cup \mathcal{B}_T \in \mathcal{I}\}$. Assume $A \subseteq \hat{\mathcal{I}}$, then

$$|A| = \text{rk}_{\mathcal{M}/T}(A) = \text{rk}_{\mathcal{M}}(A \cup T) - \text{rk}_{\mathcal{M}}(T).$$

Since \mathcal{B}_T is a basis of T in \mathcal{M} , $A \cup \mathcal{B}_T$ contains a basis of $A \cup T$, hence $\text{rk}_{\mathcal{M}}(A \cup T) = \text{rk}_{\mathcal{M}}(A \cup \mathcal{B}_T)$. With \mathcal{B}_T being a basis of $\mathcal{M}|T$, this returns

$$|A| = \text{rk}_{\mathcal{M}}(A \cup \mathcal{B}_T) - |\mathcal{B}_T| \implies |A + \mathcal{B}_T| = \text{rk}_{\mathcal{M}}(A \cup \mathcal{B}_T).$$

This shows $A \cup \mathcal{B}_T \in \mathcal{I}$, completing the proof. \square

Lemma 3.35. *Let rk be a rank function of a matroid \mathcal{M} on a finite set Ω , and let rk^\perp be the rank function of its dual \mathcal{M}^\perp . Then for any subset $T \subseteq \Omega$ and $A \subseteq \Omega - T$ we have*

$$(\text{rk}_{\mathcal{M}/T})^\perp(A) = \text{rk}^\perp(A).$$

Proof. We compute

$$(\text{rk}_{\mathcal{M}/T})^\perp(A) = |A| + \text{rk}_{\mathcal{M}/T}(\overline{T} - A) - \text{rk}_{\mathcal{M}/T}(\overline{T}),$$

where $\text{rk}_{\mathcal{M}/T}(\overline{T} - A) = \text{rk}((\overline{T} - A) \cup T) - \text{rk}(T)$ and $\text{rk}_{\mathcal{M}/T}(\overline{T}) = \text{rk}(\overline{T} \cup T) - \text{rk}(T)$, hence

$$(\text{rk}_{\mathcal{M}/T})^\perp(A) = |A| + \text{rk}(\Omega - A) - \text{rk}(\Omega) = \text{rk}^\perp(A). \quad \square$$

The next lemma shows, how contraction combines the operations of deletion and taking duals for matroids.

Theorem 3.36. *For a matroid $\mathcal{M} = (\Omega, \text{rk})$ and a subset $T \subseteq \Omega$, the following holds*

$$(\mathcal{M}/T)^\perp = \mathcal{M}^\perp - T \quad \text{and} \quad \mathcal{M}^\perp/T = (\mathcal{M} - T)^\perp.$$

Proof. We can directly use the previous lemma. For the rank function of the matroid

$$(\mathcal{M}/T)^\perp = (\Omega, \text{rk}_{\mathcal{M}/T})^\perp = (\Omega - T, (\text{rk}_{\mathcal{M}/T})^\perp)$$

we have $\text{rk}_{\mathcal{M}/T}^\perp(A) = \text{rk}^\perp(A)$ for subsets $A \subseteq \Omega - T$. However, for subsets $A \subseteq \Omega - T$, the restriction of any rank function to $\Omega - T$ stays the same. Hence, $\text{rk}^\perp(A) = (\text{rk}^\perp)_{\mathcal{M}-T}(A)$ for all subsets $A \subseteq \Omega - T$. But the matroid $\mathcal{M}^\perp - T = (\Omega, \text{rk}^\perp) - T = (\Omega - T, (\text{rk}^\perp)_{\mathcal{M}-T})$ has the same rank function $(\text{rk}^\perp)_{\mathcal{M}-T}$ on subsets $A \subseteq \Omega - T$. Therefore,

$$(\mathcal{M}/T)^\perp = \mathcal{M}^\perp - T.$$

By duality,

$$(\mathcal{M}^\perp/T)^\perp = \mathcal{M}^{\perp\perp} - T = \mathcal{M} - T. \quad \square$$

Remark 3.37. If e, f are distinct elements of a matroid \mathcal{M} , then

$$(M - e)/f = (M/f) - e.$$

This shows that the resulting matroid is independent of the order of the operations. By induction for any subsets A and $B \subseteq \Omega$, we have

$$(\mathcal{M} - A)/B = (\mathcal{M}/B) - A.$$

The actions of deleting and contracting an element $e \in \mathcal{M}$ are in fact the same if and only if e is a loop or a coloop of \mathcal{M} .

Lemma 3.38. *Let e be an element of a matroid \mathcal{M} . Then $\mathcal{M} - e = M/e$ if and only if e is a loop or a coloop of \mathcal{M} .*

Proof. Let e be a loop in \mathcal{M} . Then $\text{rk}(e) = 0$, thus for a subset $A \subseteq \Omega - e$,

$$\text{rk}_{\mathcal{M}/e}(A) = \text{rk}(A \cup e) - \text{rk}(e) = \text{rk}(A \cup e).$$

We now show that, $\text{rk}(A) = \text{rk}(A \cup e)$ for a loop e :

$$\text{rk}(A) \leq \text{rk}(A \cup e) \leq \text{rk}(A) + \text{rk}(e) - \text{rk}(A \cap e) = \text{rk}(A) + 0 - \text{rk}(\emptyset) = \text{rk}(A)$$

Now let e be a coloop of a matroid \mathcal{M} , then it is a loop of the dual matroid M^\perp . With part one of this Theorem we get

$$M^\perp - e = M^\perp/e.$$

We use the duality in Theorem 3.36 and get

$$(M/e)^\perp = M^\perp - e = M^\perp/e = (M - e)^\perp,$$

where we can use Corollary 3.29 and end with

$$M/e = (M/e)^{\perp\perp} = (M - e)^{\perp\perp} = M - e. \quad \square$$

We will now introduce the glueing of two matroids.

Theorem 3.39. *Let \mathcal{M}_1 and \mathcal{M}_2 be matroids with disjoint ground sets Ω_1 and Ω_2 respectively and set of independent sets \mathcal{I}_1 and \mathcal{I}_2 respectively. Then $(\Omega_1 \cup \Omega_2, \mathcal{I})$ such that $\mathcal{I} = \{I_1 \cup I_2 \mid I_1 \in \mathcal{I}_1, I_2 \in \mathcal{I}_2\}$ is a matroid.*

Proof. Since \mathcal{M}_1 and \mathcal{M}_2 are matroids, \mathcal{I} can not be empty. Now let $I \in \mathcal{I}$. Then $I = I_1 \cup I_2$ and any subset $J \subseteq I$ is of the form $J = J_1 \cup J_2$ with $J_1 \subseteq I_1$ and $J_2 \subseteq I_2$, thus $J \in \mathcal{I}$. Therefore, properties (I1) and (I2) are satisfied. For property (I3) let I' and I'' be in \mathcal{I} with $|I''| > |I'|$ then $I' = I'_1 \cup I'_2$ and $I'' = I''_1 \cup I''_2$. Hence at least one of the following must be true: $|I''_1| > |I'_1|$ or $|I''_2| > |I'_2|$. Without loss of generality let the first case be true, then since \mathcal{I}_1 is a set of independent sets, with (I3) we can find an element $e \in I''_1$ such that $I'_1 \cup \{e\} \in \mathcal{I}_1$. Therefore $I' \cup \{e\} = I'_1 \cup \{e\} \cup I'_2 \in \mathcal{I}$. \square

Definition 3.40. We call the matroid, whose existence was established in the previous theorem, the *direct sum* of \mathcal{M}_1 and \mathcal{M}_2 and denote it by

$$\mathcal{M} = \mathcal{M}_1 \oplus \mathcal{M}_2.$$

The following theorem shows how the rank function on a direct sum of two matroids corresponds to the sum of the rank functions of those matroids, such that we can define the direct sum of two matroids as the union of the groundsets and the rank function defined as follows.

Theorem 3.41. *Let $\mathcal{M} = \mathcal{M}_1 \oplus \mathcal{M}_2$ be the direct sum of $(\mathcal{M}_1, \text{rk}_{\mathcal{M}_1})$ and $(\mathcal{M}_2, \text{rk}_{\mathcal{M}_2})$, then the rank function $\text{rk}_{\mathcal{M}}$ of \mathcal{M} satisfies*

$$\text{rk}_{\mathcal{M}}(A) = \text{rk}_{\mathcal{M}_1}(A \cap \Omega_1) + \text{rk}_{\mathcal{M}_2}(A \cap \Omega_2).$$

Proof. By the definition of the rank function, $\text{rk}_{\mathcal{M}}(A)$ is the cardinality of a basis of $\mathcal{M}|A$. By the definition of the direct sum, it is easy to see that \mathcal{B} is a basis in $\mathcal{M}|A$ if and only if $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2$ with \mathcal{B}_1 a basis in $\mathcal{M}_1|A_1$ and \mathcal{B}_2 a basis in $\mathcal{M}_2|A_2$. Then

$$\text{rk}_{\mathcal{M}}(A) = |\mathcal{B}| = |\mathcal{B}_1| + |\mathcal{B}_2| = \text{rk}_{\mathcal{M}_1}(A_1) + \text{rk}_{\mathcal{M}_2}(A_2). \quad \square$$

Example 3.42. Let us deepen our understanding of this definition by looking at the two matroids on an one-element set \mathcal{U}_1^0 and \mathcal{U}_1^1 . Then \mathcal{U}_1^0 has groundset $\{a\}$ and collection of independent sets $\{\{\emptyset\}\}$, and \mathcal{U}_1^1 has groundset $\{b\}$ and collection of independent sets $\{\emptyset, \{b\}\}$. Specifically,

$$\mathcal{U}_1^0 = (\{a\}, \{\emptyset\}), \mathcal{U}_1^1 = (\{b\}, \{\emptyset, \{b\}\}) \text{ and } \mathcal{U}_1^0 \oplus \mathcal{U}_1^1 = (\{a, b\}, \{\emptyset, \{b\}\}).$$

With the previous theorem we get

$$\text{rk}_{\mathcal{U}_1^0 \oplus \mathcal{U}_1^1}(A) = \min\{0, |A \cap \{a\}|\} + \min\{1, |A \cap \{b\}|\} = \min\{1, |A \cap \{b\}|\}$$

for any subset $A \subseteq \{a, b\}$.

Lemma 3.43. *Let \mathcal{M} be a matroid. If $e \in \mathcal{M}$ is a loop or coloop in \mathcal{M} , then*

$$\mathcal{M} = (\mathcal{M}|e) \oplus (\mathcal{M} - e)$$

Proof. We want to show that the following statement holds for the rank function on any subset of the matroid \mathcal{M} :

$$\text{rk}_{\mathcal{M}}(A) = \text{rk}_{\mathcal{M}|e}(A \cap \{e\}) + \text{rk}_{\mathcal{M}-e}(A \cap (\Omega - e)).$$

Let A be an arbitrary set of the matroid \mathcal{M} . If $e \notin A$ then by definition $\text{rk}_{\mathcal{M}}(A) = |\mathcal{B}_1|$ for some basis \mathcal{B}_1 of $\mathcal{M}|A$. More specifically, $\mathcal{B}_1 \subseteq A$ inclusion maximal and $\mathcal{B}_1 \in \mathcal{I}$. Moreover $\text{rk}_{\mathcal{M}-e}(A) = |\mathcal{B}_2|$ with \mathcal{B}_2 being a basis of $(\mathcal{M} - e)|A$. More specifically, $\mathcal{B}_2 \subseteq A$ inclusion maximal and $\mathcal{B}_2 \in \mathcal{I}(\mathcal{M} - e)$. Together, $|\mathcal{B}_2| = |\mathcal{B}_1|$, hence $\text{rk}_{\mathcal{M}}(A) = \text{rk}_{\mathcal{M}-e}(A)$. With $A \cap \{e\} = \emptyset$ we get that the following holds:

$$\text{rk}_{\mathcal{M}-e}(A) = \text{rk}_{\mathcal{M}|e}(\emptyset) + \text{rk}_{\mathcal{M}-e}(A - e) = \text{rk}_{\mathcal{M}}(A).$$

Now if $e \in A$ we need to differ between loops and coloops. Let e be a loop, then by definition $\text{rk}(e) = 0$. A loop can not be contained in any basis of a matroid, since with (I2) it would be independent itself, thus $\text{rk}(e) = 1$. Hence, if \mathcal{B} is a basis of \mathcal{M} , then $e \notin \mathcal{B}$ and the cardinality of a basis in \mathcal{M} contained in A equals the cardinality of a basis in $\mathcal{M} - e$ contained in $A - e$. Therefore,

$$\text{rk}_{\mathcal{M}-e}(A - e) = \text{rk}_{\mathcal{M}|e}(e) + \text{rk}_{\mathcal{M}-e}(A - e) = \text{rk}_{\mathcal{M}}(A)$$

is true. Lastly let $e \in A$ be a coloop, then by definition $\text{rk}^\perp(e) = 0$, hence no basis of \mathcal{M}^\perp contains e . By duality every basis of \mathcal{M} has to contain e , thus the cardinality of a basis in \mathcal{M} contained in A is the cardinality of a basis in $\mathcal{M} - e$ contained in $A - e$ increased by one. Thus

$$\text{rk}_{\mathcal{M}}(A) = \text{rk}_{\mathcal{M}|e}(e) + \text{rk}_{\mathcal{M}-e}(A - e) = 1 + \text{rk}_{\mathcal{M}-e}(A - e)$$

holds. □

3.4 The Tutte Polynomial for Matroids

After introducing matroids and their dual, we can finally define the *Tutte Polynomial*. We start by defining this two-variable polynomial through its subset expansion and compute it for some uniform matroids. Theorem 3.48 proves that the Tutte Polynomial on the the dual matroid \mathcal{M}^\perp is obtained by switching the two variables of the Tutte polynomial of \mathcal{M} . Theorem 3.50 states the deletion-contraction algorithm for the Tutte polynomial, which we use to compute the Tutte polynomial for some uniform matroids. We finish this section by proving that the Tutte polynomial is multiplicative on direct sums.

Definition 3.44. Let \mathcal{M} be a Matroid on Ω with rank function rk , we call

$$T(\mathcal{M}; x, y) = \sum_{A \subseteq \Omega} (x - 1)^{\text{rk}(\Omega) - \text{rk}(A)} (y - 1)^{\text{rk}^\perp(\Omega) - \text{rk}^\perp(\bar{A})}$$

the *Tutte Polynomial* of \mathcal{M} .

Remark 3.45. We can get rid of the dual rank function by substituting it with

$$\begin{aligned} \text{rk}^\perp(\Omega) - \text{rk}^\perp(\bar{A}) &= |\Omega| + \text{rk}(\emptyset) - \text{rk}(\Omega) - (|\bar{A}| + \text{rk}(A) - \text{rk}(\Omega)) \\ &= |A| - \text{rk}(A). \end{aligned}$$

We define the nullity of a subset A by $\text{n}(A) = |A| - \text{rk}(A)$. Now we can define the Tutte polynomial by

$$T(\mathcal{M}; x, y) = \sum_{A \subseteq \Omega} (x - 1)^{\text{rk}(\Omega) - \text{rk}(A)} (y - 1)^{\text{n}(A)}.$$

If in this definition $\text{rk}(\Omega) - \text{rk}(A) = 0$ or $|A| - \text{rk}(A) = 0$, is satisfied, we interpret $(x - 1)^0$ or $(y - 1)^0$ respectively, to have value 1 even if $x = 1$ or $y = 1$ respectively. Therefore, the empty matroid \mathcal{U}_0^0 we get $T(\mathcal{U}_0^0; x, y) = 1$.

Example 3.46. We apply this definition to the two matroids of an one element set \mathcal{U}_1^0 and \mathcal{U}_1^1 from Example 3.42 and get

$$T(\mathcal{U}_1^0; x, y) = 1 + (y - 1) = y \quad \text{and} \quad T(\mathcal{U}_1^1; x, y) = (x - 1) + 1 = x.$$

Example 3.47. We can also use our combinatorial knowledge to determine the Tutte polynomial of a uniform matroid more easily. For the rank-2 matroid on a 4-element set Ω we can divide up the set of all subsets $A \subseteq \Omega$ using their cardinality $k := |A|$. There are $\binom{n}{k}$ -many subsets of size k . Using the rank definition for uniform matroids $\text{rk}(A) = \min\{|A|, r\}$, we get

$$\begin{aligned} \binom{4}{0} (x-1)^{2-0} (y-1)^{0-0} &= \binom{4}{0} (x-1)^2 = (x-1)^2; \\ \binom{4}{1} (x-1)^{2-1} (y-1)^{1-1} &= \binom{4}{1} (x-1); \\ \binom{4}{2} (x-1)^{2-2} (y-1)^{2-2} &= \binom{4}{2}; \\ \binom{4}{3} (x-1)^{2-2} (y-1)^{3-2} &= \binom{4}{3} (y-1); \\ \binom{4}{4} (x-1)^{2-2} (y-1)^{4-2} &= (y-1)^2. \end{aligned}$$

Thus,

$$\begin{aligned} T(U_4^2; x, y) &= (x-1)^2 + \binom{4}{1} (x-1) + \binom{4}{2} + \binom{4}{3} (y-1) + (y-1)^2 \\ &= x^2 + 2x + 2y + y^2. \end{aligned}$$

In the previous example, the Tutte polynomial of the uniform matroid did not have summands containing the product xy . In fact, this is not surprising. Let \mathcal{U}_n^r be a rank- r uniform matroid and $A \subseteq \Omega$. Either $r > |A|$ or $r \leq |A|$ is satisfied, thus we can bipartite Ω and get

$$T(U_n^r; x, y) = \sum_{\substack{A \subseteq \Omega \\ |A| < r}} (x-1)^{\text{rk}(\Omega) - \text{rk}(A)} (y-1)^{\text{n}(A)} + \sum_{\substack{A \subseteq \Omega \\ |A| \geq r}} (x-1)^{\text{rk}(\Omega) - \text{rk}(A)} (y-1)^{\text{n}(A)}.$$

If $r > |A|$, then

$$\text{rk}(\Omega) - \text{rk}(A) = \min\{|\Omega|, r\} - \min\{|A|, r\} = r - |A|$$

and

$$|A| - \text{rk}(A) = |A| - \min\{|A|, r\} = |A| - |A| = 0.$$

If $r \leq |A|$, then

$$\text{rk}(\Omega) - \text{rk}(A) = \min\{|\Omega|, r\} - \min\{|A|, r\} = r - r = 0$$

and

$$|A| - \mathbf{rk}(A) = |A| - r.$$

Together this results in

$$T(\mathcal{U}_n^r; x, y) = \sum_{\substack{A \subseteq \Omega \\ |A| < r}} (x-1)^{r-|A|} + \sum_{\substack{A \subseteq \Omega \\ |A| \geq r}} (y-1)^{|A|-r}.$$

Using the binomial theorem and other combinatorial identities for the binomial coefficient, it is possible to show the following formula from [EMM22]:

$$T(\mathcal{U}_n^r; x, y) = \begin{cases} x^n & \text{if } r = n; \\ y^n & \text{if } r = 0; \end{cases}$$

and otherwise,

$$T(\mathcal{U}_n^r; x, y) = \sum_{i=0}^{r-1} \binom{n-r-1+i}{i} x^{r-i} + \sum_{j=0}^{n-r-1} \binom{r-1+j}{j} y^{n-r-j}.$$

The next theorem shows how the Tutte polynomial of a matroid corresponds to the Tutte polynomial of its dual.

Theorem 3.48. *Let \mathcal{M} be a matroid, and \mathcal{M}^\perp be its dual, then*

$$T(\mathcal{M}^\perp; x, y) = T(\mathcal{M}; y, x).$$

Proof. We will show that $\mathbf{rk}^\perp(\Omega) - \mathbf{rk}^\perp(A) = \mathbf{n}(\bar{A})$ and $\mathbf{n}^\perp(A) = \mathbf{rk}(\Omega) - \mathbf{rk}(\bar{A})$. This suffices because the summation includes every subset $A \subseteq \Omega$. Using the definition of the dual rank function and the dual nullity function, we get

$$\mathbf{rk}^\perp(\Omega) - \mathbf{rk}^\perp(A) = |\Omega| - \mathbf{rk}(\Omega) - |A| - \mathbf{rk}(\bar{A}) + \mathbf{rk}(\Omega) = |\bar{A}| - \mathbf{rk}(\bar{A}) = \mathbf{n}(\bar{A})$$

and

$$\mathbf{n}^\perp(A) = |A| - \mathbf{rk}^\perp(A) = |A| - |A| - \mathbf{rk}(\bar{A}) + \mathbf{rk}(\Omega) = \mathbf{rk}(\Omega) - \mathbf{rk}(\bar{A}). \quad \square$$

Lemma 3.49. *Let $M = (\Omega, \mathbf{rk})$ be a matroid. Then*

$$\mathbf{rk}(\Omega) = \begin{cases} \mathbf{rk}(\Omega - e) + 1, & \text{if } e \text{ is a coloop;} \\ \mathbf{rk}(\Omega - e), & \text{otherwise.} \end{cases} \quad (3.2)$$

Let $\mathbf{rk}_{\mathcal{M}/e}$ and $\mathbf{n}_{\mathcal{M}/e}$ denote the rank and nullity functions of \mathcal{M}/e , then for all subsets $A \subseteq \Omega - e$ we have

$$\mathbf{rk}_{\mathcal{M}/e}(A) = \begin{cases} \mathbf{rk}(A \cup e), & \text{if } e \text{ is a loop;} \\ \mathbf{rk}(A \cup e) - 1, & \text{otherwise;} \end{cases} \quad (3.3)$$

and

$$\mathbf{n}_{\mathcal{M}/e}(A) = \begin{cases} \mathbf{n}(A \cup e) - 1, & \text{if } e \text{ is a loop;} \\ \mathbf{n}(A \cup e), & \text{otherwise.} \end{cases} \quad (3.4)$$

Proof. It was already proven that $\text{rk}(\Omega - e) = \text{rk}(\Omega) - 1$ if and only if e is a coloop. If e is not a coloop, then

$$\begin{aligned} 1 &= rk^\perp(e) = |e| + \text{rk}(\Omega - e) - \text{rk}(\Omega) = 1 + \text{rk}(\Omega - e) - \text{rk}(\Omega) \\ &\iff \text{rk}(\Omega - e) = \text{rk}(\Omega) \end{aligned}$$

Now for the rank and nullity functions of \mathcal{M}/e we use their definitions:

$$\text{rk}_{\mathcal{M}/e}(A) = \text{rk}(A \cup e) - \text{rk}(e).$$

If e is a loop $\text{rk}(e) = 0$. Otherwise $0 < \text{rk}(e) \leq |\{e\}| = 1$. Moreover,

$$\text{n}_{\mathcal{M}/e}(A) = |A| - \text{rk}_{\mathcal{M}/e}(A) = |A| - \text{rk}(A \cup e) + \text{rk}(e).$$

If e is a loop we get

$$\text{n}_{\mathcal{M}/e}(A) = |A \cup e| - 1 - \text{rk}(A \cup e) = \text{n}(A \cup e) - 1$$

and otherwise

$$\text{n}_{\mathcal{M}/e}(A) = |A| - \text{rk}(A \cup e) + 1 = |A \cup e| - \text{rk}(A \cup e) = \text{n}(A \cup e).$$

□

With this lemma we can now formulate the deletion-contraction algorithm of the Tutte polynomial.

Theorem 3.50. *Let e be an element of a matroid \mathcal{M} . Then*

$$T(\mathcal{M}; x, y) = \begin{cases} 1, & \text{if } \Omega = \emptyset; \\ yT(\mathcal{M} - e; x, y), & \text{if } e \text{ is a loop}; \\ xT(\mathcal{M}/e; x, y), & \text{if } e \text{ is a coloop}; \\ T(\mathcal{M} - e; x, y) + T(\mathcal{M}/e; x, y), & \text{otherwise.} \end{cases}$$

Proof. Let e be an element of the matroid $M = (\Omega, \text{rk})$. Clearly

$$T(M; x, y) = \sum_{\substack{A \subseteq \Omega \\ e \notin A}} (x-1)^{\text{rk}(\Omega) - \text{rk}(A)} (y-1)^{\text{n}(A)} + \sum_{\substack{A \subseteq \Omega \\ e \in A}} (x-1)^{\text{rk}(\Omega) - \text{rk}(A)} (y-1)^{\text{n}(A)}. \quad (3.5)$$

Let us look at the first term on the right hand side, where

$$\sum_{\substack{A \subseteq \Omega \\ e \notin A}} (x-1)^{\text{rk}(\Omega) - \text{rk}(A)} (y-1)^{\text{n}(A)} = \sum_{A \subseteq \Omega - e} (x-1)^{\text{rk}(\Omega) - \text{rk}(A)} (y-1)^{\text{n}(A)}.$$

Now using (3.2) from the previous lemma we get

$$\sum_{\substack{A \subseteq \Omega \\ e \notin A}} (x-1)^{\text{rk}(\Omega) - \text{rk}(A)} (y-1)^{\text{n}(A)} = \begin{cases} (x-1) \sum_{A \subseteq \Omega - e} x^{\text{rk}(\Omega - e) - \text{rk}(A)} y^{\text{n}(A)}, & \text{if } e \text{ is a coloop}; \\ \sum_{A \subseteq \Omega - e} x^{\text{rk}(\Omega - e) - \text{rk}(A)} y^{\text{n}(A)}, & \text{otherwise.} \end{cases}$$

Hence

$$\sum_{\substack{A \subseteq \Omega \\ e \notin A}} (x-1)^{\mathbf{rk}(\Omega) - \mathbf{rk}(A)} (y-1)^{\mathbf{n}(A)} = \begin{cases} (x-1)T(\mathcal{M} - e; x, y), & \text{if } e \text{ is a coloop;} \\ T(\mathcal{M} - e; x, y), & \text{otherwise.} \end{cases} \quad (3.6)$$

Now consider the second term on the right-hand side of (3.5). With

$$\sum_{\substack{A \subseteq \Omega \\ e \in A}} (x-1)^{\mathbf{rk}(\Omega) - \mathbf{rk}(A)} (y-1)^{\mathbf{n}(A)} = \sum_{A \subseteq \Omega - e} (x-1)^{\mathbf{rk}((\Omega - e) \cup e) - \mathbf{rk}(A \cup e)} (y-1)^{\mathbf{n}(A \cup e)}$$

and (3.3) and (3.4) we get

$$\begin{aligned} & \sum_{\substack{A \subseteq \Omega \\ e \in A}} (x-1)^{\mathbf{rk}(\Omega) - \mathbf{rk}(A)} (y-1)^{\mathbf{n}(A)} \\ &= \begin{cases} (y-1) \sum_{A \subseteq \Omega - e} (x-1)^{\mathbf{rk}_{\mathcal{M}/e}(\Omega - e) - \mathbf{rk}_{\mathcal{M}/e}(A)} (y-1)^{\mathbf{n}_{\mathcal{M}/e}(A)}, & \text{if } e \text{ is a loop;} \\ \sum_{A \subseteq \Omega - e} (x-1)^{\mathbf{rk}_{\mathcal{M}/e}(\Omega - e) - \mathbf{rk}_{\mathcal{M}/e}(A)} (y-1)^{\mathbf{n}_{\mathcal{M}/e}(A)}, & \text{otherwise.} \end{cases} \end{aligned}$$

Hence

$$\sum_{\substack{A \subseteq \Omega \\ e \in \Omega}} (x-1)^{\mathbf{rk}(\Omega) - \mathbf{rk}(A)} (y-1)^{\mathbf{n}(A)} = \begin{cases} (y-1)T(\mathcal{M}/e; x, y), & \text{if } e \text{ is a loop;} \\ T(\mathcal{M}/e; x, y), & \text{otherwise.} \end{cases} \quad (3.7)$$

Now by substituting (3.6) and (3.7) into (3.5), we obtain

$$T(\mathcal{M}; x, y) = \begin{cases} yT(\mathcal{M}/e; x, y) & \text{if } e \text{ is a loop,} \\ xT(\mathcal{M} - e; x, y) & \text{if } e \text{ is a coloop,} \\ T(\mathcal{M} - e; x, y) + T(\mathcal{M}/e; x, y) & \text{otherwise.} \end{cases}$$

The result now follows with Lemma 3.38, which states that $\mathcal{M} - e = \mathcal{M}/e$ if and only if e is a loop or a coloop of \mathcal{M} . \square

Remark 3.51. From the previous theorem it is obvious, that if \mathcal{M} is a matroid with k bridges and l loops and no other edges, then its Tutte polynomial is $T(\mathcal{M}; x, y) = x^k y^l$.

Example 3.52. The Tutte polynomial for the two matroids on an one-element set are also easily determined with this equivalent definition. For the rank-0 uniform matroid we see that $e = \{1\}$ is a loop, since $\mathbf{rk}(\{1\}) = 0$. Therefore

$$T(\mathcal{U}_1^0; x, y) = y \cdot T(\mathcal{U}_1^0 - \{1\}; x, y) = y \cdot T(\mathcal{U}_0^0; x, y) = y \cdot 1 = y.$$

The dual matroid $(\mathcal{U}_1^1)^\perp$ has rank function $\mathbf{rk}^\perp(A) = |A| - \min(|\overline{A}|, 1) - 0$. Thus for $A = \{1\}$ we get $\mathbf{rk}^\perp(\{1\}) = 1 - 1 = 0$, which means that $\{1\}$ is a coloop in \mathcal{U}_1^1 . Therefore

$$T(\mathcal{U}_1^1; x, y) = x \cdot T(\mathcal{U}_1^1 / \{1\}; x, y) = x \cdot T((\emptyset, \mathbf{rk}_{\mathcal{U}_1^1 / \{1\}}); x, y) = x \cdot T((\emptyset, 1); x, y) = x \cdot 1 = x.$$

The following theorem proves that the Tutte polynomial is multiplicative on direct sums. We will use this in the next section to argue that the Tutte polynomial is a Tutte-Grothendieck invariant.

Theorem 3.53. *Let \mathcal{M}_1 and \mathcal{M}_2 be two matroids. Then*

$$T(\mathcal{M}_1 \oplus \mathcal{M}_2; x, y) = T(\mathcal{M}_1; x, y) \cdot T(\mathcal{M}_2; x, y).$$

Proof. Let $\mathcal{M} := \mathcal{M}_1 \oplus \mathcal{M}_2$ and A be a subset of $\Omega = \Omega_1 \cup \Omega_2$. We can write $A = A_1 \cup A_2$ such that $A_1 \subseteq \Omega_1$ and $A_2 \subseteq \Omega_2$. Therefore

$$T(\mathcal{M}_1 \oplus \mathcal{M}_2; x, y) = \sum_{A \subseteq \Omega_1 \cup \Omega_2} (x-1)^{\text{rk}_{\mathcal{M}}(\Omega_1 \cup \Omega_2) - \text{rk}_{\mathcal{M}}(A_1 \cup A_2)} (y-1)^{|A_1 \cup A_2| - \text{rk}_{\mathcal{M}}(A_1 \cup A_2)}. \quad (3.8)$$

Now we can use Theorem 3.41, such that the right hand side of equation (3.8) equals

$$\sum_{A_1 \subseteq \Omega_1} \sum_{A_2 \subseteq \Omega_2} (x-1)^{\text{rk}_{\mathcal{M}_1}(\Omega_1) + \text{rk}_{\mathcal{M}_2}(\Omega_2) - \text{rk}_{\mathcal{M}_1}(A_1) - \text{rk}_{\mathcal{M}_2}(A_2)} (y-1)^{|A_1| + |A_2| - \text{rk}_{\mathcal{M}_1}(A_1) - \text{rk}_{\mathcal{M}_2}(A_2)}.$$

Using that exponents are either dependent of subsets of Ω_1 or Ω_2 we get

$$\begin{aligned} & \sum_{A_1 \subseteq \Omega_1} (x-1)^{\text{rk}_{\mathcal{M}_1}(\Omega_1) - \text{rk}_{\mathcal{M}_1}(A_1)} (y-1)^{|A_1| - \text{rk}_{\mathcal{M}_1}(A_1)} \\ & \quad \cdot \sum_{A_2 \subseteq \Omega_2} (x-1)^{\text{rk}_{\mathcal{M}_2}(\Omega_2) - \text{rk}_{\mathcal{M}_2}(A_2)} (y-1)^{|A_2| - \text{rk}_{\mathcal{M}_2}(A_2)}. \end{aligned}$$

But this is exactly the product of the Tutte Polynomials

$$T(\mathcal{M}_1 \oplus \mathcal{M}_2; x, y) = T(\mathcal{M}_1; x, y) \cdot T(\mathcal{M}_2; x, y). \quad \square$$

Example 3.54. Continuing our example of the two matroids on an one-element set and considering their direct sum from Example 3.42 again, this theorem tells us

$$T(\mathcal{U}_1^0 \oplus \mathcal{U}_1^1; x, y) = x \cdot y.$$

3.5 The Tutte Polynomial as a Matroid Invariant

In this section, we define *matroid isomorphisms* and *matroid isomorphism invariants*, specifically the *Tutte-Grothendieck invariants*. We also talk about the *characteristic polynomial* of a matroid and use its characteristics to argue that it is in fact a Tutte-Grothendieck invariant. We prove the *recipe theorem* of Dominic Welsh in Theorem 3.61 and show that the characteristic polynomial of a matroid is in fact just a specialization of the Tutte polynomial.

Definition 3.55. Let \mathcal{M}_1 and \mathcal{M}_2 be two matroids and $\psi : \Omega_1 \rightarrow \Omega_2$ be a bijection such that for all $A \subseteq \Omega_1$ the set $\psi(A)$ is independent in \mathcal{M}_2 if and only if A is independent in \mathcal{M}_1 . We call such a bijection ψ an *isomorphism* from \mathcal{M}_1 to \mathcal{M}_2 , say \mathcal{M}_1 and \mathcal{M}_2 are *isomorphic* and denote it by $\mathcal{M}_1 \cong \mathcal{M}_2$.

Definition 3.56. A *matroid isomorphism invariant* is a function f on the class of all matroids, such that if $\mathcal{M}_1 \cong \mathcal{M}_2$ then $f(\mathcal{M}_1) = f(\mathcal{M}_2)$.

Theorem 3.57. *The Tutte polynomial is a matroid isomorphism invariant.*

Proof. Let $\mathcal{M}_1 = (\Omega_1, \mathcal{I}_1)$ and $\mathcal{M}_2 = (\Omega_2, \mathcal{I}_2)$ be two matroids and let $\psi : \mathcal{M}_1 \rightarrow \mathcal{M}_2$ be a matroid isomorphism. Then by definition of bijection, $|A| = |\psi(A)|$ for any subset $A \subseteq \Omega_1$, particularly $|I_1| = |\psi(I_1)|$ for any independent set $I_1 \in \mathcal{I}_1$. Since the rank function of a set A is defined as the cardinality of any inclusion-maximal independent set contained in A , all values needed for the computation of the Tutte Polynomial are constant under the isomorphism. In particular, $\text{rk}(\Omega_1) = \text{rk}(\Omega_2)$, $\text{rk}(A) = \text{rk}(\psi(A))$ and $|A| = |\psi(A)|$, for all $A \subseteq \Omega_1$. Together,

$$T(\mathcal{M}_1; x, y) = T(\mathcal{M}_2; x, y). \quad \square$$

We want to point out once more, that the rank function of a subset does not alter under matroid isomorphisms. Evaluating the Tutte polynomial for specific x and y values returns information about different attributes of the matroid.

Theorem 3.58. *Let $\mathcal{M} = (\Omega, \text{rk})$ be a matroid. Then we have the following evaluations:*

1. $T(\mathcal{M}; 1, 1)$ is the number of bases of \mathcal{M} ,
2. $T(\mathcal{M}; 2, 1)$ is the number of independent sets of \mathcal{M} ,
3. $T(\mathcal{M}; 1, 2)$ is the number of spanning sets of \mathcal{M} ,
4. $T(\mathcal{M}; 2, 2) = 2^{|\Omega|}$.

Proof. Firstly,

$$T(\mathcal{M}; 1, 1) = \sum_{A \subseteq \Omega} 0^{\text{rk}(\Omega) - \text{rk}(A)} \cdot 0^{|A| - \text{rk}(A)}$$

and

$$0^{\text{rk}(\Omega) - \text{rk}(A)} \cdot 0^{|A| - \text{rk}(A)} \neq 0 \iff \text{rk}(\Omega) = \text{rk}(A) \wedge |A| = \text{rk}(A),$$

therefore A is an independent set and has size $\text{rk}(\Omega)$, hence A is a basis. Secondly,

$$T(\mathcal{M}; 2, 1) = \sum_{A \subseteq \Omega} 1^{\text{rk}(\Omega) - \text{rk}(A)} 0^{|A| - \text{rk}(A)} = \sum_{A \subseteq \Omega} 0^{|A| - \text{rk}(A)}$$

and

$$0^{|A| - \text{rk}(A)} \neq 0 \iff |A| = \text{rk}(A),$$

thus this counts the number of independent sets. Thirdly,

$$T(\mathcal{M}; 1, 2) = \sum_{A \subseteq \Omega} 0^{\text{rk}(\Omega) - \text{rk}(A)} \cdot 1^{|A| - \text{rk}(A)} = \sum_{A \subseteq \Omega} 0^{\text{rk}(\Omega) - \text{rk}(A)}$$

and

$$0^{\text{rk}(\Omega) - \text{rk}(A)} \neq 0 \iff \text{rk}(\Omega) = \text{rk}(A)$$

which is true if and only if A is a spanning set. Lastly,

$$T(\mathcal{M}; 2, 2) = \sum_{A \subseteq \Omega} 1^{\text{rk}(\Omega) - \text{rk}(A)} \cdot 1^{|A| - \text{rk}(A)} = \sum_{A \subseteq \Omega} 1 = |\mathcal{P}(\Omega)| = 2^{|\Omega|} \quad \square$$

In Chapter 2 we discussed different graph invariants. We will now introduce a matroid invariant that is computable through a recursive deletion-contraction algorithm.

Definition 3.59. The *characteristic polynomial* $\chi(\mathcal{M}; \lambda)$ of a matroid \mathcal{M} is

$$\chi(\mathcal{M}; \lambda) = \sum_{A \subseteq \Omega} (-1)^{|A|} \lambda^{\text{rk}(\mathcal{M}) - \text{rk}(A)}.$$

This polynomial is also known as the *chromatic polynomial* of \mathcal{M} .

Definition 3.60. Let \mathcal{C} be a class of matroids that is closed under isomorphism and the taking of minors. Let \mathfrak{R} be a commutative ring with unity. An isomorphism invariant $f : \mathcal{C} \rightarrow \mathfrak{R}$ is called a *Tutte-Grothendieck invariant* or *T-G-invariant* if it satisfies the following conditions for every matroid $\mathcal{M}, \mathcal{M}_1, \mathcal{M}_2$ in \mathcal{C} and every element e of \mathcal{M} .

- 1) (Deletion-contraction) $f(\mathcal{M}) = f(\mathcal{M} - e) + f(\mathcal{M}/e)$ if e is ordinary in \mathcal{M} ;
- 2) (Direct sum) $f(\mathcal{M}_1 \oplus \mathcal{M}_2) = f(\mathcal{M}_1)f(\mathcal{M}_2)$.

As discussed in [Zas87] by Thomas Zaslavsky, it is possible to prove that the characteristic polynomial of a matroid is a T-G-invariant by showing that for arbitrary matroids $\mathcal{M}, \mathcal{M}_1, \mathcal{M}_2$, it satisfies

$$\chi(\mathcal{M}; \lambda) = \chi(\mathcal{M} - e; \lambda) - \chi(\mathcal{M}/e; \lambda),$$

if e is not a coloop, and

$$\chi(\mathcal{M}_1 \oplus \mathcal{M}_2) = \chi(\mathcal{M}_1) \cdot \chi(\mathcal{M}_2).$$

We will refrain from proving this, because we would need to introduce the so-called *Möbius invariant* and discuss its characteristics. However, we only want to give an example of a matroid isomorphism invariant, that is a T-G-invariant for matroids. According to the following theorem, we will then be able to prove that the characteristic polynomial is just a specialization of the Tutte polynomial.

By Theorems 3.50 and 3.53 the Tutte polynomial is a T-G-invariant, it is in fact the universal Tutte-Grothendieck invariant. Dominic Welsh [Wel99] called this result the *Recipe Theorem* and that name has persisted. We will replace the deletion-contraction formula by a more general recursion. Thus we will not only prove that any T-G-invariant is an evaluation of the Tutte-polynomial, but also any function that satisfies the modified deletion-contraction formula.

Theorem 3.61 (Recipe Theorem). *Let σ and τ be elements of a field \mathbb{F} . Let \mathcal{C} be a class of matroids that is closed under direct sums and the taking of minors. Furthermore let f be an isomorphism invariant mapping \mathcal{C} into \mathbb{F} . Suppose f satisfies the following recursions for all matroids \mathcal{M} and all elements $e \in \mathcal{M}$:*

- 1) $f(\mathcal{M}) = \sigma f(\mathcal{M} - e) + \tau f(\mathcal{M}/e)$ if e is neither a loop nor a coloop of \mathcal{M} ;
- 2) $f(\mathcal{M}_1 \oplus \mathcal{M}_2) = f(\mathcal{M}_1)f(\mathcal{M}_2)$ for any matroids $\mathcal{M}_1, \mathcal{M}_2 \in \mathcal{C}$.

Then

$$f(\mathcal{M}) = \sigma^{|\Omega| - \text{rk}(\Omega)} \tau^{\text{rk}(\Omega)} T\left(\mathcal{M}; \frac{x_0}{\tau}, \frac{y_0}{\sigma}\right),$$

where x_0, y_0 are the values f takes on coloops and loops respectively.

Remark 3.62. Condition 2) of a T-G-invariant gives information about what it does on an empty set. Namely let $\mathcal{M} = (\emptyset, \{\emptyset\})$, then $f(\mathcal{M}) = f(\mathcal{M} \oplus \mathcal{M}) = f(\mathcal{M})f(\mathcal{M})$, which can only be true if $f(\mathcal{M}) = 1$. After we have established this result, we can substitute condition 2 with the following conditions:

2.1) $f(\mathcal{M}) = 1$, where \mathcal{M} is the matroid on a empty set.

2.2) $f(\mathcal{M}) = f(\mathcal{M}|e)f(\mathcal{M} - e)$, where \mathcal{M} is any matroid and e is either a loop or coloop.

Condition 2.2) follows from condition 2) by Lemma 3.45, since $\mathcal{M} = \mathcal{M}|e \oplus \mathcal{M} - e$ for any matroid \mathcal{M} if e is a loop or coloop of \mathcal{M} . Therefore condition 2) is equivalent to 2.1) and 2.2).

Proof of Theorem 3.62. We will prove by induction on the cardinality of the ground set Ω . First let $|\Omega| = 0$, this is possible if and only if the matroid on Ω is $\mathcal{M} = (\emptyset, \{\emptyset\})$. As established in the last remark $f(\mathcal{M}) = 1$ and with $\text{rk}(\emptyset) = 0$ and $T((\emptyset, \{\emptyset\}); \frac{x_0}{\tau}, \frac{y_0}{\sigma}) = 1$ we get

$$1 = f(\mathcal{M}) = \sigma^0 \tau^0 \cdot 1 = 1.$$

Let $\mathcal{M} = (\Omega, \mathcal{I})$ be an arbitrary matroid with ground set Ω such that $|\Omega| = m + 1$ for some $m \in \mathbb{N}$. Suppose the statement holds for all matroids with ground set $\Omega - e$ for any element $e \in \Omega$. Then for the inductive step we want to show that the statement holds for $\mathcal{M} = (\Omega, \mathcal{I})$. First let e be a loop in \mathcal{M} , then as noted before $f(\mathcal{M}) = f(\mathcal{M}|e)f(\mathcal{M} - e)$. With $f(\mathcal{M}|e) = y_0$, since e is a loop, we get

$$f(\mathcal{M}) = f(\mathcal{M}|e)f(\mathcal{M} - e) = y_0 \cdot f(\mathcal{M} - e).$$

Because $\mathcal{M} - e$ is a matroid on $\Omega - e$ the induction hypothesis holds for this matroid, hence it is a specialization of the Tutte polynomial and

$$f(\mathcal{M}) = y_0 \cdot \sigma^{|\Omega - e| - \text{rk}_{\mathcal{M} - e}(\Omega - e)} \tau^{\text{rk}_{\mathcal{M} - e}(\Omega - e)} T\left(\mathcal{M} - e; \frac{x_0}{\tau}, \frac{y_0}{\sigma}\right).$$

We know $\mathcal{M} - e = \mathcal{M}/e$ for a loop and $\text{rk}_{\mathcal{M}/e}(\Omega - e) = \text{rk}_{\mathcal{M}}(\Omega - e \cup e) = \text{rk}_{\mathcal{M}}(\Omega)$, hence we can conclude

$$f(\mathcal{M}) = y_0 \cdot \sigma^{|\Omega - e| - \text{rk}_{\mathcal{M}}(\Omega)} \tau^{\text{rk}_{\mathcal{M}}(\Omega)} T\left(\mathcal{M} - e; \frac{x_0}{\tau}, \frac{y_0}{\sigma}\right). \quad (3.9)$$

Now with Theorem 3.50, since e is a loop, we have

$$\frac{y_0}{\sigma} \cdot T\left(\mathcal{M} - e; \frac{x_0}{\tau}, \frac{y_0}{\sigma}\right) = T\left(\mathcal{M}; \frac{x_0}{\tau}, \frac{y_0}{\sigma}\right).$$

Thus, continuing equation (3.9), we proved the statement:

$$f(\mathcal{M}) = \sigma^{|\Omega| - \text{rk}_{\mathcal{M}}(\Omega)} \tau^{\text{rk}_{\mathcal{M}}(\Omega)} T\left(\mathcal{M}; \frac{x_0}{\tau}, \frac{y_0}{\sigma}\right).$$

Now let e be a coloop in \mathcal{M} . Then $f(\mathcal{M}) = f(\mathcal{M}|e)f(\mathcal{M} - e)$ and $f(\mathcal{M}|e) = x_0$, since e is a coloop. Therefore,

$$f(\mathcal{M}) = f(\mathcal{M}|e)f(\mathcal{M} - e) = x_0 \cdot f(\mathcal{M} - e),$$

and again $\mathcal{M} - e$ is a matroid on $\Omega - e$, hence the induction hypothesis holds, stating

$$f(\mathcal{M}) = x_0 \cdot \sigma^{|\Omega - e| - \text{rk}_{\mathcal{M} - e}(\Omega - e)} \tau^{\text{rk}_{\mathcal{M} - e}(\Omega - e)} T\left(\mathcal{M} - e; \frac{x_0}{\tau}, \frac{y_0}{\sigma}\right).$$

Now we can use Lemma 3.49 for the coloop e , hence $\text{rk}(\Omega) = \text{rk}(\Omega - e) + 1$ and we get

$$f(\mathcal{M}) = x_0 \cdot \sigma^{|\Omega| - \text{rk}_{\mathcal{M}}(\Omega)} \tau^{\text{rk}_{\mathcal{M}}(\Omega) - 1} T\left(\mathcal{M} - e; \frac{x_0}{\tau}, \frac{y_0}{\sigma}\right). \quad (3.10)$$

Because e is a coloop, we again have $\mathcal{M} - e = \mathcal{M}/e$. Therefore Theorem 3.50 gives us

$$\frac{x_0}{\tau} T\left(\mathcal{M} - e; \frac{x_0}{\tau}, \frac{y_0}{\sigma}\right) = \frac{x_0}{\tau} T\left(\mathcal{M}/e; \frac{x_0}{\tau}, \frac{y_0}{\sigma}\right) = T\left(\mathcal{M}; \frac{x_0}{\tau}, \frac{y_0}{\sigma}\right)$$

Finally equation (3.10) proves the statement for a coloop:

$$f(\mathcal{M}) = \sigma^{|\Omega| - \text{rk}_{\mathcal{M}}(\Omega)} \tau^{\text{rk}_{\mathcal{M}}(\Omega)} T\left(\mathcal{M}; \frac{x_0}{\tau}, \frac{y_0}{\sigma}\right).$$

Lastly, let e be an element that is ordinary, then by condition 1) of a T-G-invariant we have

$$f(\mathcal{M}) = \sigma f(\mathcal{M} - e) + \tau f(\mathcal{M}/e).$$

and we can use the induction hypothesis for $\mathcal{M} - e$ and \mathcal{M}/e , which returns

$$\begin{aligned} f(\mathcal{M}) = & \sigma(\sigma^{|\Omega - e| - \text{rk}_{\mathcal{M} - e}(\Omega - e)} \tau^{\text{rk}_{\mathcal{M} - e}(\Omega - e)} T\left(\mathcal{M} - e; \frac{x_0}{\tau}, \frac{y_0}{\sigma}\right) + \\ & \tau(\sigma^{|\Omega - e| - \text{rk}_{\mathcal{M}/e}(\Omega - e)} \tau^{\text{rk}_{\mathcal{M}/e}(\Omega - e)} T\left(\mathcal{M}/e; \frac{x_0}{\tau}, \frac{y_0}{\sigma}\right)). \end{aligned}$$

We can use $\text{rk}_{\mathcal{M} - e}(\Omega - e) = \text{rk}_{\mathcal{M}}(\Omega - e)$, $\text{rk}_{\mathcal{M}/e}(\Omega - e) = \text{rk}_{\mathcal{M}}(\Omega) - 1$ from Lemma 3.49 for ordinary elements of a matroid. This will leave us with

$$f(\mathcal{M}) = \sigma^{|\Omega| - \text{rk}_{\mathcal{M}}(\Omega)} \tau^{\text{rk}_{\mathcal{M}}(\Omega)} \left(T\left(\mathcal{M} - e; \frac{x_0}{\tau}, \frac{y_0}{\sigma}\right) + T\left(\mathcal{M}/e; \frac{x_0}{\tau}, \frac{y_0}{\sigma}\right) \right). \quad (3.11)$$

We can again use Theorem 3.50 to obtain

$$T\left(\mathcal{M} - e; \frac{x_0}{\tau}, \frac{y_0}{\sigma}\right) + T\left(\mathcal{M}/e; \frac{x_0}{\tau}, \frac{y_0}{\sigma}\right) = T\left(\mathcal{M}; \frac{x_0}{\tau}, \frac{y_0}{\sigma}\right)$$

and get with equation (3.11) the final result

$$f(\mathcal{M}) = \sigma^{|\Omega| - \text{rk}_{\mathcal{M}}(\Omega)} \tau^{\text{rk}_{\mathcal{M}}(\Omega)} T\left(\mathcal{M}; \frac{x_0}{\tau}, \frac{y_0}{\sigma}\right). \quad \square$$

We are closing this chapter by showing that the characteristic polynomial of a matroid is just a specialization of the Tutte polynomial. Let $\mathcal{M} = (\Omega, \text{rk})$ be a matroid. Then

$$\chi(\mathcal{M}; \lambda) = (-1)^{\text{rk}(\Omega)} T(\mathcal{M}; 1 - \lambda, 0).$$

We have seen that χ is a Tutte-Grothendieck invariant. Hence we only need to insert the specific values into the recipe theorem, where $\sigma = 1$, $\tau = -1$, $y_0 = 0$ and $x_0 = \lambda - 1$. Thus,

$$\chi(\mathcal{M}; \lambda) = (-1)^{\text{rk}(\Omega)} T\left(\mathcal{M}; \frac{\lambda - 1}{-1}, 0\right).$$

4 Graphs as Matroids

In the last two chapters we introduced graphs and matroids independently. We now want to give detailed connections between the two notions. The goal of this chapter is to show that graph polynomials introduced in Chapter 2 are specializations of the Tutte polynomial for graphs. In Section 4.1 we start by defining the matroid for a given graph G , called the *Cycle Matroid*, and discuss a convenient way to deduce the rank of a subset from the drawing of the graph G . We introduce the dual matroid to the cycle matroid, called the *Bond Matroid* and shortly discuss so-called *graphic* matroids. In Section 4.3 we use the cycle matroid of a graph to define the Tutte polynomial of a graph, which is also computable by a deletion-contraction algorithm. Lastly, in Section 4.4 we consider the Tutte polynomial as a graph invariant and define Tutte-Grothendieck invariants for graphs. This enables us to state and prove the recipe theorem for graphs. Unfortunately, the polynomials in Chapter 2 do not satisfy all conditions to be T-G-invariants for graphs, so that we need to modify the recipe theorem. Using the modified recipe theorem, we are then able to directly prove that the chromatic polynomial, the flow polynomial and the reliability polynomial are all specializations of the Tutte polynomial for graphs.

4.1 The Cycle Matroid

This section provides a short overview of the most important properties of a matroid deduced from a graph G . The matroid is constructed by taking the set of edges $E(G)$ as ground set and defining a rank function on the subsets of $E(G)$. The most useful information of this section is Theorem 4.3, where we prove that the rank of a subset can be directly read off of the drawing of a graph. More specifically, we obtain the rank of a subset by subtracting the number of components of the underlying subgraph from the number of vertices of G . We finish this section by showing that deleting or contracting a set from the cycle matroid of G is equal to deleting or contracting the set from G and constructing the cycle matroid afterwards. With this information, everything that was proven for matroids in Chapter 3 holds for cycle matroids too.

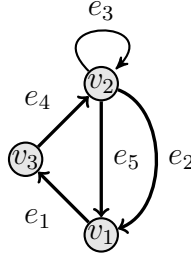
Definition 4.1. Let $G = (V, E)$ be a graph with $|V| = n$ and I be the incidence matrix of an arbitrary orientation of G . Let $\Omega := E(G)$ and for a subset $A \subseteq E$ we identify the elements of A with the corresponding columns of I by $e_i \in A$ only if $i \in S \subseteq \{1, \dots, n\}$. Now we define the rank function to be

$$\mathbf{grk}(A) := \text{rank}(I_S)$$

where I_S is the submatrix with the columns indexed by S and $\text{rank}(I_S) = \dim(\text{span}(A))$. We call $(E(G), \mathbf{grk})$ the *cycle matroid* of G and denote it by $\mathcal{M}(G)$.

We are going to identify $A \subseteq E(G)$ with the spanning subgraph of G on the edge set A for the rest of the chapter.

Example 4.2. Consider the plane graph G in Figure 14. We want to look at the cycle matroid of the graph G in more detail.

Figure 14: Graph G from Example 4.2 with orientation ω .

The incidence matrix for an orientation ω of G^ω is

$$D_G = \begin{matrix} & e_1 & e_2 & e_3 & e_4 & e_5 \\ \begin{matrix} v_1 \\ v_2 \\ v_3 \end{matrix} & \begin{pmatrix} 1 & -1 & 0 & 0 & -1 \\ 0 & 1 & 0 & -1 & 1 \\ -1 & 0 & 0 & 1 & 0 \end{pmatrix} \end{matrix}$$

and the associated matroid is

$$\mathcal{M}(G) = \left(\left\{ e_1, e_2, e_3, e_4, e_5 \right\}, \left\{ \{e_1\}, \{e_2\}, \{e_4\}, \{e_5\}, \{e_1, e_2\}, \{e_1, e_4\}, \{e_1, e_5\}, \{e_2, e_4\}, \{e_4, e_5\} \right\} \right).$$

The next theorem shows how we can see the rank of a subgraph without setting up the incidence matrix first.

Theorem 4.3. *Let G be a graph with $|V| = n$ and $A \subseteq E$. Then*

$$\mathbf{grk}(A) = n - c(A).$$

Proof. We start by noting that for the definition of the rank function of a cycle matroid, the dimension formula for any matrix $A \in \mathbb{R}^{n \times m}$ holds:

$$\mathbf{grk}(A) = \text{rank}(I_S) = \dim(\text{img}(I_S)) = m - \dim(\ker(I_S)).$$

For the transpose $A^T \in \mathbb{R}^{m \times n}$ we have

$$\mathbf{grk}(A^T) = \text{rank}(I_S^T) = \dim(\text{img}(I_S^T)) = n - \dim(\ker(I_S^T)).$$

To prove the theorem, we only need to compare the number of connected components of the subset A with the dimension of the kernel of I_S^T .

Now for an element $x \in \ker(I_S^T) = \{x \in \mathbb{R}^n : I_S^T x = 0\} = \{x \in \mathbb{R}^n : x^T I_S = 0\}$ the following holds for each column I_i such that $i \in S$:

$$0 = x^T I_i = x_1 I_{i_1} + x_2 I_{i_2} + \cdots + x_n I_{i_n}.$$

Each column only has two nonzero entries, at the incident vertices of the corresponding edge. Let k and l be the indices of the vertices u and v with the edge corresponding to i being directed $u \rightarrow v$. Then

$$0 = x^T I_i = x_k - x_l \iff x_k = x_l.$$

Hence, the entries of x have to be equal whenever the corresponding vertices are connected in A . Therefore, for each connected component of A there is exactly one element in the basis of $\ker(I_S^T)$, giving us $\dim(\ker(I_S^T)) = c(A)$. \square

Lemma 4.4. *Let G be a graph. A subset $A \subseteq E(G)$ is a dependent set of the cycle matroid $\mathcal{M}(G)$ if and only if the induced subgraph on A has a cycle.*

Proof. Let A be a subset of $E(G)$ and $Y \subseteq A$ be a connected induced subgraph of A , hence we only consider the vertices which are incident to some edge in Y . With the last theorem we get $\mathbf{grk}(Y) = |V(Y)| - 1$. Now suppose Y is independent, then since $\mathbf{grk}(Y) = |E(Y)|$ we get

$$|E(Y)| = |V(Y)| - 1. \quad (4.1)$$

However, we proved in Theorem 2.11 that a connected graph satisfies equation (4.1) if and only if the graph is a tree, hence if and only if it is acyclic. \square

Remark 4.5. With the previous lemma, we showed that the independent sets in the cycle matroid of a graph are exactly those where the induced subgraph does not contain a cycle. Moreover, it follows that the circuits of the cycle matroid $\mathcal{M}(G)$ are the cycles of G and the bases of $\mathcal{M}(G)$ are the maximal spanning forests of G .

Lemma 4.6. *If G is a graph, then $e \in G$ is a loop if and only if $e \in \mathcal{M}(G)$ is a loop.*

Proof. An element $e \in \mathcal{M}(G)$ is by definition a loop if it satisfies $\mathbf{grk}(e) = 0$. With the definition of the rank function for a cycle matroid, this means that the column in the incidence matrix of G corresponding to the edge e must have rank 0. But this is true if and only if the column has only zeroes as entries. But by the definition of the incidence matrix, it has a column with only zero-entries if and only if the corresponding edge is a loop in the graph. \square

The previous lemma justifies the name "loop" for an element with rank zero of a matroid.

Theorem 4.7. *Let G be a graph, and $T \subseteq E(G)$. Then*

$$\mathcal{M}(G) - T = \mathcal{M}(G - T) \quad \text{and} \quad \mathcal{M}(G)/T = \mathcal{M}(G/T).$$

Proof. The first statement is clear from the definition of deletion for independent sets. For the second one we want to show that for an arbitrary edge $e \in E(G)$

$$\mathcal{M}(G)/e = \mathcal{M}(G/e).$$

If e is a loop of G then $G/e = G - e$ and by Lemma 3.38 $\mathcal{M} - e = \mathcal{M}/e$. The result then follows with the first statement of this lemma. Now suppose that e is not a loop of G . Then we need to compare the sets of independent sets. By definition, and since e is not a loop, the set of independent sets $\tilde{\mathcal{I}}$ of $\mathcal{M}(G)/e$ is

$$\tilde{\mathcal{I}} = \{I \subseteq E(G) - e \mid I \cup \{e\} \in \mathcal{I}\},$$

where \mathcal{I} is the set of independent sets of \mathcal{M} . And with Lemma 4.4 these are exactly the subsets not containing a cycle in G/e . Let $A \in \tilde{\mathcal{I}}$. Then $A = I \cup \{e\}$ does not contain a cycle of G . If we prove that $I \cup \{e\}$ is acyclic in G if and only if I is acyclic in G/e , the set of independent sets of the matroids are the same and the

result follows.

Let $I \cup \{e\}$ be acyclic in G . Then there is no path in $I \cup \{e\} - \{e\}$ connecting the end-vertices of e , hence I is acyclic in G/e . Let u, v denote the end-vertices of e and w the vertex identified with u and v after contracting. If I is acyclic in G/e , then there is no path in I from the vertex w to itself, thus before contracting there is no path in I connecting the vertices u and v . Therefore, adding the edge e will not result in a cycle. \square

4.2 The Bond Matroid

We now want to discuss the dual matroid of the cycle matroid, by taking the definition of \mathbf{rk}^\perp from Chapter 3 and applying it to \mathbf{grk} . We will construct the bond matroid of a graph and shortly discuss so-called *graphic* matroids. These are matroids that are isomorphic to a cycle matroid of a graph. In fact, not all matroids are graphic. We will consider the smallest matroid that is not graphic in Example 4.12.

Definition 4.8. Let G be a graph. The dual of the cycle matroid $\mathcal{M}(G)$ is called the *bond matroid* of a graph and denoted by $\mathcal{M}^\perp(G)$.

Lemma 4.9. If G is graph, then $e \in G$ is a bridge if and only if $e \in \mathcal{M}(G)$ is a coloop.

Proof. An element $e \in \mathcal{M}(G)$ is a coloop if and only if $\mathbf{grk}(E(G) - e) = \mathbf{grk}(E(G)) - 1$. Now let $c(G - e)$ be the number of connected components of $G - e$. With Theorem 4.3 and Lemma 3.49 we get

$$n - c(G - e) = \mathbf{grk}(E(G) - e) = \mathbf{grk}(E(G)) - 1 = n - c(G) - 1 \iff c(G - e) = c(G) - 1.$$

Thus, deleting the edge e results in having one more connected component making e a bridge by definition. \square

By this lemma, an edge $e \in G$ is a bridge if and only if e is a loop in the bond matroid $\mathcal{M}^\perp(G)$.

Lemma 4.10. Let $A \subseteq E(G)$. Then A is independent in $\mathcal{M}^\perp(G)$ if and only if $c(\bar{A}) = c(E(G))$, or equivalently, if A does not contain a set of edges F such that $c(G - F) > c(G)$.

Proof. We can use Theorem 4.3 to receive

$$\begin{aligned} \mathbf{grk}^\perp(A) &= |A| + \mathbf{grk}(\bar{A}) - \mathbf{grk}(E(G)) = |A| + (n - c(\bar{A})) - (n - c(E(G))) \\ &= |A| - c(\bar{A}) + c(E(G)). \end{aligned}$$

Hence

$$0 = \mathbf{grk}^\perp(A) - |A| \iff c(\bar{A}) = c(E(G)).$$

For the second part of this lemma, assume $c(\bar{A}) = c(E(G))$ holds. This is equivalent to $c(G - A) = c(E(G))$, from which $c(G - F) = c(E(G))$ follows for any subset $F \subseteq A$. Now assume $c(G - F) \leq c(E(G))$, then $c(G - A) \leq c(E(G))$ follows directly, which is equivalent to $c(\bar{A}) \leq c(E(G))$. But $c(\bar{A})$ can not be smaller than $c(E(G))$, thus $c(\bar{A}) = c(E(G))$. \square

Definition 4.11. Let \mathcal{M} be a matroid. We call \mathcal{M} *graphic* if there exists a graph G such that

$$\mathcal{M} \cong \mathcal{M}(G).$$

Not all matroids are graphic as the following example shows.

Example 4.12. Consider the uniform matroid \mathcal{U}_4^2 of rank 2 on a 4-element set. Then

$$\mathcal{U}_4^2 = \left(\left\{ 1, 2, 3, 4 \right\}, \left\{ \emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\} \right\} \right),$$

hence the dependent sets of \mathcal{U}_4^2 are $\{1, 2, 3\}, \{1, 2, 4\}, \{2, 3, 4\}, \{1, 2, 3, 4\}$. In Remark 4.5 we deduced that the circuits of the cycle matroid of some graph are exactly the cycles in the graph. The circuits of \mathcal{U}_4^2 are its 3-element dependent sets. Thus if \mathcal{U}_4^2 is isomorphic to the cycle matroid $\mathcal{M}(G)$ for some graph G , then G has 3 cycles of length 3. Now a graph with 4 edges can have at most one cycle of length 3. Thus \mathcal{U}_4^2 is not graphic.

Example 4.13. We want to continue Example 4.2 and compare the cycle matroid of G in Figure 14 with the cycle matroid of the dual graph G^* .

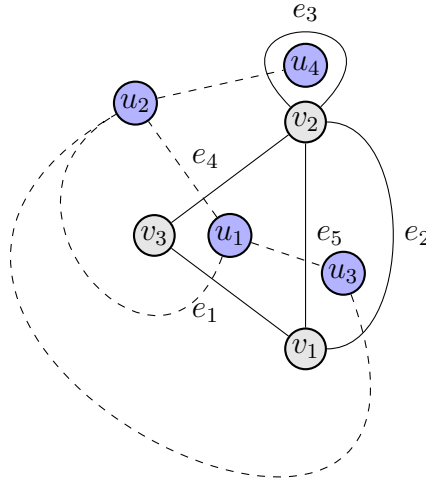


Figure 15: Graph G with dual graph G^*

We assign the graph G the same orientation as in Example 4.2 and assign an arbitrary orientation to G^* . The incidence matrix of G^* and the collection of independent sets of $\mathcal{M}(G^*)$ are

$$D_{G^*} = \begin{matrix} & \hat{e}_1 & \hat{e}_2 & \hat{e}_3 & \hat{e}_4 & \hat{e}_5 \\ \begin{matrix} u_1 \\ u_2 \\ u_3 \\ u_4 \end{matrix} & \begin{pmatrix} -1 & 0 & 0 & -1 & 1 \\ 1 & -1 & -1 & 1 & 0 \\ 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix} \end{matrix}$$

$$\mathcal{M}(G^*) = \left(\left\{ \hat{e}_1, \hat{e}_2, \hat{e}_3, \hat{e}_4, \hat{e}_5 \right\}, \right. \\ \left. \left\{ \{\hat{e}_1\}, \{\hat{e}_2\}, \{\hat{e}_3\}, \{\hat{e}_4\}, \{\hat{e}_5\}, \right. \right. \\ \left. \left\{ \hat{e}_5, \hat{e}_4\}, \{\hat{e}_5, \hat{e}_2\}, \{\hat{e}_5, \hat{e}_1\}, \{\hat{e}_4, \hat{e}_2\}, \{\hat{e}_2, \hat{e}_1\}, \{\hat{e}_3, \hat{e}_5\}, \{\hat{e}_3, \hat{e}_4\}, \{\hat{e}_3, \hat{e}_2\}, \right. \right. \\ \left. \left. \{\hat{e}_3, \hat{e}_1\}, \{\hat{e}_5, \hat{e}_2, \hat{e}_3\}, \{\hat{e}_5, \hat{e}_1, \hat{e}_3\}, \{\hat{e}_5, \hat{e}_4, \hat{e}_3\}, \{\hat{e}_4, \hat{e}_2, f_3\}, \{\hat{e}_2, \hat{e}_1, \hat{e}_3\} \right\} \right).$$

Now let us have a closer look at the sets of bases $\mathcal{B}_1, \mathcal{B}_2$ of $\mathcal{M}(G), \mathcal{M}(G^*)$ respectively:

$$\begin{aligned} \mathcal{B}_1 &= \{\{e_1, e_2\}, \{e_1, e_4\}, \{e_1, e_5\}, \{e_2, e_4\}, \{e_4, e_5\}\} \\ \mathcal{B}_2 &= \{\{\hat{e}_5, \hat{e}_2, \hat{e}_3\}, \{\hat{e}_5, \hat{e}_1, \hat{e}_3\}, \{\hat{e}_5, \hat{e}_4, \hat{e}_3\}, \{\hat{e}_4, \hat{e}_2, f_3\}, \{\hat{e}_2, \hat{e}_1, \hat{e}_3\}\}. \end{aligned}$$

Together with the incidence matrices, the sets \mathcal{B}_1 and \mathcal{B}_2 suggest a bijection:

$$\begin{aligned} \psi : E(G) &\rightarrow E(G^*) \\ e_i &\mapsto \psi(e_i) = \hat{e}_i \quad \text{for all } i \in \{1, 2, 3, 4, 5\}. \end{aligned}$$

With this bijection we see that the bases of $\mathcal{M}(G^*)$ are the complements of the bases of $\mathcal{M}(G)$. This shows that the cycle matroid of G is isomorphic to the cycle matroid of G^* and also suggests that the cycle matroid of G is the bond matroid of G^* .

In [Oxl11], James Oxley discusses duality of graphic matroids in great detail. He proves that the dual matroids of the cycle matroids for the graphs K_5 and $K_{3,3}$ are not graphic. Moreover, he shows that for the geometric dual G^* of a graph G ,

$$\mathcal{M}(G^*) \cong \mathcal{M}^\perp(G) \tag{4.2}$$

holds. Therefore, the cycle matroid of G^* is isomorphic to the bond matroid of G . However, the most interesting result is that for a graph G , $\mathcal{M}^\perp(G)$ is graphic if and only if G is planar. In Chapter 2 we noted the importance of the graphs K_5 and $K_{3,3}$ in graph theory. We want to mention a variant of Kuratowski's Theorem, due to Wagner, which states that a graph is planar if and only if it has no minor isomorphic to K_5 and $K_{3,3}$. He concludes that a graph G is planar if and only if $\mathcal{M}(G)$ has no minor isomorphic to $\mathcal{M}(K_5)$ or $\mathcal{M}(K_{3,3})$.

Let G be a planar graph and G^* a geometric dual. By equation (4.2) and Theorem 3.48 we can conclude

$$T(\mathcal{M}(G^*); x, y) = T(\mathcal{M}(G); y, x).$$

4.3 The Tutte Polynomial for Graphs

In the previous sections, we described thoroughly how we can construct a matroid from a graph. This way, all statements proved in chapter 3 for matroids also hold for the cycle and bond matroids of a graph. Thus we can use Definition 3.44 to

define the Tutte polynomial for graphs. We will compute the Tutte polynomials of some graphs, using the subgraph expansion and the deletion-contraction algorithm. At the end of this section, we will define the *one-point join* and the *disjoint union* of graphs and prove that the Tutte polynomial is multiplicative on both constructions.

Definition 4.14. Let G be a graph with $|V| = n$. The *Tutte polynomial* of G is the Tutte polynomial of its cycle matroid $\mathcal{M}(G)$:

$$T(G; x, y) := T(\mathcal{M}(G); x, y) = \sum_{A \subseteq E(G)} (x-1)^{\text{grk}(E(G)) - \text{grk}(A)} (y-1)^{n(A)}.$$

Example 4.15. Consider the graph in Figure 16. We want to compute its Tutte polynomial, thus we have to look at all subsets of $E(G)$.

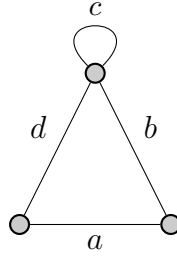


Figure 16: Graph G .

A	$\text{grk}(A)$	$\text{grk}(E) - \text{grk}(A)$	$ A - \text{grk}(A)$	A	$\text{grk}(A)$	$\text{grk}(E) - \text{grk}(A)$	$ A - \text{grk}(A)$
\emptyset	0	2	0	$\{b, c\}$	1	1	1
$\{a\}$	1	1	0	$\{b, d\}$	2	0	0
$\{b\}$	1	1	0	$\{c, d\}$	1	1	1
$\{c\}$	0	2	1	$\{a, b, c\}$	2	0	1
$\{d\}$	1	1	0	$\{a, b, d\}$	2	0	1
$\{a, b\}$	2	0	0	$\{a, c, d\}$	2	0	1
$\{a, c\}$	1	1	1	$\{b, c, d\}$	2	0	1
$\{a, d\}$	2	0	0	$\{a, b, c, d\}$	2	0	2

Table 1: all subgraphs of G in Example 4.15 with their corresponding rank and nullity functions

We can get all information from table 1 and get,

$$T(G; x, y) = \sum_{A \subseteq E(G)} (x-1)^{\text{grk}(E(G)) - \text{grk}(A)} (y-1)^{|A| - \text{grk}(A)} = x^2y + xy + y^2.$$

The last example showed how impractical it can be to compute the Tutte polynomial according to Definition 4.14. However, Theorem 3.50 also holds for the cycle matroids of graphs.

Theorem 4.16. Let G be a graph. Then the Tutte polynomial for the cycle matroid $\mathcal{M}(G)$ satisfies the following deletion-contraction relations

$$T(G; x, y) = \begin{cases} xT(G/e; x, y), & \text{if } e \text{ is a bridge;} \\ yT(G - e; x, y), & \text{if } e \text{ is a loop;} \\ T(G - e; x, y) + T(G/e; x, y), & \text{if } e \text{ is ordinary;} \\ 1, & \text{if } E(G) = \emptyset. \end{cases}$$

Proof. By Theorem 4.7, we have $\mathcal{M}(G)/e = \mathcal{M}(G/e)$ and $\mathcal{M}(G) - e = \mathcal{M}(G - e)$. The theorem then follows directly from Theorem 3.50. \square

Example 4.17. Now we can compute the Tutte polynomial of the graph in Example 4.15 in a more efficient way:

$$\begin{aligned}
 T \left(\begin{array}{c} \text{graph with vertices } d, b, a \text{ and edges } (d,b), (d,a), (b,a), (c,d) \end{array} \right) &= y \cdot \left(\begin{array}{c} \text{graph with vertices } d, b, a \text{ and edges } (d,b), (d,a), (b,a) \end{array} \right) \\
 &= y \cdot \left(T \left(\begin{array}{c} \text{graph with vertices } d, b, a \text{ and edges } (d,b), (d,a) \end{array} \right) + T \left(\begin{array}{c} \text{graph with vertices } d, b, a \text{ and edges } (d,b), (b,a) \end{array} \right) \right) \\
 &= y \cdot \left(x \cdot T \left(\begin{array}{c} \text{graph with vertices } d, a \text{ and edge } (d,a) \end{array} \right) + \left(\left(\begin{array}{c} \text{graph with vertices } d, a \text{ and edge } (d,a) \end{array} \right) + \left(\begin{array}{c} \text{graph with vertex } a \text{ and edge } (a,a) \end{array} \right) \right) \right) \\
 &= y \cdot (x \cdot x + (x + y)) \\
 &= x^2 y + y^2 + xy.
 \end{aligned}$$

Definition 4.18. A *one-point join* of two disjoint graphs G and H , denoted by $G \star_{u,v} H$, is formed by identifying a vertex u of G and a vertex v of H into a single vertex w of $G \star H$. The edge set and incidence relations of $G \star_{u,v} H$ are induced from those of G and H .

One can think of the one-point join of two graphs as glueing the graphs together at a selected vertex. If we are not interested in the chosen vertices for the one-point join, we simply write $G \star H$.

Lemma 4.19. *If G and H are graphs, then*

$$T(G \sqcup H; x, y) = T(G; x, y) \cdot T(H; x, y),$$

and

$$T(G \star H; x, y) = T(G; x, y) \cdot T(H; x, y).$$

Proof. We call G and H the blocks of $G \sqcup H$ and $G \star H$. Given any edge $e \in G \sqcup H$, both of its end-vertices lie in the same block. The same holds for $G \star H$. Therefore we can prove both statements at once, since the only information we will use, is in which block both endvertices of some edge e are contained. We can generalize our two graph constructions and write $G \cup H$ for $G \sqcup H$ and for $G \star H$. We will induct on the number of edges $|E(G \sqcup H)| = k = |E(G \star H)|$. By the construction of the disjoint union and one point join, it is clear that for an edge $e \in G$, we have

$$(G \cup H) - e = (G - e) \cup H \text{ and } (G \cup H)/e = (G/e) \cup H.$$

Let $k = 1$, and suppose without loss of generality that $e \in G$. Since e is the only edge, it is either a loop or bridge of G , hence it is either a loop or coloop of $G \cup H$. If e is a loop, then $G - e \cup H$ is empty. We can use Theorem 4.7 and Theorem 4.16 and get

$$\begin{aligned} T(\mathcal{M}(G \cup H); x, y) &= y \cdot T(\mathcal{M}(G \cup H) - e; x, y) \\ &= y \cdot T(\mathcal{M}(G - e \cup H); x, y) = y \cdot 1 = T(\mathcal{M}(G); x, y) \cdot T(\mathcal{M}(H); x, y). \end{aligned}$$

On the other hand, if e is a bridge, Theorem 4.7 and 4.16 yield

$$\begin{aligned} T(\mathcal{M}(G \cup H); x, y) &= x \cdot T(\mathcal{M}(G \cup H)/e; x, y) \\ &= x \cdot T(\mathcal{M}(G/e \cup H); x, y) = x \cdot 1 = T(\mathcal{M}(G); x, y) \cdot T(\mathcal{M}(H); x, y). \end{aligned}$$

Now suppose the statement is true for $k = m$ and let $k = m + 1$. Deleting or contracting any edge e only decreases the number of edges. Without loss of generality, suppose both end-vertices of e lie in the block of G . Firstly, if e is a loop, then with Theorem 4.16 and Theorem 4.7 we have

$$T(\mathcal{M}(G \cup H); x, y) = y \cdot T(\mathcal{M}(G \cup H) - e; x, y) = y \cdot T(\mathcal{M}(G - e \cup H); x, y).$$

Then by the induction hypothesis and Theorem 4.16 we know

$$T(\mathcal{M}(G \cup H); x, y) = y \cdot T(\mathcal{M}(G - e); x, y) T(\mathcal{M}(H); x, y) = T(\mathcal{M}(G); x, y) T(\mathcal{M}(H); x, y).$$

Similarly, if e is a bridge, Theorem 4.16 and Theorem 4.7 show that

$$T(\mathcal{M}(G \cup H); x, y) = x \cdot T(\mathcal{M}(G \cup H)/e; x, y) = x \cdot T(\mathcal{M}(G/e \cup H); x, y).$$

Again, by the induction hypothesis and Theorem 4.16 this results in

$$T(\mathcal{M}(G \cup H); x, y) = x \cdot T(\mathcal{M}(G/e); x, y) T(\mathcal{M}(H); x, y) = T(\mathcal{M}(G); x, y) T(\mathcal{M}(H); x, y).$$

Let $e \in G \cup H$ be an edge that is ordinary. Then by Theorem 4.16 it follows that

$$T(\mathcal{M}(G \cup H); x, y) = T(\mathcal{M}(G \cup H) - e; x, y) + T(\mathcal{M}(G \cup H)/e; x, y). \quad (4.3)$$

With Theorem 4.7 we can continue equation (4.3), so that

$$T(\mathcal{M}(G \cup H); x, y) = T(\mathcal{M}(G - e \cup H); x, y) + T(\mathcal{M}(G/e \cup H); x, y) \quad (4.4)$$

Now we can use the induction hypothesis, such that the right hand side of equation (4.4) equals

$$T(\mathcal{M}(G - e); x, y) \cdot T(\mathcal{M}(H); x, y) + T(\mathcal{M}(G/e); x, y) \cdot T(\mathcal{M}(H); x, y). \quad (4.5)$$

Hence,

$$T(\mathcal{M}(G \cup H); x, y) = T(\mathcal{M}(H); x, y) \cdot [T(\mathcal{M}(G - e); x, y) + T(\mathcal{M}(G/e); x, y)],$$

where we can use Theorem 4.16 a second time to receive

$$T(\mathcal{M}(G \cup H); x, y) = T(\mathcal{M}(G); x, y) T(\mathcal{M}(H); x, y). \quad \square$$

4.4 The Tutte Polynomial as a Graph Invariant

The chromatic polynomial, the flow polynomial and the reliability polynomial are graph polynomials that satisfy a deletion-contraction recurrence as shown in Chapter 2. We would like to present these invariants as specializations of the Tutte polynomial, using the recipe theorem from Section 3.5. Unfortunately, when translating a graph into its cycle matroid, we lose information about possible isolated vertices. Moreover, the direct sum of two cycle matroids is isomorphic to the cycle matroid of the disjoint union and the one-point join of the underlying graphs, which are in general not the same graphs. But the chromatic polynomial, for example, is not multiplicative on one-point joins. Consequently, we need to reformulate the recipe theorem, which is the main result of this chapter and also one of the most important results of this thesis. With the modified recipe theorem we will be able to show that the graph polynomials considered in Chapter 2 are specializations of the Tutte polynomial.

Definition 4.20. Let \mathcal{G} be a minor-closed class of graphs, \mathfrak{R} be a commutative ring with unity and $a, b \in \mathfrak{R}$. A graph invariant $f : \mathcal{G} \rightarrow \mathfrak{R}$ is a *Tutte-Grothendieck invariant*, or *T-G-invariant*, if

$$\begin{aligned} f(G) &= af(G - e) + bf(G/e) \text{ if } e \text{ is ordinary,} \\ f(\bullet) &= 1, \\ f(G \sqcup H) &= f(G) \cdot f(H), \\ f(G \star H) &= f(G) \cdot f(H). \end{aligned}$$

Remark 4.21. The last three conditions replace the second condition for a T-G-invariant for matroids, from which we deduced that $f(\mathcal{M}) = 1$ for an empty matroid. The independent sets of the direct sum of two matroids \mathcal{M}_1 and \mathcal{M}_2 were defined as the union of two independent sets I_1, I_2 from \mathcal{M}_1 and \mathcal{M}_2 respectively. Recall that the independent sets in the cycle matroid of a graph are its acyclic forests. Since we lose some information about the vertices if we translate a graph into its cycle matroid, the forests in $G \sqcup H$ are exactly the forests in $G \star H$, explaining the last two conditions.

Theorem 4.22. Let \mathcal{G} be a minor-closed class of graphs, let \mathfrak{R} be a commutative ring with unity and let $f : \mathcal{G} \rightarrow \mathfrak{R}$. If there exists $a, b \in \mathfrak{R}$ such that f is a Tutte-Grothendieck invariant, then

$$f(G) = a^{|E(G)| - \text{grk}(E(G))} b^{\text{grk}(E(G))} T\left(\mathcal{M}(G); \frac{x_0}{b}, \frac{y_0}{a}\right),$$

where $f(\bullet \text{---} \bullet) = x_0$ and $f(\bullet \circlearrowleft) = y_0$.

Proof. We will proceed similarly to the proof of the recipe theorem for matroids and induct on the number of edges. Let G be a graph with no edges and $V(G) = n$. Since f is a Tutte-Grothendieck invariant and the Tutte polynomial equals 1 on the empty graph, we get

$$\begin{aligned} f(G) &= f(\bullet \sqcup \bullet \sqcup \cdots \sqcup \bullet) = f(\bullet) \cdot f(\bullet) \cdot \dots \cdot f(\bullet) \\ &= f(\bullet)^n = 1 = a^0 \cdot b^0 \cdot 1 = a^0 \cdot b^0 T\left(\mathcal{M}(G); \frac{x_0}{b}, \frac{y_0}{a}\right). \end{aligned}$$

Now let G be a graph with $|E(G)| = m + 1$ and suppose the statement holds for all graphs with m edges. If $e \in E(G)$ is a loop, then

$$f(G) = f(\bullet \bigcirc \star G/e) = f(\bullet \bigcirc) \star f(G/e).$$

Here we can use the induction hypothesis, since G/e is a graph on m edges, to get

$$f(G) = y_0 \cdot a^{|E(G)-e|-\mathbf{grk}_{\mathcal{M}(G/e)}(E(G)-e)} b^{\mathbf{grk}_{\mathcal{M}(G/e)}(E(G)-e)} T\left(\mathcal{M}(G/e); \frac{x_0}{b}, \frac{y_0}{a}\right). \quad (4.6)$$

With $\mathcal{M}(G/e) = \mathcal{M}(G)/e$ and by Theorem 4.7, Lemma 3.49 and equation (4.6) is equal to

$$\frac{y_0}{a} f(G) = y_0 \cdot a^{|E(G)|-1-\mathbf{grk}(E(G))} b^{\mathbf{grk}(E(G))} T\left(\mathcal{M}(G); \frac{x_0}{b}, \frac{y_0}{a}\right),$$

hence,

$$f(G) = a^{|E(G)|-\mathbf{grk}(E(G))} b^{\mathbf{grk}(E(G))} T\left(\mathcal{M}(G); \frac{x_0}{b}, \frac{y_0}{a}\right).$$

The case for $e = (u, v)$ being a bridge is similar. We use that G is a one point join of the graphs G_1, G_2 and e , where G_1 is the connected component of $G - e$ that contains the vertex u and G_2 is a disjoint union of all connected components of $G - e$ that do not contain u . With this construction we can use the properties of a Tutte-Grothendieck invariant and get

$$\begin{aligned} f(G) &= f((G_1 \star \bullet \text{---} \bullet) \star G_2) = f(G_1) f(G_2) f(\bullet \text{---} \bullet) \\ &= f(G_1 \sqcup G_2) f(\bullet \text{---} \bullet) = f(G - e) f(\bullet \text{---} \bullet). \end{aligned}$$

Then with the induction hypothesis we get

$$f(G) = x_0 \cdot a^{|E(G)-e|-\mathbf{grk}_{\mathcal{M}(G-e)}(E(G)-e)} b^{\mathbf{grk}_{\mathcal{M}(G-e)}(E(G)-e)} T\left(\mathcal{M}(G-e); \frac{x_0}{b}, \frac{y_0}{a}\right).$$

Here we use Theorem 4.7 and $\mathcal{M}(G) - e = \mathcal{M}(G - e)$ to obtain

$$\frac{x_0}{b} f(G) = x_0 \cdot a^{|E(G)|-1-(\mathbf{grk}(E(G))-1)} b^{\mathbf{grk}(E(G))-1} T\left(\mathcal{M}(G); \frac{x_0}{b}, \frac{y_0}{a}\right).$$

Concluding,

$$f(G) = a^{|E(G)|-\mathbf{grk}(E(G))} b^{\mathbf{grk}(E(G))} T\left(\mathcal{M}(G); \frac{x_0}{b}, \frac{y_0}{a}\right).$$

Finally, let $e \in E(G)$ be an ordinary edge. Then

$$f(G) = af(G - e) + bf(G/e),$$

and by the induction hypothesis

$$af(G - e) = a \cdot a^{|E(G)|-1-\mathbf{grk}_{\mathcal{M}(G-e)}(E(G)-e)} b^{\mathbf{grk}_{\mathcal{M}(G-e)}(E(G)-e)} T\left(\mathcal{M}(G - e); \frac{x_0}{b}, \frac{y_0}{a}\right) \quad (4.7)$$

and

$$bf(G/e) = b \cdot a^{|E(G)|-1-\mathbf{grk}_{\mathcal{M}(G/e)}(E(G)-e)} b^{\mathbf{grk}_{\mathcal{M}(G/e)}(E(G)-e)} T\left(\mathcal{M}(G/e); \frac{x_0}{b}, \frac{y_0}{a}\right). \quad (4.8)$$

By Lemma 3.49 and equations (4.7) and (4.8) we know

$$af(G - e) = a^{|E(G)| - \text{grk}(E(G))} b^{\text{grk}(E(G))} T\left(\mathcal{M}(G - e); \frac{x_0}{b}, \frac{y_0}{a}\right)$$

and

$$bf(G/e) = a^{E(G)-1-(\text{grk}(E(G))-1)} b^{\text{grk}(E(G))-1+1} T\left(\mathcal{M}(G/e); \frac{x_0}{b}, \frac{y_0}{a}\right).$$

From this we obtain

$$f(G) = a^{|E(G)| - \text{grk}(E(G))} b^{\text{grk}(E(G))} \left(T\left(\mathcal{M}(G - e); \frac{x_0}{b}, \frac{y_0}{a}\right) + T\left(\mathcal{M}(G/e); \frac{x_0}{b}, \frac{y_0}{a}\right) \right)$$

and by Theorem 4.7 we conclude

$$f(G) = a^{|E(G)| - \text{grk}(E(G))} b^{\text{grk}(E(G))} T\left(\mathcal{M}(G); \frac{x_0}{b}, \frac{y_0}{a}\right). \quad \square$$

Lemma 4.23. *Let G be a graph. Then*

- a) $T(\mathcal{M}(G); 1, 1)$ is the number of spanning trees in G if it is connected.
- b) $T(\mathcal{M}(G); 2, 1)$ is the number of forests in G .

Proof. First note that the bases of the cycle matroid of some graph G are the maximal spanning forests by Remark 4.5. If G is connected, the bases are the maximal spanning trees. Also, Lemma 3.58 showed that $T(\mathcal{M}(G); 1, 1)$ is exactly the number of bases of $\mathcal{M}(G)$.

Furthermore, Remark 4.5 also noted that the independent sets of a cycle matroid are exactly the forests of the underlying graph. Hence, with Lemma 3.58 $T(G; 2, 1)$ is exactly the number of forests in G . \square

Remark 4.24. Note that the chromatic polynomial is not a Tutte-Grothendieck invariant, as $P(\bullet, \lambda) = \lambda$ for each λ . Secondly consider the graph G consisting of two vertices and an edge connecting these. Then by the combinatorial rule of sum

$$P(G \sqcup H, \lambda) = \lambda(\lambda - 1) + \lambda(\lambda - 1) = 2\lambda(\lambda - 1) \neq \lambda^2(\lambda - 1)^2 = P(G, \lambda)P(H, \lambda).$$

Finally, the chromatic polynomial of a one-point join depends on the specific vertex at which the two graphs are joined. Consider the graph G_1 consisting of vertices v_1, v_2, v_3 with edge set $E(G_1) = \{(v_1, v_2)\}$ and the graph G_2 being the induced subgraph of G_1 on $V(G_2) = \{v_1, v_2\} \subset V(G_1)$. Then joining G_1 and G_2 at vertex v_3 and any vertex of G_2 results in the chromatic polynomial

$$P(G_1 \star_1 G_2, \lambda) = \lambda(\lambda - 1) + \lambda(\lambda - 1) = 2\lambda(\lambda - 1) = 2\lambda^2 - 2\lambda.$$

However, the join at vertex v_1 of G_1 and any vertex of G_2 results in the chromatic polynomial

$$P(G_1 \star_2 G_2, \lambda) = \lambda + \lambda(\lambda - 1)^2 = \lambda^3 - 2\lambda^2 + 2\lambda.$$

Unfortunately, the last remark shows that we can not use the recipe theorem for graph invariants directly for the chromatic polynomial. But the next theorem proves that there is a unique universal polynomial, which is computed through a deletion-contraction recursion, and that this universal polynomial is an specialization of the Tutte polynomial.

Theorem 4.25. *Let \mathcal{G} be a minor-closed class of graphs. Then there is a unique map $U : \mathcal{G} \rightarrow \mathbb{Z}[x, y, a, b, \alpha]$ such that*

$$U(G) = \begin{cases} x U(G - e), & \text{if } e \text{ is a bridge;} \\ y U(G - e), & \text{if } e \text{ is a loop;} \\ a U(G - e) + b U(G/e), & \text{if } e \text{ is ordinary;} \\ \alpha^n, & \text{if } E(G) = \emptyset \text{ and } V(G) = n. \end{cases}$$

Moreover

$$U(G) = \alpha^{c(G)} a^{n(G)} b^{\text{rk}(G)} T\left(G; \frac{\alpha x}{b}, \frac{y}{a}\right). \quad (4.9)$$

Proof. The uniqueness follows immediately from $U(G)$ being determined by $U(G - e)$ and $U(G/e)$ for an edge $e \in E(G)$. Hence we only need to prove that the function U given by (4.9) has the required properties. Let G be an arbitrary graph and denote by $\deg_x(T)$ and $\deg_y(T)$ the degree of x, y respectively in $T(\mathcal{M}(G); x, y)$. Then $U(G) \in \mathbb{Z}[x, y, a, b, \alpha]$ since

$$\begin{aligned} \deg_x(T) &= \max\{\text{grk}(G) - \text{grk}(A) : A \subseteq E(G)\} = \text{grk}(G) \\ \deg_y(T) &= \max\{\mathbf{n}(A) : A \subseteq E(G)\} = \mathbf{n}(G). \end{aligned}$$

If G is an empty graph on n vertices, then $c(G) = n$ and $\text{rk}(G) = \mathbf{n}(G) = 0$, hence

$$U(G) = \alpha^n T\left(\mathcal{M}(G); \frac{\alpha x}{b}, \frac{y}{a}\right) = \alpha^n.$$

Lastly, we need to show, that $U(G)$ as in (4.9) satisfies the reduction formulae. Let $e \in E(G)$ be a bridge. then with Theorem 4.7 $\mathcal{M}(G - e) = \mathcal{M}(G/e)$ holds and with Theorem 4.16 we obtain

$$U(G) = \alpha^{c(G)} a^{\mathbf{n}(G)} b^{\text{grk}(G)} \frac{\alpha x}{b} T\left(\mathcal{M}(G/e); \frac{\alpha x}{b}, \frac{y}{a}\right). \quad (4.10)$$

From Lemma 3.49 we know $c(G - e) = c(G) + 1$, $\mathbf{n}(G - e) = \mathbf{n}(G)$ and $\text{rk}(G - e) = \text{rk}(G) - 1$, so that

$$U(G) = x \cdot \alpha^{c(G-e)} a^{\mathbf{n}(G-e)} b^{\text{grk}(G-e)} T(\mathcal{M}(G - e); \frac{\alpha x}{b}, \frac{y}{a}),$$

from which we obtain

$$U(G) = x \cdot U(G - e).$$

Now let $e \in E(G)$ be a loop. Similarly to the first case, we use Theorem 4.16 to obtain

$$U(G) = \alpha^{c(G)} a^{\mathbf{n}(G)} b^{\text{grk}(G)} \frac{y}{a} T\left(\mathcal{M}(G - e); \frac{\alpha x}{b}, \frac{y}{a}\right).$$

With $c(G) = c(G - e)$, $\mathbf{n}(G - e) = \mathbf{n}(G) - 1$ and $\text{grk}(G - e) = \text{grk}(G)$ it follows that

$$U(G) = \alpha^{c(G-e)} a^{\mathbf{n}(G-e)} b^{\text{grk}(G-e)} y T\left(\mathcal{M}(G - e); \frac{\alpha x}{b}, \frac{y}{a}\right) = y U(G - e).$$

Lastly, if $e \in E(G)$ is an ordinary edge, then by Theorem 4.16 we know

$$U(G) = \alpha^{c(G)} a^{\mathbf{n}(G)} b^{\text{grk}(G)} \left(T(\mathcal{M}(G - e); \frac{\alpha x}{b}, \frac{y}{a}) + T(\mathcal{M}(G/e); \frac{\alpha x}{b}, \frac{y}{a}) \right). \quad (4.11)$$

Since e is ordinary, $c(G - e) = c(G/e) = c(G)$, $\mathbf{n}(G - e) = \mathbf{n}(G) - 1$, $\mathbf{n}(G/e) = \mathbf{n}(G)$, $\mathbf{grk}(G - e) = \mathbf{grk}(G)$ and $\mathbf{grk}(G/e) = \mathbf{grk}(G) - 1$, so that (4.11) equals

$$\alpha^{c(G-e)} a^{\mathbf{n}(G-e)+1} b^{\mathbf{grk}(G-e)} T(\mathcal{M}(G-e); \frac{\alpha x}{b}, \frac{y}{a}) + \alpha^{c(G/e)} a^{\mathbf{n}(G/e)} b^{\mathbf{grk}(G/e)+1} T(\mathcal{M}(G/e); \frac{\alpha x}{b}, \frac{y}{a}).$$

Together we obtain,

$$U(G) = a \cdot U(G - e) + b \cdot U(G/e). \quad \square$$

This result helps us prove that the Tutte polynomial specializes to the polynomials introduced in Chapter 2.

Theorem 4.26. *The chromatic polynomial of a graph G is a specialization of the Tutte polynomial:*

$$P(G; \lambda) = (-1)^{\mathbf{grk}(G)} \lambda^{c(G)} T(G; 1 - \lambda, 0).$$

Proof. The deletion-contraction formula for the chromatic polynomial proved in Theorem 2.37 satisfies the conditions of Theorem 4.25, with $\alpha = \lambda$, $a = 1$, $b = -1$, $y = 0$ and $x = \frac{\lambda-1}{\lambda}$. Hence,

$$P(G, \lambda) = U\left(G; \frac{\lambda-1}{\lambda}, 0, \lambda, 1, -1\right) = \lambda^{c(G)} (-1)^{\mathbf{rk}(G)} T(G; 1 - \lambda, 0),$$

as claimed. \square

Theorem 4.27. *The flow polynomial of an oriented graph G^ω is a specialization of the Tutte polynomial:*

$$F(G^\omega; k) = (-1)^{\mathbf{n}(G)} T(G; 0, 1 - k).$$

Proof. The flow polynomial $F(G^\omega; k)$ satisfies the conditions in Theorem 4.25. From the deletion-contraction formula in Theorem 2.45 we get $x = 0$, $y = k - 1$, $a = -1$, $b = 1$ and $\alpha = 1$. Thus,

$$\begin{aligned} F(G^\omega; k) &= U(G; 0, k - 1, -1, 1, 1) = 1^{c(G)} (-1)^{\mathbf{n}(G)} 1^{\mathbf{grk}(G)} T\left(G; 0, \frac{k-1}{-1}\right) \\ &= (-1)^{\mathbf{n}(G)} T(G; 0, 1 - k). \end{aligned} \quad \square$$

Theorem 4.28. *The Reliability Polynomial of a graph G is a specialization of the Tutte polynomial:*

$$C(G; p) = (1 - p)^{\mathbf{n}(G)} p^{\mathbf{grk}(G)} T(\mathcal{M}(G); 1, \frac{1}{1-p}).$$

Proof. From the deletion-contraction formula of the reliability polynomial in Theorem 2.50 we see that $C(G; p)$ satisfies the conditions of Theorem 4.25 with $a = (1-p)$, $b = p$, $x = p$, $y = 1$ and $\alpha = 1$. Thus,

$$C(G; p) = U(G; p, 1, (1-p), p, 1) = 1^{c(G)} (1-p)^{\mathbf{n}(G)} p^{\mathbf{grk}(G)} T\left(G; 1, \frac{1}{(1-p)}\right). \quad \square$$

5 Complexity and Applications

In the last chapters we discussed the Tutte polynomial and its properties in great detail. We now want to focus on applications of the Tutte polynomial and its exact complexity. This chapter is only going to scratch the surface of each topic. For a more detailed analysis refer to [EMM22] and [GR01].

5.1 Computational Complexity of the Tutte Polynomial

The Tutte polynomial, being an isomorphism invariant, is an important tool to identify and extract information from a graph or matroid. Oftentimes we face the task of computing or evaluating the Tutte polynomial for a family of graphs or matroids. Detailed techniques can be found in Chapter 7 of [EMM22]. When evaluating the Tutte polynomial, we are usually concerned with computing the exact value of $T(G; a, b)$ where the input is a graph G and two numbers $a, b \in \mathbb{C}$. If we can evaluate efficiently, we can then use interpolation to compute the coefficients of the polynomial.

Dominic Welsh [Wel93] gives a nice short introduction into the basics of complexity theory.

A *decision problem* is a computational problem for which the answer is either "yes" or "no". An example of a decision problem is: For a given λ , does a given graph G have a proper λ -coloring?

A computational problem for which the answer is the number of satisfying configurations is called a *counting problem*. An example of a counting problem is: For a given λ , how many proper λ -colorings does a given graph G have?

We denote the set of decision problems, respectively counting problems, which can be solved in time polynomial in the size of the input by P , respectively FP . This means that the computation time is bounded by a polynomial which has the input parameters as variables. We consider the problems in P or FP to be efficiently computable.

The set of decision problems for which we can verify whether a given configuration is correct in polynomial time in the size of the input will be denoted by NP .

The set of counting problems which count configurations whose correctness can be verified in polynomial time will be denoted by $\#P$.

The problem of deciding whether a given graph G has a proper λ -coloring is in NP and computing the number of proper λ -colorings is $\#P$. Whether

$$P \stackrel{?}{=} NP \text{ and } FP \stackrel{?}{=} \#P$$

are famous and difficult open problems.

A problem is called *NP-hard*, *$\#P$ -hard* respectively, if in terms of asymptotic runtime it is at least as hard as the hardest problems in NP , $\#P$ respectively.

A problem that is NP and NP-hard is called *NP-complete*.

A problem that is #P and #P-hard is called *#P-complete*.

These problems are not considered effectively computable, unless $\text{NP} = \text{P}$, $\text{FP} = \text{\#P}$ respectively.

F. Jaeger, D. Vertigan and D. Welsh began the study of the complexity of the Tutte polynomial in their paper [JVW90]. Their main result is the following dichotomy theorem. For a graph G , let H_1 be the hyperbola

$$H_1 := \{(x, y) \in \mathbb{C}^2 : (x - 1)(y - 1) = 1\}$$

and let H be the union of H_1 with

$$\{(1, 1), (-1, -1), (0, -1), (-1, 0), (i, -i), (-i, i), (j, j^2), (j^2, j)\},$$

where $j = e^{2\pi i/3}$. Then, for every $(a, b) \in \mathbb{C}^2$ they showed:

- (1) if $(a, b) \notin H$, then $T(G; a, b)$ is #P-hard;
- (2) if $(a, b) \in H$, then $T(G; a, b)$ is computable in polynomial time.

D. Vertigan and D. Welsh [VW92] studied the complexity of evaluating the Tutte polynomial of graphs that are both bipartite and planar. Consider the hyperbola

$$H_2 := \{(x, y) \in \mathbb{C}^2 : (x - 1)(y - 1) = 2\},$$

and let H_{bp} be the union of $\{(1, 1), (-1, -1), (j^2, j), (j, j^2)\}$, H_1 and H_2 . For every $(a, b) \in \mathbb{C}^2$,

- (1) if $(a, b) \notin H_{bp}$, then $T(G; a, b)$ is #P-hard for bipartite planar graphs;
- (2) if $(a, b) \in H_{bp}$, then $T(G; a, b)$ is computable in polynomial-time for bipartite planar graphs.

However, we can introduce structural graph parameters, called *tree-width* and *clique-width*, such that the Tutte polynomial is efficiently computable on graphs of bounded tree-width or clique-width. Steven Noble proved in [Nob98] that $T(G; x, y)$ can be evaluated in $O(|V|)$ for graphs with bounded tree-width. For the case of bounded clique-width, in [GHN06] was proven that $T(G; x, y)$ can be computed in time $\exp(O(|V|^{1-\frac{1}{k+2}}))$ on graphs with a clique-width of at most k .

5.2 Applications of the Tutte Polynomial

Despite its computational hardness, the Tutte polynomial has many applications in various scientific fields, such as topological knot theory, coding theory and statistical mechanics. We will focus on the first two. The results for the latter one and many more applications can be found in [EMM22].

5.2.1 Knot Theory

Consider piecewise-linear closed curves in \mathbb{R}^3 , called *knots*. A knot is usually defined with some orientation. A collection of pairwise disjoint knots is called a *link*. We call a link *alternating* if, following the orientation on the strand, it alternates in over- and undercrossings. Two links are called *equivalent* if they can be deformed into the other by moving it around without passing one strand through another. A formal definition of equivalence uses isotopy and Reidemeister moves and can be found in Chapter 16 of [GR01]. The fundamental problem in topological knot theory is to determine whether two knots are equivalent. If two knots are equivalent, we can find a sequence of isotopies and Reidemeister moves to deform one knot into the other.

For many knots it is very hard to find such a sequence. In fact, deciding whether a diagram of a knot can be detangled to the knot without crossings with a given number of moves, as part of the input, is known to be NP-complete. Therefore, the main approach to this problem is to develop knot invariants. As in graph theory, if such an invariant takes different values on different knots, then they can not be equivalent. The main tools are topological, such as fundamental groups or homology. In 1984 Vaughan Jones [Jon85] discovered the Jones polynomial, another topological tool, which was used to answer a number of open questions about knots.

However, we do not need topological notions to discuss knots, as it is very easy to view links as purely combinatorial objects. We consider link diagrams, which are projections of links into \mathbb{R}^2 . One can think of the projections of a link as the shadow it casts on the plane. It is possible to look at the projections as a plane graph, in which every vertex is incident to exactly four edges, possibly multiple edges are counted twice. The graph must contain information about the over- and under-crossings of the link. Therefore each edge will be assigned either a "+"-sign or "-"-sign, depending on the orientation at each under- and overcrossing. Hence we can think of a signed graph. Now Béla Bollobás [Bol98] states that the Jones polynomial of an alternating oriented link is just a specialization of the Tutte polynomial. More information about the connection between knot theory and graph theory can be found in [GR01]. Colin Adams [Ada94] gives a figurative approach to knot theory and also discusses how we can model DNA using knot theory.

5.2.2 Coding Theory

Another application of the Tutte polynomial can be found in coding theory. Let \mathbb{F}_q be the finite field with q elements, where q is a prime power. Set $E := \{1, \dots, n\}$ for some positive integer n . Let $\mathbb{F}_q^n := \mathbb{F}_q^E$ be the vector space of ordered n -tuples of elements from \mathbb{F}_q indexed by E . A *linear code* C over \mathbb{F}_q is a vector space over \mathbb{F}_q . More specifically, an $[n, k]$ linear code C over \mathbb{F}_q is a k -dimensional subspace of the vector space \mathbb{F}_q^n . We call each vector in C a *codeword*. The *support* and *weight* of a codeword $x = (x_1, \dots, x_n) \in \mathbb{F}_q^n$ is given by

$$\begin{aligned} \text{supp}(x) &:= \{i : x_i \neq 0\} \text{ and} \\ \text{wt}(x) &:= |\text{supp}(x)|. \end{aligned}$$

Similarly, the *support* and *weight* of each subset $B \subseteq \mathbb{F}_q^n$ are defined

$$\begin{aligned}\text{supp}(B) &:= \bigcup_{x \in B} \text{supp}(x) \text{ and} \\ \text{wt}(B) &:= |\text{supp}(B)|.\end{aligned}$$

The *weight enumerator* $W_C(x, y)$ of an $[n, k]$ linear code C over \mathbb{F}_q enumerates the number of codewords of each given weight as follows:

$$W_C(x, y) := \sum_{i=0}^n A_i x^{n-i} y^i,$$

where $A_i = |\{v \in C : \text{wt}(v) = i\}|$.

The *vector matroid* \mathcal{M}_C of a $[n, k]$ linear code C with coordinates E is the matroid $\mathcal{M}_C := (E, \mathbf{rk}_{\mathcal{M}_C})$ with rank function $\mathbf{rk}_{\mathcal{M}_C} := \dim(C|X)$ for each subset $X \subseteq E$, where $C|X$ is the linear code obtained by removing the coordinates $E - X$ from each codeword of C . With this definition we can compute the Tutte polynomial for a matroid belonging to a code. In his paper [Gre76] from 1976 Curtis Greene showed how the weight enumerator of a linear code can be expressed as an evaluation of the Tutte polynomial. The result is known as *Greene's theorem* and is celebrated because it created a link between coding theory and matroid theory.

References

- [Ada94] Colin C. Adams. *The knot book*. W. H. Freeman and Company, New York, 1994. An elementary introduction to the mathematical theory of knots.
- [Bol98] Béla Bollobás. *Modern graph theory*, volume 184 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1998.
- [EMM22] Joanna Ellis-Monaghan and Iain Moffatt. *Handbook of the Tutte Polynomial and Related Topics*. CRC Press, 2022.
- [GHN06] Omer Giménez, Petr Hliněný, and Marc Noy. Computing the Tutte polynomial on graphs of bounded clique-width. *SIAM J. Discrete Math.*, 20(4):932–946, 2006.
- [GR01] Chris Godsil and Gordon Royle. *Algebraic graph theory*, volume 207 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2001.
- [Gre76] Curtis Greene. Weight enumeration and the geometry of linear codes. *Studies in Appl. Math.*, 55(2):119–128, 1976.
- [Jon85] Vaughan F. R. Jones. A polynomial invariant for knots via von Neumann algebras. *Bull. Amer. Math. Soc. (N.S.)*, 12(1):103–111, 1985.
- [JVW90] F. Jaeger, D. L. Vertigan, and D. J. A. Welsh. On the computational complexity of the Jones and Tutte polynomials. *Math. Proc. Cambridge Philos. Soc.*, 108(1):35–53, 1990.
- [Nob98] S. D. Noble. Evaluating the Tutte polynomial for graphs of bounded tree-width. *Combin. Probab. Comput.*, 7(3):307–321, 1998.
- [Oxl11] James Oxley. *Matroid theory*, volume 21 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, second edition, 2011.
- [Tut47] W. T. Tutte. A ring in graph theory. *Proc. Cambridge Philos. Soc.*, 43:26–40, 1947.
- [VW92] D. L. Vertigan and D. J. A. Welsh. The computational complexity of the Tutte plane: the bipartite case. *Combin. Probab. Comput.*, 1(2):181–187, 1992.
- [Wel76] D. J. A. Welsh. *Matroid theory*, volume No. 8 of *L. M. S. Monographs*. Academic Press [Harcourt Brace Jovanovich, Publishers], London-New York, 1976.
- [Wel93] D. J. A. Welsh. *Complexity: knots, colourings and counting*, volume 186 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1993.

- [Wel99] Dominic Welsh. The Tutte polynomial. volume 15, pages 210–228. 1999. Statistical physics methods in discrete probability, combinatorics, and theoretical computer science (Princeton, NJ, 1997).
- [Zas87] Thomas Zaslavsky. The Möbius function and the characteristic polynomial. In *Combinatorial geometries*, volume 29 of *Encyclopedia Math. Appl.*, pages 114–138. Cambridge Univ. Press, Cambridge, 1987.