RWTH Aachen

Master Thesis

From the lattice of essential flats to the Tutte polynomial of a matroid

Author:
Jens Niklas Eberhardt

Supervisor:
Prof. Dr. W. Plesken

Lehrstuhl B für Mathematik
Faculty of Mathematics, Computer Science and Natural Sciences
RWTH Aachen

April 2014

Contents

Preface

Matroids are combinatorial objects capturing notions of independence in various mathematical structures. There are different equivalent ways of defining matroids, for example by their independent sets, bases, flats or rank functions. This thesis considers matroids by their essential flats, i.e. flats whose complements are flats in the dual matroid as well. They have been extensively studied in [1], where - amongst other insights - an axiom scheme for essential flats and their ranks is given.

We are interested in essential flats because they yield new perspectives on the rank generating polynomial or equivalently the TUTTE polynomial, an important invariant with applications in different branches of combinatorics like matroid and coding theory (c.f. [2]). Formulas and interpretations for the rank generating polynomial using essential flats can be found in [3] and [4]. Based upon [3], we explore how much information about the essential flats is really necessary for the computation of the rank generating polynomial.

We introduce the (essential flat) **configuration** of a matroid, which is the abstract lattice of its essential flats enriched with their ranks and cardinalities, and present an algorithm to compute the rank generating polynomial from it. Inspired by [5] we shrink down the configuration of a matroid to a **condensed** (essential flat) **configuration**, a statistic of the arrangement of the orbits of essential flats under its automorphism group. Then we present a generalized version of the first algorithm which applies to condensed configurations as well. It follows that matroids with identical (condensed) configurations have the same rank generating polynomial. As an example we show how this generalizes a similiar statement for perfect matroid designs given in [6]. The results of this thesis can be used to construct large families of non-isomorphic matroids with the same rank generating polynomial (c.f. different approaches in [7]). Likewise they can be used computationally. The condensed configuration provides a good overview of the matroid and it can be encoded in a -for highly symmetrical matroids really small- integer matrix. For example the condensed configuration of the GOLAY code matroid mostly fits in a 6×6 matrix.

This thesis comes with a GAP[8] implementation of the algorithms.

We proceed as follows. The first chapter introduces the basics of matroid and lattice theory and results about essential flats from [1]. The second chapter contains the main results of this thesis. First the interpretation of the rank generating polynomial by its essential flats from [3] is recapitulated introducing the notion of the cloud and flock polynomial. Using the GOLAY code matroid as an example we show how to find all essential flats of a matroid by its rank generating polynomial. Then configurations, the basic algorithm, condensed configurations and the generalized algorithm are finally introduced and illustrated by examples. The last chapter is about further examples and an implementation of the algorithms. We show how perfect matroid designs can be transformed into condensed configurations, study root systems by their essential flats and construct an interesting matroid closely related to the GOLAY code matroid.

Chapter 1

Matroids, lattices and essential flats

In this chapter we introduce the basic facts about matroids, lattices and essential (cyclic, isthmus-free) flats. If you are familiar with matroids and lattices you can skip right into the third section about essential flats.

1.1 Matroids

We introduce the most important definitions based on [9].

Equivalent definitions

Definition 1.1 (Matroid)**.** Let E be a finite set and $\mathcal{I}$ a family of subsets of E. A **matroid** M is a tuple $(E, \mathcal{I})$, fulfilling:

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

(I2) If $I \in \mathcal{I}$ and $J \subseteq I$, then $J \in \mathcal{I}$.

(I3) If $I_1, I_2 \in \mathcal{I}$ and $|I_1| = |I_2| + 1$ then there is a $x \in I_1 - I_2$, s.t. $I_2 \cup \{x\} \in \mathcal{I}$.

The elements of $\mathcal{I}(M) := \mathcal{I}$ are called **independent**, the elements of $\mathcal{I}(M)^c$ **dependent** and $\mathcal{E}(M) := E$ the **ground set** of M.

Example 1.1. *1.) Let A be a matrix over a field with columns $a_1, \ldots, a_n$. Let $E := \underline{n}$ be the set of column indices and $\mathcal{I}$ consist of all subsets of E corresponding to linearly independent columns. This defines a matroid $M[A] := (E, \mathcal{I})$, called the* ***vector matroid***

of A.
2.) Let $r, n \in \mathbb{Z}_{\geq 0}$ and $r \leq n$. Then $\mathrm{U}_{r,n} = (\underline{n}, \mathrm{Pot}(\underline{n})_{\leq r})$ is a matroid, called the ***uniform matroid*** *of rank r on n points.*

Definition 1.2 (Rank function)**.** Let M be a matroid. For $X \in \mathcal{E}(M)$ let $\mathrm{r}_M(X)$ be the maximal cardinality of all independent sets contained in X. Then

$$\mathrm{r}_M : \mathrm{Pot}(\mathcal{E}(M)) \to \mathbb{Z}_{\geq 0}$$

is called the **rank function** of M.

Remark 1.3. The rank function r_M of a matroid M fulfills the following axioms:

(R1) For $X, Y \subseteq \mathcal{E}(M)$, $\mathrm{r}_M(X \cup Y) \leq \mathrm{r}_M(X) + \mathrm{r}_M(Y) - \mathrm{r}_M(X \cap Y)$, i.e r_M is a submodular function.

(R2) For $X \subseteq Y \subseteq \mathcal{E}(M)$, $\mathrm{r}_M(X) \leq \mathrm{r}_M(Y)$, i.e r_M is a monotonic.

Moreover $\mathcal{I}(M) = \{I \subseteq \mathcal{E}(M) \mid \mathrm{r}_M(I) = |I|\}$.

A matroid can be defined by its rank function. If a function $r : \mathrm{Pot}(E) \to \mathbb{Z}_{\geq 0}$ fulfills (R1) and (R2) for a finite set E, then setting $\mathcal{I} := \{I \subseteq \mathcal{E}(M) \mid r(I) = |I|\}$ defines a matroid $M := (E, \mathcal{I})$ with $r = \mathrm{r}_M$.

Definition 1.4 (Corank and nullity)**.** Let M be a matroid. For a set X in M the **corank** of X in M is $\mathrm{r}_M(M) - \mathrm{r}_M(X)$ and the **nullity** of X in M is $|X| - \mathrm{r}_M(X)$.

Example 1.2. *Let A be a matrix over a field F with columns $a_1, \ldots, a_n \in F^r$. Then*

$$\mathrm{r}_{M[A]}(X) = \dim_F(\langle a_i \mid i \in X \rangle)$$

and the nullity of X in M is $dim_F(Ker((a_i)_{i \in X}))$. So the rank coincides with the usual notion of rank or dimension in vector spaces.

Definition 1.5 (Closure operator)**.** Let M be a matroid. For $X \in \mathcal{E}(M)$ we define $\mathrm{cl}_M(X) := \{x \in \mathcal{E}(M) \mid \mathrm{r}_M(X \cup \{x\}) = \mathrm{r}_M(X)\}$. Then $\mathrm{cl}_M : \mathrm{Pot}(\mathcal{E}(M)) \to \mathrm{Pot}(\mathcal{E}(M))$ is called the **closure operator** of M.

Remark 1.6. The closure operator cl_M of a matroid M fulfills the following axioms:

(S1) For $X \subseteq \mathcal{E}(M)$, $X \subseteq \mathrm{cl}_M(X)$.

(S2) For $X \subseteq \mathcal{E}(M)$, $\mathrm{cl}_M(X) = \mathrm{cl}_M(\mathrm{cl}_M(X))$.

(S3) For $X \subseteq Y \subseteq \mathcal{E}(M)$, $\mathrm{cl}_M(X) \subseteq \mathrm{cl}_M(Y)$.

(S4) For $x, y \in \mathcal{E}(M)$ and $X \subseteq \mathcal{E}(M)$

$$x \in \mathrm{cl}_M(X \cup \{y\}) - \mathrm{cl}_M(X) \Rightarrow y \in \mathrm{cl}_M(X \cup \{x\}) - \mathrm{cl}_M(X).$$

Moreover $\mathcal{I}(M) = \{I \subseteq \mathcal{E}(M) \mid \mathrm{cl}_M(I - x) \subsetneq I \text{ for all } x \in I\}$.

Again a matroid can be defined by a function fulfilling (S1)-(S4).

Definition 1.7 (Flat)**.** Let M be a matroid. $X \in \mathcal{E}(M)$ is called a **flat** if $X = \mathrm{cl}_M(X)$. The family of flats of the matroid M is denoted by $\mathcal{L}(M)$.

Remark 1.8. The family of flats of a matroid M, $\mathcal{L}(M)$, fulfills the following axioms:

(F1) The ground set of M is a flat, $\mathcal{E}(M) \in \mathcal{L}(M)$.

(F2) For $X, Y \in \mathcal{L}(M)$, $X \cap Y \in \mathcal{L}(M)$.

(F3) For $X \in \mathcal{L}(M)$ the flats $\{Y\}$ covering X, i.e. $X \subsetneq Y$ and there is no flat in between, partition $\mathcal{E}(M) - X$.

Moreover the closure of a set X in M is the smallest flat containing X.

A family of subsets of a finite set fulfilling (F1)-(F3) defines a matroid as well.

Definition 1.9 (Circuit)**.** Let M be a matroid. A minimal dependent set in X in M is called a **circuit**. The family of circuits in M is denoted by $\mathcal{C}(M)$.

Remark 1.10. The family of circuits of a matroid M, $\mathcal{C}(M)$, fulfills the following axioms:

(C1) No proper subset of a circuit is a circuit.

(C2) For $C_1 \neq C_2 \in \mathcal{C}(M)$ and $x \in C_1 \cap C_2$, there is a circuit contained in $C_1 \cup C_2 - x$.

A set in M is independent iff it contains no circuit.

Matroid operations

Definition 1.11 (Restriction)**.** Let M be a matroid and X a set in M. Then $M|X := (X, \mathcal{I}(M) \cap X)$, where $\mathcal{I}(M) \cap X = \{I \cap X \mid I \in \mathcal{I}(M)\}$, is a matroid, called the **restriction** of M to X.

Definition 1.12 (Contraction)**.** Let M be a matroid and X a set in M and B be a basis of $M|X$. Then $M/X := (X, \mathcal{I})$, where $\mathcal{I} := \{I \subseteq \mathcal{E}(M) - X \mid I \cup B \in \mathcal{I}(M)\}$, is a matroid, called the **contraction** of M by X.

Definition 1.13 (Direct sum)**.** Let M_1 and M_2 be matroids. Then the **direct sum** of M_1 and M_2 is the matroid $M_1 \oplus M_1 := (\mathcal{E}(M_1) \uplus \mathcal{E}(M_2), \mathcal{I})$, where

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

Definition 1.14 (Loops and coloops)**.** Let M be a matroid. An element $x \in \mathcal{E}(M)$ is called a **loop** if $\{x\}$ is dependent in M and a **coloop** if x is contained in every basis of M.

Remark 1.15. Let M be a matroid and X a set in M. Let Y be the set of loops M/X, then $\mathrm{cl}_M(X) = X \cup Y$. In particular X is a flat in M iff M/X contains no loops.

Definition 1.16 (Dual matroid)**.** Let M be a matroid. Then $M^* := (\mathcal{E}(M), \mathcal{I})$, where $\mathcal{I} := \{I \subseteq \mathcal{E}(M) \mid I \text{ is contained a complement of a basis of } M\}$, is called the **dual matroid** of M.

Remark 1.17. Let M be a matroid, X a set in M and $x \in \mathcal{E}(M)$. Then

1. $(M^*)^* = M$,
2. $M/X = (M^*|(\mathcal{E}(M) - X))^*$ and
3. x is a loop in M iff x is a coloop in M^*.

Matroid isomorphism

Definition 1.18. Let M_1 and M_2 be matroids and $\phi : \mathcal{E}(M_1) \to \mathcal{E}(M_2)$ a map. Then ϕ is called an **matroid isomorphism** if

1. ϕ is a bijection and
2. for $X \subseteq \mathcal{E}(M_1)$, X is independent in M_1 iff $\phi(X)$ is independent in M_2.

M_1 and M_2 are called isomorphic if there is a matroid isomorphism between them. This yields the definition for **automorphisms** and the **automorphism group** $\mathrm{Aut}(M)$ of a matroid M.

1.2 Lattices

A lattice is a partially ordered set, s.t. each two elements have an infimum and supremum. Since the set of all (essential) flats of a matroid forms a lattice w.r.t. inclusion, we introduce the basics of lattice theory in this section based on [10].

Definitions

Definition 1.19 (Partially ordered sets and Lattices)**.** 1.) Let $L \neq \varnothing$ be a set and $\leq_L \subseteq L \times L$ a relation. Then L is called a **partially ordered set** (w.r.t. $\leq_L$) if

1. $\leq_L$ is antisymmetric, i.e. $x \leq_L y$ and $y \leq_L x$ implies $x = y$,
2. $\leq_L$ is transitive, i.e. $x \leq_L y$ and $y \leq_L z$ implies $x \leq_L z$, and
3. $\leq_L$ is reflexive, i.e. $x \leq_L x$ for all $x \in L$.

2.) Let L be a partially ordered set w.r.t. $\leq_L$ and $X \subseteq L$. Then $s \in L$ is called a **supremum** of X if

1. $x \leq_L s$ for all $x \in X$ and
2. $x \leq_L s'$ for all $x \in X$ implies $s \leq_L s'$.

The **infimum** is defined analogously.
3.) A partially ordered set L is called a **lattice** if for any two elements $x, y \in L$ the supremum, denoted by $x \vee_L y$, and the infimum, denoted by $x \wedge_L y$, exist. $\vee_L$ and $\wedge_L$ are called **join** and **meet** of L respectively.

Equivalently a lattice can be defined by join and meet operators fulfilling (V1)-(V4) of the following remark.

Remark 1.20. Let L be a lattice. Then $\vee_L$ and $\wedge_L$ fulfill the following axioms:

(V1) $x \vee_L y = y \vee_L x$ and $x \wedge_L y = y \wedge_L x$.

(V2) $(x \vee_L y) \vee_L z = x \vee_L (y \vee_L z)$ and $(x \wedge_L y) \wedge_L z = x \wedge_L (y \wedge_L z)$.

(V3) $x \vee_L x = x$ and $x \wedge_L x = x$.

(V4) $(x \vee_L y) \wedge_L x = x$ and $(x \wedge_L y) \vee_L x = x$.

Furthermore $x \leq_L y$ iff $x \wedge_L y = x$.

Definition 1.21 (Top and bottom)**.** Let L be a finite lattice. Then L contains two elements 0_L, called **bottom**, and 1_L, called **top**, s.t.

$$0_L \leq_L x \leq_L 1_L, \text{ for all } x \in L.$$

Example 1.3. *Let M be a matroid. Then $\mathcal{L}(M)$, the set of flats of M, forms a lattice w.r.t. inclusion. Meet and join are given by*

$$X \vee_{\mathcal{L}(M)} Y = \mathrm{cl}_M(X \cup Y) \text{ and}$$
$$X \wedge_{\mathcal{L}(M)} Y = X \cap Y \text{ for all } X, Y \in \mathcal{L}(M).$$

Constructions

Definition 1.22. Let L be a lattice and $x \leq_L y$. Then $[x,y]_L := \{z \in L \,|\, x \leq_L z \leq_L y\}$ is called the **interval** of x and y and is a lattice as well.

Definition 1.23. Let L be a lattice. By setting $x \leq_{L^*} y$ iff $y \leq_L x$, L becomes a lattice w.r.t. $\leq_{L^*}$. This is called the **dual lattice** of L and is denoted by L^*. The join operator of L is the meet operator in L^* and vice versa.

Homomorphisms

Definition 1.24. Let L_1 and L_2 be lattices and $\phi : L_1 \to L_2$ a map. Then ϕ is called a **lattice homomorphism** if

$$\phi(x \wedge_{L_1} y) = \phi(x) \wedge_{L_2} \phi(y) \text{ and } \phi(x \vee_{L_1} y) = \phi(x) \vee_{L_2} \phi(y) \text{ for all } x, y \in L_1.$$

If ϕ is bijective it is called a **lattice isomorphism**.

Example 1.4. *Let M be a matroid and $X \subset Y$ be flats in M. Then*

$$\phi : [X,Y]_{\mathcal{L}(M)} \to \mathcal{L}(M|Y/X) : Z \mapsto Z - X$$

*is a lattice isomorphism. Notice that the dual of the lattice of flats of a matroid is not generally isomorphic to the lattice of flats of the dual matroid. This problem is fixed by the notion of **essential flats** introduced in the next section.*

1.3 Essential flats

We introduce essential flats and some of their properties. A flat X in a matroid M is called **essential** (cyclic or isthmus-free) if $M|X$ contains no coloops. Like the set of all flats in a matroid M, the set of its essential flats, $\mathcal{Z}(M)$, forms a lattice w.r.t. inclusion and behaves well under restriction and contraction. But it has the advantage that its dual lattice is the lattice of essential flats of the dual matroid. Furthermore essential flats and their ranks can be used to define a matroid. In [1] a list of axioms for a lattice of subsets $\mathcal{Z}$ and a function $r : \mathcal{Z} \to \mathbb{Z}_{\geq 0}$ to be the lattice of essential flats of a matroid M, s.t. $r = \mathrm{r}_M|_{\mathcal{Z}}$, is given.

Definition 1.25 (Essential Flats)**.** Let M be a matroid and X be a flat of M. We call X an **essential** (cyclic, isthmus-free) **flat**, if $M|X$ contains no coloops.
We denote the collection of essential flats of M by $\mathcal{Z}(M)$.

Uniform matroids are distinguished by the triviality of their essential flats.

Example 1.5. *Let $r \leq n$.*
A subset X of $\mathrm{U}_{r,n}$ is a flat if $|X| < r$ or $X = \underline{n}$. In the first case $\mathrm{U}_{r,n}|X \cong \mathrm{U}_{|X|,|X|}$ consists of coloops and in the latter $\mathrm{U}_{r,n}|X = \mathrm{U}_{r,n}$ has coloops iff $r = n$. So summarizing

$$\mathcal{Z}(\mathrm{U}_{r,n}) = \begin{cases} \{\varnothing, \underline{n}\}, & \text{if } r < n, \\ \{\varnothing\}, & \text{if } r = n. \end{cases}$$

Conversely a matroid M is uniform iff it only has trivial essential flats. To see this, notice that the closure of a circuit is an essential flat. So if M has a non-trivial circuit C, the closure of C is a non-trivial essential flat.

Being an essential flat is a symmetric condition for a subset to be a flat and its complement to be a flat in the dual matroid as well.

Remark 1.26. Let M be a matroid and $X \subseteq \mathcal{E}(M)$. Then t.f.s.a.e.:

1. X is an essential flat.
2. M/X contains no loops and $M|X$ contains no coloops.
3. X is a flat in M and $\mathcal{E}(M) - X$ is a flat in M^*.
4. X is a flat and a union of circuits.
5. X is a flat and there is no $e \in X$, s.t. $\mathrm{r}_M(X - e) = \mathrm{r}_M(X) - 1$.

It follows that $\mathcal{Z}(M^*) = \{\mathcal{E}(M) - X \mid X \in \mathcal{Z}(M)\}$.

Each flat of a matroid contains a unique maximal essential flat which can be obtained by removing the coloops of its restriction.

Definition 1.27 (Essentiality operator)**.** Let M be a matroid.
Let X be a flat in M and $e_1, \ldots, e_s$ the coloops in $M|X$. We set

$$\mathrm{e}_M(X) := X - \{e_1, \ldots, e_s\}.$$

This defines a map

$$\mathrm{e}_M : \{\text{flats in } M\} \to \{\text{ess. flats in } M\},$$

the **essentiality operator** of M.

The essential flats of a matroid form a lattice w.r.t. inclusion.

Remark 1.28. Let M be a matroid. Then $\mathcal{Z}(M)$ is a lattice w.r.t. $\subseteq$ and join and meet are given by

1. $X_1 \wedge X_2 = \mathrm{e}_M(X_1 \cap X_2)$ and
2. $X_1 \vee X_2 = \mathrm{cl}_M(X_1 \cup X_2)$ for all $X_1, X_2 \in \mathcal{Z}(M)$.

Furthermore the lattice $\mathcal{Z}(M)$ is isomorphic to the dual lattice of $\mathcal{Z}(M^*)$.

Proof. Observe that $\mathrm{e}_M : \mathcal{L}(M) \to \mathcal{Z}(M)$ is surjective and monotonic (w.r.t. $\subseteq$). Hence $\mathcal{Z}(M)$ becomes a lattice and e_M a lattice homomorphism (i.e. it respects join and meet). The first two statements follow immediately by using join and meet in $\mathcal{L}(M)$. The last statement concerning the dual matroid follows from Remark 1.26. □

The lattice of essential flats behaves well under restriction and contraction.

Remark 1.29. Let M be a matroid and $L \subseteq U$ essential flats in M. Then

$$\phi : [L, U]_{\mathcal{Z}(M)} \to \mathcal{Z}(M|U/L) : X \mapsto X - L$$

is a lattice isomorphism.

Proof. One easily verifies that ϕ and

$$\mathcal{Z}(M|U/L) \to [L, U]_{\mathcal{L}(M)} : X \mapsto X \cup L$$

are well defined, monotonic and mutually inverse. □

The circuits, independent set, flats, etc. of a matroid can be recovered from its essential flats and their ranks.

Lemma 1.30. *Let M be a matroid. Then*

1. *$I \subseteq \mathcal{E}(M)$ is independent iff $|X \cap I| \leq \mathrm{r}_M(X)$ for all $X \in \mathcal{Z}(M)$,*
2. *$C \subseteq \mathcal{E}(M)$ is a circuit iff C is minimal with the property that there is an $X \in \mathcal{Z}(M)$ with $C \subseteq X$ and $|C| = \mathrm{r}_M(X) + 1$ and*
3. *$Y \subseteq \mathcal{E}(M)$ is a flat iff there is an $X \in \mathcal{Z}(M)$ s.t. $Y = X \uplus C$ and there is no $X' \in \mathcal{Z}(M)$ and $C' \subseteq C$ s.t. $X \cup C' \subsetneq X'$ and $\mathrm{r}_M(X') \leq \mathrm{r}_M(X) + |C'|$.*

Proof. 1.) and 2.) C.f. [1].
3.) Think of X as $\mathrm{e}_M(Y)$ and keep in mind that the closure of a circuit is an essential flat. □

Corollary 1.31. *A matroid M is determined by $\mathcal{Z}(M)$ and $\mathrm{r}_M|_{\mathcal{Z}(M)}$.*

We can also define a matroid by its essential flats and their ranks.

Theorem 1.32. *Let E be a finite set, $\mathcal{Z} \subseteq \mathrm{Pot}(E)$ and $r : \mathcal{Z} \to \mathbb{Z}_{\geq 0}$.*
There is a matroid M with $\mathcal{E}(M) = E$, $\mathcal{Z}(M) = \mathcal{Z}$ and $\mathrm{r}_M|_{\mathcal{Z}} = r$ iff

(Z1) $\mathcal{Z}$ is a lattice w.r.t. inclusion,

(Z2) $r(0_{\mathcal{Z}}) = 0$,

(Z3) for all $X, Y \in \mathcal{Z}$ with $X \subsetneq Y$

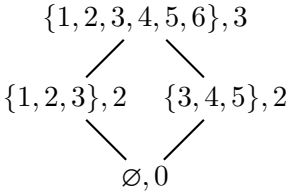
$$0 < r(Y) - r(X) < |Y| - |X|$$

(Z4) and for all $X, Y \in \mathcal{Z}$

$$r(X) + r(Y) \geq r(X \vee Y) + r(X \wedge Y) + |(X \cap Y) - (X \wedge Y)|.$$

Proof. C.f. [1]. The basic idea is to define a set $\mathcal{C}$ according to Lemma 1.30 and to show that $\mathcal{C}$ is the set of circuits of a matroid M. It then remains to show that $\mathcal{Z}(M) = \mathcal{Z}$ and $\mathrm{r}_M|_{\mathcal{Z}} = r$. □

Example 1.6. *We are now able to define a matroid by a lattice of subsets together with ranks.*
1.) Consider the lattice given by



where we marked all sets with their rank. Its easy to see that axioms (Z1)-(Z4) are fulfilled and the circuits and bases of the resulting matroid M are

$$\mathcal{C}(M) = \{\{1, 2, 3\}, \{3, 4, 5\}\} \text{ and}$$
$$\mathcal{B}(M) = \mathrm{Pot}(\underline{6}) - \mathcal{C}(M).$$

2.) It is important that the lattice of essential flats is given by a concrete realization as a lattice of subsets. Let $r \in \mathbb{Z}_{\geq 0}$. Then the uniform matroids $\mathrm{U}_{r,n}$ are non-isomorphic for all pw. distinct $n > r$, but their abstract lattice of essential flats together with their ranks coincide (cf. Example 1.5).

Chapter 2

Essential flats and the rank generating polynomial

2.1 Flocks, clouds and the rank generating polynomial.

The rank generating polynomial of a matroid M can be expressed in terms of its essential flats (c.f [4] and [3]). All results of this thesis are based upon the cloud/flock interpretation of [3], which we will recapitulate in this section.

Definition 2.1 (Rank generating polynomial)**.** Let M be a matroid.
$\mathrm{S}(M;\mathrm{x},\mathrm{y}) \in \mathbb{Z}[\mathrm{x},\mathrm{y}]$, the **rank generating polynomial** of M, is defined by

$$\mathrm{S}(M;\mathrm{x},\mathrm{y}) = \sum_{X \subseteq \mathcal{E}(M)} \mathrm{x}^{\mathrm{r}_M(M)-\mathrm{r}_M(X)}\,\mathrm{y}^{|X|-\mathrm{r}_M(X)}.$$

Remark 2.2. A perhaps more famous invariant, the Tutte **polynomial** $\mathrm{T}(M;\mathrm{x},\mathrm{y})$ of a matroid M, can be obtained from the rank generating polynomial by a simple substitution

$$\mathrm{T}(M;\mathrm{x},\mathrm{y}) = \mathrm{S}(M;x-1,y-1).$$

Example 2.1. *We will often represent the rank generating polynomial* $\mathrm{S}(M;\mathrm{x},\mathrm{y}) = \sum_{i,j} a_{i,j}\,\mathrm{x}^i\,\mathrm{y}^j$ *of a matroid* M *by its coefficient matrix* $(a_{i,j})_{i,j}$*. Let* $r < n$*. Consider* $\mathrm{U}_{r,n}$*, the uniform matroid of rank* r *and cardinality* n*. Its rank generating polynomial is*

$$\sum_{0 \le i < r} \binom{n}{i} \mathrm{x}^{r-i} + \sum_{r \le i \le n} \binom{n}{i} \mathrm{y}^{i-r}$$

which yields the coefficient matrix:

$$\begin{array}{c|ccc} \binom{n}{r} & \cdots & \binom{n}{n-1} & \mathbf{1} \\ \vdots & & & \\ \binom{n}{1} & & & \\ \mathbf{1} & & & \end{array}$$

To interpret the rank generating polynomial of a matroid M in terms of its essential flats we sort the subsets of $\mathcal{E}(M)$ by

$$\mathrm{Pot}(\mathcal{E}(M)) \xrightarrow{\mathrm{cl}_M} \mathcal{L}(M) \xrightarrow{\mathrm{e}_M} \mathcal{Z}(M)$$

where $\mathcal{L}(M)$ is the set of flats and $\mathcal{Z}(M)$ the set of the essential flats of M. This yields

$$\mathrm{Pot}(\mathcal{E}(M)) = \biguplus_{X \in \mathcal{Z}(M)} \mathrm{cl}_M^{-1}(\mathrm{e}_M^{-1}(\{X\})).$$

The basic idea is to group together the summands of the rank generating polynomial according to this. We define

Definition 2.3 (Flock and cloud)**.** Let M be a Matroid.

1. For an essential flat X in M we call $\mathrm{e}_M^{-1}(X)$ the **cloud** of X in M.
2. For a flat X in M we call $\mathrm{cl}_M^{-1}(X)$ the **flock** of X in M.

and counting polynomials for clouds and flocks

Definition 2.4 (Cloud and flock polynomial)**.** Let M be a matroid.

1. Let X be an essential flat in M. Then $\mathrm{c}(M, X; \mathrm{x}) \in \mathbb{Z}[\mathrm{x}]$, the **cloud polynomial** of X in M is
$$\mathrm{c}(M, X; \mathrm{x}) := \sum_{Y \in \mathrm{e}_M^{-1}(X)} \mathrm{x}^{\mathrm{r}_M(M) - \mathrm{r}_M(Y)}.$$
2. Let X be a flat in M. Then $\mathrm{f}(M, X; \mathrm{y}) \in \mathbb{Z}[\mathrm{y}]$, the **flock polynomial** of X in M is
$$\mathrm{f}(M, X; \mathrm{y}) := \mathrm{S}(M; 0, y) = \sum_{Y \in \mathrm{cl}_M^{-1}(X)} \mathrm{y}^{|Y| - \mathrm{r}_M(Y)}.$$

Example 2.2. *Let $r < n$. Then the cloud of $\varnothing$ in $\mathrm{U}_{r,n}$ is $\mathrm{Pot}_{<r}(\underline{n}) = \{X \subseteq \underline{n} \,|\, |X| < r\}$, the flock of $\underline{n}$ is $\mathrm{Pot}_{\geq r}(\underline{n})$, the flock of $\varnothing$ is $\{\varnothing\}$ and the cloud of $\underline{n}$ is $\{\underline{n}\}$. Summarizing*

$$\begin{aligned} \mathrm{c}(\mathrm{U}_{r,n}, \varnothing; \mathrm{x}) &= \textstyle\sum_{0 \leq i < r} \binom{n}{i} \mathrm{x}^{r-i} & \mathrm{f}(\mathrm{U}_{r,n}, \varnothing; \mathrm{y}) &= 1 \\ \mathrm{f}(\mathrm{U}_{r,n}, \underline{n}; \mathrm{y}) &= \textstyle\sum_{r \leq i \leq n} \binom{n}{i} \mathrm{y}^{i-r} & \mathrm{c}(\mathrm{U}_{r,n}, \underline{n}; \mathrm{x}) &= 1. \end{aligned}$$

We are now able to state the cloud and flock formula for the rank generating polynomial.

Theorem 2.5. *Let M be a matroid. Then*

$$\mathrm{S}(M;\mathrm{x},\mathrm{y}) = \sum_{X\in\mathcal{Z}(M)} \mathrm{f}(M,X;\mathrm{y})\,\mathrm{c}(M,X;\mathrm{x}).$$

For the proof we notice that the flock polynomials of flats in one cloud coincide.

Lemma 2.6. *Let M be a matroid, X be an essential flat, Y be in the cloud of X and $e_1,\dots,e_s$ (pairwise distinct) be the coloops in $M|Y$. Then*

$$\mathrm{cl}_M^{-1}(Y) \to \mathrm{cl}_M^{-1}(X) : Z \mapsto Z - \{e_1,\dots,e_s\}$$

is a bijection and

$$\mathrm{f}(M,Y;\mathrm{y}) = \mathrm{f}(M,X;\mathrm{y}).$$

Proof. The first statement is trivial. For the second one notice that for Z the flock of Y

$$|Z| - \mathrm{r}_M(Z) = |Z - \{e_1,\dots,e_s\}| - \mathrm{r}_M(Z - \{e_1,\dots,e_s\})$$

□

Proof of Theorem 2.5. The partition of $\mathcal{E}(M)$ yields

$$\mathrm{S}(M;\mathrm{x},\mathrm{y}) = \sum_{X\in\mathcal{Z}(M)} \sum_{Y\in\mathrm{e}_M^{-1}(X)} \sum_{Z\in\mathrm{cl}_M^{-1}(Y)} \mathrm{y}^{|Z|-\mathrm{r}_M(Z)}\,\mathrm{x}^{\mathrm{r}_M(M)-\mathrm{r}_M(Z)}.$$

For all $Z \in \mathrm{cl}_M^{-1}(Y)$, $\mathrm{r}_M(Z) = \mathrm{r}_M(Y)$, hence

$$\begin{aligned} &= \sum_{X\in\mathcal{Z}(M)} \sum_{Y\in\mathrm{e}_M^{-1}(X)} \mathrm{x}^{\mathrm{r}_M(M)-\mathrm{r}_M(Y)} \sum_{Z\in\mathrm{cl}_M^{-1}(Y)} \mathrm{y}^{|Z|-\mathrm{r}_M(Z)} \\ &= \sum_{X\in\mathcal{Z}(M)} \sum_{Y\in\mathrm{e}_M^{-1}(X)} \mathrm{x}^{\mathrm{r}_M(M)-\mathrm{r}_M(Y)}\,\mathrm{f}(M,Y;\mathrm{y}). \end{aligned}$$

Now Lemma 2.6 yields

$$\begin{aligned} &= \sum_{X\in\mathcal{Z}(M)} \sum_{Y\in\mathrm{e}_M^{-1}(X)} \mathrm{x}^{\mathrm{r}_M(M)-\mathrm{r}_M(Y)}\,\mathrm{f}(M,X;\mathrm{y}) \\ &= \sum_{X\in\mathcal{Z}(M)} \mathrm{f}(M,X;\mathrm{y})\,\mathrm{c}(M,X;\mathrm{x}). \end{aligned}$$

□

Example 2.3. *Let $r < n$. In the light of Theorem 2.5 we can interpret the rank generating polynomial of $\mathrm{U}_{r,n}$ in terms of clouds and flocks. Remember that the essential flats of $\mathrm{U}_{r,n}$ are $\varnothing$ and $\underline{n}$ (Example 1.5). Hence*

$$\begin{aligned}\mathrm{S}(\mathrm{U}_{r,n};\mathrm{x},\mathrm{y}) &= \mathrm{f}(\mathrm{U}_{r,n},\varnothing;\mathrm{y})\,\mathrm{c}(\mathrm{U}_{r,n},\varnothing;\mathrm{x}) + \mathrm{f}(\mathrm{U}_{r,n},\underline{n};\mathrm{y})\,\mathrm{c}(\mathrm{U}_{r,n},\underline{n};\mathrm{x}) \\ &= \sum_{0\le i<r}\binom{n}{i}\mathrm{x}^{r-i} + \sum_{r\le i\le n}\binom{n}{i}\mathrm{y}^{i-r}\,.\end{aligned}$$

In the next section we will discuss some more involved examples. An important property of clouds, flocks and their polynomials is that they only depend on the contraction, resp. restriction of the matroid by the considered set.

Lemma 2.7. *Let M be a Matroid and X an essential flat.*

1. *The cloud of X in M and the cloud of $\varnothing$ in M/X are in bijection*

$$\mathrm{e}_M^{-1}(\{X\}) \to \mathrm{e}_{M/X}^{-1}(\{\varnothing\}) : Y \mapsto Y - X$$

and the cloud polynomials coincide

$$\mathrm{c}(M,X;\mathrm{x}) = \mathrm{c}(M/X,\varnothing;\mathrm{x}).$$

2. *The flock of X in M and the flock of X in $M|X$ are the same*

$$\mathrm{e}_M^{-1}(\{X\}) = \mathrm{e}_{M|X}^{-1}(\{X\})$$

and the flock polynomials coincide

$$\mathrm{f}(M,X;\mathrm{y}) = \mathrm{f}(M|X,X;\mathrm{y}).$$

2.2 Using the rank generating polynomial to find all essential flats

In this section we formulate an algorithm briefly addressed in [3] to find all essential flats in a matroid M using its rank generating polynomial. An easy way to find essential flats is to take a random subset $X \subseteq \mathcal{E}(M)$ and calculate $\mathrm{e}_M(\mathrm{cl}_M(X))$. Theorem 2.5 can be used as a break condition for this probabilistic approach. We just continuously subtract the share of newly found essential flats on the rank generating polynomial until it disappears. The random search will be structured by the extreme exponents of the rank generating polynomial.

Definition 2.8. Let $f = \sum_{i,j} a_{i,j} X^i Y^j \in \mathbb{Z}[\mathrm{x},\mathrm{y}]$. We call the exponent (i,j) **extreme** if $a_{i,j} > 0$, $a_{i+k,j} = 0$ and $a_{i,j+k} = 0$ for all $k \geq 1$.

Lemma 2.9. *Let M be a matroid and $\mathrm{S}(M;\mathrm{x},\mathrm{y}) = \sum_{i,j} a_{i,j} X^i Y^j$. If (i,j) is extreme in $\mathrm{S}(M;\mathrm{x},\mathrm{y})$ then there are exactly $a_{i,j}$ essential flats of corank i and nullity j in M.*

Proof. The coefficient $a_{i,j}$ is the number of subsets of M with corank i and nullity j. Now let X be such a subset.
Assume $X \subsetneq \mathrm{cl}_M(X)$. Then $\mathrm{cl}_M(X)$ has the same corank but greater nullity then X. Hence $a_{i,j+k} > 0$ for $k = |\mathrm{cl}_M(X) - X|$ which is a contradiction. So X is a flat.
Analogously assume $\mathrm{e}_M(X) \subsetneq X$. Then $\mathrm{e}_M(X)$ has the same nullity but greater corank than X. Hence $a_{i+k,j} > 0$ for $k = |X - \mathrm{e}_M(X)|$ which is a contradiction. So X is an essential flat. □

We first illustrate the algorithm by an example.

Example 2.4 (Golay code)**.** *Consider the matrix*

$$A := \begin{pmatrix}
1&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&1&\cdot&1&\cdot&1&1&1&\cdot&\cdot&\cdot&1&1\\
\cdot&1&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&1&1&1&1&1&\cdot&\cdot&1&\cdot&\cdot&1&\cdot\\
\cdot&\cdot&1&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&1&1&\cdot&1&\cdot&\cdot&1&\cdot&1&\cdot&1&1\\
\cdot&\cdot&\cdot&1&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&1&1&\cdot&\cdot&\cdot&1&1&1&\cdot&1&1&\cdot\\
\cdot&\cdot&\cdot&\cdot&1&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&1&1&\cdot&\cdot&1&1&\cdot&1&1&\cdot&\cdot&1\\
\cdot&\cdot&\cdot&\cdot&\cdot&1&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&1&1&\cdot&\cdot&1&1&\cdot&1&1&\cdot&1\\
\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&1&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&1&1&\cdot&\cdot&1&1&\cdot&1&1&1\\
\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&1&\cdot&\cdot&\cdot&\cdot&1&\cdot&1&1&\cdot&1&1&1&1&\cdot&\cdot&\cdot\\
\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&1&\cdot&\cdot&\cdot&\cdot&1&\cdot&1&1&\cdot&1&1&1&1&\cdot&\cdot\\
\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&1&\cdot&\cdot&\cdot&\cdot&1&\cdot&1&1&\cdot&1&1&1&1&\cdot\\
\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&1&\cdot&1&\cdot&1&1&1&\cdot&\cdot&\cdot&1&1&\cdot&1\\
\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&1&\cdot&1&\cdot&1&1&1&\cdot&\cdot&\cdot&1&1&1
\end{pmatrix} \in \mathbb{F}_2^{12\times 24}.$$

Then the row space of A is the extended binary Golay *code and the columns of A form the* Golay *code matroid $M := M[A]$. Its automorphism group is the* Mathieu *group M_{24} and generated by*

$g_1 := (1,22,8,19,21,12,6,13,5,10,3,23)(2,11,20,4,9,15,16,18,14,17,24,7)$ *and*
$g_2 := (1,10,22,18,4,2,20)(3,9,15,7,21,19,17,24,5,6,8,16,23,12)(13,14)$.

The coefficient matrix of the rank generating polynomial is

1391040	2071104	1870176	1295360	734712	346104	$\binom{24}{6}$	$\cdots$	**1**
2071104	1277696	425040	91080	12144	**759**			
1870176	425040	**35420**						
1295360	91080							
734712	12144							
346104	**759**							
$\binom{24}{6}$								
$\vdots$								
1								

We marked the coefficients corresponding to the extreme exponents, namely $(12,0)$,$(5,1)$, $(2,2)$, $(1,5)$ *and* $(0,12)$, *in bold. The corresponding essential flats are all conjugated under the automorphism group and representatives for the five orbits are given by*

$$
\begin{aligned}
R_1 &:= \varnothing \\
R_2 &:= \{1,2,3,5,6,10,19,20\} \\
R_3 &:= \{1,2,3,4,5,6,7,8,9,10,19,20\} \\
R_4 &:= \{1,2,3,4,5,6,7,8,9,10,11,13,15,19,20,21\} \\
R_5 &:= \underline{24}
\end{aligned}
$$

We calculate cloud and flock polynomials of $R_2,\ldots,R_4$ *and see that*

$$\mathrm{S}(M;\mathrm{x},\mathrm{y}) - \sum_{i=2}^{4} |M_{24}.R_i|\,\mathrm{c}(M,R_i;\mathrm{x})\,\mathrm{f}(M,R_i;\mathrm{y}).$$

has the new extreme exponent $(1,1)$ *with coefficient* 2576. *Corresponding to this coefficient we find another orbit of length* 2576 *with representative*

$$R_4^a := \{1,3,4,5,6,7,8,12,13,14,17,23\}.$$

Now the only extreme coefficients left in

$$\mathrm{S}(M;\mathrm{x},\mathrm{y}) - \sum_{i=2}^{4} |M_{24}.R_i|\,\mathrm{c}(M,R_i;\mathrm{x})\,\mathrm{f}(M,R_i;\mathrm{y}) - |M_{24}.R_3^a|\,\mathrm{c}(M,R_4^a;\mathrm{x})\,\mathrm{f}(M,R_4^a;\mathrm{y})$$

are $(12,0)$ *and* $(0,12)$ *corresponding to* $\varnothing$ *and* $\underline{24}$. *So we know that*

$$\mathcal{Z}(M) = \biguplus_{i=1}^{5} M_{24}.R_i \uplus M_{24}.R_4^a$$

and we found all essential flats in M.
Let $P := \{R_1, R_2, R_3, R_4^a, R_4, R_5\}$. For an overview of the lattice $\mathcal{Z}(M)$ we calculate $w(R,S) := |\{R \subseteq X | X \in M_{24}.S\}|$, the number of times R appears as a subset in the orbit of S for $R, S \in B$. Then

$$(w(R,S))_{R,S\in P} = \begin{pmatrix} 1 & 759 & 35420 & 2576 & 759 & 1 \\ 0 & 1 & 140 & 0 & 30 & 1 \\ 0 & 0 & 1 & 0 & 3 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

$$(|R|)_{R\in P} = (0, 8, 12, 12, 16, 24) \text{ and}$$
$$(\mathrm{r}_M(R))_{R\in P} = (0, 7, 10, 11, 11, 12).$$

In the next sections we will see how conversely the rank generating polynomial of M can be computed from the matrix $(w(R,S))_{R,S\in P}$ and the ranks an cardinalities of the $R \in P$.

To proceed we first need algorithms to compute rank generating, cloud and flock polynomials. The standard recursive deletion/contraction algorithm for the rank generating polynomial is derived from the following theorem.

Theorem 2.10 (Deletion/contraction formula)**.** *Let M be a matroid, $e \in \mathcal{E}(M)$ a point in M, $r_1 := 1 - \mathrm{r}_M(\{e\})$ and $r_2 := \mathrm{r}_M(\mathcal{E}(M)) - \mathrm{r}_M(\mathcal{E}(M) - e)$. Then*

$$\mathrm{S}(M; \mathrm{x}, \mathrm{y}) = \mathrm{y}^{r_1}\, \mathrm{S}(M|\,\mathcal{E}(M) - e; \mathrm{x}, \mathrm{y}) + \mathrm{x}^{r_2}\, \mathrm{S}(M/e; \mathrm{x}, \mathrm{y}).$$

There are many optimized implementations of this algorithm which is inherently exponential in the size of the ground set of the matroid; for example in the GAP[8] package alcove. It immediately yields an algorithm for the flock polynomial since for an essential flat X in a matroid M

$$\mathrm{f}(M, X; \mathrm{y}) = \mathrm{f}(M|X, X; \mathrm{y}) = \mathrm{S}(M|X; 0, \mathrm{y})$$

(c.f. Lemma 2.7). The cloud polynomial of an essential flat X cannot be obtained from the rank generating polynomial by a substitution. Instead we just compute the whole cloud of X by successively adding points to X and checking if the resulting set is still a flat. Summarized we get the algorithm:
EssentialFlats:
Input: A matroid M on n points of rank r without loops an coloops (optional: $G \leq \mathrm{Aut}(M)$).

Output: $\mathcal{Z}(M)$, the essential flats of M.
Algorithm:
1.) Calculate $S \coloneqq \mathrm{S}(M;\mathrm{x},\mathrm{y})$, set $\mathcal{Z} \coloneqq \varnothing$.
2.) Set $C \coloneqq \{\text{extreme coefficients in } S\}$.
3.) If $C = \{(r,0),(0,n)\}$ return $\mathcal{Z} \cup \{\varnothing, \mathcal{E}(M)\}$.
4.) Search for an essential flat $X \notin \mathcal{Z}$ corresponding to an exponent in $C - \{(r,0),(0,n)\}$.
5.) Set $S \coloneqq S - |G.X|\,\mathrm{c}(M,X;\mathrm{x})\,\mathrm{f}(M,X;\mathrm{y})$ and $\mathcal{Z} \coloneqq Z \cup G.X$.
6.) Goto 2.)

Notice that the algorithm avoids the computation of the cloud and flock polynomial for the empty set and the ground set of the matroid M, since their computations are the most expensive and can be evaded.

2.3 Essential flat configurations

In the last sections we interpreted the rank generating polynomial of a matroid in terms of its essential flats. We will use this perspective to show that the rank generating polynomial of a matroid only depends on a statistic on the abstract lattice of its essential flats. This approach yields a new algorithm for the computation of the rank generating polynomial. We will first give a basic version of our results. We introduce the (essential flat) **configuration** of matroid, i.e. the abstract lattice of its essential flats together with their ranks and cardinalities, and show how to compute the rank generating polynomial from it. Then we will, for highly symmetrical matroids dramatically, shrink down the information needed by the first basic algorithm. We introduce the **condensed** (essential flat) **configuration** of matroid, our statistic of orbits of its essential flats, and present the final algorithm, which will show that the rank generating polynomial of matroid only depends from this condensed information. An implementation of this algorithm can be found in the last chapter of this thesis.

2.3.1 The essential flat configuration

The essential flats of a matroid form a lattice under inclusion and together with their ranks determine the matroid. Forgetting the realization of this lattice as an lattice of subsets and only considering the abstract lattice of essential flats together with their cardinalities and ranks affords the essential flat configuration.

Definition 2.11. An (essential flat) **configuration** $\mathcal{Z} = (L, n, r)$ is a lattice L together with

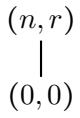
1. $n : L \to \mathbb{Z}_{\geq 0}$ monotonic, the **cardinality function**, and
2. $r : L \to \mathbb{Z}_{\geq 0}$ monotonic, the **rank function**.

Let M be a matroid without loops and coloops. We call $\mathcal{Z} = (L, n, r)$ the (essential flat) **configuration** of M, if there is a lattice isomorphism $\phi : \mathcal{Z}(M) \to L$, s.t.

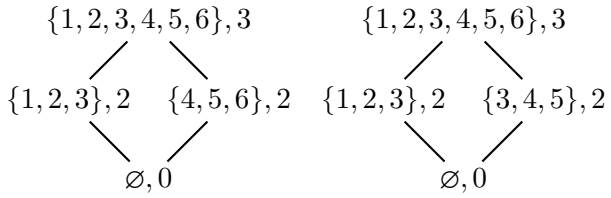
1. $\mathrm{r}_M(X) = r(\phi(X))$ and
2. $|X| = n(\phi(X))$ for all $X \in \mathcal{Z}(M)$.

Notice that we only define configurations for matroids without loops and coloops. This will be more convenient in some proofs and is not a real restriction.

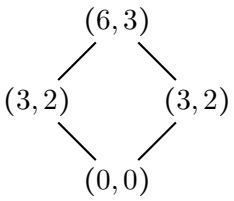
Example 2.5. *1.) We represent a configuration $\mathcal{Z} = (L, n, r)$ by the Hasse diagram of L and labels $(n(X), r(X))$ for the rank and cardinality of the $X \in L$. The configuration of a uniform matroid $\mathrm{U}_{r,n}$ for $r < n$ is given by*



Notice that $\mathrm{U}_{r,n}$ is the only matroid with this particular configuration (c.f. Example 1.5). Generally there a large families of non-isomorphic matroids with the same configuration: 2.) We define two matroids by their essential flats with their ranks



They are clearly non-isomorphic and have the same configuration



In this case the configuration "cannot see" the cardinality of the intersection of the two non-trivial essential flats.

By abuse of notation we introduce the notion of an interval for configurations.

Definition 2.12. Let $\mathcal{Z} = (L, n, r)$ be a configuration $X, Y \in L$ with $X \leq_L Y$. Then we define the configuration $[X, Y]_{\mathcal{Z}} := ([X, Y]_L, n', r')$, where

1. $n'(Z) := n(Z) - n(X)$ and
2. $r'(Z) := r(Z) - r(X)$ for all $Z \in L$.

Essential flat configurations are compatible with restriction and contraction by essential flats.

Lemma 2.13. *Let M be a matroid with configuration $\mathcal{Z}$ w.r.t. the lattice isomorphism ϕ and $X \subseteq Y$ be essential flats in M. Then $[\phi(X), \phi(Y)]_{\mathcal{Z}}$ is the configuration of $M|Y/X$.*

2.3.2 From a configuration to the rank generating polynomial

We are now able to state our first main theorem.

Theorem 2.14. *The rank generating polynomial of a matroid is already determined by its essential flat configuration.*

We prove this by introducing an algorithm, which recursively computes the cloud and flock polynomials of all essential flats of a matroid using only its essential flat configuration. This actually proves a stronger statement, since the cloud and flock polynomials contain more information than the rank generating polynomial taken by itself. The algorithm is based on the following idea. Both cloud and flock polynomial of the empty set and the ground set of a matroid are already determined by the cloud and flock polynomials of all remaining essential flats. These polynomials only depend on a proper interval in the configuration and can hence be computed recursively. This is illustrated in the next example.

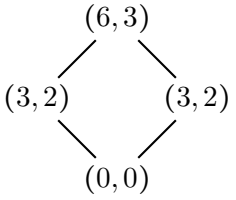
Example 2.6. *We continue with example 2.5.*
1.) For $r < n$ a matroid M with the configuration

$$\begin{array}{c}(n,r)\\ \big|\\ (0,0)\end{array}$$

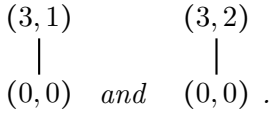
is isomorphic to $\mathrm{U}_{r,n}$. Hence (c.f. Example 2.2)

$$\begin{aligned} \mathrm{c}(M,\varnothing;\mathrm{x}) &= \textstyle\sum_{0\leq i<r}\binom{n}{i}\mathrm{x}^{r-i} & \mathrm{f}(M,\varnothing;\mathrm{y}) &= 1\\ \mathrm{f}(M,\mathcal{E}(M);\mathrm{y}) &= \textstyle\sum_{r\leq i\leq n}\binom{n}{i}\mathrm{y}^{i-r} & \mathrm{c}(M,\mathcal{E}(M);\mathrm{x}) &= 1 \end{aligned}$$

2.) Now lets consider a matroid M with configuration



Denote the essential flats of M corresponding to $(3,2)$ by X_1 and X_2. By Lemma 2.13 the configurations of M/X_i, resp. $M|X_i$ are



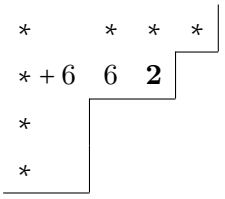
Hence using Lemma 2.7 and 1.)

$$\begin{aligned} &\mathrm{c}(M, X_i; \mathrm{x}) = \mathrm{c}(M/X_i, \varnothing; \mathrm{x}) = \mathrm{x} \quad \textit{and} \\ &\mathrm{f}(M, X_i; \mathrm{y}) = \mathrm{f}(M|X_i, X_i; \mathrm{y}) = 3 + 3\,\mathrm{y} + \mathrm{y}^2 . \end{aligned}$$

Since $\mathrm{c}(M, \mathcal{E}(M); \mathrm{x}) = \mathrm{f}(M, \varnothing; \mathrm{y}) = 1$ the rank generating polynomial of M is

$$\begin{aligned} \mathrm{S}(M; \mathrm{x}, \mathrm{y}) &= \sum_{X \in \mathcal{Z}(M)} \mathrm{f}(M, X; \mathrm{y})\, \mathrm{c}(M, X; \mathrm{x}) \\ &= 2x(3 + 3\,\mathrm{y} + \mathrm{y}^2) + \mathrm{c}(M, \varnothing; \mathrm{x}) + \mathrm{f}(M, \mathcal{E}(M); \mathrm{y}) \end{aligned}$$

and its coefficient matrix looks like



To fill in the gaps we use the identity

$$\begin{aligned} \mathrm{S}(M; \mathrm{x}, \mathrm{x}^{-1}) &= \sum_{X \subseteq \mathcal{E}(M)} \mathrm{x}^{\mathrm{r}_M(M) - \mathrm{r}_M(X)}\, \mathrm{x}^{-(|X| - \mathrm{r}_M(X))} \\ &= \sum_{X \subseteq \mathcal{E}(M)} \mathrm{x}^{\mathrm{r}_M(M) - |X|} \\ &= \sum_{0 \le i \le 6} \binom{6}{i} \mathrm{x}^{3-i} \end{aligned}$$

which means that the sum over the i-th diagonal (starting with $i = 0$ *and counting from bottom to top) in the coefficient matrix of* $\mathrm{S}(M;\mathrm{x},\mathrm{y})$ *equals* $\binom{6}{i}$*. Hence the rank generating polynomial of* M *is given by*

$$\begin{array}{llll} 14 & 13 & 6 & \mathbf{1} \\ 9+6 & 6 & \mathbf{2} & \\ 6 & & & \\ \mathbf{1} & & & \end{array}$$

Apparently M *is not a direct sum of coloops, so* $\mathrm{c}(M,\varnothing;\mathrm{x})$ *has no constant term and hence*

$$\mathrm{c}(M,\varnothing;\mathrm{x}) = 1\,\mathrm{x}^3 + 6\,\mathrm{x}^2 + 9\,\mathrm{x} \quad \textit{and}$$
$$\mathrm{f}(M,\mathcal{E}(M);\mathrm{y}) = 14 + 13\,\mathrm{y} + 6\,\mathrm{y}^2 + \mathrm{y}^3\,.$$

The following definition and lemma provide necessary tools for our algorithm.

Definition 2.15. We define $\mathbb{Z}$-linear maps

$$\mathrm{d}_\mathrm{x} : \mathbb{Z}[\mathrm{x},\mathrm{y}] \to \mathbb{Z}[\mathrm{x}], f \mapsto \sum_{1\le i} a_i\,\mathrm{x}^i, \text{ for } f(\mathrm{x},\mathrm{x}^{-1}) = \sum_i a_i\,\mathrm{x}^i \text{ and}$$
$$\mathrm{d}_\mathrm{y} : \mathbb{Z}[\mathrm{x},\mathrm{y}] \to \mathbb{Z}[\mathrm{y}], f \mapsto \sum_{0\le i} b_i\,\mathrm{y}^i, \text{ for } f(\mathrm{y}^{-1},\mathrm{y}) = \sum_i b_i\,\mathrm{y}^i$$

and for $r < n$ a notation for the cloud and flock polynomials of the uniform matroid $\mathrm{U}_{r,n}$:

$$\mathrm{cu}_{n,r}(\mathrm{x}) := \mathrm{d}_\mathrm{x}(\mathrm{S}(\mathrm{U}_{r,n};\mathrm{x},\mathrm{y})) = \mathrm{c}(\mathrm{U}_{r,n},\varnothing;\mathrm{x}) = \sum_{0\le i<r} \binom{n}{i} \mathrm{x}^{r-i} \text{ and}$$
$$\mathrm{fu}_{n,r}(\mathrm{y}) := \mathrm{d}_\mathrm{y}(\mathrm{S}(\mathrm{U}_{r,n};\mathrm{x},\mathrm{y})) = \mathrm{f}(\mathrm{U}_{r,n},\underline{n};\mathrm{y}) = \sum_{r\le i\le n} \binom{n}{i} \mathrm{y}^{i-r}\,.$$

and for $r = k = 0$

$$\mathrm{cu}_{0,0}(\mathrm{x}) := \mathrm{fu}_{0,0}(\mathrm{y}) = 1.$$

Lemma 2.16. *Let* M *be a matroid of rank* r *on* n *points without loops and coloops. Then*

1. $\mathrm{S}(M;\mathrm{x},\mathrm{x}^{-1}) = \sum_{0\le i\le n} \binom{n}{i} \mathrm{x}^{r-i}$,
2. $\mathrm{d}_\mathrm{x}(\mathrm{S}(M;\mathrm{x},\mathrm{y})) = \mathrm{cu}_{n,r}(\mathrm{x})$,
3. $\mathrm{d}_\mathrm{y}(\mathrm{S}(M;\mathrm{x},\mathrm{y})) = \mathrm{fu}_{n,r}(\mathrm{y})$,
4. $\mathrm{c}(M,\mathcal{E}(M);\mathrm{x}) = \mathrm{f}(M,\varnothing;\mathrm{y}) = 1$,

5. $\mathrm{d_x}(\mathrm{c}(M,\varnothing;\mathrm{x})) = \mathrm{c}(M,\varnothing;\mathrm{x})$ *and*
   $\mathrm{d_y}(\mathrm{c}(M,\varnothing;\mathrm{x})) = 0$,

6. $\mathrm{d_x}(\mathrm{f}(M,\mathcal{E}(M);\mathrm{y})) = 0$ *and*
   $\mathrm{d_y}(\mathrm{f}(M,\mathcal{E}(M);\mathrm{y})) = \mathrm{f}(M,E;\mathrm{y})$.

Proof. 1.) follows by substituting y by x^{-1} in the definition of the rank generating polynomial (c.f. Example 2.6 2.)).
2.) and 3.) follow from 1.) by the definition of $\mathrm{d_x}$, $\mathrm{d_y}$, $\mathrm{cu}_{n,r}(\mathrm{x})$ and $\mathrm{fu}_{n,r}(\mathrm{y})$.
4.) We have $\mathrm{e}_M^{-1}(\mathcal{E}(M)) = \{\mathcal{E}(M)\}$ and $\mathrm{cl}_M^{-1}(\varnothing) = \{\varnothing\}$.
5.) Since M does not consist of coloops there is no set of rank r in the cloud of $\varnothing$. Hence $\mathrm{c}(M,\varnothing;\mathrm{x}) \in \mathbb{Z}[\mathrm{x}]$ has no constant term and by the definition of $\mathrm{d_x}$ and $\mathrm{d_y}$

$$\mathrm{d_x}(\mathrm{c}(M,\varnothing;\mathrm{x})) = \mathrm{c}(M,\varnothing;\mathrm{x}) \text{ and}$$
$$\mathrm{d_y}(\mathrm{c}(M,\varnothing;\mathrm{x})) = 0.$$

6.) Clear since $\mathrm{f}(M,\mathcal{E}(M);\mathrm{y}) \in \mathbb{Z}[\mathrm{y}]$. □

Together those identities yield the following important corollary, which is crucial for our algorithms.

Corollary 2.17. *Let M be a matroid of rank r on n points without loops and coloops. Then*

$$\mathrm{c}(M,\varnothing;\mathrm{x}) = \mathrm{cu}_{n,r}(\mathrm{x}) - \mathrm{d_x}\Big[\sum_X \mathrm{c}(M/X,\varnothing;\mathrm{x})\,\mathrm{f}(M|X,X;\mathrm{y})\Big] \text{ and}$$
$$\mathrm{f}(M,E;\mathrm{y}) = \mathrm{fu}_{n,r}(\mathrm{y}) - \mathrm{d_y}\Big[\sum_X \mathrm{c}(M/X,\varnothing;\mathrm{x})\,\mathrm{f}(M|X,X;\mathrm{y})\Big],$$

where X ranges over $\mathcal{Z}(M) - \{\varnothing, E\}$.

Proof. By applying 2.) of Lemma 2.16 to the formula for the rank generating polynomial from Theorem 2.5 we have

$$\mathrm{cu}_{n,r}(\mathrm{x}) = \mathrm{d_x}(\mathrm{S}(M;\mathrm{x},\mathrm{y})) = \mathrm{d_x}\Big[\sum_{X\in\mathcal{Z}(M)} \mathrm{c}(M/X,\varnothing;\mathrm{x})\,\mathrm{f}(M|X,X;\mathrm{y})\Big].$$

Solving this equation for $\mathrm{c}(M,\varnothing;\mathrm{x})$ by using the $\mathbb{Z}$-linearity of $\mathrm{d_x}$ and 4.)-6.) of Lemma 2.16 yields the first statement. The second one follows analogously. □

We are finally able to state the algorithms for the computation of cloud, flock and rank generating polynomials by the essential flat configuration:

`cloud`:

Input: An essential flat configuration $\mathcal{Z} = (L, n, r)$ of a Matroid M.

Output: $\mathrm{c}(M, \varnothing; \mathrm{x})$.

Algorithm:

1.) Calculate $\mathtt{S} := \sum_X \mathtt{cloud}([X, 1_L]_{\mathcal{Z}})\mathtt{flock}([0_L, X]_{\mathcal{Z}})$, where $X \in L - \{0_L, 1_L\}$.

2.) Return $\mathrm{cu}_{n(1_L), r(1_L)}(\mathrm{x}) - \mathrm{d}_{\mathrm{x}}(S)$.

`flock`:

Input: An essential flat configuration $\mathcal{Z} = (L, n, r)$ of a Matroid M.

Output: $\mathrm{f}(M, \mathcal{E}(M); \mathrm{y})$.

Algorithm:

1.) Calculate $\mathtt{S} := \sum_X \mathtt{cloud}([X, 1_L]_{\mathcal{Z}})\mathtt{flock}([0_L, X]_{\mathcal{Z}})$, where $X \in L - \{0_L, 1_L\}$.

2.) Return $\mathrm{fu}_{n(1_L), r(1_L)}(\mathrm{y}) - \mathrm{d}_{\mathrm{y}}(S)$.

and

`RankGeneratingPolynomial`:

Input: An essential flat configuration $\mathcal{Z} = (L, n, r)$ of a Matroid M.

Output: $\mathrm{S}(M; \mathrm{x}, \mathrm{y})$, the rank generating polynomial of M.

Algorithm:

Return $\sum_X \mathtt{cloud}([X, 1_L]_{\mathcal{Z}})\mathtt{flock}([0_L, X]_{\mathcal{Z}})$, where $X \in L$.

Since the height of the lattices of the configurations decrease in every recursion step of `cloud` and `flock`, the algorithms terminate and their correctness follows from Corollary 2.17 and Lemma 2.13.

2.4 The condensed essential flat configuration

2.4.1 The condensed essential flat configuration

Symmetries in the lattice of essential flats of a matroid can be used to dramatically shrink down the information necessary for the computation of the rank generating polynomial. Think of the Golay code matroid, which has about 35,000 essential flats grouping together to just 6 orbits under its automorphism group, the Mathieu group M_{24} (c.f. Example 2.4). Now in a condensed essential flat configuration we will just store the cardinalities and ranks of an element of each orbit and how often an element of one orbit appears as subset in the other orbits. For the Golay code matroid this information fits in two small lists for the cardinalities and ranks and one 6×6 matrix. But still the rank generating polynomial can be recovered.

First we want to generalize the notion of orbits.

Definition 2.18. Let M be a matroid. We call a partition P of the lattice of essential flats of M, $\mathcal{Z}(M)$, a **condensation** if for all $B, C \in P$

1. rank and cardinality are constant on B and
2. $|\{Y \in C \,|\, X \subseteq Y\}|$ is equal for all $X \in B$.

For a condensation P and $B, C \in P$ we set

1. $w_P(B,C) := |\{Y \in C \,|\, X \subseteq Y\}|$, $X \in B$, and
2. $B \leq_P C :\Leftrightarrow w(B,C) > 0$.

This is well-defined and P becomes a lattice w.r.t. $\leq_P$.

Example 2.7. *Let M be a matroid and $G \leq \mathrm{Aut}(M)$ be a subgroup of its automorphism group. Then the G-orbits of $\mathcal{Z}(M)$ are a condensation of $\mathcal{Z}(M)$.*

A condensation now yields a condensed essential flat configuration by forgetting its concrete realization as a partition of a set.

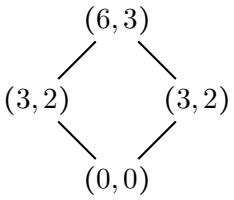
Definition 2.19. A **condensed** (essential flat) **configuration** $\mathcal{Z} = (L, n, r, w)$ is a lattice L together with

1. $n : L \to \mathbb{Z}_{\geq 0}$ monotonic, the **cardinality function**,
2. $r : L \to \mathbb{Z}_{\geq 0}$ monotonic, the **rank function** and
3. $w : L \times L \to \mathbb{Z}_{\geq 0}$, the **weight function**, with
   $0 < w(A,B)$ iff $A \leq_L B$, for all $A, B \in L$.

Let M be a matroid without loops and coloops. $\mathcal{Z} = (L, n, r, w)$ is a **condensed** (essential flat) **configuration** of M, if there is a condensation P of $\mathcal{Z}(M)$ with a bijection $\phi : P \to L$, s.t. for all $B, C \in P$

1. $|X| = n(\phi(B))$, $X \in B$,
2. $\mathrm{r}_M(X) = r(\phi(B))$, $X \in B$, and
3. $w_P(B,C) = w(\phi(B), \phi(C))$.

Example 2.8. *1.) Recall Example 2.5. Let M be a matroid with configuration*



and denote the two essential flats corresponding to $(3,2)$ *by* X_1 *and* X_2*. Then*

$$P = \{\{\varnothing\}, \{X_1, X_2\}, \{\mathcal{E}(M)\}\}$$

is a condensation of M*.* $(P, \leq_P)$ *has the Hasse diagram*

$$\begin{array}{c} \{\mathcal{E}(M)\} \\ | \\ \{X_1, X_2\} \\ | \\ \{\varnothing\} \end{array}$$

and w_P *is given by the matrix*

$$(w_P(B,C))_{B,C\in P} = \begin{array}{c} \\ \{\varnothing\} \\ \{X_1,X_2\} \\ \{\mathcal{E}(M)\} \end{array} \begin{array}{c} \begin{array}{ccc} \{\varnothing\} & \{X_1,X_2\} & \{\mathcal{E}(M)\} \end{array} \\ \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \end{array},$$

which can be thought of as a generalized adjacency matrix of P *w.r.t* $\leq_P$ *since replacing all non-zero entries with one yields the actual adjacency matrix.*
The corresponding condensed configuration now can be represented by $(|R_B|)_{B\in P} = (0,3,6)$*,* $(\mathrm{r}_M(R_B))_{B\in P} = (0,2,3)$ *and* $(w_P(B,C))_{B,C\in P}$*, where* $R_B \in B$ *are representatives.*

2.) Let M *be the* Golay *code matroid. In Example 2.4 we saw that* $\mathrm{Aut}(M) = M_{24}$ *acts transitively on the essential flats of* M *of given rank and has 6 orbits altogether. The condensed configuration* (L,n,r,w) *is given by*

$$(w(B,C))_{B,C\in L} = \begin{pmatrix} 1 & 759 & 35420 & 2576 & 759 & 1 \\ 0 & 1 & 140 & 0 & 30 & 1 \\ 0 & 0 & 1 & 0 & 3 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

$$(n(B))_{B\in L} = (0,8,12,12,16,24) \text{ and}$$
$$(r(B))_{B\in L} = (0,7,10,11,11,12).$$

2.4.2 From a condensed configuration to the rank generating polynomial

Now to the second main theorem:

Theorem 2.20. *A condensed essential flat configuration of a matroid determines its rank generating polynomial.*

We proceed similar to the prove for Theorem 2.14, namely by stating an algorithm which computes the rank generating polynomial using just a condensed configuration. Recall that the algorithms concerning configurations actually retrieve all cloud and flock polynomials of all intervals in the lattice of essential flats of the corresponding matroids. Contrary to configurations, this is not possible for condensed configurations, since generally a condensed configuration does not exactly know which intervals appear in the lattice of essential flats of the matroid. But we will be able to retrieve *average* cloud and flock polynomials. Using the condensed configuration corresponding to a condensation P of a matroid M we will for example be able to compute

$$\sum_{\substack{Y \in C \\ X \subseteq Y}} \mathrm{c}(M|Y/X, \varnothing; \mathrm{x})$$

for $B, C \in P$, $B \leq_P C$ and $X \in B$. These *average* cloud and flock polynomials then suffice to compute the rank generating polynomial.

Definition 2.21. Let M be a matroid and P a condensation of $\mathcal{Z}(M)$. For $B \leq_P C$ we recursively define

$$\begin{aligned} \underline{\mathrm{c}}(P, B, C; \mathrm{x}) &:= w_P(B, C)\, \mathrm{cu}_{n,r}(\mathrm{x}) - \mathrm{d}_{\mathrm{x}}(S(B, C)) \text{ and} \\ \underline{\mathrm{f}}(P, B, C; \mathrm{y}) &:= w_P(B, C)\, \mathrm{fu}_{n,r}(\mathrm{y}) - \mathrm{d}_{\mathrm{y}}(S(B, C)), \text{ for} \\ S(B, C) &:= \sum_D \underline{\mathrm{c}}(P, D, C; \mathrm{x})\, \underline{\mathrm{f}}(P, B, D; \mathrm{y}) \end{aligned}$$

where D ranges over $[B, C]_P - \{B, C\}$, $n := |Y| - |X|$ and $r := \mathrm{r}_M(Y) - \mathrm{r}_M(X)$, for $X \in B$ and $Y \in C$.

Lemma 2.22. *In the notation of Definition 2.21 we choose representatives $R_B \in B$ for all $B \in C$. Then for all $B, C \in P$ with $B \subseteq C$*

$$\begin{aligned} \underline{\mathrm{c}}(L, B, C; \mathrm{x}) &= \sum_{\substack{Y \in C \\ R_B \subseteq Y}} \mathrm{c}(M|Y, R_B; \mathrm{x}) \text{ and} \\ \underline{\mathrm{f}}(L, B, C; \mathrm{y}) &= \sum_{\substack{Y \in C \\ R_B \subseteq Y}} \mathrm{f}(M/R_B, Y - R_B; \mathrm{y}). \end{aligned}$$

Notice that this implies that the right hand sides are independent of the choice of $R_B \in B$.

Proof. We proof this by induction over the height of $[B,C]_P$. As per definition

$$\underline{\mathrm{c}}(P,B,C;\mathrm{x}) = w(B,C)\,\mathrm{cu}_{n,r}(\mathrm{x}) - \mathrm{d}_{\mathrm{x}}(S(B,C))$$

where

$$S(B,C) = \sum_D \underline{\mathrm{c}}(P,D,C;\mathrm{x})\,\underline{\mathrm{f}}(P,B,D;\mathrm{y})$$

and D ranges over $[B,C]_P - \{B,C\}$.
If $[B,C]_P = \{B,C\}$ then $S(B,C) = 0$ and $M|Y/X \cong \mathrm{U}_{r,n}$, for all $X \in B$ and $Y \in C$ with $X \subseteq Y$, and the claim follows.
Otherwise, since for all D, $[D,C]_P$ and $[B,D]_P$ have lower height than $[B,C]_P$, we can apply induction and get

$$\begin{aligned} S(B,C) &= \sum_D \sum_{\substack{Y\in C\\ R_D\subseteq C}} \mathrm{c}(M|Y,R_D;\mathrm{x}) \sum_{\substack{Z\in D\\ R_B\subseteq Z}} \mathrm{f}(M/R_B,Z-R_B;\mathrm{y}) \\ &= \sum_D \sum_{\substack{Z\in D\\ R_B\subseteq Z}} \big[\mathrm{f}(M/R_B,Z-R_B;\mathrm{y}) \sum_{\substack{Y\in C\\ R_D\subseteq C}} \mathrm{c}(M|Y,R_D;\mathrm{x})\big]. \end{aligned}$$

By induction the rightmost sum is independent of the choice of R_D, so

$$\begin{aligned} &= \sum_D \sum_{\substack{Z\in D\\ R_B\subseteq Z}} \big[\mathrm{f}(M/R_B,Z-R_B;\mathrm{y}) \sum_{\substack{Y\in C\\ Z\subseteq C}} \mathrm{c}(M|Y,Z;\mathrm{x})\big] \\ &= \sum_D \sum_{\substack{Z\in D\\ R_B\subseteq Z}} \sum_{\substack{Y\in C\\ Z\subseteq C}} \mathrm{c}(M|Y,Z;\mathrm{x})\ \mathrm{f}(M/R_B,Z-R_B;\mathrm{y}). \end{aligned}$$

The three sums range over $\{(Z,Y)|Z \in \mathcal{Z}(M), Y \in C \text{ with } R_B \subsetneq Z \subsetneq Y\}$ and can hence be rearranged to

$$= \sum_{\substack{Y\in C\\ R_B\subseteq Y}} \sum_Z \mathrm{c}(M|Y,Z;\mathrm{x})\,\mathrm{f}(M/R_B,Z-R_B;\mathrm{y}),$$

where $Z \in [R_B,Y]_{\mathcal{Z}(M)} - \{R_B,Y\}$. Applying this to $\underline{\mathrm{c}}(P,B,C;\mathrm{x})$ yields

$$\begin{aligned} \underline{\mathrm{c}}(P,B,C;\mathrm{x}) &= w(B,C)\,\mathrm{cu}_{n,r}(\mathrm{x}) - \mathrm{d}_{\mathrm{x}}\Big(\sum_{\substack{Y\in C\\ R_B\subseteq Y}} \sum_Z \mathrm{c}(M|Y,Z;\mathrm{x})\,\mathrm{f}(M/R_B,Z-R_B;\mathrm{y})\Big) \\ &= \sum_{\substack{Y\in C\\ R_B\subseteq Y}} \Big[\mathrm{cu}_{n,r}(\mathrm{x}) - \mathrm{d}_{\mathrm{x}}\Big(\sum_Z \mathrm{c}(M|Y,Z;\mathrm{x})\,\mathrm{f}(M/R_B,Z-R_B;\mathrm{y})\Big)\Big]. \end{aligned}$$

By Corollary 2.17 and the definition of n and r this is

$$= \sum_{\substack{Y \in C \\ R_B \subseteq Y}} \mathrm{c}(M|Y, R_B; \mathrm{x}).$$

The statement for the flock polynomial follows analogously. □

Corollary 2.23. *In the notation of Lemma 2.22*

$$\mathrm{S}(M; \mathrm{x}, \mathrm{y}) = \sum_{B \in P} \underline{\mathrm{c}}(P, B, 1_P; \mathrm{x})\, \underline{\mathrm{f}}(P, 0_P, B; \mathrm{y}),$$

where $1_P = \{\mathcal{E}(M)\}$ *and* $0_P = \{\varnothing\}$.

Proof. By Lemma 2.22

$$\begin{aligned}\sum_{B \in P} \underline{\mathrm{c}}(P, B, 1_P; \mathrm{x})\, \underline{\mathrm{f}}(P, 0_P, B; \mathrm{y}) &= \sum_{B \in P} \sum_{\substack{Y \in 1_P \\ R_B \subseteq Y}} \mathrm{c}(M|Y, R_B; \mathrm{x}) \sum_{\substack{X \in B \\ \varnothing \subseteq X}} \mathrm{f}(M, X; \mathrm{y}) \\ &= \sum_{B \in P} \sum_{X \in B} \sum_{\substack{Y \in 1_P \\ R_B \subseteq Y}} \mathrm{c}(M|Y, R_B; \mathrm{x})\ \mathrm{f}(M, X; \mathrm{y}).\end{aligned}$$

Using the independence of choice of $R_B \in B$

$$= \sum_{B \in P} \sum_{X \in B} \sum_{\substack{Y \in 1_P \\ X \subseteq Y}} \mathrm{c}(M|Y, X; \mathrm{x})\ \mathrm{f}(M, X; \mathrm{y}),$$

and since $1_P = \{\mathcal{E}(M)\}$ this yields

$$\begin{aligned}&= \sum_{B \in P} \sum_{X \in B} \mathrm{c}(M, X; \mathrm{x})\, \mathrm{f}(M, X; \mathrm{y}) \\ &= \mathrm{S}(M; \mathrm{x}, \mathrm{y}).\end{aligned}$$

□

The condensed configuration is constructed to contain all necessary information for the computation of $\underline{\mathrm{c}}(M, B, C; \mathrm{x})$ and $\underline{\mathrm{f}}(M, B, C; \mathrm{y})$. So we are finally able to state the algorithms.

`averageCloud`:

Input: A condensed configuration $\mathcal{Z} = (L, n, r, w)$ and $B, C \in L$ with $B \leq_L C$.

Output: If $\mathcal{Z}$ is the condensed configuration of a matroid M corresponding to a condensation P with bijection $\phi : P \to L$ then:

$$\underline{\mathrm{c}}(P, \phi^{-1}(B), \phi^{-1}(C); \mathrm{x})$$

Algorithm:

1.) Set $n \coloneqq n(C) - n(B)$, $r \coloneqq r(C) - r(B)$.

2.) Calculate $S \coloneqq \sum_D \texttt{averageCloud}(\mathcal{Z}, D, C)\texttt{averageFlock}(\mathcal{Z}, B, D)$,
where $D \in [B, C]_L - \{B, C\}$.

3.) Return $w(B, C)\,\mathrm{cu}_{n,r}(\mathrm{x}) - \mathrm{d}_{\mathrm{x}}(S)$.

averageFlock:

Input: A condensed configuration $\mathcal{Z} = (L, n, r, w)$ and $B, C \in L$ with $B \leq_L C$.

Output: If $\mathcal{Z}$ is the condensed configuration of a matroid M corresponding to a condensation P with bijection $\phi : P \to L$ then:

$$\underline{\mathrm{f}}(P, \phi^{-1}(B), \phi^{-1}(C); \mathrm{y})$$

Algorithm:

1.) Set $n \coloneqq n(C) - n(B)$, $r \coloneqq r(C) - r(B)$.

2.) Calculate $S \coloneqq \sum_D \texttt{averageCloud}(\mathcal{Z}, D, C)\texttt{averageFlock}(\mathcal{Z}, B, D)$,
where $D \in [B, C]_L - \{B, C\}$.

3.) Return $w(B, C)\,\mathrm{fu}_{n,r}(\mathrm{y}) - \mathrm{d}_{\mathrm{y}}(S)$.

RankGeneratingPolynomial:

Input: A condensed configuration $\mathcal{Z} = (L, n, r, w)$ of a Matroid M.

Output: $\mathrm{S}(M; \mathrm{x}, \mathrm{y})$, the rank generating polynomial of M.

Algorithm:

Return $\sum_X \texttt{averageCloud}([X, 1_L]_{\mathcal{Z}})\texttt{averageFlock}([0_L, X]_{\mathcal{Z}})$, where $X \in L$.

The correctness of the algorithms follows from Lemma 2.22 and Corollary 2.23.

Chapter 3

Examples and Implementations

3.1 Perfect matroid designs

A matroid is a **perfect matroid design** (PMD) if all flats of a given rank i have the same cardinality k_i. In [6] it was shown that the rank generating polynomial of a perfect matroid design only depends on those k_i. In this section we will see how to recover the condensed essential flat configuration of a perfect matroid design from the k_i as well. Since the rank generating polynomial only depends on the condensed configuration, this yields an alternative proof.

Definition 3.1 (Perfect matroid design)**.** A matroid M of rank r is a **perfect matroid design** if the cardinality of all flats of rank i is k_i for $i = 0, \dots, r$ and suitable $k_i \in \mathbb{Z}_{\geq 0}$. We then describe M as a $\mathrm{PMD}(k_0, \dots, k_r)$.

Remark 3.2. In a $\mathrm{PMD}(k_0, k_1, \dots, k_r)$, k_0 is the number of loops and k_1 the size of the parallel classes. By deleting the loops and identifying elements in parallel classes we obtain a $\mathrm{PMD}(0, 1, \dots, (k_r - k_0)/k_1)$. So usually we assume $k_0 = 0$ and $k_1 = 1$.

Example 3.1. *(cf. [2] for a comprehensive overview)*
1.) The vector matroid consisting of all elements in $\mathbb{F}_q^n$ is a

$$\mathrm{PMD}(1, q, q^2, \dots, q^n).$$

By passing to the projective space $\mathbb{P}(\mathbb{F}_q^n)$ we obtain a

$$\mathrm{PMD}(0, 1, (q^2+1)/(q-1), \dots, (q^n-1)/(q-1)).$$

2.) From a condensed configuration of a matroid M one can decide whether M is a

perfect matroid design, since the cardinality and rank of all flats in M can be determined by the cloud polynomials of its essentials flats.

We will now construct a condensed configuration for a perfect matroid design. We note that

Theorem 3.3. *Let M be a $\mathrm{PMD}(k_0, \ldots, k_r)$ and B_i the set of all flats of rank i. Then for all R in B_i*

$$|\{X \in B_j \,|\, R \subseteq X\}| = \prod_{h=i}^{j-1} \frac{k_r - k_h}{k_j - k_h}.$$

Proof. C.f. [6]. □

So after removing all flats which are not essential we can construct a condensed configuration.

Remark 3.4. Let M be a $\mathrm{PMD}(k_0, \ldots, k_r)$, $k_0 = 0$, $k_1 = 1$ and B_i the set of all flats of rank i. Then B_i consists of essential flats iff $k_i > k_{i-1}+1$. So let $I := \{i \in \{0, \ldots, r\} \,|\, k_i > k_{i-1}+1\}$. Then $P := \{B_i | i \in I\}$ is a condensation of $\mathcal{Z}(M)$, the set of essential flats in M, and a condensed configuration (I, n, r, w) of M is given by

$$\begin{aligned} n(i) &:= k_i, \\ r(i) &:= i \text{ and} \\ w(i,j) &:= \prod_{h=i}^{j-1} \frac{k_r - k_h}{k_j - k_h}. \end{aligned}$$

This yields another proof for the theorem in [6].

Corollary 3.5. *The rank generating* (Tutte) *polynomial of a $\mathrm{PMD}(k_0, \ldots, k_r)$ is already determined by the k_i.*

Since we can actually compute average cloud polynomials, we know the cardinality and rank of all flats which have to appear. This yields a new way of excluding the existence of certain perfect matroid designs.

3.2 Matroids induced by root systems

In this section we study matroids induced by root system with respect to their essential flats and rank generating polynomials.

Definition 3.6 (Root system)**.** A **root system** Φ is a a finite configuration of vectors, called **roots**, in an Euclidian space $(V, (\ ,\ ))$ fulfilling

1. $\langle\Phi\rangle_{\mathbb{R}} = V$,
2. for all $\alpha \in \Phi$, Φ is invariant under σ_α, the reflection through the hyperplane orthogonal to α,
3. for all $\alpha \in \Phi$, $\langle\alpha\rangle_{\mathbb{R}} \cap \Phi = \{\alpha, -\alpha\}$ and
4. $\langle\alpha, \beta\rangle := 2\frac{(\alpha,\beta)}{(\beta,\beta)} \in \mathbb{Z}$ for all $\alpha, \beta \in \Phi$.

The group $W \leq \mathrm{O}(V)$ generated by the reflections σ_α, $\alpha \in \Phi$, is called the Weyl group of Φ.

Root systems are classified by their Dynkin diagrams, i.e. a graph encoding $\langle\alpha, \beta\rangle$ and length information for a all α, β in a basis of the root system. For precise definitions and the classifaction c.f. [11]. Like every finite configuration of vectors, a root systems Φ can be regarded as a matroid, which is highly symmetrical since the Weyl group of Φ embeds in its automorphism group. Furthermore the essential flats of the matroid correspond to the root systems contained in Φ which have no direct summand isomorphic to A_1, the trivial root system $\{\alpha, -\alpha\}$.

3.2.1 The root system A_l

Let $l > 2$. We want to compute the rank generating polynomial of the root system

$$A_{l-1} = \{e_{i,j} \in V \mid i \neq j\} \subseteq V := \mathbb{R}^l,$$

where $e_{i,j} := e_i - e_j$ and $\{e_i\}$ is an orthonormal basis of V. To avoid parallel classes we only consider the set of positive roots w.r.t. to the basis $\{e_{i,i+1}\}$ namely

$$A^+_{l-1} = \{e_{i,j} \in V | i < j\}.$$

Let $M := M[A^+_{l-1}]$. Then $\mathrm{Aut}(M) = S_l$, where $\sigma.e_{i,j} := \pm e_{\sigma(i),\sigma(j)}$ for $\sigma \in S_l$. Our goal is to compute all S_l-orbits of essential flats of M and their cloud and flock polynomials. The orbits of essential flats can be parameterized by

$$P := \{\lambda = (\lambda_1, \ldots, \lambda_s) \in \mathbb{N}^s \mid \lambda_1 \geq \cdots \geq \lambda_s > 2 \text{ and } \sum_i \lambda_i \leq l\}.$$

For $\lambda = (\lambda_1, \dots, \lambda_s) \in P$ let

$$R_\lambda := \biguplus_{k=1}^{s} \{e_{i,j} \mid i < j, i, j \in \{\lambda_1 + \cdots + \lambda_{k-1} + 1, \dots, \lambda_1 + \cdots + \lambda_k\}\},$$

where the empty list $() \in P$ and $R_() = \varnothing$. Then

$$\mathcal{Z}(M) = \biguplus_{\lambda \in P} S_l.R_\lambda$$

Let $\lambda = (\lambda_1, \dots, \lambda_s) \in P$, $\bar{\lambda} := \sum_i \lambda_i$, $\{\lambda_1, \dots, \lambda_s\} = \{\lambda_{i_1}, \dots, \lambda_{i_r}\}$ for λ_{i_j} pw. distinct and μ_{i_j} the multiplicity of λ_{i_j} in λ. Then

$$\begin{aligned}
M|R_\lambda &\cong \bigoplus_i M[A^+_{\lambda_i - 1}], \\
|R_\lambda| &= \sum_i \binom{\lambda_i}{2}, \\
\mathrm{r}_M(R_\lambda) &= \sum_i (\lambda_i - 1), \\
\mathrm{Stab}_{S_l}(R_\lambda) &\cong S_{l-\bar{\lambda}} \times \bigtimes_j S_{\lambda_{i_j}} \wr S_{\mu_{i_j}} \text{ and} \\
|S_l.R_\lambda| &= \frac{n!}{(l-\bar{\lambda})! \prod_j (\lambda_{i_j}!)^{\mu_{i_j}} \mu_{i_j}!}.
\end{aligned}$$

Now the flock polynomial of a direct sum is the product of the flock polynomials of the summands and hence

$$\mathrm{f}(M, R_\lambda; \mathrm{y}) = \prod_i \mathrm{f}(M[A^+_{\lambda_i - 1}], \mathcal{E}(M[A^+_{\lambda_i - 1}]); \mathrm{y}),$$

which can be computed recursively for all $\lambda \neq (l)$. The cloud of R_λ is

$$\mathrm{e}_M^{-1}(\{R_\lambda\}) = \{R_\lambda \cup \{e_{i_1,j_1}, \dots e_{i_m,j_m}\} \mid \bar{\lambda} < i_k < j_k \leq l, \text{and the } \{i_k, j_k\} \text{ pw. disjoint}\}.$$

Hence the cloud polynomial of R_λ in M is

$$\mathrm{c}(M, R_\lambda; \mathrm{x}) = \sum_k \binom{l-\bar{\lambda}}{2k} \frac{(2k)!}{2^k k!} x^{\mathrm{r}_M(M) - (\mathrm{r}_M(R_\lambda) + k)}.$$

We can now compute the flock polynomial of $\mathcal{E}(M) = R_{(l)}$, the ground set of M, according to Lemma 2.16:

$$\mathrm{f}(M, \mathcal{E}(M); \mathrm{y}) = \mathrm{fu}_{\binom{l}{2}, l-1}(\mathrm{y}) - \mathrm{d}_\mathrm{y}\Big[\sum_{\substack{\lambda \in P \\ \lambda \neq (), (l)}} |S_l.R_\lambda| \, \mathrm{c}(M, R_\lambda; \mathrm{x}) \, \mathrm{f}(M, R_\lambda; \mathrm{y})\Big].$$

The rank generating polynomial of M is

$$\mathrm{S}(M;\mathrm{x},\mathrm{y}) = \sum_{\lambda\epsilon P} |S_l.R_\lambda|\,\mathrm{c}(M,R_\lambda;\mathrm{x})\,\mathrm{f}(M,R_\lambda;\mathrm{y}).$$

As an example we compute the rank generating polynomials for some l.
Let $l = 3$. Then $P = \{(),(3)\}$ and $M[A_2^+] \cong \mathrm{U}_{2,3}$ and for the rank generating polynomial cf. Example 2.2.
Let $l = 4$. Then $P = \{(),(3),(4)\}$ and

$$\begin{aligned}
\mathrm{c}(M[A_3^+],R_{()};\mathrm{x}) &= \mathrm{x}^3+6\,\mathrm{x}^2+3\,\mathrm{x}^3\\
\mathrm{f}(M[A_3^+],R_{()};\mathrm{y}) &= 1\\
\mathrm{c}(M[A_3^+],R_{(3)};\mathrm{x}) &= \mathrm{x}\\
\mathrm{f}(M[A_3^+],R_{(3)};\mathrm{y}) &= 3+\mathrm{y}\\
\mathrm{c}(M[A_3^+],R_{(4)};\mathrm{x}) &= 1
\end{aligned}$$

and via Lemma 2.16

$$\begin{aligned}
\mathrm{f}(M[A_3^+],R_{(4)};\mathrm{y}) &= \mathrm{fu}_{3,6}(\mathrm{y}) - \mathrm{d}_\mathrm{y}\left[\mathrm{x}^3+3\,\mathrm{x}^2+4\,\mathrm{x}(3+\mathrm{y})\right]\\
&= 16+15\,\mathrm{y}+6\,\mathrm{y}^2+\mathrm{y}^3\,.
\end{aligned}$$

Hence the coefficient matrix of $\mathrm{S}(M[A_3^+];\mathrm{x},\mathrm{y})$ is

16	15	6	**1**
15	**4**		
6			
1			

Let $l = 5$. Then $P = \{(),(3),(4),(5)\}$ and

$$\begin{aligned}
\mathrm{c}(M[A_4^+],R_{()};\mathrm{x}) &= \mathrm{x}^4+30\,\mathrm{x}^2+15\,\mathrm{x}^3\\
\mathrm{c}(M[A_4^+],R_{(3)};\mathrm{x}) &= \mathrm{x}^2+\mathrm{x}\\
\mathrm{f}(M[A_4^+],R_{(3)};\mathrm{y}) &= 3+\mathrm{y}\\
\mathrm{c}(M[A_4^+],R_{(4)};\mathrm{x}) &= \mathrm{x}\\
\mathrm{f}(M[A_4^+],R_{(4)};\mathrm{y}) &= 16+15\,\mathrm{y}+6\,\mathrm{y}^2+\mathrm{y}^3\\
\mathrm{c}(M[A_3^+],R_{(5)};\mathrm{x}) &= 1
\end{aligned}$$

and again via Lemma 2.16

$$\mathrm{f}(M[A_3^+],R_{(5)};\mathrm{y}) = 125+222\,\mathrm{y}+210\,\mathrm{y}^2+120\,\mathrm{y}^3+10\,\mathrm{y}^4+\mathrm{y}^5\,.$$

Hence the coefficient matrix of $\mathrm{S}(M[A_4^+];\mathrm{x},\mathrm{y})$ is

125	222	210	120	10	**1**
110	85	30	**5**		
45	**10**				
10					
1					

3.2.2 The root system E_6

To construct another highly symmetrical matroid we start with the root system $E_6 \subseteq \mathbb{R}^6$. Again to avoid parallel classes we take representatives for $\{\beta, -\beta\} \subseteq E_6$ and consider the matroid $M := M[A]$, where $A \in \mathbb{R}^{6\times 36}$ is

$$A := \begin{pmatrix}
1&1&1&1&0&1&1&0&1&0&0&1&0&0&0&0&1&1&0&1&0&0&1&0&0&0&1&0&0&0&1&0&1&0&0&1\\
1&2&1&1&1&1&1&1&0&0&0&1&1&1&0&0&1&1&1&0&0&0&1&1&1&0&0&0&0&1&1&1&0&0&1&0\\
2&2&2&1&1&2&1&1&1&1&0&1&1&0&0&0&2&1&1&1&1&0&1&1&0&0&1&1&0&0&1&1&1&1&0&0\\
2&3&3&2&2&2&1&1&1&1&0&2&2&1&1&0&2&1&1&1&1&0&2&2&1&1&0&0&1&1&1&1&1&1&0&0\\
2&2&2&2&2&1&1&1&1&1&1&1&1&1&1&0&1&1&1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0
\end{pmatrix} \in \mathbb{R}^{6\times 36}$$

The automorphism group is given by the reflections through the hyperplanes orthogonal to the roots w.r.t. to the Gram matrix

$$\begin{pmatrix}
2&0&-1&0&0&0\\
0&2&0&-1&0&0\\
-1&0&2&-1&0&0\\
0&-1&-1&2&-1&0\\
0&0&0&-1&2&-1\\
0&0&0&0&-1&2
\end{pmatrix}$$

The coefficient matrix of the rank generating polynomial is

846720	6102000	26665560	89442580	⋯						⋯	**1**
285120	1012122	2183580	3562785	⋯					⋯	**27**	
54135	90252	88680	62100	31995	12060	3186	540	**45**			
7020	4770	1620	**270**								
630	**120**										
36											
1											

The extreme exponents are $(0,6)$, $(1,4)$, $(3,3)$, $(2,8)$, $(1,15)$ and $(0,30)$. The essential flats corresponding to the extreme exponents are in one G-orbit each and representatives

are given by

$$
\begin{aligned}
R_1 &:= \varnothing,\\
A_2 \equiv R_2 &:= \{2,7,24\},\\
A_3 \equiv R_3 &:= \{7,14,16,18,25,27\},\\
D_4 \equiv R_4 &:= \{2,7,8,12,13,16,18,19,23,24,29,36\},\\
D_5 \equiv R_5 &:= \{1,2,4,5,7,8,11,14,17,20,21,23,24,26,27,28,30,31,32,36\} \text{ and}\\
E_6 \equiv R_6 &:= \underline{36}.
\end{aligned}
$$

We subtract the share of $R_2, \ldots, R_5$ from the rank generating polynomial of M. Then the coefficient matrix of $\mathrm{S}(M;\mathrm{x},\mathrm{y}) - \sum_{i=2}^{5} |G.R_i|\,\mathrm{c}(M,R_i;\mathrm{x})\,\mathrm{f}(M,R_i;\mathrm{y})$ is

846720	⋯						⋯	**1**
76896	⋯					⋯	**36**	
28080	48672	44400	25920	9720	2160	**216**		
540								
270								
36								
1								

Representatives for the orbits of the essential flats corresponding to the new extreme exponents $(2,6)$ and $(1,10)$ are

$$
\begin{aligned}
A_4 \equiv R_4^a &:= \{1,3,4,9,19,24,25,28,29,34\} \text{ and}\\
A_5 \equiv R_5^a &:= \{2,5,8,13,14,17,18,21,22,23,26,28,29,31,34\}.
\end{aligned}
$$

Proceeding this way we find one more orbit of 120 essential flats of rank 4

$$A_2 \perp A_2 \equiv R_4^b := \{1,3,4,9,19,24,25,28,29,34\}.$$

Now let $P := \{R_1, R_2, R_3, R_4, R_4^a, R_4^b, R_5, R_5^a, R_6\}$, then

$$\mathcal{Z}(M) = \biguplus_{R \in P} G.R$$

and we found all essential flats in M. We define $w(R,S) \coloneqq |\{X \in G.S \,|\, R \in X\}|$ for $R, S \in P$ and obtain a condensed configuration

$$(R)_{R\in P} \equiv (\varnothing, A_2, A_3, D_4, A_4, A_2 \perp A_2, D_5, A_5, E_6),$$

$$(w(R,S))_{R,S\in P} = \begin{pmatrix} 1 & 120 & 270 & 45 & 216 & 120 & 27 & 36 & 1 \\ 0 & 1 & 9 & 6 & 18 & 2 & 9 & 6 & 1 \\ 0 & 0 & 1 & 2 & 4 & 0 & 5 & 2 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 3 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 2 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 3 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

$$(|R|)_{R\in P} = (0, 3, 6, 12, 10, 6, 20, 15, 36) \text{ and}$$

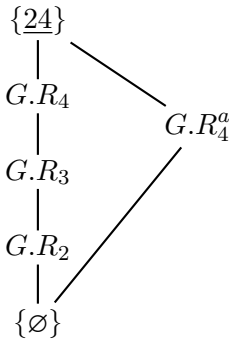
$$(\mathrm{r}_M(R))_{R\in P} = (0, 2, 3, 4, 4, 4, 5, 5, 6).$$

3.3 Another matroid for the Mathieu group M_{24}

Let G be the Mathieu group M_{24}. The Golay code matroid M discussed in Example 2.4 and 2.8 appears naturally in the representation theory of G. Over $\mathbb{F}_2$ the 24-dimensional permutation module of G has a unique 12-dimensional submodule, which yields M as a vector matroid. In this section we transform M into another G-transitive matroid $\tilde{M}$ which cannot be found in the representation theory of G. Recall that there are 6 orbits of essential flats in M represented by

$$\begin{aligned} R_1 &\coloneqq \varnothing, \\ R_2 &\coloneqq \{1,2,3,5,6,10,19,20\}, \\ R_3 &\coloneqq \{1,2,3,4,5,6,7,8,9,10,19,20\}, \\ R_4 &\coloneqq \{1,2,3,4,5,6,7,8,9,10,11,13,15,19,20,21\}, \\ R_4^a &\coloneqq \{1,3,4,5,6,7,8,12,13,14,17,23\} \text{ and} \\ R_5 &\coloneqq \underline{24}. \end{aligned}$$

The orbits afford a condensation P of $\mathcal{Z}(M)$ (c.f. Example 2.7). The condensation P is a lattice w.r.t. $\leq_P$ (c.f. Definition 2.21) with Hasse diagram



So the essential flats in $G.R_4^a$ interact trivially with the others. We can hence remove $G.R_4^a$ from $\mathcal{Z}(M)$ and still obtain a matroid. Let

$$\mathcal{Z} := \mathcal{Z}(M) - G.R_4^a \text{ and}$$
$$r := r_M|_{\mathcal{Z}}.$$

Then $\mathcal{Z}$ and r fulfill the axioms (Z1)-(Z4) from Theorem 1.32 and define a matroid $\tilde{M}$ with ground set $\underline{24}$. The matroid $\tilde{M}$ is still self-dual with $\mathrm{Aut}(\tilde{M}) = \mathrm{Aut}(M) = G$. The elements of $G.R_4^a$ are now bases in $\tilde{M}$ and $\mathcal{I}(\tilde{M}) = \mathcal{I}(M) \cup G.R_4^a$. Since trivially $\tilde{P} := P - G.R_4^a$ is a condensation of $\tilde{M}$, a condensed essential flat configuration (L, n, r, w) of $\tilde{M}$ is given by

$$(w(B,C))_{B,C\in L} = \begin{pmatrix} 1 & 759 & 35420 & 759 & 1 \\ 0 & 1 & 140 & 30 & 1 \\ 0 & 0 & 1 & 3 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$
$$(n(B))_{B\in L} = (0, 8, 12, 16, 24) \text{ and}$$
$$(r(B))_{B\in L} = (0, 7, 10, 11, 12).$$

And using the algorithms introduced in Chapter II we obtain the rank generating polynomial of $\tilde{M}$ given by its coefficient matrix

1393616	2071104	1870176	1295360	734712	346104	$\binom{24}{6}$	$\cdots$	**1**
2071104	*1275120*	425040	91080	12144	**759**			
1870176	425040	**35420**						
1295360	91080							
734712	12144							
346104	**759**							
$\binom{24}{6}$								
$\vdots$								
1								

The coefficients that differ from the rank generating polynomial of M are printed in italics.

Since the the essential flats in $G.R_2$ - which by the way are the blocks of the Steiner system $S(5,8,24)$- already determine the matrix representation of M over $\mathbb{F}_2$, $\tilde{M}$ is not $\mathbb{F}_2$-representable anymore.

Another possibility is to remove the orbits of R_2, R_3 and R_4 from the set of essential flats of the GOLAY code matroid. We denote the afforded matroid by $\hat{M}$. Again $\hat{M}$ is self-dual with automorphism group is M_{24}. The bases of $\hat{M}$ are all 12-element subsets except for the orbit of R_4^a. A condensed configuration (L,n,r,w) of $\hat{M}$ is given by

$$(w(B,C))_{B,C\in L} = \begin{pmatrix} 1 & 2576 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix},$$
$$(n(B))_{B\in L} = (0,12,24) \text{ and}$$
$$(r(B))_{B\in L} = (0,11,12).$$

The coefficient matrix of its rank generating polynomial is

2701580	2465232	$\binom{24}{14}$	$\cdots$	1
2465232	**2576**			
$\binom{24}{10}$				
$\vdots$				
1				

3.4 Implementations

In this section we will discuss the GAP[8] package ghost, an implementation of the algorithms introduced in Chapter 2 Section 4 for the computation of the rank generating polynomial from a condensed essential flat configuration.

3.4.1 The GAP package ghost

In the GAP package ghost we implemented a data structure and the most important operations for lattices. So one can define a lattice by the adjacency matrix of its order and ask for the top (one) and bottom (zero) of a lattice or construct an interval.

```
gap> L := Lattice( [[1, 1, 1, 1],
                    [0, 1, 0, 1],
                    [0, 0 ,1, 1],
                    [0, 0, 0, 1]] );;
gap> One( L );
4
gap> Zero( L ):
1
gap> LInterval := Lattice( L, 2, 4 );
gap> Display( AdjacencyMatrix( LInterval ) );
[[1, 1],
 [0, 1]]
```

We realized condensed essential flat configurations as lattices with additional cardinality, rank and weight functions. One can input a condensed essential flat configuration $\mathcal{Z} = (L, n, r, w)$ by a matrix $(w(R,S))_{R,S\in L}$ and two lists $(n(R))_{R\in L}$ and $(r(R))_{R\in L}$. We input the condensed essential flat configuration from Example 2.5:

```
gap> w := [[1, 2, 1],
           [0, 1, 1],
           [0, 0, 1]];;
gap> n := [0, 3, 6];;
gap> r := [0, 2, 3];;
gap> Z1 := CondensedConfiguration( w, n, r );;
```

We exemplary show the implementation of the algorithm for the flock polynomial:

```
AverageFlock := function( conf, lower, this )
  local sum, ret, i, rank, cardinality, weight;

  weight := WeightFunction( conf );
  rank := RankFunction( conf );
  card := CardinalityFunction( conf );

  # Check whether this average cloud polynomial has already been computed
  if IsBound( conf!.flocks[lower][this] ) then
    return conf!.flocks[lower][this];
  fi;

  #Calculate the sum of the intermediate cloud and flock polynomials
  sum := 0;
  for i in GroundSet( Lattice( conf, lower, this ) ) do
    if not( i = lower or i=this ) then
      sum := sum + AverageFlock( lower, i ) * AverageCloud( i, this );
    fi;
  od;

  #Calculate the average flock polynomial
  ret := weight( lower, this ) * FU( card( this ) - card( lower ),
                                     rank( this ) - rank( lower ) )
         - DeltaY( sum );

  #Save it
  conf!.flocks[lower][this]:=ret;

  #Return it
  return ret;
end;
```

Here the functions `DeltaX` and `DeltaY` are the polynomial operators d_x and d_y and `FU( n, r )` is $fu_{n,r}(y)$. Note that already computed average cloud and flock polynomials will be saved. This dramatically increases the speed of the algorithms since the average cloud and flock polynomials of the same intervals will be invoked multiple times during one calculation. The algorithm for the rank generating polynomial is now implemented easily:

```
RankGeneratingPolynomial := function( conf )
 return Sum( List( GroundSet( conf ),
```

```
                  r ->  AverageFlock( Zero( conf ), r ) *
                        AverageCloud( r, One( conf ) ) ) );
end;
```

We return to Example 2.5:

```
gap> S := RankGeneratingPolynomial( Z1 );;
gap> DisplayBivariatePolynomial( S );
[ [  18,  15,   6,   1 ],
  [  15,   2 ],
  [   6 ],
  [   1 ] ]
```

and once more consider the Golay code matroid:

```
gap> w := [ [      1,    759,  35420,   2576,    759,      1 ],
            [      0,      1,    140,      0,     30,      1 ],
            [      0,      0,      1,      0,      3,      1 ],
            [      0,      0,      0,      1,      0,      1 ],
            [      0,      0,      0,      0,      1,      1 ],
            [      0,      0,      0,      0,      0,      1 ] ];;
gap> n := [ 0, 8, 12, 12, 16, 24 ];;
gap> r := [ 0, 7, 10, 11, 11, 12 ];;
gap> ZGolay := CondensedConfiguration( w, n, r );;
gap> S := RankGeneratingPolynomial( ZGolay );;
gap> DisplayBivariatePolynomial( S );
[ [  1391040,  2071104,  1870176,  1295360,   734712,   346104,   134596,
     42504,    10626,     2024,      276,       24,        1 ],
  [  2071104,  1277696,   425040,    91080,    12144,      759 ],
  [  1870176,   425040,    35420 ],
  [  1295360,    91080 ],
  [   734712,    12144 ],
  [   346104,      759 ],
  [   134596 ],
  [    42504 ],
  [    10626 ],
  [     2024 ],
  [      276 ],
  [       24 ],
  [        1 ] ]
```

One can also convert a perfect matroid design into a condensed essential flat configuration. So for instance the rank generating polynomial of the matroid $\mathbb{P}(\mathbb{F}_2^4)$, which is a $\mathrm{PMD}(0,1,3,7,15)$, can be computed by:

```
gap> ZP24 := CondensedConfigurationByPMD( [ 0, 1, 3, 7, 15] );
gap> S := RankGeneratingPolynomial( ZP24 );;
gap> DisplayBivariatePolynomial( S );
[ [ 840, 2688, 4900, 6420, 6435, 5005, 3003, 1365,  455,  105,  15,    1 ],
  [ 420,  525,  315,  105,   15 ],
  [ 105,   35 ],
  [  15 ],
  [   1 ] ]
```

3.4.2 Runtime analysis

The actual runtime of the algorithm for the computation of the rank generating polynomial from a condensed essential flat configuration $\mathcal{Z} = (L, n, r, w)$ depends not only on the lattice L but also significantly on n, r and w, since they determine how large the polynomials in the computation in terms of their degree and coefficients will get. But if we consider polynomial operations in $O(1)$ and disregard the lookups for already computed flock and cloud polynomials, the algorithm is linear in the number of intervals in the lattice L and hence quadratic in its cardinality.
First we will revisit some examples and list the runtimes for the given matroids M with condensed essential flat configurations $\mathcal{Z} = (L, n, r, w)$.

M	$\lvert M\rvert$	rank M	$\lvert L\rvert$	runtime
Golay	24	12	6	10ms
E_6	36	6	9	36ms
M_{S_4}	36	14	506	3min

Here the M_{S_4} matroid is a highly symmetrical matroid which consist of certain elements in $\mathbb{Q}[S_4]$. To see the impact of the rank and cardinality of the matroid on the runtime we study the matroids $\mathbb{P}(\mathbb{F}_q^n)$ from Example 3.1 which are

$$\mathrm{PMD}(0, 1, (q^2-1)/(q-1) \ldots, (q^n-1)/(q-1)).$$

At first we consider a series of matroids $\mathbb{P}(\mathbb{F}_q^4)$, where q is a power of a prime:

q	$\lvert\mathbb{P}(\mathbb{F}_q^4)\rvert$	runtime
$q = 2$	15	4ms
$q = 4$	85	13ms
$q = 7$	400	76ms
$q = 9$	820	243ms
$q = 11$	1464	820ms
$q = 13$	2380	1807ms
$q = 16$	4369	10020ms

Note that the lattices of their condensed essential flat configurations are pairwise isomorphic but still the runtime drastically increases for larger q due to the larger coefficients in the polynomials occurring in the computation; the sum of all coefficient in the rank generating polynomial is $2^{\lvert\mathbb{P}(\mathbb{F}_q^4)\rvert}$. At last we consider the series $\mathbb{P}(\mathbb{F}_2^n)$, where the lattice and the coefficients are both getting larger.

n	$\lvert\mathbb{P}(\mathbb{F}_2^n)\rvert$	runtime
$n = 4$	15	10ms
$n = 6$	63	36ms
$n = 8$	255	273ms
$n = 10$	1023	2434ms
$n = 12$	4047	38780ms

Index

Symbols

Let M be a matroid and L be a lattice.

Symbol	Description	Page
0_L	bottom or zero of L	5
1_L	top or one of L	5
$[x, y]_L$	interval between $x \leq_L y$	6
$M\|X$	restriction of M by a set X in M	3
M/X	contraction of M by a set X in M	3
M^*	dual matroid of M	4
$\mathcal{C}(M)$	family of circuits of M	1
$\mathrm{c}(M, X; \mathrm{x})$	cloud polynomial of an essential flat X in M	12
$\mathrm{cu}_{n,r}(\mathrm{x})$	cloud polynomial of the empty set in $\mathrm{U}_{r,n}$ (for $r < n$)	22
cl_M	closure operator of M	2
$\mathrm{d}_\mathrm{x}, \mathrm{d}_\mathrm{y}$	polynomial operators	22
$\mathcal{E}(M)$	ground set of M	1
e_M	essentiality operator of M	7
$\mathrm{f}(M, X; \mathrm{y})$	flock polynomial of a flat X in M	12
$\mathrm{fu}_{n,r}(\mathrm{y})$	flock polynomial of the ground set in $\mathrm{U}_{r,n}$ (for $r < n$)	22
$\mathcal{I}(M)$	independent sets of M	3
r_M	rank function of M	2
$\mathrm{S}(M; \mathrm{x}, \mathrm{y})$	rank generating polynomial of M	11
$\mathrm{T}(M; \mathrm{x}, \mathrm{y})$	TUTTE polynomial of M	11
$\mathrm{U}_{r,n}$	uniform matroid of rank r on n points	1
$\mathcal{Z}(M)$	lattice of essential flats of M	6

Bibliography

[1] Joseph E. Bonin and Anna de Mier. The lattice of cyclic flats of a matroid. *Ann. Comb.*, 12(2):155–170, 2008. ISSN 0218-0006. doi: 10.1007/s00026-008-0344-3. URL http://dx.doi.org/10.1007/s00026-008-0344-3.

[2] Peter J. Cameron. Polynomial aspects of codes, matroids and permutation groups, 2002.

[3] Wilhelm Plesken and Thomas Bächler. Counting polynomials for linear codes, hyperplane arrangements, and matroids. *Documenta Mathematica*, 19:285–312, 2014.

[4] W. Kook, V. Reiner, and D. Stanton. A convolution formula for the Tutte polynomial. *J. Combin. Theory Ser. B*, 76(2):297–300, 1999. ISSN 0095-8956. doi: 10.1006/jctb.1998.1888. URL http://dx.doi.org/10.1006/jctb.1998.1888.

[5] Wilhelm Plesken. Counting with groups and rings. *J. Reine Angew. Math.*, 334: 40–68, 1982. ISSN 0075-4102. doi: 10.1515/crll.1982.334.40. URL http://dx.doi.org/10.1515/crll.1982.334.40.

[6] Eunice Gogo Mphako. Tutte polynomials of perfect matroid designs. *Combin. Probab. Comput.*, 9(4):363–367, 2000. ISSN 0963-5483. doi: 10.1017/S0963548300004338. URL http://dx.doi.org/10.1017/S0963548300004338.

[7] Ken Shoda. *Large Families of Matroids with the Same Tutte Polynomial*. PhD thesis, The George Washington University, August 2012.

[8] GAP. *GAP – Groups, Algorithms, and Programming, Version 4.7.4*. The GAP Group, 2014. URL http://www.gap-system.org.

[9] James Oxley. *Matroid theory*, volume 21 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, second edition, 2011. ISBN 978-0-19-960339-8.

[10] Wilhelm Plesken. *Computeralgebra*. Skript zur Vorlesung Computeralgebra, Sommersemester 2009.

[11] Nicolas Bourbaki. *Lie groups and Lie algebras. Chapters 4–6*. Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 2002. ISBN 3-540-42650-7. Translated from the 1968 French original by Andrew Pressley.

Acknowledgments

I would like to express my deep gratitude to Prof. Dr. Wilhelm Plesken for having an open door for me at any time and for providing me with an interesting and fruitful subject. I would also like to thank all the people at Lehrstuhl B for their willingness to answer any of my questions. Finally, I wish to thank my family for all their support and encouragement throughout my study.

Erklärung

Hiermit versichere ich, dass ich diese Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.

Aachen, den 26. März 2014 Jens Niklas Eberhardt