Computing the Tutte Polynomial of a Matroid from its Lattice of Cyclic Flats

Jens Niklas Eberhardt

Lehrstuhl B für Mathematik
RWTH Aachen University
Germany

jens.eberhardt@rwth-aachen.de

Abstract

We show how the Tutte polynomial of a matroid M can be computed from its *condensed configuration*, which is a statistic of its lattice of cyclic flats. The results imply that the Tutte polynomial of M is already determined by the abstract lattice of its cyclic flats together with their cardinalities and ranks. They furthermore generalize similiar statements for perfect matroid designs and near designs due to Brylawski (1980) and help to understand families of matroids with identical Tutte polynomials as constructed by Giménez and later improved by Shoda (2012).

Keywords: matroid theory; Tutte polynomial; cyclic flats; perfect matroid designs

1 Introduction

The Tutte polynomial is a central invariant in matroid theory, but passing from a matroid M to its Tutte polynomial $\mathrm{T}(M; \mathrm{x}, \mathrm{y})$ generally means a big loss of information. This paper gives one explanation for this phenomenon by showing how little information about the *cyclic flats* of a matroid is really needed for the computation of its Tutte polynomial.

From now on let M be a matroid. A flat X in M is called *cyclic* if $M|X$ contains no coloops. Section 2 will recapitulate some basic facts about cyclic flats and show how the Tutte polynomial can be expressed in terms of *cloud* and *flock polynomials* of cyclic flats as introduced by Plesken in [7]. Then Section 3 establishes some important identities for cloud and flock polynomials needed later on.

The set $\mathcal{Z}(M)$ of cyclic flats of M is a lattice with respect to inclusion (see Figure 1). In Section 4 we introduce the *configuration* of M: the abstract lattice (or the isomorphism class of the lattice) of its cyclic flats together with their cardinalities and ranks. We then prove:
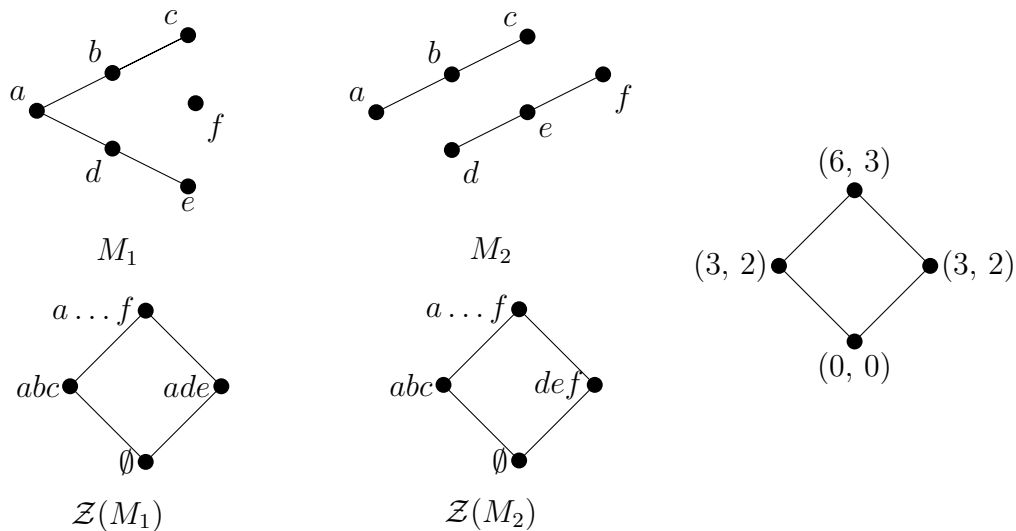
Figure 1: On the left: two non isomorphic matroids and their lattices of cyclic flats. On the right: their configuration (with labels $(|X|, \mathrm{r}_{M_i}(X))$ for $X \in \mathcal{Z}(M_i)$).

Theorem 4.1. *The Tutte polynomial of a matroid is determined by its configuration.*

While M is determined by its cyclic flats and their ranks (see [1]), it generally is far from being determined by its configuration (see Figure 1); there are even superexponential families of matroids with identical configurations (see [3] and [8]). So Theorem 4.1 explains one big part of the information lost when passing from a matroid to its Tutte polynomial.

In Section 5 we incorporate symmetries in M to shrink down the information needed for its Tutte polynomial even more. Let $G \leqslant \mathrm{Aut}(M)$, P be the set of G-orbits of $\mathcal{Z}(M)$ and $\{R_B\}_{B \in P}$ a system of representatives. The *condensed configuration* of M corresponding to P consists of the cardinalities and ranks of the R_B and the matrix $(\mathrm{A}_P(B,C))_{B,C \in P}$ where

$$\mathrm{A}_P(B,C) := |\{X \in B : X \subseteq R_C\}|.$$

This *generalized adjacency matrix* was introduced by Plesken in [6]; for $G = \{1\}$ it is simply the adjacency matrix of the lattice $\mathcal{Z}(M)$.

After discussing some examples, such as a condensed configuration for the Golay code matroid, we will prove:

Theorem 5.1. *The Tutte polynomial of M is determined by a condensed configuration of M.*

Section 6 then shows how to obtain a condensed configuration of a perfect matroid design using only the cardinalities of flats of given rank. Together with Theorem 5.1 this yields a new proof of Brylawski's results about the Tutte polynomial of perfect matroid designs in [2] (later reproved by Mphako in [5]).

Acknowledgments

2   Background

We quickly recapitulate the most important facts about cyclic flats and the cloud/flock formula for the rank generating polynomial from [7], while assuming familiarity with the basics of matroid theory. From now on let M be a matroid without loops and coloops with rank function r_M, closure operator cl_M and ground set $\mathcal{E}(M)$.

2.1   Cyclic flats

A flat X in M is called a *cyclic flat* if $M|X$, the restriction of M to X, contains no coloops. We denote the set of flats by $\mathcal{L}(M)$ and that of cyclic flats by $\mathcal{Z}(M)$; both form a lattice with respect to inclusion.

Example 1. Let $r < n$ and consider $\mathrm{U}_{r,n}$, the uniform matroid of rank r on n points. The lattice of flats $\mathcal{L}(\mathrm{U}_{r,n})$ is the set $\mathcal{P}_{<r}([n]) \cup \{[n]\}$ of subsets of $[n]$ of cardinality less than r, along with $[n]$, while the lattice of cyclic flats $\mathcal{Z}(\mathrm{U}_{r,n})$ is just $\{\emptyset, [n]\}$. If vice versa $|\mathcal{Z}(M)| = 2$, then M, which by assumption has no coloops, is a uniform matroid.

An arbitrary flat in M contains a unique maximal cyclic flat $\mathrm{e}_M(X)$, obtained by removing the coloops in $M|X$ from X. This induces a surjective and order-preserving map

$$\mathrm{e}_M : \mathcal{L}(M) \to \mathcal{Z}(M).$$

Like the lattice of flats, the lattice of cyclic flats behaves well with respect to restriction and contraction.

Remark 1. *If $X \subseteq Y$ are cyclic flats in M, then*

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

is an isomorphism of lattices and furthermore

$$\mathrm{r}_{M|Y/X}(Z - X) = \mathrm{r}_M(Z) - \mathrm{r}_M(X).$$

2.2 Cloud/flock formula for the rank generating polynomial

Instead of the Tutte polynomial $T(M; x, y)$ of M we will from now on study its *rank generating polynomial* $S(M; x, y)$ which is

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

The Tutte and rank generating polynomial can be transformed into each other since

$$T(M; x, y) = S(M; x - 1, y - 1).$$

The summands of the rank generating polynomial of M can be conveniently resorted using the cloud and flock polynomials of its cyclic flats introduced by Plesken in [7].

Definition 1. *Let X be a cyclic flat in M. The* cloud, *resp.* flock polynomial *of X in M is defined by*

$$c(M, X; x) := \sum_{Y \in e_M^{-1}(\{X\})} x^{r_M(M) - r_M(Y)}, \ resp.$$

$$f(M, X; y) := \sum_{Y \in cl_M^{-1}(\{X\})} y^{|Y| - r_M(Y)}.$$

Theorem 2.1 (Cloud/flock formula [7])**.**

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

Proof. See [7]. *Sketch:* Notice that $\mathcal{E}(M) = \biguplus_{X \in \mathcal{Z}(M)} cl_M^{-1}(e_M^{-1}(\{X\}))$ and that corank is constant on the fibers of cl_M and nullity (cardinality minus rank) is constant on the fibers of e_M. □

We note that the cloud/flock formula for the rank generating polynomial looks very similar to a convolution formula for the Tutte polynomial in [4] but is in fact not equivalent.

Example 2. We again consider the uniform matroid $U_{r,n}$ for $r < n$. Then $cl_{U_{r,n}}^{-1}(\{\emptyset\}) = \{\emptyset\}$ and $e_{U_{r,n}}^{-1}(\{[n]\}) = \{[n]\}$, hence

$$f(U_{r,n}, \emptyset; y) = c(U_{r,n}, [n]; x) = 1.$$

Furthermore $e_{U_{r,n}}^{-1}(\{\emptyset\}) = \mathcal{P}_{<r}([n])$, hence

$$c(U_{r,n}, \emptyset; x) = \sum_{0 \leqslant i < r} \binom{n}{i} x^{r-i}.$$

Analogously $cl_{U_{r,n}}^{-1}(\{[n]\}) = \mathcal{P}_{\geqslant r}([n])$ and

$$f(U_{r,n}, [n]; y) = \sum_{r \leqslant i \leqslant n} \binom{n}{i} y^{i-r}.$$

3 Identities for cloud and flock polynomials

We state some useful identities for cloud and flock polynomials and show that the cloud polynomial $c(M, \varnothing; x)$ and flock polynomial $f(M, \mathcal{E}(M); y)$ are already determined by the cloud and flock polynomials of all other cyclic flats. This is crucial for the recursive algorithms introduced later on.

The rank generating polynomial $S(M; x, y)$ of M is by definition a sum over all subsets of $\mathcal{E}(M)$ and it is easy to see that for $n = |\mathcal{E}(M)|$ and $r = r_M(M)$

$$S(M; x, x^{-1}) = \sum_{i=0}^{n} \binom{n}{i} x^{r-i}. \tag{3.1}$$

To make use of this identity we define the $\mathbb{Z}$-linear maps

$$d_x : \mathbb{Z}[x, y] \to \mathbb{Z}[x], \ f \mapsto \sum_{1 \leqslant i} a_i \, x^i, \ \text{for } f(x, x^{-1}) = \sum_i a_i \, x^i \ \text{and}$$

$$d_y : \mathbb{Z}[x, y] \to \mathbb{Z}[y], \ f \mapsto \sum_{0 \leqslant i} b_i \, y^i, \ \text{for } f(y^{-1}, y) = \sum_i b_i \, y^i.$$

Notice the subtle difference between the definitions of d_x and d_y: d_x cuts off the constant term, whereas d_y does not.

We furthermore define a notation for the cloud and flock polynomials in the uniform matroid $U_{r,n}$. For $r < n$ let

$$c_{r,n}(x) := c(U_{r,n}, \varnothing; x) = \sum_{0 \leqslant i < r} \binom{n}{i} x^{r-i} \ \text{and}$$

$$f_{r,n}(y) := f(U_{r,n}, [n]; y) = \sum_{r \leqslant i \leqslant n} \binom{n}{i} y^{i-r}.$$

In this notation equation (3.1) becomes

$$d_x(S(M; x, y)) = c_{r,n}(x) \ \text{and} \tag{3.2}$$
$$d_y(S(M; x, y)) = f_{r,n}(y). \tag{3.3}$$

Applying these identities to the cloud/flock formula of the rank generating polynomial we obtain:

Lemma 3.1. *The cloud polynomial of the empty set and the flock polynomial of the ground set depend only on the cloud and flock polynomials of the cyclic flats $X \notin \{\emptyset, \mathcal{E}(M)\}$:*

$$c(M, \varnothing; x) = c_{r,n}(x) - d_x\Big[\sum_X c(M, X; x) \, f(M, X; y)\Big] \ \text{and}$$

$$f(M, \mathcal{E}(M); y) = f_{r,n}(y) - d_y\Big[\sum_X c(M, X; x) \, f(M, X; y)\Big],$$

where $X \in \mathcal{Z}(M) - \{\emptyset, \mathcal{E}(M)\}$, n is the number of points and r the rank of M.

Proof. Equation (3.2) yields

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

Using the $\mathbb{Z}$-linearity of $\mathrm{d_x}$ we solve for $\mathrm{c}(M,\varnothing;\mathrm{x})$.

$$\mathrm{d_x}(\mathrm{c}(M,\varnothing;\mathrm{x})\,\mathrm{f}(M,\varnothing;\mathrm{y})) = c_{r,n}(\mathrm{x}) - \mathrm{d_x}\Big[\sum_{\substack{X \in \mathcal{Z}(M) \\ X \neq \emptyset}} \mathrm{c}(M,\emptyset;\mathrm{x})\,\mathrm{f}(M,X;\mathrm{y})\Big].$$

Now firstly $\mathrm{f}(M,\varnothing;\mathrm{y}) = \mathrm{c}(M,\mathcal{E}(M);\mathrm{x}) = 1$. Secondly $\mathrm{d_x}(\mathrm{c}(M,\varnothing;\mathrm{x})) = \mathrm{c}(M,\varnothing;\mathrm{x})$, since M does not consist of coloops and hence $\mathrm{c}(M,\varnothing;\mathrm{x})$ has no constant term. Furthermore $\mathrm{d_x}(\mathrm{f}(M,\mathcal{E}(M);\mathrm{y})) = 0$ since $\mathrm{d_x}$ cuts off the constant term. This yields the first statement. The second one follows analogously. $\qquad\square$

Another important fact is that for a cyclic flat X the cloud polynomial of X depends only on M/X and the flock polynomial of X depends only on $M|X$.

Lemma 3.2. *If X is a cyclic flat in M, then*

$$\mathrm{c}(M,X;\mathrm{x}) = \mathrm{c}(M/X,\emptyset;\mathrm{x}) \ \ and$$
$$\mathrm{f}(M,X;\mathrm{y}) = \mathrm{f}(M|X,X;\mathrm{y}).$$

Proof. Remark 1 yields a nullity-preserving bijection between $\mathrm{e}_M^{-1}(\{X\})$ and $\mathrm{e}_{M/X}^{-1}(\{\emptyset\})$ which implies the first identity. The second one is obvious. $\qquad\square$

4 Configurations

We introduce the *configuration* of a matroid and show how to compute the rank generating polynomial only using the configuration.

Definition 2. *The* configuration *of M consists of*

1. *the abstract lattice of cyclic flats in M, i.e., the isomorphism class of the lattice $(\mathcal{Z}(M), \subseteq)$, together with*

2. *the cardinalities and ranks of the cyclic flats.*

The configuration of a matroid describes how it is is build up from uniform matroids as the following example illustrates:

Example 3. 1.) According to Example 1, a matroid without coloops is isomorphic to the uniform matroid $\mathrm{U}_{r,n}$ $(r < n)$ if and only if its configuration is

$$\begin{array}{l} (n,\,r)\bullet \\ (0,\,0)\bullet \end{array}$$

2.) According to Remark 1, the configuration of the minor $M|Y/X$ (for cyclic flats $X \subset Y$) corresponds to the interval $[X, Y]$ in the configuration of M.

Consider for example the matroid M_i ($i = 1, 2$) from Figure 1 and let X be one of the cyclic flats of rank 2. Then from the configuration of M_i one can deduce that $M|X \cong U_{2,3}$ and $M/X \cong U_{1,3}$ since their configurations are

$$\begin{array}{cc} (3, 2)\bullet & (3, 1)\bullet \\ (0, 0)\bullet & \text{and} \quad (0, 0)\bullet. \end{array}$$

The motivation for introducing configurations is the following main theorem.

Theorem 4.1. *The rank generating polynomial of a matroid can be computed from its configuration.*

Proof. Lemmas 3.2 and 3.1 in effect provide a recursive method for computing the cloud and flock polynomials of all cyclic flats in M only using the configuration of M.

Using Lemma 3.2, cloud and flock polynomials of all non trivial cyclic flats $X \notin \{\emptyset, \mathcal{E}(M)\}$ can be recursively computed by the configurations of M/X and $M|X$, which in turn can be determined by the configuration of M (see Remark 1 and Example 3).

The cloud and flock polynomials of the empty set and the ground set of M can be determined using Lemma 3.1. The statement follows using the cloud/flock formula for the rank generating polynomial (Theorem 2.1). $\qquad\square$

In unpublished work by Giménez [3], later improved by Shoda [8], superexponential families of matroids with identical rank generating polynomials are constructed; as it turns out they all have - by construction - the same configuration. Theorem 4.1 now immediately proves that they have the same rank generating polynomial.

5 Condensed configurations

We show how to incorporate symmetries in M to shrink down the information needed for the computation of the rank generating polynomial even more by introducing the *condensed configuration*.

First, we generalize the notion of the set of orbits of cyclic flats.

Definition 3. *Let P be a partition of $\mathcal{Z}(M)$. We call P a condensation of $\mathcal{Z}(M)$ if for all $B, C \in P$:*

1. *cardinality and rank are constant on B and*

2. *$\mathrm{A}_P(B, C) := |\{X \in B : X \subseteq Y\}|$ is independent of the choice of $Y \in C$.*

For a condensation P we set $B \leqslant_P C$ if and only if $\mathrm{A}_P(B, C) > 0$, for $B, C \in P$. Then $(P, \leqslant_P)$ is a lattice.

Notice that conditions 1 and 2 are automatically satisfied if P is the set of G-orbits of $\mathscr{Z}(M)$ for $G \leqslant \mathrm{Aut}(M)$. Another interesting example is to take P as the set of equivalence classes of the relation $X \sim Y \Leftrightarrow M|X \cong M|Y$.

There can be many different condensations of $\mathscr{Z}(M)$; but since the supremum of two condensations in the lattice of partitions of $\mathscr{Z}(M)$ (with respect to coarseness) is also a condensation, there is always a unique coarsest condensation.

By forgetting the concrete realization of a condensation P as a partition of $\mathscr{Z}(M)$ we obtain something we want to call a *condensed configuration* of M.

Definition 4. *Let P be a condensation of $\mathscr{Z}(M)$ and $\{R_B\}_{B \in P}$ a system of representatives. The* condensed configuration *(corresponding to P) of M consists of*

1. the matrix $(\mathrm{A}_P(B, C))_{B,C \in P}$ and

2. cardinality and rank of R_B, for all $B \in P$.

Especially if M is highly symmetrical, a condensed configurations can give a really comprehensive overview of the arrangement of the cyclic flats in M as the following examples illustrate.

Example 4. 1.) If P is the trivial partition $P = \{\{X\} : X \in \mathscr{Z}(M)\}$, then the condensed configuration corresponding to P is the configuration of M, since $(\mathrm{A}_P(B, C))_{B,C \in P}$ is just the adjacency matrix of the lattice $(\mathscr{Z}(M), \subseteq)$.

2.) Consider the matroid $M = M_i$ $(i = 1, 2)$ from Figure 1 and denote the cyclic flats of rank 2 by X_1 and X_2. Clearly $P = \{\{\emptyset\}, \{X_1, X_2\}, \{\mathcal{E}(M)\}\}$ is a condensation of $\mathscr{Z}(M)$ and the corresponding condensed configuration can be represented by

$$
(\mathrm{A}_P(B, C))_{B,C \in P} = \begin{array}{c} \\ (0,0) \\ (3,2) \\ (6,3) \end{array} \begin{pmatrix} \overset{(0,0)}{1} & \overset{(3,2)}{1} & \overset{(6,3)}{1} \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix},
$$

where each row and column is labeled by $(|X|, \mathrm{r}_M(X))$, $X \in B$.

3.) Let M be the matroid induced by the extended binary Golay Code. The automorphism group of M, which is the Mathieu group M_{24}, acts transitively on the cyclic flats of M of given cardinality and rank and has six orbits on $\mathscr{Z}(M)$ altogether. The corresponding condensed configuration is

	(0, 0)	(8, 7)	(12, 10)	(12, 11)	(16, 11)	(24, 12)
(0, 0)	1	1	1	1	1	1
(8, 7)	0	1	3	0	30	75
(12, 10)	0	0	1	0	140	35420
(12, 11)	0	0	0	1	0	2576
(16, 11)	0	0	0	0	1	759
(24, 12)	0	0	0	0	0	1

.

From this we can for example read off that the cyclic flats of cardinality 12 and rank 11 are neither contained in nor contain any other non trivial cyclic flats in M. Hence we can safely remove this orbit of cyclic flats from $\mathcal{Z}(M)$ by circuit-hyperplane relaxation and obtain a new interesting matroid, which still has M_{24} as automorphism group, but cannot be found "in nature" like M.

The definition of a condensed configuration is motivated by the following generalization of Theorem 4.1.

Theorem 5.1. *The rank generating polynomial can be computed by a condensed configuration.*

Recall that in the proof of Theorem 4.1 we actually showed how to compute the cloud and flock polynomials in all minors $M|X/Y$ for cyclic flats $X \subset Y$. Generally, this is not possible in the case of condensed configurations, for the simple reason that from a condensed configuration we cannot derive exactly which minors appear in M. But we will be able to compute certain sums of cloud and flock polynomials.

Let P be a condensation of M, $\{R_B\}_{B \in P}$ a system of representatives. To prove Theorem 5.1, we show how to compute the rank generating polynomial of M only using the condensed configuration corresponding to P, i.e., the matrix $(\mathrm{A}_P(B,C))_{B,C \in P}$ and the cardinalities and ranks of the R_B, for $B \in P$.

Definition 5. *For $B, C \in P$ with $B \leqslant_P C$ we recursively define*

$$\underline{\mathrm{c}}(P, B, C; \mathrm{x}) := \mathrm{A}_P(B,C)\,\mathrm{c}_{r,n}(\mathrm{x}) - \mathrm{d}_\mathrm{x}(S(B,C)) \; and$$
$$\underline{\mathrm{f}}(P, B, C; \mathrm{y}) := \mathrm{A}_P(B,C)\,\mathrm{f}_{r,n}(\mathrm{y}) - \mathrm{d}_\mathrm{y}(S(B,C)), \; for$$
$$S(B,C) := \sum_D \underline{\mathrm{c}}(P, D, C; \mathrm{x})\,\underline{\mathrm{f}}(P, B, D; \mathrm{y})$$

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

Lemma 5.2. *In the notation of Definition 5,*

$$\underline{\mathrm{c}}(P, B, C; \mathrm{x}) = \sum_{\substack{X \in B \\ X \subseteq R_C}} \mathrm{c}(M|R_C, X; \mathrm{x}) \; and$$
$$\underline{\mathrm{f}}(P, B, C; \mathrm{y}) = \sum_{\substack{X \in B \\ X \subseteq R_C}} \mathrm{f}(M/X, R_C - X; \mathrm{y}).$$

Thus, the right hand sides are independent of the choice of $R_C \in C$, since the left hand sides are.

Proof. We proof this by induction on $\big|[B,C]_P\big|$. By definition

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

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

and D ranges over $[B,C]_P - \{B,C\}$.

If $[B,C]_P = \{B,C\}$ then $S(B,C) = 0$ and $M|R_C/X \cong \mathrm{U}_{r,n}$, for all $X \in B$ with $X \subseteq R_C$, and the claim follows.

Otherwise, since for all $D \in [B,C]_P - \{B,C\}$, both $\big|[D,C]_P\big|$ and $\big|[B,D]_P\big|$ are less than $\big|[B,C]_P\big|$, we can apply induction and get

$$S(B,C) = \sum_D \sum_{\substack{Y \in D \\ Y \subseteq R_C}} c(M|R_C,Y;\mathrm{x}) \sum_{\substack{X \in B \\ X \subseteq R_D}} f(M/X, R_D - X;\mathrm{y})$$
$$= \sum_D \sum_{\substack{Y \in D \\ Y \subseteq R_C}} \Big[c(M|R_C,Y;\mathrm{x}) \sum_{\substack{X \in B \\ X \subseteq R_D}} f(M/X, R_D - X;\mathrm{y}) \Big].$$

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

$$\sum_D \sum_{\substack{Y \in D \\ Y \subseteq R_C}} \Big[c(M|R_C,Y;\mathrm{x}) \sum_{\substack{X \in B \\ X \subseteq Y}} f(M/X, Y - X;\mathrm{y}) \Big]$$
$$= \sum_D \sum_{\substack{Y \in D \\ Y \subseteq R_C}} \sum_{\substack{X \in B \\ X \subseteq Y}} c(M|R_C,Y;\mathrm{x})\,f(M/X, Y - X;\mathrm{y}).$$

The three sums range over $\{(X,Y) : Y \in \mathcal{Z}(M),\ X \in B \text{ with } X \subsetneq Y \subsetneq R_C\}$ and can hence be rearranged to

$$\sum_{\substack{X \in B \\ X \subseteq R_C}} \sum_Y c(M|R_C,Y;\mathrm{x})\ f(M/X, Y - X;\mathrm{y}),$$

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

$$\underline{c}(P,B,C;\mathrm{x}) = \mathrm{A}_P(B,C)\,\mathrm{c}_{r,n}(\mathrm{x})$$
$$- \mathrm{d}_{\mathrm{x}}\Big(\sum_{\substack{X \in B \\ X \subseteq R_C}} \sum_Y c(M|R_C,Y;\mathrm{x})\,f(M/X, Y - X;\mathrm{y}) \Big)$$
$$= \sum_{\substack{X \in B \\ X \subseteq R_C}} \Big[\mathrm{c}_{r,n}(\mathrm{x}) - \mathrm{d}_{\mathrm{x}}\Big(\sum_Y c(M|R_C,Y;\mathrm{x})\,f(M/X, Y - X;\mathrm{y}) \Big) \Big].$$

By Lemma 3.1 and the definition of n and r this is

$$\sum_{\substack{X \in B \\ X \subseteq R_C}} c(M|R_C, X;\mathrm{x}).$$

The statement for the flock polynomial follows analogously. $\qquad\square$

Those sums of cloud and flock polynomials suffice for the computation of the rank generating polynomial and analogously to the cloud/flock formula we obtain:

Lemma 5.3.

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

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

Proof. By Lemma 5.2

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

$$= \sum_{B \in P} \sum_{\substack{X \in B \\ X \subseteq \mathcal{E}(M)}} c(M|\mathcal{E}(M), X; x) \sum_{\substack{Y \in 0_P \\ Y \subseteq R_B}} f(M/Y, R_B - Y; y).$$

Using the independence of choice of $R_B \in B$ the above sum is

$$\sum_{B \in P} \sum_{X \in B} \sum_{\substack{Y \in 0_P \\ Y \subseteq X}} c(M, X; x) f(M/Y, X - Y; y).$$

And finally, since $0_P = \{\emptyset\}$, this simplifies to

$$\sum_{B \in P} \sum_{X \in B} c(M, X; x) f(M, X; y)$$
$$= S(M; x, y). \qquad \square$$

The condensed configuration is constructed to contain all necessary information for the computation of the $\underline{c}(P, B, C; x)$ and $\underline{f}(P, B, C; y)$. This proves Theorem 5.1.

6 Condensed Configurations of Perfect Matroid Designs

A matroid M is called a *perfect matroid design* if all flats in M of given rank i have the same cardinality, say k_i. In [2] Brylawski showed that the rank generating polynomial of a perfect matroid design is already determined by the numbers k_i. We show how to recover a condensed configuration of a perfect matroid design from the numbers k_i as well. Combined with Theorem 5.1 this yields a new proof of Brylawski's result.

Let M be a perfect matroid design of rank r, let k_i be the cardinality of a flat of rank i and B_i the set of flats of rank i. Notice that B_i consists of cyclic flats if and only if $k_i > k_{i-1} + 1$. According to [2] for all $i \leqslant j$ and $Y \in B_j$ we have

$$|\{X \in B_i | X \subseteq Y\}| = \prod_{h=0}^{i-1} \frac{k_j - k_h}{k_i - k_h}.$$

Hence $P := \{B_i : k_i > k_{i-1} + 1\}$ is a condensation of $\mathcal{Z}(M)$. The condensed configuration of M corresponding to P depends only on the numbers k_i since the $\mathrm{A}_P(B_i, B_j)$ and the cardinalities and ranks of the cyclic flats are determined by the k_i. Summarizing this yields a new proof of:

Theorem 6.1 (Brylawski [2] and later Mphako [5])**.** *The rank generating (Tutte) polynomial of perfect matroid design depends only on the cardinalities and ranks of its flats.*

Notice that we actually proved a stronger statement, since we can moreover compute the sums of cloud and flock polynomials $\underline{c}(P, B_i, B_j; \mathrm{x})$ and $\underline{f}(P, B_i, B_j; \mathrm{y})$ now. This yields a new method to prove the nonexistence of certain perfect matroid designs. Firstly the coefficients of all those sums of cloud and flock polynomials have to be positive integers. Secondly cardinality and rank of all flats which have to appear in the matroid can be determined by the exponents of the sums of cloud polynomials and may not differ from the k_i.

The results are easily extended to *near designs*, which are like perfect matroid designs except that hyperplanes are allowed to have different cardinalities (see [2]). A condensed configuration of a near design can be recovered from the cardinalities of all flats of corank at most two and the number of hyperplanes of given rank and cardinality.

References

[1] Joseph E. Bonin and Anna de Mier. The lattice of cyclic flats of a matroid. *Ann. Comb.*, 12(2):155–170, 2008.

[2] Thomas Brylawski. The Tutte polynomial part I: General theory. *Third C.I.M.E. Conference on Matroid Theory and its Applications*, 1980.

[3] Omer Giménez. Unpublished work (sketched in [1]).

[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.

[5] Eunice Gogo Mphako. Tutte polynomials of perfect matroid designs. *Combin. Probab. Comput.*, 9(4):363–367, 2000.

[6] Wilhelm Plesken. Counting with groups and rings. *J. Reine Angew. Math.*, 334:40–68, 1982.

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

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