Counting Polynomials for Linear Codes, Hyperplane Arrangements, and Matroids

Wilhelm Plesken, Thomas Bächler

Received: February 17, 2012
Revised: May 22, 2013

Communicated by Thomas Peternell

Abstract. Thomas-decomposition of a polynomial systems and the resulting counting polynomials are applied to the theory of linear codes, hyperplane arrangements, and vector matroids to reinterpret known polynomials such as characteristic polynomials and weight enumerator, to introduce a new polynomial counting the matrices defining the same matroid, and to introduce the concept of essential flats revealing a structure which allows to rewrite the rank generating polynomial as a sum of products of univariate polynomials. Our concepts make no essential distinction between finite and infinite fields.

2000 Mathematics Subject Classification: Primary: 05B35, 05E20, 13P99; Secondary: 05-04
Keywords and Phrases: linear codes, hyperplane arrangements, weight enumerator, vector matroid, rank generating polynomial, Thomas decomposition, counting polynomial

1 Introduction

This paper is concerned with two topics: Recognizing known polynomial invariants in the theory of codes, hyperplane arrangements, and matroids such as characteristic polynomials, weight enumerators etc. as counting polynomials and finding a further example of counting polynomials, cf. [Ple 09a], [Ple 09b], in this area. Secondly, on the background of this, analysing the structure of the lattice of flats of a matroid by means of the Tutte-polynomial or rather the rank generating polynomial by singling out a special class of flats which we call essential. Though we started with linear codes and hyperplane arrangements, we realized that matroids yield a more appropriate language for our investigation.

The basic ideas of counting polynomials, which are based on the Thomas decomposition for systems of polynomial equations and inequations into disjoint simple systems, cf, [Tho 37], [Ple 09a], [BGLR 11], are briefly described in Section 2, in particular the relevant case of this paper, where the splitting behaviour of the polynomials in the resulting simple systems allows an enumeration of the possibly infinitely many solutions. In this case, the resulting counting polynomial yields the number of solutions of the system in the following cases: For a finite ground field K the number of solutions over any finite extension field E of K are obtained by substituting the number $|E|$ for the indeterminate. For a global field K as ground field the number of solutions over the residue class field F of the valuation ring for almost all discrete valuations of K are found upon substituting the order $|F|$ of the residue class field into the counting polynomial, e. g. $K = \mathbb{Q}$ with the finite prime fields $\mathbb{F}_p$ being the most common example. At the beginning of Section 2, the construction of counting polynomials is summarized as a finitely additive measure defined on the set of solution sets of polynomial systems (of equations and inequations) and taking values in the polynomial ring $\mathbb{Z}[u]$, where u is an indeterminate standing in some sense for the order of the field, even if it is infinite. In this way, for instance, the characteristic polynomial of a hyperplane arrangement gets a less formal and more algebraic-combinatorial meaning in the case of infinite fields, since it is simply the measure of the complement of the arrangement. Also, the critical theorem by Crapo and Rota, cf. [CrR 70] gets an interpretation in the case of infinite fields, so does the (comprehensive) weight enumerator of a linear code which Greene constructed from the Tutte-polynomial, cf. [Gre 76]. Whereas these examples deal with linear inequations, the final example, i. e. the counting polynomial of the set of rank r matrices of degree $k \times n$ requires slightly more background preparation.

Section 3 applies these ideas to introduce the matrix counter of a matroid which counts the "number" of matrices yielding the given matroid. If this is possible, the matroid is called polynomially countable. In this case, the matrix counter is shown to factorize into three factors: Firstly $\mathrm{gl}(k, u)$, where k is the rank of the matroid and $\mathrm{gl}(k, u) := (u^k - 1)(u^k - u) \cdots (u^k - u^{k-1})$ is the counting polynomial of the general linear group $\mathrm{GL}(n, \cdot)$. Secondly a factor $(u - 1)^{n-l}$, where n is the number of elements of the underlying set of the matroid and l is the number of connected components of the matroid. Finally, a factor called orbit counter. If the orbit counter is 1, the matroid seems to be particularly interesting from a geometrical combinatorial point of view. We call the matroid rigid in this case, note however that it is the simplest case from the point of view of the matrix counter. Some examples are discussed such as root systems of type A_n and B_n and the extended Golay code over $\mathbb{F}_2$ of length 24. On the other extreme is the matrix counter of the uniform matroid. Indeed, it would be a challenge to find which uniform matroids are polynomially countable.

Section 4 is a suggestion to reconstruct the lattice of flats out of the rank generating polynomial. The converse direction is well understood, cf. Example 2.4. The rank generating polynomial of a matroid M is defined as a sum over all subsets of the underlying set E of the matroid. By putting together all subsets with the same flat as closure, this sum gets a lot more structured. But then one can also put together all those flats whose complements in E have the same closure with respect to the dual M^* of the original matroid. This common closure has again an M-flat as complement in E, which we call an essential flat. As a result of this the generating polynomial of M becomes a sum over the essential flats only. The summand corresponding to an essential flat X is the product of a polynomial in the first variable x depending only on the minor M/X of M and a polynomial in the second variable y depending only on the restiction $M|X$. This can be used to discover all the essential flats from the rank generating polynomial as described in Remark 4.11. The theory and two examples, the first being the Golay-code of length 24 are discussed in Section 4.

The final Section 5 discusses matroids of rank 3. The counting polynomials are computed for all matroids on up to seven points, and some examples on 8 points are given to demonstrate new phenomena. The tables of this section depend on heavy computer calculations with the program [BLH 13] to compute the Thomas decomposition of a polynomial system of equations and inequations. Various interesting issues come up, such as two nonisomorphic matroids with the same rank generating polynomial but different counting polynomials, different behaviours in different characteristics, factorization properties of the orbit counter, non-split examples where the matrix counter is not defined, etc.
We are grateful to the referees to point out very helpful, relevant comments and literature.

2 Counting Polynomials

We first collect the facts from [Ple 09a] and [Ple 09b] relevant for this paper. Let K be a field with algebraic closure $\overline{K}$. Consider subsets of $\overline{K}^n$ of the form $N_p := \{a \in \overline{K}^n | p(a) = 0\}$ with $p \in K[x_1, \dots, x_n]$, i. e. hypersurfaces defined over K. Denote by $\mathcal{L}(K, n)$ the set of subsets of $\overline{K}^n$ obtained by taking finite intersections, unions, and complements of the N_p for various such $p \in K[x_1, \dots, x_n]$ iteratively. Clearly, if

$$\pi_n : \overline{K}^n \to \overline{K}^{n-1} : (a_1, \dots, a_n) \mapsto (a_1, \dots, a_{n-1})$$

denotes the projection (in case $n > 1$), then $\pi_n(S) \in \mathcal{L}(K, n-1)$ for any $S \in \mathcal{L}(K, n)$. Moreover $\lambda_S(b) := \{a \in \overline{K} | (b, a) \in S\} \in \mathcal{L}(K, 1)$ for each $b \in \pi_n(S)$.

Proposition 2.1. *Let K be a field of characteristic zero. For every $n \in \mathbb{N}$ there is a unique map*

$$c = c_n : \mathcal{L}(K, n) \to \mathbb{Z}[u] : S \mapsto c(S) = c(S, u)$$

(where $c(S, u)$ is called the counting polynomial of S) with the following properties:
1.) For finite sets $S \in \mathcal{L}(K, n)$, one has $c(S, u) = |S|$, the number of elements in S.
2.) For any k-dimensional affine subspace N of $\overline{K}^n$ defined over K one has $c(N, u) = u^k$.
3.) For any $S, T \in \mathcal{L}(K^n)$, one has $c(S, u) + c(T, u) = c(S \cap T, u) + c(S \cup T, u)$, in particular, $c(K^n - S, u) = u^n - c(S, u)$.
4.) In case $n > 1$, for any $S \in \mathcal{L}(K, n)$ where $c_1(\lambda_S(b), u) \in \mathbb{Z}[u]$ is independent of $b \in \pi_n(S)$ one has

$$c_n(S, u) = c_{n-1}(\pi_n(S), u) \cdot c_1(\lambda_S(b), u)$$

The proof is based on a finite decomposition of the systems of equations and inequations into certain triangular systems called simple, which were introduced by J. M. Thomas, cf. [Tho 37]. Various algorithmic refinements of this decomposition algorithm and an implementation are discussed in [BGLR 11]. It is work in progress extending [LMW 10] to show that the above result also holds for fields K of positive characteristic. The cases relevant for this paper, the so called split systems, were discussed in [Ple 09b] and require no assumptions on the characteristic of K. In any case, the implementation in [BLH 13] has worked successfully for all examples of this paper.

Though the counting polynomial in general only says something about the set of solutions over the algebraic closure, for the present investigation we want to use the counting polynomials to count the number of solutions over finite fields. This is not always possible. Namely, if one specifies the free variables in the equations of a triangular system to lie in a fixed field, the resulting univariate polynomials in general do not split over this field. However, if we have split simple systems, i. e. if the polynomials of the simple systems factorize into degree-one-polynomials in their leading variable, cf. [Ple 09b], it becomes possible. To cover as many cases as possible we go beyond [Ple 09b] and distinguish three cases:

Definition 2.2. *Let $S \in \mathcal{L}(K, n)$ for some field K.*
1.) S is called uniformly enumerable *if S can be decomposed into disjoint split simple systems, in the sense of [Ple 09b], where the variables of $K[x_1, \ldots, x_n]$ are taken in the same order for all simple systems.*
2.) S is called enumerable *if S can be decomposed into disjoint systems $S_i \in \mathcal{L}(K, n)$, such that for every i there exists a split simple system $T_i \in \mathcal{L}(K, n)$ and a bijection $T_i \to S_i$ defined by some rational function over*

K.
3.) S is called POLYNOMIALLY COUNTABLE *if S is the union of finitely many systems $S_i \in \mathcal{L}(K,n)$, $i \in I$ such that at least one of $\cap_{i\in J} S_i$ or the complement $\overline{K}^n - \cap_{i\in J} S_i$ is enumerable for each subset J of I.*

Clearly, uniformly enumerable sets are enumerable and enumerable ones are polynomially countable. The notion of polynomial countability becomes especially interesting if K is finite. In case K is a global field, $S \in \mathcal{L}(K,n)$ defines a set $S_L \in \mathcal{L}(L,n)$ for all but finitely many finite residue class fields L corresponding to a non Archimedian valuation of K. In case S satisfies one of the three properties above, so does S_L in all but finitely many residue class fields L.

PROPOSITION 2.3. *Let $S \in \mathcal{L}(K,n)$ be a polynomially countable system over a field K.*
1.) In case K is finite there is a unique polynomial $c(S,u) \in \mathbb{Z}[u]$ satisfying

$$|S \cap L^n| = c(S, |L|)$$

for all finite field extension (L/K).
2.) In case K is a global field, there is a unique polynomial $c(S,u) \in \mathbb{Z}[u]$ satisfying

$$|S_L \cap L^n| = c(S, |L|)$$

for all but finitely many residue class fields L defined by valuations of K.
In both cases, we call $c(S,u)$ the FAITHFUL COUNTING POLYNOMIAL *of S.*

Proof. The uniqueness of the faithful counting polynomial is in both cases clear, since infinitely many values of it are specified. We come to the existence. In the uniformly enumerable case one simply takes the counting polynomial, cf. [Ple 09b], and in the enumerable case the sum of the counting polynomials of the split simple systems T_i. The general case of polynomially countable systems is reduced to the enumerable case via the inclusion exclusion principle. □

Note that the faithful counting polynomial is independent of the ordering of the variables or more generally of the choice of the coordinates (over the ground field K). Whether a faithful counting polynomial is uniquely defined for more general fields is interesting but not relevant for the applications in the present paper. To demonstrate the difference between counting polynomial and faithful counting polynomial, look at $S := N_p$ for $p := x^2 - y \in \mathbb{Q}[x,y]$. Taking the variables in the order $y < x$ yields $2(u-1)+1$ as counting polynomial, which is not faithful, whereas the order $x < y$ yields the faithful counting polynomial u.
The simplest case of a polynomially countable system is one given by linear (degree one) equations and inequations. In fact such a system is uniformly enumerable, but usually one obtains the faithful counting polynomial by the inclusion exclusion principle, since the computation of THOMAS-decomposition

becomes rather expensive once a certain number of inequations is involved. We remark that, in this case, no assumptions on the field K are necessary and the counting polynomials are independent of the choice of the coordinate system. Here are some examples.

Example 2.4. *1.) Characteristic polynomial of a central hyperplane arrangement.*
Let V be a K-vector space of dimension k and $\varphi_i \in V^* - \{0\}$ for $i = 1, \dots, n$ be linear forms on V. Then the counting polynomial $c(S, u)$ of the system $\varphi_i(x) \neq 0$ for $i = 1, \dots n$ is called the characteristic polynomial of the hyperplane arrangement of the $\ker(\varphi_i)$. In case K is finite it counts the number of elements in $V - \cup_i \ker(\varphi_i)$ in a faithful way as explained above, i. e. it also counts the corresponding number of elements for any finite extension field of K. It clearly is monic of degree k and the coefficient of u^{k-1} is the negative of the number of different hyperplanes $\ker(\varphi_i)$, cf. [CrR 70], [OrT 92],[Ath 96]. For a recent survey on the interplay of linear codes, hyperplane arrangements, and matroids cf. e. g. [Sta 07].
2.) (Comprehensive or) Support weight enumerator of a code.
Let $A \in K^{k \times n}$ a matrix of rank k and let V be the K-vector space spanned by the rows of A. We want to count the vectors of V (and the scalar extensions of V) having exactly j components zero for $j = 0, \dots, n$. To this aim let φ_i be the projection of the row space of A corresponding to the i-th column. For each subset I of $\underline{n}$ let $S_I \in \mathcal{L}(K, k)$ be the system defined by $\varphi_j(v) = 0$ for $j \in I$ and $\varphi_j(v) \neq 0$ for $j \notin I$. Then the (comprehensive) weight enumerator

$$\omega_A(u, x, y) := \sum_{I \subseteq \underline{n}} c(S_I, u) x^{|I|} y^{n-|I|}$$

gives exactly the weight enumerator for any finite extension field L of K, in case K is finite, if one substitutes $|L|$ for u. (Note however, this weight enumerator also makes sense if K is not finite, even beyond Proposition 2.3.) Note also, the $I \subseteq \underline{n}$ with $c(S_I, u) \neq 0$ are just the flats of the matroid induced by the matrix A, cf. 3.1 below. In a splendid piece of work, it was shown in [Gre 76] how this weight enumerator could be obtained from the Tutte *polynomial $T_A(x, y)$ as follows:*

$$\omega_A(u, x, y) = (1-u)^k u^{n-k} T_A\left(\frac{1 + (u-1)x}{1-x}, \frac{1}{x}\right),$$

cf also [Bri 02]. Conversely, the Tutte*-polynomial is determined by the support weight enumerator, cf. [Jur 12] and [JuP 13], where also the most recent account is given on these results, as well as on the connections between matroids, codes, and hyperplane arrangements. (All these results do not depend on the finiteness of K, as assumed in the original papers.)*

More general systems described by polynomials of degree one in each variable still have some chance to be enumerable or at least polynomially countable.

For instance the $n \times n$-determinant *det* yields the faithful system $\det(x_{ij}) \neq 0$ with polynomial

$$\mathrm{gl}(n,u) := (u^n-1)(u^n-u)\cdots(u^n-u^{n-1})$$

well known from the order of the general linear group over a finite field. The group theoretic counting of orbits can be used to find faithful counting polynomials. Here is an example from determinantal varieties, where we set $\mathrm{gl}(0,u) := 1$:

Proposition 2.5. *The set of $k \times n$-matrices of rank r defined over a field K is uniformly enumerable. Its (faithful) counting polynomial is given by*

$$\frac{\mathrm{gl}(k,u)\mathrm{gl}(n,u)}{\mathrm{gl}(r,u)\mathrm{gl}(k-r,u)\mathrm{gl}(n-r,u)u^{(k-r)r+(n-r)r}}$$

Proof. It follows from Theorem 2.8 of [Ple 09b] that the system is uniformly enumerable over any field. Therefore one has a faithful counting polynomial. We compute it by viewing the set as the orbit of the matrix

$$\begin{pmatrix} I_r & O_{r\times(n-r)} \\ O_{(k-r)\times r} & O_{(k-r)\times(n-r)} \end{pmatrix}$$

under the group $\mathrm{GL}(k,K) \times \mathrm{GL}(n,K)$ acting on $K^{k\times n}$ via

$$(\mathrm{GL}(k,K) \times \mathrm{GL}(n,K)) \times K^{k\times n} \to K^{k\times n} : ((g,h),m) \mapsto gmh^{-1}.$$

By computing the stabilizer, one gets exactly the denominator of the above number with u substituted by $|K|$ for any finite field K. Since we know that the result must be a polynomial, we have found it via these infinitely many values. $\square$

Note, the degree of the polynomial just derived is $r(-r+n+k)$, which is increasing in r for $r = 0,\ldots,k$, so that the dimension of the so called generic determinantal variety of $k \times n$-matrices of rank $\leq r$ is equal to $r(-r+n+k)$, which is well known.

3 Matrix counters

We proceed into a different direction now, by restricting the group action in the last proof to $\mathrm{GL}(k,K) \times \mathrm{Diag}(n,K)$, where $\mathrm{Diag}(n,K) \leq \mathrm{GL}(n,K)$ is the subgroup of all diagonal matrices of $\mathrm{GL}(n,K)$. For this action one has a finer invariant than the rank, namely the vector matroid represented by the matrices. We use the following notation: For $n \in \mathbb{N}$ let $\underline{n} := \{1,2,\ldots,n\}$ and $\mathrm{Pot}_k(\underline{n})$ the set of all k-element subsets of $\underline{n}$.

Definition 3.1. *Let $k \leq n$. The map*

$$\mu : K^{k\times n} \to \mathrm{Pot}(\underline{n}) : A \mapsto \{X \in \mathrm{Pot}(\underline{n}) \mid |X| = \mathrm{rank}(A) = \mathrm{rank}(A_{|X})\}$$

is called the matroid map, *where $A_{|X}$ denotes the submatrix of A formed by the columns with column indices in X. For $A \in K^{k\times n}$ of rank r, the pair $(\underline{n}, \mu(A))$ with $\mu(A) \subseteq \mathrm{Pot}_r(\underline{n})$ is called the* (vector) matroid *of A.*

We shall usually assume that the matrix A is of rank k. An (abstract) matroid is a pair consiting of a ground set $\underline{n}$ and a subset B of $\mathrm{Pot}_k(\underline{n})$ satisfying certain axioms similar to the Steinitz exchange properties of bases, cf. [Oxl 11] or [Wel 76]. If the ground set is clear, we only refer to B as the matroid. If B is of the form $\mu(A)$ for some matrix over the field K, the matroid B is called K-representable. It should be noted that the weight enumerator, cf. Example 2.4, of the linear code spanned by the rows of a matrix $A \in K^{k\times n}$ only depends on the matroid $\mu(A)$. These issues are concerned with linear equations and inequations and therefore the counting polynomials in this context are faithful. However, the counting polynomial defined next is defined via polynomials which are of degree at most one in each of their variables, where it is not clear whether or not they are faithful.

Definition 3.2. *1.) Let K be a field,*

$$R_{k,n} := K[x_{1,1}, x_{2,1}, \ldots, x_{k,1}, x_{1,2}, \ldots, x_{k,2}, \ldots, x_{k,n}]$$

and $X := (x_{ij})_{i\in\underline{k}, j\in\underline{n}} \in R_{k,n}^{k\times n}$ denotes a $k \times n$-matrix of indeterminates. Finally $X_{|b} := (x_{i,j}) \in R_{k,n}^{k\times k}$ with $i \in \underline{k}, j \in b$ denotes the submatrix of X with column indices in $b \in \mathrm{Pot}_k(\underline{n})$.
2.) For a non empty subset B of $\mathrm{Pot}_k(\underline{n})$ denote by $S(B) \in \mathcal{L}(K, kn)$ the set of solutions over the algebraic closure $\overline{K}$ of K of the polynomial system

$$\det(X_{|b}) \neq 0 \textit{ for } b \in B, \det(X_{|b}) = 0 \textit{ for } b \in \mathrm{Pot}_k(\underline{n}) - B.$$

3.) In case $S(B) \neq \emptyset$ we call B uniformly enumerable, enumerable, *resp.* polynomially countable *(over K) if $S(B)$ has this property. In either of these cases the faithful counting polynomial $c(S(B), u) \in \mathbb{Z}[u]$ is called the* full matrix counter *of B and denoted by $c(B, u)$ or $c_B(u)$.*

Hence B is a matroid representable over $\overline{K}$ if and only if the counting polynomial of $S(B)$ with respect to some order of the variables is not zero. Clearly in the above definition, one might assume K to be a prime field.

Example 3.3. *1.) $k := 1$. Any non empty subset B of $\mathrm{Pot}_1(\underline{n})$ is a representable matroid. Its matrix counter is $(u-1)^{|B|}$.*
2.) For $k := 2$ the representable matroids are given as follows: Let $\underline{n} = \biguplus_{i=0}^{s} M_i$ with M_0 (representing the zero columns) possibly empty, but the other M_j (called parallel classes) nonempty and $s \geq 2$. Then

$$B := \{\{a, b\} \mid \textit{ there are } i, j \textit{ with } 0 < i < j \leq s, a \in M_i, b \in M_j\}$$

and the full matrix counter of B is given by

$$c_B(u) = u \cdot (u+1) \cdot (u-1)^{n-|M_0|} \cdot \prod_{i=1}^{s-2}(u-i),$$

which can easily be obtained in the same way as one computes the order $(u^2-1)(u^2-u)$ of the full linear group: In the critical case $|M_i| = 1$ for $i > 0$ one has

$$\prod_{i=1}^{s}(u^2-1-(i-1)(u-1)) = (u-1)^s \prod_{i=1}^{s}(u+1-(i-1)).$$

Note, the characteristic of the underlying field has no relevance in this particular case. However, if K is finite, one might have $c_B(|K|) = 0$.

Here is a first property of the full matrix counter.

Proposition 3.4. *Let $B \subseteq \mathrm{Pot}_k(\underline{n})$ be polynomially countable over any prime field. Then*

$$\mathrm{gl}(k,u) \mid c_B(u), \text{ i. e. } c_B(u) = \mathrm{gl}(k,u) \cdot r_B(u)$$

for some $r_B(u) \in \mathbb{Z}[u]$, which we call reduced matrix counter *of B.*

Proof. If K is of characteristic zero, we may assume without loss of generality $K = \mathbb{Q}$, since the equations and inequations come from determinants and hence only involve integers. Since in the process of computing simple systems, only finitely many denominators come up, we may choose any prime p dividing none of these and pass to the finite field $\mathbb{F}_p$ and still retain the same matroid B. Since B is polynomially countable, $c_B(|L|)$ is equal to the number of matrices $A \in L^{k\times n}$ with $\mu(A) = B$ for any finite extension field L of $\mathbb{F}_p$. Since $\mathrm{GL}(k, L)$ acts semiregularly on this set of matrices, i. e. any stabilizer is trivial and all orbits have length $\mathrm{gl}(k, |L|)$, one easily gets $\mathrm{gl}(k,u) \mid c_B(u)$. □

Often the reduced matrix counter of $B \subseteq \mathrm{Pot}_k(\underline{n})$ is the counting polynomial of $S(B)$ intersected with the set of those $k \times n$-matrices for which certain k columns form the unit matrix. Unfortunately, it is in general not true that a split simple system with an equation of the form $x_i - k$ for some $k \in K$ added can be decomposed into split simple systems. Here is a practical sufficient criterion for B to be polynomially countable.

Proposition 3.5. *Let $B \subseteq \mathrm{Pot}_k(\underline{n})$ and choose some $a \in B$. By $S(a, B) \in \mathcal{L}(K, kn)$ we denote the set of solutions of the system*

$$X_a = I_k, \det(X_{|b}) \neq 0 \text{ for } b \in B, \det(X_{|b}) = 0 \text{ for } b \in \mathrm{Pot}_k(\underline{n}) - B,$$

where I_k denotes the $k\times k$ unit matrix. If $S(a, B)$ is polynomially countable with faithful counting polynomial $c(S(a, B), u)$, then B is polynomially countable with reduced matrix counter $r_B(u) = c(S(a, B), u)$.

Proof. Let $S(a) \in \mathcal{L}(K, kn)$ be the set of solutions of $X_a = I_k$, and $S'(a) \in \mathcal{L}(K, kn)$ be the set of solutions of $\det(X_a) \neq 0$. Then

$$\mathrm{GL}(k, \overline{K}) \times S(a) \to S'(a) : (g, A) \mapsto g \cdot A$$

is a bijective birational map defined over K. Note, $\mathrm{GL}(k, \overline{K})$ is uniformly enumerable by [Ple 09b], say

$$\mathrm{GL}(k, \overline{K}) = \biguplus G_i$$

with finitely many split simple systems G_i. Assume first that $S(a, B)$ is enumerable, say $S(a, B) = \biguplus C_j$. Then above bijection restricts to a birational bijection $G_i \times C_j \to G_i \cdot C_j$ for every pair (i, j). Since

$$S(B) = \mathrm{GL}(k, \overline{K}) \cdot S(a, B) = \biguplus_{i,j} G_i \cdot C_j,$$

the claim follows in this case.
If $S(a, B)$ is only polynomially enumerable, the proof is a slight modification. $\square$

Lemma 3.6. *In the situation of $S(a, B)$ above, for any given pair $(i, j) \in \underline{k} \times (\underline{n} - a)$ one either has $x_{ij} = 0$ for all $X \in S(a, B)$ or $x_{ij} \neq 0$ for all $X \in S(a, B)$.*

Proof. Let k be the unique element of a such that the k-th column of X is the i-th column of the identity matrix. Let $c := (a - \{k\}) \cup \{j\}$. Either $c \in B$, in which case $x_{ij} = \pm\mathrm{Det}(X_{|c}) \neq 0$ or $c \notin B$, in which case $x_{ij} = \pm\mathrm{Det}(X_{|c}) = 0$. $\square$

Beyond the action of the general linear group $\mathrm{GL}(k, K)$ one can take the torus action into account, i. e. the action of $(K^*)^n$ which results in further irreducible factors of the matrix counter. Recall that a vector matroid is called decomposable or disconnected if it is of the form $\pi(\mu(\mathrm{Diag}(A_1, A_2)))$ for some matrices $A_1 \in K^{k' \times n'}, A_2 \in K^{k'' \times n''}$ with $k' + k'' = k$ and $n' + n'' = n$ and for some permutation $\pi \in S_n$.

Proposition 3.7. *If in the notation of Proposition 3.5 $S(a, B)$ is polynomially countable, then $(u-1)^{n-l} | r_B(u)$, where l is the number of connected components of B. The polynomial $o_B(u) := (u-1)^{-(n-l)} r_B(u) \in \mathbb{Z}[u]$ is called the* orbit counter *of B.*

Proof. Since r_B is obviously multiplicative in the components of B, it suffices to assume that B is a connected matroid. Also we may assume $a = \underline{k}$. The group $D_n := (\overline{K}^*)^n$ acts on $S(a, B) \in \mathcal{L}(K, kn)$ by

$$D_n \times S(a, B) \to S(a, B) : (d, A) \mapsto (d_i^{-1} A_{i,j} d_j)_{i \in \underline{k}, j \in \underline{n}},$$

where the factors d_i^{-1} make sure that the submatrix of the first k columns remains the unit matrix. Note, by Lemma 3.6 for any $(i, j) \in \underline{k} \times \underline{n}$ either

$A_{ij} = 0$ for all $A \in S(a, B)$ or $A_{ij} \neq 0$ for all $A \in S(a, B)$. Call $T \subseteq \underline{k} \times (\underline{n} - \underline{k})$ a RIGIDITY FRAME, if
1.) $|T| = n - 1$,
2.) $(i, j) \in T$ implies $A_{ij} \neq 0$ for all $A \in S(a, B)$, and
3.) $\pi_1(T) = \underline{k}, \pi_2(T) = \underline{n} - \underline{k}$, where π_i denotes the projection onto the i-th component for $i = 1, 2$.
Since B is connected, such a rigidity frame T exists. It gives rise to the system of equations

$$A_{i,j} d_j = d_i \qquad (i, j) \in T$$

for the d_i, the solutions of which transforms $A \in S(a, B)$ into a matrix of

$$S_T(a, B) := \{A \in S(a, B) | A_{i,j} = 1 \text{ for all } (i, j) \in T\}.$$

Since the stabilizer of any $A \in S_T(a, B)$ in D_n, which is isomorphic to K^*, acts trivially on $S_T(a, B)$, it follows that $S_T(a, B)$ is a set of representatives of the action of D_n on $S(a, B)$. Hence we have a bijective rational function

$$\tilde{D}_n \times S_T(a, B) \to S(a, B) : (d, A) \mapsto (d_i^{-1} A_{i,j} d_j)_{i \in \underline{k}, j \in \underline{n}}$$

defined over the ground field, where $\tilde{D}_n$ is the subgroup of all $d \in D_n$ with $d_1 = 1$. The claim follows. ☐

Clearly $o_B(u)$ counts the orbits of $\mathrm{GL}(k, K) \times (K^*)^n$ on $S(B)$. If $o_B(u) = 1$, B is called RIGID. In practice, one often proceeds by the above ideas, however in reversed order:

COROLLARY 3.8. *In the notation of the last proof let $T \subseteq \underline{k} \times (\underline{n} - \underline{k})$ be a rigidity frame and assume that $S_T(a, B)$ is polynomially countable with faithful counting polynomial $o_B(u)$. Then $S(a, B)$ is polynomially countable with reduced matrix counter $(u-1)^{n-l} \cdot o_B(u)$ and B is polynomially countable with matrix counter $c_B(u) = \mathrm{gl}(k, u) \cdot (u-1)^{n-l} \cdot o_B(u)$.*

Here are some examples demonstrating how one may proceed:

EXAMPLE 3.9. *The root system A_n viewed as its matrix of positive roots in $K^{n \times \binom{n+1}{2}}$ gives rise to the matroid $\mu(A_n)$ which is rigid, i. e. whose reduced matrix counter is*

$$(u-1)^{\binom{n+1}{2} - 1}.$$

Proof. Let $(e_0, \ldots, e_n)$ be a basis on an $n+1$-dimensional vector space over a field K. Consider the set of vectors $X_n := \{e_i - e_j | 0 \leq i < j \leq n\}$. As basis we choose $(e_0 - e_i | i = 1, \ldots n)$. The coordinate columns of the elements of X_n yield a matrix M with $\mu(M) = \mu(A_n)$. For convenience we index the columns of our matrix by the set of 2-element subsets of $\{0, 1, \ldots, n\}$. In particular the basis part of the matrix has indices $\{0, i\}$ for $i \in \underline{n}$. Call this set a. Now let

$A \in S(a, \mu(A_n))$. We look at the submatrix with column indices in $\mathrm{Pot}_2(\underline{n})$ in the spirit of the last proof. We may choose as rigidity frame the set

$$L := \{(i, \{i, j\}) | i \in \underline{n-1}, i < j\} \cup \{(i, \{1, i\}) | i = 2, \ldots, n\}.$$

We may assume $A_{s,t} = 1$ for $(s,t) \in L$. Clearly A also has zeroes in the positions where M has zeroes. In particular the first unknown entry of A is $A_{3,\{2,3\}}$. The central observation is that $\{\{1,2\}, \{1,3\}, \{2,3\}\}$ is a cycle of our matroid, i. e. the three corresponding column vectors are linearly dependent. We know all the entries of theses three column vectors except $A_{3,\{2,3\}}$. Hence we know exactly what the linear dependence looks like:

$$A_{-,\{1,2\}} - A_{-,\{1,3\}} - A_{-,\{2,3\}} = 0.$$

This determines the unkonwn entry. Similarly all the other entries can be determined and the claim follows. □

Example 3.10. *The root system B_n viewed as its matrix of positive roots in $K^{n \times n^2}$ gives rise to the matroid $\mu(B_n)$ whose reduced matrix counter is*

$$(u-1)^3(u-2) \text{ for } n = 2 \text{ and } (u-1)^{n^2-1} \text{ for } n > 2.$$

Proof. The case $n = 2$ is an easy exercise. We look at the case $n = 3$ from which the general proof will be clear.

$$A := \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & -1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & -1 & 1 & -1 & 1 \end{pmatrix}$$

yields $\mu(B_3)$. Note columns 1,2,3,4,6,8 yield A_3. The decisive linear dependence for the rest is $A_{-,5} - A_{-,6} + A_{-,9} = 0$. Otherwise the proof is similar to the one for A_n. □

The case of root systems D_n for $n \geq 3$ can be reduced to the previous cases and results in the appropriate power of $u - 1$ for the reduced matrix counter. Here is another source of examples for polynomially countable vector matroids. As a third exampel we look at the Golay code.

Example 3.11. *Let $M \in \mathbb{F}_2^{12 \times 24}$ be the generator matrix of the extended* Golay *code of length 24 over $\mathbb{F}_2$. The induced matroid is rigid, i. e. the orbit counter is* 1 *and the reduced matrix counter* $(u-1)^{23}$.

Proof. By Corollary 3.8 and Proposition 3.5, we are free to choose any basis of $\mu(M)$. Since the automophism group M_{24} has exactly two orbits on the bases of the induced matroid $\mu(M)$ of M, cf. Example 4.12, there are essentially two different types of matrices possible for M. In either case we may assume (after

permuting the columns of M appropriately) that the submatrix of the first 12 columns of M is the identity matrix, i. e. $M = (I_{12}|N)$. In the first type of bases each row and column of N has exactly 7 ones and 5 zeroes. Since this type is slightly more awkward to treat, we choose the second type. Here one has apart 11 columns with exactly 7 ones and exactly one pair of a row and a column intersecting in a zero but otherwise consisting of ones (referred to as cross of ones below).
Let K be a field containing $\mathbb{F}_2$. For any matrix $A \in K^{12\times 24}$ with $\mu(A) = \mu(M)$ we may assume the same shape $A = (I_{12}|X)$. By Lemma 3.6, the positions with zeroes in X are exactly the same as in N. As rigidity frame T, we choose the set of positions in the cross of ones in N, where the position of the zero in the crossing is replaced by some index pair (i, j) outside the cross with $N_{ij} = 1$. In X, we may also choose these 23 positions to be one and we remain with $11 \cdot (7 - 1) - 1$ positions where the entry is not zero, but otherwise not known. We start with the i-th row: We know $X_{ij} = 1$. Let k be such that $X_{ik} \neq 0$ and X_{ik} is not yet known. Let l be the row index of the row of ones in the cross. Then $X_{li} = X_{lk} = 1$ and the four numbers form a submatrix whose determinant is zero, because the determinant of the corresponding submatrix of N is zero. (Note, this submatrix can be complemented to a submatrix of 12 complete columns by choosing from among the first 12 columns of M similarly as in the proof of Lemma 3.6.) Coming back to the submatrix of X, it has three entries equal to 1 and determinant 0, which implies $X_{ik} = 1$ for the last entry. In this way we conclude that all the remaining non zero entries of the i-th row of X are equal to 1. Similarly all the non zero entries of the j-th column of X are equal to 1. With each new position proved to contain a one, by the same argument, its complete row and column has all its non-zero entries equal to 1. Since the matroid is obviously connected, this finally shows that all unknown entries are equal to one. □

PROPOSITION 3.12. *Let $B \subseteq \mathrm{Pot}_k(\underline{n})$ be a matroid and $a \in B$ such that $S(a, B)$ is uniformly enumerable, enumerable, resp. polynomially countable, then so is $S(\underline{n} - a, B^*)$ where $B^* := \{\underline{n} - b | b \in B\}$ is the dual matroid of B. In this case, the reduced matrix counters are equal: $r_B(u) = r_{B^*}(u)$.*

Proof. We may assume $a = \underline{k}$. Then $(I_k|A) \in S(a, B)$ if and only if $(-A^{tr}|I_{n-k}) \in S(\underline{n} - a, B^*)$. The claim follows easily. □

It seems that matroids with few bases have a tendency to be polynomially countable. In [Sko 96] a survey of the number of representations of uniform rank 3 matroids on 7, 8, and 9 point is given, which indicates that polynomial countability for 8 and 9 points is only given if certain univariate quadratic polynomials split over the ground field, though the number of solutions can be described in the other cases as well. This phenomenon in called quasisplit case in [Ple 09b], cf. Example 5.9 1) for simpler examples. One might suspect that sooner or later one gets examples which are not polynomially countable and not even quasisplit. A good candidate for this might be the matroid of rank

3 on 11 points in [Stu 93], pg. 101, where among the equations for $S(a, B)$ the absolutely irreducible polynomial given there turns up. In the last chapter, rank 3 vector matroids on up to 7 points are given with their matrix counters. There are also examples given there with the same Tutte polynomial, but different matrix counters; on the other hand there is also an abundance of pairs of non isomorphic matroids with the same matrix counter.

4 The rank generating polynomial

In this section, M denotes a matroid on the set E of n elements with rank function $\rho : \mathrm{Pot}(E) \to \mathbb{Z}_{\geq 0}$. The rank generating polynomial is defined as

$$S(M; x, y) := \sum_{X \subseteq E} x^{\rho(E)-\rho(X)} y^{|X|-\rho(X)} \in \mathbb{Z}[x, y].$$

A good example is the rank generating polynomial

$$p_{n,k}(x, y) := \binom{n}{k} + \sum_{i=1}^{n-k} \binom{n}{k+i} y^i + \sum_{i=1}^{k} \binom{n}{k-i} x^i$$

of the uniform matroid of rank k, where every k-element subset of E forms a basis of M. The aim of this section is to reduce the summation over all subsets of E to something more manageable. One rather simple approach is to define the deviation polynomial

$$\delta(M; x, y) := p_{n,k}(x, y) - S(M; x, y) \in \mathbb{Z}[x, y]$$

where k is the rank of M. For matroids with a big number of bases, $\delta(M; x, y)$ will have few terms and the rank generating polynomial can be easily recovered form $\delta(M; x, y)$. Since in both $p_{n,k}(x, y)$ and in $S(M; x, y)$ all $\binom{n}{k-s}$ subsets of M with $k - s$ elements are taken into account, one has the following.

Remark 4.1. *Let $\delta(M; x, y) = \sum_{i,j} a_{ij} x^i y^j$, then for each $s \in \mathbb{Z}$ one has*

$$\sum_i a_{s+i,i} = 0$$

A more serious attempt to analyse and understand the sum with the idea of simplification is by grouping together the summands belonging to one flat.

Definition 4.2. *1.) The polynomial*

$$S(M; y) := S(M; 0, y) \in \mathbb{Z}[y]$$

is called the generator generating polynomial *of M.*
2.) For $X \subseteq E$ let

$$\sigma(X) := \{e \in E | \rho(X) = \rho(X \cup \{e\})\}$$

the closure operator *with respect to* M *and for any* flat $X = \sigma(X)$ *call*

$$\sigma^{-1}(\{X\}) := \{Y \subseteq E | \sigma(Y) = X\}$$

flock *of* X*. Finally*

$$\mathcal{L}(M) := \{X \subseteq E | \sigma(X) = X\}$$

the set of all flats of M*.*

Clearly $S(M;y) = \sum_{X \in \sigma^{-1}(\{M\})} y^{|X|-\rho(X)}$. If we simply write $S(X;y)$ for $S(M|X;y)$ for any flat X of M, where $M|X$ denotes the restriction of M to X, then the original definition of the rank generating polynomial becomes:

$$S(M;x,y) = \sum_{X \in \mathcal{L}(M)} x^{\rho(E)-\rho(X)} S(X;y).$$

To proceed further, we exhibit flats with the same generator generating polynomial. Recall that a coloop of M is an element e of E occuring in each basis of M, i. e. $\rho(E - \{e\}) = \rho(E) - 1$.

Definition 4.3. *A flat* $X \in \mathcal{L}(M)$ *is called* essential *if* $M|X$ *has no coloop.*

One clearly has the following lemma.

Lemma 4.4. *Let* $X \in \mathcal{L}(M)$*. Then there exists a unique essential flat* Y*, called the essential flat* $\epsilon(X)$ *of* X*, such that*

$$M|X = M|Y \oplus M|\{e_1\} \oplus \cdots \oplus M|\{e_r\}$$

where $e_1, \ldots, e_r$ *are the coloops of* $M|X$*. Moreover*

$$\sigma^{-1}(\{Y\}) \to \sigma^{-1}(\{X\}) : Z \mapsto Z \cup \{e_1, \ldots, e_r\}$$

is a bijection so that

$$S(X;y) = S(Y;y).$$

This leads to the following definiton.

Definition 4.5. *For any essential flat* $Y \in \epsilon(\mathcal{L}(M))$ *call* $\epsilon^{-1}(\{Y\})$ *the* cloud *of* Y *and*

$$S(M,Y;x) := \sum_{X \in \epsilon^{-1}(\{Y\})} x^{\rho(E)-\rho(X)}$$

the cloud polynomial *of* Y*.*

Summarizing, we have the following.

Proposition 4.6. *Let M be a matroid without loops on the set E. Then*

$$\mathrm{Pot}(E) = \biguplus_{Y \in \epsilon(\mathcal{L}(M))} \sigma^{-1}(\epsilon^{-1}(\{Y\}))$$

with a bijection

$$\sigma^{-1}(\epsilon^{-1}(\{Y\})) \to \epsilon^{-1}(\{Y\}) \times \sigma^{-1}(\{Y\}) : Z \mapsto (\sigma(Z), Z \cap Y)$$

for every essential flat Y. In particular

$$S(M; x, y) = \sum_{Y \in \epsilon(\mathcal{L}(M))} S(M, Y; x) S(Y; y).$$

Whereas the generator generating polynomial $S(Y; y)$ depends on Y or, more precisely, $M|Y$ only, the cloud polynomial $S(M, Y; x)$ depends on the embedding of Y in M. In fact, it depends only on the minor M/Y:

Proposition 4.7. *Let M be a matroid without loops on the set E and Y an essential flat of M. Then $\emptyset$ is an essential flat of the minor M/Y and there is a bijection between the clouds:*

$$\epsilon_M^{-1}(\{Y\}) \to \epsilon_{M/Y}^{-1}(\{\emptyset\}) : X \mapsto X - Y.$$

In particular, $S(M, Y; x) = S(M/Y, \emptyset; x)$.

Proof. $\emptyset$ is an essential flat of M/Y if and only if no element $a \in E - Y$ is dependent, i. e. $\rho_M(Y \cup \{a\}) > \rho_M(Y)$ for all $a \in E - Y$. This however is clear, since Y is a flat. Clearly the map $X \mapsto X - Y$ maps flats (contained in E) with respect to M containing Y to flats (contained in $E - Y$) with respect to M/Y, where $\rho_{M/Y}(X - Y) = \rho_M(X) - \rho_M(Y)$. The claim follows. □

To get a better understanding, we connect the result to the passage to the dual matroid M^*. Denote the closure operator on $\mathrm{Pot}(E)$ with respect to M^* by σ^* and the essentiality operator on $\mathcal{L}(M^*)$ by ϵ^*.

Lemma 4.8. *Let $X \subseteq E$ and $Y := \complement X = E - X$. For $a \in E$ the following statements are equivalent:*
1.) $a \in \sigma(X) - X$.
2.) a is a coloop of $M^*|Y$.

Proof. Clearly 1.) is equivalent to a being a loop of the minor $M/X = M.Y$. Hence 1.) holds iff a is a coloop of $(M.Y)^*$, which by Theorem 4.3.2 of [Wel 76] is isomorpic to $M^*|Y$. □

If X is an essential flat of M, we need to distinguish between $\epsilon^{-1}(\{X\})$ and $\epsilon^{\uparrow}(X) := \{Z \subseteq E | X \subseteq Z, Z - X$ consists of coloops of $M|Z\}$.

Theorem 4.9. *Let M be a matroid on E without loops and coloops. Let $\complement$: $\mathrm{Pot}(E) \to \mathrm{Pot}(E) : X \mapsto E - X$.*
*1.) $\complement$ induces a bijection (*Galois*-correspondence) between $\epsilon(\mathcal{L}(M))$, the set of essential flats of E with respect to M, and $\epsilon^*(\mathcal{L}(M^*))$, the set of essential flats of E with respect to M^*.*
2.) For an essential flat X in E with respect to M, the bijection $\complement$ induces a bijection between $\sigma^{-1}(\{X\})$ and $\epsilon^{*\uparrow}(E-X)$ and a bijection between $\epsilon^{\uparrow}(X)$ and $\sigma^{*-1}(\{E-X\})$.
3.) For an essential flat X in E with respect to M one has $\epsilon^{-1}(\{X\}) \subseteq \epsilon^{\uparrow}(X)$, indeed $\epsilon^{-1}(\{X\})$ consists of all the flats in $\epsilon^{\uparrow}(X)$.

Proof. 1.) Let $X \subseteq E$. Then X is a flat with respect to M, if and only if $M^*|(E-X)$ has no coloops by Lemma 4.8. If $X \subseteq E$ is an M-flat, then X is an essemtial M-flat, if and only if $M|X$ has no coloops. So $X \subseteq E$ is an essential flat of M, iff $M^*|(E-X)$ has no coloops and $M|X$ has no coloops. By applying the same argument in reverse, with the roles of $M|X$ and $M^*|(E-X)$ interchanged, this is again equivalent to $E-X$ being an essential M^*-flat.
2.) Immediately from Lemma 4.8. 3.) Clear by definition. □

Here are some examples and characterizations of essential flats. The proofs are straightforward.

Remark 4.10. *Let M be a matroid on the set E without loops and coloops.*
1.) $\emptyset$ and E are essential flats.
2.) If a hyperplanes (of codimension 1) is an essential flat, its cloud polynomial is x.
3.) If $S(M,x,y) = \sum_{i=0}^{\rho(E)} x^i g_i(y)$ and $\deg g_i(y) > \deg g_{i+1}(y)$ for one i, then M has α_i essential flats of dimension $\rho(E)-i$ consisting of $\deg g_i(y)$ elements, where α_i is the leading coefficient of $g_i(y)$.
4.) If $X \subseteq E$ is an essential flat and $M|X = M|A \oplus M|B$ with $X = A \uplus B$, then A, B are essential flats.
5.) If S is a set of circuits of M, then $\sigma(\bigcup_{X\in S} X)$ is an essential flat of M. Every essential flat is of this form for a suitable set S of circuits.
6.) The minimal number $|S|$ of circuits such that $E = \sigma(\bigcup_{X\in S} X)$ may be called the covering number *of M. It measures certain aspects of the complexity of M. For instance the uniform matroid of rank k on n elements has the covering number 1.*

The rank generating polynomial can of course be computed from the information about the essential flats $\neq E$ using the above results, however, we can also get information about the lattice of flats from the rank generating polynomial.

Remark 4.11. *For a polynomial $p(x,y) = \sum_{i,j} a_{i,j}x^iy^j \in \mathbb{Z}[x,y]$ with non negative coefficients $a_{i,j}$, call the exponent (i,j) extreme if $a_{i,j} > 0, a_{i+k,j} = 0, a_{i,j+k} = 0$ for all $k \geq 1$. Starting with the rank generating polynomial $p(x,y) = \sum_{i,j} a_{i,j}x^iy^j$ of M and an extreme exponent (i,j) one knows of the existence of $a_{i,j}$ essential flats. Subtract the contribution of these essential flats* *from $p(x,y)$ and proceed in the same way with the difference polynomials to get the next set of essential flats.*

Example 4.12. *The* Golay*-code C of length 24 and dimension 12 over $\mathbb{F}_2$ gives rise to a selfdual matroid with rank generating polynomial $p_{24,12}(x,y) - \delta(C;x,y)$, where $\delta(C;x,y)$ is given by*

$$(1-xy)(r(y) + 644(55xy + 2039) + r(x))$$

with

$$r(t) := 759t^4 + 12144t^3 + 91080t^2 + 425040t$$

The automorphism group is known to be the Mathieu*-group M_{24} of order $|M_{24}| = 2^{10}3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$ and by means of GAP, cf. [GAP] some relevant orbits of M_{24} in $\mathrm{Pot}(\underline{24})$ can easily be computed towards the following results. The essential flats fall into 6 orbits: The empty set, the circuits of length 8, certain 10-dimensional flats of covering number 2, circuits of length 12, the complements of the 8-circuits (the dual of which are isomorphic to the matroid of affine 4-space over $\mathbb{F}_2$), and finally the full set. Here is the rank generating polynomial split up into the corresponing sum of 6 summands, each of which is a product of the length of the orbit, the cloud polynomial (in x), and the generator generating polynomial (in y):*

$$\begin{gathered}
1 \cdot (\textstyle\sum_{i=0}^{6} \binom{24}{i} x^{12-i} + |M_{24}| \cdot (\frac{1}{720}x^5 + \frac{1}{384}x^4 + \frac{1}{432}x^3 + \frac{1}{1440}x^2)) \cdot 1 + \\
759 \cdot (x^5 + 16x^4 + 120x^3) \cdot (y+8) + \\
35420 \cdot x^2 \cdot (y^2 + 12y + 48) + \\
2576 \cdot x \cdot (y+12) + \\
759 \cdot x \cdot (y^5 + 16y^4 + 120y^3 + 560y^2 + 1680y + 2688) + \\
1 \cdot 1 \cdot (\textstyle\sum_{i=0}^{7} \binom{24}{i} y^{12-i} + |M_{24}|(\frac{121}{40320}y^4 + \frac{1}{189}y^3 + \frac{11}{1440}y^2 + \frac{67}{7920}y + \frac{1}{176}))
\end{gathered}$$

Because of the presence of the 12-circuits one easily sees that the covering number of the full matroid is 2. We list some additional information about the orbits of M_{24} on the set of 12-subsets of $\{1, 2, \ldots, 24\}$ as an interpretation of the coefficients of $(xy)^i$ in the rank generating polynomial above: Two orbits of bases of lengths 1020096 and 370944, one orbit of 12-circuits of length 2576 (stabilizers isomorphic to M_{12}), and one further orbit of length $1275120 = 759 \cdot 1680$, of which each element has one linear relation and has the complement of an octave as its closure. Finally, there is one orbit of essential flats with two relations of length 35420. Of course, the above way to write the rank generating polynomial encodes much more information than the polynomial itself.

We finish this chapter with an example of a non selfdual matroid of rank 8 on 15 points. Its combinatorial structure is sufficiently clear so that its rank generating polynomial as a sum of the products of its cloud and generator generating polynomials can in principle be computed by hand using the results of this chapter. One way to describe it is as the dual of the matroid of the columns of $p_{15}(A_{15})$, where $p_{15}(t)$ is the 15-cyclotomic polynomial and A_{15}

is the permutation matrix of a 15-circuit or, if one prefers it, the companion matrix of $t^{15}-1$. So the example can be considered as a cyclic code over $\mathbb{Q}$. In the actual formulation of the example, a different description is given, which results in a permutation of the ground set, but gives a clearer picture of the structure.

EXAMPLE 4.13. *Let $Z_k \in \mathbb{Q}^{(k-1)\times k}$ the matrix whose first $k-1$ columns form the unit matrix and whose last column has all entries equal to -1. Note, the matroid of the columns of Z_k is a k-circuit. Choose $A \in \mathbb{Q}^{8\times 15}$ to be the* KRONECKER *product $A := Z_5 \otimes Z_3$. The associated matroid M is of rank 8 on $E := \underline{15}$. Its structure is governed by the (essential) circuits given by the sets of entries in one of the rows or colums of the matrix*

$$\kappa := \begin{pmatrix} 1 & 4 & 7 & 10 & 13 \\ 2 & 5 & 8 & 11 & 14 \\ 3 & 6 & 9 & 12 & 15 \end{pmatrix}$$

The automorphism group of M is the direct product $S_3 \times S_5$ whose action on E is induced by the action of S_3 on the rows and of S_5 on the columns of κ. The closure operator σ takes a subset $X \subseteq E$ and obtains $\sigma(X)$ as the union of X, of the column sets of κ whose intersection with X has two elements, and of the row sets of κ whose intersection with X has four elements. The essentiality operator ϵ takes a flat $X \subseteq E$ and removes all elements from X for which neither its full row nor its full column is contained in X. In particular, the essential flats are unions of complete rows (0, 1, or 3) and complete columns (0,1,2,3, or 5). The notation for the $S_3 \times S_5$-orbits is forced upon one: $i_r j_c$ meaning $i \in \mathbb{Z}_{\geq 0}$ rows and $j \in \mathbb{Z}_{\geq 0}$ columns. With this information it is not so difficult to compute the generator generating polynomials and the cloud polynomials except maybe the cloud polynomial for 0_r0_c and the generator generating polynomial for 3_r5_c. However, these con be easily obtained from Remark 4.1, once everything else is computed. Here is the result: The first factor in each summand is the length of the $S_3 \times S_5$-orbit, followed by the cloud polynomial, and finally by the generator generating polynomial. On the right the symbol for the orbit of the essential flat is given.

$$\begin{array}{c|l} 1\cdot 1\cdot (y^4+6y^3+24y^2+50y+75)(3+y)^3+ & 3_r5_c \\ 30\cdot x\cdot (y^2+5y+12)(3+y)^2+ & 1_r3_c \\ 30\cdot x^2\cdot (y^2+6y+13)(3+y)+ & 1_r2_c \\ 10\cdot x^2\cdot (3+y)^3+ & 0_r3_c \\ 15\cdot x^3\cdot (14+7y+y^2)+ & 1_r1_c \\ 10\cdot (x^4+9x^3+18x^2+6x)\cdot (3+y)^2+ & 0_r2_c \\ 3\cdot x^4\cdot (5+y)+ & 1_r0_c \\ 5\cdot (x^6+12x^5+54x^4+96x^3+54x^2)\cdot (3+y)+ & 0_r1_c \\ 1\cdot (x^8+15x^7+90x^6+270x^5+390x^4+210x^3)\cdot 1 & 0_r0_c \end{array} .$$

For completeness we add the corresponding information for the dual matroid. The notation for the $S_3 \times S_5$-orbits is kept, though one has to take the comple-

ments of the sets above.

$$\begin{array}{c|l}
1 \cdot 1 \cdot (y^8 + 15y^7 + 105y^6 + 450y^5 + 1305y^4 + 2670y^3 + 3870y^2 & \\
\qquad + 3780y + 2025)+ & 0_r0_c \\
5 \cdot x \cdot (y^6 + 12y^5 + 66y^4 + 216y^3 + 456y^2 + 612y + 432)+ & 0_r1_c \\
3 \cdot x \cdot (y^4 + 10y^3 + 40y^2 + 80y + 80)+ & 1_r0_c \\
10 \cdot x^2 \cdot (y^4 + 9y^3 + 36y^2 + 78y + 81)+ & 0_r2_c \\
15 \cdot (x^2 + x) \cdot (y + 4)(y^2 + 4y + 8)+ & 1_r1_c \\
10 \cdot x^3 \cdot (12 + 6y + y^2)+ & 0_r3_c \\
30 \cdot (x^3 + 2x^2 + x) \cdot (12 + 6y + y^2)+ & 1_r2_c \\
30 \cdot (x^4 + 3x^3 + 3x^2 + x) \cdot (4 + y)+ & 1_r3_c \\
1 \cdot (x^7 + 15x^6 + 105x^5 + 335x^4 + 495x^3 + 303x^2 + 15x) \cdot 1 & 3_r5_c
\end{array}$$

5 Vector matroids of rank 3

Call a vector matroid simple [Wel 76] if it has no circuits of length 1 or 2. Any matroid can easily be reduced to such a one, and conversely all the other matroids can easily be constructed from the simple matroids once their automorphism groups are known. Moreover, the matrix counters change by an easily computed power of $u - 1$. In this section we compute the matrix counters for the simple matroids of rank three on $n \leq 7$ points. The first aim is to introduce a symbol for each simple matroid of rank 3, cf. [Wel 76] Section 1.11. Our formalization of the graphical notation there has the advantage that permutations of the underlying set E can be easily dealt with, i. e. automorphism groups can almost be read off. The rank three matroids are best understood via their nontrivial hyperplanes.

Definition 5.1. *Let M be a matroid of rank 3 with underlying set E.*
1.) A hyperplane of M of more than 2 elements is called nontrivial.
2.) For $i \in E$ let $\mathrm{Hy}(i)$ denote the set of all nontrivial hyperplanes containing i.
3.) $i \in E$ is called conglomerator, *if $\mathrm{Hy}(i)$ contains more than one element.*
4.) The set of all conglomerators of M is denoted by $\mathrm{Congl}(M)$.
5.) $i \in E$ is called lazy *if it is not contained in any nontrivial hyperplane.*

Example 5.2. *Let M be a simple matroid of rank* 3.
Let $|E| = 4$, then M has no conglomerators. It either consists only of lazy elements, or has exactly one nontrivial hyperplane, which then necessarily contains 3 elements. So either all elements are lazy or exactly one is lazy.
Let $|E| = 5$, then M has at most one conglomerator. In this case there are no lazy elements and one has two nontrivials hyperplanes of length 3 having the conglomerator in common.

Definition 5.3. *Let M be a simple matroid of rank* 3 *on a set E. The symbol $[M]$ of M is an element of the free abelian group $\mathbb{Z}[\mathrm{Pot}(E) \times \{3, 4, \ldots |E| - 1\}]$*

with $\mathbb{Z}$*-basis* $\mathrm{Pot}(E) \times \{3, 4, \dots |E| - 1\}$*, where for brevity the basis elements are written as* X_a *rather than* (X, a) *for* $X \subseteq E, a \in \{3, 4, \dots |E| - 1\}$*. The symbol* $[M]$ *is then defined as follows:*

$$[M] := \sum_H (H \cap \mathrm{Congl}(M))_{|H|},$$

where the sum is taken over all nontrivial hyperplanes H*. If* E *or the number of elements of* E *are not clear from the context, we write* $[M]_E$ *or* $[M]_{|E|}$ *instead of* $[M]$*.*

Note that M can be recovered from $[M]$ up to the names of the elements not contained in $\mathrm{Congl}(M)$.

Example 5.4. *Let* M *be a simple matroid of rank* 3 *and* $E := \underline{n}$*.*
Let $|E| = 4$*, then* $[M]$ *is either* 0 *for the uniform matroid or* $\emptyset_3$ *for any rank 3 matroid on* E *with exactly one (unspecified) nontrivial hyperplane, which then consists of 3 elements.*
Let $|E| = 5$*, then* $[M]$ *is either* 0*,* $\emptyset_3$*,*$\emptyset_4$*, or* $2\{i\}_3$ *for some* $i \in E$*.*
Note, the matroid on 5 elements with symbol $(\emptyset_3)_5$ *is obtained from the one with symbol* $(\emptyset_3)_4$ *on four elements by adding one lazy element.*

It is clear that the symbol determines the matroid up to isomorphism. To list all rank 3 simple matroids on n elements up to isomorphism by their symbols, we may (and will) restrict to the symbols of matroids M with $\mathrm{Congl}(M) = \underline{a}$ for some $a \leq n$. It remains to deal with the problem of isomorphism for these symbols.

Example 5.5. *Let* $n := 6$*. Then one has exactly 9 isomorphism classes of simple matroids. They are represented by the symbols*

$$0,\ \emptyset_3,\ \emptyset_4,\ 2\{1\}_3$$

obtained from matroids on less than 6 elements by adding lazy elements, further the ones with $|\mathrm{Congl}(M)| \leq 3$*:*

$$\emptyset_5,\ 2\emptyset_3,\ \{1\}_3 + \{1\}_4,\ \{1,2\}_3 + \{1,3\}_3 + \{2,3\}_3,$$

and one with $|\mathrm{Congl}(M)| = 6$*:*

$$\{1,3,4\}_3 + \{1,5,6\}_3 + \{2,3,6\}_3 + \{2,4,5\}_3.$$

It is clear that the symbols satisfy certain obvious conditions, which we list.

Remark 5.6. *Let* $\alpha \in \mathbb{Z}[\mathrm{Pot}(\underline{n}) \times \{3, 4, \dots, n-1\}]$ *be a symbol of a rank 3 matroid. Then*
1.) If S_a *occurs in* α*, then* $|S| \leq a$*.*
2.) If $S_a \neq T_b$ *both occur in* α*, then* $|S \cap T| \leq 1$*. Also the coefficient of* S_a *can be at most 1 unless* $|S| = 1$*.*

3.) Let $\mathrm{Congl}(\alpha)$ *denote the union of the sets in the first component of the terms of* α*. Then for each* $i \in \mathrm{Congl}(\alpha)$ *there occur at least two* S_a*,* T_b *in* α *with* $i \in S$ *and* $i \in T$*.*
4.) The smallest cardinality $|E|$ *for the ground set of a matroid with symbol* α *is*

$$|\mathrm{Congl}(\alpha)| + \sum_{S_a} (a - |S|)$$

where the sum is taken over all terms S_a *(with multiplicities) occuring in* α*.*
5.) The rank generating polynomial can be read off from the symbol α*, more precisely from the indices of the summands of the symbol:*

$$p_{n,3}(x,y) - \delta_\alpha(x,y) \text{ with } \delta_\alpha(x,y) = (1-xy)\sum_{l=0}^{n} y^l \sum_{H\in\mathcal{H}} \binom{|H|}{3+l}$$

where $\mathcal{H}$ *is the set of all nontrivial hyperplanes.*

Existence of vector matroids cannot a priori be read off from the symbol, but usually has to be computed explicitly. Our main interest is to find the matrix counters in the cases where it is possible, including the relevant information on the fields. The following tables were computed as follows: For a given rank 3 matroid, a basis and a rigidity frame, cf. proof of Proposition 3.7, is fixed. This gives an ansatz for the matrix with a unit matrix and a matrix of indeterminates as complemetary submatrices. By the choice of the rigidity frame, certain indeterminates are substituted by 1. Each 3×3-minor results in an equation or inequation, depending on whether we have dependence or a basis in the matroid. This system is put into the AlgebraicThomas-program, cf. [BLH 13]. For many cases a suitable order of the variables yields a faithful counting polynomial, i. e. an orbit counter right away, including information on the characteristics. If not all systems split, one might try a different order of variables. If the system is too big, we use the inclusion-exclusion principle to generate systems of equations only, which often can be used to obtain a faithful counting polynomial of a polynomially countable set. The question of enumerability usually remains open in these cases.

Example 5.7. *For* $|E| = n = 6$*, Table 1 lists the orbit counters of the simple matroids of rank 3 up to* S_n*-action sorted according to the degrees of the matrix counters. These matroids are all indecomposable except for* $\emptyset_5$*, which has two compontents and the orbit counter has to be multiplied by* $(u-1)^4$ *instead of* $(u-1)^5$ *to obtain the reduced matrix counter* $r_B(u)$*. Note also that* $2\emptyset_3$ *and* $2\{1\}_3$*, which have the same rank generating polynomial, are distinguished by their matrix counter. In the uniform case* 0*, the system* $S_T(a, B)$*, cf. Corollary 3.8, is polynomially countable, where all characteristics* $\neq 2$ *can be treated simultaneously, however the final faithful counting polynomial is the same for all characteristics including 2. In all the other cases we have uniform enumerability for* $S_T(a, B)$*, with the restriction that for* $\emptyset_3$ *characteristic 2 has to be treated separately, but again yields the same orbit counter. We note that for*

symbol cf. 5.3	$o_B(u)$ (orbit counter cf. 3.7)	$\lvert S_6\text{-orbit}\rvert$
0	$(u-2)(u-3)(u^2-9u+21)$	1
$\emptyset_3$	$(u-2)(u-3)(u-4)$	20
$2\emptyset_3$	$(u-2)^2$	10
$2\{1\}_3$	$(u-2)(u-3)$	90
$\emptyset_4$	$(u-2)(u-3)$	15
$\{1\}_3+\{1\}_4$	$(u-2)$	60
$\{1,2\}_3+\{1,3\}_3+\{2,3\}_3$	$(u-2)$	120
$\emptyset_5$	$(u-2)(u-3)$	6
$\{1,2,4\}_3+\{1,3,5\}_3+$ $\{2,3,6\}_3+\{4,5,6\}_3$	1	30

Table 1: Orbit counters for simple rank 3-matroids on 6 points, cf. Example 5.7

the uniform matroid 0 *the above mentioned inclusion-exclusion count has been applied. However, in this particular case, it can be avoided by also computing the contribution of the non simple matroids towards the counting polynomial for all rank 3 matrices in* $K^{3\times 6}$*, cf. Proposition 2.5. After division by* $\mathrm{gl}(3,u)$*, this is the product of the 2nd, 4-th, 5-th, and 6-th cyclotomic polynomial*

$$\begin{aligned}&(u+1)(u^2+1)(u^4+u^3+u^2+u+1)(u^2-u+1)\\ =\ &10(3u-1)(3u^2-3u+1)\\ &+(u^2+2u-5)(u^3+3u^2-10)(u-1)^4\\ &+5(u+3)(13u^2-14u+4)(u-1)^2\\ &+3(5u-3)(u^3+4u^2+u-11)(u-1)^3\end{aligned}$$

where the i*-th summand gives the contribution* $\sum_B r_B(u)$ *of the matrices whose matroid* B *reduces to a simple matroid on* $2+i$ *elements for* $i=1,2,3,4$.
Finally, the factors of the orbit polynomials can usually be given interpretations. For instance, in the case of the uniform matroid $[0]_6$*, the factors* $u-2$ *and* $u-3$ *mean that there are no representations of the matroid over a field of 2 or three elements. For bigger fields they can be interpreted as follows: Once three columns of the matrix are chosen to form the unit matrix and, say one column and one row of the remaining matrix is chosen to be equal to 1 in each position as rigidity frame, cf. proof of Proposition 3.7, choose a fixed column* C *among the two other columns. The first remaining position of* C *can be chosen to be* $a\neq 1,0$ *and the second remaining position of* C *can be chosen to be* $c\neq 0,1,a$*. Independently of these choices, the matrix can be completed in* $(u^2-9u+21)$ *ways.*

The next example treats the simple rank 3 matroids on 7 points. By Propostion 3.12 this can be turned into (almost all of) the corresponding list of orbit counters of rank 4 matroids on 7 points. The orbit counters for 0 in Examples 5.7 and 5.8 have already been known by different methods, cf. [Sko 96] last section and the references there. Also the more complicated cases of rank 3 matroids on 8 and 9 points are described there, cf. also [ISS 95]. For a more geometric approach to these problems, cf. [Sko 92] and [RoS 96].

Example 5.8. *For $|E| = n = 7$ the matroids of rank 3 are all polynomially countable. Table 2 lists the orbit counters of the simple matroids of rank 3 up to S_n-action sorted according to the degrees of the matrix counters. These matroids are all indecomposable except of $\emptyset_6$, which has two compontents and the orbit counter has to be multiplied by $(u-1)^5$ instead of $(u-1)^6$ to obtain the reduced matrix counter $r_B(u)$. In this case of 7 points for E, one often gets different orbit counters for characteristic 2. Remarkably the orbit counters of the same matroid (of rank 3 on 7 points) for characteristic 2 and characteristic $\neq 2$ differ only by a number. Therefore in Table 2 the δ_2 is 1 if the characteristic of the field is 2, otherwise it is zero. Usually, an orbit counter in characteristic 2 factors similarly to the corresponding one for the other characteristics, e. g. for $\emptyset_3$ we have*

$$6\cdot\delta_2+(u-5)(u-3)(u^3-13u^2+54u-66) = (u-4)(u-2)(u^3-15u^2+75u-123)$$

Since the matroids of rank 3 on less than 7 elements are all polynomially countable with polynomials independent of the characteristic of the field, the contribution of the non simple matroids to the counting polynomial of 3×7-matrices is also independent of the characteristic, and therefore also the contribution of all simple matroids (listed in Table 2) together, since the counting polynomial for all 3×7-matrices of rank 3 is independent of the characteristic, cf. Propsition 2.5. This amounts to saying that the differences of the general reduced matrix counters to the characteristic 2 ones multiplied by the orbit lengths in the last column of the table should add up to zero, because the multiplicities of the factor $u-1$ are the same in all relevant cases. But in fact, these product do not only add up to zero, but (for us unexpectedly) cancel in pairs (zeroes omitted):

$$[30, -210, 630, -840, -210, 210, 840, -630, 210, -30]$$

Concerning the individual orbit counters, the ones for $0, \emptyset_3, 2\emptyset_3, 2\{1\}_3$ were obtained via inclusion-exclusion, in all other bases directly so that at least the transversal there is uniformly enumerable. In the case of the uniform matroid 0, even for the inclusion-exclusion approach to work, one had to change the order of the coordinates for some of the simple systems, i. e. the investigated systems were probably not uniformly enumerable, but only enumerable, resulting in polynomially countable systems for the final result. Note, the last matroid corresponds to the projective plane over $\mathbb{F}_2$.

It is known, cf. [Wel 76] pg. 306, that there are 68 simple rank 3 matroids on 8 points, all listed in the supplement of [BCH 73]. Instead of going through

symbol cf. 5.3	$o_B(u)$ (orbit counter cf. 3.7)	$\|S_7\text{-orbit}\|$
0	$-30 \cdot \delta_2 + (u-3)(u-5)\cdot$ $(u^4 - 20u^3 + 148u^2 - 468u + 498)$	1
$\emptyset_3$	$6 \cdot \delta_2 + (u-5)(u-3)\cdot$ $(u^3 - 13u^2 + 54u - 66)$	35
$2\emptyset_3$	$(u-5)(u-2)(u-3)(u-4)$	70
$2\underline{1}_3$	$-2 \cdot \delta_2 + (u-3)(u^3 - 12u^2 + 46u - 54)$	315
$\emptyset_4$	$(u-5)(u-2)(u-3)(u-4)$	35
$\underline{1}_3 + \underline{1}_4$	$(u-2)(u-3)(u-4)$	420
$\underline{12}_3 + \underline{13}_3 + \underline{23}_3$	$\delta_2 + (u-3)(u^2 - 7u + 11)$	840
$\emptyset_5$	$(u-2)(u-3)(u-4)$	21
$3\underline{1}_3$	$2 \cdot \delta_2 + (u-3)^2(u-4),$	105
$\emptyset_3 + \emptyset_4$	$(u-3)(u-2)^2$	35
$\underline{1}_3 + \underline{2}_3 + \underline{12}_3$	$(u-4)(u-3)(u-2)$	630
$\underline{124}_3 + \underline{135}_3 +$ $\underline{236}_3 + \underline{456}_3$	$-\delta_2 + (u-3)^2$	210
$\underline{1}_3 + \underline{1}_5$	$(u-2)(u-3)$	105
$\underline{12}_3 + \underline{13}_3 + \underline{23}_4$	$(u-3)(u-2)$	1260
$\underline{1}_4 + \underline{1}_4$	$(u-2)^2$	70
$\emptyset_6$	$(u-2)(u-3)(u-4)$	7
$\underline{12}_3 + \underline{13}_3 +$ $\underline{14}_3 + \underline{234}_3$	$-\delta_2 + (u-3)^2$	840
$\underline{23}_3 + \underline{45}_3 +$ $\underline{124}_3 + \underline{135}_3$	$(u-3)(u-2)$	1260
$\underline{124}_4 + \underline{136}_3 +$ $\underline{256}_3 + \underline{345}_3$	$(u-2)(u-3)$	840
$\underline{12}_3 + \underline{135}_3 + \underline{146}_3 +$ $\underline{234}_3 + \underline{256}_3$	$\delta_2 + (u-3)$	630
$\underline{124}_3 + \underline{135}_3 + \underline{167}_3 +$ $\underline{236}_3 + \underline{457}_3$	$(u-2)$	420
$\underline{126}_3 + \underline{135}_3 + \underline{147}_3 +$ $\underline{237}_3 + \underline{245}_3 + \underline{346}_3$	$-\delta_2 + 1$	210
$\underline{126}_3 + \underline{135}_3 + \underline{147}_3 +$ $\underline{237}_3 + \underline{245}_3 + \underline{346}_3 +$ $\underline{567}_3$	δ_2	30

Table 2: Orbit counters for simple rank 3-matroids on 7 points, cf. Example 5.8, where $\{i,j,k\}$ in the symbol is abbreviated as $\underline{ijk}$.

all possibilities, we only give two examples demonstrating phenomena not yet occurring in the case of $|E| = 7$ points.

Example 5.9. *Let $|E| = 8$, i. e. we consider some examples of rank 3 matroids on 8 points.*
1.) The matroid $B := \{1,2\}_3 + \{1,4\}_3 + \{2,3\}_3 + \{3,4\}_3$ gives rise to a system $S_T(\{1,2,3\}, B)$ for a suitable rigidity frame T, cf. proof of Proposition 3.7, saying that all the 3×3-minors of the matrix

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

which do not vanish identically in the four variables are not equal to zero. The system is too big to be treated directly so that one has to use the inclusion-exclusion count. In doing that it turns out that at characteristic 2 one has a different behaviour, but otherwise all simple system coming up are split, except for one, which is only quasisplit in the sense of [Ple 09b]:

$$x_{3,5} - x_{2,2} = 0, x_{2,3} - x_{2,2} = 0, x_{3,4} - x_{2,2} = 0, x_{2,2}^2 - x_{2,2} + 1 = 0,$$

i. e. becomes split after a suitable finite field extension. The counting polynomial for the whole system is

$$c(u) := u^4 - 16u^3 + 93u^2 - 231u + 208.$$

Now the interpretation is slightly more complicated: If the field in question does not contain a primitive sixth root of unity, the number of solutions (or rather the counting polynomial for these solutions) is $c(u) - 2$. If it contains a primitive sixth root of unity and the characteristic is not (2 or) 3, then it is $c(u)$ as it stands. If the characteristic is 3, then it is clearly $c(u) - 1 = (u-3)(u^3 - 13u^2 + 54u - 69)$, since $x_{2,2}^2 - x_{2,2} + 1$ has a double root then. Finally the case of characteristic 2 has to be treated separately in the same manner. One obtains the counting polynomial $c(u) - 4$, which is correct if the ground field contains a primitive third root of unity and $c(u) - 6$ if not. Of course more complicated systems which cannot be decomposed into quasisplit systems sooner or later come in abundance.

2.) The matroid $2\{1\}_3 + \{1\}_4$ has the orbit counter $o_B(u) = (u-5)(u-3)(u-4)^2$ in every characteristic $\neq 2$ and in characteristi 2 it has $(u-2)(u-4)(u^2 - 10u + 27)$ as orbit counter, both obtainable via the inclusion exclusion count. The difference of the two is $-6u + 24$, which is no longer a constant like in the matroids on 7 points.

3.) Here is a list of isomorphism classes of the rigid rank 3 matroids on 8 points:

a) $\{1,2,4\}_3+\{1,3,7\}_4+\{1,5,6\}_3+\{2,3,5\}_3+\{2,6,7\}_3+\{3,4,6\}_3+\{4,5,7\}_3$ *in characteristic 2 (length of orbit under S_8 is 1680).*
b) $\{1,2,4\}_3+\{1,5,6\}_3+\{2,3,5\}_3+\{2,6,7\}_3+\{3,4,6\}_3+\{4,5,8\}_3+\{1,3,7,8\}_4$ *in any characteristic (length of orbit under S_8 is 5040).*
c) $\{1,2,4\}_3+\{1,3,7\}_3+\{1,6,8\}_3+\{2,3,8\}_3+\{2,5,6\}_3+\{3,4,5\}_3+\{4,6,7\}_3+\{5,7,8\}_3$ *in characteristic 3.*
The last matroid is not rigid in in characteristics $\neq 3$: In characteristic 2 one has no solutions and in characteristics $\neq 2,3$ one has 2 or 0 solutions, depending on whether x^2-x+1 does or does not split over the ground field, similarly to part 1) of this example. One is tempted to call this situation Galois*-rigid, since the* Galois *group acts transitively on the solutions. (Length of orbit under S_8 is 840.)*

References

[Aig 79] Aigner, M., *Combinatorial Theory.* Springer, 1979.

[Ath 96] Athanasiadis, C. A. *Characteristic polynomials of subspace arrangements and finite fields.* Adv. Math. 122 (1996), no. 2, 193–233.

[BGLR 11] Bächler, T., Gerdt, V., Lange-Hegermann, M., Robertz, D., *Algorithmic Thomas decomposition of algebraic and differential systems*, Journal of Symbolic Computation, Available online 24 December 2011, ISSN 0747-7171, 10.1016/j.jsc.2011.12.043. (`http://www.sciencedirect.com/science/article/pii/S074771711100246X`)

[BLH 13] Bächler, T., Lange-Hegermann, M., 2008-2013. AlgebraicThomas and DifferentialThomas: Thomas Decomposition for algebraic and differential systems. (`http://wwwb.math.rwth-aachen.de/thomasdecomposition/`).

[BCH 73] Blackburn, J. E.; Crapo, H. H.; Higgs, D. A. *A catalogue of combinatorial geometries.* Math. Comp. 27 (1973), 155–166; addendum, ibid. 27 (1973), no. 121, loose microfiche suppl. A12–G12.

[Bri 02] Britz, T., *MacWilliams identities and matroid polynomials.* Electron. J. Combin. 9 (2002), no. 1, Research Paper 19, 16 pp.

[CrR 70] Crapo, H. H.; Rota, G.-C. *On the foundations of combinatorial theory: Combinatorial geometries.* Preliminary edition. The M.I.T. Press, Cambridge, Mass.-London, 1970. iv+289.

[GAP] The GAP Group, *GAP - Groups, Algorithms, Programming - a System for Computational Discrete Algebra* (`http://www.gap-system.org/`).

[Gre 76] Greene, C. *Weight enumeration and the geometry of linear codes.* Studies in Appl. Math. 55 (1976), no. 2, 119–128.

[ISS 95] Iampolskaia, A. V., Skorobogatov, A. N., Sorokin, E. A., *Formula for the number of [9,3] MDS codes.* Special issue on algebraic geometry codes. IEEE Trans. Inform. Theory 41 (1995), no. 6, part 1, 1667–1671.

[Jur 12] Jurrius, R.P.M.J.,*Codes, arrangements, matroids, and their polynomial links.* PhD thesis. Eindhoven University of Technology., (2012).

[JuP 13] Jurrius, R.P.M.J., Pellikaan, R., *Codes, arrangements and matroids.* in Series on Coding Theory and Cryptology vol. 8 Algebraic Geometry Modeling in Information Theory, E. Martinez-Moro Ed., pp. 219–325, World Scientific 2013.

[LMW 10] Li, Xiaoliang; Mou, Chenqi; Wang, Dongming *Decomposing polynomial sets into simple sets over finite fields: the zero-dimensional case.* Comput. Math. Appl. 60 (2010), no. 11, 2983–2997.

[Oxl 11] Oxley, James *Matroid theory.* Second edition. Oxford Graduate Texts in Mathematics, 21. Oxford University Press, Oxford, 2011. xiv+684 pp

[OrT 92] Orlik, P., Terao, H., *Arrangements of hyperplanes.* Springer 1992.

[Ple 09a] Plesken, W., *Counting solutions of polynomial systems via iterated fibrations.* Arch. Math. 92 (2009), no. 1, 44–56.

[Ple 09b] Plesken, W., *Gauss-Bruhat decomposition as an example of Thomas decomposition.* Arch. Math. 92 (2009), no. 2, 111–118.

[RoS 96] Rolland, R., Skorobogatov, A. N.,*Denombrement des configurations dans le plan projectif.* Arithmetic, geometry and coding theory (Luminy, 1993), 199–207, de Gruyter, Berlin, 1996.

[Sko 92] Skorobogatov, A. N., *Linear codes, strata of Grassmannians, and the problems of Segre.* Coding theory and algebraic geometry (Luminy, 1991), 210–223, Lecture Notes in Math., 1518, Springer, Berlin, 1992.

[Sko 96] Skorobogatov, A. N., *On the number of representations of matroids over finite fields.* Des. Codes Cryptogr. 9 (1996), no. 2, 215–226.

[Sta 07] Stanley, R. P., *An introduction to hyperplane arrangements.* Geometric combinatorics, 389–496, IAS/Park City Math. Ser., 13, Amer. Math. Soc., Providence, RI, 2007.

[Stu 93] Sturmfels, B., *Algorithmic Invariant Theory.* Springer 1993

[Tho 37] Thomas, J. M., *Differential Systems.* AMS Colloquium Publications vol XXI, 1937.

[Wel 76] Welsh, D. J. A. *Matroid theory.* L. M. S. Monographs, No. 8. Academic Press,London-New York, 1976.

Wilhelm Plesken
Lehrstuhl B für Mathematik
RWTH Aachen
Templergraben 64
52062 Aachen, Germany
plesken@momo.math.rwth-aachen.de

Thomas Bächler
Lehrstuhl B für Mathematik
RWTH Aachen
Templergraben 64
52062 Aachen, Germany
thomas@momo.math.rwth-aachen.de