arXiv:1701.06384v4 [math.CO] 22 Nov 2017

ALGEBRAIC MATROIDS AND FROBENIUS FLOCKS

GUUS P. BOLLEN, JAN DRAISMA, AND RUDI PENDAVINGH

Abstract. We show that each algebraic representation of a matroid M in positive characteristic determines a matroid valuation of M, which we have named the *Lindström valuation*. If this valuation is trivial, then a linear representation of M in characteristic p can be derived from the algebraic representation. Thus, so-called rigid matroids, which only admit trivial valuations, are algebraic in positive characteristic p if and only if they are linear in characteristic p.

To construct the Lindström valuation, we introduce new matroid representations called flocks, and show that each algebraic representation of a matroid induces flock representations.

1. Introduction

Several years before Whitney defined matroids in [23], Van der Waerden [22] recognized the commonality between algebraic and linear independence which is the defining property of matroids (see [18, Section 39.10b]). Today, linear matroids are the subject of some of the deepest theorems in combinatorics. By contrast, our understanding of *algebraic* matroids is much less advanced.

Algebraic matroids seem forebodingly hard to deal with, compared to linear matroids. Deciding if a matroid has a linear representation over a given field amounts to solving a system of polynomial equations over that field, which makes the linear representation problem decidable over algebraically closed fields (for the situation of representability over $\mathbb{Q}$, see [21]). We do not know of any procedure to decide if a matroid has an algebraic representation; for example, it is an open problem if the Tic-Tac-Toe matroid, a matroid of rank 5 on 9 elements, is algebraic [8]. It is possible to describe the set of all linear representations of a given matroid as being derived from a 'universal' matroid representation of that matroid over a partial field [16]. We tried to find a full set of invariants to classify (equivalence classes of) algebraic representations of the tiny uniform matroid $U_{2,3}$, and failed. Since algebraic representations appear so difficult to deal with in full detail, we are pleased to report that we found a nontrivial invariant of algebraic matroid representations in positive characteristic, taking inspiration in particular from the work of Lindström [13].

Throughout the paper, we use the language of algebraic geometry to describe matroid representations, and we work over an algebraically closed field K. An irreducible algebraic variety $X \subseteq K^E$ determines a matroid $M(X)$ with ground set E by declaring a set $I \subseteq E$ independent if the projection of X on K^I is dominant, that is, if the closure of $\{x_I : x \in X\}$ in the Zariski topology equals K^I. In the special case that X is a linear space, $M(X)$ is exactly the matroid represented by the columns of any matrix whose rows span X. We next translate results of Ingleton and Lindström to the language of algebraic geometry.

Ingleton argued that if K has characteristic 0, then for any sufficiently general point $x \in X$, the tangent space T_xX of X at x will have the same dominant projections as X itself, so that then $M(X) = M(T_xX)$. Since such a sufficiently general point always exists — it suffices that x avoids finitely many hypersurfaces in X — a matroid which has an algebraic representation over K also has a linear representation over K, in the form of a tangent space T_xX.

Ingletons argument does not generalize to fields K of positive characteristic p. Consider the variety $X = V(x_1 - x_2^p) = \{x \in K^2 : x_1 - x_2^p = 0\}$, which represents the matroid on $E = \{1, 2\}$ with independent sets $\emptyset, \{1\}, \{2\}$. The tangent space of X at any $x \in X$ is $T_xX = V(x_1)$, which represents a matroid in which $\{1\}$ is a dependent set. Thus, $M(X) \neq M(T_xX)$ for all $x \in X$.

Lindström demonstrated that for some varieties X this obstacle may be overcome by applying the Frobenius map $F : x \mapsto x^p$ to some of the coordinates, to derive varieties from X which

GPB is funded by a grant from Stichting Computer Algebra Nederland.
JD is partially funded by Vidi and Vici grants from the Netherlands Organisation for Scientific Research (NWO).

represent the same matroid. In case of the counterexample $X = V(x_1 - x_2^p)$ above, we could define $X' = \{(x_1, F(x_2)) : x \in X\}$. Then $M(X') = M(X)$, and $X' = V(x_1 - x_2)$, so that $M(X') = M(T_{x'}X')$ for some (in fact, all) $x' \in X'$. In general for an $X \subseteq K^E$, if we fix a vector $\alpha \in \mathbb{Z}^E$, put

$$\alpha x := (F^{-\alpha_i} x_i)_{i \in E} \text{ and } \alpha X := \{\alpha x : x \in X\},$$

then it can be argued that $M(\alpha X) = M(X)$. This gives additional options for finding a suitable tangent space.

Lindström showed in [13] that if X is any algebraic representation of the Fano matroid, then there necessarily exists an α so that $M(X) = M(T_\xi \alpha X)$ for a sufficiently general $\xi \in \alpha X$. Thus any algebraic representation of the Fano matroid spawns a linear representation in the same characteristic.

The choice of the matroid in Lindström's argument is not arbitrary. If we consider an algebraic representation X of the non-Fano matroid in characteristic 2, then there cannot be an $\alpha \in \mathbb{Z}^E$ so that in a sufficiently general point $\xi \in \alpha X$ we have $M(X) = M(T_\xi \alpha X)$: then the tangent space would be a linear representation of the non-Fano matroid in characteristic 2, which is not possible. Thus any attempt to balance out the Frobenius actions $\alpha \in \mathbb{Z}^E$ will be fruitless in this case.

In the present paper, we consider the overall structure of the map $\alpha \mapsto M(T_{\xi_\alpha} \alpha X)$, where for each α, ξ_α is the generic point of αX. A central result of this paper is that a sufficiently general $x \in X$ satisfies $M(T_{\alpha x} \alpha X) = M(T_{\xi_\alpha} \alpha X)$ for all $\alpha \in \mathbb{Z}^E$ (Theorem 38). This is nontrivial, as now x must *a priori* avoid countably many hypersurfaces, which one might think could cover all of X.

Fixing such a general x, the assignment $V : \alpha \mapsto V_\alpha := T_{\alpha x} \alpha X$ is what we have named a *Frobenius flock*: each V_α is a linear subspace of K^E of fixed dimension $\dim V_\alpha = \dim X =: d$, and moreover

(FF1) $V_\alpha / i = V_{\alpha + e_i} \backslash i$ for all $\alpha \in \mathbb{Z}^E$ and $i \in E$; and
(FF2) $V_{\alpha + \mathbf{1}} = \mathbf{1} V_\alpha$ for all $\alpha \in \mathbb{Z}^E$.

Here we wrote $W/i := \{w_{E-i} : w \in W, w_i = 0\}$ and $W \backslash i := \{w_{E-i} : w \in W\}$; $\mathbf{1}$ is the all-one vector and e_i is the i-th unit vector, with i-th coordinate 1 and 0 elsewhere.

In this paper, we are primarily concerned with properties of the matroids represented by the vector spaces V_α — in particular, we want to understand when there exists an $\alpha \in \mathbb{Z}^E$ so that $M(X) = M(V_\alpha)$. We will call an assignment $M : \alpha \mapsto M_\alpha$ of a matroid of rank d on E to each $\alpha \in \mathbb{Z}^E$ a *matroid flock* if it satisfies

(MF1) $M_\alpha / i = M_{\alpha + e_i} \backslash i$ for all $\alpha \in \mathbb{Z}^E$ and $i \in E$; and
(MF2) $M_\alpha = M_{\alpha + \mathbf{1}}$ for all $\alpha \in \mathbb{Z}^E$.

Clearly, any Frobenius flock V gives rise to a matroid flock by taking $M_\alpha = M(V_\alpha)$. In particular, each algebraic matroid representation $X \subseteq K^E$ gives rise to a matroid flock $M : \alpha \mapsto M(T_{\alpha x} \alpha X)$. This matroid flock does not depend on the choice of the very general point $x \in X$, since $M(T_{\alpha x} \alpha X) = M(T_{\alpha x'} \alpha X)$ for any two such very general points.

The matroid flock axioms (MF1), (MF2) may not appear to be very restrictive, but matroid flocks (and Frobenius flocks) are remarkably structured. For instance, while a matroid flock is *a priori* specified by an infinite amount of data, it follows from our work that a finite description always exists. More precisely, we show that for each matroid flock M there is a matroid valuation $\nu : \binom{E}{d} \to \mathbb{Z} \cup \{\infty\}$ in the sense of Dress and Wenzel [5], which conversely determines each M_α as follows: B is a basis of M_α if and only if

$$\sum_{i \in B} \alpha_i - \nu(B) \geq \sum_{i \in B'} \alpha_i - \nu(B')$$

for all $B' \in \binom{E}{d}$ (Theorem 7).

In case the matroid flock M derives from an algebraic representation X, this valuation ν gives us the overview over the matroids $M(T_{\alpha x} \alpha X)$ we sought. In particular, we have $M(X) = M_\alpha = M(T_{\alpha x} \alpha X)$ if and only if $\nu(B) = \sum_{i \in B} \alpha_i$ for all bases B of $M(X)$, i.e. if ν is a *trivial* valuation. Recognizing the seminal work of Bernt Lindström, we named ν the *Lindström valuation* of X.

Dress and Wenzel call a matroid *rigid* if it supports trivial valuations only; and so we obtain a main result of this paper, that if a matroid M is rigid, then M is algebraic in characteristic p if and only if M is linear in characteristic p (Theorem 47).

In summary, we find that an irreducible variety $X \subseteq K^E$ not only determines a matroid $M(X)$, but also a valuation of that matroid. This reminds of the way a matrix A over a valuated field (K, val) not only determines a linear matroid $M(A)$, but also a valuation $\nu : B \mapsto \mathrm{val}(\det(A_B))$ of $M(A)$. We will demonstrate that the valuated matroids obtained from algebraic representations in characteristic p include all the valuated matroids obtained from linear representations over the valuated field $(\mathbb{Q}, \mathrm{val}_p)$.

It is an open problem to characterize the valuated matroids which may arise from algebraic representations in characteristic p.

Acknowledgement. We thank Josephine Yu for identifying the lifting functions associated with alcoved polytopes. Her answer to our query led us to conjecture what became Theorem 7 below.

2. Preliminaries

2.1. **Matroids.** A *matroid* is a pair $(E, \mathcal{B})$ where E is a finite set and $\mathcal{B} \subseteq 2^E$ is a set satisfying

(B1) $\mathcal{B} \neq \emptyset$; and
(B2) for all $B, B' \in \mathcal{B}$ and $i \in B \setminus B'$, there exists a $j \in B' \setminus B$ so that both $B - i + j \in \mathcal{B}$ and $B' + i - j \in \mathcal{B}$.

Here we used the shorthand $B - i + j := (B \cup \{j\}) \setminus \{i\}$. The set E is the *ground set* of the matroid $M = (E, \mathcal{B})$, and we call the elements $B \in \mathcal{B}$ the *bases* of M. We refer to Oxley [15] for standard definitions and results in matroid theory. We summarize a few notions which are used in this paper below.

If $M = (E, \mathcal{B})$ is a matroid, then a set $I \subseteq E$ is *independent* if $I \subseteq B$ for some basis B of M. The independent sets of a matroid satisfy the following *independence axioms*:

(I1) $\emptyset$ is independent;
(I2) if I is independent and $J \subseteq I$, then J is independent; and
(I3) if I and J are independent and $|I| < |J|$, then there exists a $j \in J \setminus I$ so that $I + j$ is independent.

A basis of a matroid may be characterized as an inclusionwise maximal independent set, and the independence axioms (I1), (I2), (I3) then imply the basis axioms (B1) and (B2). The independence axioms thus constitute an alternative definition of matroids.

The *rank function* of a matroid $M = (E, \mathcal{B})$ is the function $r_M : 2^E \to \mathbb{N}$ determined by

$$r_M(J) := \max\{|J \cap B| : B \in \mathcal{B}\}$$

for each $J \subseteq E$. We have $B \in \mathcal{B}$ if and only if $|B| = r_M(B) = r_M(E)$, and so (E, r_M) fully determines M. We will write $r(M) := r_M(E)$ for the rank of the entire matroid. Given $I \subseteq E$, $M \backslash I$ is the matroid on ground set $E \backslash I$ with rank function $r_{M\backslash I} : J \mapsto r_M(J)$, and M/I is the matroid on $E \backslash I$ with rank function $r_{M/I} : J \mapsto r_M(I \cup J) - r_M(I)$.

The *connectivity function* of a matroid $M = (E, \mathcal{I})$ is the function $\lambda_M : 2^E \to \mathbb{N}$ determined by

$$\lambda_M(J) := r_M(J) + r_M(\overline{J}) - r_M(E)$$

for each $J \subseteq E$. Here and henceforth we denote $\overline{J} := E \backslash J$, where E is the ground set.

2.2. **Linear spaces and linear matroids.** Let K be a field and let E be a finite set. If $w \in K^E$, and $I \subseteq E$, then $w_I \in K^I$ is the restriction of w to I. For a linear subspace $W \subseteq K^E$ and a set $I \subseteq E$, we define

$$W \backslash I := \{w_{\overline{I}} : w \in W\} \text{ and } W/I := \{w_{\overline{I}} : w \in W, w_I = 0\}$$

Let $r_W : 2^E \to \mathbb{N}$ be the function determined by $r_W(I) := \dim(W \backslash \overline{I})$. The following is well known.

Lemma 1. *Let K be a field, let E be a finite set, and let $W \subseteq K^E$ be a linear subspace. Then r_W is the rank function of a matroid on E.*

We write $M(W)$ for the matroid on E with rank function r_W. Taking minors of $M(W)$ commutes with taking 'minors' of W: for each $I \subseteq E$, we have $M(W)\backslash I = M(W\backslash I)$, and $M(W)/I = M(W/I)$.

If $M = M(W)$, then $\lambda_M(I) = 0$ exactly if

$$\dim W = r_M(E) = r_M(\overline{I}) + r_M(I) = \dim(W\backslash I) + \dim(W\backslash \overline{I}).$$

This is equivalent with $W = (W\backslash I) \times (W\backslash \overline{I})$.

2.3. **Matroid valuations.** For a finite set E and a natural number d, we write

$$\binom{E}{d} := \{J \subseteq E : |J| = d\},$$

and we will abbreviate $\mathbb{R}_\infty := \mathbb{R} \cup \{\infty\}$ and $\mathbb{Z}_\infty := \mathbb{Z} \cup \{\infty\}$. A *matroid valuation* is a function $\nu : \binom{E}{d} \to \mathbb{R}_\infty$, such that

(V1) there is a $B \in \binom{E}{d}$ so that $\nu(B) < \infty$; and

(V2) for all $B, B' \in \binom{E}{d}$ and $i \in B \setminus B'$, there exists a $j \in B' \setminus B$ so that

$$\nu(B) + \nu(B') \geq \nu(B - i + j) + \nu(B' + i - j).$$

Matroid valuations were introduced by Dress and Wenzel in [5]. For any valuation ν, the set

$$\mathcal{B}^\nu := \left\{ B \in \binom{E}{d} : \nu(B) < \infty \right\}$$

satisfies the matroid basis axioms (B1) and (B2), so that $M^\nu := (E, \mathcal{B}^\nu)$ is a matroid, the *support matroid* of ν. If $N = M^\nu$, then we also say that ν is a valuation of N.

2.4. **Murota's discrete duality theory.** We briefly review the definitions and results we use from [14]. For an $x \in \mathbb{Z}^n$, let

$$\mathrm{supp}(x) := \{i : x_i \neq 0\},\ \mathrm{supp}^+(x) := \{i : x_i > 0\},\ \mathrm{supp}^-(x) := \{i : x_i < 0\}.$$

For any function $f : \mathbb{Z}^n \to \mathbb{R}_\infty$, we write $\mathrm{dom}(f) := \{x \in \mathbb{Z}^n : f(x) \in \mathbb{R}\}$. We write e_i for the i-th unit vector, with i-th coordinate 1 and 0 elsewhere.

Definition 2. *A function $f : \mathbb{Z}^n \to \mathbb{Z}_\infty$ is called* M-convex *if:*

1. *$dom(f) \neq \emptyset$; and*
2. *for all $x, y \in dom(f)$ and $i \in supp^+(x - y)$, there exists $j \in supp^-(x - y)$ so that $f(x) + f(y) \geq f(x - e_i + e_j) + f(y + e_i - e_j)$.*

Let $x, y \in \mathbb{Z}^n$. We write $x \vee y := (\max\{x_i, y_i\})_i$ and $x \wedge y := (\min\{x_i, y_i\})_i$, and let $\mathbf{1}$ denote the all-one vector.

Definition 3. *A function $g : \mathbb{Z}^n \to \mathbb{Z}_\infty$ is* L-convex *if*

1. *$dom(g) \neq \emptyset$;*
2. *$g(x) + g(y) \geq g(x \vee y) + g(x \wedge y)$ for all $x, y \in \mathbb{Z}^n$; and*
3. *there exists an $r \in \mathbb{Z}$ so that $g(x + \mathbf{1}) = g(x) + r$ for all $x \in \mathbb{Z}^n$.*

For any $h : \mathbb{Z}^n \to \mathbb{Z}_\infty$ with nonempty domain, the *Legendre-Fenchel dual* is the function $h^\bullet : \mathbb{Z}^n \to \mathbb{Z}_\infty$ defined by

$$h^\bullet(x) = \sup\{x^T y - h(y) : y \in \mathbb{Z}^n\}.$$

The following key theorem describes the duality of M-convex and L-convex functions [14].

Theorem 4. *Let $f, g : \mathbb{Z}^n \to \mathbb{Z}_\infty$. The following are equivalent.*

1. *f is M-convex, and $g = f^\bullet$; and*
2. *g is L-convex, and $f = g^\bullet$.*

Finally, Murota provides the following local optimality criterion for L-convex functions. Let $e_I := \sum_{i \in I} e_i$ for any $I \subseteq \{1, \ldots, n\}$, and let $\mathbf{1}$ denote the all-one vector.

Lemma 5. *(Murota [14], 7.14) Let G be an L-convex function on $\mathbb{Z}^n$, and let $x \in \mathbb{Z}^n$. Then*

$$\forall y \in \mathbb{Z}^n : G(x) \leq G(y) \iff \begin{cases} \forall I \subset \{1, \ldots, n\} : G(x) \leq G(x + e_I), \\ G(x) = G(x + \mathbf{1}). \end{cases}$$

3. Matroid flocks

A *matroid flock of rank d on E* is a map M which assigns a matroid M_α on E of rank d to each $\alpha \in \mathbb{Z}^E$, satisfying the following two axioms.

(MF1) $M_\alpha/i = M_{\alpha+e_i}\backslash i$ for all $\alpha \in \mathbb{Z}^E$ and $i \in E$.

(MF2) $M_\alpha = M_{\alpha+\mathbf{1}}$ for all $\alpha \in \mathbb{Z}^E$.

Example 6. *Let $E = \{1, 2\}$ and let M_0 be the matroid on E with bases $\{1\}$ and $\{2\}$. We claim that this extends in a unique manner to a matroid flock M on E of rank 1. Indeed, by (MF1) the rank-zero matroid $M_0/1$ equals $M_{e_1}\backslash 1$, so that $\{1\}$ is the only basis in M_{e_1}. Repeating this argument, we find $M_{ke_1} = M_{e_1}$ for all $k > 0$. Similarly, M_{ke_2} is the matroid with only one basis $\{2\}$ for all $k > 0$. Using (MF2) this determines M_α for all $\alpha = (k, l)$: it equals M_0 if $k = l$, M_{e_1} if $k > l$, and M_{e_2} if $k < l$. The phenomenon that most M_α follow from a small number of them, like migrating birds follow a small number of leaders, inspired our term* matroid flock. ♣

For a matroid valuation $\nu : \binom{E}{d} \to \mathbb{R}_\infty$ and an $\alpha \in \mathbb{R}^E$, let

$$\mathcal{B}^\nu_\alpha := \left\{ B \in \binom{E}{d} : e_B^T\alpha - \nu(B) = g^\nu(\alpha) \right\}, \text{ where } g^\nu(\alpha) = \sup\left\{ e_{B'}^T\alpha - \nu(B') : B' \in \binom{E}{d} \right\}$$

and put $M^\nu_\alpha := (E, \mathcal{B}^\nu_\alpha)$.

The main result of this section will be the following characterization of matroid flocks.

Theorem 7. *Let E be a finite set, let $d \in \mathbb{N}$, and let M_α be a matroid on E of rank d for each $\alpha \in \mathbb{Z}^E$. The following are equivalent:*

1. *$M : \alpha \mapsto M_\alpha$ is a matroid flock; and*
2. *there is a matroid valuation $\nu : \binom{E}{d} \to \mathbb{Z}_\infty$ so that $M_\alpha = M^\nu_\alpha$ for all $\alpha \in \mathbb{Z}^E$.*

In what follows, we will first prove this characterization, and then derive a few facts about matroid flocks which will be used later in the paper.

3.1. The characterization of matroid flocks.

The implication (2)⇒(1) of Theorem 7 is relatively straightforward.

Lemma 8. *Let $\nu : \binom{E}{d} \to \mathbb{Z}_\infty$ be a valuation. Then*

1. *$M^\nu_\alpha/i = M^\nu_{\alpha+e_i}\backslash i$ for all $\alpha \in \mathbb{Z}^E$ and $i \in E$; and*
2. *$M^\nu_\alpha = M^\nu_{\alpha+\mathbf{1}}$ for all $\alpha \in \mathbb{Z}^E$.*

Proof. We prove (1). Consider $\alpha \in \mathbb{Z}^E$ and $i \in E$. If i is a loop of M^ν_α, then $g^\nu(\alpha + e_i) = g^\nu(\alpha)$. Then B is a basis of M^ν_α/i if and only if

$$e_B^T(\alpha + e_i) - \nu(B) = e_B^T\alpha - \nu(B) = g^\nu(\alpha) = g^\nu(\alpha + e_i)$$

if and only if B is a basis of $M^\nu_{\alpha+e_i}\backslash i$. On the other hand, if i is not a loop of M^ν_α, then $g^\nu(\alpha + e_i) = g^\nu(\alpha) + 1$, and then B' is a basis of M^ν_α/i if and only if $B = B' + i$ is a basis of M^ν_α, if and only if

$$e_B^T(\alpha + e_i) - \nu(B) = e_B^T\alpha - \nu(B) + 1 = g(\alpha) + 1 = g(\alpha + e_i)$$

if and only if B' is a basis of $M^\nu_{\alpha+e_i}\backslash i$.

To see (2), note that $g^\nu(\alpha + \mathbf{1}) = g^\nu(\alpha) + d$. Then B is a basis of M^ν_α if and only if

$$e_B^T(\alpha + \mathbf{1}) - \nu(B) = e_B^T\alpha - \nu(B) + d = g^\nu(\alpha) + d = g^\nu(\alpha + \mathbf{1})$$

if and only if B is a basis of $M^\nu_{\alpha+\mathbf{1}}$. □

We show the implication (1)⇒(2) of Theorem 7. Our proof makes essential use of the discrete duality theory of Murota [14]. Specifically, we will first construct an L-convex function $g : \mathbb{Z}^E \to \mathbb{Z}$ from the matroid flock M. The Fenchel dual f of g is then an M-convex function, from which we derive the required valuation ν. Before we can prove the existence of a suitable function g, we need a few technical lemmas.

In the context of a matroid flock M, we will write r_α for the rank function of the matroid M_α. We first extend (MF1).

Lemma 9. *Let M be a matroid flock on E, let $\alpha \in \mathbb{Z}^E$ and let $I \subseteq E$. Then $M_\alpha / I = M_{\alpha+e_I} \backslash I$.*

Proof. By induction on I. Clearly the lemma holds if $I = \emptyset$. If $I \neq \emptyset$, pick any $i \in I$. Using the induction hypothesis for α and $I - i$, followed by (MF1) for $\alpha + e_{I-i}$ and i, we have

$$M_\alpha/I = M_\alpha/(I-i)/i = M_{\alpha+e_{I-i}}\backslash(I-i)/i = M_{\alpha+e_{I-i}}/i\backslash(I-i) = M_{\alpha+e_I}\backslash i\backslash(I-i) = M_{\alpha+e_I}\backslash I,$$

as required. □

Lemma 10. *Let M be a matroid flock on E, let $\alpha \in \mathbb{Z}^E$ and let $I \subseteq J \subseteq E$. Then*

$$r_\alpha(J) = r_\alpha(I) + r_{\alpha+e_I}(J\backslash I).$$

Proof. Using Lemma 9, we have $r_{\alpha+e_I}(J\backslash I) = r(M_{\alpha+e_I}\backslash I\backslash \overline{J}) = r(M_\alpha/I\backslash\overline{J}) = r_\alpha(J) - r_\alpha(I)$, as required. □

If $\alpha, \beta \in \mathbb{R}^E$, we write $\alpha \leq \beta$ if $\alpha_i \leq \beta_i$ for all $i \in E$.

Lemma 11. *Let M be a matroid flock on E, let $\alpha, \beta \in \mathbb{Z}^E$ and let $I \subseteq E$. If $I \cap supp(\beta - \alpha) = \emptyset$ and $\alpha \leq \beta$, then $r_\alpha(I) \geq r_\beta(I)$.*

Proof. We use induction on $\max_i(\beta_i - \alpha_i)$. Let $J := \text{supp}(\beta - \alpha)$. Then

$$r_\alpha(I) = r(M_\alpha\backslash J\backslash\overline{I \cup J}) \geq r(M_\alpha/J\backslash\overline{I\cup J}) = r(M_{\alpha+e_J}\backslash J\backslash\overline{I\cup J}) = r_{\alpha+e_J}(I).$$

Taking $\alpha' := \alpha + e_J$, we have $\alpha' \leq \beta$, $\max_i(\beta_i - \alpha'_i) < \max_i(\beta_i - \alpha_i)$ and $\text{supp}(\beta - \alpha') \subseteq \text{supp}(\beta - \alpha)$. Hence

$$r_\alpha(I) \geq r_{\alpha+e_J}(I) \geq r_\beta(I),$$

by using the induction hypothesis for α', β. □

We are now ready to show the existence of the function g alluded to above.

Lemma 12. *Let M be a matroid flock on E. There is a unique function $g : \mathbb{Z}^E \to \mathbb{Z}$ so that*

(1) *$g(0) = 0$, and*
(2) *$g(\alpha + e_I) = g(\alpha) + r_\alpha(I)$ for all $\alpha \in \mathbb{Z}^E$ and $I \subseteq E$.*

Proof. Let $D = (\mathbb{Z}^E, A)$ be the infinite directed graph with arcs

$$A := \{(\alpha, \alpha + e_I) : \ \alpha \in \mathbb{Z}^E, \ \emptyset \neq I \subseteq E\}.$$

Let $l : A \to \mathbb{Z}$ be a length function on the arcs determined by $l(\alpha, \alpha + e_I) = r_\alpha(I)$. This length function extends to the undirected walks $W = (\alpha^0, \ldots, \alpha^k)$ of D in the usual way, by setting

$$l(W) := \begin{cases} l(\alpha^0, \ldots, \alpha^{k-1}) + l(\alpha^{k-1}, \alpha^k) & \text{if } (\alpha^{k-1}, \alpha^k) \in A \\ l(\alpha^0, \ldots, \alpha^{k-1}) - l(\alpha^k, \alpha^{k-1}) & \text{if } (\alpha^k, \alpha^{k-1}) \in A \end{cases}$$

if $k > 0$, and $l(W) = 0$ otherwise. A walk $(\alpha^0, \ldots, \alpha^k)$ is *closed* if it starts and ends in the same vertex, i.e. if $\alpha^0 = \alpha^k$.

If we assume that $l(W) = 0$ for each closed walk W, then we can construct a function g satisfying (1) and (2) as follows. For each $\alpha \in \mathbb{Z}^E$, let W^α be an arbitrary walk from 0 to α, and put $g(\alpha) = l(W^\alpha)$. Then $g(0) = l(W^0) = 0$ by our assumption, since W^0 is a walk from 0 to 0. Also, if $\alpha \in \mathbb{Z}^E$ and $I \subseteq E$, then writing $\beta := \alpha + e_I$ we have

$$l(W^\alpha) + l(\alpha, \beta) - l(W^\beta) = l(\alpha^0, \ldots, \alpha^k, \beta^m, \ldots, \beta^0) = 0,$$

by our assumption, where $W^\alpha = (\alpha^0, \ldots, \alpha^k)$ and $W^\beta = (\beta^0, \ldots, \beta^m)$. It follows that

$$g(\alpha + e_I) = l(W^\beta) = l(W^\alpha) + l(\alpha, \beta) = g(\alpha) + r_\alpha(I),$$

as required. So to prove the lemma, it will suffice to show that $l(W) = 0$ for each closed walk W.

Suppose for a contradiction that $W = (\alpha^0, \ldots, \alpha^k)$ is a closed walk with $l(W) \neq 0$. Fix any $i \in E$ so that $\alpha_i^0 \neq \alpha_i^1$. If $J \subseteq E$ is such that $i \in J$, then for any $\alpha \in \mathbb{Z}^E$ we have

$$l(\alpha, \alpha + e_J) = r_\alpha(J) = r_\alpha(i) + r_{\alpha+e_i}(J - i) = l(\alpha, \alpha + e_i, \alpha + e_J) \tag{1}$$

by applying Lemma 10 with $I = \{i\}$. Hence, if we replace each subsequence $(\alpha^{t-1}, \alpha^t) = (\alpha, \alpha + e_J)$ of W with $i \in J$ by $(\alpha, \alpha + e_i, \alpha + e_J)$, and each subsequence $(\alpha^{t-1}, \alpha^t) = (\alpha + e_J, \alpha)$ with $i \in J$ by

$(\alpha+e_J, \alpha+e_i, \alpha)$, then we obtain a closed walk $U = (\beta^0, \dots, \beta^m)$ with $l(U) = l(W) \neq 0$, such that if $\beta^t - \beta^{t-1} = \pm e_J$, then $i \notin J$ or $J = \{i\}$, and moreover such that $\beta^t - \beta^{t-1} = \pm e_i$ for some t. Pick such U, i with m as small as possible, and minimizing $|U|_i := \sum\{t \in \{1, \dots, m\} : \beta^t_i \neq \beta^{t-1}_i\}$.

We claim that there is no $t > 0$ so that $\beta^{t-1}_i = \beta^t_i \neq \beta^{t+1}_i$. Consider that by applying Lemma 10 with $I = J - i$, we have

$$l(\alpha, \alpha + e_J) = r_\alpha(J) = r_\alpha(J - i) + r_{\alpha+e_{J-i}}(i) = l(\alpha, \alpha + e_{J-i}, \alpha + e_J), \tag{2}$$

so that using (1) we obtain $l(\alpha, \alpha + e_{J-i}, \alpha + e_J, \alpha + e_i, \alpha) = 0$. Hence, $l(\alpha, \alpha + e_{J-i}, \alpha + e_J) = l(\alpha, \alpha + e_i, \alpha + e_J)$ and $l(\alpha + e_{J-i}, \alpha, \alpha + e_i) = l(\alpha + e_{J-i}, \alpha + e_J, \alpha + e_i)$. It follows that any subsequence $(\beta^{t-1}, \beta^t, \beta^{t+1})$ of U with $\beta^{t-1}_i = \beta^t_i \neq \beta^{t+1}_i$ can be rerouted to $(\beta^{t-1}, \beta', \beta^{t+1})$ with $\beta^{t-1}_i \neq \beta'_i = \beta^{t+1}_i$, which would result in a closed walk U' with $|U'|_i < |U|_i$, a contradiction.

So there exists an $m' \in \{1, \dots, m\}$ such that $\beta^t - \beta^{t-1} = \pm e_i$ if and only if $t \leq m'$. Then $\beta^0 = \beta^{m'} = \beta^m$, and $l(\beta^0, \dots, \beta^{m'}) = 0$. Hence

$$l(\beta^{m'}, \dots, \beta^m) = l(\beta^0, \dots, \beta^{m'}) + l(\beta^{m'}, \dots, \beta^m) = l(U) \neq 0,$$

which contradicts the minimality of m. □

For any matroid flock M, let g^M denote the unique function g from Lemma 12.

Theorem 13. *Let M be a matroid flock of rank d on E, and let $g = g^M$. Then*

(1) $g(\alpha) + g(\beta) \geq g(\alpha \vee \beta) + g(\alpha \wedge \beta)$ *for all* $\alpha, \beta \in \mathbb{Z}^E$*; and*
(2) $g(\alpha + \mathbf{1}) = g(\alpha) + d$ *for all* $\alpha \in \mathbb{Z}^E$.

Proof. We first show (1). Let $\alpha, \beta \in \mathbb{Z}^E$. Since $(\beta - \alpha) \vee 0 \geq 0$, there are $I_1 \subseteq \dots \subseteq I_k \subseteq E$ so that $(\beta - \alpha) \vee 0 = \sum_{j=1}^k e_{I_j}$. Let $\gamma(t) := \alpha \wedge \beta + \sum_{j=1}^t e_{I_j}$. Then $\gamma(0) = \alpha \wedge \beta$, $\gamma(k) = \alpha \wedge \beta + (\beta - \alpha) \vee 0 = \beta$, and $\gamma(t) = \gamma(t-1) + e_{I_t}$, so that

$$g(\beta) - g(\alpha \wedge \beta) = \sum_{t=1}^k g(\gamma(t)) - g(\gamma(t-1)) = \sum_{t=1}^k r_{\gamma(t-1)}(I_t).$$

Let $\delta := (\alpha - \beta) \vee 0$. Then $\gamma(0) + \delta = \alpha$ and $\gamma(k) + \delta = \alpha \vee \beta$, and we also have

$$g(\alpha \vee \beta) - g(\alpha) = \sum_{t=1}^k g(\gamma(t) + \delta) - g(\gamma(t-1) + \delta) = \sum_{t=1}^k r_{\gamma(t-1)+\delta}(I_t).$$

For each t we have $I_t \cap \mathrm{supp}(\delta) \subseteq \mathrm{supp}((\beta - \alpha) \vee 0) \cap \mathrm{supp}((\alpha - \beta) \vee 0) = \emptyset$, and $\delta \geq 0$. By Lemma 11, it follows that $r_{\gamma(t-1)}(I_t) \geq r_{\gamma(t-1)+\delta}(I_t)$ for each t, and hence

$$g(\beta) - g(\alpha \wedge \beta) = \sum_{t=1}^k r_{\gamma(t)}(I_t) \geq \sum_{t=1}^k r_{\gamma(t)+\delta}(I_t) = g(\alpha \vee \beta) - g(\alpha),$$

which implies (1).

To see (2), note that $g(\alpha + \mathbf{1}) = g(\alpha) + r_\alpha(E) = g(\alpha) + d$. □

It follows that for any matroid flock M, the function g^M is L-convex in the sense of Murota.

Lemma 14. *Let M be a matroid flock on E, let $g = g^M$ and $f := g^\bullet$, and let $\alpha, \omega \in \mathbb{Z}^E$. The following are equivalent.*

(1) $\omega^T \alpha = f(\omega) + g(\alpha)$*; and*
(2) $\omega = e_B$ *for some basis B of M_α.*

Proof. We first show that (1) implies (2). So assume that $\omega^T \alpha = f(\omega) + g(\alpha)$. Then $f(\omega)$ is finite, as $g(\alpha)$ and $\omega^T \alpha$ are both finite. Since $f = g^\bullet$, we have

$$\omega^T \alpha - g(\alpha) = f(\omega) = \sup\{\omega^T \beta - g(\beta) : \beta \in \mathbb{Z}^E\},$$

and hence α minimizes the function $G : \beta \mapsto g(\beta) - \omega^T \beta$ over all $\beta \in \mathbb{Z}^E$. Since

$$0 \leq G(\alpha - e_i) - G(\alpha) = g(\alpha - e_i) - \omega^T(\alpha - e_i) - g(\alpha) + \omega^T \alpha = -r_{\alpha - e_i}(i) + \omega_i$$

for each $i \in E$, it follows that $\omega \geq 0$. Since

$$0 \leq G(\alpha + e_i) - G(\alpha) = g(\alpha + e_i) - \omega^T(\alpha + e_i) - g(\alpha) + \omega^T\alpha = r_\alpha(i) - \omega_i,$$

we have $\omega \leq \mathbf{1}$. Hence $\omega = e_B$ for some $B \subseteq E$. Then

$$0 \leq G(\alpha + e_B) - G(\alpha) = g(\alpha + e_B) - \omega^T(\alpha + e_B) - g(\alpha) + \omega^T\alpha = r_\alpha(B) - |B|,$$

so that $r_\alpha(B) = |B|$. Moreover,

$$0 \leq G(\alpha - e_{\overline{B}}) - G(\alpha) = g(\alpha - e_{\overline{B}}) - \omega^T(\alpha - e_{\overline{B}}) - g(\alpha) + \omega^T\alpha = -r_{\alpha - e_{\overline{B}}}(\overline{B}),$$

so that $r_{\alpha - e_{\overline{B}}}(\overline{B}) = 0$. It follows by Lemma 9 that

$$|B| = r_\alpha(B) = r(M_\alpha \backslash \overline{B}) = r(M_{\alpha - e_{\overline{B}}} / \overline{B}) = d - r_{\alpha - e_{\overline{B}}}(\overline{B}) = d,$$

and hence that B is a basis of M_α.

We now show that (2) implies (1). Suppose $\omega = e_B$ for some basis B of M_α. Consider again the function $G : \alpha \mapsto g(\alpha) - \omega^T\alpha$ over $\mathbb{Z}^E$. As g is L-convex, G is L-convex. We show that α minimizes G over $\mathbb{Z}^E$, using the optimality condition for L-convex functions given in Lemma 5. First, note that as $g(\alpha + \mathbf{1}) = g(\alpha) + d$, we have

$$G(\alpha + \mathbf{1}) = g(\alpha + \mathbf{1}) - \omega^T(\alpha + \mathbf{1}) = g(\alpha) + d - \omega^T\alpha - |B| = G(\alpha).$$

Let $I \subseteq E$. As B is a basis of M_α, we have $|B \cap I| \leq r_\alpha(I)$, and hence

$$G(\alpha + e_I) - G(\alpha) = g(\alpha + e_I) - \omega^T(\alpha + e_I) - g(\alpha) - \omega^T\alpha = r_\alpha(I) - |B \cap I| \geq 0.$$

Thus α minimizes G over $\mathbb{Z}^E$, hence $f(\omega) = \sup\{-G(\alpha) : \alpha \in \mathbb{Z}^E\} = \omega^T\alpha - g(\alpha)$, as required. □

Let M be a matroid flock on E of rank d. We define the function $\nu^M : \binom{E}{d} \to \mathbb{Z}_\infty$ by setting $\nu^M(B) := f(e_B)$ for each $B \in \binom{E}{r}$, where $f = g^\bullet$ is the Lagrange-Fenchel dual of $g = g^M$.

Lemma 15. *Let M be a matroid flock, and let $\nu = \nu^M$. Then ν is a valuation, and $M^\nu_\alpha = M_\alpha$ for all $\alpha \in \mathbb{Z}^E$.*

Proof. Suppose M is a matroid flock. Then $g = g^M$ is L-convex by Theorem 13, and $f := g^\bullet$ is M-convex by Theorem 4. That $\nu : B \mapsto f(e_B)$ is a matroid valuation is straightforward from the fact that f is M-convex. We show that $M^\nu_\alpha = M_\alpha$ for all $\alpha \in \mathbb{Z}^E$. By Theorem 4, we have $g = f^\bullet$. By Lemma 14, we have

$$g(\alpha) = f^\bullet(\alpha) = \sup\{\omega^T\alpha - f(\omega) : \omega \in \mathbb{Z}^E\} = \sup\left\{e^T_{B'}\alpha - \nu(B') : B' \in \binom{E}{r}\right\},$$

as the first supremum is attained by ω only if $\omega = e_{B'}$ for some $B' \in \binom{E}{r}$. Again by Lemma 14, B is a basis of M_α if and only if $g(\alpha) = e^T_B\alpha - \nu(B)$, i.e. if B is a basis of M^ν_α. □

This proves the implication (1)⇒(2) of Theorem 7. Finally, we note:

Lemma 16. *Let M be a matroid flock, and let $\nu = \nu^M$. Then $g^M = g^\nu$.*

Proof. Let $f : \mathbb{Z}^E \to \mathbb{Z}_\infty$ be defined by $f(e_B) = \nu(B)$ for all $B \in \binom{E}{d}$, and $= \infty$ otherwise. Then $g^M = f^\bullet = g^\nu$, as required. □

3.2. **The support matroid and the cells of a matroid valuation.** If M is a matroid flock, then the *support matroid of M* is just the support matroid M^ν of the associated valuation $\nu = \nu^M$.

Lemma 17. *Suppose $M : \alpha \mapsto M_\alpha = (E, \mathcal{B}_\alpha)$ is a matroid flock with support matroid $N = (E, \mathcal{B})$. Then $\mathcal{B} = \bigcup_{\alpha \in \mathbb{Z}^E} \mathcal{B}_\alpha$.*

Proof. Let $\nu = \nu^M$, and put $g = g^\nu$. By Lemma 15, we have

$$\mathcal{B}_\alpha = \mathcal{B}^\nu_\alpha = \left\{B \in \binom{E}{d} : e^T_B\alpha - \nu(B) = g(\alpha)\right\}$$

for all $\alpha \in \mathbb{Z}^E$, and $\mathcal{B} = \{B \in \binom{E}{d} : \nu(B) < \infty\}$. Since $\nu(B') < \infty$ for some $B' \in \binom{E}{d}$ by (V1), we have $g(\alpha) > -\infty$ for all $\alpha \in \mathbb{Z}^E$. Consider a $B \in \binom{E}{d}$.

Suppose first that $B \in \mathcal{B}$, i.e. $\nu(B) < \infty$. Consider the difference $h(\alpha) := g(\alpha) - e_B^T\alpha + \nu(B)$. Then $h(\alpha)$ is nonnegative and finite for all $\alpha \in \mathbb{Z}^E$, and $B \in \mathcal{B}_\alpha$ if and only if $h(\alpha) = 0$. Moreover, if B is not a basis of M_α^ν, then $g(\alpha + e_B) \leq g(\alpha) + |B| - 1$ and $e_B^T(\alpha + e_B) = e_B^T\alpha + |B|$, so that $h(\alpha + e_B) \leq h(\alpha) - 1$. It follows that for any fixed α and any sufficiently large $k \in \mathbb{Z}$, we have $h(\alpha + ke_B) = 0$, and then $B \in \mathcal{B}_{\alpha+ke_B}$. Then $B \in \bigcup_{\alpha\in\mathbb{Z}^E} \mathcal{B}_\alpha$.

If on the other hand $B \notin \mathcal{B}^\nu$, i.e. $\nu(B) = \infty$, then $e_B^T\alpha - \nu(B) = -\infty < g(\alpha)$ for all $\alpha \in \mathbb{Z}^E$, so that $B \notin \mathcal{B}_\alpha$ for any $\alpha \in \mathbb{Z}^E$. Then $B \notin \bigcup_{\alpha\in\mathbb{Z}^E} \mathcal{B}_\alpha$. □

The geometry of valuations is quite intricate, and is studied in much greater detail in tropical geometry [20, 7]. We mention only a few results we need in this paper. For any matroid valuation $\nu : \binom{E}{d} \to \mathbb{R}_\infty$, put $C_\beta^\nu := \{\alpha \in \mathbb{R}^E : \mathcal{B}_\alpha^\nu \supseteq \mathcal{B}_\beta^\nu\}$.

Lemma 18. *Let $\nu : \binom{E}{d} \to \mathbb{Z}_\infty$ be a matroid valuation, and let $\beta \in \mathbb{R}^E$. Then*

$$C_\beta^\nu = \{\alpha \in \mathbb{R}^E : \alpha_i - \alpha_j \geq \nu(B) - \nu(B') \text{ for all } B \in \mathcal{B}_\beta^\nu,\ B' \in \mathcal{B}^\nu \text{ s.t. } B' = B - i + j\}.$$

Proof. Let C denote the right-hand side polyhedron in the statement of the lemma. Directly from the definition of $\mathcal{B}_\alpha^\nu$, it follows that $\mathcal{B}_\alpha^\nu \supseteq \mathcal{B}_\beta^\nu$ if and only if

$$e_B^T\alpha - \nu(B) \geq e_{B'}^T\alpha - \nu(B')$$

for all $B \in \mathcal{B}_\beta^\nu$ and $B' \in \mathcal{B}^\nu$. In particular, $C_\beta^\nu \subseteq C$.

To see that $C_\beta^\nu \supseteq C$, suppose that $\alpha \notin C_\beta^\nu$, that is, $\mathcal{B}_\alpha^\nu \not\supseteq \mathcal{B}_\beta^\nu$, so that

$$e_B^T\alpha - \nu(B) < e_{B'}^T\alpha - \nu(B')$$

for some $B \in \mathcal{B}_\beta^\nu$ and $B' \in \mathcal{B}^\nu$. Consider the valuation $\nu' : B \mapsto \nu(B) - e_B^T\alpha$. Pick $B \in \mathcal{B}_\beta^\nu, B' \in \mathcal{B}^\nu$ such that $\nu'(B) > \nu'(B')$ with $B\backslash B'$ as small as possible. If $|B\backslash B'| > 1$, then by minimality of $|B\backslash B'|$ we have

$$\nu'(B) + \nu'(B) > \nu'(B) + \nu'(B') \geq \nu'(B - i + j) + \nu'(B' + i - j) \geq \nu'(B) + \nu'(B),$$

for some $i \in B\backslash B'$ and $j \in B'\backslash B$, since ν' is a valuation. This is a contradiction, so $|B\backslash B'| = 1$ and $B' = B - i + j$, and hence

$$\alpha_i - \alpha_j = (e_B^T - e_{B'}^T)\alpha < \nu(B) - \nu(B'),$$

so that $\alpha \notin C$. □

Thus the cells C_β^ν are 'alcoved polytopes' (see [11]). The relative interior of such cells is connected also in a discrete sense.

Lemma 19. *Let $M : \alpha \mapsto M_\alpha$ be a matroid flock on E, and let $\alpha, \beta \in \mathbb{Z}^E$. If $M_\alpha = M_\beta$, then there is a walk $\gamma^0, \ldots, \gamma^k \in \mathbb{Z}^E$ from $\alpha = \gamma^0$ to $\beta = \gamma^k$ so that $M_{\gamma^i} = M_\alpha$ for $i = 0, \ldots, k$, and for each i there is a J_i so that $\gamma^i - \gamma^{i-1} = \pm e_{J_i}$*

Proof. By (MF2), there is a feasible walk from α to $\alpha + k\mathbf{1}$ for any $k \in \mathbb{Z}$, taking steps of the form $\pm\mathbf{1}$. Fixing any $i_0 \in E$, we may assume that $\alpha_{i_0} = 0$, and similarly that $\beta_{i_0} = 0$.

Let $\nu = \nu^M$. Using Lemma 18, we have $\{\gamma \in \mathbb{R}^E : M_\gamma = M_\alpha\} = (C_\alpha^\nu)^\circ$, where $(C_\alpha^\nu)^\circ$ denotes the relative interior of C_α^ν. For each i, j let $c_{ij} := \min\{\alpha_i - \alpha_j, \beta_i - \beta_j\}$. Then by inspection of the system of inequalities which defines C_α^ν (Lemma 18), we have

$$\alpha, \beta \in C := \{\gamma \in \mathbb{R}^E : \gamma_i - \gamma_j \geq c_{ij} \text{ for all } i, j, \text{ and } \gamma_{i_0} = 0\} \subseteq \{\gamma \in \mathbb{R}^E : M_\gamma = M_\alpha\}.$$

Then C is a bounded polyhedron defined by a totally unimodular system of inequalities with integer constant terms c_{ij}. It follows that C is an integral polytope. Moreover α, β are both vertices of C, and hence there is a walk from α to β over the 1-skeleton of C. Since C has integer vertices, and each edge of C is parallel to e_J for some $J \subseteq E$, the lemma follows. □

Lemma 20. *Let $M : \alpha \mapsto M_\alpha$ be a matroid flock on E, let $\alpha \in \mathbb{Z}^E$, and let $J \subseteq E$. If $M_\alpha = M_{\alpha+e_J}$, then $\lambda_{M_\alpha}(J) = 0$.*

Proof. By Lemma 9, we have $M_\alpha/J = M_{\alpha+e_J}\backslash J = M_\alpha\backslash J$. The lemma follows. □

4. Frobenius flocks from algebraic matroids

Let E be a finite set, and let K be an algebraically closed field of positive characteristic $p > 0$, so that the Frobenius map $F : x \mapsto x^p$ is an automorphism of K. For any $w \in K^E$ and $\alpha \in \mathbb{Z}^E$, let

$$\alpha w := (F^{-\alpha_i}(w_i))_{i \in E},$$

and for a subset $W \subseteq K^E$, let $\alpha W := \{\alpha w : w \in W\}$.

A *Frobenius flock of rank d on E over K* is a map V which assigns a linear subspace $V_\alpha \subseteq K^E$ of dimension d to each $\alpha \in \mathbb{Z}^E$, such that

(FF1) $V_\alpha / i = V_{\alpha+e_i} \backslash i$ for all $\alpha \in \mathbb{Z}^E$ and $i \in E$; and
(FF2) $V_{\alpha+\mathbf{1}} = \mathbf{1} V_\alpha$ for all $\alpha \in \mathbb{Z}^E$.

By inspection of the definition of a matroid flock, it is clear that the map $\alpha \mapsto M(V_\alpha)$ is a matroid flock. We write $M(V)$ for the support matroid of this associated matroid flock. In view of Lemma 17, we may consider a flock V as a representation of its support matroid $M(V)$.

Our interest in Frobenius flocks originates from the observation that they can represent arbitrary algebraic matroids. This is especially interesting since in positive characteristic no other "linear" representation of arbitrary algebraic matroids was available so far. In this section, we first introduce some preliminaries on algebraic matroids, and then establish their representability by Frobenius flocks.

4.1. Preliminaries on algebraic matroids.

Let K be a field and L an extension field of K. Elements $a_1, \dots, a_n \in L$ are called *algebraically independent* over K if there exists no nonzero polynomial $f \in K[x_1, \dots, x_n]$ such that $f(a_1, \dots, a_n) = 0$. Algebraic independence satisfies the matroid independence axioms (I1)—(I3) [15], and this leads to the following notion.

Definition 21. *Let M be a matroid on a finite set E. An* algebraic representation *of M over K is a pair (L, ϕ) consisting of a field extension L of K and a map $\phi : E \to L$ such that any $I \subseteq E$ is independent in M if and only if the multiset $\phi(I)$ is algebraically independent over K.*

For our purposes it will be useful to take a more geometric viewpoint; a good general reference for the algebro-geometric terminology that we will use is [4]; and we refer to [10, 17] for details on the link to algebraic matroids.

First, we assume throughout this section that K is algebraically closed. This is no loss of generality in the following sense: take an algebraic closure L' of L and let K' be the algebraic closure of K in L'. Then for any subset $I \subseteq E$ the set $\phi(I) \subseteq L$ is algebraically independent over K if and only if $\phi(I)$ is algebraically independent over K'.

Second, there is clearly no harm in assuming that L is generated by $\phi(E)$. Then let P be the kernel of the K-algebra homomorphism from the polynomial ring $R := K[(x_i)_{i \in E}]$ into L that sends x_i to $\phi(i)$. Since L is a domain, P is a prime ideal, so the quotient R/P is a domain and L is isomorphic to the field of fractions of this domain.

By Hilbert's basis theorem, P is finitely generated, and one can store algebraic representations on a computer by means of a list of generators (of course, this requires that one can already compute with elements of K). In these terms, a subset $I \subseteq E$ is independent if and only if $P \cap K[x_i : i \in I] = \{0\}$. Given generators of P, this intersection can be computed using Gröbner bases [4, Chapter 3, §1, Theorem 2].

The vector space K^E is equipped with the Zariski topology, in which the closed sets are those defined by polynomial equations; we will use the term *variety* or *closed subvariety* for such a set. In particular, let $X \subseteq K^E$ be the closed subvariety defined as the $\{a \in K^E : \forall f \in P : f(a) = 0\}$. Since P is prime, X is an irreducible closed subvariety, and by Hilbert's Nullstellensatz, P is exactly the set of all polynomials that vanish everywhere on X.

We have now seen how to go from an algebraic representation over K of a matroid on E to an irreducible subvariety of K^E. Conversely, every irreducible closed subvariety Y of K^E determines an algebraic representation of some matroid, as follows: let $Q \subseteq R$ be the prime ideal of polynomials vanishing on Y, let $K[Y] := R/Q$ be the integral domain of regular functions on Y, and set $L := K(Y)$, the fraction field of $K[Y]$. The map ϕ sending i to the class of x_i in L is a representation of the matroid M in which $I \subseteq E$ is independent if and only if $Q \cap K[x_i : i \in I] = \{0\}$.

This latter condition can be reformulated as saying that the image of Y under the projection $\pi_I : K^E \to K^I$ is dense in the latter space, i.e., that Y projects *dominantly* into K^I. Our discussion is summarised in the following definition and lemma.

Definition 22. *An* algebro-geometric representation *of a matroid M on the ground set E over the algebraically closed field K is an irreducible, closed subvariety Y of K^E such that $I \subseteq E$ is independent in M if and only if $\overline{\pi_I(Y)} = K^I$. We denote the matroid M represented by Y as $M(Y)$.*

We have seen:

Lemma 23. *A matroid M admits an algebraic representation over the algebraically closed field K if and only if it admits an algebro-geometric representation over K.* □

The rank function on M corresponds to dimension:

Lemma 24. *If Y is an algebro-geometric representation of M, then for each $I \subseteq E$ the rank of I in M is the dimension of the Zariski closure $\overline{\pi_I(Y)}$.* □

Because of this equivalence between algebraic and algebro-geometric representations, we will continue to use the term algebraic representation for algebro-geometric representations.

4.2. **Tangent spaces.** Crucial to our construction of a flock from an algebraic matroid are tangent spaces, which were also used in [13] in the study of characteristic sets of algebraic matroids. In this subsection, $Y \subseteq K^E$ is an irreducible, closed subvariety with vanishing ideal $Q \subseteq R$, $K[Y] := R/Y$ is its coordinate ring, and $K(Y)$ its function field.

Definition 25. *Define the $K[Y]$-module*

$$J_Y := \left\{ \left(\frac{\partial f}{\partial x_j} + Q \right)_{j \in E} : f \in Q \right\} \subseteq K[Y]^E.$$

For any $v \in Y$, define the tangent space $T_vY := J_Y(v)^\perp \subseteq K^E$, where $J_Y(v) \subseteq K^E$ is the image of J_Y under evaluation at v. Let $\eta \in K(Y)^E$ be the generic point of Y, i.e., the point $(x_j + Q)_{j \in E}$, and define $T_\eta Y$ as $(K(Y) \otimes_{K[Y]} J_Y)^\perp \subseteq K(Y)^E$. The variety Y is called smooth *at v (and v a* smooth point *of Y) if $\dim_K T_vY = \dim_{K(Y)} T_\eta Y$.*

The $K[Y]$-module J_Y is generated by the rows of the Jacobi matrix $(\frac{\partial f_i}{\partial x_j} + Q)_{i,j}$ for any finite set of generators $f_1, \ldots, f_r$ of Q. The right-hand side in the smoothness condition also equals the transcendence degree of $K(Y)$ over K and the Krull dimension of Y. The smooth points in Y form an open and dense subset of Y.

We recall the following property of smooth points.

Lemma 26. *Assume that Y is smooth at $v \in Y$ and let S be the local ring of Y at v, i.e., the subring of $K(Y)$ consisting of all fractions f/g where $g(v) \neq 0$. Then $M := S \otimes_{K[Y]} J_Y \subseteq S^E$ is a free S-module of rank equal to $|E| - \dim Y$, which is saturated in the sense that $su \in M$ for $s \in S$ and $u \in S^E$ implies $u \in M$.* □

Now we come to a fundamental difference between characteristic zero and positive characteristic.

Lemma 27. *Let $v \in Y$ be smooth, and let $I \subseteq E$. Then $\dim \pi_I(T_vY) \leq \dim \overline{\pi_I(Y)}$. If, moreover, the characteristic of K is equal to zero, then the set of smooth points $v \in Y$ for which equality holds is an open and dense subset of Y.* □

The inequality is fairly straightforward, and it shows that $M(T_vY)$ is always a weak image of $M(Y)$ (of the same rank as the latter). For a proof of the statement in characteristic zero, see for instance [19, Chapter II, Section 6]. A direct consequence of this lemma is the following, well-known theorem [9].

Theorem 28 (Ingleton)**.** *If $\operatorname{char} K = 0$, then every matroid that admits an algebro-geometric representation over K also admits a linear representation over K.*

Proof. If $Y \subseteq K^E$ represents M, then the set of smooth points $v \in Y$ such that $\dim \pi_I(T_vY) = \dim \overline{\pi_I(M)}$ for all $I \subseteq E$ is a finite intersection of open, dense subsets, and hence open and dense. For any such point v, the linear space T_vY represents the same matroid as Y. □

A fundamental example where this reasoning fails in positive characteristic was given in the introduction. As we will see next, Frobenius flocks are a variant of Theorem 28 in positive characteristic.

4.3. **Positive characteristic.** Assume that K is algebraically closed of characteristic $p > 0$. Then we have the action of $\mathbb{Z}^E$ on K^E by $\alpha w := (F^{-\alpha_i} w_i)_{i \in E}$.

Let $X \subseteq K^E$ be an irreducible closed subvariety. To study the orbit of X under $\mathbb{Z}^E$, we need the following lemma.

Lemma 29. *The action of $\mathbb{Z}^E$ on K^E is via homeomorphisms in the Zariski topology.*

These homeomorphisms are not polynomial automorphisms since $F^{-1} : K \to K, c \mapsto c^{1/p}$, while well-defined as a map, is not polynomial.

Proof. Let $\alpha \in \mathbb{Z}^E$ and let $Y \subseteq K^E$ be closed with vanishing ideal Q. Then

$$\alpha Y = \{v \in K^E : \forall_{f \in Q} f(\alpha^{-1}v) = 0\}.$$

Now for $f \in Q$ the function $g : K \to K,\ v \mapsto f(\alpha^{-1}v)$ is not necessarily polynomial if α has negative entries. But for every $e \in \mathbb{Z}$ the equation $g(v) = 0$ has the same solutions as the equation $g(v)^{p^e} = 0$; and by choosing e sufficiently large, $h(v) := g(v)^{p^e}$ *does* become a polynomial. Hence αY is Zariski-closed, and the map $K^E \to K^E$ defined by α is continuous. The same applies to α^{-1}, so α is a homeomorphism. □

As a consequence of the lemma, αX is an irreducible subvariety of K^E for each $\alpha \in \mathbb{Z}^E$, and has the same Krull dimension as X—indeed, both of these terms have purely topological characterisations. The ideal of αX can be obtained explicitly from that of X by writing $\alpha = c\mathbf{1} - \beta$ with $c \in \mathbb{Z}$ and $\beta \in \mathbb{Z}^E_{\geq 0}$ and applying the following two lemmas.

Lemma 30. *Let $Y \subseteq K^E$ be closed with vanishing ideal Q, and $\beta \in \mathbb{Z}^E_{\geq 0}$. Then the ideal of $(-\beta)Y$ equals*

$$\left\{ f((x_i)_{i \in E}) : f\left((x_i^{(p^{\beta_i})})_{i \in E}\right) \in Q \right\}.$$

Proof. The variety $(-\beta)Y$ is the image of Y under a polynomial map, and by elimination theory [4, Chapter 3, §3, Theorem 1] its ideal is obtained from the intersection $Q \cap K\left[\left(x_i^{(p^{\beta_i})}\right)_{i \in E}\right]$ by replacing $x^{(p^{\beta_i})}$ by x_i. □

Note that the ideal in the lemma can be computed from Q by means of Gröbner basis calculations, again using [4, Chapter 3,§1, Theorem 2].

Lemma 31. *Let $Y \subseteq K^E$ be closed with vanishing ideal generated by $f_1, \ldots, f_k$. Then for each $c \in \mathbb{Z}$ the ideal of $(c\mathbf{1})Y$ is generated by $g_1 := F^{-c}(f_1), \ldots, g_k := F^{-c}(f_k)$, where F^{-c} acts on the coefficients of these polynomials only.*

Proof. A point $a \in K^E$ lies in $(c\mathbf{1})Y$ if and only if $(-c\mathbf{1})a \in Y$, i.e., if and only if $f_i(F^c(a)) = 0$ for all i, which is equivalent to $g_i(a) = 0$ for all i. So by Hilbert's Nullstellensatz the vanishing ideal of αY is the radical of the ideal generated by the g_i. But the g_i are the images of the f_i under a ring automorphism $R \to R$, and hence generate a radical ideal since the f_i do. □

Lemma 32. *For each $\alpha \in \mathbb{Z}^E$, the variety αX represents the same matroid as X.*

Proof. If $I \subseteq E$ is independent in the matroid represented by X, then the map $\pi_I : X \to K^I$ has a dense image. But the image of the projection $\alpha X \to K^I$ equals $(\alpha|_I) \operatorname{im} \pi_I$, and is hence also dense in K^I. So all sets independent for X are independent for αX, and the same argument with $-\alpha$ yields the converse. □

Lemma 33. *Let $Y \subseteq K^E$ be an irreducible, closed subvariety with generic point η and let $j \in E$. Then $e_j \in T_\eta Y$ if and only if the vanishing ideal of Y is generated by polynomials in x_j^p and the x_i with $i \neq j$.*

Proof. If the ideal Q of Y is generated by polynomials in which all exponents of x_j are multiples of p, then Q is stable under the derivation $\frac{\partial}{\partial x_j}$. This means that the projection of $J_Y \subseteq K[Y]^E$ onto the j-th coordinate is identically zero, so that $e_i \perp (K(Y) \otimes_{K[Y]} J_Y)$. This proves the "if" direction.

For "only if" suppose that $e_j \in T_\eta Y$, let G be a reduced Gröbner basis of Q relative to any monomial order, and let $g \in G$. Then $f := \frac{\partial g}{\partial x_j}$ is zero in $K[Y]$, i.e., $f \in Q$. Assume that f is a nonzero polynomial. Then the leading monomial u of f is divisible by the leading monomial u' of some element of $G \setminus \{g\}$. But u equals v/x_j for some monomial v appearing in g, and hence v is divisible by u'; this contradicts the fact that G is reduced. Hence $\frac{\partial g}{\partial x_j} = 0$, and therefore all exponents of x_j in elements of G are multiples of p. □

For any closed, irreducible subvariety $X \subseteq K^E$, let $M(X, \alpha) := M(T_\xi \alpha X)$, where ξ is the generic point of αX.

Theorem 34. *Let K be algebraically closed of characteristic $p > 0$, $X \subseteq K^E$ a closed, irreducible subvariety. Let $v \in X$ be such that for each $\alpha \in \mathbb{Z}^E$, we have*

$$M(T_{\alpha v} \alpha X) = M(X, \alpha) \qquad (*)$$

Then the assignment $V : \alpha \mapsto V_\alpha := T_{\alpha v} \alpha X$ is a Frobenius flock that satisfies $M(V) = M(X)$.

Definition 35. *This Frobenius flock is called the* Frobenius flock associated to the pair (X, v).

Proof of Theorem 34. For each $\alpha \in \mathbb{Z}^E$ we have $M(T_{\alpha v} \alpha X) = M(T_\xi \alpha X)$, and this implies that $\dim_K V_\alpha = \dim X =: d$.

Next, for $j \in E$ the action by $(-e_j) \in \mathbb{Z}^E$ sends $Y := (\alpha + e_j)X$ into $(-e_j)Y = \alpha X$ by raising the j-th coordinate to the power p. Hence the derivative of this map at $y := (\alpha + e_j)v$, which is the projection onto $e_j^\perp$ along e_j, maps $V_{\alpha+e_j} = T_y Y$ into $V_\alpha = T_{(-e_j)y}(-e_j)Y$, and therefore $V_{\alpha+e_j} \setminus j \subseteq V_\alpha / j$. If the left-hand side has dimension d, then equality holds, and (FF1) follows.

If not, then $e_j \in T_y Y$, i.e., j is a co-loop in $M(T_y Y)$. Then by (*) j is also a co-loop in $M(T_\eta Y)$, where η is the generic point of Y. By Lemma 33 the ideal of Y is generated by polynomials $f_1, \ldots, f_r$ in which all exponents of x_j are multiples of p. By Lemma 30, replacing x_j^p by x_j in these generators yields generators $g_1, \ldots, g_r$ of the ideal of $e_j Y$. Now the Jacobi matrix of $g_1, \ldots, g_r$ at $(-e_j)y$ equals that of $f_1, \ldots, f_r$ at y except that the j-th column may have become nonzero. But this means that V_α / j has dimension equal to that of $V_{\alpha+e_j} \setminus j$, namely, $d - 1$. Hence (FF1) holds in this case, as well.

For (FF2), let $Z := \alpha Y$ and $z := \alpha y$, pick any generating set $f_1, \ldots, f_r$ of I_Z, raise all f_i to the $(1/p)$-th power, and replace each x_j in the result by x_j^p. By Lemma 31, the resulting polynomials $g_1, \ldots, g_r$ generate $I_{\mathbf{1}Z}$. The Jacobi matrix of $g_1, \ldots, g_r$ at $\mathbf{1}z$ equals that of $f_1, \ldots, f_r$ at z except with F^{-1} applied to each entry. Hence $V_{\alpha+\mathbf{1}} = \mathbf{1}V_\alpha$ as claimed. This proves that V is a Frobenius flock.

We next verify that $M(V) = M(X)$; by Lemma 32 the right-hand side is also $M(\alpha X)$ for each $\alpha \in \mathbb{Z}^E$. Assume that I is independent in $M(V_\alpha)$ for some α. This means that the projection $T_{\alpha v} \alpha X \to K^I$ is surjective and since αv is a smooth point of αX by (*) we find that the projection $\alpha X \to K^I$ is dominant, i.e., I is independent in $M(X)$.

Conversely, assume that I is a basis for $M(X)$, so that $|I| = d$. Then $K(X)$ is an algebraic field extension of $K(x_i : i \in I) =: K'$. If this is a separable extension, then by [2, AG.17.3] the projection $T_u X \to K^I$ is surjective (i.e., a linear isomorphism) for general $u \in X$, hence also for $u = v$ by (*). If not, then for each $j \in \bar{I}$ let $\alpha_j \in \mathbb{Z}_{\geq 0}$ be minimal such that $x_j^{(p^{\alpha_j})}$ *is* separable over K', and set $\alpha_i = 0$ for $i \in I$. Then the extension $K' \subseteq K((-\alpha)X)$ *is* separable, and hence the projection $T_{(-\alpha)v} : (-\alpha X) \to K^I$ surjective. □

For *fixed* $\alpha \in \mathbb{Z}^E$, the condition (*) holds for v in some open dense subset of X, i.e., for *general* v in the language of algebraic geometry—indeed, it says that certain subdeterminants of the Jacobi matrix that do not vanish at the generic point of αX do not vanish at the point αv either. However, we require that (*) holds for *all* $\alpha \in \mathbb{Z}^E$. This means that v must lie outside a countable union of proper Zariski-closed subsets of X, i.e., it must be *very general* in the language of algebraic geometry. *A priori*, that K is algebraically closed does not imply the existence of such a very general point v. This can be remedied by enlarging K. For instance, if we change the base field to $K(X)$, then the generic point of X satisfies (*); alternatively, if K is taken uncountable (in addition to algebraically closed), then a very general v also exists. But in fact, as we will see in Theorem 38, certain general finiteness properties of flocks imply that, after all, it *does* suffice that K is algebraically closed.

Corollary 36. *Let K be algebraically closed of characteristic $p > 0$, and let $X \subseteq K^E$ be a closed, irreducible subvariety. Then $M : \alpha \mapsto M(X, \alpha)$ is a matroid flock with support matroid $M(X)$.*

Proof. Let v be the generic point of X over the enlarged base field $K(X)$. Then the Frobenius flock V associated with (X, v) satisfies $M(V_\alpha) = M(X, \alpha)$. As V is a Frobenius flock, the assignment $\alpha \mapsto M(V_\alpha)$, and hence M, is a matroid flock. By Theorem 34, the support matroid of V, and hence of its matroid flock M, is $M(X)$. □

We now prove that under certain technical assumptions, if v satisfies (*) at some $\alpha \in \mathbb{Z}^E$, then it also satisfies (*) at $\alpha - e_I$. This will reduce the number of conditions on v from countable to finite, whence ensuring that a general v satisfies them.

Lemma 37. *Let $v \in X$ satisfy (*) for some $\alpha \in \mathbb{Z}^E$, and let $I \subseteq E$ be such that $M(X, \alpha) = M(X, \alpha - e_I)$. Then v satisfies (*) for $\alpha - e_I$.*

Proof. Set $Y := \alpha X$ and set $W := K(Y) \otimes_{K[Y]} J_Y \subseteq K(Y)^E$. By Lemma 20 applied to the matroid flock $\alpha \mapsto M(X, \alpha)$, we find that the connectivity of I in $M(W) = M(X, \alpha)$ is zero, and hence that $W = (W/I) \times (W/\bar{I})$.

We claim that the same decomposition happens over the local ring S of Y at αv. Let $M := S \otimes_{K[Y]} J_X \subseteq S^E$. Let $m \in M$ and write $m = m_1 + m_2$ where m_1, m_2 have nonzero entries only in $I, \bar{I}$, respectively. By the decomposition of W, we have $m_1, m_2 \in W$, and by clearing denominators it follows that $s_1 m_1, s_2 m_2 \in J_Y \subseteq M$ for suitable $s_1, s_2 \in K[Y] \subseteq S$. Then by Lemma 26, m_1, m_2 themselves already lie in M. Thus $M = (M/I) \times (M/\bar{I})$, as claimed.

This means that there exist generators $f_1, \ldots, f_r, g_1, \ldots, g_s$ of the maximal ideal of S with $r + s = |E| - \dim Y$ and such that $\frac{\partial f_i}{\partial x_j} = 0 \in S$ for all $i = 1, \ldots, r$ and $j \in \bar{I}$ and $\frac{\partial g_i}{\partial x_j} = 0 \in S$ for all $i = 1, \ldots, s$ and $j \in I$. Thus the Jacobi matrix of $f_1, \ldots, f_r, g_1, \ldots, g_t$ looks as follows:

$$A = \begin{array}{c} f_1 \\ \vdots \\ f_r \\ g_1 \\ \vdots \\ g_s \end{array} \begin{array}{c|c} I & \bar{I} \\ \hline A_{11} & 0 \\ \hline 0 & A_{22} \end{array}$$

By (*) the K-row space of $A(y)$ defines the same matroid as the $K(Y)$-row space of A itself.

It follows that the exponents of x_j with $j \in I$ in the g_i are multiples of p, and so are the exponents of the x_j with $j \in \bar{I}$ in the f_i. Let g'_i be the polynomial obtained from g_i by replacing x_j^p with x_j for $j \in I$, and let f'_i be the polynomial obtained from f_i^p by replacing each x_j^p with x_j for $j \in I$. Then the f'_i and g'_i lie in the maximal ideal of $(-e_I)Y$ at $(-e_I)y$, and their Jacobi matrix looks like this:

$$A = \begin{array}{c} f'_1 \\ \vdots \\ f'_r \\ g'_1 \\ \vdots \\ g'_s \end{array} \begin{array}{c|c} I & \bar{I} \\ \hline FA_{11} & 0 \\ \hline A_{21} & A_{22} \end{array}$$

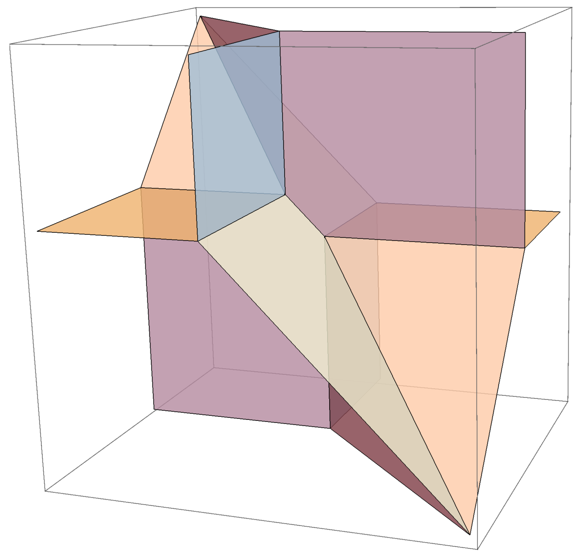

FIGURE 1. The cell decomposition for a matroid flock; the two zero-dimensional cells are 0 and $-ge_2 - ge_3$.

Here FA_{11} is the matrix over S whose entries are obtained by applying the Frobenius automorphism to all coefficients. In particular, the evaluation $A'((-e_I)y)$ has full K-rank $r+s$, $(-e_I)Y$ is smooth at $(-e_I)y$, and the f_i' and the g_i' generate the maximal ideal of the local ring of $(-e_I)Y$ at $(-e_I)y$. Moreover, if a subset I' of the columns of A is independent, then the columns labelled by I' are also independent in $A'((-e_I)y)$. This means that $M(T_{(-e_I)y}(-e_I)Y)$ has at least as many bases as $M(T_\xi Y) = M(T_\eta e_I Y)$, but it cannot have more, so that v satisfies (*) at $\alpha - e_I$. ☐

Theorem 38. *Let K be algebraically closed of characteristic $p > 0$ and let $X \subseteq K^E$ be an irreducible closed subvariety of dimension d. Then for a general point $v \in X$ the map $V : \alpha \mapsto T_{\alpha v}\alpha X$ is a matroid flock of rank d over K such that $M(X, \alpha) = M(V_\alpha)$ for each $\alpha \in \mathbb{Z}^E$.*

Proof. By Theorem 34 it suffices to prove that there exists a $v \in X$ satisfying (*) at every $\alpha \in \mathbb{Z}^E$. For some field extension $K' \supseteq K$ there does exist a K'-valued point $v' \in X(K')$ that satisfies (*) at every α, and we may form the Frobenius flock V' associated to (X, v') over K'.

For each matroid M' on E the points $\alpha \in \mathbb{Z}^E$ with $M(V'_\alpha) = M'$ are connected to each other by means of moves of the form $\alpha \to \alpha + \mathbf{1}$ or $\alpha \to \alpha - e_I$ for some subset $I \subseteq E$ of connectivity 0 in M'; see Lemma 19. Hence by Lemma 37, for a $v \in X(K)$ to satisfy (*) for all $\alpha \in \mathbb{Z}^E$ it suffices that v satisfies this condition for one representative α for each matroid M'. Since there are only finitely many matroids M' to consider, we find that, after all, a general $v \in X(K)$ suffices these conditions. ☐

Observe the somewhat subtle structure of this proof: apart from commutative algebra, it also requires the entire combinatorial machinery of flocks.

Example 39. *Let $E = \{1, 2, 3, 4\}$ and consider the polynomial map $\phi : K^2 \to K^4$ defined by $\phi(s, t) = (s, t, s+t, s+t^{(p^g)})$ where $p = \operatorname{char} K$ and $g > 0$. This is a morphism of (additive) algebraic groups, hence $X := \operatorname{im}\phi$ is closed. The polynomials in the parameterisation ϕ are pairwise algebraically independent, so that $M(X)$ is the uniform matroid on E of rank 2.*

One can verify that the point 0 is general in the sense of Theorem 38, and

$$T_0X = \operatorname{im} d_0\phi = \text{the row space of } \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}.$$

Note that in $M(T_0X)$ the elements 1 and 4 are parallel. Compute

$$(-e_2-e_3)X = \{(s, t^p, s^p+t^p, s+t^{(p^g)}) : s,t \in K\} = \{(s, t, s^p+t, s+t^{(p^{g-1})}) : s,t \in K\};$$

so

$$T_0(-e_2-e_3)X = \text{the row space of } \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}.$$

Here, not only 1 and 4 are parallel, but also 2 and 3. We see the same matroid for $(-ke_2-ke_3)X$ with $k=2,\ldots,g-1$. But $(-ge_2-ge_3)X = \{(s,t,s^{p^g}+t, s+t) : s,t \in K\}$, so

$$T_0(-ge_2-ge_3)X = \text{the row space of } \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}.$$

Here only 2 and 3 are parallel. The alcoved polytopes from Subsection 3.2, intersected with the hyperplane where one of the coordinates is zero, are depicted in Figure 1. ♣

5. Algebraic and linear matroids

If X is an algebraic matroid representation, and $M : \alpha \mapsto M(X, \alpha)$ is the associated matroid flock (Corollary 36), then we call $\nu^X := \nu^M$ the *Lindström valuation* of X. In this section, we consider the role of the Lindström valuation in the relation between algebraic representability in characteristic p, and linear representability in characteristics p and 0.

5.1. **Rational matroids.** Matroids which are linear over $\mathbb{Q}$ are algebraic in each positive characteristic. We will describe the construction to obtain an algebraic representation X from a linear representation over $\mathbb{Q}$, and then express the flock valuation of X in terms of the linear representation over $\mathbb{Q}$.

Suppose $N = (E, \mathcal{B})$ is linear over $\mathbb{Q}$, and K is an algebraically closed field of characteristic p. As N is rational, there exists a subspace $W \subseteq \mathbb{Q}^E$ so that $N = M(W)$.

Let $A \in \mathbb{Z}^{d\times E}$ be any matrix whose rows form a basis of W, let $a_j, j \in E$ be the columns of A, and consider the homomorphism of algebraic tori $\phi : (K^*)^d \to (K^*)^E$ given by $\phi(t) = (t^{a_j})_{j\in J}$. Then $Y = Y(W) := \operatorname{im}\phi$ is a closed subtorus in $(K^*)^E$, independent of the choice of A, of dimension d. Let $X = X(W)$ be its Zariski closure in K^E, a d-dimensional irreducible variety.

Lemma 40. *The matroids $M(W)$ and $M(X)$ coincide.*

Proof. For $J \subseteq E$ the columns $a_j, j \in J$ are linearly dependent over $\mathbb{Q}$ if and only if the monomials $t^{a_j}, j \in J$ in the variables $t_1, \ldots, t_d$ are algebraically dependent over K. □

Let $\mathbb{Z}^E$ act on $\mathbb{Q}^E$ by $\alpha w := (w_j/(p^{\alpha_j}))_{j\in E}$.

Lemma 41. *For all $\alpha \in \mathbb{Z}^E$ we have $\alpha(Y(W)) = Y(\alpha W)$, and similarly for X.*

Proof. It suffices to prove this for $\alpha = -\mathbf{1}$ and for $\alpha = e_j$. For $\alpha = -\mathbf{1}$ note that $\alpha W = W$ and also $\alpha Y = Y$.

Suppose that $\alpha = e_j$ and let $A' \in \mathbb{Z}^{d\times E}$ be a matrix whose rows span $e_i W$. Then the rows of the matrix A obtained from A' by multiplying the j-th column with p span W, and by inspection $Y(W)$ is obtained from $Y(e_jW)$ by raising the j-th coordinate to the power p. □

Lemma 42. *The all-one vector $\mathbf{1} \in X$ satisfies condition (*) from Theorem 34 for each $\alpha \in \mathbb{Z}^E$.*

Proof. The torus Y is smooth, and its tangent space $T_{\phi(t)}Y = T_{\phi(t)}X$ at the point $\phi(t)$ equals $\phi(t)\cdot T_{\mathbf{1}}X$, where $\cdot$ is the componentwise multiplication and $\mathbf{1}$ is the unit element in the torus $(K^*)^E$. This implies that $M(T_{\phi(t)}X) = M(T_{\mathbf{1}}X)$.

For each $\alpha \in \mathbb{Z}^E$ we have $\alpha X = \overline{\alpha Y}$, where αY is also a d-dimensional torus with unit element $\mathbf{1} = \alpha\mathbf{1}$. Hence the previous paragraph applies. □

Lemma 43. *Let $A \in \mathbb{Z}^{d\times E}$ such that its rows generate the lattice $W \cap \mathbb{Z}^E$. Then $T_{\mathbf{1}}X$ is the span in K^E of the rows of A.*

Proof. As $\mathbb{Z}^E/(W \cap \mathbb{Z}^E)$ is torsion-free, A can be extended to an integral $|E| \times E$-matrix with determinant 1. This latter determinant is an integral linear combination of the $d \times d$-subdeterminants of A, so at least one $d \times d$-submatrix A_J of A has $p \not| \det(A_J)$. Hence the image of A in $K^{d\times E}$ has rank d. This image, acting on row vectors, is also the matrix of the derivative $d_{\mathbf{1}}\phi$. We conclude that $T_{\mathbf{1}}X = \operatorname{im} d_{\mathbf{1}}\phi$ and that this space is spanned by the images in K^E of the rows of A. □

Let $\mathrm{val}_p : \mathbb{Q} \to \mathbb{Z}$ denote the p-adic valuation.

Lemma 44. *Let $A' \in \mathbb{Q}^{d\times E}$ be any matrix whose rows span W. Then for $B \in \binom{E}{d}$ we have $B \in M(T_{\mathbf{1}}X)$ if and only if $\mathrm{val}_p(A'_B) \le \mathrm{val}_p(A'_{B'})$ for all $B' \in \binom{E}{d}$.*

Proof. For $A' = A$ as in the previous lemma this is evident by the previous lemma: these are the subdeterminants that are not divisible by p. Any other A' is related to such an A via $A' = gA$, where $g \in \mathbb{Q}^{d\times d}$ is an invertible linear transformation, and then $\det(A'_B) = \det(g)\det(A_B)$ is minimal if and only if $\det(A_B)$ is. □

Theorem 45. *Let $A \in \mathbb{Z}^{d\times E}$ as in Lemma 43. Then the Lindström valuation associated to the flock of X maps $B \in \binom{E}{d}$ to $\mathrm{val}_p(\det A_B)$.*

Proof. Let $\alpha \in \mathbb{Z}^E$ and set $A' := A\,\mathrm{diag}(p^{-\alpha})$. The rows of this matrix span αW, and by Lemma 41 as well as Lemma 44 applied to αX a $B \in \binom{E}{d}$ is a basis in $M(T_{\mathbf{1}}\alpha X)$ if and only if $\mathrm{val}_p(A'_B) \le \mathrm{val}_p(A'_{B'})$ for all $B' \in \binom{E}{d}$. This translates into the inequality $\mathrm{val}_p(A_B) - e_B^T\alpha \le \mathrm{val}_p(A_{B'}) - e_B^T\alpha$. Now the result follows from Lemma 42 and the characterisation in Theorem 7 of the Lindström valuation. □

5.2. **Rigid matroids.** A matroid valuation $\nu : \binom{E}{d} \to \mathbb{R}_\infty$ is *trivial* if there exists an $\alpha \in \mathbb{R}^E$ so that $\nu(B) = e_B^T\alpha$ for all $B \in \mathcal{B}^\nu$.

Lemma 46. *Suppose $\nu : \binom{E}{d} \to \mathbb{Z}_\infty$ is a matroid valuation. Then there is an $\alpha \in \mathbb{Z}^E$ such that $M^\nu_\alpha = M^\nu$ if and only if ν is trivial.*

Proof. Necessity: if $M^\nu_\alpha = M^\nu$ for some $\alpha \in \mathbb{Z}^E$, then $e_B^T\alpha - \nu(B) = g^\nu(\alpha)$ for all bases B of M^ν. Equivalently, $\nu(B) = e_B^T\alpha - g^\nu(\alpha) = e_B^T\alpha'$ for all bases B of M^ν, where $\alpha' = \alpha - (g^\nu(\alpha)/d)\mathbf{1}$. Then ν is trivial.

Sufficiency: If ν is trivial, then there exists a $\beta \in \mathbb{R}^E$ so that $\nu(B) = e_B^T\beta$ for all bases B of M^ν, or equivalently, $M^\nu_\beta = M^\nu$. By Lemma 18, the set $C^\nu_\beta := \{\alpha \in \mathbb{R}^E : \mathcal{B}^\nu_\alpha \supseteq \mathcal{B}^\nu_\beta\}$ is determined by a totally unimodular system of inequalities. As C^ν_β is nonempty, it must also contain an integer vector $\alpha \in \mathbb{Z}^E$. □

Following Dress and Wenzel, we call a matroid M *rigid* if all valuations of M are trivial.

Theorem 47. *Let N be a matroid, and let K be an algebraically closed field of positive characteristic. If N is rigid, then N is algebraic over K if and only if N is linear over K.*

Proof. If N is linear over K, then clearly N is also algebraic over K. We prove the converse. Let $X \subseteq K^E$ be an algebraic representation of N, and let $\nu = \nu^X$ be the Lindström valuation of X. Since we assumed that N is rigid, and ν is a valuation with support matroid $M(X) = N$, it follows that ν is trivial. By Lemma 46, there exists an $\alpha \in \mathbb{Z}^E$ such that $M(X,\alpha) = M^\nu_\alpha = M^\nu = N$ for some $\alpha \in \mathbb{Z}^E$. For a sufficiently general $x \in \alpha X$, we have $M(T_x\alpha X) = M(X,\alpha)$, and then $T_x\alpha X$ is a linear representation of N over K. □

We will give a brief account of the work of Dress and Wenzel on matroid rigidity. The following lemma, which is given in much greater generality in [5], points out how the structure of a matroid M restricts the set of valuations of M.

Lemma 48 (Dress and Wenzel)**.** *Let ν be a matroid valuation with support matroid $M = (E,\mathcal{B})$. Let $F \subseteq E$ and let $a,b,c,d \in E \setminus F$ be distinct. If $F+a+c,\ F+b+d,\ F+a+d,\ F+b+c \in \mathcal{B}$, but $F+a+b \notin \mathcal{B}$, then*

$$\nu(F+a+c) + \nu(F+b+d) = \nu(F+a+d) + \nu(F+b+c). \tag{3}$$

Proof. Apply (V2) to bases $B = F + a + c,\ B' = F + b + d$ and the element $i = a \in B \setminus B'$. Since $F + a + b \notin \mathcal{B}$, the only feasible exchange element is $j = b$. Hence

$$\nu(F+a+c)+\nu(F+b+d) = \nu(B)+\nu(B') \leq \nu(B-i+j)+\nu(B'+i-j) = \nu(F+b+c)+\nu(F+a+d).$$

We similarly obtain the complementary inequality

$$\nu(F + b + c) + \nu(F + a + d) \leq \nu(F + a + c) + \nu(F + b + d)$$

by considering $B = F + b + c,\ B' = F + a + d$, and $i = b$. □

So from any given matroid $M = (E, \mathcal{B})$ we obtain a list of linear equations (3) which together confine the valuations of M to a subspace of $\mathbb{R}^{\mathcal{B}}$ (ignoring the $B \notin \mathcal{B}$, which are fixed to $\nu(B) = \infty$). If this subspace coincides with the set of trivial valuations of M, then M is rigid. A straightforward calculation reveals that this happens, for example, if M is the Fano matroid.

Using a consideration about the *Tutte group*, which essentially relies on Lemma 48, Dress and Wenzel showed [5, Thm 5.11]:

Theorem 49. *If the inner Tutte group of a matroid M is a torsion group, then M is rigid. In particular:*

1. *binary matroids are rigid; and*
2. *if $r \geq 3$ and q is a prime power, then the finite projective space $PG(r-1, q)$ is rigid.*

Rigidity is a rather strong condition of matroids. The following is straightforward from the definition of matroid valuations.

Lemma 50. *Let $M = (E, \mathcal{B})$ be a matroid of rank d, and let $B_0 \in \mathcal{B}$ be such that $B_0 - i + j \in \mathcal{B}$ for all $i \in B_0$ and all $j \in E \backslash B_0$. Then $\nu : \binom{E}{d} \to \mathbb{R}_\infty$ defined by*

$$\nu(B) := \begin{cases} v & \text{if } B = B_0 \\ 0 & \text{if } B \in \mathcal{B}, B \neq B_0 \\ \infty & \text{otherwise} \end{cases}$$

is a valuation of M for all $v \geq 0$.

We will demonstrate next how conditions weaker than strict rigidity of M can be used to derive linear representations from algebraic representations.

5.3. **Lazarson matroids.** Lindström's technique for deriving a linear representation of a matroid from an algebraic representation was applied on at least three occasions: by Bernt Lindström [13], to Lazarson matroids; by Gary Gordon [6], to Reid geometries; and more recently by Aner Ben-Efraim [1], to a certain single-element extension of a Dowling geometry of rank 3. In each case, the matroids in question are not rigid. We illustrate the role of the Lindström valuation in the argumentation here.

Two valuations $\nu, \nu' : \binom{E}{d} \to \mathbb{R}_\infty$ are *equivalent*, notation $\nu \sim \nu'$, if there exists an $\alpha \in \mathbb{R}^E$ so that $\nu(B) = \nu'(B) + e_B^T\alpha$ for all $B \in \binom{E}{d}$. Thus a valuation ν is trivial if and only if $\nu \sim 0$.

A valuation $\nu : \binom{E}{d} \to \mathbb{R}_\infty$ of a matroid M induces valuations of the minors and the dual of M. If i is not a coloop of M, then $\nu\backslash i : \binom{E-i}{d} \to \mathbb{R}_\infty$ obtained by restricting ν to $\binom{E-i}{d}$ is a valuation of $M\backslash i$, and if i is not a loop, then $\nu/i : \binom{E-i}{d-1} \to \mathbb{R}_\infty$ determined by $\nu/i : B \mapsto \nu(B+i)$ is a valuation of M/i. Finally, $\nu^* : \binom{E}{|E|-d} \to \mathbb{R}_\infty$ determined by $\nu : B \mapsto \nu(\overline{B})$ is a valuation of M^*.

Lemma 51. *Suppose M is a matroid, and $\{i, j\}$ is a circuit of M. If ν, ν' are valuations of M so that $\nu\backslash j = \nu'\backslash j$, then $\nu \sim \nu'$.*

Proof. Let ν be any valuation of M, and B, B' be such that $i \in B \cap B'$ and $B' = B - k + l$, where $j \neq k, l$. By Lemma 48, we have $\nu(B)+\nu(B'-i+j) = \nu(B-i+j)+\nu(B')$, since $B-k+j = B'-l+j$ is not a basis as it contains the dependent set $\{i, j\}$. Hence $\nu(B)-\nu(B-i+j) = \nu(B')-\nu(B'-i+j)$ for any adjacent bases B, B' both containing i. Since any two bases of $M\backslash j$ are connected by a walk along adjacent bases, it follows that there is a constant c so that $\nu(B) - \nu(B - i + j) = c$ for any basis B of $M\backslash j$ with $i \in B$. If ν' is any other valuation of M, then by the same reasoning there is a c' so that $\nu'(B) - \nu'(B - i + j) = c'$ for any basis B of $M\backslash j$ with $i \in B$. If $\nu'\backslash j = \nu\backslash j$, then $\nu(B) + e_B^T(ce_j) = \nu'(B) + e_B^T(c'e_j)$ for all bases B of M, and it follows that $\nu \sim \nu'$, as required. $\square$

If M is a matroid then $si(M)$, the *simplification* of M, is a matroid whose elements are the parallel classes of M, and which is isomorphic to any matroid which arises from M by restricting to one element from each parallel class. Directly from the previous lemma, we obtain:

Lemma 52. *Suppose M is a matroid. If $si(M)$ is rigid, then M is rigid.*

Lemma 53. *Suppose $M \cong U_{1,n}$ or $M \cong U_{n-1,n}$. Then M is rigid.*

Proof. If $M \cong U_{1,n}$, then $si(M) \cong U_{1,1}$ which is rigid. Hence by Lemma 52, M is rigid. If $M = U_{n-1,n}$, then $M^* = U_{1,n}$ is rigid, and hence M is rigid. $\square$

Let $n \geq 2$ be a natural number, and let M_n^- be matroid which is linearly represented over $\mathbb{Q}$ by the matrix

$$\begin{array}{c} \quad x_0 \quad x_1 \quad \cdots \quad x_n \quad z \quad y_0 \quad y_1 \quad \cdots \quad y_n \\ \begin{pmatrix} 1 & & & & 1 & 0 & 1 & & 1 \\ & 1 & & & 1 & 1 & 0 & & 1 \\ & & \ddots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ & & & 1 & 1 & 1 & 1 & & 0 \end{pmatrix}. \end{array} \tag{4}$$

Then M_n, the *Lazarson matroid*, is the matroid on the same ground set with base set $\mathcal{B}(M_n) := \mathcal{B}(M_n^-)\backslash\{\{y_0, \dots, y_n\}\}$. Note that M_2 is the Fano matroid, and M_2^- is the non-Fano matroid.

Theorem 54 (Lindström [13])**.** *Let p be a prime. If M_p has an algebraic representation over a field K, then the characteristic K is p.*

Let us say that a basis B of M_n or M_n^- is *central* if it is of the form $B = \{x_i : i \notin I\} \cup \{y_i : i \in I\}$ for some $I \subseteq \{0, \dots, n\}$ such that $|I| > 2$.

Lemma 55. *Let $n \geq 2$, and let ν be a valuation of $M_n = (E, \mathcal{B})$. Then there is a $\beta \in \mathbb{R}^E$ such that if $B \in \mathcal{B}$ and B is not central, then $B \in \mathcal{B}_\beta^\nu$.*

Proof. Since $si(M_n/z) \cong U_{n,n+1}$, the matroid M_n/z is rigid. Passing to an equivalent valuation if necessary, we may assume that $\nu(B) = 0$ for all $B \in \mathcal{B}$ so that $z \in B$. Let $B^0 := \{x_0, \dots, x_n\}$ and $B^1 := \{y_0, \dots, y_n\}$. Again by moving to an equivalent valuation $B \mapsto \nu(B) + e_B^T\alpha$, where $\alpha = a(\mathbf{1} - (n+1)e_z)$ for an appropriate $a \in \mathbb{R}$, we may ensure that $\nu(B^0) = 0$ while preserving that $\nu(B) = 0$ for all $B \in \mathcal{B}$ so that $z \in B$.

We show that if B is not central and $z \notin B$, then $\nu(B) = 0$. We argue by induction on $|B\backslash B^0|$. Assume that $|B \backslash B^0| > 0$. As B is a basis, $z \notin B$ and B is not central, we have $x_i, y_i \in B$ and $x_j, y_j \notin B$ for some i, j. If there is a $k \neq i$ such that $y_k \in B$, then consider the basis $B' := B + x_j - y_k + z - x_i$. The set $B + z - y_k$ is not a basis, as it contains the circuit $\{z, x_i, y_i\}$. By Lemma 48, we obtain

$$\nu(B) + \nu(B') = \nu(B + z - x_i) + \nu(B + x_j - y_k).$$

Since $z \in B'$ and $z \in B + z - x_i$, we have $\nu(B') = \nu(B + z - x_i) = 0$. Since $B + x_j - y_k$ is not central and closer to B^0 than B is, we have $\nu(B + x_j - y_k) = 0$ by induction. It follows that $\nu(B) = 0$. If there is no $k \neq i$ such that $y_k \in B$, then $B = B^0 - x_j + y_i$. Noting that $B^0 - x_i + y_i$ is dependent in M_n, we obtain

$$\nu(B) + \nu(B^0 - x_i + z) = \nu(B^0) + \nu(B^0 - x_i - x_j + y_i + z)$$

from Lemma 48. As $z \in B^0 - x_i + z$ and $z \in B^0 - x_i - x_j + y_i + z$, we have $\nu(B^0 - x_i + z) = \nu(B^0 - x_i - x_j + y_i + z) = 0$, so that $\nu(B) = \nu(B^0) = 0$.

Next, we argue that if B is central, then $\nu(B) \geq 0$, again by induction on $|B \backslash B^0|$. Then there are i, j so that $\nu(B) + \nu(B^0) \geq \nu(B - i + j) + \nu(B^0 + i - j)$. Since $\nu(B^0) = 0$, and $\nu(B - i + j), \nu(B^0 + i - j) \geq 0$ as both bases are closer to B^0 than B is, this implies that $\nu(B) \geq 0$.

It follows that $g^\nu(0) = \sup\{e_B^T 0 - \nu(B) : B \in \mathcal{B}\} = 0$, so that

$$\mathcal{B}_0^\nu := \{B \in \mathcal{B} : e_B^T 0 - \nu(B) = g^\nu(0)\} = \{B \in \mathcal{B} : \nu(B) = 0\}$$

contains each non-central basis of M_n. Therefore, $\beta = 0$ satisfies the lemma. $\square$

We obtain a minor extension of Lindström's Theorem.

Theorem 56. *Let p be a prime and let n be a natural number. If M_n has an algebraic representation over a field of characteristic p, then p divides n.*

Proof. Let X be an algebraic representation of M_n over a field K of characteristic p. Without loss of generality, we may assume that K is algebraically closed. Let ν be the Lindström valuation of X. Let $\beta \in \mathbb{R}^E$ be the vector obtained in Lemma 55. As ν is integral, there is an $\alpha \in C^\nu_\beta \cap \mathbb{Z}^E$, so that $\mathcal{B}^\nu_\alpha \supseteq \mathcal{B}^\nu_\beta$.

Let W be a tangent space of αX satisfying $M(W) = M^\nu_\alpha$ and let A be a $d \times E$ matrix whose rows span W. Since $B^0 := \{x_0, \ldots, x_n\} \in \mathcal{B}^\nu_\alpha$, we may assume that $A_{B^0} = I$. Since for each $B \in \binom{E}{n+1}$ with $|B \setminus B^0| \leq 2$ we have $B \in \mathcal{B}$ if and only if $B \in \mathcal{B}^\nu_\alpha$, it is straightforward that by scaling rows and columns in A we may obtain the matrix (4). Hence M^ν_α is linearly represented over $GF(p)$ by (4).

Let $B^1 := \{y_0, \ldots, y_n\}$. The determinant of A_{B^1} over $\mathbb{Z}$ equals $n(-1)^n$. Since $B^1 \notin \mathcal{B}$, we must have $B^1 \notin \mathcal{B}^\nu_\alpha$, so that $\det A_{B^1} = n(-1)^n \mod p = 0$. Hence p divides n. $\square$

6. Final remarks

From any irreducible, d-dimensional algebraic variety $X \subseteq K^E$ in characteristic $p > 0$ we have constructed a valuation $\nu^X : \binom{E}{d} \to \mathbb{Z} \cup \{\infty\}$ through a somewhat elaborate procedure. In the case of toric varieties, we have seen that the tropical linear space associated to this valuation equals the tropicalisation of an associated rational linear space relative to the p-adic valuation on $\mathbb{Q}$; see Subsection 5.1. A natural question is whether the Lindström valuation also has a similar direct interpretation for general varieties, or at least for other specific classes of varieties. Shortly after the first version of this paper appeared on `arXiv`, Dustin Cartwright established an alternative construction of ν^X which will likely be very useful in this regard: for any basis B of $M(X)$, $\nu^X(B)$ equals the logarithm with base p of the *inseparable degree* of $K(x_i : i \in B)$ in $K(X)$; that is

$$\nu^X(B) = \log_p[K(X) : K(x_i : i \in B)^{sep}]$$

where $K(x_i : i \in B)^{sep}$ denotes the separable closure of $K(x_i : i \in B)$ in $K(X)$ (see [12, Ch. V]). Cartwright has described his construction of ν^X, together with a direct proof that this gives a matroid valuation of $M(X)$, in [3].

Frobenius flocks are a special case of flocks of vector spaces over a field equipped with an automorphism playing the role of the Frobenius map. In a forthcoming paper, we develop the structure theory of such vector space flocks: contraction, deletion, and duality, as well as circuit hyperplane relaxations. In a more computational direction, we plan to develop an algorithm for computing the Lindström valuation from an algebraic variety given by its prime ideal.

Our research raises many further questions. One of the most tantalising is to what extent one can bound the locus of Lindström valuations of algebraic matroids inside the corresponding Dressian—good upper bounds of this type might shed light on the number of algebraic matroids compared to the number of all matroids.

References

[1] Aner Ben-Efraim. Secret-sharing matroids need not be algebraic. *Discrete Math.*, 339(8):2136–2145, 2016.

[2] Armand Borel. *Linear algebraic groups. 2nd enlarged ed.* New York etc.: Springer-Verlag, 2nd enlarged ed. edition, 1991.

[3] Dustin Cartwright. Construction of the Lindström valuation of an algebraic extension. Preprint, available on arXiv:1704.08671, 2017.

[4] David Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms.* Undergraduate Texts in Mathematics. Springer, New York, third edition, 2007. An introduction to computational algebraic geometry and commutative algebra.

[5] Andreas W. M. Dress and Walter Wenzel. Valuated matroids. *Adv. Math.*, 93(2):214–250, 1992.

[6] Gary Gordon. Algebraic characteristic sets of matroids. *J. Combin. Theory Ser. B*, 44(1):64–74, 1988.

[7] Simon Hampe. Tropical linear spaces and tropical convexity. *Electron. J. Combin.*, 22(4):Paper 4.43, 20, 2015.

[8] Winfried Hochstättler. About the Tic-Tac-Toe matroid. Technical Report 97.272, Universität zu Köln, Angewandte Mathematik und Informatik, 1997.
[9] A. W. Ingleton. Representation of matroids. In *Combinatorial Mathematics and its Applications (Proc. Conf., Oxford, 1969)*, pages 149–167. Academic Press, London, 1971.
[10] Franz J. Király, Zvi Rosen, and Louis Theran. Algebraic matroids with graph symmetry. Preprint, available on arXiv:1312.3777, 2013.
[11] Thomas Lam and Alexander Postnikov. Alcoved polytopes. I. *Discrete Comput. Geom.*, 38(3):453–478, 2007.
[12] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.
[13] Bernt Lindström. On the algebraic characteristic set for a class of matroids. *Proc. Amer. Math. Soc.*, 95(1):147–151, 1985.
[14] Kazuo Murota. *Discrete convex analysis*. SIAM Monographs on Discrete Mathematics and Applications. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 2003.
[15] James Oxley. *Matroid theory*, volume 21 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, second edition, 2011.
[16] Rudi Pendavingh and Stefan van Zwam. Confinement of matroid representations to subsets of partial fields. *J. Combin. Theory Ser. B*, 100(6):510–545, 2010.
[17] Zvi Rosen. Computing algebraic matroids. Preprint, available on arXiv:1403.8148, 2014.
[18] Alexander Schrijver. *Combinatorial optimization. Polyhedra and efficiency. Vol. B*, volume 24 of *Algorithms and Combinatorics*. Springer-Verlag, Berlin, 2003. Matroids, trees, stable sets, Chapters 39–69.
[19] Igor R. Shafarevich. *Basic algebraic geometry. 1: Varieties in projective space. Transl. from the Russian by Miles Reid. 2nd, rev. and exp. ed.* Berlin: Springer-Verlag, 2nd, rev. and exp. ed. edition, 1994.
[20] David E. Speyer. Tropical linear spaces. *SIAM J. Discrete Math.*, 22(4):1527–1558, 2008.
[21] Bernd Sturmfels. On the decidability of diophantine problems in combinatorial geometry. *Bull. Am. Math. Soc., New Ser.*, 17:121–124, 1987.
[22] Bartel Leendert van der Waerden. *Moderne Algebra*. J. Springer, Berlin, 1940.
[23] Hassler Whitney. On the Abstract Properties of Linear Dependence. *Amer. J. Math.*, 57(3):509–533, 1935.

(Guus P. Bollen) Department of Mathematics and Computer Science, Eindhoven University of Technology, P.O. Box 513, 5600 MB Eindhoven, The Netherlands
E-mail address: g.p.bollen@tue.nl

(Jan Draisma) Mathematical Institute, University of Bern, Sidlerstrasse 5, 3012 Bern, Switzerland; and Eindhoven University of Technology, The Netherlands
E-mail address: jan.draisma@math.unibe.ch

(Rudi Pendavingh) Department of Mathematics and Computer Science, Eindhoven University of Technology, P.O. Box 513, 5600 MB Eindhoven, The Netherlands
E-mail address: r.a.pendavingh@tue.nl