MATROIDS OVER HYPERFIELDS

MATTHEW BAKER

Abstract. We present an algebraic framework which simultaneously generalizes the notion of linear subspaces, matroids, valuated matroids, and oriented matroids, as well as complex matroids in the sense of Anderson-Delucchi. We call the resulting objects *matroids over hyperfields*. We give "cryptomorphic" axiom systems for such matroids in terms of circuits, Grassmann-Plücker functions, and dual pairs, and establish some basic duality theorems. For idempotent semifields and certain other hyperfields equipped with extra structure, we give a cryptomorphic description of matroids analogous to the vector axioms for (usual) matroids.

1. Introduction

Matroid theory is a remarkably rich part of combinatorics with links to algebraic geometry, optimization, and many other areas of mathematics. Matroids provide a useful abstraction of the notion of linear independence in vector spaces, and can be thought of as combinatorial analogues of linear subspaces of K^m, where K is a field. A key feature of matroids is that they possess a duality theory which abstracts the concept of orthogonal complementation from linear algebra. There are a number of important enhancements of the notion of matroid, including oriented matroids, valuated matroids, and complex matroids in the sense of Anderson-Delucchi. In this paper, we provide a simple algebraic framework for unifying of all of these enhancements, introducing what we call **matroids over hyperfields**.

1.1. Hyperfields.

A (commutative) **hyperring** is an algebraic structure akin to a commutative ring but where addition is allowed to be multivalued. There is still a notion of additive inverse, but rather than requiring that x plus $-x$ equals 0, one merely assumes that 0 *belongs to the set* x plus $-x$. A hyperring in which every nonzero element has a multiplicative inverse is called a **hyperfield**.

Multivalued algebraic operations might seem exotic, but in fact hyperrings and hyperfields appear quite naturally in a number of mathematical settings and their properties have been explored by numerous authors in recent years.

The simplest hyperfield which is not a field is the so-called **Krasner hyperfield** $\mathbb{K}$, which as a multiplicative monoid consists of 0 and 1 with the usual multiplication rules. (This monoid is often denoted $\mathbb{F}_1$ in the algebraic geometry literature.) The addition law is almost the usual one as well, except that 1 plus 1 is defined to be the *set* $\{0, 1\}$. Our definition of matroids over hyperfields will be such that a matroid over $\mathbb{K}$ turns out to be the same thing as a matroid in the usual sense.

A field K can trivially be considered as a hyperfield, and with our definitions a matroid over K will be the same thing as a linear subspace of K^m for some positive integer m.

Date: January 7, 2016.

The author's research was supported by the National Science Foundation research grant DMS-1529573.

Some other hyperfields of particular interest are as follows (we write $x \boxplus y$ for the sum of x and y to emphasize that the sum is a set and not an element):

- (Hyperfield of signs) Let $\mathbf{S} := \{0, 1, -1\}$ with the usual multiplication law and hyperaddition defined by $1 \boxplus 1 = \{1\}$, $-1 \boxplus -1 = \{-1\}$, $x \boxplus 0 = 0 \boxplus x = \{x\}$, and $1 \boxplus -1 = -1 \boxplus 1 = \{0, 1, -1\}$. Then $\mathbf{S}$ is a hyperfield, called the **hyperfield of signs**.
- (Tropical hyperfield) Let $\mathbf{T} := \mathbf{R} \cup \{-\infty\}$, and for $a, b \in \mathbf{T}$ define their product by the rule $a \odot b := a + b$. Addition is defined by setting $a \boxplus b = \max(a, b)$ if $a \neq b$ and $a \boxplus b = \{c \in \mathbf{T} \mid c \leq a\}$ if $a = b$. Thus 0 is a multiplicative identity element, $-\infty$ is an additive identity, and $\mathbf{T}$ is a hyperfield called the **tropical hyperfield**. O. Viro has illustrated the utility of the hyperfield $\mathbf{T}$ for the foundations of tropical geometry in several interesting papers (see e.g. [Vir10, Vir11]); we mention in particular that 0 belongs to the hypersum $a_1 \boxplus \cdots \boxplus a_n$ of $a_1, \ldots, a_n \in \mathbf{T}$ $(n \geq 2)$ if and only if the maximum of the a_i occurs at least twice.
- (Phase hyperfield) Let $\mathbf{P} := S^1 \cup \{0\}$, where S^1 denotes the complex unit circle. Multiplication is defined as usual (so corresponds on S^1 to addition of phases). The hypersum $x \boxplus y$ of nonzero elements x, y is defined to be $\{0, x, -x\}$ if $y = -x$, and otherwise to consist of all points in the shorter of the two arcs of S^1 connecting x and y. Then $\mathbf{P}$ is a hyperfield, called the **phase hyperfield**.

With our general definition of matroid over a hyperfield, we will find that:

- A matroid over $\mathbf{S}$ is the same thing as an **oriented matroid** in the sense of Bland–Las Vergnas [BLV78].
- A matroid over $\mathbf{T}$ is the same thing as a **valuated matroid** in the sense of Dress–Wenzel [DW92].
- A matroid over $\mathbf{P}$ is the same thing as a **complex matroid** in the sense of Anderson–Delucchi [AD12].

Thus the notion of matroids over a hyperfield is general enough to include not only classical linear subspaces and matroids in the usual sense, but also the three different flavors of enhanced matroids above. What is particularly noteworthy is that matroids over hyperfields are also sufficiently specific that one can prove a number of non-trivial theorems about them; for example, they admit a duality theory which generalizes the existing duality theories in each of the above examples. All known proofs of the basic duality theorems for oriented (resp. valuated, complex) matroids are rather long and involved (not to mention tricky). One of our goals is to give a unified treatment of all of these duality results so that one only has to do the hard work once.

1.2. **Cryptomorphic axiomatizations.** Matroids famously admit a number of "cryptomorphic" descriptions, meaning that there are numerous axiom systems for them which turn out to be non-obviously equivalent. Two of the most useful cryptomorphic axiom systems for matroids (resp. oriented, valuated, complex matroids) are the descriptions in terms of *circuits* (resp. signed, valuated circuits, phased circuits) and *basis exchange axioms* (resp. chirotopes, valuated bases, phirotopes). A third (less well-known but also very useful) cryptomorphic description in all of these contexts involves *dual pairs*. We generalize all of these cryptomorphic descriptions with a single set of theorems and proofs. The proof of the duality theorem utilizes the equivalence of these different descriptions.

The circuit description of matroids over hyperfields is a bit technical to state, see §3 for the precise definition. Roughly speaking, though, if F is a hyperfield, a subset $\mathcal{C}$ of F^m not containing the zero-vector is the set of **circuits of a matroid with coefficients in** F (or just an F-matroid, for short) if it is stable under scalar multiplication, satisfies a support-minimality condition, and obeys a *modular elimination law*. (The **support** of $X \in \mathcal{C}$ is the set of all i such that $X_i \neq 0$.) The "modular elimination" property means that if the supports of $X, Y \in \mathcal{C}$ are "sufficiently close" (in a precise poset-theoretic sense) and $X_i = -Y_i$ for some i, then one can find a "quasi-sum" $Z \in \mathcal{C}$ with $Z_i = 0$ and $Z_j \in X_j \boxplus Y_j$ for all j. The underlying idea is that the circuits of an F-matroid behave like the set of support-minimal vectors in a linear subspace of a vector space. The most subtle part of the definition is the restriction that the supports of X and Y be sufficiently close; this restriction is not encountered "classically" when working with matroids, oriented matroids, or valuated matroids, but it is necessary in the general context in which we work, as has already been demonstrated by Anderson and Delucchi in their work on complex matroids [AD12]. They give an example of a complex matroid which satisfies modular elimination but not a more robust elimination property.

In the general context of matroids over hyperfields, the simplest and most useful way to state the "basis exchange" or chirotope / phirotope axioms is in terms of what we call *Grassmann-Plücker functions*. A nonzero function $\varphi : F^r \to F$ is called a **Grassmann-Plücker function** if it is alternating and satisfies (hyperfield analogues of) the basic algebraic identities satisfied by the determinants of the $(r \times r)$-minors of an $r \times m$ matrix of rank r (see §3.3 for a precise definition). By a rather non-obvious construction, the definition of F-matroids in terms of circuits turns out to be cryptomorphically equivalent to the definition in terms of Grassmann-Plücker functions. One can think of a Grassmann-Plücker function as a point on a hyperfield-scheme analogous to the Grassmannian variety $G(r, m)$ (c.f. §3.4).

The "dual pair" description of F-matroids is perhaps the easiest one to describe in a non-technical way, assuming that one already knows what a matroid is. If $\underline{M}$ is a matroid in the usual sense, we call a (pairwise support-incomparable) subset $\mathcal{C}$ of F^m an **F-signature** of $\underline{M}$ if the support of $\mathcal{C}$ in $E = \{1, \ldots, m\}$ is the set of circuits of $\underline{M}$. The **inner product** of two vectors $X, Y \in F^m$ is $X \odot Y := \boxplus_{i=1}^m X_i \odot Y_i$, and we call X and Y **orthogonal** (written $X \perp Y$) if $0 \in X \odot Y$. A pair $(\mathcal{C}, \mathcal{D})$ consisting of an F-signature $\mathcal{C}$ of $\underline{M}$ and an F-signature $\mathcal{D}$ of the dual matroid $\underline{M}^*$ is called a **dual pair** if $X \perp Y$ for all $X \in \mathcal{C}$ and $Y \in \mathcal{D}$. By a rather complex chain of reasoning, it turns out that an F-matroid in either of the above two senses is equivalent to a dual pair $(\mathcal{C}, \mathcal{D})$ as above.

1.3. **Duality and functoriality.** If $\mathcal{C}$ is the collection of circuits of an F-matroid M and $(\mathcal{C}, \mathcal{D})$ is a dual pair of F-signatures of the matroid $\underline{M}$ underlying M (whose circuits are the supports of the circuits of M), it turns out that $\mathcal{D}$ is precisely the set of (non-empty) support-minimal elements of the orthogonal complement of $\mathcal{C}$ in F^m, and $\mathcal{D}$ forms the set of circuits of a F-matroid M^* which we call the **dual F-matroid**. Duality behaves as one would hope: for example $M^{**} = M$, duality is compatible in the expected way with the notions of deletion and contraction, and the underlying matroid of the dual is the dual of the underlying matroid.

Matroids over hyperfields admit a useful push-forward operation: given a hyperfield homomorphism $f : F \to F'$ and an F-matroid M, there is an induced F'-matroid f_*M which can be defined using any of the cryptomorphically equivalent axiomatizations. The "underlying matroid" construction coincides with the push-forward of an F-matroid M to the

Krasner hyperfield $\mathbb{K}$ (which is a final object in the category of hyperfields) via the canonical homomorphism $\psi : F \to \mathbb{K}$. If $\sigma : \mathbb{R} \to \mathbb{S}$ is the map taking a real number to its sign and $W \subseteq \mathbb{R}^m$ is a linear subspace (considered in the natural way as an $\mathbb{R}$-matroid), the push-forward $\sigma_*(W)$ coincides with the oriented matroid which one traditionally associates to W. Similarly, if $v : K \to \mathbb{T}$ is the valuation on a non-Archimedean field and $W \subseteq K^m$ is a linear subspace, $v_*(W)$ is just the **tropicalization** of W considered as a *valuated matroid* (c.f. [MS15]). There is a similar story for complex matroids and the natural "phase map" $p : \mathbb{C} \to \mathbb{P}$.

1.4. **Vector axioms.** It would be nice if, instead of generalizing the notion of "support-minimal elements of a linear subspace of K^m", one could directly generalize the notion of a linear subspace itself. This is the point of the *vector axioms* in matroid theory, which also appear in the context of oriented and valuated matroids. Despite the appeal of this point of view, there seems to be no workable cryptomorphic axiomatization of matroids over hyperfields in terms of vectors. For one thing, a vector is usually defined as a finite sum of circuits, and such a notion of "sum" does not exist for hyperfields. An even more serious problem is the example from [AD12] of linear subspaces W_1, W_2 of $\mathbb{C}^m$ whose associated complex matroids (= push-forwards via $p : \mathbb{C} \to \mathbb{P}$) are the same, but such that $p(W_1) \neq p(W_2)$. (In any reasonable theory of vectors, one would like the set of vectors associated to the push-forward $f_*(W)$ of a linear subspace to be the image of W under f.)

Having voiced these objections, there are certainly many interesting examples of hyperfields where one *does* have a natural notion of (single-valued) sum, for example in $\mathbb{K}$ or $\mathbb{T}$ (where one can define $a \oplus b := \max\{a, b\}$) or more generally any idempotent semifield. In order to include examples like $\mathbb{S}$ and classical fields as well, we axiomatize the existence of a suitable sum operation $\oplus$ which is "compatible" with the hyperaddition $\boxplus$. We call the resulting algebraic structure a **partial demifield**. (The adjective "partial" makes the definition a bit awkward but is necessary if we want to include $\mathbb{S}$, since there is no way to define $1 \oplus (-1)$ in $\mathbb{S}$ so that the resulting binary operation $\oplus$ on $\mathbb{S}$ is both commutative and associative, and we would rather not give up on those properties in the present context.) As the actual definition is a bit technical, we refer the reader to §4.

If F is a demifield (meaning that $a \oplus b$ is always defined), we define a subset V of F^m to be a **linear subspace** if it contains 0, is closed under $\oplus$ and scalar multiplication, is generated by its elements of nonzero minimal support, and satisfies the *vector elimination axiom* that if $X, Y \in V$ and $X_i = -Y_i$, there exists $Z \in V$ such that $Z_i = 0$ and $Z_j \in X_j \boxplus Y_j$ for all j. In the case of partial demifields, there is a similar but more technical definition of what it means to be a linear subspace of F^m. We call a partial demifield P for which the notion of linear subspace is cryptomorphically equivalent to the notion of F-matroid for the hyperfield F underlying P **vectorial**. It turns out that P is vectorial in each of the following examples:

- $P = K$ is a field.
- $P = \mathbb{S}$ is the partial demifield of signs.
- P arises from an idempotent semifield S (such as $\mathbb{K}$ or $\mathbb{T}$).

We also give an example of a non-vectorial partial demifield.

The vector axioms are nice because they capture the intuition that a linear space over, say, an idempotent semifield S should be more than just an S-submodule of S^m (stable under $\odot$ and $\oplus$); it should also admit a limited "subtraction" operation. The point is that general S-submodules of S^m can be rather nasty; for example, there does not appear to be a reasonable notion of *dimension* for them, nor a theory of bases or duality. However, once we impose the magical *vector elimination axiom*, which serves as a partial substitute for the lack of subtraction, we suddenly get a notion of dimension (the rank of the underlying matroid), duality theory, and more.

A particularly interesting class of partial demifields are the so-called *partial fields* of Semple and Whittle [SW96], whose connection to matroid theory has been studied in detail by Pendavingh and van Zwam [PvZ10, PvZ13]. There are several interesting theorems in the literature characterizing certain well-known families of matroids, such as regular or dyadic matroids, in terms of representability over a particular partial field. We show that the notion of representability over partial fields can be generalized to the setting of partial demifields via the vector axioms discussed above.

1.5. **Related work.** While we believe our point of view in this paper to be original, and hopefully in the set {important, interesting, useful} as well, we should certainly point out that the idea of unifying various flavors of matroids via an "exotic" algebraic structure is not a new one. Indeed, in [Dre86] Andreas Dress introduced the notion of a **fuzzy ring** and defined matroids over such a structure, showing that linear subspaces, matroids in the usual sense, and oriented matroids are all examples of matroids over a fuzzy ring. In [DW92], Dress and Wenzel introduced the notion of *valuated matroids* as a special case of matroids over a fuzzy ring. The results of Dress and Wenzel in [Dre86, DW91, DW92] include a duality theorem and a cryptomorphic characterization of matroids over fuzzy rings in terms of Grassmann-Plücker functions. (They also work with possibly infinite ground fields, whereas for simplicity we restrict ourselves to the finite case.) However, we believe our work has some important advantages over the Dress–Wenzel theory, including:

- The notion of hyperfield is arguably simpler and more natural than the notion of a fuzzy ring. A less subjective variant of this assertion is the observation that, according to *MathSciNet*, very few authors besides Dress and Wenzel themselves have studied or used their notion of fuzzy ring, whereas there are dozens of papers in the literature concerned with hyperfields (including the recent interesting work of Connes–Consani [CC10, CC11] and Jun [Jun15a, Jun15b]).
- Dress and Wenzel do not give cryptomorphic axioms for matroids over fuzzy rings in terms of circuits or dual pairs. Circuits, in particular, are quite fundamental to matroid theory, so this appears to be an important bit of unfinished business in the Dress–Wenzel theory.
- From a pedagogical point of view, the complexity inherent in the definition of a fuzzy ring and the generality in which Dress and Wenzel work makes their papers challenging to read. We hope that our theory will help some readers rediscover and perhaps make connections with the somewhat overlooked work of Dress–Wenzel. We confess that we have not been able to understand the definition of fuzzy rings well enough to determine what the precise relationship with hyperrings and hyperfields might be.)

We should also point out that, while the proofs of our main theorems are somewhat long and technical, in principle almost all of the hard work has already been done and it is mostly a matter of pointing out that certain existing arguments in the literature go through *mutatis mutandis* in the general setting of matroids over hyperfields. So the main innovation of the present paper is really in finding the right definitions; after that, anyone sufficiently patient and familiar with the relevant literature on matroid theory could presumably figure out how to adapt the existing proofs to the present context. In particular, the arguments in [AD12] go through largely unchanged; complex matroids behave sufficiently like "general F-matroids" that their proofs typically work in our setting. (That being said, a few small but important changes are necessary, and there are some errors in *loc. cit.* which might lead a casual reader astray; we have collected the most important of these errata in an Appendix.) By way of contrast, the proofs in the standard works on oriented and valuated matroids tend to rely on special properties of the corresponding hyperfields which do not readily generalize.

Despite the formal similarity in their titles, the theory in this paper generalizes matroids in a rather different way from the paper "Matroids over a Ring" by Fink and Moci [FM15]. For example, if K is any field, a matroid over K in the sense of Fink–Moci is just a matroid in the usual sense (independent of K), while for us a matroid over K is a linear subspace of K^m. The work of Fink–Moci generalizes, among other things, the concept of *arithmetic matroids*, which we do not discuss. It is possible that there is a Grand Unified Theory of matroids over hyperrings which encompasses both points of view, but we have not given this matter serious thought. In principle, we could formulate many of the definitions in this paper over *hyperrings*, and not just over hyperfields, but we do not know how to say anything useful in this general context so we restrict ourselves to the case where we're actually able to prove theorems.

The thesis of Bart Frenk [Fre13] deals with matroids over certain kinds of algebraic objects which he calls tropical semifields; these are defined as sub-semifields of $\mathbb{R} \cup \{\infty\}$. Matroids over tropical semifields include, as special cases, both matroids in the traditional sense and valuated matroids, but not for example oriented matroids, linear subspaces of K^m for a field K, or complex matroids. Tropical semifields are a particular special case of idempotent semifields, and matroids over the latter are the subject of an interesting recent paper by the Giansiracusa brothers [GG15]. They characterize matroids over idempotent semifields in a way which is unlikely to generalize to the present setting of hyperfields.

1.6. **A brief chronology.** As a historical note, it is perhaps worth mentioning that I came up with the idea of unifying matroids, linear subspaces, oriented matroids, and valuated matroids via matroids over hyperfields independently of the work of Dress–Wenzel and Anderson–Delucchi. I was trying to better understand valuated matroids because of some applications to tropical geometry which Ravi Vakil and I had in mind, and for completely different reasons I was also thinking at that time about oriented matroids. I was struck by the formal similarities but subtle differences in the two theories, and I felt sure there must be a common framework.

I had some useful conversations on the subject with experts like Felipe Rincon and Eric Katz at IMPA in June 2015, but was not satisfied with the current state of knowledge as they explained it to me. I realized in July 2015 that the key to unifying things should be to allow a multivalued addition law. A Google search revealed a relatively extensive literature on hyperstructures, and in particular the work of Viro [Vir10, Vir11], Connes–Consani [CC10, CC11], and Jun [Jun15a, Jun15b], which together made me rather excited about the theory of hyperrings and hyperfields and its potential to do exactly what I wanted. However, when I tried to prove a duality theorem in this context and formulate various cryptomorphic axioms for F-matroids, I got stuck numerous times and found it tricky to nail down the right definitions which would make everything work; the proofs in the book [BLVS+99] and the paper [MT01] just didn't seem to go through in the generality that I needed. I could see that there was a subtle problem generalizing the circuit axioms to this framework, but didn't know what the fix should be.

This was a rather big headache until, more or less by accident, I discovered the paper of Anderson and Delucchi [AD12]. When my progress stalled, I had decided to look at more examples, turning once again to Google to see what other flavors of matroids were out there. Again the Internet did not disappoint: when I discovered the notion of complex matroids in the sense of [AD12] and saw the modular elimination axiom in their paper, I quickly realized that this was the missing ingredient I had been searching for. At that point I was able to formulate the correct definitions and theorems, and realized that the majority of the proofs in [AD12] would go through as well. As I worked through the (rather intricate) details, I looked up the paper of Dress and Wenzel which Anderson and Delucchi cite in their bibliography and realized, somewhat to my surprise, that these authors had already discovered a unified notion of matroid 20+ years earlier encompassing what I originally had in mind. As I discuss above, though, there are several reasons why the work of Dress–Wenzel does not make the theory in this paper obsolete or uninteresting.

I would like to conclude this section by quoting from Viro's paper [Vir10]:

> Krasner, Marshall, Connes and Consani and the author came to hyperfields for different reasons, motivated by different mathematical problems, but we came to the same conclusion: the hyperrings and hyperfields are great, very useful and very underdeveloped in the mathematical literature...I believe the taboo on multivalued maps has no real ground, and eventually will be removed. Hyperfields, as well as multigroups, hyper- rings and multirings, are legitimate algebraic objects related in many ways to the classical core of mathematics.

Given that I came to study hyperfields independently of the other authors that Viro mentions, and for yet different reasons, I share Viro's feeling that they should be viewed as fundamental mathematical objects. I also share his view that they suit the foundations of tropical geometry better than (idempotent) semifields. On the other hand, I am not convinced that hyperrings are the correct algebraic structure on which to base a general geometric theory; Oliver Lorscheid's theory of ordered blueprints [Lor15] appears perhaps better suited for this purpose (see Remark 3.15 below and also [Jun15a]).

1.7. **Structure of the paper.** We define hyperfields in Section 2 and discuss some key examples. In Section 3 we present different axiom systems for matroids over hyperfields, formulate a result saying that they are all cryptomorphically equivalent, and state the main results of duality theory. Proofs of the main theorems are deferred to Section 6. Vector axioms and partial demifields are discussed in Section 4. Section 5 contains the definition of hyperfield homomorphisms along with a discussion of the push-forward operations on F-matroids and linear spaces over partial demifields. There is a brief Appendix at the end of the paper collecting some errata from [AD12].

1.8. **Acknowledgments.** I thank Felipe Rincon and Eric Katz for pointing out the key differences between valuated and oriented matroids, Ravi Vakil and Oliver Lorscheid for useful conversations on hyperstructures, and Laura Anderson and Emanuele Delucchi for writing their paper, the discovery of which saved me a lot of work. Thanks also to Eric Katz and Robin Thomas for pointing me toward the papers [PvZ10, PvZ13].

2. Hyperstructures

2.1. **Basic definitions.** A hypergroup (reps. hyperring, hyperfield) is an algebraic structure similar to a group (resp. ring, field) except that addition is multivalued. More precisely, addition is a *hyperoperation* on R, i.e., a map from $R \times R$ to the collection of non-empty subsets of R. All hypergroups and hyperrings in this paper will be *commutative*. For more on hyperstructures, see for example [CC11] and [Jun15b, Appendix B].

Definition 2.1. A (commutative) **hypergroup** is a tuple $(G, \boxplus, 0)$, where $\boxplus$ is a commutative and associative hyperoperation on G such that:

- (H0) $0 \boxplus x = \{x\}$ for all $x \in G$.
- (H1) For every $x \in G$ there is a unique element of G (denoted $-x$ and called the **hyperinverse** of x) such that $0 \in x \boxplus -x$.

For $m \geq 2$ and $x_1, \ldots, x_m \in G$, we define the hypersum $x_1 \boxplus \cdots \boxplus x_m$ recursively by the formula

$$x_1 \boxplus \cdots \boxplus x_m := \bigcup_{x' \in x_2 \boxplus \cdots \boxplus x_m} x_1 \boxplus x'.$$

The following is left as an exercise for the reader:

Lemma 2.2. *If G is a hypergroup and $x, y, z \in G$, then:*

1. *$x \in y \boxplus z$ if and only if $z \in x \boxplus (-y)$.*
2. *$0 \in x \boxplus y \boxplus z$ if and only if $-z \in x \boxplus y$.*

Definition 2.3. A (commutative) **hyperring** is a tuple $(R, \odot, \boxplus, 1, 0)$ such that:

- $(R, \odot, 1)$ is a commutative semigroup.
- $(R, \boxplus, 0)$ is a a commutative hypergroup.
- (Absorption rule) $0 \odot x = x \odot 0 = 0$ for all $x \in R$.
- (Distributive Law) $a \odot (x \boxplus y) = (a \odot x) \boxplus (a \odot y)$ for all $a, x, y \in R$.

As usual, we will denote a hyperring by its underlying set R when no confusion will arise. Note that any commutative ring R with 1 may be considered in a trivial way as a hyperring. We will sometimes write xy (resp. x/y) instead of $x \odot y$ (resp. $x \odot y^{-1}$) if there is no risk of confusion.

Remark 2.4. Let A be a multiplicative semigroup, let R be a commutative ring with 1, and let $\phi : R \twoheadrightarrow A$ be a surjective homomorphism of multiplicative semigroups such that $\phi^{-1}(0) = \{0\}$. The *induced hyperring structure* on A is defined by the hyperaddition law

$$x \boxplus y := \phi(\phi^{-1}(x) + \phi^{-1}(y)).$$

In particular, if R is a commutative ring with 1 and G is a subgroup of the group $R^\times$ of units in R, then the set R/G of orbits for the action of G on R by multiplication has a natural hyperring structure (cf. [CC11, Proposition 2.5]).

Definition 2.5. A hyperring F is called a **hyperfield** if $0 \neq 1$ and every non-zero element of F has a multiplicative inverse.

2.2. **Examples.** We now give some examples of hyperfields which will be important to us in the sequel.

Example 2.6. (Fields) If $F = K$ is a field, then F can be trivially considered as a hyperfield by setting $a \oplus b = a \cdot b$ and $a \boxplus b = a + b$.

Example 2.7. (Krasner hyperfield) Let $\mathbf{K} = \{0, 1\}$ with the usual multiplication rule, but with hyperaddition defined by $0 \boxplus x = x \boxplus 0 = \{x\}$ for $x = 0, 1$ and $1 \boxplus 1 = \{0, 1\}$. Then $\mathbf{K}$ is a hyperfield, called the **Krasner hyperfield** by Connes and Consani in [CC11]. This is the hyperfield structure on $\{0, 1\}$ induced (in the sense of Remark 2.4) by the field structure on F, for any field F, with respect to the trivial valuation $v : F \to \{0, 1\}$ sending 0 to 0 and all non-zero elements to 1.

Example 2.8. (Tropical hyperfield) Let $\mathbf{T}_+ := \mathbf{R} \cup \{-\infty\}$, and for $a, b \in \mathbf{T}_+$ define $a \cdot b = a + b$ (with $-\infty$ as an absorbing element). The hyperaddition law is defined by setting $a \boxplus b = \{\max(a, b)\}$ if $a \neq b$ and $a \boxplus b = \{c \in \mathbf{T}_+ \mid c \leq a\}$ if $a = b$. (Here we use the standard total order on $\mathbf{R}$ and set $-\infty \leq x$ for all $x \in \mathbf{R}$.) Then $\mathbf{T}_+$ is a hyperfield, called the **tropical hyperfield**. The additive hyperidentity is $-\infty$ and the multiplicative identity is 0. Because it can be confusing that $0, 1 \in \mathbf{R}$ are not the additive (resp. multiplicative) identity elements in $\mathbf{T}_+$, we will work instead with the isomorphic hyperfield $\mathbf{T} := \mathbf{R}_{\geq 0}$ in which $0, 1 \in \mathbf{R}$ are the additive (resp. multiplicative) identity elements and multiplication is the usual multiplication. Hyperaddition is defined so that the map $\exp : \mathbf{T}_+ \to \mathbf{T}$ is an isomorphism of hyperfields.

Example 2.9. (Valuative hyperfields) More generally, if Γ is any totally ordered abelian group (written multiplicatively), there is a canonical hyperfield structure on $\Gamma \cup \{0\}$ defined in a similar way as for $\mathbf{T}$. The hyperfield structure on $\Gamma \cup \{0\}$ is induced from that on F by $\|\cdot\|$ for any surjective norm $\|\cdot\| : F \twoheadrightarrow \Gamma \cup \{0\}$ on a field F. We call a hyperfield which arises in this way a *valuative hyperfield*. In particular, both $\mathbf{K}$ and $\mathbf{T}$ are valuative hyperfields.

Example 2.10. (Hyperfield of signs) Let $\mathbf{S} := \{0, 1, -1\}$ with the usual multiplication law, and hyperaddition defined by $1 \boxplus 1 = \{1\}$, $-1 \boxplus -1 = \{-1\}$, $x \boxplus 0 = 0 \boxplus x = \{x\}$, and $1 \boxplus -1 = -1 \boxplus 1 = \{0, 1, -1\}$. Then $\mathbf{S}$ is a hyperfield, called the **hyperfield of signs**. The underlying multiplicative monoid of $\mathbf{S}$ is sometimes denoted by $\mathbf{F}_{1^2}$. The hyperfield structure on $\{0, 1, -1\}$ is induced from that on $\mathbf{R}$ by the map $\sigma : \mathbf{R} \to \{0, 1, -1\}$ taking 0 to 0 and a nonzero real number to its sign.

Example 2.11. (Phase hyperfield) Let $\mathbf{P} := S^1 \cup \{0\}$, where $S^1 = \{z \in \mathbf{C} \mid |z| = 1\}$ is the complex unit circle. Multiplication is defined as usual, and the hyperaddition law is defined for $x, y \neq 0$ by setting $x \boxplus -x := \{0, x, -x\}$ and $x \boxplus y := \{\frac{\alpha x + \beta y}{\|\alpha x + \beta y\|} \mid \alpha, \beta \in \mathbf{R}_{>0}\}$ otherwise. The hyperfield structure on $S^1 \cup \{0\}$ is induced from that on $\mathbf{C}$ by the map $p : \mathbf{R} \to S^1 \cup \{0\}$ taking 0 to 0 and a nonzero complex number z to its phase $z/|z| \in S^1$.

Many other interesting examples of hyperstructures are given in Viro's papers [Vir10, Vir11] and the papers [CC10, CC11] of Connes and Consani. Here are a couple of examples taken from these papers:

Example 2.12. (Triangle hyperfield) Let Δ be the set $\mathbb{R}_{\geq 0}$ of nonnegative real numbers with the usual multiplication and the hyperaddition rule

$$a \boxplus b := \{c \in \mathbb{R}_{\geq 0} \ : \ |a - b| \leq c \leq a + b\}.$$

(In other words, $a \boxplus b$ is the set of all real numbers c such that there exists a Euclidean triangle with side lengths a, b, c.) Then Δ is a hyperfield, closely related to the notion of *Litvinov-Maslov dequantization* (c.f. [Vir10, §9]).

Example 2.13. (Adèle class hyperring) If K is a global field and A_K is its ring of adèles, the commutative monoid A_K/K^* (which plays an important role in Connes' conjectural approach to proving the Riemann hypothesis) is naturally endowed with the structure of a hyperring by Remark 2.4. It is, moreover, an algebra over the Krasner hyperfield $\mathbb{K}$ in a natural way. One of the interesting discoveries of Connes and Consani [CC11] is that if K is the function field of a curve C over a finite field, the groupoid of prime elements of the hyperring A_K/K^* is canonically isomorphic to the loop groupoid of the maximal abelian cover of C.

2.3. **Modules, linear independence, and orthogonality.**

Definition 2.14. Let R be a hyperring. An R**-module** is a commutative hypergroup M together with a map $R \times M \to M$, denoted $(r, m) \mapsto r \odot m$, such that

- $0 \odot x = x \odot 0 = 0$ for all $x \in M$.
- $(a \odot b) \odot x = a \odot (b \odot x)$ for all $a, b \in R$ and $x \in M$.
- $a \odot (x \boxplus y) = (a \odot x) \boxplus (a \odot y)$ for all $a \in R$ and $x, y \in M$.
- $(a \boxplus b) \odot x = (a \odot x) \boxplus (b \odot x)$ for all $a, b \in R$ and $x \in M$, where for $A \subset R$ and $x \in M$ we define $A \odot x := \{a \odot x \mid a \in A\}$.

Example 2.15. If R is a hyperring and E is a set, the set R^E of functions from E to R with pointwise multiplication and hyperaddition is naturally an R-module. If $E = \{1, \ldots, m\}$, we sometimes write R^m instead of R^E.

The **support** of $X \in R^E$, denoted $\underline{X}$ or $\mathrm{supp}(X)$, is the set of $e \in E$ such that $X(e) \neq 0$. If $A \subset R^E$, we set $\mathrm{supp}(A) := \{\underline{X} \mid X \in A\}$ and we consider $\mathrm{supp}(A)$ as a lattice (in the poset-theoretic sense) with respect to inclusion.

The **projective space** $\mathbb{P}(R^E)$ is defined to be the set of equivalence classes of elements of R^E under the equivalence relation where $X_1 \sim X_2$ if and only if $X_1 = \alpha \odot X_2$ for some $\alpha \in R^\times$. Note that the support of $X \in R^E$ depends only on its equivalence class in $\mathbb{P}(R^E)$. We let $\pi : R^E \backslash \{0\} \twoheadrightarrow \mathbb{P}(R^E)$ denote the natural projection.

We will define linear dependence in an R-module M by the condition that 0 lies in a certain hypersum, where the hypersum of $x_1, \ldots, x_k \in M$, is defined in the evident way (see the remarks following Definition 2.1). To orient the reader, we provide some illustrative examples.

Example 2.16. If $x_1, \ldots, x_k \in \mathbf{K}$, then $0 \in x_1 \boxplus \cdots \boxplus x_k$ iff $\{i \mid x_i = 1\}$ does not have exactly one element.

Example 2.17. If $x_1, \ldots, x_k \in \mathbf{T}$, then $0 \in x_1 \boxplus \cdots \boxplus x_k$ if and only if the maximum of the x_i occurs (at least) twice, or $k = 1$ and $x_1 = 0$.

Example 2.18. If $x_1, \ldots, x_k \in \mathbf{S}$, then $0 \in x_1 \boxplus \cdots \boxplus x_k$ if and only if all $x_i = 0$ or the nonzero x_i's are not all equal.

Definition 2.19. (Linear independence) Let M be a module over the hyperring R. We say that elements $m_1, \ldots, m_k$ are **linearly dependent** if there exist $c_1, \ldots, c_k \in R$, not all 0, such that

$$0 \in (c_1 \odot m_1) \boxplus \cdots \boxplus (c_k \odot m_k).$$

Elements which are not linearly dependent are called **linearly independent**.

Example 2.20. If R is a commutative ring (resp. semiring) with 1, a module over R considered as a hyperring is the same as a module over R considered as a ring (resp. semiring). In particular, if K is a field, then a K-module (with K considered as a hyperfield) is the same as a vector space V over K, and $v_1, \ldots, v_k \in V$ are linearly (in)dependent in the sense of hyperfields if and only if they are linearly (in)dependent in the usual sense.

The following definition will play an important role in the theory of duality which we develop later in this paper.

Definition 2.21. (Orthogonality) Let R be a hyperring and let $M = R^m$, considered as an R-module. The **inner product** of $x = (x_1, \ldots, x_m)$ and $y = (y_1, \ldots, y_m)$ is defined to be the set $x \odot y := (x_1 \odot y_1) \boxplus \cdots \boxplus (x_m \odot y_m)$. We say that x, y are **orthogonal**, denoted $x \perp y$, if $0 \in x \odot y$. If $S \subseteq M$, we denote by $S^\perp$ the set of all $x \in M$ such that $x \perp y$ for all $y \in S$.

Note for later reference that the condition $x \perp y$ only depends on the equivalence classes of x, y in $\mathbb{P}(R^n)$.

3. Matroids over hyperfields

In this section, we will define what it means to be a **matroid** on a (finite) ground set E with coefficients in a hyperfield F, or (for brevity) a **matroid over** F or F**-matroid**. Our definition will be such that:

- When $F = K$ is a field, a matroid on E with coefficients in K is the same thing as a vector subspace of K^E in the usual sense.
- A matroid over $\mathbf{K}$ is the same thing as a **matroid**.
- A matroid over $\mathbf{T}$ is the same thing as a **valuated matroid** in the sense of Dress–Wenzel [DW92].
- A matroid over $\mathbf{S}$ is the same thing as an **oriented matroid** in the sense of Bland–Las Vergnas [BLV78].
- A matroid over $\mathbf{P}$ is the same thing as an **complex matroid** in the sense of Anderson–Delucchi [AD12].

See §3.8 for further details on the compatibility of our notion of F-matroid with various existing definitions in these particular examples.

3.1. Modular pairs.

As in the investigation of complex matroids by Anderson–Delucchi, a key ingredient for obtaining a robust notion of matroid in the general setting of hyperfields is the concept of *modular pairs*. We recall the definition in the general context of **lattices** following [Del11] and [AD12].

Let $(P, \leq)$ be a partially ordered set (poset). A **chain** in P is a totally ordered subset J; the **length** of a chain is $\ell(J) := |J| - 1$. The **length** of P is the supremum of $\ell(J)$ over all chains J of P.

Given $x \in P$ we write $P_{\leq x} = \{y \in P \mid y \leq x\}$ and $P_{\geq x} = \{y \in P \mid y \geq x\}$. These are sub-posets of P. Let $x, y \in P$. If the poset $P_{\geq x} \cap P_{\geq y}$ has a unique minimal element, this element is denoted $x \vee y$ and called the **join** of x and y. If the poset $P_{\leq x} \cap P_{\leq y}$ has a unique maximal element, this element is denoted $x \wedge y$ and called the **meet** of x and y. The poset P is called a **lattice** if the meet and join and defined for any $x, y \in P$.

Every finite lattice L has a unique minimal element 0 and a unique maximal element 1. An element $x \in L$ is called an **atom** if there is no $z \in L$ with $0 < z < x$. Two atoms $x, y \in L$ form a **modular pair** if $\ell(L_{\leq x \vee y}) = 2$, i.e., $x \neq y$ and there do not exist $z, z' \in L$ with $0 < z < z' < x \vee y$.

If S is any family of subsets of a set E, the set $U(S) := \{\bigcup T \mid T \subseteq S\}$ forms a lattice when equipped with the partial order coming from inclusion of sets, with meet and join corresponding to union and intersection, respectively. If the elements of S are incomparable, then every $x \in S$ is atomic as an element of $U(S)$. We say that two elements $x, y \in S$ are a **modular pair** if they are a modular pair in $U(S)$.

Our interest in modular pairs comes in part from the observation of Anderson and Delucchi that there is a nice axiomatization of *complex matroids* in terms of modular pairs of *phased circuits*, but general pairs of phased circuits do not obey circuit elimination. The following facts about modular pairs will come in quite handy:

Lemma 3.1 (c.f. [Del11]). *Let $\mathcal{C}$ be a collection of non-empty incomparable subsets of a finite set E. Then the following are equivalent:*

(1) *$\mathcal{C}$ is the set of circuits of a matroid M on E.*
(2) *Every pair C_1, C_2 of distinct elements of $\mathcal{C}$ satisfies* **circuit elimination***: if $e \in C_1 \cap C_2$ then there exists $C_3 \in \mathcal{C}$ such that $C_3 \subseteq (C_1 \cup C_2) \backslash e$.*
(3) *Every modular pair in $\mathcal{C}$ satisfies circuit elimination.*

The following lemma, which can be pieced together from [Whi87, Lemma 2.7.1] and [MT01, Lemma 4.3] (and also makes a nice exercise), might help the reader get a better feeling for the concept of modular pairs in the context of matroid theory:

Lemma 3.2. *Let M be a matroid with rank function r, and let C_1, C_2 be distinct circuits of M. Then the following are equivalent:*

(1) *C_1, C_2 are a modular pair of circuits.*
(2) $r(C_1 \cup C_2) + r(C_1 \cap C_2) = r(C_1) + r(C_2)$.
(3) $r(C_1 \cup C_2) = |C_1 \cup C_2| - 2$.
(4) *For each $e \in C_1 \cap C_2$, there is a unique circuit C_3 with $C_3 \subseteq (C_1 \cup C_2) \backslash e$, and this circuit has the property that C_3 contains the symmetric difference $C_1 \Delta C_2$.*
(5) *There are a basis B for M and a pair e_1, e_2 of distinct elements of $E \backslash B$ such that $C_1 = C(B, e_1)$ and $C_2 = C(B, e_2)$, where $C(B, e)$ denotes the fundamental circuit with respect to B and e.*

In particular, if M is the cycle matroid of a connected graph G then C_1, C_2 are a modular pair if and only if they are fundamental cycles associated to the same spanning tree T.

Note that for general circuits C_1 and C_2 in a matroid M, the **submodular inequality** asserts that $r(C_1 \cup C_2) + r(C_1 \cap C_2) \leq r(C_1) + r(C_2)$. Condition (2) of the lemma says that C_1 and C_2 form a modular pair if and only if *equality* holds in this inequality (hence the name "modular pair").

3.2. **Circuit axioms.**

Definition 3.3. Let E be a non-empty finite set and let F be a hyperfield. A **matroid** M **on** E **with coefficients in** F, or more simply an F**-matroid on** E, is a subset $\mathcal{C}$ of F^E, called the **circuits** of M, satisfying the following axioms:

- (C0) $0 \notin \mathcal{C}$.
- (C1) If $X \in \mathcal{C}$ and $\alpha \in F^\times$, then $\alpha \odot X \in \mathcal{C}$.
- (C2) [Incomparability] If $X, Y \in \mathcal{C}$ and $\underline{X} \subseteq \underline{Y}$, then there exists $\alpha \in F^\times$ such that $X = \alpha \odot Y$.
- (C3) [Modular Elimination] If $X, Y \in \mathcal{C}$ are a **modular pair of circuits** (meaning that $\underline{X}, \underline{Y}$ are a modular pair in $\mathrm{supp}(\mathcal{C})$) and $e \in E$ is such that $X(e) = -Y(e) \neq 0$, there exists a circuit $Z \in \mathcal{C}$ such that $Z(e) = 0$ and $Z(f) \in X(f) \boxplus Y(f)$ for all $f \in E$.

This is equivalent to the axiom system given in [AD12] in the case of complex matroids (i.e., when $F = \mathbf{P}$). Also, the circuit Z in (C3) is *unique*. (Both of these observations follow easily from Lemma 3.2.)

If M is a matroid over F with ground set E, there is an underlying matroid (in the usual sense) $\underline{M}$ on E whose circuits are the supports of the circuits of M. (It is straightforward, in view of Lemma 3.1, to check that the circuit axioms for a matroid are indeed satisfied.)

Definition 3.4. The *rank* of M is defined to be the rank of the underlying matroid $\underline{M}$.

A **projective circuit** of M is an equivalence class of circuits of M under the equivalence relation $X_1 \sim X_2$ if and only if $X_1 = \alpha \odot X_2$ for some $\alpha \in F^\times$. Axioms (C0)-(C2) together imply that the map from projective circuits of M to circuits of $\underline{M}$ which sends a projective circuit C to its support is a *bijection*. In particular, M has only finitely many projective circuits, and one can think of a matroid over F as a matroid $\underline{M}$ together with a function associating to each circuit $\underline{C}$ of $\underline{M}$ an element $X(\underline{C}) \in \mathbb{P}(F^E)$ such that modular elimination holds for $\mathcal{C} := \pi^{-1}(\{X(\underline{C})\})$.

Remark 3.5. [AD12, Example 6.1] gives an example of a matroid with coefficients in the hyperfield $\mathbf{P}$ whose circuits do not satisfy the following strong version of the elimination axiom:

- (C3)$'$ [Strong Elimination] If $X, Y \in \mathcal{C}$ and $X(e) = -Y(e) \neq 0$, there exists a circuit $Z \in \mathcal{C}$ such that $Z(e) = 0$ and $Z(f) \in X(f) \boxplus Y(f)$ for all $f \in E$.

We call a hyperfield F a *strong hyperfield* if every matroid M with coefficients in F satisfies the strong elimination axiom (C3)$'$. Thus the hyperfield $\mathbf{P}$ is not strong. However, many other hyperfields of interest are strong.

Example 3.6. Every field is a strong hyperfield. This follows from Example 3.19 and elementary linear algebra.

Example 3.7. The hyperfield $\mathbf{S}$ of signs is strong. This follows from Example 3.22 together with [BLVS$^+$99, Corollary 3.7.7].

Example 3.8. Every valuative hyperfield F is strong. This follows from [MT01, Proof of Lemma 4.9], which is phrased in the setting $F = \mathbf{T}$ but works *mutatis mutandis* in the general case.

3.3. **Grassmann-Plücker functions.** We now describe a cryptomorphic description of matroids over a hyperfield F in terms of **Grassmann-Plücker functions** (called "chirotopes" in the theory of oriented matroids and "phirotopes" in [AD12]). In addition to being interesting in its own right, this description will be crucial for establishing a duality theory for matroids over F.

Definition 3.9. Let E be a non-empty finite set, let F be a hyperfield, and let r be a positive integer. A **Grassmann-Plücker function of rank r on E with coefficients in F** is a function $\varphi : E^r \to F$ such that:

- (GP1) φ is not identically zero.
- (GP2) φ is alternating.
- (GP3) [Grassmann–Plücker relations] For any two subsets $\{x_1, \ldots, x_{r+1}\}$ and $\{y_1, \ldots, y_{r-1}\}$ of E,

$$0 \in \boxplus_{k=1}^{r+1} (-1)^k \varphi(x_1, x_2, \ldots, \hat{x}_k, \ldots, x_{r+1}) \odot \varphi(x_k, y_1, \ldots, y_{r-1}). \tag{3.10}$$

For example, if $F = K$ is a field and A is an $r \times m$ matrix of rank r with columns indexed by E, it is a classical fact that the function φ_A taking an r-element subset of E to the determinant of the corresponding $r \times r$ minor of A is a Grassmann-Plücker function. The function φ_A depends (up to a non-zero scalar multiple) only on the row space of A, and conversely the row space of A is uniquely determined by the function φ_A (this is equivalent to the well-known fact that the *Plücker relations* cut out the Grassmannian $G(r, m)$ as a projective algebraic set).

We say that two Grassmann-Plücker functions φ_1 and φ_2 are **equivalent** if $\varphi_1 = \alpha \odot \varphi_2$ for some $\alpha \in F^\times$.

Theorem 3.11. *Let E be a non-empty finite set, let F be a hyperfield, and let r be a positive integer. There is a natural bijection between equivalence classes of Grassmann-Plücker functions of rank r on E with coefficients in F and matroids of rank r on E with coefficients in F.*

The bijective map from equivalence classes of Grassmann-Plücker functions to F-matroids in Theorem 3.11 can be described explicitly as follows. Let B_φ be the **support** of φ, i.e., the collection of all subsets $\{x_1, \ldots, x_r\} \subset E$ such that $\varphi(x_1, \ldots, x_r) \neq 0$. Then B_φ is the set of bases for a rank r matroid M_φ (in the usual sense) on E (cf. [AD12, Remark 2.5]). For each circuit C of M_φ, we define a corresponding projective circuit $X \in \mathbb{P}(\mathbb{F}^E)$ with $\mathrm{supp}(X) = C$ as follows. Let $x_0 \in C$ and let $\{x_1, \ldots, x_r\}$ be a basis for M_φ containing $C \backslash x_0$. Then

$$\frac{X(x_i)}{X(x_0)} = (-1)^i \frac{\varphi(x_0, \ldots, \hat{x}_i, \ldots, x_r)}{\varphi(x_1, \ldots, x_r)}. \tag{3.12}$$

We will show that this is well-defined, and give an explicit description of the inverse map from F-matroids to equivalence classes of Grassmann-Plücker functions.

We will also see, in Theorem 6.22, that Axiom (GP3) above can be replaced by the following *a priori* weaker axiom:

- (GP3)$'$ The support of φ is a (rank r) matroid on E, and (3.10) holds for any two subsets $I = \{x_1, \ldots, x_{r+1}\}$ and $J = \{y_1, \ldots, y_{r-1}\}$ of E with $|I \backslash J| = 3$ (i.e., φ satisfies the "3-term Grassmann-Plücker relations").

3.4. **Dressians.** For concreteness and ease of notation, write $E = \{e_1, \ldots, e_m\}$ and let S denote the collection of r-element subsets of $\{1, \ldots, m\}$, so that $|S| = \binom{m}{r}$. Given a Grassmann-Plücker function φ, define the corresponding *Plücker vector* $p = (p_I)_{I \in S} \in F^S$ by $p_I := \varphi(e_{i_1}, \ldots, e_{i_r})$, where $I = \{i_1, \ldots, i_r\}$ and $i_1 < \cdots < i_r$. Clearly φ can be recovered uniquely from p. The vector p satisfies an analogue of the Grassmann–Plücker relations (GP3); for example, the 3-term relations can be rewritten as follows: for every $A \subset \{1, \ldots, m\}$ of size $r-2$ and $i, j, k, \ell \in \{1, \ldots, m\} \backslash A$, we have

$$0 \in p_{A \cup i \cup j} \odot p_{A \cup k \cup \ell} \boxplus -p_{A \cup i \cup k} \odot p_{A \cup j \cup \ell} \boxplus p_{A \cup i \cup \ell} \odot p_{A \cup j \cup k}. \tag{3.13}$$

More generally, for all subsets I, J of $\{1, \ldots, m\}$ with $|I| = r+1$, $|J| = r-1$, and $|I \backslash J| \geq 3$, the point $p = (p_I)$ lies on the "subvariety" of the projective space in the $\binom{m}{r}$ homogeneous variables x_I for $I \in S$ defined by

$$0 \in \boxplus_{i \in I} \mathrm{sign}(i; I, J) \odot x_{J \cup i} \odot x_{J \backslash i}, \tag{3.14}$$

where $\mathrm{sign}(i; I, J) = (-1)^s$ with s equal to the number of elements $i' \in I$ with $i < i'$ plus the number of elements $j \in J$ with $i < j$.

Although we will not explore this further in the present paper, one can view the "equations" (3.14) as defining a hyperring scheme $D(r, m)$ in the sense of [Jun15a], which (following [MS15, §4.4]) we call the *F-Dressian*. In this geometric language, Theorem 3.11 says that a matroid of rank r on $\{1, \ldots, m\}$ over a hyperfield F can be identified with an F-valued point of $D(r, m)$; thus $D(r, m)$ is a "moduli space" for rank r matroids over F. If $F = K$ is a field, the K-Dressian $D(r, m)$ coincides with the Grassmannian variety $G(r, m)$ over K.

Remark 3.15. Oliver Lorscheid has pointed out to us that if one works in the larger category of ordered blueprints [Lor15], which contains hyperrings as a full subcategory, admits tensor products, and has an initial object $\mathbf{F}_1$, we may identify the F-hyperring scheme $D(r, m)$ with the base change from $\mathbf{F}_1$ to F of a universal ordered blue scheme over $\mathbf{F}_1$, the "$\mathbf{F}_1$-Dressian". One could then define a matroid over an ordered blueprint S to be an S-point of the $\mathbf{F}_1$-Dressian, generalizing our notion of matroids over hyperfields. It seems rather unlikely, however, that there are nice generalizations of the circuit or dual pair "cryptomorphic" axiom systems in this generality.

3.5. **Duality.** There is a duality theory for matroids over hyperfields which generalizes the established duality theory for matroids, oriented matroids, valuated matroids, etc. (For matroids over fields, it corresponds to orthogonal complementation.)

Theorem 3.16. *Let E be a non-empty finite set with $|E| = m$, let F be a hyperfield, and let M be an F-matroid of rank r on E with circuit set $\mathcal{C}$ and Grassmann-Plücker function φ. There is an F-matroid M^* of rank $m-r$ on E, called the* **dual F-matroid** *of M, with the following properties:*

- *The set $\mathcal{C}^*$ of circuits of M^* are the elements of $\mathrm{Min}(\mathcal{C}^\perp)$, where $\mathrm{Min}(S)$ denotes the elements of S of minimal non-empty support.*
- *A Grassmann-Plücker function φ^* for M^* is defined by the formula*
$$\varphi^*(x_1, \ldots, x_{m-r}) = \mathrm{sign}(x_1, \ldots, x_{m-r}, x'_1, \ldots, x'_r)\varphi(x'_1, \ldots, x'_r),$$
where $x'_1, \ldots, x'_r$ is any ordering of $E \backslash \{x_1, \ldots, x_{m-r}\}$.
- *The underlying matroid of M^* is the dual of the underlying matroid of M, i.e., $\underline{M^*} = \underline{M}^*$.*
- *$M^{**} = M$.*

The circuits of M^* are called the **cocircuits** of M, and vice-versa.

3.6. **Dual pairs.** Let M be a (classical) matroid with ground set E. We call a subset $\mathcal{C}$ of F^E an **F-signature of** M if taking supports gives a bijection from the projectivization of $\mathcal{C}$ to circuits of M.

We say that $(\mathcal{C}, \mathcal{D})$ is a **dual pair of F-signatures of** M if:

- (DP1) $\mathcal{C}$ is an F-signature of the matroid M.
- (DP2) $\mathcal{D}$ is an F-signature of the dual matroid M^*.
- (DP3) $\mathcal{C} \perp \mathcal{D}$, meaning that $X \perp Y$ for all $X \in \mathcal{C}$ and $Y \in \mathcal{D}$.

Theorem 3.17. *Let M be a matroid on E, let $\mathcal{C}$ be an F-signature of M, and let $\mathcal{D}$ be an F-signature of M^*. Then $\mathcal{C}$ and $\mathcal{D}$ are the set of circuits and cocircuits, respectively, of an F-matroid with underlying matroid M if and only if $\mathcal{C} \perp \mathcal{D}$.*

We will see, in Theorem 6.22, that Theorem 3.17 still holds when (DP3) is replaced by the following *a priori* weaker axiom:

- (DP3)$'$ $X \perp Y$ for every pair $X \in \mathcal{C}$ and $Y \in \mathcal{D}$ with $|\underline{X} \cap \underline{Y}| \leq 3$.

3.7. **Minors.** Let $\mathcal{C}$ be the set of circuits of an F-matroid M on E, and let $A \subseteq E$. For $X \in \mathcal{C}$, define $X[A] \in F^{E \backslash A}$ by $(X[A])(e) = X(e)$ for $e \notin A$.

Let $\mathcal{C} \backslash A = \{X \backslash A \mid X \in \mathcal{C},\ \underline{X} \cap A = \emptyset\}$. Similarly, let $\mathcal{C}/A = \mathrm{Min}(\{X \backslash A \mid X \in \mathcal{C}\})$.

Theorem 3.18. *Let $\mathcal{C}$ be the set of circuits of an F-matroid M on E, and let $A \subseteq E$. Then $\mathcal{C} \backslash A$ is the set of circuits of an F-matroid $M \backslash A$ on $E \backslash A$, called the* **deletion** *of M with respect to A, whose underlying matroid is $\underline{M} \backslash A$. Similarly, $\mathcal{C}/A$ is the set of circuits of an F-matroid M/A on $E \backslash A$, called the* **contraction** *of M with respect to A, whose underlying matroid is $\underline{M}/A$. Moreover, we have $(\underline{M} \backslash A)^* = M^*/A$ and $(\underline{M}/A)^* = M^* \backslash A$.*

3.8. **Equivalence of different definitions.** We briefly indicate how to see the equivalence of various flavors of matroids in the literature with our notion of F-matroid, for some specific choices of the hyperfield F.

Example 3.19. When $F = K$ is a field, a matroid on E with coefficients in K is the same thing as a vector subspace of K^E in the usual sense. Indeed, the equivalence of (V0)-(V3) with (GP1)-(GP3) is a classical fact about the Grassmannian $G(r, m)$ (see e.g. [KL72]), and the equivalence of (GP1)-(GP3) with (C0)-(C3) is part of Theorem 6.21.

Example 3.20. A matroid over $\mathbf{K}$ is the same thing as a matroid in the usual sense. This follows, for example, from [AD12, Lemma A.3].

Example 3.21. A matroid over $\mathbf{T}$ is the same thing as a valuated matroid in the sense of Dress–Wenzel [DW92]. This follows, for example, from [MT01, Theorem 3.2].

Example 3.22. A matroid over $\mathbf{S}$ is the same thing as an **oriented matroid** in the sense of Bland–Las Vergnas [BLV78]. This follows from [BLVS$^+$99, Theorem 3.6.1]; see also Theorem 3.4.3 and Corollary 3.5.12 of *loc. cit.*.

Example 3.23. A matroid over $\mathbf{P}$ is the same thing as an **complex matroid** in the sense of Anderson–Delucchi [AD12] (see for example Theorem A of *loc. cit.*).

4. Partial demifields and vector axioms

As explained in Anderson–Delucchi [AD12], in the case $F = \mathbf{P}$ there is no reasonable axiomatization of F-matroids in terms of **vectors**. On the other hand, it is well-known that there is such an axiomatization for matroids, valuated matroids, and oriented matroids (and trivially for vector spaces as well). The explanation for this discrepancy is that the hyperfields $\mathbf{K}, \mathbf{T}, \mathbf{S}, K$ all naturally come equipped with the additional structure of a **partial demifield**, to be defined below. For many interesting examples of partial demifields F, there is a cryptomorphic characterization of F-matroids in terms of vector axioms.

4.1. Partial demifields and partial fields.

Definition 4.1. A **partial demifield** P is a pair (F, S) consisting of a hyperfield $(F, \boxplus, \odot)$ and a commutative semiring $(S, \oplus, \odot)$, together with an identification of $(F, \odot)$ with a submonoid of $(S, \odot)$ taking 0 to 0 and 1 to 1, such that:

- (Compatibility) $a \oplus b \in a \boxplus b$ whenever a, b, and $a \oplus b$ all belong to F.
- (Minimality) F generates the semiring S.

The reason for the adjective "partial" is that one can view the operation $\oplus$ on R as providing a partially-defined addition operation on F. The compatibility axiom says that whenever the sum $a \oplus b$ is defined, it should belong to the hypersum $a \boxplus b$. When we write $x \in P$, we will mean $x \in F$. When $F = S$, we will usually write F instead of P and we call F a **demifield** (without the word partial).

The notion of partial demifield can be seen as an enrichment and generalization of the notion of *partial field*. The following definition is taken from [PvZ13, Definition 2.1] (except that we have added a minimality condition):

Definition 4.2. A **partial field** P is a pair $(F = G \cup \{0\}, R)$ consisting of a commutative ring R and a subgroup G of the group $R^\times$ of units of R such that:

- (Negatives) -1 belongs to G.
- (Minimality) G generates the ring R.

Note that a partial field with $F = R$ is the same thing as a *field*. We will sometimes write the binary operations on a partial field as $+$ and $\cdot$, rather than $\oplus$ and $\odot$ as we write them in the case of partial demifields, to emphasize that R is a ring and not just a semiring.

One can view a partial field as a partial demifield by defining a hyperaddition law on F for $x, y \neq 0$ by $x \boxplus y = F$ if $x = -y$ and $x \boxplus y = G$ if $x \neq -y$. (We have $x \boxplus 0 = 0 \boxplus x = \{x\}$ for all $x \in F$, of course.) It is perhaps more natural to view a partial field P as an *equivalence class* of partial demifields, where we identify $P' = (F', R')$ and $P'' = (F'', R'')$ if $R' = R''$ and $F' = F''$ as submonoids of $(R', \odot) = (R'', \odot)$ (i.e., P' and P'' differ only in their hyperaddition structures). We call any hyperfield F' such that (F', R') represents the equivalence class of P an **underlying hyperfield** for the partial field P.

4.2. Examples.

Here are some examples of (partial) demifields:

Example 4.3. (Krasner demifield) There is a canonical demifield structure on $\mathbf{K}$ defined by $0 \oplus x = x$ for $x = 0, 1$ and $1 \oplus 1 = 1$.

Example 4.4. (Idempotent semifield) More generally, if Γ is any totally ordered abelian group (written multiplicatively), there is a canonical demifield structure on the valuative hypergroup $S := \Gamma \cup \{0\}$, where we define $x \oplus y = \max(x, y)$. If we forget the hyperaddition, the resulting triple $(S, \odot, \oplus)$ is an idempotent semifield.

Conversely every idempotent semifield arises in this way: one defines a total order by declaring that $x \leq y$ iff there exists $z \in S$ with $x \oplus z = y$, and hyperaddition is defined as $x \boxplus y := \{z \in S \ : \ z \leq x \oplus y\}$. We will usually use the more standard term "idempotent semifield" instead of "valuative demifield", though it is to be understood that S also comes equipped with the natural hyperaddition law above.

In particular, if $\Gamma = \mathbf{R}_{>0}$ the resulting demifield will be called the **tropical demifield** $\mathbb{T}$.

Example 4.5. (Partial demifield of signs) There is a natural partial demifield structure on the hyperfield $\mathbf{S}$. Define the semiring $\hat{\mathbf{S}}$ to be $\{0, 1, -1, \infty\}$ together with the following operations. The addition law $\oplus$ is defined as the join (least upper bound) operator with respect to the partial order $0 < 1, -1 < \infty$. The multiplication law $\odot$ is such that $\mathbf{S} = (\{0, 1, -1\}, \odot)$ is a submonoid, and we define $0 \odot \infty = 0$ and $x \odot \infty = \infty$ for $x \neq 0$. It is straightforward to check that the distributive law holds. We call the resulting pair $(\mathbf{S}, \hat{\mathbf{S}})$ the **partial demifield of signs**.

Example 4.6. (Partial fields) There many interesting examples of partial fields given in [PvZ10]. We mention in particular the following:

- The **regular partial field** $\mathbb{U}_0 := (\{\pm 1\}, \mathbb{Z})$.
- The **dyadic partial field** $\mathbb{D} := (\langle -1, 2 \rangle, \mathbb{Z}[\frac{1}{2}])$.
- The **near-regular partial field** $\mathbb{U}_1 := (\{\langle -1, T, 1-T \rangle\}, \mathbb{Z}[\frac{1}{T}, \frac{1}{1-T}])$, where T is an indeterminate.

4.3. **Linear subspaces.** In linear algebra, if K is a field then a linear subspace of K^m is just a K-submodule of K^m. If we replace the field K by a demifield F, there are many F-submodues V of F^m which do not behave much like linear spaces. We need to impose an extra axiom which allows us to perform a kind of "multivalued subtraction" in V. Thus, we will define a linear subspace of F^E to be an F-submodule of F^E satisfying an additional axiom generalizing the *vector elimination axiom* from matroid theory.

If $P = (F, S)$ is just a *partial* demifield, it is not even clear *a priori* what it should mean to be a P-submodule of F^m, so there is an additional wrinkle to consider. Motivated by these considerations, and by Tutte's theory of chain groups as generalized in [PvZ13], we make the following definitions.

Definition 4.7. (Elementary vector) Let $P = (F, S)$ be a partial demifield, let E be a finite set, and let A be a subset of S^E. An element $v \in A$ is called an **elementary vector** of A if it has minimal support among all nonzero elements of A. We denote by $\mathcal{E}(A)$ the set of all elementary vectors of A.

Definition 4.8. (Primitive vector) Let $P = (F, S)$ be a partial demifield and let E be a finite set. An element $v \in S^E$ is called **primitive** if it belongs to F^E.

Definition 4.9. (Linear subspace) Let $P = (F, S)$ be a partial demifield, let E be a finite set, and let V be a subset of F^E. We say that V is a P**-linear subspace** of F^E (or just a **linear subspace** if P is understood) if:

- (V0) There is an S-submodule V_S of S^E such that $V = V_S \cap F^E$.
- (V1) Every elementary vector $X \in \mathcal{H}_S := \mathcal{E}(V_S)$ is a scalar multiple of a primitive vector Y, i.e., there exist $s \in S$ and $Y \in F^E$ such that $X = s \odot Y$.

- (V2) Every $X \in V_S$ (resp. $X \in V$) can be written as $X = X_1 \oplus \cdots \oplus X_t$ where the $X_i \in \mathcal{H}_S$ (resp. $X_i \in \mathcal{H} := \mathcal{H}_S \cap F^E$) and $\underline{X_i} \subseteq \underline{X}$.
- (V3) If $X, Y \in V$ and $X(e) = -Y(e)$ for some $e \in E$, there exists $Z \in V$ such that $Z(e) = 0$ and $Z(f) \in X(f) \boxplus Y(f)$ for all $f \in E$.

Remark 4.10. If $P = F$ is a demifield, then (V0)-(V3) are equivalent to the following simpler axioms:

- (DV0) $0 \in V$.
- (DV1) If $X_1, X_2 \in V$ and $c_1, c_2 \in F$ then $c_1X_1 \oplus c_2X_2 \in V$.
- (DV2) Every $X \in V$ can be written as $X = X_1 \oplus \cdots \oplus X_t$ where the X_i are elementary vectors and $\underline{X_i} \subseteq \underline{X}$.
- (DV3) If $X, Y \in V$ and $X(e) = -Y(e)$ for some $e \in E$, there exists $Z \in V$ such that $Z(e) = 0$ and $Z(f) \in X(f) \boxplus Y(f)$ for all $f \in E$.

Lemma 4.11. *Let $P = (F, S)$ be a partial demifield, let E be a finite set, and let V be a linear subspace of F^E. Let $\mathcal{H}$ be the set of primitive elementary vectors of V_S. Then $\mathcal{H}$ is the set of circuits of an F-matroid M.*

Proof. Axioms (C0) and (C1) are trivial.

For (C2), we need to check that if $X, Y \in \mathcal{H}$ and $\underline{X} = \underline{Y}$, then there exists a nonzero $\alpha \in F$ such that $X = \alpha Y$. Choose $e \in \underline{X}$ and, without loss of generality, scale Y so that $X(e) = -Y(e)$. By (V3), there exists $Z \in V$ such that $Z(e) = 0$ and $Z(f) \in X(f) \boxplus Y(f)$ for all $f \in E$. But then $\underline{Z} \subseteq (\underline{X} \cup \underline{Y}) \backslash e = \underline{X} \backslash e$, a contradiction unless $Z = 0$. Therefore $0 \in X(f) \boxplus Y(f)$ for all $f \in E$, which means that $X(f) = -Y(f)$ for all f and hence $X = -Y$ and X is a scalar multiple of Y as desired.

For (C3), we need to check that if $X, Y \in \mathcal{H}$, $\underline{X}, \underline{Y}$ are a modular pair in $\underline{\mathcal{H}}$, and $X(e) = -Y(e) \neq 0$, then there exists $Z \in \mathcal{H}$ such that $Z(e) = 0$ and $Z(f) \in X(f) \boxplus Y(f)$ for all $f \in E$. By (V3) there is such a Z in V, and we need to prove that $Z \in \mathcal{H}$. By (V2), we can write $Z = Z_1 \oplus \cdots \oplus Z_t$ with $Z_i \in \mathcal{H}$ and $\underline{Z_i} \subseteq \underline{Z} \subseteq (\underline{X} \cup \underline{Y}) \backslash e$. Since $\underline{X}, \underline{Y}$ are a modular pair in $\underline{\mathcal{H}}$, it follows from the definition that $Z_1 = \cdots = Z_t$. But $Z = Z_1 \oplus \cdots \oplus Z_t$ implies that $\underline{Z} \subseteq \cup \underline{Z_i} = \underline{Z_1}$. Hence $\underline{Z} = \underline{Z_1}$, which by (C2) means that Z is a scalar multiple of Z_1. Thus $Z \in \mathcal{H}$ as desired. □

We will write $\mathcal{M}(V)$ for the F-matroid M in the statement of Lemma 4.11. By (V2), $\mathcal{M}(V)$ uniquely determines V.

Definition 4.12. An F-matroid M is **representable over** P if $M = \mathcal{M}(V)$ for some P-linear subspace V of F^E.

Thus Lemma 4.11 establishes a bijection between linear subspaces of F^E and F-matroids which are representable over P.

If M is an F-matroid on E with collection of circuits $\mathcal{C} \subset F^E$, let $\mathcal{V}(M)_S \subseteq S^E$ be the S-submodule of S^E generated by $\mathcal{C}$, and let $\mathcal{V}(M) = \mathcal{V}(M)_S \cap F^E$. It is easy to see that M is representable over P if and only if $\mathcal{V}(M) \subseteq F^E$ is a linear subspace whose set of primitive elementary vectors is $\mathcal{C}$.

We call a partial demifield $P = (F, S)$ **vectorial** if every F-matroid is representable over P. In other words, P is vectorial if and only if the axioms (V0)-(V3) for a linear subspace are cryptomorphically equivalent to the F-matroid circuit axioms (C0)-(C3) via the correspondence $V \rightsquigarrow \mathcal{M}(V)$ and $M \rightsquigarrow \mathcal{V}(M)$.

Many partial demifields P, including all of the examples we've seen so far, turn out to be vectorial.

Theorem 4.13. (1) *Every field K is vectorial.*
(2) *The partial demifield of signs $\mathbb{S}$ is vectorial.*
(3) *The Krasner demifield $\mathbb{K}$ and the tropical semifield $\mathbb{T}$ are vectorial. More generally, every idempotent semifield S is vectorial.*

Proof. The fact that every field is vectorial is an elementary consequence of Example 3.19 (see also Theorem 4.16 below).

The fact that $\mathbb{S}$ is vectorial follows from Example 3.22 and Theorem 3.7.5, Corollaries 3.7.6-3.7.8 of [BLVS$^+$99].

The fact that every idempotent semifield S is vectorial follows from [MT01, Proof of Theorems 3.4-3.6]. The proofs there are written in the specific case $S = \mathbb{T}$ but they hold *mutatis mutandis* for any idempotent semifield S. □

In light of these examples, one might wonder if *every* partial demifield is vectorial. The answer is *no*, even if one restricts to partial fields. We will construct a counterexample (Example 5.19) in the next section as a consequence of our next theorem. In order to state it, we need two definitions:

Definition 4.14. Let M be an F-matroid. A triple (C_1, C_2, C_3) of distinct circuits of M is called a **modular triple** if any of the following equivalent conditions is satisfied:

- $r(\underline{C_1} \cup \underline{C_2} \cup \underline{C_3}) = |\underline{C_1} \cup \underline{C_2} \cup \underline{C_3}| - 2$.
- $\underline{C_1}$ and $\underline{C_2}$ are a modular pair and $\underline{C_3} \subseteq \underline{C_1} \cup \underline{C_2}$.
- For any permutation (i, j, k) of $\{1, 2, 3\}$, $\underline{C_i}$ and $\underline{C_j}$ are a modular pair and $\underline{C_k} \subseteq \underline{C_i} \cup \underline{C_j}$.

Definition 4.15. Let $P = (F, R)$ be a partial field. Elements $X_1, \ldots, X_n$ of F^E are called **linearly dependent over** P if there are $c_1, \ldots, c_n \in F$, not all zero, such that $c_1X_1 \oplus \cdots \oplus c_nX_n = 0$ in R. (This is different from the notion of F-linear dependence for a hyperfield F.)

Theorem 4.16. *Let $P = (F, R)$ be a partial field, and let M be F-matroid whose set of circuits is $\mathcal{C}$. Let $\mathcal{H}$ be the set of primitive elementary vectors of $\mathcal{V}(M)_R$ as in the statement of Lemma 4.11.The following are equivalent:*
(1) *M is representable over P.*
(2) *$\mathcal{V}(M)$ satisfies (V1) and $\mathcal{H} = \mathcal{C}$.*
(3) *Every modular triple of circuits of M is linearly dependent over P.*

Proof. Let $V = \mathcal{V}(M) \subseteq F^E$. By definition, M is representable over P if and only if V is a linear subspace whose set of primitive elementary vectors is $\mathcal{C}$. Trivially, V satisfies (V0), and thus $V_R := \mathcal{V}(M)_R$ is an R**-chain group** in the sense of Tutte [PvZ13, Definition 3.2]. Furthermore, V satisfies (V1) if and only if V_R is a P**-chain group** in the sense of [PvZ13, Definition 3.5].

(1)⇒(2): trivial.

(2)⇔(3): This is a consequence of [PvZ13, Theorem 3.20].

(2)⇒(1): It remains to show that V satisfies (V2) and (V3). Verifying (V3) in this situation is trivial; in fact, V satisfies the following property which is stronger than (V3) (take $Z = X + Y$):

- $(V3)'$ If $X, Y \in V$, there exists $Z \in V$ such that $Z(f) = X(f) + Y(f)$ for all $f \in E$.

For (V2), we show by induction on $\underline{X}$ that every $X \in V_R$ is a sum of elementary vectors X_i with $\underline{X_i} \subseteq \underline{X}$. Let $X_1 \in \mathcal{H}_R$ be an elementary vector with $\underline{X_1} \subseteq \underline{X}$, let $e \in \underline{X_1}$, and let $X' = X - \lambda X_1$ where $\lambda = X(e)/X_1(e)$. Then $\underline{X'} \subseteq \underline{X}\backslash e$, so by induction $X' = X_2 + \cdots + X_t$ with $X_i \in \mathcal{H}_R$ and $\underline{X_i} \subseteq \underline{X}$ for all i. Then $X = \lambda X_1 + X_2 + \cdots + X_t$ as required. The same argument (with $\mathcal{H}_R$ replaced by $\mathcal{H}$ throughout) shows that every $X \in V$ is a sum of primitive elementary vectors X_i with $\underline{X_i} \subseteq \underline{X}$. □

We do not know a precise characterization of which partial demifields are vectorial, nor a simple generalization of Theorems 4.13 and Theorem 4.16 together with a unified proof covering all cases.

5. Realizability and representability

In this section we discuss the concepts of *realizability* and *representability* (over hyperfields and partial demirings, respectively) in the general context of push-forward maps.

5.1. Homomorphisms.

Definition 5.1. A **hypergroup homomorphism** is a map $f : G \to H$ such that $f(0) = 0$ and $f(x \boxplus y) \subseteq f(x) \boxplus f(y)$ for all $x, y \in G$.

A **hyperring homomorphism** is a map $f : R \to S$ which is a homomorphism of additive hypergroups as well as a homomorphism of multiplicative monoids (i.e., $f(1) = 1$ and $f(x \odot y) = f(x) \odot f(y)$ for $x, y \in R$).

A **hyperfield homomorphism** is a homomorphism of the underlying hyperrings.

We define the **kernel** $\ker(f)$ of a hyperring homomorphism f to be $f^{-1}(0)$. Note that a hyperring homomorphism must send units to units, and therefore if $f : R \to S$ is a homomorphism and R is a hyperfield, we must have $\ker(f) = \{0\}$.

Remark 5.2. When the hyperring structure on a demigroup A is induced from a map $f : R \twoheadrightarrow A$ as in Remark 2.4, the map f becomes a homomorphism of hyperrings with $\ker(f) = \{0\}$.

Example 5.3. A hyperring homomorphism from a commutative ring R with 1 to the hyperfield $\mathbf{K}$ is the same thing as a prime ideal of R, via the correspondence $\mathfrak{p} := \ker(f)$.

Example 5.4. A hyperring homomorphism from a commutative ring R with 1 to the tropical hyperfield $\mathbf{T}$ is the same thing as a prime ideal $\mathfrak{p}$ of R together with a real valuation on the residue field of $\mathfrak{p}$ (i.e., the fraction field of $R/\mathfrak{p}$). (Similarly, a hyperring homomorphism from R to $\Gamma \cup \{0\}$ for some totally ordered abelian group Γ is the same thing as a prime ideal $\mathfrak{p}$ of R together with a Krull valuation on the residue field of $\mathfrak{p}$.) In particular, a hyperring homomorphism from a field K to $\mathbf{T}$ is the same thing as a real valuation on K. These observations allow one to reformulate the basic definitions in Berkovich's theory of analytic spaces [Ber90] in terms of hyperrings, though we will not explore this further in the present paper.

Example 5.5. A hyperring homomorphism from a commutative R with 1 to the hyperfield of signs $\mathbf{S}$ is the same thing as prime ideal $\mathfrak{p}$ together with an ordering on the residue field of $\mathfrak{p}$ (see e.g. [Mar06, §3]). In particular, a hyperring homomorphism from a field K to $\mathbf{S}$ is the same thing as an ordering on K. This observation allows one to reformulate the notion of *real spectrum* [BPR06, Mar96] in terms of hyperrings, and provides an interesting lens through which to view the analogy between Berkovich spaces and real spectra.

5.2. **Push-forwards and realizability.** Recall that if F is a hyperfield and M is an F-matroid on E, there is an underlying classical matroid $\underline{M}$, and that classical matroids are the same as matroids over the hyperfield $\mathbf{K}$. We now show that the "underlying matroid" construction is a special case of a general push-forward operation on matroids over hyperfields.

The following lemma is straightforward from the various definitions involved:

Lemma 5.6. *If $f : F \to F'$ is a homomorphism of hyperfields and M is an F-matroid on E, the image under the induced map $f_* : F^E \to (F')^E$ of the set of circuits of M is the set of circuits of an F'-matroid $f_*(M)$ on E, called the* **push-forward** *of M.*

Remark 5.7. If F is a hyperfield, there is a canonical homomorphism $\psi : F \to \mathbf{F}_1$ sending 0 to 0 and all non-zero elements of F to 1. If M is an F-matroid, the push-forward $\psi_*(M)$ coincides with the underlying matroid $\underline{M}$.

Given a Grassmann-Plücker function $\varphi : E^r \to F$ and a homomorphism of hyperfields $f : F \to F'$, we define the **push-forward** $f_*\varphi : E^r \to F'$ by the formula

$$(f_*\varphi)(e_1, \ldots, e_r) = f(\varphi(e_1, \ldots, e_r)).$$

As an immediate consequence of (3.12), we see that the push-forward of an F-matroid can be defined using either circuits or Grassmann-Plücker functions:

Lemma 5.8. *If M_φ is the F-matroid associated to the Grassmann-Plücker function $\varphi : E^r \to F$ and $f : F \to F'$ is a homomorphism of hyperfields, then $f_*(M_\varphi) = M_{f_*\varphi}$.*

Definition 5.9. Let $f : F \to F'$ be a homomorphism of hyperfields, and let M' be a matroid on E with coefficients in F'. We say that M' is **realizable with respect to** f if there is a matroid M over F such that $f_*(M) = M'$.

If $F' = \mathbb{K}$ is the Krasner hyperfield, so that M' is a matroid in the usual sense, we say that M' is **realizable over** F if there is a matroid M over F such that $\psi_*(M) = M'$, where $\psi : F \to \mathbb{K}$ is the canonical homomorphism.

5.3. **Linear spaces and representability.**

Definition 5.10. A **homomorphism of partial demirings** from $P = (F, S)$ to $P' = (F', S')$ is a semiring homomorphism $f : S \to S'$ taking F to F' such that $f|_F$ is a homomorphism of hyperfields.

Definition 5.11. Let $f : P \to P'$ be a homomorphism of partial demifields, and let V be a P-linear subspace of F^E. It is not difficult to check that $f_*(V) := \{f(v) \ : \ v \in V\}$ is a P'-linear subspace of $(F')^E$. We call $f_*(V)$ the **push-forward** of V to P'.

Example 5.12. If K is a field equipped with a non-archimedean valuation $v : K \to \mathbf{T}$ and W is a linear subspace of K^E, the push-forward $v_*(W)$ is just the *tropicalization* of W in the sense of [MS15, §3.2]. The matroid with coefficients in $\mathbf{T}$ corresponding to $v_*(W)$ is precisely the *valuated matroid associated to* W in the usual sense of tropical geometry (cf. [MS15, §4.4]). Similar remarks apply when $K = \mathbf{R}$ and $\sigma : \mathbf{R} \to \mathbf{S}$ is the corresponding homomorphism; in this case one recovers the *oriented matroid associated to* W in the sense of [BLVS+99, §1.2]. The case $F = \mathbf{P}$ corresponds to the notion of *phase tropicalization*, c.f. [BBM14].

Definition 5.13. Let $P = (F, S)$ be a partial demifield and let $f : F \to F'$ be a homomorphism of hyperfields. We say than an F'-matroid M' is **representable with respect to** f if $M' = f_*(M)$ for some F-matroid M with is representable over P in the sense of Definition 4.12.

In particular, if $F' = \mathbb{K}$ and M' is a matroid in the usual sense, we say that M' is **representable over** P if it is representable with respect to the canonical homomorphism $\psi : F \to \mathbb{K}$.

It is easy to see from Theorem 4.16 that if P is a partial field and M' is a matroid, then M' is representable over P in the sense of Definition 5.13 if and only if it is representable over P in the sense of [PvZ13]. In particular, Theorem 4.16 implies that whether or not M' is representable over $P = (F, R)$ is independent of the choice of hyperfield structure on F (i.e., we can choose F to be any hyperfield underlying P).

If K is a field then by part (1) of Theorem 4.13, the following are equivalent:

(1) M' is representable over K in the sense of Definition 5.13.
(2) M' is realizable over K in the sense of Definition 5.9.
(3) M' is realizable over K in the usual sense of matroid theory.

Example 5.14. Let K be a field and let $f : K \to F$ be a homomorphism of hyperfields. If an F-matroid M on E is representable with respect to f by a linear subspace $V \subset K^E$, then the dual F-matroid M^* is representable by the orthogonal complement $V^\perp$. This is a straightforward consequence of Theorem 3.16 and the definition of orthogonality for circuits.

Example 5.15. If $P = (F, R)$ is a partial field and a matroid M is representable over P by the linear subspace $W \subset F^E$, the dual matroid M^* is representable by the orthogonal complement

$$W^\perp := \{(v_1, \dots, v_m) \in F^E \ : \ v_1 w_1 \oplus \cdots \oplus v_m w_m = 0 \ \forall \ (w_1, \dots, w_m) \in W\}.$$

This follows from [PvZ13, Theorem 3.12]. Note that this orthogonal complement is defined slightly differently from the previous example.

The above definitions put the theory of representability of matroids over fields, or more generally over partial fields, into a broader framework. This is interesting because there are numerous classical theorems about representability of matroids which can be interpreted and/or enriched using the language of partial fields. For example:

Example 5.16. A matroid is called **regular** if it is representable over every field. By [PvZ10, Theorem 2.29] (which generalizes classical result of Tutte), the following are equivalent:

(1) M is regular.
(2) M is representable over every partial field.
(3) M is representable over GF(2) and GF(3).
(4) M is representable over the partial field $\mathbb{U}_0$.

Example 5.17. A matroid is called **dyadic** if it is representable over every field of characteristic different from 2. By [PvZ10, Theorem 4.3] (which generalizes classical result of Whittle), the following are equivalent:

(1) M is dyadic.
(2) M is representable over GF(3) and GF(5).
(3) M is representable over the partial field $\mathbb{D}$.

Example 5.18. A matroid is called **near-regular** if it is representable over every field except possibly GF(2). By [PvZ10, Theorem 4.5] (which generalizes a classical result of Whittle), the following are equivalent:

(1) M is near-regular.
(2) M is representable over $\mathrm{GF}(3), \mathrm{GF}(4)$, and $\mathrm{GF}(5)$.
(3) M is representable over the partial field $\mathbb{U}_1$.

Using Example 5.16 and Theorem 4.16, we can give an example of a non-vectorial partial field.

Example 5.19. Let $P = \mathbb{U}_0 = (\pm 1, \mathbb{Z})$, and let $F = 0 \cup \{1, -1\}$ be the field GF(3), which is an underyling hyperfield for P. Let $M' = F_7^-$ be the **non-Fano matroid** (cf. [Oxl92, Example 1.5.12]). By [Oxl92, Proposition 6.4.8(ii)], M' is representable over a field K if and only if the characteristic of K is not 2. In particular, M' is representable over GF(3). Choose an F-matroid M whose underlying matroid is F_7^-. Since M is not representable over any field of characteristic 2, M is not representable over $\mathbb{U}_0$ (see Example 5.16). In particular, the partial field $\mathbb{U}_0$ is not vectorial (the vector axioms over $\mathbb{U}_0$ are strictly stronger than the circuit axioms over F).

We can see this concretely, without using any theorems about the non-Fano matroid or regular matroids, as follows. With the elements of E labeled 1 through 7 as in [Oxl92, Figure 1.15], we can represent the linear subspace $\mathcal{V}(M)$ of F^E corresponding to M as the row space of the following matrix with entries in $GF(3)$:

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

Any three circuits with support $\{3, 4, 5\}, \{2, 3, 4, 6\}, \{2, 4, 5, 6\}$, respectively, form a modular triple, since their union has 5 elements and F_7^- has rank 3. We can represent these circuits by the vectors $(0, 0, 1, 1, -1, 0, 0), (0, -1, 1, -1, 0, 1, 0)$, and $(0, -1, 0, 1, 1, 1, 0)$, respectively. Although these vectors are linearly dependent over GF(3), if we view them as elements of $\mathbb{Z}^7$ then they are linearly independent. By Theorem 4.16, $\mathcal{V}(M)$ is not a $\mathbb{U}_0$-linear subspace of $\mathbb{Z}^7$, i.e., M is not representable over $\mathbb{U}_0$.

Given a matroid M and a hyperfield F or a partial demifield P, we can ask if M is realizable over F or representable over P. In some cases these notions coincide, but in others they do not. In view of the vast supply of hyperfields and partial demifields which nature has to offer, we hope this point of view on realizability and representability will be of future use in matroid theory for generating analogues of results like those in Examples 5.16, 5.17, and 5.18.

6. Proofs

In this section, we provide proofs of the main theorems of the paper. We closely follow the arguments of Anderson–Delucchi from [AD12]; when the proof is a straightforward modification of a corresponding result in *loc. cit.* we sometimes omit details.

6.1. **Grassmann-Plücker functions and Duality.** Given a Grassmann-Plücker function φ of rank r on the ground set E, the set

$$\mathbf{B}_\varphi := \{\{b_1, \ldots, b_r\} \mid \varphi(b_1, \ldots, b_r) \neq 0\}$$

is well-known to be the set of bases of a matroid of rank r, which we denote by M_φ and call the **underlying matroid** of φ.

In what follows, we fix a total order on E.

Definition 6.1. Let φ be a rank r Grassmann-Plücker function on E, and for every ordered tuple $(x_1, x_2, \ldots, x_{m-r}) \in E^{m-r}$ let $x'_1, \ldots, x'_r$ be an ordering of $E \backslash \{x_1, x_2, \ldots, x_{m-r}\}$. Define the **dual Grassmann-Plücker function** φ^* by

$$\varphi^*(x_1, \ldots, x_{m-r}) := \mathrm{sign}(x_1, \ldots, x_{m-r}, x'_1, \ldots, x'_r)\varphi(x'_1, \ldots, x'_r).$$

Note that, up to a global change in sign, φ^* is independent of the choice of ordering of $E \backslash \{x_1, x_2, \ldots, x_{m-r}\}$.

Remark 6.2. Our definition differs slightly from [AD12, Definition 3.1] in that they use $\varphi(x'_1, \ldots, x'_r)^{-1}$ in the above definition instead of $\varphi(x'_1, \ldots, x'_r)$. This is because in Definition 2.12, Anderson and Delucchi use an inner product modeled on the standard Hermitian inner product on $\mathbb{C}^m$ to define the notion of orthogonality, whereas we use an inner product modeled on the standard inner product on $\mathbb{R}^m$. The proofs in [AD12] actually become a bit simpler when one uses our modified definition.

Lemma 6.3. *φ^* is a rank $(m-r)$ Grassmann-Plücker function, and the underlying matroid M_{φ^*} is the matroid dual of M_φ.*

Proof. The fact that $\mathbf{B}_{\varphi^*}$ is the set of bases for M_φ^* follows from [AD12, Theorem A.5] as in the proof of [AD12, Lemma 3.2]. To see that φ^* is a rank $(m-r)$ Grassmann-Plücker function, it suffices to prove (GP3) since (GP1) and (GP2) are clear. Suppose $X := \{x_0, \ldots, x_{m-r}\}$ and $Y := \{y_1, \ldots, y_{m-r-1}\}$, numbered so that $X \cap Y = \{x_{m-r-\ell}, \ldots, x_{m-r}\} = \{y_1, \ldots, y_\ell\}$. Choose a total order A on $E \backslash (X \cap Y)$, and let

$$x_0, \ldots, x_{m-r}, y_{\ell+1}, \ldots, y_{m-r-1}, A$$

be the corresponding ordering of E. Then, by the proof of [AD12, Lemma 3.2], we have

$$\begin{aligned} &\varphi^*(x_0, \ldots, \hat{x}_k, \ldots, x_{m-r}) \odot \varphi^*(x_k, y_1, \ldots, y_{m-r-1}) \\ = \ &\sigma \odot \varphi(x_k, y_{\ell+1}, \ldots, y_{m-r-1}, A) \odot \varphi(x_0, \ldots, \hat{x}_k, \ldots, x_{m-r-1}, A) \end{aligned}$$

where

$$\sigma = \mathrm{sign}(x_0, \ldots, x_{m-r}, y_{\ell+1}, \ldots, y_{m-r-1}, A) \odot \mathrm{sign}(y_1, \ldots, y_{m-r-1}, x_0, \ldots, x_{m-r-\ell}, A).$$

This implies the desired result. □

6.2. **Grassmann-Plücker functions and Minors.** Let φ be a rank r Grassmann-Plücker function on E, and let $A \subset E$.

Definition 6.4. (1) (Contraction) Let ℓ be the rank of A in M_φ, and let $\{a_1, a_2, \ldots, a_\ell\}$ be a maximal φ-independent subset of A. Define $\varphi/A : (E \backslash A)^{r-\ell} \to F$ by

$$(\varphi/A)(x_1, \ldots, x_{r-\ell}) := \varphi(x_1, \ldots, x_{r-\ell}, a_1, \ldots, a_\ell).$$

(2) (Deletion) Let k be the rank of $E\backslash A$ in M_φ, and choose $a_1, \ldots, a_{r-k} \subseteq A$ such that $(E\backslash A) \cup \{a_1, \ldots, a_{r-k}\}$ is a basis of M_φ. Define $\varphi\backslash A : (E\backslash A)^k \to F$ by

$$(\varphi\backslash A)(x_1, \ldots, x_k) := \varphi(x_1, \ldots, x_k, a_1, \ldots, a_{r-k}).$$

The proof of the following lemma is the same as the proofs of Lemmas 3.3 and 3.4 of [AD12]:

Lemma 6.5. (1) *Both φ/A and $\varphi\backslash A$ are Grassmann-Plücker functions, and that their definitions are independent of all choices up to global multiplication by a nonzero element of F.*
(2) *$M_{\varphi/A} = M_\varphi/A$ and $M_{\varphi\backslash A} = M_\varphi\backslash A$.*
(3) *$(\varphi\backslash A)^* = \varphi^*/A$.*

6.3. **Dual Pairs from Grassmann-Plücker functions.** Let φ be a rank r Grassmann-Plücker function on E with underlying matroid M_φ.

Lemma 6.6. *Let C be a circuit of M_φ, and let $e, f \in C$. The quantity*

$$\frac{\varphi(e, x_2, \ldots, x_r)}{\varphi(f, x_2, \ldots, x_r)} := \varphi(e, x_2, \ldots, x_r) \odot \varphi(f, x_2, \ldots, x_r)^{-1}$$

is independent of the choice of $x_2, \ldots, x_r$ such that $\{f, x_2, \ldots, x_r\}$ is a basis for M_φ containing $C\backslash e$.

Proof. (cf. [AD12, Lemma 4.1]) Let $\{f, x_2, \ldots, x_{r-1}, x'_r\}$ be another basis for M_φ containing $C\backslash e$. By Axiom (GP3), we have

$$0 \in \varphi(f, x_2, \ldots, x_r) \odot \varphi(e, x_2, \ldots, x_{r-1}, x'_r) \boxplus -\varphi(e, x_2, \ldots, x_r) \odot \varphi(f, x_2, \ldots, x_{r-1}, x'_r)$$

which implies, by Axiom (H1) in Definition 2.1, that

$$\varphi(f, x_2, \ldots, x_r) \odot \varphi(e, x_2, \ldots, x_{r-1}, x'_r) = \varphi(e, x_2, \ldots, x_r) \odot \varphi(f, x_2, \ldots, x_{r-1}, x'_r).$$

This proves the lemma for φ-bases which differ by a single element, and the general case follows by induction on the number of elements by which two chosen bases differ. □

Definition 6.7. Define $\mathcal{C}_\varphi$ to be the collection of all $X \in F^E$ such that:
(1) $\underline{X}$ is a circuit of M_φ
(2) For every $e, f \in E$ and every basis $B = \{f, x_2, \ldots, x_r\}$ with $\mathrm{supp}(X)\backslash e \subseteq B$, we have

$$\frac{X(f)}{X(e)} = -\frac{\varphi(e, x_2, \ldots, x_r)}{\varphi(f, x_2, \ldots, x_r)}.$$

It is easy to see that $\mathcal{C}_\varphi$ depends only on the equivalence class of φ. Set $\mathcal{D}_\varphi := \mathcal{C}_{\varphi^*}$.

Lemma 6.8. (1) *The sets $\mathcal{C}_\varphi$ and $\mathcal{D}_\varphi$ form a dual pair of F-signatures of M_φ in the sense of §3.6.*
(2) *$\mathcal{C}_{\varphi/e} = \mathcal{C}_\varphi/e$ and $\mathcal{C}_{\varphi\backslash e} = \mathcal{C}_\varphi\backslash e$.*

Proof. (cf. [AD12, Proposition 4.3]) The only nontrivial thing to check is that $\mathcal{C}_\varphi \perp \mathcal{D}_\varphi$. To see this, let $X \in \mathcal{C}$ and $Y \in \mathcal{D}$. If $\underline{X} \cap \underline{Y} = \emptyset$ then $X \perp Y$ by definition. Otherwise, we can write $\underline{X} = \{x_1, \ldots, x_k\}$ and $\underline{Y} = \{y_1, \ldots, y_\ell\}$ with the elements of $\underline{X} \cap \underline{Y} = \{x_1, \ldots, x_n\} = \{y_1, \ldots y_n\}$ written first, so that $m \geq 1$ and $x_i = y_i$ for $1 \leq i \leq n$.

Since $\underline{X}\backslash x_i$ is independent for all $i = 1, \ldots, k$, we must have $k \leq r+1$, and similarly $\ell \leq m-r+1$. As M_φ is a matroid, there are extensions $\{x_1, \ldots, x_{r+1}\}$ of $\underline{X}$ and $\{y_1, \ldots, y_{m-r+1}\}$

of $\underline{Y}$, respectively, such that $\underline{X}\backslash x_i$ (resp. $\underline{Y}\backslash y_j$) is a basis of M_φ (resp. M_{φ^*}) for all $1 \le i \le k$ (resp. $1 \le j \le \ell$). Write $E\backslash\{y_1, \ldots, y_{m-r+1}\} = \{z_1, \ldots, z_{r-1}\}$. By (GP3), we have

$$\begin{aligned} 0 &\in \boxplus_{i=1}^{r+1}(-1)^i \odot \varphi(x_1, \ldots, \hat{x}_i, \ldots, x_{r+1}) \odot \varphi(x_i, z_1, \ldots, z_{r-1}) \\ &= \boxplus_{i=1}^{n}(-1)^i \odot \varphi(x_1, \ldots, \hat{x}_i, \ldots, x_{r+1}) \odot \varphi(x_i, z_1, \ldots, z_{r-1}) \\ &= \boxplus_{i=1}^{n}\sigma \odot \varphi(x_1, \ldots, \hat{x}_i, \ldots, x_{r+1}) \odot \varphi^*(y_1, \ldots, \hat{y}_i, \ldots, y_{m-r+1}), \end{aligned} \tag{6.9}$$

where

$$\sigma = (-1)^{r-1}\mathrm{sign}(z_1, \ldots, z_{r-1}, y_1, \ldots, y_{m-r+1}).$$

Multiplying both sides of (6.9) by

$$\sigma \odot \varphi(x_2, \ldots, x_{r+1})^{-1} \odot \varphi^*(y_2, \ldots, y_{m-r+1})^{-1}$$

gives

$$0 \in \boxplus_{i=1}^{n} X(x_i) \odot X(x_1)^{-1} \odot Y(x_i) \odot Y(y_1)^{-1}. \tag{6.10}$$

Multiplying both sides of (6.10) by $X(x_1) \odot Y(y_1)$ then shows that $X \perp Y$. □

Corollary 6.11. *With notation as in Lemma 6.8, we have:*

(1) *For every $x_i, x_j \in \underline{X}$,*

$$\frac{X(x_i)}{X(x_j)} = (-1)^{i-j}\frac{\varphi(x_1, \ldots, \hat{x}_i, \ldots, x_{r+1})}{\varphi(x_1, \ldots, \hat{x}_j, \ldots, x_{r+1})}.$$

(2) *For every $y_i, y_j \in \underline{Y}$,*

$$\frac{Y(y_j)}{Y(y_i)} = \frac{\varphi(y_j, z_1, \ldots, z_{r-1})}{\varphi(y_i, z_1, \ldots, z_{r-1})}.$$

Proof. Same as the proof of [AD12, Corollary 4.4], except now we have $Z(y_i)Y(y_i) = -Z(y_j)Y(y_j)$ instead of $Z(y_j)Y(y_i) = -Z(y_i)Y(y_j)$. □

6.4. **Grassmann-Plücker functions from Dual Pairs.** In the previous section, we associated a dual pair $(\mathcal{C}_\varphi, \mathcal{D}_\varphi)$, depending only on the equivalence class of φ, to each Grassmann-Plücker function φ. However, we don't yet know that $\mathcal{C}_\varphi$ and $\mathcal{D}_\varphi$ satisfy the modular elimination axiom (although this will turn out later to be the case). In this section, we go the other direction, associating a Grassmann-Plücker function to a dual pair.

Theorem 6.12. *Let $\mathcal{C}$ and $\mathcal{D}$ be a dual pair of F-signatures of a matroid $\underline{M}$ of rank r. Then $\mathcal{C} = \mathcal{C}_\varphi$ and $\mathcal{D} = \mathcal{D}_\varphi$ for a rank r Grassmann-Plücker function φ which is uniquely determined up to equivalence.*

Proof. The proof of this result, while rather long and technical, is essentially the same as the special case of complex matroids given in [AD12, Proposition 4.6]. Rather than reproduce the entire argument, which takes up 4.5 pages of [AD12], we will content ourselves with indicating the (minor) changes which need to be made in the present context.

Step 1 from *loc. cit.* goes through without modification. In Step 2, the orthogonality relation $\mathcal{C} \perp \mathcal{D}$ now imples that $Y(f) \odot Y(e)^{-1} = -X(e) \odot X(f)^{-1}$ rather than $Y(e)Y(f)^{-1} = -X(e)X(f)^{-1}$. Thus the displayed equation (4) needs to be replaced with

$$\frac{Y(e)}{Y(f)} = \varphi_{\mathcal{C}}(e, t_2, \ldots, t_r) \odot \varphi_{\mathcal{C}}(f, t_2, \ldots, t_r)$$

(instead of the reciprocal of the right-hand side).

In Step 3, equations (3) and (4) and the assumption $X \perp Y$ show (with notation from *loc. cit.*) that

$$
\begin{aligned}
0 &\in \boxplus_{x_i \in C_S \cap D_T} X(x_i) \odot Y(x_i) \\
&= \boxplus_{x_i \in C_S \cap D_T} \frac{X(x_i)}{X(x_0)} \odot \frac{Y(x_i)}{Y(x_0)} \\
&= \boxplus_{x_i \in C_S \cap D_T} (-1)^i \frac{\varphi_{\mathcal{C}}(x_0, \ldots, \hat{x}_i, \ldots, x_r)}{\varphi_{\mathcal{C}}(x_1, \ldots, x_r)} \odot \frac{\varphi_{\mathcal{C}}(x_i, y_2, \ldots, y_r)}{\varphi_{\mathcal{C}}(x_0, y_2, \ldots, y_r)}
\end{aligned} \tag{6.13}
$$

and multiplying both sides of (6.13) by $\varphi_{\mathcal{C}}(x_1, \ldots, x_r) \odot \varphi_{\mathcal{C}}(x_0, y_2, \ldots, y_r)$ gives

$$0 \in \boxplus_{x_i \in C_S \cap D_T} (-1)^i \odot \varphi_{\mathcal{C}}(x_0, \ldots, \hat{x}_i, \ldots, x_r) \odot \varphi_{\mathcal{C}}(x_i, y_2, \ldots, y_r),$$

which is (GP3). □

6.5. **From Grassmann-Plücker functions to Circuits.** In this section, we prove that the set $\mathcal{C}_\varphi$ of elements of F^E induced by a Grassmann-Plücker function φ is the set of circuits of an F-matroid with support M_φ. The only non-trivial axiom is the Modular Elimination axiom (C3).

Theorem 6.14. *Let φ be a Grassmann-Plücker function on E. Then the set $\mathcal{C}_\varphi \subseteq F^E$ satisfies the Modular Elimination axiom (C3).*

Proof. (cf. [AD12, Proposition 5.3]) For ease of notation we prove this for the dual matroid, i.e., we show that $\mathcal{C}_{\varphi^*}$ satisfies (C3). Let $\underline{M}$ be the matroid on E corresponding to the support of φ. Fix $X, Y \in \mathcal{C}_{\varphi^*}$ and $e \in E$ such that $\underline{X}$ and $\underline{Y}$ form a modular pair in $\underline{M}^*$ and $X(e) = -Y(e) \neq 0$. Since $\underline{X}$ and $\underline{Y}$ form a modular pair, there exist $x, y \in E$ and $A \subset E$ such that $\underline{X} = E \backslash \mathrm{cl}(A \cup \{x\})$ and $\underline{Y} = E \backslash \mathrm{cl}(A \cup \{y\})$. We must have $x \in \underline{Y} \backslash \underline{X}$ and $y \in \underline{X} \backslash \underline{Y}$, for otherwise $\underline{X} = \underline{Y}$ and then $X = \alpha Y$ for some $\alpha \in F^*$, a contradiction.

Fix let D be the unique cocircuit of $\underline{M}$ contained in $(\underline{X} \cup \underline{Y}) \backslash \{e\}$. Note that $x, y \in D$. Fix an ordering $a_2, \ldots, a_d$ of A, and define $Z \in F^E$ by $Z(f) = 0$ if $f \notin D$, $Z(y) = X(y)$, and

$$\frac{Z(f)}{Z(y)} := \frac{\varphi(f, e, A)}{\varphi(y, e, A)}. \tag{6.15}$$

for $f \in D$.

It is clear from the definitions that $Z \in \mathcal{C}_{\varphi^*}$. We need to show that

$$Z(f) \in X(f) \boxplus Y(f) \text{ for all } f \in E. \tag{6.16}$$

Since $Z(f) = X(f) = Y(f) = 0$ for $f \notin D$, we may assume that $f \in D$. When $f \in \underline{Z} \backslash \underline{X}$, one calculates as in the proof of [AD12, Proposition 5.3] that $Z(f) = Y(f)$, and similarly when $f \in \underline{Z} \backslash \underline{Y}$ we have $Z(f) = X(f)$. So (6.16) holds in these cases (and, in particular, $Z(x) = Y(x)$).

We may therefore assume that $f \in \underline{Z} \cap \underline{X} \cap \underline{Y}$. In this case, the proof of [AD12, Proposition 5.3] shows that

$$0 \in \varphi(f, e, A) \odot \varphi(y, x, A) \boxplus -\varphi(y, e, A) \odot \varphi(f, x, A) \boxplus \varphi(y, f, A) \odot \varphi(e, x, A). \tag{6.17}$$

Multiplying both sides of (6.17) by $\varphi(y, e, A)^{-1} \odot \varphi(y, x, A)^{-1}$ gives

$$0 \in \frac{\varphi(f, e, A)}{\varphi(y, e, A)} \boxplus -\frac{\varphi(f, x, A)}{\varphi(y, x, A)} \boxplus \left(\frac{\varphi(y, f, A)}{\varphi(y, x, A)} \odot \frac{\varphi(e, x, A)}{\varphi(y, e, A)} \right),$$

which by Corollary 6.11 gives

$$0 \in \frac{Z(f)}{Z(y)} \boxplus -\frac{X(f)}{X(y)} \boxplus \left(-\frac{Y(f)}{Y(x)} \odot \frac{Z(x)}{Z(y)}\right).$$

Using the fact that $Z(x) = Y(x)$ and multiplying by $Z(y) = X(y)$, this gives

$$0 \in Z(f) \boxplus -X(f) \boxplus -Y(f),$$

which by Lemma 2.2 is equivalent to the desired result $Z(f) \in X(f) \boxplus Y(f)$. □

6.6. **From Circuits to Dual Pairs.** We begin with the following result giving a weak version of the modular elimination axiom which holds for pairs of F-circuits that are not necessarily modular.

Lemma 6.18. *Let $\mathcal{C}$ be the set of circuits of an F-matroid M. Then for all $X, Y \in \mathcal{C}$, $e, f \in E$ with $X(e) = -Y(e) \neq 0$ and $Y(f) \neq -X(f)$, there is $Z \in \mathcal{C}$ with $f \in \underline{Z} \subseteq (\underline{X} \cup \underline{Y}) \backslash e$.*

Proof. This follows from the proof of [AD12, Lemma 5.4], where $X'(g) \leq X(g)$ in *loc. cit.* is interpreted to mean that $X'(g) = 0$ or $X'(g) = X(g)$ (and similarly for $Y'(g)$ and $Y(g)$). Note that the proof of [AD12, Proposition 5.1], which is used in the proof of Lemma 5.4 of *loc. cit.*, holds *mutatis mutandis* for matroids over a hyperfield F. □

The proof of the following result diverges somewhat from the treatment of the analogous fact in [AD12].

Theorem 6.19. *Let M be an F-matroid, and let $\mathcal{C}$ denote the set of circuits of M. There is a unique F-signature $\mathcal{D}$ of $\underline{M}^*$ such that $(\mathcal{C}, \mathcal{D})$ form a dual pair of F-signatures of $\underline{M}$.*

Proof. Let D be a cocircuit of $\underline{M}$. As in the proof of [AD12, Proposition 5.6], choose a maximal independent subset A of D^c. For $e, f \in D$, choose $X_{D,e,f} \in \mathcal{C}$ with support equal to the unique circuit $C_{D,e,f}$ of $\underline{M}$ with support contained in $A \cup \{e, f\}$. Define $\mathcal{D}$ to be the collection of all $W \in F^E$ such that

$$\frac{W(e)}{W(f)} = -\frac{X_{D,e,f}(f)}{X_{D,e,f}(e)} \tag{6.20}$$

for all $e, f \in D := \mathrm{supp}(W)$.

By the proof of Claim 1 in [AD12, Proof of Proposition 5.6], the set $\mathcal{D}$ is well-defined and independent of the choice of $X_{D,e,f}$.

It remains to prove that $\mathcal{C} \perp \mathcal{D}$. (It is easy to see that any F-signature $\mathcal{D}'$ of $\underline{M}^*$ such that $\mathcal{C} \perp \mathcal{D}'$ must coincide with $\mathcal{D}$.) Our argument here differs from the proof of [AD12, Proposition 5.6, Proof of Claims 2 and 3], following instead the outline of [BLVS+99, Proof of Proposition 3.4.1].

Assume for the sake of contradiction that $\mathcal{C} \not\perp \mathcal{D}$, and choose $X \in \mathcal{C}$ and $Y \in \mathcal{D}$ with $X \not\perp Y$ and such that $|\underline{X} \cap \underline{Y}|$ is minimal with this property. We may assume that $|\underline{X} \cap \underline{Y}| \geq 3$, since otherwise one checks easily from the definitions that $X \perp Y$.

By [AD12, Lemma 5.5] applied to $\underline{M}^*$, there exist $e, f \in \underline{X} \cap \underline{Y}$ and $X' \in \mathcal{C}$ such that:

(1) $\underline{X}$ and $\underline{X'}$ are a modular pair.
(2) $e \in \underline{X'} \cap \underline{Y} \subseteq (\underline{X} \cap \underline{Y}) \backslash f$.

Without loss of generality, we may assume that $X'(e) = -X(e)$. Since $|\underline{X'} \cap \underline{Y}| < |\underline{X} \cap \underline{Y}|$, we have $X' \perp Y$.

Modular elimination of e from X' and X gives $X'' \in \mathcal{C}$ such that $X''(f) = X(f) \neq 0$ and

$$X''(g) \in X(g) \boxplus X'(g)$$

for all $g \in E$.

Since $\underline{X''} \subseteq (\underline{X} \cup \underline{X'}) \backslash e$ we have $|\underline{X''} \cap \underline{Y}| < |\underline{X} \cap \underline{Y}|$ and therefore $X'' \perp Y$.

We claim that $X' \perp Y$, $X'' \perp Y$, and $X''(g) \in X(g) \boxplus X'(g)$ for all g imply that $X \perp Y$ (which will give the desired contradiction). To see this, note first that since $X'(e) = -X(e)$ and $X' \perp Y$, we have

$$X(e) \odot Y(e) = -X'(e) \odot Y(e) = \boxplus_{g \neq e} X'(g) \odot Y(g).$$

On the other hand, since $X'' \perp Y$ and $X''(g) \in X(g) \boxplus X'(g)$ for all g we have

$$\begin{aligned} 0 &\in \boxplus_{g \neq e} X''(g) \odot Y(g) \\ &\subseteq (\boxplus_{g \neq e} X(g) \odot Y(g)) \boxplus (\boxplus_{g \neq e} X'(g) \odot Y(g)) \\ &= (\boxplus_{g \neq e} X(g) \odot Y(g)) \boxplus (X(e) \odot Y(e)) \\ &= X \odot Y \end{aligned}$$

as desired. □

6.7. **Cryptomorphic axiom systems for F-matroids.** We can finally prove the main theorems from §3. We begin by proving Theorems 3.11 and 3.17 together in the following result:

Theorem 6.21. *Let E be a finite set. There are natural bijections between the following three kinds of objects:*

(C) *Collections $\mathcal{C} \subset F^E$ satisfying (C0),(C1),(C2),(C3).*
(GP) *Equivalence classes of Grassmann-Plücker functions on E satisfying (GP1),(GP2),(GP3).*
(DP) *Matroids $\underline{M}$ on E together with a dual pair $(\mathcal{C}, \mathcal{D})$ satisfying (DP1),(DP2),(DP3).*

Proof. (GP)⇒(C): If φ is a Grassmann-Plücker function, Theorem 6.14 shows that the set C_φ from Definition 6.7 satisfies (C0)-(C3).

(C)⇒ (DP): If $\mathcal{C}$ satisfies (C0)-(C3) and M denotes the corresponding F-matroid, Theorem 6.19 shows that there is a unique signature $\mathcal{D}$ of $\underline{M}^*$ such that $(\mathcal{C}, \mathcal{D})$ is a dual pair of F-signatures of $\underline{M}$.

(DP)⇒(GP): If $(\mathcal{C}, \mathcal{D})$ is a dual pair of F-signatures of a rank r matroid $\underline{M}$, Theorem 6.12 shows that there is a unique equivalence class of Grassmann-Plücker function $\varphi : E^r \to F$ such that $\mathcal{C} = \mathcal{C}_\varphi$ and $\mathcal{D} = \mathcal{D}_\varphi$. □

We also have the following supplement:

Theorem 6.22. *Let E be a finite set.*

(1) *A function $\varphi : E^r \to F$ satisfies* (GP1),(GP2), *and* (GP3) *if and only if φ satisfies* (GP1),(GP2), *and* (GP3)$'$.
(2) *If $\underline{M}$ is a matroid on E, a pair $(\mathcal{C}, \mathcal{D})$ satisfies* (DP1),(DP2), *and* (DP3) *if and only if it satisfies* (DP1),(DP2), *and* (DP3)$'$.

Proof. It is enough to prove that the natural bijections between (C), (GP), and (DP) in Theorem 6.21 induce bijections between:

(C) Collections $\mathcal{C} \subset F^E$ satisfying (C0),(C1),(C2),(C3).

(GP)$'$ Equivalence classes of Grassmann-Plücker functions φ on E satisfying (GP1),(GP2), and (GP3)$'$.

(DP)$'$ Matroids $\underline{M}$ on E together with a dual pair $(\mathcal{C}, \mathcal{D})$ satisfying (DP1),(DP2), and (DP3)$'$.

(C)$\Rightarrow$ (DP)$'$: This follows from Theorem 6.21, since (DP) trivially implies (DP)$'$.

(DP)$'$ $\Rightarrow$ (GP)$'$: This follows by inspection from the fact that, in the proof of Theorem 6.12 (and the corresponding results [AD12, Lemma 4.5 and Proposition 4.6]), in order to verify the 3-term Grassmann-Plücker relations one only uses the hypothesis $X \perp Y$ in a setting where $|X \cap Y| \leq 3$.

(GP)$'$ $\Rightarrow$ (C): This follows by inspection from the fact that the proof of Theorem 6.14 (and the corresponding result [AD12, Proposition 5.3]) only makes use of the 3-term Grassmann-Plücker relations and the fact that the support of φ is the set of bases of a matroid. □

6.8. **Duality for F-matroids.** In this section, we prove Theorems 3.16 and 3.18. We begin with the following preliminary result:

Lemma 6.23. *Let $\mathcal{C} \subseteq F^E$ be the set of circuits of an F-matroid M. Then the set of elements of $\mathcal{C}^\perp \backslash \{0\}$ of minimal non-empty support is exactly the signature $\mathcal{D}$ of $\underline{M}^*$ given by Theorem 6.19.*

Proof. This is proved exactly like [AD12, Proof of Proposition 5.8]. □

Proof of Theorem 3.16: This follows from Theorem 6.21, Lemma 6.3, and Proposition 6.8 and 6.23, exactly as in [AD12, Proof of Theorem B]. □

Proof of Theorem 3.18: (cf. [AD12, Proof of Theorem D]) This follows from Theorem 6.21 and Lemmas 6.5 and 6.8. □

Appendix A. Errata to [AD12]

Since we rely so heavily in this paper on [AD12], and there are a few small errors in *loc. cit.*, we include the following list of errata:

(1) In Definition 2.4, there should be an additional axiom that the zero vector is not a phased circuit. And axiom (C1) should say $\mathrm{supp}(X) \subseteq \mathrm{supp}(Y)$ rather than $\mathrm{supp}(X) = \mathrm{supp}(Y)$.
(2) In the first bulleted point of §4.2 (top of page 822), b_0 should be b_1.
(3) In the statement of Lemma 5.2, $X(e) = Y(e)$ should be $X(e) = -Y(e)$ and $\mathcal{C}$ should be $\mathcal{C}_\varphi$. Note also that Lemma 5.2 is not actually used in any of the subsequent arguments.
(4) In the statements of Proposition 5.3 and Lemma 5.4, the hypothesis $X(f) \neq Y(f)$ should be replaced with $X(f) \neq -Y(f)$. And in the third line from the end of the proof of Lemma 5.4, $X(f) \neq Y(f) = Y'(f)$ should be $-X(f) \neq Y(f) = Y'(f)$.
(5) In Lemmas 4.5 and Proposition 5.6, the correct hypotheses are that $\mathcal{C}$ and $\mathcal{D}$ form a dual pair of circuit signatures for some matroid M. This is all that is used in the proofs, and if one makes the stronger assumption in Proposition 5.6 that $\mathcal{C}, \mathcal{D}$ are the phased circuits (resp. cocircuits) of a complex matroid then the proof of Corollary 5.7 is incomplete.

(6) In the second line of the proof of Proposition 5.3, the authors refer to the cocircuits of the complex matroid defined by φ, but one doesn't actually know at this point in their chain of reasoning that the modular elimination axiom holds for what eventually ends up being the complex matroid defined by φ. Their proof is nevertheless correct.

Remark A.1. In Definition 2.4, the authors write $Z(g) \leq \max\{X(g), Y(g)\}$ in the "else" case, but this inequality can be replaced with equality; this follows from the "symmetric difference" part of [Whi87, Lemma 2.7.1]. The latter result also implies that axiom (ME) in Definition 2.4 (and also in Proposition A.21) can be replaced with a stronger axiom in which one asks for a **unique** $Z \in \mathcal{C}$ with the stated properties.

References

[AD12] Laura Anderson and Emanuele Delucchi. Foundations for a theory of complex matroids. *Discrete Comput. Geom.*, 48(4):807–846, 2012.

[BBM14] Benoît Bertrand, Erwan Brugallé, and Grigory Mikhalkin. Genus 0 characteristic numbers of the tropical projective plane. *Compos. Math.*, 150(1):46–104, 2014.

[Ber90] Vladimir G. Berkovich. *Spectral theory and analytic geometry over non-Archimedean fields*, volume 33 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 1990.

[BLV78] Robert G. Bland and Michel Las Vergnas. Orientability of matroids. *J. Combinatorial Theory Ser. B.*, 24(1):94–123, 1978.

[BLVS+99] Anders Björner, Michel Las Vergnas, Bernd Sturmfels, Neil White, and Günter M. Ziegler. *Oriented matroids*, volume 46 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1999.

[BPR06] Saugata Basu, Richard Pollack, and Marie-Françoise Roy. *Algorithms in real algebraic geometry*, volume 10 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, second edition, 2006.

[CC10] Alain Connes and Caterina Consani. From monoids to hyperstructures: in search of an absolute arithmetic. In *Casimir force, Casimir operators and the Riemann hypothesis*, pages 147–198. Walter de Gruyter, Berlin, 2010.

[CC11] Alain Connes and Caterina Consani. The hyperring of adèle classes. *J. Number Theory*, 131(2):159–194, 2011.

[Del11] Emanuele Delucchi. Modular elimination in matroids and oriented matroids. *European J. Combin.*, 32(3):339–343, 2011.

[Dre86] Andreas W. M. Dress. Duality theory for finite and infinite matroids with coefficients. *Adv. in Math.*, 59(2):97–123, 1986.

[DW91] Andreas W. M. Dress and Walter Wenzel. Grassmann-Plücker relations and matroids with coefficients. *Adv. Math.*, 86(1):68–110, 1991.

[DW92] Andreas W. M. Dress and Walter Wenzel. Valuated matroids. *Adv. Math.*, 93(2):214–250, 1992.

[FM15] Alex Fink and Luca Moci. Matroids over a ring. To appear in *J. of the European Mathematical Society*. Preprint available at `arXiv:1209.6571`, 48 pages, 2015.

[Fre13] Bart Frenk. Tropical varieties, maps, and gossip. Ph.D. thesis. Available at `http://alexandria.tue.nl/extra2/750815.pdf`, 167 pages, 2013.

[GG15] Jeff Giansiracusa and Noah Giansiracusa. A grassmann algebra for matroids. Preprint. Available at `arxiv:math.AG/1510.04584`, 18 pages, 2015.

[Jun15a] Jaiung Jun. Algebraic geometry over hyperrings. Preprint. Available at `arxiv:math.AG/1512.04837`, 37 pages, 2015.

[Jun15b] Jaiung Jun. Valuations of semirings. Preprint. Available at `arxiv:math.AG/1503.01392`, 12 pages, 2015.

[KL72] Steven L. Kleiman and Dan Laksov. Schubert calculus. *Amer. Math. Monthly*, 79:1061–1082, 1972.

[Lor15] Oliver Lorscheid. Scheme theoretic tropicalization. Preprint. Available at `arxiv:math.AG/1508.07949`, 56 pages, 2015.

[Mar96] Murray A. Marshall. *Spaces of orderings and abstract real spectra*, volume 1636 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1996.

[Mar06] Murray A. Marshall. Real reduced multirings and multifields. *J. Pure Appl. Algebra*, 205(2):452–468, 2006.

[MS15] Diane Maclagan and Bernd Sturmfels. *Introduction to tropical geometry*, volume 161 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2015.

[MT01] Kazuo Murota and Akihisa Tamura. On circuit valuation of matroids. *Adv. in Appl. Math.*, 26(3):192–225, 2001.

[Oxl92] James G. Oxley. *Matroid theory*. Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1992.

[PvZ10] R. A. Pendavingh and S. H. M. van Zwam. Lifts of matroid representations over partial fields. *J. Combin. Theory Ser. B*, 100(1):36–67, 2010.

[PvZ13] R. A. Pendavingh and S. H. M. van Zwam. Skew partial fields, multilinear representations of matroids, and a matrix tree theorem. *Adv. in Appl. Math.*, 50(1):201–227, 2013.

[SW96] Charles Semple and Geoff Whittle. Partial fields and matroid representation. *Adv. in Appl. Math.*, 17(2):184–208, 1996.

[Vir10] Oleg Y. Viro. Hyperfields for Tropical Geometry I. Hyperfields and dequantization. Preprint. Available at `arxiv:math.AG/1006.3034`, 45 pages, 2010.

[Vir11] Oleg Y. Viro. On basic concepts of tropical geometry. *Tr. Mat. Inst. Steklova*, 273(Sovremennye Problemy Matematiki):271–303, 2011.

[Whi87] Neil White, editor. *Combinatorial geometries*, volume 29 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 1987.

E-mail address: `mbaker@math.gatech.edu`

School of Mathematics, Georgia Institute of Technology, Atlanta GA 30332-0160, USA