

Partial Fields in Matroid Theory

PROEFSCHRIFT

ter verkrijging van de graad van doctor aan de
Technische Universiteit Eindhoven, op gezag van de
rector magnificus, prof.dr.ir. C.J. van Duijn, voor een
commissie aangewezen door het College voor
Promoties in het openbaar te verdedigen
op maandag 31 augustus 2009 om 16.00 uur

door

Stefan Hendrikus Martinus van Zwam

geboren te Eindhoven

Dit proefschrift is goedgekeurd door de promotor:

prof.dr.ir. A.M.H. Gerards

Copromotor:

dr. R.A. Pendavingh

A catalogue record is available from the
Eindhoven University of Technology Library

ISBN: 978-90-386-1934-7

Acknowledgements

THE book in front of you — or, if you have downloaded it from the internet, the stack of paper, or even the set of pixels currently on your screen — is the result of four years of study and research. Even though it has a single author, many people contributed to it, in a variety of ways. I will mention a few.

First and foremost I thank Rudi Pendavingh, my supervisor. It has been a real privilege to work with him so intensively for the past five years, first as a Master student, then as a PhD student. His enthusiasm was nearly boundless. On several occasions he kept insisting, while my thoughts were “this cannot possibly be true”. Of course, most often he would be right. Furthermore, his guidance improved my writing immensely.

Next, I thank Bert Gerards, my promotor. Although he was not directly involved in the research during these four years, he did contribute in two important ways. First, he gave, in our seminar on graph and matroid theory, an excellent series of lectures in which he introduced and proved the most important matroid-theoretical concepts. Second, he made a number of valuable suggestions that improved this thesis considerably.

I thank Geoff Whittle and Dillon Mayhew for making my three months in Wellington not only very successful in terms of new results, but also very pleasant.

My colleagues at the Combinatorial Optimization group in Eindhoven provided me with a great working environment. I particularly enjoyed the daily coffee breaks with the PhD students: Christian, John, Leo, Maciej, Matthias, Murat, and Peter.

Tenslotte bedank ik mijn familie, in het bijzonder mijn ouders, mijn broer Marcel, en mijn opa en oma, die me altijd gesteund en aangemoedigd hebben, en die voor de noodzakelijke afleiding zorgden.

Funding

NWO, the Dutch Organization for Scientific Research, funded my position through grant 613.000.561 from the “Open Competitie”. Part of my New Zealand visit was funded by the Marsden Fund of New Zealand.

Contents

Contents	v
1 Introduction	1
1.1 Cross ratios in projective geometry	1
1.2 Matroid theory	7
1.3 Cross ratios in matroid representations	16
1.4 This thesis	18
2 Partial fields, matrices, and matroids	25
2.1 The big picture	25
2.2 Elementary properties of partial fields	26
2.3 \mathbb{P} -matrices	30
2.4 \mathbb{P} -matroids	40
2.5 Examples	47
2.6 Axiomatic partial fields	58
2.7 Skew partial fields and chain groups	64
2.8 Open problems	72
3 Constructions for partial fields	77
3.1 The product of partial fields	78
3.2 The Dowling lift of a partial field	79
3.3 The universal partial field of a matroid	82
3.4 Open problems	92
4 Lifts of matroid representations	95
4.1 The theorem and its proof	98
4.2 Applications	107
4.3 Lift ring	110
4.4 Open problems	112
5 Connectivity	115
5.1 Loops, coloops, elements in series, and elements in parallel	115
5.2 The connectivity function	117
5.3 Blocking sequences	120
5.4 Branch width	121
5.5 Crossing 2-separations	124

6	Confinement to sub-partial fields	129
6.1	The theorem and its proof	131
6.2	Two corollaries	136
6.3	Applications	138
6.4	Open problems	144
7	Excluded-minor characterizations	147
7.1	N -fragile matroids	148
7.2	The theorem and its proof	151
7.3	Applications	159
7.4	Open problems	162
A	Background	165
A.1	Fields, rings, and groups	165
A.2	Algebraic number theory	166
A.3	Matrices and determinants	168
A.4	Graph theory	168
B	A catalog of partial fields	173
	Curriculum Vitae	179
	Summary	181
	Bibliography	183
	Index	189
	Notation	193



Introduction

MATROID theory is a fascinating subject with many faces. One of these is the study of combinatorial aspects of projective geometry. Roughly speaking, a matroid prescribes the *incidence structure* of sets of points: which points are on the same line, which are in the same plane, and so on. An important theme in matroid research is the question how well this information approximates the original structure. For example, can we construct a set of points in projective space with prescribed incidences?

In the answer to such questions a certain invariant under projective transformations features prominently: the *cross ratio*. In this thesis we will study the interplay between cross ratios and geometric structure. On the one hand we will see that the incidence structure imposes restrictions on the cross ratios in potential representations. On the other hand we will see how conditions on the cross ratios may restrict the incidence structures.

In this introduction we treat the necessary background material. In Section 1.1 we will see a glimpse of classical projective geometry, including two definitions of the cross ratio. In Section 1.2 we will continue with a survey of the basic concepts and results of matroid theory. In Section 1.3 we give some examples of how cross ratios show up in matroid representations, and in Section 1.4 we give a summary of the results of this thesis.

1.1 Cross ratios in projective geometry

In the house of mathematics there are many mansions and of these the most elegant is projective geometry.

Morris Kline (in [Newman, 1956](#), p. 613)

The roots of projective geometry can be traced back to the study of perspective by Renaissance painters. In 1525, Albrecht Dürer published a treatise on the



FIGURE 1.1

“The Designer of the Sitting Man”, by Albrecht Dürer, 1525

subject, which included the woodcut reproduced in Figure 1.1. We will illustrate the ideas using photography as an example instead.

Imagine a photographer taking a picture of a chessboard. For simplicity we assume he or she does not have a fancy device with a lens, but merely a box with a tiny hole in one side, and some light-sensitive film on the opposite side. Observed from the side this scene might look something like Figure 1.2(i); the resulting picture would be similar to Figure 1.2(ii). This operation distorts many of the features of the chessboard: angles, lengths, and ratios of lengths are changed, and parallel lines suddenly converge.

Not all structure is lost, however. Straight lines are mapped to straight lines, and if two lines intersect in the original, they intersect in the image. But there is more! Consider the following expression, in which AB denotes the length of the line segment between points A and B . Lengths are “directed”: if AD is positive, then CB is negative, and so on.

1.1.1 DEFINITION. The *cross ratio* of an ordered quadruple of collinear points A, B, C, D is

$$\frac{AC \cdot DB}{CB \cdot AD}.$$

◇

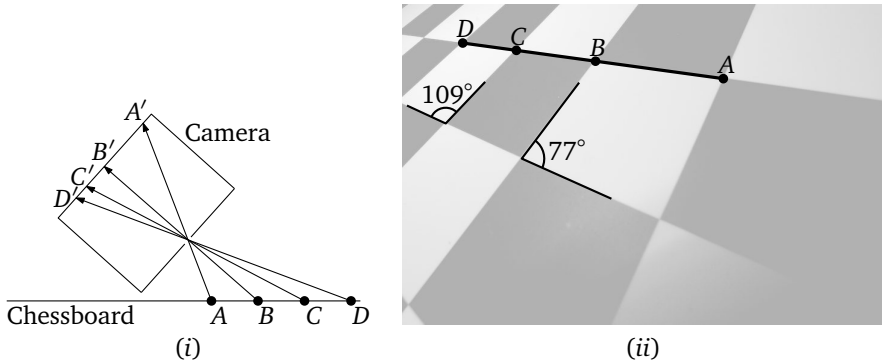


FIGURE I.2
Taking a picture of a chessboard.

The Greek mathematician Pappus of Alexandria, who lived approximately 290–350 A. D., was the first to observe that, in Figure 1.2(i), the following equality holds:

$$\frac{AC \cdot DB}{CB \cdot AD} = \frac{A'C' \cdot D'B'}{C'B' \cdot A'D'}.$$

In other words: the cross ratio is invariant under “projective transformations”! How may we describe such a transformation? A first attempt is the following:

- (i) Pick a point O outside P ;
- (ii) Pick a plane P' not containing O ;
- (iii) For every point $A \in P$, let l_A be the line that passes through A and O ;
- (iv) The image of A is the point on the intersection of l_A and P' .

We say that we have *projected* A *onto* P' *from* O . A sequence of such transformations is called a *projectivity*.

There is one omission in this description, to which we will return shortly, but still it gives the right intuition, so we will dwell on it some more.

I.I.2 EXAMPLE. Consider Figure 1.3. If we project onto P' from O , then onto P'' from O' , and finally back onto P from O'' , we see that we have exchanged A and B , and C and D . ◇

By symmetry it follows that we can exchange any pair, after which the complementary pair will also be exchanged. A consequence of this is that, although the cross ratio depends on the ordering of the points, changing the order will result in at most six distinct values! Another consequence is that in projective geometry there will be no notion of “betweenness”.

Not all is well, though. Consider the projection onto P' from O in Figure 1.4. Where is the image of point C ? Since the line through O and C is parallel to P' , there is no point of intersection! The only way to prevent C from becoming lost is to introduce idealized “points at infinity”, one for each direction, and a “line

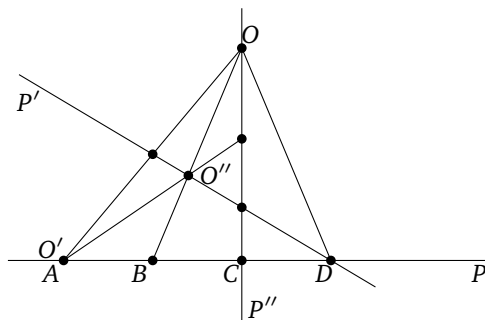


FIGURE 1.3
Exchanging pairs of vertices on a line

at infinity” containing all these points. This approach was invented by Desargues (1591–1661). However, a mathematically more satisfying solution exists, which we introduce now.

1.1.1 Projective space

The key is to reconsider what our basic objects of study are. Instead of taking the points in some plane, why not take the lines through O as our basic objects? For plane projective geometry this leads to the following definition:

1.1.3 DEFINITION. Let \mathbb{F} be a field. The *projective plane* $\text{PG}(2, \mathbb{F})$ over \mathbb{F} is the triple (P, L, I) , where P is the set of 1-dimensional linear subspaces of \mathbb{F}^3 , L is the set of 2-dimensional linear subspaces of \mathbb{F}^3 , and $I : P \times L \rightarrow \{0, 1\}$ is a function defined by

$$I(p, l) = \begin{cases} 1 & \text{if } p \cap l = p \\ 0 & \text{if } p \cap l = \{0\}. \end{cases} \quad \diamond$$

We refer to elements of P as *points* of the projective plane and to elements of L as *lines*. We say a point $p \in P$ is *on* a line $l \in L$ if $I(p, l) = 1$. Symmetrically, we say that a line $l \in L$ is *on* a point $p \in P$ if $I(p, l) = 1$. The following observations are consequences of basic results in linear algebra:

1.1.4 LEMMA. Let $A, B \in P$, and $l, m \in L$.

- (i) There is a unique line $n \in L$ such that both A and B are on n ;
- (ii) There is a unique point $C \in P$ such that both l and m are on C .

In words, every two points are on exactly one line, and every two lines intersect in exactly one point! This fact is a fundamental difference between projective geometry and Euclidean geometry: in the latter parallel lines exist.

There is an obvious extension of Definition 1.1.3 to other dimensions: in projective n -space the *planes* are 3-dimensional subspaces of \mathbb{F}^{n+1} , and so on. The n -dimensional projective geometry over \mathbb{F} is denoted by $\text{PG}(n, \mathbb{F})$. Note that our definitions hold for arbitrary fields!

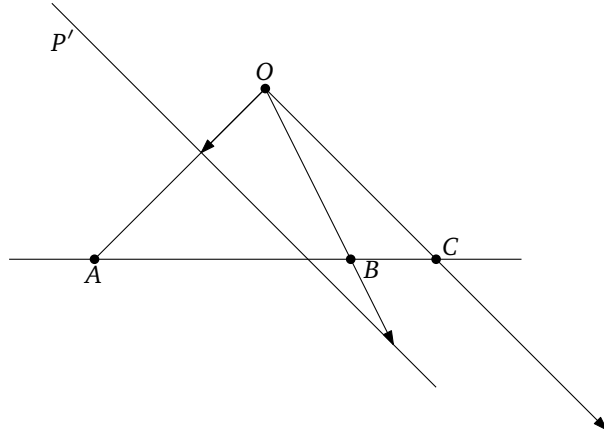


FIGURE I.4
Projection to a “point at infinity”

1.1.2 Projective transformations

What other transformations preserve the incidence structure of a projective space? We might try to modify the definition of projectivity given earlier, by considering the following basic transformation of a projective geometry $\text{PG}(n, \mathbb{F})$:

- (i) Pick an affine hyperplane P in \mathbb{F}^{n+1} not containing O ;
- (ii) Pick a point $O' \in \mathbb{F}^{n+1}$ not in P ;
- (iii) For every point $A \in G$, define $x_A := A \cap P$, the intersection of the 1-dimensional subspace with P ;
- (iv) The image of A is the line through O' and x_A .

See Figure 1.5 for a low-dimensional illustration of this. It turns out that it is possible to describe sequences of such transformations in a much more elementary way: they are *linear transformations*! Let D be an $(n+1) \times (n+1)$ invertible matrix over \mathbb{F} . Viewed as a linear map $D : \mathbb{F}^{n+1} \rightarrow \mathbb{F}^{n+1}$, D maps subspaces to subspaces and preserves incidence. Hence D induces an automorphism of $\text{PG}(n, \mathbb{F})$.

I.I.5 DEFINITION. The group of projective transformations of $\text{PG}(n, \mathbb{F})$ is $\text{GL}_{n+1}(\mathbb{F})$, the group of invertible $(n+1) \times (n+1)$ matrices over \mathbb{F} . \diamond

It is natural to wonder if other incidence-preserving transformations exist. This is certainly the case: field automorphisms are an example. However, as it turns out, that is all:

I.I.6 THEOREM (Fundamental Theorem of Projective Geometry). *If $n \geq 2$, then every incidence-preserving transformation of $\text{PG}(n, \mathbb{F})$ is the composition of an automorphism of \mathbb{F} and a projective transformation.*

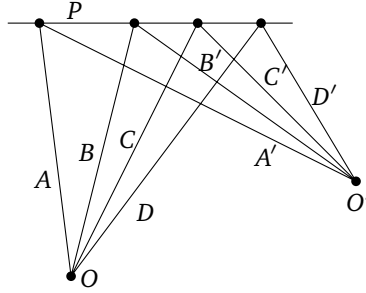


FIGURE 1.5
Elementary projective transformation

1.1.3 The cross ratio

How do we define the cross ratio in this context? Again it will be an element of \mathbb{F} associated to an ordered quadruple of collinear points (i.e. four 1-dimensional subspaces that lie in a 2-dimensional subspace). One option is to project the points onto some affine line contained in the 2-dimensional subspace, and use the cross ratio of this projection as definition. However, this option works only if the field is \mathbb{R} , because it relies on Euclidean distance. The following definition (also found, for example, in [Kaplansky, 1969](#)) works for any field, and even for skew fields:

1.1.7 DEFINITION. Let A, B, C, D be four collinear points in $\text{PG}(n, \mathbb{F})$. Let a, b, c, d be vectors in the 1-dimensional subspaces A, B, C, D respectively, such that

$$\begin{aligned} c &= a + \alpha b \\ d &= a + b \end{aligned}$$

for some $\alpha \in \mathbb{F}$. Then α is the *cross ratio* of the ordered quadruple A, B, C, D . \diamond

Remark that α does not depend on the particular choice of a, b, c, d . It can be checked that Definition 1.1.7 is equivalent to Definition 1.1.1 if $\mathbb{F} = \mathbb{R}$, as follows. Note that

$$\frac{AC \cdot DB}{CB \cdot AD} = \frac{OAC \cdot ODB}{OCB \cdot OAD},$$

where OXY denotes the area of the triangle through points O, X , and Y . Every such area is half the area of a parallelogram, and the latter area can be computed by evaluating a determinant. The result follows by choosing O appropriately, and by considering the effect of scaling on the various determinants.

With this definition it is immediately clear that the cross ratio does not change under projective transformations:

1.1.8 THEOREM. Let A, B, C, D be four collinear points in $\text{PG}(n, \mathbb{F})$. If $F \in \text{GL}_{n+1}(\mathbb{F})$, then the cross ratio of FA, FB, FC, FD equals the cross ratio of A, B, C, D .

Proof: Pick a, b, c, d as in Definition 1.1.7.

$$Fc = Fa + \alpha Fb$$

$$Fd = Fa + Fb,$$

by linearity of F . ■

As before, changing the order of the points results in at most six different values for the cross ratio. This will be our final result before turning to matroid theory.

1.1.9 LEMMA. *Let A, B, C, D be an ordered quadruple of collinear points in $\text{PG}(n, \mathbb{F})$ having cross ratio $\alpha \notin \{0, 1\}$, and let $\sigma \in S_4$ be a permutation. Then the cross ratio of the ordered quadruple $A^\sigma, B^\sigma, C^\sigma, D^\sigma$ is one of*

$$\left\{ \alpha, 1 - \alpha, \frac{1}{1 - \alpha}, \frac{\alpha}{\alpha - 1}, \frac{\alpha - 1}{\alpha}, \frac{1}{\alpha} \right\}.$$

Note that not all six need to be distinct. For instance, if $\alpha = -1$ then this set has only three distinct values.

1.1.4 Further reading

In this section we have seen only a glimpse of projective geometry. The interested reader is referred to Kline (in [Newman, 1956](#), pp. 613–631) for a historical account, and to [Kaplansky \(1969, Chapter 3\)](#) for a mathematical introduction that blends geometry and linear algebra in a way that is close, in spirit, to matroid representation theory. Both texts are very well-written and a joy to read. For a synthetic treatment of the subject [Coxeter \(1964\)](#) is one possible choice.

1.2 Matroid theory

Just as group axioms formalize the intuitive notion of symmetry, matroid axioms formalize the notion of dependence.

Joseph Kung (in [Hazewinkel, 1996](#), p. 159)

In 1935, [Whitney](#) published a paper titled “On the abstract properties of linear dependence.” This title summarizes quite accurately what is studied in *matroid theory*^{*}. In this section we give a short survey of the main concepts of this branch of mathematics.

Let us start by finding out what exactly these abstract properties of dependence are. First we fix some notation. If X and Y are sets, then we denote the set difference as $X - Y := \{x \in X \mid x \notin Y\}$. The expression $|X|$ denotes the cardinality of X . We write $X \cup e$ for $X \cup \{e\}$ and $X - e$ for $X - \{e\}$.

^{*}Despite some resistance, the name “matroid theory” has stuck. Rota (in [Crapo and Rota, 1970](#)) wrote “... the resulting structure is often described by the ineffably cacophonous term “matroid”, which we prefer to avoid in favour of the term “pregeometry”.”

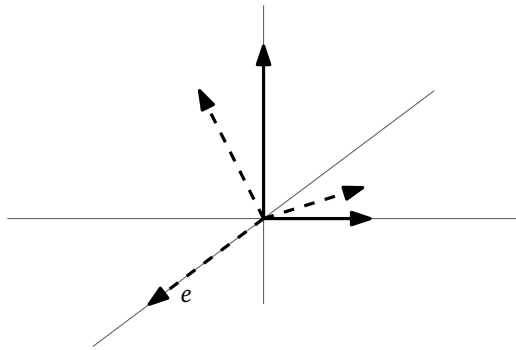


FIGURE 1.6

Two sets of linearly independent vectors in \mathbb{R}^3 . The vectors with solid lines form Y ; the vectors with dashed lines form X .

I.2.1 DEFINITION (Whitney, 1935). A matroid is a pair (E, \mathcal{I}) , where E is a finite set, and \mathcal{I} a collection of subsets of E such that

- (i) $\emptyset \in \mathcal{I}$;
- (ii) If $X \in \mathcal{I}$, and $Y \subseteq X$, then $Y \in \mathcal{I}$;
- (iii) If $X, Y \in \mathcal{I}$, and $|X| > |Y|$, then there is an element $e \in X - Y$ such that $Y \cup e \in \mathcal{I}$. ◇

The set of elements of a matroid M is denoted by $E(M)$, and is called the *ground set* of M . A subset $X \subseteq E(M)$ is *independent* if $X \in \mathcal{I}$, and *dependent* otherwise. Let us illustrate the definition with two examples.

I.2.2 EXAMPLE. Let E be a finite set of vectors in a vector space V , and let $X, Y \subseteq E$ be linearly independent subsets of vectors. Since the vectors in X are linearly independent, the linear subspace U spanned by X has dimension $|X|$. Likewise the linear subspace W spanned by Y has dimension $|Y|$. If $|X| > |Y|$, then not all vectors in X are contained in W . Hence there exists a vector $e \in X - Y$ such that $Y \cup \{e\}$ is linearly independent. See also Figure 1.6. ◇

For the next example we need some basic notions of graph theory. Definitions can be found in Appendix A.4.

I.2.3 EXAMPLE. Let $G = (V, E)$ be a graph, and let $X, Y \subseteq E$ be such that the graphs (V, X) and (V, Y) are forests. The number of components of (V, X) is $|V| - |X|$. Likewise the number of components of (V, Y) is $|V| - |Y|$. If $|X| > |Y|$, then some edge in X must connect two of the components of (V, Y) . Hence there exists an edge $e \in X - Y$ such that $(V, Y \cup e)$ is a forest. See also Figure 1.7. ◇

These two examples are precisely those that led Whitney (1935) to the formulation of Definition 1.2.1. However, there are many more “abstract properties of linear dependence”. Surprisingly often, the structures obtained by taking these properties as axioms are equivalent to the structures of Definition 1.2.1!

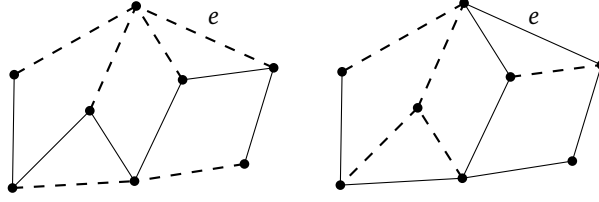


FIGURE I.7

Two forests in a graph G . The edges in X are the dashed lines in the leftmost picture; the edges of Y are the dashed edges in the rightmost picture.

Whitney already observed several instances of this phenomenon. [Birkhoff \(1967\)](#) coined the word *cryptomorphism* for such an equivalence[†]; [Brylawski \(1986\)](#) lists no fewer than thirteen cryptomorphic definitions of a matroid. We now turn to the cryptomorphisms that Whitney found.

1.2.1 Three matroid cryptomorphisms

A *circuit* of a matroid M is an inclusionwise minimal dependent set. Since the independent sets are precisely those that do not contain a circuit, the set of all circuits uniquely determines a matroid. In fact, matroids can be characterized by properties of the set of circuits, as follows:

I.2.4 THEOREM (see [Oxley, 1992](#), Corollary 1.1.5). *Let E be a finite set, and \mathcal{C} a collection of subsets of E . Then \mathcal{C} is the set of circuits of a matroid on E if and only if*

- (i) $\emptyset \notin \mathcal{C}$;
- (ii) If $C, C' \in \mathcal{C}$ and $C' \subseteq C$, then $C' = C$;
- (iii) If $C, C' \in \mathcal{C}$ and $e \in C \cap C'$, then there is a set $C'' \subseteq (C \cup C') - e$ such that $C'' \in \mathcal{C}$.

A *basis* of a matroid M is an inclusionwise maximal independent set. It is an easy consequence of 1.2.1(iii) that all bases have the same size. Moreover, if B, B' are bases, and $e \in B - B'$, then 1.2.1(iii) implies that there is an $f \in B' - B$ such that $B \Delta \{e, f\}$ is a basis. Here we used the *symmetric difference* $X \Delta Y := (X - Y) \cup (Y - X)$. This property, too, characterizes matroids:

I.2.5 THEOREM (see [Oxley, 1992](#), Corollary 1.2.5). *Let E be a finite set, and \mathcal{B} a collection of subsets of E . Then \mathcal{B} is the set of bases of a matroid on E if and only if*

- (i) $\mathcal{B} \neq \emptyset$;
- (ii) If $B, B' \in \mathcal{B}$, and $e \in B - B'$, then there exists an element $f \in B' - B$ such that $B \Delta \{e, f\} \in \mathcal{B}$.

[†]Actually, Birkhoff uses the word *cryptohomomorphism*, but the shortened version seems to prevail these days.

Yet another characterization of matroids is based on the rank function. We denote the collection of all subsets of E by 2^E . Note also that \mathbb{N} , the set of natural numbers, includes 0 in this thesis.

1.2.6 DEFINITION. Let $M = (E, \mathcal{J})$ be a matroid. The *rank function* of M , $\text{rk}_M : 2^E \rightarrow \mathbb{N}$, is defined as

$$\text{rk}_M(X) := \max \{ |Y| \mid Y \subseteq X, Y \in \mathcal{J} \}. \quad \diamond$$

If it is clear which matroid is intended, then we omit the subscript M . We use the shorthand $\text{rk}(M)$ for $\text{rk}_M(E)$.

1.2.7 THEOREM (see [Oxley, 1992](#), Corollary 1.3.4). *Let E be a finite set, and $r : 2^E \rightarrow \mathbb{N}$ a function. Then r is the rank function of a matroid on E if and only if*

- (i) *For all $X \subseteq E$, $0 \leq r(X) \leq |X|$;*
- (ii) *If $Y \subseteq X$ then $r(Y) \leq r(X)$;*
- (iii) *For all $X, Y \subseteq E$,*

$$r(X) + r(Y) \geq r(X \cap Y) + r(X \cup Y). \quad (1.1)$$

A function satisfying (1.1) for all subsets $X, Y \subseteq E$ is called *submodular*.

1.2.2 Matroid representation

By now we have established that matroid axioms are indeed an abstraction of the notion of linear dependence. A natural question is how well these axioms approximate linear dependence. Therefore a central problem in matroid theory is the following: when can the set of dependencies prescribed by the matroid be realized by a set of vectors in some vector space? A first remark is that the answer is “not always”. For some matroids the field underlying the vector space needs to have a certain characteristic. For some matroids a skew field is needed, and for some there exists no set of vectors whatever the vector space may be! A second remark is that scaling individual vectors by a nonzero constant does not change the matroid. Hence we are looking for an embedding of the matroid into $\text{PG}(n, \mathbb{F})$. It will be convenient to choose explicit basis vectors for the points of this projective space, and to collect these as the columns of a matrix.

Now we formalize the notion of representability. First we introduce some notation related to matrices. Recall that formally, for ordered sets X and Y , an $X \times Y$ matrix A over a field \mathbb{F} is a function $A : X \times Y \rightarrow \mathbb{F}$. By virtue of the set-theoretic construction of the natural numbers it is meaningful to talk about $k \times k$ matrices as well. In this case we will number the rows and columns from 1 up to k , rather than from 0 up to $k - 1$ as the set-theoretic construction would suggest.

If $X' \subseteq X$ and $Y' \subseteq Y$, then we denote by $A[X', Y']$ the submatrix of A obtained by deleting all rows and columns in $X - X'$, $Y - Y'$. If Z is a subset of $X \cup Y$ then we define $A[Z] := A[X \cap Z, Y \cap Z]$. Also, $A - Z := A[X - Z, Y - Z]$.

Let A_1 be an $X \times Y_1$ matrix over \mathbb{F} and A_2 an $X \times Y_2$ matrix over \mathbb{F} , where $Y_1 \cap Y_2 = \emptyset$. Then $A := [A_1 A_2]$ denotes the $X \times (Y_1 \cup Y_2)$ matrix with $A_{xy} = (A_1)_{xy}$, for $y \in Y_1$, and $A_{xy} = (A_2)_{xy}$ for $y \in Y_2$. If X is an ordered set, then I_X is the $X \times X$ identity matrix. If A is an $X \times Y$ matrix over \mathbb{F} , then we use the shorthand $[I_X A]$ for $[I_X A]$.

I.2.8 THEOREM (see [Oxley, 1992](#), Proposition 1.1.1). *Let A be an $r \times E$ matrix over \mathbb{F} , and define*

$$\mathcal{J} := \{X \subseteq E \mid \text{rk}(A[r, X]) = |X|\}.$$

Then (E, \mathcal{J}) is a matroid.

The matroid of Theorem 1.2.8 is denoted by $M[A]$. Note that $M[A]$ is exactly the matroid of Example 1.2.2, where the vectors form the columns of A . We say that a matroid M is *representable* over a field \mathbb{F} if there exists a matrix over \mathbb{F} such that $M = M[A]$.

Projective transformations preserve a matroid. We will prove a more general version of the following proposition in Chapter 2.

I.2.9 PROPOSITION. *Let A be an $r \times E$ matrix over \mathbb{F} , and let F be an $r \times r$ nonsingular matrix over \mathbb{F} . Then $M[A] = M[FA]$.*

Matroids that are representable over a number of distinct fields form an important theme of this thesis. We give some examples. A matrix over the real numbers is *totally unimodular* if the determinant of every square submatrix is in the set $\{-1, 0, 1\}$. Such matrices are important in the theory of integer optimization (see [Schrijver, 1986](#)). A matroid is *regular* if it can be represented by a totally unimodular matrix. Tutte proved the following characterization of regular matroids:

I.2.10 THEOREM ([Tutte, 1965](#)). *Let M be a matroid. The following are equivalent:*

- (i) *M is representable over both $\text{GF}(2)$ and $\text{GF}(3)$;*
- (ii) *M is representable over $\text{GF}(2)$ and some field \mathbb{F} that does not have characteristic 2;*
- (iii) *M is representable over \mathbb{R} by a totally unimodular matrix;*
- (iv) *M is representable over every field.*

[Whittle \(1995, 1997\)](#) proved very interesting results of a similar nature. Here is one representative example. We say that a matrix over the real numbers is *totally dyadic* if the determinant of every square submatrix is in the set $\{0\} \cup \{\pm 2^k \mid k \in \mathbb{Z}\}$.

I.2.11 THEOREM ([Whittle, 1997](#)). *Let M be a matroid. The following are equivalent:*

- (i) *M is representable over both $\text{GF}(3)$ and $\text{GF}(5)$;*
- (ii) *M is representable over \mathbb{R} by a totally dyadic matrix;*
- (iii) *M is representable over every field that does not have characteristic 2.*

A third example is the following result, which was announced by Vertigan, though he never published his proof. We say that a matrix over the real numbers is *golden ratio* if the determinant of every square submatrix is in the set $\{0\} \cup \{\pm \tau^k \mid k \in \mathbb{Z}\}$. Here τ is the golden ratio, i.e. the positive root of $x^2 - x - 1 = 0$.

I.2.12 THEOREM (Vertigan, unpublished). *Let M be a matroid. The following are equivalent:*

- (i) *M is representable over both $\text{GF}(4)$ and $\text{GF}(5)$;*

- (ii) M is representable by a golden ratio matrix;
- (iii) M is representable over $\text{GF}(p)$ for all primes p such that $p = 5$ or $p \equiv \pm 1 \pmod{5}$, and also over $\text{GF}(p^2)$ for all primes p .

In this thesis we will give new proofs for these three results.

1.2.3 Duality

In this subsection and the next we describe some fundamental ways to create new matroids out of an existing one.

1.2.13 THEOREM (see [Oxley, 1992](#), Proposition 2.1.1). *Let \mathcal{B} be the set of bases of a matroid M on ground set E . Define*

$$\mathcal{B}^* := \{E - B \mid B \in \mathcal{B}\}.$$

Then \mathcal{B}^ is the set of bases of a matroid.*

The matroid of Theorem 1.2.13 is called the *dual* of M , and denoted by M^* . For representable matroids a representation of the dual is particularly easy to compute:

1.2.14 PROPOSITION (see [Oxley, 1992](#), Theorem 2.2.8). *Let X, Y be disjoint sets. Suppose $M = M[A]$, where A is an $X \times (X \cup Y)$ matrix of the form $A = [I \ D]$, with D an $X \times Y$ matrix. Let A^* be the $Y \times (X \cup Y)$ matrix $A^* := [-D^T \ I]$. Then $M^* = M[A^*]$.*

We will see in the next chapter that every representable matroid can be represented by a matrix of the form $[I \ D]$. It follows that the set of matroids representable over a fixed field \mathbb{F} is closed under duality. The rank function of the dual matroid is the following:

1.2.15 PROPOSITION (see [Oxley, 1992](#), Proposition 2.1.9). *Let M be a matroid, and $X \subseteq E(M)$. Then*

$$\text{rk}_{M^*}(X) = |X| - \text{rk}(M) + \text{rk}_M(E(M) - X).$$

A basis of M^* is called a *cobasis* of M . *Cocircuit*, *corank*, *coindependent* are defined analogously. We give two results concerning cocircuits. In Proposition 1.2.14, the row spaces of A and A^* are orthogonal. The nonzero entries of each row of A correspond to a cocircuit of M , and the nonzero entries of each row of A^* correspond to a circuit of M . The following abstract property of circuits and cocircuits is necessary for this orthogonality to hold:

1.2.16 PROPOSITION (see [Oxley, 1992](#), Proposition 2.1.11). *Let C be a circuit of M , and D a cocircuit of M . Then $|C \cap D| \neq 1$.*

The second result is the following:

1.2.17 PROPOSITION (see [Oxley, 1992](#), Proposition 2.1.16). *Let D be a cocircuit of M , and let B be a basis of M . Then $D \cap B \neq \emptyset$.*

1.2.4 Minors

We continue our survey of basic matroid theory with another central concept: the *minor* of a matroid. First we need to define what it means for matroids to be isomorphic:

I.2.18 DEFINITION. Let $M_1 = (E_1, \mathcal{J}_1)$, $M_2 = (E_2, \mathcal{J}_2)$ be matroids. If there is a bijection $\sigma : E_1 \rightarrow E_2$ such that $X \in \mathcal{J}_1$ if and only if $\sigma(X) \in \mathcal{J}_2$, then we say M_1 and M_2 are *isomorphic*. This is denoted by $M_1 \cong M_2$. \diamond

The matroids M_1 and M_2 are *equal* if $E_1 = E_2$ and $\mathcal{J}_1 = \mathcal{J}_2$.

I.2.19 DEFINITION. Let $M = (E, \mathcal{J})$ be a matroid, and $X \subseteq E$. The *deletion* of X from M is the matroid

$$M \setminus X := (E - X, \{Z \in \mathcal{J} \mid Z \cap X = \emptyset\}). \quad \diamond$$

Occasionally we use the notation $M|X := M \setminus (E(M) - X)$.

I.2.20 DEFINITION. Let M be a matroid, and $X \subseteq E(M)$. The *contraction* of X from M is the matroid

$$M/X := (M^* \setminus X)^*. \quad \diamond$$

In a representation, contraction can be described as follows. Let V be the subspace orthogonal to the space spanned by the vectors in X . Project every vector onto V , and then delete X . Hence *projection* might be a better name for contraction, but history decided otherwise. The name *contraction* has been derived from the corresponding operation in graphs.

Deletion and contraction have the following effect on the rank function:

I.2.21 LEMMA (see Oxley, 1992, Proposition 3.1.6). Let M be a matroid, $X \subseteq E(M)$, and $Y \subseteq E(M) - X$. Then

$$\begin{aligned} \text{rk}_{M \setminus X}(Y) &= \text{rk}_M(Y); \\ \text{rk}_{M/X}(Y) &= \text{rk}_M(X \cup Y) - \text{rk}_M(X). \end{aligned}$$

Matroids are partially ordered with respect to deletion and contraction:

I.2.22 DEFINITION. If a matroid N can be obtained from a matroid M by deleting and contracting elements then N is a *minor* of M . \diamond

I.2.23 DEFINITION. We write $N \preceq M$ if matroid N is isomorphic to a minor of matroid M . \diamond

Note that the order in which elements are deleted and contracted is not important.

I.2.24 THEOREM (see Oxley, 1992, Proposition 3.1.26). Let $e, f \in E(M)$, $e \neq f$. Then
(i) $(M \setminus e) \setminus f = (M \setminus f) \setminus e$;

- (ii) $(M/e)/f = (M/f)/e$;
- (iii) $(M \setminus e)/f = (M/f) \setminus e$.

I.2.25 PROPOSITION. Let M be a matroid representable over a field \mathbb{F} . If $N \preceq M$ then N is representable over \mathbb{F} .

In Chapter 2 we will return to this subject, and show how to construct a representation matrix for N . If a class of matroids is closed under taking minors, then we say it is *minor-closed*.

I.2.26 DEFINITION. Let \mathcal{M} be a minor-closed class of matroids. A matroid M is an *excluded minor* for \mathcal{M} if $M \notin \mathcal{M}$ but, for all $e \in E(M)$, both $M \setminus e \in \mathcal{M}$ and $M/e \in \mathcal{M}$. \diamond

In other words: an excluded minor for a class \mathcal{M} is a matroid not in \mathcal{M} that is minimal in the minor order with respect to this property. The following is obvious:

I.2.27 LEMMA. Let \mathcal{M} be a minor-closed class of matroids, and let M be any matroid. Exactly one of the following holds:

- (i) $M \in \mathcal{M}$;
- (ii) $N \preceq M$ for some excluded minor N for \mathcal{M} .

We denote the class of \mathbb{F} -representable matroids by $\mathcal{M}(\mathbb{F})$. The most famous conjecture in matroid theory is the following:

I.2.28 CONJECTURE (Rota's Conjecture, [Rota, 1971](#)). Let q be a prime power. There are finitely many excluded minors for $\mathcal{M}(\text{GF}(q))$.

So far, Rota's Conjecture has been proven for only three fields. Let $U_{2,4} := M[A]$, where A is the following matrix over \mathbb{R} :

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

I.2.29 THEOREM ([Tutte, 1958](#)). The unique excluded minor for $\mathcal{M}(\text{GF}(2))$ is $U_{2,4}$.

We will not list the excluded minors in the following two theorems explicitly.

I.2.30 THEOREM ([Bixby, 1979](#); [Seymour, 1979](#)). There are exactly 3 excluded minors for $\mathcal{M}(\text{GF}(3))$.

I.2.31 THEOREM ([Geelen, Gerards, and Kapoor, 2000](#)). There are exactly 7 excluded minors for $\mathcal{M}(\text{GF}(4))$.

In contrast, there is an infinite number of excluded minors for the class of \mathbb{R} -representable matroids ([Oxley, 1992](#), p. 208, based on a result by [Lazarson, 1958](#)).

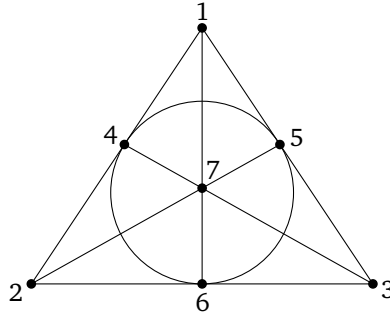


FIGURE I.8
The Fano matroid, F_7 .

1.2.5 Geometric depiction of matroids

If \mathbb{F} is finite then the points of $\text{PG}(n, \mathbb{F})$ are the elements of a matroid, with as independent sets the subsets X of points such that the subspace spanned by them has dimension $|X|$. This matroid is also denoted by $\text{PG}(n, \mathbb{F})$ or, if $\mathbb{F} = \text{GF}(q)$, by $\text{PG}(n, q)$. We can pick a basis vector for each of the 1-dimensional subspaces. If A is the matrix whose columns consist of these basis vectors, then $\text{PG}(n, q) = M[A]$. This matroid does not depend on the particular basis vectors chosen. A different choice amounts to scaling of the columns of A .

If a matroid M has low rank, then it is often convenient to describe it by means of a diagram. In such diagrams the elements of a matroid are indicated by points, if three elements are dependent then they are connected by a line, and if four elements are dependent they lie on a common plane.

I.2.32 EXAMPLE. Consider the Fano matroid, $F_7 := \text{PG}(2, 2)$. It has seven elements. We have $F_7 = M[A]$, where A is the following matrix over $\text{GF}(2)$:

$$\begin{bmatrix} & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} & \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} & \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} & \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} & \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} & \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} & \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \end{bmatrix}.$$

A geometric depiction of F_7 is shown in Figure 1.8. ◇

Note that not all “lines” have to be straight. They will, however, always be connected, and two distinct lines will always have at most one point in common. It is customary to omit lines containing only two points of the matroid from these geometric depictions.

While any two lines intersect in exactly one point in a projective plane, this point of intersection does not have to be an element of the matroid. One curious consequence of this is the following.

I.2.33 EXAMPLE. Consider the two matroids displayed in Figure 1.9. In both matroids, no three of the points are on a common line. Hence these matroids have the same

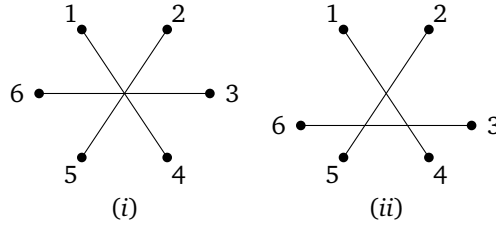


FIGURE 1.9
Two geometric depictions of the matroid $U_{3,6}$. Some lines containing two points are shown.

collection of bases. However, no projective transformation will turn one into the other. \diamond

Not every picture containing points and curves gives rise to a matroid. For pictures in the plane one requirement is that two lines meet in exactly one point. We will not delve into the precise conditions here, but refer again to [Oxley \(1992, Section 1.5\)](#).

1.2.6 Further reading

To keep things focused, proofs have been omitted from this section. For these we have usually referred to the book by [Oxley \(1992\)](#), which serves both as an introduction to the subject, and as a reference to the most important results. [Truemper \(1992b\)](#) has written an introductory textbook with a strong focus on binary matroids and matrices. In particular he describes a technique called “path shortening”, which we will apply several times throughout this thesis. Surveys discussing the historical development of matroid theory can be found in [Schrijver \(2003, Volume B, Chapter 39\)](#) and [Kung \(1986\)](#).

1.3 Cross ratios in matroid representations

Let us see how cross ratios crop up in matroid representation theory. One matroid is especially important in this discussion.

1.3.1 DEFINITION. The *uniform matroid of rank two on four elements* is

$$U_{2,4} := (\{1, 2, 3, 4\}, \{X \subseteq \{1, 2, 3, 4\} \mid |X| \leq 2\}). \quad \diamond$$

A geometric depiction is shown in [Figure 1.10](#). The matroid $U_{2,4}$ is sometimes referred to as the *four-point line*. Let us try to find a representation of $U_{2,4}$ over some field. Since $\text{rk}(U_{2,4}) = 2$, we need to look at vectors in \mathbb{F}^2 . Any set of four distinct nonzero vectors will do. This explains immediately why $U_{2,4}$ is not representable over $\text{GF}(2)$: in $\text{GF}(2)^2$ there are only three distinct nonzero vectors.

Projective transformations of a representation matrix do not change the matroid that is represented. It is well-known that any (ordered) set of $n + 2$ points of

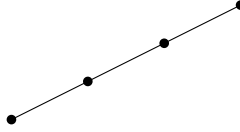


FIGURE I.10
Geometric representation of $U_{2,4}$.

$\text{PG}(n, \mathbb{F})$, of which no subset of $n + 1$ is dependent, can be mapped to any other such set by projective transformations, so we may assume[‡] that our representation matrix is of the following form:

$$A = \begin{matrix} & \begin{matrix} 1 & 2 & 3 & 4 \end{matrix} \\ \begin{matrix} 1 \\ 2 \end{matrix} & \begin{bmatrix} 1 & 0 & 1 & x \\ 0 & 1 & 1 & 1 \end{bmatrix} \end{matrix},$$

where $\det(A'[\{1, 2\}, \{3, 4\}]) = 1 - x \neq 0$. Compare this with Definition 1.1.7. Finding a representation of $U_{2,4}$ boils down to choosing a cross ratio for the ordered quadruple 1, 2, 3, 4! Indeed, if we permute the columns, and apply projective transformations and column scaling to get a matrix of the same form as A , then we obtain each of the following matrices four times:

$$\begin{bmatrix} 1 & 0 & 1 & x \\ 0 & 1 & 1 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 1 & 1-x \\ 0 & 1 & 1 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 1 & \frac{x}{x-1} \\ 0 & 1 & 1 & 1 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & 1 & 1/x \\ 0 & 1 & 1 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 1 & \frac{1}{1-x} \\ 0 & 1 & 1 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 1 & \frac{x-1}{x} \\ 0 & 1 & 1 & 1 \end{bmatrix}.$$

The matroid $U_{2,4}$ is the simplest example of a general phenomenon: finding a representation of a matroid is equivalent to choosing cross ratios for all four-point lines that it has as a minor. From this we conclude that it should be fairly easy to represent binary matroids: there are no four-point lines (by Theorem 1.2.29), so there is nothing to choose. And indeed, it is well-known that binary matroids representable over a field \mathbb{F} have a unique representation over that field (up to projective transformations and column scaling). For $\text{GF}(3)$ the situation is also fine: there is a unique cross ratio, namely -1 . But for bigger fields unique representability no longer holds.

1.3.2 EXAMPLE. Consider the matroid depicted in Figure 1.11. Over $\text{GF}(4)$ there are two possible cross ratios: ω and $\frac{1}{\omega} = 1 + \omega$, where ω is a generator of $\text{GF}(4)$. Suppose we have a representation where the cross ratio of $0abc$ is x , and the cross ratio of $0a'b'c'$ is y . The cross ratio of $0acb$ is x^{-1} , which is different from x . Either $x = y$ or $x^{-1} = y$.

If we swap the labels of the elements b and c then we do not change the matroid. Hence we have constructed two representations of the matroid, one

[‡]A formal proof will be given in Section 2.3.1. Alternatively, see Oxley (1992, Section 6.4).

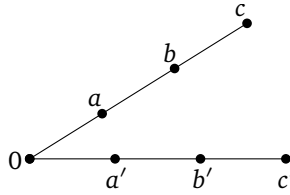


FIGURE I.II

A matroid that is not uniquely representable over $\text{GF}(4)$.

where the cross ratio of $0abc$ is equal to that of $0a'b'c'$, and one where it is not equal. These two representations are not equivalent. No combination of projective transformations and field automorphisms will map one to the other. \diamond

In Example 1.3.2 the cross ratios of the two four-point line minors are completely independent of each other. Often, though, cross ratios interact, and choosing one will fix some others, or at least limit the number of remaining choices. We give one example.

I.3.3 EXAMPLE. Consider the extension of the Non-Fano matroid depicted in Figure 1.12. We assume that this matroid is representable over a field \mathbb{F} . Suppose the cross ratio of 1324 is $p \in \mathbb{F}$. Projecting onto the line through 1 and $4'$ from point 6 we find that the cross ratio of $13'2'4'$ is also p , and projecting onto the line through 1 and 4 from point 5 we find that the cross ratio of 1342 is also p . But 1342 is a permutation of 1324, and its cross ratio is equal to p^{-1} . It follows that $p^{-1} = p$, or $p^2 = 1$. Since $p \notin \{0, 1\}$, we have that $p = -1$.

If \mathbb{F} has characteristic 2, then -1 is equal to 1. Since a cross ratio of 1 indicates that two elements, in this case 2 and 4, are in parallel, the matroid of Figure 1.12 is not representable over \mathbb{F} if \mathbb{F} has characteristic two. \diamond

1.4 This thesis

We will now turn to a short overview of the main results, and how they fit in with other research. This thesis is a study of the interplay between the geometric structure of the matroid and the cross ratios in representations of that matroid. On the one hand, certain structures will enforce certain cross ratios. On the other hand, if the cross ratios are restricted then some geometric configurations will become impossible.

A recurring theme will be matroids that can be represented over a number of different fields. Tutte (1958) was the first to study such matroids. In fact, he studied the class of matroids representable over *every* field, and one of his main results was Theorem 1.2.10, which he proved with his Homotopy Theorem. Whittle (1995, 1997) found several results of a similar nature in his investigation of the representability of ternary matroids, including Theorem 1.2.11. The common feature of Theorems 1.2.10, 1.2.11, and 1.2.12 is that representability over a set of fields is characterized by the existence of a representation matrix over one spe-

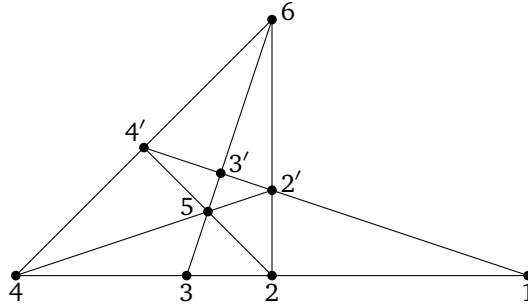


FIGURE I.12
An extension of the Non-Fano matroid.

cific field, such that the determinants of all square submatrices are restricted to a certain set S . Lee (1990) studied representations of a similar nature. Semple and Whittle (1996b) introduced the notion of a partial field to study such results in a systematic way (see also Semple, 1997). Roughly speaking, a partial field is an algebraic structure where multiplication is as usual, but addition is not always defined. The condition “all determinants of square submatrices are in a set S ” then becomes “all determinants of square submatrices are defined”.

In Chapter 2 we build up the theory of partial fields, their homomorphisms, partial-field matrices, and partial-field-representable matroids. Our definition of a partial field, in Section 2.1, differs from that by Semple and Whittle. In Section 2.6 we compare the approaches, show that they are essentially equivalent, and argue that our approach has some conceptual advantages. In Section 2.7 we discuss a third way to build up the theory of partial-field matrices, this time by generalizing the notion of a chain group. Chain groups can already be found in Whitney’s (1935) founding paper, but were developed to a great extent by Tutte (1965). This third definition of a partial-field matrix has the advantage that commutativity is not required. For commutative partial fields it coincides with the first definition.

There are many ways to construct partial fields. In Chapter 3 we give three examples. The first example, in Section 3.1, is the product partial field. With this construction it becomes possible to combine several distinct representations of a matroid into one representation over a new partial field. As a first application we give a very short proof of Theorem 1.2.10.

The second construction, in Section 3.2, is the Dowling lift of a partial field. It provides some insight in the representability of Dowling geometries, an important class of matroids. This class was studied, for instance, by Dowling (1973), Kahn and Kung (1982), and Zaslavsky (1989).

The third, and probably most important, construction is concerned with quite a different representation problem. Rather than looking at a class of matroids with some property, we study the possible representations of a single matroid. This problem has been studied, in various degrees of formalism, by Brylawski and Lucas (1976) (see also Oxley, 1992, Section 6.4), Vámos (1971), White (1975a,b), Fenton (1984), and Baines and Vámos (2003). In Section 3.3 we combine several

of these ideas to define the *universal partial field* of a matroid M , which is the most general partial field over which M is representable. The universal partial field encodes all information on representations of M , and algebraic techniques such as Gröbner-basis computations can be applied to extract some of this information.

In Chapter 4 we prove the *Lift Theorem*, which provides us with the tools to prove results like Theorems 1.2.11 and 1.2.12. In these theorems the difficult part is to show that (i) implies (ii); the remaining implications follow in a straightforward way by exhibiting partial-field homomorphisms. For the difficult implication we are provided with $\varphi(A)$, the image of a partial-field matrix under a partial-field homomorphism. In the chapter we construct a matrix A' such that $\varphi(A') = \varphi(A)$. The Lift Theorem then provides a sufficient condition under which this preimage is actually a partial-field matrix. In Section 4.3 we give an algebraic construction of a partial field for which the preimage is guaranteed to be a partial-field matrix, and in Section 4.2 we give a number of applications of our theorem, including a new proof of Theorem 1.2.11 and a proof of Theorem 1.2.12. The proof of the Lift Theorem is a generalization of Gerards' (1989) proof of the excluded-minor characterization for the class of regular matroids.

For Chapters 6 and 7 we need some more results on matroid connectivity. These results are presented in Chapter 5. Most of these results can be found in the existing literature, and the new results are not deep, nor are they hard to prove.

A major difficulty that arises when we study representations over fields with more than three elements is the existence of inequivalent representations of a single matroid. That is, several matrices that are not equivalent under projective transformations, still have the same independence structure. In some cases the problem can be resolved by imposing a lower bound on the connectivity of the matroids under consideration. A notable result in this context is Kahn's (1988) theorem that a 3-connected, $\text{GF}(4)$ -representable matroid is uniquely representable over that field. Oxley, Vertigan, and Whittle (1996) proved that a 3-connected, $\text{GF}(5)$ -representable matroid has at most six inequivalent representations over $\text{GF}(5)$, and that for no bigger field a bound on the number of $\text{GF}(q)$ -representations of 3-connected matroids exists. Other approaches to control the inequivalent representations include Whittle's (1999) Stabilizer Theorem (which can be used to obtain a concise proof of Kahn's and Oxley et al.'s results), the extension to strong and universal stabilizers by Geelen, Oxley, Vertigan, and Whittle (1998), and the theorem on totally free expansions by the same four authors (2002). The *Confinement Theorem*, which we will prove in Chapter 6, is related to these efforts.

Let M and N be 3-connected matroids, where N is a minor of M . If M is representable over a partial field, and N is representable over a sub-partial field, then the Confinement Theorem states that either M is representable over the sub-partial field, or there is a small extension of N that is already not representable over the sub-partial field.

After proving the Confinement Theorem we give a number of applications, including the following characterization of the inequivalent representations of quinary[§] matroids:

[§]Some authors prefer the word *quinternary*, which has the disadvantage of not being in the dictionary.

1.4.1 THEOREM. *Let M be a 3-connected matroid.*

- (i) *If M has at least two inequivalent representations over $\text{GF}(5)$, then M is representable over \mathbb{C} , over $\text{GF}(p^2)$ for all primes $p \geq 3$, and over $\text{GF}(p)$ when $p \equiv 1 \pmod{4}$.*
- (ii) *If M has at least three inequivalent representations over $\text{GF}(5)$, then M is representable over every field with at least five elements.*
- (iii) *If M has at least four inequivalent representations over $\text{GF}(5)$, then M is not binary and not ternary.*
- (iv) *If M has at least five inequivalent representations over $\text{GF}(5)$, then M has six inequivalent representations over $\text{GF}(5)$.*

The Confinement Theorem does more than that: it is a versatile tool in many different situations. For instance, Whittle’s Stabilizer Theorem is an easy corollary. Another example is a relatively short proof of the following theorem, which is equivalent to [Whittle \(1997, Theorem 1.5\)](#):

1.4.2 THEOREM. *Let M be a 3-connected matroid representable over $\text{GF}(3)$ and some field that does not have characteristic 3. Then M is representable over at least one of $\text{GF}(4)$ and $\text{GF}(5)$.*

A final corollary of the Confinement Theorem which needs to be mentioned is the *Settlement Theorem*. This result combines the theory of universal partial fields with the Confinement Theorem to give conditions under which the number of inequivalent representations of a matroid is bounded by the number of representations of a certain minor. The Settlement Theorem can be seen as an algebraic analogue of the theory on totally free expansions by [Geelen et al. \(2002\)](#).

Let \mathbb{P} be a partial field, and let $\mathcal{M}(\mathbb{P})$ be the class of \mathbb{P} -representable matroids. A natural question is to ask what the set of excluded minors is for $\mathcal{M}(\mathbb{P})$. This question is very difficult in general, and has been settled only for a handful of partial fields and, indeed, for less than a handful of *fields*. Even the question whether such a set is finite is still open for most (partial) fields. Some partial results towards the latter problem are the theorem by [Geelen and Whittle \(2002\)](#) that, for each integer k , finitely many excluded minors have branch width k , and the theorem by [Geelen, Gerards, and Whittle \(2006\)](#) that excluded minors do not have large projective geometries as a minor.

In Chapter 7 we prove a theorem that gives a sufficient condition for the set of excluded minors to be finite. We show that this theorem implies the finiteness of the set of excluded minors in all cases that were previously known. Moreover, we indicate how the techniques of this chapter might be applied in the future to yield a proof that there are finitely many excluded minors for $\mathcal{M}(\text{GF}(5))$. Our proof invokes the main result of [Geelen and Whittle \(2002\)](#), and makes heavy use of the theory of blocking sequences, developed by [Geelen et al. \(2000\)](#) for their proof of the excluded-minor characterization of $\mathcal{M}(\text{GF}(4))$.

1.4.1 Publications

The results in this thesis are based on the following six papers:

- RHIANNON HALL, DILLON MAYHEW, and STEFAN H. M. VAN ZWAM, The excluded minors for near-regular matroids (2009). Submitted.

- DILLON MAYHEW, GEOFF WHITTLE, and STEFAN H. M. VAN ZWAM, An obstacle to a decomposition theorem for near-regular matroids (2009). Submitted.
- DILLON MAYHEW, GEOFF WHITTLE, and STEFAN H. M. VAN ZWAM, Rota's Conjecture and N -fragile matroids (2009). In preparation.
- R. A. PENDAVINGH and S. H. M. VAN ZWAM, Confinement of matroid representations to subsets of partial fields (2008). Submitted.
- R. A. PENDAVINGH and S. H. M. VAN ZWAM, Lifts of matroid representations over partial fields. *J. Combin. Theory Ser. B* (2009). In press.
- R. A. PENDAVINGH and S. H. M. VAN ZWAM, Representing some non-representable matroids (2009). In preparation.



Partial fields, matrices, and matroids

IN this chapter we introduce our main objects of study: partial fields. Partial fields were introduced by [Semple and Whittle \(1996b\)](#) to study generalizations of totally unimodular matrices and regular matroids in a systematic way (see also [Semple, 1997](#)). Our definition will be different: we will start from a ring.

In Section 2.1 the three main subjects of this chapter are introduced: partial fields, matrices, and homomorphisms. These subjects are treated in the next three sections, followed by a section containing many examples of partial fields. In Sections 2.6 and 2.7 we describe two alternative ways to define partial fields and partial-field matroids. In the first of these, the axiomatic approach by Semple and Whittle is described. There we also discuss the precise relationship between partial-field homomorphisms and ring homomorphisms. In Section 2.7 we abandon commutativity of the multiplicative structure and introduce skew partial fields. We use a notion of representability that does not require us to specify a specific basis: the chain group. We conclude the chapter with some open problems.

Several results in this chapter were first proven by [Semple and Whittle \(1996b\)](#). Since we use a different definition, our proofs generally differ from theirs. These proofs, as well as all new results, are based on [Pendavingh and Van Zwam \(2008, 2009a\)](#). Theorem 2.4.26 appears, with a proof sketch, in [Mayhew, Whittle, and Van Zwam \(2009\)](#). A paper containing the results from Section 2.7 is currently in preparation ([Pendavingh and Van Zwam, 2009b](#)).

2.1 The big picture

We start with the definition of a partial field.

2.1.1 DEFINITION. A *partial field* is a pair (R, G) , where R is a commutative ring, and G is a subgroup of R^* such that $-1 \in G$. \diamond

If $\mathbb{P} = (R, G)$ is a partial field, and $p \in R$, then we say that p is an *element of \mathbb{P}* (notation: $p \in \mathbb{P}$) if $p = 0$ or $p \in G$. We define $\mathbb{P}^* := G$. Clearly, if $p, q \in \mathbb{P}$ then also $p \cdot q \in \mathbb{P}$, but $p + q$ need not be an element of \mathbb{P} .

2.1.2 DEFINITION. A partial field is *trivial* if $1 = 0$. ◇

Clearly a partial field is trivial if and only if its ring is the trivial ring. From this it follows that there is a unique trivial partial field.

2.1.3 DEFINITION. Let $\mathbb{P} = (R, G)$ be a partial field, and let A be an $r \times E$ matrix with entries in R . Then A is a *weak \mathbb{P} -matrix* if, for all $X \subseteq E$ such that $|X| = r$, $\det(A[r, X]) \in \mathbb{P}$. ◇

An $r \times E$ weak \mathbb{P} -matrix A is *nondegenerate* if there exists an $X \subseteq E$ with $|X| = r$ and $\det(A[r, X]) \neq 0$. Note that A is always degenerate if \mathbb{P} is trivial.

2.1.4 PROPOSITION. Let $\mathbb{P} = (R, G)$ be a partial field, A a nondegenerate $r \times E$ weak \mathbb{P} -matrix, and define

$$\mathcal{B} := \{X \subseteq E \mid |X| = r, \det(A[r, X]) \neq 0\}.$$

Then \mathcal{B} is the set of bases of a matroid.

Proof: If R is a field then the result is trivial. By Lemma A.1.1(i) there exists a maximal ideal $I \subsetneq R$. By Lemma A.1.1(ii) $\mathbb{F} := R/I$ is a field. Let $\varphi : R \rightarrow \mathbb{F}$ be defined by $\varphi(p) = p + I$ for all $p \in R$. Then φ is a ring homomorphism, and therefore $\det(\varphi(A[r, X])) = \varphi(\det(A[r, X]))$. Since $\varphi(G) \subseteq \mathbb{F}^*$, $\det(\varphi(A[r, X])) = 0$ if and only if $\det(A[r, X]) = 0$. Therefore

$$\mathcal{B} = \{X \subseteq E \mid |X| = r, \det(\varphi(A[r, X])) \neq 0\}.$$

Since A is nondegenerate, $\mathcal{B} \neq \emptyset$. The result now follows from Theorem 1.2.8. ■

In this proof we can already discern an attractive feature of partial fields: homomorphisms can produce distinct representations of a matroid. Following the notation for matroids representable over fields, we denote the matroid of Proposition 2.1.4 by $M[A]$. Some more terminology:

2.1.5 DEFINITION. Let M be a matroid. We say M is *representable* over a partial field \mathbb{P} (or, shorter, \mathbb{P} -representable) if there exists a nondegenerate weak \mathbb{P} -matrix such that $M = M[A]$. Moreover, we refer to A as a *representation matrix* of M , and say M is *represented by A* . ◇

We will denote the set of \mathbb{P} -representable matroids by $\mathcal{M}(\mathbb{P})$. In the rest of this chapter we will build up the theory of partial fields, partial-field matrices, and partial-field matroids.

2.2 Elementary properties of partial fields

From Definition 2.1.1 it follows immediately that the following is an example of a partial field:

2.2.1 EXAMPLE. If \mathbb{F} is a field then $(\mathbb{F}, \mathbb{F}^*)$ is a partial field. \diamond

Throughout this thesis we will see the field \mathbb{F} as the partial field $(\mathbb{F}, \mathbb{F}^*)$. Many more examples will be given in Section 2.5. Partial fields have several properties in common with fields. In particular, cancellation holds:

2.2.2 PROPOSITION. Let $\mathbb{P} = (R, G)$ be a partial field, and let $p, q \in \mathbb{P}$. Then $pq = 0$ if and only if $p = 0$ or $q = 0$.

Proof: The proposition holds trivially for the trivial partial field, so we assume \mathbb{P} is nontrivial. If $p = 0$ then clearly $pq = 0$. Suppose now that $pq = 0$ and $p \neq 0$. If $q \neq 0$ then $p, q \in G$, and therefore $pq \in G$, so $pq \neq 0$, a contradiction. Hence $q = 0$. \blacksquare

2.2.1 Homomorphisms

2.2.3 DEFINITION. Let $\mathbb{P}_1, \mathbb{P}_2$ be partial fields. A function $\varphi : \mathbb{P}_1 \rightarrow \mathbb{P}_2$ is a *partial-field homomorphism* if

- (i) $\varphi(1) = 1$;
- (ii) For all $p, q \in \mathbb{P}_1$, $\varphi(pq) = \varphi(p)\varphi(q)$;
- (iii) For all $p, q, r \in \mathbb{P}_1$ such that $p + q = r$, $\varphi(p) + \varphi(q) = \varphi(r)$. \diamond

We list some elementary properties:

2.2.4 LEMMA. Let $\mathbb{P}_1, \mathbb{P}_2$ be partial fields and $\varphi : \mathbb{P}_1 \rightarrow \mathbb{P}_2$ a partial-field homomorphism.

- (i) $\varphi(0) = 0$;
- (ii) $\varphi(-1) = -1$;

Proof: By 2.2.3(iii), since $1 + 0 = 1 \in \mathbb{P}_1$, $\varphi(1) + \varphi(0) = \varphi(1)$. Hence $\varphi(0) = 0$. Likewise, since $1 + (-1) = 0$, $\varphi(1) + \varphi(-1) = \varphi(0)$. Hence $\varphi(-1) = -1$. \blacksquare

If $\mathbb{P}_1 = (R_1, G_1)$, $\mathbb{P}_2 = (R_2, G_2)$, and $\varphi : R_1 \rightarrow R_2$ is a ring homomorphism such that $\varphi(G_1) \subseteq G_2$, then the restriction of φ to \mathbb{P}_1 is a partial-field homomorphism. There exist partial-field homomorphisms that are not the restriction of a ring homomorphism:

2.2.5 EXAMPLE. Let $R := \text{GF}(2) \times \text{GF}(3)$ be the product ring of $\text{GF}(2)$ and $\text{GF}(3)$. Let $\mathbb{P} := (R, R^*)$, and $\mathbb{U}_0 := (\mathbb{Q}, \{-1, 0, 1\})$. Let $\varphi : \mathbb{P} \rightarrow \mathbb{U}_0$ be defined by $\varphi(0, 0) = 0$, $\varphi(1, 1) = 1$, $\varphi(1, -1) = -1$. Both partial fields have but three elements, and it is easily checked that φ is a partial-field homomorphism (in fact, an isomorphism). However, in R we have

$$\sum_{k=1}^6 (1, 1) = (0, 0),$$

whereas in \mathbb{Q} we have

$$\sum_{k=1}^6 \varphi(1, 1) = 6.$$

It follows that φ can not be extended to a ring homomorphism. \diamond

Still, partial-field homomorphisms are closely related to ring homomorphisms. We will show in Theorem 2.6.11 that every partial-field homomorphism can be obtained as the composition of a partial-field isomorphism $\mathbb{P}_1 \rightarrow (R'_1, G'_1)$ and the restriction of a ring homomorphism $R'_1 \rightarrow R_2$.

The following proposition illustrates just how much partial fields resemble fields.

2.2.6 PROPOSITION. *Let $\mathbb{P} = (R, G)$ be a partial field. There exists a field \mathbb{F} such that there is a partial-field homomorphism $\varphi : \mathbb{P} \rightarrow \mathbb{F}$.*

We omit the proof, which is already contained in the proof of Proposition 2.1.4. Finally we single out some special homomorphisms:

2.2.7 DEFINITION. Let $\mathbb{P}_1, \mathbb{P}_2$ be partial fields, and let $\varphi : \mathbb{P}_1 \rightarrow \mathbb{P}_2$ be a homomorphism. Then φ is an *isomorphism* if

- (i) φ is a bijection;
- (ii) $\varphi(p) + \varphi(q) \in \mathbb{P}_2$ if and only if $p + q \in \mathbb{P}_1$. \diamond

2.2.8 DEFINITION. A partial-field *automorphism* is an isomorphism $\varphi : \mathbb{P} \rightarrow \mathbb{P}$. \diamond

If there is an isomorphism $\varphi : \mathbb{P}_1 \rightarrow \mathbb{P}_2$ then we write $\mathbb{P}_1 \cong \mathbb{P}_2$. The notion of a partial-field isomorphism is much less restrictive than, for instance, the notion of a ring isomorphism. If $(R, G) \cong (R', G')$ then it is true that G and G' are isomorphic groups, but R and R' can be very different rings.

2.2.2 Fundamental elements

2.2.9 DEFINITION. Let \mathbb{P} be a partial field. An element $p \in \mathbb{P}$ is *fundamental* if

$$1 - p \in \mathbb{P}. \quad \diamond$$

We denote the set of fundamental elements of a partial field by $\mathcal{F}(\mathbb{P})$. Note that

$$p + q = p \left(1 - \frac{-q}{p} \right). \quad (2.1)$$

It follows from Definition 2.2.7 and from (2.1) that the partial field \mathbb{P} is determined, up to isomorphism, by its multiplicative group \mathbb{P}^* and the pairs $\{(p, q) \in \mathbb{P}^2 \mid p + q = 1\}$. For many of the partial fields we will consider, $\mathcal{F}(\mathbb{P})$ will be a finite set. This helps to implement those partial fields efficiently on a computer (cf. Hliněný, 2004).

2.2.10 PROPOSITION. *Let \mathbb{P} be a partial field, and p a fundamental element of \mathbb{P} , with $p \notin \{0, 1\}$. Then*

$$\left\{ p, 1 - p, \frac{1}{1 - p}, \frac{p}{p - 1}, \frac{p - 1}{p}, \frac{1}{p} \right\} \subseteq \mathcal{F}(\mathbb{P}).$$

Proof: We show that, if $p \in \mathcal{F}(\mathbb{P}) - \{0, 1\}$, then $1 - p \in \mathcal{F}(\mathbb{P})$ and $\frac{1}{p} \in \mathcal{F}(\mathbb{P})$. The result then follows by repeated application of $x \mapsto 1 - x$ and $x \mapsto \frac{1}{x}$.

Since $1 - (1 - p) = p$, $p \in \mathcal{F}(\mathbb{P})$ immediately implies $1 - p \in \mathcal{F}(\mathbb{P})$. For the second part,

$$1 - \frac{1}{p} = \frac{p - 1}{p}.$$

Since $-1, 1 - p, \frac{1}{p} \in \mathbb{P}$, also $\frac{p-1}{p} \in \mathbb{P}$. ■

Proposition 2.2.10 enables us to describe $\mathcal{F}(\mathbb{P})$ a bit more succinctly:

2.2.II DEFINITION. Let $p \in \mathcal{F}(\mathbb{P})$. The set of associates of p is

$$\text{Asc}(p) := \begin{cases} \{0, 1\} & \text{if } p \in \{0, 1\} \\ \left\{ p, 1 - p, \frac{1}{1-p}, \frac{p}{p-1}, \frac{p-1}{p}, \frac{1}{p} \right\} & \text{otherwise.} \end{cases}$$

Let $S \subseteq \mathcal{F}(\mathbb{P})$. Then the set of associates of S is

$$\text{Asc}(S) = \bigcup_{p \in S} \text{Asc}(p). \quad \diamond$$

Note that $\text{Asc}(S)$ is closed under the operations $x \mapsto 1 - x$ and $x \mapsto \frac{1}{x}$. Remarkably, if $p \notin \{0, 1\}$ then the set $\text{Asc}(p)$ is identical to the set of cross ratios from Lemma 1.1.9. This similarity is not a coincidence. We will study the relation between associates and cross ratios in Section 2.3.4.

Partial-field homomorphisms map fundamental elements to fundamental elements:

2.2.I2 LEMMA. Let $\mathbb{P}_1, \mathbb{P}_2$ be partial fields, $\varphi : \mathbb{P}_1 \rightarrow \mathbb{P}_2$ a partial-field homomorphism, and $p \in \mathcal{F}(\mathbb{P}_1)$. Then $\varphi(p) \in \mathcal{F}(\mathbb{P}_2)$.

Proof: Since $1 - p = r \in \mathbb{P}_1$, $\varphi(1) - \varphi(p) = \varphi(r) \in \mathbb{P}_2$, by Definition 2.2.3(iii). By Definition 2.2.3(i), $\varphi(1) = 1$. The result follows. ■

2.2.3 Sub-partial fields

At several places in this thesis we will run into situations where a partial field is “too large”. In those cases it will be useful to look at sub-partial fields.

2.2.I3 DEFINITION. A pair $\mathbb{P}' = (R', G')$ is a sub-partial field of $\mathbb{P} = (R, G)$ if R' is a subring of R and G' is a subgroup of G , such that $G' \subseteq R'$ and $-1 \in G'$. ◇

We denote this relationship by $\mathbb{P}' \subseteq \mathbb{P}$. The following is obvious:

2.2.I4 PROPOSITION. Let $\mathbb{P}_1, \mathbb{P}_2$ be partial fields, $\varphi : \mathbb{P}_1 \rightarrow \mathbb{P}_2$ a partial-field homomorphism, and $\mathbb{P}'_1 \subseteq \mathbb{P}_1$. Then the restriction of φ to \mathbb{P}'_1 is a partial-field homomorphism $\mathbb{P}'_1 \rightarrow \mathbb{P}_2$.

A useful sub-partial field is the following:

2.2.15 DEFINITION. Let $\mathbb{P} = (R, G)$ be a partial field, and let $S \subseteq \mathbb{P}^*$. Then the sub-partial field generated by S is

$$\mathbb{P}[S] := (R, \langle S \cup \{-1\} \rangle). \quad \diamond$$

Of particular interest will be $\mathbb{P}[\mathcal{F}(\mathbb{P})]$.

2.2.16 PROPOSITION. Let $\mathbb{P}_1, \mathbb{P}_2$ be partial fields and $\varphi : \mathbb{P}_1 \rightarrow \mathbb{P}_2$ a partial-field homomorphism. Then there exists a partial-field homomorphism $\varphi' : \mathbb{P}_1[\mathcal{F}(\mathbb{P}_1)] \rightarrow \mathbb{P}_2[\mathcal{F}(\mathbb{P}_2)]$.

Proof: Let $\mathbb{P}'_1 := \mathbb{P}_1[\mathcal{F}(\mathbb{P}_1)]$ and let $\mathbb{P}'_2 := \mathbb{P}_2[\mathcal{F}(\mathbb{P}_2)]$. Then $\varphi' := \varphi|_{\mathbb{P}'_1} : \mathbb{P}'_1 \rightarrow \mathbb{P}_2$ is a partial-field homomorphism by Proposition 2.2.14. Clearly $\varphi(-1) = -1$. Let $p = p_1 \cdots p_k \in \mathbb{P}'_1$, where $p_1, \dots, p_k \in \mathcal{F}(\mathbb{P}'_1)$. Then $\varphi(p) = \varphi(p_1) \cdots \varphi(p_k) \in \mathbb{P}'_2$, by Lemma 2.2.12. Hence the image of φ' is contained in \mathbb{P}'_2 , which completes the proof. ■

2.2.17 DEFINITION. A sub-partial field \mathbb{P}' of \mathbb{P} is *induced* if

$$\mathcal{F}(\mathbb{P}') = \mathcal{F}(\mathbb{P}) \cap \mathbb{P}'. \quad \diamond$$

If $\mathbb{P}' \subseteq \mathbb{P}$ then $\mathcal{F}(\mathbb{P}') \subseteq \mathcal{F}(\mathbb{P})$, but the precise relationship between the two sets may be unclear. For induced sub-partial fields this relationship is easily described:

2.2.18 LEMMA. If $\mathbb{P}' = (R', G')$ is a sub-partial field of $\mathbb{P} = (R, G)$, and there exists a subring $R'' \subseteq R'$ such that $G' = G \cap (R'')^*$, then \mathbb{P}' is an induced sub-partial field.

Proof: This follows immediately since $-1 \in R''$ and R'' is closed under addition. ■

Not every sub-partial field is induced. Consider, for example, the partial field $\mathbb{K}_2 := (\mathbb{Q}(\alpha), \langle -1, \alpha, 1 - \alpha, 1 + \alpha \rangle)$. Then $\mathbb{U}_1 := (\mathbb{Q}(\alpha), \langle -1, \alpha, 1 - \alpha \rangle)$ is a sub-partial field. We have $\alpha^2 \in \mathcal{F}(\mathbb{K}_2)$, since $1 - \alpha^2 = (1 - \alpha)(1 + \alpha)$, and $\alpha^2 \in \mathbb{U}_1$, but $\alpha^2 \notin \mathcal{F}(\mathbb{U}_1)$. The latter fact will be proven in Section 2.5.

2.3 \mathbb{P} -matrices

The following lemma allows for some manipulation of weak \mathbb{P} -matrices.

2.3.1 LEMMA. Let \mathbb{P} be a partial field, and A an $r \times E$ weak \mathbb{P} -matrix. Let D be an $r \times r$ matrix with $\det(D) \in \mathbb{P}^*$. Then DA is a weak \mathbb{P} -matrix. Moreover, $\det((DA)[r, X]) = 0$ if and only if $\det(A[r, X]) = 0$, for all $X \subseteq E$ such that $|X| = r$.

Proof: Let $X \subseteq E$ be such that $|X| = r$. Then

$$\det((DA)[r, X]) = \det(D(A[r, X])) = \det(D) \det(A[r, X]).$$

Since $\det(D) \in \mathbb{P}^*$, and $\det(A[r, X]) \in \mathbb{P}$, the result follows. ■

Note that Lemma 2.3.1 contains row operations (scaling a row by an element of \mathbb{P}^* , exchanging rows, adding a multiple of one row to another) as a special case. However, there is no analogue of Gaussian reduction. In fact, it is well possible that no entry of A is a unit.

While weak \mathbb{P} -matrices provide a reasonable theory of matroid representation, there are some shortcomings. For instance, ring homomorphisms map weak \mathbb{P} -matrices to weak \mathbb{P} -matrices*, but it is not clear if partial-field homomorphisms have this property. A more serious shortcoming is that it is not obvious that being representable over \mathbb{P} is a minor-closed property. To overcome these limitations we will define a more restricted class of matrices over a partial field. In the remainder of this section we prove some basic results on this class, and in the next section we connect these with matroid representation.

- 2.3.2 DEFINITION. Let $\mathbb{P} = (R, G)$ be a partial field, and let A be an $X \times Y$ matrix with entries in R . Then A is a *strong \mathbb{P} -matrix* if $\det(A[X', Y']) \in \mathbb{P}$, for all $X' \subseteq X$, $Y' \subseteq Y$ such that $|X'| = |Y'|$. \diamond

We will use the term *subdeterminant* for the determinant of a square submatrix of A . Definition 2.3.2 can then be reformulated as “ A is a strong \mathbb{P} -matrix if every subdeterminant is in \mathbb{P} .”

- 2.3.3 PROPOSITION. Let $\mathbb{P} = (R, G)$ be a partial field, and let A be an $X \times Y$ nondegenerate weak \mathbb{P} -matrix. Let $Y' \subseteq Y$ be such that $|Y'| = |X|$ and $\det(A[X, Y']) \neq 0$, and let $D := A[X, Y']^{-1}$. Then DA is a strong \mathbb{P} -matrix.

Proof: Let $Y' \subseteq Y$ be such that $|Y'| = |X|$ and $\det(A[X, Y']) \neq 0$. By Lemma A.3.3(ii), $A[X, Y']$ has an inverse. Let $D := A[X, Y']^{-1}$. For simplicity we assume that both the rows and columns of D are labelled by X , so DA is an $X \times Y$ matrix. Observe that $(DA)[X, Y']$ is an identity matrix. By Lemma 2.3.1 DA is a weak \mathbb{P} -matrix, so all determinants of $|X| \times |X|$ submatrices are in \mathbb{P} . Suppose now that all $(k+1) \times (k+1)$ subdeterminants are in \mathbb{P} , and let $X'' \subset X, Y'' \subset Y$ be such that $|X''| = |Y''| = k$. Pick an $x \in X - X''$. There is a unique $y \in Y'$ such that $(DA)_{xy} = 1$. If $y \in Y''$ then $DA[X'', Y'']$ contains an all-zero column, and $\det(DA[X'', Y'']) = 0$. Therefore we may assume $y \notin Y''$. Now $\det(DA[X'' \cup x, Y'' \cup y]) = (-1)^s \det(DA[X'', Y''])$ for some $s \in \{0, 1\}$, which can be seen by expanding the determinant along column y . But since the former is in \mathbb{P} by assumption, so is the latter. The result follows by induction. \blacksquare

- 2.3.4 PROPOSITION. Let A be a strong \mathbb{P} -matrix. Then A^T and $[IA]$ are also strong \mathbb{P} -matrices.

Proof: The first statement follows trivially from $\det(A) = \det(A^T)$. We prove the second. Let $A = [ID]$ be a $Z \times (X \cup Y)$ matrix with entries in \mathbb{P} such that $|X| = |Z|$ and $A[Z, Y]$ is a strong \mathbb{P} -matrix. Now let $Z' \subseteq Z \cup X \cup Y$ such that $A[Z']$ is square. We prove that $\det(A[Z']) \in \mathbb{P}$ by induction on $|Z' \cap X|$, the case $Z' \cap X = \emptyset$ being trivial. Pick $x \in Z' \cap X$. If $A_{zx} = 0$ for all $z \in Z' \cap Z$ then $\det(A[Z']) = 0$ and we

*This fact is easily proven using arguments similar to the proof of Proposition 2.1.4.

are done. Suppose that $z \in Z' \cap Z$ is such that $A_{zx} = 1$. By expanding $\det(A[Z'])$ along column x we find that

$$\det(A[Z']) = (-1)^s \det(A[Z' - \{z, x\}])$$

for some $s \in \{0, 1\}$. ■

We will sometimes refer to the rank of a strong \mathbb{P} -matrix.

2.3.5 DEFINITION. Let A be an $X \times Y$ strong \mathbb{P} -matrix. The *rank* of A is

$$\text{rk}(A) := \max \{ k \in \mathbb{N} \mid \text{there are } X' \subseteq X, Y' \subseteq Y \text{ with } |X'| = |Y'| = k, \\ \text{and } \det(A[X', Y']) \neq 0 \}. \quad \diamond$$

The following is easily checked:

2.3.6 LEMMA. Let \mathbb{P} be a partial field, let \mathbb{F} be a field, and let $\varphi : \mathbb{P} \rightarrow \mathbb{F}$ be a partial-field homomorphism. If A is a square strong \mathbb{P} -matrix, then $\text{rk}(A) = \text{rk}(\varphi(A))$, where the right-hand side is the usual matrix rank function.

From now on we will drop the adjective “strong”, and take “ \mathbb{P} -matrix” to mean “strong \mathbb{P} -matrix”.

2.3.1 Permuting and scaling

Several operations can be defined mapping \mathbb{P} -matrices to \mathbb{P} -matrices. The easiest of these is permuting the rows or permuting the columns of A . The following follows immediately from Proposition A.3.2(ii) and Proposition 2.3.4:

2.3.7 PROPOSITION. Let A be a \mathbb{P} -matrix. If A' is obtained from A by swapping two rows or swapping two columns, then A' is a \mathbb{P} -matrix.

We may occasionally permute rows and columns implicitly. For the remainder of this section we consider a more interesting operation: row and column scaling. The following is a direct corollary of Proposition A.3.2(iii) and Proposition 2.3.4.

2.3.8 PROPOSITION. Let A be a \mathbb{P} -matrix. If A' is obtained from A by multiplying all entries of a row or column of A by p for some $p \in \mathbb{P}$, then A' is a \mathbb{P} -matrix.

If $p \in \mathbb{P}^*$ then A can again be obtained from A' . This prompts the following definition:

2.3.9 DEFINITION. Let A, A' be $X \times Y$ \mathbb{P} -matrices. We say that A and A' are *scaling-equivalent*, denoted by $A \sim A'$, if A' can be obtained from A by scaling rows and columns by elements from \mathbb{P}^* . ◇

A necessary condition for scaling-equivalence is that $A_{xy} = 0$ if and only if $A'_{xy} = 0$. Scaling-equivalence is transitive, and it is often useful to have a normal form. For that we resort to graph theory. We repeat that relevant definitions can be found in Appendix A.4.

2.3.10 DEFINITION. Let A be an $X \times Y$ matrix for disjoint sets X, Y . Then $G(A)$ is the bipartite graph with vertices $X \cup Y$ and edges $\{xy \in X \times Y \mid A_{xy} \neq 0\}$. \diamond

We can scale the entries of a spanning forest of $G(A)$ arbitrarily. The following lemma is the generalization of a well-known result by [Brylawski and Lucas \(1976\)](#) to partial fields (see also [Oxley, 1992](#), Theorem 6.4.7).

2.3.11 LEMMA. Let \mathbb{P} be a partial field, and A an $X \times Y$ \mathbb{P} -matrix for disjoint sets X, Y . Let T be a spanning forest of $G(A)$ with edges e_1, \dots, e_k . Let $p_1, \dots, p_k \in \mathbb{P}^*$. Then there exists a matrix $A' \sim A$ such that $A'_{e_i} = p_i$ for $i = 1, \dots, k$.

Proof: Suppose $G(A) = (X \cup Y, E)$, and let T be a spanning forest of $G(A)$. Let $F \subseteq E(T)$, and suppose $A_{e_i} = p_i$ for all i such that $e_i \in F$. Now pick $e_i \in E(T) - F$. Then $e_i = vw$ connects two components of $(X \cup Y, F)$. Suppose $v \in X$ and let C be the set of vertices of one of the component containing v . Let A' be the matrix obtained from A by scaling all rows in $C \cap X$ by p_i/A_{e_i} , and all columns in $C \cap Y$ by A_{e_i}/p_i . Since $w \notin C$, $A'_{e_i} = p_i$, and for all j such that $e_j \in F$, $A'_{e_j} = p_j$. The result follows by induction. \blacksquare

In fact, the matrix A' is unique:

2.3.12 LEMMA. If $A' \sim A$ and $A'_e = A_e$ for all edges e of a spanning forest of $G(A)$, then $A' = A$.

Proof: Suppose that there exist matrices $A \sim A'$ and a spanning forest T of $G(A)$, such that $A_e = A'_e$ for all $e \in T$ but $A \neq A'$. Let H be the subgraph of $G(A)$ consisting of all edges $e \in E(G(A))$ such that $A_e = A'_e$. For every edge $e = vw \in E(G(A)) - E(H)$ there is a $v - w$ path contained in H , since $T \subseteq H$ and T is a spanning forest. Pick such an $e = vw$ minimizing the length of a shortest $v - w$ path in H . Then e completes an induced cycle C with this path, say $C = (r_1, c_1, r_2, c_2, \dots, r_k, c_k, r_1)$ for $r_1, \dots, r_k \subseteq X$ and $c_1, \dots, c_k \subseteq Y$, $v = r_1$, and $w = c_k$. Since $A' \sim A$, also $A'[V(C)] \sim A[V(C)]$. Suppose $A'[V(C)]$ can be obtained from $A[V(C)]$ by scaling row r_1 by $p_1 \in \mathbb{P}^*$. Since $A_{r_1 c_1} = A'_{r_1 c_1}$, column c_1 then needs to be scaled by p_1^{-1} . Since $A_{r_2 c_1} = A'_{r_2 c_1}$, row r_2 then needs to be scaled by p_1 . Continuing this argument we conclude that column c_k needs to be scaled by p_1^{-1} . But then $A'_{r_1 c_k} = p_1 p_1^{-1} A_{r_1 c_k} = A_{r_1 c_k}$, contradicting our choice of H . \blacksquare

A slightly more concise proof can be given by invoking Lemma 2.3.38(i) once the cycle C has been found.

2.3.13 DEFINITION. Let A be a matrix and T a spanning forest for $G(A)$. We say that A is T -normalized if $A_{xy} = 1$ for all $xy \in T$. We say that A is normalized if it is T -normalized for some spanning forest T , the *normalizing* spanning forest. \diamond

By Lemma 2.3.11 there is always an $A' \sim A$ that is T -normalized.

2.3.2 Pivoting

With weak \mathbb{P} -matrices any invertible linear transformation resulted in another weak \mathbb{P} -matrix. We would like a similar operation for (strong) \mathbb{P} -matrices. One problem is that, if A, D are square \mathbb{P} -matrices, DA is not necessarily a \mathbb{P} -matrix. Hence we need to replace Lemma 2.3.1 by something more restricted. That operation is the pivot.

2.3.14 DEFINITION. Let A be an $X \times Y$ matrix over a ring R , and let $x \in X, y \in Y$ be such that $A_{xy} \in R^*$. Then we define A^{xy} to be the $(X - x) \cup y \times (Y - y) \cup x$ matrix with entries

$$(A^{xy})_{uv} = \begin{cases} (A_{xy})^{-1} & \text{if } uv = yx \\ (A_{xy})^{-1}A_{xv} & \text{if } u = y, v \neq x \\ -A_{uy}(A_{xy})^{-1} & \text{if } v = x, u \neq y \\ A_{uv} - A_{uy}(A_{xy})^{-1}A_{xv} & \text{otherwise.} \end{cases} \quad \diamond$$

We say that A^{xy} is obtained from A by *pivoting* over xy . The motivation behind this definition is as follows. Consider the matrix $[IA]$, say

$$[IA] = \begin{array}{c} x \\ x' \end{array} \left[\begin{array}{c|c|c|c} x & x' & y & y' \\ \hline 1 & 0 \cdots 0 & a & c \\ \hline 0 & & b & D \\ \hline \vdots & I_{X'} & & \\ \hline 0 & & & \end{array} \right].$$

We wish to turn the submatrix indexed by the columns $X' \cup y$ into an identity matrix. First we apply row operations to give y the desired form. Let

$$F := \begin{array}{c} y \\ x' \end{array} \left[\begin{array}{c|c} x & x' \\ \hline a^{-1} & 0 \cdots 0 \\ \hline -a^{-1}b & I_{X'} \end{array} \right]. \quad (2.2)$$

The matrix F is the inverse of $[IA][X, y \cup X']$. Then

$$F[IA] = \begin{array}{c} y \\ x' \end{array} \left[\begin{array}{c|c|c|c} x & x' & y & y' \\ \hline a^{-1} & 0 \cdots 0 & 1 & a^{-1}c \\ \hline -a^{-1}b & I_{X'} & 0 & D - a^{-1}bc \\ \hline \vdots & & \vdots & \\ \hline 0 & & 0 & \end{array} \right].$$

Next we swap columns x and y . Let P be the corresponding permutation matrix. Then

$$F[IA]P = \begin{array}{c} y \\ x' \end{array} \left[\begin{array}{c|c|c|c} y & x' & x & y' \\ \hline 1 & 0 \cdots 0 & a^{-1} & a^{-1}c \\ \hline 0 & & -a^{-1}b & D - a^{-1}bc \\ \hline \vdots & I_{X'} & & \\ \hline 0 & & & \end{array} \right].$$

By comparing this with Definition 2.3.14 we conclude the following:

2.3.15 LEMMA. *Let F be as in (2.2), and P the permutation matrix swapping x and y . Then*

$$F[IA]P = [IA^{xy}].$$

Pivots map \mathbb{P} -matrices to \mathbb{P} -matrices:

2.3.16 PROPOSITION. *Let A be an $X \times Y$ \mathbb{P} -matrix, and let $x \in X, y \in Y$ be such that $A_{xy} \neq 0$. Then A^{xy} is a \mathbb{P} -matrix.*

Proof: This follows immediately from Lemma 2.3.15 and Proposition 2.3.3. ■

The following lemma can be proven directly from the definition:

2.3.17 LEMMA. $(A^{xy})^{yx} = A$.

Pivots can be used to compute determinants:

2.3.18 LEMMA. *Let R be a ring, and let A be an $r \times r$ matrix over R such that $A_{xy} \in R^*$. Then*

$$\det(A) = (-1)^{x+y} A_{xy} \det(A^{xy} - \{x, y\}).$$

Proof: Since A_{xy} is invertible, we can apply row reduction. Suppose $x = 1, y = 1$. Then

$$A = \begin{matrix} & \begin{matrix} y & Y' \end{matrix} \\ \begin{matrix} x \\ X' \end{matrix} & \begin{bmatrix} a & c \\ b & D \end{bmatrix} \end{matrix}.$$

Let F be as in (2.2). Then $\det(F) = a^{-1}$, so by Lemma 2.3.1 we have $\det(FA) = a^{-1} \det(A)$. Moreover,

$$FA = \begin{matrix} & \begin{matrix} y & Y' \end{matrix} \\ \begin{matrix} x \\ X' \end{matrix} & \begin{bmatrix} 1 & c \\ 0 & D - a^{-1}bc \end{bmatrix} \end{matrix}.$$

Note that $FA - \{x, y\} = A^{xy} - \{x, y\}$. The lemma follows by expanding $\det(FA)$ along the first column. If x, y do not label the first row and column, then row and column exchanges account for the $(-1)^{x+y}$ multiplier. ■

The following result follows immediately from Lemma 2.3.15.

2.3.19 LEMMA. *Let A be an $X \times Y$ \mathbb{P} -matrix for disjoint sets X, Y , and let $Z \subseteq X \cup Y$ be such that $|Z| = |X|$. Let $x \in X, y \in Y$ be such that $A_{xy} \neq 0$. Then*

$$\det([IA][X, Z]) = 0 \text{ if and only if } \det([IA^{xy}][X \Delta \{x, y\}, Z]) = 0.$$

Pivots form the ingredient that makes partial-field homomorphisms work:

2.3.20 PROPOSITION. *Let \mathbb{P}, \mathbb{P}' be partial fields, A a \mathbb{P} -matrix, and $\varphi : \mathbb{P} \rightarrow \mathbb{P}'$ a partial-field homomorphism. Then $\varphi(A)$ is a \mathbb{P}' -matrix, and $\det(\varphi(A[Z])) = \varphi(\det(A[Z]))$ for all Z such that $A[Z]$ is square.*

The main idea behind the proof is that it is possible to evaluate determinants such that all intermediate results are in the partial field.

Proof: Suppose the proposition is false, and let A be a counterexample with as few rows and columns as possible. Then A is a square matrix, say of size $k \times k$. For $k = 1$ the proposition holds, so assume $k \geq 2$. Every row and column of A has at least one nonzero entry, since otherwise $\det(\varphi(A)) = 0$. Without loss of generality we assume $A_{11} \neq 0$. From Lemma 2.3.18 we learn that

$$\begin{aligned}\det(A) &= A_{11} \det(A^{11}[\{2, \dots, k\}, \{2, \dots, k\}]), \\ \det(\varphi(A)) &= \varphi(A_{11}) \det(\varphi(A^{11}[\{2, \dots, k\}, \{2, \dots, k\}])).\end{aligned}$$

By induction we have

$$\begin{aligned}\det(\varphi(A)) &= \varphi(A_{11}) \det(\varphi(A^{11}[\{2, \dots, k\}, \{2, \dots, k\}])) \\ &= \varphi(A_{11}) \varphi(\det(A^{11}[\{2, \dots, k\}, \{2, \dots, k\}])) \\ &= \varphi(A_{11} \det(A^{11}[\{2, \dots, k\}, \{2, \dots, k\}])) \\ &= \varphi(\det(A)),\end{aligned}$$

which contradicts our choice of A . The proposition follows. ■

2.3.3 Minors and equivalence

2.3.21 DEFINITION. Let A be an $X \times Y$ \mathbb{P} -matrix. We say that A' is a *minor*[†] of A if A' can be obtained from A by a sequence of the following operations:

- (i) Permuting rows or columns (and permuting labels accordingly);
- (ii) Multiplying the entries of a row or column by an element of \mathbb{P}^* ;
- (iii) Deleting rows or columns;
- (iv) Pivoting over a nonzero entry.

◇

2.3.22 PROPOSITION. *If A' is a minor of A then A' is a \mathbb{P} -matrix.*

Proof: That the third operation preserves \mathbb{P} -matrices is obvious from Definition 2.3.2. The remaining claims follow from Propositions 2.3.7, 2.3.8, and 2.3.16. ■

We now introduce a number of notions of equivalence of \mathbb{P} -matrices.

2.3.23 DEFINITION. Let A be an $X \times Y$ \mathbb{P} -matrix, and let A' be an $X' \times Y'$ \mathbb{P} -matrix. Then A and A' are *isomorphic* if there exist bijections $f : X \rightarrow X'$, $g : Y \rightarrow Y'$ such that for all $x \in X, y \in Y$, $A_{xy} = A'_{f(x)g(y)}$. ◇

[†]Be aware that in linear algebra a “minor of a matrix” is defined differently. We use Definition 2.3.21 because of its relation with matroid minors, which will be explained in the next section. For a determinant of a square submatrix we use the word *subdeterminant*.

2.3.24 DEFINITION. We write $A' \preceq A$ if A' is isomorphic to a minor of A . \diamond

We have already seen scaling-equivalence in Definition 2.3.9, but we repeat it here for convenience:

2.3.25 DEFINITION. Let A, A' be $X \times Y$ \mathbb{P} -matrices. If A' can be obtained from A by scaling rows and columns by elements from \mathbb{P}^* , then we say that A and A' are *scaling-equivalent*, which we denote by $A \sim A'$. \diamond

The next two definitions introduce pivots:

2.3.26 DEFINITION. Let A be an $X \times Y$ \mathbb{P} -matrix for disjoint sets X, Y , and let A' be an $X' \times Y'$ \mathbb{P} -matrix for disjoint sets X', Y' , such that $X \cup Y = X' \cup Y'$. If A' is a minor of A , and A is a minor of A' , then we say that A and A' are *strongly equivalent*, which we denote by $A' \approx A$. \diamond

2.3.27 DEFINITION. If $\varphi(A') \approx A$ for some partial-field automorphism φ , then we say A' and A are *equivalent*. \diamond

The order in which scalings and pivot operations are carried out does not matter:

2.3.28 PROPOSITION. Let A, A' be $X \times Y$ \mathbb{P} -matrices for disjoint sets X, Y , such that $A \approx A'$. Then $A \sim A'$.

Proof: Since $A \approx A'$, we have

$$[I_X A'] = F[I_X A]D \quad (2.3)$$

for an invertible matrix F and a diagonal $(X \cup Y) \times (X \cup Y)$ matrix D , by Lemma 2.3.15. From (2.3) we conclude that

$$I_X = FI_X D[X, X].$$

This is impossible unless F is a diagonal matrix. But then $A \sim A'$, as desired. \blacksquare

We remark here that Proposition 2.3.28 generalizes Theorem 1.1.8 from the introduction. To see this we need to find the cross ratios involved. This is the topic of the next section.

2.3.4 Cross ratios and signatures

In the introduction we defined the cross ratio of four ordered collinear points. Cross ratios will crop up several times in this thesis. Usually we study the set of cross ratios of four-point lines that can be obtained as minors of $[I A]$ for some \mathbb{P} -matrix A . This is formalized in the following definition.

2.3.29 DEFINITION. Let A be a \mathbb{P} -matrix. We define the *cross ratios* of A as the set

$$\text{Cr}(A) := \left\{ p \mid \begin{bmatrix} 1 & 1 \\ p & 1 \end{bmatrix} \preceq A \right\}. \quad \diamond$$

2.3.30 LEMMA. If $A' \preceq A$ then $\text{Cr}(A') \subseteq \text{Cr}(A)$.

Proof: If $\begin{bmatrix} 1 & 1 \\ p & 1 \end{bmatrix} \preceq A'$ and $A' \preceq A$, then $\begin{bmatrix} 1 & 1 \\ p & 1 \end{bmatrix} \preceq A$. ■

There is a strong relation between cross ratios and fundamental elements.

2.3.31 LEMMA. Let A be a \mathbb{P} -matrix. Then $\text{Cr}(A) \subseteq \mathcal{F}(\mathbb{P})$.

Proof: Since $\det\left(\begin{bmatrix} 1 & 1 \\ p & 1 \end{bmatrix}\right) = 1 - p \in \mathbb{P}$, $p \in \mathcal{F}(\mathbb{P})$. ■

2.3.32 PROPOSITION. Let $p \in \mathcal{F}(\mathbb{P})$. Then $\text{Cr}\left(\begin{bmatrix} 1 & 1 \\ p & 1 \end{bmatrix}\right) = \text{Asc}(p)$.

Proof: If $A' = \begin{bmatrix} 1 & 1 \\ p' & 1 \end{bmatrix} \preceq \begin{bmatrix} 1 & 1 \\ p & 1 \end{bmatrix} = A$ then A was obtained from A' by exchanging rows, exchanging columns, pivoting, and scaling. This gives 24 potential values for p' (if $p \notin \{0, 1\}$), and the result follows after a straightforward check. ■

Sometimes we wish to restrict our attention to a sub-partial field of \mathbb{P} . Cross ratios show to what extent this is possible.

2.3.33 DEFINITION. Let \mathbb{P}, \mathbb{P}' be partial fields with $\mathbb{P}' \subseteq \mathbb{P}$, and let A be a \mathbb{P} -matrix. We say that A is a *scaled \mathbb{P}' -matrix* if $A \sim A'$ for some \mathbb{P}' -matrix A' . ◇

The main result from this section is the following:

2.3.34 THEOREM. Let A be a \mathbb{P} -matrix. Then A is a scaled $\mathbb{P}[\text{Cr}(A)]$ -matrix.

For the proof we need a *signature function*, which we introduce below. First we make a few further remarks. Normalization plays an important role:

2.3.35 LEMMA. If A is a scaled \mathbb{P}' -matrix and A is normalized, then A is a \mathbb{P}' -matrix.

Proof: Let T be a normalizing spanning forest for A , and let $A' \sim A$ be a \mathbb{P}' -matrix. By Lemma 2.3.11 there exists a T -normalized \mathbb{P}' -matrix $A'' \sim A'$. But by Lemma 2.3.12, $A'' = A$. ■

Still, it may not be easy to test if a \mathbb{P} -matrix with entries in \mathbb{P}' is actually a \mathbb{P}' -matrix (see the discussion at the end of Section 2.2.3). However, if the sub-partial field is induced then this is straightforward:

2.3.36 LEMMA. Let \mathbb{P}, \mathbb{P}' be partial fields such that \mathbb{P}' is an induced sub-partial field of \mathbb{P} . Let A be a \mathbb{P} -matrix such that all entries of A are in \mathbb{P}' . Then A is a \mathbb{P}' -matrix.

Proof: Suppose $p, q \in \mathbb{P}'$, and $p + q \in \mathbb{P}$. It follows from Definition 2.2.15 that then $p + q \in \mathbb{P}'$. This fact, together with Lemma 2.3.18, implies the result. ■

Now we will introduce the signature function of a matrix.

2.3.37 DEFINITION. Let A be an $X \times Y$ matrix with entries in a partial field \mathbb{P} . The *signature* of A is the function $\sigma_A : (X \times Y) \cup (Y \times X) \rightarrow \mathbb{P}$ defined by

$$\sigma_A(vw) := \begin{cases} A_{vw} & \text{if } v \in X, w \in Y \\ 1/A_{vw} & \text{if } v \in Y, w \in X. \end{cases}$$

If $C = (v_0, v_1, \dots, v_{2n-1}, v_{2n})$ is a cycle of $G(A)$ then we define

$$\sigma_A(C) := (-1)^{|V(C)|/2} \prod_{i=0}^{2n-1} \sigma_A(v_i v_{i+1}). \quad \diamond$$

Observe that the signature of a cycle does not depend on the choice of the start vertex v_0 . If C' is the cycle $(v_{2n}, v_{2n-1}, \dots, v_1, v_0)$ then $\sigma_A(C') = 1/\sigma_A(C)$. The following lemma describes the effect of pivoting and scaling on the signature. The last property exhibits a close connection between the signature and cross ratios.

2.3.38 LEMMA. Let A be an $X \times Y$ matrix with entries in a partial field \mathbb{P} .

- (i) If $A' \sim A$ then $\sigma_{A'}(C) = \sigma_A(C)$ for all cycles C in $G(A)$.
- (ii) Let $C = (v_0, \dots, v_{2n})$, $v_{2n} = v_0$, be an induced cycle of $G(A)$ with $v_0 \in X$ and $n \geq 3$. Suppose $A' := A^{v_0 v_1}$ is such that all entries are in \mathbb{P} . Then $C' = (v_2, v_3, \dots, v_{2n-1}, v_2)$ is an induced cycle of $G(A')$ and $\sigma_{A'}(C') = \sigma_A(C)$.
- (iii) Let $C = (v_0, \dots, v_4)$, $v_4 = v_0$, be a cycle of $G(A)$ with $v_0 \in X$. Suppose $A' := A^{v_0 v_1}$ is such that all entries are in \mathbb{P} . Then $C' = (v_1, v_0, v_2, v_3, v_1)$ is an induced cycle of $G(A')$ and $\sigma_{A'}(C') = 1 - \sigma_A(C)$.
- (iv) Let $C = (v_0, \dots, v_{2n})$, $v_{2n} = v_0$, be an induced cycle of $G(A)$. If A' is obtained from A by scaling rows and columns so that $A'_{v_i v_{i+1}} = 1$ for all $i > 0$, then $A'_{v_0 v_1} = (-1)^{|V(C)|/2} \sigma_A(C)$, and $\det(A[V(C)]) = 1 - \sigma_A(C)$.

Proof: Let C be a cycle of $G(A)$, and suppose A' was obtained from A by multiplying all entries in row v by $p \in \mathbb{P}^*$. If $v \notin C$ then $A'[C] = A[C]$, so clearly $\sigma_{A'}(C) = \sigma(C)$. If $v \in C$ then v meets two consecutive edges of C , say $uv, vw \in E(C)$. Now $\sigma_{A'}(uv) = 1/(pA_{vu}) = \sigma_A(uv)/p$, and likewise $\sigma_{A'}(vw) = p\sigma_A(vw)$. Since all other entries indexed by edges of C remain unaltered, we have $\sigma_{A'}(C) = \sigma_A(C)$, and (i) follows.

Let $C = (v_0, \dots, v_{2n})$ be an induced cycle of $G(A)$ with $n \geq 3$, and let $C' = (v_2, \dots, v_{2n-1}, v_2)$. By Proposition 2.3.28 we may assume $A_{v_0 v_1} = A_{v_2 v_1} = A_{v_0 v_{2n-1}} = 1$. In $A^{v_0 v_1}$, then, we have $(A^{v_0 v_1})_{v_2 v_{2n-1}} = -1$; all other entries of $A^{v_0 v_1}[C']$ are identical to the corresponding entry of $A[C']$. From this (ii) follows easily.

We omit the straightforward proof of (iii). Finally, (iv) follows from (ii) and (iii). ■

A direct consequence of Lemma 2.3.38(iv) is the following:

2.3.39 COROLLARY. Let A be a \mathbb{P} -matrix. If C is an induced cycle of $G(A)$ then $\sigma_A(C) \in \text{Cr}(A) \subseteq \mathcal{F}(\mathbb{P})$.

Roughly speaking, the induced cycles of $G(A)$ display some of the cross ratios of A .

Proof of Theorem 2.3.34: Let A be a counterexample with $|X| + |Y|$ minimal, and define $\mathbb{P}' := \mathbb{P}[\text{Cr}(A)]$. Without loss of generality we assume that A is normalized with normalizing spanning forest T .

2.3.39.I CLAIM. *If every entry of A is in \mathbb{P}' and $A' \sim A$ is T' -normalized for some spanning forest T' then every entry of A' is in \mathbb{P}' .*

Proof: We prove this for the case $T' = (T - xy) \cup x'y'$ for edges $xy, x'y'$ with $x, x' \in X$ and $y, y' \in Y$. The claim then follows by induction. Without loss of generality assume T, T' are trees. Let $X_1 \cup Y_1, X_2 \cup Y_2$ be the components of $T - e$ such that $x \in X_1, y \in Y_2$. Let $p := A_{x'y'}$. Then A' is the matrix obtained from A by multiplying all entries in $A[X, Y_2]$ by p^{-1} and all entries in $A[X_2, Y]$ by p . Since $p \in \mathbb{P}'$ the claim follows. \square

2.3.39.2 CLAIM. *Every entry of A is in \mathbb{P}' .*

Proof: Suppose this is not the case. Let T be a normalizing spanning forest for A , and let H be the subgraph of $G(A)$ consisting of all edges $x'y'$ such that $A_{x'y'} \in \mathbb{P}'$. Let xy be an edge of $G(A) - H$, i.e. $p := A_{xy} \in \mathbb{P} - \mathbb{P}'$. Clearly $1 \in \mathbb{P}'$, so $T \subseteq H$. Therefore H contains an $x - y$ path P . Choose xy and P such that P has minimum length. Then $C := P \cup xy$ is an induced cycle of $G(A)$. By changing the spanning forest stepwise, as in the previous claim, we may assume $P \subseteq T$. But then Corollary 2.3.39 implies that one of p and $-p$ is in $\text{Cr}(A)$, a contradiction. \square

Suppose A has a square submatrix A' such that $\det(A') \notin \mathbb{P}'$. Since $|X| + |Y|$ is minimal and we can extend a spanning forest of A' to a spanning forest of A , we have that $A = A'$. A can not be a 2×2 matrix, since all possible determinants of such matrices are in \mathbb{P}' by definition. Pick an edge xy such that $A_{xy} \neq 0$. Assume that A is normalized with a normalizing spanning forest T containing all edges $x'y'$ such that $A_{x'y'} \neq 0$ and $x'y$ such that $A_{x'y} \neq 0$. Consider A^{xy} . All entries of this matrix are in \mathbb{P}' . By Lemma 2.3.18 we have $\det(A) = \det(A^{xy} - \{x, y\})$. The latter is the determinant of a strictly smaller matrix which is, by induction, a \mathbb{P}' -matrix, a contradiction. \blacksquare

2.3.40 COROLLARY. *A is a scaled \mathbb{P}' -matrix if and only if $\text{Cr}(A) \subseteq \mathbb{P}'$.*

Clearly $\mathbb{P}[\text{Cr}(A)]$ is the smallest partial field $\mathbb{P}' \subseteq \mathbb{P}$ such that A is a scaled \mathbb{P}' -matrix.

2.4 \mathbb{P} -matroids

In Section 1.4 we already defined $\mathcal{M}(\mathbb{P})$ as the set of matroids representable over a partial field \mathbb{P} . Using Proposition 2.3.4 we can prove the following:

2.4.I PROPOSITION. *If $M \in \mathcal{M}(\mathbb{P})$ then $M^* \in \mathcal{M}(\mathbb{P})$.*

Proof: By Proposition 2.3.3, $M = M[I A]$ for some \mathbb{P} -matrix A . By Proposition 2.3.4, $[-A^T I]$ is also a \mathbb{P} -matrix. The result now follows from Proposition 1.2.14, using the same ring homomorphism as in the proof of Proposition 2.1.4. ■

The name “minor” in Definition 2.3.21 was not chosen by accident:

2.4.2 **LEMMA.** *Suppose $M = M[I A]$ for some $X \times Y$ \mathbb{P} -matrix A , and let $x \in X$ and $y \in Y$. Then*

- (i) $M \setminus y = M[I (A - y)]$;
- (ii) $M/x = M[I (A - x)]$;
- (iii) *If $A' \sim A$ then $M[I A'] = M[I A]$;*
- (iv) *If $A_{xy} \neq 0$ then $M = M[I A^{xy}]$.*

Proof: Statement (i) follows easily from Definition 1.2.19 and Proposition 2.1.4. Statement (ii) follows from (i) and Proposition 2.4.1. Statement (iii) follows from elementary properties of determinants, with the additional remark that after multiplying row x of $[I A]$ by p , we have to multiply column x of $[I A]$ by p^{-1} to restore the identity matrix. Finally, statement (iv) follows from Lemma 2.3.19. ■

In particular, Lemma 2.4.2(iii) and (iv) imply that strongly equivalent matrices represent the same matroid:

2.4.3 **PROPOSITION.** *Let A, A' be \mathbb{P} -matrices such that $A \approx A'$. Then $M[I A] = M[I A']$.*

It follows immediately that $\mathcal{M}(\mathbb{P})$ is minor-closed:

2.4.4 **PROPOSITION.** *If A, A' are \mathbb{P} -matrices such that $A' \preceq A$, then $M[I A'] \preceq M[I A]$. Conversely, if $N \preceq M[I A]$, then there is a \mathbb{P} -matrix $A' \preceq A$ such that $N = M[I A']$.*

Partial-field homomorphisms preserve the matroid:

2.4.5 **PROPOSITION.** *Let \mathbb{P}, \mathbb{P}' be partial fields, A a \mathbb{P} -matrix, and $\varphi : \mathbb{P} \rightarrow \mathbb{P}'$ a partial-field homomorphism. Then $M[A] = M[\varphi(A)]$.*

Proof: This follows directly from Proposition 2.3.20. ■

We note a corollary of Theorem 2.3.34:

2.4.6 **PROPOSITION.** *If a matroid M is representable over a partial field \mathbb{P} , then M is representable over $\mathbb{P}[\mathcal{F}(\mathbb{P})]$.*

Inequivalent representations form an important complication that arises in the study of partial fields with more than one cross ratio.

2.4.7 **DEFINITION.** A matroid M has k inequivalent representations over \mathbb{P} if there exist \mathbb{P} -matrices A_1, \dots, A_k such that the A_i are pairwise inequivalent. ◇

When restricted to fields, our definition of equivalence of matroid representations is weaker than the definition given by Oxley (1992, Section 6.3). However, for matroids that have rank at least 3 the notions coincide.

2.4.8 EXAMPLE. The matroid in Example 1.3.2 has exactly two inequivalent representations over $\text{GF}(4)$. \diamond

2.4.9 EXAMPLE. The matroid $U_{2,5}$ can be defined as $U_{2,5} = M[IA]$ for the \mathbb{P} -matrix

$$A = \begin{bmatrix} 1 & 1 & 1 \\ 1 & p & q \end{bmatrix},$$

with $p, q \notin \{0, 1\}$, $p \neq q$. Over $\text{GF}(5)$ this matroid has six inequivalent representations. \diamond

2.4.1 Connectivity in matroids and matrices

We start with the usual notion of connectivity in a matroid.

2.4.10 DEFINITION. Let M be a matroid with ground set E . The connectivity function of M , $\lambda_M : 2^E \rightarrow \mathbb{N}$ is defined by

$$\lambda_M(Z) := \text{rk}_M(Z) + \text{rk}_M(E - Z) - \text{rk}(M). \quad \diamond$$

2.4.11 DEFINITION. A partition of the ground set (Z_1, Z_2) is a k -separation if $|Z_1|, |Z_2| \geq k$ and $\lambda_M(Z_1) < k$. A k -separation is *exact* if $\lambda_M(Z_1) = k - 1$. A matroid is k -connected if it has no k' -separation for any $k' < k$, and it is *connected* if it is 2-connected. \diamond

For representable matroids, the following lemma gives a characterization of the connectivity function in terms of the ranks of certain submatrices of A .

2.4.12 LEMMA (Truemper, 1985). Suppose A is an $(X_1 \cup X_2) \times (Y_1 \cup Y_2)$ \mathbb{P} -matrix (where X_1, X_2, Y_1, Y_2 are pairwise disjoint). Then

$$\lambda_{M[IA]}(X_1 \cup Y_1) = \text{rk}(A[X_1, Y_2]) + \text{rk}(A[X_2, Y_1]).$$

Proof: Let $M := M[IA]$.

$$\text{rk}_M(X_1 \cup Y_1) = \text{rk}([IA][X_1 \cup X_2, X_1 \cup Y_1]) = |X_1| + \text{rk}(A[X_2, Y_1]).$$

Likewise,

$$\text{rk}_M(X_2 \cup Y_2) = \text{rk}([IA][X_1 \cup X_2, X_2 \cup Y_2]) = |X_2| + \text{rk}(A[X_1, Y_2]).$$

Since $\text{rk}(M) = |X_1 \cup X_2| = |X_1| + |X_2|$, the result follows by substitution. \blacksquare

We will say that a matrix A is k -connected if $M[IA]$ is k -connected.

2.4.13 DEFINITION. A nonempty set $X \subseteq E(M)$ is a *separator* of M if $\lambda_M(X) = 0$. \diamond

2.4.14 DEFINITION. Let M_1, M_2 be matroids such that $E(M_1) \cap E(M_2) = \emptyset$. The *direct sum* of M_1 and M_2 , denoted $M_1 \oplus M_2$, is the matroid on $E(M_1) \cup E(M_2)$ with rank function

$$\text{rk}_{M_1 \oplus M_2}(X) := \text{rk}_{M_1}(X \cap E(M_1)) + \text{rk}_{M_2}(X \cap E(M_2)). \quad \diamond$$

The following is well-known and easy to see:

2.4.15 LEMMA. A matroid M has a separator if and only if $M = M_1 \oplus M_2$ for some proper minors M_1, M_2 of M .

Direct sums preserve representability:

2.4.16 LEMMA. If M_1 and M_2 are \mathbb{P} -representable, then $M_1 \oplus M_2$ is \mathbb{P} -representable.

Proof: Let A_1 be an $X_1 \times Y_1$ \mathbb{P} -matrix such that $M_1 = M[I A_1]$, and let A_2 be an $X_2 \times Y_2$ \mathbb{P} -matrix such that $M_2 = M[I A_2]$. We claim

$$M_1 \oplus M_2 = M[I A],$$

where

$$A = \begin{matrix} & \begin{matrix} Y_1 & Y_2 \end{matrix} \\ \begin{matrix} x_1 \\ x_2 \end{matrix} & \begin{bmatrix} A_1 & 0 \\ 0 & A_2 \end{bmatrix} \end{matrix}.$$

First of all, note that A is a \mathbb{P} -matrix, since for all $Z \subseteq E(M_1) \cup E(M_2)$ such that $A[Z]$ is square and has no all-zero rows or columns,

$$\det(A[Z]) = \det(A[Z \cap E(M_1)]) \det(A[Z \cap E(M_2)]).$$

Now, for any $Z \subseteq X_1 \cup Y_1 \cup X_2 \cup Y_2$ we have

$$\begin{aligned} \text{rk}_{M[I A]}(Z) &= |(X_1 \cup X_2) \cap Z| + \text{rk}(A[(X_1 \cup X_2) - Z, (Y_1 \cup Y_2) \cap Z]) \\ &= |X_1 \cap Z| + |X_2 \cap Z| + \text{rk}(A_1[X_1 - Z, Y_1 \cap Z]) + \text{rk}(A_2[X_2 - Z, Y_2 \cap Z]) \\ &= \text{rk}_{M_1}((X_1 \cup Y_1) \cap Z) + \text{rk}_{M_2}((X_2 \cup Y_2) \cap Z), \end{aligned}$$

and the result follows. ■

2.4.2 Bipartite graphs

Let M be a rank- r matroid with ground set E , and let B be a basis of M . Let $G(M, B)$ be the bipartite graph with vertices $V(G) = B \cup (E - B)$ and edges $E(G) = \{xy \in B \times (E - B) \mid (B \triangle \{x, y\}) \in \mathcal{B}\}$. For each $y \in E - B$ there is a unique matroid circuit $C_{B, y} \subseteq B \cup y$, the *B-fundamental circuit* of y .

2.4.17 LEMMA. Let M be a matroid, and B a basis of M .

- (i) $xy \in E(G)$ if and only if $x \in C_{B, y}$.
- (ii) M is connected if and only if $G(M, B)$ is connected.
- (iii) If M is 3-connected, then $G(M, B)$ is 2-connected.

Proof: This follows from consideration of the B -fundamental-circuit incidence matrix. See, for example, Oxley (1992, Section 6.4).

2.4.18 LEMMA. Let \mathbb{P} be a partial field. Suppose $M = M[IA]$ for an $X \times Y$ \mathbb{P} -matrix A for disjoint sets X, Y . Then $G(M, X) = G(A)$.

Proof: If $A_{xy} \neq 0$ then a pivot over xy is possible, and $X \Delta \{x, y\} \in \mathcal{B}$. Hence $E(G(A)) \subseteq E(G(M, X))$. Now let $x \in X, y \in Y$ be such that $X \Delta \{x, y\}$ is a basis. Let $A' := [IA][X, X \Delta \{x, y\}]$. By Proposition 2.1.4, $\det(A') \neq 0$. Since all entries of $A'[x, X - \{x, y\}]$ equal zero, $A'[x, y] = A_{xy} \neq 0$, so $E(G(M, X)) \subseteq E(G(A))$. ■

2.4.3 Generalized parallel connection

In this section we study ways to “glue together” two \mathbb{P} -representable matroids. The results generalize those of Brylawski (1975) to partial fields. This section was inspired by paper by Lee (1990), who generalized Brylawski’s results to a precursor of partial fields, namely matroids representable over a multiplicatively closed set in a field. The main result of this subsection, Theorem 2.4.26, appears in Mayhew et al. (2009). Apart from Corollary 2.4.31, the results of this section are not used elsewhere in this thesis. We start by defining a closure operator for a matroid (cf. Oxley, 1992, Section 1.4).

2.4.19 DEFINITION. Let $M = (E, \mathcal{J})$ be a matroid, and $X \subseteq E$. Then the *closure* of X in M is

$$\text{cl}_M(X) := \{e \in E \mid \text{rk}_M(X \cup e) = \text{rk}_M(X)\}. \quad \diamond$$

Trivially $X \subseteq \text{cl}(X)$, and it is not difficult to show that $\text{cl}(\text{cl}(X)) = \text{cl}(X)$. A *flat* is a closed set.

2.4.20 DEFINITION. A pair (X, Y) of flats of a matroid M is a *modular pair* if

$$\text{rk}_M(X) + \text{rk}_M(Y) = \text{rk}_M(X \cap Y) + \text{rk}_M(X \cup Y). \quad \diamond$$

2.4.21 DEFINITION. If Z is a flat of M such that (Z, Y) is a modular pair for all flats Y of M , then Z is a *modular flat*. ♦

The following lemma contains some obvious examples:

2.4.22 LEMMA (see Oxley, 1992, Section 6.9). Let M be a matroid. Then $E(M)$, $\text{cl}(\emptyset)$, all rank-1 flats, and all separators are modular flats.

The next result is known as the modular short-circuit axiom (Brylawski, 1975, Theorem 3.11). We use Oxley’s formulation (Oxley, 1992, Theorem 6.9.9), and refer to that book for a proof.

2.4.23 THEOREM. Let M be a matroid and $X \subseteq E$ nonempty. The following statements are equivalent:

- (i) X is a modular flat of M ;
- (ii) For every circuit C such that $C - X \neq \emptyset$, there is an element $x \in X$ such that $(C - X) \cup x$ is dependent.
- (iii) For every circuit C , and for every $e \in C - X$, there is an $f \in X$ and a circuit C' such that $e \in C'$ and $C' \subseteq (C - X) \cup f$.

Suppose \mathbb{P} is a partial field, A a \mathbb{P} -matrix, $M = M[I A]$, and B a basis of M . In the next lemma we use the notation A_B for a $B \times (E(M) - B)$ \mathbb{P} -matrix $A_B \approx A$. By Proposition 2.3.28, A_B is unique up to row and column scaling. The following is an extension of Proposition 4.1.2 in Brylawski (1975) to partial fields. Note that Brylawski proves an “if and only if” statement, whereas we only state the “only if” direction. In this section we use the notation $M|X := M \setminus (E(M) - X)$.

2.4.24 **LEMMA.** *Let $M = (E, \mathcal{J})$ be a matroid, and X a modular flat of M . Suppose B_X is a basis for $M|X$, and $B \supseteq B_X$ a basis of B . Suppose A is a $B \times (E - B)$ \mathbb{P} -matrix such that $M = M[I A]$. Then every column of $A[B_X, E - (B \cup X)]$ is a \mathbb{P} -multiple of a column of $[I A[B_X, X - B]]$.*

For the proof we need the following technical lemma:

2.4.25 **LEMMA.** *Let A be an $X \times Y$ \mathbb{P} -matrix. Then $\text{rk}(A) < |Y|$ if and only if there is a vector c with entries in \mathbb{P} such that c is not the all-zero vector and $Ac = 0$.*

Proof: Without loss of generality, assume A contains a $(|Y| - 1) \times (|Y| - 1)$ submatrix A' such that $\det(A') \neq 0$, so $\text{rk}(A) \geq |Y| - 1$. Observe that, if F is an invertible $X \times X$ matrix then $Ac = 0$ if and only if $(FA)c = 0$. Using matrices as in the proof of Lemma 2.3.19 we can transform A into a matrix of the form

$$\begin{bmatrix} I & d \\ 0 & d' \end{bmatrix},$$

where d, d' are column vectors of appropriate size. If d' contains a nonzero entry then Lemma 2.3.18 implies that A contains a $|Y| \times |Y|$ submatrix with nonzero determinant, contradicting our choice. Hence $d' = 0$, and the following vector satisfies the requirement of the lemma:

$$c := \begin{bmatrix} -d \\ 1 \end{bmatrix}.$$

For the converse, we may assume without loss of generality that A is a square matrix with $\det(A) \neq 0$ yet $Ac = 0$ for some nonzero vector c over \mathbb{P} . Suppose $c_i \neq 0$. Consider the matrix A' obtained from A by replacing column i by Ac . This matrix can be obtained from A by elementary column operations, so $\det(A') = c_i \det(A)$. However, A' contains an all-zero column, so $\det(A') = 0$, contradicting our choice of A . ■

Proof of Lemma 2.4.24: Let M, X, B_X, B, A be as in the lemma, so

$$A = \begin{matrix} & B_X & \\ B - B_X & \begin{bmatrix} X - B & E - (B \cup X) \\ A_1 & A_2 \\ 0 & A_3 \end{bmatrix} \end{matrix}.$$

Let $v \in E - (B \cup X)$, and let C be the B -fundamental circuit containing v . If $C \cap X = \emptyset$ then $A_2[B_X, v]$ is an all-zero vector and the result holds, so assume $B_X \cap C \neq \emptyset$. By Theorem 2.4.23(iii) there is an $x \in X$ and a circuit C' with $v \in C'$ and $C' \subseteq (C - X) \cup x$.

From Lemma 2.4.25 we conclude that there exists a vector $c \in \mathbb{P}^E$ such that $c_i \neq 0$ if and only if $i \in C'$, and such that $[I A]c = 0$. But this is only possible if $c_x[I A[X]] [B_X, x] + c_v A[B_X, v] = 0$. Since $c_x, c_v \neq 0$, the result follows. ■

2.4.26 THEOREM. Suppose A_1, A_2 are \mathbb{P} -matrices with the following structure:

$$A_1 = \begin{matrix} & Y_1 & Y \\ X_1 & \begin{bmatrix} D'_1 & 0 \\ D_1 & D_X \end{bmatrix} \\ X & \end{matrix}, \quad A_2 = \begin{matrix} & Y & Y_2 \\ X & \begin{bmatrix} D_X & D_2 \\ 0 & D'_2 \end{bmatrix} \\ X_2 & \end{matrix},$$

where X, Y, X_1, Y_1, X_2, Y_2 are pairwise disjoint. If X is a modular flat of $M[I A_1]$, then

$$A := \begin{matrix} & Y_1 & Y & Y_2 \\ X_1 & \begin{bmatrix} D'_1 & 0 & 0 \\ D_1 & D_X & D_2 \\ 0 & 0 & D'_2 \end{bmatrix} \\ X & \\ X_2 & \end{matrix}$$

is a \mathbb{P} -matrix.

Proof: Let A_1, A_2, A be as in the theorem, and define $E := X_1 \cup X_2 \cup X \cup Y_1 \cup Y_2 \cup Y$. Suppose there exists a $Z \subseteq E$ such that $A[Z]$ is square, yet $\det(A[Z]) \notin \mathbb{P}$. Assume A_1, A_2, A, Z were chosen so that $|Z|$ is as small as possible.

If $Z \subseteq X_i \cup Y_i \cup X \cup Y$ for some $i \in \{1, 2\}$ then the result follows. Therefore we may assume that Z meets both $X_1 \cup Y_1$ and $X_2 \cup Y_2$. We may also assume that $A[Z]$ contains no row or column with only zero entries, so either there are $x \in X_1 \cap Z$, $y \in Y_1 \cap Z$ with $A_{xy} \neq 0$ or $x \in X \cap Z$, $y \in Y_1 \cap Z$ with $A_{xy} \neq 0$.

In the former case, pivoting over xy leaves D_X, D_2, D'_2 unchanged, yet by Lemma 2.3.18 $\det(A[Z]) \in \mathbb{P}$ if and only if $\det(A^{xy}[Z - \{x, y\}]) \in \mathbb{P}$. This contradicts minimality of $|Z|$. Therefore $Z \cap X_1 = \emptyset$.

Define $X' := Z \cap (X \cup X_2)$. Now pick some $y \in Y_1$. By Lemma 2.4.24 the column $A[X', y]$ is either a unit vector (i.e. a column of an identity matrix) or parallel to $A[X', y']$ for some $y' \in Y$. In the former case, Lemma 2.3.18 implies again that $\det(A[Z]) \in \mathbb{P}$ if and only if $\det(A[Z - \{x, y\}]) \in \mathbb{P}$, contradicting minimality of $|Z|$. In the latter case, if $y' \in Z$ then $\det(A[Z]) = 0$. Otherwise we can replace y by y' without changing $\det(A[Z])$ (up to possible multiplication with -1). It follows that $\det(A[Z]) = (-1)^s \det(A[Z'])$, where $Z' \subseteq X \cup X_2 \cup Y \cup Y_2$. But $\det(A[Z']) \in \mathbb{P}$, so also $\det(A[Z]) \in \mathbb{P}$, a contradiction. ■

2.4.27 DEFINITION. If A_1, A_2, A are as in Theorem 2.4.26 and $M_1 = M[I A_1]$, $M_2 = M[I A_2]$, $N = M_1|(X \cup Y)$, then we call the matroid $M[I A]$ the *generalized parallel connection* of M_1 and M_2 , denoted by $P_N(M_1, M_2)$. ◇

Note that Brylawski defined generalized parallel connection for general matroids, the only condition being that the intersection of the ground sets is a modular flat in one of the two constituents. An important condition in Theorem 2.4.26

is that the representations of $M_1|(X \cup Y)$ and $M_2|(X \cup Y)$ are identical. An example in Oxley (1992, Example 12.4.18) shows that, while M_1, M_2 may be representable over a field \mathbb{F} , $P_N(M_1, M_2)$ (in Brylawski's sense) need not be \mathbb{F} -representable.

We end this section with a special case.

- 2.4.28 DEFINITION. Let M, N be matroids such that $E(M) \cap E(N) = \{p\}$, and suppose $\{p\}$ is not a separator in M and N , and $\text{cl}_M(p) = \{p\}$. Then the 2-sum of M and N is

$$M \oplus_2 N := P_{M|p}(M, N) \setminus p. \quad \diamond$$

Note that, if $\text{cl}_M(p) \supset \{p\}$, then we can form a matroid by constructing $M' := P_{M|p}(M \setminus (\text{cl}_M(p) - p), N)$, adding to M' an element e parallel to p for each $e \in \text{cl}_M(p) - p$, and finally deleting p . We will denote this matroid by $M \oplus_2 N$ as well.

A direct consequence of Theorem 2.4.26 and Lemma 2.4.22 is the following.

- 2.4.29 COROLLARY. Let A_1, A_2 be \mathbb{P} -matrices, and $M_1 := M[I A_1]$, $M_2 := M[I A_2]$ be such that $E(M_1) \cap E(M_2) = \{p\}$. Then $M_1 \oplus_2 M_2$ is \mathbb{P} -representable.

The proof of the following well-known theorem can be found in Oxley (1992, Proposition 7.1.19, Theorem 8.3.1).

- 2.4.30 THEOREM. (i) M_1 and M_2 are isomorphic to proper minors of $M_1 \oplus_2 M_2$;
(ii) A matroid M is not connected if and only if $M = M_1 \oplus_2 M_2$ for some proper minors M_1, M_2 of M ;
(iii) A 2-connected matroid M is not 3-connected if and only if $M = M_1 \oplus_2 M_2$, for some M_1, M_2 that are isomorphic to proper minors of M .

Note that Theorem 2.4.30 does not generalize to higher connectivity. In this thesis we will often prove that a certain minor-closed class of matroids is representable over a partial field. It follows from Lemma 2.4.16, Corollary 2.4.29, and Theorem 2.4.30 that we only need to prove this for the 3-connected members of the class.

- 2.4.31 COROLLARY. The class $\mathcal{M}(\mathbb{P})$ is closed under direct sums and 2-sums.

A second special case is the *segment-cosegment exchange* studied by Oxley, Semple, and Vertigan (2000), which generalizes the *Delta-Y exchange* studied by Akkari and Oxley (1993). We refer to Oxley et al. (2000) for details.

2.5 Examples

In this section we define the partial fields that will be encountered in this thesis, determine their fundamental elements, and study their homomorphisms. Figure 2.1 shows the relations between these partial fields. All properties of the partial fields studied in this thesis are also collected in Appendix B.

- 2.5.1 DEFINITION. The *regular partial field* is

$$\mathbb{U}_0 := (\mathbb{Z}, \{-1, 0, 1\}). \quad \diamond$$

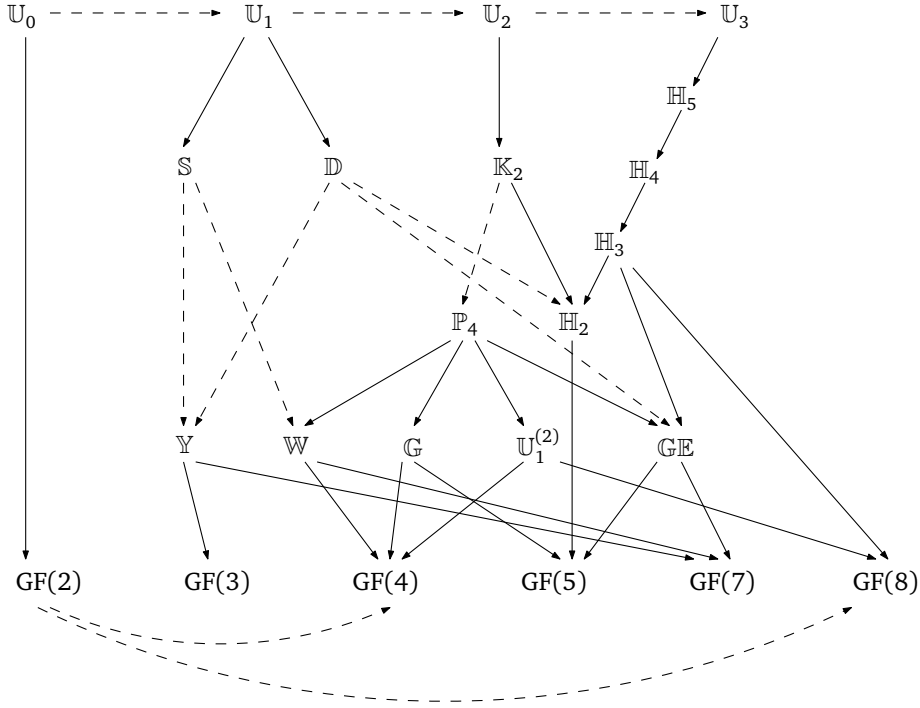


FIGURE 2.1

Some partial fields and their homomorphisms. A (dashed) arrow from \mathbb{P}' to \mathbb{P} indicates that there is an (injective) homomorphism $\mathbb{P}' \rightarrow \mathbb{P}$.

It is straightforward to characterize the possible homomorphisms:

2.5.2 LEMMA. *Let \mathbb{P} be a partial field. There is a unique partial-field homomorphism $\mathbb{U}_0 \rightarrow \mathbb{P}$.*

Proof: Let \mathbb{P} be a partial field, and let $\varphi : \mathbb{U}_0 \rightarrow \mathbb{P}$ be defined by $\varphi(0) = 0$, $\varphi(1) = 1$, $\varphi(-1) = -1$. Then φ satisfies all conditions of Definition 2.2.3, so φ is a partial-field homomorphism. Uniqueness follows immediately from Lemma 2.2.4. ■

Since this partial field has only 3 elements, the set of fundamental elements is easily found:

2.5.3 LEMMA.

$$\mathcal{F}(\mathbb{U}_0) = \{0, 1\}.$$

2.5.4 DEFINITION. The dyadic partial field is

$$\mathbb{D} := \left(\mathbb{Z}[\tfrac{1}{2}], \langle -1, 2 \rangle \right).$$

◇

2.5.5 LEMMA. *Let \mathbb{F} be a field of characteristic other than 2. There is a homomorphism $\mathbb{D} \rightarrow \mathbb{F}$.*

Proof: It suffices to show the result for $\mathbb{F} = \mathbb{Q}$ and $\mathbb{F} = \text{GF}(p)$ where p is a prime number other than 2. The first is obvious: the ring $\mathbb{Z}[\frac{1}{2}]$ is a subring of \mathbb{Q} . For the second, fix a prime $p \neq 2$. Let $\varphi : \mathbb{Z}[\frac{1}{2}] \rightarrow \text{GF}(p)$ be the ring homomorphism defined by $\varphi(x) = x + (p)$ for $x \in \mathbb{Z}$ and $\varphi(\frac{1}{2}) = 2^{p-2} + (p)$. Clearly $\varphi(\langle -1, 2 \rangle) \subseteq \text{GF}(p)^*$, so the restriction of φ to \mathbb{D} is indeed a partial-field homomorphism as desired. The result follows. ■

2.5.6 LEMMA.

$$\mathcal{F}(\mathbb{D}) = \left\{ 0, 1, -1, 2, \frac{1}{2} \right\}.$$

Proof: We find all solutions of

$$1 - p = q$$

where $p = (-1)^s 2^x$ and $q = (-1)^t 2^y$. If $x < 0$ then we divide both sides by p . Likewise if $y < 0$ then we divide both sides by q . We may multiply both sides with -1 . After rearranging and dividing out common factors we need to find all solutions of

$$2^{x'} + (-1)^{s'} 2^{y'} + (-1)^{t'} = 0$$

where $x', y' \geq 0$. This equation has solutions only if one of $2^{x'}, 2^{y'}$ is odd. This implies that we just need to find all solutions of

$$2^{x''} + (-1)^{s''} + (-1)^{t''} = 0.$$

Equality can hold only if $x'' = 1$, and then we should choose s'' and t'' odd, say $s'' = t'' = 1$. Now the result follows. ■

2.5.7 DEFINITION. The *near-regular partial field* is

$$\mathbb{U}_1 := \left(\mathbb{Z}[\alpha, \frac{1}{1-\alpha}, \frac{1}{\alpha}], \langle -1, \alpha, 1-\alpha \rangle \right),$$

where α is an indeterminate. ◇

2.5.8 LEMMA. *Let \mathbb{F} be a field other than $\text{GF}(2)$. There is a homomorphism $\mathbb{U}_1 \rightarrow \mathbb{F}$.*

Proof: Let \mathbb{F} be a field other than $\text{GF}(2)$. Then there exists an $x \in \mathbb{F} - \{0, 1\}$. Let $\varphi : \mathbb{Z}[\alpha, \frac{1}{1-\alpha}, \frac{1}{\alpha}] \rightarrow \mathbb{F}$ be defined by $\varphi(\alpha) = x$, and $\varphi(n) = n + (p)$ for $n \in \mathbb{Z}$, where p is the characteristic of \mathbb{F} . Then φ is a ring homomorphism[‡]. Since $\varphi(1-\alpha) \neq 0$, $\varphi(\langle -1, \alpha, 1-\alpha \rangle) \subseteq \mathbb{F}^*$, and therefore the restriction of φ to \mathbb{U}_1 is a partial-field homomorphism. ■

[‡]This will be the last time that we mention the effect of homomorphisms on the elements of the subring \mathbb{Z} .

2.5.9 LEMMA.

$$\mathcal{F}(\mathbb{U}_1) = \left\{ 0, 1, \alpha, 1 - \alpha, \frac{1}{1 - \alpha}, \frac{\alpha}{\alpha - 1}, \frac{\alpha - 1}{\alpha}, \frac{1}{\alpha} \right\}.$$

Proof: We find all $p = (-1)^s \alpha^x (1 - \alpha)^y$ such that $1 - p \in \mathbb{U}_1$. Consider the homomorphism $\varphi : \mathbb{U}_1 \rightarrow \mathbb{D}$ determined by $\varphi(\alpha) = 2$. Then

$$\varphi((-1)^s \alpha^x (1 - \alpha)^y) = (-1)^{s+y} 2^x.$$

Since fundamental elements must map to fundamental elements, it follows that $x \in \{-1, 0, 1\}$. Likewise, $\psi : \mathbb{U}_1 \rightarrow \mathbb{D}$, determined by $\psi(\alpha) = -1$, shows that $y \in \{-1, 0, 1\}$. Now a finite check remains. ■

Both the regular and near-regular partial fields are special cases of a family of partial fields:

2.5.10 DEFINITION. Let $\alpha_1, \dots, \alpha_k$ be indeterminates. Define the set

$$U_k := \{x - y \mid x, y \in \{0, 1, \alpha_1, \dots, \alpha_k\}, x \neq y\}.$$

The k -uniform partial field is

$$\mathbb{U}_k := (\mathbb{Q}(\alpha_1, \dots, \alpha_k), \langle U_k \rangle). \quad \diamond$$

The k -uniform partial fields were introduced by [Semple \(1997, 1998\)](#), who calls them *k-regular*. Among other things he determined the fundamental elements and automorphisms for these partial fields. Since we will not use these results, we refer the interested reader to [Semple \(1997\)](#) and to [Oxley et al. \(2000\)](#).

To find the homomorphisms in the next four examples we resort to algebraic number theory. The relevant results can be found in [Appendix A.2](#).

2.5.11 DEFINITION. The *sixth-roots-of-unity* ($\sqrt[6]{1}$) partial field is

$$\mathbb{S} := (\mathbb{Z}[\zeta], \langle \zeta \rangle),$$

where ζ is a root of $x^2 - x + 1 = 0$. ◇

We have $\zeta^3 = -1$, so this is indeed a partial field. Denote the other root of $x^2 - x + 1 = 0$ by $\bar{\zeta} := \zeta^5$. See also [Figure 2.2](#).

2.5.12 LEMMA. Let p be a prime. There is a homomorphism $\mathbb{S} \rightarrow \text{GF}(p^2)$. If $p = 3$ or $p \equiv 1 \pmod{3}$ then there is a homomorphism $\mathbb{S} \rightarrow \text{GF}(p)$.

Proof: $\mathbb{Z}[\zeta]$ is the ring of integers of the algebraic number field $\mathbb{Q}(\zeta) = \mathbb{Q}(\sqrt{-3})$. If I is a prime ideal of $\mathbb{Z}[\zeta]$, then $\mathbb{F} := \mathbb{Z}[\zeta]/I$ is a finite field. There is an obvious ring homomorphism $\varphi : \mathbb{Z}[\zeta] \rightarrow \mathbb{F}$. Since all elements of \mathbb{S} are units of $\mathbb{Z}[\zeta]$, $\varphi(\mathbb{S}^*) \subseteq \mathbb{F}^*$, so the restriction of φ to \mathbb{S} is a partial-field homomorphism.

The result now follows from [Theorem A.2.12](#) and the observation that, if there is a homomorphism $\mathbb{S} \rightarrow \text{GF}(p)$, then there is a homomorphism $\mathbb{S} \rightarrow \text{GF}(p^2)$ (because $\text{GF}(p)$ is a subfield of $\text{GF}(p^2)$). ■

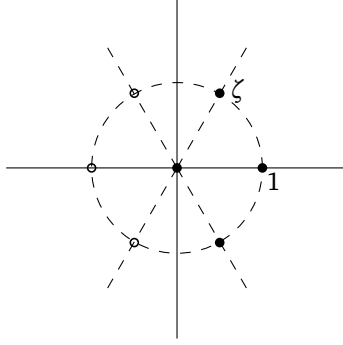


FIGURE 2.2

The elements of \mathbb{S} in the complex plane. Black dots are fundamental elements, outlined dots are other elements.

Like \mathbb{U}_0 , \mathbb{S} has finitely many elements. Hence the following is easily checked:

2.5.13 LEMMA.

$$\mathcal{F}(\mathbb{S}) = \{0, 1, \zeta, \bar{\zeta}\}.$$

The following partial field is the smallest that has both \mathbb{D} and \mathbb{S} as a sub-partial field:

2.5.14 DEFINITION. The partial field \mathbb{Y} is

$$\mathbb{Y} := (\mathbb{Z}[\zeta, \frac{1}{2}], \langle -1, 2, \zeta \rangle),$$

where ζ is a root of $x^2 - x + 1 = 0$. ◇

See also Figure 2.3.

2.5.15 LEMMA.

$$\mathcal{F}(\mathbb{Y}) = \left\{ 0, 1, \zeta, \bar{\zeta}, -1, 2, \frac{1}{2} \right\}.$$

Proof: Clearly all these elements are fundamental elements. The complex argument of every element of \mathbb{Y} is equal to a multiple of $\pi/3$, and the norm of each element is a power of 2. From this it follows easily that no other fundamental elements exist. ■

2.5.16 LEMMA. *Let $p > 2$ be a prime. There is a homomorphism $\mathbb{Y} \rightarrow \text{GF}(p^2)$. If $p \equiv 1 \pmod{3}$ then there is a homomorphism $\mathbb{Y} \rightarrow \text{GF}(p)$.*

Proof: As observed before, Theorem A.2.12 implies that there is a homomorphism $\mathbb{Z}[\zeta] \rightarrow \text{GF}(p)$ if $p \equiv 1 \pmod{3}$ or $p = 3$. But the ring we are interested in, $\mathbb{Z}[\zeta, \frac{1}{2}]$,

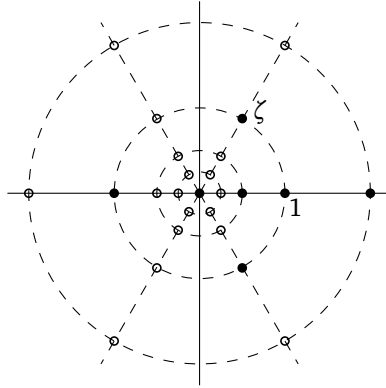


FIGURE 2.3

Some elements of \mathbb{Y} in the complex plane. Black dots are fundamental elements, outlined dots are other elements.

is not the ring of integers of a number field! Still, every element is of the form $2^k x$ for some $k \in \mathbb{Z}$, $x \in \mathbb{Z}[\zeta]$. Hence there are no homomorphisms to finite fields of characteristic 2, but every other ring homomorphism $\mathbb{Z}[\zeta] \rightarrow \text{GF}(q)$ can be extended to a ring homomorphism $\mathbb{Z}[\zeta, \frac{1}{2}] \rightarrow \text{GF}(q)$. The result follows. ■

2.5.17 DEFINITION. The golden ratio partial field is

$$\mathbb{G} := (\mathbb{Z}[\tau], \langle -1, \tau \rangle),$$

where τ is the golden ratio, i.e. the positive root of $x^2 - x - 1 = 0$. ◇

2.5.18 LEMMA. Let p be a prime. There is a homomorphism $\mathbb{G} \rightarrow \text{GF}(p^2)$. If $p = 5$ or $p \equiv \pm 1 \pmod{5}$ then there is a homomorphism $\mathbb{G} \rightarrow \text{GF}(p)$.

Proof: $\mathbb{Z}[\tau]$ is the ring of integers of $\mathbb{Q}(\sqrt{5})$. The result now follows from Theorem A.2.13. ■

2.5.19 LEMMA.

$$\mathcal{F}(\mathbb{G}) = \text{Asc}\{1, \tau\} = \{0, 1, \tau, -\tau, 1/\tau, -1/\tau, \tau^2, 1/\tau^2\}.$$

Proof: Remark that for all $k \in \mathbb{Z}$, $\tau^k = f_k + f_{k+1}\tau$, where $f_0 = 0, f_1 = 1$, and $f_{i+2} - f_{i+1} - f_i = 0$ for all $i \in \mathbb{Z}$, i.e. the Fibonacci sequence, extended to hold for negative k as well. If $p = (-1)^s(f_k + f_{k+1}\tau)$ is a fundamental element, then $\{ |(-1)^s f_k - 1|, |f_{k+1}| \}$ has to be a set of two consecutive Fibonacci numbers. This is true for finitely many values k , from which the result can be deduced. We leave out the remaining details. ■

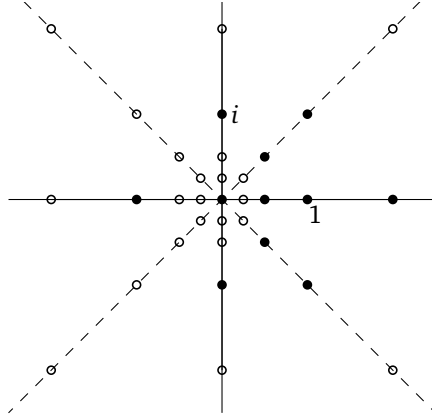


FIGURE 2.4

Some elements of \mathbb{H}_2 in the complex plane. Black dots are fundamental elements, outlined dots are other elements.

2.5.20 DEFINITION. The *Gaussian* partial field is

$$\mathbb{H}_2 := \left(\mathbb{Z}\left[i, \frac{1}{2}\right], \langle i, 1-i \rangle \right),$$

where i is a root of $x^2 + 1 = 0$. ◇

Note that $(1-i)^{-1} = \frac{1}{2}(1+i) \in \mathbb{Z}[i, \frac{1}{2}]$, and $i^2 = -1$, so this is indeed a partial field. See also Figure 2.4.

2.5.21 LEMMA. Let p be an odd prime. There is a homomorphism $\mathbb{H}_2 \rightarrow \text{GF}(p^2)$. If $p \equiv 1 \pmod{4}$ then there is a homomorphism $\mathbb{H}_2 \rightarrow \text{GF}(p)$.

Proof: $\mathbb{Z}[i]$ is the ring of integers of $\mathbb{Q}(i)$. Now Theorem A.2.14 implies that there is a homomorphism $\mathbb{Z}[i] \rightarrow \text{GF}(p)$ if $p \equiv 1 \pmod{4}$ or $p = 2$.

The ring we are interested in, $\mathbb{Z}[i, \frac{1}{2}]$, is not the ring of integers of a number field. However, every element is of the form $2^k x$ for some $k \in \mathbb{Z}$, $x \in \mathbb{Z}[i]$. Hence there are no homomorphisms to finite fields of characteristic 2, but every other homomorphism $\mathbb{Z}[i] \rightarrow \text{GF}(q)$ can be extended to a homomorphism $\mathbb{Z}[i, \frac{1}{2}] \rightarrow \text{GF}(q)$. The result follows. ■

2.5.22 LEMMA.

$$\mathcal{F}(\mathbb{H}_2) = \text{Asc}\{1, 2, i\} = \left\{ 0, 1, -1, 2, \frac{1}{2}, i, i+1, \frac{i+1}{2}, 1-i, \frac{1-i}{2}, -i \right\}.$$

Proof: The ring $\mathbb{Z}[i, \frac{1}{2}]$ embeds in a natural way in \mathbb{C} . Viewed in this way, the complex argument of every element of \mathbb{H}_2 is a multiple of $\pi/4$. It follows that if $p = i^x(1-i)^y$ is a fundamental element and $p \in \mathbb{C} - \mathbb{R}$, then $\frac{1}{\sqrt{2}} \leq |p| \leq \sqrt{2}$. Therefore there are finitely many fundamental elements in $\mathbb{C} - \mathbb{R}$. It is easily checked that all elements on the real line are powers of 2. The result follows. ■

As the notation suggests, \mathbb{H}_2 is a member of a family of partial fields, the *Hydra- k* partial fields[§]. There is one such partial field for $k = 1, \dots, 6$, with $\mathbb{H}_1 = \text{GF}(5)$ and \mathbb{H}_2 as above.

2.5.23 DEFINITION. The *Hydra-3 partial field* is

$$\mathbb{H}_3 := (\mathbb{Q}(\alpha), \langle -1, \alpha, 1 - \alpha, \alpha^2 - \alpha + 1 \rangle),$$

where α is an indeterminate. ◇

2.5.24 LEMMA. Let \mathbb{F} be a field with at least 5 elements. There is a homomorphism $\varphi : \mathbb{H}_3 \rightarrow \mathbb{F}$.

Proof: Suppose \mathbb{F} has at least 5 elements. Let $x \in \mathbb{F}$ be such that each of $x, 1 - x, x^2 - x + 1$ is nonzero. Since these polynomials block at most 4 elements of \mathbb{F} , x certainly exists. The map defined by $\varphi(\alpha) = x$ is easily seen to be a partial-field homomorphism, and the result follows. ■

2.5.25 LEMMA.

$$\mathcal{F}(\mathbb{H}_3) = \text{Asc} \left\{ 1, \alpha, \alpha^2 - \alpha + 1, \frac{\alpha^2}{\alpha - 1}, \frac{-\alpha}{(\alpha - 1)^2} \right\}.$$

Proof: We proceed along the lines of the proof of Lemma 2.5.9. All fundamental elements of \mathbb{H}_2 are of the form $(-1)^s \alpha^x (\alpha - 1)^y (\alpha^2 - \alpha + 1)^z$. The homomorphism $\varphi : \mathbb{H}_3 \rightarrow \mathbb{H}_2$ determined by $\varphi(\alpha) = i$ yields $-2 \leq y \leq 2$, since fundamental elements must map to fundamental elements. Similarly, $\psi : \mathbb{H}_3 \rightarrow \mathbb{H}_2$ determined by $\psi(\alpha) = 1 - i$ yields $-2 \leq x \leq 2$ and $\rho : \mathbb{H}_3 \rightarrow \mathbb{H}_2$ determined by $\rho(\alpha) = \frac{1-i}{2}$ yields, together with the preceding bounds, $-3 \leq z \leq 3$. This reduces the proof to a finite check, which we omit. ■

2.5.26 DEFINITION. The *hydra-4 partial field* is

$$\mathbb{H}_4 := (\mathbb{Q}(\alpha, \beta), \langle -1, \alpha, \beta, \alpha - 1, \beta - 1, \alpha\beta - 1, \alpha + \beta - 2\alpha\beta \rangle),$$

where α, β are indeterminates. ◇

The proof of the following lemma uses the same ideas as the proof of Lemma 2.5.25 and is therefore omitted.

2.5.27 LEMMA.

$$\mathcal{F}(\mathbb{H}_4) = \text{Asc} \left\{ 1, \alpha, \beta, \alpha\beta, \frac{\alpha-1}{\alpha\beta-1}, \frac{\beta-1}{\alpha\beta-1}, \frac{\alpha(\beta-1)}{\beta(\alpha-1)}, \frac{(\alpha-1)(\beta-1)}{1-\alpha\beta}, \frac{\alpha(\beta-1)^2}{\beta(\alpha\beta-1)}, \frac{\beta(\alpha-1)^2}{\alpha(\alpha\beta-1)} \right\}.$$

[§]The Hydra is a many-headed mythological monster that grows back two heads whenever you cut off one. The most famous is the Lernaean Hydra, which was killed by Herakles.

2.5.28 DEFINITION. The *hydra-5 partial field* is

$$\mathbb{H}_5 := (\mathbb{Q}(\alpha, \beta, \gamma), \langle -1, \alpha, \beta, \gamma, \alpha - 1, \beta - 1, \gamma - 1, \alpha - \gamma, \gamma - \alpha\beta, (1 - \gamma) - (1 - \alpha)\beta \rangle),$$

where α, β, γ are indeterminates. \diamond

Again we omit the proof of the following lemma.

2.5.29 LEMMA.

$$\mathcal{F}(\mathbb{H}_5) = \text{Asc} \left\{ 1, \alpha, \beta, \gamma, \frac{\alpha\beta}{\gamma}, \frac{\alpha}{\gamma}, \frac{(1-\alpha)\gamma}{\gamma-\alpha}, \frac{(\alpha-1)\beta}{\gamma-1}, \frac{\alpha-1}{\gamma-1}, \frac{\gamma-\alpha}{\gamma-\alpha\beta}, \frac{(\beta-1)(\gamma-1)}{\beta(\gamma-\alpha)}, \frac{\beta(\gamma-\alpha)}{\gamma-\alpha\beta}, \frac{(\alpha-1)(\beta-1)}{\gamma-\alpha}, \frac{\beta(\gamma-\alpha)}{(1-\gamma)(\gamma-\alpha\beta)}, \frac{(1-\alpha)(\gamma-\alpha\beta)}{\gamma-\alpha}, \frac{1-\beta}{\gamma-\alpha\beta} \right\}.$$

The final definition is easy:

2.5.30 DEFINITION. The *hydra-6 partial field* is

$$\mathbb{H}_6 := \mathbb{H}_5. \quad \diamond$$

At this point there is no obvious relation between the \mathbb{H}_k partial fields, except for the following property:

2.5.31 LEMMA. Let $k \in \{1, 2, 3, 4, 6\}$. There are exactly k homomorphisms $\mathbb{H}_k \rightarrow \text{GF}(5)$.

Proof: A homomorphism is uniquely determined by the images of α, β, γ . There are finitely many possibilities, and it is easily checked which of these keep all group members nonzero. ■

The following family of partial fields was suggested by Hendrik Lenstra.

2.5.32 DEFINITION. The *k-cyclotomic partial field* is

$$\mathbb{K}_k := (\mathbb{Q}(\alpha), \langle -1, \alpha, \alpha - 1, \alpha^2 - 1, \dots, \alpha^k - 1 \rangle),$$

where α is an indeterminate. \diamond

We omit the straightforward proof of the following lemma.

2.5.33 LEMMA. Let \mathbb{F} be a field with an element x whose multiplicative order is at least $k + 1$. Then there exists a homomorphism $\mathbb{K}_k \rightarrow \mathbb{F}$. In particular, there exists a homomorphism $\mathbb{K}_k \rightarrow \text{GF}(q)$ for $q \geq k + 2$.

Let $\Phi_0(\alpha) := \alpha$. For $j \in \mathbb{N}$, $j > 0$, let Φ_j be the j th cyclotomic polynomial, i.e. the polynomial whose roots are exactly the primitive j th roots of unity. A straightforward observation is the following:

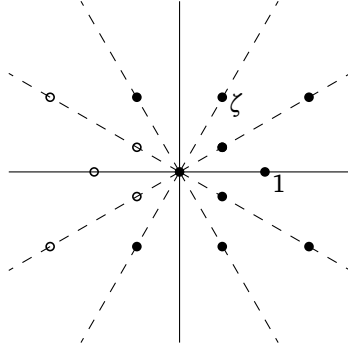


FIGURE 2.5

Some elements of \mathbb{W} in the complex plane. Black dots are fundamental elements, outlined dots are other elements.

2.5.34 LEMMA.

$$\mathbb{K}_k = \left(\mathbb{Q}(\alpha), \langle \{-1\} \cup \{\Phi_j(\alpha) \mid j = 0, \dots, k\} \rangle \right).$$

In particular $\mathbb{K}_2 = (\mathbb{Q}(\alpha), \langle -1, \alpha, \alpha - 1, \alpha + 1 \rangle)$.

2.5.35 LEMMA.

$$\mathcal{F}(\mathbb{K}_2) = \text{Asc}\{1, \alpha, -\alpha, \alpha^2\}.$$

Proof: Suppose $p := (-1)^s \alpha^x (\alpha - 1)^y (\alpha^2 - 1)^z$ is a fundamental element. Every homomorphism $\varphi : \mathbb{K}_2 \rightarrow \mathbb{G}$ and every homomorphism $\varphi : \mathbb{K}_2 \rightarrow \mathbb{H}_2$ gives bounds on x, y, z . After combining several of these bounds a finite number of possibilities remains. We leave out the details. ■

The role played in this thesis by the final four partial fields of this section is modest.

2.5.36 DEFINITION. The partial field \mathbb{W} is

$$\mathbb{W} := \left(\mathbb{Z}[\zeta, \frac{1}{1+\zeta}], \langle -1, \zeta, 1 + \zeta \rangle \right),$$

where ζ is a root of $x^2 - x + 1 = 0$. ◇

See also Figure 2.5. The proof of the following lemma is based on the same ideas as the proof of Lemma 2.5.22 and is omitted.

2.5.37 LEMMA.

$$\mathcal{F}(\mathbb{W}) = \text{Asc}\{1, \zeta, \zeta^2\} = \left\{ 0, 1, \zeta, \bar{\zeta}, \zeta^2, \bar{\zeta}^2, \zeta + 1, (\zeta + 1)^{-1}, (\bar{\zeta} + 1)^{-1}, \bar{\zeta} + 1 \right\}.$$

2.5.38 DEFINITION. The *Gersonides partial field* is

$$\mathbb{GE} := \left(\mathbb{Z}[\frac{1}{2}, \frac{1}{3}], \langle -1, 2, 3 \rangle \right). \quad \diamond$$

This partial field is similar to the dyadic partial field:

2.5.39 LEMMA. Let $p > 3$ be a prime. There is a partial-field homomorphism $\mathbb{GE} \rightarrow \text{GF}(p)$.

2.5.40 LEMMA.

$$\begin{aligned} \mathcal{F}(\mathbb{GE}) = \text{Asc}\{1, 2, 3, 4, 9\} = \left\{ 0, 1, 2, \frac{1}{2}, -1, 3, \frac{1}{3}, \frac{2}{3}, \frac{3}{2}, -\frac{1}{2}, -2, \right. \\ \left. 4, \frac{1}{4}, \frac{3}{4}, \frac{4}{3}, -\frac{1}{3}, -3, 9, \frac{1}{9}, \frac{8}{9}, \frac{9}{8}, -\frac{1}{8}, -8 \right\}. \end{aligned}$$

Proof: Elements of this partial field have the form

$$(-1)^s 2^a 3^b.$$

Finding all elements p of this form such that $1 - p$ is also of this form reduces, after multiplying to get rid of negative exponents, to finding all solutions to

$$2^x 3^z \pm 2^w 3^y = \pm 2^v 3^u.$$

We may divide out common factors. If a factor occurs in two terms, then it must occur in all three. Hence we only need to solve

$$2^x \pm 3^y = \pm 1$$

in nonnegative integers x, y . But the only solutions to this system are

$$\begin{aligned} 2^1 - 3^0 &= 1 \\ 2^1 - 3^1 &= -1 \\ 2^2 - 3^1 &= 1 \\ 2^3 - 3^2 &= -1, \end{aligned}$$

a theorem by Gersonides (see, for instance, [Peterson, January 25, 1999](#)). From this the result follows. ■

2.5.41 DEFINITION. The partial field \mathbb{P}_4 is

$$\mathbb{P}_4 := (\mathbb{Q}(\alpha), \langle -1, \alpha, \alpha - 1, \alpha + 1, \alpha - 2 \rangle),$$

where α is an indeterminate. ◇

2.5.42 LEMMA. Let $q \geq 4$ be a prime power. There is a homomorphism $\varphi : \mathbb{P}_4 \rightarrow \text{GF}(q)$.

2.5.43 LEMMA.

$$\mathcal{F}(\mathbb{P}_4) = \text{Asc}\{1, \alpha, -\alpha, \alpha^2, \alpha - 1, (\alpha - 1)^2\}.$$

Again the proof consists of finding homomorphisms to a partial field with known fundamental elements in order to bound the exponents. In this case \mathbb{GE} can be used. We leave out the details.

2.5.44 DEFINITION. The *near-regular partial field modulo two* is

$$\mathbb{U}_1^{(2)} = (\text{GF}(2)(\alpha), \langle \alpha, \alpha + 1 \rangle),$$

where α is an indeterminate. \diamond

2.5.45 LEMMA. Let $k \in \mathbb{N}$, $k \geq 2$. There is a homomorphism $\mathbb{U}_1^{(2)} \rightarrow \text{GF}(2^k)$.

Contrary to previous examples, this partial field has infinitely many fundamental elements!

2.5.46 LEMMA.

$$\mathcal{F}(\mathbb{U}_1^{(2)}) = \{0, 1\} \cup \text{Asc} \left\{ \alpha^{2^k} \mid k \in \mathbb{N} \right\}.$$

Proof: Elements of this partial field have the form

$$\alpha^a(\alpha + 1)^b.$$

Finding all p of this form such that $1 - p = 1 + p$ is also of this form reduces, after multiplying to get rid of negative exponents, to finding all solutions to

$$\alpha^x(\alpha + 1)^z + \alpha^w(\alpha + 1)^y = \alpha^v(\alpha + 1)^u.$$

We may divide out common factors. If a factor occurs in two terms, then it must occur in all three. Hence we only need to solve

$$\alpha^x + (\alpha + 1)^y = 1 \tag{2.4}$$

in nonnegative integers x, y . It follows immediately, by considering the degree of the polynomials, that $x = y$. Now, for $k < y$, the coefficient of α^k on the left-hand side is

$$\frac{y!}{k!(y-k)!} \pmod{2}.$$

For (2.4) to hold, we need that $\binom{y}{k}$ has a factor 2 for all $0 < k < y$. A theorem by [Fine \(1947\)](#) states that this holds if and only if $y = 2^t$ for some $t \in \mathbb{N}$. ■

2.6 Axiomatic partial fields

As mentioned before, [Semple and Whittle \(1996b\)](#) introduced partial fields axiomatically. We will now give their definition, and show that a partial field obtained in this way can be embedded in a ring. After this proof we will discuss the relative merits of the two definitions, and conclude the section with a closer look at the relation between partial-field homomorphisms and ring homomorphisms. The remainder of this thesis does not depend on the content of this section.

2.6.1 DEFINITION. Let P be a set with distinguished elements called 0, 1. Suppose \cdot is a binary operation and $+$ a partial binary operation on P . An *axiomatic partial field* is a 5-tuple

$$\mathbb{A} := (P, +, \cdot, 0, 1)$$

satisfying the following axioms:

- (P1) $(P - \{0\}, \cdot, 1)$ is an abelian group.
- (P2) For all $p \in P$, $p + 0 = p$.
- (P3) For all $p \in P$, there is a unique element $q \in P$ such that $p + q = 0$. We denote this element by $-p$.
- (P4) For all $p, q \in P$, if $p + q$ is defined, then $q + p$ is defined and $p + q = q + p$.
- (P5) For all $p, q, r \in P$, $p \cdot (q + r)$ is defined if and only if $p \cdot q + p \cdot r$ is defined. Then $p \cdot (q + r) = p \cdot q + p \cdot r$.
- (P6) The *associative law* holds for $+$. ◇

If $p, q \in P$ then we abbreviate $p \cdot q$ to pq . We write $p + q \doteq r$ for “ $p + q$ is defined and equal to r .” Before proceeding we need to define the associative law.

Given a multiset $S = \{p_1, \dots, p_n\}$ of elements of P , a *pre-association* is a vertex-labelled binary tree T with root r such that the leaves are labelled with the elements of S (and each element labels a unique leaf). Moreover, let v be a non-leaf node of $T - r$ with children labelled u, w . Then $u + w$ must be defined and v is labelled by $u + w$. Let T be a pre-association for S . If u, w are the labels of the children of r and $u + w$ is defined, then the labelled tree obtained from T by labeling r with $u + w$ is called an *association* of S .

Let T be an association for S with root node r , and let T' be a pre-association for the same set (but possibly with completely different tree and labeling). Let u', w' be the labels of the children of the root node of T' . Then T' is *compatible* with T if $u' + w' \doteq r$. The *associative law* is the following:

- (P6) For every multiset S of elements of P for which some association T exists, every pre-association of S is compatible with T .

Axiomatic partial fields generalize partial fields:

2.6.2 PROPOSITION. Let $\mathbb{P} = (R, G)$ be a partial field. Then $(G \cup \{0\}, +, \cdot, 0, 1)$ is an *axiomatic partial field*.

Proof: All axioms are equal to group or ring axioms, or can be derived from them easily. ■

Next we define a notion of isomorphism between axiomatic partial fields.

2.6.3 DEFINITION. Let $\mathbb{A}_1, \mathbb{A}_2$ be axiomatic partial fields. A function $\varphi : \mathbb{A}_1 \rightarrow \mathbb{A}_2$ is an *axiomatic-partial-field homomorphism* if

- (i) $\varphi(1) = 1$;
- (ii) For all $p, q \in \mathbb{P}_1$, $\varphi(pq) = \varphi(p)\varphi(q)$;
- (iii) For all $p, q, r \in \mathbb{P}_1$ such that $p + q \doteq r$, $\varphi(p) + \varphi(q) \doteq \varphi(r)$. ◇

2.6.4 DEFINITION. Let $\mathbb{A}_1, \mathbb{A}_2$ be axiomatic partial fields, and let $\varphi : \mathbb{A}_1 \rightarrow \mathbb{A}_2$ be a homomorphism. Then φ is an *isomorphism* if

- (i) φ is a bijection;
- (ii) $\varphi(p) + \varphi(q)$ is defined if and only if $p + q$ is defined. \diamond

If there exists an isomorphism $\varphi : \mathbb{A}_1 \rightarrow \mathbb{A}_2$ then we write $\mathbb{A}_1 \cong \mathbb{A}_2$.

2.6.5 DEFINITION. Let $\mathbb{P} = (R, G)$ be a partial field, and \mathbb{A} an axiomatic partial field. If

$$\mathbb{A} \cong (G \cup \{0\}, +, \cdot, 0, 1)$$

then we say that \mathbb{P} represents \mathbb{A} . \diamond

Partial-field isomorphism can be restated as follows:

2.6.6 LEMMA. Let $\mathbb{P}_1, \mathbb{P}_2$ be partial fields. Then $\mathbb{P}_1 \cong \mathbb{P}_2$ if and only if there is an axiomatic partial field \mathbb{A} such that both \mathbb{P}_1 and \mathbb{P}_2 represent \mathbb{A} .

Proof: If $\mathbb{P}_1 = (R_1, G_1)$, then $\mathbb{A} := (G \cup \{0\}, +, \cdot, 0, 1)$ is the obvious choice. The result follows by comparing Definitions 2.2.3, 2.2.7 with Definitions 2.6.3, 2.6.4. ■

Now we can state the converse of Proposition 2.6.2. Vertigan was the first to observe this, but he never published his result, and the proof below was found independently.

2.6.7 THEOREM. Let \mathbb{A} be an axiomatic partial field. Then there exist a ring R and a group $G \subseteq R^*$ such that $\mathbb{P} := (R, G)$ is a partial field, and \mathbb{P} represents \mathbb{A} .

Proof: Let $\mathbb{A} = (P, \oplus, \cdot, 0, 1_{\mathbb{A}})$, and define $G := (P - \{0\}, \cdot, 1_{\mathbb{A}})$. Consider the group ring

$$\mathbb{Z}[G] := \left\{ \sum_{p \in G} a_p \cdot p \mid a_p \in \mathbb{Z}, \text{ finitely many } a_p \text{ are nonzero} \right\},$$

where addition of two elements is componentwise and multiplication is defined by

$$\left(\sum_{p \in G} a_p \cdot p \right) \left(\sum_{p \in G} b_p \cdot p \right) = \sum_{p, q \in G} a_p b_q \cdot pq. \quad (2.5)$$

We identify $z \in \mathbb{Z}$ with $\sum_{i=1}^z 1_{\mathbb{A}}$. We drop the \cdot from the notation from now on. For clarity we write $p \oplus q$ if we mean addition in \mathbb{A} , and $p + q$ if we mean addition in $\mathbb{Z}[G]$. Consider the following subset of $\mathbb{Z}[G]$:

$$V_1 := \{p + q \mid p \oplus q \doteq 0\},$$

and define the ideal $I_1 := (V_1)$.

2.6.7.I CLAIM. If $x \in I_1$ then $x = \pm s_1 \pm \cdots \pm s_k$ for some $s_1, \dots, s_k \in V_1$.

Proof: By definition $x = r_1 s_1 + \cdots + r_k s_k$ for $r_1, \dots, r_k \in \mathbb{Z}[G]$ and $s_1, \dots, s_k \in V_1$. We consider one term.

$$r_i s_i = \left(\sum_{t \in G} a_t t \right) (p + q) = \sum_{t \in G} (a_t t (p + q)) = \sum_{t \in G} (a_t (tp + tq)),$$

where the last equality follows from (2.5). Since $p \oplus q \doteq 0$, also $tp \oplus tq \doteq 0$, by (P5). Hence $tp + tq \in V_1$. If $a_t > 0$ then

$$r_i s_i = \underbrace{(tp + tq) + \cdots + (tp + tq)}_{a_t \text{ terms}}.$$

If $a_t < 0$ then

$$r_i s_i = \underbrace{-(tp + tq) - \cdots - (tp + tq)}_{-a_t \text{ terms}}.$$

Summing over i now yields the claim. \square

2.6.7.2 CLAIM. $1_{\mathbb{A}} \notin I_1$.

Proof: Suppose $1 \in I_1$. By Claim 2.6.7.1, $1 = \pm s_1 \pm \cdots \pm s_k$ for some $s_1, \dots, s_k \in V_1$. We focus on the s_i in which the coefficient of $1_{\mathbb{A}}$ is not equal to 0. The only element of V_1 for which this holds is $1_{\mathbb{A}} + (-1_{\mathbb{A}})$. It follows that, in $\pm s_1 \pm \cdots \pm s_k$, the coefficient of $(-1_{\mathbb{A}})$ is equal to that of $1_{\mathbb{A}}$, which contradicts the assumption that $\pm s_1 \pm \cdots \pm s_k = 1$. \square

Now let $R_1 := \mathbb{Z}[G]/I_1$. Consider the following subset of R_1 :

$$V_2 := \{p + q + r + I_1 \mid (p \oplus q) \oplus r \doteq 0\},$$

and define the ideal $I_2 := (V_2)$.

2.6.7.3 CLAIM. If $x \in I_2$ then $x = s_1 + \cdots + s_k$ for some $s_1, \dots, s_k \in V_2$.

Proof: By definition $x = r_1 s_1 + \cdots + r_k s_k$ for $r_1, \dots, r_k \in R_1$ and $s_1, \dots, s_k \in V_2$. We consider one term.

$$\begin{aligned} r_i s_i &= \left(\sum_{t \in G} a_t t \right) (p + q + u) + I_1 = \sum_{t \in G} (a_t t (p + q + u)) + I_1 \\ &= \sum_{t \in G} (a_t (tp + tq + tu)) + I_1. \end{aligned}$$

Since $(p \oplus q) \oplus u \doteq 0$, also $(tp \oplus tq) \oplus tu \doteq 0$, by (P5). Hence $tp + tq + tu + I_1 \in V_2$. If $a_t > 0$ then

$$r_i s_i = \underbrace{(tp + tq + tu) + \cdots + (tp + tq + tu)}_{a_t \text{ terms}} + I_1.$$

If $a_t < 0$ then we observe that $-p + I_1 = (-p) + I_1$, and obtain

$$r_i s_i = \underbrace{((-tp) + (-tq) + (-tu)) + \cdots + ((-tp) + (-tq) + (-tu))}_{-a_t \text{ terms}} + I_1.$$

Summing over i now yields the claim. \square

Now let $R_2 := R_1/I_2$, $G_2 := \langle \{p + I_1 + I_2 \mid p \in G\} \rangle$, and define $\mathbb{P} := (R_2, G_2)$. Define the axiomatic partial field $\mathbb{A}' := (G_2 \cup \{0\}, +, \cdot, 0, 1_{\mathbb{A}} + I_1 + I_2)$. Our aim is to prove $\mathbb{A} \cong \mathbb{A}'$. Consider the function $\varphi : \mathbb{A} \rightarrow \mathbb{A}'$ defined by

$$\varphi(p) := p + I_1 + I_2.$$

2.6.7.4 CLAIM. φ is an axiomatic-partial-field homomorphism.

Proof: $\varphi(1_{\mathbb{A}}) = 1_{\mathbb{A}} + I_1 + I_2$. For $p, q \in P$, $\varphi(p)\varphi(q) = (p + I_1 + I_2)(q + I_1 + I_2) = pq + I_1 + I_2 = \varphi(pq)$. If $p, q, r \in P$ such that $p \oplus q \doteq r$ then $\varphi(p) + \varphi(q) = p + q + I_1 + I_2 = -(-r) + I_1 + I_2 = r + I_1 + I_2 = \varphi(p \oplus q)$, since $p + q + (-r) \in V_2$ and $r + (-r) \in V_1$. Clearly $r + I_1 + I_2 \in G_2 \cup \{0\}$, so $\varphi(p) + \varphi(q) \doteq \varphi(r)$. \square

2.6.7.5 CLAIM. φ is a bijection.

Proof: Obviously φ is surjective. Suppose $p, q \in P$ are such that $p \neq q$ yet $\varphi(p) = \varphi(q)$. Then $p - q + I_1 \in I_2$. By Claim 2.6.7.3, $p - q = s_1 + \dots + s_k$ for some $s_1, \dots, s_k \in V_2$. For each s_i , pick representatives $p_i, q_i, r_i \in P$ such that $s_i = p_i + q_i + r_i + I_1$ and $(p_i \oplus q_i) \oplus r_i \doteq 0$. Define the multiset

$$S := \bigcup_{i=1}^k \{p_i, q_i, r_i\}.$$

We build two associations for S . First, since $(p_i \oplus q_i) \oplus r_i \doteq 0$ and $0 \oplus 0 \doteq 0$, we can build an association whose root node is labelled by 0. Second, pick an $s \in S$. The only elements of S contributing to the coefficient of $s + I_1$ in $s_1 + \dots + s_k$ are s and $(-s)$. Hence, for each $s \in S - \{p, (-q)\}$, there is an element $(-s) \in S - \{p, q\}$. By repeatedly pairing these elements we can build a pre-association where the children of the root node are labelled p and $(-q)$. But the associative law then implies $p \oplus (-q) \doteq 0$, and hence $p = q$, contradicting our assumption. \square

In particular, Claim 2.6.7.5 implies that R_2 is nontrivial.

2.6.7.6 CLAIM. φ is an isomorphism.

Proof: Let $p, q, r \in P$ be such that $p + q + I_1 + I_2 = r + I_1 + I_2$. We have to show that $p \oplus q \doteq r$. Since $p + q + (-r) + I_1 \in I_2$, there are $s_1, \dots, s_n \in V_2$ such that $p + q + (-r) + I_1 = s_1 + \dots + s_n$. For each s_i , pick representatives $p_i, q_i, r_i \in P$ such that $s_i = p_i + q_i + r_i + I_1$ and $(p_i \oplus q_i) \oplus r_i \doteq 0$. Define the multiset

$$S := \{r\} \cup \bigcup_{i=1}^n \{p_i, q_i, r_i\}.$$

Using the same argument as in the previous claim we construct two pre-associations for S : one where the children of the root node are $r, 0$, and one where the children of the root node are p, q . Since $r \oplus 0 \doteq r$, the result follows from the associative law. \square

With this claim the proof is complete. ■

We have seen two ways to build a theory of partial fields: starting from a ring, as we did in Definition 2.1.1, and starting from a system of axioms, as we did in Definition 2.6.1. The axiomatic definition has certain advantages. For instance, the definition of axiomatic partial-field isomorphism is exactly what one expects: a bijection between the elements of the two structures. The definition of partial-field isomorphism, Definition 2.2.7, allows partial fields with wildly different underlying rings to be isomorphic.

However, the lack of reference to a ring also leads to additional technicalities when developing the theory. Matrix theory over axiomatic partial fields needs to be built from the ground up. For instance, it is not obvious what it means for a determinant (or, more generally, a sum having more than two terms) to be defined: the traditional definition of a determinant does not suggest an association for the terms. Semple and Whittle (1996b) attempted to give a definition, but their proof of the analogue of Proposition 2.3.22 was flawed under that definition. In Pendavingh and Van Zwam (2009a) a more suitable definition was proposed, under which Semple and Whittle's results could be recovered. We refer to that paper for more details.

Overall, the price we paid for not starting with the axiomatic definition appears modest. With the exception of the definition of a sub-partial field, none of our definitions depend on the ring underlying the partial field. The gain is considerable: the axiomatic equivalent of Section 2.1 would take much more effort.

For the remainder of this section we focus again on partial fields as in Definition 2.1.1. The partial field constructed in the proof of Theorem 2.6.7 can be seen as the *universal* representation of \mathbb{A} . We introduce some notation. In the next definition, addition in the partial field \mathbb{P} is denoted by \oplus .

2.6.8 DEFINITION. Let \mathbb{P} be a partial field. Let $I_{\mathbb{P}}$ be the ideal of $\mathbb{Z}[\mathbb{P}^*]$ generated by

$$\{p + q \mid p, q \in \mathbb{P}^*, p \oplus q = 0\} \cup \{p + q + r \mid p, q, r \in \mathbb{P}^*, p \oplus q \oplus r = 0\}.$$

Then $R_{\mathbb{P}} := \mathbb{Z}[\mathbb{P}^*]/I_{\mathbb{P}}$. ◇

It is straightforward to show that $R_{\mathbb{P}}$ is isomorphic to the ring R_2 for $(\mathbb{P}^* \cup \{0\}, +, \cdot, 0, 1)$, as constructed in the proof of Theorem 2.6.7.

2.6.9 DEFINITION. Let $\varphi_{\mathbb{P}} : \mathbb{P} \rightarrow (R_{\mathbb{P}}, \mathbb{P}^*)$ be defined by $\varphi(p) = p + I_{\mathbb{P}}$. ◇

By repeating the arguments in the proof of Theorem 2.6.7 we can show the following:

2.6.10 LEMMA. *The function $\varphi_{\mathbb{P}}$ is a partial-field isomorphism.*

Now we can obtain more information about the relation between partial-field homomorphisms and ring homomorphisms.

2.6.11 THEOREM. *Let $\mathbb{P} = (R, G)$, $\mathbb{P}' = (R', G')$ be partial fields, and $\varphi : \mathbb{P} \rightarrow \mathbb{P}'$ a partial-field homomorphism. There exists a ring homomorphism $\psi' : R_{\mathbb{P}} \rightarrow R'$ such that*

the restriction of ψ' to the partial field $(R_{\mathbb{P}}, \mathbb{P}^*)$, denoted $\psi : (R_{\mathbb{P}}, \mathbb{P}^*) \rightarrow \mathbb{P}'$, is a partial-field homomorphism for which the following diagram commutes:

$$\begin{array}{ccc}
 & (R_{\mathbb{P}}, \mathbb{P}^*) & \\
 \varphi_{\mathbb{P}} \uparrow & \searrow \psi & \\
 \mathbb{P} & \xrightarrow{\varphi} & \mathbb{P}'
 \end{array}$$

Proof: Let $\psi'' : \mathbb{Z}[\mathbb{P}^*] \rightarrow R'$ be the ring homomorphism defined by $\psi''(p) = \varphi(p)$ for all $p \in \mathbb{P}^*$. Since φ is a partial-field homomorphism, it follows that $I_{\mathbb{P}} \subseteq \ker(\psi'')$. Hence there is a well-defined ring homomorphism $\psi' : R_{\mathbb{P}} \rightarrow R'$ such that $\psi'(p + I_{\mathbb{P}}) = \varphi(p)$. Now the result follows. ■

2.7 Skew partial fields and chain groups

Until now we have assumed that the multiplicative group of a partial field is abelian. This restriction is not essential: matroids can also be represented over skew fields. In this section we will extend the definition of a \mathbb{P} -representable matroid to *skew partial fields*. As in the commutative case, we start with a definition. Note that in this section a ring R is not necessarily commutative. The remainder of this thesis does not depend on the content of this section.

2.7.1 DEFINITION. A *skew partial field* is a pair (R, G) , where R is a ring, and G is a subgroup of the group of units R^* of R , such that $-1 \in G$. ◇

While it is possible to define a notion of determinant over skew fields (such as the *Dieudonné determinant*, see [Hazewinkel, 1989](#), Page 67), we will not take that route. Instead, we will revisit the pioneering matroid representation work by [Tutte \(1965\)](#). He defines representations by means of a *chain group*. Unlike representations by (strong) \mathbb{P} -matrices, this is a basis-free definition of a representation. [Whitney \(1935\)](#) already mentioned chain groups in the appendix to the paper in which he introduced matroids, but Tutte (see, for instance, [Tutte, 1965](#)) was the first who studied their properties in great detail. The definitions below generalize Tutte's definitions from skew fields to skew partial fields.

2.7.2 DEFINITION. Let R be a ring, and E a finite set. An R -chain group on E is a subset $C \subseteq R^E$ such that

- (i) $f + g \in C$, and
- (ii) $rf \in C$,

for all $f, g \in C$ and $r \in R$. ◇

In this definition, addition and (left) multiplication with an element of R are defined componentwise. Using more modern terminology, a chain group is a submodule of a free left R -module. Chain groups generalize linear subspaces. The

elements of C are called *chains*. The *support* or *domain* of a chain $c \in C$ is

$$\|c\| := \{e \in E \mid c_e \neq 0\}.$$

We denote the chain whose support is the empty set by 0.

2.7.3 DEFINITION. A chain $c \in C$ is *elementary* if $c \neq 0$ and there is no $c' \in C - \{0\}$ with $\|c'\| \subsetneq \|c\|$. \diamond

2.7.4 DEFINITION. Let G be a subgroup of R^* . A chain $c \in C$ is *G-primitive* if $c \in (G \cup \{0\})^E$. \diamond

Now we are ready for our main definition.

2.7.5 DEFINITION. Let $\mathbb{P} = (R, G)$ be a skew partial field, and E a finite set. A \mathbb{P} -*chain group* on E is an R -chain group C on E such that every elementary chain $c \in C$ can be written as

$$c = rc'$$

for some primitive chain $c' \in C$ and $r \in R$. \diamond

Primitive elementary chains are unique up to scaling:

2.7.6 LEMMA. Suppose c, c' are primitive elementary chains such that $\|c\| = \|c'\|$. Then $c = gc'$ for some $g \in G$.

Proof: Pick $e \in \|c\|$, and define $c'' := c'_e c - c_e c'$. Then $\|c''\| \subsetneq \|c\|$. Since c is elementary, $c'' = 0$. Hence $c' = (c_e)^{-1} c'_e c$. \blacksquare

Chain groups can be used to represent matroids, as follows:

2.7.7 DEFINITION. The set of supports of elementary chains of C is

$$\mathcal{C}_C := \{\|c\| \mid c \in C, \text{ elementary}\}.$$

\diamond

2.7.8 THEOREM. Let $\mathbb{P} = (R, G)$ be a skew partial field, and let C be a \mathbb{P} -chain group on E . Then \mathcal{C}_C is the set of cocircuits of a matroid on E .

Proof: It is easy to see that \mathcal{C}_C satisfies (i) and (ii) of Theorem 1.2.4. Let $c, c' \in C$ be distinct G -primitive, elementary chains such that $e \in \|c\| \cap \|c'\|$. Define $d := c_e c' - c'_e c$. Since $c_e, c'_e \in G$, it follows that d is nonzero and $\|d\| \subseteq (\|c\| \cup \|c'\|) - e$. Let d' be an elementary chain of C with $\|d'\| \subseteq \|d\|$. Then $\|d'\| \in \mathcal{C}_C$, as desired. \blacksquare

We denote the matroid of Theorem 2.7.8 by $M(C)$.

2.7.9 DEFINITION. We say a matroid M is \mathbb{P} -*representable* if there exists a \mathbb{P} -chain group C such that $M = M(C)$. \diamond

Of course, we would like this notion to coincide with Definition 2.1.5 when \mathbb{P} is commutative. For that we introduce a generator matrix of C .

2.7.10 DEFINITION. Let A be a matrix with entries in a ring R . The row span of A is

$$\text{span}(A) := \{zA \mid z \in R^r\}. \quad \diamond$$

Clearly $\text{span}(A)$ is an R -chain group. Every \mathbb{P} -chain group has a generator matrix with $\text{rk}(M(C))$ rows:

2.7.11 LEMMA. If $\mathbb{P} = (R, G)$ is a skew partial field, and C is a \mathbb{P} -chain group on E , then there is a matrix A , with $\text{rk}(M(C))$ rows and entries in R , such that $C = \text{span}(A)$.

Proof: Pick a basis B of $M(C)$, and for each $e \in B$, pick a primitive chain a^e such that $\|a^e\| = C_{B,e}$, the B -fundamental cocircuit of e (cf. Section 2.4.2), and such that $(a^e)_e = 1$. Let A be the $B \times E$ matrix whose e th row is a^e .

2.7.11.1 CLAIM. $C = \text{span}(A)$.

Proof: Suppose this is false. Then there is a chain $c \in C - \text{span}(A)$. Choose such c with minimal support. If c is not elementary, then there is an elementary chain d whose support is contained in c . Suppose $e \in \|c\| \cap \|d\|$. Without loss of generality, we assume $d_e = 1$. Then $\|c - c_e d\| \subsetneq \|c\|$. Since $d \in \text{span}(A)$, $c - c_e d \notin \text{span}(A)$, a contradiction.

It follows that $c = rc'$ for a primitive chain c' , where $c' \notin \text{span}(A)$. Define

$$c'' := c' - \sum_{e \in B} c'_e a^e.$$

Then $c'' \neq 0$, so $\|c''\|$ contains a cocircuit. On the other hand, $\|c''\| \cap B = \emptyset$. This is a contradiction to Proposition 1.2.17, so the claim follows. \square

Since $A[B, B] = I_B$, the result follows. \blacksquare

A \mathbb{P} -matrix can be defined as follows:

2.7.12 DEFINITION. Let \mathbb{P} be a skew partial field. An $X \times E$ matrix A is a weak \mathbb{P} -matrix if $\text{span}(A)$ is a \mathbb{P} -chain group. We say that A is nondegenerate if $|X| = \text{rk}(\text{span}(A))$. We say that A is a strong \mathbb{P} -matrix if $[I \ A]$ is a weak \mathbb{P} -matrix. \diamond

We omit the straightforward proof of the following lemma, which allows some manipulation of weak \mathbb{P} -matrices.

2.7.13 LEMMA. Let $\mathbb{P} = (R, G)$ be a skew partial field, let A be an $X \times E$ weak \mathbb{P} -matrix, and let F be an invertible $X \times X$ matrix with entries in R . Then FA is a weak \mathbb{P} -matrix.

Again, nondegenerate weak \mathbb{P} -matrices can be converted to strong \mathbb{P} -matrices:

2.7.14 LEMMA. Let \mathbb{P} be a skew partial field, let A be an $X \times Y$ nondegenerate \mathbb{P} -matrix, and let B be a basis of $M(\text{span}(A))$. Then $A[X, B]$ is invertible.

$$x \left[\begin{array}{c|c} y & \\ \hline \alpha & c \\ b & D \end{array} \right] \rightarrow y \left[\begin{array}{c|c} x & \\ \hline \alpha^{-1} & \alpha^{-1}c \\ -b\alpha^{-1} & D - b\alpha^{-1}c \end{array} \right]$$

FIGURE 2.6
Pivoting over xy

Proof: For all $e \in B$, let a^e be a primitive chain such that $\|a^e\|$ is the B -fundamental cocircuit of e . Then $a^e = f^e A$ for some $f^e \in R^r$. Let F be the $B \times X$ matrix whose e th row is f^e . Then $(FA)[B, B] = I_B$, and the result follows. ■

We immediately have

2.7.15 COROLLARY. Let $\mathbb{P} = (R, G)$ be a skew partial field, and let A be an $X \times Y$ nondegenerate weak \mathbb{P} -matrix. Then there exists an invertible matrix D over R such that DA is a strong \mathbb{P} -matrix.

Again we can pivot in a strong \mathbb{P} -matrix. We need to distinguish carefully between left and right multiplication:

2.7.16 DEFINITION. Let A be an $X \times Y$ matrix over a ring R , and let $x \in X, y \in Y$ be such that $A_{xy} \in R^*$. Then we define A^{xy} to be the $(X - x) \cup y \times (Y - y) \cup x$ matrix with entries

$$(A^{xy})_{uv} = \begin{cases} (A_{xy})^{-1} & \text{if } uv = yx \\ (A_{xy})^{-1}A_{xv} & \text{if } u = y, v \neq x \\ -A_{uy}(A_{xy})^{-1} & \text{if } v = x, u \neq y \\ A_{uv} - A_{uy}(A_{xy})^{-1}A_{xv} & \text{otherwise.} \end{cases} \quad \diamond$$

We say that A^{xy} is obtained from A by *pivoting over xy* . See also Figure 2.6.

2.7.17 LEMMA. Let \mathbb{P} be a skew partial field, let A be an $X \times Y$ strong \mathbb{P} -matrix, and let $x \in X, y \in Y$ be such that $A_{xy} \neq 0$. Then A^{xy} is a strong \mathbb{P} -matrix.

Proof: Observe that, if A equals the first matrix in Figure 2.6, then $[IA^{xy}]$ can be obtained from $[IA]$ by left multiplication with

$$F := \begin{array}{c} y \\ x' \end{array} \left[\begin{array}{cc} x & x' \\ \hline a^{-1} & 0 \cdots 0 \\ -ba^{-1} & I_{X'} \end{array} \right], \quad (2.6)$$

followed by a column exchange. Exchanging columns clearly preserves weak \mathbb{P} -matrices, and F is invertible. The result now follows from Lemma 2.7.13. ■

The set of bases can be characterized in terms of the generator matrix:

2.7.18 THEOREM. *Let \mathbb{P} be a skew partial field, and A an $X \times Y$ nondegenerate weak \mathbb{P} -matrix. Then B is a basis of $M(\text{span}(A))$ if and only if $A[X, B]$ is invertible.*

Proof: We have already seen that $A[X, B]$ is invertible for every basis B . Suppose the converse does not hold, so there is a $B \subseteq Y$ such that $A[X, B]$ is invertible, but B is not a basis. Let F be the inverse of $A[X, B]$, and consider $A' := FA$. Since F is invertible, it follows that $\text{span}(A') = \text{span}(A)$. Let $C \subseteq B$ be a circuit, and pick an $e \in C$. Let $C' := \|A'[e, E]\|$, the support of the e th row of A' . Clearly $A'[e, E]$ is elementary, so C' is a cocircuit. Then $|C \cap C'| = 1$, a contradiction to Proposition 1.2.16. Hence B contains no circuit, so B is independent, and hence a basis. ■

It follows that Definition 2.7.9 is indeed a generalization of Definition 2.1.5, and that Definition 2.7.12 is indeed a generalization of Definitions 2.1.3 and 2.3.2. We can write $M[A] := M(\text{span}(A))$ for a weak \mathbb{P} -matrix A .

Duality is a bit more subtle. The following definitions are inspired by those found, for instance, in Buekenhout and Cameron (1995).

2.7.19 DEFINITION. Let $R = (S, +, \cdot, 0, 1)$ be a ring. The *opposite* of R is

$$R^\circ := (S, +, \circ, 0, 1),$$

where \circ is the binary operation defined by $p \circ q := q \cdot p$, for all $p, q \in S$. ◇

2.7.20 DEFINITION. Let $\mathbb{P} = (R, G)$ be a skew partial field. The *opposite* of \mathbb{P} , denoted by \mathbb{P}° , is defined as

$$\mathbb{P}^\circ := (R^\circ, G^\circ),$$

where G° is the subgroup of $(R^\circ)^*$ generated by the elements of G . ◇

2.7.21 THEOREM. *Let M be a \mathbb{P} -representable matroid. Then M^* is \mathbb{P}° -representable.*

We omit the proof, which can be based on the following lemma.

2.7.22 LEMMA. *Let R be a ring, let A be an $X \times Y$ matrix over R for disjoint sets X, Y , and let $x \in X, y \in Y$ be such that A_{xy} is invertible. Let $\varphi : R \rightarrow R^\circ$ be the obvious bijection. Then*

$$\varphi \left(-(A^{xy})^T \right) = (-\varphi(A^T))^{yx}.$$

This result follows immediately from Definition 2.7.16 and Definition 2.7.19.

Our final result in this section provides a necessary and sufficient condition for an R -chain group to be a \mathbb{P} -chain group. The theorem generalizes a result by Tutte (1965, Theorem 5.11. See also Oxley, 1992, Proposition 6.5.13). We need the following definition:

2.7.23 DEFINITION. A set $\{C_1, \dots, C_k\}$ of distinct cocircuits of a matroid M is *simply intersecting* if

$$\text{rk}(M/S) = 2,$$

where $S := E(M) - (C_1 \cup \dots \cup C_k)$. \diamond

2.7.24 THEOREM. Let M be a matroid with ground set E and set of cocircuits \mathcal{C}^* . Let $\mathbb{P} = (R, G)$ be a skew partial field. For each $D \in \mathcal{C}^*$, let a^D be a primitive chain with $\|a^D\| = D$. Define the R -chain group

$$C := \left\{ \sum_{D \in \mathcal{C}^*} r_D a^D \mid r_D \in R \right\}.$$

Then C is a \mathbb{P} -chain group with $M = M(C)$ if and only if there exist, for each simply intersecting triple $D, D', D'' \in \mathcal{C}^*$, elements $p, p', p'' \in G$ such that

$$pa^D + p'a^{D'} + p''a^{D''} = 0. \quad (2.7)$$

While we do not use Theorem 2.7.24 in this thesis, it provides a unique insight in the inner workings of partial fields and \mathbb{P} -matroids. We adapt the proof by White (1987, Proposition 1.5.5) of Tutte's theorem. First we prove the following lemma:

2.7.25 LEMMA. Let M and C be as in Theorem 2.7.24, and suppose (2.7) holds. Let B be a basis of M , and let D_1, \dots, D_r be the set of B -fundamental cocircuits of M . Let A be the matrix whose i th row is a^{D_i} . Then $C = \text{span}(A)$.

Proof: We show that any a^D can be obtained through pivoting and scaling.

Pick $x \in B$, $y \in E(M) - B$ such that $B \triangle \{x, y\}$ is a basis.

2.7.25.I CLAIM. Let F be as in (2.6), and define $A' := FA$. Then each row of A' is a G -multiple of a chain $a^{D''}$, for some $D'' \in \mathcal{C}^*$.

Proof: Let D be the B -fundamental cocircuit of x . Pick $x' \in B$, $x' \neq x$, and let D' be the B -fundamental cocircuit of x' . Let D'' be the $B \triangle \{x, y\}$ -fundamental cocircuit of x' . We will show that

$$A'[x', E] = ra^{D''} \quad (2.8)$$

for some $r \in G$. If $y \notin D'$ then $D'' = D'$. Moreover, $A'[x', E] = A[x, E]$, so (2.8) follows. Therefore we may assume $y \in D'$. Clearly $y \notin D''$, so D, D', D'' are pairwise distinct.

CLAIM. The set $\{D, D', D''\}$ is simply intersecting.

Subproof: Define $B' := B - \{x, x'\}$, and note that $B' \cap (D \cup D' \cup D'') = \emptyset$. Then $\text{rk}(M/B') = 2$. If $y' \in E(M) - (B \cup D \cup D' \cup D'')$, then $\text{rk}_{M/B'}(y') = 0$, so $(M/B')/y' = M/B' \setminus y'$. \square

It follows from (2.7) and the previous claim that there exist $p, p', p'' \in G$ such that

$$p'' a^{D''} = -p a^D - p' a^{D'}.$$

Since $y \notin D''$, we have $-p a_y^D = p' a_y^{D'}$. Now

$$\begin{aligned} A'[x', E] &= a^{D'} - a_y^{D'} (a_y^D)^{-1} a^D \\ &= a^{D'} + (p')^{-1} p a^D \\ &= (p')^{-1} p'' a^{D''}, \end{aligned}$$

as desired. \square

For each cocircuit $D \in \mathcal{C}^*$, and for each $e \in D$, there is a basis B' of M such that $B' \cap D = \{e\}$, since $D - e$ can be extended to a cobasis. It follows that $C = \text{span}(A)$. ■

Proof of Theorem 2.7.24: Suppose C is a \mathbb{P} -chain group such that $M = M(C)$. Let $D, D', D'' \in \mathcal{C}^*$ be simply intersecting, and let $S := E(M) - \{D, D', D''\}$. Pick $e \in D - D'$, and $f \in D' - D$. Since D, D' are cocircuits in M/S , $\{e, f\}$ is a basis of M/S , by Proposition 1.2.16. Now D and D' are the $\{e, f\}$ -fundamental cocircuits in M/S , and it follows from the proof of Lemma 2.7.11 that $a^{D''} = p a^D + p' a^{D'}$ for some $p, p' \in R$. But $a_e^{D''} = p a_e^D$, and $a_f^{D''} = p' a_f^{D'}$, so $p, p' \in G$, and (2.7) follows.

For the converse, it follows from Lemma 2.7.25 that, for all $D \in \mathcal{C}^*$, a^D is elementary, and that for every elementary chain c such that $\|c\| \in \mathcal{C}^*$, there is an $r \in R$ such that $c = r a^{\|c\|}$. Suppose there is an elementary chain $c \in C$ such that $\|c\| \notin \mathcal{C}^*$. Clearly $\|c\|$ does not contain any $D \in \mathcal{C}^*$. Therefore $\|c\|$ is coindependent in M . Let B be a basis of M disjoint from $\|c\|$, and let D_1, \dots, D_r be the B -fundamental cocircuits of M . Then $c = p_1 a^{D_1} + \dots + p_r a^{D_r}$ for some $p_1, \dots, p_r \in R$. But, since $c_e = 0$ for all $e \in B$, $p_1 = \dots = p_r = 0$, a contradiction. ■

2.7.1 A note on terminology

Tutte's notation and terminology (in Tutte, 1965) differ markedly from the terminology used in more recent matroid theory texts. In Section 1.1, he associates *atoms* with the polygons of a graph. One would be inclined to identify these with the circuits of a matroid. However, it turns out that a more natural interpretation is to identify these with the *cocircuits* of a matroid. After this the rank function defined by Tutte coincides with Definition 1.2.6, and “the contraction of M to $S \subseteq E(M)$ ” coincides with Definition 1.2.20. Furthermore he uses the word “cell” where we would use “element”, and “dendroid” where we would use “basis”.

In Section 4 he develops a geometric language. In his words, a *flat* of a matroid is a union of cocircuits. In modern terminology this would be the *complement* of a flat. The *dimension* of a flat S is $\text{rk}(M/(E(M) - S)) - 1$. Flats of dimension zero are then called “points” (they coincide with atoms), flats of dimension one are called lines, and so on. Theorem 2.7.24 is then formulated in terms of lines with at least three points, so-called *connected lines*. An important feature of this geometric language is that two points C, D are not necessarily on a common line: the dimension of $C \cup D$ may exceed one. This is easiest visualized in planar graphs.

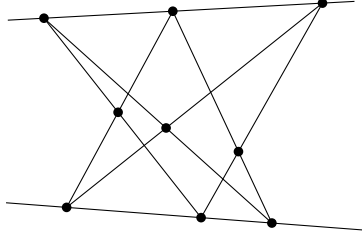


FIGURE 2.7
The Non-Pappus matroid

Dualize, so that cocircuits of the matroid correspond with cycles in the graph, and take two cycles whose intersection has more than one component. This same example inspired our terminology of “simply intersecting cocircuits.”

Tutte’s famous Homotopy Theorem is also formulated using this geometric language. It speaks about paths, which are sequences of points such that two consecutive points are on a connected line. Further details are beyond the scope of this thesis.

2.7.2 An example

2.7.26 DEFINITION. The group ring over $\text{GF}(3)$ of the quaternion group is

$$R_3 := \text{GF}(3)[G],$$

where G is the quaternion group, i.e. the (non-commutative) group generated by $i, j, k, -1$ such that

$$i^2 = j^2 = k^2 = ijk = -1; (-1)^2 = 1.$$

The skew partial field \mathbb{P}_3 is

$$\mathbb{P}_3 := (R_3, R_3^*). \quad \diamond$$

Contrary to the quaternions, R_3 is not a skew field: it has zero divisors. For instance, $(i + j + k)^2 = 0$. Moreover, it can be checked that R_3 has no proper (two-sided) ideals. The units are as follows. First we have the images of the units of the ring of Hürwitz integers, i.e. all elements of the form $\pm 1 \pm i \pm j \pm k$ (see [Conway and Smith, 2003](#), for a definition). Furthermore we have all elements of the form $\pm l$ for all $l \in \{i, j, k\}$, and all elements of the form $\pm 1 \pm l$, for all $l \in \{i, j, k\}$.

2.7.27 DEFINITION. The *Non-Pappus matroid* is the matroid whose geometrical representation is shown in Figure 2.7. \diamond

See also [Oxley \(1992, Example 1.5.14\)](#). It is well-known that the Non-Pappus matroid is not representable over any field, but is representable over some skew fields. We claim that it is also representable over the skew partial field \mathbb{P}_3 .

2.7.28 THEOREM. The Non-Pappus matroid is representable over \mathbb{P}_3 .

Sketch of proof: Let A be the following matrix with entries in \mathbb{P}_3 :

$$A = \begin{bmatrix} 0 & i & -1+i-j-k & -1-i-j+k & i & 1 \\ j & i & 1 & i & k & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

Then A is a strong \mathbb{P}_3 -matrix, and the Non-Pappus matroid is equal to $M[IA]$. We leave the calculations out: those are best left to a computer. ■

A second, more dramatic, example is the following. We will not give a formal definition of Dowling geometry here, referring to Section 3.2 for the representable case (which does not include the example below), and to [Zaslavsky \(1989\)](#) for the general case.

2.7.29 DEFINITION. Let $Q_3(G)$ be the rank-three Dowling group geometry of the quaternion group G , and let $\text{PG}(2, 3)$ be the projective plane over $\text{GF}(3)$. Define $M := Q_3(G) \oplus \text{PG}(2, 3)$. ◇

2.7.30 THEOREM. The matroid M defined in Definition 2.7.29 is representable over \mathbb{P}_3 . Moreover, every representation of M over a skew partial field $\mathbb{P} = (R, G)$ can be obtained from a \mathbb{P}_3 -representation through a ring homomorphism $R_3 \rightarrow R$.

We omit the proof, which is similar to the arguments used in the proof of Theorem 3.3.25. Surprisingly, we have the following corollary:

2.7.31 COROLLARY. There exist matroids that are representable over a skew partial field but not over any skew field.

A remarkable feature of \mathbb{P}_3 is that the skew partial field is *finite*. This is in stark contrast to Wedderburn's theorem that every finite skew field is a field.

2.8 Open problems

By now it is clear that it is useful to know the fundamental elements of a partial field. All the examples in Section 2.5 were proven using ad hoc techniques, the only recurring tool being homomorphisms to partial fields whose fundamental elements had been computed earlier. It is desirable to have results that determine the fundamental elements for complete classes of partial fields. Only for one infinite class have the fundamental elements been characterized: [Sample \(1997\)](#) determined the fundamental elements for the k -uniform partial fields. As we have seen in the case of $\mathbb{U}_1^{(2)}$, the number of fundamental elements of even very simple partial fields can be infinite.

The following problem is more modest. A positive answer would imply that we can compute with partial fields even when we do not know the full set of fundamental elements.

2.8.1 PROBLEM. Let I be an ideal of the multivariate polynomial ring $\mathbb{Z}[x_1, \dots, x_k]$ such that x_1, \dots, x_k are units of $R := \mathbb{Z}[x_1, \dots, x_k]/I$, and let G be the subgroup of

R^* generated by x_1, \dots, x_k . Is there an algorithm to determine, for $p \in G$, if $1 - p \in G$? \diamond

Note that we do not ask for a polynomial-time algorithm.

Next we consider induced sub-partial fields, which were introduced in Section 2.2.3. We wonder if the converse of Lemma 2.2.18 holds.

- 2.8.2 **PROBLEM.** Suppose \mathbb{P}' is an induced sub-partial field of \mathbb{P} , with $\mathcal{F}(\mathbb{P}') - \{0, 1\} \neq \emptyset$. Are there rings $R, R' \subseteq R$, and groups $G \subseteq R^*, G' \subseteq G$ such that $\mathbb{P} \cong (R, G)$, $\mathbb{P}' \cong (R', G')$, and $G' = G \cap R'$? \diamond

The ring R that we have in mind is the ring constructed in the proof of Theorem 2.6.7. It is not unlikely that the answer to this question is “not always”. The condition that there is a nontrivial fundamental element cannot be omitted: Andries Brouwer (personal communication) found a counterexample for which $\mathcal{F}(\mathbb{P}') = \{0, 1\}$.

The next few conjectures concern the relation between a partial field and the (finite) fields to which it has a homomorphism.

- 2.8.3 **QUESTION.** To what extent is a partial field \mathbb{P} determined by the set of finite fields $\text{GF}(q)$ for which there exists a homomorphism $\varphi : \mathbb{P} \rightarrow \text{GF}(q)$? \diamond

\mathbb{P} is certainly not uniquely determined: both \mathbb{K}_2 and \mathbb{U}_2 have homomorphisms to all finite fields with at least 4 elements, but some \mathbb{K}_2 -representable matroids are not \mathbb{U}_2 -representable. Let $\mathcal{P}_0 := \{0\} \cup \{x \in \mathbb{N} \mid x \text{ is prime}\}$.

- 2.8.4 **DEFINITION.** Let \mathbb{P} be a partial field. The *characteristic set* of \mathbb{P} is

$$\chi(\mathbb{P}) := \{p \in \mathcal{P}_0 \mid \text{There is a homomorphism } \mathbb{P} \rightarrow \mathbb{F} \text{ for some field of characteristic } p\}. \quad \diamond$$

- 2.8.5 **PROBLEM.** For which subsets S of \mathcal{P}_0 does there exist a partial field \mathbb{P} with $\chi(\mathbb{P}) = S$? \diamond

Our inspiration for this problem lies in the characteristic set of a matroid, which will be discussed in Section 3.3. The problem seems to become easier if we restrict our attention to ring homomorphisms.

Finally we turn our attention to skew partial fields, the subject of Section 2.7. We have seen in Corollary 2.7.31 that Proposition 2.2.6 does not generalize to skew partial fields. This raises new questions: what types of matroids are representable over skew partial fields? Some obvious non-representable matroids, such as the Non-Desargues matroid, the Vámos matroid, and non-representable relaxations of P_8 , are also not representable over skew partial fields. A criterion satisfied by all matroids representable over some skew field is *Ingleton's Inequality* (Ingleton, 1971).

- 2.8.6 **QUESTION.** Does Ingleton's Inequality hold for matroids representable over a skew partial field? \diamond

The matroid in Definition 2.7.29 has 37 elements and rank 6. By replacing $\text{PG}(2, 3)$ by some smaller matroid, and by taking the 2-sum rather than the direct sum, these numbers can be reduced to some extent. However, it is quite possible that there exists a much smaller matroid having the same property:

- 2.8.7 **PROBLEM.** Find small matroids that are representable over a skew partial field but not over a skew field. \diamond
- 2.8.8 **PROBLEM.** Find a 3-connected matroid that is representable over a skew partial field but not over a skew field. \diamond



Constructions for partial fields

IN Section 2.5 we introduced many partial fields. However, we defined them without giving any clue why these were of interest or how they were found. Nearly all of these arise from constructions related to specific classes of matroids. Most of these constructions can be found in this chapter; one more construction will be presented in Section 4.3.

We start, in Section 3.1, with a construction that crops up throughout this thesis. It provides a way to combine distinct representations of a matroid into one representation over a new partial field.

It is a well-known fact that all graphic matroids are regular. In Section 3.2 we study a generalization of this. We introduce the class of \mathbb{P} -graphic matroids for a partial field \mathbb{P} . This is a subset of the set of minors of the Dowling geometries over the group \mathbb{P}^* . We construct a partial field $\mathbb{D}\mathbb{P}$ over which all \mathbb{P} -graphic matroids are representable.

In Section 3.3 we zoom in on a single matroid M , and compute its *universal partial field*. It has the following useful property:

3.A THEOREM. *Let M be a matroid, let X be a basis of M , and let $Y := E(M) - X$. There exist a partial field \mathbb{P}_M and an $X \times Y$ \mathbb{P}_M -matrix A , such that there is a homomorphism $\varphi : \mathbb{P}_M \rightarrow \mathbb{P}'$ with $\varphi(A) \sim A'$ for every partial field \mathbb{P}' and for every $X \times Y$ \mathbb{P}' -matrix A' with $M = M[I A']$.*

In other words, every representation of M , over every partial field, can be obtained from A .

This chapter is based on joint work with Rudi Pendavingh. Most results in this chapter can be found in (Pendavingh and Van Zwam, 2008, 2009a); a paper containing the results from Section 3.2 is currently in preparation (Pendavingh and Van Zwam, 2009b).

3.1 The product of partial fields

Recall that the product $R_1 \times R_2$ of two rings is again a ring, where addition and multiplication are componentwise, the zero element is $(0, 0)$, and the identity is $(1, 1)$. A fundamental construction for partial fields is the following:

3.1.1 DEFINITION. Let $\mathbb{P}_1 = (R_1, G_1)$, $\mathbb{P}_2 = (R_2, G_2)$ be partial fields. The *direct product* is

$$\mathbb{P}_1 \times \mathbb{P}_2 := (R_1 \times R_2, G_1 \times G_2). \quad \diamond$$

Note that, if $\mathbb{F}_1, \mathbb{F}_2$ are fields, $\mathbb{F}_1 \times \mathbb{F}_2$ can denote either the product ring or the product partial field. Unless stated otherwise, always the second option is intended.

3.1.2 PROPOSITION. If $\mathbb{P}_1, \mathbb{P}_2$ are partial fields then $\mathbb{P}_1 \times \mathbb{P}_2$ is a partial field. Moreover,

$$\begin{aligned} \mathcal{F}(\mathbb{P}_1 \times \mathbb{P}_2) = & \{(0, 0), (1, 1)\} \cup \\ & \{(p, q) \mid p \in \mathcal{F}(\mathbb{P}_1) - \{0, 1\}, q \in \mathcal{F}(\mathbb{P}_2) - \{0, 1\}\}. \end{aligned}$$

Proof: $R_1 \times R_2$ is a commutative ring, and $G_1 \times G_2$ an abelian group containing $(-1, -1)$, so $\mathbb{P}_1 \times \mathbb{P}_2$ is a partial field. Now let $(p, q) \in \mathbb{P}_1 \times \mathbb{P}_2$ be a fundamental element other than $(0, 0), (1, 1)$. Then $(1, 1) - (p, q) = (1 - p, 1 - q) \in G_1 \times G_2$. The result follows. ■

3.1.3 DEFINITION. Let $\mathbb{P}, \mathbb{P}_1, \mathbb{P}_2$ be partial fields, and $\varphi_1 : \mathbb{P} \rightarrow \mathbb{P}_1$, $\varphi_2 : \mathbb{P} \rightarrow \mathbb{P}_2$ partial-field homomorphisms. Then the *product homomorphism* $\varphi_1 \times \varphi_2 : \mathbb{P} \rightarrow \mathbb{P}_1 \times \mathbb{P}_2$ is defined by

$$(\varphi_1 \times \varphi_2)(p) := (\varphi_1(p), \varphi_2(p)). \quad \diamond$$

3.1.4 LEMMA. $\varphi_1 \times \varphi_2$ is a partial-field homomorphism.

The proof is elementary and therefore omitted.

3.1.5 PROPOSITION. Let $\mathbb{P}_1, \mathbb{P}_2$ be partial fields, A_1 an $X \times Y$ \mathbb{P}_1 -matrix, and A_2 an $X \times Y$ \mathbb{P}_2 -matrix for disjoint sets X, Y , such that $M[I A_1] = M[I A_2]$. Let A be the $X \times Y$ matrix over $\mathbb{P}_1 \times \mathbb{P}_2$ such that $A_{xy} = ((A_1)_{xy}, (A_2)_{xy})$. Then A is a $\mathbb{P}_1 \times \mathbb{P}_2$ -matrix, and $M[I A] = M[I A_1]$.

Proof: Since $M[I A_1] = M[I A_2]$, $(A_1)_{xy} = 0$ if and only if $(A_2)_{xy} = 0$. Likewise, if $(A_1)_{xy} \neq 0$, then $((A_1)^{xy})_{uv} = 0$ if and only if $((A_2)^{xy})_{uv} = 0$. Then it follows from Lemma 2.3.18 that all subdeterminants of A are in $\mathbb{P}_1 \times \mathbb{P}_2$. ■

3.1.1 Examples

As an illustration of the power of the direct product we give short proofs of two well-known results. The first, a classical theorem by Tutte, was already mentioned in the introduction. Recall that \mathbb{U}_0 is the regular partial field.

3.1.6 THEOREM (Tutte, 1965). *Let M be a matroid. The following are equivalent:*

- (i) M is representable over both $\text{GF}(2)$ and $\text{GF}(3)$;
- (ii) M is representable over $\text{GF}(2)$ and some field \mathbb{F} that does not have characteristic 2;
- (iii) M is representable by a \mathbb{U}_0 -matrix;
- (iv) M is representable over every field.

Proof: That (iii) implies (iv) follows from Lemma 2.5.2. Clearly, if (iv) holds then also (i) holds, and if (i) holds then also (ii) holds. It follows that we only have to prove that (ii) implies (iii). Let \mathbb{F} be a field that is not of characteristic 2, and consider the partial field $\mathbb{P} := \text{GF}(2) \times \mathbb{F}$. Its elements are $\{(0, 0)\} \cup \{(1, p) \mid p \in \mathbb{F}^*\}$. The element $(0, 0)$ is fundamental. Suppose $(1, p)$ is a fundamental element for some $p \in \mathbb{F}^*$. Then $(1, 1) - (1, p) = (0, 1 - p) \in \mathbb{P}$. It follows that $1 - p = 0$, so $p = 1$. Hence $\mathcal{F}(\mathbb{P}) = \{(0, 0), (1, 1)\}$. By Proposition 2.2.16 any \mathbb{P} -representable matroid is also representable over $\mathbb{P}' := \mathbb{P}[(0, 0), (1, 1)]$. This partial field has but 3 elements: $\{(0, 0), (1, 1), (1, -1)\}$. \mathbb{F} does not have characteristic 2, so $(1, 1) \neq (1, -1)$. Now the unique partial-field homomorphism $\varphi : \mathbb{U}_0 \rightarrow \mathbb{P}'$ is an isomorphism, and the result follows. ■

The next result is part of Whittle's (1995; 1997) classification of ternary matroids in terms of representability over other fields. Recall the $\sqrt[3]{1}$ partial field, \mathbb{S} .

3.1.7 THEOREM (Whittle, 1997). *Let M be a matroid. The following are equivalent:*

- (i) M is representable over $\text{GF}(3) \times \text{GF}(4)$;
- (ii) M is \mathbb{S} -representable;
- (iii) M is representable over $\text{GF}(3)$, over $\text{GF}(p^2)$ for all primes p , and over $\text{GF}(p)$ when $p \equiv 1 \pmod{3}$.

Proof: It follows from Lemma 2.5.12 that (ii) implies (iii). Again, (i) is a special case of (iii).

Let $\varphi : \mathbb{S} \rightarrow \text{GF}(3) \times \text{GF}(4)$ be determined by $\varphi(\zeta) = (-1, \omega)$, where $\omega \in \text{GF}(4) - \{0, 1\}$ is a generator of $\text{GF}(4)^*$. Then φ is an isomorphism, and hence (i) implies (ii). ■

The proofs of Whittle's other results, such as Theorem 1.2.11, require other tools besides partial-field homomorphisms. This need becomes apparent from the fact that $(\text{GF}(3) \times \text{GF}(5))^*$ is finite whereas \mathbb{D}^* is infinite. We will address this issue in Chapter 4, and give alternative proofs of Whittle's results in Section 4.2. In Section 6.3 we will give an alternative proof of his classification theorem.

3.2 The Dowling lift of a partial field

In 1972, Dowling introduced a class of geometric lattices associated with a finite group. Today these are known as *Dowling geometries*. Just as partition lattices correspond to the matroids of complete graphs (see Oxley, 1992, Page 57), the Dowling geometries correspond to the matroids of group-labelled graphs (sometimes called gain graphs). This theory and its generalizations were developed by

Zaslavsky in a series of papers starting with (Zaslavsky, 1989). The matroids we consider in this section will be minors of Dowling geometries. We will not describe the theory in its full generality here. The remainder of this thesis does not depend on the content of this section.

3.2.1 DEFINITION. A matrix A is *graphic* if each column of A has at most two nonzero entries. \diamond

3.2.2 DEFINITION. Let \mathbb{P} be a partial field. A matroid M is \mathbb{P} -*graphic* if there exists a graphic \mathbb{P} -matrix A such that $M = M[A]$. \diamond

Note that we do not require A to have a displayed identity matrix, but we do require A to be a strong \mathbb{P} -matrix. The class of \mathbb{P} -graphic matroids is minor-closed:

3.2.3 PROPOSITION. Let M be a \mathbb{P} -graphic matroid, and $N \preceq M$. Then N is \mathbb{P} -graphic.

Proof: It suffices to prove the result when $|E(N)| = |E(M)| - 1$. If $N = M \setminus e$ for $e \in E(M)$ then this is obvious, so suppose $N = M/e$. Let A be an $X \times E$ graphic \mathbb{P} -matrix such that $M = M[A]$. Define $M' := M[I A]$, so $M = M' \setminus X$. If all entries of $A[X, e]$ are zero then $M/e = M \setminus e$, so we may assume that $A_{xe} \neq 0$ for some $x \in X$. Consider A^{xe} . Every column of this matrix has at most three nonzero entries, and if a column has exactly three nonzero entries, then one of these is in the row now indexed by e . Therefore $A^{xe} - e$ is again a graphic \mathbb{P} -matrix, and $M'/e = M[I(A^{xe} - e)]$. The result follows since $M/e = M'/e \setminus X$. ■

3.2.4 LEMMA. Let A be a graphic \mathbb{P} -matrix, and C a cycle of $G(A)$. Then C is an induced cycle.

Proof: Suppose the lemma is false for an $X \times Y$ graphic \mathbb{P} -matrix A , where X and Y are disjoint. Let C be a cycle of $G(A)$ that is not induced. Let $v, w \in V(C)$ be nonadjacent vertices such that $vw \in E(G(A))$. In $G(A)$ all vertices labelled by Y have degree at most two. v and w have degree three, so $v, w \in X$. But all edges of $G(A)$ have one end vertex in X and one in Y , a contradiction. ■

For readers familiar with Dowling geometries and gain graphs we note that the graph usually associated with a \mathbb{P} -graphic matroid is obtained from $G(A)$ by contracting one of the edges of each $X - Y - X$ path. The gains on the cycles correspond to the signature (Definition 2.3.37) of the corresponding cycle of $G(A)$.

3.2.5 PROPOSITION. Let A be a matrix with entries in \mathbb{P} with at most two nonzero entries in each column. Then A is a \mathbb{P} -matrix if and only if $\sigma_A(C) \in \mathcal{F}(\mathbb{P})$ for all cycles C of $G(A)$.

Proof: Necessity follows immediately from Lemma 3.2.4 and Corollary 2.3.39. To prove sufficiency, suppose that there exist disjoint sets X, Y , and an $X \times Y$ matrix A with entries in \mathbb{P} and at most two nonzero entries in each column, such that $\sigma_A(C) \in \mathbb{P}$ for all cycles C of $G(A)$, but A is not a \mathbb{P} -matrix. Then $\det(A[Z]) \notin \mathbb{P}$ for some $Z \subseteq X \cup Y$. Suppose Z was chosen such that $|Z|$ is minimal. If $A[Z]$ has an

all-zero row or column then $\det(A[Z]) = 0 \in \mathbb{P}$, a contradiction. Suppose Z has a row or column z with at most one non-zero entry, say $A_{xy} \neq 0$ with $z \in \{x, y\}$. Expanding $\det(A[Z])$ along z we obtain $\det(A[Z]) = A_{xy} \det(A[Z - \{x, y\}])$, contradicting minimality of $|Z|$. Hence each row and each column of $A[Z]$ has at least two nonzero entries. Each column then has exactly two nonzero entries, and since A is square, necessarily each row has exactly two nonzero entries. But then $G(A[Z])$ consists of disjoint cycles. Since these are induced cycles of $G(A)$, it follows from Lemma 2.3.38(iv) that $\det(A[Z]) \in \mathbb{P}$, a contradiction. ■

From Proposition 3.2.5 and Definition 2.3.37 it follows that only the multiplicative structure of \mathbb{P} is relevant for \mathbb{P} -graphic matroids. This motivates the following definition:

3.2.6 DEFINITION. Let \mathbb{P} be a partial field. The *Dowling lift* of \mathbb{P} is

$$\mathbb{D}\mathbb{P} := (D_{\mathbb{P}}/J_{\mathbb{P}}, \langle \{-1\} \cup \overline{G}_{\mathbb{P}} \rangle).$$

Here $\overline{G}_{\mathbb{P}} := \langle \overline{G} \cup \overline{Q}_{\mathbb{P}} \rangle$, where \overline{G} is an isomorphic copy of \mathbb{P}^* with elements $\{\overline{p} \mid p \in \mathbb{P}^*\}$, $\overline{Q}_{\mathbb{P}} := \{\overline{q}_p \mid p \in \mathcal{F}(\mathbb{P}) - \{0, 1\}\}$ is a set of indeterminates, $D_{\mathbb{P}} := R[\overline{Q}_{\mathbb{P}}]$ is the ring of polynomials in $\overline{Q}_{\mathbb{P}}$ over the group ring $R := \mathbb{Z}[\overline{G}]$, and $J_{\mathbb{P}}$ is the ideal in $D_{\mathbb{P}}$ generated by

$$\{\overline{1} - 1\} \cup \{\overline{q}_p(1 - \overline{p}) - 1 \mid p \in \mathcal{F}(\mathbb{P}) - \{0, 1\}\}. \quad \diamond$$

3.2.7 LEMMA. There is a partial-field homomorphism $\varphi : \mathbb{D}\mathbb{P} \rightarrow \mathbb{P}$.

Proof: Suppose $\mathbb{P} = (R, G)$. Let $\varphi'' : D_{\mathbb{P}} \rightarrow R$ be the ring homomorphism defined by $\varphi''(\overline{p}) = p$ for all $p \in G$, and $\varphi''(\overline{q}_p) = (1 - p)^{-1}$ for all $p \in \mathcal{F}(\mathbb{P})$. Then $J_{\mathbb{P}} \subseteq \ker(\varphi'')$, so there is a well-defined ring homomorphism $\varphi' : D_{\mathbb{P}}/J_{\mathbb{P}} \rightarrow R$. Then the restriction $\varphi := \varphi'|_{\mathbb{D}\mathbb{P}}$ is the desired partial-field homomorphism. ■

We denote the canonical homomorphism constructed in the proof by $\varphi_{\mathbb{D}\mathbb{P}}$. There are many more homomorphisms:

3.2.8 THEOREM. Let \mathbb{P}' be a partial field such that \mathbb{P}^* is isomorphic to a subgroup of $(\mathbb{P}')^*$. Then there is a partial-field homomorphism $\mathbb{D}\mathbb{P} \rightarrow \mathbb{P}'$.

Dowling (1973) already observed this in the case that \mathbb{P} is a field. We omit the straightforward proof. Our main result of this section is the following:

3.2.9 THEOREM. Let \mathbb{P} be a partial field, and $M = M[A]$ for a graphic \mathbb{P} -matrix A . Then there is a $\mathbb{D}\mathbb{P}$ -matrix A' such that $A = \varphi_{\mathbb{D}\mathbb{P}}(A')$.

Proof: Let A' be defined by $A'_{xy} := \overline{A}_{xy} + J_{\mathbb{P}}$ if $A_{xy} \neq 0$, and $A'_{xy} := 0 + J_{\mathbb{P}}$ otherwise. Let C be a cycle of $G(A')$, and suppose $\sigma_A(C) = p$. Then $\sigma_{A'}(C) = \overline{p} + J_{\mathbb{P}}$. Since $p \in \mathcal{F}(\mathbb{P})$, $1 - \overline{p} + J_{\mathbb{P}} = \overline{q}_p + J_{\mathbb{P}} \in \mathbb{P}$. Hence $\overline{p} + J_{\mathbb{P}} \in \mathcal{F}(\mathbb{D}\mathbb{P})$. It follows from Proposition 3.2.5 that A' is a $\mathbb{D}\mathbb{P}$ -matrix. By construction $\varphi_{\mathbb{D}\mathbb{P}}(A') = A$. ■

\mathbb{P}	$\text{GF}(2)$	$\text{GF}(3)$	$\text{GF}(4)$	$\text{GF}(5)$	\mathbb{S}	\mathbb{G}
\mathbb{DP}	\mathbb{U}_0	\mathbb{D}	\mathbb{W}	\mathbb{H}_2	\mathbb{U}_1	\mathbb{K}_2

TABLE 3.1
Some Dowling lifts of partial fields.

3.2.1 Examples

We give a few examples. The results can be obtained by computing a Gröbner basis over the integers for $J_{\mathbb{P}}$.

3.2.IO THEOREM. $\mathbb{D}\text{GF}(2) \cong \mathbb{U}_0$.

Proof: Following Definition 3.2.6 we find $\overline{G}_{\mathbb{P}} = \{\overline{1}\}$, $D_{\mathbb{P}} = \mathbb{Z}[\{\overline{1}\}]$, and $J_{\mathbb{P}} = \{\overline{1} - 1\}$. Hence $D_{\mathbb{P}}/J_{\mathbb{P}} \cong \mathbb{Z}$, and therefore $\mathbb{D}\text{GF}(2) \cong (\mathbb{Z}, \{-1, 0, 1\}) = \mathbb{U}_0$. ■

In other words, all graphic matroids are regular, a well-established fact (see Oxley, 1992, Proposition 5.1.2 for an alternative proof).

3.2.II THEOREM. $\mathbb{D}\text{GF}(3) \cong \mathbb{D}$.

Proof: We find $\overline{G}_{\mathbb{P}} = \{\overline{1}, \overline{-1}, \overline{q_{-1}}\}$, $D_{\mathbb{P}} = \mathbb{Z}[\{\overline{1}, \overline{-1}\}][\overline{q_{-1}}]$, and $J_{\mathbb{P}}$ is generated by $\{\overline{1} - 1, \overline{q_{-1}}(1 - \overline{-1}) - 1\}$. Since $\overline{-1}^2 = \overline{1}$, we find

$$(1 + \overline{-1})(\overline{q_{-1}}(1 - \overline{-1}) - 1) + J_{\mathbb{P}} = -\overline{-1} - 1 + J_{\mathbb{P}},$$

so $-\overline{-1} + J_{\mathbb{P}} = -1 + J_{\mathbb{P}}$. Then $2\overline{q_{-1}} - 1 \in J_{\mathbb{P}}$, and the result follows. ■

More results are collected in Table 3.1; we omit the proofs. Note that computing \mathbb{DP} is only of interest if the fundamental elements of \mathbb{P} have nontrivial additive structure.

3.3 The universal partial field of a matroid

In this section we find the “most general” partial field over which a single matroid is representable. We start with an example. Figure 3.1 is a geometric representation of the matroid $\text{AG}(2, 3)$. In Figure 3.1 there are no loops, and all points are in distinct positions. Hence all circuits have size at least three. All points are in the same plane, so every set of four points is dependent. Therefore the matroid has rank three.

Consider the following matrix with entries in \mathbb{S} :

$$A := \begin{matrix} & \begin{matrix} 4 & 5 & 6 & 7 & 8 & 9 \end{matrix} \\ \begin{matrix} 1 \\ 2 \\ 3 \end{matrix} & \begin{bmatrix} \textcircled{1} & 0 & \textcircled{1} & \textcircled{1} & \textcircled{1} & \textcircled{1} \\ \textcircled{1} & \textcircled{1} & 0 & \zeta & 1 & \zeta \\ 0 & \textcircled{1} & \zeta^2 & \zeta^2 & \zeta & \zeta \end{bmatrix} \end{matrix}.$$

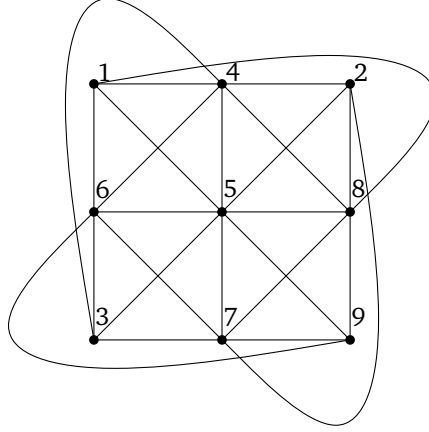


FIGURE 3.1
Geometric representation of the matroid $AG(2, 3)$.

It is readily checked that A is an \mathbb{S} -matrix, and $AG(2, 3) = M[I A]$. The entries corresponding to the edges of a spanning tree T of $G(A)$ have been circled. We will prove the following theorem, which states that every representation of $AG(2, 3)$ can be obtained from A :

3.3.I THEOREM. Let $\mathbb{P}' = (R', G')$ be a partial field, and A' a T -normalized $\{1, 2, 3\} \times \{4, 5, 6, 7, 8, 9\}$ \mathbb{P}' -matrix such that $AG(2, 3) = M[I A']$. Then there is a ring homomorphism $\varphi : \mathbb{Z}[\zeta] \rightarrow R'$ such that $A' = \varphi(A)$.

Proof: By Lemma 2.4.18, $G(A') = G(A)$. Hence T is a spanning tree of $G(A')$, so there are $t, u, v, w, x, y, z \in \mathbb{P}'$ such that

$$A' = \begin{matrix} & \begin{matrix} 4 & 5 & 6 & 7 & 8 & 9 \end{matrix} \\ \begin{matrix} 1 \\ 2 \\ 3 \end{matrix} & \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & z & y & x \\ 0 & 1 & w & v & u & t \end{bmatrix} \end{matrix}.$$

Since $\{2, 6, 7\}$ is dependent, $\det([I A][\{1, 2, 3\}, \{2, 6, 7\}]) = v - w = 0$, so $v = w$. Since $\{3, 7, 9\}$ is dependent, $z = x$. Since $\{2, 8, 9\}$ is dependent, $u = t$. Since $\{1, 5, 9\}$ is dependent, $x = t$. Since $\{3, 4, 8\}$ is dependent, $y = 1$. Since $\{1, 7, 8\}$ is dependent, $v = z^2$. So we have

$$A = \begin{matrix} & \begin{matrix} 4 & 5 & 6 & 7 & 8 & 9 \end{matrix} \\ \begin{matrix} 1 \\ 2 \\ 3 \end{matrix} & \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & z & 1 & z \\ 0 & 1 & z^2 & z^2 & z & z \end{bmatrix} \end{matrix}.$$

Since $\{4, 5, 7\}$ is dependent, $z^2 - z + 1 = 0$. It follows that there is a ring homomorphism $\varphi : \mathbb{Z}[\zeta] \rightarrow R'$, determined by $\varphi(\zeta) = z$. ■

As indicated in the introduction, this is not an isolated result. In the remainder of this section we will show how to construct a universal representation for any matroid. Our construction is based on the bracket ring that was introduced by [White \(1975a\)](#).

3.3.1 The bracket ring

Let M be a rank- r matroid with ground set E and set of bases \mathcal{B} . For every r -tuple $Z \in E^r$ we introduce a symbol $[Z]$, the “bracket” of Z , and a symbol $[\overline{Z}]$. Suppose $Z = (x_1, \dots, x_r)$. Define $\{Z\} := \{x_1, \dots, x_r\}$, and $Z/x \rightarrow y$ as the r -tuple obtained from Z by replacing each occurrence of x by y . We define

$$\mathcal{Z}_M := \{[Z] \mid Z \in E^r\} \cup \{[\overline{Z}] \mid \{Z\} \in \mathcal{B}\}.$$

3.3.2 DEFINITION. I_M is the ideal in $\mathbb{Z}[\mathcal{Z}_M]$ generated by the following polynomials:

- (i) $[Z]$, for all Z such that $\{Z\} \notin \mathcal{B}$;
- (ii) $[Z] - \text{sgn}(\sigma)[Z^\sigma]$, for all Z and all permutations $\sigma : \{1, \dots, r\} \rightarrow \{1, \dots, r\}$;
- (iii) $[x_1, x_2, U][y_1, y_2, U] - [y_1, x_2, U][x_1, y_2, U] - [y_2, x_2, U][y_1, x_1, U]$, for all $x_1, x_2, y_1, y_2 \in E$ and $U \in E^{r-2}$;
- (iv) $[Z][Z] - 1$, for all $Z \in E^r$ such that $\{Z\} \in \mathcal{B}$. ◇

3.3.3 DEFINITION. $B_M := \mathbb{Z}[\mathcal{Z}_M]/I_M$. ◇

Relations (i)–(iii) are the same as those in White’s (1975a) construction. They accomplish that the brackets behave like determinants in B_M . A special case of (i) occurs when $|\{Z\}| < r$. In that case Z must have repeated elements. Relations (iv) are not present in the work of White.

3.3.4 LEMMA. Let $\mathbb{P} = (R, G)$ be a partial field and A an $r \times E$ \mathbb{P} -matrix such that $M = M[A]$. Then there exists a ring homomorphism $\varphi : B_M \rightarrow R$.

Proof: Let $\varphi' : \mathbb{Z}[\mathcal{Z}_M] \rightarrow \mathbb{F}$ be such that $\varphi'([Z]) = \det(A[r, Z])$ and $\varphi'([\overline{Z}]) = \det(A[r, Z])^{-1}$ if $\{Z\} \in \mathcal{B}$, and such that $\varphi'([Z]) = 0$ otherwise. We show that $I_M \subseteq \ker(\varphi')$, from which the result follows. Relations (i) follow from linear dependence, Relations (ii) from antisymmetry of the determinant, and Relations (iii) from the so-called 3-term Grassmann-Plücker relations (see, for example, [Björner et al., 1993](#), Page 127). ■

With our addition to White’s construction we are actually able to represent M over the partial field $(B_M, \langle \mathcal{Z}_M \cup \{-1\} \rangle)$. Note that, as soon as $\text{rk}(M) \geq 2$, we can pick a basis Z and an odd permutation σ of the elements of Z to obtain $[Z^\sigma][\overline{Z}] = -1 \in \langle \mathcal{Z}_M \rangle$, making the -1 in the definition of the partial field redundant. From now on we will be slightly sloppy in our notation and write Z rather than $\{Z\}$, if it is clear that Z has no repeated elements.

3.3.5 DEFINITION. Let M be a rank- r matroid. Let $B \in E^r$ be such that $\{B\}$ is a basis of M . $A_{M,B}$ is the $B \times (E - B)$ matrix with entries in B_M given by

$$(A_{M,B})_{uv} := [B/u \rightarrow v]/[B]. \quad \diamond$$

3.3.6 LEMMA. $A_{M,B}$ is a (B_M, B_M^*) -matrix.

Proof: Let $A := A_{M,B}$. Let $x \in B, y \in E - B$ be such that $B' := B \triangle \{x, y\}$ is again a basis. We study the effect of a pivot over xy . Let $u \in B - x, v \in (E - B) - y$. We have

$$(A^{xy})_{yx} = A_{xy}^{-1} = [B]/[B/x \rightarrow y], \quad (3.1)$$

$$\begin{aligned} (A^{xy})_{yv} &= A_{xy}^{-1} A_{xv} = ([B]/[B/x \rightarrow y])([B/x \rightarrow v]/[B]) \\ &= [B'/y \rightarrow v]/[B/x \rightarrow y], \end{aligned} \quad (3.2)$$

$$\begin{aligned} (A^{xy})_{ux} &= -A_{xy}^{-1} A_{uy} = -([B]/[B/x \rightarrow y])([B/u \rightarrow y]/[B]) \\ &= [B/x \rightarrow y/u \rightarrow x]/[B/x \rightarrow y], \end{aligned} \quad (3.3)$$

$$\begin{aligned} (A^{xy})_{uv} &= A_{uv} - A_{xy}^{-1} A_{uy} A_{xv} \\ &= \frac{[B/u \rightarrow v]}{[B]} - \frac{[B]}{[B/x \rightarrow y]} \frac{[B/u \rightarrow y]}{[B]} \frac{[B/x \rightarrow v]}{[B]} \\ &= \frac{[B/x \rightarrow y][B/u \rightarrow v] - [B/u \rightarrow y][B/x \rightarrow v]}{[B][B/x \rightarrow y]} \\ &= \frac{[B][B/x \rightarrow y/u \rightarrow v]}{[B][B/x \rightarrow y]}. \end{aligned} \quad (3.4)$$

For (3.3) we note that $[B/x \rightarrow y/u \rightarrow x]$ is a permutation of $[B/u \rightarrow y]$; by 3.3.2(ii) the minus sign vanishes. For (3.4) we use 3.3.2(iii). In short, for every entry $u \in B', v \in (E - B')$ we have

$$(A^{xy})_{uv} = [B'/u \rightarrow v]/[B'],$$

so $(A_{M,B})^{xy} = A_{M,B'}$. By Lemma 2.3.18 we find that every subdeterminant is equal to $\prod_{i=1}^k [Z_i]/[B_i]$ for some $Z_i, B_i \in E^r$ with all B_i bases, and therefore, by 3.3.2(iv), every subdeterminant is either equal to zero or invertible. The lemma follows. ■

3.3.7 LEMMA. Let M be a matroid such that B_M is nontrivial. If B is a basis of M then $M = M[I A_{M,B}]$.

Proof: By construction M and $M[I A_{M,B}]$ have the same set of bases. ■

The following theorem gives a characterization of representability:

3.3.8 THEOREM. M is representable if and only if B_M is nontrivial.

Proof: $\varphi(1) = 1$ for any homomorphism φ . Therefore, if M is representable then Lemma 3.3.4 implies that B_M is nontrivial. Conversely, if B_M is nontrivial then Lemma 3.3.7 shows that M is representable over the partial field (B_M, B_M^*) . ■

The following lemma can be proven by adapting the proof of the corresponding result in White (1975a, Theorem 8.1):

3.3.9 LEMMA. $B_{M^*} \cong B_M$.

Finally we consider the effect of taking a minor.

3.3.10 DEFINITION. Let M be a matroid, and let $U, V \subseteq E(M)$ be disjoint ordered subsets such that U is independent and V coindependent. Then we define

$$\tilde{\varphi}_{M,U,V} : B_{M/U \setminus V} \rightarrow B_M$$

by $\tilde{\varphi}_{M,U,V}([Z]) := [Z \ U]$ for all $Z \in (E - (U \cup V))^{r-|U|}$. \diamond

Note that, in a slight abuse of notation, we have written $M/U \setminus V$ instead of $M/\{U\} \setminus \{V\}$.

3.3.11 LEMMA. $\tilde{\varphi}_{M,U,V}$ is a ring homomorphism.

Proof: Let $\tilde{\varphi}' : \mathbb{Z}[\mathcal{X}_{M/U \setminus V}] \rightarrow B_M$ be determined by $\tilde{\varphi}'([Z]) := [Z \ U]$. It is easy to see that $I_{M/U \setminus V} \subseteq \ker(\tilde{\varphi}')$. The result follows. \blacksquare

3.3.2 The universal partial field

In principle Theorem 3.3.8 gives a way to compute whether a matroid is representable: all one needs to do is to test whether $1 \in I_M$, which can be achieved by computing a Gröbner basis over the integers for I_M (see Baines and Vámos, 2003, for details). However, for practical computations the partial field (B_M, B_M^*) is somewhat unwieldy. In this subsection we rectify this problem.

3.3.12 DEFINITION. If M is a matroid, then the set of *cross ratios* of M is

$$\text{Cr}(M) := \text{Cr}(A_{M,B}). \quad \diamond$$

Note that $\text{Cr}(M)$ does not depend on the choice of B . We introduce the following subring of B_M :

$$R_M := \mathbb{Z}[\text{Cr}(M)].$$

3.3.13 DEFINITION. The *universal partial field* of M is

$$\mathbb{P}_M := (R_M, \langle \text{Cr}(M) \cup \{-1\} \rangle), \quad \diamond$$

By Theorem 2.3.34 we have that, if M is representable, then M is representable over $\mathbb{P}[\text{Cr}(A_{M,B})] = \mathbb{P}_M$ by a matrix that is scaling-equivalent to $A_{M,B}$. We give an alternative construction of this partial field. Let M be a rank- r matroid with ground set E and set of bases \mathcal{B} , let $B \in \mathcal{B}$, and let T be a spanning forest for $G(M, B)$. For every $x \in B, y \in E - B$ we introduce a symbol a_{xy} . For every $B' \in \mathcal{B}$ we introduce a symbol $i_{B'}$. We define

$$\mathcal{Y}_M := \{a_{xy} \mid x \in B, y \in E - B\} \cup \{i_{B'} \mid B' \in \mathcal{B}\}.$$

Let $\hat{A}_{M,B}$ be the $B \times (E - B)$ matrix with entries a_{xy} .

3.3.14 DEFINITION. $I_{M,B,T}$ is the ideal in $\mathbb{Z}[\mathcal{Y}_M]$ generated by the following polynomials:

- (i) $\det(\widehat{A}_{M,B}[B\Delta Z])$ if $|Z| = |B|$, $Z \notin \mathcal{B}$;
 - (ii) $\det(\widehat{A}_{M,B}[B\Delta Z])_{i_Z} - 1$ if $|Z| = |B|$, $Z \in \mathcal{B}$;
 - (iii) $a_{xy} - 1$ if $xy \in T$;
- for all $Z \in \{Z' \subseteq E \mid |Z'| = r\}$. \diamond

Now we define

$$B_{M,B,T} := \mathbb{Z}[\mathcal{Y}_M]/I_{M,B,T}$$

and

$$\mathbb{P}_{M,B,T} := (B_{M,B,T}, \langle \{i_{B'} \mid B' \in \mathcal{B}\} \cup \{-1\} \rangle).$$

Finally, $\widehat{A}_{M,B,T}$ is the matrix $\widehat{A}_{M,B}$, viewed as a matrix over $\mathbb{P}_{M,B,T}$.

The construction of $\mathbb{P}_{M,B,T}$ is essentially the same as the construction in [Fenton \(1984\)](#). As above, the difference between his construction and ours is that we ensure that the determinant corresponding to each basis is invertible. The proof of Lemma 3.3.4 can be adapted to prove the following lemma.

3.3.15 LEMMA. *Let $\mathbb{P} = (R, G)$, and let $M = M[I A]$ for some $B \times (E - B)$ \mathbb{P} -matrix A that is T -normalized for a spanning forest T of $G(A)$. Then there exists a ring homomorphism $\varphi : B_{M,B,T} \rightarrow R$ such that $\varphi(\widehat{A}_{M,B,T}) = A$.*

3.3.16 THEOREM. $B_{M,B,T} \cong R_M$ and $\mathbb{P}_{M,B,T} \cong \mathbb{P}_M$.

Proof: Let $A_{M,B,T}$ be the unique T -normalized matrix with $A_{M,B,T} \sim A_{M,B}$. By Theorem 2.3.34, $A_{M,B,T}$ is a \mathbb{P}_M -matrix. By Lemma 3.3.15 there exists a homomorphism $\varphi : B_{M,B,T} \rightarrow R_M$ such that $\varphi(\widehat{A}_{M,B,T}) = A_{M,B,T}$. By Lemma 3.3.4 there exists a homomorphism $\psi' : B_M \rightarrow B_{M,B,T}$ such that $\psi'(A_{M,B}) = \widehat{A}_{M,B,T}$. Note that also $\psi'(A_{M,B,T}) = \widehat{A}_{M,B,T}$. Let $\psi := \psi'|_{R_M}$. Now φ and ψ are both surjective and $\varphi(\psi(A_{M,B})) = A_{M,B}$, so that we have $\varphi(\psi(p)) = p$ for all $p \in \text{Cr}(M)$. Since R_M is generated by $\text{Cr}(M)$, the result follows. \blacksquare

In particular, it follows that $\mathbb{P}_{M,B,T}$ does not depend on the choice of basis or spanning tree.

3.3.17 DEFINITION. We say that a partial field \mathbb{P} is *universal* if $\mathbb{P} = \mathbb{P}_M$ for some matroid M . \diamond

The next lemma, which has a straightforward proof, gives a good reason to study universal partial fields.

3.3.18 LEMMA. *Let \mathbb{P} be a universal partial field, and let \mathcal{M} be the class of \mathbb{P} -representable matroids. Then all $M \in \mathcal{M}$ are \mathbb{P}' -representable if and only if there exists a homomorphism $\varphi : \mathbb{P} \rightarrow \mathbb{P}'$.*

We conclude this section by studying how dualizing and taking a minor affect the universal partial field. It is easy to see that $\text{Cr}(-A^T) = \text{Cr}(A)$. From this and Lemma 3.3.9 we conclude the following:

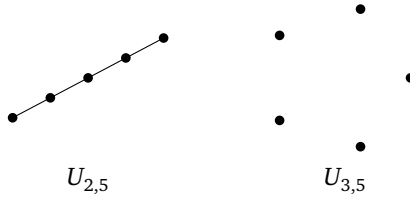


FIGURE 3.2
Some uniform matroids

3.3.19 LEMMA. $\mathbb{P}_{M^*} \cong \mathbb{P}_M$.

Recall $\tilde{\varphi}_{M,U,V}$ from Definition 3.3.10.

3.3.20 DEFINITION. Let M be a matroid, and $U, V \subseteq E(M)$ disjoint ordered subsets such that U is independent and V coindependent. Then $\varphi_{M,U,V}$ is the restriction of $\tilde{\varphi}_{M,U,V}$ to $\mathbb{Z}[\text{Cr}(M/U \setminus V)]$. \diamond

The proof of the following lemma is straightforward.

3.3.21 LEMMA. $\varphi_{M,U,V}$ is a ring homomorphism $R_{M/U \setminus V} \rightarrow R_M$.

Note that, because of the restriction to cross ratios, $\varphi_{M,U,V}$ does not depend on the particular ordering of U and V . $\varphi_{M,U,V}$ is the *canonical homomorphism* $R_{M/U \setminus V} \rightarrow R_M$ and induces a partial-field homomorphism $\mathbb{P}_{M/U \setminus V} \rightarrow \mathbb{P}_M$. Again, the proof of the following lemma is straightforward.

3.3.22 LEMMA. Let M be a matroid with ground set E and set of bases \mathcal{B} , and $U, V \subseteq E$ disjoint subsets such that U is independent and V coindependent. Let $B \in \mathcal{B}$ be such that $U \subseteq B$, and let T be a spanning forest for $G(M, B)$ extending a spanning forest T' for $G(M/U \setminus V, B \setminus U)$. Then

$$\varphi_{M,U,V}(A_{M/U \setminus V, B \setminus U, T'}) = A_{M,B,T} - U - V.$$

3.3.3 Examples

In this section we prove that several partial fields from Section 2.5 are universal. The following theorem and its proof appear, in essence, also in Fenton (1984).

3.3.23 DEFINITION. The rank- r uniform matroid on n elements, denoted $U_{r,n}$, is the matroid with ground set $E = \{1, \dots, n\}$ and set of bases $\mathcal{B} = \{X \subseteq 2^E \mid |X| = r\}$. \diamond

Geometric representations of some uniform matroids are shown in Figure 3.2.

3.3.24 THEOREM. $\mathbb{P}_{U_{2,k+3}} \cong \mathbb{U}_k$.

Proof: Let $B := \{1, 2\}$, and $T := \{23\} \cup \{1j \mid j \in \{3, \dots, k+3\}\}$. Then

$$\widehat{A}_{U_{2,k+3},B,T} = \begin{matrix} & \begin{matrix} 3 & 4 & \cdots & k+3 \end{matrix} \\ \begin{matrix} 1 \\ 2 \end{matrix} & \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & \alpha_1 & \cdots & \alpha_k \end{bmatrix} \end{matrix}$$

where $\alpha_i := a_{2,i+3}$. Let $\alpha_0 := 1$. For $3 \leq i < j \leq k+3$ we have $\{i, j\} \in \mathcal{B}$. Hence $\det(A_{U_{2,k+3},B,T}[\{1, 2\}, \{i, j\}]) = \alpha_{j-3} - \alpha_{i-3}$ is invertible. The result follows. \blacksquare

It follows from Lemma 3.3.19 that $\mathbb{P}_{U_{k+1,k+3}} \cong \mathbb{U}_k$. In particular, $\mathbb{P}_{U_{2,4}} \cong \mathbb{U}_1$ and $\mathbb{P}_{U_{2,5}} \cong \mathbb{P}_{U_{3,5}} \cong \mathbb{U}_2$.

Next we describe, for each q , a rank-three matroid on $3q+1$ elements for which the universal partial field is $\text{GF}(q)$. For q a prime power, let Q_q be the rank-3 matroid consisting of three distinct $q+1$ -point lines $L_1, L_2, L_3 \subset \text{PG}(2, q)$ such that $L_1 \cap L_2 \cap L_3 = \emptyset$. Then $Q_q = Q_3(\text{GF}(q)^*)$, the rank-3 Dowling geometry for the multiplicative group of $\text{GF}(q)$. For instance, $Q_2 \cong M(K_4)$. Now Q_q^+ is the matroid obtained from Q_q by adding a point $e \in \text{PG}(2, q) - (L_1 \cup L_2 \cup L_3)$. For instance, $Q_2^+ \cong F_7$.

3.3.25 THEOREM. $\mathbb{P}_{Q_q^+} \cong \text{GF}(q)$.

Proof: Let $\{e_1\} = L_2 \cap L_3$, $\{e_2\} = L_1 \cap L_3$, and $\{e_3\} = L_1 \cap L_2$. Then $B := \{e_1, e_2, e_3\}$ is a basis of Q_q^+ . If α is a generator of $\text{GF}(q)^*$ then a B -representation of Q_q^+ is the following:

$$A = \begin{matrix} & \begin{matrix} e & a_0 & a_1 & & a_{q-2} & b_0 & & b_{q-2} & c_0 & & c_{q-2} \end{matrix} \\ \begin{matrix} e_1 \\ e_2 \\ e_3 \end{matrix} & \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 1 & \cdots & 1 & 1 & \cdots & 1 \\ 1 & 1 & 1 & & 1 & 0 & & 0 & 1 & & \alpha^{q-2} \\ 1 & 1 & \alpha & \cdots & \alpha^{q-2} & 1 & \cdots & \alpha^{q-2} & 0 & \cdots & 0 \end{bmatrix} \end{matrix}.$$

Let T be the spanning tree of $G(A)$ with edges e_1x , e_2x , e_3x , and e_2a_i , e_1b_i , e_1c_i for all $i \in \{0, \dots, q-2\}$. Then

$$\widehat{A}_{Q_q^+,B,T} = \begin{matrix} & \begin{matrix} e & a_0 & a_1 & & a_{q-2} & b_0 & & b_{q-2} & c_0 & & c_{q-2} \end{matrix} \\ \begin{matrix} e_1 \\ e_2 \\ e_3 \end{matrix} & \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 1 & \cdots & 1 & 1 & \cdots & 1 \\ 1 & 1 & 1 & & 1 & 0 & & 0 & z_0 & & z_{q-2} \\ 1 & x_0 & x_1 & \cdots & x_{q-2} & y_0 & \cdots & y_{q-2} & 0 & \cdots & 0 \end{bmatrix} \end{matrix}.$$

3.3.25.I CLAIM. $x_0 = y_0 = z_0 = 1$.

Proof: $\det(A[B - e_1, \{e, a_0\}]) = 0$, so $\det(\widehat{A}_{Q_q^+,B,T}[B - e_1, \{e, a_0\}]) = x_0 - 1 = 0$. Similarly $y_0 = 1$ and $z_0 = 1$. \square

3.3.25.2 CLAIM. If $\alpha^k = -1$ then $x_k = y_k = z_k = -1$.

Proof: $\det(A[B, \{a_0, b_0, c_k\}]) = \det(\alpha^k + 1) = 0$, so $\det(\widehat{A}_{Q_q^+,B,T}[B, \{a_0, b_0, c_k\}]) = z_k + 1 = 0$ and $z_k = -1$. Similarly $x_k = -1$ and $y_k = -1$. \square

3.3.25.3 CLAIM. $x_l = y_l = z_l$ for all l .

Proof: Let k be such that $x_k = -1$. Then $\det(A[B, \{a_k, b_l, c_l\}]) = 0$, so we have $\det(\widehat{A}_{Q_q^+, B, T}[B, \{a_k, b_l, c_l\}]) = y_l - z_l = 0$. Therefore $y_l = z_l$. Similarly $y_l = x_l$. \square

By replacing a_k by a_0 in the previous subproof we obtain

3.3.25.4 CLAIM. If $\alpha^m = -\alpha^l$ then $x_m = -x_l$, for all k, l .

Now we establish the multiplicative structure of $\text{GF}(q)$:

3.3.25.5 CLAIM. If $\alpha^k \alpha^l = \alpha^m$ then $x_k x_l = x_m$.

Proof: Let n be such that $\alpha^m = -\alpha^n$. Then $\det(A[B, \{a_k, b_n, c_l\}]) = \alpha^k \alpha^l + \alpha^n = 0$, so $\det(\widehat{A}_{Q_q^+, B, T}[B, \{a_k, b_n, c_l\}]) = x_k x_l + x_n = 0$, so $x_k x_l = x_m$. \square

Finally we establish the additive structure.

3.3.25.6 CLAIM. If $\alpha^k = \alpha^l + 1$ then $x_k = x_l + 1$.

Proof: Let m be such that $\alpha^m = -\alpha^l$. Then $\det(A[B, \{e, a_k, b_m\}]) = \alpha^k + \alpha^m - 1 = 0$, so $\det(\widehat{A}_{Q_q^+, B, T}[B, \{e, a_k, b_m\}]) = x_k + x_m - 1 = 0$, so $x_k = x_l + 1$. \square

This completes the proof. \blacksquare

We made no attempt to find a smallest matroid with $\text{GF}(q)$ as universal partial field. For q prime it is known that fewer elements suffice: one may restrict the line L_3 to e_2, e_3 , and the point collinear with e_1 and e . [Brylawski \(1982\)](#) showed that yet more points may be omitted. [Lazarson \(1958\)](#) described, for primes p , a rank- $(p+1)$ matroid with characteristic set $\{p\}$.

Another result is the following:

3.3.26 THEOREM. $\mathbb{P}_{Q_q} \cong \mathbb{D}\text{GF}(q)$.

The proof is similar to that of Theorem 3.3.25, and is therefore omitted. Also without proof we claim the following:

3.3.27 THEOREM. Let F_7^- , B_{11} , $M(K_4)^+$, F_7^+ , P_8 , and M_{8591} be the matroids depicted in Figure 3.3. Then we have the following:

- (i) $\mathbb{P}_{F_7^-} \cong \mathbb{P}_{P_8} \cong \mathbb{D}$;
- (ii) $\mathbb{P}_{B_{11}} \cong \mathbb{G}$;
- (iii) $\mathbb{P}_{M(K_4)^+} \cong \mathbb{K}_2$;
- (iv) $\mathbb{P}_{F_7^+} \cong \mathbb{U}_1^{(2)}$;
- (v) $\mathbb{P}_{M_{8591}^{\gamma\Delta}} \cong \mathbb{P}_4$.

The matroid P_8 can be described as follows: take a cube, and rotate one of its faces over 45 degrees. The matroid P_8 has as elements the eight vertices of the cube, it has rank four, and its circuits have size four or five. The ten four-element circuits are precisely the ten four-point planes in the twisted cube.

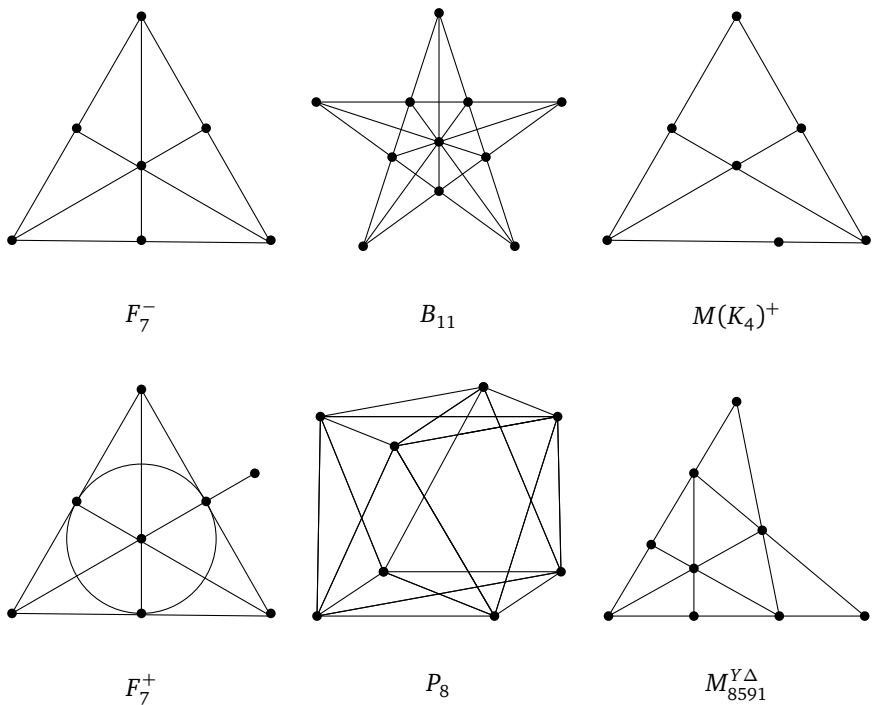


FIGURE 3.3
Some matroids

\mathbb{P}_M	\mathbb{U}_k	$\text{GF}(q)$	$\mathbb{D}\text{GF}(q)$	\mathbb{D}	\mathbb{D}
M	$U_{2,k+3}$	Q_q^+	Q_q	F_7^-	P_8
\mathbb{P}_M	\mathbb{S}	\mathbb{G}	\mathbb{K}_2	$\mathbb{U}_1^{(2)}$	\mathbb{P}_4
M	$\text{AG}(2,3)$	B_{11}	$M(K_4)^+$	F_7^+	$M_{8591}^{Y\Delta}$

TABLE 3.2
Some universal partial fields.

We have collected the results of this section in Table 3.2.

The matroid B_{11} is known as the *Betsy Ross* matroid. The matroid $M_{8591}^{Y\Delta}$ was obtained from the 8591st matroid in Mayhew and Royle's (2008) catalog of small matroids through a $Y - \Delta$ exchange.

3.4 Open problems

3.4.1 PROBLEM. What is the relation between $\mathcal{F}(\mathbb{P})$ and $\mathcal{F}(\mathbb{DP})$? ◇

It is clear that $\{q \in \mathcal{F}(\mathbb{DP}) \mid \varphi(q) = p\} \supseteq \{\bar{p}, 1 - \overline{1 - p}, \frac{1}{1 - 1 - p^{-1}}\}$. It follows from $\mathbb{D} \text{GF}(4) = \mathbb{W}$ that this inclusion can be strict. The following special case may be slightly easier:

3.4.2 PROBLEM. What is $\mathcal{F}(\mathbb{D} \text{GF}(q))$? ◇

Perhaps all possible “surplus” fundamental elements come from sub-partial fields isomorphic to \mathbb{S} .

3.4.3 PROBLEM. What is $\mathbb{P}_{\text{AG}(n,q)}$? ◇

We have seen that $\mathbb{P}_{\text{AG}(2,3)} \cong \mathbb{S}$. As shown in Table 3.2, several known partial fields are universal. Notable omissions in that table are the Hydra- k partial fields for $k \geq 3$. We do not know if these are universal. The problem here is that many partial fields have exactly k homomorphisms to $\text{GF}(5)$, and all examples that we tried from Mayhew and Royle's (2008) catalog of small matroids turned out to have slightly different universal partial fields.

In Section 2.4.3 we already mentioned the *segment-cosegment exchange* introduced by Oxley et al. (2000). The k -uniform partial fields are important in this context. It should not be too hard to show the following:

3.4.4 CONJECTURE. If M' is obtained from M through a segment-cosegment exchange, then $\mathbb{P}_{M'} \cong \mathbb{P}_M$.

The following conjecture links fundamental elements and universal partial fields.

3.4.5 CONJECTURE. If \mathbb{P}_N has finitely many fundamental elements, then all \mathbb{P}_N -representations of N are equivalent.

This conjecture cannot be strengthened by much: the homomorphism $\varphi : \mathbb{U}_1^{(2)} \rightarrow \mathbb{U}_1^{(2)}$ determined by $\alpha \mapsto \alpha^2$ is not an automorphism.

Geelen, Gerards, and Whittle are working on a project that aims to show that the matroids representable over a fixed finite field are well-quasi-ordered. If true, this immediately implies that the set $\{\mathbb{P} \mid \mathbb{P} \text{ universal}, \exists \varphi : \mathbb{P} \rightarrow \mathbb{F}\}$ is well-quasi-ordered for every finite field \mathbb{F} , where the order is induced by the homomorphisms: $\mathbb{P}' \preceq \mathbb{P}$ if and only if there is a homomorphism $\mathbb{P}' \rightarrow \mathbb{P}$.

3.4.6 QUESTION. Let \mathbb{F} be a finite field. Is there a direct proof that

$$\{\mathbb{P} \mid \mathbb{P} \text{ universal}, \exists \varphi : \mathbb{P} \rightarrow \mathbb{F}\}$$

is well-quasi-ordered? ◇

The question might become easier if we drop the condition that $\mathbb{P} \cong \mathbb{P}_M$, thus enlarging the set under consideration and reducing the question to an algebraic one.

Indeed, not all partial fields are universal. For instance, it is not hard to construct partial fields with homomorphisms to $\text{GF}(3)$ different from the ones in Theorem 6.3.1.

3.4.7 PROBLEM. What distinguishes universal partial fields from partial fields in general? ◇

In other words, what is the structure of the ideal I_M ? Possibly Theorem 2.7.24 can shed some light on this. The final problem ties in with Section 2.7. Theorem 2.7.24 can also be used as a starting point for the following research project:

3.4.8 PROBLEM. Develop a theory of universal skew partial fields. ◇



Lifts of matroid representations

THE direct product of two partial fields is a powerful tool. In Section 3.1.1 we have seen that it can be used for a concise proof of Tutte’s characterization of the regular matroids. Whittle (1995, 1997) proved several similar results. We already mentioned one of them in Section 1.4, which we repeat here:

4.A THEOREM (Whittle, 1997). *Let M be a matroid. The following are equivalent:*

- (i) M is representable over both $\text{GF}(3)$ and $\text{GF}(5)$;
- (ii) M is representable by a \mathbb{D} -matrix;
- (iii) M is representable over every field that does not have characteristic 2.

Here $\mathbb{D} = \left(\mathbb{Z}[\frac{1}{2}], \langle -1, 2 \rangle\right)$ is the dyadic partial field, which we introduced in Section 2.5.

We cannot use the techniques from Section 3.1.1 here, because the partial field $\text{GF}(3) \times \text{GF}(5)$ is finite, but the dyadic partial field has an infinite number of elements. Hence the two cannot be isomorphic.

Still, there is a homomorphism $\varphi : \mathbb{D} \rightarrow \text{GF}(3) \times \text{GF}(5)$, determined by $\varphi(2) = (-1, 2)$. To prove the implication (i) \Rightarrow (ii) we will try to find a preimage for every $\text{GF}(3) \times \text{GF}(5)$ -matrix. The main result of this chapter gives sufficient conditions under which such a preimage can indeed be found:

4.B THEOREM (Lift Theorem, simplified version). *Let $\mathbb{P}, \widehat{\mathbb{P}}$ be two partial fields, let A be a \mathbb{P} -matrix, and let $\varphi : \widehat{\mathbb{P}} \rightarrow \mathbb{P}$ be a homomorphism such that the restriction of φ to the fundamental elements, $\varphi|_{\mathcal{F}(\widehat{\mathbb{P}})} : \mathcal{F}(\widehat{\mathbb{P}}) \rightarrow \mathcal{F}(\mathbb{P})$, is a bijection. Then exactly one of the following is true:*

- (i) *There is a $\widehat{\mathbb{P}}$ -matrix \widehat{A} such that $\varphi(\widehat{A}) \sim A$;*
- (ii) *A has a minor D such that*
 - a) *There is no $\widehat{\mathbb{P}}$ -matrix \widehat{D} such that $\varphi(\widehat{D}) = D$;*

b) D or D^T equals

$$\begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix} \text{ or } \begin{bmatrix} 1 & 1 & 1 \\ 1 & p & q \end{bmatrix} \quad (4.1)$$

for some distinct $p, q \in \mathcal{F}(\mathbb{P}) - \{0, 1\}$.

The use of this result is best illustrated with an example. Hence we will first use it to prove Theorem 4.A, and defer the proof of Theorem 4.B to the next section.

Proof of Theorem 4.A: The implication (ii) \Rightarrow (iii) follows from Lemma 2.5.5 and Proposition 2.4.5, and (i) is a special case of (iii). Hence it suffices to prove (i) \Rightarrow (ii). We will apply Theorem 4.B with partial fields $\mathbb{P} = \text{GF}(3) \times \text{GF}(5)$ and $\widehat{\mathbb{P}} = \mathbb{D}$. From Lemma 2.5.6 and Proposition 3.1.2 we find that

$$\begin{aligned} \mathcal{F}(\mathbb{D}) &= \{ \quad 0, \quad 1, \quad 2, \quad 1/2, \quad -1 \}, \\ \mathcal{F}(\text{GF}(3) \times \text{GF}(5)) &= \{ (0,0), (1,1), (-1,2), (-1,3), (-1,-1) \}. \end{aligned}$$

Let $\varphi : \mathbb{D} \rightarrow \text{GF}(3) \times \text{GF}(5)$ be the partial-field homomorphism determined by $\varphi(2) = (-1, 2)$. It is easily checked that $\varphi(\mathcal{F}(\mathbb{D})) = \mathcal{F}(\text{GF}(3) \times \text{GF}(5))$, so $\varphi|_{\mathcal{F}(\mathbb{D})}$ is a bijection.

Let D_1 be the following matrix with entries in $\text{GF}(3) \times \text{GF}(5)$:

$$D_1 := \begin{bmatrix} (0,0) & (1,1) & (1,1) & (1,1) \\ (1,1) & (0,0) & (1,1) & (1,1) \\ (1,1) & (1,1) & (0,0) & (1,1) \end{bmatrix}.$$

It is easily checked that D_1 is a $\text{GF}(3) \times \text{GF}(5)$ -matrix.

4.A.1 CLAIM. *There is a \mathbb{D} -matrix \widehat{D}_1 such that $\varphi(\widehat{D}_1) = D_1$.*

Proof: Let \widehat{D}_1 be the following matrix with entries in \mathbb{D} :

$$\widehat{D}_1 := \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}.$$

Clearly $\varphi(\widehat{D}_1) = D_1$. It is easily checked that $\det(\widehat{D}') \in \mathbb{D}$ for every square submatrix \widehat{D}' of \widehat{D}_1 . The claim follows. \square

Let $p, q \in \mathcal{F}(\text{GF}(3) \times \text{GF}(5)) - \{(0,0), (1,1)\}$, and let D_2 be the following matrix with entries in the partial field $\text{GF}(3) \times \text{GF}(5)$:

$$D_2 := \begin{matrix} & \overset{3}{(1,1)} & \overset{4}{(1,1)} & \overset{5}{(1,1)} \\ \overset{1}{(1,1)} & & & \\ \overset{2}{(1,1)} & & p & q \end{matrix}.$$

4.A.2 CLAIM. *D_2 is a $\text{GF}(3) \times \text{GF}(5)$ -matrix if and only if $p = q$.*

Proof: Note that $\det(D_2[\{1, 2, 4, 5\}]) = q - p = (0, r)$ for some $r \in \text{GF}(5)$. But $(0, r) \in \text{GF}(3) \times \text{GF}(5)$ if and only if $r = 0$, by Proposition 3.1.2. The claim follows. \square

Let M be a matroid that is representable over both $\text{GF}(3)$ and $\text{GF}(5)$. By Proposition 3.1.5 there is a $\text{GF}(3) \times \text{GF}(5)$ -matrix A such that $M = M[I A]$. From Claims 4.A.1 and 4.A.2 it follows that A has no minor D satisfying the conditions in 4.B(ii). But then Theorem 4.B implies that there exists a \mathbb{D} -matrix \hat{A} such that $\varphi(\hat{A}) \sim A$. By Proposition 2.4.5 and Lemma 2.4.2(iii), $M = M[I \hat{A}]$. Hence M is \mathbb{D} -representable, and the theorem follows. \blacksquare

Before embarking on the proof of the Lift Theorem we make a few remarks. The matrices (4.1) crop up regularly in matroid theory. Suppose

$$D = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}.$$

Then D is a \mathbb{P} -matrix if and only if $1 + 1 \in \mathbb{P}$. Then $M[I D] = F_7$, the Fano matroid, if $1 + 1 = 0 \in \mathbb{P}$, and $M[I D] = F_7^-$, the Non-Fano matroid, otherwise. In the former case $\chi(\mathbb{P}) = \{2\}$, i.e. all fields \mathbb{F} such that there is a homomorphism $\mathbb{P} \rightarrow \mathbb{F}$ have characteristic 2. In the latter case $2 \notin \chi(\mathbb{P})$. Next, suppose

$$D = \begin{bmatrix} 1 & 1 & 1 \\ 1 & p & q \end{bmatrix},$$

for distinct $p, q \in \mathcal{F}(\mathbb{P}) - \{0, 1\}$. Then $M[I D] = U_{2,5}$, the uniform rank-two matroid on five elements. In Chapter 6 we will prove the theorem, by Semple and Whittle (1996a), that a representable matroid with no $U_{2,5}$ - and no $U_{3,5}$ -minor is also representable over at least one of $\text{GF}(2)$ and $\text{GF}(3)$.

Tutte's original proof of Theorem 1.2.10 used a deep result known as Tutte's Homotopy Theorem (Tutte, 1958). The Lift Theorem is a descendant of that result, and in fact it is likely that the Lift Theorem can be proven from Tutte's Homotopy Theorem, using the chain groups over a partial field that were defined in Section 2.7. The idea underlying Tutte's proof, and all known excluded-minor characterizations for classes of representable matroids ((Tutte, 1965; Seymour, 1979; Bixby, 1979; Geelen et al., 2000; Hall, Mayhew, and Van Zwam, 2009); see also Chapter 7), is the same as that underlying the proof of the Lift Theorem: construct a candidate matrix with entries in $\widehat{\mathbb{P}}$, show that it is the only possible candidate, and analyse its structure to identify the minimal obstructions to being a $\widehat{\mathbb{P}}$ -matrix. In the case of the Lift Theorem it is not difficult to prove uniqueness of the candidate representation; in Chapter 7 this requires more effort. The analysis of the obstructions essentially follows Gerards' (1989) proof of Theorem 1.2.10.

The result we will prove is more general than Theorem 4.B. Unfortunately this introduces a few extra technicalities. For all applications in Section 4.2 the statement of Theorem 4.B would suffice. The more general version is required for the algebraic construction from Section 4.3.

This chapter is based on joint work with Rudi Pendavingh (Pendavingh and Van Zwam, 2009a). The proof presented here differs from the proof in that paper,

though all changes are cosmetic, not conceptual. The current presentation is closer to Gerards' (1989) proof, and was chosen because it exhibits many parallels with the results in Chapter 7.

4.1 The theorem and its proof

Before stating the generalization of Theorem 4.B that we will prove, we need a few definitions. Our starting point is a lifting function.

- 4.1.1 DEFINITION. Let $\mathbb{P}, \widehat{\mathbb{P}}$ be partial fields, let A be a \mathbb{P} -matrix, and let $\varphi : \widehat{\mathbb{P}} \rightarrow \mathbb{P}$ be a partial-field homomorphism. A *lifting function* for φ is a function $\uparrow : \text{Cr}(A) \rightarrow \widehat{\mathbb{P}}$ such that for all $p, q \in \text{Cr}(A)$:
- (i) $\varphi(p^\uparrow) = p$;
 - (ii) if $p + q = 1$ then $p^\uparrow + q^\uparrow = 1$;
 - (iii) if $p \cdot q = 1$ then $p^\uparrow \cdot q^\uparrow = 1$. ◇

Hence a lifting function maps $\text{Asc}\{p\}$ to $\text{Asc}\{p^\uparrow\}$ for all $p \in \text{Cr}(A)$. Observe that, if $\varphi|_{\mathcal{F}(\widehat{\mathbb{P}})}$ is a bijection between the fundamental elements, then $(\varphi|_{\mathcal{F}(\widehat{\mathbb{P}})})^{-1}$ determines a lifting function. We will use the lifting function to create a preimage of a \mathbb{P} -matrix A , as follows:

- 4.1.2 DEFINITION. Let $\mathbb{P}, \widehat{\mathbb{P}}$ be partial fields, let A be an $X \times Y$ \mathbb{P} -matrix, let $\varphi : \widehat{\mathbb{P}} \rightarrow \mathbb{P}$ be a homomorphism, and let $\uparrow : \text{Cr}(A) \rightarrow \widehat{\mathbb{P}}$ be a lifting function for φ . An $X \times Y$ matrix \widehat{A} is a *local \uparrow -lift* of A if
- (i) $\varphi(\widehat{A}) \sim A$;
 - (ii) \widehat{A} is an $X \times Y$ $\widehat{\mathbb{P}}$ -matrix;
 - (iii) for every induced cycle C of $G(A)$ we have

$$\sigma_A(C)^\uparrow = \sigma_{\widehat{A}}(C). \quad \diamond$$

If \widehat{A} is a $\widehat{\mathbb{P}}$ -matrix, then so is \widehat{A}^{xy} . If $\varphi(\widehat{A}) \sim A$ then $\varphi(\widehat{A}^{xy}) \sim A^{xy}$. However, it is not guaranteed that (iii) is preserved after pivoting. The point is that there may be more than one $\widehat{p} \in \mathcal{F}(\widehat{\mathbb{P}})$ such that $\varphi(\widehat{p}) = p \in \mathcal{F}(\mathbb{P})$. Therefore we have to define a stronger notion of lift, which commutes with pivoting.

- 4.1.3 DEFINITION. Let $\mathbb{P}, \widehat{\mathbb{P}}$ be two partial fields, let $\varphi : \widehat{\mathbb{P}} \rightarrow \mathbb{P}$ be a homomorphism, let A be a \mathbb{P} -matrix, and let $\uparrow : \text{Cr}(A) \rightarrow \widehat{\mathbb{P}}$ be a lifting function for φ . A matrix \widehat{A} is a *global \uparrow -lift* of A if \widehat{A} is a local \uparrow -lift of A , and \widehat{A}' is a local \uparrow -lift of $\varphi(\widehat{A}')$ for all $\widehat{A}' \approx \widehat{A}$. ◇

We now have all ingredients to state the main theorem.

- 4.1.4 THEOREM (Lift Theorem). Let $\mathbb{P}, \widehat{\mathbb{P}}$ be two partial fields, let A be a \mathbb{P} -matrix, let $\varphi : \widehat{\mathbb{P}} \rightarrow \mathbb{P}$ be a homomorphism, and let $\uparrow : \text{Cr}(A) \rightarrow \widehat{\mathbb{P}}$ be a lifting function for φ . Then exactly one of the following is true:
- (i) A has a global \uparrow -lift.
 - (ii) A has a minor D such that
 - a) D has no local \uparrow -lift;

b) D or D^T equals

$$\begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix} \text{ or } \begin{bmatrix} 1 & 1 & 1 \\ 1 & p & q \end{bmatrix} \quad (4.2)$$

for some distinct $p, q \in \mathcal{F}(\mathbb{P}) - \{0, 1\}$.

Note that the distinction between local and global \uparrow -lifts is only necessary for the proof of this theorem, not for the proof of Theorem 4.B. The following lemma links local and global lifts. Its proof is rather technical, and is deferred to Section 4.1.3.

4.1.5 LEMMA. Suppose that for all $A' \approx A$, A' has a local \uparrow -lift. Then A has a global \uparrow -lift.

If we only want to prove Theorem 4.B then this lemma has a straightforward proof. Since the restriction of φ to $\mathcal{F}(\widehat{\mathbb{P}})$ is now a bijection between $\mathcal{F}(\widehat{\mathbb{P}})$ and $\mathcal{F}(\mathbb{P})$, there is a unique $\widehat{p} \in \mathcal{F}(\widehat{\mathbb{P}})$ such that $\varphi(\widehat{p}) = \sigma_{A'}(C)$, for all $A' \approx A$ and induced cycles C of $G(A')$. Lemma 4.1.5 then follows immediately from Proposition 2.3.16 and the fact that $\varphi(A^{xy}) = (\varphi(A))^{xy}$.

We will usually apply the following corollary of Theorem 4.1.4, which has a more algebraic flavour:

4.1.6 COROLLARY. Let $\mathbb{P}, \widehat{\mathbb{P}}, \varphi, \uparrow, A$ be as in Theorem 4.1.4. Suppose that

- (i) If $1 + 1 = 0$ in \mathbb{P} then $1 + 1 = 0$ in $\widehat{\mathbb{P}}$;
 - (ii) If $1 + 1 \in \mathbb{P} - \{0\}$, then $1 + 1 \in \widehat{\mathbb{P}} - \{0\}$;
 - (iii) For all $p, q, r \in \text{Cr}(A)$ such that $pqr = 1$, we have $p^\uparrow q^\uparrow r^\uparrow = 1$.
- Then a matroid is \mathbb{P} -representable if and only if it is $\widehat{\mathbb{P}}$ -representable.

Proof: Assume that \uparrow is as in the corollary. Since there is a nontrivial homomorphism $\varphi : \widehat{\mathbb{P}} \rightarrow \mathbb{P}$, every matroid that is $\widehat{\mathbb{P}}$ -representable is also \mathbb{P} -representable. To prove the other implication it suffices to show that A has a global \uparrow -lift. Suppose that this is false. By Theorem 4.1.4, A must have a minor D as in (4.2) that does not have a local \uparrow -lift. Suppose there are $p', q' \in \text{Cr}(A) - \{0, 1\}$ such that the following \mathbb{P} -matrix has no local \uparrow -lift:

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & p' & q' \end{bmatrix}.$$

This matrix has a local \uparrow -lift if and only if

$$\left(\frac{p'}{q'} \right)^\uparrow = \frac{(p')^\uparrow}{(q')^\uparrow}. \quad (4.3)$$

Pick $p := p'$, $q := (q')^{-1}$, and $r := q'/p'$. Then (4.3) holds if and only if $p^\uparrow q^\uparrow r^\uparrow = 1$, which follows from (iii). It follows that A has a minor

$$D = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}$$

which has no local \uparrow -lift. Note that D has a cycle with signature -1 (obtained by deleting the last column). Hence $1 - (-1)^\uparrow$ must be defined in \mathbb{P} , and hence also in $\widehat{\mathbb{P}}$. Since $\varphi(1) + \varphi((-1)^\uparrow) = 0$, we have $(-1)^\uparrow = -1$. Moreover, (i) and (ii) imply that $1 + 1 = 0$ in \mathbb{P} if and only if $1 + 1 = 0$ in $\widehat{\mathbb{P}}$, since $\varphi(1) = 1$. Let \widehat{D} be a $\widehat{\mathbb{P}}$ -matrix such that $\widehat{D}_{xy} = 1$ if $D_{xy} = 1$ and $\widehat{D}_{xy} = 0$ if $D_{xy} = 0$. It is easily checked that all conditions of Definition 4.1.2 are met, so \widehat{D} is a local \uparrow -lift of D , a contradiction. ■

4.1.1 Deletion pairs and incriminating sets

For all results in this section we assume that \mathbb{P} and $\widehat{\mathbb{P}}$ are partial fields, A is an $X \times Y$ \mathbb{P} -matrix for disjoint sets X, Y , $\varphi : \widehat{\mathbb{P}} \rightarrow \mathbb{P}$ is a partial-field homomorphism, and $\uparrow : \text{Cr}(A) \rightarrow \widehat{\mathbb{P}}$ is a lifting function.

4.1.7 DEFINITION. A weak deletion pair of A is a set $\{u, v\} \subseteq Y$ such that $A - u$, $A - v$, and $A - \{u, v\}$ are all connected. ◇

A weak contraction pair is a weak deletion pair of A^T . It is not hard to find a weak deletion pair or a weak contraction pair:

4.1.8 LEMMA (Gerards, 1989, Lemma 1). If $G(A)$ is connected, and neither a path nor a cycle, then A has a weak deletion pair or a weak contraction pair.

Proof: $G(A)$ has a vertex w of degree at least three. There is a spanning tree of $G(A)$ containing all edges incident with w . This tree has at least three leaves, so either X or Y contains at least two leaves, say u and v . Clearly $G(A - u)$, $G(A - v)$, and $G(A - \{u, v\})$ are connected. ■

In the remainder of this section, $u, v \subseteq Y$ will be a weak deletion pair of A .

Weak deletion pairs are useful in arguments involving matrices for which every proper minor has a lift. The following theorem illustrates this.

4.1.9 THEOREM. If $A - u$ has a local lift \widehat{A}_1 , and $A - v$ has a local lift \widehat{A}_2 , then there is an $X \times Y$ matrix \widehat{A} with entries in $\widehat{\mathbb{P}}$ such that

(i) $\widehat{A} - u \sim \widehat{A}_1$;

(ii) $\widehat{A} - v \sim \widehat{A}_2$.

Moreover, \widehat{A} is unique up to scaling of rows and columns.

The proof is based on the following two lemmas, the first of which will also be of use in Chapter 7:

4.1.10 LEMMA. Let D, D' be $X \times Y$ matrices with entries in a partial field \mathbb{P} . Let $u, v \in Y$ be such that

(i) $D - u \sim D' - u$ and $D - v \sim D' - v$;

(ii) $D - \{u, v\}$ is connected.

Then $D \sim D'$.

Proof: If one of $D[X, u]$ and $D[X, v]$ is an all-zero column then the result is trivially true, so we assume this is not the case. Since $D - \{u, v\}$ is connected, also

$G(D - \{u, v\})$ is connected, by Lemma 2.4.17. Now let T' be a spanning tree for $G(D - \{u, v\})$, and let $T := T' \cup \{xu, x'v\}$ for some $x, x' \in X$ with $D_{xu} \neq 0$, $D_{x'v} \neq 0$. Then T is a spanning tree for $G(D)$. Assume, without loss of generality, that D and D' are T -normalized. Then $D - u$ and $D' - u$ are $(T - xu)$ -normalized, and hence, by Lemma 2.3.12, $D - u = D' - u$. Likewise $D - v = D' - v$. But then $D = D'$, and the result follows. ■

If a local \uparrow -lift exists, it is unique up to scaling:

4.1.II LEMMA. Suppose \hat{A}_1, \hat{A}_2 are local \uparrow -lifts of A . Then $\hat{A}_1 \sim \hat{A}_2$.

Proof: Suppose the lemma is false and let A, \hat{A}_1, \hat{A}_2 form a counterexample. Let T be a spanning forest of $G(A)$ and rescale \hat{A}_1, \hat{A}_2 so that they are T -normalized. Let H be the subgraph of $G(A)$ consisting of all edges $x'y'$ such that $(\hat{A}_1)_{x'y'} = (\hat{A}_2)_{x'y'}$. Let xy be an edge not in H such that the minimum length of an $x - y$ path P in H is minimal. Then $C := P \cup xy$ is an induced cycle of $G(A)$. We have

$$\sigma_A(C)^\uparrow = \sigma_{\hat{A}_1}(C) = \sigma_{\hat{A}_2}(C).$$

But this is only possible if $(\hat{A}_1)_{xy} = (\hat{A}_2)_{xy}$, a contradiction. ■

It is straightforward to turn this proof into an algorithm that constructs a matrix \hat{A} satisfying Definition 4.1.2(i) and (iii) for a subset of the cycles such that, if A has a local \uparrow -lift, \hat{A} is one.

Proof of Theorem 4.1.9: Suppose \hat{A}_1, \hat{A}_2 are as in the theorem. Both $\hat{A}_1 - v$ and $\hat{A}_2 - u$ are local lifts of $A - \{u, v\}$. By Lemma 4.1.11, $\hat{A}_1 - v \sim \hat{A}_2 - u$. Without loss of generality we assume $\hat{A}_1 - v = \hat{A}_2 - u$. Now let \hat{A} be the matrix obtained from \hat{A}_2 by appending column $\hat{A}_1[X, v]$. Then \hat{A} satisfies all properties of the theorem. Uniqueness follows from Lemma 4.1.10. ■

For most of the time we will apply Theorem 4.1.9 to matrices that have no local \uparrow -lift. If a lift candidate is not a local lift, then it must have one of two problems, described by the next definition.

4.1.I2 DEFINITION. Let \hat{A} be an $X \times Y$ matrix with entries in $\widehat{\mathbb{P}}$ such that $\varphi(\hat{A}) = A$, where X, Y are disjoint sets. A set $Z \subseteq X \cup Y$ *incriminates* the pair (A, \hat{A}) if one of the following holds:

- (i) $\det(\hat{A}[Z]) \notin \widehat{\mathbb{P}}$;
- (ii) $G(\hat{A}[Z])$ is a cycle C , but $\sigma_A(C)^\uparrow \neq \sigma_{\hat{A}}(C)$. ◇

The proof of the following lemma is obvious, and therefore omitted.

4.1.I3 LEMMA. Let \hat{A} be an $X \times Y$ matrix with entries in $\widehat{\mathbb{P}}$ such that $\varphi(\hat{A}) = A$. Exactly one of the following statements is true:

- (i) \hat{A} is a local \uparrow -lift of A ;
- (ii) Some $Z \subseteq X \cup Y$ incriminates (A, \hat{A}) .

In the remainder of this section, \hat{A} will be a matrix with entries in $\widehat{\mathbb{P}}$, such that $\hat{A} - u$ is a global \uparrow -lift of $A - u$, and $\hat{A} - v$ is a global \uparrow -lift of $A - v$. It is often desirable

to have a small incriminating set. If we have some information about minors of A then this can be achieved by pivoting.

4.1.14 THEOREM. *Suppose $Z \subseteq X \cup Y$ incriminates (A, \widehat{A}) . Then there exist $X' \times Y'$ matrices A', \widehat{A}' , and $a, b \in X'$, such that $u, v \in Y'$, $A' \approx A$, $\widehat{A} - u \approx \widehat{A}' - u$, $\widehat{A} - v \approx \widehat{A}' - v$, and $\{a, b, u, v\}$ incriminates (A', \widehat{A}') .*

Proof: Suppose the theorem is false. Let $X, Y, A, \widehat{A}, u, v, Z$ form a counterexample, and suppose the counterexample was chosen so that $|Z \cap Y|$ is minimal. Clearly $u, v \in Z$. Suppose $y \in Z$ for some $y \in Y - \{u, v\}$.

4.1.14.1 CLAIM. *Some entry of $A[X \cap Z, y]$ is nonzero.*

Proof: Suppose all entries of $A[X \cap Z, y]$ equal zero. Then $G(A[Z])$ is not a cycle. But $\det(\widehat{A}[Z]) = 0 \in \widehat{\mathbb{P}}$, a contradiction. \square

Now let $X' := X \triangle \{x, y\}$, $Y' := Y \triangle \{x, y\}$, $A' := A^{xy}$, $\widehat{A}' := \widehat{A}^{xy}$, and $Z' := Z - \{x, y\}$. Since $\widehat{A}^{xy} - u = (\widehat{A} - u)^{xy}$, $\widehat{A} - u$ is a global \uparrow -lift of $A - u$. Likewise $\widehat{A} - v$ is a global \uparrow -lift of $A - v$.

4.1.14.2 CLAIM. *Z' incriminates (A', \widehat{A}') .*

Proof: Note that $\det(\widehat{A}'[Z']) = \pm \widehat{A}_{xy}^{-1} \det(\widehat{A}[Z])$, by Lemma 2.3.18. Hence $\det(\widehat{A}'[Z']) \in \widehat{\mathbb{P}}$ if and only if $\det(\widehat{A}[Z]) \in \widehat{\mathbb{P}}$. Therefore 4.1.12(ii) holds and $G(A[Z])$ is a cycle, C say. But then Lemma 2.3.38(ii) implies that $G(\widehat{A}'[Z'])$ is a cycle C' , and $\sigma_{\widehat{A}'}(C') = \sigma_{\widehat{A}}(C)$. The claim follows. \square

But $Z' \cap Y' = (Z \cap Y) - y$, contradicting minimality of $|Z \cap Y|$. \blacksquare

In the remainder of this section, $a, b \in X$ will be such that $\{a, b, u, v\}$ incriminates (A, \widehat{A}) . Pivots were used to create a small incriminating set, but they may destroy it too. We identify some pivots that don't.

4.1.15 DEFINITION. If $x \in X, y \in Y - \{u, v\}$ are such that $A_{xy} \neq 0$, then a pivot over xy is *allowable* if there are $a', b' \in X \triangle \{x, y\}$ such that $\{a', b', u, v\}$ incriminates $(A^{xy}, \widehat{A}^{xy})$. \diamond

4.1.16 LEMMA. *If $x \in X - \{a, b\}, y \in Y - \{u, v\}$ are such that $A_{xy} \neq 0$, and either $A_{xu} = A_{xv} = 0$, or $A_{ay} = A_{by} = 0$, then $\{a, b, u, v\}$ incriminates $(A^{xy}, \widehat{A}^{xy})$.*

Proof: This follows from the observation that $A^{xy}[\{a, b, u, v\}] = A[\{a, b, u, v\}]$ and $\widehat{A}^{xy}[\{a, b, u, v\}] = \widehat{A}[\{a, b, u, v\}]$. \blacksquare

4.1.2 The proof of Theorem 4.1.4

Proof of Theorem 4.1.4: Observe that (i) and (ii) can not hold simultaneously. Suppose the theorem fails for partial fields $\mathbb{P}, \widehat{\mathbb{P}}$ with homomorphism φ and lifting function \uparrow . Then there exists a matrix A for which neither (i) nor (ii) holds. By

Lemma 4.1.5 there exists such an $X \times Y$ matrix A that has no local lift. Assume that $X \cap Y = \emptyset$. Assume that A was chosen such that $|X| + |Y|$ is minimal. Since paths and cycles do have a local lift, A has a weak deletion pair or a weak contraction pair, by Lemma 4.1.8. Possibly after transposing we may assume $\{u, v\}$ is a weak deletion pair. Let \hat{A} be a matrix as specified in Theorem 4.1.9. We say that \hat{A} is a *lift candidate* for $(A, \{u, v\})$. Then some set Z incriminates (A, \hat{A}) . By Theorem 4.1.14 we may assume $Z = \{a, b, u, v\}$ for $a, b \in X$.

4.1.4.1 CLAIM. All entries of $A[Z]$ are nonzero.

Proof: If some entry of $\hat{A}[Z]$ equals 0 then $\det(\hat{A}[Z])$ is the product of two entries in \hat{A} , and hence $\det(\hat{A}[Z]) \in \hat{\mathbb{P}}$. But $G(A[Z])$ is not a cycle, so Z does not incriminate (A, \hat{A}) , a contradiction. \square

Since all four entries of $\hat{A}[Z]$ are nonzero, $G(A[Z])$ is a cycle, say $C = (a, u, b, v, a)$, and if $\det(\hat{A}[Z]) \notin \hat{\mathbb{P}}$ then

$$\sigma_{\hat{A}}(C) \neq \sigma_A(C)^\dagger. \quad (4.4)$$

Hence there is no need to distinguish the case $\det(\hat{A}[Z]) \notin \hat{\mathbb{P}}$. Denote the distance between vertices in a graph by $d_G(u, v)$.

4.1.4.2 ASSUMPTION. We assume that, subject to the above, A, u, v, a, b were chosen such that $d_{G(A-\{u,v\})}(a, b)$ is as small as possible.

4.1.4.3 CLAIM. $d_{G(A-\{u,v\})}(a, b) \leq 4$.

Proof: Suppose not. Then $d_{G(A-\{u,v\})}(a, b) \geq 6$. Let a, v_0, v_1, v_2 be the start of a shortest $a - b$ path. Then $A_{av_2} = A_{bv_2} = 0$, so a pivot over $v_1 v_2$ is allowable by Lemma 4.1.16. But $A^{v_1 v_2}$ contains a shorter $a - b$ path, a contradiction. \square

Let P be a shortest $a - b$ path. Then Z incriminates $(A[Z \cup P], \hat{A}[Z \cup P])$, and u, v is a weak deletion pair of $A[Z \cup P]$. But then, by minimality of $|X| + |Y|$, $A = A[Z \cup P]$.

4.1.4.4 CLAIM. $d_{G(A-\{u,v\})}(a, b) = 4$.

Proof: If $P = (a, x, b)$ then

$$A \sim \begin{matrix} & \begin{matrix} x & u & v \end{matrix} \\ \begin{matrix} a \\ b \end{matrix} & \begin{bmatrix} 1 & 1 & 1 \\ 1 & p & q \end{bmatrix} \end{matrix},$$

and A satisfies (ii) of the theorem, a contradiction. \square

Possibly after scaling we have

$$A = \begin{matrix} & \begin{matrix} x & w & u & v \end{matrix} \\ \begin{matrix} y \\ a \\ b \end{matrix} & \begin{bmatrix} \textcircled{1} & \textcircled{1} & p & q \\ 0 & \textcircled{1} & \textcircled{1} & \textcircled{1} \\ \textcircled{1} & 0 & r & s \end{bmatrix} \end{matrix}.$$

Let $\widehat{p}, \widehat{q}, \widehat{r}, \widehat{s}$ be the entries of \widehat{A} corresponding to p, q, r, s . From (4.4) it follows that

$$\frac{\widehat{r}}{\widehat{s}} \neq \left(\frac{r}{s}\right)^\uparrow. \quad (4.5)$$

4.I.4.5 CLAIM. p and q are not both zero.

Proof: If $p = q = 0$ then pivoting over yx would be allowable, a contradiction to minimality of the length of P . \square

4.I.4.6 CLAIM. Either $p = 0$ or $q = 0$.

Proof: Suppose $p \neq 0, q \neq 0$. Then $\widehat{p} = p^\uparrow, \widehat{q} = q^\uparrow, \widehat{r} = (r/p)^\uparrow p^\uparrow$, and $\widehat{s} = (s/q)^\uparrow q^\uparrow$.

The matrix A is minor-minimal, so $A[\{y, a, b\}, \{u, v\}]$ has a local $^\uparrow$ -lift. This matrix is scaling-equivalent to the following normalized matrices:

$$\begin{matrix} & \begin{matrix} u & v \end{matrix} \\ \begin{matrix} y \\ a \\ b \end{matrix} & \begin{bmatrix} \textcircled{1} & q/p \\ \textcircled{1} & \textcircled{1} \\ r/s & \textcircled{1} \end{bmatrix}, \quad \begin{matrix} & \begin{matrix} u & v \end{matrix} \\ \begin{matrix} y \\ a \\ b \end{matrix} & \begin{bmatrix} \textcircled{1} & \textcircled{1} \\ \textcircled{1} & p/q \\ \textcircled{1} & ps/(qr) \end{bmatrix}. \end{matrix}$$

Since these matrices have a local $^\uparrow$ -lift we conclude, using $(1/p)^\uparrow = 1/(p^\uparrow)$, that

$$\left(\frac{p}{q}\right)^\uparrow \left(\frac{s}{r}\right)^\uparrow = \left(\frac{ps}{qr}\right)^\uparrow.$$

Likewise $A[\{y, b\}, \{x, u, v\}]$ has a local $^\uparrow$ -lift. This gives

$$\left(\frac{p}{r}\right)^\uparrow \left(\frac{s}{q}\right)^\uparrow = \left(\frac{ps}{qr}\right)^\uparrow.$$

Finally, $A_1[\{y, a\}, \{w, u, v\}]$ has a local $^\uparrow$ -lift. This gives

$$\frac{p^\uparrow}{q^\uparrow} = \left(\frac{p}{q}\right)^\uparrow.$$

But then

$$\left(\frac{r}{s}\right)^\uparrow = \left(\frac{r}{p}\right)^\uparrow p^\uparrow / \left(\left(\frac{s}{q}\right)^\uparrow q^\uparrow\right) = \frac{\widehat{r}}{\widehat{s}},$$

a contradiction to (4.5). \square

By symmetry we may assume $p = 0$.

4.1.4.7 CLAIM. $q = 1$.

Proof: Suppose $p = 0, q \neq 0, q \neq 1$. Then A^{aw} is scaling-equivalent to

$$A' := \begin{matrix} & \begin{matrix} x & a & u & v \end{matrix} \\ \begin{matrix} y \\ w \\ b \end{matrix} & \begin{bmatrix} \textcircled{1} & \textcircled{1} & p' & q' \\ 0 & \textcircled{1} & \textcircled{1} & \textcircled{1} \\ \textcircled{1} & 0 & r' & s' \end{bmatrix} \end{matrix}$$

with $p' = 1, q' = 1 - q, r' = -r, s' = -s$. A spanning tree T' has been circled. Let \widehat{A}' be a T' -normalized lift candidate for $(A', \{u, v\})$. By minimality of $|X| + |Y|$, $\widehat{A}' - u$ is a global lift of $A' - u$ and $\widehat{A}' - v$ is a global lift of $A' - v$. Therefore $\widehat{A}' \sim \widehat{A}^{aw}$. But $\widehat{A}^{aw}[Z] \sim \widehat{A}[Z]$, so by (4.4) and Lemma 2.3.38(i) we have $\sigma_{\widehat{A}}(w, u, b, v, w) \neq \sigma_{A'}(w, u, b, v, w)^\uparrow$. But this is impossible by Claim 4.1.4.6. \square

Now $p = 0, q = 1$. Then

$$\widehat{s} = s^\uparrow \text{ and } \widehat{r} = -(-r)^\uparrow. \quad (4.6)$$

Scale column u of A by $1/r$ and then row a by r . After permuting some rows and columns we obtain

$$A' := \begin{matrix} & \begin{matrix} u & x & w & v \end{matrix} \\ \begin{matrix} b \\ y \\ a \end{matrix} & \begin{bmatrix} \textcircled{1} & \textcircled{1} & 0 & s \\ 0 & \textcircled{1} & \textcircled{1} & \textcircled{1} \\ \textcircled{1} & 0 & r & r \end{bmatrix} \end{matrix}.$$

A spanning tree T' has been circled. Let \widehat{A}' be the T' -normalized lift candidate for $(A', \{w, v\})$. Then $\widehat{A}'_{aw} = -(-r)^\uparrow$ and $\widehat{A}'_{av} = (r/s)^\uparrow s^\uparrow$. But then $\sigma_{\widehat{A}'}(y, w, a, v, y) \neq \sigma_{A'}(y, w, a, v, y)^\uparrow$, by (4.5) and (4.6). By Claim 4.1.4.7 we now have $s = 1$. We can now repeat the argument and conclude that also $r = 1$. Hence (ii) of the theorem holds, contradicting our choice of A . This completes the proof of the theorem. \blacksquare

4.1.3 The proof of Lemma 4.1.5

Proof of Lemma 4.1.5: A pair (A, xy) , where A is an $X \times Y$ \mathbb{P} -matrix and $x \in X, y \in Y$ is such that $A_{xy} \neq 0$, is called a *bad-pivot pair* if A has a local lift \widehat{A} , but \widehat{A}^{xy} is not a local lift of A^{xy} .

Suppose the lemma is false, and let A be an $X \times Y$ matrix that is a counterexample. Assume that $X \cap Y = \emptyset$, and that A was chosen so that $|X| + |Y|$ is minimal. That is, A has a local lift \widehat{A} , but \widehat{A} is not a global $^\uparrow$ -lift for A . Then there exist sequences A_0, \dots, A_k and $\widehat{A}_0, \dots, \widehat{A}_k$ such that $A_0 = A, \widehat{A}_0 = \widehat{A}$, and for $i = 1, \dots, k$, $A_i = (A_{i-1})^{x_i y_i}$ and $\widehat{A}_i = (\widehat{A}_{i-1})^{x_i y_i}$, such that \widehat{A}_k is not a local $^\uparrow$ -lift of A_k . Assume A and these sequences were chosen such that k is as small as possible. Then $k = 1$, so there is a bad-pivot pair (A, xy) . Clearly A is connected.

4.1.5.1 CLAIM. If (A, xy) is a bad-pivot pair, and $\{u, v\}$ is a weak deletion pair or a weak contraction pair of A , then $\{x, y\} \cap \{u, v\} \neq \emptyset$.

Proof: If A has a weak deletion pair $\{u, v\}$ such that $y \notin \{u, v\}$, then $\widehat{A}^{xy} - u$ is a global \uparrow -lift of $A^{xy} - u$, and $\widehat{A}^{xy} - v$ is a global \uparrow -lift of $A^{xy} - v$, by minimality of $|X| + |Y|$. But then Theorem 4.1.9 implies that \widehat{A}^{xy} is a local \uparrow -lift of A , a contradiction. \square

Since a \mathbb{P} -matrix A is connected if and only if A^{xy} is connected, we also have:

4.1.5.2 CLAIM. *If (A, xy) is a bad-pivot pair, and $\{u, v\}$ is a weak deletion pair or a weak contraction pair of A^{xy} , then $\{x, y\} \cap \{u, v\} \neq \emptyset$.*

Let C be a cycle of $G(A^{xy})$ such that $\sigma_{A^{xy}}(C)^\uparrow \neq \sigma_{\widehat{A}^{xy}}(C)$. C exists since \widehat{A}^{xy} is not a local lift of A^{xy} . Let $Z := V(C)$. By minimality of $|X| + |Y|$, $X \cup Y = Z \cup \{x, y\}$.

Let N_x be the set consisting of all neighbours of x in $G(A^{xy})$, and N_y the set consisting of all neighbours of y in $G(A^{xy})$. If $N_x \cap Z = \emptyset$ or $N_y \cap Z = \emptyset$ then $A^{xy}[Z] = A[Z]$, and $\widehat{A}^{xy}[Z] = \widehat{A}[Z]$, a contradiction. It follows that $G(A^{xy})$ is 2-connected.

4.1.5.3 CLAIM. *Either $\{x, y\} \subseteq Z$ or $\{x, y\} \cap Z = \emptyset$.*

Proof: Suppose without loss of generality that $y \in Z$, $x \notin Z$. Then x has a neighbour, v say, in Z . Let e_1, e_2 be the edges of C containing v . Since v is not adjacent to y , $C - \{e_1, e_2\} \cup \{xy, xv\}$ is a tree having three leaves, with x, y as internal vertices. But then A^{xy} has a weak deletion pair or a weak contraction pair disjoint from $\{x, y\}$, contradicting Claim 4.1.5.2. \square

4.1.5.4 CLAIM. *For some $p, q \in \mathbb{P}$ with $q \neq 0$, we have*

$$A \sim \begin{matrix} & & \begin{matrix} y & g & h \end{matrix} \\ \begin{matrix} x \\ e \\ f \end{matrix} & \begin{bmatrix} \textcircled{1} & \textcircled{1} & 0 \\ \textcircled{1} & p & \textcircled{1} \\ 0 & \textcircled{1} & q \end{bmatrix} \end{matrix}. \quad (4.7)$$

Proof: Suppose $\{x, y\} \subseteq Z$. We have to show that $|Z| = 6$. Clearly $|Z| \geq 6$. Suppose $|Z| \geq 8$, and let $x'y'$ be the edge of $G(A^{xy})$ having maximum distance from xy . Now $G(A)$ has exactly one edge more than $G(A^{xy})$, which connects the neighbours of xy . Let v be the neighbour adjacent to x in $G(A^{xy})$ (and hence adjacent to y in $G(A)$), and let w be the other neighbour of v in $G(A^{xy})$. Then $G(A) - \{vy, vw\}$ is a spanning tree having three leaves. Since $|Z| \geq 8$, $w \notin \{x', y'\}$, so x' and y' are not leaves. Hence, by Claim 4.1.5.2, $\widehat{A}^{x'y'}$ is a local lift of $A^{x'y'}$. By Lemma 2.3.38(ii), $\sigma_{(A^{xy})^{x'y'}}(C - \{x', y'\}) = \sigma_{A^{xy}}(C)$ and $\sigma_{(\widehat{A}^{xy})^{x'y'}}(C - \{x', y'\}) = \sigma_{\widehat{A}^{xy}}(C)$. It follows that $(A^{x'y'} - \{x', y'\}, xy)$ is a bad-pivot pair, contradicting minimality of $|X| + |Y|$.

Therefore $\{x, y\} \cap Z = \emptyset$. Let w, z be neighbours of xy in A^{xy} . If w, z are nonadjacent in $G(A^{xy})$, then a weak deletion pair or weak contraction pair $\{u, v\} \subseteq Z$ can be found, where w, u, z, v occur in that order in the cycle Z . This contradicts Claim 4.1.5.2, so w, z are adjacent. Hence both x and y have exactly one neighbour in Z . Suppose $|Z| \geq 6$, and let $x'y'$ be the edge of C having maximum distance from xy in A^{xy} . The same argument as above shows

that $(A^{x'y'} - \{x', y'\}, xy)$ is a bad-pivot pair, again contradicting minimality of $|X| + |Y|$.

It follows that

$$A^{xy} \sim \begin{matrix} & & x & g & h \\ & y & & & \\ e & \begin{bmatrix} 1 & 1 & 0 \\ 1 & p' & 1 \\ 0 & 1 & q' \end{bmatrix} \\ & f & & & \end{matrix},$$

where $p', q' \in \mathbb{P}$ and $q' \neq 0$. Pivoting over yx completes the proof. \square

Suppose A and \widehat{A} are normalized such that the entries circled in (4.7) equal 1. It follows from Lemma 2.3.38(ii) that $p \neq 0$. Then $\widehat{A}_{eg} = p^\uparrow$ and $\widehat{A}_{fh} = (pq)^\uparrow / p^\uparrow$.

After a pivot over xy and scaling we have

$$A^{xy} \sim A' = \begin{matrix} & & x & g & h \\ & y & & & \\ e & \begin{bmatrix} \textcircled{1} & \textcircled{1} & 0 \\ \textcircled{1} & 1-p & \textcircled{1} \\ 0 & \textcircled{1} & -q \end{bmatrix} \\ & f & & & \end{matrix}.$$

If $p = 1$ then $\{x, y\} \subseteq Z = V(C)$. But $\sigma_{A^{xy}}(C) = q = \sigma_A(C - \{x, y\})$, and $\sigma_{\widehat{A}^{xy}}(C) = q^\uparrow = \sigma_{\widehat{A}}(C - \{x, y\})$, a contradiction. The normalized local $^\uparrow$ -lift \widehat{A}' of A' has $\widehat{A}'_{eg} = (1-p)^\uparrow$ and $\widehat{A}'_{fh} = (q(p-1))^\uparrow / (1-p)^\uparrow$. By definition of the lifting function $(1-p)^\uparrow = 1 - p^\uparrow$ and $\left(\frac{p}{p-1}\right)^\uparrow = \frac{p^\uparrow}{p^\uparrow - 1}$. Since \widehat{A}' is not scaling-equivalent to \widehat{A}^{xy} , we must have

$$-(pq)^\uparrow / p^\uparrow \neq (q(p-1))^\uparrow / (1-p)^\uparrow. \quad (4.8)$$

Consider

$$A^{xg} = \begin{matrix} & & y & x & h \\ & g & & & \\ e & \begin{bmatrix} 1 & 1 & 0 \\ 1-p & -p & 1 \\ -1 & -1 & q \end{bmatrix} \\ & f & & & \end{matrix}.$$

Since A is minor-minimal, $A^{xg}[\{e, f\}, \{y, x, h\}]$ has a global $^\uparrow$ -lift. If we normalize with respect to tree $T' = \{ey, ex, eh, fy\}$ then we find

$$\left(\frac{p-1}{p}\right)^\uparrow (pq)^\uparrow = ((1-p)q)^\uparrow,$$

which contradicts (4.8). Therefore A does have a global $^\uparrow$ -lift, and the result follows. \blacksquare

4.2 Applications

We will now apply the Lift Theorem to prove a number of results.

4.2.1 Binary matroids

On his way to a proof of Theorem 1.2.10, Tutte (1965) proved the following characterization of regular matroids:

4.2.1 THEOREM. *Let M be a binary matroid. Exactly one of the following is true:*

- (i) M is regular;
- (ii) M has a minor isomorphic to one of F_7 and F_7^* .

The shortest known proof of this result is by Gerards (1989). The techniques used to prove the Lift Theorem generalize those used by Gerards, so it is no surprise that Theorem 4.2.1 can also be proven using the Lift Theorem.

Proof: Let $\mathbb{P} := \text{GF}(2)$, let $\widehat{\mathbb{P}} := \mathbb{U}_0 = (\mathbb{Z}, \{-1, 0, 1\})$, let $\varphi : \widehat{\mathbb{P}} \rightarrow \mathbb{P}$ be defined by $\varphi(-1) = \varphi(1) = 1$, $\varphi(0) = 0$, and let $\uparrow : \mathcal{F}(\mathbb{P}) \rightarrow \widehat{\mathcal{F}}(\widehat{\mathbb{P}})$ be defined by $0^\uparrow := 0$, $1^\uparrow := 1$. It is readily checked that this is a lifting function.

We have seen in Section 3.3 that F_7 and F_7^* are not regular. For the converse, let M be a binary matroid without F_7 - and F_7^* -minor, and let A be a \mathbb{P} -matrix such that $M = M[I A]$. All rank-2 binary matroids are regular, so A has no minor isomorphic to a matrix as in (4.2). But then Theorem 4.1.4 implies that A has a global $\widehat{\mathbb{P}}$ -lift, and hence M is regular. ■

4.2.2 Ternary matroids

Next we give new proofs of two more results of Whittle (1997). We have already seen a proof of two other results by Whittle, namely Theorems 3.1.7 and 4.A.

Recall from Definition 2.5.7 that the near-regular partial field is defined as $\mathbb{U}_1 = (\mathbb{Z}[\alpha, \frac{1}{1-\alpha}, \frac{1}{\alpha}], \langle -1, \alpha, 1-\alpha \rangle)$ for an indeterminate α .

4.2.2 THEOREM (Whittle, 1997). *Let M be a matroid. The following are equivalent:*

- (i) M is representable over $\text{GF}(3) \times \text{GF}(4) \times \text{GF}(5)$;
- (ii) M is representable over $\text{GF}(3) \times \text{GF}(8)$;
- (iii) M is \mathbb{U}_1 -representable;
- (iv) M is representable over every field with at least 3 elements.

Proof: Let $\varphi : \mathbb{U}_1 \rightarrow \text{GF}(3) \times \text{GF}(4) \times \text{GF}(5)$ be determined by $\varphi(\alpha) = (-1, \omega, 2)$, where ω is a generator of $\text{GF}(4)$. Then $\varphi|_{\mathcal{F}(\mathbb{U}_1)} : \mathcal{F}(\mathbb{U}_1) \rightarrow \mathcal{F}(\text{GF}(3) \times \text{GF}(4) \times \text{GF}(5))$ is a bijection, so we use $(\varphi|_{\mathcal{F}(\mathbb{U}_1)})^{-1}$ as lifting function and apply Corollary 4.1.6 to prove (i) \Leftrightarrow (iii).

Likewise, let $\psi : \mathbb{U}_1 \rightarrow \text{GF}(3) \times \text{GF}(8)$ be determined by $\varphi(\alpha) = (-1, \omega)$, where ω is a generator of $\text{GF}(8)$. Then $\varphi|_{\mathcal{F}(\mathbb{U}_1)} : \mathcal{F}(\mathbb{U}_1) \rightarrow \mathcal{F}(\text{GF}(3) \times \text{GF}(8))$ is a bijection, so we use $(\varphi|_{\mathcal{F}(\mathbb{U}_1)})^{-1}$ as lifting function and apply Corollary 4.1.6 to prove (i) \Leftrightarrow (iii). This requires some case checking which we omit here.

The implication (iii) \Rightarrow (iv) was proven as Lemma 2.5.8, and (i), (ii) are special cases of (iv). ■

Recall from Definition 2.5.14 that $\mathbb{Y} = (\mathbb{Z}[\zeta, \frac{1}{2}], \langle -1, 2, \zeta \rangle)$, where ζ is a root of $x^2 - x + 1 = 0$.

4.2.3 THEOREM (Whittle, 1997). *Let M be a matroid. The following are equivalent:*

- (i) M is representable over $\text{GF}(3) \times \text{GF}(7)$;
- (ii) M is \mathbb{Y} -representable;
- (iii) M is representable over $\text{GF}(3)$, over $\text{GF}(p^2)$ for all primes $p > 2$, and over $\text{GF}(p)$ when $p \equiv 1 \pmod{3}$.

Proof: Let $\varphi : \mathbb{Y} \rightarrow \text{GF}(3) \times \text{GF}(7)$ be determined by $\varphi(2) = (-1, 2)$ and $\varphi(\zeta) = (-1, 3)$. Again $\varphi|_{\mathcal{F}(\mathbb{Y})} : \mathcal{F}(\mathbb{Y}) \rightarrow \mathcal{F}(\text{GF}(3) \times \text{GF}(7))$ is a bijection, so we use $(\varphi|_{\mathcal{F}(\mathbb{Y})})^{-1}$ as lifting function and apply Corollary 4.1.6 to prove (i) \Leftrightarrow (ii). The implication (ii) \Rightarrow (iii) follows from Lemma 2.5.16. Finally, (i) is a special case of (iii). ■

4.2.3 Quaternary and quinary matroids

Recall from Definition 2.5.17 that the golden ratio partial field is defined as $\mathbb{G} = (\mathbb{Z}[\tau], \langle -1, \tau \rangle)$, where τ is the golden ratio.

4.2.4 THEOREM (Vertigan). *Let M be a matroid. The following are equivalent:*

- (i) M is representable over $\text{GF}(4) \times \text{GF}(5)$;
- (ii) M is \mathbb{G} -representable;
- (iii) M is representable over $\text{GF}(5)$, over $\text{GF}(p^2)$ for all primes p , and over $\text{GF}(p)$ when $p \equiv \pm 1 \pmod{5}$.

Proof: Let $\varphi : \mathbb{G} \rightarrow \text{GF}(4) \times \text{GF}(5)$ be determined by $\varphi(\tau) = (\omega, 3)$, where ω is a generator of $\text{GF}(4)$. Again $\varphi|_{\mathcal{F}(\mathbb{G})} : \mathcal{F}(\mathbb{G}) \rightarrow \mathcal{F}(\text{GF}(4) \times \text{GF}(5))$ is a bijection, so we use $(\varphi|_{\mathcal{F}(\mathbb{G})})^{-1}$ as lifting function and apply Corollary 4.1.6 to prove (i) \Leftrightarrow (ii).

The implication (ii) \Rightarrow (iii) follows from Lemma 2.5.18. Finally, (i) is a special case of (iii). ■

Our next result requires more advanced techniques. Recall from Definition 2.5.20 that the Gaussian partial field is $\mathbb{H}_2 = (\mathbb{Z}[i, \frac{1}{2}], \langle i, 1-i \rangle)$, where i is a root of $x^2 + 1 = 0$. The following lemma is a corollary of Whittle's Stabilizer Theorem (Whittle, 1999). We will state and prove the Stabilizer Theorem in Section 6.2.1.

4.2.5 LEMMA (Whittle, 1999). *Let M be a 3-connected quinary matroid with a minor N isomorphic to one of $U_{2,5}$ and $U_{3,5}$. Then any representation of M over $\text{GF}(5)$ is determined up to strong equivalence by the induced representation of N .*

4.2.6 LEMMA. *Let M be a 3-connected matroid.*

- (i) *If M has at least 2 inequivalent representations over $\text{GF}(5)$, then M is representable over \mathbb{H}_2 .*
- (ii) *If M has a $U_{2,5}$ - or $U_{3,5}$ -minor and M is representable over \mathbb{H}_2 , then M has at least 2 inequivalent representations over $\text{GF}(5)$.*

Proof: Let $\varphi : \mathbb{H}_2 \rightarrow \text{GF}(5) \times \text{GF}(5)$ be determined by $\varphi(i) = (2, 3)$. Then $\varphi(2) = \varphi(i(1-i)^2) = (2, 2)$. Let $\varphi_i : \text{GF}(5) \times \text{GF}(5) \rightarrow \text{GF}(5)$ be determined by $\varphi_i((x_1, x_2)) = x_i$ for $i = 1, 2$. Let

$$A := \begin{bmatrix} 1 & 1 & 1 \\ 1 & p' & q' \end{bmatrix}$$

for some, $p', q' \in \mathbb{H}_2$. If A is an \mathbb{H}_2 -matrix then $p', q' \in \mathcal{F}(\mathbb{H}_2)$. A finite check then shows that for each of these, $\varphi_1(\varphi(A)) \neq \varphi_2(\varphi(A))$. This proves (ii).

Let M be a 3-connected matroid having two inequivalent representations over $\text{GF}(5)$. Then there exists a $\text{GF}(5) \times \text{GF}(5)$ -matrix A such that $M = M[I A]$ and $\varphi_1(A) \not\sim \varphi_2(A)$.

The restriction $\varphi|_{\mathcal{F}(\mathbb{H}_2)} : \mathcal{F}(\mathbb{H}_2) \rightarrow \mathcal{F}(\text{GF}(5) \times \text{GF}(5))$ is a bijection. If we apply Theorem 4.1.4 with lifting function $(\varphi|_{\mathcal{F}(\mathbb{H}_2)})^{-1}$ then Case 4.1.4(ii) holds only for $\text{GF}(5) \times \text{GF}(5)$ -matrices A having a minor

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & p & q \end{bmatrix} \text{ or } \begin{bmatrix} 1 & 1 \\ 1 & p \\ 1 & q \end{bmatrix},$$

where $p, q \in \{(2, 2), (3, 3), (4, 4)\}$. But Theorem 6.3.7 implies that if A has such a minor, then $\varphi_1(A)$ and $\varphi_2(A)$ will be strongly equivalent. Since both matrices have the same row and column indices, this implies $\varphi_1(A) \sim \varphi_2(A)$, a contradiction. Now (i) follows. ■

4.2.7 THEOREM. *Let M be a 3-connected matroid with a $U_{2,5}$ - or $U_{3,5}$ -minor. The following are equivalent:*

- (i) M has 2 inequivalent representations over $\text{GF}(5)$;
- (ii) M is \mathbb{H}_2 -representable;
- (iii) M has two inequivalent representations over $\text{GF}(5)$ and is representable over $\text{GF}(p^2)$ for all primes $p \geq 3$ and over $\text{GF}(p)$ when $p \equiv 1 \pmod{4}$.

Proof: The implication (i) \Leftrightarrow (ii) follows from the previous lemma. The implication (ii) \Rightarrow (iii) follows from Lemma 2.5.21, and (i) is a special case of (iii). ■

Recall from Definition 2.5.32 that the 2-cyclotomic partial field is defined as $\mathbb{K}_2 = (\mathbb{Q}(\alpha), \langle -1, \alpha, 1 - \alpha, 1 + \alpha \rangle)$ for an indeterminate α . We conclude this section with the following result:

4.2.8 THEOREM. *Let M be a matroid. The following are equivalent:*

- M is representable over $\text{GF}(4) \times \mathbb{H}_2$;
- M is representable over \mathbb{K}_2 .

The proof consists, once more, of an application of Corollary 4.1.6.

4.3 Lift ring

Rather than guessing a pair $\mathbb{P}, \widehat{\mathbb{P}}$ for which the Lift Theorem may hold, and then verifying all conditions, it is possible to *construct* a partial field $\widehat{\mathbb{P}}$ for any partial field \mathbb{P} , such that the conditions of the Lift Theorem are guaranteed to hold. This construction is the subject of this section. If \mathcal{A} is a set of \mathbb{P} -matrices, then we define

$$\text{Cr}(\mathcal{A}) := \cup_{A \in \mathcal{A}} \text{Cr}(A),$$

the set of all cross ratios occurring in \mathcal{A} .

4.3.1 DEFINITION. Let \mathbb{P} be a partial field, and \mathcal{A} a set of \mathbb{P} -matrices. We define the \mathcal{A} -lift of \mathbb{P} as

$$\mathbb{L}_{\mathcal{A}}\mathbb{P} := (R_{\mathcal{A}}/I_{\mathcal{A}}, \langle \{-1\} \cup \tilde{F}_{\mathcal{A}} \rangle),$$

where $\tilde{F}_{\mathcal{A}} := \{\tilde{p} \mid p \in \text{Cr}(\mathcal{A})\}$ is a set of indeterminates, $R_{\mathcal{A}} := \mathbb{Z}[\tilde{F}]$ is the polynomial ring over \mathbb{Z} with indeterminates $\tilde{F}_{\mathcal{A}}$, and $I_{\mathcal{A}}$ is the ideal generated by the following polynomials in $R_{\mathcal{A}}$:

- (i) $\tilde{0} - 0; 1 - 1;$
- (ii) $\tilde{-1} + 1$ if $-1 \in \text{Cr}(\mathcal{A})$;
- (iii) $\tilde{p} + \tilde{q} - 1$, where $p, q \in \text{Cr}(\mathcal{A})$, $p + q = 1$;
- (iv) $\tilde{p}\tilde{q} - 1$, where $p, q \in \text{Cr}(\mathcal{A})$, $pq = 1$;
- (v) $\tilde{p}\tilde{q}\tilde{r} - 1$, where $p, q, r \in \text{Cr}(\mathcal{A})$, $pqr = 1$, and

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & p & q^{-1} \end{bmatrix} \preceq A$$

for some $A \in \mathcal{A}$. ◇

If \mathcal{A} is the set of all \mathbb{P} -matrices, then $\text{Cr}(\mathcal{A}) = \mathcal{F}(\mathbb{P})$. In that case we write $\mathbb{L}\mathbb{P}$ for $\mathbb{L}_{\mathcal{A}}\mathbb{P}$. We will show that a matroid M such that $M = M[I A]$ for some $A \in \mathcal{A}$ is also $\mathbb{L}_{\mathcal{A}}\mathbb{P}$ -representable. First we need a lemma.

4.3.2 LEMMA. Let \mathbb{P} be a partial field. There exists a partial-field homomorphism $\varphi : \mathbb{L}_{\mathcal{A}}\mathbb{P} \rightarrow \mathbb{P}$ such that $\varphi(\tilde{p} + I_{\mathcal{A}}) = p$ for all $p \in \text{Cr}(\mathcal{A})$.

Proof: Suppose $\mathbb{P} = (R, G)$. Then $\psi : R_{\mathcal{A}} \rightarrow R$ determined by $\psi(\tilde{p}) = p$ for all $\tilde{p} \in \tilde{F}_{\mathcal{A}}$ is obviously a ring homomorphism. Clearly $I_{\mathcal{A}} \subseteq \ker(\psi)$, so $\varphi' : R_{\mathcal{A}}/I_{\mathcal{A}} \rightarrow R$ determined by $\varphi'(\tilde{p} + I_{\mathcal{A}}) = \psi(p)$ for all $\tilde{p} \in \tilde{F}_{\mathcal{A}}$ is a well-defined ring homomorphism. Then $\varphi := \varphi'|_{\mathbb{L}_{\mathcal{A}}\mathbb{P}}$ is the desired partial-field homomorphism. ■

The main result of this section is the following:

4.3.3 THEOREM. Let \mathbb{P} be a partial field and \mathcal{A} a set of \mathbb{P} -matrices. If $M = M[I A]$ for some $A \in \mathcal{A}$ then M is $\mathbb{L}_{\mathcal{A}}\mathbb{P}$ -representable.

Proof: Let $\widehat{\mathbb{P}} := \mathbb{L}_{\mathcal{A}}\mathbb{P}$ and let φ be the homomorphism from Lemma 4.3.2. We define $\uparrow : \text{Cr}(\mathcal{A}) \rightarrow \mathcal{F}(\widehat{\mathbb{P}})$ by $p^\uparrow := \tilde{p} + I_{\mathcal{A}}$. By 4.3.1(iii),(iv) this is a lifting function for φ . Now all conditions of Corollary 4.1.6 are satisfied. ■

The partial field $\mathbb{L}_{\mathcal{A}}\mathbb{P}$ is the most general partial field for which the lift theorem holds, in the following sense:

4.3.4 THEOREM. Let \mathcal{A} be a set of \mathbb{P} -matrices, and suppose $\mathbb{P}, \widehat{\mathbb{P}}, \varphi, \uparrow$ are such that the conditions of Corollary 4.1.6 are satisfied for all $A \in \mathcal{A}$. Then there exists a nontrivial homomorphism $\psi : \mathbb{L}_{\mathcal{A}}\mathbb{P} \rightarrow \widehat{\mathbb{P}}$.

Proof: Let $\psi' : R_{\mathcal{A}} \rightarrow \widehat{\mathbb{P}}$ be determined by $\psi'(\tilde{p}) = p^\uparrow$ for all $p \in \text{Cr}(\mathcal{A})$. This is clearly a ring homomorphism. But since all conditions of Corollary 4.1.6 hold, $I_{\mathcal{A}} \subseteq \ker(\psi')$. It follows that there exists a well-defined homomorphism $\psi : \mathbb{L}_{\mathcal{A}}\mathbb{P} \rightarrow \widehat{\mathbb{P}}$, as desired. ■

\mathbb{P}	$\text{GF}(2) \times \text{GF}(3)$	$\text{GF}(3) \times \text{GF}(4)$	$\text{GF}(3) \times \text{GF}(5)$
\mathbb{LP}	\mathbb{U}_0	\mathbb{S}	\mathbb{D}
\mathbb{P}	$\text{GF}(3) \times \text{GF}(7)$	$\text{GF}(3) \times \text{GF}(8)$	$\text{GF}(4) \times \text{GF}(5)$
\mathbb{LP}	\mathbb{Y}	\mathbb{U}_1	\mathbb{G}
\mathbb{P}	$\text{GF}(5) \times \text{GF}(7)$	$\text{GF}(5) \times \text{GF}(8)$	$\text{GF}(4) \times \text{GF}(5) \times \text{GF}(7)$
\mathbb{LP}	$\text{GF}(5) \times \text{GF}(7)$	$\text{GF}(5) \times \text{GF}(8)$	$\mathbb{G} \times \text{GF}(7)$

TABLE 4.1
Some lifts of partial fields.

We use algebraic tools such as Gröbner basis computations over rings to get insight in the structure of \mathbb{LP} . In particular, we adapted the method described by [Baines and Vámos \(2003\)](#) to verify the claims in Table 4.1.

4.4 Open problems

Theorems such as those in Section 4.2 show the equivalence between representability over infinitely many fields and over a finite number of finite fields. The following conjecture generalizes the characterization of the near-regular matroids:

4.4.1 CONJECTURE. *Let k be a prime power. There exists a number n_k such that, for all matroids M , M is representable over all fields with at least k elements if and only if it is representable over all finite fields $\text{GF}(q)$ with $k \leq q \leq n_k$.*

To our disappointment the techniques in this chapter failed to prove this conjecture even for $k = 4$. We offer the following candidate:

4.4.2 CONJECTURE. *A matroid M is representable over all finite fields with at least 4 elements if and only if M is representable over*

$$\mathbb{P}_4 := (\mathbb{Q}(\alpha), \langle -1, \alpha, \alpha - 1, \alpha + 1, \alpha - 2 \rangle),$$

where α is an indeterminate.

Originally we posed this conjecture with \mathbb{K}_2 instead of \mathbb{P}_4 . This would imply that all such matroids have at least two inequivalent representations over $\text{GF}(5)$. But $M_{8591}^{\text{Y}\Delta}$, introduced in Section 3.3.3, is representable over $\text{GF}(4)$, $\text{GF}(7)$, $\text{GF}(8)$, and uniquely representable over $\text{GF}(5)$. Its universal partial field is \mathbb{P}_4 , and there is clearly no homomorphism from \mathbb{P}_4 to \mathbb{K}_2 .

The partial field \mathbb{LP} gives information about the representability of the set of \mathbb{P} -representable matroids over other fields. An interesting question is how much information it gives.

- 4.4.3 QUESTION. Which partial fields \mathbb{P} are such that whenever the set of \mathbb{P} -representable matroids is also representable over a field \mathbb{F} , there exists a homomorphism $\varphi : \mathbb{LP} \rightarrow \mathbb{F}$? \diamond

Each of \mathbb{U}_0 , \mathbb{S} , \mathbb{D} , \mathbb{U}_1 , \mathbb{Y} , \mathbb{G} , \mathbb{H}_2 has this property, since each of these is the universal partial field of some matroid.

- 4.4.4 QUESTION. Let $\varphi : \mathbb{LP} \rightarrow \mathbb{P}$ be the canonical homomorphism. For which partial fields \mathbb{P} is $\varphi|_{\mathcal{F}(\mathbb{LP})} : \mathcal{F}(\mathbb{LP}) \rightarrow \mathcal{F}(\mathbb{P})$ a bijection? \diamond

This bijection exists for all examples in Section 4.2, and results in an obvious choice of lifting function. If there is always such a bijection then it is not necessary to introduce an abstract lifting function. We have seen that the proof of the Lift Theorem can be simplified in that case, since Lemma 4.1.5 becomes trivial. A related conjecture is the following:

- 4.4.5 CONJECTURE. $\mathbb{L}^2\mathbb{P} \cong \mathbb{LP}$.

The following conjecture seems to be only just outside the scope of the Lift Theorem:

- 4.4.6 CONJECTURE. A matroid is representable over $\text{GF}(2^k)$ for all $k > 1$ if and only if it is representable over $\mathbb{U}_1^{(2)}$.

We say that a partial field \mathbb{P} is *level* if $\mathbb{P} = \mathbb{L}_{\mathcal{A}}\mathbb{P}'$ for some partial field \mathbb{P}' , where \mathcal{A} is the class of \mathbb{P}' -representable matroids.

- 4.4.7 QUESTION. Under what conditions is \mathbb{P}_M level? \diamond

The converse of the latter question is also of interest.

- 4.4.8 QUESTION. When is a level partial field also universal? \diamond

A somewhat weaker statement is the following. Let \mathcal{M} be a class of matroids. A partial field \mathbb{P} is \mathcal{M} -universal if, for every partial field \mathbb{P}' such that every matroid in \mathcal{M} is \mathbb{P}' -representable, there exists a homomorphism $\varphi : \mathbb{P} \rightarrow \mathbb{P}'$.

- 4.4.9 CONJECTURE. Let \mathcal{M} be the set of all \mathbb{P} -representable matroids, where \mathbb{P} is a level partial field. Then \mathbb{P} is \mathcal{M} -universal.

Looking at Table 4.1, an obvious question is the following:

- 4.4.10 QUESTION. Is $\mathbb{LP} \not\cong \mathbb{P}$ for other choices of $\mathbb{P} = \text{GF}(q_1) \times \cdots \times \text{GF}(q_k)$? \diamond

The last three entries in Table 4.1 indicate that sometimes the answer is negative. In these finite fields there seem to be relations that enforce $\mathbb{LP} \cong \mathbb{P}$. But Theorems 4.2.7 and 4.2.8 indicate that the Lift Theorem may find other uses still.



Connectivity

RECALL from Section 2.4.1 that the connectivity function of a matroid M is defined by $\lambda_M(X) := \text{rk}_M(X) + \text{rk}_M(E(M) - X) - \text{rk}(M)$. For the final two chapters of this thesis we need some more results on connectivity. These results, which are either well-known or straightforward observations, are collected in this chapter. For the Confinement Theorem in Chapter 6, only Sections 5.2 (up to Section 5.2.1) and 5.3 are relevant. The remainder of this chapter serves as setup for Chapter 7.

5.1 Loops, coloops, elements in series, and elements in parallel

We will need some elementary properties of loops, series classes, and parallel classes.

5.1.1 DEFINITION. Let $M = (E, \mathcal{I})$ be a matroid. Then $e \in E$ is a *loop* of M if $\{e\} \notin \mathcal{I}$. Furthermore, $e \in E$ is a *coloop* of M if e is a loop of M^* . \diamond

Loops do not have an effect on the representability of a matroid:

5.1.2 PROPOSITION. Let M be a matroid, and $e \in E(M)$ a loop of M . If A is an $X \times Y$ \mathbb{P} -matrix for disjoint sets X, Y , such that $M \setminus e = M[I A]$, then there is a unique $X \times (Y \cup e)$ \mathbb{P} -matrix A' such that $M = M[I A']$ and $A' - e = A$.

Proof: Let A' be the $X \times (Y \cup e)$ matrix with $A'_{xy} = A_{xy}$ for all $x \in X, y \in Y$, and $A'_{xe} = 0$ for all $x \in X$. Then $\text{rk}(A[X, e]) = 0$, so e is not in any independent set. It follows immediately that $M = M[I A']$.

Suppose now that A'' is such that $A'' - e = A - e$, $M = M[I A'']$, yet $A'' \neq A'$. Then $A''_{xe} \neq 0$ for some $x \in X$. But then $\text{rk}(A[X, e]) = 1$, contradicting the fact that e is not in any independent set. \blacksquare

5.1.3 DEFINITION. Let $M = (E, \mathcal{J})$ be a matroid. Then $e, f \in E$ are in parallel in M if $\{e\}, \{f\} \in \mathcal{J}$, but $\{e, f\} \notin \mathcal{J}$. Furthermore, $e, f \in E$ are in series in M if they are in parallel in M^* . \diamond

We omit the elementary proofs of the following statements.

5.1.4 PROPOSITION. Let $M = (E, \mathcal{J})$ be a matroid.

- (i) If e, f are in parallel in M , and f, g are in parallel in M , then e, g are in parallel in M .
- (ii) If e, f are in parallel in M , and $e \in X \subseteq E$, then $\text{rk}_M(X \cup f) = \text{rk}_M(X)$.
- (iii) If e, f are in parallel in M , and $e \in X \subseteq (E - f)$, then $\text{rk}_M(X \Delta \{e, f\}) = \text{rk}_M(X)$.
- (iv) If e, f are in parallel in M , and $e \in X \subseteq (E - f)$, then $\text{rk}_{M^*}(X \Delta \{e, f\}) = \text{rk}_{M^*}(X)$.
- (v) If e, f are in parallel in M , and e, g are in series in M , then $f = g$ and $\{e, f\}$ is a separator of M .

It follows from Proposition 5.1.4(i) that, for connected matroids, $E(M)$ can be partitioned into parallel classes. Roughly speaking, Proposition 5.1.4(iii), (iv) state that two elements in parallel are indistinguishable. It will be useful to consider the matroid obtained from a connected matroid M by replacing each class of elements in parallel by a representative from that class.

5.1.5 DEFINITION. Let M be a matroid. Define

$$S_e := \{f \in E(M) \mid e, f \text{ are in parallel in } M\}.$$

Then the *simplification* of M , denoted by $\text{si}(M)$, is the matroid on ground set $\{S_e \mid e \in E\}$ having rank function

$$\text{rk}_{\text{si}(M)}(X) := \text{rk}_M\left(\bigcup_{S \in X} S\right). \quad \diamond$$

It follows easily from Proposition 5.1.4(ii), (iii) that $\text{si}(M)$ is indeed a matroid, that $\text{si}(M)$ has no loops and no elements in parallel, and that $\text{si}(M) \preceq M$.

5.1.6 DEFINITION. Let M be a matroid. The *cosimplification* of M is

$$\text{co}(M) := \text{si}(M^*)^*. \quad \diamond$$

Like loops, parallel and series classes have no influence on the representability of a matroid. The following statement is stronger than Corollary 2.4.29: for general 2-separations it does not hold that the representation is unique.

5.1.7 PROPOSITION. Let M be a matroid, and let e, f be in parallel in M . If A is an $X \times Y$ \mathbb{P} -matrix for disjoint sets X, Y , such that $M \setminus e = M[IA]$, then there is an $X \times (Y \cup e)$ \mathbb{P} -matrix A' such that $M = M[IA']$ and $A' - e = A$. Moreover, A' is unique up to scaling of column e .

Proof: We may assume $f \notin X$. Let A' be the $X \times (Y \cup e)$ matrix with $A'_{xy} = A_{xy}$ for all $x \in X$, $y \in Y$, and $A'_{xe} = A_{xf}$ for all $x \in X$. Then $\text{rk}(A[X, \{e, f\}]) = 1$. It follows easily that $M = M[I A']$.

Suppose now that A'' is such that $A'' - e = A - e$, $M = M[I A'']$, yet $A'' \not\sim A'$. Then $A''[X, e]$ is not a multiple of $A''[X, f]$. But then $\text{rk}(A[X, \{e, f\}]) = 2$, a contradiction. ■

5.2 The connectivity function

We start with some elementary properties of the connectivity function. The first lemma follows immediately from Proposition 1.2.15:

5.2.1 LEMMA. *Let M be a matroid and $X \subseteq E(M)$. Then*

$$\lambda_M(X) = \text{rk}_M(X) + \text{rk}_{M^*}(X) - |X|. \quad (5.1)$$

Since (5.1) is self-dual we have:

5.2.2 COROLLARY. *Let M be a matroid and $X \subseteq E(M)$. Then*

$$\lambda_{M^*}(X) = \lambda_M(X).$$

Like the rank function, the connectivity function is submodular:

5.2.3 LEMMA. *Let M be a matroid, and $X, Y \subseteq E(M)$. Then*

$$\lambda_M(X) + \lambda_M(Y) \geq \lambda_M(X \cap Y) + \lambda_M(X \cup Y).$$

Proof: This is a straightforward consequence of Lemma 5.2.1 and submodularity of the rank function.

$$\begin{aligned} \lambda_M(X) + \lambda_M(Y) &= \text{rk}_M(X) + \text{rk}_M(Y) + \text{rk}_{M^*}(X) + \text{rk}_{M^*}(Y) - |X| - |Y| \\ &\geq \text{rk}_M(X \cap Y) + \text{rk}_M(X \cup Y) + \text{rk}_{M^*}(X \cap Y) + \text{rk}_{M^*}(X \cup Y) - \\ &\quad |X \cap Y| - |X \cup Y| \\ &= \lambda_M(X \cap Y) + \lambda_M(X \cup Y). \end{aligned} \quad \blacksquare$$

The following lemma, together with its dual, shows that the connectivity function is monotone under taking minors.

5.2.4 LEMMA. *Let M be a matroid, $e \in E(M)$, and $X \subseteq E(M) - e$. Then*

$$\lambda_{M \setminus e}(X) \leq \lambda_M(X) \leq \lambda_{M \setminus e}(X) + 1.$$

Proof: Let $Y := E(M) - X$.

$$\lambda_{M \setminus e}(X) = \text{rk}_M(X) + \text{rk}_M(Y - e) - \text{rk}(M \setminus e).$$

By Theorem 1.2.7 we have $\text{rk}_M(Y) \leq \text{rk}_M(Y - e) + 1$ and $\text{rk}(M) \leq \text{rk}(M \setminus e) + 1$. But if $\text{rk}(M) = \text{rk}(M \setminus e) + 1$ then e is a coloop of M , so also $\text{rk}_M(Y) = \text{rk}_M(Y \setminus e) + 1$. The result follows. ■

After some rearrangement we obtain the following:

5.2.5 COROLLARY. *Let M be a k -connected matroid. Then $M \setminus e$ is $(k - 1)$ -connected.*

To keep track of the connectivity of minors of M it is convenient to introduce some extra notation. The following definition mimics the notation for submatrices found on Page 10.

5.2.6 DEFINITION. Let M be a matroid, B a basis of M , and $Y = E(M) - B$. If $Z \subseteq E(M)$ then $M_B[Z] := M/(B - Z) \setminus (Y - Z)$, and $M_B - Z := M_B[E - Z]$. \diamond

The following is easily seen:

5.2.7 LEMMA. *If $M = M[IA]$ for an $X \times Y$ \mathbb{P} -matrix A , sets X and Y are disjoint, and $Z \subseteq X \cup Y$, then $M_X[Z] = M[IA[Z]]$.*

To counter the stacking of subscripts we introduce alternative notation for the connectivity function. This definition generalizes Lemma 2.4.12 to arbitrary matroids M , and to arbitrary minors of M . It is equal to the definition found in Geelen et al. (2000).

5.2.8 DEFINITION. Let M be a matroid, and B a basis of M . Then $\lambda_B : 2^{E(M)} \times 2^{E(M)} \rightarrow \mathbb{N}$ is defined as

$$\lambda_B(X, Y) := \text{rk}_{M/(B-Y)}(X - B) + \text{rk}_{M/(B-X)}(Y - B)$$

for all $X, Y \subseteq E(M)$. \diamond

The following lemma shows that this is indeed the connectivity function of a minor of M when X and Y are disjoint:

5.2.9 LEMMA. *Let M be a matroid, B a basis of M , and X, Y disjoint subsets of $E(M)$. Then*

$$\lambda_B(X, Y) = \lambda_{M_B[X \cup Y]}(X).$$

Proof: The proof boils down to an application of Lemma 1.2.21:

$$\begin{aligned} \lambda_B(X, Y) &= \text{rk}_{M_B[X \cup Y]/(X \cap B)}(X - B) + \text{rk}_{M_B[X \cup Y]/(Y \cap B)}(Y - B) \\ &= \text{rk}_{M_B[X \cup Y]}((X - B) \cup (X \cap B)) - \text{rk}_{M_B[X \cup Y]}(X \cap B) \\ &\quad + \text{rk}_{M_B[X \cup Y]}((Y - B) \cup (Y \cap B)) - \text{rk}_{M_B[X \cup Y]}(Y \cap B) \\ &= \text{rk}_{M_B[X \cup Y]}(X) + \text{rk}_{M_B[X \cup Y]}(Y) - |B \cap (X \cup Y)|, \end{aligned}$$

from which the result follows. \blacksquare

5.2.1 The Splitter Theorem

Sometimes we want a stronger result than Corollary 5.2.5: we want to delete or contract preserving connectivity, and usually also a specified minor. The next

two theorems provide such a guarantee. For proofs we refer to [Oxley \(1992, Proposition 4.3.6, Corollary 11.2.1\)](#).

5.2.10 THEOREM. *Let M and N be connected matroids, such that $N \preceq M$, and $|E(N)| < |E(M)|$. Then there is an $e \in E(M)$ such that some $M' \in \{M \setminus e, M/e\}$ is connected with $N \preceq M'$.*

For 3-connected matroids a more subtle result holds. We define two special families of matroids.

5.2.11 DEFINITION. For each $n \in \mathbb{N}$, $x \in \mathbb{U}_1$, define the following matrix over $\mathbb{Q}(x)$:

$$A_n(x) := \begin{matrix} & \begin{matrix} r_1 & r_2 & & \cdots & r_n \end{matrix} \\ \begin{matrix} s_1 \\ s_2 \\ \\ \vdots \\ s_n \end{matrix} & \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & x \\ 1 & 1 & 0 & \cdots & 0 & 0 \\ & 0 & 1 & 1 & \ddots & \vdots & \vdots \\ & 0 & 0 & \ddots & \ddots & 0 & 0 \\ & \vdots & \vdots & \ddots & \ddots & 1 & 0 \\ 0 & \cdots & 0 & 0 & 1 & 1 \end{bmatrix} \end{matrix}.$$

The *rank- n wheel* is the matroid $\mathcal{W}_n := M[I A_n((-1)^n)]$. The *rank- n whirl* is the matroid $\mathcal{W}^n := M[I A_n((-1)^n \alpha)]$, where $A_n((-1)^n \alpha)$ is interpreted as an \mathbb{U}_1 -matrix. \diamond

Our notation for the wheel differs slightly from the notation used by [Oxley \(1992\)](#), but we will not use the wheel much anyway. The following is easy to prove, since $A_n((-1)^n)$ is a \mathbb{U}_0 -matrix, and $A_n((-1)^n \alpha)$ is a \mathbb{U}_1 -matrix:

5.2.12 PROPOSITION. *\mathcal{W}_n is representable over every partial field; \mathcal{W}^n is representable over every partial field for which $\mathcal{F}(\mathbb{P}) - \{0, 1\} \neq \emptyset$.*

Now we can state the 3-connected version of Theorem [5.2.10](#), which is the famous Splitter Theorem by [Seymour \(1980\)](#):

5.2.13 THEOREM (Splitter Theorem). *Let M and N be 3-connected matroids, such that $N \preceq M$, $|E(M)| > |E(N)| \geq 4$, and M is not isomorphic to a wheel or a whirl. Then there is an $e \in E(M)$ such that some $M' \in \{M \setminus e, M/e\}$ is 3-connected with $N \preceq M'$.*

Many reformulations and variants of this result exist. For instance, [Oxley, Semple, and Whittle \(2008\)](#) have proven a variant of the theorem above in which, under a few extra conditions, contraction can take place in a fixed basis of M , and deletion outside this basis. Note that in both Theorem [5.2.10](#) and Theorem [5.2.13](#) we preserve a minor isomorphic to N . It is, in general, not possible to maintain a fixed minor $M/S \setminus T$.

5.2.2 The number of 2-separations

In Chapter 7 we will need to bound the number of 2-separations in small extensions of a 3-connected matroid. The following lemma does just that.

5.2.14 LEMMA. *If M is a connected matroid, $N \preceq M$, N is 3-connected, and $|E(M)| - |E(N)| \leq k$, then M has at most 2^{k+1} 2-separations.*

Proof: Let t_k denote the maximum number of k -separations of a k -element extension of a 3-connected matroid. We argue by induction on k . By Theorem 5.2.10 there exist a basis B of M , a subset X of $E(M)$, and an ordering e_1, \dots, e_k of the elements of $E(M) - X$ such that $N \cong M_B[X]$, and for all $i \in \{1, \dots, k\}$, $M_B[X \cup \{e_1, \dots, e_i\}]$ is connected.

If $k = 1$ then Proposition 5.1.4(i) implies that e_1 can be in series or in parallel with at most one element of $M_B[X]$, and Proposition 5.1.4(v) implies it can not be both in series and in parallel. Hence $t_1 = 1$.

By duality we may assume $e_k \notin B$. Let (Z_1, Z_2) be a 2-separation of M , with $e_k \in Z_1$. If $|Z_1| \geq 3$ then Lemma 5.2.4 implies $\lambda_{M \setminus e_k}(Z_2) \leq 1$, and connectivity of $M \setminus e_k$ implies that equality holds. Hence $(Z_1 - e_k, Z_2)$ is a 2-separation of $M \setminus e_k$. This leads to at most two 2-separations of M : (Z_1, Z_2) and $(Z_1 - e_k, Z_2 \cup e_k)$.

If a 2-separation of M is not an extension of a 2-separation of $M \setminus e_k$, then we must have $|Z_1| = 2$. There is one of these for each $f \in E(M) - \{e_k\}$ such that e_k, f are in series or in parallel. But e_k can, again, be in series or in parallel with at most one element of X , and with each of e_1, \dots, e_{k-1} , so it follows that

$$t_k \leq 2t_{k-1} + k.$$

Define $t'_k := 2^{k+1} - k - 2$. We claim that $t_k \leq t'_k$. Indeed: $t'_1 = t_1 = 1$, and if the claim is valid for $k - 1$, then

$$t_k \leq 2t_{k-1} + k \leq 2t'_{k-1} + k = 2(2^k - (k-1) - 2) + k = 2^{k+1} - k - 2 = t'_k.$$

Obviously $t'_k \leq 2^{k+1}$, and the result follows. ■

5.3 Blocking sequences

The following definitions are from Geelen et al. (2000).

5.3.1 DEFINITION. Let M be a matroid on ground set E , B a basis of M , $M' := M_B[E']$ for some $E' \subseteq E$, and (Z'_1, Z'_2) a k -separation of M' . We say that (Z'_1, Z'_2) is *induced* in M if there exists a k -separation (Z_1, Z_2) of M with $Z'_1 \subseteq Z_1$ and $Z'_2 \subseteq Z_2$. ◇

5.3.2 DEFINITION. A *blocking sequence* for (Z'_1, Z'_2) is a sequence of elements v_1, \dots, v_t of $E - E'$ such that

- (i) $\lambda_B(Z'_1, Z'_2 \cup v_1) = k$;
- (ii) $\lambda_B(Z'_1 \cup v_i, Z'_2 \cup v_{i+1}) = k$ for $i = 1, \dots, t - 1$;
- (iii) $\lambda_B(Z'_1 \cup v_t, Z'_2) = k$; and
- (iv) No proper subsequence of v_1, \dots, v_t satisfies the first three properties. ◇

Like the Splitter Theorem, blocking sequences find their origin in Seymour's work on regular matroid decomposition (Seymour, 1980, Section 8). The first general formulation was due to Truemper (1986), but blocking sequences truly earned their place in the matroid theorists' toolkit with the publication of Geelen, Gerards, and Kapoor's proof of Rota's Conjecture for $\text{GF}(4)$ (Geelen et al., 2000). We have chosen for their notation rather than the notation used in, for instance, Geelen, Hliněný, and Whittle (2005), because Definition 5.3.2 clearly exhibits the symmetry.

The following theorem illustrates the usefulness of blocking sequences:

5.3.3 THEOREM (Geelen et al., 2000, Theorem 4.14). *Let M be a matroid on ground set E , B a basis of M , $M' := M_B[E']$ for some $E' \subseteq E$, and (Z'_1, Z'_2) an exact k -separation of M' . Exactly one of the following holds:*

- (i) *There exists a blocking sequence for (Z'_1, Z'_2) ;*
- (ii) *(Z'_1, Z'_2) is induced in M .*

A useful property of blocking sequences is the following:

5.3.4 LEMMA. *If v_1, \dots, v_t is a blocking sequence for the k -separation (Z'_1, Z'_2) , then $v_i \in B$ implies $v_{i+1} \in E - B$ and $v_i \in E - B$ implies $v_{i+1} \in B$ for $i = 1, \dots, t-1$.*

We will use the following lemma in Chapter 6:

5.3.5 LEMMA (Geelen et al., 2000, Proposition 4.16(i)). *Let v_1, \dots, v_t be a blocking sequence for (Z'_1, Z'_2) . If $Z''_2 \subseteq Z'_2$ is such that $|Z''_2| \geq k$ and $\lambda_B(Z'_1, Z''_2) = k-1$, then v_1, \dots, v_{t-1} is a blocking sequence for the exact k -separation $(Z'_1, Z''_2 \cup v_t)$.*

5.4 Branch width

A graph $T = (V, E)$ is a *cubic tree* if T is a tree, and each vertex has degree exactly one or three. We denote the leaves of T by $L(T)$.

5.4.1 DEFINITION. Let M be a matroid. A *partial branch decomposition* of M is a pair (T, l) , where T is a cubic tree, and $l : L(T) \rightarrow 2^{E(M)}$ a function assigning a subset of $E(M)$ to each vertex of T , such that $\{l(v) \mid v \in V(T)\}$ partitions $E(M)$. \diamond

If T is a tree, and $e = vw \in E(T)$, then we denote by T_v the component of $T \setminus e$ containing v .

5.4.2 DEFINITION. Let M be a matroid, and let (T, l) be a partial branch decomposition of M . We define $w_{(T,l)} : V^2 \rightarrow \mathbb{N}$ as

$$w_{(T,l)}(v, w) = \begin{cases} \lambda_M(\bigcup_{u \in V(T_v)} l(u)) + 1 & \text{if } vw \in E(T); \\ 0 & \text{otherwise.} \end{cases} \quad \diamond$$

In words, $w_{(T,l)}(v, w)$ is the degree of the separation of M displayed by the edge vw . Note that $(\bigcup_{u \in V(T_v)} l(u), \bigcup_{u \in V(T_w)} l(u))$ is a partition of $E(M)$, so $w_{(T,l)}(v, w) =$

$w_{(T,l)}(w, v)$. Hence, for $e = vw \in E(T)$, we will write $w_{(T,l)}(e)$ as shorthand for $w_{(T,l)}(v, w)$.

5.4.3 DEFINITION. Let M be a matroid, and let (T, l) be a partial branch decomposition of M . The *width* of (T, l) is

$$w(T, l) := \begin{cases} \max_{e \in E(T)} w_{(T,l)}(e) & \text{if } E(T) \neq \emptyset \\ 1 & \text{otherwise.} \end{cases} \quad \diamond$$

5.4.4 DEFINITION. Let M be a matroid. A *branch decomposition* of M is a partial branch decomposition such that $|l(v)| \leq 1$ for all $v \in L(T)$, and $l(v) = \emptyset$ for all $v \in V(T) - L(T)$. \diamond

5.4.5 DEFINITION. Let M be a matroid. A *reduced branch decomposition* of M is a branch decomposition such that $|l(v)| = 1$ for all $v \in L(T)$. \diamond

We denote the set of reduced branch decompositions of M by \mathcal{D}_M .

5.4.6 DEFINITION. Let M be a matroid. The *branch width* of M is

$$\text{bw}(M) := \min_{(T,l) \in \mathcal{D}_M} w(T, l). \quad \diamond$$

We start with some elementary and well-known observations.

5.4.7 LEMMA. Let (T, l) be a branch decomposition of a matroid M . There is a reduced branch decomposition (T', l') of M such that $w(T, l) = w(T', l')$.

Proof: Let M be a matroid, and (T, l) a branch decomposition of M having width w . Suppose the lemma is false. Since the lemma is obviously true for matroids with at most one element, we may assume $|E(M)| \geq 2$. We may also assume that (T, l) was chosen among all branch decompositions of width w such that $|\{v \in L(T) \mid l(v) = \emptyset\}|$ is as small as possible. Pick $v \in L(T)$ is such that $l(v) = \emptyset$. Let w be the neighbour of v , so $w_{(T,l)}(vw) = \lambda_M(\emptyset) + 1 = 1$. If w is a leaf too, then $V(T) = \{v, w\}$. The pair (T', l') , where $T' = (\{w\}, \emptyset)$, and $l'(w) = l(w)$, is obviously again a branch decomposition, and $w(T', l') = 1 = w(T, l)$. But T' has fewer leaves that are labelled by the empty set, a contradiction to our choice of (T, l) .

Hence w is not a leaf. Let $e_1 = vw_1$, $e_2 = ww_2$ be the edges incident with w other than vw . Since $T \setminus e_1$ and $T \setminus e_2$ induce the same partition of $E(M)$, $w(e_1) = w(e_2)$. Now define $T' := T \setminus vw/e_1$ (where we label the vertex into which e_1 was contracted by w), and $l' : V(T') \rightarrow 2^{E(M)}$ by $l'(v') := l(v')$ for all $v' \in E(T) - \{v, w, w_2\}$, and $l'(w) := l(w) \cup l(w_1)$. Then (T', l') is again a branch decomposition, and $w(T', l') = \max\{w_{(T,l)}(vw), w(T, l)\} = w(T, l)$. But T' has fewer leaves that are labelled by the empty set, which again contradicts our choice of (T, l) . \blacksquare

5.4.8 PROPOSITION. *Let M be a matroid, and $e \in E(M)$. Then*

$$\text{bw}(M \setminus e) \leq \text{bw}(M) \leq \text{bw}(M \setminus e) + 1.$$

Proof: For the first inequality, let (T, l) be a branch decomposition of M , and let v be the leaf of T such that $l(v) = \{e\}$. Let $l' : V(T) \rightarrow 2^{E(M)}$ be such that $l'(u) = l(u)$ for $u \neq v$, and $l'(v) = \emptyset$. Clearly (T, l') is a branch decomposition for $M \setminus e$. Let $f \in E(T)$. By Lemma 5.2.4, $w_{(T, l')}(f) \leq w_{(T, l)}(f)$. Hence $w(T, l') \leq w(T, l)$, and therefore $\text{bw}(M \setminus e) \leq \text{bw}(M)$.

For the second inequality, let (T, l) be a branch decomposition of $M \setminus e$ such that $\text{bw}(M \setminus e) = w(T, l)$. Without loss of generality we assume that $l(v) = \emptyset$ for some $v \in L(T)$. Let $l' : V(T) \rightarrow 2^{E(M)}$ be such that $l'(u) = l(u)$ for $u \neq v$, and $l'(v) = \{e\}$. Then (T, l) is a branch decomposition for M . By Lemma 5.2.4 we have $w_{(T, l')}(f) \leq w_{(T, l)}(f) + 1$. Therefore $w(T, l') \leq w(T, l) + 1$, and hence $\text{bw}(M) \leq \text{bw}(M \setminus e) + 1$. ■

Series and parallel classes do not have an effect on the branch width of a matroid:

5.4.9 PROPOSITION. *Let M be a matroid with $\text{bw}(M) \geq 2$. Then $\text{bw}(M) = \text{bw}(\text{si}(M))$.*

Proof: We prove the theorem by induction on $|E(M)| - |E(\text{si}(M))|$. Let $x, y \in E(M)$ be a parallel pair, and let (T, l) be a reduced branch decomposition for $M \setminus x$ having minimal width. By induction $w(T, l) = \text{bw}(M \setminus x)$. Let v be the leaf of T with $l(v) = \{y\}$. Let T' be the tree obtained from T by adding vertices z, z' and edges $zv, z'v$. Define $l' : V(T') \rightarrow 2^{E(M)}$ as

$$l'(u) := \begin{cases} \{x\} & \text{for } u = z \\ \{y\} & \text{for } u = z' \\ \emptyset & \text{for } u = v \\ l(u) & \text{otherwise.} \end{cases}$$

Now $w_{(T', l')}(e) = w_{(T, l)}(e)$ for all $e \in E(T)$, by Proposition 5.1.4, and $w_{(T', l')}(vz) = w_{(T', l')}(vz') = 2$. It follows that $\text{bw}(M) \leq \text{bw}(M \setminus x)$. By Proposition 5.4.8, $\text{bw}(M) \geq \text{bw}(M \setminus x)$. The result follows. ■

Branch width is a powerful concept. Geelen and Whittle (2002) proved the following result, which will play a key role in Chapter 7:

5.4.10 THEOREM. *Let \mathbb{F} be a finite field and $k \in \mathbb{N}$. Let \mathcal{M} be a minor-closed class of \mathbb{F} -representable matroids. Then finitely many excluded minors of \mathcal{M} have branch width k .*

Geelen et al. (2005, Theorem 1.4) proved the following result, which states that a blocking sequence does not increase branch width by much:

5.4.11 THEOREM. *Let M be a matroid having basis B , and let $Z \subseteq E(M)$. Suppose $M_B[Z]$ has a k -separation (X, Y) , and that v_1, \dots, v_t is a blocking sequence for (X, Y) in M . Then $\text{bw}(M_B[Z \cup \{v_1, \dots, v_t\}]) \leq \text{bw}(M_B[Z]) + k$.*

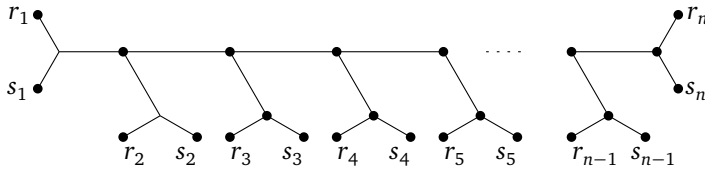


FIGURE 5.1
Reduced branch decomposition of \mathcal{W}^n having width 3

As an example, which we will need in Chapter 7, we determine the branch width of the rank- n whirl:

5.4.12 LEMMA. For all $n \geq 2$, $\text{bw}(\mathcal{W}^n) = 3$.

Proof sketch: There is, up to isomorphism, exactly one cubic tree with four leaves. Label the leaves of this tree T arbitrarily with the elements of $\mathcal{W}^2 = U_{2,4}$, and label the internal vertices with the empty set. If $e \in E(T)$ is adjacent to a leaf then $w(e) = 2$, otherwise $w(e) = 3$. It follows that $\text{bw}(\mathcal{W}^2) = 3$.

Now Lemma 5.4.8 implies that $\text{bw}(\mathcal{W}^n) \geq 3$. If we label the elements of \mathcal{W}^n by $s_1, r_1, s_2, r_2, \dots, s_n, r_n$ as in Definition 5.2.11, then $\text{rk}_{\mathcal{W}^n}(\{s_i, r_i, s_{i+1}\}) = 2$ for all $i \in \{1, \dots, n\}$ (where indices are interpreted modulo n), and the reduced branch decomposition shown in Figure 5.1 has width 3. ■

5.5 Crossing 2-separations

The following definitions are from Geelen et al. (2000).

5.5.1 DEFINITION. Let M be a matroid, and let (X_1, X_2) and (Y_1, Y_2) be 2-separations of M . If $X_i \cap Y_j \neq \emptyset$ for all $i, j \in \{1, 2\}$, then we say that (X_1, X_2) and (Y_1, Y_2) cross. ◇

5.5.2 DEFINITION. Let M be a matroid, and let (X_1, X_2) be a 2-separation of M . We say that (X_1, X_2) is crossed if there exists a 2-separation (Y_1, Y_2) of M such that (X_1, X_2) and (Y_1, Y_2) cross. Otherwise we say (X_1, X_2) is uncrossed. ◇

Crossing 2-separations have previously been studied by Cunningham and Edmonds (1980). In a very interesting paper Oxley, Semple, and Whittle (2004) characterized crossing 3-separations in 3-connected matroids, and those results have been generalized to crossing k -separations by Aikin and Oxley (2008). In Aikin and Oxley's terminology, $(X_1 \cap Y_1, X_1 \cap Y_2, X_2 \cap Y_2, X_2 \cap Y_1)$ would be a two-flower*. We have no need for the full theory in this thesis, so we will confine our attention to some isolated observations.

5.5.3 LEMMA. If (X_1, X_2) and (Y_1, Y_2) are crossing 2-separations in a connected matroid M , then $\lambda_M(X_i \cap Y_j) = 1$ for all $i, j \in \{1, 2\}$.

*No Luggage in sight.

Proof: By submodularity we have

$$\lambda_M(X_1) + \lambda_M(Y_1) \geq \lambda_M(X_1 \cap Y_1) + \lambda_M(X_1 \cup Y_1).$$

Now $X_1 \cap Y_1 \neq \emptyset$. Since M is connected, M has no loops, so $\lambda_M(X_1 \cap Y_1) \geq 1$. Also $\lambda_M(X_1 \cup Y_1) \geq 1$. But $\lambda_M(X_1) + \lambda_M(Y_1) = 2$, so $\lambda_M(X_1 \cap Y_1) = 1$. ■

5.5.4 LEMMA. *Let M be a connected matroid having a 2-separation (X, Y) . If $\text{bw}(M) \geq 3$ then M has an uncrossed 2-separation (X', Y') .*

Proof: Suppose the lemma is false for some connected matroid M with 2-separation (X, Y) . That is, $\text{bw}(M) \geq 3$ yet M has no uncrossed 2-separation. Let (T, l) be a partial branch decomposition of M such that

- (i) $l(v) = \emptyset$ for all $v \in V(T) - L(T)$;
- (ii) $\lambda_M(l(v)) = 1$ for all $v \in L(T)$;
- (iii) $w(T, l) = 2$.

Such a partial branch decomposition certainly exists: we can take (T, l) for $T = (\{v, w\}, \{vw\})$ and $l(v) = X, l(w) = Y$.

5.5.4.I CLAIM. *If (T, l) is such that $|L(T)|$ is as large as possible, then (T, l) is a reduced branch decomposition of M .*

Proof: Let (T, l) be a partial branch decomposition maximizing $|L(T)|$. Since $\lambda_M(\emptyset) = 0$, it follows that $l(v) \neq \emptyset$ for all $v \in L(T)$. If (T, l) is not a reduced branch decomposition then there exists a $v \in L(T)$ such that $|l(v)| \geq 2$. Then $(l(v), E(M) - l(v))$ is a 2-separation of M . This 2-separation is crossed by assumption, so by Lemma 5.5.3 there is a partition (Z, Z') of $l(v)$ such that $\lambda_M(Z) = \lambda_M(Z') = 1$. Let T' be the tree obtained from T by adding vertices z, z' and edges $zv, z'v$. Define $l' : V(T') \rightarrow 2^{E(M)}$ as

$$l'(u) := \begin{cases} Z & \text{for } u = z \\ Z' & \text{for } u = z' \\ \emptyset & \text{for } u = v \\ l(u) & \text{otherwise.} \end{cases}$$

Now $w_{(T', l')}(e) = w_{(T, l)}(e)$ for all $e \in E(T)$, and $w_{(T', l')}(vz) = w_{(T', l')}(vz') = 2$. Hence $w(T', l') = 2$. Therefore (T', l') satisfies (i)–(iii). But $|L(T')| > |L(T)|$, contradicting our choice of T . The claim follows. □

But this is impossible, since $2 = w(T, l) \geq \text{bw}(M)$, yet $\text{bw}(M) \geq 3$. This contradiction completes the proof. ■

5.5.5 THEOREM. *Let M be a connected matroid such that (X, Y) is a 2-separation of M , and such that $N \preceq M$ for some non-binary matroid N . Then M has an uncrossed 2-separation.*

Proof: Since N is non-binary, $\mathcal{W}^2 \preceq N \preceq M$, by Theorem 1.2.29. But then it follows from Proposition 5.4.8 and Lemma 5.4.12 that $\text{bw}(M) \geq 3$. The result now follows from Lemma 5.5.4. ■

Uncrossed 2-separations are relevant because they can be bridged without introducing new 2-separations:

5.5.6 LEMMA (Geelen et al., 2000, Proposition 4.17). *Let M be a matroid, B a basis of M , $E' \subseteq E$, and (Z'_1, Z'_2) an uncrossed 2-separation of $M_B[E']$. Let v_1, \dots, v_t be a blocking sequence for (Z'_1, Z'_2) . If (Z_1, Z_2) is a 2-separation of $M_B[E' \cup \{v_1, \dots, v_t\}]$ then, for some $i, j \in \{1, 2\}$, $Z'_i \cup \{v_1, \dots, v_t\} \subseteq Z_j$.*

5.5.7 COROLLARY. *Let M be a matroid, B a basis of M , $E' \subseteq E$, and (Z'_1, Z'_2) an uncrossed 2-separation of the connected matroid $M_B[E']$. Let v_1, \dots, v_t be a blocking sequence for (Z'_1, Z'_2) . Then $M_B[E' \cup \{v_1, \dots, v_t\}]$ has strictly fewer 2-separations than $M_B[E']$.*

Proof: Let (Z_1, Z_2) be a 2-separation of $M_B[E' \cup \{v_1, \dots, v_t\}]$. Possibly after relabelling, Lemma 5.5.6 implies that $Z'_2 \cup \{v_1, \dots, v_t\} \subseteq Z_2$. Therefore we know that $|Z_2 - \{v_1, \dots, v_t\}| \geq 2$. Also $|Z_1| \geq 2$ so, since $M_B[E']$ is connected, $1 \leq \lambda_B(Z_1, Z_2 - \{v_1, \dots, v_t\}) \leq \lambda_B(Z_1, Z_2) = 1$. Hence $(Z_1, Z_2 - \{v_1, \dots, v_t\})$ is a 2-separation of $M_B[E']$, and the result follows. ■



Confinement to sub-partial fields

SOMETIMES a matroid that is representable over a partial field \mathbb{P} is in fact also representable over a sub-partial field $\mathbb{P}' \subseteq \mathbb{P}$. We have already seen an example of this phenomenon in the proof of Theorem 1.2.10. Let M, N be matroids such that N is a minor of M . Suppose that, whenever a \mathbb{P} -representation A of M contains a scaled \mathbb{P}' -representation of N , A itself is a scaled \mathbb{P}' -representation of M . Then we say that N *confines* M to \mathbb{P}' . The following theorem reduces verifying if N confines M to a finite check.

6.A THEOREM. *Let \mathbb{P}, \mathbb{P}' be partial fields such that \mathbb{P}' is an induced sub-partial field of \mathbb{P} . Let M, N be 3-connected matroids such that $N = M/S \setminus T$. Then exactly one of the following holds:*

- (i) *N confines M to \mathbb{P}' ;*
- (ii) *M has a 3-connected minor M' such that*
 - *N does not confine M' to \mathbb{P}' ;*
 - *N is isomorphic to M'/x , $M' \setminus y$, or $M'/x \setminus y$ for some $x, y \in E(M')$;*
 - *If N is isomorphic to $M'/x \setminus y$ then at least one of $M'/x, M' \setminus y$ is 3-connected.*

Recall that if a sub-partial field is induced, then $p + q \in \mathbb{P}'$ whenever $p, q \in \mathbb{P}'$ and $p + q \in \mathbb{P}$. The Confinement Theorem (Theorem 6.1.3), the main result of this chapter, will be stated in terms of individual representation matrices. Theorem 6.A is a direct corollary of it.

The most basic applications of the Confinement Theorem involve restricting matroid representations to sub-partial fields. A clear example is the following result due to Whittle. Recall the partial field $\mathbb{Y} = (\mathbb{Z}[\zeta, \frac{1}{2}], \langle -1, 2, \zeta \rangle)$.

6.B THEOREM (Whittle, 1997). *Let M be a \mathbb{Y} -representable matroid. Then M can be obtained from \mathbb{S} -representable matroids and \mathbb{D} -representable matroids by direct sums and 2-sums.*

Proof: By Theorem 2.4.30 it suffices to show that every 3-connected \mathbb{Y} -representable matroid is either \mathbb{S} -representable or \mathbb{D} -representable. Suppose the theorem fails for a matroid M . Then M is a 3-connected \mathbb{Y} -representable matroid, say $M = M[IA]$ for an $X \times Y$ \mathbb{Y} -matrix, and A is not a scaled \mathbb{D} -matrix, and not a scaled \mathbb{S} -matrix. Both \mathbb{S} and \mathbb{D} are sub-partial fields of \mathbb{Y} , but of these two only \mathbb{D} is an induced sub-partial field of \mathbb{Y} . Suppose $2 \in \text{Cr}(A)$. Then we may assume, possibly after pivoting and scaling, that

$$A[Z] = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix}$$

for some $Z \subseteq X \cup Y$. Let $N := M_X[Z]$. The only 3-connected single-element extension of $U_{2,4}$ is $U_{2,5}$, which is not \mathbb{Y} -representable. The only 3-connected single-element coextension of $U_{2,4}$ is $U_{3,5}$, which is not \mathbb{Y} -representable. It follows from Theorem 6.A that N is a \mathbb{D} -confiner for M , and hence A is a scaled \mathbb{D} -matrix, a contradiction. Therefore $\text{Cr}(A) \subseteq \{0, 1, \zeta, \bar{\zeta}\}$. By Theorem 2.3.34, A is a scaled $\mathbb{Y}[\text{Cr}(A)]$ -matrix. But then A is a scaled \mathbb{S} -matrix, again a contradiction. ■

The Confinement Theorem has other applications. From Theorem 4.2.1 it is easily seen that a binary matroid is either representable over every field, or only representable over fields of characteristic two. Whittle gave a similar characterization of the matroids representable over $\text{GF}(3)$:

6.C THEOREM (Whittle, 1997). *Let \mathbb{F} be a field, and let \mathcal{M} be the set of matroids representable over both $\text{GF}(3)$ and \mathbb{F} . Then $\mathcal{M} = \mathcal{M}(\text{GF}(3) \times \text{GF}(q))$ for some $q \in \{2, 3, 4, 5, 7, 8\}$.*

One of the goals of this chapter is to give an alternative proof of this result. The Lift Theorem will feature prominently alongside the Confinement Theorem. A similar argument suffices to prove Semple and Whittle's (1996a) result that every representable matroid with no $U_{2,5}$ - and no $U_{3,5}$ -minor is either binary or ternary. These proofs appear in Section 6.3.1.

The Confinement Theorem closely resembles several results related to inequivalent representations of matroids. These results are Whittle's Stabilizer Theorem (Whittle, 1999), the extension to universal stabilizers by Geelen et al. (1998), and the theory of free expansions of Geelen et al. (2002). In fact, Whittle's Stabilizer Theorem is a corollary of the Confinement Theorem. We will prove this in Section 6.2.1. Furthermore, in Section 6.2.2 we will introduce an algebraic relative of the theory of free expansions, based on the theory of universal partial fields from Section 3.3.

We were led to the Confinement Theorem by our study of matroids with inequivalent representations over $\text{GF}(5)$. Using the Lift Theorem and the Confinement Theorem we were able to prove Theorem 1.4.1, which we repeat here for convenience:

6.D THEOREM. *Let M be a 3-connected matroid.*
 (i) *If M has at least two inequivalent representations over $\text{GF}(5)$, then M is representable over \mathbb{C} , over $\text{GF}(p^2)$ for all primes $p \geq 3$, and over $\text{GF}(p)$ when $p \equiv 1 \pmod{4}$.*

- (ii) If M has at least three inequivalent representations over $\text{GF}(5)$, then M is representable over every field with at least five elements.
- (iii) If M has at least four inequivalent representations over $\text{GF}(5)$, then M is not binary and not ternary.
- (iv) If M has at least five inequivalent representations over $\text{GF}(5)$, then M has six inequivalent representations over $\text{GF}(5)$.

Note that (iii) is a special case of a result by Whittle (1996). Oxley et al. (1996) proved that a 3-connected quinary matroid never has more than 6 inequivalent representations. To prove Theorem 6.D the Hydra- k partial fields, introduced in Section 2.5, will be used. This proof appears in Section 6.3.2. We conclude the chapter with some open problems.

This chapter is based on joint work with Rudi Pendavingh (Pendavingh and Van Zwam, 2008).

6.1 The theorem and its proof

6.1.1 DEFINITION. Let \mathbb{P}, \mathbb{P}' be partial fields with $\mathbb{P}' \subseteq \mathbb{P}$, let D be a \mathbb{P}' -matrix, and M a \mathbb{P} -representable matroid. Then D *confines* M if, for all \mathbb{P} -matrices A such that $M = M[I A]$ and $D \preceq A$, A is a scaled \mathbb{P}' -matrix. \diamond

6.1.2 DEFINITION. Let \mathbb{P}, \mathbb{P}' be partial fields with $\mathbb{P}' \subseteq \mathbb{P}$, and N, M matroids such that $N \preceq M$. Then N *confines* M if D confines M for every \mathbb{P}' -matrix D with $N = M[I D]$. \diamond

Note that if D confines M , then every \mathbb{P}' -matrix $D' \approx D$ confines M , and D^T confines M^* .

The following theorem reduces verifying whether D confines a matroid M to a finite check, provided that M and D are 3-connected and \mathbb{P}' is induced.

6.1.3 THEOREM (Confinement Theorem). Let \mathbb{P}, \mathbb{P}' be partial fields such that $\mathbb{P}' \subseteq \mathbb{P}$ and \mathbb{P}' is induced. Let D be a 3-connected scaled \mathbb{P}' -matrix. Let A be a 3-connected \mathbb{P} -matrix with D as a submatrix. Then exactly one of the following is true:

- (i) A is a scaled \mathbb{P}' -matrix;
- (ii) A has a 3-connected minor A' with rows X' , columns Y' , such that
 - A' is not a scaled \mathbb{P}' -matrix.
 - D is isomorphic to $A' - U$ for some U with $|U \cap X'| \leq 1, |U \cap Y'| \leq 1$;
 - If D is isomorphic to $A' - \{x, y\}$ then at least one of $A' - x, A' - y$ is 3-connected.

Let $\mathbb{P}, \mathbb{P}', D$ be as in Definition 6.1.1. If there exists a $p \in \mathcal{F}(\mathbb{P}) - \mathcal{F}(\mathbb{P}')$, then the 2-sum of $M[I D]$ with $U_{2,4}$ will have a representation by a \mathbb{P} -matrix A that has a minor $\begin{bmatrix} 1 & 1 \\ p & 1 \end{bmatrix}$, by Corollary 2.4.29, and therefore A is not a scaled \mathbb{P}' -matrix. It follows that the 3-connectivity requirements in the theorem are essential.

6.1.1 Preliminary results

We need some preliminary results before proving Theorem 6.1.3. The effect of a pivot over xy is limited to entries having a distance close to that of x and y . The following lemma makes this explicit.

6.I.4 LEMMA. Let A be an $X \times Y$ \mathbb{P} -matrix for disjoint sets X, Y , and let d be the distance function of $G(A)$. Let $x \in X, y \in Y$ be such that $A_{xy} \neq 0$. Let $X' := \{x' \in X \mid d_{G(A)}(x', y) > 1\}$ and $Y' := \{y' \in Y \mid d_{G(A)}(x, y') > 1\}$. Then $A^{xy}[X', Y - y] = A[X', Y - y]$ and $A^{xy}[X - x, Y'] = A[X - x, Y']$.

Proof: Note that $A_{xy'} = 0$ whenever $d_{G(A)}(x, y') > 1$. Likewise, $A_{x'y} = 0$ whenever $d_{G(A)}(x', y) > 1$. The result follows immediately from Definition 2.3.14. ■

6.I.5 DEFINITION. Let $G = (V, E)$ be a connected graph, and let $U \subseteq V$ be such that $G[U]$ is connected. A U -tree T is a spanning tree for G such that T contains a shortest $v - U$ path for every $v \in V - U$. If T' is a spanning tree of $G[U]$ then T is a U -tree extending T' if T is a U -tree and $T' \subseteq T$. ◇

6.I.6 LEMMA. Let $G = (V, E)$ be a connected graph, let $U \subseteq V$, and let T be a U -tree for G . Let $x, y, y' \in V - U$ such that $d_G(U, y) = d_G(U, y') = d_G(U, x) - 1$, $xy \in T$, and $xy' \in E - T$. Then $T' := (T - xy) \cup xy'$ is a U -tree.

Proof: Let $W \subseteq V$ be the set of vertices of the component containing x in $T - xy$. For all $v \in W$, $d_G(U, v) \geq d_G(U, x)$. Therefore $y' \notin W$ and T' is a spanning tree of $G(A)$. Clearly T' contains a shortest $U - x$ path, from which the result follows. ■

6.I.7 LEMMA. Let A be a connected $X \times Y$ \mathbb{P} -matrix for disjoint sets X, Y , let $U \subseteq X \cup Y$, and let T be a U -tree for $G(A)$. Let $x \in X - U, y, y' \in Y$ be such that $d_{G(A)}(U, y) = d_{G(A)}(U, y') = d_{G(A)}(U, x) - 1$, $xy \in T$, and $xy' \in E(G(A)) - T$. Let W be the set of vertices of the component containing x in $T - xy$. Suppose A is T -normalized. If $A' \sim A$ is $((T - xy) \cup xy')$ -normalized, then $A'[X - W, Y - W] = A[X - W, Y - W]$.

Proof: A' is obtained from A by scaling all rows in $X \cap W$ by $(A_{xy'})^{-1}$ and all columns in $Y \cap W$ by $A_{xy'}$. ■

The following technical lemma deals with 2-separations that may crop up in certain minors of A .

6.I.8 LEMMA. Let \mathbb{P}, \mathbb{P}' be partial fields such that \mathbb{P}' is an induced sub-partial field of \mathbb{P} . Let A be a 3-connected $X \times Y$ \mathbb{P} -matrix, with $X \cap Y = \emptyset$, that has a submatrix $A' = A[V, W]$ such that

- (i) $V = X_0 \cup x_1, W = Y_0 \cup \{y_1, y_2\}$ for some nonempty X_0, Y_0 and $x_1 \in X - X_0, y_1, y_2 \in Y - Y_0$;
- (ii) $A[X_0, Y_0 \cup \{y_1\}]$ is connected;
- (iii) $A[X_0, Y_0 \cup \{y_1\}]$ is a scaled \mathbb{P}' -matrix;
- (iv) A' is not a scaled \mathbb{P}' -matrix;
- (v) $\lambda_{A'}(X_0 \cup Y_0) = 1$.

Then there exists a $\tilde{X} \times \tilde{Y}$ \mathbb{P} -matrix $\tilde{A} \approx A$ with a submatrix $\tilde{A}' = \tilde{A}[\tilde{V}, \tilde{W}]$ such that

- (I) $|\tilde{V}| = |V|, |\tilde{W}| \leq |W|$;
- (II) $X_0 \subset \tilde{V}, Y_0 \subset \tilde{W}$, and $\tilde{A}[X_0, Y_0] = A[X_0, Y_0]$;
- (III) There exists a $\tilde{y}_1 \in \tilde{W} - Y_0$ such that $\tilde{A}[X_0, \tilde{y}_1] \cong A[X_0, y_1]$;
- (IV) \tilde{A}' is not a scaled \mathbb{P}' -matrix;
- (V) $\lambda_{\tilde{A}'}(X_0 \cup Y_0) \geq 2$.

Proof: Let $\mathbb{P}, \mathbb{P}', A, X_0, Y_0, x_1, y_1, y_2$ be as in the lemma. We say that a quadruple $(\tilde{A}, \tilde{x}_1, \tilde{y}_1, \tilde{y}_2)$ is *bad* if $\tilde{A} \approx A$, Conditions (I)–(IV) hold with $\tilde{V} = X_0 \cup \tilde{x}_1$ and $\tilde{W} = Y_0 \cup \{\tilde{y}_1, \tilde{y}_2\}$, but $\lambda_{\tilde{A}}(X_0 \cup Y_0) = 1$. Clearly (A, x_1, y_1, y_2) is a bad quadruple.

Since A is 3-connected, there exists a blocking sequence for the 2-separation $(X_0 \cup Y_0, \{\tilde{x}_1, \tilde{y}_1, \tilde{y}_2\})$ of $\tilde{A}[V, W]$. Suppose $(\tilde{A}, \tilde{x}_1, \tilde{y}_1, \tilde{y}_2)$ was chosen such that the length of a shortest blocking sequence v_1, \dots, v_t is as small as possible. Without loss of generality $(\tilde{A}, \tilde{x}_1, \tilde{y}_1, \tilde{y}_2) = (A, x_1, y_1, y_2)$.

$A[X_0, y_2]$ cannot consist of only zeroes, because otherwise A' could not be anything other than a scaled \mathbb{P}' -matrix. By scaling we may assume that

$$A' = \begin{matrix} & \begin{matrix} Y_0 & y_1 & y_2 \end{matrix} \\ \begin{matrix} X_0 \\ x_1 \end{matrix} & \begin{bmatrix} A_0 & c & c \\ 0 & 1 & p \end{bmatrix} \end{matrix},$$

with X_0, Y_0 nonempty, $p \notin \mathbb{P}'$, $c_i \in \mathbb{P}'$ for all $i \in X_0$, and $c_i = 1$ for some $i \in X_0$. We will now analyse the blocking sequence v_1, \dots, v_t .

Case I. Suppose $v_t \in X$. By Definition 5.3.2(iii) and Lemma 2.4.12 we have $\text{rk}(A[X_0 \cup v_t, \{y_1, y_2\}]) = 2$. If $A_{v_t y_2} = 0$ then $A_{v_t y_1} \neq 0$. Since (A, x_1, y_2, y_1) is a bad quadruple that also has v_1, \dots, v_t as blocking sequence, we may assume that $A_{v_t y_2} \neq 0$. Define $r := A_{v_t y_1}$ and $s := A_{v_t y_2}$. Then $r \neq s$.

Suppose $r/s \notin \mathbb{P}'$. If $t > 1$ then $A_{v_t y} = 0$ for all $y \in Y_0$. But then (A, v_t, y_1, y_2) is again a bad quadruple, and by Lemma 5.3.5, v_1, \dots, v_{t-1} is a blocking sequence for the 2-separation $(X_0 \cup Y_0, \{v_t, y_1, y_2\})$ of $A[X_0 \cup v_t, Y_0 \cup \{y_1, y_2\}]$, contradicting our choice of (A, x_1, y_1, y_2) . If $t = 1$ then there is some $y \in Y_0$ such that $A_{v_t y} \neq 0$. Let \tilde{A} be obtained from A by multiplying row v_t with $(A_{v_t y})^{-1}$. Then $A_{v_t y_i} \notin \mathbb{P}'$ for exactly one $i \in \{1, 2\}$. Then $\tilde{A}, \tilde{V} := X_0 \cup v_t, \tilde{W} := Y_0 \cup y_i$ satisfy (I)–(V).

Therefore $r/s \in \mathbb{P}'$. Consider the matrix \tilde{A} obtained from $A^{x_1 y_2}$ by scaling column y_1 by $(1 - p^{-1})^{-1}$, column x_1 by $-p$, and row y_2 by $(1 - p^{-1})$. Then

$$\tilde{A}[X_0 \cup \{v_t, y_2\}, Y_0 \cup \{y_1, x_1\}] = \begin{matrix} & \begin{matrix} Y_0 & y_1 & x_1 \end{matrix} \\ \begin{matrix} X_0 \\ v_t \\ y_2 \end{matrix} & \begin{bmatrix} A_0 & c & c \\ d & \frac{rp-s}{p-1} & s \\ 0 & 1 & 1-p \end{bmatrix} \end{matrix}.$$

Clearly $(\tilde{A}, y_2, y_1, x_1)$ is a bad quadruple. Suppose $\frac{rp-s}{p-1} = q \in \mathbb{P}'$. Then $(q - r)p = q - s$. But this is only possible if $q - r = q - s = 0$, contradicting the fact that $r \neq s$. The set $\{v_1, \dots, v_t\}$ still forms a blocking sequence of this matrix. Hence we can apply the arguments of the previous case and obtain again a shorter blocking sequence.

Case II. Suppose $v_t \in Y$. Then $A_{x_1 v_t} \neq 0$, again by Definition 5.3.2(iii) and Lemma 2.4.12. Suppose all entries of $A[X_0, v_t]$ are zero. Let \tilde{A} be the matrix obtained from $A^{x_1 y_1}$ by multiplying column y_1 with -1 , column y_2 by $(1 - p)^{-1}$, and row x_1 by -1 . Then $(\tilde{A}, y_1, x_1, y_2)$ is a bad quadruple, v_1, \dots, v_t is a blocking sequence, and $\tilde{A}[X_0, v_t]$ is parallel to $A[X_0, y_1]$. Therefore we may assume that some entry of $A[X_0, v_t]$ is nonzero.

If $A_{x_1 v_t} \in \mathbb{P}'$ then let \tilde{A} be the matrix obtained from A by scaling row x_1 by p^{-1} . Otherwise $\tilde{A} = A$. Then $(\tilde{A}, x_1, y_2, y_1)$ is again a bad quadruple, and v_1, \dots, v_t is still a blocking sequence. Hence we may assume that $A_{x_1 v_t} \notin \mathbb{P}'$. Suppose $t > 1$. Since v_1, \dots, v_{t-1} is not a blocking sequence, we must have $A_{v_{t-1} y_1} = A_{v_{t-1} y_2}$. But then v_1, \dots, v_{t-1} is a blocking sequence for the 2-separation $(X_0 \cup Y_0, \{x_1, y_1, v_t\})$ of $A[X_0 \cup x_1, Y_0 \cup \{y_1, v_t\}]$. But (A, x_1, y_1, v_t) is a bad quadruple, contradicting minimality of v_1, \dots, v_t .

Hence $t = 1$. But then $\text{rk}(A[X_0, \{v_t, y_1, y_2\}]) = 2$ and therefore $A, \tilde{V} := X_0 \cup x_1, \tilde{W} := Y_0 \cup \{y_1, v_t\}$ satisfy (I)–(V). ■

Truemper (1986, Theorem 13.2) and, independently, Geelen et al. (2005) show that, in the worst case, a minimum blocking sequence for a 2-separation has length 5. The difference between that result and Lemma 6.1.8 is that in our case the minor we wish to preserve is contained in one side of the separation.

6.1.2 The proof of Theorem 6.1.3

Proof of Theorem 6.1.3: Let \mathbb{P}, \mathbb{P}' be partial fields such that \mathbb{P}' is an induced sub-partial field of \mathbb{P} , and let D be an $X_0 \times Y_0$ \mathbb{P}' -matrix. We may assume that D is normalized, say with spanning tree T_0 . Note that the theorem holds for A, D if and only if it holds for A^T, D^T . Suppose now that the theorem is false. Then there exists an $X \times Y$ \mathbb{P} -matrix A with the following properties:

- A is 3-connected;
- $X_0 \subseteq X, Y_0 \subseteq Y$, and $D = A[X_0, Y_0]$;
- Neither (i) nor (ii) holds.

We call such a matrix *bad*. The following is clear:

6.1.3.1 CLAIM. *If A is a bad matrix and $\tilde{A} \approx A$ is such that $\tilde{A}[X_0, Y_0] = D$, then \tilde{A} is also bad.*

We say that a triple (A, T, xy) is a *bad triple* if

- A is bad;
- T is an $(X_0 \cup Y_0)$ -tree extending T_0 ;
- A is T -normalized;
- $x \in X, y \in Y$, and $A_{xy} \in \mathbb{P} - \mathbb{P}'$.

Since we assumed the existence of bad matrices, by Lemma 2.3.36 bad triples must also exist.

For $v \in X \cup Y$ we define $d_A(v) := d_{G(A)}(v, X_0 \cup Y_0)$. If xy is an edge of $G(A)$ then $d_A(xy) := \max\{d_A(x), d_A(y)\}$. If xy is an edge of $G(A)$ then $|d_A(x) - d_A(y)| \leq 1$.

6.1.3.2 CLAIM. *There exists a bad triple (A, T, xy) with $d_A(xy) \leq 1$.*

Proof: Let (A, T, xy) be chosen among all bad triples such that $d_A(xy)$ is minimal, and after that such that $|d_A(x) - d_A(y)|$ is maximal. By transposing A, D if necessary we may assume that $d_A(x) \geq d_A(y)$. For $i \geq 1$ we define $X_i := \{x \in X \mid d_A(x) = i\}$ and $Y_i := \{y \in Y \mid d_A(y) = i\}$. We also define $X_i^{\leq} := X_0 \cup \dots \cup X_i$ and $Y_i^{\leq} := Y_0 \cup \dots \cup Y_i$. Suppose $d_A(xy) > 1$. We distinguish two cases.

Case I. Suppose $d_A(x) = d_A(y) = i$. If $X_{i-1} = \emptyset$ then $Y_i = \emptyset$, contradicting our choice of y . Since A is normalized, $A_{xy'} = 1$ for some $y' \in Y_{i-1}$, and $A_{x'y} = 1$ for some $x' \in X_{i-1}$. Let $p := A_{xy}$ and $q := A_{x'y'}$. Then $q \in \mathbb{P}'$.

Let \tilde{A} be the matrix obtained from A^{xy} by multiplying row y with p and column x with $-p$.

Let \tilde{T} be an $(X_0 \cup Y_0)$ -tree extending T_0 in $G(A^{xy})$, such that $uv \in \tilde{T}$ for all $uv \in T[(X - x) \cup Y_{i-2}^{\leq}]$ and all $uv \in T[X_{i-2}^{\leq} \cup (Y - y)]$. By Lemma 6.1.4 such a tree exists. Let $\tilde{A} \sim A^{xy}$ be \tilde{T} -normalized. By Lemma 6.1.4 and Lemma 6.1.7, $\tilde{A}_{x'y'} = (A^{xy})_{x'y'}$. But $\tilde{A}_{x'y'} = q - p^{-1} \notin \mathbb{P}'$, so $(\tilde{A}, \tilde{T}, x'y')$ is a bad triple with $d_{\tilde{A}}(x'y') = i - 1 < i$, a contradiction.

Case II. Suppose $d_A(x) = i + 1$, $d_A(y) = i$. Since A is normalized, $A_{xy'} = 1$ for some $y' \in Y$ with $d_A(y') = i$. If $\text{rk}(A[X_i^{\leq}, \{y', y\}]) = 1$ then we apply Lemma 6.1.8 with $A' = A[X_i^{\leq} \cup x, Y_{i-1}^{\leq} \cup \{y', y\}]$. If $|\tilde{W}| < |W|$ then $\tilde{A}[\tilde{x}_1, Y_0]$ has some nonzero entry. But then $(\tilde{A}, \tilde{T}, \tilde{x}_1\tilde{y}_1)$ would be a bad triple for some $(X_0 \cup Y_0)$ -tree \tilde{T} with $d_{\tilde{A}}(\tilde{x}_1\tilde{y}_1) \leq i$, a contradiction. Therefore $\tilde{W} = Y_0 \cup \{\tilde{y}_1, \tilde{y}_2\}$ for some \tilde{y}_1, \tilde{y}_2 , and $\text{rk}(\tilde{A}[X_0, \{\tilde{y}_1, \tilde{y}_2\}]) = 2$. Now $\tilde{A}[X_0, \tilde{W}]$ must be a scaled \mathbb{P}' -matrix, since $d_{\tilde{A}}(v) \leq i$ for all $v \in X_0 \cup \tilde{W}$.

It follows that we may assume that (A, T, xy) were chosen such that $xy' \in T$ and $\text{rk}(A[X_i^{\leq}, \{y', y\}]) = 2$. Suppose there exists an $x_1 \in X_i^{\leq}$ with $d_A(x_1) = i - 1$ such that $A_{x_1y} \neq 0$ and $A_{x_1y'} \neq 0$. Again by Lemma 6.1.7 we may assume that $x_1y, x_1y' \in T$. Since

$$\text{rk}(A[X'', \{y', y\}]) = 2,$$

there is a row $x_2 \in X_i^{\leq}$ such that

$$A[\{x_1, x_2, x\}, \{y', y\}] = \begin{bmatrix} 1 & 1 \\ r & s \\ 1 & p \end{bmatrix}$$

with $r \neq s$ and $p \in \mathbb{P} - \mathbb{P}'$. Consider A^{xy} . By Lemma 6.1.4 we have $d_{A^{xy}}(x_1) = i - 1$ and $d_{A^{xy}}(y') = i$. By the same lemma, there is a spanning tree T' of $G(A^{xy})$ with $yy', x_1y', x_1x \in T'$ and, for all $u \in X - x$ and $v \in Y$ with $d_{A^{xy}}(v) \leq i - 1$, $uv \in T'$ if and only if $uv \in T$. Let $A' \sim A^{xy}$ be T' -normalized. Then

$$A'[\{x_1, x_2, y\}, \{y', x\}] = \begin{bmatrix} 1 & 1 \\ \frac{pr-s}{p-1} & s \\ 1 & 1-p \end{bmatrix}$$

But $\frac{pr-s}{p-1} \notin \mathbb{P}'$. Therefore (A', T', x_2y') is a bad triple, and $d_{A'}(x_2y') \leq i$, contradicting our choice of (A, T, xy) . Therefore we cannot find an x_1 such that $A_{x_1y'} \neq 0$ and $A_{x_1y} \neq 0$. But in that case there exist x_1, x_2 with $d_A(x_1) = d_A(x_2) = i - 1$ and $A_{x_1y'} \neq 0, A_{x_2y} \neq 0$. Again we may assume without loss of generality that $x_1y', x_2y, xy' \in T$. Then

$$A[\{x_1, x_2, x\}, \{y', y\}] = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & p \end{bmatrix}.$$

Again, consider A^{xy} . By Lemma 6.1.4 we have $d_{A^{xy}}(x_1) = d_{A^{xy}}(x_2) = i - 1$ and $d_{A^{xy}}(y') = i$. By the same lemma, there is a spanning tree T' of $G(A^{xy})$ with $yy', x_1y', x_2x \in T'$ and, for all $u \in X - x$ and $v \in Y$ with $d_{A^{xy}}(v) \leq i - 1$, $uv \in T'$ if and only if $uv \in T$. Let $A' \sim A^{xy}$ be T' -normalized. Then

$$A'[\{x_1, x_2, y\}, \{y', x\}] = \begin{bmatrix} 1 & 0 \\ -p^{-1} & 1 \\ 1 & -p \end{bmatrix}$$

But then (A', T', x_2y') is a bad triple, and $d_{A'}(x_2y') \leq i$, again contradicting our choice of (A, T, xy) . \square

Let (A, T, xy) be a bad triple with $d_A(xy) = 1$.

6.1.3.3 CLAIM. $d_A(x) = d_A(y) = 1$.

Proof: Suppose that $x \in X_0, y \in Y_1$. Let $A' := A[X_0, Y_0 \cup y]$. $A'[X_0, y]$ contains a 1, since y is at distance 1 from D and therefore spanned by T_1 . It also contains an entry equal to p , so it has at least two nonzero entries and cannot be a multiple of a column of D . It follows that A' satisfies the conditions of Case (ii) of the theorem, a contradiction. \square

Therefore $x \in X_1, y \in Y_1$. Consider the submatrix $A' := A[X_0 \cup x, Y_0 \cup y]$. Row $A_{xy_0} = 1$ for some $y_0 \in Y_0$, $A_{x_0y} = 1$ for some $x_0 \in X_0$. Define $b := A[X_0, y]$ and $c := A[x, Y_0]$.

6.1.3.4 CLAIM. Without loss of generality, b is parallel to $A[X_0, y_0]$ for some $y_0 \in Y_0$ and c is a unit vector (i.e. a column of an identity matrix) with $A_{xy_0} = 1$.

Proof: If b is not a unit vector and not parallel to a column of D , then A' satisfies all conditions of Case (ii), a contradiction. If both b and c are unit vectors, and c is such that $A_{xy_0} = 1$, then $A^{xy_0}[X_0, (Y_0 - y_0 \cup x) \cup y]$ satisfies all conditions of Case (ii), a contradiction.

By transposing A, D if necessary we may assume that b is parallel to some column y' of D . We scale column y so that the entries of b are equal to those of $A[X_0, y']$. If c has a nonzero in a column $y_0 \neq y'$, then the matrix $A[X_0, Y_0 - y' \cup y]$ is isomorphic to D , and the matrix $A'' := A[X_0 \cup x, (Y_0 - y') \cup y]$ satisfies all conditions of (ii), a contradiction. \square

Now we apply Lemma 6.1.8 with $A' = A[X_0 \cup x, Y_0 \cup y]$, where $y_1 = y_0$ and $y_2 = y$. But the resulting minor \tilde{A} satisfies all conditions of Case (ii), a contradiction. \blacksquare

6.2 Two corollaries

6.2.1 Whittle's Stabilizer Theorem

Whittle's (1999) Stabilizer Theorem is an easy corollary of the Confinement Theorem.

6.2.1 DEFINITION. Let \mathbb{P} be a partial field, and N a \mathbb{P} -representable matroid on ground set $X' \cup Y'$, where X' and Y' are disjoint, and X' is a basis. Let M be a matroid on ground set $X \cup Y$ with minor N , such that X and Y are disjoint, X is a basis of M , $X' \subseteq X$, and $Y' \subseteq Y$. Let A_1, A_2 be $X \times Y$ \mathbb{P} -matrices such that $M = M[I A_1] = M[I A_2]$. Then N is a \mathbb{P} -stabilizer for M if $A_1[X', Y'] \sim A_2[X', Y']$ implies $A_1 \sim A_2$ for all choices of A_1, A_2 . \diamond

6.2.2 DEFINITION. Let \mathcal{M} be a class of matroids. A matroid N is a \mathbb{P} -stabilizer for \mathcal{M} if it is a \mathbb{P} -stabilizer for each 3-connected $M \in \mathcal{M}$ such that $N \preceq M$. \diamond

6.2.3 THEOREM (Stabilizer Theorem). Let \mathbb{P} be a partial field, and N a 3-connected \mathbb{P} -representable matroid. Let M be a 3-connected \mathbb{P} -representable matroid having an N -minor. Then exactly one of the following is true:

- (i) N stabilizes M ;
- (ii) M has a 3-connected minor M' such that
 - N does not stabilize M' ;
 - N is isomorphic to M'/x , $M' \setminus y$, or $M'/x \setminus y$, for some $x, y \in E(M')$;
 - If N is isomorphic to $M'/x \setminus y$ then at least one of M'/x , $M' \setminus y$ is 3-connected.

Proof: Consider $\mathbb{P}_0 := \mathbb{P} \times \mathbb{P}$, and define $\mathbb{P}'_0 := \{(p, p) \mid p \in \mathbb{P}\}$. Then \mathbb{P}'_0 is an induced sub-partial field of \mathbb{P}_0 , by Lemma 2.2.18. Apply Theorem 6.1.3 to all matrices A, D such that $M = M[I A]$, $N = M[I D]$, $D \preceq A$, A is a \mathbb{P}_0 -matrix, and D is a \mathbb{P}'_0 -matrix. \blacksquare

Geelen et al. (1998) define a *strong stabilizer* as follows:

6.2.4 DEFINITION. Let \mathcal{M} be a class of matroids. We say that N is a *strong \mathbb{P} -stabilizer* for \mathcal{M} if N is a \mathbb{P} -stabilizer, and every representation over \mathbb{P} of N extends to a representation of M , for all 3-connected $M \in \mathcal{M}(\mathbb{P})$ with $N \preceq M$. \diamond

There seems to be no systematic way to test if a stabilizer is strong, except for the following result:

6.2.5 LEMMA. Let N be a stabilizer over \mathbb{P} for \mathcal{M} . If N is uniquely representable over \mathbb{P} then N is strong.

6.2.2 The Settlement Theorem

The following theorem is a close relative of a theorem on totally free expansions of matroids from Geelen et al. (2002, Theorem 2.2). The results in this section build on the theory of universal partial fields from Section 3.3.

6.2.6 DEFINITION. Let M, N be matroids such that $N = M/U \setminus V$ with U independent and V coindependent, and let $\varphi_{M,U,V} : R_N \rightarrow R_M$ be the canonical ring homomorphism. Then N *settles* M if $\varphi_{M,U,V}$ is surjective. \diamond

6.2.7 THEOREM. Let M, N be matroids such that $N = M/U \setminus V$ with U independent and V coindependent. Exactly one of the following is true:

- (i) N settles M ;
- (ii) There exists a 3-connected matroid $M' \preceq M$ such that
 - a) N' does not settle M' ;
 - b) for some $e, f \in E(M')$, N is isomorphic to some $N' \in \{M'/e, M' \setminus f, M'/e \setminus f\}$;
 - c) If $N' = M'/e \setminus f$ then at least one of M'/e and $M' \setminus f$ is 3-connected.

Recall the definition of $\text{Cr}(M)$ from Section 3.3.2.

Proof: Let $\mathbb{P} := \mathbb{P}_M = (R_M, \langle \text{Cr}(M) \cup \{-1\} \rangle)$. Let

$$\mathbb{P}' := (\varphi_{M,U,V}(R_N), \langle \text{Cr}(M) \cup \{-1\} \rangle \cap \varphi_{M,U,V}(R_N)).$$

Then \mathbb{P}' is an induced sub-partial field of \mathbb{P} , by Lemma 2.2.18. Let B be a basis of M with $U \subseteq B$ and T be a spanning forest of $G(M, B)$ extending a spanning forest T' of $G(N, B - U)$. Define $D := \varphi_{M,U,V}(A_{N,B-U,T'})$ and $A := A_{M,B,T}$. By Lemma 3.3.22 $D \preceq A$. The theorem follows if we apply the Confinement Theorem to \mathbb{P}' , \mathbb{P} , D , and A . ■

Like the theory of totally free expansions, Theorem 6.2.7 can be used to show that certain classes of matroids have a bounded number of inequivalent representations. We give one example, which generalizes a result by Whittle (1996) to partial fields.

6.2.8 THEOREM. *Suppose M is a ternary, non-binary matroid representable over a partial field \mathbb{P} . The number of inequivalent representations of M over \mathbb{P} is bounded by $|\mathcal{F}(\mathbb{P})| - 2$.*

Proof: Since M is non-binary, $U_{2,4} \preceq M$. No 3-connected 1-element extension or coextension of $U_{2,4}$ is a minor of M . Hence $U_{2,4}$ settles M . Let B be a basis of M such that $U \subseteq B$, $V \subseteq E - B$, and $M/U \setminus V = U_{2,4}$. Let $\{e_1, e_2, e_3, e_4\}$ be the elements of $U_{2,4}$, with $e_1, e_2 \in B$, and let T be a spanning tree for $G(A_{M,B})$ containing e_1e_3, e_1e_4, e_2e_4 . Suppose A_1, \dots, A_k are inequivalent, T -normalized $B \times (E(M) - B)$ \mathbb{P} -matrices such that $M = M[I A_i]$ for $i = 1, \dots, k$. Then there exist homomorphisms $\varphi_i : \mathbb{P}_M \rightarrow \mathbb{P}$ such that $\varphi_i(\widehat{A}_{M,B,T}) = A_i$. But for each i , φ_i is determined uniquely by the image of

$$\widehat{A}_{M,B,T}[\{e_1, e_2\}, \{e_3, e_4\}] = \begin{bmatrix} 1 & 1 \\ p & 1 \end{bmatrix}.$$

Clearly $\varphi_i(p) \in \mathcal{F}(\mathbb{P}) - \{0, 1\}$. The result follows. ■

6.3 Applications

6.3.1 Ternary matroids

We will combine the Lift Theorem, in particular Theorem 4.3.3, with the Confinement Theorem to prove Theorem 6.C. In fact, Theorem 6.C follows from Theorems 1.2.10, 3.1.7, 4.A, 4.2.2, 4.2.3, 6.B, and the following result:

6.3.1 THEOREM (Whittle, 1997). *Let M be a 3-connected matroid that is representable over $\text{GF}(3)$ and some field that is not of characteristic 3. Then M is representable over at least one of the partial fields $\mathbb{U}_0, \mathbb{U}_1, \mathbb{S}, \mathbb{D}$.*

Proof: Let \mathbb{F} be a field that is not of characteristic 3, and define $\mathbb{P} := \text{GF}(3) \times \mathbb{F}$. Let \mathcal{A} be the set of \mathbb{P} -matrices. An \mathbb{F} -representable matroid M is ternary if and only if $M = M[I A]$ for some $A \in \mathcal{A}$. We study $\mathbb{P}' := \mathbb{L}_{\mathcal{A}}\mathbb{P}$. Since neither $U_{2,5}$ nor $U_{3,5}$ are ternary, $I_{\mathcal{A}}$, as in Definition 4.3.1, is generated by relations (i)–(iv). Consider the set $C := \{\text{Asc}\{\tilde{p}\} \subseteq \mathbb{P}' \mid \tilde{p} \in \tilde{F}_{\mathbb{P}}\}$. Each relation of types (iii), (iv) implies that two elements of $\tilde{F}_{\mathbb{P}}$ are equal. This results either in the identification of two members of C , or in a relation *within* one set of associates.

6.3.1.1 CLAIM. *If $\tilde{p} \in \tilde{F}_{\mathbb{P}}$ then $\mathbb{P}'[\text{Asc}\{\tilde{p}\}]$ is isomorphic to one of $\mathbb{U}_0, \mathbb{U}_1, \mathbb{D}, \mathbb{S}$.*

Proof: If $\tilde{p} \in \{0, 1\}$ then $\mathbb{P}'[\text{Asc}\{\tilde{p}\}] \cong \mathbb{U}_0$, so assume $\tilde{p} \neq 0, 1$. Consider $R := \mathbb{Z}[p_1, \dots, p_6]$. For each $D \subseteq \{(i, j) \mid i, j \in \{1, \dots, 6\}, i \neq j\}$, let I_D be the ideal generated by

- $p_i + p_{i+1} - 1$, for $i = 1, 3, 5$;
- $p_i p_{i+1} - 1$, for $i = 2, 4, 6$ (where indices are interpreted modulo 6);
- $p_i - p_j$, for all $(i, j) \in D$.

By the discussion above, $\mathbb{P}'[\text{Asc}\{\tilde{p}\}] \cong (R/I_D, \langle p_1, \dots, p_6 \rangle)$ for some D . There are only finitely many sets D , so the claim can be proven by a finite check.

If $D = \emptyset$ then $\mathbb{P}'[\text{Asc}\{\tilde{p}\}] \cong \mathbb{U}_1$.

If $|D| = 1$ then we may assume $D = \{(1, j)\}$ for some $j \in \{2, \dots, 6\}$. Elementary manipulations of the ideal show that if $j \in \{2, 4, 6\}$ then $R/I_D \cong \mathbb{Z}[1/2]$, whereas for $j \in \{3, 5\}$, $R/I_D \cong \mathbb{Z}[\zeta]$, where ζ is a root of $x^2 - x + 1 = 0$. We show this for one case, leaving the remaining cases out. Assume $j = 6$. Then $p_1(p_2 p_3 - 1) = p_1((1 - p_1)p_3 - 1) = p_1 p_3 - p_1^2 p_3 - p_1 = p_1 p_3 - p_3 - p_1 \in I_D$, since $p_1^2 = p_1 p_6 = 1$ in R/I_D . Substituting $p_1 + p_3$ for $p_1 p_3$ in $(1 - p_1)p_3 - 1$ yields $-p_1 - 1 \in I$, so $p_1 = p_6 = -1$, and the result follows easily.

If $|D| = 2$ then we may assume $D = \{(1, j), (i, j')\}$ for some $i \in \{1, \dots, 6\}$ and $j, j' \in \{2, \dots, 6\}$. Note that $R/I_D \cong R/I_{\{(1, j)\}}/I_{\{(i, j')\}}$. Checks similar to the previous case show that always $R/I_D \cong \mathbb{Z}[1/2]$ or $R/I_D \cong \mathbb{Z}[\zeta]$ or $R/I_D \cong \text{GF}(3)$. The latter can never occur since we assumed that the \mathbb{P}' -representable matroids are also representable over a field that does not have characteristic 3. In the other cases no new relations are implied, so $I_D = I_{\{(1, j)\}}$. Again we leave out the details.

It follows that no new rings arise for $|D| \geq 2$, and the proof is complete. \square

6.3.1.2 CLAIM. *Suppose $2 \in \mathbb{P}'$. Then each of the following matrices is a \mathbb{D} -confiner in \mathbb{P} :*

$$\begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1/2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}.$$

Proof: Observe that, since there is no $U_{2,5}$ -minor in $\text{GF}(3)$, there exist no ternary 3-connected 1-element extensions or coextensions of these three matrices. Hence the claim must hold by the Confinement Theorem. \square

We immediately have

6.3.1.3 CLAIM. Let $A \in \mathcal{A}$ be 3-connected such that $2 \in \text{Cr}(A)$. Then A is a scaled \mathbb{D} -matrix.

We now solve the remaining case.

6.3.1.4 CLAIM. Let $A \in \mathcal{A}$ be 3-connected such that $2 \notin \text{Cr}(A)$. Then A is a scaled \mathbb{U}_0 -matrix or a scaled \mathbb{U}_1 -matrix or a scaled \mathbb{S} -matrix.

Proof: Without loss of generality assume that A is normalized. Clearly $2 \notin \mathbb{P}'[\text{Cr}(A)]$. Suppose there exists a $\tilde{p} \in \text{Cr}(A) - \{0, 1\}$. Define the sub-partial field $\mathbb{P}'' := \mathbb{P}'[\text{Asc}\{\tilde{p}\}]$. Since all additive relations are restricted to just one set of associates, we have

$$\mathcal{F}(\mathbb{P}'') = \mathcal{F}(\mathbb{P}'[\text{Cr}(A)]) \cap \mathbb{P}''.$$

By the Confinement Theorem, then, we have that $\begin{bmatrix} 1 & 1 \\ p & 1 \end{bmatrix}$ is a \mathbb{P}'' -confiner in $\mathbb{P}'[\text{Cr}(A)]$. The result follows by Claim 6.3.1.1.

Finally, if $\text{Cr}(A) = \{0, 1\}$ then define $\mathbb{P}'' := \mathbb{P}'[\emptyset]$. Clearly $\mathbb{P}'' \cong \mathbb{U}_0$, and the proof of the claim is complete. \square

This completes the proof of the theorem. \blacksquare

A closely related result is the following theorem by Semple and Whittle. We will not give a full proof, since the overlap with the previous proof is considerable.

6.3.2 THEOREM (Semple and Whittle, 1996a). Let M be a 3-connected matroid representable over some field. If M has no $U_{2,5}$ - and no $U_{3,5}$ -minor, then M is either binary or ternary.

Sketch of proof: Let M be a 3-connected, \mathbb{F} -representable matroid with no $U_{2,5}$ - and no $U_{3,5}$ -minor, say $M = M[I A]$. If M has no $U_{2,4}$ -minor then M is binary, by Theorem 1.2.29. Hence we may assume that M does have a $U_{2,4}$ -minor.

Let \mathcal{A} be the set of all minors of A , and define $\mathbb{P}' := \mathbb{L}_{\mathcal{A}}\mathbb{F}$. Then $I_{\mathcal{A}}$ is generated by 4.3.1(i)–(iv). Since there is a homomorphism $\varphi : \mathbb{P}' \rightarrow \mathbb{F}$, the partial field \mathbb{P}' is nontrivial. The further analysis of \mathbb{P}' is the same as the analysis in the proof of Theorem 6.3.1. \blacksquare

6.3.2 Quinary matroids

In this subsection we combine the Lift Theorem, the Confinement Theorem, and the theory of universal partial fields to obtain a detailed description of the representability of 3-connected quinary matroids with a specified number of inequivalent representations over $\text{GF}(5)$. First we deal with those quinary matroids that have no $U_{2,5}$ - and no $U_{3,5}$ -minor.

6.3.3 LEMMA. Each of the following matrices is a \mathbb{D} -stabilizer for the class of dyadic matroids:

$$\begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1/2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}.$$

Proof: Observe that, since there is no $U_{2,5}$ -minor in \mathbb{D} , there exist no 3-connected 1-element extensions or coextensions of these matrices. The result follows from Theorem 6.2.3. ■

Define the following matrices over \mathbb{Q} :

$$A_7 := \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}, \quad A_8 := \begin{bmatrix} 0 & 1 & 1 & 2 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 2 & 1 & 1 & 0 \end{bmatrix}.$$

Then $F_7^- = M[I A_7]$ and $P_8 = M[I A_8]$. Geometric representations for these matroids can be found in Section 3.3.3.

6.3.4 LEMMA. *The following statements hold for $M \in \{F_7^-, (F_7^-)^*, P_8\}$:*

- (i) *M is uniquely representable over \mathbb{D} ;*
- (ii) *M is a stabilizer for \mathbb{D} ;*
- (iii) *\mathbb{D} is a universal partial field for M .*

Proof: Statement (iii) was proven in Theorem 3.3.27. Statement (i) follows from (iii) and Lemma 3.3.15. Statement (ii) follows from Lemma 6.3.3. ■

6.3.5 LEMMA. *Let M be a 3-connected matroid.*

- (i) *If M is regular then M is uniquely representable over every partial field.*
- (ii) *If M is near-regular then M is uniquely representable over \mathbb{U}_1 .*
- (iii) *If M is dyadic but not near-regular and M is representable over a partial field \mathbb{P} then M is uniquely representable over \mathbb{P} .*

Proof: The first result is well-known. For the second result, let M be a \mathbb{U}_1 -representable matroid. Note that for every $p \in \text{Asc}\{\alpha\}$, there is an automorphism $\varphi : \mathbb{U}_1 \rightarrow \mathbb{U}_1$ such that $\varphi(\alpha) = p$. By Lemma 2.2.12, no other automorphisms exist. It follows that $U_{2,4}$ is uniquely representable over \mathbb{U}_1 . An application of Theorem 6.2.3 shows that all \mathbb{U}_1 -representable extensions of $U_{2,4}$ are uniquely representable over \mathbb{U}_1 . If M has no $U_{2,4}$ -minor then M is regular, and we are back in the first case.

For the third result, let M be a dyadic matroid that is not near-regular. The excluded minors for $\mathcal{M}(\mathbb{U}_1)$ were determined by Hall et al. (2009). The only three that are dyadic are F_7^- , $(F_7^-)^*$, and P_8 . Therefore M must have one of these as a minor. From the previous lemma it follows that M is uniquely representable over \mathbb{D} , and that every representation of M over a partial field \mathbb{P} is obtained by a homomorphism $\mathbb{D} \rightarrow \mathbb{P}$. Since $\varphi(1) = 1$ we have $\varphi(2) = \varphi(1) + \varphi(1) = 1 + 1$. Therefore this homomorphism is unique, which completes the proof. ■

6.3.6 THEOREM. *Let M be a 3-connected quinary matroid with no $U_{2,5}$ - and no $U_{3,5}$ -minor. Exactly one of the following holds:*

- (i) *M is regular. In this case M is uniquely representable over $\text{GF}(5)$.*
- (ii) *M is near-regular but not regular. In this case M has exactly 3 inequivalent representations over $\text{GF}(5)$.*

- (iii) M is dyadic but not near-regular. In this case M is uniquely representable over $\text{GF}(5)$.

Proof: Only the second part does not follow directly from the previous theorem. Let $\varphi_2, \varphi_3, \varphi_4$ be homomorphisms $\mathbb{U}_1 \rightarrow \text{GF}(5)$ determined by $\varphi_i(\alpha) = i$. This gives three inequivalent representations over $\text{GF}(5)$. By Theorem 6.2.8 these are all. ■

It follows that we only have to characterize those 3-connected quinary matroids that do have a $U_{2,5}$ - or $U_{3,5}$ -minor. The following lemma is a reformulation of Lemma 4.2.5. Its proof consists of an application of the Stabilizer Theorem.

- 6.3.7 LEMMA (Whittle, 1999). $U_{2,5}$ and $U_{3,5}$ are $\text{GF}(5)$ -stabilizers for the class of quinary matroids.

Now, at long last, the mysterious \mathbb{H}_k partial fields make an appearance. We have already hinted at the following property:

- 6.3.8 THEOREM. Let M be a 3-connected, quinary matroid that has a $U_{2,5}$ - or $U_{3,5}$ -minor, and let $k \in \{1, \dots, 6\}$. The following are equivalent:
- (i) M is representable over \mathbb{H}_k ;
 - (ii) M has at least k inequivalent representations over $\text{GF}(5)$.

First we sketch how to construct the Hydra- k partial fields. For $k = 1$ we pick $\mathbb{H}_1 := \text{GF}(5)$. For $k > 1$ we consider $\mathbb{P}_k := \prod_{i=1}^k \text{GF}(5)$. Let $\varphi_i : \mathbb{P}_k \rightarrow \text{GF}(5)$ be defined by $\varphi_i(x) = x_i$, and let \mathcal{A}_k be the class of 3-connected \mathbb{P}_k -matrices A for which the $\varphi_i(A)$, $i = 1, \dots, k$ are pairwise inequivalent. Then $\mathbb{H}'_k := \mathbb{L}_{\mathcal{A}_k} \mathbb{P}_k$, as in Definition 4.3.1. Let $\psi_k : \mathbb{H}'_k \rightarrow \mathbb{P}_k$ be the canonical homomorphisms. The partial fields \mathbb{H}_k were obtained from the \mathbb{H}'_k by computing a Gröbner basis over the integers for the ideal, choosing a suitable set of generators, and discarding some superfluous generators using the Confinement Theorem.

Let M be a 3-connected matroid having a $U_{2,5}$ - or $U_{3,5}$ -minor, and at least k inequivalent representations over $\text{GF}(5)$. Then $M = M[I A]$ for some \mathbb{P}_k -matrix $A \in \mathcal{A}_k$, and hence M is representable over $\mathbb{L}_{\mathcal{A}_k} \mathbb{P}_k$, by Theorem 4.3.3.

For the converse we cannot rule out a priori that there exists an \mathbb{H}_k -representation A' of $U_{2,5}$ such that $\{\varphi_i(\psi_k(A')) \mid i = 1, \dots, k\}$ contains fewer than k inequivalent representations over $\text{GF}(5)$. To prove that this degeneracy does not occur, one may simply check each normalized \mathbb{H}_k -representation of $U_{2,5}$. This is feasible because all of $\mathbb{H}_1, \dots, \mathbb{H}_6$ have a finite number of fundamental elements.

With this background we proceed with the description of the partial fields and their properties. First Hydra-2. This turns out to be the Gaussian partial field. For convenience we repeat Lemma 4.2.6 and Theorem 4.2.7:

- 6.3.9 LEMMA. Let M be a 3-connected matroid.
- (i) If M has at least 2 inequivalent representations over $\text{GF}(5)$, then M is representable over \mathbb{H}_2 .
 - (ii) If M has a $U_{2,5}$ - or $U_{3,5}$ -minor and M is representable over \mathbb{H}_2 , then M has at least 2 inequivalent representations over $\text{GF}(5)$.

6.3.10 THEOREM. *Let M be a 3-connected matroid with a $U_{2,5}$ - or $U_{3,5}$ -minor. The following are equivalent:*

- (i) *M has 2 inequivalent representations over $\text{GF}(5)$;*
- (ii) *M is \mathbb{H}_2 -representable;*
- (iii) *M has two inequivalent representations over $\text{GF}(5)$, is representable over $\text{GF}(p^2)$ for all primes $p \geq 3$, and over $\text{GF}(p)$ when $p \equiv 1 \pmod{4}$.*

Next up is Hydra-3. Recall from Definition 2.5.23 that $\mathbb{H}_3 = (\mathbb{Q}(\alpha), \langle -1, \alpha, \alpha - 1, \alpha^2 - \alpha + 1 \rangle)$.

6.3.11 LEMMA. *Let M be a 3-connected matroid.*

- (i) *If M has at least 3 inequivalent representations over $\text{GF}(5)$, then M is representable over \mathbb{H}_3 .*
- (ii) *If M has a $U_{2,5}$ - or $U_{3,5}$ -minor and M is representable over \mathbb{H}_3 , then M has at least 3 inequivalent representations over $\text{GF}(5)$.*

Proof: Let $\psi : \mathbb{H}_3 \rightarrow \prod_{i=1}^3 \text{GF}(5)$ be determined by $\psi(\alpha) = (2, 3, 4)$. A finite check shows that for all \mathbb{H}_3 -matrices $A = \begin{bmatrix} 1 & 1 & 1 \\ 1 & p & q \end{bmatrix}$, $|\{\varphi_i(\psi(A)) \mid i = 1, \dots, 3\}| = 3$. Together with Lemma 6.3.7 this proves (ii).

We have $\mathbb{H}'_3 = \mathbb{L}_{\mathcal{A}_3} \prod_{i=1}^3 \text{GF}(5) \cong (\mathbb{Q}(\alpha), \langle -1, 2, \alpha, \alpha - 1, \alpha^2 - \alpha + 1 \rangle)$. Let $\varphi : \mathbb{H}'_3 \rightarrow \prod_{i=1}^3 \text{GF}(5)$ be determined by $\varphi(\alpha) = (2, 3, 4)$ and $\varphi(2) = (2, 2, 2)$. Then $\varphi|_{\mathcal{F}(\mathbb{H}'_3)} : \mathcal{F}(\mathbb{H}'_3) \rightarrow \mathcal{F}(\prod_{i=1}^3 \text{GF}(5))$ is a bijection and by Theorem 4.3.3 and Lemma 6.3.7 all matroids in \mathcal{A}_k are representable over \mathbb{H}'_3 .

Now $\mathbb{D} \subseteq \mathbb{H}'_3$, and $\mathcal{F}(\mathbb{D}) = \mathcal{F}(\mathbb{H}'_3) \cap \mathbb{D}$. Using the Confinement Theorem it can be checked that each of

$$\begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1/2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$$

is a \mathbb{D} -confiner in \mathbb{H}'_3 . Together with Lemma 6.3.5 this proves (i). ■

Next up is Hydra-4. From now on we omit the proofs since no new technicalities arise.

6.3.12 LEMMA. *Let M be a 3-connected matroid.*

- (i) *If M has at least 4 inequivalent representations over $\text{GF}(5)$, then M is representable over \mathbb{H}_4 .*
- (ii) *If M has a $U_{2,5}$ - or $U_{3,5}$ -minor and M is representable over \mathbb{H}_4 , then M has at least 4 inequivalent representations over $\text{GF}(5)$.*

Next up is Hydra-5.

6.3.13 LEMMA. *Let M be a 3-connected matroid.*

- (i) *If M has at least 5 inequivalent representations over $\text{GF}(5)$, then M is representable over \mathbb{H}_5 .*
- (ii) *If M has a $U_{2,5}$ - or $U_{3,5}$ -minor and M is representable over \mathbb{H}_5 , then M has at least 5 inequivalent representations over $\text{GF}(5)$.*

Finally we consider \mathbb{H}_6 . There exists a homomorphism $\varphi : \mathbb{H}_5 \rightarrow \prod_{k=1}^6 \text{GF}(5)$ determined by

$$\varphi(\alpha) = (2, 3, 4, 2, 3, 4),$$

$$\varphi(\beta) = (3, 2, 3, 4, 2, 4),$$

$$\varphi(\gamma) = (3, 2, 3, 4, 4, 2).$$

It turns out that for every \mathbb{H}_5 -representation A' of $U_{2,5}$,

$$|\{\varphi_i(\varphi(A')) \mid i = 1, \dots, 6\}| = 6.$$

Therefore we define

$$\mathbb{H}_6 := \mathbb{H}_5$$

and immediately obtain the following strengthening of Lemma 6.3.13:

6.3.14 LEMMA. *Let M be a 3-connected matroid.*

- (i) *If M has at least 5 inequivalent representations over $\text{GF}(5)$, then M is representable over \mathbb{H}_5 .*
- (ii) *If M has a $U_{2,5}$ - or $U_{3,5}$ -minor and M is representable over \mathbb{H}_5 , then M has at least 6 inequivalent representations over $\text{GF}(5)$.*

We now have all ingredients for the proof of Theorem 6.D from the introduction of this chapter.

Proof of Theorem 6.D: Let M be a 3-connected quinary matroid. By Theorem 6.3.6 all of (i)–(iv) hold when M does not have a $U_{2,5}$ - or $U_{3,5}$ -minor. Therefore we may assume that M does have a $U_{2,5}$ - or $U_{3,5}$ -minor.

Statement (i) follows from Theorem 6.3.10. For statement (ii), let \mathbb{F} be a field, and let $p \in \mathbb{F}$ be an element that is not a root of the polynomials $x, x-1, x^2-x+1$. If $|\mathbb{F}| \geq 5$ then such an element must certainly exist. In that case $\varphi : \mathbb{H}_3 \rightarrow \mathbb{F}$ determined by $\varphi(\alpha) = p$ is a nontrivial homomorphism.

Statement (iv) follows from Lemma 6.3.14. ■

One could suspect that Theorem 6.D(iv) is true by observing that there is a bijection between the representations of $U_{2,5}$ in \mathcal{A}_5 and those in \mathcal{A}_6 . But there seems to be no obvious reason why this bijection should extend to all $A \in \mathcal{A}_5$.

As a final remark we note that the partial fields \mathbb{H}_k possess a large automorphism group, since permutations of coordinates in $\prod_{i=1}^k \text{GF}(5)$ must correspond with automorphisms of \mathbb{H}_k . Our representations of \mathbb{H}_k obscure this fact, but expose other information in return. The automorphism groups will prove useful in Chapter 7.

6.4 Open problems

While the Stabilizer Theorem guarantees that a representation of N extends uniquely to a representation of M , it does not give information on what the representation of M looks like. A positive answer to the following problem would be of interest.

- 6.4.1 **PROBLEM.** Let \mathbb{P} be a partial field such that $\mathcal{F}(\mathbb{P})$ is finite, let $N = M \setminus e$, and let A' be a \mathbb{P} -matrix such that $N = M[I \ A']$. Suppose it is known that M is \mathbb{P} -representable, that N is a \mathbb{P} -stabilizer for M , and that there is a polynomial-time algorithm to evaluate the rank function of M . Is there a polynomial-time algorithm to construct a \mathbb{P} -matrix A such that $M = M[I \ A]$ and $A - e = A'$? \diamond

The following conjecture is related to Conjecture 3.4.5:

- 6.4.2 **CONJECTURE.** *If N is 3-connected then N is a \mathbb{P}_N -stabilizer for the class of \mathbb{P}_N -representable matroids.*

Even if this is only true when N is uniquely \mathbb{P}_N -representable this conjecture would have important implications. For example a theorem by [Geelen et al. \(2006\)](#) would follow immediately and could, in fact, be strengthened.

As mentioned before, the Settlement Theorem is reminiscent of the theory of free expansions from [Geelen et al. \(2002\)](#). We offer the following conjecture:

- 6.4.3 **CONJECTURE.** *Let M be a representable matroid. $M \setminus e$ settles M if and only if e is fixed in M .*

Define the set

$$\xi_{\mathbb{P}} := \{\mathbb{P}_M \mid M \text{ 3-connected, } \mathbb{P}\text{-representable matroid}\}.$$

Whittle's classification, Theorem 6.3.1, amounts to

$$\xi_{\text{GF}(3)} = \{\mathbb{U}_0, \mathbb{U}_1, \mathbb{D}, \mathbb{S}, \text{GF}(3)\}.$$

It is known that $\xi_{\text{GF}(4)}$ is infinite, but it might be possible to determine $\xi_{\mathbb{P}}$ for other partial fields. A first candidate is the golden ratio partial field \mathbb{G} . Unfortunately our proof of Theorem 6.3.1 can not be adapted to this case, since we no longer have control over the set of fundamental elements. We outline a different approach. For all $\mathbb{P}_M \in \xi_{\mathbb{P}}$, there exists a “totally free” matroid $N \preceq M$ that settles M . Moreover, it is known that all totally free \mathbb{P} -representable matroids can be found by an inductive search. Clearly $R_M \cong R_N / I_{N,M}$ for some ideal $I_{N,M}$. The main problem, now, consists of finding the possible ideals $I_{N,M}$.

- 6.4.4 **CONJECTURE.** *If $N = M \setminus e$, N, M are 3-connected, and N settles M , then $I_{N,M}$ is an ideal generated by relations $p - q$, where $p, q \in \text{Cr}(N)$.*

The conjecture holds for all 3-connected 1-element extensions of a 6-element, rank-3 matroid. One example is $N = U_{3,6}$ and $M = \Phi_3^+$, the rank-3 free spike with tip.



Excluded-minor characterizations

RECALL from Section 1.2.4 that Rota’s Conjecture, which is widely regarded as the most important open problem in matroid theory, is as follows.

7.A CONJECTURE (Rota’s Conjecture, [Rota, 1971](#)). *For all prime powers q , $\mathcal{M}(\text{GF}(q))$ can be characterized by a finite set of excluded minors.*

To state a more general conjecture we make the following definition:

7.B DEFINITION. A partial field \mathbb{P} is *finitary* if there exists a partial-field homomorphism $\mathbb{P} \rightarrow \text{GF}(q)$ for some prime power q . \diamond

7.C CONJECTURE. *For every finitary partial field \mathbb{P} , $\mathcal{M}(\mathbb{P})$ can be characterized by a finite set of excluded minors.*

The condition that \mathbb{P} is finitary can not be omitted: \mathbb{R} is a field, and therefore a partial field, yet $\mathcal{M}(\mathbb{R})$ has an infinite number of excluded minors.

At the moment Geelen, Gerards, and Whittle carry out a colossal project aimed at proving that $\mathcal{M}(\text{GF}(q))$ is well-quasi-ordered with respect to the minor-order (see, for instance, [Geelen et al., 2006](#)). That result, when combined with a proof of Conjecture 7.A, would imply Conjecture 7.C, since proper minor-closed classes of $\mathcal{M}(\text{GF}(q))$ would be characterized by a finite set of excluded minors. However, partial fields may play a useful part in proving Conjecture 7.A, since they can be used to get control over inequivalent representations of matroids, an essential ingredient of nearly all excluded-minor proofs known today (Theorem 5.4.10 is an exception). In this chapter we set the stage for a proof of Rota’s Conjecture for $q = 5$, by reducing it to a conjecture that, unlike Rota’s Conjecture, has a plan of attack behind it. Indeed, it should be a consequence of the structure theory being developed for the well-quasi-ordering project.

To state our main result we need a few definitions. One of these is the notion of a strong stabilizer, defined in Section 6.2.1. Another notion is the following.

7.D DEFINITION. Let N, M be matroids. Then M is *N -fragile* if, for all $e \in E(M)$, at least one of $M \setminus e, M/e$ has no minor isomorphic to N . If M is N -fragile and $N \preceq M$ then M is *strictly N -fragile*. \diamond

If \mathbb{P} is a partial field then we denote the class of \mathbb{P} -representable strictly N -fragile matroids by $\mathcal{M}_{N,\mathbb{P}}$.

7.E DEFINITION. N has *bounded canopy* over a partial field \mathbb{P} if there exists an integer l , depending only on N and \mathbb{P} , such that $\text{bw}(M) \leq l$ for all $M \in \mathcal{M}_{N,\mathbb{P}}$. \diamond

The main result of this chapter is the following:

7.F THEOREM. Let \mathbb{P} be a finitary partial field, and let N be a \mathbb{P} -representable matroid such that

- (i) N is 3-connected and non-binary;
- (ii) N is a strong stabilizer for the class of \mathbb{P} -representable matroids;
- (iii) N has bounded canopy over \mathbb{P} .

Then there are finitely many excluded minors for the class of \mathbb{P} -representable matroids having an N -minor.

The proof has been modelled after the proof, by Geelen et al. (2000), of Rota's Conjecture for $q = 4$. Recently Hall et al. (2009) generalized that proof to show that $\mathcal{M}(\mathbb{U}_1)$ can be characterized by a finite number of excluded minors. We will show, in Section 7.3, that both results can be derived from Theorem 7.F. However, both Geelen et al. and Hall et al. prove a much stronger result: they determine the exact set of excluded minors. The bounds involved in the proof of Theorem 7.F are so crude that it is infeasible to derive the set of excluded minors from them.

The condition that N has bounded canopy is needed because our result depends crucially on Theorem 5.4.10. At first it may seem like a rather strong restriction. However, it is expected that, if \mathbb{P} is finitary, every matroid N has bounded canopy over \mathbb{P} . The following is Conjecture 5.9 in Geelen, Gerards, and Whittle (2007).

7.G CONJECTURE. Let N be a $\text{GF}(q)$ -representable matroid. There is an integer l , depending only on N and q , such that, if M is a $\text{GF}(q)$ -representable matroid with $\text{bw}(M) > l$, and $N \preceq M$, then there exists an $e \in E(M)$ for which both $M \setminus e$ and M/e have a minor isomorphic to N .

This chapter is based on joint work with Dillon Mayhew and Geoff Whittle, and a paper containing these results is currently in preparation (Mayhew, Whittle, and Van Zwam, 2009).

7.1 N -fragile matroids

We establish a few basic properties of N -fragile matroids. The following is easy to see from the definition:

7.1.1 **LEMMA.** *If M is N -fragile and $M' \preceq M$ then M' is N -fragile.*

7.1.2 **PROPOSITION.** *Let N be a 3-connected matroid with at least 3 elements, and let M be a strictly N -fragile matroid. Then M is 3-connected up to series and parallel classes.*

Proof: Let M be a counterexample having as few elements as possible. Obviously M has no loops or coloops, and M is connected. Suppose $N = M/S \setminus T$ for an independent set S and a coindependent set T . Let B be a basis of M containing S , and disjoint from T . Now suppose that M has an exact 2-separation (X, Y) .

7.1.2.1 **CLAIM.** *Either $|X \cap E(N)| \leq 1$ or $|Y \cap E(N)| \leq 1$.*

Proof: Let $X' := X \cap E(N)$, and $Y' := Y \cap E(N)$, and suppose both have at least two elements. Then $\lambda_B(X', Y') \leq \lambda_B(X, Y) = 1$, so (X', Y') is a 2-separation of N , a contradiction. \square

We assume that $|Y \cap E(N)| \leq 1$. Define $R := Y \cap E(N)$. By minimality of M we have $Y - R = S \cup T$. We will assume $R \cap B = \emptyset$.

7.1.2.2 **CLAIM.** *$T \neq \emptyset$, and $S \neq \emptyset$.*

Proof: Suppose $S = \emptyset$. Then $B \subseteq X$, and B spans Y . But $\lambda_B(X, Y) = \text{rk}_M(X) + \text{rk}_M(Y) - \text{rk}(M) = 1$, so $\text{rk}_M(Y) = 1$. But then Y is a parallel class, a contradiction.

Suppose $T = \emptyset$. Then $B' := E(M) - B \subseteq X \cup R$. If $R = \emptyset$ then $\text{rk}_{M^*}(X) + \text{rk}_{M^*}(Y) - \text{rk}(M^*) = 1$, so $\text{rk}_{M^*}(Y) = 1$, and Y is a series class, a contradiction. Therefore $R = \{r\}$, say. Now from Definition 5.2.8 it follows that either $\text{rk}_{M/(B-Y)}(X - B) = 0$ or $\text{rk}_{M/(B-X)}(Y - B) = 0$. In the latter case r is a loop in M/S , in the former case each $s \in S$ is in series with r . This contradiction completes the proof. \square

7.1.2.3 **CLAIM.** *M/S has no loops. If $R = \emptyset$ then $M \setminus T$ has no coloops.*

Proof: If $e \in E(M/S)$ is a loop then clearly $e \in T$. But then $(M/S) \setminus e = (M/S)/e$, a contradiction. If $R = \emptyset$ then this argument dualizes to yield the second claim. \square

But now it follows that $R \neq \emptyset$: otherwise both $\text{rk}_{M/(B-Y)}(X - B) > 0$ and $\text{rk}_{M/(B-X)}(Y - B) > 0$, and (X, Y) would not be a 2-separation. Say $R = \{r\}$.

Pick an $s \in S$ and $t \in T$, and define $M' := M_B[X \cup \{r, s, t\}]$. Definition 5.2.8 implies that s is a coloop in $M' \setminus \{r, t\}$. If s is a coloop in $M' \setminus t$ then we are done, so we must have that s and r are in series in $M' \setminus t$. Consider M'/r . $(X, \{t, s\})$ is a 2-separation of M'/r , so either t is a loop or t is in parallel with s . In the former case we can either delete or contract t , a contradiction. In the latter case we can delete s , a contradiction. The result follows. \blacksquare

7.1.3 **DEFINITION.** Let M, N be matroids. Let $e \in E(M)$.

- (i) If M/e has an N -minor then e is N -contractible;
- (ii) If $M \setminus e$ has an N -minor then e is N -deletable;

(iii) If neither $M \setminus e$ nor M/e has an N -minor then e is N -essential. \diamond

We will drop the prefix “ N -” if it is clear from the context which matroid is intended. For readers familiar with the work of Truemper (1992a) this definition may cause some confusion: Truemper defines a *con* element of M as an element such that M/e has no N -minor, and a *del* element as an element such that $M \setminus e$ has no N -minor. The reasoning behind his choice is clear: rather than studying F_7 -fragile binary matroids, he studies *almost regular* binary matroids. Hence losing the minor is a good thing for him. For us N will be a stabilizer, so we want to keep it by all means. We use the following notation:

7.1.4 DEFINITION. Let M, N be matroids.

$$\mathbf{C}_{N,M} := \{e \in E(M) \mid e \text{ is } N\text{-contractible}\};$$

$$\mathbf{D}_{N,M} := \{e \in E(M) \mid e \text{ is } N\text{-deletable}\};$$

$$\mathbf{E}_{N,M} := \{e \in E(M) \mid e \text{ is } N\text{-essential}\}.$$

\diamond

We omit the straightforward proofs of the following two lemmas.

7.1.5 LEMMA. If M is N -fragile, then $\mathbf{C}_{N,M}$, $\mathbf{D}_{N,M}$, $\mathbf{E}_{N,M}$ are pairwise disjoint and partition $E(M)$.

7.1.6 LEMMA. Suppose M is N -fragile. Then $\mathbf{C}_{N^*,M^*} = \mathbf{D}_{N,M}$, $\mathbf{D}_{N^*,M^*} = \mathbf{C}_{N,M}$, and $\mathbf{E}_{N^*,M^*} = \mathbf{E}_{N,M}$.

Taking a minor of M has the following effect on these sets:

7.1.7 LEMMA. Let N, M', M be matroids such that $M' \preceq M$, and such that M' and M are N -fragile.

- (i) If $e \in E(M')$ and $e \in \mathbf{C}_{N,M}$ then $e \in \mathbf{C}_{N,M'} \cup \mathbf{E}_{N,M'}$;
- (ii) If $e \in E(M')$ and $e \in \mathbf{D}_{N,M}$ then $e \in \mathbf{D}_{N,M'} \cup \mathbf{E}_{N,M'}$;
- (iii) If $e \in E(M')$ and $e \in \mathbf{E}_{N,M}$ then $e \in \mathbf{E}_{N,M'}$.

Proof: Suppose the lemma is false. Then, possibly after dualizing and applying Lemma 7.1.6, there exist N -fragile matroids M', M , and an element $e \in E(M') \cap E(M)$ such that $e \in \mathbf{D}_{N,M}$ but $e \notin \mathbf{C}_{N,M'}$. Suppose $M' = M/S \setminus T$. Then

$$M'/e = (M/S \setminus T)/e = (M/e)/S \setminus T.$$

Since M'/e has an N -minor, also M/e has an N -minor, a contradiction with Lemma 7.1.5. \blacksquare

We can delete one element of a parallel pair:

7.1.8 LEMMA. Let N be a 3-connected matroid, and let $M \in \mathcal{M}_{N,\mathbb{P}}$. If $\text{rk}_M(\{e, f\}) = 1$ then e and f are both deletable.

Proof: First we show $f \notin \mathbf{C}_{N,M}$. Indeed: suppose M/f has an N -minor. Now e is a loop of M/f , and hence, by Proposition 7.1.2, not essential. But then both M/e and $M \setminus e$ have an N -minor, a contradiction.

Now suppose $e \in E(N')$, where $N' \cong N$ and $N' = M/S \setminus T$ for sets S, T . Then $f \notin E(N')$, since otherwise f is in parallel with e in N' . It follows that $f \in \mathbf{D}_{N,M}$. But $M \setminus e \cong M \setminus f$. Hence also $e \in \mathbf{D}_{N,M}$ and the result follows. ■

By duality we can contract one element of a series pair:

7.1.9 COROLLARY. *Let N be a 3-connected matroid, and let $M \in \mathcal{M}_{N,\mathbb{P}}$. If $\text{rk}_{M^*}(\{e, f\}) = 1$ then e and f are both contractible.*

7.2 The theorem and its proof

In this section we will prove Theorem 7.F. Our aim is to show that excluded minors having a minor N as in the theorem have bounded branch width, after which we apply Theorem 5.4.10.

7.2.1 Preliminary results

The results in this section are well-known, and easy to prove.

7.2.1 LEMMA. *Let M be an excluded minor for $\mathcal{M}(\mathbb{P})$. Then M^* is an excluded minor for $\mathcal{M}(\mathbb{P})$.*

Proof: By Proposition 2.4.1, M^* is not representable over \mathbb{P} . Suppose there is an $e \in E(M^*)$ such that $M^* \setminus e$ is not \mathbb{P} -representable. Then $(M^* \setminus e)^* = M/e$ is not \mathbb{P} -representable, and M is not an excluded minor, a contradiction. Similarly, M^*/e is \mathbb{P} -representable for all $e \in E(M^*)$, and the result follows. ■

7.2.2 LEMMA. *Let M be an excluded minor for $\mathcal{M}(\mathbb{P})$. Then M is 3-connected.*

Proof: If M has a 2-separation then, by Theorem 2.4.30, $M = M_1 \oplus_2 M_2$ for proper minors M_1, M_2 of M . Since M_1 and M_2 are proper minors, they are \mathbb{P} -representable. But then, by Corollary 2.4.29, also M is \mathbb{P} -representable, a contradiction. ■

7.2.3 LEMMA. *Let M be a finitary partial field, and $r \in \mathbb{N}$. There are finitely many rank- r excluded minors for $\mathcal{M}(\mathbb{P})$.*

Proof: Suppose there is a homomorphism $\varphi : \mathbb{P} \rightarrow \text{GF}(q)$. If M is a \mathbb{P} -representable matroid of rank r , then $M \preceq \text{PG}(r-1, q)$. Hence every 3-connected rank- r matroid on $|E(\text{PG}(r-1, q))| + 1$ elements contains an excluded minor for $\mathcal{M}(\mathbb{P})$. As there are finitely many such matroids, the result follows. ■

We conclude with a basic lemma on the set of bases of a matroid. In Theorem 1.2.5(ii) we chose the element to be removed from the basis B , and were provided with an element to replace it with. It is also possible to specify the element we would like to have in our basis, and then be provided with an element to be removed:

7.2.4 LEMMA (see Oxley, 1992, Lemma 2.1.2). Let M be a matroid with set of bases \mathcal{B} . If $B, B' \in \mathcal{B}$, and $f \in B' - B$, then there exists an $e \in B - B'$ such that $B \Delta \{e, f\} \in \mathcal{B}$.

7.2.2 Deletion pairs and incriminating sets

The results in this section are quite similar to those in Section 4.1.1. Our first ingredient is an easy corollary of a theorem by Whittle (1999). We start by defining a *deletion pair*.

7.2.5 DEFINITION. Let M be a matroid having an N -minor. Then $\{u, v\} \subseteq E(M)$ is a *deletion pair preserving N* if $M \setminus \{u, v\}$ is connected, and $\text{co}(M \setminus u)$, $\text{co}(M \setminus v)$, $\text{co}(M \setminus \{u, v\})$ are 3-connected and have an N -minor. \diamond

A deletion pair is guaranteed to exist, provided that M is sufficiently large:

7.2.6 THEOREM (Whittle, 1999, Theorem 3.2). Let M, N be matroids such that $N \preceq M$, $\text{rk}(M) - \text{rk}(N) \geq 3$, and both M and N are 3-connected. If there exists a $u \in E(M)$ such that $\text{si}(M/u)$ is 3-connected and has an N -minor, then there exists a $v \in E(M)$, $v \neq u$, such that $\text{si}(M/v)$ and $\text{si}(M/\{u, v\})$ are both 3-connected, and $\text{si}(M/\{u, v\})$ has an N -minor.

7.2.7 COROLLARY. Let M and N be 3-connected matroids, with $N \preceq M$, and suppose M is not a wheel or a whirl. If $\text{rk}(M) - \text{rk}(N) \geq 3$ and $\text{rk}(M^*) - \text{rk}(N^*) \geq 3$, then for some $(M', N') \in \{(M, N), (M^*, N^*)\}$, M' has a deletion pair $\{u, v\}$ preserving N' . Moreover, $\{u, v\}$ can be chosen such that $M \setminus u$ is 3-connected.

Proof: By the Splitter Theorem there is a $u \in E(M)$ such that either $M \setminus u$ is 3-connected with an N -minor, or M/u is 3-connected with an N -minor. Using duality we may assume, without loss of generality, that the former holds. Then the dual of Theorem 7.2.6 implies the existence of a $v \in E(M) - u$ such that $\text{co}(M \setminus v)$ and $\text{co}(M \setminus \{u, v\})$ are 3-connected with an N -minor. To ensure that $\{u, v\}$ is a deletion pair we need to prove that $M \setminus \{u, v\}$ is connected. But $M \setminus \{u, v\} = (M \setminus u) \setminus v$, and since $M \setminus u$ is 3-connected, Corollary 5.2.5 implies that $M \setminus \{u, v\}$ is 2-connected. ■

In the remainder of this section \mathbb{P} will be a partial field, N will be a 3-connected \mathbb{P} -representable matroid that is a strong \mathbb{P} -stabilizer for $\mathcal{M}(\mathbb{P})$, M will be a 3-connected matroid, and $\{u, v\} \subseteq E(M)$ a deletion pair preserving N .

Next we employ the deletion pair to create a candidate \mathbb{P} -representation for M . The precise formulation of the following theorem is somewhat involved. Informally, the theorem says that, if M is a 3-connected matroid such that $M \setminus u$, $M \setminus v$, and $M \setminus \{u, v\}$ are connected and \mathbb{P} -representable with a strong stabilizer N as minor, then there is a matrix A such that, if M were \mathbb{P} -representable, then A would be a representation.

7.2.8 THEOREM. Let D be a \mathbb{P} -matrix such that $N = M[ID]$. Let B be a basis of $M \setminus \{u, v\}$, and let $E_N \subseteq E(M) - \{u, v\}$ be such that $M_B[E_N] = N$. Suppose $M \setminus u$ and $M \setminus v$ are \mathbb{P} -representable. Then there is a $B \times (E(M) - B)$ matrix A with entries in \mathbb{P} such that

- (i) $A - u$ and $A - v$ are \mathbb{P} -matrices;
- (ii) $M[I(A - u)] = M \setminus u$ and $M[I(A - v)] = M \setminus v$;

(iii) $A[E_N] \sim D$.

Moreover, A is unique up to scaling of rows and columns.

Proof: Suppose D, B, E_N are as in the theorem. Let T be a spanning tree for $G(M, B)$ having u and v as leaves. T exists since $\{u, v\}$ is a deletion pair. Since N is a strong \mathbb{P} -stabilizer, there is a unique $(T - u)$ -normalized \mathbb{P} -matrix A' such that $A'[E_N] \sim D$ and $M \setminus u = M[I A']$, and a unique $(T - v)$ -normalized \mathbb{P} -matrix A'' such that $A''[E_N] \sim D$ and $M \setminus v = M[I A'']$. Since N is a strong \mathbb{P} -stabilizer, also $A' - u = A'' - v$. Now let A be the matrix obtained from A' by appending column $A''[B, v]$. Then A satisfies all properties of the theorem. Uniqueness follows from Lemma 4.1.10. ■

For most of the time we will apply Theorem 7.2.8 to matroids that are not \mathbb{P} -representable. Hence the matrix A will not represent M . If a matrix does not represent a matroid, then it must have one of three problems, described by the next definition.

7.2.9 DEFINITION. Let B be a basis of M , and let A be a $B \times (E(M) - B)$ matrix with entries in \mathbb{P} . A set $Z \subseteq E(M)$ *incriminates* the pair (M, A) if one of the following holds:

- (i) $\det(A[Z]) \notin \mathbb{P}$;
- (ii) $\det(A[Z]) = 0$ but $B \Delta Z$ is a basis of M ;
- (iii) $\det(A[Z]) \neq 0$ but $B \Delta Z$ is dependent in M . ◇

The proof of the following lemma is obvious, and therefore omitted.

7.2.10 LEMMA. Let A be an $X \times Y$ matrix, where X and Y are disjoint, and $X \cup Y = E(M)$. Exactly one of the following statements is true:

- (i) A is a \mathbb{P} -matrix and $M = M[I A]$;
- (ii) Some $Z \subseteq X \cup Y$ incriminates (M, A) .

For the remainder of this section we will assume that A is an $X \times Y$ matrix with entries in \mathbb{P} such that X and Y are disjoint, and $X \cup Y = E(M)$ and $u, v \in Y$.

It is often desirable to have a small incriminating set. If we have some information about minors of A then this can be achieved by pivoting.

7.2.11 THEOREM. Suppose $A - u, A - v$ are \mathbb{P} -matrices, and $M \setminus u = M[I(A - u)]$, $M \setminus v = M[I(A - v)]$. Suppose $Z \subseteq X \cup Y$ incriminates (M, A) . Then there exists an $X' \times Y'$ matrix A' , and $a, b \in X'$, such that $u, v \in Y'$, $A - u \approx A' - u$, $A - v \approx A' - v$, and $\{a, b, u, v\}$ incriminates (M, A') .

Proof: Suppose the theorem is false. Let X, Y, A, u, v, M, Z form a counterexample, and suppose the counterexample was chosen such that $|Z \cap Y|$ is minimal. Clearly $u, v \in Z$. Suppose $y \in Z$ for some $y \in Y - \{u, v\}$.

7.2.11.1 CLAIM. Some entry of $A[X \cap Z, y]$ is nonzero.

Proof: Suppose all entries of $A[X \cap Z, y]$ equal zero. Then $\det(A[Z]) = 0$. Since Z incriminates (M, A) , this implies that $X \triangle Z$ is a basis of M . Now Theorem 7.2.4 implies that, for some $x \in Z \cap X$, $B := X \triangle \{x, y\}$ is a basis of M . But since $u, v \notin B$, B is also a basis of $M \setminus \{u, v\}$. Since $M \setminus u = M[I(A - u)]$, this implies that $A_{xy} \neq 0$, a contradiction. \square

Now let $X' := X \triangle \{x, y\}$, $Y' := Y \triangle \{x, y\}$, $A' := A^{xy}$, and $Z' := Z - \{x, y\}$. Since $A^{xy} - u = (A - u)^{xy}$, $A - u$ is a \mathbb{P} -matrix, and $M \setminus u = M[I(A' - u)]$. Likewise $A - v$ is a \mathbb{P} -matrix, and $M \setminus v = M[I(A' - v)]$.

7.2.II.2 CLAIM. Z' incriminates (M, A') .

Proof: Note that $\det(A'[Z']) = \pm A_{xy}^{-1} \det(A[Z])$. Hence $\det(A'[Z']) \in \mathbb{P}$ if and only if $\det(A[Z]) \in \mathbb{P}$, and $\det(A'[Z']) = 0$ if and only if $\det(A[Z]) = 0$. The result follows easily after observing that $X' \triangle Z' = X \triangle Z$. \square

But $Z' \cap Y' = (Z \cap Y) - y$, contradicting minimality of $|Z \cap Y|$. \blacksquare

For the remainder of this section we assume $A - u$, $A - v$ are \mathbb{P} -matrices, and $M \setminus u = M[I(A - u)]$, $M \setminus v = M[I(A - v)]$. We also assume that $a, b \in X$ are such that $\{a, b, u, v\}$ incriminates (M, A) .

Pivots were used to create a small incriminating set, but they may destroy it too. We identify some pivots that don't.

7.2.I2 DEFINITION. If $x \in X, y \in Y - \{u, v\}$ are such that $A_{xy} \neq 0$, then a pivot over xy is *allowable* if there are $a', b' \in X \triangle \{x, y\}$ such that $\{a', b', u, v\}$ incriminates (M, A^{xy}) . \diamond

7.2.I3 LEMMA. If $x \in \{a, b\}, y \in Y - \{u, v\}$ are such that $A_{xy} \neq 0$, then $\{a, b, u, v\} \triangle \{x, y\}$ incriminates (M, A^{xy}) .

Proof: By symmetry we may assume $x = a$. Let $Z := \{a, b, u, v\}$ and $Z' := \{y, b, u, v\}$. First suppose $\det(A[Z]) \notin \mathbb{P}$, but $\det(A^{ay}[Z']) \in \mathbb{P}$. Then $A^{ay}[Z \cup y]$ is a \mathbb{P} -matrix. Indeed: all entries are in \mathbb{P} , $\det(A^{ay}[\{y, b, a, u\}]) \in \mathbb{P}$, and $\det(A^{ay}[\{y, b, a, v\}]) \in \mathbb{P}$. This is clearly impossible, since $(A^{ay})^{ya} \sim A$, after which Proposition 2.3.16 implies that A is a \mathbb{P} -matrix. Hence $\det(A^{ay}[Z']) \notin \mathbb{P}$, and the lemma follows.

Next suppose $\det(A[Z]) = 0$, and $X \triangle Z$ is a basis of M . Consider $M' := M_X[Z \cup y]$. Since $\det(A[Z]) \in \mathbb{P}$, $A[Z \cup y]$ is a \mathbb{P} -matrix. Let $N' := M[I(A[Z \cup y])]$. We have $N' \neq M'$, since $\{u, v\}$ is a basis of M' yet dependent in N' . But since $\{u, v\}$ is dependent in N' , we have $\det(A^{ay}[Z']) = 0$. Since $X \triangle Z = (X \triangle \{a, y\}) \triangle Z'$, the lemma follows.

The final case, where $\det(A[Z]) \in \mathbb{P}^*$ and $B \triangle Z$ is dependent in M , is similar to the second and we omit the proof. \blacksquare

7.2.I4 LEMMA. If $x \in X - \{a, b\}, y \in Y - \{u, v\}$ are such that $A_{xy} \neq 0$, and either $A_{xu} = A_{xv} = 0$, or $A_{ay} = A_{by} = 0$, then $\{a, b, u, v\}$ incriminates (M, A^{xy}) .

Proof: Let $Z := \{a, b, u, v\}$, and define $X' := X \triangle \{x, y\}$. Since $A^{xy}[Z] = A[Z]$, we have $\det(A^{xy}[Z]) \in \mathbb{P}$ if and only if $\det(A[Z]) \in \mathbb{P}$. Therefore we only need to prove the two cases where $\det(A[Z]) \in \mathbb{P}$. Define $M' := M_X[Z \cup \{x, y\}]$.

7.2.14.1 CLAIM. x and y are either in series or in parallel in M' .

Proof: If $A_{ay} = A_{by} = 0$ then x and y are clearly in parallel, since they are in parallel in $M' \setminus v = M[IA[\{x, a, b, y, u\}]]$. Now assume $A_{xu} = A_{xv} = 0$. If x and y are not in series, then $\{x, y, z\}$ is a cobasis of M' for some $z \in Z$. Clearly $\{y, u, v\}$ is a cobasis of M' , so Theorem 7.2.4 implies that $\{x, y, u'\}$ is a cobasis of M' for some $u' \in \{u, v\}$. Without loss of generality, assume $u' = u$. But then a pivot over xv should be possible in $M' \setminus u = M[IA[\{x, a, b, y, v\}]]$, contradicting $A_{xv} = 0$. \square

But now it follows from Proposition 5.1.4(iii) and the dual statement of Proposition 5.1.4(iv) that $\{x, u, v\}$ is a basis of M' if and only if $\{y, u, v\}$ is a basis of M' , and hence that $X \triangle Z$ is a basis of M if and only if $X' \triangle Z$ is a basis of M , and the lemma follows. \blacksquare

The next theorem gives sufficient conditions under which a certain minor of M can be shown to be non- \mathbb{P} -representable.

7.2.15 THEOREM. Suppose $C \subseteq E(M)$ is such that $M_X[C]$ is strictly N -fragile. If there exist subsets $Z, Z_1, Z_2 \subseteq E(M)$ such that

- (i) $u \in Z_1 - Z_2, v \in Z_2 - Z_1$;
 - (ii) $C \cup \{a, b\} \subseteq Z \subseteq Z_1 \cap Z_2$;
 - (iii) $M_X[Z]$ is connected;
 - (iv) $M_X[Z_1]$ is 3-connected up to series and parallel classes;
 - (v) $M_X[Z_2]$ is 3-connected up to series and parallel classes;
 - (vi) $\{a, b, u, v\}$ incriminates $(M_X[Z_1 \cup Z_2], A[Z_1 \cup Z_2])$;
- then $M_X[Z_1 \cup Z_2]$ is not \mathbb{P} -representable.

Proof: Let C, Z_1 , and Z_2 be as in the theorem. Suppose that, contrary to the result claimed, $M_X[Z_1 \cup Z_2]$ is \mathbb{P} -representable, say $M_X[Z_1 \cup Z_2] = M[IA']$, where A' is an $(X \cap (Z_1 \cup Z_2)) \times (Y \cap (Z_1 \cup Z_2))$ \mathbb{P} -matrix. Since N is a strong stabilizer for $\mathcal{M}(\mathbb{P})$, we may assume that $A'[C] = A[C]$. But then $A'[Z_1] \sim A[Z_1]$, and $A'[Z_2] \sim A[Z_2]$. Since $Z \subseteq Z_1 \cap Z_2$, also $A'[Z \cup u] \sim A[Z \cup u]$ and $A'[Z \cup v] \sim A[Z \cup v]$. Since $M_X[Z]$ is connected, it follows from Lemma 4.1.10 that $A'[Z \cup \{u, v\}] \sim A[Z \cup \{u, v\}]$. But then $\text{Cr}(A'[\{a, b, u, v\}]) = \text{Cr}(A[\{a, b, u, v\}])$, and hence $\{a, b, u, v\}$ incriminates $(M_X[Z_1 \cup Z_2], A')$, a contradiction. \blacksquare

7.2.3 The proof of Theorem 7.F

Now we are equipped to prove Theorem 7.F, which we repeat here for convenience.

7.2.16 THEOREM. Let \mathbb{P} be a finitary partial field, and let N be a \mathbb{P} -representable matroid such that

- (i) N is 3-connected and non-binary;

(ii) N is a strong stabilizer for the class of \mathbb{P} -representable matroids;

(iii) N has bounded canopy over \mathbb{P} .

Then there are finitely many excluded minors for the class of \mathbb{P} -representable matroids having an N -minor.

The proof can be summarized as follows. First, we pick a big excluded minor having an N -minor, and select a deletion pair $\{u, v\}$, and a small incriminating set, $\{a, b, u, v\}$. Then we identify a 3-connected N -fragile minor M' of $M \setminus \{u, v\} / \{a, b\}$. Now $\{u, v\}$ may not be a deletion pair for M' since the connectivity of $\text{co}(M' \setminus u)$, $\text{co}(M' \setminus v)$, $\text{co}(M' \setminus \{u, v\})$ may be too low. We count the 1- and 2-separations, and find that the number does not depend on N or \mathbb{P} . But then only a constant number of blocking sequences is needed, and the branch width of the final product is removed from the branch width of the N -fragile matroid by an additive constant.

Proof: Fix a finitary partial field \mathbb{P} and strong \mathbb{P} -stabilizer N . If for all excluded minors M having an N -minor we have $\min\{\text{rk}(M) - \text{rk}(N), \text{rk}(M^*) - \text{rk}(N^*)\} < 3$, then Lemma 7.2.1 and Lemma 7.2.3 imply that the theorem holds. Hence we may assume that there exists an excluded minor, M say, for $\mathcal{M}(\mathbb{P})$ such that $\text{rk}(M) - \text{rk}(N) \geq 3$, $\text{rk}(M^*) - \text{rk}(N^*) \geq 3$, and $N \preceq M$. Let E be the ground set of M . By Corollary 7.2.7, some $M' \in \{M, M^*\}$ has a deletion pair $\{u, v\}$ such that $M' \setminus u$ is 3-connected. By swapping N with N^* and M with M^* if necessary, we may assume $M' = M$. Let B be a basis of M , and $E_N \subseteq E - \{u, v\}$, such that $M_B[E_N] \cong N$. Fix a strongly stabilizing representation D of N , and let A' be the matrix described in Theorem 7.2.8.

Since M is not \mathbb{P} -representable, some $S \subseteq E$ incriminates (M, A') . Clearly $u, v \in S$. By Theorem 7.2.11, there exists an $X \times Y$ matrix $A \approx A'$ such that $a, b \in X$, $u, v \in Y$, and $\{a, b, u, v\}$ incriminates (M, A) . By Proposition 2.3.28, A is unique up to scaling.

Let $C \subseteq E - \{u, v\}$ be an inclusionwise minimal set such that $M_X[C]$ has an N -minor.

7.2.16.1 CLAIM. $M_X[C]$ is 3-connected.

Proof: For all $x \in C$, $M_X[C - x]$ has no N -minor. Hence, if $x \in C \cap X$ then $x \notin \mathbf{C}_{N,M}$, and if $x \in C \cap Y$ then $x \notin \mathbf{D}_{N,M}$. It follows that $M_X[C]$ is strictly N -fragile. Clearly $M_X[C]$ has no loops or coloops. By Proposition 7.1.2, $M_X[C]$ is 3-connected up to series and parallel classes. Suppose $M_X[C]$ is not 3-connected, and let $\{e, f\}$ be a parallel pair. By Lemma 7.1.8, $e, f \in \mathbf{D}_{N,M}$. Since X is a basis of M and $\text{rk}_M(\{e, f\}) = 1$, $|X \cap \{e, f\}| \leq 1$, say $f \notin X$. But then $N \preceq M_X[C - f]$, a contradiction. \square

We now refine the choice of our small incriminating set, as follows:

7.2.16.2 ASSUMPTION. X, a, b, C were chosen such that $(d_X(a, C), d_X(b, C))$ is lexicographically minimal.

We now start constructing sets Z, Z_1, Z_2 satisfying the properties of Theorem 7.2.15.

7.2.16.3 CLAIM. *There exists a set $Z \subseteq E - \{u, v\}$, with $C \cup \{a, b\} \subseteq Z$, such that $M_X[Z]$ is connected. Moreover, $|Z| \leq |C| + 8$.*

Proof: Let P_a be a shortest $a - C$ path in $G(M, X)$, and suppose $|P_a| = k > 3$, say $P_a = (a, x_1, x_2, x_3, \dots, x_k)$, where $x_k \in C$. Then x_2 labels a row of A , $A_{x_2c} = 0$ for all $c \in C$, and $A_{ax_3} = A_{bx_3} = 0$. It follows that a pivot over x_2x_3 is allowable and $A^{x_2x_3}[C] = A[C]$. However, $d_{X \triangle \{x_2, x_3\}}(a, C) < d_X(a, C)$, a contradiction to Assumption 7.2.16.2.

Similarly, if P_b is a shortest $b - (C \cup P_a)$ path, then $|P_b| \leq 3$. Now $M_X[C \cup P_a \cup P_b]$ is connected, and the result follows. \square

Let Z be as in Claim 7.2.16.3. Note that $\text{bw}(M_X[Z]) \leq \text{bw}(M_X[C]) + 8$, by Proposition 5.4.8. Since $\{u, v\}$ is a deletion pair, $\text{co}(M \setminus v)$ is 3-connected.

7.2.16.4 CLAIM. *There is a set $S \subseteq (X - Z) \cup \{a, b\}$ such that $M_X[E - (S \cup v)]$ is 3-connected and isomorphic to $\text{co}(M \setminus v)$.*

Proof: Let S_1 be a series class in $M \setminus v$. At most one element of S_1 is not in X . It follows that we can obtain a matroid isomorphic to $\text{co}(M \setminus v)$ by contracting only elements from X . Let $S \subset X$ be such that $\text{co}(M \setminus v) \cong M/S \setminus v$, and suppose S was chosen such that $|S \cap (Z - \{a, b\})|$ is minimal. Let $x \in (X - (C \cup \{a, b\})) \cap Z$. Then x is in a shortest $a - C$ path or in a shortest $b - C$ path. In either case $A[x, Y - v]$ has at least two nonzero entries. Likewise, if $x \in X \cap C$ then $A[x, Y - v]$ has at least two nonzero entries, since $M_X[C]$ is 3-connected. It follows that, if $x \in (Z - \{a, b\}) \cap S$, then also $y \in X$ for all y such that x, y are in series. Clearly $y \notin Z - \{a, b\}$, as $M_X[Z - \{a, b\}]$ has no series classes. There is such a y that is not in S . But then $M_X[Z - (S \cup v)] \cong M_X[Z - (S \triangle \{x, y\} \cup v)]$, contradicting minimality of $|S \cap (Z - \{a, b\})|$. \square

Let S be as in Claim 7.2.16.4.

7.2.16.5 CLAIM. *Let $Z'_0 \subseteq E - (v \cup S)$ be such that $(Z - S) \cup u \subseteq Z'_0$, and such that $M_X[Z'_0]$ has exactly k distinct 2-separations. Then there exists a set $Z_0 \subseteq E - (v \cup S)$ such that $Z_0 \supseteq Z'_0$, $M_X[Z_0]$ is 3-connected, and $\text{bw}(M_X[Z_0]) \leq \text{bw}(M_X[Z'_0]) + 2k$.*

Proof: The result is obvious if $k = 0$, so we suppose $k > 0$. Since $M_X[Z'_0]$ is a minor of the 3-connected matroid $M/S \setminus v$, no 2-separation of $M_X[Z'_0]$ is induced. Since N is non-binary, $U_{2,4} \preceq N$. It then follows from Lemma 5.4.12 and Proposition 5.4.8 that $\text{bw}(M_X[Z'_0]) \geq 3$. Therefore, by Lemma 5.5.4, $M_X[Z'_0]$ has an uncrossed 2-separation, say (W_1, W_2) . Let v_1, \dots, v_t be a blocking sequence for (W_1, W_2) . By Theorem 5.4.11, $\text{bw}(M_X[Z'_0 \cup \{v_1, \dots, v_t\}]) \leq \text{bw}(M_X[Z'_0]) + 2$. By Corollary 5.5.7, $M_X[Z'_0 \cup \{v_1, \dots, v_t\}]$ has $k' < k$ 2-separations. The result now follows by induction. \square

Pick $Z'_0 = (Z - S) \cup u$. Then $|Z'_0| - |C| \leq 9$, by Claim 7.2.16.3. By Lemma 5.2.14, $M_X[Z'_0]$ has at most 2^{9+1} distinct 2-separations. Then Claim 7.2.16.5 proves the existence of a set $Z_0 \supseteq Z'_0$ such that $M_X[Z_0]$ is 3-connected, and $\text{bw}(M_X[Z_0]) \leq \text{bw}(M_X[Z'_0]) + 2 \cdot 2^{9+1}$.

Define $Z_1 := Z_0 \cup \{a, b\}$. For all $x \in S \cap \{a, b\}$, $Z_0 \cup x$ is either 3-connected or has a series pair. It follows that $M_X[Z_1]$ is 3-connected up to series classes. Also, $\text{bw}(M_X[Z_1]) \leq \text{bw}(M_X[Z_0]) + 2$.

7.2.16.6 CLAIM. Let $Z'_2 \subseteq E - u$ be such that $Z \cup v \subseteq Z'_2$, and such that $M_X[Z'_2]$ has exactly k distinct 2-separations. Then there exists a set $Z_2 \subseteq E - u$ such that $Z_2 \supseteq Z'_2$, $M_X[Z_2]$ is 3-connected, and $\text{bw}(M_X[(Z_1 - u) \cup Z_2]) \leq \text{bw}(M_X[(Z_1 - u) \cup Z'_2]) + 2k$.

Proof: The result is obvious if $k = 0$, so we suppose $k > 0$. Since $M_X[Z'_2]$ is a minor of the 3-connected matroid $M \setminus u$, no 2-separation of $M_X[Z'_2]$ is induced. Again $\text{bw}(M_X[Z'_2]) \geq 3$, so $M_X[Z'_2]$ has an uncrossed 2-separation, say (W_1, W_2) . If (W_1, W_2) is bridged in $M_X[(Z_1 - u) \cup Z'_2]$ then we set $T = \emptyset$. Otherwise let (W'_1, W'_2) be a 2-separation of $M_X[(Z_1 - u) \cup Z'_2]$ such that $W_1 \subseteq W'_1$ and $W_2 \subseteq W'_2$. Let $v'_1, \dots, v'_{p'}$ be a blocking sequence for (W'_1, W'_2) , and set $T := \{v'_1, \dots, v'_{p'}\}$.

Now (W_1, W_2) is bridged in $M_X[(Z_1 - u) \cup Z'_2 \cup T]$, so there is a blocking sequence v_1, \dots, v_t contained in $Z_1 - u \cup T$. By Theorem 5.4.11, $\text{bw}(M_X[(Z_1 - u) \cup Z'_2 \cup \{v_1, \dots, v_t\}]) \leq \text{bw}(M_X[(Z_1 - u) \cup Z'_2 \cup T]) \leq \text{bw}(M_X[(Z_1 - u) \cup Z'_2]) + 2$. By Corollary 5.5.7, $M_X[(Z_1 - u) \cup Z'_2 \cup \{v_1, \dots, v_t\}]$ has $k' < k$ 2-separations. The result now follows by induction. \square

Pick $Z'_2 := Z \cup v$. Then $|Z'_2| - |C| \leq 9$, by Claim 7.2.16.3. By Lemma 5.2.14, $M_X[Z'_2]$ has at most 2^{9+1} distinct 2-separations. Then Claim 7.2.16.6 proves the existence of a set $Z_2 \supseteq Z'_2$ such that $M_X[Z_2]$ is 3-connected, and $\text{bw}(M_X[Z_1 \cup Z_2]) \leq \text{bw}(M_X[(Z_1 - u) \cup Z'_2]) + 1 \leq \text{bw}(M_X[(Z_1 - u) \cup Z'_2]) + 2 \cdot 2^{9+1} + 1$.

It now follows from Theorem 7.2.15 that $M_X[Z_1 \cup Z_2]$ is not \mathbb{P} -representable. But M is an excluded minor for $\mathcal{M}(\mathbb{P})$, so we must have $M = M_X[Z_1 \cup Z_2]$. Since N has bounded canopy, there is a constant, l say, such that all strictly N -fragile \mathbb{P} -representable matroids have branch width at most l . By liberal application of Proposition 5.4.8 we can now deduce

$$\text{bw}(M) = \text{bw}(M_X[Z_1 \cup Z_2]) \quad (7.1)$$

$$\leq \text{bw}(M_X[(Z_1 - u) \cup Z_2]) + 1 \quad (7.2)$$

$$\leq \text{bw}(M_X[(Z_1 - u) \cup Z'_2]) + 2 \cdot 2^{9+1} + 1 \quad (7.3)$$

$$\leq \text{bw}(M_X[Z_1 - u]) + 2 \cdot 2^{9+1} + 2 \quad (7.4)$$

$$\leq \text{bw}(M_X[Z_1]) + 2 \cdot 2^{9+1} + 2 \quad (7.5)$$

$$\leq \text{bw}(M_X[Z_0]) + 2 \cdot 2^{9+1} + 4 \quad (7.6)$$

$$\leq \text{bw}(M_X[Z'_0]) + 4 \cdot 2^{9+1} + 4 \quad (7.7)$$

$$\leq \text{bw}(M_X[Z'_0 - v]) + 4 \cdot 2^{9+1} + 5 \quad (7.8)$$

$$\leq \text{bw}(M_X[Z]) + 4 \cdot 2^{9+1} + 5 \quad (7.9)$$

$$\leq \text{bw}(M_X[C]) + 4 \cdot 2^{9+1} + 13 \quad (7.10)$$

$$\leq l + 4 \cdot 2^{9+1} + 13, \quad (7.11)$$

where (7.3) follows from Claim 7.2.16.6, (7.4) holds because $Z'_2 - (Z_1 - u) = \{v\}$, (7.6) holds because $Z_1 - Z_0 \subseteq \{a, b\}$, (7.7) follows from Claim 7.2.16.5, (7.9)

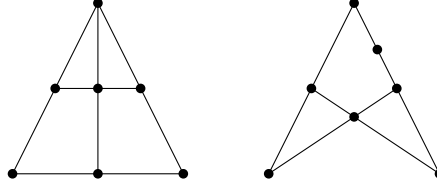


FIGURE 7.1

Geometric representations of P_7 and O_7

holds because $Z - (Z_0 - v) \subseteq \{a, b\}$, and (7.10) follows from Claim 7.2.16.3. But now Theorem 5.4.10 implies that only finitely many excluded minors for $\mathcal{M}(\mathbb{P})$ have an N -minor, and our proof is complete. ■

7.3 Applications

7.3.1 Excluded minors for the classes of near-regular and $\sqrt[6]{1}$ matroids

We apply Theorem 7.F to give an alternative proof of the following result:

7.3.1 THEOREM (Hall et al., 2009). $\mathcal{M}(\mathbb{U}_1)$ has a finite number of excluded minors.

7.3.2 LEMMA. Let M be an excluded minor for $\mathcal{M}(\mathbb{U}_1)$. If $M \notin \{F_7, F_7^*\}$, then M has a $U_{2,4}$ -minor.

Proof: It is readily checked that F_7 is an excluded minor for $\mathcal{M}(\mathbb{U}_1)$. But if M has no minor in $\{F_7, F_7^*, U_{2,4}\}$, then M is regular, and hence certainly near-regular. ■

7.3.3 LEMMA. If $M \in \mathcal{M}(\mathbb{U}_1)$ is 3-connected and strictly $U_{2,4}$ -fragile, then M is a whirl.

This follows easily from the following result:

7.3.4 LEMMA (Geelen et al., 2000, Lemma 3.3). Let M be a 3-connected, non-binary matroid that is not a whirl. Then M has a minor in the set

$$\{U_{2,5}, U_{3,5}, F_7^-, (F_7^-)^*, P_7, P_7^*, O_7, O_7^*\}.$$

Geometric representations of P_7 and O_7 are shown in Figure 7.1.

Proof of Lemma 7.3.3: $U_{2,5}$, F_7^- , and their duals are not near-regular. Each $M \in \{P_7, O_7\}$ has an element e such that both $M \setminus e$ and M/e have a $U_{2,4}$ -minor. The result follows. ■

7.3.5 LEMMA. $U_{2,4}$ is a strong stabilizer for $\mathcal{M}(\mathbb{U}_1)$.

Proof: We have already seen that $U_{2,4}$ is a stabilizer. But $U_{2,4}$ is uniquely representable over \mathbb{U}_1 , so it must be strong. ■

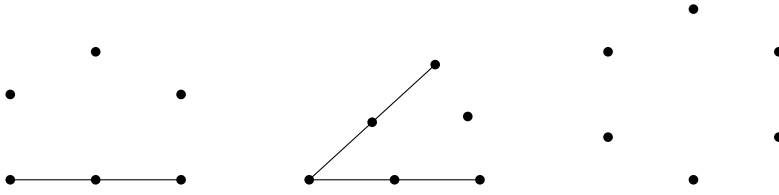


FIGURE 7.2

Geometric representations of P_6 , Q_6 , and $U_{3,6}$

Proof of Theorem 7.3.1: Lemma 7.3.2 implies that finitely many excluded minors have no $U_{2,4}$ -minor. But $U_{2,4}$ is non-binary, 3-connected, a strong stabilizer, and has bounded canopy over \mathbb{U}_1 (by Lemma 7.3.3 and Lemma 5.4.12). Hence Theorem 7.F implies that finitely many excluded minors do have a $U_{2,4}$ -minor, and the result follows. ■

All results above remain valid if we replace \mathbb{U}_1 by \mathbb{S} . Hence we also have

7.3.6 THEOREM (Geelen et al., 2000). $\mathcal{M}(\mathbb{S})$ has a finite number of excluded minors.

7.3.2 Excluded minors for the class of quaternary matroids

Using almost the same arguments as in the previous section we can give an alternative proof of the following:

7.3.7 THEOREM (Geelen et al., 2000). $\mathcal{M}(\text{GF}(4))$ has a finite number of excluded minors.

7.3.8 LEMMA. Let M be an excluded minor for $\mathcal{M}(\text{GF}(4))$. Then M has a $U_{2,4}$ -minor.

Proof: If M has no $U_{2,4}$ -minor then M is binary, and hence certainly $\text{GF}(4)$ -representable. ■

7.3.9 LEMMA. If $M \in \mathcal{M}(\text{GF}(4))$ is 3-connected and strictly $U_{2,4}$ -fragile, then M is a whirl or $M \in \{U_{2,5}, U_{3,5}\}$.

The proof is slightly more involved than that of Lemma 7.3.3. We need the following additional result:

7.3.10 LEMMA (see Oxley, 1992, Corollary 11.2.19). Let M be a 3-connected, non-binary matroid such that $\text{rk}(M) \geq 3$ and $\text{rk}(M^*) \geq 3$. Then M has a minor in the set

$$\{\mathcal{W}^3, P_6, Q_6, U_{3,6}\}.$$

Geometric representations of P_6 , Q_6 , and $U_{3,6}$ are shown in Figure 7.2.

Proof of Lemma 7.3.9: F_7^- and $(F_7^-)^*$ are not quaternary. Each $M \in \{P_7, O_7\}$ has an element e such that both $M \setminus e$ and M/e have a $U_{2,4}$ -minor. Since $U_{2,6}$ is not quaternary it remains to verify that all 3-connected coextensions of $U_{2,5}$ are not

$U_{2,4}$ -fragile. It is easily checked that each $M \in \{P_6, Q_6, U_{3,6}\}$ has an element e such that both $M \setminus e$ and M/e have a $U_{2,4}$ -minor. The result follows. ■

7.3.II LEMMA. $U_{2,4}$ is a strong stabilizer for $\mathcal{M}(\text{GF}(4))$.

Proof: From Theorem 6.2.3 and Lemma 7.3.10 it is not hard to verify that $U_{2,4}$ is a $\text{GF}(4)$ -stabilizer. Since $U_{2,4}$ is uniquely representable over $\text{GF}(4)$, it is also strong. ■

Proof of Theorem 7.3.7: Lemma 7.3.8 implies that all excluded minors have a $U_{2,4}$ -minor. But $U_{2,4}$ is non-binary, 3-connected, a strong stabilizer, and has bounded canopy over $\text{GF}(4)$ (by Lemma 7.3.9 and Lemma 5.4.12). Hence Theorem 7.F implies that finitely many excluded minors do have a $U_{2,4}$ -minor, and the result follows. ■

7.3.3 On Rota's Conjecture for quinary matroids

We will show the following result:

7.3.12 THEOREM. Conjecture 7.G implies that $\mathcal{M}(\text{GF}(5))$ has a finite number of excluded minors.

We will find the excluded minors using an inductive search, starting with $\mathbb{H}_5 = \mathbb{H}_6$.

7.3.13 LEMMA. Let M be an excluded minor for \mathbb{H}_k , for $k < 5$. Then M contains an excluded minor for \mathbb{H}_{k+1} .

Proof: If M contains no excluded minor for \mathbb{H}_{k+1} , then M is \mathbb{H}_{k+1} -representable. But there is a partial-field homomorphism $\mathbb{H}_{k+1} \rightarrow \mathbb{H}_k$, so M is also \mathbb{H}_k -representable, a contradiction. ■

We use the following proposition:

7.3.14 PROPOSITION. The automorphism group of \mathbb{H}_k is isomorphic to S_k , the symmetric group on k elements.

Proof sketch: \mathbb{H}_k is obtained by lifting $\text{GF}(5)^k$. It can be checked (by finding suitable substitutions for the generators) that each permutation of the coordinates in $\text{GF}(5)^k$ leads to an automorphism of \mathbb{H}_k , and that no other automorphisms exist. ■

The following observation is a key step towards our result:

7.3.15 LEMMA. Let M be an excluded minor for \mathbb{H}_{k+1} . If M is representable over \mathbb{H}_k , then M is uniquely representable over \mathbb{H}_k .

Proof: Suppose first that M is ternary. For $k \geq 3$, there is a homomorphism $\varphi : \mathbb{H}_k \rightarrow \text{GF}(8)$. Hence $\mathcal{M}(\text{GF}(3) \times \mathbb{H}_k) = \mathcal{M}(\mathbb{U}_1)$; for $k = 1, 2$ $\mathcal{M}(\text{GF}(3) \times \mathbb{H}_k) = \mathcal{M}(\mathbb{D})$. It follows that we only have to prove the claim for $k = 2$. Hall et al. (2009)

have proven that the only dyadic excluded minors for $\mathcal{M}(\mathbb{U}_1)$ are F_7^- , its dual, and P_8 . Hence we have $M \in \{F_7^-, (F_7^-)^*, P_8\}$. Each of these is uniquely representable over \mathbb{H}_2 .

If M is not ternary, then M has a minor in $\{U_{2,5}, U_{3,5}\}$, since $F_7 \notin \mathcal{M}(\text{GF}(5))$. Therefore M has at least k representations over $\text{GF}(5)$. Since $M \notin \mathcal{M}(\mathbb{H}_{k+1})$, M has exactly k representations over $\text{GF}(5)$. Hence there is, up to permutations of the coordinates, a unique representation of M over $\text{GF}(5)^k$ such that the k projections are pairwise inequivalent. By Proposition 7.3.14 each such permutation yields an automorphism of \mathbb{H}_k , and the result follows. ■

We also need a starting point:

7.3.16 LEMMA. $U_{2,5}$ is uniquely representable over \mathbb{H}_5 .

Proof sketch: The automorphism group of \mathbb{H}_5 is equal to S_6 , the symmetric group on six elements. It can be checked that $U_{2,5}$ has exactly 720 inequivalent representations over \mathbb{H}_5 , and that there is a partial field automorphism between any pair of them. ■

Proof of Theorem 7.3.12: Suppose Conjecture 7.G holds. $U_{2,5}$ is a strong \mathbb{H}_5 -stabilizer, so finitely many excluded minors for $\mathcal{M}(\mathbb{H}_5)$ have a $U_{2,5}$ -minor, by Theorem 7.F. If M is an excluded minor for $\mathcal{M}(\mathbb{H}_5)$ without $U_{2,5}$ -minor, then M is an excluded minor for $\mathcal{M}(\mathbb{U}_1)$. There are finitely many of these by Theorem 7.3.1.

Suppose now that there are finitely many excluded minors for $\mathcal{M}(\mathbb{H}_{k+1})$. Let M be an excluded minor for $\mathcal{M}(\mathbb{H}_k)$. Then M contains an excluded minor, M' say, for $\mathcal{M}(\mathbb{H}_{k+1})$. Now M' is a strong \mathbb{H}_k -stabilizer, so finitely many excluded minors for \mathbb{H}_k have M' as a minor. But then there are finitely many excluded minors for $\mathcal{M}(\mathbb{H}_k)$. ■

7.4 Open problems

Theorem 7.F formalizes the intuition that uniquely extending representations provide sufficient structure to bound the number of excluded minors. The matroid minors project mentioned previously will show that there are no infinite antichains of strongly stabilizing \mathbb{P} -representable matroids if \mathbb{P} is finitary. Proving Rota's Conjecture for new partial fields, then, reduces to finding those excluded minors whose proper minors are not uniquely representable.

7.4.I CONJECTURE. If, for a class \mathcal{M} of matroids the set of totally free expansions is finite, then the following process terminates:

- Determine the binary excluded minors for \mathcal{M} ; store these in a set T .
- Determine the set S of excluded minors for $\mathcal{M}(\mathbb{U}_1) \cap \mathcal{M}$.
- While $S \neq \emptyset$, do the following. Pick $M \in S$. If $M \notin \mathcal{M}$, then replace S by $S - M$, and T by $T \cup M$. If $M \in \mathcal{M}$, then find the set of excluded minors S' containing M for $\mathcal{M}(\mathbb{P}_M)$. Replace S by $(S - M) \cup S'$.

If true, then at the end T contains the excluded minors for \mathcal{M} . To make this practical, we need that M is a strong stabilizer for \mathbb{P}_M , and that we do not get an

infinite chain of universal partial fields. The latter would probably follow since we either introduce more freedom (free expansion, which we assume stops after a finite number of steps), or we introduce new dependencies. Of course, we also need to compute the set of excluded minors explicitly.

A first candidate for this approach would be the class of golden ratio matroids, where there is a finite set of totally free matroids. The starting point would be to determine the set of excluded minors for \mathbb{U}_2 . It would be interesting to find a few of those, and see what horrors we might encounter in the partial fields that come next. It is likely that the 2-cyclotomic partial field, as well as \mathbb{P}_4 , will occur. For the proof of the excluded minors for $\mathcal{M}(\text{GF}(5))$ we switched strategies: rather than looking at \mathbb{U}_2 we directly proceeded to \mathbb{H}_5 .

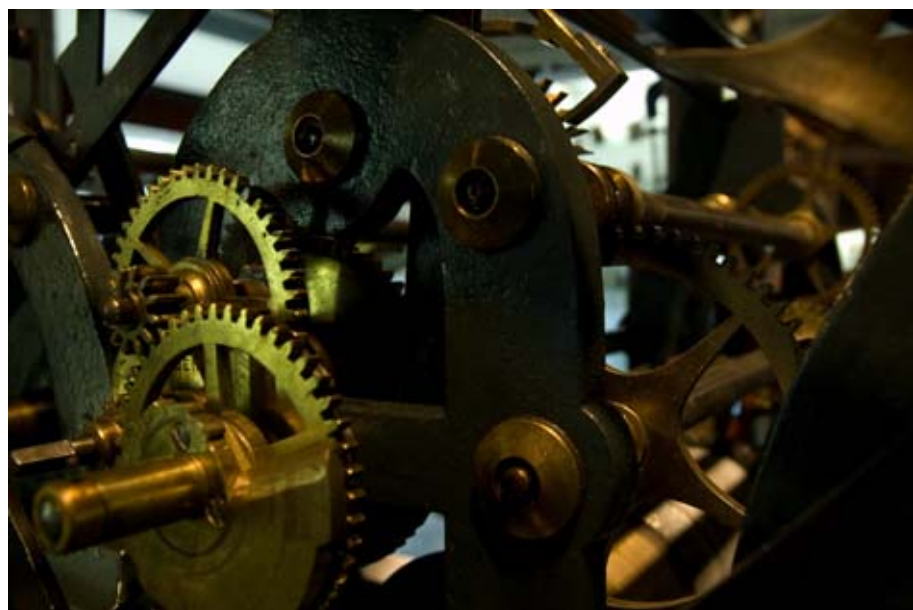
How could this all help for Rota's Conjecture in general? It is well-known that there is no bound on the number of inequivalent $\text{GF}(q)$ -representations of a 3-connected matroid when $q \geq 7$. Hence we have no finite set of "starting points", such as $U_{2,5}$ and $U_{3,5}$ in the case of $\text{GF}(5)$. A positive resolution of the next conjecture would rectify this situation:

7.4.2 DEFINITION. The set \mathcal{M}_q^k is the smallest set that is closed under duality, direct sums, 2-sums, and minors, and that contains all 3-connected matroids that have at least k inequivalent representations over $\text{GF}(q)$. \diamond

7.4.3 CONJECTURE. *For every prime power q there is a constant k such that there are finitely many excluded minors for \mathcal{M}_q^k .*

Now suppose that one of these excluded minors, N say, has exactly $k' < k$ representations over $\text{GF}(q)$. Consider the class of matroids that is $\text{GF}(q)^{k'}$ -stabilized by N . Then we can formulate a statement similar to Theorem 7.F, with pretty much the same proof.

I am confident that one day in the not too distant future we will know that Rota's Conjecture is true.



Background

IN this appendix we list some basic results that are invoked from the main text. All results can be found in standard works in the literature; many could be considered classical. We usually give references rather than proofs.

A.1 Fields, rings, and groups

We start by fixing some notation. Let q be a prime power. We denote the finite field with q elements by $\text{GF}(q)$. This leaves us free to work with lists of fields $\mathbb{F}_1, \mathbb{F}_2, \dots, \mathbb{F}_n$.

We use the convention that a ring always has a multiplicative identity. Let R be a ring. An element $x \in R$ is a *unit* if there exists a $y \in R$ such that $xy = yx = 1$. A ring R is *commutative* if $xy = yx$ for all $x, y \in R$. The set of units of a ring forms a group, denoted by R^* . For a commutative ring R , if $S \subseteq R$ then $\langle S \rangle$ denotes the *ideal generated by S* . If $I, J \subseteq R$ are ideals, then $IJ := (\{xy \mid x \in I, y \in J\})$.

If G is a group, and $S \subseteq G$, then $\langle S \rangle$ is the *subgroup generated by S* . If $S \subseteq R^*$ for some ring, then $\langle S \rangle$ is the multiplicative subgroup of R^* generated by S .

The following is a basic result from commutative algebra. An ideal I of a ring R is *maximal* if $I \subsetneq R$, and if $I \subseteq J \subsetneq R$ then $I = J$.

A.1.1 LEMMA. *Let R be a commutative ring, and I a proper ideal of R .*

- (i) *There is a maximal ideal of R containing I ;*
- (ii) *I is maximal if and only if R/I is a field.*

The first claim is known as *Krull's Theorem*. See, for instance, [Matsumura \(1986\)](#) for a proof. A proof of the second claim can be found in [Stewart and Tall \(2002, Lemma 5.1\)](#).

We denote the polynomial ring over R in x_1, \dots, x_n by $R[x_1, \dots, x_n]$. The x_i may be indeterminates, or may satisfy some algebraic relations.

If R_1, R_2 are rings, then the *product ring* $R_1 \times R_2$ is the ring whose elements are $\{(p, q) \mid p \in R_1, q \in R_2\}$, and whose addition and multiplication operators are

componentwise:

$$\begin{aligned}(p_1, q_1) + (p_2, q_2) &= (p_1 + p_2, q_1 + q_2); \\ (p_1, q_1) \cdot (p_2, q_2) &= (p_1 p_2, q_1 q_2).\end{aligned}$$

A.2 Algebraic number theory

The results in this section are used to compute the set of homomorphisms for some partial fields in Section 2.5. We state only the bare minimum set of definitions and results, and provide no proofs. [Stewart and Tall \(2002\)](#) have written a very accessible book on the subject. For a few results that are not proven by Stewart and Tall we refer to [Hardy and Wright \(1954\)](#) instead.

A.2.1 DEFINITION. An element $\alpha \in \mathbb{C}$ is an *algebraic number* if there is a polynomial $p \in \mathbb{Q}[x]$ such that $p(\alpha) = 0$. ◇

A.2.2 DEFINITION. A *number field* is a finite-dimensional extension field of \mathbb{Q} . ◇

An immediate implication is that every element of a number field \mathbb{F} is algebraic, i.e. $\mathbb{F} = \mathbb{Q}(\alpha_1, \dots, \alpha_n)$ for some algebraic numbers $\alpha_1, \dots, \alpha_n$. A first result is the following:

A.2.3 THEOREM (see [Stewart and Tall, 2002](#), Theorem 2.2). *If \mathbb{F} is a number field then $\mathbb{F} = \mathbb{Q}(\theta)$ for some algebraic number θ .*

A.2.4 DEFINITION. An algebraic number α is an *algebraic integer* if $p(\alpha) = 0$ for some polynomial $p \in \mathbb{Q}[x]$ of the form

$$p(x) = \sum_{i=0}^n a_i x^i,$$

with $a_i \in \mathbb{Z}$ for $i = 1, \dots, n$, and $a_n = 1$. ◇

A.2.5 DEFINITION. Let $\mathbb{Q}(\theta)$ be a number field. The *ring of integers* of $\mathbb{Q}(\theta)$ is

$$R_\theta := \{x \in \mathbb{Q}(\theta) \mid x \text{ is an algebraic integer}\}. \quad \diamond$$

A.2.6 LEMMA (see [Stewart and Tall, 2002](#), Theorem 2.9). *R_θ is a ring.*

We are interested in ring homomorphisms to finite fields. For these we need to study the maximal ideals, by Lemma A.1.1.

A.2.7 DEFINITION. A proper ideal I of a ring R is *prime* if, for all ideals J_1, J_2 with $J_1 J_2 \subseteq I$, either $J_1 \subseteq I$ or $J_2 \subseteq I$. ◇

A.2.8 LEMMA (see [Stewart and Tall, 2002](#), Corollary 5.2, Theorem 5.3). *Let R_θ be the ring of integers of a number field and I a proper ideal of R_θ .*

- (i) R_θ/I is a finite ring;
- (ii) I is maximal if and only if it is prime.

A.2.9 DEFINITION. Let R_θ be the ring of integers of a number field, and I an ideal of R_θ . The *norm* of I is

$$N(I) := |R_\theta/I|. \quad \diamond$$

An important observation is that norms are multiplicative:

A.2.10 LEMMA (see [Stewart and Tall, 2002](#), Theorem 5.12). If I, J are nonzero ideals of R_θ then

$$N(IJ) = N(I)N(J).$$

We will encounter rings of integers for a few quadratic number fields, so we will zoom in on these.

A.2.11 LEMMA (see [Stewart and Tall, 2002](#), Proposition 3.1, Theorem 3.2).

- (i) Every quadratic number field is equal to $\mathbb{Q}(\sqrt{d})$ for some squarefree* integer d ;
- (ii) If $d \equiv 1 \pmod{4}$ then $R_{\sqrt{d}} = \mathbb{Z}[\frac{1}{2} + \frac{1}{2}\sqrt{d}]$;
- (iii) If $d \not\equiv 1 \pmod{4}$ then $R_{\sqrt{d}} = \mathbb{Z}[\sqrt{d}]$;
- (iv) If $I = (a + b\sqrt{d})$ then $N(I) = a^2 - db^2$.

If $I = (p)$ for some prime p , then $N(I) = p^2$. By Lemma A.2.10, either I is prime, in which case $R_{\sqrt{d}}/I \cong \text{GF}(p^2)$, or $I = J_1J_2$, with $N(J_1) = p$. Lemma A.2.10 then implies that $R_{\sqrt{d}}/J_1 \cong \text{GF}(p)$. For instance, in $R_i = R_{\sqrt{-1}}$, $(5) = (2+i)(2-i)$, and $N(2+i) = 5$. At last we can state the results that we were after.

Let ζ be a root of $x^2 - x + 1 = 0$.

A.2.12 THEOREM (see [Hardy and Wright, 1954](#), Theorem 255). Let p be a prime number. The ideal (p) is prime in R_ζ if and only if $p \equiv 2 \pmod{3}$.

Note here that, if $p \equiv 0 \pmod{3}$, then $p = 3$.

Let τ be a root of $x^2 - x - 1 = 0$.

A.2.13 THEOREM (see [Hardy and Wright, 1954](#), Theorem 257). Let p be a prime number. The ideal (p) is prime in R_τ if and only if $p \equiv \pm 2 \pmod{5}$.

Let i be a root of $x^2 + 1 = 0$.

A.2.14 THEOREM (see [Hardy and Wright, 1954](#), Theorem 252). Let p be a prime number. The ideal (p) is prime in R_i if and only if $p \equiv 3 \pmod{4}$.

*We say $x \in \mathbb{Z}$ is *squarefree* if the prime factorization of x has no repeating factors.

A.3 Matrices and determinants

In this section we list some basic results on matrices over commutative rings. We refer to [Brown \(1993\)](#) for an extensive treatment of the subject and for proofs of all but the most classical results.

A.3.1 DEFINITION. Let A be an $n \times n$ matrix with entries in a ring R . The *determinant* of A is

$$\det(A) := \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)},$$

where S_n is the group of permutations of $\{1, 2, \dots, n\}$, and, for $\sigma \in S_n$, $\operatorname{sgn}(\sigma)$ is the signature of σ . \diamond

A.3.2 PROPOSITION. Let R be a ring, and A an $n \times n$ matrices over R .

- (i) If D is obtained from A by transposition, then $\det(D) = \det(A)$;
- (ii) If D is obtained from A by interchanging a pair of rows, then $\det(D) = -\det(A)$;
- (iii) If D is obtained from A by multiplying a row by $p \in R$, then $\det(D) = p \det(A)$;
- (iv) If $A = \begin{bmatrix} x & A' \end{bmatrix}$ and $D = \begin{bmatrix} y & A' \end{bmatrix}$ for some $x, y \in R^n$ and $A' \in R^{n \times (n-1)}$, then $\det(\begin{bmatrix} (x+y) & A' \end{bmatrix}) = \det(A) + \det(D)$;
- (v) If $A = \begin{bmatrix} x & y & A' \end{bmatrix}$ for some $x, y \in R^n$ and $A' \in R^{n \times (n-2)}$, then $\det(\begin{bmatrix} (x+y) & y & A' \end{bmatrix}) = \det(A)$.

A.3.3 PROPOSITION. Let R be a ring, and A, D $n \times n$ matrices over R .

- (i) $\det(AD) = \det(A) \det(D)$;
- (ii) $\det(A) \in R^*$ if and only if there exists a matrix A^{-1} with $AA^{-1} = A^{-1}A = I$.

Note that, even if A is invertible, it may not be possible to apply Gaussian elimination to A , as in the case of fields.

A.3.4 DEFINITION. The *empty matrix* is the unique 0×0 matrix. If A is the empty matrix then we define $\det(A) = 1$. \diamond

A.4 Graph theory

In this thesis we do not go beyond the most basic notions of graph theory. We give brief definitions here; for a thorough introduction the book by [Diestel \(2005\)](#) can be consulted.

A.4.1 DEFINITION. A *graph* is a tuple $G = (V, E)$, where V is a finite set, the *vertices*, and E is a collection of unordered pairs from V , the *edges*. \diamond

An edge $\{v, w\}$ is often denoted by vw . The set of vertices of a graph G is denoted by $V(G)$, the set of edges by $E(G)$.

A.4.2 EXAMPLE. Consider Figure [A.1](#). The set V consists of the points in the figure, and the set E consists of all pairs of vertices such that the corresponding dots are connected by a line segment meeting no other vertex. \diamond

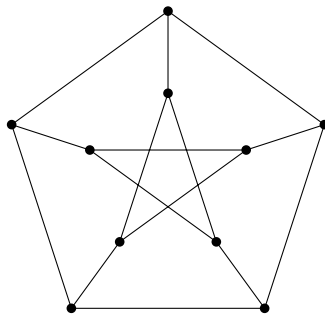


FIGURE A.1

Image of a graph with 10 vertices and 15 edges.

A.4.3 DEFINITION. A *subgraph* of $G = (V, E)$ is a graph $G' = (V', E')$ such that $V' \subseteq V$, $E' \subseteq E$, and $e \subseteq V'$ for all $e \in E'$. \diamond

A.4.4 DEFINITION. A subgraph $G' = (V', E')$ of $G = (V, E)$ is *induced* if

$$E' = \{e \in E \mid e \subseteq V'\}.$$

We write $G' = G[V']$. \diamond

A.4.5 DEFINITION. A graph $G = (V, E)$ is *bipartite* if V can be partitioned into sets U, W such that all $e \in E$ satisfy $|e \cap U| = |e \cap W| = 1$. \diamond

A.4.6 DEFINITION. A *walk* in a graph $G = (V, E)$ is a sequence (v_0, \dots, v_n) of vertices such that $v_i v_{i+1} \in E$ for all $i \in \{0, \dots, n-1\}$. If $v_i \neq v_j$ for all $0 \leq i < j < n$ then we say that W is a *path* if $v_n \neq v_0$, and a *cycle*[†] if $v_n = v_0$. \diamond

A.4.7 DEFINITION. A graph is *connected* if there is a path between every pair of vertices. \diamond

A.4.8 DEFINITION. A *component* of a graph is an inclusionwise maximal connected induced subgraph. \diamond

A.4.9 DEFINITION. A *forest* is a graph with no cycles, and a *tree* is a connected forest. \diamond

A.4.10 DEFINITION. A forest T *spans* G if it is a subgraph of G , and adding any edge of G to T introduces a cycle. \diamond

A.4.11 DEFINITION. The *degree* of a vertex v is $|\{e \in E \mid v \in e\}|$. \diamond

A.4.12 DEFINITION. The *distance* between two vertices $u, v \in V(G)$ is the minimum, over all $u - v$ paths P in G , of the number of edges in P , and is denoted by $d_G(u, v)$. \diamond

[†]We reserve the word *circuit* for a minimal dependent set in a matroid.

A.4.13 DEFINITION. Let $U, W \subseteq V(G)$. Then

$$d_G(U, W) := \min_{u \in U, v \in W} d_G(u, v). \quad \diamond$$



A catalog of partial fields

IN this appendix we summarize all partial fields described in this thesis, and some of their basic properties. Like rings, partial fields form a category. The regular partial field, \mathbb{U}_0 , has a homomorphism to every other partial field. For convenience we have repeated Figure 2.1 as well.

The regular partial field, \mathbb{U}_0 :

- $\mathbb{U}_0 = (\mathbb{Z}, \{-1, 0, 1\})$;
- $\mathcal{F}(\mathbb{U}_0) = \{0, 1\}$ (Lemma 2.5.3);
- There is a homomorphism to every partial field \mathbb{P} (Lemma 2.5.2);
- Isomorphic to $\mathbb{L}(\text{GF}(2) \times \text{GF}(3))$ (Section 4.3);
- Isomorphic to $\mathbb{D}\text{GF}(2)$ (Section 3.2.1);
- There are finitely many excluded minors for \mathbb{U}_0 -representability (Theorem 4.2.1).

The near-regular partial field, \mathbb{U}_1 :

- $\mathbb{U}_1 = \left(\mathbb{Z}[\alpha, \frac{1}{1-\alpha}, \frac{1}{\alpha}], \langle -1, \alpha, 1-\alpha \rangle \right)$, where α is an indeterminate;
- $\mathcal{F}(\mathbb{U}_1) = \text{Asc}\{1, \alpha\} = \left\{ 0, 1, \alpha, 1-\alpha, \frac{1}{1-\alpha}, \frac{\alpha}{\alpha-1}, \frac{\alpha-1}{\alpha}, \frac{1}{\alpha} \right\}$ (Lemma 2.5.9);
- There is a homomorphism to every field with at least three elements (Lemma 2.5.8);
- Isomorphic to $\mathbb{L}(\text{GF}(3) \times \text{GF}(8))$ and $\mathbb{L}(\text{GF}(3) \times \text{GF}(4) \times \text{GF}(5))$ (Section 4.3);
- Isomorphic to $\mathbb{D}\mathbb{S}$ (Section 3.2.1);
- There are finitely many excluded minors for \mathbb{U}_1 -representability (Theorem 7.3.1).

The k -uniform partial field, \mathbb{U}_k :

- $\mathbb{U}_k = (\mathbb{Q}(\alpha_1, \dots, \alpha_k), \langle U_k \rangle)$, where

$$U_k := \{x - y \mid x, y \in \{0, 1, \alpha_1, \dots, \alpha_k\}, x \neq y\},$$

and $\alpha_1, \dots, \alpha_k$ are indeterminates;

- Introduced by Sample (1997) as the k -regular partial field;

- [Sample \(1997\)](#) proved that

$$\mathcal{F}(\mathbb{U}_k) = \left\{ \frac{a-b}{c-b} \mid a, b, c \in \{0, 1, \alpha_1, \dots, \alpha_k\}, \text{ distinct} \right\} \cup \left\{ \frac{(a-b)(c-d)}{(c-b)(a-d)} \mid a, b, c, d \in \{0, 1, \alpha_1, \dots, \alpha_k\}, \text{ distinct} \right\};$$

- There is a homomorphism to every field with at least $k + 2$ elements (see [Sample, 1997](#));
- Finitely many excluded minors for \mathbb{U}_k -representability are $\mathbb{U}_{k'}$ -representable for some $k' > k$ (see [Oxley et al., 2000](#)).

The sixth-roots-of-unity ($\sqrt[6]{1}$) partial field, \mathbb{S} :

- $\mathbb{S} = (\mathbb{Z}[\zeta], \langle \zeta \rangle)$, where ζ is a root of $x^2 - x + 1 = 0$.
- $\mathcal{F}(\mathbb{S}) = \text{Asc}\{1, \zeta\} = \{0, 1, \zeta, 1 - \zeta\}$ (Lemma 2.5.13);
- There is a homomorphism to $\text{GF}(3)$, to $\text{GF}(p^2)$ for all primes p , and to $\text{GF}(p)$ when $p \equiv 1 \pmod{3}$ (Lemma 2.5.12);
- Isomorphic to $\mathbb{L}(\text{GF}(3) \times \text{GF}(4))$ (Section 4.3);
- There are finitely many excluded minors for \mathbb{S} -representability (Theorem 7.3.6).

The dyadic partial field, \mathbb{D} :

- $\mathbb{D} = (\mathbb{Z}[\frac{1}{2}], \langle -1, 2 \rangle)$;
- $\mathcal{F}(\mathbb{D}) = \text{Asc}\{1, 2\} = \{0, 1, -1, 2, 1/2\}$ (Lemma 2.5.6);
- There is a homomorphism to every field that does not have characteristic two (Lemma 2.5.5);
- Isomorphic to $\mathbb{L}(\text{GF}(3) \times \text{GF}(5))$ (Section 4.3);
- Isomorphic to $\mathbb{D} \text{GF}(3)$ (Section 3.2.1);

The union of $\sqrt[6]{1}$ and dyadic, \mathbb{Y} :

- $\mathbb{Y} = (\mathbb{Z}[\zeta, \frac{1}{2}], \langle -1, 2, \zeta \rangle)$, where ζ is a root of $x^2 - x + 1 = 0$;
- $\mathcal{F}(\mathbb{Y}) = \text{Asc}\{1, 2, \zeta\} = \{0, 1, -1, 2, 1/2, \zeta, 1 - \zeta\}$ (Lemma 2.5.15);
- There is a homomorphism to $\text{GF}(3)$, to $\text{GF}(p^2)$ for all odd primes p , and to $\text{GF}(p)$ when $p \equiv 1 \pmod{3}$ (Lemma 2.5.16);
- Isomorphic to $\mathbb{L}(\text{GF}(3) \times \text{GF}(7))$ (Section 4.3).

The 2-cyclotomic partial field, \mathbb{K}_2 :

- $\mathbb{K}_2 = (\mathbb{Q}(\alpha), \langle -1, \alpha, \alpha - 1, \alpha + 1 \rangle)$, where α is an indeterminate;
- $\mathcal{F}(\mathbb{K}_2) = \text{Asc}\{1, \alpha, -\alpha, \alpha^2\}$ (Lemma 2.5.35);
- There is a homomorphism to $\text{GF}(q)$ for $q \geq 4$ (Lemma 2.5.33);
- Isomorphic to $\mathbb{L}(\text{GF}(4) \times \mathbb{H}_2)$ (Section 4.3);
- Isomorphic to $\mathbb{D}\mathbb{G}$ (Section 3.2.1).

The k -cyclotomic partial field, \mathbb{K}_k :

- $\mathbb{K}_k = (\mathbb{Q}(\alpha), \langle -1, \alpha, \alpha - 1, \alpha^2 - 1, \dots, \alpha^k - 1 \rangle)$, where α is an indeterminate;
- $\mathbb{K}_k = (\mathbb{Q}(\alpha), \langle \{-1\} \cup \{\Phi_j(\alpha) \mid j = 0, \dots, k\} \rangle)$, where $\Phi_0(\alpha) = \alpha$ and Φ_j is the j th cyclotomic polynomial (Lemma 2.5.34);
- There is a homomorphism to $\text{GF}(q)$ for $q \geq k + 2$ (Lemma 2.5.33).

The Dowling lift of $\text{GF}(4)$, \mathbb{W} :

- $\mathbb{W} := (\mathbb{Z}[\zeta, \frac{1}{1+\zeta}], \langle -1, \zeta, 1 + \zeta \rangle)$, where ζ is a root of $x^2 - x + 1 = 0$;
- $\mathcal{F}(\mathbb{W}) = \text{Asc}\{1, \zeta, \zeta^2\} = \{0, 1, \zeta, \bar{\zeta}, \zeta^2, \bar{\zeta}^2, \zeta + 1, (\zeta + 1)^{-1}, (\bar{\zeta} + 1)^{-1}, \bar{\zeta} + 1\}$ (Lemma 2.5.37);

- Isomorphic to $\mathbb{D}\text{GF}(4)$ (Section 3.2.1);
- There is a homomorphism to every field with an element of multiplicative order 3 (Theorem 3.2.8).

The Gersonides partial field, $\mathbb{G}\mathbb{E}$:

- $\mathbb{G}\mathbb{E} = \left(\mathbb{Z}[\frac{1}{2}, \frac{1}{3}], \langle -1, 2, 3 \rangle\right)$;
- $\mathcal{F}(\mathbb{G}\mathbb{E}) = \text{Asc}\{1, 2, 3, 4, 9\}$ (Lemma 2.5.40);
- There is a homomorphism to every field that does not have characteristic two or three (Lemma 2.5.39).

The partial field \mathbb{P}_4 :

- $\mathbb{P}_4 = (\mathbb{Q}(\alpha), \langle -1, \alpha, \alpha - 1, \alpha + 1, \alpha - 2 \rangle)$, where α is an indeterminate;
- $\mathcal{F}(\mathbb{P}_4) = \text{Asc}\{1, \alpha, -\alpha, \alpha^2, \alpha - 1, (\alpha - 1)^2\}$ (Lemma 2.5.43);
- There is a homomorphism to every field with at least four elements (Lemma 2.5.42).

The Gaussian partial field, \mathbb{H}_2 :

- $\mathbb{H}_2 = \left(\mathbb{Z}[i, \frac{1}{2}], \langle i, 1 - i \rangle\right)$, where i is a root of $x^2 + 1 = 0$;
- $\mathcal{F}(\mathbb{H}_2) = \text{Asc}\{1, 2, i\} = \left\{0, 1, -1, 2, \frac{1}{2}, i, i + 1, \frac{i+1}{2}, 1 - i, \frac{1-i}{2}, -i\right\}$ (Lemma 2.5.22);
- There is a homomorphism to $\text{GF}(p^2)$ for all primes $p \geq 3$, and to $\text{GF}(p)$ when $p \equiv 1 \pmod{4}$ (Lemma 2.5.21);
- A matroid is \mathbb{H}_2 -representable if and only if it is dyadic or has at least two inequivalent $\text{GF}(5)$ -representations (Lemma 4.2.6);
- Isomorphic to $\mathbb{D}\text{GF}(5)$ (Section 3.2.1).

The Hydra-3 partial field, \mathbb{H}_3 :

- $\mathbb{H}_3 = (\mathbb{Q}(\alpha), \langle -1, \alpha, 1 - \alpha, \alpha^2 - \alpha + 1 \rangle)$, where α is an indeterminate;
- $\mathcal{F}(\mathbb{H}_3) = \text{Asc}\left\{1, \alpha, \alpha^2 - \alpha + 1, \frac{\alpha^2}{\alpha - 1}, \frac{-\alpha}{(\alpha - 1)^2}\right\}$ (Lemma 2.5.25);
- There is a homomorphism to every field with at least five elements (Lemma 2.5.24);
- A matroid is \mathbb{H}_3 -representable if and only if it is near-regular or has at least three inequivalent $\text{GF}(5)$ -representations (Lemma 6.3.11).

The Hydra-4 partial field, \mathbb{H}_4 :

- $\mathbb{H}_4 = (\mathbb{Q}(\alpha, \beta), \langle -1, \alpha, \beta, \alpha - 1, \beta - 1, \alpha\beta - 1, \alpha + \beta - 2\alpha\beta \rangle)$, where α, β are indeterminates;
- $\mathcal{F}(\mathbb{H}_4) = \text{Asc}\left\{1, \alpha, \beta, \alpha\beta, \frac{\alpha - 1}{\alpha\beta - 1}, \frac{\beta - 1}{\alpha\beta - 1}, \frac{\alpha(\beta - 1)}{\beta(\alpha - 1)}, \frac{(\alpha - 1)(\beta - 1)}{1 - \alpha\beta}, \frac{\alpha(\beta - 1)^2}{\beta(\alpha\beta - 1)}, \frac{\beta(\alpha - 1)^2}{\alpha(\alpha\beta - 1)}\right\}$ (Lemma 2.5.27);
- There is a homomorphism to every field with at least five elements;
- A matroid is \mathbb{H}_4 -representable if and only if it is near-regular or has at least four inequivalent $\text{GF}(5)$ -representations (Lemma 6.3.12).

The Hydra-5 partial field, $\mathbb{H}_5 = \mathbb{H}_6$:

- $\mathbb{H}_5 = (\mathbb{Q}(\alpha, \beta, \gamma), \langle -1, \alpha, \beta, \gamma, \alpha - 1, \beta - 1, \gamma - 1, \alpha - \gamma, \gamma - \alpha\beta, (1 - \gamma) - (1 - \alpha)\beta \rangle)$, where α, β, γ are indeterminates;
- $\mathcal{F}(\mathbb{H}_5) = \text{Asc}\left\{1, \alpha, \beta, \gamma, \frac{\alpha\beta}{\gamma}, \frac{\alpha}{\gamma - \alpha}, \frac{(1 - \alpha)\gamma}{\gamma - \alpha}, \frac{(\alpha - 1)\beta}{\gamma - 1}, \frac{\alpha - 1}{\gamma - 1}, \frac{\gamma - \alpha}{\gamma - \alpha\beta}, \frac{(\beta - 1)(\gamma - 1)}{\beta(\gamma - \alpha)}, \frac{\beta(\gamma - \alpha)}{\gamma - \alpha\beta}, \frac{(\alpha - 1)(\beta - 1)}{\gamma - \alpha}, \frac{\beta(\gamma - \alpha)}{(1 - \gamma)(\gamma - \alpha\beta)}, \frac{(1 - \alpha)(\gamma - \alpha\beta)}{\gamma - \alpha}, \frac{1 - \beta}{\gamma - \alpha\beta}\right\}$ (Lemma 2.5.29);
- There is a homomorphism to every field with at least five elements;
- A matroid is \mathbb{H}_5 -representable if and only if it is near-regular or has at least six inequivalent $\text{GF}(5)$ -representations (Lemma 6.3.13).

The near-regular partial field modulo two, $\mathbb{U}_1^{(2)}$:

- $\mathbb{U}_1^{(2)} = (\text{GF}(2)(\alpha), \langle \alpha, 1 + \alpha \rangle)$, where α is an indeterminate;
- $\mathcal{F}(\mathbb{U}_1^{(2)}) = \{0, 1\} \cup \text{Asc}\{\alpha^{2^k} \mid k \in \mathbb{N}\}$ (Lemma 2.5.46);
- There is a homomorphism to $\text{GF}(2^k)$ for all $k \geq 2$ (Lemma 2.5.45).

The golden ratio partial field, \mathbb{G} :

- $\mathbb{G} = (\mathbb{Z}[\tau], \langle -1, \tau \rangle)$, where τ is the positive root of $x^2 - x - 1 = 0$;
- $\mathcal{F}(\mathbb{G}) = \text{Asc}\{1, \tau\} = \{0, 1, \tau, -\tau, 1/\tau, -1/\tau, \tau^2, 1/\tau^2\}$ (Lemma 2.5.19);
- There is a homomorphism to $\text{GF}(5)$, to $\text{GF}(p^2)$ for all primes p , and to $\text{GF}(p)$ when $p \equiv \pm 1 \pmod{5}$ (Lemma 2.5.18);
- Isomorphic to $\mathbb{L}(\text{GF}(4) \times \text{GF}(5))$ (Section 4.3).

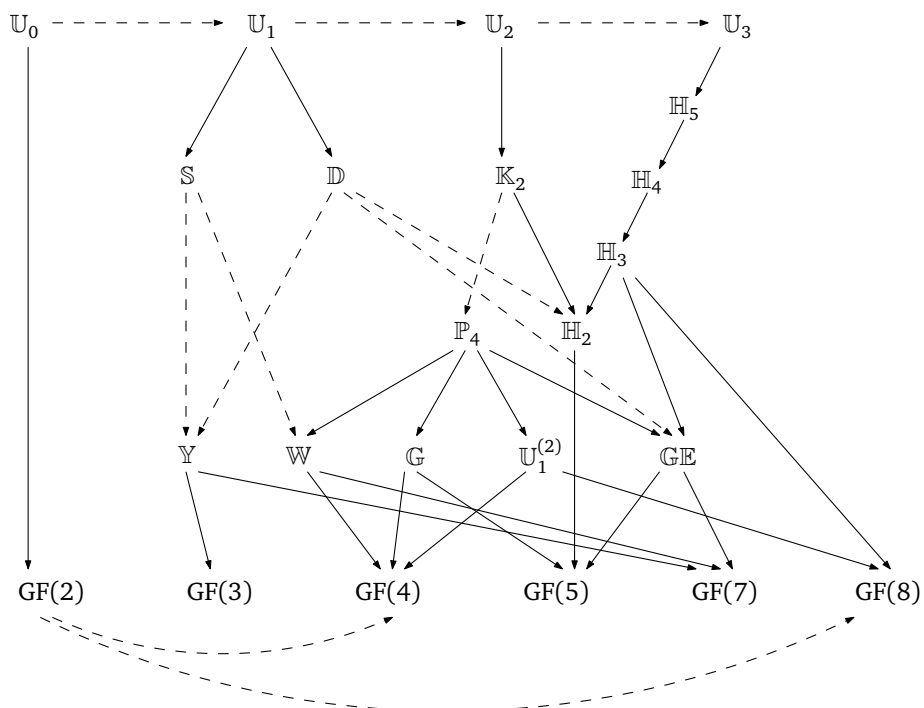


FIGURE B.1

Some partial fields and their homomorphisms. A (dashed) arrow from \mathbb{P}' to \mathbb{P} indicates that there is an (injective) homomorphism $\mathbb{P}' \rightarrow \mathbb{P}$.

Curriculum Vitae

STEFAN van Zwam was born in Eindhoven, the Netherlands on November 28, 1981. In 2000 he obtained his VWO diploma at the Scholengemeenschap Augustinianum in Eindhoven. In July of that year he participated in the International Physics Olympiad, after placing fourth in the national competition. He enrolled at the Technische Universiteit Eindhoven to study Mathematics and Computer Science, and continued with Mathematics after his first year. In 2005 he obtained his Master's degree in Industrial and Applied Mathematics, with his thesis titled "Properties of lattices : a semidefinite programming approach", completed under the supervision of Rudi Pendavingh. In the same year he started as a PhD student, again at the Technische Universiteit Eindhoven. He will defend his thesis on August 31, 2009.

In 2004 Stefan spent three months at the Università degli Studi di Roma "La Sapienza", Italy, where he worked with Stefano Leonardi and Guido Schäfer on problems in algorithmic game theory. In 2008 he spent three months at the Victoria University of Wellington, New Zealand, where he worked with Dillon Mayhew and Geoff Whittle on problems in matroid theory.

After his defense, Stefan will work as a postdoctoral researcher at the Centrum voor Wiskunde en Informatica in Amsterdam, the Netherlands, and at the University of Waterloo in Canada.

Apart from mathematics, Stefan enjoys reading a good book, plays the trumpet, and takes an interest in photography.

Partial Fields in Matroid Theory

Summary

MATROID theory is the study of abstract properties of linear dependence. A matroid consists of a finite set, and a partition of its subsets into “dependent” and “independent” ones. For example, if E is a finite set of vectors in some vector space, then we can define a matroid on E by partitioning the subsets into those that are linearly dependent and those that are linearly independent. Conversely we may ask, for a given matroid, if there exists a set of vectors such that the linearly (in)dependent subsets are precisely those prescribed by the matroid. This is the matroid representation problem.

In this thesis we study, using a blend of algebraic, combinatorial, and geometric techniques, matroids that have representations over several distinct fields. Some classes of such matroids have been characterized by the property that, among the representation matrices for each of its members, there is one with special structure: the determinants of all square submatrices are restricted to a certain subset of the field. Semple and Whittle introduced the notion of a partial field to study such characterizations systematically. A partial field is an algebraic structure where multiplication is as usual, but addition is not always defined. The “matrices with special structure” then correspond with “matrices for which all determinants of square submatrices are defined”.

In Chapter 2 we build up the theory of partial fields. Our definition of a partial field differs from that by Semple and Whittle, and we obtain a number of results more easily. We also propose a generalization to include skew partial fields.

There are many ways to construct partial fields. In Chapter 3 we give three examples. The first example is the product partial field, in which we combine several distinct representations of a matroid into one representation over a new partial field. The second construction is the Dowling lift of a partial field, which gives insight in the representability of Dowling geometries. The third construction is the universal partial field of a matroid M , which is the most general partial field over which M is representable. Moreover, any representation of M , over any field, can be derived from it.

In Chapter 4 we prove the Lift Theorem, which can be used to characterize sets of matroids representable over a number of fields. For instance, the set of matroids

representable over both $\text{GF}(4)$ and $\text{GF}(5)$ equals the set of matroids representable over \mathbb{R} by a matrix for which every subdeterminant is a power of the golden ratio.

Let M and N be 3-connected matroids, where N is a minor of M . If M is representable over a partial field, and N is representable over a sub-partial field, then the Confinement Theorem, the main result of Chapter 6, states that either M is representable over the sub-partial field, or there is a small extension of N that is already not representable over the sub-partial field.

The Confinement Theorem has a number of applications, including a characterization of the inequivalent representations of quinary matroids. A corollary is the Settlement Theorem. This result combines the theory of universal partial fields with the Confinement Theorem to give conditions under which the number of inequivalent representations of a matroid is bounded by the number of representations of a certain minor.

A minor of a representable matroid M is a matroid obtained from M by repeatedly applying certain reductions. An excluded minor for a class of matroids is a matroid that is not in the class, but after any single reduction the resulting matroid is in the class. The most famous conjecture in matroid theory is Rota's Conjecture, which states that for each prime power q , the set of matroids representable over $\text{GF}(q)$ has a finite number of excluded minors. Rota's Conjecture has been proven only for $q = 2, 3, 4$.

In Chapter 7 we prove a theorem that gives sufficient conditions for the set of excluded minors for the class of matroids representable over a fixed partial field to be finite. We show that this theorem implies the finiteness of the set of excluded minors in all cases that were previously known. Moreover, we indicate how the techniques of this chapter might be applied in the future to yield a proof that there are finitely many excluded minors for the class of matroids representable over $\text{GF}(5)$.

Bibliography

- J. AIKIN and J. OXLEY (2008). The structure of crossing separations in matroids, *Adv. in Appl. Math.*, volume 41, no. 1, pp. 10–26. Cited on p. [124](#).
- S. AKKARI and J. OXLEY (1993). Some local extremal connectivity results for matroids, *Combin. Probab. Comput.*, volume 2, no. 4, pp. 367–384. Cited on p. [47](#).
- R. BAINES and P VÁMOS (2003). An algorithm to compute the set of characteristics of a system of polynomial equations over the integers, *J. Symbolic Comput.*, volume 35, no. 3, pp. 269–279. Cited on pp. [19](#), [86](#), and [112](#).
- G. BIRKHOFF (1967). *Lattice Theory*, Third edition. American Mathematical Society Colloquium Publications, Vol. XXV, American Mathematical Society, Providence, R.I. Cited on p. [9](#).
- R. E. BIXBY (1979). On Reid’s characterization of the ternary matroids, *J. Combin. Theory Ser. B*, volume 26, no. 2, pp. 174–204. Cited on pp. [14](#) and [97](#).
- A. BJÖRNER, M. LAS VERGNAS, B. STURMFELS, N. WHITE, and G. M. ZIEGLER (1993). *Oriented Matroids*, volume 46 of *Encyclopedia of Mathematics and its Applications*, Cambridge University Press, Cambridge, ISBN 0-521-41836-4. Cited on p. [84](#).
- W. C. BROWN (1993). *Matrices over Commutative Rings*, volume 169 of *Mono-graphs and Textbooks in Pure and Applied Mathematics*, Marcel Dekker Inc., New York, ISBN 0-8247-8755-2. Cited on p. [168](#).
- T. BRYLAWSKI (1975). Modular constructions for combinatorial geometries, *Trans. Amer. Math. Soc.*, volume 203, pp. 1–44. Cited on pp. [44](#) and [45](#).
- T. BRYLAWSKI (1982). Finite prime-field characteristic sets for planar configurations, *Linear Algebra Appl.*, volume 46, pp. 155–176. Cited on p. [90](#).
- T. BRYLAWSKI (1986). Appendix of matroid cryptomorphisms, in *Theory of matroids*, volume 26 of *Encyclopedia Math. Appl.*, pp. 298–316, Cambridge Univ. Press, Cambridge. Cited on p. [9](#).
- T. BRYLAWSKI and D. LUCAS (1976). Uniquely representable combinatorial geometries, in *Colloquio Internazionale sulle Teorie Combinatorie (Roma, 3–15 settembre 1973)*, Tomo I, volume 17 of *Atti dei Convegni Lincei*, pp. 83–104, Accad. Naz. Lincei, Roma. Cited on pp. [19](#) and [33](#).
- F. BUEKENHOUT and P CAMERON (1995). Projective and affine geometry over division rings, in *Handbook of incidence geometry*, pp. 27–62, North-Holland, Amsterdam. Cited on p. [68](#).
- J. H. CONWAY and D. A. SMITH (2003). *On Quaternions and Octonions: Their Geometry, Arithmetic, and Symmetry*, A K Peters Ltd., Natick, MA, ISBN 1-56881-134-9. Cited on p. [71](#).

- H. S. M. COXETER (1964). Projective Geometry, Blaisdell Publishing Co. Ginn and Co. New York-London-Toronto. Cited on p. 7.
- H. H. CRAPO and G.-C. ROTA (1970). On the Foundations of Combinatorial Theory: Combinatorial Geometries, preliminary edition, The M.I.T. Press, Cambridge, Mass.-London. Cited on p. 7.
- W. H. CUNNINGHAM and J. EDMONDS (1980). A combinatorial decomposition theory, *Canad. J. Math.*, volume 32, no. 3, pp. 734–765. Cited on p. 124.
- R. DIESTEL (2005). Graph Theory, volume 173 of *Graduate Texts in Mathematics*, 3rd edition, Springer-Verlag, Berlin, ISBN 978-3-540-26182-7; 3-540-26182-6; 978-3-540-26183-4. Cited on p. 168.
- T. A. DOWLING (1973). A class of geometric lattices based on finite groups, *J. Combinatorial Theory Ser. B*, volume 14, pp. 61–86. Cited on pp. 19, 79, and 81.
- N. E. FENTON (1984). Matroid representations—an algebraic treatment, *Quart. J. Math. Oxford Ser. (2)*, volume 35, no. 139, pp. 263–280. Cited on pp. 19, 87, and 88.
- N. J. FINE (1947). Binomial coefficients modulo a prime, *Amer. Math. Monthly*, volume 54, pp. 589–592. Cited on p. 58.
- J. GEELEN, B. GERARDS, and G. WHITTLE (2006). On Rota’s conjecture and excluded minors containing large projective geometries, *J. Combin. Theory Ser. B*, volume 96, no. 3, pp. 405–425. Cited on pp. 21, 145, and 147.
- J. GEELEN, B. GERARDS, and G. WHITTLE (2007). Towards a matroid-minor structure theory, in *Combinatorics, complexity, and chance*, volume 34 of *Oxford Lecture Ser. Math. Appl.*, pp. 72–82, Oxford Univ. Press, Oxford. Cited on p. 148.
- J. GEELEN, P. HLINĚNÝ, and G. WHITTLE (2005). Bridging separations in matroids, *Siam Journal on Discrete Mathematics*, volume 18, pp. 638–646. Cited on pp. 121, 123, and 134.
- J. GEELEN, J. OXLEY, D. VERTIGAN, and G. WHITTLE (1998). Weak maps and stabilizers of classes of matroids, *Adv. in Appl. Math.*, volume 21, no. 2, pp. 305–341. Cited on pp. 20, 130, and 137.
- J. GEELEN, J. OXLEY, D. VERTIGAN, and G. WHITTLE (2002). Totally free expansions of matroids, *J. Combin. Theory Ser. B*, volume 84, no. 1, pp. 130–179. Cited on pp. 20, 21, 130, 137, and 145.
- J. GEELEN and G. WHITTLE (2002). Branch-width and Rota’s conjecture, *J. Combin. Theory Ser. B*, volume 86, no. 2, pp. 315–330. Cited on pp. 21 and 123.
- J. F. GEELEN, A. M. H. GERARDS, and A. KAPOOR (2000). The excluded minors for $\text{GF}(4)$ -representable matroids, *J. Combin. Theory Ser. B*, volume 79, no. 2, pp. 247–299. Cited on pp. 14, 21, 97, 118, 120, 121, 124, 126, 148, 159, and 160.
- A. M. H. GERARDS (1989). A short proof of Tutte’s characterization of totally unimodular matrices, *Linear Algebra Appl.*, volume 114/115, pp. 207–212. Cited on pp. 20, 97, 98, 100, and 108.
- R. HALL, D. MAYHEW, and S. H. M. VAN ZWAM (2009). The excluded minors for near-regular matroids. Submitted. Preprint at arXiv:0902.2071v2 [math.CO]. Cited on pp. 97, 141, 148, 159, and 161.
- G. H. HARDY and E. M. WRIGHT (1954). An Introduction to the Theory of Numbers, Oxford, at the Clarendon Press. 3rd ed. Cited on pp. 166 and 167.
- M. HAZEWINKEL (editor) (1989). Encyclopaedia of Mathematics. Vol. 3. D–Feynman Measure, Kluwer Academic Publishers, Dordrecht, ISBN 1-55608-002-6. Available online at <http://eom.springer.de/D/default.htm>. Cited on p. 64.

- M. HAZEWINKEL (editor) (1996). Handbook of Algebra. Vol. 1, North-Holland Publishing Co., Amsterdam, ISBN 0-444-82212-7. Cited on p. 7.
- P. HLINĚNÝ (2004). Using a computer in matroid theory research, *Acta Univ. M. Belii Ser. Math.*, no. 11, pp. 27–44. Cited on p. 28.
- A. W. INGLETON (1971). Representation of matroids, in *Combinatorial Mathematics and its Applications* (Proc. Conf., Oxford, 1969), pp. 149–167, Academic Press, London. Cited on p. 73.
- J. KAHN (1988). On the uniqueness of matroid representations over $\text{GF}(4)$, *Bull. London Math. Soc.*, volume 20, no. 1, pp. 5–10. Cited on p. 20.
- J. KAHN and J. P. S. KUNG (1982). Varieties of combinatorial geometries, *Trans. Amer. Math. Soc.*, volume 271, no. 2, pp. 485–499. Cited on p. 19.
- I. KAPLANSKY (1969). Linear Algebra and Geometry. A Second Course, Allyn and Bacon Inc., Boston, Mass. Cited on pp. 6 and 7.
- J. P. S. KUNG (1986). A Source Book in Matroid Theory, Birkhäuser. Cited on p. 16.
- T. LAZARSON (1958). The representation problem for independence functions, *J. London Math. Soc.*, volume 33, pp. 21–25. Cited on pp. 14 and 90.
- J. LEE (1990). The incidence structure of subspaces with well-scaled frames, *J. Combin. Theory Ser. B*, volume 50, no. 2, pp. 265–287. Cited on pp. 19 and 44.
- H. MATSUMURA (1986). Commutative Ring Theory, volume 8 of *Cambridge Studies in Advanced Mathematics*, Cambridge University Press, Cambridge, ISBN 0-521-25916-9. Translated from the Japanese by M. Reid. Cited on p. 165.
- D. MAYHEW and G. F. ROYLE (2008). Matroids with nine elements, *J. Combin. Theory Ser. B*, volume 98, no. 2, pp. 415–431. Cited on p. 92.
- D. MAYHEW, G. WHITTLE, and S. H. M. VAN ZWAM (2009). An obstacle to a decomposition theorem for near-regular matroids. Submitted. Preprint at arXiv:0905.3252 [Math.CO]. Cited on pp. 25, 44, and 148.
- J. R. NEWMAN (1956). The World of Mathematics. Vols. I–IV, Simon & Schuster, New York. A small library of the literature of mathematics from A'h-mosé the Scribe to Albert Einstein, presented with commentaries and notes. Cited on pp. 1 and 7.
- J. OXLEY, C. SEMPLE, and D. VERTIGAN (2000). Generalized Δ -Y exchange and k -regular matroids, *J. Combin. Theory Ser. B*, volume 79, no. 1, pp. 1–65. Cited on pp. 47, 50, 92, and 174.
- J. OXLEY, C. SEMPLE, and G. WHITTLE (2004). The structure of the 3-separations of 3-connected matroids, *J. Combin. Theory Ser. B*, volume 92, no. 2, pp. 257–293. Cited on p. 124.
- J. OXLEY, C. SEMPLE, and G. WHITTLE (2008). Maintaining 3-connectivity relative to a fixed basis, *Adv. in Appl. Math.*, volume 41, no. 1, pp. 1–9. Cited on p. 119.
- J. OXLEY, D. VERTIGAN, and G. WHITTLE (1996). On inequivalent representations of matroids over finite fields, *J. Combin. Theory Ser. B*, volume 67, no. 2, pp. 325–343. Cited on pp. 20 and 131.
- J. G. OXLEY (1992). Matroid Theory, Oxford University Press. Cited on pp. 9, 10, 11, 12, 13, 14, 16, 17, 19, 33, 42, 44, 47, 68, 71, 79, 82, 119, 152, and 160.
- R. A. PENDAVINGH and S. H. M. VAN ZWAM (2008). Confinement of matroid representations to subsets of partial fields. Submitted. Preprint at arXiv:0806.4487 [math.CO]. Cited on pp. 25, 77, and 131.

- R. A. PENDAVINGH and S. H. M. VAN ZWAM (2009a). Lifts of matroid representations over partial fields, *J. Combin. Theory Ser. B*. In press. Preprint at arXiv:0804.3263 [math.CO]. Cited on pp. 25, 63, 77, and 97.
- R. A. PENDAVINGH and S. H. M. VAN ZWAM (2009b). Representing some non-representable matroids. In preparation. Cited on pp. 25 and 77.
- I. PETERSON (January 25, 1999). Medieval harmony, in Ivars Peterson's MathTrek, MAA Online column. http://www.maa.org/mathland/mathtrik_1_25_99.html. Cited on p. 57.
- G.-C. ROTA (1971). Combinatorial theory, old and new, in *Actes du Congrès International des Mathématiciens (Nice, 1970)*, Tome 3, pp. 229–233, Gauthier-Villars, Paris. Cited on pp. 14 and 147.
- A. SCHRIJVER (1986). *Theory of Linear and Integer Programming*, Wiley-Interscience Series in Discrete Mathematics, John Wiley & Sons Ltd., Chichester, ISBN 0-471-90854-1. A Wiley-Interscience Publication. Cited on p. 11.
- A. SCHRIJVER (2003). *Combinatorial Optimization. Polyhedra and Efficiency*, volume 24 of *Algorithms and Combinatorics*, Springer-Verlag, Berlin, ISBN 3-540-44389-4. Cited on p. 16.
- C. SEMPLE (1997). k -regular matroids, in *Combinatorics, complexity, & logic (Auckland, 1996)*, Springer Ser. Discrete Math. Theor. Comput. Sci., pp. 376–386, Springer, Singapore. Cited on pp. 19, 25, 50, 72, 173, and 174.
- C. SEMPLE and G. WHITTLE (1996a). On representable matroids having neither $U_{2,5}$ - nor $U_{3,5}$ -minors, in *Matroid theory (Seattle, WA, 1995)*, volume 197 of *Contemp. Math.*, pp. 377–386, Amer. Math. Soc., Providence, RI. Cited on pp. 97, 130, and 140.
- C. SEMPLE and G. WHITTLE (1996b). Partial fields and matroid representation, *Adv. in Appl. Math.*, volume 17, no. 2, pp. 184–208. Cited on pp. 19, 25, 58, and 63.
- C. A. SEMPLE (1998). *k -Regular Matroids*, Ph.D. thesis, Victoria University of Wellington. Cited on p. 50.
- P. D. SEYMOUR (1979). Matroid representation over $GF(3)$, *J. Combin. Theory Ser. B*, volume 26, no. 2, pp. 159–173. Cited on pp. 14 and 97.
- P. D. SEYMOUR (1980). Decomposition of regular matroids, *J. Combin. Theory Ser. B*, volume 28, no. 3, pp. 305–359. Cited on pp. 119 and 121.
- I. STEWART and D. TALL (2002). *Algebraic Number Theory and Fermat's Last Theorem*, 3rd edition, A K Peters Ltd., Natick, MA, ISBN 1-56881-119-5. Cited on pp. 165, 166, and 167.
- K. TRUEMPER (1985). A decomposition theory for matroids. I. General results, *J. Combin. Theory Ser. B*, volume 39, no. 1, pp. 43–76. Cited on p. 42.
- K. TRUEMPER (1986). A decomposition theory for matroids. III. Decomposition conditions, *J. Combin. Theory Ser. B*, volume 41, no. 3, pp. 275–305. Cited on pp. 121 and 134.
- K. TRUEMPER (1992a). A decomposition theory of matroids. VI. Almost regular matroids, *J. Combin. Theory Ser. B*, volume 55, no. 2, pp. 235–301. Cited on p. 150.
- K. TRUEMPER (1992b). *Matroid Decomposition*, Academic Press, Inc. Available online at <http://www.emis.de/monographs/md/>. Cited on p. 16.
- W. T. TUTTE (1958). A homotopy theorem for matroids. I, II, *Trans. Amer. Math. Soc.*, volume 88, pp. 144–174. Cited on pp. 14, 18, and 97.
- W. T. TUTTE (1965). Lectures on matroids, *J. Res. Nat. Bur. Standards Sect. B*, volume 69B, pp. 1–47. Cited on pp. 11, 19, 64, 68, 70, 79, 97, and 108.

- P VÁMOS (1971). A necessary and sufficient condition for a matroid to be linear, in Möbius algebras (Proc. Conf., Univ. Waterloo, Waterloo, Ont., 1971), pp. 162–169, Univ. Waterloo, Waterloo, Ont. Cited on p. [19](#).
- N. WHITE (1987). Coordinatizations, in Combinatorial geometries, volume 29 of *Encyclopedia Math. Appl.*, pp. 1–27, Cambridge Univ. Press, Cambridge. Cited on p. [69](#).
- N. L. WHITE (1975a). The bracket ring of a combinatorial geometry. I, *Trans. Amer. Math. Soc.*, volume 202, pp. 79–95. Cited on pp. [19](#), [84](#), and [85](#).
- N. L. WHITE (1975b). The bracket ring of a combinatorial geometry. II. Unimodular geometries, *Trans. Amer. Math. Soc.*, volume 214, pp. 233–248. Cited on p. [19](#).
- H. WHITNEY (1935). On the abstract properties of linear dependence, *Amer. J. Math.*, volume 57, no. 3, pp. 509–533. Cited on pp. [7](#), [8](#), [19](#), and [64](#).
- G. WHITTLE (1995). A characterisation of the matroids representable over $\text{GF}(3)$ and the rationals, *J. Combin. Theory Ser. B*, volume 65, no. 2, pp. 222–261. Cited on pp. [11](#), [18](#), [79](#), and [95](#).
- G. WHITTLE (1996). Inequivalent representations of ternary matroids, *Discrete Math.*, volume 149, no. 1-3, pp. 233–238. Cited on pp. [131](#) and [138](#).
- G. WHITTLE (1997). On matroids representable over $\text{GF}(3)$ and other fields, *Trans. Amer. Math. Soc.*, volume 349, no. 2, pp. 579–603. Cited on pp. [11](#), [18](#), [21](#), [79](#), [95](#), [108](#), [129](#), [130](#), and [139](#).
- G. WHITTLE (1999). Stabilizers of classes of representable matroids, *J. Combin. Theory Ser. B*, volume 77, no. 1, pp. 39–72. Cited on pp. [20](#), [109](#), [130](#), [136](#), [142](#), and [152](#).
- T. ZASLAVSKY (1989). Biased graphs. I. Bias, balance, and gains, *J. Combin. Theory Ser. B*, volume 47, no. 1, pp. 32–52. Cited on pp. [19](#), [72](#), and [80](#).

Index

- 3-connected, 119
- 1-sum, *see* direct sum
- 2-connected, 119
- 2-separation, 126, 132
 - crossing, 124, 156
 - number of $-$ s, 120
- 2-sum, 47, 129, 131
- 3-connected, 149, 151

- Affine geometry, 82
- associates, 29

- basis, 9
- Betsy Ross matroid, 92
- blocking sequence, 120, 123, 126, 132
- bounded canopy, 148
- bracket ring, 84
- branch decomposition, 122
- branch width, 122, 148, 156

- chain group, 64, 97
- characteristic set, 73
- circuit, 9, 169
 - fundamental $-$, 43
- closure, 44
- cobasis, 12
- cocircuit, 12
- coincident set, 12
- coloop, 115
- component, 8, 169
- confine, 131
- Confinement Theorem, 115, 129, 131, 143
- connected, 42
- connectivity
 - graph $-$, 169
 - matroid $-$, 42, 115, 117, 119

- contraction, 13
- contraction pair
 - weak $-$, 100
- cosimplification, 123
- cross ratio, 2, 6, 16, 29, 37, 39, 86, 110, 138
- cryptomorphism, 9
- cycle, 169

- degree, 169
- deletion, 13
- deletion pair, 152
 - weak $-$, 100
- Delta-Y exchange, 47, 92
- determinant, 35, 168
- direct product, 78, 95
- direct sum, 42
- distance, 169
- Dowling geometry, 77, 80
- Dowling lift, 81, 90
- dual, 12, 40, 85, 117, 150, 151

- equivalence, 37, 92
 - scaling, *see* scaling-equivalent
 - scaling- $-$, 100, 116
 - strong $-$, 37, 41
- excluded minor, 14, 21, 97, 108, 123, 147, 151, 159

- Fano matroid, 15, 97, 108, 159
- flat, 44
 - modular $-$, 44
- flower, 124
- forest, 8, 169
- fragile, *see* N -fragile
- fundamental element, 28, 38, 41, 47, 72, 78

- of induced sub-partial field, 30
- generalized parallel connection, 46
- Gröbner basis, 82, 86, 112, 142
- graph, 8, 168
 - bipartite –, 33, 43, 169
- ground set, 8
- homomorphism, *see* partial field homomorphism
- ideal, 165
 - maximal, 26
 - maximal –, 165
 - prime, 166
- incriminating set, 101, 153
- induced
 - k -separation, *see* k -separation
 - sub-partial field, 30, 38, 73, 129
 - subgraph, *see* subgraph
- isomorphism
 - between matrices, 36
 - between matroids, 13
 - between partial fields, *see* partial field
- k -connected, 42, 118
- k -separation, 42, 121
 - induced –, 120
- Krull's Theorem, 165
- lift
 - global –, 98, 105
 - local –, 98
- lift ring, *see* partial field, lift
- Lift Theorem, 20, 95, 98
- lifting function, 98
- linear dependence, 8
- loop, 115
- matrix, 10
 - golden ratio –, 11
 - graphic –, 80
 - identity –, 10
 - operations, 168
 - strong \mathbb{P} –, *see* \mathbb{P} -matrix
 - totally dyadic –, 11
 - totally unimodular –, 11
 - weak \mathbb{P} –, 26, 30, 31
 - nondegenerate –, 26
- matroid, 8, 40
 - binary –, 11, 14, 15, 17, 79, 82, 108, 130, 140, 150
 - geometric representation, 15
 - graphic, 8
 - \mathbb{P} -graphic, 80
 - quaternary –, 11, 14, 82, 92, 109, 110, 160
 - quinary –, 20, 54, 82, 109, 130, 140, 161
 - regular –, 11, 79, 121
 - ternary –, 11, 14, 17, 21, 79, 82, 95, 108, 130, 138–140
 - theory, 7
- minor, 118
 - of a matrix, 36, 41
 - of a matroid, 13, 41, 80, 88, 116
- minor-closed, 14, 41
- N -fragile, 148, 148, 156
- Non-Fano matroid, 97, 159
- Non-Pappus matroid, 71
- normalized, 33, 38, 87, 132
- \mathbb{P} -matrix, 31, 32, 36
 - scaled –, 38
- parallel, 116, 123, 150
- partial field, 19, 25
 - $\sqrt[6]{1}$ –, 50, 79, 82, 92, 129, 139, 160
 - automorphism, 28, 92
 - axioms, 58
 - dyadic, 139
 - dyadic –, 48, 82, 92, 95, 129, 140
 - finitary –, 147
 - Gaussian –, 52, 82, 109
 - Gersonides –, 57
 - golden ratio –, 52, 82, 92, 109
 - homomorphism, 26, 27, 36, 41, 47, 63, 78, 98, 137
 - hydra- k , 142–144
 - hydra- k –, 52–55, 161
 - isomorphism, 28, 79
 - k -cyclotomic –, 55, 82, 92
 - k -regular, *see* k -uniform

- k -uniform –, 50, 88
 - level –, 113
 - lift –, 111, 139, 142
 - near-regular –, 49, 82, 108, 139, 159
 - regular –, 47, 79, 82, 108, 139
 - sixth-roots-of-unity –, *see* $\sqrt[6]{1}$
 - skew –, 64, 93
 - sub –, 29, 38, 40, 41, 129
 - induced, *see under* induced
 - trivial, 26
 - universal, 77
 - universal –, 86, 87, 137
- path, 169
- permuting, 32
- perspective, 1
- pivot, 34, 67, 85, 102, 132, 153
- product ring, 165
- projection, 13
- projective
 - geometry, 4, 15
 - plane, 4
 - space, 4
 - transformation, 5, 17
- projectivity, 3
- quaternion, 71
- rank, 10
- representation, 10, 17
 - over $\text{GF}(q)$, *see* matroid: binary, ternary, ...
 - over a field, 11, 11, 79, 85, 108
 - over a partial field, 26, 40, 43, 47, 79, 108, 115
 - over a skew partial field, 65
- ring of integers of a number field, 166
- Rota's Conjecture, 14, 147
- row span, 65
- scaling-equivalent, 32
- segment-cosegment exchange, 47, 92
- separation, *see* k -separation
- separator, 42, 44
- series, 116, 123, 150
- settle, 137
- Settlement Theorem, 137
- Seymour's Splitter Theorem, 119, 152
- signature, 39
- simplification, 116, 123
- spanning
 - forest, 88, 169
 - tree, *see* spanning forest
- spike, 145
- Splitter Theorem, *see* Seymour's Splitter Theorem
- stabilizer, 136, 140, 142
 - strong, 137
 - strong –, 148, 152
- Stabilizer Theorem, *see* Whittle's Stabilizer Theorem
- subdeterminant, 31
- subgraph, 168
 - induced –, 80, 169
- submodular, 10, 117
- totally free expansion, 137
- tree, 169
 - cubic, 121
- Tutte's Homotopy Theorem, 70, 97
- unit, 165
- units
 - group of, 165
- walk, 169
- Wedderburn's Theorem, 72
- wheel, 119
- whirl, 119, 124
- Whittle's Stabilizer Theorem, 109, 136

Notation

The index of notation has been divided into five categories. Notation used only in a single section has not been included. Numbers refer to the page where the concept is defined. Usually letters such as A, D, F refer to matrices, M, N to matroids, G to a group or a graph, R to a ring, \mathbb{F} to a field, and \mathbb{P} to a partial field. Other capital letters are generally sets. For individual partial fields such as \mathbb{D} , \mathbb{S} , and \mathbb{U}_k , see Appendix B.

Sets, groups, rings, fields, functions

2^E	Power set. Collection of all subsets of E , 13
$f(S)$	The set $\{f(s) \mid s \in S\}$
$\text{GF}(q)$	Finite field with q elements
$\ker(f)$	The elements s in the domain of f with $f(s) = 0$
\mathbb{N}	Natural numbers. In this thesis $0 \in \mathbb{N}$, 13
\mathbb{Q}	The field of rational numbers
\mathbb{C}	The field of complex numbers
\mathbb{R}	The field of real numbers
$R_1 \times R_2$	The product ring of R_1 and R_2 , 203
R^*	The group of units of the ring R
$R[x_1, \dots, x_n]$	The ring of polynomials over R in variables x_1, \dots, x_n
(S)	The ideal generated by set S
$\langle S \rangle$	The (multiplicative) group generated by set S
$X - Y$	Set difference, 11
$X \cup e$	$X \cup \{e\}$, 11
$X \Delta Y$	The symmetric difference, i.e. $(X - Y) \cup (Y - X)$, 13
$X - e$	$X - \{e\}$, 11
$ X $	Cardinality of set X , 11
\mathbb{Z}	The ring of integers

Partial fields

$\uparrow : \mathcal{F}(\mathbb{P}) \rightarrow \mathcal{F}(\widehat{\mathbb{P}})$	Lifting function: partial inverse of a homomorphism $\varphi : \widehat{\mathbb{P}} \rightarrow \mathbb{P}$, 118
$\text{Asc}(S)$	The set of <i>associates</i> of S , i.e. the smallest set $T \supseteq S$ such that $1 - p \in T$ for all $p \in T$, and $1/p \in T$ for all nonzero $p \in T$, 36
$\mathbb{D}\mathbb{P}$	Dowling lift of \mathbb{P} , 98
$\varphi_{M,U,V}$	The canonical homomorphism $\mathbb{P}_{M/U \setminus V} \rightarrow \mathbb{P}_M$, 106
$\mathcal{F}(\mathbb{P})$	The set of fundamental elements of \mathbb{P} , i.e. $\{p \in \mathbb{P} \mid 1 - p \in \mathbb{P}\}$, 35
$\mathbb{L}\mathbb{P}$	The lift partial field of \mathbb{P} , 134

$\mathbb{P} = (R, G)$	The partial field with ring R and group $G \subseteq R^*$, such that $-1 \in G$, 32
$\mathbb{P}_1 \cong \mathbb{P}_2$	There is a partial-field isomorphism $\mathbb{P}_1 \rightarrow \mathbb{P}_2$, 35
$\mathbb{P}_1 \times \mathbb{P}_2$	The direct product of $\mathbb{P}_1, \mathbb{P}_2$, 94
$\mathbb{P}' \subseteq \mathbb{P}$	\mathbb{P}' is a sub-partial field of \mathbb{P} , 37
\mathbb{P}_M	The universal partial field of matroid M , 104
$\mathbb{P}[S]$	Sub-partial field of \mathbb{P} generated by S , i.e. $(R, \langle S \cup \{-1\} \rangle)$, 37
Graphs	
$d_G(u, v)$	The distance between vertices u, v in graph G , 208
$d_G(U, W)$	The distance between vertex sets U, W in graph G , 209
$G[V']$	Subgraph of G induced by vertices V' , 207
$G = (V, E)$	Graph with vertices V and edges E , 207
(v_0, \dots, v_n)	Walk in a graph, 208
Matroids	
$\text{bw}(M)$	The branch width of M , 149
$\text{co}(M)$	The cosimplification of M , 143
$E(M)$	Set of elements of a matroid M , 11
F_7	The Fano matroid, 20
$G(M, B)$	The B -fundamental-circuit incidence graph, 54
$\lambda_M(Z)$	The connectivity of set Z in M , i.e. $\text{rk}_M(Z) + \text{rk}_M(E - Z) - \text{rk}(M)$, 52
$\lambda_B(X, Y)$	Connectivity with respect to B , i.e. $\text{rk}_{M/(B-Y)}(X-B) + \text{rk}_{M/(B-X)}(Y-B)$, 145
$M = (E, \mathcal{I})$	Matroid with ground set E and independent sets \mathcal{I} , 11
$M \oplus_2 N$	The 2-sum of M and N , 58
$M_1 \oplus M_2$	The direct sum of matroid M_1 and M_2 , 53
$M[A]$	Matroid induced by the columns of matrix A , 33
$M_B[Z]$	If $Y = E(M) - B$, then this is $M/(B - Z) \setminus (Y - Z)$, 144
$M_B - Z$	Equal to $M_B[E(M) - Z]$, 144
M/X	Contraction of X from M , 17
$M \setminus X$	Deletion of X from M , 17
$M \cong N$	Matroids M and N are isomorphic, 17
$\mathcal{M}(\mathbb{P})$	The set of matroids representable over the partial field \mathbb{P} , 33
M^*	Dual matroid of M , 16
$N \preceq M$	N is a minor of M , i.e. $N \cong M/S \setminus T$ for some $S, T \subseteq E(M)$, 18
P_8	The matroid P_8 , 110
$\text{PG}(n, \mathbb{F})$	Projective space of dimension n over \mathbb{F} , 8
$\text{PG}(n, q)$	Equal to $\text{PG}(n, \text{GF}(q))$, 19
$\text{rk}_M(X)$	Rank of set X in matroid M , 13
$\text{rk}(M)$	Rank of matroid M , 13
$\text{si}(M)$	The simplification of M , 142
$U_{2,4}$	Rank-2 uniform matroid on 4 elements, 21
$U_{r,n}$	The rank- r uniform matroid on n elements
\mathcal{W}_n	The rank- n wheel, 146
\mathcal{W}^n	The rank- n whirl, 146
Matrices	
$A' \preceq A$	A' is isomorphic to a minor of matrix A , 46
$A' \approx A$	A' can be obtained from A through pivoting, scaling, and permut-

	ing, 46
$[A_1 A_2]$	Composition of two matrices, 14
$[I A]$	Defined as $[I_X A]$, if A is an $X \times Y$ matrix, 14
$A \sim A'$	A and A' are scaling-equivalent, 40
$A[X', Y']$	Submatrix of A induced by rows X' and columns Y' , 14
A^{xy}	The matrix obtained from A by pivoting over xy , 42
$A[Z]$	Submatrix of the $X \times Y$ matrix A induced by rows $X \cap Z$ and columns $Y \cap Z$, 14
$A - Z$	Submatrix of the $X \times Y$ matrix A induced by rows $X - Z$ and columns $Y - Z$, 14
$\text{Cr}(A)$	The set of cross ratios of A , 47
$\det(A)$	Determinant of the square matrix A , 206
$G(A)$	The bipartite graphs with the rows and columns of A as vertex classes and the nonzero entries as edges, 41
I_X	The $X \times X$ identity matrix, 14
$\text{rk}(A)$	The rank of a \mathbb{P} -matrix A , i.e. the size of the biggest square submatrix with nonzero determinant, 40
$\sigma_A(C)$	Signature of the cycle C of $G(A)$, 48