Lifts of matroid representations over partial fields

R. A. Pendavingh and S. H. M. van Zwam*

April 21, 2008

Dedicated to Lex Schrijver on the occasion of his sixtieth birthday.

Abstract

There exist several theorems which state that when a matroid is representable over distinct fields $\mathbb{F}_1, \ldots, \mathbb{F}_k$, it is also representable over other fields. We prove a theorem, the Lift Theorem, that implies many of these results.

First, parts of Whittle's characterization of representations of ternary matroids follow from our theorem. Second, we prove the following theorem by Vertigan: if a matroid is representable over both GF(4) and GF(5), then it is representable over the real numbers by a matrix such that the absolute value of the determinant of every nonsingular square submatrix is a power of the golden ratio. Third, we give a characterization of the 3-connected matroids having at least two inequivalent representations over GF(5). We show that these are representable over the complex numbers.

Additionally we provide an algebraic construction that, for any set of fields $\mathbb{F}_1, \ldots, \mathbb{F}_k$, gives the best possible result that can be proven using the Lift Theorem.

1 Introduction

Questions regarding the representability of matroids pervade matroid theory. They underly some of the most celebrated results of the field, as well as some tantalizing conjectures. A famous theorem is the characterization of regular matroids due to Tutte. We say that a matrix over the real numbers is *totally unimodular* if the determinant of every square submatrix is in the set $\{-1, 0, 1\}$.

Theorem 1.1 (Tutte [Tut65])**.** *Let M be a matroid. The following are equivalent:*

(i) M is representable over both GF(2) *and* GF(3)*;*

(ii) M is representable by a totally unimodular matrix;

(iii) M is representable over every field.

*E-mail: rudi@win.tue.nl, svzwam@win.tue.nl. This research was supported by NWO, grant 613.000.561.

Whittle [Whi95, Whi97] proved very interesting results of a similar nature. Here is one example. We say that a matrix over the real numbers is *dyadic* if the determinant of every square submatrix is in the set $\{0\} \cup \{\pm 2^k \mid k \in \mathbb{Z}\}$.

Theorem 1.2 (Whittle [Whi97]). *Let M be a matroid. The following are equivalent:*

(i) *M is representable over both* GF(3) *and* $GF(5)$*;*

(ii) *M is representable by a dyadic matrix;*

(iii) *M is representable over every field that does not have characteristic 2.*

A third example is the following result. 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 $x^2 - x - 1 = 0$.

Theorem 1.3 (Vertigan). *Let M be a matroid. The following are equivalent:*

(i) *M is representable over both* GF(4) *and* $GF(5)$*;*

(ii) *M is representable by a golden ratio matrix;*

(iii) *M is representable over* $\mathrm{GF}(p)$ *for all primes p such that $p = 5$ or $p \equiv \pm 1 \mod 5$, and also over* $\mathrm{GF}(p^2)$ *for all primes p.*

The common feature of these theorems is that representability over a set of finite fields is characterized by the existence of a representation matrix over some field such that the determinants of square submatrices are restricted to a certain set S. Semple and Whittle [SW96] generalized this idea. They introduced *partial fields*: algebraic structures 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 this paper we present a general theorem on partial fields from which results like Theorems 1.1–1.3 follow. We employ a mixture of combinatorial and algebraic techniques.

We start our paper, in Section 2, with a summary of the work of Semple and Whittle [SW96]. We note here that we have changed the definition of what it means for a sum to be *defined*, because with the definition proposed by Semple and Whittle a basic proposition, on which much of their work is based, is false. We give numerous additional definitions and basic results, and introduce notation to facilitate reasoning about representation matrices of a matroid. The ideas behind our definitions are ubiquitous — they capture the way Truemper [Tru92] relates matroids and representation matrices, they occur in Section 6.4 of Oxley [Oxl92], and even the "representative matrices associated with a dendroid" in Tutte [Tut58] are essentially the same thing. There appears to be no consensus about notation.

Section 3 contains the main theorem of this paper, the Lift Theorem (Theorem 3.5). It gives a sufficient condition under which a matroid that is representable over a partial field $\mathbb{P}$ is also representable over a partial field $\widehat{\mathbb{P}}$. The condition is such that it can be checked for classes of matroids as well.

In Section 4 we give applications of the Lift Theorem. First we give alternative proofs for a significant part of Whittle's [Whi97] characterization of the ternary matroids that are representable over some field of characteristic other than 3. We also prove Theorem 1.3 and two new results, namely a characterization of the 3-connected matroids that have at least two inequivalent representations over GF(5), and a characterization of the subset of these that is also representable over GF(4).

Another result by Vertigan, Theorem 2.16, states that every partial field can be seen as a subgroup of the group of units of a commutative ring. We give a proof of this theorem in Section 5. We show that a matroid representable over some partial field is in fact representable over a field. This complements the theorem by Rado [Rad57] that every matroid representable over a field is also representable over a finite field. We also show that for every partial field homomorphism there exists a ring homomorphism between the corresponding rings.

We use these insights to define a ring and corresponding partial field for which, by construction, the premises of the Lift Theorem hold. With this partial field we can formulate a result like Theorems 1.1–1.3 for any finite set of finite fields. We show that our construction gives the "best possible" partial field to which the Lift Theorem applies.

Finally we present, in Section 6, a number of unsolved problems that arose during our investigations.

In a related paper [PZ] we show that in some instances the Lift Theorem can be pushed a little further. In particular we show that for a 3-connected matroid M it may happen that only a sub-partial field is needed to represent M.

The statements of Theorems 1.3 and 2.16 were mentioned in Geelen et al. [GOVW98] and in Whittle [Whi05] as unpublished results of Vertigan. This work was started because we wanted to understand Vertigan's results. Our proofs were found independently. Vertigan informs us that he proved Theorem 1.3 through a general construction similar to Definition 5.6.

2 Preliminaries

2.1 Notation

If S, T are sets, and $f : S \to T$ is a function, then we define

$$f(S) := \{f(s) \mid s \in S\}. \tag{1}$$

We denote the restriction of f to $S' \subseteq S$ by $f|_{S'}$. We may simply write e instead of the singleton set $\{e\}$.

If S is a subset of elements of some group, then $\langle S \rangle$ is the subgroup generated by S. If S is a subset of elements of a ring, then $\langle S \rangle$ denotes the *multiplicative* subgroup generated by S. All rings are commutative with identity. The group of elements with a multiplicative inverse (the *units*) of a ring $\mathbb{O}$ is denoted by $\mathbb{O}^*$. If $\mathbb{O}$ is a ring and S a set of symbols, then we denote the *free* $\mathbb{O}$*-module* on S by $\mathbb{O}[S]$.

Our graph-theoretic notation is mostly standard. All graphs encountered are simple. We use the term *cycle* for a simple, closed path in a graph, reserving *circuit* for a minimal dependent set in a matroid. An undirected edge (directed edge) between vertices u and v is denoted by uv and treated as a set $\{u,v\}$ (an ordered pair (u,v)). We define $\delta(v) := \{e \in E(G) \mid e = uv \text{ for some } u \in V\}$.

For matroid-theoretic concepts we follow the notation of Oxley [Oxl92]. Familiarity with the definitions and results in that work is assumed.

2.2 The partial-field axioms

The following definitions are taken from Semple and Whittle [SW96].

Definition 2.1. *Let P be a set with distinguished elements called* 0, 1. *Suppose $\cdot$ is a binary operation and $+$ a partial binary operation on P. If $p,q \in P$ then we abbreviate $p \cdot q$ to pq. A* partial field *is a 5-tuple*

$$\mathbb{P} := (P, +, \cdot, 0, 1) \tag{2}$$

satisfying the following axioms:

(P1) $(P \setminus \{0\}, \cdot, 1)$ *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 $p,q,r \in P$, $p(q + r)$ is defined if and only if $pq + pr$ is defined. Then $p(q + r) = pq + pr$.*

(P6) *The* associative law *holds for $+$.*

We write $p + q \doteq r$ if we mean "the sum of p and q is defined and is equal to r". The group in Axiom (P1) is denoted by $\mathbb{P}^*$, and we write $p \in \mathbb{P}$ if p is an element of the set P underlying the partial field.

Given a multiset $S = \{p_1, \ldots, p_n\}$ 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 $u + w$. 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.

We say that the expression $p_1+\cdots+p_n$ is *defined* if there exists a finite multiset Z of the form $\{z_1,-z_1,z_2,-z_2,\ldots,z_k,-z_k\}$ such that there exists an association for $\{p_1,\ldots,p_n\}\cup Z$. The value of $p_1+\cdots+p_n$ is then defined as the value of r for any association T of S. Note that this definition differs from the one given by Semple and Whittle. A justification for this modification is given in Appendix A.

Partial fields share several basic properties with fields. We use the following implicitly in this paper:

Proposition 2.2. *Let $\mathbb{P}$ be a partial field. The following statements hold for all $p,q\in\mathbb{P}$:*

(i) $0p=0$;

(ii) $pq=0$ *if and only if* $p=0$ *or* $q=0$;

(iii) $(-1)^2=1$;

(iv) if $p^2=1$, *then* $p=1$ *or* $p=-1$;

(v) if $p+q\doteq r$, *then* $r-q\doteq p$.

The proofs are elementary.

2.3 Partial-field matrices

Recall that formally, for ordered sets X and Y, an $X\times Y$ matrix A with entries in a partial field $\mathbb{P}$ is a function $A:X\times Y\to\mathbb{P}$. Let A be an $n\times n$ matrix with entries in $\mathbb{P}$. Then the *determinant* of A is, as always,

$$\det(A):=\sum_{\sigma\in S_n}\operatorname{sgn}(\sigma)a_{1\sigma(1)}a_{2\sigma(2)}\cdots a_{n\sigma(n)}. \tag{3}$$

We say that $\det(A)$ is *defined* if this sum is defined.

Proposition 2.3 ([SW96, Proposition 3.1])**.** *Let $\mathbb{P}$ be a partial field and let A be an $n\times n$ matrix with entries in $\mathbb{P}$ such that $\det(A)$ is defined.*

(i) If B is obtained from A by transposition, then $\det(B)\doteq\det(A)$.

(ii) If B is obtained from A by interchanging a pair of rows, then $\det(B)\doteq-\det(A)$.

(iii) If B is obtained from A by multiplying a row by a non-zero element $p\in\mathbb{P}^*$, then $\det(B)\doteq p\det(A)$.

(iv) If B is obtained from A by adding two rows whose sum is defined, then $\det(B)\doteq\det(A)$.

An $X\times Y$ matrix A with entries in $\mathbb{P}$ is a *$\mathbb{P}$-matrix* if $\det(A')$ is defined for every square submatrix A' of A. For such a matrix we define the *rank*

$$\operatorname{rank}(A):=\max\{r\mid A\text{ has an }r\times r\text{ submatrix }A'\text{ with }\det(A')\neq 0\}. \tag{4}$$

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 we define A^{xy} to be the $(X\setminus x\cup y)\times(Y\setminus y\cup x)$ matrix given by

$$(A^{xy})_{uv}=\begin{cases}A_{xy}^{-1} & \text{if } uv=yx\\ A_{xy}^{-1}A_{xv} & \text{if } u=y,v\neq x\\ -A_{xy}^{-1}A_{uy} & \text{if } v=x,u\neq y\\ A_{uv}-A_{xy}^{-1}A_{uy}A_{xv} & \text{otherwise.}\end{cases} \tag{5}$$

We say that A^{xy} is obtained from A by *pivoting* over xy. In other words, if $X = X' \cup x, Y = Y' \cup y$, and

$$A = \begin{array}{c} \\ x \\ X' \end{array} \begin{array}{c} \begin{array}{cc} y & Y' \end{array} \\ \left[\begin{array}{c|c} a & b \\ \hline c & D \end{array}\right] \end{array}, \tag{6}$$

where $a \in \mathbb{P}^*$, b is a row vector, c a column vector, and D an $X' \times Y'$ matrix, then

$$A^{xy} = \begin{array}{c} \\ y \\ X' \end{array} \begin{array}{c} \begin{array}{cc} x & Y' \end{array} \\ \left[\begin{array}{c|c} a^{-1} & a^{-1}b \\ \hline -a^{-1}c & D - a^{-1}cb \end{array}\right] \end{array}. \tag{7}$$

Definition 2.4. *Let A be an $X \times Y$ $\mathbb{P}$-matrix. We say that A' is a* minor *of A (notation: $A' \preceq A$) if A' can be obtained from A by a sequence of the following operations:*

(i) Multiplying the entries of a row or column by an element of $\mathbb{P}^*$;

(ii) Deleting rows or columns;

(iii) Permuting rows or columns (and permuting labels accordingly);

(iv) Pivoting over a nonzero entry.

Be aware that in linear algebra a minor of a matrix has a different definition. We use Definition 2.4 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*.

Proposition 2.5 ([SW96, Proposition 3.3])**.** *Let A be a $\mathbb{P}$-matrix. Then A^T is also a $\mathbb{P}$-matrix. If $A' \preceq A$ then A' is a $\mathbb{P}$-matrix.*

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 $X \setminus X'$, $Y \setminus Y'$. If Z is a subset of $X \cup Y$ then we define $A[Z] := A[X \cap Z, Y \cap Z]$. Also, $A - Z := A[X \setminus Z, Y \setminus Z]$. The following observation is used throughout this paper:

Lemma 2.6. *Let A be an $X \times Y$ matrix with entries in $\mathbb{P}$ such that $|X| = |Y|$. If $\det(A^{xy} - \{x, y\})$ is defined then $\det(A)$ is defined, and*

$$\det(A) = A_{xy} \det(A^{xy} - \{x, y\}). \tag{8}$$

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 $f : X \to X'$, $g : Y \to Y'$ such that for all $x \in X, y \in Y, A_{xy} = A'_{f(x)g(y)}$.

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 $A \sim A'$.

Let A be an $X \times Y$ $\mathbb{P}$-matrix, and let A' be an $X' \times Y'$ $\mathbb{P}$-matrix such that $X \cup Y = X' \cup Y'$. If $A' \preceq A$ and $A \preceq A'$, then we say that A and A' are *strongly equivalent*, which we denote by $A' \approx A$. If $\varphi(A') \approx A$ for some partial field automorphism φ (see below for a definition), then we say A' and A are *equivalent*.

2.4 Partial-field matroids

Let A be an $r \times E$ $\mathbb{P}$-matrix of rank r. We define the set

$$\mathscr{B}_A := \{B \subseteq E \mid |B| = r, \det(A[r,B]) \neq 0\}. \tag{9}$$

Theorem 2.7 ([SW96, Theorem 3.6]). *$\mathscr{B}_A$ is the set of bases of a matroid.*

We denote this matroid by $M(A) = (E, \mathscr{B}_A)$. Conversely, let M be a matroid. If there exists a $\mathbb{P}$-matrix A such that $M = M(A)$, then we say that M is $\mathbb{P}$-representable. These matroids share many properties of representable matroids.

Lemma 2.8 ([SW96, Proposition 4.1]). *Let A be an $r \times E$ $\mathbb{P}$-matrix, and B a basis of $M(A)$. Then there exists a $\mathbb{P}$-matrix A' such that $M(A') = M(A)$ and $A'[r,B]$ is an identity matrix.*

Conversely, let A be an $X \times Y$ matrix with entries in $\mathbb{P}$, where $X \cap Y = \emptyset$. Let A' be the $X \times (X \cup Y)$ matrix $A' = [I|A]$, where I is an $X \times X$ identity matrix. For all $X' \subseteq X \cup Y$ with $|X'| = |X|$ we have $\det(A'[X,X']) = \pm\det(A[X \setminus X', Y \cap X'])$. Hence A' is a $\mathbb{P}$-matrix if and only if A is a $\mathbb{P}$-matrix. We say that $M = M([I|A])$ is the matroid *associated with* A, and that $[I|A]$ is an *X-representation* of M for basis X.

If N is a minor of a matroid M, say $N = M\backslash S/T$, then a B-representation *displays* N if $B \cap T = T$ and $B \cap S = \emptyset$; then $N = M([I'|A'])$, where $A' = A - S - T$. Likewise we say that A *displays* A' if $A' = A - U$ for some $U \subseteq X \cup Y$.

Lemma 2.9. *If $M = M([I|A])$, then $N \preceq M$ if and only if $N \cong M([I'|A'])$ for some $A' \preceq A$.*

2.5 Partial-field homomorphisms

A function $\varphi : \mathbb{P}_1 \to \mathbb{P}_2$ is a *homomorphism* if, for all $p, q \in \mathbb{P}_1$, $\varphi(pq) = \varphi(p)\varphi(q)$ and, when $p + q$ is defined, then $\varphi(p) + \varphi(q) \doteq \varphi(p+q)$. A homomorphism is *trivial* if its kernel is equal to $\mathbb{P}_1$. This happens if and only if $\varphi(1) = 0$.

Proposition 2.10 ([SW96, Proposition 5.1]). *Let $\mathbb{P}_1, \mathbb{P}_2$ be partial fields and let $\varphi : \mathbb{P}_1 \to \mathbb{P}_2$ be a homomorphism. Let A be a $\mathbb{P}_1$-matrix. Then*

(i) *$\varphi(A)$ is a $\mathbb{P}_2$-matrix.*

(ii) *If A is square and $\det(A) = 0$ then $\det(\varphi(A)) = 0$.*

(iii) *If A is square and φ is nontrivial then $\det(A) = 0$ if and only if $\det(\varphi(A)) = 0$.*

This leads to the following easy corollary:

Corollary 2.11 ([SW96, Corollary 5.3]). *Let $\mathbb{P}_1$ and $\mathbb{P}_2$ be partial fields and let $\varphi : \mathbb{P}_1 \to \mathbb{P}_2$ be a nontrivial homomorphism. If A is a $\mathbb{P}_1$-matrix then $M(\varphi(A)) = M(A)$. It follows that, if M is a $\mathbb{P}_1$-representable matroid, then M is also $\mathbb{P}_2$-representable.*

A partial field isomorphism $\varphi : \mathbb{P}_1 \to \mathbb{P}_2$ is a bijective homomorphism with the additional property that $\varphi(p+q)$ is defined if and only if $p+q$ is defined. If $\mathbb{P}_1$ and $\mathbb{P}_2$ are isomorphic then we denote this by $\mathbb{P}_1 \cong \mathbb{P}_2$. A partial field automorphism is an isomorphism $\varphi : \mathbb{P} \to \mathbb{P}$.

2.6 Constructions

For a general partial field the associative law is hard to wield. Semple and Whittle get around this difficulty by constructing partial fields as restrictions of bigger partial fields, starting their construction with a field.

Definition 2.12. *Let $\mathbb{P}$ be a partial field, and let S be a set of elements of $\mathbb{P}^*$. Then*

$$\mathbb{P}[S] := (\langle S \cup -1\rangle \cup 0, 0, 1, +, \cdot), \tag{10}$$

where multiplication and addition are the restriction of the operations in $\mathbb{P}$, i.e. $p+q$ is defined only if $p+q \doteq r$ in $\mathbb{P}$ and $r \in \langle S \cup -1\rangle \cup 0$.

Proposition 2.13 ([SW96, Proposition 2.2])**.** *$\mathbb{P}[S]$ is a partial field.*

We need $-1 \in \mathbb{P}[S]$ to ensure that 1 has an additive inverse.

Instead of constructing a partial field as the restriction of a field, one can also take a ring as starting structure.

Definition 2.14. *Let $\mathbb{O}$ be a commutative ring, and let S be a subset of $\mathbb{O}^*$. Then*

$$\mathbb{P}(\mathbb{O}, S) := (\langle S \cup -1\rangle \cup 0, 0, 1, +, \cdot), \tag{11}$$

where multiplication and addition are the restriction of the operations in $\mathbb{O}$, i.e. $p+q$ is defined only if the resulting element of $\mathbb{O}$ is again in $\langle S \cup -1\rangle \cup 0$.

Proposition 2.15. *$\mathbb{P}(\mathbb{O}, S)$ is a partial field.*

Proof. First remark that $1 \in \mathbb{P}$ and that -1 is invertible in $\mathbb{O}$. The other axioms are then inherited from the corresponding ring axioms. □

In fact, Proposition 2.13 is a special case of this result. This follows from the following theorem:

Theorem 2.16 (Vertigan)**.** *If $\mathbb{P}$ is a partial field, then there exists a ring $\mathbb{O}$ and a set $S \subseteq \mathbb{O}^*$ such that $\mathbb{P} \cong \mathbb{P}(\mathbb{O}, S)$.*

We present a proof of this theorem in Section 5. A third source of partial fields is the following. If $\mathbb{P}_1, \mathbb{P}_2$ are partial fields, then we define the *direct product*

$$\mathbb{P}_1 \otimes \mathbb{P}_2 := (P, +, \cdot, (0,0), (1,1)), \tag{12}$$

where

$$P = \{(p_1, p_2) \in \mathbb{P}_1 \times \mathbb{P}_2 \mid p_1 \neq 0 \text{ if and only if } p_2 \neq 0\} \tag{13}$$

and addition and multiplication are defined componentwise, i.e. $(p_1, p_2) + (q_1, q_2) \doteq (p_1 + q_1, p_2 + q_2)$ if and only if both $p_1 + q_1$ and $p_2 + q_2$ are defined and $p_1 + q_1 = 0$ if and only if $p_2 + q_2 = 0$.

Lemma 2.17. *$\mathbb{P}_1 \otimes \mathbb{P}_2$ is a partial field.*

Proof. This follows from an application of Proposition 2.14: if $\mathbb{P}_i = \mathbb{P}(\mathbb{O}_i, S_i)$ then $\mathbb{P}_1 \otimes \mathbb{P}_2 = \mathbb{P}(\mathbb{O}_1 \times \mathbb{O}_2, S_1 \times S_2)$. □

Suppose $\mathbb{P}, \mathbb{P}_1, \mathbb{P}_2$ are partial fields such that there exist homomorphisms $\varphi_1 : \mathbb{P} \to \mathbb{P}_1$ and $\varphi_2 : \mathbb{P} \to \mathbb{P}_2$. Then we define $\varphi_1 \otimes \varphi_2 : \mathbb{P} \to \mathbb{P}_1 \otimes \mathbb{P}_2$ by $(\varphi_1 \otimes \varphi_2)(p) := (\varphi_1(p), \varphi_2(p))$.

Lemma 2.18. *$\varphi_1 \otimes \varphi_2$ is a partial field homomorphism.*

The proof is straightforward and therefore omitted.

Let X, Y be finite, disjoint sets, let A_1 be an $X \times Y$ $\mathbb{P}_1$-matrix, and let A_2 be an $X \times Y$ $\mathbb{P}_2$-matrix. Let $A := A_1 \otimes A_2$ be the $X \times Y$ matrix such that $A_{uv} = ((A_1)_{uv}, (A_2)_{uv})$.

Lemma 2.19. *If A_1 is a $\mathbb{P}_1$-matrix, A_2 is a $\mathbb{P}_2$-matrix, and $M([I|A_1]) = M([I|A_2])$ then $A_1 \otimes A_2$ is a $\mathbb{P}_1 \otimes \mathbb{P}_2$-matrix and $M([I|A_1 \otimes A_2]) = M([I|A_1])$.*

Proof. Let $X' \subseteq X, Y' \subseteq Y$ such that $A' := A[X', Y']$ is a square submatrix of A. Since $M([I|A_1]) = M([I|A_2])$, $\det(A_1[X', Y']) = 0$ if and only if $\det(A_2[X', Y']) = 0$. This holds for all 1×1 submatrices as well, so all entries of A are from $\mathbb{P}_1 \otimes \mathbb{P}_2$. By Lemma 2.6, a determinant can be computed by a sequence of pivots. It follows that $\det(A')$ is defined, which completes the proof. □

The following corollary plays a central role in this paper.

Corollary 2.20. *Let M be a matroid. M is representable over each of $\mathbb{P}_1, \ldots, \mathbb{P}_k$ if and only if it is representable over the partial field*

$$\mathbb{P} := \mathbb{P}_1 \otimes \cdots \otimes \mathbb{P}_k. \tag{14}$$

2.7 Cross ratios and fundamental elements

Let $B = \left[\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right]$ be a $\mathbb{P}$-matrix with $ps \neq 0$. We define the *cross ratio* of B as

$$\mathrm{cr}(B) := \frac{qr}{ps}. \tag{15}$$

The motivation for this name comes from projective geometry. If $\mathrm{cr}(B) \notin \{0, 1\}$ then the matroid $M([I|B])$ is the four-point line. In projective geometry the cross ratio is a number defined for any ordered set of four collinear points. It is invariant under projective transformations. For a fixed set of points this number can take six different values, depending on the order.

Let A be an $X \times Y$ $\mathbb{P}$-matrix. We define the *cross ratios* of A as the set

$$\mathrm{Cr}(A) := \left\{ \mathrm{cr}\left(\left[\begin{smallmatrix} 1 & 1 \\ p & 1 \end{smallmatrix}\right]\right) \mid \left[\begin{smallmatrix} 1 & 1 \\ p & 1 \end{smallmatrix}\right] \preceq A \right\}. \tag{16}$$

The following is obvious from the definition:

Lemma 2.21. *If $A' \preceq A$ then $\mathrm{Cr}(A') \subseteq \mathrm{Cr}(A)$.*

Note that $\det\left(\left[\begin{smallmatrix} 1 & 1 \\ p & 1 \end{smallmatrix}\right]\right) = 1 - p$. This prompts the following definition. An element $p \in \mathbb{P}$ is called *fundamental* if $1 - p \in \mathbb{P}$. As remarked by Semple [Sem97], $p + q$ is defined if and only if $p^{-1}(p + q) = 1 - (-q/p)$ is defined. For most partial fields that we consider, the equation $1 - p = q$ has only finitely many solutions. This is convenient if one wants to

compute in partial fields (cf. Hliněný [Hli04]). We denote the set of fundamental elements of $\mathbb{P}$ by $\mathscr{F}(\mathbb{P})$.

Suppose $F \subseteq \mathscr{F}(\mathbb{P})$. We define the *associates* of F as

$$\operatorname{asc} F := \bigcup_{p \in F} \operatorname{Cr}\left(\left[\begin{smallmatrix} 1 & 1 \\ p & 1 \end{smallmatrix}\right]\right). \tag{17}$$

We have

Proposition 2.22. $\operatorname{asc}\{p\} \subseteq \mathscr{F}(\mathbb{P})$.

The following lemma gives a complete description of the structure of $\operatorname{asc}\{p\}$.

Lemma 2.23. *If $p \in \{0,1\}$ then $\operatorname{asc}\{p\} = \{0,1\}$. If $p \in \mathscr{F}(\mathbb{P}) \setminus \{0,1\}$ then*

$$\operatorname{asc}\{p\} = \{p, 1-p, \frac{1}{1-p}, \frac{p}{p-1}, \frac{p-1}{p}, \frac{1}{p}\}. \tag{18}$$

The proof consists of a straightforward enumeration. By Lemma 2.21, $\operatorname{asc}\{p\} \subseteq \operatorname{Cr}(A)$ for every $p \in \operatorname{Cr}(A)$.

2.8 Normalization

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 $V(G) = B \cup (E \setminus B)$ and edges $E(G) = \{xy \in B \times (E \setminus B) \mid (B \setminus x) \cup y \in \mathscr{B}\}$. For each $y \in E \setminus B$ there is a unique matroid circuit $C_{B,y} \subseteq B \cup y$, the *$B$-fundamental circuit* of y.

Lemma 2.24. *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 [Oxl92, Section 6.4]. □

Let A be an $X \times Y$ matrix. With A we associate a bipartite graph $G(A) := (V,E)$, where $V := X \cup Y$ and let $E := \{xy \in X \times Y \mid A_{xy} \neq 0\}$.

Lemma 2.25. *Let $\mathbb{P}$ be a partial field. Suppose $M = M([I|A])$.*

(i) *$G(M,X) = G(A)$.*

(ii) *Let T be a spanning forest of $G(A)$ with edges $e_1, \ldots, e_k$. Let $p_1, \ldots, p_k \in \mathbb{P}^*$. Then there exists a matrix $A' \sim A$ such that $A'_{e_i} = p_i$.*

The proof of the corresponding theorem in Oxley [Oxl92, Theorem 6.4.7] generalizes directly to partial fields.

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 $xy \in T$. By the lemma there is always an $A' \sim A$ that is T-normalized. We say that A is *normalized* if it is T-normalized for some spanning forest T, the *normalizing* spanning forest.

The following definitions are needed for the statement and proof of Theorem 3.5. As usual, a *walk* in a graph $G = (V, E)$ is a sequence $W = (v_0, \ldots, v_n)$ of vertices such that $v_i v_{i+1} \in E$ for all $i \in \{0, \ldots, n-1$. If $v_n = v_0$ and $v_i \neq v_j$ for all $0 \leq i < j < n$ then we say that W is a *cycle*.

Definition 2.26. *Let A be an $X \times Y$ matrix with entries in a partial field $\mathbb{P}$. The* signature *of A is the function $\sigma_A : (X \times Y) \cup (Y \times X) \to \mathbb{P}$ defined by*

$$\sigma_A(vw) := \begin{cases} A_{vw} & \text{if } v \in X, w \in Y \\ 1/A_{vw} & \text{if } v \in Y, w \in X. \end{cases} \tag{19}$$

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

$$\sigma_A(C) := (-1)^{|V(C)|/2} \prod_{i=0}^{2n-1} \sigma_A(v_i v_{i+1}). \tag{20}$$

Observe that the signature of a cycle does not depend on the choice of v_0. If C' is the cycle $(v_{2n}, v_{2n-1}, \ldots, v_1, v_0)$ then $\sigma_A(C') = 1/\sigma_A(C)$. The proof of the following lemma is straightforward. The last property exhibits a close connection between the signature and determinants.

Lemma 2.27. *Let A be an $X \times Y$ matrix with entries from 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 $C = (v_0, \ldots, v_{2n})$ 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 defined. Then $C' = (v_2, v_3, \ldots, v_{2n})$ is an induced cycle of $G(A')$ and $\sigma_{A'}(C') = \sigma_A(C)$.

(iii) Let $C = (v_0, \ldots, v_{2n})$ be an induced cycle of $G(A)$. If A' is obtained from A by scaling rows and columns such that $A'_{v_i v_{i+1}} = 1$ for all $i > 0$, then $A'_{v_0 v_1} = \sigma_A(C)$ and $\det(A[V(C)]) = 1 - \sigma_A(C)$.

Corollary 2.28. *Let A be an $X \times Y$ $\mathbb{P}$-matrix. If C is an induced cycle of $G(A)$ then $\sigma_A(C) \in \mathrm{Cr}(A) \subseteq \mathscr{F}(\mathbb{P})$.*

2.9 Examples

We can now give a very short proof of Theorem 1.1. First we restate it using our new terminology. We define the *regular* partial field

$$\mathbb{U}_0 := \mathbb{P}(\mathbb{Q}, \emptyset). \tag{21}$$

It has just three elements: $\{-1, 0, 1\}$. Clearly a $\mathbb{U}_0$-matrix is a totally unimodular matrix.

Theorem 2.29 (Tutte [Tut65])**.** *Let M be a matroid. The following are equivalent:*

(i) M is representable over $\mathrm{GF}(2) \otimes \mathrm{GF}(3)$;

(ii) M is $\mathbb{U}_0$-representable.

(iii) M is representable over every partial field.

Proof. Every partial field $\mathbb{P}$ contains a multiplicative identity and, by Axiom (P3), an element -1. Therefore there exists a nontrivial homomorphism $\varphi : \mathbb{U}_0 \to \mathbb{P}$, which proves (*ii*)⇒(*iii*). The partial field GF(2)⊗GF(3) has fundamental elements $\{(0,0),(1,1)\}$. We have an obvious homomorphism $\varphi' : \mathrm{GF}(2) \otimes \mathrm{GF}(3) \to \mathbb{U}_0$, which proves (*i*)⇒(*ii*). (*iii*)⇒(*i*) is trivial. □

We define the *sixth roots of unity* partial field $\mathbb{S} := \mathbb{P}(\mathbb{C}, \zeta)$, where ζ is a root of $x^2 - x + 1 = 0$, i.e. ζ is a primitive sixth root of unity. Whittle proved the following theorem:

Theorem 2.30 (Whittle [Whi97])**.** *Let M be a matroid. The following are equivalent:*

(i) *M is representable over* $\mathrm{GF}(3) \otimes \mathrm{GF}(4)$*;*

(ii) *M is $\mathbb{S}$-representable;*

(iii) *M is representable over* $\mathrm{GF}(3)$*, over* $\mathrm{GF}(p^2)$ *for all primes p, and over* $\mathrm{GF}(p)$ *when* $p \equiv 1 \mod 3$.

Proof. Note that $\mathbb{S}$ is finite, with $\mathscr{F}(\mathbb{S}) = \{0, 1, \zeta, 1-\zeta\}$. Let $\varphi : \mathbb{S} \to \mathrm{GF}(3)\otimes\mathrm{GF}(4)$ be determined by $\varphi(\zeta) = (-1, \omega)$, where $\omega \in \mathrm{GF}(4)\setminus\{0,1\}$ is a generator of $\mathrm{GF}(4)^*$. Then φ is a bijective homomorphism, which proves (*i*)⇔(*ii*).

(*i*)⇒(*iii*) is again trivial. We will use results from algebraic number theory to prove (*ii*)⇒(*iii*). See, for example, Stewart and Tall [ST87] for the necessary background. For (*ii*)⇒(*iii*), remark that $\mathbb{S}^*$ is the group of units of $\mathbb{Z}[\zeta]$, the ring of integers of the algebraic number field $\mathbb{Q}(\zeta) = \mathbb{Q}(\sqrt{-3})$. If I is a maximal ideal then $\mathbb{Z}[\zeta]/I$ is a finite field. We find the values $q = p^m$ for which there exists a prime ideal I with norm $N(I) := |\mathbb{Z}[\zeta]/I| = q$. If I is a principal ideal, i.e. $I = (a + b\sqrt{-3})\mathbb{Z}[\zeta]$ with $a, b \in \frac{1}{2}\mathbb{Z}$, then $N(I) = a^2 + 3b^2$.

Suppose $I = (\sqrt{-3})\mathbb{Z}[\zeta]$. Then $N(I) = 3$ which is prime, so $\mathbb{Z}[\zeta]/I \cong \mathrm{GF}(3)$. This gives a ring homomorphism $\varphi : \mathbb{Z}[\zeta] \to \mathrm{GF}(3)$. Suppose $I = p\mathbb{Z}[\zeta]$. Then $N(p\mathbb{Z}[\zeta]) = p^2$. Either I is prime, in which case $\mathbb{Z}[\zeta]/I \cong \mathrm{GF}(p^2)$, or I splits and there exists a prime ideal J with $\mathbb{Z}[\zeta]/J \cong \mathrm{GF}(p)$. A well-known result in number theory (see e.g. Hardy and Wright [HW54, Theorem 255]) states that I splits if and only if $p \equiv 1 \mod 3$. □

Whittle gave characterizations for several other classes of matroids. However, the proofs of these are more complicated, because the partial fields involved are no longer isomorphic. In the next section we develop a general tool to overcome this difficulty.

3 The lift theorem

Let $\mathbb{P}, \widehat{\mathbb{P}}$ be partial fields and let $\varphi : \widehat{\mathbb{P}} \to \mathbb{P}$ be a homomorphism. Let A be an $X \times Y$ $\mathbb{P}$-matrix. In what follows we would like to construct an $X \times Y$ $\widehat{\mathbb{P}}$-matrix $\widehat{A}$ such that $\varphi(\widehat{A}) = A$. To that end we make the following definitions.

Definition 3.1. *Let $\mathbb{P}, \widehat{\mathbb{P}}$ be partial fields, and let $\varphi : \widehat{\mathbb{P}} \to \mathbb{P}$ be a partial field homomorphism. A* lifting function *for φ is a function $^\uparrow : \mathscr{F}(\mathbb{P}) \to \widehat{\mathbb{P}}$ such that for all $p, q \in \mathscr{F}(\mathbb{P})$:*

- $\varphi(p^\uparrow) = p$;
- *if $p + q \doteq 1$ then $p^\uparrow + q^\uparrow \doteq 1$;*
- *if $p \cdot q = 1$ then $p^\uparrow \cdot q^\uparrow = 1$.*

Hence a lifting function maps $\operatorname{asc}\{p\}$ to $\operatorname{asc}\{p^\uparrow\}$ for all $p \in \mathscr{F}(\mathbb{P})$.

Definition 3.2. *Let $\mathbb{P}, \widehat{\mathbb{P}}$ be two partial fields, let $\varphi : \widehat{\mathbb{P}} \to \mathbb{P}$ be a homomorphism, and let $^\uparrow : \mathscr{F}(\mathbb{P}) \to \widehat{\mathbb{P}}$ be a lifting function for φ. Let A be an $X \times Y$ $\mathbb{P}$-matrix. An $X \times Y$ matrix $\widehat{A}$ is a* local $^\uparrow$-lift *of A if*

(i) $\varphi(\widehat{A}) = A$;

(ii) *$\widehat{A}$ is an $X \times Y$ $\widehat{\mathbb{P}}$-matrix;*

(iii) *for every induced cycle C of $G(A)$ we have*

$$\sigma_A(C)^\uparrow = \sigma_{\widehat{A}}(C). \tag{22}$$

First we show that, if a local $^\uparrow$-lift exists, it is unique up to scaling.

Lemma 3.3. *Let $\mathbb{P}, \widehat{\mathbb{P}}$ be two partial fields, let $\varphi : \widehat{\mathbb{P}} \to \mathbb{P}$ be a homomorphism, and let $^\uparrow : \mathscr{F}(\mathbb{P}) \to \widehat{\mathbb{P}}$ be a lifting function for φ. Let A be an $X \times Y$ $\mathbb{P}$-matrix, and suppose $\widehat{A}_1, \widehat{A}_2$ are local $^\uparrow$-lifts of A. Then $\widehat{A}_1 \sim \widehat{A}_2$.*

Proof. Suppose the lemma is false and let $A, \widehat{A}_1, \widehat{A}_2$ form a counterexample. Let T be a spanning forest of $G(A)$ and rescale $\widehat{A}_1, \widehat{A}_2$ so that they are T-normalized. Let H be the subgraph of $G(A)$ consisting of all edges $x'y'$ such that $(\widehat{A}_1)_{x'y'} = (\widehat{A}_2)_{x'y'}$. 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

$$\sigma_A(C)^\uparrow = \sigma_{\widehat{A}_1}(C) = \sigma_{\widehat{A}_2}(C). \tag{23}$$

But this is only possible if $(\widehat{A}_1)_{xy} = (\widehat{A}_2)_{xy}$, a contradiction. □

It is straightforward to turn this proof into an algorithm that constructs a matrix $\widehat{A}$ satisfying (*i*) and (*iii*) for a subset of the cycles such that, if A has a local $^\uparrow$-lift, $\widehat{A}$ is one. Next we define a stronger notion of lift, which commutes with pivoting.

Definition 3.4. *Let $\mathbb{P}, \widehat{\mathbb{P}}$ be two partial fields, let $\varphi : \widehat{\mathbb{P}} \to \mathbb{P}$ be a homomorphism, and let $^\uparrow : \mathscr{F}(\mathbb{P}) \to \widehat{\mathbb{P}}$ be a lifting function for φ. A matrix $\widehat{A}$ is a* global $^\uparrow$-lift *of $\varphi(\widehat{A})$ if $\widehat{A}'$ 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.

Theorem 3.5 (Lift Theorem)**.** *Let $\mathbb{P}, \widehat{\mathbb{P}}$ be two partial fields, let $\varphi : \widehat{\mathbb{P}} \to \mathbb{P}$ be a homomorphism, and let $^\uparrow : \mathscr{F}(\mathbb{P}) \to \widehat{\mathbb{P}}$ be a lifting function for φ. Let A be an $X \times Y$ $\mathbb{P}$-matrix. Then exactly one of the following is true:*

(i) *A has a global $^\uparrow$-lift.*

(ii) *A has a minor B such that*

(a) B has no global $^{\uparrow}$-lift;
(b) B or B^T equals

$$\begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix} \text{ or } \begin{bmatrix} 1 & 1 & 1 \\ 1 & p & q \end{bmatrix} \tag{24}$$

for some distinct $p, q \in \mathscr{F}(\mathbb{P}) \setminus \{0, 1\}$.

In the proof of this theorem we use techniques similar to those found in, for example, [Ger89, Tru92, LS99]. First we prove a graph-theoretic lemma.

Lemma 3.6. *Let $G = (V, E)$ be a 2-connected bipartite graph with bipartition (U, W). Then either G is a cycle or there exists a spanning tree of G with set of leaves L, such that $|L| \geq 3$ and $L \cap U \neq \emptyset$, $L \cap W \neq \emptyset$.*

Proof. Suppose G is a counterexample. By 2-connectivity G has a cycle C. If $V(C) = V(G)$, then C must have a chord f. Let v be one of the end vertices of f. Then $T := (C \setminus \delta(v)) \cup f$ is a spanning tree as required. Therefore we may assume that $V(G) \setminus V(C) \neq \emptyset$. Let f be an edge such that $f \in \delta(C)$, say $f = uv$ with $v \notin C$. Since C has at least 4 vertices, there is an edge $e \in C$ disjoint from f. $T' := (C \setminus e) \cup f$ is a tree satisfying the conditions of the theorem, but may not yet span all vertices.

Let $T' \subset G$ be a tree with at least three leaves, not all in the same vertex class, and $V(T)$ maximal. Let $v \in V(G) \setminus V(T')$. By Menger's Theorem there exist two internally vertex-disjoint $v - T'$ paths P_1, P_2. Choose an edge $e \in P_1 \cup P_2$ as follows. If one of the end vertices of $P_1 \cup P_2$ is the unique leaf in U or in W, choose e equal to the edge incident with this vertex. Otherwise choose e arbitrarily. Then $(T' \cup P_1 \cup P_2) \setminus e$ is again a tree with the required property. Indeed: adding P_1 and P_2 to T' destroys at most two leaves. However, deleting e creates equally many leaves again, and if there are two such new leaves, then there is one in each of U and W. T' had a third leaf which remains unaffected by this construction. But this contradicts our initial choice of T', and the proof is complete. □

Whittle [Whi95] proves that, if M is 3-connected, elements $e, f, g \in E(M)$ can be chosen such that the cosimplification of $M \setminus S/T$ is again 3-connected for all $S \subseteq \{e, f\}, T \subseteq \{g\}$. He called such elements a *distinguished triple*. The leaves in the lemma correspond to three elements of the matroid $M = M([I|A])$ with properties similar to, yet weaker than, a distinguished triple. Lemma 3.6 suffices for the results in this paper, and its proof is much shorter.

We also need the following lemma. Semple and Whittle [SW96] proved that the 2-sum of two $\mathbb{P}$-matrices is again a $\mathbb{P}$-matrix. We need something slightly stronger.

Lemma 3.7. *Let A be a $\mathbb{P}$-matrix, and X_1, X_2, Y_1, Y_2 partitions of X and Y such that*

$$A = \begin{array}{c} \\ X_1 \\ X_2 \end{array} \begin{array}{c} \begin{array}{cc} Y_1 & Y_2 \end{array} \\ \left[\begin{array}{c|c} A_1' & a_1 a_2 \\ \hline 0 & A_2' \end{array}\right] \end{array}, \tag{25}$$

where A'_1, A'_2 are submatrices, a_1 is a column vector, and a_2 is a row vector. If both

$$A_1 := \begin{bmatrix} A'_1 & a_1 \\ 0 & 1 \end{bmatrix} \text{ and } A_2 := \begin{bmatrix} 1 & a_2 \\ 0 & A'_2 \end{bmatrix} \tag{26}$$

have a global $^\uparrow$-lift then A has a global $^\uparrow$-lift.

The following proof sketch omits some details, but the remaining difficulties are purely notational.

Sketch of proof. Let A, A_1, A_2 be as in the lemma, and let $\widehat{A}_1, \widehat{A}_2$ be global $^\uparrow$-lifts of A_1, A_2. We define

$$\widehat{A} := \begin{matrix} \\ X_1 \\ X_2 \end{matrix} \begin{bmatrix} \overset{Y_1}{\widehat{A}'_1} & \overset{Y_2}{\widehat{a}_1 \widehat{a}_2} \\ 0 & \widehat{A}'_2 \end{bmatrix}. \tag{27}$$

By Lemma 2.6 every subdeterminant of $\widehat{A}$ is of the form $\det(\widehat{D}_1)\det(\widehat{D}_2)$, where $\widehat{D}_1 \preceq \widehat{A}_1$ and $\widehat{D}_2 \preceq \widehat{A}_2$, from which it follows easily that $\widehat{A}$ is a local lift of A. Pick an $x \in X, y \in Y$ with $A_{xy} \neq 0$. Then A^{xy} has a minor equivalent to A_1 (up to relabelling of rows and columns) and a minor equivalent to A_2 (up to relabelling of rows and columns). Moreover A^{xy} can be obtained from these minors in the same way A was obtained from A_1 and A_2. Therefore $\widehat{A}^{xy}$ must be a local lift of A^{xy}. It follows that A has a global lift. □

Proof of Theorem 3.5. (*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.

Claim 3.5.1. *If A is a counterexample to the theorem with $|X|+|Y|$ minimal then $G(A)$ is 2-connected.*

> *Proof.* If $G(A)$ is not connected then one of the components of A has no local $^\uparrow$-lift, contradicting minimality of $|X| + |Y|$. If $G(A)$ has a cut vertex then A is of the form of Lemma 3.7 with one of a_1, a_2 equal to a unit vector. Again minimality of $|X| + |Y|$ gives a contradiction. □

A pair $(A, \{e, f, g\})$, where A is an $X \times Y$ $\mathbb{P}$-matrix and $\{e, f, g\} \subseteq X \cup Y$, is called a *bad pair* if

(*i*) A is a counterexample to the theorem with $|X| + |Y|$ minimal;

(*ii*) There exists a spanning tree T of $G(A)$ such that $\{e, f, g\}$ are leaves of T;

(*iii*) $e, f \in X$ and $g \in Y$.

Claim 3.5.2. *If $(A, \{e, f, g\})$ is a bad pair then there exists a matrix $\widehat{A}$ such that $\widehat{A} - U$ is a global lift of $A - U$ for all U such that $U \cap \{e, f, g\} \neq \emptyset$.*

Proof. Without loss of generality A is T-normalized for a tree T in which e, f, g are leaves. Note that $T - U$ is a spanning tree of $A - U$ for all nonempty $U \subseteq \{e, f, g\}$. By Lemma 3.3 there exists a unique $T - U$-normalized global $^\uparrow$-lift $\widehat{A - U}$ for $A - U$. Hence there is a unique matrix $\widehat{A}$ such that $\widehat{A} - U = \widehat{A - U}$ for all nonempty $U \subseteq \{e, f, g\}$. □

We say that $\widehat{A}$ is a *lift candidate* for $(A, \{e, f, g\})$.

Claim 3.5.3. *If $(A, \{e, f, g\})$ is a bad pair with lift candidate $\widehat{A}$ and $x \in X, y \in Y$ are such that $A_{xy} \neq 0$ and $\{x, y\} \cap \{e, f, g\} = \emptyset$, then $(A^{xy}, \{e, f, g\})$ is a bad pair with lift candidate $\widehat{A}^{xy}$.*

Proof. Obviously A^{xy} must be a minimal counterexample to the theorem. Since $G(A - U)$ is connected for all $U \subseteq \{e, f, g\}$, Lemma 2.24(*ii*) implies that $G(A^{xy} - U)$ is connected for all $U \subseteq \{e, f, g\}$. A spanning tree T' for A^{xy} with leaves $\{e, f, g\}$ is now easily found, so $(A, \{e, f, g\})$ is indeed a bad pair. Pivoting commutes with deleting rows and columns other than x, y. From this and the fact that $\widehat{A} - U$ is a global $^\uparrow$-lift of $A - U$ for all nonempty $U \subseteq \{e, f, g\}$ it follows that $\widehat{A}^{xy}$ is a lift candidate for $(A^{xy}, \{e, f, g\})$. □

We say that $(A, \{e, f, g\})$ is a *local* bad pair if a lift candidate $\widehat{A}$ is not a local lift of A. In that case there exist $X' \subseteq X, Y' \subseteq Y$, $|X'| = |Y'|$, such that either

(*i*) $\det(\widehat{A}[X', Y'])$ is undefined, or

(*ii*) $G(A[X', Y'])$ is a cycle C but $\sigma_{\widehat{A}}(C) \neq \sigma_A(C)^\uparrow$.

We call (X', Y') a *certificate*.

Claim 3.5.4. *If there exists a counterexample A to the theorem with $|X|+|Y|$ minimal such that A has no local lift then there exist $e, f, g \in X \cup Y$ such that one of $(A, \{e, f, g\})$ and $(A^T, \{e, f, g\})$ is a bad pair.*

Proof. Let A be a counterexample to the theorem with $|X|+|Y|$ minimal such that A has no local lift. By Claim 3.5.1 $G(A)$ is 2-connected. From Lemma 2.27(*iii*) it follows that $G(A)$ is not a cycle. By Lemma 3.6 there exists a spanning tree T of $G(A)$ which has leaves e, f, g, with $e, f \in X$ and $g \in Y$ or $e, f \in Y$ and $g \in X$. Clearly if A is a counterexample then so is A^T. The claim follows. □

Claim 3.5.5. *Let $(A, \{e, f, g\})$ be a local bad pair with certificate (X', Y') such that $|X'|$ is minimal. Then $|X'| = 2$ and all entries of $A[X', Y']$ are nonzero.*

Proof. By Claim 3.5.2 we have $X' \cup Y' \supseteq \{e, f, g\}$ so $|X'| \geq 2$. If there is an $x \in X' \setminus \{e, f\}$, $y \in Y' \setminus g$ with $A_{xy} \neq 0$ then it follows from Claim 3.5.3 and one of Lemma 2.6 and Lemma 2.27(*ii*) that $(A^{xy}, \{e, f, g\})$ is a bad pair with lift candidate $\widehat{A}^{xy}$ and certificate $(X' \setminus x, Y' \setminus y)$, which contradicts minimality of $|X'| + |Y'|$.

If there is an $x \in X' \setminus \{e, f\}$ then $A_{xy} = 0$ for all $y \in Y' \setminus \{g\}$. Then $\det(\widehat{A}[X', Y']) = \widehat{A}_{xg} \det(\widehat{A}[X' \setminus x, Y' \setminus g])$. But $\widehat{A} - \{x, g\}$ is a square submatrix of $\widehat{A} - g$ so its determinant is defined, a contradiction.

If some entry of $\widehat{A}[X',Y']$ equals 0 then $\det(\widehat{A}[X',Y'])$ is the product of entries in $\widehat{A}$, a contradiction.The claim follows. □

Suppose $(A,\{e,f,g\})$ is a local bad pair with minimal certificate (X',Y'). Suppose $X'=\{e,f\}, Y'=\{g,h\}$. Since all four entries of $\widehat{A}[X',Y']$ are nonzero, clearly $\sigma_{\widehat{A}}(C)\neq\sigma_A(C)^{\uparrow}$ for $C=(e,g,f,h,e)$.

Claim 3.5.6. *If $(A,\{e,f,g\})$ is a local bad pair with minimal certificate then there exist $p,q,r,s\in\mathbb{P}$ such that A is scaling-equivalent to one of the following matrices:*

$$A_1 := \begin{array}{c} \\ i \\ e \\ f \end{array}\!\!\begin{array}{c} \begin{array}{cc} h & g \end{array} \\ \begin{bmatrix} \textcircled{1} & \textcircled{1} \\ \textcircled{1} & p \\ \textcircled{1} & q \end{bmatrix} \end{array}, \quad A_2 := \begin{array}{c} \\ i \\ k \\ e \\ f \end{array}\!\!\begin{array}{c} \begin{array}{ccc} j & h & g \end{array} \\ \begin{bmatrix} \textcircled{1} & 0 & \textcircled{1} \\ \textcircled{1} & \textcircled{1} & 0 \\ p & \textcircled{1} & r \\ q & \textcircled{1} & s \end{bmatrix} \end{array}. \tag{28}$$

Proof. Let (X',Y') be a minimal certificate, say $X'=\{e,f\}$ and $Y'=\{g,h\}$ for some $g\in Y$. Since $G(A-\{e,f\})$ is connected, there exists a $g-h$ path P in $G(A-\{e,f\})$. Let P be a shortest such path. Then $G(A[V(P)])=P$. Then $T:=P\cup\{he,hf\}$ is a spanning tree for $A':=A[V(P)\cup\{e,f\}]$ with leaves $\{e,f,g\}$. But then $(A',\{e,f,g\})$ is a local bad pair with certificate $(\{e,f\},\{g,h\})$, so by minimality of $|X|+|Y|$ we have $A=A'$.

If $|V(P)|\geq 7$ then P has an edge xy with $x\in X$ such that $A_{xg}=A_{xh}=0$. By Claim 3.5.3 we have that $(A^{xy},\{e,f,g\})$ is a local bad pair with minimal certificate. But A^{xy} has a shorter $g-h$ path, which again contradicts minimality of $|X|+|Y|$. Therefore $|V(P)|=3$ or $|V(P)|=5$, from which the claim follows. □

Claim 3.5.7. *There does not exist a local bad pair.*

Proof. Suppose $(A,\{e,f,g\})$ is a local bad pair with minimal certificate. Since (*ii*) does not hold we have $A\not\sim A_1$. Therefore $A\sim A_2$. Assume, without loss of generality, that $A=A_2$ for some p,q,r,s. Let $\widehat{p},\widehat{q},\widehat{r},\widehat{s}$ be the entries of $\widehat{A}$ corresponding to p,q,r,s.

Claim 3.5.0.1. *p and q are not both zero.*

Proof. $A^{ij}-\{i,j\}$ is scaling-equivalent to a matrix of the form A_1, a contradiction. □

Claim 3.5.0.2. *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 $\widehat{s}=(s/q)^{\uparrow}q^{\uparrow}$. Since $\sigma_{\widehat{A}}(C)\neq\sigma_A(C)^{\uparrow}$ for $C=(e,g,f,h,e)$ it follows that

$$\frac{\widehat{r}}{\widehat{s}}\neq\left(\frac{r}{s}\right)^{\uparrow}. \tag{29}$$

A is minor-minimal, so $A[\{e,f\},\{j,h,g\}]$ has a local $^\uparrow$-lift. This matrix is scaling-equivalent to the following normalized matrices:

$$\begin{array}{c} \\ e \\ f \end{array}\begin{array}{c} \begin{array}{ccc} j & h & g \end{array} \\ \begin{bmatrix} \textcircled{1} & \textcircled{1} & r/s \\ q/p & \textcircled{1} & \textcircled{1} \end{bmatrix} \end{array}, \quad \begin{array}{c} \\ e \\ f \end{array}\begin{array}{c} \begin{array}{ccc} j & h & g \end{array} \\ \begin{bmatrix} \textcircled{1} & \textcircled{1} & \textcircled{1} \\ \textcircled{1} & p/q & \frac{ps}{qr} \end{bmatrix} \end{array}. \tag{30}$$

Since these matrices have a local $^\uparrow$-lift we conclude, using $(1/p)^\uparrow = 1/(p^\uparrow)$, that

$$\left(\frac{p}{q}\right)^\uparrow \left(\frac{s}{r}\right)^\uparrow = \left(\frac{ps}{qr}\right)^\uparrow. \tag{31}$$

Likewise $A[\{i,e,f\},\{j,g\}]$ has a local $^\uparrow$-lift. This gives

$$\left(\frac{p}{r}\right)^\uparrow \left(\frac{s}{q}\right)^\uparrow = \left(\frac{ps}{qr}\right)^\uparrow. \tag{32}$$

Finally, $A_1[\{k,e,f\},\{j,h\}]$ has a local $^\uparrow$-lift. This gives

$$\frac{p^\uparrow}{q^\uparrow} = \left(\frac{p}{q}\right)^\uparrow. \tag{33}$$

But then

$$\left(\frac{r}{s}\right)^\uparrow = \left(\frac{r}{p}\right)^\uparrow p^\uparrow / \left(\left(\frac{s}{q}\right)^\uparrow q^\uparrow\right) = \frac{\widehat{r}}{\widehat{s}}, \tag{34}$$

a contradiction. □

By symmetry we may assume $p = 0$.

Claim 3.5.0.3. $q = 1$.

Proof. Suppose $p = 0, q \neq 0, q \neq 1$. Then A^{kh} is scaling-equivalent to

$$A' := \begin{array}{c} \\ i \\ h \\ e \\ f \end{array}\begin{array}{c} \begin{array}{ccc} j & k & g \end{array} \\ \begin{bmatrix} \textcircled{1} & 0 & \textcircled{1} \\ \textcircled{1} & \textcircled{1} & 0 \\ p' & \textcircled{1} & r' \\ q' & \textcircled{1} & s' \end{bmatrix} \end{array} \tag{35}$$

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 $(A, \{e,f,g\})$. By Claim 3.5.3 $\widehat{A'} \sim \widehat{A}^{kh}$. But $\widehat{A'}[\{e,f\},\{h,g\}] \sim \widehat{A}[\{e,f\},\{h,g\}]$, so again $\sigma_{\widehat{A}}(C) \neq \sigma_A(C)^\uparrow$ for $C = (e,g,f,h,e)$. But this is impossible by Claim 3.5.0.2. □

Now $p = 0, q = 1$. Then $\widehat{s} = s^\uparrow$ and $\widehat{r} = -(-r)^\uparrow$. Scale row e of A by $1/r$ and then column h by r. After permuting some rows and columns we obtain

$$A' := \begin{array}{c} \\ e \\ i \\ k \\ f \end{array}\begin{array}{c} \begin{array}{ccc} g & j & h \end{array} \\ \begin{bmatrix} \textcircled{1} & 0 & \textcircled{1} \\ \textcircled{1} & \textcircled{1} & 0 \\ 0 & \textcircled{1} & r \\ s & \textcircled{1} & r \end{bmatrix} \end{array}. \tag{36}$$

A spanning tree T' has been circled. Let $\widehat{A'}$ be the T'-normalized lift candidate for $(A', \{k, f, h\})$. Then $\widehat{A'}_{kh} = -(-r)^{\uparrow}$ and $\widehat{A'}_{fh} = (r/s)^{\uparrow} s^{\uparrow}$. But then $\sigma_{\widehat{A}}(C) \neq \sigma_A(C)^{\uparrow}$ for $C' = (k, j, f, h, k)$. By Claim 3.5.0.3 we have $s = 1$. We can now repeat the argument and conclude that also $r = 1$. Hence (*ii*) holds, contradicting our choice of A. This ends the proof of Claim 3.5.7. □

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

(*i*) A is a counterexample to the theorem with $|X| + |Y|$ minimal;

(*ii*) A has a local lift $\widehat{A}$, but $\widehat{A}^{xy}$ is not a local lift of A^{xy}.

Claim 3.5.8. *There exists a bad-pivot pair.*

Proof. Let A be a counterexample to the theorem with $|X| + |Y|$ minimal. By Claim 3.5.7 A has a local lift $\widehat{A}$. Suppose $\widehat{A}$ is not a global $^{\uparrow}$-lift for A. Then there exist sequences $A_0, \ldots, A_k$ and $\widehat{A}_0, \ldots, \widehat{A}_k$ such that $A_0 = A$, $\widehat{A}_0 = \widehat{A}$, and for $i = 1, \ldots, k$, $A_i = (A_{i-1})^{x_i y_i}$ 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. Choose A and these sequences such that k is as small as possible. But then $k = 1$, so there is an edge $xy \in G(A)$ such that $A_{xy} \neq 0$ and $\widehat{A}^{xy}$ is not a local $^{\uparrow}$-lift of A^{xy}. □

By Claim 3.5.3 we have

Claim 3.5.9. *If $(A, \{e, f, g\})$ is a bad pair and (A, xy) is a bad-pivot pair, then $\{x, y\} \cap \{e, f, g\} \neq \emptyset$.*

Let T' be a tree such that $x, y \in T'$ and T' has three leaves $\{e', f', g'\}$, not all rows and not all columns, such that $\{x, y\} \cap \{e', f', g'\} = \emptyset$. From the proof of Lemma 3.6 we conclude that we can extend T' to a spanning tree of $G(A)$ with three leaves $\{e, f, g\}$, not all rows and not all columns, such that $\{x, y\} \cap \{e, f, g\} = \emptyset$. We call T' "good for xy". It follows that there is no good tree for xy in $G(A)$.

Claim 3.5.10. *There exists a bad-pivot pair (A, xy) such that, for some $p, q \in \mathbb{P}$, we have*

$$A = \begin{array}{c} \\ x \\ e \\ f \end{array} \begin{array}{c} \begin{array}{ccc} y & g & h \end{array} \\ \begin{bmatrix} \textcircled{1} & \textcircled{1} & 0 \\ \textcircled{1} & p & \textcircled{1} \\ 0 & \textcircled{1} & q \end{bmatrix} \end{array}. \tag{37}$$

Proof. Let (A, xy) be a bad-pivot pair. By Claim 3.5.1 $G(A)$ is 2-connected, so there exists a cycle C containing xy. By Lemma 2.27(*ii*),(*iii*) $G(A)$ is not a cycle. Then there exists an edge $x'y'$ not in C. Find two vertex-disjoint $x'y' - C$ paths P_1, P_2, and set $P := P_1 \cup P_2 \cup \{x'y'\}$. If some vertex $v \in P \cap C$ is not in $\delta(\{x, y\})$ then we delete the two edges of C adjacent to v and obtain a good tree for xy, a contradiction. If $P \cap C = xy$ then we delete an edge of C not adjacent to xy and an edge of P not adjacent to xy to obtain a good tree for xy, a contradiction. Since $G(A)$ is simple and bipartite, both C and $P \cup \{xy\}$ have girth at least 4, so such edges exist. Therefore we may assume that all such paths P have the neighbours of xy as end vertices. If P has length at least 3 and C has length at least 6

then again a good tree for xy can be found. Therefore, without loss of generality, P has length 1.

Assume a bad-pivot pair (A, xy) was chosen such that the length of P is 1 and the length of C is as small as possible. Suppose C has length more than 6. Let $x'y'$ be the edge of C at maximum distance from xy. We can find a good tree for $x'y'$, so $\widehat{A'} := \widehat{A}^{x'y'}$ is a local $^\uparrow$-lift of $A' := A^{x'y'}$. But in $G(A')$ there is a good tree for xy, so $(\widehat{A'})^{xy}$ is a local lift for $(A')^{xy}$. But $((\widehat{A'})^{xy})^{y'x'} = \widehat{A}^{xy}$, so there is no good tree for $y'x'$ in $(A')^{xy}$. This is only the case if A^{xy} is a cycle. But it is easily checked that in this case $\widehat{A^{xy}} = \widehat{A}^{xy}$, a contradiction. The claim follows. □

Suppose (A, xy) is a bad-pivot pair with A as in (37) for some $p, q \in \mathbb{P}$. The normalized local $^\uparrow$-lift $\widehat{A}$ of A has $\widehat{A}_{eg} = p^\uparrow$ and $\widehat{A}_{fh} = (pq)^\uparrow/p^\uparrow$. After a pivot over xy and renormalization we have

$$A' = \begin{array}{c} \\ y \\ e \\ f \end{array} \begin{array}{c} \begin{array}{ccc} x & g & h \end{array} \\ \begin{bmatrix} \textcircled{1} & \textcircled{1} & 0 \\ \textcircled{1} & 1-p & \textcircled{1} \\ 0 & \textcircled{1} & -q \end{bmatrix} \end{array}. \tag{38}$$

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

$$-(pq)^\uparrow/p^\uparrow \neq (q(p-1))^\uparrow/(1-p)^\uparrow. \tag{39}$$

Consider

$$A^{xg} = \begin{array}{c} \\ g \\ e \\ f \end{array} \begin{array}{c} \begin{array}{ccc} y & x & h \end{array} \\ \begin{bmatrix} 1 & -1 & 0 \\ 1-p & p & 1 \\ -1 & 1 & q \end{bmatrix} \end{array}. \tag{40}$$

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

$$\left(\frac{p-1}{p}\right)^\uparrow (pq)^\uparrow = ((1-p)q)^\uparrow \tag{41}$$

which contradicts (39). Therefore A does have a global $^\uparrow$-lift. It follows that no counterexample exists, which completes the proof of the theorem. □

We remark here that for most of our applications, including all examples in the next section, $\varphi|_{\mathscr{F}(\widehat{\mathbb{P}})}$ is a bijection between $\mathscr{F}(\widehat{\mathbb{P}})$ and $\mathscr{F}(\mathbb{P})$. Then $(\varphi|_{\mathscr{F}(\widehat{\mathbb{P}})})^{-1}$ is an obvious choice for the lifting function. We did not specify this lifting function in the theorem statement because we need the more general version for the proof of Lemma 5.8.

We have the following corollary:

Corollary 3.8. *Let $\mathbb{P}, \widehat{\mathbb{P}}, \varphi, {}^{\uparrow}$ be as in Theorem 3.5. Suppose that*

(i) If $1+1 \doteq 0$ in $\mathbb{P}$ then $1+1 \doteq 0$ in $\widehat{\mathbb{P}}$;

(ii) If $1+1 \doteq 2$ in $\mathbb{P}$ then $1+1 \doteq 2$ in $\widehat{\mathbb{P}}$;

(iii) For all $p, q, r \in \mathscr{F}(\mathbb{P})$ 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. Consider the following $\mathbb{P}$-matrix:

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & p' & q' \end{bmatrix}. \tag{42}$$

This matrix has a local ${}^{\uparrow}$-lift if and only if

$$\left(\frac{p'}{q'}\right)^{\uparrow} = \frac{(p')^{\uparrow}}{(q')^{\uparrow}}. \tag{43}$$

Pick $p := p'$, $q := (q')^{-1}$, and $r := q'/p'$. Then (43) holds if and only if $p^{\uparrow}q^{\uparrow}r^{\uparrow} = 1$, which proves (*iii*). (*i*) and (*ii*) arise from the first matrix in (24) by similar considerations. □

4 Applications

4.1 Ternary matroids

Our first applications of the Lift Theorem consist of new proofs of three results of Whittle [Whi97].

First we prove Theorem 1.2 from the introduction. A matroid is called *dyadic* if it is representable over the partial field $\mathbb{D} := \mathbb{P}(\mathbb{Q}, 2)$.

Lemma 4.1. $\mathscr{F}(\mathbb{D}) = \operatorname{asc}\{1, 2\} = \{0, 1, -1, 2, 1/2\}$.

Proof. We find all solutions of

$$1 - p = q \tag{44}$$

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

$$2^{x'} + (-1)^{s'} 2^{y'} + (-1)^{t'} = 0 \tag{45}$$

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

$$2^{x''} + (-1)^{s''} + (-1)^{t''} = 0. \tag{46}$$

There are finitely many solutions. Enumeration of these completes the proof. □

Theorem 4.2 (Whittle [Whi97]). *Let M be a matroid. The following are equivalent:*

(i) *M is representable over $\mathrm{GF}(3) \otimes \mathrm{GF}(5)$;*

(ii) *M is $\mathbb{D}$-representable;*

(iii) *M is representable over every field that does not have characteristic 2.*

Proof. Let $\varphi_3 : \mathbb{D} \to \mathrm{GF}(3)$ be determined by $\varphi(2) = -1$. Let $\varphi_5 : \mathbb{D} \to \mathrm{GF}(5)$ be determined by $\varphi(2) = 2$. Clearly both are partial field homomorphisms. But then $\varphi = \varphi_3 \otimes \varphi_5$ is a partial field homomorphism $\mathbb{D} \to \mathrm{GF}(3) \otimes \mathrm{GF}(5)$. $\varphi|_{\mathscr{F}(\mathbb{D})} : \mathscr{F}(\mathbb{D}) \to \mathscr{F}(\mathrm{GF}(3) \otimes \mathrm{GF}(5))$ is readily seen to be a bijection. Taking $(\varphi|_{\mathscr{F}(\mathbb{D})})^{-1}$ as lifting function we apply Corollary 3.8, thereby proving (*i*)⇔(*ii*). For (*ii*)⇒(*iii*), use again a suitable homomorphism. The implication (*iii*)⇒(*i*) is trivial. □

A matroid is called *near-regular* if it is representable over the partial field $\mathbb{U}_1 := \mathbb{P}(\mathbb{Q}(\alpha), \alpha)$.

Lemma 4.3. $\mathscr{F}(\mathbb{U}_1) = \mathrm{asc}\{1, \alpha\}$.

Proof. We find all $p = (-1)^s \alpha^x (1-\alpha)^y$ such that $1 - p \doteq q$ in $\mathbb{U}_1$. Consider the homomorphism $\varphi : \mathbb{U}_1 \to \mathbb{D}$ determined by $\varphi(\alpha) = 2$. Since fundamental elements must map to fundamental elements, it follows that $x \in \{-1, 0, 1\}$. Likewise, $\psi : \mathbb{U}_1 \to \mathbb{D}$, determined by $\psi(\alpha) = -1$, shows that $y \in \{-1, 0, 1\}$. Again, a finite check remains. □

Theorem 4.4 (Whittle [Whi97]). *Let M be a matroid. The following are equivalent:*

(i) *M is representable over $\mathrm{GF}(3) \otimes \mathrm{GF}(4) \otimes \mathrm{GF}(5)$;*

(ii) *M is representable over $\mathrm{GF}(3) \otimes \mathrm{GF}(8)$;*

(iii) *M is $\mathbb{U}_1$-representable;*

(iv) *M is representable over every partial field with at least 3 elements.*

Proof. Let $\varphi : \mathbb{U}_1 \to \mathrm{GF}(3) \otimes \mathrm{GF}(4) \otimes \mathrm{GF}(5)$ be determined by $\varphi(\alpha) = (-1, \omega, 2)$. Again $\varphi|_{\mathscr{F}(\mathbb{U}_1)} : \mathscr{F}(\mathbb{U}_1) \to \mathscr{F}(\mathrm{GF}(3) \otimes \mathrm{GF}(4) \otimes \mathrm{GF}(5))$ is a bijection, so we use $(\varphi|_{\mathscr{F}(\mathbb{U}_1)})^{-1}$ as lifting function and apply Corollary 3.8 to prove (*i*)⇔(*iii*). For (*iii*)⇒(*iv*), use a homomorphism φ' such that $\varphi'(\alpha) = p$ for any $p \in \mathbb{P} \setminus \{0, 1\}$. Similar constructions prove the remaining implications. □

Let $\mathbb{Y} := \mathbb{P}(\mathbb{C}, \{2, \zeta\})$, where ζ is a primitive complex sixth root of unity.

Lemma 4.5. $\mathscr{F}(\mathbb{Y}) = \mathrm{asc}\{1, 2, \zeta\} = \{0, 1, -1, 2, 1/2, \zeta, 1-\zeta\}$.

Proof. Clearly all these elements are fundamental elements. The complex argument of every element of $\mathbb{Y}$ is equal to a multiple of $\pi/3$, from which it follows easily that no other fundamental elements exist. □

Theorem 4.6 (Whittle [Whi97]). *Let M be a matroid. The following are equivalent:*

(i) *M is representable over* $\mathrm{GF}(3) \otimes \mathrm{GF}(7)$*;*

(ii) *M is $\mathbb{Y}$-representable;*

(iii) *M is representable over* $\mathrm{GF}(3)$*, over* $\mathrm{GF}(p^2)$ *for all primes* $p > 2$*, and over* $\mathrm{GF}(p)$ *when* $p \equiv 1 \mod 3$.

Proof. Let $\varphi : \mathbb{Y} \to \mathrm{GF}(3) \otimes \mathrm{GF}(7)$ be determined by $\varphi(2) = (-1, 2)$ and $\varphi(\zeta) = (-1, 3)$. Again $\varphi|_{\mathscr{F}(\mathbb{Y})} : \mathscr{F}(\mathbb{Y}) \to \mathscr{F}(\mathrm{GF}(3) \otimes \mathrm{GF}(7))$ is a bijection, so we use $(\varphi|_{\mathscr{F}(\mathbb{Y})})^{-1}$ as lifting function and apply Corollary 3.8 to prove (*i*)⇔(*ii*). For (*ii*)⇒(*iii*) we use an argument similar to the proof of Theorem 2.30. Note that the ring $\mathbb{Z}[\frac{1}{2}, \zeta]$ is not the ring of integers of an algebraic number field, but every element is of the form $2^k x$ for some $k \in \mathbb{Z}$, $x \in \mathbb{Z}[\zeta]$. Hence, in contrast to the partial field $\mathbb{S}$, there are no homomorphisms to finite fields of characteristic 2. (*i*) is a special case of (*iii*). □

4.2 Quaternary and quinary matroids

Our next example is a proof of Theorem 1.3. A matroid is called *golden ratio* (in [Whi05] "golden mean" is used) if it is representable over the partial field $\mathbb{G} := \mathbb{P}(\mathbb{R}, \tau)$, where τ is the golden ratio, i.e. the positive root of $x^2 - x - 1 = 0$.

Lemma 4.7. $\mathscr{F}(\mathbb{G}) = \mathrm{asc}\{1, \tau\} = \{0, 1, \tau, -\tau, 1/\tau, -1/\tau, \tau^2, 1/\tau^2\}$.

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 $f_{i+2} - f_{i+1} - f_i = 0$, 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. We leave out the remaining details. □

Theorem 4.8 (Vertigan)**.** *Let M be a matroid. The following are equivalent:*

(i) *M is representable over* $\mathrm{GF}(4) \otimes \mathrm{GF}(5)$*;*

(ii) *M is $\mathbb{G}$-representable;*

(iii) *M is representable over* $\mathrm{GF}(5)$*, over* $\mathrm{GF}(p^2)$ *for all primes p, and over* $\mathrm{GF}(p)$ *when* $p \equiv \pm 1 \mod 5$.

Proof. Let $\varphi : \mathbb{G} \to \mathrm{GF}(4) \otimes \mathrm{GF}(5)$ be determined by $\varphi(\tau) = (\omega, 3)$. Again $\varphi|_{\mathscr{F}(\mathbb{G})} : \mathscr{F}(\mathbb{G}) \to \mathscr{F}(\mathrm{GF}(4) \otimes \mathrm{GF}(5))$ is a bijection, so we use $(\varphi|_{\mathscr{F}(\mathbb{G})})^{-1}$ as lifting function and apply Corollary 3.8 to prove (*i*)⇔(*ii*).

For (*ii*)⇒(*iii*) we use an argument similar to the proof of Theorem 2.30. (*i*) is a special case of (*iii*). □

A matroid is called *Gaussian* if it is representable over the partial field $\mathbb{H}_2 := \mathbb{P}(\mathbb{C}, \{i, 1 - i\})$, where i is a root of $x^2 + 1 = 0$.

Lemma 4.9.

$$\mathscr{F}(\mathbb{H}_2) = \mathrm{asc}\{1, 2, i\} = \left\{0, 1, -1, 2, \tfrac{1}{2}, i, i+1, \tfrac{i+1}{2}, 1-i, \tfrac{1-i}{2}, -i\right\}. \quad (47)$$

Proof. First note that 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, then $\frac{1}{\sqrt{2}} \leq p \leq \sqrt{2}$. Therefore there are finitely many fundamental elements in $\mathbb{C} \setminus \mathbb{R}$. It is easily checked that all numbers on the real line are powers of 2. The result follows. □

Our next result requires more advanced techniques. The following lemma is a corollary of Whittle's Stabilizer Theorem [Whi99].

Theorem 4.10 (Whittle [Whi99])**.** *Let M be a 3-connected quinary matroid with a minor N isomorphic to one of $U_{2,5}$ and $U_{3,5}$. Then the representation of M over* GF(5) *is determined up to strong equivalence by the representation of N.*

Lemma 4.11. *Let M be a 3-connected matroid.*

(i) If M has at least 2 inequivalent representations over 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 GF(5)*.*

Proof. Let $\varphi : \mathbb{H}_2 \to \mathrm{GF}(5) \otimes \mathrm{GF}(5)$ be determined by $\varphi(i) = (2,3)$. Then $\varphi(2) = \varphi(i(1-i)^2) = (2,2)$. Let $\varphi_i : \mathrm{GF}(5) \otimes \mathrm{GF}(5) \to \mathrm{GF}(5)$ be determined by $\varphi_i(x) = x_i$ for $i = 1, 2$. Let

$$A := \begin{bmatrix} 1 & 1 & 1 \\ 1 & p' & q' \end{bmatrix} \tag{48}$$

for some, $p', q' \in \mathbb{H}_2$. If A is a $\mathbb{H}_2$-matrix then $p', q' \in \mathscr{F}(\mathbb{H}_2)$. 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 GF(5). Then there exists a GF(5) ⊗ GF(5)-matrix A such that $M = M([I|A])$ and $\varphi_1(A) \not\sim \varphi_2(A)$.

$\varphi|_{\mathscr{F}(\mathbb{H}_2)} : \mathscr{F}(\mathbb{H}_2) \to \mathscr{F}(\mathrm{GF}(5) \otimes \mathrm{GF}(5))$ is a bijection. If we apply Theorem 3.5 with lifting function $(\varphi|_{\mathscr{F}(\mathbb{H}_2)})^{-1}$ then Case 3.5(*ii*) holds only for GF(5) ⊗ GF(5)-matrices A having a minor

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & p & q \end{bmatrix} \text{ or } \begin{bmatrix} 1 & 1 \\ 1 & p \\ 1 & q \end{bmatrix}, \tag{49}$$

where $p, q \in \{(2,2), (3,3), (4,4)\}$. But Theorem 4.10 implies that if A has such a minor, then $\varphi_1(A) \sim \varphi_2(A)$, a contradiction. (*i*) follows. □

Theorem 4.12. *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 GF(5)*;*

(ii) M is $\mathbb{H}_2$-representable;

(iii) M has two inequivalent representations over GF(5)*, is representable over* GF(p^2) *for all primes $p \geq 3$, and over* GF(p) *when $p \equiv 1 \mod 4$.*

Proof. (*i*)⇔(*ii*) follows from the previous lemma. For (*ii*)⇒(*iii*) we use an argument similar to the proof of Theorem 2.30 where, like in the proof of Theorem 4.6, every element of $\mathbb{H}_2$ is of the form $2^k x$ for some $k \in \mathbb{Z}$, $x \in \mathbb{Z}[i]$. (*i*) is a special case of (*iii*). □

A matroid is called *k-cyclotomic* if it is representable over the partial field

$$\mathbb{K}_k := \mathbb{P}(\mathbb{Q}(\alpha), \{\alpha, \alpha - 1, \alpha^2 - 1, \ldots, \alpha^k - 1\}). \tag{50}$$

Lemma 4.13. *If M is $\mathbb{K}_k$-representable, then it is representable over every field that has an element x whose multiplicative order is at least $k+1$. In particular, M is representable over* GF(q) *for $q \geq k+2$.*

Let $\Phi_0(\alpha) := \alpha$ and let Φ_j be the jth *cyclotomic polynomial*, i.e. the polynomial whose roots are exactly the primitive jth roots of unity. A straightforward observation is the following:

Lemma 4.14. $\mathbb{K}_k = \mathbb{P}(\mathbb{Q}(\alpha), \{\Phi_j(\alpha) \mid j = 0, \ldots, k\})$.

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

Lemma 4.15. $\mathscr{F}(\mathbb{K}_2) = \text{asc}\{1, \alpha, -\alpha, \alpha^2\}$.

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

We conclude this section with the following result:

Theorem 4.16. *Let M be a matroid. The following are equivalent:*

- *M is representable over* GF$(4) \otimes \mathbb{H}_2$*;*
- *M is representable over $\mathbb{K}_2$.*

The proof consists, once more, of an application of Corollary 3.8.

5 An algebraic construction

With a theorem as general as the Lift Theorem, an interesting question becomes whether we can construct suitable partial fields $\widehat{\mathbb{P}}$ to which a given class of matroids lifts. In this section, we find the "most general" or "algebraically most free" partial field to which all $\mathbb{P}$-representable matroids lift, a notion that we will make precise soon. Our starting point is Theorem 2.16, which we prove now. For convenience we repeat the theorem here.

Theorem 5.1 (Vertigan)**.** *If $\mathbb{P}$ is a partial field, then there exists a ring $\mathbb{O}$ and a set $S \subseteq \mathbb{O}^*$ such that $\mathbb{P} \cong \mathbb{P}(\mathbb{O}, S)$.*

Proof. Given a partial field $\mathbb{P}$, we define the following group ring on the multiplicative group $\mathbf{G} := \mathbb{P}^*$:

$$\mathbb{Z}[\mathbf{G}] := \{\sum_{p\in\mathbf{G}} a_p \cdot p \mid a_p \in \mathbb{Z}, \text{finitely many } a_p \text{ are nonzero}\}, \tag{51}$$

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

$$(\sum_{p\in\mathbf{G}} a_p \cdot p)(\sum_{p\in\mathbf{G}} b_p \cdot p) = \sum_{p,q\in\mathbf{G}} a_p b_q \cdot pq. \tag{52}$$

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

$$I_F := \{p + q + (-r) \mid p, q, r \in \mathbb{P}, p \oplus q \doteq r\}. \tag{53}$$

Let I be the ideal generated by I_F. We define the ring $\mathbb{O} := \mathbb{Z}[\mathbf{G}]/I$. Note that $r + (-r) \in I_F$, so we identify $(-r)$ with $(-1) \cdot r$ in $\mathbb{O}$.

Claim 5.1.1. *If $q \in I$ then $q = \pm s_1 \pm \cdots \pm s_n$, where $s_1, \ldots, s_n \in I_F$.*

Proof. By definition $q = r_1 s_1 + \cdots + r_k s_k$ for some $r_1, \ldots, r_k \in \mathbb{O}, s_1, \ldots, s_k \in I_F$. We consider one term.

$$r_i s_i = (\sum_{p\in\mathbf{G}} a_p p)(t + u - v) = \sum_{p\in\mathbf{G}} (a_p p(t + u - v)). \tag{54}$$

Since $p(t \oplus u \oplus (-v)) = pt \oplus pu \oplus -pv \doteq 0$, we have $p(t + u - v) \in I_F$ for all $p \in \mathbf{G}$. Combining this with the identification of $z \in \mathbb{Z}$ with $1_{\mathbb{P}} + \cdots + 1_{\mathbb{P}}$ we see that $r_i s_i$ is of the desired form. Summing over i yields the claim. □

Claim 5.1.2. *Suppose $s_1, \ldots, s_n \in I_F$. Then $s_1' \oplus \cdots \oplus s_n' \doteq 0$, where $s_i' := t \oplus u \oplus (-v)$ for $s_i = t + u - v$.*

Proof. $t \oplus u \doteq v$ by definition of I_F, so $((t \oplus u) \oplus -v) \doteq 0$, with an association as indicated by the parentheses. Using $0 \oplus 0 \doteq 0$ we find an association of the desired sum. □

Claim 5.1.3. $1 \notin I$.

Proof. Suppose that $1 \in I$. Then $1 = s_1 + \cdots + s_n$ for some $s_1, \ldots, s_n \in I_F$. We create two different associations of $s_1' \oplus \cdots \oplus s_n'$. First note that $s_1' \oplus \cdots \oplus s_n' \doteq 0$ by Claim 5.1.2. Furthermore note that $s_i \in \{-1, 0, 1\}^{\mathbf{G}}$ with a nonzero in at most 3 positions. n is finite, so we can interpret $s_1 + \cdots + s_n$ as a finite sum over a finite-dimensional vector space, where each element occurs with coefficient $+1$ or -1. Clearly if $p \neq 1$ then for every term p in the sum there must be a term $-p$. Only the number of times a 1 occurs should exceed the number of times a -1 occurs by one. By repeatedly grouping terms $p, -p$, we find a pre-association of $s_1' \oplus \cdots \oplus s_n'$ with 1 and 0 as children of the root, a contradiction. □

Claim 5.1.4. *If $p \in \mathbf{G}$, then $p + I$ is a unit of $\mathbb{O}$.*

Proof. Let p^{-1} be the inverse of p in $\mathbf{G}$, then $(p+I)(p^{-1}+I) = 1+I$. □

It follows that we can view $\mathbf{G}$ as a subgroup of the group of units of $\mathbb{O}$. Let $\mathbb{P}' := \mathbb{P}(\mathbb{O}, \mathbf{G})$. Consider the following map:

$$\varphi : \mathbb{P} \to \mathbb{P}' : p \mapsto p + I. \tag{55}$$

Claim 5.1.5. *φ is a nontrivial homomorphism.*

Proof. Clearly $\varphi(pq) = \varphi(p)\varphi(q)$. For addition, note that if $p \oplus q \doteq r$, then $p+q-r \in I_F$, so $(p+I)+(q+I) = p+q+I = r+I$, and therefore $\varphi(p) + \varphi(q) \doteq \varphi(p \oplus q)$. φ is not trivial since $1 \notin I$. □

Claim 5.1.6. *φ is a bijection.*

Proof. Suppose this is not the case, so there are $p, q \in \mathbb{P}$, $p \neq q$, but $p + I = q + I$. Then $p - q \in I$, so $p - q = s_1 + \cdots + s_n$ for some $s_1, \ldots, s_n \in I_F$. By Claim 5.1.2, $s_1' \oplus \cdots \oplus s_n' \doteq 0$. As before, note that for every term $t \neq p, -q$ in $s_1' \oplus \cdots \oplus s_n'$ there must be a corresponding term $-t$, and elements $p, -q$ occur with a surplus of one (after terms $-p, q$ are discounted). It follows that there exists a pre-association of $s_1' \oplus \cdots \oplus s_n'$ such that the children of r are labelled $p, -q$, from which it follows, by the associative law, that $p \oplus -q \doteq 0$, i.e. $p = q$, a contradiction. □

Claim 5.1.7. *If $p + I + q + I \doteq r + I$ in $\mathbb{P}'$, then $p \oplus q \doteq r$.*

Proof. Since $p+q-r \in I$, there are $s_1, \ldots, s_n \in I_F$ such that $p+q-r = s_1 + \cdots + s_n$. Using the same argument as in the previous claim we construct two associations for $s_1' \oplus \cdots \oplus s_n' \oplus r$: the obvious one with as children of the root $r, 0$, and the one where the children of the root are p, q. □

It follows that φ is a partial field isomorphism, by which the proof is complete. □

Note that we have not guaranteed that $\mathbb{P}' = \mathbb{P}(\mathbb{O}, \mathbb{O}^*)$. It could be that there are other units besides the elements of $\mathbf{G}$.

Corollary 5.2. *If M is representable over a partial field $\mathbb{P}$ then M is representable over a field.*

Proof. Let $\mathbb{P} = \mathbb{P}(\mathbb{O}, S)$, and let A be a $\mathbb{P}$-matrix such that $M = M([I|A])$. If every $x \in \mathbb{O} \setminus 0$ is invertible then $\mathbb{O}$ is a field. If some $x \in \mathbb{O} \setminus 0$ is not invertible then $x\mathbb{O}$ is a proper ideal of $\mathbb{O}$. A standard result from commutative ring theory implies the existence of a maximal ideal $I \supseteq x\mathbb{O}$, and then $\mathbb{O}/I$ is a field (see, for example, Page 2 of Matsumura [Mat86]). There is a nontrivial ring homomorphism $\varphi : \mathbb{O} \to \mathbb{O}/I$, and therefore $M = M([I|\varphi(A)])$. □

Clearly every ring homomorphism yields a partial field homomorphism. On the other hand, not all partial field homomorphisms extend to ring homomorphisms. The following example shows this. Let $\mathbb{O} :=$

GF(2) × GF(7), and let $\mathbb{P} := \mathrm{GF}(2) \otimes \mathrm{GF}(7)$. Let $\varphi : \mathbb{P} \to \mathbb{U}_0$ be determined by $\varphi(1,1) = \varphi(1,2) = \varphi(1,4) = 1$ and $\varphi(1,6) = \varphi(1,5) = \varphi(1,3) = -1$. This is a partial field homomorphism. However, in $\mathbb{O}$ we have $(1,2) + (1,4) = (1,3) + (1,3) = (0,6)$. It follows that φ can not be extended to a homomorphism $\varphi' : \mathbb{O} \to \mathbb{Q}$. The following theorem overcomes this problem.

Theorem 5.3. *Let $\mathbb{P}_1, \mathbb{P}_2$ be partial fields such that $\mathbb{P}_1 = \mathbb{P}_1[\mathscr{F}(\mathbb{P}_1)]$ and $\mathbb{P}_2 = \mathbb{P}_2[\mathscr{F}(\mathbb{P}_2)]$. If there exists a partial field homomorphism $\varphi : \mathbb{P}_1 \to \mathbb{P}_2$ then φ can be extended to a ring homomorphism $\varphi' : \mathbb{O}_1 \to \mathbb{O}_2$ for some rings $\mathbb{O}_1, \mathbb{O}_2$ such that $\mathbb{P}_i = \mathbb{P}(\mathbb{O}_i, S_i)$ for some sets S_i.*

Proof. Let $\mathbb{O}_1, \mathbb{O}_2$ be the rings constructed in the proof of Theorem 5.1. Every element of $\mathbb{P}_i$ can be expressed as a product of fundamental elements and -1. From this it follows that there exists a ring homomorphism $\varphi'' : \mathbb{Z}[\mathbb{P}_1^*] \to \mathbb{O}_2$. But $I_{F_1} \subseteq \ker(\varphi'')$. It follows that there exists a well-defined homomorphism $\varphi' : \mathbb{O}_1 \to \mathbb{O}_2$. □

The restriction on $\mathbb{P}_1, \mathbb{P}_2$ in this theorem is rather light, as the following propositions show. We prove the first in [PZ]. The main idea is to look at induced cycles in the bipartite graph of a normalized representation.

Proposition 5.4. *If a matroid M is representable over a partial field $\mathbb{P}$, then M is representable over $\mathbb{P}[\mathscr{F}(\mathbb{P})]$.*

Proposition 5.5. *Let $\mathbb{P}_1, \mathbb{P}_2$ be partial fields and $\varphi : \mathbb{P}_1 \to \mathbb{P}_2$ a partial field homomorphism. Then there exists a partial field homomorphism $\varphi' : \mathbb{P}_1[\mathscr{F}(\mathbb{P}_1)] \to \mathbb{P}_2[\mathscr{F}(\mathbb{P}_2)]$.*

Proof. Let $\mathbb{P}_1' := \mathbb{P}_1[\mathscr{F}(\mathbb{P}_1)]$ and let $\mathbb{P}_2' := \mathbb{P}_2[\mathscr{F}(\mathbb{P}_2)]$. Then $\varphi' := \varphi|_{\mathbb{P}_1'} : \mathbb{P}_1' \to \mathbb{P}_2$ is a partial field homomorphism. Clearly $\varphi(-1) = -1$. Let $p = p_1 \cdots p_k \in \mathbb{P}_1'$, where $p_1, \ldots, p_k \in \mathscr{F}(\mathbb{P}_1')$. Then $\varphi(p) = \varphi(p_1) \cdots \varphi(p_k) \in \mathbb{P}_2'$. Hence the image of φ' is contained in $\mathbb{P}_2'$, which completes the proof. □

The above paves the way for a construction of partial fields $\widehat{\mathbb{P}}$ satisfying the conditions of Corollary 3.8.

Definition 5.6. *Let $\mathbb{P}$ be a partial field. We define the* lift *of $\mathbb{P}$ as*

$$\mathbb{L}\mathbb{P} := \mathbb{P}(\mathbb{O}_{\mathbb{P}}/I_{\mathbb{P}}, \widetilde{F}_{\mathbb{P}}), \tag{56}$$

where $\widetilde{F}_{\mathbb{P}} := \{\widetilde{p} \mid p \in \mathscr{F}(\mathbb{P})\}$ is a set of symbols, one for every fundamental element, $\mathbb{O}_{\mathbb{P}} := \mathbb{Z}[\widetilde{F}]$ is the free $\mathbb{Z}$-module on $\widetilde{F}_{\mathbb{P}}$, and $I_{\mathbb{P}}$ is the ideal generated by the following polynomials in $\mathbb{O}_{\mathbb{P}}$:

(i) $\widetilde{0} - 0$; $\widetilde{1} - 1$;

(ii) $\widetilde{-1} + 1$ *if* $-1 \in \mathscr{F}(\mathbb{P})$;

(iii) $\widetilde{p} + \widetilde{q} - 1$, *where* $p, q \in \mathscr{F}(\mathbb{P})$, $p + q \doteq 1$;

(iv) $\widetilde{p}\widetilde{q} - 1$, *where* $p, q \in \mathscr{F}(\mathbb{P})$, $pq = 1$;

(v) $\widetilde{p}\widetilde{q}\widetilde{r} - 1$, *where* $p, q, r \in \mathscr{F}(\mathbb{P})$, $pqr = 1$.

A partial field $\mathbb{P}$ is level *if $\mathbb{L}\mathbb{P} \cong \mathbb{P}$.*

We show that a matroid is $\mathbb{P}$-representable if and only if it is $\mathbb{L}\mathbb{P}$-representable. First we need a lemma.

Lemma 5.7. *Let $\mathbb{P}$ be a partial field. There exists a nontrivial partial field homomorphism $\varphi : \mathbb{L}\mathbb{P} \to \mathbb{P}$ such that $\varphi(\widetilde{p} + I_{\mathbb{P}}) = p$ for all $p \in \mathscr{F}(\mathbb{P})$.*

Proof. Let $\mathbb{O}$ be a ring such that $\mathbb{P} = \mathbb{P}(\mathbb{O}, S)$ for some S. Then $\psi : \mathbb{O}_{\mathbb{P}} \to \mathbb{O}$ determined by $\psi(\widetilde{p}) = p$ for all $\widetilde{p} \in \widetilde{F}_{\mathbb{P}}$ is obviously a ring homomorphism. Clearly $I_{\mathbb{P}} \subseteq \ker(\psi)$, so $\varphi' : \mathbb{O}_{\mathbb{P}}/I_{\mathbb{P}} \to \mathbb{O}$ determined by $\varphi'(\widetilde{p} + I_{\mathbb{P}}) = \psi(p)$ for all $\widetilde{p} \in \widetilde{F}_{\mathbb{P}}$ is a well-defined ring homomorphism. Then $\varphi := \varphi'|_{\mathbb{L}\mathbb{P}}$ is the desired partial field homomorphism. Since $1 \notin I_{\mathbb{P}}$, φ is nontrivial. □

Lemma 5.8. *Let $\mathbb{P}$ be a partial field. A matroid is $\mathbb{P}$-representable if and only if it is $\mathbb{L}\mathbb{P}$-representable.*

Proof. Let $\widehat{\mathbb{P}} := \mathbb{L}\mathbb{P}$ and let φ be the homomorphism from Lemma 5.7. We define ${}^{\uparrow} : \mathscr{F}(\mathbb{P}) \to \mathscr{F}(\widehat{\mathbb{P}})$ by $p^{\uparrow} = \widetilde{p} + I_{\mathbb{P}}$. By 5.6(*iii*),(*iv*) this is a lifting function for φ. Now all conditions of Corollary 3.8 are satisfied. □

The partial field $\mathbb{L}\mathbb{P}$ is the most general partial field for which the lift theorem holds, in the following sense:

Theorem 5.9. *Suppose $\mathbb{P}, \widehat{\mathbb{P}}, \varphi, {}^{\uparrow}$ are such that all conditions of Corollary 3.8 are satisfied. Then there exists a nontrivial homomorphism $\psi : \mathbb{L}\mathbb{P} \to \widehat{\mathbb{P}}$.*

Proof. Let $\psi' : \mathbb{O}_{\mathbb{P}} \to \widehat{\mathbb{P}}$ be determined by $\psi'(\widetilde{p}) = p^{\uparrow}$ for all $p \in \mathscr{F}(\mathbb{P})$. This is clearly a ring homomorphism. But since all conditions of Corollary 3.8 hold, $I_{\mathbb{P}} \subseteq \ker(\psi')$. It follows that there exists a well-defined homomorphism $\psi : \mathbb{L}\mathbb{P} \to \widehat{\mathbb{P}}$ as desired. □

The definition of a level partial field makes sense, as can be seen from the following proposition whose straightforward proof is omitted.

Proposition 5.10. $\mathbb{L}^2\mathbb{P} \cong \mathbb{L}\mathbb{P}$.

Homomorphisms between level partial fields are more well-behaved than homomorphisms between arbitrary partial fields:

Lemma 5.11. *Let $\mathbb{P}_1, \mathbb{P}_2$ be partial fields, and let $\mathbb{O}_{\mathbb{P}_1}/I_{\mathbb{P}_1}, \mathbb{O}_{\mathbb{P}_2}/I_{\mathbb{P}_2}$ be the rings as in Definition 5.6. Let $\varphi_i : \mathbb{L}\mathbb{P}_i \to \mathbb{P}_i$ be the homomorphisms from Lemma 5.7. Suppose that there exists a nontrivial partial field homomorphism $\varphi : \mathbb{P}_1 \to \mathbb{P}_2$. Then there exists a nontrivial ring homomorphism $\psi : \mathbb{O}_{\mathbb{P}_1}/I_{\mathbb{P}_1} \to \mathbb{O}_{\mathbb{P}_2}/I_{\mathbb{P}_2}$ such that the following diagram commutes:*

$$\begin{array}{ccc} \mathbb{L}\mathbb{P}_1 & \xrightarrow{\psi} & \mathbb{L}\mathbb{P}_2 \\ {\scriptstyle\varphi_1}\downarrow & & \downarrow{\scriptstyle\varphi_2} \\ \mathbb{P}_1 & \xrightarrow{\varphi} & \mathbb{P}_2 \end{array} \tag{57}$$

Proof. We define $\psi' : \mathbb{O}_{\mathbb{P}_1} \to \mathbb{O}_{\mathbb{P}_2}/I_{\mathbb{P}_2}$ by $\psi'(\widetilde{p}) = \widetilde{q} + I_{\mathbb{P}_2}$, where $\widetilde{q}$ is such that $\varphi(p) = q$. Again, this is obviously a ring homomorphism, and $I_{\mathbb{P}_1} \subseteq \ker(\psi')$. The homomorphism $\psi : \mathbb{O}_{\mathbb{P}_1}/I_{\mathbb{P}_1} \to \mathbb{O}_{\mathbb{P}_2}/I_{\mathbb{P}_2}$ determined by $\psi(\widetilde{p} + I_{\mathbb{P}_1}) = \psi'(\widetilde{p})$ is therefore well-defined. The diagram now commutes by definition, and therefore nontriviality of ψ follows from that of φ. □

$\mathbb{P}$	$\mathrm{GF}(2) \otimes \mathrm{GF}(3)$	$\mathrm{GF}(3) \otimes \mathrm{GF}(4)$	$\mathrm{GF}(3) \otimes \mathrm{GF}(5)$
$\mathbb{LP}$	$\mathbb{U}_0$	$\mathbb{S}$	$\mathbb{D}$
$\mathbb{P}$	$\mathrm{GF}(3) \otimes \mathrm{GF}(7)$	$\mathrm{GF}(3) \otimes \mathrm{GF}(8)$	$\mathrm{GF}(4) \otimes \mathrm{GF}(5)$
$\mathbb{LP}$	$\mathbb{Y}$	$\mathbb{U}_1$	$\mathbb{G}$
$\mathbb{P}$	$\mathrm{GF}(5) \otimes \mathrm{GF}(7)$	$\mathrm{GF}(5) \otimes \mathrm{GF}(8)$	$\mathrm{GF}(4) \otimes \mathrm{GF}(5) \otimes \mathrm{GF}(7)$
$\mathbb{LP}$	$\mathrm{GF}(5) \otimes \mathrm{GF}(7)$	$\mathrm{GF}(5) \otimes \mathrm{GF}(8)$	$\mathbb{G} \otimes \mathrm{GF}(7)$

Table 1: *Some level partial fields.*

The importance of Lemma 5.8 is that we can now *construct* partial fields for which the conditions of Corollary 3.8 hold. 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 [BV03] to verify the claims in Table 1.

The obvious question is now: is $\mathbb{LP} \ncong \mathbb{P}$ for other choices of $\mathbb{P} = \mathrm{GF}(q_1) \otimes \cdots \otimes \mathrm{GF}(q_k)$? The last three entries in Table 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 4.12 and 4.16 indicate that there are other uses still for the Lift Theorem. We conclude this section with a modification of Definition 5.6 that accommodates the characterization of the Gaussian partial field.

Definition 5.12. *Let $\mathbb{P}$ be a partial field and $\mathscr{A}$ a set of $\mathbb{P}$-matrices. We define the $\mathscr{A}$-*lift *of $\mathbb{P}$ as*

$$\mathbb{L}_{\mathscr{A}}\mathbb{P} := \mathbb{P}(\mathbb{O}_{\mathbb{P}}/I_{\mathbb{P}}, \widetilde{F}_{\mathbb{P}}), \tag{58}$$

where $\widetilde{F}_{\mathbb{P}} := \{\widetilde{p} \mid p \in \mathscr{F}(\mathbb{P})\}$ is a set of symbols, one for every fundamental element, $\mathbb{O}_{\mathbb{P}} := \mathbb{Z}[\widetilde{F}]$ is the free $\mathbb{Z}$-module on $\widetilde{F}_{\mathbb{P}}$, and $I_{\mathbb{P}}$ is the ideal generated by the following polynomials in $\mathbb{O}_{\mathbb{P}}$:

(i) $\widetilde{0} - 0$; $\widetilde{1} - 1$;

(ii) $\widetilde{-1} + 1$ *if* $-1 \in \mathscr{F}(\mathbb{P})$;

(iii) $\widetilde{p} + \widetilde{q} - 1$, *where* $p, q \in \mathscr{F}(\mathbb{P})$, $p + q \doteq 1$;

(iv) $\widetilde{p}\widetilde{q} - 1$, *where* $p, q \in \mathscr{F}(\mathbb{P})$, $pq = 1$;

(v) $\widetilde{p}\widetilde{q}\widetilde{r} - 1$, *where* $p, q, r \in \mathscr{F}(\mathbb{P})$, $pqr = 1$, *and*

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & p & q^{-1} \end{bmatrix} \preceq A \tag{59}$$

for some $A \in \mathscr{A}$.

We omit the proof of the following lemma.

Lemma 5.13. *Let $\mathbb{P}$ be a partial field and $\mathscr{A}$ a set of $\mathbb{P}$-matrices, and let M be a matroid. If $M = M([I|A])$ for some $A \in \mathscr{A}$ then M is $\mathbb{L}_{\mathscr{A}}\mathbb{P}$-representable.*

6 A number of questions and conjectures

While writing this paper we asked ourselves numerous questions. To some the answer can be found in this paper or in [PZ], but in this section we present a few that are still open.

Theorems such as those in Section 4 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:

Conjecture 6.1. *Let $k = p^m$, p prime, $m > 0$. 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* GF(q) *with $k \leq q \leq n_k$.*

To our disappointment the techniques in the present paper failed to prove this conjecture even for $k = 4$. We offer the following candidate:

Conjecture 6.2. *A matroid M is representable over all finite fields with at least* 4 *elements if and only if M is representable over*

$$\mathbb{P}_4 := \mathbb{P}(\mathbb{Q}(\alpha), \{\alpha, \alpha - 1, \alpha + 1, \alpha - 2\}). \tag{60}$$

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 GF(5). But consider $M_{8591} := M([I|A_{8591}])$, where A_{8591} is the following $\mathbb{P}_4$-matrix:

$$A_{8591} := \begin{bmatrix} 1 & 1 & 0 & \alpha & 1 \\ 0 & 1 & 1 & \alpha & \alpha^{-1} \\ 1 & 0 & \alpha & \alpha & 1 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix}. \tag{61}$$

This matroid was found by Royle in Mayhew and Royle's catalog of small matroids [MR08] as a matroid representable over GF(4), GF(7), GF(8) and uniquely representable over GF(5). M_{8591} is not representable over $\mathbb{K}_2$ (a fact that can be proven using tools from our forthcoming paper [PZ]).

Question 6.3. *To what extent is a partial field $\mathbb{P}$ determined by the set of finite fields* GF(q) *for which there exists a homomorphism $\varphi : \mathbb{P} \to$ GF(q)?*

The previous example shows that $\mathbb{P}$ is certainly not uniquely determined: both $\mathbb{K}_2$ and $\mathbb{P}_4$ have homomorphisms to all finite fields with at least 4 elements, but M_{8591} is only representable over the latter.

Question 6.4. *Are there systematic methods to determine the full set of fundamental elements for (certain types of) partial fields?*

Semple [Sem97] determined the set of fundamental elements for a class of partial fields that he calls the k-regular partial fields. In this paper we computed $\mathscr{F}(\mathbb{P})$ using ad hoc techniques, the only recurring argument being the fact that a homomorphism $\varphi : \mathbb{P} \to \mathbb{P}'$ maps $\mathscr{F}(\mathbb{P})$ to $\mathscr{F}(\mathbb{P}')$. We give two further illustrations. First, consider the partial field $\mathbb{P}(\mathbb{Q}, \{2, 3\})$. This innocent-looking set, reminiscent of the dyadic partial

field, has a finite number of fundamental elements, the least obvious of which are obtained from the relation $3^2 - 2^3 = 1$. That there is indeed no other such relation is a classical but nonobvious result. It was proven by Gersonides in 1342 (see, for example, Peterson [Pet99] for a modern exposition). Consideration of $\mathbb{P}(\mathbb{Q}, \{x, y\})$ for other pairs x, y brings us into the realm of Catalan's Conjecture. This conjecture was posed more than 150 years ago and settled only in 2002.

Second, consider the partial field

$$\mathbb{U}_1^{(2)} := \mathbb{P}(\mathrm{GF}(2)(\alpha), \{\alpha, 1+\alpha\}). \tag{62}$$

$\mathscr{F}(\mathbb{U}_1^{(2)})$ has infinite size, since $\alpha^{2^k} - 1 = (\alpha+1)^{2^k}$ for all $k \geq 0$.

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.

Question 6.5. *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 $\varphi : \mathbb{LP} \to \mathbb{F}$?*

In [PZ] we will show that each of $\mathbb{U}_0, \mathbb{S}, \mathbb{D}, \mathbb{U}_1, \mathbb{Y}, \mathbb{G}, \mathbb{H}_2$ has this property.

Question 6.6. *Let $\varphi : \mathbb{LP} \to \mathbb{P}$ be the canonical homomorphism. For which partial fields $\mathbb{P}$ is $\varphi|_{\mathscr{F}(\mathbb{LP})} : \mathscr{F}(\mathbb{LP}) \to \mathscr{F}(\mathbb{P})$ a bijection?*

This bijection exists for all examples in this paper 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. In that case the proof of the Lift Theorem can be simplified to some extent.

We end with two conjectures that seem to be only just outside the scope of the Lift Theorem:

Conjecture 6.7. *A matroid is representable over $\mathrm{GF}(2^k)$ for all $k > 1$ if and only if it is representable over $\mathbb{U}_1^{(2)}$.*

Conjecture 6.8. *A matroid is representable over $\mathrm{GF}(4) \otimes \mathbb{R}$ if and only if it is representable over $\mathbb{G}$.*

Perhaps a starting point for the latter is finding an alternative proof for Whittle's theorem that a matroid is representable over $\mathrm{GF}(3) \otimes \mathbb{Q}$ if and only if it is dyadic.

Acknowledgements We thank Hendrik Lenstra for suggesting the k-Cyclotomic partial field. We also thank Christian Eggermont for some helpful comments on rings of integers in algebraic number fields. Finally we thank Gordon Royle for his quick and friendly responses when we asked him for data from the catalog of small matroids [MR08]. His examples prevented the authors from embarking on several wild goose chases.

A When should we call a sum "defined"?

The notion of a sum $p_1+\cdots+p_n$ being *defined* appears somewhat complicated. Semple and Whittle [SW96] give a simpler definition: $p_1+\cdots+p_n$ is defined if there exists some association of $\{p_1,\ldots,p_n\}$. Unfortunately, this simpler definition has a problem. Consider the following matrices:

$$A := \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & b+a & c & d-a & -1 \\ 0 & -a & 0 & a & 1 \end{bmatrix}, B := \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & b & c & d & 0 \\ 0 & -a & 0 & a & 1 \end{bmatrix}, \quad (63)$$

where B is obtained from A by adding the last row to the next to last. Then $\det(A) = (b+a)+c+(d-a)-a+a$ and $\det(B) = b+c+d$. In both sums no cancellation has taken place: all terms missing from the formal determinant are 0. Now consider the following instantiation over $\mathbb{O} := \mathbb{Z}/51\mathbb{Z}$:

$$a = 37, b = 7, c = 23, d = 11. \quad (64)$$

Then none of $b+c, b+d, c+d$ are invertible, yet $a, b, c, d, 1, -1, (b+a), ((b+a)+c), d-a, ((b+a)+c)+(d-a)$ are. It follows that in $\mathbb{P}(\mathbb{O}, \mathbb{O}^*)$, $\det(A)$ is defined in the sense of Semple and Whittle [SW96], whereas $\det(B)$ is not.

This is a counterexample to Proposition 2.3(*iv*), which is therefore false under the old definition. This proposition is used for pretty much everything that comes after it in Semple and Whittle [SW96], so it is important to find a way to fix it. The proposed change in the meaning of a sum being *defined* is one way to do that. To make absolutely sure that this is indeed the case, we give a proof of Proposition 2.3 using the new definition.

Proof of Proposition 2.3. Assume B was obtained from A by transposition. Then

$$\det(B) = \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) b_{1\sigma(1)} b_{2\sigma(2)} \cdots b_{n\sigma(n)} \quad (65)$$

$$= \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) a_{\sigma(1)1} a_{\sigma(2)2} \cdots a_{\sigma(n)n} \quad (66)$$

which is nothing but a permutation of the terms of $\det(A)$.

Assume B was obtained from A by swapping rows 1 and 2. Then

$$\det(B) = \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) b_{1\sigma(1)} b_{2\sigma(2)} b_{3\sigma(3)} \cdots b_{n\sigma(n)} \quad (67)$$

$$= \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) a_{2\sigma(1)} a_{1\sigma(2)} a_{3\sigma(3)} \cdots a_{n\sigma(n)} \quad (68)$$

$$= \sum_{\sigma'\in S_n} \operatorname{sgn}(\sigma') a_{2\sigma'(2)} a_{1\sigma'(1)} a_{3\sigma'(3)} \cdots a_{n\sigma'(n)} \quad (69)$$

where $\sigma' = \sigma \circ (1,2)$ (in cycle notation; cycles act from the right). Therefore $\operatorname{sgn}(\sigma') = -\operatorname{sgn}(\sigma)$, from which the second part of the proposition follows.

For the third part, assume we multiply row 1 by a constant p. Then

$$\det(B) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) b_{1\sigma(1)} b_{2\sigma(2)} \cdots b_{n\sigma(n)} \tag{70}$$

$$= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) p a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)} \tag{71}$$

$$= p \det(A). \tag{72}$$

Here the last line follows from Axiom (P5).

For the final part we prove the following, more general lemma:

Lemma A.1. *Let $A = [a|X]$ and $B = [b|X]$ be $n \times n$ matrices with entries in $\mathbb{P}$ such that $A[n, \{2, \ldots, n\}] = B[n, \{2, \ldots, n\}] = X$. If $\det(A), \det(B), \det(A) + \det(B)$ and all entries of the vector $a + b$ are defined, then $\det([a+b|X]) \doteq \det(A) + \det(B)$.*

Proof. Set $C = [a + b|X]$. Then

$$\det(C) \quad = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) c_{1\sigma(1)} c_{2\sigma(2)} \cdots c_{n\sigma(n)} \tag{73}$$

$$= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) (a+b)_{1\sigma(1)} c_{2\sigma(2)} \cdots c_{n\sigma(n)} \tag{74}$$

$$\begin{aligned} = &\sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) (a+b)_{1\sigma(1)} c_{2\sigma(2)} \cdots c_{n\sigma(n)} \\ &- \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) b_{1\sigma(1)} c_{2\sigma(2)} \cdots c_{n\sigma(n)} \\ &+ \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) b_{1\sigma(1)} c_{2\sigma(2)} \cdots c_{n\sigma(n)} \end{aligned} \tag{75}$$

$$\begin{aligned} = &\sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} c_{2\sigma(2)} \cdots c_{n\sigma(n)} \\ &+ \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) b_{1\sigma(1)} c_{2\sigma(2)} \cdots c_{n\sigma(n)}. \end{aligned} \tag{76}$$

For (76) we used the fact that, if $(a + b)$ is defined, then $(a + b) - b \doteq a$ (an easy consequence of Axioms (P2) and (P6)), together with Axiom (P5). For the final expression it is easy to provide an association: take associations T_A, T_B for $\det(A), \det(B)$; add a new root vertex r and edges $r_A r, r_B r$. This is a pre-association for $\det(C)$. Since r_A is labelled by $\det(A)$ and r_B by $\det(B)$, we have that r is labelled by $\det(A)+\det(B)$, which was defined by assumption. □

Returning to the proof of the proposition, let B be obtained from A by adding row i to row 1, where we assume that $a_{1j} + a_{ij}$ is defined for all j. Let A' be the matrix obtained by replacing the first row of A by the ith row, and leaving all other rows unaltered. Since the first and the ith row of A' are identical, $\det(A') = 0$ (it is easy to find an association, since the terms of the determinant cancel pairwise). Applying the lemma to A, A' we conclude that $\det(B) \doteq \det(A) + \det(A') = \det(A)$, as desired. □

Since the proposed change occurs at the fringes of the definitions related to partial fields, it does not cause much damage. In fact, all other propositions, lemmas and theorems of [SW96, Sections 1–6] are true under the new definition.

As a final remark we note that, even with our definition, the following occurs. Consider the sum $1+1+1$ in $\mathbb{O} := \mathbb{Z}/4\mathbb{Z}$. The units of this ring are $1, 3$, and the only nontrivial sum that is defined in $\mathbb{P}(\mathbb{O}, \mathbb{O}^*)$ is $1 + 3 \doteq 0$. It follows that $1 + 1 + 1$ is undefined in $\mathbb{P}(\mathbb{Z}/4\mathbb{Z}, (\mathbb{Z}/4\mathbb{Z})^*)$ yet a unit in $\mathbb{O}$.

References

[BV03] R. Baines and P. Vámos, An algorithm to compute the set of characteristics of a system of polynomial equations over the integers. *J. Symbolic Comput.*, vol. 35, no. 3, pp. 269–279 (2003). Cited in Section 5.

[Ger89] A. M. H. Gerards, A short proof of Tutte's characterization of totally unimodular matrices. *Linear Algebra Appl.*, vol. 114/115, pp. 207–212 (1989). Cited in Section 3.

[GOVW98] J. Geelen, J. Oxley, D. Vertigan, and G. Whittle, Weak maps and stabilizers of classes of matroids. *Adv. in Appl. Math.*, vol. 21, no. 2, pp. 305–341 (1998). Cited in Section 1.

[Hli04] P. Hliněný, Using a computer in matroid theory research. *Acta Univ. M. Belii Ser. Math.*, , no. 11, pp. 27–44 (2004). Cited in Section 2.7.

[HW54] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers* (Oxford, at the Clarendon Press, 1954). 3rd ed. Cited in Section 2.9.

[LS99] J. Lee and M. Scobee, A characterization of the orientations of ternary matroids. *J. Combin. Theory Ser. B*, vol. 77, no. 2, pp. 263–291 (1999). Cited in Section 3.

[Mat86] H. Matsumura, *Commutative ring theory*, *Cambridge Studies in Advanced Mathematics*, vol. 8 (Cambridge University Press, Cambridge, 1986). Translated from the Japanese by M. Reid. Cited in Section 5.

[MR08] D. Mayhew and G. F. Royle, Matroids with nine elements. *J. Comb. Theory Ser. B*, vol. 98, no. 2, pp. 415–431 (2008). Cited in Section 6.

[Oxl92] J. G. Oxley, *Matroid Theory* (Oxford University Press, 1992). Cited in Sections 1, 2.1, and 2.8.

[Pet99] I. Peterson, Medieval harmony. Online article (1999). http://www.sciencenews.org/pages/sn_arc99/1_23_99/mathland.htm. Cited in Section 6.

[PZ] R. A. Pendavingh and S. H. M. van Zwam, Confinement of matroid representations to subfields of partial fields. In preparation. Cited in Sections 1, 5, and 6.

[Rad57] R. RADO, Note on independence functions. *Proc. London Math. Soc. (3)*, vol. 7, pp. 300–320 (1957). Cited in Section 1.

[Sem97] C. SEMPLE, k-regular matroids. In *Combinatorics, complexity, & logic (Auckland, 1996)*, Springer Ser. Discrete Math. Theor. Comput. Sci., pp. 376–386 (Springer, Singapore, 1997). Cited in Sections 2.7 and 6.

[ST87] I. STEWART and D. TALL, *Algebraic number theory*. Chapman and Hall Mathematics Series (Chapman & Hall, London, 1987), 2nd edition. Cited in Section 2.9.

[SW96] C. SEMPLE and G. WHITTLE, Partial fields and matroid representation. *Adv. in Appl. Math.*, vol. 17, no. 2, pp. 184–208 (1996). Cited in Sections 1, 2.2, 2.3, 2.5, 2.7, 2.8, 2.10, 2.11, 2.13, 3, and A.

[Tru92] K. TRUEMPER, *Matroid Decomposition* (Academic Press, Inc., 1992). Available online at http://www.emis.de/monographs/md/. Cited in Sections 1 and 3.

[Tut58] W. T. TUTTE, A homotopy theorem for matroids. I, II. *Trans. Amer. Math. Soc.*, vol. 88, pp. 144–174 (1958). Cited in Section 1.

[Tut65] W. T. TUTTE, Lectures on matroids. *J. Res. Nat. Bur. Standards Sect. B*, vol. 69B, pp. 1–47 (1965). Cited in Sections 1.1 and 2.29.

[Whi95] G. WHITTLE, A characterisation of the matroids representable over GF(3) and the rationals. *J. Combin. Theory Ser. B*, vol. 65, no. 2, pp. 222–261 (1995). Cited in Sections 1 and 3.

[Whi97] G. WHITTLE, On matroids representable over GF(3) and other fields. *Trans. Amer. Math. Soc.*, vol. 349, no. 2, pp. 579–603 (1997). Cited in Sections 1, 1.2, 2.30, 4.1, 4.2, 4.4, and 4.6.

[Whi99] G. WHITTLE, Stabilizers of classes of representable matroids. *J. Combin. Theory Ser. B*, vol. 77, no. 1, pp. 39–72 (1999). Cited in Sections 4.2 and 4.10.

[Whi05] G. WHITTLE, Recent work in matroid representation theory. *Discrete Math.*, vol. 302, no. 1-3, pp. 285–296 (2005). Cited in Sections 1 and 4.2.