university of groningen

faculty of science
and engineering

mathematics and applied
mathematics

Cross ratios for finite field geometries

Bachelor's Project Mathematics

February 2024

Student: P. K. Silins

First supervisor: Prof. Dr. O. Lorscheid

Second assessor: Prof. Dr. J. Top

Abstract

In this thesis we study matroids whose elements are the points of a projective plane over some finite field. We start by introducing matroids, giving multiple ways of defining a matroid, and explaining what it means for a matroid to be representable. We also touch upon the cross ratio, an essential invariant in projective geometry, and explore the connection to matroid representability. To formally establish this connection, partial fields are introduced. Partial fields are an algebraic structure which was originally studied to classify certain kinds of matroids that can be represented by a matrix whose subdeterminants are constrained to some multiplicative group. The final concept we introduce is the universal partial field. If a partial field is the universal partial field of a matroid, then every other representation of the matroid can be obtained from this universal partial field. We explain how to compute the universal partial field, which is where cross ratios become relevant again. In the results section we define a matroid represented over the finite field of order p. We then show that its universal partial field is exactly equal to this field for infinitely many primes p and for $p < 1000$.

Contents

1 Introduction

A subject of interest in combinatorics is the study of incidence structures. An incidence structure describes what is left after stripping away all of the more complicated concepts of a geometry, leaving only points, lines, and their relations. Affine and projective geometries are the simplest examples of these structures. In this thesis we will be studying projective planes over finite fields.

Projective geometry became a field of study when Renaissance painters were trying to establish the laws of perspective. They wanted to formally establish what happens when a three-dimensional object is turned into a two-dimensional image. In this process angles and relative magnitudes of lines easily become distorted. Even parallel lines might converge, even if only at some far-away point. Still, if two lines meet at a point, they will still meet at the same point after the image is finished. These observations form the basis of the projective plane and were later used to generalize the concept further. Projective transformations are then those that preserve these aspects of a geometry. The cross ratio features prominently when studying projective geometries, especially projective planes and lines. It is an invariant that ascribes a magnitude to an ordered quadruple of collinear points. The cross ratio remains unchanged under projective transformations. Due to this property it is the most fundamental invariant of projective geometry[1].

The study of the combinatorial aspects of point-line configurations will require the introduction of matroids. A matroid is an abstraction of the concept of linear independence. An incidence structure of a projective plane defines a matroid. In this thesis we will establish some elementary properties of matroids. Then we will explain what it means for a matroid to be represented over some field. We will also investigate why a matroid might be representable by a point-line configuration over one field but not another. As it turns out, the answer is heavily related to cross ratios.

We will also introduce partial fields and universal partial fields. A partial field is an algebraic structure first conceived by Semple and Whittle for the purpose of studying matroid representations[2]. The universal partial field was defined by Pendavingh and van Zwam, see [3] [4]. It is the final concept covered in the background section. We will explain how it is important, give its definition and a way of computing it. This thesis is built around van Zwam's PhD thesis [5].

In the results section we will show some attempts to explicitly compute the universal partial field of a matroid represented by a specific matrix, which was described by Brylawski in 1982 [6] to prove a related result. This is a rank-three matrix with $2\lfloor \log_2(p+1) \rfloor + 6$ elements. We would like to show that the universal partial field of this matroid is exactly $\mathbb{Z}/p\mathbb{Z}$. What we will show is that its universal partial field is a sub-partial field of $\mathbb{Z}/p\mathbb{Z}$ and that it is in fact isomorphic to $\mathbb{Z}/p\mathbb{Z}$ for primes smaller than a thousand.

A full dive into representation theory of matroids would be beyond the scope of the thesis, so if one wants to develop a more in-depth understanding, the joint works of Pendavingh and van Zwam [3] [4] [7], as well as van Zwam's PhD thesis [5] are excellent starting points. The textbook by Oxley [8] is also incredibly helpful for those with interest in matroid theory.

2 Preliminaries

2.1 Finite fields

It is assumed that the reader has at least rudimentary knowledge of the theory of fields, rings and groups. In this section we will outline some notation and conventions used from now on. An arbitrary field throughout the thesis will typically be denoted by $\mathbb{F}$. The finite field with q elements, where q is some prime power, will typically be denoted by $\mathbb{F}_q$. We will also point out that $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$ when p is a prime number. The unit group of a field $\mathbb{F}$ will typically be denoted by $\mathbb{F}^*$.

2.2 The projective plane

In this subsection we will give a brief overview of the basics of projective geometry. We use $\underline{S}$ to denote the linear subspace spanned by elements in S.

Definition 2.2.1. [9, Def. 2.1] For any vector space V define $P(V) = \{\underline{v} | 0 \neq v \in V\}$ and the dimension of $P(V)$ is $\dim(V) - 1$. Also define $\mathrm{PG}(n, \mathbb{F}) = P(\mathbb{F}^{n+1})$.

Definition 2.2.2. [9, Def. 2.3] For $F \subseteq E$ we can write $P(F)$. If F is a linear subspace of E we say that $P(F)$ is a projective subspace of $P(E)$. The 0, 1, and 2-dimensional cases are referred to as *projective points, lines and planes* respectively.

Definition 2.2.3. [9, Def. 2.2] We say $\underline{v} \in P(V)$ has *homogeneous coordinates* $[h^1 : h^2 : \ldots : h^n]$ with respect to the basis $b_1, \ldots, b_n$ of V if $v = \sum_{i=1}^{n} h^i b_i$.

Homogeneous coordinates are unique up to multiplication by a scalar. When working over $\mathbb{F}^n$, the basis will typically be the standard basis $\{e_i\}_{i \in \{1,\ldots,n\}}$, where $e_i^j = 0$ if $i \neq j$ and $= 1$ if $i = j$.

Definition 2.2.4. [9, Def. 2.6] To any injective linear map $L : V \to W$ we associate a map $P(L) : P(V) \to P(W)$ defined by $P(L)(\underline{v}) = \underline{L(v)}$, called the associated *projective transformation.*

Applying a projective transformation is the same as multiplying a vector consisting of the homogeneous coordinates by an invertible square matrix of appropriate size. In fact, the group of projective transformations of $\mathrm{PG}(n, \mathbb{F})$ is $\mathrm{GL}(\mathbb{F})_{n+1}$ [5]. Projective transformations map collinear points to collinear points[1]. In this thesis we will mostly concern ourselves with $\mathrm{PG}(2, \mathbb{F}_q)$, or the *projective plane* over $\mathbb{F}_q$. We will often simply write $\mathrm{PG}(2, q)$. $\mathrm{PG}(2, q)$ has exactly $q^2 + q + 1$ points and lines. Every two points are on exactly one line, and every two lines intersect in exactly one point[5].

2.3 Graph theory

In this subsection we will briefly give the necessary definitions from graph theory needed to understand the rest of thesis.

Definition 2.3.1. A *graph* $G = (V, E)$ is a pair consisting of a set of points V, the *vertices*, and a set of connections between these points, the *edges*.
An edge $\{x, y\}$ is denoted by xy. The set of vertices of a graph G is written as $V(G)$, the set of edges as $E(G)$.

Definition 2.3.2. The graph $G^{'} = (V^{'}, E^{'})$ is *subgraph* of the graph $G = (V, E)$ if all of its vertices and edges are also in G. It is called an *induced subgraph* if $E^{'} = \{e \in E | e \subseteq V^{'}\}$.

Definition 2.3.3. A graph $G = (V, E)$ is *bipartite* if V can be partitioned into sets U, W such that all $e \in E$ satisfy $|e \cap U| = |e \cap W| = 1$.

Definition 2.3.4. A *walk* in a graph $G = (V, E)$ is a sequence $(v_0, \ldots, v_n)$ of vertices such that, for $i = 0, 1, \ldots, n-1$, $v_i v_{i+1} \in E$. If $v_n = v_0$ the walk is called a *cycle.*

Definition 2.3.5. A graph is *connected* if there is a path between every pair of vertices.

Definition 2.3.6. A *forest* is a graph with no cycles, a *tree* is a connected forest.

Definition 2.3.7. A forest T spans a graph G if it is a subgraph of G, and adding any edge of G to T induces a cycle.

2.4 Matrices and set theory

We will briefly go through the set theoretic conventions used in this thesis. The set of natural numbers $\mathbb{N}$ contains 0. If X and Y are sets, $X - Y := X \backslash Y$. If X and Y are sets, we define their *symmetric difference* as $X \triangle Y := X - Y \cup Y - X$.

We will now describe the matrix notation used in this thesis. For ordered sets X and Y, an $X \times Y$ matrix over a field $\mathbb{F}$ is a function $A : X \times Y \to \mathbb{F}$. An $\mathbb{F}^{n \times m}$ matrix would then be described as a $\{1, \ldots, n\} \times \{1, \ldots, m\}$ matrix over $\mathbb{F}$.

If $X^{'} \subseteq X$ and $Y^{'} \subseteq Y$, then we denote by $A[X^{'}, Y^{'}]$ the submatrix of A obtained by deleting all rows and columns in $X - X^{'}$, $Y - Y^{'}$. If Z is a subset of $X \cup Y$ then we define $A[Z] := A[X \cap Z, Y \cap Z]$. Let A_1 be an $X \times Y_1$ matrix over $\mathbb{F}$ and A_2 an $X \times Y_2$ matrix over $\mathbb{F}$, where $Y_1 \cap Y_2 = \emptyset$. Then $A := [A_1 A_2]$ denotes the $X \times (Y_1 \cup Y_2)$ matrix with $A_{xy} = (A_i)_{xy}$ for $y \in Y_i, i \in \{1, 2\}$. If X is an ordered set, then I_X is the $X \times X$ identity matrix. If A is an $X \times X$ matrix, we usually shorten $[I_X A]$ as $[IA]$.

3 Background

3.1 Cross ratios

We will start with the traditional definition of a cross ratio. In it, for example, AD refers to the signed distance between two points. Under the ordering we give, if AC is positive, then DB would be negative.

Definition 3.1.1. [5, Def. 1.1.1] The *cross ratio* of an ordered quadruple of collinear points $A, B, C, D \in \mathbb{R}^n$ is

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

The value of the cross ratio does not change under various transformations. In fact, for $\lambda_A, \lambda_B, \lambda_C, \lambda_D \in \mathbb{R}^*$, the cross ratio of $(\lambda_A A, \lambda_B B, \lambda_C C, \lambda_D D)$ equals the cross ratio of (A, B, C, D). The same holds true if we instead multiply each of the points by a $n \times n$ matrix with a non-zero determinant. This means that cross ratios are unchanged by projective transformations.

Defining the cross ratio for fields other than $\mathbb{R}$ will require some adaptation, since there is no clear notion of distance. The following definition is meant to address this.

Definition 3.1.2. [5, Def. 1.1.7] Let A, B, C, D be four collinear points in $\mathrm{PG}(n, \mathbb{F})$. Let a, b, c, d be vectors in the 1-dimensional subspaces A, B, C, D respectively, such that

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

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

The two definitions are equivalent when working over $\mathbb{R}$. The invariance under scaling and projective transformations is also preserved. What does still matter is the order of the points, as can be seen in the following lemma.

Lemma 3.1.3. *[5, Lemma 1.1.9] Let A, B, C, D be an ordered quadruple of points in $PG(n, \mathbb{F})$ having cross ratio $\alpha \notin \{0, 1\}$, and let $\sigma \in S_4$ be a permutation. Then the cross ratio of the ordered quadruple $A^\sigma, B^\sigma, C^\sigma, D^\sigma$ is one of*

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

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

When working over $\mathbb{R}$, the cross ratio is useful, as it assigns a numerical value to four points that is invariant under projection. In this thesis we want to explore the combinatorial information encoded in a cross ratio. For this purpose we will introduce matroids.

3.2 Matroids

Matroids were originally introduced by Whitney in 1935, see [10]. Their introduction was motivated by an interest in finding some commonality between the concepts of dependence found in graph theory and linear algebra. Matroids are therefore considered to be an abstraction of (linear) independence.

Definition 3.2.1. [5, Def. 1.2.1] A *matroid* is a pair $(E, \mathscr{I})$, where E is a finite set, and $\mathscr{I}$ a collection of subsets of E such that

(i) $\emptyset \in \mathscr{I}$;

(ii) If $X \in \mathscr{I}$, and $Y \subseteq X$, then $Y \in \mathscr{I}$;

(iii) If $X, Y \in \mathscr{I}$, and $|X| > |Y|$, then there is an element $e \in X - Y$ such that $Y \cup e \in \mathscr{I}$.

The set of elements of a matroid M is denoted by $E(M)$, and is called the *ground set* of M. A subset $X \subseteq E(M)$ is *independent* if $X \in \mathscr{I}$, and *dependent* otherwise.

The following example is given to highlight how linear independence might translate from vector spaces to the more abstract world of matroids.

Example 3.2.2. [5, Ex. 1.2.2] Let E be a finite set of vectors in a vector space V, and let $\mathscr{I}$ be the set of all linearly independent subsets of E. Then $(E, \mathscr{I})$ is a matroid. To see this, let $X, Y \subseteq E$ be linearly independent subsets of vectors. Since the vectors in X are linearly independent, the linear subspace U spanned by X has dimension $|X|$. Likewise the linear subspace W spanned by Y has dimension $|Y|$. If $|X| > |Y|$, then not all vectors in X are contained in W. Hence there exists a vector $e \in X - Y$ such that $Y \cup \{e\}$ is linearly independent.

While somewhat less relevant to this thesis, the following example shows how matroids are connected to graph theory.

Example 3.2.3. [5, Ex. 1.2.3] Let $G = (V, E)$ be a graph, and let $\mathscr{I}$ be the edge-set of all forests of G. Then $(E, \mathscr{I})$ is a matroid. To see this, let $X, Y \subseteq E$ be such that the graphs (V, X) and (V, Y) are forests. The number of components of (V, X) is $|V| - |X|$. Likewise the number of components of (V, Y) is $|V| - |Y|$. If $|X| > |Y|$, then some edge in X must connect two of the components of (V, Y). Hence there exists an edge $e \in X - Y$ such that $(V, Y \cup e)$ is a forest.

The task of abstracting linear independence can approached in ways that are seemingly distinct from the one we give in definition 3.2.1. However, as it turns out, trying to do so often leads to an equivalent construction. These equivalences are called *cryptomorphisms*[11]. We will now give the two examples originally formulated by Whitney[10].

A *circuit* is of a matroid M is an inclusionwise minimal dependent set. This definition is particularly useful in graph theory, since the set of edge sets of cycles of a graph is the set of circuits of a matroid [8, prop. 1.1.7]. The following theorem allows us to uniquely characterize matroids by properties of the set of circuits:

Theorem 3.2.4. *[5, Thrm. 1.2.4] Let E be a finite set, and $\mathscr{C}$ a collection of subsets of E. Then $\mathscr{C}$ is the set of circuits of a matroid on E if and only if*

(i) $\emptyset \notin \mathscr{C}$;

(ii) If $C, C^{'} \in \mathscr{C}$ *and* $C^{'} \subseteq C$, *then* $C^{'} = C$;

(iii) If $C, C^{'} \in \mathscr{C}$ *and* $e \in C \cap C^{'}$, *then there is a set* $C^{''} \subseteq (C \cup C^{'}) - e$ *such that* $C^{''} \in \mathscr{C}$.

A *basis* of a matroid M is an inclusionwise maximal independent set. As the name might suggest, this cryptomorphism is inherited from linear algebra. This will be made more explicit in later sections. The following property characterizes matroids using a set of bases:

Theorem 3.2.5. *[5, Thrm 1.2.5] Let E be a finite set, and $\mathscr{B}$ a collection of subsets of E. Then $\mathscr{B}$ is the set of basis of a a matroid if and only if*

(i) $\mathscr{B} \neq \emptyset$;

(ii) If $B, B^{'} \in \mathscr{B}$, *and* $e \in B - B^{'}$, *then there exists an element* $f \in B^{'} - B$ *such that* $B \triangle \{e, f\} \in \mathscr{B}$.

We also also define the *rank of a matroid*. The connection between the rank of a matrix and the rank of a matroid will also be highlighted later on.

Definition 3.2.6. [5, Def. 1.2.6] Let $M = (E, \mathscr{I})$ be a matroid. The *rank function* of M, $\mathrm{rk}_M : 2^E \to \mathbb{N}$, is defined as

$$\mathrm{rk}_M(X) := \max\{|Y| \big| Y \subseteq X, Y \in \mathscr{I}\}.$$

If it is clear from context, the subscript M may be omitted. We use $\mathrm{rk}(M)$ for $\mathrm{rk}_M(E)$.

The rank function can be used to define another cryptomorphism [8].

3.2.1 Representability

As matroids inherit a lot of concepts from linear algebra, it would be useful to introduce some way of getting a matroid from a matrix, or to go from a matroid to a matrix. This leads us to one of the core concepts of this thesis, that being matroid representability.

Theorem 3.2.7. *[5, Thrm. 1.2.8] Let A be an $r \times E$ matrix over $\mathbb{F}$, and define*

$$\mathscr{I} := \{X \subseteq E \big| rk(A[r, X]) = |X|\}.$$

Then $(E, \mathscr{I})$ is a matroid.

The matroid of theorem 3.2.7 is denoted by $M[A]$. This is the same matroid described in example 3.2.2, where the columns of A are the vectors. We say that a matroid M is *representable* over a field $\mathbb{F}$ if there exists a matrix over $\mathbb{F}$ such that $M = M[A]$.

Characterizing matroids based on which field they are representable over is very central to matroid theory. We will provide one way of tackling this problem in the following sections. Before that, we still have to explore matroids a bit more.

Example 3.2.8. The *uniform matroid of rank two on four elements* is

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

This matroid is sometimes called the four-point line. Over $\mathbb{R}$ the matroid can be represented by the matrix

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

In fact, $U_{2,4}$ can be represented by A as a matrix over almost every field, the only exception being $\mathbb{F}_2$.

It is also possible to define a matroid using the points of $\mathrm{PG}(n, \mathbb{F})$, where $\mathbb{F}$ is a finite field. The base set of this matroid consists of the points in $\mathrm{PG}(n, \mathbb{F})$, and the independent set consists of subsets X of points such that the subspace spanned by them has dimension $|X|$. This matroid is denoted as $\mathrm{PG}(n, \mathbb{F})$. If A is the matrix consisting of the basis vectors of each of the 1-dimensional subspaces, then $M[A] = \mathrm{PG}(n, \mathbb{F})$. If $\mathbb{F} = \mathbb{F}_q$ we can also replace $\mathrm{PG}(n, \mathbb{F})$ with $\mathrm{PG}(n, q)$. The matroid does not depend on the specific basis vectors. Choosing different basis vectors is equivalent to scaling the columns of A. It is common to describe such a matroid using diagrams. In such a diagram the elements of the matroid are indicated by points. If three elements are dependent they are connected by a line (not necessarily straight), if four elements are dependent they lie on a common plane.

Example 3.2.9. [5, Ex. 1.2.32] Consider the Fano matroid, $F_7 := \mathrm{PG}(2, 2)$. It has seven elements. We have $F_7 = M[A]$, where A is the following matrix over $\mathbb{F}_2$:

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

In figure 1 we give a geometric representation of the Fano matroid.

3.2.2 Duals and minors of matroids

We will now introduce the *dual* of a matroid.

Theorem 3.2.10. *[5, Thrm. 1.2.13] Let $\mathscr{B}$ be the set of bases of a matroid M on ground set E. Define*

$$\mathscr{B}^* := \{E - B \big| B \in \mathscr{B}\}.$$

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

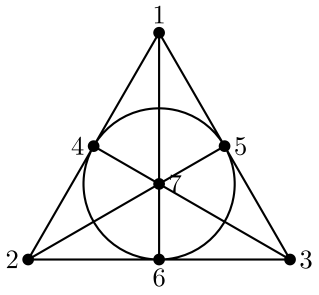

Figure 1: F_7, the Fano matroid

The matroid of theorem 3.2.10 is called the *dual* of M, and is denoted by M^*. The following proposition is related to the representability of the dual.

Proposition 3.2.11. *[5, Prop. 1.2.14] Let X, Y be disjoint sets. Suppose $M = M[A]$, where A is an $X \times (X \cup Y)$ matrix of the form $A = [ID]$, with D an $X \times Y$ matrix. Let A^* be the $Y \times (X \cup Y)$ matrix $A^* := [-D^T I]$. Then $M^* = M[A^*]$.*

Definition 3.2.12. [5, Def. 1.2.18] Let $M_1 = (E_1, \mathscr{I}_1), M_2 = (E_2, \mathscr{I}_2)$ be matroids. If there is a bijection $\sigma : E_1 \to E_2$ such that $X \in \mathscr{I}_1$ if and only if $\sigma(X) \in \mathscr{I}_2$, then we say M_1 and M_2 are *isomorphic*. This is denoted by $M_1 \cong M_2$.

We will also introduce some matroid operations.

Definition 3.2.13. [5, Def. 1.2.19] Let $M = (E, \mathscr{I})$ be a matroid, and $X \subseteq E$. The *deletion* of X from M is the matroid

$$M \backslash X := (E - X, \{Z \in \mathscr{I} \big| Z \cap X = \emptyset\}).$$

Definition 3.2.14. [5, Def. 1.2.20] Let M be a matroid, and $X \subseteq E(M)$. The *contraction* of X from M is the matroid

$$M/X := (M^* \backslash X)^*.$$

We can now talk about *minors* of matroids.

Definition 3.2.15. [5, Def. 1.2.22] If a matroid N can be obtained from a matroid M by deleting and contracting elements then N is a *minor* of M.

Definition 3.2.16. [5, Def. 1.2.23] We write $N \preceq M$ if matroid N is isomorphic to a minor of matroid M.

Proposition 3.2.17. *[5, Prop. 1.2.25] Let M be a matroid representable over a field $\mathbb{F}$. If $N \preceq M$ then N is representable over $\mathbb{F}$.*

3.2.3 Cross ratios in matroid representations

To explain how cross ratios and matroid representation are related, we will be returning to the matroid $U_{2,4}$. This is how it was done in van Zwam's thesis [5]. We already gave an example of a matrix representation of this matroid. As it turns out, any four distinct non-zero vectors in $\mathbb{F}^2$ are satisfactory. This is also the reason why $U_{2,4}$ is not representable over $\mathbb{F}_2$, since $\mathbb{F}_2^2$ only has three distinct non-zero vectors. What we would now like to do is find the constellations of points in $\mathrm{PG}(2, q)$ that let us define this matroid. Applying projective transformations to a representation matrix does not change the matroid, so we will assume that it has the form

$$\begin{bmatrix} 1 & 0 & 1 & \alpha \\ 0 & 1 & 1 & 1 \end{bmatrix},$$

where $\alpha \notin \{0,1\}$. If we permute the columns and rescale the matrix, we can obtain a matrix that has one of the following forms:

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

$$\begin{bmatrix}1 & 0 & 1 & \frac{1}{\alpha}\\ 0 & 1 & 1 & 1\end{bmatrix}, \begin{bmatrix}1 & 0 & 1 & \frac{1}{1-\alpha}\\ 0 & 1 & 1 & 1\end{bmatrix}, \begin{bmatrix}1 & 0 & 1 & \frac{\alpha-1}{\alpha}\\ 0 & 1 & 1 & 1\end{bmatrix}.$$

Recalling the set given in lemma 3.1.3 suggests some connection between cross ratios and matroid representability. What we meant to illustrate with this is that finding a representation of $U_{2,4}$ is equivalent to picking 4 collinear points in $\mathrm{PG}(2,\mathbb{F})$, then picking a cross ratio obtained by changing their order. Over $\mathbb{F}_2$ this is impossible, as there are no four-point lines. Over $\mathbb{F}_3$ there is one unique cross ratio, that being -1. Over $\mathbb{F}_4 = \{0,1,\omega,\omega^2\}$ there a two different cross ratios, those being ω and ω^2. As a consequence, there is no unique representation of $U_{2,4}$ over $\mathbb{F}_4$ or any bigger field.

Finding a representation of a matroid is then the same as choosing a cross ratio for all four-point lines it has as a minor. We will eventually give a possible way to explicitly find the cross ratios of a matroid.

3.3 Partial fields

Partial field is an algebraic structure that was first introduced by Semple and Whittle in 1996 [2]. It is possible to classify certain matroids based on values of the subdeterminants of their representation matrices. For example, it is well known result that a matroid is representable over $\mathbb{F}_2$ and another field of characteristic other than 2 if and only if it can be represented over the rationals by a matrix whose subdeterminants are contained in $\{0,1,-1\}$ [12]. Partial fields were originally defined in an axiomatic way, however, we will use a definition involving rings and multiplicative groups, which was also utilized by Pendavingh and van Zwam[3].

Definition 3.3.1. [5, Def. 2.1.1] A *partial field* is a pair (R,G), where R is a commutative ring, and G is a subgroup of R^* such that $-1 \in G$.

If $\mathbb{P} = (R,G)$ is a partial field, and $p \in R$, then we say that p is an element of $\mathbb{P}$ (write $p \in \mathbb{P}$) if $p = 0$ or $p \in G$. We define $\mathbb{P}^* := G$. We will now look at how certain concepts from algebraic structures can be translated into the language of partial fields.

Definition 3.3.2. [5, Def. 2.1.2] A partial field is *trivial* if $1 = 0$.

Example 3.3.3. [5, Ex. 2.2.1] Perhaps the simplest example of a partial field is the pair $(\mathbb{F},\mathbb{F}^*)$, where $\mathbb{F}$ is a field. Throughout the thesis the field $\mathbb{F}$ will be seen as this partial field.

Definition 3.3.4. [5, Def. 2.2.4] Let $\mathbb{P}_1, \mathbb{P}_2$ be partial fields. A function $\varphi : \mathbb{P}_1 \to \mathbb{P}_2$ is a *partial-field homomorphism* if

(i) $\varphi(1) = 1$;

(ii) For all $p.q \in \mathbb{P}_1, \varphi(pq) = \varphi(p)\varphi(q)$;

(iii) For all $p,q,r \in \mathbb{P}_1$ such that $p+q=r$, $\varphi(p)+\varphi(q)=\varphi(r)$.

φ is a *partial-field isomorphism* [5, Def. 2.2.7] if

(i) φ is a bijection;

(ii) $\varphi(p)+\varphi(q) \in \mathbb{P}_2$ if and only if $p+q \in \mathbb{P}_1$.

Definition 3.3.5. [5, Def. 2.2.13] A pair $\mathbb{P}' = (R', G')$ is a *sub-partial field of* $\mathbb{P} = (R,G)$ if R' is a subring of R and G' is a subgroup of G, such that $G' \subseteq R'$ and $-1 \in G'$.

Definition 3.3.6. [5, Def. 2.2.15] Let $\mathbb{P} = (R, G)$ be a partial field, and let $S \subseteq \mathbb{P}^*$. Then the sub-partial field *generated by* S is

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

Finally, we will introduce the concept of *fundamental elements.*

Definition 3.3.7. [5, Def. 2.2.9] Let $\mathbb{P}$ be a partial field. An element $p \in \mathbb{P}$ is fundamental if

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

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

Proposition 3.3.8. *[5, Prop. 2.2.10] Let $\mathbb{P}$ be a partial field, and p a fundamental element of $\mathbb{P}$, with $p \notin \{0, 1\}$. Then*

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

A connection between cross ratios and fundamental elements should be starting to become more apparent, and will be made explicit later on.

3.3.1 $\mathbb{P}-$matrices

Recalling the motivation for defining partial fields, it would be very useful to introduce some notion of a matroid being represented over a partial field. As a first step, we will introduce *weak* $\mathbb{P}$*-matrices.*

Definition 3.3.9. [5, Def. 2.1.3] Let $\mathbb{P} := (R, G)$ be a partial field, and let A be an $r \times E$ matrix with entries in R. Then A is *weak* $\mathbb{P}-$*matrix* if, for all $X \subseteq E$ such that $|X| = r$, $\det(A[r, X]) \in \mathbb{P}$.

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

Proposition 3.3.10. *[5, Prop. 2.1.4] Let $\mathbb{P} = (R, G)$ be a partial field, A a nondegenerate $r \times E$ weak $\mathbb{P}-$matrix, and define*

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

Then $\mathscr{B}$ is the set of basis of a matroid.

The matroid of proposition 3.3.10 is denoted by $M[A]$.

Definition 3.3.11. [5, Def. 2.1.5] Let M be a matroid. We say M is *representable* by over a partial field $\mathbb{P}$ (or, shorter, $\mathbb{P}-$representable) if there exists a non-degenerate weak $\mathbb{P}-$matrix such that $M = M[A]$. Moreover, we refer to A as a *representation matrix* of M, and say M is *represented* by A.

Weak $\mathbb{P}$-matrices are a good start for what we were trying to accomplish. As explained by van Zwam, "ring homomorphisms map weak $\mathbb{P}$-matrices to weak $\mathbb{P}-$matrices, but it is not clear if partial-field homomorphisms have this property" and "it is not obvious that being representable over $\mathbb{P}$ is a mirror-closed property"[5, p. 31]. What we will introduce now is a more restricted class of matrices over partial fields.

Definition 3.3.12. [5, Def. 2.3.2] Let $\mathbb{P} = (R, G)$ be a partial field, and let A be an $X \times Y$ matrix with entries in R. Then A is a *strong* $\mathbb{P}-$matrix if $\det(A[X', Y']) \in \mathbb{P}$, for all $X' \subseteq X$, $Y' \subseteq Y$ such that $|X'| = |Y'|$.

We will use the term *subdeterminant* for the determinant of a square matrix of A.

Proposition 3.3.13. *[5, Prop. 2.3.4] Let A be a strong $\mathbb{P}$-matrix. Then A^T and $[IA]$ are also strong $\mathbb{P}$-matrices.*

Definition 3.3.14. [5, Def. 2.3.5] Let A be an $X \times Y$ strong $\mathbb{P}$-matrix. The *rank* of A is

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

From now on, a strong $\mathbb{P}-$matrix will simply be referred to as a $\mathbb{P}-$matrix.

We will now explain how to obtain minors of $\mathbb{P}$-matrices as well as introduce some notion of equivalence between two different $\mathbb{P}$-matrices. We should be careful, since minors of $\mathbb{P}-$matrices are not the same as minors of matrices.

Definition 3.3.15. [5, Def. 2.3.14] Let A be an $X \times Y$ matrix over a ring R, and let $x \in X, y \in Y$ be such that $A_{xy} \in R^*$. Then we define A^{xy} to be the $(X - x) \cup y \times (Y - y) \cup x$ matrix with entries

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

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

Definition 3.3.16. [5, Def. 2.3.21] Let A be an $X \times Y$ $\mathbb{P}-$matrix. We say that $A^{'}$ is a *minor* of A if $A^{'}$ can be obtained from A by a sequence of the following operations:

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

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

(iii) Deleting rows or columns;

(iv) Pivoting over a nonzero entry.

Proposition 3.3.17. *[5, Prop. 2.3.22] If $A^{'}$ is a minor of A then $A^{'}$ is a $\mathbb{P}-$matrix.*

Definition 3.3.18. [5, Def. 2.3.23] 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 $x \in X, y \in Y, A_{xy} = A^{'}_{f(x)g(y)}$.

Definition 3.3.19. [5, Def. 2.3.24] We write $A^{'} \preceq A$ if $A^{'}$ is isomorphic to a minor of A.

Definition 3.3.20. [5, Def. 2.3.25] 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 $A \sim A^{'}$.

We finally revisit cross ratios and give a new, appropriate definition.

Definition 3.3.21. [5, Def. 2.3.29] Let A be a $\mathbb{P}-$matrix. We define the *cross ratios* of A as the set

$$\mathrm{Cr}(A) := \left\{ p \Big| \begin{bmatrix} 1 & 1 \\ p & 1 \end{bmatrix} \preceq A \right\}.$$

Example 3.3.22. We will now briefly return to our example of $U_{2,4}$. It can be represented over a partial field $\mathbb{P}$ by the following matrix

$$A = \begin{bmatrix} 1 & 0 & 1 & \alpha \\ 0 & 1 & 1 & 1 \end{bmatrix},$$

where $\alpha \notin \{0, 1\}$, $\alpha \in \mathscr{F}(\mathbb{P})$. Then $\{\alpha, 1 - \alpha, \frac{1}{1-\alpha}, \frac{\alpha}{1-\alpha}, \frac{1-\alpha}{\alpha}, \frac{1}{\alpha}\} \subseteq \mathrm{Cr}(A)$, as we might expect based on our brief discussion in subsection 3.2.3.

As promised, we will also now explain one way in which cross ratios and fundamental elements are related.

Lemma 3.3.23. *[5, Lemma 2.3.30] Let A be an $\mathbb{P}$-matrix. Then $Cr(A) \subseteq \mathscr{F}(\mathbb{P})$.*

Cross ratios are also useful when focusing on sub-partial fields.

Definition 3.3.24. [5, Def. 2.3.33] Let $\mathbb{P}, \mathbb{P}^{'}$ be partial fields with $\mathbb{P}^{'} \subseteq \mathbb{P}$, and let A be a $\mathbb{P}$-matrix. We say that A is a scaled $\mathbb{P}^{'}$-matrix if $A \sim A^{'}$ for some $\mathbb{P}^{'}$-matrix $A^{'}$.

Theorem 3.3.25. *[5, Thrm. 2.3.34] Let A be a $\mathbb{P}$-matrix. Then A is a scaled $\mathbb{P}[Cr(A)]$-matrix.*

Before moving on to universal partial fields, we state one last result.

Proposition 3.3.26. *[5, Prop. 2.4.6] If a matroid M is representable over a partial field $\mathbb{P}$, then M is representable over $\mathbb{P}[\mathscr{F}(\mathbb{P})]$.*

3.4 Universal partial field of a matroid

The universal partial field was introduced by R. A. Pendavingh and S. H. M. van Zwam in [3], see also [4]. In this section we will explain the motivation behind defining this universal partial field and give two methods for computing it for some specific matroid.
The universal partial field of a matroid has the following property[1] :

Theorem 3.4.1. *[5, Thrm 3.A] Let M be a matroid, let X be a basis of M, and let $Y := E(M) - X$. If $\mathbb{P}_M$ is the universal partial field of M, there exists an $X \times Y$ $\mathbb{P}_M-$matrix A, such that there is a homomorphism $\varphi : \mathbb{P}_M \to \mathbb{P}^{'}$ with $\varphi(A) \sim A^{'}$ for every partial field $\mathbb{P}^{'}$ and for every $X \times Y$ $\mathbb{P}-$matrix $A^{'}$ with $M = M[IA']$.*

What this means is that every representation of M, over every partial field, can be obtained from A. The universal partial field is hence the most general partial field over which a single matroid is representable. Before showing how to formally compute universal partial field of a matroid we will jump a little bit forward and state the following lemma:

Lemma 3.4.2. *[5, Lemma 3.3.18] Let $\mathbb{P}$ be the universal partial field for some matroid, and let $\mathscr{M}$ be the class of $\mathbb{P}-$representable matroids. Then all $M \in \mathscr{M}$ are $\mathbb{P}^{'}$-representable if and only if there exists a homomorphism $\varphi : \mathbb{P} \to \mathbb{P}^{'}$.*

This result is very simple to write down, while also providing some motivation behind why the universal partial field is worth studying.

3.4.1 The bracket ring

Below is given one of the ways of constructing the universal partial field of a matroid. This construction is taken from [5, section 3.3.1]. It was based on the bracket ring as introduced by White in [13].

Let M be a rank-r matroid with ground set E and set of bases $\mathscr{B}$. For every $r-$tuple $Z \in E^r$ we introduce a symbol $[Z]$, the "bracket" of Z, and symbol $\overline{[Z]}$. Suppose $Z = (x_1, \dots, x_r)$. Define $\{Z\} := \{x_1, \dots, x_r\}$, and $Z/x \to y$ as the $r-$tuple obtained from Z by replacing each occurrence of x by y. We define

$$\mathscr{X}_M := \{[Z] \big| Z \in E^r\} \cup \{\overline{[Z]} \big| \{Z\} \in \mathscr{B}\}.$$

Definition 3.4.3. [5, Def. 3.3.2] I_M is the ideal in $\mathbb{Z}[\mathscr{X}_M]$ generated by the following polynomials:

(i) $[Z]$, for all Z such that $\{Z\} \notin \mathscr{B}$;

(ii) $[Z]$ - $\text{sgn}(\sigma)[Z^\sigma]$, for all Z and permutations $\sigma : \{1, \dots, r\} \to \{1, \dots, r\}$;

(iii) $[x_1, x_2, U][y_1, y_2, U] - [y_1, x_2, U][y_1, x_1, U]$, for all $x_1, y_1, x_2, y_2 \in E$ and $U \in E^{r-2}$;

(iv) $[Z]\overline{[Z]} - 1$, for all $Z \in E^r$ such that $\{Z\} \in \mathscr{B}$.

Definition 3.4.4. [5, Def. 3.3.3] $B_M := \mathbb{Z}[\mathscr{X}_M]/I_M$.

[1] The original theorem simply guaranteed the existence of some partial field $\mathbb{P}_M$ such that this property holds. This property does not characterize the universal partial field.

Definition 3.4.5. Let M be a rank-r matroid. Let $B \in E^r$ be such that $\{B\}$ is a basis of M. $A_{M,B}$ is the $B \times (E - B)$ matrix with entries in B_M given by

$$(A_{M,B})_{u,v} := [B/u \to v]/[B].$$

Definition 3.4.6. [5, Def. 3.3.12] If M is a matroid, then the set of *cross ratios of* M is

$$\mathrm{Cr}(M) := \mathrm{Cr}(A_{M,B}).$$

Note that $\mathrm{Cr}(M)$ does not depend on choice of B. We introduce the following subring of B_M:

$$R_M := \mathbb{Z}[\mathrm{Cr}(M)]/I_M.$$

Definition 3.4.7. [5, Def 3.3.13] The *universal partial field* of M is

$$\mathbb{P}_M := (R_M, \langle \mathrm{Cr}(M) \cup \{-1\} \rangle).$$

3.4.2 An alternative construction

We give another way of constructing the partial field of a matroid, taken from [5, section 3.3.2]. This is the definition we will use later on to calculate the universal partial field of the relevant matroids.

Let M be a rank-r matroid with ground set E and set of bases $\mathscr{B}$, let $B \in \mathscr{B}$, and let $G(M, B)$ be the bipartite graph with vertices $V(G) = B \cup (E - B)$ and edges $\{xy \in B \times (E - B) \big| B \triangle \{x, y\} \in \mathscr{B}\}$. Finally, let T be a spanning forest for $G(M, B)$. For every $x \in B, y \in E - B$ we introduce a symbol a_{xy}. For every $B^{'} \in \mathscr{B}$ we introduce a symbol $i_{B'}$. We define

$$\mathscr{Y}_M := \{a_{xy} \big| x \in B, y \in E - B\} \cup \{i_{B'} \big| B^{'} \in \mathscr{B}\}.$$

Let $\hat{A}_{M,B}$ be the $B \times (E - B)$ matrix with entries a_{xy}.

Definition 3.4.8. [5, Def. 3.3.14] $I_{M,B,T}$ is the ideal in $\mathbb{Z}[\mathscr{Y}_M]$ generated by the following polynomials:

(i) $\det(\hat{A}_{M,B}[B \triangle Z])$ if $|Z| = |B|, Z \notin \mathscr{B}$;

(ii) $\det(\hat{A}_{M,B}[B \triangle Z]) i_Z - 1$ if $|Z| = |B|$, $Z \in \mathscr{B}$;

(iii) $a_{xy} - 1$ if $xy \in T$

for all $Z \in \{Z^{'} \subseteq \big| |Z| = r\}$.

Now we define

$$B_{M,B,T} := \mathbb{Z}[\mathscr{Y}_M]/I_{M,B,T}$$

and

$$\mathbb{P}_{M,B,T} := (B_{M,B,T}, \langle \{i_{B'} \big| B^{'} \in \mathscr{B}\} \cup \{-1\} \rangle).$$

Finally, $\hat{A}_{M,B,T}$ is the matrix $\hat{A}_{M,B}$, viewed as a matrix over $\mathbb{P}_{M,B,T}$.

Theorem 3.4.9. *[5, Thrm. 3.3.16]* $B_{M,B,T} \cong R_M$ *and* $\mathbb{P}_{M,B,T} \cong \mathbb{P}_M$.

Note that $\mathbb{P}_{M,B,T}$ does not depend on choice of basis or spanning tree. We will now give some example computations of the universal partial fields of some select matroids.

Example 3.4.10. $\mathbb{P}_{U_{2,4}} \cong (\mathbb{Z}[\alpha, \frac{1}{\alpha}, \frac{1}{\alpha - 1}], \langle \{\alpha, (\alpha - 1), -1\} \rangle)$.
Let $B := \{1, 2\}$, and T be the spanning forest of $G(U_{2,4}, B)$ with edges $13, 14, 23$. Then

$$\hat{A}_{U_{2,4},B,T} = \begin{array}{c} \\ 1 \\ 2 \end{array} \begin{array}{c} \begin{array}{cc} 3 & 4 \end{array} \\ \begin{bmatrix} 1 & 1 \\ 1 & \alpha \end{bmatrix} \end{array}$$

where α is some indeterminate element. Next we notice that $\{3, 4\} \in \mathscr{B}$, so $\det(\hat{A}_{U_{2,4},B,T}[\{1, 2\} \triangle \{3, 4\}]) = \alpha - 1$, which implies $i_{3,4} = (\alpha - 1)^{-1}$. Similarly, $\{1, 4\} \in \mathscr{B}$ and $\det(\hat{A}_{U_{2,4},B,T}[\{1, 2\} \triangle \{1, 4\}]) = \alpha$, which implies $i_{1,4} = \alpha^{-1}$. All of the other i_Zs are equal to 1. The result then follows.

Example 3.4.11. Recall the Fano matroid, F_7, the matroid defined over $\mathrm{PG}(2,2)$. Then $\mathbb{P}_{F_7} \cong \mathbb{F}_2$. Let $B := \{1,2,3\}$ and T be the spanning forest of $G(F_7, B)$ with edges $17, 27, 37, 14, 15, 26$. Then

$$\hat{A}_{F_7,B,T} = \begin{array}{c|cccc} & 4 & 5 & 6 & 7 \\ \hline 1 & 1 & 1 & 0 & 1 \\ 2 & a & 0 & 1 & 1 \\ 3 & 0 & b & c & 1 \end{array}.$$

Notice that $\det(A[3,\{3,4,7\}]) = 0$, so $\det(\hat{A}_{F_7,B,T}[\{1,2,3\} \triangle \{3,4,7\}]) = 1 - a$ and therefore $a = 1$. Similarly, by using $Z = \{2,5,7\}$ and $Z = \{1,6,7\}$, we can show that $b = 1$ and $c = 1$, respectively. All $i_{B'}$s are also equal to 1. Finally, noticing that $\det(A[3,\{4,5,6\}]) = 0$ and $\det(\hat{A}_{F_7,B,T}[\{1,2,3\} \triangle \{4,5,6\}]) = -2$ is enough to conclude that in the universal partial field $2 = 0$ and that it is isomorphic to $\mathbb{F}_2$.

Example 3.4.12. For each prime power q we will describe a rank-three matroid on $3q+1$ elements with partial field $\mathbb{F}_q$. Let Q_q be the rank-three matroid consisting of three distinct $q+1-$point lines $L_1, L_2, L_3 \subset \mathrm{PG}(2,q)$ such that $L_1 \cap L_2 \cap L_3 = \emptyset$. Then Q_q^+ is the matroid obtained by adding a point $e \in \mathrm{PG}(2,q) - L_1 \cup L_2 \cup L_3$ to Q_q. Then $\mathbb{P}_{Q_q^+} \cong \mathbb{F}_q$. Additionally, Q_q^+ can be represented by the following matrix:

$$\begin{array}{ccccccccccccccc} e_1 & e_2 & e_3 & e & a_0 & a_1 & & a_{q-2} & b_0 & & b_{q-2} & c_0 & & c_{q-2} \\ 1 & 0 & 0 & 1 & 0 & 0 & \dots & 0 & 1 & \dots & 1 & 1 & \dots & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & & 1 & 0 & & 0 & 1 & & \alpha^{q-2} \\ 0 & 0 & 1 & 1 & 1 & \alpha & \dots & \alpha^{q-2} & 1 & \dots & \alpha^{q-2} & 0 & \dots & 0 \end{array},$$

where α is a generator of $\mathbb{F}_q^*$. For proof and additional details, see [5, Thrm. 3.3.25].

4 Results

The main goal of this thesis was to find a (potentially minimal) matroid represented by $\mathrm{PG}(2, \mathbb{F}_q)$ such that the universal partial field of this matroid is $\mathbb{F}_q$. In example 3.4.12 we show that there exists a rank-3 matroid with $3q+1$ elements such that this holds. This, with the exception of F_7, is not the minimal such matroid. The matroid represented by

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & \omega^2 \\ 0 & 1 & 0 & 1 & 1 & \omega & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & \omega & 0 & 1 & \omega & 1 & 1 \end{bmatrix}$$

over $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$ has this property and the matrix has only 10 elements. The universal partial field of the matroid represented by the following matrix over $\mathbb{F}_5$

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 2 \\ 0 & 1 & 0 & 1 & 1 & 2 & 3 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 2 & 1 & 1 \end{bmatrix}$$

is equal to $\mathbb{F}_5$, while the matrix has only 11 elements. More details can be found in [14]. It is also noteworthy that these matrices are isomorphic to minors of the ones given in example 3.4.12.

4.1 A matroid over $\mathrm{PG}(2, \mathbb{F}_p)$

The structure of the following matrix is taken from [6], a paper referenced in van Zwam's PhD thesis [5]. That paper is concerned with characteristic sets of matroids represented by a projective plane. The characteristic set of a configuration of points and lines is the the set of prime numbers such that this configuration can be represented only over fields with this characteristic. The matrix we will investigate in the rest of this thesis was shown to have characteristic set $\{p\}$. This result is at least somewhat analogous to what we want to obtain by calculating the universal partial field. The rest of this section consists of my attempts to translate and expand the proof given in [6] into the language of universal partial fields.

Let p be an odd prime greater than 3, and let $l = \lfloor \log_2(p+1) \rfloor$. For $i = 0, 1, 2, \ldots, l$, set b_i equal to $\lfloor (p+1)/2^{l-i+1} \rfloor$. Then $b_0 = 0, b_1 = 1, b_l = \frac{p+1}{2}$. Also notice that $b_{i+1} = 2b_i$ or $b_{i+1} = 2b_i + 1$. For a fixed prime p, let A be the following matrix over $\mathbb{F}_p$ with $i = 1, 2, \ldots, l-1$:

$$\begin{array}{c} \\ A = \end{array} \begin{array}{cccccccccccccc} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 & e_8 & & e_{2i+7} & e_{2i+8} & & e_{2l+5} & e_{2l+6} \\ \left[\begin{matrix} 1 \\ 0 \\ 0 \end{matrix}\right. & \begin{matrix} 0 \\ 1 \\ 0 \end{matrix} & \begin{matrix} 0 \\ 0 \\ 1 \end{matrix} & \begin{matrix} 1 \\ 1 \\ 1 \end{matrix} & \begin{matrix} 1 \\ 1 \\ 0 \end{matrix} & \begin{matrix} 1 \\ 0 \\ 1 \end{matrix} & \begin{matrix} 0 \\ 1 \\ 1 \end{matrix} & \begin{matrix} 1 \\ 2 \\ 1 \end{matrix} & \begin{matrix} \ldots \\ \ldots \\ \ldots \end{matrix} & \begin{matrix} 1 \\ 2 \\ b_{i+1} \end{matrix} & \begin{matrix} 0 \\ 1 \\ b_{i+1} \end{matrix} & \begin{matrix} \ldots \\ \ldots \\ \ldots \end{matrix} & \begin{matrix} 1 \\ 2 \\ b_l \end{matrix} & \left.\begin{matrix} 0 \\ 1 \\ b_l \end{matrix}\right] \end{array}.$$

Theorem 4.1.1. *Let $M = M[A]$ be the matroid represented by A. If the universal partial field of M is $\mathbb{P}_M = (R_M, G)$, where R_M is a ring and G is a subgroup of R_M^*, then $R_M \cong \mathbb{F}_p$ and G is a subgroup of $\mathbb{F}_p^*$.*

Proof: Let $B := \{e_1, e_2, e_3\}$, which is then a basis of M. Let T be a spanning tree of $G(M, B)$ with edges e_1e_4, e_2e_4, e_3e_4, e_1e_5, e_1e_6, e_1e_8, e_1e_{2i+7}, e_2e_7, e_2e_{2i+8} for $i = 1, 2, \ldots, l-1$. Then

$$\begin{array}{c} \\ \hat{A}_{M,B,T} = \end{array} \begin{array}{c|ccccccccccc|} & e_4 & e_5 & e_6 & e_7 & e_8 & & e_{2i+7} & e_{2i+8} & & e_{2l+5} & e_{2l+6} \\ e_1 & 1 & 1 & 1 & 0 & 1 & \ldots & 1 & 0 & \ldots & 1 & 0 \\ e_2 & 1 & 1 & 0 & 1 & d_1 & \ldots & d_{i+1} & 1 & \ldots & d_l & 1 \\ e_3 & 1 & 0 & 1 & a_1 & c_1 & \ldots & a_{i+1} & c_{i+1} & \ldots & a_l & c_l \end{array}$$

Claim 4.1.1.1. $a_1 = c_1 = 1$.

Proof: $\det(A[\{1,2,3\}, \{e_1, e_4, e_7\}]) = 0$, so we have $\det(\hat{A}_{M,B,T}[B - e_1, \{e_4, e_7\}]) = a_1 - 1 = 0$, and therefore $a_1 = 1$. Similarly $\det(A[\{1,2,3\}, \{e_2, e_6, e_8\}]) = 0$, so $\det(\hat{A}_{M,B,T}[B - e_2, \{e_6, e_8\}] = c_i - 1 = 0$, showing that $c_i = 1$. □

Claim 4.1.1.2. $d_i = 2$ *for* $i = 1, 2, \ldots, l$.

Proof: For $i = 1, 2, \ldots, l-1$, $\det(A[\{1,2,3\}, e_3, e_8, e_{2i+7}]) = 0$, so $\det(\hat{A}_{M,B,T}[B - e_3, \{e_8, e_{2i+7}\}] = d_{i+1} - d_1 = 0$, which shows the pairwise equality of the d_i's. But $\det(A[\{1,2,3\}, \{e_5, e_7, e_8\}]) = 0$, so $\det(\hat{A}_{M,B,T}[B, \{e_5, e_7, e_8\}]) = 2 - d_1 = 0$, and $d_1 = 2$. □

Claim 4.1.1.3. $a_i = c_i$ *for* $i = 2, \ldots, l$.

Proof: For $i = 2, \ldots, l$, $\det(A[\{1,2,3\}, \{e_5, e_{2i+5}, e_{2i+6}\}]) = 0$, so $\det(\hat{A}_{M,B,T}[B, \{e_5, e_{2i+5}, e_{2i+6}\}]) = c_i - a_i = 0$, hence $c_i = a_i$. □

Claim 4.1.1.4. $a_i = b_i$ *for* $i = 2, \ldots, l$.

Proof: Recall that for $i = 1, \ldots, l-1$, $b_{i+1} = 2b_i$ or $b_{i+1} = 2b_i + 1$. If $b_{i+1} = 2b_i$, then $\det(A[\{1,2,3\}, \{e_1, e_{2i+6}, e_{2i+7}\}) = 2b_i - b_{i+1} = 0$. Then $\det(\hat{A}_{M,B,T}[B - e_1, \{e_{2i+6}, e_{2i+7}\}]) = a_{i+1} - 2a_i = 0$. Likewise, if $b_{i+1} = 2b_i + 1$, then $\det(A[\{1,2,3\}, \{e_6, e_{2i+6}, e_{2i+7}\}]) = b_{i+1} - 2b_i - 1 = 0$, so $\det(\hat{A}_{M,B,T}[B, \{e_6, e_{2i+6}, e_{2i+7}\}]) = a_{i+1} - 2a_i - 1 = 0$. To conclude the proof, it is enough to recall claim 4.1.1.1. □

Claim 4.1.1.5. $I_{M,B,T}$ *contains* (p).

Proof: Since $b_l = \frac{p+1}{2}$, $\det(A[\{1,2,3\}, \{e_1, e_8, e_{2l+6}\}) = p \equiv 0$, so $\det(\hat{A}_{M,B,T}[B - e_1, \{e_8, e_{2l+6}\}]) = p = 0$. □

4.2 Computation of the multiplicative group

We begin by recalling that the multiplicative group of the universal partial field is generated by $\{i_{B'} | B' \in \mathscr{B}\} \cup \{-1\}$. The $i_{B'}$s themselves can be calculated by using the polynomial $\det(\hat{A}_{M,B.T}[B \triangle Z])i_Z - 1$ for $Z \in \mathscr{B}$. Below we will highlight certain relations related to the multiplicative group G of our matroid. For $i = 1, \dots l-1$:

$$\det(A[\{1,2,3\},\{e_1,e_2,e_{2i+7}\}]) = b_{i+1} \implies b_{i+1} \in G; \tag{1}$$
$$\det(A[\{1,2,3\},\{e_5,e_6,e_{2i+7}\}]) = -b_{i+1} - 1 \implies b_{i+1} + 1 \in G; \tag{2}$$
$$\det(A[\{1,2,3\},\{e_2,e_4,e_{2i+7}\}]) = -b_{i+1} + 1 \implies b_{i+1} - 1 \in G. \tag{3}$$

And for $i = 2, \dots l-1$:

$$\det(A[\{1,2,3\},\{e_1,e_4,e_{2i+7}\}]) = b_{i+1} - 2 \implies b_{i+1} - 2 \in G; \tag{4}$$
$$\det(A[\{1,2,3\},\{e_1,e_7,e_{2i+7}\}]) = b_{i+1} - 3 \implies b_{i+1} - 3 \in G. \tag{5}$$

Notice that these relations always generate a unique element in G for $i = 2, \dots, l-1$. The same is not guaranteed for the following ones. For $i = 1, \dots l-3, j = i+2, \dots l-1$:

$$\det(A[\{1,2,3\},\{e_6,e_{2i+8},e_{2j+7}\}]) = b_{j+1} - 2b_{i+1} - 1 \implies b_{j+1} - 2b_{i+1} - 1 \in G; \tag{6}$$
$$\det(A[\{1,2,3\},\{e_5,e_{2i+8},e_{2j+7}\}]) = b_{j+1} - b_{i+1} \implies b_{j+1} - b_{i+1} \in G; \tag{7}$$
$$\det(A[\{1,2,3\},\{e_4,e_{2i+8},e_{2j+7}\}]) = b_{j+1} - b_{i+1} - 1 \implies b_{j+1} - b_{i+1} - 1 \in G. \tag{8}$$

Proposition 4.2.1. *[15, Corollary 1] At least one of 2, 3, or 5 is a primitive root modulo infinitely many primes p.*

This lets us state the following proposition:

Proposition 4.2.2. *$\mathbb{P}_M \cong \mathbb{F}_p$ for infinitely many primes p.*

Proof: By proposition 4.2.1 it is sufficient to show that $2, 3, 5 \in G$. To do this we will go through all possible values of b_2, b_3.

1. $b_2 = 2, b_3 = 4$.
   $3 \in G$ by (3), $5 \in G$ by (2).

2. $b_2 = 2, b_3 = 5$
   $3 \in G$ by (4).

3. $b_2 = 3, b_3 = 6$
   $2 \in G$ by (3), $5 \in G$ by (2).

4. $b_2 = 3, b_3 = 7$
   $2 \in G$ by (3), $5 \in G$ by (4).

□

In general, we would like to show that G always contains a primitive root, since then we could claim that the universal partial field of our matroid is always equal to $\mathbb{F}_p$. Unfortunately, I was unable to show that this is the case. In lieu of that I checked whether or not this is true for all primes smaller than 1000. First, I consulted the sequence A046145 in the OEIS [16] of smallest primitive roots. It quickly became apparent that for most of these primes their smallest primitive root was one of 2, 3, or 5. For the remaining primes, I wrote a computer program (see appendix A) to calculate the value of the b_is and used `https://www.wolframalpha.com/` to obtain a list of their primitive roots. By using the relations I established earlier, I then showed that at least one of their primitive roots is in G. See appendix B and table 1 for full details.

5 Conclusion

In this thesis we gave an introduction of representability theory of matroids, mainly through the lens of cross ratios. To properly talk about matroid representations, we introduced matroid cryptomorphisms, duals, and minors. After establishing some methods of interacting with matroids, we could finally talk about geometric representations of matroids and how they are related to cross ratios.

Our main focus was on matroids representable over finite fields. This motivated the introduction of the partial field. This algebraic structure was originally introduced to study matroids representable by a matrix, all of whose non-zero subdeterminants are constrained to some unit group. We could then talk about matrices and matroid being representable over a partial field. Progressing further required us to introduce minors, scaling equivalence, and cross ratios of $\mathbb{P}-$matrices. We could finally start discussing the relation between cross ratios and matroid representability.

The background section was closed out by the introduction of the universal partial field. Knowing the universal partial field of some matroid can let us state some results regarding its representability over other partial fields. We gave two ways of computing the universal partial field of a matroid.

In the result's section we introduced a matroid representable over $\mathbb{F}_p$ by a rank-three matrix with $2\lfloor \log_2(p+1) \rfloor + 6$ elements. Next, we computed the universal partial field of this matroid and concluded that it is always a sub-partial field of $\mathbb{F}_p$. While we did not show that if $\mathbb{P}_M = (\mathbb{F}_p, G)$, then G is isomorphic to $\mathbb{F}_p^*$, we did manage to show that there are infinitely many primes for which this is true. Additionally, we showed that this holds for all primes smaller than 1000.

5.1 Further research

It is clear that the matroid $M = M[A]$ could be studied a lot more. We did not prove that the multiplicative group G of the universal partial field $\mathbb{P}_M$ is always equal to $\mathbb{F}_p^*$. The most straightforward course of action is to simply keep doing computations for bigger and bigger primes. If there is a somewhat small counterexample, this might be very fruitful. There are other avenues of research, even if a counterexample is found. We could investigate the asymptotic behaviour of $\mathbb{P}_M$ and how it relates to the behaviour of prime generators, which is a deep area of research. It might also be interesting to see what happens when the prime has a specific form, for example Mersenne primes (which actually were somewhat addressed in [6]).

Part of my motivation for finding a smaller matrix, for which $\mathbb{P}_{M[A]} \cong \mathbb{F}_q$ is to help with the computation of another invariant - the foundation. While it has not been addressed in this theses, the foundation is also related to matroid representability and cross ratios. Some more information and research of foundations can be found in [17] [14]. From my brief experience with them, I got the impression that computing them is practically more difficult. For this reason, computing the foundation of $M[A]$ might be another avenue for further research.

A Code used to calculate b_is

```
import math
def findb(p):
  l = math.floor(math.log2(p+1))
  for j in range (2, l + 1):
    print(math.floor((p+1)/math.pow(2,l - j + 1)))
  return true
```

B Primitive roots of $\mathbb{F}_p$ in G for select primes

Table 1 consists of all primes smaller than 1000 whose smallest primitive root is not one of 2, 3, or 5. We denote such primes by p, then a_p denotes the primitive root we do show to be in G. We also indicate the relation used to show that it is in G, as well as the relevant equation with the b_is plugged in.

Table 1: Primes whose smallest primitive root is bigger than 5.

p	a_p	relation	equation
41	6	(2)	$b_3 + 1$
71	7	(4)	$b_4 - 2$
109	6	(1)	$b_3 = 6$
151	6	(5)	$b_4 - 3$
191	22	(4)	$b_5 - 2$
229	6	(3)	$b_3 - 1$
239	7	(1)	$b_3 = 7$
241	7	(1)	$b_3 = 7$
251	6	(3)	$b_3 - 1$
271	6	(4)	$b_4 - 2$
311	17	(4)	$b_5 - 2$
313	10	(2)	$b_4 + 1$
337	10	(1)	$b_4 = 10$
359	21	(3)	$b_5 - 1$
367	6	(3)	$b_3 + 1$
409	26	(2)	$b_5 + 1$
431	7	(2)	$b_3 + 1$
439	23	(8)	$b_5 - b_2 - 1 = 27 - 3 - 1$
457	13	(3)	$b_4 - 1$
479	13	(4)	$b_4 - 2$
499	7	(1)	$b_3 = 7$
599	7	(4)	$b_4 - 2$
601	7	(4)	$b_4 - 2$
643	11	(2)	$b_4 + 1$
719	11	(1)	$b_4 = 11$
733	6	(2)	$b_3 = 6$
761	6	(2)	$b_3 + 1$
769	11	(3)	$b_4 - 1$
839	11	(4)	$b_4 - 2$
911	29	(2)	$b_5 + 1$
919	7	(1)	$b_3 = 7$
971	6	(3)	$b_3 - 1$
991	6	(3)	$b_3 - 1$
997	7	(1)	$b_3 = 7$

References

[1] J. Richter-Gebert, *Perspectives on Projective Geometry.* Springer Berlin, Heidelberg, 2011.

[2] C. Semple and G. Whittle, "Partial fields and matroid representation.," *Advances in Applied Mathematics, 17*, pp. 184 – 208, 1996.

[3] R. A. Pendavingh and S. H. M. van Zwam, "Confinement of matroid representations to subsets of partial fields," *Journal of Combinatorial Theory, Series B*, vol. 100, p. 510–545, Nov. 2010.

[4] R. A. Pendavingh and S. H. M. van Zwam, "Representing some non-representable matroids," *Communications of The ACM - CACM*, June 2011.

[5] S. H. M. van Zwam, *Partial fields in matroid theory.* PhD thesis, Technische Universiteit Eindhoven, 2009.

[6] T. Brylawski, "Finite prime-field characteristic sets for planar configurations," *Linear Algebra and its applications 46*, pp. 155 – 176, 1982.

[7] R. A. Pendavingh and S. H. M. van Zwam, "Lifts of matroid representations over partial fields," *Journal of Combinatorial Theory, Series B*, vol. 100, p. 36–67, Jan. 2010.

[8] J. Oxley, *Matroid theory.* Oxford university press, 2011.

[9] R. van der Veen, "Geometry." `https://www.rolandvdv.nl/#teaching`, 2022.

[10] H. Whitney, "On the abstract properties of linear dependence," *American Journal of Mathematics, 57(3)*, pp. 509 – 533, 1935.

[11] G. Birkhoff, *Lattice theory, Third edition.* American Mathematical Society Colloquium Publications, Vol. XXV, American Mathematical Society, Providence, R.I., 1967.

[12] W. T. Tutte, "A homotopy theorem for matroid i, ii," *Transactions of the American Mathematical Society 88*, pp. 144 – 174, 1958.

[13] N. L. White, "The bracket ring of a combinatorial geometry. i," *Transactions of the American Mathematical Society*, pp. 79 – 95, 1975.

[14] M. Baker, O. Lorscheid, and T. Zhang, "Foundations of matroids – part 2: Further theory, examples, and computational methods," 2023.

[15] D. R. Heath-Brown, "Artin's conjecture for primitive roots," *The Quarterly Journal of Mathematics. 37*, pp. 27 – 38, 1986.

[16] E. W. Weisstein, "Smallest primitive root modulo n, or 0 if no root exists." `https://oeis.org/A046145`, 2005.

[17] M. Baker and O. Lorscheid, "Foundations of matroids i: Matroids without large uniform minors," 2020.