Realisation Spaces of Matroids

by

Megan Masters

MA4K9 Dissertation

Submitted to The University of Warwick

Mathematics Institute

April, 2022

Contents

1 Introduction

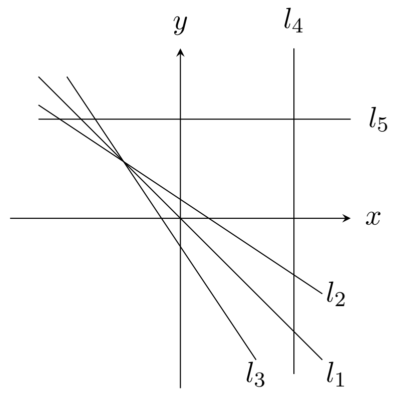
The universality theorem is a wide ranging theorem which encompasses aspects of topology, combinatorics and graph theory. It has many applications, including topics in algebraic geometry such as Murphy's law. There is a large amount of literature pertaining to the applications of the theorem, but the literature is lacking good examples of constructions. Therefore, this dissertation aims to fill that gap, and produce a concise and accessible proof, with examples throughout. We will define the concept of a matroid and see its wide ranging applications to mathematics. We will then define the constructions found within the universality theorem. Finally, we will prove the theorem, by combining our constructions.

A matroid is a set, where each subset is defined as either independent or dependent. This definition must satisfy the three rules:

1. The empty set is independent.
2. Any subset of an independent set is independent.
3. Given two independent sets A, B, with $|A| < |B|$, there is an element e of B, not in A, such that $A \cup e$ is also independent.

Firstly, we define a general matroid of lines in $\mathbb{P}^2$. We say that any two distinct lines in $\mathbb{P}^2$ form an independent set, and any 4 lines form a dependent set. Then three lines are dependent if and only if there is a point in $\mathbb{P}^2$ which lies on all three lines.

For instance, consider the matroid of five lines in $\mathbb{P}^2$, with exactly three lines meeting at a single point, shown here in the $z = 1$ plane.



This matroid has five elements, where any two elements are independent, and all but one triple of elements is also independent.

We will then introduce the concept of realisation spaces of matroids in $\mathbb{P}^2$. The realisation space of a matroid of lines in $\mathbb{P}^2$ tells us where we are allowed to move the lines whilst still achieving the same matroid structure.

Given a $3 \times n$ matrix which is rank 3, we form the corresponding matroid by creating n lines in $\mathbb{P}^2$, where each column of the matrix is the normal vector of a line. Now three lines in the matroid will meet at a single point, and will therefore be a dependent set, if and only if the corresponding 3×3 minor is zero. Given any matroid which can be represented as a set of lines in $\mathbb{P}^2$, we can calculate the set of all $3 \times n$ matrices which would produce the same matroid.

We note that given any matrix which represents a matroid, we can scale each column of the matrix by a non-zero scalar in a field K and achieve the exact same set of lines, as the normal vector to any line can always be scaled by a non-zero scalar. Also, we want to consider any two matrices which only differ by a change-of-basis, and so only differ by multiplication by an element of PGL_3, to be equivalent.

Therefore, the realisation space is then the set of matrices which will produce the same matroid structure, quotiented by PGL_3 and $(K^*)^n$.

For instance, the realisation space of the matroid above is the set of matrices of the form

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & a & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix},$$

with $a \in \mathbb{Z}$ non-zero.

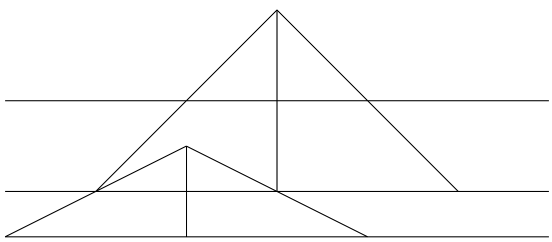
We will then introduce the universality theorem. Its statement is

Theorem. *[3, p.20] Consider a finitely generated $\mathbb{Z}$-algebra R. Then there exists a matroid M, whose realisation space $\mathbf{R}_M$ is an open subset of $\mathrm{Spec}(R) \times \mathbb{A}^N$, such that $\mathbf{R}_M$ projects surjectively onto $\mathrm{Spec}(R)$.*

To prove the theorem, we introduce the ideas of tensor products and the cross-ratio. We will then demonstrate that, for the atomic equations of multiplication, equality and addition, the universality theorem holds. We do this by creating explicit constructions of matroids with the required realisation spaces. For instance, the ring

$$\mathbb{Z}[x_1, x_2, x_3]/(x_1x_2 - x_3),$$

which corresponds to the atomic equation of multiplication, is constructed by creating the matroid in $\mathbb{P}^2$ of 9 lines:



After demonstrating that the theorem is true for the atomic equations, we combine the atomic equations to create more complicated examples.

We finish the proof of the universality theorem by producing step by step instructions for generating any finitely generated $\mathbb{Z}$-algebra R. The steps are:

1. Write the finitely generated $\mathbb{Z}$-algebra R as the quotient of a polynomial ring by an ideal.
2. Write the ideal as the generating set of a finite number of polynomials.
3. Construct the generating set as the combination of atomic equations.
4. Identify free variables.
5. Reorder the other variables.
6. Construct the variables as points on lines in $\mathbb{P}^2$ by using the atomic constructions.

We then calculate the realisation space of this matroid, calculating the polynomials which are forced to be non-zero. The product of these polynomials, D, gives us the open set $\{D \neq 0\}$ which is the realisation space of the matroid lying within $\text{Spec}(R) \times \mathbb{A}^n$. To make sure this set maps surjectively to $\text{Spec}(R)$, we map the free variables y_i to some other variables x_i with $x_i = y_i + t$. Then as D is finite, we choose t such that $D \neq 0$ and so we generate a map from $\{D \neq 0\}$ to $\text{Spec}(R)$.

In Section 2, we define the general theory of matroids, and introduce the concept of matroids in $\mathbb{P}^2$. Then in Section 3, we introduce realisation spaces of matroids in $\mathbb{P}^2$, and calculate the realisation space of some matroids. Next, in Section 4, we state the universality theorem and show that any polynomial can be written as the combination of atomic equations. Then, in Sections 5 and 6, we define tensor products and the cross-ratio, tools which we will use in our proof of the theorem. In Section 7, we show that the universality theorem holds for the atomic equations. Finally, in Section 8, we demonstrate how to combine the atomic equations to form any finitely generated $\mathbb{Z}$-algebra we want, proving the theorem.

2 Matroids

In this section, we will define the concept of matroids. First, we will define them through the idea of independent sets, and consider bases of a matroid. Then we will look at dependent sets of a matroid, and there we will consider circuits of a matroid. We will see that all these concepts are equivalent to each other.

Then, once we have defined matroids, we will see some of their wide-ranging applications in mathematics. We will see how the concept of matroids appears in both graph theory and combinatorics, and how we can apply the general theorems of matroids to many different mathematical topics.

2.1 Linear independence and matroids

Linear independence is a measure of how related vectors are to each other. A set of vectors is linearly independent if no vector can be made by a linear combination of the other vectors in the set.

Matroids form a generalisation of linear independence, which allows ideas from algebra to be applied to other areas of mathematics. There are many equivalent definitions of a matroid. One way to define a matroid is in terms of independent sets.

Definition 2.1. [8, p.7] A *finite matroid* is a finite set E along with a family I of subsets of E, called independent sets, which satisfy

(I1) The empty set is independent; and

(I2) a subset of an independent set is independent; and

(I3) if A and B are independent sets, and $|A| < |B|$, then there is an element e of $B - A$ such that $A \cup e$ is independent.

Consider a finite set E of vectors in a vector space V. We define the set I to be the subsets of E which are linearly independent. It is clear that the set E, together with the family of subsets I, satisfies (I1) and (I2). So to show that this forms a matroid we only have to show that (I3) is satisfied.

Lemma 2.2. *[2, p.2] A finite set of vectors, together with the family of linearly independent subsets, forms a matroid.*

Proof. Suppose that (I3) does not hold. Then there exists linearly independent sets $A = \{a_1, ..., a_i\}$ and $B = \{b_1, ..., b_j\}$ such that $i < j$, but for all $b_t \in B - A$, $A \cup b_t$ is not independent. This means that each b_t is a linear combination of $\{a_1, ..., a_i\}$. Now also every $b_t \in B \cap A$ is a linear combination of $\{a_1, ..., a_i\}$, as it is equal to one of $\{a_1, ..., a_i\}$. So we must have that $\text{Span}(B) \subset \text{Span}(A)$. But then $j = \dim(\text{Span}(B)) \leq \dim(\text{Span}(A)) = i$, which is a contradiction. Hence, there is a $b_t \in B \cap A$ which is not a linear combination of elements of A. Therefore, the set $A \cup \{b_t\}$ is linearly independent. $\square$

Example 2.3. Consider the matrix

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

Now number each column 1 to 5. Then the set $E = \{1, 2, 3, 4, 5\}$, together with the set $I = \{\emptyset, \{1\}, \{3\}, \{4\}, \{5\}, \{1, 3\}, \{1, 4\}, \{1, 5\}, \{3, 4\}, \{3, 5\}\}$, is a matroid.

2.2 Bases of matroids

The second definition of matroids comes from the concept of bases of vector spaces. In linear algebra, a basis of a set E of vectors is an independent subset which spans E.

Lemma 2.4. *A subset B of a set of vectors E over a field K is a basis if and only if it is maximally linearly independent. That is, it is a linearly independent subset of vectors which becomes dependent when you add any other vector.*

Proof. First assume that B is a basis of E. Then by definition, B must be a linearly independent set. So we only need to show that B is maximally linearly independent. But any $v \in E - B$, as B spans E, is a linear combination of elements of B. Hence, $B \cup v$ is linearly dependent. So B must be maximally linearly independent.

Now assume that B is maximally linearly independent. Then trivially it is independent. So we must only show that it spans E. Now for any $v \in B$, clearly $v \in Span(B)$. Also for any $v \in E - B$, $B \cup v$ must be linearly dependent. So $k_v v - \sum_{i=1}^{n} k_i b_i = 0$, for some $k_1, ..., k_n, k_v \in K$ not all zero, and some $b_1, ..., b_n \in B$. Then $k_v \neq 0$, otherwise B would be a linearly dependent set, and so $v = 1/k_v \sum_{i=1}^{n} k_i b_i$. Therefore, v is in $Span(B)$, and so B spans the whole of E. Hence, B is a basis of E. □

We can then extend this definition to an arbitrary finite matroid.

Definition 2.5. [8, p.15] Let $M = (E, I)$ be a matroid. Then a *basis* of M is a subset of E which is maximally independent. That is, it is an independent set which becomes dependent by adding any other element to the set.

Example 2.6. Consider the matroid from Example 2.3. Then the bases of this matroid are $\{1,3\}, \{1,4\}, \{1,5\}, \{3,4\}$ and $\{3,5\}$.

We can define a matroid in terms of its bases, and this definition is entirely equivalent to (I1)-(I3). A proof of this can be found in Oxley [8, pp.15-17].

Proposition 2.7. *A set $\mathcal{B}$ is the collection of bases for a matroid if and only if the following hold:*

(B1) The set $\mathcal{B}$ is non-empty.

(B2) If $B_1, B_2 \in \mathcal{B}$, and $x \in B_1 - B_2$, we can find $y \in B_2 - B_1$ such that $(B_1 - x) \cup y$ is also an element of $\mathcal{B}$.

Any basis of a vector space has the same number of vectors, so it is logical to also require this condition to hold for an arbitrary finite matroid.

Lemma 2.8. *[8, p.16] All bases of a matroid have the same size.*

Proof. Let $\mathcal{B}$ be the set of bases for a matroid E. Let $B_1, B_2 \in \mathcal{B}$ be two distinct elements such that $|B_1| > |B_2|$ and $|B_1 - B_2|$ is minimal over all pairs of elements in $\mathcal{B}$. Now by definition, B_1 and B_2 are independent sets, so by (I3), there is an element $x \in B_1 - B_2$ such that $B_2 \cup x$ is independent. But this contradicts B_2 being a maximally independent set.

Therefore, there can be no elements B_1, B_2 of $\mathcal{B}$ with $|B_1| > |B_2|$. Hence, all elements of $\mathcal{B}$ have equal size. □

2.3 Circuits

We have seen that matroids can be defined using both independent sets and bases. For vector spaces we define dependent sets as exactly the sets which are not linearly independent. This definition can be extended to an arbitrary matroid.

We define a dependent set of a matroid (E, I) as a set which is not in I.

Definition 2.9. [8, p.8] A *circuit* in a matroid $M = (E, I)$ is a minimally dependent subset of E. That is, it is a dependent set, which becomes independent after removing any one element.

Example 2.10. Consider the same matroid from Example 2.3. Then the minimally dependent sets, or circuits, are $\{2\}, \{4, 5\}, \{1, 3, 4\}$ and $\{1, 3, 5\}$.

Circuits are a very useful tool in matroid theory as it is often easier to specify a matroid in terms of its minimally dependent sets. In fact, the independent set axioms (I1)-(I3) are entirely equivalent to a similar set of axioms on the circuits of a matroid, a proof of which can be found in Oxley [8, pp.8-11].

Proposition 2.11. *A set $\mathcal{C}$ is the collection of circuits for a matroid if and only if the following hold:*

(C1) The set $\emptyset \notin \mathcal{C}$.

(C2) If $C_1, C_2 \in \mathcal{C}$ and $C_1 \subseteq C_2$, then $C_1 = C_2$.

(C3) If $C_1, C_2 \in \mathcal{C}$ are distinct and $e \in C_1 \cap C_2$, then there exists $C_3 \in \mathcal{C}$ such that $C_3 \subseteq (C_1 \cup C_2) - e$.

2.4 Graph theory

An example of a matroid outside algebra can be found in graph theory.

Definition 2.12. A *cycle* in a graph is a non-empty set of distinct edges $\{e_1 = u_1v_1, ..., e_n = u_nv_n\}$ such that $v_i = u_{i+1}$ for $i \in \{1, ...n - 1\}$ and $u_1 = v_n$.

Given any graph, we let the set E be the edges of the graph, and the independent sets be the subsets of edges which form forests. These are graphs that do not contain a cycle as a subgraph.

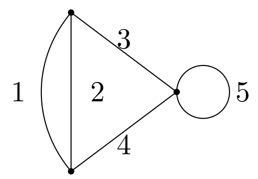
Lemma 2.13. *[8, pp.10-11] Given any finite graph G, consider the set of edges of the graph. Then the subsets of edges which are forests form the independent sets of a matroid.*

Proof. We will use the circuits definition (Proposition 2.11) to prove this lemma. Let $\mathcal{C}$ be the set of subsets of edges which are cycles. We claim that $\mathcal{C}$ is the set of circuits of a matroid. Firstly, (C1) is satisfied as the empty set of edges is not a cycle.

Now, (C2) is satisfied as there is no proper subgraph of a cycle which is also a cycle.

So it remains to show that (C3) is satisfied. Let $C_1, C_2 \in \mathcal{C}$ be two distinct cycles with a shared edge e. Let $e = uv$, where u and v are vertices of the graph. Our aim is to form a cycle in G completely contained within $(C_1 \cup C_2) - e$. As C_1 is a cycle, there is a path P_1 from u to v in $C_1 - e$. Similarly, there is a path P_2 from u to v in $C_2 - e$. Now start at u, and traverse P_1. Let w be the first vertex of P_1 such that the next edge is not in P_2. Now let x be the first vertex after w contained in P_2. Now the section of P_1 from x to w contains no edges from P_2. Hence, there is a cycle created from joining the section of P_1 from x to w, going in the opposite direction, together with the section of P_2 from w to x. This clearly does not contain e and is contained in $C_1 \cup C_2$. Therefore, (C3) is satisfied. $\square$

Example 2.14. [8, p.11]



Consider the graph above. Then this forms a matroid with $E = \{1, 2, 3, 4, 5\}$ and circuits $\{5\}, \{1, 2\}, \{1, 3, 4\}$ and $\{2, 3, 4\}$.

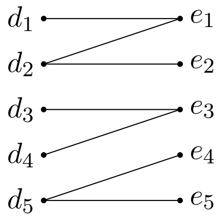
2.5 Combinatorics

We also find an application of matroid theory within combinatorics. We consider the matching problem.

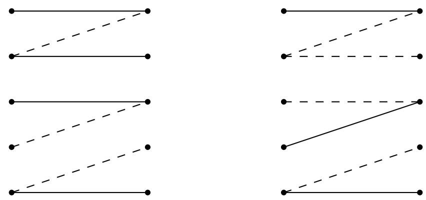
Definition 2.15. Given two sets D and E, and a collection $T \subseteq \{(u, v) : u \in D, v \in E\}$, a *matching* is a subset M of T where each element $u \in D$ and each element $v \in E$ appears in at most one pair of M.

We can represent this structure in terms of a bipartite graph $G = (V, D \cup E)$, where the vertices are the two sets D and E, and there is an edge between two vertices u and v if and only if $(u, v) \in T$. With this representation, a matching is a subgraph where each vertex has degree at most 1.

Example 2.16. Consider the two sets $D = \{d_1, d_2, d_3, d_4, d_5\}$ and $E = \{e_1, e_2, e_3, e_4, e_5\}$, and a collection $T = \{(d_1, e_1), (d_2, e_1), (d_2, e_2), (d_3, e_3), (d_4, e_3), (d_5, e_4), (d_5, e_5)\}$. The graphical representation of this is



Two possible matchings are



Now we can consider all the subsets of E that appear in a matching with D.

Example 2.17. Consider the sets in Example 2.13. Then subsets of E which appear in a matching are

$$\{\emptyset, \{e_1\}, \{e_2\}, \{e_3\}, \{e_4\}, \{e_5\}, \{e_1, e_2\}, \{e_1, e_3\}, \{e_1, e_4\}, \{e_1, e_5\}, \{e_2, e_3\}, \{e_2, e_4\},$$

$$\{e_2, e_5\}, \{e_3, e_4\}, \{e_3, e_5\}, \{e_1, e_2, e_3\}, \{e_1, e_2, e_4\}, \{e_1, e_2, e_5\}, \{e_1, e_3, e_4\}, \{e_1, e_3, e_5\},$$

$$\{e_2, e_3, e_4\}, \{e_2, e_3, e_5\}, \{e_1, e_2, e_3, e_4\}, \{e_1, e_2, e_3, e_5\}\}.$$

Lemma 2.18. *[1, p.4] Given a bipartite graph with bipartition (D,E), the family of subsets of E which can be matched to D form the independent sets of a matroid.*

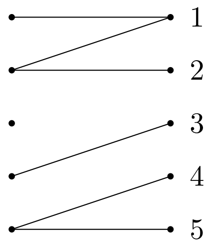
Proof. We use the independent sets definition (Proposition 2.7) to prove this lemma. Let I be the set of subsets of E which are contained in a matching. First we consider the condition (I1). A valid matching of a bipartite graph is to take the empty set of edges. This corresponds to the empty subset of E. So the empty set is independent.

Now we prove (I2). Any subset of a matching is also a matching. Therefore, any subset of an independent set is contained in a matching, and so must be independent.

Finally we prove (I3). Assume for a contradiction that $A, B \in I$ such that $|A| < |B|$. Let M be a matching corresponding to A, and let N be a matching corresponding to B. Both M and N must exist as, by definition, A and B are independent so are covered by a matching. Now any vertex has degree at most 1 in M, and at most 1 in N. So a vertex has degree at most 2 in $M \cup N$. Therefore, any non-trivial connected component of $M \cup N$ must be either a path or an even cycle, both with alternating edges from M and N. Now each edge in M corresponds to exactly one element to A, and each edge in N corresponds to exactly one edge to B. So the assumption that $|A| < |B|$ implies that there are fewer edges in M than N. Hence, there must be at least one non-trivial connected component with more edges from N than M, and this must be a path P, with start vertex v in B but not A.

We claim that $A \cup v$ is also an independent set. So we are claiming that there is a collection of edges which form a matching and which cover all of $A \cup v$. To construct this matching, we take the edges of P which are within N. This will cover v and some of A. We then take all other elements of M which are not in P. This will cover the rest of A. Now this forms a matching as the elements of P which are within N form a matching, as does the elements of M which are not in P, as they are subsets of matchings. Then their union is a matching as these two sets of edges share no common vertices, by construction of P. Therefore, $A \cup v$ is an independent set, and so (I3) is satisfied. □

Example 2.19. Consider the bipartite graph



Then the set $E = \{1, 2, 3, 4, 5\}$, together with the bases $\{1, 2, 3, 4\}$ and $\{1, 2, 3, 5\}$ form a matroid.

2.6 Matroids constructed in $\mathbb{P}^2$

From this point on, we will be focusing on matroids in $\mathbb{P}^2$. To form a matroid in $\mathbb{P}^2$, we fix a set of lines in $\mathbb{P}^2$. We then define all distinct pairs of lines as independent, and all sets of four lines as dependent. Then we say that a set of three lines is dependent if and only if there is a point in $\mathbb{P}^2$ which lies on all three lines.

We can represent a line of $\mathbb{P}^2$ by stating its normal vector as an element of $\mathbb{P}^2$. In this way, there is a bijective map between points and lines in $\mathbb{P}^2$. For instance, the point $[a : b : c]$ has corresponding line

$$ax + by + cz = 0.$$

Lemma 2.20. *Three lines in $\mathbb{P}^2$ meet at a single point if and only if their normal vectors are linearly dependent.*

Proof. Consider three lines

$$l_1 : a_1x + b_1y + c_1z = 0$$
$$l_1 : a_2x + b_2y + c_2z = 0$$
$$l_1 : a_3x + b_3y + c_3z = 0$$

in $\mathbb{P}^2$ Then these three lines meet at a single point if and only if these three simultaneous equations have a non-zero solution. This is exactly if and only if the matrix

$$\begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{pmatrix}$$

is not invertible. Now this is exactly the situation that the vectors (a_1, b_1, c_1), (a_2, b_2, c_2), and (a_3, b_3, c_3) are linearly dependent. But these are just the normal vectors to the three lines. □

Now we are able to show that lines in $\mathbb{P}^2$ form a matroid.

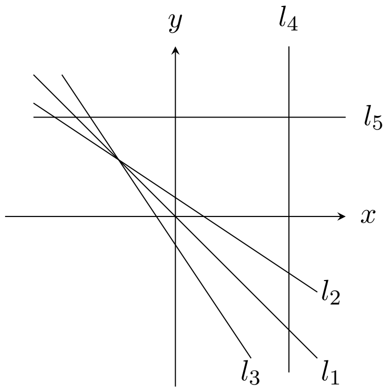
Lemma 2.21. *A set of lines in $\mathbb{P}^2$, with independent sets defined above, form a matroid.*

Proof. Consider three lines in $\mathbb{P}^2$. Then these lines meet at a point in $\mathbb{P}^2$ if and only if their normal vectors are linearly dependent. Therefore, given any set of lines in $\mathbb{P}^2$, we can map to vectors in $\mathbb{A}^3$ by sending each line to its normal vector. Then this forms a matroid by our previous discussion, with each two distinct vectors being independent, all sets of four vectors being dependent, and a set of three vectors being independent if and only if they are linearly independent. Therefore, this mapping exactly preserves the independent sets. Therefore, as this is a matroid, the original set of lines in $\mathbb{P}^2$ must also form a matroid. □

Example 2.22. Consider the five lines

$$l_1 : x + y = 0,$$
$$l_2 : 2x + 3y = z,$$
$$l_3 : 3x + 2y = -z,$$
$$l_4 : x = 2z,$$
$$l_5 : y = 4z.$$

We can view these lines on the $z = 1$ plane:



We can see that lines l_1, l_2, and l_3 meet at one point : $[-1 : 1 : 1]$. The normal vectors of these three lines are $(1, 1, 0)$, $(2, 3, -1)$, and $(3, 2, 1)$. Indeed, these vectors are linearly dependent.

No other triple of lines meet at a single point. Therefore, this is the matroid of 5 lines, with all but one triple of lines defined as independent.

We can represent these five lines as a 3×5 matrix, where column i is the normal vector of line l_i.

$$\begin{pmatrix} 1 & 2 & 3 & 1 & 0 \\ 1 & 3 & 2 & 0 & 1 \\ 0 & -1 & 1 & -2 & -4 \end{pmatrix}.$$

Now the information that the first three lines are dependent is encoded in the fact that the determinant of first three columns of this matrix is zero. Also, the information that no other triple of lines is dependent is encoded in the fact that no other 3×3 minor is zero.

3 Realisation Spaces

We have seen that for any matroid which is formed by n lines in $\mathbb{P}^2$, we can represent it as a $3 \times n$ matrix, where each column is the normal vector of one of the lines.

The only important information from the lines are the intersections. We can move the lines carefully and we would still achieve the same matroid.

Definition 3.1. [6, p.44] Let M be a matroid which can be realised as lines in $\mathbb{P}^2$. A set of lines in $\mathbb{P}^2$ represents the matroid M if there is a bijection between the set of elements of M and the set of lines, which exactly preserves the independent sets. Now define Γ_M to be the set of $3 \times n$ matrices such that $A \in \Gamma_M$ if and only if the matroid of lines in $\mathbb{P}^2$, whose normal vectors are the columns of A, represents the matroid M.

Example 3.2. Consider the matroid from Example 2.22. Then the matrix

$$\begin{pmatrix} 1 & 1 & 2 & 1 & 0 \\ 2 & 3 & 5 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

also represents a matroid with three lines intersecting at a single point. In fact, if M is the matroid with five elements, any two of which are independent, all but one triple of elements is independent, and any set of 4 elements is dependent, then Γ_M is exactly the set of 3×5 matrices with exactly one zero minor. We require exactly one minor to be zero ensure that there is exactly one triple of lines which is dependent. Enforcing that only one minor can be zero also ensures that we cannot have zero columns, which does not define a line in $\mathbb{P}^2$. Finally, this criterion also enforces that no two columns are a multiple of each other. If a column was a multiple of another, this would define the same line and hence there would be a pair of elements in the matroid which were dependent.

The first important concept to notice is that if we scale the normal vector of a line by any non-zero value, we will have the same line that we started with. Therefore, we want to identify the elements of Γ_M that only differ by multiplying each column by some non-zero scalar in our scalar field K. This is achieved by taking the quotient of Γ_M by $(K^*)^n$, viewing $(K^*)^n$ as $n \times n$ diagonal matrices acting on Γ_M by right multiplication.

The second important concept is the fact that changing the basis of our space produces an isomorphic picture. We want to consider any two constructions which only differ by a change of basis as equivalent elements. This is exactly equivalent to applying an element of the group PGL_3 to the given $3 \times n$ matrix. So we also want to quotient Γ_M by PGL_3, where PGL_3 acts on Γ_M by left multiplication.

Definition 3.3. [6, p.44] By applying both of these concepts, we arrive at the set

$$\mathbf{R}_M = \Gamma_M / (\mathrm{PGL}_3 \times (K^*)^n),$$

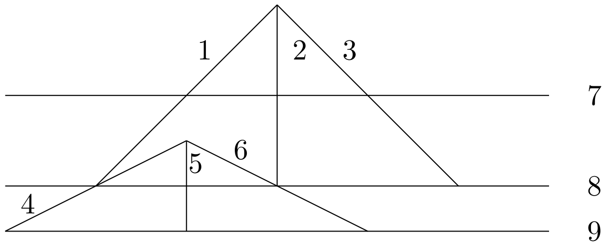
which we call the *realisation space* of our matroid.

Example 3.4. Again, consider the example of 5 lines where exactly one triple of lines is dependent, from Example 2.22. We have seen that Γ_M is the set of 3×5 matrices with exactly one zero minor. Then we note that the set $\{l_1, l_2, l_4, l_5\}$ forms a circuit of the matroid. So by a change of basis, we can map the first, second, and third lines to lines $(1, 0, 0)$, $(0, 1, 0)$ and $(0, 0, 1)$ respectively, and also send the fourth line to $(1, 1, 1)$. This will send the third vector to $(b, c, 0)$ for some non-zero values b and c. Finally, we note that we can scale the third vector by $1/b$. Therefore we are left with the set of matrices of the form

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & a & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix},$$

where a is a non-zero scalar. This is the realisation space corresponding to the matroid M.

Example 3.5. Now let us calculate the realisation space of a more complicated matroid.



Here we have 9 lines in $\mathbb{P}^2$ shown in the $z = 1$ plane. This represents a matroid M where $E = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$, with dependent sets $\{1, 2, 3\}$, $\{4, 5, 6\}$, $\{1, 4, 8\}$, $\{2, 6, 8\}$,$\{7, 8, 9\}$, and any set with 4 or more elements. We note that the set of lines $\{7, 8, 9\}$ is dependent, but within this picture do not appear to meet at one point, as they meet at a point where $z = 0$. Therefore, this point is not represented in the picture.

Given the matrix representing the arrangement of these lines, using our maps in PGL_3, we can chose any four columns corresponding to 4 lines which form a circuit, and map them to $(1, 0, 0), (0, 1, 0), (0, 0, 1)$ and $(1, 1, 1)$. So we choose to map columns 1, 2 and 7 to the identity matrix, and column 4 to the vector $(1, 1, 1)$. Now we need the 3×3 minor of the first three columns to be zero. This will ensure that lines 1, 2 and 3 are dependent. So we map column 3 to $(1, a, 0)$, remembering that we can always make the first non-zero entry be 1.

Now we also require columns 1, 4 and 8 to be linearly dependent, as the lines $\{1, 4, 8\}$ form a dependent set. So we send column 8 to $(1, d, d)$. Then lines $\{2, 6, 8\}$ also form a dependent set, so to enforce this we send column 6 to $(1, c, d)$. Again, the lines $\{7, 8, 9\}$ form a dependent set, so we send column 9 to $(1, d, f)$.

Lastly we need to enforce that the columns 4, 5 and 6 are linearly dependent. So we require the 3×3 minor created from columns $\{4, 5, 6\}$ to be zero. So we arrive at the matrix

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & a & 1 & b & c & 0 & d & d \\ 0 & 0 & 0 & 1 & e & d & 1 & d & f \end{pmatrix},$$

where we impose the extra condition that

$$\det \begin{pmatrix} 1 & 1 & 1 \\ 1 & b & c \\ 1 & e & d \end{pmatrix} = 0,$$

and hence,

$$bd - ce - d + c + e - b = 0.$$

We also need to impose that no minors except $\{1,2,3\}, \{4,5,6\}, \{1,4,8\}, \{2,6,8\}$ are zero. For instance,

$$\det \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & d \\ 0 & 1 & d \end{pmatrix} \neq 0,$$

which enforces that the set $\{2,4,8\}$ is independent, and so we require $d \neq 1$.

Forcing these minors to be non-zero, we find that we require none of a, b, c, d, e, f to be zero or one. We also require all of

$$\{a-b, a-c, a-d, b-c, b-d, b-e, c-d, d-e, d-f, e-f, cf-d^2, bd-ce, bf-de,$$

$$a-ae-b+e, a-ad-c+d, a-af-d+f, bd-ad+ae-ce, bd-ad+ae-de,$$

$$ae-de-af+bf, ad-d^2-af+cf, bf-de-b+d+e-f, cf-d^2-c+2d-f,$$

$$bd-d^2-ce+de-bf+cf, bd-ce-b+c-d+e\}$$

to be non-zero.

4 The Universality Theorem

The idea behind the universality theorem is that you can take any finitely generated $\mathbb{Z}$-algebra and find a matroid whose realisation space is an open subset of the spectrum of this ring, with some extra variables added. The main part of this project is to prove the universality theorem, and in this section we state the theorem, and start to introduce the main ingredients of the proof of the theorem.

4.1 Statement of theorem

The statement of the theorem is as follows, as written in Cartwright [3, p.20]:

Theorem 4.1. *[3, p.20] Consider a finitely generated $\mathbb{Z}$-algebra R. Then there exists a matroid M, whose realisation space $\mathbf{R}_M$ is an open subset of $\operatorname{Spec}(R) \times \mathbb{A}^N$, such that $\mathbf{R}_M$ projects surjectively onto $\operatorname{Spec}(R)$.*

4.2 Reducing to atomic equations

Our first step in the proof of the universality theorem is to reduce all equations down to atomic equations. Our first atomic equation is the equality of two variables, $x_i = x_j$. Then our second is addition of two distinct variables to equal a third variable, $x_i + x_j = x_k$. Finally our third equation is multiplication of two distinct variables to equal a third variable, $x_i x_j = x_k$.

Theorem 4.2. *[3, p.19] Every ideal in $\mathbb{Z}[x_1, ..., x_n]$ can be written as the ideal of a set of atomic equations.*

Every ideal is a set of polynomials, so we only need to demonstrate that the theorem holds for principally generated ideals. So therefore, we need to show that any polynomial in $\mathbb{Z}[x_1, ..., x_n]$ can be written as a sequence of atomic equations. This is best illustrated with an example. A general proof of the theorem can be found in Cartwright [3, p.19].

Example 4.3. [7, p.5] Consider the polynomial equation $x_1x_2 + {x_3}^2 - 2 = 0$. First, we define a new variable $x_4 = x_1x_2$, which is the atomic equation of multiplication. Now we note that our atomic equations do not allow us to multiply an element with itself. So we create a new variable $x_5 = x_3$, which is the atomic equation of equality. Now we can create the term ${x_3}^2$ by setting $x_6 = x_3x_5$. We now want to create the polynomial $x_1x_2 + {x_3}^2$, so we let $x_7 = x_4 + x_6$. This is the atomic equation of addition.

We now need to create the value -2. We do this by letting $x_8 = 1$ and $x_9 = 1$, which are two examples of the atomic equation of equality. We then construct 2 by letting $x_{10} = x_8 + x_9$. Finally, we force $x_7 = x_{10}$. Let

$$I = (x_4 - x_1x_2, x_5 - x_3, x_6 - x_3x_5, x_7 - x_4 - x_6, x_8 - 1, x_9 - 1, x_{10} - x_8 - x_9, x_7 - x_{10}).$$

This is the ideal generated by all the relations we have defined. We now arrive at an isomorphism of rings

$$\frac{\mathbb{Z}[x_1, x_2, x_3]}{(x_1x_2 + {x_3}^2 - 2)} \cong \frac{\mathbb{Z}[x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}]}{I}.$$

4.3 Spectrum of a ring

The Universality theorem refers to an open set of $\mathrm{Spec}(R) \times \mathbb{A}^n$. To understand this, we first need to define $\mathrm{Spec}(R)$, and then define the open sets within $\mathrm{Spec}(R)$.

Definition 4.4. Consider a ring R. The *spectrum* of R, denoted by $\mathrm{Spec}(R)$, is the set of prime ideals of R.

Definition 4.5. A *closed set* X of $\mathrm{Spec}(R)$ is a set of prime ideals such that there is an ideal I of R with $X = \{J \in Spec(R) : I \subset J\}$.

Example 4.6. The closed set of $\mathrm{Spec}(\mathbb{C}[x,y])$ corresponding to the ideal $I = (x^2)$ is the set

$$X = \{(x)\} \cup \{(x, y-a) : a \in \mathbb{C}\}.$$

Definition 4.7. A set X in $\mathrm{Spec}(R)$ is *open* if $\mathrm{Spec}(R) - X$ is closed.

5 Aside on Tensor Products

In our statement of the universality theorem, we want to find a matroid whose realisation space is an open subset of $\mathrm{Spec}(X) \times \mathbb{A}^n$. To make sense of this space, we need to consider the tensor product of two modules.

Definition 5.1. [4, pp.63-64] Consider two modules R and S. The *tensor product* of R and S over a field K, denoted by $R \otimes S$, is the set of linear combinations of elements of the form $r \otimes s$, where $r \in R$ and $s \in S$, modulo the relations that, for all $k \in K$, $r, r' \in R$ and $s, s' \in S$,

$$kr \otimes s = r \otimes ks,$$
$$(r + r') \otimes s = r \otimes s + r' \otimes s,$$
$$r \otimes (s + s') = r \otimes s + r \otimes s'.$$

For our proof of the universality theorem, we require the following theorem. A discussion of tensor products of $\mathbb{Z}$-algebras, and the proof of the theorem, can be found in Shinder [9, pp.4-6].

Theorem 5.2. *Let I be an ideal in $\mathbb{Z}[x_1, ..., x_n]$. Let $J = I\mathbb{Z}[x_1, ..., x_n, y_1, ..., y_m]$. Then*

$$\frac{\mathbb{Z}[x_1, ..., x_n, y_1, ..., y_m]}{J} \cong \frac{\mathbb{Z}[x_1, ..., x_n]}{I} \otimes \mathbb{Z}[y_1, ..., y_m].$$

Example 5.3. Considering the ring

$$\frac{\mathbb{Z}[x_1, x_2, x_3, a, e, f]}{(x_1x_2 - x_3)},$$

using the theorem above, we note the ideal $(x_1x_2 - x_3)$ only contains elements in $\mathbb{Z}[x_1, x_2, x_3]$. So we have that

$$\frac{\mathbb{Z}[x_1, x_2, x_3, a, e, f]}{(x_1x_2 - x_3)} \cong \frac{\mathbb{Z}[x_1, x_2, x_3]}{(x_1x_2 - x_3)} \otimes \mathbb{Z}[a, e, f].$$

The key point for our uses is the following theorem, a discussion of which can be found in Eisenbud and Harris [5, pp.35-37].

Theorem 5.4. *If X has coordinate ring R, and Y has coordinate ring S, then $X \times Y$ has coordinate ring $R \otimes S$.*

Specifically for our uses, we will be using statements like

$$\operatorname{Spec}\left(\frac{\mathbb{Z}[x_1, x_2, a, e, f]}{(x_1x_2 - x_3)}\right) \cong \operatorname{Spec}\left(\frac{\mathbb{Z}[x_1, x_2, x_3]}{(x_1x_2 - x_3)}\right) \times \operatorname{Spec}(\mathbb{Z}[a, e, f]).$$

6 The Cross-Ratio

A very important tool when working with realisation spaces is the cross-ratio.

Definition 6.1. The *cross-ratio* of 4 pairwise distinct values $a, b, c, d \in \mathbb{C}$ is

$$(a, b; c, d) = \frac{(a-b)(c-d)}{(a-c)(b-d)}.$$

Now consider 4 distinct points P_1, P_2, P_3, P_4 in $\mathbb{P}^1$. First consider the case that none of the four points are $[0:1]$. All four points can be written as $[1:z_i]$.

We want to send $[1:z_1]$ to $[1:0]$, $[1:z_3]$ to $[1:1]$, and $[1:z_4]$ to $[0:1]$, which is the point at infinity in $\mathbb{P}^1$. We then want to calculate where $[1:z_2]$ is sent under this map. We do this by using the cross-ratio.

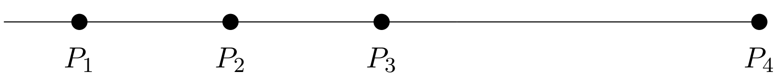
The image of P_2 under the map is exactly

$$[1 : (z_1, z_2; z_3, z_4)].$$

Now let us consider the case that one of the coordinates is $[0:1]$. In this case we remove any brackets with the corresponding term in the cross-ratio. For instance, if P_4 has coordinates $[0:1]$, then the image of P_2 under the map is

$$\left[1 : \frac{(z_1 - z_2)}{(z_1 - z_3)}\right].$$

Now for our purposes, we will be using the cross-ratio on 4 points in $\mathbb{P}^2$ lying on a line.



Our first step is to map the line and each point onto $\mathbb{P}^1$. We can choose any linear map. For our purposes, we do this by mapping to the first two coordinates, unless one of our points is $[0:0:1]$, in which case we map to the last two coordinates. We will never have the case that two of our points are $[0:0:1]$ and $[1:0:0]$, and so we will never have the problem that our projection is undefined. We then apply the cross-ratio to the mapped points in $\mathbb{P}^1$.

Example 6.2. Consider the points $P_1 = [1 : 1 : 2], P_2 = [1 : -1 : 0], P_3 = [1 : 2 : 3]$ and $P_4 = [1 : -2 : -1]$. All four of these points lie on the line

$$x + y = z.$$

Now these points map to $[1 : 1], [1 : -1], [1 : 2]$ and $[1 : -2]$. So we have

$$z_1 = 1, z_2 = -1, z_3 = 2, z_4 = -2,$$

and hence,

$$(z_1, z_2; z_3, z_4) = \frac{(z_1 - z_2)(z_3 - z_4)}{(z_1 - z_3)(z_2 - z_4)} = \frac{(1 + 1)(2 + 2)}{(1 - 2)(-1 + 2)} = -8.$$

Therefore, under then map that sends P_1 to $[1 : 0]$, P_3 to $[1 : 1]$, and P_4 to $[0 : 1]$, P_2 is sent to $[1 : -8]$.

7 Atomic Constructions

Now we are in a position to start proving the universality theorem. We will first prove that the statement is true of the atomic constructions, by making explicit constructions of matroids in $\mathbb{P}^2$.

7.1 Parallel shift

We first want to create the construction which shifts three points on a line l to another line l'. This construction will be used within our constructions of the atomic equations.

We fix an arbitrary point X, not lying on either line. We then construct the lines passing through X and the three points. Then each point maps to the intersection of their line and l'. This intersection always exists as any two points in $\mathbb{P}^2$ meet at a unique point.

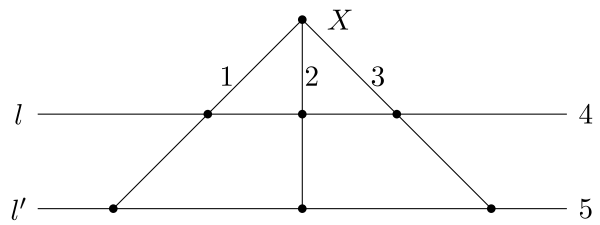


Figure 1: Diagram for parallel shift [7, p.8].

This construction represents a matroid of 5 elements $E = \{1, 2, 3, 4, 5\}$ where all sets of 4 elements, and the set $\{1, 2, 3\}$, are dependent.

Let us calculate the realisation space of this matroid. The set $\{1, 2, 4, 5\}$ is a circuit of the matroid, as removing any element creates an independent set. So we can map line 1 to the line with normal vector $(1, 0, 0)$, line 2 to the line with normal vector $(0, 1, 0)$, line 4 to the line with normal vector $(0,0,1)$, and line 5 to the line with normal vector $(1,1,1)$., under a PGL_3 map.

Now the normal vector of line 3 must be a linear combination of the normal vectors of lines 1 and 2. So we send line 3 to the line with normal vector $(1,a,0)$. Therefore, our realisation space is the set of matrices of the form

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & a & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix},$$

where no 3×3 minor, except the minor formed by the first three columns, is zero. This occurs if and only if $a \neq 0$ and $a \neq 1$.

Now let us calculate the cross-ratio of the points of intersection on line 4 and line 5. To calculate the coordinates of the first point on line 4, we take the cross product of the normal vectors of line 1 and line 4. This gives us that the first point has coordinates $[0:1:0]$. Then the centre point is the intersection of lines 2 and 4, so has coordinates $[1:0:0]$. The last point on line 4 has coordinates $[-a:1:0]$. Then the point at infinity is the intersection of lines 4 and 5. So the point at infinity is $[-1:1:0]$.

We then map to $\mathbb{P}^1$. We do this by projecting onto the first two coordinates. So the first point is mapped to $[0:1]$ (the point at infinity), the second point is mapped to $[1:0]$, the third point is mapped to $[1:-1/a]$ and the point at infinity is mapped to $[1:-1]$. Now we have that $z_2 = 0$, $z_3 = -1/a$ and $z_4 = -1$. This means that the cross-ratio of these four points is $\frac{a-1}{a}$. Therefore, under the map that sends the first point to $[1:0]$, the second point to $[1:1]$, and the point at infinity to $[0:1]$, the centre point is sent to

$$\left[1 : \frac{a-1}{a}\right].$$

We now want to do this whole process again for the three points that lie on line 5. The first, second and third points have coordinates $[0:-1:1], [1:0:-1]$ and $[a:-1:1-a]$ respectively. Therefore, when mapped to $\mathbb{P}^1$, they have coordinates $[0:1]$, $[1:0]$ and $[1:-1/a]$. Hence, we have $z_2 = 0$ and $z_3 = -1/a$. So again we get that the cross-ratio of these three points, together with the intersection of lines 4 and 5, is $\frac{a-1}{a}$. So therefore, the centre point will be sent to

$$\left[1 : \frac{a-1}{a}\right].$$

This leads us to the conclusion that the process of parallel shifting will preserve our cross-ratio.

Lemma 7.1. *Parallel shift preserves the cross ratio of three points, together with the point at infinity.*

7.2 Multiplication

The first ring we would like to construct is

$$X = \mathbb{Z}[y_1, y_2, y_3]/(y_1y_2 - y_3),$$

and so we want to enforce the equality that $y_1y_2 = y_3$. This may seem like a trivial example, as this ring is isomorphic to $\mathbb{Z}[y_1, y_2]$, but it is actually an important example to demonstrate. Once we consider more complicated equations, we need to be able to construct multiplication. For instance, later we will construct

$$\frac{\mathbb{Z}[x_1, x_2, x_3, x_4]}{(x_1x_2 - x_3x_4)},$$

which will require us to make the construction of multiplication two times.

Our first step in the construction is to define new variables $x_1 = y_1 + t \in \mathbb{Z}[y_1, y_2, y_3][t]$ and $x_2 = y_2 + t \in \mathbb{Z}[y_1, y_2, y_3][t]$, and create a new variable x_3. We want to enforce that $x_3 = x_1x_2$.

We create three dependent lines l_1, l_2 and l_3 in $\mathbb{P}^2$, which represent x_1, x_2 and x_3. We then choose three arbitrary points on l_1 and parallel shift these points onto l_3, from an arbitrary point. We then choose three arbitrary points on l_2 and parallel shift them to l_3, choosing the shifting point X such that the first point z_1 on l_2 is mapped to the first point w_1 on l_3, and the third point z_3 on l_2 is mapped to the second point w_2 on l_3. This can always be achieved by choosing the intersection of the line through z_1 and w_1 and the line through z_3 and w_2. This intersection will always exist as these lines are in $\mathbb{P}^2$, where any two lines always meet at a point.

We then form a matroid in $\mathbb{P}^2$ of the constructed lines, shown in the following picture, as viewed in the $z = 1$ plane.

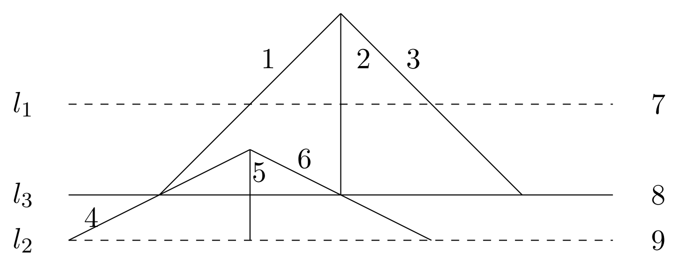


Figure 2: Diagram for multiplication construction [7, p.9].

On this diagram, the three points which represent x_3 are the first, second and fourth points on l_3.

We have seen this construction in Section 3, and have calculated its realisation space:

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & a & 1 & b & c & 0 & d & d \\ 0 & 0 & 0 & 1 & e & d & 1 & d & f \end{pmatrix},$$

where

$$\det \begin{pmatrix} 1 & 1 & 1 \\ 1 & b & c \\ 1 & e & d \end{pmatrix} = 0,$$

and hence,

$$bd - ce - d + c + e - b = 0.$$

We insist that no 3×3 minors except those formed by the columns $\{1, 2, 3\}, \{4, 5, 6\}, \{7, 8, 9\}, \{1, 4, 8\}$ and $\{2, 6, 8\}$ are zero. This imposes the conditions that no none of a, b, c, d, e, f are zero or one, and also other conditions calculated in Section 3.

So we have now imposed some equalities and inequalities on the elements a, b, c, d, e, f. Let $D \in \mathbb{Z}[a, b, c, d, e, f]$ be the product of all polynomials which are forced to be non-zero. Then we localise the ring $\mathbb{Z}[a, b, c, d, e, f]$ at D. We then also have the condition that $bd - ce - d + c + e - b = 0$, and so we quotient out by the ideal generated by $bd - ce - d + c + e - b$. We are then left with the ring

$$\mathbb{Z}\left[a, b, c, d, e, f, \frac{1}{D}\right] / (bd - ce - d + c + e - b).$$

Now we want to calculate the values of x_1, x_2 and x_3 using the cross ratio. Consider the line l_1. This line encodes the value of x_1 as the value of the centre point under the map which sends the leftmost point to 0, the rightmost point to 1, and the point at infinity to infinity.

To find the coordinates of the intersections of lines, we take the cross product of their normal vectors. Now the leftmost point has coordinates $[0 : 1 : 0]$, the centre point has coordinates $[1 : 0 : 0]$, the rightmost point has coordinates $[a : -1 : 0]$, and the point at infinity has coordinates $[-d : 1 : 0]$. So therefore, to apply the cross-ratio, we have $z_2 = 0, z_3 = -1/a$ and $z_4 = -1/d$.

Then we have

$$x_1 = \frac{z_3 - z_4}{z_2 - z_4} = \frac{a - d}{a}.$$

Following the same process we get $x_2 = \dfrac{b - e}{b - d}$ and $x_3 = \dfrac{(a - d)(b - e)}{a(b - d)}$, and we can clearly see that we have $x_1 x_2 = x_3$.

Now we note that $d = a - x_1 a$, $e = b - (b - a + x_1 a)x_2$, and

$$c = \frac{b(a - x_1 a) - (a - x_1 a) + b - (b - a + x_1 a)x_2 - b}{1 - b - (b - a + x_1 a)x_2}.$$

Then $1 - c = 1 - b - (b - a + x_1 a)x_2$ is a factor of D, and so we find that c, d and e all lie in the ring

$$\mathbb{Z}\left[x_1, x_2, x_3, a, b, f, \frac{1}{D}\right] / (x_1 x_2 - x_3).$$

Hence, our realisation space is the open set $\{D \neq 0\}$ inside

$$\operatorname{Spec}(\mathbb{Z}[x_1, x_2, x_3, a, b, f]/(x_1 x_2 - x_3)).$$

Now, we have that

$$\mathbb{Z}[x_1, x_2, x_3, a, b, f]/(x_1 x_2 - x_3) \cong \frac{\mathbb{Z}[x_1, x_2, x_3]}{(x_1 x_2 - x_3)} \otimes \mathbb{Z}[a, b, f]$$

and so by our discussion in Chapter 5, we have the isomorphism

$$\begin{aligned}\operatorname{Spec}(\mathbb{Z}[x_1, x_2, x_3, a, b, f]/(x_1 x_2 - x_3)) &\cong \operatorname{Spec}(\mathbb{Z}[x_1, x_2, x_3]/(x_1 x_2 - x_3)) \times \operatorname{Spec}(\mathbb{Z}[a, b, f]) \\ &= \operatorname{Spec}(X) \times \mathbb{A}^3.\end{aligned}$$

So considering the statement of the Universality theorem, for our finite type $\mathbb{Z}$-algebra X we have found a matroid whose realisation space is an open subset of $\operatorname{Spec}(X) \times \mathbb{A}^3$. We are left to show that this realisation space maps surjectively onto $\operatorname{Spec}(X)$.

We already have the map defined by

$$x_1 \mapsto x_1 - t = y_1$$

$$x_2 \mapsto x_2 - t = y_2.$$

To show that this map means that the realisation space maps surjectively onto $\operatorname{Spec}(X)$, we need to show that, for any choice of y_1, y_2, there is a choice of x_1, x_2, t such that our product of polynomials D is non-zero.

Now we consider all the polynomials which make up D, listed in Section 3. We notice that, as $x_1 = \dfrac{a - d}{a}$ and $x_2 = \dfrac{b - e}{b - d}$, $d \neq 0$ only enforces that $x_1 \neq 0$ and $x_2 \neq 0$. So for any given y_1, y_2, we choose $x_1, x_2 \neq 0$ such that $x_1 - x_2 = y_1 - y_2$. Then choose t such that $x_1 - t = y_1$. This forces $x_2 - t = y_2$. Then we map x_3 to $(x_1 - t)(x_2 - t) = y_3$, so that we enforce $y_1 y_2 = y_3$. Hence we have found a surjective map from $\{D \neq 0\}$ to $\operatorname{Spec}(X)$. Therefore, for the atomic equation of multiplication, the universality theorem holds.

7.3 Equality

We now want to construct the ring

$$X = \mathbb{Z}[y_1, y_2]/(y_1 - y_2) \cong \mathbb{Z}[y_1].$$

Again this may seem like a trivial example to construct, but we will need this construction explicitly for more complicated rings. We follow our strategy from constructing multiplication, and for the free variable y_1 we define a new variable $x_1 = y_1 + t \in \mathbb{Z}[y_1, t]$. We then form a matroid in $\mathbb{P}^2$ with defining lines for x_1 and another variable x_2 which enforces the equality $x_1 = x_2$.

This is the most simple construction. As we know that parallel shifting preserves the cross-ratio, we create two lines l_1 and l_2, and choose three points on each line which parallel shift to the same three points on a new line l'. Then we take the matroid of constructed lines, shown here in the $z = 1$ plane.

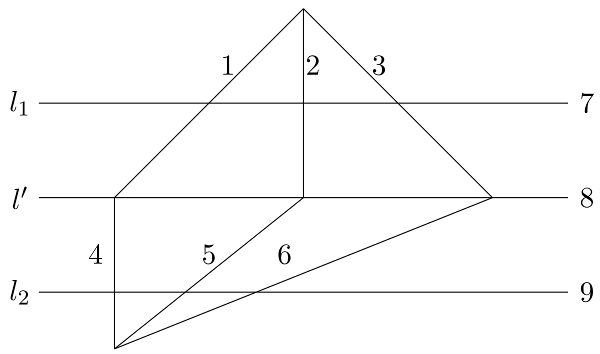


Figure 3: Diagram for equality construction.

We now want to calculate the realisation space of this matroid. Lines $\{1, 2, 7, 8\}$ form a circuit. So we can map line 1 to the line with normal vector $(1, 0, 0)$, line 2 to the line with normal vector $(0, 1, 0)$, line 8 to the line with normal vector $(0, 0, 1)$, and line 7 to the line with normal vector $(1, 1, 1)$.

Now $\{1, 2, 3\}$ is a dependent set, so column 3 must have the form $(1, a, 0)$. Then $\{1, 4, 8\}$ is also a dependent set, so column 4 must have the form $(1, 0, b)$. Now $\{7, 8, 9\}$ are dependent, so column 9 must have the form $(1, 1, e)$. We also have that $\{2, 5, 8\}$ is dependent, so column 5 has the form $(0, 1, c)$. Finally, our last dependent sets are $\{3, 6, 8\}$ and $\{4, 5, 6\}$, and so if column 6 has the form $(1, a, d)$, we require

$$\det \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & a \\ b & c & d \end{pmatrix} = 0.$$

So we arrive at the realisation space

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & a & 0 & 1 & a & 1 & 0 & 1 \\ 0 & 0 & 0 & b & c & d & 1 & 1 & e \end{pmatrix},$$

where we enforce that

$$d - ac - b = 0.$$

Furthermore, no other 3×3 minor can be zero. So none of a, b, c, d, e can be zero, or one, and none of the expressions

$$\{c-e, a-d, b-d, b-e, d-e, d-ac, ae-d, ac+b, ab-a-b, ab-ae-b, ac-c+e, a-ae+e-1,$$

$$1-b-c, e-b-c, ae-ab+b-d, c-ac+d-1, c-ac+d-e, ac-c+1, d-ac-b\}$$

can be zero. So now let $D \in \mathbb{Z}[a, b, c, d, e]$ be the product of all polynomials which are forced to be non-zero. So now we have the ring $\mathbb{Z}[a, b, ec, d, e]$, which we localise at D. We then take the quotient by the ideal $(d - ac - b)$. So we arrive at the ring

$$\mathbb{Z}\left[a, b, c, d, e, \frac{1}{D}\right] /(d - ac - b).$$

Now we want to calculate the values of x_1 and x_2 to make sure that the equality $x_1 = x_2$ is enforced. The three points on l_1 are $[0 : -1 : 1]$, $[1 : 0 : -1]$ and $[a : -1 : 1 - a]$. Then the point at infinity is $[1 : -1 : 0]$. So we have $z_2 = 0$, $z_3 = -1/a$, and $z_4 = -1$. Then, using the cross-ratio, we get

$$x_1 = \frac{a-1}{a}.$$

Following the same process for the line l_2, we have

$$x_2 = \frac{ab - ae + ac - b + e - c}{ab - ae - b + d}.$$

These expressions do not look the same. But using the fact that $d = ac + b$, we conclude

$$x_2 = \frac{ab - ae + ac - b + e - c}{ab - ae - b + ac + b} = \frac{(a-1)(b-e+c)}{a(b-e+c)} = \frac{a-1}{a}.$$

Hence, this construction enforces the equality that $x_1 = x_2$.

We note that within our localisation at D, we enforce that a cannot be zero. So we may replace a with $a' = 1/a$. We then note that $a' = 1 - x_1$. Now we can use the equality

$d = ac + b$ to eliminate d, and we arrive at the the localised ring

$$\mathbb{Z}\left[x_1, x_2, b, c, e, \frac{1}{D}\right] / (x_1 - x_2).$$

Again, we have that the realisation space of this matroid is the open set $\{D \neq 0\}$ in

$$\begin{aligned}\operatorname{Spec}\left(\frac{\mathbb{Z}[x_1, x_2, b, c, e]}{(x_1 - x_2)}\right) &\cong \operatorname{Spec}\left(\frac{\mathbb{Z}[x_1, x_2]}{(x_1 - x_2)}\right) \times \operatorname{Spec}(\mathbb{Z}[b, c, e]) \\ &= \operatorname{Spec}(X) \times \mathbb{A}^3.\end{aligned}$$

So, for our given X, we have found a matroid whose realisation space is an open set of $\operatorname{Spec}(X) \times \mathbb{A}^3$. We again need to show that this open set maps surjectively onto $\operatorname{Spec}(X)$.

We have a map which sends x_1 to $x_1 - t$. We need to show that for any y_1, there are x_1 and t such that x_1 maps to y_1 and the product of polynomials D is non-zero. But as $x_1 = \frac{a-1}{a}$, looking at the complete list of polynomials which make up the product of D, we see that we only enforce that $x_1 \neq 0$. So for any y_1, choose $x_1 = 1$ and $t = 1 - y_1$. Then x_1 maps to y_1.

So we have shown that the realisation space of this matroid maps surjectively onto $\operatorname{Spec}(X)$. Hence, for the atomic equation of equality, the universality theorem holds.

7.4 Addition

We now want to be able to construct the ring

$$X = \mathbb{Z}[y_1, y_2, y_3]/(y_1 + y_2 - y_3).$$

Therefore, we want to be able to enforce the equality $y_1 + y_2 = y_3$.

Again our first step in the construction is to define new variables $x_1 = y_1 + t$ and $x_2 = y_2 + t$, and create another new variable x_3.

We then create a matroid which enforces that $x_1 + x_2 = x_3$. We will have three lines, l_1, l_2 and l_3 associated with x_1, x_2 and x_3 respectively. We then parallel shift the three arbitrarily chosen points on l_1 onto three points on l_3. We then parallel shift, from an arbitrary point X, the first and third point on l_2 to the first and third point on l_3 respectively. Then we construct another line through X which forms a dependent set with l_1 and l_2. Finally, we parallel shift the first two points of l_2 onto the middle point of l_3 and a new arbitrary point, from a point on our newly constructed line.

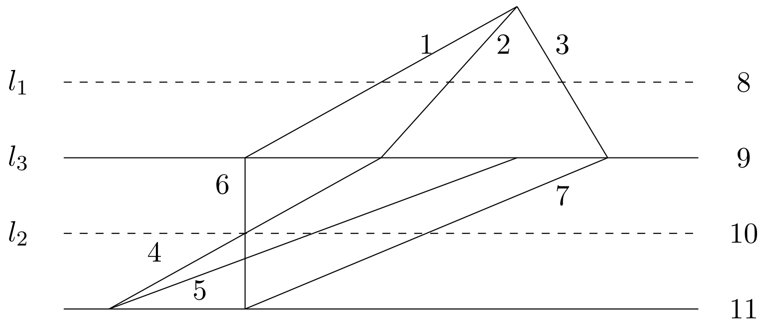


Figure 4: Diagram for addition construction [7, p.9].

Within this diagram, x_3 is represented by the first, third and fourth points on l_3.

Let us calculate the realisation space for this matrix, following the same process we have done before. Now as $\{1,2,5,9\}$ form a circuit, we send columns 1,2 and 9 to the identity matrix, and send column 5 to $(1,1,1)$. Now the set of lines $\{1,2,3\}$ forms a dependent set, and so we send column 3 to $(1,a,0)$. Again, the set of lines $\{2,4,9\}$ forms a dependent set, so we send column 4 to $(0,1,c)$. We continue this process and arrive at the realisation space

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & a & 1 & 1 & 0 & a & b & 0 & b & b \\ 0 & 0 & 0 & c & 1 & d & e & f & 1 & g & h \end{pmatrix},$$

where we impose the conditions that the the minors of columns $\{4,6,10\}, \{4,5,11\}$ and $\{6,7,11\}$ are zero. Hence,

$$\begin{aligned} d - g + bc &= 0, \\ 1 - h + bc - c &= 0, \\ ah - be + bd - ad &= 0. \end{aligned}$$

We also need to impose the conditions that no other 3×3 minor is zero. This forces all of a, b, c, d, e, f, g and h to not equal zero or one, and also all the following must be non-zero:

$$\{a-b, a-e, b-f, b-g, b-h, d-e, d-f, d-g, d-h, e-f, e-g, e-h, f-g, f-h, g-h, e-ac,$$

$$f-bc, g-bc, h-bc, ac+d, be-af, be-ag, be-ah, 1-c-d, ac-c+1, ac+d-e, bc+d-f,$$

$$bc+d-g, bc+d-h, ac-bc+f, ac-bc+g, ac-bc+h, a-ad+d, a-af-b+f, a-ag-b+g,$$

$$a-ah-b+h, ac-c-e+1, bc-c-f+1, bc-c-g+1, bc-c-h+1, bc-ac+e-f, bc-ac+e-g,$$

$$bc-ac+e-h, ad-bd-af, ad-bd-ag, ad-bd-ah, bd-ad-be+af, bd-ad-be+ag,$$

$$bd-ad-be+ah, a-ad+d-e, b-bd+b+d-f, b-bd+b+d-g, b-bd+b+d-h, af-be-a+b+e-f,$$

$$ag-be-a+b+e-g, ah-be-a+b+e-h\}.$$

Now let $D \in \mathbb{Z}[a,b,c,d,e,f,g,h]$ be the product of all polynomials which are forced to be non-zero. Then we take $\mathbb{Z}[a,b,c,d,e,f,g,h]$ and localise at D. We also quotient out by the ideal generated by $d-g+bc, 1-h+bc-c$, and $ah-be+bd-ad$. We then arrive at the ring

$$\mathbb{Z}\left[a,b,c,d,e,f,g,h,\frac{1}{D}\right]/(d-g+bc, 1-h+bc-c, ah-be+bd-ad).$$

We now compute the values for x_1, x_2 and x_3, using the same process as for the previous constructions, using the equations above to simplify the answers. The three points on l_1 are $[0:-f:b]$, $[f:0:-1]$, and $[af:-f:b-a]$. Then the point at infinity is $[-b:1:0]$. We have enforced that $a,b,f \neq 0$, and so we have $z_2 = 0, z_3 = -1/a$, and $z_4 = -1/b$. So therefore,

$$x_1 = \frac{a-b}{a}$$

Following the same process, we conclude that

$$x_2 = \frac{b^2-ab}{ab-a},$$

$$x_3 = \frac{a-b}{a-ab},$$

which indeed does give us $x_1 + x_2 = x_3$.

Again we note that our product D enforces that a is non-zero. So we may replace a with $a' = 1/a$. Then we have that $a' = \dfrac{1-x_1}{b}$, with b a factor of D.

From $d-g+bc = 1-h+bc-c = ah-be+bd-ad = 0$, we can rearrange to find c, d, and e in terms of the other variables. So we have the localised ring

$$\mathbb{Z}\left[x_1,x_2,x_3,b,f,g,h,\frac{1}{D}\right]/(x_1+x_2-x_3).$$

Therefore the realisation space of this matroid is the open set $\{D \neq 0\}$ in

$$\mathrm{Spec}(\mathbb{Z}[x_1,x_2,x_3,b,f,g,h]/(x_1+x_2-x_3)).$$

Again, from our discussion of the tensor product, we get that

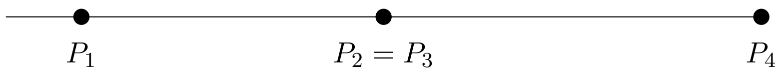
$$\begin{aligned}\mathbb{Z}[x_1,x_2,x_3,b,f,g,h]/(x_1+x_2-x_3) &\cong \frac{\mathbb{Z}[x_1,x_2,x_3]}{(x_1+x_2-x_3)} \otimes \mathbb{Z}[b,f,g,h] \\ &= \mathrm{Spec}(X) \times \mathbb{A}^4.\end{aligned}$$

So we have created a matroid whose realisation space is an open set in $\mathrm{Spec}(X) \times \mathbb{A}^4$, as required in the universality theorem. We are left to check that this realisation space maps surjectively onto Spec(X).

Again, consider the list of polynomials which make up D. As $x_1 = \dfrac{a-b}{a}$ and $x_2 = \dfrac{b^2-ab}{ab-a}$, we only enforce that $x_1 \neq 0$ and $x_2 \neq 0$. So for any y_1, y_2 we can choose $x_1, x_2 \neq 0$ such that $x_1 - x_2 = y_1 - y_2$. Then we let $t = x_1 - y_1$, which forces $x_2 + t = y_2$. We then map x_3 to $x_1 + x_2 + 2t = y_3$. Hence, we have found a map from $\{D \neq 0\}$ such that the map is surjective onto Spec(X). So we have proved the universality theorem for the atomic construction of addition.

7.5 Constructing 1

We want to be able to use 1 as a variable in our constructions of polynomials, so we want to construct a variable x_0 such that $x_0 = 1$. We do this by first constructing a line in $\mathbb{P}^2$. Then, considering our discussion of the cross-ratio, the right-most point gets sent to 1 under the cross-ratio map. Therefore, as we require the middle point to also be mapped to 1, to enforce $x_0 = 1$, we allow the middle and the right-most point to coincide. Then we will have a line with only two points, plus P_4, the point at infinity.



Now let us calculate the cross-ratio. First assume that all of P_1, P_2, P_3 and P_4 are of the form $[1 : z_i]$ under the map which sends the line to $\mathbb{P}^1$. We have that $z_2 = z_3$ by construction, as $P_2 = P_3$. Hence, the cross-ratio is

$$(z_1, z_2; z_3, z_4) = \frac{(z_1 - z_2)(z_3 - z_4)}{(z_1 - z_3)(z_2 - z_4)} = \frac{(z_1 - z_2)(z_2 - z_4)}{(z_1 - z_2)(z_2 - z_4)} = 1.$$

Now if $P_1 = [0 : 1]$ or $P_4 = [0 : 1]$ the calculation is simple and we also find that $(z_1, z_2; z_3, z_4) = 1$. Finally, if $P_2 = P_3 = [0 : 1]$, by definition we remove all brackets which contain z_2 or z_3. Hence, the product is trivially 1.

This construction is useful in constructing realisation spaces such as

$$X = \frac{\mathbb{Z}[y_1, y_2]}{(y_2 - y_1 - 1)},$$

where we want to enforce the equality $y_2 = y_1 + 1$. This is the process of incrementing the variable y_1 by one.

This is just a special case of the atomic equation of addition. First we let $x_1 = y_1 + t$, and introduce two new variables x_0 and x_2. We then note that

$$X \cong \frac{\mathbb{Z}[x_0, x_1, x_2]}{(x_0 - 1, x_2 - x_1 - x_0)}.$$

So we want to enforce that $x_0 = 1$, and we want to enforce that $x_2 = x_1 + x_0$. We follow the process above to get $x_0 = 1$. Then we use the construction of addition already defined to enforce $x_2 = x_1 + x_0$.

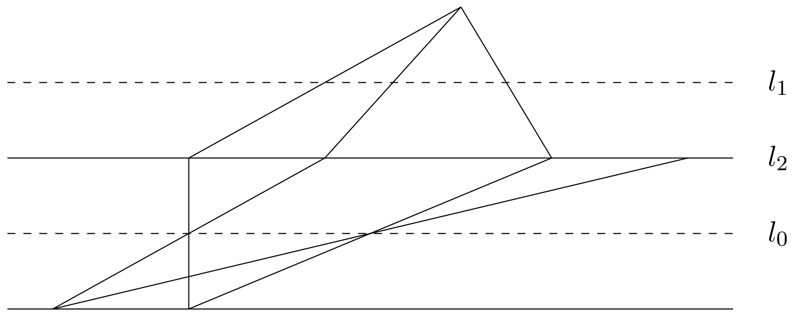


Figure 5: Diagram for incrementing construction [3, p.23].

8 Combining Atomic Constructions

Once we have reduced a polynomial equation to atomic equations, we want to combine the atomic constructions from Section 6. We will demonstrate this using an example which combines the atomic equations of equality and multiplication.

We want to construct the ring

$$X = \mathbb{Z}[y_1, y_2, y_3, y_4]/(y_1 y_2 - y_3 y_4).$$

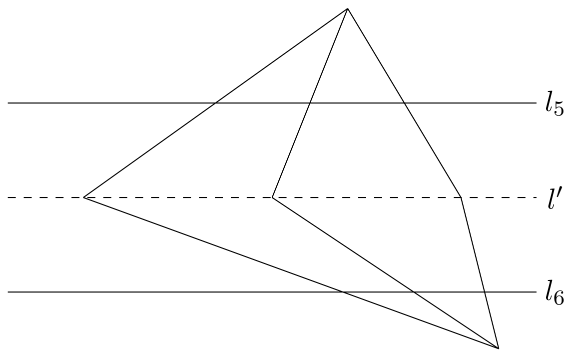
Our first task is to force the equation $y_1 y_2 - y_3 y_4$ to be equivalent to a combination of atomic equations. Firstly, we create a variable y_5 which is equal to $y_1 y_2$. Then we create another variable y_6 which is equal to $y_3 y_4$. Lastly, we want to enforce the equality that $y_5 = y_6$. Then we have the isomorphism

$$\frac{\mathbb{Z}[y_1, y_2, y_3, y_4]}{(y_1 y_2 - y_3 y_4)} \cong \frac{\mathbb{Z}[y_1, y_2, y_3, y_4, y_5, y_6]}{(y_1 y_2 - y_5, y_3 y_4 - y_6, y_5 - y_6)}.$$

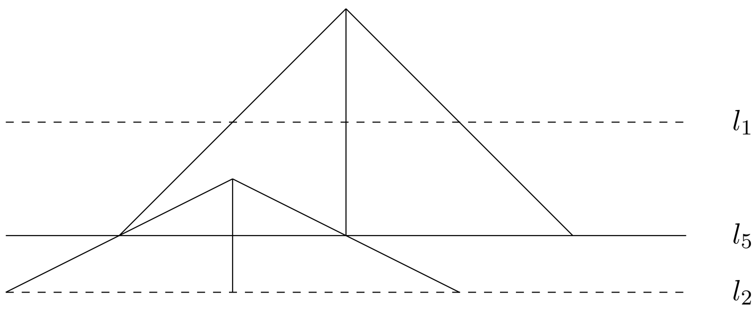
We then create new variables $x_1 = y_1 + t, x_2 = y_2 + t, x_3 = y_3 + t$ and $x_4 = y_4 + t$. We then also have two other variables x_5 and x_6. We want to enforce that $x_5 = x_1 x_2$, $x_6 = x_3 x_4$ and $x_5 = x_6$.

We start with 6 lines $l_1, l_2, l_3, l_4, l_5, l_6$ representing x_1, x_2, x_3, x_4, x_5 and x_6 respectively. We enforce that any three of these lines are dependent. We may order them in any way, and so we choose to order them such that the constructions are easiest.

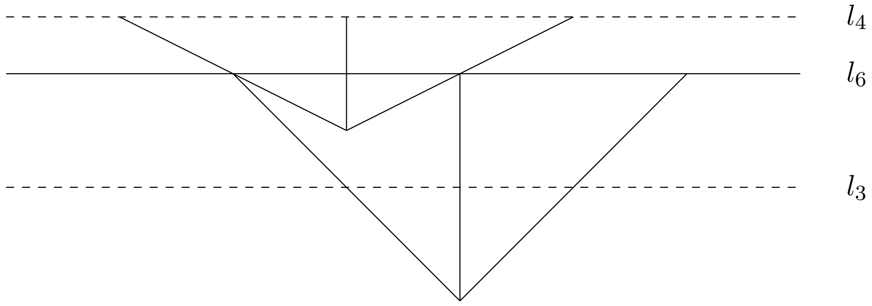
First we enforce the equality of $x_5 = x_6$. We do this by adding a new line l', and constructing three points on both l_5 and l_6 which parallel shift to the same points on l'.



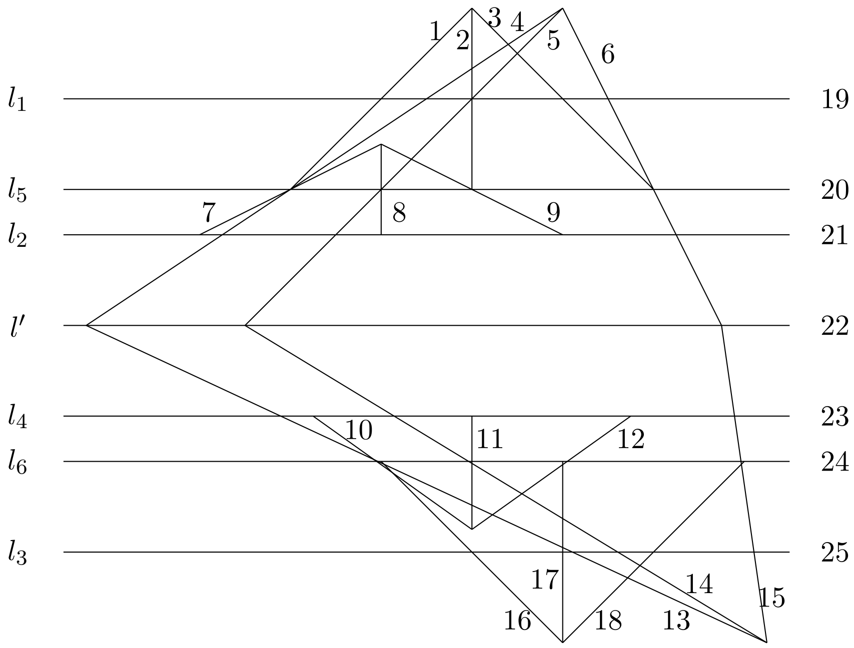
We have now fixed the points on l_5 and l_6. We now want to enforce that $x_1x_2 = x_5$. So we choose three points on l_1 and three points on l_2 such that we can construct the atomic construction of multiplication.



Again we want to enforce $x_3x_4 = x_6$, and so we choose three points on l_3 and three points on l_4 such that we can construct the atomic construction of multiplication.



Now we combine all three constructions together to form our matroid:



This is a 25 line matroid with realisation space

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & a & 0 & b & a & 0 & b & 1 & c & d & e & f & g & 1 & h & i & j & k & 0 & k & k & k & k & k \\ 0 & 0 & 0 & l & m & n & o & p & q & r & s & t & u & v & 1 & w & x & y & z & 1 & \alpha & \beta & \gamma & \delta & \epsilon \end{pmatrix},$$

where we demand that many of the 3×3 minors are zero, and the rest are non-zero. For instance, we enforce that the minor

$$\det \begin{pmatrix} 1 & 1 & 0 \\ 0 & b & 1 \\ o & p & q \end{pmatrix}$$

is zero, which enforces that $\{7, 8, 9\}$ are dependent, and therefore

$$p = qb + o.$$

Let D be the product of all polynomials forced to be non-zero, and I be the ideal generated by all the polynomials forced to be zero. Then the realisation space of this matroid is the open set $\{D \neq 0\}$ in

$$\mathrm{Spec}(\mathbb{Z}[a, b, ..., z, \alpha, ..., \epsilon]/I).$$

Now we want to show that we have the equality $x_1 x_2 = x_3 x_4$. First let us show that we have enforced the equality $x_1 x_2 = x_5$. On our line l_1, we have that our first point is $[0 : z : -k]$, our second point is $[-z : 0 : 1]$, our third point is $[-az : z : a - k]$, and the point at which the l_is meet is $[-k:1:0]$. Hence, we have

$$x_1 = \frac{a-k}{a}.$$

Now following the same process, we find that

$$x_2 = \frac{ko + b\alpha - ob - kp}{k^2q - kqb - k\alpha + ko + b\alpha - ob}.$$

But noting that we require $p = qb + o$, we have

$$x_2 = \frac{ko + b\alpha - ob - kqb - ko}{k^2q - kqb - k\alpha + ko + b\alpha - ob} = \frac{b(\alpha - o - kq)}{(b-k)(\alpha - o - kq)} = \frac{b}{b-k}.$$

Finally we calculate x_5 and find it to be

$$x_5 = \frac{kb - ab}{ka - ab} = x_1x_2.$$

Similarly, we can show that $x_6 = x_3x_4$, and that $x_5 = x_6$. So indeed this construction enforces $x_1x_2 = x_3x_4$, and so we have constructed a matroid whose realisation space is an open set in $\mathrm{Spec}(X) \times \mathbb{A}^n$.

Then this set maps surjectively to $\mathrm{Spec}(X)$ by noting that D is a finite product of polynomials, and there are no forced relations between x_1, x_2, x_3, and x_4. So these variables force $D = 0$ at only a finite amount of points. So we can just choose t outside those points to find a surjective map to $\mathrm{Spec}(X)$.

Now we have seen how to construct the atomic equations, and we have seen an example of how to combine these equations, we are at last ready to prove the universality theorem.

Proof. (of the universality theorem) Given a finitely generated $\mathbb{Z}$-algebra R, we will prove the universality theorem by explicitly stating the steps for the construction of the corresponding matroid.

1. Write the finitely generated $\mathbb{Z}$-algebra R as the quotient of $\mathbb{Z}[y_1, ..., y_n]$ by an ideal S.

2. As $\mathbb{Z}[y_1, ..., y_n]$ is Noetherian, write S as the generating set of a finite number of polynomials $f_1, ...f_m \in \mathbb{Z}[y_1, ..., y_n]$.

3. First, if needed, construct a variable x_0 with $x_0 = 1$ such as in Section 7.5.

4. Construct each f_i as the combination of atomic equations (theorem 4.2), rewriting R as the quotient of $\mathbb{Z}[x_0, y_1, ..., y_q]$ by the ideal I generated by all these atomic equations.

5. Identify your variables which, in $\mathbb{Z}[y_1, ..., y_q]/I$, are not equal to the sum or product of any other variables. Define these variables to be your free variables, with the exception that if two of these variables are forced to be equal to each other, define exactly one of them as a free variable. Now reorder the elements $y_1, ..., y_q$ such that $y_1, ..., y_k$ are the free variables, and let $x_i = y_i + t$ for these variables.

6. Reorder the other variables $y_{k+1}, ..., y_q$ such that each y_i is either equal to y_j for $j < i$, or is the addition or multiplication of y_j and y_k for $j, k < i$.

7. For each $y_{k+1}, ..., y_q$, create new variables $x_{k+1}, ..., x_q$.

8. Construct q lines in $\mathbb{P}^2$, where each triple of lines is dependent. When we view the realisation space in the $z = 1$ plane, these lines appear parallel.

9. Create the variables $x_{k+1}, ..., x_q$ one at a time by creating the construction of the atomic equation which defines x_i in turn, creating any variable $x_1, ..., x_k$ as needed. This can always be done as we have reordered the variables such that we are always constructing another variable which only relies on variables already created.

10. Produce the realisation space of this matroid, calculating the polynomials which cannot be zero, and generating their product D.

11. Then the realisation space of the matroid is the open set $\{D \neq 0\}$ in $\text{Spec}(R) \times \mathbb{A}^n$.

12. We then note that D is a finite polynomial, and there are no forced relations between $x_1, ..., x_k$, and so there are only finitely many values which $x_1, ..., x_k$ cannot take. So we can always pick a t outside the relations defined by D to map $\{D \neq 0\}$ surjectively onto $\text{Spec}(R)$ via $y_i = x_i + t$ for $i \leq k$.

□

Bibliography

References

[1] Federico Ardila. Matroid theory. In *Lecture notes*. San Francisco State University/Universidad de los Andes, 2007.

[2] Peter Cameron. Matroids. In *Advanced Combinatorics Lecture notes*. St. Andrew's University, 2015.

[3] Dustin Cartwright. Lifting matroid divisors on tropical curves. *Res. Math. Sci.*, 2:Art. 23, 24, 2015.

[4] David Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.

[5] David Eisenbud and Joe Harris. *The geometry of schemes*, volume 197 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[6] Eric Katz. Matroid theory for algebraic geometers. In *Nonarchimedean and tropical geometry*, Simons Symp., pages 435–517. Springer, 2016.

[7] Seok Hyeong Lee and Ravi Vakil. Mnëv-Sturmfels universality for schemes. In *A celebration of algebraic geometry*, volume 18 of *Clay Math. Proc.*, pages 457–468. Amer. Math. Soc., Providence, RI, 2013.

[8] James Oxley. *Matroid theory*, volume 21 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, second edition, 2011.

[9] Evgeny Shinder. Tensor products. In *MAS439 Lecture Notes*. University of Sheffield, 2018.