MATROIDS

ANDREW CHANG

Abstract. Matroids are incredibly versatile abstractions, bridging areas of mathematics ranging from geometric configurations to graph optimizations. This paper provides an introduction to the essentials for understanding the different facets of matroids and illustrates some of their most interesting applications.

1. Introduction

Consider the matrix

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

with column vectors a, b, c, d, e from left to right. We seek a geometric way to represent the properties of this matrix—not just for specialized matrices like adjacency or transition matrices, but a representation that reflects the actual columns in general. In linear algebra, one of the most important relationships is the linear independence or dependence of the column vectors, i.e. whether they can be expressed as linear combinations of each other. In the above example, for example, the vectors b and c are linearly independent, while the set of vectors a, d, and e is not. (We write column vectors horizontally for convenience.)

To obtain our visualization, imagine placing all of the column vectors at the origin, and projecting them onto a plane as shown in 1. Note that the triplets of linearly dependent vectors

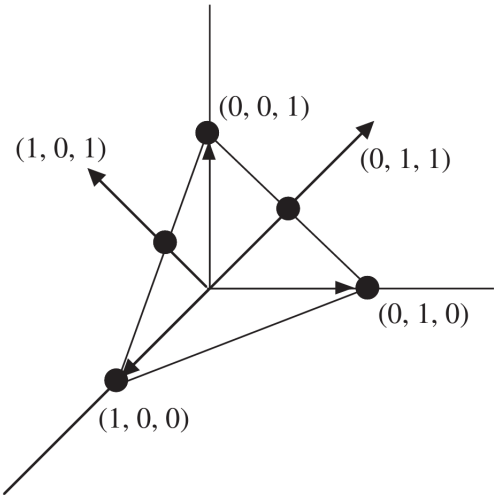

Figure 1. Our visualization.

are now collinear! Defining this correspondence allows us to work with structures from algebraic

Date: March 15, 2023.

geometry, and discover interesting results with matroid theory. As we will see, however, this is just one facet of the many connections that can be drawn with matroids. We'll introduce much of the terminology, key results, and some surprising applications of matroids (roughly following the presentation in [2]).

2. Matroids as Sets

We now introduce our first definition of a matroid. This is a very common definition to begin from—note, however, that it lacks any obvious connection to the geometric equivalence we have just introduced!

Definition 2.1. A matroid consists of a ground set E together with a collection of subsets $\mathcal{I}$, called the independent sets, such that

(I1) $\mathcal{I}$ is non-empty.
(I2) Every subset of a member of $\mathcal{I}$ is also in $\mathcal{I}$.
(I3) If I and J are in $\mathcal{I}$ and $|I| < |J|$, then there is an element x of $J \setminus I$ such that $I \cup \{x\}$ is in $\mathcal{I}$.

Some sources replace the first condition with the assertion that the empty set $\emptyset$ is in $\mathcal{I}$. This follows from our original conditions I1 and I2, while condition I1 follows from this assertion, so the two definitions are equivalent.

We call the maximal independent sets, those that are not a subset of any other member of $\mathcal{I}$, the *bases* (plural for basis). Note that these must all be the same size: if there were two differently sized bases $|I| < |J|$, then there would be a superset of I in $\mathcal{I}$ by condition I3, and I would thus not be a basis. We can characterize a matroid by its ground set and bases alone, since any member of $\mathcal{I}$ must either be either a subset of another member or a basis by definition.

Similarly, we define a circuit to be a minimal dependent set: a subset of E that isn't in $\mathcal{I}$, but where all of its proper subsets are in $\mathcal{I}$. The circuits can also be used to define a matroid like the bases, since their subsets give a collection of independent sets; and any independent set must have at least one associated circuit, by adding elements until a superset is no longer independent.

We call an element $x \in E$ that is in no basis a *loop*. (This also means the set consisting of solely x is a circuit, as no independent set contains x.) Meanwhile, an element $y \in \mathcal{I}$ that is in every basis, meaning it can be added to any independent set to create another independent set, is called a coloop or isthmus. (This also means it is in no circuits, since no dependent set containing it would be minimal.)

Since we can formulate a matroid in terms of bases or circuits, we also have some useful properties of them:

Bases $\mathcal{B}$

(B1) $\mathcal{B} \neq \emptyset$.
(B2) If $B_1, B_2 \in \mathcal{B}$ and $B_1 \subseteq B_2$, then $B_1 = B_2$.
(B2') If $B_1, B_2 \in \mathcal{B}$, then $|B_1| = |B_2|$.
(B3) If $B_1, B_2 \in \mathcal{B}$ and $x \in B_1 - B_2$, then there is an element $y \in B_2 - B_1$ so that $B_1 - x \cup \{y\} \in \mathcal{B}$.
(B3') If $B_1, B_2 \in \mathcal{B}$ with $x \in B_1 - B_2$, then there is an $y \in B_2 - B_1$, so that $B_1 - x \cup y$ and $B_2 - y \cup x$ are bases.

Circuits $\mathcal{C}$

(C1) $\emptyset \notin \mathcal{C}$.
(C2) If $C_1, C_2 \in \mathcal{C}$ and $C_1 \subseteq C_2$, then $C_1 = C_2$.
(C3) If $C_1, C_2 \in \mathcal{C}$ with $C_1 \neq C_2$, and $x \in C_1 \cap C_2$, then $C_3 \subseteq C_1 \cup C_2 - x$ for some $C_3 \in \mathcal{C}$.

(C3') If $C_1, C_2 \in \mathcal{C}$ with $C_1 \neq C_2, x \in C_1 \cap C_2$, and $y \in C_1 - C_2$ then $y \in C_3 \subseteq C_1 \cup C_2 - x$ for some $C_3 \in \mathcal{C}$.

These are also called axioms, because we can even ignore our original definition and use these rules alone to get matroids based on bases or circuits. These equivalent, or isomorphic results coming from seemingly different paths are called "cryptomorphisms" in matroid theory. We'll continue to see more equivalencies, coming from graphs and specific functions. One such function is the rank function, which gives the size of a basis of M. We can generalize this to the rank of any subset $A \subseteq E$, where $r(A)$ is the size of the largest independent subset of A. Then we have the following theorem, which we can again use to define matroids:

Theorem 2.2. *Let E be a finite set with an integer-valued function r defined on subsets of E. Then r is the rank function of a matroid if and only if for $A, B \subseteq E$:*

(R1) $0 \leq r(A) \leq |A|$;
(R2) *if $A \subseteq B$, then $r(A) \leq r(B)$;*
(R3) $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$.

Proof. We focus on proving the third axiom, which is less obvious.

Let A and B be subsets of E and let I_C be a basis of $A \cap B$, i.e., a maximal independent subset of $A \cap B$. Use axiom (I3) repeatedly to extend I_C to a basis I of $A \cup B$. Let $I_A = I \cap (A - B)$ and $I_B = I \cap (B - A)$. By construction, $r(A \cap B) = |I_C|$ and $r(A \cup B) = |I| = |I_A| + |I_B| + |I_C|$. Now, $I_A \cup I_C$ is an independent set (since it is a subset of I) contained in A. Thus, $r(A) \geq |I_A| + |I_C|$. Similarly, $r(B) \geq |I_B| + |I_C|$. Combining these results yields the desired result; $r(A) + r(B) \geq r(A \cup B) + r(A \cap B)$. □

We also introduce the concepts of flats and hyperplanes: a *flat*, also known as a closed set or a subspace of the matroid, is a maximal set of its rank. A *hyperplane* is then a flat of rank $r - 1$, i.e. a maximal flat excluding E itself.

3. Representable Matroids

A matroid that can be represented in terms of vectors, like our starting example, is called a *linear matroid*, or a *representable matroid*. Note that while all collections of vectors correspond to a matroid, the reverse is not true — there are non-linear matroids, as our basic definition is broad enough to include structures beyond pure matrices.

We now prove formally what we've already assumed: that all matrices do in fact correspond with a specific matroid.

Theorem 3.1. *Let E be the columns of a matrix A with entries in a field $\mathbb{F}$, and let $\mathcal{I}$ be those subsets of E that are linearly independent. Then $\mathcal{I}$ is the family of independent sets of a matroid.*

Proof. We need to show that $\mathcal{I}$ satisfies (I1), (I2) and (I3). (I1) is trivial, as $\emptyset$ is always a linearly independent set. (I2) is just as easy, following immediately from the definition of linear independence.

We focus on (I3), which involves some matrix manipulation. Let $|I| = s$ and $|J| = t$, where I and J are linearly independent subsets with $s < t$, and let A be the matrix whose columns correspond to $I \cup J$. Order the columns of A so that the vectors in I appear first. Then the matrix rank of A is at least t, since J is a linearly independent set.

We then row reduce A. Since I is an independent set, we can transform the first s columns into an $s \times s$ identity matrix, with rows of zeros below:

$$A \longrightarrow \left(\begin{array}{c|c} I_{s\times s} & B_1 \\ \hline 0 & B_2 \end{array}\right).$$

Since the matrix rank of A is at least t, some element of the submatrix B_2 is non-zero. Then it is clear we can add some column from $J - I$ to I and preserve linear independence. □

Representability can also depend on the field. Some matroids are binary — that is, they are representable in the field $\mathbb{F}_2$ with the numbers 0 and 1, like binary arithmetic. One example is the Fano plane, illustrated in 2.

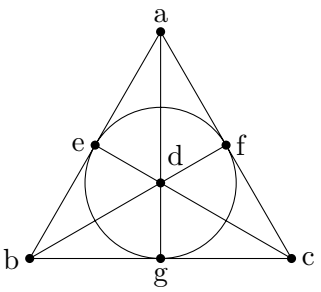

Figure 2. The Fano plane.

Based on the diagram, the empty set, singletons, pairs, and triples except for lines abe, adg, acf, bdf, bcg, cde, and efg are dependent. We can write out the corresponding matrix,

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

Because the last three vectors, representing e, f, and g, need to be linearly dependent to reflect their colinearity, we need their sum $(2, 2, 2)$ to equal the zero vector, i.e. $2 = 0$. Thus, the Fano plane is representable in fields with characteristic 2, where this is true (and only these fields!). There are also matroids that are *ternary*, meaning they are representable in $\mathbb{F}_3$, and matroids that are representable for any field, known as *regular* matroids.

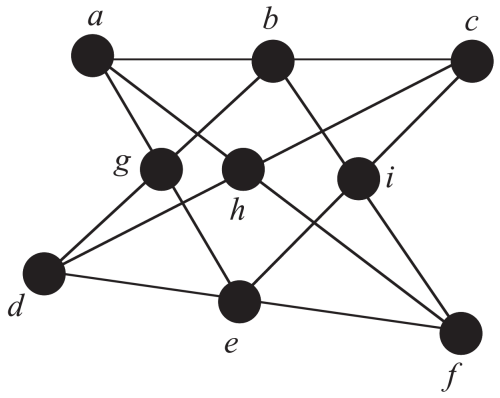

Figure 3. A non-representable matrix.

Here's an example of a matroid that isn't representable: eight points as arranged in 3, where trying to write out corresponding vectors and simplifying gives us the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & x & 1 & x & z \\ 0 & 0 & 1 & 1 & 1 & 0 & y & xy & y \end{pmatrix}$$

The full algebra won't be given here, but it boils down to showing that columns representing points that are collinear (i.e. not independent) must be linearly independent, so we can't write this matroid as a matrix. Once we have our isomorphism, the rest is just computational!

4. Graphs are Matroids

We have already seen how matroids relate to geometric structures, which somewhat resemble graphs. However, there is also another direct correspondence between matroids and graphs, based on classifying them by their cycles. (To distinguish these cycle-based graphs from similar-looking geometries, we draw the graphs with hollow vertices and the geometric structures with solid vertices.) We'll focus on undirected graphs here, but for eager readers there is an extension of matroid theory based on the idea of "oriented matroids" — generalizing ideas about directed graphs and ordered fields — as elaborated on in [1].

The basic definition is as follows:

Theorem 4.1. *Let G be a graph with edge set E, and let $\mathcal{I}$ be the collection of all subsets of E that do not contain a cycle. Then $\mathcal{I}$ forms the independent sets of a matroid on the ground set E, called the cycle matroid $M(G)$.*

Proof. We show the three matroid conditions (I1), (I2) and (I3) are all satisfied by the acyclic subsets of edges of a graph. (I1) is trivial, as $\emptyset$ is acyclic. (I2) is also trivial, since if B is a subset of edges that do not contain a cycle and $A \subseteq B$, then A is also acyclic.

Showing that (I3) is always satisfied is more difficult. We let A and B be acyclic subsets with $|A| < |B|$. We need to find an edge from B that is not in A which can be added to A without creating a cycle.

First, suppose that A is a tree (this is the easier case). Then the edges of A meet only $|A|+1$ vertices of the graph G. We need to find an edge $b \in B$ to add to A without creating a cycle. Since B is a forest, it meets $|B| + k$ vertices, where $k \geq 1$ is the number of components of B. As $|B| > |A|$, we have $|B| + k > |A| + 1$, meaning the edges of B meet some vertex of G that is not met by any edge of A. Call this vertex v and let $b \in B$ be any edge that meets v (there may be several such edges). Then $A \cup \{b\}$ must be acyclic and (I3) holds.

If A is not a tree, then things aren't as simple, but we can apply a similar strategy looking at each tree within A. Suppose A is composed of c disjoint trees $T_1, T_2, \ldots, T_c$. If the edges of B do meet a new vertex of G, then we're done; otherwise, let e_i denote the number of edges in the tree T_i, so that $e_1 + e_2 + \cdots e_c = |A|$. We claim there is an edge of B that joins up two of the trees T_i and T_j from A.

Suppose for the sake of contradiction that this isn't true, and look at the number of edges of B. As B is acyclic, it would have at most e_1 edges of T_1 (otherwise we'd get a cycle among the vertices of T_1). Similarly, B could have at most e_2 edges of T_2, and so on. Then $|B| \leq e_1 + e_2 + \cdots e_c = |A|$, which contradicts $|A| < |B|$. Thus, B must include an edge that joins the vertices of some T_i to some other T_j. This edge can now be safely added to A without creating any cycles, so (I3) is satisfied and we're done. □

From this it follows that graphs and matroids are closely related: our cryptomorphism allows us to derive results from matroids, and apply them to graphs.

It turns out that graphs and matroids have a surprisingly simple matrix to relate them: the vertex-edge incidence graph, where each row corresponds to a vertex and each column corresponds to an edge. A cell A_{ij} of the matrix is 1 if vertex v_i meets edge e_j, and 0 otherwise.

We prove that all graphs have a corresponding binary matroid:

Theorem 4.2. *Let G be a graph and A_G its vertex-edge incidence matrix. We will show the cycles of G correspond precisely to the circuits in the represented binary matroid $M(A_G)$.*

Proof. First, we resolve the loops. A loop in the graph G corresponds to a column vector of all 0's in the matrix A_G, i.e., a linearly dependent set. (One way to justify this is that the vertex incident to the loop will generate a 2 in the vertex-edge incidence matrix, but $2 \equiv 0 \pmod 2$.) Now suppose C is a cycle in G, with $C = \{c_1, c_2, \ldots, c_m\}$, where $m > 1$. Then we can reorder and/or rename the rows and columns of A_G so that the first m rows and columns of the matrix look like:

$$\begin{bmatrix} c_1 & c_2 & c_3 & \cdots & c_{m-1} & c_m \\ 1 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 1 & 1 \end{bmatrix}.$$

Thus, there are 1's along the main diagonal of this $m \times m$ square submatrix, and 1's below the main diagonal, and a single 1 in the upper right-hand corner.

Then the sum of the columns is $c_1 + c_2 + \cdots + c_m = 0$ in $\mathbb{F}_2$ since there are exactly two 1 's in each row (and all the entries in rows $m+1, m+2 \ldots$ are 0). Thus, these columns are linearly dependent.

We now show that removing any column leaves a linearly independent set. Since any of these columns can be transformed into any other column through linear operations, we choose to remove the last column without loss of generality. Then row reducing the remaining $m-1$ columns leaves an $(m-1) \times (m-1)$ identity matrix, so they are linearly independent. Thus, the columns corresponding to C form a circuit in $M(A_G)$.

For the other direction, we assume C is a circuit in the binary matroid $M(A_G)$ and show C corresponds to a cycle in G. So let $C = \{c_1, c_2, \ldots, c_m\}$ be a circuit in $M(A_G)$. Then these column vectors are linearly dependent, but any proper subset of them is linearly independent.

Let A_C be the submatrix formed by the m columns of the circuit C. Since these columns are linearly dependent, we know there are an even number of 1's in each row of A_C. Recall that the rows of A_G correspond to the vertices of G. Then we can find a cycle contained in C with the following procedure:

First, find an entry of A_C that equals 1 (since $m > 1$, there is some non-zero entry). Assume this entry is in the $a_{1,1}$ position in A_C. In the graph G, this corresponds to choosing a vertex v_1 and an edge c_1 incident to that vertex in G. Then, since there are two 1's in each column, there must be some other non-zero entry in the first column; as an example, say the $a_{2,1}$ entry is 1. In G, this corresponds to choosing the other vertex incident to c_1; here, that's v_2. Now, looking at the second row of A_C, there must be some other non-zero entry (since there are an even number of entries in every row). We assume this entry appears in position $a_{2,2}$, corresponding to an edge from c_2 incident to v_2.

$$\begin{array}{c} v_1 \\ \\ v_2 \\ \\ v_3 \\ \vdots \end{array} \begin{bmatrix} c_1 & & c_2 & & c_3 & \cdots \\ 1 & & 0 & & 0 & \cdots \\ \downarrow & & & & & \\ 1 & \rightarrow & 1 & & 0 & \cdots \\ & & \downarrow & & & \\ 0 & & 1 & \rightarrow & 1 & \cdots \\ \vdots & & \vdots & & \vdots & \cdots \end{bmatrix}.$$

We can continue in this manner, at each stage choosing a non-zero entry in a row or a column. This only ends when one of the vertical steps lands us in a row we've already visited, i.e., when we complete a cycle in the graph. Then the cycle we created must include all the edges of C; otherwise, this cycle would be a linearly dependent proper subset of C.

Thus, if C is a circuit in the binary matroid $M(A_G)$, then the edges corresponding to C in the graph G form a cycle. □

Many algorithmic problems from computer science can also be expressed with matroids like this, allowing us to work with matrices. For example, in the minimum spanning tree problem, the objective is to find a tree that covers all the vertices, while minimizing or maximizing the sum of the weights along its edges. When translated into matroids, the spanning trees are just the bases, similar to how the circuits are equivalent to cycles!

5. Some Extensions of Matroids

Here we will introduce some useful operations and terminology for operating on matroids.

Definition 5.1. Let M be a matroid on the ground set E. Then the dual matroid M^* is a matroid on the same ground set E so that

$$\mathcal{B}(M^*) = \{E - B : B \in \mathcal{B}(M)\}$$

In other words, the bases of the dual are the complement of those in the original matroid, with respect to the ground set.

In many ways, this is analogous to the concept of a dual in graph theory, where, for example, a cube and an octahedron are duals; there is a vertex in the dual for every region, or face, in the original graph, and edges are drawn between faces adjacent in the original graph. This way, each edge in the old graph crosses exactly one edge in the new graph.

Minors are matroids that can be obtained from a starting matroid by specific operations, called restriction (or deletion) and contraction — both of which essentially take out an element:

Definition 5.2. A minor is a matroid N obtained from a starting matroid M by a sequence of restriction and contraction operations as defined below.

(1) **Restriction**: For $e \in E$ (e not an isthmus), the matroid $M - e$ has ground set $E - \{e\}$ and independent sets that are those members of $\mathcal{I}$ that do not contain e.
(2) **Contraction**: For $e \in E$ (e not a loop), the matroid M/e has ground set $E - \{e\}$ and independent sets that are formed by choosing all those members of $\mathcal{I}$ that contain e, and then removing e from each such set.

One reason minors are useful is because families of matroids can be characterized by which minors they have or cannot have — the theory of "excluded minors". A well-known theorem, given by Tutte, states that all matroids are regular if and only if they do not have any of 5 special matroids as minors: $U_{2,4}, F_7, F_7^*, M(K_5)^*, M(K_{3,3})^*$. $U_{2,4}$ is a uniform matroid, defined on a ground set of 4 elements where every subset with exactly 2 elements is a basis. Geometrically, it is just the four-point line. The proof of this theorem is beyond the scope of this paper, but can be found in [4].

Another useful characteristic of matroids is the Tutte polynomial, which is commonly used in graph theory. This polynomial is general enough that famous polynomials like the chromatic polynomial (counting graph colorings) and important problems like solutions for network flow (a directed graph with limited-capacity edges receiving "flows") can be expressed as specializations of it.

Definition 5.3. The Tutte polynomial $t(M; x, y)$ of a matroid M is defined recursively as follows:

(1) $t(M; x, y) = t(M - e; x, y) + t(M \setminus e; x, y)$ if e is neither an isthmus nor a loop;
(2) $t(M; x, y) = x \cdot t(M \setminus e; x, y)$ if e is an isthmus;
(3) $t(M; x, y) = y \cdot t(M - e; x, y)$ if e is a loop;
(4) $t(M; x, y) = 1$ if $E = \emptyset$.

6. Concluding Remarks

We have been using a geometric transformation to visualize matroids. Concepts from algebraic geometry formalize this idea, and extend it significantly to allow for new results in the world of matroids. While the cutting edge of the field requires some heavy previous knowledge, the fundamentals are summed up by the idea of the projective plane: a non-Euclidean geometry where Euclid's last postulate, that exactly one line parallel to another line passes through a point not on the other line, is negated: there are no parallel lines, as all lines intersect. We let points be purely represented by vectors, where in Euclidean geometry they might more accurately represent the line from the origin to a point. Once we have this basic structure, we can prove and apply other, much more elaborate geometric theorems.

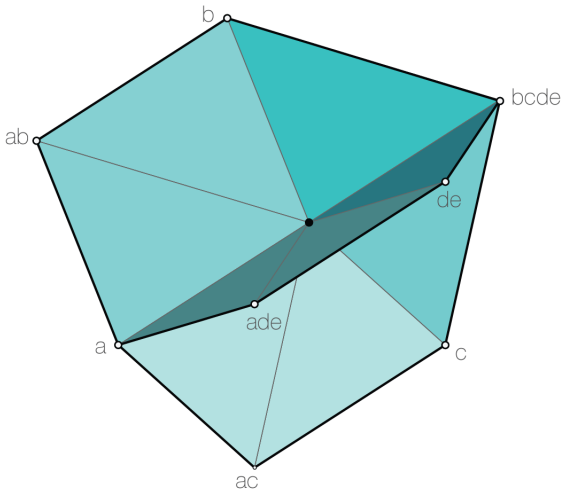

Figure 4. A Bergman fan corresponding to a matroid.

Some geometric configurations related to matroids can even yield results in very different areas. For example, using a three-dimensional hull made out of vectors derived from the bases of a matroid can allow techniques from linear programming to be applied, where a specific function has minimal values at the vertices; Jack Edmonds used this to solve the problem of finding the largest independent set shared between two matroids. There are also more advanced topics beyond the scope of this paper, including polytopes, fans, and tropical geometry applied on matroids. A significant amount of background is necessary to cover these complex, but very important results — the connections between matroids, combinatorics, and algebraic geometry are the focus of research by recent Fields Medal awardee June Huh. For a very thorough overview of the field, assuming a strong general background in algebraic geometry, one may consult [3].

References

[1] Anders Björner et al. *Oriented Matroids*. 2nd ed. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 1999. DOI: 10.1017/CBO9780511586507.
[2] Gary Gordon and Jennifer McNulty. *Matroids: A Geometric Introduction*. Cambridge University Press, 2012. DOI: 10.1017/CBO9781139049443.

[3] Eric Katz. *Matroid theory for algebraic geometers*. 2014. arXiv: 1409.3503 [math.AG].
[4] James Oxley. "372Excluded-Minor Theorems". In: *Matroid Theory*. Oxford University Press, Feb. 2011. ISBN: 9780198566946. DOI: 10.1093/acprof:oso/9780198566946.003.0011. eprint: https://academic.oup.com/book/0/chapter/297844218/chapter-pdf/40118906/acprof-9780198566946-chapter-11.pdf. URL: https://doi.org/10.1093/acprof:oso/9780198566946.003.0011.