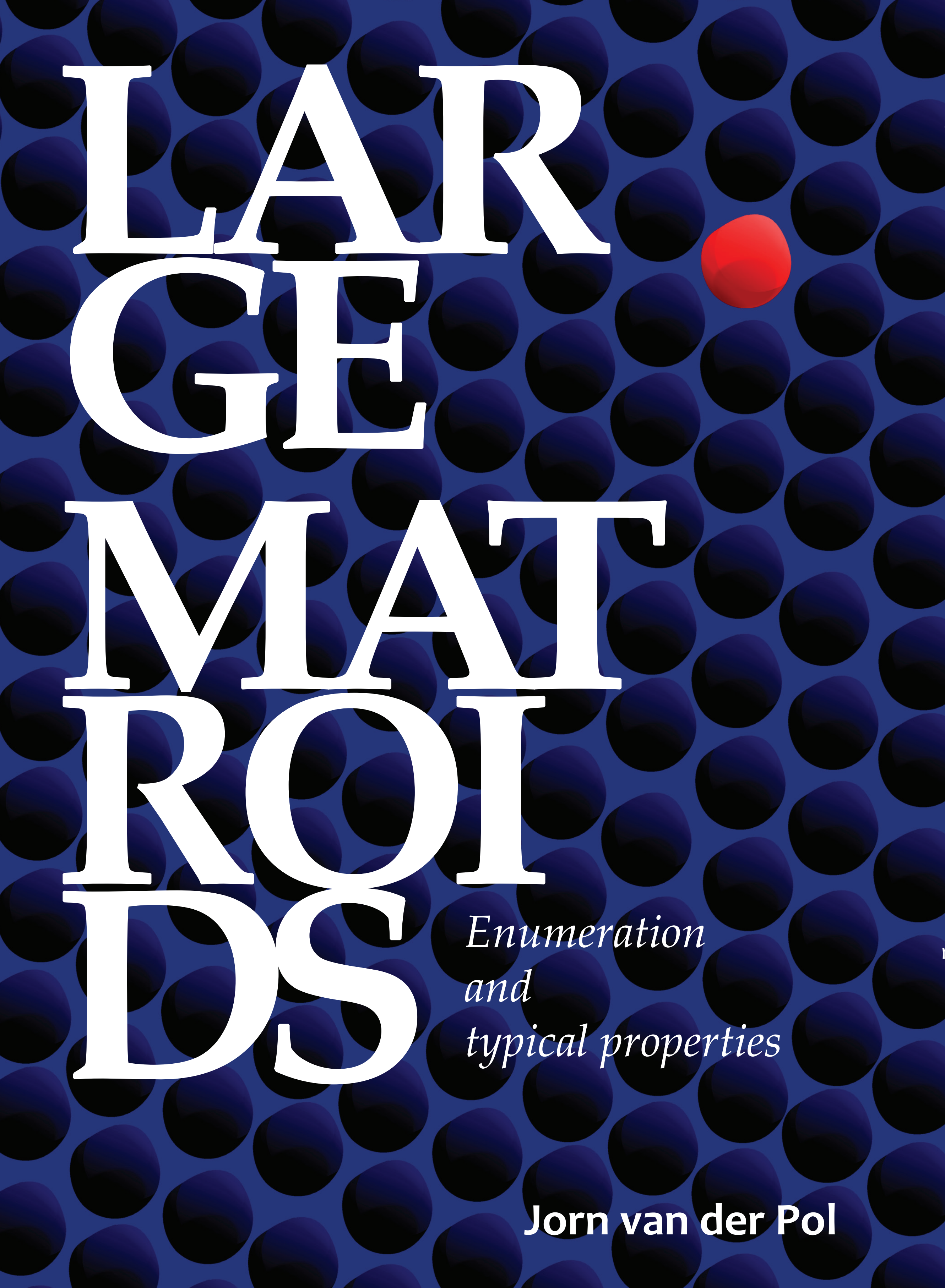
Large matroids



LARGE MATROIDS

Enumeration
and
typical properties

Jorn van der Pol

This research was supported by the Netherlands Organisation for Scientific Research (NWO) grant 613.001.211 (“Random matroids”).

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

ISBN: 978-90-386-4344-1

This document was typeset using the LaTeX document processing system originally developed by Leslie Lamport, based on TeX typesetting system created by Donald Knuth, using the memoir class created by Peter Wilson. Figures were created using the Ti*k*Z package by Till Tantau.

Printed by Ipskamp Printing.

Almost no matroids were harmed in the course of this research.

LARGE MATROIDS
ENUMERATION AND TYPICAL PROPERTIES

PROEFSCHRIFT

ter verkrijging van de graad van doctor aan de Technische Universiteit Eindhoven, op gezag van de rector magnificus prof. dr. ir. F.P.T. Baaijens, voor een commissie aangewezen door het College voor Promoties, in het openbaar te verdedigen op woensdag 20 september 2017 om 16:00 uur

door

Jorn Gerardus van der Pol

geboren te Noordoostpolder

Dit proefschrift is goedgekeurd door de promotoren en de samenstelling van de promotiecommissie is als volgt:

Voorzitter:	prof. dr. ir. B. Koren	
Promotor:	prof. dr. R.W. van der Hofstad	
Copromotor:	dr. R.A. Pendavingh	
Leden:	dr. A. Blokhuis	
	prof. dr. J.S.H. van Leeuwaarden	
	prof. dr. J.G. Oxley	*(Louisiana State University)*
	prof. dr. A. Schrijver	*(Centrum Wiskunde & Informatica/ Universiteit van Amsterdam)*
Adviseur:	dr. A.P. Nelson	*(University of Waterloo)*

Het onderzoek of ontwerp dat in dit proefschrift wordt beschreven is uitgevoerd in overeenstemming met de TU/e Gedragscode Wetenschapsbeoefening.

Summary

Large matroids: enumeration and typical properties

A matroid is an abstract geometrical configuration of points, lines, planes, and higher-dimensional analogues. Matroid theory is strongly tied to other areas of mathematics, such as linear algebra, graph theory, and the design and analysis of algorithms. Many objects that occur naturally throughout mathematics, such as graphs, vector spaces, and combinatorial designs, give rise to matroids. In addition, many combinatorial algorithms, such as Kruskal's algorithm for finding minimum-weight spanning trees in graphs, or finding maximal matchings in bipartite graphs, are special cases of matroid algorithms.

Matroids come with a notion of size: the cardinality of their ground set. This thesis focusses on large matroids, i.e. matroids whose ground set is large. It addresses two closely related problems: *asymptotic enumeration* and identification of *typical properties.*

Enumeration is a central problem in discrete mathematics. In this thesis, it pertains to obtaining good upper and lower bounds on the number of matroids on a given ground set (and given rank) as a function of its size.

There is a close relationship between enumeration and descriptive complexity. To illustrate this connection, suppose that a description of k bits suffices to describe a matroid of given size. As there are 2^k bit strings of length k, this immediately implies that there are at most 2^k matroids of that size.

In this thesis, matroid enumeration is approached by exploiting this connection. If a matroid can be encoded as an object whose complexity is known, then this complexity translates to an upper bound on the number of matroids. If such a description is concise, then the resulting upper bound is close to the actual number of matroids. Several such encoding schemes are considered:

- A method of describing a matroid as the sequence of its truncations, in which every term is generated as an erection of the previous term using a small amount of additional information. The resulting upper bound, combined with a matching lower bound, gives rise to a good approximation of the numer of matroids of fixed rank.

- A method of describing any matroid as a stable set in the Johnson graph, augmented with a relatively small amount of additional information. This method results in an improved upper bound on the number of matroids which, on logarithmic scale, comes within a factor $2 + o(1)$ of the best known lower bound.

In addition, several general methods for transferring enumeration results for matroids of fixed rank to matroids of general rank are developed.

A matroid property is typical if it is satisfied by all but a vanishing fraction of matroids on a given ground set. In discrete probability theory, this is sometimes expressed as "almost every matroid satisfies property X", or even "the random matroid satisfies property X". There is a large body of work on random discrete objects such as random graphs and random matrices. By contrast, the picture for random matroids is relatively bleak: although there is a large number of conjectured typical properties, results are scarce.

In this thesis, the relation between complexity and enumeration is used to provide a crude but effective method to prove that certain properties are typical. If absence of a certain property allows for more concise descriptions, then it implies a bound on the number of matroids not satisfying the property that is stronger than the enumeration result. If this effect is sufficiently strong, then it follows that the property is typical. Using this type of reasoning, the following results are proved:

- Almost every matroid has high girth and high connectivity.

- Almost every matroid has an automorphism group that is generated by at most one transposition.

- Almost every matroid has a number of bases that is between a $\Omega(1/n)$ and an $O\left(\log^3 n/n\right)$ fraction of r-subsets, and has rank asymptotic to half its size.

- Almost every matroid contains an N-minor, if N is either a uniform matroid or one of several small matroids.

Acknowledgements

It is my pleasure to acknowledge the support of many people without whom the completion of this thesis would not have been possible.

First and foremost, I would like to thank my advisor, Rudi Pendavingh. Rudi is one of the most versatile mathematicians and one of the most enthusiastic people that I know. Rudi, thank you for your positive attitude, for guiding me through this journey, for teaching me everything I know about matroids, for the opportunity to develop my own supervision skills, and for the many inspiring discussions. I thoroughly enjoyed working with you over the past six years.

About six years ago, I was first set on the path to random matroids by Remco van der Hofstad, my promotor, when I came to him looking for a graduation project. Working on a multidisciplinary project such as this is challenging at times, and I am amazed by Remco's perseverance and his ability to contribute to a topic that is relatively foreign to him. Remco, thank you for the insightful discussions, your patient explanations, and your support.

I feel honoured to have Aart Blokhuis, Barry Koren, Johan van Leeuwaarden, Peter Nelson, James Oxley, and Lex Schrijver on my committee. Thank you for travelling to Eindhoven and for your comments on my thesis. A special word of thanks to James Oxley, who not only commented on the mathematical content of my thesis, but also provided me with a detailed list of spelling and grammar mistakes. His effort allowed me to vastly improve the exposition in this thesis.

Thanks to Nikhil Bansal, who co-authored two of the papers on which this thesis is based, for co-advising me on my Master's thesis and for giving me the opportunity to improve my teaching skills by teaching part of his Master's level course.

Thanks to Johan van Leeuwaarden, who has been an unofficial advisor throughout my academic career. He helped me take the first steps in mathematical research when I was studying for my Bachelor's degree, gave me the opportunity to develop my teaching skills when I was doing my Master's, and he invited me along to interesting outreach activities during my PhD.

Thanks to Stefan van Zwam and Peter Nelson, for their generous hospitality during my visits to, respectively, Louisiana State University and the University of Waterloo.

Thanks to the members of our small but lively "matroid trio" seminar, Guus Bollen and Rudi Pendavingh.

Many people made my stay at TU/e a pleasant one. You know who you are, and I hope you will forgive me for not mentioning you all by name. Thanks to Aleks, Gunjan, Łukasz, Marek, and William for the pleasant atmosphere in our shared office. Thanks to Aleks for our shared love of kvetching and the pleasantries of life.

Thanks to my family and friends, for their continuous friendship and support. In particular to Elisa, who had to put up with an increasing pile of books and papers on the kitchen table, who helped me with all sorts of practical matters including the design of the cover, and who stood by me throughout the highs and lows of this endeavour.

Jorn van der Pol
Toronto, August 2017

Contents

CHAPTER 1

Introduction

1.1 Matroids

Matroids emerged in the 1930's as a common abstraction of a number of mathematical objects. In his seminal paper [Whi35], Whitney observed a number of key properties shared by independent vectors in a vector space, and spanning trees in graphs. He named set systems satisfying these properties *matroids*.

In terminology that we will use in this thesis, a matroid is a set system $(E, \mathcal{B})$ on a finite ground set E, in which the collection of *bases*, $\mathcal{B}$, is a non-empty collection of subsets of E satisfying the basis-exchange axiom

$$\begin{aligned}&\text{For all } B, B' \in \mathcal{B}, \text{ and for all } b \in B \setminus B',\\ &\qquad\text{there exists } b' \in B' \setminus B \text{ such that } (B \setminus \{b\}) \cup \{b'\} \in \mathcal{B}.\end{aligned} \tag{1.1}$$

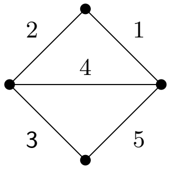
Let us consider two examples of matroids, that serve to illustrate the diverse background of matroid theory.

The first example is that of a representable matroid. Let A be a matrix over some field $\mathbb{F}$, and suppose that its columns are indexed by E. If $\mathcal{B}$ is the collection of indices such that the corresponding columns form a basis of the column space of A, then $\mathcal{B}$ satisfies (1.1). (In this setting, (1.1) follows from an application of the Steinitz exchange lemma.) Thus, matrices give rise to matroids, and matroids arising in this way are called *representable* or *linear*. (Incidentally, this example explains the origin of the term “basis”.)

The second example is that of a graphic matroid. If $G = (V, E)$ is a graph, and $\mathcal{B}$ is the collection of subsets of E that inclusionwise-maximal acyclic subgraphs (forests) in G, then $\mathcal{B}$ satisfies (1.1). This can be seen by removing the edge b from G, and then greedily extending $B \setminus \{b\}$

$$\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ \end{array}$$
$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

(a) A matrix over the binary field.



(b) A graph.

Figure 1.1: A linear and a graphic representation of the same matroid: the matroid has ground set $E = \{1, 2, 3, 4, 5\}$, whose bases are all 3-subsets except $\{1, 2, 4\}$ and $\{3, 4, 5\}$.

to a maximal acyclic subgraph of $G' = (V, E \setminus \{b\})$. Thus, graphs give rise to matroids as well, and matroids arising from graphs in this way are called *graphic*. See Figure 1.1 for an example of a matroid that has both a linear and a graphic representation.

Graphic and linear matroids are the two examples that Whitney provided in [Whi35]. Several other authors observed similar properties in different situations, such as lattices, algebraic geometry, and geometry. Kung [Kun86] reprints and comments on many of these historical papers, while Schrijver [Sch03, Chapter 39.10b] provides historical notes and connections to earlier work.

In the 1950's and 1960's, interest in matroid theory grew rapidly after their strong ties with discrete optimisation were discovered. Suppose that the elements of the ground set E each have a weight. Generalising Kruskal's algorithm for finding maximum spanning trees, a greedy algorithm can be used to find a basis of maximum weight in the matroid. One striking observation is that matroids are precisely those hereditary structures for which the greedy algorithm works, no matter how the elements are weighted (cf. [Oxl11, Section 1.8], [Sch03, Chapter 40]).

More generally, finding a maximum-weight independent set in the intersection of two matroids can be solved efficiently, due to the matroid intersection theorem by Edmonds [Edm70]. (The problem becomes NP-hard when three matroids are involved.) Matroid intersection contains as special cases the problem of finding maximal matchings in bipartite graphs, and arborescences in directed graphs. A brief account of these first connections between matroids and combinatorial optimisation can be found in Cunningham [Cun12].

More recently, matroids have become more popular in the study of various algorithmic problems, such as mechanism design (see e.g. [BIK07, FGH$^+$17]) and coding theory (see e.g. [Kas08]).

1.2 Large matroids

Reflecting the advent of data science and the emergence of large networks, working with huge discrete objects has become increasingly commonplace. One can think of large networks (graphs), such as the world wide web, protein interaction networks, and chip design [Lov12, vdH16], and large matrices, prevalent in applications such as statistics and machine learning.

This thesis deals with large matroids. More precisely, we focus on matroids on a ground set of cardinality n, and study their properties as n tends to infinity. The type of result that we are interested in, will be of the form "a typical matroid has property Π". Here, "typical" means that, as n tends to infinity, we allow for a vanishing proportion of matroids to fail property Π.

The results in this thesis fit in three themes, which themselves are strongly interrelated.

Enumeration

Enumeration, or counting, is a central problem in discrete mathematics.

Enumeration of matroids started in the 1960's. Crapo [Cra65] described a theory of extensions of matroids, which allowed him to show that there are at least 2^n non-isomorphic matroids on a ground set of n elements. Following an earlier, unpublished, enumeration of matroids up to 7 elements by Higgs, Blackburn, Crapo, and Higgs [BCH73] published a catalogue of matroids[1] on at most 8 elements. They obtain 950 such matroids on 8 elements. Their catalogue was not extended until this century, when Mayhew and Royle [MR08] extended it with the matroids on 9 elements. They obtained 383172 non-isomorphic matroids on that number of elements, of which a majority of 376467 are simple.

Write $m(n)$ for the number of matroids on ground set $[n]$. As each matroid is a set system, we obtain the easy upper bound $m(n) \leq 2^{2^n}$. Piff and Welsh [PW71] were the first to show that this double-exponential growth is essentially the right behaviour of $m(n)$, by constructing a family of non-isomorphic matroids on n elements that contains at least $n^{2^n n^{-5/2}}$ matroids. The fast growth of the number of matroids is hence not surprising, and computing catalogues of even larger matroids than the ones considered by Mayhew and Royle will be increasingly unwieldy.

[1] Strictly speaking: non-isomorphic, simple matroids. This terminology will be explained in the next chapter.

The best lower bound on $m(n)$ for large n to date follows from a bound in coding theory by Graham and Sloane [GS80] or Kløve [Klø81]. The relation between these results and matroid theory was realised by Mayhew and Welsh [MW13], who used it to prove that

$$\log m(n) \geq \frac{1}{n}\binom{n}{n/2} = \Theta\left(\frac{2^n}{n\sqrt{n}}\right).$$

The bound is obtained by constructing a large collection of so-called *sparse paving matroids*, or equivalently, a large stable set in the *Johnson graph*. Sparse paving matroids and the Johnson graph will play a central role in this thesis, and their connection is explored in Section 2.6.

In the other direction, Piff [Pif73] proved that

$$\log m(n) \leq O\left(\frac{2^n \log n}{n}\right).$$

There is a gap of size $O(\sqrt{n}\log n)$ between the upper bound and lower bound on $\log m(n)$. One of the results in this thesis is an improvement of the upper bound to within a factor $2 + o(1)$ of the lower bound.

Structure and complexity

The complexity of an object is, loosely speaking, the length of a shortest description of that object. There is a strong connection between complexity and enumeration: If all objects in a certain class are uniformly non-complex, then the class is necessarily small, since there is only a bounded number of descriptions of a certain length.

Prescription (or avoidance) of structure may have a profound effect on an object's complexity, and hence on enumeration results, even if the prescribed structure is of a very local nature. Consider the following illustrative, if somewhat contrived, example. Let Σ_n be the class of binary strings of length n. Often, the shortest description of an element in Σ_n is the string itself, so objects in Σ_n tend to be fairly complex. This is reflected in its cardinality: $|\Sigma_n| = 2^n$. On the other hand, for the subclass $\Sigma'_n \subseteq \Sigma_n$ of strings avoiding the simple local structure 10 (i.e. a 1 followed by a 0) ensures that each object can be described by a single natural number $\ell \in \{0, 1, \dots, n\}$, e.g. indicating the number of zeroes in the string. Thus, avoiding the substring 10 reduces the complexity drastically; again, this is reflected in the cardinality of Σ'_n: $|\Sigma'_n| = n + 1$.

More profound examples can be found in the area of graph theory. For example, if H is any fixed graph, then a sufficiently large random graph contains H as a subgraph (with probability close to 1) [JŁR00, Theorem 3.4], so excluding H as a subgraph necessarily reduces complexity. Similarly, it was shown in [NSTW06] that every proper minor-closed class of graphs is small, and hence particular graphs in such a class have relatively small complexity.

Randomness

Random discrete structures form perhaps the most natural setting for questions about typical structure, and there are many examples.

Perhaps the most well-known example of random discrete structures is the random graph. In its simplest form, the random graph $\boldsymbol{G}(n, p)$ consists of n labelled vertices, in which all edges are present with probability p, independently of all other edges. Since its inception by Erdős and Rényi [ER59, ER60] and Gilbert [Gil59], random graph theory has blossomed into a thriving area with a rich body of results and different models of random graphs, catering to a wide range of modelling situations (cf. [JŁR00, vdH16]).

A similarly simple model exists for random matrices over finite fields. One can construct, for example, a random rectangular matrix $\boldsymbol{A}_{m\times n}(\mathbb{F})$, whose entries are chosen from the finite field $\mathbb{F}$, randomly and independently from all other entries. This model is surveyed by Blake and Studholme [BS06]. A related model is the so-called Bernoulli ensemble, $\boldsymbol{A}_{m\times n}(\pm 1)$, in which the entries are random ± 1-values, see [TV07]. Such random matrices are in one-to-one correspondence with random directed graphs.

Although matroids generalise both graphs and matrices, to date only few results on random matroids exist. Mayhew, Newman, Welsh, and Whittle [MNWW11] comment:

> “Indeed, there are almost no results on the asymptotic behaviour of classes of matroids. This seems to be due to the lack of a successful model of a random matroid.”

Both random graphs and random matrices over finite fields admit a representation as a product probability space. Loosely speaking, a random graph can be obtained by tossing a coin for each edge, and including only these edges for which the coin came up heads. A random matrix can be constructed similarly, by choosing its elements one at a time. By contrast, matroids do not have such a straightforward construction. For example, one cannot select a random collection of subsets of $[n]$ and hope that these satisfy the basis-exchange axiom.[2]

Knuth [Knu75] described a construction of matroids that is capable of generating an arbitrary matroid, and commented that by randomising the choices made in his construction, in principle a random matroid can be constructed. Analysis of his algorithm remains an open question. Attempts to analyse random representable matroids have been more fruitful, see e.g. the works by Oxley [Oxl84], Kelly and Oxley [KO82b, KO82a, KO84], Kordecki [Kor88, Kor95, Kor96], Kordecki and Łuczak [KŁ91, KŁ99], Altschuler and Yang [AY17], and Cooper, Frieze, and Pegden [CFP17].

We close this section by mentioning two recent results in the area of random matroid theory. Both results show that a certain algorithm works well on a random (or typical) instance, while the worst-case behaviour is either unknown or bad.

- The matroid secretary problem [BIK07] is a generalisation of the classical secretary problem. Huynh and Nelson [HN16] recently proved that a particular randomised algorithm is $O(1)$-competitive for a typical matroid, while the best known result for all matroids is $O(\log\log r)$-competitive [Lac14].
- Counting the number of bases of a matroid is a problem that contains, as a special case, enumeration of spanning trees in connected graphs. Although counting spanning trees can be done in polynomial time by Kirchhoff's matrix-tree theorem, the problem of counting bases in a matroid[3] is $\sharp P$-hard. In addition, Azar, Broder, and Frieze [ABF94] proved that it is not even possible to obtain an accurate approximation of the number of bases in deterministic polynomial time. By contrast, Cloteaux [Clo10], building on work by Chávez Lomeli and Welsh [CLW96], showed that the number of matroids can be effectively approximated for a typical matroid.

1.3 In this thesis

In this section, we provide an overview of some of the open questions concerning large matroids. The questions presented here fit roughly

[2] This procedure will in fact produce a random matroid. However, the chance of success is extremely slim, and hence not useful for any practical applications. At the same time, the approach gives little possibility for a successful probabilistic analysis.

[3] Presented by an independence oracle

in three overarching themes: enumeration, minor-closed classes, and connectivity. Most of the conjectures presented below can be found in Mayhew, Newman, Welsh, and Whittle [MNWW11].

Most of the conjectures are phrased as “almost every matroid satisfies property Π”. This phrase is used in the precise meaning that the fraction of matroids on ground set $E = [n]$ that satisfy property Π tends to 1 as n tends to infinity.

Theme I: Enumeration

A central role in this thesis is played by several enumerative results. A central question in the area of large matroids is the following. Write $m(n)$ for the number of matroids on ground set $[n]$.

Question 1.3.1. *What is the asymptotic behaviour of $m(n)$?*

Given a matroid M, it can be shown that each basis of the matroid M has the same cardinality, which is called the *rank* of M. Write $m(n, r)$ for the number of matroids of rank r on ground set $[n]$. Then one could similarly consider the asymptotic behaviour of $m(n, r)$, for example when r is a fixed constant or grows linearly in n.

The function $m(n)$ is roughly doubly exponential in n. This was first shown by Piff and Welsh [PW71], who constructed a large family of so-called sparse paving matroids.Later, an even larger family of such sparse paving matroids was constructed by Knuth [Knu74], which was again improved by Graham and Sloane [GS80] and Kløve [Klø81] (we consider their construction in Section 2.8).

Mayhew, Newman, Welsh, and Whittle [MNWW11, Conjecture 1.6] conjecture that almost every matroid is a so-called paving matroid, and note that this is equivalent to the following (seemingly stronger) conjecture.[4]

Conjecture 1.3.2. *Almost every matroid is sparse paving.*

Sparse paving matroids are very benign objects compared to general matroids, and an affirmative answer to Conjecture 1.3.2 would be a very powerful result. Indeed, several hard conjectures, that have not yet

[4] Versions of the conjecture date back to the 1970’s. Based on a catalogue of matroids on up to 8 elements by Blackburn, Crapo, and Higgs [BCH73], Crapo and Rota consider it likely that paving matroids “would actually predominate in any asymptotic enumeration of [matroids]” [CR70, p. 3.17], while Welsh [Wel76, Ex. 3.2.3] asks whether the predominance of paving matroids among small matroids holds in general. Mayhew and Royle [MR08] confirmed that the paving matroids still predominate among matroids on 9 elements.

been proved for general matroids, have been proved for (sparse) paving matroids [Bon13, GH06, Jer06, MNRIVF12]. Conjecture 1.3.2 would immediately imply that each of these conjectures hold for almost every matroid.

Noting that $m(n,r) = m(n,n-r)$ for all $0 \leq r \leq n$, Welsh asked if more of a 'binomial character' is visible in the sequence $\{m(n,r) : 0 \leq r \leq n\}$. For example, is the sequence unimodal [Wel71, P19], and does it assume its maximum when $r = \lfloor n/2 \rfloor$ [Wel71, P20]?[5] Mayhew, Newman, Welsh, and Whittle propose that Welsh's problem P20 holds in the following strong sense.

Conjecture 1.3.3 ([MNWW11, Conjecture 1.10])**.** *Almost every matroid satisfies* $\operatorname{rk}(M) \in \left\{ \left\lfloor \frac{|M|}{2} \right\rfloor, \left\lceil \frac{|M|}{2} \right\rceil \right\}$.

An automorphism of a matroid is a permutation of its ground set that maps bases to bases and nonbases to nonbases. A matroid is asymmetric if the identity permutation is its only automorphism.

Conjecture 1.3.4 ([MNWW11, Conjecture 1.2])**.** *Almost every matroid is asymmetric.*

The conjecture would imply that for every property Π that does not depend on the labelling of the elements of the matroid, almost every matroid satisfies Π if and only if almost every unlabelled matroid does.

Theme II: Minor-closed classes

A matroid N is a *minor* of a matroid M if it can be obtained from M by a sequence of deletions and contractions of elements. We postpone a formal definition to Chapter 2, noting here that minors in matroids generalise the notion of minors in graphs. A class of matroids is called minor-closed if it is closed under taking minors and under relabelling of elements. Minor-closed classes can be described by listing their excluded minors: these are the matroids that themselves are outside the class, while all of their proper minors are in the class. A prototypical such *excluded-minor characterisation* in graph theory is Wagner's theorem, which identifies the planar graphs as those graphs that have neither K_5 nor $K_{3,3}$ as a minor (cf. [Die16, Theorem 4.4.6]), while a classical such characterisation in matroid theory is Tutte's characterisation of the binary matroids (matroids that are representable over the binary

[5] Actually, Welsh asksed these questions concerning non-isomorphic matroids.

field) as those matroids that do not have the uniform matroid $U(2,4)$ as a minor (cf. [Oxl11, Theorem 9.1.3]).

Mayhew, Newman, Welsh, and Whittle make the following striking conjecture about the pervasiveness of sparse paving matroids.

> **Conjecture 1.3.5** ([MNWW11, Conjecture 1.7])**.** *Let N be a sparse paving matroid. Almost every matroid has an N-minor.*

They isolate $N = V_8$, the Vámos matroid, as a case of special interest [MNWW11, Conjecture 1.8]. As V_8 is not representable over any field, an affirmative answer to Conjecture 1.3.5 would imply an affirmative answer to the following conjecture.

> **Conjecture 1.3.6** ([MNWW11, Conjecture 1.9])**.** *Almost every matroid is not representable over any field.*

Conjecture 1.3.6 was recently proved by Nelson [Nel16], using a different approach than suggested by Mayhew, Newman, Welsh, and Whittle.

Since V_8 is not algebraic over any field (which is stronger than non-representability), an affirmative answer to Conjecture 1.3.5 would also imply an affirmative answer to the following (stronger) conjecture.

> **Conjecture 1.3.7.** *Almost every matroid is not algebraic over any field.*

Theme III: Connectivity

A matroid is k-connected, roughly, if it cannot be broken into smaller pieces across small separations, similar to the way a k-connected graph cannot be broken into smaller pieces by removing few edges. Connectivity plays a pivotal role in matroid structure theory.

> **Conjecture 1.3.8** ([MNWW11, Conjecture 1.5])**.** *Let $k > 1$. Almost every matroid is k-connected.*

The special cases $k = 2$ and $k = 3$ of Conjecture 1.3.8 were proved by Lowrance, Oxley, Semple, and Welsh [LOSW13, Theorem 4.2].

1.4 Outline

Finishing the introduction, we briefly sketch the contents of the remaining chapters.

Enumeration and concise descriptions

Here, we sketch the relation between enumeration and structural complexity, which plays a central role in this thesis.

Suppose that we are interested in enumeration of the set $\mathcal{X}$. If there exists an injective function $f\colon \mathcal{X} \to \mathcal{Y}$, then we refer to f as an *encoding* of the elements of $\mathcal{X}$, and for we may call $f(X)$ a *description* of $X \in \mathcal{X}$. It is important to note that, in this context, A is *uniquely determined* by $f(A)$.

If f is an encoding of $\mathcal{X}$, then clearly $|\mathcal{X}| \leq |\mathcal{Y}|$. Therefore, the cardinality of $\mathcal{Y}$ provides an upper bound for the enumeration problem that we are interested in. Obviously, such a result is most useful if $\mathcal{Y}$ is not much larger than $\mathcal{X}$. This means that we are particularly interested in descriptions that are not only faithful, but also *concise*.

This idea is related to data compression, which is the encoding of information using fewer bits than the original representation. Such data compression is obtained by eliminating redundant information.

A large part of this thesis is dedicated to the elimination of redundant information from matroid descriptions, thus leading to concise descriptions.

Chapter 2 — Preliminaries

In Chapter 2, we establish notation and review most of the background material that is required for reading the thesis. In particular, we provide a brief introduction to matroid theory and describe the Johnson graphs, which also play a major role in this thesis.

Chapter 3 — Entropy

The entropy of a random variable is a measure for the uncertainty in any realisation. Entropy methods can be used to prove many results in discrete mathematics. In particular, Shearer's Entropy Lemma is useful for bounding the entropy of random variables in terms of projections into lower-dimensional subspaces. In Chapter 3, we use Shearer's Entropy Lemma to provide bounds on the number of matroids in a class in terms of their deletions and contractions. This allows us to bound the number of matroids in a certain class in terms of bounds on the number of matroids of a certain fixed rank in such a class.

Chapter 4 — Cover complexity

In Chapter 4, we introduce cover complexity as the minimal size of a certain faithful description of matroids. Cover complexity is a measure of structural complexity of a matroid. We show how a bound on the cover complexity of the matroids in a class implies a bound on the size of that class.

We prove a technical result that can be used to translate bounds on the cover complexity of matroids of a certain fixed rank in a minor-closed class of matroids to a bound on the size of that class, and use this result that several minor-closed classes are small.

Chapter 5 — Enumeration of matroids of fixed rank

In Chapter 5, we turn our attention to matroids of fixed rank. We show how every matroid can be encoded as a stack of paving matroids of increasing rank, and use this to obtain enumerative results. Our method shows that essential flats and their ranks give a concise description of matroids. In addition, we obtain strong bounds on the number of paving and sparse paving matroids of fixed rank.

Chapter 6 — Enumeration of matroids

Recently, the container method has found successful application in the enumeration of discrete structures such as stable sets in graphs. Sparse paving matroids can be described as such a stable set, and in Chapter 6 we use the container method to obtain an upper bound on the number of sparse paving matroids that is the square of the best lower bound.

Next, we combine the container method with some of the cover complexity results from Chapter 4 to obtain a variant of the container method that can deal with general matroids as well. This extension results in a bound on the number of matroids that is qualitatively the same as that on the number of sparse paving matroids.

In addition, a careful analysis of the method implies that most matroids have few non-bases.

Chapter 7 — Typical properties

In Chapter 7, we prove a lower bound on the likely number of bases that is complementary to the upper bound obtained in Chapter 6. As a corollary, we obtain, with relatively little additional effort, some of the strongest results in asymptotic matroid theory in this thesis. In particular, we show that most matroids have arbitrarily large uniform minors, arbitrarily high connectivity, arbitrarily high girth, and do not arise as the truncation of another matroid. In addition, we show that most matroids have an automorphism group that is either trivial or generated by a single transposition.

Chapter 8 — Discussion and future work

In this thesis a number of open questions about the structure of large matroids are answered. Many other questions remain open; perhaps the most striking of these is that of asymptotic enumeration. In Chapter 8, we consider a number of remaining questions, and indicate directions in which the results in this thesis may be extended.

CHAPTER 2

Preliminaries

In this chapter, we establish some basic notation, and introduce the protagonists of this thesis: matroids, and the Johnson graph.

In this chapter, we restrict our attention to notation and results that play a role throughout the thesis. Where, in later chapters, additional results are required that are local to that chapter, such result are introduced there.

The remainder of this chapter is organised as follows. In Section 2.1, we define some basic notation, and in Section 2.2, we review some bounds on binomial coefficients. In Section 2.3, we define matroids, and review some definitions and results that are used throughout this thesis. In Section 2.4–2.5, we define matroid classes, and give a precise definition of the phrase "almost every matroid". In Section 2.6, we introduce the Johnson graph, which in Section 2.7 is related to sparse paving matroids and Steiner systems. Finally, in Section 2.8, we review the best known lower bounds on the number of matroids.

2.1 Notation

Sets

$\mathbb{Z}$ ($\mathbb{Z}_{\geq 0}$, $\mathbb{Z}_{>0}$) denotes the set of integers (nonnegative integers, positive integers), and we write $\mathbb{Z}_n$ for the integers modulo n. In addition, $\mathbb{R}$ denotes the real number field.

For an integer $n \geq 1$, we write

$$[n] := \{1, 2, \dots, n\}.$$

If E is a set, then we write $\mathscr{P}(E)$ for its power set, and

$$\binom{E}{r} := \{X \in \mathscr{P}(E) : |X| = r\}$$

for the subsets of cardinality r, and similarly $\binom{E}{\leq r}$ for the subsets of cardinality at most r.

$A \triangle B$ denotes the symmetric difference between the sets A and B.

Throughout this thesis, we work with sets, as well as collections of subsets. Generally, sets are denoted by capital letters (e.g. $X \subseteq E$ if X is a subset of E), while collections of subsets are denoted by calligraphic letters (e.g. $\mathcal{B} \subseteq \binom{E}{r}$ indicates that $\mathcal{B}$ is a collection of r-subsets of E). In addition, the letters $\mathcal{M}$ and $\mathcal{N}$ are used for classes of matroids.

An *antichain* in $\mathscr{P}(E)$ (strictly speaking: in the lattice of subsets of E, partially ordered by inclusion) is a collections $\mathcal{A} \subseteq \mathscr{P}(E)$ with the property that for $A_1, A_2 \in \mathcal{A}$ with $A_1 \subseteq A_2$, then $A_1 = A_2$. Thus, no element of $\mathcal{A}$ is properly contained in another.

Graphs

A graph is a pair $G = (V, E)$, in which V is a finite set of *vertices*, and E is a set of unordered pairs of elements of V, which are called *edges*. An edge $\{u, v\} \in E$ is called incident on the vertices u and v. If $\{u, v\}$ is an edge, then we write $u \sim v$, and say that u and v are *adjacent* or *neighbours*; additionally, we say that u and v are the ends of the edge $\{u, v\}$. If $v \in V$, then we write $N(v) := \{w \in V : v \sim w \in E\}$ for its neighbourhood. More generally, for subsets $U \subseteq V$, we write $N(U) := \bigcup_{u \in U} N(u)$.

The degree $d(v) := |N(v)|$ of the vertex v is the number of edges incident to v. We shall write $\delta(G)$ for the minimum degree in G, and $\Delta(G)$ for the maximum degree in G. The graph G is called *regular* if $\delta(G) = \Delta(G)$, and we say that it is d-regular if this common value is d.

If U and U' are disjoint subsets of V, then we write $\nabla(U, U')$ for the set of edges with exactly one of their ends in U and U' each.

If $A \subseteq V$, then we write $G[A]$ for the subgraph *induced* by A; this is the subgraph of G obtained by restricting its vertex set to A, and its edge set to those edges that are subsets of A.

A *stable set*[1] in G is a subset $I \subseteq V$ of which the elements are pairwise nonadjacent. We write $\mathrm{Ind}(G)$ for the collection of all stable

[1] Stable sets are often called *independent sets* in graph theory. As “independent set” has a different meaning in matroid theory, our using of the phrase “stable set” in its stead serves to avoid confusion.

sets in G, and $\mathrm{ind}(G) = |\,\mathrm{Ind}(G)\,|$ for the cardinality of this collection. When necessary, we shall adorn this notation with extra parameters; for example, $\mathrm{ind}(G, \leq k)$ denotes the number of stable sets of cardinality at most k in G.

A maximum stable set is a stable set of maximum size; if I is such a maximum stable set, then we write $\alpha(G) := |I|/|V|$ for the *stability ratio*. A stable set is *maximal* if there is no stable set that strictly includes it.

The *adjacency matrix* of G is a $\{0,1\}$-matrix A, whose rows and columns are indexed by V, that encodes the edges of G by putting $A(u,v) = 1$ if and only if u and v are adjacent. The *eigenvalues* of G are the eigenvalues of its adjacency matrix; spectral graph theory studies graphs through their adjacency matrices.

A *hypergraph* is a generalisation of a graph, in which the edges can be subsets of the vertices of any cardinality. If all edges have the same cardinality u, then the hypergraph is called u-uniform; e.g. a graph is just a 2-uniform hypergraph. As in ordinary graphs, the degree of a vertex is the number of edges in which it is contained, and a hypergraph is called d-regular if each of its vertices is contained in exactly d edges.

Probabilistic notation

We require only basic probability theory. Our notation generally follows [GW14], to which we refer for a more extensive treatment of the notions mentioned here.

We write $\mathbb{P}$ for probability measures, and $\mathbb{E}$ for expected values, and we use subscripts to stress dependence on some parameter. Random variables are denoted by boldface symbols.

For any event A, we write $\overline{A} := \Omega \setminus A$ for the complementary event.

Events A and B are called independent if $\mathbb{P}(A \cap B) = \mathbb{P}(A)\,\mathbb{P}(B)$; more generally, a finite collection of events $\{A_i : i \in [n]\}$ is called mutually independent if $\mathbb{P}(\cap_{i=1}^n A_i) = \prod_{i=1}^n \mathbb{P}(A_i)$. Similarly, a finite collection of random variables, $\{\boldsymbol{X}_i : i \in [n]\}$ is mutually independent if the corresponding events $\{\boldsymbol{X}_i \in S_i\}$ are mutually independent, for all choices of $\{S_i : i \in [n]\}$.

If A and B are events such that $\mathbb{P}(B) > 0$, then the *conditional probability* of A given B is

$$\mathbb{P}(A \mid B) := \frac{\mathbb{P}(A \cap B)}{\mathbb{P}(B)}.$$

The *law of total probability* states that if $\{B_i\}$ is a countable partition of the underlying probability space, then

$$\mathbb{P}(A) = \sum_i \mathbb{P}(A \cap B_i) = \sum_i \mathbb{P}(A \mid B_i)\,\mathbb{P}(B_i)\,.$$

The following formula is known as the *chain rule* for probabilities:

$$\mathbb{P}\left(\bigcap_{i=1}^{n} A_i\right) = \prod_{i=1}^{n} \mathbb{P}\left(A_i \,\middle|\, \bigcap_{i'<i} A_{i'}\right).$$

If $\boldsymbol{X}$ and $\boldsymbol{Y}$ are random variables, then the conditional expectation of $\boldsymbol{X}$ given $\boldsymbol{Y}$ is denoted by $\mathbb{E}[\boldsymbol{X} \mid \boldsymbol{Y}]$. The *law of total expectation* states that

$$\mathbb{E}[\boldsymbol{X}] = \mathbb{E}[\mathbb{E}[\boldsymbol{X} \mid \boldsymbol{Y}]]\,.$$

Linearity of expectation refers to the property that, for $n \in \mathbb{Z}_{>0}$,

$$\mathbb{E}\left[\sum_{i=1}^{n} \boldsymbol{X}_i\right] = \sum_{i=1}^{n} \mathbb{E}[\boldsymbol{X}_i]\,,$$

provided all the expectations involved are finite.

Asymptotic notation

We use the Bachmann-Landau symbols $o(\cdot)$, $O(\cdot)$, $\Theta(\cdot)$, and $\Omega(\cdot)$ to denote asymptotics:

- $f(n) = o(g(n))$ as $n \to \infty$ means that $g(n) > 0$ and $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0$;
- $f(n) = O(g(n))$ as $n \to \infty$ means that $g(n) > 0$ and $\limsup_{n\to\infty} \frac{f(n)}{g(n)} < \infty$;
- $f(n) = \Theta(g(n))$ as $n \to \infty$ means that both $f(n) = O(g(n))$ and $g(n) = O(f(n))$; and
- $f(n) = \Omega(g(n))$ as $n \to \infty$ means that $\liminf_{n\to\infty} f(n)/g(n) > 0$.

We use $f(n) \sim g(n)$ and $f(n) = (1 + o(1))g(n)$ (both as $n \to \infty$) interchangeably to mean $\lim_{n\to\infty} f(n)/g(n) = 1$.

Additional notation

log denotes the base-2 logarithm, and ln denotes the natural logarithm. In order to avoid cluttering notation, we often write $\ln^2 n$ to mean $(\ln n)^2$, et cetera. We often use $\exp(x) := \mathrm{e}^x$, where e is the base of the natural logarithm, and $\exp_2(x) := 2^x$, especially when x is a complicated expression.

2.2 Binomial coefficients

Binomial coefficients appear throughout this thesis, and good bounds on (sums of) binomial coefficients will be instrumental in many of its results. Fortunately, a large body of standard bounds exists. We state some of these results, and point to sources containing their proofs.

The first bounds, a proof of which can be found in [Juk01, Proposition 1.4], are valid for all $0 < r \leq n$:

$$\binom{n}{r} \geq \left(\frac{n}{r}\right)^r, \qquad \text{and} \qquad \sum_{i=0}^{r} \binom{n}{i} \leq \left(\frac{\mathrm{e}n}{r}\right)^r.$$

For sums of binomial coefficients, we have

$$\sum_{i=0}^{r} \binom{n}{i} \leq 2^{\mathscr{H}(r/n)n} \qquad \text{for all } 0 \leq r \leq n/2,$$

as well [Juk01, Corollary 22.9]. Here $\mathscr{H}(\cdot)$ is the binary entropy function, defined by

$$\mathscr{H}(p) := -p \log p - (1-p)\log(1-p).$$

The following bound, which is valid for all $0 < p \leq 1$, is useful for bounding $\mathscr{H}(p)$ for small values of p:

$$\mathscr{H}(p) \leq -p \log \frac{p}{4}.$$

The binomial coefficient $\binom{n}{\lfloor n/2 \rfloor}$ is called the *central binomial coefficient*. In order to avoid cluttering notation, we ignore rounding down, and write $\binom{n}{n/2} := \binom{n}{\lfloor n/2 \rfloor}$. Stirling's approximation to the factorial (cf. [SF14, Chapter 1]) can be used to obtain the following asymptotically tight bounds:

$$\sqrt{2/\pi}\frac{2^n}{\sqrt{n}}\left(1 - \frac{1}{n}\right) \leq \binom{n}{n/2} \leq \sqrt{2/\pi}\frac{2^n}{\sqrt{n}}. \tag{2.1}$$

The bounds (2.1) allow us to compare different central binomial coefficients. In particular, we need

$$\binom{n-m}{\lfloor \frac{n-m}{2} \rfloor} \leq \frac{n}{n-1}\sqrt{\frac{n}{n-m}}2^{-m}\binom{n}{n/2}. \tag{2.2}$$

While (2.1) gives precise asymptotics for central binomial coefficients, we also require good bounds on $\binom{n}{r}$ for r close to $n/2$. Such a bound is provided by the following lemma.

Lemma 2.2.1 ([SF14, Equation (5.41)]). *If $k = o\left(n^{2/3}\right)$, then*

$$\binom{n}{\lfloor n/2 \rfloor + k} = (1 + o(1))\binom{n}{n/2} \mathrm{e}^{-2k^2/n}.$$

2.3 Matroids

In this section, we provide a selection of terminology and results that are required in later chapters. For a more comprehensive introduction to the field, the reader is referred to the monograph by Oxley [Oxl11]. With a few exceptions, our notation follows that of Oxley. Proofs of all claims in this section can be found there as well.

Basic definitions

It was already observed by Whitney [Whi35] that matroids allow many different axiomatisations. The one that is perhaps most natural in the context of this thesis is the definition in terms of *bases*. In these terms, a *matroid* is a set system $M = (E, \mathcal{B})$ on a finite *ground set* E, such that the nonempty collection of bases $\mathcal{B} \subseteq \mathscr{P}(E)$ satisfies the *basis-exchange axiom*:

For all $B, B' \in \mathcal{B}$, and for all $b \in B \setminus B'$,
there exists $b' \in B' \setminus B$ such that $(B \setminus \{b\}) \cup \{b'\} \in \mathcal{B}$.

We say that M is a matroid on E, and write $E(M)$ and $\mathcal{B}(M)$ to denote the ground set and collection of bases of M. (If there is no risk of confusion, we simply write E and $\mathcal{B}$.) We write $|M| := |E(M)|$ for the cardinality of the ground set of M.

A straightforward argument shows that all bases of M have the same cardinality, which is called the *rank* of M, and denoted by $\operatorname{rk}(M)$. If M is a matroid on E of rank r, then a subset of M of cardinality r is called a *nonbasis* if it is not a bases, and we write $\mathcal{K}(M) := \binom{E}{r} \setminus \mathcal{B}(M)$ for the collection of all nonbases.

A subset $A \subseteq E$ is called *independent* if there is a basis $B \in \mathcal{B}$ such that $A \subseteq B$. The collection of independent sets of M is denoted

$$\mathcal{I}(M) := \mathcal{B}(M)^{\downarrow} = \{I : I \subseteq B \text{ for some } B \in \mathcal{B}(M)\}.$$

Note that the bases of a matroid are precisely its inclusionwise-maximal independent sets.

Some examples

We consider a number of examples of matroids.

Uniform matroids Let E be a finite set, and let $0 \leq r \leq |E|$. The collection $\binom{E}{r}$ is the set of bases of a matroid on E. Such a matroid is called a *uniform matroid* of rank r. We write $U(r, n)$ for the uniform matroid of rank r on $E = [n]$.[2] The independent sets of $U(r, n)$ are precisely the subsets of $[n]$ of cardinality at most r.

Graphic matroids Let $G = (V, E)$ be a graph, and let $\mathcal{I} := \{F \subseteq E : (V, F) \text{ is a forest}\}$. The collection $\mathcal{I}$ is a collection of independent sets of a matroid on E. A matroid that can be obtained from a graph G in this way is called a *graphic matroid*, and written $M(G)$.

Representable and algebraic matroids Conjecture 1.3.6 and Conjecture 1.3.7 refer to representable and algebraic matroids. We already encountered representable matroids in the introduction, as one of the examples that led Whitney to his definition of a matroid.

A matroid $M = (E, \mathcal{B})$ is *representable* if there exists a function $f\colon E \to V$ from E to some vector space V with the property that $B \in \mathcal{B}$ if and only if $\{f(e) : e \in B\}$ is a basis of V. If $\mathbb{F}$ is a field, we say that M is $\mathbb{F}$-representable if we can choose V to be a vector space over $\mathbb{F}$. If M is representable, then we can assume that V has finite rank, in which case $V \cong \mathbb{F}^{\dim V}$. It follows that the function f gives us a representation of M as a matrix over $\mathbb{F}$, the columns of which are indexed by the elements from E.

Let $\mathbb{F}$ be a field. A matroid $M = (E, \mathcal{B})$ is *algebraic* over $\mathbb{F}$ if there is an extension field $\mathbb{F}^+/\mathbb{F}$, and a function $f\colon E \to \mathbb{F}^+$, such that $I \subseteq E$ is independent if and only if $\{f(e) : e \in I\}$ is algebraically independent over $\mathbb{F}$.

Additional matroid theory preliminaries

Dependent sets, circuits, and cocircuits A subset of E is called *dependent* if it is not independent. Inclusionwise-minimal dependent sets are called *circuits*. The *girth* $\mathrm{g}(M)$ of M is the minimum cardinality of a circuit of M, and $\mathrm{g}(M) = \infty$ if M does not have any circuits. Circuits can be used to axiomatise matroids.

[2] Here, our notation deviates from that of Oxley [Oxl11], who uses $U_{r,n}$ for the uniform matroid.

Proposition 2.3.1 ([Oxl11, Corollary 1.1.5]). *Let E be a finite set. A collection $\mathcal{C} \subseteq \mathscr{P}(E)$ is the collection of circuits of a matroid on E if and only if it satisfies each of the following properties:*

(i) $\emptyset \notin \mathcal{C}$*;*

(ii) Antichain: *$\mathcal{C}$ is an antichain in $\mathscr{P}(E)$; and*

(iii) Circuit-elimination: *If C_1 and C_2 are distinct members of $\mathcal{C}$, and $e \in C_1 \cap C_2$, then there is a member C_3 of $\mathcal{C}$ such that $C_3 \subseteq (C_1 \cup C_2) \setminus \{e\}$.*

In addition, a *codependent* set is a set that meets every basis, and a *cocircuit* is an inclusionwise-minimal such set.

Lemma 2.3.2. *Let M be a matroid of rank r on E, and let $X \in \binom{E}{r}$ be a set of rank $\operatorname{rk}_M(X) = r - 1$. Then M contains a unique circuit C that is contained in X, and a unique cocircuit D that is disjoint from X.*

Proof. First, we prove the existence and uniqueness of C and D. As X is dependent, it contains a circuit. Let I be a basis for X. As $\operatorname{rk}_M(X) = r - 1$, $|I| = r - 1$, and $X = I \cup \{e\}$ for some e. Every circuit in X contains e. If there are at least two circuits, then by the circuit-elimination axiom, Proposition 2.3.1(iii), there must also be a circuit contained in X that avoids e; a contradiction.

For the cocircuit, let $D' := \{f \in E \setminus X : \operatorname{rk}_M(I \cup \{f\}) = r\}$. As a cocircuit meets every basis, clearly $D' \subseteq D$ for every cocircuit D of M that is disjoint from X. We claim that D' is codependent, which implies that $D = D'$ is the unique cocircuit disjoint from X. Suppose that B is a basis; we need to show that B meets D'. If this is not the case, then $B \subseteq E \setminus D' = \operatorname{cl}_M(I)$, and thus B is contained in a hyperplane; a contradiction. □

Rank function A matroid comes with a *rank function* $\operatorname{rk}_M \colon \mathscr{P}(E) \to \mathbb{Z}_{\geq 0}$,

$$\operatorname{rk}_M(A) := \max\bigl\{|I| : I \in \mathcal{I}(M), I \subseteq A\bigr\}.$$

We use the shorthand $\operatorname{rk}(M) = \operatorname{rk}_M(E)$ for the rank of M. Rank functions can be used to axiomatise matroids.

Proposition 2.3.3 ([Oxl11, Corollary 1.3.4]). *Let E be a finite set, and let* $\operatorname{rk} \colon \mathscr{P}(E) \to \mathbb{Z}_{\geq 0}$*. The function* rk *is the rank function of a matroid on E if and only if it satisfies each of the following properties:*

(i) Boundedness: *For all $X \subseteq E$, $0 \leq \operatorname{rk}(X) \leq |X|$;*

(ii) Monotonicity: *For all* $X \subseteq Y \subseteq E$, $\mathrm{rk}(X) \leq \mathrm{rk}(Y)$*; and*

(iii) Submodularity: *For all* $X, Y \subseteq E$, $\mathrm{rk}(X \cup Y) + \mathrm{rk}(X \cap Y) \leq \mathrm{rk}(X) + \mathrm{rk}(Y)$.

A subset $X \subseteq E$ is a *spanning set* of M if $\mathrm{rk}_M(X) = \mathrm{rk}(M)$. This happens if and only if X contains a basis. More generally, a subset $X \subseteq Y$ spans Y if $\mathrm{rk}_M(X) = \mathrm{rk}_M(Y)$.

Loops, coloops, and simple matroids An element $e \in E$ is called a *loop* if it is not contained in any basis (equivalently, if $\mathrm{rk}_M(\{e\}) = 0$), and e is called a *coloop* if it is contained in every basis. The elements $e, f \in E$ are in *parallel* if neither element is a loop, and $\mathrm{rk}_M(\{e, f\}) = 1$. A matroid M is called *simple* if and only if it does not have any loops or nontrivial parallel classes. Associated with every matroid is its *simplification*, which is a simple matroid essentially obtained from M by ignoring loops and viewing parallel classes as single elements. Formally, this is the matroid whose ground set is formed by the parallel classes of M, where the rank in $\mathrm{si}(M)$ is given by the rank of their union in M.

Isomorphism Two matroids, $M_1 = (E_1, \mathcal{B}_1)$ and $M_2 = (E_2, \mathcal{B}_2)$, are called *isomorphic* (written $M_1 \cong M_2$) if there exists a bijection $\sigma\colon E_1 \to E_2$ such that $B \in \mathcal{B}_1$ if and only if $\sigma(B) \in \mathcal{B}_2$.

An *automorphism* of M is an isomorphism from M to itself. The automorphisms of M form a group under composition: the automorphism group $\mathrm{Aut}(M)$. The identity function is always an automorphism of M, and it is called the trivial automorphism. If M has an automorphism that is not the trivial automorphism, M is called *symmetric*, and it is called *asymmetric* otherwise.

Connectivity Let $k \geq 1$. A k-separation of M is a partition $\{A, B\}$ of $E(M)$ such that $|A|, |B| \geq k$, and $\mathrm{rk}(A) + \mathrm{rk}(B) < \mathrm{rk}(M) + k$. The *(Tutte) connectivity* of M is

$$\lambda(M) := \min \{k : M \text{ has a } k\text{-separation}\},$$

where we assume that the minimum over the empty set is ∞.

Flats In addition to terms that are borrowed from linear algebra and graph theory, such as "independent set" and "circuit", part of the matroid terminology comes from geometry. The rank function allows us to define the *closure operator* $\mathrm{cl}_M : \mathscr{P}(E) \to \mathscr{P}(E)$ by

$$\mathrm{cl}_M(X) := \{e \in E : \mathrm{rk}_M(X \cup \{e\}) = \mathrm{rk}_M(X)\}.$$

A subset $F \subseteq E$ is called a *flat* (or closed set) if $\mathrm{cl}_M(F) = F$. The collection of flats of a matroid, denoted by $\mathcal{F}(M)$, forms a lattice when partially ordered by inclusion. Flats of rank 1, 2, and 3 are usually called points, lines, and planes, respectively. A *hyperplane* is a flat of rank $\mathrm{rk}(M) - 1$. A line is called *long* if it contains at least three points.

A hyperplane that is also a circuit is called a *circuit-hyperplane*. The collection of circuit-hyperplanes of M is denoted by $\mathcal{W}(M)$. Each circuit-hyperplane is a nonbasis, but not every nonbasis is a circuit-hyperplane. We write $\mathcal{U}(M) := \mathcal{K}(M) \setminus \mathcal{W}(M)$.

If X is a circuit-hyperplane in M, then $\mathcal{B}' := \mathcal{B}(M) \cup \{X\}$ is again the collection of bases of a matroid. We say that the matroid $(E(M), \mathcal{B}')$ is obtained from M by *relaxing* the circuit-hyperplane X.

Geometric representations of small-rank matroids

The description of a matroid in terms of its flats provides a convenient geometrical perspective. Let us make this perspective more explicit by relating matroids to incidence structures.

An *incidence structure* is a tuple (P, L, I) consisting of (disjoint) collections P and L, suggestively named points and lines, and an incidence relation $I \subseteq P \times L$. A *partial linear space* is an incidence structure satisfying the following additional properties:

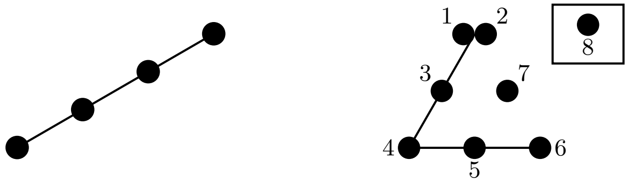
(i) Every pair of distinct points determines at most one line; and

(ii) every line contains at least two distinct points.

It is possible to draw a partial linear space as follows. First, draw a dot for each point in the partial linear space. Second, for each line in the partial linear space, draw a line passing through all of its points. The order of points on this line does not matter. To avoid cluttering the drawing, it is customary to draw only its long lines.

Let M be a matroid of rank at most 3. We can associate with M a partial linear space (P, L, I), by choosing P and L to be the sets of rank-1 flats and rank-2 flats of M, respectively. In this way, we can obtain a drawing of M as well. If M is not simple, then we can add its loops in a separate inset to the drawing, and draw non-trivial rank-1 flats as collections of touching points. See Figure 2.1.

The construction above can be extended to matroids of higher rank, by using higher-dimensional incidence structures. In general, it is hard to draw such matroids on a 2-dimensional sheet of paper, although for rank-4 matroids it is often possible to obtain a 3-dimensional drawing.



(a) $U(2,4)$ (labels suppressed). **(b)** A rank-3 matroid with a nontrivial parallel class, $\{1,2\}$, and a loop, 8.

Figure 2.1: Geometric representations of two matroids.

Duality and minors

The dual matroid and a minor of a matroid are two ways of constructing new matroids from a given matroid.

It can be shown that if $M = (E, \mathcal{B})$ is a matroid, then the collection

$$\mathcal{B}^* := \{E \setminus B : B \in \mathcal{B}\}$$

is again the set of bases of a matroid on E [Oxl11, Theorem 2.1.1]. This matroid is called the *dual* matroid of M, and is written M^*. It is easily verified that taking the dual is an involution, i.e. $(M^*)^* = M$. Note that $\operatorname{rk}(M^*) = |E| - \operatorname{rk}(M)$.

The element e is a coloop of M if and only if it is a loop in M^*. Several other objects relating to the dual matroid can be similarly recognised by the prefix "co-"; for example, the cocircuits, coindependent sets, and the corank function of M are the circuits, independent sets, and rank function of M^*.

If $M = (E, \mathcal{B})$ is a matroid, and $X \subseteq E$, then the *deletion* of X in M, written $M \backslash X$ is the matroid on ground set $E \setminus X$ whose set of bases is formed by the inclusionwise-maximal elements of $\{B \setminus X : B \in \mathcal{B}(M)\}$. At times, we shall also write $M|X := M \backslash (E \setminus X)$ for the *restriction* of M to X.

The *contraction* of X in M is the matroid on $E \setminus X$ with set of bases

$$\mathcal{B}(M/X) = \{B' \subseteq E \setminus X : B' \cup B_X \in \mathcal{B}(M)\}.$$

Here, B_X is any basis of the restriction $M|X$.

If $C, D \subseteq E$ are disjoint sets, and N is a matroid that is obtained from M by contracting the elements in C and deleting the elements in D, then N is called a *minor* of M, and we write $N = M/C \backslash D$. We say that M has an N-minor if M has a minor that is isomorphic to N.

It is customary to write, e.g. $M/e_1\backslash e_2, e_3$ for $M/\{e_1\}\backslash\{e_2, e_3\}$. If e is not a coloop of M, then

$$\mathcal{B}(M\backslash e) = \{B \in \mathcal{B}(M) : e \notin B\},$$

while if e is not a loop of M, then

$$\mathcal{B}(M/e) = \{B \setminus \{e\} : B \in \mathcal{B}(M), e \in B\}.$$

Minors and duality are related through

$$(M/C\backslash D)^* = M^*/D\backslash C.$$

A class of matroids is called *minor-closed* if it is closed under taking minors and isomorphism (contraction-closed and deletion-closed classes are defined similarly).

It is natural to describe minor-closed classes by listing their *excluded minors*, i.e. those matroids that are not in the class, but all of whose proper minors are in the class. As minor-closed classes are closed under isomorphism, it suffices to list non-isomorphic excluded minors. If $\mathcal{N}$ is a collection of matroids, write

$$\mathrm{Ex}(\mathcal{N}) := \{M \text{ a matroid} : \text{for all } N \in \mathcal{N},\ M \text{ has no } N\text{-minor}\}$$

for the minor-closed class obtained by excluding the matroids in $\mathcal{N}$ as minors. If $\mathcal{N} = \{N\}$, we shall write $\mathrm{Ex}(N) := \mathrm{Ex}(\mathcal{N})$. A well-known example is that of matroids representable of the binary field, a class that is characterised by the excluded minor $U(2, 4)$ [Oxl11, Theorem 9.1.3].

2.4 Matroid classes

We shall be interested in particular in the matroids with ground set $E = [n]$, and we write $\mathbb{M}(n)$ for this class of matroids. In addition, we write $\mathbb{M}(n, r)$ for those matroids in $\mathbb{M}(n)$ that have rank r.

Of particular importance are *sparse paving matroids*. These are matroids in which every nonbasis is a circuit-hyperplane. We shall write $\mathbb{S}(n)$ and $\mathbb{S}(n, r)$ for the sparse paving matroids in $\mathbb{M}(n)$ and $\mathbb{M}(n, r)$, respectively.

We shall write

$$\begin{aligned} m(n) &:= |\mathbb{M}(n)| \qquad & m(n,r) &:= |\mathbb{M}(n,r)| \\ s(n) &:= |\mathbb{S}(n)| \qquad & s(n,r) &:= |\mathbb{S}(n,r)| \end{aligned} \tag{2.3}$$

In addition, a matroid of rank r is *paving* if all its circuits have cardinality in $\{r, r+1\}$, and M is *sparse* if M^* is paving. Note that M is sparse paving if it is both sparse and paving.

2.5 Asymptotic matroid theory

The definitions (2.3) allow us to state precisely what it means if a property holds for "almost every" matroid. Let $\mathcal{M}$ be a class of matroids (i.e. $\mathcal{M} \subseteq \mathbb{M}$, and $\mathcal{M}$ is closed under isomorphism), and define

$$m_{\mathcal{M}}(n) := |\mathbb{M}(n) \cap \mathcal{M}|, \qquad s_{\mathcal{M}}(n) = |\mathbb{S}(n) \cap \mathcal{M}|.$$

We say that *almost every matroid* is in $\mathcal{M}$ if and only if

$$\lim_{n\to\infty} \frac{m_{\mathcal{M}}(n)}{m(n)} = 1.$$

In addition, we say that $\mathcal{M}$ is *small* if and only if

$$\lim_{n\to\infty} \frac{m_{\mathcal{M}}(n)}{m(n)} = 0.$$

If $\mathcal{M}$ is a class of matroids, then so is $\overline{\mathcal{M}} := \mathbb{M} \setminus \mathcal{M}$. Moreover, almost every matroid is in $\mathcal{M}$ if and only if $\overline{\mathcal{M}}$ is small. Similarly, we say that almost every sparse paving matroid is in $\mathcal{M}$ if

$$\lim_{n\to\infty} \frac{s_{\mathcal{M}}(n)}{s(n)} = 1, \qquad \text{or} \qquad \lim_{n\to\infty} \frac{s_{\overline{\mathcal{M}}}(n)}{s(n)} = 0.$$

The requirement that $\mathcal{M}$ be closed under isomorphism is essential, as it implies that

$$\frac{|\{M \in \mathcal{M} : E(M) = E\}|}{|\{M : E(M) = E\}|} = \frac{m_{\mathcal{M}}(n)}{m(n)}$$

for every set E of cardinality n, and so the limiting value does not depend on the particular choice of ground set.

Combining statements concerning almost every matroid with asymptotic notation is potentially confusing. Suppose that $f(M)$ is some statistic of a matroid M. We use 'almost every matroid satisfies $f(M) = O\left(a_{|M|}\right)$ as $|M| \to \infty$' with the following precise meaning: there exists a constant $C > 0$ such that almost every matroid satisfies $f(M) \leq Ca_{|M|}$. This definition coincides with the use of '$O(a_n)$ whp' in [Jan11, (D11)]. Similar definitions hold, mutatis mutandis, for other Landau notation, and for sparse paving matroids.

2.6 Johnson graphs

Definition

In this thesis, a central role is played by the so-called *Johnson graphs*. The Johnson graph $J(E, r)$ is the graph with vertex set $\binom{E}{r}$, in which any pair of vertices are adjacent if and only if they intersect in $r-1$ elements. Note that X and X' are adjacent if and only if there exist $x \in X \setminus X'$ and $x' \in X' \setminus X$ such that $X' = (X \setminus \{x\}) \cup \{x'\}$. In this case, we shall often write $X' = X \triangle \{x, x'\}$.

We shall use $J(n, r) := J([n], r)$ as a shortcut. It is easily verified that for all sets E with $|E| = n$, we have $J(E, r) \cong J(n, r)$.

Johnson graphs $J(n, r)$ and $J(n, n-r)$ are isomorphic. An explicit isomorphism is given by $X \mapsto [n] \setminus X$. For $r = 0$ and $r = 1$, the graphs $J(n, r)$ are rather dull: $J(n, 0)$ is the trivial graph with a single vertex, and $J(n, 1)$ is isomorphic to the complete graph on n vertices.

Properties

We collect some useful properties of Johnson graphs. Johnson graphs are highly regular objects that are well studied. A more in-depth discussion of these graphs, as well as proofs of the properties discussed here, can be found in [BCN89, Section 9.1].

Every permutation $\pi \in \mathrm{Sym}(n)$, acting on $\binom{[n]}{r}$, gives rise to an automorphism of $J(n, r)$. These permutations form the complete automorphism group of $J(n, r)$, except when $n = 2r$, in which case the function that swaps an r-set for its complement in $[n]$ is an automorphism as well.

Proposition 2.6.1. $\mathrm{Aut}(J(n, r)) \cong \begin{cases} \mathrm{Sym}(1) & \text{if } r = 0 \text{ or } r = n \\ \mathrm{Sym}(n) \oplus \mathbb{Z}_2 & \text{if } n = 2r \geq 4 \\ \mathrm{Sym}(n) & \text{otherwise.} \end{cases}$

Proposition 2.6.2. *The eigenvalues of $J(n, r)$ are*

$$(r - j)(n - r - j) - j, \qquad j = 0, 2, \ldots, r,$$

with multiplicity $\binom{n}{j} - \binom{n}{j-1}$.

Neighbourhood structure

Whenever $X \in \binom{E}{r}$, we shall write $N(X)$ for its neighbourhood in the Johnson graph $J(E, r)$, i.e.

$$N(X) := \left\{ X' \in \binom{E}{r} : |X \triangle X'| = 2 \right\},$$

unless explicitly stated otherwise. Clearly, $J(n,r)$ is regular of degree $r(n-r)$, and hence $|N(X)| = r(n-r)$.

The subgraph of $J(E,r)$ induced by $N(X)$ is isomorphic to the Cartesian graph product of K_r and $K_{|E|-r}$. In particular, we can distinguish 'rows'

$$R_X(x) := \{X \triangle \{x,y\} : y \in E \setminus X\}, \qquad x \in X,$$

and 'columns'

$$C_X(y) := \{X \triangle \{x,y\} : x \in X\}, \qquad y \in E \setminus X.$$

For each $X \in \binom{E}{r}$, these rows and columns induce cliques in the neighbourhood of X, see Figure 2.2. The structure of neighbourhoods in $J(n,r)$ implies the following result on maximal cliques.

Lemma 2.6.3. *Each maximal clique in $J(n,r)$ is of the form $\{X-x+y : x \in X\}$ for some $y \in [n] \setminus X$, or $\{X - x + y : y \in [n] \setminus X\}$ for some $x \in X$.*

The following lemma shows that the nonbases in the neighbourhood of a rank-$(r-1)$-set can be described by a circuit and a cocircuit.

Lemma 2.6.4. *Let M be a matroid of rank r on E, and let $X \in \binom{E}{r}$ be a set of rank $\operatorname{rk}_M(X) = r-1$. Then M contains a unique circuit C that is contained in X, and a unique cocircuit D that is disjoint from X. Moreover, the nonbases among $N(X)$ are identified through*

$$\mathcal{K}(M) \cap N(X) = \big\{(X \setminus \{e\}) \cup \{f\} : e \in X \setminus C \text{ or } f \in (E \setminus X) \setminus D\big\}. \tag{2.4}$$

Proof. Existence and uniqueness of C and D is precisely the statement of Lemma 2.3.2; it remains to prove (2.4). In fact, we will prove the equivalent statement that $Y = (X \setminus \{e\}) \cup \{f\} \in N(X)$ is a basis if and only if $e \in C$ and $f \in D$. If Y is a basis, then $e \in C$ (otherwise $C \subseteq Y$) and $f \in D$ (otherwise $D \cap Y = \emptyset$). To prove the reverse implication, note that if $e \in C$, then $\operatorname{rk}(X \setminus \{e\}) = r-1$, and if $f \in D$, then $f \notin \operatorname{cl}(X \setminus \{e\})$. It follows that $\operatorname{rk}((X \setminus \{e\}) \cup \{f\}) = r$, and hence that Y is a basis. □

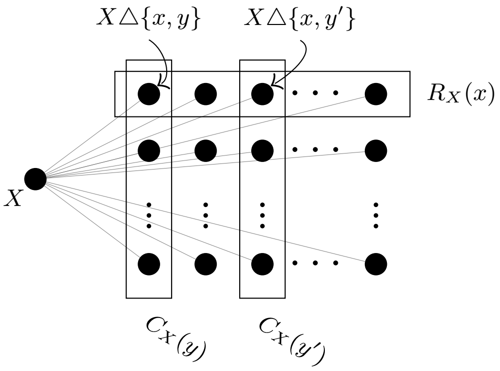


Figure 2.2: The neighbourhood of X in the Johnson graph. The rows and columns, indexed by $x \in X$, resp. $y \in E \setminus X$, form cliques.

2.7 Johnson graphs, sparse paving matroids, and partial Steiner systems

An important reason that Johnson graphs play a big role in asymptotic matroid theory is that stable sets in $J(n,r)$ correspond precisely to sparse paving matroids. This connection was used implicitly by Piff and Welsh [PW71] in an earlier lower bound on the number of matroids, and more explicitly by Mayhew and Welsh [MW13] in an upper bound on the number of sparse paving matroids.

Lemma 2.7.1. *Let E be a finite set, and let $0 < r < |E|$. The following are equivalent:*

(i) $I \in \mathrm{Ind}(J(E,r))$; and

(ii) I is the set of non-bases of a sparse paving matroid of rank r on E.

Proof. First, we prove the implication (i)⇒(ii). Suppose that I is a stable set in $J(E,r)$, and let $\mathcal{B} := \binom{E}{r} \setminus I$. We show that $\mathcal{B}$ is the set of bases of a sparse paving matroid on E.

We argue by contradiction, so suppose that $\mathcal{B}$ is not the set of bases of a sparse paving matroid on E. First, note that $\mathcal{B} \neq \emptyset$: if $\mathcal{B}$ is empty, then $I = \binom{E}{r}$, which implies that $J(E,r)$ has no edges. So the only way that $\mathcal{B}$ could fail to be the set of bases of a matroid is by failing the basis-exchange axiom, in which case there are $B, B' \in \mathcal{B}$ and $b \in B \setminus B'$ such that $(B \setminus \{b\}) \cup \{b'\} \in I$ for every $b' \in B' \setminus B$. If $|B' \setminus B| = 1$, then

$(B \setminus \{b\}) \cup \{b'\} = B' \in \mathcal{B}$, so we must have $|B' \setminus B| \geq 2$. Thus, there exist distinct elements $b'_1, b'_2 \in B' \setminus B$. Define $B_i := (B \setminus \{b\}) \cup \{b'_i\}$, $i \in \{1,2\}$. By assumption, both B_1 and B_2 are in I. On the other hand $|B_1 \triangle B_2| = |\{b'_1, b'_2\}| = 2$, so B_1 and B_2 are adjacent in $J(E,r)$, thus contradicting that I is a stable set, and hence showing that $\mathcal{B}$ is a set of bases of a matroid on E.

The resulting matroid is sparse paving; to prove this, we need to show that each $X \in I$ is a circuit-hyperplane. Fix such an X; by construction it is a non-basis. Choose $e \in E \setminus X$ and $x \in X$. As $(X \setminus \{x\}) \cup \{e\} \in \mathcal{B}$, it follows that $X \cup \{e\}$ is spanning, and as e was arbitrary, X must be a hyperplane. Similarly, $X \setminus \{x\}$ must be independent, as it is contained in the basis $(X \setminus \{x\}) \cup \{e\}$, and as x is arbitrary, it follows that X is a circuit.

Next, we prove the reverse implication, (ii)⇒(i), again arguing by contradiction. Let M be a sparse paving matroid, and suppose that X and Y are two nonbases that are adjacent in $J(E,r)$. Submodularity of the rank function shows that

$$\mathrm{rk}_M(X \cap Y) + \mathrm{rk}_M(X \cup Y) \leq \mathrm{rk}_M(X) + \mathrm{rk}_M(Y) < 2r - 1,$$

so that either $\mathrm{rk}_M(X \cap Y) < r - 1 = |X \cap Y|$, or $\mathrm{rk}_M(X \cup Y) < r$. In the former case, it follows that $X \cap Y$ is a dependent set that is strictly contained in X, so that X is not a circuit. In the latter case, $X \cup Y$ is contained in a hyperplane, thus showing that X is not a hyperplane. In both cases, it follows that X is not a circuit-hyperplane, and hence that M is not sparse paving; a contradiction. □

The implication (ii)⇒(i) admits the following generalisation.

Lemma 2.7.2. *If $M \in \mathbb{M}(n,r)$, then $\mathcal{W}(M) \in \mathrm{Ind}(J(n,r))$.*

Consider the subgraph G of the Johnson graph $J(E,r)$ induced by the nonbases of a matroid $M \in \mathbb{M}(E,r)$. Each component of G contains either only circuit-hyperplanes of M (in which case it is a singleton component), or only elements from $\mathcal{U}(M)$ (in which case the component contains at least two elements). We call a component of the latter type *complex*.

A different perspective on stable sets in Johnson graphs is given by partial Steiner systems. A *partial Steiner system* $S_p(t,k,n)$ is a set system $(E, \mathcal{X})$, consisting of a set E of cardinality n, and a collection $\mathcal{X}$ of k-subsets of E (called blocks) with the property that every t-subset of E is contained in at most one block. If every t-subset is contained in a unique block, then we speak of a *Steiner system* $S(t,k,n)$. The following lemma is easily verified.

Lemma 2.7.3. *Let E be a set of cardinality n, and let $0 < r < n$. The following are equivalent:*

(i) $I \in \operatorname{Ind}(J(E, r))$*; and*

(ii) I *is a partial Steiner system* $S_p(r-1, r, n)$*.*

In addition to their connection to matroid theory, Johnson graphs are strongly tied to coding theory. The independence number of $J(n, r)$ is the cardinality of the largest binary constant-weight code with word length n, weight r, and minimum distance 4. In the literature, this quantity is generally known as $A(n, 4, r)$; see e.g. [Ö10, Bro] and references therein.

2.8 A lower bound

The best known lower bound on the number of matroids follows from the construction of a large family of sparse paving matroids. Note that $\operatorname{Ind}(G)$ is closed under taking subsets: if I is a stable set in G, then so is every $I' \subseteq I$. Thus, the existence of a stable set of cardinality k in G implies $\operatorname{ind}(G) \geq 2^k$.

The following construction, due to Graham and Sloane [GS80], shows that $J(n, r)$ admits a stable set of cardinality at least $\frac{1}{n}\binom{n}{r}$.

Lemma 2.8.1 ([GS80, Theorem 1])**.** *For each $0 \leq r \leq n$, the Johnson graph $J(n, r)$ contains a stable set of cardinality $\frac{1}{n}\binom{n}{r}$.*

Proof. Recall that $V(J(n, r)) = \binom{[n]}{r}$. The function $c\colon V(J(n, r)) \to \mathbb{Z}_n$, defined by

$$c\colon X \mapsto \sum_{x \in X} x \mod n,$$

is a proper vertex-colouring of $J(n, r)$, for if X and X' are adjacent vertices such that $X' = (X \setminus \{x\}) \cup \{x'\}$, then

$$c(X) - c(X') = x - x' \neq 0 \mod n,$$

and so $c(X) \neq c(X')$. As each colour class of a proper colouring is a stable set, and there are n such colour classes, there is a stable set containing at least a $1/n$-fraction of all vertices. □

As stable sets in $J(n, r)$ are in one-to-one correspondence with sparse paving matroids of corresponding rank and size, the lemma implies that

$\log s(n,r) \geq \frac{1}{n}\binom{n}{r}$. Maximising over r, we obtain the following bound on $\log s(n)$.

Proposition 2.8.2. $\log s(n) \geq \frac{1}{n}\binom{n}{n/2}$.

In the proof of Lemma 2.8.1, Graham and Sloane identify $[n]$ with $\mathbb{Z}_n$, the integers modulo n, which forms a group under addition, and they use this identification to produce a proper n-colouring of $J(n,r)$. We can try to improve upon this result in two ways.

First, Graham and Sloane already commented that replacing the average cardinality of a colour class by the cardinality of the maximum colour class in this scheme sometimes yields a slightly stronger result. It is then natural to ask whether this points to a structural imbalance in the cardinalities of the colour classes. Second, perhaps replacing the group $\mathbb{Z}_n$ by a different Abelian group of order n results in better bounds.

Kløve [Klø81] showed that neitheridea asymptotically improves upon Proposition 2.8.2. Maximising over all Abelian groups of order n and all colour classes, he obtained the following bound:

$$\log s(n,r) \geq \frac{1}{n} \sum_{\substack{d \mid \gcd(n,r) \\ d \text{ square-free}}} \binom{n/d}{r/d} \prod_{\substack{p \mid d \\ p \text{ prime} \\ \text{if } r = 2 \mod 4:\ p \text{ odd}}} (p^{e_p} - 1). \tag{2.5}$$

Here, the exponents e_p are such that $n = \prod_p p^{e_p}$ is the prime decomposition of n. Restricting the right-hand side of (2.5) to the term corresponding to $d = 1$, Proposition 2.8.2 is retrieved. Separating this term, (2.5) can be written as

$$\log s(n,r) \geq \frac{1}{n}\binom{n}{r} + f(n,r),$$

with $f(n,r) \geq 0$. As each of the terms corresponding to some $d \neq 1$ is at most $\binom{\lfloor n/2 \rfloor}{\lfloor r/2 \rfloor}$, it follows that

$$f(n,r) \leq n\binom{\lfloor n/2 \rfloor}{\lfloor r/2} \leq n\binom{\lfloor n/2 \rfloor}{\lfloor n/4 \rfloor} = o\left(\frac{1}{n}\binom{n}{n/2}\right),$$

from which it follows that, asymptotically, Proposition 2.8.2 cannot be improved upon in this way.

CHAPTER 3

Entropy

This chapter is based on the journal paper [BPvdP14], which is joint work with Nikhil Bansal and Rudi Pendavingh, and on the blog post [PvdP16b], which is joint work with Rudi Pendavingh.

3.1 In this chapter...

The entropy of a random variables essentially measures the amount of information obtained in a realisation. Bounding the entropy of a random variable often gives surprisingly strong bounds on the cardinality of its support.

In this chapter, we use such information-theoretic results to bound the cardinality of $\mathcal{M}\cap\mathbb{M}(n)$ for classes of matroids that are closed under contractions or deletions. The main technical result of this chapter is the following inductive tool, which we call the Entropy Blow-Up Lemma.

Lemma 3.1.1 (Entropy Blow-Up Lemma)**.** *Let* $0 \leq t \leq r \leq n$*. If* $\mathcal{M}$ *is contraction-closed, then*

$$\frac{\log(1 + m_{\mathcal{M}}(n, r))}{\binom{n}{r}} \leq \frac{\log(1 + m_{\mathcal{M}}(n - t, r - t))}{\binom{n-t}{r-t}}$$

The Entropy Blow-Up Lemma can be used to bound the number of matroids in a contraction-closed class in terms of the number of matroids of smaller size and rank in the class. Using the Entropy Blow-Up Lemma, we obtain the following results:

- $\log m(n) = O\left(\frac{\log n}{n}\binom{n}{n/2}\right)$; and
- $\mathrm{Ex}(N)$ is small, whenever N is one of $U(2,k)$ (for some $k \geq 2$), or $U(3,6)$, thus proving several special cases of Conjecture 1.3.5.

The remainder of this chapter is organised as follows. In Section 3.2–3.3, we define the entropy of a random variable, and state some of its properties, including Shearer's Entropy Lemma. In Section 3.4, we prove the Entropy Blow-Up Lemma. Subsequently, in Section 3.5–3.6, we use the Entropy Blow-Up Lemma to bound the number of matroids, and prove that $\mathrm{Ex}(N)$ is small for the special cases mentioned above.

3.2 Entropy

Let $\boldsymbol{X}$ be a random variable taking its value in a finite set $\mathcal{X}$. For $x \in \mathcal{X}$, write $p(x) := \mathbb{P}(\boldsymbol{X} = x)$ for the probability mass function of $\boldsymbol{X}$. The *entropy* of $\boldsymbol{X}$ is defined as

$$\mathscr{H}(\boldsymbol{X}) := -\sum_{x\in\mathcal{X}} p(x)\log p(x). \tag{3.1}$$

Here, we use the convention that $0\log 0 = 0$. Note that entropy is a function of the probability mass function of $\boldsymbol{X}$, rather than of the random variable itself.

Informally, the entropy of $\boldsymbol{X}$ can be interpreted as the *expected surprise* upon learning the value of $\boldsymbol{X}$. This is perhaps more clear from the following variant of (3.1):

$$\mathscr{H}(\boldsymbol{X}) = \sum_{x\in\mathcal{X}} \mathbb{P}(\boldsymbol{X} = x)\left[-\log p(x)\right] = \mathbb{E}[-\log p(\boldsymbol{X})]\,.$$

Here, $-\log p(x)$ measures the surprise upon seeing the event $\{\boldsymbol{X} = x\}$. Two properties make $A \mapsto -\log\mathbb{P}(A)$ a reasonable measure of surprise. First, less probable events elicit larger surprise. Second, surprise is additive for independent events (i.e. events for which $\mathbb{P}(A\cap B) = \mathbb{P}(A)\,\mathbb{P}(B)$). In fact, imposing in addition to these two properties only a few regularisation properties uniquely determines the surprise function (cf. [Gal14, Exercise 2.3]).

Alternatively, entropy is the "minimum descriptive complexity of a random variable" [CT06]. This interpretation is perhaps closer in spirit to the original application of entropy to data compression by Shannon [Sha48]. Shannon's source coding theorem says that, in the limit as

$n \to \infty$, while a sequence of n independent and identically distributed random variables $\boldsymbol{X}_1, \boldsymbol{X}_2, \ldots, \boldsymbol{X}_n$ may be encoded faithfully using more than $n\mathscr{H}(\boldsymbol{X}_1)$ bits, this cannot be done using fewer than $n\mathscr{H}(\boldsymbol{X}_1)$ bits.

We say that a random variable $\boldsymbol{X}$ has the uniform distribution on $\mathcal{X}$ if $p(x) = 1/|\mathcal{X}|$ for all $x \in \mathcal{X}$. As $-\log(\cdot)$ is a convex function, it follows from Jensen's inequality that

$$\mathscr{H}(\boldsymbol{X}) \leq \log|\mathcal{X}|,$$

and that equality holds if and only if $\boldsymbol{X}$ has the uniform distribution on $\mathcal{X}$.

It is precisely this property that makes entropy useful for enumeration purposes. If we are interested in bounds on the cardinality of some set $\mathcal{X}$, then we might as well study the entropy of a random variable that is uniformly distributed on $\mathcal{X}$. Bounds on the entropy of this random variable translate directly to bounds on $|\mathcal{X}|$, and vice versa.

Information-theoretic arguments often result in surprisingly short proofs of bounds on cardinalities, see e.g. Radhakrishnan's survey paper [Rad03] or the lecture notes by Galvin [Gal14].

3.3 Some properties of entropy

In this section we briefly review some of the properties of entropy. For a more thorough introduction, and proofs of the results mentioned here, we refer to [AS08, Section 15.7], or the book by Cover, and Thomas [CT06].

Suppose that $\boldsymbol{X} = (\boldsymbol{X}_1, \boldsymbol{X}_2)$ is some random variable taking values in the finite set $\mathcal{X}_1 \times \mathcal{X}_2$, according to some joint probability mass function $p(x_1, x_2) = \mathbb{P}(\boldsymbol{X}_1 = x_1, \boldsymbol{X}_2 = x_2)$.

The *conditional entropy* of $\boldsymbol{X}_1$ given $\boldsymbol{X}_2$ is defined by

$$\mathscr{H}(\boldsymbol{X}_1 \mid \boldsymbol{X}_2) := \mathscr{H}(\boldsymbol{X}_1, \boldsymbol{X}_2) - \mathscr{H}(\boldsymbol{X}_2)\,.$$

Conditional entropy can be interpreted as the expected *additional* surprise in $\boldsymbol{X}_1$ after learning the value in $\boldsymbol{X}_2$. Note that

$$\mathscr{H}(\boldsymbol{X}_1 \mid \boldsymbol{X}_2) = \mathbb{E}_{\boldsymbol{X}_2}[\mathbb{E}_{\boldsymbol{X}_1}[-\log p(\boldsymbol{X}_1, \boldsymbol{X}_2) \mid \boldsymbol{X}_2]]\,.$$

The following properties all have intuitive interpretations in terms of expected surprise.

Lemma 3.3.1. *Let $\boldsymbol{X} = (\boldsymbol{X}_1, \boldsymbol{X}_2, \ldots, \boldsymbol{X}_n)$ be a random vector taking its values in the finite set $\mathcal{X}_1 \times \mathcal{X}_2 \times \ldots \times \mathcal{X}_n$.*

(i) $\mathscr{H}(\boldsymbol{X}) \leq \sum_{i=1}^{n} \mathscr{H}(\boldsymbol{X}_i)$*;*

(ii) $\mathscr{H}(\boldsymbol{X_1} \mid \boldsymbol{X}_2) \leq \mathscr{H}(\boldsymbol{X}_1)$*; and*

(iii) $\mathscr{H}(\boldsymbol{X}) = \sum_{i=1}^{n} \mathscr{H}(\boldsymbol{X}_i \mid \boldsymbol{X}_j, j < i)$*.*

In our applications, we require a further result that is known as Shearer's Entropy Lemma. This result first appeared in a different form in [CGFS86, Product Theorem]; its proof there actually implies Lemma 3.3.2 below. See also [AS08, Theorem 15.7.4].

For the statement of Shearer's Entropy Lemma, we require some additional notation. Suppose that $\boldsymbol{X} = (\boldsymbol{X}_i : i \in I)$ is a random vector, taking its values in the finite set $\prod_{i \in I} \mathcal{X}_i$. For $A \subseteq I$, write $\boldsymbol{X}_A := (\boldsymbol{X}_i : i \in A)$ for the projection of X onto the coordinates indexed by A. Clearly such a projection is again a random variable.

Lemma 3.3.2 (Shearer's Entropy Lemma)**.** *Let* $\boldsymbol{X} = (\boldsymbol{X}_i : i \in I)$ *be a random vector indexed by* I*, and let* $\mathcal{A} \subseteq \mathscr{P}(I)$*. If each* $i \in I$ *is contained in at least* k *members of* $\mathcal{A}$*, then*

$$\mathscr{H}(\boldsymbol{X}) \leq \frac{1}{k} \sum_{A \in \mathcal{A}} \mathscr{H}(\boldsymbol{X}_A).$$

Note that of Shearer's Entropy Lemma generalises Lemma 3.3.1(i).

3.4 The Entropy Blow-Up Lemma

Let $\mathcal{M}$ be a class of matroids that is deletion-closed or contraction-closed. In this section, we compare $m_{\mathcal{M}}(n, r)$ to $m_{\mathcal{M}}(n', r')$, where $n' < n$ or $r' < r$. The first lemma compares $m_{\mathcal{M}}(n, r)$ to $m_{\mathcal{M}}(n-1, r)$ and $m_{\mathcal{M}}(n-1, r-1)$. The key element in its proof is that (formal) deletions/contractions from r-sets correspond to projections in the sense of Shearer's Entropy Lemma, which will then imply the bounds stated in the lemma.

Lemma 3.4.1. *Let* $\mathcal{M}$ *be a class of matroids. If* $\mathcal{M}$ *is deletion-closed, then*

$$\frac{\log(1 + m_{\mathcal{M}}(n, r))}{\binom{n}{r}} \leq \frac{\log(1 + m_{\mathcal{M}}(n-1, r))}{\binom{n-1}{r}}. \tag{3.2}$$

If $\mathcal{M}$ is contraction-closed, then

$$\frac{\log(1 + m_{\mathcal{M}}(n, r))}{\binom{n}{r}} \leq \frac{\log(1 + m_{\mathcal{M}}(n-1, r-1))}{\binom{n-1}{r-1}}. \tag{3.3}$$

Proof. We start by proving (3.2).

Let E be a set of cardinality n. Encode $M \in \mathcal{M} \cap \mathbb{M}(E, r)$ by the incidence vector of its bases. This is the vector $\chi\colon \binom{E}{r} \to \{0, 1\}$, such that $\chi(B) = 1$ if and only if $B \in \mathcal{B}(M)$. Let the space $\mathcal{X} \equiv \mathcal{X}(E, r)$ consist of all incidence vectors corresponding to matroids in $\mathcal{M} \cap \mathbb{M}(E, r)$, as well as the all-zero vector. Thus, $|\mathcal{X}| = 1 + m_{\mathcal{M}}(n, r)$, and if the random variable $\boldsymbol{\chi}$ is uniformly distributed on $\mathcal{X}$, then $\mathscr{H}(\boldsymbol{\chi}) = \log(1 + m_{\mathcal{M}}(n, r))$.

For $M \in \mathcal{M} \cap \mathbb{M}(E, r)$ and $e \in E$, write $\mathcal{B}(M)\backslash e := \{B \in \mathcal{B}(M) : e \notin B\}$. If e is not a coloop of M, then $\mathcal{B}(M)\backslash e = \mathcal{B}(M\backslash e)$. In this case, $M\backslash e \in \mathcal{M} \cap \mathbb{M}(E \setminus \{e\}, r)$, and $(\chi(B) : e \notin B) \in \mathcal{X}(E \setminus \{e\}, r)$ is the incidence vector of $M\backslash e$. On the other hand, if e is a coloop of M, then $\mathcal{B}(M)\backslash e = \emptyset$, and $(\chi(B) : e \notin B) \in \mathcal{X}(E \setminus \{e\}, r)$ is the all-zero vector. These observations imply that, for each e,

$$\mathscr{H}(\boldsymbol{\chi}(B) : e \notin B) \leq \log(1 + m_{\mathcal{M}}(n-1, r)).$$

We apply Shearer's Entropy Lemma with $\mathcal{A} = \left\{\binom{E\setminus\{e\}}{r} : e \in E\right\}$. For this choice of $\mathcal{A}$, its projections are precisely the formal deletions $(\chi(B) : e \notin B)$ described above. In addition, every r-subset of E is contained in exactly $n - r$ members of $\mathcal{A}$. We obtain

$$\mathscr{H}(\boldsymbol{\chi}) \leq \frac{1}{n-r} \sum_{e \in E} \mathscr{H}(\chi(B) : e \notin B) \leq \frac{n}{n-r} \log(1 + m_{\mathcal{M}}(n-1, r)).$$

The bound (3.2) follows, as $\frac{n}{n-r} = \binom{n}{r} / \binom{n-1}{r}$. The bound (3.3) follows from (3.2) by duality. □

The bounds in Lemma 3.4.1 can be applied inductively. Doing this for (3.3) yields the Entropy Blow-Up Lemma.

Lemma 3.1.1 (Entropy Blow-Up Lemma)**.** *Let $0 \leq t \leq r \leq n$. If $\mathcal{M}$ is contraction-closed, then*

$$\frac{\log(1 + m_{\mathcal{M}}(n, r))}{\binom{n}{r}} \leq \frac{\log(1 + m_{\mathcal{M}}(n-t, r-t))}{\binom{n-t}{r-t}}$$

3.5 Bounding the size of contraction-closed classes

Applying the Entropy Blow-Up Lemma

We shall typically use the Entropy Blow-Up Lemma, Lemma 3.1.1, by choosing $t = r - s$ for some fixed small s. In this way, enumerating matroids of general rank is reduced to enumerating matroids of fixed rank s, as

$$\frac{\log(1 + m_{\mathcal{M}}(n, r))}{\binom{n}{r}} \leq \frac{\log(1 + m_{\mathcal{M}}(n - r + s, s)}{\binom{n-r+s}{s}}.$$

Thus, the Entropy Blow-Up Lemma shows that bounds on matroids of a certain fixed rank, s, in a contraction-closed class $\mathcal{M}$ propagate to matroids of general rank in that class. We show that if the initial bound on matroids of fixed rank s is sufficiently small, this implies that the class $\mathcal{M}$ itself is small.

The following straightforward lemma shows that almost every matroid satisfies $\mathrm{rk}(M) \approx |M|/2$. Let

$$R_n := \left\{ r \in \mathbb{Z}_{\geq 0} : \left| r - \frac{n}{2} \right| < \sqrt{n \ln n} \right\}.$$

Lemma 3.5.1. *Almost every matroid has* $\mathrm{rk}(M) \in R_{|M|}$.

Proof. Let $z(n) := \sum_{r \in [n] \setminus R_n} m(n, r)$. We show that $\lim_{n\to\infty} \frac{z(n)}{m(n)} = 0$, which proves the claim. By duality $m(n, r) = m(n, n - r)$, and so

$$z(n) = 2 \sum_{r=0}^{\lfloor n/2 - \sqrt{n \ln n} \rfloor} m(n, r).$$

As a matroid is determined by its collection of bases, $\log m(n, r)$ is at most $\binom{n}{r}$. Taking logarithms, we obtain

$$\begin{aligned}
\log z(n) &\leq \log(2n) + \max_{r=0}^{\lfloor n/2 - \sqrt{n \ln n} \rfloor} \binom{n}{r} \\
&\leq (1 + o(1)) \binom{n}{\left\lfloor \frac{n}{2} - \sqrt{n \ln n} \right\rfloor} \\
&= (1 + o(1)) \frac{1}{n^2} \binom{n}{n/2},
\end{aligned}$$

where the second step follows from Lemma 2.2.1. Comparing to the lower bound $\log m(n) \geq \frac{1}{n}\binom{n}{n/2}$, we obtain

$$\log \frac{z(n)}{m(n)} \leq \left(\frac{1}{n^2} - \frac{1}{n}\right)\binom{n}{n/2} \to -\infty,$$

which concludes the proof. □

In Theorem 7.3.1, we prove a stronger result, which requires a more powerful technique. Lemma 3.5.1 implies that

$$\frac{m_{\mathcal{M}}(n)}{m(n)} = o(1) + \frac{\sum_{r\in R_n} m_{\mathcal{M}}(n,r)}{m(n)} \qquad \text{as } n \to \infty,$$

so in order to show that $\mathcal{M}$ is asymptotically small, it suffices to show that

$$\frac{\sum_{r\in R_n} m_{\mathcal{M}}(n,r)}{m(n)} = o(1) \qquad \text{as } n \to \infty. \tag{3.4}$$

Lemma 3.5.2. *Let $\mathcal{M}$ be contraction-closed. If there exist a constant $0 < c < 1/2$, and natural numbers s and n_0 such that*

$$\log(1 + m_{\mathcal{M}}(n,s)) \leq \frac{c}{n}\binom{n}{s} \qquad \textit{for all } n \geq n_0, \tag{3.5}$$

then $\mathcal{M}$ is small.

Proof. We prove the lemma by establishing (3.4). First, bound

$$\log \sum_{r\in R_n} m_{\mathcal{M}}(n,r) \leq \log|R_n| + \max_{r\in R_n} \log(1 + m_{\mathcal{M}}(n,r)).$$

The first term satisfies $\log|R_n| = O(\log n)$. By the Entropy Blow-Up Lemma, applied with $t = r - s$, and (3.5), the second term is at most

$$\max_{r\in R_n} \frac{c}{n-r+s}\binom{n}{r} = \frac{2c + o(1)}{n}\binom{n}{n/2} \leq (2c + o(1))\log m(n),$$

as $\log m(n) \geq \frac{1}{n}\binom{n}{n/2}$. Thus

$$\frac{\sum_{r\in R_n} m_{\mathcal{M}}(n,r)}{m(n)} = (m(n))^{2c-1+o(1)}.$$

As $c < 1/2$, this proves (3.4), and hence the lemma. □

Restricting to unlabelled matroids

Life can be made a little easier. In fact, the problem of bounding the number of matroids of rank $s \geq 3$ in $\mathcal{M}$ can be replaced by enumeration of unlabelled simple matroids of rank s. To make this precise, we require some terminology.

An *ordered partition* of a set E is a sequence $(A_1, A_2, \ldots, A_k)$ of pairwise disjoint sets, such that $\{A_1, A_2, \ldots, A_k\}$ is a partition of E. Thus, an ordered partition is a partition in which the order of the blocks matters. Write $\overrightarrow{\Pi}(E)$ for the collection of ordered partitions of E, and let $\overrightarrow{B}(n) := \left|\overrightarrow{\Pi}([n])\right|$ be the corresponding ordered Bell numbers. A straightforward argument shows that $\overrightarrow{B}(n) \leq n^n$. Let $\mathbb{M}^\circ(n, r)$ denote the class of unlabelled simple rank-r matroids on a ground set of cardinality n.

Lemma 3.5.3. *Let E be a set of cardinality n. There exists an injective function $\mathbb{M}(E, r) \to \mathbb{M}^\circ(\leq n, r) \times \overrightarrow{\Pi}(E)$.*

An explicit injective function can be constructed as follows. If M is a labelled matroid on E, write $[\![M]\!]$ for its unlabelling, which is obtained by forgetting the labels of M.

A matroid canonisation is a canonical way of labelling the elements of a matroid. It is a function $f_C \colon \mathbb{M} \to \mathbb{M}$ with the property that $f_C(M) \cong M$, and $f_C(M) \cong f_C(N)$ if and only if $M \cong N$. Without loss of generality, we may assume that $E(f_C(M)) = [|M|]$ for all M.

If f_C is a matroid canonisation, then $f(\mathrm{si}(M))$ is precisely a labelling of the independent elements of M in which two elements obtain the same label if and only if they are in the same parallel class. Such a labelling is an ordered partition, and the lemma follows after possibly squeezing in an extra class containing the loops of M.

As a matroid class is closed under isomorphism, for any class of matroids $\mathcal{M}$ and any matroid M, the statement $M \in \mathcal{M}$ does not depend on the labelling of M. Thus, the quantity $m^\circ_{\mathcal{M}}(n, r)$, which counts the number of unlabelled rank-r matroids on a ground set of cardinality n in $\mathcal{M}$, is well-defined.

Lemma 3.5.4. *Let $\mathcal{M}$ be closed under simplification and contraction. If there exist a constant $c < 1/2$, and integers n_0 and $s \geq 3$ such that*

$$\max_{n' \leq n} \log m^\circ_{\mathcal{M}}(n', s) \leq \frac{c}{n}\binom{n}{s} \qquad \textit{for all } n \geq n_0,$$

then $\mathcal{M}$ is small.

Proof. As $\mathcal{M}$ is closed under simplification, it follows from Lemma 3.5.3 that

$$\log m_{\mathcal{M}}(n, s) \leq \log(n+1) + \max_{n' \leq n} \log m^{\circ}_{\mathcal{M}}(n', s) + \log \overrightarrow{B}(n),$$

which, for all $n \geq n_0$, is at most

$$(n+1)\log(n+1) + \frac{c}{n}\binom{n}{s} = \frac{c+o(1)}{n}\binom{n}{s}.$$

It follows that $\log(1 + m_{\mathcal{M}}(n, s)) \leq \frac{c+o(1)}{n}\binom{n}{s}$, and hence $\mathcal{M}$ is small by Lemma 3.5.2. □

3.6 Applications

In this section we exhibit two applications of the Entropy Blow-Up Lemma. In the first application, we bound the number of matroids on ground set $[n]$. Clearly the class of all matroids is contraction-closed. Taking $\mathcal{M} = \mathbb{M}$ in an application of the Entropy Blow-Up Lemma, we can lift bounds on $m(n, 2)$ to bounds on $m(n)$.

Theorem 3.6.1. $\log m(n) = O\left(\frac{\log n}{n}\binom{n}{n/2}\right)$ *as* $n \to \infty$.

By Proposition 2.8.2, $\log m(n) \geq \frac{1}{n}\binom{n}{n/2}$. In Chapter 6, we will prove the complementary upper bound $\log m(n) \leq \frac{2+o(1)}{n}\binom{n}{n/2}$. The bound obtained by an application of the Entropy Blow-Up Lemma is therefore off only by a factor $\Theta(\log n)$. In fact, up to the constant factor, this is the best possible result using the Entropy Blow-Up Lemma. Although one would hope that bootstrapping the Entropy Blow-Up Lemma with a bound on $\log m(n, s)$ for some fixed $s > 2$ yields a stronger result, we will show in Chapter 5 that $\log m(n, s) \sim \frac{\log n}{n}\binom{n}{s}$ for all fixed $s > 2$, which implies that we will always obtain an excess $O(\log n)$-factor.

In the second application, we bound $m_{\mathcal{M}}(n)$ when $\mathcal{M}$ is one of $\mathrm{Ex}(U(2, k))$ (for some $k \geq 2$) or $\mathcal{M} = \mathrm{Ex}(U(3, 6))$. This confirms a few special cases of Conjecture 1.3.5.

Theorem 3.6.2. *Let* $N = U(2, k)$ *(for some* $k \geq 2$*) or* $N = U(3, 6)$*. Then* $\mathrm{Ex}(N)$ *is small.*

An upper bound on the number of matroids

Clearly the class of all matroids is contraction-closed. If we take $\mathcal{M} = \mathbb{M}$ in an application of the Entropy Blow-Up Lemma, we can lift bounds on $m(n, 2)$ to bounds on $m(n)$.

There is a one-to-one correspondence between $\mathbb{M}(n, 2)$ and partitions of $[n + 1]$ into at least three blocks, in which the block containing $n + 1$ corresponds to the set of loops, and every other block corresponds to a rank-1 flat. It follows that $m(n, 2) < B(n + 1)$, where $B(n)$ is the n-th Bell number. We require only the straightforward bound $B(n) \leq n^n$, which implies

$$\log(1 + m(n, 2)) \leq (n + 1) \log(n + 1). \tag{3.6}$$

Proof of Theorem 3.6.1. From the Entropy Blow-Up Lemma and (3.6), we obtain

$$\log(1 + m(n, r)) \leq \frac{(n - r + 3) \log(n - r + 3)}{\binom{n-r+2}{2}} \binom{n}{r} \qquad \text{for all } r \geq 2.$$

As $m(n) = \sum_r m(n, r)$, and $m(n, 0) + m(n, 1) \leq m(n, 2)$ for sufficiently large n, it follows that

$$\begin{aligned} \log m(n) &\leq \log n + \max_{r \geq 2} \frac{(n - r + 3) \log(n - r + 3)}{\binom{n-r+2}{2}} \binom{n}{r} \\ &= O\left(\frac{\log n}{n} \binom{n}{n/2}\right). \qquad \square \end{aligned}$$

Excluding a small uniform minor

Recall that $m^\circ_{\mathcal{M}}(n, 3)$ counts the number of unlabelled simple rank-3 matroids on n points in the class $\mathcal{M}$. We will bound $m^\circ_{\mathcal{M}}(n, 3)$ for each of the classes $\mathcal{M} = \text{Ex}(U(2, k))$ and $\mathcal{M} = \text{Ex}(U(3, 6))$. Theorem 3.6.2 then follows from an application of Lemma 3.5.4.

Lemma 3.6.3. *For all $k \geq 2$, there exists a constant C_k such that*

$$m^\circ_{\text{Ex}(U(2,k))}(n, 3) \leq C_k.$$

Proof. Let M be a simple unlabelled rank-3 matroid without $U(2, k)$-minor. We show that M has a bounded number of points; this, in turn, implies that there can only be finitely many such matroids.

Fix a point p in M. Note that p is on at most $k - 1$ lines, for otherwise $\text{si}(M/p)$ would be a line with at least k points. Every point

q is on a line with p, and every line through p contains at most $k-1$ points. Thus M contains at most $1+(k-1)(k-2)$ points. □

Lemma 3.6.4. *Let M be a simple rank-3 matroid on $n \geq 56$ points. If M does not have a $U(3,6)$-restriction, then M has lines ℓ, ℓ' such that $|E(M) \setminus (\ell \cup \ell')| \leq 1$.*

Proof. Let ℓ and ℓ' be the two longest lines of M, such that $|\ell| \geq |\ell'|$.

If $|\ell| \leq 7$, then all lines of M contain at most 7 elements. Let k be the largest integer such that M contains a $U(3,k)$-restriction. By assumption, $3 \leq k \leq 5$. Let $X \subseteq E(M)$ be such that $M|X \cong U(3,k)$. Every point in M lies on a line spanned by a pair of elements of X, and there are $\binom{k}{2}$ such lines. We obtain

$$n \leq k + \binom{k}{2}(7-2) \leq 55;$$

a contradiction. Thus, we may assume that $|\ell| > 7$, and hence that $|\ell \setminus \ell'| \geq 7$.

If $|\ell'| = 2$, then M contains one long line, and the lemma follows. If $E(M) \setminus (\ell \cup \ell')$ contains at most one point, then the conclusion of the lemma holds. Thus, we may assume that $|\ell'| \geq 3$, and that $E(M) \setminus (\ell \cup \ell')$ contains two distinct points p_1 and p_2. Let $\ell'' := \text{cl}(\{p_1, p_2\})$ be the line spanned by p_1 and p_2.

If $|\ell' \setminus (\ell \cup \ell'')| \geq 2$, then M contains a $U(3,6)$-restriction, which can be found as follows. Pick any two distinct points q_1 and q_2 in $\ell' \setminus (\ell \cup \ell'')$, and let $\mathcal{J}$ be the collection of lines spanned by pairs in $\{p_1, p_2, q_1, q_2\}$. The set $\ell \setminus (\cup_{j \in \mathcal{J}} j)$ contains at least two points, s_1 and s_2, say. The required restriction is found as $M|\{p_1, p_2, q_1, q_2, s_1, s_2\} \cong U(3,6)$.

On the other hand, if $|\ell' \setminus (\ell \cup \ell'')| = 1$ and $|E(M) \setminus (\ell \cup \ell'')| \geq 2$, then M has a $U(3,6)$-restriction which can be found as follows. Let $\ell' \cap \ell'' = \{q_1\}$, and let q_2 be the unique point in $\ell' \setminus (\ell \cup \ell'')$. Pick $s \in E(M) \setminus (\ell \cup \ell' \cup \ell'')$, and pick $i \in \{1,2\}$ such that $p_i \notin \text{cl}(s, q_2)$. Let $\mathcal{J}'$ be the set of lines spanned by pairs in $\{p_i, q_1, q_2, s\}$. The set $\ell \setminus (\cup_{j \in \mathcal{J}} j)$ contains at least two points, t_1 and t_2, say, and $M|\{p_i, q_1, q_2, s, t_1, t_2\} \cong U(3,6)$. □

The constant 56 in Lemma 3.6.4 is not the best possible, but it suffices for our purposes.

Lemma 3.6.5. $m^{\circ}_{\text{Ex}(U(3,6))}(n,3) = O(n^2)$.

Proof. Let M be an unlabelled simple rank-3 matroid on n points, where n is sufficiently large for the arguments in this proof to work.

By Lemma 3.6.4, there are lines ℓ, ℓ', and a point p such that $E(M) = \ell \cup \ell' \cup \{p\}$. If $\ell \neq \ell'$ and $p \notin \ell \cup \ell'$, then M is determined by (i) the length of the shortest of the lines ℓ and ℓ', (ii) whether or not they intersect, and (iii) the number of long lines through p. It follows that there are $O(n^2)$ such matroids.

In addition, there is one matroid for which $\ell = \ell'$, and there are at most n matroids for which $p \in \ell \cup \ell'$. □

We are now ready to prove Theorem 3.6.2.

Proof of Theorem 3.6.2. Let $N = U(2,k)$ (for some $k \geq 2$), or $N = U(3,6)$. By Lemma 3.6.3 (in the former case) and Lemma 3.6.5 (in the latter case),

$$\log\Big(1 + m^{\circ}_{\mathrm{Ex}(N)}(n,3)\Big) = o(n^2).$$

It follows that Ex(N) is small by Lemma 3.5.4. □

CHAPTER **4**

Cover complexity

This chapter is based on the journal paper [PvdP15a], which is joint work with Rudi Pendavingh.

4.1 In this chapter...

In this chapter, we consider encodings of matroids in terms of flats. In particular, we introduce *flat covers*. Roughly speaking, a collection of flats and their ranks is called a *flat cover* if it faithfully describes the matroid. We call the cardinality of a smallest such flat cover *cover complexity*, and show that this notion satisfies several properties that one would expect from a notion of structural complexity.

Intuitively, it is clear that there can only be a limited number of matroids of small complexity, and hence that a bound on the cover complexity of matroids in a class should imply a bound on the size of that class. This idea generalises the method behind Piff's [Pif73] upper bound on the number of matroids, $\log m(n) = O\left(\frac{\log n}{n} 2^n\right)$, which, in the language of this chapter, is proved by obtaining a uniform bound on the cover complexity of matroids in $\mathbb{M}(n)$.

The main technical result in this chapter is the Blow-Up Lemma for cover complexity, which bounds the cover complexity of a matroid in terms of the cover complexity of its minors of lower rank. The Blow-Up Lemma thus reduces questions of enumeration to questions about flats in fixed rank.

The remainder of this chapter is organised as follows. We define flat covers and cover complexity in Section 4.2, and in Section 4.3 we show that cover complexity satisfies a number of properties that one would expect from a measure of complexity. In Section 4.4, we introduce a local version of cover complexity, and use it to construct flat covers of small cardinality. In Section 4.5, we show how a uniform bound on the cover complexity of the matroids in a certain class results in a bound on the size of that class. The main technical result, the Blow-Up Lemma, is proved in Section 4.6. In Section 4.7, we apply the Blow-Up Lemma to obtain a bound on the number of matroids, and show that several minor-closed classes are small. Finally, in Section 4.8, we consider two classes of matroids with large cover complexity, and discuss the obstacles to the application of cover complexity to showing that $\mathrm{Ex}\big(W^3\big)$ and $\mathrm{Ex}(M(K_4))$ are small.

4.2 Flat covers and cover complexity

Let X be a dependent set in a matroid M, and let F be a flat of M. If $|X \cap F| > \mathrm{rk}(F)$, then we say that the pair $(F, \mathrm{rk}(F))$ *covers* X, in which case $(F, \mathrm{rk}(F))$ acts as a witness for the dependence of X. This inspires the following definition.

Definition 4.2.1. Let M be a matroid. A collection $\mathcal{Z} \subseteq \{(F, \mathrm{rk}(F)) : F \in \mathcal{F}(M)\}$ is a *flat cover* of M if each nonbasis of M is covered by at least one pair $(F, s) \in \mathcal{Z}$. The *cover complexity* of M, denoted by $\kappa(M)$, is the cardinality of a smallest flat cover of M.

Each flat cover of M is a subset of $\{(F, \mathrm{rk}(F)) : F \in \mathcal{F}(M)\}$. The following lemma is straightforward.

Lemma 4.2.2. *The flat covers of M form an upward-closed set in the lattice of subsets of* $\{(F, \mathrm{rk}(F)) : F \in \mathcal{F}(M)\}$.

The reason that we are interested in cover complexity is that flat covers describe matroids. More precisely, if $\mathcal{Z}$ is a flat cover of $M = (E, \mathcal{B})$, then M can be reconstructed from E, $\mathrm{rk}(M)$, and $\mathcal{Z}$, as

$$\mathcal{B} = \left\{X \in \binom{E}{\mathrm{rk}(M)} : |X \cap F| \leq s \text{ for all } (F, s) \in \mathcal{Z}\right\}. \tag{4.1}$$

Hence, cover complexity gives a bound on the amount of information necessary to describe M, which explains the use of the term complexity. The following result shows that the cardinality of a class can be bounded in terms of cover complexity.

Lemma 4.2.3. *Let $\mathcal{M}$ be a class of matroids. If $\kappa(M) \leq K(n,r)$ for all $M \in \mathcal{M} \cap \mathbb{M}(n,r)$, then $m_{\mathcal{M}}(n,r) \leq \sum_{i=0}^{\lfloor K(n,r) \rfloor} \binom{2^n r}{i}$.*

Proof. The function sending M to a flat cover of minimum size is an injective function $\mathcal{M} \cap \mathbb{M}(n,r) \to \binom{\mathscr{P}(E) \times \{0,1,\ldots,r-1\}}{\leq K(n,r)}$, and hence $m_{\mathcal{M}}(n,r)$ is bounded by the cardinality of the codomain. □

To close this section, we give two examples of flat covers: those corresponding to hyperplanes and those corresponding to circuit-closures. A circuit-closure is a flat that is spanned by a circuit.

Lemma 4.2.4. *Let M be a matroid.*

(i) If $\mathcal{H}$ is the collection of hyperplanes of M, then $\{(H, \mathrm{rk}(H)) : H \in \mathcal{H}\}$ is a flat cover.

(ii) If $\mathcal{C}$ is the collection of circuits of M, then $\{(\mathrm{cl}(C), \mathrm{rk}(C)) : C \in \mathcal{C}\}$ is a flat cover.

Proof. (i) If X is a nonbasis, then it is contained in at least one hyperplane. If H is such a hyperplane, then $(H, \mathrm{rk}(H))$ covers X. (ii) If X is a nonbasis, then it contains at least one circuit. If C is such a circuit, then X is covered by $(\mathrm{cl}(C), \mathrm{rk}(C))$. □

The second claim was essentially used by Piff [Pif73] in his upper bound on the number of matroids. He showed that the number of circuit-closures of a matroid on n elements is at most $\frac{2^{n+1}}{n+1}$. Using Lemma 4.2.3 with $\mathcal{M} = \mathbb{M}$ and $K(n,r) = \frac{2^{n+1}}{n+1}$, and summing over r, Piff's upper bound is retrieved.

Theorem 4.2.5 ([Pif73])**.** $\log m(n) = O\left(\frac{\log n}{n} 2^n\right)$ *as $n \to \infty$.*

Later in this chapter, we obtain a more refined bound on $\kappa(M)$, which leads to an improved upper bound on $m(n)$ in Theorem 4.7.1.

4.3 Properties of cover complexity

In this section, we show that cover complexity satisfies some properties one would expect of a complexity measure on matroids: The dual of a matroid is as complex as the matroid itself; the minors of M are less complex than M, so they should have lower cover complexity; M can be reconstructed from $M\backslash e$ and M/e (see e.g. [Oxl11, Proposition 3.1.27]), so the sum of their complexities should should bound the complexity of M. In addition, we show that cover complexity is particularly well-behaved with respect to relaxation of circuit-hyperplanes.

Lemma 4.3.1. *$\kappa(M) = \kappa(M^*)$.*

Proof. As $(M^*)^* = M$, it suffices to show that $\kappa(M^*) \leq \kappa(M)$. Let M be a matroid on E, and let $\mathcal{Z}$ be a flat cover of M of minimum cardinality. Define

$$\mathcal{Z}^* := \left\{ \left(\mathrm{cl}^*(E \setminus F), s + |E \setminus F| - \mathrm{rk}(M) \right) : (F, s) \in \mathcal{Z} \right\}.$$

If F is a flat of rank s in M, then the set $\mathrm{cl}^*(E \setminus F)$ is a flat of rank $s + |E \setminus F| - \mathrm{rk}(M)$ in M^*. We show that $\mathcal{Z}^*$ is a flat cover of M^*. Consider a nonbasis X of M^*. The set $E \setminus X$ is a nonbasis of M, so that there exists $(F, s) \in \mathcal{Z}$ with the property that $|(E \setminus X) \cap F| > s$. For such an F,

$$(\mathrm{cl}^*(E \setminus F), s + |E \setminus F| - \mathrm{rk}(M)) \in \mathcal{Z}^*.$$

We bound

$$|X \cap \mathrm{cl}^*(E \setminus F)| \geq |X \cap (E \setminus F)| = |E \setminus F| - |E \setminus X| + |F \setminus X|.$$

Using that $|E \setminus F| = \mathrm{rk}^*(E \setminus F) - s + \mathrm{rk}(M)$, $|E \setminus X| = \mathrm{rk}(M)$, and $F \setminus X = (E \setminus X) \cap F$, we obtain

$$|X \cap \mathrm{cl}^*(E \setminus F)| > \mathrm{rk}^*(\mathrm{cl}^*(E \setminus F)).$$

It follows that $\mathcal{Z}^*$ is a flat cover for M^*, and hence that $\kappa(M^*) \leq |\mathcal{Z}^*| \leq |\mathcal{Z}| = \kappa(M)$. □

Lemma 4.3.2. *If N is a minor of M, then $\kappa(N) \leq \kappa(M)$.*

Proof. We prove the lemma for single-element deletions, $N = M \backslash e$. Lemma 4.3.1 then implies that the lemma also holds for single-element contractions, and the full lemma then follows from an straightforward induction argument.

Let $\mathcal{Z}$ be a flat cover of M of minimum cardinality, and define

$$\mathcal{Z}' := \left\{ \left(F \setminus \{e\}, \mathrm{rk}_N(F \setminus \{e\}) \right) : (F, s) \in \mathcal{Z} \right\}.$$

Note that if F is a flat of M, then $F \setminus \{e\}$ is a flat of $M \backslash e$. We claim that $\mathcal{Z}'$ is a flat cover of N. As $|\mathcal{Z}'| \leq \kappa(M)$, this suffices to prove the lemma. To prove the claim, we distinguish between two cases.

If $\mathrm{rk}(N) = \mathrm{rk}(M)$, then the nonbases of N are the M-dependent r-sets avoiding e. This is a subset of the nonbases of M, and it follows that $\mathcal{Z}'$ is a flat cover of N.

On the other hand, if $\mathrm{rk}(N) = \mathrm{rk}(M) - 1$, then the nonbases of N are those $(\mathrm{rk}(M)-1)$-sets X such that $X \cup \{e\}$ is a nonbasis of M. If F covers $X \cup \{e\}$ in M, then

$$|X \cap (F \setminus \{e\})| = \begin{cases} |(X \cup \{e\}) \cap F| - 1 \geq \mathrm{rk}_M(F) \\ \qquad\qquad > \mathrm{rk}_M(F \setminus \{e\}) = \mathrm{rk}_N(F \setminus \{e\}) & \text{if } e \in F \\ |(X \cup \{e\}) \cap F| > \mathrm{rk}_M(F) = \mathrm{rk}_N(F \setminus \{e\}) & \text{if } e \notin F. \end{cases}$$

It follows that $F \setminus \{e\}$ covers X in N, and hence that $\mathcal{Z}'$ is a flat cover of N. □

Lemma 4.3.3. *Let M be a matroid, and let $e \in E(M)$. If e is neither a loop nor a coloop of M, then $\kappa(M) \leq \kappa(M\backslash e) + \kappa(M/e)$.*

Proof. Let $\mathcal{Z}_{M\backslash e}$ and $\mathcal{Z}_{(M/e)^*}$ be flat covers of $M\backslash e$ and $(M/e)^*$ of minimum cardinality. Assume that e is neither a loop nor a coloop. Let

$$\mathcal{Z}' := \big\{ \big(\mathrm{cl}_M(F), \mathrm{rk}_M(F) \big) : (F, s) \in \mathcal{Z}_{M\backslash e} \big\}$$

and let

$$\mathcal{Z}'' := \big\{ \big(\mathrm{cl}_M(E \setminus \mathrm{cl}_{M^*}(F)), \mathrm{rk}_M(E \setminus \mathrm{cl}_{M^*}(F) \big) : (F, s) \in \mathcal{Z}_{(M/e)^*} \big\}.$$

We claim that $\mathcal{Z}' \cup \mathcal{Z}''$ is a flat cover of M, which immediately implies the lemma. To prove the claim, consider a nonbasis X of M.

If $e \in X$, then X is a nonbasis of $M\backslash e$, so it is covered by some $(F, \mathrm{rk}_{M\backslash e}(F)) \in \mathcal{Z}_{M\backslash e}$. It follows that $(\mathrm{cl}_M(F), \mathrm{rk}_M(F)) \in \mathcal{Z}'$ covers X in M.

On the other hand, if $e \notin X$, then $E \setminus X$ is a nonbasis in $(M/e)^*$, so it is covered by some $(F, \mathrm{rk}_{(M/e)^*}(F)) \in \mathcal{Z}_{(M/e)^*}$. It then follows that $(\mathrm{cl}_{M^*}(F), \mathrm{rk}_{M^*}(F))$ covers $E \setminus X$ in M^*, and hence that the pair $(\widetilde{F}, \mathrm{rk}_M(\widetilde{F})$, with $\widetilde{F} := \mathrm{cl}_M(E \setminus \mathrm{cl}_{M^*}(F))$, covers X in M. □

Cover complexity provides a different characterisation of uniform matroids.

Lemma 4.3.4. *M is a uniform matroid if and only if $\kappa(M) = 0$.*

Proof. Let M be a matroid of rank r on E. M is uniform if and only if $\mathcal{B}(M) = \binom{E}{r}$. Thus, if M is a uniform matroid, then it does not have any nonbases, from which it follows that the empty set is a flat cover for M. On the other hand, if the empty set is a flat cover for M, then it follows from (4.1) that $\mathcal{B}(M) = \binom{E}{r}$, and hence that M is uniform. □

Relaxing circuit-hyperplanes decreases the cover complexity of a matroid.

Lemma 4.3.5. *If N can be obtained from M by relaxing a circuit-hyperplane, then $\kappa(M) = \kappa(N) + 1$.*

Proof. Suppose that N is obtained from M by relaxing the circuit-hyperplane H. As H is the only flat that covers H, a collection $\mathcal{Z}$ is a flat cover of N if and only if $\mathcal{Z} \cup \{H\}$ is a flat cover of M. The claim follows. □

Recall that $\mathcal{W}(M)$ is the collection of circuit-hyperplanes of M. It follows from the previous lemma that cover complexity is at least the number of circuit-hyperplanes of a matroid.

Corollary 4.3.6. $\kappa(M) \geq |\mathcal{W}(M)|$. *Moreover, equality holds if and only if M is a sparse paving matroid.*

Proof. Let N be the matroid that is obtained from M by relaxing all its circuit-hyperplanes. Repeated application of Lemma 4.3.5 shows that $\kappa(M) = |\mathcal{W}(M)| + \kappa(N)$. As $\kappa(N) \geq 0$, it follows that $\kappa(M) \geq |\mathcal{W}(M)|$.

To prove the second claim, note that M is sparse paving if and only if all its nonbases are circuit-hyperplanes, which is the case if and only if N is a uniform matroid. Therefore, by Lemma 4.3.4, M is sparse paving if and only if $\kappa(N) = 0$, which concludes the proof. □

4.4 Bounding cover complexity

A notion related to flat covers is that of a local cover. A local cover of a matroid M of rank r is a collection of flats (and their ranks) that allows us to identify the nonbases in the neighbourhood of an r-set. In this section, we prove two results on local covers. The first states that small local covers exist: each r-set admits a local cover of cardinality at most r. The second result is that local covers can be combined to form flat covers. Combining these results results in an upper bound on cover complexity.

Recall that $N(X)$ denotes the neighbourhood of $X \in \binom{E}{r}$ in $J(E, r)$.

Definition 4.4.1. Let M be a matroid of rank r on E, and let $X \in \binom{E}{r}$. A collection $\mathcal{Z}_X \subseteq \{(F, \mathrm{rk}(F)) : F \in \mathcal{F}(M)\}$ is a *local cover* of M at X, if each nonbasis in $\{X\} \cup N(X)$ is covered by an element from $\mathcal{Z}_X$.

Clearly any flat cover is a local cover at X, for every $X \in \binom{E}{r}$. However, we can be much more economical.

Lemma 4.4.2. *Let M be a matroid of rank r on E. For every $X \in \binom{E}{r}$, there exists a local cover $\mathcal{Z}_X$ at X such that $|\mathcal{Z}_X| \leq r$.*

Proof. Fix $X \in \binom{E}{r}$, and define

$$\mathcal{Z}_X := \{(\mathrm{cl}(X \setminus \{x\}), \mathrm{rk}(X \setminus \{x\})) : x \in X\}.$$

Clearly, $|\mathcal{Z}_X| \leq r$. To show that $\mathcal{Z}_X$ is a local cover at X, consider a nonbasis $Y \in \{X\} \cup N(X)$.

If $Y = X$, then there exists $x_0 \in X$ such that $Y \subseteq \mathrm{cl}(X \setminus \{x_0\})$, in which case

$$|Y \cap \mathrm{cl}(X \setminus \{x_0\})| = r > \mathrm{rk}(X \setminus \{x_0\}),$$

and so Y is covered by $(\mathrm{cl}(X \setminus \{x_0\}), \mathrm{rk}(X \setminus \{x_0\}))$.

The case $Y \in N(X)$ remains. Suppose that $Y = (X \setminus \{x_0\}) \cup \{y_0\}$. If $(\mathrm{cl}(X \setminus \{x_0\}), \mathrm{rk}(X \setminus \{x_0\}))$ covers Y, then we are done. Otherwise

$$r - 1 = |X \setminus \{x_0\}| \leq |Y \cap \mathrm{cl}(X \setminus \{x_0\})| \leq \mathrm{rk}(X \setminus \{x_0\}) \leq r - 1,$$

so that equality holds throughout. This implies that $y_0 \notin \mathrm{cl}(X \setminus \{x_0\})$, and hence that Y is a basis. □

Knowing that X is dependent allows us to construct an even smaller local cover.

Lemma 4.4.3. *Let M be a matroid of rank r on E, and let X be a nonbasis of M. There exists a local cover $\mathcal{Z}_X$ at X such that $|\mathcal{Z}_X| \leq 2$.*

Proof. We distinguish between two cases, depending on the rank of X.

If $\mathrm{rk}(X) < r - 1$, pick $\mathcal{Z}_X = \{(\mathrm{cl}(X), \mathrm{rk}(X))\}$. The set $\mathcal{Z}_X$ is a local cover at X, since for every $Y \in \{X\} \cup N(X)$,

$$|Y \cap \mathrm{cl}(X)| \geq r - 1 > \mathrm{rk}(X).$$

If $\mathrm{rk}(X) = r - 1$, then there is a unique circuit C contained in X. Pick $\mathcal{Z}_X = \{(\mathrm{cl}(X), \mathrm{rk}(X)), (\mathrm{cl}(C), \mathrm{rk}(C))\}$. To show that $\mathcal{Z}_X$ is a local cover at X, first note that X is covered by $(\mathrm{cl}(X), \mathrm{rk}(X))$. It remains to show that each nonbasis $Y \in N(X)$ is covered by some some element of $\mathcal{Z}_X$. Let $Y = (X \setminus \{x_0\}) \cup \{y_0\}$ be such a nonbasis. By Lemma 2.6.4,

Y is a nonbasis if and only if $x_0 \notin C$, or $y_0 \in \mathrm{cl}(X)$. In the former case, Y is covered by $(\mathrm{cl}(C), \mathrm{rk}(C))$, while in the latter case it is covered by $((\mathrm{cl}(X), \mathrm{rk}(X))$. □

By combining such small local covers in a clever way, we can obtain a small flat cover. First, we require an additional result.

A local cover at X identifies the nonbases in $\{X\} \cup N(X)$. By combining local covers, we are able to identify the nonbases in a larger area. Of particular interest is the situation in which we have a collection of local covers at the members of a so-called *dominating set*: a subset $\mathcal{X} \subseteq V(G)$ is called dominating if every vertex in $V(G) \setminus \mathcal{X}$ has a neighbour in $\mathcal{X}$. The cardinality of a minimum dominating set in G is denoted $\gamma(G)$. The following lemma is easily verified.

Lemma 4.4.4. *Let M be a matroid of rank r on E. If $\mathcal{X} \subseteq \binom{[n]}{r}$, and $\mathcal{Z}_X$ is a local cover at X for each $X \in \mathcal{X}$, then $\bigcup_{X \in \mathcal{X}} \mathcal{Z}_X$ covers each nonbasis in $\mathcal{X} \cup N(\mathcal{X})$. In particular, if $\mathcal{X}$ is a dominating set in $J(E, r)$, then $\bigcup_{X \in \mathcal{X}} \mathcal{Z}_X$ is a flat cover of M.*

A probabilistic argument (see e.g. [AS08, Theorem 1.2.2]) shows that if G is a graph on N vertices with minimum degree δ, then

$$\gamma(G) \leq \frac{\ln(\delta + 1) + 1}{\delta + 1} N. \tag{4.2}$$

Lemma 4.4.5. *Let M be a matroid of rank r on a ground set E of cardinality n. Then*

$$\kappa(M) \leq \frac{\ln(r(n-r)+1)+1}{r(n-r)+1} \binom{n}{r} \min\{r, n-r\}.$$

Proof. As $\kappa(M) = \kappa(M^*)$, we may assume that $2r \leq n$. Let $\mathcal{X}$ be a dominating set of minimum cardinality in $J(E, r)$. As the Johnson graph has $\binom{n}{r}$ vertices, and is regular of degree $r(n-r)$, it follows from (4.2) that $|\mathcal{X}| \leq \frac{\ln(r(n-r)+1)+1}{r(n-r)+1}\binom{n}{r}$. By Lemma 4.4.2, to each $X \in \mathcal{X}$ we may associate a local cover $\mathcal{Z}_X$ of cardinality at most r. By Lemma 4.4.4, the collection $\bigcup_{X \in \mathcal{X}} \mathcal{Z}_X$ is a flat cover of cardinality at most $|\mathcal{X}|r$, which implies the lemma. □

4.5 Bounding the size of a class by cover complexity

As a matroid of rank r on ground set E is determined by any of its flat covers, bounding the cover complexity of a class should result in a bound on the cardinality of that class. This is made precise in the following lemma, which is related to Lemma 4.2.3.

Lemma 4.5.1. *Let $\mathcal{M}$ be a class of matroids, and let $g\colon \mathbb{Z}_{\geq 0} \to \mathbb{R}$ be a function such that $1/\binom{n}{n/2} \leq g(n) \leq 1$ and $\kappa(M) \leq g(n)\binom{n}{n/2}$ for all $M \in \mathcal{M} \cap \mathbb{M}(n)$, for sufficiently large n. Then*

$$\log m_{\mathcal{M}}(n) \leq g(n)\binom{n}{n/2} \log \frac{\sqrt{8\pi} n^{3/2}(1+o(1))}{g(n)}.$$

Proof. Let $h(n) = g(n)\binom{n}{n/2}$. A function $\mathcal{M} \cap \mathbb{M}(n,r) \to \binom{\mathscr{P}(E)\times\{0,1,\ldots,n\}}{\leq \lfloor h(n) \rfloor}$ sending M to a flat cover of M of minimum cardinality is injective . It follows that

$$\begin{aligned}
|\mathcal{M} \cap \mathbb{M}(n,r)| &\leq \sum_{i=0}^{\lfloor h(n) \rfloor} \binom{2^n(n+1)}{i} \\
&\leq \exp_2\left(\mathscr{H}\left(\frac{h(n)}{2^n(n+1)}\right) 2^n(n+1)\right).
\end{aligned}$$

Summing over r and taking logarithms, we obtain

$$\begin{aligned}
\log m_{\mathcal{M}}(n) &\leq \log(n+1) + \mathscr{H}\left(\frac{h(n)}{2^n(n+1)}\right) 2^n(n+1) \\
&\leq h(n) \log \frac{2^{n+2}(n+1)+1}{h(n)}.
\end{aligned}$$

The result now follows as $h(n) = g(n)\sqrt{\frac{2}{\pi n}}2^n\,(1-o(1))$. □

4.6 Fractional cover complexity and the Blow-Up Lemma

Fractional cover complexity

Cover complexity can be obtained as the value of an integer linear programme:

$$\begin{aligned} \kappa(M) = \min \quad & \sum_{F \in \mathcal{F}(M)} z(F) & & \\ \text{s.t.} \quad & \sum_{F\colon F \text{ covers } X} z(F) \geq 1 & & \text{for all } X \in \mathcal{K}(M) \\ & z(F) \in \mathbb{Z}_{\geq 0} & & \text{for all } F \in \mathcal{F}(M). \end{aligned} \tag{4.3}$$

The *linear relaxation* of (4.3) is obtained by allowing the variables to take non-integral values, i.e. by replacing the integrality constraint "$z(F) \in \mathbb{Z}_{\geq 0}$" with "$z(F) \geq 0$". We call a feasible solution to the relaxation a *fractional cover* of M. In addition, we write $\kappa^*(M)$ for the value of the relaxation, and refer to $\kappa^*(M)$ as the *fractional cover complexity* of M.

Clearly $\kappa^*(M) \leq \kappa(M)$. Using a standard randomised rounding technique (cf. [You95]), we may also put an upper bound on $\kappa(M)$ in terms of $\kappa^*(M)$.

Lemma 4.6.1. *For all matroids M of rank r on a ground set of n elements,*

$$\kappa(M) \leq \left\lceil \kappa^*(M) \left(1 + \ln \frac{\binom{n}{r}}{\kappa^*(M)} \right) \right\rceil .$$

Proof. Let z be an fractional cover of M of value $\kappa^*(M)$. Define a function $p\colon \mathcal{F}(M) \to [0,1]$ by $p(F) := z(F)/\kappa^*(M)$. As the entries of p sum to 1, p is a probability mass function on $\mathcal{F}(M)$.

Let

$$m := \left\lceil \kappa^*(M) \ln \left(\binom{n}{r} \Big/ \kappa^*(M) \right) \right\rceil ,$$

and let $\boldsymbol{\mathcal{Z}}_0$ be a random subset of $\mathcal{F}(M)$, obtained by drawing objects (independently, with repetitions) according to p. The probability that any fixed nonbasis X is not covered by $\boldsymbol{\mathcal{Z}}_0$ is

$$\left(1 - \sum_{F\colon F \text{ covers } X} \frac{z(F)}{\kappa^*(M)} \right)^m \leq \left(\mathrm{e}^{-1/\kappa^*(M)} \right)^m \leq \frac{\kappa^*(M)}{\binom{n}{r}}, \tag{4.4}$$

where we used the inequality $1 - x \leq \mathrm{e}^{-x}$. Let $\boldsymbol{\mathcal{E}}$ be the collection of those nonbases that are not covered by $\boldsymbol{\mathcal{Z}}_0$. By (4.4), the expected number of elements in $\boldsymbol{\mathcal{E}}$ is at most $\kappa^*(M)$.

The collection $\boldsymbol{\mathcal{Z}} := \boldsymbol{\mathcal{Z}}_0 \cup \{(\mathrm{cl}(X), \mathrm{rk}(X)) : X \in \boldsymbol{\mathcal{E}}\}$ is a flat cover of M, and it contains in expectation at most $m + \kappa^*(M)$ elements. Hence, there is a flat cover of at most this cardinality. □

The Blow-Up Lemma

Our main use for fractional cover complexity is the following result, the *Blow-Up Lemma* which states that bounds on fractional cover complexity can be obtained from bounds on fractional cover complexity of smaller matroids.

Lemma 4.6.2 (Blow-Up Lemma)**.** *Let $\mathcal{M}$ be a class of matroids that is closed under contraction. For any $t < r < n$,*

$$\frac{1}{\binom{n}{r}} \max\left\{\kappa^*(M) : M \in \mathcal{M} \cap \mathbb{M}(n, r)\right\} \\ \leq \frac{1}{\binom{n-t}{r-t}} \max\left\{\kappa^*(M) : M \in \mathcal{M} \cap \mathbb{M}(n-t, r-t)\right\}.$$

Proof. Let $M \in \mathcal{M} \cap \mathbb{M}(n, r)$. We construct a fractional cover z of bounded cost from a collection of "local" fractional covers z^S, one for each t-subset S of $[n]$. Let S be such a set; the construction of z^S depends on whether or not S is dependent or independent in M:

- If S is dependent, then put $z^S(F) = 1$ if $F = \mathrm{cl}_M(S)$, and $z^S(F) = 0$ otherwise. Note that $\mathrm{cl}_M(S)$ covers each r-set which contains S.
- If S is independent, then let z' be a fractional cover of the contraction M/S of value $\kappa^*(M/S)$, and let $z^S(F) = z'(F \setminus S)$ if $S \subseteq F$, and $z^S(F) = 0$ otherwise.

Define $z \colon \mathcal{F}(M) \to \mathbb{R}_{\geq 0}$ by putting

$$z(F) := \frac{1}{\binom{r}{t}} \sum_{S \in \binom{[n]}{t}} z^S(F).$$

Clearly, $z(F) \geq 0$ for all $F \in \mathcal{F}(M)$. We claim that z is a fractional cover of M. To prove this, let X be any nonbasis, and note that

$$\begin{aligned}\sum_{F\colon F \text{ covers } X} z(F) &= \frac{1}{\binom{r}{t}} \sum_{F\colon F \text{ covers } X} \sum_{S \in \binom{[n]}{t}} z^S(F)\\ &= \frac{1}{\binom{r}{t}} \sum_{S \in \binom{[n]}{t}} \sum_{F\colon F \text{ covers } X} z^S(F)\\ &\geq \frac{1}{\binom{r}{t}} \sum_{S \in \binom{X}{t}} \sum_{F\colon F \text{ covers } X} z^S(F) \geq 1.\end{aligned}$$

Thus, z is a fractional cover, and it remains to bound $\sum_{F \in \mathcal{F}(M)} z(F)$. If S is independent in M, then M/S is isomorphic to a matroid in $\mathcal{M} \cap \mathbb{M}(n-t, r-t)$, so that for each such S,

$$\sum_{F \in \mathcal{F}(M)} z^S(F) \leq \max\bigl\{\kappa^*(M) : M \in \mathcal{M} \cap \mathbb{M}(n-t, r-t)\bigr\}. \tag{4.5}$$

In fact, (4.5) holds for dependent S as well, as in that case the left-hand side equals 1. We obtain

$$\begin{aligned}\kappa^*(M) \leq \sum_{F \in \mathcal{F}(M)} z(F) &= \frac{1}{\binom{r}{t}} \sum_{S \in \binom{[n]}{t}} \sum_{F \in \mathcal{F}(M)} z^S(F)\\ &\leq \frac{\binom{n}{t}}{\binom{r}{t}} \max\bigl\{\kappa^*(M) : M \in \mathcal{M} \cap \mathbb{M}(n-t, r-t)\bigr\},\end{aligned}$$

where the final step follows from (4.5). The lemma now follows from the identity $\binom{n}{t}\binom{n-t}{r-t} = \binom{n}{r}\binom{r}{t}$. □

Bounding the size of a class using the Blow-Up Lemma

Combining the Blow-Up Lemma with the results in Section 4.5, we obtain a bound on the size of a contraction-closed class in terms of the cover complexity of the matroids in the class of a certain fixed rank.

Theorem 4.6.3. *Let $\mathcal{M}$ be a contraction-closed class of matroids. If, for some natural number $s \geq 1$ and nonincreasing function $f\colon \mathbb{Z}_{\geq 0} \to \mathbb{R}$,*

$$\max\bigl\{\kappa(M) : M \in \mathcal{M} \cap \mathbb{M}(n, s)\bigr\} \leq \frac{f(n)}{n}\binom{n}{s},$$

then

$$\log m_{\mathcal{M}}(n) = O\left(\frac{f(n)\log^2 n}{n}\binom{n}{n/2}\right).$$

The theorem is proved in three steps: (i) use the Blow-Up Lemma to obtain a bound $\kappa^*(M)$ that is valid for all $M \in \mathcal{M} \cap \mathbb{M}(n,r)$, $s \leq r \leq n/2$; (ii) use the rounding result to obtain a bound on $\kappa(M)$ for all $M \in \mathcal{M} \cap \mathbb{M}(n)$; (iii) apply Lemma 4.5.1 to obtain the result.

Proof. We may assume that $f(n) = \Omega\left(n^{1-s}\right)$.

Step (i): Let $s \leq r \leq n/2$. An application of the Blow-Up Lemma, Lemma 4.6.2 (with $t = r - s$) yields

$$\begin{aligned}
&\max\left\{\kappa^*(M) : M \in \mathcal{M} \cap \mathbb{M}(n,r)\right\} \\
&\qquad \leq \frac{\binom{n}{r}}{\binom{n-r+s}{s}} \max\left\{\kappa(M) : M \in \mathcal{M} \cap \mathbb{M}(n-r+s,s)\right\} \\
&\qquad\qquad \leq \frac{f(n-r+s)}{n-r+s}\binom{n}{r}.
\end{aligned}$$

Step (ii): Using the rounding result, Lemma 4.6.1, we obtain

$$\begin{aligned}
&\max\left\{\kappa(M) : M \in \mathcal{M} \cap \mathbb{M}(n,r)\right\} \\
&\qquad \leq \left\lceil \frac{f(n-r+s)}{n-r+s}\binom{n}{r}\left(1 + \ln\frac{n-r+s}{f(n-r+s)}\right)\right\rceil \\
&\qquad\qquad \leq \frac{2f(\lfloor n/2 \rfloor)}{n}\binom{n}{n/2}\left(1 + \ln\frac{n}{f(n)}\right) + 1
\end{aligned}$$

for all $s \leq r \leq n/2$. Since $\kappa(M) \leq \binom{n}{s}$ for all $M \in \mathbb{M}(n,r)$, $r < s$, and $\kappa(M) = \kappa(M^*)$, it follows that

$$\max\left\{\kappa(M) : M \in \mathcal{M} \cap \mathbb{M}(n)\right\} = O\left(\frac{f(n)\log n}{n}\binom{n}{n/2}\right).$$

Step (iii): An application of Lemma 4.5.1, with $g(n) = Cf(n)\log n$ for a sufficiently large constant C, concludes the proof. □

Theorem 4.6.3 has the following corollary.

Corollary 4.6.4. *Let $\mathcal{M}$ be a contraction-closed class of matroids. If, for some natural number $s \geq 1$,*

$$\max\left\{\kappa(M) : M \in \mathcal{M} \cap \mathbb{M}(n,s)\right\} = o\left(\frac{n^{s-1}}{\log^2 n}\right) \qquad \text{as } n \to \infty,$$

then $\mathcal{M}$ is a small class.

Proof. An application of Theorem 4.6.3 with $f(n) = o(1/\log^2 n)$, implies

$$\log m_{\mathcal{M}}(n) = o\left(\frac{1}{n}\binom{n}{n/2}\right).$$

Comparing to the lower bound $\log m(n) \geq \frac{1}{n}\binom{n}{n/2}$, it follows that

$$\log\frac{m_{\mathcal{M}}(n)}{m(n)} \leq -\frac{1-o(1)}{n}\binom{n}{n/2} \to -\infty,$$

which proves the claim. □

The dual programme

Consider the dual linear programme of the linear relaxation of (4.3):

$$\begin{aligned} \mu(M) = \max \quad & \sum_{X\in\mathcal{K}(M)} y(X) & & \\ \text{s.t.} \quad & \sum_{X:\ F \text{ covers } X} y(X) \leq 1 & & \text{for all } F \in \mathcal{F}(M), \\ & y(X) \in \mathbb{Z}_{\geq 0} & & \text{for all } X \in \mathcal{K}(M), \end{aligned} \tag{4.6}$$

and write $\mu^*(M)$ for the value of its relaxation. By linear programming duality,

$$\kappa(M) \leq \kappa^*(M) = \mu^*(M) \leq \mu(M).$$

The programme (4.6) asks for a maximum subset of the nonbases such that each flat covers at most one of them. Thus, we obtain the following generalisation of the first claim in Lemma 4.3.6.

Lemma 4.6.5. *Let $\mathcal{X} \subseteq \mathcal{K}(M)$ be such that each flat $F \in \mathcal{F}(M)$ covers at most one of the nonbases in $\mathcal{X}$. Then $\kappa(M) \geq |\mathcal{X}|$.*

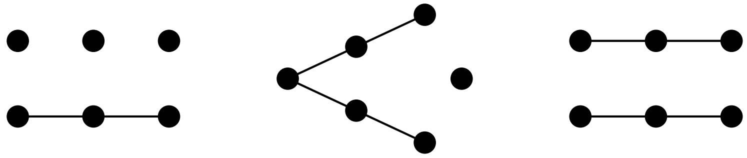
4.7 Applications

In this section, we prove the following results.

Theorem 4.7.1. $\log m(n) = O\left(\frac{\log^2 n}{n}\binom{n}{n/2}\right)$ *as $n \to \infty$.*

Theorem 4.7.2. *Let N be one of $U(2,k)$ (for any $k \geq 2$), $U(3,6)$, P_6, Q_6, or R_6. Almost every matroid has an N-minor.*

Geometric representations of each of the named matroids P_6, Q_6 and R_6 are displayed in Figure 4.1.



(a) P_6. **(b)** Q_6. **(c)** R_6.

Figure 4.1: The named matroids appearing in Theorem 4.7.2.

Bounding the number of matroids

We provide two alternative proofs of Theorem 4.7.1. The first proof uses Theorem 4.6.3 to turn a bound on the cover complexity of matroids of rank 1 into a bound on $m(n)$. The second approach applies the upper bound on $\kappa(M)$ from Lemma 4.5.1 to obtain a bound that is qualitatively the same.

Proof of Theorem 4.7.1. If M is matroid of rank 1, then $\mathcal{Z} := \{\mathrm{cl}_M(\emptyset)\}$ is a flat cover of M, so $\kappa(M) \leq 1$. Let $\mathcal{M}$ be the class of all matroids. An application of Theorem 4.6.3 with $s = 1$, and $f(n) \equiv 1$ yields the desired inequality. □

Proof of Theorem 4.7.1 (alternative). Let

$$K(n, r) := \frac{\ln(r(n-r)+1)+1}{r(n-r)+1}\binom{n}{r}\min\{r, n-r\}.$$

As $K(n, n-r) = K(n, r)$ for all $0 \leq r \leq n$, and $K(n, r+1) \geq K(n, r)$ for all $0 \leq r \leq \lfloor n/2 \rfloor - 1$, it follows that $K(n, r) \leq K(n, \lfloor n/2 \rfloor)$ for all $0 \leq r \leq n$. An application of Lemma 4.5.1 with $\mathcal{M} = \mathbb{M}$, and $g(n) = K(n, \lfloor n/2 \rfloor)/\binom{n}{n/2}$ shows that, for sufficiently large n,

$$\log m(n) \leq K(n, \lfloor n/2 \rfloor) \log \frac{2n^{5/2}}{\ln n},$$

from which the claim follows. □

Excluding a long line

First, we prove Theorem 4.7.2 for the special case $N = U(2, k)$. This case follows from the following lemma after an application of Corollary 4.6.4 (with $s = 2$).

Lemma 4.7.3. *If $M \in \mathrm{Ex}(U(2, k)) \cap \mathbb{M}(n, 2)$, then $\kappa(M) \leq k$.*

Proof. As M has rank 2, we can write $E(M) = E_0 \dot{\cup} E_1 \dot{\cup} E_2 \dot{\cup} \ldots \dot{\cup} E_m$, such that

(i) $E_i \neq \emptyset$ for all $i > 0$, and

(ii) $\{a, b\}$ is a basis of M if and only if there are distinct $i, j > 0$ such that $a \in E_i$ and $b \in E_j$.

If this is the case, then $\mathrm{rk}(E_0) = 0$, and $\mathrm{rk}(E_0 \cup E_i) = 1$ for all $i > 0$. It follows that

$$\mathcal{Z} := \{(E_0, 0)\} \cup \{(E_0 \cup E_i, 1) : i \in [m]\}$$

is a flat cover of M, and so $\kappa(M) \leq m + 1$. Picking $e_i \in E_i$ for all $i \in [m]$, we find that the restriction $M|\{e_1, e_2, \ldots, e_m\} \cong U(2, m)$, so $m \leq k - 1$, and hence $\kappa(M) \leq k$. □

Excluding rank-3 minors

Four cases of Theorem 4.7.2 remain, each of which concerns a matroid of rank 3. We prove these cases by an application of Corollary 4.6.4 with $s = 3$. In Lemma 4.7.5–Lemma 4.7.8 below, we prove for each of these cases that the cover complexity of matroids in $\mathrm{Ex}(N) \cap \mathbb{M}(n, 3)$ is at most linear in n. The following lemma shows that it suffices to consider the number of long lines in such matroids.

Lemma 4.7.4. *Let $M \in \mathbb{M}(n, 3)$ have L long lines. Then $\kappa(M) \leq 1 + n/2 + L$.*

Proof. Consider the collection of flats $\mathcal{Z} := \mathcal{Z}_0 \cup \mathcal{Z}_1 \cup \mathcal{Z}_2$, where $\mathcal{Z}_0 := \{\mathrm{cl}(\emptyset)\}$, $\mathcal{Z}_1 := \{F \in \mathcal{F}(M) : \mathrm{rk}(F) = 1, |F| > 1\}$, and

$$\mathcal{Z}_2 := \left\{ F \in \mathcal{F}(M) : \begin{array}{l} \mathrm{rk}(F) = 2 \\ F \text{ contains at least three rank-1 flats} \end{array} \right\}.$$

We claim that $\mathcal{Z}$ is a flat cover of M. If X is a nonbasis of M, then either it contains a loop (in which case it is covered by $\mathcal{Z}_0$), or it contains a pair of parallel elements (in which case it is covered by $\mathcal{Z}_1$), or it spans a long line (in which case it is covered by $\mathcal{Z}_2$). We have $|\mathcal{Z}_0| = 1$, $|\mathcal{Z}_1| \leq n/2$, and $|\mathcal{Z}_2| = L$, and so $\kappa(M) \leq |\mathcal{Z}| \leq 1 + n/2 + L$. □

Excluding $U(3, 6)$ The special case $N = U(3, 6)$ of Theorem 4.7.2 was already proved in Theorem 3.6.2. The working ingredient in that argument was a structural result for matroids of rank 3 without $U(3, 6)$-restriction, Lemma 3.6.4, which states that the ground set of such a matroid is the union of two lines and a point, provided that the matroid is sufficiently large. Here, we use the same structural result to bound the cover complexity of such a matroid.

Lemma 4.7.5. *Let $M \in \mathbb{M}(n, 3)$. If M does not have a $U(3, 6)$-minor, then $\kappa(M) \leq 496 + n$.*

Proof. Let $M \in \mathbb{M}(n, 3)$ be a matroid without a $U(3, 6)$-minor, and let $M' = \text{si}(M)$. We bound the number of long lines of M', after which the lemma follows from Lemma 4.7.4.

If $n \leq 55$, then M has at most $\binom{55}{2}/3 = 495$ long lines. If $n \geq 56$, then by Lemma 3.6.4 there are lines ℓ, ℓ' and a point p such that $E(M) = \ell \cup \ell' \cup \{p\}$. If either $\ell = \ell'$, or $p \in \ell \cup \ell'$, then M contains at most 2 long lines; otherwise, M contains at most $\lfloor (n-1)/2 \rfloor + 2$ long lines. □

Excluding P_6, Q_6, or R_6 We start with bounding the cover complexity of matroids without Q_6-minor.

Lemma 4.7.6. *Let $M \in \mathbb{M}(n, 3)$. If M does not have a Q_6-minor, then $\kappa(M) \leq 41 + n$.*

Proof. Let $M' := \text{si}(M)$. If M' does not have any intersecting pair of long lines, then M' has at most $n/3$ long lines, and then $\kappa(M) \leq 1 + n/2 + n/3$ by Lemma 4.7.4. So suppose M' has two long lines ℓ and ℓ' that intersect in point e. If $E(M') = \ell \cup \ell'$, then ℓ and ℓ' are the only two long lines of M', and then $\kappa(M) \leq 1 + n/2 + 2$. So consider a point $f \in E(M') \setminus (\ell \cup \ell')$. Each point $p \in \ell \setminus \{e\}$ determines a line ℓ_p through p and f that intersects ℓ' in at most one point, so that if $|\ell'| > 4$, we may obtain a Q_6-restriction of M' on $\{e, f, p, q, p', q'\}$ by arbitrarily taking $p, q \in \ell \setminus \{e\}$ and $p', q' \in \ell' \setminus (\{e\} \cup \ell_p \cup \ell_q)$. So $|\ell'| \leq 4$, and by symmetry $|\ell| \leq 4$ as well.

If $|\ell'| = 4$, and there is some $f \in E(M') \setminus (\ell \cup \ell')$ that is on at most one line ℓ'' which intersects both $\ell \setminus \{e\}$ and $\ell' \setminus \{e\}$, then we may choose $\{e, f, p, q, p', q'\}$ spanning a Q_6-minor as before. If that is the case, then each point f is determined by two such lines, and hence there are no more than 9 points in $E(M') \setminus (\ell \cup \ell')$. Then $|M'| \leq 16$, and M' has no more than $\binom{16}{2}/3 = 40$ long lines, so that $\kappa(M) \leq 1 + n/2 + 40$.

So $|\ell'| = 3$, and indeed every long line of M' that intersects another has length 3. Moreover, each $f \in E(M') \setminus (\ell \cup \ell')$ is on some line ℓ'' which intersects both $\ell \setminus \{e\}$ and $\ell' \setminus \{e\}$, and each such line has length 3. There are no more than 4 such lines ℓ'', so that there are at most 4 points $f \in E(M') \setminus (\ell \cup \ell')$. Then the number of points in M' is at most 9, and the number of long lines is at most $\binom{9}{2}/3 = 12$. Then $\kappa(M) \leq 1 + n/2 + 12$. □

Next, we consider matroids without R_6-minor.

Lemma 4.7.7. *Let $M \in \mathbb{M}(n, 3)$. If M does not have an R_6-minor, then $\kappa(M) \leq 2n$.*

Proof. Let $M' := \mathrm{si}(M)$. As M' has no R_6-minor, any two long lines of M' must have a common point. If M' has a line ℓ with exactly three points, then each long line of M' other than ℓ is determined by one point of ℓ and one point in $E(M')\backslash\ell$, and contains at least one further point of $E(M')\backslash\ell$. In that case, M' has at most $1+3(|M'|-3)/2 \leq (3/2)n-(7/2)$ long lines, so that $\kappa(M) \leq 1+n/2+(3/2)n-(7/2) \leq 2n$ by Lemma 4.7.4. If on the other hand M' does not have any line ℓ with exactly three points, then each long line will have at least 4 points and any two long lines will contain R_6 as a restriction. So then there is at most one long line in M', and $\kappa(M) \leq 1 + n/2 + 1 \leq 2n$ by Lemma 4.7.4 (and using that $n \geq r(M) = 3$). □

Finally, we bound the cover complexity of matroids without P_6-minor.

Lemma 4.7.8. *Let $M \in \mathbb{M}(n, 3)$. If M does not have a P_6-minor, then $\kappa(M) \leq 3 + 19n$.*

Proof. If $M' := \mathrm{si}(M)$ does not have an R_6-minor, then neither does M, and then $\kappa(M) \leq 2n$ by the previous lemma. If M' does have an R_6-minor, fix one such minor with the two lines $\{e_1, e_2, e_3\}$ and $\{f_1, f_2, f_3\}$. There are 9 lines spanned by pairs $\{e_i, f_j\}$, and hence the set U of intersection points between pairs of these lines contains at most $\binom{9}{2} = 36$ points of M'. Let $\ell := \mathrm{cl}_{M'}\{e_1, e_2, e_3\}, \ell' := \mathrm{cl}_{M'}\{f_1, f_2, f_3\}$ be the two long lines of M' spanned by the lines of the R_6-minor. If M' contains any element g not in $\ell \cup \ell' \cup U$, then $\{e_1, e_2, e_3, f_1, f_2, f_3, g\}$ contains a P_6-minor. So each long line of M' other than ℓ, ℓ' intersects U. It follows that M' has at most $2 + (36(n/2))$ long lines, and hence $\kappa(M) \leq 1 + n/2 + (2 + 18n) \leq 3 + 19n$ by Lemma 4.7.4. □

4.8 Barriers

Cover complexity and entropy

Comparing Blow-Up Lemmas The Blow-Up Lemma for cover complexity, Lemma 4.6.2, bears a striking similarity to the Entropy Blow-Up Lemma 3.1.1, both in form and purpose. The entropy bound may sometimes succeed to prove that a class is small, where the cover complexity does not. This is the case for contraction-closed classes in which the number of matroids of fixed rank is small, while the maximum cover complexity among such matroids is large.

Proving Theorem 4.6.3 using entropy Entropy provides an alternative route to bounding the size of a class based on a bound on the cover complexity of matroids of fixed rank in the class. However, the bound is not as strong as one might hope. If $\kappa(M) \leq K(n,s)\binom{n}{s}$ for all $M \in \mathcal{M} \cap \mathbb{M}(n,s)$ for some fixed rank s, then an application of Lemma 4.2.3 results in

$$\log m_{\mathcal{M}}(n,s) \leq K(n,s)\binom{n}{s} \log\left(\frac{2^n(n+1)}{K(n,s)\binom{n}{s}}\right).$$

As $\binom{n}{s}$ is too small to compensate for the factor 2^n, the logarithm gives rise to an additional factor n in the upper bound. The additional factor persists when the Entropy Blow-Up Lemma is used to obtain a bound on $\log m_{\mathcal{M}}(n,r)$ for general rank r.

Small classes with large cover complexity

In the previous section, we showed that some classes of matroids admit a small uniform bound on the cover complexity of its members in terms of their size. We are not always so lucky: in this section, we provide two examples of classes of matroids that have cover complexity that is exponential in the number of elements: graphic matroids and spikes.

Graphic matroids Consider $M(K_{r+1})$, the graphic matroid associated with the complete graph K_{r+1}. We show that the cover complexity of $M(K_{r+1})$ is exponential in r.

Lemma 4.8.1. *Let $r > 3$, and let $M = M(K_{r+1})$. The collection of hyperplanes and their ranks form a flat cover of M, and $\kappa(M) = |\mathcal{H}(M)| = 2^r - 1$.*

Proof. It follows from Lemma 4.2.4(i) that the hyperplanes and their ranks form a flat cover, and hence $\kappa(M) \leq |\mathcal{H}(M)|$. Hyperplanes in

$M(K_{r+1})$ correspond to edge cuts in K_{r+1}, of which there are $\frac{2^{r+1}-2}{2} = 2^r - 1$.

To show that $\kappa(M) \geq 2^r - 1$ as well, we construct a collection of $2^r - 1$ nonbases, each of which is covered by a single flat, and apply Lemma 4.6.5. For each bipartition $\{U, W\}$ of $V(K_{r+1})$, let $X_{\{U,W\}}$ be a nonbasis constructed as follows. Assume, without loss of generality, that $|U| \geq |W|$. Then $|U| \geq 3$, and we can pick a circuit C_U spanning U as well as a tree T_W spanning W. Put $X_{\{U,W\}} = C_U \cup T_W$.

The collection of $X_{\{U,W\}}$ is a collection of nonbases of the required size, and it remains to show that each of them is covered by at most one flat. Note that if F is a flat that covers $X_{\{U,W\}}$, then F must contain C_U, and be disjoint from $\nabla(U, V(K_{r+1}) \setminus U)$. Suppose that some flat F covers both $X_{\{U_1,W_1\}}$ and $X_{\{U_2,W_2\}}$. As each U_i contains at least half of the vertices in $V(K_{r+1})$, it follows that $|U_1| + |U_2| \geq |V(K_{r+1})|$. Since $U_1 \neq W_2$, it follows that $U_1 \cap U_2 \neq \emptyset$. Since F is disjoint from $\nabla(U_1, V(K_{r+1}) \setminus U_1)$, and $C_{U_2} \subseteq F$, it follows that $U_2 \subseteq U_1$. By symmetry, $U_1 \subseteq U_2$, and hence $U_1 = U_2$. So, F cannot cover two distinct $X_{\{U,W\}}$, which is what had to be shown. □

Spikes Let $S = (G, \mathcal{D})$ be a set system on a ground set of cardinality $n := |G|$, and assume that S has the property that no two elements in $\mathcal{D}$ differ in exactly one element. Let $\{a_i : i \in G\}$ and $\{b_j : j \in G\}$ be two disjoint sets. There is a unique matroid $\Lambda(S)$ on ground set $\{a_i : i \in G\} \cup \{b_j : j \in G\}$ such that

(i) for distinct $i, j \in G$, the set $\{a_i, b_i, a_j, b_j\}$ is both a circuit and a cocircuit; and

(ii) for each $X \subseteq G$, the set $\{a_i : i \in X\} \cup \{b_j : j \in G \setminus X\}$ is dependent if and only if $X \in \mathcal{D}$.

Any matroid that is isomorphic to a matroid constructed in this way is called a (tipless) *spike*; it is a rank-n matroid on $2n$ elements. The sets $\{a_i, b_i\}$ are called the *legs* of the spike, and $\{a_i : i \in D\} \cup \{b_i : j \in G \setminus D\}$, with $D \in \mathcal{D}$, is a *dependent transversal* of the legs. Our definition of a spike is taken from [Gee08].

There are many spikes, so in view of Lemma 4.2.3, there must be spikes with large cover complexity. We exhibit such a spike.

Lemma 4.8.2. *Let $S = (G, \mathcal{D})$ be the set system with $G = [n]$ and $\mathcal{D} = \binom{[n]}{\lfloor n/2 \rfloor}$. Then $\kappa(\Lambda(S)) \geq \binom{n}{n/2}$.*

Proof. As each dependent transversal is a circuit-hyperplane in $\Lambda(S)$, the number of circuit-hyperplanes in $\Lambda(S)$ is at least $\binom{n}{n/2}$. The claim now follows from Corollary 4.3.6. □

Excluding $M(K_4)$ and W^3

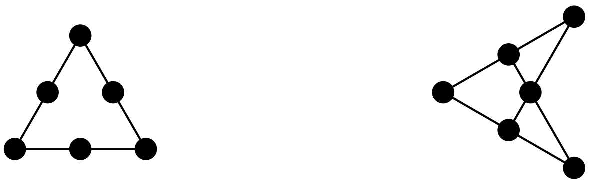
Using cover complexity, we have been able to show that almost every matroid contains an N-minor, whenever N is one of $U(3,6)$, P_6, Q_6 or R_6; all of these cases were shown using an application of Corollary 4.6.4 with $s = 3$. The list above covers all sparse paving matroids of rank 3 on six elements, except the whirl W^3 and the wheel $M(K_4)$ (see Figure 4.2). It turns out that these matroids are closely related to several hard problems in discrete mathematics.

Excluding $M(K_4)$ In the theory of Steiner triple systems, $M(K_4)$ is referred to as the *Pasch configuration* or *quadrilateral*. The following result shows that $\mathrm{Ex}(M(K_4))$ cannot be shown to be small using Theorem 4.6.3 with $s = 3$.

Proposition 4.8.3 ([GrGrWh00]). *For each $n \geq 15$ such that $n = 1 \mod 6$ or $n = 3 \mod 6$, there exists a Steiner triple system that does not contain a Pasch-configuration.*

Later in this section, we construct a large family of sparse paving matroids without $M(K_4)$-minor. The construction suggests that showing that $\mathrm{Ex}(M(K_4))$ is a small class requires a much more subtle argument than the arguments relying on entropy or cover complexity techniques.

Excluding W^3 A *cap-set* is a subset S of the affine geometry $\mathrm{AG}(3,n)$ that does not contain a long line. Let $C(n)$ be the cardinality of a maximum cap-set in $\mathrm{AG}(3,n)$. Clearly $C(n) \leq 3^n$. Recently, Ellenberg and Gijswijt [EG17] proved that $C(n) \leq 2.76^n$. In the other direction,



(a) W^3.

(b) $M(K_4)$.

Figure 4.2: Two sparse paving matroids on six elements.

since $\{0,1\}^n$ is a cap-set, we have $C(n) \geq 2^n$. A better lower bound was obtained by Edel [Ede04], who showed that $C(n) \geq 2.21^n$.

The following construction, due to Blokhuis (private communication), shows that large cap-sets give rise to large rank-3 sparse paving matroids without W^3-minor. Combined with Edel's lower bound on $C(n)$, it proves the existence of rank-3 sparse paving matroids without W^3-minor that have cover complexity at least n^γ, where $\gamma \approx 1.72$.

Lemma 4.8.4 (Blokhuis). *There exists a sparse paving matroid $M \in \operatorname{Ex}\bigl(W^3\bigr)$ of rank 3 on 3^{n+1} elements that contains $C(n)3^{n+1}$ long lines.*

Proof. Let $S \subseteq \mathrm{AG}(3,n)$ be a cap-set of cardinality $C(n)$. By the natural inclusion $\mathrm{AG}(3,n) \subseteq \mathrm{PG}(3,n)$, the set S may be viewed as a subset of $\mathrm{PG}(3,n)$ such that no line of $\mathrm{PG}(3,n)$ contains more than two elements from S.

In turn, the projective geometry $\mathrm{PG}(3,n+1)$ can be written as the disjoint union of $AG(3,n+1)$ and $PG(3,n)$. For a line ℓ of $AG(3,n+1)$, write $\dot{\ell}$ for the unique element in $PG(3,m)$ so that $\ell \cup \{\dot{\ell}\}$ is a line of $PG(3,m+1)$. Let U be the set of all lines ℓ in $AG(3,m+1)$ having $\dot{\ell} \in S$, and note that $|U| = |S|3^n = C(n)3^n$. The set U does not contain three lines ℓ_1, ℓ_2, ℓ_3 that form a W^3, for if this were the case, then $\dot{\ell}_1, \dot{\ell}_2, \dot{\ell}_3$ would lie on the same line in $PG(3,n)$.

Let M be the matroid on ground set $E = AG(3,n+1)$ and set of bases $\binom{E}{3} \setminus U$. Note that $|E| = 3^{m+1}$, and that M has rank 3 by construction. As distinct pairs of elements in U intersect in at most one point, M is sparse paving. Note that U is exactly the set of long lines in M. As no three of these long lines form a W^3, M does not have W^3 as a restriction, and hence as a minor. □

Excluding $M(K_4)$ and W^3 One might hope that excluding both $M(K_4)$ and W^3 as a minor would give more traction on the problem, but the following discussion suggests that it is in fact of little help.

The circuit-hyperplanes of a sparse paving matroid of rank 3 in $\operatorname{Ex}\bigl(M(K_4), W^3\bigr)$ form a hypergraph with the property that any set of three edges spans at least seven vertices, or alternatively, that any set of at most six vertices spans at most two edges. Write $g(n)$ for the maximum number of edges in a 3-uniform hypergraph on n vertices such that any six vertices span at most two edges. We also construct a graph G from the circuit-hyperplanes, by adding a triangle to the graph for each circuit-hyperplane. As circuit-hyperplanes intersect in at most one element, the resulting triangles are edge-disjoint, or equivalently the resulting graph is diamond-free (i.e. it has no subgraph isomorphic to $K_4\backslash e$), or equivalently all its triangles are edge-disjoint. Write $f(n)$ for the maximum number of edges in a diamond-free graph. We have the following relation:

$$\max_{M \in \mathrm{Ex}(M(K_4), W^3) \cap \mathbb{S}(n,3)} \kappa(M) = f(n) \leq g(n).$$

The Rusza-Szemerédi (6,3)-theorem [RS78] uses an early version of the celebrated Szemerédi regularity lemma to prove that $g(n) \leq \frac{n^2}{\mathrm{RS}(n)}$ for some slowly growing function RS. A better upper bound was proved by Fox [Fox11], but the best upper bound remains of the form $O\left(\frac{n^2}{\ln^* n}\right)$.[1]

Three distinct elements $a_1 < a_2 < a_3$ in $[n]$ are called a *3-term arithmetic progression* if $a_3 - a_2 = a_2 - a_1$. Write $r_3(n)$ for the cardinality of the largest subset of $[n]$ that does not contain such an arithmetic progression. Behrend constructed a large such set.

Proposition 4.8.5 ([Beh46]). *There is a constant $c > 0$ such that $r_3(n) \geq n\mathrm{e}^{-c\sqrt{\log n}}$.*

The function $f(n)$ is related to $r_3(n)$; in fact, we have $f(n) = \Omega(nr_3(n))$, see [RS78]. Thus, combining Behrend's construction, Proposition 4.8.5, with the upper bound on $g(n)$, we have

$$\frac{n^2}{\mathrm{e}^{c\sqrt{\log n}}} \leq \max_{M \in \mathrm{Ex}(M(K_4), W^3)} \kappa(M) \leq O\left(\frac{n^2}{\log^* n}\right).$$

The upper bound is too weak to apply Theorem 4.6.3 with $s = 3$ to prove that $\mathrm{Ex}\big(M(K_4), W^3\big)$ is a small class; on the other hand, the lower bound is too small to preclude the possibility that the upper bound may be improved so much that an application of Theorem 4.6.3 becomes possible. It is likely that a successful application of Theorem 4.6.3 with $s = 3$ to prove that $\mathrm{Ex}\big(M(K_4), W^3\big)$ is small results in an improved upper bound on the functions $f(n)$ and $g(n)$.

Two classes with large cover complexity

In the final section of this chapter, we exhibit two classes of matroids that contain matroids of large cover complexity.

[1] Here, $\ln^*$ denotes the iterated logarithm, which is defined recursively as

$$\ln^*(n) := \begin{cases} 0 & \text{if } n \leq 1 \\ 1 + \ln^*(\ln(n)) & \text{otherwise.} \end{cases}$$

Theorem 4.8.6. *If n is an odd integer, then $\mathrm{Ex}(M(K_4)) \cap \mathbb{M}(n)$ contains a matroid with cover complexity at least $\frac{1}{n}\binom{n}{n/2}$. Moreover,*

$$\limsup_{n\to\infty} \frac{\log m_{\mathrm{Ex}(M(K_4))}(n)}{\frac{1}{n}\binom{n}{n/2}} \geq 1$$

Theorem 4.8.7. *If n is an odd integer, then $\mathrm{Ex}(V_8) \cap \mathbb{M}(n)$ contains a matroid with cover complexity at least $\frac{1}{n}\binom{n}{n/2}$.*

Recall that the Graham-Sloane bound on the number of matroids is obtained by identifying the elements of $[n]$ with elements of the additive group $\mathbb{Z}_n$, and then colouring each vertex of $J(n, r)$ by the sum of its elements. Let us write $S(n, r, \gamma)$ for the sparse paving matroid whose circuit-hyperplanes are those vertices that receive colour $\gamma \in \mathbb{Z}_n$.

We will prove Theorem 4.8.6 and Theorem 4.8.7 by showing that a suitably chosen sequence of $S(n, r, \gamma)$ does not have the matroids under consideration as a minor. We set up a framework that is more general then strictly necessary for proving the theorems.

For a matroid N and increasing sequence (n_k), let $\Pi(N, (n_k))$ be the property that for all k, all $0 \leq r \leq n_k$, and all $\gamma \in \mathbb{Z}_{n_k}$, the matroid $S(n_k, r, \gamma)$ does not have an N-minor.

Lemma 4.8.8. *Let N be a matroid, and let (n_k) be an increasing sequence such that $\Pi(N, (n_k))$ holds. For all k, there exists a matroid $M \in \mathrm{Ex}(N) \cap \mathbb{M}(n_k)$ such that $\kappa(M) \geq \frac{1}{n_k}\binom{n_k}{n_k/2}$. Moreover, if $\mathrm{Ex}(N)$ is closed under the relaxation of circuit-hyperplanes, then*

$$\limsup_{n\to\infty} \frac{\log m_{\mathrm{Ex}(N)}(n)}{\frac{1}{n}\binom{n}{n/2}} \geq 1, \tag{4.7}$$

and if, in addition, the sequence (n_k) has bounded differences, then there exists $c > 0$ such that

$$\liminf_{n\to\infty} \frac{\log_{\mathrm{Ex}(N)}(n)}{\frac{1}{n}\binom{n}{n/2}} \geq c. \tag{4.8}$$

Proof. Let $M_k(\gamma) = S(n_k, \lfloor n_k/2 \rfloor, \gamma)$. As in the Graham-Sloane argument, the circuit-hyperplanes of the $M_k(\gamma)$ partition the vertex set of $J(n_k, \lfloor n_k/2 \rfloor)$, so for at least one choice of γ, $M_k(\gamma)$ has at least $\frac{1}{n_k}\binom{n_k}{n_k/2}$ circuit-hyperplanes. Let γ_k be such a value of γ, then by Corollary 4.3.6, $\kappa(M_k(\gamma_k)) \geq \frac{1}{n_k}\binom{n_k}{n_k/2}$. By the assumption that $\Pi(N, (n_k))$ holds, $M_k(\gamma)$ does not have an N-minor, which proves the first claim.

To prove the second claim, assume that Ex(N) is closed under relaxation of circuit-hyperplanes. Then relaxing any subset of circuit-hyperplanes in $M_k(\gamma_k)$ yields a matroid in Ex(N)$\cap\mathbb{M}(n_k, \lfloor n_k/2\rfloor)$, which proves (4.7).

The lower bound (4.8) follows by a similar argument. For a given n, let n_k be the largest member of the sequence (n_k) that is smaller than n. A large family of matroids in Ex(N)$\cap\mathbb{M}(n)$ can be constructed by adding $n - n_k$ loops to relaxations of $M_k(\gamma_k)$. In this way, at least $\frac{1}{n_k}\binom{n_k}{n_k/2}$ are constructed. Equation (4.8) now follows by comparing central binomial coefficients, and using the assumption that $n - n_k$ is bounded. □

The next two lemmas show that $M(K_4)$ and V_8 satisfy the property Π for a suitably chosen sequence (n_k).

Lemma 4.8.9. *If n is an odd integer, $0 \leq r \leq n$, and $\gamma \in \mathbb{Z}_n$, then $S(n, r, \gamma)$ does not have an $M(K_4)$-minor.*

Proof. Clearly $S(n, r, \gamma)$ does not have a V_8-minor if $n < 6$ or $r < 3$, so we may assume that $n \geq 7$ and $r \geq 3$. Suppose, for the sake of contradiction, that $S(n, r, \gamma)$ has an $M(K_4)$-minor, so that $S(n, r, \gamma)/A\backslash B \cong M(K_4)$ for some disjoint sets A and B. Without loss of generality, we may assume that A is independent in $S(n, r, \gamma)$, and hence that $S(n, r, \gamma)$ has circuit-hyperplanes $A \cup \{a, b, c\}$, $A \cup \{a, d, e\}$, $A \cup \{b, e, f\}$, and $A \cup \{c, d, f\}$, with a, b, c, d, e, and f all distinct. Letting $\gamma' = \gamma - \sum_{x \in A} x \mod n$, it follows that

$$a + b + c = a + d + e = b + e + f = c + d + f = \gamma' \mod n,$$

We obtain

$$0 = (a + b + c) + (a + d + e) - (b + e + f) - (c + d + f) = 2(a - f).$$

By assumption, n is odd, and hence 2 has a multiplicative inverse in $\mathbb{Z}_n$. It follows that $a = f$: a contradiction. □

Lemma 4.8.10. *If n is an odd integer, $0 \leq r \leq n$, and $\gamma \in \mathbb{Z}_n$, then $S(n, r, \gamma)$ does not have a V_8-minor.*

Proof. Clearly $S(n, r, \gamma)$ does not have a V_8-minor if $n < 8$ or $r < 4$, so we may assume that $n \geq 9$ and $r \geq 4$. For the sake of contradiction, assume that $S(n, r, \gamma)$ has a V_8-minor, so that $S(n, r, \gamma)/A\backslash B \cong V_8$ for some disjoint sets A and B. Without loss of generality, we may assume that A is independent in $S(n, r, \gamma)$, in which case M has circuit-hyperplanes of the form $A \cup X$, with X any of the following sets:

$$\{a, a', b, b'\}, \quad \{a, a', c, c'\}, \quad \{a, a', d, d'\}, \quad \{b, b', c, c'\}, \quad \{b, b', d, d'\},$$

where all elements a, a', b, b', c, c', d, and d' are distinct and not contained in A. Writing $\gamma' = \gamma - \sum_{x \in A} x \mod n$, we have in particular that

$$a + a' + b + b' = a + a' + c + c' = b + b' + c + c' = \gamma' \mod n,$$

from which it follows that $2(a + a') = 2(b + b') = 2(c + c') = \gamma' \mod n$. Similarly, it follows from

$$a + a' + b + b' = a + a' + d + d' = b + b' + d + d' = \gamma' \mod n$$

that $2(d + d') = \gamma' \mod n$. As 2 has a multiplicative inverse in $\mathbb{Z}_n$, it follows that $c+c'+d+d' = \gamma' \mod n$, and hence that $A \cup \{c+c'+d+d'\}$ is a circuit-hyperplane in $S(n, r, \gamma)$: a contradiction. □

Theorem 4.8.6 follows from Lemma 4.8.9 and Lemma 4.8.8, combined with the observation that $\mathrm{Ex}(M(K_4))$ is closed under the relaxation of circuit-hyperplanes. Similarly, Theorem 4.8.7 follows follows upon combining Lemma 4.8.10 with Lemma 4.8.8.

CHAPTER 5

Enumeration of matroids of fixed rank

This chapter is partly based on the journal paper [PvdP17], which is joint work with Rudi Pendavingh, and on joint work with Remco van der Hofstad and Rudi Pendavingh.

5.1 In this chapter...

This chapter focusses on the enumeration of matroids of fixed rank. The results in this section imply in particular that for each fixed $r \geq 3$,

$$\log s(n,r) \sim \log m(n,r) \sim \frac{\log n}{n}\binom{n}{r} \quad \text{as } n \to \infty(5.1)$$

Although (5.1) succinctly represents the main asymptotic results of this chapter, most of the work in this chapter is in proving detailed non-asymptotic results that have (5.1) as a consequence. The upper bound in (5.1) follows from the following bound on $m(n,r)$.

Theorem 5.1.1. *For all $r \geq 3$ and all $n \geq r + 12$,*

$$\log m(n,r) \leq \frac{1}{n-r+1}\binom{n}{r}\log\left(\mathrm{e}(n-r+1)\right).$$

By summing over r, Theorem 5.1.1 in particular provides an alternative proof of Theorem 3.6.1, which states that $\log m(n) = O\left(\frac{\log n}{n}\binom{n}{n/2}\right)$ as $n \to \infty$.

Our proof of Theorem 5.1.1 relies heavily on the theory of truncations and erections of matroids, which was developed by Crapo [Cra70] and Knuth [Knu75]. The truncation of a matroid is obtained by removing its hyperplanes from the lattice of flats, and erection is essentially the inverse operation. Every matroid can be described as its truncation augmented by some extra information to describe its hyperplanes. We show that the information required to reconstruct the hyperplanes encodes a paving matroid. Inductively, this allows us to describe every matroid as a finite sequence of paving matroids of increasing rank. Careful analysis of this sequence results in a proof of Theorem 5.1.1.

After proving Theorem 5.1.1, we focus on sparse paving matroids. Keevash [Kee15] recently obtained good estimates of the number of designs. As sparse paving matroids of fixed rank are closely related to designs, his results strongly suggest that similar results should hold for sparse paving matroids. Here, we adapt his techniques to sparse paving matroids to obtain the following result.

Theorem 5.1.2. *For all fixed $r \geq 3$,*

$$\log s(n,r) = \frac{1}{n-r+1}\binom{n}{r}\log\left(\mathrm{e}^{1-r}n + o(n)\right) \qquad \text{as } n \to \infty.$$

Theorem 5.1.1 and Theorem 5.1.2 suffice to prove (5.1). The gap between the upper bound of Theorem 5.1.1 and the lower bound of Theorem 5.1.2 is dominated by the different coefficients of n inside the logarithm. In the final section of this chapter, an attempt is made towards shrinking this gap, by improving the upper bound on $p(n,3)$, the number of paving matroids of rank 3.

Theorem 5.1.3.

$$\log p(n,3) \leq \frac{1}{n-2}\binom{n}{3}\log\left(\mathrm{e}^{0.35}n + o(n)\right).$$

Matroids of rank 0, 1, and 2 are in correspondence with well-known combinatorial objects. For the sake of completeness, these results are contained in Section 5.2. In Section 5.3, we review some of the theory of truncations and erections that we will need in later chapters. Here, essential flats are defined as well. In Section 5.4, the essential flats are compared to the flat covers of the previous chapter. In Section 5.5, we consider paving matroids. Paving matroids are easier to analyse than general matroids, and the results in this section serve as a motivating example for the more general results in Section 5.6. In Section 5.7, we use the structural description of matroids obtained in the previous chapters to obtain an upper bound on $m(n,r)$. Sections 5.8–5.9 focus on (sparse) paving matroids. The extra structure in these classes allows us to prove the bounds of Theorem 5.1.2 on sparse paving matroids in Section 5.8, and the improved upper bound for rank-3 paving matroids of Theorem 5.1.3 in Section 5.9.

5.2 Matroids of rank at most 2

We start by considering matroids of rank at most 2. Such matroids correspond to well-known objects in discrete mathematics, more precisely set partitions with various additional properties. In this section, all matroids have ground set $[n]$.

There is only one matroid of rank 0: the uniform matroid $U(0, n)$. This matroid is sparse paving, and hence $s(n, 0) = p(n, 0) = m(n, 0) = 1$. Each rank-1 matroid is determined by its rank-0 flat, which is a proper subset of $[n]$. Each of these matroids is paving, so $p(n, 0) = m(n, 0) = 2^n - 1$. Such a matroid is sparse paving if it has at most one loop, so $s(n, 1) = n + 1$ (provided $n \geq 2$).

The situation is more interesting for matroids of rank 2. Each rank-2 matroid on ground set $[n]$ is determined by its rank-1 flats: the loops of such a matroid are those elements that appear in every rank-1 flat. Thus, each matroid gives rise to a partition of $[n]$ with at least three blocks, one of which (corresponding with the set of loops) is distinguished from the others, and allowed to be non-empty. Such partitions can be encoded as a partition of $[n + 1]$, where the block containing $n+1$ corresponds with the set of loops. Thus, $m(n, 2) = B(n+1) - 2^n$, where $B(n)$ is the n-th Bell number. An asymptotic formula for Bell numbers is obtained by Moser and Wyman [MW55], from whose work it follows that $\log B(n) \sim n \log n$.

A rank-2 matroid is paving if and only if it does not contain any loops, so such matroids are partitions of $[n]$ into at least two sets, so $p(n, 2) = B(n) - 1$. A rank-2 matroid is sparse paving if, in addition to having no loops, all blocks contain at most two elements. Such matroids are in correspondence with involutions, which are counted by the telephone (or triangular) numbers $T(n)$. Thus, $s(n, 2) = T(n)$. Asymptotics for telephone numbers can be found in [Knu98, p. 64], from which we obtain the estimate $\log T(n) \sim \frac{1}{2} n \log n$.

Theorem 5.2.1. *As $n \to \infty$,*

$$2 \log s(n, 2) \sim \log p(n, 2) \sim \log m(n, 2) \sim n \log n.$$

In addition, as the classes of matroids and sparse paving matroids are closed under duality, $\log s(n, n-2) = \log s(n, 2)$ and $\log m(n, n-2) = \log m(n, 2)$.

The formulas obtained above can also be used to the asymptotic fraction of (sparse) paving matroids among matroids of rank 2.

Theorem 5.2.2. $\lim\limits_{n\to\infty} \frac{s(n,2)}{p(n,2)} = \lim\limits_{n\to\infty} \frac{p(n,2)}{m(n,2)} = 0.$

5.3 Truncation and erection

In the remainder of this chapter, we consider matroids of fixed rank $r \geq 3$. Our analysis of such matroids relies heavily on the operations of truncation and erection of matroids. These operations were studied extensively by Crapo [Cra70] and Knuth [Knu75], in particular in relation to the reconstruction of erections using extra information.

In this section, we define truncation and erection. We describe some of the results of Crapo and Knuth, and reprove these results in a common framework, that of complete sets.

Truncation and erection

Let M be a matroid of rank r, and let $\mathcal{F}(M)$ be its lattice of flats. For $k \leq r$, the *rank-k truncation* of M is obtained by removing from $\mathcal{F}(M)$ the flats of rank $k, k+1, \ldots, r-1$, while preserving the partial order. The resulting partial order is again the lattice of flats of a matroid, which we denote by $M^{(k)}$. There are several alternative definitions of $M^{(k)}$; for example, its independent sets are given by

$$\mathcal{I}\left(M^{(k)}\right) = \left\{I \in \mathcal{I}(M) : |I| \leq k\right\}. \tag{5.2}$$

We are particularly interested in the rank-$(r-1)$ truncation of M, and write $T(M) := M^{(r-1)}$. If no particular truncation is specified, the truncation of M refers to $T(M)$.

Following Crapo [Cra70], we call N an *erection* of M if $M = T(N)$, or $N = M$. In the latter case, we say that N is the *trivial erection* of M. If N is an erection of M, then $\mathrm{rk}(N) = \mathrm{rk}(M) + 1$, unless N is the trivial erection. While the truncation of a matroid is unique, it may have many erections. For example, the truncation of a paving matroid is always a uniform matroid. This follows, for example, from (5.2). Matroid erections were first studied by Crapo [Cra70], who recognised the lattice structure of erections under the *weak order* (if M and N are matroids on the same ground set, then M is said to be at most N in the weak order if every independent set in N is also independent in M).

Remark 5.3.1. Duke [Duk87] showed that the lattice of erections is isomorphic to the interval $[\mathscr{M}_0, \mathscr{M}_c]$ in the lattice of modular cuts of M^*, ordered by the superset-relation. Here, $\mathscr{M}_0$ is the set of all flats of M^*, and $\mathscr{M}_c$ is the modular cut generated by the cyclic flats of M^*. If M and L are matroids on the same ground set, then L is called a *lift* of M if there is a matroid M' such that $M = M'/e$ and $L = M'\backslash e$. As $(M'/e)^* = (M')^*\backslash e$, the lifts of M are in one-to-one correspondence with single-element extensions of M^*. Erections are special lifts, and Duke's result asserts that those lifts that are erections correspond precisely with modular cuts in $[\mathscr{M}_0, \mathscr{M}_c]$. □

Crapo's characterisation of erections

A set $X \subseteq E$ is *k-closed* in M if $\mathrm{cl}_M(Y) \subseteq X$ for all $Y \subseteq X$ such that $|Y| \leq k$. Alternatively, X is k-closed if and only if $X \cap F$ is closed for all rank-k flats F in M [Cra70, Theorem 1].

The *k-closure* of a set X is

$$\mathrm{cl}_k(X) := \bigcap \{Y \subseteq E : Y \text{ is } k\text{-closed}, Y \supseteq X\}.$$

The intersection of k-closed sets is again k-closed, so $\mathrm{cl}_k(X)$ is in fact the smallest k-closed set containing X.

Crapo obtained the following characterisation of erections in terms of their rank-r flats. Note that if M is a matroid of rank r, then the rank-r flats of its erection are hyperplanes, unless the erection is trivial.

Theorem 5.3.2 ([Cra70, Theorem 2])**.** *Let M be a matroid on E of rank r, and let $\mathcal{H} \subseteq \mathscr{P}(E)$. $\mathcal{H}$ is the set of rank-r flats of an erection of M if and only if*

(i) each $H \in \mathcal{H}$ has rank r in M;

(ii) each $H \in \mathcal{H}$ is $(r-1)$-closed; and

(iii) each basis of M is contained in a unique element of $\mathcal{H}$.

Knuth's construction of erections

Independently of Crapo, Knuth [Knu75] describes a procedure which, given a matroid M on E of rank r and a collection $\mathcal{U}$ of subsets of E, generates the largest possible set $\mathcal{H}$ of the rank-r flats of an erection of M with the additional property that each $U \in \mathcal{U}$ is contained in some element of $\mathcal{H}$.

```
Input:   Matroid $M$ of rank $r$
         Collection of sets $\mathcal{U}$
Output:  $\mathcal{H}$

$\mathcal{H} \leftarrow \mathcal{U} \cup \{F + e : F$ a hyperplane of $M, e \notin F\}$      (Initialise)
while $\exists H, H' \in \mathcal{H}$ such that $H \neq H'$, $r_M(H \cap H') = r$ do
    $\mathcal{H} \leftarrow (\mathcal{H} \setminus \{H, H'\}) \cup \{H \cup H'\}$      (Update)
```

Figure 5.1: Knuth's procedure

Knuth's procedure is described in Figure 5.1. As $\mathcal{H}$ decreases by 1 in each iteration of *Update*, the procedure terminates after a finite number of steps on any input $\mathcal{U} \subseteq \mathscr{P}(E)$. It is not obvious that the output of the procedure is independent of the choice of H and H' in each application of *Update*, but Knuth shows that this is the case.

Theorem 5.3.3 ([Knu75, Section 5–6])**.** *The output $\mathcal{H}$ of the procedure depends only on the input M and $\mathcal{U}$. Moreover, for any matroid M of rank r on E, and any set $\mathcal{H} \subseteq \mathscr{P}(E)$, the following are equivalent:*

(i) $\mathcal{H}$ is the output of the procedure on some input $\mathcal{U} \subseteq \mathscr{P}(E)$; and

(ii) $\mathcal{H}$ is the set of rank-r flats of an erection of M.

The second part of Theorem 5.3.3 shows that Knuth's procedure can be used to construct all possible erections. In the remainder of this chapter, we write $\mathcal{H}(M,\mathcal{U})$ for the output of Knuth's procedure on input $\mathcal{U}$, and $M{\uparrow}\mathcal{U}$ for the erection of M of which $\mathcal{H}(M,\mathcal{U})$ is the collection of rank-r flats.

Complete sets

Let M be a matroid on E of rank r. A collection $\mathcal{X} \subseteq \mathscr{P}(E)$ is called *complete* (with respect to M) if the following properties hold:

(i) if $X \in \mathcal{X}$, and $Y \subseteq X$ then $Y \in \mathcal{X}$;

(ii) each basis of M is in $\mathcal{X}$;

(iii) $\mathrm{cl}_{r-1}(X) \in \mathcal{X}$ whenever $X \subseteq \mathcal{X}$; and

(iv) $X \cup Y \in \mathcal{X}$ for all $X, Y \in \mathcal{X}$ such that $\mathrm{rk}_M(X \cap Y) = r$.

Complete sets are in one-to-one correspondence with erections of M; the following lemma describes this correspondence.

Lemma 5.3.4. *Let $\mathscr{X} \subseteq \mathscr{P}(E)$. Then $\mathscr{X}$ is complete with respect to M if and only if $\mathscr{X} = \{X \subseteq E : \mathrm{rk}_N(X) \leq r\}$ for some erection N of M.*

Proof. It is straightforward to prove sufficiency, so here we only prove necessity. Assume that $\mathscr{X}$ is complete with respect to M, and let $\mathrm{rk}'\colon \mathscr{P}(E) \to \mathbb{Z}_{\geq 0}$ be defined by

$$\mathrm{rk}'(X) := \begin{cases} \mathrm{rk}_M(X) & \text{if } X \in \mathscr{X} \\ r+1 & \text{otherwise,} \end{cases}$$

so that $\mathscr{X} = \{X \subseteq E : \mathrm{rk}'(X) \leq r\}$. If rk' is the rank function of a matroid N, then N is an erection of M. So, in order to prove the lemma, it suffices to verify that rk' satisfies the rank axioms.

Clearly, $\mathrm{rk}'(X) \geq 0$ for all $X \in E$. That $\mathrm{rk}'(Y) \leq \mathrm{rk}'(X)$ for all $Y \subseteq X$ follows from the fact that $\mathscr{X}$ is closed under taking subsets. It remains to show that rk' is submodular, i.e.

$$\mathrm{rk}'(X) + \mathrm{rk}'(Y) \geq \mathrm{rk}'(X \cup Y) + \mathrm{rk}'(X \cap Y). \tag{5.3}$$

Suppose that rk' is not submodular. Pick $X, Y \subseteq E$ violating (5.3) with $|X| + |Y|$ as large as possible. If $X \notin \mathscr{X}$, then $X \cup Y \notin \mathscr{X}$ so that

$$\begin{aligned}\mathrm{rk}'(X) + \mathrm{rk}'(Y) = (r+1) + \mathrm{rk}'(Y) &\geq (r+1) + \mathrm{rk}'(X \cap Y) \\ &\geq \mathrm{rk}'(X \cup Y) + \mathrm{rk}'(X \cap Y),\end{aligned}$$

so $\{X, Y\}$ does not violate (5.3). It follows that $X \in \mathscr{X}$, and by a similar argument $Y \in \mathscr{X}$. As $\mathscr{X}$ is closed under taking subsets, we have $X \cap Y \in \mathscr{X}$ as well, and

$$\begin{aligned}\mathrm{rk}'(X \cup Y) &> \mathrm{rk}'(X) + \mathrm{rk}'(Y) - \mathrm{rk}'(X \cap Y) \\ &= \mathrm{rk}_M(X) + \mathrm{rk}_M(Y) - \mathrm{rk}_M(X \cap Y) \geq \mathrm{rk}_M(X \cup Y).\end{aligned}$$

Hence $X \cup Y \notin \mathscr{X}$, and therefore $\mathrm{rk}'(X \cup Y) = r + 1 = \mathrm{rk}_M(X \cup Y) + 1$. If $\mathrm{rk}_M(X \cap Y) = r$, then $X \cup Y \in \mathscr{X}$ as $\mathscr{X}$ is complete, a contradiction. It follows that $\mathrm{rk}_M(X \cap Y) < r$. Hence

$$\mathrm{rk}_M(X) + \mathrm{rk}_M(Y) = \mathrm{rk}_M(X \cap Y) + \mathrm{rk}_M(X \cup Y) \leq (r-1) + r,$$

so that $\mathrm{rk}_M(X) < r$ or $\mathrm{rk}_M(Y) < r$. Without loss of generality $r_M(X) < r$. Let I be a basis of X, so that $\mathrm{cl}(I) = \mathrm{cl}_{r-1}(I) \supseteq X$. As $\mathrm{rk}_M(X \cup Y) = r > \mathrm{rk}_M(X)$, we can extend I by elements of Y to a basis B of M. Let $X' := \mathrm{cl}_{r-1}(B)$. As $B \in \mathscr{X}$, we have $X' \in \mathscr{X}$ as well. As I is strictly contained in B, X is strictly contained in X'; in particular, $|X'| > |X|$. The pair X', Y violates (5.3), thus contradicting maximality of $|X| + |Y|$. □

Item (i) in the definition of complete sets states that complete sets are downward-closed. If $\mathcal{H}$ is the set of inclusionwise-maximal elements of $\mathcal{X}$, then $\mathcal{X}$ can be obtained from $\mathcal{H}$ by

$$\mathcal{H}^{\downarrow} := \{X : X \subseteq H \text{ for some } H \in \mathcal{H}\}.$$

The inclusionwise-maximal elements of $\mathcal{X}$ form an antichain in $\mathscr{P}(E)$, and every antichain arises in this way from a downward-closed set, thus showing that downward-closed sets are in one-to-one correspondence with antichains.

The proof of the following lemma is straightforward.

Lemma 5.3.5. *Let $\mathcal{X} \subseteq \mathscr{P}(E)$ be a downward-closed collection, and let $\mathcal{H}$ be the set of the inclusionwise-maximal elements of $\mathcal{X}$. $\mathcal{X}$ is complete if and only if $\mathcal{H}$ satisfies conditions (i)–(iii) of Theorem 5.3.2.*

Lemma 5.3.5 suffices to prove Crapo's characterisation.

Proof of Theorem 5.3.2. By Lemma 5.3.4, erections are in one-to-one correspondence with complete sets, which in turn, by Lemma 5.3.5, are in one-to-one correspondence with collections satisfying the conditions in Theorem 5.3.2. □

The intersection of complete sets is again complete. It follows that the *completion*,

$$\operatorname{comp}(\mathcal{Z}) := \bigcap \{\mathcal{X} : \mathcal{X} \text{ is complete with respect to } M,\ \mathcal{Z} \subseteq \mathcal{X}\}, \tag{5.4}$$

is the smallest complete set containing $\mathcal{Z}$. Note that $\operatorname{comp}(\mathcal{Z})$ depends on the matroid M; if we want to emphasise this dependence, we shall write comp_M. The properties of complete sets immediately imply the following properties of completions.

Lemma 5.3.6. *Let M be a matroid on E, and let $\mathcal{U} \subseteq \mathscr{P}(E)$. Then*

(i) $\operatorname{comp}(\mathcal{U}) = \operatorname{comp}(\mathcal{U} \cup \mathcal{B}(M))$;

(ii) $\operatorname{comp}(\mathcal{U}) = \operatorname{comp}(\{\operatorname{cl}_{r-1}(U) : U \in \mathcal{U}\})$;

(iii) $\operatorname{comp}(\mathcal{U}) = \operatorname{comp}(\mathcal{U} \cup \{F + e : F \in \mathcal{H}(M), e \notin F\})$.

The following lemma shows that Knuth's procedure essentially determines completions.

Lemma 5.3.7. *Let M be a matroid on E. If $\mathcal{U} \subseteq \mathscr{P}(E)$, then $\mathcal{H}(M,\mathcal{U})$ is the collection of inclusionwise-maximal elements of* $\operatorname{comp}_M(\mathcal{U})$.

Proof. Suppose that $\mathcal{X}$ is complete, and $\mathcal{U} \subseteq \mathcal{X}$. Then $\mathcal{H}(M,\mathcal{U}) \subseteq \mathcal{X}$, and so $\mathcal{H}(M,\mathcal{U}) \subseteq \mathrm{comp}(\mathcal{U})$. Next, consider $\big(\mathcal{H}(M,\mathcal{U})\big)^{\downarrow}$. This is a complete set, and $\mathcal{U} \subseteq \big(\mathcal{H}(M,\mathcal{U})\big)^{\downarrow}$. Combining these two observations, we obtain

$$\mathcal{H}(M,\mathcal{U}) \subseteq \mathrm{comp}(\mathcal{U}) \subseteq \big(\mathcal{H}(M,\mathcal{U})\big)^{\downarrow}.$$

It follows that $\mathrm{comp}(\mathcal{U}) = \mathcal{H}(M,\mathcal{U})^{\downarrow}$, and as $\mathcal{H}(M,\mathcal{U})$ is the set of inclusionwise-maximal elements of $\mathcal{H}(M,\mathcal{U})^{\downarrow}$, this implies the lemma. □

Knuth's theorem follows from Lemma 5.3.7.

Proof of Theorem 5.3.3. As $\mathrm{comp}(\mathcal{U})$ depends only on M and $\mathcal{U}$, so does $\mathcal{H}(M,\mathcal{U})$. That $\mathcal{H}(M,\mathcal{U})$ is the collection of rank-r flats in an erection of M follows from an application of Lemma 5.3.4; this shows that (i) implies (ii). Note that if N is an erection of M, then $\mathcal{H}(M, \mathcal{H}(N))$ is the set of rank-r flats of N, so (ii) implies (i) as well. □

Remark 5.3.8. Recall the interval $[\mathscr{M}_0, \mathscr{M}_c]$ in the lattice of modular cuts of M^*. The collection of modular cuts of M^*, and hence of the interval $[\mathscr{M}_0, \mathscr{M}_c]$, is closed under taking arbitrary intersections, so every set of flats of M^* generates a minimal modular cut containing the set. The completion operator (5.4) is a specialisation of this closure operator for modular cuts.

Complete sets and modular cuts in $[\mathscr{M}_0, \mathscr{M}_c]$ can be linked directly through the function $\mathscr{M} \mapsto \{A \subseteq E(M) : \mathrm{cl}^*(E \setminus A) \in \mathscr{M}\}$ and its inverse $\mathcal{X} \mapsto \{\mathrm{cl}^*(E \setminus A) : A \in \mathcal{X}\}$; where $\mathrm{cl}^*(X)$ denotes the coclosure of X. □

Reconstructing a matroid from its truncation

The goal of the next section is to obtain a method of describing a matroid M in terms of its truncation $T(M)$ augmented with extra information in an economic way. To make this more precise, we are interested in finding $\mathcal{U}$ such that $M = T(M)\!\uparrow\!\mathcal{U}$, while $\mathcal{U}$ is as 'small' as possible. Recall that $M = T(M) \uparrow \mathcal{H}(M)$ for any matroid M. It turns out that we can be more economical.

Crapo notes that certain flats F in M are 'predictable', in the sense that the restriction $M|F$ has no nontrivial erection. If this happens, then the occurrence of F as a flat in M is unavoidable given the structure of $M|F$. If the hyperplane H is predictable, then its structure $M|H$ follows already from $T(M)$.

Flats that are not predictable are called *essential*. Hence, we may restrict $\mathcal{U} = \mathcal{H}(M)$ to essential hyperplanes. No 'intrinsic' characterisation of the essential flats of a matroid is known[1], but the following lemma, which in particular implies that independent flats are predictable, provides a necessary condition.

Lemma 5.3.9 ([Cra70, Theorem 12])**.** *Let M be a matroid on E, and let F be a rank-k flat in M. If there exists $I \in \mathcal{I}(M)$ such that $F = \mathrm{cl}_{k-1}(I)$, then F is not essential.*

5.4 Describing a matroid by a collection of flats

So far, we have encountered several subcollections of flats that determine a matroid. In Chapter 4, we defined flat covers: collections of flats that suffice to reconstruct a matroid in a particular way. Cover complexity, the size of a smallest such flat cover, provided a useful notion of structural complexity of matroids, and led, among other things, to an upper bound on the number of matroids. Essential flats, introduced at the end of the previous chapter, provide another collection of flats that can be used to unambiguously determine a matroid. Higgs (in [Cra70]) suggested that essential flats provide a very concise description of matroids. The aim of this section is to compare flat covers, essential flats, and other subcollections of flats. It is not crucial to the arguments in this chapter, but it may shed some light on its result.

Recall that a flat is essential if the restriction $M|F$ has at least one nontrivial erection. Let us call a flat F of rank k *pseudo-essential* if there is no independent set I such that $F = \mathrm{cl}_{k-1}(I)$. By Lemma 5.3.9, every essential flat is pseudo-essential. The following lemma shows that every pseudo-essential flat is a circuit-closure.

Lemma 5.4.1. *Let F be a flat of rank k. If there is no independent set I such that $F = \mathrm{cl}_{k-1}(I)$, then $F = \mathrm{cl}(C)$ for some circuit C.*

Proof. Suppose that F is not a circuit-closure. We will show that $F = \mathrm{cl}_{k-1}(I)$ whenever I is a basis of F. So let I be a basis of F. If $x \in F \setminus I$, then $I \cup \{x\}$ contains a circuit C', which necessarily contains x. By assumption, C' is properly contained in $I \cup \{x\}$. It follows that $C' \cap I$ has cardinality at most $k - 1$, and hence that $x \in \mathrm{cl}_{k-1}(I)$. As x was arbitrary, the lemma follows. □

[1] Finding an 'intrinsic' characterisation is posed as an open problem in [Cra70]. To the best of our knowledge, it has not been solved yet.

Greene [Gre91] calls a collection of flats $\mathcal{F}' \subseteq \mathcal{F}(M)$ *descriptively sufficient* if

$$\mathcal{I}(M) = \{X \in \mathscr{P}(E(M)) : |X \cap F| \leq \operatorname{rk}(F) \text{ for all } F \in \mathcal{F}'\}\,. \tag{5.5}$$

He provides several equivalent definitions of descriptive sufficiency, and proves in particular that a collection of flats is descriptively sufficient if and only if it contains all circuit-closures [Gre91, Proposition 3.2]. Equation (5.5) is reminiscent of the defining property of flat covers. In fact, since the circuit-closures of a matroid form a flat cover, it follows that every descriptively sufficient set forms a flat cover as well.

Lemma 5.4.2. *If $\mathcal{F}' \subseteq \mathcal{F}(M)$ is a descriptively sufficient collection of flats, then $\{(F, \operatorname{rk}(F)) : F \in \mathcal{F}'\}$ is a flat cover.*

The reverse implication if false in general; in fact, the cover complexity can be much smaller than the number of circuit-closures. We encountered one example for which this is true in Section 4.8: the graphic matroids $M(K_{r+1})$.

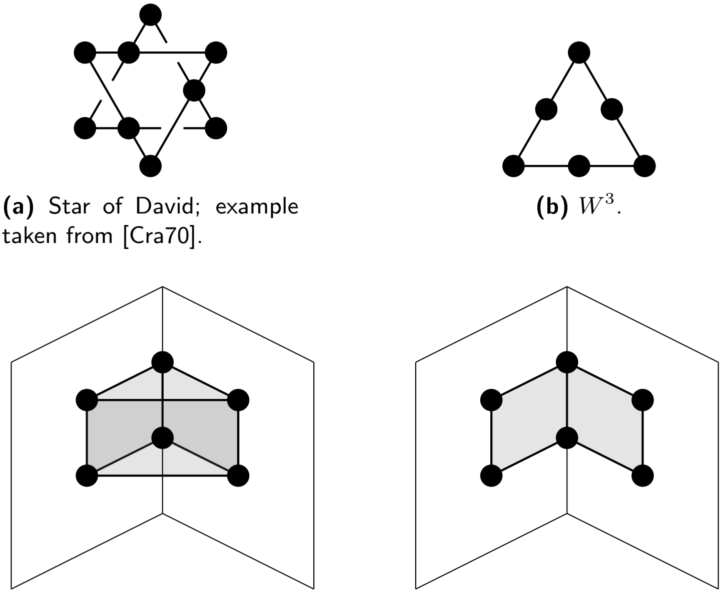
Two well-known examples of descriptively sufficient collections of flats are the *cyclic flats* (flats that are unions of circuits), and *dependent nondecomposable flats* (flats of the form $F' \cup \operatorname{cl}(\emptyset)$ such that $|F'| \geq 2$ and $M|F'$ is connected).

The results in this section can be summarised as the following sequence of inclusions:

$$\begin{array}{l}
\text{essential flats}\\
\quad \subseteq \text{pseudo-essential flats}\\
\left.\begin{array}{l}
\qquad \subseteq \text{circuit-closures}\\
\qquad\quad \subseteq \text{dependent nondecomposable flats}\\
\qquad\qquad \subseteq \text{cyclic flats}
\end{array}\right\}
\begin{array}{l}\text{flat cover;}\\ \text{desc. sufficient}\end{array}
\end{array}$$

Each of these inclusions can be strict. The first inclusion is strict for the 9-point matroid on the hexagram that is displayed in Figure 5.2(a); this example is given by Crapo [Cra70, Theorem 12]. The second inclusion is strict for the whirl W^3 (Figure 5.2(b)). The third inclusion is strict for the rank-4 graphic matroid $M(K_{2,3})$ in Figure 5.2(c), and the fourth inclusion is strict for the matroid depicted in Figure 5.2(d), which is obtained from the previous example by relaxing one of the circuit-hyperplanes.

The collection of essential flats of a matroid can be much smaller than its cover complexity. The rank-4 matroid in Figure 5.3 provides a



(a) Star of David; example taken from [Cra70].

(b) W^3.

(c) $M(K_{2,3})$.

(d) Circuit-hyperplane relaxation of $M(K_{2,3})$.

Figure 5.2: Some examples to show that each of the inclusions can be strict.

counter-example to the tempting conjectures that (i) (pseudo-)essential flats and their ranks necessarily form a flat cover, and (ii) the essential flats are contained in every flat cover. The matroid in the figure has four essential flats: the two long lines, and the two highlighted 4-element hyperplanes. None of these four flats cover the selected nonbasis, thus disproving (i). To disprove (ii), consider the flat cover formed by the hyperplanes, and note that the two long lines are flats of lower rank.

5.5 An upper bound on the number of paving matroids

In this section, we shall obtain an upper bound on the number of paving matroids of rank $r \geq 3$. The reason for considering paving matroids before general matroids is two-fold: not only does the additional structure

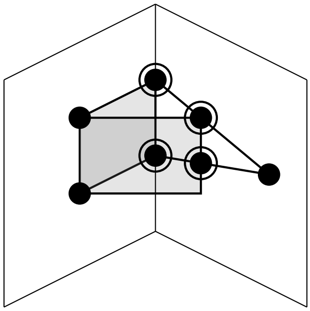


Figure 5.3: The essential flats do not form a flat cover. This example was used in [Cra70] to illustrate the "remarkable economy afforded by essential flats".

of paving matroids result in a more transparent exposition of the technique, it will actually be used as an inductive step in the analysis of general matroids.

The graded lexicographic order

In this section and the next, we will need a particular order on subsets that favours sets of small cardinality. Such an order is provided by the *graded lexicographic order*. Fix the ground set $E = [n]$, and the rank $r \geq 3$. The ground set comes with a natural order, which induces the graded lexicographic order on $\mathscr{P}(E)$. For $X, Y \subseteq E$, we say that X precedes Y in the graded lexicographic order (and write $X \prec Y$) if

- $|X| < |Y|$; or
- $|X| = |Y|$ and $\min(X \triangle Y) \in X$.

Describing a paving matroid by its hyperplanes

Recall that the hyperplanes of a matroid M of rank r on E are its rank-$(r-1)$ flats. We shall write $\mathcal{H}(M)$ for the collection of hyperplanes of M. Any matroid M on E of rank r is determined by $\mathcal{H}(M)$.

If M is a paving matroid, then its hyperplanes have a particularly nice structure: if M has rank at least 2, then its hyperplanes form a set system known as an $(r-1)$-*partition* (see e.g. [Oxl11, Proposition 2.1.24]): this is a collection of at least two subsets $\mathcal{H} \subseteq \mathscr{P}(E)$ such that

- each $H \in \mathcal{H}$ contains at least $r - 1$ elements; and

- each $(r-1)$-set in E is contained in exactly one $H \in \mathcal{H}$.

Note that 1-partitions are precisely ordinary set partitions into at least two parts. For the remainder of this section, we shall assume that $r \geq 3$.

Write $\mathcal{H}^+(M) := \{H \in \mathcal{H}(M) : |H| \geq r\}$ for the dependent hyperplanes of M. If M is a paving matroid, then $\mathcal{H}(M)$ (and hence M) is determined by $\mathcal{H}^+(M)$ as well: since in this case the hyperplanes of M form an $(r-1)$-partition, it is necessarily the case that

$$\mathcal{H}(M) = \mathcal{H}^+(M) \cup \left\{ X \in \binom{E}{r-1} : X \not\subseteq H \text{ for all } H \in \mathcal{H}^+(M) \right\}.$$

If M is a paving matroid, and all dependent hyperplanes in M contain exactly r elements, then each dependent hyperplane is a circuit-hyperplane, and M is a sparse paving matroid. If this is the case, then $\mathcal{H}^+(M)$ is a partial Steiner system, and it follows that

$$|\mathcal{H}^+(M)| \leq \frac{1}{r}\binom{n}{r-1} = \frac{1}{n-r+1}\binom{n}{r}. \tag{5.6}$$

This observation immediately puts an upper bound on the number of sparse paving matroids, a result that was originally proved by Mayhew, and Welsh [MW13].

Theorem 5.5.1. *For all* $0 < r < n$,

$$\log s(n,r) \leq \frac{1}{n-r+1}\binom{n}{r} \log\left(\mathrm{e}(n-r+1)\right).$$

Proof. If M is a sparse paving matroid of rank r on $[n]$, then M is determined by $\mathcal{H}^+(M)$. As $\mathcal{H}^+(M)$ is a collection of r-subsets of M, by the bound (5.6) on the cardinality of $\mathcal{H}^+(M)$ it follows that

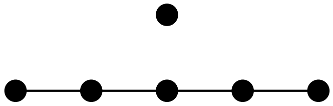
$$s(n,r) \leq \sum_{i=0}^{\frac{1}{n-r+1}\binom{n}{r}} \binom{\binom{n}{r}}{i} \leq (\mathrm{e}(n-r+1))^{\frac{1}{n-r+1}\binom{n}{r}},$$

and the result follows upon taking logarithms. □

The antichain $\mathcal{V}(M)$

Write $p(n,r)$ for the number of paving matroids of rank r on $[n]$.

The aim of this section is to prove the following generalisation of Theorem 5.5.1.



- $|\mathcal{H}(M)| = 6$
- $|\mathcal{H}^+(M)| = 1$
- $|\mathcal{V}_\subseteq(M)| = 10$
- $|\mathcal{V}(M)| = 3$
- $\frac{1}{n-r+1}\binom{n}{r} = 5$

Figure 5.4: $\mathcal{V}_\subseteq(M)$ contains too many r-sets.

Theorem 5.5.2. *For all $n \geq r \geq 3$,*

$$\log p(n,r) \leq \frac{1}{n-r+1}\binom{n}{r} \log\left(\mathrm{e}(n-r+1)\right).$$

Unfortunately, the proof of Theorem 5.5.1 does not carry over to the case of paving matroids. Although (5.6) still holds for paving matroids, $\mathcal{H}^+(M)$ possibly contains sets of cardinality larger than r. The aim of this section therefore is to construct a collection $\mathcal{V}(M)$ of r-sets such that $\mathcal{H}^+(M)$ can be reconstructed from $\mathcal{V}(M)$, and $|\mathcal{V}(M)| \leq \frac{1}{n-r+1}\binom{n}{r}$. More precisely, $\mathcal{V}(M)$ will be constructed in such a way that $M = U(r-1,E)\!\uparrow\!\mathcal{V}(M)$.

As a first attempt, one might construct $\mathcal{V}_\subseteq(M) := \bigcup_{H\in\mathcal{H}^+(M)}\binom{H}{r}$. Note that $\mathcal{V}_\subseteq(M)$ contains only r-sets, and $M = U(r-1,E)\!\uparrow\!\mathcal{V}_\subseteq(M)$. However, $|\mathcal{V}_\subseteq|$ can be much larger than the required bound, as illustrated in Figure 5.4.

We provide a related, but more economical, construction. Define, for $H \in \mathcal{H}(M)$,

$$\mathcal{V}(H) := \left\{V \in \binom{H}{r} : V \text{ is } \textit{consecutive} \text{ in } H\right\},$$

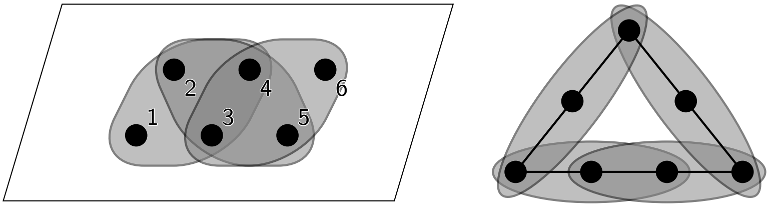
where V is a *consecutive* subset of H if and only if H does not contain any ordered triple $h_1 < h_2 < h_3$ such that $h_1, h_3 \in V$, and $h_2 \in H \setminus V$ (see Figure 5.5a for an example). Clearly

$$|\mathcal{V}(H)| = |H| - r + 1 \qquad \text{for all } H \in \mathcal{H}(M). \tag{5.7}$$

Define

$$\mathcal{V}(M) := \bigcup_{H\in\mathcal{H}(M)} \mathcal{V}(H).$$

We show that $\mathcal{H}(M)$, and hence M, can be reconstructed from $\mathcal{V}(M)$, for which we require the following elementary observation.



(a) Three consecutive subsets in a 6-point plane.

(b) A rank-3 paving matroid, and its antichain $\mathcal{V}(M)$.

Figure 5.5: Consecutive sets and $\mathcal{V}(M)$.

Lemma 5.5.3. *Let M be a paving matroid of rank r. If X and X' are dependent r-sets in M with the property that $|X \cap X'| = r - 1$, then $\mathrm{cl}_M(X) = \mathrm{cl}_M(X')$.*

This observation can be used to recombine members in $\mathcal{V}(M)$ to hyperplanes. More precisely, define a relation $\sim$ on $\mathcal{V}(M)$ by declaring $V \sim V'$ if and only if there exists a sequence $V = V_0, V_1, \ldots, V_k = V'$ in $\mathcal{V}(M)$ such that $|V_i \cap V_{i-1}| = r - 1$ for all $i \in [k]$. It is easily verified that $\sim$ is an equivalence relation, and that its equivalence classes are precisely of the form $\mathcal{V}(H)$, $H \in \mathcal{H}^+(M)$. We thus obtain the following result.

Lemma 5.5.4. *$M \mapsto \mathcal{V}(M)$ is an injective function on paving matroids in $\mathbb{M}(n, r)$.*

Lemma 5.5.5. *If $M \in \mathbb{M}(n, r)$ is a paving matroid, then $|\mathcal{V}(M)| \leq \frac{1}{n-r+1}\binom{n}{r}$.*

Proof. By (5.7), if H is a hyperplane of cardinality k, then $|\mathcal{V}(H)| = k - r + 1$, so if we write h_k for the number of hyperplanes of cardinality k in M, then $|\mathcal{V}(M)| = \sum_{k=r-1}^{n-1} h_k(k - r + 1)$.

As M is paving, each $(r-1)$-subset of E is contained in a unique hyperplane. It follows that the h_k satisfy $\sum_{k=r-1}^{n-1} h_k \binom{k}{r-1} = \binom{n}{r-1}$.

Maximising over the possible values of h_k, we obtain that

$$
\begin{aligned}
|\mathcal{V}(M)| &\leq \max \left\{ \sum_{k=r-1}^{n-1} h_k(k-r+1) : \begin{array}{l} \sum\limits_{k=r-1}^{n-1} h_k \binom{k}{r-1} = \binom{n}{r-1} \\ h_k \geq 0 \\ \qquad \text{for all } k = r-1, r, \ldots, n-1 \end{array} \right\} \\
&= \min \left\{ y\binom{n}{r-1} : \begin{array}{l} y\binom{k}{r-1} \geq k-r+1 \\ \qquad \text{for all } k = r-1, r, \ldots, n-1 \end{array} \right\} \\
&= \frac{1}{r}\binom{n}{r-1}.
\end{aligned}
$$

Here, the first equality follows from linear programming duality, and the solution to the dual programme follows from the fact that $\frac{k-r+1}{\binom{k}{r-1}}$ is maximised for $k = r$. The lemma follows from the identity $\frac{1}{r}\binom{n}{r-1} = \frac{1}{n-r+1}\binom{n}{r}$. □

Theorem 5.5.2 now follows by counting the number of possible collections of r-sets of cardinality at most $\frac{1}{n-r+1}\binom{n}{r}$.

5.6 The antichain $\mathcal{V}(M)$ for general matroids

In this section, we generalise the results from Section 5.5 from paving matroid to general matroids.

This generalisation involves the truncation and its inverse operation erection from Section 5.3. In Section 5.5, each paving matroid was described as the erection of a uniform matroid; the extra information required to construct the erection was recorded in the antichain $\mathcal{V}(M)$. Here, we generalise this construction. The nature of general matroids require them to be built 'from the ground up', i.e. the truncations of M are constructed subsequently, starting from the unique rank-0 matroid. The information required to construct this sequence of truncations can again be stored in an antichain $\mathcal{V}(M)$, which for paving matroids coincides with the previous definition.

$(r-2)$-closures

Recall that we are interested in finding a set $\mathcal{U}$ such that $M = T(M)\uparrow\mathcal{U}$. For sparse paving matroids, it suffices to take $\mathcal{U} = \mathcal{H}^+(M)$, which for paving matroids was generalised to $\mathcal{U} = \mathcal{V}(M)$ in Section 5.5. In this section, we further generalise te construction of $\mathcal{V}(M)$ to matroids that are not necessarily sparse paving, but before we do so, we make an additional improvement.

Each of the k-closures $\mathrm{cl}_k(\cdot)$, $0 \le k \le r-2$, in M depends only on the information in $T(M)$. It follows that if $M = T(M)\!\uparrow\!\mathcal{U}$, and there is $U \in \mathcal{U}$ such that $U = \mathrm{cl}_{r-2}(U')$ for some $U' \subseteq U$, then $M = T(M)\!\uparrow\!\mathcal{U}'$, where $\mathcal{U}' := \mathcal{U} \triangle \{U, U'\}$.

The following lemma combines the observations on essential flats and $(r-2)$-closures.

Lemma 5.6.1. *Let M be a matroid of rank r on E, and let $\mathcal{H}$ be the set of hyperplanes of M. Suppose that for each $H \in \mathcal{H}$, U_H is such that $\mathrm{cl}_{r-2}(U_H) = H$. If $\mathcal{U} := \{U_H : H \in \mathcal{H}, |U_H| \ge r\}$, then $M = T(M)\!\uparrow\!\mathcal{U}$.*

Proof. For each $H \in \mathcal{H}(M)$, either $U_H \in \mathcal{U}$, or U_H is a basis of $T(M)$. It follows that

$$\mathcal{W} := \{\mathrm{cl}_{r-2}(X) : X \in \mathcal{B}(T(M)) \cup \mathcal{U}\}$$

contains all hyperplanes of M, and in addition some sets $\mathrm{cl}_{r-2}(X) \subseteq \mathrm{cl}_M(X)$, where $\mathrm{cl}_M(X)$ is a hyperplane of M. Thus $\mathcal{H}(M)$ are the inclusionwise-maximal elements of $\mathcal{W}$, and it follows that $T(M)\!\uparrow\!\mathcal{W} = M$. By Lemma 5.3.6, $\mathrm{comp}_{T(M)}(\mathcal{W}) = \mathrm{comp}_{T(M)}(\mathcal{U})$, and so $T(M)\!\uparrow\!\mathcal{U} = T(M)\!\uparrow\!\mathcal{W}$. The lemma follows. □

Having restricted $\mathcal{U}$ to $(r-2)$-spanning subsets of essential hyperplanes, there is still some freedom in the particular choice of $\mathcal{U}$. If it is our objective to describe the reconstruction of M from $T(M)$ as economically as possible, a sensible first optimisation is to choose each of the elements of $\mathcal{U}$ as small as possible. Thus, we define

$$U^*_H := \prec\text{-min}\{U : \mathrm{cl}_{r-2}(U) = H\} \qquad \text{for all } H \in \mathcal{H}(M),$$

and

$$\mathcal{U}^*_{r-1} := \{U^*_H : H \in \mathcal{H}(M), |U_H| \ge r\}. \tag{5.8}$$

Note that $\mathcal{U}^*_{r-1}$ satisfies the premisses of Lemma 5.6.1, and hence $M = T(M)\!\uparrow\!\mathcal{U}^*_{r-1}$.

Properties of $\mathcal{U}^*_{r-1}$

Recall that the girth $\mathrm{g}(M)$ of the matroid M is the cardinality of a smallest circuit in M. More generally, we can define the *girth function* of M by $\mathrm{g}(X) \equiv \mathrm{g}_M(X) := \mathrm{g}(M|X)$.

Lemma 5.6.2. *Let $X \subseteq E$ be a $(k-1)$-closed set. Any inclusionwise-minimal $U \subseteq X$ such that $\mathrm{cl}_{k-1}(U) = X$ has $\mathrm{g}(U) > k$.*

Proof. If U contains a circuit C of cardinality at most k, and $e \in C$, then $\mathrm{cl}_{k-1}(U \setminus \{e\}) = X$; this contradicts minimality of U. □

By construction, we immediately obtain the following.

Lemma 5.6.3. *For all $U \in \mathcal{U}^*_{r-1}$,*

- *U is dependent;*
- *$\mathrm{rk}(U) = r - 1$;*
- *$\mathrm{g}(U) = r$; and*
- *$\mathrm{cl}_{r-1}(U) = \mathrm{cl}(U)$.*

The following lemma shows that $\mathcal{U}^*_{r-1}$ encodes a paving matroid.

Lemma 5.6.4. *$\mathcal{U}^*_{r-1}$ is the set of dependent hyperplanes of a paving matroid of rank r on E.*

Proof. By construction, each $U \in \mathcal{U}^*_{r-1}$ contains at least $r-1$ elements, so it suffices to show that each $(r-1)$-subset of E is contained in at most one element of $\mathcal{U}^*_{r-1}$. If this is not the case, then there would be two distinct hyperplanes $H, H' \in \mathcal{H}(M)$ such that $|U^*_H \cap U^*_{H'}| \geq r - 1$. By Lemma 5.6.3, $\mathrm{g}(U^*_H), \mathrm{g}(U^*_{H'}) = r$, and hence $\mathrm{g}(U^*_H \cap U^*_{H'}) \geq r$. On the other hand, $\mathrm{rk}(U^*_H \cap U^*_{H'}) \leq \mathrm{rk}(H \cap H') \leq r - 2$, so $U^*_H \cap U^*_{H'}$ is dependent and hence $\mathrm{g}(U^*_H \cap U^*_{H'}) \leq r - 1$: a contradiction. □

Write

$$P_{r-1}(M) = U\left(r-1, E(M)\right)) {\uparrow} \mathcal{U}^*_{r-1}$$

for the paving matroid whose dependent hyperplanes are $\mathcal{U}^*_{r-1}$.

Lemma 5.6.5. *The map $M \mapsto (T(M), P_{r-1}(M))$ is an injective function $\mathbb{M}(n,r) \to \mathbb{M}(n, r-1) \times \mathbb{P}(n,r)$.*

It is easily verified that the inverse map is given by $(N, P) \mapsto N \uparrow \mathcal{H}^+(P)$.

As a consequence of Lemma 5.6.4, we find that any matroid on n elements of rank r has at most $p(n, r+1)$ erections, where $p(n, r+1)$ is the number of paving matroids on the same ground set and rank $r+1$. This maximum number of erections is attained by the uniform matroid, as it has all paving matroids as erections.

Theorem 5.6.6. *The uniform matroid has the largest number of erections among all matroids of the same rank on the same ground set.*

Constructing matroids from the ground up

Let M be a matroid of rank r on E. In (5.8), we have constructed a collection $\mathcal{U}^*_{r-1}$ such that $M = T(M)\uparrow\mathcal{U}^*_{r-1}$. There is nothing that stops us from giving the truncation $T(M)$ the same treatment, and writing $T(M) = T(T(M))\uparrow\mathcal{U}^*_{r-2}$, and so on. Continuing in this fashion, we obtain a sequence $(\mathcal{U}^*_k : k = 0, 1, \ldots, r-1)$ such that

$$M = (\ldots(M_0\uparrow\mathcal{U}^*_0)\uparrow\ldots)\uparrow\mathcal{U}^*_{r-1}.$$

where M_0 is the unique matroid of rank 0 on E.

For any $k < s \leq r$, we have $\mathcal{U}^*_k(M) = \mathcal{U}^*_k\left(M^{(s)}\right)$. This implies that $\mathcal{U}^*_k$ can be defined directly in terms of the flats of rank k in M.

Lemma 5.6.7. *For a rank-k flat F, write $U^*_F := \prec\text{-min}\{U : \mathrm{cl}_{k-1}(U) = F\}$. Then $\mathcal{U}^*_k = \{U^*_F : F \in \mathcal{F}(M), \mathrm{rk}(F) = k, |U^*_F| > k\}$.*

For a matroid M of rank r, define

$$\mathcal{U}^*(M) := \bigcup_{k=0}^{r-1} \mathcal{U}^*_k.$$

Lemma 5.6.8. *$\mathcal{U}^*(M)$ is an antichain.*

Proof. Suppose that $U, U' \in \mathcal{U}^*(M)$ are such that $U \subseteq U'$. The properties laid out in Lemma 5.6.3 imply that

$$\mathrm{rk}(U) + 1 = g(U) \geq g(U') = \mathrm{rk}(U') + 1 \geq \mathrm{rk}(U) + 1,$$

so in particular $\mathrm{rk}(U) = \mathrm{rk}(U')$. It follows that $\mathrm{cl}(U) = \mathrm{cl}(U')$, and hence equality holds throughout in

$$\mathrm{cl}(U) = \mathrm{cl}_{r-1}(U) \subseteq \mathrm{cl}_{r-1}(U') = \mathrm{cl}(U').$$

So, with $F = \mathrm{cl}(U)$, we have $U = U' = U^*_F$. □

Lemma 5.6.9. *Let F, F' be flats of M of rank k, k', respectively, such that $k' > k$. Let $X \in \binom{U^*_F}{k}$. If $X \subseteq U^*_{F'}$, then $X = \prec\text{-min}\binom{U_F}{k}$.*

Proof. We argue by contradiction. Suppose that $X \subseteq U^*_{F'}$, but $X \neq \prec\text{-min}\binom{U_F}{k}$. Let $X^* = \prec\text{-min}\binom{U_F}{k}$, and define $U' = (U^*_{F'} \setminus X) \cup X^*$. By Lemma 5.6.3, any k-subset of U^*_F spans F, so $\mathrm{cl}(X^*) = F = \mathrm{cl}(X)$. As $k' > k$, this implies $\mathrm{cl}_{k'-1}(X^*) = \mathrm{cl}_{k'-1}(X)$, and hence $\mathrm{cl}_{k'-1}(U') = \mathrm{cl}_{k'-1}(U^*_{F'})$. Moreover, we have $U' \prec U^*_{F'}$, thus contradicting minimality of $U^*_{F'}$. □

Encoding a matroid as a sequence of paving matroids

Let $P_k(M)$ be the paving matroid of rank $k+1$ whose set of dependent hyperplanes is $\mathcal{U}_k^*$. The map

$$M \mapsto (P_0(M), P_1(M), \ldots, P_{r-1}(M))$$

is an injective function. The function encodes a given matroid as a sequence of paving matroids of increasing rank.

It follows in particular that $m(n,r) \leq \prod_{i=0}^{r-1} p(n,i)$. Substituting the upper bound on $p(n,i)$, we obtain, at least for $r = o(n)$,

$$\begin{aligned}\log m(n,r) \leq \sum_{i=0}^{r-1} \frac{1}{n-i}\binom{n}{i+1} \log\left(\mathrm{e}(n-i)\right) \\ = o\left(\frac{1}{n-r}\binom{n}{r+1}\log\left(\mathrm{e}(n-r)\right)\right).\end{aligned}$$

In Section 5.7, we improve this bound to $\log m(n,r) \sim \log p(n,r)$ as $n \to \infty$, provided $r \geq 3$ remains fixed. In order to do this, it is necessary to consider the sequence $(P_0(M), P_1(M), \ldots, P_{r-1}(M))$ of paving matroids associated with M simultaneously, rather than separatel. This can be done by generalising the antichain $\mathcal{V}(M)$, which was defined for paving matroids in Section 5.5, to general matroids.

For $k = 0, 1, \ldots, r-1$, define

$$\mathcal{V}_k(M) = \mathcal{V}(P_k(M)), \tag{5.9}$$

where $\mathcal{V}$ is the function defined in Section 5.5. In addition, define $\mathcal{V}(M) := \bigcup_{k=0}^{r-1} \mathcal{V}_k(M)$. If M is a paving matroid, we now have two definitions of $\mathcal{V}(M)$. Fortunately, the following lemma implies that for paving matroids, the new definition coincides with the definition from Section 5.5.

Lemma 5.6.10. *If M is a paving matroid of rank r, then $P_{r-1}(M) = M$, and $P_k(M) \cong U(k,n)$ for all $k < r-1$.*

Proof. The lemma follows immediately from the observation that for paving matroids $\mathcal{U}^*(M) = \mathcal{H}^+(M)$. □

The following lemma shows that, although it may be the case that some of the $P_i(M)$ are the same for different matroids, the sequence $(\mathcal{V}_k(M))_{k=0}^{r-1}$ determines M, thus generalising Lemma 5.5.4.

Lemma 5.6.11. *The map $M \mapsto \mathcal{V}(M)$ is injective.*

Properties of $\mathcal{V}(M)$

We conclude this section by listing some of the structural properties of the antichain $\mathcal{V}(M)$. To start with, each set in $\mathcal{V}(M)$ is a circuit of M.

Lemma 5.6.12. *$\mathcal{V}(M) \subseteq \mathcal{C}(M)$.*

Proof. Suppose that $V \in \mathcal{V}(M)$ has cardinality $k+1$. Then $V \in \mathcal{V}_k(M)$. By Lemma 5.6.7, there exists a flat of rank k in M such that $V \in \binom{U_F^*}{k+1}$. It follows that $\mathrm{rk}(V) \leq \mathrm{rk}(F) = k$, so V is dependent. On the other hand, by Lemma 5.6.3, $\mathrm{g}(V) \geq \mathrm{g}(U_F^*) = k+1$. It follows that V is a circuit. □

Lemma 5.6.12 immediately implies the following result.

Lemma 5.6.13. *$\mathcal{V}(M)$ is an antichain.*

Recall that if M is a paving matroid, then distinct r-sets in $\mathcal{V}(M)$ do not intersect in $r-1$ elements, unless they are consecutive subsets of the same hyperplane. The following lemma generalises the structural implications.

Lemma 5.6.14. *Let $V, V' \in \mathcal{V}(M)$ with $|V| = k+1$, $|V'| = k'+1$, and $|V \cap V'| = k$.*

(i) If $k' > k$, then $V \cap V' = \prec\text{-min}\binom{V}{k}$. If in addition $V \in \binom{U_F^*}{k+1}$, then $V = \prec\text{-min}\binom{U_F^*}{k+1}$.

(ii) If $k' = k$ and $V \prec V'$, then $V \cap V' = \prec\text{-max}\binom{V}{k} = \prec\text{-min}\binom{V'}{k}$.

Proof. Suppose that F and F' are flats of rank k and k', respectively, so that $V \in \mathcal{V}(U_F^*)$ and $V' \in \mathcal{V}(U_{F'}^*)$. The set $V \cap V'$ is a k-subset of both U_F^* and $U_{F'}^*$. (i) If $k' > k$, we have by Lemma 5.6.9 that $V \cap V' = \prec\text{-min}\binom{U_F^*}{k}$. It follows that there is only one consecutive $(k+1)$-set in U_F^* containing $V \cap V'$, and this is $\prec\text{-min}\binom{U_F^*}{k+1}$. (ii) If $k = k'$ and $V \prec V'$, then $F = \mathrm{cl}(V \cap V') = F'$, and the claim follows from the fact that V and V' must be consecutive sets. □

5.7 An upper bound on the number of matroids

In Section 5.5, the antichain $\mathcal{V}(M)$ was introduced as a concise description of paving matroids. Noting that each element of $\mathcal{V}(M)$ has cardinality r, an upper bound on $p(n, r)$ was obtained by bounding $|\mathcal{V}(M)|$.

In Section 5.6, the definition of $\mathcal{V}(M)$ was extended to general matroids. In Theorem 5.7.1 below, the bound on $|\mathcal{V}(M)|$ of Lemma 5.5.5 is extended to general matroids. As a result, we obtain a bound on the number $m(n, r)$ of matroids, as well as a bound on the number of essential flats that a matroid can have.

Analysis of $\mathcal{V}(M)$

We prove the following generalisation of Lemma 5.5.5.

Theorem 5.7.1. *Suppose that $r \geq 3$ and $n \geq 2r$. For all $M \in \mathbb{M}(n, r)$, $|\mathcal{V}(M)| \leq \frac{1}{n-r+1}\binom{n}{r}$.*

A central result in the theory of antichains is the well-known *LYM-inequality*, a proof of which can be found in [Juk01, Theorem 8.6].

Lemma 5.7.2. *Let E be a set of cardinality n, and let $\mathcal{A}$ be an antichain in $\mathscr{P}(E)$. Then $\sum_{A \in \mathcal{A}} \frac{1}{\binom{n}{|A|}} \leq 1$.*

As $\mathcal{V}(M)$ is an antichain, we would like to apply the LYM-inequality to it to obtain a bound on its cardinality. However, a direct application of the LYM-inequality shows only that $|\mathcal{V}(M)| \leq \binom{n}{r}$. Instead, we prove a bound on a related antichain, $\mathcal{A}(M)$, which is defined as follows. For all $U \in \mathcal{U}_k^*$, put

$$\mathcal{A}(U) := \begin{cases} \binom{U}{r-1} & \text{if } k = r-1 \\ \binom{U}{k}^- & \text{if } 0 < k < r-1 \\ \binom{U}{1} & \text{if } k = 0 \end{cases}$$

where $\binom{U}{k}^- := \binom{U}{k} \setminus \left\{ \prec\text{-min} \binom{U}{k} \right\}$, and let

$$\mathcal{A}(M) = \bigcup_{U \in \mathcal{U}^*(M)} \mathcal{A}(U).$$

Lemma 5.7.3. *$\mathcal{A}(M)$ is an antichain, and $\mathcal{A}(U) \cap \mathcal{A}(U') = \emptyset$ for distinct $U, U' \in \mathcal{U}^*(M)$.*

Proof. The first claim follows from Lemma 5.6.9. To prove the second claim, let $U \in \mathcal{U}_i^*$ and $U' \in \mathcal{U}_j^*$ be obtained from flats F and F'; without loss of generality, assume that $i \leq j$. Suppose that $\mathcal{A}(U) \cap \mathcal{A}(U') \neq \emptyset$, and let $X \in \mathcal{A}(U) \cap \mathcal{A}(U')$. Suppose that $|X| = k$.

If $i < j$, then it must be the case that $i = 0$ and $j = k = 1$. If this is the case, then the single element in X must be a loop as well as a nonloop, which cannot happen. If $i = j = 0$, then we must have $U = U'$, since $|\mathcal{U}_0^*| = 1$. If $i = j > 0$, then $k = i$. As $\mathrm{g}(X) \geq \mathrm{g}(U) = k$, X is independent. It follows that $F = \mathrm{cl}(X) = F'$, and so $U = U'$. □

Having settled that $\mathcal{A}(M)$ is an antichain, we can apply the LYM-inequality to it to obtain

$$\sum_{k=1}^{r-1} \sum_{U \in \mathcal{U}_k^*} \frac{|\mathcal{A}(U)|}{\binom{n}{k}} + \sum_{U \in \mathcal{U}_0^*} \frac{|\mathcal{A}(U)}{\binom{n}{1}} \leq 1. \tag{5.10}$$

The following lemma bounds the cardinality of $\mathcal{V}(M)$ by relating $\mathcal{V}(M)$ to $\mathcal{A}(M)$.

Lemma 5.7.4. *Suppose that $r \geq 3$ and $n \geq 2r$. For all matroids $M \in \mathbb{M}(n, r)$,*

$$\sum_{k=0}^{r-1} |\mathcal{V}_k| c_k \leq 1 \qquad \textit{where} \qquad c_k := \begin{cases} \frac{r}{\binom{n}{r-1}} & \textit{if } k = r-1 \\ \frac{k}{\binom{n}{k}} & \textit{if } 0 < k < r-1 \\ \frac{1}{n} & \textit{if } k = 0. \end{cases} \tag{5.11}$$

Proof. We prove (5.11) by relating $\mathcal{V}(M)$ to $\mathcal{A}(M)$, and then applying (5.10). For all $U \in \mathcal{U}_{r-1}^*$, we have $|\mathcal{A}(U)| = \binom{|U|}{r-1}$, while $|\mathcal{V}(M)| = |U| - r + 1$. Consequently, it follows that $|\mathcal{A}(U)| \geq r|\mathcal{V}(U)|$. Similarly, if $0 < k < r-1$, and $U \in \mathcal{U}_k^*$, then $|\mathcal{A}(U)| = \binom{|U|}{k} - 1$, while $|\mathcal{V}(U)| = |U| - k$; hence $|\mathcal{A}(U)| \geq k|\mathcal{V}(U)|$. Finally, for $U \in \mathcal{U}_0^*$, we have $\mathcal{V}(U) = \mathcal{A}(U)$, and so $|\mathcal{V}(U)| = |\mathcal{A}(U)|$. Substituting these relations into (5.10), and observing that $|\mathcal{V}_k| = \sum_{U \in \mathcal{U}_k^*} |\mathcal{V}(U)|$, we obtain the desired bound (5.11). □

Lemma 5.7.4 implies Therem 5.7.1.

Proof of Theorem 5.7.1. First, consider the case $n = 2r = 6$. Let $M \in \mathbb{M}(6, 3)$. Suppose that M has ℓ loops, so that $|\mathcal{V}_0| = \ell$. Write $\mathcal{P}$ for its set of parallel classes. Each parallel class $P \in \mathcal{P}$ gives rise to $|P| - 1$ elements in $\mathcal{V}_1$, so $|\mathcal{V}_1| \leq \sum_{P \in \mathcal{P}} (|P| - 1)$. In addition, the number of 3-circuits in M is at most $|\mathcal{P}| - 2$; thus

$$|\mathcal{V}(M)| \leq \ell + \sum_{P \in \mathcal{P}} (|P| - 1) + |\mathcal{P}| - 2 = 4,$$

which is strictly smaller than the required bound, which is 5.

Having settled the case $n = 2r = 6$, we may assume that $n \geq \max\{2r, 7\}$. For $0 < k < r-2$, we have

$$\frac{c_{k+1}}{c_k} = \frac{(k+1)^2}{k(n-k)} \leq 1, \qquad \text{while} \qquad \frac{c_{r-1}}{c_{r-2}} = \frac{r(r-1)}{(r-2)(n-r+2)} \leq 1.$$

In particular, $c_k \geq c_{r-1}$ for all $k > 0$, and as $c_0 = c_1$, also $c_0 \geq c_{r-1}$. It follows from Lemma 5.7.4 that

$$|\mathcal{V}(M)| = \sum_{i=0}^{r-1} |\mathcal{V}_k| \leq \frac{1}{c_{r-1}} \sum_{i=0}^{r-1} c_k |\mathcal{V}_k| \leq \frac{1}{r}\binom{n}{r-1} = \frac{1}{n-r+1}\binom{n}{r},$$

which concludes the proof. □

An upper bound on the number of matroids of fixed rank

By now we have established that for all $M \in \mathbb{M}(n,r)$, $\mathcal{V}(M)$ is a collection of at most $\frac{1}{n-r+1}\binom{n}{r}$ subsets of $[n]$, each of cardinality at most r. Bounding the number of such collections immediately gives the bound

$$\log m(n,r) \leq \frac{1}{n-r+1}\binom{n}{r} \log\left(\mathrm{e}n + o(n)\right),$$

for each fixed $r \geq 3$. A slightly more careful analysis results in a proof of the more precise Theorem 5.1.1, which we repeat here for convenience.

Theorem 5.1.1. *For all $r \geq 3$ and all $n \geq r + 12$,*

$$\log m(n,r) \leq \frac{1}{n-r+1}\binom{n}{r} \log\left(\mathrm{e}(n-r+1)\right).$$

Lemma 5.7.5. *For all $n \geq 15$, $m(n,3) \leq (\mathrm{e}(n-2))^{\frac{1}{n-2}\binom{n}{3}} - 1$.*

Proof. A matroid of rank 3 on ground set $[n]$ is determined by the triple $(\mathcal{V}_0, \mathcal{V}_1, \mathcal{V}_2)$, where $\mathcal{V}_k \subseteq \binom{[n]}{k+1}$. Writing $v_k = |\mathcal{V}_k|$, it follows from Lemma 5.7.4 that $v_0\frac{1}{n} + v_1\frac{1}{n} + v_2\frac{3}{\binom{n}{2}} \leq 1$, and hence

$$m(n,3) \leq \sum \binom{\binom{n}{1}}{v_0}\binom{\binom{n}{2}}{v_1}\binom{\binom{n}{3}}{v_2},$$

where the sum is over all triples $(v_0, v_1, v_2) \in \mathbb{Z}^3_{\geq 0}$ such that $v_0\frac{1}{n} + v_1\frac{1}{n} + v_2\frac{3}{\binom{n}{2}} \leq 1$. We split the sum over all possible values of $v := v_0 + v_1$. Note that $\sum \binom{\binom{n}{1}}{v_0}\binom{\binom{n}{2}}{v_1} = \binom{\binom{n+1}{2}}{v}$, where the sum is over all pairs

(v_0, v_1) such that $v_0 + v_1 = v$. We obtain

$$m(n,3) \le \sum_{v=0}^{n} \binom{\binom{n+1}{2}}{v} \sum_{v_2=0}^{\frac{(n-v)(n-1)}{6}} \binom{\binom{n}{3}}{v_2} = \sum_{v_2=0}^{\frac{n(n-1)}{6}} \binom{\binom{n}{3}}{v_2} T_n(v_2),$$

with

$$T_n(v_2) = \sum_{v=0}^{\lfloor n - v_2 \frac{6}{n-1} \rfloor} \binom{\binom{n+1}{2}}{v}.$$

Note that $T_n(v_2) = 1$ whenever $n - v_2 \frac{6}{n-1} < 1$, while otherwise we have

$$T_n(v_2) \le \left(\frac{\mathrm{e}\binom{n+1}{2}}{\left\lfloor n - v_2 \frac{6}{n-1} \right\rfloor} \right)^{\lfloor n - v_2 \frac{6}{n-1} \rfloor} \le \left(\mathrm{e}\binom{n+1}{2} \right)^{\frac{6}{n-1}\left(\frac{n(n-1)}{6} - v_2\right)}.$$

It follows that $T_n(v_2) \le (n-2)^{\frac{n(n-1)}{6} - v_2}$ as soon as $n \ge 15$, and a slightly more careful analysis shows that in that case even $T_n(0) \le (n-2)^{\frac{n(n-1)}{6}} - 1$. By the binomial theorem, we obtain

$$\begin{aligned} m(n,3) &\le \sum_{v_2=0}^{\frac{n(n-1)}{6}} \binom{\binom{n}{3}}{v_2} (n-2)^{\frac{n(n-1)}{6} - v_2} - 1 \\ &\le (n-2)^{\frac{n(n-1)}{6}} \left(1 + \frac{1}{n-2}\right)^{\binom{n}{3}} - 1, \end{aligned}$$

and the lemma follows from the bound $1 + x \le \mathrm{e}^x$. □

Proof of Theorem 5.1.1. By Lemma 5.7.5, combined with the Entropy Blow-Up Lemma, we obtain

$$\begin{aligned} \log(m(n,r)+1) &\le \frac{\binom{n}{r}}{\binom{n-r+3}{3}} \log(m(n-r+3,3)+1) \\ &\le \frac{1}{n-r+1}\binom{n}{r} \log\left(\mathrm{e}(n-r+1)\right), \end{aligned}$$

if only $n - r + 3 \ge 15$. □

As a by-product we obtain the following result, which lends credence to Higgs's suggestion that essential flats offer a concise description of matroids.

Theorem 5.7.6. *Suppose that $r \ge 3$ and $n \ge 2r$. A matroid of rank r on n elements has at most $\frac{1}{n-r+1}\binom{n}{r}$ essential flats.*

Proof. By Lemma 5.3.9, every essential flat is pseudo-essential. The number of pseudo-essential flats is $|\mathcal{U}^*(M)|$. As $|\mathcal{U}^*(M)| \le |\mathcal{V}(M)|$, and $|\mathcal{V}(M)| \le \frac{1}{n-r+1}\binom{n}{r}$, the desired result follows. □

5.8 The number of sparse paving matroids of fixed rank

This section focusses on sparse paving matroids. In particular, the following result is proved.

Theorem 5.1.2. *For all fixed $r \ge 3$,*

$$\log s(n,r) = \frac{1}{n-r+1}\binom{n}{r}\log\left(\mathrm{e}^{1-r}n + o(n)\right) \qquad \text{as } n \to \infty.$$

The lower bound is based on Keevash's proof of a corresponding lower bound on the number of designs [Kee15], which in turn is based on the analysis by Bennett and Bohman of the random greedy hypergraph matching process [BB12]. Here, the presentation of Keevash's proof is adapted to our setting. The upper bound relies on the entropy method. It is an extension to partial Steiner systems of Keevash's [Kee15] generalisation to designs of a result by Linial and Luria [LL13] on the number of Steiner triple systems.

Lower bound

Steiner systems and Keevash's counting result Let us write $D(n,r,q)$ for the number of Steiner systems $S(n,r,q)$. Designs do not always exist, and $D(n,r,q) = 0$ for many values of n, r, and q. In particular, designs can only exist if the parameters satisfy certain divisibility conditions. Keevash shows that these conditions are also sufficient for suffiently large n; moreover, he provides the following lower bound.

Theorem 5.8.1 ([Kee15, Theorem 6.1])**.** *For all $r > q \ge 2$, there exists n_0 such that if $n > n_0$ and $\binom{r-i}{q-i} | \binom{n-i}{q-i}$ for all $0 \le i \le q-1$, then*

$$D(n,r,q) \ge \left(\mathrm{e}^{1-Q}N + o(N)\right)^{Q^{-1}\binom{n}{q}},$$

where $N = \binom{n-q}{r-q}$ and $Q = \binom{r}{q}$.

As each Steiner system $S(n,r,r-1)$ is the set of dependent hyperplanes of a sparse paving matroid of rank r, we have $s(n,r) \ge$

$D(n, r, r-1)$, and it follows that

$$\log s(n,r) \geq \frac{1}{n-r+1}\binom{n}{r}\log\left(\mathrm{e}^{1-r}n + o(n)\right), \tag{5.12}$$

for fixed r as $n \to \infty$, provided

$$(r-i) | \binom{n-i}{r-i-1} \qquad \text{for all } 0 \leq i \leq r-2. \tag{5.13}$$

Unfortunately, (5.13) is not satisfied for all possible values of n and r, so in many cases, the bound $s(n,r) \geq D(n,r,r-1)$ reduces to the trivial bound $s(n,r) \geq 0$. In this section, we show that (5.12) holds, even if (5.13) fails, thus proving the lower bound of Theorem 5.1.2.

The random greedy hypergraph matching process Keevash's proof of Theorem 5.8.1 is phrased in terms of hypergraph *matchings*; a matching in a hypergraph $\mathcal{G}$ is a collection of vertex-disjoint edges in $\mathcal{G}$. Write $\mathrm{maxmatch}\,(\mathcal{G})$ for the cardinality of a maximum-size matching in $\mathcal{G}$, and $\mathrm{match}\,(\mathcal{G})$ for the number of matchings in $\mathcal{G}$.

Let $\mathcal{G}(n,r)$ be the hypergraph with vertex set $\binom{[n]}{r-1}$ and edge set $\left\{\binom{X}{r-1} : X \in \binom{[n]}{r}\right\}$. Matchings in $\mathcal{G}(n,r)$ are in one-to-one correspondence with partial Steiner systems $S_p(n,r,r-1)$, and hence with sparse paving matroids in $\mathbb{S}(n,r)$. Thus,

$$s(n,r) = \mathrm{match}\,(\mathcal{G}(n,r)).$$

Keevash's proof of Theorem 5.8.1 is based on the randomised construction of a large collection of matchings in $\mathcal{G}(n,r)$. We might expect that it extends to a lower bound on $\mathrm{match}\,(\mathcal{G}(n,r))$ for general n and r for the following reason.

Let Z be any matching in $\mathcal{G}(n,r)$. Each vertex in $\mathcal{G}(n,r)$ is contained in at most one edge in Z, and each edge in Z contains exactly r vertices. It follows that

$$\mathrm{maxmatch}\,(\mathcal{G}(n,r)) \leq \frac{1}{r}\binom{n}{r-1} = \frac{1}{n-r+1}\binom{n}{r}. \tag{5.14}$$

Whenever a Steiner system exists, the upper bound in (5.14) is achieved. The Erdős-Hanani conjecture [EH63] (first proved by Rödl [Röd85] using a semi-random technique that is now known as the Rödl nibble) states that

$$\mathrm{maxmatch}\,(\mathcal{G}(n,r)) \geq (1-o(1))\frac{1}{n-r+1}\binom{n}{r},$$

for fixed r as $n \to \infty$. Thus, partial Steiner systems can be roughly as large as the bound in (5.14), even when the parameters are such that no full Steiner system exists. It does then not require a lot of imagination to speculate that a similar result might hold for the related quantity $\operatorname{match}(\mathcal{G}(n, r))$ as well. Theorem 5.5.1 states that this is indeed the case.

The *random greedy hypergraph matching process* constructs a random maximal matching in $\mathcal{G}$ by making a series of random choices. The edges of the maximal matching are selected in order, and in each step an available edge is selected uniformly at random from among all available edges. After selecting an edge, it, and all edges that intersect it, become unavailable. The process stops when there are no available edges left.

A refined analysis of the random greedy hypergraph matching process for u-uniform, d-regular hypergraphs is provided by Bennett and Bohman [BB12]. Writing $\boldsymbol{E}(i)$ for the set of available edges in the i-th iteration of the process and $\boldsymbol{Q}(i) := |\boldsymbol{E}(i)|$, they show that with high probability, when the process terminates, all but a small fraction of the vertices are saturated by the constructed matching. Moreover, they show that (again with high probability) until the process reaches the end, $\boldsymbol{Q}(i)$ remains close to its expected value.

Bennett and Bohman provide the following heuristic derivation of the expected value of $\boldsymbol{Q}(i)$. Each edge that is chosen into the matching makes u vertices unavailable. Thus, it is reasonable that $\boldsymbol{\mathcal{G}}(i) := \mathcal{G}|\boldsymbol{E}(i)$ should be close to a random subhypergraph of $\mathcal{G}$ in which each vertex is included with probability $p_i := 1 - iu/N$. Thus, any given edge $e \in E(\mathcal{G})$ should be included in $\boldsymbol{\mathcal{G}}(i)$ with probability p_i^u, and so we should hope that

$$\boldsymbol{Q}(i) \approx |\mathcal{G}| p_i^u = \frac{Nd}{u} p_i^u.$$

Theorem 5.8.2 ([BB12]). *Let $\mathcal{G}$ be a u-uniform, d-regular hypergraph on N vertices. Assume that u is fixed, and that $d \to \infty$ as $N \to \infty$. Let L be the maximum over all pairs of distinct vertices of the number of edges containing that pair, and suppose that $L = o\left(d/\log^5 N\right)$ as $N \to \infty$. Let $\boldsymbol{T}$ be the smallest index i for which $\boldsymbol{Q}(i) \notin \frac{Nd}{u} p_i^u (1 \pm \varepsilon_i)$, where*

$$\varepsilon_i := \frac{15uLp_i^{2-2u} \log N (1 - u \log p_i)^2}{d}.$$

With high probability,

$$\boldsymbol{T} \geq \left(1 - O\left(\left(\frac{L}{d} \log^5 N\right)^{\frac{1}{2(u-1)}}\right)\right) \frac{N}{u}.$$

Proof of the lower bound The hypergraph $\mathcal{G}(n,r)$ has $N := \binom{n}{r-1}$ vertices, is r-uniform, and is regular of degree $n-r+1$. Moreover, two distinct vertices are contained in at most one edge, so $L = 1$.

We prove the lower bound of Theorem 5.1.2 by running the random greedy hypergraph matching process for many steps. This is possible by Theorem 5.8.2, which moreover gives an estimate of the number of possible choices in each step. In this way, it is shown that the random greedy matching process gives a large number of possible outputs. After compensating for double counting, this results in a large number of sparse paving matroids, thus proving the lower bound. We make the argument precise.

Proof of Theorem 5.1.2 (lower bound). We construct a large family of random matchings in $\mathcal{G}(n,r)$, or equivalently sparse paving matroids in $\mathbb{S}(n,r)$, by running the random greedy hypergraph matching process until $T := \frac{N}{r}\left[1 - d^{-\frac{1}{3(r-1)}}\right]$ edges are selected.

Note that for all $i \leq T$,

$$\varepsilon_i \leq \varepsilon_T = \frac{15rp_T^{2-2r}\log N(1 - r\log p_T)^2}{d} \leq d^{-1/4}.$$

The natural logarithm of the number of different ordered matchings that can be created in this way is at least

$$\begin{aligned}\sum_{i=1}^{m} \ln\left(\frac{Nd}{r}p_i^r\left(1 - d^{-\frac{1}{4}}\right)\right) &\geq m\left(\ln\frac{Nd}{r} - 2d^{-\frac{1}{4}}\right) + r\sum_{i=1}^{m}\ln\left(1 - \frac{ir}{N}\right)\\ &\geq m\left(\ln\frac{Nd}{r} - r - 2d^{-\frac{1}{4}}\right).\end{aligned}$$

Of course, the order in which the edges are chosen does not matter, so we must subtract

$$\ln T! = T\left(\ln T - 1 + O\left(\frac{\ln T}{T}\right)\right)$$

to obtain the number of unordered matchings obtained in this way. It follows that $\ln s(n,r)$ is at least

$$\begin{aligned}&T\left(\ln d - r + 1 - 2d^{-1/4} - O\left(\frac{\ln T}{T}\right)\right)\\ &\qquad = \frac{1}{r}\binom{n}{r-1}\left(1 - d^{-\frac{1}{3(r-1)}}\right)\left(\ln(\mathrm{e}^{1-r}d - o(d))\right),\end{aligned}$$

which concludes the proof, as $\frac{1}{r}\binom{n}{r-1} = \frac{1}{n-r+1}\binom{n}{r}$ and $d = n-r+1$. □

Sparse paving matroids with few circuit-hyperplanes

Write $s(n, r, \leq t)$ for the number of sparse paving matroids on $[n]$ of rank r that have at most t circuit-hyperplanes. The following result implies that for fixed r, almost every sparse paving matroid of rank r has $\frac{1-o(1)}{n-r+1}\binom{n}{r}$ circuit-hyperplanes.

Corollary 5.8.3. *For all $r \geq 3$, and all $0 \leq c \leq 1$,*

$$\frac{\log s\left(n, r, \leq \frac{c}{n-r+1}\binom{n}{r}\right)}{\log s(n,r)} \leq c + O\left(\frac{1}{\log n}\right) \qquad \textit{as } n \to \infty.$$

Proof. As $s(n, r, 0) = 1$, the claim holds for $c = 0$. For the remainder of the proof, assume that $c > 0$, and let $t := \frac{c}{n-r+1}\binom{n}{r}$. A sparse paving matroid is determined by its circuit-hyperplanes, so

$$s(n, r, \leq t) \leq \sum_{i=0}^{t} \binom{\binom{n}{r}}{i} \leq \left(\frac{\mathrm{e}\binom{n}{r}}{t}\right)^{t}.$$

Combining the upper bound with the lower bound on $s(n, r)$ from Theorem 5.1.2, it follows that

$$\frac{\log s(n, r, \leq t)}{\log s(n,r)} \leq c\frac{\log(\mathrm{e}n/c)}{\log(\mathrm{e}^{1-r}n + o(n))} = c\left(1 + O\left(\frac{1}{\log n}\right)\right). \qquad \square$$

Upper bound

We now turn to proving the upper bound of Theorem 5.1.2. Our proof is a generalisation to sparse paving matroids of an upper bound on Steiner triple systems by Linial and Luria [LL13]; initially, the proof follows theirs, and we indicate where our version deviates from the original.

Outline Fix $3 \leq r \leq n$, and let $\boldsymbol{X} \in \mathbb{S}(n, r)$ be chosen uniformly at random. Then $\log s(n, r) = \mathscr{H}(\boldsymbol{X})$, where $\mathscr{H}(\boldsymbol{X})$ is the entropy of $\boldsymbol{X}$.

Let $\mathcal{S} := \binom{[n]}{r} \cup \{\dagger\}$. Associated with $\boldsymbol{X}$ is a collection of $\mathcal{S}$-valued random variables $\left(\boldsymbol{X}_A : A \in \binom{[n]}{r-1}\right)$, where

$$\boldsymbol{X}_A := \begin{cases} H & \text{if } H \supseteq A \text{ is a circuit-hyperplane in } \boldsymbol{X} \\ \dagger & \text{otherwise.} \end{cases}$$

As each $(r-1)$-set is contained in at most one circuit-hyperplane, these random variables are well-defined. Suppose that $\lhd$ is a linear order on $\binom{[n]}{r-1}$. The sequence $\left(\boldsymbol{X}_A : A \in \binom{[n]}{r-1}\right)$ determines $\boldsymbol{X}$, so by Lemma 3.3.1(iii)

$$\mathscr{H}(\boldsymbol{X}) = \sum_{A\in\binom{[n]}{r-1}} \mathscr{H}(\boldsymbol{X}_A \mid (\boldsymbol{X}_{A'} : A' \lhd A))\,. \tag{5.15}$$

Computing the right-hand side of (5.15) is difficult, since each of the terms depends on those $(r-1)$-sets that come earlier in the order $\lhd$. This may be resolved by randomising the order $\lhd$. Such a random order can be constructed from a random function $\boldsymbol{\lambda}\colon \binom{[n]}{r-1} \to [0,1]$ by choosing each of the entries of $\boldsymbol{\lambda}$ independently and uniformly at random, and defining[2]

$$A \lhd A' \qquad \text{if and only if} \qquad \boldsymbol{\lambda}(A) > \boldsymbol{\lambda}(A').$$

The random variables $(\boldsymbol{X}, \boldsymbol{\lambda})$ live in the space $\Omega := \mathbb{S}(n,r) \times [0,1]^{\binom{[n]}{r-1}}$, equipped with the (uniform) product probability measure.

Bounding $s(n,r)$ by an integral The aim of this subsection is to prove that for all $\delta > 0$, there is an integer $n(\delta)$ such that for all $n \geq n(\delta)$

$$\log s(n,r) \\ \leq \binom{n}{r-1} \int_0^1 \lambda^{r-1} \log\Big[\Big(1+\lambda^{r(r-1)}(n-r)\Big)\Big(1+\delta(r-1)\lambda^{1-r}\Big)\Big]\,\mathrm{d}\lambda. \tag{5.16}$$

Let $(\boldsymbol{X}, \boldsymbol{\lambda})$ be a random sparse paving matroid and order. For any $(r-1)$-set A, one of three things may happen: either A is not contained in any circuit-hyperplanes (i.e. $\boldsymbol{X}_A = \dagger$); or A is contained in a circuit-hyperplane of $\boldsymbol{X}$, in which case either A is the first (with respect to $\lhd$) among $\binom{\boldsymbol{X}_A}{r-1}$, or it is not. Let $E_A^{\dagger}$, E_A^{+}, and E_A^{-} be the corresponding events; more precisely

$$\begin{aligned}
E_A^{\dagger} &:= \{(X,\lambda) \in \Omega : X_A = \dagger\}\,;\\
E_A^{-} &:= \left\{(X,\lambda) \in \Omega : X_A \neq \dagger, A \lhd A' \text{ for all } A' \in \binom{X_A}{r-1} \setminus \{A\}\right\};\\
E_A^{+} &:= \left\{(X,\lambda) \in \Omega : \begin{array}{l} X_A \neq \dagger, \\ \text{there exists } a' \in A \text{ such that } X_A \setminus \{a'\} \lhd A \end{array}\right\}.
\end{aligned}$$

For each A, the three events are disjoint. In addition, these events essentially partition the probability space Ω.

[2] With probability 1, no two $(r-1)$-sets get the same $\boldsymbol{\lambda}$-value. Therefore, we may assume that all $\boldsymbol{\lambda}$-values are different.

Lemma 5.8.4. *For each A,* $\mathbb{P}\Big(E_A^{\dagger} \cup E_A^{+} \cup E_A^{-}\Big) = 1$.

Proof. The complement of $E_A^{\dagger} \cup E_A^{+} \cup E_A^{-}$ is contained in the event that there exist distinct $(r-1)$-sets A and A' such that $\boldsymbol{\lambda}(A) = \boldsymbol{\lambda}(A')$, which is an event of measure 0. □

The inclusion of the event $E_A^{\dagger}$ is new compared to the work by Linial and Luria [LL13], as in a Steiner triple system (or more generally a design) every $(r-1)$-set is contained in an r-set and so $\boldsymbol{X}_A \neq \boldsymbol{\dagger}$ for all A. Arguing that inclusion of this event only has a negligible influence on the eventual estimate of $\log s(n,r)$ will take most of the remainder of this section.

Suppose that $\boldsymbol{X}_A \neq \boldsymbol{\dagger}$. Note that $\boldsymbol{X}_A \in \Big\{H' \in \binom{[n]}{r} : A \subseteq H'\Big\}$. An element $H \in \Big\{H' \in \binom{[n]}{r} : A \subseteq H'\Big\} \setminus \boldsymbol{X}_A$ is *unavailable* (for A) if

- there exists $a \in A$ such that $H \setminus \{a\} \lhd A$; or
- there exists $a \in A$ such that $\boldsymbol{X}_{H\setminus\{a\}} \neq \boldsymbol{\dagger}$, and there exists $a' \in H \setminus \{a\}$ such that $\boldsymbol{X}_{H\setminus\{a\}} \setminus \{a'\} \lhd A$.

Occurrence of either of these events rules out the possibility that $\boldsymbol{X}_A = H$, given the history $(\boldsymbol{X}_{A'} : A' \lhd A)$. Call H *available* if it not unavailable. Define the random variables $\boldsymbol{N}_A$, indexed by $(r-1)$-sets, by

$$\boldsymbol{N}_A := \begin{cases} 1 + \left|\Big\{H \in \binom{[n]}{r} \setminus X_A : H \text{ available for } X_A\Big\}\right| & \text{if } (X,\lambda) \in E_A^{-} \\ 1 & \text{otherwise.} \end{cases}$$

Let us use subscript $\boldsymbol{\lambda}$ (resp. $\boldsymbol{X}$) to indicate conditioning on $\boldsymbol{X}$ (resp. $\boldsymbol{\lambda}$), i.e.

$$\mathbb{P}_{\boldsymbol{\lambda}}(\,\cdot\,) := \mathbb{P}(\,\cdot \mid \boldsymbol{X}), \qquad \text{and} \qquad \mathbb{P}_{\boldsymbol{X}}(\,\cdot\,) := \mathbb{P}(\,\cdot \mid \boldsymbol{\lambda}),$$

and similarly $\mathbb{E}_{\boldsymbol{\lambda}}[\,\cdot\,]$ and $\mathbb{E}_{\boldsymbol{X}}[\,\cdot\,]$.

The following lemma describes the importance of the random variables $\Big(\boldsymbol{N}_A : A \in \binom{[n]}{r-1}\Big)$.

Lemma 5.8.5. $\mathscr{H}(\boldsymbol{X}) \leq \sum_{A \in \binom{[n]}{r-1}} \mathbb{E}_{\boldsymbol{\lambda}(A)}[\mathbb{E}_{\boldsymbol{X}}[\mathbb{E}_{\boldsymbol{\lambda}}[\log \boldsymbol{N}_A \mid \boldsymbol{\lambda}(A)]]]$.

Proof. Equation (5.15) implies that

$$\mathscr{H}(\boldsymbol{X}) \leq \sum_{A \in \binom{[n]}{r-1}} \mathbb{E}_{\boldsymbol{\lambda}}[\mathscr{H}(\boldsymbol{X}_A \mid (\boldsymbol{X}_{A'} : \boldsymbol{\lambda}(A') > \boldsymbol{\lambda}(A)))]\,.$$

Relative to the random order $\lhd$, after revealing $(\boldsymbol{X}_{A'} : A' \lhd A)$, all unavailable vertices have been ruled out as possible values for $\boldsymbol{X}_A$, and it follows that

$$\mathscr{H}(\boldsymbol{X}_A \mid (\boldsymbol{X}_{A'} : A' \lhd A)) \leq \log \boldsymbol{N}_A.$$

The lemma now follows by further taking the expected value with respect to $\boldsymbol{X}$, and then conditioning on $\boldsymbol{\lambda}(A)$. □

In order to prove (5.16), we shall bound the right-hand side of the expression in Lemma 5.8.5. We have

$$\begin{aligned}
\mathbb{E}_{\boldsymbol{\lambda}}[\log \boldsymbol{N}_A \mid \boldsymbol{\lambda}(A)] &= \mathbb{E}_{\boldsymbol{\lambda}}\left[\log \boldsymbol{N}_A \left(\mathbb{1}_{\left\{E_A^{\dagger}\right\}} + \mathbb{1}_{\left\{E_A^{-}\right\}} + \mathbb{1}_{\left\{E_A^{+}\right\}}\right) \middle| \boldsymbol{\lambda}(A)\right] \\
&= \mathbb{E}_{\boldsymbol{\lambda}}\left[\log \boldsymbol{N}_A \mathbb{1}_{\left\{E_A^{-}\right\}} \middle| \boldsymbol{\lambda}(A)\right] \\
&= \mathbb{P}_{\boldsymbol{\lambda}}\big(E_A^{-} \mid \boldsymbol{\lambda}(A)\big)\, \mathbb{E}_{\boldsymbol{\lambda}}\big[\log \boldsymbol{N}_A \mid E_A^{-}, \boldsymbol{\lambda}(A)\big]
\end{aligned}$$

Conditional on $\boldsymbol{\lambda}(A)$, the event E_A^{-} occurs precisely when both $\boldsymbol{X}_A \neq \dagger$ and $\boldsymbol{\lambda}(A') < \boldsymbol{\lambda}(A)$ for each $A' \in \binom{\boldsymbol{X}_A}{r-1}$. By independence, it follows that

$$\mathbb{P}_{\boldsymbol{\lambda}}\big(E_A^{-} \mid \boldsymbol{\lambda}(A)\big) = (\boldsymbol{\lambda}(A))^{r-1}\, \mathbb{1}_{\{\boldsymbol{X}_A \neq \dagger\}}, \tag{5.17}$$

and hence

$$\mathbb{P}_{\boldsymbol{X}}\big(\mathbb{E}_{\boldsymbol{\lambda}}[\log \boldsymbol{N}_A \mid \boldsymbol{\lambda}(A)] = \mathbb{E}_{\boldsymbol{\lambda}}\big[\log \boldsymbol{N}_A \mid E_A^{-}, \boldsymbol{\lambda}(A)\big]\big) = 1. \tag{5.18}$$

By Jensen's inequality,

$$\mathbb{E}_{\boldsymbol{\lambda}}\big[\log \boldsymbol{N}_A \mid E_A^{-}, \boldsymbol{\lambda}(A)\big] \leq \log \mathbb{E}_{\boldsymbol{\lambda}}\big[\boldsymbol{N}_A \mid E_A^{-}, \boldsymbol{\lambda}(A)\big]\,. \tag{5.19}$$

Introducing $\mathbb{P}_{\boldsymbol{\lambda}}^{(A)}(\,\cdot\,)$ as a shorthand for $\mathbb{P}_{\boldsymbol{\lambda}}\big(\,\cdot \mid E_A^{-}, \boldsymbol{\lambda}(A)\big)$ and $\mathbb{E}_{\boldsymbol{\lambda}}^{(A)}[\,\cdot\,]$ for the corresponding expectation, upon combining (5.17)–(5.19), we obtain

$$\mathbb{E}_{\boldsymbol{\lambda}}[\log \boldsymbol{N}_A \mid \boldsymbol{\lambda}(A)] \leq \mathbb{1}_{\{\boldsymbol{X}_A \neq \dagger\}}\, (\boldsymbol{\lambda}(A))^{r-1}\, \log \mathbb{E}_{\boldsymbol{\lambda}}^{(A)}[\boldsymbol{N}_A]\,.$$

Next, we bound $\mathbb{E}_{\boldsymbol{\lambda}}^{(A)}[\boldsymbol{N}_A]$. For $A \in \binom{[n]}{r-1}$, $a \in A$, and $f \in [n] \setminus A$, define

$$\boldsymbol{I}_A^{f,a} := \mathbb{1}_{\left\{\boldsymbol{X}_{A \triangle \{a,f\}} = \dagger\right\}}.$$

The following lemma expresses $\mathbb{E}_{\lambda}^{(A)}[\boldsymbol{N}_A]$ in terms of the indicator functions $\boldsymbol{I}_A^{f,a}$.

Lemma 5.8.6. *On* $\{\boldsymbol{X}_A \neq \boldsymbol{\dagger}\}$,

$$\mathbb{E}_{\boldsymbol{\lambda}}^{(A)}[\boldsymbol{N}_A] = 1 + (\boldsymbol{\lambda}(A))^{r(r-1)} \sum_{f \in [n] \setminus \boldsymbol{X}_A} \prod_{a \in A} \left(1 - \boldsymbol{I}_A^{f,a} + \frac{\boldsymbol{I}_A^{f,a}}{(\boldsymbol{\lambda}(A))^{r-1}}\right).$$

Proof. By linearity of expectation,

$$\mathbb{E}_{\boldsymbol{\lambda}}^{(A)}[\boldsymbol{N}_A] = 1 + \sum_{f \in [n] \setminus \boldsymbol{X}_A} \mathbb{P}_{\boldsymbol{\lambda}}^{(A)}(f \text{ is available for } A)\,. \tag{5.20}$$

For $f \in [n] \setminus A$, and $a \in A$, define the events

$$F_A^f := \big\{(X, \lambda) \in \Omega : \lambda(A) > \lambda(A \triangle \{a, f\}) \text{ for all } a \in A\big\},$$

and

$$\begin{aligned} G_A^{f,a} &:= \big\{(X,\lambda) \in \Omega : X_{A \triangle \{a,f\}} = \boldsymbol{\dagger}\big\} \\ &\cup \left\{ (X,\lambda) \in \Omega : \begin{array}{c} X_{A \triangle \{a,f\}} \neq \boldsymbol{\dagger}, \\ \lambda\left(X_{A \triangle \{a,f\}} \setminus \{a'\}\right) < \lambda(A) \\ \text{for all } a' \in A \triangle \{a,f\} \end{array} \right\}. \end{aligned}$$

Note that $f \notin \boldsymbol{X}_A$ is available for A precisely on the event $F_A^f \cap \bigcap_{a \in A} G_A^{f,a}$. By the chain rule for probabilities,

$$\begin{aligned} &\mathbb{P}_{\boldsymbol{\lambda}}^{(A)}(f \text{ is available for } A) \\ &\qquad = \mathbb{P}_{\boldsymbol{\lambda}}^{(A)}\left(F_A^f\right) \times \prod_{a \in A} \mathbb{P}_{\boldsymbol{\lambda}}^{(A)} \left(G_A^{f,a} \,\middle|\, F_A^f, \bigcap_{\substack{a' \in A \\ a' < a}} G_A^{f,a'} \right). \end{aligned} \tag{5.21}$$

We compute each of the factors separately. On the event $\{\boldsymbol{X}_A \neq \boldsymbol{\dagger}\}$, F_A^f is independent of E_A^-, and so

$$\mathbb{P}_{\boldsymbol{\lambda}}^{(A)}\left(F_A^f\right) = (\boldsymbol{\lambda}(A))^{r-1}\,. \tag{5.22}$$

For each of the remaining factors, we condition further on whether $\boldsymbol{X}_{A \triangle \{a,f\}} = \boldsymbol{\dagger}$ or not. Let $a \in A$. Since the measure $\mathbb{P}_{\boldsymbol{\lambda}}^{(A)}(\,\cdot\,)$ conditions on $\boldsymbol{X}$, we have

$$\mathbb{P}_{\boldsymbol{\lambda}}^{(A)}\big(\boldsymbol{X}_{A \triangle \{a,f\}} = \boldsymbol{\dagger}\big) = \boldsymbol{I}_A^{f,a}. \tag{5.23}$$

Since $\left\{\boldsymbol{X}_{A\triangle\{a,f\}} = \boldsymbol{\dagger}\right\} \subseteq G_A^{f,a}$,

$$\mathbb{P}_{\boldsymbol{\lambda}}^{(A)}\left(G_A^{f,a} \,\middle|\, F_A^f, \bigcap_{\substack{a'\in A\\ a'<a}} G_A^{f,a'}, \boldsymbol{X}_{A\triangle\{a,f\}} = \boldsymbol{\dagger}\right) = 1, \tag{5.24}$$

Similarly, conditional on $\boldsymbol{X}_{A\triangle\{a,f\}} \neq \boldsymbol{\dagger}$, the event $G_A^{f,a}$ happens precisely when $\boldsymbol{\lambda}\left(X_{A\triangle\{a,f\}} \setminus \{a'\}\right) < \boldsymbol{\lambda}(A)$ for all $a' \in A\triangle\{a,f\}$, so

$$\mathbb{P}_{\boldsymbol{\lambda}}^{(A)}\left(G_A^{f,a} \,\middle|\, F_A^f, \bigcap_{\substack{a'\in A\\ a'<a}} G_A^{f,a'}, \boldsymbol{X}_{A\triangle\{a,f\}} \neq \boldsymbol{\dagger}\right) = \left(\boldsymbol{\lambda}(A)\right)^{r-1}. \tag{5.25}$$

It follows from (5.23)–(5.25) that for each $a \in A$

$$\mathbb{P}_{\boldsymbol{\lambda}}^{(A)}\left(G_A^{f,a} \,\middle|\, F_A^f, \bigcap_{\substack{a'\in A\\ a'<a}} G_A^{f,a'}\right) = \boldsymbol{I}_A^{f,a} + \left(1 - \boldsymbol{I}_A^{f,a}\right)\left(\boldsymbol{\lambda}(A)\right)^{r-1}. \tag{5.26}$$

The lemma follows from substituting (5.22) and (5.26) into (5.21). □

If instead of a random sparse paving matroid, $\boldsymbol{X}$ would have been a random Steiner system, then $\boldsymbol{I}_A^{a,f} = 0$ for all A, f, and a. This would greatly simplify the right-hand side in Lemma 5.8.6, as the sum would simply reduce to $n - r$, e.g. for $r = 3$, [LL13, Lemma 3.1] is recovered. For general matroids, however, $\boldsymbol{I}_A^{f,a} = 1$ may hold for some values of its parameters. Fortunately, the following lemma shows that $\boldsymbol{I}_A^{f,a} = 0$ most of the time.

Lemma 5.8.7. *For all $\delta > 0$, there exists $n(\delta)$ such that for all $n \geq n(\delta)$, and any $A \in \binom{[n]}{r-1}$,*

$$\mathbb{P}(\boldsymbol{X}_A = \boldsymbol{\dagger}) \leq \delta.$$

Proof. By Corollary 5.8.3, all but a $\delta/2$-fraction of matroids in $\mathbb{S}(n, r)$ have at least $\frac{1-\delta/2}{n-r+1}\binom{n}{r}$ circuit-hyperplanes, provided n is sufficiently large. Hence $\boldsymbol{X}_A \neq \boldsymbol{\dagger}$ for at least $(1 - \delta/2)\binom{n}{r-1}$ $(r-1)$-sets A. It follows that $\mathbb{P}_{\boldsymbol{X}}(\boldsymbol{X}_A) \leq \delta/2 + \delta/2 = \delta$. □

For $A \in \binom{[n]}{r-1}$ and $f \notin A$, define $\boldsymbol{Z}_A^f := \sum_{a\in A} \boldsymbol{I}_A^{f,a}$. Fix $\delta > 0$, and let n be so large that the conclusion of Lemma 5.8.7 holds. It follows that $\mathbb{E}_{\boldsymbol{X}}\left[\boldsymbol{Z}_A^f\right] \leq |A|\delta = (r-1)\delta$. As

$$\prod_{a\in A}\left(1-\boldsymbol{I}_A^{f,a}+\frac{\boldsymbol{I}_A^{f,a}}{(\boldsymbol{\lambda}(A))^{r-1}}\right) \leq 1+(\boldsymbol{\lambda}(A))^{1-r}\boldsymbol{Z}_A^f,$$

it follows from Lemma 5.8.6 that

$$\begin{aligned}\mathbb{E}_{\boldsymbol{X}}\left[\mathbb{E}_{\boldsymbol{\lambda}}^{(A)}[\boldsymbol{N}_A]\right] &\leq 1+(\boldsymbol{\lambda}(A))^{r(r-1)}\sum_{f\in[n]\setminus\boldsymbol{X}_A}\left(1+(\boldsymbol{\lambda}(A))^{1-r}\mathbb{E}_{\boldsymbol{X}}\left[\boldsymbol{Z}_A^f\right]\right)\\ &\leq 1+(\boldsymbol{\lambda}(A))^{r(r-1)}(n-r)\left(1+(\boldsymbol{\lambda}(A))^{1-r}\delta(r-1)\right)\\ &\leq \left(1+(\boldsymbol{\lambda}(A))^{r(r-1)}(n-r)\right)\left(1+(\boldsymbol{\lambda}(A))^{1-r}\delta(r-1)\right).\end{aligned}$$

Substituting this bound into Lemma 5.8.5, we obtain (5.16).

Bounding the integral Changing the base of the logarithm from 2 to e, (5.16) can be written as

$$\ln s(n,r) \leq \binom{n}{r-1}(I_1+I_2), \tag{5.27}$$

where

$$I_1 := \int_0^1 \lambda^{r-1}\ln\left[1+\lambda^{r(r-1)}(n-r)\right]\mathrm{d}\lambda,$$

and

$$I_2 := \int_0^1 \lambda^{r-1}\ln\left[1+\lambda^{1-r}\delta(r-1)\right]\mathrm{d}\lambda.$$

The first of these integrals can be computed by a change of variables $u=\lambda^r$, which yields

$$\begin{aligned}I_1 = \frac{1}{r}\int_0^1 &\ln\left[1+u^{r-1}(n-r)\right]\mathrm{d}u\\ &= \frac{1}{r}\left[\ln(n-r)+1-r+o(1)\right] \qquad \text{as } n\to\infty.\end{aligned} \tag{5.28}$$

For the second integral, using that $\ln(1+x)\leq\sqrt{x}$ (which is valid for all $x\geq 0$) to bound the integrand, we obtain

$$I_2 \leq \sqrt{\delta(r-1)}\int_0^1 \lambda^{(r-1)/2}\,\mathrm{d}\lambda = \sqrt{\delta(r-1)}\frac{2}{r+1} < \frac{2\sqrt{\delta}}{\sqrt{r}}. \tag{5.29}$$

Using (5.28)–(5.29) to bound (5.27), we obtain

$$\log s(n,r) \leq \frac{1}{n-r+1}\binom{n}{r}\left[\ln\left(\mathrm{e}^{1-r}(n-r)\right) + o(1) + \frac{2\sqrt{\delta}}{\sqrt{r}}\right].$$

As δ is arbitrarily small, this proves the upper bound in Theorem 5.1.2.

5.9 A refined upper bound on the number of rank-3 paving matroids

Combining the upper bound on $\log p(n,r)$ for fixed $r \geq 3$ from Theorem 5.5.2 with the lower bound obtained in Theorem 5.1.2, we find that

$$\begin{aligned}\frac{1}{n-r+1}\binom{n}{r}\log\left(\mathrm{e}^{1-r}n - o(n)\right) &\leq \log p(n,r) \\ &\leq \frac{1}{n-r+1}\binom{n}{r}\log\left(\mathrm{e}(n-r+1)\right). \quad (5.30)\end{aligned}$$

Thus, we have established the behaviour of $\log p(n,r)$ up to the constant factor inside the logarithm. The upper bound for sparse paving matroids of fixed rank is stronger. In that case, we even know that the constant is e^{1-r}.

The method for obtaining the upper bound on $\log p(n,r)$ in (5.30) seems wasteful. It uses the bound $|\mathcal{V}(M)| \leq \frac{1}{n-r+1}\binom{n}{r}$, but ignores the additional structural properties of $\mathcal{V}(M)$ such as those provided in Lemma 5.6.14. An improved analysis of the number of possible $\mathcal{V}(M)$ may yield a bound on $\log p(n,r)$ that is as strong as the bound on sparse paving matroids. In this section, we focus on paving matroids of rank 3, for which we obtain the following improved upper bound.

Theorem 5.1.3.

$$\log p(n,3) \leq \frac{1}{n-2}\binom{n}{3}\log\left(\mathrm{e}^{0.35}n + o(n)\right).$$

Probabilistic setup

Theorem 5.1.3 is proved by analysing the probability that a random collection of triples conforms to the structure of $\mathcal{V}(M)$. We show that if the number of triples is close to the maximum possible, then this probability is exponentially small in n^2.

Specialising Lemma 5.6.14 to paving matroids of rank 3, we obtain that $\mathcal{V}(M)$ satisfies

$$\begin{aligned}&\forall\, V, V' \in \mathcal{V}(M) : \\ &\quad \Big[|V \cap V'| = 2 \implies V \triangle V' = \big\{ \prec\text{-min}\, V \cup V', \prec\text{-max}\, V \cup V' \big\} \Big]. \end{aligned} \tag{5.31}$$

Let $\boldsymbol{\mathcal{T}}$ be a set of t triples in $[n]$, chosen uniformly at random from among all sets of t triples, and let $P_n(t)$ for the probability that $\boldsymbol{\mathcal{T}}$ satisfies (5.31). Write $T := \frac{1}{n-2}\binom{n}{3}$. It was shown in Lemma 5.5.5 that $|\mathcal{V}(M)| \le T$ for paving matroids of rank 3, so that $P_n(t) = 0$ whenever $t > T$. Note that

$$p(n,3) \le \sum_{t=0}^{T} \binom{\binom{n}{3}}{t} P_n(t). \tag{5.32}$$

The following lemma shows that, in order to prove Theorem 5.1.3, it suffices to consider $P_n(t)$ for values of t close to T.

Lemma 5.9.1. *If $\beta \ge 0$ is such that*

$$\max_{(1-\frac{4}{\ln n})T \le t \le T} P_n(t) \le \mathrm{e}^{-\beta T + o(T)} \qquad \textit{as } n \to \infty, \tag{5.33}$$

then

$$\log p(n,3) \le T \ln\left(\mathrm{e}^{1-\beta} n + o(n)\right).$$

Proof. Our starting point is (5.32). Using (5.33) to bound $P_n(t)$ for values of t close to T, and the trivial bound $P_n(t) \le 1$ for smaller values of t, we obtain

$$\begin{aligned} p(n,3) &\le \sum_{t=0}^{\lfloor (1-\frac{4}{\ln n})T \rfloor} \binom{\binom{n}{3}}{t} + \mathrm{e}^{-\beta T + o(T)} \sum_{t=\lfloor (1-\frac{4}{\ln n})T \rfloor + 1}^{T} \binom{\binom{n}{3}}{t} \\ &\le \left(\frac{\mathrm{e}(n-2)}{1 - \frac{4}{\ln n}} \right)^{(1-\frac{4}{\ln n})T} + \mathrm{e}^{-\beta T + o(T)} \left(\mathrm{e}(n-2)\right)^{T}. \end{aligned}$$

The right-hand side is dominated by its second term, and the lemma follows upon taking logarithms. □

Aggregate statistics

We study the collection $\boldsymbol{\mathcal{T}}$ of t random triples through a collection of derived statistics that are defined in this section. Write $\boldsymbol{W}_{i,j}$, $2 \le i \le$

$j \le n-1$ for the number of triples of the form $\{\alpha < i < j+1\}$ that are in $\boldsymbol{\mathcal{T}}$. In addition, define the following aggregate statistics:

$$\begin{aligned}
\boldsymbol{Z}_i &:= \big|\{\{\alpha < \beta < \gamma\} \in \boldsymbol{\mathcal{T}} : \beta = i\}\big| = \sum_{k \ge i} \boldsymbol{W}_{i,k},\\
\boldsymbol{Q}_j &:= \big|\{\{\alpha < \beta < \gamma\} \in \boldsymbol{\mathcal{T}} : \gamma = j+1\}\big| = \sum_{k \le j} \boldsymbol{W}_{k,j},\\
\boldsymbol{S}_j &:= \big|\{\{\alpha < \beta < \gamma\} \in \boldsymbol{\mathcal{T}} : \beta < j, \gamma > j\}\big| = \sum_{i<j} \sum_{k \ge j} \boldsymbol{W}_{i,k};
\end{aligned}$$

and write

$$\boldsymbol{Z} := (\boldsymbol{Z}_2, \boldsymbol{Z}_3, \ldots, \boldsymbol{Z}_{n-1}), \quad \boldsymbol{Q} := (\boldsymbol{Q}_2, \boldsymbol{Q}_3, \ldots \boldsymbol{Q}_{n-1}), \qquad \text{and}$$
$$\boldsymbol{S} := (\boldsymbol{S}_2, \boldsymbol{S}_3, \ldots, \boldsymbol{S}_{n-1}).$$

We collect some easy facts about the sequences $\boldsymbol{Z}$, $\boldsymbol{Q}$ and $\boldsymbol{S}$. Observe that each triple in $\boldsymbol{\mathcal{T}}$ is counted in exactly one of the $\boldsymbol{W}_{i,j}$, which implies the following lemma.

Lemma 5.9.2. $\sum_{j=2}^{n-1} \boldsymbol{Z}_j = t$, *and* $\sum_{j=2}^{n-1} \boldsymbol{Q}_j = t$.

The following lemma shows that $\boldsymbol{S}$ can be computed from the pair $(\boldsymbol{Z}, \boldsymbol{Q})$. For given sequences z and q, in what follows we shall write $s_j(z,q)$ for the corresponding value of s_j.

Lemma 5.9.3. $\boldsymbol{S}_2 = 0$, *while* $\boldsymbol{S}_{j+1} - \boldsymbol{S}_j = \boldsymbol{Z}_j - \boldsymbol{Q}_j$ *for all* $j \ge 2$.

Proof. That $\boldsymbol{S}_2 = 0$ follows from the fact that there are no triples whose central element is 1. The second claim follows from a manipulation of sums:

$$\boldsymbol{S}_{j+1} + \boldsymbol{Q}_j = \sum_{i \le j} \sum_{k \ge j} \boldsymbol{W}_{i,k} = \boldsymbol{S}_j + \boldsymbol{Z}_j. \qquad \square$$

Bounding $P_n(t)$ in terms of the statistics

For two sequences $z = (z_2, \ldots, z_{n-1})$ and $q = (q_2, \ldots, q_{n-1})$, write

$$P_n(z,q) := \mathbb{P}(\boldsymbol{Z} = z, \boldsymbol{Q} = q),$$

and

$$P_n(t \mid z,q) := \mathbb{P}(\boldsymbol{\mathcal{T}} \text{ satisfies (5.31)} \mid \boldsymbol{Z} = z, \boldsymbol{Q} = q).$$

By the law of total probability,

$$P_n(t) = \sum_{(z,q)\in\Omega(n,t)} P_n(t \mid z,q) P_n(z,q), \tag{5.34}$$

where $\Omega(n,t)$ denotes the support of $P_n(z,q)$. The following lemma implies that the asymptotics of $\frac{1}{T}\ln P_n(t)$ are determined by the largest term in (5.34).

Lemma 5.9.4. *If* $n \geq 4$ *and* $t \leq T$*, then* $\log|\Omega(n,t)| \leq 2n \log n$*.*

Proof. If the pair (z,q) is in the support of $P_n(z,q)$, then $\sum_{i=2}^{n-1} z_i = \sum_{i=2}^{n-1} q_i = t$ by Lemma 5.9.2. It follows that there are at most $\binom{t+n-3}{n-3}$ possible sequences of $(z_i)_{i=2}^{n-1}$ and $(q_i)_{i=2}^{n-1}$ each, and hence that

$$|\Omega(n,t)| \leq \binom{t+n-3}{n-3}^2 \leq \left(\frac{\mathrm{e}(t+n-3)}{n-3}\right)^{2(n-3)}.$$

The lemma follows. □

An optimisation problem

In view of Lemma 5.9.4, maximising $P_n(t \mid z,q)P_n(z,q)$ over all pairs $(z,q) \in \Omega(n,t)$ suffices to obtain the asymptotics of $\frac{1}{T}\ln P_n(t)$. In this section, we formulate an optimisation problem that yields an upper bound. The optimisation problem is obtained by bounding each of the factors $P_n(t \mid z,q)$ and $P_n(z,q)$ and relaxing the condition that $(z,q) \in \Omega(n,t)$.

Relaxing the constraints Clearly, if $(z,q) \in \Omega(n,t)$, then $z_i \geq 0$ and $q_i \geq 0$ for all i. The following lemma shows that z_i and q_i are both at most $\min\{i-1, n-i\}$.

Lemma 5.9.5. *Let* $z \equiv (z_i)_{i=2}^{n-1}$ *and* $q \equiv (q_i)_{i=2}^{n-1}$ *be two sequences. If there exists* $i \in \{2,3,\ldots,n-1\}$ *for which* $z_i > \min\{i-1,n-i\}$ *or* $q_i > \min\{i-1,n-i\}$*, then* $P(t \mid z,q) = 0$*.*

Proof. Suppose that $z_i > \min\{i-1,n-i\}$. Conditional on $\boldsymbol{Z}_i = z_i$, there exists $j \geq i$ such that $\boldsymbol{W}_{i,j} \geq 2$; thus $\boldsymbol{\mathcal{T}}$ contains two triples that intersect in $\{i, j+1\}$. If that is the case, then $\boldsymbol{\mathcal{T}}$ certainly does not satisfy (5.31). The case that $q_i > \min\{i-1,n-i\}$ is analysed similarly. □

Bounding the factors We use the trivial bound $P_n(z,q) \leq 1$. The following lemma bounds the factor $P_n(t \mid z,q)$.

Lemma 5.9.6.

$$P_n(t|z,q) \leq \prod_{i=2}^{n-1} \prod_{k=0}^{z_i-1} \frac{(i-1-k)(n-i-k) - s_i(z,q)}{(i-1)(n-i)}.$$

Proof. Property (5.31) implies that the collection $\mathcal{V}(M)$ satisfies, for each $i \in \{2,3,\ldots,n-1\}$, the following properties:

(i) No two triples whose central element is i have the same minimum element;

(ii) For all triples whose central element is i, all $j < i$, and all T' whose central element is j, $T \setminus \{i\} \neq T' \setminus \{j\}$.

Let $\boldsymbol{\mathcal{T}}$ be a random collection of t triples, and write $\mathcal{A}_i$ for the event that $\boldsymbol{\mathcal{T}}$ satisfies the properties (i) and (ii) for index i. Using the chain rule for probabilities,

$$\begin{aligned} P_n(t|z,q) &\leq \mathbb{P}\left(\bigcap_{i=2}^{n-1} \mathcal{A}_i \,\middle|\, \boldsymbol{Z}=z, \boldsymbol{Q}=q\right) \\ &= \prod_{i=2}^{n-1} \mathbb{P}\left(\mathcal{A}_i \,\middle|\, \bigcap_{j<i} \mathcal{A}_j, \boldsymbol{Z}=z, \boldsymbol{Q}=q\right). \end{aligned} \tag{5.35}$$

We analyse each of the factors separately. For the i-th factor, we must choose z_i triples whose central element is i, such that the resulting index satisfies (i)–(ii). Note that there are $(i-1)(n-i)$ possible triples. However, the previous choices for lower indices eliminate $s_i(z,q)$ of these choices. In addition, each choice of a triple excludes one possible position to the left and one position to the right of i for inclusion in further triples, thus showing that, for $i = 2,3,\ldots,n-1$,

$$\begin{aligned} &\mathbb{P}\left(\mathcal{A}_i \,\middle|\, \bigcap_{i<j} \mathcal{A}_j, \boldsymbol{Z}=z, \boldsymbol{Q}=q\right) \\ &\qquad = \prod_{k=0}^{z_i-1} \frac{(i-1-k)(n-i-k) - s_i(z,q)}{(i-1)(n-i)}. \end{aligned} \tag{5.36}$$

The lemma follows by substituting (5.36) into (5.35). □

The optimisation problem We are now ready to formulate the optimisation problem. Define $\beta_n(t)$ as the value of the following maximisation problem over the variables $z_2, z_3, \ldots, z_{n-1}$.

$$\begin{aligned}
\beta_n(t) := \qquad \max \quad & \sum_{i=2}^{n-1} \biggl[-2z_i - (i-1) f\left(1 - \frac{z_i}{i-1}\right) \\
& \qquad\qquad - (n-i) f\left(1 - \frac{z_i}{n-i}\right)\biggr] \\
\text{s.t.} \quad & \sum_{i=2}^{n-1} z_i = t \qquad\qquad (5.37\text{a}) \\
& 0 \le z_i \le \min\{i-1, n-i\} \\
& \qquad\qquad \text{for all } i = 2, 3, \ldots, n-1. \qquad (5.37\text{b})
\end{aligned}$$

The next lemma shows that $\beta_n(t)$ provides an upper bound on $P_n(t)$.

Lemma 5.9.7. $\ln P_n(t) \le \beta_n(t) + 6n \ln n$.

Proof. From Lemma 5.9.6 and the bound $s_j(z, q) \ge 0$, it follows that

$$\ln P_n(t \mid z, q) \le \sum_{i=2}^{n-1} \sum_{k=0}^{z_i - 1} \left[\ln\left(1 - \frac{k}{i-1}\right) + \ln\left(1 - \frac{k}{n-i}\right)\right]. \qquad (5.38)$$

We approximate the inner sum by an integral. Define

$$\varepsilon_i(k) := \begin{cases} \frac{1}{2}\left[\ln\left(1 - \frac{k}{i-1}\right) - \ln\left(1 - \frac{k+1}{i-1}\right)\right] & \text{if } 0 \le k \le i-2, \\ \frac{1}{2}\ln\left(1 - \frac{i-2}{i-1}\right) - \ln\left(1 - \frac{i-3/2}{i-1}\right) & \text{if } k = i-1. \end{cases}$$

We obtain

$$\begin{aligned}
\sum_{k=0}^{z_i-1} \ln\left(1 - \frac{k}{i-1}\right) &= \sum_{k=0}^{z_i-1} \int_k^{k+1} \ln\left(1 - \frac{\lfloor x \rfloor}{i-1}\right) \mathrm{d}x \\
&\le \sum_{k=0}^{z_i-1} \left[\int_k^{k+1} \ln\left(1 - \frac{x}{i-1}\right) \mathrm{d}x + \varepsilon_i(k)\right].
\end{aligned}$$

Due to the telescoping nature of the sums of $\varepsilon_i(k)$, it follows that

$$\begin{aligned}
&\sum_{k=0}^{z_i-1} \ln\left(1 - \frac{k}{i-1}\right) \\
&\qquad \le \begin{cases} z_i \int_0^1 \ln\left(1 - \frac{x z_i}{i-1}\right) \mathrm{d}x - \frac{\ln\left(1 - \frac{z_i}{i-1}\right)}{2} & \text{if } z_i < i-1, \\ z_i \int_0^1 \ln\left(1 - \frac{x z_i}{i-1}\right) \mathrm{d}x - \ln\left(1 - \frac{i-3/2}{i-1}\right) & \text{if } z_i = i-1, \end{cases}
\end{aligned}$$

which in particular implies that

$$\sum_{k=0}^{z_i-1} \ln\left(1 - \frac{k}{i-1}\right) \leq z_i \int_0^1 \ln\left(1 - \frac{xz_i}{i-1}\right) \mathrm{d}x + \ln(2(i-1)). \quad (5.39)$$

Similarly,

$$\sum_{k=0}^{z_i-1} \ln\left(1 - \frac{k}{n-i}\right) \leq z_i \int_0^1 \ln\left(1 - \frac{xz_i}{n-i}\right) \mathrm{d}x + \ln(2(n-i)). \quad (5.40)$$

Note that

$$\int_0^1 \ln(1-\alpha x)\, \mathrm{d}x = -1 - \left(1 - \frac{1}{\alpha}\right) \ln(1-\alpha)$$

for all $0 < \alpha \leq 1$. Substituting (5.39) and (5.40) into (5.38) yields

$$\begin{aligned} \ln P_n(t \mid z, q) \leq \sum_{i=2}^{n-1} \Bigg[&- 2z_i - (i-1) f\left(1 - \frac{z_i}{i-1}\right) \\ &- (n-i) f\left(1 - \frac{z_i}{n-i}\right) \Bigg] \\ &+ \sum_{i=2}^{n-1} \big[\ln(2(i-1)) + \ln(2(n-i)) \big]. \end{aligned} \quad (5.41)$$

Note that $\sum_{i=2}^{n-1} \big[\ln(2(i-1)) + \ln(2(n-i))\big] \leq 4n \ln n$. By Lemma 5.9.4 and (5.41),

$$\begin{aligned} \ln P_n(t) &\leq 2n \ln n + \max_{(z,q)\in\Omega(n,t)} \ln P_n(t \mid z, q) \\ &\leq 6n \ln n + \max_{(z,q)\in\Omega(n,t)} \sum_{i=2}^{n-1} \Bigg[-2z_i - (i-1) f\left(1 - \frac{z_i}{i-1}\right) \\ &\qquad - (n-i) f\left(1 - \frac{z_i}{n-i}\right) \Bigg]. \end{aligned}$$

Note that, in the right-hand side, the function that is maximised does not depend on q. By Lemma 5.9.5, the bound remains true when instead the maximum is taken over all sequences $z = (z_2, z_3, \ldots, z_{n-1})$ satisfying (5.37a)–(5.37b). The lemma follows. □

Solving the optimisation problem

Finally, we solve the optimisation problem (5.37).

Lemma 5.9.8. *The optimal solution to* (5.37) *is of the form*

$$z_i^* = \frac{n-1}{2}\left(1 - \sqrt{1 - c_{n,t}\frac{(n-i)(i-1)}{(n-1)^2}}\right).$$

The $(c_{n,t})$ *tend uniformly to a constant* $c \in (0,4)$, *in the sense that*

$$\lim_{n\to\infty} \min_{(1-\frac{4}{\ln n})T \le t \le T} c_{n,t} = \lim_{n\to\infty} \max_{(1-\frac{4}{\ln n})T \le t \le T} c_{n,t} = c.$$

Moreover, there exists $\beta > 0.65$ *such that*

$$\max_{(1-\frac{4}{\ln n})T \le t \le T} \lim_{n\to\infty} \frac{1}{T}\beta_n(t) \le -\beta + o(1). \tag{5.42}$$

Proof. Consider the relaxed problem

$$\begin{aligned} \beta_n'(t) := \max \sum_{i=2}^{n-1} \Bigg[-2z_i - (i-1)f\left(1 - \frac{z_i}{i-1}\right) \\ -(n-i)f\left(1 - \frac{z_i}{n-i}\right)\Bigg] \\ \text{s.t.} \sum_{i=2}^{n-1} z_i = t, \end{aligned} \tag{5.43}$$

which is obtained from (5.37) by relaxing the bounds on z_i. We use the method of Lagrange multipliers to solve the relaxed problem (5.43). Introduce a multiplier $\lambda \equiv \lambda_{n,t}$ for the constraint. Any maximiser $(z_2, z_3, \dots, z_{n-1})$ should satisfy

$$\begin{cases} \ln\left(1 - \frac{z_i}{i-1}\right) + \ln\left(1 - \frac{z_i}{n-i}\right) = \lambda, \\ \qquad\qquad i = 2, 3, \dots, n-1 & (5.44a) \\ \sum_{i=2}^{n-1} z_i = t. & (5.44b) \end{cases}$$

The system has the unique solution $(z_2^*, z_3^*, \dots, z_{n-1}^*)$, with $c_{n,t} := 4\left(1 - e^{\lambda}\right)$. Since the z_i^* must sum to a positive quantity, at least one of them must be positive, and it follows that $c_{n,t} \ge 0$. The quantity inside the square root must be nonnegative, from which in particular it follows that $c_{n,t} \le 4$.

Next, we prove the claimed limiting behaviour of the $c_{n,t}$. Introduce

$$G_n(x) := \frac{1}{n}\sum_{i=2}^{n-1}\sqrt{1 - x\frac{(i-1)(n-i)}{(n-1)^2}},$$

and

$$G(x) := \int_0^1 \sqrt{1 - xu(1-u)}\,\mathrm{d}u.$$

Both functions are continuous on $[0, 4]$, and $G_n \to G$ pointwise. The constraint (5.44b) implies that $G_n(c_{n,t}) \to \frac{2}{3}$ as $n \to \infty$ and $t \sim T \sim \frac{n^2}{6}$. The function G is strictly decreasing, $G(0) = 1$ and $G(4) = 1/2$; whence it has a unique solution $G(c) = 2/3$, $c \approx 3.164$. By continuity, $c_{n,t} \to c$ whenever $t \sim T$ and $n \to \infty$.

As $c_{n,t} \leq 4$, we have

$$\begin{aligned} z_i^* &\leq \frac{n-1}{2} - \frac{1}{2}\sqrt{(n-1)^2 - 4(i-1)(n-i)} \\ &= \frac{n-1}{2} - \frac{1}{2}\sqrt{(n-2i+1)^2} \\ &= \min\{i-1, n-i\}. \end{aligned}$$

Thus, the sequence $(z_2^*, z_3^*, \ldots, z_{n-1}^*)$ satisfies (5.37b), which shows that it not only the optimal solution to the relaxed programme (5.43), but of the original programme (5.37) as well.

Define $\zeta(u) := 1 - \sqrt{1 - cu(1-u)}$, and note that $z_i^* \approx n\zeta(i/n)$. Let

$$\beta := 2 + 6\int_0^1 \left[uf\left(1 - \frac{\zeta(u)}{2u}\right) + (1-u)f\left(1 - \frac{\zeta(u)}{2(1-u)}\right)\right]\mathrm{d}u.$$

Numerical evaluation gives $\beta \approx 0.654\ldots$. If $t \sim T$, then $\frac{1}{t}\beta_n(t) \sim -\beta$, thus proving (5.42) and hence concluding the proof of the lemma. □

We are now ready to prove Theorem 5.1.3.

Proof of Theorem 5.1.3. Lemma 5.9.7, followed by an application of Lemma 5.9.8, yields

$$\begin{aligned} \max_{(1-\frac{4}{\ln n})T \leq t \leq T} P_n(t) &\leq \max_{(1-\frac{4}{\ln n})T \leq t \leq T} \exp\left(\beta_n(t) + 6n\log n\right) \\ &\leq \exp\left(\beta T + o(T)\right) \qquad \text{as } n \to \infty. \end{aligned}$$

The theorem now follows from an application of Lemma 5.9.1. □

$p(n,3)$ is larger than $s(n,3)$

To close this section, we prove a lower bound on $p(n,3)$ that shows that $p(n,3)$ is asymptotically larger than $s(n,3)$.

Theorem 5.9.9. $\liminf\limits_{n\to\infty} \frac{p(n,3)}{s(n,3)} > 1$.

Proof. Let M be a sparse paving matroid of rank 3 on at least five elements and let $\mathcal{H}$ be its collection of circuit-hyperplanes. Assume that M is not a uniform matroid, so $\mathcal{H} \neq \emptyset$.

Pick a circuit-hyperplane $H \in \mathcal{H}$, and an element $e \notin H$, and set $H' = H \cup \{e\}$. Consider the set system

$$\mathcal{H}' := (\mathcal{H} \cup \{H'\}) \setminus \{X \in \mathcal{H} : |X \cap H'| \geq 2\}.$$

A moment's reflection reveals that $\mathcal{H}'$ is the collection of dependent hyperplanes of a paving matroid that is not sparse. Each sparse paving matroid with k circuit-hyperplanes gives rise to $k(n-3)$ paving matroids in this way. On the other hand, each paving matroid that is obtained in this way can arise from at most $4n^3$ distinct sparse paving matroids, corresponding to the choice of e in the unique hyperplane of size 4, and at most one circuit-hyperplane for each of the three pairs $\{e, x\}$ in that hyperplane.

We claim that for some positive constant c, all but a vanishing fraction of sparse paving matroids of rank 3 on $[n]$ have $k \geq cn^2$. This is an immediate consequence of the observation that the number of sparse paving matroids with at most cn^2 circuit-hyperplanes is at most

$$\sum_{i=0}^{cn^2} \binom{\binom{n}{3}}{i} \leq \left(\frac{\mathrm{e}}{6c}n\right)^{cn^2} = o(s(n,3)),$$

provided c is sufficiently small. This proves the lemma, as

$$\frac{p(n,3)}{s(n,3)} \geq 1 + (1 - o(1))\frac{cn^2(n-3)}{4n^3} \to 1 + \frac{c}{4} > 1 \qquad \text{as } n \to \infty. \quad \square$$

Unfortunately, the argument does not generalise to arbitrary rank: in general it can be shown that an $(1-o(1))$-fraction of sparse paving matroids gives rise to $\Omega\left(n^r\right)$ paving matroids, while the number of sparse paving matroids giving rise to the same paving matroid is $O\left(n^{\binom{r}{2}}\right)$, and these bounds do not compare for $r \geq 4$. However, restricting our attention to sparse paving matroids with more underlying structure, we are able to obtain a more interesting comparison. In particular, if we restrict ourselves to Steiner systems, we obtain the following result (recall that $D(n, r, r-1)$ denotes the number of $S(r-1, r, n)$):

$$p(n,r) \geq \left(1 + \left(\frac{n}{r} - 1\right)\binom{n}{r-1}\right) D(n, r, r-1).$$

This is proved by showing that each $S(n, r, r-1)$ gives rise to $1 + \left(\frac{n}{r} - 1\right)\binom{n}{r-1}$ paving matroids: one of them is sparse, and the others are not. See [PvdP17, Section 6] for details.

CHAPTER 6

Enumeration of matroids

This chapter is based on the journal papers [BPvdP15], which is joint work with Nikhil Bansal and Rudi Pendavingh, and [PvdP15b, PvdP16c], which is joint work with Rudi Pendavingh.

6.1 In this chapter...

This chapter is concerned with the enumeration of matroids, in particular with obtaining bounds on the number $m(n)$ of matroids, and the number $s(n)$ of sparse paving matroids. Combining several results in this chapter, the following bounds on the number of matroids are obtained.

Theorem 6.1.1.

$$\frac{1}{n}\binom{n}{n/2} \leq \log s(n) \sim \log m(n) \leq \frac{2+o(1)}{n}\binom{n}{n/2} \qquad \textit{as } n \to \infty.$$

The lower bound follows from the construction by Graham and Sloane, Lemma 2.8.1, and is included for comparison.

A central role in this chapter is played by the *container method*, which is a technique that can be used to bound the number of stable sets in a graph from above. As sparse paving matroids correspond with stable sets in the Johnson graph, careful analysis of the container method in that special case results in the upper bound on $\log s(n)$ in Theorem 6.1.1.

The situation is more involved for general matroids. Where the nonbases of sparse paving matroids are precisely stable sets in the Johnson graph, nonbases of general matroids are much less restricted. Fortunately, the collection of nonbases of general matroids still has structure. This structure allows us to adapt the container method to general matroids, which leads to the main technical result of this chapter, Theorem 6.6.2.

The theorem itself is too involved to state here, but one of its corollaries is that every matroid (without loops or coloops) can be encoded as a sparse paving matroid and a small amount of additional information. This, in turn, proves the asymptotic equivalence in Theorem 6.1.1.

The results in this chapter are not sufficiently strong to prove that almost every matroid is sparse paving. However, the technical result Theorem 6.6.2 allows us to construct a class of matroids that contains almost every matroid. Essentially generalising the sparse paving matroids, the class is referred to as a 'proxy' for sparse paving matroids, and its structure provides sufficient traction to resolve several of the conjectures mentioned in Chapter 1.

In Section 6.2 and Section 6.3, the container method is introduced, and several constructions of containers are formulated in a general setting. In Section 6.4, these results are specialised to the Johnson graph, which is then used to bound the number of sparse paving matroids in Section 6.5. In Section 6.6, the container method is generalised to matroids, which eventually leads to the proof of Theorem 6.1.1 in Section 6.7. As another consequence of the container method for matroids, in Section 6.8, we construct a proxy for sparse paving matroids, which will be the starting point for the results in the next chapter.

6.2 The container method

The *container method* is a powerful tool for enumerating discrete structures that are essentially stable sets in graphs. The method was conceived by Kleitman and Winston, who used it to enumerate lattices and C_4-free graphs [KW80, KW82]. Throughout the years, similar ideas were used by various authors. Especially in recent years, the container method has developed into a popular tool; see the survey by Samotij [Sam15] for an overview of the method, and a number of historical applications in combinatorics and number theory. Recently, the container method was generalised to hypergraphs by Balogh, Morris, and Samotij [BMS15], and by Saxton and Thomason [ST15].

In this section, we briefly discuss the philosophy behind the container method, before applying the technique in our setting.

Let G be a graph, and suppose that we are interested in $\operatorname{ind}(G)$, the number of stable sets in G. Recall that $\alpha(G)$ is the stability ratio of the graph G, and write $a := \alpha(G)|V(G)|$. As stable sets are closed under taking subsets, we know that

$$2^a \leq \operatorname{ind}(G) \leq \sum_{i=0}^{a} \binom{|V(G)|}{i}. \tag{6.1}$$

The upper bound is fairly naive, and in many situations the lower bound is in fact close to the truth (cf. [Sam15]). Intuitively, the problem is that the upper bound does not take into account that inclusion of v in the stable set rules out $d(v)$ other vertices for inclusion. Therefore, if v is in the stable set, the rest of the stable set can be described as a stable set in a smaller graph, thus improving the upper bound in (6.1). More generally, knowing that a subset $S \subseteq V(G)$ is included in the stable set rules out a large part of the graph, particularly so if the vertices in S share few neighbours. Therefore, if we can associate to each stable set I a set $S \subseteq I$ with the property that $|N(S)|/|S|$ is large, while $|S|$ is small, this should improve the naive upper bound. This line of reasoning is formalised by the container method.

To state a general version of the container method, consider the following asymptotic setting: (G_n) is a sequence of graphs, and we are interested in the asymptotic behaviour of $\operatorname{ind}(G_n)$. Let $a_n := \alpha(G_n)|V(G_n)|$, and suppose that an upper bound $b_n \geq a_n$ is known. The prototypical container result states that, for each n, there is a family $\mathcal{C}_n \subseteq \mathscr{P}(V(G_n))$ of *containers* with the following properties:

(i) $|\mathcal{C}_n| \leq 2^{o(b_n)}$;

(ii) each stable set of G_n is contained in at least one container $C \in \mathcal{C}_n$;

(iii) $\max_{C \in \mathcal{C}_n} |C| \leq (1 + o(1))b_n$.

It is easily seen that (i)–(iii) imply $\log \operatorname{ind}(G_n) \leq (1 + o(1))b_n$ as $n \to \infty$. If $b_n = a_n$, then this bound matches the lower bound in (6.1) up to the $o(a_n)$-term in the exponent.

A typical application of the container method requires two ingredients:

(i) An *upper bound* on the cardinality of a stable set, say $|I| \leq \alpha N$ for all stable sets I, and

(ii) A *supersaturation result*, i.e. a lower bound on the number of edges spanned by any vertex set that is larger than the upper bound αN.

Given the upper bound and supersaturation result, obtaining the container result is mostly a mechanical endeavour, although the computations can be very involved.

6.3 Constructing containers

In this section, we describe two iterative constructions of containers. In the first construction, we construct containers of the form $S \cup A$, where $A = V(G) \setminus (S \cup N(S))$.[1] For all stable sets I, a set S is constructed iteratively, by successively selecting high-degree vertices from I into S. In each step, the degree is controlled by the supersaturation result. The second construction takes the first construction a bit further, by continuing the process until the induced subgraph $G[A]$ has low degree.

The results in this section are formulated in terms of sets K of vertices that are not necessarily stable sets. In Section 6.4, we specialise these results to stable sets, while the more general formulation of the results in this section will be useful in extending the container method to matroids in Section 6.6.

Let G be a graph, and let $\sqsubseteq$ be a linear order on $V(G)$. For $A \subseteq V(G)$, from among the vertices of $G[A]$ of maximum degree, pick v_A^* to be the one that is smallest with respect to $\sqsubseteq$. With respect to the graph G and the linear ordering $\sqsubseteq$, define the functions

$$\mathrm{Iter}_\alpha(S, A, K) = \begin{cases} \big(S,\ A\big) & \text{if } |A| \leq \alpha N, \\ \big(S,\ A \setminus \{v_A^*\}\big) & \text{if } |A| > \alpha N \text{ and } v_A^* \notin K, \\ \big(S \cup \{v_A^*\},\ A \setminus (\{v_A^*\} \cup N(v_A^*))\big) & \\ & \text{if } |A| > \alpha N \text{ and } v_A^* \in K; \end{cases}$$

[1] This notation is borrowed from Alon, Balogh, Morris, and Samotij [ABMS14], who call the vertices in S (resp. A) "selected" (resp. "available").

and, using $\Delta(G)$ for the maximum degree of the graph G,

$$\mathrm{Iter}^{\Delta}(S,A,K)=\begin{cases}\big(S,\ A\big) & \text{if } \Delta(G[A])<\Delta,\\ \big(S,\ A\setminus\{v_A^*\}\big) & \text{if } \Delta(G[A])\geq\Delta \text{ and } v_A^*\notin K,\\ \big(S\cup\{v_A^*\},\ A\setminus(\{v_A^*\}\cup N(v_A^*))\big) & \\ & \text{if } \Delta(G[A])\geq\Delta \text{ and } v_A^*\in K.\end{cases}$$

These functions will be used to construct containers iteratively, but first we establish some of their elementary properties.

Let $\mathrm{Iter}=\mathrm{Iter}_\alpha$ or $\mathrm{Iter}=\mathrm{Iter}^{\Delta}$, and let $K\subseteq V(G)$. Choose a stable set $S_0\subseteq K$ and $A_0\supseteq K\setminus(S_0\cup N(S_0))$, such that $(S_0\cup N(S_0))\cap A_0=\emptyset$. Define recursively

$$(S_{i+1},A_{i+1})=\mathrm{Iter}(S_i,A_i,K)\qquad\text{for all } i\geq 0. \tag{6.2}$$

The pairs (S_i,A_i) will be used to construct containers. The following lemma shows that they approximate the set K.

Lemma 6.3.1. *Let the sequence $(S_i,A_i)_{i=0}^\infty$ be defined as in* (6.2)*. The sequence $(S_i)_{i=0}^\infty$ is monotone increasing, while $(A_i)_{i=0}^\infty$ is monotone decreasing. For each $i\geq 0$,*

(i) S_i is a stable set in G; and

(ii) $S_i\subseteq K\subseteq S_i\cup N(S_i)\cup A_i$;

(iii) $(S_i\cup N(S_i))\cap A_i=\emptyset$.

Moreover, there exists i_0 such that

(iv) $(S_i,A_i)=(S_{i_0},A_{i_0})$ for all $i\geq i_0$.

(v) $S_{i_0}=\bigcup_{i=0}^\infty S_i$ and $A_{i_0}=\bigcap_{i=0}^\infty A_i$.

Proof. By definition of Iter, we have $S_{i+1}\supseteq S_i$ and $A_{i+1}\subseteq A_i$ for all $i\geq 0$. This proves the monotonicity claims. As G has finitely many vertices, monotonicity of $(A_i)_{i=0}^\infty$ in its turn implies that there exists $i_0\geq 0$ such that $A_{i_0+1}=A_{i_0}$, and for such i_0 it is necessarily the case that $S_{i_0+1}=S_{i_0}$ as well. This immediately implies (iv), and combining (iv) with monotonicity implies (v).

Claims (i)–(iii) hold for $i=0$ by assumption. We use induction to show that the claims hold for $i>0$ as well.

So suppose that (i)–(iii) hold for some $i\geq 0$, and consider the pair (S_{i+1},A_{i+1}). If $(S_{i+1},A_{i+1})=(S_i,A_i)$, then there is nothing to prove. So assume that $(S_{i+1},A_{i+1})\neq(S_i,A_i)$, and let $v^*:=v_{A_i}^*$.

If $v^* \notin K$, it is straightforwardly verified that (i)–(iii) hold for $i+1$ as well. If $v^* \in K$, then it follows from (iii) that v^* has no neighbours in S_i, and hence that $S_{i+1} = S_i \cup \{v^*\}$ is a stable set. It is straightforward to verify that (ii) and (iii) hold for $i+1$ as well. □

Define

$$S_\infty := \bigcup_{i=0}^{\infty} S_i, \qquad \text{and} \qquad A_\infty := \bigcup_{i=0}^{\infty} A_i.$$

Lemma 6.3.1(iv) combined with monotonicity imply that the conclusions of Lemma 6.3.1 still hold for the limit point (S_∞, A_∞). The relevance of the introduction of S_∞ and A_∞ lies in the eventual construction of containers as sets of the form $S_\infty \cup A_\infty$.

In the analysis of the sequence $(S_i, A_i)_{i=0}^{\infty}$, we need a method of analysing the structure of the set A. The following lemma, which is taken from [ABMS14, Lemma 3.4], does precisely that for the case that $\text{Iter} = \text{Iter}_\alpha$. In Corollary 6.3.3 below, it gives a lower bound on the number $e(A)$ of edges spanned by $A \subseteq V(G)$, based only on the cardinality of A and properties of G. This is the supersaturation result referred to in Section 6.2.

Lemma 6.3.2. *Let G be a d-regular graph with N vertices and minimum eigenvalue $-\lambda$. For all $A \subseteq V(G)$,*

$$2e(A) \geq |A| \left(\frac{d}{N}|A| - \lambda \frac{N - |A|}{N} \right).$$

Proof. Let B be the adjacency matrix of G, and write $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_N$ for its eigenvalues. Let $b_1, b_2, \ldots, b_N$ be the corresponding eigenvectors, scaled to unit norm. As the matrix B is symmetric, the b_i form an orthonormal basis of $\mathbb{R}^{V(G)}$. As G is d-regular, we know that $\lambda_1 = d$ and $b_1 = \frac{1}{\sqrt{N}}\mathbb{1}$. By assumption, $\lambda_N = -\lambda$.

Let a be the incidence vector of A, i.e. for all $v \in V$, $a_v = 1$ if $v \in A$, and $a_v = 0$ otherwise. The number of edges spanned by A can be expressed in terms of a as $2e(A) = a^\intercal B a$. Write $\alpha_i = a^\intercal b_i$, so that $a = \alpha_1 b_1 + \alpha_2 b_2 + \ldots + \alpha_N b_N$. Note that $\alpha_1^2 = \frac{1}{N}(a^\intercal \mathbb{1})^2 = \frac{|A|^2}{N}$, while $\sum_{i=1}^{N} \alpha_i^2 = a^\intercal a = |A|$. As $B b_i = \lambda_i b_i$, we obtain

$$\begin{aligned} 2e(A) = a^\intercal B a &= a^\intercal \left(\alpha_1 \lambda_1 b_1 + \alpha_2 \lambda_2 b_2 + \ldots + \alpha_N \lambda_N b_N \right) \\ &= \alpha_1^2 \lambda_1 + \alpha_2^2 \lambda_2 + \ldots + \alpha_N^2 \lambda_N \\ &\geq d\alpha_1^2 + \lambda_N \sum_{i=2}^{N} \alpha_i^2 \\ &= \frac{d|A|^2}{N} - \lambda \left(|A| - \frac{|A|^2}{N} \right), \end{aligned}$$

which proves the lemma. □

Corollary 6.3.3. *Let G be a d-regular graph $()d > 0)$ with N vertices and minimum eigenvalue $-\lambda$. Let $\alpha := \frac{\lambda}{d+\lambda}$. For any $\varepsilon > 0$, if $A \subseteq V(G)$ with $|A| \geq (\alpha + \varepsilon)N$, then $\Delta(G[A]) \geq \varepsilon(d + \lambda)$.*

Proof. Let $A \subseteq V(G)$ be a set of cardinality $(\alpha + \varepsilon')N$, so that $\varepsilon' \geq \varepsilon$. The average degree in $G[A]$ is $\frac{2e(A)}{|A|}$, which, by Lemma 6.3.2, is at least

$$\frac{d+\lambda}{N}|A| - \lambda = \varepsilon'(d+\lambda) \geq \varepsilon(d+\lambda).$$

In particular, $G[A]$ contains a vertex of degree at least $\varepsilon(d + \lambda)$, and so $\Delta G[A] \geq \varepsilon(d + \lambda)$. □

Remark 6.3.4. The lower bound in Lemma 6.3.2 is a one-sided version of a result that appeared in [AC88, Lemma 2.3], and earlier in [Hae79, Theorem 2.1.4(i)]. The two-sided result states that if G is a d-regular graph with N vertices such that each eigenvalue that is not equal to d is bounded in absolute value by μ, then

$$\left| e(A) - \frac{d|A|^2}{2N} \right| \leq \frac{1}{2}\mu\frac{|A|(N-|A|)}{N}. \tag{6.3}$$

The expected number of edges spanned by the set A in a random d-regular graph is roughly $\frac{d|A|^2}{2N}$. The result shows that μ controls the concentration of $e(A)$ as A ranges over all subsets of given cardinality.

The bounds in (6.3) are a specialisation of the Expander Mixing Lemma, which gives a similar bound on the number of edges between any pair of vertex sets $A, A' \subseteq V(G)$.

The bound in Corollary 6.3.3 implies that every set of vertices of cardinality strictly larger than αN spans at least one edge, and so $\alpha(G) \leq \frac{\lambda}{d+\lambda}$. This result is known as the *Hoffman bound* [Hof70]. □

The following lemma contains the main technical analysis of the pair (S_∞, A_∞) if the sequence $(S_i, A_i)_{i=0}^{\infty}$ is defined using Iter $=$ Iter$_\alpha$.

Lemma 6.3.5. *Let G be a d-regular graph, $d > 0$, with smallest eigenvalue $-\lambda$. Define $\alpha := \frac{\lambda}{d+\lambda}$ and $\sigma := \frac{\ln(d+1)}{d+\lambda}$. Let the sequence $(S_i, A_i)_{i=0}^{\infty}$ be defined as in (6.2) with Iter $=$ Iter$_\alpha$. Then $|A_\infty| \leq \alpha N$, and $|S_\infty \setminus S_0| \leq \lceil \sigma N \rceil$. Moreover, if $A_\infty = A_0$, then $S_\infty = S_0$. Otherwise, if i^* is the largest index i such that $A_i \neq A_\infty$, and $v^*_{A_{i^*}}$ has degree at least D in $G[A_{i^*}]$, then $|S_\infty \setminus S_0| \leq \lceil \sigma(D)N \rceil$, where $\sigma(D) := \frac{1}{d+\lambda}\left(\frac{D-1}{D+1} + \ln\frac{d+1}{D+1}\right)$.*

Proof. Let us first prove the bound on $|A_\infty|$. By Lemma 6.3.1(iv), there is $i_0 \geq 0$ such that $(S_{i_0}, A_{i_0}) = (S_{i_0+1}, A_{i_0+1})$, and $A_\infty = A_{i_0}$. It follows that $(S_{i_0}, A_{i_0}) = \mathrm{Iter}_\alpha(S_{i_0}, A_{i_0}, K)$, which implies that $|A_\infty| = |A_{i_0}| \leq \alpha N$.

If $i_0 = 0$, then $S_\infty = S_0$ as well, and we are done. For the remainder of the proof we may assume that $i_0 > 0$.

The bound on $|S_\infty \setminus S_0|$ requires a little more work. We partition the index set $\{i : i \geq 1\}$ into phases, and estimate the growth of S_i in each phase separately. Say that the index i is in phase $j \in [d]$ if

$$\frac{|A_i|}{N} \in \left(\alpha + \frac{j-1}{d+\lambda}, \alpha + \frac{j}{d+\lambda}\right],$$

and that i is in phase 0 if $\frac{|A_i|}{N} \leq \alpha$. It is easily verified that the phase of each i is well-defined, and that the phase is decreasing in i. Define $s(j)$ as the number of phase-j indices i for which $S_{i+1} \supsetneq S_i$. By definition, $s(0) = 0$, and $|S_\infty \setminus S_0| = \sum_{j=1}^{d} s(j)$.

Let $v_i^* := v_{A_i}^*$. By construction, if $S_{i+1} = S_i \cup \{v_i^*\}$, then $A_{i+1} = A_i \setminus (\{v_i^*\} \cup N(v_i^*))$. If index i is in phase j, then $|A_i|/N = \alpha + \varepsilon$ for some $\varepsilon > \frac{j-1}{d+\lambda}$. In that case it follows from Corollary 6.3.3 that $\Delta(G[A_i]) > j - 1$, and hence $|A_i \cap (\{v_i^*\} \cup N(v_i^*))| \geq j + 1$. Thus, each time S_i increases during phase j, at least $j + 1$ vertices are removed from the set A_i. It follows that $s(j) \leq \left\lceil \frac{1}{(d+\lambda)(j+1)} N \right\rceil$, and hence

$$\sum_{j=1}^{d} s(j) \leq \frac{1}{d+\lambda} N \sum_{j=1}^{d} \frac{1}{j+1} + d \leq \frac{\ln(d+1)}{d+\lambda} N + d.$$

The upper bound can be sharpened slightly by a more refined analysis. For each phase j, let $i(j)$ be smallest index i such that $\frac{|A_i|}{N} \leq \alpha + \frac{j}{d+\lambda}$; let u_j satisfy $|A_{i(j)}| = \left(\alpha + \frac{j}{d+\lambda}\right) N - u_j$; and define $D(j) = \Delta(G[A_{i(j-1)-1}])$ for all $j \in [d]$. Note that $u_d = 0$, $0 \leq u_j < D(j+1) + 1$, $D(j) \geq j$, and $D(j) \geq D(j-1)$.

If index i is in phase j, then

$$\left(\alpha + \frac{j-1}{d+\lambda}\right) N - u_{j-1} < |A_i| \leq \left(\alpha + \frac{j}{d+\lambda}\right) N - u_j,$$

from which we obtain the refined bound

$$s(j) \leq \frac{1}{(d+\lambda)(D(j)+1)} N + \frac{u_{j-1} - u_j}{D(j)+1}.$$

Thus,

$$\begin{aligned}\sum_{j=1}^{d} s(j) &\leq \frac{1}{d+\lambda} N \sum_{j=1}^{d} \frac{1}{D(j)+1} + \sum_{j=1}^{d} \frac{u_{j-1}-u_j}{D(j)+1} \\ &\leq \frac{1}{d+\lambda} N \sum_{j=1}^{d} \frac{1}{j+1} + \frac{u_0}{D(1)+1} < \frac{\ln(d+1)}{d+\lambda} N + 1, \qquad (6.4)\end{aligned}$$

and hence $|S_\infty \setminus S_0| \leq \lceil \sigma N \rceil$. Moreover, writing $i^* = i(0) - 1$, if $v^*_{A_{i^*}}$ has degree at least D in $G[A_{i^*}]$, then $D(1) \geq D$, and hence $D(j) \geq D$ for all $j \geq 1$. Thus, (6.4) can be replaced by the stronger bound

$$\begin{aligned}\sum_{j=1}^{d} s(j) &\leq \frac{1}{d+\lambda} N \sum_{j=1}^{d} \frac{1}{\max\{D,j\}+1} + \frac{u_0}{D(1)+1} \\ &< \frac{1}{d+\lambda} N \left(\frac{D-1}{D+1} + \sum_{j=D}^{d} \frac{1}{j+1} \right) + 1 \\ &\leq \frac{1}{d+\lambda} N \left(\frac{D-1}{D+1} + \ln \frac{d+1}{D+1} \right) + 1,\end{aligned}$$

which proves the final claim. □

We are now ready to formulate the first container result of this section.

Theorem 6.3.6. *Let G be a d-regular graph, $d > 0$, on N vertices, with minimum eigenvalue $-\lambda$. Let $\alpha := \frac{\lambda}{d+\lambda}$, and $\sigma := \frac{\ln(d+1)}{d+\lambda}$. Let $\mathfrak{S} := \mathrm{Ind}(G, \leq \lceil \sigma N \rceil)$ and $\mathfrak{A} := \binom{V(G)}{\leq \alpha N}$. There exist functions $\varphi\colon \mathscr{P}(V(G)) \to \mathfrak{S}$ and $\psi\colon \mathfrak{S} \to \mathfrak{A}$ such that*

$$\varphi(K) \subseteq K \subseteq \varphi(K) \cup N(\varphi(K)) \cup \psi(\varphi(K)) \qquad (6.5)$$

for all $K \subseteq V(G)$.

Proof. Fix a linear order on $V(G)$. For given $K \subseteq V(G)$, define the sequence $(S_i, A_i)_{i=0}^{\infty}$ by $S_0 = \emptyset$, $A_0 = V(G)$, and then iteratively

$$(S_{i+1}, A_{i+1}) = \mathrm{Iter}_\alpha(S_i, A_i, K) \qquad \text{for all } i \geq 0.$$

Define $\varphi(K) := S_\infty(K)$ and $\psi(\varphi(K)) := A_\infty(K)$.[2] By Lemma 6.3.5, $\varphi(K)$ has cardinality at most $\lceil \sigma N \rceil$, while $\psi(\varphi(K)) \in \mathfrak{A}$; in addition, Lemma 6.3.1(i) implies that $\varphi(K)$ is a stable set, and hence $\varphi(K) \in \mathfrak{S}$.

[2] Strictly speaking, this only constructs a *partial* function ψ, but this partial function can be arbitrarily extended to a function.

Finally, by Lemma 6.3.1(ii), $S_i \subseteq K \subseteq S_i \cup N(S_i) \cup A_i$ for all K and all i, and by Lemma 6.3.1(iv), the same holds in the limit $i = \infty$. This proves (6.5), and hence concludes the proof of the theorem. □

Next, we consider the second construction, which uses Iter^{Δ} in addition to Iter_{α}. The second construction is used to control the maximum degree in $G[A_\infty]$.

Lemma 6.3.7. *Let the sequence $(S_i, A_i)_{i=0}^{\infty}$ be defined as in* (6.2) *with Iter $=$ Iter$^{\Delta}$. Then $\Delta(G[A_\infty]) < \Delta$, and $|S_\infty \setminus S_0| \leq \frac{|A_0|}{\Delta}$.*

Proof. Let us first prove the bound on $\Delta(G[A_\infty])$. By Lemma 6.3.1(iv), there is $i_0 \geq 0$ such that $(S_{i_0}, A_{i_0}) = (S_{i_0+1}, A_{i_0+1})$, and $A_\infty = A_{i_0}$. It follows that $(S_{i_0}, A_{i_0}) = \text{Iter}^{\Delta}(S_{i_0}, A_{i_0}, K)$, which in turn implies that $\Delta(G[A_\infty]) = \Delta(G[A_{i_0}]) < \Delta$. To prove the bound on $|S_\infty \setminus S_0|$, note that if $S_{i+1} = S_i \cup \left\{v^*_{A_i}\right\}$, then $v^*_{A_i}$ has degree $\Delta G[A_i] \geq \Delta$ in $G[A_i]$, so $A_{i+1} = A_i \setminus \left(\{v^*_{A_i}\} \cup N(v^*_{A_i})\right)$ is obtained by removing at least $\Delta + 1$ elements from A_i. This can happen for at most $|A_0|/\Delta$ indices i before $A_i = \emptyset$. □

Lemma 6.3.7 allows us to prove a variant of Theorem 6.3.6 in which $\mathfrak{A}$ is restricted to those A for which $\Delta(G[A])$ is small, at the expense of increasing $\mathfrak{S}$.

Theorem 6.3.8. *Let G be a d-regular graph, $d > 0$, on N vertices, with smallest eigenvalue $-\lambda$, and let $\Delta > 0$. Let $\alpha := \frac{\lambda}{d+\lambda}$, and $\sigma := \frac{\ln(d+1)}{d+\lambda} + \frac{\alpha}{\Delta}$. Let $\mathfrak{S} := \text{Ind}(G, \leq \lceil \sigma N \rceil)$ and $\mathfrak{A} := \left\{ A \in \binom{V(G)}{\leq \alpha N} : \Delta(G[A]) < \Delta \right\}$. There exist functions $\varphi : \mathscr{P}(V(G)) \to \mathfrak{S}$ and $\psi \colon \mathfrak{S} \to \mathfrak{A}$ such that*

$$\varphi(K) \subseteq K \subseteq \varphi(K) \cup N(\varphi(K)) \cup \psi(\varphi(K)) \tag{6.6}$$

for all $K \subseteq V(G)$.

Proof. Let functions φ' and ψ' be as in the statement of Theorem 6.3.6. Fix a linear order on $V(G)$. Given $K \subseteq V(G)$, define the sequence $(S_i, A_i)_{i=0}^{\infty}$ by putting $S_0 = \varphi'(K)$, $A_0 = \psi'(\varphi'(K))$, and then iteratively

$$(S_{i+1}, A_{i+1}) = \text{Iter}^{\Delta}(S_i, A_i, K) \qquad \text{for all } i \geq 0.$$

Define $\varphi(K) = \varphi'(K) \cup S_\infty(K)$ and $\psi(\varphi(K)) := A_\infty(K)$.[3] By Lemma 6.3.7, $\Delta G[A_\infty] < \Delta$, while $|S_\infty \setminus S_0| \leq \frac{\alpha N}{\Delta}$. From the latter observation, it follows that $|S_\infty| = |S_0| + |S_\infty \setminus S_0| < \frac{\ln(d+1)}{d+\lambda} N + 1 + \frac{\alpha}{\Delta} N$.

[3] As in the proof of Theorem 6.3.6, this only constructs a *partial* function ψ, but as before it can be arbitrarily extended to a function.

Lemma 6.3.1 shows that S_∞ is a stable set in G, and that (6.6) holds. These observations imply the theorem. □

The value of σ in Theorem 6.3.8 is obtained by combining the worst-case bounds from Lemma 6.3.5 and Lemma 6.3.7. A slightly better bound can be obtained by a more careful analysis.

Theorem 6.3.9. *Let G be a d-regular graph, $d > 0$, on N vertices, with smallest eigenvalue $-\lambda$, and let $\Delta > 0$. Let $\alpha := \frac{\lambda}{d+\lambda}$, and $\sigma := \max_{D \in [d]} \sigma(D)$, where*

$$\sigma(D) := \begin{cases} \frac{\frac{D-1}{D+1} + \ln\left(\frac{d+2}{D+1}\right)}{d+\lambda} + \frac{\alpha}{\Delta} & \textit{if } D \geq \Delta, \\ \frac{\frac{D-1}{D+1} + \ln\left(\frac{d+2}{D+1}\right)}{d+\lambda} & \textit{otherwise.} \end{cases}$$

Let $\mathfrak{S} := \operatorname{Ind}(G, \leq \lceil \sigma N \rceil)$ and $\mathfrak{A} := \left\{ A \in \binom{V(G)}{\leq \alpha N} : \Delta G[A] < \Delta \right\}$. There exist functions $\varphi\colon \mathscr{P}(V(G)) \to \mathfrak{S}$ and $\psi\colon \mathfrak{S} \to \mathfrak{A}$ such that

$$\varphi(K) \subseteq K \subseteq \varphi(K) \cup N(\varphi(K)) \cup \psi(\varphi(K)) \tag{6.7}$$

and

$$(\varphi(K) \cup N(\varphi(K))) \cap \psi(\varphi(K)) = \emptyset \tag{6.8}$$

for all $K \subseteq V(G)$.

Proof. Fix a linear order on $V(G)$. Pick a set $K \subseteq V(G)$. Define the sequence $(S_i, A_i)_{i=0}^{\infty}$ by $S_0 = \emptyset$, $A_0 = V(G)$, and then iteratively

$$(S_{i+1}, A_{i+1}) = \operatorname{Iter}_\alpha(S_i, A_i, K) \qquad \text{for all } i \geq 0.$$

In addition, define the sequence $(S'_i, A'_i)_{i=0}^{\infty}$ by $S'_0 = S_\infty$, $A'_0 = A_\infty$, and then iteratively

$$(S'_{i+1}, A'_{i+1}) = \operatorname{Iter}^\Delta(S'_i, A'_i, K) \qquad \text{for all } i \geq 0.$$

Define $\varphi(K) := S'_\infty$, and $\psi(\varphi(K)) := A'_\infty$. Properties (6.7)–(6.8) hold by Lemma 6.3.1.

Let i^* be the largest index i such that $A_i \neq A_\infty$. If no such i exists, put $D = d$, otherwise put $D = \Delta G[A_{i^*}]$. By Lemma 6.3.5,

$$|S_\infty| < \frac{1}{d+\lambda} \left(\frac{D-1}{D+1} + \ln \frac{d+1}{D+1} \right) N + 1. \tag{6.9}$$

In addition, by Lemma 6.3.7,

$$|S'_\infty \setminus S'_0| \leq \begin{cases} 0 & \text{if } D < \Delta \\ \frac{\alpha}{\Delta} N & \text{if } D \geq \Delta. \end{cases} \tag{6.10}$$

If follows from (6.9)–(6.10) that

$$|\varphi(K)| = |S'_\infty| = |S'_\infty \setminus S_\infty| + |S_\infty| \leq \lceil \sigma(D)N \rceil\,, \tag{6.11}$$

and the bound on $|\varphi(K)|$ is obtained by maximising the right-hand side of (6.11) with respect to D. Moreover, by Lemma 6.3.1, S_∞ and S'_∞ are stable sets in G, while Lemma 6.3.5 and Lemma 6.3.7 imply that $A'_\infty \in \mathfrak{A}$. □

6.4 Enumeration of stable sets

In this section, Theorem 6.3.6, which was formulated in terms of general vertex sets K, is specialised to stable sets. This specialisation results in a bound on the number of stable sets in regular graphs.

Theorem 6.4.1. *Let G be a d-regular graph on N vertices, with smallest eigenvalue $-\lambda$. Let $\alpha := \frac{\lambda}{d+\lambda}$ and $\sigma := \frac{\ln(d+1)}{d+\lambda}$, and write $\mathfrak{S} := \mathrm{Ind}(G, \leq \lceil \sigma N \rceil)$ and $\mathfrak{A} := \binom{V(G)}{\leq \alpha N}$. There exist functions $\varphi\colon \mathrm{Ind}(G) \to \mathfrak{S}$ and $\psi\colon \mathfrak{S} \to \mathfrak{A}$ such that*

$$\varphi(I) \subseteq I \subseteq \varphi(I) \cup \psi(\varphi(I))$$

for all $I \in \mathrm{Ind}(G)$.

Proof. Obtain φ' and ψ by applying Theorem 6.3.6, and define φ as the restriction of φ' to $\mathrm{Ind}(G)$. We have

$$\varphi(I) \subseteq I \subseteq \varphi(I) \cup N(\varphi(I)) \cup \psi(\varphi(I)),$$

and as I is a stable set containing $\varphi(I)$, it follows that $I \cap N(\varphi(I)) = \emptyset$. □

Recall that $\mathrm{ind}(G)$ denotes the number of stable sets in G. In addition, write $\mathrm{ind}(G, \leq k)$ for the number of stable sets of cardinality at most k in G.

Corollary 6.4.2. *Let G be a d-regular graph on N vertices, with smallest eigenvalue $-\lambda$. Let $\alpha := \frac{\lambda}{d+\lambda}$ and $\sigma := \frac{\ln(d+1)}{d+\lambda}$. For all $k \in \mathbb{Z}_n$, the number of stable sets satisfies*

$$\mathrm{ind}(G, \leq k) \leq \sum_{i=0}^{\lceil \sigma N \rceil} \binom{N}{i} \times \sum_{j=0}^{k} \binom{\lfloor \alpha N \rfloor}{j},$$

while

$$\operatorname{ind}(G) \le \sum_{i=0}^{\lceil \sigma N \rceil} \binom{N}{i} \times 2^{\alpha N}.$$

Proof. We start by proving the first inequality. Suppose that I is a stable set of cardinality at most k.

Let φ and ψ be functions as in Theorem 6.4.1. Each independent set I is determined by the pair $(\varphi(I), I \cap \psi(\varphi(I)))$. As $|\varphi(I)| \le \lceil \sigma N \rceil$, $\varphi(I)$ can be chosen in at most $\sum_{i=0}^{\lceil \sigma N \rceil} \binom{N}{i}$ ways.

After choosing $\varphi(I)$, we need to specify $I \cap \psi(\varphi(I))$ as a subset of $\psi(\varphi(I))$. As $|I \cap \psi(\varphi(I))| \le k$, and $\psi(\varphi(I))$ is a set of cardinality at most αN, there are at most $\sum_{j=0}^{k} \binom{\lfloor \alpha N \rfloor}{j}$ possibilities for $I \cap \psi(\varphi(I))$. This proves the first inequality. The second inequality follows since $\operatorname{ind}(G) = \operatorname{ind}(G, \le \lfloor \alpha N \rfloor)$, and $\sum_{j=0}^{n} \binom{n}{j} = 2^n$. □

6.5 Enumeration of sparse paving matroids

Recall from Lemma 2.7.1 that whenever $0 < r < n$, sparse paving matroids of rank r on ground set $[n]$ are in one-to-one correspondence with stable sets in the Johnson graph $J(n, r)$. In particular, this implies

$$s(n, r) = \operatorname{ind}(J(n, r)) \qquad \text{for all } 0 < r < n. \tag{6.12}$$

As $J(n, r)$ is regular of degree $r(n - r) > 0$, we may use Corollary 6.4.2 to obtain an upper bound on $s(n, r)$. It follows from Proposition 2.6.2 that the smallest eigenvalue of $J(n, r)$ is $-\lambda_{n,r}$, with $\lambda_{n,r} := \min\{r, n - r\}$. Let us write

$$\sigma_{n,r} := \frac{\ln(r(n-r)+1)}{r(n-r) + \min\{r, n-r\}} \text{ and } \alpha_{n,r} := \frac{\min\{r, n-r\}}{r(n-r) + \min\{r, n-r\}}.$$

Thus, if σ and α are the two constants that arise in the application of Corollary 6.4.2 to $J(n, r)$, then

$$\sigma = \sigma_{n,r}, \quad \alpha = \alpha_{n,r},$$

and moreover, if σ is the constant that arises in the application of Theorem 6.3.9 with $\Delta = \lambda_{n,r}$, then $\sigma = \sigma(1) \le \sigma_{n,r}$ as well.

Note that $\alpha_{n,r} = \alpha_{n,n-r}$, and $\sigma_{n,r} = \sigma_{n,n-r}$; and if $r \le n/2$, then $\alpha_{n,r} = \frac{1}{n-r+1}$, and $\sigma_{n,r} = \frac{\ln(r(n-r)+1)}{r(n-r+1)}$. Specialising Corollary 6.4.2 to

$J(n,r)$, it follows from (6.12) that

$$s(n,r) \leq \exp_2\left(\alpha_{n,r}\binom{n}{r}\right) \times \sum_{i=0}^{\lceil \sigma_{n,r}\binom{n}{r}\rceil} \binom{\binom{n}{r}}{i}. \tag{6.13}$$

The following lemma provides useful bounds on $\sigma_{n,r}$ and $\alpha_{n,r}$.

Lemma 6.5.1. *For all* $0 < r < n$,

(i) $\lceil \sigma_{n,r}\binom{n}{r}\rceil \leq \frac{9 \ln n}{n^2}\binom{n}{n/2}$; *and*

(ii) $\alpha_{n,r}\binom{n}{r} \leq \frac{2}{n}\binom{n}{n/2}$.

Proof. Define

$$f(n,r) := \frac{2 \ln n}{r(n-r)}\binom{n}{r}.$$

Note that $f(n, n-r) = f(n,r)$, and $\sigma_{n,r}\binom{n}{r} + 1 \leq f(n,r)$. A calculation reveals that $f(n, r-1) \leq f(n,r)$ whenever $1 < r \leq \lfloor n/2 \rfloor$. Hence

$$\left\lceil \sigma_{n,r}\binom{n}{r}\right\rceil \leq f(n,r) \leq f(n, \lfloor n/2 \rfloor) \leq \frac{9\ln(n)}{n^2}\binom{n}{n/2}$$

whenever $0 < r < n$, as required. The bound $\alpha_{n,r} \leq 2/n$ is trivial, and (ii) follows from the inequality $\binom{n}{r} \leq \binom{n}{n/2}$. □

The lemma provides the necessary ingredient to analyse (6.13), and we obtain the following bound on the number of sparse paving matroids.

Theorem 6.5.2. $\log s(n) \leq \frac{2+o(1)}{n}\binom{n}{n/2}$ *as* $n \to \infty$.

Proof. We use that $s(n) = \sum\limits_{r=0}^{n} s(n,r)$, and hence

$$s(n) \leq (n+1) \max_{0 \leq r \leq n} s(n,r).$$

Note that $s(n,0) = s(n,n) = 1$. The remainder of the proof is devoted to bounding $s(n,r)$ for $0 < r < n$, the starting point for which is the inequality (6.13).

We bound the two factors on the right-hand side of (6.13) separately. First, a direct application of Lemma 6.5.1(ii) shows that

$$\exp_2\left(\alpha_{n,r}\binom{n}{r}\right) \leq \exp_2\left(\frac{2}{n}\binom{n}{n/2}\right). \tag{6.14}$$

Second, as $\binom{n}{r} \leq \binom{n}{n/2}$, and $m \mapsto \binom{m}{i}$ is nondecreasing, we can write

$$\sum_{i=0}^{\lceil \sigma_{n,r}\binom{n}{r}\rceil} \binom{\binom{n}{r}}{i} \leq \sum_{i=0}^{\lceil \sigma_{n,r}\binom{n}{r}\rceil} \binom{\binom{n}{n/2}}{i} \leq \sum_{i=0}^{\frac{9\ln(n)}{n^2}\binom{n}{n/2}} \binom{\binom{n}{n/2}}{i}, \tag{6.15}$$

where the second inequality follows from Lemma 6.5.1(i). Assume that n is so large that $\frac{9\ln n}{n^2} \leq \frac{1}{2}$. The right-hand side of (6.15) does not depend on r, and bounding the sum of binomial coefficients yields

$$\begin{aligned}\sum_{i=0}^{\lfloor \frac{9\ln(n)}{n^2}\binom{n}{n/2}\rfloor} \binom{\binom{n}{n/2}}{i} &\leq \left(\frac{\mathrm{e}n^2}{9\ln n}\right)^{\frac{9\ln n}{n^2}\binom{n}{n/2}} \\ &= \exp_2\left(O\left(\frac{\ln^2 n}{n^2}\binom{n}{n/2}\right)\right). \end{aligned}\tag{6.16}$$

Using (6.14) and (6.16) to bound the right-hand side of (6.13), we obtain

$$\max_{1\leq r\leq n-1} s(n,r) \leq \exp_2\left(\frac{2}{n}\binom{n}{n/2} + O\left(\frac{\ln^2 n}{n^2}\binom{n}{n/2}\right)\right),$$

and therefore

$$\log s(n) \leq \log(n+1) + \frac{2}{n}\binom{n}{n/2} + O\left(\frac{\ln^2 n}{n^2}\binom{n}{n/2}\right),$$

which concludes the proof. □

Using a similar argument, a bound on the number of sparse paving matroids with few circuit-hyperplanes (or equivalently, the number of small stable sets in $J(n,r)$) can be obtained. We record the following result for later use.

Lemma 6.5.3. *For every* $0 \leq \lambda \leq 1$,

$$\max_{0\leq r\leq n} \log \operatorname{ind}\left(J(n,r), \leq \frac{\lambda}{n}\binom{n}{r}\right) \leq \left(2\mathscr{H}\left(\frac{\lambda}{2}\right) + o(1)\right)\log s(n),$$

and for every $0 \leq \lambda \leq 1/2$

$$\max_{0\leq r\leq n} \log \operatorname{ind}(J(n,r), \leq \lambda \log s(n)) \leq (2\mathscr{H}(\lambda) + o(1))\log s(n).$$

Proof. We prove the first claim; the second claim can be proved using a similar argument. Fix n and r, and let $N := \binom{n}{r}$. Without loss of generality, we may assume that $r \leq n/2$. By Corollary 6.4.2,

$$\log \operatorname{ind}\left(J(n,r), \leq \frac{\lambda}{n}N\right) \leq \log \sum_{i=0}^{\lceil \sigma_{n,r}N \rceil} \binom{N}{i} + \log \sum_{i=0}^{\lfloor \frac{\lambda}{n}N \rfloor} \binom{\lfloor \alpha_{n,r}N \rfloor}{i}. \tag{6.17}$$

The first term on the right-hand side is increasing in N and $\sigma_{n,r}N$. Using Lemma 6.5.1(i) to bound $\sigma_{n,r}N$, we obtain

$$\log \sum_{i=0}^{\lceil \sigma_{n,r}N \rceil} \binom{N}{i} \leq \frac{9 \ln n}{n^2} \log\left(\frac{en^2}{9 \ln n}\right) \binom{n}{n/2}. \tag{6.18}$$

The second term on the right-hand side of (6.17) is increasing in N and $\alpha_{n,r}N$. Using Lemma 6.5.1(ii) to bound $\alpha_{n,r}N$, we obtain

$$\log \sum_{i=0}^{\lfloor \frac{\lambda}{n}N \rfloor} \binom{\lfloor \alpha_{n,r}N \rfloor}{i} \leq \mathscr{H}\left(\frac{\lambda}{2}\right) \frac{2}{n} \binom{n}{n/2}. \tag{6.19}$$

Substituting (6.18)–(6.19) into (6.17), we obtain

$$\max_{0 \leq r \leq n} \log \operatorname{ind}\left(J(n,r), \leq \frac{\lambda}{n}\binom{n}{r}\right) \leq \frac{2\mathscr{H}\left(\frac{\lambda}{2}\right) + o(1)}{n} \binom{n}{n/2}.$$

The desired result follows since $\log s(n) \geq \frac{1}{n}\binom{n}{n/2}$. □

6.6 Adapting the container method to matroids

Suppose that φ and ψ arise from an application of the container method to $J(n,r)$ and $\mathcal{K}$ is the collection of nonbases of a matroid $M \in \mathbb{M}(n,r)$. By Theorem 6.3.6,

$$\varphi(\mathcal{K}) \subseteq \mathcal{K} \subseteq \varphi(\mathcal{K}) \cup N(\varphi(\mathcal{K})) \cup \psi(\varphi(\mathcal{K})).$$

If M is sparse paving, then $\mathcal{K} \cap N(\varphi(\mathcal{K})) = \emptyset$. This observation condenses the description of $\mathcal{K}$, and eventually leads to the upper bound on $\log s(n)$ in Theorem 6.5.2. On the other hand, if M is a general matroid, then $\mathcal{K} \cap N(\varphi(\mathcal{K}))$ is not necessarily empty. As $N(\varphi(\mathcal{K}))$ is potentially huge, describing the nonbases among the sets in $N(\varphi(\mathcal{K}))$ will inflate the bound on $\log m(n)$ dramatically. This problem is addressed in Theorem 6.6.2 below, which is obtained by extending the container argument from the previous sections in two ways.

First, it employs the local covers from Chapter 4 to describe the nonbases among $N(\varphi(\mathcal{K}))$. Each r-set that is selected into $\varphi(\mathcal{K})$ is a nonbasis, and hence admits a small local cover. This allows for a concise description of the nonbases among $N(\varphi(\mathcal{K}))$.

The second extension also uses that the nonbases of a matroid are a highly structured set. In particular, if X is a dependent set, then the nonbases among $N(X)$ can be recovered from only a partial enumeration of these nonbases. We use two elementary properties of matroids.

The first is Lemma 2.6.4, which states that if $X \in \binom{E}{r}$ is a set of rank $r-1$, then it contains a unique circuit C, it avoids a unique cocircuit D, and the dependent neighbours of X are identified by

$$\begin{aligned}\mathcal{K}(M) \cap N(X)&\\ &= \Big\{ (X \setminus \{e\}) \cup \{f\} : e \in X \setminus C \text{ or } f \in (E \setminus X) \setminus D \Big\}. \quad (6.20)\end{aligned}$$

We apply (6.20) iteratively. Suppose that for a large fraction of the vertices Y in $J(n,r)$, it is known whether Y is dependent or independent. Now we add the information that X is dependent. Using (6.20), we may sometimes infer that some of the neighbours of X (whose status thus far was not known) are dependent as well. This may start a cascade effect, as subsequently we may infer that some of their neighbours are dependent as well, and so on.

Recall that the neighbourhood of X is partitioned into 'rows',

$$R_X(e) := \{X \triangle \{e,f\} : f \in E \setminus X\}, \qquad e \in X,$$

and also into 'columns',

$$C_X(f) := \{X \triangle \{e,f\} : e \in X\}, \qquad f \in E \setminus X.$$

The second property is the following.

Lemma 6.6.1. *Let M be a matroid of rank r on ground set E that does not have any loops and coloops. Let $X \in \binom{E}{r}$. If*

- *there exists $e \in X$ such that $R_X(e) \subseteq \mathcal{K}(M)$; or*
- *there exists $f \in E \setminus X$ such that $C_X(f) \subseteq \mathcal{K}(M)$,*

then $X \in \mathcal{K}(M)$.

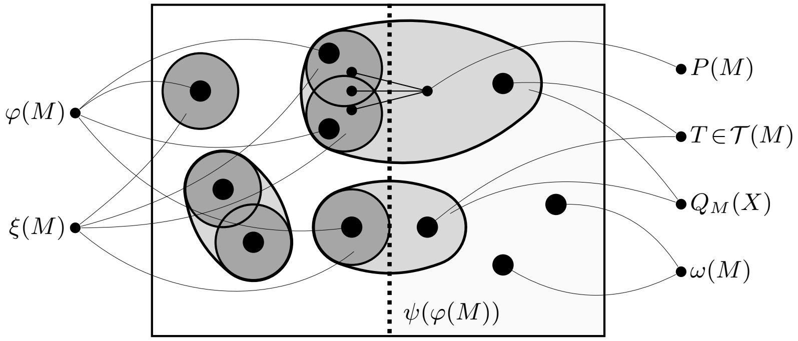


Figure 6.1: Schematic depiction of the sets mentioned in Theorem 6.6.2.

Proof. Let $e \in X$ and $f \in E \setminus X$ be as in the statement of the lemma, and suppose to the contrary that X is a basis of M. As $R_X(e) \subseteq \mathcal{K}(M)$, $f' \in \mathrm{cl}(X \setminus \{e\})$ for all $f' \in E \setminus X$. It follows that e is in every basis, and hence that e is a coloop: a contradiction. From $C_X(f) \subseteq \mathcal{K}(M)$ it follows similarly that f is a loop. □

Let

$$\widetilde{\mathbb{M}}(n,r) := \{M \in \mathbb{M}(n,r) : M \text{ has no loops or coloops}\}.$$

If $\mathcal{X}$ is a collection of non-empty sets, then a *choice function* on $\mathcal{X}$ is a function $\mathrm{ch}\colon \mathcal{X} \to \bigcup \mathcal{X}$, such that $\mathrm{ch}(X) \in X$ for all $X \in \mathcal{X}$.

We are now ready to prove the main technical result of this chapter. The theorem below shows that matroids without loops and coloops either have a compact description, or a large number of alternative descriptions.

Its rather technical formulation consists of two parts, that are perhaps easier to grasp separately. Items (i)–(iv) incorporate local covers into the standard container method, thus generalising the container method for sparse paving matroids to general matroids. Next, items (v)–(viii) make the second extension explicit. This breakdown into two parts reflects the historical development of the theorem: items (i)–(iv) appeared in [BPvdP15], while the extension (v)–(viii) appeared in the later paper [PvdP15b].

The various sets that appear in the statement of Theorem 6.6.2 and its proof are depicted schematically in Figure 6.1.

Theorem 6.6.2. *Let $0 < r < n$, and write $G := J(n,r)$. Define*

$$\mathfrak{S} := \operatorname{Ind}\left(G, \leq \left\lceil \sigma_{n,r}\binom{n}{r}\right\rceil\right)$$

and

$$\mathfrak{A} := \left\{ A \in \binom{V(G)}{\leq \alpha_{n,r}\binom{n}{r}} : \Delta G[A] < \min\{r, n-r\} \right\}.$$

There exist functions $\varphi\colon \mathbb{M}(n,r) \to \mathfrak{S}$, $\psi\colon \mathfrak{S} \to \mathfrak{A}$, and $\xi\colon \mathbb{M}(n,r) \to \mathscr{P}([n]) \times \{0,1,\ldots,n-1\}$ such that, for all $M \in \mathbb{M}(n,r)$,

(i) $\varphi(M) \subseteq \mathcal{K}(M) \subseteq \varphi(M) \cup N(\varphi(M)) \cup \psi(\varphi(M))$*;*

(ii) $\varphi(M) \cup N(\varphi(M))$ *is disjoint from* $\psi(\varphi(M))$*; and*

(iii) $|\xi(M)| \leq 2|\varphi(M)|$*; while*

(iv) $M \mapsto (\varphi(M), \xi(M), \mathcal{K}(M) \cap \psi(\varphi(M)))$ *is injective on* $\mathbb{M}(n,r)$*.*

In addition, there exist functions $t\colon \widetilde{\mathbb{M}}(n,r) \to \mathbb{Z}_{\geq 0}$, $\mathcal{T}\colon \widetilde{\mathbb{M}}(n,r) \to \mathscr{P}(\operatorname{Ind}(G))$, and $\omega\colon \widetilde{\mathbb{M}}(n,r) \to \operatorname{Ind}(G)$, such that

(v) for all $T \in \mathcal{T}(\psi(\varphi(M)))$*:* $|T| = t(M)$*;* T*,* $\omega(M)$ *and* $\varphi(M)$ *are mutually disjoint; and* $T \cup \omega(M) \cup \varphi(M) \in \operatorname{Ind}(G)$*;*

(vi) $\omega(M) \subseteq \mathcal{W}(M)$ *for all* $M \in \widetilde{\mathbb{M}}(n,r)$*;*

(vii) for any choice function ch, the function mapping

$$M \mapsto (\varphi(M) \cup ch(\mathcal{T}(M)) \cup \omega(M), \xi(M))$$

is injective on $\widetilde{\mathbb{M}}(n,r)$*;*

(viii) for any choice function ch, $\mathcal{U}(M) \mapsto (\varphi(M) \cup ch(\mathcal{T}(M)), \xi(M))$ *is injective on* $\{\mathcal{U}(M) : M \in \widetilde{\mathbb{M}}(n,r)\}$*.*

Proof. Construction of φ and ψ. Let the functions φ' and ψ be as in Theorem 6.3.9. For $M \in \mathbb{M}(n,r)$, define $\varphi(M) := \varphi'(\mathcal{K}(M))$. Items (i) and (ii) are inherited from Theorem 6.3.9.

Construction of ξ. Let $M \in \mathbb{M}(n,r)$. For each $X \in \varphi(M)$, let $\mathcal{Z}_X(M)$ be a local cover at X of cardinality at most 2; as X is dependent in M, such a local cover exists by Lemma 4.4.3. Define

$$\xi(M) := \bigcup_{X \in \varphi(M)} \mathcal{Z}_X(M).$$

Note that $|\xi(M)| \leq 2|\varphi(M)|$, so (iii) holds.

Proof of (iv). If $M \in \mathbb{M}(n,r)$ is a matroid, then by (i) and (ii) its nonbases can be partitioned as

$$\mathcal{K}(M) = \Big[\mathcal{K}(M) \cap (\varphi(M) \cup N(\varphi(M)))\Big] \cup \Big[\mathcal{K}(M) \cap \psi(\varphi(M))\Big].$$

By Lemma 4.4.4, the nonbases among $\varphi(M) \cup N(\varphi(M))$ can be reconstructed from $(\varphi(M), \xi(M))$, thus proving (iv).

Construction of t, $\mathcal{T}$, and ω. Using Lemma 6.6.1, we can exploit our knowledge of $\mathcal{K}(M) \setminus \psi(\varphi(M))$ to draw conclusions about the dependence of some elements in $\psi(\varphi(M))$. This can be formalised as follows.

Let $\mathcal{P}(M)$ be the collection of all $P \subseteq \psi(\varphi(M))$ such that if $X \in \psi(\varphi(M))$ and

- there exists $e \in X$ such that $R_X(e) \subseteq P \cup (\mathcal{K}(M) \setminus \psi(\varphi(M)))$, or
- there exists $f \in E \setminus X$ such that $C_X(f) \subseteq P \cup (\mathcal{K}(M) \setminus \psi(\varphi(M)))$,

then $X \in P$.

It is easily verified that $\mathcal{K}(M) \cap \psi(\varphi(M)) \in \mathcal{P}(M)$, and that $\mathcal{P}(M)$ is closed under taking unions and intersections. In particular, $\mathcal{P}(M)$ contains a unique minimal element $P(M)$, and since $\mathcal{P}(M)$ is closed under taking intersections, it is necessarily the case that $P(M) \subseteq \mathcal{K}(M)$. Moreover, $\mathcal{P}(M)$, and hence $P(M)$, depends on M only through the pair $(\varphi(M), \xi(M))$.

Define $\Psi(M) := \psi(\varphi(M)) \setminus P(M)$. It remains to identify the nonbases among the elements of $\Psi(M)$. We consider singleton components and larger components of $G[\mathcal{K}(M) \cap \Psi(M)]$ separately. Set

$$\omega(M) := \big\{X \in \Psi(M) : \{X\} \text{ is a component of } G[\mathcal{K}(M) \cap \Psi(M)]\big\}.$$

Let $C_1, C_2, \ldots, C_t$ be an enumeration of the non-singleton components of $G[\mathcal{K}(M) \cap \Psi(M)]$. Set $t(M) := t$, and

$$\mathcal{T}(M) := \left\{T \subseteq \bigcup_{i=1}^{t} C_i : |T \cap C_i| = 1 \text{ for } i = 1, 2, \ldots, t\right\}.$$

Proof of (v). As $|C_i| \geq 2$ for each $i = 1, 2, \ldots, t$, there are at least 2^t choices for T, so $|\mathcal{T}(M)| \geq 2^{t(M)}$.

Let $T \in \mathcal{T}(M)$. It is immediate that $|T| = t(M)$. By construction, T and $\omega(M)$ are disjoint. The set $T \cup \omega(M)$ contains exactly one vertex from each of the components of $G[\mathcal{K}(M) \cap \Psi(M)]$, and hence is a stable set in G. In addition, $\varphi(M)$ is a stable set in G. As $\Psi \subseteq \psi(\varphi(M))$

and $\psi(\varphi(M))$ is disjoint from $\varphi(M) \cup N(\varphi(M))$, it follows that $\varphi(M)$ is disjoint from T and $\omega(M)$, and that $T \cup \omega(M) \cup \varphi(M)$ is a stable set in G.

Proof of (vi). Each $X \in \omega(M)$ is a circuit-hyperplane, for if $X \in \omega(M)$ is a not a circuit-hyperplane, then there exists $e \in X$ so that $R_X(e) \subseteq \mathcal{K}(M)$, or there exists $f \in E \setminus X$ such that $C_X(f) \subseteq \mathcal{K}(M)$. In the former case, since X is an isolated vertex of $G[\mathcal{K}(M) \cap \Psi(M)]$, we have $R_X(e) \cap \Psi(M) = \emptyset$, and hence $R_X(e) \subseteq (\mathcal{K}(M) \setminus \psi(\varphi(M))) \cup P(M)$. It follows, by definition of $P(M)$, that $X \in P(M)$. The analogous argument settles the latter case.

Proof of (vii). As $\Psi(M) \subseteq \psi(\varphi(M))$, we have

$$\Delta(G[\Psi(M)]) \leq \Delta(G[\psi(\varphi(M))]) < \min\{r, n-r\}.$$

It follows that for each $X \in \Psi(M)$, there exists an $e \in X$ such that $R_X(e) \cap \Psi(M) = \emptyset$, and there exists $f \in E \setminus X$ such that $C_X(f) \cap \Psi(M) = \emptyset$.

Fix some $X \in \Psi(M)$. Let $e^* \equiv e^*(X)$ be the minimal $e \in X$ such that $R_X(e) \cap \Psi(M) = \emptyset$, and put

$$D(X) := \{y \in E \setminus X : X \triangle \{e^*, y\} \in R_X(e^*) \setminus \mathcal{K}(M)\};$$

similarly, let $f^* \equiv f^*(X)$ be the minimal $f \in E \setminus X$ such that $C_X(f) \cap \Psi(M) = \emptyset$, and put

$$C(X) := \{x \in X : X \triangle \{x, y^*\} \in C_X(f^*) \setminus \mathcal{K}(M)\}.$$

As $R_X(e^*) \setminus \mathcal{K}(M) = R_X(e^*) \setminus (\mathcal{K}(M) \setminus \Psi(M))$ and $C_X(f^*) \setminus \mathcal{K}(M) = C_X(f^*) \setminus (\mathcal{K}(M) \setminus \Psi(M))$, it follows that $C(X)$ and $D(X)$ depend only on M through $(\phi(M), \xi(M))$.

Let $X \in \Psi(M)$, and suppose that $X \in \mathcal{K}(M)$. If $D(X) = \emptyset$, then $R_X(e^*) \subseteq \mathcal{K}(M)$. This would imply $X \in P(M)$, contradicting $X \in \Psi(M)$. Thus $D(X) \neq \emptyset$. Similarly, $C(X) \neq \emptyset$. It follows that there exists $\hat{x} \in C(X)$ such that $X \triangle \{\hat{x}, f^*(X)\} \notin \mathcal{K}(M)$, and thus that $\mathrm{rk}(X) \geq r - 1$. As $C(X)$ is non-empty, it must be the unique circuit contained in X, and similarly $D(X)$ is the unique cocircuit disjoint from X, and hence, by Lemma 6.6.1,

$$\mathcal{K}(M) \cap N(X) = \{X \triangle \{x, y\} : x \in X \setminus C(X) \text{ or } y \in (E \setminus X) \setminus D(X)\}.$$

For $X \in \Psi(M)$, let $\mathcal{Q}_M(X)$ be the collection of all $Q \subseteq \Psi(M)$ such that

- $X \in Q$; and

- if $X' \in Q$, $Y \in \Psi(M)$ are such that $Y = (X' \setminus \{e\}) \cup \{f\}$, and $e \notin C(X')$ or $f \notin D(X')$, then $Y \in Q$.

It is easily verified that $\mathcal{Q}_M(X)$ is closed under taking unions and intersections. By Lemma 6.6.1, if $X \in \mathcal{K}(M) \cap \Psi(M)$, then $\mathcal{K}(M) \cap \Psi(M) \in \mathcal{Q}_M(X)$.

In particular, it follows that if $X \in \mathcal{K}(M) \cap \Psi(M)$, then there is a unique minimal element of $\mathcal{Q}_M(X)$, which we denote by $Q_M(X)$. Note that, for any $X \in \Psi(M)$, $\mathcal{Q}_M(X)$, and hence $Q_M(X)$, depends on M only through $(\varphi(M), \xi(M))$.

Let C be a component of $G[\mathcal{K}(M) \cap \Psi(M)]$, and let $X \in C$. It is easily verified that $C \in \mathcal{Q}_M(X)$, and hence that $Q_M(X) \subseteq C$. In fact, we have $Q_M(X) = C$, since $Q_M(X)$ contains $N(Y) \cap \mathcal{K}(M) \cap \Psi(M)$ whenever $Y \in Q_M(X)$.

It follows that for any matroid $M \in \mathbb{M}(n, r)$,

$$\mathcal{K}(M) = \varphi(M) \cup (\mathcal{K}(M) \cap N(\varphi(M))) \cup P(M) \cup \bigcup_{X \in \mathcal{T} \cup \omega(M)} Q_M(X).$$

<u>Proof of (viii).</u> By (vi), $\omega(M) \subseteq \mathcal{W}(M)$. It follows that $\mathcal{U}(M) \subseteq \widetilde{\mathcal{U}}$, where

$$\widetilde{\mathcal{U}} := \varphi(M) \cup (\mathcal{K}(M) \cap N(\varphi(M))) \cup P(M) \cup \bigcup_{X \in T} Q_M(X).$$

Note that $\widetilde{\mathcal{U}}$ depends on M only through $(\phi(M), \xi(M), T)$. $\mathcal{U}(M)$ can be obtained from $\widetilde{\mathcal{U}}$ by removing from it those elements that form singleton components in $G[\widetilde{\mathcal{U}}]$. □

Theorem 6.6.2 allows the encoding of matroids (without loops or coloops) as a quadruple $(\varphi(M), \xi(M), \mathcal{T}(M), \omega(M))$. The following corollary shows that this implies that every such matroid can be described as a sparse paving matroid and a little extra information.

Corollary 6.6.3. *Let $0 < r < n$. There is an injective function*

$$\widetilde{\mathbb{M}}(n, r) \to \mathbb{S}(n, r) \times \binom{\mathscr{P}([n]) \times \{0, 1, \dots, n-1\}}{\leq 2\left\lceil \sigma_{n,r}\binom{n}{r}\right\rceil}.$$

Proof. Let φ, ξ, $\mathcal{T}$ and ω be as in Theorem 6.6.2, and let ch be a choice function on $\mathscr{P}(\mathrm{Ind}(J(n, r)))$. For $M \in \widetilde{\mathbb{M}}(n, r)$, define $\mathcal{K}'(M) := \varphi(M) \cup \mathrm{ch}(\mathcal{T}(M)) \cup \omega(M)$. By Theorem 6.6.2(iv), $\mathcal{K}'(M)$ is a stable set in the Johnson graph $J(n,r)$, and so $\Big([n], \binom{[n]}{r} \setminus \mathcal{K}'(M)\Big)$ is a sparse paving matroid. By Theorem 6.6.2(vi), the map

$$M \mapsto \left(\left([n], \binom{[n]}{r} \setminus \mathcal{K}'(M)\right), \xi(M)\right)$$

is injective, thus proving the corollary. □

6.7 Enumeration of matroids

In this section, we prove Theorem 6.1.1, which we restate here for convenience.

Theorem 6.1.1.

$$\frac{1}{n}\binom{n}{n/2} \leq \log s(n) \sim \log m(n) \leq \frac{2+o(1)}{n}\binom{n}{n/2} \qquad \textit{as } n \to \infty.$$

The lower bound in the theorem follows from the construction by Graham and Sloane, Lemma 2.8.1. Two parts of the theorem remain to be proved: the upper bound, and the asymptotic equivalence of $\log m(n)$ and $\log s(n)$. We prove these separately.

Define

$$\mathscr{Z}(n,r) := \left\{ (S, \mathcal{Z}) : \begin{array}{l} S \subseteq \binom{[n]}{r}, \\ |S| \leq \left\lceil \sigma_{n,r}\binom{n}{r} \right\rceil, \\ \mathcal{Z} \subseteq \mathscr{P}([n]) \times \{0,1,\ldots,n-1\}, \\ |\mathcal{Z}| \leq 2|S| \end{array} \right\},$$

and let $z(n,r) := |\mathscr{Z}(n,r)|$. Let

$$\zeta(n) := 57\frac{\log^2 n}{n^2}\binom{n}{n/2}. \tag{6.21}$$

Lemma 6.7.1. $\log z(n,r) \leq \zeta(n)$ *for sufficiently large n.*

Proof. Ignoring the dependence between S and $\mathcal{Z}$ in the definition of $\mathscr{Z}(n,r)$, we find that $z(n,r)$ is at most the number of subsets S of size at most $\left\lceil \sigma_{n,r}\binom{n}{r} \right\rceil$ from a set of size at most $\binom{n}{n/2}$, multiplied by the number of subsets $\mathcal{Z}$ of size at most $2\left\lceil \sigma_{n,r}\binom{n}{r} \right\rceil$ from a set of size $n2^n$;

so

$$z(n,r) \leq \left(\sum_{i=0}^{N} \binom{\binom{n}{n/2}}{i}\right)\left(\sum_{i=0}^{2N} \binom{n2^n}{i}\right) \leq \left(\frac{\mathrm{e}\binom{n}{n/2}}{N}\right)^{N} \left(\frac{\mathrm{e}n2^n}{2N}\right)^{2N} \tag{6.22}$$

whenever $N \geq \lceil \sigma_{n,r}\binom{n}{r} \rceil$. The right-hand side of (6.22) increases as a function of N while $N \leq \binom{n}{n/2}/2$.

Take $N := \frac{9\ln(n)}{n^2}\binom{n}{n/2}$. By Lemma 6.5.1, we have $N \geq \lceil \sigma_{n,r}\binom{n}{r} \rceil$ for all $0 < r < n$. For this choice of N, we obtain $\mathrm{e}\binom{n}{n/2}/N \leq n^2$ and $\mathrm{e}n2^n/(2N) \leq n^{7/2}$, provided that n is sufficiently large, and hence

$$\log z(n,r) \leq N\log(n^2) + 2N\log(n^{7/2}) \leq 81\frac{\ln(n)\log(n)}{n^2}\binom{n}{n/2} \leq \zeta(n),$$

as required. □

Our interest in the quantity $z(n,r)$ is explained by its appearance in the following lemma.

Lemma 6.7.2. *For all* $0 \leq r \leq n$, $\log m(n,r) \leq z(n,r)\exp_2\left(\alpha_{n,r}\binom{n}{r}\right)$.

Proof. Note that $m(n,0) = 1$, while $z(n,0) \geq 0$ and $\alpha_{n,0}\binom{n}{0} \geq 0$. Thus, the lemma holds for $r = 0$, and similarly for $r = n$.

For the remainder of the proof, assume that $0 < r < n$. Obtain functions φ, ψ, and ξ as in Theorem 6.6.2. The function $\mathbb{M}(n,r) \to \mathscr{Z}(n,r) \times \mathscr{P}([n])$ given by

$$M \mapsto (\varphi(M), \xi(M), \mathcal{K}(M) \cap \psi(\varphi(M)))$$

is injective by Theorem 6.6.2(iv). As $|\psi(\varphi(M))| \leq \alpha_{n,r}\binom{n}{r}$, the lemma follows. □

We are now ready to prove the upper bound in Theorem 6.1.1.

Theorem 6.7.3. $\log m(n) \leq \frac{2}{n}\binom{n}{n/2} + \zeta(n) + \log(n+1)$. *In particular,* $\log m(n) \leq \frac{2+o(1)}{n}\binom{n}{n/2}$ *as* $n \to \infty$.

Proof. Let n be so large that the conclusion of Lemma 6.7.1 holds, and let $0 \leq r \leq n$. Our starting point is Lemma 6.7.2. Using Lemma 6.7.1 to bound $z(n,r)$ and Lemma 6.5.1 to bound $\alpha_{n,r}\binom{n}{r}$, we find

$$m(n,r) \leq z(n,r)\exp_2\left(\alpha_{n,r}\binom{n}{r}\right) \leq \exp_2\left(\zeta(n) + \frac{2}{n}\binom{n}{n/2}\right).$$

Summing over r and taking logarithms, we obtain

$$\log m(n) \le \log(n+1) + \zeta(n) + \frac{2}{n}\binom{n}{n/2}.$$

This proves the first part. Since $\log(n+1) + \zeta(n) = o\left(\frac{1}{n}\binom{n}{n/2}\right)$ as $n \to \infty$, the second part follows. □

It remains to prove the asymptotic equivalence of $\log m(n)$ and $\log s(n)$, for which we require the following result.

Proposition 6.7.4 ([MNWW11, Theorem 2.3])**.** *Almost every matroid has no loops or coloops.*

Theorem 6.7.5. $\log m(n) \sim \log s(n)$ *as* $n \to \infty$.

Proof. Clearly $\log m(n) \ge \log s(n)$, so it remains to prove a corresponding upper bound. In fact, we will show that $\log \widetilde{m}(n) \le (1 + o(1)) \log s(n)$, which, by Proposition 6.7.4, suffices to prove the theorem.

By Corollary 6.6.3, and Lemma 6.7.1,

$$\widetilde{m}(n,r) \le s(n,r)z(n,r) \le s(n,r)2^{\zeta(n)}.$$

This proves the theorem, since $\zeta(n) = o(\log s(n))$, and so

$$\log \widetilde{m}(n) \le \log s(n) + \zeta(n) = (1 + o(1)) \log s(n). \qquad \square$$

Theorem 6.7.5, combined with the upper bound on $\log s(n)$ obtained in Theorem 6.5.2, provides an alternative proof of the second claim in Theorem 6.7.3.

6.8 A proxy for sparse paving matroids

The techniques described in this chapter are not sufficient for proving the conjecture that almost every matroid is sparse paving. In this section, we construct a class of matroids that is slightly larger than the class of sparse paving matroids, for which we can prove that almost every matroid is in the class.

Recall the definition of $\zeta(n)$ in (6.21), and define

$$\Upsilon(n) := 5\zeta(n)\log n. \tag{6.23}$$

As $\zeta(n) = O\left(\frac{\log^2 n}{n^2}\binom{n}{n/2}\right)$, it follows that $\Upsilon(n) = O\left(\frac{\log^3 n}{n^2}\binom{n}{n/2}\right)$.

The following theorem is the main result of this section.

Theorem 6.8.1. *There exists a class $\widehat{\mathbb{S}}$ of matroids with the property that almost every matroid is in $\widehat{\mathbb{S}}$, and, for sufficiently large n,*

$$\log\left|\left\{\mathcal{U}(M) : M \in \widehat{\mathbb{S}} \cap \mathbb{M}(n)\right\}\right| \leq \Upsilon(n).$$

If almost every matroid is sparse paving, then a much stronger version of Theorem 6.8.1 holds. In that case, taking $\widehat{\mathbb{S}} = \mathbb{S}$, we even have $\left\{\mathcal{U}(M) : M \in \widehat{\mathbb{S}} \cap \mathbb{M}(n)\right\} = \{\emptyset\}$ for all n. Unfortunately, the predominance of sparse paving matroids remains conjectured rather than proved. In this section, Theorem 6.8.1 is proved by constructing a class of matroids $\widehat{\mathbb{S}}$ that relaxes the constraint on the number of possible $\mathcal{U}(M)$ that occur in matroids in the class.

Construction and properties of $\widehat{\mathbb{S}}$

The construction of the class $\widehat{\mathbb{S}}$ depends heavily on the container theorem for matroids, Theorem 6.6.2.

For all $0 < r < n$, fix a function $t_{n,r} : \widetilde{\mathbb{M}}(n,r) \to \mathbb{Z}_n$ as in Theorem 6.6.2. We will use this collection of functions to define a function t on $\widetilde{\mathbb{M}}$ that is invariant under isomorphism. Recall that a matroid canonisation is a function $f_C \colon \mathbb{M} \to \mathbb{M}$, such that $f_C(M) \cong M$ for all M, and $f_C(M) = f_C(M')$ if and only if $M \cong M'$. We may assume that $E(f_C(M)) = [|M|]$ for all M. For the remainder of this section, fix a matroid canonisation f_C. With respect to f_C, define

$$\begin{aligned} t\colon\ & \widetilde{\mathbb{M}} \to \mathbb{Z}_{\geq 0} \\ & M \mapsto t_{|M|,\mathrm{rk}(M)}(f_C(M)) \end{aligned}$$

The function t allows us to construct the class $\widehat{\mathbb{S}}$:

$$\widehat{\mathbb{S}} := \left\{M \in \widetilde{\mathbb{M}} : t(M) \leq 2\zeta(|M|)\right\}.$$

Note that t is invariant under isomorphism, so $\widehat{\mathbb{S}}$ is a class of matroids.

Theorem 6.8.1 follows by combining Lemma 6.8.2 and Lemma 6.8.3 below.

The value $t(M)$ is related to the number of complex components spanned by the nonbases of M. The intuition behind the definition of $\widehat{\mathbb{S}}$ is that if $t(M)$ is small, then $\mathcal{U}(M)$ has a concise description, while if $t(M)$ is large, then there are many different encodings (in the sense of Theorem 6.6.2).

Lemma 6.8.2. $|\mathbb{M}(n) \setminus \widehat{\mathbb{S}}| = o(s(n))$ *as* $n \to \infty$. *In particular, almost every matroid is in* $\widehat{\mathbb{S}}$.

Proof. Define $\mathcal{M} := \left\{M \in \widetilde{\mathbb{M}} : t(M) > 2\zeta(|M|)\right\}$, so that every matroid is either in $\widehat{\mathbb{S}}$, or in $\mathcal{M}$, or has a loop or coloop. As almost every matroid has no loops and coloops (Proposition 6.7.4), proving that $\mathcal{M}$ is small is tantamount to proving the lemma.

Fix $0 < r < n$; without loss of generality, we may assume that n is so large that the conclusion of Lemma 6.7.1 holds. We bound $m_{\mathcal{M}}(n, r)$. By Theorem 6.6.2(vii), for each $M \in \mathcal{M} \cap \mathbb{M}(n, r)$, there is an injective one-to-many relation mapping $f_C(M)$ to at least $2^{2\zeta(n)}$ triples $(S, \mathcal{Z}, S')$, where S and S' are stable sets in $J(n, r)$, and $(S, \mathcal{Z}) \in \mathscr{Z}(n, r)$. It follows that

$$\begin{aligned}\left|\{f_C(M) : M \in \mathcal{M} \cap \mathbb{M}(n, r)\}\right| &\leq z(n, r)s(n, r)2^{-2\zeta(n)} \\ &\leq s(n, r)2^{-\zeta(n)}. \qquad (6.24)\end{aligned}$$

On the other hand,

$$m_{\mathcal{M}}(n, r) \leq n! \left|\{f_C(M) : M \in \mathcal{M} \cap \mathbb{M}(n, r)\}\right|. \qquad (6.25)$$

Combining (6.24) with (6.25), summing over r yields

$$m_{\mathcal{M}}(n) \leq n! 2^{-\zeta(n)} s(n) = o(s(n)). \qquad \square$$

Lemma 6.8.3. $\log \left|\left\{\mathcal{U}(M) : M \in \widehat{\mathbb{S}} \cap \mathbb{M}(n, r)\right\}\right| \leq \Upsilon(n)$ *for all* $0 \leq r \leq n$ *and* n *sufficiently large.*

Proof. By Theorem 6.6.2(viii), there is an injective function

$$\left\{\mathcal{U}(f_C(M)) : \widehat{\mathbb{S}} \cap \mathbb{M}(n, r)\right\} \to \mathscr{Z}(n, r) \times \operatorname{Ind}(J(n, r)),$$

mapping $\mathcal{U}(M)$ to a triple $(S, \mathcal{Z}, T)$ which, by Theorem 6.6.2(v), satisfies $|T| = t(M) \leq 2\zeta(n)$. Using a crude bound on the number of such T, we obtain

$$\begin{aligned}\left|\{\mathcal{U}(f_C(M)) : \widehat{\mathbb{S}} \cap \mathbb{M}(n, r)\}\right| &\leq z(n, r) \sum_{i=0}^{\lfloor 2\zeta(n) \rfloor} \binom{\binom{n}{r}}{i} \\ &\leq \exp_2\left(\zeta(n) + \mathscr{H}\left(\frac{2\zeta(n)}{\binom{n}{n/2}}\right)\binom{n}{n/2}\right). \qquad (6.26)\end{aligned}$$

In addition,

$$\left|\left\{\mathcal{U}(M) : \widehat{\mathbb{S}} \cap \mathbb{M}(n,r)\right\}\right| \leq n! \left|\left\{\mathcal{U}(f_C(M)) : \widehat{\mathbb{S}} \cap \mathbb{M}(n,r)\right\}\right|. \tag{6.27}$$

Combining (6.26) with (6.27) yields the desired result, as $n! \leq n^n$, and

$$\mathscr{H}\left(\frac{2\zeta(n)}{\binom{n}{n/2}}\right)\binom{n}{n/2} \leq (4+o(1))\zeta(n)\log n. \qquad \square$$

The following lemma shows that $\widehat{\mathbb{S}}$ essentially contains the sparse paving matroids.

Lemma 6.8.4. $\mathbb{S} \cap \widetilde{\mathbb{M}} \subseteq \widehat{\mathbb{S}}$.

Proof. If M is a sparse paving matroid without loops or coloops, then $t(f_C(M)) = 0$, while $\zeta(|M|) > 0$. It follows that $M \in \widehat{\mathbb{S}}$. □

There are many different collections of circuit-hyperplanes

We conclude this section by proving the following generic tool for showing that a class of matroids is small. As each matroid on a given ground set is determined by the pair $(\mathcal{U}(M), \mathcal{W}(M))$, combining a bound on the number of possible collections $\mathcal{W}(M)$ that appear in the class with the bound in Lemma 6.8.3 bounds the class itself.

Theorem 6.8.5. *There exists a constant $c > 0$ such that if $\mathcal{M} \subseteq \mathbb{M}$ is a class of matroids satisfying*

$$\log|\{\mathcal{W}(M) : M \in \mathcal{M} \cap \mathbb{M}(n,r)\}| \leq \left(1 - c\frac{\log^3 n}{n}\right)\log s(n), \tag{6.28}$$

for all $0 \leq r \leq n$ and sufficiently large n, then $m_{\mathcal{M}}(n) = o(s(n))$. In particular, $\mathcal{M}$ is small.

Proof. Let $\mathcal{M}$ be a class of matroids for which (6.28) holds. We show that $m_{\mathcal{M}\cap\widehat{\mathbb{S}}}(n) = o(s(n))$, which, in view of Lemma 6.8.2, suffices to prove the theorem.

Let $\widehat{\mathcal{U}}(n,r) := \left\{\mathcal{U}(M) : M \in \widehat{\mathbb{S}} \cap \mathbb{M}(n,r)\right\}$. For all $0 \leq r \leq n$, the map $M \mapsto (\mathcal{U}(M), \mathcal{W}(M))$ is an injective function

$$\mathcal{M} \cap \widehat{\mathbb{S}} \cap \mathbb{M}(n,r) \to \widehat{\mathcal{U}}(n,r) \times \{W(M) : M \in \mathcal{M} \cap \mathbb{M}(n,r)\},$$

and hence

$$m_{\mathcal{M}\cap\widehat{\mathbb{S}}}(n,r) \leq \left|\widehat{\mathcal{U}}(n,r)\right| \times |\{W(M) : M \in \mathcal{M} \cap \mathbb{M}(n,r)\}|.$$

By Theorem 6.8.1, $\log\left|\widehat{\mathcal{U}}(n,r)\right| \leq \Upsilon(n)$. The second factor is bounded by (6.28), so it follows that

$$m_{\mathcal{M}\cap\widehat{\mathbb{S}}}(n,r) \leq s(n)\exp_2\left(\Upsilon(n) - c\frac{\log^3 n}{n}\log s(n)\right).$$

Summing over r, it follows that

$$m_{\mathcal{M}\cap\widehat{\mathbb{S}}}(n) \leq s(n)\exp_2\left(\log(n+1) + \Upsilon(n) - c\frac{\log^3 n}{n}\log s(n)\right),$$

which is $o(s(n))$, provided that c is sufficiently large. □

CHAPTER **7**

Typical properties

This chapter is based on the journal papers [PvdP16c, PvdP16a], which is joint work with Rudi Pendavingh.

7.1 In this chapter...

This chapter continues where the previous chapter ended. The class $\widehat{\mathbb{S}}$ of matroids, introduced in Section 6.8, contains almost every matroid. Therefore, in order to prove that a matroid property is typical, it suffices to consider the fraction of matroids in $\widehat{\mathbb{S}}$ that satisfy the property. The class $\widehat{\mathbb{S}}$ is more structured than the class of all matroids, and in this chapter we explore the extra traction this additional structure provides when proving statements about properties that hold for almost every matroid. The results in this chapter prove some of the conjectures posed in the introduction, and make progress on some of the remaining conjectures.

In Section 7.2, we start this chapter with an analysis of the typical number of bases in a matroid. The results obtained in that section are then used to show that almost every matroid

- has $\mathrm{rk}(M) = |M|/2 \pm O\left(\sqrt{|M|}\right)$ and girth $\Omega\left(\log|M|\right)$ (Section 7.3);
- has no nontrivial erections (Section 7.4);

- has Tutte connectivity, vertical connectivity, and branch-width $\Omega\left(\sqrt{\log|M|}\right)$ (Section 7.5); and
- contains a $U(k,2k)$-minor whenever $k \leq O(\log|M|)$ (Section 7.6).

In Section 7.7, we consider symmetry. In particular, it is shown there that almost every sparse paving matroid is asymmetric, while almost every matroid is, in a precise sense, close to asymmetric.

7.2 The number of bases of almost every matroid

Recall that the nonbases $\mathcal{K}(M)$ of a matroid are partitioned into two classes: the circuit-hyperplanes $\mathcal{W}(M)$, and $\mathcal{U}(M) := \mathcal{K}(M)\backslash\mathcal{W}(M)$. In this chapter, we write $b(M)$ for the *basis-density*, i.e. if M is a matroid of rank r on a ground set on n elements, then $b(M) = |\mathcal{B}(M)|/\binom{n}{r}$. The nonbasis-density $d(M)$, and circuit-hyperplane-density $w(M)$ are defined similarly, and $u(M) = d(M) - w(M)$. In this section, we prove the following result on the nonbasis-density of almost every matroid.

Theorem 7.2.1. *Almost every matroid M satisfies*

$$\Omega\left(\frac{1}{|M|}\right) \leq d(M) \leq O\left(\frac{\log^3|M|}{|M|}\right).$$

The lower bound and upper bound are proved in Lemma 7.2.2 and Lemma 7.2.8, respectively.

Almost every matroid has a few nonbases

In Lemma 6.5.3 we proved that the Johnson graph $J(n,r)$ contains many stable sets of the order $\frac{1}{n}\binom{n}{r}$, provided $r \approx n/2$. The following lemma, which implies the lower bound in Theorem 7.2.1, uses this observation to show that almost every matroid has a large number of circuit-hyperplanes. Let $\lambda_0 \approx 0.22$ be the unique solution to $\mathscr{H}(\lambda_0/2) = 1/2$ in $(0,1/2)$.

Lemma 7.2.2. *Let* $0 < \lambda < \lambda_0$. *Almost every matroid satisfies* $w(M) \geq \frac{\lambda}{|M|}$.

Proof. Let $\mathcal{M}$ be the class of matroids with $w(M) < \frac{\lambda}{|M|}$. For all $0 \leq r \leq n$,

$$\left|\left\{W(M) : M \in \mathcal{M} \cap \mathbb{M}(n,r)\right\}\right| = \operatorname{ind}\left(J(n,r), < \frac{\lambda}{n}\binom{n}{r}\right).$$

By Lemma 6.5.3, since $\lambda < \lambda_0$ there exists $\varepsilon > 0$ such that

$$\operatorname{ind}\left(J(n,r), \leq \frac{\lambda}{n}\binom{n}{r}\right) \leq (1-\varepsilon)\log s(n) \leq (1-\varepsilon)\log m(n)$$

for all sufficiently large n. The lemma now follows from Theorem 6.8.5. □

Almost every matroid has few nonbases

As $d(M) = u(M) + w(M)$, bounding each of the terms separately suffices to bound $d(M)$. The following lemma shows that the difficulty in proving the upper bound lies in bounding $u(M)$.

Lemma 7.2.3. *For any matroid M, $w(M) \leq \frac{2}{|M|}$.*

Proof. Let $r = \operatorname{rk}(M)$. As $\mathcal{W}(M)$ is a stable set in the Johnson graph, it follows that $w(M) \leq \alpha(J(n,r))$, where $\alpha(G)$ is the stability ratio of G. By the Hoffman bound (see Remark 6.3.4), $\alpha(J(n,r)) \leq \frac{1}{\max\{n-r+1,r+1\}} \leq \frac{2}{n}$, which proves the lemma. □

It remains to bound $u(M)$, for which we require a few preliminary results.

A graph is called *vertex-transitive* if, for any pair of vertices v, w, it has an automorphism mapping v to w. We will apply the following lemma to the Johnson graph $J(n,r)$, which is a vertex-transitive graph. Its proof relies on entropy, in particular on Shearer's Entropy Lemma, which was discussed in Chapter 3.

Lemma 7.2.4. *Let G be a vertex-transitive graph, and let $U \subseteq V(G)$. Then*

$$\frac{\log \operatorname{ind}(G)}{|V(G)|} \leq \frac{\log \operatorname{ind}(G[U])}{|U|}.$$

Proof. Let $\Gamma = \operatorname{Aut}(G)$. For any group element $g \in \Gamma$, write $g(U) := \{g(u) : u \in U\}$ for the image of U under g, and consider the collection $\Gamma(U) := (g(U) : g \in \Gamma)$. As Γ acts transitively on $V(G)$, we have $|\{g \in \Gamma : v \in g(U)\} = |\Gamma|\frac{|U|}{|V(G)|}$ for each $v \in V(G)$, and so each vertex is contained in precisely $|\Gamma|\frac{|U|}{|V(G)|}$ elements of $\Gamma(U)$.

Let $\boldsymbol{X}$ be an element of $\operatorname{Ind}(G)$, chosen uniformly at random, so $\mathscr{H}(\boldsymbol{X}) = \log \operatorname{ind}(G)$. For $A \subseteq V(G)$, $\boldsymbol{X} \cap A \in \operatorname{Ind}(G[A])$; such sets are projections in the sense of Shearer's Entropy Lemma. We thus obtain

$$\log \operatorname{ind}(G) = \mathscr{H}(\boldsymbol{X}) \leq \frac{|V(G)|}{|U||\Gamma|} \sum_{g \in \Gamma} \mathscr{H}(\boldsymbol{X} \cap g(U))$$
$$\leq \frac{|V(G)|}{|U||\Gamma|} \sum_{g \in \Gamma} \log \operatorname{ind}(G[g(U)]) \,.$$

The lemma now follows since $G[g(U)] \cong G[U]$ for all $g \in \Gamma$. □

For disjoint vertex sets U, U' in G, write $\nabla(U, U')$ for the set of edges with one end point in U and U' each.

Lemma 7.2.5. *Let G be a graph, and let $U, U' \subseteq V(G)$ be such that $\nabla(U, U') = \emptyset$. Then*

$$\log \operatorname{ind}(G[U]) + \log \operatorname{ind}(G[U']) \leq \log \operatorname{ind}(G) \,.$$

Proof. If S is a stable set in $G[U]$, and S' is a stable set in $G[U']$, then $S \cup S'$ is a stable set in G, since $\nabla(S, S') = \emptyset$. As $(S, S') \mapsto S \cup S'$ is injective, the claim follows. □

The following lemma shows that few matroids satisfy $\mathcal{U}(M) = U$, when $|U|$ is large.

Lemma 7.2.6. *For all $0 \leq r \leq n$ and all $0 \leq u \leq 1$, if $U \subseteq \binom{[n]}{r}$ is such that $|U|/\binom{n}{r} \geq u$, then*

$$\log \left|\left\{M \in \mathbb{M}(n, r) : \mathcal{U}(M) = U\right\}\right| \leq (1 - u) \log s(n, r).$$

Proof. Fix a collection U such that $|U|/\binom{n}{r} \geq u$. A matroid $M \in \mathbb{M}(n, r)$ such that $\mathcal{U}(M) = U$ is determined by its collection $\mathcal{W}(M)$ of circuit-hyperplanes. Write $G := J(n, r)$, and let $U' := V(G) \setminus (U \cup N(U))$. The collection $\mathcal{W}(M)$ is a stable set in $G[U']$; in the other direction, any stable set in $G[U']$ appears as the collection of circuit-hyperplanes of a matroid $M \in \mathbb{M}(n, r)$ such that $\mathcal{U}(M) = U$. It follows that

$$\log \left|\left\{M \in \mathbb{M}(n, r) : \mathcal{U}(M) = U\right\}\right| = \log \operatorname{ind}(G[U']) \,, \tag{7.1}$$

which by Lemma 7.2.5 is at most

$$\log \operatorname{ind}(G) - \log \operatorname{ind}(G[U]) \,. \tag{7.2}$$

By Lemma 7.2.4,

$$\log \operatorname{ind}(G[U]) \geq u \log \operatorname{ind}(G) \,, \tag{7.3}$$

and the lemma now follows upon combining (7.1)–(7.3) with the observation that $\operatorname{ind}(G) = s(n, r)$. □

We are now ready to prove an upper bound on $u(M)$ that holds for almost every matroid. Recall the definition of $\Upsilon(n)$ in (6.23), and define

$$v(n) := \frac{\Upsilon(n) + 2\log(n+1)}{\log s(n)}.$$

As $\Upsilon(n) = O\left(\frac{\log^3 n}{n^2}\binom{n}{n/2}\right)$, and $\log s(n) \geq \frac{1}{n}\binom{n}{n/2}$, it follows that $v(n) = O\left(\frac{\log^3 n}{n}\right)$.

Lemma 7.2.7. *Almost every matroid satisfies $u(M) \leq v(|M|)$.*

Proof. Let $\mathcal{M}$ be the class of matroids with $u(M) > v(|M|)$. We will show that $\mathcal{M}$ is small. Let $\widehat{\mathbb{S}}$ be the class of matroids in Theorem 6.8.1. As almost every matroid is in $\widehat{\mathbb{S}}$, it suffices to show that $\mathcal{M} \cap \widehat{\mathbb{S}}$ is small.

Let $\mathcal{U}(n,r) := \{\mathcal{U}(M) : M \in \widehat{\mathbb{S}} \cap \mathbb{M}(n,r)\}$. Partitioning the set $\mathcal{M} \cap \widehat{\mathbb{S}} \cap \mathbb{M}(n,r)$ by the value of $\mathcal{U}(M)$, it follows that

$$|\mathcal{M} \cap \widehat{\mathbb{S}} \cap \mathbb{M}(n,r)| \leq \sum_{\substack{U \in \mathcal{U}(n,r): \\ |U| > v(n)\binom{n}{r}}} \left|\left\{M \in \mathbb{M}(n,r) : \mathcal{U}(M) = U\right\}\right|. \tag{7.4}$$

By Theorem 6.8.1, $\log|\mathcal{U}(n,r)| \leq \Upsilon(n)$. This bounds the number of terms in the right-hand side of (7.4), while Lemma 7.2.6 bounds each of the terms, as

$$\log\left|\left\{M \in \mathbb{M}(n,r) : \mathcal{U}(M) = U\right\}\right| \leq (1 - v(n))\log s(n,r)$$

for each $U \in \mathcal{U}(n,r)$ such that $|U| > v(n)\binom{n}{r}$. Combining these bounds with (7.4), we obtain

$$\begin{aligned}\log|\mathcal{M} \cap \widehat{\mathbb{S}} \cap \mathbb{M}(n,r)| &\leq \Upsilon(n) + (1 - v(n))\log s(n,r) \\ &\leq \log s(n) - 2\log(n+1),\end{aligned}$$

and hence $|\mathcal{M} \cap \widehat{\mathbb{S}} \cap \mathbb{M}(n,r)| \leq \frac{s(n)}{(n+1)^2}$. Summing over r, and using that $m(n) \geq s(n)$, we find that

$$\frac{|\mathcal{M} \cap \widehat{\mathbb{S}} \cap \mathbb{M}(n,r)|}{m(n)} \leq \frac{1}{n+1} \to 0,$$

thus proving that $\mathcal{M}$ is small. □

We are now ready to prove the upper bound of Theorem 7.2.1.

Lemma 7.2.8. *Almost every matroid satisfies $d(M) = O\left(\frac{\log^3|M|}{|M|}\right)$.*

Proof. By Lemma 7.2.3, $w(M) \leq 2/|M|$ for all matroids M, while by Lemma 7.2.7, almost every matroid satisfies $u(M) \leq v(|M|)$. Combining the two observations, we obtain that almost every matroid satisfies

$$d(M) = u(M) + w(M) \leq v(|M|) + \frac{2}{|M|}.$$

The lemma follows as $v(n) = O\left(\frac{\log^3 n}{n}\right)$ as $n \to \infty$. □

7.3 Rank, girth, and cogirth

In this section, we show that almost every matroid has rank asymptotic to $|M|/2$, and girth and cogirth at least $\Omega(\log |M|)$.

Theorem 7.3.1. *For all $\beta > \sqrt{\frac{\ln 2}{2}} \approx 0.589\ldots$, almost every matroid satisfies*

$$\frac{|M|}{2} - \beta\sqrt{|M|} \leq \mathrm{rk}(M) \leq \frac{|M|}{2} + \beta\sqrt{|M|}.$$

Proof. Fix $\beta > \sqrt{\frac{\ln 2}{2}}$, and let $r_0 = \left\lfloor \frac{n}{2} - \beta\sqrt{n} \right\rfloor$. We will show that

$$\lim_{n\to\infty} \frac{1}{m(n)} \sum_{r \leq r_0} m(n,r) = 0, \tag{7.5}$$

which, by duality, implies the theorem. By Lemma 6.7.2, $\log m(n,r) \leq z(n,r) + \frac{1}{n-r+1}\binom{n}{r}$, which by Lemma 6.7.1 is at most $\zeta(n) + \frac{1}{n-r+1}\binom{n}{r}$ for sufficiently large n. This implies

$$\begin{aligned}\log \sum_{r\leq r_0} m(n,r) &\leq \log(r_0+1) + \zeta(n) + \max_{r \leq r_0} \frac{1}{n-r+1}\binom{n}{r} \\ &\leq \log(n) + \zeta(n) + \frac{1}{n-r_0+1}\binom{n}{r_0} \qquad (7.6)\\ &= \frac{2+o(1)}{n}\binom{n}{n/2}\exp\left(-2\beta^2\right),\end{aligned}$$

where the last step uses Lemma 2.2.1 to bound $\binom{n}{r_0}$. Combining (7.6) with the bound $\log m(n) \geq \frac{1}{n}\binom{n}{n/2}$, we obtain

$$\log \frac{\sum_{r\leq r_0} m(n,r)}{m(n)} \leq \left((2+o(1))\mathrm{e}^{-2\beta^2} - 1\right)\frac{1}{n}\binom{n}{n/2} \to -\infty,$$

which implies (7.5) and hence proves the theorem. □

Recall that the girth $\mathrm{g}(M)$ of the matroid M is the cardinality of a smallest circuit in M (and $\mathrm{g}(M) = \infty$ if M does not have any circuits). Small circuits yield large complex components, i.e. large sets of nonbases that induce connected subgraphs of $J(n,r)$. The resulting lower bound on $u(M)$, and hence on the nonbasis-density $d(M)$, is made precise in the following lemma.

Lemma 7.3.2. *Let $M \in \mathbb{M}(n,r)$. If M has a circuit of cardinality $k < r$, then $u(M) \geq \left(\frac{r-k}{n}\right)^k$.*

Proof. If C is a circuit of M, then each $X \in \binom{[n]}{r}$ that contains C is dependent. Such dependent sets induce a connected subgraph of $J(n,r)$, and so $\left\{X \in \binom{[n]}{r} : C \subseteq X\right\} \subseteq \mathcal{U}(M)$. If C has cardinality k, then

$$u(M) \geq \binom{n-k}{r-k} \Big/ \binom{n}{r} \geq \left(\frac{r-k}{n}\right)^k. \qquad \square$$

In the following result, we write $\mathrm{g}^*(M) := \mathrm{g}(M^*)$ for the cogirth of the matroid M.

Theorem 7.3.3. *For all $c < 1$, almost every matroid satisfies $\mathrm{g}(M) \geq c \log |M|$ and $\mathrm{g}^*(M) \geq c \log |M|$.*

Proof. We will show that almost all matroids satisfy $\mathrm{g}(M) \geq c \log |M|$. The claim about cogirth then follows by duality. Let $\mathcal{M}$ be defined as

$$\mathcal{M} := \left\{ M \in \mathbb{M} : \left| \mathrm{rk}(M) - \frac{|M|}{2} \right| \leq \sqrt{|M|},\ u(M) \leq \upsilon(|M|) \right\}.$$

By Lemma 7.2.7, almost every matroid satisfies $u(M) \leq \upsilon(|M|)$, and by Theorem 7.3.1 almost every matroid satisfies $|\,\mathrm{rk}(M) - |M|/2| \leq \sqrt{|M|}$. It follows that almost every matroid is in $\mathcal{M}$.

We show that matroids in $\mathcal{M} \cap \mathbb{M}(n)$ cannot have small girth, provided n is sufficiently large, which implies the theorem. For the sake of contradiction, suppose that some matroid $M \in \mathcal{M} \cap \mathbb{M}(n)$ contains a circuit of cardinality $k < c \log n$. By Lemma 7.3.2,

$$u(M) \geq \left(\frac{\mathrm{rk}(M) - k}{n}\right)^k \geq 2^{-k-1}$$

for sufficiently large n. It follows that

$$2^{-k-1} \leq \upsilon(n) = O\left(\frac{\log^3 n}{n}\right),$$

which fails for large n: a contradiction. $\square$

The following result was shown before by Lowrance, Oxley, Semple, and Welsh [LOSW13, Corollary 3.3] and generalises [MNWW11, Theorem 2.3]. It follows from Theorem 7.3.3 since a matroid is simple and cosimple precisely when both its girth and cogirth are at least 3.

Corollary 7.3.4. *Almost every matroid is simple and cosimple.*

7.4 Nontrivial erections

Recall that $T(N)$ denotes the truncation of the matroid N, and in the other direction, that N is an erection of M if $M = N$ or $M = T(N)$. In the former case, we say that N is a trivial erection; otherwise it is nontrivial. Matroid erections play a central role in Chapter 5.

Theorem 7.4.1. *Almost every matroid has only the trivial erection.*

Proof. Let $\mathcal{M}$ be the class of matroids that have a nontrivial erection. We will show that $\mathcal{M}$ is small.

Note that $\mathcal{M}\cap\mathbb{M}(n) = \{T(M) : M \in \mathbb{M}(n)\}$. If M' is obtained from M by relaxing a circuit-hyperplane, then $T(M') = T(M)$. It follows that $\mathcal{M}\cap\mathbb{M}(n) = \{T(M) : M \in \mathbb{M}(n), \mathcal{W}(M) = \emptyset\}$, and therefore that

$$|\mathcal{M}\cap\mathbb{M}(n)| \leq |\{M \in \mathbb{M}(n) : \mathcal{W}(M) = \emptyset\}|.$$

By Lemma 7.2.2, the right-hand side is $o(m(n))$, which concludes the proof. □

7.5 Connectivity and branch-width

In ths section, we address Conjecture 1.3.8, which states that almost every matroid is arbitrarily highly connected. We prove the following strong version of the conjecture.

Theorem 7.5.1. *There exists a constant $c > 0$ such that almost every matroid has connectivity at least $c\sqrt{\log|M|}$.*

Two notions that are related to connectivity are vertical connectivity and branch-width, defined below. As a corollary to Theorem 7.5.1, we obtain that almost every matroid has vertical connectivity and branch-width at least $\Omega\left(\sqrt{\log|M|}\right)$ as well.

Connectivity

We require the following easy property of connectivity.

Lemma 7.5.2. *If $\{A, B\}$ is a k-separation of M, then A is dependent or codependent.*

Proof. We argue by contradiction. Suppose that A is both independent and coindependent. Then $\mathrm{rk}(A) = |A|$, and $\mathrm{rk}(B) = r$. It follows that

$$k \geq \lambda(M) = \mathrm{rk}(A) + \mathrm{rk}(B) - r + 1 = |A| + 1 \geq k + 1,$$

which cannot be. So A must be dependent or codependent. □

The main technical work required for proving Theorem 7.5.1 is contained in the following lemma, which essentially states that low-order separations give rise to large collections of nonbases, provided that the matroid has large girth and cogirth.

Lemma 7.5.3. *Let $G\colon \mathbb{Z}_{\geq 0} \to \mathbb{R}_{\geq 0}$ be a function. There exists $c > 0$ such that for sufficiently large n, and all r satisfying $n/2 - \sqrt{n} \leq r \leq n/2 + \sqrt{n}$: if $M \in \mathbb{M}(n, r)$ has girth and cogirth at least $G(n)$, and M has a k-separation $\{A, B\}$, then $u(M) \geq 1 - ck\sqrt{\frac{n}{G(n)(n-G(n))}}$.*

Proof. Let $M \in \mathbb{M}(n, r)$ be a matroid with girth and cogirth at least $G(n)$, and let $\{A, B\}$ be a k-separation of M. We exhibit a large subset of $\mathcal{U}(M)$, which proves the lemma.

In order to build this large subset, define

$$U_S := \left\{ X \in \binom{[n]}{r} : |X \cap S| > \mathrm{rk}(S) \right\}, \qquad S \in \{A, B\}.$$

If $X \in U_A \cup U_B$, then X is a nonbasis. Thus, $d(M) \geq 1 - q/\binom{n}{r}$, where q is the number of r-sets outside $U_A \cup U_B$. Writing $a := |A|$, we obtain

$$q = \sum_{\substack{s : s \leq \mathrm{rk}(A) \\ r-s \leq \mathrm{rk}(B)}} \binom{a}{s}\binom{n-a}{r-s} \tag{7.7}$$

As $k \geq \lambda(A) = \mathrm{rk}(A) + \mathrm{rk}(B) - r + 1$, it follows that the sum in (7.7) has at most k terms, so

$$q \leq k \max_{s} \binom{a}{s}\binom{n-a}{r-s} \leq k\binom{a}{a/2}\binom{n-a}{(n-a)/2}.$$

Bounding the central binomial coefficients on the right-hand side, we obtain

$$q \le k\frac{2}{\pi}\left(\frac{2^a}{\sqrt{a}}\right)\left(\frac{2^b}{\sqrt{b}}\right) \le 2k\sqrt{\frac{2}{\pi}}\sqrt{\frac{n}{ab}}\binom{n}{n/2}.$$

By 2.2.1, there is a constant $c' > 0$ such that $\binom{n}{n/2} \le c'\binom{n}{r}$ for all r satisfying $|r - n/2| \le \sqrt{n}$. Hence

$$d(M) = 1 - \frac{q}{\binom{n}{r}} \ge 1 - 2c'k\sqrt{2}\pi\sqrt{\frac{n}{ab}}. \tag{7.8}$$

By Lemma 7.5.2, both sides of a separation contain a circuit or a cocircuit, so by the assumption on girth and cogirth, it follows that $a, b \ge G(n)$. As $a + b = n$, it follows that $ab \ge G(n)\,(n - G(n))$, which, together with (7.8), implies the conclusion of the lemma with $c := 2c'\sqrt{2}\pi$. □

We are now ready to prove Theorem 7.5.1.

Proof of Theorem 7.5.1. For $c > 0$, define

$$\mathcal{M}_c := \left\{M \in \mathbb{M} : M \text{ has a } k\text{-separation } \{A, B\} \text{ with } k \le c\sqrt{\log|M|}\right\}.$$

We shall show that there exists c such that $\mathcal{M}_c$ is small. By Theorem 7.3.1, almost every matroid satisfies $|\mathrm{rk}(M) - |M|/2| \le \sqrt{|M|}$, and by Theorem 7.3.3, there exists $c' > 0$ such that almost every matroid M has girth and cogirth at least $c' \log|M|$. Thus, it suffices to show that $\mathcal{M}'_c$ is small, where

$$\mathcal{M}'_c := \left\{M \in \mathcal{M}_c : \begin{array}{c} \mathrm{g}(M),\ \mathrm{g}^*(M) \ge c'\log|M| \\ |\mathrm{rk}(M) - |M|/2| \le \sqrt{|M|} \end{array}\right\}$$

By Lemma 7.5.3, there exists a constant $c'' > 0$ such that

$$u(M) \ge 1 - \frac{c''k}{\sqrt{\log n}} \ge 1 - c''c$$

for all $M \in \mathcal{M}'_c \cap \mathbb{M}(n)$, provided that n is sufficiently large. Picking any $c < 1/c''$, it follows that $1 - c''c > 0$ for all $M \in \mathcal{M}'_c \cap \mathbb{M}(n)$ and n sufficiently large. It follows from Theorem 7.2.1 that $\mathcal{M}'_c$ is small, and this concludes the proof. □

Vertical connectivity

Vertical connectivity is a variant notion of connectivity that is sometimes more convenient to use than Tutte connectivity. Let $k \geq 1$. A *vertical k-separation* of M is a partition $\{A, B\}$ of $E(M)$ such that $\mathrm{rk}(A), \mathrm{rk}(B) \geq k$, and $\mathrm{rk}(A) + \mathrm{rk}(B) < \mathrm{rk}(M) + k$. The *vertical connectivity* of M is[1]

$$\lambda_v(M) := \min \{k : M \text{ has a vertical } k\text{-separation}\}.$$

The only way in which a vertical k-separation is different from a k-separation is the requirement that $\mathrm{rk}(A), \mathrm{rk}(B) \geq k$, which replaces the requirement that $|A|, |B| \geq k$. It follows that $\lambda_v(M) \geq \lambda(M)$. The following result gives a stronger connection between the two quantities.

Proposition 7.5.4 ([Oxl11, Theorem 8.6.4])**.** *Let M be a matroid, and suppose that M is not isomorphic to any uniform matroid $U(r, n)$ with $n \geq 2r - 1$. Then*

$$\lambda(M) = \min \{\lambda_v(M), \mathrm{g}(M)\}.$$

Combining Proposition 7.5.4 with the results that almost every matroid has high Tutte connectivity (Theorem 7.5.1) and high girth (Theorem 7.3.3) shows that almost every matroid has high vertical connectivity.

Corollary 7.5.5. *There exists $c > 0$ such that almost every matroid satisfies $\lambda_v(M) \geq c\sqrt{\log |M|}$.*

Branch-width

The branch-width $\mathrm{bw}(M)$ of a matroid M measures, roughly, how tree-like it is; see [Oxl11, Section 14.2] for a definition. The following result links branch-width and connectivity.

Proposition 7.5.6 ([Dha96, Lemma 4.3])**.** *Let $k \geq 3$, and suppose that $\lambda(M) \geq k$. Then $\mathrm{bw}(M) \geq k$ if and only if $|M| \geq 3k - 5$.*

Combining the proposition with Theorem 7.5.1 immediately implies that almost every matroid has high branch-width.

Corollary 7.5.7. *There exists $c > 0$ such that almost every matroid has branch-width at least $c\sqrt{\log |M|}$.*

[1] Our notation deviates from that of Oxley [Oxl11]. There, $\kappa(M)$ is used for vertical connectivity, which in this thesis is already used for cover complexity.

7.6 Large uniform minors

Recall Conjecture 1.3.5, which we restate here for convenience.

Conjecture 1.3.5 ([MNWW11, Conjecture 1.7])**.** *Let N be a sparse paving matroid. Almost every matroid has an N-minor.*

In this section, we address the special case of Conjecture 1.3.5, in which N is a uniform matroid. In Chapter 3 and Chapter 4, we already proved that almost all matroids contain an arbitrarily long line, as well as $U(3,6)$, as minors. Here, we vastly improve upon these results. In particular, we prove the following theorem.

Theorem 7.6.1. *Let $c > 5/2$. Almost every matroid has a $U(k,2k)$-minor, whenever $k \leq \frac{1}{2}\left(\log|M| - c\log\log|M|\right)$.*

Note that, if N is any fixed uniform minor, Theorem 7.6.1 shows that almost every matroid contains N as a minor, thus proving Conjecture 1.3.5 for this special case.

Theorem 7.6.1 follows as a special case of the more general Theorem 7.6.3 below. The crux of the argument is that if a matroid M does not have $U(a,b)$ as a minor, then the $\mathrm{rk}(M)$-subsets of $E(M)$ cannot contain a large connected area consisting solely of bases, as such an area gives rise to a $U(a,b)$-minor. When a and b are not too large, this results in a fraction of nonbases that is much larger than the fraction of nonbases of a typical matroid, thus showing that only a small fraction of matroids have no $U(a,b)$-minor. This is made precise in the following lemma.

Lemma 7.6.2. *Let $0 \leq a \leq b$ and $0 \leq r \leq n$ be integers satisfying $a \leq r$ and $b - a \leq n - r$. If $M \in \mathbb{M}(n,r)$ is a matroid such that $U(a,b)$ is not a minor of M, then $d(M) \geq 1/\binom{b}{a}$.*

Proof. Let $C, D \subseteq E(M)$ be such that $|C| = r-a$, $|D| = (n-r)-(b-a)$, and $C \cap D = \emptyset$. Define

$$[C;D] := \left\{X \in \binom{E(M)}{r} : C \subseteq X, D \cap X = \emptyset\right\}.$$

If C is dependent, then clearly all $X \in [C;D]$ are dependent; similarly, if D is codependent, then all $X \in [C;D]$ are dependent. If C is independent and D is coindependent, then $M/C\backslash D$ is a minor of rank a on the set $E \setminus (C \cup D)$ of cardinality b. By assumption, this minor cannot be uniform, and so at least one set $Y \subseteq E \setminus (C \cup D)$ with $|Y| = a$ is a nonbasis of $M/C\backslash D$. For such a set Y, it follows that $Y \cup C \in [C;D]$ is dependent. Summarising, at least one of the $\binom{b}{a}$ elements of $[C;D]$ is a nonbasis of M. Summing over all pairs (C, D), we obtain that at least a $1/\binom{b}{a}$-fraction of the elements in $\binom{E(M)}{r}$ are nonbases. □

The following theorem uses Lemma 7.6.2 to show that, under certain conditions on a and b, almost every matroid has a $U(a, b)$-minor.

Theorem 7.6.3. *There is a constant $c > 0$ for which the following holds: If $a \equiv a(n)$ and $b \equiv b(n)$ are integer functions satisfying $0 \leq a \leq b$, and $\binom{b}{a} \leq c\frac{n}{\log^3 n}$ for all $n \geq n_0$, then almost every matroid has a $U(a(|M|), b(|M|))$-minor.*

Proof. Let $\mathcal{M}$ be the class of matroids with $d(M) \leq \upsilon(|M|) + 2/|M|$. By Lemma 7.2.7 and Lemma 7.2.3, almost every matroid is in $\mathcal{M}$, so to prove the theorem, it suffices to show that matroids in $\mathcal{M} \cap \mathbb{M}(n)$ have a $U(a, b)$-minor, whenever n is sufficiently large.

As $\upsilon(n) + 2/n = O\left(\frac{\log^3 n}{n}\right)$, there exist $c' > 0$ and n_1 such that $\upsilon(n) + 2/n < \frac{\log^3 n}{c'n}$ for all $n \geq n_1$. Let $n \geq \max\{n_0, n_1\}$, and let $M \in \mathcal{M} \cap \mathbb{M}(n)$. For the sake of contradiction, suppose that M does not have a $U(a, b)$-minor. By Lemma 7.6.2, we have

$$\frac{\log^3 n}{cn} \leq 1/\binom{b}{a} \leq d(M) \leq \upsilon(M) + 2/n \leq \frac{\log^3 n}{c'n},$$

which fails if we choose $c < c'$. In that case, M must have a $U(a, b)$-minor. □

Theorem 7.6.1 follows as a special case of Theorem 7.6.3. It also follows as a special case that almost every matroid contains a very long line as a minor.

Corollary 7.6.4. *There exists a constant $c > 0$ such that, asymptotically, almost every matroid on n elements has a $U(2, k)$-minor, where $k = c\frac{\sqrt{n}}{\log^{3/2} n}$.*

7.7 Symmetry

In this section, we describe progress on Conjecture 1.3.4, which we repeat here for convenience.

> **Conjecture 1.3.4** ([MNWW11, Conjecture 1.2]). *Almost every matroid is asymmetric.*

We present two partial resolutions to this conjecture. The first result states that almost every matroid is, in a precise sense, close to being asymmetric. A transposition is a permutation that exchanges two elements of the ground set.

Theorem 7.7.1. *Almost every matroid has an automorphism group that is either trivial or generated by a transposition.*

Our methods are not sufficiently strong to preclude the possibility of automorphisms generated by transpositions in general matroids. The class of sparse paving matroids offers considerably more traction, and we are able to prove Conjecture 1.3.4 for this class of matroids.

Theorem 7.7.2. *Almost every sparse paving matroid is asymmetric.*

Theorem 7.7.1 stops just short of proving Conjecture 1.3.4. At the end of this section, we investigate how close to proving the full conjecture we are. In particular, we prove the following connection between Conjecture 1.3.4 and the problem of enumerating matroids.

Theorem 7.7.3. *If* $\liminf_{n\to\infty} \frac{\log m(n)}{\frac{1}{n}\binom{n}{n/2}} > 1$ *or* $\limsup_{n\to\infty} \frac{\log m(n)}{\frac{1}{n}\binom{n}{n/2}} < 2$*, then almost every matroids is asymmetric.*

Notation and terminology

Before proving Theorem 7.7.1 and Theorem 7.7.2, we establish some additional notation that is required in this section.

We write $\mathrm{Sym}(n)$ for the symmetric group on $[n]$, and id for the identity element in this group. Elements of $\mathrm{Sym}(n)$ are called *permutations*; throughout this section, π will always be a permutation.

The *order* of π, denoted $\mathrm{Ord}(\pi)$, is defined as the smallest positive integer k such that $\pi^k = \mathrm{id}$. We write $\mathrm{Supp}(\pi) := \{e \in [n] : \pi(e) \neq e\}$ for the *support* of π.

A permutation π is a *cycle* if there exists a subset $\{e_1, e_2, \dots, e_k\} \subseteq [n]$ such that $\pi(e_i) = e_{i+1}$ for $i = 1, 2, \dots, k-1$, and $\pi(e_k) = e_1$, while π fixes every other element. If this is the case, then we write $\pi = (e_1, e_2, \dots, e_k)$. It is clear that $\mathrm{Supp}(\pi) = \{e_1, e_2, \dots, e_k\}$ in this case. A cycle $\pi = (e_1, e_2)$, whose support contains precisely two elements, is called a *transposition.*

Every permutation π admits a representation as a product of disjoint cycles, i.e. $\pi = \gamma_1\gamma_2\dots\gamma_M$, with γ_i a cycle for each i, and $\mathrm{Supp}(\gamma_i) \cap \mathrm{Supp}(\gamma_j) = \emptyset$ whenever $i \neq j$. This is called the *disjoint cycle decomposition* of π. A cycle of length 1 is simply a fixed point of π; we will always suppress such cycles in the disjoint cycle decomposition. The disjoint cycle decomposition is unique up to the order of the factors.

The group $\mathrm{Sym}(n)$ acts pointwise on $\binom{[n]}{r}$; if $X \in \binom{[n]}{r}$, then we write $\pi(X) := \{\pi(x) : x \in X\}$. For $\pi \in \mathrm{Sym}(n)$ and $X \in \binom{[n]}{r}$, we write $\mathrm{Orb}_\pi(X) := \{X, \pi(X), \pi^2(X), \ldots\}$; we suppress the subscript π if the permutation if clear from the context. Clearly, the cardinality of $\mathrm{Orb}_\pi(X)$ is at most the order of π, and in fact $|\mathrm{Orb}_\pi(X)|$ always divides $\mathrm{Ord}(\pi)$. Note that $\mathrm{Orb}_\pi(X)$ is a singleton if and only if $\pi(X) = X$.

A subset $\mathcal{X} \subseteq \binom{[n]}{r}$ is called *π-invariant* if $\pi(X) \in \mathcal{X}$ for all $X \in \mathcal{X}$. This is the case precisely when $\mathcal{X}$ is the union of π-orbits.

It follows from Proposition 2.6.1 that every $\pi \in \mathrm{Sym}(n)$ is an automorphism of the Johnson graph $J(n, r)$. The image of a stable set under π is again a stable set, and we write $\mathrm{ind}(J(n, r); \pi)$ for the number of π-invariant stable sets in $J(n, r)$.

Outline of the proof

We write $\mathbb{M}(n, r; \pi)$ for the rank-r matroids on $[n]$ that have π as an automorphism, i.e.

$$\mathbb{M}(n, r; \pi) := \{M \in \mathbb{M}(n, r) : \pi \in \mathrm{Aut}(M)\},$$

and $\mathbb{M}(n; \pi) := \bigcup_{r=0}^{n} \mathbb{M}(n, r; \pi)$. Moreover, for any subset $\Sigma \subseteq \mathrm{Sym}(n)$, we define $\mathbb{M}(n, r; \Sigma) = \bigcup_{\pi \in \Sigma} \mathbb{M}(n, r; \pi)$, and $\mathbb{M}(n; \Sigma) := \bigcup_{\pi \in \Sigma} \mathbb{M}(n; \pi)$. Lowercase letters are used to denote cardinalities, e.g. $m(n, r; \pi) := |\mathbb{M}(n, r; \pi)|$, and so on.

Analogously, we write $\mathbb{S}(n, r; \pi)$ for the sparse paving matroids in $\mathbb{S}(n, r)$ that have π as an automorphism, $s(n, r; \pi)$ for its cardinality, and so on.

Two sets of permutations play a prominent role; these are

$$\begin{aligned}\Sigma_{\geq 3} &:= \{\pi \in \mathrm{Sym}(n) : |\mathrm{Supp}(\pi)| \geq 3\}, \quad \text{and}\\ \Sigma_2 &:= \{\pi \in \mathrm{Sym}(n) : |\mathrm{Supp}(\pi)| = 2\}.\end{aligned}$$

Note that Σ_2 is precisely the set of transpositions in $\mathrm{Sym}(n)$. We prove the following lemmas.

Lemma 7.7.4. *$m(n; \Sigma_{\geq 3}) = o(s(n))$ as $n \to \infty$.*

Lemma 7.7.5. *$s(n; \Sigma_2) = o(s(n))$ as $n \to \infty$.*

It is easily seen that Lemma 7.7.4 and Lemma 7.7.5 together imply Theorem 7.7.1 and Theorem 7.7.2.

Interestingly, Lemma 7.7.4 and Lemma 7.7.5 are proved using different approaches. A central role in the proof of Lemma 7.7.4 will be played by the circuit-hyperplanes of matroids whose automorphism groups contain a given permutation π. Such circuit-hyperplanes form a π-invariant stable set in $J(n,r)$, and we show that there are few such stable sets. On the other hand, Lemma 7.7.5 is proved by showing that if $\pi \in \Sigma_2$, then each π-invariant sparse paving matroid gives rise to a large number of sparse paving matroids that are not π-invariant and from which the original matroid can be reconstructed.

Permutations that move at least three elements

Let $M \in \mathbb{M}(n,r)$, and $\pi \in S_n$. Observe that if $\pi \in \mathrm{Aut}(M)$, then $\mathcal{W}(M)$ is a π-invariant stable set in $J(n,r)$. In the other direction, every π-invariant stable set in $J(n,r)$ corresponds to a sparse paving matroid that has π as an automorphism, so

$$\left|\left\{\mathcal{W}(M) : M \in \mathbb{M}(n,r;\pi)\right\}\right| = \mathrm{ind}(J(n,r);\pi)\,.$$

We show that if $\pi \in \Sigma_{\geq 3}$, then the number of π-invariant stable sets in $J(n,r)$ is small—so small in fact, that even after summing over all $\pi \in \Sigma_{\geq 3}$, the resulting bound on $|\{\mathcal{W}(M) : M \in \mathbb{M}(n,r;\Sigma_{\geq 3})\}|$ is sufficiently small for an application of Theorem 6.8.5, which then implies Lemma 7.7.4.

For a permutation $\pi \in S_n$, write

$$F(\pi) := \left\{X \in \binom{[n]}{r} : \pi(X) = X\right\}$$

for the collection of r-sets that are fixed under π. Recall that we use $\mathrm{Ind}(J(n,r);\pi)$ for the collection of all π-invariant stable sets in $J(n,r)$; we identify two special subsets of $\mathrm{Ind}(J(n,r);\pi)$, namely

$$\mathrm{Ind}^0(J(n,r);\pi) := \{I \in \mathrm{Ind}(J(n,r);\pi) : I \subseteq F(\pi)\}\,,$$

and

$$\mathrm{Ind}^+(J(n,r);\pi) := \{I \in \mathrm{Ind}(J(n,r);\pi) : I \cap F(\pi) = \emptyset\}\,.$$

Each $I \in \mathrm{Ind}(J(n,r);\pi)$ is partitioned as $I = I^0 \cup I^+$, where $I^0 := I \cap F(\pi) \in \mathrm{Ind}^0(J(n,r);\pi)$, and $I^+ := I \setminus F(\pi) \in \mathrm{Ind}^+(J(n,r);\pi)$. We use lower case letters to denote cardinality, so

$$\mathrm{ind}^0(J(n,r);\pi) := |\,\mathrm{Ind}^0(J(n,r);\pi)\,|,$$

and

$$\mathrm{ind}^+(J(n,r);\pi) := |\,\mathrm{Ind}^+(J(n,r);\pi)\,|.$$

It follows that

$$\operatorname{ind}(J(n,r);\pi) = \operatorname{ind}^0(J(n,r);\pi) \ \times \ \operatorname{ind}^+(J(n,r);\pi)\,.$$

Hence, in order to bound $\operatorname{ind}(J(n,r);\pi)$, it suffices to bound the two factors on the right-hand side separately.

The following lemma bounds $\operatorname{ind}^0(J(n,r);\pi)$ in terms of stable sets in smaller Johnson graphs.

Lemma 7.7.6. *For all $0 \le r \le n$, if $\pi \in S_n$ has a disjoint cycle decomposition $\pi = \gamma_1\gamma_2\dots\gamma_M$, in which γ_j has length $\ell_j = |\operatorname{Supp}(\gamma_j)|$, then*

$$\log \operatorname{ind}^0(J(n,r);\pi) \le 2^M \log s(n-m),$$

where $m = |\operatorname{Supp}(\pi)|$.

Proof. If $X \in F(\pi)$, then for each $j \in [M]$ either $\operatorname{Supp}(\gamma_j) \cap X = \emptyset$, or $\operatorname{Supp}(\gamma_j) \subseteq X$. Let

$$P_{\mathcal{J}} := \left\{ X \in \binom{[n]}{r} : X \cap \operatorname{Supp}(\pi) = \bigcup_{j\in\mathcal{J}} \operatorname{Supp}(\gamma_j) \right\}.$$

The subgraph of $J(n,r)$ induced by $P_{\mathcal{J}}$ is isomorphic to $J(n-m,r')$, where $r' = r - \sum_{j\in\mathcal{J}} \ell_j$.

If $X \in F(\pi)$, then there exists a unique $\mathcal{J} \subseteq [M]$ such that $X \in P_{\mathcal{J}}$. It follows that if $I \in \operatorname{Ind}^0(J(n,r);\pi)$, then $\{I \cap P_{\mathcal{J}} : \mathcal{J} \subseteq [M]\}$ partitions I. As each $I \cap P_{\mathcal{J}}$ is a stable set in $J(n,r)[P_{\mathcal{J}}]$, it follows that,

$$\log \operatorname{ind}^0(J(n,r);\pi) \le \sum_{\mathcal{J}\subseteq[M]} \log \operatorname{ind}\left(J\left(n-m, r - \sum_{j\in\mathcal{J}} \ell_j \right)\right).$$

The lemma now follows since $\operatorname{ind}(J(n-m,r')) \le s(n-m)$ for all r'. □

Lemma 7.7.7. $\max\limits_{\substack{\pi\in\Sigma_{\ge 3}\\ 0\le r\le n}} \log \operatorname{ind}^0(J(n,r);\pi) \le \left(\tfrac{1}{2}+o(1)\right) \log s(n)$ *as* $n\to\infty$.

Proof. By Lemma 7.7.6, $\log \operatorname{ind}^0(J(n,r);\pi) \le 2^M \log s(n-m)$, where $m = |\operatorname{Supp}(\pi)|$ and M is the number of cycles in the disjoint cycle representation of π, for all $\pi \in S_n$ and all $0 \le r \le n$. As $M \le \lfloor m/2 \rfloor$, it follows that

$$\max_{\substack{\pi\in S_{\ge 3}\\ 0\le r\le n}} \log \operatorname{ind}^0(J(n,r);\pi) \le \max_{3\le m\le n} 2^{\lfloor m/2\rfloor} \log s(n-m). \tag{7.9}$$

It remains to bound the right-hand side of (7.9). First, we focus on the case that m is large, i.e. $m \geq \left\lceil \frac{2n}{3} \right\rceil$. We have

$$\begin{aligned}
\max_{\left\lceil \frac{2n}{3} \right\rceil \leq m \leq n} & 2^{\lfloor m/2 \rfloor} \log s(n-m) \\
&\leq 2^{\lfloor n/2 \rfloor} \log s(\lfloor n/3 \rfloor) \\
&\leq 2^{\lfloor n/2 \rfloor} \frac{6+o(1)}{n} \binom{\lfloor n/3 \rfloor}{\lfloor n/6 \rfloor} \qquad \text{by Theorem 6.5.2} \qquad (7.10) \\
&\leq \frac{6\sqrt{3}+o(1)}{n} \binom{n}{\lfloor n/2 \rfloor} 2^{-n/6} \qquad \text{by (2.1)} \\
&= o(\log s(n)),
\end{aligned}$$

where the final step follows since $\log s(n) \geq \frac{1}{n}\binom{n}{n/2}$.

Next, consider the case that m is small, i.e. $3 \leq m \leq \left\lfloor \frac{2n}{3} \right\rfloor$. As $n - m \to \infty$, an application of Theorem 6.5.2 shows that

$$2^{\lfloor m/2 \rfloor} s(n-m) \leq 2^{\lfloor m/2 \rfloor} \frac{2+o(1)}{n-m} \binom{n-m}{\left\lfloor \frac{n-m}{2} \right\rfloor},$$

which, by (2.1), is at most

$$\begin{aligned}
2^{\lfloor m/2 \rfloor} & \frac{2+o(1)}{n-m} \sqrt{\frac{n}{n-m}} 2^{-m} \binom{n}{\lfloor n/2 \rfloor} \\
&\leq 2^{-\lceil m/2 \rceil} (2+o(1)) \left(\frac{n}{n-m} \right)^{3/2} \log s(n),
\end{aligned}$$

so that

$$\max_{3 \leq m \leq \left\lfloor \frac{2n}{3} \right\rfloor} 2^{\lfloor m/2 \rfloor} s(n-m) \leq (1/2 + o(1)) \log s(n). \qquad (7.11)$$

Combining (7.10) and (7.11) with (7.9) proves the lemma. □

Observe that if I is a π-invariant stable set, and $I' \subseteq I$ contains at least one vertex from each π-orbit that is contained in I, then I can be reconstructed by closing I' under π-images. This observation is used to prove the following lemma.

Lemma 7.7.8. *There exists $\varepsilon > 0$ such that for sufficiently large n and all $0 \leq r \leq n$, if $\pi \in \Sigma_{\geq 3}$, then $\log \operatorname{ind}(J(n,r);\pi) \leq (1-\varepsilon)\log s(n)$.*

Proof. For a π-invariant stable set I in $J(n,r)$, let us write $\lambda(I)$ for the number of "large" orbits that it contains (i.e. orbits consisting of at least two vertices).

Let $\Lambda := \frac{1}{13}\log s(n)$. Call I "complex" if $\lambda(I) > \Lambda$. Either the majority of π-invariant stable sets is complex, or the majority is non-complex. We show that $\operatorname{ind}(J(n,r);\pi)$ is small either way.

Case I: Most π-invariant stable sets are complex. Each complex set gives rise to at least $3^{\lambda(I)} \geq 3^{\Lambda}$ stable sets, since we can take any non-empty subset from each large orbit. By the previous paragraph, I can be reconstructed from each such subset. Hence, if at least half of the π-invariant stable sets are complex, then

$$\operatorname{ind}(J(n,r);\pi) \leq 2\operatorname{ind}(J(n,r))\,3^{-\frac{1}{13}\log s(n)} \leq 2s(n)^{1-\frac{\log 3}{13}},$$

and the lemma follows.

Case II: Most π-invariant stable sets are non-complex. Suppose that at least half of the π-invariant stable sets are non-complex, i.e. $\lambda(I) \leq \Lambda$. Recall that each π-invariant stable set I can be written as the disjoint union of $I^0 \in \operatorname{ind}^0(J(n,r);\pi)$ and $I^+ \in \operatorname{ind}^+(J(n,r);\pi)$. We bound separately the number of I^0 and I^+ associated with non-complex I in this way.

Note that I^+ can be reconstructed from a stable set of size $\lambda(I^+) = \lambda(I) \leq \Lambda$: such a set can be constructed by restricting I^+ to a set containing a single vertex from each of its orbits, and I^+ can be obtained from this subset by closing it under π-images. Thus, the number of possible I^+ is at most $\operatorname{ind}(J(n,r), \leq \Lambda)$, which is bounded by Lemma 6.5.3. We obtain that, for sufficiently large n, the logarithm of the number of possible I^+ is at most

$$\log\operatorname{ind}(J(n,r), \leq \Lambda) \leq 0.48\log s(n). \tag{7.12}$$

An application of Lemma 7.7.7 shows that, for sufficiently large n,

$$\log\operatorname{ind}^0(J(n,r);\pi) \leq 0.51\log s(n). \tag{7.13}$$

Combining (7.12) and (7.13) shows that

$$\log\operatorname{ind}(J(n,r);\pi) \leq 1 + 0.48\log s(n) + 0.51\log s(n),$$

which proves the lemma. □

We are now ready to prove Lemma 7.7.4.

Proof of Lemma 7.7.4. By (7.7),

$$|\{\mathcal{W}(M) : M \in \mathbb{M}(n,r;\Sigma_{\geq 3})\}| \leq \sum_{\pi\in\Sigma_{\geq 3}} \operatorname{ind}(J(n,r);\pi)\,.$$

The number of terms in the last summation is at most $|\Sigma_{\geq 3}| \leq n! \leq n^n$, while (at least for large n) each term separately is bounded by Lemma 7.7.8. Thus, there exists $\varepsilon > 0$ such that, for sufficiently large n,

$$\begin{aligned}\log |\{\mathcal{W}(M) : M \in \mathbb{M}(n, r; \Sigma_{\geq 3})\}| \\ \leq n \log n + (1-\varepsilon) \log s(n) \leq (1-\varepsilon/2) \log s(n),\end{aligned}$$

for all $0 \leq r \leq n$. The lemma now follows from an application of Theorem 6.8.5. □

Transpositions

Let $\pi = (e, f) \in \Sigma_2$ be a transposition. Recall that (π-invariant) sparse paving matroids of rank r on ground set $[n]$ are in one-to-one correspondence with (π-invariant) stable sets in $J(n, r)$. The main step in the proof of Lemma 7.7.5 is showing that we can associate to any π-invariant stable set in $J(n, r)$ a large family of stable sets that are not π-invariant.

The transposition π partitions the vertex set of $J(n, r)$ into four classes, based on the intersection with the set $\{e, f\}$. Let us write $V_\emptyset$, V_e, V_f, and $V_{e,f}$ for the vertices in $J(n, r)$ whose intersection with $\{e, f\}$ is indicated by the subscript, and write $J(n, r)_\xi := J(n, r)[V_\xi]$ for the corresponding induced subgraph. Each of these graphs is isomorphic to a Johnson graph with smaller parameters, to wit

$$\begin{gathered} J(n, r)_\emptyset \cong J(n-2, r), \\ J(n, r)_e \cong J(n, r)_f \cong J(n-2, r-1), \quad \text{and} \\ J(n, r)_{e,f} \cong J(n-2, r-2). \end{gathered}$$

Moreover, there is precisely a matching between the vertices in V_e and those in V_f. It follows that $J(n, r)[V_e \cup V_f] \cong J(n-2, r-1) \square K_2$, the *Cartesian product* of $J(n-2, r-1)$ and K_2.

Each π-invariant stable set is contained in $V_\emptyset \cup V_{e,f}$; for if $X \in V_e \cup V_f$ is in the stable set, then so is $\pi(X) = X \triangle \{e, f\}$. However, X is adjacent to $X \triangle \{e, f\}$, thus contradicting stability. In fact, not only is every π-invariant stable set contained in $V_\emptyset \cup V_{e,f}$, but every π-invariant stable set in $J(n, r)$ can be constructed by combining a stable set in $V_\emptyset$ and a stable set in $V_{e,f}$. In particular, this means that

$$\operatorname{ind}(J(n, r); \pi) = \operatorname{ind}(J(n-2, r-2)) \times \operatorname{ind}(J(n-2, r)).$$

Clearly $\operatorname{ind}(J(n, r); \pi) \leq \operatorname{ind}(J(n, r))$. The following lemma gives a family of related bounds.

Lemma 7.7.9. *For all $k \geq 0$,*

$$\operatorname{ind}(J(n,r);\pi) \times \operatorname{ind}(J(n-2,r-1)\Box K_2,k) \leq (r(n-r))^k \operatorname{ind}(J(n,r)).$$

Proof. We prove the lemma by counting in two ways the number of pairs (I,A), where I is a π-invariant stable set in $J(n,r)$, and A is a stable set of cardinality k in $J(n,r)[V_e \cup V_f]$.

On the one hand, the number of such pairs is exactly $\operatorname{ind}(J(n,r);\pi)\times \operatorname{ind}(J(n-2,r-1)\Box K_2,k)$. On the other hand, we show that the number of such pairs is at most $\operatorname{ind}(J(n,r)) \times (r(n-r))^k$. Together, these two observations prove the lemma.

To prove the second observation, consider the function F which maps pairs (I,A) to $I \cup A \setminus N(A)$. Clearly, for each pair (I,A), $F(I,A)$ is a stable set in $J(n,r)$. We claim that at most $(r(n-r))^k$ of the pairs give rise to the same image under F.

Starting from $F(I,A)$, note that A is determined by $A = F(I,A) \cap (V_e \cup V_f)$; here we use that $I \subseteq V_\emptyset \cup V_{e,f}$, while $A \subseteq V_e \cup V_f$. It remains to reconstruct $I \cap N(A)$. A vertex $X \in V_e \cup V_f$ has exactly $n-r-1$ neighbours among the vertices in $V_\emptyset$ (and these vertices form a clique), and it has $r-1$ neighbours among the vertices in $V_{e,f}$ (and these form a clique as well). Thus, for each $X \in A$, $I \cap N(X)$ can take at most $r(n-r)$ different values. The claim follows by taking the product over all $X \in A$. □

We are now ready to prove Lemma 7.7.5.

Proof of Lemma 7.7.5. Let $R_n = \left\{r \in \mathbb{Z}_{\geq 0} : \left|r - \frac{n}{2}\right| \leq \sqrt{n}\right\}$. By Theorem 7.3.1, almost every matroid has $\operatorname{rk}(M) \in R_{|M|}$, in view of which it suffices to show that

$$\sum_{r \in R_n} s(n,r;\Sigma_2) = o(s(n)) \qquad \text{as } n \to \infty. \tag{7.14}$$

By Lemma 2.2.1, there is a constant $c > 0$ such that, for sufficiently large n, $\binom{n-2}{r-1} = \frac{r(n-r)}{n(n-1)}\binom{n}{r} \geq c\frac{2^n}{\sqrt{n}}$, uniformly over $r \in R_n$. Fix any transposition $\pi \in \Sigma_2$. By Lemma 7.7.9, applied here with $k = 1$,

$$s(n,r;\pi) = \operatorname{ind}(J(n,r);\pi) \leq \frac{r(n-r)}{2\binom{n-2}{r-1}} \operatorname{ind}(J(n,r)) \leq \frac{n^2\sqrt{n}}{8c2^n} s(n)$$

for sufficiently large n. As $|R_n| \leq 2\sqrt{n}+1$ and $|\Sigma_2| = \binom{n}{2}$, it follows that

$$\sum_{r \in R_n} s(n,r;\Sigma_2) \leq \sum_{r \in R_n}\sum_{\pi \in \Sigma_2} s(n,r;\pi) \leq (1+o(1))\frac{n^5}{8c2^n} s(n).$$

which proves (7.14) and hence Lemma 7.7.5. □

Towards a proof of Conjecture 1.3.4

The method used to prove Lemma 7.7.4 does not give sufficient traction on matroids whose automorphism groups are generated by a transposition to extend to a proof of the full Conjecture 1.3.4. In this section, we investigate such matroids a little closer, and prove Theorem 7.7.3.

For a transposition $\pi = (e, f)$, write

$$\mathbb{T}(n; \pi) := \{M \in \mathbb{M}(n) : \mathrm{Aut}(M) = \langle \pi \rangle\}$$

for the collection of matroids on $[n]$ whose automorphism group is generated by π, and write $t(n; \pi) := |\mathbb{T}(n; \pi)|$ for its cardinality. In addition, let $\mathbb{T}(n) := \bigcup_{\pi \in \Sigma_2} \mathbb{T}(n; \pi)$, and $t(n) := |\mathbb{T}(n)|$. In view of Theorem 7.7.1, the following conjecture is tantamount to proving Conjecture 1.3.4.

Conjecture 7.7.10. $\lim_{n\to\infty} \frac{t(n)}{m(n)} = 0$.

One might hope that the proof of Lemma 7.7.5 for sparse paving matroids generalises to matroids that are not necessarily sparse paving. The proof of Lemma 7.7.5 is based on the construction of a large number of sparse paving matroids associated with a given π-invariant sparse paving matroid. The construction works by forcing an element from the set $V_e \cup V_f$ into the nonbases of a π-invariant sparse paving matroid.

In the case of sparse paving matroids such a construction works for two reasons. First, all elements of $V_e \cup V_f$ are bases of π-invariant sparse paving matroids, so forcing such an element to be a nonbasis will result in a sparse paving matroid that is not π-invariant. Second, each such element has few neighbours among the nonbases in the original matroid. Both ideas are more complicated for matroids that are not necessarily sparse paving: in such matroids, it may happen that $V_e \cup V_f$ contains nonbases, and the collection of nonbases in the neighbourhood of any such set has a much more complicated structure. Avoiding both complications may result in a proof of Conjecture 7.7.10.

Alternatively, we may consider what happens if Conjecture 1.3.4 fails.

Lemma 7.7.11. *Let $\pi = (e, f)$ be a transposition, and let $M \in \mathbb{M}(n, r; \pi)$. M is uniquely determined by $M\backslash e, f$ and $M/e, f$.*

Proof. Note that $r-2 \le \mathrm{rk}(M/e, f) \le \mathrm{rk}(M\backslash e, f) \le r$. If $\mathrm{rk}(M/e, f) = r$, then e and f are both loops in M, and M is obtained from $M\backslash e, f$ by adjoining two loops. Similarly, if $\mathrm{rk}(M/e, f) = \mathrm{rk}(M\backslash e, f) = r-2$, then e and f are both coloops, and M is obtained from $M\backslash e, f$ by adjoining two coloops. If $\mathrm{rk}(M/e, f) = \mathrm{rk}(M\backslash e, f) = r - 1$, then $\{e, f\}$ is both a circuit and a cocircuit, and M is obtained from $M\backslash e, f$ by first adjoining a coloop e, and then adding f in parallel to e.

If $\operatorname{rk}(M/e, f) = r - 1$ and $\operatorname{rk}(M\backslash e, f) = r$, then e and f are in parallel. In this case, every basis of M is either disjoint from $\{e, f\}$ (in which case it is a basis of $M\backslash e, f)$), or intersects $\{e, f\}$ in precisely one element (in which case $B \setminus \{e, f\}$ is a basis of $M/e, f$). The collection of bases of M can be obtained from $M/e, f$ and $M\backslash e, f$ through

$$\begin{aligned}\mathcal{B}(M) = \mathcal{B}(M\backslash e, f) &\cup \{B \cup \{e\} : B \in \mathcal{B}(M/e, f)\} \\ &\cup \{B \cup \{f\} : B \in \mathcal{B}(M/e, f)\}.\end{aligned}$$

Similarly, if $\operatorname{rk}(M/e, f) = r - 2$ and $\operatorname{rk}(M\backslash e, f) = r - 1$, then

$$\begin{aligned}\mathcal{B}(M) = \{B \cup \{e, f\} : B \in \mathcal{B}(M/e, f)\} &\cup \{B \cup \{e\} : B \in \mathcal{B}(M\backslash e, f)\} \\ &\cup \{B \cup \{f\} : B \in \mathcal{B}(M\backslash e, f)\}.\end{aligned}$$

The case $\operatorname{rk}(M/e, f) = r - 2$ and $\operatorname{rk}(M\backslash e, f) = r$ remains. In this case, a basis of M can have any of the four possible intersections with $\{e, f\}$. The bases that do not intersect $\{e, f\}$ are precisely $\mathcal{B}(M\backslash e, f)$, while the bases that contain both e and f are given by $\{B \cup \{e, f\} : B \in \mathcal{B}(M/e, f)\}$. Let X be an r-set that contains e but not f. In M, the set X is a nonbasis if and only if $X \setminus \{e\}$ contains a circuit or $X \cup \{f\}$ is contained in a hyperplane. The former happens precisely when every r-subset that contains $X \setminus \{e\}$ and avoids f is a nonbasis in $M\backslash e, f$, while the latter happens precisely when every $(r - 2)$-subset that is contained in $X \cup \{f\}$ is a nonbasis of $M/e, f$. It follows that the collection $\mathcal{K}$ of nonbases of M that contain e but not f is given by

$$\begin{aligned}\mathcal{K} = &\left\{ X \in \binom{[n]}{r} : \begin{array}{c} e \in X, f \notin X, \\ (X \setminus \{e\}) \cup \{g\} \notin \mathcal{B}(M\backslash e, f) \\ \hfill \text{for all } g \in E \setminus (X \cup \{f\}) \end{array} \right\} \\ &\qquad \cup \left\{ X \in \binom{[n]}{r} : \begin{array}{c} e \in X, f \notin X, \\ X \setminus \{e, h\} \notin \mathcal{B}(M/e, f) \\ \hfill \text{for all } h \in X \setminus \{e\} \end{array} \right\},\end{aligned}$$

which depends only on $M/e, f$ and $M\backslash e, f$. As π is an automorphism of M, the bases of M that contain exactly one of e and f are precisely the complement of $\mathcal{K} \cup \{K \triangle \{e, f\} : K \in \mathcal{K}\}$ in the collection of all r-sets that contain exactly one of e and f. □

Let M be a matroid of rank r, and let $\pi = (e, f)$ be a transposition that swaps two elements of the ground set of M. It follows from the lemma and the fact that $r-2 \le \operatorname{rk}(M/e,f) \le \operatorname{rk}(M\backslash e,f) \le r$ that

$$\begin{aligned} m(n,r;\pi) &\le \big[m(n-2,r-2)+m(n-2,r-1)+m(n-2,r)\big]^2 \\ &\le m(n-2)\big[m(n-2,r-2)+m(n-2,r-1)+m(n-2,r)\big]. \end{aligned}$$

Summing over r results in $t(n;\pi) \le 3(m(n-2))^2$, and hence

$$\log t(n;\pi) \le 2\log m(n-2) + \log 3. \tag{7.15}$$

The lower bound on $\log s(n)$ in Lemma 2.8.1 and the upper bound on $\log m(n)$ in Theorem 6.7.3 imply that

$$\liminf_{n\to\infty} \frac{\log m(n)}{\frac{1}{n}\binom{n}{n/2}} \ge 1 \qquad \text{and} \qquad \limsup_{n\to\infty} \frac{\log m(n)}{\frac{1}{n}\binom{n}{n/2}} \le 2. \tag{7.16}$$

We show that if the limit in Conjecture 7.7.10 exists, then it must be equal to 0.

Lemma 7.7.12. $\liminf\limits_{n\to\infty} \frac{t(n)}{m(n)} = 0.$

Proof. We argue by contradiction. If the lemma fails, there exists $\varepsilon > 0$ such that $t(n) \ge \varepsilon m(n)$, for all n sufficiently large. Fix a transposition $\pi \in \operatorname{Sym}(n)$. By symmetry, $t(n) = \binom{n}{2} t(n;\pi)$. It follows that $\log m(n) = (1+o(1))\log t(n;\pi)$ as $n \to \infty$. Combining this with (7.15) shows that $\log m(n) \le (2+o(1))\log m(n-2)$. Comparing this observation with (7.16), we obtain

$$\frac{1+o(1)}{n}\binom{n}{n/2} \le \log m(n) \le (2+o(1))\log m(n-2) \le \frac{4+o(1)}{n-2}\binom{n-2}{(n-2)/2}$$

as $n \to \infty$. As $\binom{n-2}{(n-2)/2} = (1/4+o(1))\binom{n}{n/2}$, it follows that

$$\lim_{n\to\infty} \frac{\log m(n)}{\frac{1}{n}\binom{n}{n/2}} = 1, \qquad \text{while} \qquad \lim_{n\to\infty} \frac{\log m(n-2)}{\frac{1}{n-2}\binom{n-2}{(n-2)/2}} = 2.$$

These two statements cannot hold simultaneously, and the lemma follows. □

The following lemma, whose proof follows the structure of that of Lemma 7.7.12, implies that if Conjecture 1.3.4 fails, then the inequalities of (7.16) hold with equality.

Lemma 7.7.13. *If* $\limsup\limits_{n\to\infty} \frac{t(n)}{m(n)} > 0$, *then* $\liminf\limits_{n\to\infty} \frac{\log m(n)}{\frac{1}{n}\binom{n}{\lfloor n/2\rfloor}} = 1$ *and* $\limsup\limits_{n\to\infty} \frac{\log m(n)}{\frac{1}{n}\binom{n}{\lfloor n/2\rfloor}} = 2.$

Theorem 7.7.3 follows, as it is simply the contrapositive statement of Lemma 7.7.13.

Finally, we relate Conjecture 1.3.4 to Conjecture 1.3.3, which states that almost every matroid has rank in the set $\{\lfloor |M|/2 \rfloor, \lceil |M|/2 \rceil\}$. Write

$$m'(n) := \sum_{r<\lfloor n/2 \rfloor} m(n,r) + \sum_{r>\lceil n/2 \rceil} m(n,r).$$

Recall the function $\zeta(n) = 57\frac{\log^2 n}{n^2}\binom{n}{n/2}$ from (6.21).

Lemma 7.7.14. *If $m'(n) \le m(n)2^{-2\zeta(n)}$, then Conjecture 7.7.10 holds.*

Proof. Write $\widetilde{m}(n,r;\pi)$ for the number of matroids in $\mathbb{M}(n,r;\pi)$ that are both simple and cosimple and define

$$f(n) := \begin{cases} \displaystyle\sum_{\pi\in\Sigma_2} \widetilde{m}(n,n/2;\pi) & \text{if } n \text{ is even,} \\ \displaystyle 2\sum_{\pi\in\Sigma_2} \widetilde{m}(n,(n-1)/2;\pi) & \text{if } n \text{ is odd.} \end{cases}$$

Let $\pi = (e,f)$ be a transposition. If the matroid M of rank r is simple and cosimple, then $\operatorname{rk}(M/e,f) = r-2$ and $\operatorname{rk}(M\backslash e,f) = r$. It follows from Lemma 7.7.11 that $\widetilde{m}(n,r;\pi) \le m(n-2,r-2)m(n-2,r)$ and hence $\widetilde{m}(n,\lfloor n/2 \rfloor;\pi) \le (m'(n-2))^2$. By the assumption,

$$\begin{aligned} \log f(n) &\le 1 + \log\binom{n}{2} + 2\log m'(n-2) \\ &\le 1 + \log\binom{n}{2} + 2\log m(n-2) - 4\zeta(n-2). \end{aligned}$$

Using the detailed bound from Theorem 6.7.3 to bound $\log m(n-2)$, and the lower bound $\log m(n) \ge \frac{1}{n}\binom{n}{n/2}$, we obtain

$$\log f(n) \le \log m(n) - \left(\frac{1}{2} - o(1)\right)\zeta(n),$$

and hence $f(n) = o(m(n))$ as $n \to \infty$. As almost every matroid is both simple and cosimple (by Corollary 7.3.4) and has rank in the set $\{\lfloor |M|/2 \rfloor, \lceil |M|/2 \rceil\}$ (by assumption), this implies that $t(n) = o(m(n))$, and hence that Conjecture 7.7.10 holds. □

CHAPTER **8**

Discussion and future work

8.1 In this chapter...

We revisit the conjectures stated in Chapter 1, indicating the progress made in this thesis. As in the introduction, the conjectures are subdivided roughly into three themes: enumeration, minor-closed classes, and connectivity.

In the final section, we sum up the main results of this thesis, and identify the most pregnant open questions in the area of asymptotic matroid theory.

8.2 Theme I: Enumeration

The first question introduced in Chapter 1 is the following.

> **Question 1.3.1.** *What is the asymptotic behaviour of $m(n)$?*

We obtained several bounds on the number of matroids, in particular, Theorem 6.1.1 states that

$$\frac{1}{n}\binom{n}{n/2} \leq \log s(n) \sim \log m(n) \leq \frac{2+o(1)}{n}\binom{n}{n/2}. \qquad (8.1)$$

Here, the first bound is the lower bound due to Graham and Sloane, and Kløve, see Section 2.8. The upper bound was proved in Theorem 6.7.3, while in Theorem 6.7.5 it was proved that $\log m(n) \sim \log s(n)$.

In Chapter 5, we obtained bounds on the quantity $m(n, r)$, using a number of different techniques. For comparison, several of these bounds

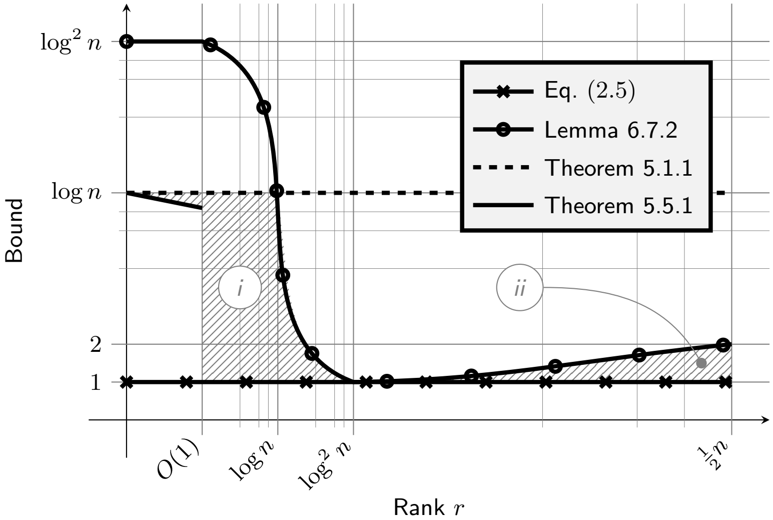


Figure 8.1: Sketch of some bounds on the function $r \mapsto \frac{m(n,r)}{\frac{1}{n}\binom{n}{r}}$.

are sketched in Figure 8.1. These bounds are on the rescaled function

$$r \mapsto \frac{\log m(n,r)}{\frac{1}{n}\binom{n}{r}}, \qquad r \leq n/2 \tag{8.2}$$

for large values of n. The shaded areas in this figure identify two regions in which the asymptotic behaviour of (8.2) is not conclusively determined. These regions correspond to (i) $r \to \infty$, but $r = o(n)$, and (ii) $r = \Theta(n)$. These areas identify two obvious questions for future research:

- Area (i) is related to extending the results of Chapter 5 to bounds on the number of matroids when the rank grows sublinearly with n;
- Area (ii) is of particular interest in the determination of the correct asymptotic behaviour of $\log m(n)$ in (8.1).

Sparse paving matroids

Sparse paving matroids play a pivotal role in matroid enumeration results. Not only is the best known lower bound obtained by the construction of a large family of sparse paving matroids, the method used to obtain the strongest upper bound in this thesis considers general matroids as small deviations from sparse paving matroids. This observation lends some credibility to the following conjecture.

Conjecture 1.3.2. *Almost every matroid is sparse paving.*

In Theorem 6.7.5, we have shown that $\log m(n) \sim \log s(n)$ as $n \to \infty$. Although this result may be seen as pointing in the direction of Conjecture 1.3.2, it is in fact a much weaker statement, owing to the slow growth of the logarithm. Indeed, as $\log s(n) \geq \frac{1}{n}\binom{n}{n/2}$, the asymptotic equivalence $\log m(n) \sim \log s(n)$ does not preclude the possibility that $m(n) = s(n) \exp\left(\frac{2^n}{n\sqrt{n}\omega(1)}\right)$, where $\omega(1)$ denotes a function that grows to infinitiy arbitrarily slowly with n; hence, the gap between $s(n)$ and $m(n)$ is potentially huge.

The proof of Theorem 6.7.5 relies on a careful application of the container method, in which it is shown that every matroid M that does not have any loops or coloops can be described by a sparse paving matroid (whose collection of circuit-hyperplanes contains the circuit-hyperplanes of M), and a relatively small amount of extra information. The extra information serves to reconstruct the collection $\mathcal{U}(M)$. It is likely that better bounds can be obtained by carefully weighing the extra information against the amount of information already present in the circuit-hyperplanes, although it is not clear how this can be implemented.

The right constant The upper and lower bound in (8.1) imply

$$\liminf_{n\to\infty} \frac{\log s(n)}{\frac{1}{n}\binom{n}{n/2}} \geq 1, \tag{8.3}$$

while

$$\limsup_{n\to\infty} \frac{\log s(n)}{\frac{1}{n}\binom{n}{n/2}} \leq 2. \tag{8.4}$$

Both statements remain true if $m(n)$ is replaced by $m(n)$. It is not known whether the inequalities (8.3)–(8.4) are strict, or indeed whether the limit $\lim\limits_{n\to\infty} \frac{\log s(n)}{\frac{1}{n}\binom{n}{n/2}}$ exists. In view of the central position of the enumeration results, it will be highly interesting to improve upon (8.3)–(8.4).

Existence of Steiner systems A positive answer to the following question would imply that (8.4) holds with equality.

Question 8.2.1. *Do there exist sequences of integers* (n_k) *and* (r_k) *such that for each* k *(i) an* $S(r_k - 1, r_k, n_k)$ *exists, while (ii)* $0 \leq \frac{n_k}{2} - r_k = o(\sqrt{n_k})$*?*

Recall that, in order for a Steiner system to exist, its parameters should satisfy certain divisibility conditions. The following lemma shows that these divisibility conditions for Steiner systems $S(r-1, r, 2r+k)$ are equivalent to primality of $r+k+1$.

Lemma 8.2.2. *The following are equivalent:*

(i) $r+k+1$ *is prime; and*

(ii) $r-i$ *divides* $\binom{2r+k-i}{r-1-i}$ *for all* $i \in \{0, 1, \ldots, r-2\}$.

Proof. Note that

$$\begin{aligned}\frac{1}{r-i}\binom{2r+k-i}{r-1-i} &= \frac{1}{r+k+1}\binom{2r+k-i}{r-i}\\ &= \frac{(2r+k-i)(2r+k-i-1)\ldots(r+k+1)}{(r+k+1)(r-i)!}, \qquad (8.5)\end{aligned}$$

so that (ii) holds if and only if $r+k+1$ divides $\binom{2r+k-i}{r-i}$ for all $i \in \{0, 1, \ldots, r-2\}$. The denominator of the right-hand side of (8.5) divides the numerator for all $i \in \{0, 1, \ldots, r-2\}$.

If $r+k+1$ is prime, then the numerator of the right-hand side of (8.5) contains only one factor equal to $r+k+1$, thus showing that $\binom{2r+k-i}{r-i}$ is divisible by $r+1$, which implies (ii).

To show the reverse implication, suppose that $r+k+1$ is composite. Let p be one of its prime factors, and suppose that $r+k+1$ is divisible by p^e, but not by p^{e+1}. Moreover, define q through $r+k+1 = pq$. Let $i = 2r+k-p(q+1)+1$, so that $2r+k-i = p(q+1)-1$ and $r-i = p$. For this choice of i, the numerator of the right-hand side of (8.5) is divisible by p^e but not by p^{e+1}, while the denominator contains is divisible by p^{e+1}. It follows that $r+k+1$ does not divide $\binom{2r+k-i}{r-i}$, and hence that (ii) does not hold. □

Lemma 8.2.2 implies that primality of $r+k+1$ is necessary for existence of Steiner systems $S(r-1, r, 2r+k)$. In Table 8.1, we indicate existence and nonexistence of the smallest such Steiner systems, for $k \leq 4$.

Based on the limited amount of information in the table, it is tempting to conjecture that Steiner systems $S(r-1, r, 2r+k)$ are not likely to exist except for sporadic small systems. However, such tables can be

Table 8.1: Existence of small Steiner systems $S(r-1, r, 2r+k)$. Source: [CM07] + updates. †All Steiner systems in this table are unique up to isomorphim.

k		Existence†	Remark
0	$S(1,2,4)$	Yes	Partition
	$S(3,4,8)$	Yes	Steiner quadruple system
	$S(5,6,12)$	Yes	Aut = Mathieu group M_{12}
	$S(9,10,20)$	No	Since $S(8,9,19)$ does not exist
	$S(11,12,24)$	No	[ÖP08]
1	$S(2,3,7)$	Yes	Fano plane

	$S(4,5,11)$	Yes	Steiner quintuple system;
			Aut = Mathieu group M_{11}

	$S(8,9,19)$	No	
	$S(10,11,23)$	No	[ÖP08]
2	$S(1,2,6)$	Yes	Partition
	$S(3,4,10)$	Yes	Steiner quadruple system
	$S(7,8,18)$	No	
	$S(9,10,22)$	No	[ÖP08]
3	$S(2,3,9)$	Yes	Steiner triple system
	$S(6,7,17)$	No	
	$S(8,9,21)$	No	[ÖP08]
4	$S(1,2,8)$	Yes	Partition
	$S(5,6,16)$	No	
	$S(7,8,20)$	No	[ÖP08]

deceiving; for example, no $S(6,7,n)$ are known, yet Keevash's [Kee14] recent breakthrough shows that such Steiner systems exist for sufficiently large n.

Results about Steiner systems $S(r-1, r, 2r+k)$ for large values of r appear to be scarce. The following result shows that if large $S(r-1, r, 2r)$ exist, then they are pretty wild. A flag in a Steiner system is a pair (v, X) consisting of an element v of the ground set, and a block X, such that $v \in X$.

Proposition 8.2.3 ([AH74])**.** *Suppose that $r > 6$. If a Steiner system $S(r-1, r, 2r)$ exists, then its automorphism group does not act transitively on its flags.*

Matroids that are not sparse paving Another result that is related to Conjecture 1.3.2 is Theorem 6.8.1, which asserts the existence of a class $\widehat{\mathbb{S}}$ of matroids that contains almost all matroids with the additional property that

$$Y(n) := \max_{0\leq r\leq n} \log \left|\left\{\mathcal{U}(M) : M \in \mathbb{M}(n,r) \cap \widehat{\mathbb{S}}\right\}\right| = O\left(\frac{\log^3 n}{n^2}\binom{n}{n/2}\right).$$

Conjecture 1.3.2 takes the extreme position that $\mathcal{U}(M) = \emptyset$ for almost all matroids, and hence that $Y(n) = 0$ for sufficiently large n. Thus, Theorem 6.8.1 allows for gradual progress towards resolution of Conjecture 1.3.2. For example, a more careful analysis of the proof of Theorem 6.8.1 may reveal that in fact $Y(n) = o\left(\frac{\log^3}{n^2}\binom{n}{n/2}\right)$, which is much weaker than Conjecture 1.3.2 but may be easier to prove.

In the analysis of matroids that are not sparse paving, complex components of nonbases play a crucial role. This raises the question what such complex components look like.

Question 8.2.4. *Let $U \subseteq V(J(n,r))$ be a set of vertices such that $J(n,r)[U]$ is a connected graph. What are necessary and sufficient conditions on U to form the set of non-bases of a matroid of rank r on $[n]$?*

The following lemma provides a necessary condition.

Lemma 8.2.5. *Let U be the set of non-bases of a matroid of rank r on $[n]$, such that $J(n,r)[U]$ is a connected graph. If u_1, u_2 are adjacent vertices in U, then there exists a maximal clique C of $J(n,r)$ such that $C \subseteq U$.*

Proof. The lemma obviously holds for singleton components. So suppose that $|U| \geq 2$, and let $X, X' \in U$ be two adjacent vertices. Let rk be the rank function of the matroid whose nonbases are U. By submodularity,

$$\mathrm{rk}(X \cup X') + \mathrm{rk}(X \cap X') \leq \mathrm{rk}(X) + \mathrm{rk}(X') \leq 2(r-1),$$

from which it follows that $\mathrm{rk}(X \cup X') \leq r-1$, or $\mathrm{rk}(X \cap X') \leq r-2$. In the first case, each r-subset of $X \cup X'$ is dependent, so $\binom{X\cup X'}{r} \subseteq U$. Moreover, $\binom{X\cup X'}{r}$ is a maximal clique in $J(n,r)$, so the lemma holds. In the second case, each r-set containing $X \cap X'$ is dependent, and it follows that $\left\{Y \in \binom{[n]}{r} : Y \supset X \cap X'\right\} \subseteq U$ is a maximal clique in $J(n,r)$, which again proves the lemma. □

It is easily verified that maximal cliques in $J(n, r)$ are in fact the simplest non-singleton connected components that appear as the set of nonbases of a matroid. The following conjecture, a proof of which may be easy, could be a stepping stone towards full resolution of Conjecture 1.3.2. Let $m'(n, r)$ denote the number of matroids of rank r on ground set $[n]$ with the property that $\mathcal{U}(M)$ precisely spans a maximal clique in $J(n, r)$, and let $m'(n) = \sum_{r=0}^{n} m'(n, r)$.

Conjecture 8.2.6. *$m'(n) = o(m(n))$.*

Structure of stable sets in $J(n, r)$

Consider the regime in which $n \to \infty$ and $|r - n/2| = o(\sqrt{n})$, so that $\binom{n}{r} \sim \binom{n}{n/2}$. We know that a sparse paving matroid in $\mathbb{S}(n, r)$ has at most $\frac{2}{n}\binom{n}{n/2}$ circuit-hyperplanes. However, only few sets of this cardinality occur as the set of circuit-hyperplanes of a sparse paving matroid. There are roughly $(\mathrm{e}n/c)^{\frac{c}{n}\binom{n}{n/2}}$ possible collections of r-sets of cardinality $\frac{c}{n}\binom{n}{n/2}$, which is much more than the number of sparse paving matroids with that number of circuit-hyperplanes (cf. 5.8.3), whenever $c = \Omega(1/\log n)$. Thus, an extremely small fraction of the vertex sets of this cardinality occurs as the set of circuit-hyperplanes. This points towards structure.

The container method makes this structure more explicit. There is a relatively small number of containers, each of size at most slightly larger than a maximum stable set (in fact, the Hoffman bound), such that each stable set is contained in one of these containers. We wonder how much such a result can be tightened. What we have in mind here is something along the following lines. In what follows, we will write $\mathrm{Ind}^*(G)$ for the collection of maximum stable sets in the graph G.

Conjecture 8.2.7. *Suppose that $|r - n/2| = o(\sqrt{n})$. Let $\boldsymbol{I}$ be drawn uniformly at random from $\mathrm{Ind}(J(n, r))$. With high probability, there exists $I^* \in \mathit{Ind}^*(J(n, r))$ such that*

(i) $\big||\boldsymbol{I} \cap I^*| - \frac{1}{2}|I^*|\big| = o\left(\frac{1}{n}\binom{n}{n/2}\right)$*; and*

(ii) $\max_{J \in \mathit{Ind}^*(J(n,r)) \setminus \{I^*\}} |\boldsymbol{I} \cap J| = o\left(\frac{1}{n}\binom{n}{n/2}\right)$.

Intuitively, the conjecture states that a random stable set in $J(n, r)$ looks like a random subset of one of its maximum stable sets. I have no good intuition as to whether the conjecture is true or false. Its formulation is based on hope as much as on circumstantial evidence.

Kahn [Kah01] showed that a version of Conjecture 8.2.7 holds for the hypercube graph Q_d, even if the uniform distribution is replaced by the more general hard-core distribution. He also showed that (i) holds in the more general setting of regular bipartite graphs. In such graphs, the structure of maximum stable sets is easily obtained: if the graph is connected, they are precisely the two colour classes of the bipartition. By contrast, it is not known what the maximum stable sets in the Johnson graph are. Identification of the maximum stable sets in $J(n,r)$ should be a useful first step towards proving results in the spirit of Conjecture 8.2.7.

Question 8.2.8. *What are the maximal stable sets in $J(n,r)$?*

Matroids of fixed rank

In Chapter 5, we proved that $\log s(n,r) \sim \log m(n,r) \sim \frac{\log n}{n}\binom{n}{n/2}$ as $n \to \infty$, for all $r \geq 3$. More precisely, it is shown in that chapter that

$$\frac{1}{n-r+1}\binom{n}{r}\log\left(\mathrm{e}^{1-r}n - o(n)\right) \leq \log s(n,r) \\ \leq \log m(n,r) \leq \frac{1}{n-r+1}\binom{n}{r}\log\left(\mathrm{e}(n-r+1)\right).$$

As indicated in Section 5.9, the upper bound is likely to be wasteful. In that section, we were able to improve the factor e inside the logarithm to $\mathrm{e}^{0.35}$, for rank-3 paving matroids. We believe that this is still not the best possible, and that in fact the lower bound is closer to the truth.

Conjecture 8.2.9. *For all fixed $r \geq 3$,*

$$\log m(n,r) = \frac{1}{n-r+1}\binom{n}{r}\log\left(\mathrm{e}^{1-r}n + o(n)\right) \qquad \textit{as } n \to \infty.$$

Theorem 5.1.2 shows that the conjecture holds for sparse paving matroids. This implies in particular that the lower bound is correct, and may provide circumstantial evidence for the conjecture.

The construction provided at the end of Section 5.9 shows that $p(n,3)$ is much larger than $s(n,3)$. A more general construction may prove the following conjecture.

Conjecture 8.2.10. *For all fixed $r \geq 3$, $\lim_{n\to\infty} \frac{s(n,r)}{p(n,r)} = 0$.*

We believe that, in addition, $\frac{p(n,r)}{m(n,r)} \to 1$ as $n \to \infty$, for all fixed $r \geq 3$. The following observation points in that direction. The uniform matroid has the largest number of erections among all matroids with the same rank and groundset. Writing $\eta(n, r)$ for the average number of nontrivial erections over all non-uniform matroids on $[n]$ of rank r, we obtain

$$m(n, r) = p(n, r) + (m(n, r-1) - 1)\eta(n, r-1).$$

Theorem 7.4.1 suggests that almost every matroid has only one erection (the trivial one). If this is also true for matroids of fixed rank, then $\eta(n, r-1)$ is close to 1, which would prove the conjecture.

Rank

Concerning rank, Mayhew, Newman, Welsh, and Whittle made the following conjecture.

Conjecture 1.3.3 ([MNWW11, Conjecture 1.10]). *Almost every matroid satisfies* $\operatorname{rk}(M) \in \left\{\left\lfloor \frac{|M|}{2} \right\rfloor, \left\lceil \frac{|M|}{2} \right\rceil\right\}$.

We have made some progress towards resolution of this conjecture by showing that almost every matroid has its rank within $O(\sqrt{|M|})$ of $|M|/2$; see Theorem 7.3.1.

Symmetry

Recall that a matroid is asymmetric if its automorphism group is trivial.

Conjecture 1.3.4 ([MNWW11, Conjecture 1.2]). *Almost every matroid is asymmetric.*

Although we have not been able to prove the full conjecture, we have been able to prove that the conjecture holds for sparse paving matroids, and that a weaker form of the conjecture, which states that almost every matroid is 'almost' asymmetric in the sense that their automorphism group is either trivial, or generated by a single transposition. Thus, proving the following conjecture now suffices to prove Conjecture 1.3.4.

Conjecture 8.2.11. *The automorphism group of almost every matroid is not generated by a single transposition.*

Conjecture 8.2.11 is strongly tied to the problem of estimating $m(n)$. In particular, it is shown in Theorem 7.7.3 that if Conjecture 8.2.11 fails, then both the upper and lower bound of (8.1) are sharp up to

$(1 + o(1))$-factors. Thus, any result that improves either the upper bound or the lower bound on $\log m(n)$ by a constant factor, immediately implies Conjecture 1.3.4.

Our attempt at proving Conjecure 1.3.4 is thwarted by the matroids whose automorphism group is generated by a single transposition. Even in the special case of sparse paving matroids, for which we have been able to prove the conjecture, the bound on the number of matroids whose automorphism group is generated by a transposition is much weaker than the corresponding bound on the number of matroids with a different nontrivial automorphism group. The apparent difficulty that tranpositions pose leads us to the following conjecture.

Conjecture 8.2.12. *Almost every symmetric matroid has an automorphism group that is generated by a transposition.*

A positive answer to Conjecture 8.2.12 would reflect the situation for graphs. It was shown by Erdős, and Rényi [ER63] that almost every graph is asymmetric. It follows from their proof that the number of symmetric graphs is dominated by the number of graphs with automorphism group generated by a single transposition.

8.3 Theme II: Minor-closed classes

The second theme concerns minor-closed classes. An important conjecture within that theme is the following.

> **Conjecture 1.3.5** ([MNWW11, Conjecture 1.7])**.** *Let N be a sparse paving matroid. Almost every matroid has an N-minor.*

A considerable portion of this thesis is devoted to proving Conjecture 1.3.5 for uniform minors (Theorem 7.6.3), as well as the small sparse paving matroids P_6, Q_6, and R_6 (Theorem 4.7.2), but a general solution still seems far away. Earlier in this chapter we considered the conjecture that almost every matroid is sparse paving. If that conjecture indeed turns out to be true, then Conjecture 1.3.5 reduces to the following conjecture.

Conjecture 8.3.1. *Let N be a sparse paving matroid. Almost every sparse paving matroid has an N-minor.*

Although this conjecture has the advantage that sparse paving matroids are more benign than general matroids, it is still likely to be hard.

Note that, with minor adaptations, the proof of each of the special cases in which we were able to prove Conjecture 1.3.5 carries over to a proof of Conjecture 8.3.1. Thus, Conjecture 8.3.1 holds for uniform N, as well as $N = P_6$, $N = Q_6$, and $N = R_6$.

Uniform minors

The following observation provides a high-level overview of the argument for proving Conjecture 1.3.5 for uniform matroids. We describe matroids M on ground set E of rank r by indicating, for each vertex of $J(E, r)$, whether it is a basis or a nonbasis of M. Let N be a uniform matroid. If M does not have N as a minor (and $|E|$ and r are so large that this does not follows from size considerations alone), then $J(E, r)$ has many subgraphs (corresponding to minors) that each contain at least one nonbasis. This, in turn, leads to a lower bound on the nonbasis-density of M.

Such an argument does not work as well when N is not uniform: in that case, each of the subgraphs may have a number of nonbases that is higher than, lower than, or exactly equal to the number of nonbases in N. In the latter case, it is only required that the nonbases in the subgraph avoid a certain configuration. Thus, for excluding general matroids a much more careful argument is necessary.

This perspective suggests that the difficulty of an argument should increase with complexity of the excluded minor, and perhaps Conjecture 1.3.5 is relatively easy to prove for sparse paving matroids with a single circuit-hyperplane. This certainly seems to be the case for the special matroids for which Conjecture 1.3.5 is proved: The conjecture holds for all sparse paving matroids of rank 3 on six elements, except for the two most “complex” among them: W^3 and $M(K_4)$. The construction in Section 4.8 of a large class of matroids without $M(K_4)$-minors or V_8-minors works more generally for matroids with sufficiently many intersecting circuit-hyperplanes.

Algebraic and representable matroids

The following two conjectures are implied by a special case ($N = V_8$) of Conjecture 1.3.5.

> **Conjecture 1.3.7.** *Almost every matroid is not algebraic over any field.*

This conjecture remains open.

Note that the Vámos matroid V_8 is not algebraic, so proving the case

$N = V_8$ of Conjecture 1.3.5 immediately implies Conjecture 1.3.7. It may be easier to prove Conjecture 1.3.5 for matroids of rank 3, in which case the 10-point non-Desargues matroid is an alternative [Lin85]. In addition, Conjecture 1.3.7 may be proved by combining special cases of Conjecture 1.3.5. For example, the Fano matroid $F_7 \equiv \mathrm{PG}(2,2)$ is algebraic only over fields of characteristic 2, while $\mathrm{PG}(2,3)$ is algebraic only over fields of characteristic 3 [Gor88]. Thus, proving Conjecture 1.3.5 for both $N = F_7$ and $N = \mathrm{PG}(2,3)$ would imply Conjecture 1.3.7.

Theorem
~~Conjecture~~ 1.3.6 ([MNWW11, Conjecture 1.9]). *Almost every matroid is not representable over any field.*

This conjecture was recently proved by Nelson [Nel16], using a different technique than proposed by Mayhew, Newman, Welsh, and Whittle. Nelson obtains a strong explicit bound on the number of representable matroids as a function of the cardinality of the ground set.

If a matroid is representable over a certain field, then it is algebraic over the same field; hence, a proof of Conjecture 1.3.7 would imply Conjecture 1.3.6. In particular, each of the special cases of Conjecture 1.3.5 mentioned after Conjecture 1.3.7 leads to a proof of Conjecture 1.3.6 as well. There are sparse paving matroids that are algebraic, but not representable over any field. One such example is the non-Pappus matroid [Oxl11, Proposition 6.1.10]. Finally, similar to the situation for algebraic matroids, there are combinations of minors that preclude representability; for example, the Fano matroid is representable only over fields of characteristic 2, while the non-Fano matroid is representable only over fields of characteristic other than 2 [Oxl11, Proposition 6.4.8].

It is conceivable that Conjecture 1.3.6 can alternatively be proved using an argument based on Theorem 6.8.5, although the resulting bound is likely to be much weaker than that obtained by Nelson. Relaxing a circuit-hyperplane in a linear matroid often results in a non-linear matroid. Geelen, Gerards, and Whittle [GGW14] note that

> "while the operation of relaxing a circuit-hyperplane does not behave well with respect to representation in general, it behaves particularly poorly with respect to representation over finite fields".

This poor behaviour may very well limit the set of all possible collections of hyperplanes, after which Conjecture 1.3.6 follows from an application of Theorem 6.8.5.

8.4 Theme III: Connectivity

The final theme concerns connectivity.

> **Theorem ~~Conjecture~~ 1.3.8** ([MNWW11, Conjecture 1.5]). *Let $k > 1$. Almost every matroid is k-connected.*

The cases $k \leq 3$ were proved by Lowrance, Oxley, Semple, and Welsh [LOSW13, Theorem 4.2], and the full conjecture was settled in Theorem 7.5.1.

In addition, we have proved that almost every matroid is arbitrarily highly vertically connected (Corollary 7.5.5) and has arbitrarily high branch-width (Corollary 7.5.7).

8.5 Conclusion

In this thesis we considered two intimately related problems: asymptotic enumeration of matroids and typical properties of matroids. As problems of the latter type are essentially questions about the enumeration in subclasses of matroids, enumeration of matroids really is the central theme of this thesis.

Enumeration is closely tied to finding concise but faithful descriptions of the objects to be counted: the number of possible such descriptions translates immediately to an upper bound on the number of objects under consideration. By providing such concise encodings of matroids, we made substantial progress on the problem of matroid enumeration in two separate settings: that of matroids of fixed rank, and that of general matroids.

For matroids of fixed rank, an upper bound on the number of matroids is obtained by providing a concise description of the essential flats of such a matroid in terms of a certain antichain. As the essential flats faithfully represent the matroid, this provides an upper bound. We obtained a complementary lower bound, which matches the upper bound on the logarithmic scale. Incidentally, this proves that essential flats provide a concise description of matroids, at least for fixed rank, which was already suspected by Higgs in the 1960's. Close analysis of the structure of the antichain should result in improved bounds on the number of matroids of fixed rank, and perhaps yield an extension to matroids whose rank is allowed to grow slowly with $|M|$. As matroids of fixed rank are closely related to Steiner systems with fixed block size, extending the techniques for matroids is likely to imply similar results for Steiner systems.

In the second setting, that of matroids of general rank, our bounds are dominated by the bounds on matroids of rank close to $|M|/2$. In that regime, our best upper bound is obtained by an extension of the container method from stable sets in graphs to matroids. The method allows us to encode a general matroid as a sparse paving matroid, augmented with a relatively small amount of additional information. This encoding in particular implies that $\log s(n) \sim \log m(n)$, thus lending credibility to the conjecture that almost every matroid is sparse paving.

In addition, the container method results in an upper bound on $\log m(n)$ that is within a factor $2 + o(1)$ of the best known lower bound. Both the upper bound and the lower bound are closely linked with statistics of stable sets in the Johnson graph. The best known lower bound is obtained by the construction of a stable set of cardinality $\frac{1}{n}\binom{n}{n/2}$ in $J(n, \lfloor n/2 \rfloor)$. As each stable set in the Johnson graph corresponds with a sparse paving matroid, this shows that $\log m(n) \geq \frac{1}{n}\binom{n}{n/2}$. It follows from the encoding of matroids as sparse paving matroids plus extra information that $\log m(n)$ is essentially determined by the number of stable sets in the $J(n, \lfloor n/2 \rfloor)$.

The main obstacle towards further improvement of these results is the lack of understanding of the stable sets of the Johnson graph. In particular, a better understanding of the maximum stable sets of $J(n, \lfloor n/2 \rfloor)$ is likely to lead to a better understanding of the behaviour of $\log m(n)$. If it can be shown that a maximum stable set in $J(n, \lfloor n/2 \rfloor)$ is close to $\frac{2}{n}\binom{n}{n/2}$, then this immediately improves the lower bound on $\log m(n)$. On the other hand, any technique that shows that a maximum stable set in $J(n, \lfloor n/2 \rfloor)$ has cardinality close to $\frac{1}{n}\binom{n}{n/2}$ is potentially useful for improving the upper bound on $\log m(n)$ as well.

The container method provides good bounds on the typical number of bases of a matroid. As many structural properties are strongly tied to the number of bases in a matroid, this insight allowed us to prove, among other things, that almost every matroid is highly connected, has arbitrarily large uniform minors, and is close to being asymmetric.

About the author

Jorn van der Pol (1989) obtained both his bachelor's (2011) and master's (2013) degrees in Industrial and Applied Mathematics from Eindhoven University of Technology, The Netherlands. His master's thesis, *Counting matroids*, was supervised by Nikhil Bansal, Remco van der Hofstad, and Rudi Pendavingh.

He was awarded the 2008 *Stieltjes Institute Young Talent Encouragement Award* (highest average grade among first-year mathematics students at Eindhoven University of Technology), and the 2014 *TU/e Academic Award* (best Master's thesis at Eindhoven University of Technology).

During his studies, Jorn was actively involved in teaching, research, and the organisation of the *International Mathematical Olympiad 2011*. In addition, he served two years as elected member in the Department Council.

After obtaining his master's degree in 2013, Jorn continued working on the topic of his Master's thesis as a doctoral candidate at Eindhoven University of Technology, under supervision of Remco van der Hofstad and Rudi Pendavingh. His work during this period is presented in this thesis, which he will defend on September 20, 2017.

References

[ABF94] Y. Azar, A.Z. Broder, and A.M. Frieze. On the problem of approximating the number of bases of a matroid. *Information Processing Letters*, 50(1):9–11, 1994.

[ABMS14] Noga Alon, Jószef Balogh, Robert Morris, and Wojciech Samotij. Counting sum-free subsets in abelian groups. *Israel Journal of Mathematics*, 199:309–344, 2014.

[AC88] N. Alon and F.R.K. Chung. Explicit construction of linear sized tolerant networks. *Discrete Mathematics*, 72:15–19, 1988.

[AH74] Edward F. Assmus, Jr. and Maria Theresa Hermoso. Non-existence of steiner systems of type $S(d-1, d, 2d)$. *Mathematische Zeitschrift*, 138:171–172, 1974.

[AS08] Noga Alon and Joel H. Spencer. *The probabilistic method.* Wiley, third edition, 2008.

[AY17] Jason Altschuler and Elizabeth Yang. Inclusion of minors in random representable matroids. *Discrete Mathematics*, 340(7):1553–1563, 2017.

[BB12] Patrick Bennett and Tom Bohman. A natural barrier in random greedy hypergraph matching. Preprint, available from `arXiv:1210.3581`, 2012.

[BCH73] John E. Blackburn, Henry H. Crapo, and Denis A. Higgs. A catalogue of combinatorial geometries. *Mathematics of Computation*, 27(121):155–166, 1973.

[BCN89] A.E. Brouwer, A.M. Cohen, and A. Neumaier. *Distance-Regular Graphs*, volume 18 of *Ergebnisse der Mathematik und ihrer Grenzgebiete*. Springer Berlin Heidelberg, 1989.

[Beh46] F.A. Behrend. On sets of integers which contain no three terms in arithmetical progression. *Proceedings of the National Academy of Sciences*, 32(12):331–332, 1946.

[BIK07] Moshe Babaioff, Nicole Immorlica, and Robert Kleiberg. Matroids, secretary problems, and online mechanisms. In *SODA'07 Proceedings of the eighteenth annual ACM-SIAM Symposium on Discrete Algorithms*, pages 434–443. Society for Industrial and Applied Mathematics, 2007.

[BMS15] József Balogh, Robert Morris, and Wojciech Samotij. Independent sets in hypergraphs. *Journal of the American Mathematical Society*, 28:669–709, 2015.

[Bon13] Joseph E. Bonin. Basis-exchange properties of sparse paving matroids. *Advances in Applied Mathematics*, 50:6–15, 2013.

[BPvdP14] N. Bansal, R.A. Pendavingh, and J.G. van der Pol. An entropy argument for counting matroids. *Journal of Combinatorial Theory, Series B*, 109:258–262, 2014.

[BPvdP15] Nikhil Bansal, Rudi A. Pendavingh, and Jorn G. van der Pol. On the number of matroids. *Combinatorica*, 35(3):253–277, 2015.

[Bro] Andries Brouwer. Bounds for binary constant weight codes. Available from `https://www.win.tue.nl/~aeb/codes/Andw.html` (accessed April 7, 2017).

[BS06] Ian F. Blake and Chris Studholme. Properties of random matrices and applications. Unpublished note; available from `http://www.cs.toronto.edu/~cvs/coding/random_report.pdf` (accessed April 4, 2017)., 2006.

[CFP17] Colin Cooper, Alan Frieze, and Wesley Pegden. Minors of a random binary matroid. Preprint, available from `arXiv:1612.02084v2`, 2017.

[CGFS86] F.R.K. Chung, R.L. Graham, P. Frankl, and J.B. Shearer. Some intersection theorems for ordered sets and graphs. *J. Comb. Theory. Ser. A*, 43(1):23–37, 1986.

[Clo10] Brian Cloteaux. Approximating the number of bases for almost all matroids. *Congressus Numerantium*, 202:149–153, 2010.

[CLW96] Laura Chávez Lomelí and Dominic Welsh. Randomised approximation of the number of bases. In Joseph E. Bonin, James G. Oxley, and Brigitte Servatius, editors, *Matroid theory*, number 197 in Contemporary Mathematics, pages 371–376. American Mathematical Society, 1996.

[CM07] Charles J. Colbourn and Rudolf Mathon. Steiner systems. In Jeffrey H. Dinitz and Charles J. Colbourn, editors, *Handbook of combinatorial designs*, pages 101–109. Chapman & Hall/CRC, second edition, 2007. Updates available from the book's website: `http://www.emba.uvm.edu/~jdinitz/hcd.html` (accessed March 18, 2017).

[CR70] Henry H. Crapo and Gian-Carlo Rota. *On the foundations of combinatorial theory: Combinatorial geometries.* The M.I.T. Press, 1970.

[Cra65] Henry H. Crapo. Single-element extensions of matroids. *Journal of Research of the National Bureau of Standards—B: Mathematics and Mathematical Physics*, 69B(1–2):55–65, 1965.

[Cra70] Henry H. Crapo. Erecting geometries. In *Proc. Second Chapel Hill Conf. on Combinatorial Mathematics and its Applications*, pages 74–99. Univ. North Carolina, 1970.

[CT06] Thomas M. Cover and Joy A. Thomas. *Elements of information theory.* Wiley, second edition, 2006.

[Cun12] William H. Cunningham. The coming of the matroids. In Martin Grötschel, editor, *Optimization stories.* Deutschen Mathematiker-Vereinigung, 2012.

[Dha96] Jack S. Dharmatilake. A min-max theorem using matroid separations. In Joseph E. Bonin, James G. Oxley, and Brigitte Servatius, editors, *Matroid theory*, number 197 in Contemporary Mathematics, pages 333–342. American Mathematical Society, 1996.

[Die16] Reinhard Diestel. *Graph theory*, volume 173 of *Graduate Texts in Mathematics.* Springer, fifth edition, 2016.

[Duk87] Roger Duke. Matroid erection and duality. *European Journal of Combinatorics*, 26(1):37–43, 1987.

[Ede04] Yves Edel. Extensions of generalized product caps. *Designs, Codes and Cryptography*, 31(1):5–14, 2004.

[Edm70] Jack Edmonds. Submodular functions, matroids and certain polyhedra. In R. Guy, H. Hanam, N. Sauer, and J. Schonheim, editors, *Combinatorial structures and their applications (Proceedings of the Calgary International Conference 1969)*, pages 69–87. Gordon and Breach, 1970.

[EG17] Jordan S. Ellenberg and Dion Gijswijt. On large subsets of $\mathbb{F}_q^n$ with no three-term arithmetic progression. *Annals of Mathematics*, 185(1):339–343, 2017.

[EH63] P. Erdős and H. Hanani. On a limit theorem in combinatorial analysis. *Publicationes Mathematicae Debrecen*, 10:10–13, 1963.

[ER59] P. Erdős and A. Rényi. On random graphs I. *Publicationes Mathematicae Debrecen*, 6:290–297, 1959.

[ER60] P. Erdős and A. Rényi. On the evolution of random graphs. *Publications of the Mathematical Institute of the Hungarian Academy of Sciences*, 5:17–61, 1960.

[ER63] P. Erdős and A. Rényi. Asymmetric graphs. *Acta Mathematica Hungarica*, 14(3–4):295–315, 1963.

[FGH$^+$17] Satoru Fujishige, Michel X. Goemans, Tobias Harks, Britta Peis, and Rico Zenklusen. Matroids are immune to Braess' paradox. *Mathematics of Operations Research*, 2017.

[Fox11] Jacob Fox. A new proof of the graph removal lemma. *Annals of Mathematics*, 174(1):561–579, 2011.

[Gal14] David Galvin. Three tutorial lectures on entropy and counting. Available from arXiv:1406.7872, 2014.

[Gee08] Jim Geelen. Some open problems on excluding a uniform matroid. *Advances in Applied Mathematics*, 41:628–637, 2008.

[GrGrWh00] M.J. Grannell, T.S. Griggs, and C.A. Whitehead. The resolution of the anti-Pasch conjecture. *Journal of Combinatorial Designs*, 8(4):300–309, 2000.

[GGW14] Jim Geelen, Bert Gerards, and Geoff Whittle. Solving Rota's conjecture. *Notices of the American Mathematical Society*, 61(7):736–743, 2014.

[GH06] Jim Geelen and Peter J. Humphries. Rota's basis conjecture for paving matroids. *SIAM Journal of Discrete Mathematics*, 20(1):1042–1045, 2006.

[Gil59] E.N. Gilbert. Random graphs. *Annals of Mathematical Statistics*, 30(4):1141–1144, 1959.

[Gor88] Gary Gordon. Algebraic characteristic sets of matroids. *Journal of Combinatorial Theory, Series B*, 44:64–74, 1988.

[Gre91] Tom Greene. Descriptively sufficient subcollections of flats in matroids. *Discrete Mathematics*, 87:149–161, 1991.

[GS80] R.L Graham and N.J.A. Sloane. Lower bounds for constant weight codes. *IEEE Transactions on Information Theory*, 26(1), 1980.

[GW14] Goeffrey Grimmett and Dominic Welsh. *Probability: An introduction.* Oxford University Press, second edition, 2014.

[Hae79] Wilhelmus Hubertus Haemers. *Eigenvalue techniques in design and graph theory.* PhD thesis, Technische Hogeschool Eindhoven, 1979.

[HN16] Tony Huynh and Peter Nelson. The matroid secretary problem for minor-closed classes and random matroids. Preprint, available from `arXiv:1603.06822v4`, 2016.

[Hof70] Alan J. Hoffman. On eigenvalues and colorings of graphs. In Bernard Harris, editor, *Graph Theory and its Applications*, pages 79–91. Academic Press, 1970.

[Jan11] Svante Janson. Probability asymptotics: notes on notation. Available from `arXiv:1108.3924.`, 2011.

[Jer06] Mark Jerrum. Two remarks concerning balanced matroids. *Combinatorica*, 26(6):733–742, 2006.

[JŁR00] Svante Janson, Tomasz Łuczak, and Andrzej Ruciński. *Random graphs*, volume 45 of *Wiley-Interscience series in discrete mathematics and optimization.* Wiley, 2000.

[Juk01] Stasys Jukna. *Extremal combinatorics: with applications in computer science.* Springer, second edition, 2001.

[Kah01] Jeff Kahn. An entropy approach to the hard-core model on bipartite graphs. *Combinatorics, Probability and Computing*, 10:219–237, 2001.

[Kas08] Navin Kashyap. A decomposition theory for binary linear codes. *IEEE Transactions on Information Teory*, 54(7):3035–3058, 2008.

[Kee14] Peter Keevash. The existence of designs. Preprint, available from `arXiv:1401.3665`, 2014.

[Kee15] Peter Keevash. Counting designs. Preprint, available from `arXiv:1504.02909`, 2015.

[KŁ91] Wojciech Kordecki and Tomasz Łuczak. On random subsets of projective spaces. *Colloquium Mathematicum*, LXII(2):353–356, 1991.

[KŁ99] Wojciech Kordecki and Tomasz Łuckzak. On the connectivity of random subsets of projective spaces. *Discrete Mathematics*, 196(1–3):207–217, 1999.

[Klø81] Torleiv Kløve. A lower bound for $A(n, 4, w)$. *IEEE Transactions on Information Theory*, 27(2), 1981.

[Knu74] Donald E. Knuth. The asymptotic number of geometries. *Journal of Combinatorial Theory, Series A*, 16:398–400, 1974.

[Knu75] Donald E. Knuth. Random matroids. *Discrete Mathematics*, 12(4):341–358, 1975.

[Knu98] Donald E. Knuth. Sorting and searching. In *The art of computer programming*, volume 3. Addison-Wesley, 2 edition, 1998.

[KO82a] D.G. Kelly and J.G. Oxley. Threshold functions for some properties of random subsets of projective spaces. *Quarterly Journal of Mathematics*, 33(2):463–469, 1982.

[KO82b] Douglas G. Kelly and James G. Oxley. Asymptotic properties of random subsets of projective spaces. *Mathematical Proceedings of the Cambridge Philosophical Society*, 91:119–130, 1982.

[KO84] D.G. Kelly and J.G. Oxley. On random representable matroids. *Studies in Applied Mathematics*, 71:181–205, 1984.

[Kor88] Wojciech Kordecki. Strictly balanced submatroids in random subsets of projective geometries. *Colloquium Mathematicum*, LXV(2):371–375, 1988.

[Kor95] Wojciech Kordecki. Maximal full subspaces in random projective spaces: thresholds and Poisson approximation. *Random Structures and Algorithms*, 6(2):297–307, 1995.

[Kor96] Wojciech Kordecki. Small submatroids in random matroids. *Combinatorics, Probability and Computing*, 5(3):257–266, 1996.

[Kun86] Joseph P.S. Kung. *A source book in matroid theory*. Birkhäuser, 1986.

[KW80] D.J. Kleitman and K.J. Winston. The asymptotic number of lattices. *Annals of Discrete Mathematics*, 6:243–249, 1980.

[KW82] Daniel J. Kleitman and Kenneth J. Winston. On the number of graphs without 4-cycles. *Discrete Mathematics*, 6:167–172, 1982.

[Lac14] Oded Lachish. $O(\log\log\text{rank})$ competitive ratio for the matroid secretary problem. In *55th annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 326–335. IEEE Computer Society, 2014.

[Lin85] B. Lindström. A desarguesian theorem for algebraic combinaorial geometries. *Combinatorica*, 5(3):237–239, 1985.

[LL13] Nathan Linial and Zur Luria. An upper bound on the number of Steiner triple systems. *Random Structures & Algorithms*, 43(4):399–406, 2013.

[LOSW13] Lisa Lowrance, James Oxley, Charles Semple, and Dominic Welsh. On properties of almost all matroids. *Advances in Applied Mathematics*, 50:115–124, 2013.

[Lov12] László Lovász. *Large networks and graph limits*, volume 60 of *Colloquium Publications*. American Mathematical Society, 2012.

[MNRIVF12] Criel Merino, Steven D. Noble, Marcelino Ramírez-Ibáñez, and Rafael Villarroel-Flores. On the structure of the h-vector of a paving matroid. *European Journal of Combinatorics*, 33:1787–1799, 2012.

[MNWW11] Dillon Mayhew, Mike Newman, Dominic Welsh, and Geoff Whittle. On the asymptotic proportion of connected matroids. *European Journal of Combinatorics*, 32(6):882–890, 2011.

[MR08] Dillon Mayhew and Gordon F. Royle. Matroids with nine elements. *Journal of Combinatorial Theory, Series B*, 98(2):415–431, 2008.

[MW55] Leo Moser and Max Wyman. An asymptotic formula for the Bell numbers. *Transactions of the Royal Society of Canada*, XLIX, 1955.

[MW13] Dillon Mayhew and Dominic Welsh. On the number of sparse paving matroids. *Advances in Applied Mathematics*, 50(1):125–131, 2013.

[Nel16] Peter Nelson. Almost all matroids are non-representable. Preprint, available from `arXiv:1605.04288v2`, 2016.

[NSTW06] Serguei Norine, Paul Seymour, Robin Thomas, and Paul Wollan. Proper minor-closed families are small. *Journal of Combinatorial Theory, Series B*, 96:754–757, 2006.

[Ö10] Patric R.J. Östergård. Classification of binary constant weight codes. *IEEE Transactions on Information Theory*, 56(8):3779–3785, 2010.

[ÖP08] Patric R.J. Östergård and Olli Pottonen. There exists no steiner system $S(4, 5, 17)$. *Journal of Combinatorial Theory, Series A*, 115:1570–153, 2008.

[Oxl84] James G. Oxley. Threshold distribution functions for some random representable matroids. *Proceedings of the Cambridge Philosophical Society*, 95:335–347, 1984.

[Oxl11] James Oxley. *Matroid theory*, volume 21 of *Oxford graduate texts in mathematics*. Oxford University Press, second edition, 2011.

[Pif73] M.J. Piff. An upper bound for the number of matroids. *Journal of Combinatorial Theory, Series B*, 14:241–245, 1973.

[PvdP15a] R.A. Pendavingh and J.G. van der Pol. Counting matroids in minor-closed classes. *Journal of Combinatorial Theory, Series B*, 111:126–147, 2015.

[PvdP15b] Rudi Pendavingh and Jorn van der Pol. On the number of matroids compared to the number of sparse-paving matroids. *Electronic Journal of Combinatorics*, 22(2):P2.51, 2015.

[PvdP16a] Rudi Pendavingh and Jorn van der Pol. Asymptotics of symmetry in matroids. Preprint, available from `arXiv:1609.04975`, 2016.

[PvdP16b] Rudi Pendavingh and Jorn van der Pol. Counting matroids by entropy, April 2016. Blog post, available from `http://matroidunion.org/?p=1675` (accessed April 14, 2017).

[PvdP16c] Rudi Pendavingh and Jorn van der Pol. On the number of bases of almost all matroids. Accepted to Combinatorica, preprint available from `arXiv:1602.04763`, 2016.

[PvdP17] Rudi Pendavingh and Jorn van der Pol. Enumerating matroids of fixed rank. *Electronic Journal of Combinatorics*, 24(1):P.1.8, 2017.

[PW71] M.J. Piff and D.J.A. Welsh. On the number of combinatorial geometries. *Bulletin of the London Mathematical Society*, 3:55–56, 1971.

[Rad03] Jaikumar Radhakrishnan. Entropy and counting. In J.C. Misra, editor, *Computational Mathematics, Modelling and Algorithms*. Narosa Publishers, 2003.

[Röd85] Vojtěch Rödl. On a packing and covering problem. *European Journal of Combinatorics*, 6:69–78, 1985.

[RS78] I.Z. Rusza and E. Szemerédi. Triple systems with no six points carrying three triangles. *Colloquia Mathematica Societatis János Bolyai*, pages 939–945, 1978.

[Sam15] Wojciech Samotij. Counting independent sets in graphs. *European Journal of Combinatorics*, 48:5–18, 2015.

[Sch03] Alexander Schrijver. *Combinatorial optimization: polyhedra and efficiency*, volume 24 of *Algorithms and combinatorics*. Springer, 2003.

[SF14] Joel Spencer and Laura Florescu. *Asymptopia*, volume 71 of *Student Mathematical Library*. American Mathematical Society, 2014.

[Sha48] C.E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27:379–423, 623–656, 1948. Reprinted in [Sha01].

[Sha01] C.E. Shannon. A mathematical theory of communication. *ACM SIGMOBILE Mobile Computing and Communications Review*, 5(1):3–55, 2001.

[ST15] David Saxton and Andrew Thomason. Hypergraph containers. *Inventiones Mathematicae*, 201(3):925–992, 2015.

[TV07] Terence Tao and Van Vu. On the singularity probability of random Bernoulli matrices. *Journal of the American Mathematical Society*, 20(3):603–628, 2007.

[vdH16] Remco van der Hofstad. *Random graphs and complex networks, Vol. 1.* Cambridge Series in Statistical and Probabilistic Mathematics. Cambridge University Press, 2016.

[Wel71] D.J.A. Welsh. Combinatorial problems in matroid theory. In D.J.A. Welsh, editor, *Combinatorial mathematics and its applications.* Academic Press, 1971.

[Wel76] D.J.A. Welsh. *Matroid theory.* Number 8 in L.M.S. Monographs. Academic Press, 1976.

[Whi35] Hassler Whitney. On the abstract properties of linear dependence. *American Journal of Mathematics*, 57:509–533, 1935.

[You95] Neal E. Young. Randomized rounding without solving the linear program. In *SODA'95 Proceedings of the sixth annual ACM-SIAM Symposium on Discrete Algorithms*, pages 170–178, 1995.

List of symbols

$G[A]$	Induced subgraph, page 14
$M/C\backslash D$	Minor, page 23
$\binom{E}{r}$, $\binom{E}{\leq r}$	Subsets of given cardinality, page 14
$X^{\downarrow}$	Downset, page 78
$\nabla(U, U')$	Edges with an endpoint in U and U' each., page 14
$\prec$	Graded lexicographic order, page 83
$\triangle$	Symmetric difference, page 14
ln, log	Natural logarithm, base-2 logarithm, page 16
$\mathrm{Sym}(n)$	Symmetric group, page 162
$M{\uparrow}\mathcal{U}$	Erection defined by $\mathcal{U}$, page 76
T	Shorthand for $\frac{1}{n-2}\binom{n}{3}$ [Section 5.9, page 109
$\mathcal{B}(M)$	Bases of M, page 18
$\mathrm{cl}_k(X)$	k-closure, page 75
$\mathrm{cl}_M(X)$	Closure of X in M, page 21
$d(v)$	Degree of v, page 14
$\Delta(G)$	Maximum degree in G, page 14
$\delta(G)$	Minimum degree in G, page 14

$\mathbb{E}$	Expectation operator, page 15
$E(M)$	Ground set of M, page 18
$\mathrm{Ex}(\mathcal{N})$, $\mathrm{Ex}(N)$	Excluded-minor characterisation, page 24
$\mathcal{F}(M)$	Flats of M, page 22
$\mathrm{g}(M)$	Girth of M, page 19
$\mathscr{H}(\boldsymbol{X})$	Entropy of $\boldsymbol{X}$, page 34
$\mathscr{H}(p)$	Binary entropy, page 17
$\mathcal{H}(M,\mathcal{U})$	Output of Knuth's procedure, page 76
$\mathcal{H}^+$	Dependent hyperplanes, page 84
$\mathcal{I}$	Independent sets of M, page 18
$J(n, r)$	Johnson graph, page 26
$\kappa^*(M)$	Fractional cover complexity, page 54
κ	Cover complexity, page 46
$\lambda(M)$	(Tutte) connectivity of M, page 21
$\mathbb{M}(n)$, $\mathbb{M}(n, r)$	Matroids on $E = [n]$ (of rank r), page 24
$m^{\circ}_{\mathcal{M}}$	Number of unlabelled matroids in $\mathcal{M}$, page 40
M^*	Dual matroid, page 23
$M^{(k)}$	Rank-k truncation of M, page 74

$M(G)$	Graphic matroid, page 19
$[n]$	$\{1, 2, \ldots, n\}$, page 13
$N(X)$, $N(v)$	Neighbourhood, page 14
$\mathbb{P}$	Probability measure, page 15
$\mathscr{P}(E)$	Power set, page 14
$p(n, r)$	Number of paving matroids, page 84
$\mathrm{rk}_M(X)$, $\mathrm{rk}(M)$	Rank of X in M, rank of M, page 20
$\Sigma_2, \Sigma_{\geq 3}$	Permuations that move 2, resp. at least 3, elements, page 163
$\mathbb{S}(n)$, $\mathbb{S}(n, r)$	Sparse paving matroids on $E = [n]$ (of rank r), page 24
$\widehat{\mathbb{S}}$	Proxy for sparse paving matroids, page 180
$T(M)$	Rank-($\mathrm{rk}(M) - 1$) truncation of M, page 74
$\mathcal{U}(M)$	$\mathcal{K}(M) \setminus \mathcal{W}(M)$, page 22
$\mathcal{V}(M)$	Antichain describing M, page 85
$\mathcal{W}(M)$	Circuit-hyperplanes of M, page 22
$\zeta(n)$	$57\frac{\log^2 n}{n^2}\binom{n}{n/2}$, page 141
$\mathbb{Z}_{\geq 0}$, $\mathbb{Z}_{>0}$	Nonnegative, positive integers, page 13

Index