Asymptotic Enumeration for Matroids

Talk by Milan Haiman (Notes by Sanjana Das)

March 24, 2023

§1 Introduction

§1.1 Definitions

Definition 1.1. A *matroid* on ground set E is a nonempty collection $\mathcal{B}$ of *bases* $B \subseteq E$ such that for any two bases B and B' and any $e \in B \setminus B'$, there exists some $e' \in B' \setminus B$ such that $B \setminus \{e\} \cup \{e'\}$ is also a basis.

In other words, given any two bases and an element in one, we can choose an element in the other to exchange it with (bringing the first basis closer to the second). This property automatically implies that any two bases have the same number of elements — if $|B| < |B'|$ then we can swap out elements of B not in B' until B is a proper subset of B', at which point there are elements in B' not in B that we can't swap out for elements in B.

Definition 1.2. The *rank* of a matroid M is defined as the common rank of all $B \in \mathcal{B}$.

Matroids are a generalization of linear independence in vector spaces:

Example 1.3

You can obtain a matroid by taking E to be a set of vectors and $\mathcal{B}$ to be the collection of all maximal linearly independent sets of these vectors.

Definition 1.4. A set $X \subseteq E$ is *independent* if $X \subseteq B$ for some $B \in \mathcal{B}$.

Similarly to in vector spaces, sets in a matroid have a notion of rank:

Definition 1.5. For a set $X \subseteq E$, its *rank* is defined as $r_M(X) = \max_{B \in \mathcal{B}} |X \cap B|$.

Definition 1.6. A *circuit* $C \subseteq E$ is a minimal dependent set.

This implies $r_M(C) = |C| - 1$ (the converse is not true, though).

Example 1.7

If the matroid comes from a vector system, a circuit corresponds to writing down some linear dependence and only taking the vectors involved in the linear dependence (where there are no smaller linear dependences between them).

Definition 1.8. A *flat* is a maximal set of some fixed rank.

(In other words, adding any new element to a flat would increase its rank.)

Definition 1.9. For a set $X \subseteq E$, the *closure* of X is the set

$$\mathrm{cl}_M(X) = \{e \in E \mid r_M(x) = r_M(X \cup \{e\})\}.$$

This implies the rank of $\mathrm{cl}_M(X)$ is the same as the rank of X. The closure is a generalization of the span in a vector space.

Fact 1.10 — Rank is submodular — $r_M(X \cup Y) + r_M(X \cap Y) \leq r_M(X) + r_M(Y)$ for any X and Y.

§1.2 Counting Matroids

Notation 1.11. Let $\mathbb{M}_n$ be the set of all matroids M on the ground set $[n]$, and let $m_n = |\mathbb{M}_n|$.

Question 1.12. How does m_n grow?

First, there's a trivial bound on m_n — any matroid is a collection of subsets of $[n]$, and there are 2^n such subsets, so $m_n \leq 2^{2^n}$. We can do a bit better by noting that all bases B are of the same size. So if we only look at collections of subsets of $[n]$ of each size r, we get the bound of

$$m_n \leq \sum_{r=0}^{n} 2^{\binom{n}{r}} \leq (n+1)2^{2^n/\sqrt{n}}.$$

As in the above calculation, in order to study m_n, we'll split it up by the rank of the matroid.

Notation 1.13. Let $\mathbb{M}_{n,r}$ be the set of matroids M on ground set $[n]$ with rank r, and let $m_{n,r} = |\mathbb{M}_{n,r}|$.

We'll study $m_{n,r}$ instead (and use it to obtain bounds on m_n). We'd expect this function to be biggest when r is close to $\frac{n}{2}$, and this is indeed true — it's known that

$$\sum_r m_{n,r} = (1 - o(1))m_n$$

where the sum is over all r within $O(\log n)$ of $\frac{n}{2}$, and it's conjectured that we don't even need the log and can replace it with a small constant such as 1 or 2.

We'll write our bounds in terms of $\log\log m_n$ (all logarithms are base 2 unless stated otherwise). Our above bound of approximately $2^{2^n/\sqrt{n}}$ gives

$$\log\log m_n \leq n - \frac{1}{2}\log n + o(1).$$

There has been the following improvement on this bound from thirty years ago:

Theorem 1.14 (Piff 1973)

We have $\log\log m_n \leq n - \log n + \log\log n + o(1)$.

There's also a *lower* bound:

Theorem 1.15 (Knuth 1974)
We have $\log\log m_n \geq n - \frac{3}{2}\log n - 1 + o(1)$.

We'll actually see a proof of this bound that obtains a constant of $+\frac{1}{2}\log\frac{2}{\pi}$ instead of -1.

Recently, the upper bound has been improved to match the term $\frac{3}{2}\log n$:

Theorem 1.16 (Bansal, Pendavingh, van der Pol 2012)
We have $\log\log m_n \leq n - \frac{3}{2}\log n + \frac{1}{2}\log\frac{2}{\pi} + 1 + o(1)$.

Together, the upper and lower bounds give that $m_n = 2^{\Theta(2^n/n^{3/2})}$, but we don't know exactly what the multiplicative constant in the exponent is (it depends on the constant term of $\log\log m_n$, in which we have a gap between $\frac{1}{2}\log\frac{2}{\pi}$ and $\frac{1}{2}\log\frac{2}{\pi} + 1$).

§2 Sparse Paving Matroids

§2.1 Paving Matroids

Definition 2.1. A matroid of rank r is *paving* if $|C| \geq r$ for all circuits C.

For matroids corresponding to vectors, paving matroids correspond to sets which are *almost* in general position. If the vectors were in general position — meaning that there were no linear dependences at all — then every set of size r is a basis and any circuit has size at least $r+1$. But there is only one such matroid (consisting of all the sets of size r), so we don't want such a restrictive condition. Instead, we add in the minimal amount of freedom we need for the objects to be interesting — we're allowed to have dependencies of size r, but none of any smaller size.

Example 2.2
For matroids corresponding to vectors in 3-dimensional space (so $r = 3$), a paving matroid cannot have any two collinear vectors (corresponding to a linear dependence of size 2), but it can have three coplanar vectors (corresponding to a linear dependence of size 3).

Another way to think about paving matroids is that every set X with $|X| \leq r - 1$ is independent. (In general position, every set with $|X| \leq r$ is independent; here we're allowing a small amount of defects by replacing r with $r - 1$.)

§2.2 Sparse Paving Matroids

Definition 2.3. For a matroid M on ground set E, its *dual* M^* is the matroid on the same ground set E whose bases are the complements of the bases of M.

In other words, the collection of bases of M^* is $\{E \setminus B \mid B \in \mathcal{B}\}$ (where $\mathcal{B}$ is the collection of bases for M). In particular, the rank of M^* is $n - r$.

Definition 2.4. A matroid M is *sparse paving* if both M and M^* are paving.

This essentially states that our matroid only has interesting things happening on the r-layer (the layer of sets with size r).

The condition for a matroid to be sparse paving can be restated without referencing the dual matroid — consider the graph on size-r subsets of $[n]$, where two subsets X and Y are adjacent (denoted $X \sim Y$) if and only if $|X \cap Y| = r - 1$ (i.e., we can go from X to Y by exchanging only one element). Then a matroid is sparse paving if and only if the non-bases of size r form an independent set in this graph.

In other words, for a matroid to be sparse paving means that if we take any two sets of size r which intersect at $r - 1$ elements, then at least one of them is a basis.

Example 2.5

For matroids which correspond to a set of vectors:

- A set of spanning vectors in $\mathbb{R}^r$ gives a paving matroid of rank r if there is no subset X of these vectors with $|X| < r$ such that $\dim \operatorname{Span}(X) < |X|$ (in other words, there are no dependencies of size smaller than r, as stated earlier).
- A set of spanning vectors in $\mathbb{R}^r$ gives a sparse paving matroid of rank r if it satisfies the above condition (so that the matroid is paving) and for any $(r - 1)$-subset of vectors, there is at most one other vector in their span. (If there were two, then the two r-subsets obtained by adding each to our $r - 1$ vectors would both be non-bases, and would be adjacent in the graph.)

You can think of the paving condition as taking a general-position matroid and introducing small defects (e.g., putting vectors into size-$(r - 1)$ subspaces), and the sparse paving condition as ensuring that these defects are isolated (e.g., there's only one other vector in the span of any given $r - 1$).

Conjecture 2.6 — Almost all matroids are sparse paving.

The reason to believe this is that once you start having bigger defects in the matroid, they put more restrictions on the sets, giving less room to make choices.

Notation 2.7. Let $s_{n,r}$ be the number of sparse paving matroids in $\mathbb{M}_{n,r}$, and let $s_n = \sum_{r=0}^{n} s_{n,r}$ be the number of sparse paving matroids in $\mathbb{M}_n$ in total.

The conjecture then states more precisely that

$$m_n = (1 + o(1))s_n.$$

Recent progress towards this conjecture shows that their *logarithms* have this property.

Theorem 2.8 (Pendavingh, van der Pol 2014)

We have $\log m_n = (1 + o(1)) \log s_n$.

§2.3 Sparse Paving Matroids as Independent Sets

Definition 2.9. The *Johnson graph* $J(n, r)$ is the graph on the vertex set $\binom{[n]}{r}$ where two sets X and Y are adjacent (denoted $X \sim Y$) if $|X \cap Y| = r - 1$.

As mentioned earlier, a sparse paving matroid of rank r on $[n]$ is a matroid whose non-bases of size r form an independent set in this graph (and there are no non-bases of smaller size). The converse is also true — any independent set in $J(n, r)$ gives a sparse paving matroid. (The basis exchange axiom holds, essentially because the defects being spread out mean they don't really prevent us from going where we want — given $e \in B$ to remove, if there are at least two choices of $e' \in B'$ which we could add then at least one works because the two resulting sets would be adjacent in the graph, while if there's only one and it fails then B' must actually not have been a basis.)

In order to obtain the *lower* bound for m_n, it suffices to lower-bound s_n (since $m_n \geq s_n$). This amounts to bounding the number of independent sets in the graph $J(n, r)$ — so we have an object to understand that doesn't involve matroids anymore.

§3 The Lower Bound

We'll now prove Knuth's theorem (the lower bound for m_n). We'll lower bound $s_{n,r}$ by coloring the Johnson graph — we can color $J(n, r)$ with n colors according to the coloring function $\phi\colon X \to [n]$ defined as

$$\phi\colon X \mapsto \sum_{x \in X} x \pmod{n}.$$

To check that this is a proper coloring, if $X \sim Y$ then we can write $Y = X \cup \{y\} \setminus \{x\}$ for some distinct x and y; then

$$\phi(Y) - \phi(X) = y - x \not\equiv 0 \pmod{n},$$

so X and Y receive different colors.

Since we have a coloring of $J(n, r)$ with n colors, there must exist an independent set of size at least $\frac{1}{n}\binom{n}{r}$. Then any of its subsets is also an independent set; so

$$s_{n,r} = \#\{\text{independent sets in } J(n, r)\} \geq 2^{\frac{1}{n}\binom{n}{r}}.$$

After working out the calculations, this gives the bound stated in Knuth's theorem, with a constant of $+\frac{1}{2}\log\frac{2}{\pi}$ (this wasn't Knuth's original proof, which gave a different constant). (In particular, from here we can see where the $-\frac{3}{2}\log n$ term comes from — the biggest contribution is from $r = \frac{n}{2}$, in which case the exponent is $\frac{1}{n}\binom{n}{n/2} \approx n^{-3/2} \cdot 2^n$.)

§4 The Upper Bound

We will first see an upper bound for the number of independent sets in $J(n, r)$ (and therefore for $s_{n,r}$); then we'll see how this technique was modified to get upper bounds for $m_{n,r}$ as well.

§4.1 Bounding Independent Sets

The upper bound on the number of independent sets comes from a nice algorithmic technique with some spectral ideas.

Theorem 4.1

Let G be a d-regular graph (on n vertices) with minimum eigenvalue $-\lambda$. Then the number of independent sets in G, denoted $i(G)$, satisfies

$$i(G) \leq 2^{\alpha n} \sum_{k=0}^{\sigma n} \binom{n}{k},$$

where $\alpha = \frac{\lambda}{d+\lambda}$ and $\sigma = \frac{\ln(d+1)}{d+\lambda}$.

The key idea in the proof of this theorem is from Kleitman and Winston (1982) who were trying to bound sets without a C_4. It was modified by Alon, Balogh, Morris, and Samotij (2012), who were looking at independent sets and sum-free subsets of integers (and similar things).

Proof Sketch. We'll see a bit of the main idea of the proof. The idea is to encode each independent set I using a *canonical subset* S — given an independent set, we want to choose some representative subset of it. We want to choose S through some sort of deterministic process which we can reverse knowing the subset; this will reduce the possibilities for the independent set by a lot. This canonical subset will have size at most σn, and it will contribute a factor of $2^{\alpha n}$.

In order to choose this canonical subset S, we want to take vertices with high degree, or more precisely high degree to the vertices we haven't yet excluded — this is because then knowing that these vertices are present in our independent set eliminates a lot of other vertices from potentially being present (and therefore restricting what the independent set could be, from looking at S — our goal is to have $S \cup N(S)$ exclude most possibilities not in I).

The spectral information (on the minimal eigenvalue) is used somewhere in the proof to show that we can always take vertices of sufficiently large degree if we haven't restricted down too far. □

The spectral information of $J(n, r)$ is known, so this theorem gives an upper bound for s_n:

Theorem 4.2 (Bansal, Pendavingh, van der Pol 2012)
We have $\log\log s_n \leq n - \frac{3}{2}\log n + \frac{1}{2}\log\frac{2}{\pi} + 1 + o(1)$.

This is the same upper bound they prove for m_n, as stated earlier. Unlike with the lower bound, this doesn't directly imply a bound for m_n, since m_n is *bigger* than s_n; but we'll see that the technique can be modified to give a result for m_n as well. In fact combining this with the theorem by Pendavingh and van der Pol from 2014, that $\log m_n = (1 + o(1))\log s_n$, would give the same upper bound on $\log\log m_n$ (up to an additive $o(1)$ term), but that theorem is from after their proof of the upper bound on m_n (which is from 2012).

First looking at s_n, combined with the lower bound above, and removing the logarithms, we now know that

$$f(n) \lesssim s_n \lesssim f(n)^2$$

for some function f (coming from the lower bound; the extra square comes from the $+1$ in the upper bound). This is the best understanding we have for independent sets of the Johnson graph; if you could come up with better independent sets or better upper bounds, then you could improve the bounds on s_n. If you could get a *lower* bound, this would immediately carry over to the problem of m_n. An *upper* bound wouldn't, but you might be able to modify the technique to work for general matroids, as here. (On the $\log\log$ scale, upper bounds for s_n *would* carry over to m_n using the theorem that $m_n = (1 + o(1))\log s_n$.)

§4.2 Flat Covers

We'll now see how to obtain the upper bound on m_n. (As before, r denotes the rank of the matroid, and we're trying to bound $m_{n,r}$.)

Again, we'll focus on the non-bases — we'd like a way to describe what the non-bases (of size r) of a given matroid are (in the case of a sparse paving matroid, they were an independent set in the Johnson graph; but in general they could be something else).

Definition 4.3. Given a dependent set $X \subseteq E$ and a flat F, we say that F *covers* X if $|F \cap X| > r_M(F)$.

Intuitively, if X is dependent then it has too much stuff somewhere, and the flat F captures *where* X has too much stuff. (Note that if X is independent, then this cannot be true for any flat F.)

Example 4.4

If M is the matroid corresponding to a set of vectors, then a flat is the set of all vectors in a subspace. If X is dependent, then there must be some subspace where X has more vectors than the dimension of that subspace; then this subspace is a flat covering X.

The way we'll describe the non-bases is by using such flats to detect whether a set is dependent.

Definition 4.5. A *flat cover* of M is a collection $\mathcal{Z}$ of flats $F \subseteq E$ such that for all $X \in \binom{E}{r}$ which are not bases, there exists a flat F which covers X, i.e., with $|X \cap F| > r_M(F)$.

The point is that a flat cover encodes what all the non-bases of size r are — given a set X of size r, to check whether it is a basis or a non-basis, we can compare it to every flat. Then X is a non-basis if and only if there exists a flat $F \in \mathcal{Z}$ with $|X \cap F| > r_M(F)$.

So if we can find a flat cover $\mathcal{Z}$ of M, then we can fully encode M with the set

$$\{(F, r_M(F)) \mid F \in \mathcal{Z}\}.$$

Our goal is then to find an *efficient* flat cover — if we can encode any matroid M with a flat cover of at most a given size, then we can obtain a bound on the number of possible matroids by bounding the number of possible such flat covers. Of course, we could obtain *a* flat cover by simply taking every non-basis, choosing a flat covering that set, and putting all these flats in a list; this is very inefficient because we'd be using one flat to cover every non-basis. The point is that we can find a much smaller flat cover.

The idea is to take the Johnson graph $J(n, r)$ again and cover it with patches, trying to be as efficient *locally* as possible; then combining these patches gives a globally good $\mathcal{Z}$. One bound used to obtain such a construction is the following.

Lemma 4.6

Given any $X \in \binom{E}{r}$, there exists a collection $\mathcal{Z}_X$ of at most r flats covering $X \cup N(X)$.

(We use $N(X)$ to refer to the neighbors of X in the Johnson graph.)

This is significantly better than the silly cover where we choose one flat for each non-basis — the degree of the Johnson graph is $r(n - r)$, so here instead of having one flat cover one set, we have r flats covering $r(n - r) + 1$ sets (which is substantially more than r).

Then given this lemma, we can choose a dominating set in the Johnson graph (which can be done by randomness), choose such a $\mathcal{Z}_X$ for each X in the dominating set, and combine them to get a flat cover $\mathcal{Z}$.

This lemma already gives the correct term of $-\frac{3}{2}\log n$ — so it's already an improvement from the upper bound from 1973 — but it gives weaker bounds for the lower-order terms (there's an extra $+2\log\log n$ or something similar). To get the bound stated above, we can use a stronger lemma.

Lemma 4.7

Given any *dependent* $X \in \binom{E}{r}$, there exists a collection $\mathcal{Z}_X$ of at most 2 flats covering $X \cup N(X)$.

So we've improved r to 2, but only when X is dependent. This means we can't just take a dominating set in the graph anymore and find $\mathcal{Z}_X$ for each of its elements, because we don't know if they're dependent. Instead, we run the algorithm from the proof of Theorem 4.1 to find a good collection of dependent sets which cover most of the graph (we only need to cover the dependent sets), and then use this lemma for those dependent sets.

This is the method used to prove the upper bound on m_n. In order to prove the log-scale equivalence with s_n (i.e., that $\log m_n = (1 + o(1)) \log s_n$), they use similar ideas, but tweak the algorithm and modify it to get a bound in terms of s_n.

As a quick description of the constructions of $\mathcal{Z}_X$ in the two lemmas, for the first lemma you construct your flats by taking the closures and removing one thing at a time. The second lemma is similar, but X being dependent allows us to only need one of those smaller sets — if $r_M(X) < r - 1$ then we can just take $\mathcal{Z}_X = \{\mathrm{cl}_M(X)\}$, while if $r_M(X) = r - 1$ then we need to include one other set as well.

(The algorithm in Theorem 4.1, given an independent set, produces an efficient subset of it whose neighborhood covers most of the graph (this is what it meant to eliminate most of the possibilities outside the subset). But it can be used even if the set we start off with isn't an independent set; and it can still be used to get something similar that's useful here.)