Report: Matroids and Derandomization of Isolation Lemma

Instructor: Rohit Gurjar

Soham Chatterjee

sohamchatterjee999@gmail.com
Website: sohamch08.github.io

2024

Contents

Chapter 1

Introduction

1.1 Matroids

Definition 1.1.1: Matroid

A matroid $M = (E, \mathcal{I})$ has a ground set E and a collection I of subsets of E called the *Independent Sets* st

1. Downward Closure: If $Y \in \mathcal{I}$ then $\forall\, X \subseteq Y$, $X \in \mathcal{I}$.
2. Extension Property: If $X, Y \in \mathcal{I}$, $|X| < |Y|$ then $\exists\, e \in Y - X$ such that $X \cup \{e\}$ also written as $X + e \in \mathcal{I}$

Observation. *A maximal independent set in a matroid is also a maximum independent set. All maximal independent sets have the same size.*

Base: Maximal Independent sets are called bases.
Rank of $S \in I$: We define the rank function of a matroid $r : \mathcal{P}(E) \to \mathbb{Z}$ where $r(S) = \max\{|X| \colon X \subseteq S, X \in I\}$ We def
Rank of a Matroid: Size of the base.
Span of $S \in I$: $\{e \in E \colon rank(S) = rank(S + e)\}$

1.2 Examples of Matroids

1.2.1 Uniform Matroid

It is denoted as $U_{k,n}$ where $E = [n]$ and $I = \{X \subseteq E \mid |X| \leq k\}$.
Free Matroid: When $k = n$ we take all possible subsets of E into I. This matroid is called Free Matroid i.e. $U_{n,n}$

1.2.2 Partition Matroid

Given $E = E_1 \sqcup E_2 \sqcup \cdots \sqcup E_l$ where $\{E_1, \ldots, E_l\}$ is a partition of E and $k_1, \ldots, k_l \in \mathbb{N} \cup \{0\}$

$$I = \{X \subseteq E \colon |X \cap E_i| \leq k_i \;\forall\, i \in [l]\}$$

then $M = (E, I)$ is a partition matroid.

Note:-

If the E_i's are not a partition then suppose E_1, E_2 has nonempty partition then we will not have a matroid.
For example: $E_1 = \{1, 2\}$, $E_2 = \{2, 3\}$ and $k_1 = k_2 = 1$ then $X = \{1, 3\}$ is independent but $Y = \{2\} \subsetneq X$ is not a matroid.

1.2.3 Linear Matroid

Given a $m \times n$ matrix denote its columns as $A_1, \ldots, A_n$. Then

$$I = \{X \subseteq [n] \colon \text{Columns corresponding to } X \text{ are linearly independent}\}$$

Here if the underlying field is $\mathbb{F}_2$ then it is called *Binary Matroid* and for $\mathbb{F}_3$ it is called *Ternary Matroid*.

1.2.4 Representable Matroid

A matroid with which we can associate a linear matroid is called a representable matroid.

Eg: $U_{2,3}$. It can be represented by the matrix $A = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$, over $\mathbb{F}_2$. Over $\mathbb{F}_3$ it is same as $U_{3,3}$.

Note:-

There are matroids which are not representable as linear matroids in some field. There are matroids which are not representable on any field as well.

Lemma 1.2.1

$U_{2,4}$ is not representable over $\mathbb{F}_2$ but representable over $\mathbb{F}_3$

1.2.5 Regular Matroid

There are the matroids which are representable over all fields.

Lemma 1.2.2

Regular Matroids are precisely those which can be represented over $\mathbb{R}$ by a Totally Uni-modular matrix

1.2.6 Graphic Matroid / Cyclic Matroid

For a graph $G = (V, E)$ the graphic matroid $M_G = (E, I)$ where

$$I = \{F \subseteq E \colon F \text{ is acyclic}\}$$

Hence I is the collection of forests of G. It follows the downward closure trivially. For extension property let $k = |F_1| < |F_2| = l$ and then there are $n - k$ and $n - l$ components. So $n - k > n - l$. So $\exists$ an edge in F_2 which joins 2 components in F_1.

Lemma 1.2.3

A subset of columns is linearly independent iff the corresponding edges don't contain a cycle in the incidence matrix

Lemma 1.2.4

Graphic Matroids are Regular Matroids

Proof Idea: Use Incidence Matrix. ■

1.2.7 Matching Matroids

We can try to define it like this but it will not work:

Problem 1.1

Is the following a matroid: $E =$ Edges of a graph and $I = \{F \subseteq E \colon F \text{ is a matching}\}$

Solution: It is not a matroid since maximal matchings can not be extended to a maximum matching.

■

Correct way will be: For a graph $G = (V, E)$ the ground set $= V$ and

$$I = \{S \subseteq V \colon \exists \text{a matching that matches all vertices in } S\}$$

The downward closure property trivially holds. For extension property is $|S| < |S'|$ then there exists another vertex in S' which is not matched with S, so we can add that vertex to S.

1.3 Axiom Systems for a Matroid

1.3.1 Circuits

Assume we have a matroid $M = (E, I)$.

Definition 1.3.1: Circuit

A minimal dependent set C such that $\forall\, e \in C$, $C - e$ is an independent set.

Theorem 1.3.1

Let $S \in I$. $S + e \notin I$. Then $\exists!\, C \subseteq S + e$.

Proof. Given $S + e \notin I$. Take the set Σ where $T \in \Sigma$ if $t \notin I$ and $T \subseteq S + e$. Σ is nonempty since $S + e \in \Sigma$. Now under the ordering of inclusion T has a minimal element. Hence this minimal element is the desired circuit C which is minimal dependent set contained in $S + e$.

Now suppose it is not unique. Let $C_1, C_2 \subseteq S + e$ be circuits. Suppose $f \in C_1 - C_2$. Then $S - e + f$ will still be dependent since $C_2 \subseteq S - e + f$. Now by definition we get that $C_1 - f$ is independent. Therefore we extend $C_1 - f$ to an independent set by adding the elements of S till we reach same size as $|S|$. Now $e \in C$ since C_1 was formed because of addition of e. Hence if we extend $C_1 - f$ till same cardinality as S we will add all the edges of S not in $C_1 - f$ except f since adding f will make C be a dependent subset of an independent set which is not possible. Hence $C_1 - f$ will be extended to $S - f + e$. Therefore $S + e - f$ is independent which contradicts our previous conclusion that $S + e - f$ is dependent. Hence contradiction. ■

Chapter 2

Isolation Lemma

Chapter 3

Matroid Polytope

Chapter 4

Matroid Parity Problem

Chapter 5

Fractional Matroid Matching

Fractional Matroid Matchings generalizes the case for Matroid Matching or Matroid Parity problem with allowing fractional solutions for the polytope which we will show below. We start with the same kind of state like Matroid Parity Problem

5.1 Fractional Matroid Matchings Polytope

Let $M = (E, \mathcal{I})$ is a matroid with ground set E of even cardinality and with elements E is partitioned into lines or pairs. Let L is the set of lines. Let $r : \mathcal{P}(E) \to \mathbb{Z}$ be the rank function and $sp : \mathcal{P}(E) \to \mathcal{P}(E)$ be the span function. Assume that $\forall\, l \in L, r(L) = 2$. With this setting (same as matroid parity problem) we now define the polytope following [Van92]

Definition 5.1.1: Fractional Matroid Matching Polytope

Let $\mathscr{L}$ denote the lattice of flats in M wtih $S_1 \wedge S_2 = S_1 \cap S_2$ and $S_1 \vee S_2 = sp(S_1 \cup S_2)$ and for each line $l \in L$ let $a_l : \mathscr{L} \to \{0, 1, 2\}$ be the function $a_l(S) = r(sp(l) \cap S)$. Now for any $S \in \mathscr{L}$ and $x \in \mathbb{R}_+^{|L|}$ let $a(S) \cdot x$ denote the vector $(a(S) \cdot x)_l = a_l(S) x_l$ for any $l \in L$. Then the set

$$FP(M) = \{x \in \mathbb{R}_+^{|L|} \mid : a(S) \cdot x \leq r(S) \text{ for each } S \in \mathscr{L}\}$$

is fractional matroid matching polytope for M and each vector $x \in FP(M)$ is called a fractional matroid matching.

Now we can also allow x to be from $\mathbb{R}^{|L|}$, not restricting only to positive vectors. This polytope is a subset of $[0, 1]^m$. We will explain the setting wtih the following example:

Example 5.1

Consider the matroid M with ground set

$$E = \{a_1, a_2, b_1, b_2, c_1, c_2, d_1, d_2\}$$

where every 4 element subset of E is a base except these 4 sets

$$\begin{array}{ccc} \{a_1, a_2, b_1, b_2\}, & \{a_1, a_2, c_1, c_2\}, & \{a_1, a_2, d_1, d_2\}, \\ \{b_1, b_2, c_1, c_2\}, & \{b_1, b_2, d_1, d_2\}, & \{c_1, c_2, d_1, d_2\} \end{array}$$

Now the lines are defined to be

$$l_1 = \{a_1, a_2\} \qquad l_2 = \{b_1, b_2\}, \qquad l_3 = \{c_1, c_2\}, \qquad l_4 = \{d_1, d_2\}$$

Now the flats of M are empty set, individual elements, every pair of elements, set consists of one element from each of three lines, pair of line and E. Hence $FP(M)$ is the set of $x \in \mathbb{R}_+^{|L|}$ satisfying

$$2x_1 + 2x_2 \leq 3 \qquad 2x_1 + 2x_3 \leq 3 \qquad 2x_1 + 2x_4 \leq 3$$
$$2x_2 + 2x_3 \leq 3 \qquad 2x_2 + 2x_4 \leq 3 \qquad 2x_3 + 2x_4 \leq 3$$
$$2x_1 + 2x_2 + 2x_3 + 2x_4 \leq 4$$

$$2x_i \leq 2 \quad \text{for each } i \in [4]$$

Now the we show the theorem Theorem 5.1.1 which states that the fractional matroid matching polytope arises as a linear relaxation of the matroid matching problem.

Theorem 5.1.1 [Van92, Theoerm 2.1]
An integer vector $x \in \mathbb{R}_+^{|L|}$ is the incidence vector of a matroid matching iff x is a fractional matroid matching.

You can clearly see this theorem by comparing the Matroid Matching Polytope and Fractional Matroid Matching Polytope so we are omitting the proof.

Theorem 5.1.2 [GP13, Theorem 1]
The vertices of the fractional matroid matching are half-integral

Definition 5.1.2: Weighted Fractional Linear Matroid Matching Problem

It is to find a fractional matroid matching x that maximizes $w \cdot x$ for a non-negative weight assignment $w : L \to \mathbb{Z}_+$
For plain Fractional Linear Matroid Matching Problem we need to find a fractional matroid matching x which maximizes the size i.e. L_1 norm of x which is $\sum_{l \in L} |x_l|$.

Gijswijt and Pap in [GP13] gave a polynomial time algorithm for weighted fractional linear matroid matching. They also gave the following characterization for maximizing face of the polytope with respect to a weight function.

Theorem 5.1.3 [GP13, Prood of Theorem 1]
Let $L = \{l_1, \ldots, l_m\}$ be a set of lines with $l_i \subseteq \mathbb{F}^n$ and $w : L \to \mathbb{Z}$ be a weight assignment on L. Let F denote the set of fractional linear matroid matchings maximizing and $S \subseteq [m]$ such that every $x \in F$ has $y_e = 0$ for all $e \in S$. Then for some $k \leq n$, $\exists$ a $k \times m$ matrix D_F and $b_F \in \mathbb{Z}^k$ such that

- $D_F \in \{0, 1, 2\}^{k \times m}$
- The sum of entries in any column of D_F is exactly 2
- A fractional matroid matching x is in F iff $y_e = 0$ for $e \in S$ and $D_F = x = b_F$.

5.2 Isolating Weight Assignment for Fractional Matroid Matching

In this section we will describe how we can construct an isolating weight assignment for fractional matroid matching with just the number of lines as input.

Now for a face F of a polytope, let $\mathcal{L}_F$ denote the lattice

$$\mathcal{L}_F = \{v \in \mathbb{Z}^{|L|} \mid v = \alpha(x_1 - x_2) \text{ for some } x_1, x_2 \in F \text{ and } \alpha \in \mathbb{R}\}$$

and $\lambda(\mathcal{L}_F)$ denote the length of the shortest vector of $\mathcal{L}_F$. Hence $\mathcal{L}_F$ consistes of all integral vectors parallel to the face F.

Now by Theorem 5.1.3 the face maximizing the size is described by the equation $D_F x = b_F$ where $D_F \in \{0,1,2\}^{k\times|L|}$ with column sum 2. Hence $\mathcal{L}_F$ is exactly the set of integral vectors in the null space of D_F. Therefore

$$\mathcal{L}_F = \{v \in \mathbb{Z}^{|L|} \mid D_F v = 0\}$$

So we will prove the following theorem which shows the number of vectors in $\mathcal{L}_F$ with size less than twice the length of shortest vector is polynomially bounded.

Theorem 5.2.1 [GOR24]
Let $D \in \{0,1,2\}^{p\times m}$ be a matroix such that the sum of entries of each column equals 2. Let $\mathcal{L}_D$ denote the lattice $\{v \in \mathbb{Z}^m \mid Dv = 0\}$. Then it holds that

$$|\{v \in \mathcal{L}_D \mid |v| < 2\lambda(\mathcal{L}_D)\}| \leq m^{O(1)}$$

With this theorem we have

Theorem 5.2.2 [GTV18, Theorem 2.5]
Let k be a positive integer and $P \subseteq \mathbb{R}^m$ a polytope such that its extreme ppoints are in $\left\{0, \frac{1}{k}, \frac{2}{k}, \ldots, 1\right\}^m$ and there exists a constant $c > 1$ with

$$|\{v \in \mathcal{L}_F \colon |v| < c\lambda(\mathcal{L}_F)\}| \leq m^{O(1)}$$

for any face F of P. Then there exists an algorithm that, given k and m, outputs a set $\mathcal{W} \subseteq \mathbb{Z}^m$ of $m^{O(\log km)}$ weight assignments with weights bounded by $m^{O(\log km)}$ such that there exists at least one $w \in \mathcal{W}$ that is isolating for P, in time $polylog(km)$ using $m^{O(\log km)}$ many parallel processors.

Using this we finally have an algorithm for isolating a fractional matroid matching polytope:

Theorem 5.2.3 [GOR24, Theorem 3.1]
There exists an algorithm that given $m \in \mathbb{Z}_+$ outputs a set $\mathcal{W} \subseteq \mathbb{Z}_+^m$ of $m^{O(\log m)}$ weight assignments with weights bounded by $m^{O(\log m)}$ such that, for any fractional matroid matching polytope P of m lines, there exists at least one $w \in \mathcal{W}$ that is isolating for P, in time $polylog(m)$ usign $m^{O(\log m)}$ many parallel processors.

Chapter 6

Bibliography

[GOR24] Rohit Gurjar, Taihei Oki, and Roshan Raj. Fractional linear matroid matching is in quasi-nc, 2024.

[GP13] Dion Gijswijt and Gyula Pap. An algorithm for weighted fractional matroid matching. *Journal of Combinatorial Theory, Series B*, 103(4):509–520, July 2013.

[GTV18] Rohit Gurjar, Thomas Thierauf, and Nisheeth K. Vishnoi. Isolating a vertex via lattices: Polytopes with totally unimodular faces, 2018.

[Van92] John H Vande Vate. Fractional matroid matchings. *Journal of Combinatorial Theory, Series B*, 55(1):133–145, 1992.