Matroids in Lean: Project Planning

Ivan Sergeev

ISTA

10 October 2024

Outline

Outline

What is Seymour's Decomposition Theorem?

- Any 1-, 2-, and 3-sum of two regular matroids is regular
- Any regular matroid can be decomposed into matroids that are graphic, cographic, or isomorphic to R_{10} by repeated 1-, 2-, and 3-sum decompositions

Why Matroids?

- Generalize vector spaces and linear independence (vector matroids)
- Generalize graphs (graphic matroids)
- Generalize extensions of fields (algebraic matroids)
- Axiomatic definition $\Rightarrow$ amenable to formalization

Why Seymour's Decomposition Theorem?

- Structural characterization of the class of regular matroids
- Efficient algorithm for testing if a binary matroid is regular
- Efficient algorithm for testing if a real matrix is totally unimodular
- Construction of $\{0, \pm 1\}$ and $\{0, 1\}$ totally unimodular matrices
- Structural approach to certain problems

Concrete Application: Cycle Polytope

- **Given:** Connected binary matroid M with weighs w_e for all elements e
- **Goal:** Find a disjoint union C of circuits of M such that $\sum_{e \in C} w_e$ is maximized
- **Note:** This includes the max cut problem, so can be NP-hard
- Regular matroid decomposition theorem leads to:
  - Characterization of the cycle polytope
  - Polyhedral approach for a special subclass: efficient separation $\Rightarrow$ optimization

Outline

Matroids: Main Definition

- Let E be a finite ground set
- Let $\mathcal{I} \subseteq 2^E$ be a family of subsets satisfying:
  - $\emptyset \in \mathcal{I}$ (non-empty)
  - if $A \subseteq B \in \mathcal{I}$, then $A \in \mathcal{I}$ (down-closed)
  - if $A, B \in \mathcal{I}$ and $|A| < |B|$, then $A + x \in \mathcal{I}$ for some $x \in B \setminus A$ (exchange property)
- Then the pair $M = (E, \mathcal{I})$ is called a **matroid**

Matroids: Key Notions

- A **base** of M is a maximal independent subset of E
- A **cobase** is the set $E - X$ for some base X
- The **dual matroid** of M is $M^* = (E, \mathcal{I}^*)$ where $\mathcal{I}^*$ is all cobases and their subsets

- For $A \subseteq E$, the **rank** of A is the cardinality of a maximal independent subset of A
- A **circuit** is a minimal dependent subset of E
- A **cocircuit** of M is a **circuit** of M^*

Graphic Matroids

- Let G be a graph with edge set E, let $\mathcal{I}$ be all forests in G
- Then the **graphic matroid** of G is $M = M(G) = (E, \mathcal{I})$
- A **cographic** matroid is the dual of a graphic matroid
- A **planar** matroid is one that is graphic and cographic

Binary Matroids

- Let F be a binary matrix over $\mathrm{GF}(2)$ with a column index set E
- Let $\mathcal{I}$ be all $Z \subseteq E$ such that the columns of F indexed by Z are independent
- The **binary matroid** generated by F is $M = (E, \mathcal{I})$

- **Note:** graphic matroids are binary (node-edge incidence matrix)

- **Representation matrix:**
  - Delete all $\mathrm{GF}(2)$-dependent rows from F
  - Perform binary row operations to arrive at $[I \mid B]$
  - B is a representation matrix (can be empty)

Regular Matroids

- A real matrix is **totally unimodular** (TU) if all its subdeterminants are 0 or ± 1
- A binary matroid is **regular** if it has a representation matrix with a TU signing

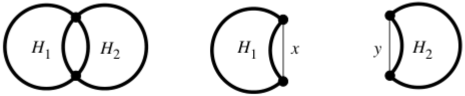
- **Important properties:**
  - A binary matroid is regular iff every representation matrix has a TU signing
  - For a regular matroid, its dual and all its minors are regular
  - Every graphic and cographic matroid is regular

Special Binary Matroids

- Nonregular F_7 is represented by $\begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$
- Regular, nongraphic, noncographic R_{10} is represented by $\begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix}$
- Regular, nongraphic, noncographic R_{12} is represented by $\begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$

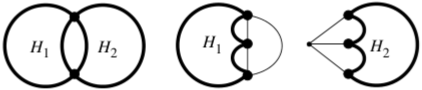
1-, 2-, and 3-Sums of Graphs

- 1-sums: identification of a node
- 2-sums:



Graph G Graph G_1 Graph G_2

- 3-sums:



Graph G Graph G_1 Graph G_2

1-sums of Binary Matroids

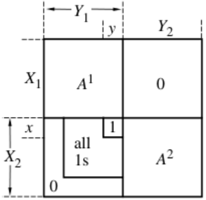
- A 1-separable matroid can be represented by

$$\begin{array}{c|c|c|} & Y_1 & Y_2 \\ \hline X_1 & A^1 & 0 \\ \hline X_2 & 0 & A^2 \\ \hline \end{array}$$

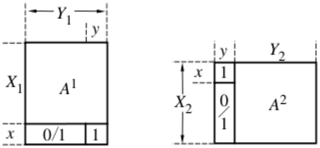
- This also defines $M_1 \oplus_1 M_2$ for M_1 and M_2 represented by A^1 and A^2

2-sums of Binary Matroids

- A 2-separable matroid can be represented by



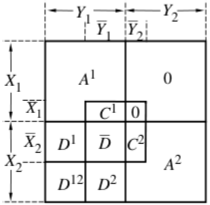
- This also defines $M_1 \oplus_2 M_2$ for M_1 and M_2 represented by



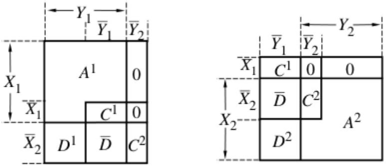
- The bottom-left submatrix is reconstructed via $\left(\text{column } y \text{ of } B^2\right) \cdot \left(\text{row } x \text{ of } B^1\right)$

3-sums of Binary Matroids

- A 3-separable matroid can be represented by



- This also defines $M_1 \oplus_3 M_2$ for M_1 and M_2 represented by



- The bottom-left submatrix is computed via a formula from these submatrices

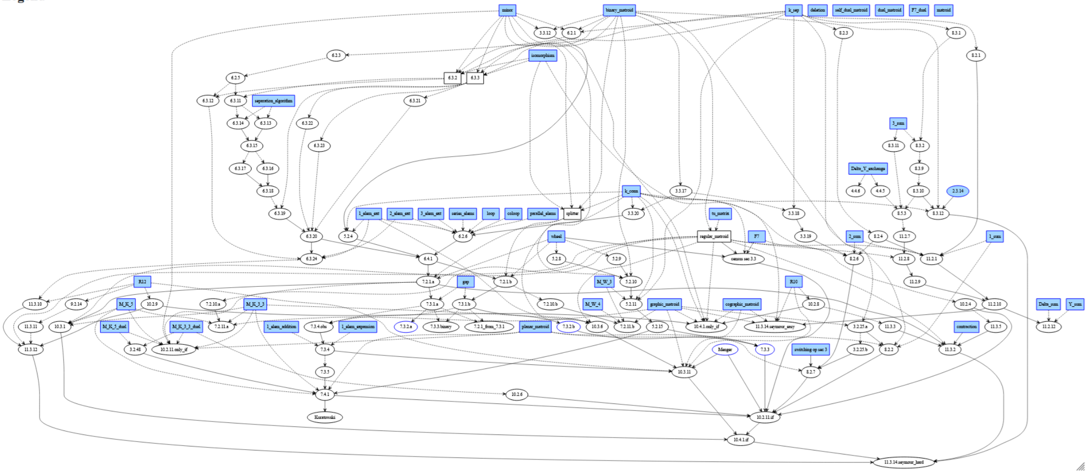
Outline

Seymour's Decomposition Theorem

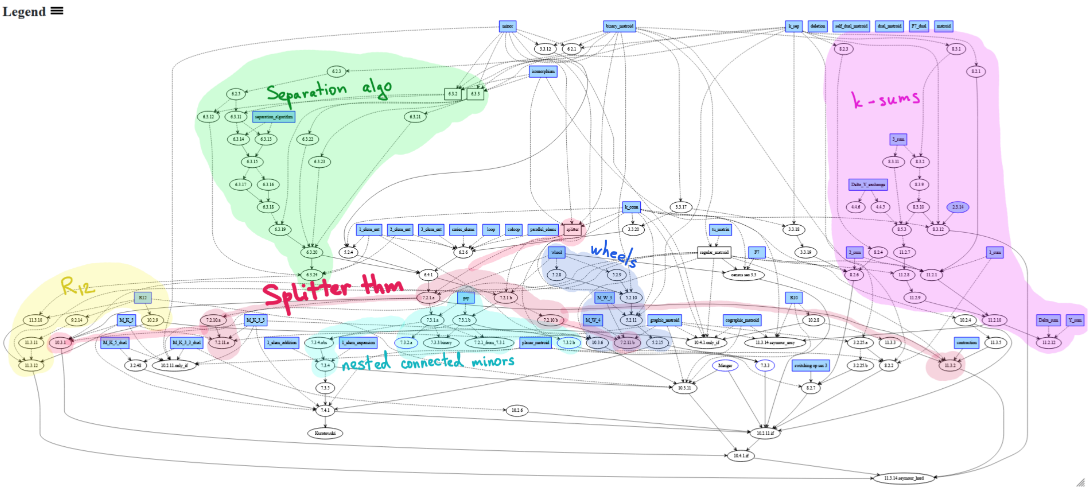
- Any 1-, 2-, and 3-sum of two regular matroids is regular
- Any regular matroid can be decomposed into matroids that are graphic, cographic, or isomorphic to R_{10} by repeated 1-, 2-, and 3-sum decompositions

Dependency Graph

Legend ≡



Dependency Graph



Easy Direction

- Any 1-, 2-, and 3-sum of two regular matroids is regular
- **Proof sketch:**
- Use the matrix representation of the 1-, 2-, or 3-sum
- Use TU signings of representations of the summands
- If necessary, sign the remaining elements via a specific formula
- Prove TUness of the composite signed matrix

Hard Direction

- Any regular matroid can be decomposed into matroids that are graphic, cographic, or isomorphic to R_{10} by repeated 1-, 2-, and 3-sum decompositions

- **Ingredients:**

1. A 3-connected regular matroid has no R_{10} or R_{12} minor $\Rightarrow$ graphic or cographic
2. A 3-connected regular matroid with an R_{10} minor is isomorphic to R_{10}
3. A regular matroid with an R_{12} minor is a 3-sum of two proper minors

Hard Direction: Proof

- Let M be a regular, nongraphic, noncographic matroid
- If M is 1- or 2-separable, then M is a 1- or 2-sum (property of k-sums)
- Given M is 3-connected, M has an R_{10} or R_{12} minor (ingredient 1)
- If M has an R_{10} minor, then it is isomorphic to R_{10} (ingredient 2)
- If M has an R_{12} minor, then M is a 3-sum (ingredient 3)

Outline

Ingredient 1

- A 3-connected regular matroid has no R_{10} or R_{12} minor $\Rightarrow$ graphic or cographic
- **Sub-ingredients:**

1. Regular matroid has no $M(K_5)$, $M(K_5)^*$, $M(K_{3,3})$, or $M(K_{3,3})^*$ minors $\Rightarrow$ planar
2. $M(K_5)$ is a splitter for regular matroids with no $M(K_{3,3})$ minors
3. Regular matroid is 3-connected, nongraphic, noncographic, has an $M(K_{3,3})$ minor, and all its proper minors are graphic or cographic $\Rightarrow$ isomorphic to R_{10} or R_{12}

Ingredient 1

- A 3-connected regular matroid has no R_{10} or R_{12} minor $\Rightarrow$ graphic or cographic
- **Sub-ingredients:**

1. Regular matroid has no $M(K_5)$, $M(K_5)^*$, $M(K_{3,3})$, or $M(K_{3,3})^*$ minors $\Rightarrow$ planar
   - Relies on many involved results: Menger's theorem, Kuratowski's theorem, the wheel theorem, and the census of small 3-connected matroids
2. $M(K_5)$ is a <u>splitter</u> for regular matroids with no $M(K_{3,3})$ minors
   - Proof = <u>splitter theorem</u> + case analysis
3. Regular matroid is 3-connected, nongraphic, noncographic, has an $M(K_{3,3})$ minor, and all its proper minors are graphic or cographic $\Rightarrow$ isomorphic to R_{10} or R_{12}
   - Relies on results about 3-connected nested extensions, which require <u>splitter theorem</u>
   - Long and technical proof with many cases and graph constructions

Ingredient 1: Proof

- Let M be a 3-connected, regular, nongraphic, noncographic matroid
- M is not planar + Ingredient 1.1 $\Rightarrow$ M or M^* has an $M(K_5)$ or $M(K_{3,3})$ minor
- Ingredient 1.2 $\Rightarrow$ M or M^* has an $M(K_{3,3})$ minor or is isomorphic to $M(K_5)$
- Latter case is a contradiction
- Former case + ingredient 1.3 $\Rightarrow$ M or M^* has R_{10} or R_{12} as a minor
- R_{10} and R_{12} are self-dual $\Rightarrow$ M has R_{10} or R_{12} as a minor

Ingredient 1: Proof

- Let M be a 3-connected, regular, nongraphic, noncographic matroid
- M is not planar + Ingredient 1.1 $\Rightarrow$ M or M^* has an $M(K_5)$ or $M(K_{3,3})$ minor
- Ingredient 1.2 $\Rightarrow$ M or M^* has an $M(K_{3,3})$ minor or is isomorphic to $M(K_5)$
- Latter case is a contradiction
- Former case + ingredient 1.3 $\Rightarrow$ M or M^* has R_{10} or R_{12} as a minor
- R_{10} and R_{12} are self-dual $\Rightarrow$ M has R_{10} or R_{12} as a minor

- There is an alternative proof [Geelen, Gerards, '04]
  - Seems shorter, but appears to heavily rely on graph-theoretic results

Ingredient 2

- A 3-connected regular matroid with an R_{10} minor is isomorphic to R_{10}
- **Equivalent statement:** R_{10} is a splitter of the class regular matroids

- **Sub-ingredients:**

1. The splitter theorem
2. R_{10} is self-dual
3. F_7 is not regular
4. "Graph plus T set" constructions for R_{10} and F_7

Ingredient 2: Proof

- Represent R_{10} as a graph plus T set
- R_{10} is self-dual, so suffices to consider 1-element additions in the splitter theorem
- Up to isomorphism, there are only 3 distinct 3-connected 1-element additions
- Case 1 (graphic): after contracting a specific edge, the resulting graph contains a subdivision of the graph plus T set for F_7 $\Rightarrow$ this extension is nonregular
- Cases 2, 3 (nongraphic): both reduce to the graph plus T set for F_7 $\Rightarrow$ nonregular

Ingredient 3

- A regular matroid with an R_{12} minor is a 3-sum of two proper minors
- **Sub-ingredients:**

1. Let $\mathcal{M}$ be a class of binary matroids closed under isomorphism and taking minors. Let N be a minor that lies in $\mathcal{M}$, but its 1- and 2-element extensions of a specific form are not in $\mathcal{M}$. Let N have a 3-separation. If $M \in \mathcal{M}$ has an N minor, then any 3-separation of any such minor corresponding to the 3-separation of N under an isomorphism induces a 3-separation of M.
   - Corollary from a characterization theorem for a separation algorithm
2. For a binary 3-connected matroid, any 3-separation (E_1, E_2) with $|E_1|, |E_2| \geq 4$ produces a 3-sum and vice versa.

Ingredient 3: Proof

- Apply Ingredient 1 with regular matroids as $\mathcal{M}$ and R_{12} as N
- Calculate all 3-connected regular 1-element extensions of R_{12}, check cases
- Apply Ingredient 2 to get a 3-sum from a 3-separation

Outline

Splitter Theorem

- Let $\mathcal{M}$ be a class of binary matroids closed under isomorphism and taking minors
- Let N be a 3-connected minor of $\mathcal{M}$ on at least 6 elements, and not a wheel
- **Claim:** The following are equivalent:
  - N is a **splitter** of $\mathcal{M}$, i.e., every $M \in \mathcal{M}$ with a proper N minor has a 2-separation
  - $\mathcal{M}$ does not contain a 3-connected 1-element extension of N
- (There is also a wheel version, it is used in 3-connected nested extensions)

Proof of Splitter Theorem

- If N is a splitter, then trivial. Assume N is not a splitter.
- Suppose no 3-connected 1-element extension of N is in $\mathcal{M}$
- Then $\exists M \in \mathcal{M}$: 3-connected, has no 2-separation, contains N as a proper minor
- Technical lemma $\Rightarrow$ M has a 3-connected minor N' that extends an N minor
- 1-extension case: contradicts the assumptions on $\mathcal{M}$
- 2-extension case: N' is derived from N by one addition and one expansion
- Analyze the structure of a binary matrix representation of N' that displays N
- Arrive at: N' contains a 3-connected 1-element extension of an N minor
- This contradicts the assumptions on $\mathcal{M}$

Technical Lemma for Splitter Theorem

- Let M be a 3-connected binary matroid
- Let N be a 3-connected proper minor of M with ≥ 6 elements
- **Claim:** M has an N minor $\overline{N}$ and a 3-connected minor N' such that
  - N' is a 1-element extension of $\overline{N}$, or
  - N' is a 2-element extension, by one addition and one expansion, of $\overline{N}$

- **Proof sketch:**
- Construct a connected minor N' that is a 1-element extension of N by $z \in M \setminus N$
- Reason about a matrix representation of N and N'
- Apply a characterization theorem for a separation algorithm, do case analysis

Corollaries of Splitter Theorem

- $M(K_5)$ is a splitter of the regular matroids with no $M(K_{3,3})$ minors
- R_{10} is a splitter of the class of regular matroids
- Theorems about nested connected minors, for example:
  - Let M be a 3-connected binary matroid
  - Let N be a 3-connected proper minor of M on ≥ 6 elements, and not a wheel
  - Then there is a sequence $M_0, \ldots, M_t = M$ of nested 3-connected minors where M_0 is isomorphic to N and where the rank $+$ corank gap $= 1$

Separation Algorithm

- Suppose a minor N of M has an exact k-separation (F_1, F_2)
- Does M have an induced k-separation (E_1, E_2) with $E_{1,2} \supseteq F_{1,2}$?
- **Separation algorithm:** explicit recursive procedure to answer this question

Separation Algorithm: Characterization Theorem

- Suppose M has at least one minor isomorphic to N
- ...that has a k-separation corresponding to (F_1, F_2) under an isomorphism
- ...and which does not induce a k-separation of M
- Suppose M is minimal with respect to the above conditions
- **Claim:** M is represented by a matrix corresponding to a 1- or 2-extension of N and satisfying certain additional properties

- **Proof** $=$ separation algorithm $+$ case analysis

Separation Algorithm: Corollary

- Let $\mathcal{M}$ be a class of binary matroids closed under isomorphism and taking minors
- Suppose $\mathcal{M}$ contains N with a k-separation, but not its 1- and 2-element extensions represented by the matrices from the characterization theorem
- Suppose $M \in \mathcal{M}$ has a minor isomorphic to N
- **Claim:** Any k-separation of any such minor corresponding to the k-separation of N under an isomorphism induces a k-separation of M

Separation Algorithm: Proof of Corollary

- $\mathcal{M}$ is closed under isomorphism $\Rightarrow$ assume that N itself is a minor of M
- Suppose the k-separation of N does not induce one in M
- Then M or its minor containing N satisfies the characterization theorem
- $\mathcal{M}$ is closed under taking minors $\Rightarrow$ $\mathcal{M}$ contains a 1- or 2-element extension of N represented by one of the matrices from the characterization theorem
- This contradicts the assumptions on $\mathcal{M}$

3-separations and 3-sums

- For a binary 3-connected matroid, any 3-separation (E_1, E_2) with $|E_1|, |E_2| \geq 4$ produces a 3-sum and vice versa

- **Proof sketch:**
- A matrix representation of a 3-sum produces a 3-separation
- Consider a 3-separation, which must be exact, as M is 3-connected
- Analyse the structure of the corresponding representation matrix
- Consider a shortest path in the corresponding bipartite graph, apply path shortening technique to reduce it to a path of length 2 via pivots
- Reason about the entries of the matrix and the effects of the pivots
- Eventually arrive at a matrix representation of a 3-sum

Outline

Motivation

Definitions

High-Level Proof of Seymour's Decomposition Theorem

First-degree Ingredients

Second-degree Ingredients

Conclusion

Conclusion

- Laid out the dependency graph for Seymour's decomposition theorem:

1. Gives a complete overview of the theorem's proof all the way down to definitions
2. Can guide formalization efforts

- Identified good first candidates for formalization:

1. Easy direction of Seymour's decomposition theorem
2. The splitter theorem and its corollaries