Applications of Matroid Methods to Coding Theory

Navin Kashyap

Dept. of Math & Stats
Queen's University
Kingston, ON, Canada

Acknowledgment:

This work was supported in part by a Discovery Grant from the Natural Sciences and Engineering Research Council (NSERC) of Canada.

Outline

1. Correspondence between Matroids and Linear Codes

   Application: a matroid-theoretic derivation of the MacWilliams identity

2. Code/Matroid Decomposition

   Application: linear-programming (LP) decoding

3. Treewidth of Graphs and Matroids

   Application: graphical realizations of codes

Matroids and Codes

Matroids

Definition

A matroid is an ordered pair $(E, \mathcal{I})$ consisting of

- $\diamond$ a finite ground set E; and
- $\diamond$ a collection $\mathcal{I}$ of independent sets, which are subsets of E satisfying the following three independence axioms:

(I1) $\emptyset \in \mathcal{I}$

(I2) if $I \in \mathcal{I}$, then for any $J \subseteq I$, $J \in \mathcal{I}$

(I3) if $J_1, J_2 \in \mathcal{I}$ with $|J_1| < |J_2|$, then
there exists $e \in J_2 \setminus J_1$ such that $J_1 \cup \{e\} \in \mathcal{I}$

- A subset of E that is not in $\mathcal{I}$ is called a dependent set
- A minimal dependent set is called a circuit

Vector Matroids

Let

$$A = \begin{bmatrix} | & | & & | \\ \mathbf{v}_1 & \mathbf{v}_2 & \dots & \mathbf{v}_n \\ | & | & & | \end{bmatrix}$$

be a matrix over a field $\mathbb{F}$.

Take $E = \{1, 2, \dots, n\}$, and define $\mathcal{I} \subseteq 2^E$ via

$I \in \mathcal{I}$ iff the columns $\mathbf{v}_i$, $i \in I$, are linearly independent over $\mathbb{F}$.

$(E, \mathcal{I})$ is a matroid referred to as the vector matroid of the matrix A over the field $\mathbb{F}$; denoted by $M[A]$ or $M_{\mathbb{F}}[A]$.

A matroid isomorphic to some vector matroid over the field $\mathbb{F}$ is said to be representable or $\mathbb{F}$-representable.

Graphic Matroids

Let $\mathcal{G}$ be an undirected graph with edge set E.

Define $\mathcal{I} \subseteq 2^E$ via
$I \in \mathcal{I}$ iff I does not contain a cycle of $\mathcal{G}$.

$(E, \mathcal{I})$ is a matroid referred to as the cycle matroid of the graph $\mathcal{G}$; denoted by $M(\mathcal{G})$.

- The circuits of $M(\mathcal{G})$ are precisely the circuits (simple cycles) of $\mathcal{G}$.

A matroid isomorphic to the cycle matroid of some graph is called a graphic matroid.

Linear Codes

Let $\mathbb{F}$ be a finite field. An $[n, k]$ linear code over $\mathbb{F}$ is a k-dimensional subspace of $\mathbb{F}^n$.

We will associate an index set E with a code $\mathcal{C}$, so that $\mathcal{C}$ is considered to be a subspace of $\mathbb{F}^E$; here, $|E| = n$.

A code $\mathcal{C}$ is specified by a generator matrix G, which is a matrix such that $\mathcal{C} = \mathrm{rowspace}_{\mathbb{F}}(G)$;

or equivalently, by a parity-check matrix H, which is a matrix such that $\mathcal{C} = \ker_{\mathbb{F}}(H)$.

The columns of any generator or parity-check matrix of $\mathcal{C}$ are also indexed by the elements of E.

Associating Matroids with Linear Codes

A matrix G over $\mathbb{F}$ determines two different objects:

the vector matroid $M = M_{\mathbb{F}}[G]$;

the code $\mathcal{C} = \text{rowspace}_{\mathbb{F}}(G)$.

Note that if G' is any matrix obtained from G via elementary row operations over $\mathbb{F}$, then $M_{\mathbb{F}}[G'] = M_{\mathbb{F}}[G]$;
G and G' are just different $\mathbb{F}$-representations of the same matroid.

Hence, to any linear code $\mathcal{C}$ over $\mathbb{F}$, we may uniquely assign an $\mathbb{F}$-representable matroid $M(\mathcal{C})$, by setting $M(\mathcal{C}) := M_{\mathbb{F}}[G]$ for any generator matrix G of $\mathcal{C}$.

Remark: We could also have set $M(\mathcal{C}) = M_{\mathbb{F}}[H]$ for a *parity-check matrix* H of $\mathcal{C}$;
this results in a "dual" version of our exposition.

Aside: MDS Codes

An $[n, k]$ linear code is said to be maximum distance separable (MDS) if its minimum distance equals $n - k + 1$.

Fact: If G generates an MDS code of dimension k, then
any set of k columns of G is linearly independent; and
any set of $k+1$ columns of G is linearly dependent.

If $\mathcal{C}$ is an $[n, k]$ MDS code, then for the matroid $M(\mathcal{C})$, the collection $\mathcal{I}$ of independent sets is

$$\mathcal{I} = \{I \subseteq [n] : |I| \leq k\}.$$

Such a matroid is called a uniform matroid, denoted by $U_{k,n}$.

Bases and Rank: Definitions

$M = (E, \mathcal{I})$ a matroid.

Definition: A basis of M is any maximal (wrt inclusion) independent set of M.

By Axiom (I3), all bases of M have the same cardinality.

Definition: The cardinality of any basis of M is called the rank of M, denoted by $\mathrm{rank}(M)$ or $r(M)$.

More generally, the rank function of M is the function $r: 2^E \to \mathbb{Z}$ defined as follows: for $X \subseteq E$,

$$r(X) = \max\{|I| : I \in \mathcal{I}, I \subseteq X\}.$$

In particular, $\mathrm{rank}(M) = r(E)$.

Rank and Dimension: Codes

$\mathcal{C}$ a linear code over $\mathbb{F}$ with index set E;
G a generator matrix for $\mathcal{C}$;
$M = M(\mathcal{C}) = M[G]$ the associated matroid.

- Rank function of M: for $X \subseteq E$,

$$r(X) = \mathrm{rank}_{\mathbb{F}}(G|_X) = \dim_{\mathbb{F}}(\mathcal{C}|_X).$$

In particular, $\mathrm{rank}(M) = \mathrm{rank}_{\mathbb{F}}(G) = \dim_{\mathbb{F}}(\mathcal{C})$.

The Dual Matroid

$M = (E, \mathcal{I})$ a matroid, with $\mathcal{B}$ its collection of bases.
For $X \subseteq E$, let $X^c = E - X$.

Define $\mathcal{I}^* = \{I^* : I^* \subseteq B^c \text{ for some } B \in \mathcal{B}\}$.

$(E, \mathcal{I}^*)$ forms a matroid, called the dual matroid of M;
denoted by M^*.

It is clear that M^* has as its collection of bases
$\mathcal{B}^* = \{B^c : \ B \in \mathcal{B}\}$.

Thus, M^* is a matroid on the same ground set as M, but whose bases are the complements of the bases of M.

Duality: Codes

$\mathcal{C}$ a linear code over $\mathbb{F}$ with index set E;
G a generator matrix for $\mathcal{C}$;
$M = M(\mathcal{C}) = M[G]$ the associated matroid.

The dual code of $\mathcal{C}$ is defined as

$$\mathcal{C}^\perp = \{\mathbf{x} \in \mathbb{F}^E : \langle \mathbf{c}, \mathbf{x} \rangle_{\mathbb{F}} = 0 \text{ for all } \mathbf{c} \in \mathcal{C}\}.$$

- $M^* = M[H]$ for any parity-check matrix, H, of $\mathcal{C}$.
  Therefore,
  $$M^*(\mathcal{C}) \stackrel{\text{def}}{=} (M(\mathcal{C}))^* = M(\mathcal{C}^\perp).$$

  In particular, the dual of an $\mathbb{F}$-representable matroid is also $\mathbb{F}$-representable.

Deletion and Contraction

Two fundamental operations on a matroid $M = (E, \mathcal{I})$, given an $X \subseteq E$.

Deletion. The matroid $M \setminus X$ is the matroid on ground set $E - X$, whose independent sets are precisely those $I \in \mathcal{I}$ that are contained in $E - X$, *i.e.*,

$$\mathcal{I}(M \setminus X) = \{I \in \mathcal{I} : \; I \subseteq E - X\}.$$

Contraction. This is the dual operation to deletion:

$$M/X = (M^* \setminus X)^*.$$

Matroid Minors

Definition

A minor of a matroid M is any matroid obtained from M via a (possibly empty) sequence of deletion and contraction operations.

Minors are central to matroid theory — e.g., they often turn up in excluded-minor characterizations:

- A matroid is binary (*i.e.*, $GF(2)$-representable) iff it contains no minor isomorphic to the uniform matroid $U_{2,4}$.
- A matroid is regular (*i.e.*, representable over any field) iff it contains no minor isomorphic to any of $U_{2,4}$, $M(\mathcal{H}_7)$ and $M^*(\mathcal{H}_7)$. [Here, $\mathcal{H}_7$ is the (binary) [7,4] Hamming code.]
- A matroid is graphic iff it contains no minor isomorphic to any of $U_{2,4}$, $M(\mathcal{H}_7)$, $M^*(\mathcal{H}_7)$, $M^*(K_5)$ and $M^*(K_{3,3})$.

Puncturing and Shortening

$\mathcal{C}$ a linear code on index set E, and $X \subseteq E$.

> Puncturing. Columns indexed by X deleted from a generator matrix for $\mathcal{C}$;
>
> thus, $\mathcal{C} \setminus X$ is the projection of $\mathcal{C}$ onto the coordinates in $E - X$.
>
> Shortening. Columns indexed by X deleted from a parity-check matrix for $\mathcal{C}$;
>
> equivalently, $\mathcal{C}/X$ is obtained by taking the subcode of $\mathcal{C}$ that has 0's in all the coordinates in X, and then deleting those coordinates from the subcode.

Then,

$$M(\mathcal{C} \setminus X) = M(\mathcal{C}) \setminus X \quad \text{and} \quad M(\mathcal{C}/X) = M(\mathcal{C})/X.$$

Code Minors

Definition

A minor of a code $\mathcal{C}$ is any code obtained from $\mathcal{C}$ via a (possibly empty) sequence of shortening and puncturing operations.

Application:
The MacWilliams Identity

The Tutte Polynomial

M a matroid on the ground set E, with rank function r.

Definition: The Tutte polynomial of M is defined as

$$T_M(x, y) = \sum_{A \subseteq E} (x-1)^{r(E)-r(A)} (y-1)^{|A|-r(A)}$$

Fact: $T_{M^*}(x, y) = T_M(y, x)$.

Remark:

The chromatic polynomial of a graph $\mathcal{G}$ can be obtained as a special case of the Tutte polynomial of $M(\mathcal{G})$.

The MacWilliams Identity

$\mathcal{C}$ an $[n, k]$ linear code over $\mathbb{F} = GF(q)$.

Definition: The homogeneous weight enumerator polynomial of $\mathcal{C}$:

$$W_{\mathcal{C}}(x, y) = \sum_{i=0}^{n} A_i x^{n-i} y^i,$$

where A_i is the number of codewords of weight i.

Theorem [Greene (1976)]

Let $M = M(\mathcal{C})$. Then,

$$W_{\mathcal{C}}(x, y) = y^{n-k}(x-y)^k \; T_M\left(\frac{x+(q-1)y}{x-y}, \frac{x}{y}\right)$$

Corollary (The MacWilliams Identity)

$$W_{\mathcal{C}^\perp}(x, y) = q^{-k} \, W_{\mathcal{C}}(x+(q-1)y, \, x-y)$$

Code Composition/Decomposition

The $\mathcal{S}_m(\mathcal{C}, \mathcal{C}')$ Construction

Let $\mathcal{C}, \mathcal{C}'$ be linear codes of length n, n', resp., over some field $\mathbb{F}$; and let m be an integer s.t. $0 \le m < \min\{n, n'\}$.

Let $G = [\mathbf{g}_1 \ \mathbf{g}_2 \ \ldots \ \mathbf{g}_n]$ and $G' = [\mathbf{g}'_1 \ \mathbf{g}'_2 \ \ldots \ \mathbf{g}'_{n'}]$
be generator matrices of $\mathcal{C}$ and $\mathcal{C}'$, respectively,

Consider the code $\widehat{\mathcal{C}}$ with generator matrix

$$\left[\begin{array}{cccccccc} \mathbf{g}_1 & \ldots & \mathbf{g}_{n-m} & \mathbf{g}_{n-m+1} & \ldots & \mathbf{g}_n & \mathbf{0} & \ldots & \mathbf{0} \\ \mathbf{0} & \ldots & \mathbf{0} & \mathbf{g}'_1 & \ldots & \mathbf{g}'_m & \mathbf{g}'_{m+1} & \ldots & \mathbf{g}'_{n'} \end{array} \right].$$

Definition

$\mathcal{S}_m(\mathcal{C}, \mathcal{C}')$ is the code of length $n + n' - 2m$ obtained by *shortening* $\widehat{\mathcal{C}}$ at the m "overlapping positions".

Some Properties of $\mathcal{S}_m(\mathcal{C}, \mathcal{C}')$

Let $\mathcal{C}_p$ and $\mathcal{C}_s$ denote the codes obtained, respectively, by puncturing and shortening $\mathcal{C}$ at its last m coordinates.

Let $\mathcal{C}'_p$ and $\mathcal{C}'_s$ denote the codes obtained, respectively, by puncturing and shortening $\mathcal{C}'$ at its first m coordinates.

Proposition

(a) $\dim(\mathcal{S}_m(\mathcal{C}, \mathcal{C}')) =$
$\dim(\mathcal{C}) + \dim(\mathcal{C}') - \dim(\mathcal{C}_s \cap \mathcal{C}'_s) - \dim(\mathcal{C}_p + \mathcal{C}'_p)$.

(b) If $\mathcal{C}, \mathcal{C}'$ are codes over a field of characteristic 2, then

$$\big(\mathcal{S}_m(\mathcal{C}, \mathcal{C}')\big)^{\perp} = \mathcal{S}_m(\mathcal{C}^{\perp}, \mathcal{C}'^{\perp}).$$

Important Special Cases

$\mathcal{C}, \mathcal{C}'$ linear codes over $\mathbb{F} = GF(q)$;

$m = (q^{r-1} - 1)/(q-1), \quad n, n' > 2m.$

r-sum, $r \geq 1$. $\mathcal{C} \oplus_r \mathcal{C}' = \mathcal{S}_m(\mathcal{C}, \mathcal{C}')$, when

- $\mathcal{C}_s = \mathcal{C}'_s = \{\mathbf{0}\}$
  $\mathcal{C}_p = \mathcal{C}'_p = [m, r-1]$ simplex (*i.e.*, Hamming dual) code

$\overline{r}$-sum, $r \geq 1$. $\mathcal{C} \,\overline{\oplus}_r\, \mathcal{C}' = \mathcal{S}_m(\mathcal{C}, \mathcal{C}')$, when

- $\mathcal{C}_s = \mathcal{C}'_s = [m, m-(r-1)]$ Hamming code
  $\mathcal{C}_p = \mathcal{C}'_p = \{0,1\}^m$

When $r = 1$, the above definitions degenerate to the direct sum:

$$\mathcal{C} \oplus_1 \mathcal{C}' = \mathcal{C} \,\overline{\oplus}_1\, \mathcal{C}' = \mathcal{S}_0(\mathcal{C}, \mathcal{C}') = \mathcal{C} \oplus \mathcal{C}'.$$

Basic Properties of r- and $\bar{r}$-sums

For the special cases of r- and $\bar{r}$-sums, the previous proposition specializes to

<u>Corollary</u>

(a) $\dim(\mathcal{C} \oplus_r \mathcal{C}') = \dim(\mathcal{C}) + \dim(\mathcal{C}') - (r-1)$.

(b) $\dim(\mathcal{C} \mathbin{\overline{\oplus}_r} \mathcal{C}') = \dim(\mathcal{C}) + \dim(\mathcal{C}') - (2^r - r - 1)$.

(c) $(\mathcal{C} \oplus_r \mathcal{C}')^\perp = \mathcal{C}^\perp \mathbin{\overline{\oplus}_r} \mathcal{C}'^\perp$.

<u>Remark</u>: For $r = 2$, the definitions of r- and $\bar{r}$-sum coincide, so that (c) above is in fact

$$(\mathcal{C} \oplus_2 \mathcal{C}')^\perp = \mathcal{C}^\perp \oplus_2 \mathcal{C}'^\perp.$$

Application:
Linear-Programming (LP) Decoding

LP Formulation of ML Decoding

Setup:

Binary linear code $\mathcal{C}$ of length n

Discrete memoryless channel: $\Pr[\mathbf{y}|\mathbf{x}] = \prod_{i=1}^{n} \Pr[y_i|x_i]$

Received word: $\mathbf{y} = (y_1, y_2, \ldots, y_n)$

Maximum-Likelihood (ML) Decoding:

determine $\arg\max_{\mathbf{x}\in\mathcal{C}} \Pr[\mathbf{y}|\mathbf{x}]$

Equiv. LP formulation [Feldman, Wainwright, Karger (2005)]:

determine $\arg\min_{\mathbf{x}\in P(\mathcal{C})} \langle \gamma, \mathbf{x} \rangle$, where

$\gamma = (\gamma_1, \ldots, \gamma_n)$ with

$$\gamma_i = \log\left(\frac{\Pr[y_i|x_i = 0]}{\Pr[y_i|x_i = 1]}\right)$$

and $P(\mathcal{C}) \stackrel{\text{def}}{=} \mathsf{conv}(\mathcal{C})$ is the codeword polytope

Relaxing the LP Formulation

ML decoding is known to be NP-hard.

Relax the LP formulation by defining a "looser" set of constraints.

In other words, find "simpler" polytopes $\widehat{P}(\mathcal{C}) \subseteq [0,1]^n$ with $P(\mathcal{C}) \subseteq \widehat{P}(\mathcal{C})$, and solve the LP over $\widehat{P}(\mathcal{C})$ instead:

$$\arg\min_{\mathbf{x} \in \widehat{P}(\mathcal{C})} \langle \gamma, \mathbf{x} \rangle$$

The vertex set of such a polytope $\widehat{P}(\mathcal{C})$ contains $\mathcal{C}$, but also contains extra "pseudocodeword" vertices.

Canonical Relaxations

For $H \subseteq \mathcal{C}^\perp$, define

$$Q(H) = \bigcap_{\mathbf{h} \in H} P(\mathbf{h}^\perp)$$

where $\mathbf{h}^\perp = \{\mathbf{x} \in \{0,1\}^n : \langle \mathbf{h}, \mathbf{x} \rangle \equiv 0 \pmod 2\}$.

LP Decoding: determine $\arg\min_{\mathbf{x} \in Q(H)} \langle \gamma, \mathbf{x} \rangle$

Canonical Relaxations

For $H \subseteq \mathcal{C}^\perp$, define

$$Q(H) = \bigcap_{\mathbf{h} \in H} P(\mathbf{h}^\perp)$$

where $\mathbf{h}^\perp = \{\mathbf{x} \in \{0,1\}^n : \ \langle \mathbf{h}, \mathbf{x} \rangle \equiv 0 \pmod 2\}$.

LP Decoding: determine $\arg\min_{\mathbf{x} \in Q(H)} \langle \gamma, \mathbf{x} \rangle$

<u>Question</u>: For which codes $\mathcal{C}$ do there exist $H \subseteq \mathcal{C}^\perp$ such that $Q(H)$ has no pseudocodewords?

<u>Answer</u>: Geometrically perfect codes, *i.e.*, codes $\mathcal{C}$ such that $P(\mathcal{C}) = Q(\mathcal{C}^\perp)$ (codeword polytope = full canonical relaxation).

Interlude — Cycle Codes of Graphs

Given a graph $\mathcal{G} = (V, E)$, the cycle code of $\mathcal{G}$ is the *binary* linear code whose *parity-check matrix* is the $|V| \times |E|$ vertex-edge incidence matrix of $\mathcal{G}$.

We will denote the cycle code of $\mathcal{G}$ by $\mathcal{C}[\mathcal{G}]$.

Note: $M(\mathcal{C}[\mathcal{G}]) = M^*(\mathcal{G})$.

A Characterization of Geom. Perfect Codes

An excluded-minor characterization ...

Theorem

[Barahona and Grötschel (1986), based on Seymour (1982)]

A binary linear code $\mathcal{C}$ is geometrically perfect iff
$\mathcal{C}$ does not contain as a minor
any code equivalent to one of the following:

- the [7,3] Hamming dual, $\mathcal{H}_7^\perp$;
- a certain [10,5] isodual code, R_{10}; and
- the dual of the cycle code of K_5, *i.e.*, $\mathcal{C}[K_5]^\perp$.

An Alternative Characterization

A characterization via code decompositions . . .

Theorem

[Grötschel and Truemper (1989), based on Seymour (1982)]

A binary linear code $\mathcal{C}$ is geometrically perfect iff
$\mathcal{C}$ can be constructed by means of coordinate permutations, direct-sums, 2-sums and 3-sums starting with codes, each of which is a minor of $\mathcal{C}$, and each of which is one of the following:

- the cycle code of some graph;
- the $[7, 4]$ Hamming code;
- $\mathcal{C}(K_{3,3})^{\perp}$;
- $\mathcal{C}(V_8)^{\perp}$.

Corollaries of the Decomposition Theorem

Let $\mathfrak{G}$ be the family of geometrically perfect codes.

- There is a polynomial-time algorithm for deciding membership in $\mathfrak{G}$.

Corollaries of the Decomposition Theorem

Let $\mathfrak{G}$ be the family of geometrically perfect codes.

- There is a polynomial-time algorithm for deciding membership in $\mathfrak{G}$.
- There is a polynomial-time algorithm that, given a $\mathcal{C} \in \mathfrak{G}$, and a vector $\gamma \in \mathbb{R}^n$, determines

$$\arg \min_{\mathbf{x} \in P(\mathcal{C})} \langle \gamma, \mathbf{x} \rangle.$$

- Therefore, there is a polynomial-time maximum-likelihood decoding algorithm for codes in $\mathfrak{G}$.

Corollaries of the Decomposition Theorem

Let $\mathfrak{G}$ be the family of geometrically perfect codes.

- There is a polynomial-time algorithm for deciding membership in $\mathfrak{G}$.
- There is a polynomial-time algorithm that, given a $\mathcal{C} \in \mathfrak{G}$, and a vector $\gamma \in \mathbb{R}^n$, determines

$$\arg \min_{\mathbf{x} \in P(\mathcal{C})} \langle \gamma, \mathbf{x} \rangle .$$

- Therefore, there is a polynomial-time maximum-likelihood decoding algorithm for codes in $\mathfrak{G}$.
- $\mathfrak{G}$ is not asymptotically good: codes from $\mathfrak{G}$ cannot have both min. dist. and dimension growing linearly with codelength.
- Therefore, pseudocodewords cannot be avoided when LP decoding is applied to good codes.

Tree Decompositions of Graphs and Matroids

Tree Decompositions of Graphs

Let $\mathcal{G}$ be a graph with vertex set $V(\mathcal{G})$.

A tree decomposition of $\mathcal{G}$ consists of a tree T, and an ordered collection $\mathcal{V} = (V_x,\ x \in V(T))$ of subsets of $V(\mathcal{G})$, satisfying

- $\bigcup_{x \in V(T)} V_x = V$;
- for each $v \in V(\mathcal{G})$, the subgraph of T induced by $\{x \in V(T) : v \in V_x\}$ is connected; and
- for each pair of adjacent vertices $u, v \in V(\mathcal{G})$, we have $\{u, v\} \subseteq V_x$ for some $x \in V(T)$.

We then define $\mathrm{width}(T, \mathcal{V}) \overset{\mathrm{def}}{=} \max_{x \in V(T)} |V_x| - 1$.

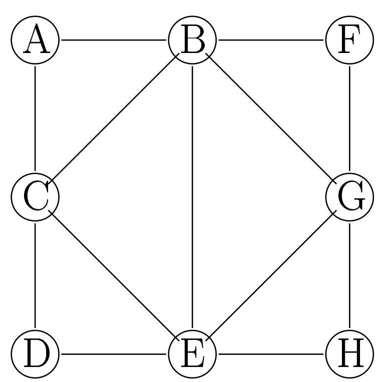
Treewidth of Graphs

Definition [Robertson & Seymour (1983)]

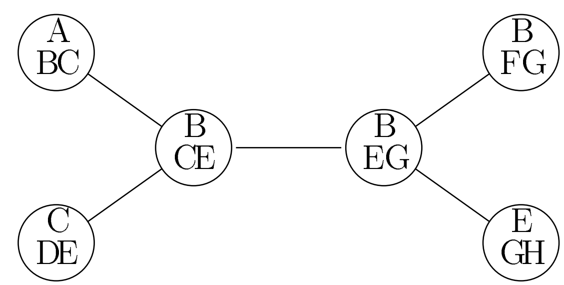
The treewidth of $\mathcal{G}$ is defined to be the least width of any tree decomposition of $\mathcal{G}$; denoted by $\kappa_{\text{tree}}(\mathcal{G})$.

Some Examples

- For any tree T, $\kappa_{\text{tree}}(T) = 1$.
- If $\mathcal{G}$ is a cycle on at least three vertices, then $\kappa_{\text{tree}}(\mathcal{G}) = 2$.
- The graph $\mathcal{G}$ shown below also has treewidth 2.



$\mathcal{G}$



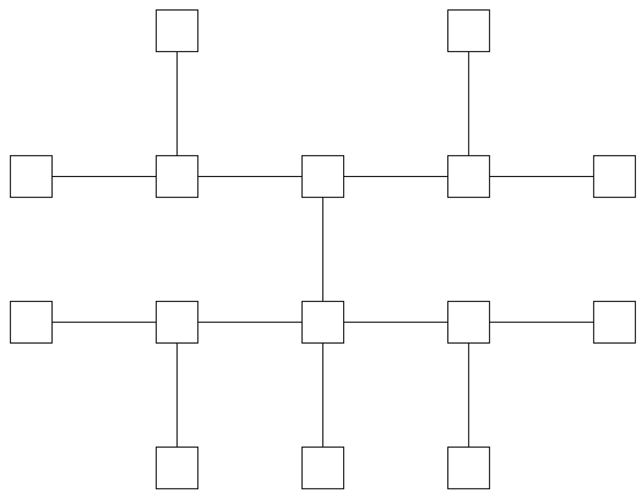
An optimal tree decomposition of $\mathcal{G}$

Tree Decompositions of Matroids

M a matroid on ground set E, with rank function r.

A tree decomposition of M is a pair (T, ω), where

- T is a tree, and

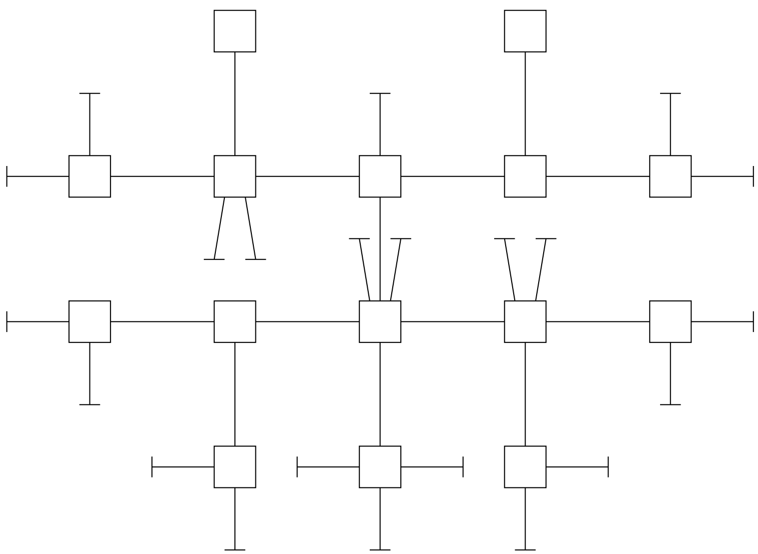


Tree Decompositions

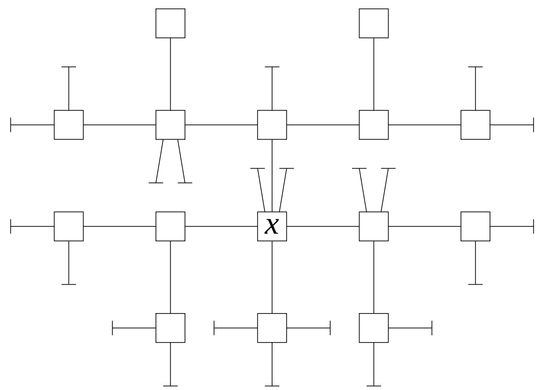
M a matroid on ground set E, with rank function r.

A tree decomposition of M is a pair (T, ω), where

- T is a tree, and
- $\omega : E \to V(T)$ is a mapping.

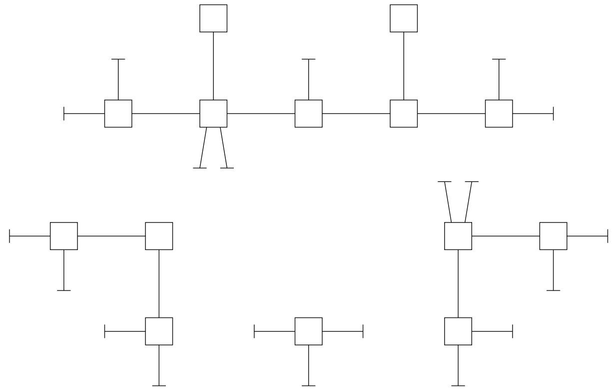


Node-width in a tree decomposition



Given a tree decomposition (T, ω) of M, and a node $x \in V(T)$

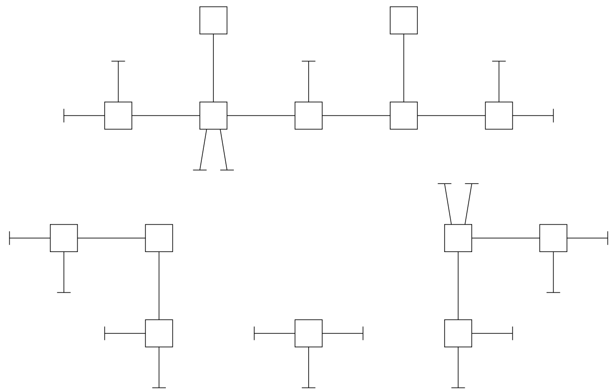
Node-width in a tree decomposition



Given a tree decomposition (T, ω) of M, and a node $x \in V(T)$:

- the removal of x from T yields a disconnected graph whose components, $T_1, \ldots, T_\delta$, are subtrees of T

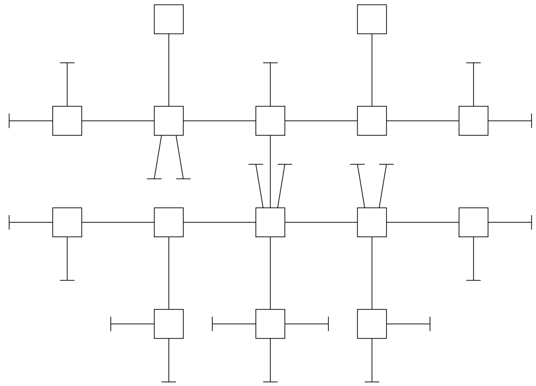
Node-width in a tree decomposition



Given a tree decomposition (T, ω) of M, and a node $x \in V(T)$:

- the removal of x from T yields a disconnected graph whose components, $T_1, \ldots, T_\delta$, are subtrees of T
- for $j = 1, \ldots, \delta$, set $F_i = \omega^{-1}(V(T_i))$
- node-width$(x) = \sum_{i=1}^{\delta} r(E - F_i) - (\delta - 1)\,\mathrm{rank}(M)$

Matroid Treewidth



$$\text{width}(T, \omega) = \max_{x \in V(T)} \text{node-width}(x)$$

Definition [Hliněný and Whittle (2006); attributed to Jim Geelen]:

The treewidth of M is defined to be

$$\kappa_{\text{tree}}(M) = \min_{(T,\omega)} \text{width}(T, \omega).$$

Relating Graph and Matroid Treewidth

Theorem [Hliněný and Whittle (2006)] For any graph $\mathcal{G}$,

$$\kappa_{\text{tree}}(M(\mathcal{G})) = \kappa_{\text{tree}}(\mathcal{G}).$$

It is known that the problem of computing the treewidth of a graph is NP-hard, and therefore, so is the corresponding problem for matroids.

Application:
Graphical Models of Codes

Graphical Models of Codes

Graphical models of codes and the associated message-passing decoding algorithms are a major focus area of modern coding theory.

Graphical models come in many flavours:

- Trellises (the Viterbi decoding algorithm)
- Tanner graphs
- Factor graphs
- Normal graphical models/realizations [Forney (2001)]

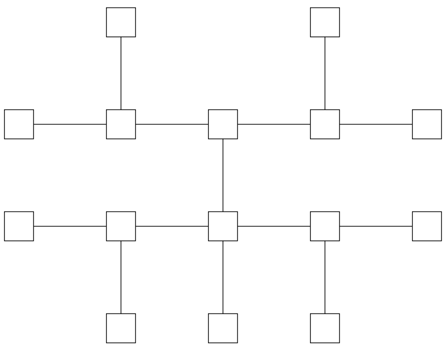
The decoding algorithms commonly associated with these models are variants of the abstract Generalized Distributive Law, as expounded by Aji & McEliece (2000).

Graph Decompositions

Let $\mathcal{C}$ be a linear code defined on an index set I.

A graph decomposition of (the index set of) $\mathcal{C}$ is a pair $(\mathcal{G}, \omega)$, where

- $\mathcal{G}$ is a connected graph, and

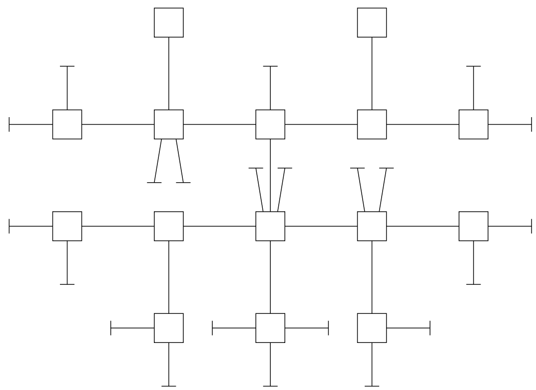


Graph Decompositions

Let $\mathcal{C}$ be a linear code defined on an index set I.

A graph decomposition of (the index set of) $\mathcal{C}$ is a pair $(\mathcal{G}, \omega)$, where

- $\mathcal{G}$ is a connected graph, and
- $\omega : I \to V(\mathcal{G})$ is a mapping.

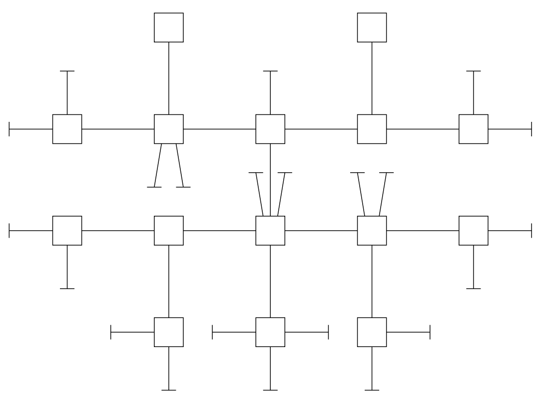


Graph Decompositions

Let $\mathcal{C}$ be a linear code defined on an index set I.

A graph decomposition of (the index set of) $\mathcal{C}$ is a pair $(\mathcal{G}, \omega)$, where

- $\mathcal{G}$ is a connected graph, and
- $\omega : I \rightarrow V(\mathcal{G})$ is a mapping.



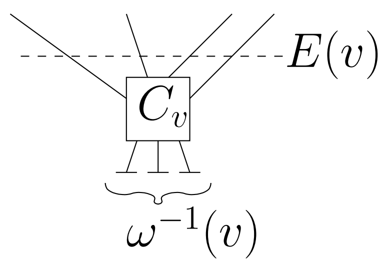
When $\mathcal{G}$ is a tree, $(\mathcal{G}, \omega)$ is called a tree decomposition.

Normal Graphical Models

For a graph $\mathcal{G} = (V, E)$, given $v \in V$, let $E(v)$ denote the set of edges of $\mathcal{G}$ incident with v.

A graph decomposition $(\mathcal{G}, \omega)$ of a code $\mathcal{C}$ can be extended to a normal graphical model $(\mathcal{G}, \omega, (\mathcal{S}_e,\ e \in E), (C_v,\ v \in V))$, where

- for each $e \in E$, $\mathcal{S}_e$ is a vector space over $\mathbb{F}$, called a state space;
- for each $v \in V$, C_v is a subspace of $\mathbb{F}^{\omega^{-1}(v)} \oplus \left(\bigoplus_{e \in E(v)} \mathcal{S}_e\right)$, called a local constraint (code).



(Normal) Graphical Realizations

A valid global configuration of a normal graphical model Γ is a vector of the form $\mathbf{b} = ((x_i,\ i \in I), (\mathbf{s}_e,\ e \in E))$, where

- for each $i \in I$, x_i is a symbol from $\mathbb{F}$;
- for each $e \in E$, $\mathbf{s}_e$ is a state from $\mathcal{S}_e$;
- for each $v \in V$, $((x_i,\ i \in \omega^{-1}(v)), (\mathbf{s}_e,\ e \in E(v))) \in C_v$.

The set of all valid global configurations forms a vector space over $\mathbb{F}$, called the full behaviour of the model; we denote this by $\mathfrak{B}$.

(Normal) Graphical Realizations

A valid global configuration of a normal graphical model Γ is a vector of the form $\mathbf{b} = ((x_i,\ i \in I), (\mathbf{s}_e,\ e \in E))$, where

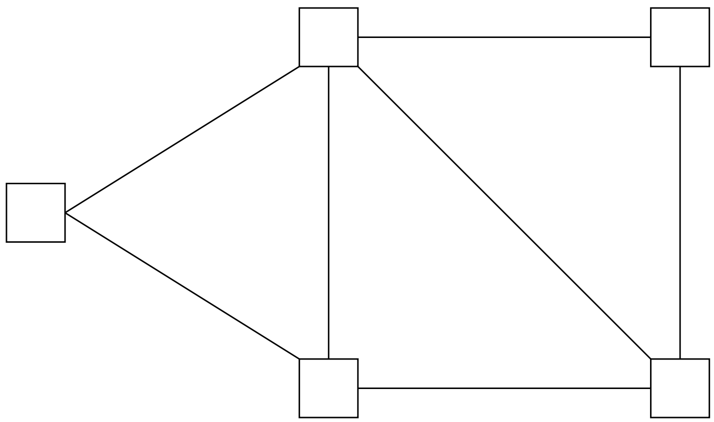
- for each $i \in I$, x_i is a symbol from $\mathbb{F}$;
- for each $e \in E$, $\mathbf{s}_e$ is a state from $\mathcal{S}_e$;
- for each $v \in V$, $((x_i,\ i \in \omega^{-1}(v)), (\mathbf{s}_e,\ e \in E(v))) \in C_v$.

The set of all valid global configurations forms a vector space over $\mathbb{F}$, called the full behaviour of the model; we denote this by $\mathfrak{B}$.

If $\mathfrak{B}|_I = \mathcal{C}$, then Γ is called a (normal) graphical realization of $\mathcal{C}$.

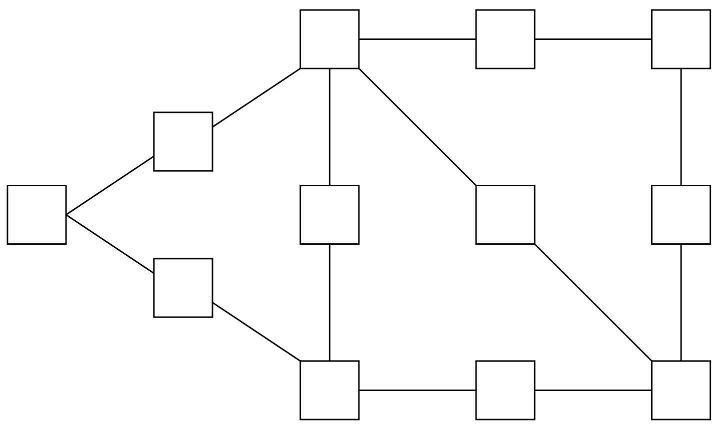
An Example

Consider an arbitrary graph $\mathcal{G}_0$:



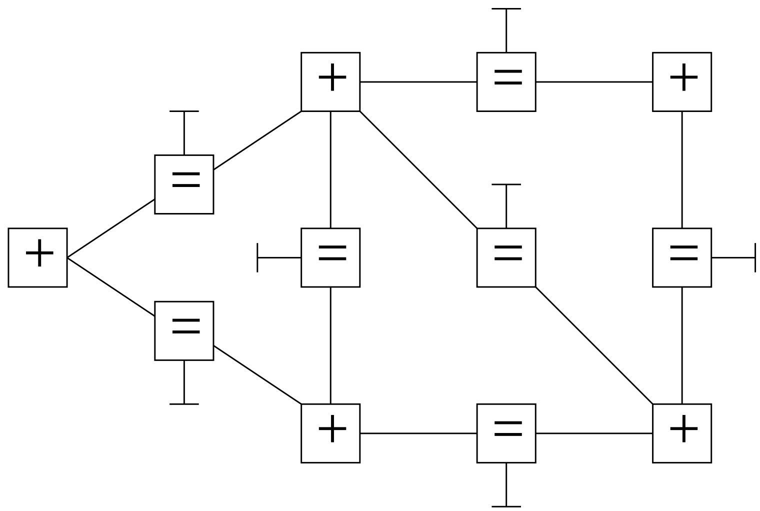
An Example

Subdivide the edges of $\mathcal{G}_0$ to form $\mathcal{G}$:



An Example

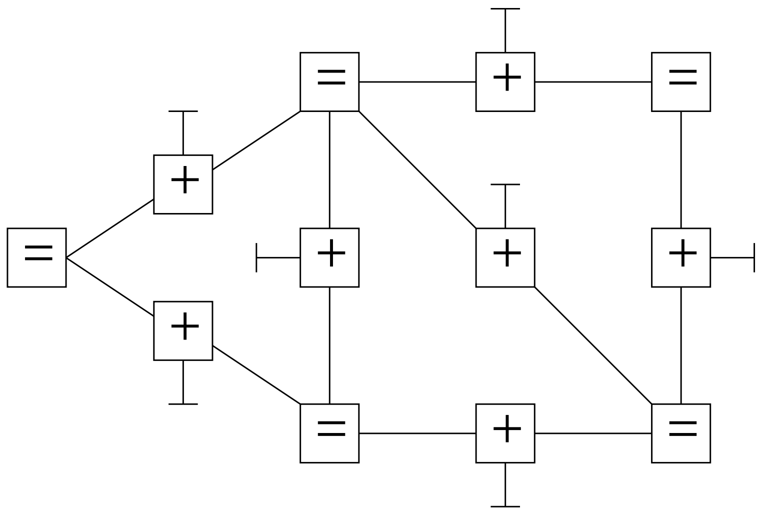
Construct a graphical model (over $\mathbb{F}_2$) on $\mathcal{G}$ as depicted below:



This is a graphical realization of the cycle code $\mathcal{C}[\mathcal{G}_0]$.

The Dual Example

Replace all $+$'s by $=$'s, and vice versa:



This is a graphical realization of the dual of $\mathcal{C}[\mathcal{G}_0]$. [Forney (2001)]

Constraint Complexity of a Realization

Any graphical realization of code has a natural associated decoding algorithm, namely, the sum-product algorithm [Forney (2001)].

The computational complexity of the sum-product algorithm is determined in large part by the dimensions of the local constraint codes in the realization.

Definition: Let $\Gamma = (\mathcal{G}, \omega, (C_v, v \in V), (\mathcal{S}_e, e \in E))$ be a graphical realization of a code $\mathcal{C}$. The constraint complexity of Γ is defined to be

$$\kappa(\Gamma) = \max_{v \in V} \dim(\mathcal{C}_v).$$

How Low Can You Go?

Given: a code $\mathcal{C}$ and a connected graph $\mathcal{G}$

Fact: Any graph decomposition $(\mathcal{G}, \omega)$ of (the index set of) $\mathcal{C}$ can be extended to a graphical realization of $\mathcal{C}$.

Question: How small can the constraint complexity of a realization of $\mathcal{C}$ on $\mathcal{G}$ be?

How Low Can You Go?

Given: a code $\mathcal{C}$ and a connected graph $\mathcal{G}$

Fact: Any graph decomposition $(\mathcal{G}, \omega)$ of (the index set of) $\mathcal{C}$ can be extended to a graphical realization of $\mathcal{C}$.

Question: How small can the constraint complexity of a realization of $\mathcal{C}$ on $\mathcal{G}$ be?

Let $\mathfrak{R}(\mathcal{C}; \mathcal{G}, \omega)$ denote the set of all realizations of $\mathcal{C}$ that extend a given graph decomposition $(\mathcal{G}, \omega)$.

$$\begin{aligned} \kappa(\mathcal{C}; \mathcal{G}, \omega) &= \min_{\Gamma \in \mathfrak{R}(\mathcal{C}; \mathcal{G}, \omega)} \kappa(\Gamma) \\ \kappa(\mathcal{C}; \mathcal{G}) &= \min_{\omega} \kappa(\mathcal{C}; \mathcal{G}, \omega) \end{aligned}$$

Tree Realizations

A tree realization of a code $\mathcal{C}$ is a graphical realization of $\mathcal{C}$ in which the underlying graph is a tree.

Since the realization is cycle-free, the associated sum-product algorithm gives an exact implementation of maximum-likelihood (ML) decoding [Forney (2001)], [Aji & McEliece (2001)].

Minimal Tree Realizations

For a given tree decomposition (T, ω) of a code $\mathcal{C}$, Forney (2001) gave a canonical method of constructing a tree realization in $\mathfrak{R}(\mathcal{C}; T, \omega)$.

Forney's construction can be shown to minimize, among all realizations in $\mathfrak{R}(\mathcal{C}; T, \omega)$, the dimension of the local constraint at each vertex of T [K. (2007)].

Let $\mathcal{M}(\mathcal{C}; T, \omega)$ denote this minimal tree realization; thus

$$\kappa(\mathcal{C}; T, \omega) = \kappa(\mathcal{M}(\mathcal{C}; T, \omega))$$

Minimal Tree Realizations

For a given tree decomposition (T, ω) of a code $\mathcal{C}$, Forney (2001) gave a canonical method of constructing a tree realization in $\mathfrak{R}(\mathcal{C}; T, \omega)$.

Forney's construction can be shown to minimize, among all realizations in $\mathfrak{R}(\mathcal{C}; T, \omega)$, the dimension of the local constraint at each vertex of T [K. (2007)].

Let $\mathcal{M}(\mathcal{C}; T, \omega)$ denote this minimal tree realization; thus

$$\kappa(\mathcal{C}; T, \omega) = \kappa(\mathcal{M}(\mathcal{C}; T, \omega))$$

Forney (2003) gave an explicit expression for the dimensions of the local constraints in $\mathcal{M}(\mathcal{C}; T, \omega)$.

Treewidth of Codes

Definition

Treewidth: $\kappa_{\text{tree}}(\mathcal{C}) = \min_{(T,\omega)} \kappa(\mathcal{C}; T, \omega)$
(minimum over all tree decompositions of $\mathcal{C}$)

Fact:

Forney's expression for the dimensions of the local constraints in a minimal tree realization shows that

$$\kappa_{\text{tree}}(\mathcal{C}) = \kappa_{\text{tree}}(M(\mathcal{C}))$$

Thus, $\kappa_{\text{tree}}(M(\mathcal{C}))$ may be viewed as a measure of the ML-decoding complexity of $\mathcal{C}$.

Realizations on Graphs with Cycles

There is little known about the problem of finding low-complexity realizations of a code $\mathcal{C}$ on a given connected graph $\mathcal{G}$, when $\mathcal{G}$ is not a tree.

When $\mathcal{G}$ is a simple cycle, the problem is one of finding optimal tailbiting trellis realizations of codes, which has been studied by Koetter and Vardy (2003).

Halford and Chugg (2008) gave a lower bound on $\kappa(\mathcal{C};\mathcal{G})$ in terms of "forest-inducing edge cuts" of $\mathcal{G}$.

Their lower bound is subsumed by (a slight modification of) the following bound [K. (2009)]:

$$\kappa(\mathcal{C};\mathcal{G}) \geq \frac{\kappa_{\text{tree}}(\mathcal{C})}{\kappa_{\text{tree}}(\mathcal{G})+1}$$

Other Complexity Measures

One can define the pathwidth of graphs, matroids, and codes, by considering only those tree decompositions in which the underlying tree is a simple path.

These notions are related to each other much like treewidth.

The pathwidth of a linear code is essentially the same as its minimal trellis complexity.

Some Interesting Results

The connections between pathwidth and treewidth of graphs, matroids, and codes can be exploited to show that

- computing the minimal trellis complexity (among all coordinate permutations) of a code is NP-hard [K. (2008)]
- the ratio between the pathwidth and the treewidth of a code grows at most logarithmically with codelength, and a logarithmic rate of growth is in fact achievable [K. (2009)]
- "Good" families of codes cannot have realizations of bounded complexity on graphs of bounded treewidth [K. (2009)]

Useful References

[1] James Oxley, *Matroid Theory*, Oxford University Press, 2006.

[2] Klaus Truemper, *Matroid Decompositions*, Academic Press, San Diego, 1992.

[3] Peter Cameron, "Polynomial aspects of codes, matroids and permutation groups," lecture notes, March 2002.

[4] Petr Hliněný, Sang-il Oum, Detlef Seese and Georg Gottlob, "Width parameters beyond tree-width and their applications," *The Computer Journal*, (advance access) Sept. 2007. DOI 10.1093/comjnl/bxm052.

[5] Hans Bodlaender, "A tourist guide through treewidth," *Acta Cybernetica*, vol. 11, pp. 1–23, 1993.

[6] G. David Forney Jr., "Codes on graphs: normal realizations," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 520–548, Feb. 2001.

[7] ———, "Codes on graphs: constraint complexity of cycle-free realizations of linear codes," *IEEE Trans. Inf. Theory*, vol. 49, no. 7, pp. 1597–1610, 2003.

[8] Navin Kashyap, "A decomposition theory for binary linear codes," *IEEE Trans. Inf. Theory*, vol. 54, no. 7, pp. 3035–3058, July 2008.

[9] ———, "On minimal tree realizations of linear codes," *IEEE Trans. Inf. Theory*, vol. 55, no. 8, pp. 3501–3519, Aug. 2009.

[10] ———, "Constraint complexity of realizations of linear codes on arbitrary graphs," to appear in *IEEE Trans. Inf. Theory*. ArXiv:0805.2199v1 [cs.DM]