Linear Matroid Intersection is in quasi-NC

Rohit Gurjar   Thomas Thierauf

Prerona Chatterjee, TIFR

July 04, 2017

Matroids

Definition

$M = (E, \mathcal{I})$ is said to be a *matroid* if

E : finite set

$\mathcal{I}$: set of Independent sets satisfying:

1. Closure under subsets
2. Augmentation Property

Matroids

Definition

$M = (E, \mathcal{I})$ is said to be a *matroid* if

E : finite set

$\mathcal{I}$: set of Independent sets satisfying:

1. Closure under subsets
2. Augmentation Property

Some Notations:

1. $m = |E|$
2. $\mathcal{B} \subseteq \mathcal{I}$: collection of maximal sets in $\mathcal{I}$.
3. $\text{rank}(A) = \max\{|I| : I \in \mathcal{I} \text{ and } I \subseteq A\}$ for every $A \subseteq E$.

Linear Matroids and the Matroid Intersection Problem

Linear Matroids

For matrix $V = [v_1, v_2, \ldots, v_m]$, define $M_V = (E, \mathcal{I})$ as:

1. $E : \{1, 2, \ldots, m\}$.
2. $I \in \mathcal{I}$ iff $\{v_i : i \in I\}$ is a set of independent columns in V.

M is said to be a *linear matroid* if $M = M_V$ for some matrix V.

Linear Matroids and the Matroid Intersection Problem

Linear Matroids

For matrix $V = [v_1, v_2, \ldots, v_m]$, define $M_V = (E, \mathcal{I})$ as:

1. $E : \{1, 2, \ldots, m\}$.
2. $I \in \mathcal{I}$ iff $\{v_i : i \in I\}$ is a set of independent columns in V.

M is said to be a *linear matroid* if $M = M_V$ for some matrix V.

Linear Matroid Intersection: Given M_1, M_2 with base sets $\mathcal{B}_1$, $\mathcal{B}_2$ respectively, find $B \in \mathcal{B}_1 \cap \mathcal{B}_2$ if it exists.

Linear Matroid Intersection is in RNC [NSV94]

Lemma

*U, V: $n \times m$ matrices; $\mathcal{B}_1$, $\mathcal{B}_2$: Bases of M_U, M_V.
Define Z to be an $m \times m$ diagonal matrix with diagonal entries $\{z_e\}_{e \in [m]}$ where z_e are variables and $D = UZV^T$. Then,*

$$M_U \text{ and } M_V \text{ have a common base iff } \det(D) \neq 0.$$

Proof. By Binet-Cauchy formula,

$$\det(D) = \sum_{B \subseteq [m],\ |B|=n} \left(\prod_{e \in B} z_e \right) \det(U_B) \det(V_B)$$

$$= \sum_{B \in \mathcal{B}_1 \cap \mathcal{B}_2} \left(\prod_{e \in B} z_e \right) \det(U_B) \det(V_B)$$

The Weight Function

$w : E \to \mathbb{Z}$ is a weight function.

Isolating Weight Function

w is said to be isolating for $\mathcal{A} \subseteq \mathcal{P}(E)$ if there is a unique minimum weight set in $\mathcal{A}$

The Weight Function

$w : E \to \mathbb{Z}$ is a weight function.

Isolating Weight Function

w is said to be isolating for $\mathcal{A} \subseteq \mathcal{P}(E)$ if there is a unique minimum weight set in $\mathcal{A}$

The Isolation Lemma [MVV87]

A random weight function with polynomially bounded weights is isolating for any family $\mathcal{A}$ with high probability.

The Plan and why it Works

1. Replace z_e in $\det(D)$ by $z^{w(e)}$ where z is a new variable. $\det(D)$ thus becomes a univariate in z and $\prod_{e \in B} z^{w(e)} = z^{w(B)}$.

The Plan and why it Works

1. Replace z_e in $\det(D)$ by $z^{w(e)}$ where z is a new variable. $\det(D)$ thus becomes a univariate in z and $\prod_{e \in B} z^{w(e)} = z^{w(B)}$.
2. If w is an isolating weight assignment for $\mathcal{B}_1 \cap \mathcal{B}_2$, and $\mathcal{B}_1 \cap \mathcal{B}_2 \neq \emptyset$, then the minimum degree term in $\det(D)$ is unique. Thus, we get $\det(D) \neq 0 \Leftrightarrow \mathcal{B}_1 \cap \mathcal{B}_2 \neq \emptyset$.

The Plan and why it Works

1. Replace z_e in $\det(D)$ by $z^{w(e)}$ where z is a new variable. $\det(D)$ thus becomes a univariate in z and $\prod_{e \in B} z^{w(e)} = z^{w(B)}$.
2. If w is an isolating weight assignment for $\mathcal{B}_1 \cap \mathcal{B}_2$, and $\mathcal{B}_1 \cap \mathcal{B}_2 \neq \emptyset$, then the minimum degree term in $\det(D)$ is unique. Thus, we get $\det(D) \neq 0 \Leftrightarrow \mathcal{B}_1 \cap \mathcal{B}_2 \neq \emptyset$.
3. A determinant with small degree univariate entries can be computed in NC [BCP83].

Algorithm 1: Linear Matroid Intersection - RNC

Input : $n \times m$ arrays U, V - the arrays underlying the matroids M_1 and M_2 with bases $\mathcal{B}_1$ and $\mathcal{B}_2$ respectively

Output: 0 if their bases have no intersection and a common base element B otherwise

```
Randomly choose a weight function w : E → [2m]
Let D be as described (with det(D) being a univariate in z)
if det(D) = 0 then
    return 0
B = ∅
for each e ∈ E do
    delete e and recompute det(D)
    if the minimum degree term disappears then
        B = B ∪ {e}
return B
```

Derandomising the RNC algorithm

What do we want?

Construct the weight assignment deterministically such that there is a unique *minimum weight* common base.

Derandomising the RNC algorithm

What do we want?

Construct the weight assignment deterministically such that there is a unique *minimum weight* common base.

How do they do it?

Find a sufficient condition for getting a unique *minimum weight* common base.

Derandomising the RNC algorithm

What do we want?

Construct the weight assignment deterministically such that there is a unique *minimum weight* common base.

How do they do it?

Find a sufficient condition for getting a unique *minimum weight* common base.

How do they get such a sufficient condition?

Look at the Matroid as a Polytope to get a better handle.

The Matroid Polytope and Extending the Weight function

$M = (E, \mathcal{I})$ is a matroid.
For any $S \in \mathcal{P}(E)$, $x^S \in \mathbb{R}^{|E|}$ is its characteristic vector if

$$x_e^S = \begin{cases} 1 & \text{if } e \in S \\ 0 & \text{otherwise.} \end{cases}$$

The *matroid polytope* is $P(\mathcal{I}) = \text{conv}\left\{x^I : I \in \mathcal{I}\right\} \subseteq \mathbb{R}^{|E|}$.

The Matroid Polytope and Extending the Weight function

$M = (E, \mathcal{I})$ is a matroid.
For any $S \in \mathcal{P}(E)$, $x^S \in \mathbb{R}^{|E|}$ is its characteristic vector if

$$x_e^S = \begin{cases} 1 & \text{if } e \in S \\ 0 & \text{otherwise.} \end{cases}$$

The *matroid polytope* is $P(\mathcal{I}) = \text{conv}\left\{x^I : I \in \mathcal{I}\right\} \subseteq \mathbb{R}^{|E|}$.

For any $x \in \mathbb{R}^{|E|}$ and $S \subseteq E$, define

$$w(x) = \sum_{e \in E} w(e) x_e,$$

$$w(S) = \sum_{e \in S} w(e).$$

Characterisation of the Matroid Polytope

For any $x \in \mathbb{R}^{|E|}$ and $S \subseteq E$, define

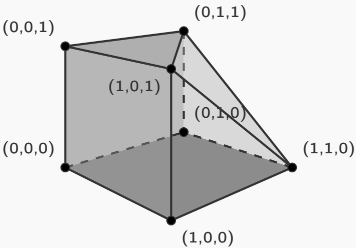
$$x(S) = \sum_{e \in S} x_e.$$

Lemma [Edm70]

For a matroid $M = (E, \mathcal{I})$, $x \in \mathbb{R}^{|E|}$ is in $P(\mathcal{I})$ iff

$$\forall e \in E, x_e \geq 0 \quad \text{and}$$

$$\forall S \subseteq E, x(S) \leq \text{rank}(S)$$



The underlying matrix:

$$\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix}$$

The Matroid Base Polytope

Characterisation

$M = (E, \mathcal{I})$: matroid;
$\mathcal{B}$: family of base sets for M.
Then $P(\mathcal{B})$: Base Polytope.

The base polytope forms a face of the matroid polytope $P(\mathcal{I})$.

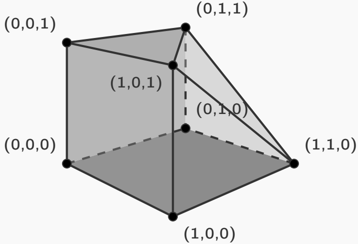
For any $x \in \mathbb{R}^{|E|}$, $x \in P(\mathcal{B})$ iff

$$\forall e \in E, x_e \geq 0,$$

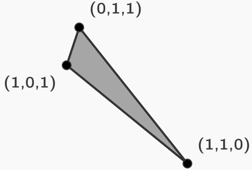
$$\forall S \subseteq E, x(S) \leq \text{rank}(S) \quad \text{and}$$

$$x(E) = \text{rank}(E)$$

The matroid polytope:



Its base polytope:



The faces are important

Observation

$w : E \to \mathbb{Z}$ is a weight assignment.
By definition, its extension to $\mathbb{R}^{|E|}$ is linear.
Thus the minimum weight points in the matroid base polytope form a face.

Notation: For $w : E \to \mathbb{Z}$, F_w is the face of min. weight points.

The faces are important

Observation

$w : E \to \mathbb{Z}$ is a weight assignment.
By definition, its extension to $\mathbb{R}^{|E|}$ is linear.
Thus the minimum weight points in the matroid base polytope form a face.

Notation: For $w : E \to \mathbb{Z}$, F_w is the face of min. weight points.

What we want: w such that F_w contains just one point.

The faces are important

Observation

$w : E \to \mathbb{Z}$ is a weight assignment.
By definition, its extension to $\mathbb{R}^{|E|}$ is linear.
Thus the minimum weight points in the matroid base polytope form a face.

Notation: For $w : E \to \mathbb{Z}$, F_w is the face of min. weight points.

What we want: w such that F_w contains just one point.

The Plan ahead:

1. Find a condition to ensure that a face in $P(\mathcal{B}_1 \cap \mathcal{B}_2)$ contains just one point
2. Find a condition on w to ensure that F_w satisfies the above condition

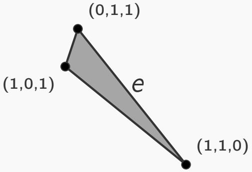
Faces of the Base Polytope

Characterisation

Any of the faces of the Matroid Base Polytope is described by additional equations of the form:

$$x_e = 0 \text{ or } x(S) = \text{rank}(S)$$

for some $S \subseteq E$.



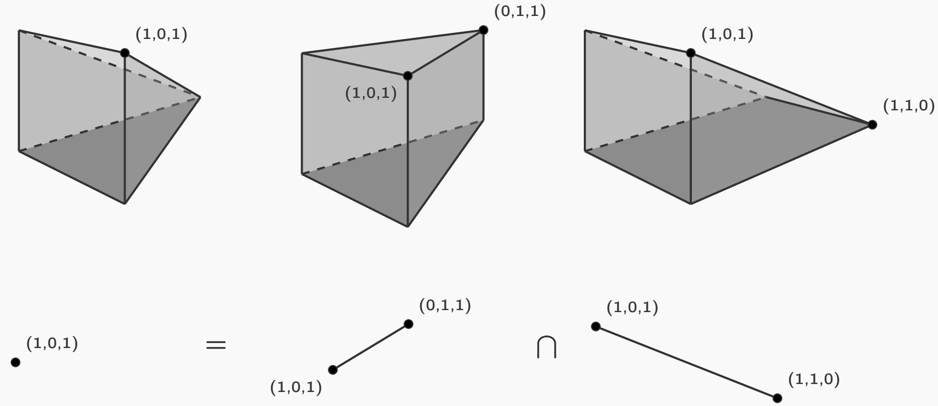
Faces of the Base Polytope:

1. $(1, 1, 0) : x_3 = 0$, $x(\{2\}) = \text{rank}(\{2\})$, $x(\{1, 2, 3\}) = \text{rank}(\{1, 2, 3\})$
2. $e : x(\{2\}) = \text{rank}(\{2\})$, $x(\{1, 2, 3\}) = \text{rank}(\{1, 2, 3\})$
3. The base polytope: $x(\{1, 2, 3\}) = \text{rank}(\{1, 2, 3\})$

Faces of the Base Intersection Polytope

Characterisation

Any face F of $P(\mathcal{B}_1 \cap \mathcal{B}_2)$ can be written as $F = F_1 \cap F_2$ for some faces F_1 and F_2 of $P(\mathcal{B}_1)$ and $P(\mathcal{B}_2)$ respectively.



Partitioning with respect to a face in the Intersection Polytope

$(E,\mathcal{I}_1)$, $(E,\mathcal{I}_2)$: matroids with base sets $\mathcal{B}_1$ and $\mathcal{B}_2$.
F: face of $P(\mathcal{B}_1 \cap \mathcal{B}_2)$.
Then, there exists partitions $\mathcal{S}$ and $\mathcal{T}$ of E satisfying:
$\forall S \in \mathcal{S},\ T \in \mathcal{T},\ \exists n_S, m_T \geq 0$ such that for any $x \in F$,

$$x(S) = n_S \text{ and } x(T) = m_T.$$

Moreover,

1. F satisfies $x(R) = \text{rank}_1(R)$ or $x(R) = \text{rank}_2(R)$
   $\Rightarrow R$ is a disjoint union of sets from $\mathcal{S}$ or $\mathcal{T}$ (resp.).
2. F satisfies $x_e = 0$
   $\Rightarrow \exists S \in \mathcal{S},\ T \in \mathcal{T}$ such that $S = T = \{e\}$ and $n_S = m_T = 0$.

Cycles in Matroid Intersection

F: a face of $P(\mathcal{B}_1 \cap \mathcal{B}_2)$ with partitions $\mathcal{S}$ and $\mathcal{T}$.
$C_F = (e_1, e_2, \ldots, e_{2r})$ is called a *cycle* with respect to the F, if:

For $i = \{1, 2, \ldots r\}$,

$$e_{2i-1}, e_{2i} \in S \quad \text{for some } S \in \mathcal{S},$$

$$e_{2i}, e_{2i+1} \in T \quad \text{for some } T \in \mathcal{T},$$

where $e_{2r+1} = e_1$.

Cycles in Matroid Intersection

F: a face of $P(\mathcal{B}_1 \cap \mathcal{B}_2)$ with partitions $\mathcal{S}$ and $\mathcal{T}$.
$C_F = (e_1, e_2, \ldots, e_{2r})$ is called a *cycle* with respect to the F, if:

For $i = \{1, 2, \ldots r\}$,

$$e_{2i-1}, e_{2i} \in S \quad \text{for some } S \in \mathcal{S},$$

$$e_{2i}, e_{2i+1} \in T \quad \text{for some } T \in \mathcal{T},$$

where $e_{2r+1} = e_1$.

Note:

Let F satisfy $x_e = 0$.
e can not appear in any cycle defined w.r.t. F because $\{e\}$ appears as a singleton in both the partitions for F.

Cycles always exist for faces with multiple bases

Lemma

Let B_1, B_2 be two bases in the face F of the polytope $P(\mathcal{B}_1 \cap \mathcal{B}_2)$. Then $B_1 \Delta B_2$ is a set of disjoint cycles.

Proof.

$x^{B_1} = (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$
$x^{B_2} = (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$

$\mathcal{S} = \{\{1, 2, 3\}, \{4, 5\}, \{6, 7, 8, 9, 10, 11, 12, 13, 14\}\} = \{S_1, S_2, S_3\}$
$\mathcal{T} = \{\{1, 2, 3, 4\}, \{5, 6, 7, 8, 9, 10, 11, 12\}, \{13, 14\}\} = \{T_1, T_2, T_3\}$

Cycles always exist for faces with multiple bases

Lemma

Let B_1, B_2 be two bases in the face F of the polytope $P(\mathcal{B}_1 \cap \mathcal{B}_2)$. Then $B_1 \Delta B_2$ is a set of disjoint cycles.

Proof.

$$x^{B_1} = (1,1,0,1,0,0,1,1,0,0,1,1,1,1)$$
$$x^{B_2} = (0,1,1,1,0,1,1,1,1,0,0,0,1,1)$$

$$\mathcal{S} = \{\{1,2,3\}, \{4,5\}, \{6,7,8,9,10,11,12,13,14\}\} = \{S_1, S_2, S_3\}$$
$$\mathcal{T} = \{\{1,2,3,4\}, \{5,6,7,8,9,10,11,12\}, \{13,14\}\} = \{T_1, T_2, T_3\}$$

1. Pick $12 \in B_1 \setminus B_2$ and let $C_1 = (12)$.
2. Note that $12 \in S_3$.
3. $|B_1 \cap S_3| = |B_2 \cap S_3|$ by property of $\mathcal{S}$.

4. Pick $9 \in (B_2 \cap S_3) \setminus (B_1 \cap S_3)$ and let $C_1 = (12, 9)$.
5. Note that $9 \in T_2$.
6. $|B_1 \cap T_2| = |B_2 \cap T_2|$ by property of $\mathcal{T}$.
7. Pick $12 \in (B_1 \cap T_2) \setminus (B_2 \cap T_2)$ and let $C_1 = (12, 9)$.
8. Set $B_1 = B_1 \setminus C_1$ and $B_2 = B_2 \setminus C_1$ and repeat.

The process stops when $B_1 = B_2$.

4. Pick $9 \in (B_2 \cap S_3) \setminus (B_1 \cap S_3)$ and let $C_1 = (12, 9)$.
5. Note that $9 \in T_2$.
6. $|B_1 \cap T_2| = |B_2 \cap T_2|$ by property of $\mathcal{T}$.
7. Pick $12 \in (B_1 \cap T_2) \setminus (B_2 \cap T_2)$ and let $C_1 = (12, 9)$.
8. Set $B_1 = B_1 \setminus C_1$ and $B_2 = B_2 \setminus C_1$ and repeat.

The process stops when $B_1 = B_2$.

Observations

Let $\mathcal{C}_F$ denote the family of all cycles with respect to the face F.

1. By the lemma: *If $\mathcal{C}_F = \emptyset$ then F has dimension 0.*
2. Going to a subface can only destroy cycles. That is:

For faces F, F' in $P(\mathcal{B}_1 \cap \mathcal{B}_2)$, $F' \subseteq F \Rightarrow \mathcal{C}_{F'} \subseteq \mathcal{C}_F$

Circulation of a Cycle

What we want: Successively eliminate cycles to reach smaller and smaller faces until we reach a face F with $\mathcal{C}_F = \varnothing$.

Circulations

For a weight assignment $w : E \to \mathbb{Z}$, the circulation $c_w(C)$ of a cycle $C = (e_1, e_2, \ldots, e_k)$ is defined as:

$$c_w(C) = |w(e_1) - w(e_2) + w(e_3) - \cdots - w(e_k)|$$

Why Circulations?

The cycles on the minimum weight face have a property which can be explained easily using it.

Cycles on the face the of Minimum Weight Common Bases

Lemma

For any face F in $P(\mathcal{B}_1 \cap \mathcal{B}_2)$, if the weight function w is such that $w(x)$ is constant on F, then $c_w(C) = 0$ for any $C \in \mathcal{C}_F$

Proof.

$C = (15, 3, 7, 11, 19, 1, 20, 18, 12, 8, 5, 10)$

$C_1 = (15, 7, 19, 20, 12, 5)$, $C_2 = (3, 11, 1, 18, 8, 10)$.

Circulation vector: $\delta_C = x^{C_1} - x^{C_2}$

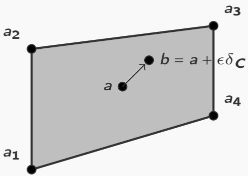
$$= (-1, 0, -1, 0, 1, 0, 1, -1, 0, -1, -1, 1, 0, 0, 1, 0, 0, -1, 1, 1)$$

$w = (1, 7, 4, 8, 3, 9, 4, 2, 10, 5, 6, 8, 2, 9, 6, 10, 1, 4, 7, 3)$

$c_w(C) = w.\delta_C = -1 - 4 + 3 + 4 - 2 - 5 - 6 + 8 + 6 - 4 + 7 + 3$

Proof (contd.)

We show that in the current setting $w.\delta_C = 0$.



$$a = \frac{a_1 + a_2 + a_3 + a_4}{4}$$

$$S_0 = \{e \in E \mid x_e = 0 \forall x \in F\}$$

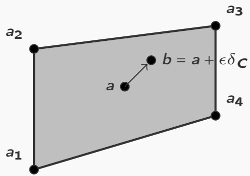
$$\mathcal{R}_1 = \{R \subseteq E \mid x(R) = \text{rank}_1(R) \forall x \in F\}$$

$$\mathcal{R}_2 = \{R \subseteq E \mid x(R) = \text{rank}_2(R) \forall x \in F\}$$

Case 1: For $e \in S_0$, $e \notin C$. Thus, $b_e = a_e = 0$.

Proof (contd.)

We show that in the current setting $w.\delta_C = 0$.



$$a = \frac{a_1 + a_2 + a_3 + a_4}{4}$$

$$S_0 = \{e \in E \mid x_e = 0 \forall x \in F\}$$

$$\mathcal{R}_1 = \{R \subseteq E \mid x(R) = \text{rank}_1(R) \forall x \in F\}$$

$$\mathcal{R}_2 = \{R \subseteq E \mid x(R) = \text{rank}_2(R) \forall x \in F\}$$

Case 1: For $e \in S_0$, $e \notin C$. Thus, $b_e = a_e = 0$.

Case 2: Let $R \in \mathcal{R}_1$ and $\mathcal{S}$: Partition of E.

$|C_1 \cap S| = |C_2 \cap S|$ for any $S \in \mathcal{S}$

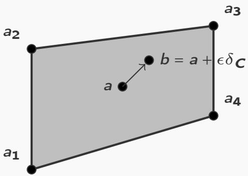
$\Rightarrow \delta_C(S) = 0$ for every $S \in \mathcal{S}$.

R is a disjoint union of sets from $\mathcal{S}$

$\Rightarrow \delta_C(R) = 0$ and $b(R) = a(R) + \epsilon\delta_C(R) = a(R) = \text{rank}_1(R)$.

Proof (contd.)

We show that in the current setting $w.\delta_C = 0$.



$$a = \frac{a_1 + a_2 + a_3 + a_4}{4}$$

$$S_0 = \{e \in E \mid x_e = 0 \forall x \in F\}$$

$$\mathcal{R}_1 = \{R \subseteq E \mid x(R) = \text{rank}_1(R) \forall x \in F\}$$

$$\mathcal{R}_2 = \{R \subseteq E \mid x(R) = \text{rank}_2(R) \forall x \in F\}$$

Case 1: For $e \in S_0$, $e \notin C$. Thus, $b_e = a_e = 0$.

Case 2: Let $R \in \mathcal{R}_1$ and $\mathcal{S}$: Partition of E.

$|C_1 \cap S| = |C_2 \cap S|$ for any $S \in \mathcal{S}$

$\Rightarrow \delta_C(S) = 0$ for every $S \in \mathcal{S}$.

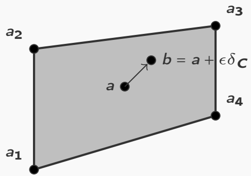
R is a disjoint union of sets from $\mathcal{S}$

$\Rightarrow \delta_C(R) = 0$ and $b(R) = a(R) + \epsilon\delta_C(R) = a(R) = \text{rank}_1(R)$.

Case 3: Similar (Take $R \in \mathcal{R}_2$ and $\mathcal{T}$: Partition of E)

Proof (contd.)

We show that in the current setting $w.\delta_C = 0$.



$$a = \frac{a_1 + a_2 + a_3 + a_4}{4}$$

$$S_0 = \{e \in E \mid x_e = 0 \forall x \in F\}$$

$$\mathcal{R}_1 = \{R \subseteq E \mid x(R) = \text{rank}_1(R) \forall x \in F\}$$

$$\mathcal{R}_2 = \{R \subseteq E \mid x(R) = \text{rank}_2(R) \forall x \in F\}$$

Case 1: For $e \in S_0$, $e \notin C$. Thus, $b_e = a_e = 0$.

Case 2: Let $R \in \mathcal{R}_1$ and $\mathcal{S}$: Partition of E.

$|C_1 \cap S| = |C_2 \cap S|$ for any $S \in \mathcal{S}$
$\Rightarrow \delta_C(S) = 0$ for every $S \in \mathcal{S}$.
R is a disjoint union of sets from $\mathcal{S}$
$\Rightarrow \delta_C(R) = 0$ and $b(R) = a(R) + \epsilon\delta_C(R) = a(R) = \text{rank}_1(R)$.

Case 3: Similar (Take $R \in \mathcal{R}_2$ and $\mathcal{T}$: Partition of E)

$$a + \epsilon\delta_C \in F \Rightarrow w(a) = w(a + \epsilon\delta_C) \Rightarrow w(\delta_C) = w.\delta_C = 0.$$

The Picture gets a little Clearer...

Putting it all together...

w: a weight function;
C: a cycle on some face of $P(\mathcal{B}_1 \cap \mathcal{B}_2)$.
Then,

$$c_w(C) \neq 0 \Rightarrow C \notin \mathcal{C}_{F_w}.$$

Thus, a sufficient condition for w to be isolating:

$$c_w(C) \neq 0 \text{ for every } C \text{ in } P(\mathcal{B}_1 \cap \mathcal{B}_2).$$

The Picture gets a little Clearer...

Putting it all together...

w: a weight function;
C: a cycle on some face of $P(\mathcal{B}_1 \cap \mathcal{B}_2)$.
Then,

$$c_w(C) \neq 0 \Rightarrow C \notin \mathcal{C}_{F_w}.$$

Thus, a sufficient condition for w to be isolating:

$$c_w(C) \neq 0 \text{ for every } C \text{ in } P(\mathcal{B}_1 \cap \mathcal{B}_2).$$

What we need to do: Ensure that such a w can be found.

Isolating Weight Assignments can be found

Lemma [CRS95]

For any number s, a set of $O(m^2 s)$ integer weight functions on the set E can be constructed with weight bounded by $O(m^2 s)$ in time $\text{poly}(ms)$ such that for any set of s cycles, one of the weight functions will give non-zero ciclulation to each of the s cycles.

Proof. Let $E = \{e_1, e_2, \ldots, e_m\}$.
Define $w(e_i) = 2^{i-1}$ for each $i \in \{1, 2, \ldots, n\}$.
Consider $\mathcal{W} = \{w \pmod{j} \mid 2 \leq j \leq t\}$ for some t to be decided.
Let $\{C_1, C_2, \ldots C_s\}$ be a set of s cycles.

What we want:

$$\exists j \leq t \ \forall i \leq s, c_{w \pmod{j}}(C_i) \neq 0.$$

Proof (contd.)

However,

$$\exists j \leq t \ \forall i \leq s, c_{w \pmod{j}}(C_i) \neq 0 \Leftarrow \exists j \leq t, \prod_{i=1}^{s} c_w(C_i) \neq 0 \pmod{j}$$
$$\Leftarrow \operatorname{lcm}(2,3,\ldots,t) \not| \prod_{i=1}^{s} c_w(C_i)$$
$$\Leftarrow \operatorname{lcm}(2,3,\ldots,t) \geq \prod_{i=1}^{s} c_w(C_i).$$

Also,

$$\prod_{i=1}^{s} c_w(C_i) \leq 2^{m^2 s}.$$

and by [Nai82], $\operatorname{lcm}(2,3,\ldots,t) \geq 2^t$ for $t \geq 7$.

Thus, $t = m^2 s$ suffices.

The final stretch

Observation

There can be exponentially many cycles - *Achieving non-zero circulation for all cycles in one go is not possible.*

The final stretch

Observation

There can be exponentially many cycles - *Achieving non-zero circulation for all cycles in one go is not possible.*

The Plan Ahead:

1. Ensure that if cycles of a certain length are removed, then not too many cycles of double this length remain.
2. Eliminate cycles in rounds - *In each round, double the length of the cycles eliminated.*

Eliminating Cycles

Lemma

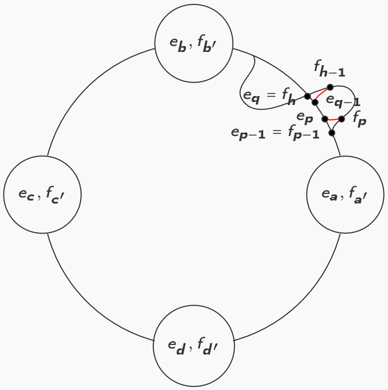
Let F be a face of $P(\mathcal{B}_1 \cap \mathcal{B}_2)$. If $\mathcal{C}_F$ has no cycles of length $\leq r$, for some even number number $r \geq 2$, then $\mathcal{C}_F$ has $\leq m^4$ cycles of length $\leq 2r$.

Proof. $\mathcal{S}$ and $\mathcal{T}$: Partitions of E w.r.t. F.
$C = (e_0, e_1, \ldots, e_{s-1})$ is a cycle of length $s \leq 2r$.
Choose fours points from C that divide it into four equal parts:

$$(a, b, c, d) = (0, \lceil s/4 \rceil, \lceil s/2 \rceil, \lceil 3s/4 \rceil)$$

Claim: The tuple (e_a, e_b, e_c, e_d) uniquley describes C.
There are at most m^4 ways of choosing the tuple.

Proof of the Claim



$C' = (f_0, f_1, \ldots, f_{t-1})$;
$(a', b', c', d') = (0, \lceil t/4 \rceil, \lceil t/2 \rceil, \lceil 3t/4 \rceil)$;
$(e_a, e_b, e_c, e_d) = (f_{a'}, f_{b'}, f_{c'}, f_{d'})$.

$e_{p-1} = f_{p-1} \Rightarrow e_p,\ f_p$ belong to a common $S \in \mathcal{S}$ or $T \in \mathcal{T}$.

Case 1: q and h have same parity.
$e_q = f_h \Rightarrow e_{q-1},\ f_{h-1}$ belong to a common $S \in \mathcal{S}$ or $T \in \mathcal{T}$.

Case 2: q and h have different parity.
$e_{q-1},\ f_h$ belong to a common $S \in \mathcal{S}$ or $T \in \mathcal{T}$.

In both cases, there is a cycle of length $\leq r$. Contradiction.

The Isolating Weight Construction

Given:

$(E, \mathcal{I}_1)$, $(E, \mathcal{I}_2)$: Matroids with collection of base sets $\mathcal{B}_1$, $\mathcal{B}_2$.

The Construction:

Let $m = |E|$ and $t = \lceil \log m \rceil$. Define $F_0 = P(\mathcal{B}_2 \cap \mathcal{B}_2)$.

The Isolating Weight Construction

Given:

$(E, \mathcal{I}_1)$, $(E, \mathcal{I}_2)$: Matroids with collection of base sets $\mathcal{B}_1$, $\mathcal{B}_2$.

The Construction:

Let $m = |E|$ and $t = \lceil \log m \rceil$. Define $F_0 = P(\mathcal{B}_2 \cap \mathcal{B}_2)$.
For $i = 0, 1, \ldots, t-1$, define:

- w_i = weight assignment such that $c_{w_i}(C) \neq 0$, for any cycle $C \in \mathcal{C}_{F_i}$ of length 2^{i+1}.
- F_{i+1} = set of minimum weight points of F_i with respect to w_i.

The Isolating Weight Construction

Given:

$(E, \mathcal{I}_1)$, $(E, \mathcal{I}_2)$: Matroids with collection of base sets $\mathcal{B}_1$, $\mathcal{B}_2$.

The Construction:

Let $m = |E|$ and $t = \lceil \log m \rceil$. Define $F_0 = P(\mathcal{B}_2 \cap \mathcal{B}_2)$.
For $i = 0, 1, \ldots, t-1$, define:

- w_i = weight assignment such that $c_{w_i}(C) \neq 0$, for any cycle $C \in \mathcal{C}_{F_i}$ of length 2^{i+1}.
- F_{i+1} = set of minimum weight points of F_i with respect to w_i.

Let N be greater than any of weights in $w_0, w_1, \ldots, w_{t-1}$.

The Isolating Weight Construction

Given:

$(E, \mathcal{I}_1)$, $(E, \mathcal{I}_2)$: Matroids with collection of base sets $\mathcal{B}_1$, $\mathcal{B}_2$.

The Construction:

Let $m = |E|$ and $t = \lceil \log m \rceil$. Define $F_0 = P(\mathcal{B}_2 \cap \mathcal{B}_2)$.

For $i = 0, 1, \ldots, t-1$, define:

- w_i = weight assignment such that $c_{w_i}(C) \neq 0$, for any cycle $C \in \mathcal{C}_{F_i}$ of length 2^{i+1}.
- F_{i+1} = set of minimum weight points of F_i with respect to w_i.

Let N be greater than any of weights in $w_0, w_1, \ldots, w_{t-1}$.

For $i = 0, 1, \ldots, t-1$, define:

$$W_i = w_0 N^i + w_1 N^{i-1} + \cdots + w_i N^0.$$

The final weight assignment: W_{t-1}.

The quasi-NC Algorithm

For each $i = 0, 1, \dots, t-1$,

- w_i has $O(m^6)$ possibilities.
- w_i has weights bounded by $O(m^6)$.

The quasi-NC Algorithm

For each $i = 0, 1, \ldots, t-1$,

- w_i has $O(m^6)$ possibilities.
- w_i has weights bounded by $O(m^6)$.

Thus,

$$W_{t-1} \text{ has } O(m^{6 \log m}) \text{ possible cominations}$$

and

$$W_{t-1} \text{ has weights bounded by } O(m^{6 \log m}).$$

The quasi-NC Algorithm

For each $i = 0, 1, \ldots, t-1$,

- w_i has $O(m^6)$ possibilities.
- w_i has weights bounded by $O(m^6)$.

Thus,

$$W_{t-1} \text{ has } O(m^{6 \log m}) \text{ possible cominations}$$

and

$$W_{t-1} \text{ has weights bounded by } O(m^{6 \log m}).$$

Try all in parallel: Plug in the wt. assignment in the determinant polynomial (as in [NSV94]) and find $B \in \mathcal{B}_1 \cap \mathcal{B}_2$ if present.

The quasi-NC Algorithm

For each $i = 0, 1, \ldots, t-1$,

- w_i has $O(m^6)$ possibilities.
- w_i has weights bounded by $O(m^6)$.

Thus,

$$W_{t-1} \text{ has } O(m^{6 \log m}) \text{ possible cominations}$$

and

$$W_{t-1} \text{ has weights bounded by } O(m^{6 \log m}).$$

Try all in parallel: Plug in the wt. assignment in the determinant polynomial (as in [NSV94]) and find $B \in \mathcal{B}_1 \cap \mathcal{B}_2$ if present.

Weights are quasi-polynomially bounded $\Rightarrow$ Entries of the determinant are expressible in quasi-polynomially many bits.

By [Ber84, BCP83], the determinant can be computed in quasi-NC.

Correctness

Claim

F_{i+1} is set of minimum weight points in $P(\mathcal{B}_1 \cap \mathcal{B}_2)$ w.r.t. W_i for $i = 0, 1, \ldots, t-1$.

Proof. By Induction.

Clearly true for $i = 0$. Assume true for F_i. Then,
F_i is set of minimum weight points in $P(\mathcal{B}_1 \cap \mathcal{B}_2)$ w.r.t. NW_{i-1}.

Correctness

Claim

F_{i+1} is set of minimum weight points in $P(\mathcal{B}_1 \cap \mathcal{B}_2)$ w.r.t. W_i for $i = 0, 1, \ldots, t-1$.

Proof. By Induction.

Clearly true for $i = 0$. Assume true for F_i. Then,
F_i is set of minimum weight points in $P(\mathcal{B}_1 \cap \mathcal{B}_2)$ w.r.t. NW_{i-1}.
Now

$$N > w_i \Rightarrow NW_{i-1} > w_i \text{ and } W_i = NW_{i-1} + w_i.$$

Thus, $W_i(x)$ is minimum for $x \in P(\mathcal{B}_1 \cap \mathcal{B}_2)$ if and only if

$$NW_{i-1}(x) \text{ is minimum for } x \in P(\mathcal{B}_1 \cap \mathcal{B}_2) \text{ (that is, } x \in F_i)$$

and $w_i(x)$ is minimum.

Correctness

Claim

F_{i+1} is set of minimum weight points in $P(\mathcal{B}_1 \cap \mathcal{B}_2)$ w.r.t. W_i for $i = 0, 1, \ldots, t-1$.

Proof. By Induction.

Clearly true for $i = 0$. Assume true for F_i. Then,
F_i is set of minimum weight points in $P(\mathcal{B}_1 \cap \mathcal{B}_2)$ w.r.t. NW_{i-1}.
Now

$$N > w_i \Rightarrow NW_{i-1} > w_i \text{ and } W_i = NW_{i-1} + w_i.$$

Thus, $W_i(x)$ is minimum for $x \in P(\mathcal{B}_1 \cap \mathcal{B}_2)$ if and only if

$$NW_{i-1}(x) \text{ is minimum for } x \in P(\mathcal{B}_1 \cap \mathcal{B}_2) \text{ (that is, } x \in F_i)$$

and $w_i(x)$ is minimum. Thus, $F_{i+1} \subseteq F_i$ and

$$W_i(x) \text{ is minimum for } x \in P(\mathcal{B}_1 \cap \mathcal{B}_2) \Leftrightarrow x \in F_{i+1}$$

Correctness (contd.)

Claim

For $i = 1, 2, \ldots, t$, $\mathcal{C}_{F_i}$ has no cycles of length $\leq 2^i$.

Proof. For $i = 1, 2, \ldots, t$,

$$c_{w_{i-1}}(C) \neq 0 \text{ for every } C \in \mathcal{C}_{F_{i-1}} \text{ of length } \leq 2^i$$

but w_{i-1} is constant over $F_i \Rightarrow c_{w_{i-1}}(C) = 0$ for every $C \in \mathcal{C}_{F_i}$.
As $C_{F_i} \subseteq C_{F_{i-1}}$, $\mathcal{C}_{F_i}$ has no cycles of length $\leq 2^i$.

Correctness (contd.)

Claim

For $i = 1, 2, \ldots, t$, $\mathcal{C}_{F_i}$ has no cycles of length $\leq 2^i$.

Proof. For $i = 1, 2, \ldots, t$,

$$c_{w_{i-1}}(C) \neq 0 \text{ for every } C \in \mathcal{C}_{F_{i-1}} \text{ of length } \leq 2^i$$

but w_{i-1} is constant over $F_i \Rightarrow c_{w_{i-1}}(C) = 0$ for every $C \in \mathcal{C}_{F_i}$.
As $C_{F_i} \subseteq C_{F_{i-1}}$, $\mathcal{C}_{F_i}$ has no cycles of length $\leq 2^i$.

Lemma

W_{t-1} is isolating.

Proof. The face minimised by W_{t-1} is F_t. That is, $F_{W_t} = F_t$.
$\mathcal{C}_{F_t}$ has no cycles of length $\leq 2^t = m$. That is, $\mathcal{C}_{F_t} = \emptyset$.

References I

Allan Borodin, Stephen A. Cook, and Nicholas Pippenger.
Parallel computation for well-endowed rings and space-bounded probabilistic machines.
Information and Control, 58(1-3):113–136, 1983.

Stuart J. Berkowitz.
On computing the determinant in small parallel time using a small number of processors.
Inf. Process. Lett., 18(3):147–150, 1984.

Suresh Chari, Pankaj Rohatgi, and Aravind Srinivasan.
Randomness-optimal unique element isolation with applications to perfect matching and related problems.
SIAM J. Comput., 24(5):1036–1050, 1995.

Jack Edmonds.
Submodular functions, matroids, and certain polyhedra.
Edited by G. Goos, J. Hartmanis, and J. van Leeuwen, 11, 1970.

References II

Ketan Mulmuley, Umesh V. Vazirani, and Vijay V. Vazirani.
Matching is as easy as matrix inversion.
Combinatorica, 7(1):105–113, 1987.

Mohan Nair.
On chebyshev-type inequalities for primes.
The American Mathematical Monthly, 89(2):126–129, 1982.

H. Narayanan, Huzur Saran, and Vijay V. Vazirani.
Randomized parallel algorithms for matroid union and intersection, with applications to arboresences and edge-disjoint spanning trees.
SIAM J. Comput., 23(2):387–397, 1994.