Dividing permutations in the semiring of functional digraphs

Florian Bridoux, Adrien Richard, Christophe Crespelle

I3S, CNRS, Université Côte d'Azur

Thi Ha Duong Phan

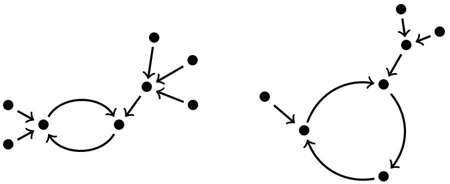
Institute of Mathematics, Vietnam Academy of Science and Technology

AUTOMATA'24

Durham, UK, July 22

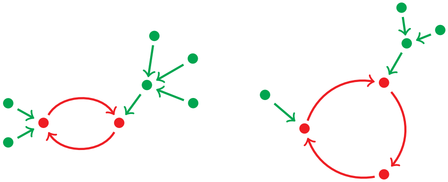
Functional digraphs

Each vertex has exactly one out-neighbor



Functional digraphs

Each vertex has exactly one out-neighbor



- Periodic part = disjoint union of cycles = **permutation**
- Transient part

Semiring on functional digraphs [Dennunzio, Dorigatti, Formenti, Manzoni, Porreca 2018]

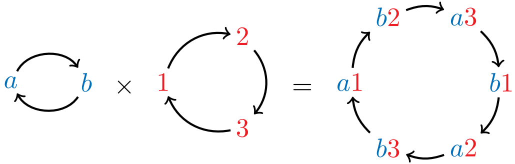
Given two functional digraphs A, B:

- the addition $A + B$ is the disjoint union of A and B,
- the product $A \times B$ (AB) is the direct product of A and B.

Semiring on functional digraphs [Dennunzio, Dorigatti, Formenti, Manzoni, Porreca 2018]

Given two functional digraphs A, B:

- the addition $A + B$ is the disjoint union of A and B,
- the product $A \times B$ (AB) is the direct product of A and B.

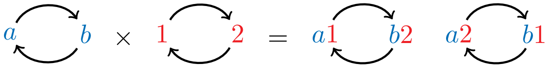


$$C_2 \times C_3 = C_6$$

Semiring on functional digraphs [Dennunzio, Dorigatti, Formenti, Manzoni, Porreca 2018]

Given two functional digraphs A, B:

- the addition $A + B$ is the disjoint union of A and B,
- the product $A \times B$ (AB) is the direct product of A and B.

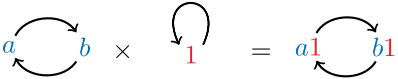


$$C_2 \times C_2 = C_2 + C_2 = 2C_2$$

Semiring on functional digraphs [Dennunzio, Dorigatti, Formenti, Manzoni, Porreca 2018]

Given two functional digraphs A, B:

- the addition $A + B$ is the disjoint union of A and B,
- the product $A \times B$ (AB) is the direct product of A and B.

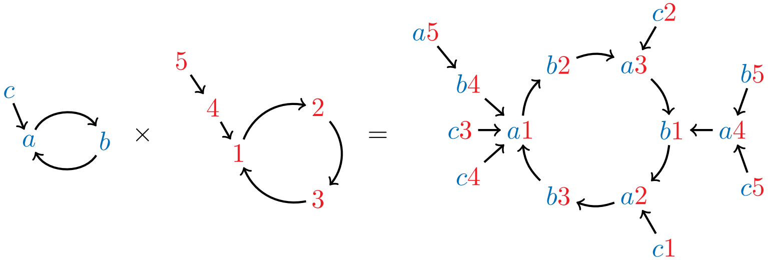


$$C_2 \times C_1 = C_2$$

Semiring on functional digraphs [Dennunzio, Dorigatti, Formenti, Manzoni, Porreca 2018]

Given two functional digraphs A, B:

- the addition $A + B$ is the disjoint union of A and B,
- the product $A \times B$ (AB) is the direct product of A and B.



Complexity issues regarding the product [Antonio E. Porreca]

1) Almost all functional digraphs X are irreducible, even for permutations

$$X = AB \quad \Rightarrow \quad A = C_1 \text{ or } B = C_1$$

Complexity issues regarding the product [Antonio E. Porreca]

1) Almost all functional digraphs X are irreducible, even for permutations

$$X = AB \quad \Rightarrow \quad A = C_1 \text{ or } B = C_1$$

$\hookrightarrow$ Complexity of testing irreducibility?

Complexity issues regarding the product [Antonio E. Porreca]

1) Almost all functional digraphs X are irreducible, even for permutations

$$X = AB \quad \Rightarrow \quad A = C_1 \text{ or } B = C_1$$

$\hookrightarrow$ Complexity of testing irreducibility?

2) Not unique factorisation into irreducibles, even for permutations.

Complexity issues regarding the product [Antonio E. Porreca]

1) Almost all functional digraphs X are irreducible, even for permutations

$$X = AB \quad \Rightarrow \quad A = C_1 \text{ or } B = C_1$$

$\hookrightarrow$ Complexity of testing irreducibility?

2) Not unique factorisation into irreducibles, even for permutations.

$$C_2 \times C_2 = 2C_2$$

$$C_2 \times 2C_1 = C_2 \times (C_1 + C_1) = C_2 + C_2 = 2C_2.$$

Complexity issues regarding the product [Antonio E. Porreca]

1) Almost all functional digraphs X are irreducible, even for permutations

$$X = AB \quad \Rightarrow \quad A = C_1 \text{ or } B = C_1$$

$\hookrightarrow$ Complexity of testing irreducibility?

2) Not unique factorisation into irreducibles, even for permutations.

$\hookrightarrow$ Complexity of finding one factorization?

Complexity issues regarding the product [Antonio E. Porreca]

1) Almost all functional digraphs X are irreducible, even for permutations

$$X = AB \quad \Rightarrow \quad A = C_1 \text{ or } B = C_1$$

$\hookrightarrow$ Complexity of testing irreducibility?

2) Not unique factorisation into irreducibles, even for permutations.

$\hookrightarrow$ Complexity of finding one factorization?

Proposition (unpublished) For infinitely many permutations X, the number of factorizations of X is at least

$$e^{|X|^{o(1)}}.$$

Complexity issues regarding the product [Antonio E. Porreca]

1) Almost all functional digraphs X are irreducible, even for permutations

$$X = AB \quad \Rightarrow \quad A = C_1 \text{ or } B = C_1$$

↪ Complexity of testing irreducibility?

2) Not unique factorisation into irreducibles, even for permutations.

↪ Complexity of finding one factorization?

Proposition (unpublished) For infinitely many permutations X, the number of factorizations of X is at least

$$e^{|X|^{o(1)}}.$$

↪ Is this lower bound tight?

Complexity issues regarding the product [Antonio E. Porreca]

3) Division is not unique: Given A, B we can have many X satisfying $AX = B$, even when A, B are permutations.

$$\underbrace{C_2}_{A} \times \underbrace{C_2}_{X} = \underbrace{2C_2}_{B}$$
$$\underbrace{C_2}_{A} \times \underbrace{2C_1}_{X} = \underbrace{2C_2}_{B}$$

Complexity issues regarding the product [Antonio E. Porreca]

3) Division is not unique: Given A, B we can have many X satisfying $AX = B$, even when A, B are permutations.

$\hookrightarrow$ Complexity of deciding if $A \mid B$, or enumerating solutions X?

Complexity issues regarding the product [Antonio E. Porreca]

3) Division is not unique: Given A, B we can have many X satisfying $AX = B$, even when A, B are permutations.

$\hookrightarrow$ Complexity of deciding if $A \mid B$, or enumerating solutions X?

Polynomial algorithm to decide if $A \mid B$ when

- B is a dendron. [Naquin, Gadouleau 24]
- A, B are permutations, and A or B homogeneous. [Dennunzio et al 2024]

Complexity issues regarding the product [Antonio E. Porreca]

3) Division is not unique: Given A, B we can have many X satisfying $AX = B$, even when A, B are permutations.

$\hookrightarrow$ Complexity of deciding if $A \mid B$, or enumerating solutions X?

Polynomial algorithm to decide if $A \mid B$ when

- B is a dendron. [Naquin, Gadouleau 24]
- A, B are permutations, and A or B homogeneous. [Dennunzio et al 2024]

Proposition (unpublished) For infinitely many permutations A, B, the number of solutions X to $AX = B$ is at least

$$e^{|A+B|^{o(1)}}.$$

Complexity issues regarding the product [Antonio E. Porreca]

3) Division is not unique: Given A, B we can have many X satisfying $AX = B$, even when A, B are permutations.

$\hookrightarrow$ Complexity of deciding if $A \mid B$, or enumerating solutions X?

Polynomial algorithm to decide if $A \mid B$ when

- B is a dendron. [Naquin, Gadouleau 24]
- A, B are permutations, and A or B homogeneous. [Dennunzio et al 2024]

Proposition (unpublished) For infinitely many permutations A, B, the number of solutions X to $AX = B$ is at least

$$e^{|A+B|^{o(1)}}.$$

$\hookrightarrow$ Is this lower bound tight?

Complexity issues regarding the product [Antonio E. Porreca]

3) Division is not unique: Given A, B we can have many X satisfying $AX = B$, even when A, B are permutations.

$\hookrightarrow$ Complexity of deciding if $A \mid B$, or enumerating solutions X?

Polynomial algorithm to decide if $A \mid B$ when

- B is a dendron. [Naquin, Gadouleau 24]
- A, B are permutations, and A or B homogeneous. [Dennunzio et al 2024]

Proposition (unpublished) For infinitely many permutations A, B, the number of solutions X to $AX = B$ is at least

$$e^{|A+B|^{o(1)}}.$$

$\hookrightarrow$ Is this lower bound tight?

4) Are there prime X?

$$X|AB \quad \Rightarrow \quad X|A \text{ or } X \mid B$$

Complexity issues regarding the product [Antonio E. Porreca]

3) Division is not unique: Given A, B we can have many X satisfying $AX = B$, even when A, B are permutations.

$\hookrightarrow$ Complexity of deciding if $A \mid B$, or enumerating solutions X?

Polynomial algorithm to decide if $A \mid B$ when

- B is a dendron. [Naquin, Gadouleau 24]
- A, B are permutations, and A or B homogeneous. [Dennunzio et al 2024]

Proposition (unpublished) For infinitely many permutations A, B, the number of solutions X to $AX = B$ is at least

$$e^{|A+B|^{o(1)}}.$$

$\hookrightarrow$ Is this lower bound tight?

4) Are there prime X? $\rightarrow$ Is primality decidable?

$$X|AB \quad \Rightarrow \quad X|A \text{ or } X \mid B$$

Division problem for permutations

instance = couple (A, B) of permutations; its size is $|A + B|$

solution = permutation X such that $AX = B$

$\mathrm{Sol}(A, B)$ = set of solutions

$\mathrm{sol}(A, B)$ = number of solutions

- decision: complexity of deciding if a solution exists $(A \mid B)$?
- counting: complexity of computing the nb of solutions?
- enumeration: complexity of enumerating the solutions?

Brut force enumeration

Proposition
The solutions X to $AX = B$ can be enumerated in $e^{O\left(\sqrt{|B|/|A|}\right)}$.

Brut force enumeration

Proposition
The solutions X to $AX = B$ can be enumerated in $e^{O\left(\sqrt{|B|/|A|}\right)}$.

A solution X is a permutation of size $n = |B|/|A|$.

A permutation X of size n can be regarded as a partition of n:

$$2C_2 + C_3 + 3C_5 \equiv 2, 2, 3, 5, 5, 5 \quad \text{(partition of } 22\text{)}$$

Brut force enumeration

Proposition
The solutions X to $AX = B$ can be enumerated in $e^{O\left(\sqrt{|B|/|A|}\right)}$.

A solution X is a permutation of size $n = |B|/|A|$.

A permutation X of size n can be regarded as a partition of n:

$$2C_2 + C_3 + 3C_5 \equiv 2, 2, 3, 5, 5, 5 \quad \text{(partition of 22)}$$

It is well known that:

- the number of partitions of n is $e^{O(\sqrt{n})}$ (Hardy-Ramanujan)
- partitions can be enumerated with polynomial delay.

Brut force enumeration

Proposition
The solutions X to $AX = B$ can be enumerated in $e^{O\left(\sqrt{|B|/|A|}\right)}$.

A solution X is a permutation of size $n = |B|/|A|$.

A permutation X of size n can be regarded as a partition of n:

$$2C_2 + C_3 + 3C_5 \equiv 2, 2, 3, 5, 5, 5 \quad \text{(partition of } 22\text{)}$$

It is well known that:

- the number of partitions of n is $e^{O(\sqrt{n})}$ (Hardy-Ramanujan)
- partitions can be enumerated with polynomial delay.

For each partition of n:

- we take the corresponding permutation X,
- we check if $AX = B$ in $O(|A||B|)$.

Brut force enumeration

Proposition
The solutions X to $AX = B$ can be enumerated in $e^{O\left(\sqrt{|B|/|A|}\right)}$.

A solution X is a permutation of size $n = |B|/|A|$.

A permutation X of size n can be regarded as a partition of n:

$$2C_2 + C_3 + 3C_5 \equiv 2, 2, 3, 5, 5, 5 \quad \text{(partition of } 22\text{)}$$

It is well known that:

- the number of partitions of n is $e^{O(\sqrt{n})}$ (Hardy-Ramanujan)
- partitions can be enumerated with polynomial delay.

For each partition of n:

- we take the corresponding permutation X,
- we check if $AX = B$ in $O(|A||B|)$.

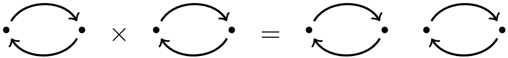
Annoying situation: no better algo, even to decide if $A \mid B$!!!

Product in more details

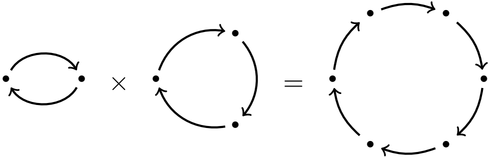
$$C_p \times C_q = \left(\frac{pq}{p \vee q}\right) C_{p \vee q}$$

Product in more details

$$C_p \times C_q = \left(\frac{pq}{p \vee q}\right) C_{p \vee q}$$



$$C_2 \times C_2 = 2C_2$$



$$C_2 \times C_3 = C_6$$

Product in more details

$$C_p \times C_q = \left(\frac{pq}{p \vee q}\right) C_{p \vee q}$$

The support L_X of a permutation X is the cycle lengths in X:

$$X = 5C_2 + 7C_3 + 3C_5 \qquad L_X = \{2, 3, 5\}$$

Product in more details

$$C_p \times C_q = \left(\frac{pq}{p \vee q}\right) C_{p \vee q}$$

The support L_X of a permutation X is the cycle lengths in X:

$$X = 5C_2 + 7C_3 + 3C_5 \qquad L_X = \{2, 3, 5\}$$

Important property: If $AX = B$ then

$$p \in L_A \text{ and } q \in L_X \quad \Rightarrow \quad p \vee q \in L_B.$$

Product in more details

$$C_p \times C_q = \left(\frac{pq}{p \vee q}\right) C_{p \vee q}$$

The support L_X of a permutation X is the cycle lengths in X:

$$X = 5C_2 + 7C_3 + 3C_5 \qquad L_X = \{2, 3, 5\}$$

Important property: If $AX = B$ then

$$p \in L_A \text{ and } q \in L_X \quad \Rightarrow \quad p \vee q \in L_B.$$

The cross-lcm between L_A and L_X is in L_B:

$$L_A \vee L_X \subseteq L_B.$$

Support of an instance

The support of an instance (A, B) is the largest set $L_{A,B}$ satisfying

$$L_A \vee L_{A,B} \subseteq L_B$$

Support of an instance

The support of an instance (A, B) is the largest set $L_{A,B}$ satisfying

$$L_A \vee L_{A,B} \subseteq L_B$$

Example:

$$\underbrace{\{2\}}_{L_A} \vee \underbrace{\{1, 2, 5, 10\}}_{L_{A,B}} = \underbrace{\{2, 10\}}_{L_B}.$$

Support of an instance

The support of an instance (A, B) is the largest set $L_{A,B}$ satisfying

$$L_A \vee L_{A,B} \subseteq L_B$$

Example:

$$\underbrace{\{2\}}_{L_A} \vee \underbrace{\{1, 2, 5, 10\}}_{L_{A,B}} = \underbrace{\{2, 10\}}_{L_B}.$$

Important property: If $AX = B$ then we saw that

$$L_A \vee L_X \subseteq L_B$$

and thus

$$L_X \subseteq L_{A,B}.$$

Support of an instance

The support of an instance (A, B) is the largest set $L_{A,B}$ satisfying

$$L_A \vee L_{A,B} \subseteq L_B$$

Example:

$$\underbrace{\{2\}}_{L_A} \vee \underbrace{\{1, 2, 5, 10\}}_{L_{A,B}} = \underbrace{\{2, 10\}}_{L_B}.$$

Important property: If $AX = B$ then we saw that

$$L_A \vee L_X \subseteq L_B$$

and thus

$$L_X \subseteq L_{A,B}.$$

Lemma A solution X is a partition of $n = |B|/|A|$ with parts in $L_{A,B}$.

Brut force approach on the support

Lemma The solutions X to $AX = B$ can be enumerated in

$$O\left(|A||B|\left(\frac{|B|}{|A|}\right)^{|L_{A,B}|}\right)$$

A solution X is a partition of $n = |B|/|A|$ with parts in $L_{A,B}$.

These partitions can be enumerated in $O(n^{|L_{A,B}|})$.

Brut force approach on the support

Lemma The solutions X to $AX = B$ can be enumerated in

$$O\left(|A||B|\left(\frac{|B|}{|A|}\right)^{|L_{A,B}|}\right)$$

A solution X is a partition of $n = |B|/|A|$ with parts in $L_{A,B}$.

These partitions can be enumerated in $O(n^{|L_{A,B}|})$.

For each partition:

- we take the corresponding permutation X,
- we check if $AX = B$ in $O(|A||B|)$.

Main result

Theorem We can compute the number of solutions X to $AX = B$ in

$$O\left(|A||B|^2\left(\frac{|B|}{|A|}\right)^{\mathrm{div}(\mathrm{lcm} L_A)}\right).$$

$\hookrightarrow$ **Polynomial when A fixed.**

Main result

Theorem We can compute the number of solutions X to $AX = B$ in

$$O\left(|A||B|^2\left(\frac{|B|}{|A|}\right)^{\operatorname{div}(\operatorname{lcm} L_A)}\right).$$

$\hookrightarrow$ **Polynomial when A fixed.**

Two cases:

- (A, B) basic: $L_{A,B} \subseteq \operatorname{Div}(\operatorname{lcm} L_A)$ $\rightarrow$ brut force approach

Main result

Theorem We can compute the number of solutions X to $AX = B$ in

$$O\left(|A||B|^2\left(\frac{|B|}{|A|}\right)^{\mathrm{div}(\mathrm{lcm} L_A)}\right).$$

$\hookrightarrow$ **Polynomial when A fixed.**

Two cases:

- (A, B) basic: $L_{A,B} \subseteq \mathrm{Div}(\mathrm{lcm}\, L_A)$ $\rightarrow$ brut force approach
- (A, B) non-basic $\rightarrow$ divide-and-conquer technique
  - split the instance (A, B) into few basic instances (A_i, B_i),
  - compute the nb of solutions s_i of (A_i, B_i) as in the fist case,
  - output the product of the s_i.

Instance split

A split of (A, B) is $(A, B_1), (A, B_2)$ with

$$B = B_1 + B_2 \qquad (B_1, B_2 \neq \emptyset).$$

Instance split

A split of (A, B) is $(A, B_1), (A, B_2)$ with

$$B = B_1 + B_2 \qquad (B_1, B_2 \neq \emptyset).$$

If $AX_1 = B_1$ and $AX_2 = B_2$, then

$$A(X_1 + X_2) = AX_1 + AX_2 = B_1 + B_2 = B$$

Instance split

A split of (A, B) is $(A, B_1), (A, B_2)$ with

$$B = B_1 + B_2 \qquad (B_1, B_2 \neq \emptyset).$$

If $AX_1 = B_1$ and $AX_2 = B_2$, then

$$A(X_1 + X_2) = AX_1 + AX_2 = B_1 + B_2 = B$$

The sum of “local” solutions is a “global” solution:

$$\mathrm{Sol}(A, B_1) + \mathrm{Sol}(A, B_2) \subseteq \mathrm{Sol}(A, B).$$

Instance split

A split of (A, B) is $(A, B_1), (A, B_2)$ with

$$B = B_1 + B_2 \qquad (B_1, B_2 \neq \emptyset).$$

If $AX_1 = B_1$ and $AX_2 = B_2$, then

$$A(X_1 + X_2) = AX_1 + AX_2 = B_1 + B_2 = B$$

The sum of “local” solutions is a “global” solution:

$$\mathrm{Sol}(A, B_1) + \mathrm{Sol}(A, B_2) \subseteq \mathrm{Sol}(A, B).$$

Important property: If $L_{A,B_1} \cap L_{A,B_2} = \emptyset$ then we have a perfect split:

$$\mathrm{Sol}(A, B_1) + \mathrm{Sol}(A, B_2) = \mathrm{Sol}(A, B)$$
$$\mathrm{sol}(A, B_1) \cdot \mathrm{sol}(A, B_2) = \mathrm{sol}(A, B)$$

Instance split

$$A = C_2 \qquad \begin{aligned} B &= 2C_2 + 2C_{10} \\ B_1 &= 2C_2 \\ B_2 &= 2C_{10} \end{aligned} \qquad \begin{aligned} L_{A,B} &= \{1, 2, 5, 10\} \\ L_{A,B_1} &= \{1, 2\} \\ L_{A,B_2} &= \{5, 10\} \end{aligned}$$

Instance split

$$A = C_2 \qquad \begin{aligned} B &= 2C_2 + 2C_{10} \\ B_1 &= 2C_2 \\ B_2 &= 2C_{10} \end{aligned} \qquad \begin{aligned} L_{A,B} &= \{1, 2, 5, 10\} \\ L_{A,B_1} &= \{1, 2\} \\ L_{A,B_2} &= \{5, 10\} \end{aligned}$$

$\mathrm{Sol}(A, B_1)$

$$\begin{aligned} C_2 \times (2C_1) &= 2C_2 \\ C_2 \times (\ C_2\ ) &= 2C_2 \end{aligned}$$

Instance split

$$A = C_2 \qquad \begin{aligned} B &= 2C_2 + 2C_{10} \\ B_1 &= 2C_2 \\ B_2 &= 2C_{10} \end{aligned} \qquad \begin{aligned} L_{A,B} &= \{1,2,5,10\} \\ L_{A,B_1} &= \{1,2\} \\ L_{A,B_2} &= \{5,10\} \end{aligned}$$

$\mathrm{Sol}(A, B_1)$

$$C_2 \times (2C_1) = 2C_2$$
$$C_2 \times (C_2) = 2C_2$$

$\mathrm{Sol}(A, B_2)$

$$C_2 \times (2C_5) = 2C_{10}$$
$$C_2 \times (C_{10}) = 2C_{10}$$

Instance split

$$A = C_2 \qquad \begin{aligned} B &= 2C_2 + 2C_{10} \\ B_1 &= 2C_2 \\ B_2 &= 2C_{10} \end{aligned} \qquad \begin{aligned} L_{A,B} &= \{1,2,5,10\} \\ L_{A,B_1} &= \{1,2\} \\ L_{A,B_2} &= \{5,10\} \end{aligned}$$

$\mathrm{Sol}(A, B_1)$

$$\begin{aligned} C_2 \times (2C_1) &= 2C_2 \\ C_2 \times (C_2) &= 2C_2 \end{aligned}$$

$\mathrm{Sol}(A, B_2)$

$$\begin{aligned} C_2 \times (2C_5) &= 2C_{10} \\ C_2 \times (C_{10}) &= 2C_{10} \end{aligned}$$

$\mathrm{Sol}(A, B) = \mathrm{Sol}(A, B_1) + \mathrm{Sol}(A, B_2)$

$$\begin{aligned} C_2 \cdot (2C_1 + 2C_5) &= 2C_2 + 2C_{10} \\ C_2 \cdot (2C_1 + C_{10}) &= 2C_2 + 2C_{10} \\ C_2 \cdot (C_2 + 2C_5) &= 2C_2 + 2C_{10} \\ C_2 \cdot (C_2 + C_{10}) &= 2C_2 + 2C_{10} \end{aligned}$$

Instance split

Lemma If (A, B) is non-basic and $\gcd L_{A,B} = 1$, then (A, B) has a perfect split, which can be computed in $O(|A||B|)$.

Instance split

Lemma If (A, B) is non-basic and $\gcd L_{A,B} = 1$, then (A, B) has a perfect split, which can be computed in $O(|A||B|)$.

- If $L_{A,B} \not\subseteq \mathrm{Div}(\mathrm{lcm}\, L_A)$ then there is a prime power p^α in the factorization of $\mathrm{lcm}\, L_B$ such that $p^\alpha \nmid \mathrm{lcm}\, L_A$.

Instance split

Lemma If (A, B) is non-basic and $\gcd L_{A,B} = 1$, then (A, B) has a perfect split, which can be computed in $O(|A||B|)$.

- If $L_{A,B} \not\subseteq \mathrm{Div}(\mathrm{lcm}\, L_A)$ then there is a prime power p^α in the factorization of $\mathrm{lcm}\, L_B$ such that $p^\alpha \nmid \mathrm{lcm}\, L_A$.
- Let $B = B_1 + B_2$ where
  - B_1 contains the the cycles of B of length kp^α,
  - B_2 contains the other cycles of B.

Instance split

Lemma If (A, B) is non-basic and $\gcd L_{A,B} = 1$, then (A, B) has a perfect split, which can be computed in $O(|A||B|)$.

- If $L_{A,B} \not\subseteq \mathrm{Div}(\operatorname{lcm} L_A)$ then there is a prime power p^α in the factorization of $\operatorname{lcm} L_B$ such that $p^\alpha \nmid \operatorname{lcm} L_A$.
- Let $B = B_1 + B_2$ where
  - B_1 contains the the cycles of B of length kp^α,
    $\hookrightarrow B_1 \neq \emptyset$ since p^α appears in the factorization of $\operatorname{lcm} L_B$.
  - B_2 contains the other cycles of B.

Instance split

Lemma If (A, B) is non-basic and $\gcd L_{A,B} = 1$, then (A, B) has a perfect split, which can be computed in $O(|A||B|)$.

- If $L_{A,B} \not\subseteq \mathrm{Div}(\mathrm{lcm}\, L_A)$ then there is a prime power p^α in the factorization of $\mathrm{lcm}\, L_B$ such that $p^\alpha \nmid \mathrm{lcm}\, L_A$.
- Let $B = B_1 + B_2$ where
  - B_1 contains the the cycles of B of length kp^α,
    $\hookrightarrow B_1 \neq \emptyset$ since p^α appears in the factorization of $\mathrm{lcm}\, L_B$.
  - B_2 contains the other cycles of B.
    $\hookrightarrow B_2 \neq \emptyset$ since otherwise $p^\alpha \mid \gcd L_{A,B}$.

Instance split

Lemma If (A, B) is non-basic and $\gcd L_{A,B} = 1$, then (A, B) has a perfect split, which can be computed in $O(|A||B|)$.

- If $L_{A,B} \not\subseteq \mathrm{Div}(\mathrm{lcm}\, L_A)$ then there is a prime power p^α in the factorization of $\mathrm{lcm}\, L_B$ such that $p^\alpha \nmid \mathrm{lcm}\, L_A$.
- Let $B = B_1 + B_2$ where
  - B_1 contains the the cycles of B of length kp^α,
    $\hookrightarrow$ $B_1 \neq \emptyset$ since p^α appears in the factorization of $\mathrm{lcm}\, L_B$.
  - B_2 contains the other cycles of B.
    $\hookrightarrow$ $B_2 \neq \emptyset$ since otherwise $p^\alpha \mid \gcd L_{A,B}$.
- p^α divides each member of L_{A,B_1} and no member of L_{A,B_2}.

Instance split

Lemma If (A, B) is non-basic and $\gcd L_{A,B} = 1$, then (A, B) has a perfect split, which can be computed in $O(|A||B|)$.

- If $L_{A,B} \not\subseteq \mathrm{Div}(\operatorname{lcm} L_A)$ then there is a prime power p^α in the factorization of $\operatorname{lcm} L_B$ such that $p^\alpha \nmid \operatorname{lcm} L_A$.
- Let $B = B_1 + B_2$ where
  - B_1 contains the the cycles of B of length kp^α,
    $\hookrightarrow$ $B_1 \neq \emptyset$ since p^α appears in the factorization of $\operatorname{lcm} L_B$.
  - B_2 contains the other cycles of B.
    $\hookrightarrow$ $B_2 \neq \emptyset$ since otherwise $p^\alpha \mid \gcd L_{A,B}$.
- p^α divides each member of L_{A,B_1} and no member of L_{A,B_2}.
  $\hookrightarrow$ $(A, B_1), (A, B_2)$ is a perfect split.

Summary

- (A, B) basic $\rightarrow$ brut force approach on the support
- (A, B) non-basic and $\gcd L_{A,B} = 1$ $\rightarrow$ perfect split

Instance reduction

Lemma Let (A, B) and $\ell = \gcd L_{A,B}$. Let (A', B') with

- A' obtained from A by replacing each $C_{k\ell}$ by ℓC_k
- B' obtained from B by replacing each $C_{k\ell}$ by C_k.

Instance reduction

Lemma Let (A, B) and $\ell = \gcd L_{A,B}$. Let (A', B') with

- A' obtained from A by replacing each $C_{k\ell}$ by ℓC_k
- B' obtained from B by replacing each $C_{k\ell}$ by C_k.

Then

- $\mathrm{sol}(A, B) = \mathrm{sol}(A', B')$
- $\operatorname{lcm} L_{A'} \mid \operatorname{lcm} L_A$
- $\gcd L_{A',B'} = 1$.

Summary

- (A, B) basic $\rightarrow$ brut force approach on the support
- (A, B) non-basic $\rightarrow$ reduction $\rightarrow$ perfect split

Main result

Theorem We can compute the number of solutions X to $AX = B$ in

$$O\left(|A||B|^2\left(\frac{|B|}{|A|}\right)^{\mathrm{div}(\mathrm{lcm} L_A)}\right).$$

Main result

Theorem We can compute the number of solutions X to $AX = B$ in

$$O\left(|A||B|^2 \left(\frac{|B|}{|A|}\right)^{\mathrm{div}(\mathrm{lcm} L_A)}\right).$$

Repeating reduction/split, we obtain in $O(|A||B|^2)$ a list of basic instances $(A_1, B_1), \ldots, (A_k, B_k)$ such that

1. $|A_i| = |A|$
2. $\mathrm{lcm}\, L_{A_i} \mid \mathrm{lcm}\, L_A$
3. $|B_1| + \cdots + |B_k| \leq |B|$
4. $\mathrm{sol}(A, B) = \prod_{i=1}^{k} \mathrm{sol}(A_i, B_i)$.

Main result

Theorem We can compute the number of solutions X to $AX = B$ in

$$O\left(|A||B|^2 \left(\frac{|B|}{|A|}\right)^{\mathrm{div}(\mathrm{lcm} L_A)}\right).$$

Repeating reduction/split, we obtain in $O(|A||B|^2)$ a list of basic instances $(A_1, B_1), \ldots, (A_k, B_k)$ such that

1. $|A_i| = |A|$
2. $\mathrm{lcm}\, L_{A_i} \mid \mathrm{lcm}\, L_A$
3. $|B_1| + \cdots + |B_k| \leq |B|$
4. $\mathrm{sol}(A, B) = \prod_{i=1}^{k} \mathrm{sol}(A_i, B_i)$.

The brut force approach on the support computes $\mathrm{sol}(A_i, B_i)$ in

$$O\left(|A_i||B_i| \left(\frac{|B_i|}{|A_i|}\right)^{\mathrm{div}(\mathrm{lcm} L_{A_i})}\right) = O\left(|A||B| \left(\frac{|B|}{|A|}\right)^{\mathrm{div}(\mathrm{lcm} L_A)}\right)$$

Conclusion and Perspectives

Given two functional digraphs A, B, complexity of deciding if $A \mid B$?

Polynomial when:

- B is a dendron. [Naquin, Gadouleau 2024]
- A, B are permutations, and A or B homogeneous [Dennunzio et al 2024+]
- A, B are permutations, A fixed. [this talk]
- A is a fixed permutation (by combining items 1 and 3). [unpublished]

Conclusion and Perspectives

Given two functional digraphs A, B, complexity of deciding if $A \mid B$?

Polynomial when:

- B is a dendron. [Naquin, Gadouleau 2024]
- A, B are permutations, and A or B homogeneous [Dennunzio et al 2024+]
- A, B are permutations, A fixed. [this talk]
- A is a fixed permutation (by combining items 1 and 3). [unpublished]

Perspectives:

- Reduce the general case to permutations. [Marius Rolland]
- Polynomial algorithm for any fixed A.
- Beat the brut force algorithm for permutations A, B, running in

$$e^{O(\sqrt{|B|/|A|})}.$$