## Finite Dynamical Systems and Divisor of Sum of Cycles

Phan Thi Ha Duong

Institute of Mathematics, Vietnam Academy of Science and Technology

November 2024 - Sophia Antipolis

## Deterministic Finite Dynamical Systems

### Definition:

- A deterministic, finite, discrete-time dynamical system is a function mapping a finite set of states to itself.
- Represented as a *functional digraph* (up to an isomorphism): a finite directed graph where each vertex has a unique out-neighbor.

### Some references:

- Alberto Dennunzio, Valentina Dorigatti, Enrico Formenti, Luca Manzoni, and Antonio E Porreca
- François Doré, Kévin Perrot, Antonio E. Porreca, Sara Riva and Marius Rolland
- Émile Naquin, Maximilien Gadouleau
- Florian Bridoux, Christophe Crespelle, Thi Ha Duong Phan, and Adrien Richard

## Algebraic Operations on Functional Digraphs

Digraph A: vertex set V(A), edge set E(A). Addition (A + B):

Disjoint union of functional digraphs A and B.

### Multiplication (AB):

- Direct product of A and B.
- ▶ Vertex set V(AB) is the Cartesian product  $V(A) \times V(B)$ .
- Edge from  $(x, y) \rightarrow (x', y')$ , if :  $x \rightarrow x'$  in A and  $y \rightarrow y'$  in B.

### Semiring Structure:

The set of functional digraphs with these operations forms a semiring.

Division Problem in Functional Digraphs

### Multiplicative Structure

### Division Problem:

Given functional digraphs A and B, does A divide B?

• Exists a solution X to AX = B?

### Complexity:

- Problem is in NP.
- General case remains open.
- Better upper bounds under certain conditions.

▲□▶ ▲□▶ ▲□▶ ▲□▶ ■ ●の00

## Structure of Functional digraph

Definition: A functional digraph A has every vertex with exactly one outgoing edge.

Components:

Cyclic Part: Collection of disjoint cycles.

### Transient Part:

- Remaining structure after removing cycles.
- Disjoint union of out-trees.

We focus on the case: each graph be a collection of disjoint cycles - called Sum of cycles

▲□▶ ▲□▶ ▲□▶ ▲□▶ ■ ●の00

## Divisors of Graphs as Sum of Cycles

### Objective:

Investigate divisors of graphs that can be represented as a sum of cycles.

### Focus Areas:

- Cycle Lengths as Powers of a Prime:
  - Initial focus on cycles where lengths are powers of the same prime number.

#### Generalization Using Recurrence:

- Employ a recurrence method.
- Based on the number of distinct prime factors in cycles.

### Sum of Cycles with One Prime Number

Ring of Polynomials on One Prime Number

Let X and Y be two sums of cycles. We define two operators, called addition and product, as follows: For sums of cycles:

$$X = x_1 C_1 + x_2 C_2 + \dots + x_m C_m,$$
  
 $Y = y_1 C_1 + y_2 C_2 + \dots + y_k C_k,$ 

**Addition**: The sum Z = X + Y is defined by

$$Z=\sum_{i=1}^m z_i C_i$$

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● ● ●

where  $z_i = x_i + y_i$ .

## Multiplication of Cycles

**Multiplication**: The product  $Z = X \cdot Y$  is defined by

$$Z = \sum_{0 \le i \le m, 0 \le j \le k} x_i y_j C_i C_j,$$

where

$$C_i C_j = \gcd(i,j) C_{\operatorname{lcm}(i,j)}.$$

We denote by n(X) the size of X, that means

$$n(X) = x_1 + 2x_2 + \cdots + mx_m.$$

◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 のへぐ

Let X be a sum of cycles where the lengths are powers of the same prime. We write X as:

$$X = x_1 C_1 + x_p C_p + x_{p^2} C_{p^2} + \dots + x_{p^m} C_{p^m}.$$

The set  $\mathbb{N}[p]$ , with the operations of addition and multiplication, forms a semiring over  $\mathbb{N}$ .

▲□▶ ▲□▶ ▲ 三▶ ▲ 三▶ 三 のへぐ

Extension: the set  $\mathbb{Q}[p]$ , with the operations of addition and multiplication, forms a ring over  $\mathbb{Q}$ .

## Algorithm to Check Divisors

#### Introduction to Divisors of Cycles

Let B be a sum of cycles, each of length being a power of the same prime p:

$$B = b_1 C_1 + b_{p^{\alpha_1}} C_{p^{\alpha_1}} + b_{p^{\alpha_2}} C_{p^{\alpha_2}} + \ldots + b_{p^{\alpha_k}} C_{p^{\alpha_k}}$$

▲ロ ▶ ▲周 ▶ ▲ 国 ▶ ▲ 国 ▶ ● の Q @

Conditions:

▶ 
$$0 = \alpha_0 < \alpha_1 < \alpha_2 < ... < \alpha_k$$
  
▶  $b_{p^{\alpha_i}} > 0$  for  $i = 1, 2, ..., k$   
▶  $b_1 \ge 0$ 

Key Question: What form must a divisor A of B take?

### Form of Divisors

#### Lemma on Forms of A and X

▶ If  $B = A \cdot X$ , then:

$$A = A_* + \sum_{i=1}^k a_{p^{\alpha_i}} C_{p^{\alpha_i}}, \quad X = X_* + \sum_{i=1}^k x_{p^{\alpha_i}} C_{p^{\alpha_i}}$$

Where:

$$\mathcal{A}_{*} = \sum_{j=0}^{lpha_{1}-1} \mathsf{a}_{p^{j}} C_{p^{j}}, \quad X_{*} = \sum_{j=0}^{lpha_{1}-1} x_{p^{j}} C_{p^{j}}$$

•  $a_{p^j}, x_{p^j}$  are non-negative integers. **Two Cases**:

• If  $b_1 \neq 0$ :

$$A_* = a_1 C_1, \quad X_* = x_1 C_1 \text{ with } x_1 = \frac{b_1}{a_1}$$

If b<sub>1</sub> = 0:

$$A_* = 0$$
 or  $X_* = 0$ 

**Note**: X is called a quotient of  $\frac{B}{A}$ , different quotients X may exist.

## Lemma: Form of A and X

For all  $1 \leq l \leq k$ :

$$(a_* + \sum_{i=1}^k a_{p^{\alpha_i}} C_{p^{\alpha_i}})(x_* + \sum_{i=1}^l x_{p^{\alpha_i}} C_{p^{\alpha_i}}) = b_1 + \sum_{i=1}^l b_{p^{\alpha_i}} C_{p^{\alpha_i}}.$$

**Special Case:** If  $b_1 \neq 0$ , then  $a_* = a_1$  and  $x_* = x_1$ .

# Computing $x_{p^{\alpha_i}}$

### In all cases:

. . .

$$\begin{aligned} a_* x_* &= b_1 \\ x_{p^{\alpha_1}} &= \frac{1}{p^{\alpha_1}} \left( \frac{b_1 + p^{\alpha_1} b_{p^{\alpha_1}}}{a_* + p^{\alpha_1} a_{p^{\alpha_1}}} - x_* \right) \\ x_{p^{\alpha_2}} &= \frac{1}{p^{\alpha_2}} \left( \frac{b_1 + \sum_{i=1}^2 p^{\alpha_i} b_{p^{\alpha_i}}}{a_* + \sum_{i=1}^2 p^{\alpha_i} a_{p^{\alpha_i}}} - \frac{b_1 + p^{\alpha_1} b_{p^{\alpha_1}}}{a_* + p^{\alpha_1} a_{p^{\alpha_1}}} \right) \end{aligned}$$

$$x_{p^{\alpha_k}} = \frac{1}{p^{\alpha_k}} \left( \frac{b_1 + \sum_{i=1}^k p^{\alpha_i} b_{p^{\alpha_i}}}{a_* + \sum_{i=1}^k p^{\alpha_i} a_{p^{\alpha_i}}} - \frac{b_1 + \sum_{i=1}^{k-1} p^{\alpha_i} b_{p^{\alpha_i}}}{a_* + \sum_{i=1}^{k-1} p^{\alpha_i} a_{p^{\alpha_i}}} \right).$$

◆□ ▶ ◆□ ▶ ◆ 臣 ▶ ◆ 臣 ▶ ○ 臣 ○ のへで

Uniqueness and Non-negativity of  $x_{p^{\alpha_i}}$  (for i = 2, ..., k)

• 
$$x_{p^{\alpha_i}} = \frac{Q_i - Q_{i-1}}{p^{\alpha_i}}$$
  
uniquely determined and non-negative iff: condition (\*):

$$Q_{i-1} = \frac{b_1 + p^{\alpha_1} b_{p^{\alpha_1}} + \ldots + p^{\alpha_{i-1}} b_{p^{\alpha_{i-1}}}}{a_* + p^{\alpha_1} a_{p^{\alpha_1}} + \ldots + p^{\alpha_{i-1}} a_{p^{\alpha_{i-1}}}} \equiv \frac{n(B)}{n(A)} \mod p^{\alpha_i}$$
$$Q_i \ge Q_{i-1}$$

•  $Q_1, Q_2, \ldots, Q_k$  satisfying (\*): suitable sequence.

#### Other Variables:

- ▶ Variables  $x_j$  with  $j \le p^{\alpha_1}$  depend on  $a_*, a_{p^{\alpha_1}}, b_1, b_{p^{\alpha_1}}$ .
- There may be no solution, one solution, or multiple solutions for these variables.

### Number of solutions

#### Solve the First Equation

- If  $a_* \neq 0$ , then the solution is unique.
- If a<sub>\*</sub> = 0, then all x<sub>p<sup>α<sub>i</sub></sub> for i ≥ 2 are already determined. For the first variables, solve the equation:</sub></sup>

$$x_1 + px_p + p^2 x_{p^2} + \ldots + p^{\alpha_1 - 1} x_{p^{\alpha_1 - 1}} + x_{p^{\alpha_1}} p^{\alpha_1} = \frac{b_{p^{\alpha_1}}}{a_{p^{\alpha_1}}}.$$

• There are  $s\left(\frac{b_p\alpha_1}{a_p\alpha_1}, p, \alpha_1\right)$  solutions, where s(n, p, k) is the number of solutions of the equation:

$$x_1 + px_p + p^2 x_{p^2} + \ldots + p^{k-1} x_{p^{k-1}} + x_{p^k} p^k = n.$$

▲□▶▲□▶▲□▶▲□▶ = のへの

Theorem: Algorithm for Divisibility in Case of single prime

#### Theorem

Let  $B = b_1 C_1 + b_{p^{\alpha_1}} C_{p^{\alpha_1}} + b_{p^{\alpha_2}} C_{p^{\alpha_2}} + \ldots + b_{p^{\alpha_k}} C_{p^{\alpha_k}}$ . Let A be a sum of cycles. There exists an algorithm with a time complexity of  $O(k^2 + \alpha_1)$  to determine if A divides B. This algorithm also describes all quotients  $X = \frac{B}{A}$ .

A D N A 目 N A E N A E N A B N A C N

Example 1: Finding Solutions for XEquation: AX = B

$$A = 2C_3 + C_9, \quad B = 80C_3 + 40C_9$$

### Solution:

By Lemma 3, X is of the form:

$$X = x_1 C_1 + x_3 C_3 + x_9 C_9$$

System of equations:

$$x_1 + 3x_3 = \frac{80}{2} = 40,$$
  
$$x_9 = \frac{1}{9} \left( \frac{3 \times 80 + 9 \times 40}{3 \times 2 + 9} - \frac{800}{2} \right) = 0$$

There are 14 solutions with x<sub>3</sub> ranging from 0 to 13, satisfying:

$$x_1 + 3x_3 = 40$$

 $\blacktriangleright X = x_1C_1 + x_3C_3$ 

Example 2: Finding Solutions for Y

**Equation:** AY = B

 $A = 32 + 8C_3 + 4C_9, \quad B = 576 + 704C_3 + 192C_9$ 

#### Solution:

▶ By Lemma 3, Y is of the form:

$$Y = y_1 C_1 + y_3 C_3 + y_9 C_9$$

System of equations:

$$y_1 = \frac{576}{32} = 18,$$
  

$$y_1 + 3y_3 = \frac{576 + 3 \times 704}{32 + 8 \times 3} = 48,$$
  

$$y_9 = \frac{1}{9} \left( \frac{576 + 3 \times 704 + 9 \times 192}{32 + 8 \times 3 + 4 \times 9} - 48 \right) = 0$$

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● ● ●

## General Sum of Cycles

#### Theorem

Let B be a general sum of cycles. Let A be a sum of cycles. There exists an algorithm to determine whether A is a divisor of B. In the affirmative case, the algorithm also describes all divisors X such that  $A \cdot X = B$ .

▲ロ ▶ ▲周 ▶ ▲ 国 ▶ ▲ 国 ▶ ● の Q @

## Semiring of Multi Variables

**Definition:** Let  $p_1, p_2, ..., p_k$  be k distinct prime numbers. Define  $\mathbb{N}[p_1, p_2, ..., p_k]$  (or  $\mathbb{Q}[p_1, p_2, ..., p_k]$ ) as the set of sums of cycles X of the form:

$$X = \sum_{0 \le i_1, i_2, \dots, i_k} x_{i_1, i_2, \dots, i_k} C_{p_1^{i_1}} C_{p_2^{i_2}} \dots C_{p_k^{i_k}}$$

where  $x_{i_1,i_2,...,i_k}$  are coefficients in  $\mathbb{N}$  (or  $\mathbb{Q}$ ).

**Operators:** Addition and Multiplication are well-defined over these sets.

**Extension:** The semiring  $\mathbb{N}[p_1, p_2, \dots, p_k, p_{k+1}]$  can be viewed as:

 $\mathbb{N}[p_1, p_2, \ldots, p_k][p_{k+1}]$ 

## Algorithm for *m* Primes

- 1. Determine the semiring of polynomials:
  - Let  $p_1, \ldots, p_m$  be the primes in the cycle lengths of *B*.
  - Write B and A in  $\mathbb{N}[p_1, p_2, \dots, p_m]$ .
  - If m = 0 or m = 1, apply the algorithm for the single case.
  - Otherwise, continue to Step 2.
- 2. If  $m \ge 2$  and the algorithm for m-1 primes has been solved:
  - Let k = m 1, express B and A in  $\mathbb{N}[p_1, p_2, \dots, p_k][p]$ , where  $p = p_m$ .
  - Find X such that  $B = A \times X$ :

$$B = b_0 C_1 + \sum_i b_{p^{\alpha_i}} C_{p^{\alpha_i}}$$

$$A = A_* + \sum_i a_{p^{\alpha_i}} C_{p^{\alpha_i}}, \quad X = X_* + \sum_i x_{p^{\alpha_i}} C_{p^{\alpha_i}}$$

with  $b_i, a_i, x_i \in \mathbb{N}[p_1, p_2, \ldots, p_k]$ .

## Find the Suitable Sequence $Q_i$

#### Challenge: The $Q_i$ may not be unique.

• Compute the quotient  $Q_k = \frac{n(B)}{n(A)}$  in  $\mathbb{N}[p_1, p_2, \dots, p_k]$ , using Algorithm for k primes.

$$Q_k = \frac{n(B)}{n(A)} = \frac{b_1 + p^{\alpha_1}b_{\alpha_1} + \dots + p^{\alpha_k}b_{\alpha_k}}{a_* + p^{\alpha_1}a_{\alpha_1} + \dots + p^{\alpha_k}a_{\alpha_k}}$$

• Let  $S_k$  be the set of all possible quotients  $Q_k$ .

For each i = k - 1, k - 2, ..., 2, 1, find all suitable elements:

$$Q_{i} = \frac{b_{1} + p^{\alpha_{1}}b_{p^{\alpha_{1}}} + \dots + p^{\alpha_{i}}b_{p^{\alpha_{i}}}}{a_{*} + p^{\alpha_{1}}a_{p^{\alpha_{1}}} + \dots + p^{\alpha_{i}}a_{p^{\alpha_{i}}}}$$

- Check the suitable conditions:
  - ▶ If there exists  $Q_k$  in  $S_k$  such that  $Q_i \equiv Q_k \mod p^{\alpha_{i+1}}$ , and

・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・

▶ If there exists  $Q_{i+1}$  marked by  $Q_k$  such that  $Q_i \leq Q_{i+1}$ .

## Find the Suitable Sequence (continued)

- 1. Check the suitable conditions:
  - ▶ If there exists  $Q_k$  in  $S_k$  such that  $Q_i \equiv Q_k \mod p^{\alpha_{i+1}}$ , and
  - ▶ If there exists  $Q_{i+1}$  marked by  $Q_k$  such that  $Q_i \leq Q_{i+1}$ .
- 2. If  $Q_i$  satisfies these two conditions, then mark  $Q_i$  by  $Q_k$ .
- 3. Add  $Q_i$  to  $S_i$ .
- 4. Delete all elements in  $S_k$  that are not used to make any  $Q_i$  in this step.

#### From suitable sequences to solutions.

- ► After Step 2.2, we obtain S<sub>1</sub>, containing all Q<sub>1</sub> which have a suitable list (Q<sub>1</sub>, Q<sub>2</sub>, Q<sub>3</sub>,..., Q<sub>k-1</sub>, Q<sub>k</sub>).
- ► For each suitable list (Q<sub>1</sub>, Q<sub>2</sub>, Q<sub>3</sub>,..., Q<sub>k-1</sub>, Q<sub>k</sub>), we have a solution:

$$\forall i \in \{1, 2, \ldots, k\}, \quad x_{p^{\alpha_i}} = \frac{Q_i - Q_{i-1}}{p^{\alpha_i}},$$

(日)((1))

which are in  $\mathbb{N}[p_1, p_2, \ldots, p_k]$ .

### Example: Find X such that $A \cdot X = B$

Given:

$$B = 72C_8 + 80C_{12} + 48C_{24} + 40C_{36} + 4C_{72},$$
  
$$A = 4C_8 + 2C_{12} + C_{36}.$$

Consider p = 3, q = 2, and  $B \in \mathbb{N}[3][2]$ . Express *B* and *A* as:

$$B = (80C_3 + 40C_9)C_{2^2} + (72 + 48C_3 + 4C_9)C_{2^3},$$
  

$$A = (2C_3 + C_9)C_{2^2} + 4C_{2^3}.$$

Form of X:

$$X = y_1 C_1 + y_2 C_2 + y_4 C_{2^2} + y_8 C_{2^3},$$

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● ● ●

where  $y_1, y_2, y_4, y_8 \in \mathbb{N}[3]$ .

Example (continued): Using the Algorithm

Using the algorithm:

$$y_1 + 2y_2 + 4y_4 = \frac{80C_3 + 40C_9}{2C_3 + C_9},$$
$$y_8 = \frac{1}{8} \left( \frac{576 + 704C_3 + 192C_9}{32 + 8C_3 + 4C_9} - \frac{80C_3 + 40C_9}{2C_3 + C_9} \right).$$

First compute:

$$\frac{576 + 704C_3 + 192C_9}{32 + 8C_3 + 4C_9} = 18C_1 + 10C_3.$$

Then:

$$y_1 + 2y_2 + 4y_4 = \frac{80C_3 + 40C_9}{2C_3 + C_9} = r_1C_1 + r_3C_3,$$

▲□▶ ▲□▶ ▲ 三▶ ▲ 三▶ 三 のへぐ

with  $r_1 + 3r_3 = 40$ .

## Example (continued): Solutions

Compute *y*<sub>8</sub>:

$$y_8 = \frac{1}{8}(18C_1 + 10C_3 - (r_1 + r_3C_3)) = \frac{18 - r_1}{8} + \frac{10 - r_3}{8}C_3,$$

where  $r_1 + 3r_3 = 40$ . Since  $y_8$  must have non-negative integer coefficients:

$$r_3 = 10, \quad r_1 = 10, \quad y_8 = 1.$$

Number of solutions:

 $y_1+2y_2+4y_4 = 10C_1+10C_3$ ,  $f(10,2,2) = 12 \Rightarrow 144$  solutions.

Example solutions:

• 
$$y_4 = C_1 + C_3, y_2 = C_1, y_1 = 4C_1 + 6C_3$$
  
•  $y_4 = 2C_1 + C_3, y_2 = 2C_3, y_1 = 2C_1 + 2C_3$   
•  $y_4 = 2C_1, y_2 = 5C_3, y_1 = 2C_1$ 

Complexity of Algorithms. Algorithm for Single Prime

**Step 1:** Takes *O*(1) time.

Step 2: For each i, it takes O(k) time.

**Step 3:** To describe all solutions, it takes O(1) time.

**Total Complexity:**  $O(k^2)$  time for a single prime.

**Number of Solutions:**  $s\left(\frac{b_{\rho}\alpha_1}{a_{\rho}\alpha_1}, p, \alpha_1\right)$ , where s(n, p, k): number of solutions of:

$$x_1 + px_p + p^2 x_{p^2} + \ldots + p^{k-1} x_{p^{k-1}} + x_{p^k} p^k = n.$$

・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・

**Time to list Solutions:**  $k \cdot s(n, p, k)$  time.

## Current and Future Tasks:

- Analyze algorithm complexity for the general case.
- Calculate the number of solutions.
- Find divisors of a given sum of cycles.
- Determine when X is a prime.
- Determine when *X* is irreducible.

### Upper Bound for s(n, p, k)

A well-studied function initiated by Mahler.

Focus on finding the upper bound.

# Thank you for your attention!

**Theorem 1:** There exists an algorithm with a time complexity of  $O(k^2 + \alpha_1)$  to determine if *A* divides *B*, and to describe all quotients  $X = \frac{B}{A}$ . **Algorithm Steps:** 

- Step 1: Handle the first condition
- ▶ Step 2: Compute all  $x_{p^i}$  for  $i \ge 1$
- Step 3: Solve the equation

## Algorithm Complexity

**Step 1**: O(1) time. **Step 2**: For each *i*, takes O(k) time. **Step 3**: Describing all solutions takes O(1) time. There are  $s\left(\frac{b_{p}\alpha_{1}}{a_{p}\alpha_{1}}, p, \alpha_{1}\right)$  solutions. Listing all solutions takes  $k \cdot s(n, p, k)$  time.

## Lemma: Form of A and X

Lemma If  $B = A \cdot X$ , then:

$$\begin{array}{ll} A_{*}X_{*} & = b_{1}C_{1} \\ (a_{*} + a_{p^{\alpha_{1}}}C_{p^{\alpha_{1}}})(x_{*} + x_{p^{\alpha_{1}}}C_{p^{\alpha_{1}}}) & = b_{1} + b_{p^{\alpha_{1}}}C_{p^{\alpha}} \\ (a_{*} + a_{p^{\alpha_{1}}}C_{p^{\alpha_{1}}} + a_{p^{\alpha_{2}}}C_{p^{\alpha_{2}}})(x_{*} + x_{p^{\alpha_{1}}}C_{p^{\alpha_{1}}} + x_{p^{\alpha_{2}}}C_{p^{\alpha_{2}}}) & = b_{1} + b_{p^{\alpha_{1}}}C_{p^{\alpha}} \\ \cdots \end{array}$$

### Lemma: Computing X

If  $B = A \cdot X$  then

$$\begin{array}{ll} A_{*}X_{*} & =b_{1}C_{1} \\ (a_{*}+a_{p^{\alpha_{1}}}C_{p^{\alpha_{1}}})(x_{*}+x_{p^{\alpha_{1}}}C_{p^{\alpha_{1}}}) & =b_{1}+b_{p^{\alpha_{1}}}C_{p^{\alpha_{1}}} \\ (a_{*}+a_{p^{\alpha_{1}}}C_{p^{\alpha_{1}}}+a_{p^{\alpha_{2}}}C_{p^{\alpha_{2}}})(x_{*}+x_{p^{\alpha_{1}}}C_{p^{\alpha_{1}}}+x_{p^{\alpha_{2}}}C_{p^{\alpha_{2}}}) & =b_{1}+b_{p^{\alpha_{1}}}C_{p^{\alpha_{1}}}+b_{p^{\alpha_{1}}} \\ \cdots \\ (a_{*}+a_{p^{\alpha_{1}}}C_{p^{\alpha_{1}}}+\dots+a_{p^{\alpha_{k}}}C_{p^{\alpha_{k}}})(x_{*}+x_{p^{\alpha_{1}}}C_{p^{\alpha_{1}}}+\dots+x_{p^{\alpha_{k}}}C_{p^{\alpha_{k}}}) & =b_{1}+b_{p^{\alpha_{1}}}C_{p^{\alpha_{1}}}+\dots \\ \end{array}$$

If  $b_1 \neq 0$ , then it follows that  $a_* = a_1$  and  $x_* = x_1$ . In all cases:

$$\begin{aligned} a_* x_* &= b_1 \\ (a_* + p^{\alpha_1} a_{p^{\alpha_1}})(x_* + p^{\alpha_1} x_{p^{\alpha_1}}) &= b_1 + p^{\alpha_1} b_{p^{\alpha_1}} \\ (a_* + p^{\alpha_1} a_{p^{\alpha_1}} + p^{\alpha_2} a_{p^{\alpha_2}})(x_* + p^{\alpha_1} x_{p^{\alpha_1}} + p^{\alpha_2} x_{p^{\alpha_2}}) &= b_1 + p^{\alpha_1} b_{p^{\alpha_1}} + p^{\alpha_2} b_{p^{\alpha_2}} \\ \cdots \\ (a_* + p^{\alpha_1} a_{p^{\alpha_1}} + \dots + p^{\alpha_k} a_{p^{\alpha_k}})(x_* + p^{\alpha_1} x_{p^{\alpha_1}} + \dots + p^{\alpha_k} x_{p^{\alpha_k}}) &= b_1 + p^{\alpha_1} b_{p^{\alpha_1}} + \dots + p^{\alpha_k} b_{p^{\alpha_k}} \end{aligned}$$

## Computing X

Or equivalently,

$$a_{*}x_{*} = b_{1}$$

$$x_{p^{\alpha_{1}}} = \frac{1}{p^{\alpha_{1}}} \left( \frac{b_{1} + p^{\alpha_{1}}b_{p^{\alpha_{1}}}}{a_{*} + p^{\alpha_{1}}a_{p^{\alpha_{1}}}} - x_{*} \right)$$

$$x_{p^{\alpha_{2}}} = \frac{1}{p^{\alpha_{2}}} \left( \frac{b_{1} + p^{\alpha_{1}}b_{p^{\alpha_{1}}} + p^{\alpha_{2}}b_{p^{\alpha_{2}}}}{a_{*} + p^{\alpha_{1}}a_{p^{\alpha_{1}}} + p^{\alpha_{2}}a_{p^{\alpha_{2}}}} - \frac{b_{1} + p^{\alpha_{1}}b_{p^{\alpha_{1}}}}{a_{*} + p^{\alpha_{1}}a_{p^{\alpha_{1}}}} \right)$$
...

$$x_{p^{\alpha_{i}}} = \frac{1}{p^{\alpha_{i}}} \left( \frac{b_{1} + p^{\alpha_{1}}b_{p^{\alpha_{1}}} + \ldots + p^{\alpha_{i}}b_{p^{\alpha_{i}}}}{a_{*} + p^{\alpha_{1}}a_{p^{\alpha_{1}}} + \ldots + p^{\alpha_{i}}a_{p^{\alpha_{i}}}} - \frac{b_{1} + p^{\alpha_{1}}b_{p^{\alpha_{1}}} + \ldots + p^{\alpha_{i-1}}b_{p^{\alpha_{i-1}}}}{a_{*} + p^{\alpha_{1}}a_{p^{\alpha_{1}}} + \ldots + p^{\alpha_{i-1}}a_{p^{\alpha_{i-1}}}} \right)$$

$$x_{p^{\alpha_{k}}} = \frac{1}{p^{\alpha_{k}}} \left( \frac{b_{1} + p^{\alpha_{1}}b_{p^{\alpha_{1}}} + \ldots + p^{\alpha_{k}}b_{p^{\alpha_{k}}}}{a_{*} + p^{\alpha_{1}}a_{p^{\alpha_{1}}} + \ldots + p^{\alpha_{k}}a_{p^{\alpha_{k}}}} - \frac{b_{1} + p^{\alpha_{1}}b_{p^{\alpha_{1}}} + \ldots + p^{\alpha_{k-1}}b_{p^{\alpha_{k-1}}}}{a_{*} + p^{\alpha_{1}}a_{p^{\alpha_{1}}} + \ldots + p^{\alpha_{k-1}}a_{p^{\alpha_{k-1}}}} \right)$$