Complexity of the resolution of univariate polynomial equations over finite discrete dynamical systems

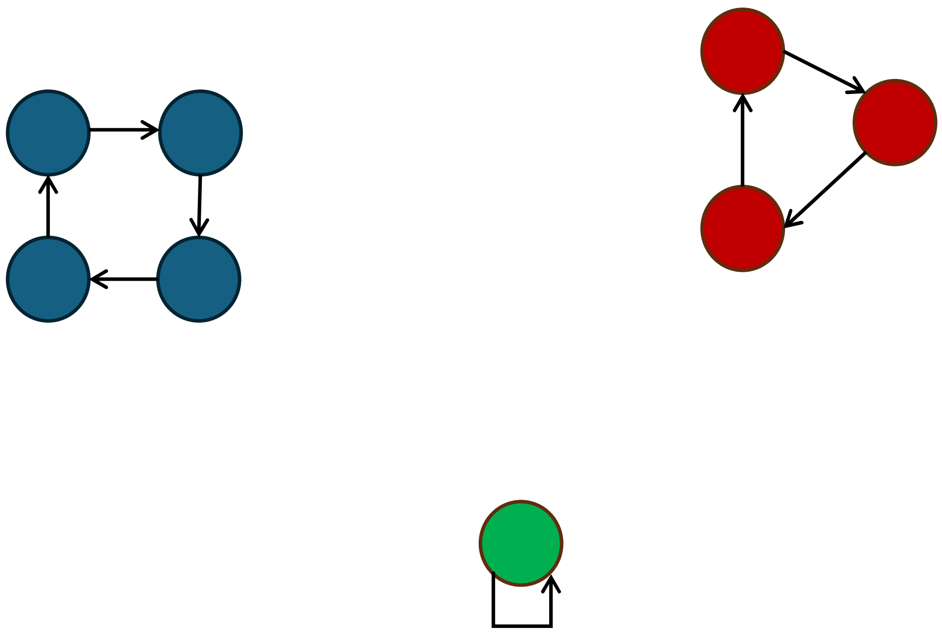
Seminar I3S
Thursday, November 14th

Marius ROLLAND,
CNRS & LIS, Marseille

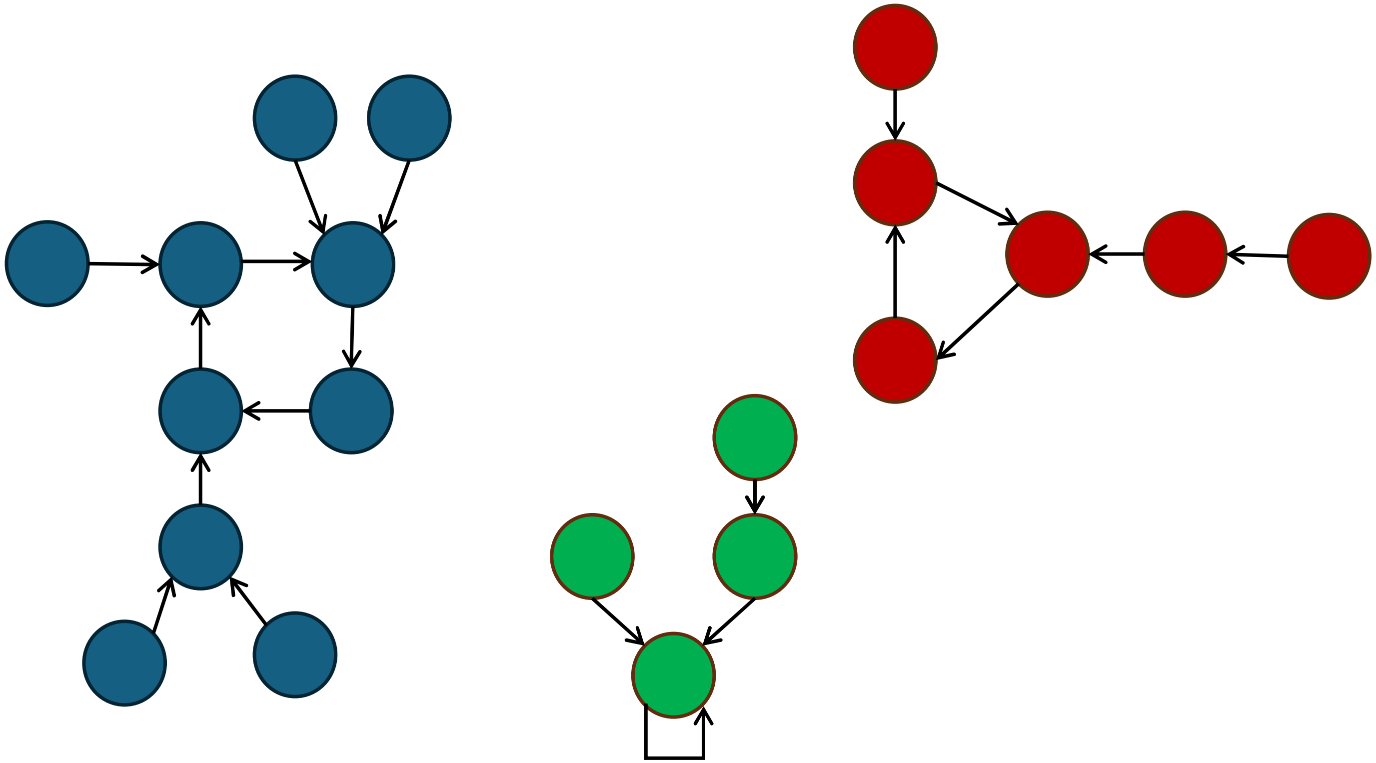
A LITTLE CONTEXT

What is a finite discrete dynamical system (FDDS) ?

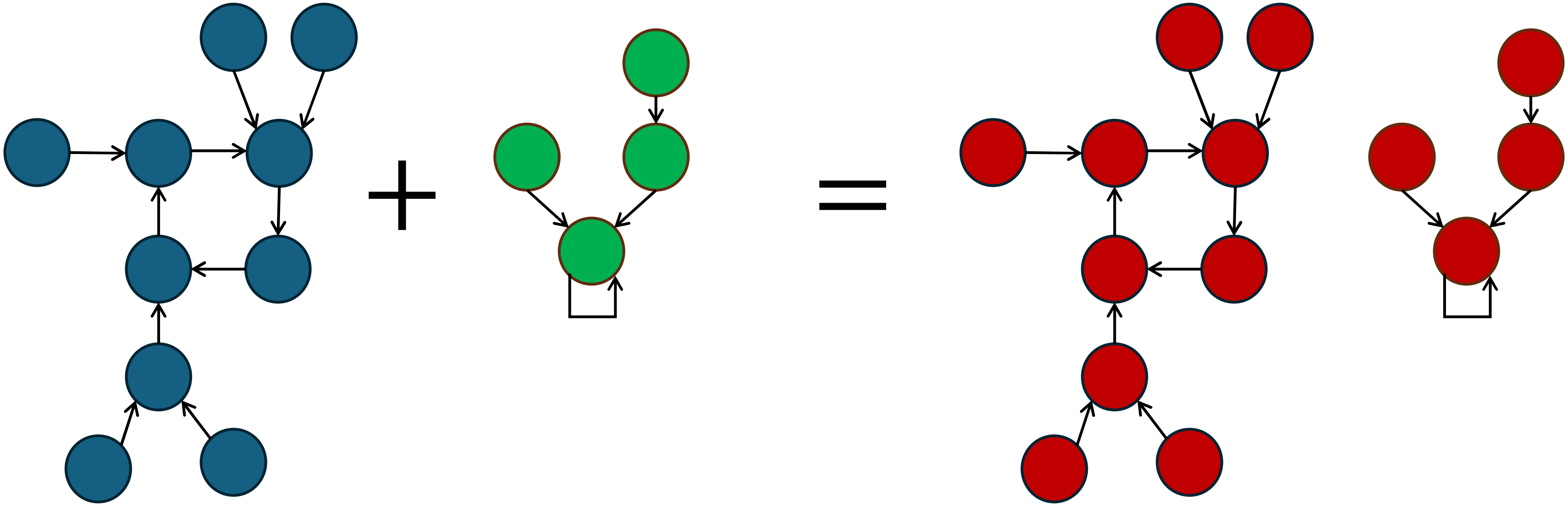
What is a finite discrete dynamical system (FDDS) ?



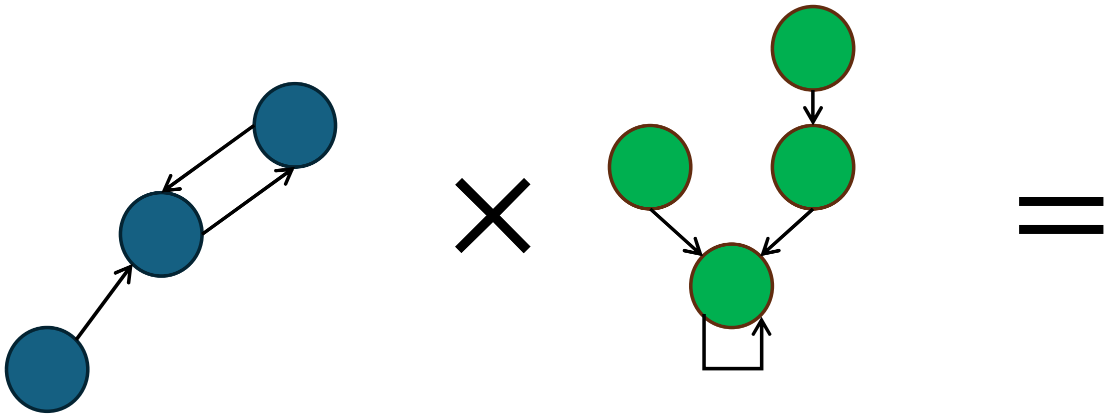
What is a finite discrete dynamical system (FDDS) ?



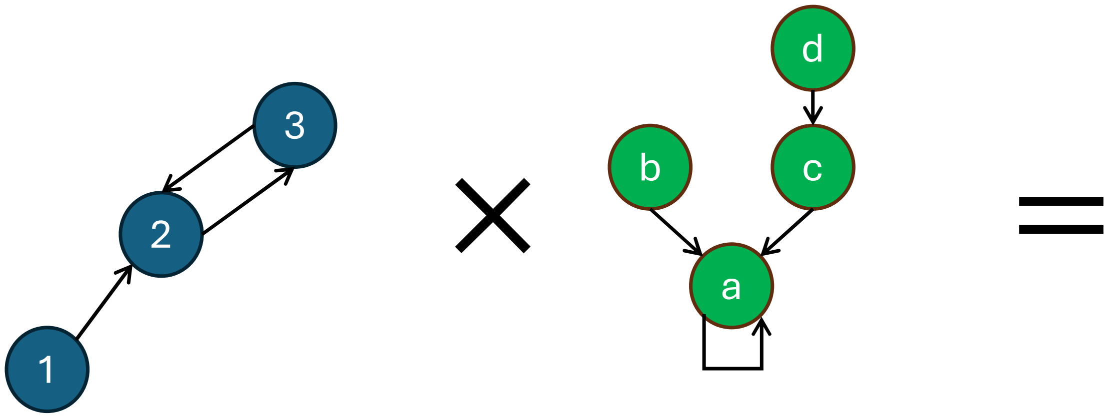
Operation : Sum



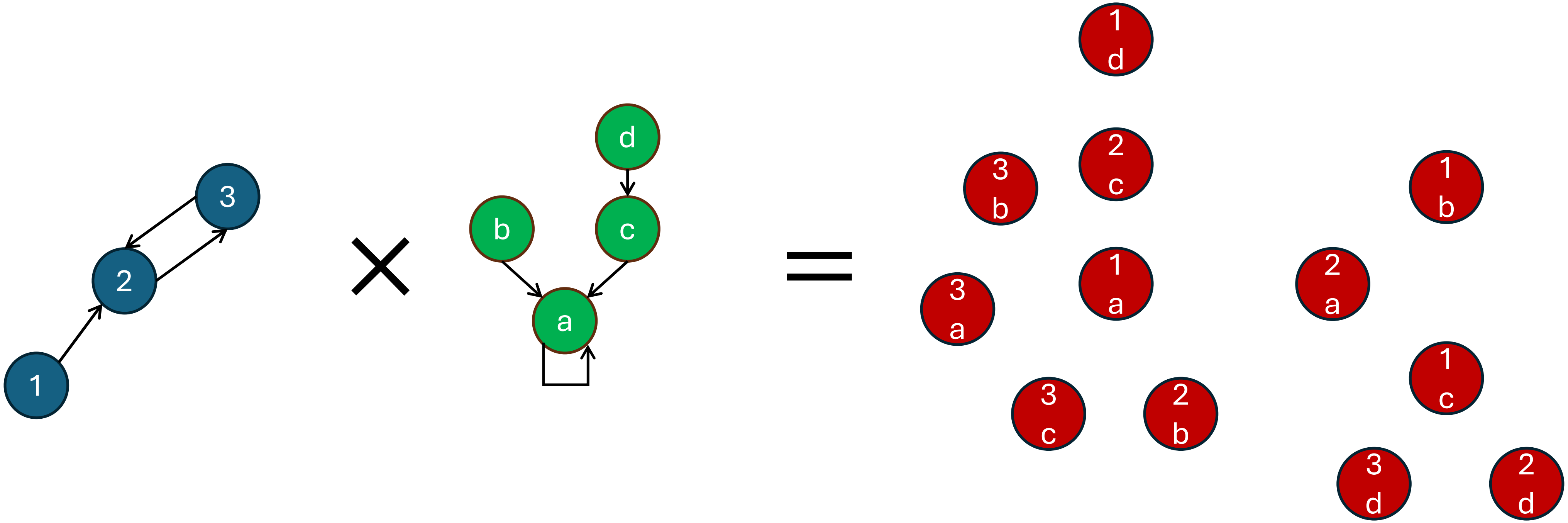
Operation : Product



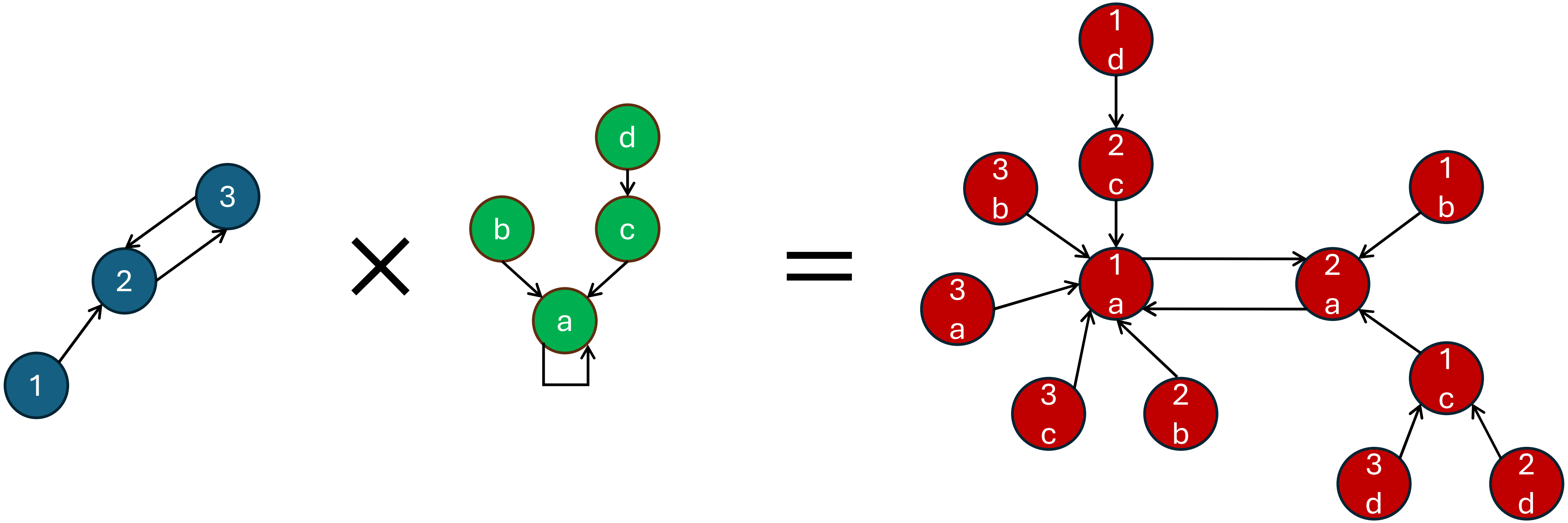
Operation : Product



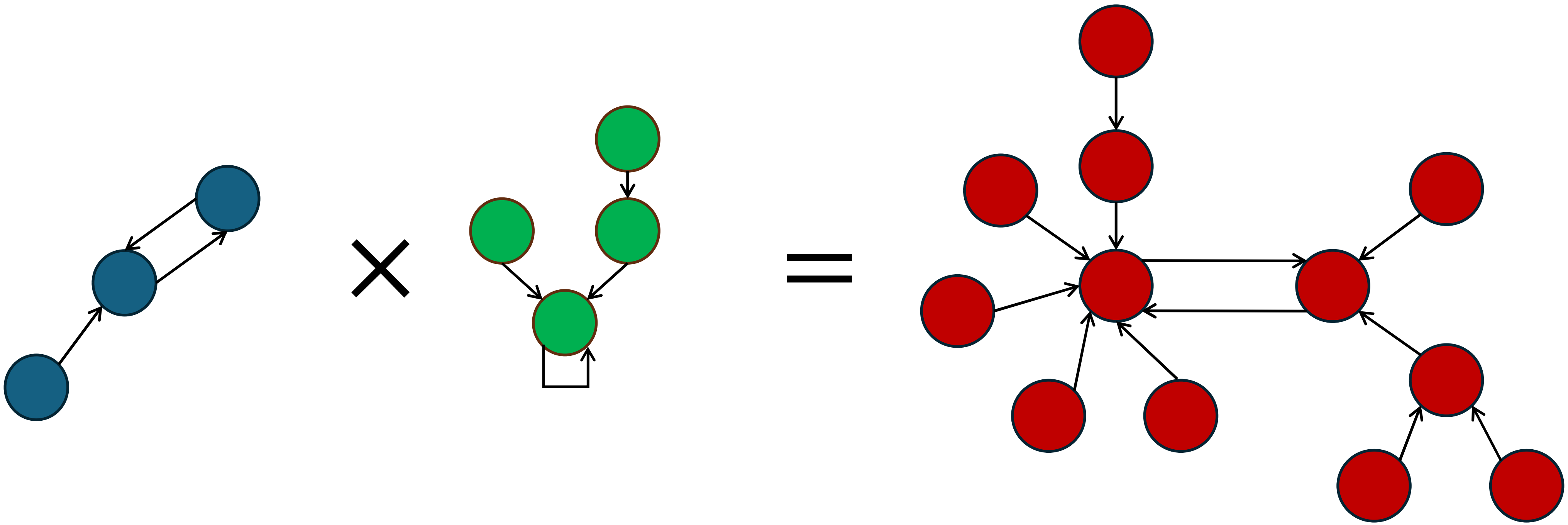
Operation : Product



Operation : Product



Operation : Product



Property of product

The product of two connected FDDS A, B with cycle lengths a, b has $gcd(a, b)$ connected components with cycle length $lcm(a, b)$.

The Semiring $(\mathbf{D}, +, \times)$

The set **D** of FDDS **up to isomorphism** with the **alternative execution** as addition and **the synchronus execution** as multiplication is a commutative semiring.

Polynomial equations over FDDS

- Undecidable in the general case : $P_1(\vec{X}) = P_2(\vec{X})$

Polynomial equations over FDDS

- Undecidable in the general case : $P_1(\vec{X}) = P_2(\vec{X})$
- NPC in general for the equation $P(\vec{X}) = \mathrm{B}$

Polynomial equations over FDDS

- Undecidable in the general case : $P_1(\vec{X}) = P_2(\vec{X})$
- NPC in general for the equation $P(\vec{X}) = \mathrm{B}$
- In P for the monomial univariate equations ($A\,X^k = B$) with connected result.

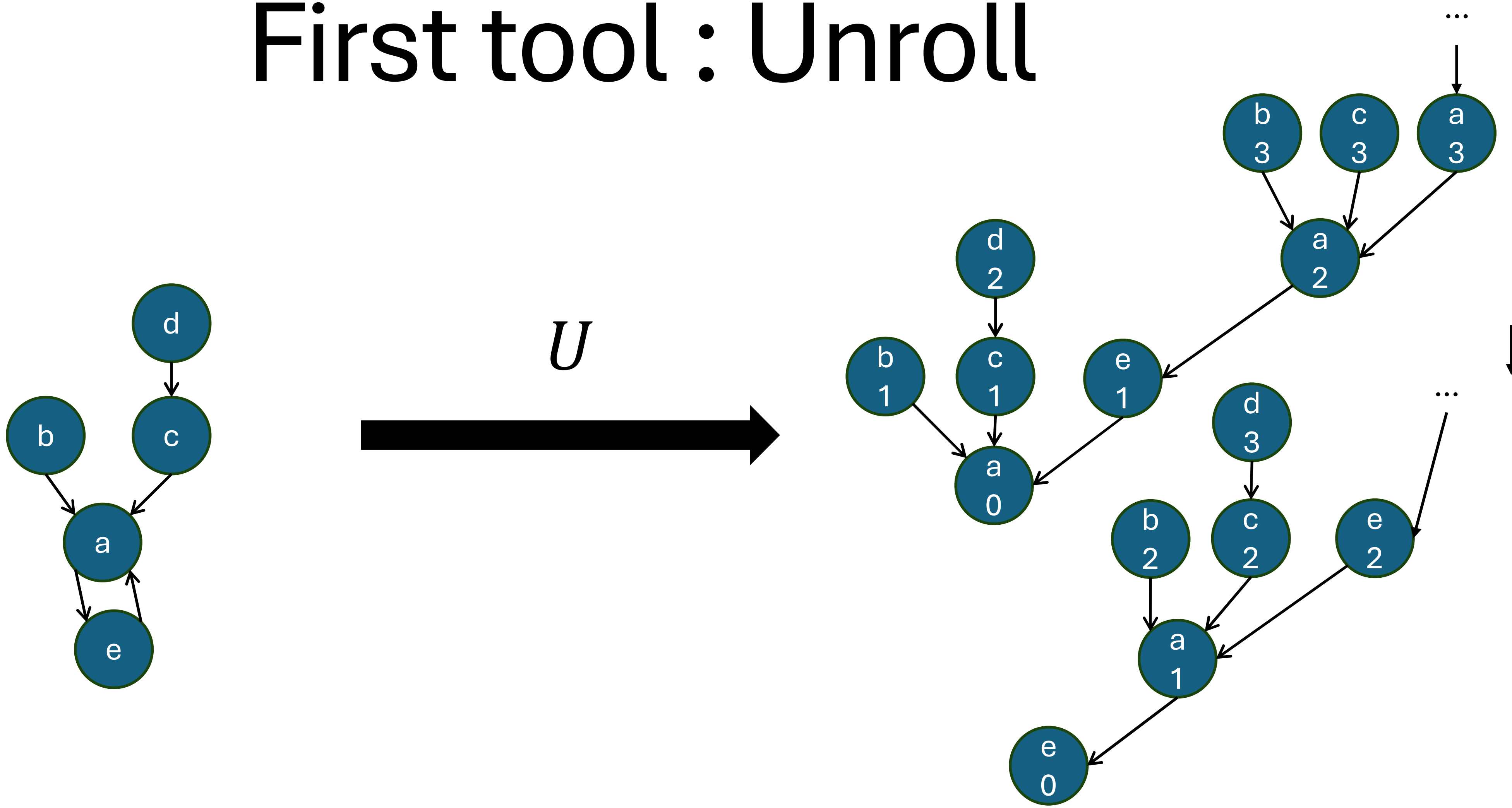
OUR NEW RESULTS

1. The behavior of transient nodes

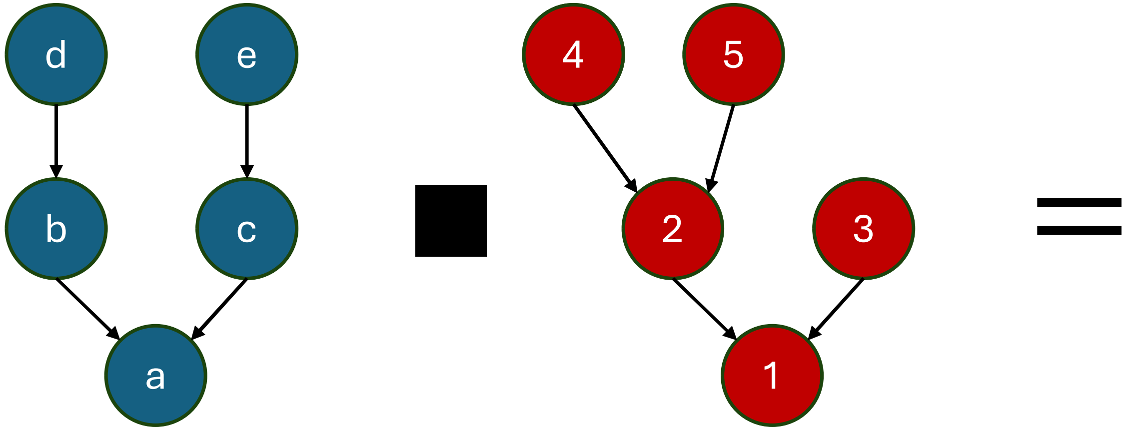
First tool : Unroll

Main idea : Transform a FDDS into a forest where each tree is rooted in a periodic nodes and represents all possible paths in the FDDS between a node and its root.

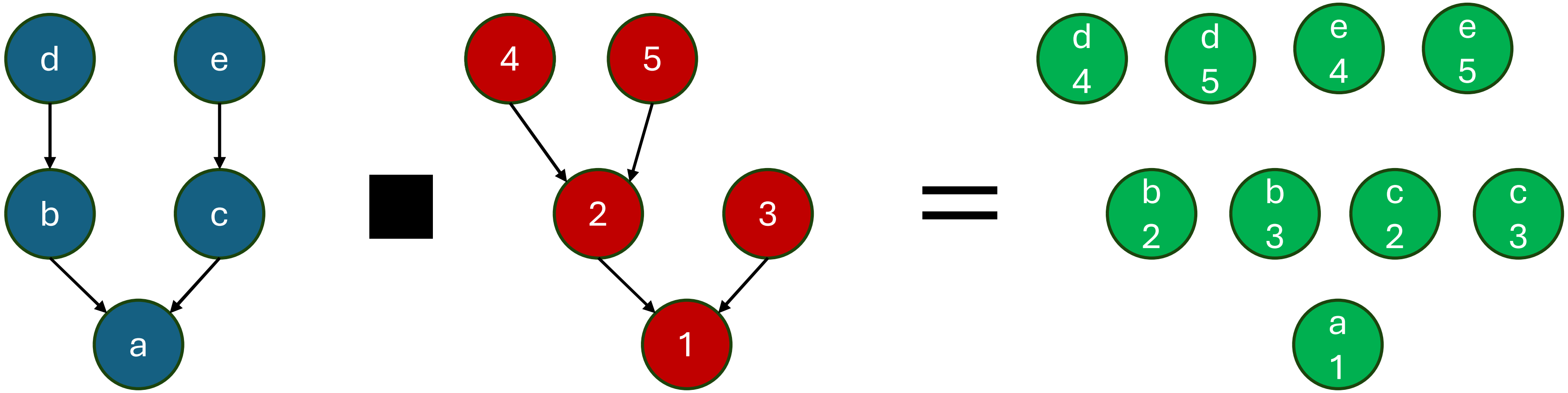
First tool : Unroll



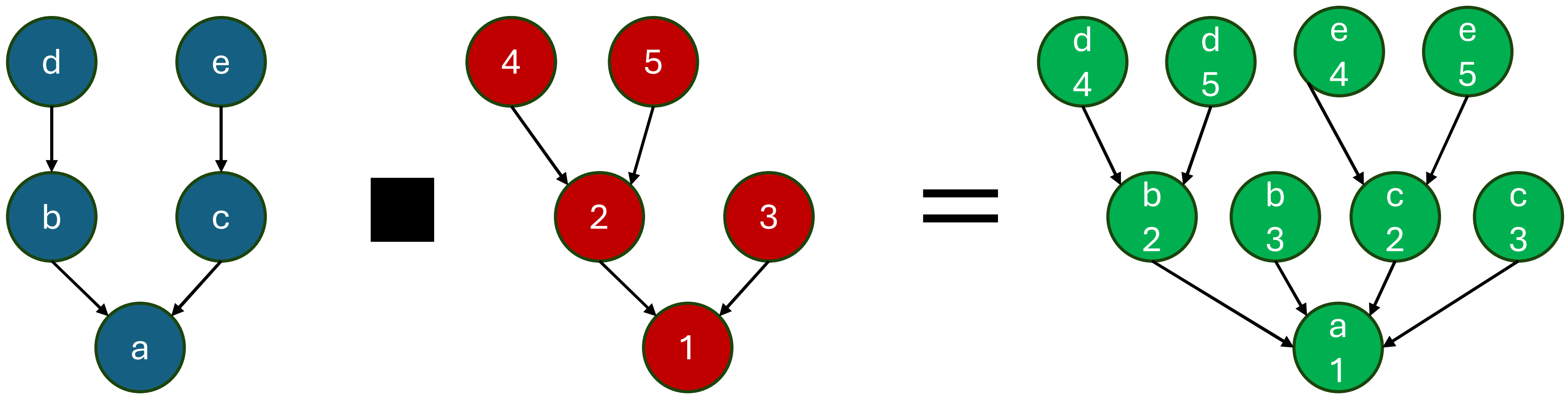
Tree product



Tree product



Tree product



The Semiring $(U(\mathbf{D}), +, \blacksquare)$

The set U(**D**) of FDDS **up to isomorphism** with the **disjoint union** as addition and the **tree product** as multiplication is a commutative semiring.

Result over Unroll:

- U is a morphisme between **D** and U(**D**) ⇒ $U\left(\sum_{i=1}^{n} A_i X^i\right) = \sum_{i=1}^{n} U(A_i)\, U(X)^i$.

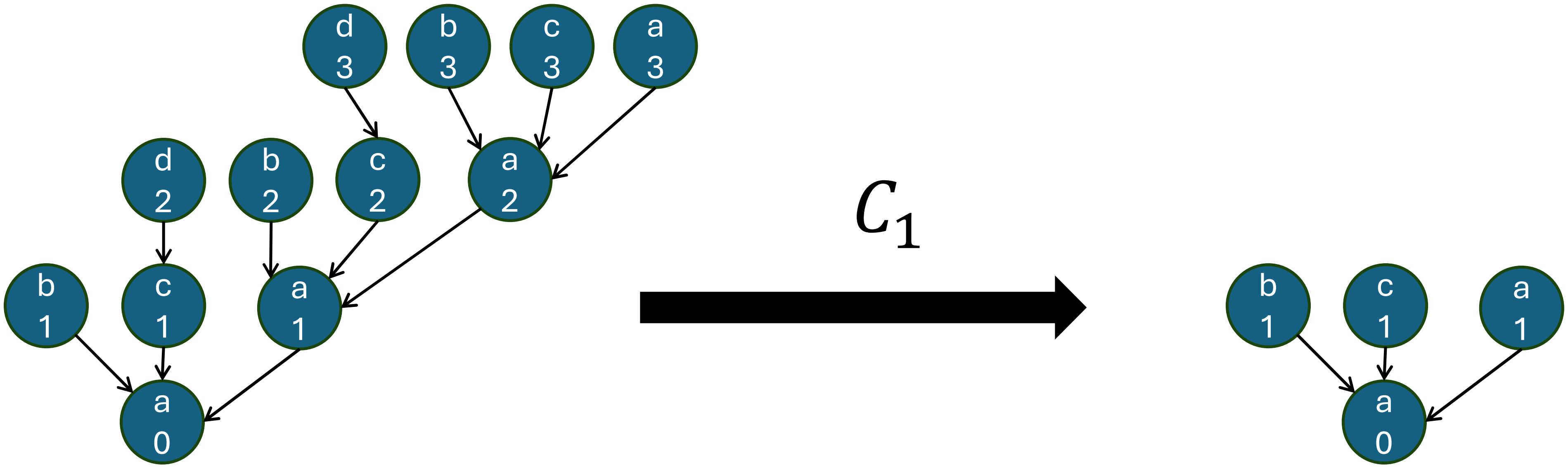
Result over Unroll:

- U is a morphisme between **D** and U(**D**) $\Rightarrow$ $U\left(\sum_{i=1}^{n} A_i X^i\right) = \sum_{i=1}^{n} U(A_i)\, U(X)^i$.
- There exists an order such that $A \leq B \Leftrightarrow A\,T \leq B\,T$ for all unroll tree A, B and T.

Second tool : Cut

Main idea : in a forest, consider only the nodes whose depth is less than a certain *n*.

Second tool : Cut



Result over Cut:

- For all integer n and FDDS A, B we have that $C_n(AB) = C_n(A)C_n(B)$.

Result over Cut:

- For all integer n and FDDS A, B we have that $C_n(AB) = C_n(A)C_n(B)$.
- There exists an integer *n* such that $\mathrm{U}\left(\sum_{i=1}^{m} A_i X^i\right) = \mathrm{U(B)} \Leftrightarrow C_n\left(\mathrm{U}\left(\sum_{i=1}^{m} A_i X^i\right)\right) = C_n(U(B))$.

Result over Cut:

- For all integer n and FDDS A, B we have that $C_n(AB) = C_n(A)C_n(B)$.
- There exists an integer *n* such that $\mathrm{U}\left(\sum_{i=1}^{m} A_i X^i\right) = \mathrm{U(B)} \Leftrightarrow C_n\left(\mathrm{U}\left(\sum_{i=1}^{m} A_i X^i\right)\right) = C_n(U(B))$.
- The previous order is such that $C_n(A) \leq C_n(B) \Leftrightarrow C_n(A)C_n(T) \leq C_n(B)C_n(T)$ for all unroll tree A, B and T.

Form of forests

Let $P = \sum_{i=1}^{m} A_i X^i$ be a polynomial over U_n and $X = \sum_{i=1}^{k} x_i$ with $x_i \leq \; x_{i+1}$. Then, there exists $i \; \in \{1, \dots, m\}$ such that :

1. The tree $\min\big(P(X)\big)$ is isomorphic to $a_1 {x_1}^i$
2. $\min(P(X) - P\big(\sum_{j=1}^{k-1} x_j)\big)$ is isomorphic to $a_1 {x_1}^{i-1} x_k$ for all $k \; \geq 2$

Where $a_1 = \; \min(A_i)$.

Proof of the assertion

- Let i such that $\min\big(P(X)\big) \in A_i X^i$.

Proof of the assertion

- Let i such that $\min(P(X)) \in A_i X^i$.
- For all j, we have that $\min(X^j) = {x_1}^j \Rightarrow \min(P(X)) \in A_i {x_1}^i$.

Proof of the assertion

- Let i such that $\min\left(P(X)\right) \in A_i X^i$.
- For all j, we have that $\min\left(X^j\right) = {x_1}^j \Rightarrow \min\left(P(X)\right) \in A_i {x_1}^i$.
- For all $a_j \in A_i$, we have that $a_1 {x_1}^i \leq a_j {x_1}^i \Rightarrow \min\left(P(X)\right) = a_1 {x_1}^i$.

Proof of the assertion

- Let i such that $\min\big(P(X)\big) \in\ A_i X^i$.
- For all j, we have that $\min\big(X^j\big) = {x_1}^j \ \Rightarrow \min\big(P(X)\big) \in\ A_i {x_1}^i$.
- For all $a_j \in\ A_i$, we have that $a_1 {x_1}^i \leq a_j {x_1}^i \ \Rightarrow \min\big(P(X)\big) =\ a_1 {x_1}^i$.
- For all j, k, we have that :

$$a_1 {x_1}^i \quad \leq \quad \min\big(A_j\big)\, {x_1}^j$$

Proof of the assertion

- Let i such that $\min(P(X)) \in A_i X^i$.
- For all j, we have that $\min(X^j) = {x_1}^j \Rightarrow \min(P(X)) \in A_i {x_1}^i$.
- For all $a_j \in A_i$, we have that $a_1 {x_1}^i \leq a_j {x_1}^i \Rightarrow \min(P(X)) = a_1 {x_1}^i$.
- For all j, k, we have that :

$$a_1 {x_1}^i \leq \min(A_j)\, {x_1}^j$$

$$\Leftrightarrow \quad a_1\, {x_1}^{i-1} \leq \min(A_j)\, {x_1}^{j-1}$$

Proof of the assertion

- Let i such that $\min\big(P(X)\big) \in A_i X^i$.
- For all j, we have that $\min\big(X^j\big) = {x_1}^j \Rightarrow \min\big(P(X)\big) \in A_i {x_1}^i$.
- For all $a_j \in A_i$, we have that $a_1 {x_1}^i \leq a_j {x_1}^i \Rightarrow \min\big(P(X)\big) = a_1 {x_1}^i$.
- For all j, k, we have that :

$$a_1 {x_1}^i \leq \min\big(A_j\big)\, {x_1}^j$$

$$\Leftrightarrow \quad a_1\, {x_1}^{i-1} \leq \min\big(A_j\big)\, {x_1}^{j-1}$$

$$\Leftrightarrow a_1 {x_1}^{i-1} x_k \leq \min\big(A_j\big)\, {x_1}^{j-1} x_k.$$

Proof of the assertion

- Let i such that $\min\big(P(X)\big) \in A_i X^i$.
- For all j, we have that $\min\big(X^j\big) = {x_1}^j \Rightarrow \min\big(P(X)\big) \in A_i {x_1}^i$.
- For all $a_j \in A_i$, we have that $a_1 {x_1}^i \leq a_j {x_1}^i \Rightarrow \min\big(P(X)\big) = a_1 {x_1}^i$.
- For all j, k, we have that :

$$
\begin{aligned}
& a_1 {x_1}^i \leq \min\big(A_j\big)\, {x_1}^j \\
\Leftrightarrow\ & a_1\, {x_1}^{i-1} \leq \min\big(A_j\big)\, {x_1}^{j-1} \\
\Leftrightarrow\ & a_1 {x_1}^{i-1} x_k \leq \min\big(A_j\big)\, {x_1}^{j-1} x_k .
\end{aligned}
$$

- for all j, we have that $\min\big(X^{j-1} x_k\big) = \min\big(X^{j-1}\big)\, x_k = {x_1}^{j-1} x_k$
- So, $\min\big(A_j\big)\, {x_1}^{j-1} x_k \leq \min\big(A_j\big)\, y x_k \leq a y x_k$, for all $y \in X^{j-1}$, $a \in A_j$.

Consequences

For all positive integer n :

1. All polynomial functions of U_n are injective (simple induction)

Consequences

For all positive integer n :

1. All polynomial functions of U_n are injective (simple induction)
2. we can solve in polynomial time $P(X) = B$ over U_n.

Consequences

For all positive integer n :

1. All polynomial functions of U_n are injective (simple induction)
2. we can solve in polynomial time $P(X) = B$ over U_n.
    1. Taking a coefficient i,

Consequences

For all positive integer n :

1. All polynomial functions of U_n are injective (simple induction)
2. we can solve in polynomial time $P(X) = B$ over U_n.
   1. Taking a coefficient i,
   2. Compute x = $\sqrt[i]{\frac{\min(B)}{\min(A_i)}}$,

Consequences

For all positive integer n :

1. All polynomial functions of U_n are injective (simple induction)
2. we can solve in polynomial time $P(X) = B$ over U_n.
   1. Taking a coefficient i,
   2. Compute x = $\sqrt[i]{\frac{\min(B)}{\min(A_i)}}$,
   3. Add to Sol the tree $\frac{\min\left(B - P(Sol)\right)}{\min(A_i)x^{i-1}}$ until $P(Sol) \not\subset B$,

Consequences

For all positive integer n :

1. All polynomial functions of U_n are injective (simple induction)
2. we can solve in polynomial time $P(X) = B$ over U_n.
    1. Taking a coefficient i,
    2. Compute x = $\sqrt[i]{\frac{\min(B)}{\min(A_i)}}$,
    3. Add to Sol the tree $\frac{\min\left(B - P(Sol)\right)}{\min(A_i)x^{i-1}}$ until $P(Sol) \not\subset B$,
    4. Return $P(Sol) = B$.

Consequences

1. We can solve in polynomial time $P(U(X)) = U(B)$ over Unroll.
2. All polynomial functions over Unroll are injective.

2. Polynomials over FDDS and algorithms

Step one: polynomials over permutations

Let k, n, m be three positive integer with $n \leq k$ and $X = X_1 + \ldots + X_k$ be an permutation such that $length(X_i) \leq length(X_{i+1})$ and $P(X) = \sum_{i=1}^{m} A_i X^i$ be a polynomial over permutation without constant term and with at least one cancellable coefficient.

Let B be a connected component of $P(X) - P(\sum_{i=1}^{n-1} X_i)$ with minimal cycle length and $p = length(B)$.

Then $length(X_n) = p$.

Step one: polynomials over permutations

1. $length(AA') = lcm\big(length(A), length(A')\big)$ for A, A' two connected FDDS.

Step one: polynomials over permutations

1. $length(AA') = lcm\big(length(A), length(A')\big)$ for A, A' two connected FDDS.
2. $a = lcm(a, 1) = lcm(a, a) \leq lcm(a, m)$ for all integers a, m greater than *1*

Step one: polynomials over permutations

1. $length(AA') = lcm\big(length(A), length(A')\big)$ for A, A' two connected FDDS.
2. $a = \; lcm(a, 1) = lcm(a, a) \leq lcm(a, m)$ for all integers a, m greater than *1* $\Rightarrow length(X_n) \; \leq length(C)$ for all connected component C of $P(X) - P(\sum_{i=1}^{n-1} X_i)$.

Step one: polynomials over permutations

1. $length(AA') = lcm\big(length(A), length(A')\big)$ for A, A' two connected FDDS.
2. $a = \ lcm(a, 1) = lcm(a, a) \leq lcm(a, m)$ for all integers a, m greater than *1* $\Rightarrow length(X_n) \ \leq length(C)$ for all connected component C of $P(X) - P(\sum_{i=1}^{n-1} X_i)$.
3. $X \ \subseteq X^i$ for all integer i greater than *1*

Step one: polynomials over permutations

1. $length(AA') = lcm\big(length(A), length(A')\big)$ for A, A' two connected FDDS.
2. $a = lcm(a, 1) = lcm(a, a) \leq lcm(a, m)$ for all integers a, m greater than *1* $\Rightarrow length(X_n) \leq length(C)$ for all connected component C of $P(X) - P(\sum_{i=1}^{n-1} X_i)$.
3. $X \subseteq X^i$ for all integer i greater than *1* $\Rightarrow X = XC_1 \subseteq P(X)$.

Step one: polynomials over permutations

$$(C_3+C_2)\, X + (C_4 + \; C_1)X^2 = 4\, C_2 + 6\, C_3 + 42\, C_4 + 4\, C_6 + 18\, C_{12}$$

Step one: polynomials over permutations

$$(C_3+C_2)\,X + (C_4 + \ C_1)X^2 = 4\,C_2 + 6\,C_3 + 42\,C_4 + 4\,C_6 + 18\,C_{12}$$

Step one: polynomials over permutations

$$(C_3+C_2)\,X + (C_4 + \;C_1)X^2 = 4\,C_2 + 6\,C_3 + 42\,C_4 + 4\,C_6 + 18\,C_{12}$$

$$Sol = C_2$$

Step one: polynomials over permutations

$$(C_3 + C_2)\, X + (C_4 + \; C_1) X^2 = 4\, C_2 + 6\, C_3 + 42\, C_4 + 4\, C_6 + 18\, C_{12}$$

$$\Updownarrow$$

$$Sol = C_2$$

$$P(X) - P(C_2\,) = 6\, C_3 + 38\, C_4 + 3\, C_6 + 4\, C_{12}$$

Step one: polynomials over permutations

$$P(X) - P(C_2) = 6\,C_3 + 28\,C_4 + 3\,C_6 + 18\,C_{12}$$

$$Sol = C_2$$

Step one: polynomials over permutations

$$P(X) - P(C_2) = 6\,C_3 + 28\,C_4 + 3\,C_6 + 18\,C_{12}$$

$$Sol = C_2 + C_3$$

Step one: polynomials over permutations

$$P(X) - P(C_2) = 6\,C_3 + 28\,C_4 + 3\,C_6 + 18\,C_{12}$$

$$Sol = C_2 + C_3$$

$$\Updownarrow$$

$$P(X) - P(C_2 + C_3) = 20\,C_4 + 11\,C_{12}$$

Step one: polynomials over permutations

$$P(X) - P(C_2 + C_3) = 20\, C_4 + 11\, C_{12}$$

$$Sol = C_2 + C_3$$

Step one: polynomials over permutations

$$P(X) - P(C_2 + C_3) = 20\, C_4 + 11\, C_{12}$$

$$Sol = C_2 + C_3 + C_4$$

Step one: polynomials over permutations

$$P(X) - P(C_2 + C_3) = 20\, C_4 + 11\, C_{12}$$

$$\Updownarrow$$

$$Sol = C_2 + C_3 + C_4$$

$$P(X) - P(C_2 + C_3 + C_4) = 0$$

Step one: polynomials over permutations

Let P be a polynomial over permutations. If at least one non-constant coefficient is cancellable then the polynomial is injective and we can solve $P(X) = B$ in polynomial time.

Step two: root

Let a, b be two integers and A, B be two connected FDDS such that $length(A) = a$ and $length(B) = b$.

Let $t_A = \min(\,U(A))$ and $t_B = \min\big(U(B)\big)$. We define the orders:

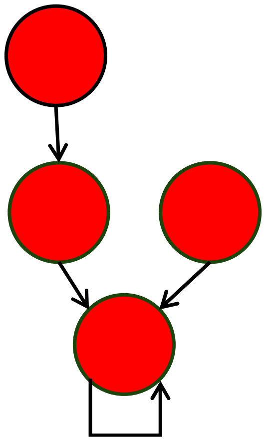
- $A \;\leq_c\; B\ if\ and\ only\ if\ \ a < b\ or\ (a = b\ and\ t_A\ \leq\ t_B)$

Step two: root

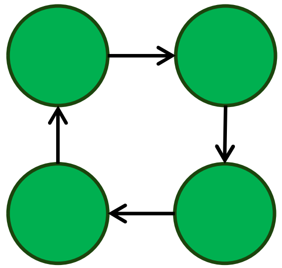
Let a, b be two integers and A, B be two connected FDDS such that $length(A) = a$ and $length(B) = b$.

Let $t_A = \min(U(A))$ and $t_B = \min\big(U(B)\big)$. We define the orders:

- $A \leq_c B$ *if and only if* $a < b$ *or* $(a = b$ *and* $t_A \leq t_B)$



$\leq_c$



Step two: root

Let a, b be two integers and A, B be two connected FDDS such that $length(A) = a$ and $length(B) = b$.

Let $t_A = \min(U(A))$ and $t_B = \min(U(B))$. We define the orders:

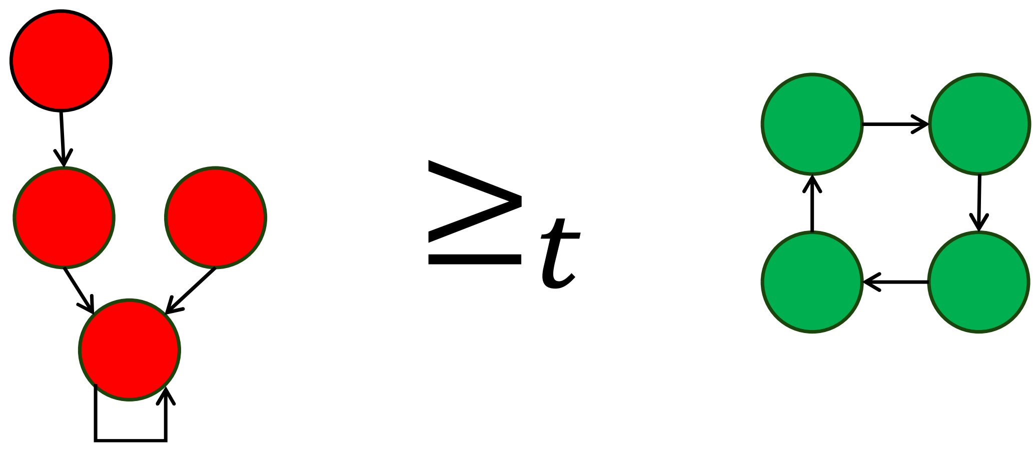
- $A \leq_c B \; if \; and \; only \; if \; a < b \; or \; (a = b \; and \; t_A \leq t_B)$
- $A \leq_t B \; if \; and \; only \; if \; t_A < t_B \; or \; (t_A = t_B \; and \; a \leq b)$

Step two: root

Let a, b be two integers and A, B be two connected FDDS such that $length(A) = a$ and $length(B) = b$.

Let $t_A = \min(U(A))$ and $t_B = \min\big(U(B)\big)$. We define the orders:

- $A \leq_c B$ *if and only if* $a < b$ *or* $(a = b$ *and* $t_A \leq t_B)$
- $A \leq_t B$ *if and only if* $t_A < t_B$ *or* $(t_A = t_B$ *and* $a \leq b)$



Step two: root

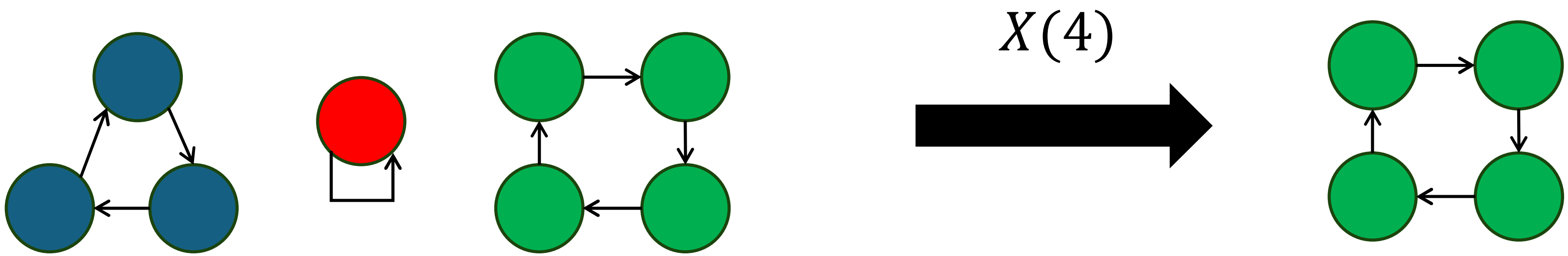
Given an FDDS X and a positive integer p, we denote by :

- $X(p)$ the multiset of connected component of X with a cycle of lenght p.

Step two: root

Given an FDDS X and a positive integer p, we denote by :

- $X(p)$ the multiset of connected component of X with a cycle of lenght p.



Step two: root

Given an FDDS X and a positive integer p, we denote by :

- $X(p)$ the multiset of connected component of X with a cycle of length p.
- $X\{p\}$ the multiset of connected component of X whose cycle length is a divisor of p.

Step two: root

Given an FDDS X and a positive integer p, we denote by :

- $X(p)$ the multiset of connected component of X with a cycle of length p.
- $X\{p\}$ the multiset of connected component of X whose cycle length is a divisor of p.

Step two: root

Let k, n, m be three positive integer with $n \leq k$ and $X = X_1 + \ldots + X_k$ be an FDDS such that $X_i \leq_c X_{i+1}$. Let B be a connected component of $\min(X^m - \left(\sum_{i=1}^{n-1} X_i\right)^m)$ according to $\leq_c$. Let $p = length(B)$.
Then B is a connected component of ${X_l}^{k-1} X_n$ with $X_l = \min(X\{p\})$ according to $\leq_t$.

Step two: root

Idea of proof :

1. The connected component B is the product of $m \; - 1$ elements of $X\{p\}$ and an element of $(X^m - \left(\sum_{i=1}^{n-1} X_i\right)^{ms})(p)$

Step two: root

Idea of proof :

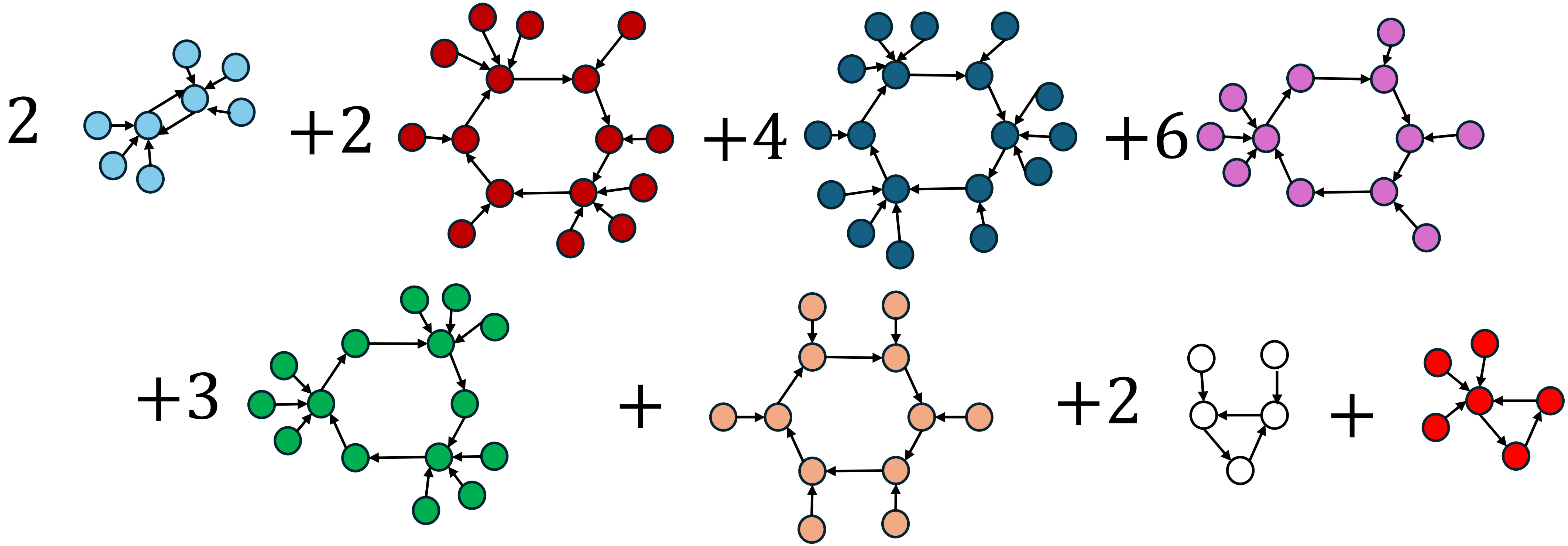
1. The connected component B is the product of $m - 1$ elements of $X\{p\}$ and an element of $(X^m - \left(\sum_{i=1}^{n-1} X_i\right)^m)(p) \Rightarrow X_n \in (X^m - \left(\sum_{i=1}^{n-1} X_i\right)^m)(p)$.

Step two: root

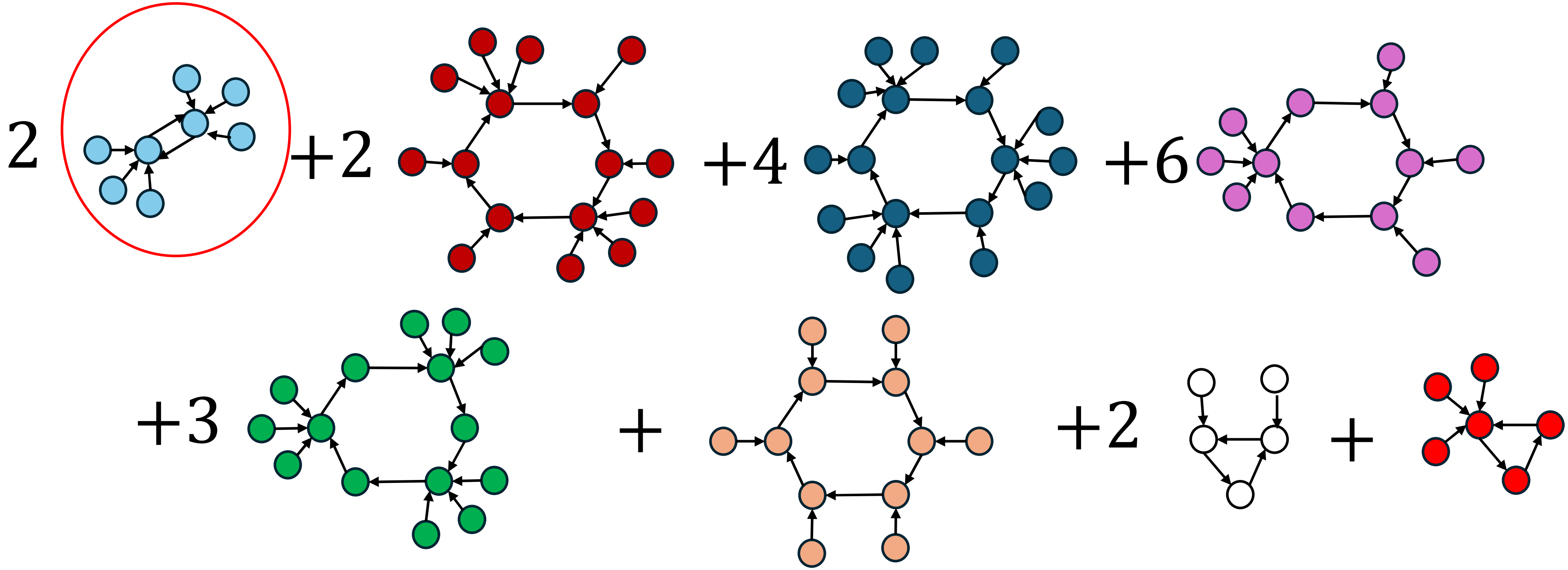
Idea of proof :

1. The connected component B is the product of $m-1$ elements of $X\{p\}$ and an element of $(X^m - \left(\sum_{i=1}^{n-1} X_i\right)^m)(p) \Rightarrow X_n \in (X^m - \left(\sum_{i=1}^{n-1} X_i\right)^m)(p)$.
2. The minimal unroll tree of B is the product of the minimal unroll tree in $X\{p\}$ raised to the power $m-1$ and the minimal unroll tree in $(X - \sum_{i=1}^{n-1} X_i)(p)$.

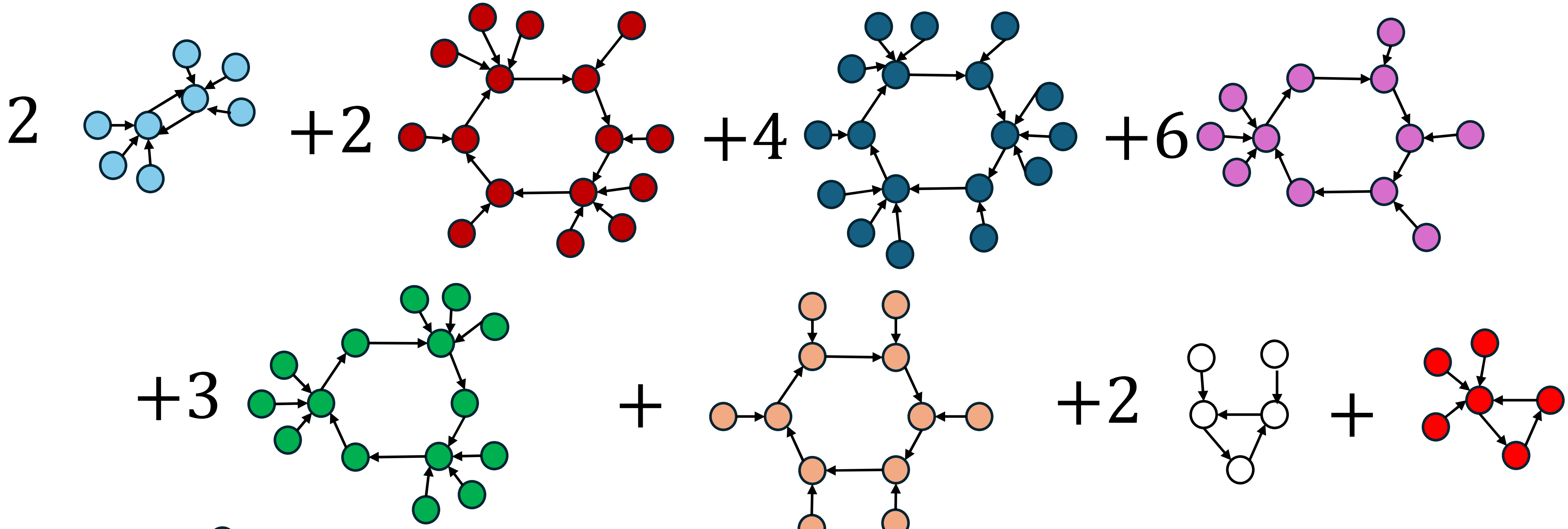
Step two: root
Example: square root

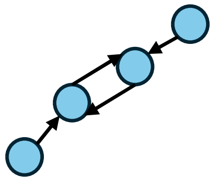


Step two: root
Example: square root

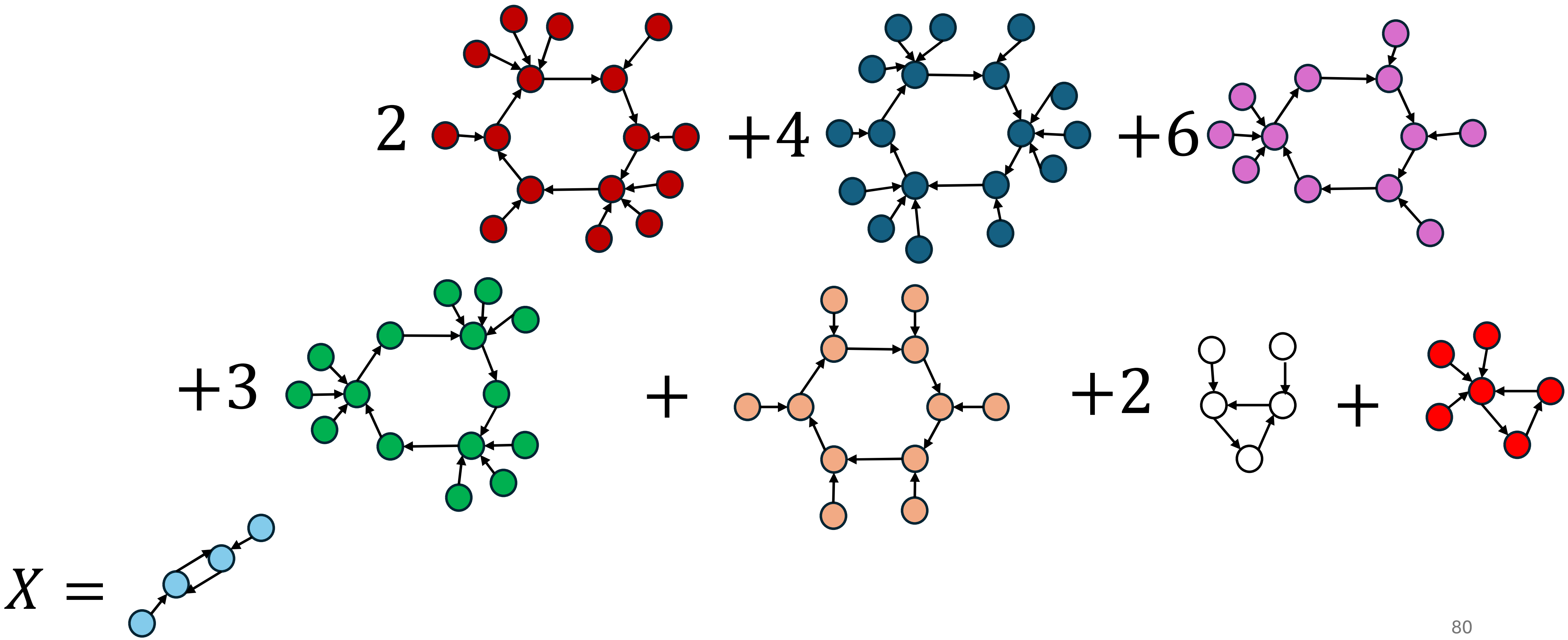


Step two: root
Example: square root

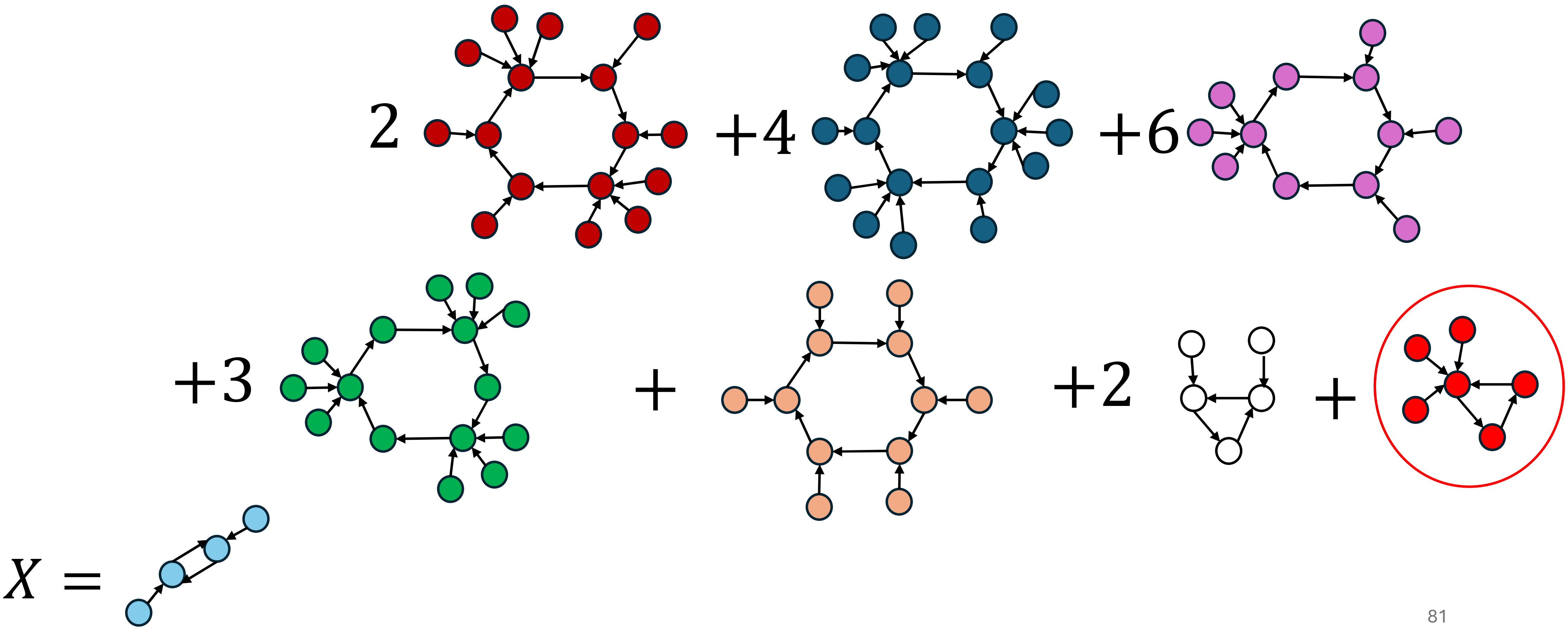


$X =$ 

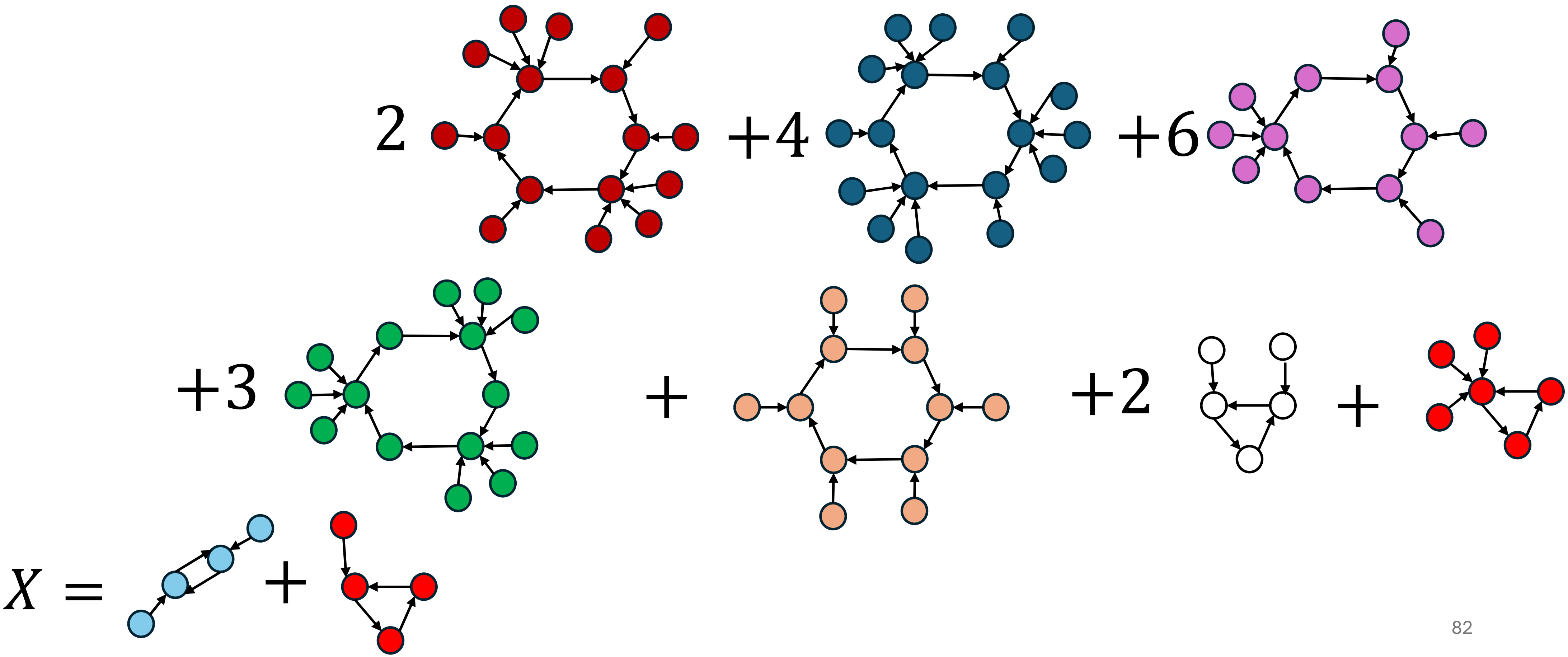
Step two: root
Example: square root



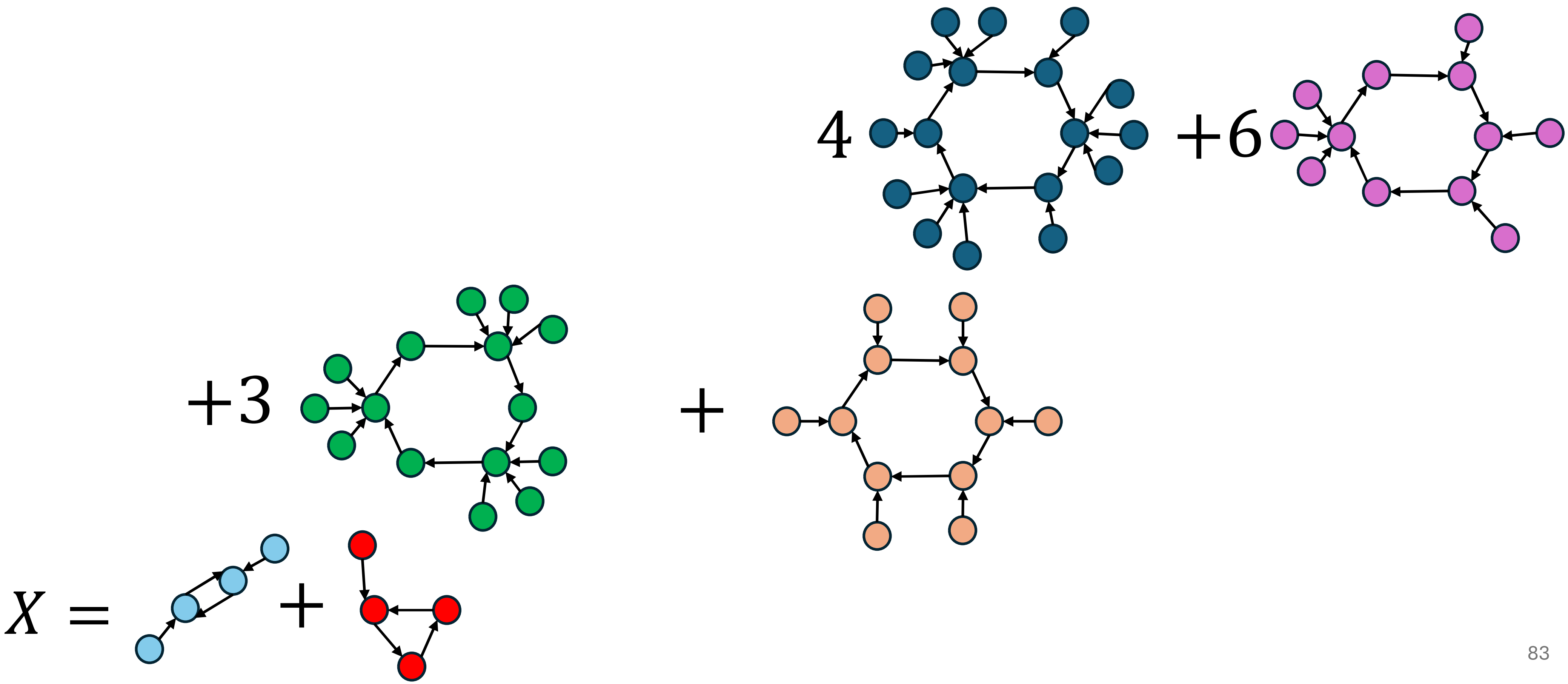
Step two: root
Example: square root



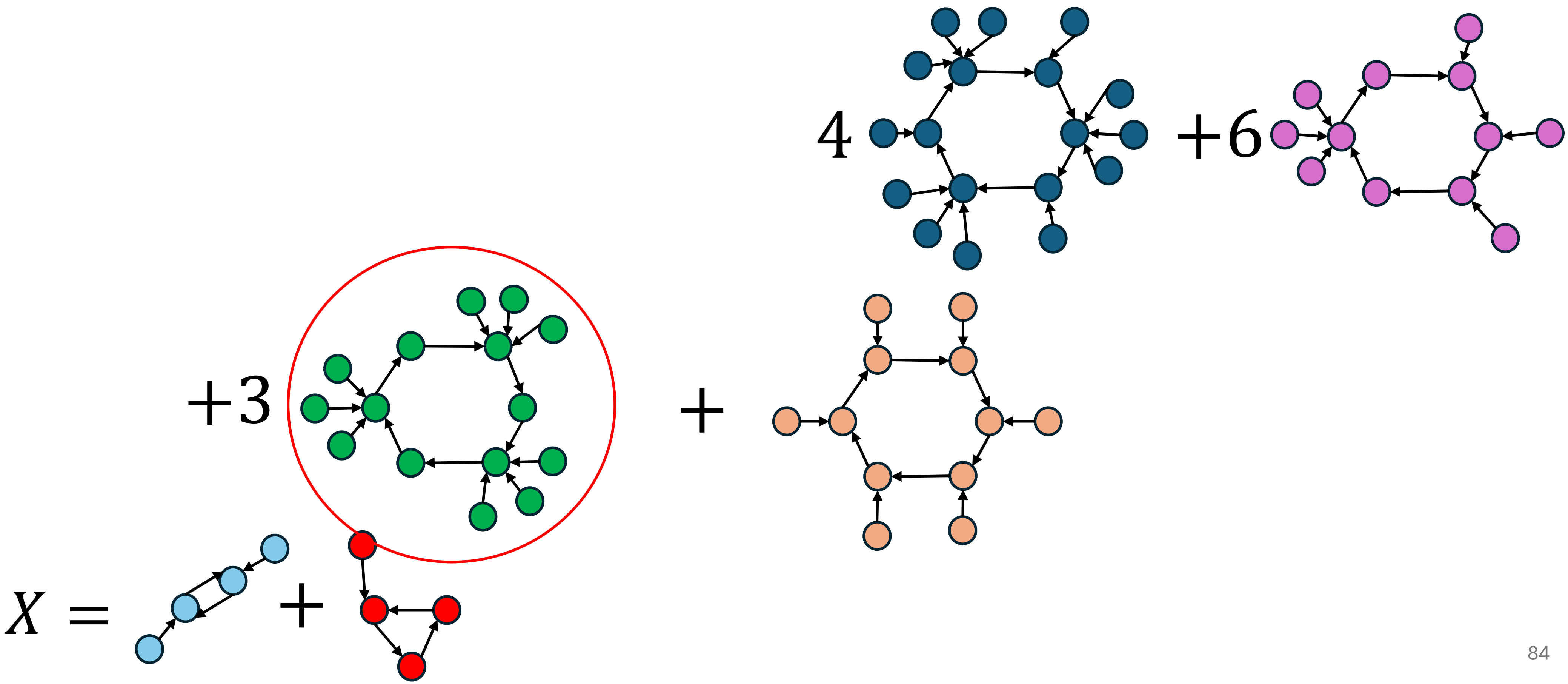
Step two: root
Example: square root



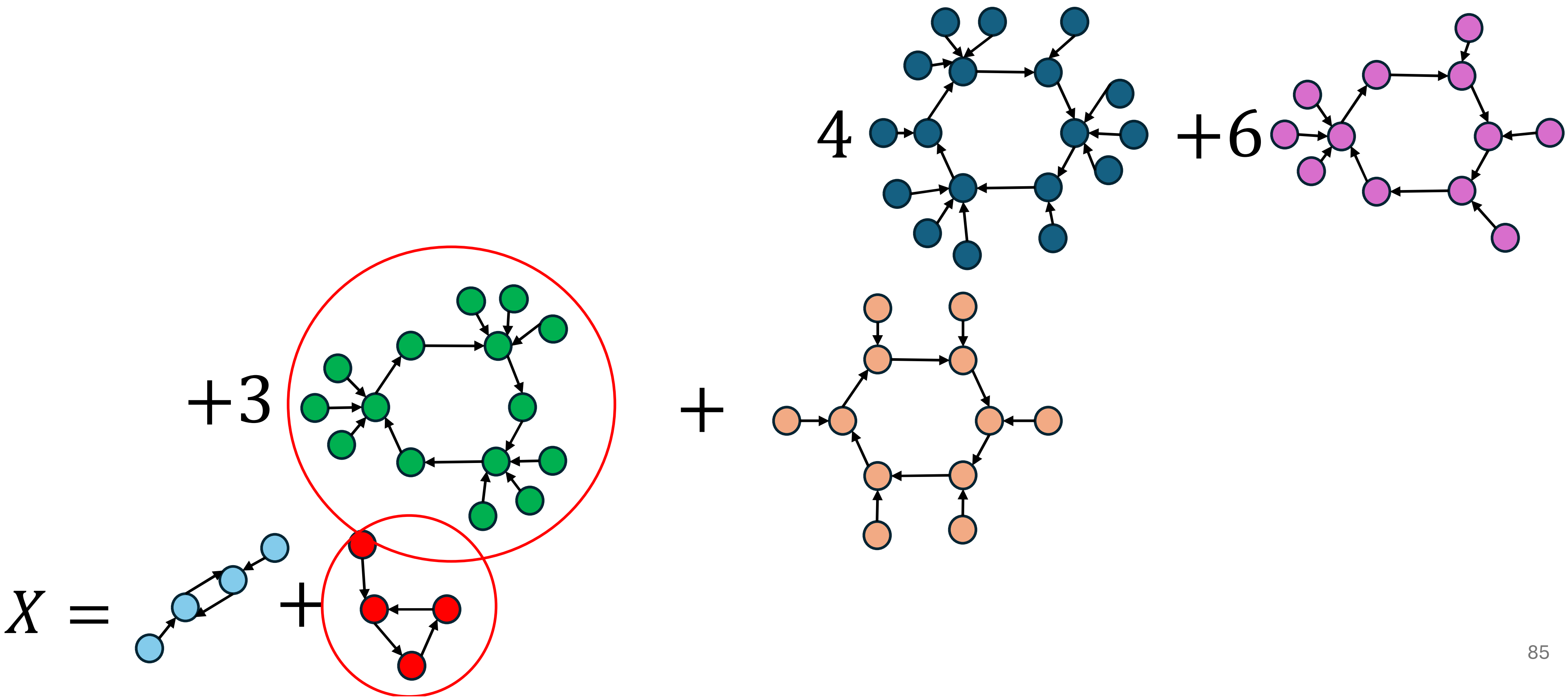
Step two: root
Example: square root



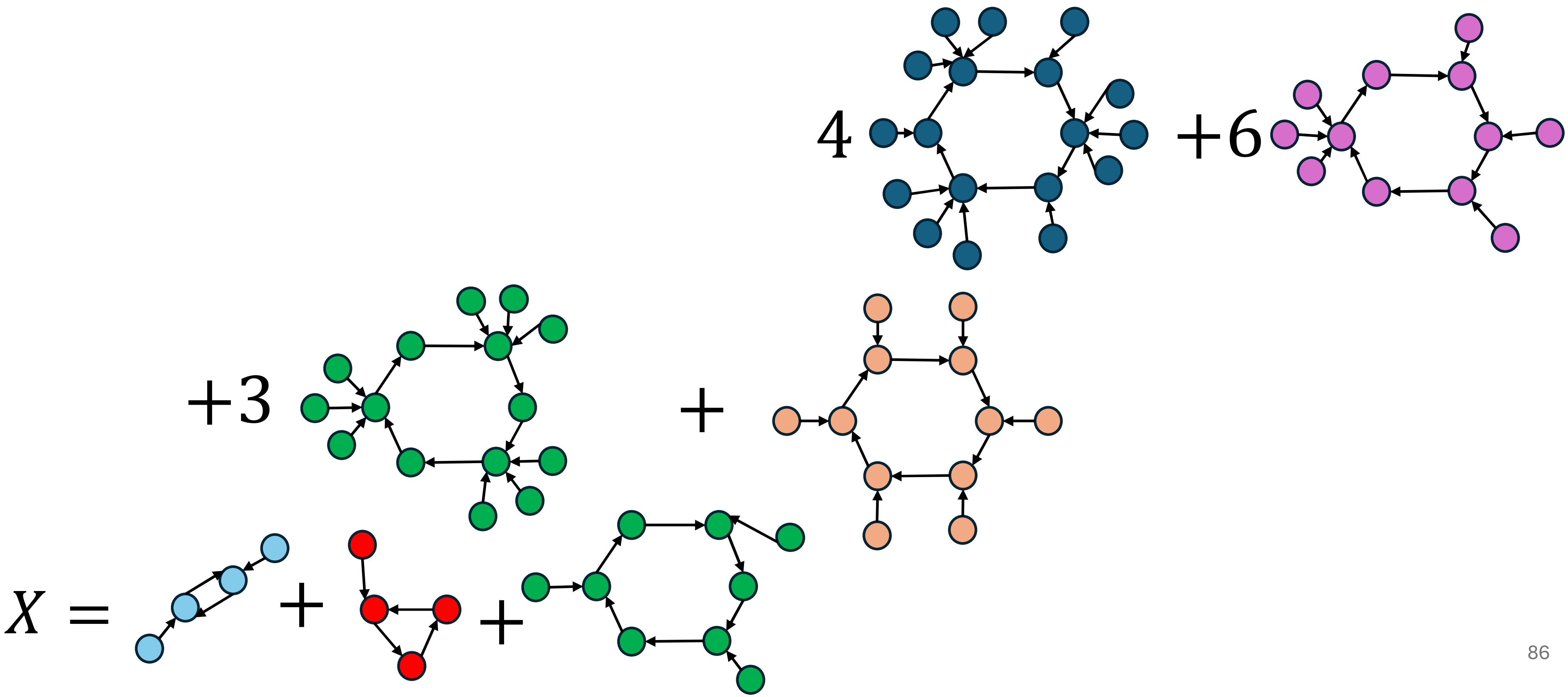
Step two: root
Example: square root



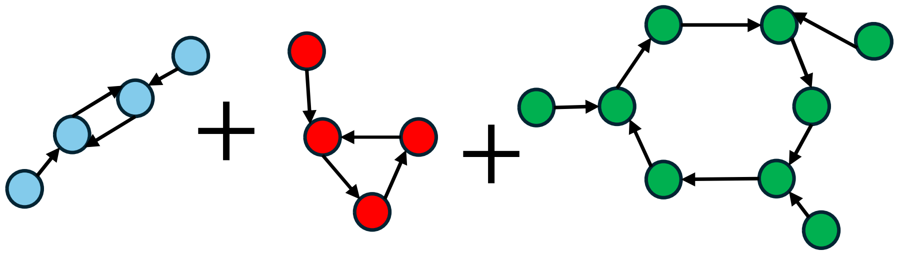
Step two: root
Example: square root



Step two: root
Example: square root



Step two: root
Example: square root

$X =$ 

Step two: root

$\sqrt[m]{\cdot}$ is injective and we can compute it in polynomial time.

Step three: general FDDS

Let k, n, m be three positive integer with $n \leq k$ and $X = X_1 + \ldots + X_k$ be an FDDS such that $X_i \leq_c X_{i+1}$ and $P = \sum_{i=1}^{m} A_i X^i$ be a polynomial without constant term and with at least one cancellable coefficient. Let B be a connected component of $\min(P(X) - P(\sum_{i=1}^{n-1} X_i))$ according to $\leq_c$ and $p = length(B)$.

Then $length(X_n) = p$.

Step three: general FDDS

- Since $length(X_n)$ is the smallest cycle length in $X - \sum_{i=1}^{n-1} X_i$, we have that $length(X_n) \leq length(B)$.

Step three: general FDDS

- Since $length(X_n)$ is the smallest cycle length in $X - \sum_{i=1}^{n-1} X_i$, we have that $length(X_n) \leq length(B)$.
- $length(x) = length(X_n)$, for all connected component x of ${X_n}^i$ and for all integer $i \geq 1$.

Step three: general FDDS

- Since $length(X_n)$ is the smallest cycle length in $X - \sum_{i=1}^{n-1} X_i$, we have that $length(X_n) \leq length(B)$.
- $length(x) = length(X_n)$, for all connected component x of ${X_n}^i$ and for all integer $i \geq 1$.
- ${X_n}^i \in X^i$ for all integer $i \geq 1$.

Step three: general FDDS

- Since $length(X_n)$ is the smallest cycle length in $X - \sum_{i=1}^{n-1} X_i$, we have that $length(X_n) \leq length(B)$.
- $length(x) = length(X_n)$, for all connected component x of ${X_n}^i$ and for all integer $i \geq 1$.
- ${X_n}^i \in X^i$ for all integer $i \geq 1$.
- Since P contains a cancellable coefficient, there exists a connected coefficient B' in $P(X) - P(\sum_{i=1}^{n-1} X_i)$ such that $length(B') = length(X_n)$

Step three: general FDDS

- Since $length(X_n)$ is the smallest cycle length in $X - \sum_{i=1}^{n-1} X_i$, we have that $length(X_n) \leq length(B)$.
- $length(x) = length(X_n)$, for all connected component x of ${X_n}^i$ and for all integer $i \geq 1$.
- ${X_n}^i \in X^i$ for all integer $i \geq 1$.
- Since P contains a cancellable coefficient, there exists a connected coefficient B' in $P(X) - P(\sum_{i=1}^{n-1} X_i)$ such that $length(B') = length(X_n) \Rightarrow length(X_n) \geq length(\mathrm{B})$.

Step three: general FDDS

1. If $P = \sum_{i=1}^{m} A_i X^i$ is a polynomial without constant terms and contains a cancellable coefficient, then P is injective (simple induction).

Step three: general FDDS

1. If $P = \sum_{i=1}^{m} A_i X^i$ is a polynomial without constant terms and contains a cancellable coefficient, then P is injective (simple induction).
2. We can solve in polynomial time the equation $P(X) = B$, by :

Step three: general FDDS

1. If $P = \sum_{i=1}^{m} A_i X^i$ is a polynomial without constant terms and contains a cancellable coefficient, then P is injective (simple induction).
2. We can solve in polynomial time the equation $P(X) = B$, by :
   1. Let p be the length of a connected component of $\min(B - P(Sol))$ according to $\leq_c$,

Step three: general FDDS

1. If $P = \sum_{i=1}^{m} A_i X^i$ is a polynomial without constant terms and contains a cancellable coefficient, then P is injective (simple induction).
2. We can solve in polynomial time the equation $P(X) = B$, by :
   1. Let p be the length of a connected component of $\min(B - P(Sol))$ according to $\leq_c$,
   2. Solve the equation $C_n\left(U\big(P(X) - P(Sol)\big)\right) = C_n\big(U(B)\big)$,

Step three: general FDDS

1. If $P = \sum_{i=1}^{m} A_i X^i$ is a polynomial without constant terms and contains a cancellable coefficient, then P is injective (simple induction).
2. We can solve in polynomial time the equation $P(X) = B$, by :
   1. Let p be the length of a connected component of $\min(B - P(Sol))$ according to $\leq_c$,
   2. Solve the equation $C_n\Big(U\big(P(X) - P(Sol)\big)\Big) = C_n\big(U(B)\big)$,
   3. Roll the minimum tree of this solution with period p,

Step three: general FDDS

1. If $P = \sum_{i=1}^{m} A_i X^i$ is a polynomial without constant terms and contains a cancellable coefficient, then P is injective (simple induction).
2. We can solve in polynomial time the equation $P(X) = B$, by :
   1. Let p be the length of a connected component of $\min(B - P(Sol))$ according to $\leq_c$,
   2. Solve the equation $C_n\left(U\left(P(X) - P(Sol)\right)\right) = C_n\left(U(B)\right)$,
   3. Roll the minimum tree of this solution with period p,
   4. Add the resulting component to Sol,

Step three: general FDDS

1. If $P = \sum_{i=1}^{m} A_i X^i$ is a polynomial without constant terms and contains a cancellable coefficient, then P is injective (simple induction).
2. We can solve in polynomial time the equation $P(X) = B$, by :
   1. Let p be the length of a connected component of $\min(B - P(Sol))$ according to $\leq_c$,
   2. Solve the equation $C_n\left(U\big(P(X) - P(Sol)\big)\right) = C_n\big(U(B)\big)$,
   3. Roll the minimum tree of this solution with period p,
   4. Add the resulting component to Sol,
   5. Repeat until $P(Sol) \not\subset B$,

Step three: general FDDS

1. If $P = \sum_{i=1}^{m} A_i X^i$ is a polynomial without constant terms and contains a cancellable coefficient, then P is injective (simple induction).
2. We can solve in polynomial time the equation $P(X) = B$, by :
   1. Let p be the length of a connected component of $\min(B - P(Sol))$ according to $\leq_c$,
   2. Solve the equation $C_n\left(U\big(P(X) - P(Sol)\big)\right) = C_n\big(U(B)\big)$,
   3. Roll the minimum tree of this solution with period p,
   4. Add the resulting component to Sol,
   5. Repeat until $P(Sol) \not\subset B$,
   6. Return $P(Sol) = B$.

Thanks for your attention

References

1. Dennunzio, A., Dorigatti, V., Formenti, E., Manzoni, L., Porreca, A.E.: Polynomials over the semiring of dynamical systems.
2. Naquin, E., Gadouleau, M.:Factorisation in the semiring of finite dynamical systems.
3. Doré, F., Perrot K., Porreca A.E., Rolland M., Riva S.: Roots in the semiring of finite deterministic dynamical systems