# Dynamical systems and their algebra

**Antonio E. Porreca • aeporreca.org**
**Université Publique, Marseille**

**Workshop on Automata Network • WAN 2021**
**CIRM, Marseille • 12–17 July 2021**

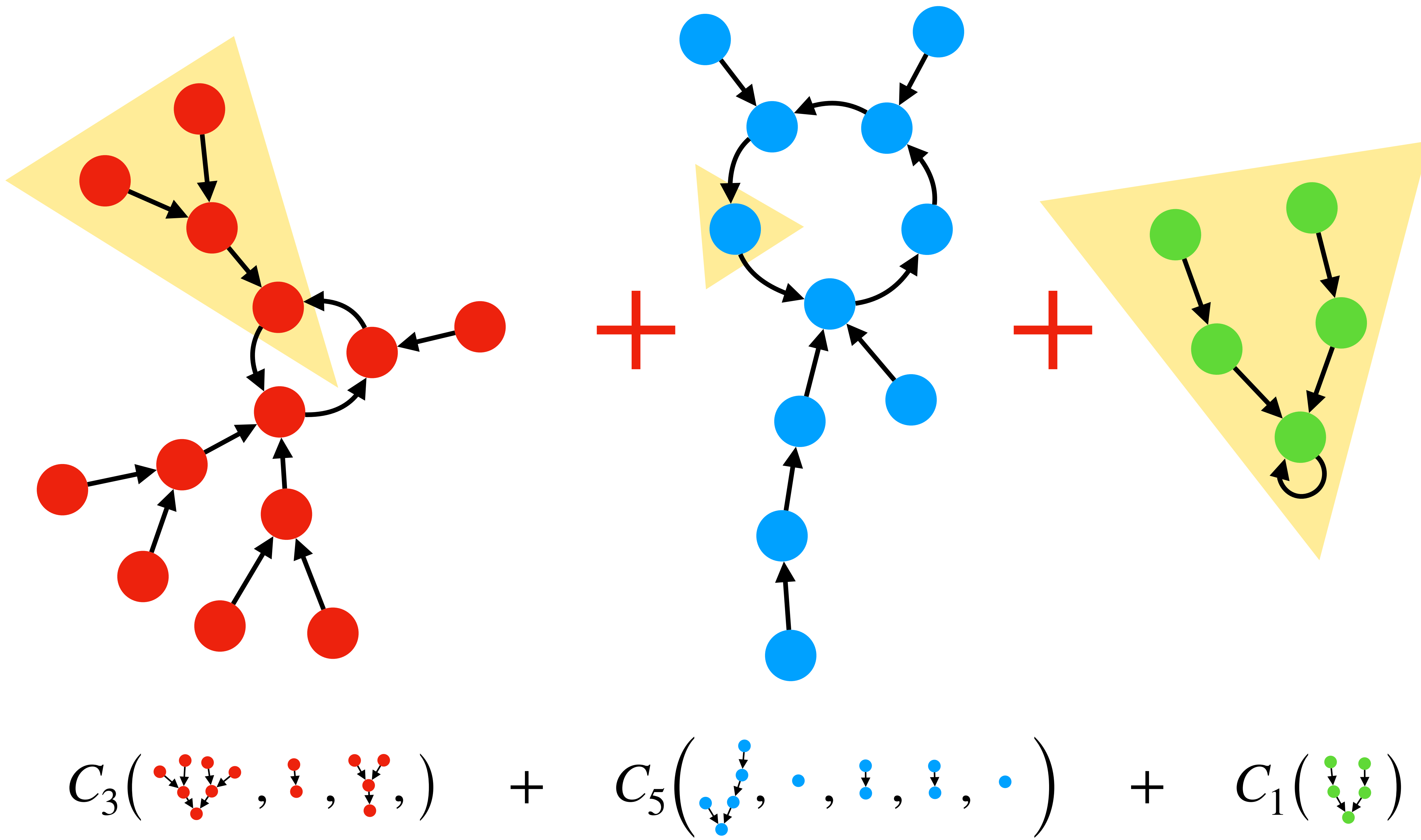
# Main idea

“If you liked it then you shoulda put a semiring on it”

Beyoncé Knowles, “Single Ladies (Put a Semiring on It)”
In: Beyoncé Knowles, Mathew Knowles (exec. prod.)
*I Am… Sasha Fierce*, Columbia Records, 2008
https://youtu.be/4m1EFMoRFvY

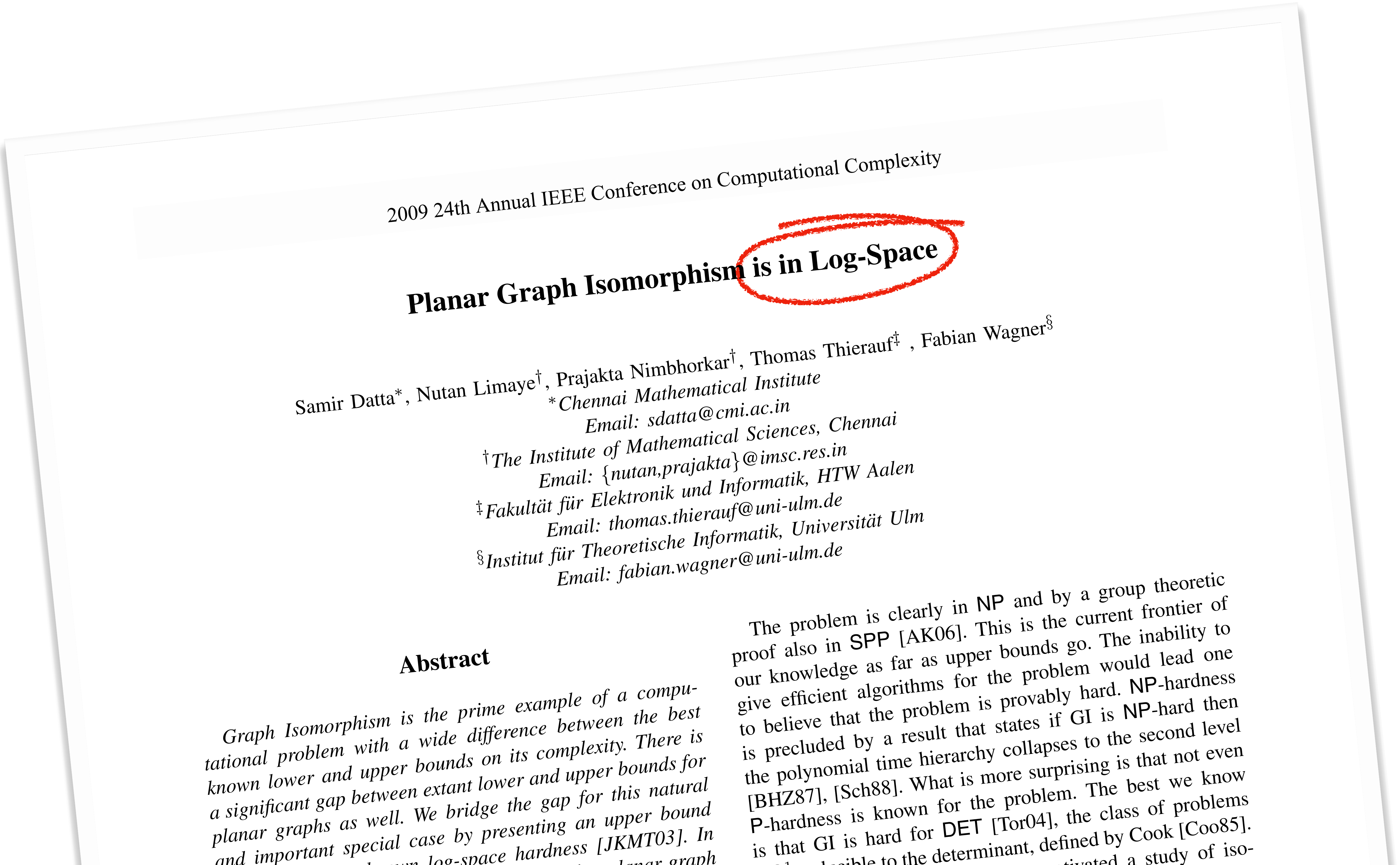
# General shape of a dynamical system

## A few limit cycles **with trees going in**



# Isomorphism of dynamical systems

## Not a problem, from a complexity perspective



2009 24th Annual IEEE Conference on Computational Complexity

**Planar Graph Isomorphism is in Log-Space**

Samir Datta*, Nutan Limaye†, Prajakta Nimbhorkar†, Thomas Thierauf‡, Fabian Wagner§

*Chennai Mathematical Institute
Email: sdatta@cmi.ac.in

†The Institute of Mathematical Sciences, Chennai
Email: {nutan,prajakta}@imsc.res.in

‡Fakultät für Elektronik und Informatik, HTW Aalen
Email: thomas.thierauf@uni-ulm.de

§Institut für Theoretische Informatik, Universität Ulm
Email: fabian.wagner@uni-ulm.de

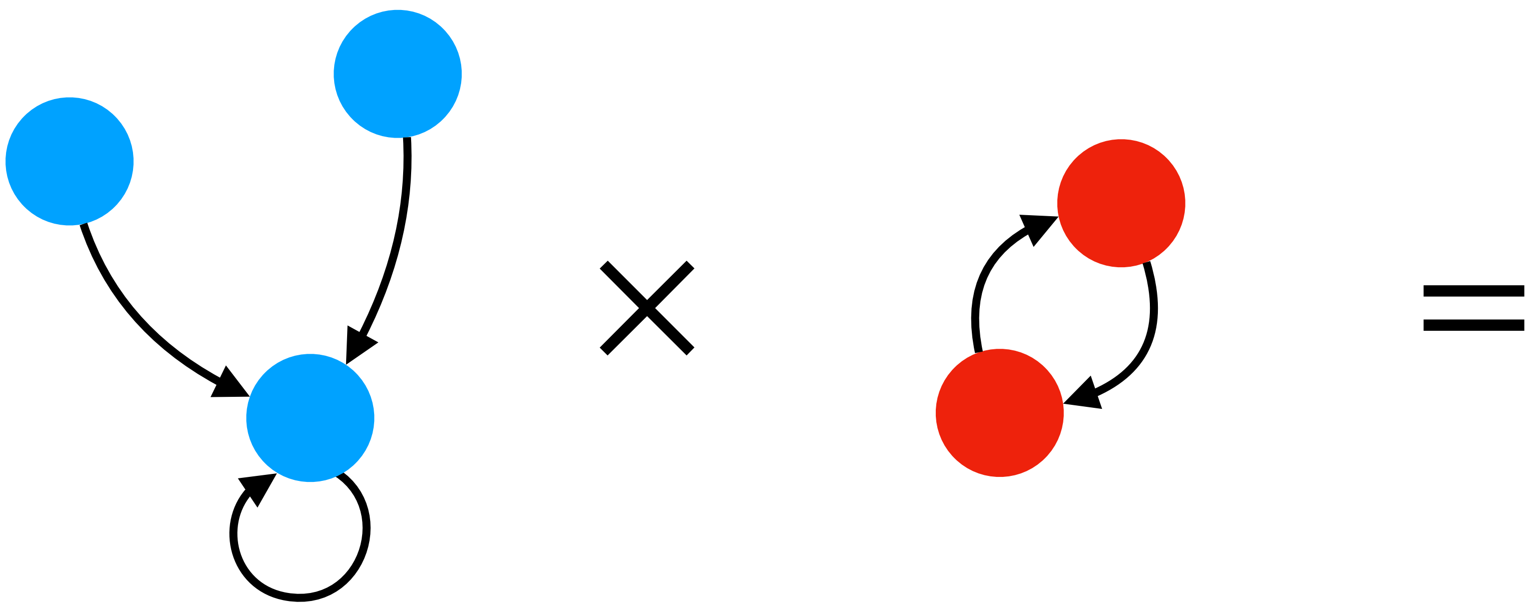
**Abstract**

*Graph Isomorphism is the prime example of a computational problem with a wide difference between the best known lower and upper bounds on its complexity. There is a significant gap between extant lower and upper bounds for planar graphs as well. We bridge the gap for this natural and important special case by presenting an upper bound ... log-space hardness [JKMT03]. In ...*

The problem is clearly in NP and by a group theoretic proof also in SPP [AK06]. This is the current frontier of our knowledge as far as upper bounds go. The inability to give efficient algorithms for the problem would lead one to believe that the problem is provably hard. NP-hardness is precluded by a result that states if GI is NP-hard then the polynomial time hierarchy collapses to the second level [BHZ87], [Sch88]. What is more surprising is that not even P-hardness is known for the problem. The best we know is that GI is hard for DET [Tor04], the class of problems ... to the determinant, defined by Cook [Coo85]. ...

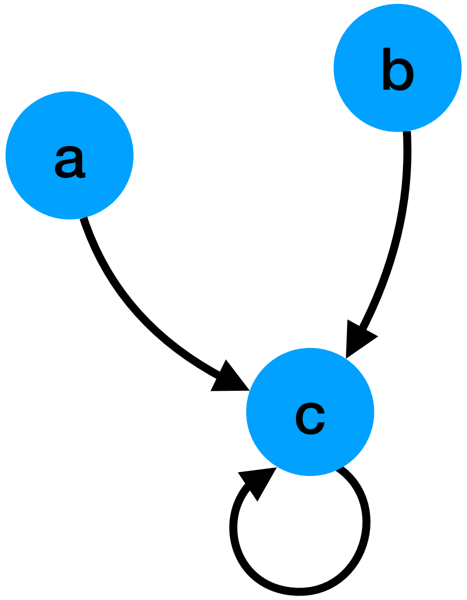
# Product is graph tensor product

## Synchronous execution of two systems

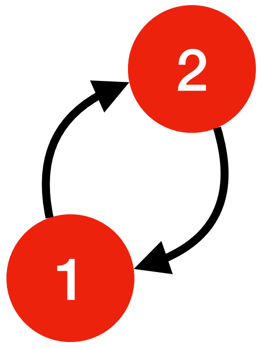


# Product in $\mathbf{D}$ is graph tensor product

## Temporary state names



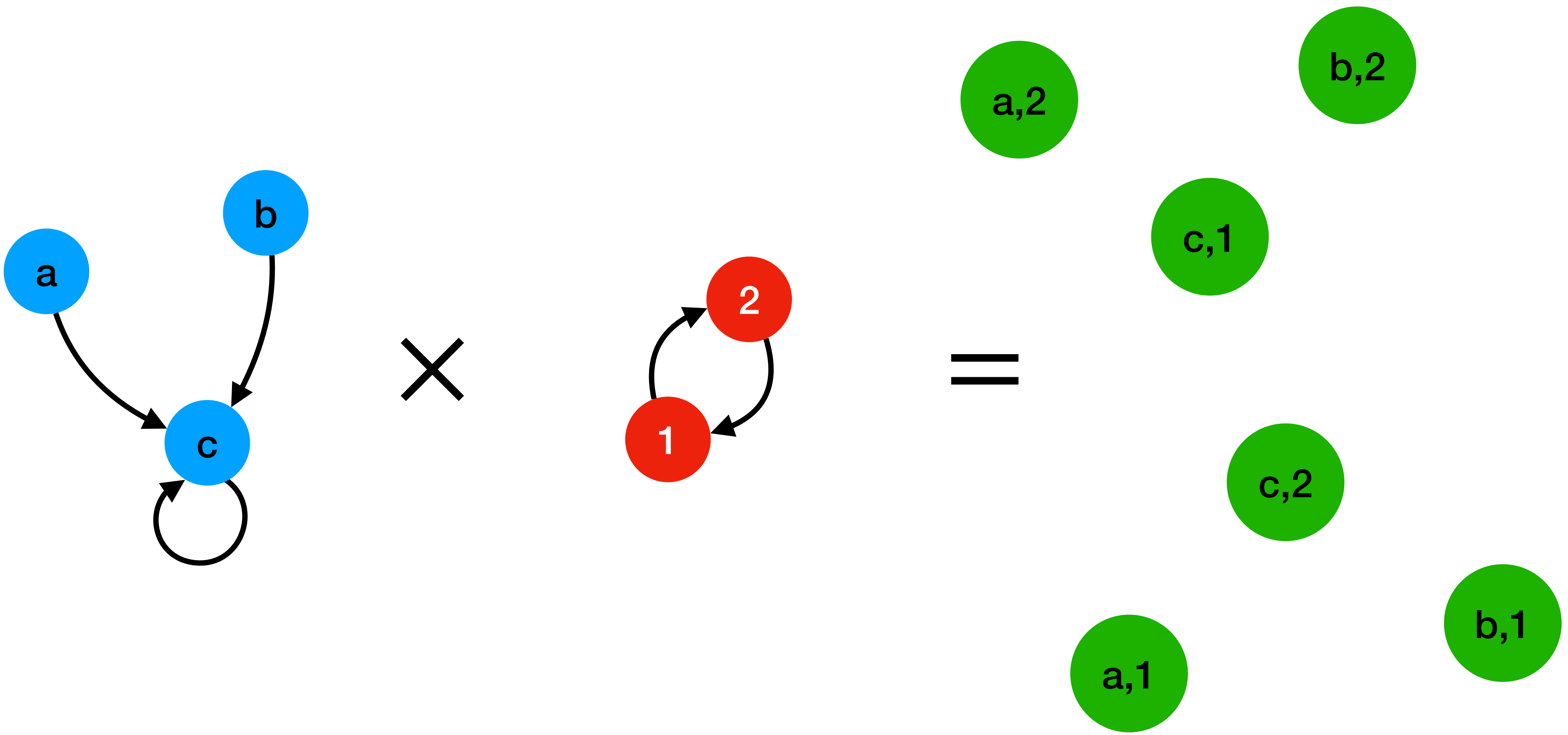

$\times$




$=$

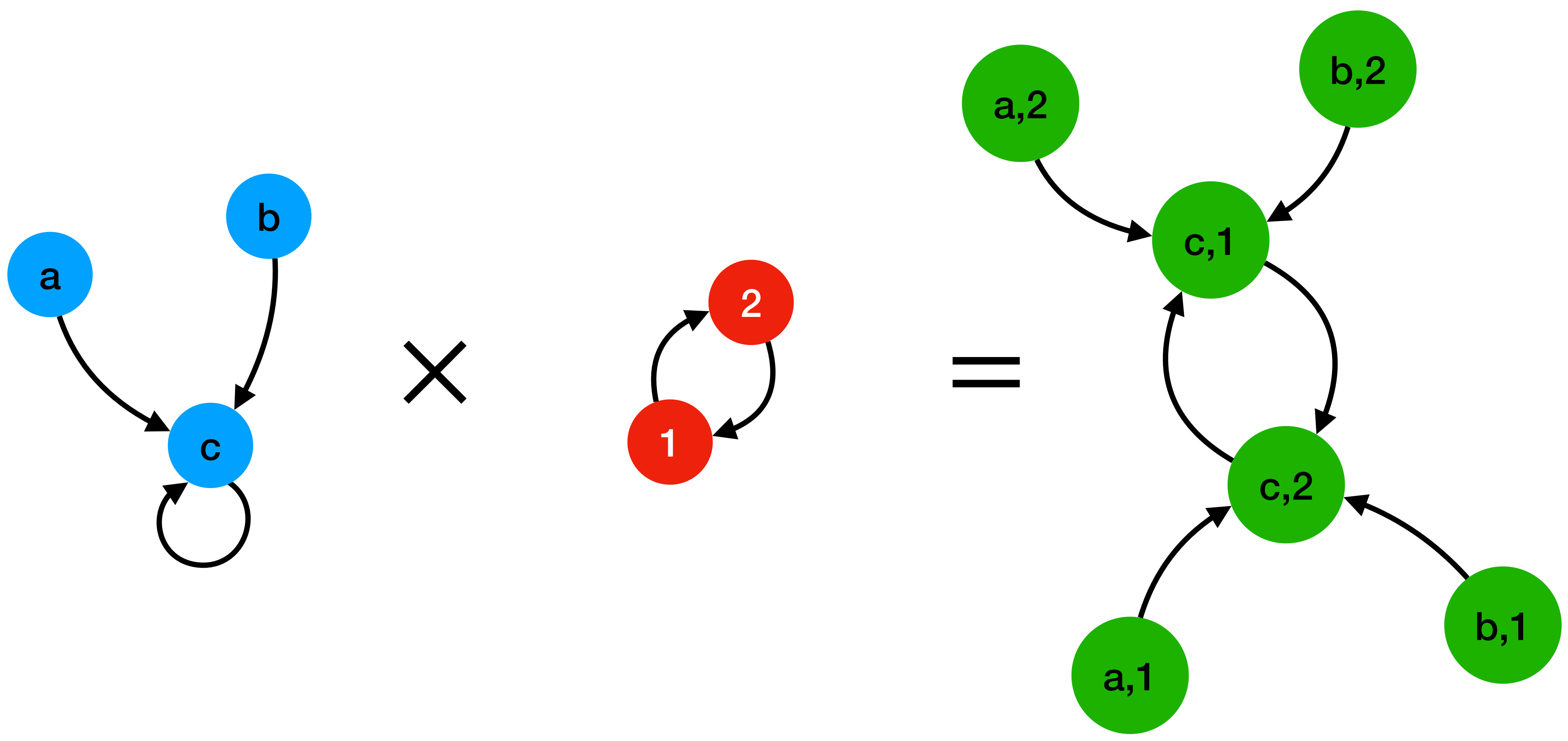
# Product in $\mathbf{D}$ is graph tensor product

## Cartesian product of the states



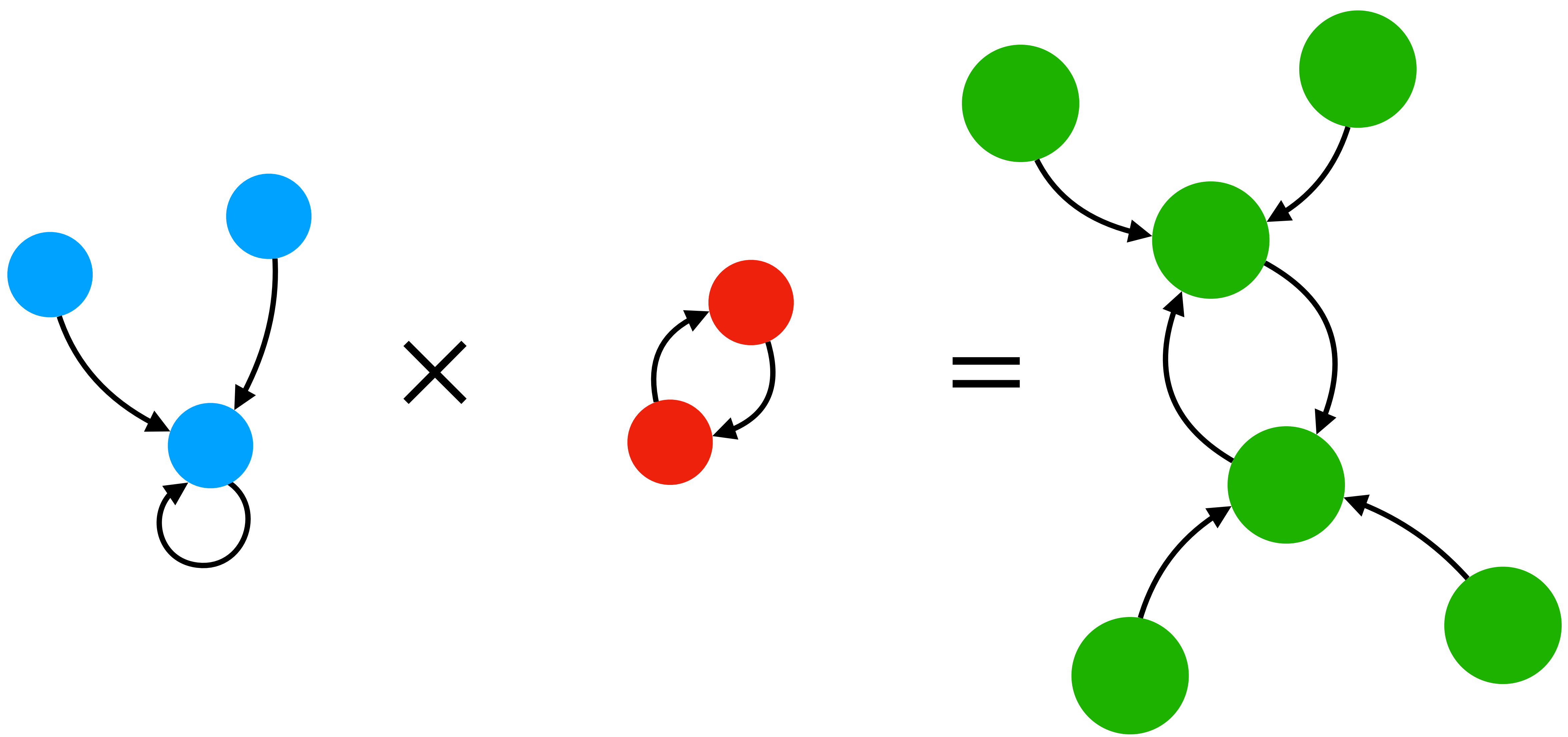
# Product in $\mathbb{D}$ is graph tensor product

## Arrows iff arrows between both components



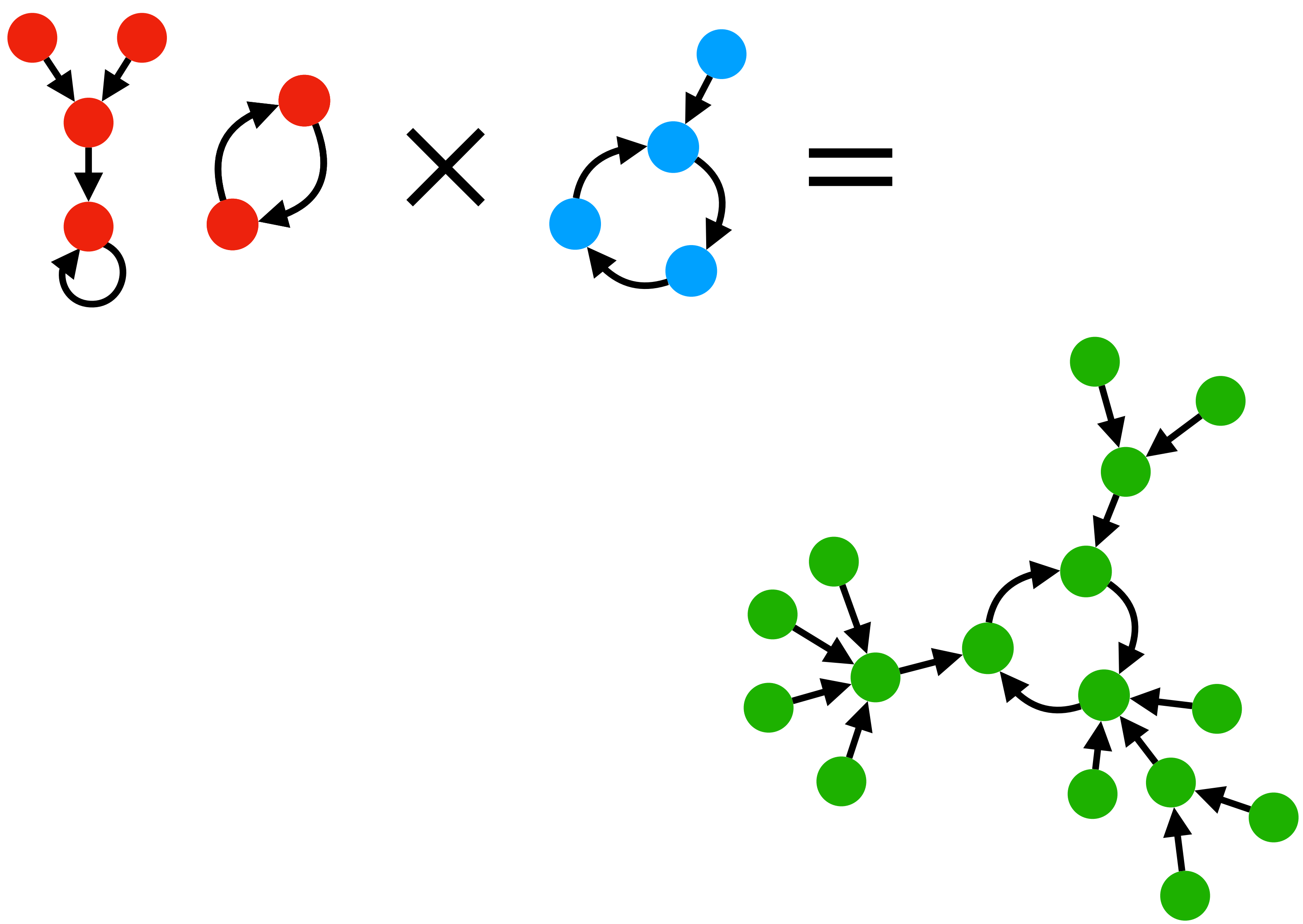
# Product in $\mathbf{D}$ is graph tensor product

## We forget the state names once again



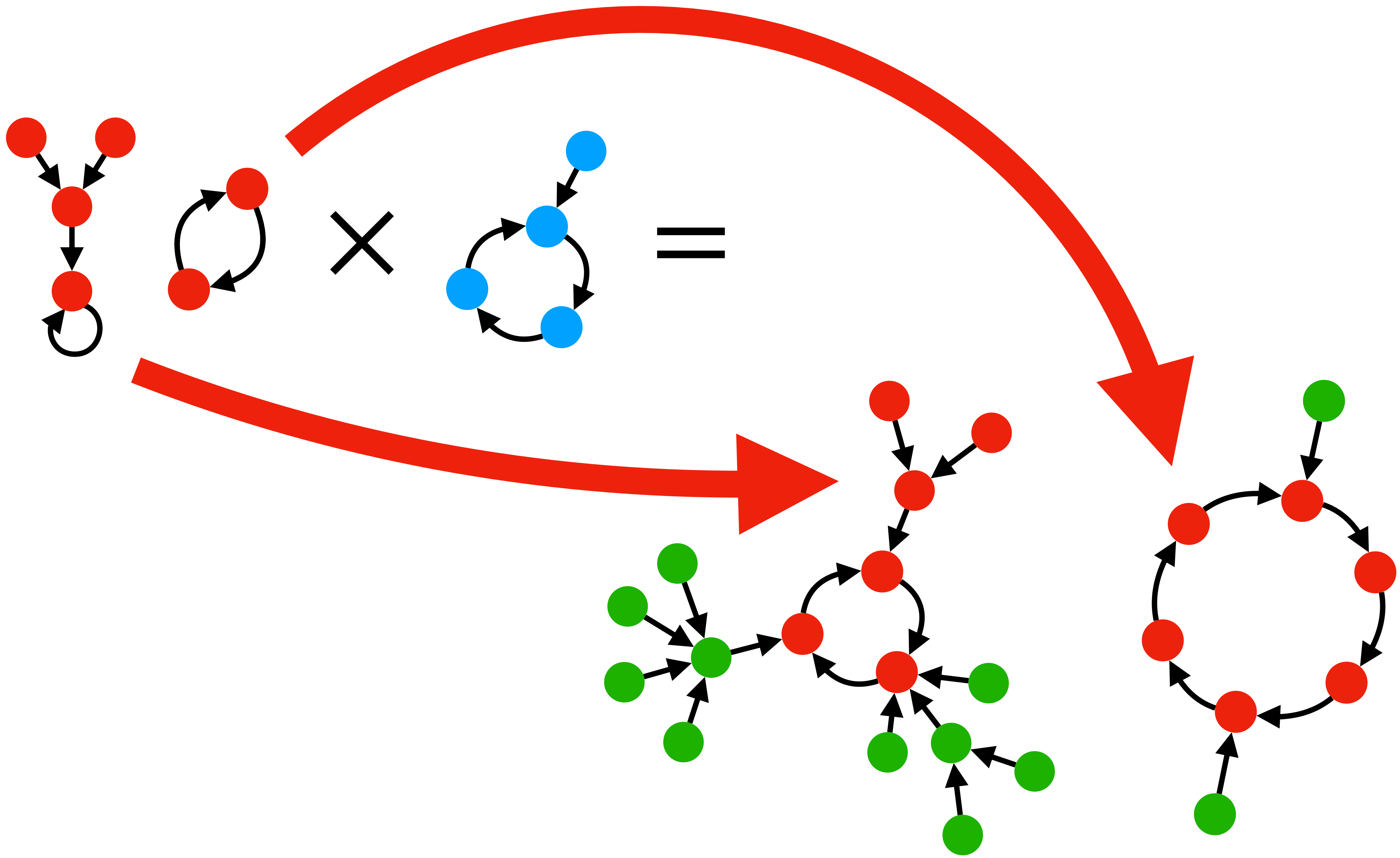
# Products “preserve” behaviours

**$A$ is a minor of $A \times B$ for $B \neq \varnothing$**



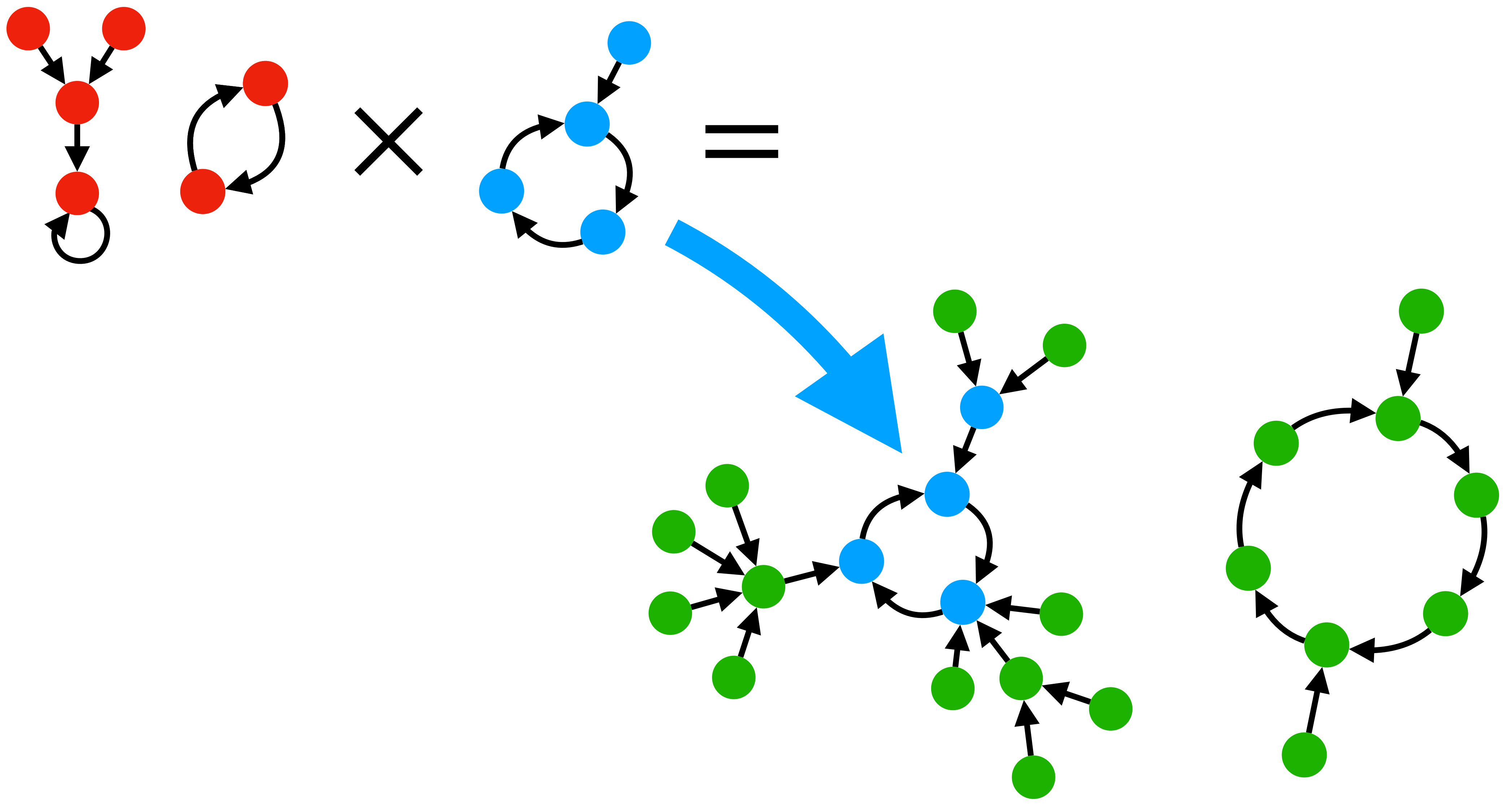
# Products “preserve” behaviours

$A$ **is a minor of** $A \times B$ **for** $B \neq \varnothing$



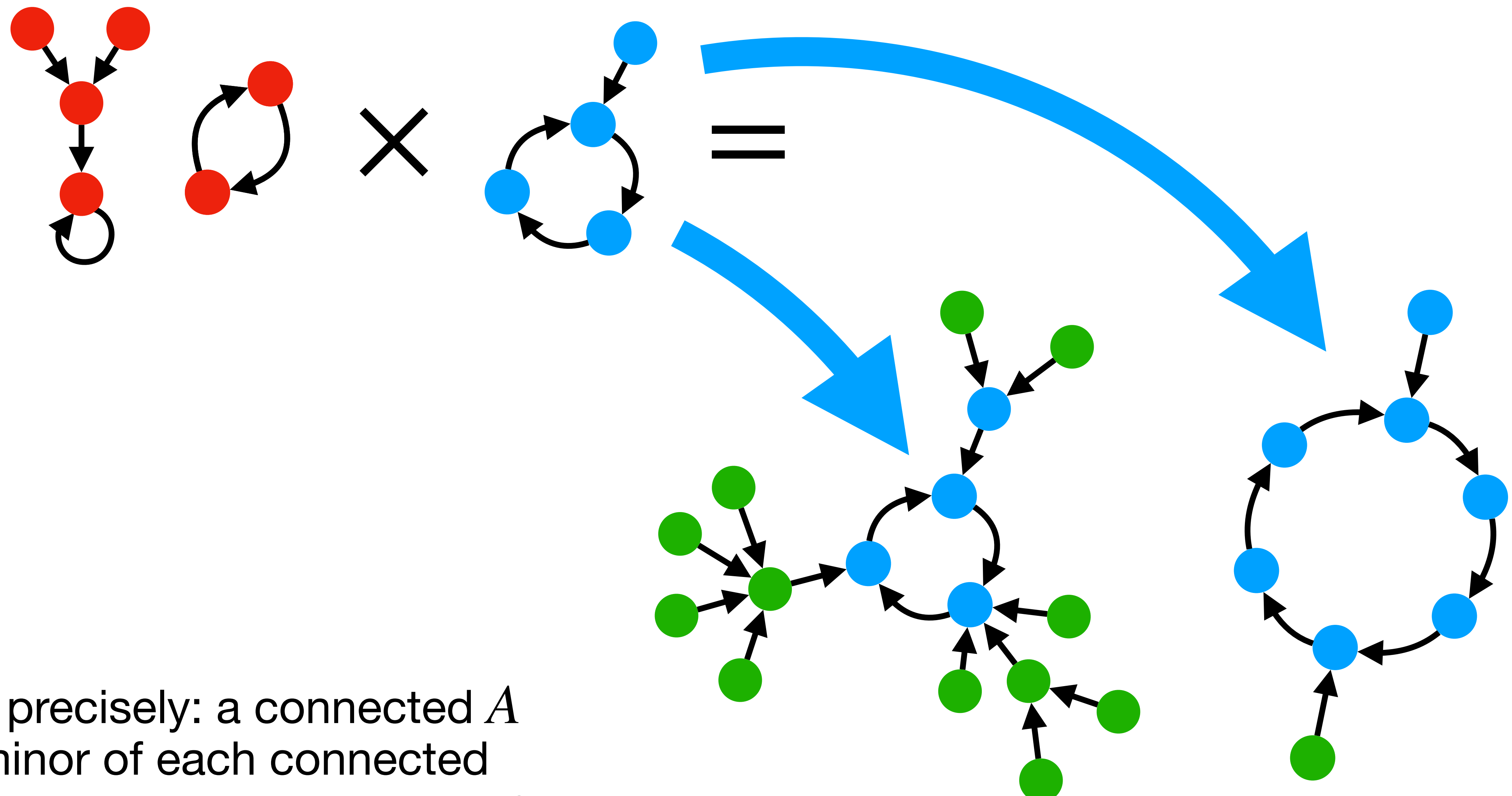
# Products “preserve” behaviours

$A$ **is a minor of** $A \times B$ **for** $B \neq \varnothing$



# Products “preserve” behaviours

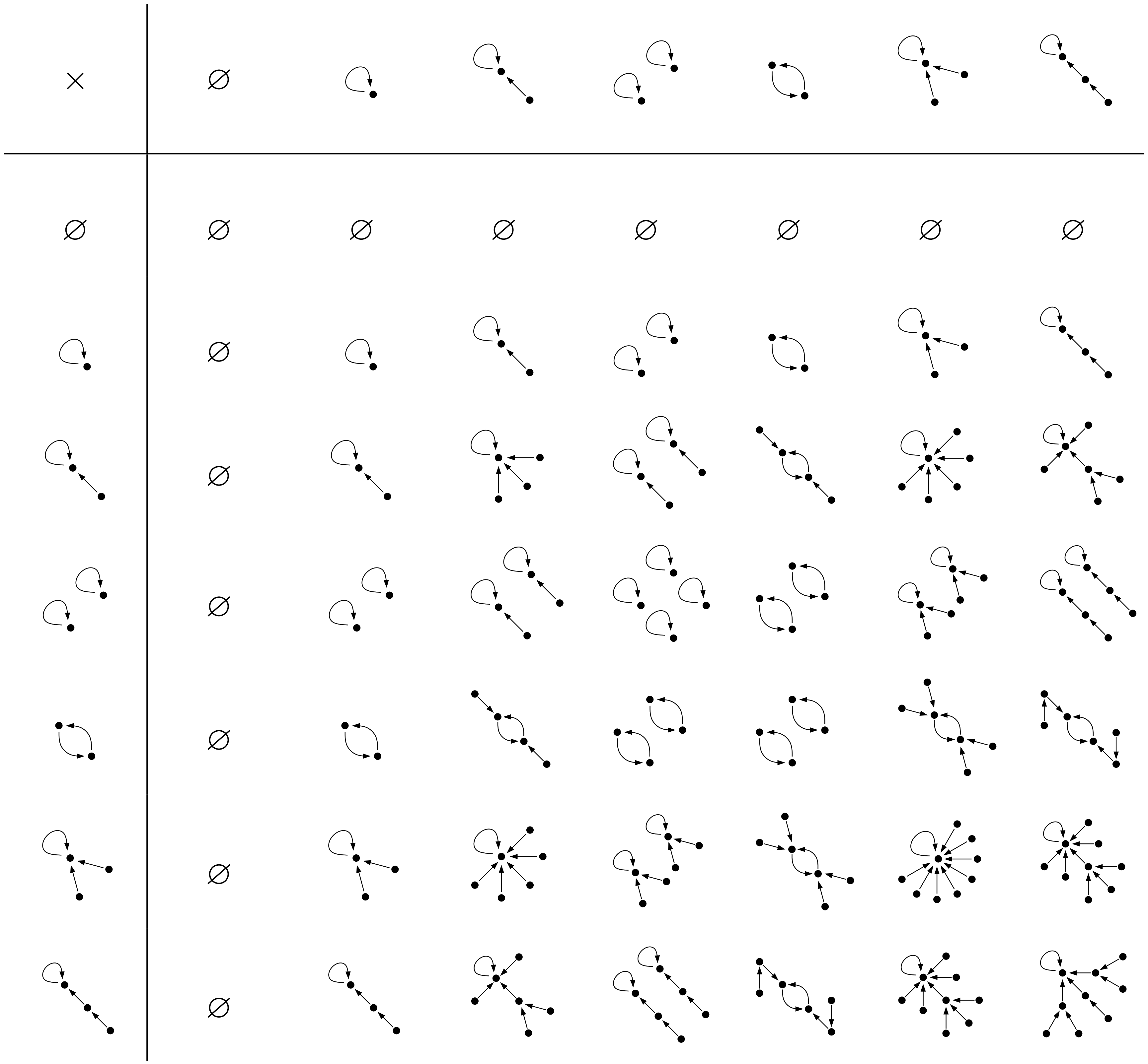
$A$ **is a minor of** $A \times B$ **for** $B \neq \varnothing$

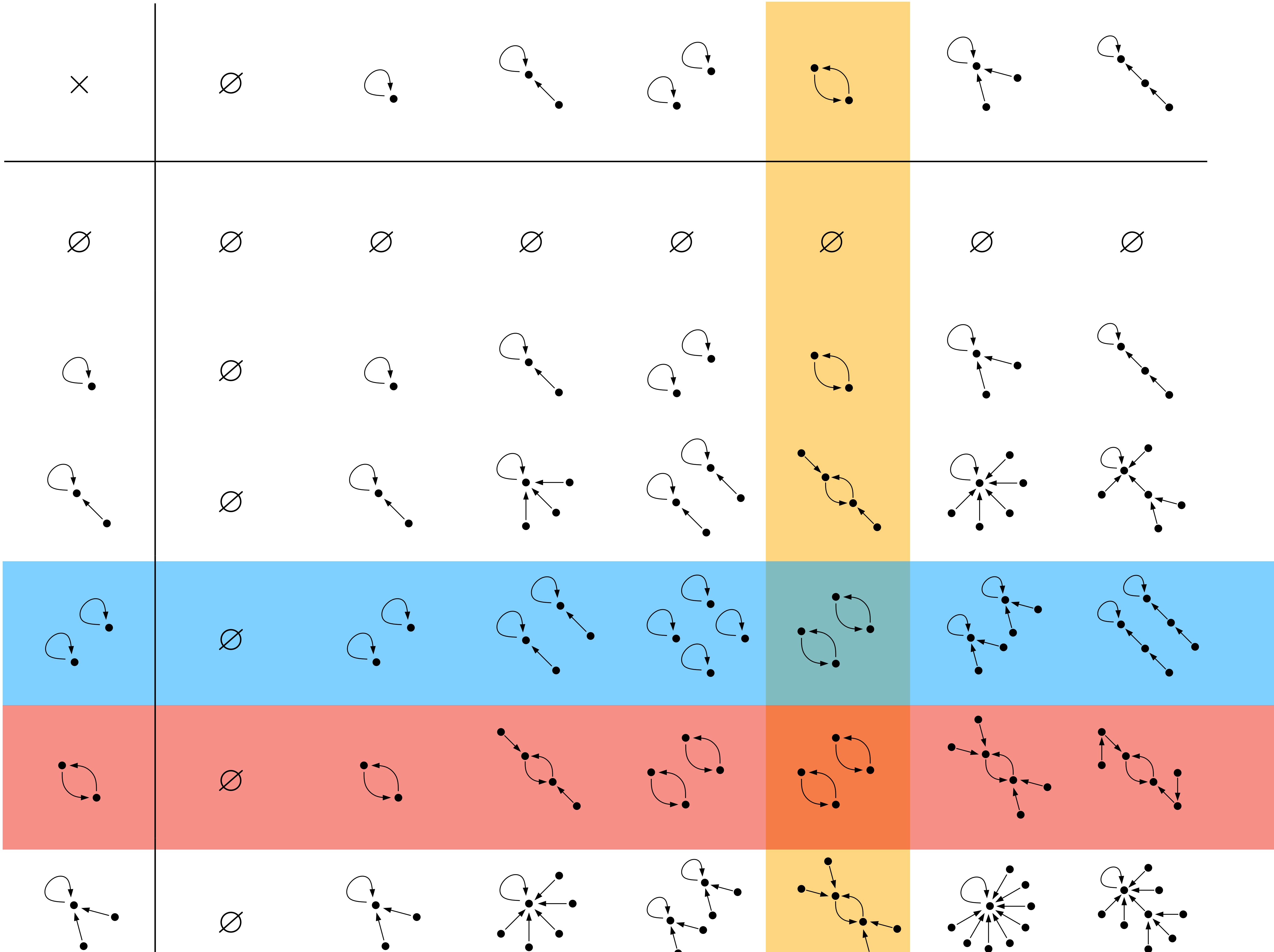


more precisely: a connected $A$ is a minor of each connected component of $A \times B$ for $B \neq 0$

# No unique factorisation 😭

# Multiplication table



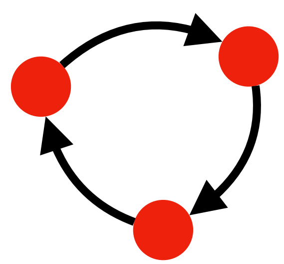
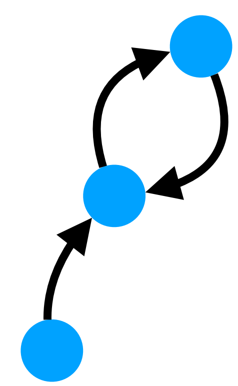
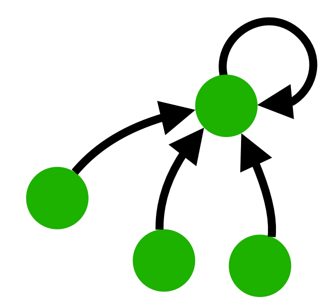


# Polynomial equations

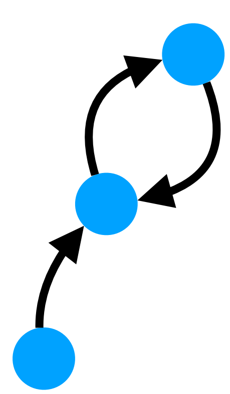
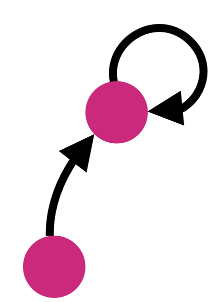
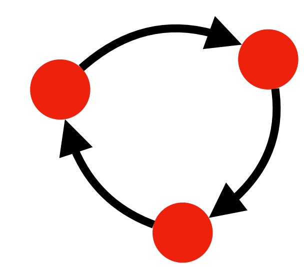
# Polynomial equations over $\mathbb{D}$

## For the analysis of complex systems

- Consider the equation

 $X + Y^2 =$  $Z +$ 

- There is least one solution

$X =$  $Y =$  $Z =$ 

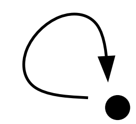
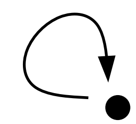
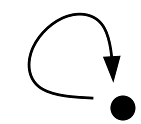
# Undecidability of polynomial equations

# $\mathbb{N}$ is a subsemiring of $\mathbf{D}$

## This means trouble

- There is an injective homomorphism $\varphi : \mathbb{N} \to \mathbf{D}$

$$\varphi(n) = \underbrace{\mathbf{1} + \mathbf{1} + \cdots + \mathbf{1}}_{n \text{ times}} =$$

 +  + $\cdots$ + 

$n$ times

- $n$ fixed points behave exactly as the integer $n$

- So $\mathbf{D}$ contains a isomorphic copy of $\mathbb{N}$

# Hilbert's 10th problem over $\mathbf{D}$

## Unsolvability of polynomial equations

- If a multivariate polynomial equation over $\mathbb{N}$ has a solution in $\mathbf{D}$, then it also has a solution in $\mathbb{N}$ (just replace each system by its size!)
- In the larger semiring $\mathbf{D}$ we may find extra solutions, but only if the equation is already solvable over the naturals
- Then, by reduction from Hilbert's 10th problem, we obtain the undecidability in $\mathbf{D}$ of polynomial equations over $\mathbb{N}$…
- …and thus of arbitrary equations over $\mathbf{D}$

# Polynomial equations with constant RHS are decidable and in $\mathbf{NP}$

# Systems of linear equations with constant RHS are $\mathbf{NP}$-complete

# NP-hardness of linear systems

## By reduction from One-in-three-3SAT

- Given a 3CNF Boolean formula $\varphi$, is there a satisfying assignment such that exactly one literal per clause is true?
- For each variable $x$ of $\varphi$ we have one equation $X + X' = 1$, forcing one between $X$ and $X'$ to be $1$, and the other to be $0$
- For each clause, for instance $(x \vee \neg y \vee z)$, we have one equation $X + Y' + Z = 1$, which forces exactly one variable to $1$
- These are all linear, constant-RHS equations over $\mathbf{D}$ and more specifically over $\mathbb{N}$, and its solutions are the same as the satisfying assignments of $\varphi$ with one true literal per clause

# A single linear, constant-RHS equation is **NP**-complete*

* Main idea by Florian Bridoux, bravo !

# $\mathbf{D}$ is a $\mathbb{N}$-semimodule

## Like a vector space, but over a semiring

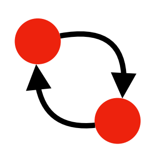
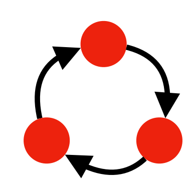
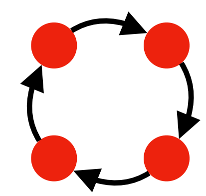
- Here the vectors are dynamical systems and the scalars are naturals
- Trivial because the semimodule axioms are a consequence of $\mathbb{N}$ being a subsemiring of $\mathbf{D}$
- $\mathbf{D}$ as a semimodule has a unique, countably infinite basis consisting of all nonempty, connected dynamical systems

# Reducing the system of equations to one

## Several $\mathbb{N}[\overrightarrow{X}]$ linear equations to one $\mathbf{D}[\overrightarrow{X}]$ equation

- Let $p_1(\overrightarrow{X}) = 1, \ldots, p_n(\overrightarrow{X}) = 1$ be the previous system of equations, with $p_i \in \mathbb{N}[\overrightarrow{X}]$

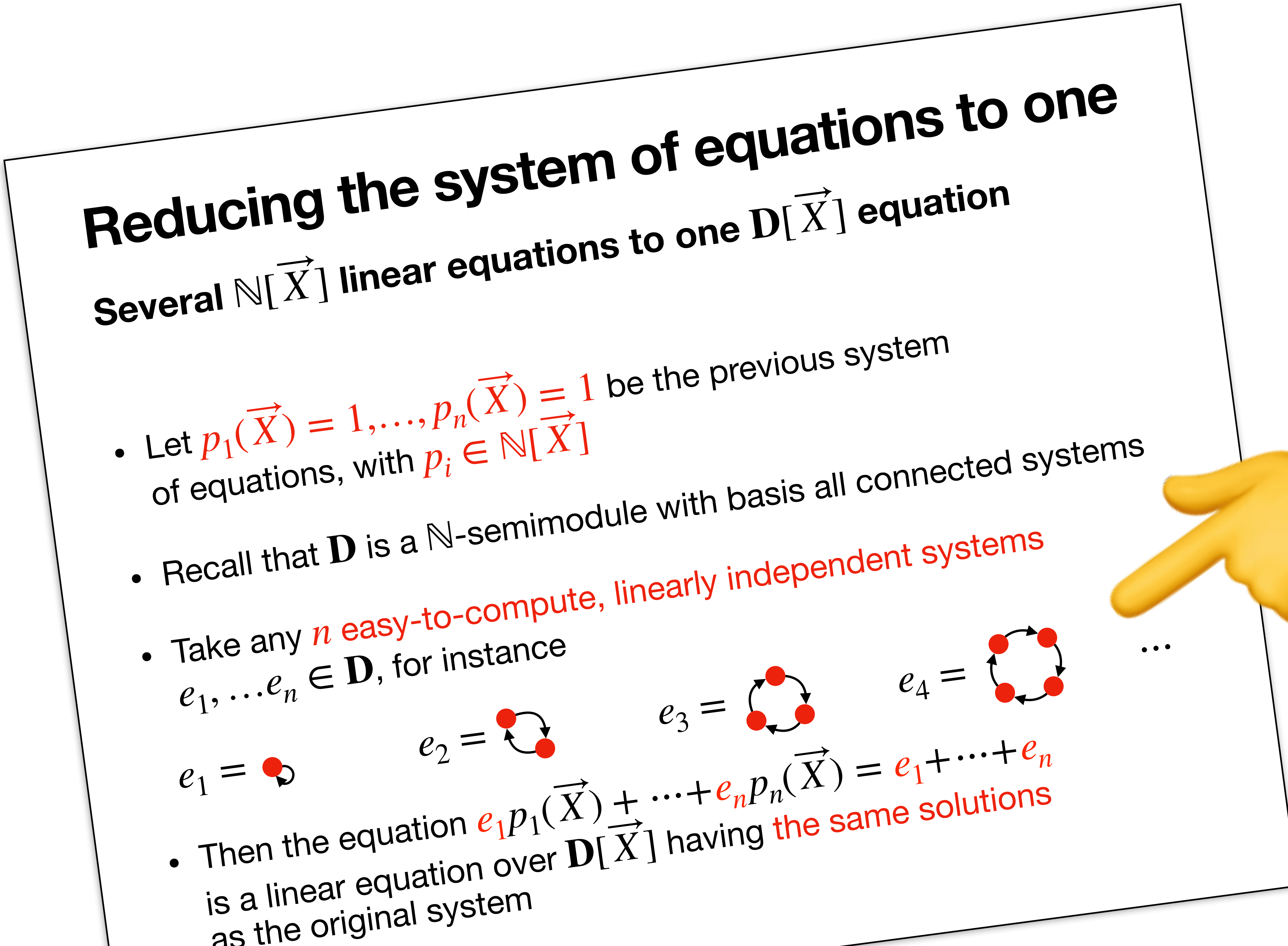
- Take any $n$ easy-to-compute, linearly independent systems $e_1, \ldots e_n \in \mathbf{D}$, for instance

$e_1 =$  $e_2 =$  $e_3 =$  $e_4 =$  $\cdots$

- Then the equation $e_1 p_1(\overrightarrow{X}) + \cdots + e_n p_n(\overrightarrow{X}) = e_1 + \cdots + e_n$ is a linear equation over $\mathbf{D}[\overrightarrow{X}]$ having the same solutions as the original system

# Linear, constant-RHS eqns are $\mathbf{NP}$-complete

## Even equations over cycles, even in explicit form!



## Reducing the system of equations to one

### Several $\mathbb{N}[\vec{X}]$ linear equations to one $\mathbf{D}[\vec{X}]$ equation

- Let $p_1(\vec{X}) = 1, \ldots, p_n(\vec{X}) = 1$ be the previous system of equations, with $p_i \in \mathbb{N}[\vec{X}]$
- Recall that $\mathbf{D}$ is a $\mathbb{N}$-semimodule with basis all connected systems
- Take any $n$ easy-to-compute, linearly independent systems $e_1, \ldots e_n \in \mathbf{D}$, for instance

$e_1 =$ $e_2 =$ $e_3 =$ $e_4 =$ …

- Then the equation $e_1 p_1(\vec{X}) + \cdots + e_n p_n(\vec{X}) = e_1 + \cdots + e_n$ is a linear equation over $\mathbf{D}[\vec{X}]$ having the same solutions as the original system

# Irreducible systems

# Most dynamical systems are irreducible

## $A$ is irreducible iff $A = BC$ implies $B = \mathbf{1}$ or $C = \mathbf{1}$

- Formally:

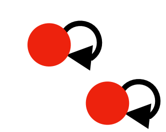
$$\lim_{n\to\infty} \frac{\text{number of reducible systems over} \leq n \text{ states}}{\text{total number of systems over} \leq n \text{ states}} = 0$$

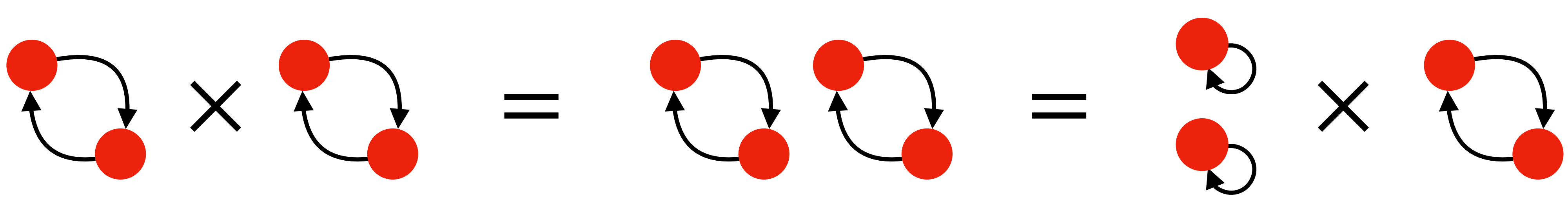
- Notice that this is the opposite of $\mathbb{N}$, where irreducible (aka prime) integers are scarce)

# Prime system

# Prime system

$P \neq 0,1$ **is prime iff** $P \mid AB$ **implies** $P \mid A$ **or** $P \mid B$

- If a prime $P$ appears in a factorisation into irreducibles of a system, then it appears in all factorisations
- On the contrary, non-prime systems can sometimes be replaced
- So prime systems are irreplaceable building blocks
- We don't know if prime systems exist yet!
- But we know several nonprimes, for instance 



# More interesting classes of nonprimes

## Work by Johan Couturier, bien joué !

- If $A$ is disconnected, then $A$ is not prime
- If $A$ is connected but of period $> 1$, then $A$ is not prime
- If $A$ is connected of period $1$, but

$$\gcd(A) = \gcd\{\#\text{preimages of } a : a \in A\} > 1$$

  then $A$ is not prime

- In particular, systems consisting of sums of cycles (i.e., the asymptotic behaviours of any system) are nonprime

# Is primality decidable?

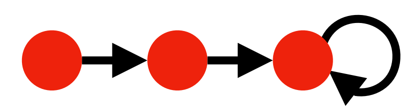
## Most. Annoying. Open. Problem. Ever. 😡

- We do not know an algorithm for primality testing!
- Nonprimes are recursively enumerable
  - Enumerate systems $A$, $B$ to find a counterexample to the primality of $P$, i.e., $P \mid AB$ but $P \nmid A$ and $P \nmid B$
  - No known way to bound the size of counterexamples
- Fun fact: if primality is undecidable, then primes do exist 😄

# Open problems

# Open problems

## Algebraic ones

- Do prime systems exist at all? Is primality decidable?
- Is this particular guy here prime? 
- What is the complexity of deciding if $A \mid B$?
  And deciding if $A$ is irreducible?
- Does it make any sense to adjoin the additive inverses in order to obtain a ring?
- Is it useful to find nondeterministic dynamical system (i.e., arbitrary graph) solutions to equations?
- Semirings of infinite discrete-time dynamical systems

# Open problems

## Solving equations

- Find larger classes of solvable equations,
  e.g., by number of variables or degree of the polynomials
- Discover classes of equations solvable efficiently
  - Probably very hard for systems in succinct form
- Find out if there exist decidable equations harder than $\mathbf{NP}$
  - It would feel strange to jump from $\mathbf{NP}$ to undecidable

Thanks for your attention!

Merci de votre attention !

# Any questions?