Composing behaviours in the semiring of dynamical systems

Antonio E. Porreca
Aix-Marseille Université &
Laboratoire d’Informatique et Systèmes 🇫🇷
aeporreca.org

Composing behaviours in the semiring of dynamical systems

Presented by
Florian Bridoux

Aix-Marseille Université &
Laboratoire d'Informatique et Systèmes 🇫🇷
aeporreca.org

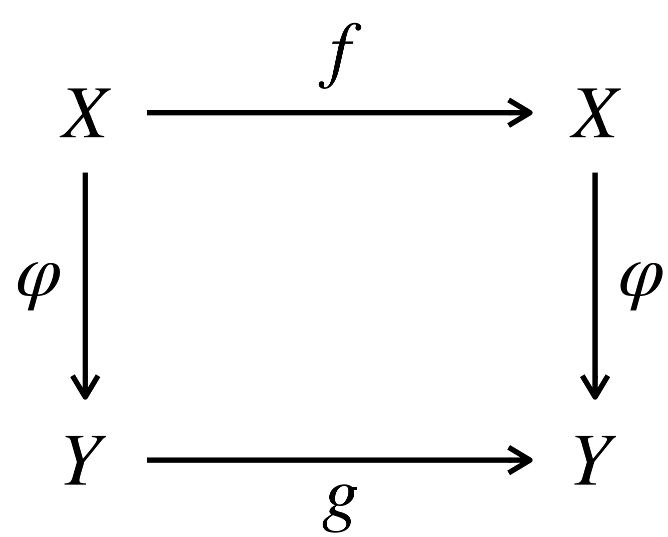
A collaboration between

- Florian Bridoux (Aix-Marseille Université & LIS 🇫🇷)
- Alberto Dennunzio (Università degli Studi di Milano-Bicocca 🇮🇹)
- Valentina Dorigatti (Università degli Studi dell'Insubria 🇮🇹)
- Enrico Formenti (Université Nice Sophia Antipolis & I3S 🇫🇷)
- Maximilien Gadouleau (Durham University 🇬🇧)
- Luca Manzoni (Università degli Studi di Trieste 🇮🇹)
- Antonio E. Porreca (Aix-Marseille Université & LIS 🇫🇷)

Finite dynamical systems and their category

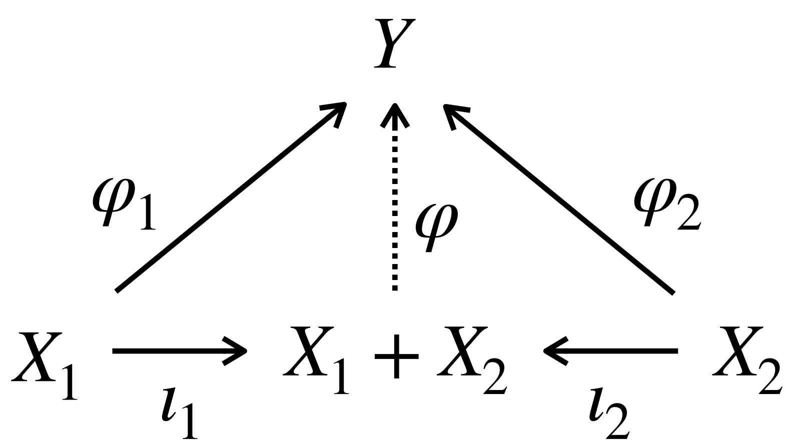
Finite dynamical systems

- A finite dynamical system is just a finite set X with a transition function $f\colon X \to X$
- The category $\mathbf{D}$ of finite dynamical systems has
  - as objects, the dynamical systems (X, f) themselves
  - as arrows between (X, f) and (Y, g), the functions $\varphi\colon X \to Y$ that make the diagram commute:



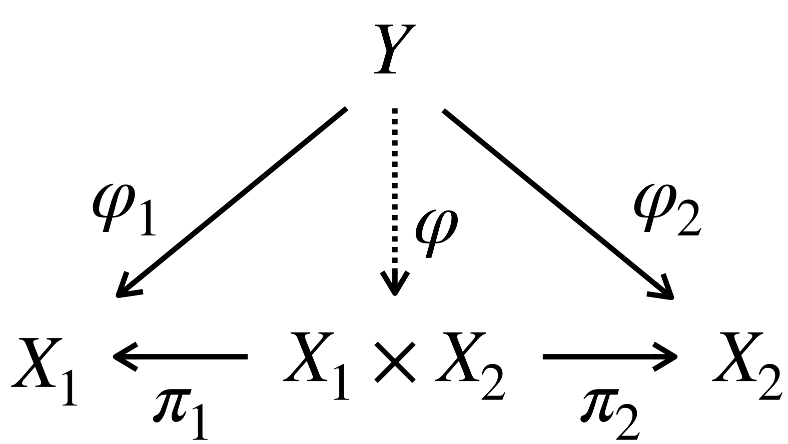
The category $\mathbf{D}$ of finite dynamical systems

- Has sums (coproducts) and initial objects



$$X \xleftarrow{\;!\;} \mathbf{0}$$

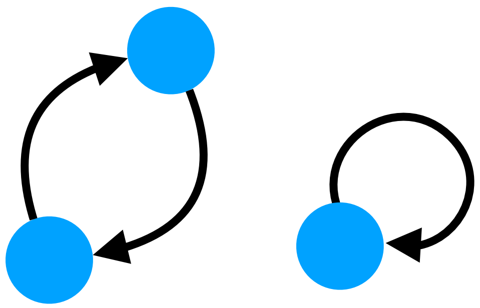
- Has products and terminal objects



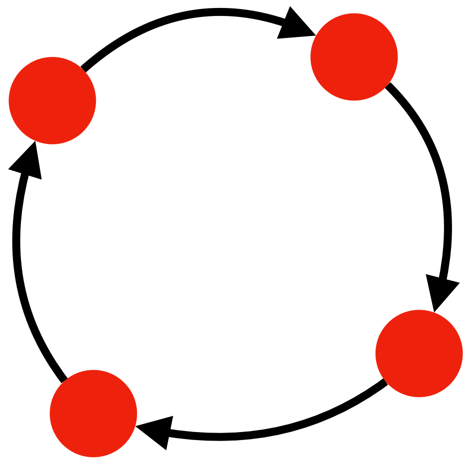
$$X \xrightarrow{\;!\;} \mathbf{1}$$

More concretely…

Sum in $\mathbf{D}$ = disjoint union

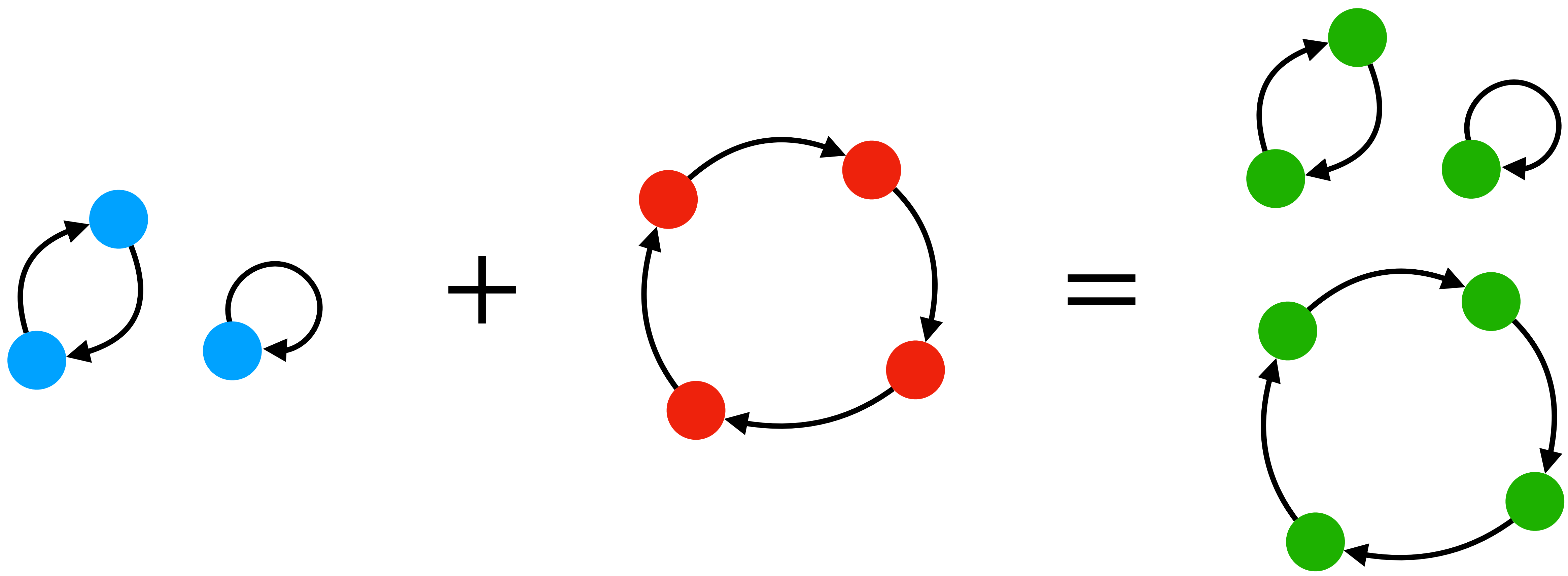


$+$

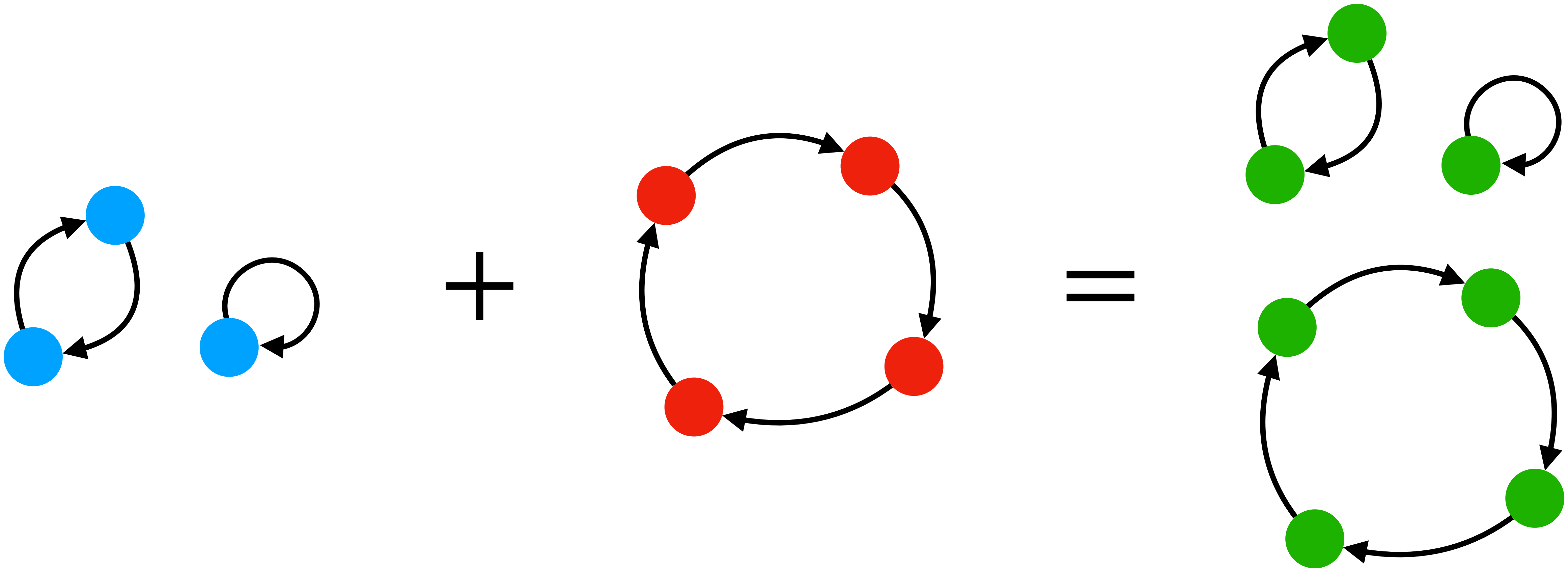


$=$

Sum in $\mathbf{D}$ = disjoint union

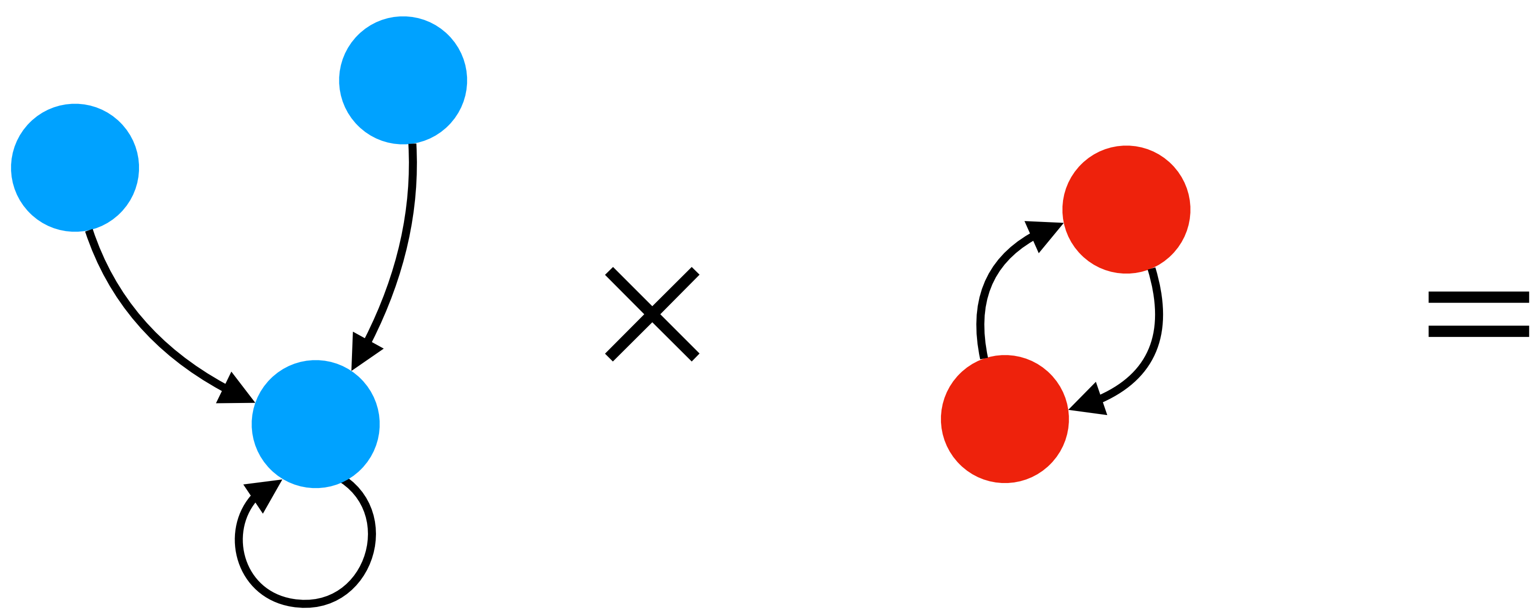


Sum in $\mathbf{D}$ = disjoint union

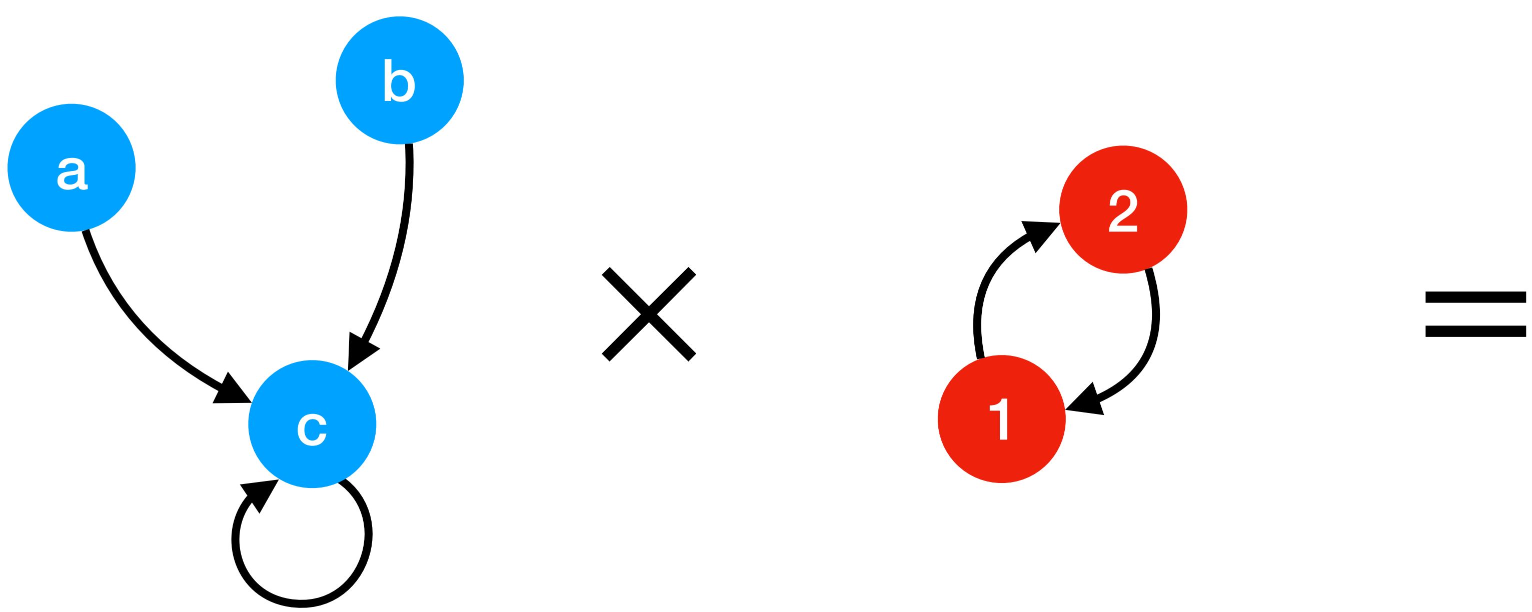


identity = $\mathbf{0}$ = $\varnothing$, the empty dynamical system

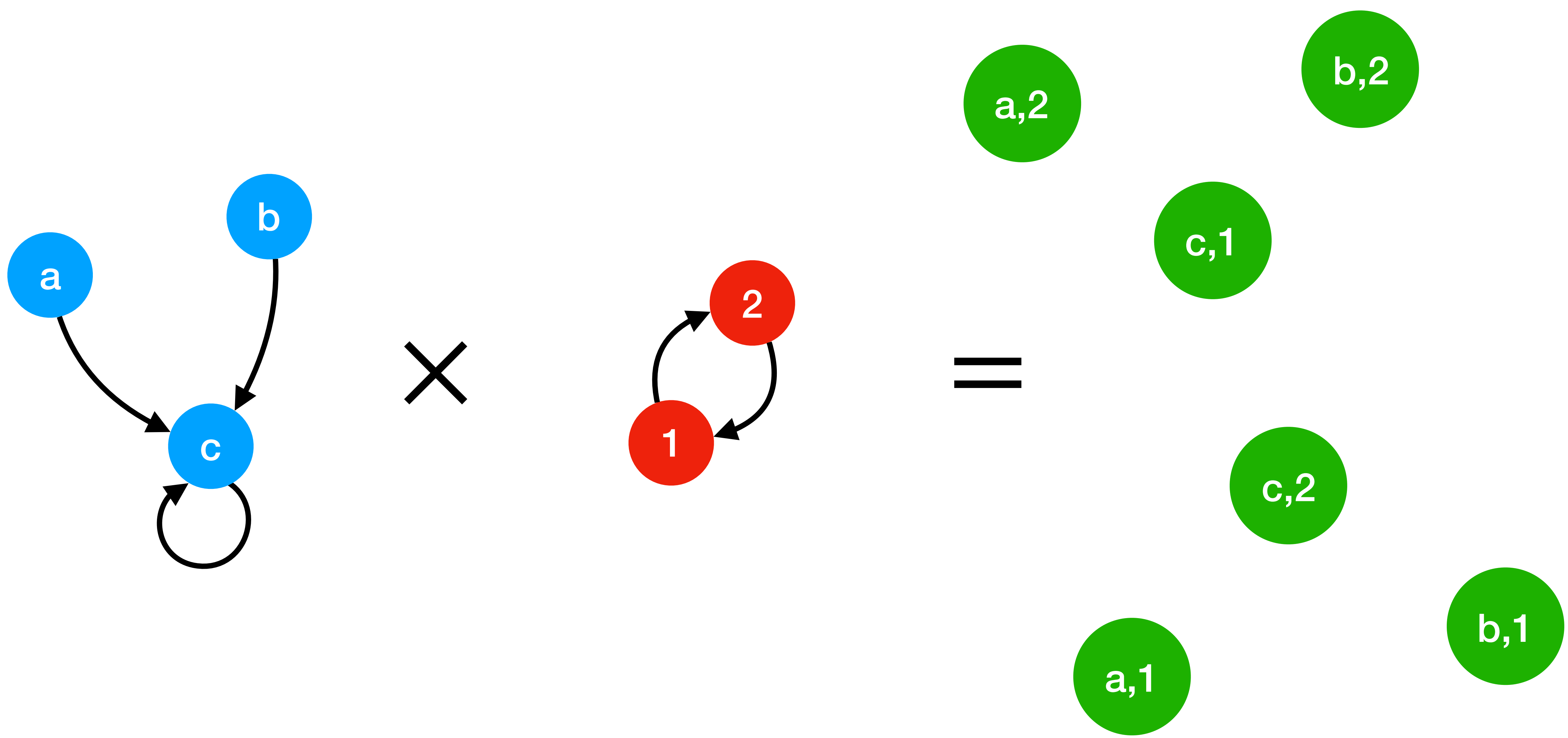
Product in $\mathbf{D}$ = cartesian product



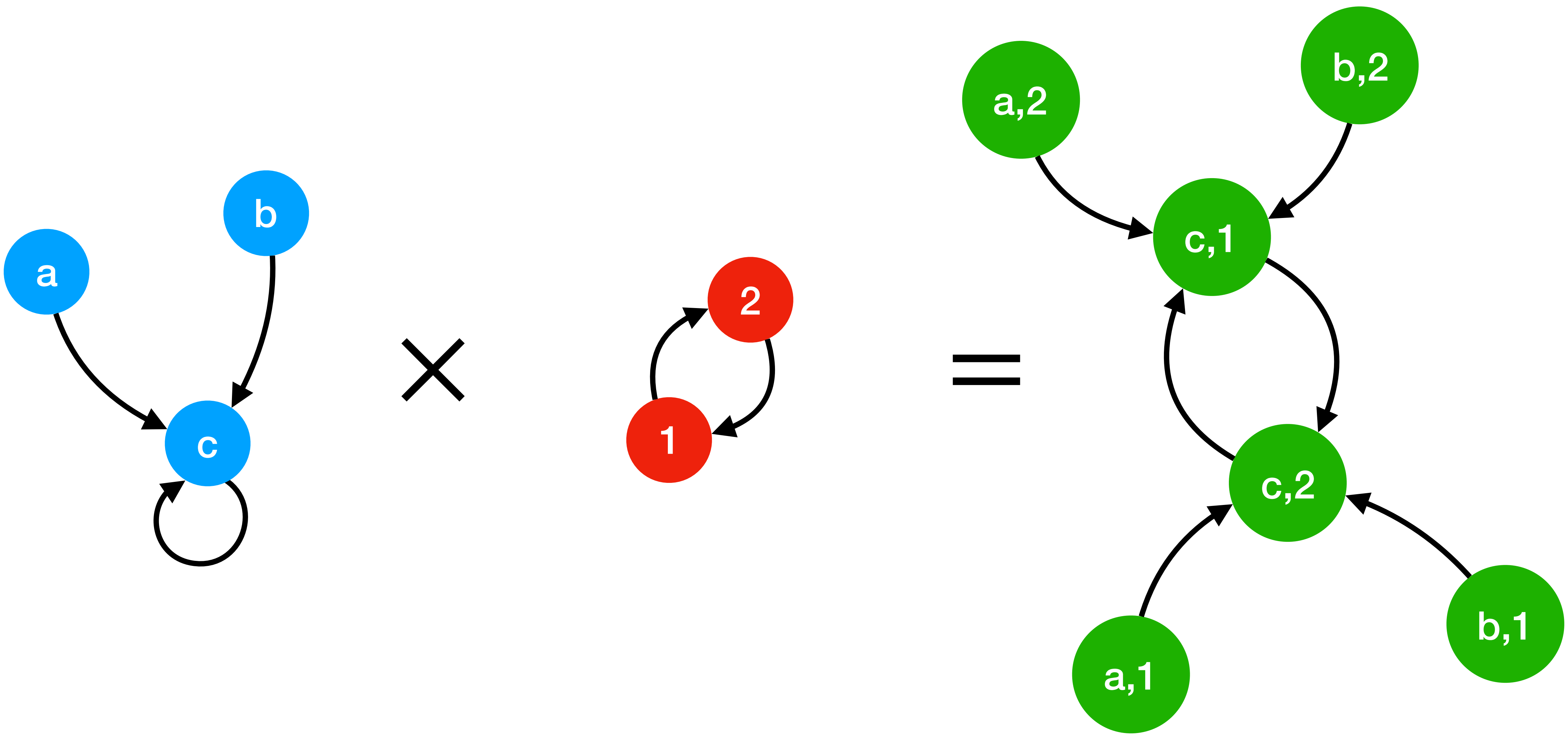
Product in $\mathbf{D}$ = cartesian product



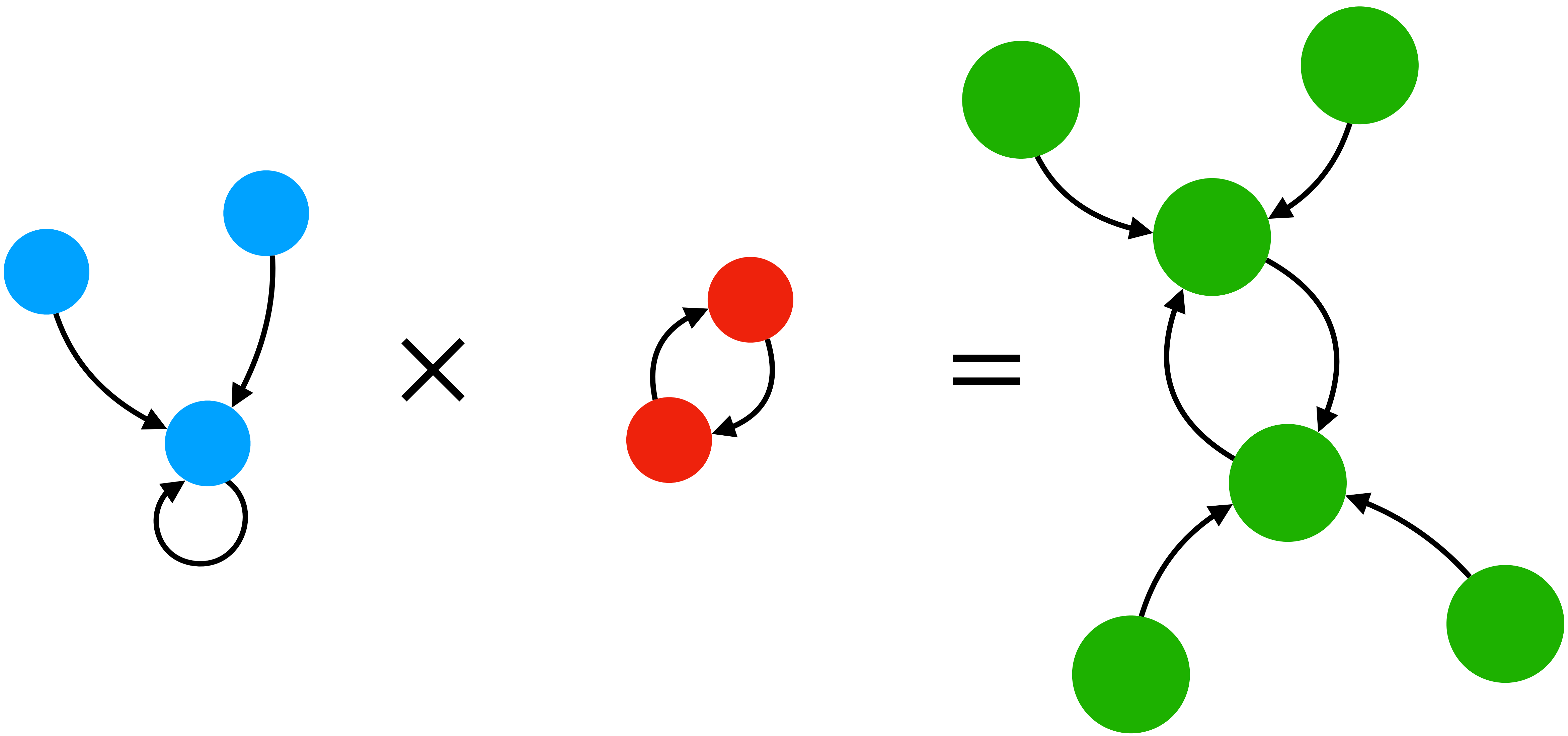
Product in $\mathbf{D}$ = cartesian product



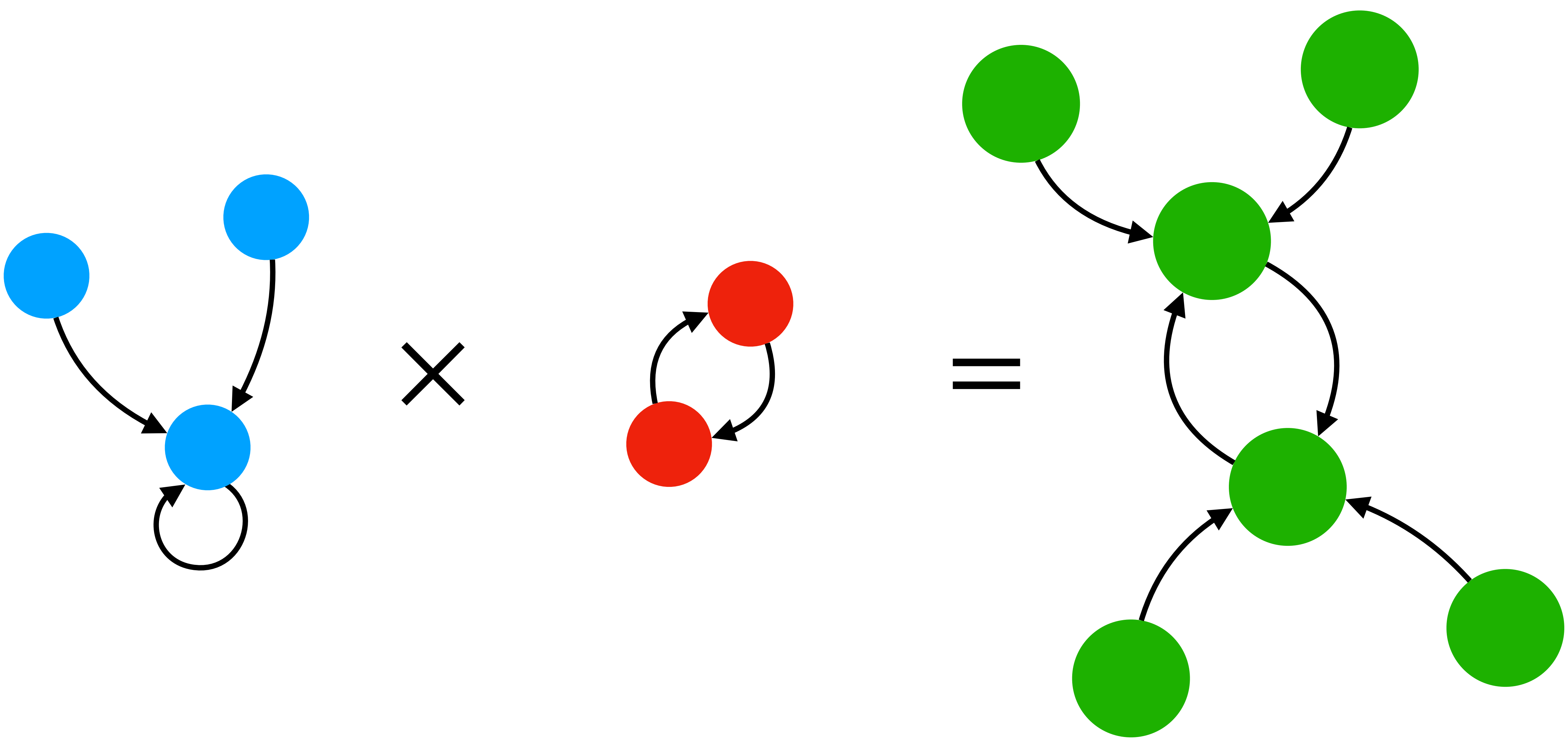
Product in $\mathbf{D}$ = cartesian product

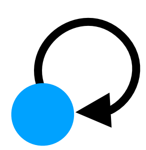


Product in $\mathbf{D}$ = cartesian product



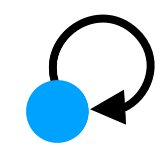
Product in $\mathbf{D}$ = cartesian product



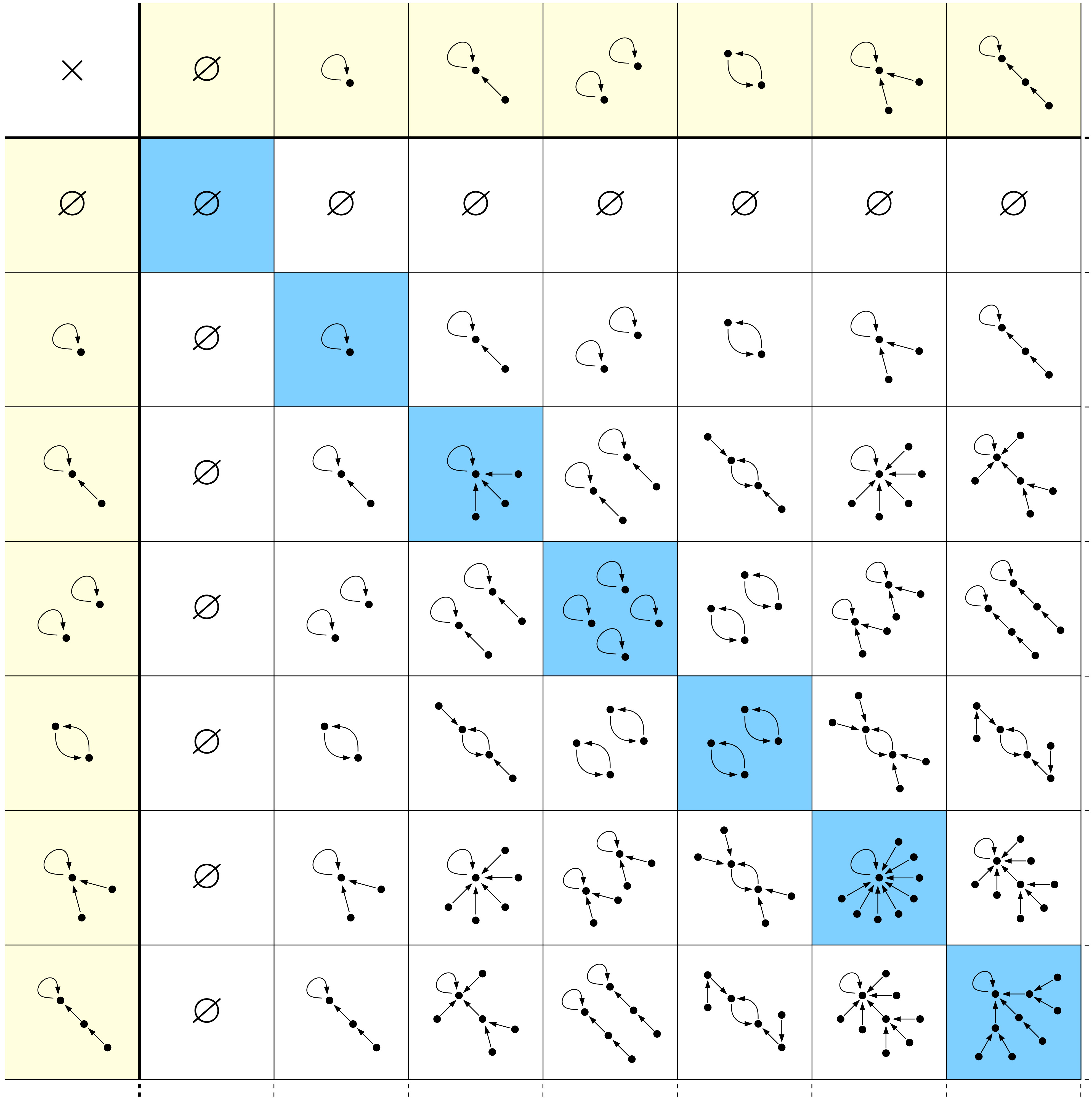
identity = $\mathbf{1}$ = 

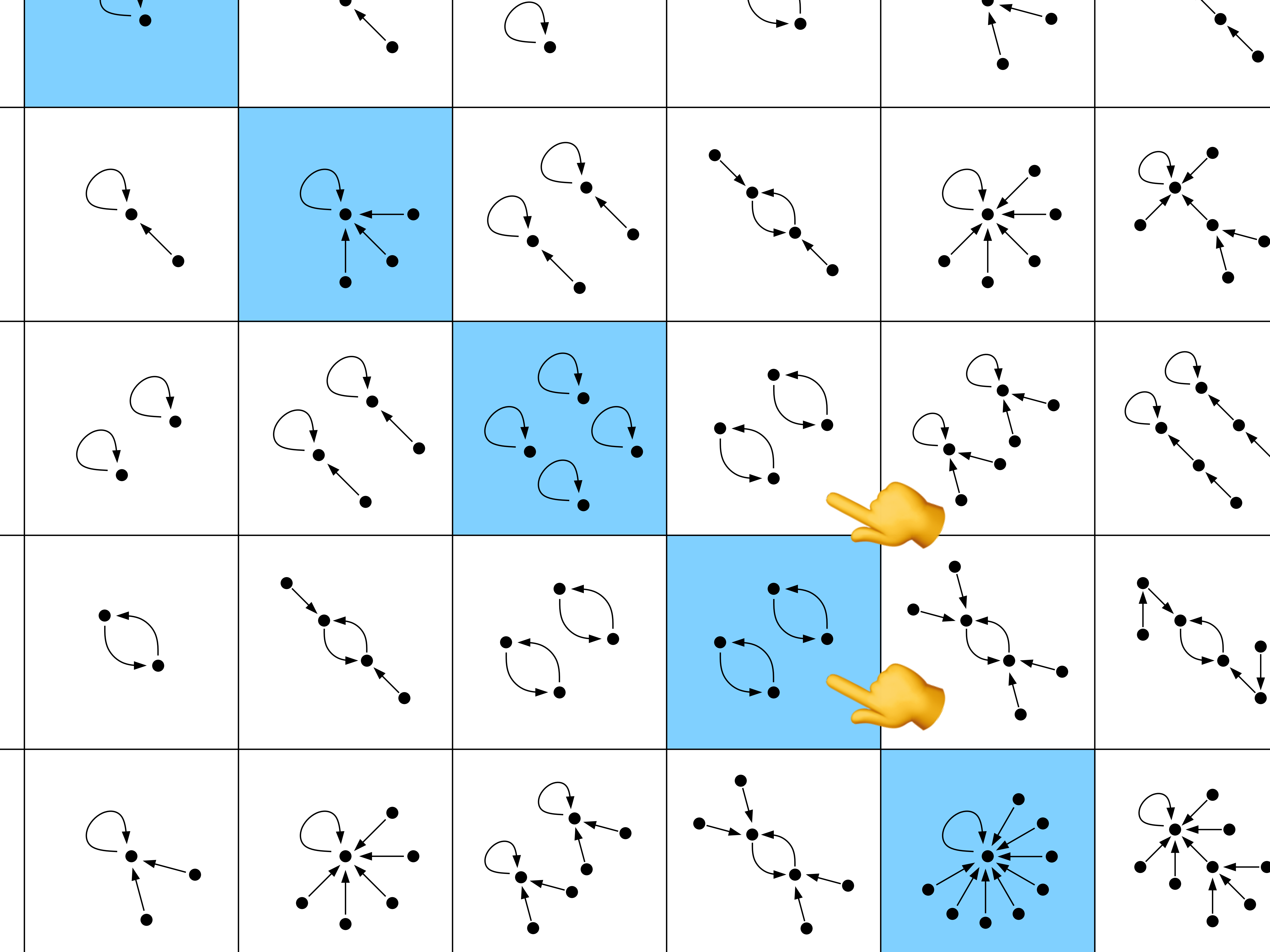
The semiring of finite dynamical systems

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

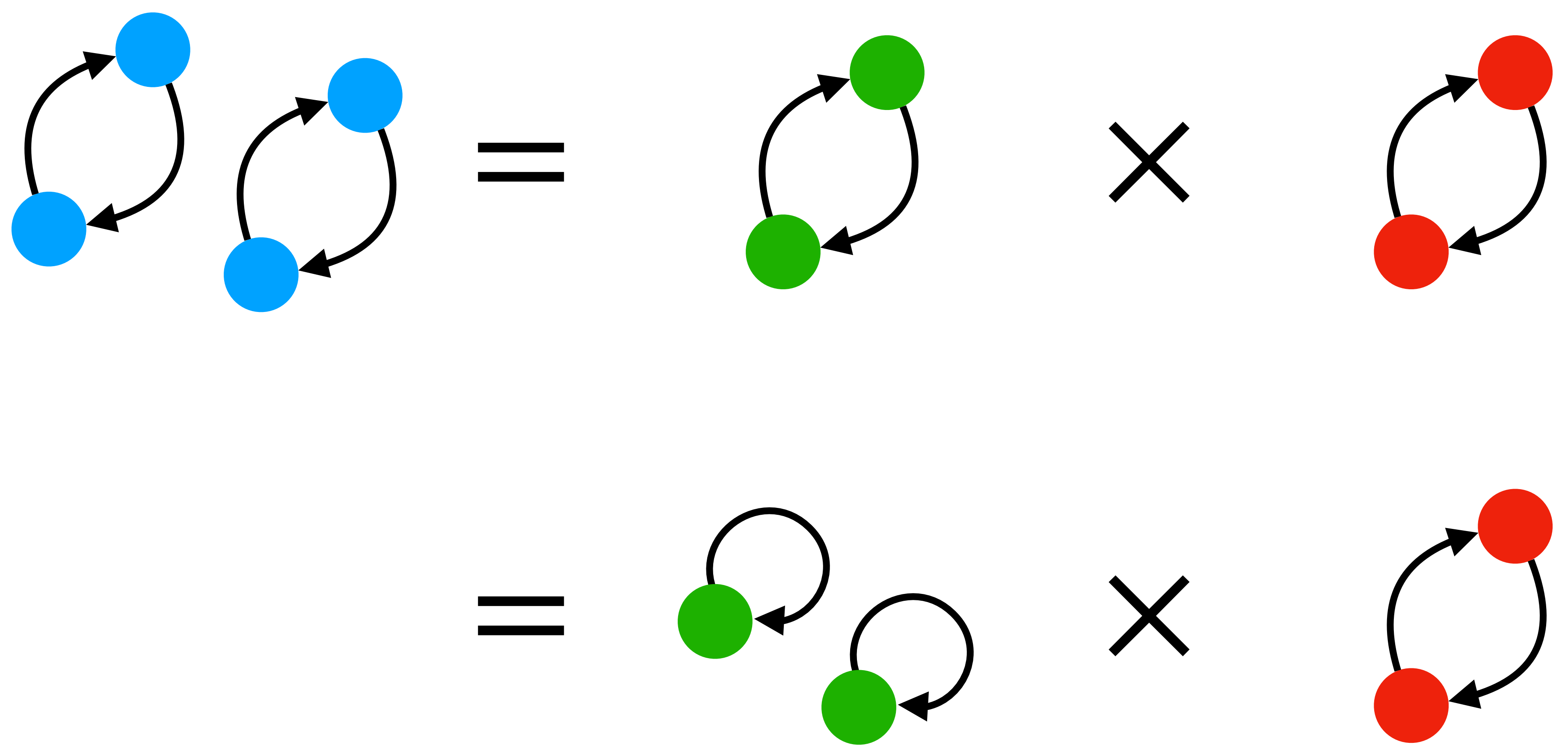
- The finite dynamical system modulo isomorphism are an infinite set $\mathbf{D}$ which is a commutative semiring:
    - $(\mathbf{D}, +)$ is a commutative monoid with identity $\mathbf{0} = \varnothing$
    - $(\mathbf{D}, \times)$ is a commutative monoid with identity $\mathbf{1} =$ 
    - Distributivity: $x(y + z) = xy + xz$
    - Absorption: $\mathbf{0}x = \mathbf{0}$
- This semiring is not a ring, because there are no additive inverses

Multiplication table of $\mathbf{D}$





⚠️ No unique factorisation into irreducible elements! ⚠️

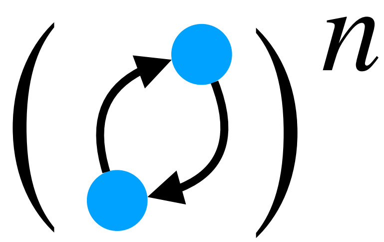


Theorem (Gadouleau)

For each n, there exist a dynamical system with at least n factorisations

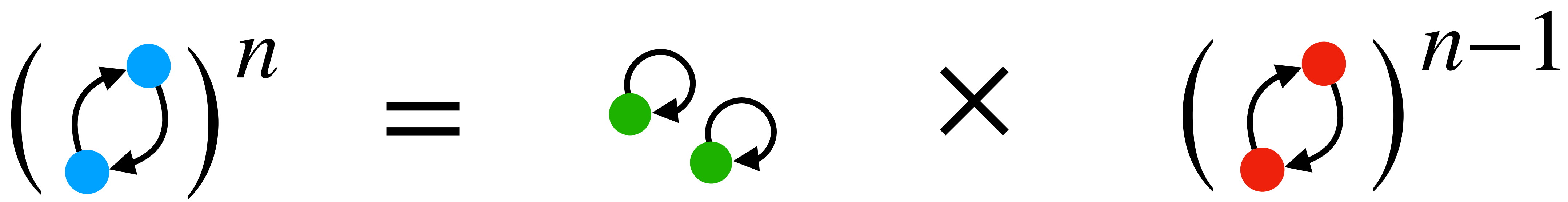
Theorem (Gadouleau)

For each n, there exist a dynamical system with at least n factorisations



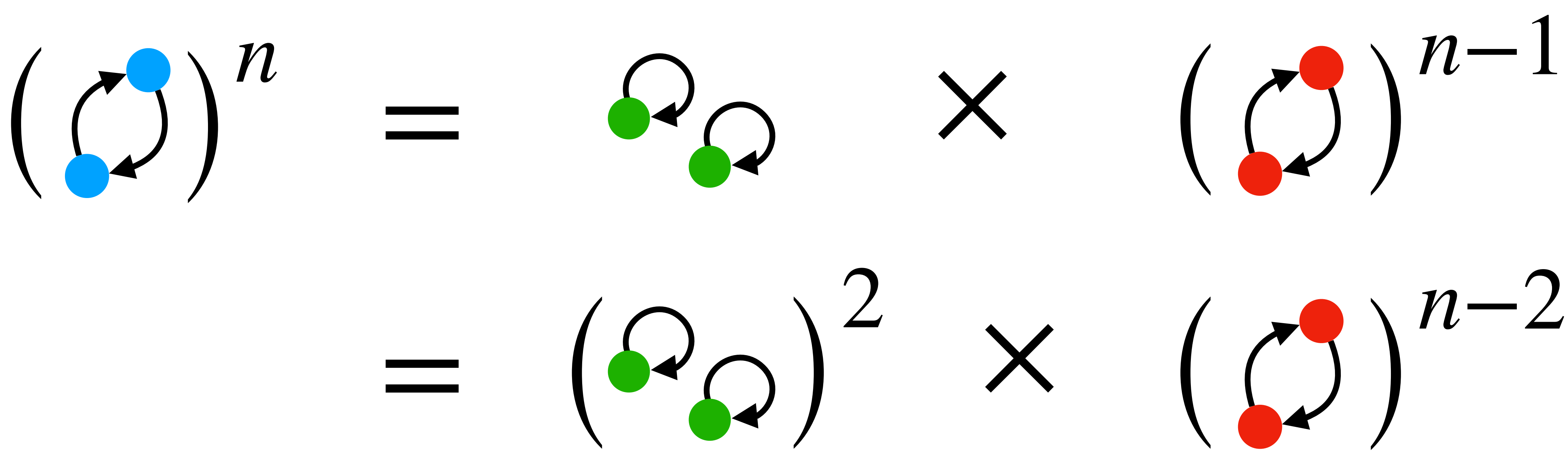
Theorem (Gadouleau)

For each n, there exist a dynamical system with at least n factorisations



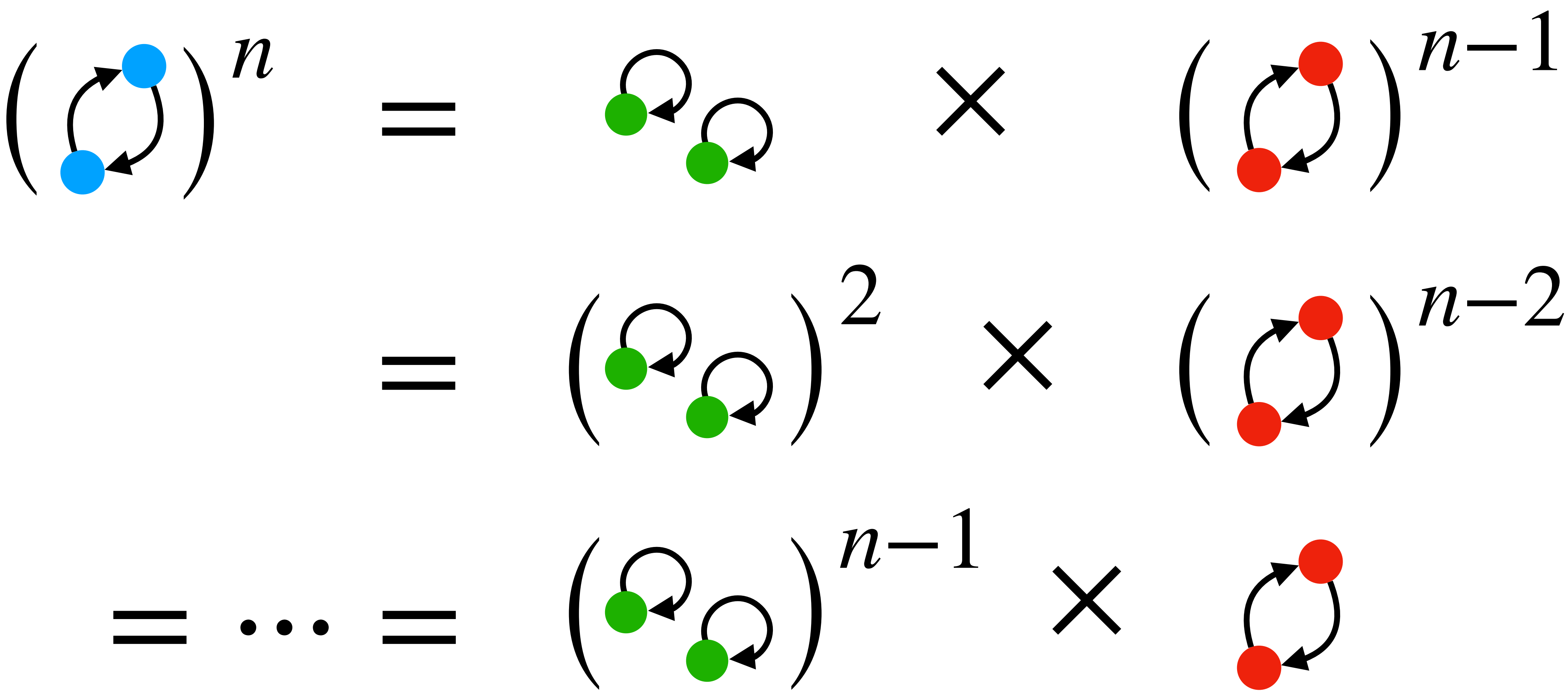
Theorem (Gadouleau)

For each n, there exist a dynamical system with at least n factorisations



Theorem (Gadouleau)

For each n, there exist a dynamical system with at least n factorisations



The majority of dynamical systems is irreducible:

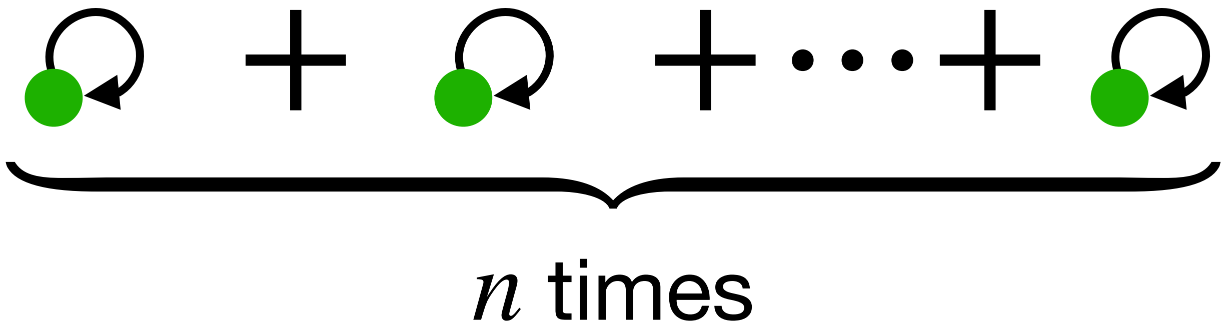
$$\lim_{n\to\infty} \frac{\text{reducible dyn sys over } n \text{ points}}{\text{total dyn sys over } n \text{ points}} = 0$$

Proof idea (Dorigatti)

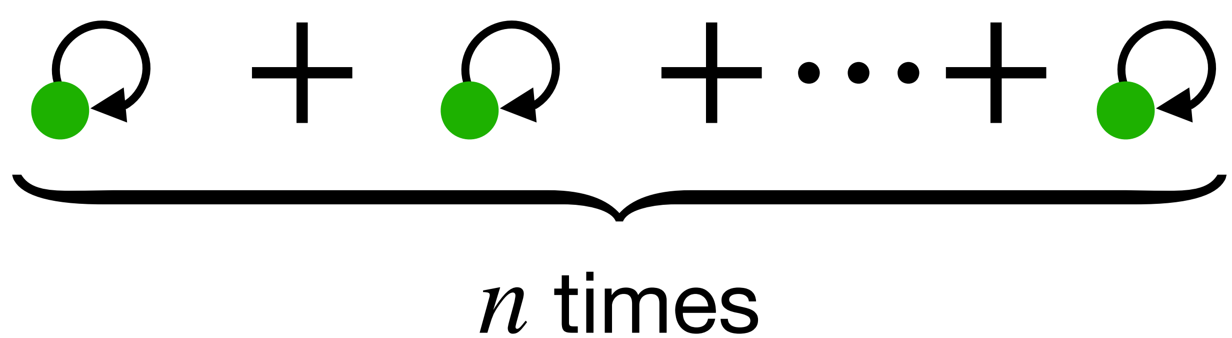
- It is a simple combinatorial argument
- There are exponentially many dynamical systems (modulo isomorphism) over n points, asymptotically $cd^n/\sqrt{n}$ with $c \approx 0.4$ and $d \approx 3$…
- …and “not enough” products in the upper-left corner of the multiplication table, so the majority must be irreducible

The semiring $\mathbf{D}$ contains the natural numbers $\mathbb{N}$ as a subsemiring

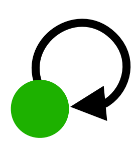
A monomorphism $\mathbb{N} \to \mathbf{D}$

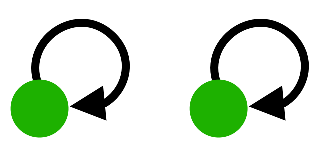
$\varphi(n) =$ 

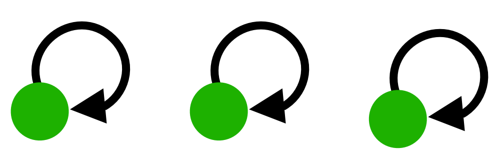
A monomorphism $\mathbb{N} \to \mathbf{D}$

$\varphi(n) =$ 

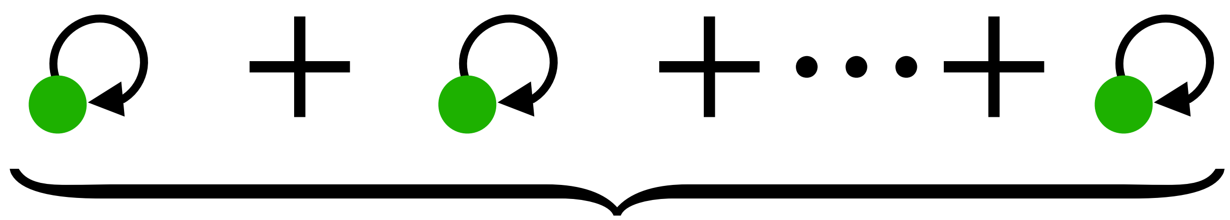
$0 \mapsto \emptyset$

$1 \mapsto$ 

$2 \mapsto$ 

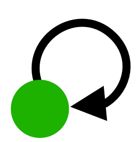
$3 \mapsto$ 

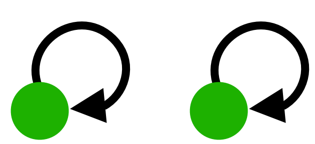
A monomorphism $\mathbb{N} \to \mathbf{D}$

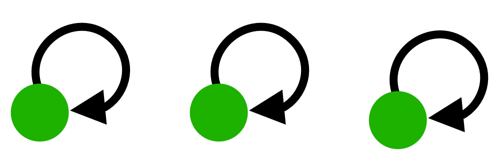
$\varphi(n) =$ 

n times

$0 \mapsto \emptyset$

$1 \mapsto$ 

$2 \mapsto$ 

$3 \mapsto$ 

$$\varphi(0) = \mathbf{0}$$

$$\varphi(1) = \mathbf{1}$$

$$\varphi(x + y) = \varphi(x) + \varphi(y)$$

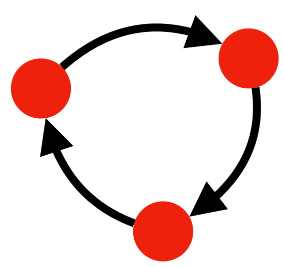
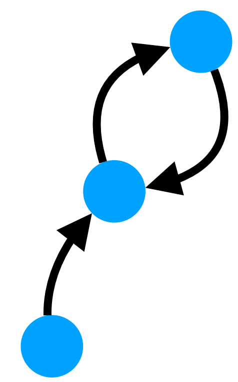
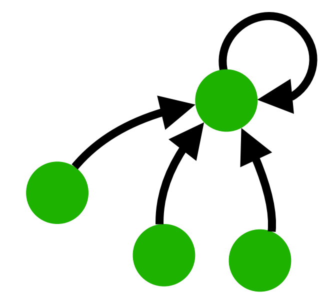
$$\varphi(xy) = \varphi(x) \times \varphi(y)$$

Some subsemirings of $\mathbf{D}$

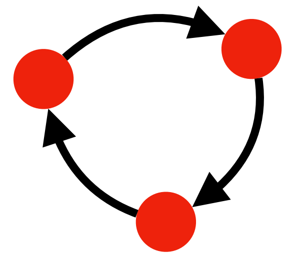
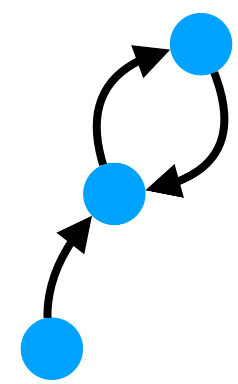
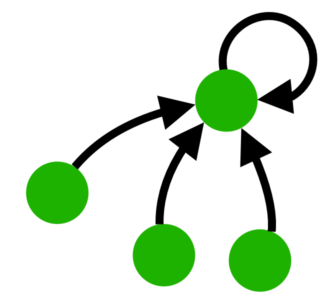
- The natural numbers $\mathbb{N}$
- The bijections, aka dynamics only containing cycles (including fixed points), aka asymptotic behaviours of dynamical systems
- Dynamical systems without limit cycles of length > 1

Polynomial equations over $\mathbf{D}[X_1, \ldots, X_m]$

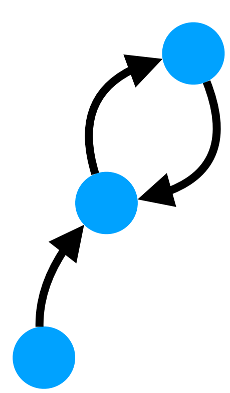
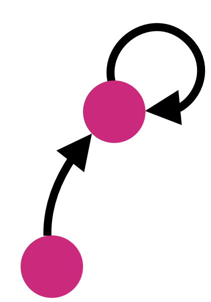
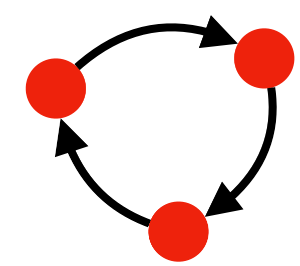
Polynomial equations for the analysis of complex behaviours

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

Polynomial equations for the analysis of complex behaviours

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

one solution:

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

Polynomial equations in semirings vs rings

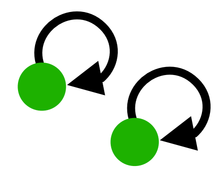
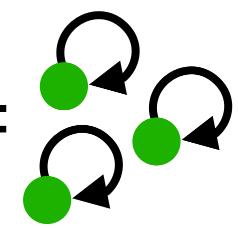
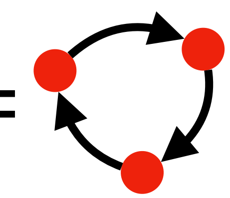
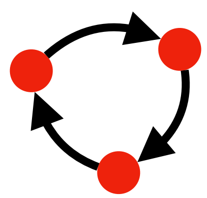
- A ring has additive inverses (aka, it has subtraction)
- So each polynomial equation in a ring can be written as $p(\overrightarrow{X}) = 0$
- This is not the case for our semiring, which has no subtraction
- So the general polynomial equation has the form $p(\overrightarrow{X}) = q(\overrightarrow{X})$ with two polynomials $p, q \in \mathbf{D}[\overrightarrow{X}]$

Solvability
of polynomial equations
over $\mathbf{D}$ is undecidable

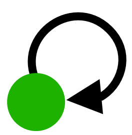
Polynomial equations over $\mathbf{D}$ are undecidable

- By reduction from the unsolvability of diophantine equations over $\mathbb{N}$ (Hilbert's 10th problem)
- Not an immediate consequence of having a subsemiring isomorphic to $\mathbb{N}$
- For example, the solvability of polynomial equations over $\mathbb{R}$ is decidable, even trivial over $\mathbb{C}$, even if they contain $\mathbb{N}$

Natural equations with non-natural solutions

- Let $p(X, Y) = 2X^2 =$  X^2, $q(X, Y) = 3Y =$  Y
- Then $2X^2 = 3Y$ has the non-natural solution $X =$ , $Y = 2$ 
- But it also has a natural solution, namely $X = 3$, $Y = 6$
- The natural solution is the size of the dynamical systems of the non-natural one
- This is not a coincidence!

The function "size" $|\cdot|: \mathbf{D} \to \mathbb{N}$ is a semiring homomorphism

- $|\varnothing| = 0$
- |  | $= 1$
- Since $+$ is the disjoint union, $|x + y| = |x| + |y|$
- Since $\times$ is the cartesian product, $|xy| = |x| \times |y|$

Notation for polynomials $p \in \mathbf{D}[\overrightarrow{X}]$ of degree $\leq d$ with $\overrightarrow{X} = (X_1, \ldots, X_k)$

$$p = \sum_{\vec{i} \in \{0,\ldots,d\}^k} a_{\vec{i}} \overrightarrow{X}^{\vec{i}}$$

where $\overrightarrow{X}^{\vec{i}} = \prod_{j=1}^{k} X_j^{i_j}$

Solvability of polynomial equations with natural coefficients

Theorem

- If a polynomial equation over $\mathbb{N}[X_1, \ldots, X_k]$ has a solution in $\mathbf{D}^k$, then it also has a solution in $\mathbb{N}^k$
- That is, in the largest semiring $\mathbf{D}$ we may find extra solutions to natural polynomial equations, but only if there is already a natural one

Proof

- Let $p(\overrightarrow{X}) = q(\overrightarrow{X})$ with $p, q \in \mathbb{N}[\overrightarrow{X}]$ and suppose $p(\overrightarrow{D}) = q(\overrightarrow{D})$ for some $\overrightarrow{D} \in \mathbf{D}^k$:

$$\sum_{i \in \{0,\ldots,d\}^k} a_{\vec{i}} \overrightarrow{D}^{\vec{i}} = \sum_{i \in \{0,\ldots,d\}^k} b_{\vec{i}} \overrightarrow{D}^{\vec{i}}$$

- Apply the size function $|\cdot|$, which is a homomorphism:

$$\left| \sum_{i \in \{0,\ldots,d\}^k} a_{\vec{i}} \overrightarrow{D}^{\vec{i}} \right| = \left| \sum_{i \in \{0,\ldots,d\}^k} b_{\vec{i}} \overrightarrow{D}^{\vec{i}} \right| \quad \Rightarrow \quad \sum_{i \in \{0,\ldots,d\}^k} a_{\vec{i}} |\overrightarrow{D}^{\vec{i}}| = \sum_{i \in \{0,\ldots,d\}^k} b_{\vec{i}} |\overrightarrow{D}^{\vec{i}}|$$

- where $|\overrightarrow{D}^{\vec{i}}| = \prod_{j=1}^{k} |D_j|^{i_j}$; notice that $|a_{\vec{i}}| = a_{\vec{i}}$ and $|b_{\vec{i}}| = b_{\vec{i}}$ since they are $\mathbb{N}$

- But that means $p(|\overrightarrow{D}|) = q(|\overrightarrow{D}|)$ where $|\overrightarrow{D}| = (|D_1|, \ldots, |D_k|)$, so $|\overrightarrow{D}|$ is a natural solution

Unsolvability of polynomial equations in $\mathbf{D}[\overrightarrow{X}]$

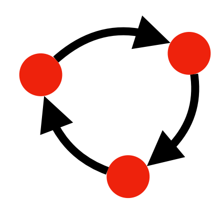
- A polynomial equation with natural coefficients has a solutions over the dynamical systems if and only if it has a natural solution

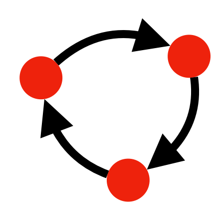
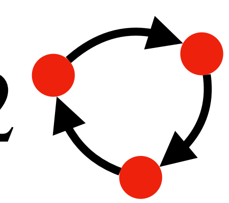
- Being able to solve polynomial equations over $\mathbf{D}[\overrightarrow{X}]$ would then contradict the unsolvability of Hilbert's 10th problem

Equations with non-natural coefficients

- Notice that equations with non-natural coefficients might have only non-natural solutions

- For instance

$$X^2 = Y +$$ 

- has the non-natural solution $X =$  , $Y = 2$  but no natural solutions

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

Nondeterministic algorithm for $p(\overrightarrow{X}) = D$ with $D \in \mathbf{D}$

- Since $+$ and $\times$ are monotonic wrt the sizes of the operands, each X_i in a solution to the equation has size $\leq |D|$
- So it suffices to guess a dynamical system of size $\leq |D|$ for each variable in polynomial time, then calculate LHS
- Finally we check whether LHS and RHS are isomorphic, exploiting the fact that graph isomorphism is in $\mathbf{NP}$
- Only one caveat: if at any time during the calculations the LHS becomes larger than $|D|$, we halt and reject (otherwise the algorithm might take exponential time)

Solvability of a systems of linear equations with constant RHS is $\mathbf{NP}$-complete

Systems of linear equations are $\mathbf{NP}$-complete

- In $\mathbf{NP}$ by the same algorithm as above, only with multiple equations
- $\mathbf{NP}$-hard by reduction from the $\mathbf{NP}$-complete problem **One-in-three-3SAT**: given a 3CNF formula φ, is there a satisfying assignment such that exactly one literal per clause is true?
- For each variable x in φ we have an equation $x + x' = 1$, forcing exactly one variable between x and x' to be 0 and the other to be 1
- For each clause, for instance $(x \vee \neg y \vee z)$, we have an equation, for instance $x + y' + z = 1$, which forces the solution to be a satisfying assignment with one true literal per clause

Solvability of an equation of unbounded degree with constant RHS is $\mathbf{NP}$-complete

Reducing n equations with RHS $= 1$ to a single equation

- We multiply the LHS and RHS of the linear equations of the **One-in-three-3SAT** reduction:

$$\begin{cases} p_1(\overrightarrow{X}) = 1 \\ \vdots \\ p_m(\overrightarrow{X}) = 1 \end{cases} \iff p_1(\overrightarrow{X}) \times \cdots \times p_m(\overrightarrow{X}) = 1$$

- The new equation has the same solutions of the old one: each $p_i(\overrightarrow{X})$ must be 1

- Thus, solving equations of unbounded degree with constant RHS is $\mathbf{NP}$-complete

Is a single linear equation $\mathbf{NP}$-complete?

- Over a ring that is also an integral domain (no nonzero elements a, b such that $ab = 0$), we can always have 0 as RHS and reduce a system to a single equation:

$$\begin{cases} p_1(\overrightarrow{X}) = 0 \\ \vdots \\ p_m(\overrightarrow{X}) = 0 \end{cases} \iff p_1(\overrightarrow{X}) \times \cdots \times p_m(\overrightarrow{X}) = 0$$

- We cannot do that in our semiring $\mathbf{D}$ due to the lack of subtraction, even if there are no nontrivial zero divisors

Reducing a system of linear equations to a single one (Bridoux)

- Possible solution: given the system of linear equations

$$\begin{cases} p_1(\overrightarrow{X}) = q_1(\overrightarrow{X}) \\ \vdots \\ p_m(\overrightarrow{X}) = q_m(\overrightarrow{X}) \end{cases}$$

- find “linearly independent” elements $e_1, \ldots, e_m \in \mathbf{D}$ such that the equation

$$e_1 p_1(\overrightarrow{X}) + \cdots + e_m p_m(\overrightarrow{X}) = e_1 q_1(\overrightarrow{X}) + \cdots + e_m q_m(\overrightarrow{X})$$

- …has the same solutions of the original system

- Conjecture: it is possible to find the “linearly independent” $e_1, \ldots, e_m \in \mathbf{D}$

Open problems and work in progress

Open problems & WIP 1

- Find subclasses of polynomial equations that are solvable in polynomial time, or that are solvable but harder than $\mathbf{NP}$

- Find an $\mathbf{NP}$-complete equation problem which does not depend on the $\mathbf{NP}$-completeness of the same problem over the naturals

    - (Bridoux) Transforming a system of equations into a single equation having the same solutions (nontrivial over semirings)

- Conjecture (Gadouleau): there is a polynomial-time algorithm for computing $\sqrt[n]{x}$ when it exists

Open problems & WIP 2

- Is finding a factorisation $\mathbf{NP}$-hard?
- (Gadouleau) Counting factorisations
- More detailed algebraic analysis of the semiring $\mathbf{D}$ (find other subsemirings? ideals? generators? primes?)
- Conjecture (Guilhem Gamard @ LIS): maybe we can find an interpretation for category-theoretical exponentiation in $\mathbf{D}$

Bibliography

- Valentina Dorigatti, Algorithms and Complexity of the Algebraic Analysis of Finite Discrete Dynamical Systems, M.Sc. thesis, Università degli Studi di Milano-Bicocca, 2018

- Dennunzio, Dorigatti, Formenti, Manzoni, Porreca, Polynomial equations over finite, discrete-time dynamical systems, 13th International Conference on Cellular Automata for Research and Industry, ACRI 2018

- Dennunzio, Formenti, Margara, Montmirail, Riva, Solving equations on discrete dynamical systems, 16th International Conference on Computational Intelligence methods for Bioinformatics and Biostatistics, CIBB 2019

¡Gracias por su atención!

¡Thanks for your attention!