Proof equivalence in MLL is hard to decide

Willem Heijltjes and Robin Houston

Proof equivalence in MLL* is hard to decide

* classical multiplicative linear logic with units

Willem Heijltjes and Robin Houston

The plan

- **0915–1000** Background and overview
- **1115–1200** Outline of the proof

Main result

- The problem of deciding whether two MLL proofs are equivalent is PSPACE-complete.

- This is true even in the unit-*only* fragment.

- (In contrast equivalence can be easily decided without units, and also in the intuitionistic case with units.)

What is MLL?

- Multiplicative linear logic
- Every premise must be used once and once only
- No contraction or weakening
- negation is written $(-)^{\perp}$
- connectives $\otimes$, $⅋$
- corresponding to $\wedge$, $\vee$ in classical logic

MLL sequent calculus

$$\frac{}{\vdash p, p^{\perp}}\ \text{Ax}$$

$$\frac{\vdash \Gamma, A, B}{\vdash \Gamma, A \parr B}\ \parr$$

$$\frac{\vdash \Gamma, A \quad \vdash \Delta, B}{\vdash \Gamma, \Delta, A \otimes B}\ \otimes$$

When are proofs equivalent?

$$\dfrac{\dfrac{\Gamma, A, B, C, D}{\Gamma, A \parr B, C, D}\,\parr}{\Gamma, A \parr B, C \parr D}\,\parr \quad \sim \quad \dfrac{\dfrac{\Gamma, A, B, C, D}{\Gamma, A, B, C \parr D}\,\parr}{\Gamma, A \parr B, C \parr D}\,\parr$$

$$\dfrac{\dfrac{\Gamma, A \qquad \Delta, B, C, D}{\Gamma, \Delta, A \otimes B, C, D}\,\otimes}{\Gamma, \Delta, A \otimes B, C \parr D}\,\parr \quad \sim \quad \dfrac{\Gamma, A \qquad \dfrac{\Delta, B, C, D}{\Delta, B, C \parr D}\,\parr}{\Gamma, \Delta, A \otimes B, C \parr D}\,\otimes$$

$$\dfrac{\Gamma, A \qquad \dfrac{\Delta, B, C \qquad \Lambda, D}{\Delta, \Lambda, B, C \otimes D}\,\otimes}{\Gamma, \Delta, \Lambda, A \otimes B, C \otimes D}\,\otimes \quad \sim \quad \dfrac{\dfrac{\Gamma, A \qquad \Delta, B, C}{\Gamma, \Delta, A \otimes B, C}\,\otimes \qquad \Lambda, D}{\Gamma, \Delta, \Lambda, A \otimes B, C \otimes D}\,\otimes$$

MLL proof nets

$$\frac{}{\vdash p,\ p^{\perp}}\ \mathrm{Ax}$$

$$\frac{\vdash \Gamma,\ A,\ B}{\vdash \Gamma,\ A \parr B}\ \parr$$

$$\frac{\vdash \Gamma,\ A \quad \vdash \Delta,\ B}{\vdash \Gamma,\ \Delta,\ A \otimes B}\ \otimes$$

MLL proof nets

$$\frac{}{\vdash p, p^{\perp}}\,\mathrm{Ax}$$

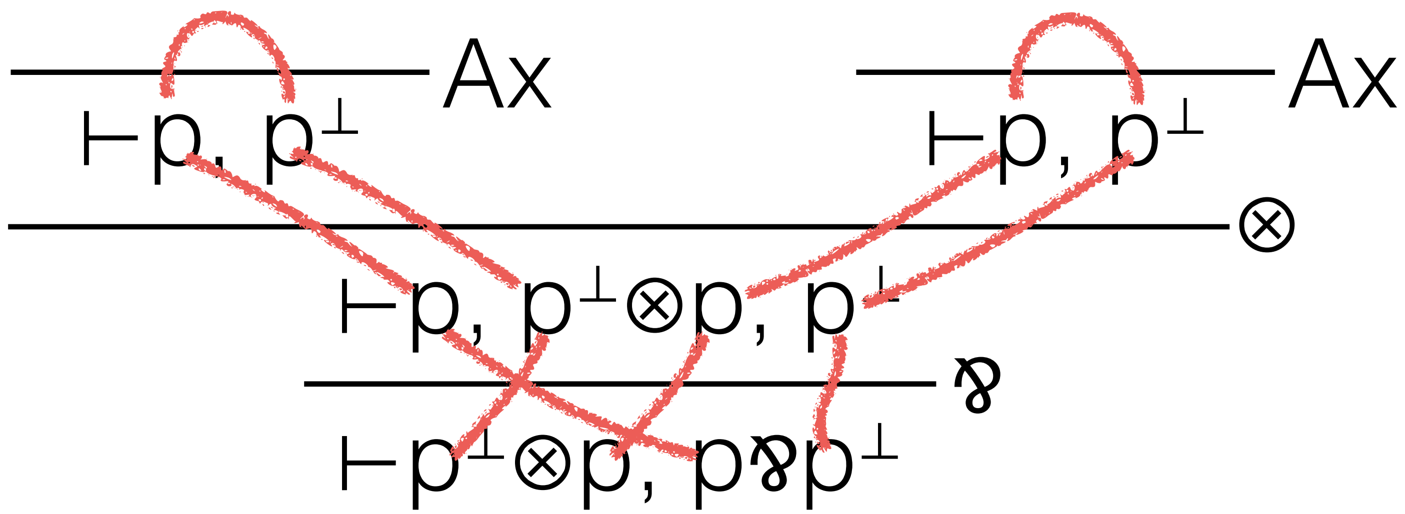
$$\frac{\vdash \Gamma, A, B}{\vdash \Gamma, A \parr B}\,\parr$$

$$\frac{\vdash \Gamma, A \qquad \vdash \Delta, B}{\vdash \Gamma, \Delta, A \otimes B}\,\otimes$$

MLL proof nets

$$\dfrac{\dfrac{}{\vdash p, p^{\perp}}\,Ax \qquad \dfrac{}{\vdash p, p^{\perp}}\,Ax}{\dfrac{\vdash p,\ p^{\perp} \otimes p,\ p^{\perp}}{\vdash p^{\perp} \otimes p,\ p \parr p^{\perp}}\,\parr}\,\otimes$$

MLL proof nets



MLL proof nets

$\vdash p^{\perp} \otimes p,\ p \parr p^{\perp}$

MLL proof nets

$$\vdash p^{\perp} \otimes p,\ p \parr p^{\perp}$$

MLL with units

The units are 1, $\bot$

$$\frac{\Gamma}{\Gamma, \bot}\,\bot \qquad\qquad \frac{}{1}\,1$$

Equivalence with units

$$\dfrac{\dfrac{\Gamma}{\Gamma, \bot_a}\,\bot}{\Gamma, \bot_a, \bot_b}\,\bot \quad\sim\quad \dfrac{\dfrac{\Gamma}{\Gamma, \bot_b}\,\bot}{\Gamma, \bot_a, \bot_b}\,\bot \qquad\qquad \dfrac{\dfrac{\Gamma, A, B}{\Gamma, A \parr B}\,\parr}{\Gamma, A \parr B, \bot}\,\bot \quad\sim\quad \dfrac{\dfrac{\Gamma, A, B}{\Gamma, A, B, \bot}\,\bot}{\Gamma, A \parr B, \bot}\,\parr$$

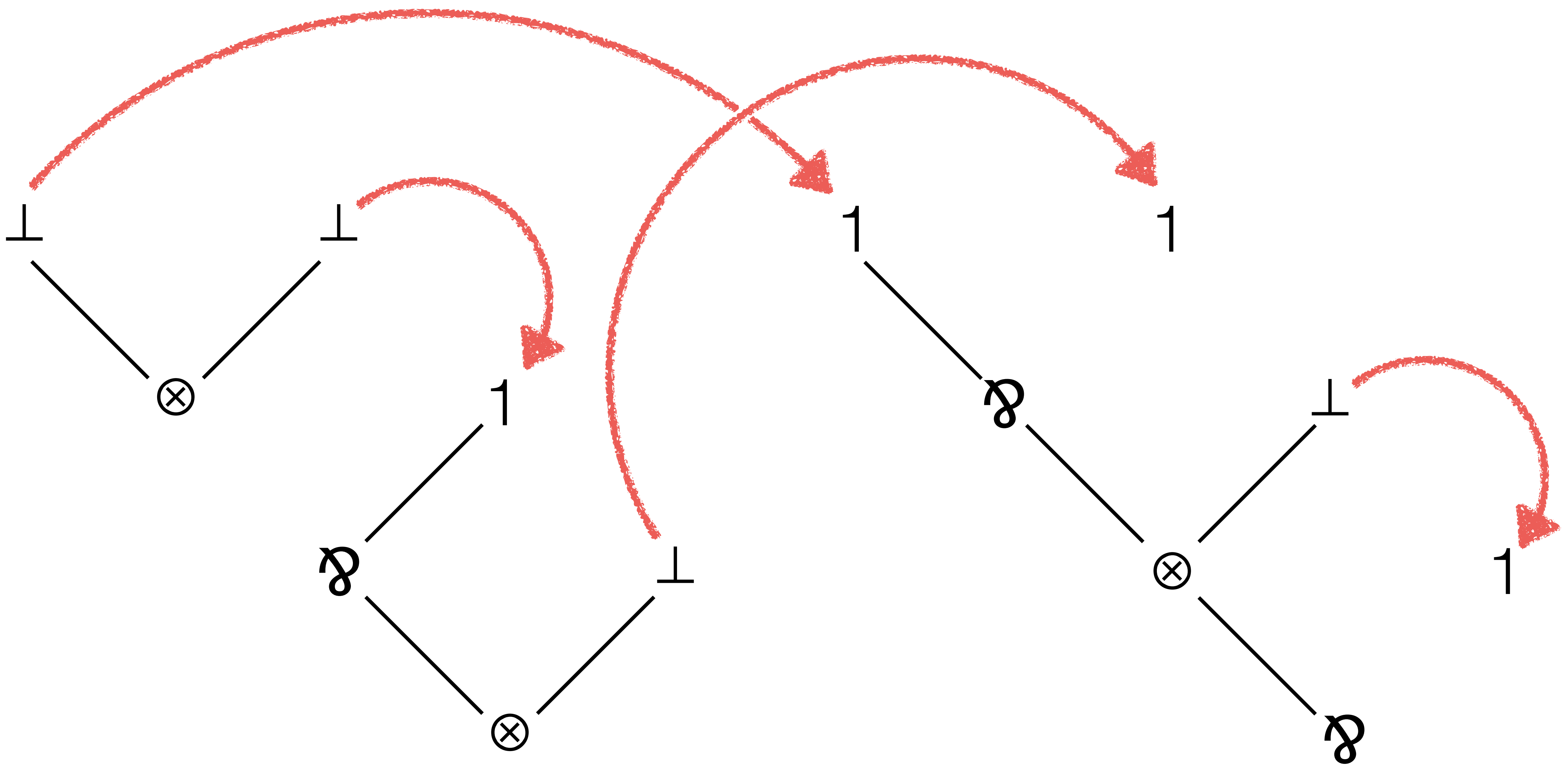
$$\dfrac{\dfrac{\Gamma, A}{\Gamma, A, \bot}\,\bot \qquad \Delta, B}{\Gamma, \Delta, A \otimes B, \bot}\,\otimes \quad\sim\quad \dfrac{\dfrac{\Gamma, A \qquad \Delta, B}{\Gamma, \Delta, A \otimes B}\,\otimes}{\Gamma, \Delta, A \otimes B, \bot}\,\bot \quad\sim\quad \dfrac{\Gamma, A \qquad \dfrac{\Delta, B}{\Delta, B, \bot}\,\bot}{\Gamma, \Delta, A \otimes B, \bot}\,\otimes$$

Proof nets for units

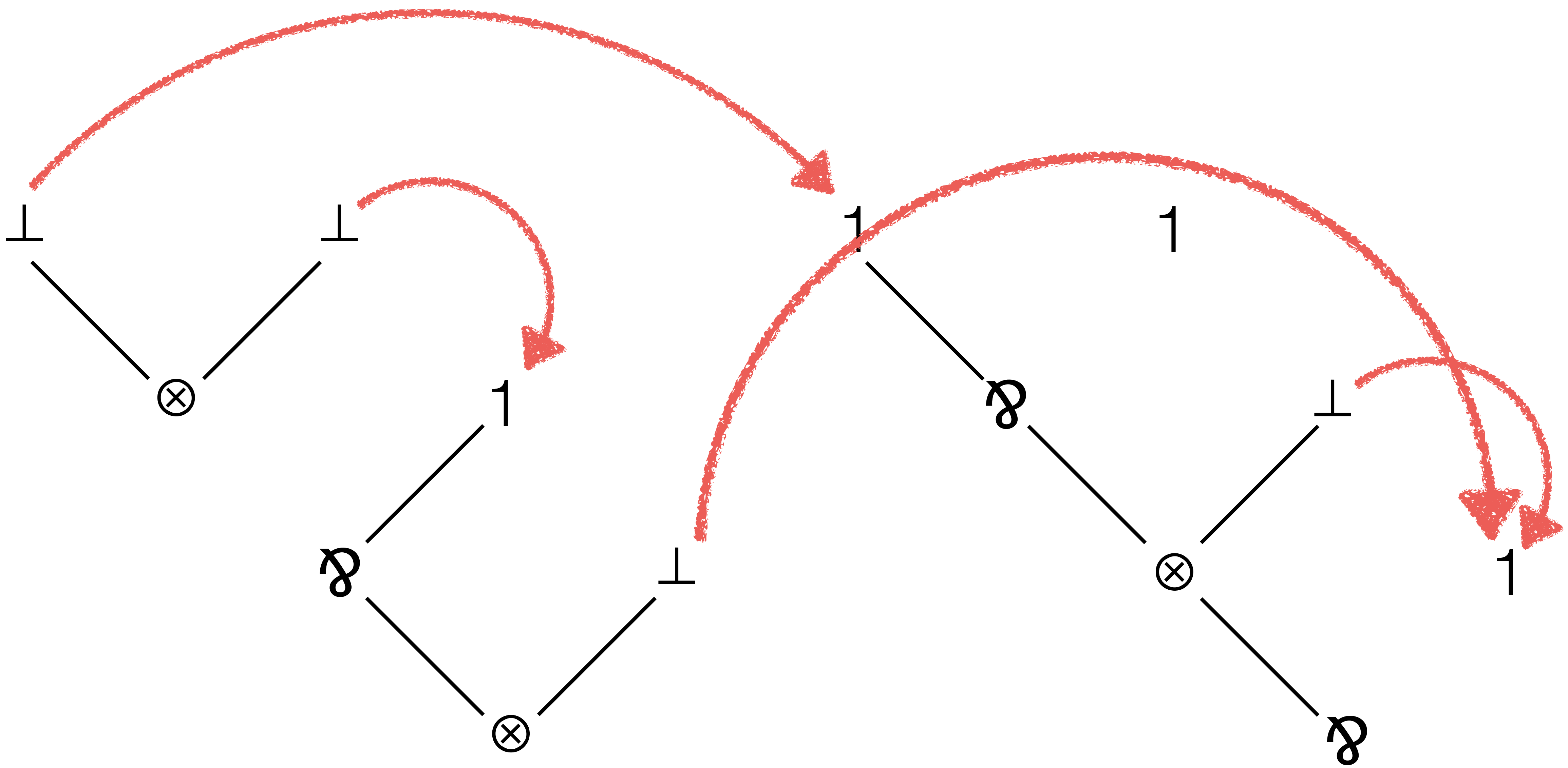
- Proof net = function from occurrences of $\bot$ to occurrences of 1 that satisfies the switching condition;

- Proof net equivalence relation generated by *rewiring*: moving a single link from a $\bot$ to a different 1.

Proof nets for units



Proof nets for units



Implications for proof theory

- It's no use looking for a canonical notion of MLL proof net (unless you believe that PSPACE = P).
- The proof nets we have for MLL may well be as nice as we're ever going to get.

The initial star-autonomous category

- “The initial X-category” is pretty boring for most values of X – typically either 0 or 1.
- Not so when X = “star-autonomous”.
- Infinite hierarchy of non-isomorphic objects:
  $1, \bot, \bot\otimes\bot, \bot\otimes\bot\otimes\bot$, etc.
  $1 ⅋ 1,\ 1 ⅋ (\bot\otimes\bot),\ 1 ⅋ (\bot\otimes\bot) ⅋ (\bot\otimes\bot\otimes\bot)$
  $(1 ⅋ (\bot\otimes\bot)) ⅋ (1 ⅋ (\bot\otimes\bot) ⅋ (\bot\otimes\bot\otimes\bot))$
  ad infinitum

What is “PSPACE-complete”

- **Really** hard.
- As hard as possible, in a sense.
- Hard even with an omniscient (but untrusted) guide.
- There are proofs that are equivalent but where the shortest rewiring from one to the other is exponentially long.

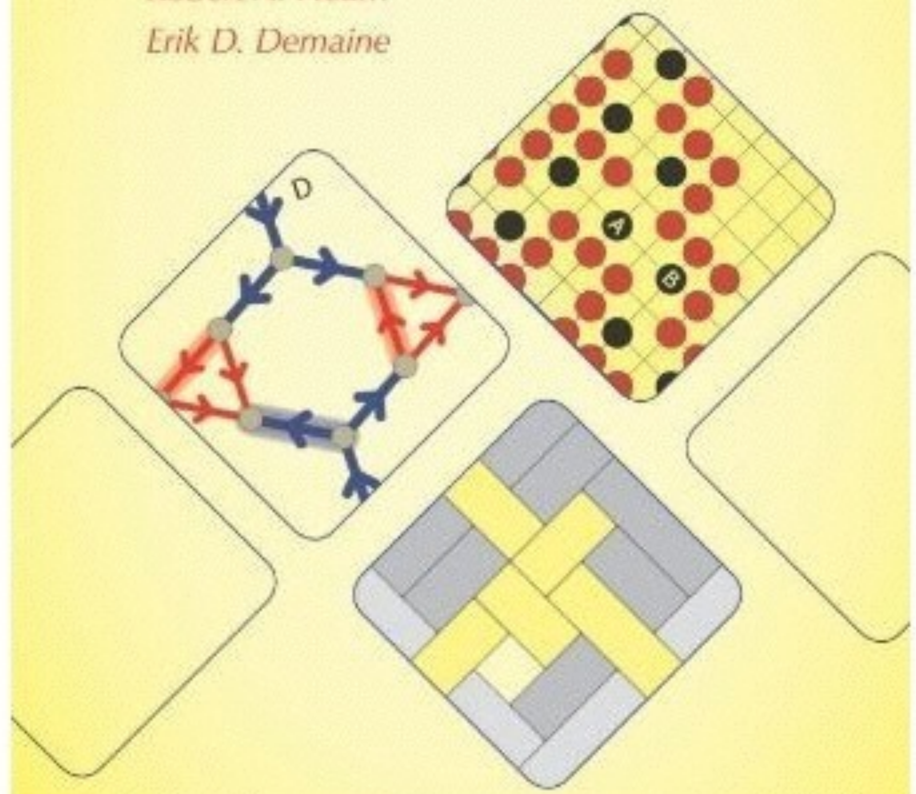
How do we prove this is PSPACE-complete?

- Reduction from a known-hard problem
- (The configuration-to-configuration problem for nondeterministic constraint logic)
- So we can solve MLL proof equivalence easily only if everything is easy (i.e. if PSPACE = P)

Constraint Logic

Games, Puzzles, & Computation

Robert A. Hearn
Erik D. Demaine



Copyrighted Material

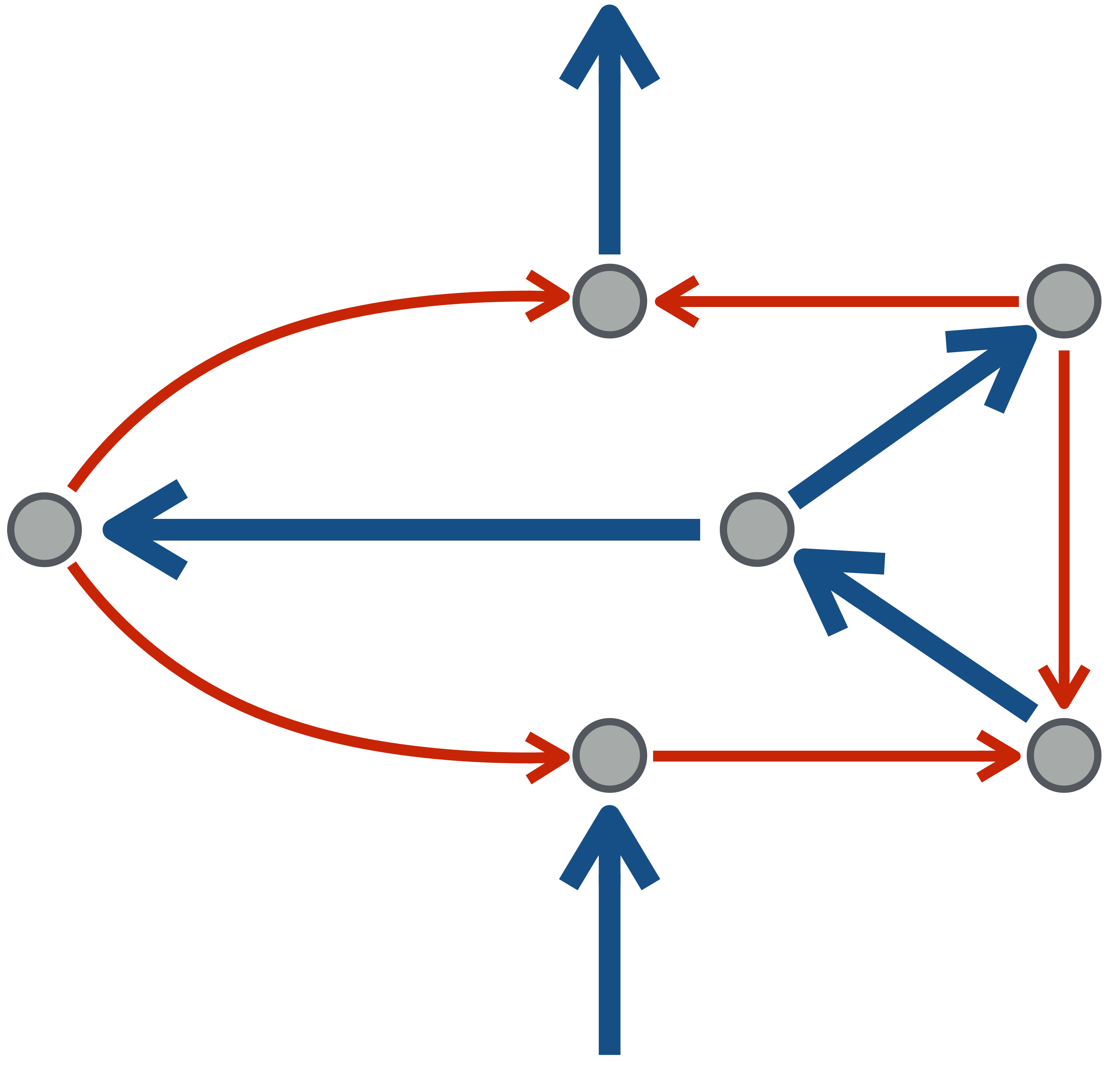
Nondeterministic constraint logic

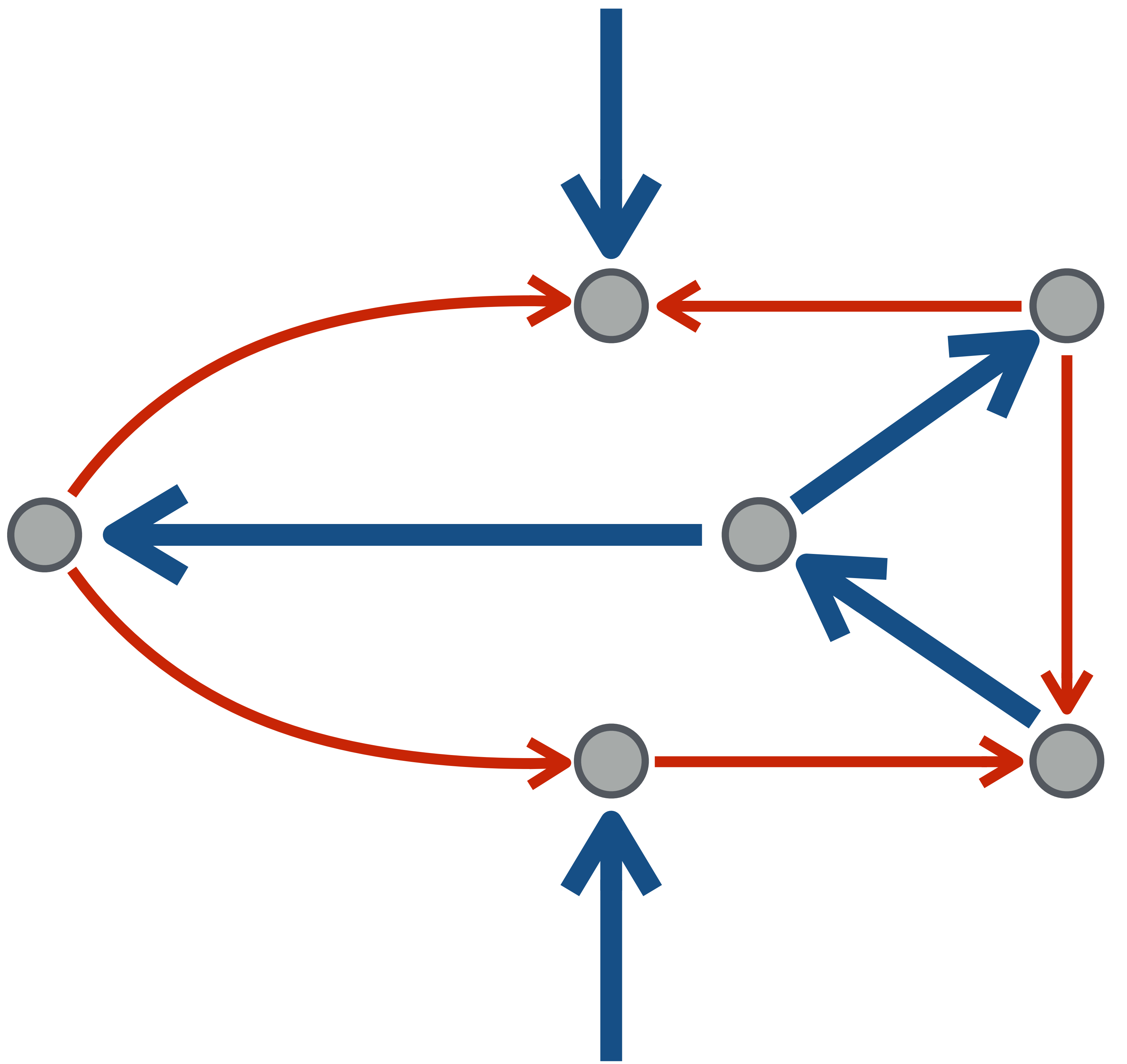
- Weighted graph
- Each node has a minimum inflow constraint $\in \mathbb{N}$
- A configuration is an assignment of a direction to each edge such that the inflow constraints are satisfied
- A move is the reversal of a single edge (s.t. constraints remain satisfied)
- Deciding whether one configuration can be changed into another is PSPACE-complete

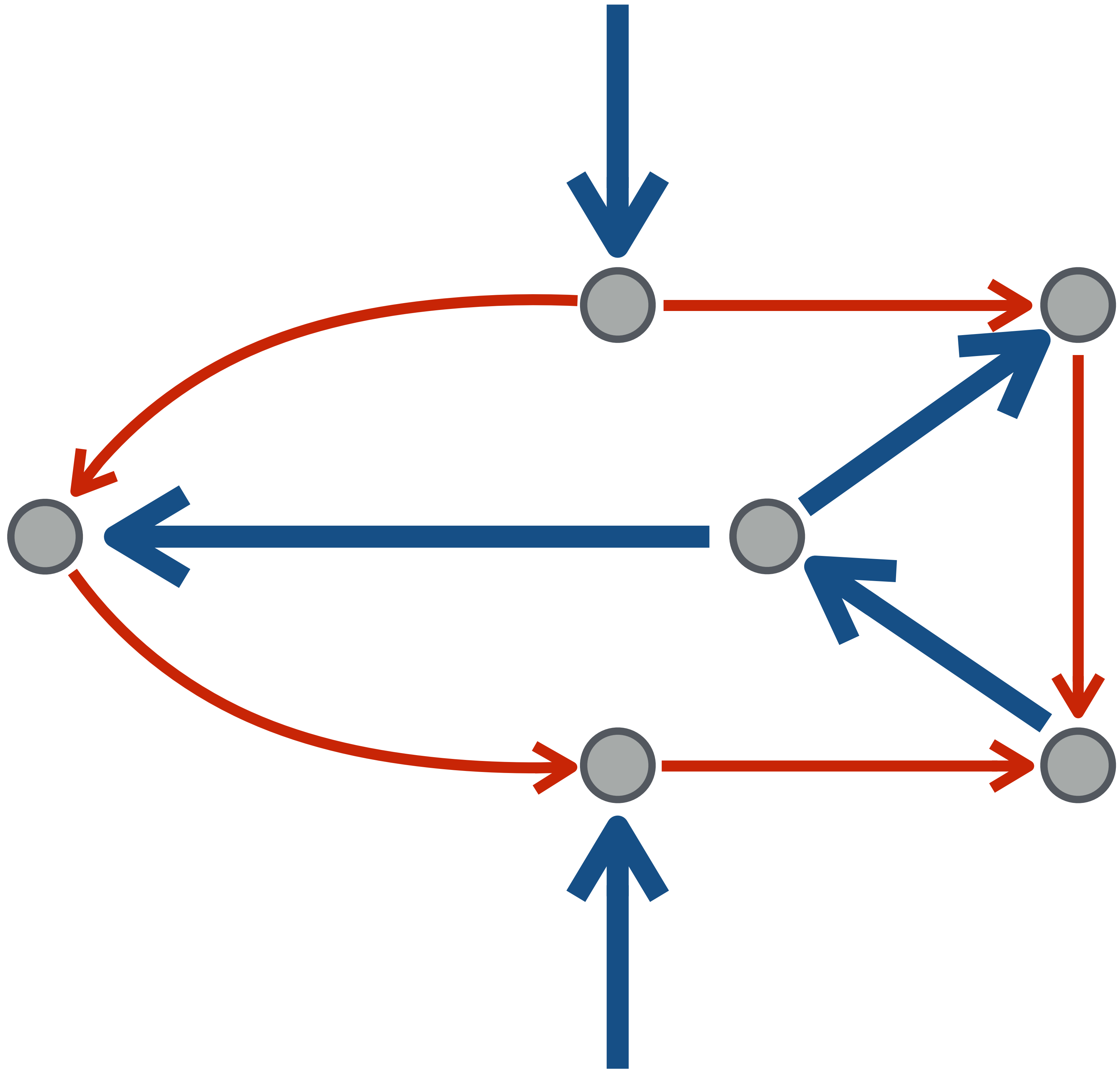
Nondeterministic constraint logic

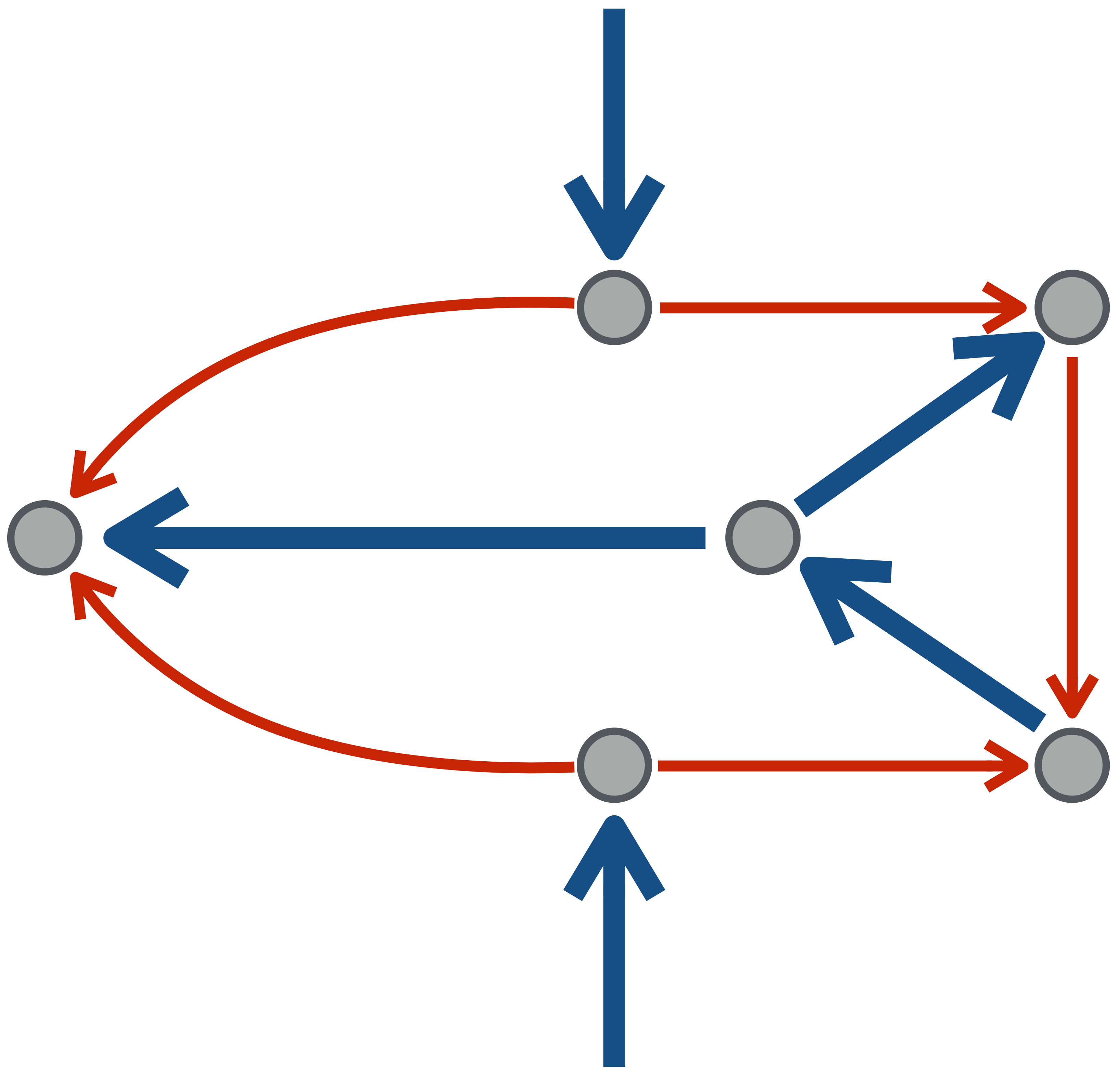
- This remains true under many restrictions on the constraint graphs. We may assume:
- Every edge has weight 1 or 2;
- Every node has minimum inflow constraint 2;
- The graph is cubic planar.

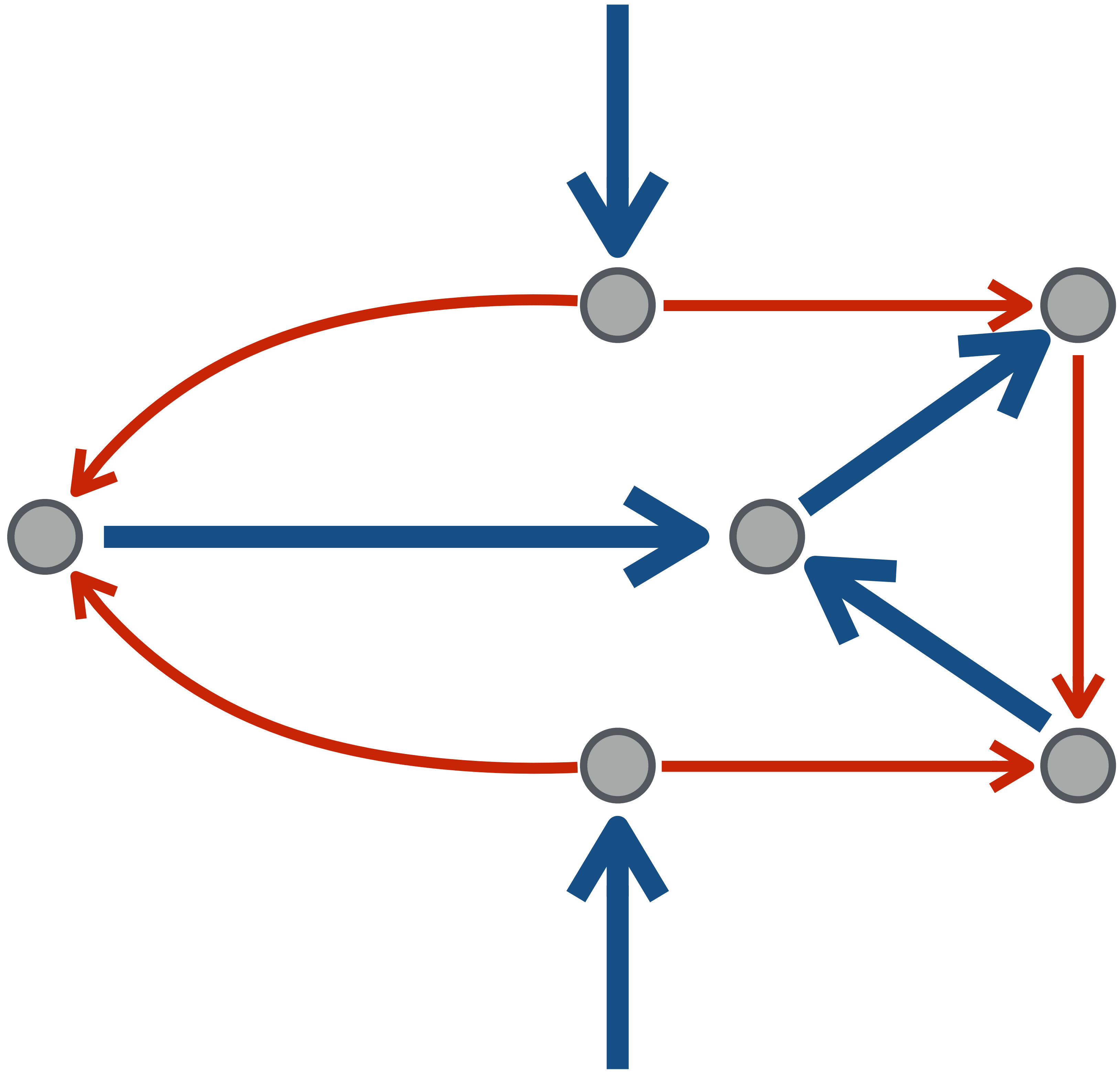
Example

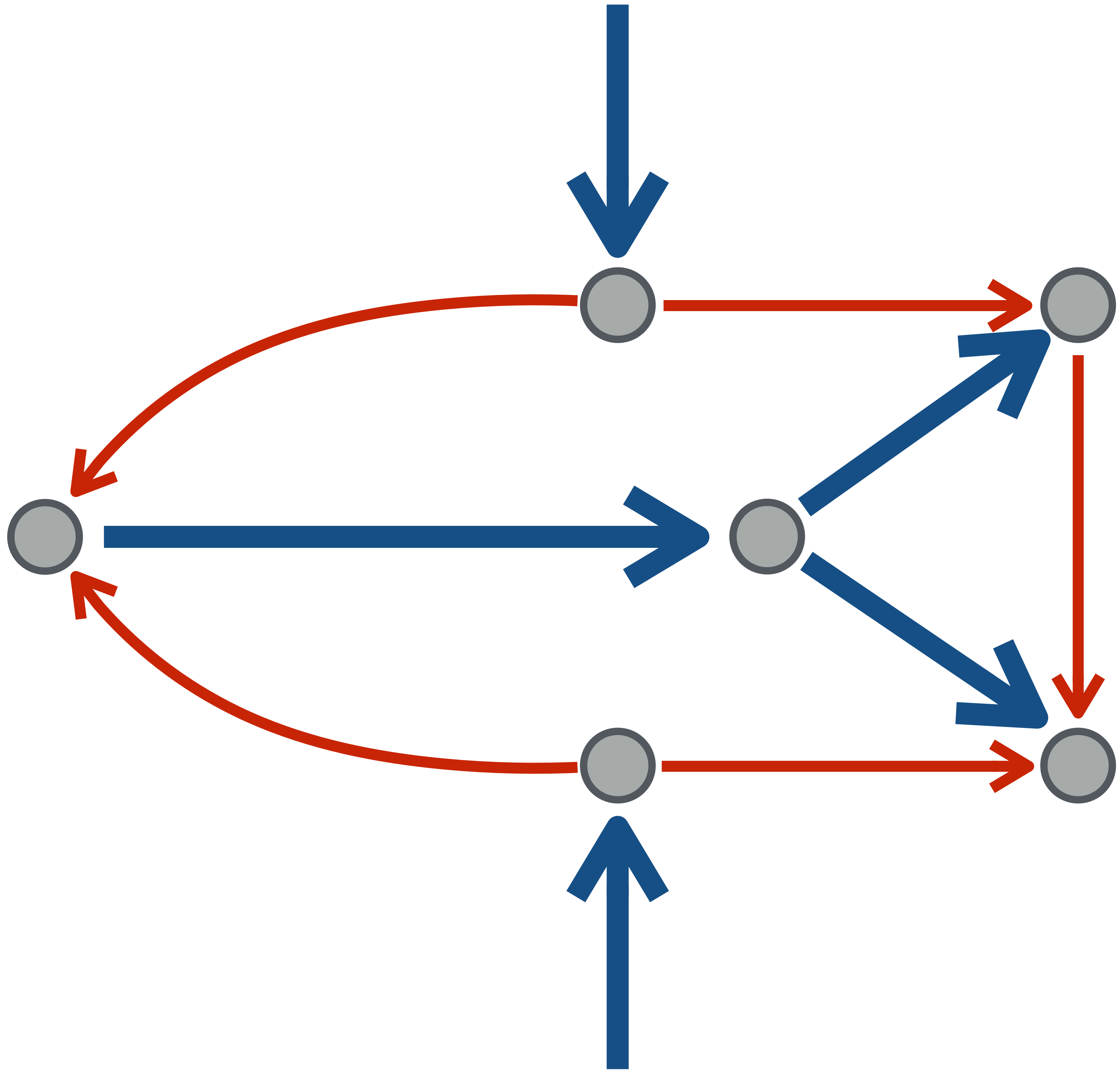


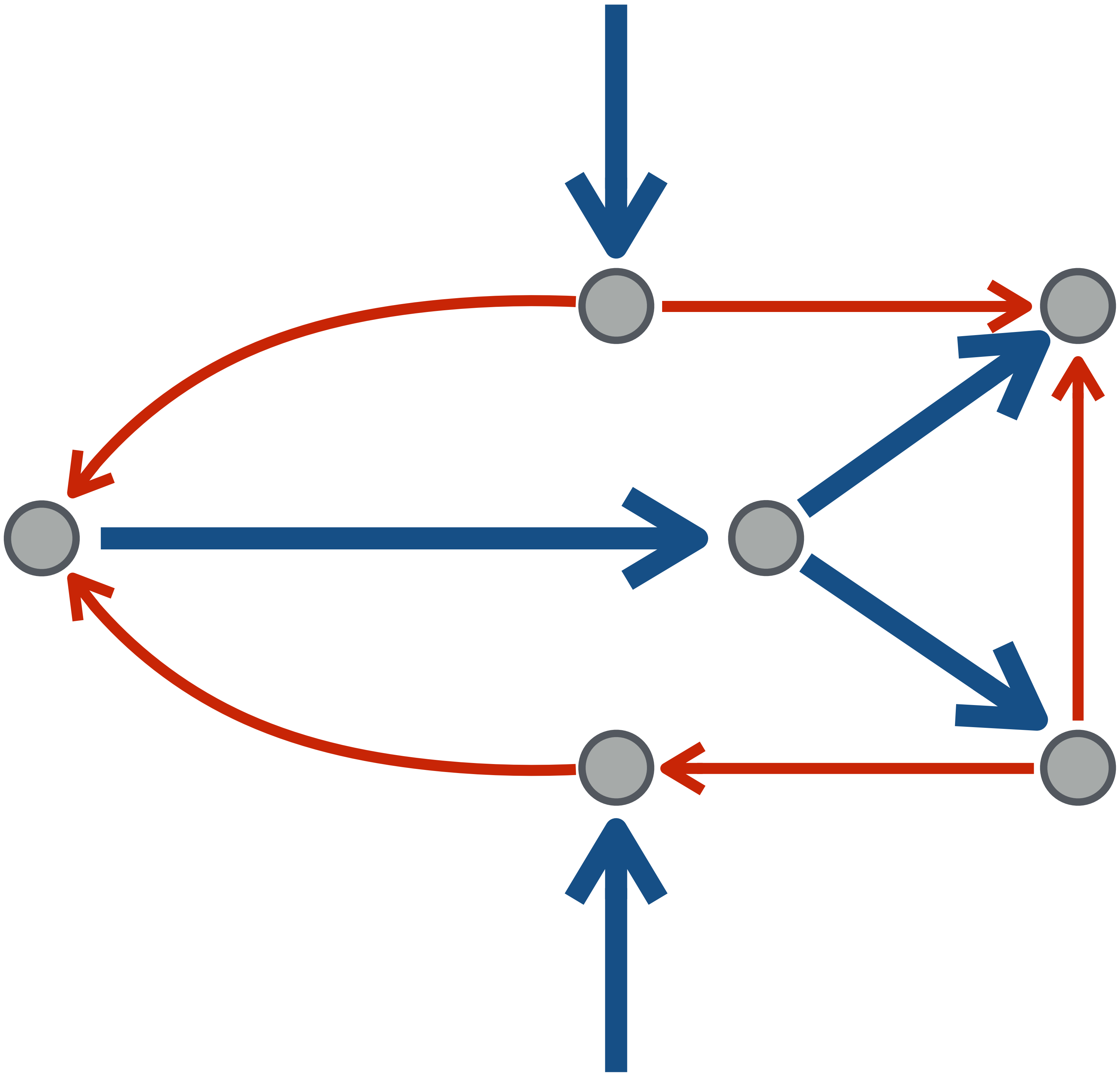


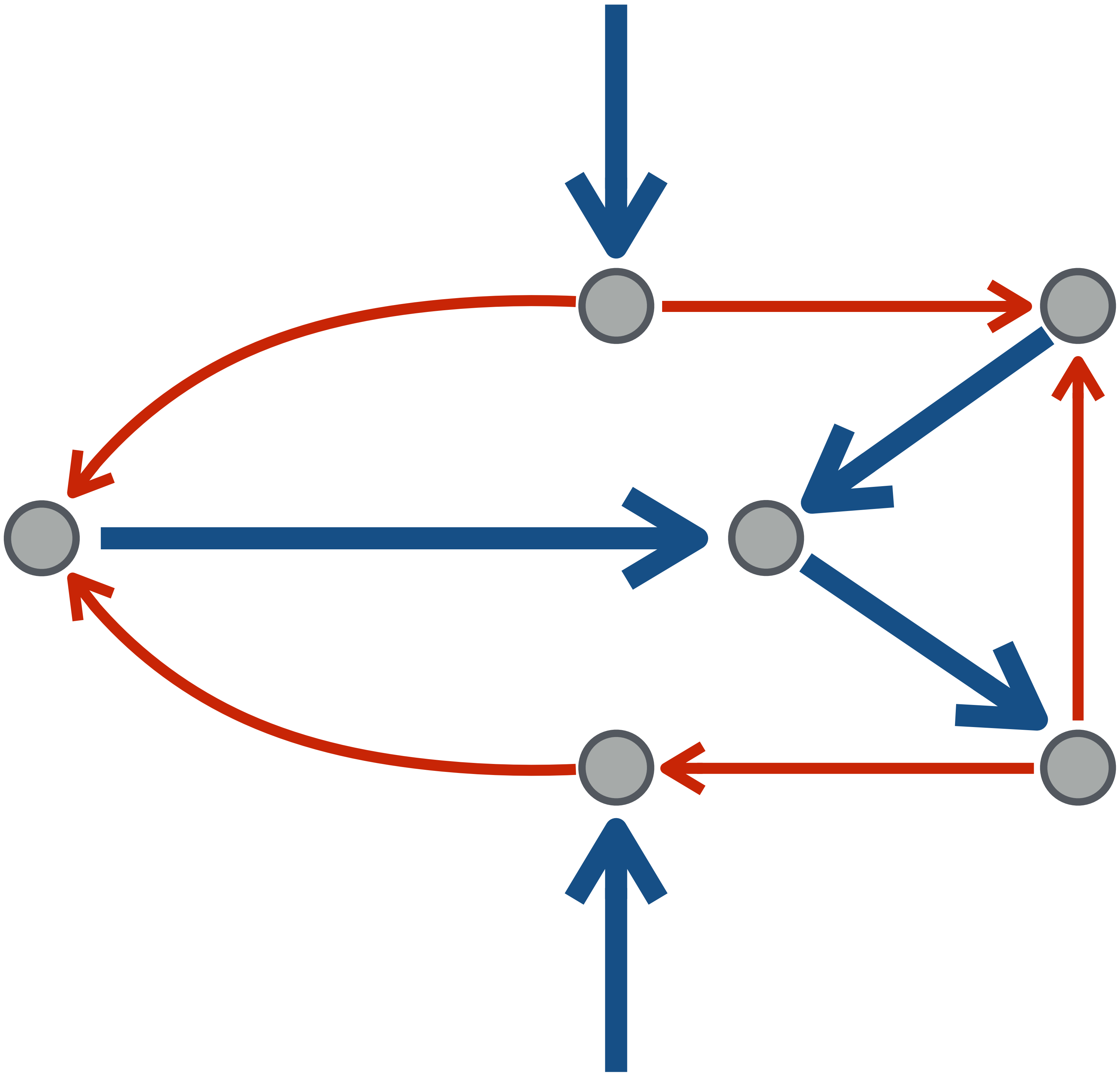


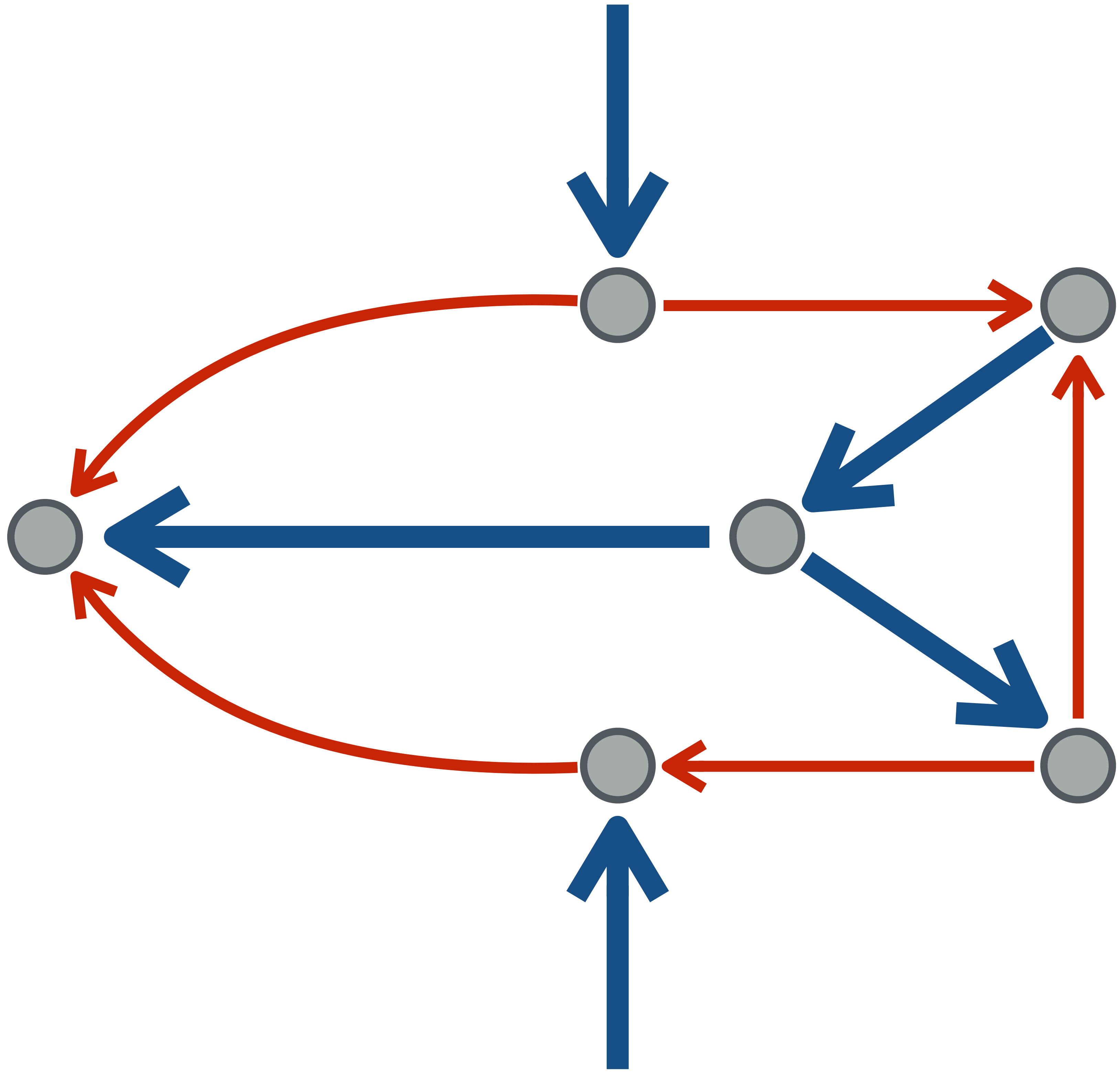


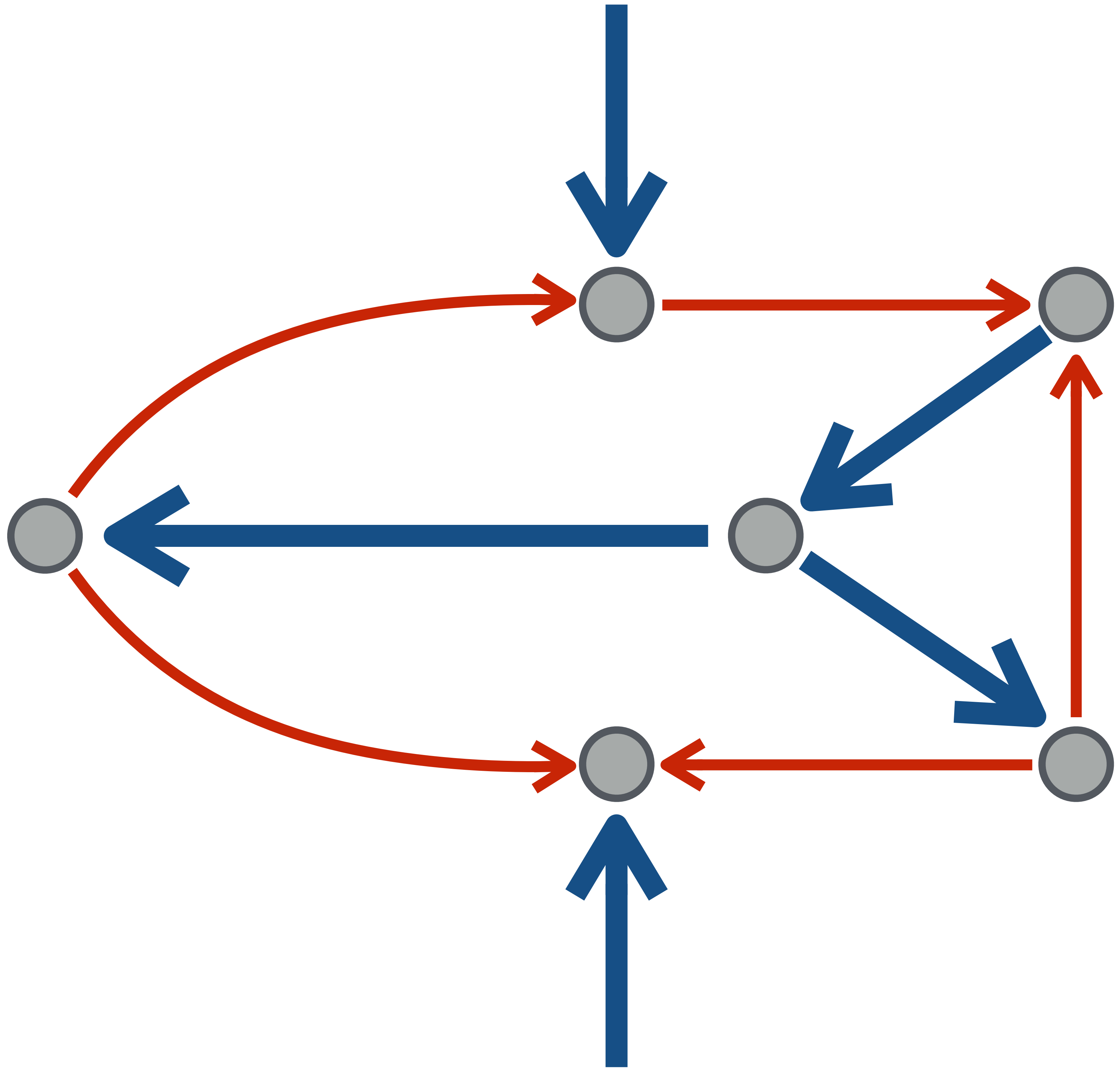


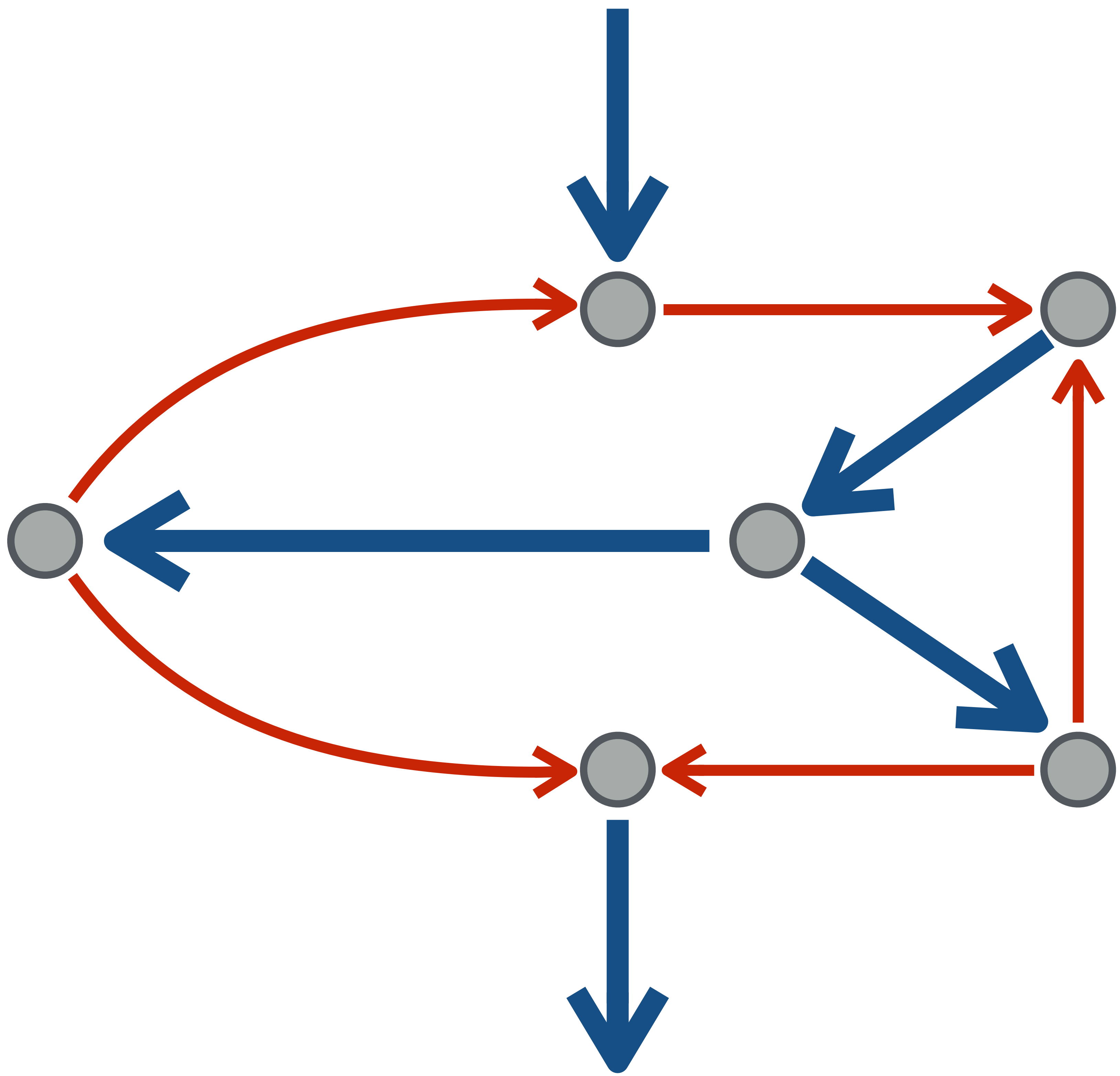


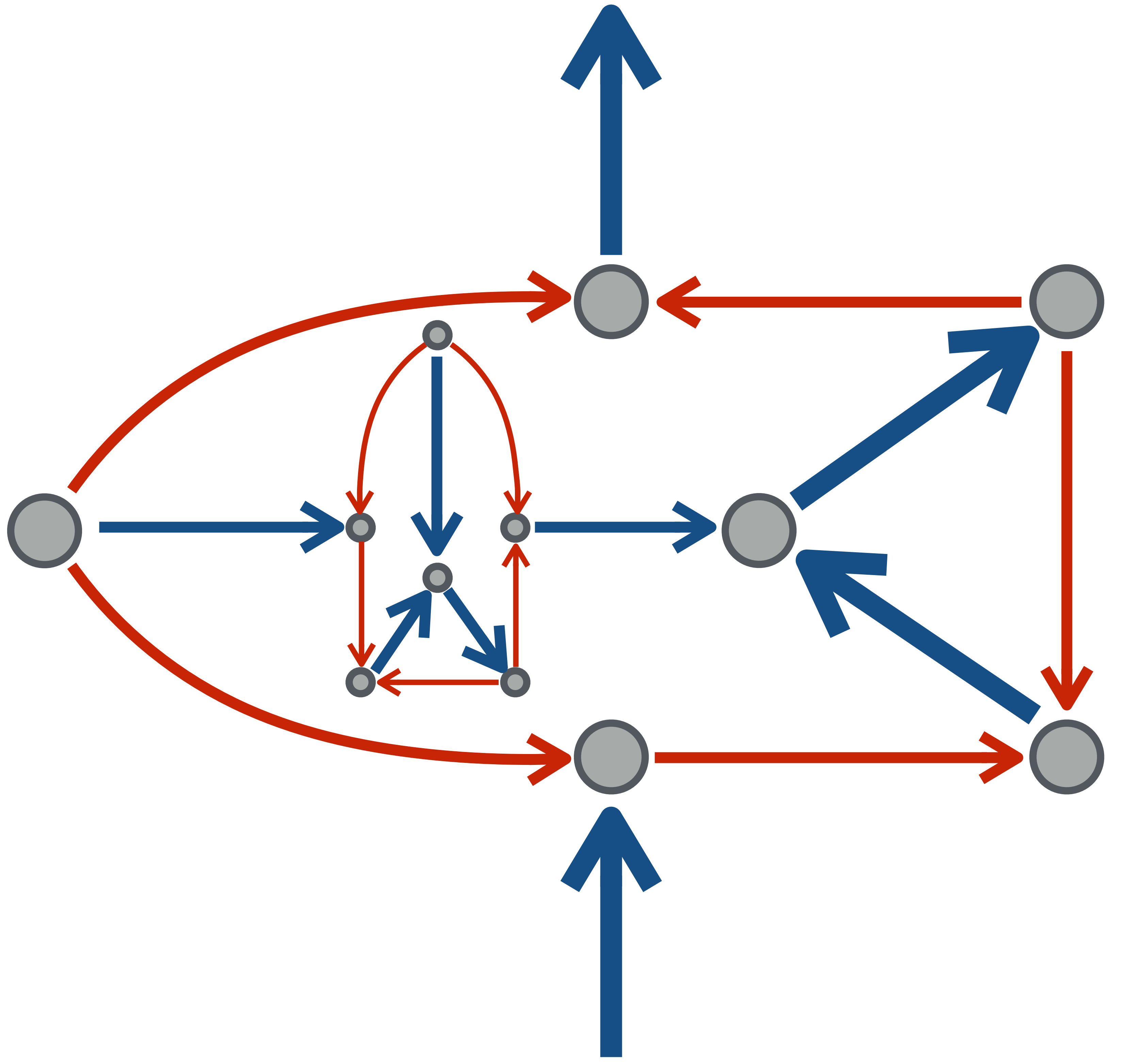












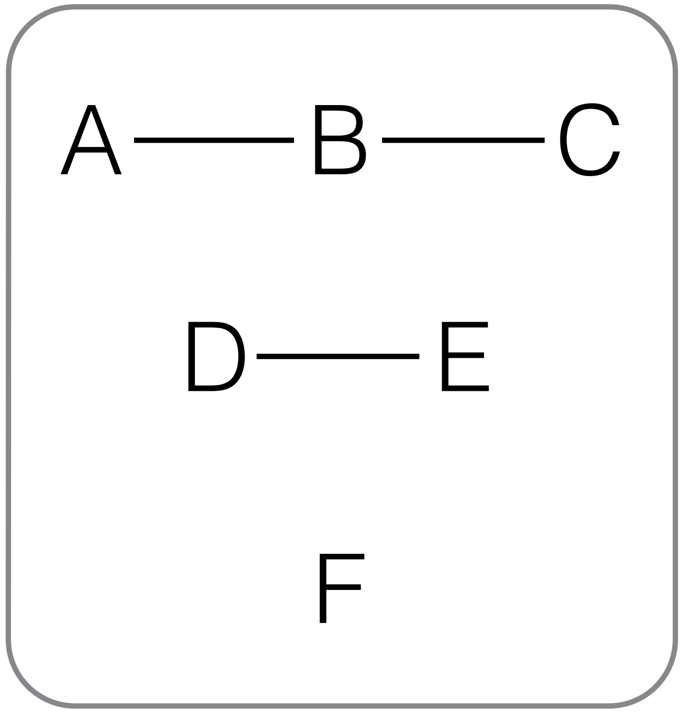
End of Part 1?

Notation

○	●
1	$\bot$

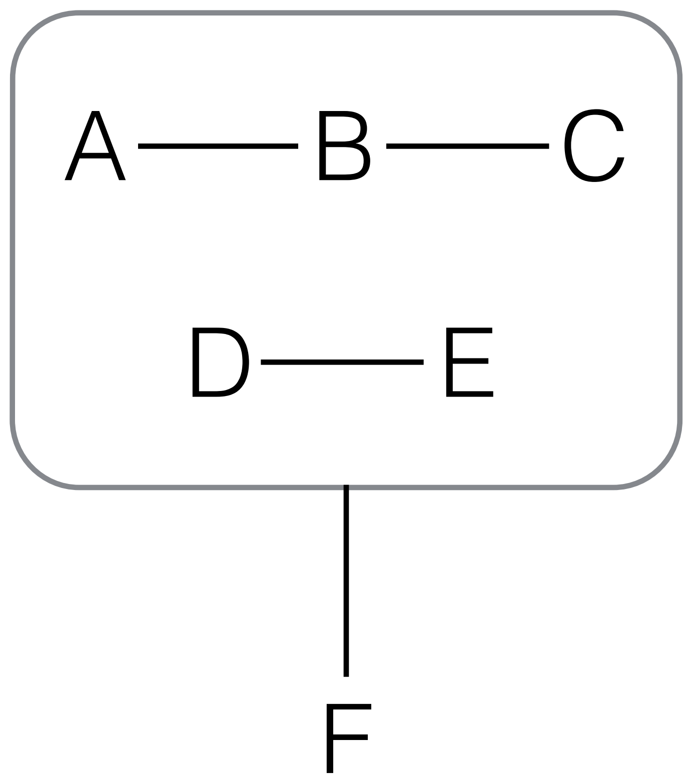
Notation

$(A \otimes B \otimes C) \parr (D \otimes E) \parr F$

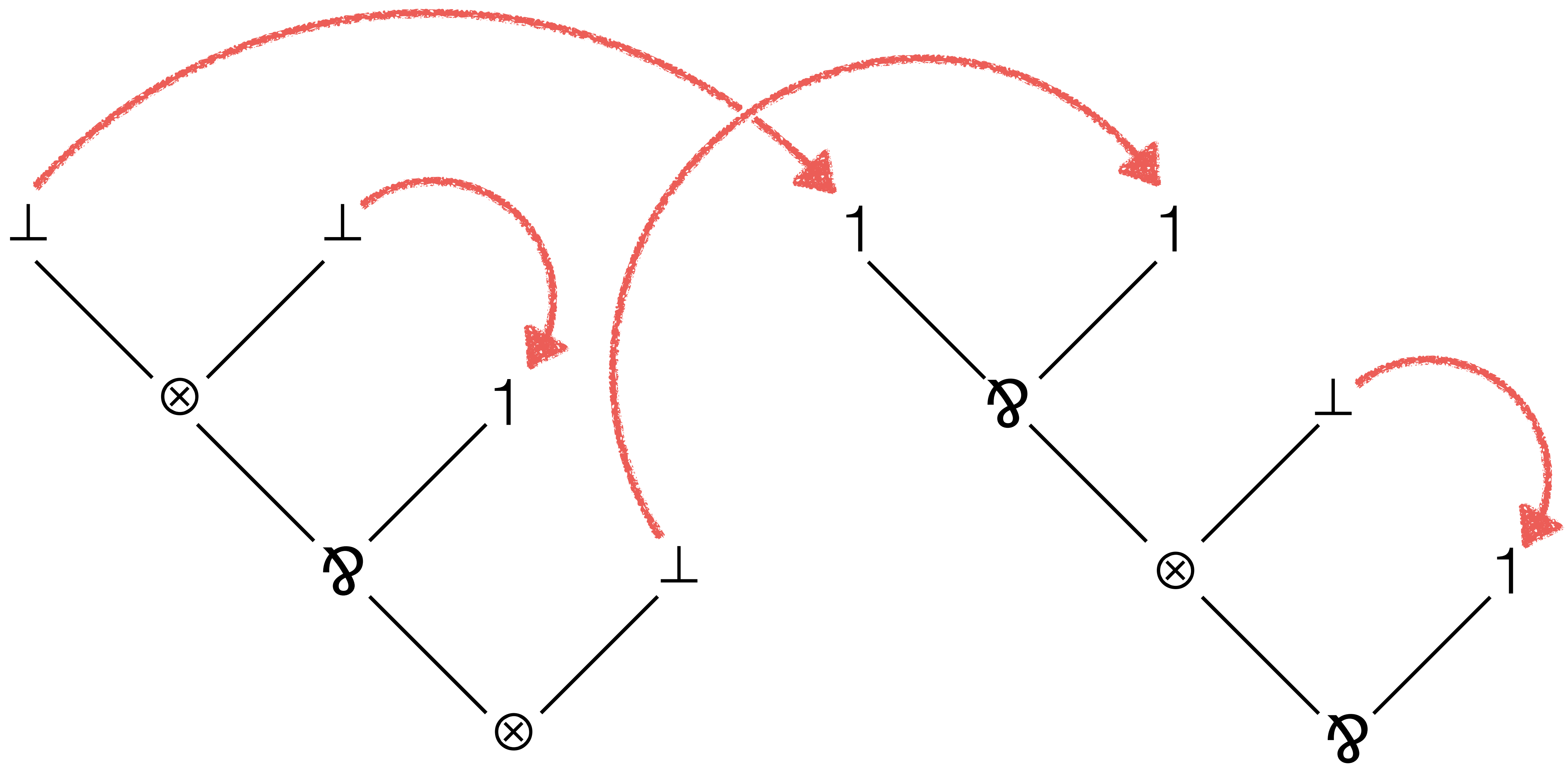


Notation

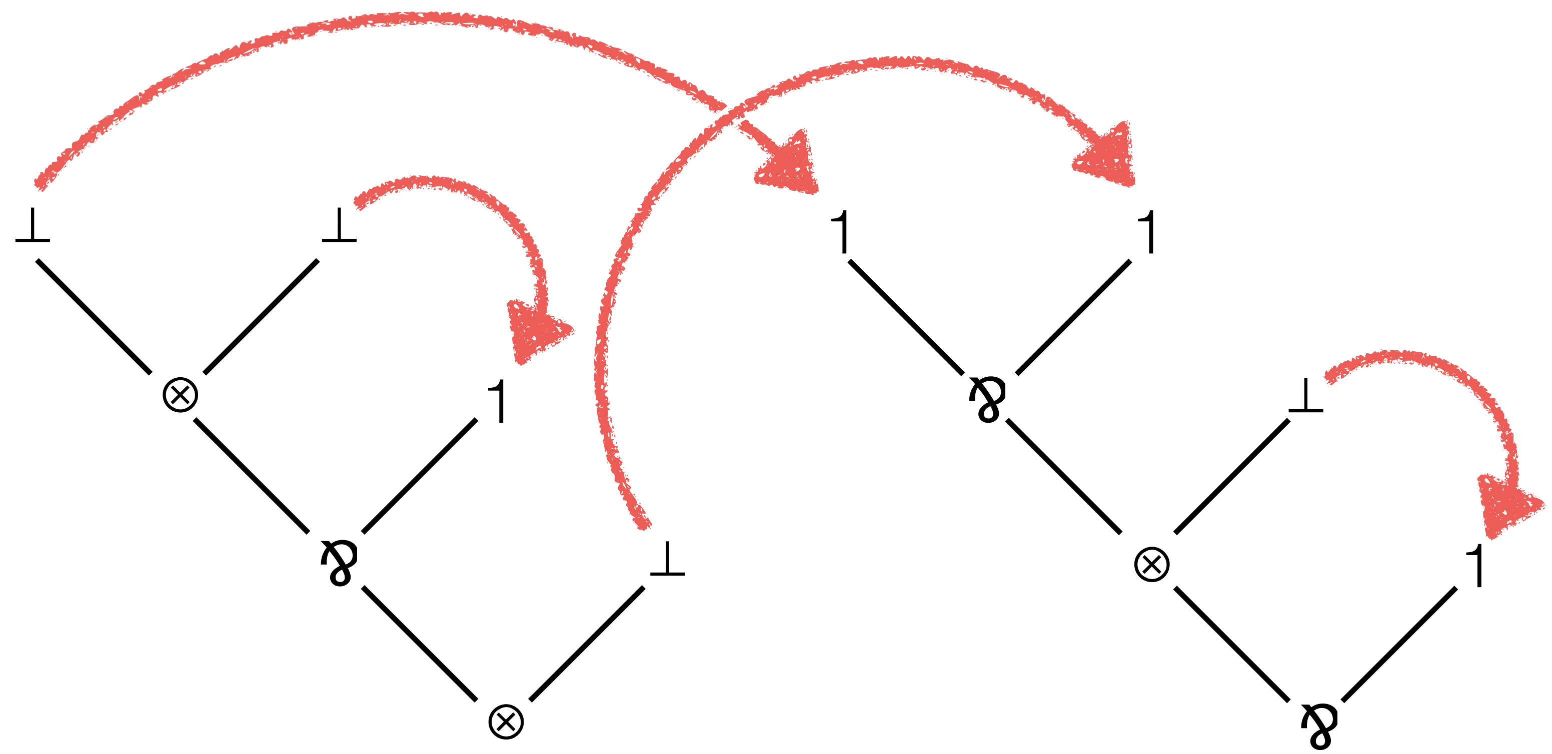
$$[(A \otimes B \otimes C) \parr (D \otimes E)] \otimes F$$

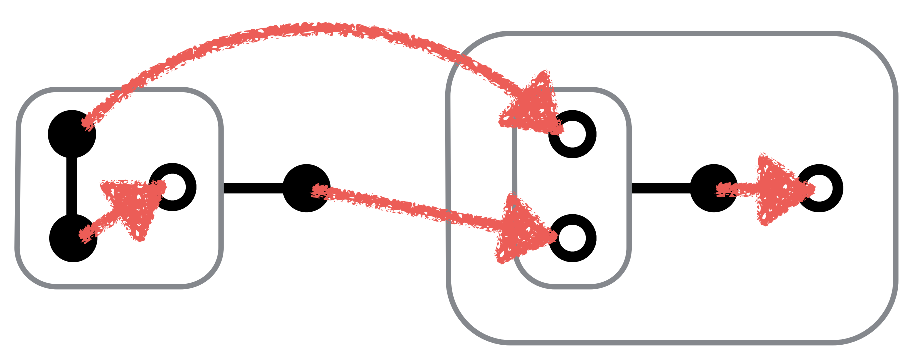


Notation example

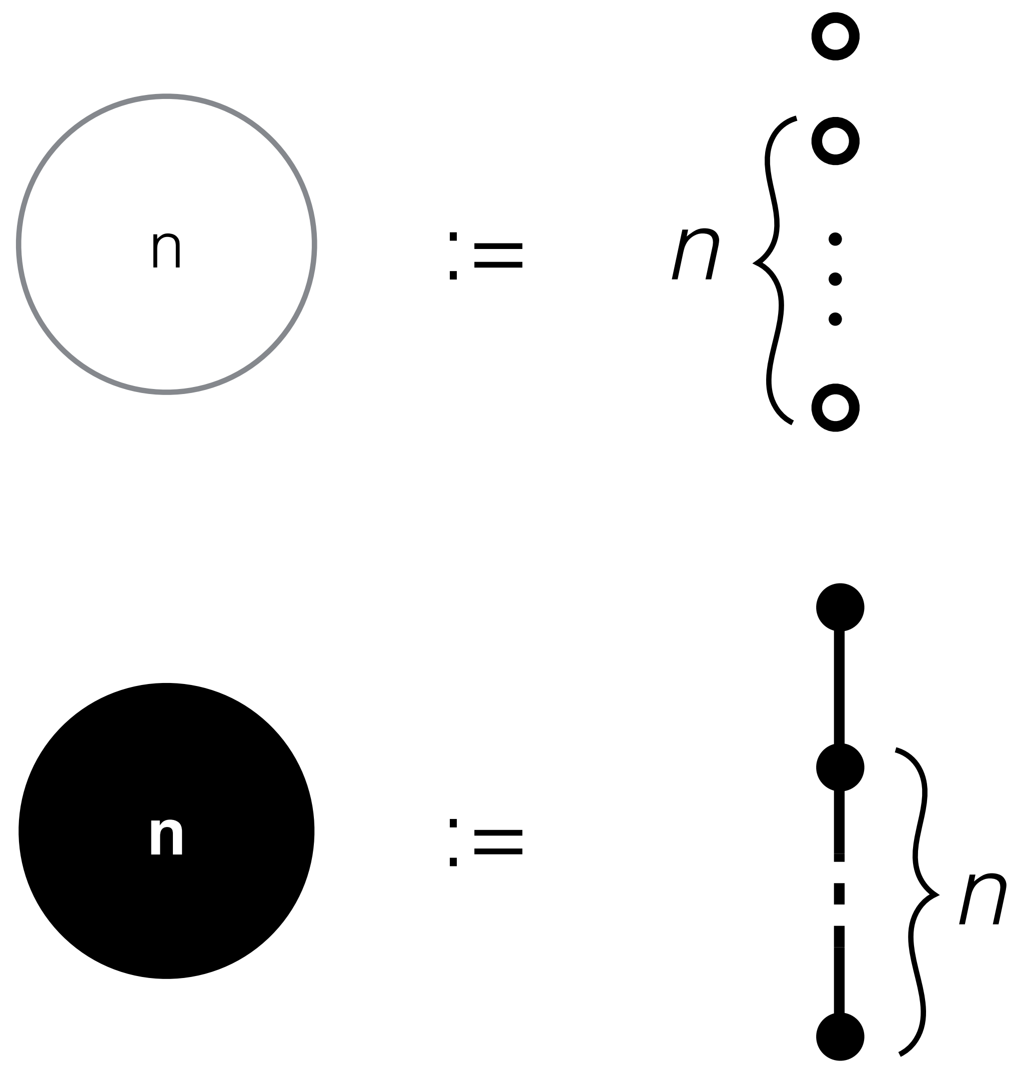


Notation example

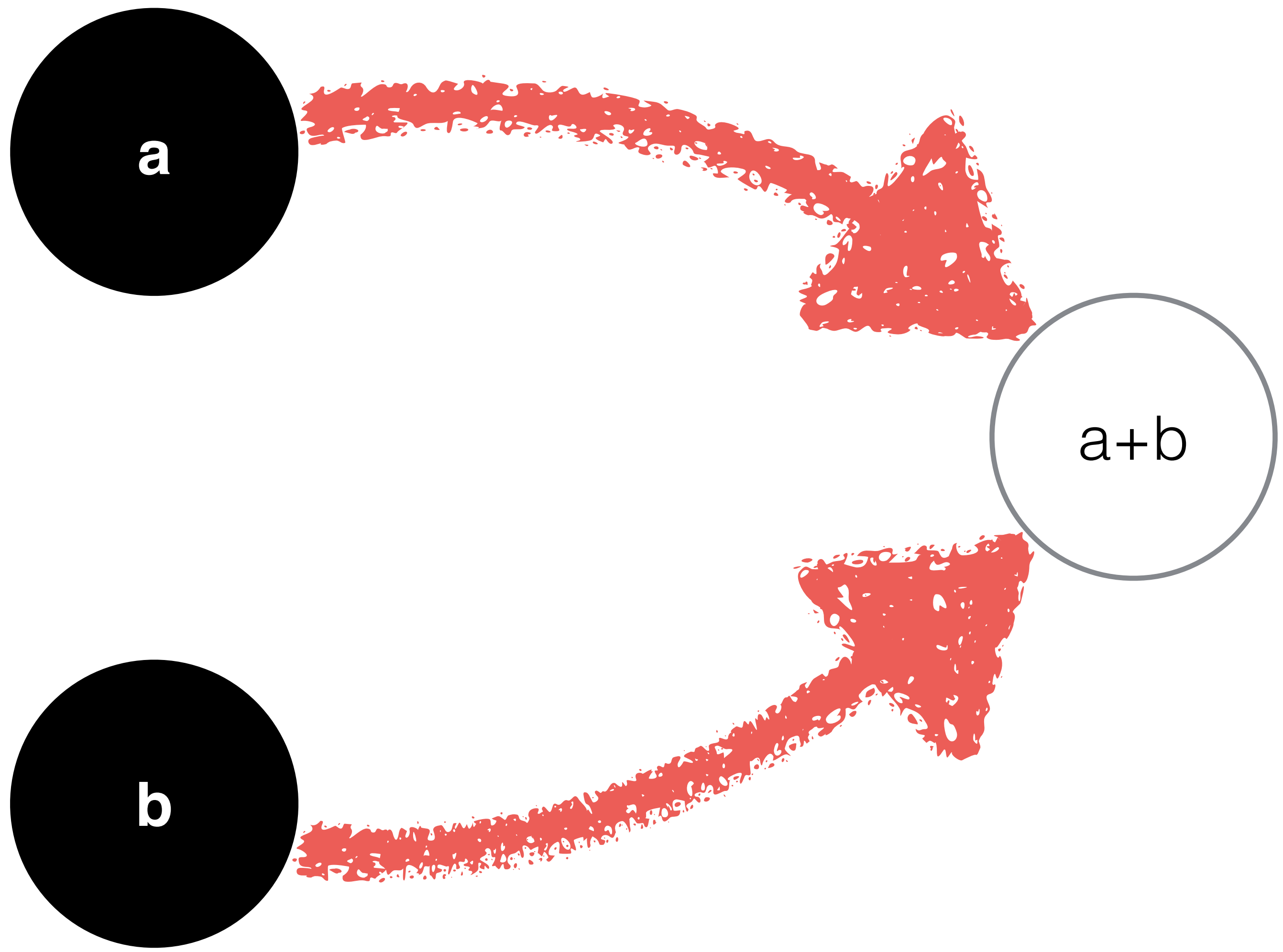




More notation

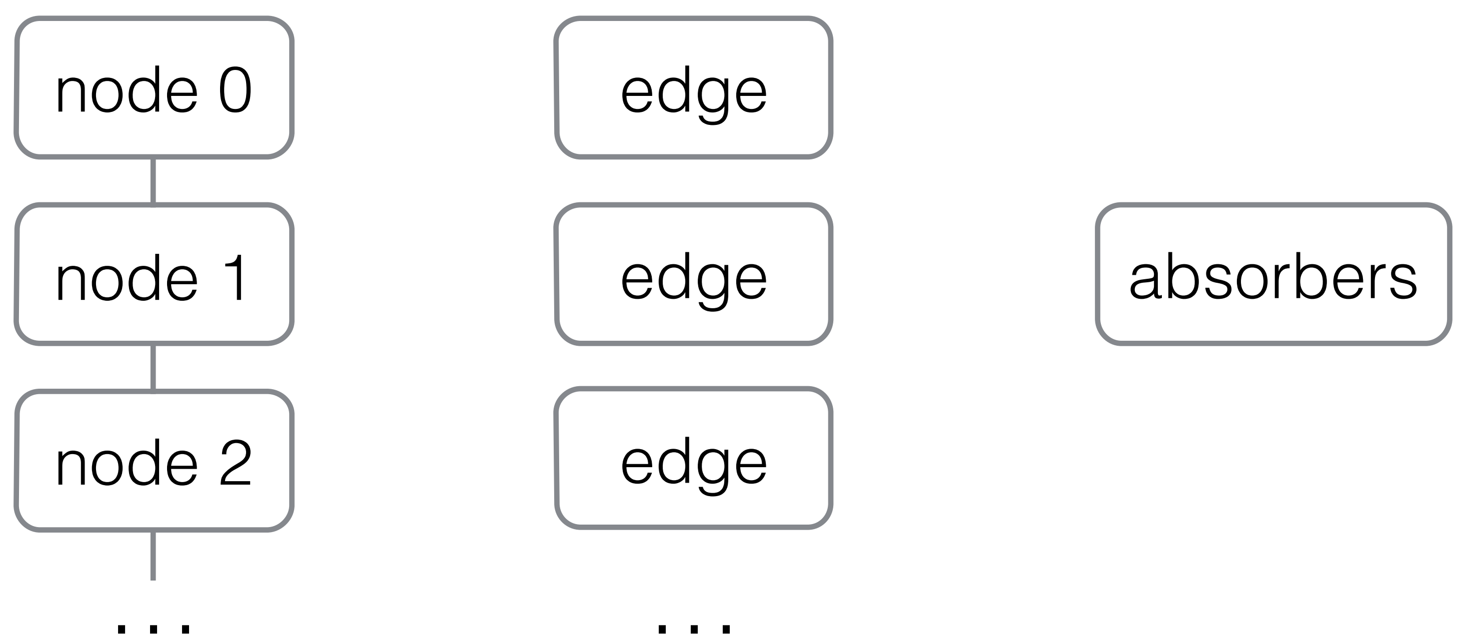


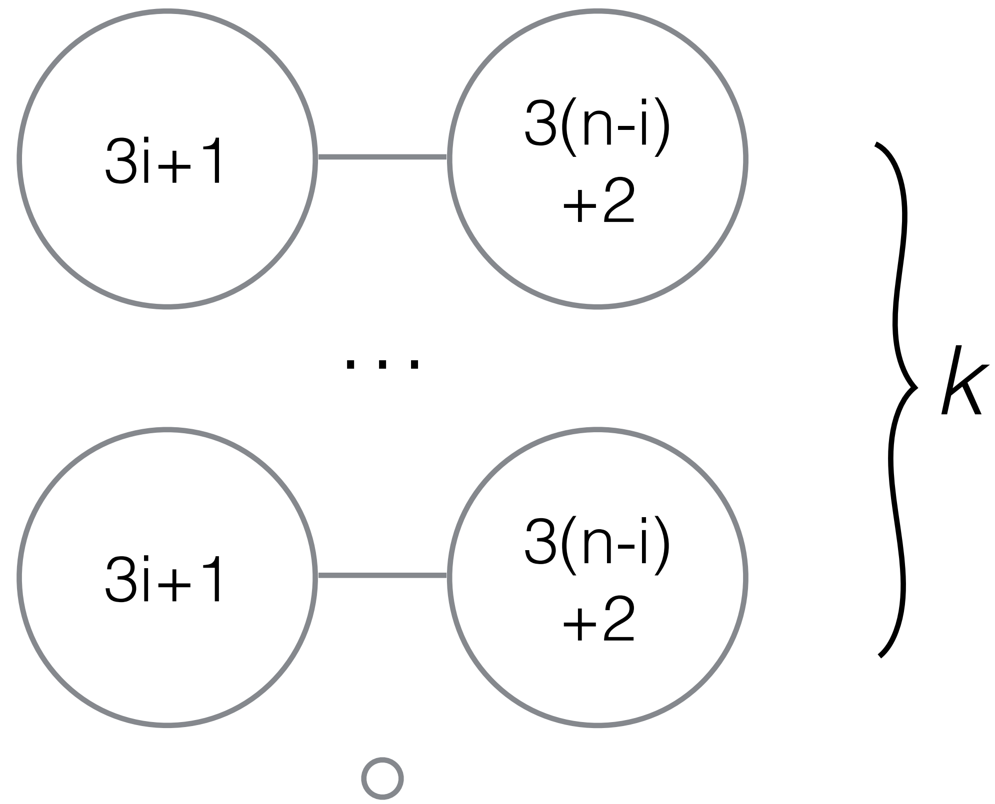
Why this notation?



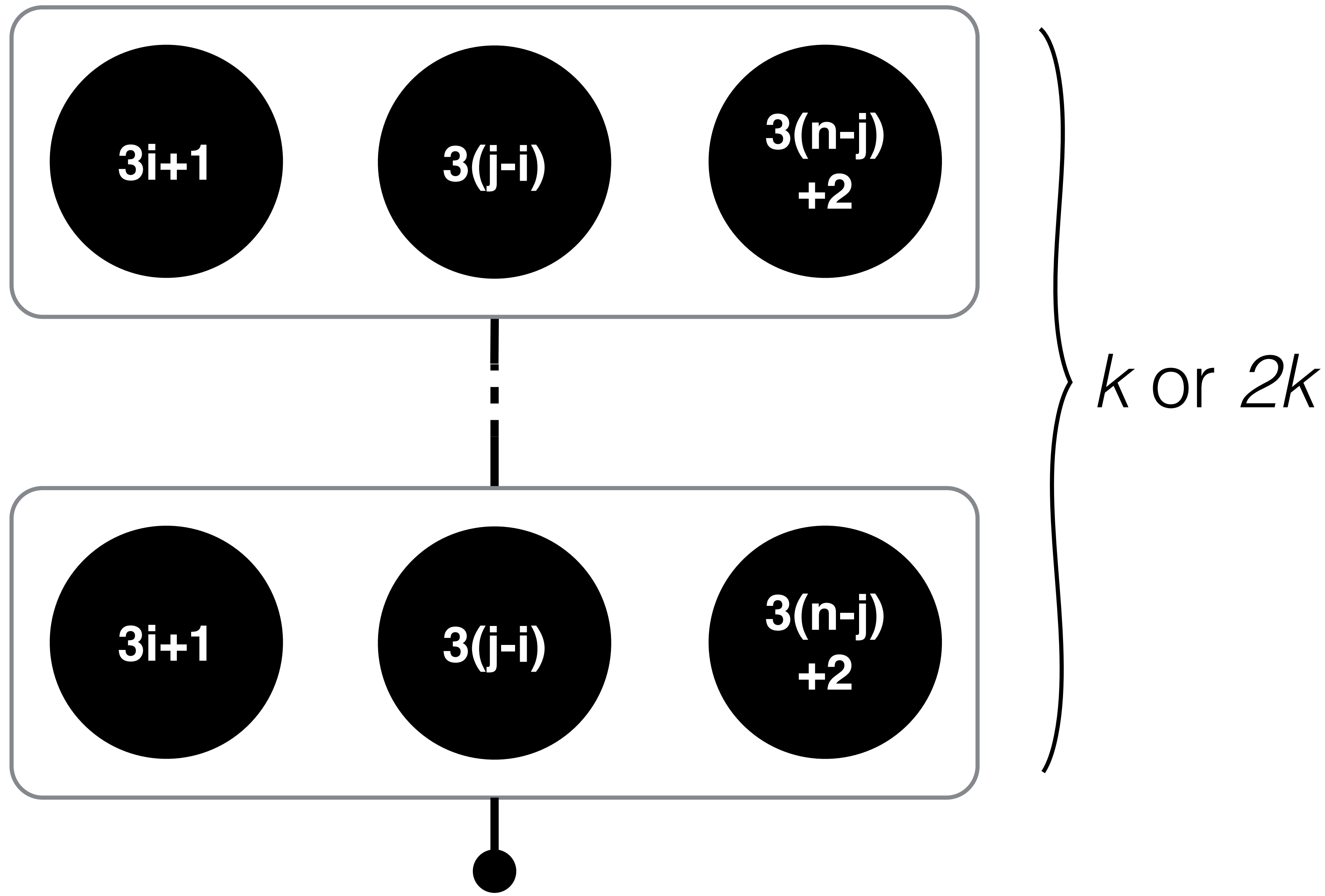
The reduction

Overall construction



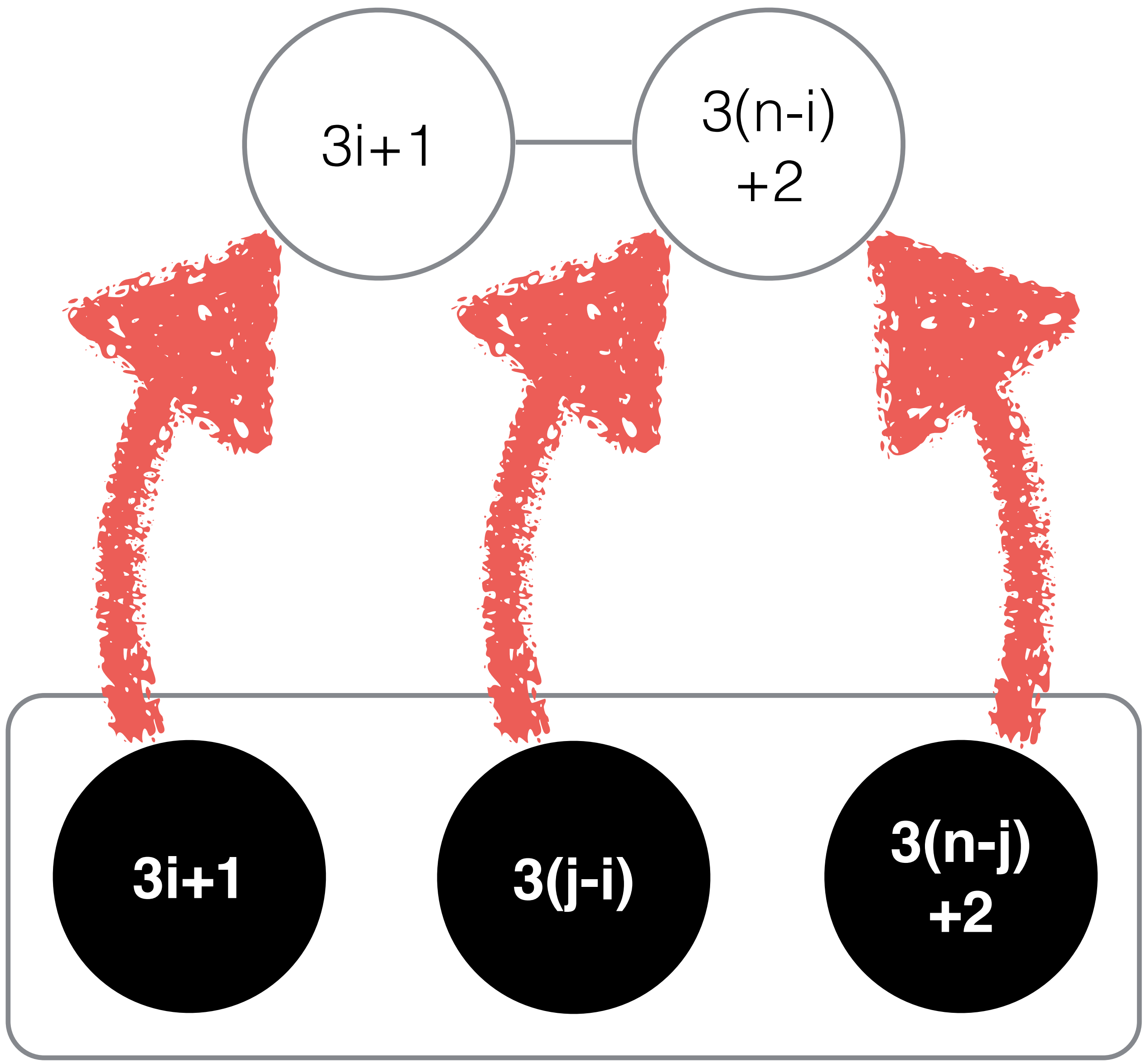


Gadget for node *i*

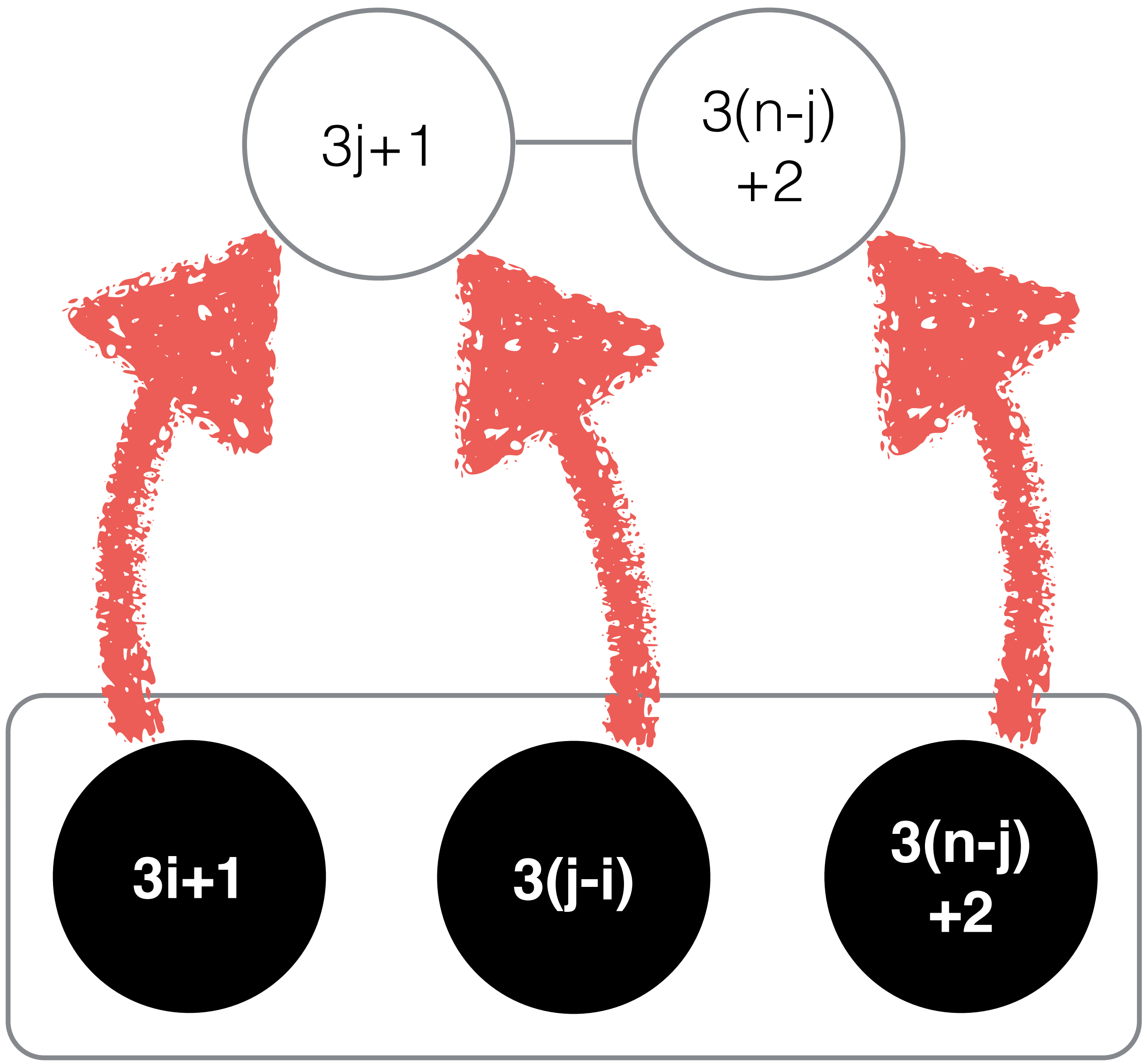


Gadget for edge *i*–*j*

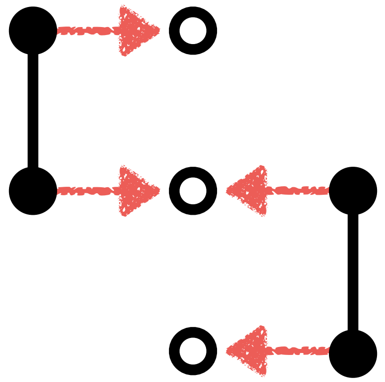
The edge *i–j* attaching to node *i*



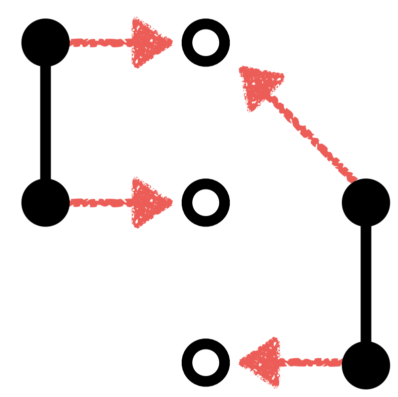
The edge *i–j* attaching to node *j*



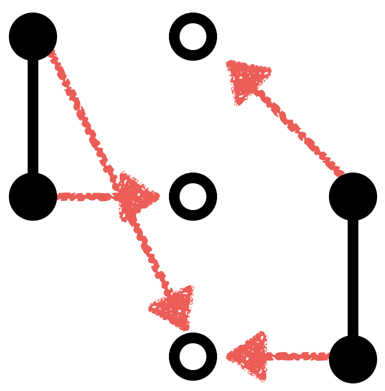
“Parity”



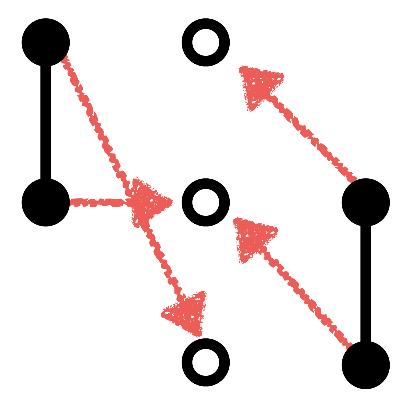
$\vdash \bot \otimes \bot, 1, 1, 1, \bot \otimes \bot$



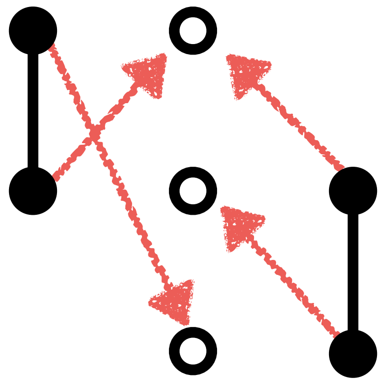
$\vdash \bot \otimes \bot, 1, 1, 1, \bot \otimes \bot$



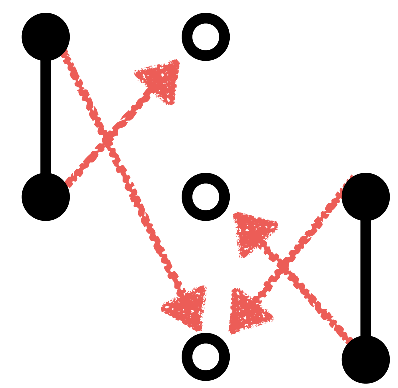
$\vdash \bot \otimes \bot, 1, 1, 1, \bot \otimes \bot$



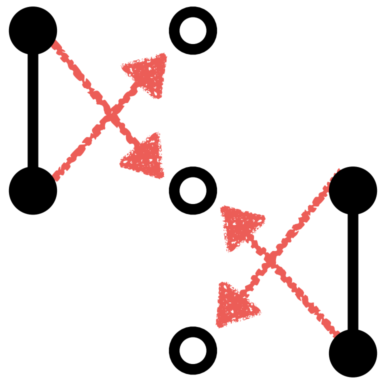
$\vdash \bot \otimes \bot, 1, 1, 1, \bot \otimes \bot$



$$\vdash \bot \otimes \bot,\ 1,\ 1,\ 1,\ \bot \otimes \bot$$

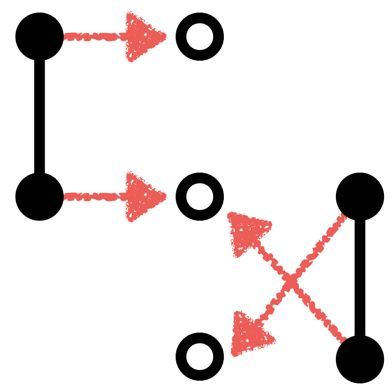


$\vdash \bot \otimes \bot, 1, 1, 1, \bot \otimes \bot$

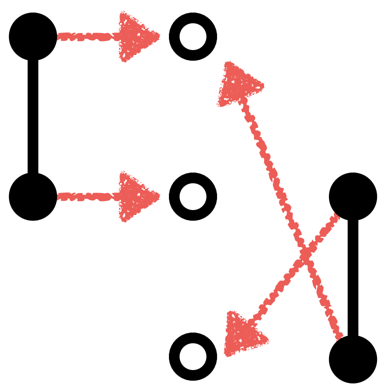


$$\vdash \bot \otimes \bot,\ 1,\ 1,\ 1,\ \bot \otimes \bot$$

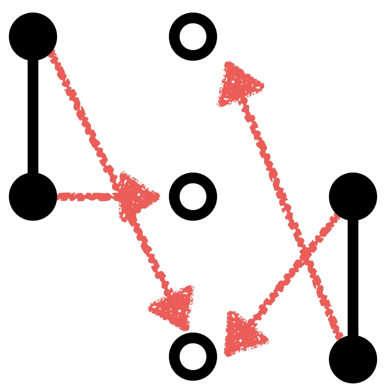
Not equivalent:



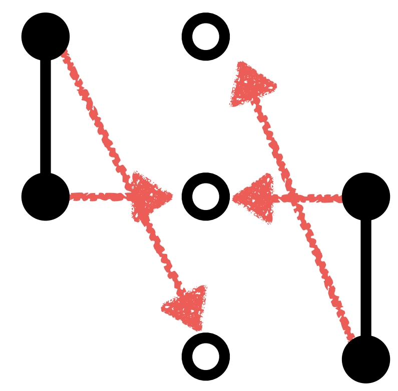
$\vdash \bot \otimes \bot, 1, 1, 1, \bot \otimes \bot$



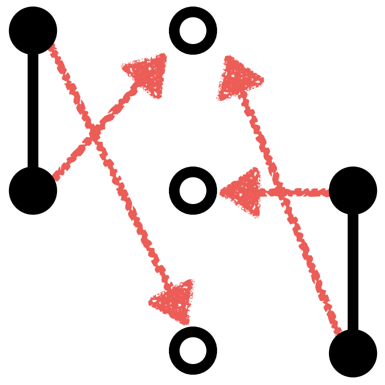
$\vdash \bot \otimes \bot,\ 1,\ 1,\ 1,\ \bot \otimes \bot$



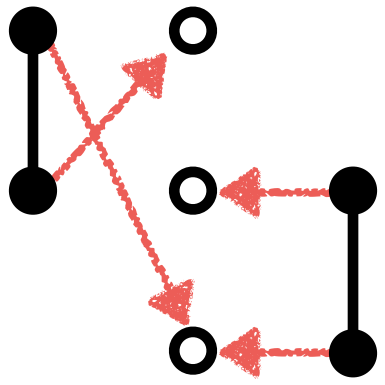
$\vdash \bot \otimes \bot, 1, 1, 1, \bot \otimes \bot$



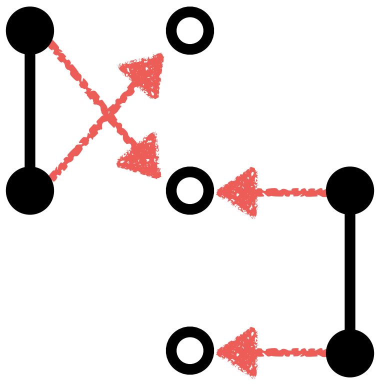
$\vdash \bot \otimes \bot, 1, 1, 1, \bot \otimes \bot$



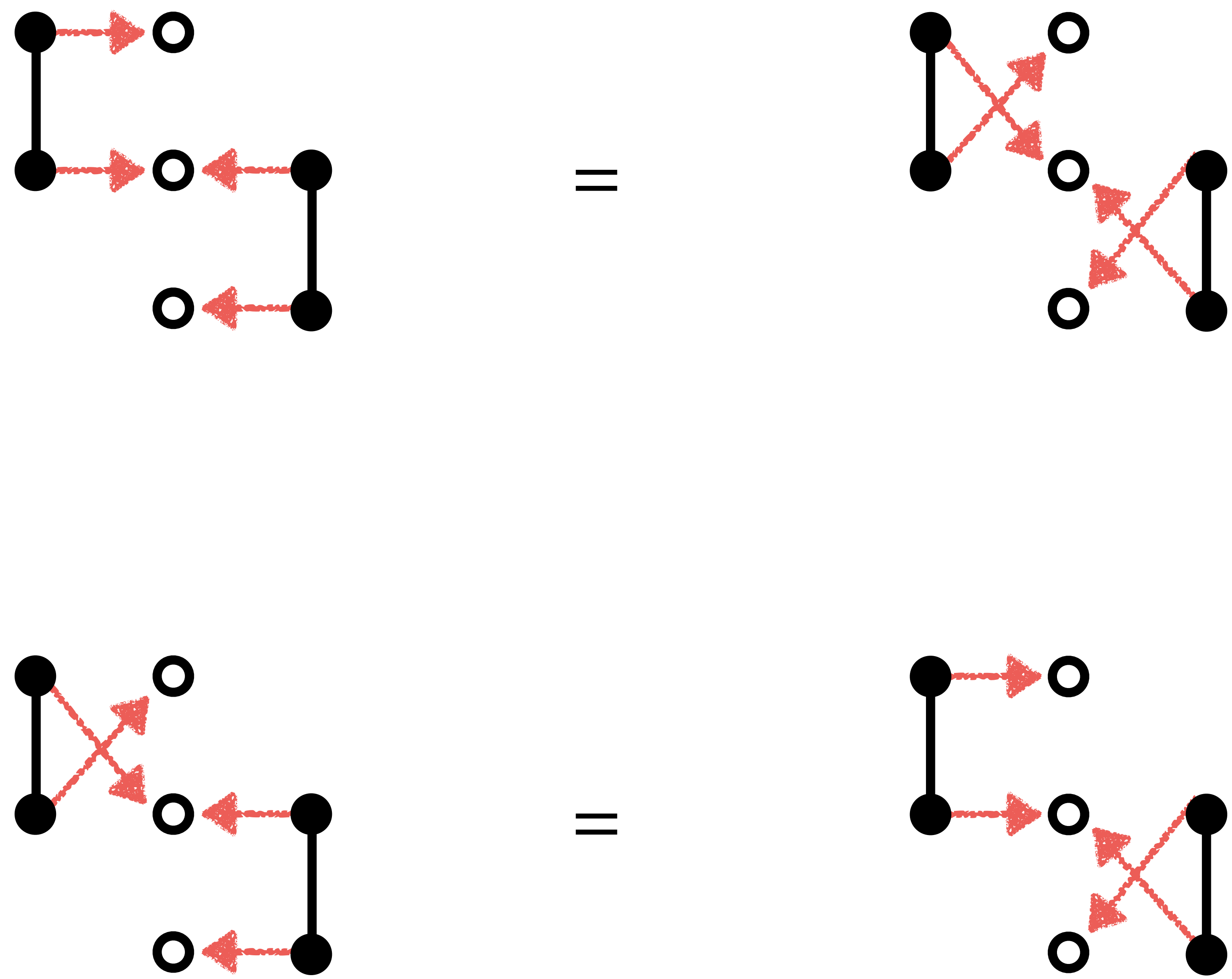
$\vdash \bot \otimes \bot, 1, 1, 1, \bot \otimes \bot$



$$\vdash \bot \otimes \bot,\ 1,\ 1,\ 1,\ \bot \otimes \bot$$



$\vdash \bot \otimes \bot, 1, 1, 1, \bot \otimes \bot$



$$\vdash \bot \otimes \bot,\ 1,\ 1,\ 1,\ \bot \otimes \bot$$

Parity

- A relationship between **two proofs** of the **same sequent**.
- Two proof nets for the same sequent stand in **even** or **odd** relationship to each other.
- **Equivalent** proof nets are always **evenly** related.

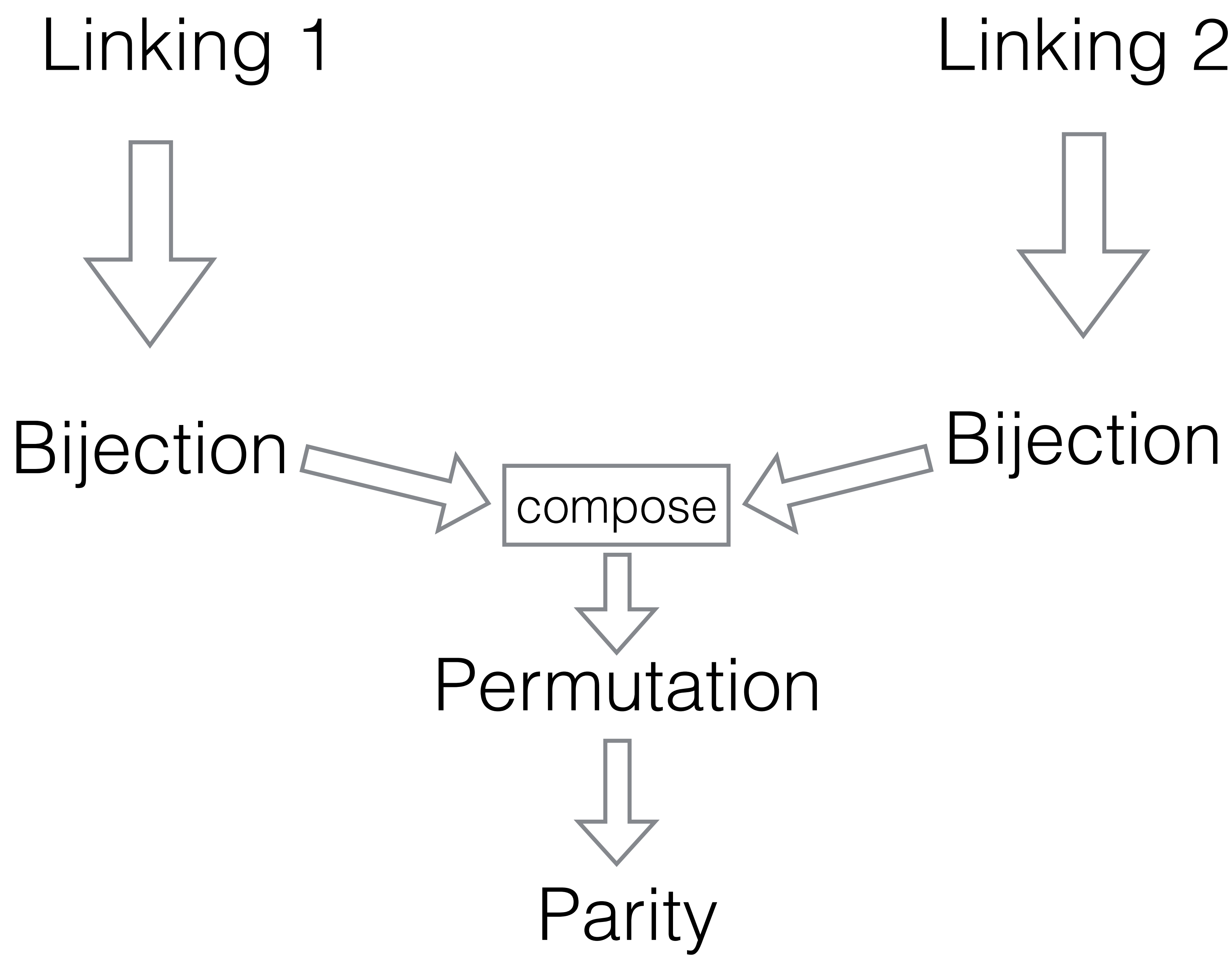
Parity defined

Sequent
+ Linking
+ Switching

A bijection between two sets associated with the sequent.

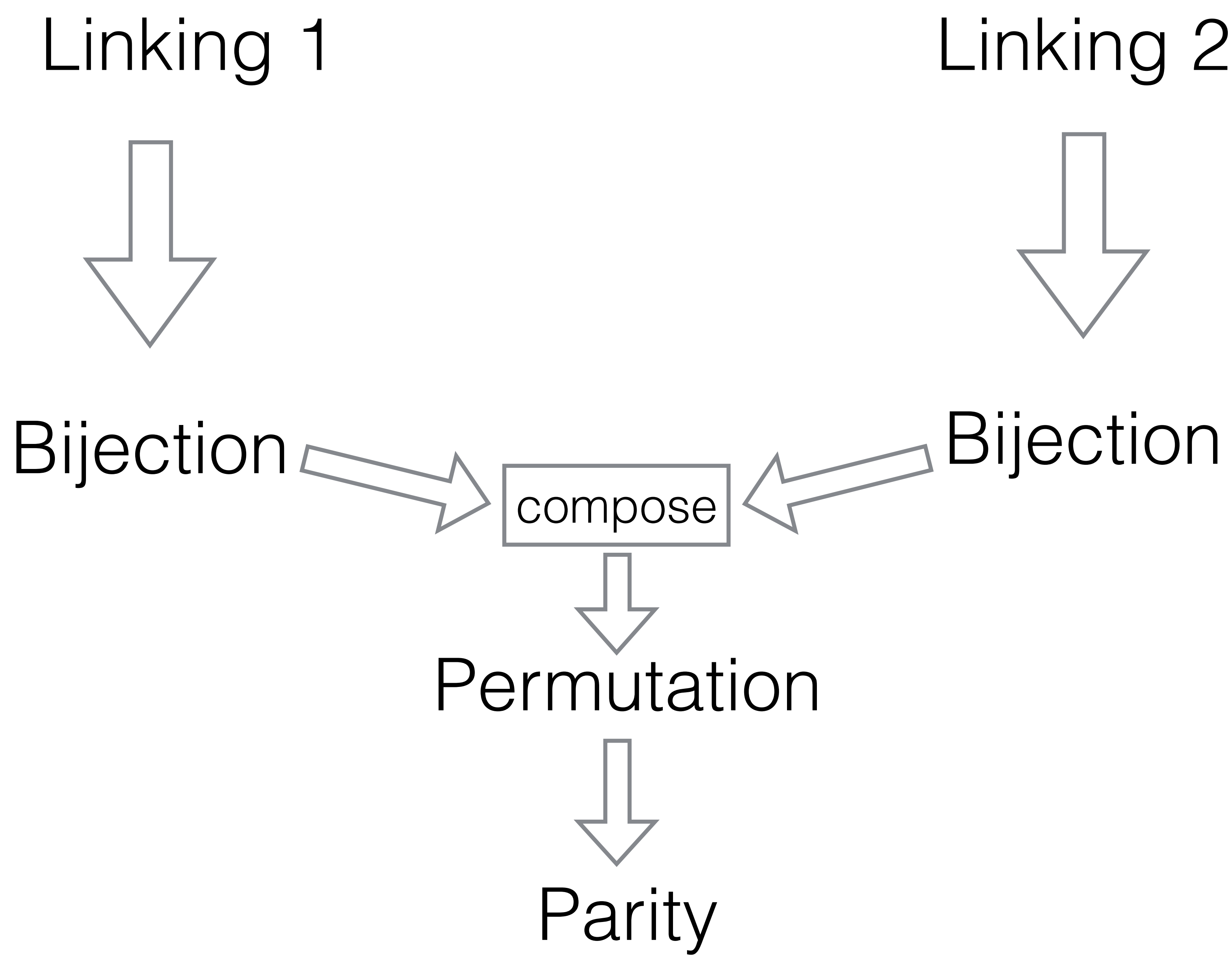
Parity defined

Sequent + Switching



Parity defined

Sequent + ~~Switching~~



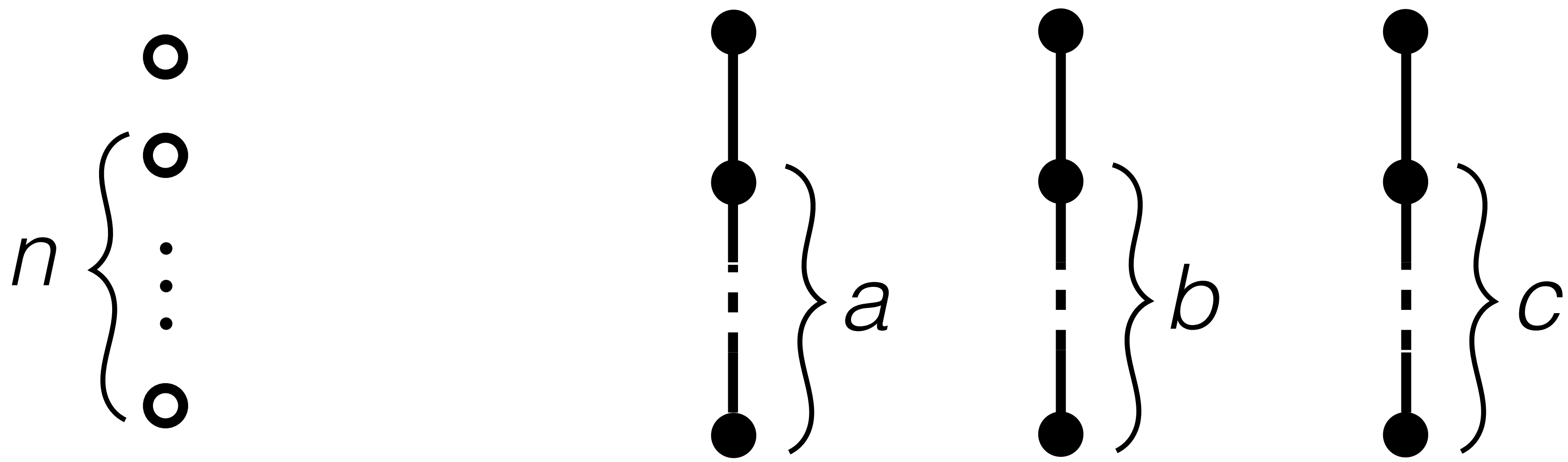
Parity

- Equivalent proofs have even parity

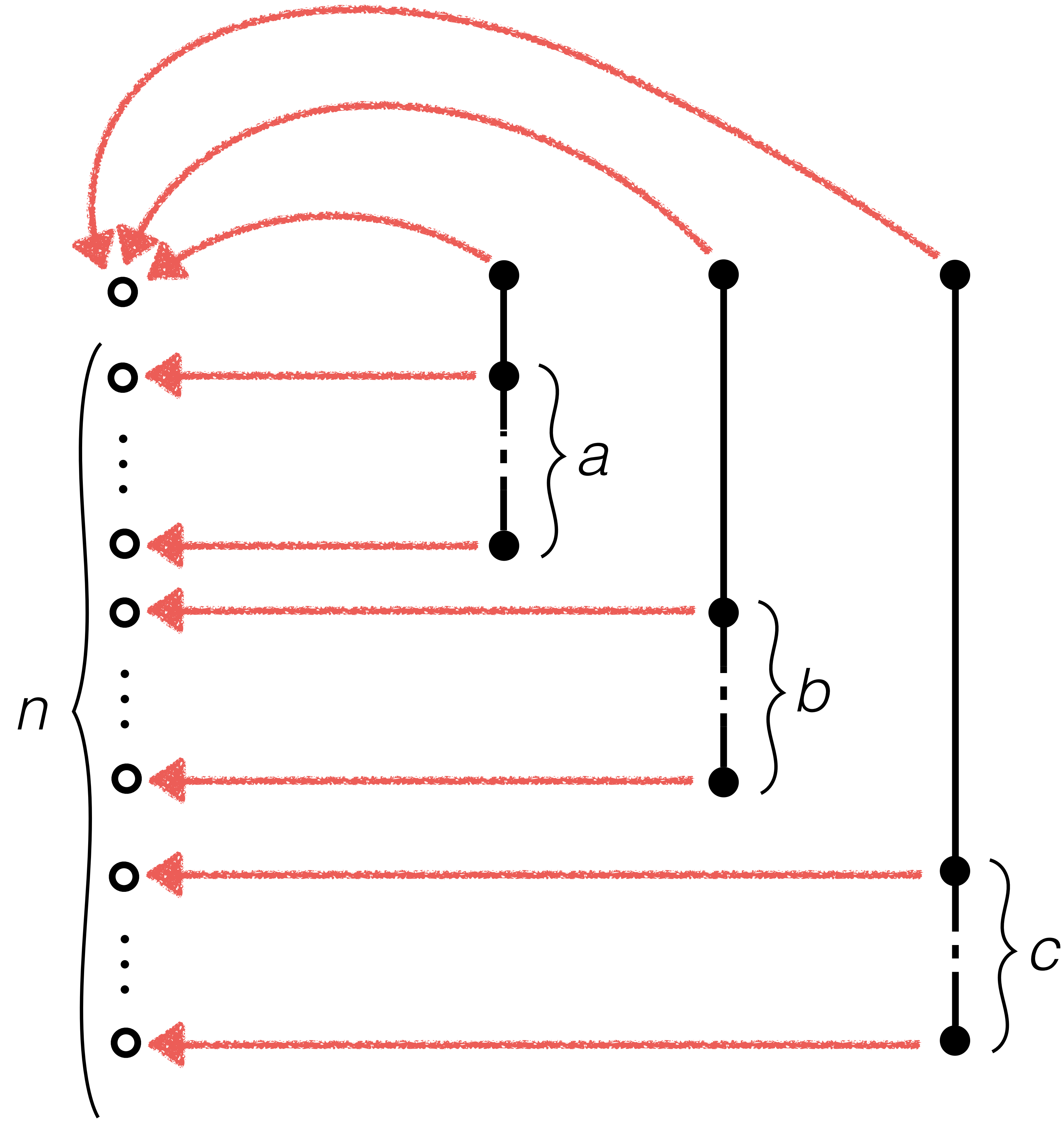
Worked example

(if there’s time)

“Matching”

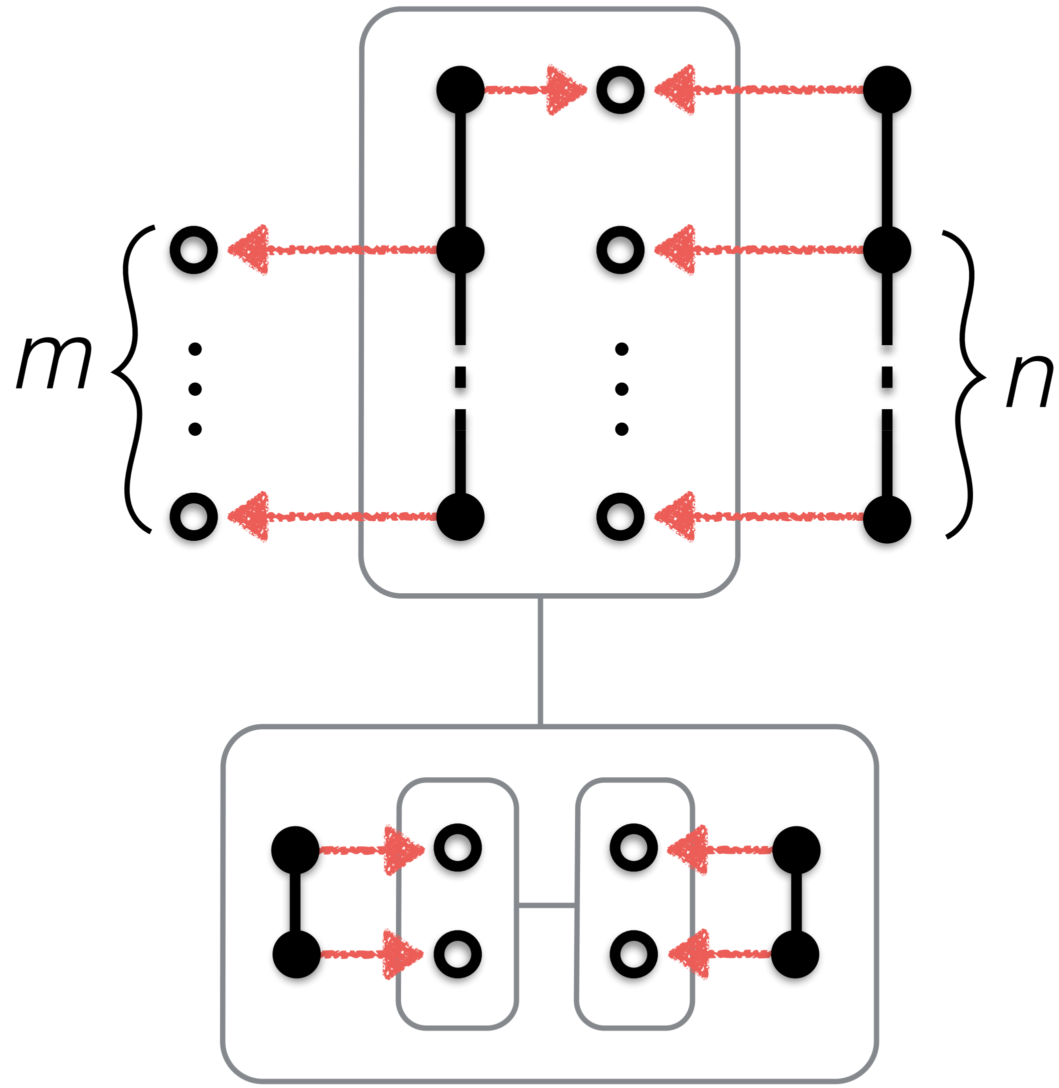


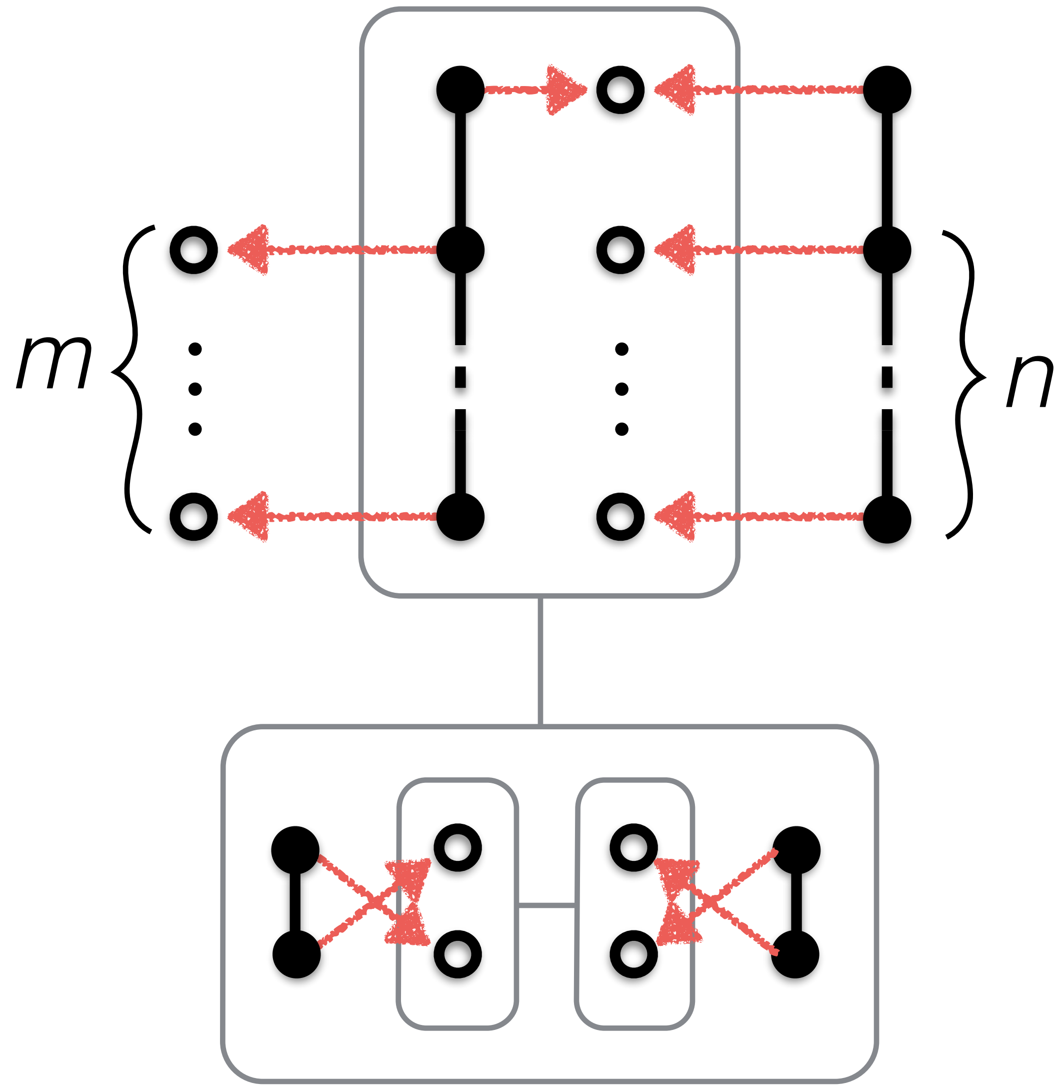
Provable iff n = a+b+c



Provable iff n = a+b+c

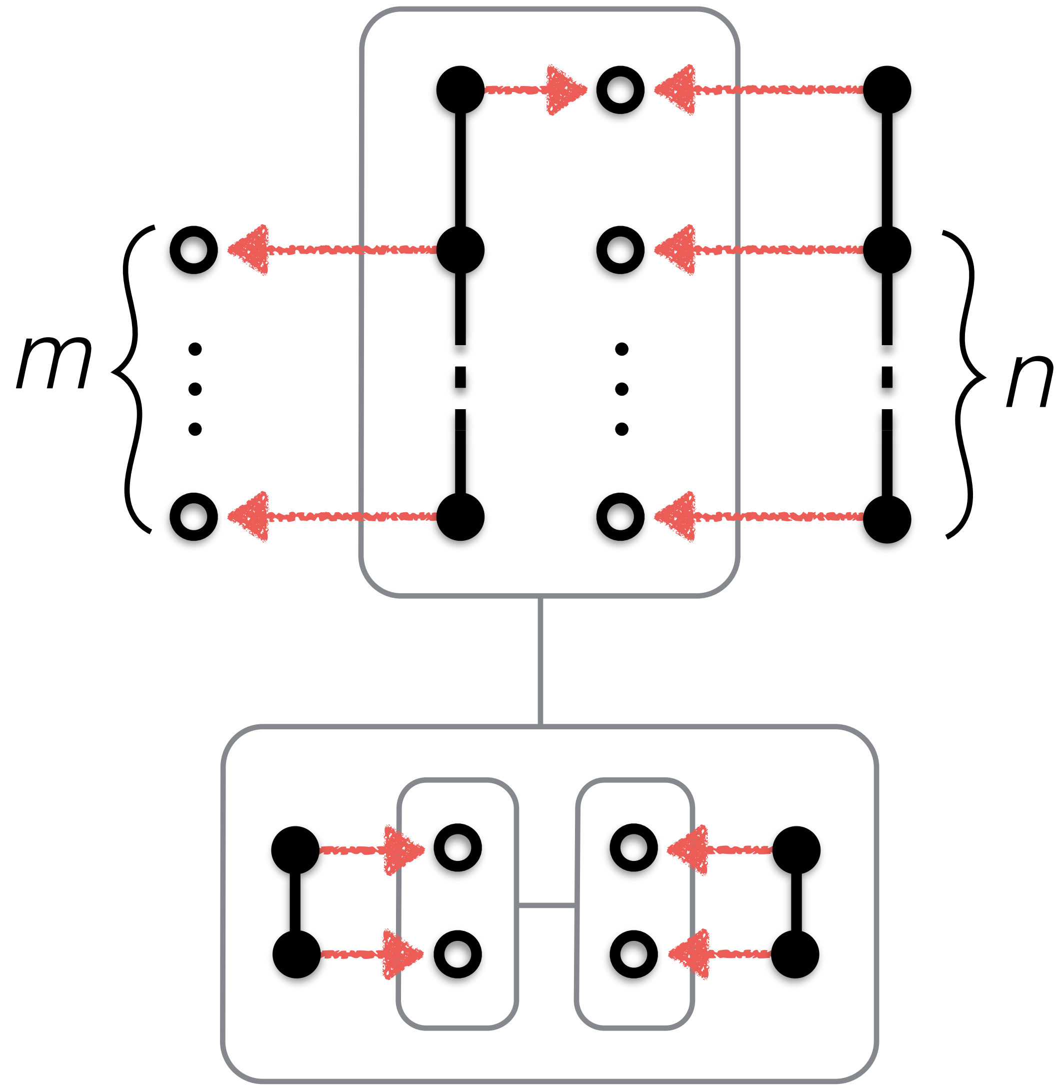
Using matching to encode arithmetic questions





m
n

Equivalent iff $m \geq n$



References

- Todd Trimble. Linear logic, bimodules, and full coherence for autonomous categories. PhD thesis, Rutgers University, 1994.

- Richard Blute, Robin Cockett, Robert Seely, and Todd Trimble. Natural deduction and coherence for weakly distributive categories. Journal of Pure and Applied Algebra, 113: 220–296, 1996.

- Dominic J.D. Hughes. Simple free star-autonomous categories and full coherence. 2012.

References

- Gary William Flake and Eric B. Baum. Rush hour is PSPACE-complete, or “Why you should generously tip parking lot attendants”. Theoretical Computer Science, 270 (1–2):895–911, 2002.

- Robert A. Hearn and Erik D. Demaine. PSPACE-completeness of sliding-block puzzles and other problems through the nondeterministic constraint logic model of computation. Theoretical Computer Science, 343(1–2):72–96, 2005.

- Robert A Hearn and Erik D Demaine. Games, puzzles, and computation. AK Peters, Ltd., 2009.