Attack of the Exponentials

Damiano Mazza

LIPN, CNRS – Université Paris 13, France

LL2016, Lyon
school: 7 and 8 November 2016

Something is missing...

- Consider the following tautologies:
  1. $\neg X \vee \neg Y \vee X$;
  2. $(X \wedge Y \wedge \neg Z) \vee (X \wedge \neg Y) \vee \neg X \vee Z$.

Something is missing...

- Consider the following tautologies:
  1. $\neg X \vee \neg Y \vee X$;
  2. $(X \wedge Y \wedge \neg Z) \vee (X \wedge \neg Y) \vee \neg X \vee Z$.
- Are they provable in multiplicative linear logic?

Something is missing...

- Consider the following tautologies:
  1. $\neg X \vee \neg Y \vee X$;
  2. $(X \wedge Y \wedge \neg Z) \vee (X \wedge \neg Y) \vee \neg X \vee Z$.
- Are they provable in multiplicative linear logic?

$$X^{\perp} \quad \parr \quad Y^{\perp} \qquad \parr \quad X$$

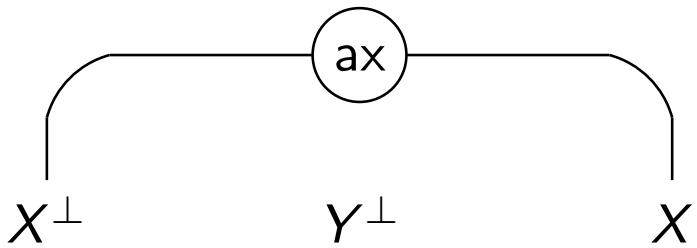
Something is missing...

- Consider the following tautologies:
  1. $\neg X \vee \neg Y \vee X$;
  2. $(X \wedge Y \wedge \neg Z) \vee (X \wedge \neg Y) \vee \neg X \vee Z$.
- Are they provable in multiplicative linear logic?

$$X^{\perp} \qquad Y^{\perp} \qquad X$$

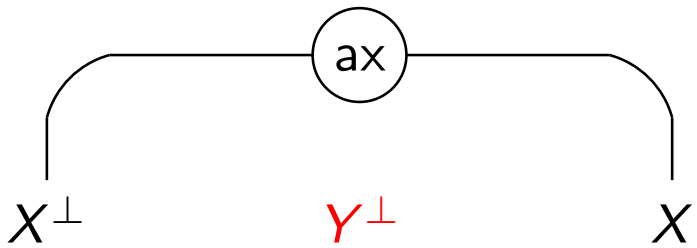
Something is missing...

- Consider the following tautologies:
  1. $\neg X \vee \neg Y \vee X$;
  2. $(X \wedge Y \wedge \neg Z) \vee (X \wedge \neg Y) \vee \neg X \vee Z$.
- Are they provable in multiplicative linear logic?



Something is missing...

- Consider the following tautologies:
  1. $\neg X \vee \neg Y \vee X$;
  2. $(X \wedge Y \wedge \neg Z) \vee (X \wedge \neg Y) \vee \neg X \vee Z$.
- Are they provable in multiplicative linear logic?



Something is missing...

- Consider the following tautologies:
  1. $\neg X \vee \neg Y \vee X$;
  2. $(X \wedge Y \wedge \neg Z) \vee (X \wedge \neg Y) \vee \neg X \vee Z$.
- Are they provable in multiplicative linear logic?

$$(X \otimes Y \otimes Z^{\perp}) \quad ⅋ \quad (X \otimes Y^{\perp}) \quad ⅋ \quad X^{\perp} \quad ⅋ \quad Z$$

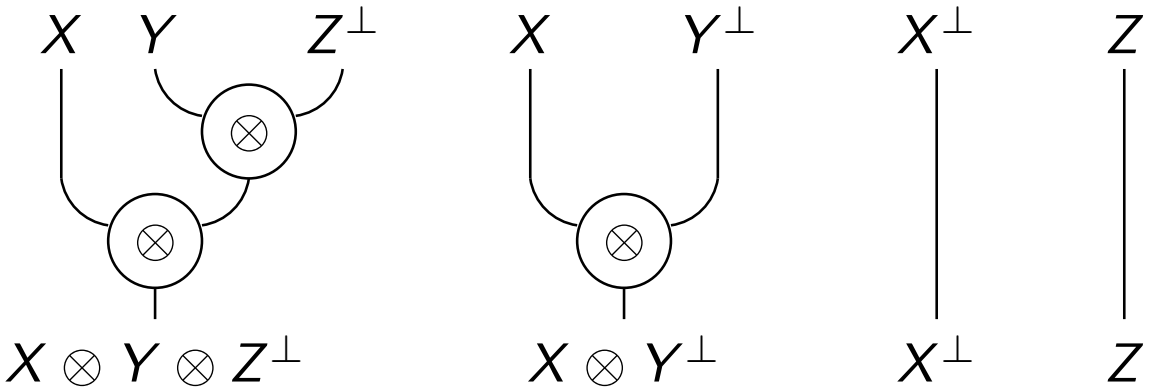
Something is missing...

- Consider the following tautologies:
  1. $\neg X \vee \neg Y \vee X$;
  2. $(X \wedge Y \wedge \neg Z) \vee (X \wedge \neg Y) \vee \neg X \vee Z$.
- Are they provable in multiplicative linear logic?

$$X \otimes Y \otimes Z^{\perp} \qquad X \otimes Y^{\perp} \qquad X^{\perp} \qquad Z$$

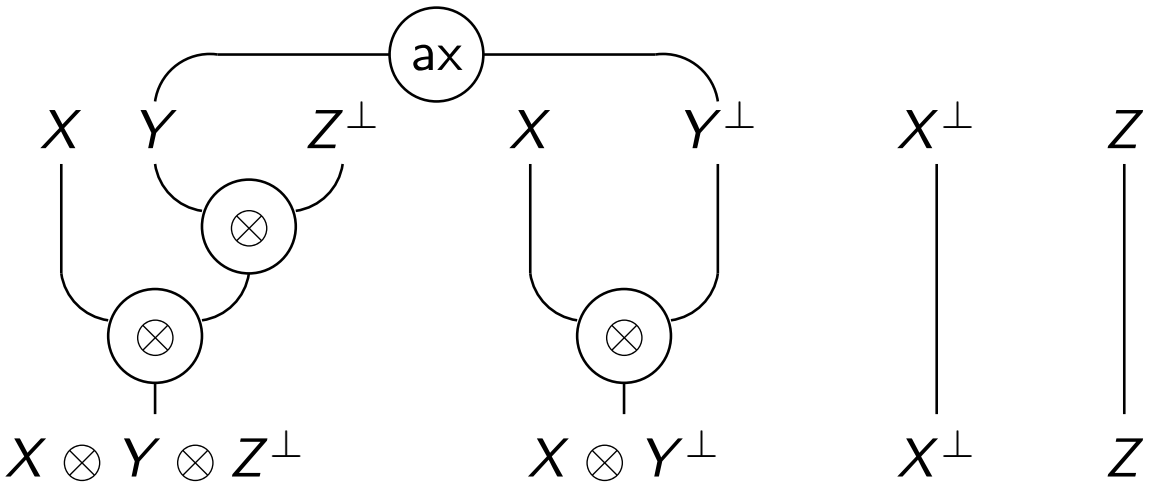
Something is missing...

- Consider the following tautologies:
  1. $\neg X \vee \neg Y \vee X$;
  2. $(X \wedge Y \wedge \neg Z) \vee (X \wedge \neg Y) \vee \neg X \vee Z$.
- Are they provable in multiplicative linear logic?



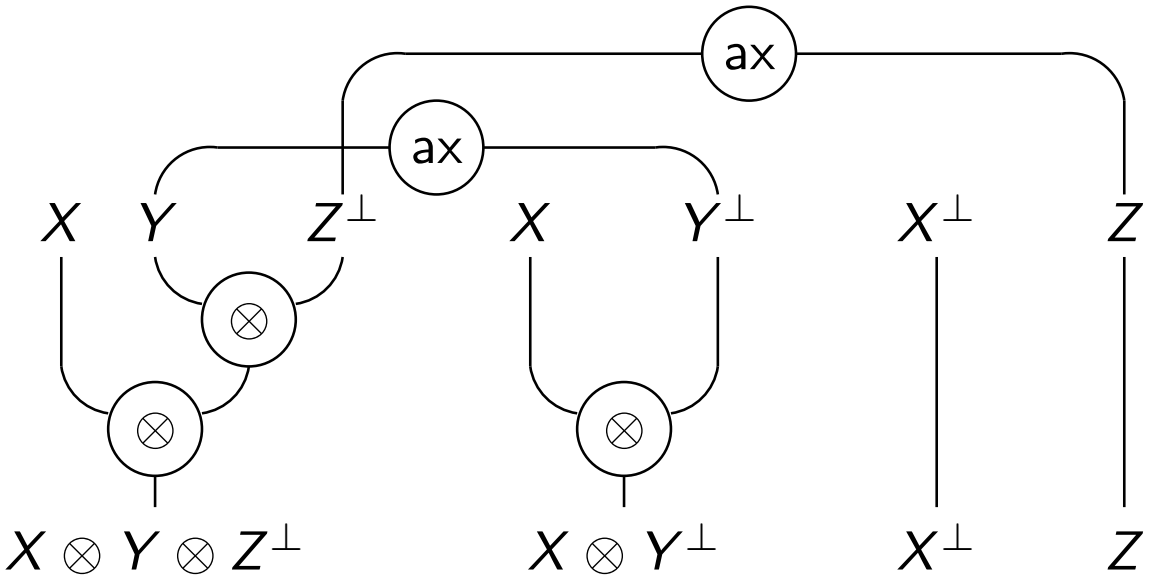
Something is missing...

- Consider the following tautologies:
  1. $\neg X \vee \neg Y \vee X$;
  2. $(X \wedge Y \wedge \neg Z) \vee (X \wedge \neg Y) \vee \neg X \vee Z$.
- Are they provable in multiplicative linear logic?



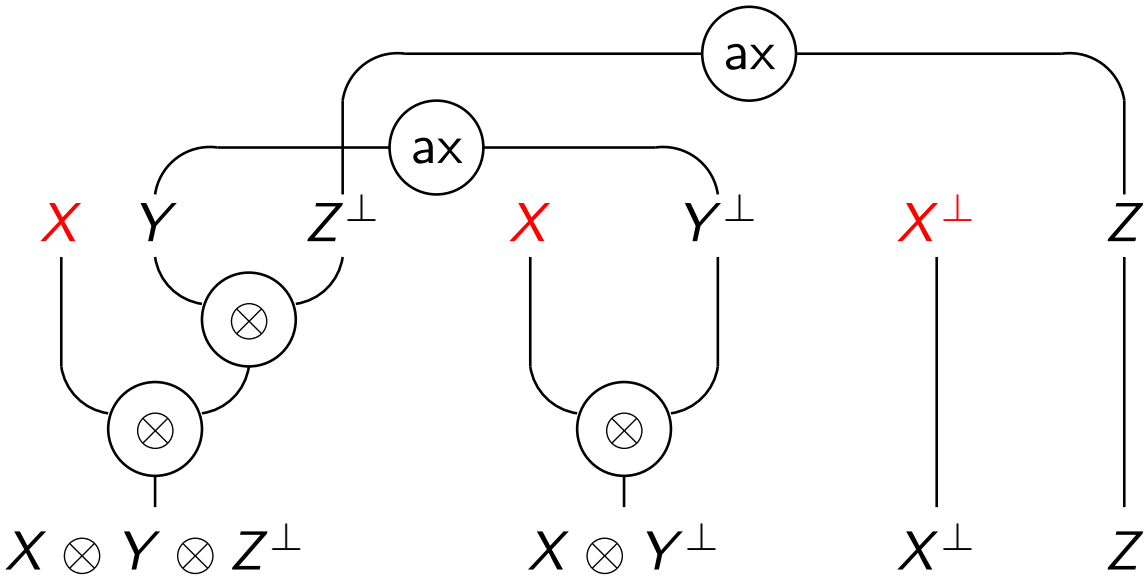
Something is missing...

- Consider the following tautologies:
  1. $\neg X \vee \neg Y \vee X$;
  2. $(X \wedge Y \wedge \neg Z) \vee (X \wedge \neg Y) \vee \neg X \vee Z$.
- Are they provable in multiplicative linear logic?



Something is missing...

- Consider the following tautologies:
  1. $\neg X \vee \neg Y \vee X$;
  2. $(X \wedge Y \wedge \neg Z) \vee (X \wedge \neg Y) \vee \neg X \vee Z$.
- Are they provable in multiplicative linear logic?



Structural rules

- Mathematical truth is *cumulative* and *inexhaustible*:

$$\frac{\Gamma \vdash C}{\Gamma, A \vdash C}\ \text{weakening} \qquad \frac{\Gamma, A, A \vdash C}{\Gamma, A \vdash C}\ \text{contraction}$$

Structural rules

- Mathematical truth is *cumulative* and *inexhaustible*:

$$\frac{\Gamma \vdash C}{\Gamma, A \vdash C}\ \text{weakening} \qquad \frac{\Gamma, A, A \vdash C}{\Gamma, A \vdash C}\ \text{contraction}$$

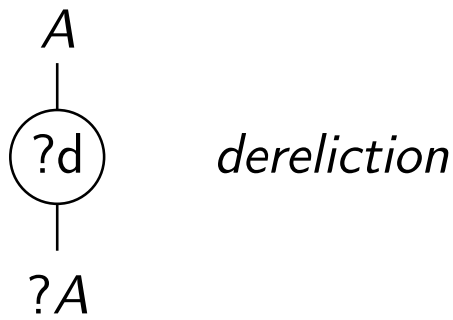
- Linear logic replaces truth with the notion of *resource*:
  - no structural rules on arbitrary formulas;
  - in other words, no arbitrary erasing and duplication:

$$A \not\multimap 1$$
$$A \not\multimap A \otimes A$$

The "why not" modality

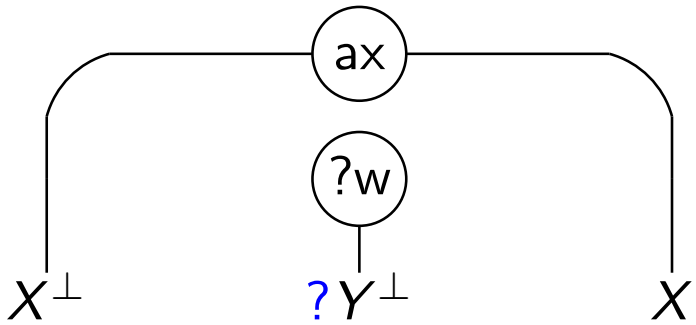
- We introduce a unary connective (*modality*) "why not", denoted by ?.
- Structural rules are allowed only on formulas of the form $?A$:

- We need to explicitly declare a formula as "contractible":



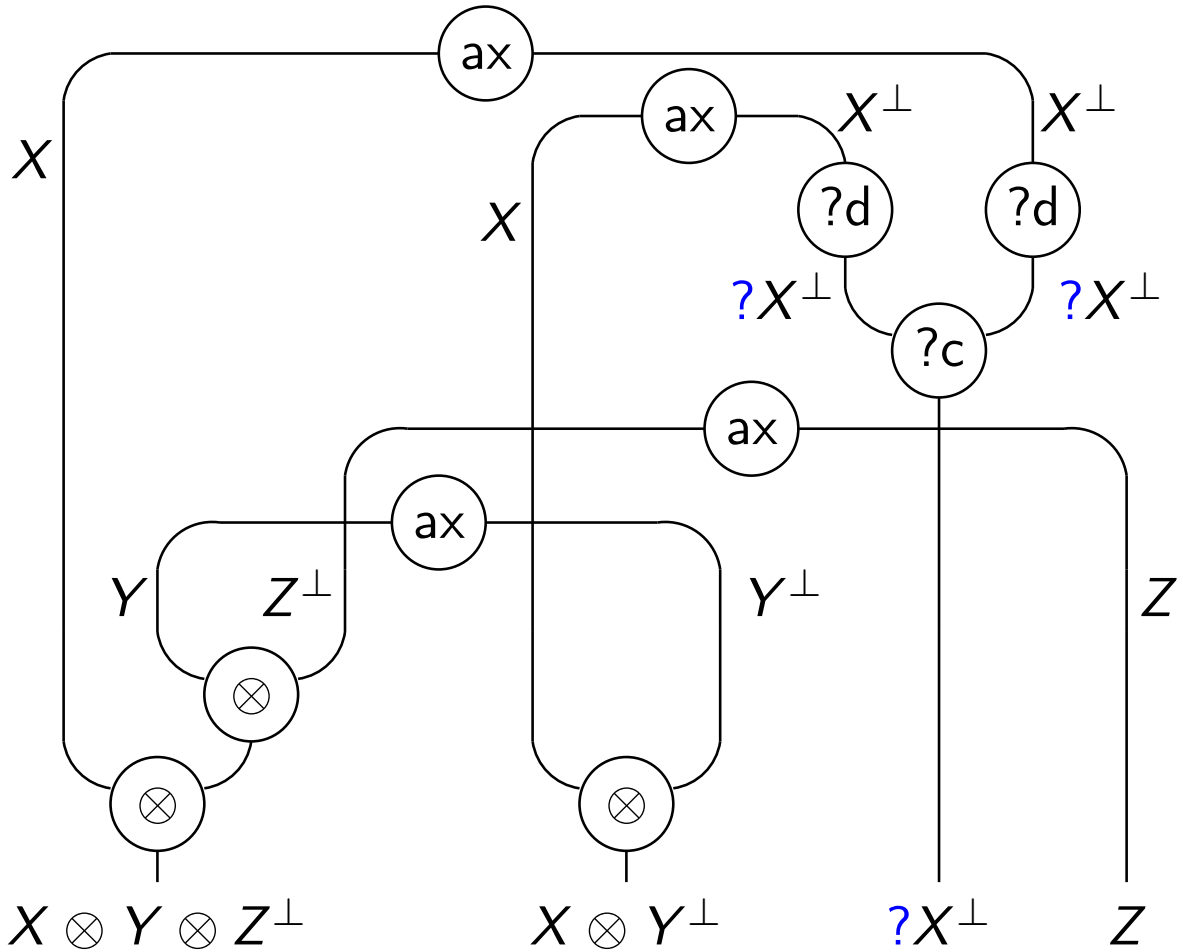
Revisiting classical tautologies

- Instead of $\neg X \vee \neg Y \vee X$, we prove $X^{\perp} \parr ?Y^{\perp} \parr X$:



Revisiting classical tautologies

- Instead of $(X \wedge Y \wedge \neg Z) \vee (X \wedge \neg Y) \vee \neg X \vee Z$, we prove $(X \otimes Y \otimes Z^{\perp}) \parr (X \otimes Y^{\perp}) \parr ?X^{\perp} \parr Z$:



The meaning of linear sequents

- In classical logic, $\vdash \Gamma$ means "one of the formulas in Γ is necessarily true".
- This is because $\Gamma \vdash \Delta$ is $\bigwedge \Gamma \Rightarrow \bigvee \Delta$.
- In linear logic, $\Gamma \vdash \Delta$ is $\bigotimes \Gamma \multimap \parr \Delta$, with $A \multimap B := A^\perp \parr B$.
- What does that mean???

$A \otimes B$	simultaneous availability of both A and B
$A \multimap B$	A is needed to yield B (loosing A in the process)
$A \parr B$	$A^\perp$ is needed to yield B *and* $B^\perp$ is needed to yield A

- So, in linear logic, $\vdash A_1, \ldots, A_n$ means

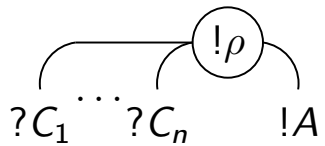
  for any $1 \leq i \leq n$, $A_1^\perp, \ldots, A_{i-1}^\perp, A_{i+1}^\perp, \ldots, A_n^\perp$ are needed to obtain A_i.

- The meaning of "why not" is best understood via duality:

$?A$	$A^\perp$ is needed an unspecified number of times
$!A$	A is available at will

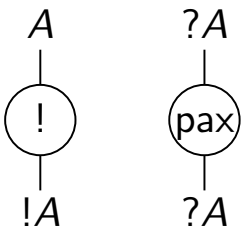
The "of course" modality

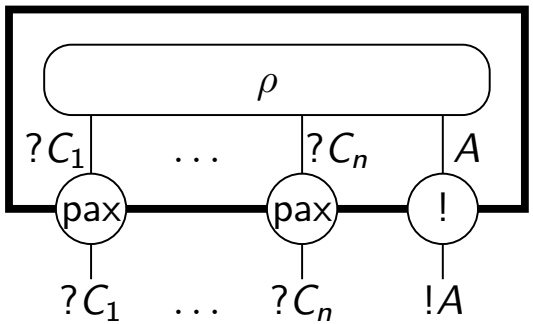
- The dual of "why not" is "of course", or "bang", denoted !.
- Two alternative presentations in nets:
  - **inductive:** nets are defined inductively on their *exponential depth*:
    - *depth* 0: as for MLL, with nodes ax, cut, $\otimes$, $\parr$, ?d, ?w and ?c;
    - *depth* $n > 0$: as above but also with nodes of the form



where ρ is a net of depth $< n$, of conclusions $?C_1, \ldots, ?C_n, A$.

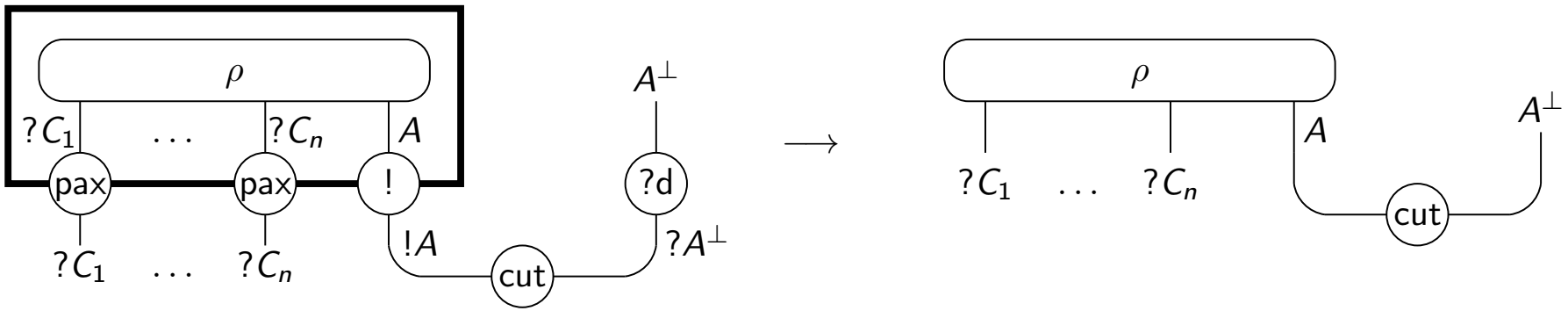
  - **global:** as depth 0 above but also with nodes ! and pax; each pax has an associated !, and each ! has an associated subnet, called *box*:





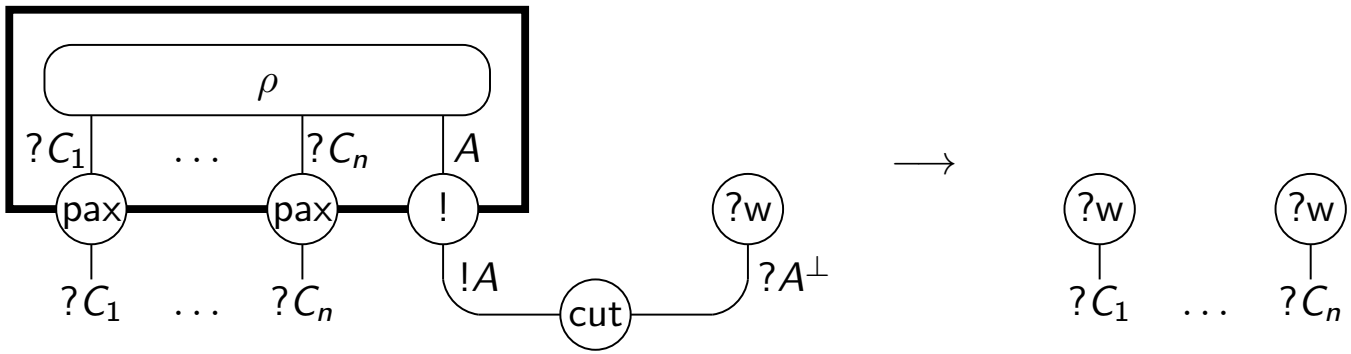
Boxes are either disjoint or included one in the other.

Cut-elimination: dereliction



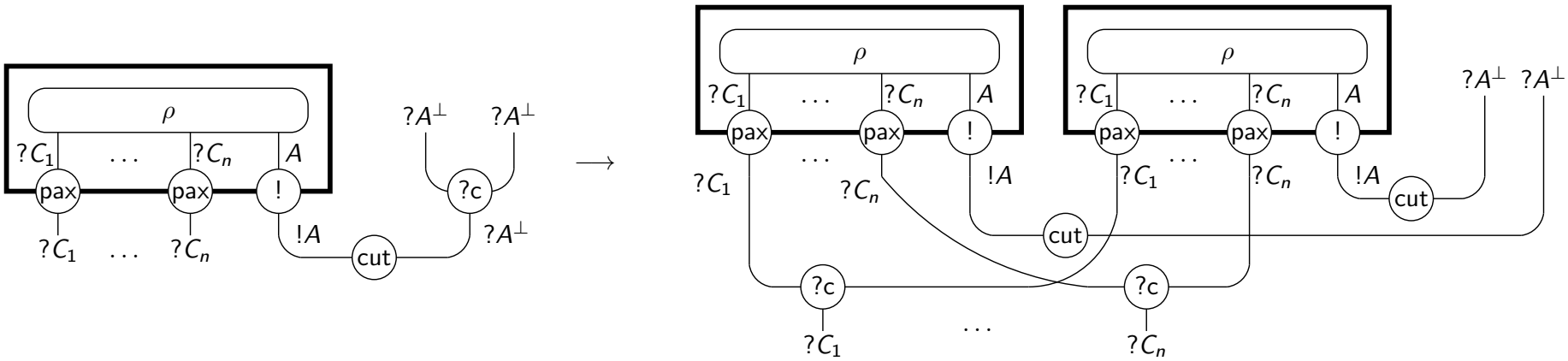
Dereliction "opens" a box.

Cut-elimination: weakening



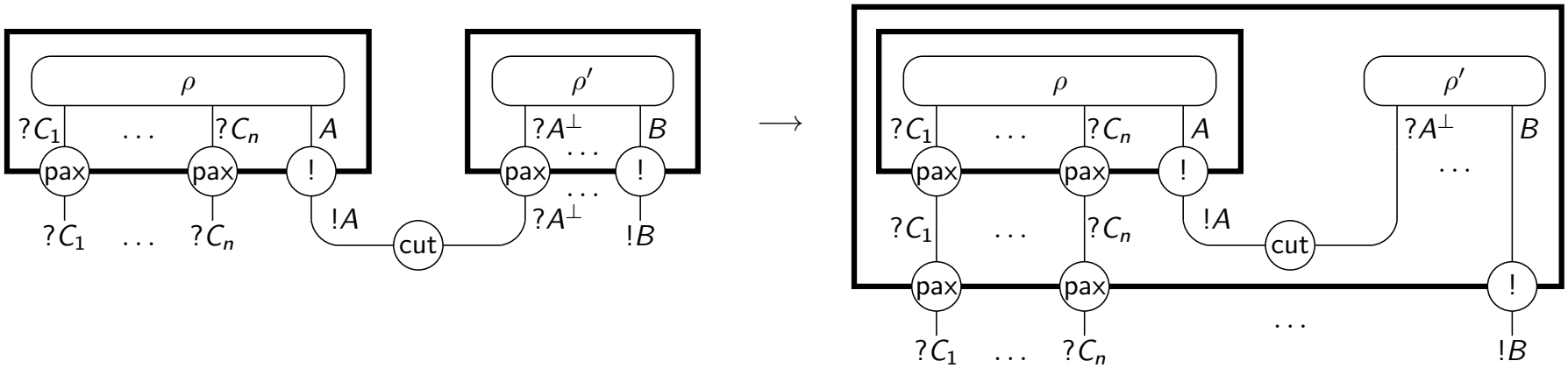
Weakening erases a box.

Cut-elimination: contraction



Contraction duplicates a box.

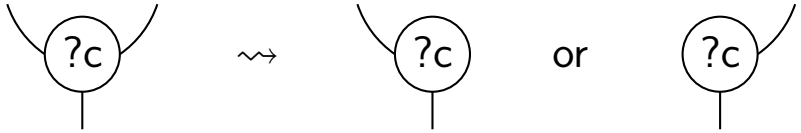
Cut-elimination: commutative step



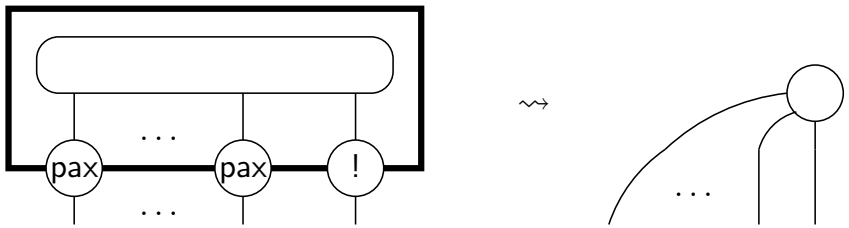
A box may "enter" inside another box.

Correctness

- Contractions are treated like $\parr$ nodes:



- Boxes are "collapsed" to a single node (that's already the case in the inductive formulation):



- A proof net is a net such that:
  - every switching (graph obtained as above) is acyclic;
  - the contents of every box is a proof net.
- Preserved by cut-elimination: ρ correct, $\rho \longrightarrow \rho'$ implies ρ' correct.
- Lack of connectedness causes a little technical problem...

Exponentials in sequent calculus

- Sequent calculus rules for the exponential modalities:

$$\frac{\vdash \Gamma, A}{\vdash \Gamma, ?A}\ ?d \qquad \frac{\vdash \Gamma}{\vdash \Gamma, ?A}\ ?w \qquad \frac{\vdash \Gamma, ?A, ?A}{\vdash \Gamma, ?A}\ ?c \qquad \frac{\vdash ?\Gamma, A}{\vdash ?\Gamma, !A}\ !$$

- Exponential axioms ("storage laws"):

functoriality:	$!(A \multimap B) \multimap !A \multimap !B$	
dereliction:	$!A \multimap A$	(retrieve)
digging:	$!A \multimap !!A$	(indirection)
weakening:	$!A \multimap 1$	(discard)
contraction:	$!A \multimap !A \otimes !A$	(copy)

Categorically: $!(-)$ is a monoidal comonad and free coalgebras are comonoids.

- The exponential isomorphism: $!(A \,\&\, B) \cong !A \otimes !B$ (just like $2^{a+b} = 2^a \cdot 2^b$)
- Lack of connectedness in proof nets corresponds to mix:

$$\frac{\vdash \Gamma_1 \quad \dots \quad \vdash \Gamma_n}{\vdash \Gamma_1, \dots, \Gamma_n}\ \mathrm{mix}$$

Recovering intuitionistic and classical logic

- Intuitionistic logic is actually a *fragment* of linear logic (at any order):

$$\begin{array}{rcccccccc} A, B & ::= & X & !A \multimap B & \forall \xi.A & \exists \xi.!A & 0 & A \,\&\, B & !A \oplus !B \\ & & X & A \Rightarrow B & \forall \xi.A & \exists \xi.A & \bot & A \wedge B & A \vee B \end{array}$$

Theorem (Embedding of intuitionistic logic)

$\Gamma \vdash A$ is provable in LJ iff $!\Gamma \vdash A$ is provable in the above fragment of LL.

Categorically: intuitionistic logic is the Kleisli category of the comonad $!(-)$.

- Other translations of intuitionistic logic in linear logic exist (CbN vs. CbV).
- Classical logic may also be translated:

$$\begin{array}{rcl} X^+ := ?!X & \qquad & (\neg X)^+ := ?!?X^\perp \\ (A \vee B)^+ := A^+ \parr B^+ & & (A \wedge B)^+ := ?(!A^+ \otimes !B^+) \\ (\forall x.A)^+ := ?!\forall x.A^+ & & (\exists x.A)^+ := ?!?\exists x.!A^+ \end{array}$$

The principle is the generalized Gödel translation $A^F = (A \Rightarrow F) \Rightarrow F$, with $F = \bot$.

Example: the drinker's formula

- In any bar, there's someone such that, if he drinks, then everyone drinks:

$$F := \exists x(D(x) \Rightarrow \forall y\, D(y)).$$

- Proof: either everyone's drinking, or there's someone who is not (*MrSober*).
  - 1st case: $D(z) \Rightarrow \forall y\, D(y)$ is true for any z, anybody is the existential witness;
  - 2nd case: $D(\mathit{MrSober}) \Rightarrow \forall y\, D(y)$ is true, so *MrSober* is our witness.

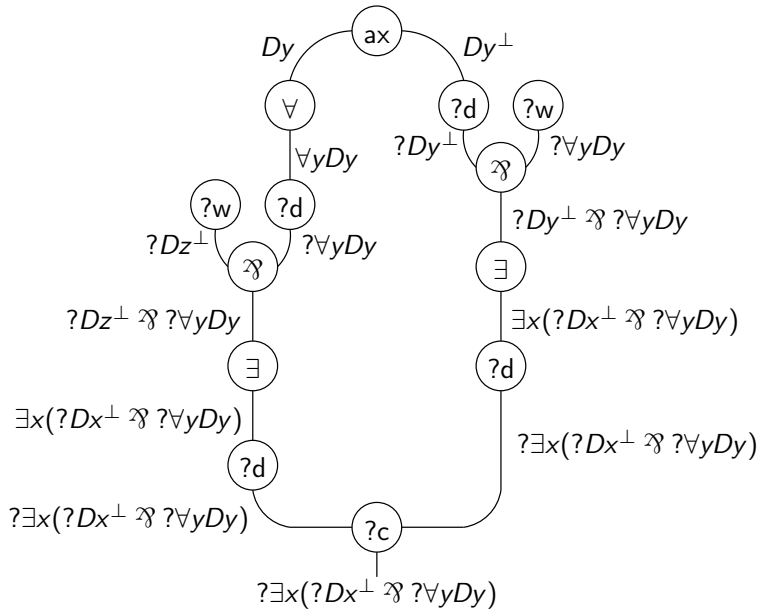
We used excluded middle (indeed, F is not provable intuitionistically).

In LK:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash Dy, \neg Dy}\,\mathrm{ax}}{\vdash Dy, \neg Dy, \forall y Dy}\,\mathrm{weak}}{\vdash Dy, \neg Dy \vee \forall y Dy}\,\vee}{\vdash Dy, F}\,\exists}{\vdash \forall y Dy, F}\,\forall}{\vdash \neg Dz, \forall y Dy, F}\,\mathrm{weak}}{\vdash \neg Dz \vee \forall y Dy, F}\,\vee}{\vdash F, F}\,\exists}{\vdash F}\,\mathrm{contr}$$

In LL:

$$F^+ \sim ?\exists x(?D(x)^\perp \parr ?\forall y D(y))$$



Curry-Howard: computation in linear logic

The Curry-Howard correspondence

logic	computer science
formula	type
proof	program
cut-elimination	execution

- Moral of the story: proof nets are programs!
- In particular: derivations of propositional NJ are simply-typed λ-terms.
- NJ (via LJ) is a fragment of LL $\Longrightarrow$ the λ-calculus embeds in proof nets.
- The decompostion $A \Rightarrow B = !A \multimap B$ appears at the level of execution:

$$(\lambda x.M)N \to M\{N/x\} \quad \text{vs.} \quad (\lambda x.M)N \to M[N/x] \to^* M\{N/x\}[N/x] \to M\{N/x\}.$$

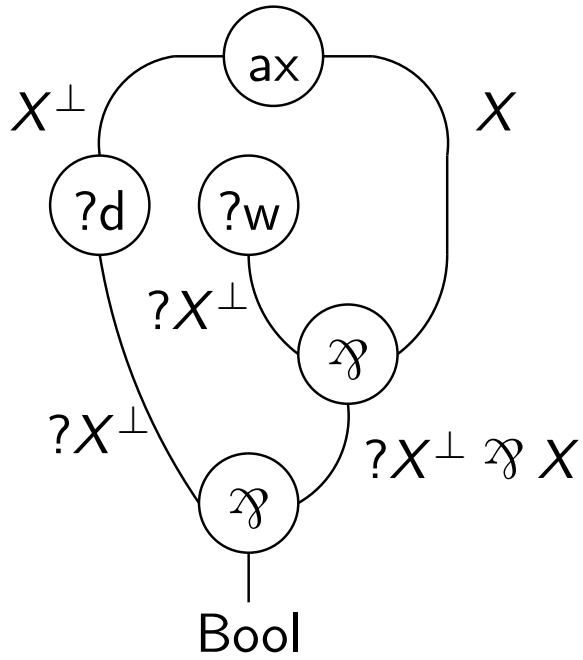
Example: Booleans and if... then... else

- Let

$$\text{Bool} \quad := \quad X \Rightarrow X \Rightarrow X \quad = \quad !X \multimap !X \multimap X \quad = \quad ?X^{\perp} \parr (?X^{\perp} \parr X).$$

- Let

$$\text{true} := \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash X^{\perp}, X}\,\text{ax}}{\vdash ?X^{\perp}, X}\,?d}{\vdash ?X^{\perp}, ?X^{\perp}, X}\,?w}{\vdash ?X^{\perp}, ?X^{\perp} \parr X}\,\parr}{\vdash \text{Bool}}\,\parr \quad \rightsquigarrow$$



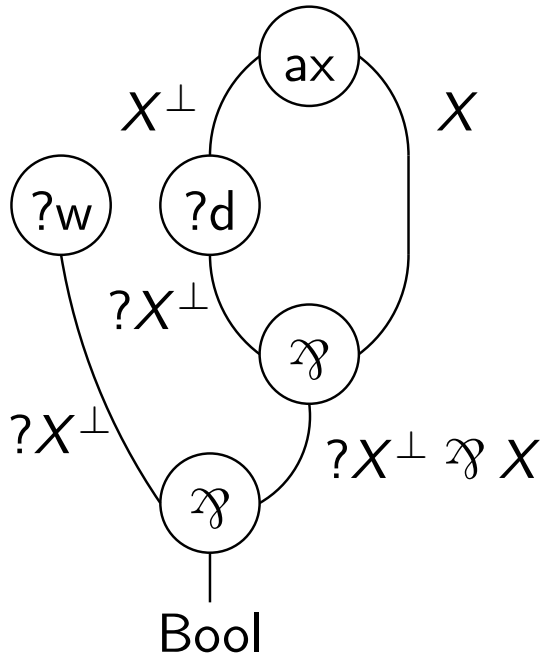
Example: Booleans and if. . . then. . . else

- Let

$$\text{Bool} \quad := \quad X \Rightarrow X \Rightarrow X \quad = \quad !X \multimap !X \multimap X \quad = \quad ?X^{\perp} \parr (?X^{\perp} \parr X).$$

- Let

$$\text{false} := \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash X^{\perp}, X}\,\text{ax}}{\vdash ?X^{\perp}, X}\,?d}{\vdash ?X^{\perp} \parr X}\,\parr}{\vdash ?X^{\perp}, ?X^{\perp} \parr X}\,?w}{\vdash \text{Bool}}\,\parr \quad \rightsquigarrow$$



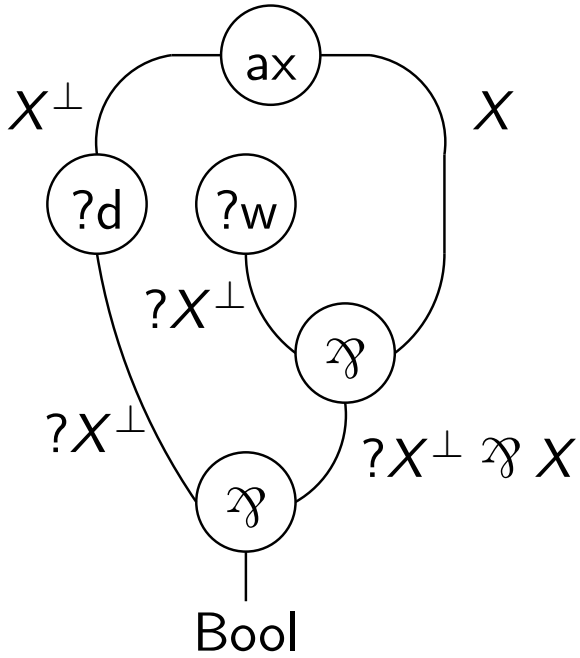
Example: Booleans and if. . . then. . . else

- Let

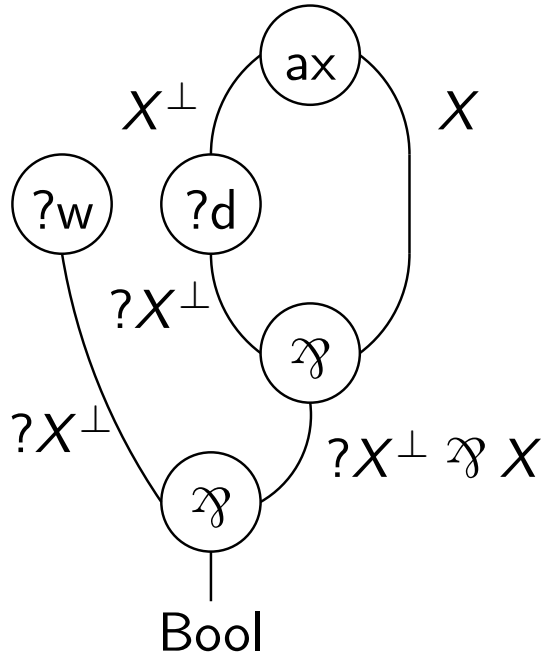
$$\mathsf{Bool} \quad := \quad X \Rightarrow X \Rightarrow X \quad = \quad !X \multimap !X \multimap X \quad = \quad ?X^{\perp} \parr (?X^{\perp} \parr X).$$

- Let

true :=



false :=



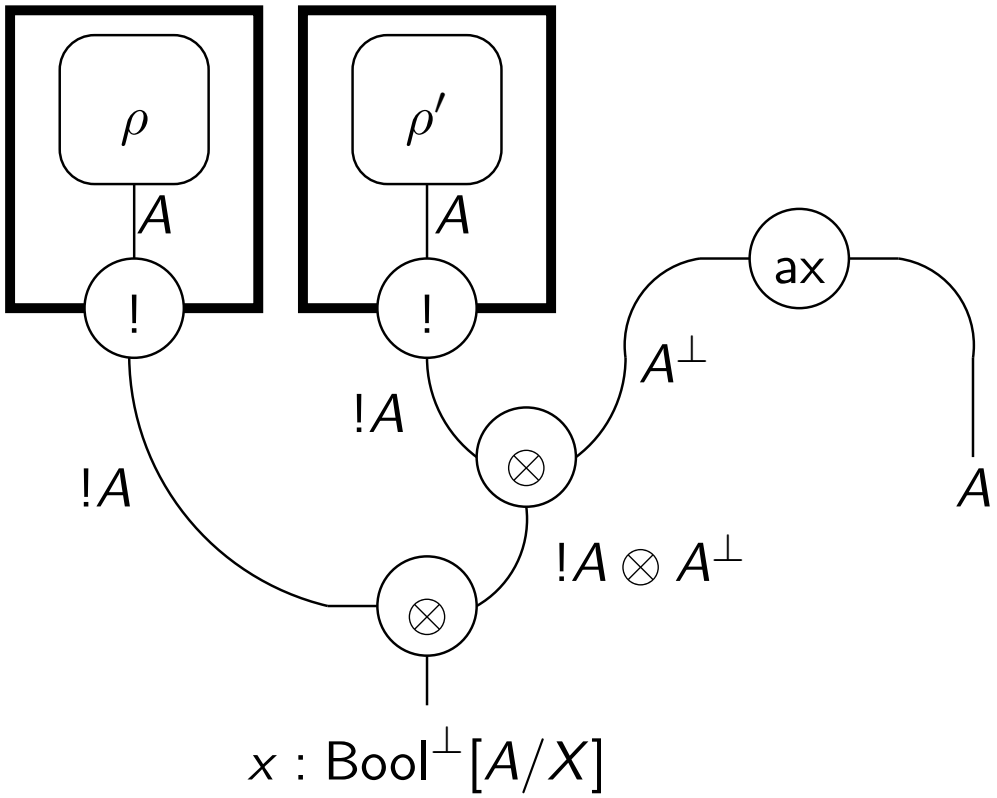
Example: Booleans and if. . . then. . . else

- We have

$$\mathsf{Bool}^{\perp} = !X \otimes (!X \otimes X^{\perp})$$

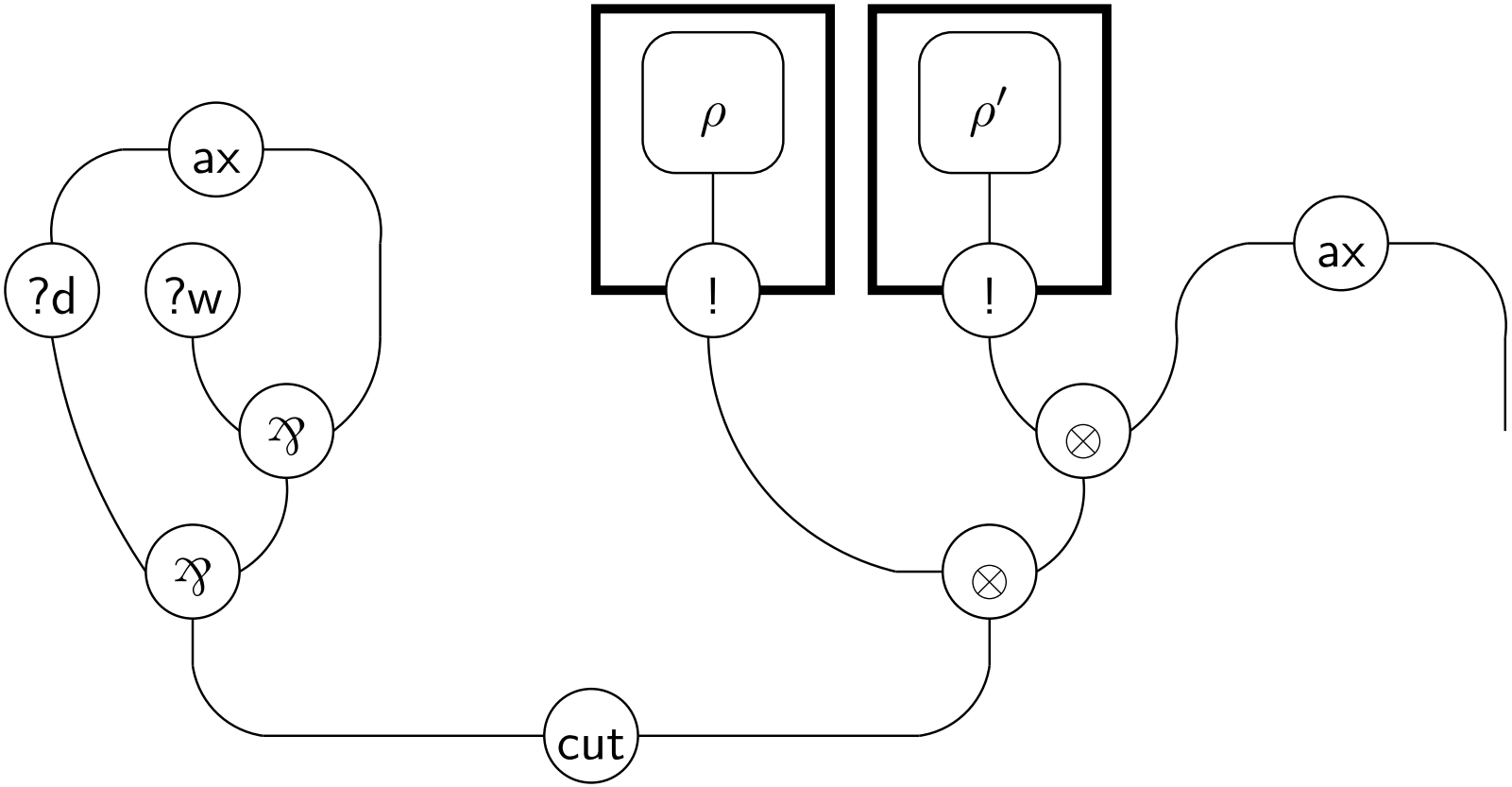
- Let $\rho, \rho' : A$ and let

if x then ρ else $\rho' :=$



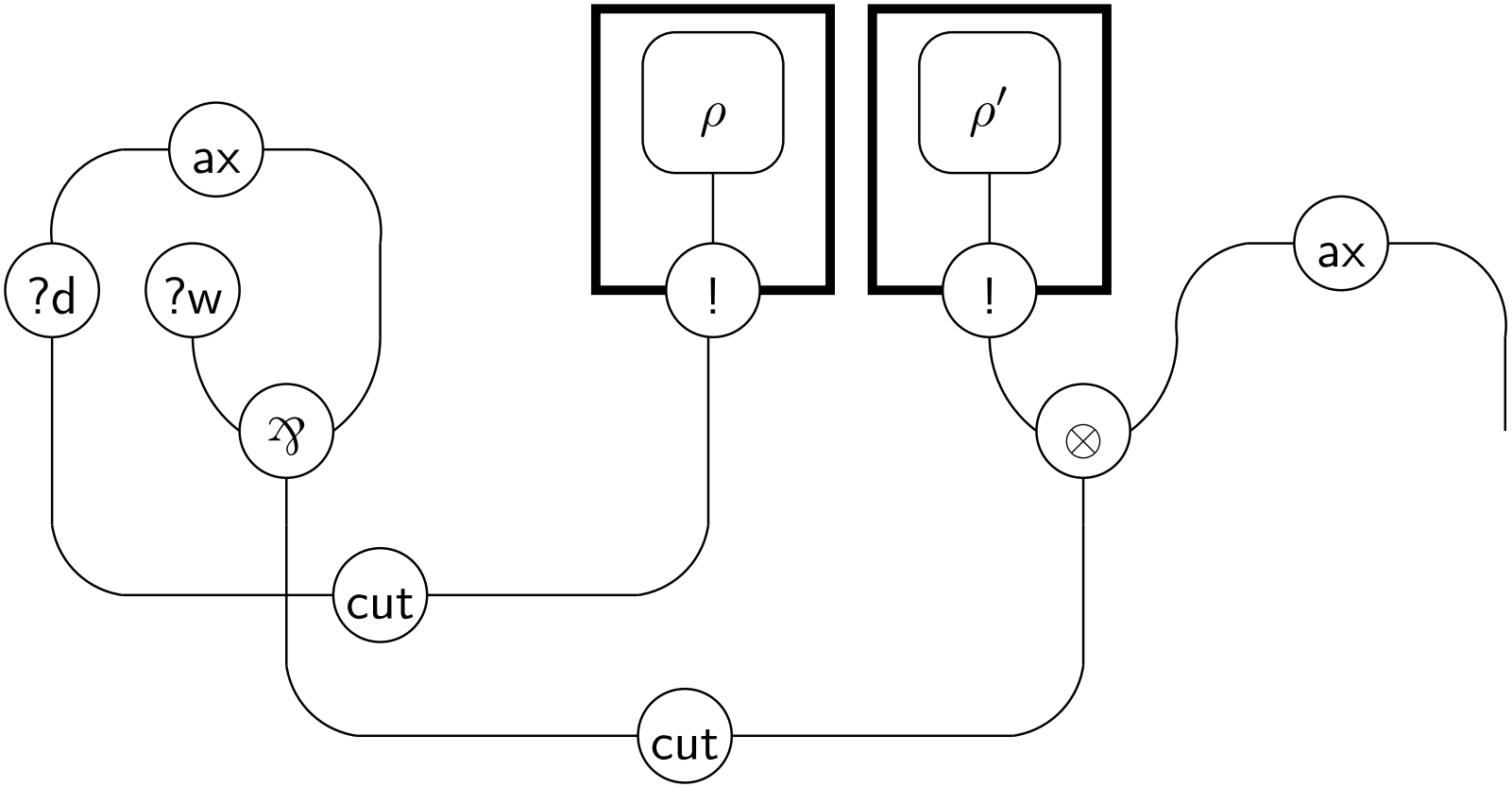
Example: Booleans and if. . . then. . . else

- Let us compute if $(\mathsf{true}[A/X])$ then ρ else ρ':



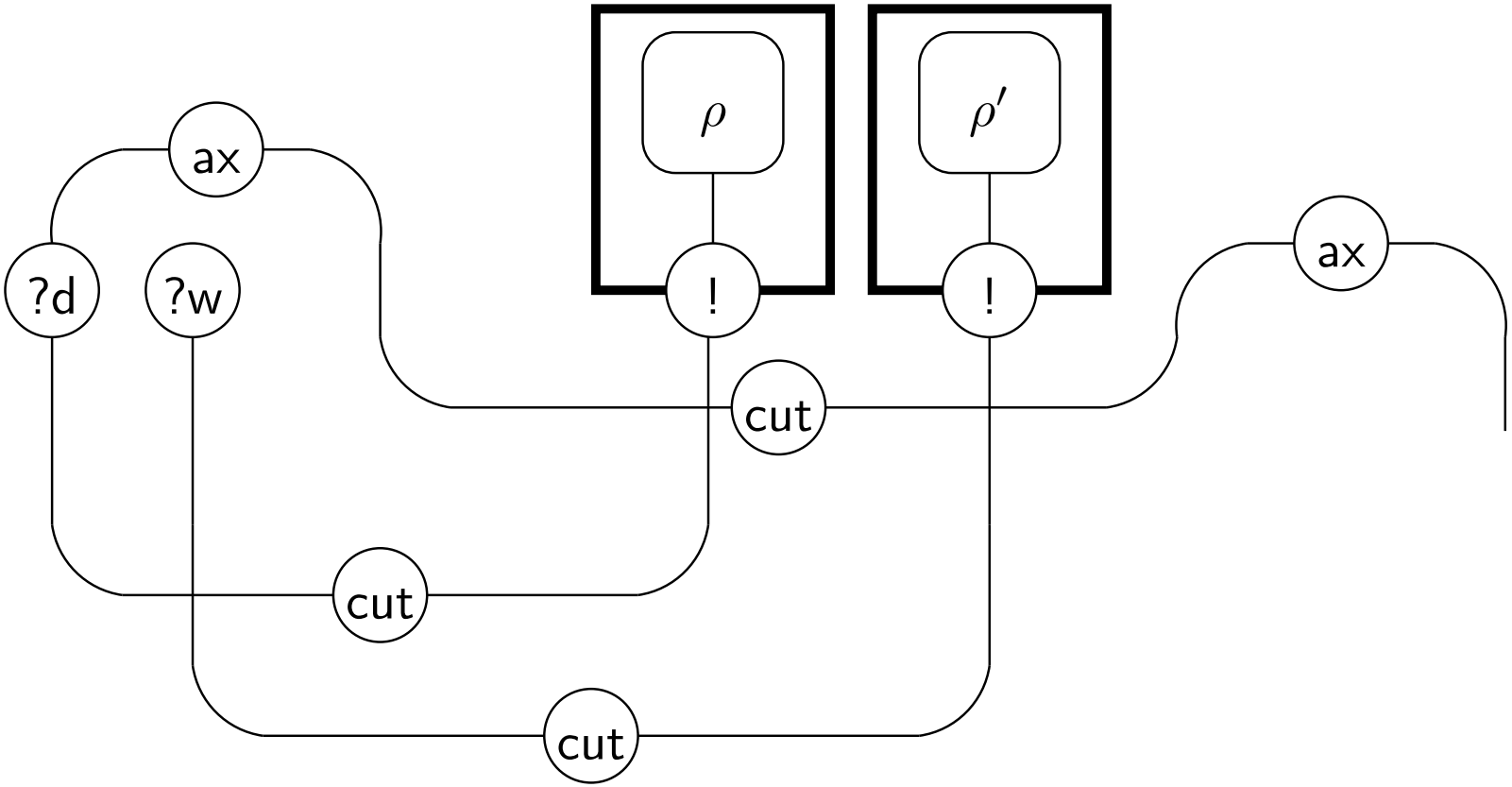
Example: Booleans and if. . . then. . . else

- Let us compute if $(\mathsf{true}[A/X])$ then ρ else ρ':



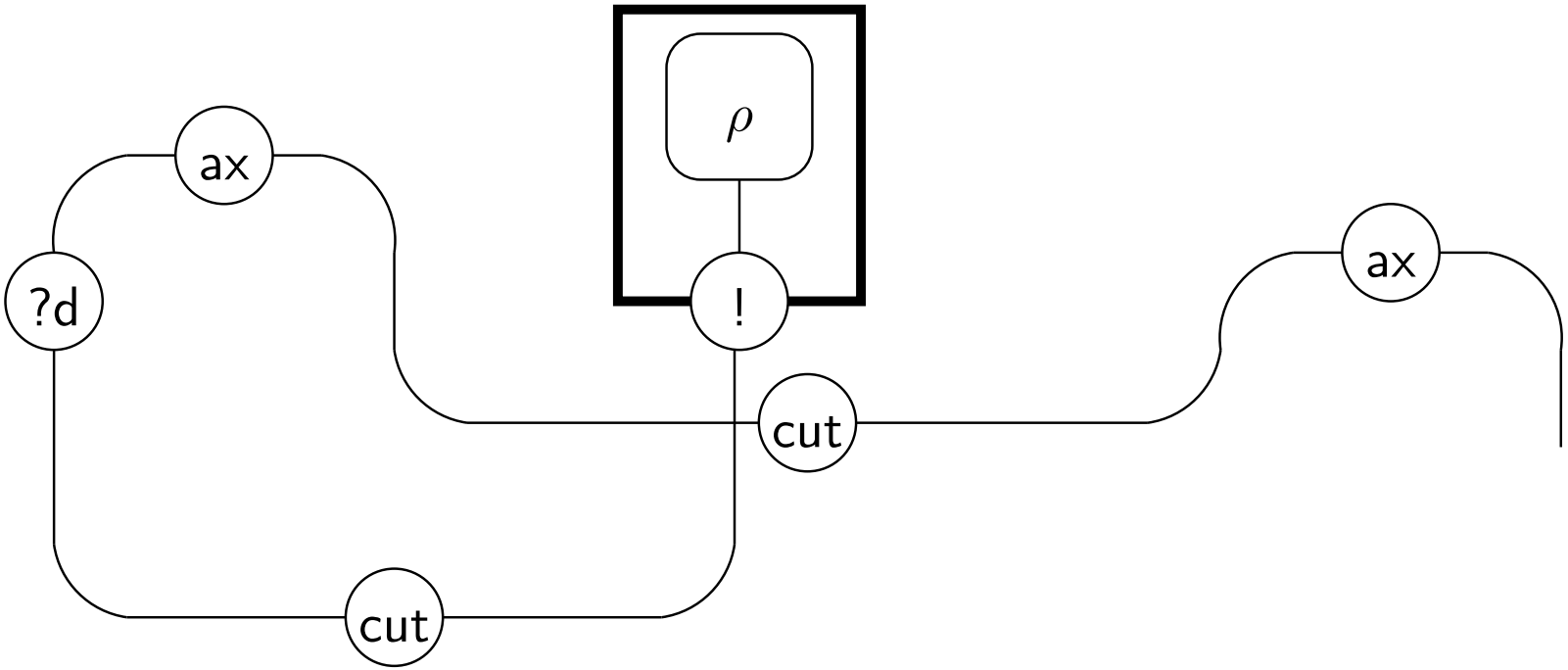
Example: Booleans and if. . . then. . . else

- Let us compute $\mathsf{if}\,(\mathsf{true}[A/X])\,\mathsf{then}\,\rho\,\mathsf{else}\,\rho'$:



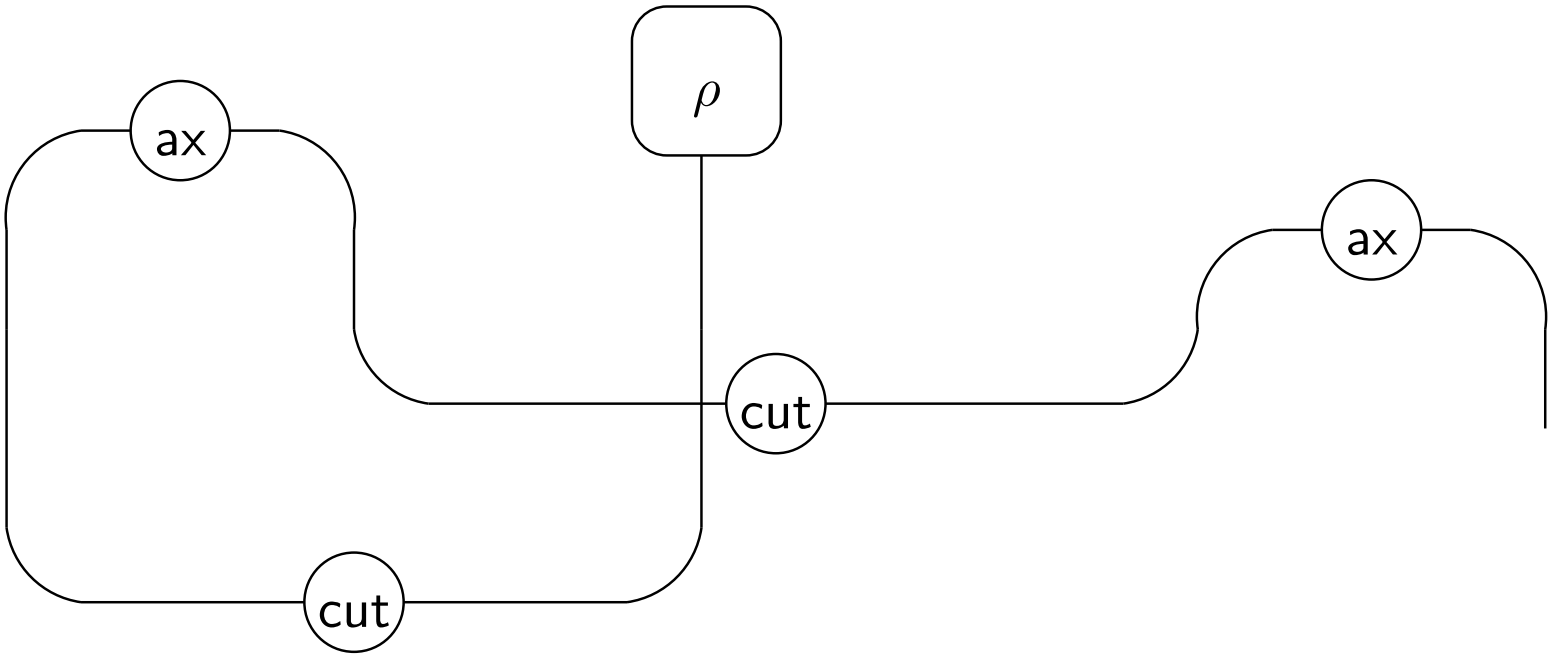
Example: Booleans and if. . . then. . . else

- Let us compute $\mathsf{if}\,(\mathsf{true}[A/X])\,\mathsf{then}\,\rho\,\mathsf{else}\,\rho'$:



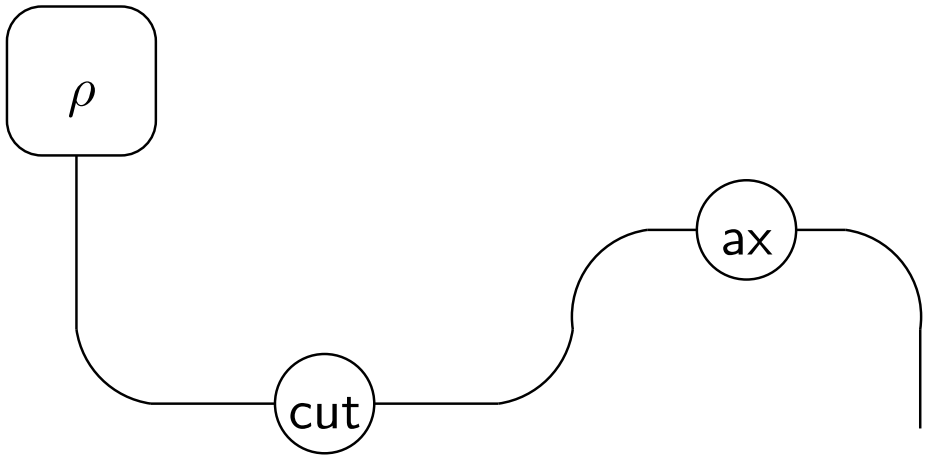
Example: Booleans and if. . . then. . . else

- Let us compute $\mathsf{if}\,(\mathsf{true}[A/X])\,\mathsf{then}\,\rho\,\mathsf{else}\,\rho'$:



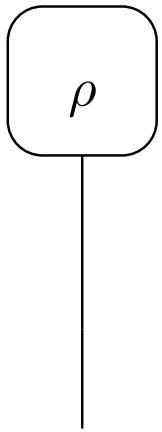
Example: Booleans and if. . . then. . . else

- Let us compute $\mathsf{if}\,(\mathsf{true}[A/X])\,\mathsf{then}\,\rho\,\mathsf{else}\,\rho'$:



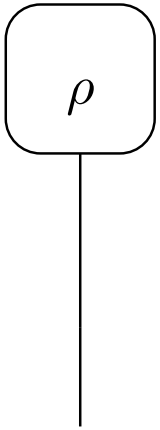
Example: Booleans and if. . . then. . . else

- Let us compute $\mathsf{if}\,(\mathsf{true}[A/X])\,\mathsf{then}\,\rho\,\mathsf{else}\,\rho'$:



Example: Booleans and if... then... else

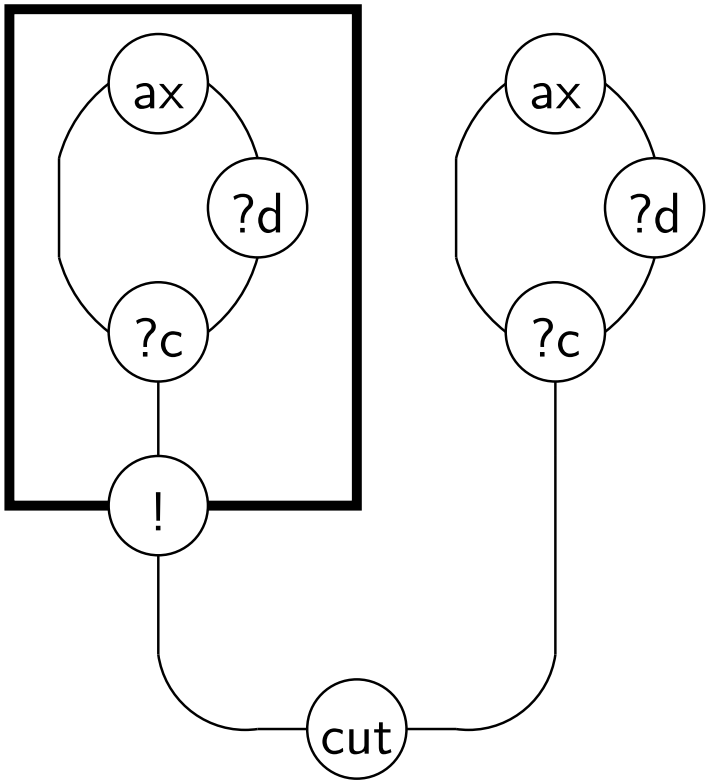
- Let us compute $\mathsf{if}\,(\mathsf{true}[A/X])\,\mathsf{then}\,\rho\,\mathsf{else}\,\rho'$:



- Observation: apart from type-checking the cut, we never used types/formulas.

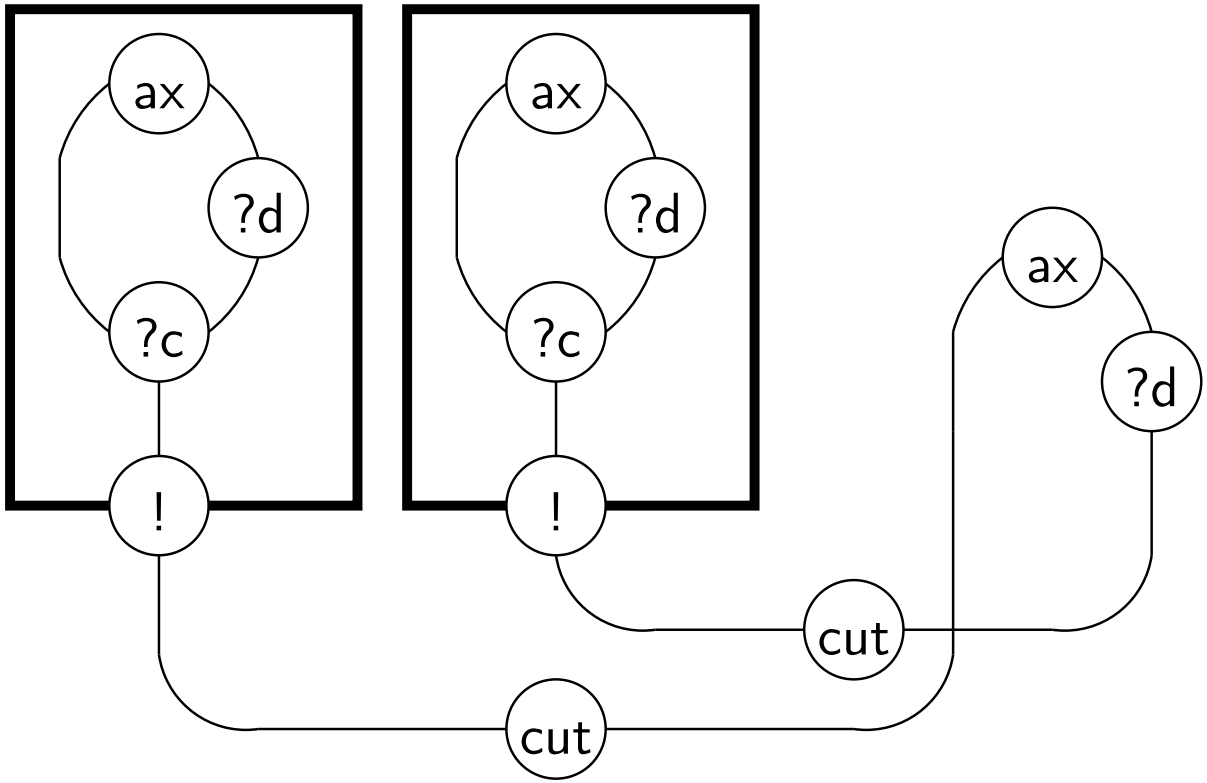
Untyped nets

- In fact, cut-elimination in nets makes sense even without formulas!



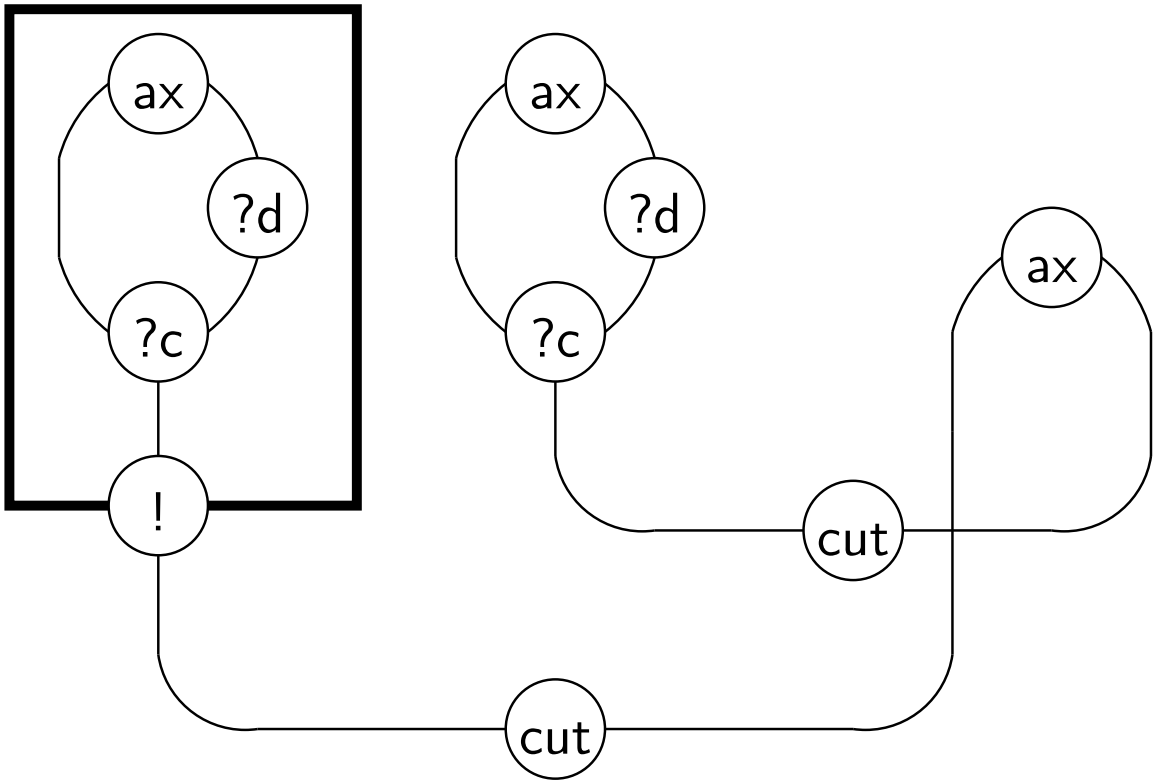
Untyped nets

- In fact, cut-elimination in nets makes sense even without formulas!



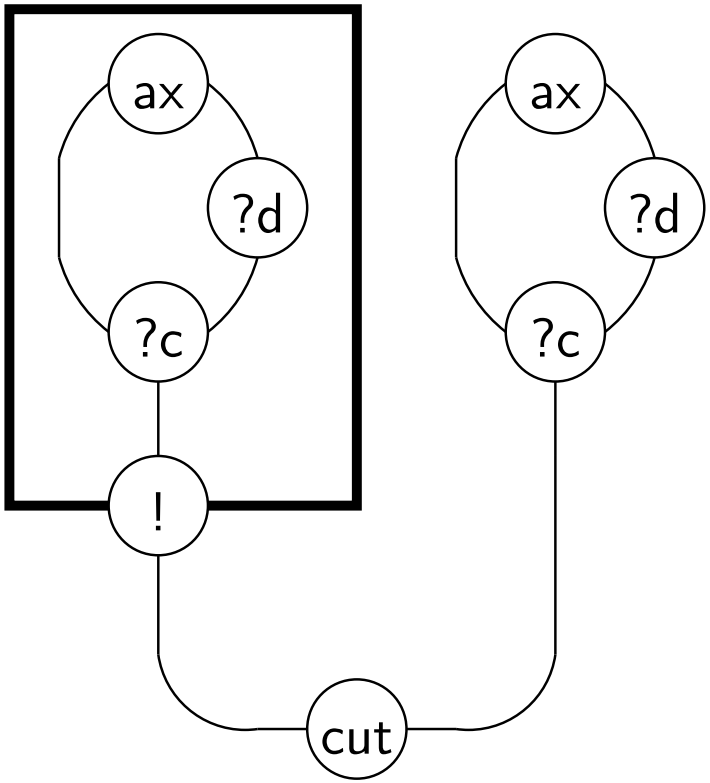
Untyped nets

- In fact, cut-elimination in nets makes sense even without formulas!



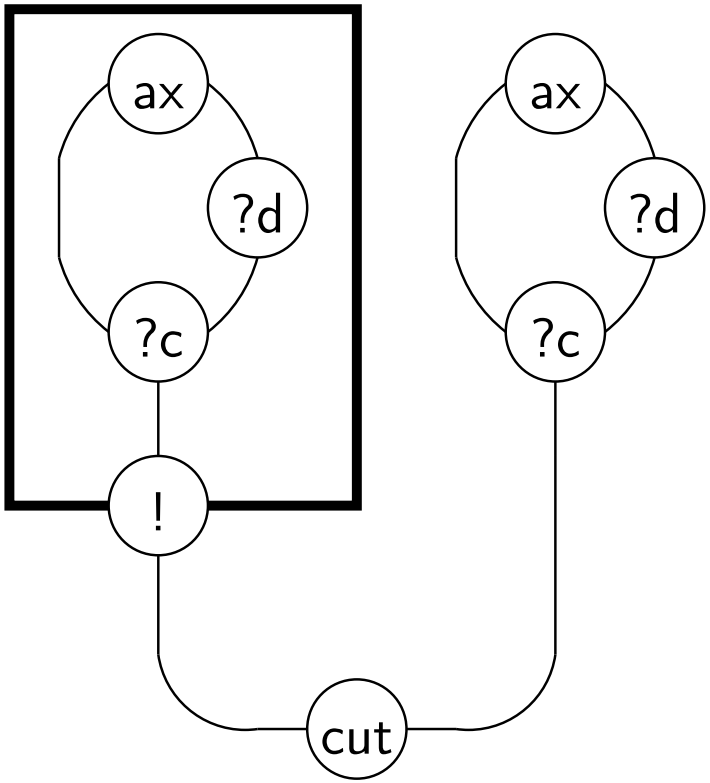
Untyped nets

- In fact, cut-elimination in nets makes sense even without formulas!



Untyped nets

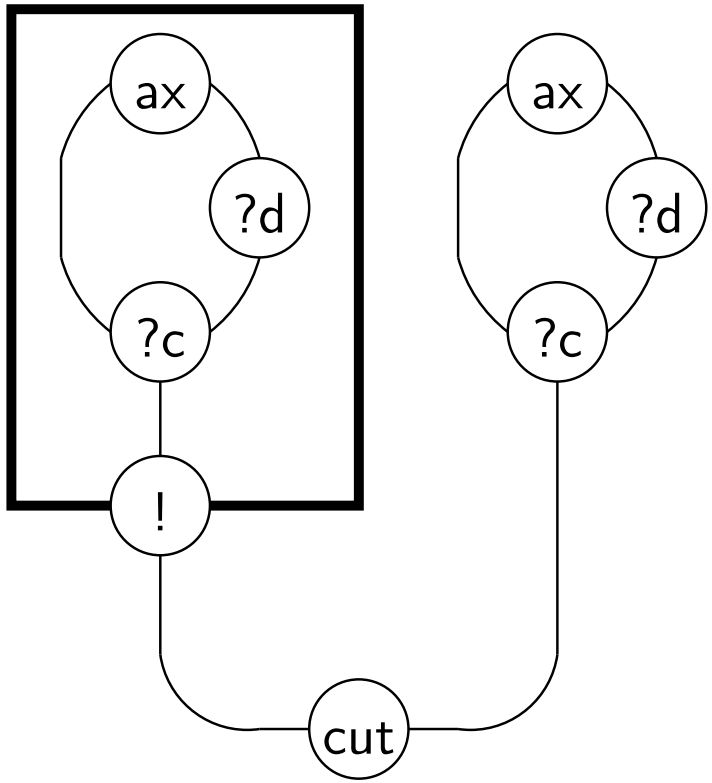
- In fact, cut-elimination in nets makes sense even without formulas!



- Untyped nets are a Turing-complete model of computation.

Untyped nets

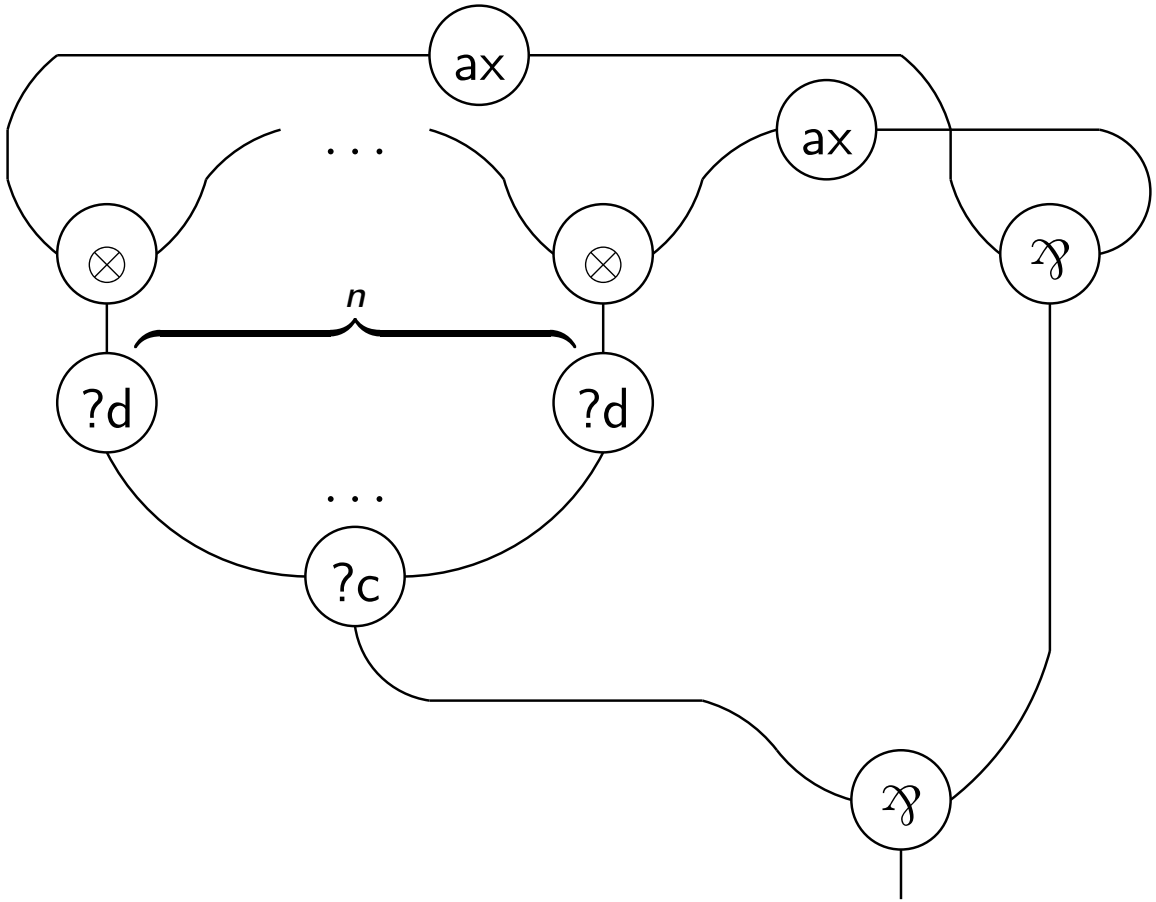
- In fact, cut-elimination in nets makes sense even without formulas!



- Untyped nets are a Turing-complete model of computation.
- Actually, the above net may be typed in presence of $!R^{\perp} = R$ (Russel's antinomy).

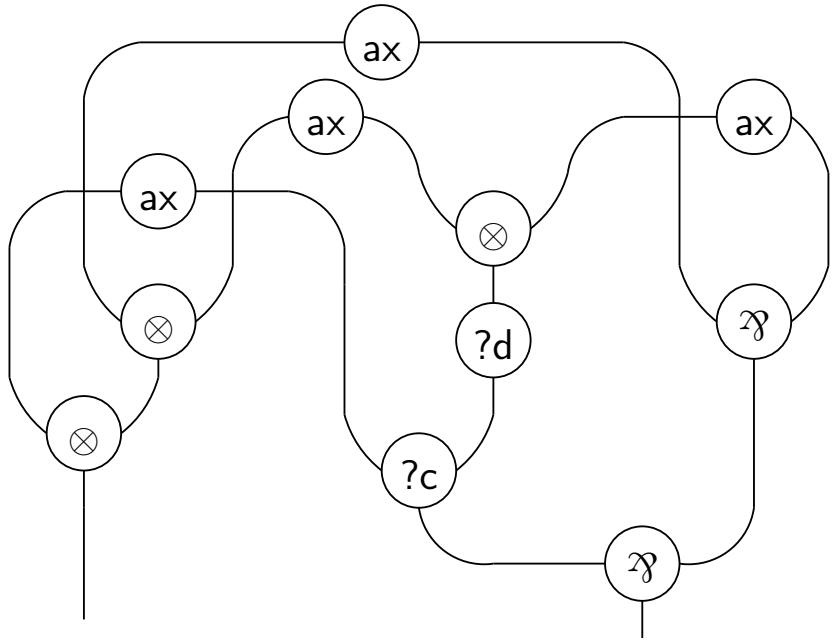
Integers

Voilà the n-th (Church) numeral, denoted by $\overline{n}$:



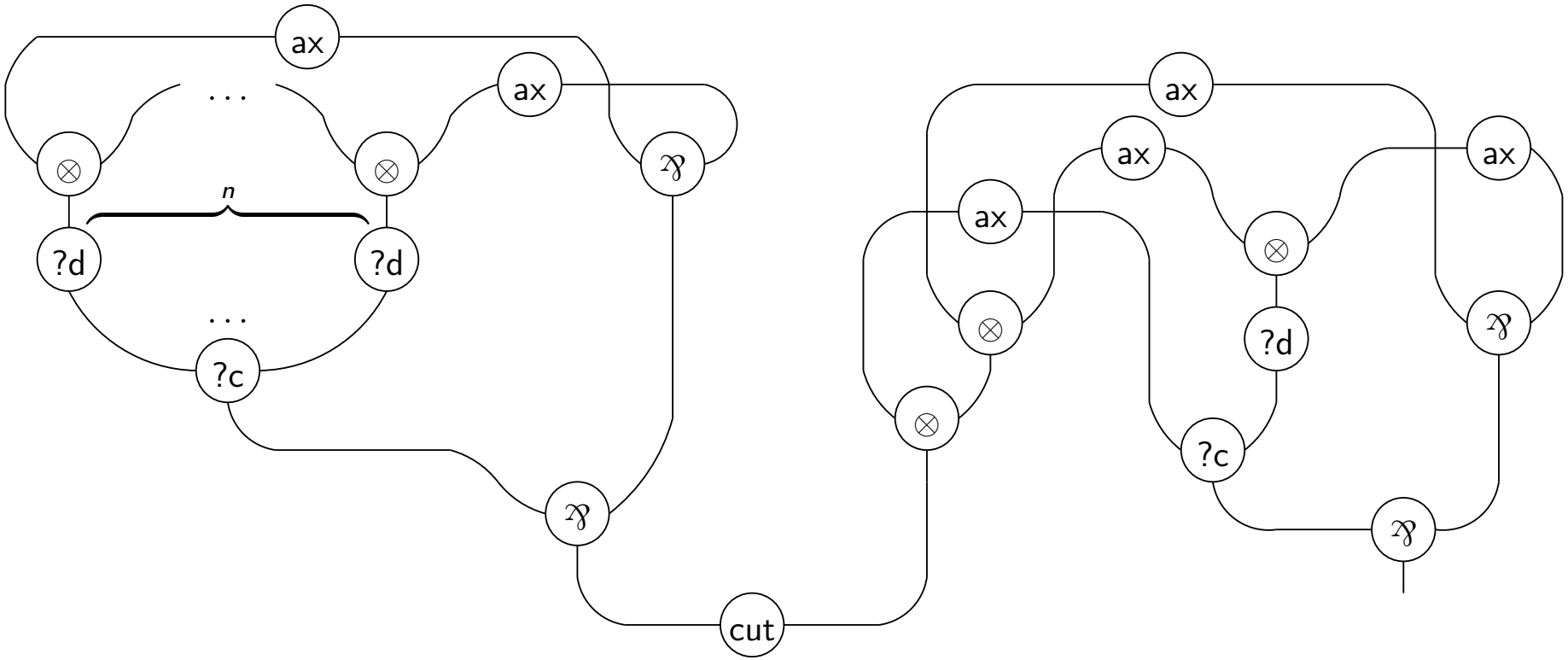
Integers

What does the following net compute?



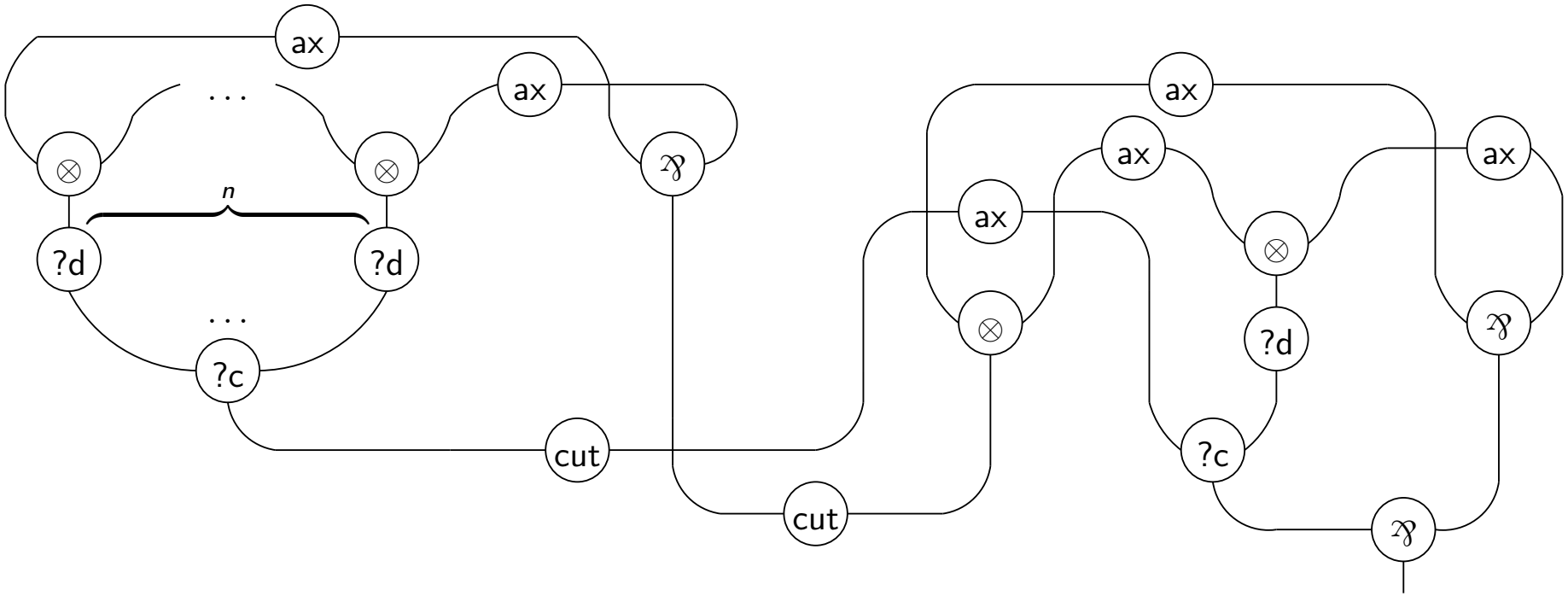
Integers

Let's find out!



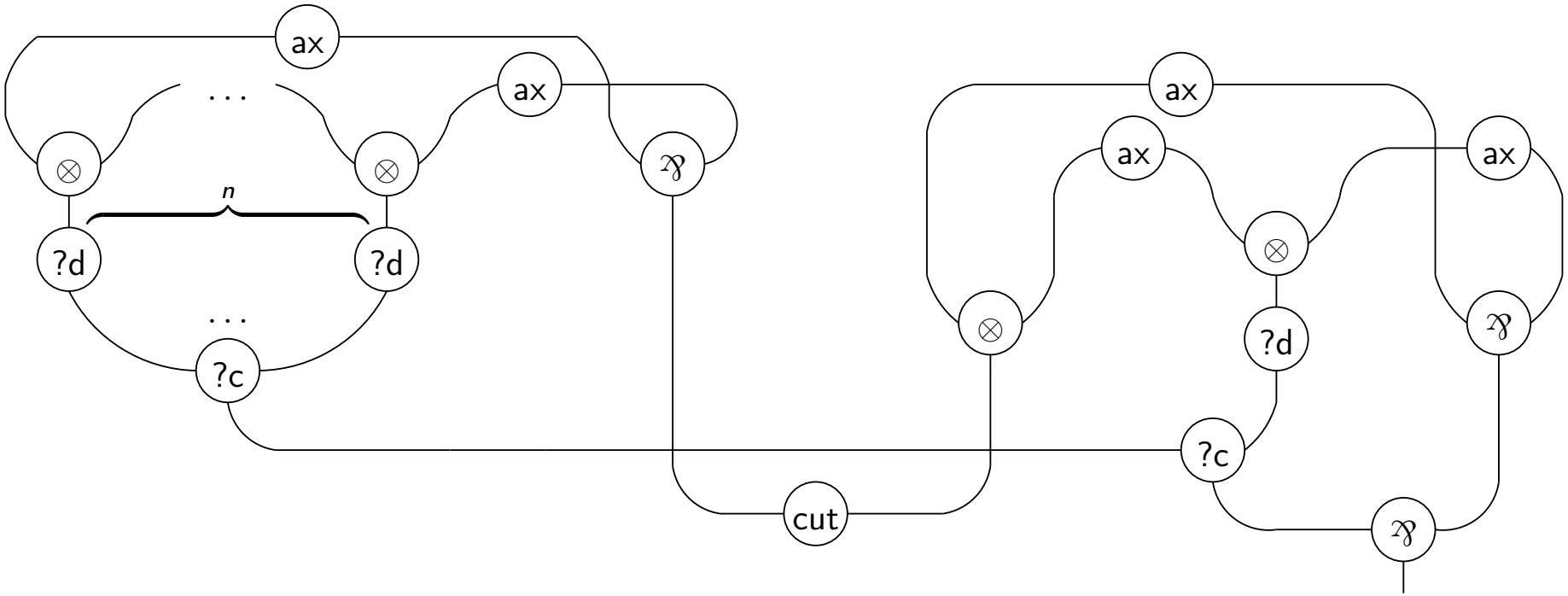
Integers

Let's find out!



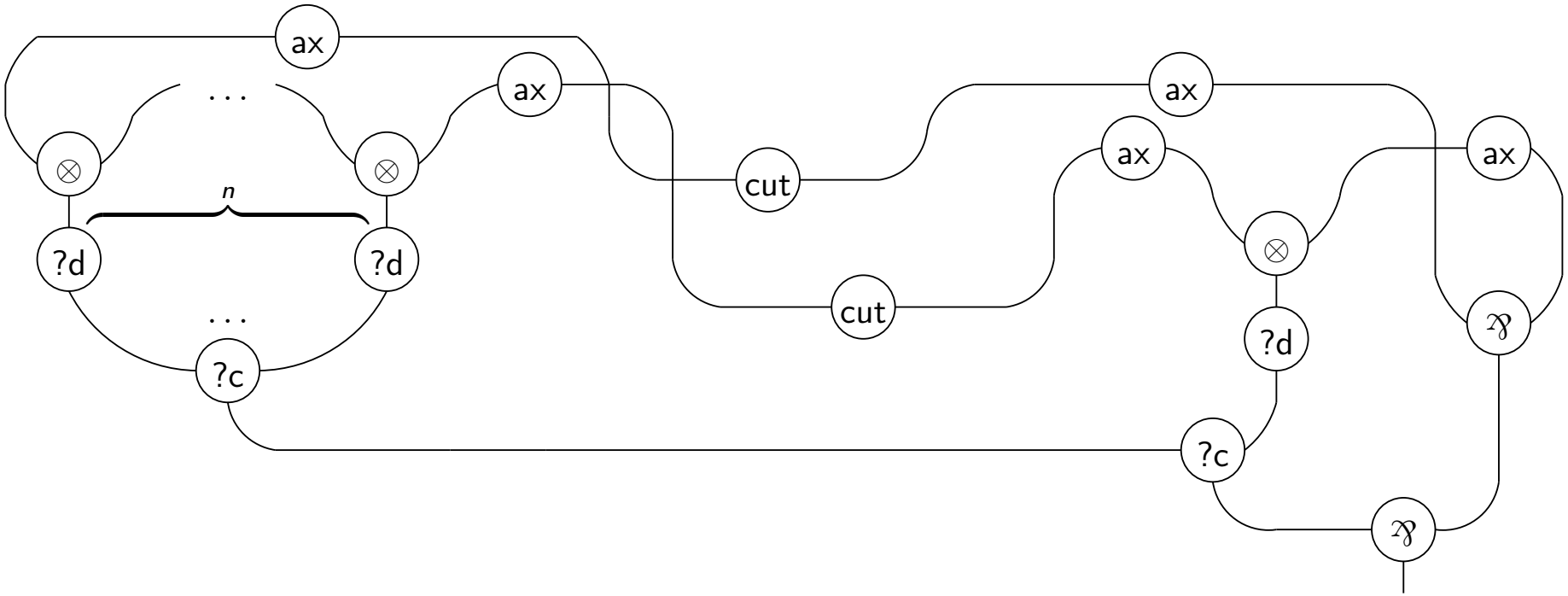
Integers

Let's find out!



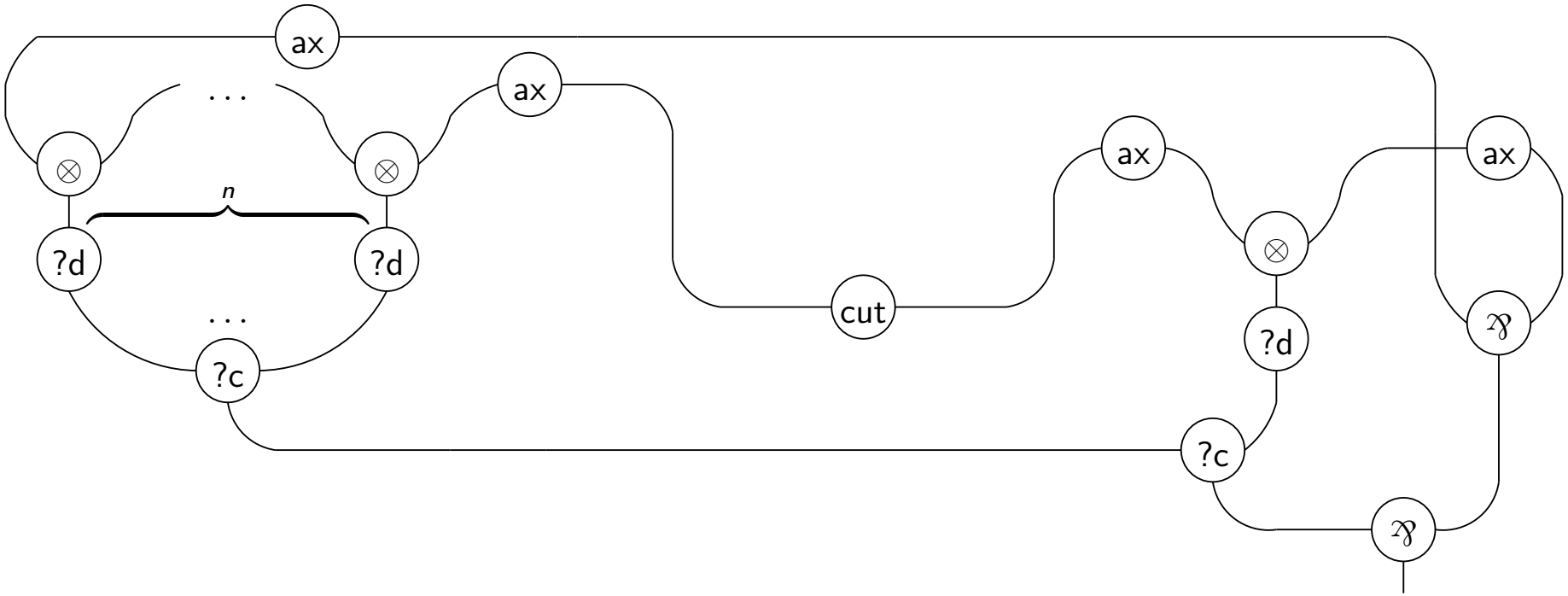
Integers

Let's find out!



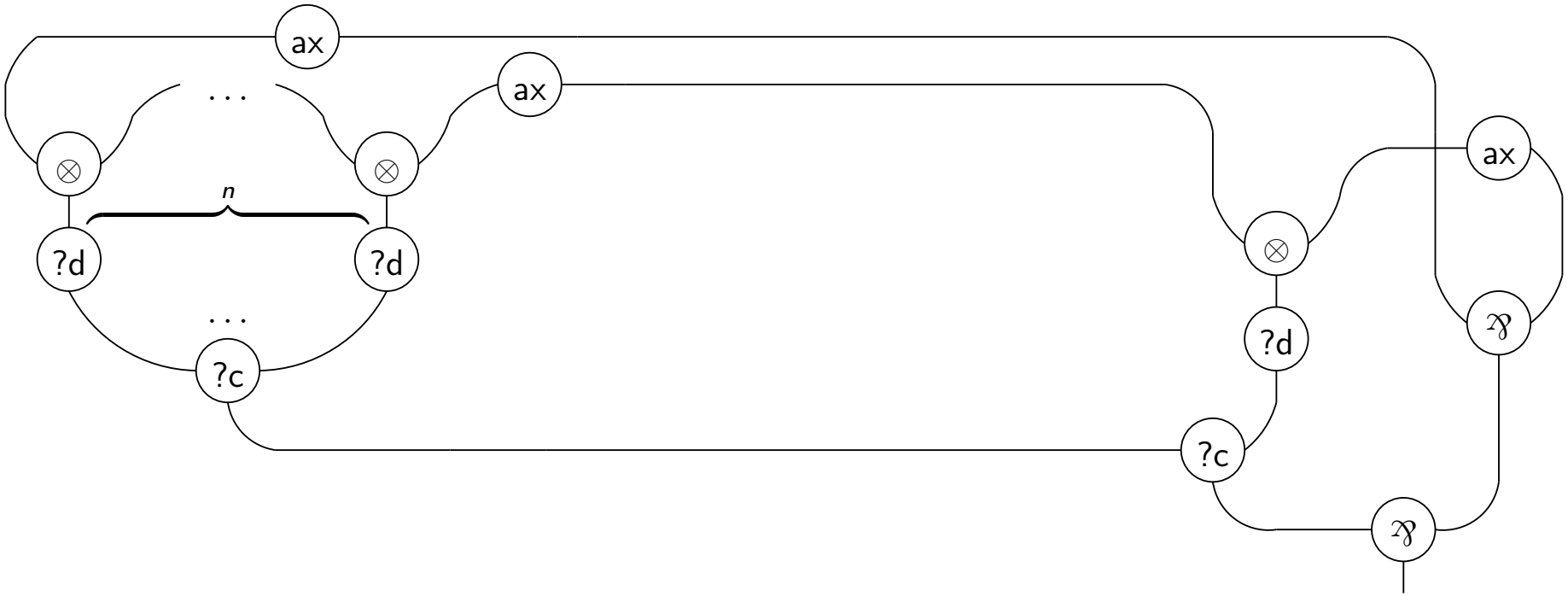
Integers

Let's find out!



Integers

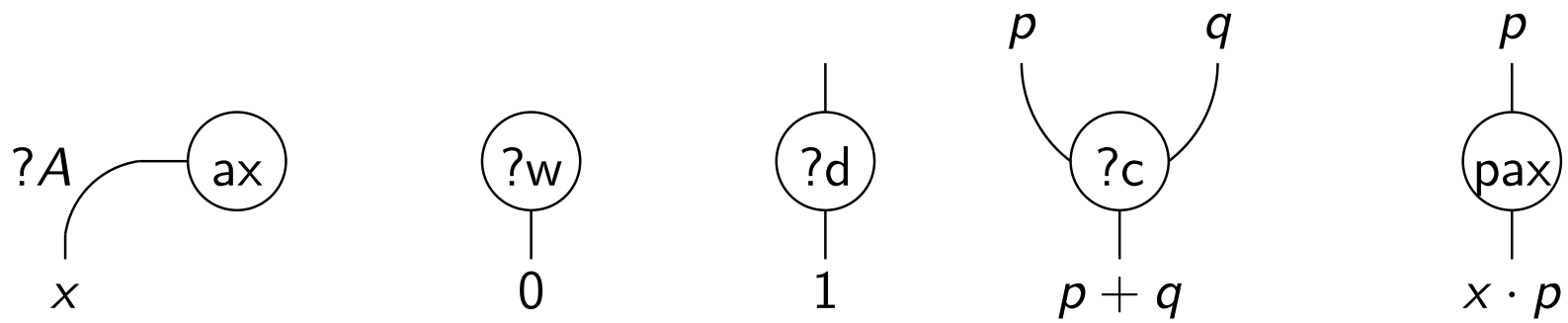
Let's find out!



It is the successor function!

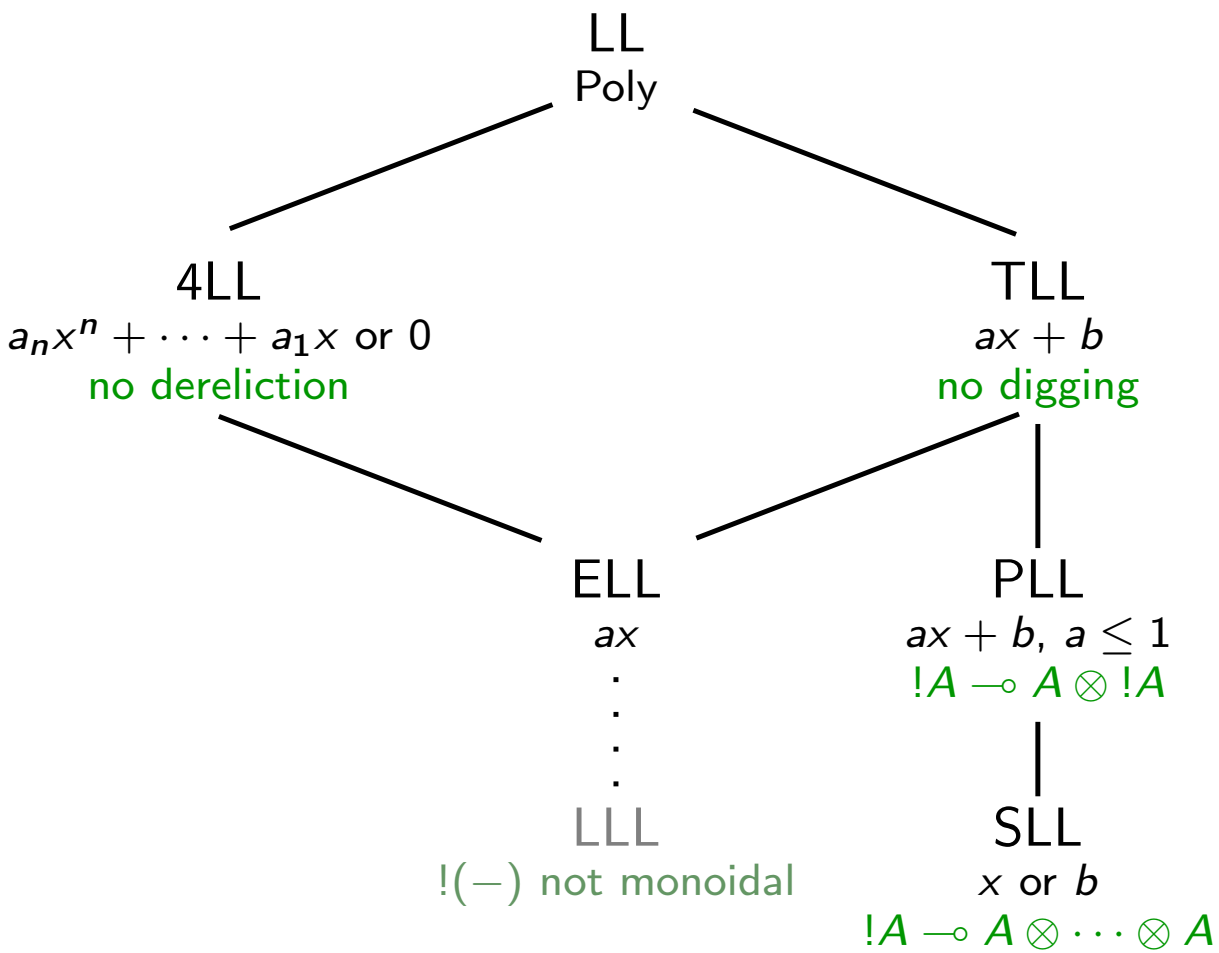
Heterodox exponentials

- Every occurrence of formula of the form $?A$ in a proof net may be assigned a polynomial with non-negative integer coefficients:

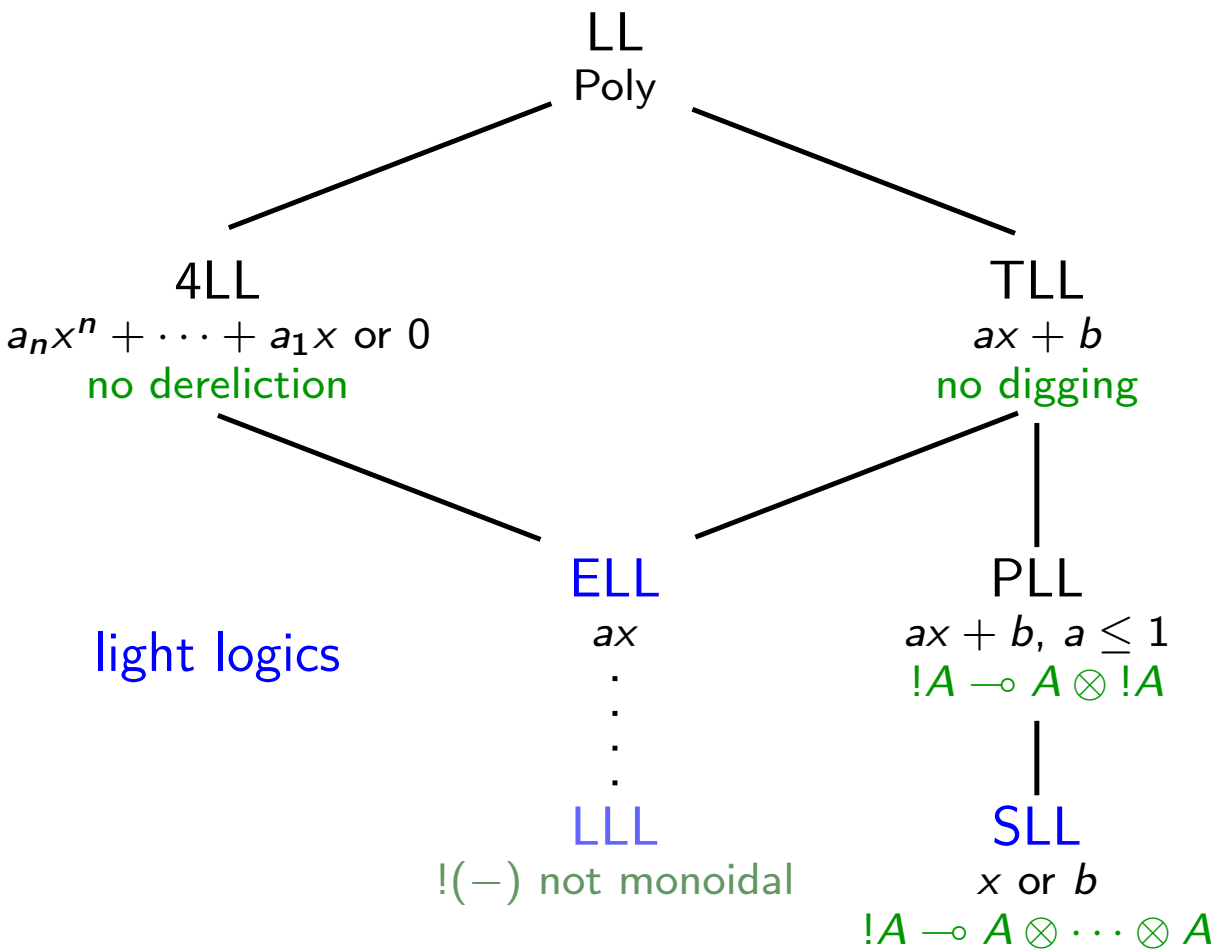


- Let Poly $:= (\mathbb{N}[x], \circ, x)$ be the monoid of polynomials under composition.
- Any submonoid $M \subseteq$ Poly induces a subsystem of linear logic (closed under cut-elimination and proving $\vdash ?A^{\perp}, !A$ for all A), as follows:
  Definition. *Call an occurrence of $?A$ in a proof net final if it is not the premise of a* ?c *or* pax *node. A proof net ρ belongs to* MELL_M *just if, whenever $?A$ is a final occurrence of ρ whose associated polynomial is p, we have $p \in M$.*

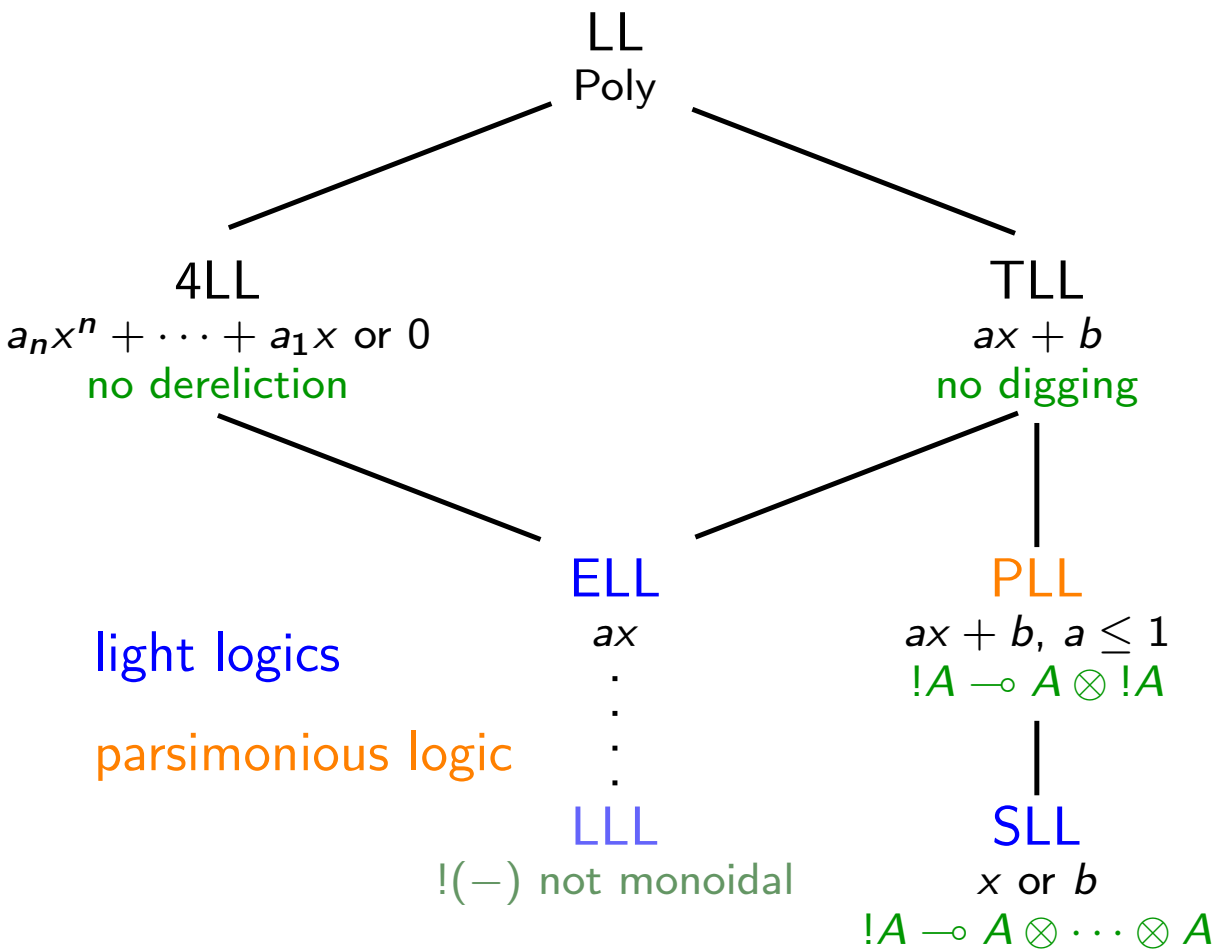
Heterodox exponentials



Heterodox exponentials



Heterodox exponentials



Implicit computational complexity

- Runtime = number of cut-elimination steps to normal form.
- Light logics have untyped cut-elimination:

  ELL: characterizes elementary time
  SLL: characterizes polynomial time
  LLL: characterizes polynomial time

- Parsimonious logic (with $!A \cong A \otimes !A$) is Turing-complete when untyped; however:

  propositional: characterizes logarithmic space
  linear 2nd order: characterizes polynomial time

- Two different approaches:

  stratification: (light logics) complexity is controlled globally;
  parsimony: complexity is controlled locally.

- The parsimonious approach also opens the way to non-uniformity, via *approximations*.

Perspectives

- Approximations (exponentials as a limit):
  - differential linear logic (DiLL) and Taylor expansion;
  - affine approximations and complexity.
- Quantitative analyses:
  - in DiLL, exponentials have non-deterministic cut-elimination;
  - bounded linear logic (modalities parametriezed by semi-ring).
- Geometry of interaction: an execution model based on tokens moving along proof nets.