Notes on proof-nets

Daniel Murfet

8/4/2016

therisingsea.org/post/seminar-proofnets/

Why proof-nets?

Traditional proof-theory deals with cut-elimination ; these results are usually obtained by means of sequent calculi, with the consequence that 75% of a cut-elimination proof is devoted to endless commutations of rules. It is hard to be happy with this, mainly because :

- the structure of the proof is blurred by all these cases ;
- whole forests have been destroyed in order to print the same routine lemmas ;
- this is not extremely elegant.

However old-fashioned proof-theory, which is concerned with the ritual question : “is-that-theory-consistent ?” never really cared. The situation changed when subtle algorithmic aspects of cut-elimination became prominent : typically the determinism of cut-elimination, its actual complexity, its implementation cannot be handled in terms of sequent calculus without paying a heavy price. Natural deduction could easily fix the main drawbacks of cut-elimination, but this improvement was limited to the negative fragment of intuitionistic logic. ?

The situation changed in 1986 with the invention of linear logic : *proof-nets* were introduced in [G86] as a new kind of syntax for linear logic, in order to cope with the problems arising from the intrinsic parallelism of linear sequent calculus. 9 years later the technology is perfectly efficient and proof-nets are now available for full linear logic [1]. Using implicit translations, proof-nets are also available for classical and intuitionistic logics, i.e. for extant logical systems.

Girard “Proof-nets: the parallel syntax for proof-theory”

The formulas of second order unit-free multiplicative exponential linear logic (**meLL**) are generated by the following grammar, where $X, X^{\perp}$ range over a denumerable set of propositional variables:

$$A, B ::= X \mid X^{\perp} \mid A \otimes B \mid A \parr B \mid\ !A \mid ?A \mid \exists X.A \mid \forall X.A \mid \S A.$$

Linear negation is defined through De Morgan laws:

$$\begin{array}{rclrcl}
(X)^{\perp} & = & X^{\perp} & (X^{\perp})^{\perp} & = & X \\
(A \otimes B)^{\perp} & = & B^{\perp} \parr A^{\perp} & (A \parr B)^{\perp} & = & B^{\perp} \otimes A^{\perp} \\
(!A)^{\perp} & = & ?A^{\perp} & (?A)^{\perp} & = & !A^{\perp} \\
(\exists X.A)^{\perp} & = & \forall X.A^{\perp} & (\forall X.A)^{\perp} & = & \exists X.A^{\perp}
\end{array}$$

$$(\S A)^{\perp} = \S A^{\perp}$$

Two connectives exchanged by negation are said to be *dual*. Note that the self-dual paragraph modality is not present in the standard definition of **meLL** [Girard, 1987]; we include it here for convenience. Also observe that full linear logic has a further pair of dual binary connectives, called *additive* (denoted by & and $\oplus$), which we shall briefly discuss in Sect. 5. They are not strictly needed for our purposes, hence we restrict to **meLL** in the paper.

Linear implication is defined as $A \multimap B = A^{\perp} \parr B$. Multisets of formulas will be ranged over by $\Gamma, \Delta, \ldots$

For technical reasons, it is also useful to consider *discharged formulas*, which will be denoted by $\flat A$, where A is a formula.

Baillot, Mazza "Linear logic by levels and bounded time complexity", 2009.

Sequent calculus

$$\dfrac{}{\vdash A^{\perp}, A}\ \text{Axiom} \qquad \dfrac{\vdash \Gamma, A \quad \vdash \Delta, A^{\perp}}{\vdash \Gamma, \Delta}\ \text{Cut}$$

$$\dfrac{\vdash \Gamma, A \quad \vdash \Delta, B}{\vdash \Gamma, \Delta, A \otimes B}\ \text{Tensor} \qquad \dfrac{\vdash \Gamma, A, B}{\vdash \Gamma, A \parr B}\ \text{Par}$$

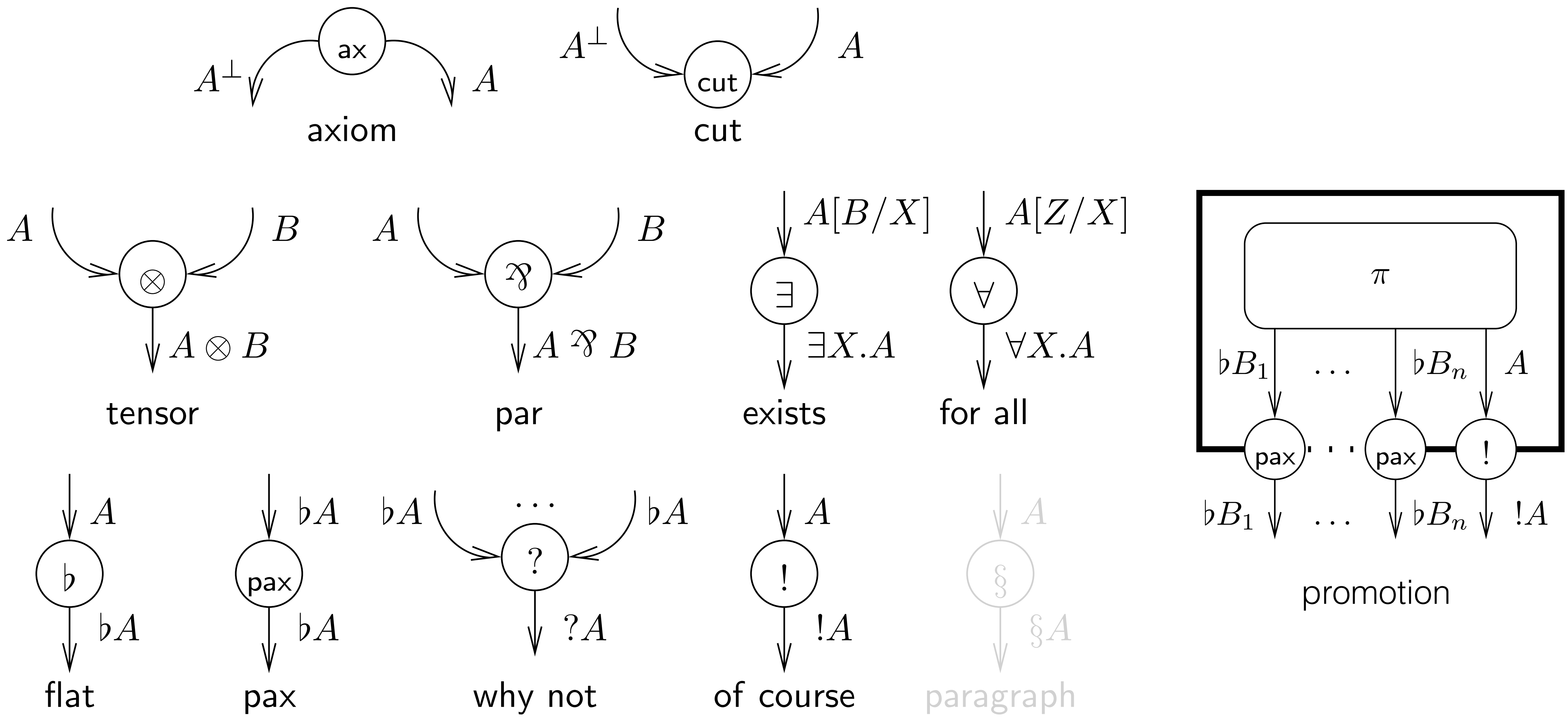
$$\dfrac{\vdash \Gamma, A}{\vdash \Gamma, \forall X.A}\ \text{For all } (X \text{ not free in } \Gamma) \qquad \dfrac{\vdash \Gamma, A[B/X]}{\vdash \Gamma, \exists X.A}\ \text{Exists}$$

$$\dfrac{\vdash ?\Gamma, A}{\vdash ?\Gamma, !A}\ \text{Promotion} \qquad \dfrac{\vdash \Gamma, A}{\vdash \Gamma, ?A}\ \text{Dereliction}$$

$$\dfrac{\vdash \Gamma}{\vdash \Gamma, ?A}\ \text{Weakening} \qquad \dfrac{\vdash \Gamma, ?A, ?A}{\vdash \Gamma, ?A}\ \text{Contraction}$$

$$\dfrac{}{\vdash}\ \text{Daimon} \qquad \dfrac{\vdash \Gamma \quad \vdash \Delta}{\vdash \Gamma, \Delta}\ \text{Mix} \qquad ?$$

Proof-net links



? dereliction, weakening

Baillot, Mazza "Linear logic by levels and bounded time complexity", 2009.

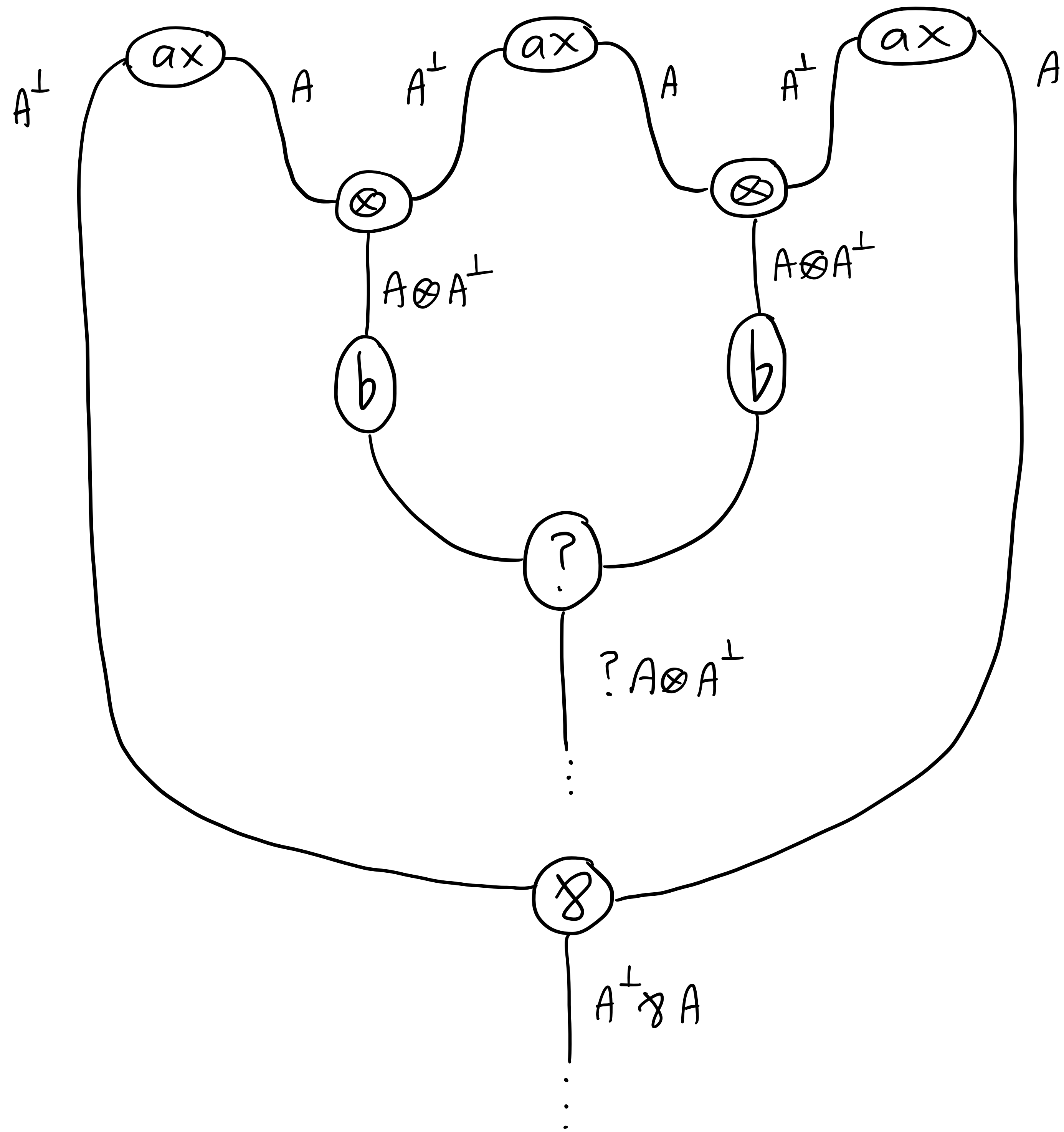
Example of a proof-net

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A\vdash A}\qquad\dfrac{\dfrac{}{A\vdash A}\quad\dfrac{}{A\vdash A}}{A, A\multimap A\vdash A}}{A, A\multimap A, A\multimap A\vdash A}}{A\multimap A, A\multimap A\vdash A\multimap A}}{!(A\multimap A), !(A\multimap A)\vdash A\multimap A}\ \text{der}}{!(A\multimap A)\vdash A\multimap A}\ \text{ctr}$$

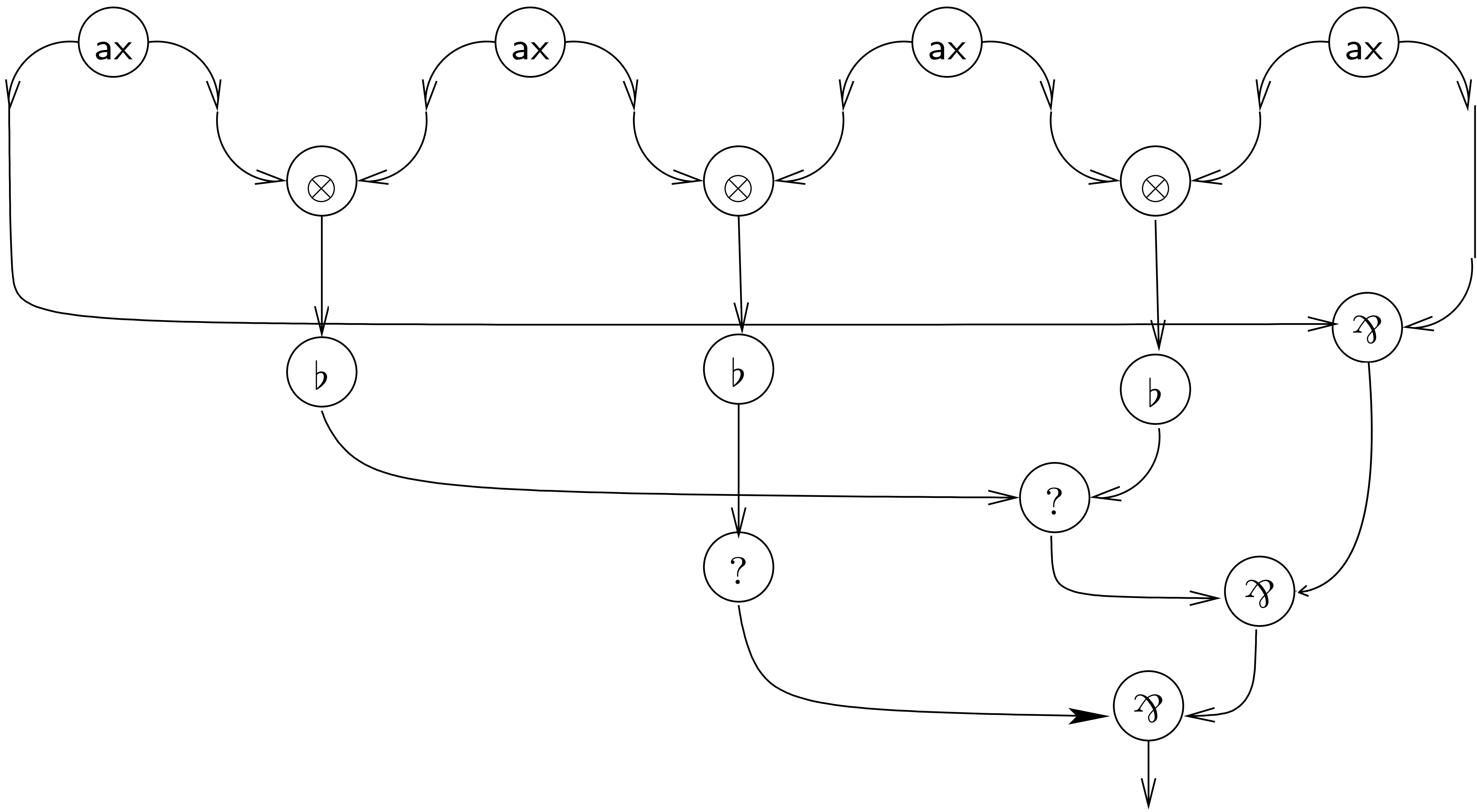
Church numeral **2**

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash A^\perp, A}\qquad\dfrac{\dfrac{}{\vdash A^\perp, A}\quad\dfrac{}{\vdash A^\perp, A}}{\vdash A^\perp, A\otimes A^\perp, A}}{\vdash A^\perp, A\otimes A^\perp, A\otimes A^\perp, A}}{\vdash A\otimes A^\perp, A\otimes A^\perp, A^\perp \parr A}}{\vdash ?(A\otimes A^\perp), ?(A\otimes A^\perp), A^\perp \parr A}}{\vdash ?(A\otimes A^\perp), A^\perp \parr A}$$

2 in one-sided sequent calculus



Exercise: what is this?



Cut-elimination

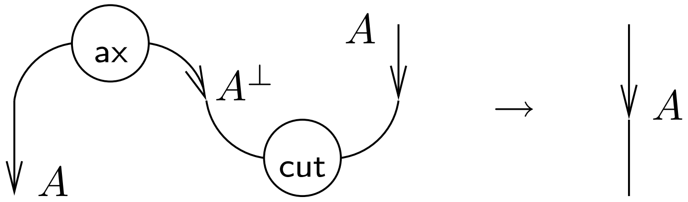


Figure 4: Axiom step.

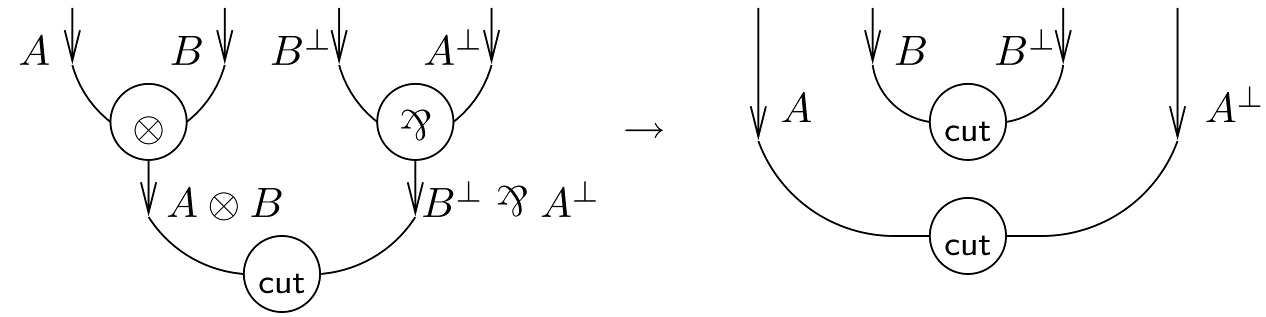


Figure 5: Multiplicative step.

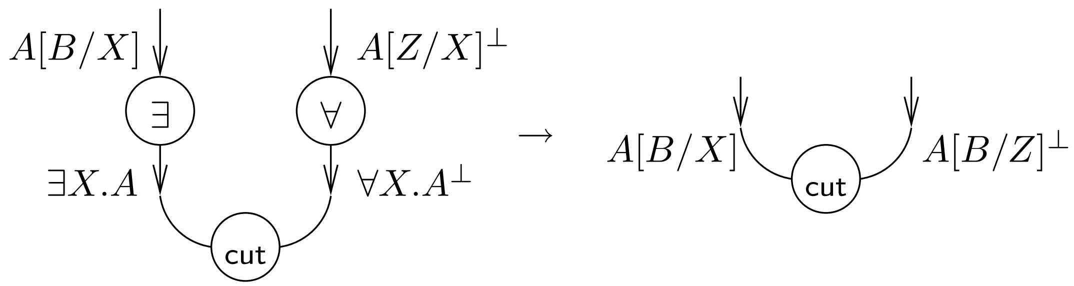
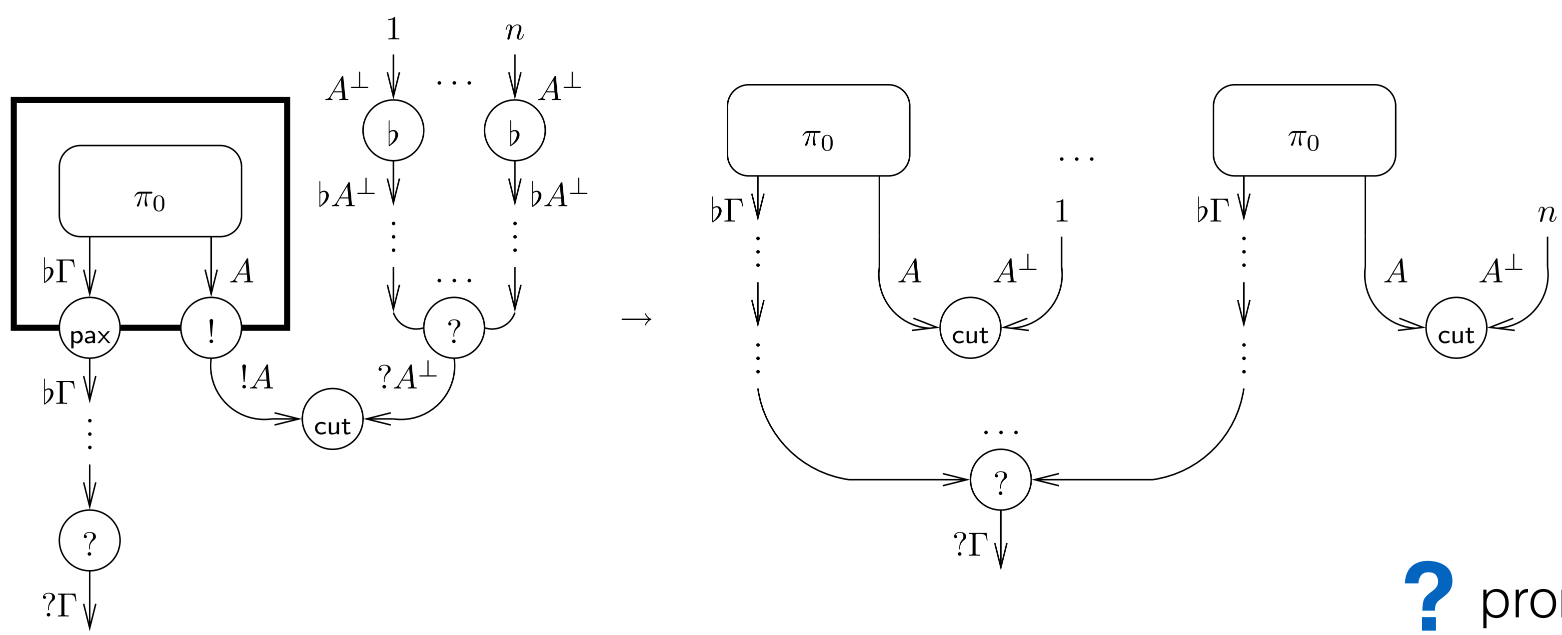


Figure 6: Quantifier step; the substitution is performed on the whole net.



? prom/der, prom/weak

Figure 7: Exponential step; $\flat\Gamma$ is a multiset of discharged formulas, so one pax link, why not link, or wire in the picture may in some case stand for several (including zero) pax links, why not links, or wires.

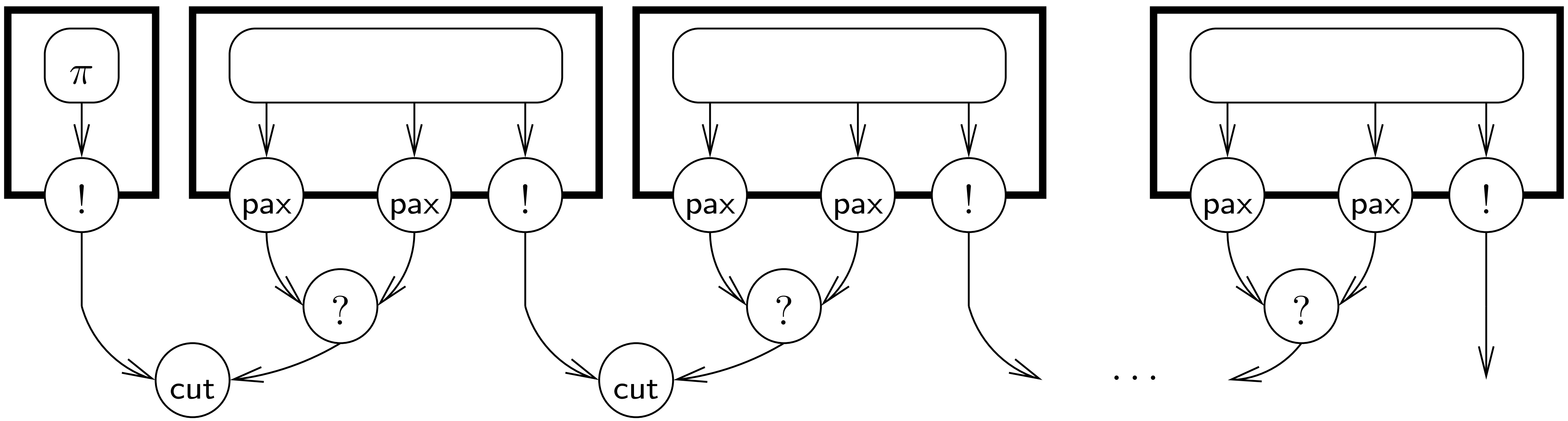
Cut-elimination

statement of strong normalisation

(from Pagani-Tortora de Falco “Strong Normalization Property for Second Order Linear Logic”)

Cut-elimination: explosion

(cut-elimination introduces new cuts at higher depth)



From sequent calculus proofs to proof-nets

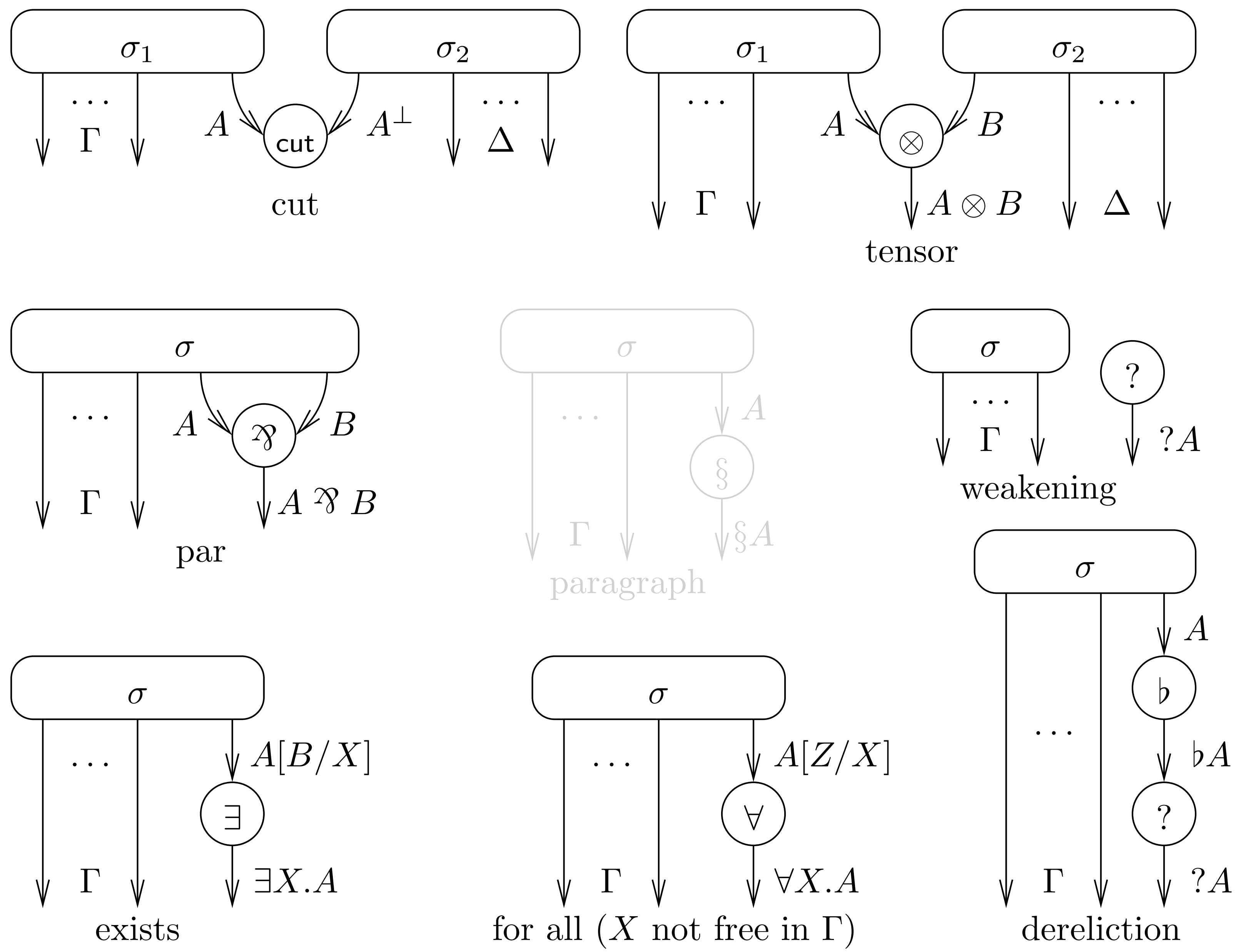
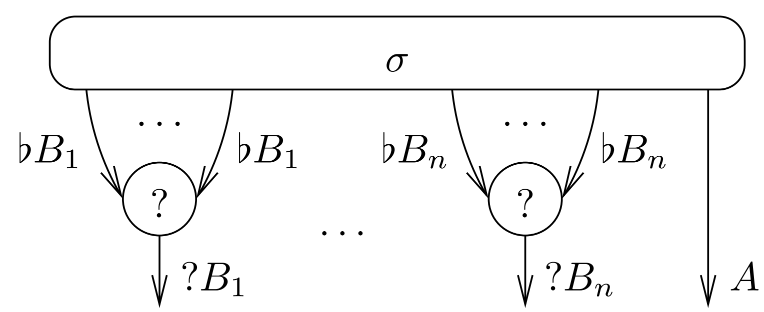


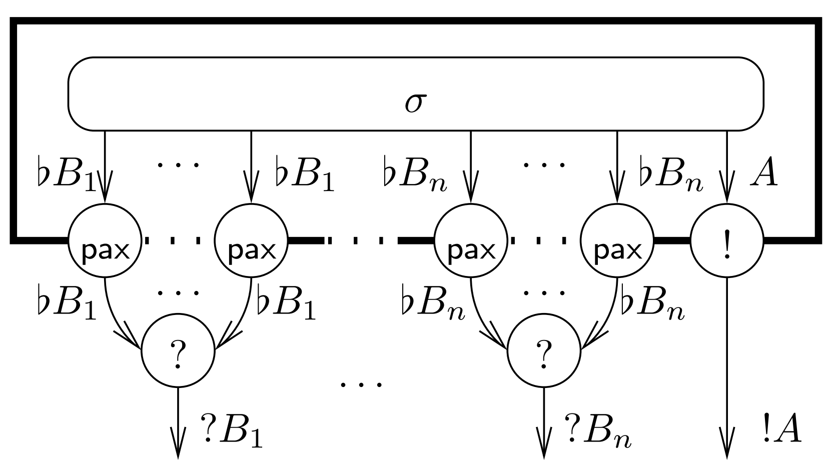
Figure 3: Rules for building sequentializable nets.

From sequent calculus proofs to proof-nets

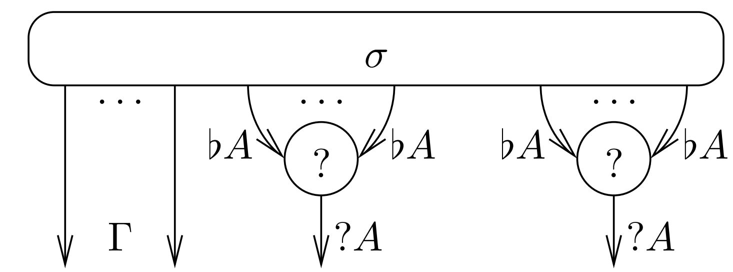
Definition 5 (Sequentializable net) *We define the set of* sequentializable nets *inductively: the empty net and the net consisting of a single* axiom *link are sequentializable (daimon and axiom); the juxtaposition of two sequentializable nets is sequentializable (mix); if σ, σ_1, σ_2 are sequentializable nets of suitable conclusions, the nets of Fig. 3 are sequentializable; if*



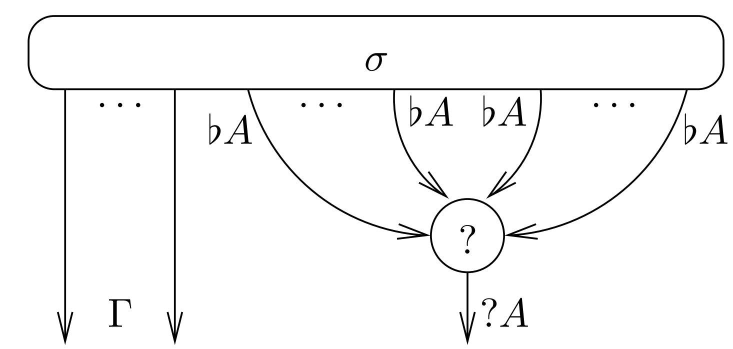
is a sequentializable net, then the net



is sequentializable (promotion); if



is a sequentializable net, then the net



is sequentializable (contraction).

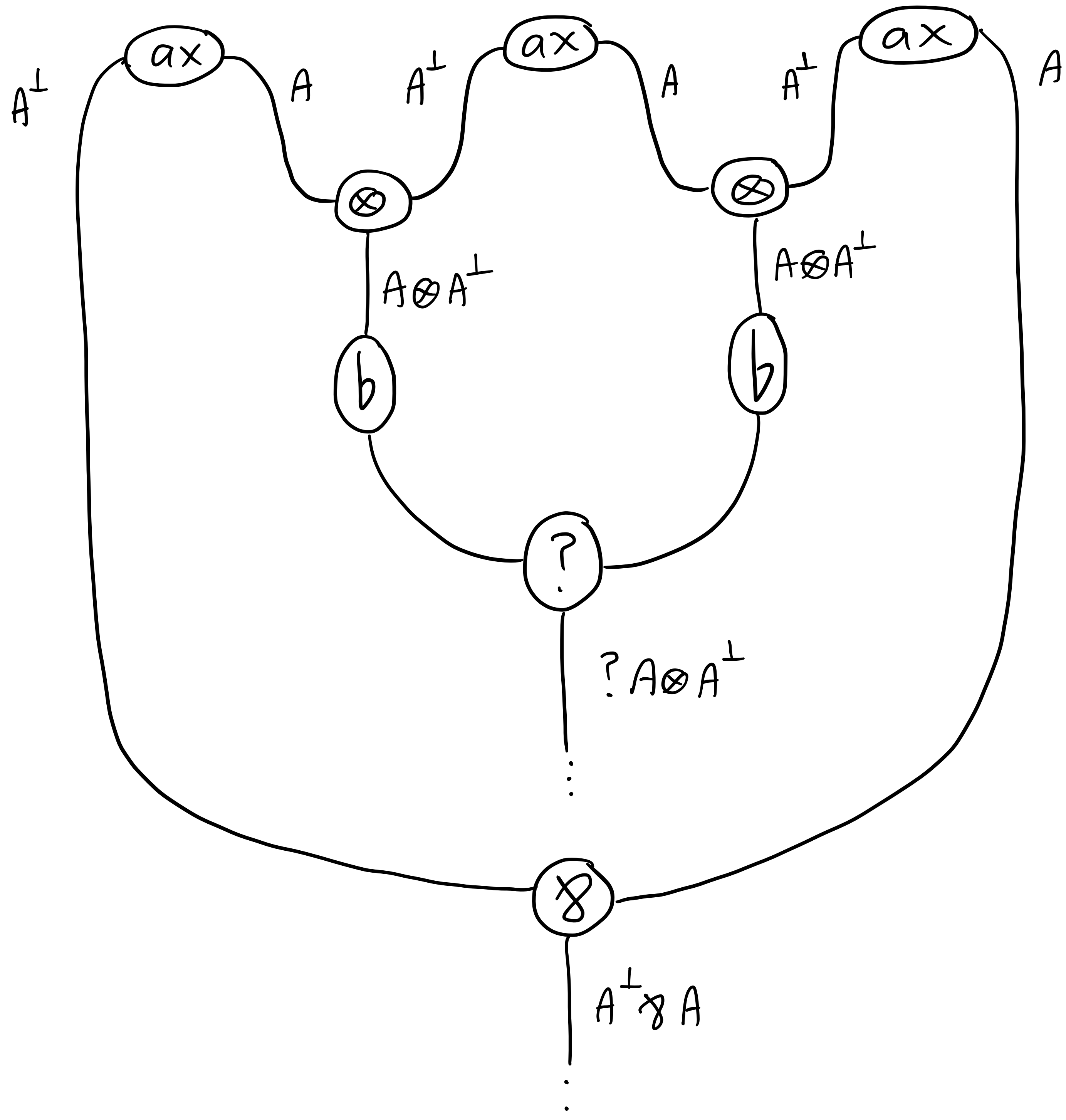
sequent calculus proofs with the same proof-net

(from Davoren “A Lazy Logician’s Guide to Linear Logic” p.140, p.156, p.157)

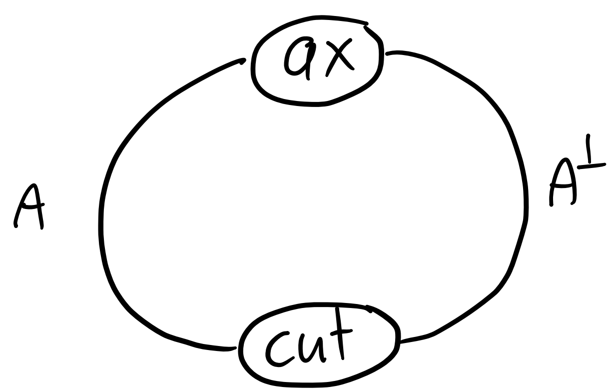
definition of switching

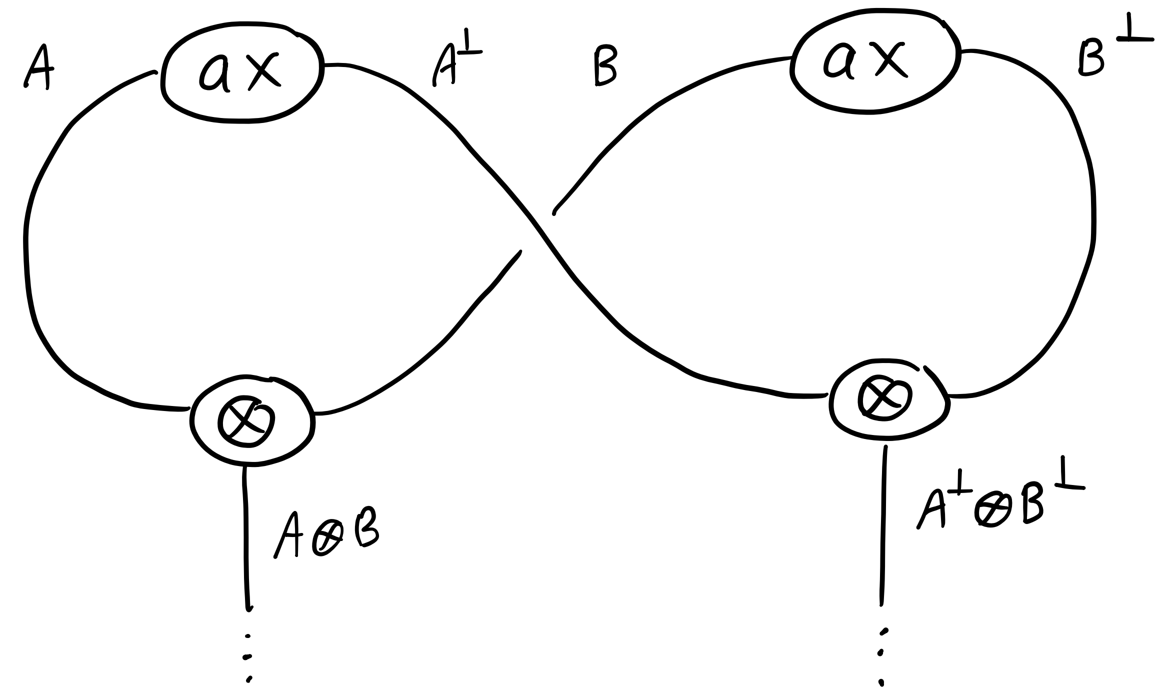
(note Baillot-Mazza is wrong, see Pagani-Tortora de Falco
and Girard “Proof-nets: the parallel syntax for proof-theory”)

Example of switching acyclicity



Example of switching cyclicity (non proof-nets)





statement of sequentialisation theorem

(from Girard)