Reti dimostrative (proof nets)   Girard, 1987   frammenti di LL

frammento moltiplicativo $MLL \subsetneq LL$

<u>proof nets</u>   <u>triplice natura</u>:

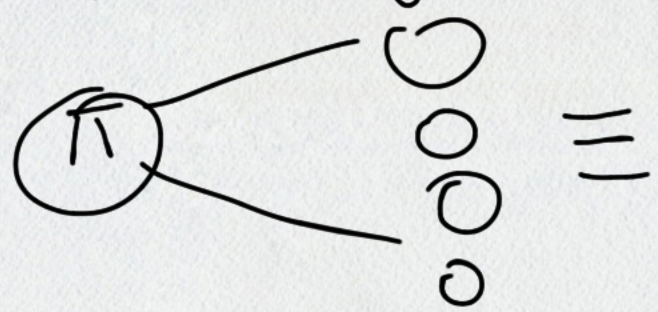
1) <u>sintattica</u>: parlare di <u>dimostrazioni come oggetti finiti</u>: <u>grafi</u>

grafi in informatica (algoritmi di agenti di flusso)

grafi regolatori in biologia

2) <u>semantica</u>   una proof nets rappresenta una classe di equivalenza di dimostrazioni di LL

quoziente classi di dimostrazioni equivalenti a meno di permutazioni di regole logiche



3) <u>computazionale</u>

perché "spiega" l'eliminazione del taglio in maniera <u>efficace</u>:

- <u>locale</u>, <u>parallela</u>, <u>confluenza</u> (<u>normalizzazione forte</u>)

frammento MLL puro

tensore par

- formule $F ::= \underbrace{a \mid a^\perp}_{\text{letterali}} \mid F \otimes G \mid F ⅋ G \mid F^\perp$ negazione De Morgan

$$(A \otimes B)^\perp = A^\perp ⅋ B^\perp \qquad (A ⅋ B)^\perp = A^\perp \otimes B^\perp$$

- sequenti sono ad una sola parte $\vdash \Gamma$

seppur $\Gamma \vdash \Delta \iff \vdash (\otimes \Gamma)^\perp, \Delta$

$\Gamma = A_1 \dots A_n$

$(\otimes_i A_i)^\perp = (\otimes \Gamma)^\perp$

Regole:

identità

$$\frac{}{\vdash A, A^\perp}\,ax$$

atomico

cut

$$\frac{\vdash \Gamma, A \qquad \vdash \Delta, A^\perp}{\vdash \Gamma, \Delta}\,cut$$

moltiplicative

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

unità

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

Dimostrazioni di MLL

una dimostrazione $\vdash_{MLL} \Gamma$ è un albero

- le foglie sono etichettate da assiomi/identità $\overline{A, A^\perp}$ "$\vdash$" omettiamo
- la conclusione/radice è etichettata dal sequente $\vdash \Gamma$
- ogni nodo intermedio è etichettato da un sequente derivato mediante una delle regole di MLL usate prima.

Esempio

$$
* \left\{ \dfrac{\dfrac{\overline{A, A^\perp} \quad \overline{B, B^\perp}}{A \otimes B, A^\perp, B^\perp}\otimes}{A \otimes B, A^\perp \parr B^\perp}\parr \right. \qquad , \qquad \dfrac{\dfrac{\dfrac{\overline{B, B^\perp} \quad \overline{C, C^\perp}}{B^\perp \otimes C^\perp, B, C}\otimes \qquad \overline{A, A^\perp}}{A \otimes B, B^\perp \otimes C^\perp, A^\perp, C}\otimes}{A \otimes B, B^\perp \otimes C^\perp, A^\perp \parr C}\parr
$$

$$
\overline{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}
$$

$$
A \otimes B, B^\perp \otimes C^\perp, A^\perp \parr C
$$

Osservazione la regola del $\parr$ è invertibile $\quad \vdash \Gamma, A \parr B \overset{\Leftarrow}{\Longleftrightarrow} \vdash \Gamma, A, B$

$$
\dfrac{\vdash \Gamma, A, B}{\vdash \Gamma, A \parr B}\parr \qquad \dfrac{\Gamma, A \parr B \qquad A^\perp \otimes B^\perp, A, B}{\vdash \Gamma, A, B}\,\mathrm{cut}
$$

Eliminazione del taglio: **Teorema** ogni dimostrazione di $\vdash \Gamma$ può essere trasformata in una dim di $\vdash \Gamma$ senza tagli

* complessità logica o rango della cut-formula # dei connettivi della cut formula

$$\delta(A \otimes B) = 1$$

* λ profondità del taglio   max delle profondità delle premesse $+1$

$$\lambda(A \otimes B, A^\perp \parr B^\perp) = \max\{3, 4\} + 1 = 5$$

Esempio

$$
\begin{prooftree}
\AxiomC{$\vdash A, A^\perp$}
\AxiomC{$\vdash B, B^\perp$}
\RightLabel{$\otimes$}
\BinaryInfC{$\vdash A \otimes B, A^\perp, B^\perp$}
\RightLabel{$\parr$}
\UnaryInfC{$\vdash A \otimes B, A^\perp \parr B^\perp$}
\AxiomC{$\vdash B, B^\perp$}
\AxiomC{$\vdash C, C^\perp$}
\RightLabel{$\otimes$}
\BinaryInfC{$\vdash B^\perp \otimes C^\perp, B, C$}
\AxiomC{$\vdash A, A^\perp$}
\RightLabel{$\otimes$}
\BinaryInfC{$\vdash A \otimes B, B^\perp \otimes C^\perp, A^\perp, C$}
\RightLabel{$\parr$}
\UnaryInfC{$\vdash A \otimes B, B^\perp \otimes C^\perp, A^\perp \parr C$}
\RightLabel{(cut)}
\BinaryInfC{$\vdash A \otimes B, B^\perp \otimes C^\perp, A^\perp \parr C$}
\end{prooftree}
$$

lv(5)

$\lambda(\text{cut}) = 5$

$\delta(\text{cut}) = 1$

~~taglio~~ passo commutativo

Esempio

$$
* \left\{ \dfrac{\dfrac{\vdash A, A^\perp \qquad \vdash B, B^\perp}{\vdash A\otimes B, A^\perp, B^\perp}\,\otimes}{\vdash A\otimes B, A^\perp ⅋ B^\perp}\,⅋ \right.
\qquad
\dfrac{\dfrac{\vdash B, B^\perp \qquad \vdash C, C^\perp}{\vdash B^\perp\otimes C^\perp, B, C}\,\otimes \qquad \vdash A, A^\perp}{\vdash A\otimes B, B^\perp\otimes C^\perp, A^\perp, C}\,\otimes
$$

$$
\dfrac{\dfrac{\vdash A\otimes B, A^\perp ⅋ B^\perp \qquad \vdash A\otimes B, B^\perp\otimes C^\perp, A^\perp, C}{\vdash A\otimes B, B^\perp\otimes C^\perp, A^\perp, C}\,\text{cut}}{\vdash A\otimes B, B^\perp\otimes C^\perp, A^\perp ⅋ C}\,⅋
$$

cut $\delta(A\otimes B) = 1$

$\lambda(A\otimes B)_{\text{cut}} = 4$

cut è logico

commutation step, + tagli axiom

$$
\dfrac{\dfrac{\dfrac{\vdash A, A^\perp \qquad \vdash B, B^\perp}{\vdash A\otimes B, A^\perp, B^\perp} \qquad \dfrac{\vdash B, B^\perp \qquad \vdash C, C^\perp}{\vdash B^\perp\otimes C^\perp, B, C}}{\vdash A\otimes B, A^\perp, B^\perp\otimes C^\perp, C}\,\text{cut} \qquad \cancel{\vdash A, A^\perp}}{\vdash A\otimes B, B^\perp\otimes C^\perp, C, A^\perp}\,\text{cut}
$$

$$
\dfrac{\dfrac{\vdash A\otimes B, B^\perp\otimes C^\perp, C, A^\perp}{\vdash A\otimes B, B^\perp\otimes C^\perp, A^\perp, C}\,\text{scambio}}{\vdash A\otimes B, B^\perp\otimes C^\perp, A^\perp ⅋ C}\,⅋
$$

dimostrazione normale.

$$\cfrac{\cfrac{\cfrac{\cfrac{}{A, A^\perp} \qquad \cfrac{}{B, B^\perp}}{A\otimes B, A^\perp, B^\perp}\otimes \qquad \cfrac{}{C, C^\perp}}{A\otimes B, B^\perp\otimes C^\perp, A^\perp, C}\otimes}{A\otimes B, B^\perp\otimes C^\perp, A^\perp \parr C}\parr$$

normale

Π_3

no cut

Π_1

ordine delle regole

$$\cfrac{\cfrac{\cfrac{\cfrac{}{A, A^\perp} \qquad \cfrac{}{B, B^\perp}}{A\otimes B, A^\perp, B^\perp}\otimes}{A\otimes B, A^\perp \parr B^\perp}\parr \qquad \cfrac{\cfrac{\cfrac{\cfrac{}{B, B^\perp} \qquad \cfrac{}{C, C^\perp}}{B^\perp\otimes C^\perp, B, C}\otimes \qquad \cfrac{}{A, A^\perp}}{A\otimes B, B^\perp\otimes C^\perp, A^\perp, C}\otimes}{A\otimes B, B^\perp\otimes C^\perp, A^\perp \parr C}\parr}{A\otimes B, B^\perp\otimes C^\perp, A^\perp \parr C}\text{cut}$$

$*$

$\parr$

Π_2

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{}{A, A^\perp} \qquad \cfrac{}{B, B^\perp}}{A\otimes B, A^\perp, B^\perp}\otimes}{A\otimes B, A^\perp \parr B^\perp}\parr \qquad \cfrac{\cfrac{\cfrac{}{B, B^\perp} \qquad \cfrac{}{C, C^\perp}}{B^\perp\otimes C^\perp, B, C}\otimes \qquad \cfrac{}{A, A^\perp}}{A\otimes B, B^\perp\otimes C^\perp, A^\perp, C}\otimes}{A\otimes B, B^\perp\otimes C^\perp, A^\perp, C}\text{cut}}{A\otimes B, B^\perp\otimes C^\perp, A^\perp \parr C}\parr$$

$*$

$\parr$

cut $\delta(A\otimes B) = 1$

$h(A\otimes B) = 4$

quando due dimostrazioni sono **equivalenti**?

- **accezione debole**: due dimostrazioni Π_1, Π_2 sono debolmente equivalenti se dimostrano le stesse cose $\vdash \Gamma$
  dimostrano le stesse "cose"

- **accezione forte**: due dim. Π_1 e Π_2 sono fortemente equivalenti se dimostrano le stesse cose $\vdash \Gamma$ allo stesso modo

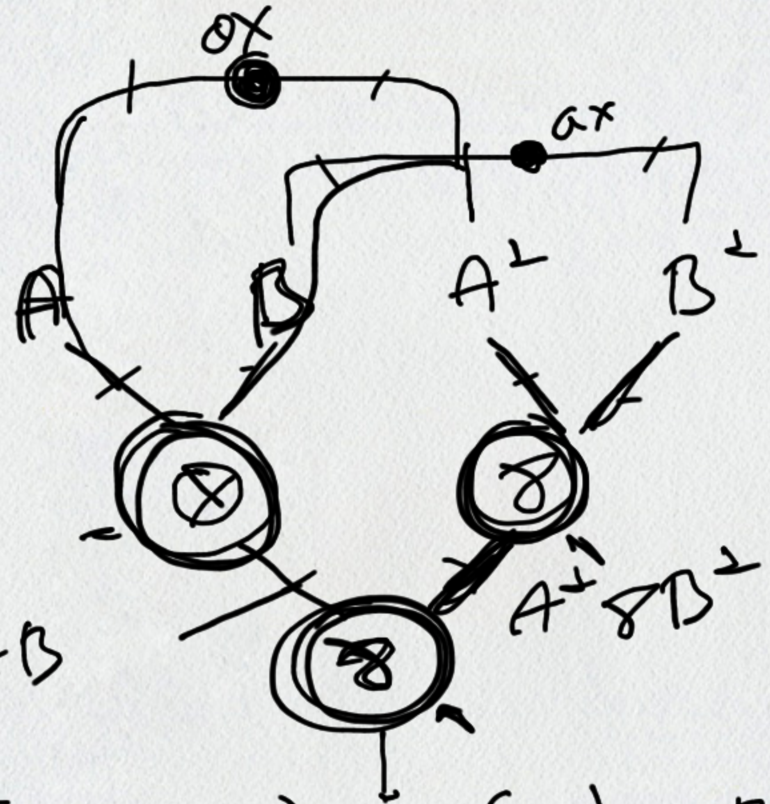
$\downarrow$

differiscono solo per l'ordine con il quale abbiamo applicato le regole

Proof nets — idea intuitiva

$E \subseteq V \times V$

grafo $G : \langle V, E \rangle$

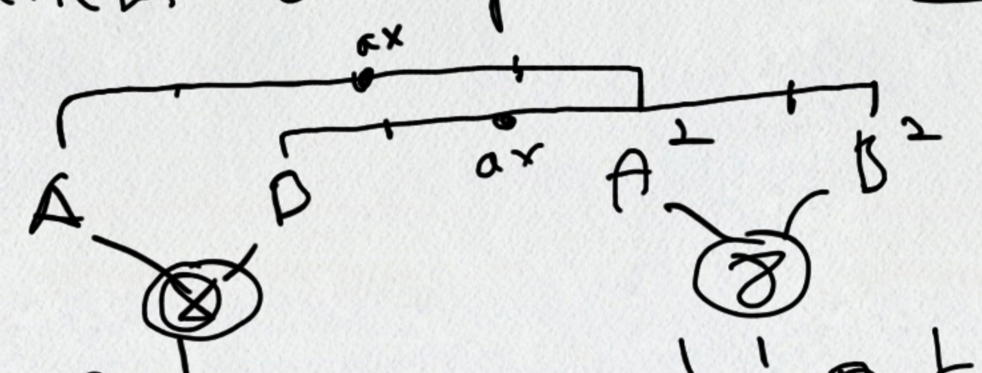


albero sintattico della formula F

$$F = (A \otimes B) \parr (A^\perp \parr B^\perp)$$

una proof net è un grafo

- i nodi sono etichettati da $\otimes$, $\parr$, assiomi (ax), cut
- gli archi sono etichettati da formule di MLL

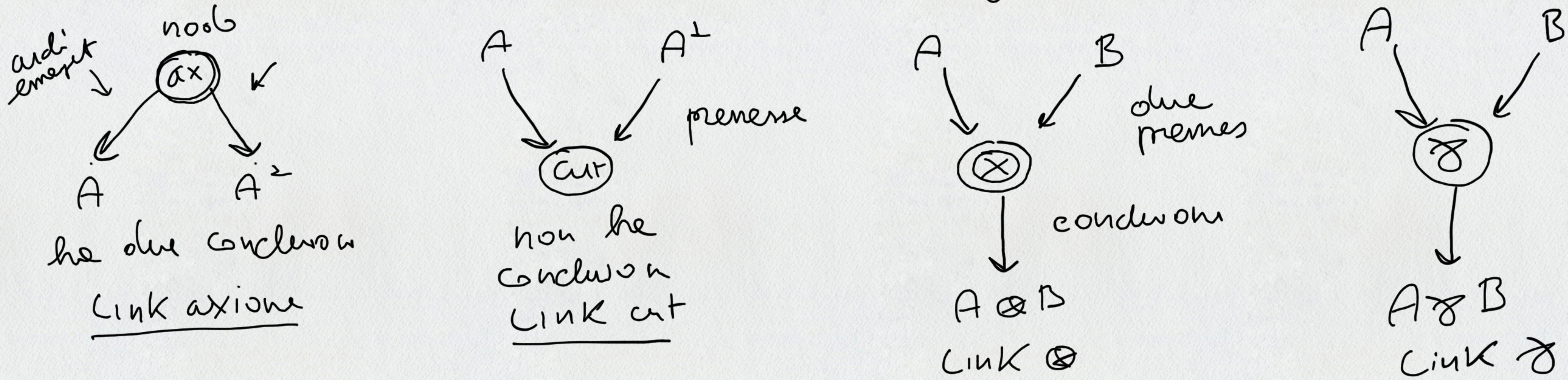


$$\vdash \underset{F_1}{A \otimes B}, \underset{F_2}{A^\perp \parr B^\perp}$$

grafo etichettato

più formule la definizione

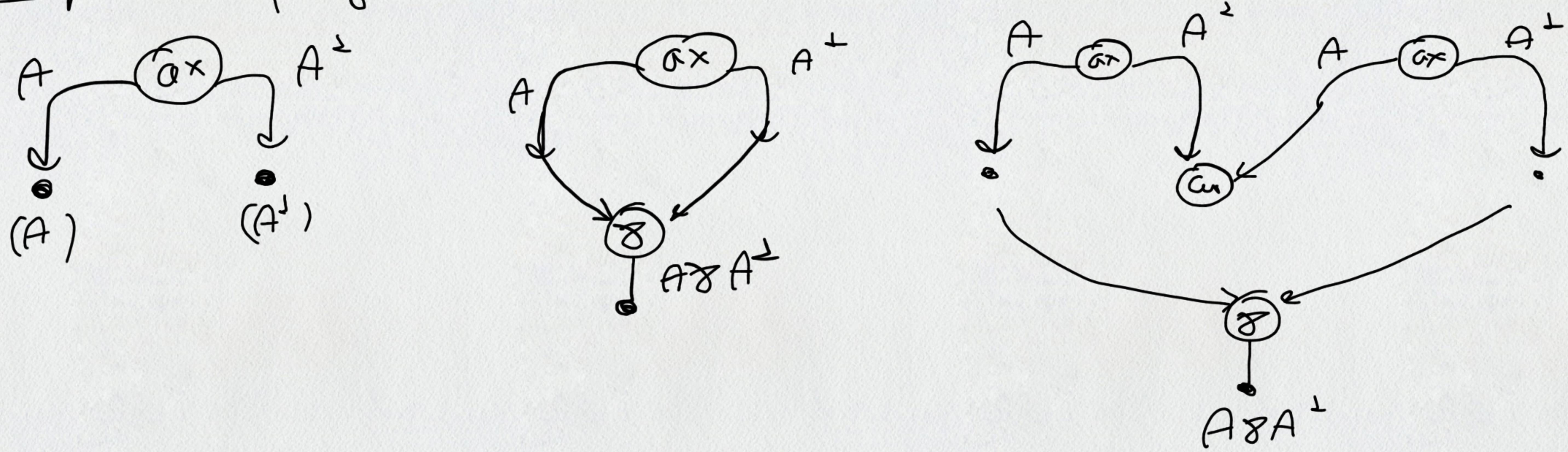
Proof-structure (strutture di prove) un grafo orientato costruito mediante LINK



Def. una struttura di prova (PS) π è un grafo costruito a partire dai link (di sopra) e tale che:

- ogni arco è la conclusione di esattamente un nodo e la premessa di al massimo un nodo
- le conclusioni di π che non sono premesse di altri legami (LINK) sono dette conclusioni della struttura di prova.
- sulle conclusioni aggiungiamo dei nodi speciali • per marcare le conclusioni i nodi.

Esempi di proof structure



$A, A^\perp$ ⊗

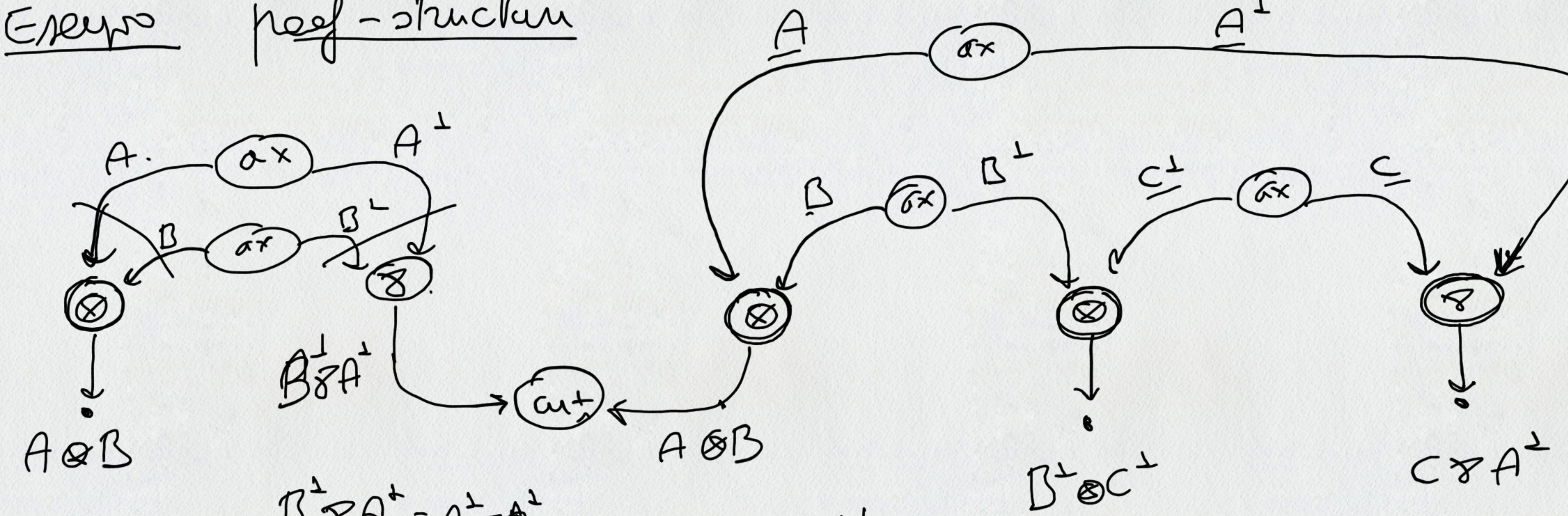
C

$A^\perp ⅋ C$

$A ⊗ B, \ldots ⊗ C^\perp, A^\perp ⅋ C$

cut $\delta(A ⊗ B) = 1$
$\partial(A ⊗ B) = 4$

Esempio proof-structure



PS

$B^\perp \parr A^\perp \equiv A^\perp \parr B^\perp$

commut-$\parr$

$\Downarrow$?

Π_1 ordine delle regole

$$
\dfrac{
\dfrac{\dfrac{A, A^\perp \qquad B, B^\perp}{A\otimes B, A^\perp, B^\perp}\otimes}{A\otimes B, A^\perp \parr B^\perp}\parr
\qquad
\dfrac{\dfrac{\dfrac{\dfrac{B, B^\perp \qquad C, C^\perp}{B^\perp\otimes C^\perp, B, C}\otimes \qquad A, A^\perp}{A\otimes B, B^\perp\otimes C^\perp, A^\perp, C}\otimes}{A\otimes B, B^\perp\otimes C^\perp, A^\perp \parr C}\parr}{}
}{A\otimes B, B^\perp\otimes C^\perp, A^\perp \parr C}\text{cut}
$$

?

Π_2

$$
\dfrac{\dfrac{
\dfrac{\dfrac{A, A^\perp \qquad B, B^\perp}{A\otimes B, A^\perp, B^\perp}\otimes}{A\otimes B, A^\perp \parr B^\perp}\parr
\qquad
\dfrac{\dfrac{\dfrac{B, B^\perp \qquad C, C^\perp}{B^\perp\otimes C^\perp, B, C}\otimes \qquad A, A^\perp}{A\otimes B, B^\perp\otimes C^\perp, A^\perp, C}\otimes
}{A\otimes B, B^\perp\otimes C^\perp, A^\perp, C}\text{cut}}{A\otimes B, B^\perp\otimes C^\perp, A^\perp \parr C}\parr
$$

cut $\delta(A\otimes B) = 1$
$h(A\otimes B) = 4$

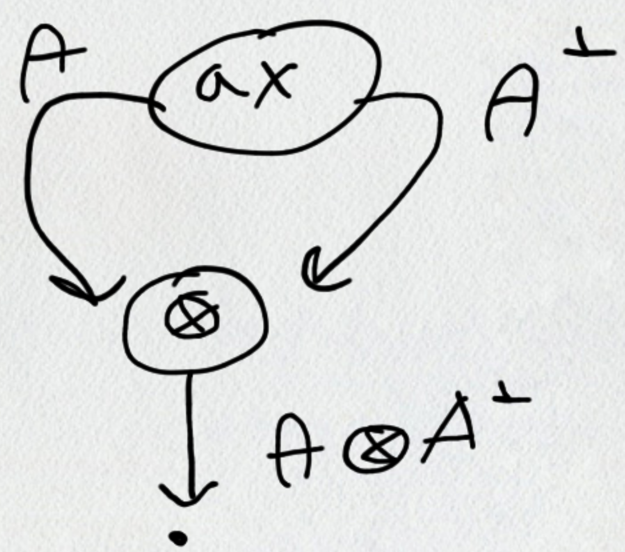
Corrispondenza PS vs dim. MLL

- **Correttezza**: se π è una PS con conclusioni Γ, allora $\vdash \Gamma$ è dimostrabile in MLL sequent calculus ?

- **Completezza**: se $\vdash \Gamma$ è dimostrabile nel calcolo dei sequenti di MLL allora esiste una PS π con conclusioni Γ ?

$$\text{dim } \vdash \Gamma \text{ in MLL} \iff \exists \text{ una PS di } \Gamma$$

Esempio

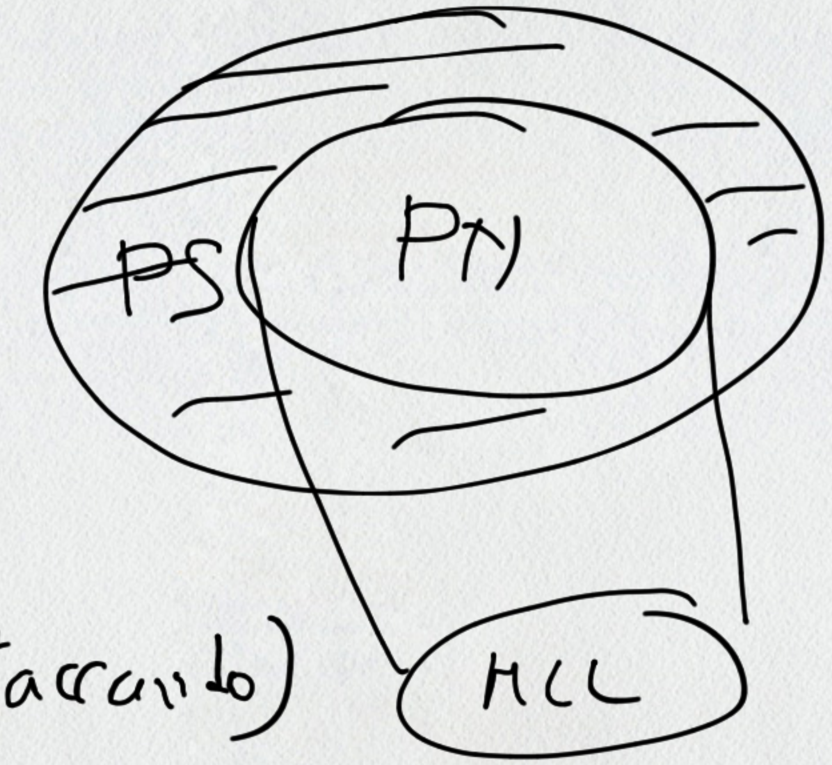


ma $\not\vdash_{MLL} A \otimes A^\perp$!!!

$\exists$ più PS che dim. in MLL !! bisogna restringere la nozione di PS

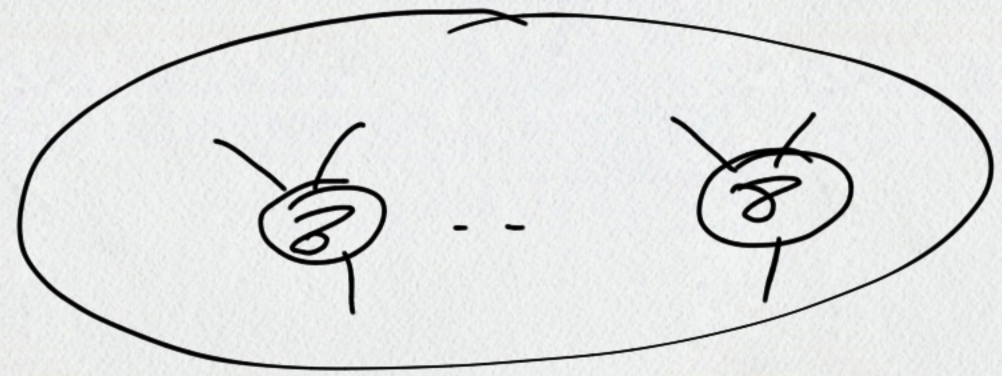
PS + correttezza (invarianze geometriche)

idea interattiva : Test

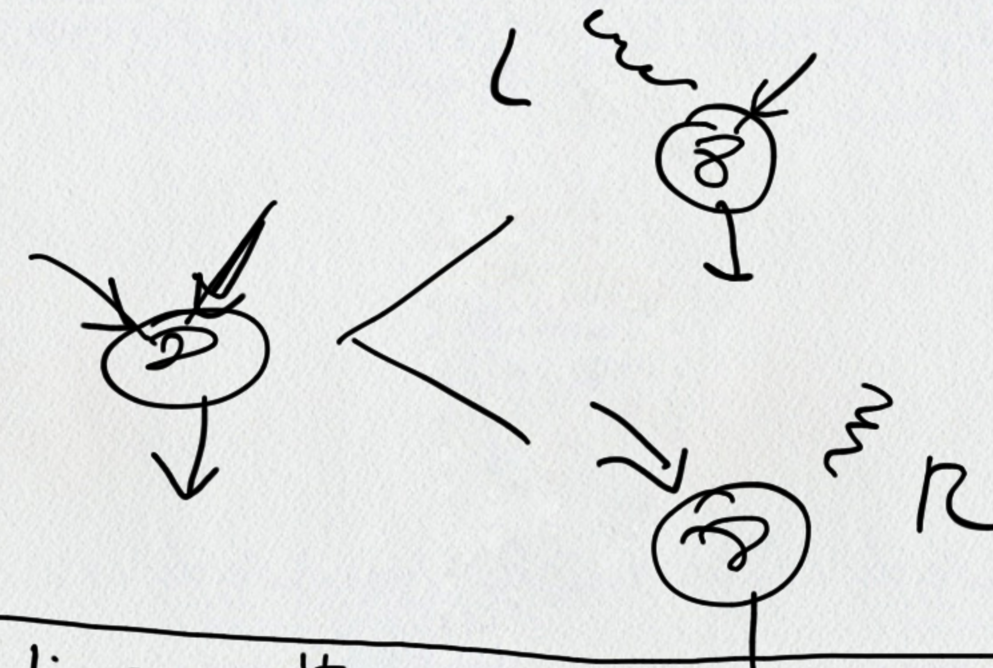


Def

- un Test per una PS π : è il grafo che si ottiene da π, mutilando (staccando) una delle due premesse di ogni link $⅋$

π 

switch : $\varphi : ⅋ \longmapsto \{L/R\}$



switching/test di π

test $\quad S_\varphi(\pi)$

Def. criterio di correttezza

Una PS π è corretta (è una proof net) sse $\forall \varphi$, test $S_\varphi(\pi)$ è un grafo aciclico, connesso (ACC)

(non riferito al grafo orientato)
grafo non-orientato

Osservo: se Π è una PS e contiene n link $\wp$
quanti test ammette?

$\wp_1$ 0 1 0
0 0 1
$\vdots$ 0 0
0 0
0 0
$\wp_n$ 0 1

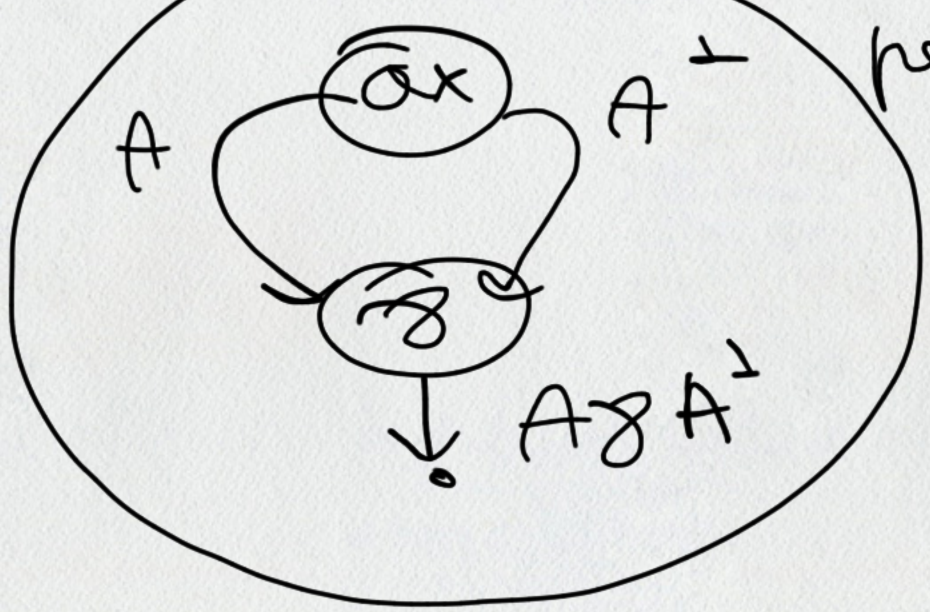
gli switch possibili $S\varphi(\Pi)$ sono 2^n

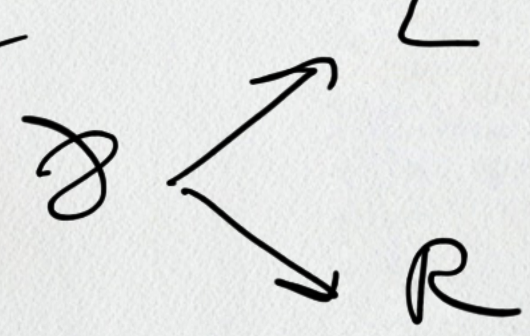
i test sono costosi!
il costo è esponenziale! nel $\# \wp$

Esempio

è corretta!
è una proofnet!

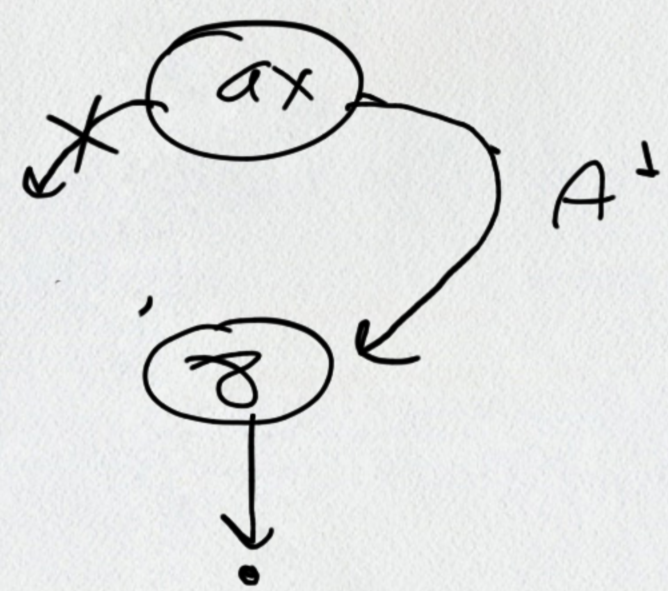
Π:



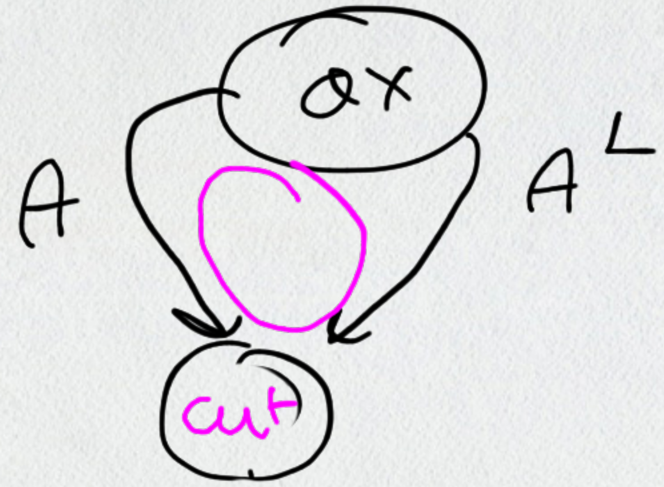


$\checkmark$

quanti i test di Π $\quad S\varphi(\Pi) = \{$



Es.

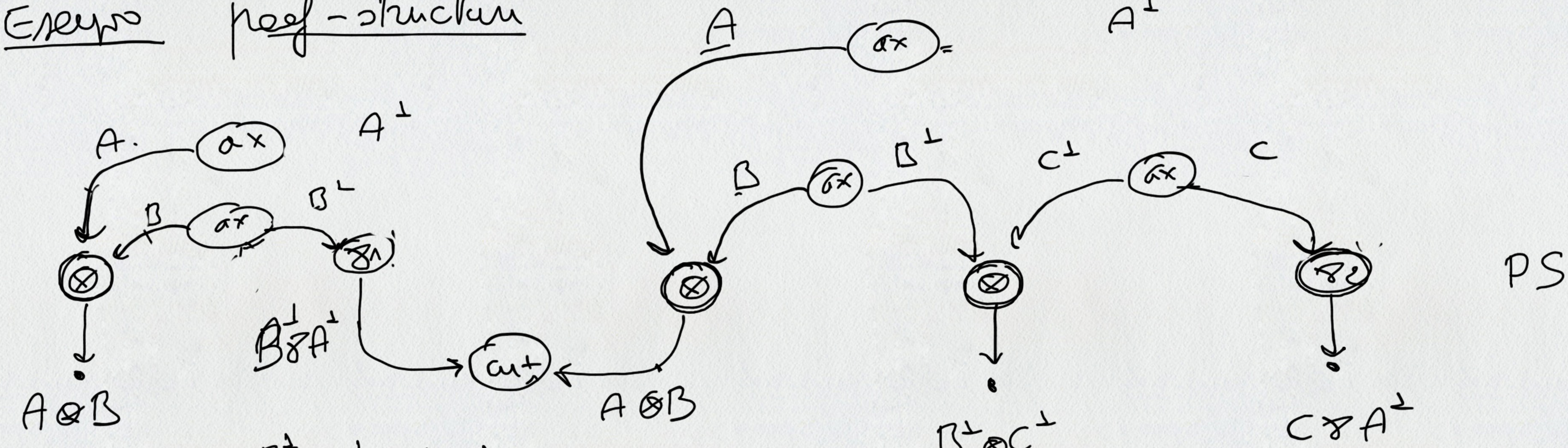


non è corretto! non è una proof net

è corretta?

deadlock! loop

Esempio proof-structure

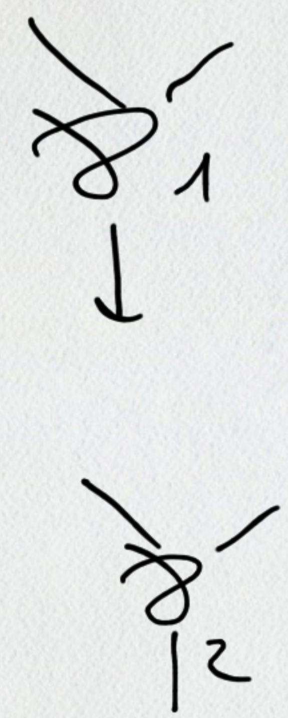


$B^\perp \wp A^\perp \equiv A^\perp \wp B^\perp$

domanda è una PN ?

quanti $\wp$-link ? 2 quanti interruttori 2

quanti $S\varphi(\pi)$? $2^2 = 4$ test



Def. induttiva delle PN

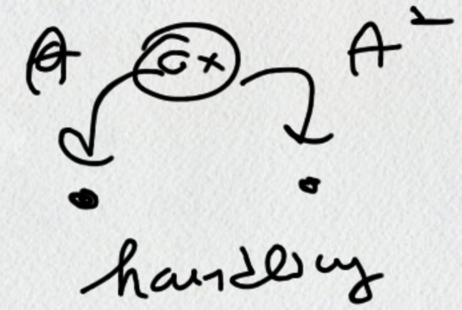
$\Longrightarrow$ correttezza

de-sequenzializzazione

se π è una deriv. nel C.S di MLL di $\vdash \Gamma$ allora $\exists$ una PN π di Γ

S.C

in MLL S.C. $\overline{\vdash A, A^\perp}$ $\longrightarrow$ PN



è PS, $\forall S(\pi)$ è ACC.

base ind.

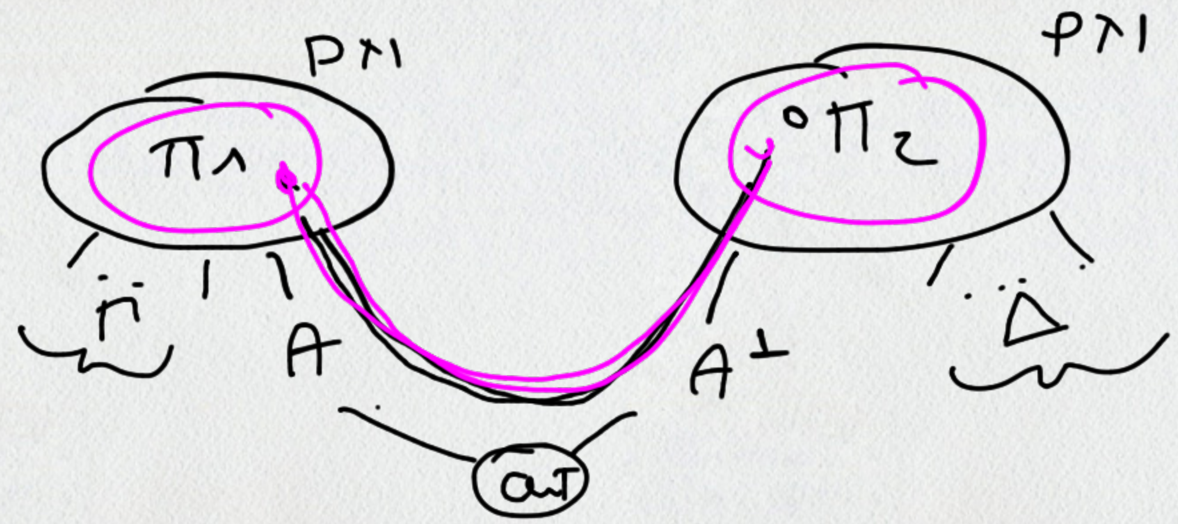
passo induttivo

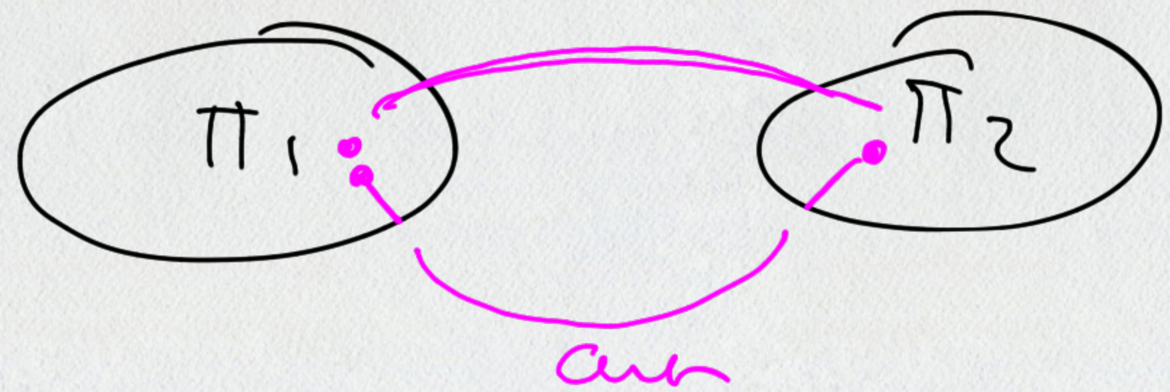
$h(\pi)$

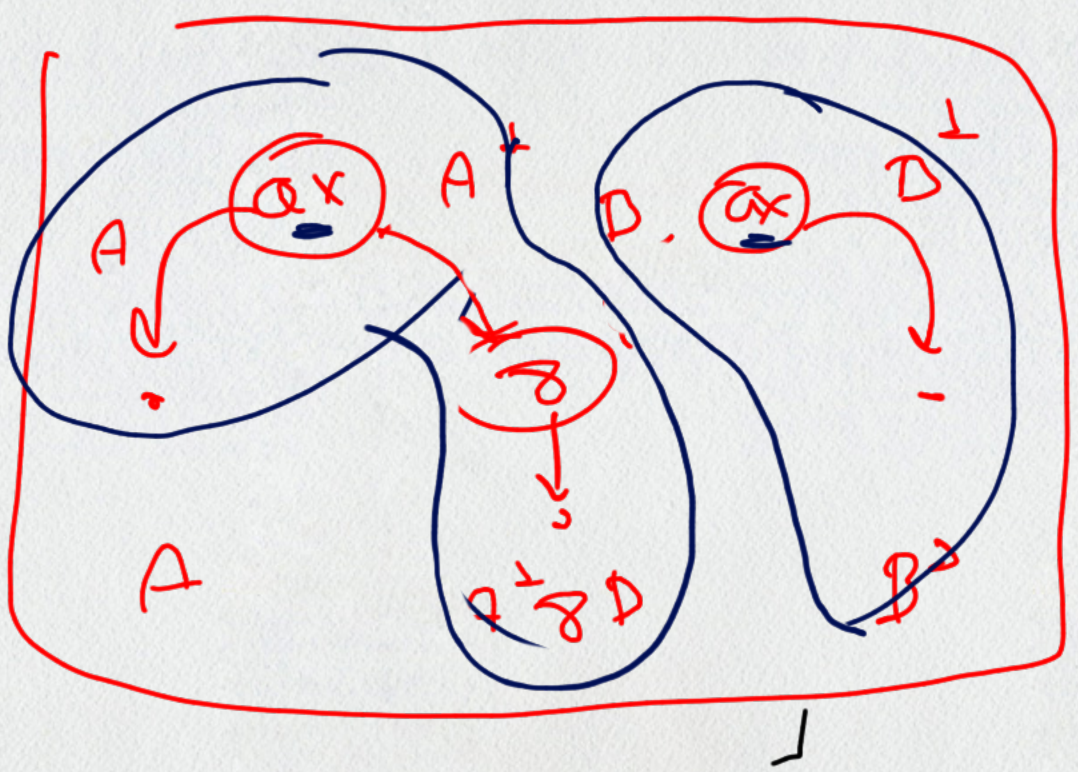
induzione

$$\dfrac{\begin{matrix}\Pi_1 \\ \vdash \Gamma, A\end{matrix} \qquad \vdash \Delta, A^\perp}{\vdash \Gamma, \Delta}\text{cut} \longrightarrow$$

PN ip. ind.





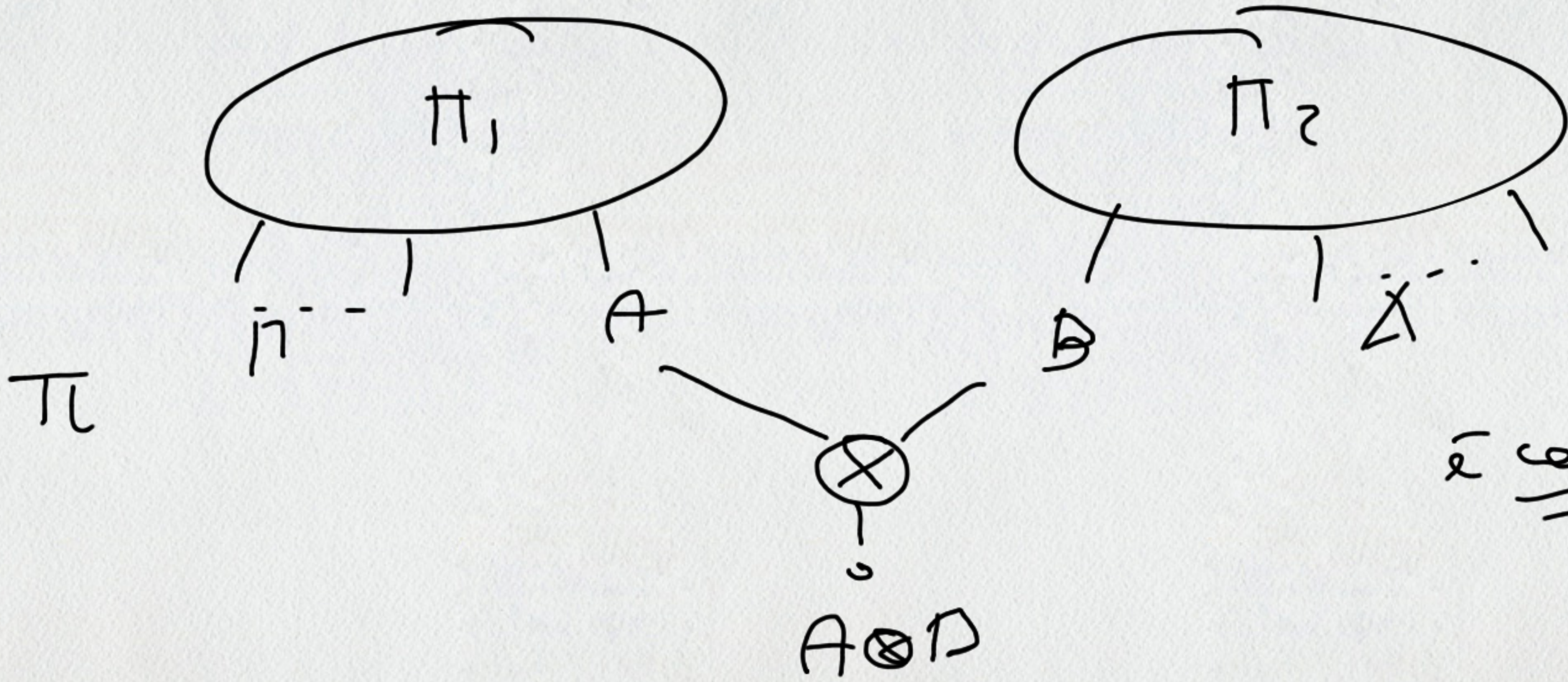


$\overline{\vdash A, A^\perp}$

$\vdots$?

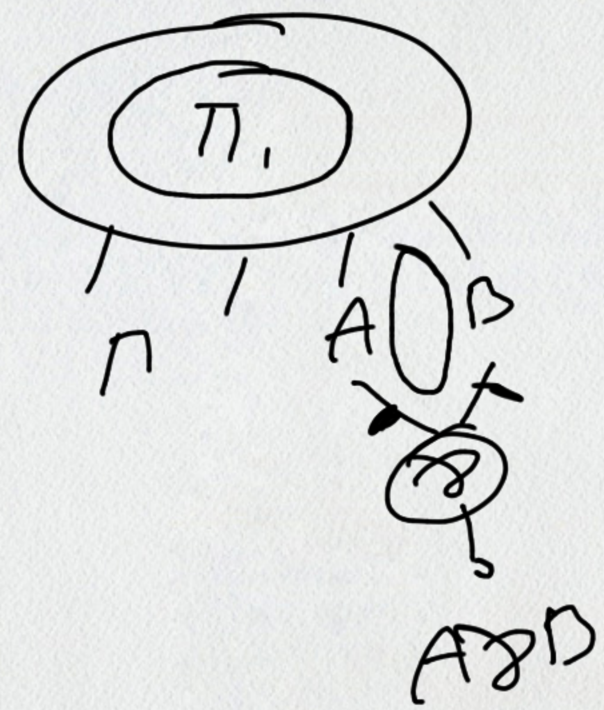
$$\dfrac{\vdash A, A^\perp, ~~?B~~, ~~?B^\perp~~}{\not\vdash A, A^\perp ⅋ B, B^\perp}⅋$$

$$\pi : \frac{\vdash \Gamma, A \qquad \vdash \Delta, B}{\vdash \Gamma, A \otimes B}\otimes \;\longmapsto$$



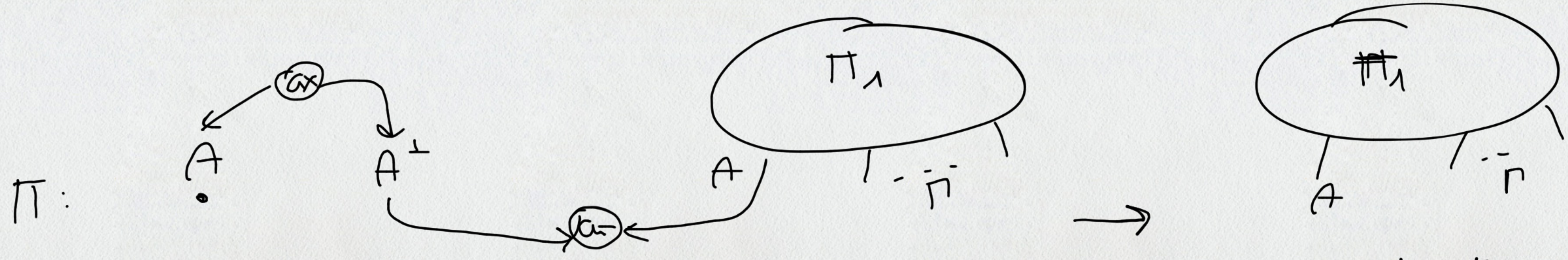
è corretto

$$\pi \quad \begin{array}{c}\pi_1 \\ \dfrac{\vdash \Gamma, A, B}{\vdash \Gamma, A \parr B}\parr\end{array} \longrightarrow$$



$S_\varphi(\pi)$

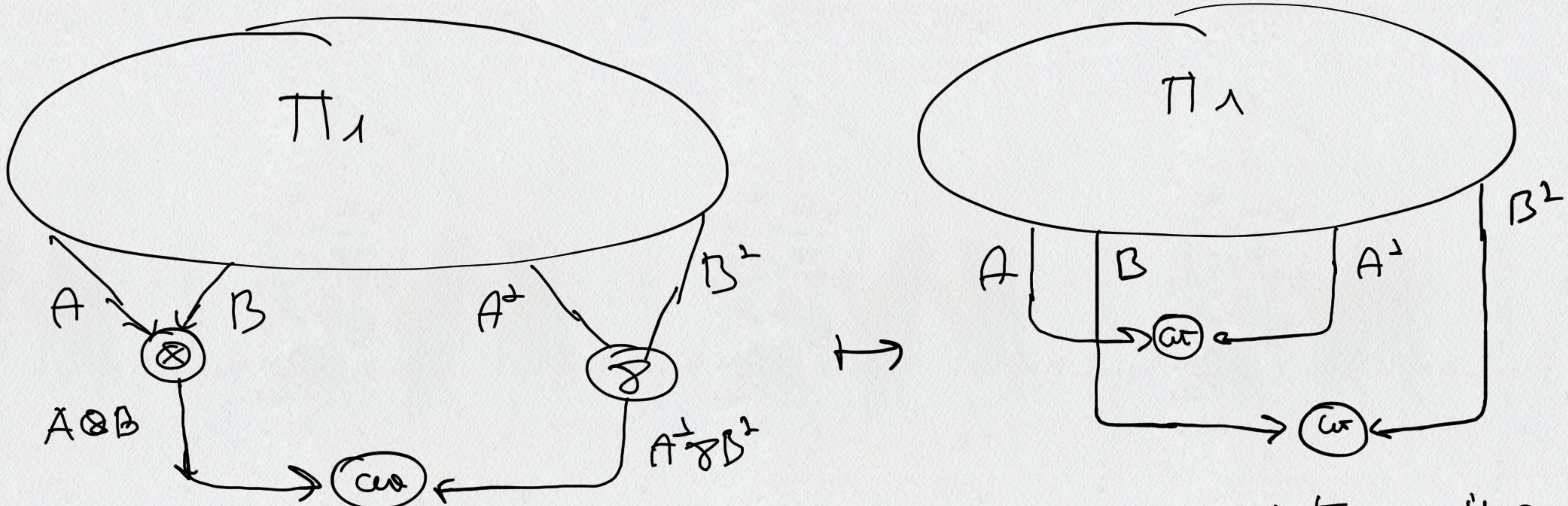
Cut- elim. steps



rid. axiom

redex - axiom

reductum.

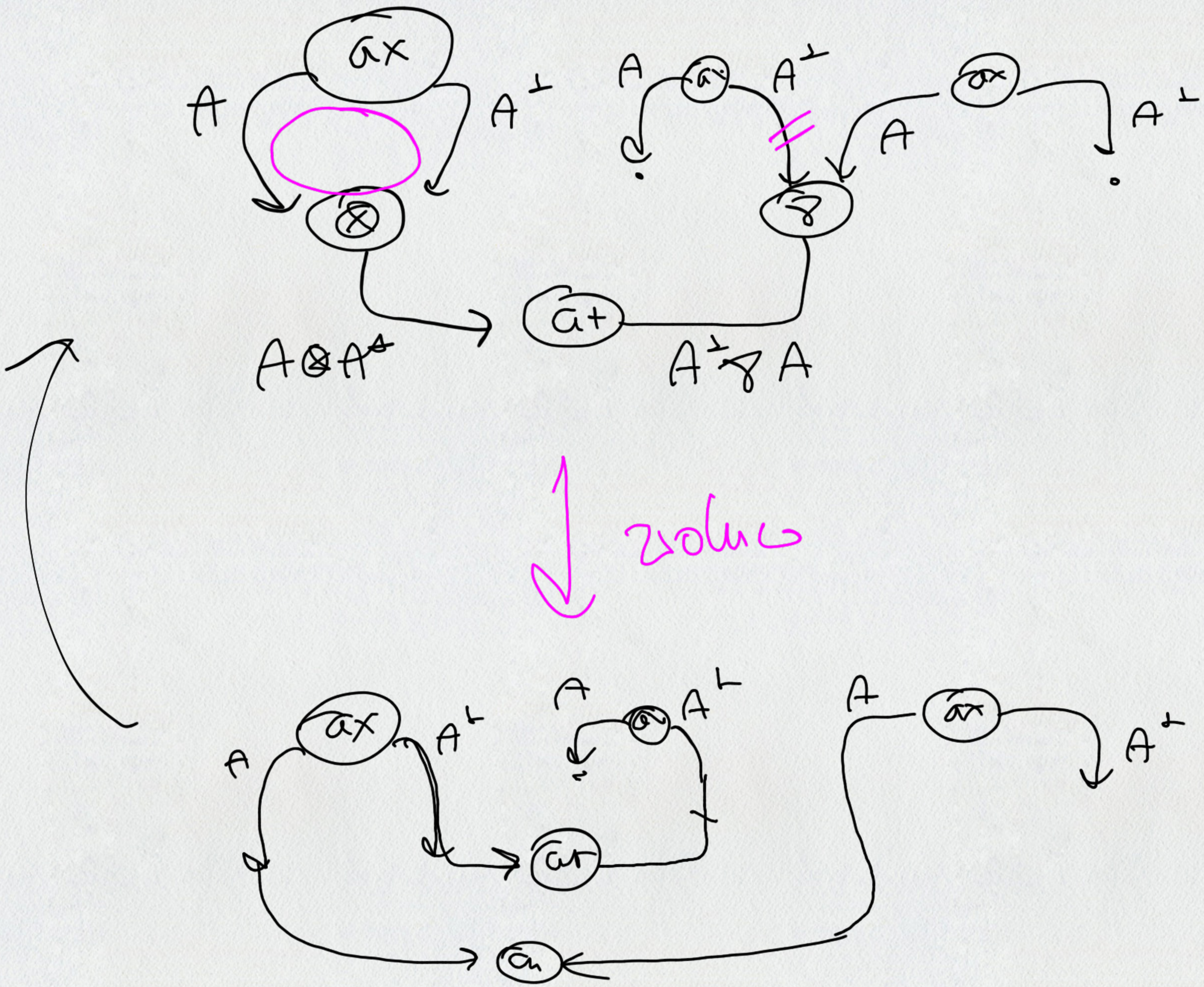


redex $A \otimes B$

$(A^\perp ⅋ B^\perp)^\perp$

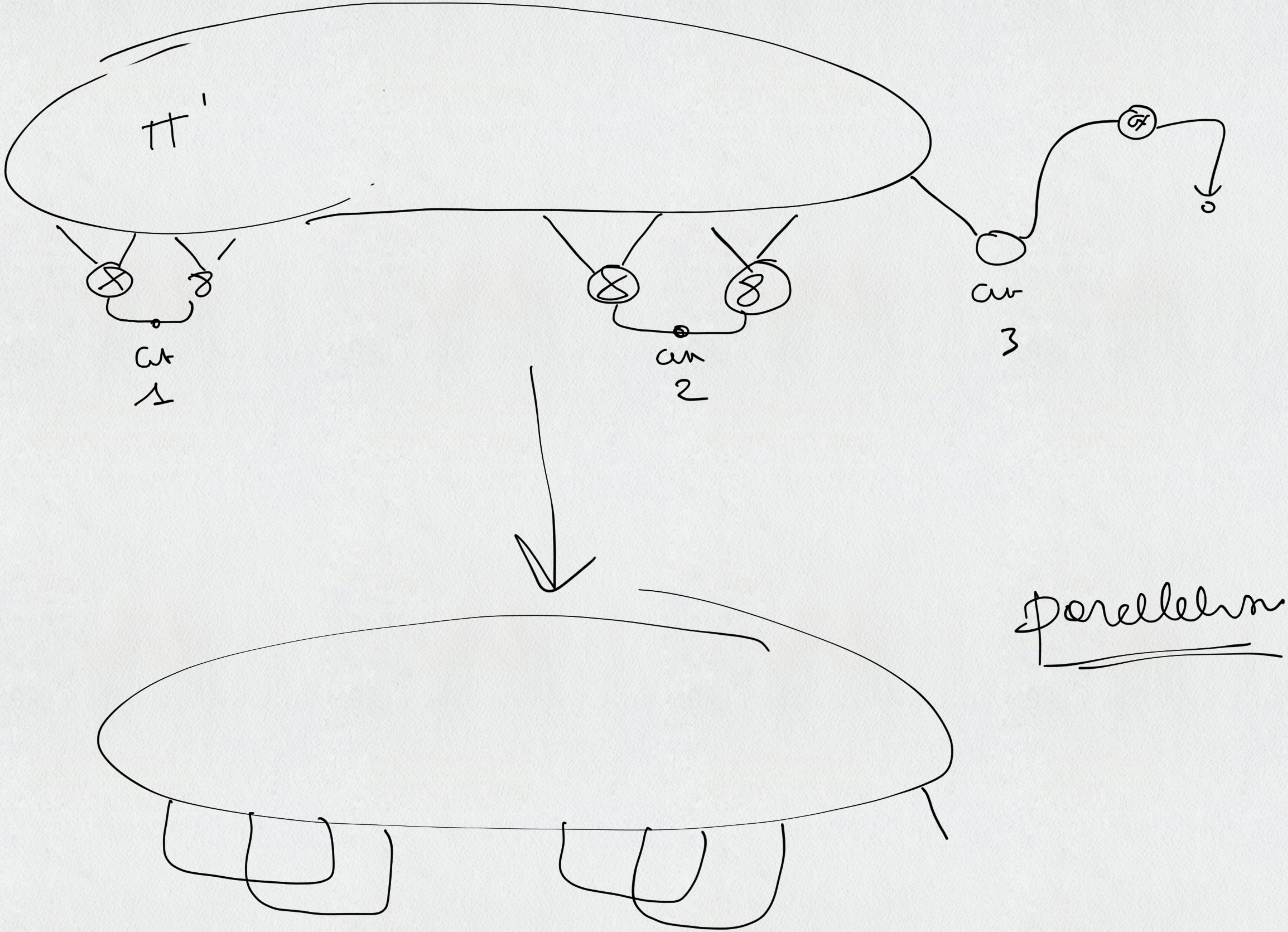
Probleme : termine, confluence

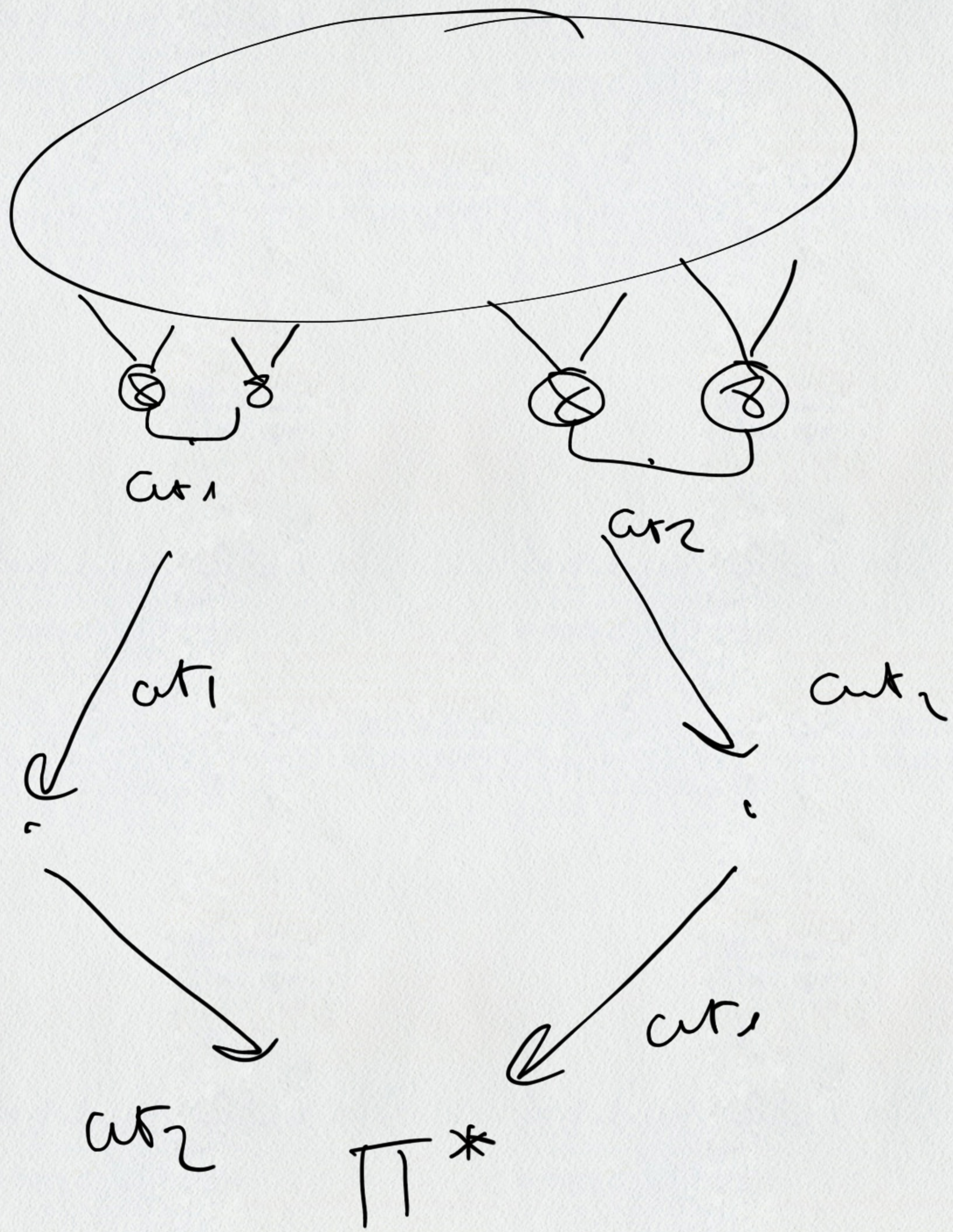
stabilità della correttezza (ACC) under cut-reduction



PS che non è corretto!!!
non è una PN.

<u>corretta</u>


H'
cut 1
cut 2
cut 3
parallelism



Confluenza locale!

Reduction

- sequenzializzazioni
- riduzioni

normalizzazione — cut-reduction Python λ-calc

focalizzazione — proof-search dimostrazione automatica Prolog.

- Correttezza 2^n ove $n = \#⅋$ esponenziale

$\downarrow$

contrazioni quadratico n^2 $\quad O(n^2) < O(2^n)$

$\downarrow$

lineari $\#V$

lineari le cut reduction

MALL

MELL

MLL