Lezione $\sharp$
Introduzione alla Logica Lineare

Roberto Maieli

Università degli Studi "Roma Tre"
maieli@uniroma3.it
http://logica.uniroma3.it/~maieli/teaching

Corso di Logica (II livello, magistrale):
Introduzione alla Proof-Theory ed ai suoi più recenti sviluppi

Corso di Logica II Livello: pre-requisiti

Assumiamo che lo studente, possibilmente appartenente ad un CdS Magistrale in Filosofia, abbia già seguito con profitto un

Corso introduttivo di Logica di I Livello (triennale, 36H, 6CFU)

nel quale abbia appreso alcune nozioni di logica di base quali:

- Cos'è una proposizione logica, quali sono i modi per stabilire (dimostrare) o respingere (refutare) una proposizione
- Calcolo Proposizionale: connettivi, dualità, tavole di verità, leggi logiche;
- Calcolo dei Predicati: quantificatori e formule del Primo Ordine; proposizioni categoriche, soddisfacibilità, validità, conseguenza logica; chiusure universali ed esistenziali. Enunciati (senza dimostrazioni) dei Teoremi di Completezza ed Incompletezza dei Gödel

Corso di Logica II Livello: obiettivi e contenuti

Questo corso di II livello mira ad una moderna introduzione alla

Teoria della Dimostrazione e i suoi sviluppi (36H, 6CFU).

Principali argomenti trattati ($\sim$6H per argomento):

1. Deduzione Naturale e Calcoli dei Sequenti per LJ ed LK.
2. Teorema di Eliminazione del Taglio di Gentzen.
3. Teorema di Compattezza e Completezza.
4. Questioni di (Ind-)Decidibilità e Teoremi di Incompletezza di Gödel.
5. Recenti sviluppi della Teoria della Dimostrazione: la Logica Lineare
   - 5.1 **frammento Moltiplicativo e Reti Dimostrative** (**lez. oggi**)
   - 5.2 frammento Additivo ed Esponenziale: le regole strutturali.
   - 5.3 interazioni/applicazioni della LL con/alle altre scienze: filosofia, linguistica, informatica, biologia.

Logica intuizionista, classica e lineare

- la Logica Lineare (Girard, 1987), un raffinamento della logica classica ed intuizionista:
  - **Logica Classica ed Intuizionista** pone l'accento sulle nozioni di **veritá** e **validitá** (cruciali in Filosofia e Matematica)
  - **Logica Lineare** pone l'accento piuttosto sulle nozioni di **azione** e **risorsa** (cruciali in Informatica, Fisica, Biologia)
- La principale novità introdotta dalla LL è la nozione di : **rete dimostrativa** (o **proof-net**)
- I proof-nets sono la chiave di volta per studiare l'intera LL.

la novità della LL: i *proof-nets*

Il concetto di rete dimostrativa ha *triplice natura*:

- sintattica: perché parla di dimostrazioni come oggetti geometrici finiti (*grafi*) ... l'informatica parla di grafi (*programmi*), la biologia parla di grafi (*regolatori*);
- semantica: perché consente di catturare la nozione di *equivalenza tra dimostrazioni*: un proof-net (oggetto finito) intuitivamente rappresenta una classe (potenzialmente infinita) di dimostrazioni del calcolo dei sequenti equivalenti a meno di operazioni burocratiche (permutabilità di regole logiche, ordine delle regole,...)
- computazionale: perché consente di esprimere l'eliminazione del taglio (vero motore computazionale della logica) in maniera efficace: i tagli vengono eliminati in maniera locale, parallela e confluente.

Il frammento moltiplicativo di LL: le regole

- *Formule*: $A, B, \ldots$ sono definite induttivamente a partire dai *letterali* (atomi o atomi negati) per mezzo dei connettivi lineari:

$$\otimes \ (\textit{tensore o congiunzione}), \ \parr \ (\textit{par o disgiunzione}).$$

- *Negazione*: $(.)^\perp$ si estende alle formule via le Leggi di de Morgan:

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

- *Sequenti (ad una parte)*: Γ, Δ sono insiemi (una disgiunzione) di occorrenze di formule $A_1, \ldots, A_{n \geq 1}$, derivati usando le regole:

identitá :
$$\frac{}{\vdash A, A^\perp}\,\mathrm{ax} \qquad \frac{\vdash \Gamma, A \qquad \vdash \Delta, A^\perp}{\vdash \Gamma, \Delta}\,\mathrm{cut}$$

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

Osservazione: $\Gamma \vdash \Delta \ \Leftrightarrow \ \vdash (\otimes\Gamma)^\perp, \Delta$, via negazione

Il frammento moltiplicativo di LL: le dimostrazioni

Una derivazione (prova o dimostrazione) del sequente $\vdash \Gamma$ é un albero:

- le foglie sono etichettate dagli assiomi logici,
- la conclusione è etichettata dal sequente $\vdash \Gamma$, ed
- ogni nodo intermedio é etichettato da un sequente derivato mediante una delle regole logiche o cut.

Esempio 1 (omettiamo "$\vdash$"):

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

Esercizio: la $\parr$-regola è invertibile: $\vdash \Gamma, A, B \quad \Leftrightarrow \quad \vdash \Gamma, A \parr B$

($\Rightarrow$) ovvio. ($\Leftarrow$) $\dfrac{\Gamma, A \parr B \qquad A^\perp \otimes B^\perp, A, B}{\Gamma, A, B}\,\mathit{cut}$

problemi del calcolo dei sequenti: eliminazione del taglio

TEOREMA : ogni dimostrazione di $\vdash \Gamma$ puó essere trasformata in una dimostrazione "equivalente" (con la stessa conclusione Γ) senza tagli.

IDEA DELLA PROVA (assumiamo una dimostrazione con un solo cut) : per induzione (lessicografica) sulla coppia $\langle \delta, \lambda \rangle$ dove:

- δ é la complessitá (il numero di connettivi $\otimes / \parr$) della cut-formula;
- λ é la profonditá di un taglio (la profonditá di una inferenza é data dal *max* delle profonditá delle eventuali premesse + 1; gli assiomi sono a profonditá 1).

ESEMPIO 2: qui sotto l'unico cut ha complessitá 1 e profonditá 5.

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

problemi del calcolo dei sequenti: eliminazione del taglio

TEOREMA : ogni dimostrazione di $\vdash \Gamma$ puó essere trasformata in una dimostrazione "equivalente" (con la stessa conclusione Γ) senza tagli.

IDEA DELLA PROVA (assumiamo una dimostrazione con un solo cut) : per induzione (lessicografica) sulla coppia $\langle \delta, \lambda \rangle$ dove:

- δ é la complessitá (il numero di connettivi $\otimes / \parr$) della cut-formula;
- λ é la profonditá di un taglio (la profonditá di una inferenza é data dal *max* delle profonditá delle eventuali premesse $+ 1$; gli assiomi sono a profonditá 1).

ESEMPIO 2: via invertibilitá della regola $\parr$ trasformiamo la prova in una equivalente con un cut di uguale complessitá ma minore profonditá (4).

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

Possiamo applicare l'ipotesi di induzione (**QUANTA BUROCRAZIA!**)

problemi del calcolo dei sequenti: equivalenza tra dimostrazioni (1/2)

Il teorema di eliminazione del taglio pone una questione logica e filosofica importante: **quando due dimostrazioni sono equivalenti?**

- (*accezione debole*): due dimostrazioni sono equivalenti se dimostrano la stessa **cosa** (denotano la stessa cosa).
- (*accezione forte*): due dimostrazioni sono equivalenti se dimostrano la stessa **cosa** nello stesso **modo** (hanno lo stesso "senso").

problemi del calcolo dei sequenti: equivalenza (2/2)

ESEMPIO 3: tre dimostrazioni equivalenti, ma in senso diverso!

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

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

le prime due differiscono per la permutazione di $\parr/\mathit{cut}$

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

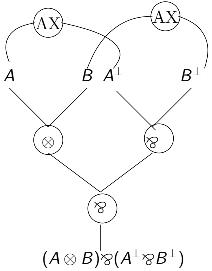
la terza é ció che si ottiene dalle prime due, dopo aver eliminato i tagli

Che fare?

- Per rispondere a queste questioni introduciamo una nuova sintassi: le reti dimostrative (proof-nets).
- Sinteticamente: una proof net è una classe di equivalenza modulo invertibilita' delle regole di dimostrazioni
- In maniera meno roboante: una proof net rappresenta (sintatticamente) una classe di dimostrazioni che differiscono solo per l'ordine in cui le regole logiche sono applicate.
- Ha una duplice natura (ne vedremo una terza):
  – semantica, in quanto sta per una classe di oggetti equivalenti; e
  – sintattica, perché parla di dimostrazioni come oggetti finiti, grafi.

strutture dimostrative: intuitivamente

è possibile vedere una dimostrazione (senza tagli) di una formula F come un grafo ottenuto aggiungendo all'albero sintattico di F degli archi (assiomi) tra due letterali duali (X ed $X^\perp$).

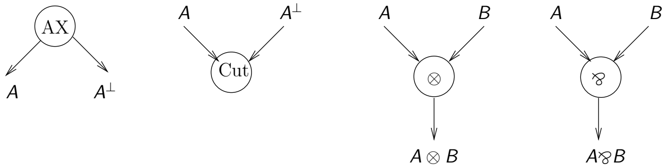


Informalmente: una rete dimostrativa è un grafo, detto struttura di prova, tale che:
1) – i nodi sono etichettati da $\otimes$, $\parr$, *Axiom* o *Cut*,
2) – gli archi sono etichettati da formule;
3) – soddisfa una proprietá geometrica (*criterio di correttezza*).

strutture dimostrative: formalmente

– un **legame** (o link) é uno dei seguenti grafi:

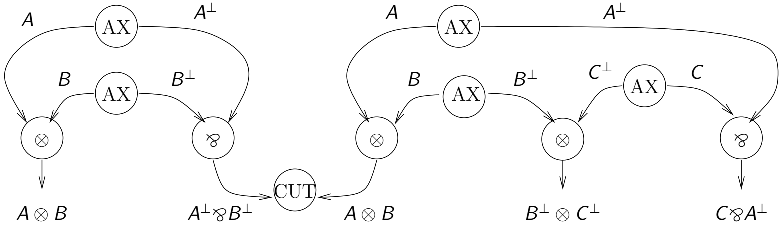
- i nodi sono etichettati dai Connettivi ($\otimes, \parr$), Axioma o Cut;
- gli archi orientati sono etichettati da formule:
  – gli archi incidenti un nodo sono dette *premesse*,
  – quelli emergenti sono chiamati *conclusioni* del legame



– una **struttura di prova** π é un grafo costruito a partire dai legami e tale che: ogni arco é la conclusione di esattamente un nodo e la premessa di al massimo un nodo.

– conclusioni che non sono premesse di altri legami sono dette *conclusioni della struttura di prova*.

Esempio 4: una struttura dimostrativa



Esiste un rapporto passa tra questo grafo e la dimostrazione seguente ?

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

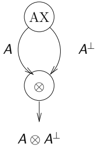
strutture dimostrative vs dimostrazioni

a-priori vorremmo che le strutture dimostrative fossero corrette e complete rispetto al calcolo dei sequenti.

- **Correttezza**: se π é una struttura dimostrativa con conclusione Γ, allora $\vdash \Gamma$ é dimostrabile nel Calcolo dei Sequenti.
- **Completezza**: se $\vdash \Gamma$ é dimostrabile nel Calcolo dei Sequenti allora esiste una struttura dimostrativa π con conclusioni Γ.

Problema: ci sono piú strutture dimostrative che dimostrazioni del calcolo dei sequenti; ci sono strutture prive di "senso dimostrativo" (... ma non per questo "insensate"!)

ESEMPIO 5: una struttura di prova con conclusione $A \otimes A^{\perp}$



ma $\nvdash A \otimes A^{\perp}$!

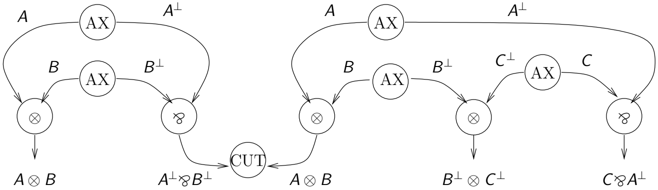
Morale: occorre dunque restringere la nozione di struttura dimostrativa e caratterizzare esattamente quelle che provengono da dimostrazioni del Calcolo dei Sequenti.

le strutture dimostrative corrette: proof nets (e tests)

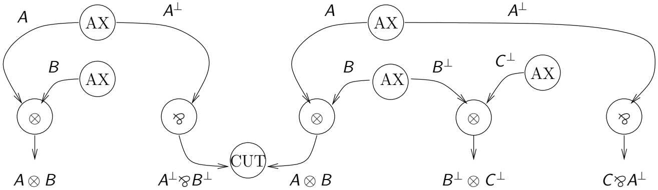
- **Idea interattiva**: consideriamo corrette solo quelle strutture che resistono a tutti gli attacchi o **test**.
- un **test** τ per una struttura dimostrativa π é il grafo che si ottiene da π mutilando una delle due premesse di ogni legame $\parr$.
- **Criterio di Correttezza**: una struttura dimostrativa π é corretta (cioè un **proof-net**) se ogni test é un grafo connesso e aciclico (un albero).
- OSSERVAZIONE: testare la correttezza di una struttura π richiede a-priori "troppo lavoro": *esponenziale* nel numero dei legami $\parr$ (infatti, se π ha n legami $\parr$, allora $\exists 2^n$ tests per π);

  In pratica, peró, il criterio puó essere reso piú efficiente: in tempo *lineare* nel numero dei legami $\parr$ (si usano *algoritmi di unificazione*).

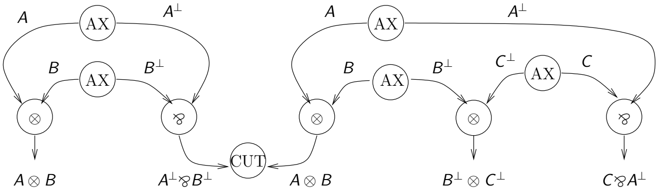
Esempio di rete dimostrativa: resiste ai tests (1/4)



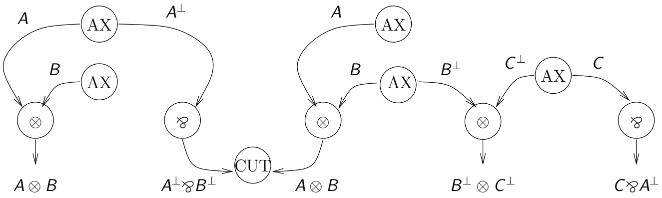
resiste a tutti e 4 i possibili tests:
il primo test é infatti un grafo connesso e aciclico (un albero)



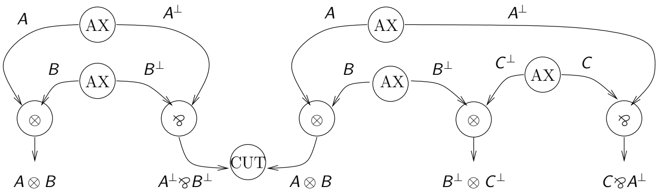
Esempio di rete dimostrativa: resiste ai tests (2/4)



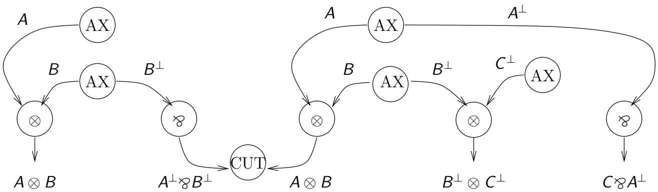
resiste a tutti e 4 i possibili tests:
il secondo test é infatti un grafo connesso e aciclico (un albero)



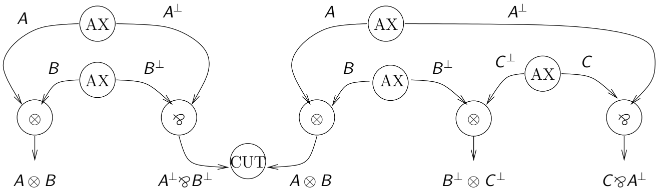
Esempio di rete dimostrativa: resiste ai tests (3/4)



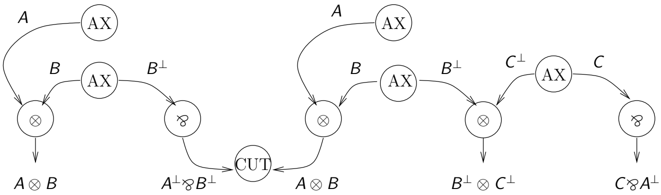
resiste a tutti e 4 i possibili tests:
il terzo test é un grafo connesso e aciclico (un albero)



Esempio di rete dimostrativa: resiste ai tests (4/4)



resiste a tutti e 4 i possibili tests:
il quarto ed ultimo test é ancora un grafo connesso e aciclico (un albero)

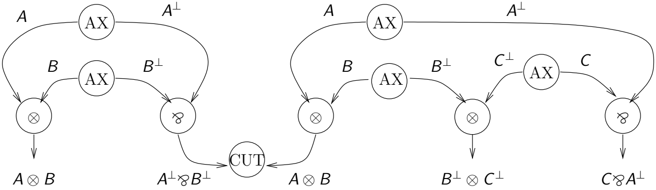


Il Criterio di Correttezza è necessario e sufficiente

- TEOREMA [**sequenzializzazione**]: ogni dimostrazione Π con conclusioni $\vdash \Gamma$ puó essere trasformata in una rete dimostrativa π con le stesse conclusioni e viceversa.
- DIMOSTRAZIONE:
  - ($\Rightarrow$) "ogni dimostrazione Π di $\vdash \Gamma$ può essere de-sequenzializzata in una struttura corretta π con le stesse conclusioni".
    Dimostrazione facile: per induzione sulla profondità della dimostrazione Π *del calcolo dei sequenti.*
  - ($\Leftarrow$) "ogni struttura corretta π con conclusioni Γ puó essere sequenzializzata in una dimostrazione Π di $\vdash \Gamma$".
    Dimostrazione difficile: per induzione sulla taglia (numero dei nodi) della rete dimostrativa (come esercizio provate il caso con strutture prive di cut).
- COROLLARIO [**equivalenza sintattica**]: Se due dimostrazioni si de-sequenzializzano nella medesima rete dimostrativa, allora sono equivalenti .

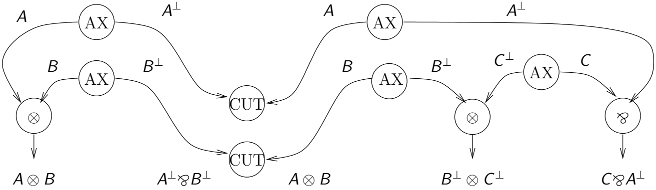
significato computazionale: *Hauptsatz* (1/4)

- TEOREMA: ogni rete dimostrativa con tagli puó essere trasformata in una rete con le stesse conclusioni e senza tagli.
- DIMOSTRAZIONE: per induzione sulla complessitá logica (numero dei connettivi) delle formule tagliate.
- ESEMPIO: la rete dimostrativa con un solo taglio di complessitá 1



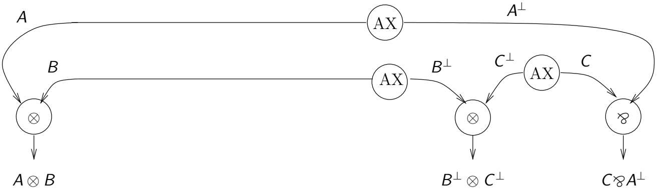
significato computazionale: *Hauptsatz* (2/4)

- TEOREMA: ogni rete dimostrativa con tagli puó essere trasformata in una rete con le stesse conclusioni e senza tagli.
- DIMOSTRAZIONE: per induzione sulla complessitá logica (numero dei connettivi) delle formule tagliate.
- ESEMPIO: si riduce ad una rete con due tagli di complessitá 0



significato computazionale: *Hauptsatz* (3/4)

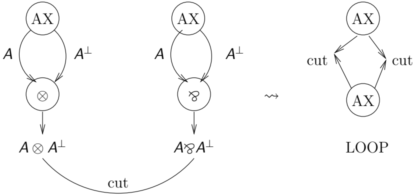
- TEOREMA: ogni rete dimostrativa con tagli puó essere trasformata in una rete con le stesse conclusioni e senza tagli.
- DIMOSTRAZIONE: per induzione sulla complessitá logica (numero dei connettivi) delle formule tagliate.
- ESEMPIO: che si riduce infine ad una rete priva di tagli (*normale*).



significato computazionale: *Hauptsatz* (4/4)

La procedura di eliminazione del taglio:

- è **fortemente normalizzante**: termina sempre con la stessa forma normale;
- è **locale**: solo i nodi immediatamente contigui al cut sono coinvolti;
- è **concorrente**: i passi di riduzione possono esser eseguiti simultaneamente;
- **preserva la nozione di struttura di prova**: ma non tutti gli oggetti scorretti hanno un "senso computazionale";



- **preserva la correttezza** (proof-net).

fine

- ESERCITAZIONE: ...
- PROSSIME LEZIONI:
  – regole strutturali,
  – connettivi additivi ed esponenziali,
  – interazione/applicazioni con/alle altre scienze.
- Grazie per l'attenzione!