

# Proofs and Types

## Cut Elimination (Hauptsatz)

Bow-Yaw Wang

Academia Sinica

Spring 2012

# Cut

- ▶ Recall the cut rule:

$$\frac{\underline{A} \vdash C, \underline{B} \quad \underline{A'}, C \vdash \underline{B'}}{\underline{A}, \underline{A'} \vdash \underline{B}, \underline{B'}} \text{ Cut}$$

- ▶ If the cut rule were necessary, proof search would be difficult.
  - ▶ How can a theorem prover “guess” the cut formula  $C$ ?
- ▶ Gentzen showed that the cut rule is redundant in sequent calculus.
- ▶ More precisely, a proof with cuts in sequent calculus can be transformed to a proof without cuts.
- ▶ We begin by considering the forms of the cut formula.

## Key Cases

- ▶ A conjunction ( $\mathcal{R}\wedge$  and  $\mathcal{L}1\wedge$ ).

$$\frac{\frac{\underline{A} \vdash C, \underline{B} \quad \underline{A'} \vdash D, \underline{B'}}{\underline{A}, \underline{A'} \vdash C \wedge D, \underline{B}, \underline{B'}} \mathcal{R}\wedge \quad \frac{\underline{A''}, C \vdash \underline{B''}}{\underline{A''}, C \wedge D \vdash \underline{B''}} \mathcal{L}1\wedge}{\underline{A}, \underline{A'}, \underline{A''} \vdash \underline{B}, \underline{B'}, \underline{B''}} \text{Cut}$$

is transformed to

$$\frac{\frac{\underline{A} \vdash C, \underline{B} \quad \underline{A''}, C \vdash \underline{B''}}{\underline{A}, \underline{A''} \vdash \underline{B}, \underline{B''}} \text{Cut}}{\underline{A}, \underline{A'}, \underline{A''} \vdash \underline{B}, \underline{B'}, \underline{B''}}$$

- ▶ A conjunction ( $\mathcal{R}\wedge$  and  $\mathcal{L}2\wedge$ ).

$$\frac{\frac{\underline{A} \vdash C, \underline{B} \quad \underline{A'} \vdash D, \underline{B'}}{\underline{A}, \underline{A'} \vdash C \wedge D, \underline{B}, \underline{B'}} \mathcal{R}\wedge \quad \frac{\underline{A''}, D \vdash \underline{B''}}{\underline{A''}, C \wedge D \vdash \underline{B''}} \mathcal{L}2\wedge}{\underline{A}, \underline{A'}, \underline{A''} \vdash \underline{B}, \underline{B'}, \underline{B''}} \text{Cut}$$

is transformed to

$$\frac{\frac{\underline{A} \vdash D, \underline{B} \quad \underline{A'}, D \vdash \underline{B'}}{\underline{A}, \underline{A'} \vdash \underline{B}, \underline{B'}} \text{Cut}}{\underline{A}, \underline{A'}, \underline{A''} \vdash \underline{B}, \underline{B'}, \underline{B''}}$$

## Key Cases

- ▶ A disjunction ( $\mathcal{R}1\vee$  and  $\mathcal{L}\vee$ ).

$$\frac{\frac{\underline{A} \vdash C, \underline{B}}{\underline{A} \vdash C \vee D, \underline{B}} \mathcal{R}1\vee \quad \frac{\underline{A'}, C \vdash \underline{B'} \quad \underline{A''}, D \vdash \underline{B''}}{\underline{A'}, \underline{A''}, C \vee D \vdash \underline{B'}, \underline{B''}} \mathcal{L}\vee}{\underline{A}, \underline{A'}, \underline{A''} \vdash \underline{B}, \underline{B'}, \underline{B''}} \text{Cut}$$

is transformed to

$$\frac{\frac{\underline{A} \vdash C, \underline{B} \quad \underline{A'}, C \vdash \underline{B'}}{\underline{A}, \underline{A'} \vdash \underline{B}, \underline{B'}} \text{Cut}}{\underline{A}, \underline{A'}, \underline{A''} \vdash \underline{B}, \underline{B'}, \underline{B''}}$$

- ▶ A disjunction ( $\mathcal{R}2\vee$  and  $\mathcal{L}\vee$ ).

$$\frac{\frac{\underline{A} \vdash D, \underline{B}}{\underline{A} \vdash C \vee D, \underline{B}} \mathcal{R}2\vee \quad \frac{\underline{A'}, C \vdash \underline{B'} \quad \underline{A''}, D \vdash \underline{B''}}{\underline{A'}, \underline{A''}, C \vee D \vdash \underline{B'}, \underline{B''}} \mathcal{L}\vee}{\underline{A}, \underline{A'}, \underline{A''} \vdash \underline{B}, \underline{B'}, \underline{B''}} \text{Cut}$$

is transformed to

$$\frac{\frac{\underline{A} \vdash D, \underline{B} \quad \underline{A''}, D \vdash \underline{B''}}{\underline{A}, \underline{A''} \vdash \underline{B}, \underline{B''}} \text{Cut}}{\underline{A}, \underline{A'}, \underline{A''} \vdash \underline{B}, \underline{B'}, \underline{B''}}$$

## Key Cases

- ▶ A negation ( $\mathcal{R}\neg$  and  $\mathcal{L}\neg$ ).

$$\frac{\frac{\underline{A}, C \vdash \underline{B}}{\underline{A} \vdash \neg C, \underline{B}} \mathcal{R}\neg \quad \frac{\underline{A'} \vdash C, \underline{B'}}{\underline{A'}, \neg C \vdash \underline{B'}} \mathcal{L}\neg}{\underline{A}, \underline{A'} \vdash \underline{B}, \underline{B'}} \text{Cut}$$

is transformed to

$$\frac{\underline{A'} \vdash C, \underline{B'} \quad \underline{A}, C \vdash \underline{B}}{\underline{A'}, \underline{A} \vdash \underline{B'}, \underline{B}} \text{Cut}$$

$$\underline{\underline{A}, \underline{A'} \vdash \underline{B}, \underline{B'}}$$

- ▶ An implication ( $\mathcal{R}\Rightarrow$  and  $\mathcal{L}\Rightarrow$ ).

$$\frac{\frac{\underline{A}, C \vdash D, \underline{B}}{\underline{A} \vdash C \Rightarrow D, \underline{B}} \mathcal{R}\Rightarrow \quad \frac{\underline{A'} \vdash C, \underline{B'} \quad \underline{A''}, D \vdash \underline{B''}}{\underline{A'}, \underline{A''}, C \Rightarrow D \vdash \underline{B'}, \underline{B''}} \mathcal{L}\Rightarrow}{\underline{A}, \underline{A'}, \underline{A''} \vdash \underline{B}, \underline{B'}, \underline{B''}} \text{Cut}$$

is transformed to

$$\frac{\underline{A'} \vdash C, \underline{B'} \quad \underline{A}, C \vdash D, \underline{B}}{\underline{A'}, \underline{A} \vdash \underline{B'}, D, \underline{B}} \text{Cut}$$

$$\underline{\underline{A}, \underline{A'} \vdash \underline{B}, D, \underline{B'}}$$

# Key Cases

- ▶ A universal quantification ( $\mathcal{R}\forall$  and  $\mathcal{L}\forall$ ).

$$\frac{\frac{\underline{A} \vdash C, \underline{B}}{\underline{A} \vdash \forall \xi. C, \underline{B}} \mathcal{R}\forall \quad \frac{\underline{A'}, C[a/\xi] \vdash \underline{B'}}{\underline{A'}, \forall \xi. C \vdash \underline{B'}} \mathcal{L}\forall}{\underline{A}, \underline{A'} \vdash \underline{B}, \underline{B'}} \text{Cut}$$

is transformed to

$$\frac{\underline{A} \vdash C[a/\xi], \underline{B} \quad \underline{A'}, C[a/\xi] \vdash \underline{B'}}{\underline{A}, \underline{A'} \vdash \underline{B}, \underline{B'}} \text{Cut}$$

- ▶ An existential quantification ( $\mathcal{R}\exists$  and  $\mathcal{L}\exists$ ).

$$\frac{\frac{\underline{A} \vdash C[a/\xi], \underline{B}}{\underline{A} \vdash \exists \xi. C, \underline{B}} \mathcal{R}\exists \quad \frac{\underline{A'}, C \vdash \underline{B'}}{\underline{A'}, \exists \xi. C, \underline{B'}} \mathcal{L}\exists}{\underline{A}, \underline{A'} \vdash \underline{B}, \underline{B'}} \text{Cut}$$

is transformed to

$$\frac{\underline{A} \vdash C[a/\xi], \underline{B} \quad \underline{A'}, C[a/\xi] \vdash \underline{B'}}{\underline{A}, \underline{A'} \vdash \underline{B}, \underline{B'}} \text{Cut}$$

# Principal Lemma

- ▶ Let  $A$  be a formula. The *degree*  $\partial(A)$  is defined as follows.
  - ▶ If  $A$  is atomic,  $\partial(A) = 1$ .
  - ▶  $\partial(A \wedge B) = \partial(A \vee B) = \partial(A \Rightarrow B) = \max(\partial(A), \partial(B)) + 1$ .
  - ▶  $\partial(\neg A) = \partial(\forall \xi. A) = \partial(\exists \xi. A) = \partial(A) + 1$ .
- ▶ Observe that  $\partial(A[a/\xi]) = \partial(A)$ .
- ▶ The *degree* of a cut rule is the degree of the cut formula.
  - ▶ The key cases show how to replace a cut with at most two cuts with lower degree.
- ▶ The degree  $d(\pi)$  for a proof  $\pi$  is the sup of the degrees of its cuts.
  - ▶ Hence  $d(\pi) = 0$  if  $\pi$  is cut-free.
- ▶ The *height*  $h(\pi)$  of a proof  $\pi$  is the height of its associated tree.
  - ▶ If  $\pi$  ends in a rule with premises  $\pi_1, \pi_2, \dots, \pi_n$ , then  $h(\pi) = \sup(h(\pi_i)) + 1$ .
- ▶ If  $\underline{A}$  is a sequence of formulae,  $\underline{A} - C$  denotes the sequence obtained by removing all occurrences of  $C$  from  $\underline{A}$ .

# Principal Lemma

## Lemma 1

Let  $C$  be a formula of degree  $d$ , and  $\pi, \pi'$  proofs of  $\underline{A} \vdash \underline{B}$  and  $\underline{A}' \vdash \underline{B}'$  of degrees less than  $d$ . Then there is a proof  $\varpi$  of  $\underline{A}, \underline{A}' - C \vdash \underline{B} - C, \underline{B}'$  of degree less than  $d$ .

## Proof.

By induction on  $h(\pi) + h(\pi')$ . Suppose the last rule  $r$  of  $\pi$  has premises  $\pi_i : \underline{A}_i \vdash \underline{B}_i$ , and the last rule  $r'$  of  $\pi'$  has premises  $\pi'_j : \underline{A}_j \vdash \underline{B}_j$ . Consider

- ▶  $\pi$  is an axiom.
  - ▶  $\pi$  proves  $C \vdash C$ . Then  $\varpi : C, \underline{A}' - C \vdash \underline{B}'$  is obtained from  $\pi'$  through structural rules.
  - ▶  $\pi$  proves  $D \vdash D$ . Then  $\varpi : D, \underline{A}' - C \vdash D, \underline{B}'$  is obtained from  $\pi$  through structural rules.
- ▶  $\pi'$  is an axiom. Handled as in the previous case.
- ▶  $r$  is a structural rule. By IH on  $\pi_1$  and  $\pi'$ , there is  $\varpi_1 : \underline{A}_1, \underline{A}' - C \vdash \underline{B}_1 - C, \underline{B}'$ .  $\varpi$  is obtained from  $\varpi_1$  through structural rules.
- ▶  $r'$  is a structural rule. Dual of the previous case.

# Principal Lemma

## Proof (cont'd).

- ▶  $r$  is a logical rule other than an  $\mathcal{R}$ -rule with the principal formula  $C$ . By IH on  $\pi_i$  and  $\pi'$ , there are  $\varpi_i : \underline{A}_i, \underline{A}' - C \vdash \underline{B}_i - C, \underline{B}'$ . Since the rule  $r$  does not create any  $C$  from  $\underline{B}_i$ ,  $\varpi$  is obtained by applying the rule  $r$  to  $\varpi_i$ .
- ▶  $r'$  is a logical rule other than an  $\mathcal{L}$ -rule with the principal formula  $C$ . Dual of the previous case.
- ▶  $r$  is a logical  $\mathcal{R}$ -rule with the principal formula  $C$  and  $r'$  is a logical  $\mathcal{L}$ -rule with the principal formula  $C$ . By IH on  $\pi_i$  and  $\pi'$ ,  $\pi$  and  $\pi'_j$ , there are

$$\begin{aligned}\varpi_i &: \underline{A}_i, \underline{A}' - C \vdash \underline{B}_i - C, \underline{B}' & (\pi_i \text{ and } \pi') \\ \varpi'_j &: \underline{A}, \underline{A}' - C \vdash \underline{B} - C, \underline{B}'_j & (\pi \text{ and } \pi'_j)\end{aligned}$$

Apply  $r$  to  $\varpi_i$  and  $r'$  to  $\varpi'_j$  and obtain

$$\begin{aligned}\underline{A}, \underline{A}' - C \vdash C, \underline{B} - C, \underline{B}' & \quad (\text{apply the } \mathcal{R}\text{-rule } r \text{ to } \varpi_i) \\ \underline{A}, \underline{A}' - C, C \vdash \underline{B} - C, \underline{B}' & \quad (\text{apply the } \mathcal{L}\text{-rule } r' \text{ to } \varpi'_j)\end{aligned}$$

We obtain  $\underline{A}, \underline{A}' - C, \underline{A}, \underline{A}' - C \vdash \underline{B} - C, \underline{B}', \underline{B} - C, \underline{B}'$  through the cut rule

# Hauptsatz

## Lemma 2

If  $\pi$  is a proof of a sequent of degree  $d > 0$ , a proof  $\varpi$  of the same sequent with a lower degree can be constructed.

## Proof.

Induction on  $h(\pi)$ . Let  $r$  be the last rule of  $\pi$  with premises  $\pi_i$ .

- ▶  $r$  is not a cut of degree  $d$ . By IH on  $\pi_i$ , we have  $\varpi_i$  of degree  $< d$ .  $\varpi$  is obtained by applying  $r$  to  $\varpi_i$ .
- ▶  $r$  is a cut of degree  $d$ :

$$\frac{\underline{A} \vdash C, \underline{B} \quad \underline{A'}, C \vdash \underline{B'}}{\underline{A}, \underline{A'} \vdash \underline{B}, \underline{B'}} \text{ Cut}$$

By IH on  $\pi_i$ , we have  $\varpi_i$  of degree  $< d$ . Apply the principal lemma to obtain  $\varpi$  of degree  $< d$ . □

## Theorem 3 (Gentzen, 1934)

The cut rule is redundant in sequent calculus.

# Complexity of Cut Elimination

- ▶ We give a simple bound on the height of the cut-free proof obtained from cut elimination.
- ▶ The principal lemma is linear.
  - ▶ Eliminating a cut multiplies the height by 4 in the worst case.
  - ▶ Prove by induction.
- ▶ Lemma 2 is exponential.
  - ▶ Reducing the degree by 1 increases the height  $h$  of the proof by  $4^h$ .
    - ▶ Apply the principal lemma to  $h$  cuts.

$$\overbrace{4^{\dots 4}}^h$$

- ▶ Hauptsatz is hyperexponential. That is,  $4^{\overbrace{4^{\dots 4}}^h}$ .

# Resolution

- ▶ Consider *proper* axioms that models domain knowledge.
  - ▶ Say, for example,  
 $\text{parent}(x, y), \text{parent}(y, z) \vdash \text{grandparent}(x, z)$
- ▶ If a cut has an instance of a proper axiom as a premise, the cut cannot be eliminated.
- ▶ In other words, the cut rule (restricted to those sequents obtained from proper axioms) is not redundant.
- ▶ Moreover, if we have only atomic sequents as proper axioms, logical rules are not needed.
  - ▶ An *atomic* sequent is uilt from atomic formulae.
  - ▶ Example.  
 $\text{parent}(x, y), \text{parent}(y, z) \vdash \text{grandparent}(x, z)$
  - ▶ Counterexample.  
 $\text{parent}(x, y) \vdash \text{father}(x, y) \vee \text{mother}(x, y)$

# PROLOG

- ▶ In PROLOG, proper axioms are atomic intuitionistic sequents (or *Horn clauses*)  $\underline{A} \vdash B$ .
- ▶ We want to prove  $\vdash B$  (a *goal*).
- ▶ The PROLOG proof system has the following rules
  - ▶ instances  $\underline{A} \vdash B$  of proper axioms;
  - ▶ identity axioms  $A \vdash A$  with  $A$  atomic;
  - ▶ cut; and
  - ▶ the structural rules.
- ▶ We will show contraction and weakening are redundant in the PROLOG proof system.
  - ▶ Hence only exchange rules are needed.

# PROLOG

## Lemma 4

If the atomic sequent  $\underline{A} \vdash \underline{B}$  is provable in PROLOG, there is an intuitionistic sequent  $\underline{A}' \vdash B'$  proved without contraction nor weakening with  $\underline{A}' \subseteq \underline{A}$  and  $B' \in \underline{B}$ .

## Proof.

Induction on  $\pi : \underline{A} \vdash \underline{B}$ .

- ▶ If  $\pi$  is an axiom, then  $\underline{A} \vdash \underline{B}$  is intuitionistic (that is,  $|\underline{B}| = 1$ ).
- ▶ If  $\pi$  ends in a structural rule with the premise  $\underline{A}_1 \vdash \underline{B}_1$ , we have  $\underline{A}'_1 \vdash B'_1$  with  $\underline{A}'_1 \subseteq \underline{A}_1$  and  $B'_1 \in \underline{B}_1$ . Take  $\underline{A}' = \underline{A}'_1$  and  $B' = B'_1$ .
- ▶ If  $\pi$  ends in a cut

$$\frac{\underline{A}_1 \vdash C, \underline{B}_1 \quad \underline{A}_2, C \vdash \underline{B}_2}{\underline{A}_1, \underline{A}_2 \vdash \underline{B}_1, \underline{B}_2} \text{Cut}$$

By IH, we have  $\underline{A}'_1 \vdash B'_1$  and  $\underline{A}'_2 \vdash B'_2$ . There are two cases:

- ▶  $B'_1 \neq C$ . Take  $\underline{A}' = \underline{A}'_1$  and  $B' = B'_1$ .
- ▶  $B'_1 = C$ . If  $C$  occurs  $n$  times in  $\underline{A}'_2$ , obtain  $\underline{A}'_1, \underline{A}'_1, \dots, \underline{A}'_1, \underline{A}'_2 - C \vdash B'_2$  through exchanges and  $n$  cuts.  $\equiv$

# PROLOG

- ▶ Recall the goals are of the form  $\vdash B$ .
- ▶ Contraction and weakening rules are hence redundant (Lemma 4).
- ▶ Note that the deduction must be in the intuitionistic fragment.
  - ▶  $\mathcal{R}X$  is never applicable.
- ▶ But then,  $\mathcal{L}X$  can always be eliminated by reordering cuts.
- ▶ Moreover, cuts with an identity axiom is redundant.

$$\frac{\underline{A} \vdash C \quad C \vdash C}{\underline{A} \vdash C} \text{Cut}$$

- ▶ In summary, we have

## Theorem 5

*In order to prove a goal, one only needs to use cut with instances of proper axioms.*