Lecture 19 - More Natural Deduction

Vaishnavi Sundararajan

COL703/COL7203 - Logic for Computer Science

Recap: Natural deduction proof system

- Proof system that more closely mirrors human reasoning
- No axiom schema, all proof rules
- Each operator gets an introduction rule and/or an elimination rule
- Introduction rule: Operator appears in the conclusion
- Elimination rule: Operator appears in the (RHS of) premise(s), does not appear in the conclusion
- More amenable to automation; enjoys some nice properties

Recap: Proof rules for propositional fragment

Introduction rule	**Elimination rule**
$\dfrac{\Gamma \vdash \varphi_0 \qquad \Gamma \vdash \varphi_1}{\Gamma \vdash \varphi_0 \wedge \varphi_1} \wedge i$	$\dfrac{\Gamma \vdash \varphi_0 \wedge \varphi_1}{\Gamma \vdash \varphi_j} \wedge e_j$
$\dfrac{\Gamma \vdash \varphi_j}{\Gamma \vdash \varphi_0 \vee \varphi_1} \vee i_j$	$\dfrac{\Gamma \vdash \varphi_0 \vee \varphi_1 \qquad \Gamma, \varphi_0 \vdash \psi \qquad \Gamma, \varphi_1 \vdash \psi}{\Gamma \vdash \psi} \vee e$
$\dfrac{\Gamma, \varphi \vdash \psi}{\Gamma \vdash \varphi \supset \psi} \supset i$	$\dfrac{\Gamma \vdash \varphi \supset \psi \qquad \Gamma \vdash \varphi}{\Gamma \vdash \psi} \supset e$
$\dfrac{\Gamma, \varphi \vdash \neg\psi \qquad \Gamma, \varphi \vdash \psi}{\Gamma \vdash \neg\varphi} \neg i$	$\dfrac{\Gamma \vdash \neg\neg\varphi}{\Gamma \vdash \varphi} \neg e$

Recap: Proof rules for ∃ and ∀

Introduction rule	Elimination rule
$\dfrac{\Gamma \vdash \varphi\{y/x\}}{\Gamma \vdash \forall x.\ [\varphi]}$ ∀i (y fresh)	$\dfrac{\Gamma \vdash \forall x.\ [\varphi]}{\Gamma \vdash \varphi\{t/x\}}$ ∀e
$\dfrac{\Gamma \vdash \varphi\{t/x\}}{\Gamma \vdash \exists x.\ [\varphi]}$ ∃i	$\dfrac{\Gamma \vdash \exists x.\ [\varphi] \quad \Gamma, \varphi\{y/x\} \vdash \psi}{\Gamma \vdash \psi}$ ∃e (y fresh)

where t is a term in the language, and $y \in \mathscr{V}$ is fresh if $y \notin \mathsf{vars}(\Gamma \cup \{\varphi, \psi\})$.

$$\frac{}{\Gamma \vdash \varphi}\ \text{Ax} \quad (\varphi \in \Gamma)$$

We say that $\Gamma \vdash_{\mathscr{G}} \varphi$ if there is a proof of φ from assumptions Γ using Ax and the rules in both the above tables.

Unnecessary detours in proofs

$$\dfrac{\dfrac{}{\varphi, \psi \vdash \varphi}\,\text{Ax} \qquad \dfrac{}{\varphi, \psi \vdash \psi}\,\text{Ax}}{\dfrac{\varphi, \psi \vdash \varphi \land \psi}{\varphi, \psi \vdash \varphi}\,\land e_0}\,\land i \qquad (1)$$

$$\dfrac{}{\varphi, \psi \vdash \varphi}\,\text{Ax} \qquad (2)$$

- In (1), we first introduce an $\land$, and then immediately eliminate it.
- Could have replaced this entire proof by (2), without any such wasteful detours involving large expressions.
- Clearly both valid proofs of the same sequent.
- Prefer (2), since no large expression ($\varphi \land \psi$ in this case) is introduced only to be immediately eliminated.
- What other useless detours are possible? Can we get rid of those also?

Removing unnecessary detours: $\land$

Suppose $\Gamma \vdash \varphi_0$ via a proof π_0 and $\Gamma \vdash \varphi_1$ via π_1.

$$\dfrac{\dfrac{\begin{matrix}\pi_0\\ \vdots\\ \Gamma \vdash \varphi_0\end{matrix} \qquad \begin{matrix}\pi_1\\ \vdots\\ \Gamma \vdash \varphi_1\end{matrix}}{\Gamma \vdash \varphi_0 \land \varphi_1}\ \land\mathrm{i}}{\Gamma \vdash \varphi_i}\ \land\mathrm{e}_i \qquad \rightsquigarrow \qquad \begin{matrix}\pi_i\\ \vdots\\ \Gamma \vdash \varphi_i\end{matrix}$$

Removing unnecessary detours: $\vee$

Suppose $\Gamma \vdash \varphi_0$ via π, $\Gamma, \varphi_0 \vdash \psi$ via π_0, and $\Gamma, \varphi_1 \vdash \psi$ via π_1.

$$\dfrac{\dfrac{\begin{array}{c}\pi\\ \vdots\\ \Gamma \vdash \varphi_0\end{array}}{\Gamma \vdash \varphi_0 \vee \varphi_1}\,\vee\mathrm{i}_0 \qquad \begin{array}{c}\pi_0\\ \vdots\\ \Gamma, \varphi_0 \vdash \psi\end{array} \qquad \begin{array}{c}\pi_1\\ \vdots\\ \Gamma, \varphi_1 \vdash \psi\end{array}}{\Gamma \vdash \psi}\,\vee\mathrm{e} \quad \rightsquigarrow \quad \dfrac{\begin{array}{c}\pi_0\\ \vdots\\ \Gamma, \varphi_0 \vdash \psi\end{array} \quad \begin{array}{c}\pi\\ \vdots\\ \Gamma \vdash \varphi_0\end{array}}{\Gamma \vdash \psi}\,\mathrm{Cut}$$

Exercise: What about an application of $\vee\mathrm{i}_i$ in the second or third premise? Is that a detour to be handled?

Unnecessary detours: $\supset$

Suppose $\Gamma \vdash \varphi$ via a proof π_0 and $\Gamma, \varphi \vdash \psi$ via a proof π_1.

$$\dfrac{\dfrac{\begin{matrix}\pi_1\\ \vdots\\ \Gamma, \varphi \vdash \psi\end{matrix}}{\Gamma \vdash \varphi \supset \psi}\supset\mathrm{i} \qquad \begin{matrix}\pi_0\\ \vdots\\ \Gamma \vdash \varphi\end{matrix}}{\Gamma \vdash \psi}\supset\mathrm{e} \quad \rightsquigarrow \quad \dfrac{\begin{matrix}\pi_1\\ \vdots\\ \Gamma, \varphi \vdash \psi\end{matrix} \quad \begin{matrix}\pi_0\\ \vdots\\ \Gamma \vdash \varphi\end{matrix}}{\Gamma \vdash \psi}\mathrm{Cut}$$

Normal proofs

- We can eliminate the unnecessary detours for $\wedge$, $\vee$, and $\supset$.
- If we keep getting rid of these useless detours, eventually, we arrive at a **normal proof** with no detours.
- Every proof can be converted to a normal equivalent (**How?**)
- Is a smaller proof inherently better?
- How large can a proof of $\Gamma \vdash \varphi$ be?

Normal proofs

- We can eliminate the unnecessary detours for $\wedge$, $\vee$, and $\supset$.
- If we keep getting rid of these useless detours, eventually, we arrive at a **normal proof** with no detours.
- Every proof can be converted to a normal equivalent (**How?**)
- Is a smaller proof inherently better?
- How large can a proof of $\Gamma \vdash \varphi$ be?
- No ab initio bound, since we still need to instantiate each proof rule with expressions.
- Is there a bound on the size of any expression that can occur in any proof of $\Gamma \vdash \varphi$?

Proof search: System without negation

- A normal proof will satisfy a **subformula property**
- Any expression occurring in any normal proof of $\Gamma \vdash \varphi$ is a subformula of φ, or of some expression in Γ.
- Need to consider subformulas of the conclusion only when the last rule is an introduction rule! Just subformulas of Γ for elimination rules.
- Consider the set S of subformulae of Γ and φ. S is perhaps large, depending on how big Γ is (but still finite)!
- No longer have to consider arbitrary expressions in any proof; gives us an algorithm for proof search!
- Algorithm is non-deterministic: Guess the last rule of a possible proof, and check if premises are derivable.

Proof search algorithm

- Want to determine if $\Gamma \vdash \varphi$. Let the last rule of a proof be r.
- Suppose φ is $\alpha \wedge \beta$, and we guess r to be $\wedge i$
- Then, check if $\Gamma \vdash \alpha$ and $\Gamma \vdash \beta$
- Both (recursive) calls need to succeed!
- What if φ is $\alpha \supset \beta$, and we guess r to be $\supset i$?
- Left hand side has to be enlarged!
- Recursive call to check if $\Gamma, \alpha \vdash \beta$

Proof search algorithm – continued

- Why all the song and dance about a subformula property?
- Suppose we guess r to be $\wedge e_0$
- Then, we have to guess a ψ such that $\varphi \wedge \psi \in S$, and the recursive call is to check if $\Gamma \vdash \varphi \wedge \psi$
- Could be an enlarged LHS if r guessed to be $\vee e$
- If we "mark" formulas and contexts for which we have proofs, then only polynomially many recursive calls are made to check if $\Gamma \vdash \varphi$
- One gets a PSPACE algorithm
- Theorem provers often use smart heuristics to improve this!

About negation

- Does this strategy lift to all of $\vdash_{\mathscr{G}}$?

About negation

- Does this strategy lift to all of $\vdash_{\mathscr{G}}$?
- What if I have to apply $\neg$e to get φ?
- Have to consider $\neg\neg\varphi$ one level up. Not a subformula!
- Perhaps still doable; add $\neg\neg\varphi$ to the set of "subformulae" of φ
- What about $\neg$i? Recall that we had to carefully think about *which* expression to derive in contradictory forms.
- What tells me which such expression is the correct one?
- Not much more than intuition, it would seem!
- Negation seems to complicate life, even in the propositional fragment

More about negation

- Write $\neg\varphi$ as $\varphi \supset \bot$
- Can capture $\neg$i as follows.

$$\dfrac{\dfrac{\begin{array}{c}\vdots \\ \Gamma, \varphi \vdash \psi \supset \bot\end{array} \quad \begin{array}{c}\vdots \\ \Gamma, \varphi \vdash \psi\end{array}}{\Gamma, \varphi \vdash \bot} \supset e}{\Gamma \vdash \varphi \supset \bot} \supset i$$

- What about $\neg$e? No equivalent rule as such!

More about negation

- Write $\neg\varphi$ as $\varphi \supset \bot$
- Can capture $\neg$i as follows.

$$\dfrac{\dfrac{\dfrac{\vdots}{\Gamma, \varphi \vdash \psi \supset \bot} \quad \dfrac{\vdots}{\Gamma, \varphi \vdash \psi}}{\Gamma, \varphi \vdash \bot} \supset e}{\Gamma \vdash \varphi \supset \bot} \supset i$$

- What about $\neg$e? No equivalent rule as such! Can write the following rule to capture the effect of $\neg$e

$$\dfrac{\Gamma, \neg\varphi \vdash \bot}{\Gamma \vdash \varphi} \neg\text{new}$$

- Moves an expression from left to right, and removes a negation
- Can still normalize and get **some** notion of a “subformula” property

Can we handle $\neg$ better?

- $\neg e$ a consequence of the law of excluded middle (LEM)
- LEM: $\varphi \vee \neg\varphi$ is valid for any expression φ
- What if we threw away LEM?
- Reject classical logic; move to **intuitionistic logic**
- Introduced by Brouwer in the first decade of the 20th century
- Basic idea: every proof needs to be **constructive**
- Informally: "An expression could be True, False, or **unknown**"
- Not allowed to get a proof of $\varphi \vee \neg\varphi$ without proving φ or $\neg\varphi$

Intuitionistic logic: Propositional fragment

- Ax, and the rules for $\wedge$, $\vee$, and $\supset$ as earlier; remove rules for $\neg$
- Use the $\bot$ operator, and the following (elimination) rule

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash \varphi}\ \bot e$$

- $\neg$i can be captured using $\bot$ and $\supset$i as follows

$$\dfrac{\dfrac{\begin{matrix}\vdots\\ \Gamma, \varphi \vdash \psi \supset \bot\end{matrix} \quad \begin{matrix}\vdots\\ \Gamma, \varphi \vdash \psi\end{matrix}}{\Gamma, \varphi \vdash \bot}\ \supset e}{\Gamma \vdash \varphi \supset \bot}\ \supset i$$

- Subformula property: $\bot$ is a subformula of any φ; still a finite set!

And one more thing...

- What about normalization though?
- Do earlier rewrites suffice? Do we need to handle detours due to $\perp$?

And one more thing...

- What about normalization though?
- Do earlier rewrites suffice? Do we need to handle detours due to $\bot$?
- What about a proof of the following shape?

$$\dfrac{\dfrac{\begin{matrix}\vdots \\ \Gamma \vdash \bot\end{matrix}}{\Gamma \vdash \alpha \land \beta}\ \bot e}{\Gamma \vdash \alpha}\ \land e_0$$

- Could have got α directly from $\bot$; unnecessarily introduced $\alpha \land \beta$
- **New normalization rule**: No rule follows an application of $\bot e$
- Any normal proof enjoys the subformula property involving $\bot$
- Clean proof search (that also handles negation-without-LEM)

What about FO now?

Are there unnecessary detours for $\forall$ and $\exists$ as well?

Suppose $\Gamma \vdash \varphi(y)$ for some fresh $y \notin \mathsf{vars}(\Gamma)$ via a proof π.

$$\dfrac{\dfrac{\begin{array}{c}\pi \\ \vdots \\ \Gamma \vdash \varphi(y)\end{array}}{\Gamma \vdash \forall x.\ [\varphi(x)]}\ \forall\mathsf{i}}{\Gamma \vdash \varphi(t)}\ \forall\mathsf{e} \qquad \rightsquigarrow \qquad \begin{array}{c}\pi' \\ \vdots \\ \Gamma \vdash \varphi(t)\end{array}$$

Here, π' is the proof π where every occurrence of y has been replaced by t.

Γ is unaffected since y is fresh.

What about FO now?

$$\dfrac{\dfrac{\begin{matrix}\pi_1\\ \vdots\\ \Gamma \vdash \varphi(t)\end{matrix}}{\Gamma \vdash \exists x.\ [\varphi(x)]}\ \exists\mathsf{i} \qquad \begin{matrix}\pi_2\\ \vdots\\ \Gamma, \varphi(z) \vdash \psi\end{matrix}}{\Gamma \vdash \psi}\ \exists\mathsf{e} \quad \rightsquigarrow \quad \dfrac{\begin{matrix}\pi_1\\ \vdots\\ \Gamma \vdash \varphi(t)\end{matrix} \qquad \begin{matrix}\pi_2'\\ \vdots\\ \Gamma, \varphi(t) \vdash \psi\end{matrix}}{\Gamma \vdash \psi}\ \text{Cut}$$

Here, π_2' is the proof π_2 where every occurrence of z has been replaced by t. The proof is unaffected since $z \notin \mathsf{vars}(\Gamma \cup \{\psi\})$, so replacing it by t (which might or might not appear in Γ or ψ) makes no difference to the overall structure of the proof.

What about FO now?

- Subformula property has to be modified
- Every $\varphi(t)$ a subformula of $\exists x.\ [\varphi(x)]$ (introduction rule)
- Every $\varphi(y)$ a subformula of $\forall x.\ [\varphi(x)]$
- Can remove detours; but the set of subformulae is now infinite!
- Unfortunately, no getting around this in the general case
- Proof search is not decidable
- But depending on the application, one might be able to restrict the shapes of these rules to get decidability
- A security application, for example, might only existentially quantify terms that a principal can generate – not arbitrary ones.