$\{p\}$ $\qquad\qquad$ $\{p, \neg r\}$

$\{\neg p\}$ $\qquad\qquad$ $\{\neg p\}$

$\square$ $\qquad\qquad$ $\{\neg r\}$

Combining the righthand proofs (in C) and resolving $\{r\}, \{\neg r\} \to \square$ gives a refutation of C!

Hilbert style formal proofs:

- can view resolution as a method of proof
- ie. a method for showing (given S, A) that $S \models A$

- point is: $S \models A$ iff there is $S_0 = \{A_1, \ldots, A_n\}$ s.t. $S_0 \models A$ (compactness v2)

  iff $A_1 \wedge \ldots \wedge A_n \models A$

  iff $A_1 \wedge \ldots \wedge A_n \wedge \neg A$ is unsat'able

  iff A^* is unsat'able

  in cnf and sat'able iff $A_1 \wedge \ldots \wedge A_n \wedge \neg A$ is (HW4)

  iff there is a refutation of A^* using resolution (last time)

- method only applies to cnf fmlas
- one "deduction rule": resolution.

- today: "Hilbert style proofs"
- apply to wffs that only use $\Rightarrow$ and $\neg$
- closer to our usual conception of deduction ("if A and $A \Rightarrow B$, then B")
- now allowed to invoke certain axioms in our proofs.

Conventions

- we now assume all wffs use only $\Rightarrow, \neg$ as connectives
- view $(A \wedge B)$, $(A \vee B)$, $(A \Leftrightarrow B)$ as abbreviations

  $(A \wedge B)$ for $\neg(A \Rightarrow \neg B)$ ← $\neg(\neg A \vee \neg B)$
  $A \wedge B$

  $(A \vee B)$ for $(\neg A \Rightarrow B)$

  $(A \Leftrightarrow B)$ for $\neg((A \Rightarrow B) \Rightarrow \neg(B \Rightarrow A))$

- we describe a proof system for such wffs
- consists of ① axioms and a ② deduction rule

① An axiom (or logical axiom) is any wff of one of the three forms:

(i) $A \Rightarrow (B \Rightarrow A)$

(ii) $(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$

(iii) $((\neg B \Rightarrow \neg A) \Rightarrow ((\neg B \Rightarrow A) \Rightarrow B))$

A, B, C are arbitrary wffs, so have ∞ many axioms.

- can check: these are tautologies
- their significance as axioms is obscure but we'll see: allows us to prove the Completeness Theorem, which is key point

- whereas resolution gave us a way of proving a given A is a tautology (iff $\neg A$ unsatisfiable iff $\neg A$ resolves to $\square$)
... having axioms in our system will allow us to generate (proofs of) all tautologies

② our deduction rule is "modus ponens" (MP): says "From A and $A \Rightarrow B$, deduce B"

- write

$$\frac{A, \quad A \Rightarrow B}{B}$$

- or in tree form

$$\begin{tikzcd}[column sep=small] & B \arrow[dl, dash] \arrow[dr, dash] & \\ A & & A \Rightarrow B \end{tikzcd}$$

Def'n Sps S is a set of wffs (using only $\neg, \Rightarrow$). A formal proof from S is a finite sequence:

$$A_1, A_2, \ldots, A_n$$

of wffs s.t. each A_i is either
(i) an axiom, or
(ii) in S or
(iii) deduced by MP from A_j, A_k for some $j, k < i$
(i.e. A_k is $A_j \Rightarrow A_i$)

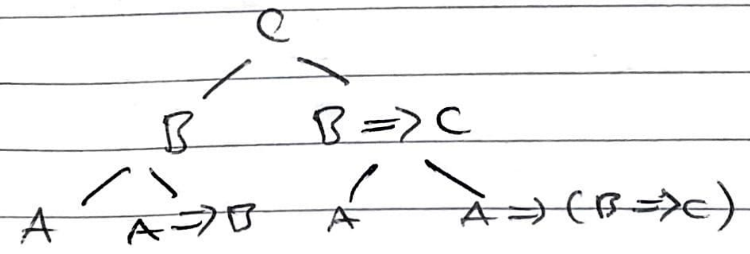
Also call this a <u>formal</u> <u>proof</u> <u>of A_n</u> (from S)

<u>Def'n</u> We write $S \vdash A$ if there is a formal proof of A from S
Write $\vdash A$ if $\emptyset \vdash A$.

<u>Ex</u> Let $S = \{(A \Rightarrow B), A \Rightarrow (B \Rightarrow C), A\}$
The following formal proof shows $S \vdash C$:

1. $A \Rightarrow (B \Rightarrow C)$ (in S)
2. A (in S)
3. $B \Rightarrow C$ (MP from 1, 2)
4. $A \Rightarrow B$ (in S)
5. B (MP from 2, 4)
6. C (MP from 3, 5)

<u>Pic:</u>



– didn't need axioms for this proof!

<u>Ex</u>: following pf shows $\vdash A \Rightarrow A$

1. $\left(\underbrace{A}_{A} \Rightarrow \left(\underbrace{(A \Rightarrow A)}_{B} \Rightarrow \underbrace{A}_{C}\right)\right) \Rightarrow \left(\left(A \Rightarrow \underbrace{(A \Rightarrow A)}_{B}\right) \Rightarrow \underbrace{(A \Rightarrow A)}_{C}\right)$ Ax. (ii)
2. $A \Rightarrow \left(\underbrace{(A \Rightarrow A)}_{B} \Rightarrow A\right)$ Ax. (i)
3. $(A \Rightarrow (A \Rightarrow A)) \Rightarrow (A \Rightarrow A)$ MP 1,2
4. $A \Rightarrow (A \Rightarrow A)$ Ax. (i)
5. $A \Rightarrow A$ ✓ MP 3,4

<u>Some observations</u>

(i) if $S \vdash A$ and $T \supseteq S$ then $T \vdash A$ (any S proof is also a T proof)

(ii) if $S \vdash A$, there is a finite $S_0 \subseteq S$ s.t. $S_0 \vdash A$ (look @ pf for $S \vdash A$ ... only uses finitely many wffs in S!)

(iii) if $T \vdash A$, and for every $B \in T$ we have $S \vdash B$, then $S \vdash A$ (look @ wffs B from T needed to prove A – only finitely many; ~~[illegible]~~ insert pfs of these B's from S in orig. pf to get pf of A from S)

— Main fact about our proof system is that it is <u>complete</u>

<u>Theorem</u> (Completeness theorem for propositional logic)
For any set of wffs S and any wff A we have
$S \models A$ iff $S \vdash A$

(says: "holding under any valuation $v \models S$" (semantic notion) equiv to "provable from S" (syntactic notion – proofs are just sequences of deductions! purely syntactic formally))

ez direction — $S \vdash A \Rightarrow S \models A$ is called "soundness"
$S \models A \Rightarrow S \vdash A$ is called "completeness"

hard direction — we split pf up into these directions.

<u>Soundness</u>. Sps $S \vdash A$. Then $S \models A$

<u>Pf</u>. Let $A_1, \dots, A_n = A$ be a proof of A from S

<u>Claim</u>: $S \models A_i$ for every $i \leq n$
↳ done if we can prove, since then
$S \models A_n = A$

pf: induction on i.

- A_1 is either in S or an axiom (can't be deduced by MP – nothing precedes it)
- if in S, clearly $S \models A_1$
- if an axiom then $\models A_1$ (all axioms are tautologies) hence $S \models A_1$ ✓

Now
- Sps $S \models \{A_1, .., A_i\}$ and consider A_{i+1}.
- if in S or an axiom, $S \models A_{i+1}$ as above
- o/w A_{i+1} deduced by MP from $A_j, A_k (= A_j \Rightarrow A_{i+1})$ for some $j, k \leq i$
- by induction $S \models A_j$ and $S \models A_j \Rightarrow A_{i+1}$
- but then clearly $S \models A_{i+1}$ by def'n of $\models$ for conditional wffs. ✓

- For the completeness direction, need some theorems about our proof system
  ("metatheorems" – i.e. theorems about proofs!)

<u>Theorem</u> (Deduction Lemma): if $S \cup \{A\} \vdash B$ then $S \vdash A \Rightarrow B$

<u>Pf</u>. Sps $A_1, .., A_n = B$ is a pf of B from $S \cup \{A\}$

<u>Claim</u> $S \vdash A \Rightarrow A_i$ for every $i \leq n$
(then done since $A_n = B$)

Pf: if not, let i be least s.t.
$S \nvdash A \Rightarrow A_i$

- several possibilities

(i) A_i is in S or an axiom

Then: A_i (axiom or in S)
$A_i \Rightarrow (A \Rightarrow A_i)$ (ax. 1)
$A \Rightarrow A_i$ (MP)
shows $S \vdash A \Rightarrow A_i$, contradiction

(ii) $A_i = A$

Then: knew $\vdash A \Rightarrow A$ (example above)
so $S \vdash A \Rightarrow A$, contradiction

(iii) A_i is deduced by MP from A_j, $A_j \Rightarrow A_i$ appearing before A_i in proof

Then: $S \vdash A_j$
and $S \vdash A_j \Rightarrow A_i$ (minimality of i)

- concatenate these two proofs

then add:

$(A \Rightarrow (A_j \Rightarrow A_i)) \Rightarrow ((A \Rightarrow A_j) \Rightarrow (A \Rightarrow A_i))$ (Ax. ii)

$((A \Rightarrow A_j) \Rightarrow (A \Rightarrow A_i))$ by MP

$A \Rightarrow A_i$ by MP

contradiction again ✓

Def'n S is <u>inconsistent</u> if for some A, we have both $S \vdash A$ and $S \vdash \neg A$
otherwise S is <u>consistent</u>

Prop'n ("Proof by contradiction") if $S \cup \{A\}$ is inconsistent, then $S \vdash \neg A$

Pf: HWS

Prop'n ("Proof by contrapositive") if $S \cup \{A\} \vdash \neg B$ then $S \cup \{B\} \vdash \neg A$
Pf: HWS

- taking these prop'ns for granted we can prove completeness theorem
- we actually prove:

Theorem: if S is consistent, then S is satisfiable

- Sps we've proved this, can prove completeness as follows:
  - Sps $S \vDash A$. WTS $S \vdash A$
  - Have $S \cup \{\neg A\}$ is unsat'able
  - by thm $S \cup \{\neg A\}$ is inconsistent
  - by proof by contradiction, $S \vdash \neg\neg A$
  - then by HWS #1, $S \vdash A$ ✓

- remains to prove theorem; will need some lemmas

<u>Def'n</u> a set of wffs $\bar{S}$ is called <u>complete</u> if for every wff A, either $A \in \bar{S}$ or $\neg A \in \bar{S}$

<u>Observe</u>: if $\bar{S}$ complete and <u>consistent</u>, must have <u>exactly</u> <u>one</u> of $A, \neg A \in S$

<u>Lemma</u> <u>If</u> S is consistent, there is a complete and consistent $\bar{S} \supseteq S$ extending S.

<u>pf</u>: as in previous proofs, we enumerate all wffs as $A_1, A_2, \ldots$
→ we recursively define a sequence of sets of wffs $S_0 \subseteq S_1 \subseteq \ldots$ as follows:

$$S_0 = S$$
$$S_{n+1} = \begin{cases} S_n \cup \{A_{n+1}\} & \text{if } S_n \cup \{A_{n+1}\} \text{ is consistent} \\ S_n \cup \{\neg A_{n+1}\} & \text{otherwise.} \end{cases}$$

<u>Claim</u> S_n is consistent for all n

→ will need:

<u>Sublemma</u>: if T is consistent and A is a w.f.f., then at least one of $T \cup \{A\}$ and $T \cup \{\neg A\}$ is consistent.

<u>Pf</u>: - Sps not: then both $T \cup \{A\}$ and $T \cup \{\neg A\}$ inconsistent

- Since $T \cup \{\neg A\}$ inconsistent, as before (using contradiction and HWS #1) have $T \vdash A$
- Since $T \cup \{A\}$ inconsistent, have $T \cup \{A\} \vdash B$ and $T \cup \{A\} \vdash \neg B$ for some B.
- But then $T \vdash B$ and $T \vdash \neg B$ (start these proofs w/ proofs of A, then copy proofs guaranteed in prev. step)
- Contradiction: we assumed T consistent ✓

<u>Pf of claim</u>: Follows immediately from sublemma ✓

- Let $\bar{S} = \bigcup_n S_n$
- Observe: $\bar{S}$ is complete: given A have $A = A_n$ for some n
  ↳ either $A \in S_n$ or $\neg A \in S_n$ by construction
- <u>Also</u>: $\bar{S}$ is consistent
  <u>why</u>: if not $\bar{S} \vdash B$ and $\bar{S} \vdash \neg B$ for some B.

- these pfs are finite, hence all wffs in them belong to S_n for some n
- but then $S_n \vdash B$ and $S_n \vdash \neg B$ contradicting consistency of S_n ✓

↳ Lemma is proved! (Found $\bar{S} \supseteq S$ complete, consistent)

- to finish proof of theorem:
  - let $\bar{S} \supseteq S$ be our consistent, complete extension guaranteed by Lemma
  - we show $\bar{S}$ is satisfiable (hence S too: $S \subseteq \bar{S}$)
  - since $\bar{S}$ complete, exactly one of $p, \neg p \in \bar{S}$ for every var. p
  ↳ define v by:

$$v(p) = 1 \quad \text{if } p \in \bar{S}$$
$$v(p) = 0 \quad \text{if } \neg p \in \bar{S}$$

<u>Claim</u> $v(A) = 1$ iff $A \in \bar{S}$

Pf: HWS

- but then $v \models \bar{S}$. Done! ✓

- we can use completeness thm. to give an alternate pf of compactness thm.

Pf: - Sps S is unsat'able
- then for any A,

$S \models A$ and $S \models \neg A$

(trivially: if $v \models S$ then $v \models A, \neg A$
... because there are no such v!)

- by completeness theorem

$S \vdash A$ and $S \vdash \neg A$

- these proofs are finite
- hence for some finite $S_0 \subseteq S$ have

$S_0 \vdash A$ and $S_0 \vdash \neg A$

- hence

$S_0 \models A$ and $S_0 \models \neg A$ (by soundness)

- but since no $v \models A, \neg A$
must have S_0 unsatisfiable!