# LECTURE 2

**De MORGAN L.:** $0, 1, \wedge, \vee, \neg$

$\boxed{\text{COMPLETE}}$

$\Updownarrow$ df.

ALL BOOLEAN FUNCTIONS

$$f : \{0,1\}^n \longrightarrow \{0,1\}$$

CAN BE DEFINED BY FLAS IN THE LANG.

# OTHER COMPLETE LANG'S:

(i) $\neg, \vee$ : $0 \equiv (x \wedge \neg x)$, $x \vee y \equiv \neg(\neg x \wedge \neg y)$

$1 \equiv (x \vee \neg x)$

(ii) $\neg, \rightarrow$ : $x \vee y \equiv \neg x \rightarrow y$

(iii) $NAND(x,y) := \neg(x \wedge y)$ $\qquad \neg x \equiv NAND(x,x)$

$x \wedge y \equiv \neg NAND(x,y)$

$\vdots$

# FREGE INFERENCE RULES

(*)

$$\frac{\alpha_1(p_1,\dots,p_n)\ ,\ \dots\dots\ ,\ \alpha_r(p_1,\dots,p_n)}{\alpha_0(p_1,\dots,p_n)}$$

r can be $= 0$

s.t.

$$\alpha_1(\bar{p}),\dots,\alpha_r(\bar{p}) \models \alpha_0(\bar{p})$$

LOGICALLY IMPLIES

$\stackrel{df.}{\Longleftrightarrow}$

ALL TRUTH ASSIGN'S SATISFYING ALL $\alpha_i$, $i=1,\dots,r$, SATISFY $\alpha_0$ TOO

## INSTANCE OF THE RULE.

$$\frac{\alpha_1(\psi_1,\ldots,\psi_m), \quad \ldots \quad , \alpha_n(\psi_1,\ldots,\psi_m)}{\alpha_0(\psi_1,\ldots,\psi_m)}$$

where $\psi_1,\ldots,\psi_m$ are $\boxed{\text{ARBITRARY}}$ FLAS.

WE SAY THAT $\alpha_0(\bar{\psi})$ **FOLLOWS** FROM $\alpha_i(\bar{\psi})$, $i \geq 1$.

A FREGE PROOF SYSTEM ($\approx$ HILBERT-STYLE CALCULUS)

A FINITE COLLECTION $F$ of FREGE RULES

IN A COMPLETE LANG. S.T.:

"$F$ IS IMPLICATIONALLY COMPLETE"

$\Updownarrow$ df.

WHENEVER A FLA $\varphi$ LOGICALLY FOLLOWS

FROM A SET OF FLAS $\Gamma$, $\Gamma \models \varphi$

THEN

"THERE IS AN $\underbrace{F\text{-PROOF}}$ OF $\varphi$ FROM $\Gamma$"

$\Downarrow$

# AN F-PROOF OF $\varphi$ FROM $\Gamma$:

$$\theta_1, \dots, \theta_k$$

S.T.:

(1) EACH $\theta_i$ IS: EITHER $\theta_i \in \Gamma$

OR: $\theta_i$ FOLLOWS BY AN F-RULE FROM

$\boxed{\text{EARLIER}}$ $\theta_{j_1}, \dots, \theta_{j_n}$, $\boxed{j_1, \dots, j_n < i}$

(2) $\theta_k = \varphi$

NOTATION: $\Gamma \vdash_F \varphi$ OR $\vdash_F \varphi$ IF $\Gamma = \emptyset$.

## EXAMPLES

(A) DeMORGAN L., ALL RULES SIMULATING "ALG. PROPERTIES"

LIKE ASSOC.: OR COMM.:

$$\frac{\alpha \vee (\beta \vee \gamma)}{(\alpha \vee \beta) \vee \gamma} \qquad \frac{\alpha \vee \beta}{\beta \vee \alpha}$$

OR DeMORGAN RULES:

$$\frac{\neg(\alpha \wedge \beta)}{\neg\alpha \vee \neg\beta} \qquad \frac{\neg(\alpha \vee \beta)}{\neg\alpha \vee \neg\beta}$$

INCLUDE ENOUGH OF THEM TO ABLE TO TRANSFORM EACH FLA INTO CNF .....

(B) $L: \neg, \rightarrow$

AX's: $p \rightarrow (q \rightarrow p)$

$$[p \rightarrow (q \rightarrow r)] \rightarrow [(p \rightarrow q) \rightarrow (p \rightarrow r)]$$

$$(\neg p \rightarrow \neg q) \rightarrow [(\neg p \rightarrow q) \rightarrow p]$$

RULE: MODUS PONENS

$$\frac{p \quad p \rightarrow q}{q}$$

[p.41]

RECKHOW'S THM (informally)

PROOFS IN ONE FREGE SYSTEM CAN BE TRANSLATED BY A P-TIME ALG. INTO PROOFS IN ANY OTHER FREGE SYSTEM, IN ANY COMPLETE LANGUAGE.

THAT IS: "FREGE SYSTEM" IS A VERY ROBUST NOTION

IDEA OF THE PROOF IF $F_1$ ($\rightarrow F_2$) HAVE SAME LANG.

general case is much harder

$F_1$-rule
$$\frac{\alpha_1(\bar{p}), \ldots, \alpha_n(\bar{p})}{\alpha_0(\bar{p})}$$

$F_2$ is IMPL. COMPL. $\Rightarrow$

$$\pi: \alpha_1(\bar{p}), \ldots, \alpha_n(\bar{p}) \vdash_{F_2} \alpha_0(\bar{p})$$

ANY USE OF THE RULE IN A $F_1$-PROOF CAN BE $\boxed{\text{"SIMULATED"}}$ BY (A SUBST. INSTANCE) OF THE $F_2$-proof $\pi$.

FOR NEXT FEW PROOF SYSTEMS WE CONSIDER ONLY PROOFS OF DNF-flas

(*) $\quad \ldots\ldots \vee (\underbrace{\ell_1 \wedge \ldots \wedge \ell_t}_{D}) \vee \ldots$

AND, IN FACT, REPLACE THE TAST TO PROVE * BY THE TASK $\boxed{\text{TO REFUTE}}$ (i.e. DERIVE $\emptyset$) FROM CLAUSES

$\ldots\ldots, \underbrace{\{\neg\ell_1, \ldots, \neg\ell_t\}}_{C}, \ldots\ldots$

C REPRESENTS

$\neg\ell_1 \vee \ldots \vee \neg\ell_t$ WHICH IS $\neg D$.

# THE SET-UP

- $\mathcal{C}$ : a set OF INITIAL CLAUSES $C_1, \ldots, C_m$
  in ATOMS $p_1, \ldots, p_n$
- A $\boxed{\text{CLAUSE}}$ $C$ IS SATISFIED $\iff$ AT LEAST ONE LITERAL IS TRUE
- $\boxed{\text{SAT}}$ $\mathcal{C}$ IS SATISFIED $\iff$ ALL $C \in \mathcal{C}$ ARE SAT.
- THE $\boxed{\text{EMPTY CLAUSE}}$ $\emptyset$ CANNOT BE SATISFIED

## $\mathcal{R}$ = RESOLUTION SYSTEM

- ALL LINES IN A PROOF ARE CLAUSES
- ONLY ONE "RESOLUTION RULE"

$$\frac{A \cup \{p\} \qquad B \cup \{\neg p\}}{A \cup B}$$

<u>OBSERVATION:</u> THE RULE IS $\boxed{\text{SOUND}}$ : ANY ASSIGN. SATISFYING BOTH HYPOTHESES SATISFIES $A \cup B$ TOO.

$\square$

# R-REFUTATIONS OF $\mathcal{C}$

$$D_1, \ldots, D_k \quad \text{(ALL CLAUSES)}$$

S.T.

- EACH $D_i$ → EITHER $\in \mathcal{C}$

  → OR DERIVED FROM SOME $D_{j_1}, j_2$, $\boxed{j_1, j_2 < i}$ BY THE R-RULE

- $D_k = \phi$ (= THE EMPTY CLAUSE).

## THEOREM

R is $\boxed{\text{SOUND}}$:

- REFUTABLE C CANNOT BE SATISFIED

AND $\boxed{\text{COMPLET}}$ :

- WHENEVER C CANNOT BE SATISFIED
  THERE IS AN R-REFUTATION OF C.

PRF: OBVIOUS BY THE SOUNDNESS OF THE R-RULE.

PRF - COMPLETENESS : BY IND ON $n$ = the nb. of ATOMS

$n=1$ THERE ARE 4 POSSIBLE CLAUSES

$$\emptyset, \quad \underbrace{\{p_1\}, \quad \{\neg p_1\}}, \quad \underbrace{\{p_1, \neg p_1\}}_{\text{irrelevant for SAT}}$$

- if $\emptyset \in \mathcal{C}$, OK

- IF $\emptyset \notin \mathcal{C}$ BUT $\mathcal{C}$ UNSAT THEN BOTH HAVE TO $\in \mathcal{C}$ : APPLY THE R-RULE

$$\frac{\{p\} \qquad \{\neg p\}}{\emptyset}$$

$n-1 \Rightarrow n$

no $p_n$

$\mathcal{C}_{00}$

ALL go to $\mathcal{C}_{n-1}$

$p_n$ yes
$\neg p_n$ no

$\mathcal{C}_{10}$

$p_n$ no
$\neg p_n$ yes

$\mathcal{C}_{01}$

both $p_n \neg p_n$

$\mathcal{C}_{11}$

irrelevant

FOR EACH PAIR

$D \cup \{p_n\}$ $\quad$ $E \cup \{\neg p_n\}$

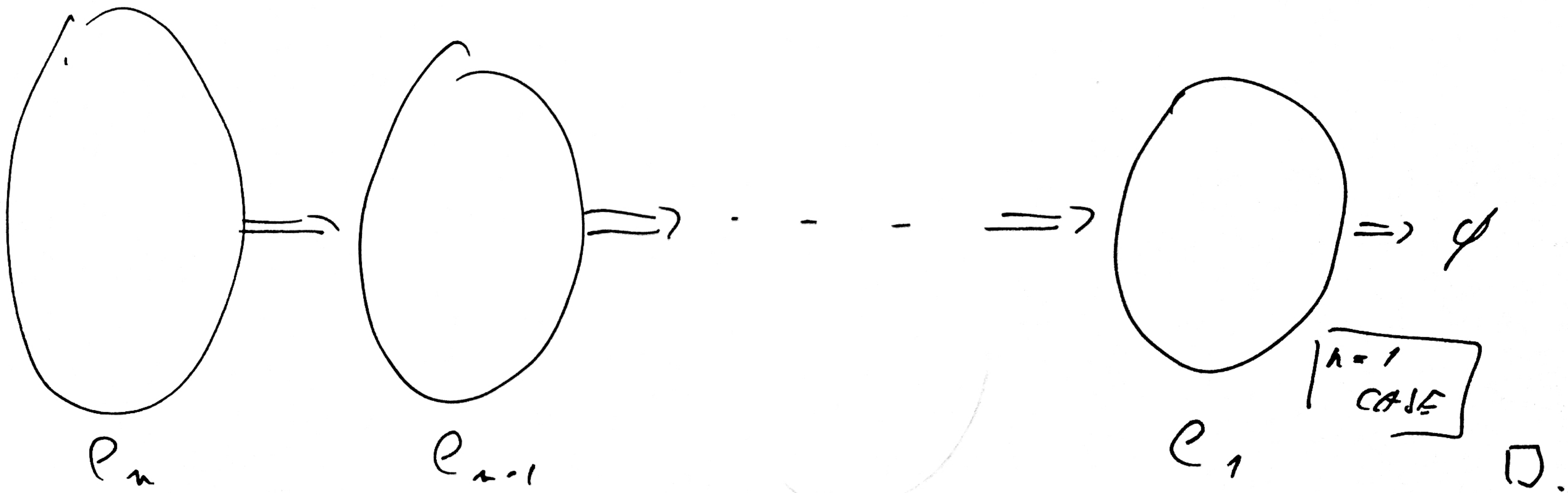
INCLUDE IN

$\mathcal{C}_{n-1}$ the CLAUSE $D \cup E$.

<u>CLAIM</u>: (i) VAR's in $\mathcal{C}_{n-1}$ ARE AMONG $p_1, \dots, p_{n-1}$

(ii) $\mathcal{C}_n$ SAT $\iff$ $\mathcal{C}_{n-1}$ SAT

(iii) ALL CLAUSES in $\mathcal{C}_{n-1}$ ARE R-DERIVABLE FROM $\mathcal{C}_n$ $\square$




$\square$.

# (LINEAR) GEOMETRIC PERSPECTIVE

- REPRES.: $x_i$ by $t_i$

  $\neg x_i$ by $1 - t_i$

- CLAUSE $\{l_1, \ldots, l_t\}$

$$\Downarrow$$

$$l_1 + \cdots + l_t \geq 1$$

INTEGER LIN. INEQUALITY

**CUTTING PLANE SYSTEM CP** : to **REFUTE** INITIAL SET OF INEQU

- LINES IN A REFUTATION:

$$a_1 x_1 + \cdots + a_n x_n \geq b$$

- all $a_i, b \in \mathbb{Z}$

ABBREV.: $\bar{a} \cdot \bar{x} \geq b$

AX'S : $x \geq 0$ , $-x \geq -1$ (repres. $x \leq 1$)

RULES :

$$\frac{\bar{a}\cdot\bar{x} \geq b \quad \bar{c}\cdot\bar{x} \geq d}{(\bar{a}+\bar{c})\cdot\bar{x} \geq b+d} \qquad \frac{\bar{a}\cdot\bar{x} \geq b}{(c\cdot\bar{a})\cdot\bar{x} \geq c\cdot b}\ ,\ c>0$$

[ADDITION] [MULTIPL.]

KEY DIVISION RULE :

$$\frac{\sum_i a_i x_i \geq b}{\sum_i \left(\frac{a_i}{c}\right)\cdot x_i \geq \left\lceil \frac{b}{c} \right\rceil}$$

ASSUMING : $c \mid a_i$ all $i$
$c > 0$

$\boxed{\text{ROUNDED UP !}}$

$\leftarrow$ CHVÁTAL-GOMORY CUT

CP-REFUTATION OF $\mathcal{L}$

$$L_1, \dots, L_k$$

S.T.

EACH $L_i$ → EITHER $\in \mathcal{L}$ (INITIAL)

→ OR IS AXIOM

OR IS DERIVED FROM EARLIER $L_{j_1}, L_{j_2}, j_1, j_2 < i$ BY A RULE

AND

$$L_k = 0 \geq 1 \; . \; \square$$

THM CP IS SOUND AND COMPLETE.

EASIER: JUST CHECK THAT ALL RULES ARE SOUND

HERE THE ROUNDING IN THE DIVISION RULE IS KEY

[Sec. 6.3]

# ALGEBRAIC APPROACH

CLAUSE $C : \{l_1, \ldots, l_t\}$

IS REPRES. BY POLYNOMIAL

$$f_C : (1 - l_1) \cdot \ldots \cdot (1 - l_t)$$

IN THE SENSE THAT

$$C \text{ true} \iff f_C = 0$$

POLYNOMIAL CALCULUS PC → LINES = POLYNOMIALS

(OVER ANY FIELD $\mathbb{F}$) "line $f$" repres. equation "$f=0$"

AX'S : $x^2 - x$ $(=0)$

RULES : $\dfrac{f \quad g}{f+g}$ $\dfrac{f}{f \cdot h}$

PC-REFUTATION OF $\mathcal{F}$ : AN INIT. SET OF POLYS

$h_1, \ldots, h_k \in \mathbb{F}[\bar{x}]$

EACH $h_i$: → EITHER $\in \mathcal{F}$

→ OR AX

→ OR DERIVED FROM EARLIER BY RULES

AND

$h_k = 1$

THM.: (OVER ANY FIELD $\mathbb{F}$)

PC IS SOUND AND COMPLETE. ∎

$\mathcal{F}$

IF $\mathcal{F}$ cannot BE SOLVED by 0-1 TLEL IT CAN BE PC-REFUTED

A PC-REFUTABLE $\mathcal{F}$ CANNOT BE SOLVED WITH $x_i \in \{0,1\}$

[EASY, AS IT WAS BEFORE]

# HILBERT'S NULLSTELLENSATZ

$\mathcal{F}$ is NOT SOLVABLE IN $\mathbb{F}^{acl}$ IFF

$\mathcal{F}$ generates THE TRIVIAL IDEAL (i.e. CONTAINING 1)

rules of PC $\Leftrightarrow$ rules generating ideals

$\neg$ all's $x^2 - x$ FORCE THAT ANY SOLUTION IS A 0-1 SOLUTION.

$\square$

A DIFFERENT EX.:

T : A FIRST-ORDER THEORY IN WHICH WE CAN DEVELOP SOME LOGIC

Ex's : ZFC : TACITLY ASSUMED IN ALL COURSES

PA (= Peano Ar.) $\approx$ finite ZFC (Ax. of $\infty$ replaced by its $\neg$)

HENCE IN $T$ WE CAN FORMALIZE A STATEMENT

"$\tau$ IS A TAUTOLOGY".

$\boxed{\text{Define}}$ PROOF SYSTEM $P_T$:

A $P_T$-proof of $\tau$ $\stackrel{\text{df.}}{=}$ a $T$-proof of "$\tau$ is a tautology".

$P_T$ ⋯→ SOUND, IF $T$ IS SOUND

→ COMPLETE: CAN DO EXH. SEARCH OVER ALL ASSIGN'S.

# NEXT TIME

- WE SHALL LOOK WHAT ALL THESE EX'S OF PROOF SYSTEMS HAVE IN COMMON
- IDENTIFY KEY DEF'S AND PROBLEMS OF THE AREA.