# LECTURE 4

**LAST TIME**: DPLL $\approx R^*$ ↘ TREE-LIKE R

**SIMILAR RELATIONS**:

→ CDCL, . . . $\approx$ R + ITS VARIANTS

→ LINEAR ALGEBRAIC ALG'S $\approx$ CP

→ SEMI-ALG. GEOMETRE ALG'S $\approx$ SOS, . . .

↑

[Sec. 6.4]

REMARKS:

A PAPER BY S. BUSS & J. NORDSTRÖM SURVES LINKS PRF-COMPL. $\leftrightarrows$ SAT SOLVING

LINK IS A THE LECTURE PAGE.

A PROOF W/LINES $L_1, \ldots, L_k$ IS $\boxed{\text{TREE-LIKE}}$ IFF EACH LINE WAS USED $\leq 1$ AS A HYPOTHESIS OF AN INFERENCE

PROOF-GRAPH: ARROWS FROM HYPOTHESES TO CONCLUSION IS A TREE; IN GENERAL IT IS ONLY DAG.

$$\boxed{P^* := \text{"tree-like } P\text{"}}$$

UNARY PREDICATE $P \subseteq [0,n]$

ASSUMPTION: $\exists x \le n \; P(x)$ (1)

WANT TO DERIVE: $\exists x \le n \, \forall y < x, \; P(x) \wedge \neg P(y)$ (2)

[ = THE LEAST NO. PRINCIPLE, LNP ]

FO-PROOF: BY IND ON $t = 0, 1, \ldots$ PROVE FROM (1) & $\neg$(2)

$$\psi(t) := \forall x \le t \; \neg P(x).$$

(i) $\psi(0)$ : BECAUSE 0 CANNOT BE MIN

(ii) $\psi(t) \to \psi(t+1)$ : $-$ ,, $t+1$

For $t = n$ this CONTRADICTS (1). $\square$

## PROPOSITIONAL VERSION:

ATOMS: $p_0, \dots, p_n$ [$p_i$ REPRESENTS $i \in P$]

ASSUMP: $A := (p_0 \vee \dots \vee p_n)$

WANT: $W := \bigvee_i (p_i \wedge \bigwedge_{0 \le j < i} \neg p_j)$

$\equiv$

WE CAN SIMULATE THE IND-PROOF.

IND-FLA $\varphi(t) \rightsquigarrow \bigwedge_{j \le t} \neg p_j$

THE IND-STEP $\varphi(t) \to \varphi(t+1)$, i.e.

$$\left(\bigwedge_{j \le t} \neg p_j\right) \to \left(\bigwedge_{j \le t+1} \neg p_j\right)$$

IS DERIVED USING TW:

$$\bigwedge_i \left(p_i \to \bigvee_{j<i} p_j\right)$$

WHICH YIELDS

$$p_{t+1} \to \left(\bigvee_{j\le t} p_j\right) \qquad . \square$$

SO WE CAN $\boxed{\text{TRANSLATE}}$ (SOME) FO - PROOFS INTO PROPOSITIONAL PROOF.

SAME EX. WRITTEN FOR $R$ AS A SET OF UNSAT CLAUSES:

$D : \{p_0, \ldots, p_n\}$

$C_i : \{\neg p_i, p_0, \ldots, p_{i-1}\}$, ONE FOR EACH $i = 0, \ldots, n$

$=$

$C_0 = \{\neg p_0\}$ : USING IT RESOLVE WITH $D$ to GET

$D' : \{p_1, \ldots, p_n\}$

AND WITH ALL $C_1, \ldots, C_n$ TO GET

$C_i' : \{\neg p_i, p_1, \ldots, p_{i-1}\}$

reduced from $[0, n]$ to $[1, n]$

REPEAT. $\square$

MODIFIED EX.: TWO PREDICATES $P_1, P_2' \subseteq [0,n)$

AND THE LNP FOR "$x \in P_1 \cap P_2'$". I.E. ATOMS

$P_i$ ARE NOW REPLACED BY THE CONJUNCTION

$$P_i \wedge P_i'.$$

THE FO-PRF AND ITS PROP. TRANS. GO THROUGH

ANALOGOUSLY BUT THE R-PROOF DOES

NOT: YOU CANNOT (λ in R) OPERATE WITH

CLAUSES FORMED BY CONJUNCTIONS.

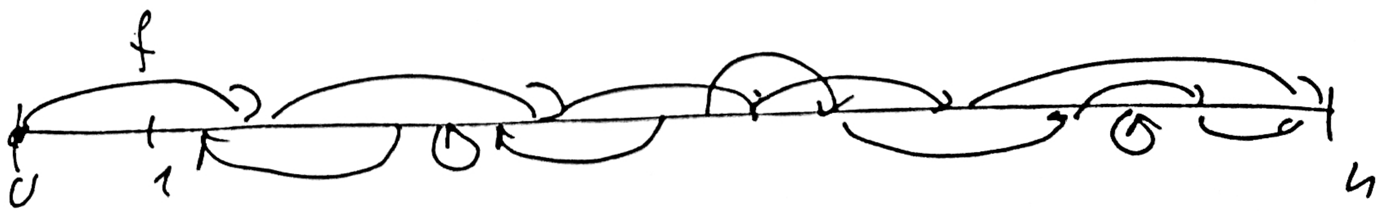
HARDER EX - EASY IND PROOF BUT NOT SO EASY TO SEE DIRECTLY PROPOSIT. ONE

$$f : [0, n] \longrightarrow [0, n]$$

ASSUMP.: $0 < f(0)$

$$\forall x < n,\ x < f(x) \longrightarrow (f(x) < f(f(x)) \lor f(x) = n).$$

WANT: $\exists x < n,\ f(x) = n.$



AN IND-PROOF, $t = 0, \dots, n-1$.

$$\Theta(t) :: \exists x \le t,\ t < f(x).$$

$\Theta(0) \iff 0 < f(0)$ [IS ASSUMP.]

$\Theta(t) \to \Theta(t+1)$ : EASY

FOR $\Theta(n-1)$ : $\exists x < n;\ f(x) = n$. $\square$

PROP. ATOMS $p_i$ OR $r_{ij}$. EXPRESS $i \in R$ OR $(i,j) \in R$

BUT THEY CANNOT EXPRESS $f(i)$

$$\Downarrow$$

NEED TO FORMULATE STATEMENTS IN

A RELATIONAL LANG. W/ CONSTANTS

$$\Downarrow$$

A FUNCTION $f : [0,n] \to [0,n]$

IS REPRESENTED BY ITS GRAPH

$$R \subseteq [0,n] \times [0,n].$$

# RE-WRITTING THE PRINCIPLE USING R

**Hypoth:**

$$\left\{\begin{array}{l} \neg R(0,0) \\ \forall x \le n\ \exists y \le n\ R(x,y) \\ \forall x \le n\ \forall y \ne y' \le n\ (\neg R(x,y) \vee \neg R(x,y')) \end{array}\right\} \text{R IS A GRAPH OF A FUNC.}$$

$0 < f(0)$

$$\forall x < n\ \forall y \le n,\ (R(x,y) \wedge x < y) \rightarrow$$

$$(\exists z \le n,\ R(y,z) \wedge y < z)$$

$x < f(x)$ $\qquad$ $f(x) < ff(x)$.

**WANT:** $\exists x < n\ R(x,n)$.

[THIS LOOKS RATHER COMPLICATED TO TREAT PROPOSITIONALLY]

# A GENERAL METHOD : PROPOSITIONAL TRANSLATIONS

FO - FLAS :

LANG. : $0, 1, +, \cdot, \leq, <$ + symbol $R(x,y)$

AX'S : A FINITE NUMBER OF AXIOMS ABOUT & WE SHALL CALL IT $\boxed{\text{BASIC}}$

IND-SCHEME :

$$\neg A(0) \vee [\exists y < x,\ A(y) \wedge \neg A(y+1)] \vee A(x)$$

FOR ~~A~~ FLAS ONLY
$\Delta_0(R)$

$\Downarrow$

## $\Delta_0(R)$-FLAS:

FORMULAS WITH BOUNDED QUANT'S ONLY:

$$\exists y \leq t(\bar{x})\ B(\bar{x}, y)$$

$$\Delta_0(R)$$

$$\forall z \leq s(\bar{x})\ C(\bar{x}, z)$$

$$\boxed{\text{THE THEORY: } I\Delta_0(R)}$$

## THE TRANSLATION

LET $A(x_1, \dots, x_n) \in \Delta_0(R)$, $n_1, \dots, n_n \geq 0$

$$\downarrow$$

$\langle A(\bar{x}) \rangle_{n_1, \dots, n_n}$ : A PROP. FLA

<u>ATOMS</u> : $r_{ij}$, any $0 \leq i, j$

REPRESENTS "$R(i,j)$"

DEF. BY <u>IND.</u> ON LOGICAL DEPTH OF $A(\bar{x})$

$$\langle t(\bar{x}) = s(\bar{x}) \rangle_{\bar{n}} := \begin{cases} 1, & \text{if } t(\bar{n}) = s(\bar{n}) \\ 0, & \text{otherwise} \end{cases}$$

$$\langle t(\bar{x}) \leq s(\bar{x}) \rangle_{\bar{n}} := \begin{cases} 1, & \text{if } t(\bar{n}) \leq s(\bar{n}) \\ 0, & \text{otherwise} \end{cases}$$

$$\langle t(\bar{x}) < s(\bar{x}) \rangle_{\bar{n}} := \quad \ldots\ldots$$

$$\langle R(t(\bar{x}), s(\bar{x}))\rangle_{\bar{n}} := r_{i,j} \quad , \text{ where } \begin{array}{l} i = t(\bar{n}) \\ j = s(\bar{n}) \end{array}$$

$\langle \ldots \rangle_{\bar{n}}$ COMMUTES W/ $\wedge, \vee, \neg$ :

$$\langle A \wedge B\rangle_{\bar{n}} := \langle A\rangle_{\bar{n}} \wedge \langle B\rangle_{\bar{n}} \;, \quad \text{ETC.}$$

$$\langle \exists y \leq t(\bar{x})\, B(\bar{x}, y)\rangle_{\bar{n}} := \bigvee_{m \leq t(\bar{n})} \langle B(\bar{x}, y)\rangle_{\bar{n}, m}$$

$$\langle \forall \quad \ldots \ldots \rangle := \bigwedge \quad \ldots \ldots$$

LEMMA: FOR ANY $A(\bar{x}) \in \Delta_0(R)$

THERE ARE $c, d \geq 1$ S.T.

(i) $|\langle A \rangle_{n_1,\dots,n_k}| \leq (n_1 + \dots + n_k + 2)^c$

[i.e. $\langle A \rangle_{\bar{n}}$ has poly($\bar{n}$) size]

(ii) $dp(\langle A \rangle_{\bar{n}}) \leq d$

THE DEPTH: MAX NB. OF ALTERNATION OF CONNECTIVES

[Sec. 2.5]

PRF: (i) THE SIZE IS MULTIPLIED IN THE

$\exists/\forall$ - STEPS.

$\downarrow$

use: terms $t(\bar{x}) \leq \mathrm{poly}(\bar{x})$.

(ii) EACH CONNECTIVE OR QUANTIFIER ADDS

1 to THE dp. . I.e.

$$dp(\langle A \rangle_{\bar{n}}) \leq \text{logical depth}(A).$$

$\square$

## SIMULATION THM. [J. PARIS & A. WILKIE]

LET $A(\bar{x}) \in \Delta_0(R)$ AND ASSUME

$$I\Delta_0(R) \vdash A(\bar{x}).$$

THEN THERE ARE $c, d \geq 1$ S.T.

FOR ALL $\bar{n}$ :

(i) $\langle A(\bar{x}) \rangle_{\bar{n}} \in TAUT$

(ii) $\langle A(\bar{x}) \rangle_{\bar{n}}$ HAS A SIZE $\leq (n_1 + \dots + n_k + 2)^c$ FREGE PROOF IN WHICH ALL FLAS HAVE DEPTH $dp \leq d$.

$\square$

## PROOF - IDEA:

NEED TO USE

A PROOF - THEORETIC FACT: IF $I\Delta_0(R) \vdash A(\vec{x})$

THEN THERE IS SUCH A PROOF:

$$\theta_1, \ldots, \theta_k (= A)$$

IN WHICH ALL $\theta_i \in \Delta_0(R)$. $\square$

- TRANSLATE $\langle \ldots \rangle$ $\theta_1, \theta_2, \ldots$

IND-SIMULATION

$\hookrightarrow \quad \neg B(0) \lor \exists y < n\,(B(y) \land \neg B(y+1)) \lor B(x)$

$x := n$

ASSUME: WE HAVE ~~PB~~

$$\begin{cases} \langle B \rangle_0 \\ \langle B \rangle_t \to \langle B \rangle_{t+1}, \quad \text{all } 0 \le t < n \end{cases}$$

APPLY REPEATEDLY MODUS PONENS

TO DERIVE: $\langle B \rangle_1, \langle B \rangle_2, \ldots, \langle B_n \rangle$.

TOTAL SIZE: $\sim$($n$ STEPS) + (poly($n$) SIZE OF FLAS)

$\le$ poly($n$). $\square$

## A BRIEF RETURN TO SAT ALG'S

ASSUME $A$ IS A SAT ALG.

IN PARTICULAR:

$$(*) \qquad \varphi(\bar{x}) \in SAT \longrightarrow \varphi(A(\varphi)) = 1.$$

$$\left.\begin{array}{l} \text{FLA } \varphi \\ \text{RUN OF } A \text{ ON } \varphi \\ \text{TRUTH ASSIGN TO } \bar{x} \end{array}\right\} \begin{array}{l} \text{- REPRESENTED} \\ \text{BY REL'S ON} \\ [0, n] \end{array} \qquad \begin{array}{l} \cdots\; F \\ W \\ B \end{array}$$

~~EX.: $\varphi$ := a SE~~

__EX.__: $\varphi$ ... A SET OF CLAUSES IN $p_0, \dots, p_n$

$C_1, \dots, C_k$

$\updownarrow$

REPRESENT BY $F \subseteq [1, \dots, k] + [0, \dots, 2n+1]$

$\downarrow$

$p_i \in C_j \iff (j, i) \in F$

$\neg p_i \in C_j \iff (j, i+n+1) \in F$

- ASSIGN $B$ TO $p_0, \dots, p_n \iff B \subseteq [0, \dots, n]$

- $W$ .... DEPENDS ON $A$ ....

THIS ALLOWS TO WRITE (*)

AS A $D_0(F, W, B)$ - FLA.

$REF_A$ := $[\![$ $^{\#}$( IF W IS A RUN OF A ON F

& B SATISFIES F )

$\Rightarrow$ ( THE OUTPUT OF

W SATISFIES F

AS WELL.) $]\!]$

YOU QUANTIFY OVER POSITIONS (= COORDINATES)

BOUNDED BY n and THE TIDE OF W

## COROLLARY (INFORMALLY):

IF $ID_0(F, w, B) \vdash REF_A$

THEN $F \geq P_A$

IN FACT: CONST-DP $F \geq A$.

## PRF-IDEA:

- USE THE SIMUL. THM TO PROVE

"OUTPUT OF $w$ DOES NOT SATISFY $F$

$\Rightarrow$ $B$ DOES NOT SATISFY $F$"

- FOR GIVEN $F, w$ evaluate the ATOMS CORRESP. TO ~~the~~ $e, w_q$ BY 0/1 AND SHOW:

"OUTPUT OF $w$ DOES NOT SATISFY $F$" $\equiv 1$

↑

EVAL. OF TRUE SENTENCE

$\Downarrow$

- BY MODUS PONENS GET A PROOF OF:

"$\bar{x}$ DOES NOT SATISFY $\varphi$"

- FROM THIS $\Downarrow$ .... THIS IS TECHNICAL BUT ELEMENTARY AND AMOUNTS TO VERIFYING

$\neg\varphi(\bar{x})$

"if $\bar{x}$ DOES NOT SATISFY $\varphi(\bar{x})$ THEN $\neg\varphi(\bar{x})$ is A TAUTOLOGY".

$\Box$.

## SUMMARY:

- UPPER BOUNDS (= SHORT PROOFS) IS OFTEN EASIER TO CONSTRUCT BY FIRST FINDING AN FO-PROOF ($I\Delta_0(R)$) AND TRANSLATING IT
- THE RETION $I\Delta(R) \overset{?}{\rightleftarrows}$ CONST-DP $F$ CAN BE GENERALIZED TO ALL $P$ AND ALL CONSISTENT R.E. T:

$$T_P \overset{?}{\rightleftarrows} P$$

$$S \overset{?}{\rightleftarrows} Q_S$$

[SEC. 8.6]

- IF $T_P \vdash$ "SOUNDNESS OF SAT ALG. $A$"

THEN $P \geq P_A$.

$\Downarrow$

HENCE: LOWER BOUNDS FOR $S_P(n)$

$\Downarrow$

TIME-LOWER BOUNDS FOR $A$

$$time_A(n) \geq S_P(n)^{\Omega(1)}. \quad \square$$