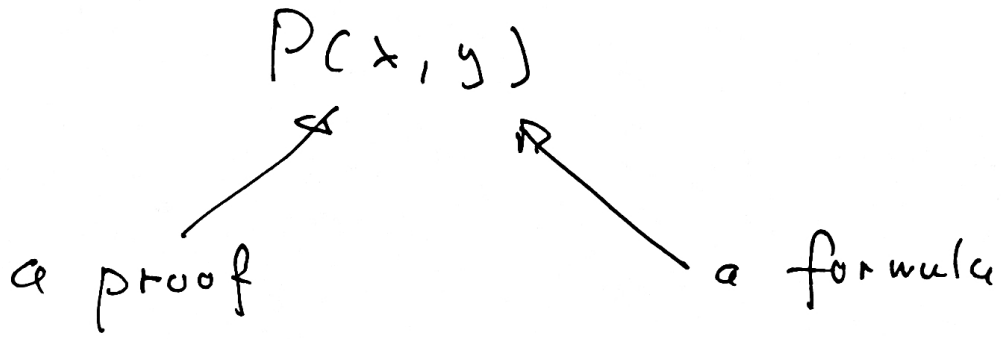
LECTURE 3

PROVABILITY PREDICATE:



Ex's: "x IS A FREGE PROOF OF y"

"x IS A PC-REFUTATION OF F,
WHERE F IS A SET OF IF-POLYNOMIALS
EXPRESSING THE CNF "$\neg y$" "

BT LIMITED EXT.

2 PROPERTIES

SOUNDNESS : $\exists \pi\ P(\pi, \tau) \Rightarrow \tau \in TAUT$

COMPLETENESS : $\tau \in TAUT \Rightarrow \exists \pi\ P(\pi, \tau)$

TOGETHER :

$$\tau \in TAUT \iff \exists \pi\ P(\pi, \tau)$$

THIS ALONE DOES NOT SAY MUCH:

Ex: DEFINE:

$P(x,y) \overset{\text{def.}}{\Longleftrightarrow} y \in \text{TAUT}$.

↑ dummy

WHAT ELSE DO THE EXAMPLES FROM LECT. 2 HAVE IN COMMON?

FEASIBILITY :

"$P(x,y)$ IS p-time DECIDABLE."

Ex.: FREGE PROOF

$\mathcal{P}$: $\Theta_1, \Theta_2, \ldots, \Theta_k$

→ NEED TO CHECK THAT Θ_i ARE FLAS,

$\Theta_k = \top$, AND THAT RULES WERE CORRECTLY

USED : $\dfrac{P \quad P \to Q}{Q}$: $\dfrac{\alpha \quad \alpha \to \beta}{\beta}$

$\mathcal{L}$: CP

$$\frac{\sum_i a_i \cdot x_i \geq b \qquad \sum_i c_i \cdot x_i \geq d}{\sum_i e_i \cdot x_i \geq f}$$

NEED TO CHECK : $\forall i$: $e_i = a_i + b$, AND $f = b + d$

$$\frac{\sum a_i \cdot x_i \geq b}{\sum a_i' \cdot x_i \geq b'} \quad c > 0$$

→ OR : $a_i' = c \cdot a_i$ and $b' = c \cdot b$

[INTEGER ARITH. is p-time]

$\underline{\mathcal{E}}$: PC OVER A FIELD IF

$$\frac{f \qquad g}{h=(f+g)}$$

NEED TO CHECK : $h = f+g$ in $IF[\pm]$

↳ IN PARTICULAR : OPERATIONS ON IF NEED TO BE P-TIME, AND IN FACT IF MUST BE REPRESENTABLE BY $SLOW^*$

⇒ IF countable

$\mathcal{E}$: IF_p , $\mathbb{Q}$, $\mathbb{Q}[\xi]$, ...

Σ_k - cont'd: Assume $IF = Q_k$.

GIVEN 3 POLYS $f, g, h \in \mathbb{Z}[x]$, CAN WE CHECK IN P-TIME IF $h = f \cdot g \in \mathbb{Z}[x]$?

→ WHAT DOES IT MEAN?

↓

NATURAL CHOICE: ANY TERMS BUILT FROM $x_1, \ldots, x_n$, elmt's of $\mathbb{Z}$, $+$ and $\cdot$.

PROBLEM: GIVEN 2 TERMS (h and $f \cdot g$), DO THEY DEFINE THE SAME POLYNOMIAL?

↑

PIT

PIT : UNKNOWN TO BE P-TIME DECIDABLE

↑

[randomized P-TIME alg. ∃]

HENCE WE INSISTS THAT POLYS ARE REPRESENTED

AS EXPLICIT $\mathbb{Q}$-linear COMBINATIONS

OF MONOMIALS :

$$\cdots\cdots + a\, x_1^{d_1} \cdots x_n^{d_n} + \cdots\cdots$$

[DENSE REPRESENTATION]

Ex: T = "theory of MATH" := ZFC

$\text{PROV}_{ZFC}(\pi, \varphi)$

π is a ZFC-proof of φ

IS P-TIME : NEED TO CHECK THAT A PURPORTED

AX IS AN INSTANCE OF ONE OF

FINITELY MANY AX-SCHEMES

~~$\exists$~~ "φ is ZFC-provable" $\in$ P-TIME

DEF. (COOK-RECKHOW)

A BINARY REL. $P(x,y)$ IS A

PROPOSITIONAL PROOF SYSTEM (a PPS)

$\Updownarrow$ def.

(i) $P(x,y) \in \mathcal{P}$

(ii) soundness : $\exists \pi\, P(\pi,\tau) \Rightarrow \tau \in TAUT$

(iii) completeness : $\tau \in TAUT \Rightarrow \exists \pi\, P(\pi,\tau)$

□

AN ALTERNATIVE - FUNCTIONAL - DEF.:

A pps is ANY p-time FUNCTION $G : \{0,1\}^* \xrightarrow[\text{ONTO}]{} TAUT.$

□

$G(w) = \tau \iff$ "w is a G-proof of τ"

- THE 2 DEF'S ARE "EQUIVALENT":

  - GIVEN G, DEFINE $P(x,y) := G(x) = y$

  - GIVEN P, DEFINE $G(w) = y$

    $\Updownarrow$

    $w = (x,y) \wedge P(x,y)$

□

THE LENGTH-OF-PROOFS FUNCTION

$$s_P(\tau) := \min\{|\pi| \mid P(\pi, \tau)\}$$

↑ MIN SIZE OF A P-PROOF OF τ

DEF.: P is **p-bounded** $\overset{\text{def.}}{\iff}$ $\exists c \geq 1 \; \forall \tau \in TAUT$

$$s_P(\tau) \leq |\tau|^c$$

(should write $(|\tau|+2)^c$)

THM [COOK-RECKHOW]

$\exists$ p-bounded pps P $\Leftrightarrow$ $NP = coNP$

$L : \{0,1\}^* \setminus L \in NP$

Proof:

TAUT CAN BE DEFINED BY

$\exists x\, (|x| \leq |y|^c)\, P(x,y)$

WHICH IS NP-DEF., I.E. TAUT $\in NP$

$\Downarrow$

BY coNP-COMPLET- OF TAUT

$NP \subseteq coNP$

$\Downarrow$

$NP = coNP$

(⇐) if NP = coNP ⇒ TAUT CAN BE DEFINED IN THE NP-FORMAT:

$$y \in TAUT = \exists x \, (|x| \le |y|^d) \; R(x,y)$$

R p-time

THEN $R(x,y)$ is a PPS, AND IT IS p-BOUNDED.

□.

COOK'S APPROACH TO P/NP

PROVE THAT NO DPS IS p-BOUNDED

$\Downarrow$ – previous thm

$NP \neq coNP$

$\Downarrow$

$P \neq NP$

HENCE THE FUNDAMENTAL PROBLEM IS:

$$NP \stackrel{?}{=} coNP$$

- THIS SEEMS HARDER THAN P≠NP BUT IT MAY HAVE A STRUCTURE (LOGIC CALCULI) THAT IS NOT IN P/NP. WELL, WE SHALL SEE.

=

- WE CANNOT HOPE TO SHOW THAT NO p-BOUNDED PPS EXISTS ONE-BY-ONE: THERE IS ∞ MANY OF THEM.

→ OR MAYBE NOT

DEF.: $P \geq Q$, P SIMULATES Q ,

$\Leftrightarrow$

$$s_P(\tau) \leq s_Q(\tau)^{O(1)} \text{ , all } \tau \in TAUT$$

IN WORDS: P-PROOFS ARE AT MOST POLY-LONGER THAN Q-PROOF.

OBSERVATION: $P \geq Q$ & Q p-BOUNDED

$\Downarrow$

P p-BOUNDED.

2nd FUNDAMENTAL PROBLEM

IS THERE A $\succeq$-RATIONAL PPS?

called "OPTIMAL"

. □

$\succeq$: A QUASI-ORDERING

$x \succeq y$ and $y \succeq x \not\Rightarrow x = y$

but often $\sim$ IT IS A PARTIAL ORDER

DEF: $P \geq_p Q$, P p-SIMULATE Q

$\Leftrightarrow$

$\exists$ p-time $f : \{0,1\}^* \longrightarrow \{0,1\}^*$ $\forall x$: $P(f(x)) = Q(x)$

[using functional def. of pps]

rel. def.. $f : (\{0,1\}^*)^2 \to \{0,1\}^*$

$\forall x, \tau$: $Q(x, \tau) \longrightarrow P(f(x, \tau), \tau)$

f = p-simulation : translates Q-PROOFS INTO P-PROOFS

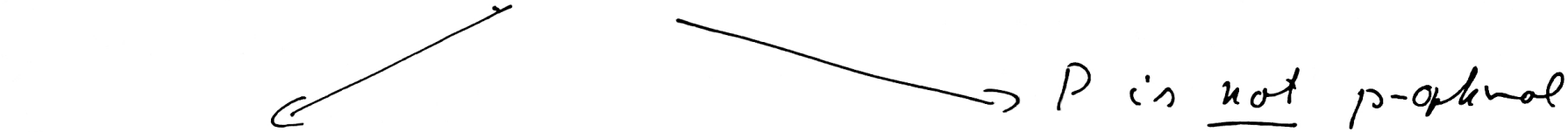
P-OPTIMALITY PROBLEM $\exists \Sigma_p$-MAX PPS ?

WHAT ARE POSSIBILITIES

CASE 1 : A p-bounded PPS P EXISTS

⇓

P is also OPTIMAL



P is p-optimal too

⋮

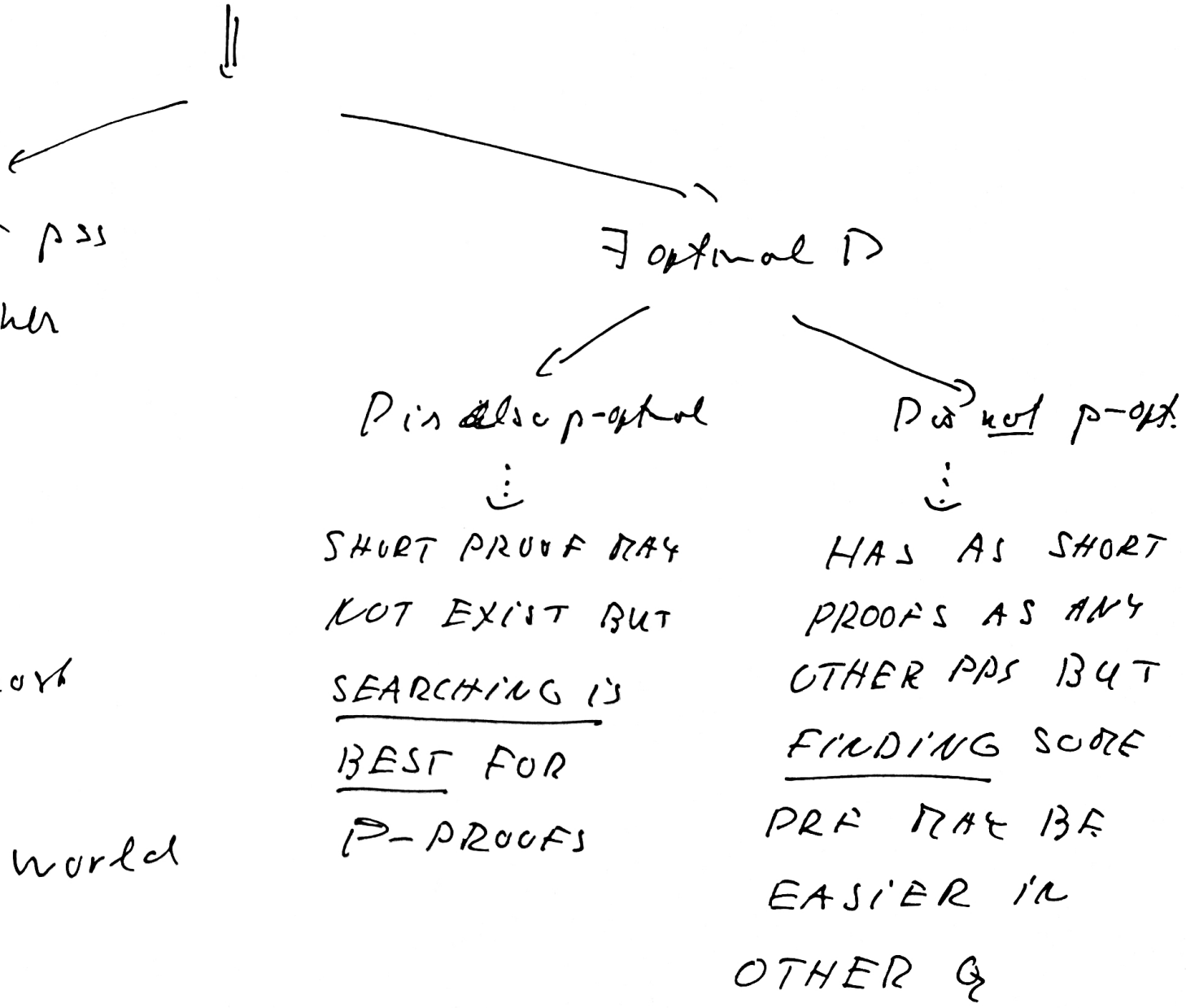
IDEAL PPS: HAVE SHORT PROOFS AND SEARCHING FOR PROOFS CAN BE DONE ONLY IN P

P is not p-optimal

⋮

IF ANY G has a SHORT PROOF OF T, so DOES P, BUT IT MAY BE EASIER TO FIND G-PROOFS THAN P-PROOFS.

Case 2 : NO p-bounded pps ∃



PRESENT SITUATION

- WE KNOW EXPONENTIAL LOWER BOUNDS FOR $S_P(\tau)$ FOR P : R (resolution), PC, CP, ...

- IT IS POSSIBLE THAT FREGE SYSTEM IS p-BOUNDED & p-OPTIMAL

A NATURAL Q: WHAT CAN WE DERIVE (AND ABOUT P/NP, IN PARTICULAR) FROM LOWER BOUNDS FOR ONE SPECIFIC P?

SAT alg.: A

→ EITHER DECISION PROBLEM:

COMPUTES χ_{SAT}

→ OR SEARCH PROBLEM:

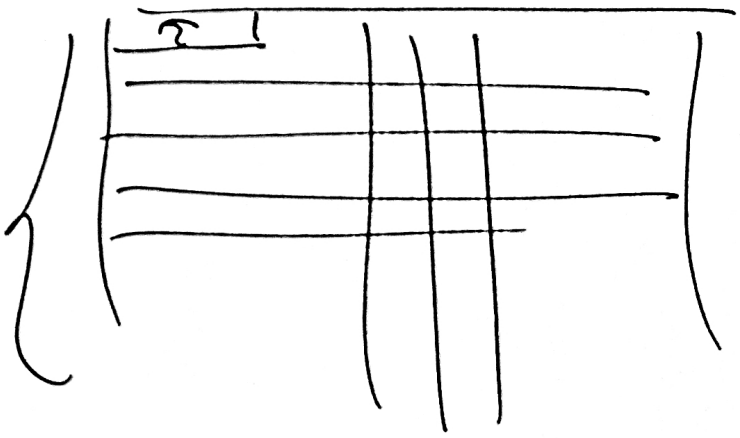
$$\varphi \in SAT \Rightarrow \varphi(\underbrace{A(\varphi)}_{\text{SATIS. ASSIGN.}}) = 1$$

SAT ALG. A AS A PPS

$P_A(\pi, \tau) \underset{df.}{\rightleftarrows}$ [π is THE TRANSCRIPT OF THE COMPUTATION OF A ON τ ENDING WITH DECLARATION "NOT SATISFIABLE"]

$|\pi| \leq O(time_A(\tau)^2)$

time



LEMMA : LET A BE A SAT ALG., Q A PPS AND ASSUME $Q \geq P_A$. THEN:

$$time_A(\tau) \geq S_Q(\tau)^{\Omega(1)} \quad \ldots \varepsilon > 0 \ldots$$

I.E.: SIZE LOWER B. FOR Q $\Rightarrow$ TIME LOWER B. FOR A

PRF.: BY THE DEF. OF $\geq$:

$$S_Q(\tau) \leq S_{P_A}(\tau)^{O(1)}$$

BY THE EARLIER OBSERVATION: $S_{P_A}(\tau) \leq O(time_A(\tau)^2)$.

□.

TO SHOW $G \geq P_A$ WE MAY

↳ USE A DIRECT TRANSFORMATION OF COMPUTATIONS INTO PROOFS

(today)

↳ OR USE A MORE GENERAL BUT LESS ELEMENTARY ~~WAY~~ WAY VIA "PROVING IN G THE SOUNDNESS OF A"

(later)

DPLL procedure (Davis, Putnam, Logemann, Loveland)

GIVEN : A SET $\mathcal{C}$ OF CLAUSES

WANT : EITHER FIND A SAT. ASSIGN. OR REJECT $\mathcal{C}$ AS UNSAT.

THE PROCEDURE : 1. SELECT ATOM p

2. GIVE p A VALUE, SAY 0

3. DELETE ALL CLAUSES CONTAINING $\neg p$ (THEY ARE SAT)

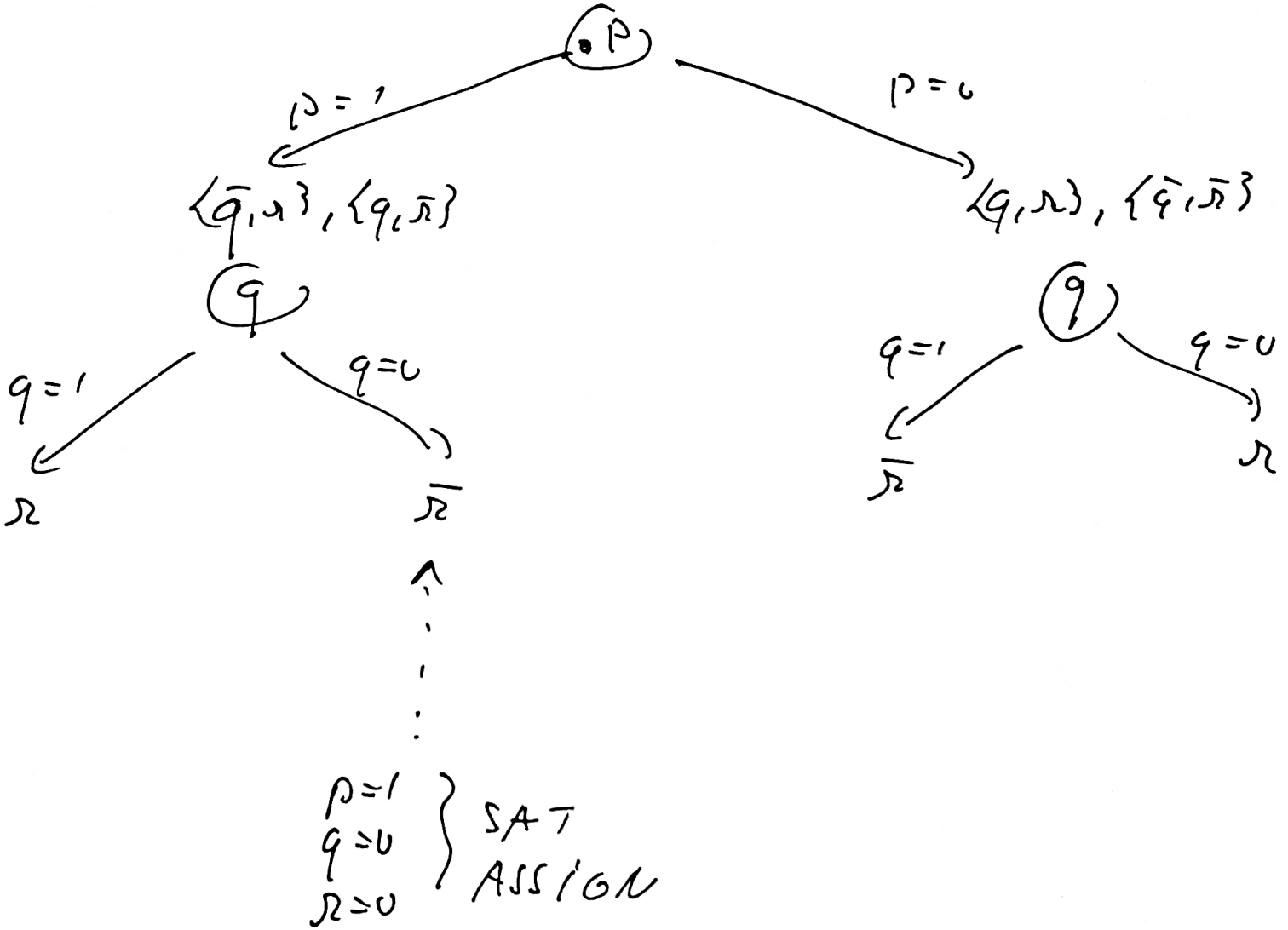
4. DELETE ALL ATOMS p (BUT NOT $\neg p$) FROM ALL CLAUSES

5. IF THE EMPTY CLAUSE WAS CREATED : BACKTRACK

6. IF ALL CLAUSES WERE DELETED : YOU HAVE A SAT. ASSIGN.

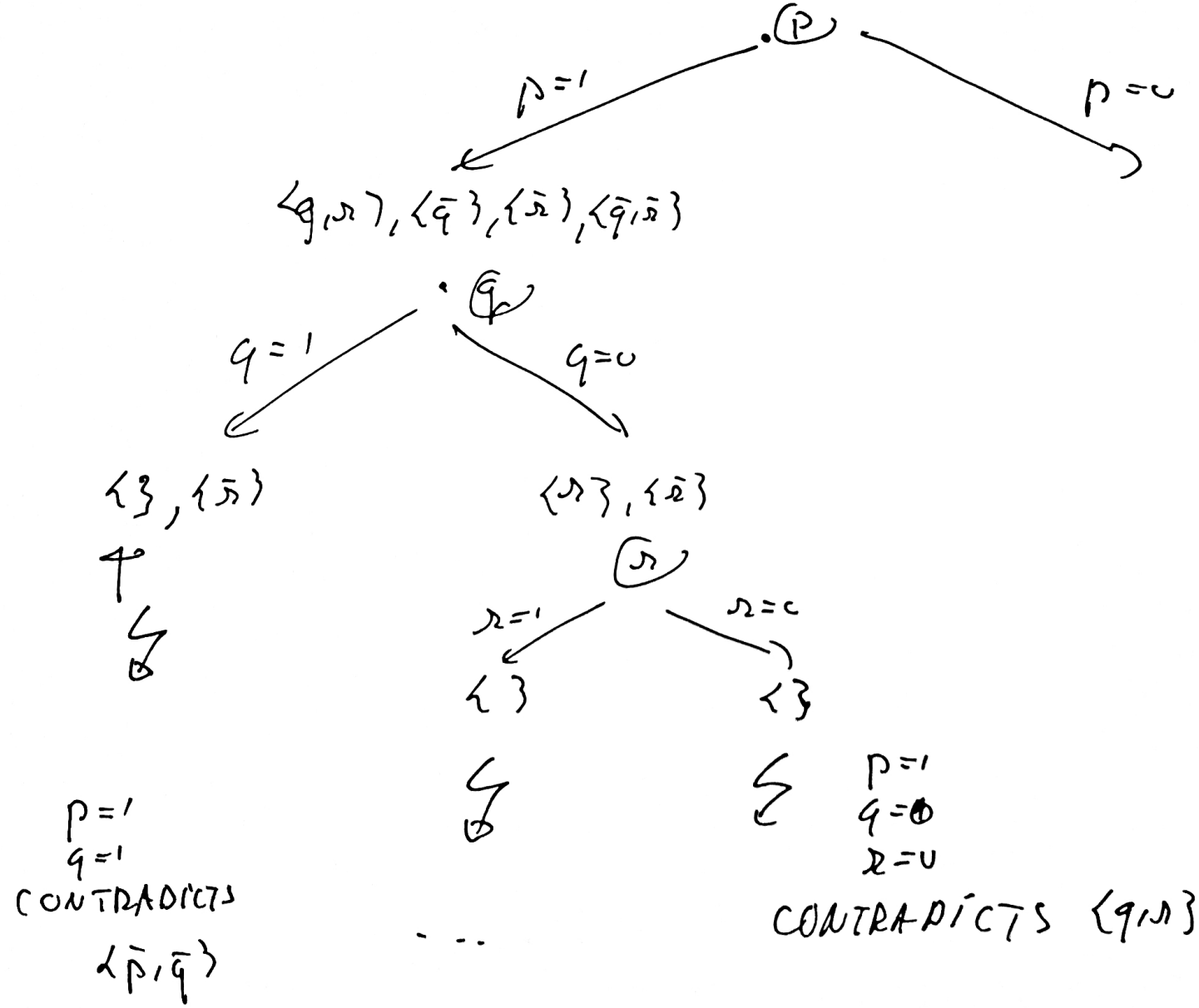
Ex.: $p \oplus q \oplus r = 1$, $\mathcal{C}: \{p,q,r\}, \{\bar{p},\bar{q},r\}, \{\bar{p},q,\bar{r}\}, \{p,\bar{q},\bar{r}\}$

Notation: $\bar{p} := \neg p$, $l^1 := l$, $l^0 := \neg l$



Ex: $p+q=1$
$p+r=1$
$q+r=1$

C: $\{p,q\}$ $\{p,r\}$ $\{q,r\}$
$\{\bar{p},\bar{q}\}$ $\{\bar{p},\bar{r}\}$ $\{\bar{q},\bar{r}\}$



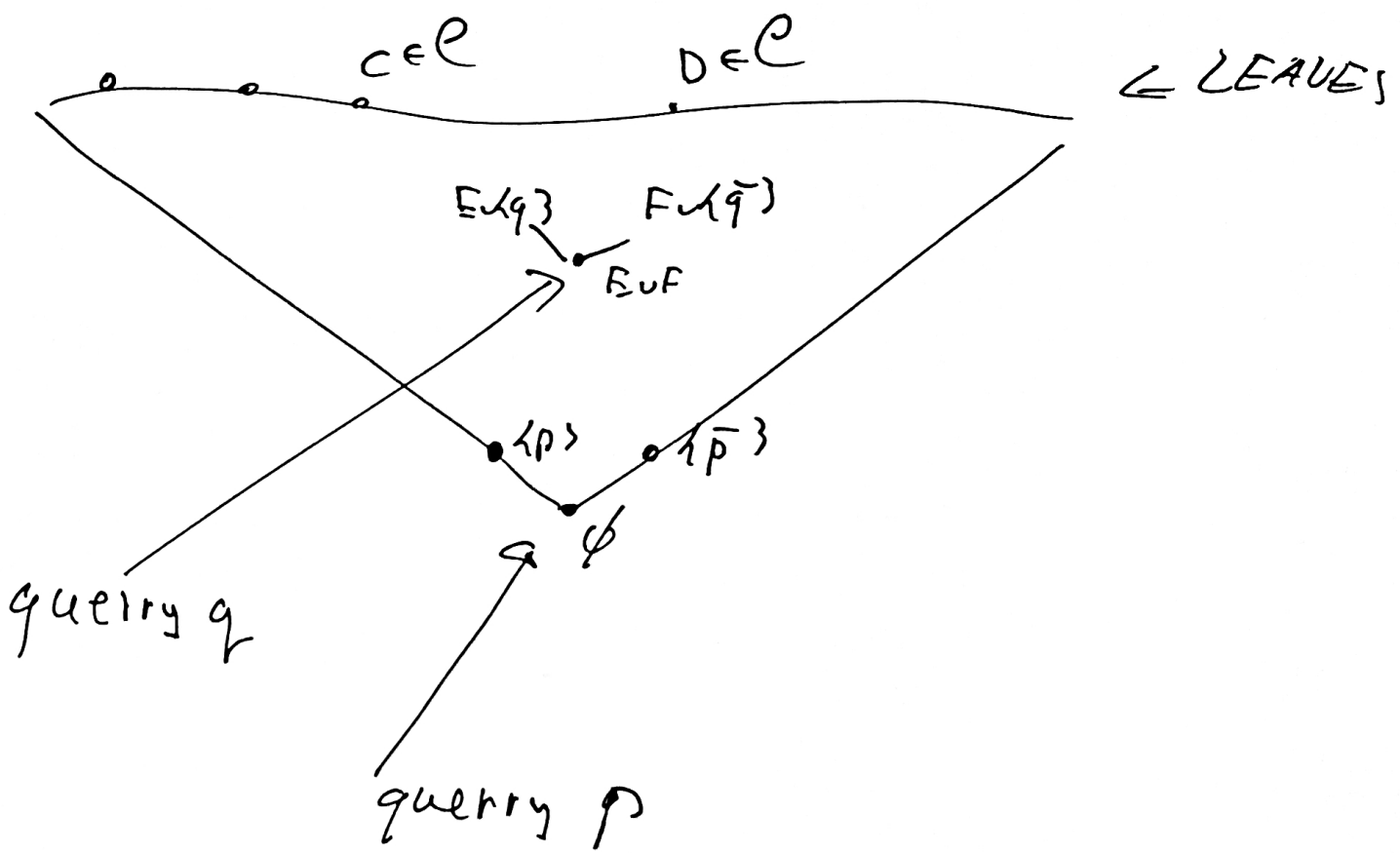
THEOREM: (1) THE TREE OF A DPLL COMPUTATION REJECTING $\mathcal{C}$ AS UNSAT CAN BE:

- TURNED UPSIDE DOWN
- LABELLED BY CLAUSES

S.T. THE RESULT IS A TREE-LIKE R-REFUT. OF $\mathcal{C}$.

(2) VICE VERSA: ANY TREE-LIKE R-REFUT. OF $\mathcal{C}$ CAN BE TURNED INTO A DPLL REFUTATION WITH THE SAME TREE.

(2) [EASIER] π



TRAVEL FROM BOTTOM ($\emptyset$) TO A LEAF VIA FALSE CLAUSES : THIS IS POSSIBLE AS R-RULE IS SOUND.

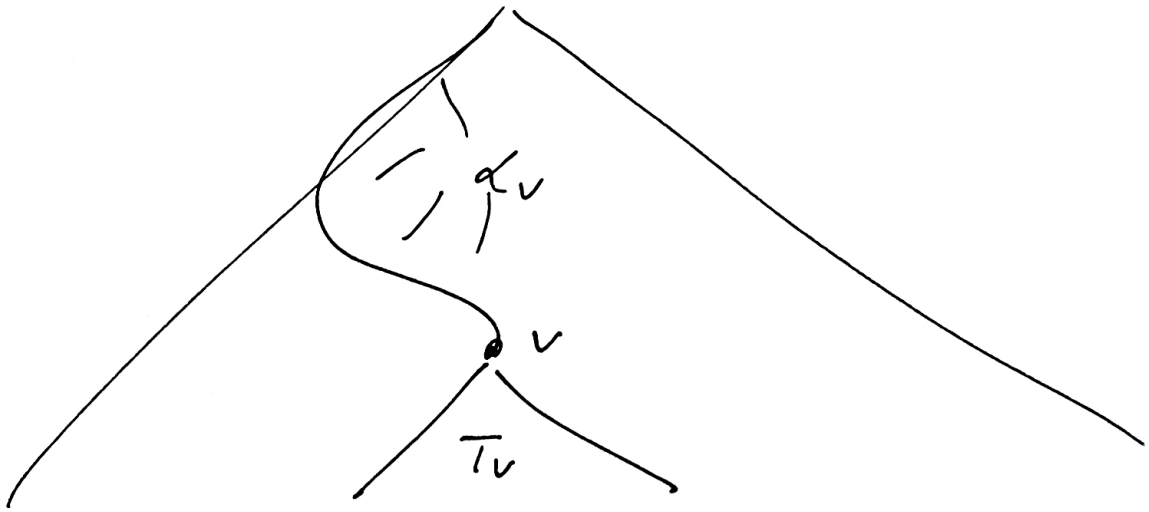
NOTATION: R^* = TREE-LIKE REFUT.

(1) v : a vertex in the TREE (= COMPUT. OF DPLL)

α_v : ~~a CONJUNCT~~ LOGICAL TERM (= CONJ.) OF ALL ATOMS p, IF $p=1$ on the PATH TO v, OR $\bar{p}$ IF $p=0$ THERE.

T_v : THE SUBTREE STARTING WITH v

(v LEAF $\Rightarrow$ T_v JUST ONE NODE)



PUT : E_v := THE CLAUSE $\neg\alpha_v$

CLAIM : THERE IS $E'_v \subseteq E_v$ AND AN R^*-DERIVATION OF E'_v FROM $\mathcal{C}$ WHOSE TREE IS T_v.

PRF : BY IND. ON THE DEPTH OF T_v.

$dp(T_v) = 0$, i.e. v IS A LEAF:

AS THE COMPUT. IS REJECTING, AN EMPTY CLAUSE WAS CREATED.

THAT IS : α_v KILLS SOME $C \in \mathcal{C}$

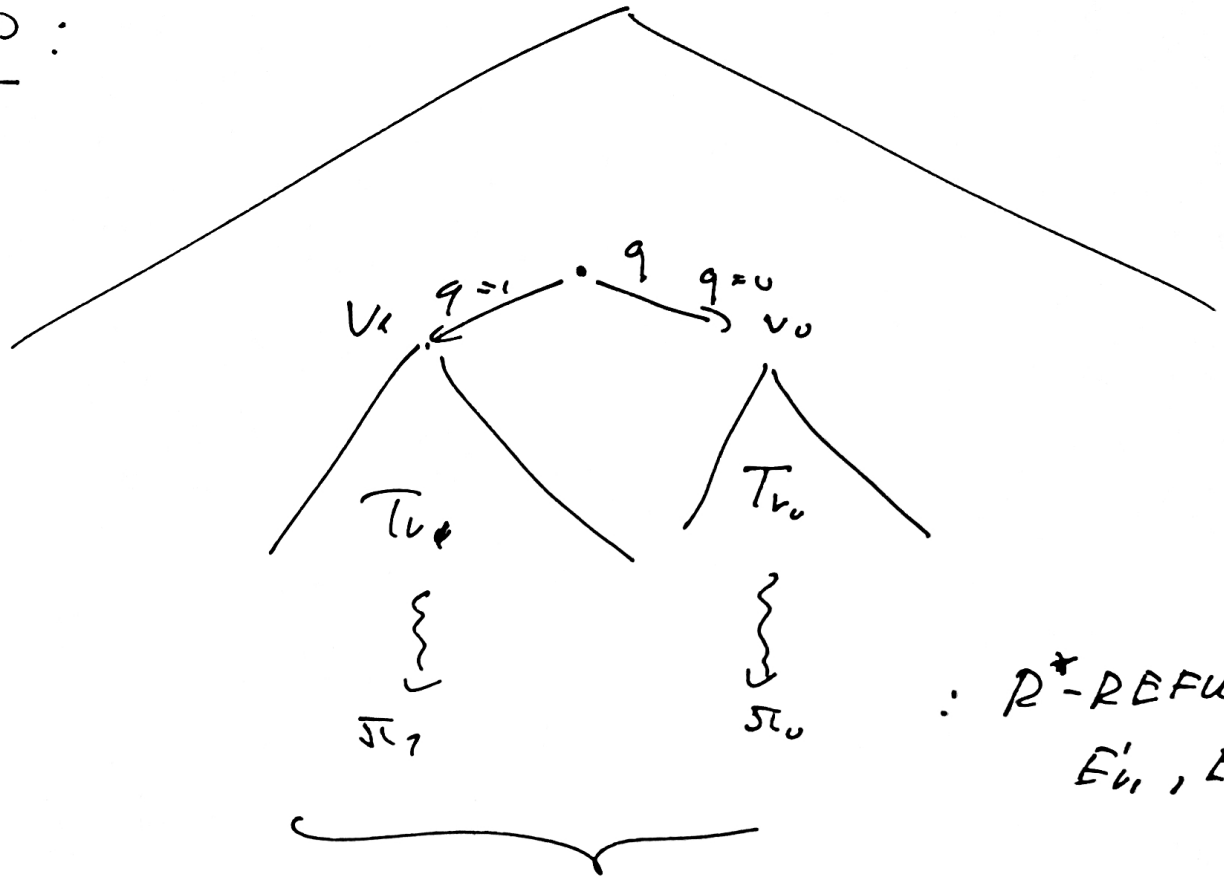
$$\Downarrow\!\!\Downarrow$$

$$C \subseteq E_v$$

$$\uparrow$$

$$=: E'_v$$

IND. STEP :



: R^*-REFUT'S OF E'_1, E'_0

JOIN THEM BY RESOLVING ON ATOM q

END OF THE PROOF

FOR $v := root$: $E_{root} = \varphi$

SO T_{root} (= THE WHOLE TREE) BECOMES

AN R^* – REFUT. OF $\mathcal{C}$

□.

REMARK : DETAILS IN [SEC. 5.2]