The NATURE of PROOF COMPLEXITY

Jan Krajíček

Charles University

- propositional proof system (pps)

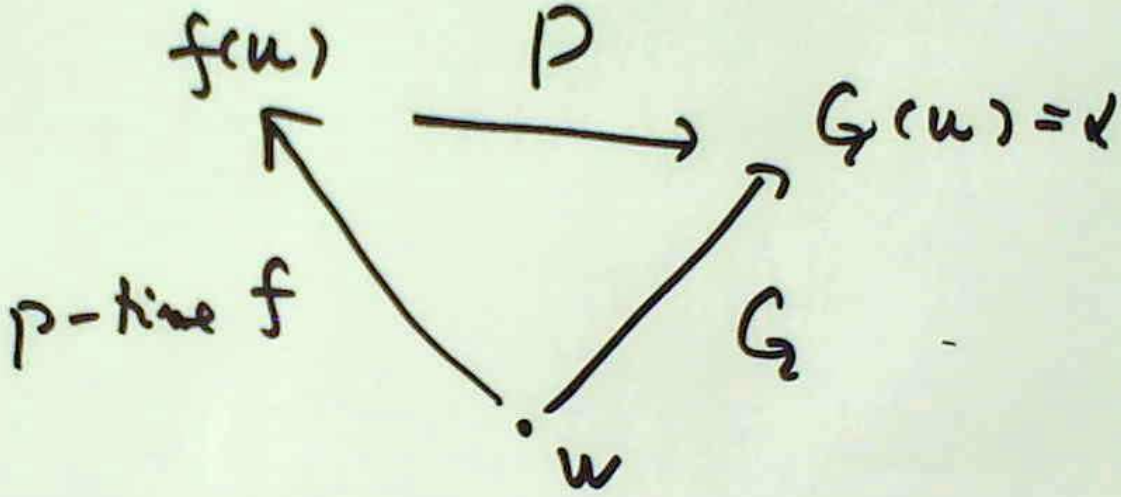
$$P : \{0,1\}^* \xrightarrow[\text{p-time}]{} TAUT$$

- $s_P(\alpha) := \min |w| \text{ s.t. } P(w) = \alpha$

- P p-bounded $\iff s_P(\alpha) \leq |\alpha|^{O(1)}$

- $P \geq G$ simulation $\Leftrightarrow$ $s_P(\alpha) \leq s_G(\alpha)$ $\quad \alpha(\tau)$

- p - simulation :



- P optimal $\Leftrightarrow$ $\geq$ - max

Fundamental problems

- (1) $NP =_? coNP$
- (2) $\exists$ optimal pps ?
- ..... (3) ... proof search ...

4 levels

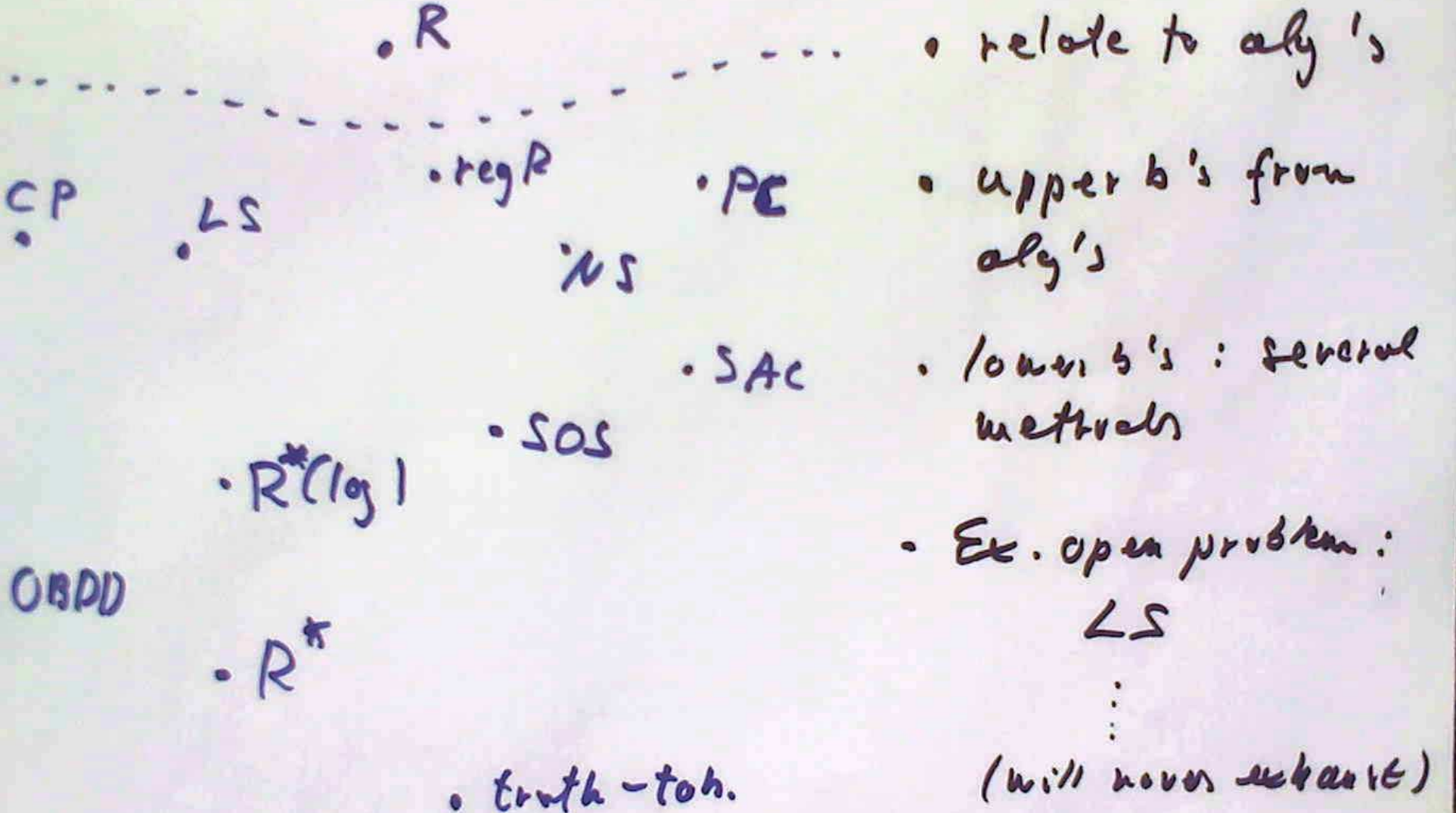
→ Mathematical

→ Logical

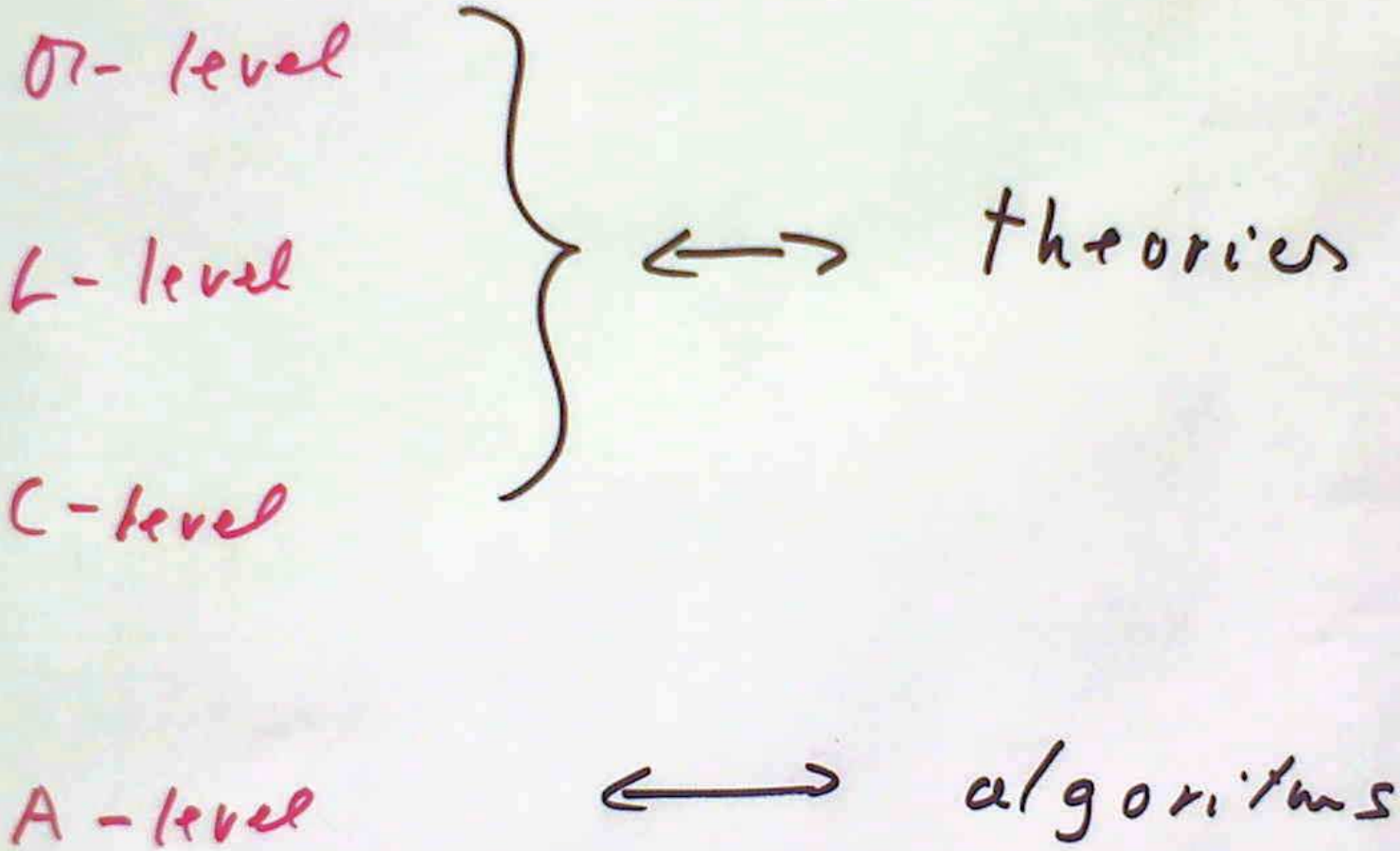
→ Combinatorial

→ Algorithmic

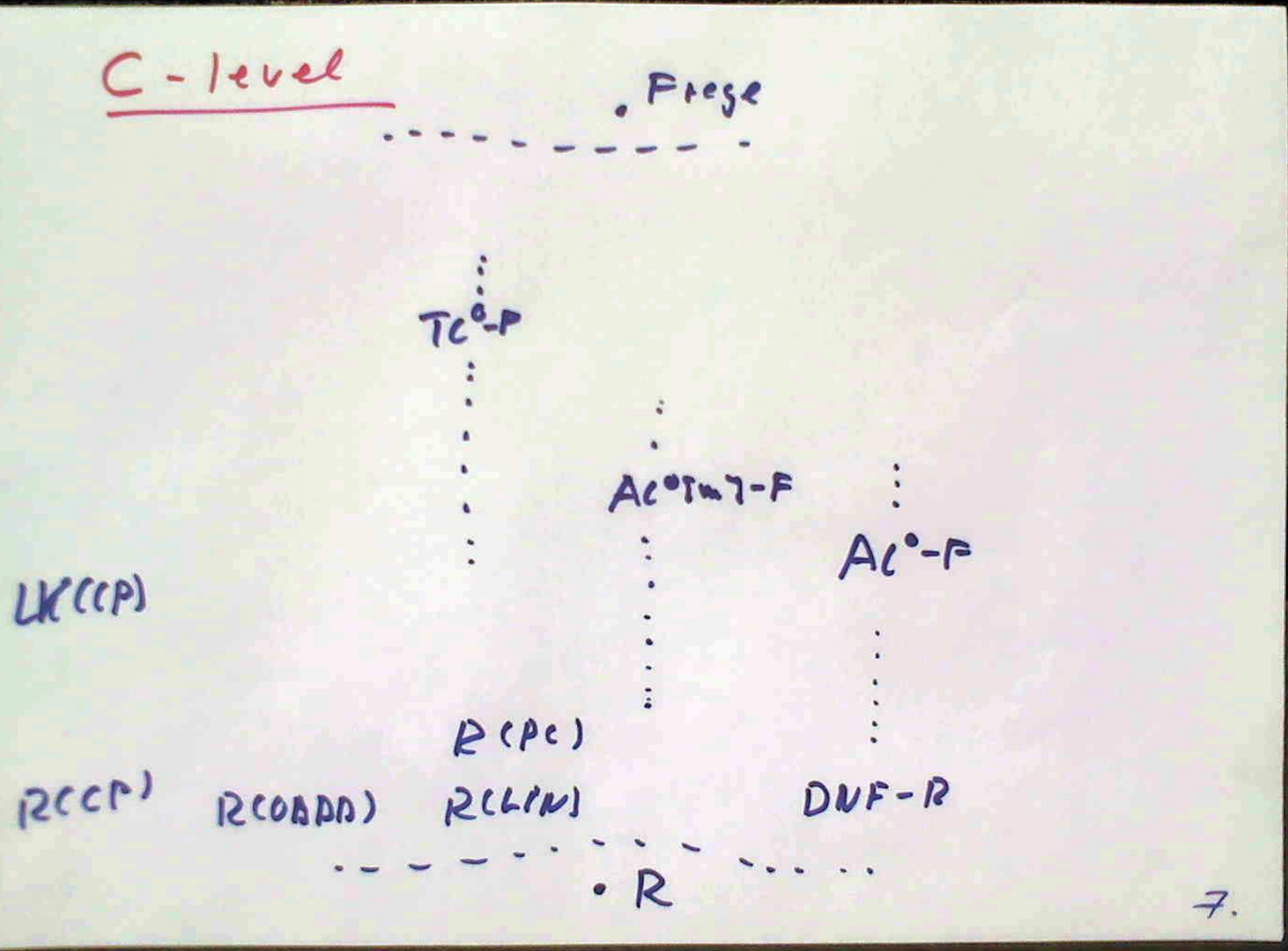
A-level


R
relate to alg's
regR
PE
upper b's from alg's
CP
LS
NS
SAC
lower b's: several methods
SOS
R*(log)
Ex. open problem:
OBDD
LS
R*
truth-tab.
(will never exhaust)

J.



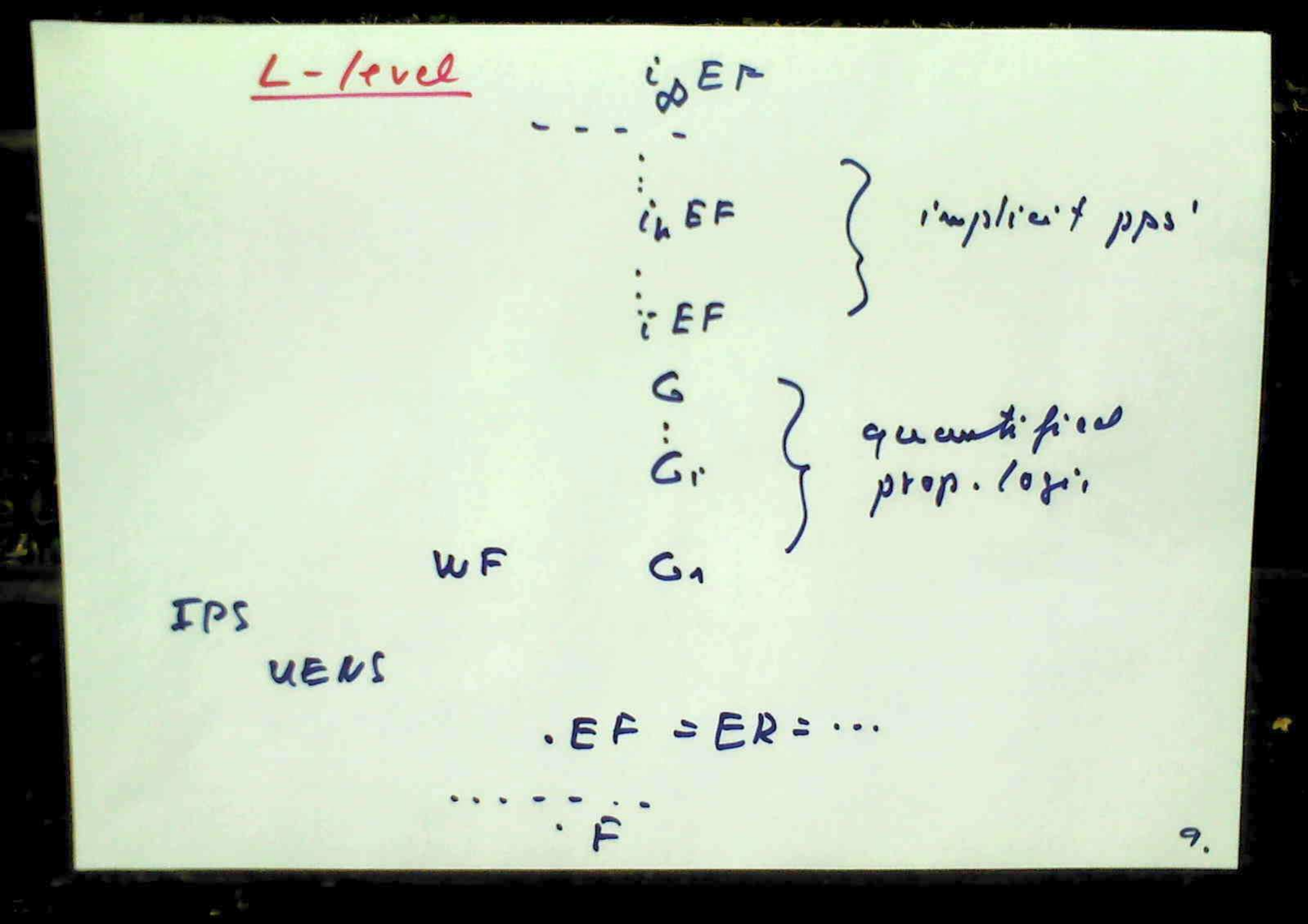
G.


C-level
Frege
TC°-F
AC°Tm7-F
AC°-F
LK(CP)
R(PC)
R(CP)
R(CONTR)
R(CUT)
DNF-R
R

C-level theories

- objects : strings
- quantify & count in various ways bit-pairs
- IND
- simple operations on strings

[bounded arithmetic]
↳ Parikh '73, Paris-Wilkie, Buss, ...


L-level
$i_\omega EF$
$i_n EF$
$i EF$
implicit ops
G
G_1
quantified prop. logic
WF
G_1
IPS
UENS
$.EF = ER = \cdots$
F

L - level theories

- objects : strings, B. fct's, functionals, ...
- quantify: over Σ^* with p-bounded size parameter n
- some IND
- p-time operations on strings
- range from PV ↑ [Cook'76] to $\exists\Delta_0\text{-}\Omega_1$, S_2, U_2^1, V_2^1, ... $\langle \exists\Delta_0 + \mathrm{Exp}$

Π-level : only theories !

GS set th.

ZFC

⋮

finite set th. = PA ... Peano arith.

⋮

PRA

⋮

• $I\Delta_0 + \Omega_1$

. . . . . .

theory T $\rightleftarrows$ pps P_T correspondence

↓

any consistent r.e. theory $\supseteq$ ... PV

- PV : names for all p-time alg's and their defining universal conditions [Cook '76, Cobham '64]

$P_{PV} = EF$

- Ex: ZFC + PV

PA ($\supseteq$ finite set theory)

propositional translation

open $\mathcal{L}_{PL}$ - fla $\varphi(x)$

↓

seq. of prop. form $\|\varphi\|^n$, $n \geq 1$

Fact: $\forall a \in \{0,1\}^n$, $\varphi(a)$ true

⇕

$\|\varphi\|^n(a) = 1$

Hence: $\forall x\, \varphi(x)$ true $\Rightarrow$ $\|\varphi\|^n \in TAUT_n$, all $n \geq 1$

key properties : $T \longrightarrow P_T$ (pps as a collection ...)

(1) $T \vdash \forall x\, \gamma(x) \Rightarrow P_T \underset{\text{poly}(n)}{\vdash\!\!\!-\!\!\!-} \|\gamma\|^m$

(The P_T-proofs are p-time constr. from γ)

(2) $T \vdash$ "P_T is sound"

$\updownarrow$ flo $\quad Ref_{P_T}$

Key corollaries

(3) $P_T \vdash_{\text{poly}(n)} \|\text{Ref}_{P_T}\|^n$

so Gödel's 2nd thm "fails" here.

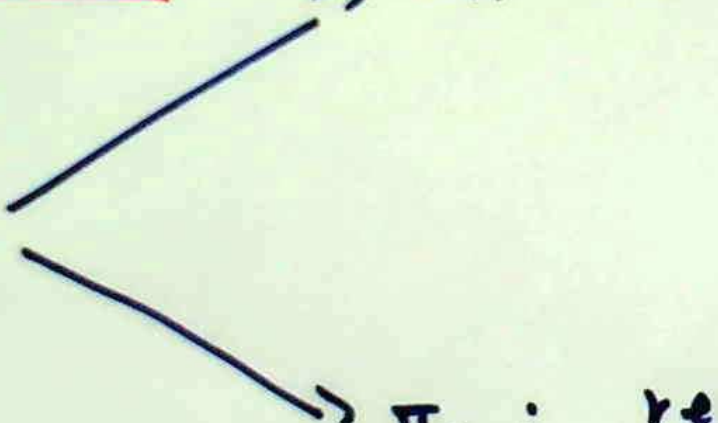
(4) $\not\vdash \text{Ref}_G \Rightarrow P_T \not\equiv_P Q$

(somewhat simplified statement)

p-time Turing mach. M ⟶ p-size circuit C_n

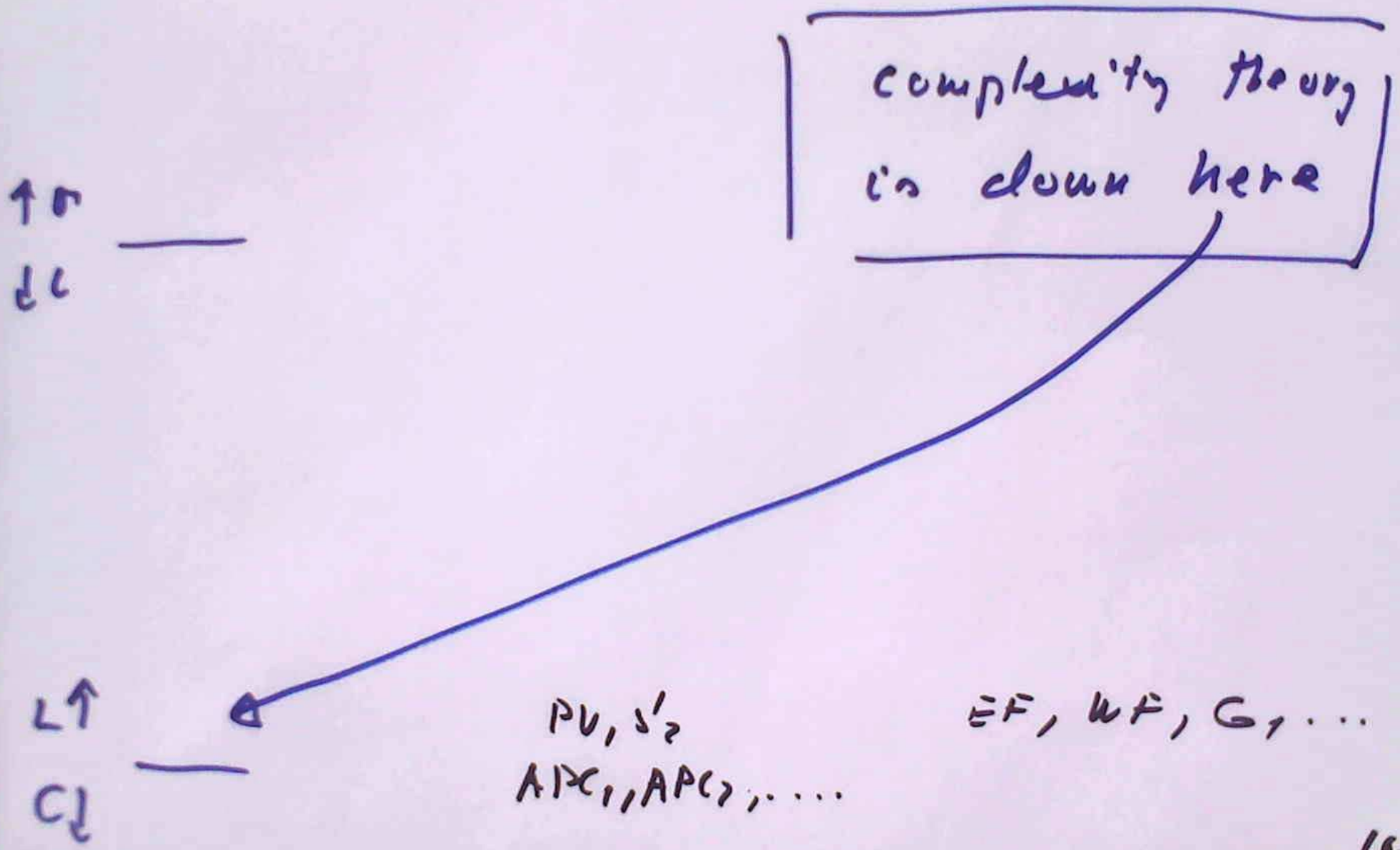
analogous: one universal T-proof yields a sequence of short prop. proofs π_n

discrepancy:



[counting args's also out]

key meta-fact



- formulization : uses standard text-book def's

- Ex's : NP-compl. problems
PCP-thm
Goldreich-Levin thm
OWF $\longrightarrow$ PRNGs constr.
derandomization via MK
natural proofs and ....
sorting networks
expander constructions
⋮

meta-math. significance

Fact: super-poly lower bounds for P_T-proofs of **any** sequence of tautologies imply that $P \neq NP$ is consistent with T:

$T \nvdash$ Sat$(\varphi, a) \longrightarrow$ Sat$(\varphi, A(\varphi))$ for any alg (p-time) A

(universal)

[counts towards the truth of $P \neq NP$]

Proof: $G := $ "check that $Sat(\alpha, A(\overline{\alpha}))$"

- A p-time $\Rightarrow$ G pp.
- if $T \vdash \ldots$ then $T \vdash Ref_G$
- $\Rightarrow P_T \geq G \Rightarrow P_T$ - bounded
- $\lightning$ with the hypothesis

□

remark : there are other consistency results for PV (and more) obtained differently

Ex's:

- $NP \not\subseteq P/poly$, assuming a weaker hypothesis [Rook-K.]

- $P \not\subseteq Size(n^c)$, unconditionally [K.-Oliveira]

.

.

.

Remark: "A does not solve SAT i.o."
can be expressed on a uniform sentence
too.

Thm yields: ~~T~~ $P \neq NP$, i.e.

T + A solves SAT is consistent,
follows from super-poly p_T-lower
bound but for specific flas.

[counts towards "barriers"]

Tasks in the fundamental problems:

(1) Given P find $\alpha_1, \alpha_2, \ldots \in TAUT$ hard for P.

(2) Given P find $Q(P)$ s.t. $P \not\equiv Q(P)$.

Fact: (2) $\Leftrightarrow$ (1) with the additional requirement that $L(\alpha_k)_k$ is p-time constructible (or in P, or in NP, or ...)

Two pitfalls:

(i) $T \vdash$ l.bound for G_φ $\Rightarrow$ $T \vdash Ref_\varphi$

$\Downarrow$

$P_T \simeq G_\varphi$

(ii) $T \vdash P_T \not\simeq G_\varphi(P_T)$

$\Rightarrow$

$T \not\vdash G_\varphi(P_T)$ is a pps

remark: the non-uniform case may be very different

(a) [Cook - K.] There is an optimal pps among "pps with advice"

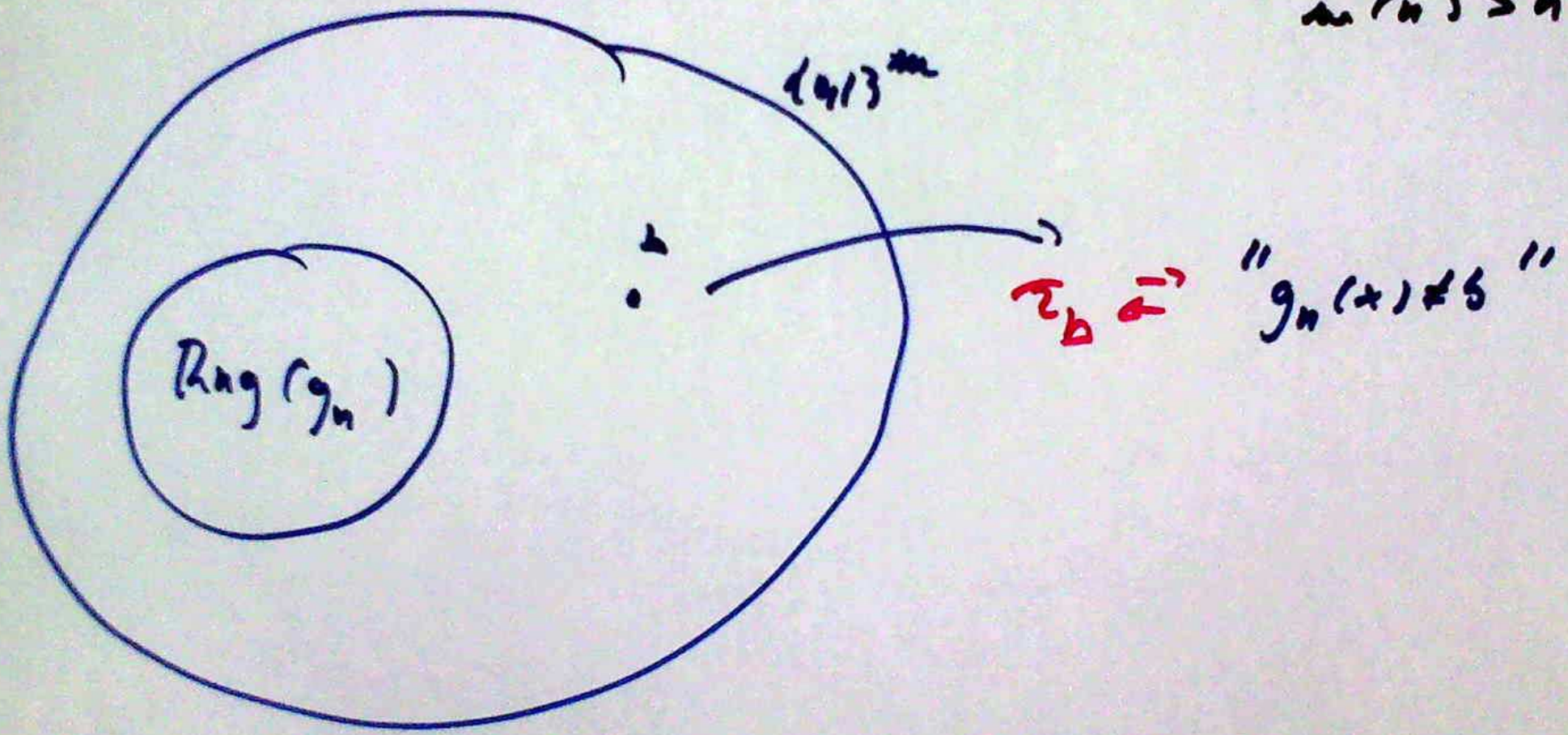
(b) Witnessing that a sequence of p-size non-det. circuits is not sound and complete pps requires exponential time.

[assuming OWP $\exists x$]

Proof complexity generators

p-time (P/poly, NP ∩ coNP/poly) $g_n : \{0,1\}^* \to \{0,1\}^{m(n)}$

$m(n) > n$



[A(BS)RW '04, K '01]

$g = \{g_n\}_n$ is hard for P $\Rightarrow$ $\forall c \geq 1$, all but finitely many x_0 need P-circuit $> |x_0|^c$

Three ex's:

(i) truth-table f: small $C \to$ hard C

(ii) variants of the NW generator

(iii) gadget generator

$\Rightarrow$ f has explicit circuit lb. bounds

Can we prove any l. bounds at the Σ- or Π- level?

Π-level: the only method in sight is diagonalization

No l. bounds but some things can be proved.

Ex Thm: One of (i)-(iii) is true:

(i) $E \notin Size(2^{n^{o(1)}})$

(ii) $NP \neq coNP$

(iii) $\exists$ p-optimal proof systems

For L-level ?

Working hypothesis : Feasible interpolation also can be extended.

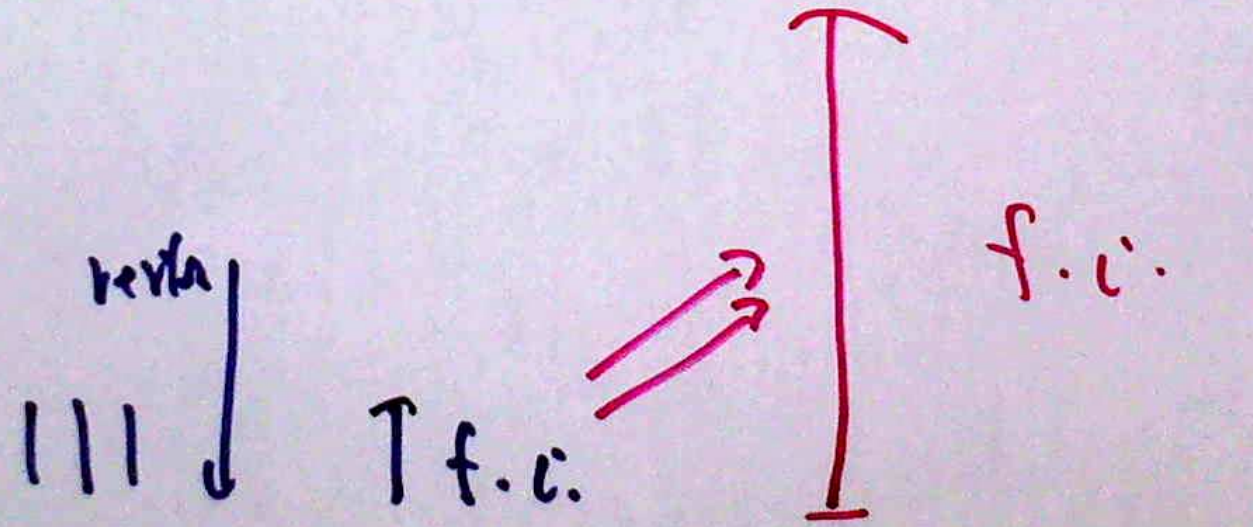
methods in:

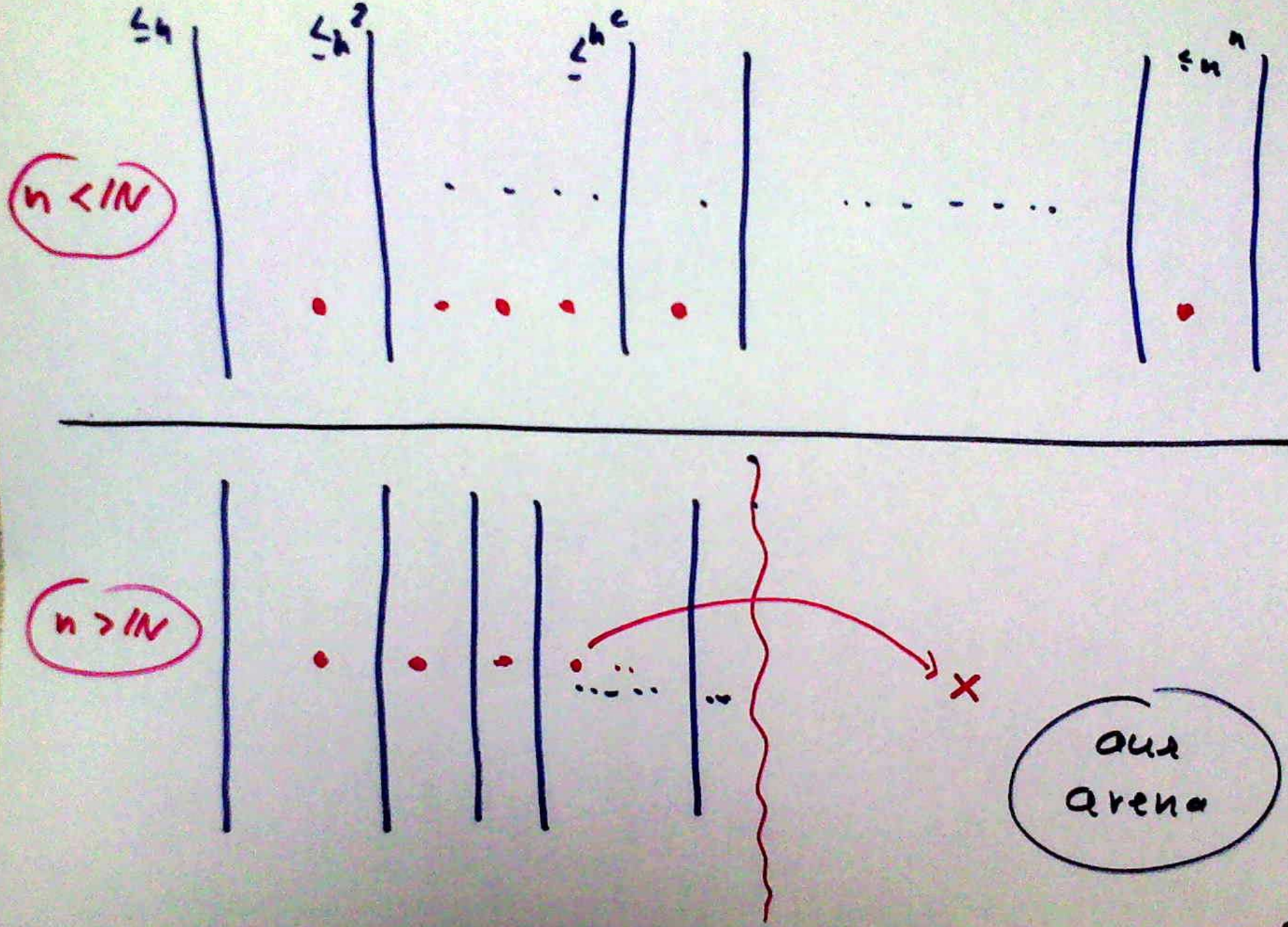
N-

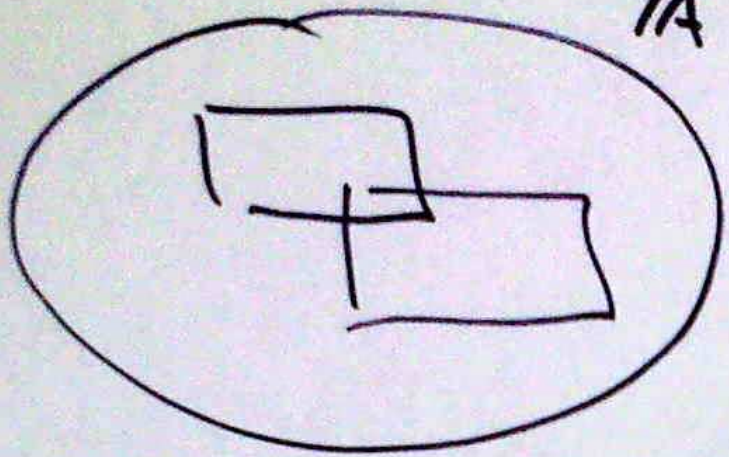
L-

C-

A-

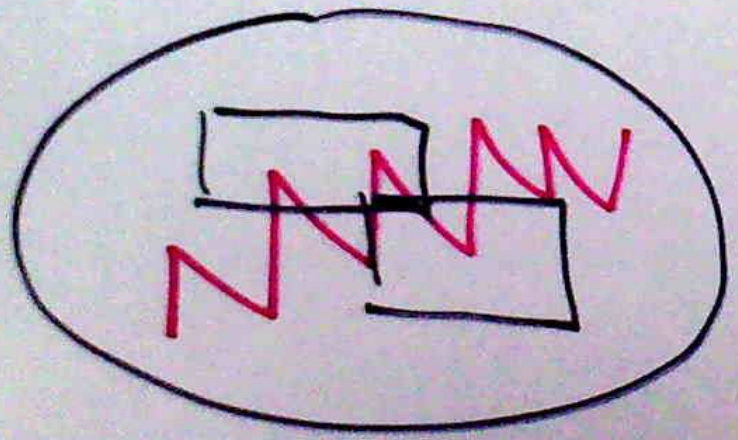



$\leq n$
$\leq n^2$
$\leq n^c$
$\leq n^n$
$n < IN$
$n > IN$
X
aus
arena



pseudo-finite structure
↳ encodes tautology τ, proof π, ...

1. bound tost ⇓ extend/expand by R



↳ encodes a falsifying assignement for τ
&
$(\mathcal{A}, R) \models \tau$ ....

[Ajtai]

forcing w. random var's

- F : a family of r.v. $\alpha : \Omega \to \mathbb{A}$

  ⇓

  determines structure $\mathcal{K}(F)$ ext./ess $\mathbb{A}$

- r.v.'s α : often defined by some compact device

  ↳ circuits, dec. trees, protocols for 2-player games, ...

a reduction of 1. bounds:

- properties of $K(F) \rightleftarrows$ prop's of F
- Ω^*/F are often defined in a way that it is "clear" that $K(F)$ satisfies what is needed, assuming that it is well-def.
- Key lemma: All $\alpha \in F$ are cl.fined a.e..

$\Uparrow$

"No $\alpha \in F$ solves task to ... "

ref's can be found in

- "Proof Complexity" book available at my www
  [Part IV, in particular]

- for formalizations of complexity th. start with [Krajíček – Pudlák '89]

- for alternative views: { intro. in Razborov's 02/03 paper

  → Pudlák's book on "Logical Found. of Math. & Comp. Compl."

(A, P): A is an alg. searching for P-proofs

$(A, P) \gtrsim (B, Q)$ ... as good as ...

$\Updownarrow$

$\exists c \geq 1 .\ \exists E \subseteq TAUT,\ E \in P/poly$ s.

$\forall \alpha \in TAUT \setminus E,\ size_A(\alpha) \leq size_B(\alpha)^c$.

Problem: Is there a $\gtrsim$-max (A, P)?

[See Chpt. 21 in "Proof compl."]