LECTURE 13

- optimality
- meta-mathematical big picture

OPTIMALITY PROBLEMS

- IS THERE AN OPTIMAL PPS?

  [$\geq$, $\geq_p$ in Lect. 3]

- IS THERE AN OPTIMAL WAY TO SEARCH FOR PROPOSITIONAL PROOF?

RECALL: $P \geq Q$ (P simulates Q)

$\uparrow\downarrow$ def.

$\exists\, c \geq 1\ \forall\, \tau \in TAUT: \quad S_P(\tau) \leq S_Q(\tau)^c$

$:= \min\{|\pi| \mid \pi \text{ is a } P\text{-prf of } \tau\}$

P optimal $\rightleftharpoons$ $P \geq$-maximal.

FIX A PPS Q.

$P_{F_Q} \subseteq \{0,1\}^* \times \{0,1\}^*$: THE PROVABILITY PREDICATE

$P_{F_Q}(x,y) \Leftrightarrow$ "x is a Q-proof of y"

BY THE DEF. : P_{F_Q} IS p-TIME AND

HENCE p-reducible TO CAT-SAT

IN THE FOLLOWING "UNIVERSAL" WAY.

$1^{(s)}, 1^{(n)} \xrightarrow[\text{p-time}]{} \text{CNF } [\![Pr_Q]\!]_{s,n}(\bar{p}, \bar{q}, \bar{r})$

$\bar{p} = p_1, \ldots, p_s$ .... bits of a Q-proof

$\bar{q} = q_1, \ldots, q_n$ ... bits of a FLA

$\bar{r} = r_1, \ldots, r_{poly(s,n)}$ ... Auxil. VARs

s.t.: $\forall \pi, \varphi \in \{0,1\}^*$: $|\pi| \le s$, $|\varphi| \le n$

$Pr_Q(\pi, \varphi) \Leftrightarrow [\![Pr_Q]\!]_{s,n}(\pi, \varphi, \bar{r}) \in SAT$.

DEFINE SET $A/_{G_2}$ CONSISTING OF ALL FORMULAS:

$$(*)_\varphi \quad \left[\!\left[\Pr_{G_2} \right]\!\right]_{S,n} (\bar{\pi}, \varphi, \bar{s}) \longrightarrow \varphi$$

FOR ALL $S \geq n \geq 1$ and ALL FCTS φ, $|\varphi| \leq n$, ALL STRINGS $\bar{s}$, $|\bar{s}| \leq S$

INFORMALLY: $(*)_\varphi$ SAYS THAT IF φ

IS G_2 – PROVABLE THEN

IT IS A TAUTOLOGY

CLAIM 1 : $H_{\mathcal{Q}} \subseteq TAUT.$

→ BECAUSE G IS SOUND. □

CLAIM 2 : $H_{\mathcal{Q}}$ IS P-TIME DECIDABLE.

→ OBVIOUS : IT IS DEFINED BY A SYNTACTIC PROPERTY. □

THM.: ASSUME $\mathcal{P}$ IS CLOSED UNDER MODUS PONENS IN THE FOLLOWING SENSE:

(#). $S_{\mathcal{P}}(\alpha) = S_1,\ S_{\mathcal{P}}(\alpha \to \beta) = S_2 \to S_{\mathcal{P}}(\beta) \le poly(S_1, S_2)$.

ASSUME $\exists c \ge 1\ \forall T \in H_Q,\ S_{\mathcal{P}}(T) \le |T|^c$.

THEN $P \ge Q$.

$=$

→ [A TECHNICAL CONDITION]

PRF: ASSUME $\pi, |\pi| = s$, IS A G-PROOF OF α, $|\alpha| = n \le s$

BY THE HYPOTHESIS P PROVES $\tau \in HL_G$:

$$\tau : [\![\Pr_{G_r} \tau_{s,n}(\pi, \alpha, F) \to \alpha$$

IN SIZE $\le poly(s, n) = poly(s)$.

BY THE CONSTR. τ IS $\in SAT$ SO

FOR SOME $\bar{a} \in \{0,1\}^*$:

$$[\![\Pr_{G_r} \tau_{s,n}(\pi, \alpha, \bar{a}) = 1.$$

A P-PRF OF α IS OBTAINED BY:

(i) PRF OF ~~Π~~ τ

(ii) PRF OF $\langle \Pi Pr_{\mathcal{L}} \forall_{S,n} (\pi, \alpha, \bar{a}) \rangle$

[JUST ELABORATION]

(iii) α BY MODUS PONENS.

TOTAL SIZE $\leq s^{O(1)}$.

$\square$

[WE OUGHT TO ADD THIS TITLE TO (#) SEE SEC. 21.1.1]

[THIS INCREASES SIZE POLYNOMIALLY AT MOST BY (#)]

COR. :(21.1.2)

P SATISFYING (#) IS OPTIMAL

$\Updownarrow$

$\forall H \subseteq TAUT, H \in P\text{-TIME} \Rightarrow \exists c \geq 1 \forall \tau \in H$

$Sp(\tau) \leq |\tau|^c$.

COR. : ANY G CAN BE SIMULATED BY

F + A P-TIME SET OF TAUTOLOGIES AS

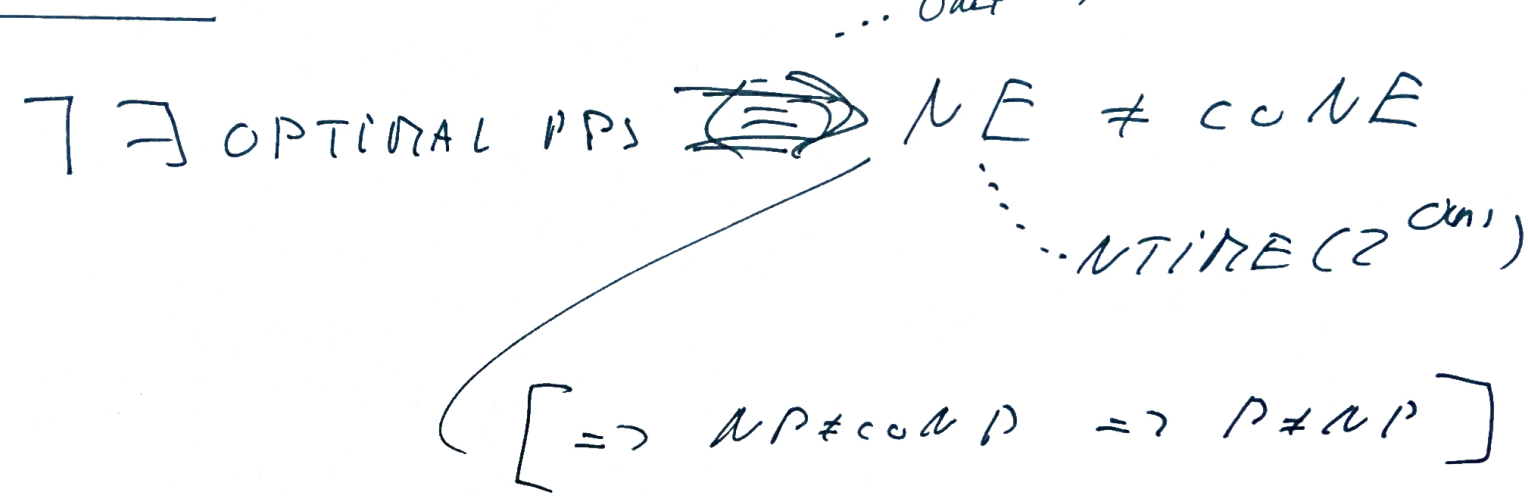
$\uparrow$ EXTRA AXIOMS

FREGE

.

TWO OTHER COROLLARIES OF THE CONSTRUCTION:

COR. 21.1.3



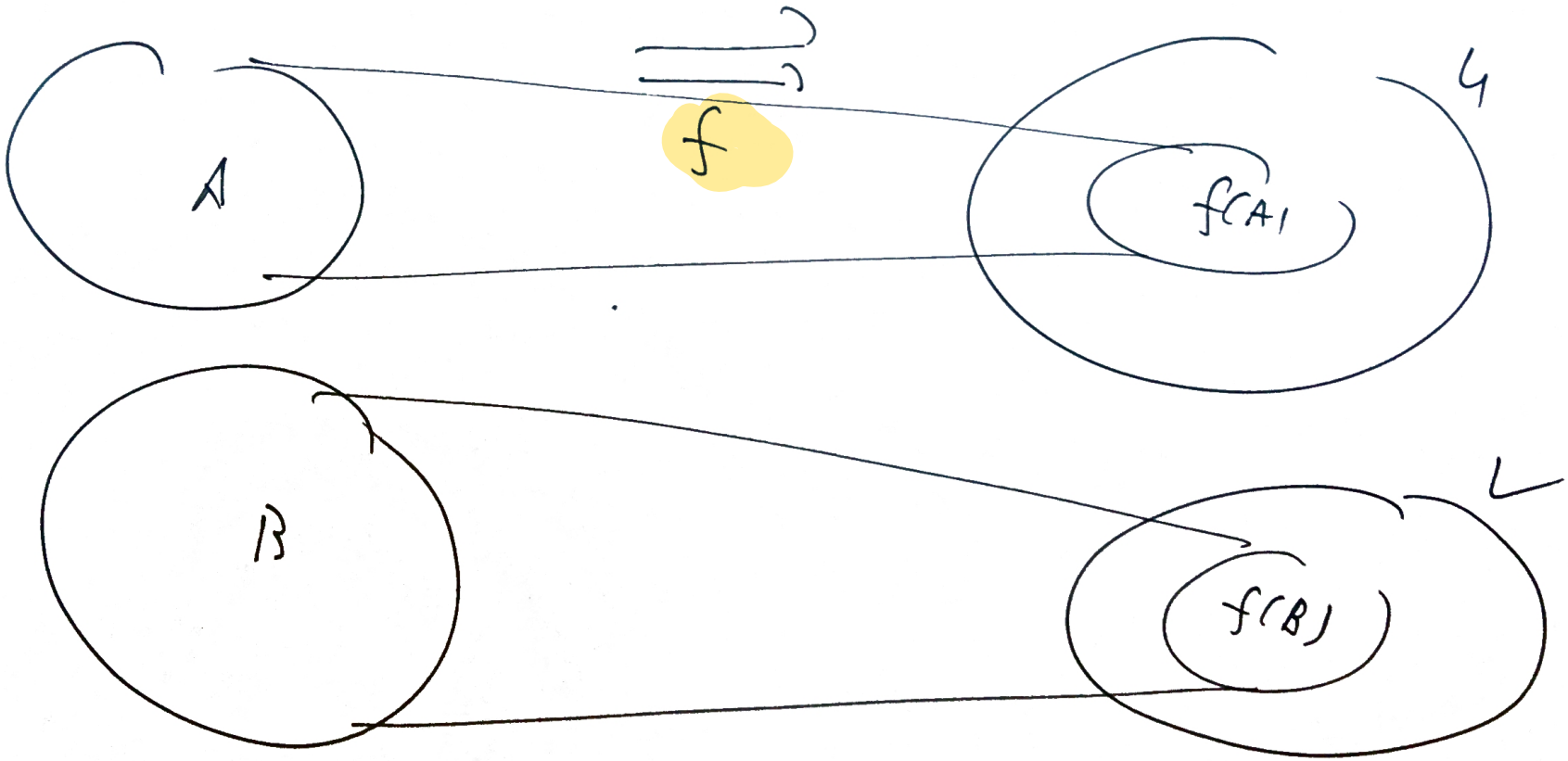
17.

COR.: ¬∃ OPTIMAL PPS => SPECTRA OF FO SENTENCES ARE NOT CLOSED UNDER COMPLEMENTATION.

16.

DISJOINT NI-PAIRS : $(A,B) \leq (U,V)$

$\Updownarrow$ def



I.E.: WE CAN SEPARATE U/V $\Rightarrow$ WE CAN SEP. A/B TOO.

COR. 21.2.3: $\neg\exists$ COMPLETE (W.R.T. $\leq$) DISJOINT NP-PAIR

$\Updownarrow$

$\neg\exists$ OPTIMAL PPS.

THERE ARE OTHER STATEMENTS EQUIVALENT (OR RELATED) TO THE $\exists$ OF OPTIMAL PPS.

↓

[Chpt 21.]

(VERY VARIED)

QUANTITATIVE GÖDEL'S THM

SET-UP (NOT MOST GENERAL BUT EASY TO USE!)

→ language : $L \supseteq L_{ARITH.}$: $0, ', +, \cdot, \leq$
(finite)

→ theory : T : finite (OR p-time set of ax's)

→ $T \supseteq$ SOME BASIC ARITHMETIC (S? e.g.)

→ consistent

$Con_T(x) \in L_{ARITH.}$ - fla EXPRESSING

"THERE IS NO T-PROOF OF $0 \neq 0$

OF SIZE $\leq x$"

$\forall x\, Con_T(x) = Con_T$: "T IS CONSISTENT"

GÖDEL'S 2nd THM:

$$T \nvdash Con_T.$$

DYADIC NUMERALS: $\underline{0} := 0$

$\underline{1} := 1$

$\underline{2k} := ((1+1)\cdot \underline{k})$, $\underline{2k+1} := (\underline{2k} + 1)$

ADVANTAGE:

$$|\underline{n}| \sim \log n$$

OVER $S_n := (\underbrace{(1+1)+1)\cdots+1)}_{n\text{-TIME}}$,

THM. (H. FRIEDMAN, P. PUDLÁK)

(1) $\exists \varepsilon > 0 \; \forall n \geq c$: ANY T-PROOF OF $Con_T(\underline{n})$ MUST HAVE SIZE $\geq n^{\varepsilon}$.

---- EXP. IN |----|

(2) $\exists c \geq 1 \; \forall n \geq 0$: THERE ARE T-PROOFS OF $Con_T(\underline{n})$ OF SIZE $\leq n^c$.

EXP. BETTER THAN EXH. SEARCH.

17

[SEE THM. 21.3.3 - FOR REF'S]

THM (K. & P.P.)

$\exists$ OPTIMAL PPS

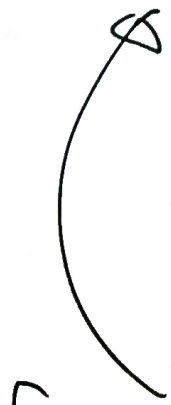
$\Uparrow$

$\exists$ theory S (OBEYING THE SET-UP)

$\forall$ th. T $\exists c \geq 1$ $\forall n \gg 0$:

$Con_T(\underline{n})$ HAS SIZE $\leq n^c$ S-PROOFS.

$\square$



[$\exists$ OF SUCH S DOES NOT LOOK VERY LIKELY]

TOWARDS PROOF SEARCH ALG's

⇒ DEF: A PAIR (A, P):

(i) P IS A PPS

(ii) A IS A DET. ALG. THAT STOPS ON ALL INPUTS AND S.T

$\forall T \in TAUT$: $A(T)$ is a P-PROOF OF T

$time_A(T)$:= "time on input T"

LEMMA: FOR $\forall$ PPS P $\exists$ ALG. A S.T. (A,P)

IS TIME-OPTIMAL AMONG ALL (B,P):

$$time_A(x) \leq time_B(x)^{O(1)}, \text{ ALL } x \in TAUT.$$

PRF: [LEVIN'S UNIVERSAL SEARCH]

- an algorithm $=$ a string (= the program)
- Order all alg's as $A_1, A_2, \ldots$ lexicographically.
- ~~RUN~~ FOR $i = 1, 2, \ldots$ RUN FIRST i ALG'S FOR i STEPS UNTIL A P-PROOF OF x IS FOUND.

□

A_p : THE ALG. FROM THE PROOF

QUESTION : ~~If~~ $\exists (A, p)$ time-optimal among all (B, q) ?

any q.

RECALL : $P \geq_p Q \iff \exists$ p-time f $\forall \pi, T$

$Pr_Q(\pi, z) \to Pr_P(f(\pi, T), T)$

p-SIMULATION.

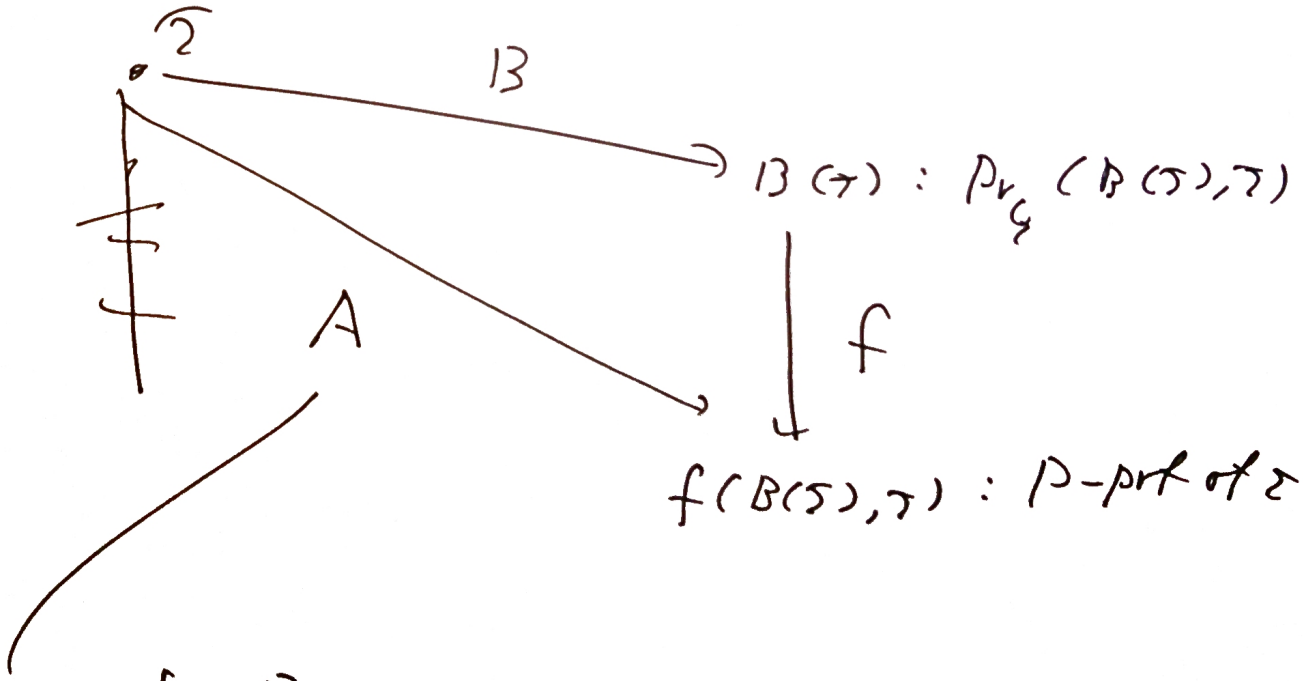
$(\leq_p \subseteq \leq)$.

~~LEMMA~~ LEMMA: IF P IS p-OPTIMAL ($\Leftrightarrow \exists_p$-DA+1)

THEN (A_p, P) IS TIME OPTIMAL AMONG

ALL (B, Q).

Prf:



□

THM: P IS p-OPTIMAL $\Leftrightarrow$ (A_p, P) IS TIME OPTIMAL (AMONG ALL (B, Q)).

$\Rightarrow$: THE LEMMA

$\Leftarrow$ USES SETS H_Q AGAIN.

□

THAT IS:

THE QUESTION $\Leftrightarrow \exists$ OF p-OPTIMAL P'S

[I.E.: NOT REALLY A NEW QUESTION]

HOW "MATHEMATICALLY STRONG" PROP. PROOF SYSTEMS ARE?

Ex.: [PARIS-WILKIE SIMULATION THM.]

$$I\Delta_0(R) \longmapsto \forall x\, \varphi(x,R), \quad \varphi \in \Delta_0(R)$$

$$\downarrow\!\downarrow$$

$\langle \varphi \rangle_n$ HAVE p-SIZE F_d-PROOFS

$\Delta_0(R)$ - fla $\varphi(x, R)$, informally:

$\varphi(n, R) \rightleftharpoons$ A FO-PROPERTY OF $([n], R \cap [n], \ldots)$

I.E.:

$ID(R) \rightleftharpoons$ IND FOR FO-PROPERTIES OF FINITE STRUCTURES

$\Sigma^1_1(R)$ - fla's $\rightleftharpoons$ NP-properties of fi'n. v's

theory V^1 $\rightleftharpoons$ IND FOR NP-prop. OF FINITE STRUCTURES

$\exists$ rel. S $\underbrace{\psi(x, R, S)}_{\Delta_0(R,S)}$

Th. V' FORMALIZES A LOT OF COMPLEXITY TH:

- NP-COMPL. OF SAT
- VARIOUS CIRCUIT LOWER BOUNDS
- CRYPTO CONSTR'S : GOLDREICH-LEVIN, OWF $\Rightarrow$ PRG, ..
- NISAN-WIGDERSON'S GENERATORS
- SORTING NETWORKS
- THE PCP THM.

⋮

[p. 475 - 2nd parogr.]

FACT : ER (= EXTENDED R) SIMULATES

~~AC°~~ V' IN THE SAME SENSE AS

AC°-F SIM's ID_c(R).

HENCE

"ER IS VERY STRONG"

→ [A LOT IS, IN FACT, IN F TOO]

→ RECALL : ER $\equiv_p$ "F OPERATING W/ CIRCUITS"

TO WHICH TYPE OF STATEMENTS / HYPOTHESES
KNOWN
DOES THE SIMUL. APPLY?

↳ Ex: P=NP as witnessed by p-time
alg A:

$$Sat(w, \varphi) \longrightarrow Sat(A(\varphi), \varphi)$$

$\forall$ (only p-time prop's)

Ex: $P \neq NP$ or, more specifically, no p-time alg. A solves SAT on infinitely many input lengths.

$$\forall n \geq n_0 \; \exists\, q, u \; (|q| = n), \; Sat(u, q) \wedge \neg Sat(A(q), q).$$

→ SPOILS THE $\forall$-FORM

BUT, A CAN BE USED TO FIND

ITS OWN ERRORS AND THE $\exists$-quant.

CAN BE REMOVED.

↓

[pp. 475-476]

Ex.: ANOTHER STATEMENT TO WHICH SIMUL-OF U' BEAVER APPLIES IS RIEMANN HYPOTHESIS.

SUMMARY: IF WE WANT TO PROVE LOWER BOUNDS FOR STRONGER PPSs AS IN ER WE OUGHT TO KNOW HOW TO PROVE INDEPENDENCE OF "UNIVERSAL" STATEMENTS FROM NON-TRIVIAL THEORIES.

→ A BIG OPEN PROBLEM IN MATH. LOGIC