LECTURE 8

$\rightarrow$ Ajtai's thm:

- corollaries
- variants
- open problems

RECALL: (Lect. 4) $\longrightarrow$ THEORY $I\Delta_0(R)$

- $\underbrace{0, 1, +, \cdot, \leq, <}_{L_A}, R(x,y)$
- ax's: $\longrightarrow$ FINITE NB. AX'S ABOUT L_A

  $\longrightarrow$ IND - induction

  FOR ALL $\Delta_0(R)$ - FLAS

  $\longrightarrow$ BOUNDED QUAN'S

SIMULATION THM. (Paris - Wilkie) - (Lect. 4 / slide 20)

$I\Delta_0(R) \vdash \mathrm{onto}PHP(R, x)$ .... $f : [x+1] \twoheadrightarrow [x]$

$\Downarrow$

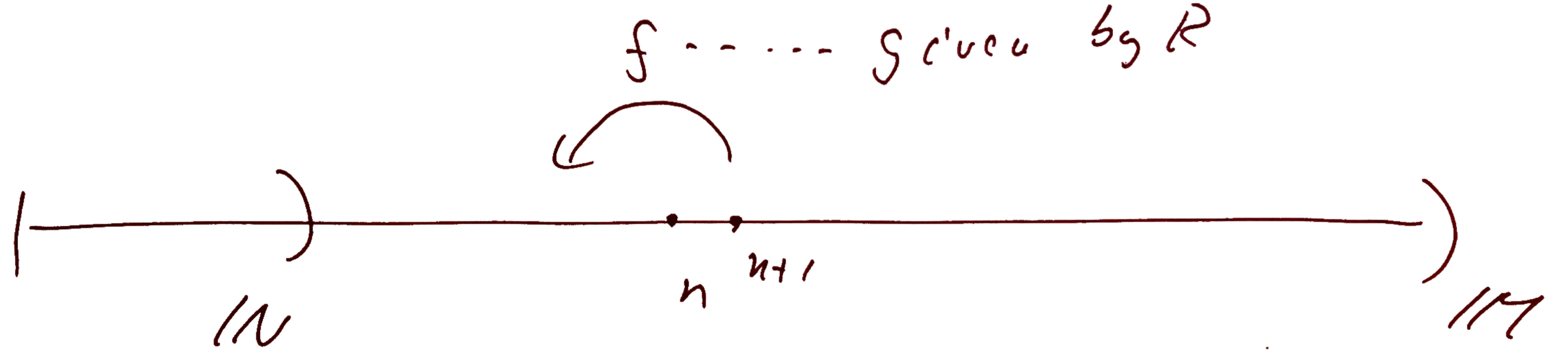
AC^0-F REFUTES $\neg \mathrm{onto}PHP_n$ in SIZE $\leq n^c$.
(some Fd)

COROLLARY: $I\Delta_0(R) \nvdash \mathrm{onto}PHP(R, x)$.
(Ajtai)

THIS IMPLIES VIA THE COMPLETENESS THM: THE ~~E~~EXISTENCE OF MODEL

$$\mathbb{M} \models I\Delta_0(R) + \neg\, \mathrm{onto}\,PHP(R, n)$$

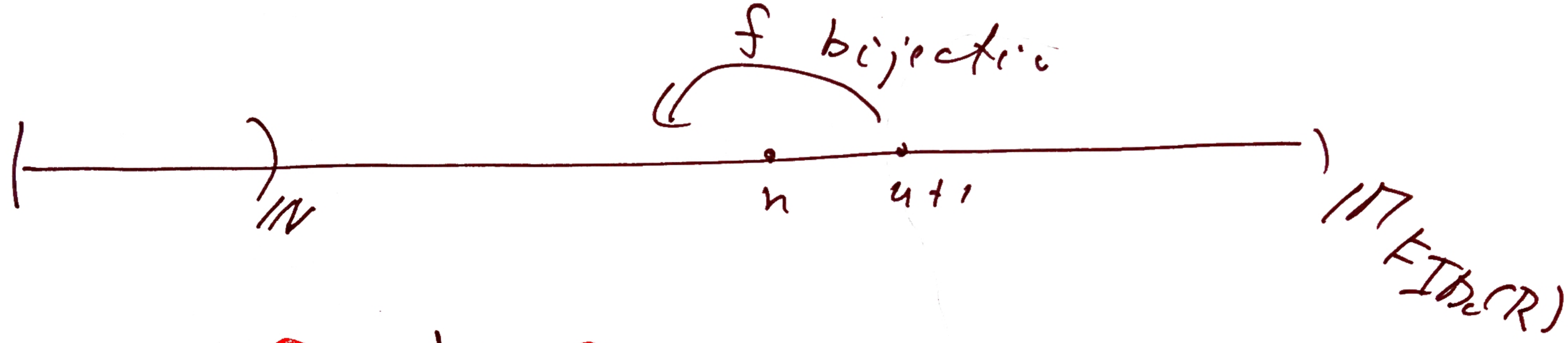
some $n \in M$.



$$\mathbb{M} = (M, 0, 1, +, \cdot, \leq, <, R^{\mathbb{M}}) \quad \cdots\; f : [n+1] \twoheadrightarrow [n])$$

WHAT ABOUT THE OPPOSITE?

I.E.: ASSUME WE CONSTRUCT



$$\overset{?}{\Downarrow}\,\overset{?}{}$$

LOWER BOUNDS FOR F_d-REF's

OF $\mathrm{Onto}\,PHP_m$ ($m >> 1$)

FACT: YES, ASSUMING M ALSO

SATISFIES ..... [Sec. 8.5]

OPEN PROBLEMS

1st type : ABOUT $I\Delta_0$

$I\Delta_0 \vdash \text{onto}\,PHP(\varphi, x)$,

~~F~~FOR ALL Δ_0-FLAS $\varphi(x,y)$?

I. ~~E~~. : NO SYMBOL R

IT IS DEFINED BY φ

[Macintyre's problem, 1980s]

2nd type: about Fd SYSTEMS AND OTHER COMBINATORIAL PRINCIPLES:

- WEAK PHP
- COUNTING PRINCIPLES
- .....

WEAK PHP

$\neg WPHP_n^{2n}$: FORMALIZES

$$f : [2n] \xrightarrow[\text{1-to-1}]{} [n]$$

$\neg WPHP_n^{n^2}$:

$$g : [n^2] \xrightarrow[\text{1-to-1}]{} [n]$$

OPEN : SUPER-POLY LOWER BOUNDS FOR F_d's

SURPRISING FACTS (PARIS-WILKIE-WOODS)

(i) $\exists d, c \geq ?$ s.t. BOTH

$\neg WPHP_n^{2n}$ and $\neg WPHP_n^{n^2}$

HAVE SIZE $\leq \boxed{n^{c \cdot \log n}}$ F_d-REF's

[QUASI-POLYNOMIAL]

(ii) $\forall k \geq 1 \; \exists d_k \geq ?$ S.T. $\neg WPHP_n^{n^2}$

HAS F_{d_k}-REF OF SIZE $\leq \boxed{n^{\log^{(k)}(n)}}$

k-times
iterated log

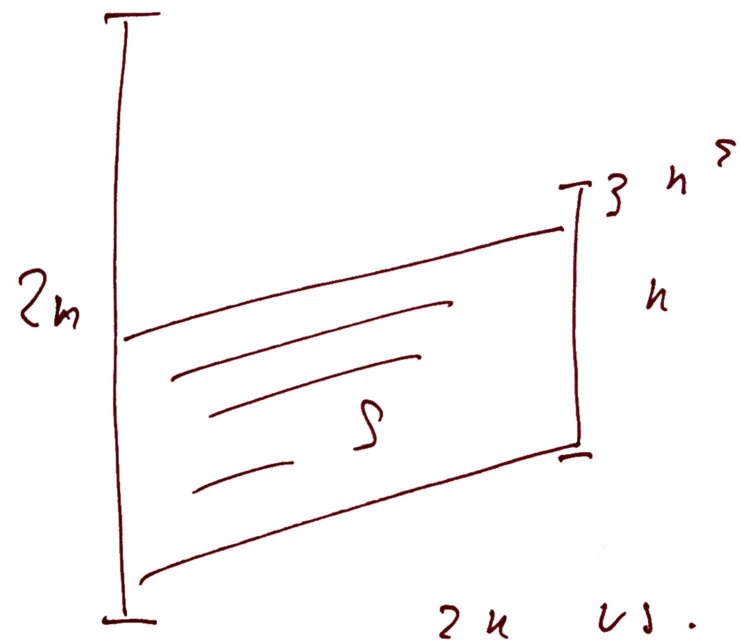
WHAT FAILS IN THE METHOD?

$n+1$ vs. n

$\Big\downarrow$ restr. ρ

$n^\varepsilon+1$ vs. n^ε

(STILL SAME SITUATION)



$2n$ vs. n

$\Big\downarrow \rho$

$n+n^\varepsilon$ vs. n^ε

(RATIO DRAMATICALLY INCREASES)

COUNT_m^2 :

ATOMS q_e, all $e \subseteq [m]$, $|e| = 2$

CLAUSES OF $\neg\mathrm{Count}_n^2$:

- $\bigvee_{e \ni i} q_e$, ONE FOR EACH $i \in [m]$
- $\neg q_e \vee \neg q_f$, if $e \neq f$, $e \cap f \neq \emptyset$ $(e \perp f)$

<u>FACT</u> : $\neg\mathrm{Count}_m^2 \in \mathrm{SAT} \iff m$ even.

THM. (INFORMALLY)

$\forall d\ \exists \delta > 0\ \forall n >> 0$ ODD,

F_d DOES NOT REFUTE $\neg Count_n^2$

IN SIZE $\leq 2^{n^\delta}$.

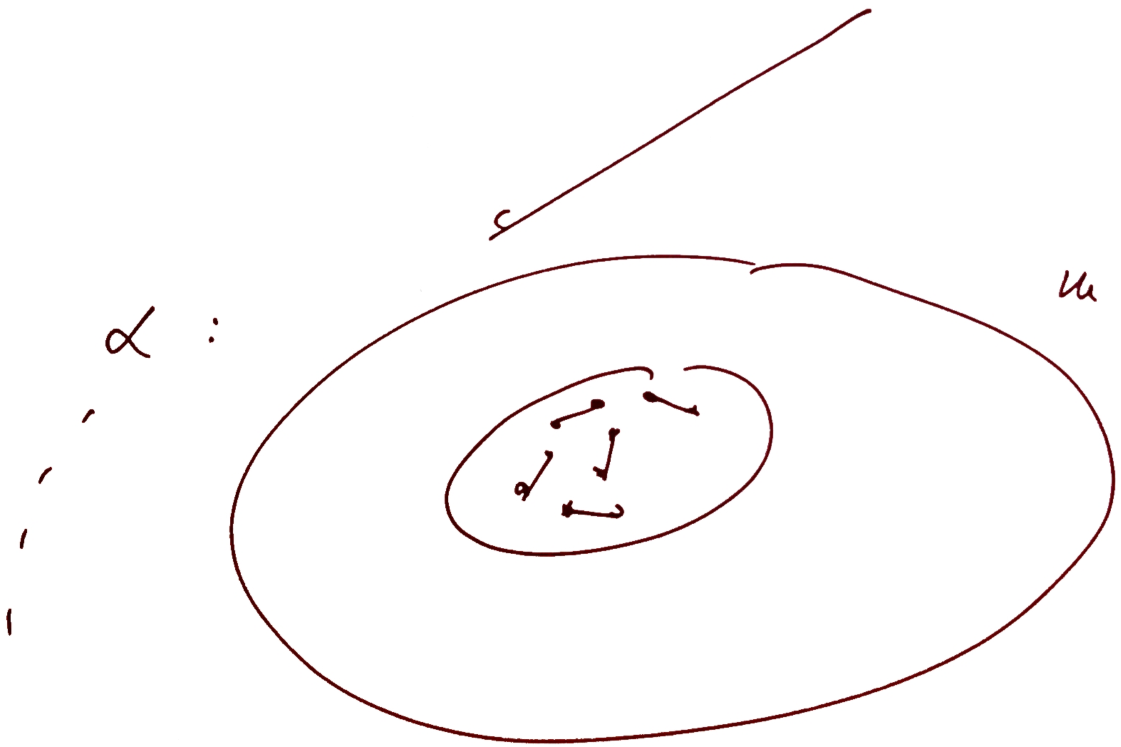
$\square$

- SAME FOR $\neg COUNT_n^q$, any $q \geq 2$ and

any $n \not\equiv 0 \pmod q$.

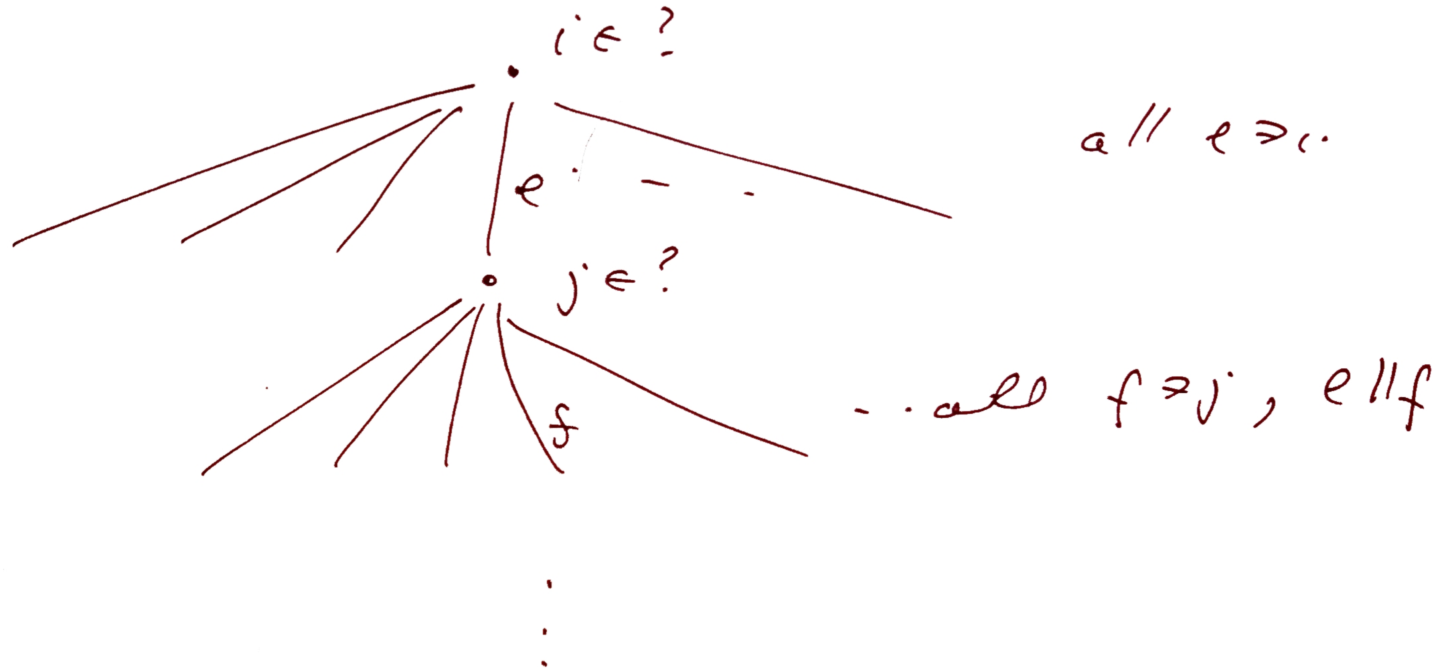
MODIFICATION OF THE METHOD NEEDED

- INSTEAD OF maps USE Pairings



partial pairings on $S[m]$

- NEW TREES:



- THE REST IS ANALOGOUS

RELATION OF PHP / COUNT? :

→ DOES

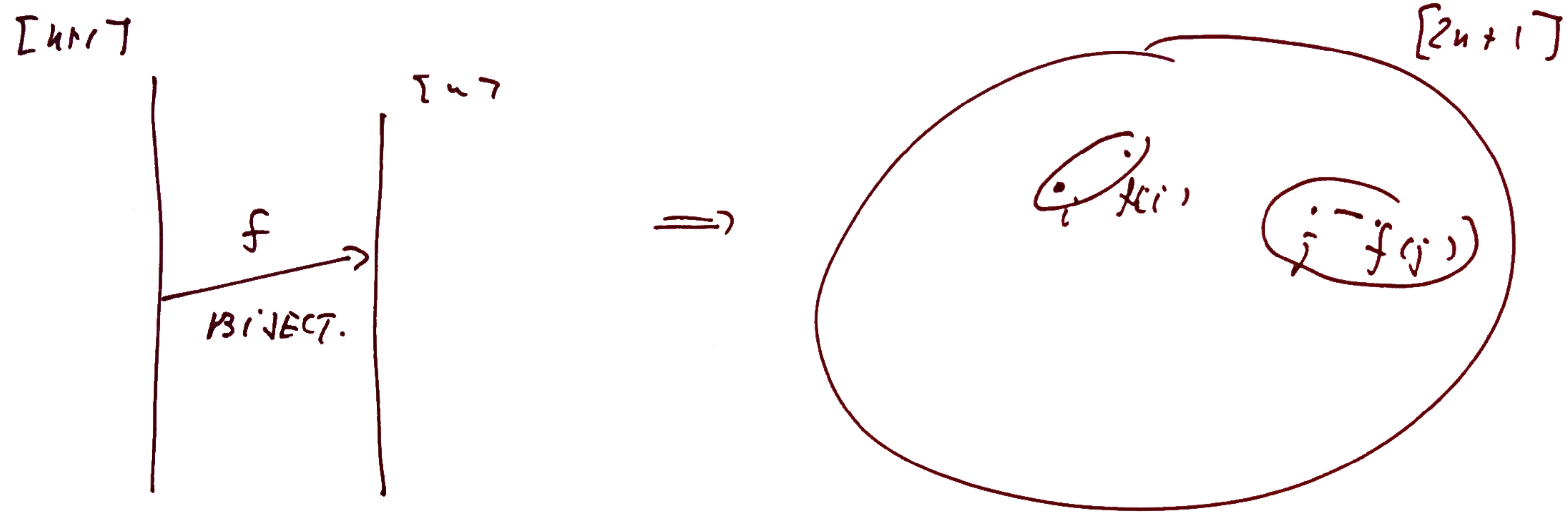
(a) ontoPHP ⇒ Count?
?

OR

(b) COUNT? ⇒ onto PHP
?

I.E. DO ALL INSTANCES OF Count?
imply ~~ontoPHP~~ ontoPHP.

(b) - EASIER



IS A TOTAL PAIRING (IF WE IDENTIFY $[n+1] \cup [n]$ with $[2n+1]$).

NOTE: THE PAIRING IS DEFINED FROM R

FORMALLY :

$\neg$ onto PHP_n .... with atoms p_{ij}

IMPLIES BY A SHORT (poly(n)) F_{d_0}-proof

$\neg Count^2_{2m+1}(q_e / \varphi_e)$

φ_e ... A CONST. DEPTH FLAS BUILT

FROM ATOMS p_{ij}

(ONE FOR EACH e).

(a) - harder

ASSUME INSTANCES OF cutoPHP

IMPLY Count^2

W.L.O.G. : JUST ONE INSTANCE SUFFICES

$$\text{cutoPHP}_n(\varphi_{ij}) \longrightarrow \text{COUNT}^2_m(\varphi)$$

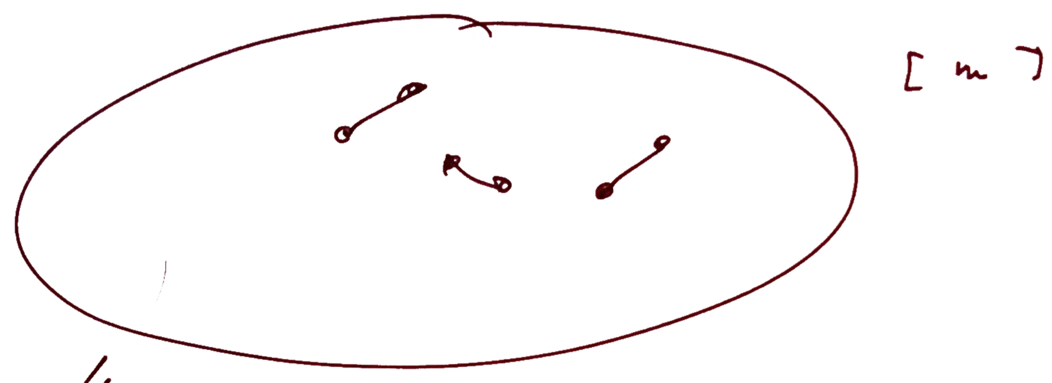
(some $n \geq 1$)

, m odd (any)

BUILT FROM ATOM φ

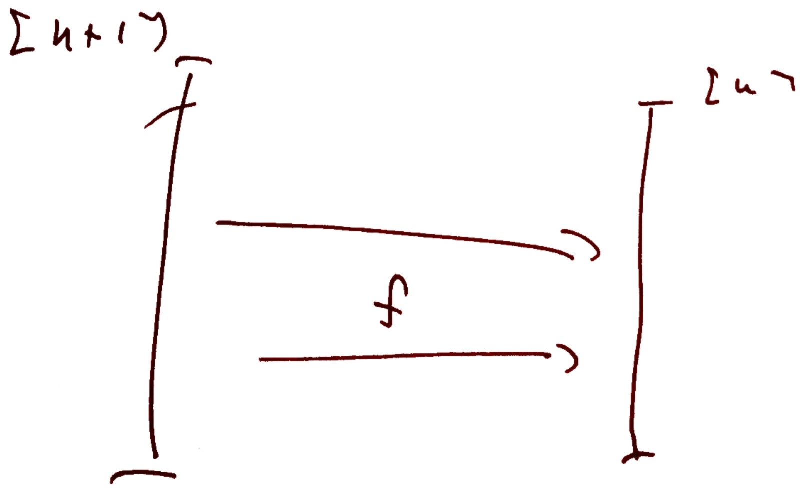
PICTURE:

WE HAVE TOTAL PAIRING S ON ODD m



$\Downarrow$ HOW TO DEFINE FROM S

SOME BIJECTION f ?



[DOES NOT SEEM TO BE POSSIBLE]

THM (Ajtai + later improvements)

$\forall d \geq 2\ \exists \delta > 0\ \forall m >> 0$ ODD,

ANY F_d - PROOF OF $COUNT^2_m$ FROM

INSTANCES OF $\text{onto}PHP_n$, $n \geq 1$,

NEEDS SIZE $\geq 2^{n^\delta}$. $\square$

- PRF - IDEA : NEXT SLIDE

FACTS : $Count^2$ AND $COUNT^3$ (AND MORE GENERALLY...)

ARE ALSO "MUTUALLY INDEPENDENT"

Let Γ be ALL FLAS OCCURRING IN A "SHORT" F_d - PROOF OF

(*) $\underline{\neg \mathrm{ontoPHP}_n(x_{ij}) \vee \mathrm{COUNT}^?_m(\vec{q_e})}$, n odd

—

USE a k-EVAL. (H, S) of Γ (USING PAIRING TREES!). THEN:

(i) (*) is (H, S)-TRUE

(ii) $\mathrm{COUNT}^?_m(\bar{q_e})$ is (H, S)-FALSE ($H = \emptyset$)

[≈ LEMMAS 6-7 BEFORE - LECT. 6]

HENCE :

$\neg \mathrm{Cut}\text{-}\mathrm{PHP}_n(y_{ij})$ is (H,S)-TRUE.

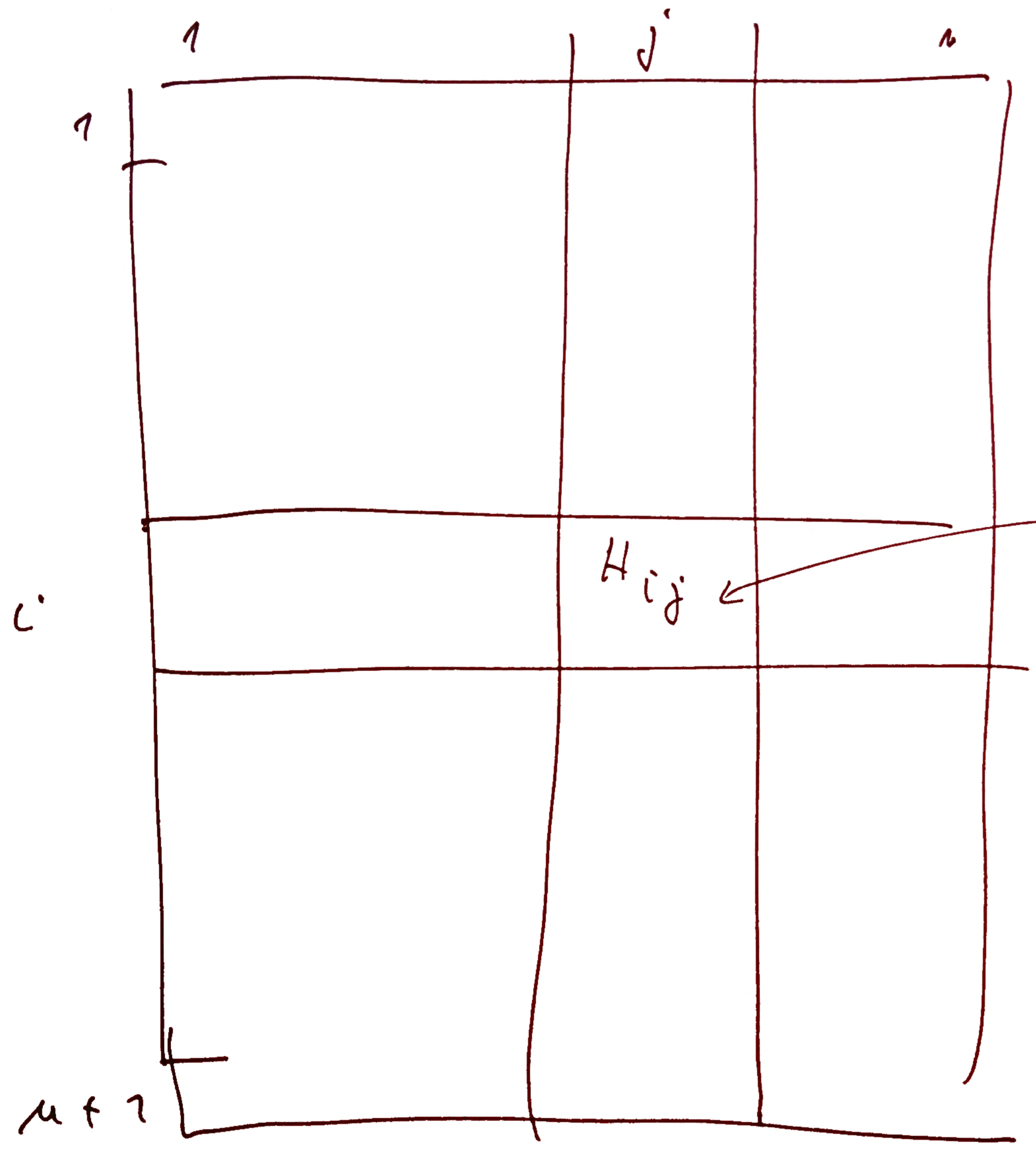
PUT:

$H_{ij} := H_{y_{ij}} \subseteq$ Pairings

ASSUME $\exists T \supset H_{ij}$, all i,j.

[THIS IS OVER-SIMPLIFICATION : THE ACTUAL ARGUMENT IS TECHNICALLY MORE SUBTLE.]

CONSIDER MATRIX



a set of pairings α, $|\alpha| \leq k$ "small"

PROPERTIES (USING TREET):

(i) $H_{ij_1} \cap H_{ij_2} = \emptyset$ .... f is a map

(ii) $\bigcup_j H_{ij} = T$ dom $f = [n+1]$

(iii) $H_{i_1 j} \cap H_{i_2 j} = \emptyset$ f is 1-to-1

(iv) $\bigcup_i H_{ij} = T$ Rng$(f) = [n]$

THEN ARGUE THAT THIS IS IMPOSSIBLE.

→ USES ALGEBRAIC PROOF SYSTEM, H_{ij} REPRE BY POLYNOMIALS

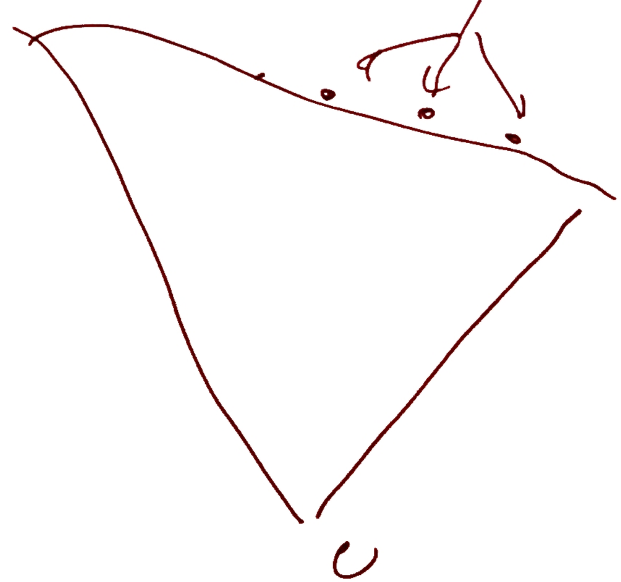
INTERPRETING THE PHP-PROOF AS AN ADVERSARY ARGUMENT

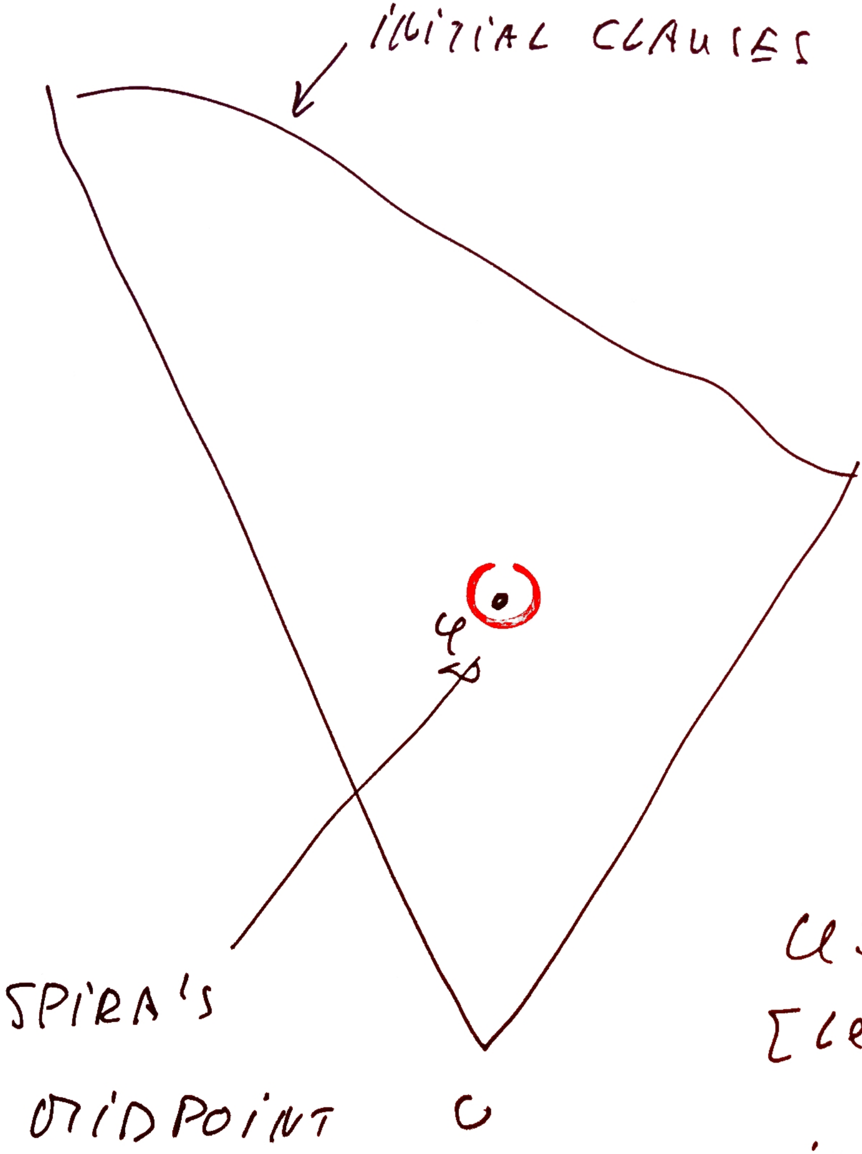
π .... an F_d-REF. OF $\neg$onto-PHP_n

FACT: CHANGING d to $d' \geq d$ ($\times\, d+1$)

WE MAY ASSUME π IS

TREE-LIKE





$(H_1 S)$: k-eval.

$$\boxed{\varphi \approx \bigvee_{\alpha \in H_\varphi} P_\alpha} \quad : \quad k\text{-DNF}$$

$$P_\alpha := \bigwedge_{(i,j) \in \alpha} p_{ij}$$

$$\boxed{\neg\varphi \approx \bigvee_{\beta \notin H_\varphi} P_\beta} \quad : \quad \text{also } k\text{-DNF}$$

$\ldots \beta \in J_\varphi \setminus H_\varphi$

USE ADV. ARG. AS FOR R^+ [lect. 5], USING $\bigvee_\alpha P_\alpha$ INSTEAD OF φ

$$\Rightarrow \text{size}(\pi) \geq \left(3/2\right)^{n^{\varepsilon}/k} = \left(3/2\right)^{n^{\varepsilon-\delta}}$$

n_ρ

OPEN PROBLEM:

PROVE A SUPER-POLY (BETTER EXP.) LOWER BOUND FOR SYSTEM $F_d(\oplus)$

ANALOGOUS TO F_d BUT THEIR LANG. HAS ALSO THE PARITY

FACTS: $F_d(\oplus)$ DOES PROVE SHORTLY (poly(n)) BOTH ontoPHP_n and $Count_m^2$.

) OFTEN DESCRIBED AS THE EASIEST OF HARD PROBLEMS

) FOR > 30 YEARS NOW!