9.IV.2025

Last time

(A) Herbrand's thm - proposit. version

(B) Herbandization:

$\varphi \longrightarrow \varphi_H$

[review first]

= - ax's

$x = x$, $x = y \to y = x$,

$(x = y \wedge y = z) \to x = z$

$\bar{x} = \bar{y} \to f(\bar{x}) = f(\bar{y})$

$\bar{x} = \bar{y} \longrightarrow R(\bar{x}) \equiv R(\bar{y})$

$\bigwedge_i x_i = y_i$

$\underline{\underline{\mathcal{E}}}$: all instances of $=$-ax's for all terms in the resp. lang.

<u>Ex</u>:

$$t = s \rightarrow s = t$$

$$\bigwedge_i t_i = s_i \rightarrow R(\bar{t}) \equiv R(\bar{s})$$

translation [...] :

q-free flo α $\longrightarrow$ prop. flo $[\alpha]$

- α atomic : $[\alpha] := p_\alpha$
  "p with index α"

- [ ] commutes with $\wedge, \vee, \neg$

A-review

Thm (J. Herbrand '30)

If $\models \forall x \exists y\, \alpha(x,y)$, α open,

then for some $E_i \in \mathcal{E}$ and some terms t_j:

$$\left[\bigwedge_i E_i \longrightarrow \bigvee_j \alpha(x, t_j) \right]$$

is a propositional tautology. ($\in$ TAUT)

$$\varphi = \forall x \, \exists y \, \forall z \, \alpha(x, y, z)$$

$$\Big\downarrow \text{Herbrandization}$$

$$\varphi_H := \exists y \, \alpha(c, y, h(c, y))$$

new symbols

<u>Fact</u>: $\models \varphi \iff \models \varphi_H$.

KPT theorem

Assume $\models \forall x \exists y \forall z\, \alpha(x,y,z)$, α open.

Then $\exists$ terms $t_1(x)$, $t_2(x, z_1)$, $\dots$

$\dots\ t_k(x, z_1, \dots, z_{k-1})$ s.t.

$$\models \bigvee_{1 \le i \le k} \alpha(x, t_i, z_i)$$

(The opposite also holds.)

Ex.: $k = 2$ / opposite direction

$$\models \alpha(x, t_1(x), z_1) \vee \alpha(x, t_2(x, z_1), z_2)$$

$$\Downarrow$$

$$\models \alpha(x, t_1(x), z_1) \vee \forall z\, \alpha(x, t_2(x, z_1), z)$$

$$\Downarrow$$

$$\models \alpha(x, t_1(x), z_1) \vee \exists y \forall z\, \alpha(x, y, z)$$

$$\Downarrow$$

$$\models \forall z\, \alpha(x, t_1(x), z) \vee \exists y \forall z\, \alpha(x, y, z)$$

$$\Downarrow$$

$$\models \exists y \forall z \vee \exists y \forall z \implies \models \exists y \forall z \implies \models \forall x \exists y \forall z.$$

Simple lemma

If γ open and z a variable not occurring in γ, and γ' is:

γ' := $\boxed{\text{"replace all occurrences of some term } t \text{ in } \gamma \text{ by } z\text{"}}$

Then $[\gamma]$ equals to $[\gamma']$ after renaming atoms.

In particular: $[\gamma] \in TAUT \iff [\gamma'] \in TAUT$.

Prf.:

Mapping $P_\alpha \longrightarrow P_{\alpha'}$

is injective as it has inverse:

"replace all occurrences of z in α' by term t".

q.e.d.

Ex: $f(t, g(t)) = 0 \longrightarrow f(z, g(z)) = 0$

$\Longleftarrow$

Prf. of KPT

$$\models \forall x \exists y \exists z\, \alpha(x,y,z)$$

$$\Downarrow \; \text{B}$$

$$\models \exists y\, \alpha(c,y,h(c,y))$$

$$\Updownarrow$$

$$\models \forall x \exists y\, \alpha(x,y,h(x,y))$$

$$\Downarrow \; \text{A}$$

$$\vdots$$

$\exists$ terms $s_1, \ldots, s_k$ s.t.

$$\models \bigwedge_i E_i \longrightarrow \bigvee_{j \le k} \alpha(x, s_j, h(x, s_j))$$

and $[\ldots\ldots] \in TAUT$.

Simplification: All substitutions we shall make transform $=$-ax's into another $=$-ax. Hence we leave them out from the notation.

Eq. - simpl.

$$t = s \longrightarrow f(t) = s$$

$$\Big\downarrow \; \text{subst/replacement } t \text{ by } z$$

$$z = s \longrightarrow f(z) = s$$

also $\in E$.

Prf - cont'd

$$\left[\bigvee_{j \le k} \alpha(x, s_j, h(x, s_j)) \right] \in TAUT$$

Order $s_1, \ldots, s_k$ s.t. $\text{size}(s_1) \le \ldots \le \text{size}(s_k)$

Claim: $h(x, s_k)$ does not occur in

any $\alpha(x, s_j, h(x, s_j))$ for $j < k$.

$\square$

Replace $\underline{h(x, s_k)}$ by new var. $\underline{z_k}$

everywhere:

$$\left[\bigvee_{j \leq k-1} \alpha(x, s_j, h(x, s_j))\right] \vee \left[\alpha(x, s_k, z_k)\right]$$

Claim: $h(x, s_{k-1})$ may occur in s_k but not in any $\alpha(x, s_j, h(x, s_j))$ for $j < k-1$. ↻

Replace everywhere $\underline{h(x, s_{k-1})}$ by $\underline{z_{k-1}}$:

$$\left[\bigvee_{j\le k-2} \alpha(x, s_j, h(x, s_j))\right] \vee \left[\alpha(x, s_{k-1}, z_{k-1})\right]$$

$$\vee \left[\alpha(x, s_k'(x, z_{k-1}), z_k)\right]$$

obtained from $s_k(x)$.

After k rounds we get:

$$\bigvee_{j \leq k} \left[\alpha(x, t_j(x, z_1, \dots, z_{j-1}), z_j) \right]$$

s.t. it propositionally follows from some [= 'all's].

<u>Hence</u>:

$$\vdash \boxed{\bigvee_{j \leq k} \alpha(x, t_j(x, z_1, \dots, z_{j-1}), z_j)}$$

<u>q.e.d.</u>

An interpretation

A game between 2 players:

Student (S) : usually computationally limited

Teacher (T) : unlimited powers (an oracle)

The game on $\forall x \exists y \forall z\, \alpha(x,y,z)$

Round 1: Both S/T get $x := a$, and

S puts forward candidate witness
$y := b_1$:

$$\forall z\, \alpha(a, b_1, z)$$

T: either says that b_1 is OK
or provides a counter-ex.:
some $z := c_1$ s.t. $\neg\alpha(a, b_1, c_1)$.

Round 2 :

(S) : puts new candidate $y := b_2$

(T) : either OK it

or gives $z := c_2$ s.t.

$$\neg\alpha(a, b_2, c_2).$$

Corollary of the KPT

$$\mathcal{H} \models \forall x \exists y \forall z\, \alpha(x,y,z),\ \alpha \text{ open}$$

then there is $k \geq 1$ s.t. there exist <u>student S</u> s.t.:

(1) S solves the task in S-T game in $\boxed{\leq k \text{ rounds.}}$

(2) Moves of S are $\boxed{\text{computed by}}$ $\boxed{\text{terms}}$ in the language.

Ex. $k=3$ KPT yields

$$\models \alpha(x, t_1(x), z_1) \lor \alpha(x, t_2(x, z_1), z_2)$$
$$\lor\, \alpha(x, t_3(x, z_1, z_2), z_3).$$

If $b_1 := t_1(a)$ incorrect and $\neg\alpha(a, b_1, c_1)$

then either ... $b_2 := t_2(a, c_1)$ correct

or, if $\neg\alpha(a, b_2, c_2)$,

$b_3 := t_3(a, c_1, c_2)$ must be correct.

$\square$

Ex. 1 - min principle

L : $<$, ...

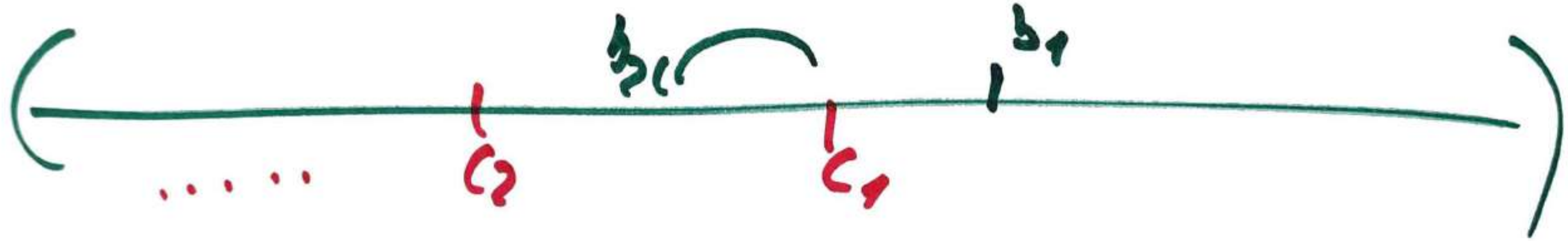
T : $\forall_1$-th. containing "$<$ is strict lin.ord."

Question : $T \models_? \exists \min_<$

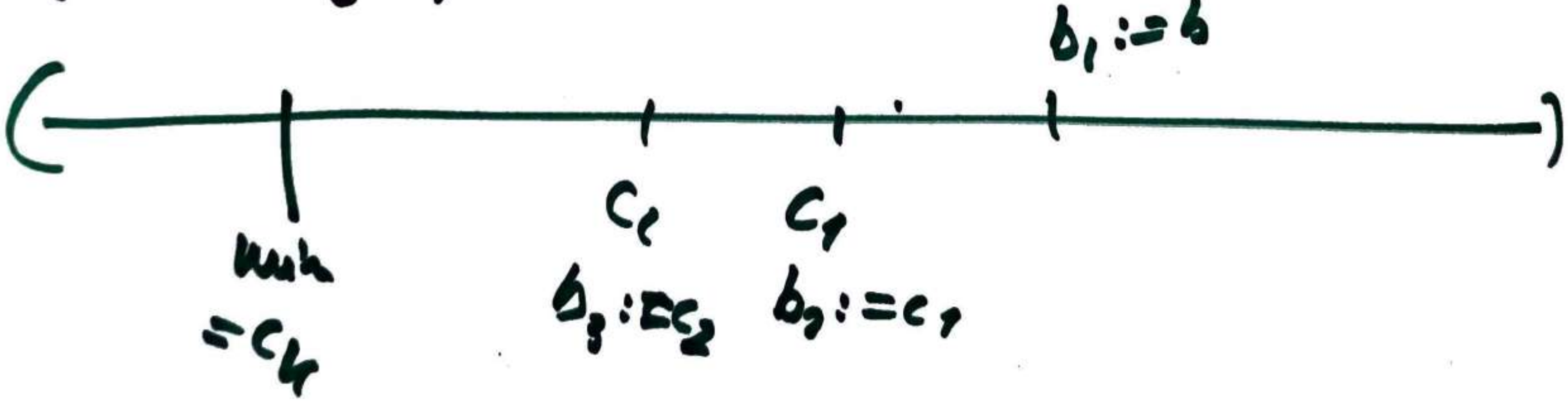
$$\exists y \forall z \, (z \neq y \rightarrow y < z)$$

(Remark : true in finite lin. ord.'s.)

KPT $\Rightarrow$ $\exists S$ computed by terms finding $\min_<$ in 4 rounds:



E.g. $L = \{<, b\}$



Ex. 2 - dual WPHP

$L = L_{PV}$, $T = T_{PV}$ (true $\forall_1$ L_{PV}-sentences)

$T \models_?$ "$\underbrace{g \text{ cannot map } \{0,1\}^n \ \underline{\underline{\text{onto}}}\ \{0,1\}^{n+1}}$"

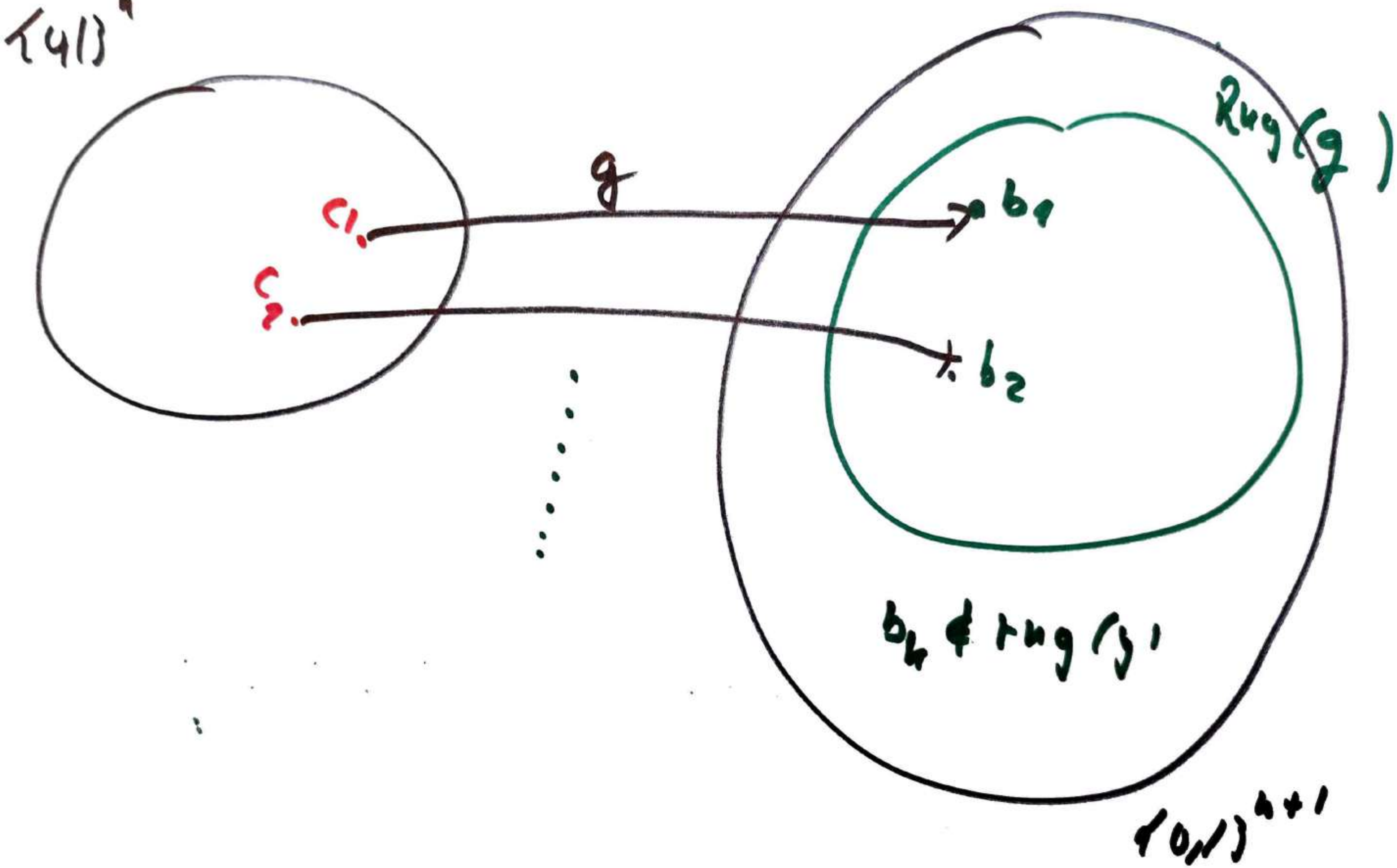
Simplify: $T \models |g(x)| = |x| + 1$

$$\forall x \exists y \forall z \left(|y| = |x| + 1 \wedge \left(|z| = |+| \rightarrow g(z) \neq y \right) \right)$$

$|x| = n$

$y \in \{0,1\}^{n+1}$

$z \in \{0,1\}^n$


{0,1}^n
g
c1
c2
b1
b2
Rng(g)
b_k ∉ rng(g)
{0,1}^{n+1}

Ex.3 – "ODD DEGREE" search problem

L: $R(x,y)$, b

T: $\forall_1$-th. ~~[illegible]~~: +

(i) R is symmetric and without loops

(ii) degree of any vertex is ≤ 2

(iii) $\deg(b) = 1$ .... $\exists y \neq b \, \forall z : R(b,y) \wedge (z \neq y \rightarrow \neg R(b,z))$

$\exists_2$

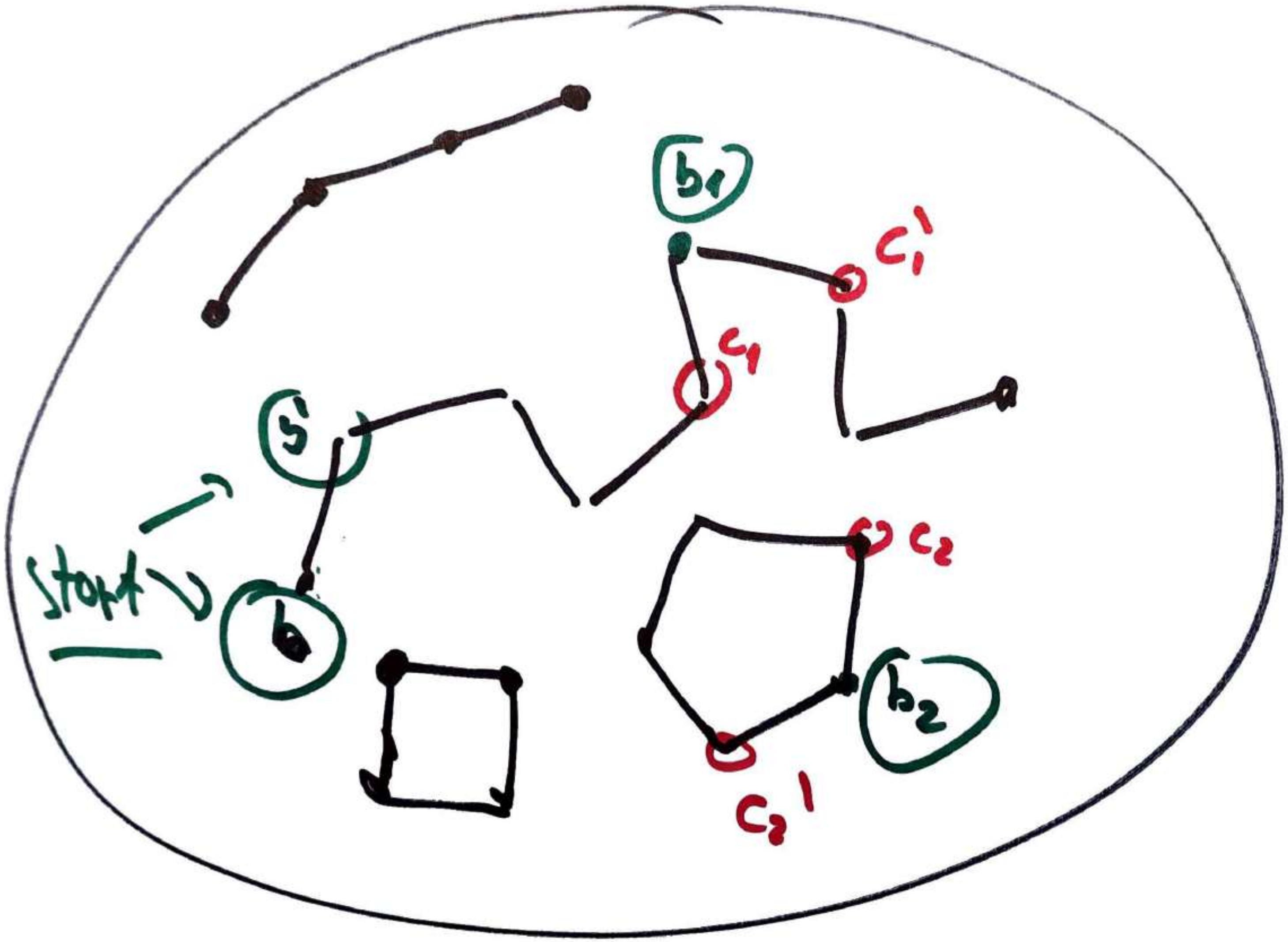
$$\forall x, y_1, y_2, y_3 \left(\bigwedge_{i \leq 3} R(x, y_i) \longrightarrow \bigvee_{j_1 \neq j_2} y_{j_1} = y_{j_2} \right)$$

$\forall_1$

$$T \models_{?} \underbrace{\text{"}\exists \text{ vertex} \neq b \text{ of degree } 1\text{"}}_{\text{true in finite graphs as } \Sigma \text{ degrees is even}}$$

$$\exists y \neq b, y' \exists z \, (\overbrace{y \neq y' \wedge R(y,y')}^{\deg(y) \geq 1}$$

$$\wedge \, (\underbrace{z \neq y' \to \neg R(y,z)}_{\deg(y) \leq 1}))$$



b_1
c_1'
c_1
s
Start
b
c_2
b_2
c_2'

Adding "some" IND

$L = L_{PV}^{u(c)}, \quad T := T_{PV} +$

"IND for $\exists u \le x\, \alpha(x,u)$ from 0 to c"

A $\quad \neg\alpha(0,0) \vee$

B $\quad \exists x < c\, \left(\exists u \le x\, \alpha(x,u) \wedge \forall v \le x+1\, \neg\alpha(x+1,v)\right) \vee$

C $\quad \exists u \le c\, \alpha(c,u)$

<u>Assume</u> $T^+ \models \exists y \forall z \beta$

$$\Downarrow$$

$T \models A \Rightarrow \exists y \forall z \beta$

$T \models B \Rightarrow \exists y \forall z \beta$

$\vdots$

$T \models C \Rightarrow \exists y \forall z \beta$

A-cor:

$T \vdash \neg\alpha(0,0) \to \exists y \forall z \beta$

$\Downarrow$

KPT gets student S_A which, $\underline{\underline{\text{if } \neg\alpha(0,0)}}$, finds y in $O(1)$ rounds.

What if $\alpha(0,0)$ holds?

<u>B-case</u> : $T \vdash B \to \exists y \forall z \beta$

$T \vdash \forall x < c \, \forall u \le x \, \exists v \le x+1 \, (\alpha(x,u) \to \alpha(x+1,v))$

$\vee \; \exists y \forall z \beta$

$\neg B \vee \dots$

S_B : given x, u s.t. $\alpha(x,u)$

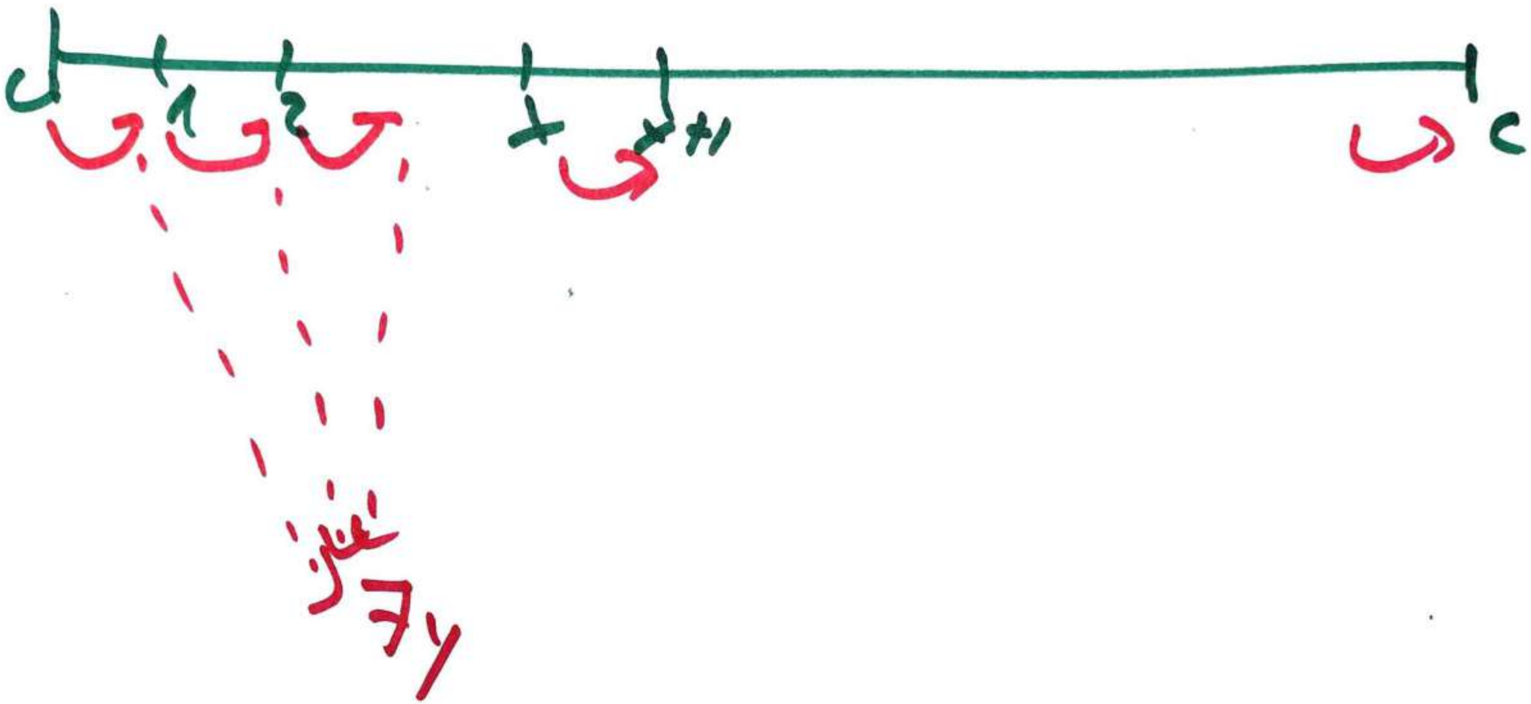
<u>either</u> : finds $v \le x+1$; $\alpha(x+1,v)$

<u>or</u> : finds witness for $\exists y$

Iterate, starting with $x = u := 0$, i.e. $\alpha(0,0)$

S_B : either witness $\exists y$ or finds $w \le c$: $\alpha(c,w)$.

$\le O(c)$ rounds



If S_B fails to find $\exists y$

then it witnesses $\exists u \leq c\, \alpha(c,u)$

Case C (simplest) $T \vDash c \to \exists y \forall z \beta$

$$T \vDash \forall w \leq c \neg \alpha(c, w) \vee \exists y \forall z \beta$$

S_C : finds witness for $\exists y$

as we can provide $w \leq c\ \alpha(c, w)$

via $S_A + S_B$

$\swarrow$

either S_A finds $\exists y \forall z \beta$

or S_B finds $\exists w \leq c\ \alpha(c, w)$

and so S_C finds $\exists y$ - witness. //