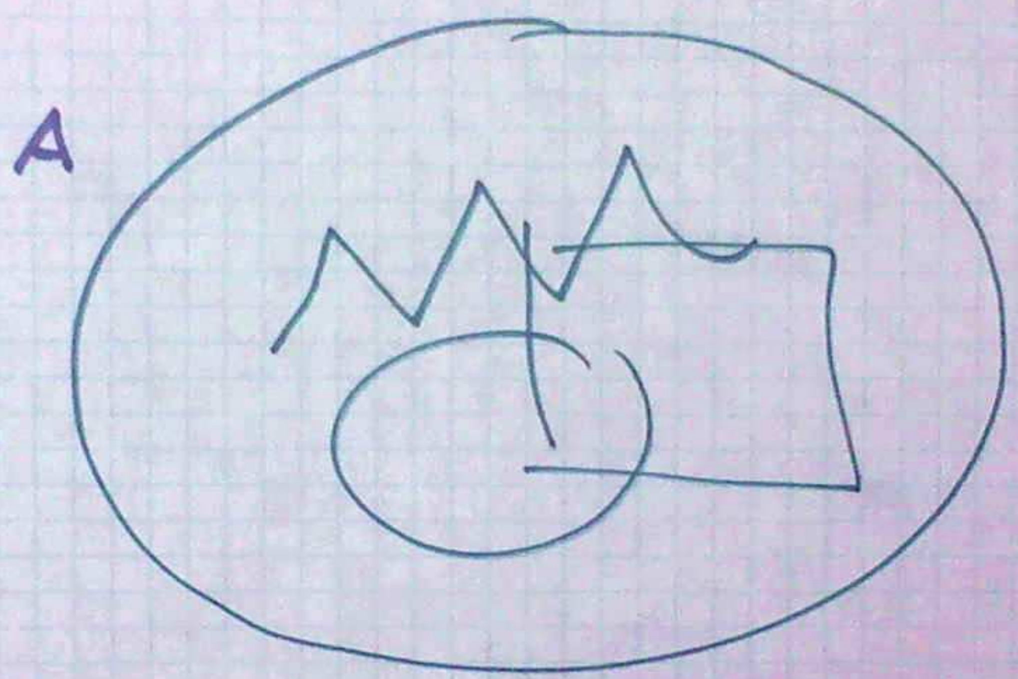
PSEUDOFINITE

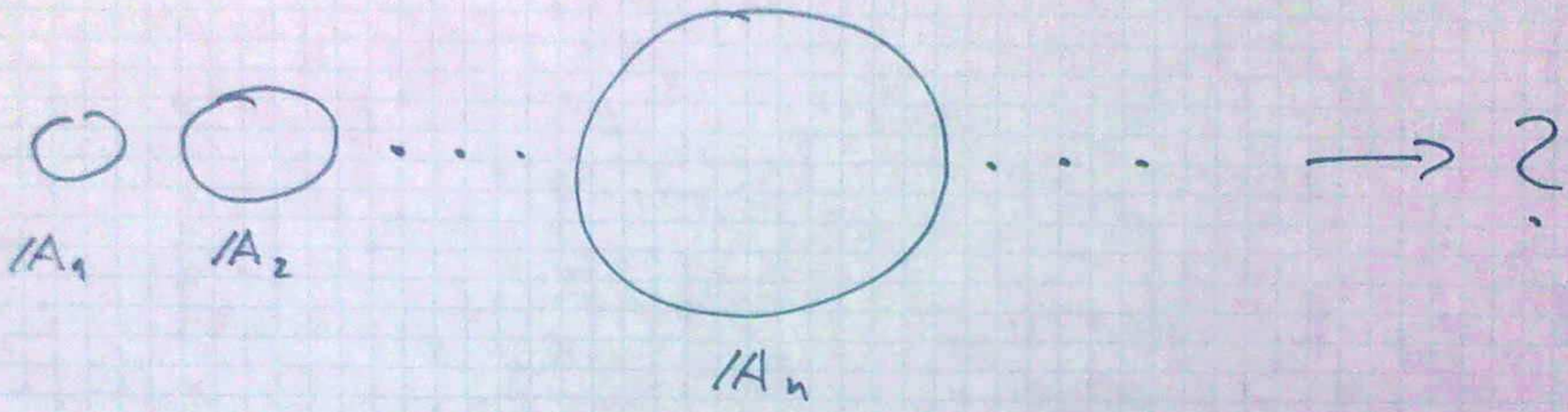
EULER STRUCTURES

Jan Krajíček (KA)

a first-order structure $\mathbb{A}$:

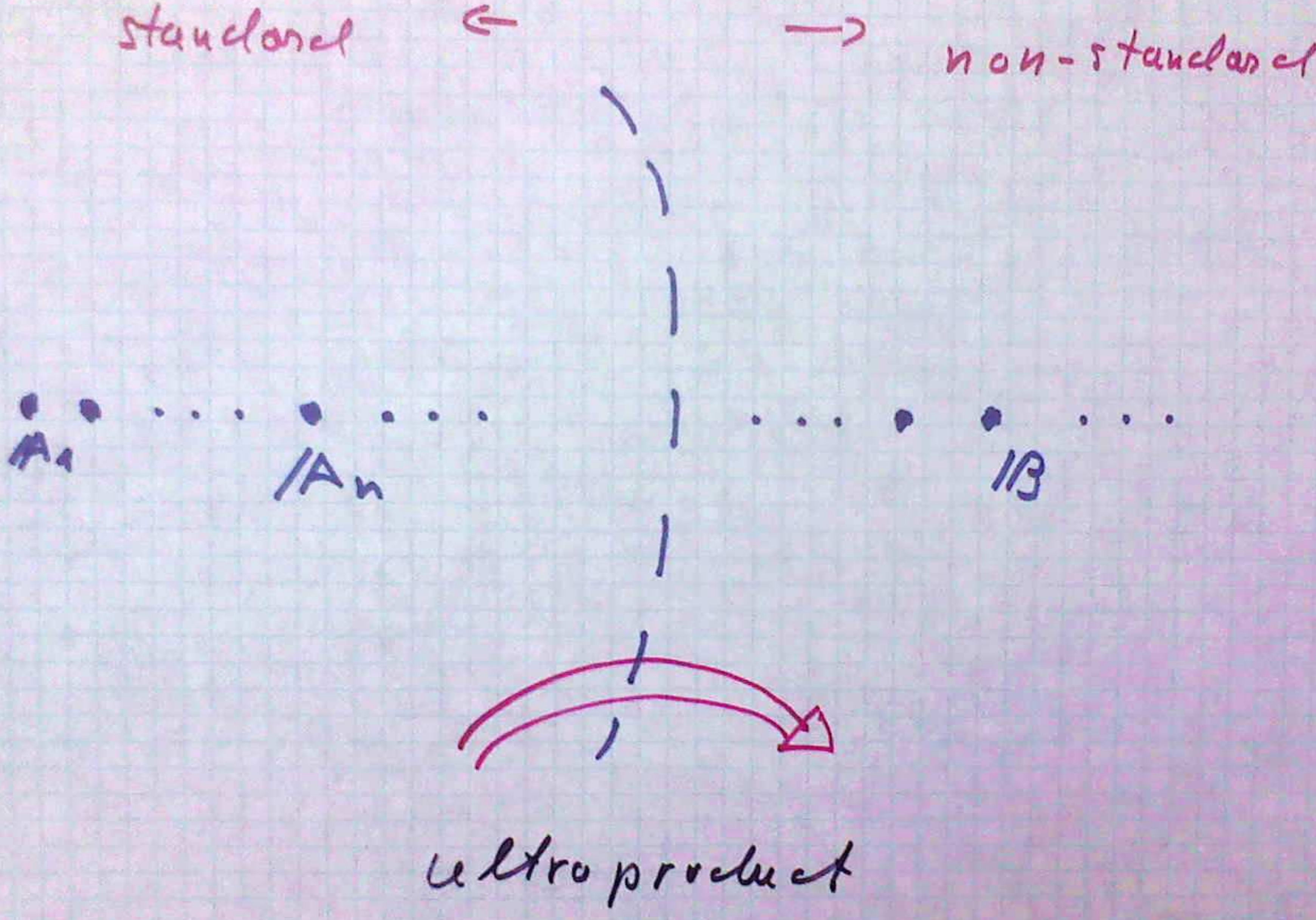


$R(x,y), \ldots, f(u,v,w), \ldots, c, \ldots$



$|\mathbb{A}_n| \geq n$

– asymptotic properties


standard
non-standard
$\mathbb{A}_1$
$\mathbb{A}_n$
$\mathbb{B}$
ultraproduct

infinite $\mathbb{B}$ is pseudofinite (psf.)

$$\Updownarrow \text{def}$$

$$\mathbb{B} \models \varphi \implies \exists \text{ finite } \mathbb{A} \models \varphi$$

$$\Updownarrow \text{easy fact}$$

$\mathbb{B}$ is elem. equivalent to an <u>ultraproduct of finite structures</u>

(our interest)

Counting measure

definable $X \subseteq A_n \longrightarrow \frac{|X|}{n}$ $\quad (n = |A_n|)$

lifted by the ultraproduct

def. $X \subseteq B \longrightarrow \frac{|X|}{N}$ $\quad (N = |B|)$

$\in \mathbb{Q}^*$

non-stand. rational

- $\frac{|X|}{N} \in \mathbb{Q}^* \xrightarrow[\text{standard part}]{st} \mu(X) :=$ the nearest real in $[0,1]$

- μ : countably additive and lifts to a measure : Loeb's measure

FACT : $Z \subseteq [0,1]$ is Lebesgue measurable iff $st^{-1}(Z)$ is Loeb measurable, and the measures agree.

Loeb's measure (& related dimension fact)

has nice applications in:

- combinatorics: regularity lemmas, Szemerédi's thm, Fürstenberg corresp., ...

- linear approx. grps and additive combinatorics

- model theory

[LNs by I. Goldbring, A. Pillay, ...]

Boolean circuits

- inputs $x_1, \dots, x_n$

- intermed. values : $y_1, \dots, y_i, \dots, y_s$

  y_i : $\boxed{\text{easy}}$ to compute from $x_1, \dots, x_n, y_1, \dots, y_{i-1}$

- output : y_s

$\boxed{\text{size} = s}$

P.

- circuit C of size $s \leq n^c$

  easy to encode by a structure on $[n]$
  $= \{1, \dots, n\}$

- But: not so easy to define what it computes

FACT: FO definable property of $U \subseteq [n]$

$$\Updownarrow$$

AC^0-computable property of $U \in \{0,1\}^n$

Ex. $(\mathbb{B}, \mathcal{U})$ psf , $B = [N]$

$f_0 : k \in [N] \longrightarrow$ the parity of $|\mathcal{U} \cap [k]|$

• a (seemingly) contradictory situation (*):

$$\begin{tikzcd}[row sep=small]
 & (\mathbb{B}, \mathcal{U}, f_0) \\
(\mathbb{B}, \mathcal{U}) \arrow[ur] \arrow[dr] & \\
 & (\mathbb{B}, \mathcal{U}, f_1)
\end{tikzcd}$$

• both psf

• but $f_0(N) \neq f_1(N)$

FACT (involves only classic math. logic):

A situation like (*) can arise

$$\Updownarrow$$

parity function $\oplus_n : \{0,1\}^n \longrightarrow \sum_i t_i \bmod 2$

is not AC^0-computable

[Ajtai, Fürst-Saxe-Sipser, ...]

• propositional proof system

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

$\boxed{p\text{-time}}$

- P-proof of τ : any w s.t. $P(w) = \tau$

- **FACT** : $NP = coNP \iff \exists$ pps P with p-size proofs exists

[Cook - Reckhow]

- o structure : may encode a formula, a proof, ...

- A type of a situation $(\dagger)$:

$$(\mathbb{B}, \le, \dots) \longrightarrow (\mathbb{B}, \le, \dots, f)$$

psf — not psf

– $(\mathbb{B}, \le, \dots, f) \models f : [N] \xhookrightarrow[\text{1-to-1}]{} [N-1]$

(PHP fails)

$\models$ LNP for all flas holds

<u>FACT</u> : A situation like (+) can arise

$\Uparrow$

propositional PHP_n formulas have no p-size

proofs in a calculus using only bounded

depth flas

atom

$p_{ij} \rightleftharpoons f(i)=j \quad , \; i \in [n], \; j \in [n-1]$

$\ldots \wedge \bigwedge_{i_1 \neq i_2} \bigwedge_{j} (\neg p_{i_1 j} \vee \neg p_{i_2 j}) \wedge \ldots$

Summary :

- lower bounds in circuit / proof complexity are often equivalent to the existence of expansions of psf - structures with specific properties
- current frontier: $\boxed{\text{violate}}$ · property of $\boxed{\text{counting}}$ while preserving $\boxed{\text{"a lot of" ps-finiteness}}$

EULER STRUCTURES

- $\mathrm{Def}^k(\mathbb{A})$: def. $X \subseteq A^k$, $\mathrm{Def}^\infty(\mathbb{A}) := \bigcup_k \mathrm{Def}^k(\mathbb{A})$

- Euler char. $\chi : \mathrm{Def}^\infty(\mathbb{A}) \to R$: commut. ring with 1_R

  1. $\chi(\emptyset) = 0$, $\chi(\text{singleton}) = 1_R$

  2. $\chi(A \,\dot\cup\, B) = \chi(A) + \chi(B)$

  3. $\chi(A \times B) = \chi(A) \cdot \chi(B)$

  4. $A \xleftrightarrow[\text{def.}]{} B \Rightarrow \chi(A) = \chi(B)$

  $\vdots$

may add more conditions

Ex: $\mathbb{R}(0,1,\leq,+,\cdot)$: the o-minimal real closed field

$\chi : \mathrm{Def}^{\infty}(\mathbb{R}) \longrightarrow \mathbb{Z}$ exists

$\chi((a,b)) = -1$, $\chi(\mathbb{R}) = -1$, ...

Ex: $\mathbb{N}(0,1,+,\cdot,\leq)$: no non-trivial ($0_R \neq 1_R$)

χ / R exists because

$x \longrightarrow x+1$ violates onto PHP

$\exists$ def. bijection between a set and the set minus one point.

FACT : $\mathbb{A}$ admits non-trivial χ/R

$$\Updownarrow$$

$\mathbb{A}$ satisfies ontoPHP.

Variants:

- PHP (no $f : X \leftrightarrow X' \underset{\neq}{\subseteq} X$) $\longleftrightarrow$ $\exists$ part. schem. χ/R
- $WPHP^{2n}_{n}$ (no $f : X \dot\cup X \leftrightarrow X'$) $\longleftrightarrow$ $\exists$ approximate χ/R
- $WPHP^{n^2}_{n}$ (no $f : X^2 \leftrightarrow X$) $\longleftrightarrow$ $\exists$ dimension function.

[Schanuel, K., Scanlon, ...]

Universal construction: for $U, V \in \mathrm{Def}^{\infty}(\mathbb{A})$

$$U \sim V \overset{\text{def.}}{\Longleftrightarrow} \exists W \in \mathrm{Def}^{\infty},\ U \sqcup W \underset{\text{def.}}{\longleftrightarrow} V \sqcup W$$

- $0 := [\emptyset]$, $1 := [\text{singleton}]$
- $+$ and $\cdot$: $\sqcup$ and $\times$
- has cancellation (rig, semiring, ...)

  $\searrow$ definable isomorphisms

$$K_0(\mathbb{A}) := \text{ the Grothendieck ring of } \mathbb{A}$$

Ex.: $K_0(\mathbb{C}(0,1,+,\cdot))$:

- $\cong \mathbb{Z}[2^{\aleph_0} \text{ variables}]$ [K.-Scanlon]

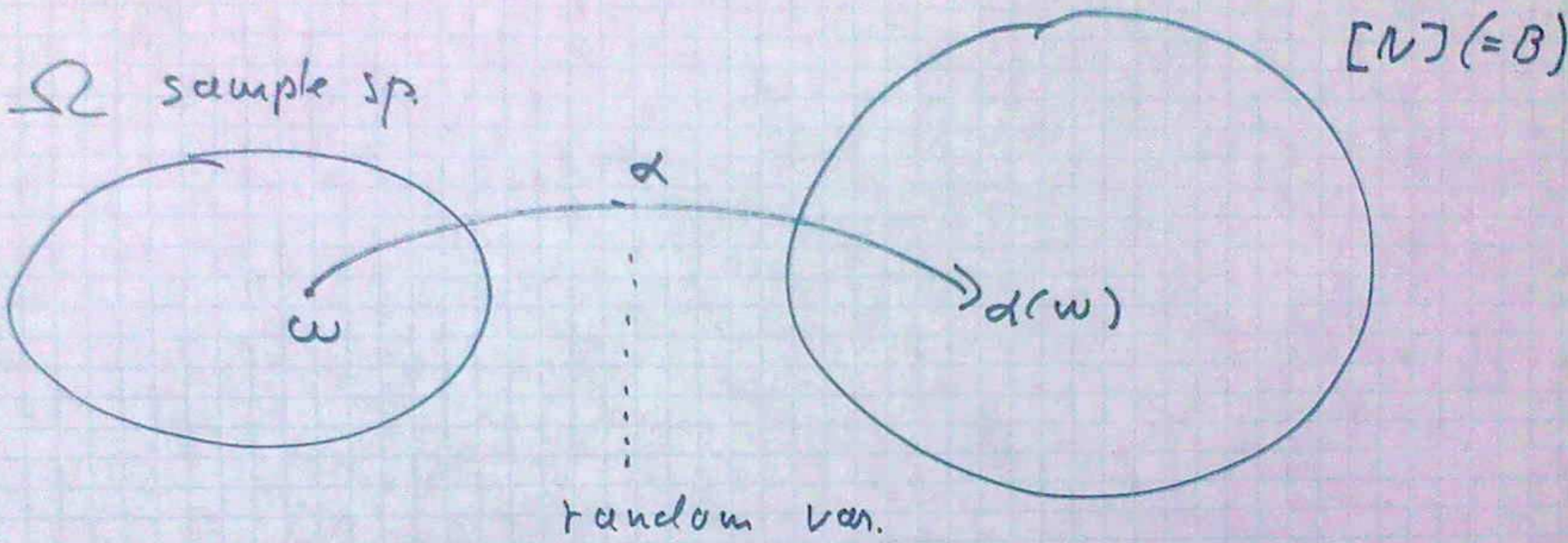
- admits $\mathbb{Z}[u,v]$ as a quotient [Denef-Loeser]

- $\mathbb{B} \models PHP \Rightarrow K_0(\mathbb{B}) \cong \mathbb{Z}[u]$

- $\mathbb{B} \models Count_p \Longrightarrow \mathbb{F}_p$ is a quotient of $K_0(\mathbb{B})$

cannot p-partition $\underbrace{X \cup \dots \cup X}_{p\text{-times}} \cup \{\text{one point}\}$

forcing w/ random variables



F : a family of rand. var's

$K(F)$: a structure w/ universe F

↳ Boolean valued

$$[\![\alpha = \beta]\!] := \{\omega \in \Omega \mid \alpha(\omega) = \beta(\omega)\} \big/ \mathcal{J}$$

the ideal of definable subsets of Ω of an <u>infinitesimal counting measure</u>

$$\mathbb{B} := \left(\mathcal{P}(\Omega) \cap \mathrm{Def}^{\infty}(\mathbb{B})\right) \big/ \mathcal{J}$$

<u>Key fact</u>: $\mathbb{B}$ is a complete Bool. alg.

truth evaluation:

- $[\![\varphi \wedge \psi]\!] := [\![\varphi]\!] \wedge [\![\psi]\!]$

  - same for $\vee, \neg$

- $[\![\exists x\, \varphi(x)]\!] := \bigvee_{\alpha \in F} [\![\varphi(\alpha)]\!]$

- $\ldots \forall \ldots\ldots\ldots \bigwedge \ldots\ldots$

new requirement: $[\![PHP(x)]\!] < 1_{\mathcal{B}}$.

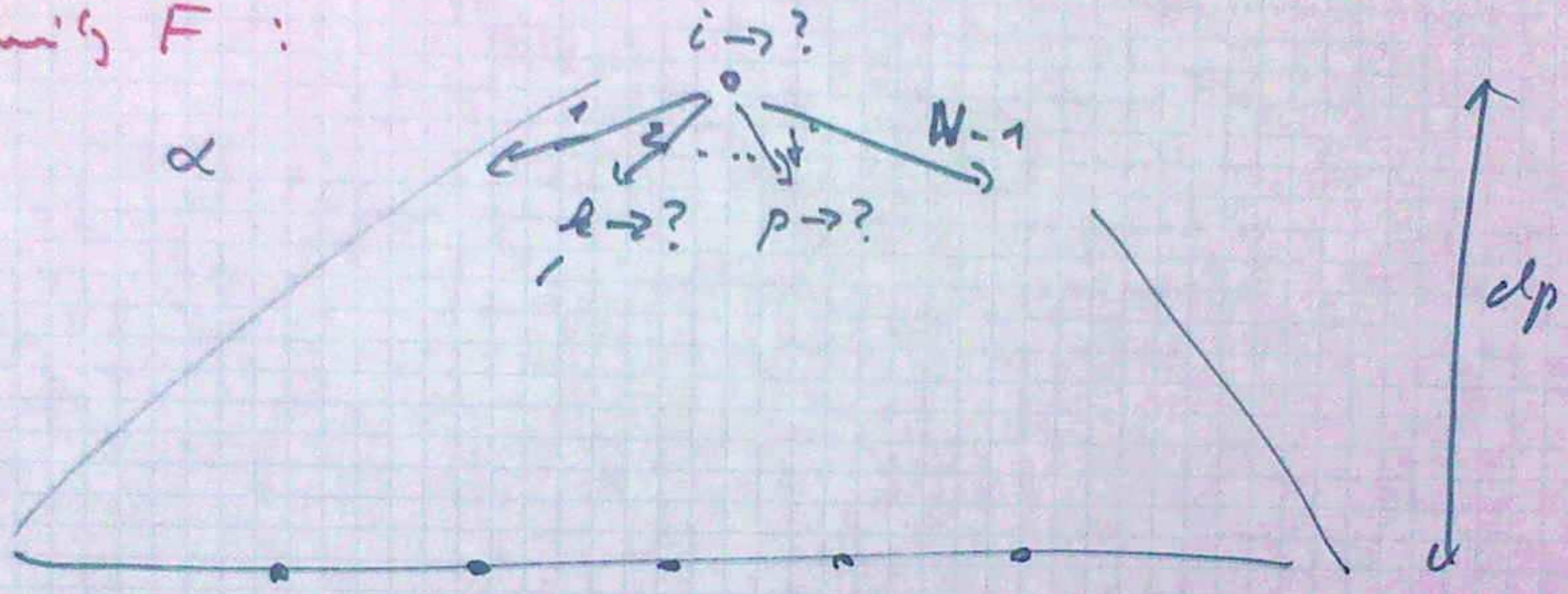
Fact: • φ logically valid $\Rightarrow$ $[\![\varphi]\!] = 1_{\mathcal{B}}$

• $T \models \varphi \Rightarrow \left(\bigwedge_{\psi \in T} [\![\psi]\!] \right) \leq [\![\varphi]\!]$

• $[\![\varphi]\!]$ comes with a standard measure and $\mathcal{B}$ is equipped with a metric "respecting" logic operations

Ex. a model for $\neg PHP$

family F :



leaves labelled by elmts of $[N]$

Ω : $\omega : \subseteq [N] \xhookrightarrow[\text{1-to-1}]{} [N-1]$, $|\omega| = N-1$

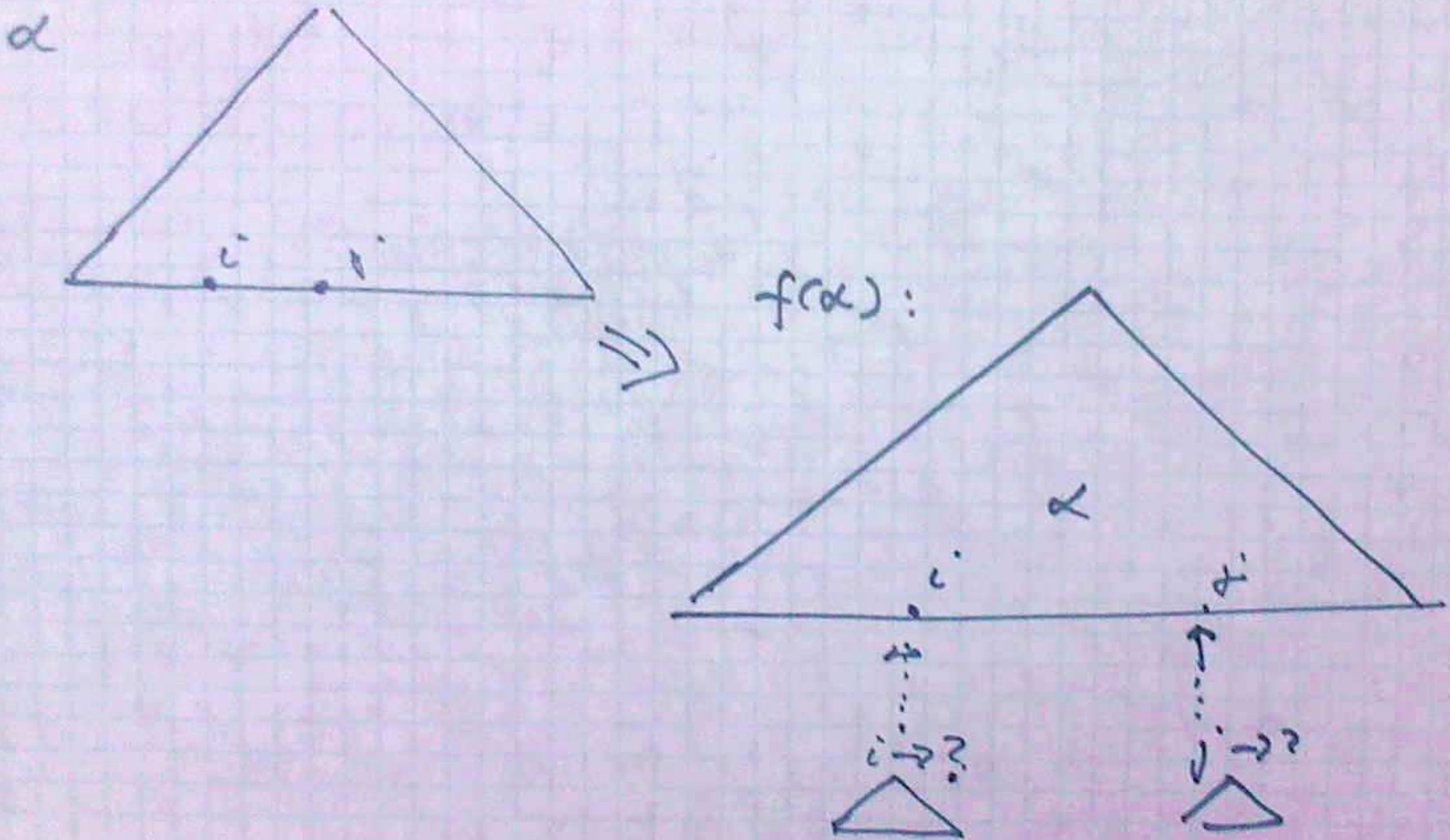
Fact: (i) $\underset{\omega}{\mathrm{Prob}}\left[\alpha(\omega) \text{ undefined}\right] \leq O\left(\frac{dp}{n}\right)$

(ii) dp's closed under $\cdot \log n$ $\Rightarrow$ induction for open fla's is true

(iii) a little bit more subtle set-up :

$\Rightarrow$ quant. elimination is valid and hence IND for all flas (i.e. the LNP too).

a map violating PHP in $K(F)$



$d_p \rightsquigarrow d_p + 1$

we want: $\mu(F)$ with properties as above

but also admitting definable $\mu / \mathbb{F}_2$

- $X \subseteq B^{k+l}$, $\bar{b} \in B^k$, $X_{\bar{b}} \subseteq B^l$ the fiber

then $\mu(X_{\bar{b}})$ is a definable function of $\bar{b}$

needs: F defined by algebraic trees and "suitable" sample set Ω

Refs :

- 2011 book : about the method
- new book / Chapt. 20 : about moral theory
  and complexity

  ↳ offers a number of pointers
  towards relevant ref's.