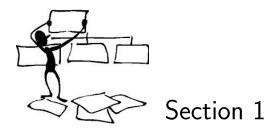
Higher randomness

Benoit Monin - LIAFA - University of Paris VII



Victoria university - 16 April 2014

Introduction



Introduction

The Cantor space

What do we work with ?

Our playground	The Cantor space
Denoted by	2^{ω}
Topology	The one generated by the cylinders $[\sigma]$, the set of sequences extending σ , for every string σ
An open set \mathcal{U} is	A union of cylinders

What does it mean for a binary sequence to be random ?

Intuitively : Is it reasonable to think that c_1, c_2 or c_3 could have been obtained by a fair coin tossing ?

 $c_1:00001100000001000100001000100010100001000100\dots$

What does it mean for a binary sequence to be random ?

Intuitively : Is it reasonable to think that c_1, c_2 or c_3 could have been obtained by a fair coin tossing ?

What does it mean for a binary sequence to be random ?

Intuitively : Is it reasonable to think that c_1, c_2 or c_3 could have been obtained by a fair coin tossing ?

What does it mean for a binary sequence to be random ?

Intuitively : Is it reasonable to think that c_1, c_2 or c_3 could have been obtained by a fair coin tossing ?

Kolmogorov had the idea that our intuition of randomness for finite strings, corresponds to the incompressibility of finite strings.

Definition (Kolmorogov)

For a given machine $M: 2^{<\omega} \to 2^{<\omega}$, the *M*-Kolmorogov complexity $C_M(\sigma)$ of a string σ if the size of the smallest program which outputs σ via M.

Proposition/Definition (Kolmorogov)

There is a machine $U: 2^{<\omega} \to 2^{<\omega}$, universal in the sense that for any machine M we have $C_U(\sigma) \leq C_M(\sigma) + c_M$ with c_M a constant depending on M. The value $C(\sigma) = C_U(\sigma)$ is the **Kolmogorov** complexity of the string σ , well defined up to a constant.

Proposition/Definition (Kolmorogov)

A string σ is *d*-incompressible if $C(\sigma) > |\sigma| - d$. The smallest *d* is, the more random σ is.

How to extend this notion of randomness for strings, to infinite sequences ? A first idea : A sequence X should be random if there is some d so that each prefix of X is d-incompressible.

But that fails, as for any d we have:

 $=\sigma$ with $|\sigma|=d$ $=\tau$ with $|\tau|=\sigma$ seen as an integer

Then the machine $M(\tau) = |\tau|^{\uparrow} \tau$ can *d*-compress some prefix of *X*, for any *d*.

Complexity of sets



Section 2

Complexity of sets

Arithmetical complexity of sets

Following a work started by **Baire** in 1899 (Sur les fonctions de variables réelles), pursued by **Lebesgue** in his PhD thesis (1905), and many others (in particular **Lusin** and his student **Suslin**), we define the **Borel sets** on the Cantor space:

Σ_1^0 sets are	Open sets
${\sf \Pi}_1^0$ sets are	Closed sets
$\mathbf{\Sigma_{n+1}^{0}}$ sets are	Countable unions of Π^0_n sets
${\sf \Pi}_{n+1}^0$ sets are	Complements of $\mathbf{\Sigma}_{n+1}^{0}$ sets

Effectivize the arithmetical complexity of sets (1)

This has latter been effectivized, following a work of **Kleene** and Mostowsky:

Definition (Effectivization of open sets)

A set \mathcal{U} is Σ_1^0 , or **effectively open**, if there is a code *e* for a program enumerating string such that so that \mathcal{U} is the union of the cylinders corresponding to the enumerated strings.

Definition (Effectivization of closed sets)

A set \mathcal{U} is Π_1^0 , or **effectively closed**, if is the complement of a Σ_1^0 set.

Effectivize the arithmetical complexity of sets (2)

We can then continue inductively:
$$\left(\text{Notation} : [W_e] = \bigcup_{\sigma \in W_e} [\sigma] \right)$$

Σ_1^0 sets are	of the form $[W_e]$
Π^0_1 sets are	of the form $[W_e]^c$
Σ_2^0 sets are	of the form $\bigcup_{n \in W_e} [W_n]^c$
Π_2^0 sets are	of the form $\bigcap_{n \in W_e} [W_n]$



Algorithmic randomness

Martin-Löf's intuition

The first satisfactory definition of randomness for infinite sequences has been made by Martin-Löf in 1966.

Intuition

A sequence of 2^{ω} should be random if it belongs to no set of measure 0 (using Lebesgue measure, the uniform measure).

Problem

Any sequence X belongs to the set $\{X\}$, which is of measure 0.

Solution

We can pick countably many sets of measure 0. The effective hierarchy provides a range of natural candidates.

Martin-Löf's definition

Definition (Martin-Löf randomness)

A sequence is **Martin-Löf random** if it belongs to no Π_2^0 set 'effectively of measure 0'. A Π_2^0 set 'effectively of measure 0' is called a **Martin-Löf test**.

Definition (Effectively of measure 0)

An intersection $\bigcap A_n$ of sets is effectively of measure 0 if $\lambda(A_n) \leq 2^{-n}$.

Fact

One can equivalently require that the function $f : n \to \lambda(A_n)$ is bounded by a computable function going to 0.

Why Martin-Löf's definition ?

Question

Why don't we just take Π^0_2 sets of measure 0 ? How important is the 'effectively of measure 0' condition ?

Answer(1)

The 'effectively of measure 0' condition implies that there is a universal **Martin-Löf test**, that is a Martin-Löf test containing all the others.

Answer(2)

It is not true anymore if we drop the 'effectively of measure 0' condition. Instead we get a notion known as **weak-2-randomness**.

We can build a hierachy of randomness notions:

1-random	Every Π_2^0 sets 'effectively of measure 0'
weakly-2-random	Every Π_2^0 sets of measure 0
2-random	Every Π_3^0 sets 'effectively of measure 0'
weakly-3-random	Every Π_3^0 sets of measure 0

We have:

1-random \leftarrow w2-random \leftarrow 2-random \leftarrow w3-random \leftarrow ...

All implications are strict

Introduction Complexity of sets Algorithmic randomness Beyond arithmetic Higher randomness Topological differences

Beyond arithmetic



Beyond arithmetic

Hyperarithmetical complexity of sets

We can extend the definition of Borel sets by induction over the ordinals:

Σ_1^0 sets are	Open sets
Π^0_1 sets are	Closed sets
$\mathbf{\Sigma}_{lpha+1}^{0}$ sets are	Countable unions of ${\sf \Pi}^0_lpha$ sets
$\Sigma^{0}_{\sup_{n} \alpha_{n}}$ sets are	Countable unions of Π^0_β sets for $\beta < \sup_n \alpha_n$
Π^0_{lpha} sets are	Complements of $\mathbf{\Sigma}^{0}_{lpha}$ sets

It is clear that no new sets are define at step ω_1 , by uncountablity of ω_1 . Before that one can prove that the hierarchy is strict.

Effective Hyperarithmetical complexity of sets

How about the effective version ? The challange is to be able to effectively 'unfold' all the components of a Σ^0_{α} set.

(Notation : The set of index *n* is denoted by $\{n\}$)

Σ_1^0 sets are	of the form $[W_e]$	with index	$\langle 0, e angle$
Π^0_{lpha} sets are	of the form $\{e\}^c$	with index	$\langle 1, e angle$
Σ^0_{lpha} sets are	of the form $\bigcup_{n \in W_e} \{n\}$ where n is an index for a Π_{β}^0 set with $\beta < \alpha$	with index	$\langle 2, e \rangle$

Question : At what ordinal α no new set is added in the hierarchy ?

Computable ordinals

Definition (Computable ordinals)

An ordinal α is computable if there is a c.e. well-order $R \subseteq \omega \times \omega$ so that $|R| = \alpha$.

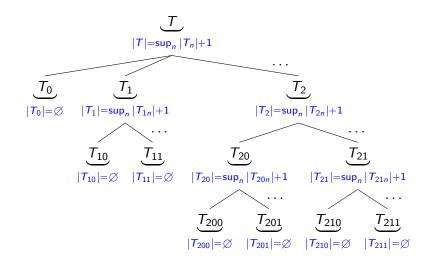
Proposition (Strict initial segment)

The computable ordinals form a strict initial segment of the countable ordinals.

Proposition (well-founded trees)

An ordinal is computable iff it is the order-type of a c.e. well-founded tree (tree with no infinite path).

Order-type of well-founded trees



Computable ordinals and effective Borel sets (1)

Definition (smallest non-computable ordinal)

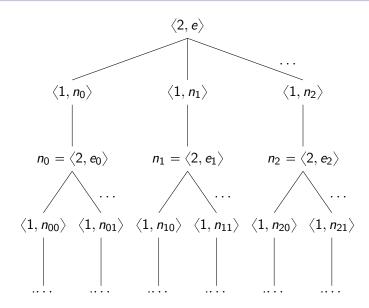
The smallest non-computable ordinal is denoted by $\omega_1^{\rm ck}$, where the ck stands for 'Church-Kleene'.

It is of historical interest to notice that the **Kleene's recursion theorem** has been 'cooked up' to work with codes of computable ordinals. Indeed, the theorem appear for the first time in 1938, in the paper called 'On notation for ordinal numbers'.

Claim

Indices of effective Borel sets are 'essentially' codes for computably enumerable well-founded trees.

Computable ordinals and effective Borel sets (1)



Computable ordinals

It follows that every effective Borel set is Σ_{α}^{0} for $\alpha < \omega_{1}^{ck}$. Again one can prove that the hierarchy is strict before ω_{1}^{ck} .

Definition (Hyperarithmetical sets)

The effective Borel sets are called hyperarithmetical sets.

Every Σ_n^0 set for *n* finite is definable by a first-order formula of arithmetic. It is not the case anymore with Σ_{ω}^0 and beyond. We can however define them with second order formulas of arithmetic.

Analytic and co-analytical sets (1)

Definition (Σ_1^1 sets)

A subset $\mathcal{A} \subseteq 2^{\omega}$ is Σ_1^1 if it can be defined by a formula of arithmetic whose second order quantifiers are only existential (with no negation in front of them).

Definition $(\Pi_1^1 \text{ sets})$

A subset $\mathcal{A} \subseteq 2^{\omega}$ is Π_1^1 if it can be defined by a formula of arithmetic whose second order quantifiers are only univeral (with no negation in front of them).

Definition $(\Delta_1^1 \text{ sets})$

A subset $\mathcal{A} \subseteq 2^{\omega}$ is Δ_1^1 if it is both Σ_1^1 and Π_1^1 .

Analytic and co-analytical sets (2)

Proposition

An effective Borel set is both Σ_1^1 and Π_1^1 .

While this proposition is essentially a tedious but straightforward induction over the computable ordinals, the converse is less tedious but much clever. A non-effective version was first prove by Suslin in 1917 ("Sur une definition des ensembles mesurables B sans nombres transfinis"). Then the effective version was proved much latter (after the effective concepts were introduced) by Kleene in 1955 ('Hierarchies of number theoretic predicates').

Theorem (Suslin, Kleene)

An set is effective Borel iff it is both Σ_1^1 and Π_1^1 .

Analytic and co-analytical sets (3)

Notation

We denote by \boldsymbol{W} the set of codes for computable ordinals, and \boldsymbol{W}^X the set of X-codes for X-computable ordinals. We denote by \boldsymbol{W}_{α} the set of codes for computable ordinals, coding for ordinal strictly smaller than α .

Example : we have
$$\pmb{W}=\pmb{W}_{\pmb{\omega}_1^{ ext{ck}}}$$
 and $\pmb{W}^X=\pmb{W}_{\pmb{\omega}_1^X}$

We now have that the set W, play the same role as \emptyset' , but for Π_1^1 predicates

Theorem (Complete Π_1^1 set)

A set of integers A is Π_1^1 iff there is a computable function $f : \omega \mapsto \omega$ so that $n \in A$ iff $f(n) \in W$.

Analytic and co-analytical sets (4)

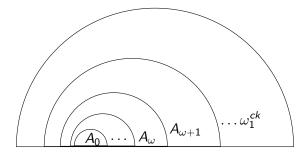
${\cal A}$ is	a set of integer	a set of sequences
Π^1_1	$n \in \mathcal{A} \leftrightarrow f(n) \in W$	$X \in \mathcal{A} \leftrightarrow e \in W^X$
	$n \in \mathcal{A} \leftrightarrow f(n) \in W$ for some computable function f	for some <i>e</i>
Δ^1_1	$n \in \mathcal{A} \leftrightarrow f(n) \in \boldsymbol{W}_{\alpha}$	$X \in \mathcal{A} \leftrightarrow e \in \boldsymbol{W}^X_{lpha}$
	for some computable function f and some computable ordinal α	for some e and some ordinal $lpha$

Π_1^1 sets : Increasing union over the ordinals (1)

Suppose $A \subseteq \omega$ is Π_1^1 with index *e* and let us denote

$$A_{lpha} = \{ n : \varphi_{e}(n) \in W_{lpha} \}$$

Then A is an increasing union of Δ_1^1 sets:

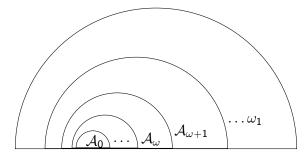


Π_1^1 sets : Increasing union over the ordinals (2)

Suppose $\mathcal{A} \subseteq 2^{\omega}$ is Π_1^1 with index *e* and let us denote

$$\mathcal{A}_{lpha} = \{X : e \in \boldsymbol{W}_{lpha}^X\}$$

Then \mathcal{A} is an increasing union of $\mathbf{\Delta}_1^1$ sets:



An important example of Π_1^1 set of sequences

The set
$$\left\{X \; : \; \omega_1^X > \omega_1^{ck}
ight\}$$
 is a Π_1^1 set :

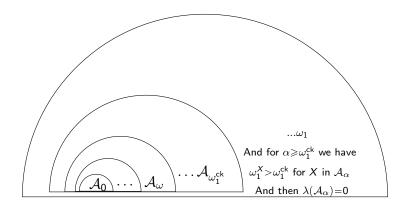
$$\begin{cases} \exists e \in \boldsymbol{W}^X \quad \forall n \quad \forall f \\ X: \quad f \text{ is not a bijection between the relation coded by } n \\ \text{ and the one coded by } e \end{cases}$$

Theorem (Sacks)

The set
$$\{X : \omega_1^X > \omega_1^{ck}\}$$
 is of measure 0.

Consequences of Sacks theorem

Suppose $\mathcal{A} \subseteq 2^{\omega}$ is Π_1^1 with index *e*, we then have :



Higher randomness



Section 5

Higher randomness

Higher randomness

We can now define higher randomness notions

Definition Δ_1^1 -random (Martin-Löf)

A sequence is Δ_1^1 -random if it belongs to no Δ_1^1 set of measure 0.

Definition Π_1^1 -random (Sacks)

A sequence is Π_1^1 -random if it belongs to no Π_1^1 set of measure 0.

What about Σ_1^1 -randomness ?

Theorem (Sacks)

A sequence is Σ_1^1 -random iff it is Δ_1^1 -random

Π_1^1 randomness

Theorem (Keckris, Nies, Hjorth)

There is a universal Π_1^1 set of measure 0, that is one containing all the others.

As the set of $\{X : \omega_1^X > \omega_1^{ck}\}$ is a Π_1^1 set of measure 0. Therefore if something is Π_1^1 -random, then $\omega_1^X = \omega_1^{ck}$. We have a very nice theorem about the converse:

Theorem (Chong, Yu, Nies)

A sequence X is Π_1^1 -random iff it is Δ_1^1 -random and $\omega_1^X = \omega_1^{ck}$.

Another hierarchy (1)

Definition (Π_1^1 open set)

A Π_1^1 open set is an open set \mathcal{U} so that for a Π_1^1 set of strings A we have $\mathcal{U} = \bigcup \{ [\sigma] : \sigma \in A \}.$

Definition (Index for Π_1^1 open set)

For a Π_1^1 open set $\mathcal{U} = \bigcup \{ [\sigma] : f(\sigma) \in \mathbf{W} \}$ with f a computable function, we say that a code e for f is an **index** for \mathcal{U} , and we write $\mathcal{U} = [W_e^{\omega_1^{ck}}].$

Definition (Σ_1^1 closed set)

A Σ_1^1 closed set is the complement of a Π_1^1 open set.

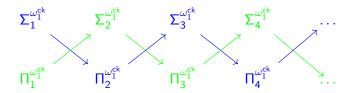
Another hierarchy (2)

We can establish a new hierarchy by taking successive effective union and effective intersection of Π_1^1 open sets and Σ_1^1 closed sets.

$\mathbf{\Sigma}_1^{\omega_1^{ ext{ck}}}$ sets are	Π^1_1 open sets $[W^{\omega^{ck}_1}_e]$	with index	е
-	Σ^1_1 closed sets $[W^{\omega^{ck}_1}_e]^c$	with index	е
$\mathbf{\Sigma}_{n+1}^{\omega_1^{ ext{ck}}}$ sets are	$\bigcup_{m \in W_e} \{m\} \text{ where each } m \text{ is an}$ index for a $\prod_{n=1}^{\omega_1^{ck}}$	with index	е
$\Pi_{n+1}^{\omega_1^{ck}}$ sets are	$\bigcap_{m \in W_e} \{m\} \text{ where each } m \text{ is an}$ index for a $\sum_{n}^{\omega_1^{ck}}$	with index	е

Another hierarchy (3)

Unlike what we have with the other hierarchies, we now have that a $\sum_{n}^{\omega_{1}^{ck}}$ is not necessarily $\sum_{n+1}^{\omega_{1}^{ck}}$:



The blue sets are Π_1^1 sets

The green sets are Σ_1^1 sets

Other higher randomness notions (1)

We can now define:

Definition Π_1^1 -MLR (Hjorth, Nies)

A sequence is Π_1^1 -MLR if it belongs to no $\Pi_2^{\omega_1^{ck}}$ sets effectively of measure 0

Definition weakly- Π_1^1 -random (Nies)

A sequence is strongly- Π_1^1 -MLR if it belongs to no $\Pi_2^{\omega_1^{ck}}$ set of measure 0.

Other higher randomness notions (2)

We cannot straightforwardly continue to define randomness notions along the hierarchy, because for example, Π_3^0 sets of measure 0 are Σ_1^1 sets ($\bigcap_n \bigcup_m F_{n,m}$ where each $F_{n,m}$ is Σ_1^1 closed), and then fail to capture even Π_1^1 -MLR.

And we can however define the notion of being captured by $\Pi_n^{\omega_1^{ck}}$ sets of measure 0 for *n* even. But it collapse for n = 4:

Theorem

A sequence is no $\Pi_4^{\omega_1^{ck}}$ sets of measure 0 iff it is in no Π_1^1 sets of measure 0 iff it is in no $\Pi_n^{\omega_1^{ck}}$ sets of measure 0 for any *n*.

The question has not been investigated for $\Pi_4^{\omega_1^{ck}}$ sets effectively of measure 0.

Other higher randomness notions (3)

What is known:

$$\Delta_{1}^{1} random \leftarrow \Pi_{1}^{1} MLR \leftarrow strongly \Pi_{1}^{1} MLR \leftarrow$$
$$\Pi_{1}^{1} random = `strongly \Pi_{4}^{\omega_{1}^{ck}} MLR'$$

All the implications are strict. The proof of separation between $\Pi_2^{\omega_1^{ck}}\textit{random}$ and $\Pi_1^1\textit{random}$ requires a refinement of the notion of being Δ_2^0 that would not make sense in the lower world.

Higher Δ_2^0 (1)

In the lower case: A Δ_2^0 sequence X:

$$X = \lim_{s \in \omega} X_s$$

we have that $\{X_s\}_{s \leq \omega}$ is a closed set, by definition of convergence

In the higher case: A $\Delta_2^{\omega_1^{ck}}$ sequence X:

$$X = \lim_{s \in \omega_1^{\rm ck}} X_s$$

There is no reason for $\{X_s\}_{s\leqslant \omega_1^{\operatorname{ck}}}$ to be a closed set...

Higher $\overline{\Delta_2^0(2)}$

Definition (closed approximation)

A sequence X has a **closed approximation** if $X = \lim_{s \in \omega_1^{ck}} X_s$ where each X_s is Δ_1^1 uniformly in s and where $\{X_s\}_{s \le \omega_1^{ck}}$ is a closed set.

Definition (wicked approximation)

A sequence X has a **wicked approximation** if $X = \lim_{s \in \omega_1^{ck}} X_s$ where each X_s is Δ_1^1 uniformly in s and where for any $t < \omega_1^{ck}$ we have $X \notin \overline{\{X_s\}_{s \leq t}}$ Introduction Complexity of sets Algorithmic randomness Beyond arithmetic Higher randomness Topological differences

Topological differences



Topological differences

The first Δ_1^1 continuous reduction

In the bottom world, the following four definitions are equivalent:

 $A \ge_T X$

- Phere is a Σ₁⁰ partial map R : 2^{<ω} → 2^{<ω}, consistent on prefixes of A, such that
 ∀n ∃τ < X ∃σ < A |τ| ≥ n ∧ ⟨σ, τ⟩ ∈ R
- There is a Σ₁⁰ partial map R : 2^{<ω} → 2^{<ω}, consistent everywhere, such that
 ∀n ∃τ < X ∃σ < A |τ| ≥ n ∧ ⟨σ, τ⟩ ∈ R
- There is a Σ₁⁰ partial map R : 2^{<ω} → 2^{<ω}, consistent everywhere and closed under prefixes, such that ∀n ∃τ < X ∃σ < A |τ| ≥ n ∧ ⟨σ, τ⟩ ∈ R

The first Δ_1^1 continuous reduction

A first attempt to use continuous version of hyperarithmetic reducibility was made by Hjorth and Nies in order to study higher analogue of Kucera-Gacs and Higher analogue of Base for randomness. They defined fin-h reductions, corresponding to the strongest notion among those defined in the previous slides:

Definition

A fin-h reduction is a Π_1^1 partial map $R: 2^{<\omega} \to 2^{<\omega}$, consistent everywhere and closed under prefixes, such that $\forall n \ \exists \tau < X \ \exists \sigma < A \ |\tau| \ge n \land \langle \sigma, \tau \rangle \in R$

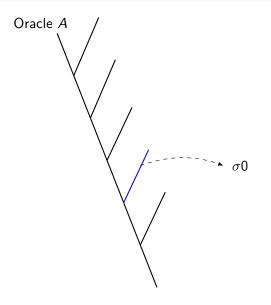
We say that $A \ge_{fin-h} X$ if for a fin-h reduction M we have $\forall n \ \exists \tau < X \ \exists \sigma < A \ |\tau| \ge n \land \langle \sigma, \tau \rangle \in M.$

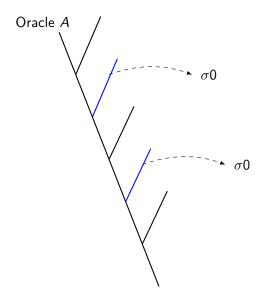
A topological difference

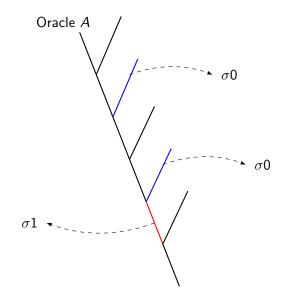
The bottom world	The higher world	
At any time t of the enumera-	At any time α of the enumera-	
tion, the set of strings mapped	tion, the set of strings mapped	
so far is a clopen set	so far is an open set .	

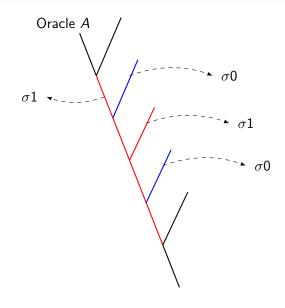
This make the three previous notions different in the higher world.

Oracle A



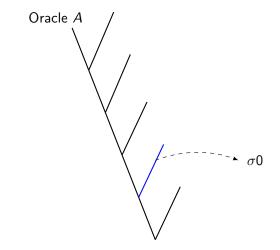






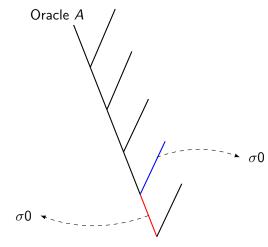
Oracle A

Basic strategy:



Basic strategy: Wait for

the opponent to decide sth. on all the prefixes.

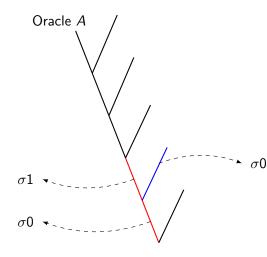


Basic strategy:

Wait for

the opponent to decide sth. on all the prefixes.

Suppose it matches one prefix to $\sigma 0$ as well...



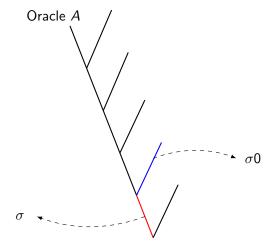
Basic strategy:

Wait for

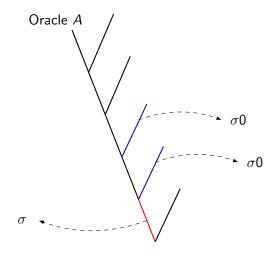
the opponent to decide sth. on all the prefixes.

Suppose it matches one prefix to $\sigma 0$ as well...

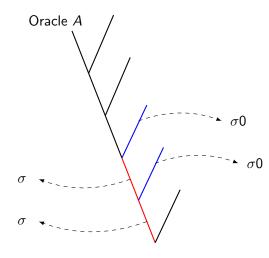
Then you win



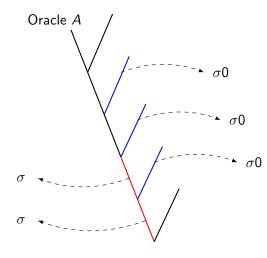
Basic strategy: Wait for the opponent to decide sth. on all the prefixes.



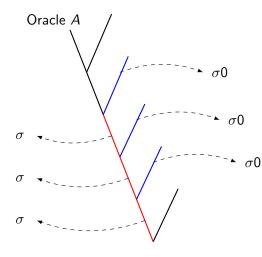
Basic strategy: Wait for the opponent to decide sth. on all the prefixes.



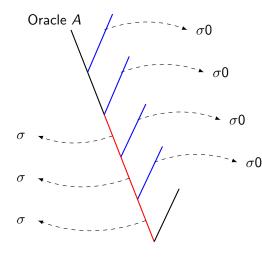
Basic strategy: Wait for the opponent to decide sth. on all the prefixes.



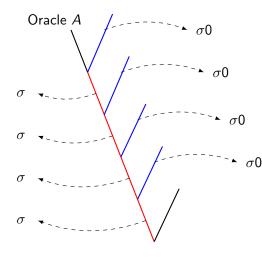
Basic strategy: Wait for the opponent to decide sth. on all the prefixes.



Basic strategy: Wait for the opponent to decide sth. on all the prefixes.



Basic strategy: Wait for the opponent to decide sth. on all the prefixes.

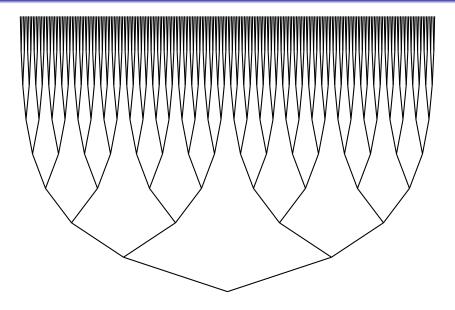


Basic strategy: Wait for the opponent to decide sth. on all the prefixes.

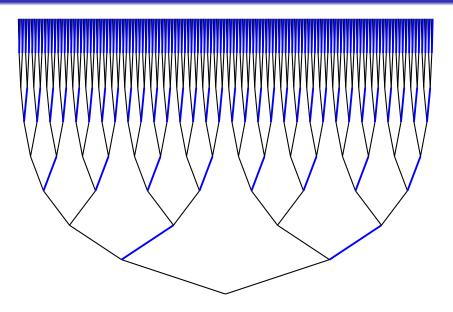
This is only one strategy. The problem is that one machine can force you to pick an entire oracle in order to defeat it. How to continue the construction and defeat other requirements ?

One solution : The perfect treesh-bone !

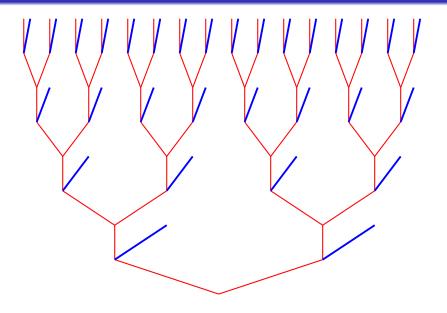
The treesh-bone (1)



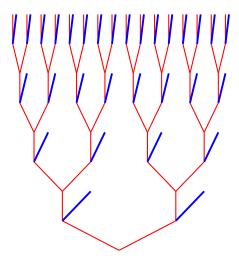
The treesh-bone (2)



The treesh-bone (3)



The treesh-bone (4)



Put σ 0

along all the blue strings

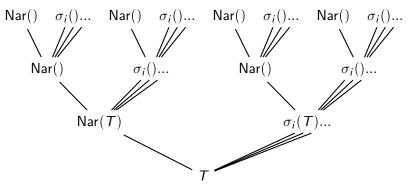
Even if we

are forced to stay along the red part of the tree, we still have a prefect tree that we can continue to work with !

-: Nar(T), The narrow subtree of T-: $\sigma_i(T)$, the subtree of T extending the string σ_i

The tree of trees (1)

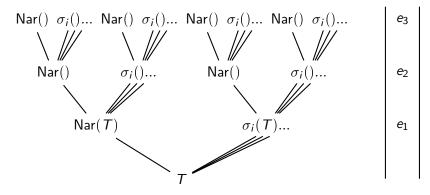
We can imagine that working in a tree of trees.



- The left node of T correspond to Nar(T)
- There is infinitely many right node $\sigma_i(T)$

The tree of trees (2)

We now order the requirement to do a higher finite injury argument:



The Higher Turing reduction

So some consistent map of strings cannot be made equivalent to some consistent map of strings whose domain is closed by prefixes.

Similarly we can prove that if a map of strings, not consistent everywhere, sends X to Y, there is not necessarily a consistent map of strings sending X to Y.

These brings the new definition:

Definition

We say that $A \ge_{\mathcal{T}} B$ if there is a Π_1^1 partial map $R : 2^{<\omega} \to 2^{<\omega}$, consistent on prefixes of A, such that $\forall n \exists \tau < X \ \exists \sigma < A \ |\tau| \ge n \land \langle \sigma, \tau \rangle \in R.$

Oracles for which reductions collapses

For a large class of oracles, in a measure theoretic sense, the three notions of reductions are the same:



Thank you