Construction of random and non-random sets

Kenshi Miyabe, Meiji University
宮部賢志，明治大学

9 Dec 2018 @ SLS2018

Introduction

Goal

The goal of this talk is to give a proof idea of separation between

(i) computable randomness and ML-randomness,
(ii) Schnorr randomness and computable randomness.

These are basic facts in the theory of algorithmic randomness.

Random

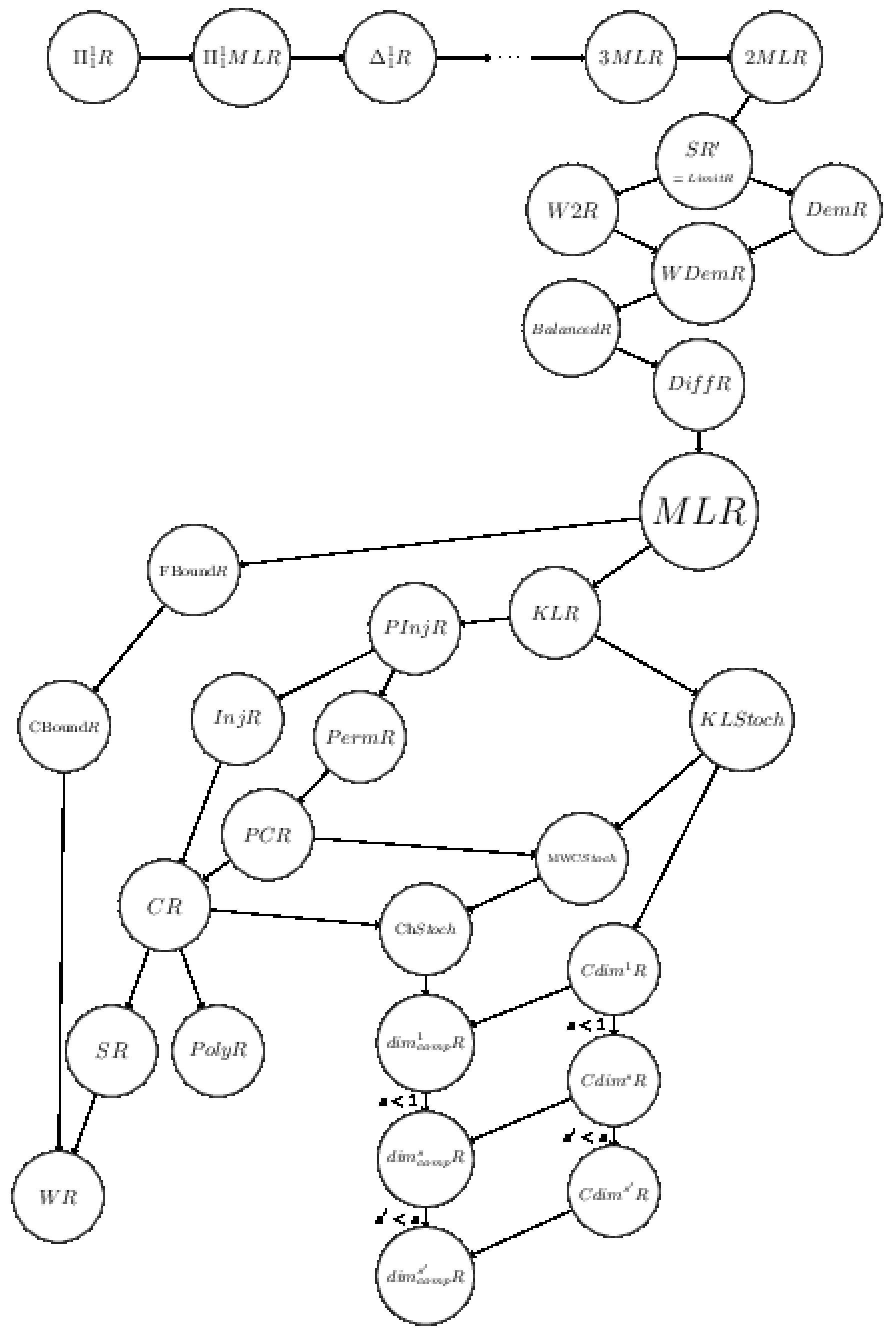
X: an infinite binary sequence or a set of natural numbers

$$0100101101001001101010001011000101010111101001\cdots$$

Seems random, but what mean?

Randomness Zoo

Antoine Taveneaux

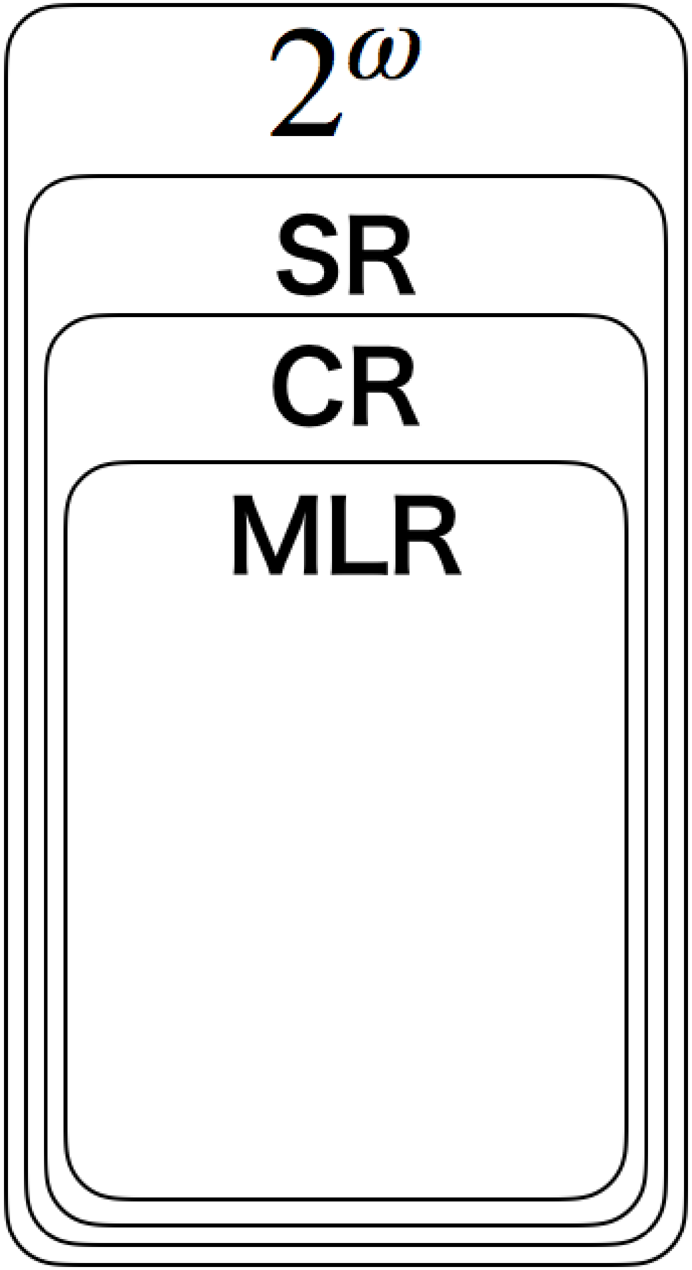


Randomness notions

SR: the class of Schnorr random sets
CR: the class of computably random sets
MLR: the class of Martin-Löf random sets

$$\mathrm{SR} \supsetneq \mathrm{CR} \supsetneq \mathrm{MLR}$$

The first task is to separate the notions.


2^ω
SR
CR
MLR

Martingale

A (super)martingale is a function $M : 2^{<\omega} \to \mathbb{R}^+$ such that

$$M(\sigma) = (\geq) \frac{M(\sigma 0) + M(\sigma 1)}{2}$$

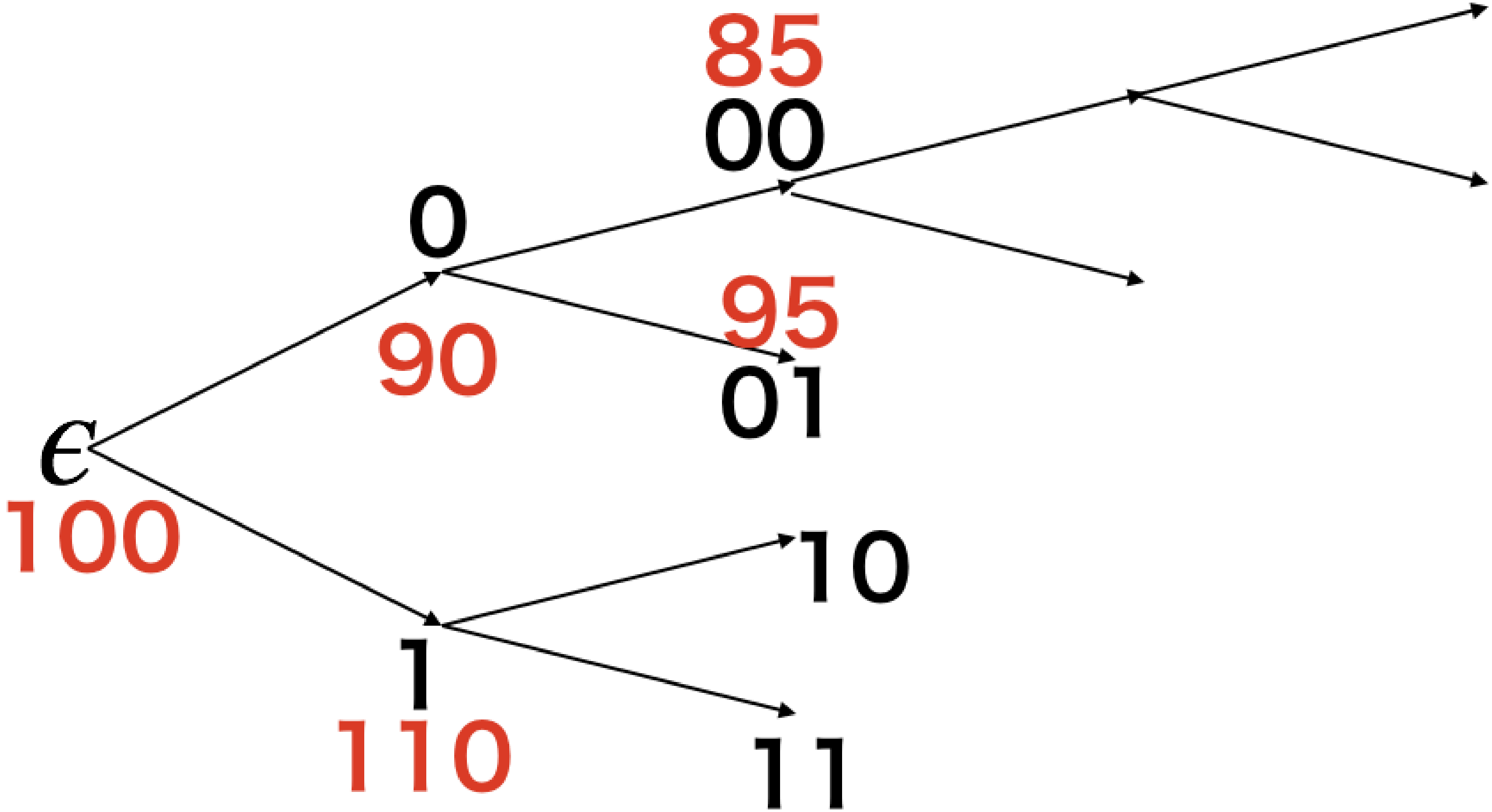
for all $\sigma \in 2^{<\omega}$.

This is called the fairness condition. M is a capital process and the average should be the same as the previous amount.

$x \in \mathbb{R}$ is comp. if $\exists (a_n)_n \in \mathbb{Q}$:comp. s.t. $|a_n - x| < 2^{-n}$.

$x \in \mathbb{R}$ is left-c.e. if $\exists (a_n)_n \uparrow \in \mathbb{Q}$: comp. s.t. $\lim_n a_n = x$.

$f : 2^{<\omega} \to \mathbb{R}^+$ is comp. or left-c.e. if so is $f(\sigma)$ uniformly.



85
00
0
95
90
01
ϵ
100
10
1
110
11

Definition

$X \in 2^\omega$ is ML-random if $\sup_n M(X \restriction n) < \infty$ for each left-c.e. martingale M.
X is computably random if $\sup_n M(X \restriction n) < \infty$ for each computable martingale M.
X is Schnorr random if $M(X \restriction n) < f(n)$ a.a. for each comp. mart. M and each comp. order f.

Random if the capital by any betting strategy is bounded.

Goal

Theorem 1 (Nies-Stephan-Terwijn 2005). *The following are equivalent.*

(i) A *is high.*

(ii) *There is a set* $B \equiv_T A$ *that is computably random but not ML-random.*

(iii) *There is a set* $C \equiv_T A$ *that is Schnorr random but not computably random.*

Construction of computably random sets

Enumerability

Observation 2. *We can computably enumerate all left-c.e. martingales.*
So there exists a universal left-c.e. martingale.
We can not computably enumerate all computable martingales.
We can computably enumerate all partial computable martingales.

Object	Enumerability
partial comp. func.	Yes
total comp. func.	No
left-c.e. mart.	Yes
partial comp. mart.	Yes
comp. mart.	No

ML-randomness

Proposition 3. *There exists a ML-random set.*

Proof. For a universal martingale M, construct a set X so that

$$\sigma_{n+1} = \sigma_n a, \ a \in \{0,1\},$$
$$M(\sigma_n) \geq M(\sigma_{n+1}),$$
$$\sigma_n \preceq \sigma_{n+1} \prec X.$$

With a little trick,

$$X \leq_T M \leq_T \emptyset'$$

□

Computable randomness

Proposition 4. *There exists a computably random set that is not ML-random.*

We need a more delicate method.

(i) Construct a martingale M that multiplicatively dominates all computable martingales.
(ii) Construct a computably random set X from M.
(iii) Construct another martingale N that succeeds along X.

1st try

Define a martingale M by

$$M = \sum_e 2^{-e} M_e$$

where $\{M_e\}$ is a non-effective enumeration of all computable martingales.
Define a set X so that M does not increase along X.
By the non-effectiveness, the Turing degree of M cannot be bounded and X may be really complicated.

2nd try, enumerate

Define a supermartingale M by

$$M = \sum_e 2^{-e} M_e$$

where $\{M_e\}$ is a uniform sequence of all partial computable martingales.
Define a set X so that M does not increase along X.
To compute $X \upharpoonright n$, it suffices to know which $M_e(\sigma)$ is defined.
The number of σ is bounded but not small.
The number of e is unbounded.

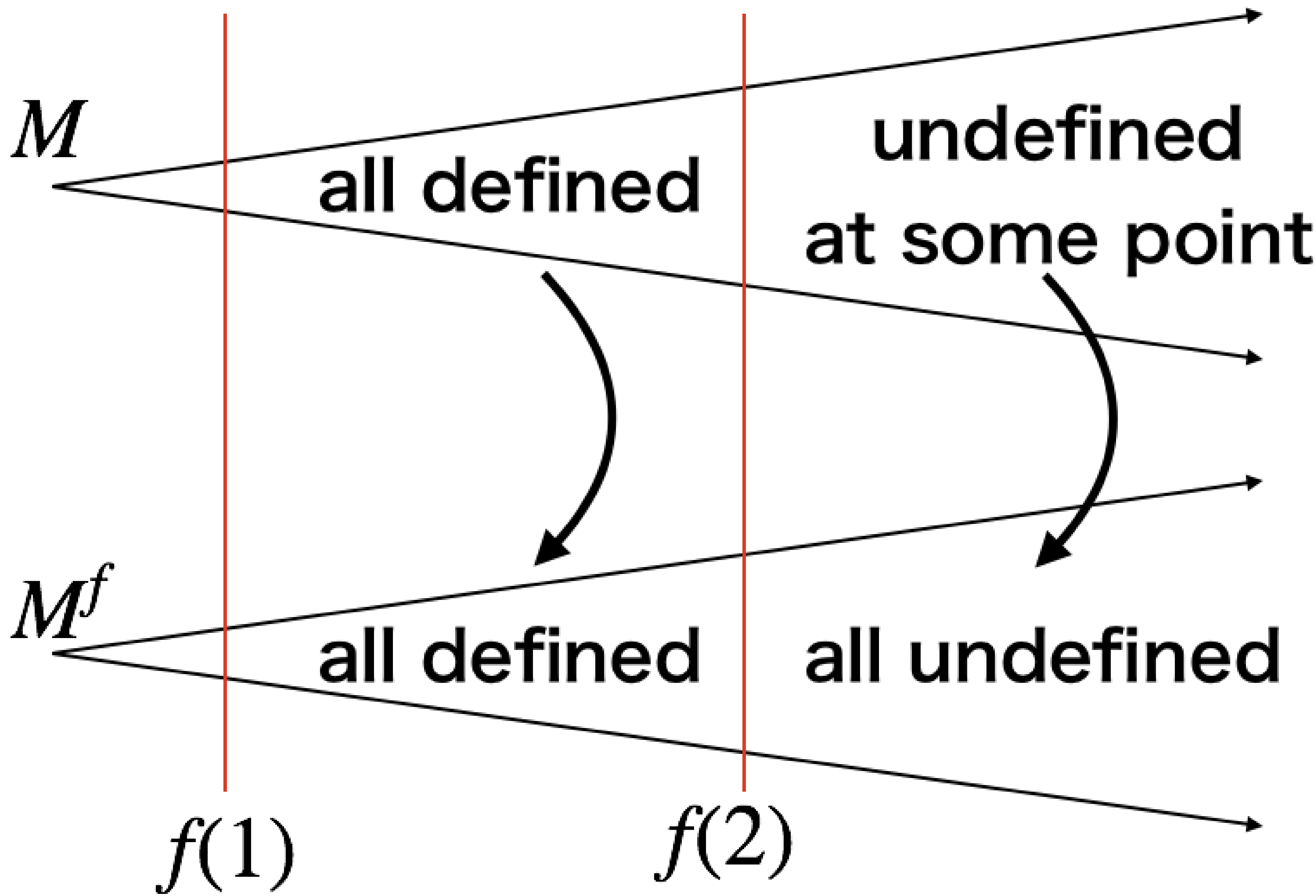
Unite

M: a (maybe partial) computable martingale
f: a computable order
Modify M via f as follows.

$$M^f(\sigma) = \begin{cases} M(\sigma) & \text{if } M(\tau)\downarrow \text{ for all } |\tau| \leq f(n_\sigma) \\ \uparrow & \end{cases}$$

where

$$n_\sigma = \min\{f(k) : \ k \in \mathbb{N}, \ |\sigma| \leq f(k)\}$$



M
all defined
undefined
at some point
M^f
all defined
all undefined
$f(1)$
$f(2)$

Wait

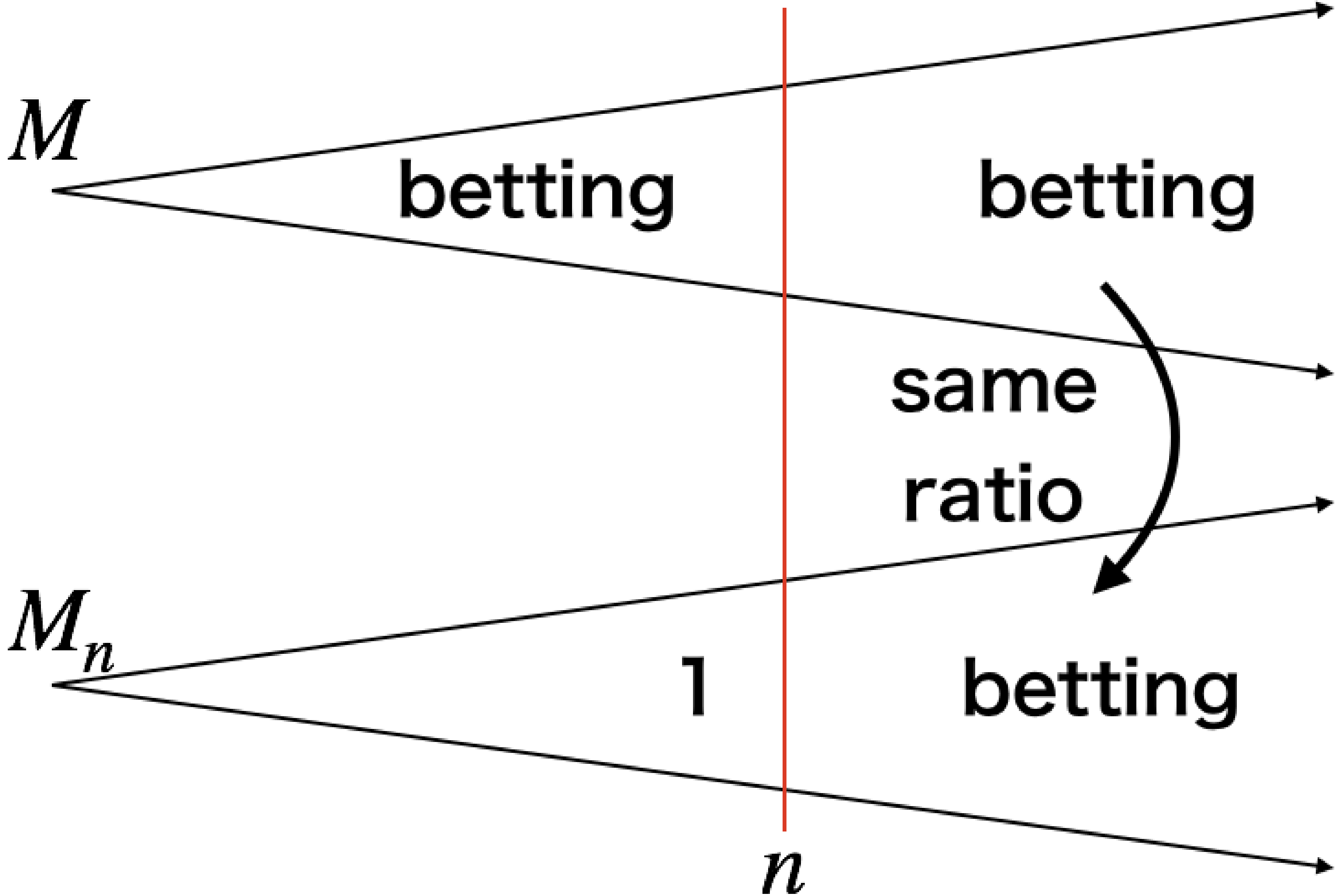
M: a (maybe partial) computable martingale
n: a natural number
Modify M via n as follows.

$$M_n(\sigma) = 1 \text{ for } |\sigma| \leq n$$

($M_n(\sigma)$ is defined even if $M(\sigma)$ is undefined)
and

$$\frac{M_n(\sigma a)}{M_n(\sigma)} = \frac{M(\sigma a)}{M(\sigma)} \text{ for } |\sigma| \geq n$$

($M_n(\sigma)$ is undefined if $M(\sigma)$ is undefined).


M
betting
betting
same
ratio
M_n
1
betting
n

3rd try

f : a computable order (fast growing)
Define a supermartingale M by

$$M = \sum_e 2^{-e} M^f_{e,f(e)}$$

M multiplicatively dominates each $M^f_{e,f(e)}, M_{e,f(e)}, M_e$.
Define a set X so that M does not increase along X.
To compute $X \upharpoonright n$, it suffices to know which $M_e(\sigma)$ is defined.
The number is roughly $(f^{-1}(n))^2/2$, which is much smaller than n.

e	<f(1)	<f(2)	⋯	<f(n)
1	1	1	⋯	1
2	0	1	⋯	1
⋮				
n	0	0	0	1

3rd try (continued)

Hence,

$$K(X \restriction n) \ll n$$

and X is not ML-random.
The computation of $X \restriction n$ is valid only if the input argument is correct.
So we can not replace K with K_M for a decidable machine M.

Some extension

Highness is necessary

Which degree contains a set $X \in \mathrm{CR} \setminus \mathrm{MLR}$?

Theorem 5 (Nies-Stephan-Terwijn 2005)**.** *If a set X is Schnorr random and not high, then X is already ML-random.*

Recall that A is high if and only if A computes a function f that dominates all computable functions.

Highness is sufficient

Proposition 6. *Every high set A computes a computably random set.*

We only care about computable martingales.
M: a computable martingale
$g_M(n)$: the maximum of time to compute $M(\sigma)$ with $|\sigma| \leq n$
Then, g_M is a computable order.

Proof 1

$\{M_e\}$: a uniform sequence of all partial computable martingales
Define a supermartingale M by

$$M(\sigma) = \sum_e 2^{-e} M_{e,e}(\sigma)[f(e + |\sigma|)]$$

Define a set X so that M does not increase along X.

$$X \leq_T M \leq_T f \leq_T A$$

Proof 2

Suppose M_e is a total computable martingale.
f dominates g_{M_e}
$\exists e'$ s.t. $M_e = M'_e$ and $g_{M'_e}(n) \leq f(e' + n)$ for all n.
Since $\sup_n M(X \restriction n)$ is bounded, so is $\sup_n M_e(X \restriction n)$.
Hence, X is computably random.

Encode

To construct a computably random set $X \equiv_T A$, we use Kučera-Gács coding.

Theorem 7 (Kučera '85, Gács '86)**.** *Every set is computable from a ML-random set.*

In particular, for each $A \geq_T \emptyset'$, there exists a ML-random set $X \equiv_T A$.
We skip the details.
By combining all techniques, given a high set A, we can construct a set $X \equiv_T A$ s.t. $X \in \mathrm{CR} \setminus \mathrm{MLR}$.

Construction of Schnorr random sets

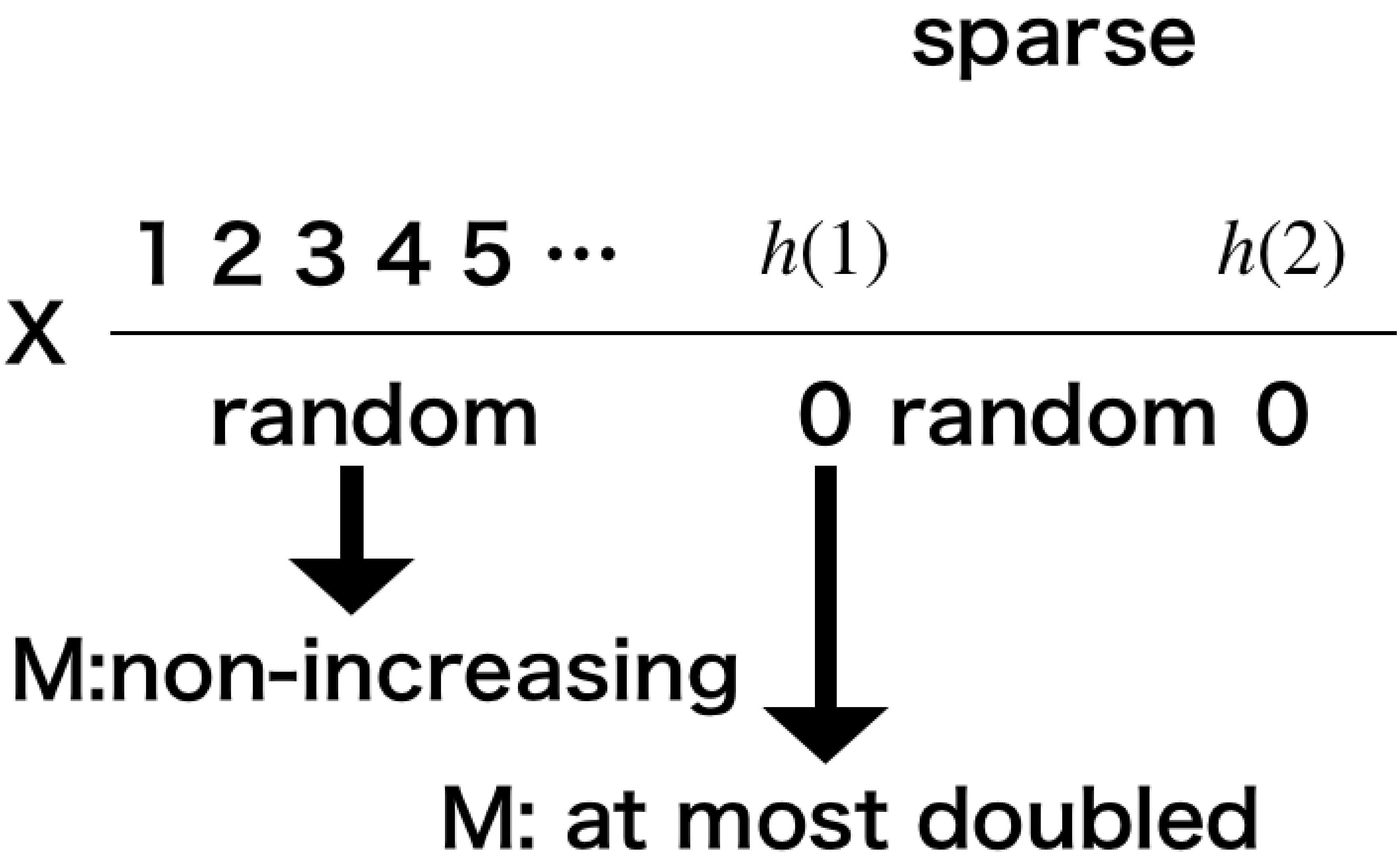
Schnorr randomness

X is computably random if $\sup_n M(X \upharpoonright n) < \infty$ for each computable martingale M.
X is Schnorr random if $M(X \upharpoonright n) < f(n)$ a.a. for each comp. mart. M and each comp. order f.

Proposition 8. *There exists a Schnorr random set X that is not computably random.*

We construct a set X s.t.

(i) every comp. mart. increases more slowly than an comp. order along X.
(ii) some comp. mart. is unbounded along X.


sparse
X
1 2 3 4 5 ⋯
h(1)
h(2)
random
0 random 0
M:non-increasing
M: at most doubled

Mistakes

The function $h(i)$ should be

(i) incomputable so that any computable martingale grows more slowly than any computable order ($\Rightarrow$ Schnorr random)

(ii) computable in some sense so that some computable martingale succeeds ($\Rightarrow$ not computably random)

Idea:

We allow the martingale to make mistakes limited times.

So how many?

Martingale

Martingales can refer to

(i) a tack used to control horses,
(ii) a betting strategy,
(iii) a nonnegative capital process introduced by Ville in 1939 to criticize von Mises,
(iv) a stochastic process developed by Doob in probability theory

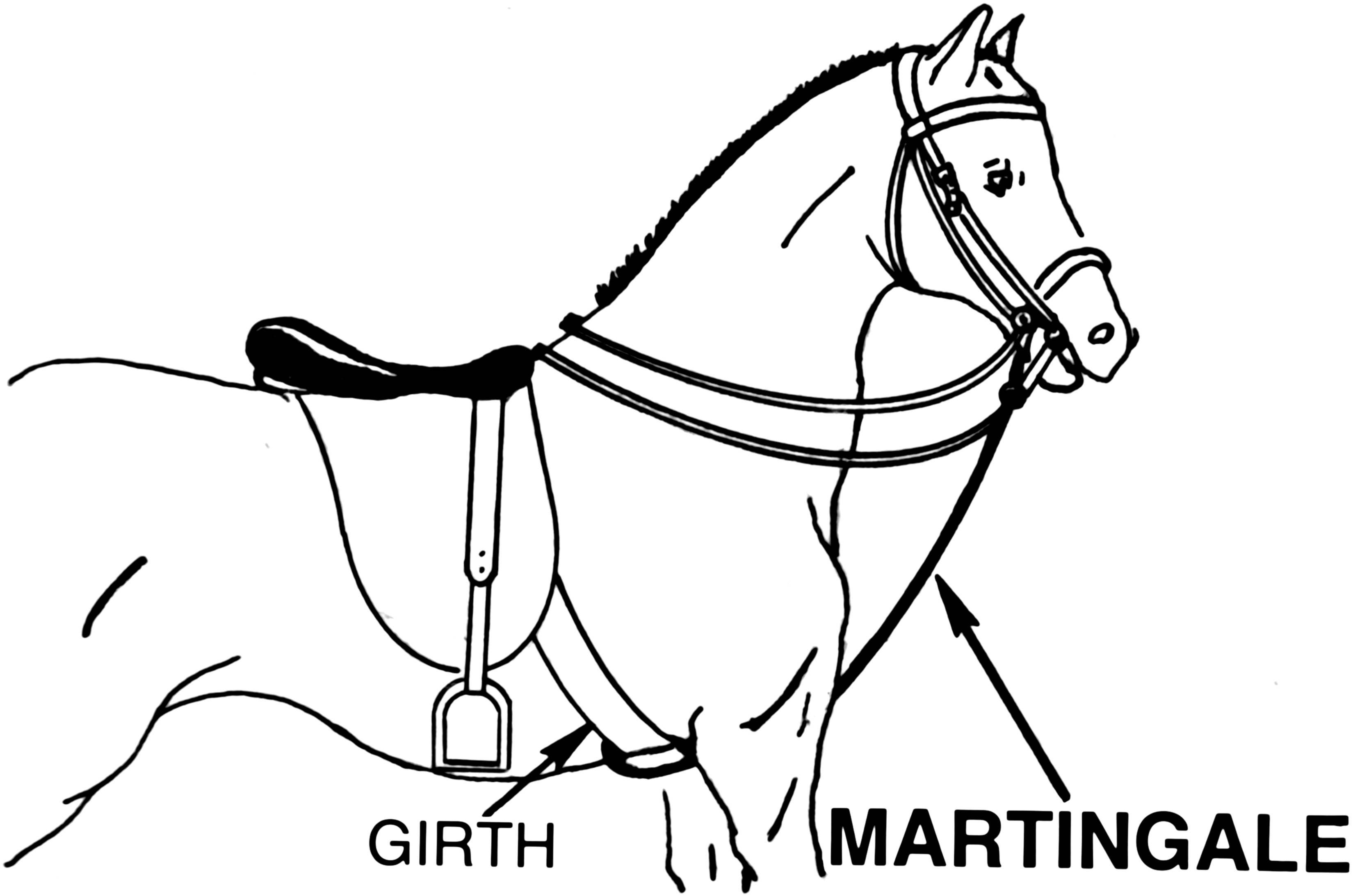


Figure 1: Martingale from wikimedia

Martingale strategy

Martingale strategy:
Is the next bit 0 or 1?
One starts to bet a yen on 0 (or 1).
If lost, then doubles their wager.
Almost surely, one will win eventually, after k-times lost.
The sum of lost capital is

$$a + 2a + 2^2 a + \cdots + 2^{k-1} a = (2^k - 1)a$$

and they will get $2^k a$ by the winning,
so they will gain a yen.
By iterating this, they will gain infinite sum of money.
This is the martingale strategy.

Martingale strategy to work

The martingale strategy does not work in reality.
The number k of lost becomes larger a.s.
With finite initial capital, they will bankrupt eventually.

At n-th round, one starts to bet n^{-1}.
If the number of lost is bounded by $\log n$, then
he sum of lost capital is bounded by

$$\frac{2^k - 1}{n} \leq \frac{2^{\log n} - 1}{n} \leq 1$$

By iterating this, one will gain

$$\sum n^{-1} = \infty$$

Conditions for n

The function h should satisfy the following:

(i) h dominates every computable function.
(ii) $H(x)$ is the set of the candidates of $h(x)$.
(iii) The relation $s \in H(x)$ is computable.
(iv) $|H(x)| \leq \log x$.

We construct such a function n by modifying the busy beaver function.

Busy beaver function

The busy beaver function $BB(x)$ can be defined by

$$BB(x) = \max\{s \ : \ U(\sigma)\downarrow \text{ at } s, \ |\sigma| \leq x\}$$

where U is a universal Turing machine.

$$H(x) = \{s \ : \ U(\sigma)\downarrow \text{ at } s, \ |\sigma| \leq x\}$$

can be the set of the candidates,
and $s \in T(x)$ is a computable relation,
but $|H(x)|$ seems larger than $\log x$.

Modified BB function

$$H(x) = \{\langle e, x, s\rangle + 1 \;:\; \Phi_e(x)\downarrow \text{ at } s,\; e < \log p(x) - 1\}$$

and

$$h(x) = \max\{T(x)\}$$

where p is comp. with $p(x) \leq x$.
h dominates all computable functions.
$t \in H(x)$ is a computable relation.
$|H(x)| \leq \log p(x) - 1$.
At $p(x)$-th round, $H(x)$ will be used.
By filling the gap, we conclude $\exists X \in \mathrm{SR} \setminus \mathrm{CR}$.

Summary

- We gave a proof idea of $\exists X \in \mathrm{CR} \setminus \mathrm{MLR}$.
- The key ideas are to enumerate, unite and wait.
- Highness is the necessary and sufficient degree to compute such sets.
- The Kučera-Gács coding allows us to compute the converse.
- We gave a proof idea of $\exists Y \in \mathrm{SR} \setminus \mathrm{CR}$.
- The key notions are modified versions of the martingale strategy and the busy beaver function.

End

Thank you.