# How powerful are integer-valued martingales?

Laurent Bienvenu (LIAFA, CNRS & Université Paris 7) Based on work of L. Bienvenu, A. Chalcraft, R. Dougherty, C. Freiling, F. Stephan & J. Teutsch

4th Workshop on Game-Theoretic Probability Tokyo, Japan November 13, 2012



The talk is based on the two following papers:

**[BST]** L. Bienvenu, F. Stephan, J. Teutsch. *How powerful are integer-valued martingales?* Theory of Computing Systems, 51(3):330-351, 2012.

**[CDFT]** A. Chalcraft, R. Dougherty, C. Freiling, J. Teutsch. *How to build a probability-free casino*. Information and Computation, 211:160-164, 2012.

1. Randomness = unpredictability

In the previous talks, randomness for infinite binary sequences was discussed, in particular the notion of Martin-Löf randomness.

A sequence  $X \in 2^{\omega}$  is Martin-Löf random iff it avoids every effectively null  $\Pi_2^0$  class iff all its initial segments are incompressible (= have high Kolmogorov complexity).

#### The unpredictability paradigm

Schnorr proposed another approach: an infinite binary sequence *X* is random if no computable gambling strategy makes (a lot of) money by betting on the values of the bits of *X*.

Strategy:

- starts with some finite capital
- at each turn, bets some amount of money between 0 and current capital – on the value of the next bit (e.g. bets \$0.3 on the value 1 for next bit)
- next bit is revealed, the strategy doubles its stake if correct, loses it otherwise
- strategy succeeds if the capital reaches arbitrarily high values throughout the game (i.e. the lim sup of the capital is  $+\infty$ ).

# 



































A strategy can be thought as a function which maps a finite sequence of bits (the sequence of bits already revealed) to a bet, i.e. a 0/1 guess and a stake (any real number between 0 and current capital). This allows us to talk about computable strategies.

A sequence  $X \in 2^{\omega}$  is computably random if there is no computable strategy which succeeds on *X* (with succeeds = reaches arbitrarily high values of capital).

### Computable randomness (2)

Examples of non-computably random sequences:

- computable sequences
- sequences which do not satisfy the law of large numbers
- sequences such that any prefix contains more 0's than 1's
- sequences X such that X(i) = 0 for all *i* power of 2

#### Computable randomness (2)

Examples of non-computably random sequences:

- computable sequences
- sequences which do not satisfy the law of large numbers
- sequences such that any prefix contains more 0's than 1's
- sequences X such that X(i) = 0 for all *i* power of 2

Computable randomness is significantly weaker than Martin-Löf randomness, but is sufficient to capture most classical probability laws.

Recently, it was shown by Brattka, Miller, Nies that it has strong connections with computable analysis (differentiability).

2. Integer-valued strategies

In any "real-world" situation involving gambling, the money is discrete, i.e. the values of possible bets are all multiples of an "atomic" value (one cent, one token, etc.).

Therefore, it makes sense to look at integer-valued strategies. We call  $\mathbb{N}$ -random a sequence *X* such that no computable integer-valued strategy succeeds on *X*.

In any "real-world" situation involving gambling, the money is discrete, i.e. the values of possible bets are all multiples of an "atomic" value (one cent, one token, etc.).

Therefore, it makes sense to look at integer-valued strategies. We call  $\mathbb{N}$ -random a sequence *X* such that no computable integer-valued strategy succeeds on *X*.

Does this give a weaker notion?

Computable  $\mathbb N$ -valued strategies are much weaker than real-valued ones, in the sense that they can be defeated more easily.

Computable  $\mathbb{N}$ -valued strategies are much weaker than real-valued ones, in the sense that they can be defeated more easily.

How to defeat a computable **real-valued** strategy? One possibility: at each step, if the strategy guesses 0, put a 1, if the strategy guesses 1, put a 0. Computable  $\mathbb{N}$ -valued strategies are much weaker than real-valued ones, in the sense that they can be defeated more easily.

How to defeat a computable **real-valued** strategy? One possibility: at each step, if the strategy guesses 0, put a 1, if the strategy guesses 1, put a 0.

We can extend this technique to a finite number of strategies: indeed *n* strategies together can be thought as a single player. Computable  $\mathbb{N}$ -valued strategies are much weaker than real-valued ones, in the sense that they can be defeated more easily.

How to defeat a computable **real-valued** strategy? One possibility: at each step, if the strategy guesses 0, put a 1, if the strategy guesses 1, put a 0.

We can extend this technique to a finite number of strategies: indeed *n* strategies together can be thought as a single player.

One typically builds computably random reals by diagonalization, adding more and more strategies.

# $\mathbb{N}$ -valued strategies are weak (2)

For  $\mathbb{N}$ -valued strategies, the situation is even better: one can completely defeat any given strategy after **finitely many bets**.

# $\mathbb{N}$ -valued strategies are weak (2)

For  $\mathbb{N}$ -valued strategies, the situation is even better: one can completely defeat any given strategy after **finitely many bets**.

Suppose we want to defeat an  $\mathbb{N}$ -valued strategy *S* which has already seen some finite sequence  $\sigma$  of bits. There are two cases:

- either *S* does not make any bet (= stake 0) on any extension of  $\sigma$ . In that case, *S* is dormant and is defeated no matter what extension of  $\sigma$  we choose.
- or S bets on some extension τ of σ, we pick the shortest such τ, and chose the extension τ0 if the strategy guesses 1 and the extension τ1 if the strategy guesses 0. This causes the strategy to lose at least 1.

# $\mathbb{N}$ -valued strategies are weak (2)

For  $\mathbb{N}$ -valued strategies, the situation is even better: one can completely defeat any given strategy after **finitely many bets**.

Suppose we want to defeat an  $\mathbb{N}$ -valued strategy *S* which has already seen some finite sequence  $\sigma$  of bits. There are two cases:

- either *S* does not make any bet (= stake 0) on any extension of  $\sigma$ . In that case, *S* is dormant and is defeated no matter what extension of  $\sigma$  we choose.
- or S bets on some extension τ of σ, we pick the shortest such τ, and chose the extension τ0 if the strategy guesses 1 and the extension τ1 if the strategy guesses 0. This causes the strategy to lose at least 1.

We repeat this process. The second case cannot happen infinitely often, so eventually the strategy is either broke or "gives up".

In a diagonalization, this technique gives the opportunity to treat  $\mathbb N\text{-valued}$  strategies one after the other, instead of all at the same time.

In a diagonalization, this technique gives the opportunity to treat  $\mathbb N\text{-valued}$  strategies one after the other, instead of all at the same time.

What we just proved is that for every  $\mathbb{N}$ -valued strategy *S*, there exists a dense open set of sequences that defeat *S*. Since there are only countably many computable such strategies, this shows that the set of  $\mathbb{N}$ -random sequences is co-meager.

In a diagonalization, this technique gives the opportunity to treat  $\mathbb N\text{-valued}$  strategies one after the other, instead of all at the same time.

What we just proved is that for every  $\mathbb{N}$ -valued strategy *S*, there exists a dense open set of sequences that defeat *S*. Since there are only countably many computable such strategies, this shows that the set of  $\mathbb{N}$ -random sequences is co-meager.

This is very large. For example the set of sequences that satisfy the Law of Large Numbers is meager.
## $\mathbb{N}$ -randomness and category (2)

We can look at effective versions of category.

We can look at effective versions of category.

A sequence  $X \in 2^{\omega}$  is is weakly *n*-generic if for every **dense**  $\Sigma_1^0(\emptyset^{(n-1)})$  set  $\mathcal{U}, X$  belongs to  $\mathcal{U}$ .

We can look at effective versions of category.

A sequence  $X \in 2^{\omega}$  is is weakly *n*-generic if for every **dense**  $\Sigma_1^0(\emptyset^{(n-1)})$  set  $\mathcal{U}$ , X belongs to  $\mathcal{U}$ .

*X* is *n*-generic if for every  $\Sigma_1^0(\emptyset^{(n-1)})$  set  $\mathcal{U}$ , *X* is either in  $\mathcal{U}$  or in the interior of the complement of  $\mathcal{U}$ .

We can look at effective versions of category.

A sequence  $X \in 2^{\omega}$  is is weakly *n*-generic if for every **dense**  $\Sigma_1^0(\emptyset^{(n-1)})$  set  $\mathcal{U}$ , X belongs to  $\mathcal{U}$ .

*X* is *n*-generic if for every  $\Sigma_1^0(\emptyset^{(n-1)})$  set  $\mathcal{U}$ , *X* is either in  $\mathcal{U}$  or in the interior of the complement of  $\mathcal{U}$ .

For all *n*, weakly-(n + 1)-generic  $\Rightarrow$  *n*-generic  $\Rightarrow$  weakly-*n*-generic.

### $\mathbb{N}$ -randomness and category (3)

How much genericity is needed to guarantee  $\mathbb{N}$ -randomness?

How much genericity is needed to guarantee  $\mathbb{N}$ -randomness?

### Theorem (BST)

Any weakly-2-generic sequence X is  $\mathbb{N}$ -random. This does not hold anymore with 1-genericity in place of weak-2-genericity.

There is another well-known "randomness" notion whose corresponding class of random reals is co-meager: Kurtz randomness. A sequence *X* is Kurtz random if it belongs to every  $\Sigma_1^0$  set of measure 1. Since a  $\Sigma_1^0$  of measure 1 must be dense, any 1-generic sequence is Kurtz random.

So Kurtz random does not imply  $\mathbb N$ -randomness, but does the reverse implication hold?

There is another well-known "randomness" notion whose corresponding class of random reals is co-meager: Kurtz randomness. A sequence *X* is Kurtz random if it belongs to every  $\Sigma_1^0$  set of measure 1. Since a  $\Sigma_1^0$  of measure 1 must be dense, any 1-generic sequence is Kurtz random.

So Kurtz random does not imply  $\mathbb N$ -randomness, but does the reverse implication hold?

We show that it is not the case.

To prove this, we use a characterization of Kurtz randomness in terms of strategies.

#### Theorem (Wang)

A sequence X is **not** Kurtz random if and only if there is a computable real-valued strategy S and a computable non-decreasing unbounded function h such that the capital of S after n bets on X is at least h(n).















It is sufficient to build a computable probability measure  $\mu$  such that when choosing *X* at random w.r.t.  $\mu$ :

- With  $\mu$ -probability 1, *X* is  $\mathbb{N}$ -random
- With μ-probability 1, *X* is not Kurtz random

Idea: we use generalized Bernoulli measures. These are the measures we get when for all *i* the *i*-th bit is chosen at random independently of the others, but with probablity  $1/2 + \delta_i$  to be 0.

### $\mathbb{N}$ -randomness vs Kurtz randomness (3)

A result of Bienvenu and Merkle (after Muchnik): If  $\sum_i \delta_i^2 = +\infty$ , then with  $\mu$ -probability 1, *X* is not Kurtz random. Indeed, the **optimal strategy** which for all *i* guesses that the *i*-th bit will be 0 and bets a fraction  $2\delta_i$  of its capital will make money steadily, ensuring that *X* not Kurtz random.

### $\mathbb{N}$ -randomness vs Kurtz randomness (3)

A result of Bienvenu and Merkle (after Muchnik): If  $\sum_i \delta_i^2 = +\infty$ , then with  $\mu$ -probability 1, *X* is not Kurtz random. Indeed, the **optimal strategy** which for all *i* guesses that the *i*-th bit will be 0 and bets a fraction  $2\delta_i$  of its capital will make money steadily, ensuring that *X* not Kurtz random.

Also, if a strategy S' **bets too much** on the *i*-th bit (stake  $\gg$  fraction  $2\delta_i$  of the capital), **then it loses quickly**.

### $\mathbb{N}$ -randomness vs Kurtz randomness (3)

A result of Bienvenu and Merkle (after Muchnik): If  $\sum_i \delta_i^2 = +\infty$ , then with  $\mu$ -probability 1, *X* is not Kurtz random. Indeed, the **optimal strategy** which for all *i* guesses that the *i*-th bit will be 0 and bets a fraction  $2\delta_i$  of its capital will make money steadily, ensuring that *X* not Kurtz random.

Also, if a strategy S' **bets too much** on the *i*-th bit (stake  $\gg$  fraction  $2\delta_i$  of the capital), **then it loses quickly**.

Idea: take the  $\delta_i$  such that  $\sum_i \delta_i^2 = +\infty$  but sufficiently small in such a way that any strategy wins very slowly, and hence, for an  $\mathbb{N}$ -valued strategy, betting 1 or more at stage *i* is too costly. One can take

$$\delta_i = (i \log i)^{-1/2}$$

3. Bounding the bets

In many situations, on top of being discrete, the set of possible bets is bounded (hence finite). If  $\mathcal{V}$  is a finite set of integers, we call  $\mathcal{V}$ -random a sequence *X* which defeats all computable martingales which are only allowed to bet amounts of money belonging to  $\mathcal{V}$ .

In many situations, on top of being discrete, the set of possible bets is bounded (hence finite). If  $\mathcal{V}$  is a finite set of integers, we call  $\mathcal{V}$ -random a sequence *X* which defeats all computable martingales which are only allowed to bet amounts of money belonging to  $\mathcal{V}$ .

Does this too make a difference?

In many situations, on top of being discrete, the set of possible bets is bounded (hence finite). If  $\mathcal{V}$  is a finite set of integers, we call  $\mathcal{V}$ -random a sequence *X* which defeats all computable martingales which are only allowed to bet amounts of money belonging to  $\mathcal{V}$ .

Does this too make a difference?

Yes:

#### Theorem (BST)

For any finite set  $\mathcal{V}$ ,  $\mathcal{V}$ -randomness is weaker than  $\mathbb{N}$ -randomness.

Idea of the proof: we split the set of integers (positions of bits) into consecutive blocks. Start with 1 block of length 1, then 2 blocks of length 2, 4 blocks of length 3 and so on, i.e.  $2^n$  intervals of length n + 1 for all n in order.

We make sure that  $X \in 2^{\omega}$  satisfies the condition

For any block *B*, there is an  $i \in B$  such that X(i) = 0 (\*)

# $\mathbb{N}$ -randomness vs $\mathcal{V}$ -randomness (2)

Any *X* satisfying the condition (\*) can be defeated by an  $\mathbb{N}$ -valued strategy. Use the D'Alembert martingale on each block: first bet \$1 on value 0, and every time one loses, double the stake on the next bit. This guarantees a gain of \$1 per block, and thus a gain of  $2^n$  on the set of blocks of length n + 1. This is enough to ensure that the strategy has enough money to play the D'Alembert martingales on blocks of length n + 2.

Any *X* satisfying the condition (\*) can be defeated by an  $\mathbb{N}$ -valued strategy. Use the D'Alembert martingale on each block: first bet \$1 on value 0, and every time one loses, double the stake on the next bit. This guarantees a gain of \$1 per block, and thus a gain of  $2^n$  on the set of blocks of length n + 1. This is enough to ensure that the strategy has enough money to play the D'Alembert martingales on blocks of length n + 2.

However, a strategy which is only allowed bounded bets cannot use the D'Alembert martingale, and in fact it is not too hard to diagonalize against all  $\mathcal{V}$ -valued strategies while enforcing condition (\*).

# The importance of $\mathcal{V}$ (1)

Ok, putting a bound on the bets makes a difference, but does the set of allowed values matter itself?

# The importance of $\mathcal{V}$ (1)

Ok, putting a bound on the bets makes a difference, but does the set of allowed values matter itself?

Example: three players are betting on a sequence *X*.

- Asuka can make bets in  $\mathcal{A} = \{0, 1, 2, 3, 4, 5\}$
- Bachiko can make bets in  $\mathcal{B} = \{1, 2, 3, 4, 10, 20\}$
- Chihiro can make bets in  $\ensuremath{\mathfrak{C}}=\{0,2,4,6,8,10,15\}$

Does any of the players have an advantage?

# The importance of $\mathcal{V}$ (1)

Ok, putting a bound on the bets makes a difference, but does the set of allowed values matter itself?

Example: three players are betting on a sequence *X*.

- Asuka can make bets in  $\mathcal{A} = \{0, 1, 2, 3, 4, 5\}$
- Bachiko can make bets in  $\mathcal{B} = \{1, 2, 3, 4, 10, 20\}$
- Chihiro can make bets in  $C = \{0, 2, 4, 6, 8, 10, 15\}$

Does any of the players have an advantage?

Pairs  $(\mathcal{A}, \mathcal{B})$ ,  $(\mathcal{B}, \mathcal{C})$  are not clear. However, one can see immediately that Chihiro has an advantage over Asuka. The reason is that  $2\mathcal{A} \subseteq \mathcal{B}$ , so Chihiro can just copy Asuka's strategy, just making bets twice bigger (and even has the opportunity to use the 15 option; if we remove this option then the rules of Asuka and Chihiro are "equivalent").

This observation gives us directly:

**Lemma** If for some  $k \in \mathbb{Q}^{>0}$  we have  $(k \cdot A) \subseteq B$ , then B-randomness implies A-randomness.

## The importance of $\mathcal{V}$ (3)

A remarkable result: the converse holds!

A remarkable result: the converse holds!

### Theorem (CDFT)

If  $\mathcal{B}$ -randomness implies  $\mathcal{A}$ -randomness, then there is some  $k \in \mathbb{Q}^{>0}$  such that  $(k \cdot \mathcal{A}) \subseteq \mathcal{B}$ .

**Proof sketch.** Suppose that  $(k \cdot A) \not\subseteq B$  for any *k*. We want to show that there is an *X* which can be defeated by a computable *A*-strategy *S* but no computable *B*-strategy (in fact, we can diagonalize against any countable set of *B*-strategies).

**Proof sketch.** Suppose that  $(k \cdot A) \not\subseteq B$  for any *k*. We want to show that there is an *X* which can be defeated by a computable *A*-strategy *S* but no computable *B*-strategy (in fact, we can diagonalize against any countable set of *B*-strategies).

Think of a situation where S is the strategy of a stooge player, who works in collusion with the casino which provides the sequence X.

**Proof sketch.** Suppose that  $(k \cdot A) \not\subseteq B$  for any *k*. We want to show that there is an *X* which can be defeated by a computable *A*-strategy *S* but no computable *B*-strategy (in fact, we can diagonalize against any countable set of *B*-strategies).

Think of a situation where S is the strategy of a stooge player, who works in collusion with the casino which provides the sequence X.

Let  $\mathcal{A} = \{a_1, a_2, ..., a_n\}$ . The strategy *S* will be simple: bet  $a_1$  on 0, then  $a_2$ ,  $a_3$ , ...,  $a_n$ , and repeat. This is clearly computable!!
Now suppose a player with strategy M enters the casino. The goal is to defeat M while giving money to S. The casino has a two-phase plan.

Now suppose a player with strategy M enters the casino. The goal is to defeat M while giving money to S. The casino has a two-phase plan.

Phase 1. At each step, the casino does the following:

• if *M* bets money on value 1, then the casino outputs a 0 (this way *S* makes money and *M* loses money... best case scenario!)

Now suppose a player with strategy M enters the casino. The goal is to defeat M while giving money to S. The casino has a two-phase plan.

Phase 1. At each step, the casino does the following:

- if *M* bets money on value 1, then the casino outputs a 0 (this way *S* makes money and *M* loses money... best case scenario!)
- otherwise it computes the ratio
  k = (capital of S)/(capital of M) and compares it with
  k' = (bet of S)/(bet of M)

Now suppose a player with strategy M enters the casino. The goal is to defeat M while giving money to S. The casino has a two-phase plan.

Phase 1. At each step, the casino does the following:

- if *M* bets money on value 1, then the casino outputs a 0 (this way *S* makes money and *M* loses money... best case scenario!)
- otherwise it computes the ratio
  k = (capital of S)/(capital of M) and compares it with
  k' = (bet of S)/(bet of M)
  - if k' ≥ k, the casino output a 0 (both S and M win some money, but S wins more proportionally to its capital)
  - ► if k' < k, the casino output a 1 (both S and M lose some money, but M loses more proportionally to its capital)

During phase 1, the ratio (capital of *S*)/(capital of *M*) is non-decreasing over time. One can show by contradiction that in fact it has to tend to  $+\infty$ . If not, it tends to some  $k^*$ . But then, the best strategy for *M* to prevent the increase of (capital of *S*)/(capital of *M*) would be to multiply each bet of *S* by  $1/k^*$ . By assumption, this is not possible. We have established that (capital of S)/(capital of M)  $\rightarrow +\infty$ .

We have established that (capital of S)/(capital of M)  $\rightarrow +\infty$ .

When this ratio becomes large enough, then the casino enters **phase 2**, where it will try to make *M* lose money no matter how much it costs *S*. Since *S* is sufficiently wealthy at the beginning of this phase, it will "survive" until the end, i.e., when *M* is defeated.

We have established that (capital of S)/(capital of M)  $\rightarrow +\infty$ .

When this ratio becomes large enough, then the casino enters **phase 2**, where it will try to make *M* lose money no matter how much it costs *S*. Since *S* is sufficiently wealthy at the beginning of this phase, it will "survive" until the end, i.e., when *M* is defeated.

To complete the proof, a bit more care is needed: how to play against different players, how to handle the case where players appear to be dormant (stops betting) but could wake up later, etc.

#### Further work

Is this work useful "in practice"? (i.e., does it explain some real-life phenomena?)

Is this work useful "in practice"? (i.e., does it explain some real-life phenomena?)

Does  $\mathbb{N}$ -randomness has interesting interactions with computability theory? (e.g. what is lowness for  $\mathbb{N}$ -randomness?)

- Is this work useful "in practice"? (i.e., does it explain some real-life phenomena?)
- Does  $\mathbb{N}$ -randomness has interesting interactions with computability theory? (e.g. what is lowness for  $\mathbb{N}$ -randomness?)

Can the separation of A-randomness and B-randomness always be witnessed by a 1-generic?

Thank you どうもありがとうございました