Feasible analysis, randomness, and base invariance

Santiago Figueira

University of Buenos Aires

Joint work with André Nies

AJNZ Workshop – UoA
2 Dec. 2013

Base invariance of randomness notions

Algorithmic randomness notions are usually defined not for real numbers, but for their *digit representations* with respect to a fixed base.

That a randomness notion $\mathcal{R}$ is base invariant means:

if X and Y are infinite sequences over different alphabets that denote the same real, then X satisfies $\mathcal{R}$ iff Y satisfies $\mathcal{R}$.

Outline

Notation

- A rational in base r is a rational number with finite representation in base r, i.e. a rational of the form $z \cdot r^{-n}$, for some $z \in \mathbb{Z}$ and $n \in \mathbb{N}$.
  - $\mathtt{Rat}_r$ is the set of rationals in base r
- $\Sigma_r = \{0, \dots, r-1\}$
- We represent $q \in \mathtt{Rat}_r$ with the pair $\langle \sigma, \tau \rangle$, where σ and τ are strings in Σ_r^* representing the integer and fractional part of q, respectively. If $p, q \in \mathtt{Rat}_r$ have both length n then
  - $\langle p, q \rangle \mapsto p + q \in \mathrm{DTIME}(n)$
  - $\langle p, q \rangle \mapsto p \cdot q \in \mathrm{DTIME}(n \cdot \log^2 n)$.
- The function t will be a time bound such that $t(n) \geq n$.

Betting strategies

A martingale formalizes the concept of betting strategy that tries to gain capital along $Z \in \Sigma_r^\infty$ by predicting $Z(n)$ after having seen $Z(0), \ldots, Z(n-1)$.

Definition

Let $r \in \mathbb{N}^{>1}$.

- A martingale in base r is a function $M : \Sigma_r^* \to \mathbb{R}^{\geq 0}$ such that

$$(\forall \sigma \in \Sigma_r^*) \; r \cdot M(\sigma) = \sum_{b \in \Sigma_r} M(\sigma^\frown b) \qquad (*)$$

- M is a $t(n)$-martingale in base r if M is $\mathtt{Rat}_r^{\geq 0}$-valued and $M \in \mathrm{DTIME}(t(n))$.

Betting strategies

A martingale formalizes the concept of betting strategy that tries to gain capital along $Z \in \Sigma_r^\infty$ by predicting $Z(n)$ after having seen $Z(0), \ldots, Z(n-1)$.

Definition

Let $r \in \mathbb{N}^{>1}$.

- A martingale in base r is a function $M : \Sigma_r^* \to \mathbb{R}^{\geq 0}$ such that

$$(\forall \sigma \in \Sigma_r^*)\ r \cdot M(\sigma) = \sum_{b \in \Sigma_r} M(\sigma^\frown b) \qquad (*)$$

- M is a $t(n)$-martingale in base r if M is $\mathtt{Rat}_r^{\geq 0}$-valued and $M \in \mathrm{DTIME}(t(n))$.

$M(\sigma)$ represents the capital after having seen σ.

- We start with capital $M(\lambda) > 0$
- $(*)$ is a fairness condition: the expected value of our capital after a bet is equal to our capital before the bet.

The underlying strategy is as follows:

- Bet $\frac{M(\sigma^\frown b)}{rM(\sigma)}$ of your current capital to the symbol will be b.

Success of a betting strategy

Definition

M succeeds on $Z \in \Sigma_r^\infty$ iff

$$\limsup_n M(Z \upharpoonright_n) = \infty.$$

M succeeds on Z when, following the strategy given by M, the capital we get along Z is unbounded.

Polynomial time randomness

Definition

Let $Z \in \Sigma_r^\infty$

- Z is computably random if no computable martingale in base r succeeds on Z.
- Z is $t(n)$-random in base r if no $t(n)$-martingale in base r succeeds on Z.
- Z is polynomial time random in base r if Z is n^c-random for all $c \geq 1$.

Outline

Real-valued to rational-valued martingales

Definition

Let $M : \Sigma_r^* \to \mathbb{R}^{\geq 0}$. A computable function $\widehat{M} : \Sigma_r^* \times \mathbb{N} \to \mathtt{Rat}_r^{\geq 0}$ such that

$$|\widehat{M}(\sigma, i) - M(\sigma)| \leq r^{-i}$$

is called a computable approximation of M.

- The complexity of $\widehat{M}$ on argument (σ, i) is measured in $|\sigma| + i$.
- A $t(n)$-computable approximation is a computable approximation in $\mathrm{DTIME}(t(n))$.

Real-valued to rational-valued martingales

Definition

Let $M : \Sigma_r^* \to \mathbb{R}^{\geq 0}$. A computable function $\widehat{M} : \Sigma_r^* \times \mathbb{N} \to \mathtt{Rat}_r^{\geq 0}$ such that

$$|\widehat{M}(\sigma, i) - M(\sigma)| \leq r^{-i}$$

is called a computable approximation of M.

- The complexity of $\widehat{M}$ on argument (σ, i) is measured in $|\sigma| + i$.
- A $t(n)$-computable approximation is a computable approximation in $\mathrm{DTIME}(t(n))$.

Recall that a $t(n)$-martingale is always $\mathtt{Rat}_r^{\geq 0}$-valued.

Lemma

If M is a martingale in base r with a $t(n)$-computable approximation then there is an $n \cdot t(n)$-martingale N in base r such that $N \geq M$.

Savings property

If M is a martingale in base r then

$$M(\sigma) \leq M(\emptyset) \cdot r^{|\sigma|}.$$

We say that a martingale M in base r has the savings property if there is $c > 0$ such that for all $\tau, \sigma \in \Sigma_r^*$,

$$\tau \succeq \sigma \Rightarrow M(\tau) \geq M(\sigma) - c.$$

Savings property

If M is a martingale in base r then

$$M(\sigma) \leq M(\emptyset) \cdot r^{|\sigma|}.$$

We say that a martingale M in base r has the savings property if there is $c > 0$ such that for all $\tau, \sigma \in \Sigma_r^*$,

$$\tau \succeq \sigma \Rightarrow M(\tau) \geq M(\sigma) - c.$$

Proposition

If M is a martingale in base r with the savings property via c then

$$(\forall \sigma \in \Sigma_r^*)\ M(\sigma) \leq (r-1) \cdot c \cdot |\sigma| + M(\emptyset).$$

Savings property

If M is a martingale in base r then

$$M(\sigma) \leq M(\emptyset) \cdot r^{|\sigma|}.$$

We say that a martingale M in base r has the savings property if there is $c > 0$ such that for all $\tau, \sigma \in \Sigma_r^*$,

$$\tau \succeq \sigma \Rightarrow M(\tau) \geq M(\sigma) - c.$$

Proposition

If M is a martingale in base r with the savings property via c then

$$(\forall \sigma \in \Sigma_r^*)\ M(\sigma) \leq (r-1) \cdot c \cdot |\sigma| + M(\emptyset).$$

Lemma (Time bounded savings property)

For each $t(n)$-martingale L in base r there is an $n \cdot t(n)$-martingale M in base r such that

- *M has the savings property and*
- *M succeeds on all the sequences that L succeeds on.*

Savings property

Given a $t(n)$-martingale L in base r, let $M = G + E$, where

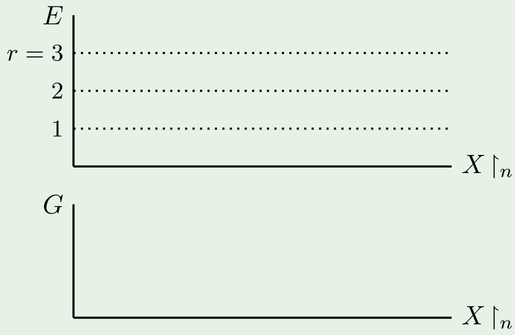
- $G(\sigma)$ is the balance of the savings account at σ
- $E(\sigma)$ is the balance of the checking account at σ

Savings property

Given a $t(n)$-martingale L in base r, let $M = G + E$, where

- $G(\sigma)$ is the balance of the savings account at σ
- $E(\sigma)$ is the balance of the checking account at σ

Example

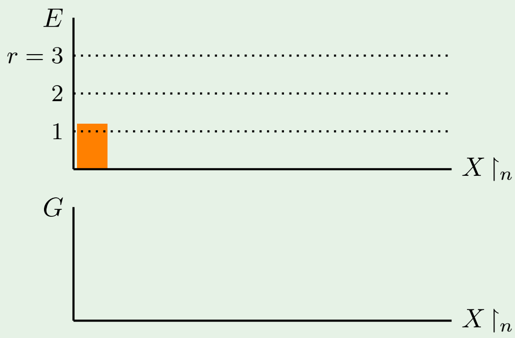


Savings property

Given a $t(n)$-martingale L in base r, let $M = G + E$, where

- $G(\sigma)$ is the balance of the savings account at σ
- $E(\sigma)$ is the balance of the checking account at σ

Example

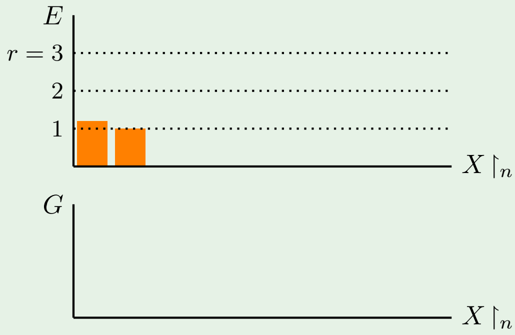


Savings property

Given a $t(n)$-martingale L in base r, let $M = G + E$, where

- $G(\sigma)$ is the balance of the savings account at σ
- $E(\sigma)$ is the balance of the checking account at σ

Example

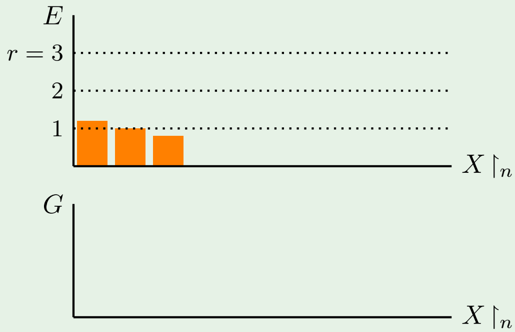


Savings property

Given a $t(n)$-martingale L in base r, let $M = G + E$, where

- $G(\sigma)$ is the balance of the savings account at σ
- $E(\sigma)$ is the balance of the checking account at σ

Example

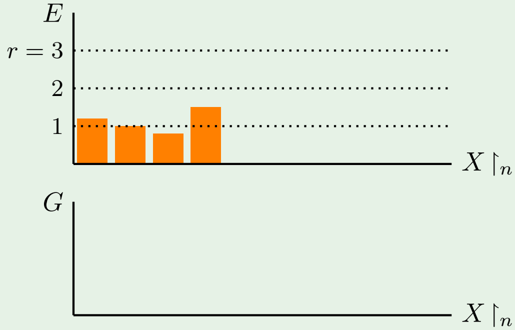


Savings property

Given a $t(n)$-martingale L in base r, let $M = G + E$, where

- $G(\sigma)$ is the balance of the savings account at σ
- $E(\sigma)$ is the balance of the checking account at σ

Example

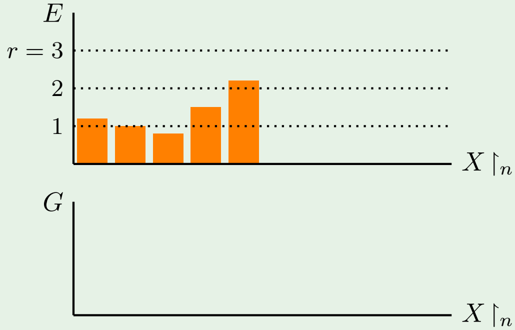


Savings property

Given a $t(n)$-martingale L in base r, let $M = G + E$, where

- $G(\sigma)$ is the balance of the savings account at σ
- $E(\sigma)$ is the balance of the checking account at σ

Example

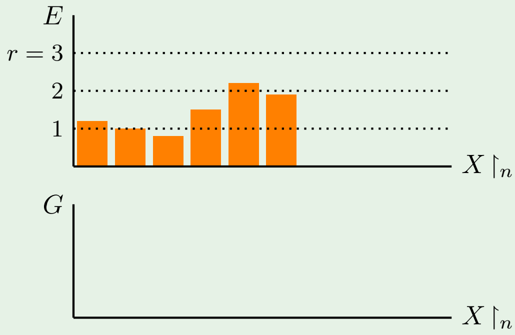


Savings property

Given a $t(n)$-martingale L in base r, let $M = G + E$, where

- $G(\sigma)$ is the balance of the savings account at σ
- $E(\sigma)$ is the balance of the checking account at σ

Example

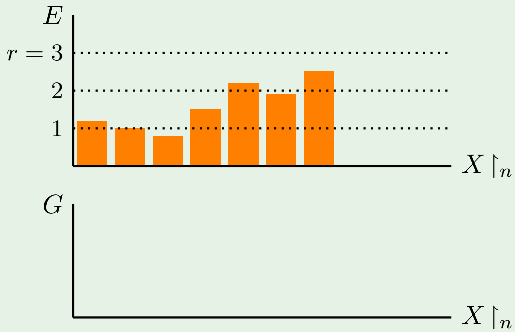


Savings property

Given a $t(n)$-martingale L in base r, let $M = G + E$, where

- $G(\sigma)$ is the balance of the savings account at σ
- $E(\sigma)$ is the balance of the checking account at σ

Example

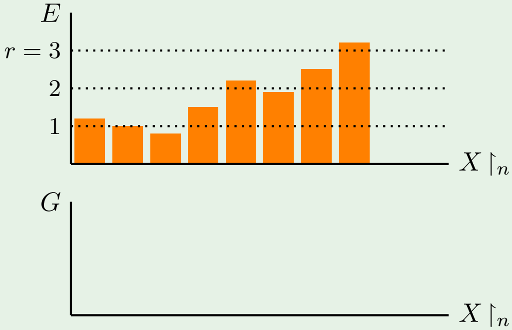


Savings property

Given a $t(n)$-martingale L in base r, let $M = G + E$, where

- $G(\sigma)$ is the balance of the savings account at σ
- $E(\sigma)$ is the balance of the checking account at σ

Example

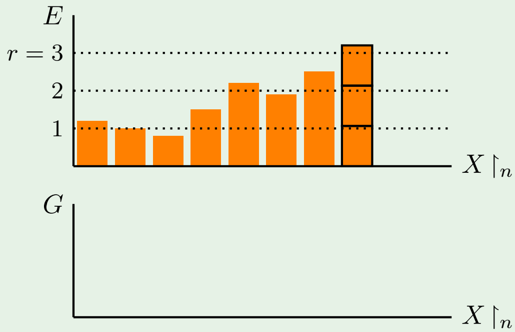


Savings property

Given a $t(n)$-martingale L in base r, let $M = G + E$, where

- $G(\sigma)$ is the balance of the savings account at σ
- $E(\sigma)$ is the balance of the checking account at σ

Example

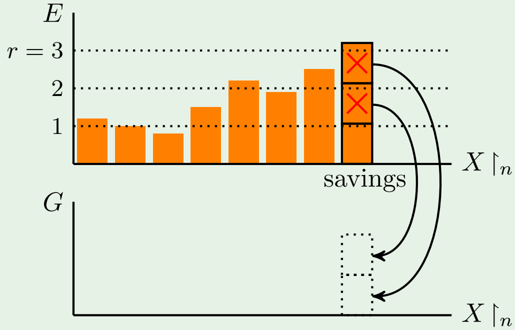


Savings property

Given a $t(n)$-martingale L in base r, let $M = G + E$, where

- $G(\sigma)$ is the balance of the savings account at σ
- $E(\sigma)$ is the balance of the checking account at σ

Example

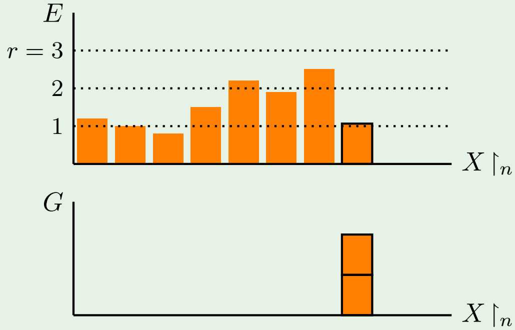


Savings property

Given a $t(n)$-martingale L in base r, let $M = G + E$, where

- $G(\sigma)$ is the balance of the savings account at σ
- $E(\sigma)$ is the balance of the checking account at σ

Example

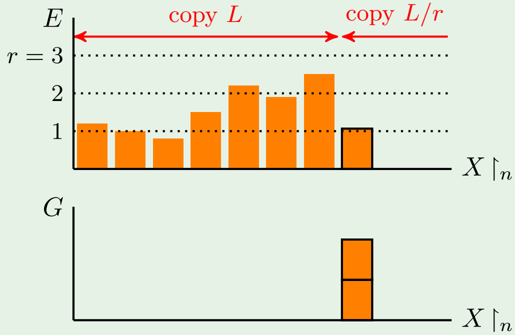


Savings property

Given a $t(n)$-martingale L in base r, let $M = G + E$, where

- $G(\sigma)$ is the balance of the savings account at σ
- $E(\sigma)$ is the balance of the checking account at σ

Example

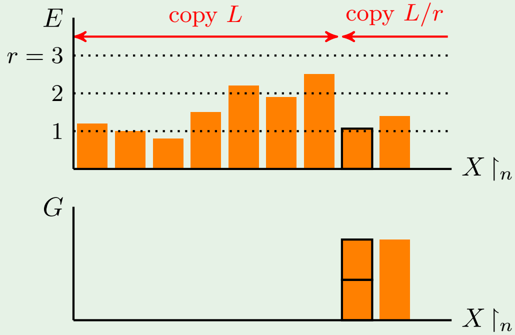


Savings property

Given a $t(n)$-martingale L in base r, let $M = G + E$, where

- $G(\sigma)$ is the balance of the savings account at σ
- $E(\sigma)$ is the balance of the checking account at σ

Example

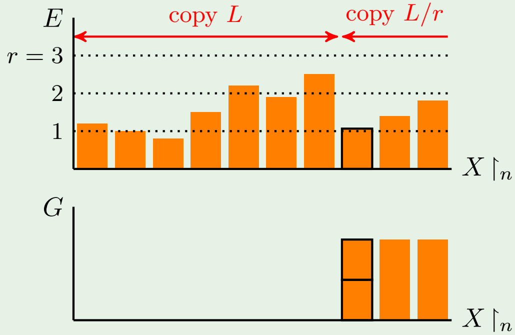


Savings property

Given a $t(n)$-martingale L in base r, let $M = G + E$, where

- $G(\sigma)$ is the balance of the savings account at σ
- $E(\sigma)$ is the balance of the checking account at σ

Example

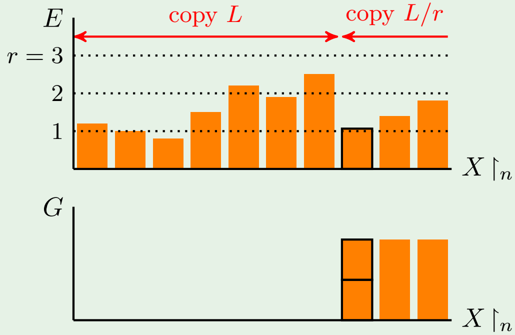


Savings property

Given a $t(n)$-martingale L in base r, let $M = G + E$, where

- $G(\sigma)$ is the balance of the savings account at σ
- $E(\sigma)$ is the balance of the checking account at σ

Example



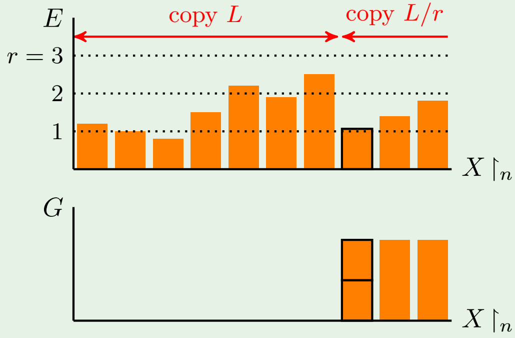
- If $\tau \succeq \sigma$ then
  - $G(\tau) \geq G(\sigma)$

Savings property

Given a $t(n)$-martingale L in base r, let $M = G + E$, where

- $G(\sigma)$ is the balance of the savings account at σ
- $E(\sigma)$ is the balance of the checking account at σ

Example



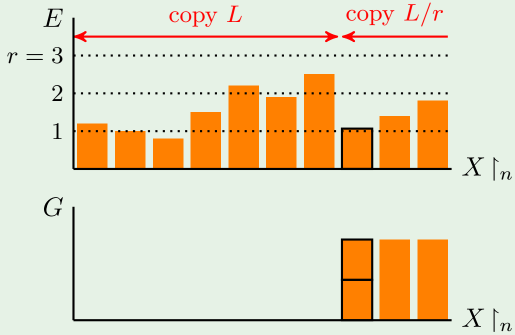
- If $\tau \succeq \sigma$ then
  - $G(\tau) \geq G(\sigma)$
  - $M(\sigma) - M(\tau) \leq E(\sigma) - E(\tau) \leq E(\sigma) \leq r$

Savings property

Given a $t(n)$-martingale L in base r, let $M = G + E$, where

- $G(\sigma)$ is the balance of the savings account at σ
- $E(\sigma)$ is the balance of the checking account at σ

Example



- If $\tau \succeq \sigma$ then
  - $G(\tau) \geq G(\sigma)$
  - $M(\sigma) - M(\tau) \leq E(\sigma) - E(\tau) \leq E(\sigma) \leq r$
- $\limsup_n L(X\restriction_n) = \infty \Rightarrow \lim_n G(X\restriction_n) = \infty$
- $E(\sigma), G(\sigma) \in \mathrm{DTIME}(n \cdot t(n))$
- M is an $n \cdot t(n)$-martingale in base r.

Outline

More notation

- If $\sigma \in \Sigma_r^*$ then $\langle 0.\sigma \rangle_r$ represents the rational in $[0, 1]$ whose representation in base r is $0.\sigma$, i.e.

$$\langle 0.\sigma \rangle_r = \sum_{i=0}^{|\sigma|-1} \sigma(i) \cdot r^{-i-1}.$$

- If $Z \in \Sigma_r^\infty$, then $\langle 0.Z \rangle_r$ represents the real in $[0, 1]$ whose expansion in base r is Z, i.e.

$$\langle 0.Z \rangle_r = \sum_{i \in \mathbb{N}} Z(i) \cdot r^{-i-1}.$$

Base conversion

We want a functional $\Gamma : \Sigma_r^\infty \times \mathbb{N} \to \Sigma_s$ which converts from base r to base s:

for all $X \in \Sigma_r^\infty, Y \in \Sigma_s^\infty$

$$\Gamma^X \text{ is total and } \Gamma^X = Y \Rightarrow \langle 0.X \rangle_r = \langle 0.Y \rangle_s$$

Base conversion

We want a functional $\Gamma : \Sigma_r^\infty \times \mathbb{N} \to \Sigma_s$ which converts from base r to base s:

for all $X \in \Sigma_r^\infty, Y \in \Sigma_s^\infty$

$$\Gamma^X \ \textit{is total and}\ \Gamma^X = Y \Rightarrow \langle 0.X \rangle_r = \langle 0.Y \rangle_s$$

Example

$X = \ldots$ $\qquad$ $Y = \ldots$

$r = 3$ $\quad$ 0 $\qquad$ 1

$r = 2$ $\quad$ 0 $\qquad$ 1

Base conversion

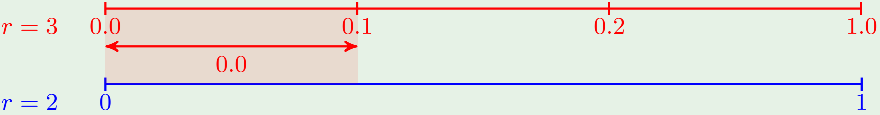
We want a functional $\Gamma : \Sigma_r^\infty \times \mathbb{N} \to \Sigma_s$ which converts from base r to base s:

for all $X \in \Sigma_r^\infty, Y \in \Sigma_s^\infty$

$$\Gamma^X \textit{ is total and } \Gamma^X = Y \Rightarrow \langle 0.X \rangle_r = \langle 0.Y \rangle_s$$

Example

$X = 0\ldots$ $Y = \ldots$



Base conversion

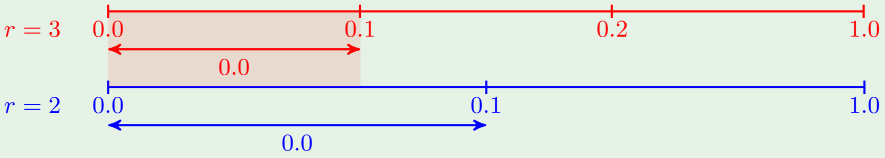
We want a functional $\Gamma : \Sigma_r^\infty \times \mathbb{N} \to \Sigma_s$ which converts from base r to base s:

for all $X \in \Sigma_r^\infty, Y \in \Sigma_s^\infty$

$$\Gamma^X \text{ is total and } \Gamma^X = Y \Rightarrow \langle 0.X \rangle_r = \langle 0.Y \rangle_s$$

Example

$X = 0 \ldots$ $\qquad$ $Y = 0 \ldots$



Base conversion

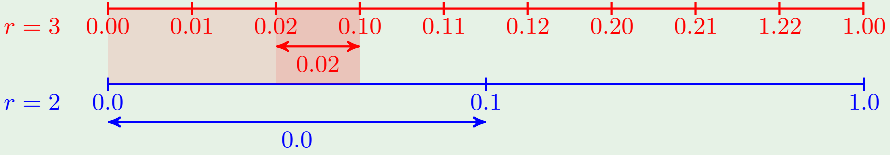
We want a functional $\Gamma : \Sigma_r^\infty \times \mathbb{N} \to \Sigma_s$ which converts from base r to base s:

for all $X \in \Sigma_r^\infty, Y \in \Sigma_s^\infty$

$$\Gamma^X \textit{ is total and } \Gamma^X = Y \Rightarrow \langle 0.X \rangle_r = \langle 0.Y \rangle_s$$

Example

$X = 02\ldots$ $\quad$ $Y = 0\ldots$



Base conversion

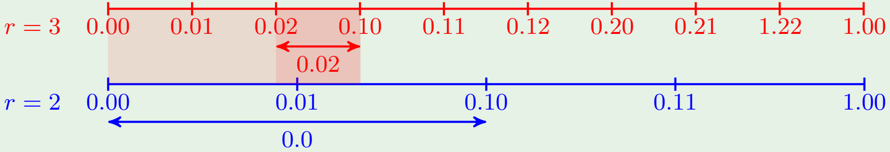
We want a functional $\Gamma : \Sigma_r^\infty \times \mathbb{N} \to \Sigma_s$ which converts from base r to base s:

for all $X \in \Sigma_r^\infty, Y \in \Sigma_s^\infty$

$$\Gamma^X \text{ is total and } \Gamma^X = Y \Rightarrow \langle 0.X \rangle_r = \langle 0.Y \rangle_s$$

Example

$X = 02\ldots$ $\qquad$ $Y = 0\ldots$



Base conversion

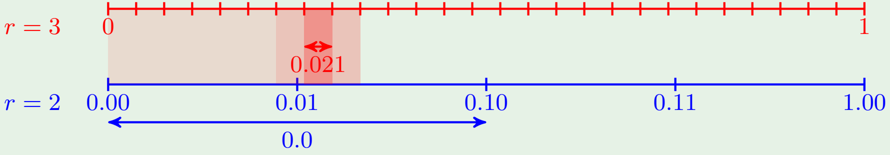
We want a functional $\Gamma : \Sigma_r^\infty \times \mathbb{N} \to \Sigma_s$ which converts from base r to base s:

for all $X \in \Sigma_r^\infty, Y \in \Sigma_s^\infty$

$$\Gamma^X \textit{ is total and } \Gamma^X = Y \Rightarrow \langle 0.X \rangle_r = \langle 0.Y \rangle_s$$

Example

$X = 021\ldots$ $\quad$ $Y = 0\ldots$



Base conversion

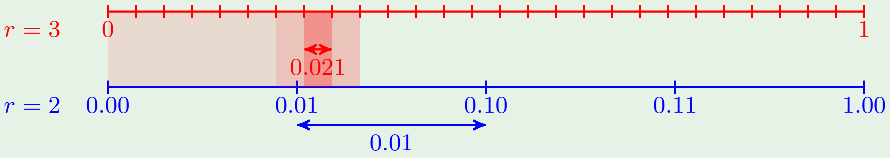
We want a functional $\Gamma : \Sigma_r^\infty \times \mathbb{N} \to \Sigma_s$ which converts from base r to base s:

for all $X \in \Sigma_r^\infty, Y \in \Sigma_s^\infty$

$$\Gamma^X \textit{ is total and } \Gamma^X = Y \Rightarrow \langle 0.X \rangle_r = \langle 0.Y \rangle_s$$

Example

$X = 021\ldots$ $\quad$ $Y = 01\ldots$



Base conversion

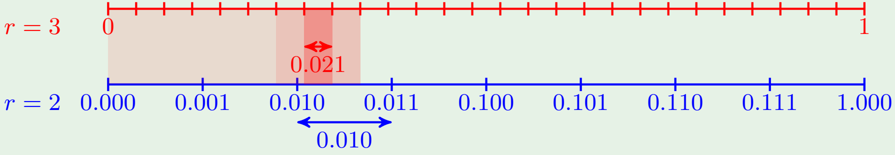
We want a functional $\Gamma : \Sigma_r^\infty \times \mathbb{N} \to \Sigma_s$ which converts from base r to base s:

for all $X \in \Sigma_r^\infty, Y \in \Sigma_s^\infty$

$$\Gamma^X \text{ is total and } \Gamma^X = Y \Rightarrow \langle 0.X \rangle_r = \langle 0.Y \rangle_s$$

Example

$X = 021\ldots$ $\qquad$ $Y = 010\ldots$



Base conversion is not honest!

Example

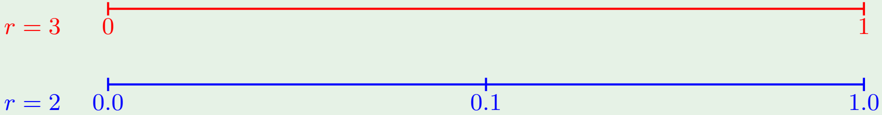
$X = \dots$

$Y = \dots$

Base conversion is not honest!

Example

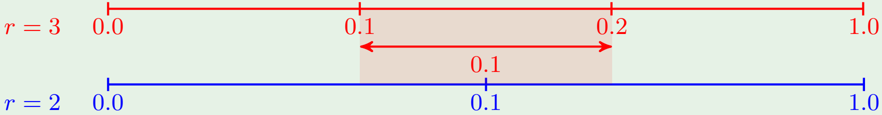
$X = \dots$ $Y = \dots$



Base conversion is not honest!

Example

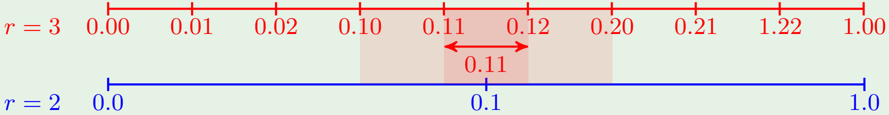
$X = 1\ldots$ $\qquad$ $Y = \ldots$



Base conversion is not honest!

Example

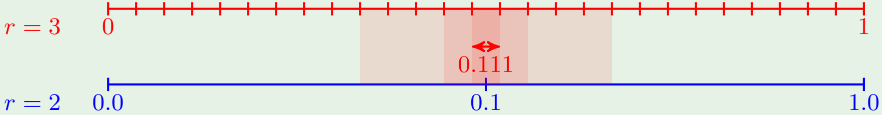
$X = 11\ldots$ $Y = \ldots$



Base conversion is not honest!

Example

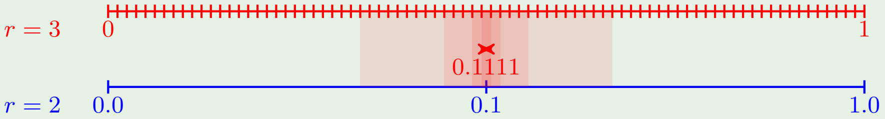
$X = 111\ldots$ $Y = \ldots$



Base conversion is not honest!

Example

$X = 1111\ldots$ $\qquad$ $Y = \ldots$



So there is no such Γ.

Base conversion with small error

For $\tau \in \Sigma_s^*$ and $i \in \mathbb{N}$, let

- $\mathsf{bc}^-_{s \text{ to } r}(\tau, i)$ be the string σ in Σ_r^* of minimal length such that

$$0 \leq \langle 0.\tau \rangle_s - \langle 0.\sigma \rangle_r < r^{-i},$$

- $\mathsf{bc}^+_{s \text{ to } r}(\tau, i)$ be the string σ in Σ_r^* of minimal length such that

$$0 \leq \langle 0.\sigma \rangle_r - \langle 0.\tau \rangle_s < r^{-i},$$

Base conversion with small error

For $\tau \in \Sigma_s^*$ and $i \in \mathbb{N}$, let

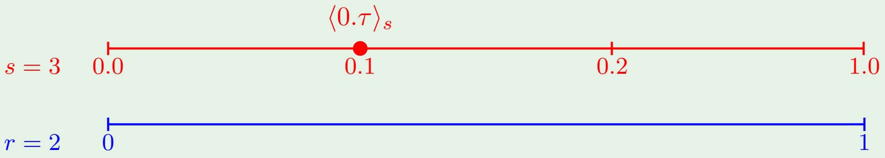
- $\mathsf{bc}^-_{s \text{ to } r}(\tau, i)$ be the string σ in Σ_r^* of minimal length such that

$$0 \leq \langle 0.\tau \rangle_s - \langle 0.\sigma \rangle_r < r^{-i},$$

- $\mathsf{bc}^+_{s \text{ to } r}(\tau, i)$ be the string σ in Σ_r^* of minimal length such that

$$0 \leq \langle 0.\sigma \rangle_r - \langle 0.\tau \rangle_s < r^{-i},$$

Example



Base conversion with small error

For $\tau \in \Sigma_s^*$ and $i \in \mathbb{N}$, let

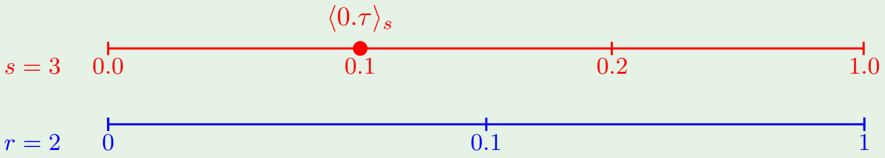
- $\mathsf{bc}^-_{s \text{ to } r}(\tau, i)$ be the string σ in Σ_r^* of minimal length such that

$$0 \le \langle 0.\tau \rangle_s - \langle 0.\sigma \rangle_r < r^{-i},$$

- $\mathsf{bc}^+_{s \text{ to } r}(\tau, i)$ be the string σ in Σ_r^* of minimal length such that

$$0 \le \langle 0.\sigma \rangle_r - \langle 0.\tau \rangle_s < r^{-i},$$

Example



Base conversion with small error

For $\tau \in \Sigma_s^*$ and $i \in \mathbb{N}$, let

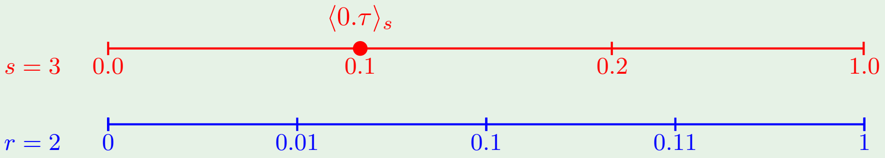
- $\mathsf{bc}^-_{s \text{ to } r}(\tau, i)$ be the string σ in Σ_r^* of minimal length such that

$$0 \leq \langle 0.\tau \rangle_s - \langle 0.\sigma \rangle_r < r^{-i},$$

- $\mathsf{bc}^+_{s \text{ to } r}(\tau, i)$ be the string σ in Σ_r^* of minimal length such that

$$0 \leq \langle 0.\sigma \rangle_r - \langle 0.\tau \rangle_s < r^{-i},$$

Example



Base conversion with small error

For $\tau \in \Sigma_s^*$ and $i \in \mathbb{N}$, let

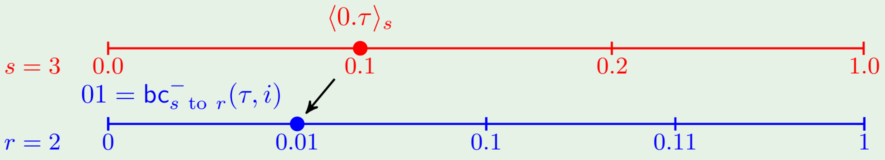
- $\mathsf{bc}^-_{s \text{ to } r}(\tau, i)$ be the string σ in Σ_r^* of minimal length such that

$$0 \leq \langle 0.\tau \rangle_s - \langle 0.\sigma \rangle_r < r^{-i},$$

- $\mathsf{bc}^+_{s \text{ to } r}(\tau, i)$ be the string σ in Σ_r^* of minimal length such that

$$0 \leq \langle 0.\sigma \rangle_r - \langle 0.\tau \rangle_s < r^{-i},$$

Example



Base conversion with small error

For $\tau \in \Sigma_s^*$ and $i \in \mathbb{N}$, let

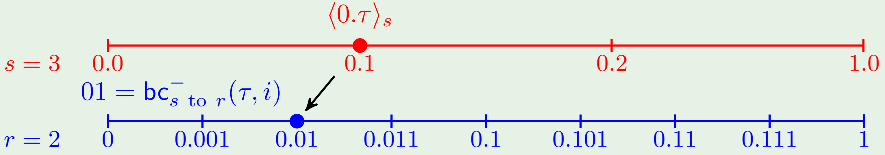
- $\mathsf{bc}^-_{s \text{ to } r}(\tau, i)$ be the string σ in Σ_r^* of minimal length such that

$$0 \leq \langle 0.\tau \rangle_s - \langle 0.\sigma \rangle_r < r^{-i},$$

- $\mathsf{bc}^+_{s \text{ to } r}(\tau, i)$ be the string σ in Σ_r^* of minimal length such that

$$0 \leq \langle 0.\sigma \rangle_r - \langle 0.\tau \rangle_s < r^{-i},$$

Example



Base conversion with small error

For $\tau \in \Sigma_s^*$ and $i \in \mathbb{N}$, let

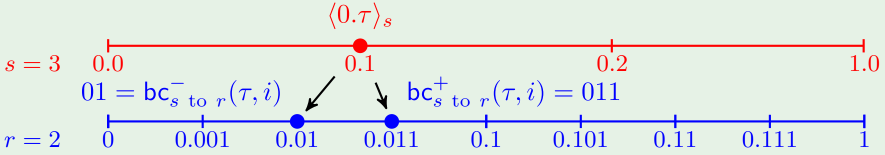
- $\mathsf{bc}^-_{s \text{ to } r}(\tau, i)$ be the string σ in Σ_r^* of minimal length such that

$$0 \leq \langle 0.\tau \rangle_s - \langle 0.\sigma \rangle_r < r^{-i},$$

- $\mathsf{bc}^+_{s \text{ to } r}(\tau, i)$ be the string σ in Σ_r^* of minimal length such that

$$0 \leq \langle 0.\sigma \rangle_r - \langle 0.\tau \rangle_s < r^{-i},$$

Example



Base conversion with small error

For $\tau \in \Sigma_s^*$ and $i \in \mathbb{N}$, let

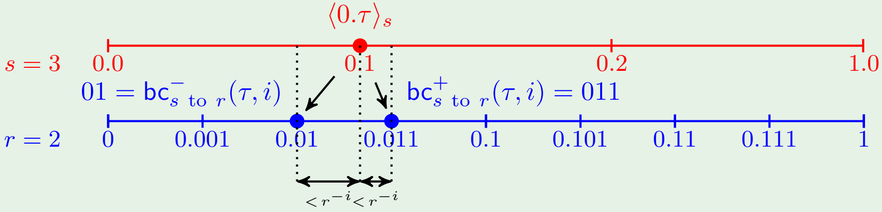
- $\mathsf{bc}^-_{s \text{ to } r}(\tau, i)$ be the string σ in Σ_r^* of minimal length such that

$$0 \le \langle 0.\tau \rangle_s - \langle 0.\sigma \rangle_r < r^{-i},$$

- $\mathsf{bc}^+_{s \text{ to } r}(\tau, i)$ be the string σ in Σ_r^* of minimal length such that

$$0 \le \langle 0.\sigma \rangle_r - \langle 0.\tau \rangle_s < r^{-i},$$

Example



Base conversion with small error

Approximation of a rational in base s with a rational in base r

input : $\tau \in \Sigma_s^*$ and $i \in \mathbb{N}$
output: $\sigma \in \Sigma_r^*, \sigma = \mathsf{bc}^-_{s \text{ to } r}(\tau, i)$

$\sigma := \emptyset$
while $\langle 0.\tau \rangle_s - \langle 0.\sigma \rangle_r > r^{-i}$ **do**
  Find the largest $x \in \Sigma_r$ such that $\langle 0.\sigma^\frown x \rangle_r \leq \langle 0.\tau \rangle_s$
  $\sigma := \sigma^\frown x$

Base conversion with small error

Approximation of a rational in base s with a rational in base r

---

input : $\tau \in \Sigma_s^*$ and $i \in \mathbb{N}$
output: $\sigma \in \Sigma_r^*, \sigma = \mathsf{bc}^-_{s \text{ to } r}(\tau, i)$

$\sigma := \emptyset$
while $\langle 0.\tau \rangle_s - \langle 0.\sigma \rangle_r > r^{-i}$ **do**
    Find the largest $x \in \Sigma_r$ such that $\langle 0.\sigma^\frown x \rangle_r \leq \langle 0.\tau \rangle_s$
    $\sigma := \sigma^\frown x$

The time complexity of $\mathsf{bc}^+_{s \text{ to } r}$ or $\mathsf{bc}^-_{s \text{ to } r}$ on argument (τ, i) is measured in $n = |\tau| + i$.

Theorem

$\mathsf{bc}^-_{s \text{ to } r}(\tau, i), \mathsf{bc}^+_{s \text{ to } r}(\tau, i) \in \mathrm{DTIME}(n^2)$.

Outline

Martingales and analysis - Brattka, Miller, Nies 2011

Each martingale M in base r induces a measure μ_M on the algebra of clopen sets defined by

$$\mu_M([\sigma]) = \frac{M(\sigma)}{r^{|\sigma|}}, \text{for } \sigma \in \Sigma_r^*.$$

Via Carathéodory's extension theorem this measure can be extended to a Borel measure on Cantor space, and if μ_M is atomless, we can also think of it as a Borel measure on $[0,1]$: μ_M is determined by

$$\mu_M\left(\left[\langle 0.\sigma\rangle_r, \langle 0.\sigma\rangle_r + r^{-|\sigma|}\right]\right) = \frac{M(\sigma)}{r^{|\sigma|}}.$$

Martingales and analysis - Brattka, Miller, Nies 2011

Each martingale M in base r induces a measure μ_M on the algebra of clopen sets defined by

$$\mu_M([\sigma]) = \frac{M(\sigma)}{r^{|\sigma|}}, \text{for } \sigma \in \Sigma_r^*.$$

Via Carathéodory's extension theorem this measure can be extended to a Borel measure on Cantor space, and if μ_M is atomless, we can also think of it as a Borel measure on $[0,1]$: μ_M is determined by

$$\mu_M\left(\left[\langle 0.\sigma\rangle_r, \langle 0.\sigma\rangle_r + r^{-|\sigma|}\right]\right) = \frac{M(\sigma)}{r^{|\sigma|}}.$$

Fact

If M has the savings property then μ_M is atomless.

The cumulative distribution function associated with μ_M, notated $\mathsf{cdf}_M(x) : [0,1] \to [0,1]$, is defined by:

$$\mathsf{cdf}_M(x) = \mu_M([0,x)).$$

Martingales and analysis - Brattka, Miller, Nies 2011

Lemma (BMN 2011)

Suppose M is a martingale in base r with the savings property. Let $N : \Sigma_s^* \to \mathbb{R}^{\geq 0}$ be the following martingale in base s:

$$\begin{aligned} N(\tau) &= \textit{slope of } \mathsf{cdf}_M \textit{ at points } \langle 0.\tau \rangle_s + s^{-|\tau|} \textit{ and } \langle 0.\tau \rangle_s \\ &= \frac{\mathsf{cdf}_M(\langle 0.\tau \rangle_s + s^{-|\tau|}) - \mathsf{cdf}_M(\langle 0.\tau \rangle_s)}{s^{-|\tau|}}. \end{aligned}$$

Suppose $X \in \Sigma_r^\infty$ and $Y \in \Sigma_s^\infty$ are such that $\langle 0.X \rangle_r \notin \mathtt{Rat}_r$, $\langle 0.Y \rangle_s \notin \mathtt{Rat}_s$ and $\langle 0.X \rangle_r = \langle 0.Y \rangle_s$. If M succeeds on X then N succeeds on Y.

Corollary (BMN 2011)

Computable randomness is base invariant.

Outline

Some properties of cdf_M

Proposition (An 'almost Lipschitz' condition)

Let M be a martingale in base r with the savings property. Then there are constants $k, \varepsilon > 0$ such that for every $x, y \in [0,1]$, if $y - x \leq \varepsilon$ then

$$\mathsf{cdf}_M(y) - \mathsf{cdf}_M(x) \leq -k \cdot (y-x) \cdot \log(y-x).$$

Some properties of cdf_M

Proposition (An 'almost Lipschitz' condition)

Let M be a martingale in base r with the savings property. Then there are constants $k, \varepsilon > 0$ such that for every $x, y \in [0,1]$, if $y - x \leq \varepsilon$ then

$$\mathsf{cdf}_M(y) - \mathsf{cdf}_M(x) \leq -k \cdot (y - x) \cdot \log(y - x).$$

Lemma (Complexity of cdf_M)

Let M be a $t(n)$-martingale in base r with the savings property.

- cdf_M *restricted to rationals in base r is a rational in base r.*
- *For $\sigma \in \Sigma_r^n$, $\mathsf{cdf}_M(\langle 0.\sigma \rangle_r) \in \mathrm{DTIME}(n \cdot t(n))$ (output represented in base r).*

Polynomial time randomness is base invariant

Lemma (F, Nies 2013)

For any $t(n)$-martingale M in base r with the savings property there is a (real-valued) martingale N in base s such that:

- *if M succeeds on $X \in \Sigma_r^\infty$, and $Y \in \Sigma_s^\infty$ is such that $\langle 0.X \rangle_r = \langle 0.Y \rangle_s$, then N succeeds on Y.*
- *N has an $n \cdot t(n)$-computable approximation.*

Proof of the lemma

Restatement. Given M an n^k-martingale with the savings property in base r. Get a martingale N in base s with a n^{k+1}-computable approximation such that

$$M \text{ succeeds on a real} \Rightarrow N \text{ succeeds on it}$$

Proof of the lemma

Restatement. Given M an n^k-martingale with the savings property in base r. Get a martingale N in base s with a n^{k+1}-computable approximation such that

$$M \text{ succeeds on a real} \Rightarrow N \text{ succeeds on it}$$

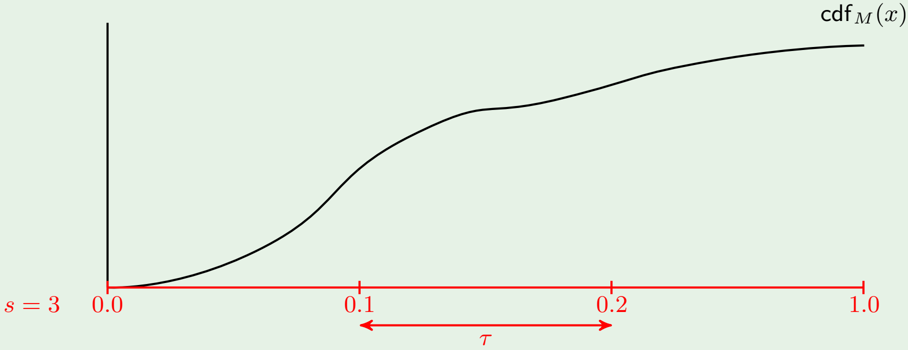
Define $N(\tau) = \frac{\mathsf{cdf}_M(q) - \mathsf{cdf}_M(p)}{s^{-|\tau|}}$, $\quad p = \langle 0.\tau \rangle_s, \quad q = \langle 0.\tau \rangle_s + s^{-|\tau|}$

Proof of the lemma

Restatement. Given M an n^k-martingale with the savings property in base r. Get a martingale N in base s with a n^{k+1}-computable approximation such that

$$M \text{ succeeds on a real} \Rightarrow N \text{ succeeds on it}$$

Define $N(\tau) = \frac{\mathsf{cdf}_M(q) - \mathsf{cdf}_M(p)}{s^{-|\tau|}}, \quad p = \langle 0.\tau \rangle_s, \quad q = \langle 0.\tau \rangle_s + s^{-|\tau|}$

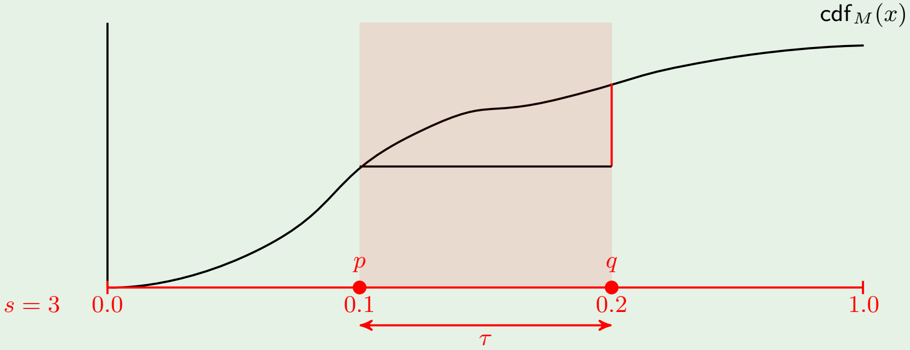


Proof of the lemma

Restatement. Given M an n^k-martingale with the savings property in base r. Get a martingale N in base s with a n^{k+1}-computable approximation such that

$$M \text{ succeeds on a real} \Rightarrow N \text{ succeeds on it}$$

Define $N(\tau) = \frac{\mathsf{cdf}_M(q) - \mathsf{cdf}_M(p)}{s^{-|\tau|}}, \quad p = \langle 0.\tau \rangle_s, \quad q = \langle 0.\tau \rangle_s + s^{-|\tau|}$

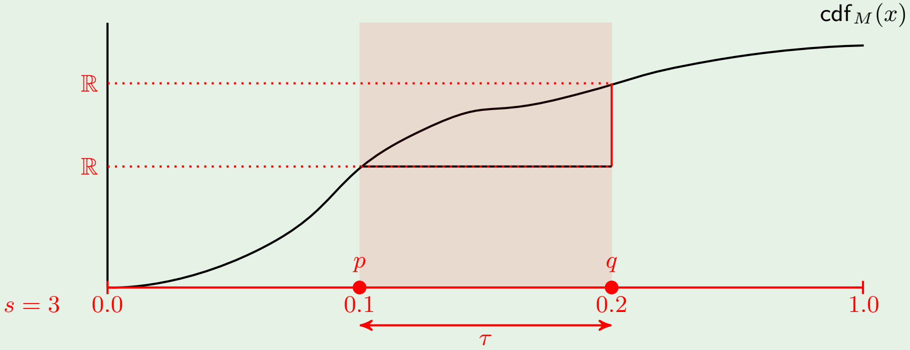


Proof of the lemma

Restatement. Given M an n^k-martingale with the savings property in base r. Get a martingale N in base s with a n^{k+1}-computable approximation such that

$$M \text{ succeeds on a real} \Rightarrow N \text{ succeeds on it}$$

Define $N(\tau) = \frac{\mathsf{cdf}_M(q) - \mathsf{cdf}_M(p)}{s^{-|\tau|}}, \quad p = \langle 0.\tau \rangle_s, \quad q = \langle 0.\tau \rangle_s + s^{-|\tau|}$

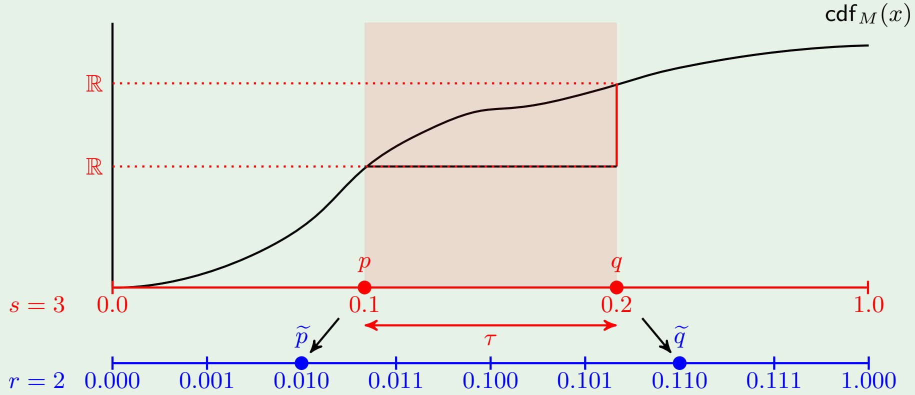


Proof of the lemma

Restatement. Given M an n^k-martingale with the savings property in base r. Get a martingale N in base s with a n^{k+1}-computable approximation such that

$$M \text{ succeeds on a real} \Rightarrow N \text{ succeeds on it}$$

Define $N(\tau) = \frac{\mathsf{cdf}_M(q) - \mathsf{cdf}_M(p)}{s^{-|\tau|}}$, $\quad p = \langle 0.\tau \rangle_s$, $\quad q = \langle 0.\tau \rangle_s + s^{-|\tau|}$ Approximate $p, q \in \mathtt{Rat}_s$ with $\widetilde{p}, \widetilde{q} \in \mathtt{Rat}_r$ resp.

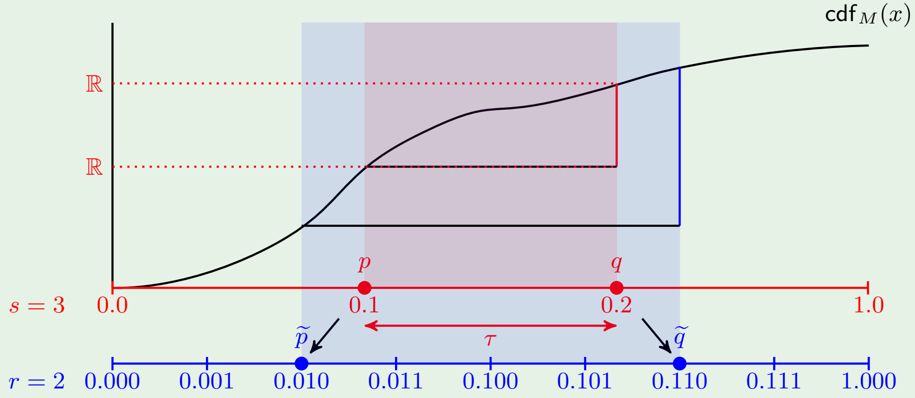


Proof of the lemma

Restatement. Given M an n^k-martingale with the savings property in base r. Get a martingale N in base s with a n^{k+1}-computable approximation such that

$$M \text{ succeeds on a real} \Rightarrow N \text{ succeeds on it}$$

Define $N(\tau) = \frac{\mathsf{cdf}_M(q) - \mathsf{cdf}_M(p)}{s^{-|\tau|}}$, $\quad p = \langle 0.\tau \rangle_s, \quad q = \langle 0.\tau \rangle_s + s^{-|\tau|}$ Approximate $p, q \in \mathtt{Rat}_s$ with $\widetilde{p}, \widetilde{q} \in \mathtt{Rat}_r$ resp. Approximate $\mathsf{cdf}_M(q) - \mathsf{cdf}_M(p)$ with $\mathsf{cdf}_M(\widetilde{q}) - \mathsf{cdf}_M(\widetilde{p})$

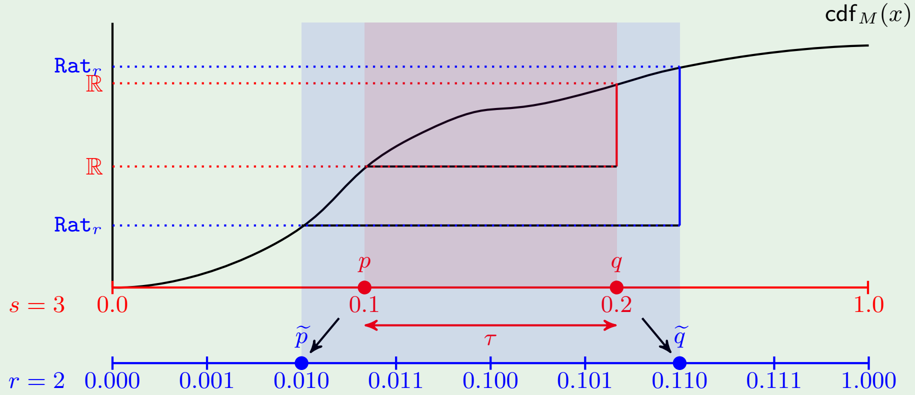


Proof of the lemma

Restatement. Given M an n^k-martingale with the savings property in base r. Get a martingale N in base s with a n^{k+1}-computable approximation such that

$$M \text{ succeeds on a real} \Rightarrow N \text{ succeeds on it}$$

Define $N(\tau) = \frac{\mathsf{cdf}_M(q) - \mathsf{cdf}_M(p)}{s^{-|\tau|}}$, $p = \langle 0.\tau \rangle_s$, $q = \langle 0.\tau \rangle_s + s^{-|\tau|}$ Approximate $p, q \in \mathtt{Rat}_s$ with $\widetilde{p}, \widetilde{q} \in \mathtt{Rat}_r$ resp. Approximate $\mathsf{cdf}_M(q) - \mathsf{cdf}_M(p)$ with $\mathsf{cdf}_M(\widetilde{q}) - \mathsf{cdf}_M(\widetilde{p}) \in \mathtt{Rat}_r$

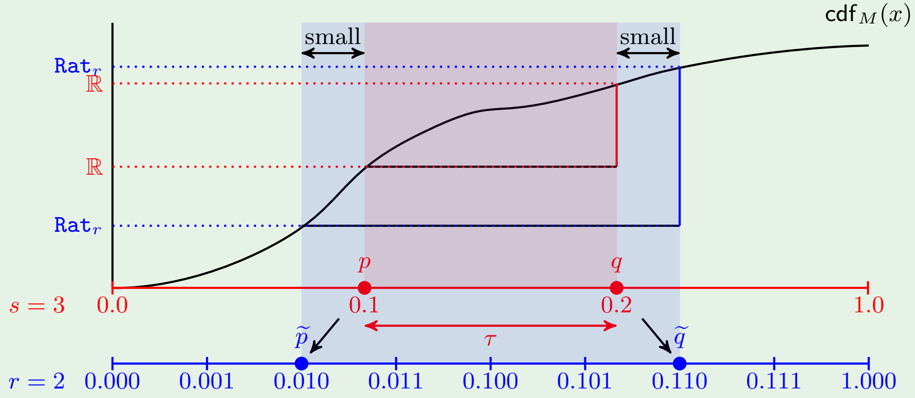


Proof of the lemma

Restatement. Given M an n^k-martingale with the savings property in base r. Get a martingale N in base s with a n^{k+1}-computable approximation such that

$$M \text{ succeeds on a real} \Rightarrow N \text{ succeeds on it}$$

Define $N(\tau) = \frac{\mathsf{cdf}_M(q) - \mathsf{cdf}_M(p)}{s^{-|\tau|}}$, $\quad p = \langle 0.\tau \rangle_s$, $\quad q = \langle 0.\tau \rangle_s + s^{-|\tau|}$ Approximate $p, q \in \mathtt{Rat}_s$ with $\widetilde{p}, \widetilde{q} \in \mathtt{Rat}_r$ resp. Approximate $\mathsf{cdf}_M(q) - \mathsf{cdf}_M(p)$ with $\mathsf{cdf}_M(\widetilde{q}) - \mathsf{cdf}_M(\widetilde{p}) \in \mathtt{Rat}_r$

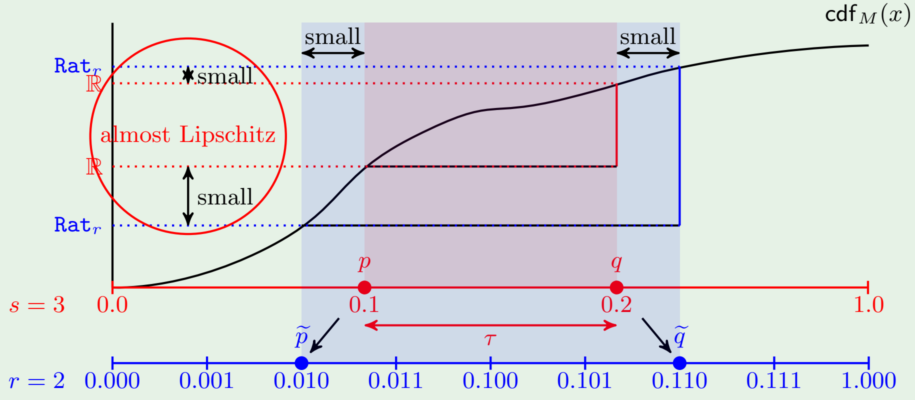


Proof of the lemma

Restatement. Given M an n^k-martingale with the savings property in base r. Get a martingale N in base s with a n^{k+1}-computable approximation such that

$$M \text{ succeeds on a real} \Rightarrow N \text{ succeeds on it}$$

Define $N(\tau) = \frac{\mathsf{cdf}_M(q) - \mathsf{cdf}_M(p)}{s^{-|\tau|}}$, $\quad p = \langle 0.\tau \rangle_s$, $\quad q = \langle 0.\tau \rangle_s + s^{-|\tau|}$ Approximate $p, q \in \mathtt{Rat}_s$ with $\widetilde{p}, \widetilde{q} \in \mathtt{Rat}_r$ resp. Approximate $\mathsf{cdf}_M(q) - \mathsf{cdf}_M(p)$ with $\mathsf{cdf}_M(\widetilde{q}) - \mathsf{cdf}_M(\widetilde{p}) \in \mathtt{Rat}_r$



Polynomial time randomness is base invariant

Theorem (F, Nies 2013)

Let $k \geq 1$. If $Y \in \Sigma_s^\infty$ is n^{k+3}-random in base s and $X \in \Sigma_r^\infty$ is such that $\langle 0.X \rangle_r = \langle 0.Y \rangle_s$ then X is n^k-random in base r. In particular, polynomial time randomness is base invariant.

Polynomial time randomness is base invariant

Theorem (F, Nies 2013)

Let $k \geq 1$. If $Y \in \Sigma_s^\infty$ is n^{k+3}-random in base s and $X \in \Sigma_r^\infty$ is such that $\langle 0.X \rangle_r = \langle 0.Y \rangle_s$ then X is n^k-random in base r. In particular, polynomial time randomness is base invariant.

Proof.

- Suppose that $X \in \Sigma_r^\infty$ is not n^k-random in base r

Polynomial time randomness is base invariant

Theorem (F, Nies 2013)

Let $k \geq 1$. If $Y \in \Sigma_s^\infty$ is n^{k+3}-random in base s and $X \in \Sigma_r^\infty$ is such that $\langle 0.X \rangle_r = \langle 0.Y \rangle_s$ then X is n^k-random in base r. In particular, polynomial time randomness is base invariant.

Proof.

- Suppose that $X \in \Sigma_r^\infty$ is not n^k-random in base r
- Let M be an n^k-martingale in base r which succeeds on X

Polynomial time randomness is base invariant

Theorem (F, Nies 2013)

Let $k \geq 1$. If $Y \in \Sigma_s^\infty$ is n^{k+3}-random in base s and $X \in \Sigma_r^\infty$ is such that $\langle 0.X \rangle_r = \langle 0.Y \rangle_s$ then X is n^k-random in base r. In particular, polynomial time randomness is base invariant.

Proof.

- Suppose that $X \in \Sigma_r^\infty$ is not n^k-random in base r
- Let M be an n^k-martingale in base r which succeeds on X
- There is a n^{k+1}-martingale $\widetilde{M}$ in base r with the savings property such that $\widetilde{M}$ succeeds on X

Polynomial time randomness is base invariant

Theorem (F, Nies 2013)

Let $k \geq 1$. If $Y \in \Sigma_s^\infty$ is n^{k+3}-random in base s and $X \in \Sigma_r^\infty$ is such that $\langle 0.X \rangle_r = \langle 0.Y \rangle_s$ then X is n^k-random in base r. In particular, polynomial time randomness is base invariant.

Proof.

- Suppose that $X \in \Sigma_r^\infty$ is not n^k-random in base r
- Let M be an n^k-martingale in base r which succeeds on X
- There is a n^{k+1}-martingale $\widetilde{M}$ in base r with the savings property such that $\widetilde{M}$ succeeds on X
- By the lemma there is a (real-valued) martingale N in base s with an n^{k+2}-computable approximation, which succeeds on Y.

Polynomial time randomness is base invariant

Theorem (F, Nies 2013)

Let $k \geq 1$. If $Y \in \Sigma_s^\infty$ is n^{k+3}-random in base s and $X \in \Sigma_r^\infty$ is such that $\langle 0.X \rangle_r = \langle 0.Y \rangle_s$ then X is n^k-random in base r. In particular, polynomial time randomness is base invariant.

Proof.

- Suppose that $X \in \Sigma_r^\infty$ is not n^k-random in base r
- Let M be an n^k-martingale in base r which succeeds on X
- There is a n^{k+1}-martingale $\widetilde{M}$ in base r with the savings property such that $\widetilde{M}$ succeeds on X
- By the lemma there is a (real-valued) martingale N in base s with an n^{k+2}-computable approximation, which succeeds on Y.
- There is an n^{k+3}-martingale $\widetilde{N} \geq N$ in base s

$\square$

Outline

Normality and absolute normality

Let $\mathsf{occ}_\sigma(\tau)$ denote the number of occurrences of σ in τ,

Definition

- $Z \in \Sigma_r^\infty$ is normal in base r if it satisfies a general form of the law of large numbers:

$$(\forall \sigma \in \Sigma_r^*)\ \lim_n \frac{\mathsf{occ}_\sigma(Z\restriction_n)}{n} = \frac{1}{r^{|\sigma|}}.$$

- $z \in [0,1]$ is absolutely normal if whenever $z = \langle 0.Z\rangle_r$ for some $Z \in \Sigma_r^\omega$, we have that Z is normal in base r.

How much randomness is needed to be (abs.) normal?

The following result similar to Schnorr's (1971) and Wang's (1996) but with better complexity and relative to any base:

Theorem (F, Nies 2013)

If Z is $n \cdot \log^2 n$-random in base r then Z is normal in base r.

How much randomness is needed to be (abs.) normal?

The following result similar to Schnorr's (1971) and Wang's (1996) but with better complexity and relative to any base:

Theorem (F, Nies 2013)

If Z is $n \cdot \log^2 n$-random in base r then Z is normal in base r.

Using the change-of-base lemma for martingales one can show:

Theorem (F, Nies 2013)

If $Y \in \Sigma_s^\infty$ is n^4-random in base s then $y = \langle 0.Y \rangle_s$ is absolutely normal.

Computing n^k-randoms

Proposition

There is an n^k-random computable in time $O(n^{k+2} \cdot \log^3 n)$.

Proposition

There is an absolutely normal real computable in time $O(n^5 \cdot \log^3 n)$.

Becher, Heiber, Slaman (2013) have a direct construction for an absolutely normal real in time just above $O(n^2)$.

Outline

Uniformly distributed sequences and normality

A sequence $(y_j)_{j\in\mathbb{N}}$ of reals in $[0,1]$ is uniformly distributed in $[0,1]$ (u.d.) if for each interval $[u,v]\subseteq[0,1]$, the proportion of $i<N$ with $y_j\in[u,v]$ tends to $v-u$ as $N\to\infty$, that is:

$$\lim_{N\to\infty}\frac{|\{j<N \mid y_j\in[u,v]\}|}{N}=v-u.$$

Uniformly distributed sequences and normality

A sequence $(y_j)_{j \in \mathbb{N}}$ of reals in $[0,1]$ is uniformly distributed in $[0,1]$ (u.d.) if for each interval $[u,v] \subseteq [0,1]$, the proportion of $i < N$ with $y_j \in [u,v]$ tends to $v-u$ as $N \to \infty$, that is:

$$\lim_{N \to \infty} \frac{|\{j < N \mid y_j \in [u,v]\}|}{N} = v - u.$$

The following result is well-known:

Theorem

Let $Z \in \Sigma_r^\infty$ and let $z = \langle 0.Z \rangle_r$. Then Z is normal in base r iff $(\{z \cdot r^n\})_{n \in \mathbb{N}}$ is u.d.

($\{x\}$ denotes the fractional part of x.)

Rationally normal reals

A real z is absolutely normal iff for all integers $a > 1$, the sequence $(\{z \cdot a^n\})_{n \in \mathbb{N}}$ is u.d.

Definition

$z \in [0, 1]$ is rationally normal if for all rationals $r > 1$ the sequence $(\{z \cdot r^n\})_{n \in \mathbb{N}}$ is u.d.

Proposition (Special case of Brown, Moran, Pearce 1986)

Rationally normal is stronger than absolutely normal.

Open questions

Theorem (F, Nies, at the retreat 2013)

Schnorr randomness implies rational normality.

The proof is a modification of a result of Avigad (2013):

> *if z is Schnorr random then for any computable sequence of distinct integers $(a_n)_{n\in\mathbb{N}}$, the sequence $(\{z \cdot a_n\})_{n\in\mathbb{N}}$ is u.d.*

In fact, we can show something stronger:

> *if z is Schnorr random then for any computable sequence of rationals $(q_n)_{n\in\mathbb{N}}$ such that $(\exists c > 0)(\forall k, l, k \neq l)|q_k - q_l| > c$, the sequence $(\{z \cdot q_n\})_{n\in\mathbb{N}}$ is u.d.*

Open questions

Theorem (F, Nies, at the retreat 2013)

Schnorr randomness implies rational normality.

The proof is a modification of a result of Avigad (2013):

> *if z is Schnorr random then for any computable sequence of distinct integers $(a_n)_{n\in\mathbb{N}}$, the sequence $(\{z \cdot a_n\})_{n\in\mathbb{N}}$ is u.d.*

In fact, we can show something stronger:

> *if z is Schnorr random then for any computable sequence of rationals $(q_n)_{n\in\mathbb{N}}$ such that $(\exists c > 0)(\forall k, l, k \neq l)|q_k - q_l| > c$, the sequence $(\{z \cdot q_n\})_{n\in\mathbb{N}}$ is u.d.*

Conjecture

Polynomial time randomness implies rational normality.

In fact for some k, n^k-random should imply rational normality.

Question

What is the smallest such k?

Other open questions

For many of our results it may be possible to improve time bounds.

We showed a method for approximating rationals in a given base with rationals in another.

Question

Is it possible to compute $\mathsf{bc}^{-}_{s,r}(\sigma)$ in less than quadratic time?

We showed that n^{k+3}-randomness in a given base implies n^k-randomness in another base.

Question

Can we lower the '+3', or even show that n^k-randomness is base invariant (for large enough k)?

We showed that $n \cdot \log^2 n$-randomness implies normality.

Question

Does linear-randomness in base r imply normality in base r?

References

J. Avigad.
Uniform distribution and algorithmic randomness.
Journal of Symbolic Logic, 78:334–344, 2013

V. Becher, P. Heiber and T. Slaman.
A polynomial-time algorithm for computing absolutely normal numbers.
Information and Computation, 232: 1–9, 2013

V. Brattka, J. S. Miller and A. Nies.
Randomness and differentiability.
To appear in Trans. Amer. Math. Soc.

S. Figueira and A. Nies.
Feasible analysis, randomness, and base invariance.
To appear in Theory of Computing Systems.

C-P Schnorr.
Zufälligkeit und Wahrscheinlichkeit.
Lecture Notes in Mathematics, 218, 1971.

Y. Wang.
Randomness and Complexity.
PhD thesis, University of Heidelberg, 1996.