Effective fractal dimension theory: exploring the extreme cases (III)

Elvira Mayordomo

Universidad de Zaragoza, Iowa State University

August 25th 2017

Today

0. Introduction of effective dimension
1. Resource-bounded Hausdorff dimension for Complexity Classes
2. Compression and dimension for low resource bounds. **Very effective construction of a normal sequence**
3. Looking back at fractal geometry, other metric spaces

Normal numbers

Borel, 1909:

- A real number α is **normal** in base b ($b \geq 2$) if, for every finite sequence w of base-b digits,

$$\lim_{n} \frac{\mathrm{N}_{\alpha}(w, n)}{n} = \frac{1}{b^{|w|}}$$

  the asymptotic, empirical frequency of w in the base-b expansion of α is $b^{-|w|}$.

- α is **absolutely normal** if it is normal in every base $b \geq 2$.

Computing absolutely normal numbers

- (Becher, Heiber, and Slaman 2013, simultaneous work from other authors) Algorithm that computes an absolutely normal number in polynomial time.
- Specifically, they compute the binary expansion of an absolutely normal number x, with the nth bit of x appearing after $O(n^2 \mathrm{polylog}(n))$ steps.
- Here we present a new algorithm that computes an absolutely normal in **nearly linear time**. Our algorithm computes the binary expansion of an absolutely normal number x, with the nth bit of x appearing after $O(n \mathrm{polylog}(n))$ steps.

Note: The term "nearly linear time" was introduced by Gurevich and Shelah (1989). While linear time computability is very model-dependent, nearly linear time is very robust.

Gales and martingales in base b

- $\Sigma_b = \{0, \ldots, b-1\}$ the base b alphabet
- Σ_b^* are finite sequences, Σ_b^∞ infinite sequences
- For $s \in [0, \infty)$, an s-gale is a function $\Sigma_b^* \to [0..\infty)$ such that for $w \in \Sigma_b^*$

$$d(w) = \frac{\sum_{i \in \Sigma_b} d(wi)}{b^s}$$

- A **martingale** is a function $d : \Sigma_b^* \to [0..\infty)$ with the fairness property, for every finite sequence w,

$$d(w) = \frac{\sum_{i \in \Sigma_b} d(wi)}{b}$$

- The success set of an s-gale d is

$$S^\infty[d] = \left\{ x \in \Sigma_b^\infty \,\middle|\, \limsup_n d(x \upharpoonright n) = \infty \right\}$$

- **Notice that if d is an s-gale then $d'(w) = b^{(1-s)|w|} d(w)$ is a martingale**

Finite-state randomness

Definition

x is **FS random** if no finite automata computable martingale succeeds on x

Notice that if $\dim_{\mathrm{FS}}(x) < 1$ then x is not FS-random

Normality and Finite-state randomness

- If x is the base b representation of a non-normal number, w is a finite string that is "unbalanced" in x, for instance i.o. w appears more often than it should, then a finite automata can bet a bit more than its fair share and make infinite money ...
- Clearly FS random sequences are representations of base b normal numbers
- Even better **FS-random = normal** –Schnorr and Stimm (1972)

Finite-State dimension

Schnorr and Stimm (1972) implicitly defined **finite-state martingales** and proved that every sequence $S \in \Sigma_b^\infty$ obeys this dichotomy:

1. If S is b-normal, then no finite-state base-b martingale succeeds on S. (In fact, every finite-state base-b martingale decays exponentially on S.)
2. If S is not b-normal, then some finite-state base-b martingale **succeeds exponentially** on S.

Using dimension terminology

1. If S is b-normal, then S is FS-random.
2. If S is not b-normal, then $\dim_{\mathrm{FS}}(S) < 1$.

Therefore **FS-dimension 1** $=$ **normal**

Remember ...

- **Objective** Compute a (provably) absolutely normal number $x \in (0,1)$ **fast**.
- Absolutely normal number means that is normal in every base
- We need to construct a single real number that is b-normal for every base b
- We will use Lempel-Ziv algorithm that is universal for FS-compressors **in a single base**

Lempel-Ziv martingales

Feder (1991) implicitly defined the **base-b Lempel-Ziv martingale** $d_{\mathrm{LZ}(b)}$ and proved that it is at least as successful **on every sequence** as every finite-state martingale.

$\therefore$ if $S \in \Sigma_b^\infty$ is not normal, then $\dim_{d_{\mathrm{LZ}(b)}}(S) < 1$.

$\therefore$ $x \in (0,1)$ is absolutely normal if none of the martingales $d_{\mathrm{LZ}(b)}$ succeed **exponentially** on the base-b expansion of x.

Moreover, $d_{\mathrm{LZ}(b)}$ has a fast and beautiful theory.

Celebrated Lempel-Ziv compression algorithm and martingale can be both computed very efficiently (time very close to linear)

Lempel-Ziv martingales

How $d_{\mathrm{LZ}(b)}$ works:
Parse $w \in \Sigma_b^*$ into distinct **phrases**, using a growing tree whose leaves are all of the previous phrases.
At each step, bet on the next digit in proportion to the number of leaves below each of the b options.

Base change notation

- For a real x, $\mathrm{seq}_b(x) \in \Sigma_b^\infty$ is the base-b representation of x
- For a sequence $S \in \Sigma_b^\infty$, $\mathrm{real}_b(S) \in [0,1]$ is the real number represented by S

How to construct an absolutely normal number

- For each base b, we need to construct x such that b-Lempel-Ziv martingale does not succeed on x
- We need to construct a single real number that is b-normal for every base b
- It suffices to translate b-Lempel-Ziv martingale into base 2 (very efficiently)
- We need a martingale $d : \Sigma_2^* \to [0, \infty)$ that succeeds on base 2 representations of the numbers for which b-Lempel-Ziv martingale succeeds
- For this translation to be possible (**and efficient**) the martingale must be quite well behaving ...

How to construct an absolutely normal number

1. Transform b-Lempel-Ziv martingale into a better behaving and still efficient martingale that still succeeds on not b-normal sequences
2. Efficiently change base for the resulting martingale
3. Efficiently combine all resulting martingales into one
4. Diagonalize resulting martingale

Savings Accounts, strong success

- The value of Lempel-Ziv martingale $d_{\mathrm{LZ}(b)}$ on a certain infinite string S can fluctuate a lot
- This makes base change more complicated (and time consuming)
- We use the notion of "savings account" here, we are looking at an alternative martingale that **keeps money aside for the bad times to come**

The strong success set of an s-supergale d is

$$S^{\infty}_{\mathrm{str}}[d] = \left\{ x \in \{0,1\}^{\infty} \,\middle|\, \lim_{n} d(x \upharpoonright n) = \infty \right\}$$

Savings Accounts, strong success

- We construct a new martingale d'_b that is a conservative version of $d_{\mathrm{LZ}(b)}$
- d'_b strongly succeeds at least on non-b-normal sequences

$$\{S \,|\dim_{LZ}(S) < 1\} \subseteq S^{\infty}_{\mathrm{str}}[d'_b]$$

- d'_b can be computed in nearly linear time
- If $S \notin S^{\infty}_{\mathrm{str}}[d'_b]$ then S is b-normal

Base Change

- We want an absolutely normal real number x, that is, the base b representation $seq_b(x)$ is not in $S^\infty[d'_b]$
- For this we convert d'_b into a base-2 martingale $d_b^{(2)}$ succeeding on the **base-2 representations of the reals with base-b representation in $S^\infty_{\mathrm{str}}[d'_b]$**
- Again, $d_b^{(2)}$ succeeds on $\mathrm{seq}_2(\mathrm{real}_b(S^\infty_{\mathrm{str}}[d'_b])$

$$\mathrm{real}_b(S^\infty_{\mathrm{str}}[d'_b]) \subseteq \mathrm{real}_2(S^\infty_{\mathrm{str}}[d_b^{(2)}])$$

- We use Carathéodory construction to define measures
- Computing in nearly linear time is also delicate
- In fact our computation $\widehat{d_b^{(2)}}$ approximates slowly $d_b^{(2)}$

$$|\widehat{d_b^{(2)}}(y) - d_b^{(2)}(y)| \leq \frac{1}{|y|^3}$$

Absolutely Normal Numbers

- From previous steps we have a family of martingales $(d_b^{(2)})_b$ so that $d_b^{(2)}$ **succeeds on base-2 representations of non-b-normal sequences**
- For each b we have a nearly linear time computation $\widehat{d_b^{(2)}}$
- We want to construct $S \notin S^\infty[d_b^{(2)}]$ for every b
- Nearly linear time makes it painful to construct a martingale d for the union of $S^\infty[d_b^{(2)}]$
- Then we diagonalize over d to construct S

Martingale diagonalization

- For a martingale d, how to construct x such that d martingale does not succeed on x (with time similar to the computation time for d)?
- Recursive construction, if we have the prefix $x \upharpoonright n$ choose the next symbol i such that

  $$d(x \upharpoonright ni)$$

  is the minimum over all possible symbols
- By the fairness condition of a martingale

  $$d(w) = \frac{\sum_{i \in \Sigma_b} d(wi)}{b}$$

  d does not succeed on the resulting x
- Time is $n \cdot t(n)$ if d is computable in time $t(n)$

Time bounds ...

- All the steps were performed in nearly linear time on a common **time bound independent of base** b
- Many technical details were simplified in this presentation ... please read paper

Base invariance

- Normality corresponds exactly to the lowest level of algorithmic randomness, Finite-State randomness
- Finite-State randomness and Finite-State dimension are not closed under base change
- p-dimension and p-randomness are closed under base change
- What about intermediate levels, PD, LZ, nearly linear time?

Conclusions

- Lots of remaining questions,
  - can we substitute "suspected" absolute normal numbers by proven absolutely normal numbers in Cryptography?
  - "biased-normality"? (based on FS-dimension)
  - Tight complexity for the operation of base change
  - The algorithm of Becher, Heiber, and Slaman's has nearly quadratic time but (apparently) a much lower discrepancy. Can we improve our discrepancy while maintaining nearly linear time?

References for construction of absolutely normal numbers

- J. H. Lutz and E. Mayordomo, Computing absolutely normal numbers in nearly linear time, submitted. (arxiv 1611.05911)
- V. Becher, P.A. Heiber, and T. Slaman, A polynomial-time algorithm for computing absolutely normal numbers, Information and Computation 232: 1–9, 2013.
- C. Aistleitner, V. Becher, A.-M. Scheerer, and T. Slaman, On the construction of absolutely normal numbers, 2017, to appear in Acta Arithmetica. (arXiv 1707.02628)
- V. Becher, S.Figueira, and R. Picchi, Turing's unpublished algorithm for normal numbers, Theoretical Computer Science 377: 126-138, 2007.

References

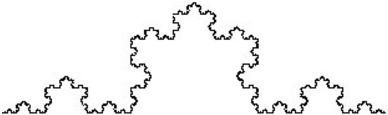
- V. Becher and S. Yuhjtman, On absolutely normal and continued fraction normal numbers, 2017, to appear in International Mathematics Research Notices. (arXiv 1704.03622)
- V. Becher, P.A. Heiber and T. Slaman, A computable absolutely normal Liouville number, Mathematics of Computation 84(296): 2939–2952, 2015.

Next

0. Introduction of effective dimension
1. Resource-bounded Hausdorff dimension for Complexity Classes
2. Compression and dimension for low resource bounds. Very effective construction of a normal sequence
3. **Looking back at fractal geometry, other metric spaces**

Hausdorff definition of dimension

Hausdorff, 1919: Rigorous formulation of dimension.



Hausdorff definition of dimension

Let ρ be a metric on a set X.

- The diameter of a set $A \subseteq X$ is

$$\operatorname{diam}(A) = \sup\{\rho(x,y) \,|\, x, y \in A\}.$$

- For $A \subseteq X$ and $\delta > 0$, a δ-cover of A is a collection $\mathcal{U}$ such that for all $U \in \mathcal{U}$, $\operatorname{diam}(U) \leq \delta$ and

$$A \subseteq \bigcup_{U \in \mathcal{U}} U.$$

- For $s \geq 0$,
  $H^s_\delta(A) = \inf_{\mathcal{U} \text{ is a } \delta\text{-cover of } A} \sum_{U \in \mathcal{U}} \operatorname{diam}(U)^s$

- $H^s(A) = \lim_{\delta \to 0} H^s_\delta(A)$

$H^s(A) =$ the s-dimensional Hausdorff measure of A

Hausdorff definition of dimension

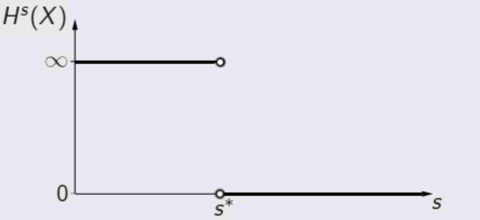
$H^s_\delta(A) = \inf_{\mathcal{U} \text{ is a } \delta\text{-cover}} \sum_{U \in \mathcal{U}} \operatorname{diam}(U)^s$

$H^s(A) = \lim_{\delta \to 0} H^s_\delta(A)$

Definition (Fractal Dimension)

Let ρ be a metric on X, and let $A \subseteq X$.

- (Hausdorff 1919) The Hausdorff dimension of A is
  $$\dim_{\mathrm{H}}(A) = \inf\{s \,|\, H^s(A) = 0\}.$$



Characteristics of effective dimension in Cantor and Euclidean spaces

- It is non necessarily zero and meaningful on singletons
- It coincides with Hausdorff dimension in many interesting cases
- It can be characterized in terms of Kolmogorov complexity

Individual points

Definition

Let $x \in \Sigma^\infty$ ($x \in \mathbb{R}^m$).

- The dimension of x is $\dim(x) = \mathrm{cdim}(\{x\})$.

Absolute Stability of Constructive Dimension

Theorem

For all $A \subseteq \Sigma^\infty$ ($A \subseteq \mathbb{R}$),
$\mathrm{cdim}(A) = \sup_{x \in A} \dim(x)$.

(Contrast with countable stability of classical dimension.)

$\therefore$ Constructive dimension is investigated in terms of individual points.

Correspondence principle

A correspondence principle for an effective dimension is a theorem stating that, on sufficiently simple sets, the effective dimension coincides with its classical counterpart. (Terminology stolen from N. Bohr by Lutz.)

Correspondence Principle for Constructive Dimension

Theorem (Hitchcock 2002)

If $X \subseteq \Sigma^\infty$ is any union (not necessarily effective) of computably closed (i.e., Π^0_1) sets then $\mathrm{cdim}(X) = \dim_{\mathrm{H}}(X)$.

Kolmogorov complexity characterization for Euclidean space

What is the information content of $x \in \mathbb{R}^m$?

Definition

Let $x \in \mathbb{R}^m$, let $r \in \mathbb{N}$. The Kolmogorov complexity of x at precision r is

$$\mathrm{K}_r(x) = \inf \left\{ \mathrm{K}(q) \,\middle|\, q \in \mathbb{Q}, |q - x| \leq 2^{-r} \right\}.$$

with $\mathrm{K}_r(x) = \infty$ if not such w exists.

Theorem

Let $x \in \mathbb{R}^m$,

$$\mathrm{cdim}(x) = \liminf_r \frac{\mathrm{K}_r(x)}{r}.$$

Effective dimension in Euclidean space

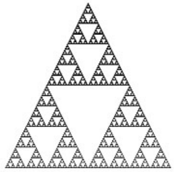
Goals:

- Pointwise analysis of dimensions
- Calculation of dimensions
- Extensions of computable analysis

Results so far

Effective dimension in Euclidean space has analyzed the dimension of points in

- self-similar fractals,
- random self-similar fractals,
- lines in $\mathbb{R}^2$



For each of them we can

- know the dimension spectra of the points in the set
- find a maximal dimension point (closest to a random point in the set)

Why should effective dimension be interesting in fractal geometry?

Point to set principle

Theorem (Lutz, Lutz 2017)

For every $E \subseteq \{0,1\}^\infty$ *(*$E \subseteq \mathbb{R}^m$*),*
$\dim(E) = \min_{B \subseteq \{0,1\}^*} \mathrm{cdim}^B(E)$.

- **This theorem allows us to prove classical dimension results using Kolmogorov complexity**

We now get results in classical fractal geometry ...

- N. Lutz shows that a known intersection formula for Borel sets holds for arbitrary sets, and it significantly simplifies the proof of a known product formula. So for arbitrary $E, F \subseteq \mathbb{R}^m$, for almost every $z \in \mathbb{R}^m$,

$$\dim_{\mathrm{H}}(E \cap (F + z)) = \max\{0, \dim_{\mathrm{H}}(E \times F) - m\}$$

- N. Lutz and D. Stull get an improved lower bound on the (classical) Hausdorff dimension of generalized sets of Furstenberg type.
- Lutz and Lutz give a simpler proof of the two-dimensional case of the Kakeya conjecture.

General spaces

- Effective dimension was first defined on the Cantor space (set of infinite binary sequences)
- At very low resource-bounds **alphabet matters** (Finite-State compressors/gamblers), so we use infinite sequences over an arbitrary finite alphabet
- Hausdorff dimension is well studied over Euclidean space, effective dimension has meaningful geometric results too
- Can we effectivize dimension in other metric spaces retaining the robustness properties?

General spaces

- In many interesting cases, a gambling characterization of classical Hausdorff dimension is proven, allowing effectivization
- We have the same strong properties: pointwise dimension, Kolmogorov Complexity characterization, ...
- We also have a point to set principle: classical dimension can be characterized in terms of oracle effective dimension

Interesting examples

- the set of polynomials with real coefficients and bounded degree, together with the metric $d(f,g) = \|f - g\|_\infty$.
- The space of compact subsets of [0,1] with the Hausdorff distance.

References

- J. H. Lutz and E. Mayordomo, Dimensions of points in self-similar fractals, SIAM Journal on Computing, 38 (2008)
- X. Gu, J. H. Lutz, E. Mayordomo, and P. Moser, Dimension spectra of random subfractals of self-similar fractals, Annals of Pure and Applied Logic 165 (2014).
- Jack H. Lutz and Neil Lutz, Algorithmic information, plane Kakeya sets, and conditional dimension, STACS 2017.
- N. Lutz, Fractal Intersections and Products via Algorithmic Dimension, MFCS 2017.
- N. Lutz and D. M. Stull, Bounding the Dimension of Points on a Line TAMC 2017.
- Elvira Mayordomo, Effective dimension in general metric spaces, submitted

Rod's request on $\dim_{\mathrm{p}}(\mathrm{NP}) > 0$ implies hard sets are dense

Theorem

If $\dim_{\mathrm{p}}(\mathrm{NP}) > 0$ then all $\leq^{\mathrm{p}}_{n^{\alpha}-\mathrm{T}}$-hard sets for NP are dense

Based on ...

Theorem

(Hitchcock 2005, Harkins Hitchcock 2011) Let $\alpha < 1$, *then*

$$\dim_{\mathrm{p}}(\mathrm{P}_{n^\alpha-\mathrm{T}}(\mathrm{DENSE}^c)) = 0$$

Ideas about the proof

- Allender et al. (92) prove that $\mathrm{P}_{1-\mathrm{tt}}(\mathrm{DENSE}^c) \subseteq \mathrm{P}_d(\mathrm{DENSE}^c)$ (more or less)
- This leads to

$$\mathrm{P}_{n^\alpha-\mathrm{T}}(\mathrm{DENSE}^c) \subseteq \mathrm{DTIME}(2^{n^\delta})_d(\mathrm{DENSE}^c)$$

- the set of reducible to learnable concepts has p-dimension 0
- sets that disjunctively reduce to nondense are reducible to learnable classes (monotone disjunctions with few literals)

We covered

0. Introduction of effective dimension
1. Resource-bounded Hausdorff dimension for Complexity Classes
2. Compression and dimension for low resource bounds. Very effective construction of a normal sequence
3. Looking back at fractal geometry, other metric spaces