Accepted in Seventh International Conference on Computability, Complexity and Randomness (CCR 2012)

2-6 July 2012, Isaac Newton Institute for Mathematical Science, Cambridge, Great Britain

Normality and differentiability

Verónica Becher Pablo Ariel Heiber
vbecher@dc.uba.ar pheiber@dc.uba.ar
Departamento de Computación, Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires
February 2012

We obtain a characterization of the property of Borel normality on real numbers, by transferring to the world of functions computable by finite automata the classical theorem of numerical analysis establishing that every non-decreasing real valued function is almost everywhere differentiable. We consider functions mapping infinite sequences to infinite sequences and a notion of differentiability that, on the class of non-decreasing real valued functions, coincides with standard differentiability.

Theorem. The following are equivalent, for a real $xin[0, 1]$:

(1) x is normal to base b.

(2) Every non-decreasing function computable by a finite automaton mapping infinite sequences to infinite sequences is differentiable at the expansion of x in base b.

(3) Every non-decreasing function computable by a finite automaton in base b mapping real numbers to real numbers is differentiable at x.

The proof of the Theorem relies in the characterization of normal sequences as those incompressible by lossless finite-state compressors. This result that follows from [7, 5, 6], a direct and elementary proof can be read in [1]. An adaptation is needed to deal with the non-decreasing condition.

The statement of the above theorem was motivated by the pleasing recent result of Brattka, Miller and Nies [2] that shows the counterpart result in the world of functions computable by Turing machines: a real number r in the unit interval is computably random if and only if every nondecreasing computable function from the unit interval to the real numbers is differentiable at r. However, the techniques in their proof are completeley different from the technique we use in the context of finite automata. We just give here the definitions needed to give a precise meaning to the Theorem.

For a real number r we consider the unique expansion in base b of the form $r = \lfloor x \rfloor + \sum_{n=1}^{\infty} a_n b^{-n}$ where the integers $0 \leq a_n < b$, and $a_n < b - 1$ infinitely many times. This last condition over a_n ensures a unique representation of every rational number. Let us recall that Borel's original definition of normality in [3] is equivalent to the following simpler one [4].

Definition. A real number r is simply normal to a given base b if each digit in $\{0, 1, .., (b-1)\}$ occurs with the same limiting frequency $1/b$ in the expansion of r in base b. A number is *normal to base* b if it is simply normal to the each base b^i, for very positive integer i.

For a finite set of symbols $\mathcal{A}$ we write $\mathcal{A}^*$ and $\mathcal{A}^\omega$ to denote, respectively, the set of finite and infinite sequences of symbols in $\mathcal{A}$, We consider finite automata endowed with an output function (often called finite transducers).

Definition. (1) A *finite automaton* is a 4-uple $C = \langle \mathcal{Q}, q_0, \delta, o \rangle$, where $\mathcal{Q}$ is a finite set of states, $q_0 \in \mathcal{Q}$ is the initial state, $\delta : \mathcal{Q} \times \mathcal{A} \to \mathcal{Q}$ is the transition function and $o : \mathcal{Q} \times \mathcal{A} \to \mathcal{A}^*$ is the output function. A finite automaton processes the input symbols according to the current state q. When a symbol $a \in \mathcal{A}$ is read, the automaton moves to state $\delta(q,a)$ and outputs $o(q,a)$. The extension of δ and o to process strings are $\delta^* : \mathcal{Q} \times \mathcal{A}^* \to \mathcal{Q}$ and $o^* : \mathcal{Q} \times \mathcal{A}^* \to \mathcal{A}^*$ such that, for $a \in \mathcal{A}$, $s \in \mathcal{A}^*$ and λ the empty string, $\delta^*(q,\lambda) = q$, $\delta^*(q,as) = \delta^*(\delta(q,a),s)$, and $o^*(q,\lambda) = \lambda$, $o^*(q,as) = o(q,a)o^*(\delta(q,a),s)$. The extension of o to infinite sequences $o^* : \mathcal{Q} \times A^\omega \to A^\omega$ is $o^*(q,x) = \lim_{k\to\infty} o(q,x[1..k])$.

(2) The function $f_C : A^\omega \to A^\omega$ computed by $C = \langle \mathcal{Q}, q_0, \delta, o \rangle$ is $f_C(x) = o^*(q_0, x)$.

(3) A function $f : A^\omega \to A^\omega$ is computable by a finite automaton when $f = f_C$ for some finite automaton C. A function $f : A^\omega \to \mathbb{R}$ is computable by a finite automaton when $f = \mathrm{conv}(f_C)$ for some finite automaton C, where $\mathrm{conv} : A^\omega \to \mathbb{R}$ is the usual map $\mathrm{conv}(x) = \sum_{i\geq 1} t^{-i}x[i]$, with t the cardinality of $\mathcal{A}$.

The following example shows that the obvious definition of differentiability is not appropriate for our purposes.

Example. Let $I = \langle q, q, \pi_1, \pi_2 \rangle$ where π_1 and π_2 are respectively the projections functions of the first and second argument. So, the function $f_I : \{0,1\}^\omega \to \mathbb{R}$ is the identify function mapped to the unit interval. The obvious definition of differentiability would yield $\lim_{k\to\infty} 2^{-k}(\mathrm{conv}(\pi_2^*(q, x[1..k-1]1)) - \mathrm{conv}(\pi_2^*(q, x[1..k-1]0))) = 1$. Now, let $C = \langle \{q, r_0, r_1\}, q, \delta, o \rangle$ such that for $a, b \in \mathbf{2}$, $\delta(q,b) = r_b, \delta(r_b, a) = q, o(q,b) = \lambda, o(r_b,a) = ba$. It is easy to check that $f_C : \{0,1\}^\omega \to \mathbb{R}$ is also the identify function mapped to the unit interval. However, $\lim_{k\to\infty} 2^{-k}(\mathrm{conv}(o^*(q, x[1..k-1]0)) - \mathrm{conv}(o^*(q, x[1..k-1]0)))$ does not exist for any x.

Definition. The differential of a non-decreasing function $f : A^\omega \to \mathbb{R}$ at x is

$$Df(x) = \lim_{k\to\infty} \mu(f(T_{x[1..k]}))/\mu(T_{x[1..k]}),$$

where t is the cardinality of $\mathcal{A}$, $T_s = \{sx : x \in A^\omega\}$ is the cone defined by the string s, and $f(T_s) = \{f(sx) : x \in A^\omega\}$. We say that f is differentiable at x if $Df(x)$ exists.

Proposition. Let $f : A^\omega \to \mathbb{R}$ be non-decreasing. Then, for every x is

$$D_f(x) = \lim_{k\to\infty} t^{-k}(f(x[1..k]1^\omega) - f(x[1..k]0^\omega)).$$

References

[1] Becher, V., P.A.Heiber. 2012. Normal numbers and finite automata, submitted.

[2] Brattka,V., Miller, J.S., Nies, A. 2011. Randomness and differentiability, submitted. Available at http://arxiv.org/abs/1104.4465

[3] Borel, Émile. 1909. Les probabilités dénombrables et leurs applications arithmétiques. *Rendiconti del Circolo Matematico di Palermo*, 27:247–271.

[4] Bugeaud, Yann. 2012. *Distribution Modulo One and Diophantine Approximation*, Cambridge University Press.

[5] Bourke, C., Hitchcock, J., Vinodchandran, N. 2005. Entropy rates and finite-state dimension. *Theoretical Computer Science*, 349 (3): 392–406.

[6] Dai, L., J., Lutz, J., Mayordomo, E. 2004. Finite-state dimension *Theoretical Computer Science*, 310:1–33.

[7] Schnorr, Claus-Peter, Stimm, H. 1972. Endliche Automaten und Zufallsfolgen, *Acta Informatica* 1: 345–359.