# A Constructive Generalization of the Borel-Cantelli Lemma with Application to the Complexity of Infinite Strings

Richard A. DeMillo
Richard J. Lipton

Research Report #59

December 1975

This research was supported in part by the Office of Naval Research under Grant N00014-75-C-0752.

# A Constructive Generalization of the Borel-Cantelli Lemma with Application to the Complexity of Infinite Strings

Richard A. DeMillo
Department of Electrical
Engineering and Computer Science
University of Wisconsin
Milwaukee, Wisconsin 53201

Richard J. Lipton
Department of Computer Science
Yale University
New Haven, Connecticut 06520

## 1. Introduction

This paper concerns a constructive adaptation of the Borel-Cantelli lemma and the variants of it known as 0,1 laws [1]. In general we restrict our attention to techniques that allow us to solve problems of the following variety: Given effective rules for constructing finite objects and measuring their complexity, when does there exist an infinite object that is decomposable into infinitely many finite parts that are maximally complex? We choose to set such problems in the context of the complexity theory for infinite strings, since results phrased in this way have implications for other aspects of complexity theory (e.g. the complexity of polynomial evaluation [2,3]).

Let $\{0,1\}^*$ denote the set of all finite strings over the alphabet $\{0,1\}$, let $\{0,1\}^\omega$ denote the set of all infinite 0,1 strings, and let N denote the set of non-negative integers.

By a complexity measure on strings we mean a function

$$c: \{0,1\}^* \to N.$$

There are several natural examples of such measures: Let $\alpha \in \{0,1\}^*$; then, for instance, we can take $c(\alpha_0,\ldots,\alpha_k)$ to be either

(i) the complexity in the sense of [6] of the string $\alpha_0,\ldots,\alpha_k$

or (ii) the length of the shortest straightline program that evaluates the polynomial

$$\sum_{i=0}^{k} \alpha_k x^i$$

with coefficients $\alpha_0,\ldots,\alpha_k$.

From all strings of length k, we can choose those with maximal complexity $c_k$:

$$c_k = \max_{\alpha\in\{0,1\}^*} \{c(\alpha) : |\alpha| = k\}^\dagger$$

With this notation, we can phrase our problem more precisely:

When does there exist $\alpha \in \{0,1\}^\omega$ such that (*)

$c(\alpha_0,\ldots,\alpha_{k-1}) = c_k$ for infinitely many $k \in N$?

Problems such as (*) have comcrete motivation. Consider polynomials with 0,1 coefficients that are hard to evaluate in the sense of [3], that is, polynomials with the property that the 0,1 string obtained by concatenation of coefficients is of maximal complexity. Conversely, if $\alpha$ is a finite or infinite string over {0,1}, then $\alpha$ corresponds in a natural way to a power series

$$q^\alpha(x) = \sum_{i=0}^{|\alpha|} \alpha_i x^i.$$

For $|\alpha| < \infty$, we can take $c(\alpha_0,\ldots,\alpha_{|\alpha|-1})$ to be the number of non-scalar multiplications required to evaluate the polynomial $q^\alpha(x)$ by a straightline

---

† We use $|\alpha|$ to denote the length of $\alpha$. If $\alpha \in \{0,1\}^\omega$, then by convention $|\alpha| = \infty$.

program. Suppose that $c(\alpha_0,\ldots,\alpha_{k-1}) = c_k$. Then by adaptation of (*) we ask whether there is an infinite power series

$$\sum_{i=0}^{\infty} \alpha_i x^i$$

for which there are infinitely many hard initial segments; i.e. for infinitely many $n \in N$, the polynomial

$$\sum_{i=0}^{n} \alpha_i x^i$$

gives $c(\alpha_0,\ldots,\alpha_n) = c_{n+1}$. A specific instance of this problem has been examined by Lipton [3], who showed the following.

*Theorem 1:* There is a power series

$$\sum_{i=0}^{\infty} \alpha_i x^i$$

with $\alpha_i \in \{0,1\}$, $i = 0,..,$ such that for infinitely many $n \in N$

$$c(\alpha_0,\ldots,\alpha_n) = c_{n+1} \geq \frac{\epsilon n^{1/4}}{\log n}$$

for some fixed $\epsilon > 0$.

Our main result is a step toward solving (*) in a more general context. Let $M_k$ be the number of strings $\alpha \in \{0,1\}^*$ such that $|\alpha| = k$ and $c(\alpha) = c_k$. If there exists a real $\epsilon$, $0 < \epsilon \leq 1$, such that

$$\frac{M_k}{2^k} \geq \epsilon$$

for infinitely many k, then there exists an infinite $\beta \in \{0,1\}^\omega$ such that

$$c(\beta_0,\ldots,\beta_n) = c_{n+1}$$

for infinitely many $n \in N$. We actually present two proofs of this result. One proof is an easy corollary of the nonconstructive Borel-Cantelli lemma. This proof gives almost no information regarding the string $\beta$ beyond its existence with nonzero probability -- indeed, all this is provided by such a proof is an infinite set of strings that satisfy the conclusion. For our purposes, however, more insight is needed into the construction of $\beta$. Therefore we give a more careful counting argument, which shows that if the complexity measure c is a recursive function then the construction corresponds to a computation in the Turing degree 0" [7]. Thus, even when viewed as a strictly measure-theoretic argument, our result carries independent interest since it gives a constructive proof technique for a class of theorems whose only previous proofs have been nonconstructive existence proofs (Erdös [4]).

## 2. Red Trees

Problems of the form (*) can be viewed as problems concerning infinite trees by making a simple observation. By way of analogy with Theorem 1, we call finite strings with maximal complexity hard strings and say that an infinite string is hard infinitely often if it has infinitely many hard initial prefixes. Since there is a natural correspondence between sets of strings closed under the prefix relation and trees, we will interpret (*) as dealing with infinite trees in which nodes can be colored red or white. A red branch from the root will be a hard string. We will show how to construct infinite branches that are red infinitely often for trees having the required distribution of red nodes.

By a red tree we mean a countably infinite binary tree whose nodes are partitioned into white nodes, denoted $V_W$, and red nodes, denoted $V_R$. If T is a tree and $x \in V_R \cup V_W$, then $T_x$ denotes the subtree of T with root x. For $A \subseteq V_R \cup V_W$, A' denotes the set of descendants of elements of A; i.e.

$$A' = \bigcup_{x \in A} T_x.$$

For any tree T and any node x of T, $d_T(x)$ denotes the depth of x in T, i.e. the length of the branch joining x with the root of T. A level of T is the set of nodes at a given depth; for $k \in N$,

$$\ell_T(k) = \{x: d_T(x) = k\}.$$

If T is a red tree and $\varepsilon$ is a real number, $0 < \varepsilon \leq 1$, then we say that T is $\varepsilon$-red if for infinitely many $k \in N$

$$|\ell_T(k) \cap V_R| \geq \varepsilon 2^k.$$

Intuitively, we sat that T is $\varepsilon$-red if there are infinitely many levels at which some fixed positive fraction of the nodes are colored red.

The key property of $\varepsilon$-red trees is established by the following theorem.

*Theorem 2:* If T is an $\varepsilon$-red tree, then for some $\varepsilon' > 0$ and some $x \in V_R$, $T_x$ is $\varepsilon'$-red.

*Proof:* For any node $x \in V_R \cup V_W$ and $\lambda > 0$, we define $f(x,\lambda)$ as follows:

$$f(x,\lambda) = \mu k[(\forall n)(n \geq k \rightarrow |\ell_{T_x}(n) \cap V_R| < \lambda 2^n]. \dagger \qquad (2.1)$$

If there are $x \in V_R$ and $\lambda > 0$ such that $f(x,\lambda) = \infty$, then for all k there exists $n \geq k$ such that

$$|\ell_{T_x}(n) \cap V_R| \geq \lambda 2^n,$$

and thus $T_x$ is $\lambda$-red. Hence, it is sufficient to assume that for all $x \in V_R$ and $\lambda > 0$

$$f(x,\lambda) < \infty$$

in order to derive a contradiction.

Choose $d \in N$, $\delta < 0$, such that

$$1 - d\varepsilon + (d-1)\cdot\delta < 0. \qquad (2.2)$$

---

† For any predicate $P(v,x_1,\ldots,x_n)$, $\mu y[P(y,x_1,\ldots,x_n)]$ denotes the smallest $v \in N$ such that $P(v,x_1,\ldots,x_n)$ holds.

We will now describe a construction that at its $n$*th* stage define :

(i) a depth $k_n$ of T,

(ii) a set of white nodes $W_n$,

(iii) a set of red nodes $NR_n$,

(iv) a set of red nodes $OR_n$,

(v) a set of red nodes $R_n = NR_n \cup OR_n$.

The distribution of $W_n$, $NR_n$, $OR_n$ at the $n$*th* stage of construction is shown in Figure 1. Using the fact that $f(x,\lambda) < \infty$ at each stage, our construction will allow us to accumulate red nodes discarded at previous stages, the old red nodes $OR_n$, along with the new red nodes $NR_n$ encountered at the current stage and white nodes $W_n$ until at some achievable stage the assumption that $f(x,\lambda) < \infty$ forces an impossible condition on $W_n$.

We now give an inductive description of the construction.

*Stage 1:* (i) construction of $k_1$: Since T is $\varepsilon$-red, there is some $b \in N$ such that

$$|\ell_T(b) \cap V_R| \geq \varepsilon 2^b;$$

therefore set $k_1 = b$;

(ii) $W_1 = V_W \cap \ell_T(k_1)$;

(iii) $NR_1 = V_R \cap \ell_T(k_1)$;

(iv) $OR_1 = \phi$ ($\phi$ = empty set);

(v) $R_1 = NR_1 \cup OR_1$.

Assume that Stages 1,...,n are complete and consider

To establish this claim, consider Stage n of the construction outlined above (see Figure 1). By step (iv),

$$OR_n = \bigcup_{i=1}^{n-1} Q_i$$

where $Q_i \subseteq V_R \cap \ell_T(k_n) \cap R_i'$. But for $1 \le i < n$

$$|Q_i| \le |R_i| \cdot \max_{x \in R_i} |\ell_T(k_n) \cap V_R \cap T_x|,$$

and since for $\Phi$ defined by (2.4)

$$k_n \ge \max \{f(x, \frac{\delta}{(n-1)\Phi(n-1)}) : x \in R_1 \cup R_2 \cup \ldots \cup R_{n-1}\}$$

it follows that for $i = 1,\ldots,n-1$

$$|Q_i| \le \frac{|R_i| \cdot \delta \cdot 2^{k_n}}{(n-1)\Phi(n-1)} .$$

Therefore

$$\begin{aligned} & |OR_n| \qquad (2.5) \\ & \le \sum_{i=1}^{n-1} \frac{|R_i| \cdot \delta 2^{k_n}}{(n-1)\Phi(n-1)} \\ & \le \delta 2^{k_n} \sum_{i=1}^{n-1} \frac{|R_i|}{(n-1)\Phi(n-1)} \\ & \le \delta 2^{k_n}, \end{aligned}$$

establishing our claim.

Now, by the definition of $k_n$,

$$|OR_n| + |NR_n| \ge \varepsilon 2^{k_n},$$

and thus by (2.5)

$$|NR_n| \geq (\varepsilon-\delta)2^{k_n}. \tag{2.6}$$

We know by steps (iii) and (iv) of Stage n that $W_n \cap NR_n = \Phi$ and

$$W_n \cup NR_n = W'_{n-1} \cap \ell_T(k_n),$$

so that

$$|W_n| + |NR_n| = |W_{n-1}| \cdot 2^{k_n-k_{n-1}},$$

and therefore, by (2.6),

$$|W_n| \leq |W_{n-1}| \cdot 2^{k_n-k_{n-1}} - (\varepsilon-\delta)2^{k_n}.$$

Proceeding inductively, we finally obtain

$$\begin{aligned} & |W_n| \\ \leq\ & (1 - (n-1)\varepsilon + (n-2)\delta) \cdot 2^{k_{n-1}} \cdot 2^{k_n-k_{n-1}} - (\varepsilon-\delta)2^{k_n} \\ \leq\ & (1 - n\varepsilon + (n-1)\delta) \cdot 2^{k_n}. \quad \square \end{aligned}$$

Returning now to the proof of the main theorem, let us consider Stage n = d of the construction. By (2.2) and the lemma, we have

$$|W_d| \leq (1 - d\varepsilon + (d-1)\delta) \cdot 2^{k_d} < 0,$$

which is clearly impossible. Thus we conclude that for some $x \in V_R$ and $0 < \lambda \leq 1$ $f(x,\lambda) = \infty$. $\square$

We are now ready to prove our main result. The constructive proof will follow directly from Theorem 2, while the nonconstructive proof relies on the following technical fact:

*Lemma* (Lemperti [5]): Let $M = A_1,\ldots,A_n,\ldots$ be events in a sample space and let $\nu$ be a probability measure such that

$$\sum_{i=1}^{\infty} \nu(A_i) = \infty$$

and for some real $\varepsilon > 0$

$$\nu(A_n \cap A_m) \leq \varepsilon\, \nu(A_n)\, \nu(A_m)$$

for infinitely many $n,m \in N$. Then

$$\nu(\limsup_{n\to\infty} A_n) > 0,$$

i.e. the events $A_1,\ldots$ occur infinitely often with nonzero probability.

*Theorem 3:* Let T be $\varepsilon$-red for some real $\varepsilon > 0$. Then T contains an infinite branch that is red infinitely often.

*Proof* (Constructive Version): By Theorem 2 we can inductively form the following branch:

(i) Let $x_1 \in V_R$ be the first node in an enumeration of $V_R \cup V_W$ such that $T_{x_1}$ is $\varepsilon'$-red for some $\varepsilon' > 0$ and let $\beta_1$ be the branch from the root of T to $x_1$.

(ii) Assume we have constructed branch $\beta_n$. Then $T_{x_n}$ is $\varepsilon$-red for some $\varepsilon > 0$ and there is a first node $x_{n+1}$ in $V_R \cup V_W$ such that $T_{x_{n+1}}$ is $\varepsilon'$-red. Let $\gamma$ be the path from $x_n$ to $x_{n+1}$ and define $\beta_{n+1} = \beta_n\gamma$.

Clearly $\bigcup_{n=1}^{\infty} \beta_n$ is infinite and red infinitely often. □

*Proof* (Non-constructive Version): Let $\nu(A_i)$ be the probability of achieving a branch from the rest of T through $\ell_T(i)$ containing a red node x. Then by Lemperti's lemma there is, with non-zero probability, an infinite branch that is red infinitely often. □

As we promised, the constructive version of the theorem yields more information about the hard path than the non-constructive proof does. Observe that the construction used in the proof of Theorem 2 requires only finitely many evaluations of $f(x,\lambda)$ at known arguments and that determination of $f(x,\lambda)$ requires only Turing machine computations that ask oracle questions of the type $(\forall n)(\exists k)R(n,k,x)$ for some recursive R. Thus the procedure is recursive in 0". Conversely, every 0" computation is recursive in the $f(x,\lambda)$ construction. The following corollary states this precisely.

*Corollary:* The function defined by the constructive proof of Theorem 3 is in the Turing degree 0".

*Proof:* By the observation above, the construction defines a set in $\Sigma_3 \cap \Pi_3$ in the arithmetical hierarchy and thus the construction is recursive in 0" (see e.g. Theorem VIII, page 314 [7]). On the other hand, given a predicate of the form $(\forall n)(\exists k)R(n,k)$, we may form the red tree T, which has $\ell_T(n) \subseteq V_R$ if $(\exists k)R(n,k)$ and $\ell_T(m) \subseteq V_w$ for all $m \geq n$ if $\sim(\exists k)R(n,k)$. Therefore, the 0" computations are recursive in our construction. □

References

[1] K. L. Chung and P. Erdös.
On the applicability of the Borel-Cantelli lemma.
Transactions of the American Mathematical Society 72:179-186, 1952.

[2] V. Strassen.
Polynomials with rational coefficients which are hard to compute.
SIAM Journal of Computing 3:128-148, 1974.

[3] R. Lipton.
Polynomials with 0,1 coefficients that are hard to compute.
16th IEEE Symposium on Foundations of Computer Science, 6-10. 1975.

[4] P. Erdös and J. Spencer.
Probabalistic Methods in Combinatorics.
Academic Press, 1974.

[5] J. Lemperti.
Wiener's test and Markov chains.
J. Math. Anal. Appl. 6:58-66, 1963.

[6] A. N. Kolmogorov.
Three approaches to the quantitative definition of information.
Promlemy Pederachi Informatsii 1:3-11, 1965.

[7] H. Rogers.
Theory of Recursive Functions and Effective Computability.
McGraw-Hill, 1967.