Multiple Usage of Random Bits in Finite Automata

Rūsiņš Freivalds

Institute of Mathematics and Computer Science, University of Latvia,
Raiņa bulvāris 29, Rīga, Latvia*
Rusins.Freivalds@mii.lu.lv

Abstract. Finite automata with random bits written on a separate 2-way readable tape can recognize languages not recognizable by probabilistic finite automata. This shows that repeated reading of random bits by finite automata can have big advantages over one-time reading of random bits.

1 Introduction

What is a *probabilistic finite automaton*? The usual answer is *a deterministic finite automaton with an access to random bits.* However, much depends on precise terms how the random bits are allowed to use. The first models of the probabilistic finite automata have shown to be not the most powerful ones.

Michael O. Rabin [22] proved that probabilistic finite automata with one-way tape reading and isolated cut-point (bounded error) can recognize only regular languages, i.e. the same languages as deterministic finite automata can recognize. Freivalds [7] proved that two-way probabilistic finite automata with isolated cut-point can recognize some non-regular languages. This result showed that probabilistic automata differ from nondeterministic and alternating automata because for the language recognition capabilities of one-way and two-way automata are the same.

It was quite a surprise when it turned out that for some problems the communication complexity using public coins can be lower than the communication complexity using private coins [20]. Before that it was silently assumed that there is only one possibility how to use randomization in constructing efficient algorithms. Now it was shown that random bits may be a help in more than one way. This was even more surprising because the papers [1,11,12] showed that public and private coins had nearly the same power in interactive proof systems.

We discover in this paper another unusual property of randomization in finite automata in this paper. We show that finite automata that can read the random bits repeatedly have advantages over automata that can read these random bits only once.

* The research was supported by Project 2009/0216/1DP/1.1.1.2.0/09/IPIA/VIA/044 from the European Social Fund.

M. Agrawal, S.B. Cooper, and A. Li (Eds.): TAMC 2012, LNCS 7287, pp. 537–547, 2012.

What is a *random string of bits*? Are we to demand a correct result for arbitrary "random" string, including a string consisting only of zeros? We are to answer all these questions before we propose a formal definition.

In our case, the advice is supposed to be an arbitrary *infinite* Martin-Löf random sequence but the finite automaton can use only a finite initial fragment of this sequence. The length of the used fragment of the random sequence is up to the finite automaton. We demand that the result is to be correct with arbitrary Martin-Löf random sequence used. We demand also that no other restrictions on the randomness are used. Moreover, after Theorem 1 we notice that this our "naive" definition allows to simulate an additional counter, and it is well-known that automata with one counter can recognize nonregular languages. To avoid this additional possibility, we make our definition more complicated demanding that our sequence of random bits is infinite to both ends. It has no beginning and no end. One no more can simulate a counter but still our determnistic finite automaton with random bits written on a separate tape can recognize languages not recognizable by probabilistic finite automata.

Martin-Löf's original definition of a random sequence was in terms of constructive null covers; he defined a sequence to be random if it is not contained in any such cover. Leonid Levin and Claus-Peter Schnorr proved a characterization in terms of Kolmogorov complexity: a sequence is random if there is a uniform bound on the compressibility of its initial segments. An infinite sequence S is Martin-Löf random if and only if there is a constant c such that all of S's finite prefixes are c-incompressible. Schnorr gave a third equivalent definition in terms of martingales (a type of betting strategy). M.Li and P.Vitanyi's book [19] is an excellent introduction to these ideas.

However, the positive results in our paper use only one property of Martin-Löf random sequences. Namely, it is well known that for arbitrary Martin-Löf random sequence S and for arbitrary finite string w of zeros and ones it is true that S contains infinitely many occurencies of w.

Hence we introduce a notion of *primitive Martin-Löf random sequence* which suffices to prove all the positive results in our paper on usage of random binary strings.

Definition 1. *We say that an infinite sequence S of bits is a primitive Martin-Löf random sequence if for arbitrary finite binary string w, it is true that S contains infinitely many occurrences of the string w.*

It is obvious that arbitrary Martin-Löf random sequence is a primitive Martin-Löf random sequence.

This paper originated from re-considering the notion of "automata that take an advice". This notion was introduced by R.Karp/R.Lipton [15] for Turing machines, by T.Yamakami et al. [21,26,27] for finite automata and in a different way by R.Freivalds [10].

In this paper we notice that a meaningful advice which complies with the philosophy of the abovementioned papers can bring no information about the input word (where *information* is understood in terms used by Claude Shannon

[25]). This seems impossible but this is a simple corollary of the advantages of multiple usage of random bits versus single-time usage of them.

2 Preliminary Results

Deterministic, nondeterministic and alternating 2-way finite automata recognize only regular languages. On the other hand, it was proved in [7] (see also the survey [8]) that 2-way probabilistic finite automata (shortly: 2pfa) with bounded error can recognize nonregular languages.

C. Dwork and L. Stockmeyer proved in [4] a theorem on limitations of 2-way probabilistic finite automata with bounded error. This theorem is useful for us:

Theorem A. [4] *Let $L \subseteq \Sigma^*$. Suppose there is an infinite set I of positive integers and, for each $m \in I$, an integer $N(m)$ and sets $W_m = \{w_1, w_2, \cdots, w_{N(m)}\}$, $U_m = \{u_1, u_2, \cdots, u_{N(m)}\}$ and $V_m = \{v_1, v_2, \cdots, v_{N(m)}\}$ of words such that*

1. *$\mid w \mid \leq m$ for all $w \in W_m$,*
2. *for every integer k there is an m_k such that $N(m) \geq m^k$ for all $m \in I$ with $m \geq m_k$, and*
3. *for all $1 \leq i, j \leq N(m), u_j w_i v_j \in L$ iff $i = j$.*

Then L is not recognizable by 2-way probabilistic finite automata with bounded error.

We use this result to prove our Theorem 1. We have not yet defined our model of automaton but Theorem 1 already contains the essence of later constructions. The rest of this Section contains easy constructions showing why the model must be defined in a rather complicated way. We wish to show that multiple usage of random bits gives us advantages over single-time usage of them. However, the model is to be defined carefully to avoid many possible trivialities that can arise from allowing seemingly harmless simplifications of the model.

Theorem 1. *(1)The language $L = \{x2x \mid x \in \{0,1\}^*\}$ cannot be recognized with a bounded error by a probabilistic 2-way finite automaton.*
(2) The language $L = \{x2x \mid x \in \{0,1\}^*\}$ can be recognized by a deterministic non-writing 2-tape finite automaton one tape of which contains the input word, and the other tape contains a primitive Martin-Löf random sequence, the automaton is 2-way on every tape, and it stops producing a the correct result in a finite number of steps for arbitrary input word.

Proof. (1) Let m be an arbitrary integer. For arbitrary $i \in \{0, 1, 2, \cdots, 2^m - 1\}$ we define the word $x_i(m)$ as the word number i in the lexicographical ordering of all the binary words of the length m. We define the words u_i, w_i, v_i in our usage of Theorem A as $\{\emptyset, x_i(m), 2x_i(m)\}$.

(2) Let the input word be $x(r)2z(s)$ where r and s are the lengths of the corresponding words. At first, the 2-tape automaton finds a fragment $01111 \cdots$

which has the length at least r and uses it as a counter to test whether $r = s$. Then the automaton searches for another help-word. If the help-word turns out to be y then the automaton tests whether $x(r) = y$ and whether $z(s) = y$. $\square$

The definition used in the second item of Theorem 1 is our first (but not final) attempt to formalize the main idea of the notion of help from outside bringing zero information about the problem to be solved. Unfortunately, this definition allows something that was not intended to use. Such automata can easily simulate a counter, and 2-way automata with a counter, of course, can recognize nonregular languages. Hence we try to present a more complicated definition of help from outside bringing zero information to avoid the possibility to simulate a counter.

Definition 2. *A 2-infinite sequence of bits is a sequence* $\{a_i\}$ *where* $i \in (-\infty, \infty)$ *and all* $a_i \in \{0, 1\}$.

Definition 3. *We say that a 2-infinite sequence of bits is primitive Martin-Löf random if for arbitrary* $i \in (-\infty, \infty)$ *the sequence* $\{b_n\}$ *where* $b_n = a_{i+n}$ *for all* $i \in \mathbb{N}$ *is primitive Martin-Löf random, and the sequence* $\{c_n\}$ *where* $c_n = a_{i-n}$ *for all* $i \in \mathbb{N}$ *is primitive Martin-Löf random.*

Definition 4. *A deterministic* finite automaton with written random bits *(shortly: wrb) is a deterministic non-writing 2-tape finite automaton one tape of which contains the input word , and the other tape contains a 2-infinite primitive Martin-Löf random sequence, the automaton is 2-way on every tape, and it stops producing a the correct result in a finite number of steps for arbitrary input word. Additionally it is demanded that the head of the automaton never goes beyond the markers showing the beginning and the end of the input word.*

Nondeterministic, probabilistic, alternating, etc. automata with wrb differ from deterministic ones only in the nature of the automata but not in usage of tapes or Martin-Löf random sequences.

Definition 5. *We say that a language* L *is recognizable by a deterministic finite automaton* A *with wrb if* A *for arbitrary 2-infinite primitive Martin-Löf random sequence accepts every input word* $x \in L$ *and rejects every input word* $x \notin L$.

Definition 6. *We say that a language* L *is enumerable by a deterministic finite automaton* A *with wrb if* A *for arbitrary 2-infinite primitive Martin-Löf random sequence accepts every input word* $x \in L$ *and do not accept any input word* $x \notin L$.

Our Definition 4 contains an unexplained restriction forbidding the head on on the input tape to go beyond markers. This restriction was introduced because of undesired advantages of such machines considered in the following definition and subsequent Theorem 2.

Definition 7. *A deterministic finite automaton with wrb on unbounded input is a deterministic read-only 2-tape finite automaton one tape of which contains the input word , and the other tape contains a 2-infinite primitive Martin-Löf* *random sequence, the automaton is 2-way on every tape, and it stops producing a the correct result in a finite number of steps for arbitrary input word. It is not demanded that the head of the automaton always remains between the markers showing the beginning and the end of the input word.*

Recognition and enumeration of languages by deterministic finite automata with wrb is not particularly interesting because of the following two theorems.

Theorem 2. *A language L is enumerable by a deterministic finite automaton with wrb on unbounded input if and only if it is recursively enumerable.*

Proof. J.Bārzdiņš [2] proved that arbitrary one-tape deterministic Turing machine can be simulated by a 2-way finite deterministic automaton with 3 counters directly and by a 2-way finite deterministic automaton with 2 counters using a simple coding of the input word. (Later essentially the same result was rediscovered by other authors.) Hence there exists a a 2-way finite deterministic automaton with 3 counters accepting every word in L and only words in L.

Let x be an arbitrary word in L. To describe the processing of x by the 3-couter automaton we denote the content of the counter i ($i \in \{1, 2, 3\}$) at the moment t by $d(i, t)$. The word

$$00000101^{d(1,0)}0101^{d(2,0)}0101^{d(3,0)}000101^{d(1,1)}0101^{d(2,1)}0101^{d(3,1)}00\cdots$$

$$\cdots 00101^{d(1,s)}0101^{d(2,s)}0101^{d(3,s)}0000$$

where s is the halting moment, is a complete description of the processing of x by the automaton.

Our automaton with wrb tries to find a fragment of the 2-infinite primitive Martin-Löf random sequence on the help-tape such that:

1. it starts and ends by 0000,
2. the initial fragment
$$0101^{d(1,0)}0101^{d(2,0)}0101^{d(3,0)}00$$
is exactly 0000010010010, (i.e., the all 3 counters are empty,
3. for arbitrary t the fragment
$$0101^{d(1,t)}0101^{d(2,t)}0101^{d(3,t)}0101^{d(1,t+1)}0101^{d(2,t+1)}0101^{d(3,t+1)}$$
coresponds to a legal instruction of the automaton with the counters.

Since the 2-infinite sequence is primitive Martin-Löf random, such a fragment definitely exists in the sequence infinitely many times. The correctness of the fragment can be tested using the 3 auxiliary constructions below.

Construction 1. Assume that $w_k \in \{0, 1\}^*$ and $w_m \in \{0, 1\}^*$ are two subwords of the input word x such that:

1. they are immediately preceded and immediately followed by symbols other than $\{0, 1\}$,

2. a deterministic finite 1-tape 2-way automaton has no difficulty to move from w_k to w_m and back, clearly identifying these subwords,

Then there is a deterministic finite automaton with wrb recognizing whether or not $w_k = w_m$.

Proof. As in Theorem 1. □

Construction 2. Assume that 1^k and 1^m are two subwords of the help-word y such that:

1. they are immediately preceded and immediately followed by symbols other than $\{0, 1\}$,

2. a deterministic finite 1-tape 2-way automaton has no difficulty to move from w_k to w_m and back, clearly identifying these subwords,

3. both k and m are integers not exceeding the length of the input word.

Then there is a deterministic finite automaton with wrb recognizing whether or not $k = m$.

Proof. Similar the proof of Construction 1.

Construction 3. Assume that $1^{k_1}, 1^{k_2}, \cdots, 1^{k_s}$ and $1^{m_1}, 1^{m_2}, \cdots, 1^{m_t}$ are subwords of the help-word y such that:

1. they are immediately preceded and immediately followed by symbols other than 1,
2. a deterministic finite 1-tape 2-way automaton has no difficulty to move from one subword to another and back, clearly identifying these subwords,

3. both $k_1 + k_2 + \cdots + k_s$ and $m_1 + m_2 + \cdots + m_t$ are integers not exceeding the length of the input word.

Then there is a deterministic finite automaton with wrb recognizing whether or not $k_1 + k_2 + \cdots + k_s = m_1 + m_2 + \cdots + m_t$.

Proof. Similar the proof of Construction 2. □

Corollary of Theorem 2. *A language L is recognizable by a deterministic finite automaton with wrb on unbounded input if and only if it is recursive.*
Theorem 2 and its corollary show that the standard definition of the automaton with wrb should avoid the possibility to use the input tape outside the markers. However, even our standard definition allows recognition and enumeration of nontrivial languages. The proof of Theorem 1 can be easily modified to prove

Theorem 3. *1. The language $L = \{x2x \mid x \in \{0, 1\}^*\}$ cannot be recognized with a bounded error by a probabilistic 2-way finite automaton,*

2. *The language $L = \{x2x \mid x \in \{0,1\}^*\}$ can be recognized by a deterministic finite automaton with wrb.*

What happens if we allow to have two (or more) help-tapes containing 2-infinite primitive Martin-Löf sequences? We will see below that again this help turns out to be superfluous.

Definition 8. *A deterministic finite automaton with wrb with 2 help tapes is a deterministic non-writing 3-tape finite automaton one tape of which contains the input word , and each of the two other tapes contains a 2-infinite primitive Martin-Löf random sequence, the automaton is 2-way on every tape, and it stops producing a the correct result in a finite number of steps for arbitrary input word. It is not demanded that the head of the automaton always remains between the markers showing the beginning and the end of the input word.*

Theorem 4. *A language L is enumerable by a deterministic finite automaton with wrb with 2 help tapes if and only if it is recursively enumerable.*

Theorem 5. *A language L is recognizable by a deterministic finite automaton with wrb with 2 help tapes if and only if it is recursive.*

3 Main Results

Theorem 6. *The unary language PERFECT SQUARES $= \{1^n \mid (\exists m)(n = m^2)\}$ can be recognized by a deterministic finite automaton with wrb.*

Proof. It is well-known that

$$1 + 3 + 5 + \cdots + (2n-1) = n^2.$$

The deterministic automaton with wrb searches for a help-word (being a fragment of the given 2-infinite primitive Martin-Löf sequence) of a help-word

$$00101110111110 \cdots 01^{2n-1}00.$$

At first, the input word is used as a counter to test whether each substring of 1's is exactly 2 symbols longer than the preceding one. Then the help-word is used to test whether the length of the input word coincides with the number of 1's in the help-word. □

Theorem 7. *The unary language PERFECT CUBES $= \{1^n \mid (\exists m)(n = m^3)\}$ can be recognized by a deterministic finite automaton with wrb.*

Proof. In a similar manner the formula

$$1 + 3(n-1) + 3(n-1)^2 = n^3 - (n-1)^3$$

suggests a help-word

$$000[1]00[101110111]00[1011111101111111111]00 \cdots 00[101^{n-1}01^{(n-1)^2}]000$$

where symbols [,] are invisible. At first, the input word is used as a counter to test whether the help-word is correct but not whether its length is sufficient. Then the help-word is used to test whether the length of the input word coincides with the number of 1's in the help-word. □

Theorem 8. *The unary language PRIMES* $= \{1^n \mid n \textit{ is prime}\}$ *can be recognized by a deterministic finite automaton with wrb.*

We define a language UNARY 3-SAT as follows. The term $term_1 = x_k$ is coded as $[term_1]$ being 21^k, the term $term_2 = \neg x_k$ is coded as $[term_2]$ being 31^k, the subformula f being $(term_1 \vee term_2 \vee term_3)$ is coded as $[f]$ being $[term_1] \vee [term_2] \vee [term_3]$. The CNF being $f_1 \wedge f_2 \wedge \cdots \wedge f_m$ is coded as $[f_1] \wedge [f_2] \wedge \cdots \wedge [f_m]$.

Theorem 9. *Every* $L \in NP$ *is reducible by a deterministic log-space bounded Turing machine to a language* L' *such that* L' *is enumerable by a deterministic finite automaton with wrb.*

Proof. 3-SAT is NP-complete. Hence L is reducible by a deterministic *log*-space bounded Turing machine to 3-SAT. The language 3-SAT is reducible by a deterministic *log*-space bounded Turing machine to $unary3 - SAT$. The language UNARY 3-SAT is enumerable by a deterministic finite automaton B with wrb which can be constructed using Construction 1, Construction 2 and Construction 3. □

Theorem 10. *If a language* L *is enumerable by a nondeterministic finite automaton with wrb then* $L \in NP$.

Idea of the proof. R.Fagin's theorem [5] in descriptive complexity theory states that the set of all properties expressible in existential second-order logic is precisely the complexity class NP. N.Immerman 1999 gave a detailed proof of the theorem [13].

Our proof rather closely simulates Immerman's proof. Essentially, we use second-order existential quantifiers to choose existentially a help-word and a computation tableau. For every timestep, we arbitrarily choose the finite state control's state, the contents of every tape cell, and which nondeterministic choice we must make. Verifying that each timestep follows from each previous timestep can then be done with a first-order formula. □

The paper [10] contains the following

Theorem 11. *There exists a nonrecursive language* L *such that it can be nonconstructively recognized with nonconstructivity* $(\log n)^2$.

In constrast, we have a result showing that if the nonconstructive help is a primitive Martin-Löf sequence, then the language can be only recursive. Moreover, we have

Theorem 12. *If a language* L *is recognizable by a nondeterministic finite automaton with wrb then* $L \in NP \cap co - NP$.

Unfortunately, we have no strengthening of Theorems 10,12 for deterministic finite automata with wrb. Theorem 13 below shows that this open problem can be difficult.

Theorem 13. *Every language enumerable by a deterministic finite automaton with wrb is also recognizable by a nondeterministic finite automaton with wrb if and only if $P = NP$.*

Proof. Immediately from Theorem 12 and Lemma 1 below. □

Lemma 1. *If every language enumerable by a deterministic finite automaton with wrb is also recognizable by a nondeterministic finite automaton with wrb then $P = NP$.*

Proof. Let L be an arbitrary language in NP. Then by Theorem 9 L is reducible by a *log*-space DTM to a language $L' \in NP$ such that L' is enumerable by a deterministic finite automaton with wrb. The assumption of our theorem implies that L' recognizable by a nondeterministic finite automaton with wrb, and, consequently, also the complement of L' is recognizable by a nondeterministic finite automaton with wrb. By Theorem 12 it follows that $L' \in co-NP$, and by Theorem 9 it follows that $L \in co-NP$. □

Theorem 14. *If a language L is enumerable by a nondeterministic finite automaton with wrb then L is also enumerable by a deterministic finite automaton with wrb.*

Proof. The deterministic automaton with wrb searches for a help-word (being a fragment of the given 2-infinite primitive Martin-Löf sequence) of a special kind described below.

Let $x \in L$ be an input word , a help-word w (we denote the length of w by h) and let an computation path P by the nondeterministic automaton on (x, w) be fixed such that the head on w never leaves w. At first, we describe a word y containing enough information about the nondeterministic choices and later we use this word y to construct a deterministic finite automaton with wrb to accept the word (x, z) with an appropriate z. Let w be a unary word $w_1 w_2 w_3 \cdots w_m$. Then

$$y = w_1 2 c_{(1,1)} c_{(2,1)} \cdots c_{(h,1)} 2 w_2 2 c_{(1,2)} c_{(2,2)} \cdots c_{(h,2)} 2 w_3 \cdots 2 w_m 2 c_{(1,m)} \cdots c_{(h,m)}$$

where $c_{(i,j)}$ denotes:

- $\oslash$, if at the computation path P there is no occurrence when the head on the help-tape is on the symbol w_j and the head on the input tape at this moment is on the i-th symbol of x;

- code of triple (p, s, i), if at the computation path P there is an occurrence when the head on the help-tape is on the symbol w_j and the head on the input tape at this moment is on the i-th symbol of x, and at this moment the state of the automaton is p , the instruction s is performed on the computation path P, and the number i in a unary notation. (Please notice that p and s are elements of finite sets with a cardinality bounded by a constant depending only on the program of the nondeterministic automaton.)

Let z be an expression of y in binary notation by a symbol-to-symbol translation of the word y. The needed deterministic automaton working on arbitrary 2-infinite primitive Martin-Löf sequence searches for a fragment z of the given 2-infinite sequence. This search involves a huge amount of comparisons (1) whether or not the tested help-word is compatible with the instructions of the nondeterministic finite automaton with wrb and (2) whether the tested help-word is compatible with the computation path of the nondeterministic finite automaton with wrb. For instance, let at some moment it appears that the current instruction of the nondeterministic automaton (contained in $c_{(i,j)}$)prescribes moving the head on the help-tape one position to the right with the head on the input tape staying at the same position. Then the head of the deterministic automaton with wrb leaves its position and for a time being the input tape is used only as a counter. The moves to the leftmost position and then the counter is used to move the help-tape head to the position of $c_{(i,j+1)}$ simultaneously comparing whether $c_{(i,j+1)}$ contains an instruction compatible with the instruction performed at the previous step. If at some moment it turns out that the help word is not correct (i.e. it does not correspond either to the instructions of the nondeterministic automaton, or it does not correspond to a legal path of computation), the deterministic automaton searches for a new help-word. Since the help tape contains a 2-infinite primitive Martin-Löf random sequence, if there is an accepting path of the nondeterministic automaton there is also an accepting path of the deterministic automaton. □

Corollary of Theorem 14. If a language L is recognizable by a nondeterministic finite automaton with wrb then L is also recognizable by a deterministic finite automaton with wrb.

References

1. Babai, L., Moran, S.: Arthur-Merlin games: a randomized proof system, and a hierarchy of complexity classes. Journal of Computer and System Sciences 36(2), 254–276 (1988)
2. Barzdin, J.M.: On a Class of Turing Machines (Minsky Machines). Algebra i Logika 3(1) (1963) (Russian); Review in the Journal of Symbolic Logic 32(4), 523–524 (1967)
3. Calude, C.S., Staiger, L.: Generalisations of disjunctive sequences. Mathematical Logic Quarterly 51(2), 120–128 (2005)
4. Dwork, C., Stockmeyer, L.: Finite state verifiers I: the power of interaction. Journal of the Association for Computing Machinery 39(4), 800–828 (1992)
5. Fagin, R.: Generalized first-order spectra and polynomial-time recognizable sets. In: Karp, R. (ed.) SIAM-AMS Proceedings of the Complexity of Computation, vol. 7, pp. 27–41 (1974)

6. Freivalds, R.: Probabilistic machines can use less running time. In: Gilchrist, B. (ed.) Information Processing 1977, Proceedings of IFIP Congress 1977, pp. 839–842. North-Holland, Amsterdam (1977)
7. Freivalds, R.: Probabilistic Two-way Machines. In: Gruska, J., Chytil, M.P. (eds.) MFCS 1981. LNCS, vol. 118, pp. 33–45. Springer, Heidelberg (1981)
8. Freivalds, R.: Complexity of Probabilistic Versus Deterministic Automata. In: Barzdins, J., Bjorner, D. (eds.) Baltic Computer Science. LNCS, vol. 502, pp. 565–613. Springer, Heidelberg (1991)
9. Freivalds, R.: Non-constructive methods for finite probabilistic automata. International Journal of Foundations of Computer Science 19(3), 565–580 (2008)
10. Freivalds, R.: Amount of nonconstructivity in finite automata. Theoretical Computer Science 411(38-39), 3436–3443 (2010)
11. Goldwasser, S., Micali, S., Rackoff, C.: The Knowledge complexity of interactive proof-systems. In: Proceedings of ACM STOC 1985, pp. 291–304 (1985)
12. Goldwasser, S., Sipser, M.: Private coins versus public coins in interactive proof systems. In: Proceedings of ACM STOC 1986, pp. 58–68 (1986)
13. Immerman, N.: Descriptive Complexity, pp. 113–119. Springer, New York (1999)
14. Jürgensen, H., Thierrin, G.: On ω-Languages whose syntactic monoid is trivial. International Journal of Parallel Programming 12(5), 359–365 (1983)
15. Karp, R.M., Lipton, R.: Turing machines that take advice. L' Enseignement Mathematique 28, 191–209 (1982)
16. Kolmogorov, A.N.: Three approaches to the quantitative definition of information. Problems in Information Transmission 1, 1–7 (1965)
17. Levin, L.A.: On the notion of a random sequence. Soviet Mathematics Doklady 14, 1413–1416 (1973)
18. Martin-Löf, P.: The definition of random sequences. Information and Control 9(6), 602–619 (1966)
19. Li, M., Vitányi, P.M.B.: An Introduction to Kolmogorov Complexity and its Applications, 2nd edn. Springer (1997)
20. Newman, I.: Private vs. common random bits in communication complexity. Information Processing Letters 39, 67–71 (1991)
21. Nishimura, H., Yamakami, T.: Polynomial time quantum computation with advice. Information Processing Letters 90(4), 195–204 (2004)
22. Rabin, M.O.: Probabilistic automata. Information and Control 6, 230–245 (1963)
23. Schnorr, C.-P.: A unified approach to the definition of random sequences. Mathematical Systems Theory 5(3), 246–258 (1971)
24. Schnorr, C.-P.: Process complexity and effective random tests. Journal of Computer and System Sciences 7(4), 376–388 (1973)
25. Shannon, C.: Communication theory of secrecy systems. Bell System Technical Journal 28(4), 656–715 (1949)
26. Tadaki, K., Yamakami, T., Lin, J.C.H.: Theory of one-tape linear-time Turing machines. Theoretical Computer Science 411(1), 22–43 (2010)
27. Yamakami, T.: The Roles of Advice to One-Tape Linear-time Turing machines and finite automata. International Journal of Foundations of Computer Science 21(6), 941–962 (2010)