Ker-I Ko and the Study of Resource-Bounded Kolmogorov Complexity*

Eric Allender[0000−0002−0650−028X]

Rutgers University, New Brunswick NJ 08854, USA
allender@cs.rutgers.edu
http://www.cs.rutgers.edu/∼allender

Abstract. Ker-I Ko was among the first people to recognize the importance of resource-bounded Kolmogorov complexity as a tool for better understanding the structure of complexity classes. In this brief informal reminiscence, I review the milieu of the early 1980's that caused an up-welling of interest in resource-bounded Kolmogorov complexity, and then I discuss some more recent work that sheds additional light on the questions related to Kolmogorov complexity that Ko grappled with in the 1980's and 1990's.
In particular, I include a detailed discussion of Ko's work on the question of whether it is NP-hard to determine the time-bounded Kolmogorov complexity of a given string. This problem is closely connected with the Minimum Circuit Size Problem (MCSP), which is central to several contemporary investigations in computational complexity theory.

Keywords: Kolmogorov Complexity · Complexity Theory · Minimum Circuit Size Problem

1 Introduction: A Brief History of Time-Bounded Kolmogorov Complexity

In the beginning, there was Kolmogorov complexity, which provided a satisfying and mathematically precise definition of what it means for something to be "random", and gave a useful measure of the amount of information contained in a bitstring.[1] But the fact that the Kolmogorov complexity function is not computable does limit its application in several areas, and this provided some of the original motivation for the study of resource-bounded Kolmogorov complexity.

A version of time-bounded Kolmogorov complexity appears already in Kolmogorov's original 1965 paper [41]. However, for the purposes of the story being told here, the first significant development came with the work of Kolmogorov's doctoral student Leonid Levin.[2] Levin's fundamental work on NP-completeness

* Supported in part by NSF Grants CCF-1514164 and CCF-1909216.

[1] If the reader is not familiar with Kolmogorov complexity, then we recommend some excellent books on this topic [44, 25].

[2] Levin was Kolmogorov's student, but he did not receive his Ph.D. until after he emigrated to the US, and Albert Meyer was his advisor at MIT. The circumstances

[42] has, as its second theorem, a result that can easily be proved[3] by making use of a notion of time-bounded Kolmogorov complexity called Kt, which Levin developed in the early 1970's, but whose formal definition did not appear in a published article until 1984 [43]. Adleman acknowledges communication with Levin in a 1979 MIT technical report [1] that discusses a very similar notion, which he called "potential".[4] Since Kt will be discussed at greater length later on, let us give the definition here:

Definition 1. *For any Turing machine M and strings x and y, $\mathsf{Kt}_M(x|y)$ is the minimum, over all "descriptions" d such that $M(d, y) = x$ in t steps, of the sum $|d| + \log t$. (If no such d exists, then $\mathsf{Kt}_M(x|y)$ is undefined.) $\mathsf{Kt}_M(x)$ is defined to be $\mathsf{Kt}_M(x|\lambda)$, where λ is the empty string.*

If M is chosen to be a universal Turing machine, then $\mathsf{Kt}_M(x|y)$ is always defined. As is usual when discussing Kolmogorov complexity we select one such universal machine U, and define $\mathsf{Kt}(x|y)$ to be equal to $\mathsf{Kt}_U(x|y)$. Kt has the appealing property that it can be used to design optimal search algorithms for finding witnesses for problems in NP. For instance, $\mathsf{P} = \mathsf{NP}$ iff every $\phi \in \mathsf{SAT}$ has some assignment v such that $\mathsf{Kt}(v|\phi) = O(\log |\phi|)$ [42, 1]. See [44] for a discussion.

Li and Vitányi [44], in their discussion of the origins of time-bounded Kolmogorov complexity, highlight not only the work of Adleman and Levin discussed above, but also a 1977 paper by Daley [24], where time-bounded Kolmogorov complexity is studied in the context of inductive inference. Indeed, in Ko's first paper that deals with K-complexity [37], Daley's work [24] is one of the four papers that Ko mentions as containing prior work on resource-bounded Kolmogorov complexity. (The others are [42], and the papers of Hartmanis and of Sipser that are discussed below.) But I think that this is only part of the story.

Adleman's work [1] remains even today an unpublished MIT technical report, which did not circulate widely. Levin's work [42] was still not particularly well-known in the early 1980's, and the published paper contains very little detail. Daley's work [24] was part of the inductive inference research community, which

around Levin being denied his Ph.D. in Moscow are described in the excellent article by Trakhtenbrot [59].

[3] This result also appears as Exercise 13.20 in what was probably the most popular complexity theory textbook for the early 1980's [33], which credits Levin for that result, but *not* for what is now called the Cook-Levin theorem.

[4] In [1], in addition to Levin, Adleman also credits Meyer and McCreight [46] with developing similar ideas. I have been unable to detect any close similarity, although the final paragraph of [46] states "Our results are closely related to more general definitions of randomness proposed by Kolmogorov, Martin-Löf, and Chaitin" [and here the relevant literature is cited, before continuing] "A detailed discussion must be postponed because of space limitations" [and here Meyer and McCreight *include a citation to a letter from the vice-president of Academic Press* (which presumably communicated the space limitations to the authors).] Indeed, Meyer and McCreight were interested in when a decidable (and therefore very non-random) set can be said to "look random" and thereby deserve to be called pseudorandom. We will return to this topic later in the paper.

was then and remains today rather distinct from the complexity theory community. Thus I would also emphasize the impact that the 1980 STOC paper by Paul, Seiferas, and Simon [52] had, in bringing the tools and techniques of Kolmogorov complexity to the STOC/FOCS community in the context of proving lower bounds. At the following FOCS conference, Gary Peterson introduced a notion of resource-bounded Kolmogorov complexity [54]. Peterson's article has a very interesting and readable introduction, highlighting the many ways in which different notions of succinctness had arisen in various other work on complexity theory. Peterson's FOCS'80 paper also introduces a theme that echoes in more recent work, showing how various open problems in complexity theory can be restated in terms of the relationships among different notions of resource-bounded Kolmogorov complexity. However, the precise model of resource-bounded Kolmogorov complexity that is introduced in [54] is rather abstruse, and it seems that there has been no further work using that model in the following four decades.

Perhaps it was in part due to those very deficiencies, that researchers were inspired to find a better approach. At the 1983 STOC, Sipser introduced a notion of polynomial-time "distinguishing" Kolmogorov complexity, in the same paper in which he showed that BPP lies in the polynomial hierarchy [58]. At FOCS that same year, Hartmanis introduced what he termed "Generalized Kolmogorov Complexity", in part as a tool to investigate the question of whether all NP-complete sets are isomorphic. Both Sipser and Hartmanis cited Ko's work, which would eventually appear as [37], as presenting yet another approach to studying resource-bounded Kolmogorov complexity.

Ko's motivation for developing a different approach to resource-bounded Kolmogorov complexity arose primarily because of the groundbreaking work of Yao [62] and Blum and Micali [18], which gave a new approach to the study of pseudorandom generators. Ko sought to find a relationship between the new notion of pseudorandomness and the classical notions of Martin-Löf randomness for *infinite sequences*. Other notions of "pseudorandomness" had been proposed by Meyer and McCreight [46] and by Wilbur [61], and Ko succeeded in finding the relationships among these notions, and in presenting new definitions that provided a complexity-theoretic analog of Martin-Löf randomness. (This analog is more successful in the context of space-bounded Kolmogorov complexity, than for time.)

One of the people who had a significant impact on the development on resource-bounded Kolmogorov complexity at this time was Ron Book. Book took an active interest in mentoring young complexity theoreticians, and he organized some informal workshops in Santa Barbara in the mid-to-late 1980's. That was where I first met Ker-I Ko. Some of the others who participated were José Balcázar, Richard Beigel, Lane Hemaspaandra, Jack Lutz, Uwe Schöning, Jacobo Torán, Jie Wang, and Osamu Watanabe. Resource-bounded Kolmogorov complexity was a frequent topic of discussion at these gatherings. Four members of that group (Ko, Orponen, Schöning, and Watanabe) incorporated time-bounded Kolmogorov complexity into their work investigating the question of

what it means for certain instances of a computational problem to be hard, whereas other instances can be easy [40]; I first learned about this work at Book's 1986 Santa Barbara workshop, shortly before the paper was presented at the first Structure in Complexity Theory conference (which was the forerunner to the Computational Complexity Conference (CCC)). A partial list of other work on resource-bounded Kolmogorov complexity whose origin can be traced in one way or another to Book's series of workshops includes [2, 13, 16, 20, 26, 28], as well as the volume edited by Osamu Watanabe [60].

Research in resource-bounded Kolmogorov complexity has continued at a brisk pace in the succeeding years. This article will not attempt to survey – or even briefly mention – all of this work. Instead, our goal in this section is to sketch the developments that influenced Ker-I Ko's work on resource-bounded Kolmogorov complexity. Ko's research focus shifted toward other topics after the early 1990's, and thus later work such as [5, 15, 22, 23] does not pertain to this discussion.

But there is one more paper that Ko wrote that deals with resource-bounded Kolmogorov complexity [38], which constitutes an important milestone in a line of research that is very much an active research topic today. In the next section, we place Ko's 1990 COLT paper [38] in context, and discuss how it connects to the current frontier in computational complexity theory.

2 Time-Bounded Kolmogorov Complexity and NP-Completeness

Ko was not the first to see that there is a strong connection between resource-bounded Kolmogorov complexity and one of the central tasks of computational learning theory: namely, to find a succinct explanation that correctly describes observed phenomena. But he does appear to have been the first to obtain theorems that explain the obstacles that have thus far prevented a classification of the complexity of this problem, where "succinct explanation" is interpreted operationally in terms of an efficient algorithm with a short description. There had been earlier work [55, 56] showing that it is NP-hard to find "succinct explanations" that have size at all close to the optimal size, if these "explanations" are required to be finite automata or various other restricted formalisms. But for general formalisms such as programs or circuits, this remains an open problem.[5]

Ko approached this problem by defining a complexity measure called LT for partially-specified Boolean functions (which now are more commonly referred to as "promise problems"). Given a list of "yes instances" Y and a list of "no instances" N, $\mathsf{LT}(Y, N, t)$ is the length of the shortest description d such that $U(d, x) = 1$ in at most t steps for all $x \in Y$, and $U(d, x) = 0$ in at most t steps for all $x \in N$, where U is some fixed universal Turing machine (in the tradition

[5] During the review and revision phase of preparing this paper, I was given a paper that settles this question! Ilango, Loff, and Oliveira have now shown that the "circuit" version of this problem (which they call Partial-MCSP) is NP-complete [35]. For additional discussion of this result and how it contrasts with Ko's work [38], see [4].

of Kolmogorov complexity). Given any oracle A, one can define a relativized measure LT^A, merely by giving the machine U access to A; for any A, the set $\mathsf{MinLT}^A ::= \{(Y, N, 0^s, 0^t) : \mathsf{LT}^A(Y, N, t) \leq s\}$ is in NP^A. Ko showed that there are oracles A relative to which MinLT^A is not NP^A-complete under polynomial-time Turing reductions. In other words, the question of whether this version of the canonical learning theory problem is NP-complete cannot be answered via relativizing techniques.

Ko proves his results about MinLT by first proving the analogous results about a problem he calls $\mathsf{MinKT} ::= \{(x, 0^s, 0^t) : \exists d\ |d| \leq s \wedge U(d) = x$ in at most t steps$\}$. Note that MinKT is essentially MinLT restricted to the case where $Y \cup N$ is equal to the set of all strings of length n (in which case this information can be represented by a string x of length 2^n). Quoting from [39]: "Indeed, there seems to be a simple transformation of the proofs of the results about MinKT to the proofs of analogous results about MinLT. This observation supports our viewpoint of treating the problem MinKT as a simpler version of MinLT, and suggests an interesting link between program-size complexity and learning in the polynomial-time setting." One can see that Ko had been working for quite some time on the question of whether it is NP-hard to determine the time-bounded Kolmogorov complexity of a given string (i.e, the question of whether MinKT is NP-complete), because this question also appears in [37], where it is credited to some 1985 personal communication from Hartmanis.

Ko's question about the difficulty of computing time-bounded Kolmogorov complexity was also considered by Levin in the early 1970's, as related by Trakhtenbrot[6] [59]; see also the discussion in [12]. More precisely, Levin was especially interested in what is now called the Minimum Circuit Size Problem $\mathsf{MCSP} ::= \{(x, s) | x$ is a string of length 2^k representing the truth-table of a k-ary Boolean function that is computed by a circuit of size at most $s\}$. A small circuit for a Boolean function f can be viewed as a short description of f, and thus it was recognized that MCSP was similar in spirit to questions about time-bounded Kolmogorov complexity, although there are no theorems dating to this period that make the connection explicit. Trakhtenbrot [59] describes how MCSP had been the focus of much attention in the Soviet Union as early as the late 1950's; Levin had hoped to include a theorem about the complexity of MCSP (or of time-bounded Kolmogorov complexity) in [42], but these questions remain unresolved even today.

The modern study of the computational complexity of MCSP can really be said to have started with the STOC 2000 paper by Kabanets and Cai [36]. They were the first to show that MCSP must be intractable if cryptographically-secure one-way functions are to exist, and they were the first to initiate an investigation of the consequences that would follow if MCSP were NP-complete under various types of reducibilities.

A tighter connection between MCSP and resource-bounded Kolmogorov complexity was established in [6]. Prior to [6] most studies of time-bounded Kolmogorov complexity either concentrated on Levin's measure Kt, or else on a

[6] In particular, this is the problem that Trakhtenbrot calls "Task 5" in [59].

measure (similar to what Ko studied) that we can denote K^t for some time bound t (typically where $t(n) = n^{O(1)}$), where $K^t(x)$ is the length of the shortest d such that $U(d) = x$ in at most $t(|x|)$ steps. Although both of these definitions are very useful in various contexts, there are some drawbacks to each. Computing $\mathsf{Kt}(x)$ does not seem to lie in NP (and in fact it is shown in [6] that computing Kt is complete for EXP under $\mathsf{P/poly}$ reductions). The value of $K^t(x)$ can vary quite a lot, depending on the choice of universal Turing machine U; the usual way of coping with this is to observe that $K^t(x)$, as defined using some machine U_1 is bounded above by $K^{t'}(x)$ as defined using a different machine U_2, for some time bound t' that is not too much larger than t. Both definitions yield measures that have no clear connection to circuit complexity.

The solution presented in [6] is to modify Levin's Kt measure, to obtain a new measure called KT, as follows. First, note that Levin's Kt measure remains essentially unchanged if Definition 1 is replaced by

Definition 2. *Let $x = x_1x_2\ldots x_n$ be a string of length n. $\mathsf{Kt}(x)$ is the minimum, over all "descriptions" d such that $U(d,i) = x_i$ in t steps, of the sum $|d| + \log t$.*

In other words, the description d still describes the string x, but the way that U obtains x from d is to compute $U(d,i)$ for each $i \in \{1,\ldots n\}$. The main thing that is gained from this modification, is that now the runtime of U can be much less than $|x|$. This gives us the flexibility to replace "$\log t$" in the definition of Kt, with "t", to obtain the definition of KT:

Definition 3. *Let $x = x_1x_2\ldots x_n$ be a string of length n. $\mathsf{KT}(x)$ is the minimum, over all "descriptions" d such that $U(d,i) = x_i$ in t steps, of the sum $|d| + t$. (A more formal and complete definition can be found in [6].)*

When x is a bit string of length 2^k representing a k-ary Boolean function f, the circuit size of f is polynomially-related to $\mathsf{KT}(x)$ [6]. Thus it has been productive to study MCSP (the problem of computing the circuit size function) in tandem with MKTP (the problem of computing the KT function) [6, 7, 9–11, 31, 45, 49, 57]. This has led to improved hardness results for MCSP (and MKTP) [6, 7, 9, 31, 57] and some non-hardness results [9–11]. (The non-hardness results of [47] for MCSP apply equally well to MKTP, and should also be listed here.) We now know that MCSP and MKTP are hard for a complexity class known as SZK under BPP-Turing reductions [7], and they cannot be shown to be NP-complete under polynomial-time many-one reductions without first proving that $\mathsf{EXP} \neq \mathsf{ZPP}$ [47]. These hardness results also hold for Ko's languages MinKT and MinLT.

Somewhat surprisingly, some hardness proofs currently work only for MKTP and the corresponding hardness conditions for MCSP are either not known to hold [8, 9] or seem to require different techniques [27].

Some researchers have begun to suspect that MCSP may be hard for NP under sufficiently powerful notions of reducibility, such as $\mathsf{P/poly}$ reductions. Interestingly, Ko explicitly considered the possibility that MinKT is NP-complete under a powerful notion of reducibility known as SNP reducibility. (Informally, "A is SNP reducible to B" means that A is $(\mathsf{NP} \cap \mathsf{coNP})$-reducible to B.) More

recently, Hitchcock and Pavan have shown that this indeed holds under a plausible hypothesis [32]. Interestingly, Ilango has shown that a variant of MCSP is NP-complete under (very restrictive) AC^0 reductions [34]. Hirahara has shown that, if a certain version of time-bounded Kolmogorov complexity is NP-hard to compute, then this implies strong worst-case-to-average-case reductions in NP [30].

One especially intriguing recent development involves what has been termed "hardness magnification". This refers to the phenomenon wherein a seemingly very modest and achievable lower bound can be "magnified" to yield truly dramatic lower bounds which would solve longstanding open questions about the relationships among complexity classes. The problems MCSP, MKTP, and even MKtP (the problem of computing Kt complexity) figure prominently in this line of work [50, 49, 45]. In particular, it is shown in [49] that if one were able to show a certain lower bound for MKtP that is *known* to hold for the apparently much easier problem of computing the inner product mod 2, then it would follow that $\mathsf{EXP} \not\subseteq \mathsf{NC}^1$.

3 Conclusions

Ker-I Ko has left us. But he has left us a rich legacy. This brief article has touched on only a small part of his scientific accomplishments, and how they continue to affect the scientific landscape. Even within the very limited focus of this paper, much has been left out. For instance, the connection between resource-bounded Kolmogorov complexity and learning theory could itself be the subject of a much longer article; as a sample of more recent work in this line, let us mention [48].

References

1. Adleman, L.M.: Time, space and randomness. Tech. Rep. MIT/LCS/TM-131, MIT (1979)
2. Allender, E.: Some consequences of the existence of pseudorandom generators. In: Proceedings of the 19th Annual ACM Symposium on Theory of Computing (STOC). pp. 151–159 (1987). https://doi.org/10.1145/28395.28412, see also [3].
3. Allender, E.: Some consequences of the existence of pseudorandom generators. J. Comput. Syst. Sci. **39**(1), 101–124 (1989). https://doi.org/10.1016/0022-0000(89)90021-4
4. Allender, E.: The new complexity landscape around circuit minimization. In: Proc. 14th International Conference on Language and Automata Theory and Applications (LATA) (2020), to appear
5. Allender, E., Buhrman, H., Friedman, L., Loff, B.: Reductions to the set of random strings: The resource-bounded case. Logical Methods in Computer Science **10**(3) (2014). https://doi.org/10.2168/LMCS-10(3:5)2014
6. Allender, E., Buhrman, H., Koucký, M., van Melkebeek, D., Ronneburger, D.: Power from random strings. SIAM Journal on Computing **35**, 1467–1493 (2006). https://doi.org/10.1137/050628994

7. Allender, E., Das, B.: Zero knowledge and circuit minimization. Information and Computation **256**, 2–8 (2017). https://doi.org/10.1016/j.ic.2017.04.004, special issue for MFCS '14
8. Allender, E., Grochow, J., van Melkebeek, D., Morgan, A., Moore, C.: Minimum circuit size, graph isomorphism and related problems. SIAM Journal on Computing **47**, 1339–1372 (2018). https://doi.org/10.1137/17M1157970
9. Allender, E., Hirahara, S.: New insights on the (non)-hardness of circuit minimization and related problems. ACM Transactions on Computation Theory (ToCT) **11**(4), 27:1–27:27 (2019). https://doi.org/10.1145/3349616
10. Allender, E., Holden, D., Kabanets, V.: The minimum oracle circuit size problem. Computational Complexity **26**(2), 469–496 (2017). https://doi.org/10.1007/s00037-016-0124-0
11. Allender, E., Ilango, R., Vafa, N.: The non-hardness of approximating circuit size. In: Computer Science - Theory and Applications - 14th International Computer Science Symposium in Russia (CSR). Lecture Notes in Computer Science, vol. 11532, pp. 13–24. Springer (2019). https://doi.org/10.1007/978-3-030-19955-5_2
12. Allender, E., Koucký, M., Ronneburger, D., Roy, S.: The pervasive reach of resource-bounded Kolmogorov complexity in computational complexity theory. J. Comput. Syst. Sci. **77**, 14–40 (2010). https://doi.org/10.1016/j.jcss.2010.06.004
13. Allender, E., Watanabe, O.: Kolmogorov complexity and degrees of tally sets. In: Proceedings: Third Annual Structure in Complexity Theory Conference. pp. 102–111. IEEE Computer Society (1988). https://doi.org/10.1109/SCT.1988.5269, see also [14]
14. Allender, E., Watanabe, O.: Kolmogorov complexity and degrees of tally sets. Inf. Comput. **86**(2), 160–178 (1990). https://doi.org/10.1016/0890-5401(90)90052-J
15. Antunes, L., Fortnow, L., van Melkebeek, D., Vinodchandran, N.V.: Computational depth: Concept and applications. Theor. Comput. Sci. **354**(3), 391–404 (2006). https://doi.org/10.1016/j.tcs.2005.11.033
16. Arvind, V., Han, Y., Hemachandra, L.A., Köbler, J., Lozano, A., Mundhenk, M., Ogiwara, M., Schöning, U., Silvestri, R., Thierauf, T.: Reductions to sets of low information content. In: Automata, Languages and Programming, 19th International Colloquium (ICALP). Lecture Notes in Computer Science, vol. 623, pp. 162–173. Springer (1992). https://doi.org/10.1007/3-540-55719-9_72, see also [17].
17. Arvind, V., Han, Y., Hemachandra, L.A., Köbler, J., Lozano, A., Mundhenk, M., Ogiwara, M., Schöning, U., Silvestri, R., Thierauf, T.: Reductions to sets of low information content. In: Ambos-Spies, K., Homer, S., Schöning, U. (eds.) Complexity Theory: Current Research, pp. 1–46. Cambridge University Press (1993)
18. Blum, M., Micali, S.: How to generate cryptographically strong sequences of pseudo random bits. In: 23rd Annual Symposium on Foundations of Computer Science (FOCS). pp. 112–117 (1982). https://doi.org/10.1109/SFCS.1982.72, see also [19]
19. Blum, M., Micali, S.: How to generate cryptographically strong sequences of pseudo-random bits. SIAM J. Comput. **13**(4), 850–864 (1984). https://doi.org/10.1137/0213053
20. Book, R.V., Lutz, J.H.: On languages with very high information content. In: Proceedings of the Seventh Annual Structure in Complexity Theory Conference. pp. 255–259. IEEE Computer Society (1992). https://doi.org/10.1109/SCT.1992.215400, see also [21].
21. Book, R.V., Lutz, J.H.: On languages with very high space-bounded Kolmogorov complexity. SIAM J. Comput. **22**(2), 395–402 (1993). https://doi.org/10.1137/0222029

22. Buhrman, H., Fortnow, L., Laplante, S.: Resource-bounded Kolmogorov complexity revisited. SIAM J. Comput. **31**(3), 887–905 (2001). https://doi.org/10.1137/S009753979834388X
23. Buhrman, H., Mayordomo, E.: An excursion to the Kolmogorov random strings. J. Comput. Syst. Sci. **54**, 393–399 (1997). https://doi.org/10.1006/jcss.1997.1484
24. Daley, R.: On the inference of optimal descriptions. Theoretical Computer Science **4**(3), 301–319 (1977). https://doi.org/10.1016/0304-3975(77)90015-9
25. Downey, R., Hirschfeldt, D.: Algorithmic Randomness and Complexity. Springer (2010)
26. Gavaldà, R., Torenvliet, L., Watanabe, O., Balcázar, J.L.: Generalized Kolmogorov complexity in relativized separations (extended abstract). In: Mathematical Foundations of Computer Science, (MFCS). Lecture Notes in Computer Science, vol. 452, pp. 269–276. Springer (1990). https://doi.org/10.1007/BFb0029618
27. Golovnev, A., Ilango, R., Impagliazzo, R., Kabanets, V., Kolokolova, A., Tal, A.: AC^0[p] lower bounds against MCSP via the coin problem. In: 46th International Colloquium on Automata, Languages, and Programming,(ICALP). LIPIcs, vol. 132, pp. 66:1–66:15. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik (2019). https://doi.org/10.4230/LIPIcs.ICALP.2019.66
28. Hemachandra, L.A., Wechsung, G.: Using randomness to characterize the complexity of computation. In: Information Processing 89, Proceedings of the IFIP 11th World Computer Congress. pp. 281–286. North-Holland/IFIP (1989), see also [29].
29. Hemachandra, L.A., Wechsung, G.: Kolmogorov characterizations of complexity classes. Theor. Comput. Sci. **83**(2), 313–322 (1991). https://doi.org/10.1016/0304-3975(91)90282-7
30. Hirahara, S.: Non-black-box worst-case to average-case reductions within NP. In: 59th IEEE Annual Symposium on Foundations of Computer Science (FOCS). pp. 247–258 (2018). https://doi.org/10.1109/FOCS.2018.00032
31. Hirahara, S., Santhanam, R.: On the average-case complexity of MCSP and its variants. In: 32nd Conference on Computational Complexity, CCC. LIPIcs, vol. 79, pp. 7:1–7:20. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik (2017). https://doi.org/10.4230/LIPIcs.CCC.2017.7
32. Hitchcock, J.M., Pavan, A.: On the NP-completeness of the minimum circuit size problem. In: Conference on Foundations of Software Technology and Theoretical Computer Science (FST&TCS). LIPIcs, vol. 45, pp. 236–245. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik (2015). https://doi.org/10.4230/LIPIcs.FSTTCS.2015.236
33. Hopcroft, J.E., Ullman, J.D.: Introduction to Automata Theory, Languages and Computation. Addison-Wesley (1979)
34. Ilango, R.: Approaching MCSP from above and below: Hardness for a conditional variant and $AC^0[p]$. In: 11th Innovations in Theoretical Computer Science Conference, ITCS. LIPIcs, vol. 151, pp. 34:1–34:26. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik (2020). https://doi.org/10.4230/LIPIcs.ITCS.2020.34
35. Ilango, R., Loff, B., Oliveira, I.C.: NP-hardness of minimizing circuits and communication (2019), manuscript
36. Kabanets, V., Cai, J.Y.: Circuit minimization problem. In: ACM Symposium on Theory of Computing (STOC). pp. 73–79 (2000). https://doi.org/10.1145/335305.335314
37. Ko, K.: On the notion of infinite pseudorandom sequences. Theor. Comput. Sci. **48**(3), 9–33 (1986). https://doi.org/10.1016/0304-3975(86)90081-2

38. Ko, K.: On the complexity of learning minimum time-bounded Turing machines. In: Proceedings of the Third Annual Workshop on Computational Learning Theory, (COLT). pp. 82–96 (1990), see also [39].
39. Ko, K.: On the complexity of learning minimum time-bounded Turing machines. SIAM J. Comput. **20**(5), 962–986 (1991). https://doi.org/10.1137/0220059
40. Ko, K., Orponen, P., Schöning, U., Watanabe, O.: What is a hard instance of a computational problem? In: Structure in Complexity Theory. Lecture Notes in Computer Science, vol. 223, pp. 197–217. Springer (1986). https://doi.org/10.1007/3-540-16486-3_99, see also [51]
41. Kolmogorov, A.N.: Three approaches to the quantitative definition ofinformation'. Problems of information transmission **1**(1), 1–7 (1965)
42. Levin, L.: Universal search problems. Problems of Information Transmission **9**, 265–266 (1973)
43. Levin, L.A.: Randomness conservation inequalities; information and independence in mathematical theories. Information and Control **61**(1), 15–37 (1984). https://doi.org/10.1016/S0019-9958(84)80060-1
44. Li, M., Vitányi, P.M.B.: An Introduction to Kolmogorov Complexity and Its Applications, 4th Edition. Texts in Computer Science, Springer (2019). https://doi.org/10.1007/978-3-030-11298-1
45. McKay, D.M., Murray, C.D., Williams, R.R.: Weak lower bounds on resource-bounded compression imply strong separations of complexity classes. In: Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing (STOC). pp. 1215–1225 (2019). https://doi.org/10.1145/3313276.3316396
46. Meyer, A., McCreight, E.: Computationally complex and pseudo-random zero-one valued functions. In: Theory of Machines and Computations, pp. 19–42. Elsevier (1971)
47. Murray, C., Williams, R.: On the (non) NP-hardness of computing circuit complexity. Theory of Computing **13**(4), 1–22 (2017). https://doi.org/10.4086/toc.2017.v013a004
48. Oliveira, I., Santhanam, R.: Conspiracies between learning algorithms, circuit lower bounds and pseudorandomness. In: 32nd Conference on Computational Complexity, CCC. LIPIcs, vol. 79, pp. 18:1–18:49. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik (2017). https://doi.org/10.4230/LIPIcs.CCC.2017.18
49. Oliveira, I.C., Pich, J., Santhanam, R.: Hardness magnification near state-of-the-art lower bounds. In: 34th Computational Complexity Conference (CCC). LIPIcs, vol. 137, pp. 27:1–27:29. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik (2019). https://doi.org/10.4230/LIPIcs.CCC.2019.27
50. Oliveira, I.C., Santhanam, R.: Hardness magnification for natural problems. In: 59th IEEE Annual Symposium on Foundations of Computer Science (FOCS). pp. 65–76 (2018). https://doi.org/10.1109/FOCS.2018.00016
51. Orponen, P., Ko, K., Schöning, U., Watanabe, O.: Instance complexity. J. ACM **41**(1), 96–121 (1994). https://doi.org/10.1145/174644.174648
52. Paul, W.J., Seiferas, J.I., Simon, J.: An information-theoretic approach to time bounds for on-line computation (preliminary version). In: Proceedings of the Twelfth Annual ACM Symposium on Theory of Computing. pp. 357–367. STOC '80, ACM, New York, NY, USA (1980). https://doi.org/10.1145/800141.804685, see also [53]
53. Paul, W.J., Seiferas, J.I., Simon, J.: An information-theoretic approach to time bounds for on-line computation. J. Comput. Syst. Sci. **23**(2), 108–126 (1981). https://doi.org/10.1016/0022-0000(81)90009-X

54. Peterson, G.L.: Succinct representation, random strings, and complexity classes. In: 21st Annual Symposium on Foundations of Computer Science (FOCS). pp. 86–95 (1980). https://doi.org/10.1109/SFCS.1980.42
55. Pitt, L., Valiant, L.G.: Computational limitations on learning from examples. J. ACM **35**(4), 965–984 (1988). https://doi.org/10.1145/48014.63140
56. Pitt, L., Warmuth, M.K.: The minimum consistent DFA problem cannot be approximated within any polynomial. J. ACM **40**(1), 95–142 (1993). https://doi.org/10.1145/138027.138042
57. Rudow, M.: Discrete logarithm and minimum circuit size. Information Processing Letters **128**, 1–4 (2017). https://doi.org/10.1016/j.ipl.2017.07.005
58. Sipser, M.: A complexity theoretic approach to randomness. In: Proceedings of the 15th Annual ACM Symposium on Theory of Computing (STOC). pp. 330–335 (1983). https://doi.org/10.1145/800061.808762
59. Trakhtenbrot, B.A.: A survey of Russian approaches to perebor (brute-force searches) algorithms. IEEE Annals of the History of Computing **6**(4), 384–400 (1984)
60. Watanabe, O.: Kolmogorov Complexity and Computational Complexity. Springer Publishing Company, Incorporated, 1st edn. (2012)
61. Wilber, R.E.: Randomness and the density of hard problems. In: 24th Annual Symposium on Foundations of Computer Science (FOCS). pp. 335–342 (1983). https://doi.org/10.1109/SFCS.1983.49
62. Yao, A.C.: Theory and applications of trapdoor functions (extended abstract). In: 23rd Annual Symposium on Foundations of Computer Science (FOCS). pp. 80–91 (1982). https://doi.org/10.1109/SFCS.1982.45