NEW ZEALAND JOURNAL OF MATHEMATICS
Volume 52 (2021), 585–604
https://doi.org/10.53733/148

# VAUGHAN JONES, KOLMOGOROV COMPLEXITY, AND THE NEW COMPLEXITY LANDSCAPE AROUND CIRCUIT MINIMIZATION

Eric Allender

(Received 31 July, 2021)

Abstract. We survey recent developments related to the Minimum Circuit Size Problem and time-bounded Kolmogorov Complexity.

## 1. Introduction

When listing the many accomplishments of Vaughan Jones, the obituaries did not mention the fact that he is indirectly responsible for much of the modern development of the study of Algorithmic Information Theory, also known as Kolmogorov Complexity. This is because much of this modern development was spurred on by Rod Downey and Denis Hirschfeldt, who wrote, in the preface and acknowledgments for their influential book [**22**]:

> At the time, neither of us knew much about Kolmogorov complexity, but we had a distinct interest in it after Lance Fortnow's illuminating lectures at Kaikoura in January 2000. . . . As mentioned in the preface, our early interest in Kolmogorov complexity was stimulated by a talk given by Lance Fortnow at a conference in Kaikoura . . .

The conference in Kaikoura in January, 2000 was organized by the New Zealand Mathematical Research Institute (NZMRI), which owes its existence to the efforts of Vaughan Jones. I was also a participant in the 2000 Kaikoura conference, and that was the first time I met Vaughan. It was indeed a stimulating conference, and it led to other research-related visits to New Zealand.

One of those visits included participation in a meeting held to celebrate a significant birthday for Rod Downey, and I wrote a contribution to the Festschrift surveying the connections between Kolmogorov complexity and computational complexity theory [**1**]. Three years later, that survey was already out of date, with several of the open questions that were mentioned in [**1**] newly resolved, and some of the conjectures mentioned in [**1**] consigned to the scrap heap. (In particular, recent work [**29**] shows that these conjectures are extremely unlikely to be true.) Thus, when I was invited to give a keynote address at a conference in Milan in 2020 (which was postponed to the fall of 2021 due to COVID) I wrote a survey article [**2**] entitled "The *New* Complexity Landscape around Circuit Minimization" (emphasis added), where by "New" I signaled my intent to avoid repeating too many of the observations that were made in [**1**]. (It turns out that the studies of Circuit Minimization

*Key words and phrases:* Complexity Theory, Kolmogorov Complexity, Minimum Circuit Size Problem.

and Kolmogorov Complexity are closely related.) That survey began with these paragraphs:

> *Over the past few years, there has been an explosion of interest in the Minimum Circuit Size Problem (*MCSP*) and related problems. Thus the time seemed right to provide a survey, describing the new landscape and offering a guidebook so that one can easily reach the new frontiers of research in this area.*
>
> *It turns out that this landscape is extremely unstable, with new features arising at an alarming rate. Although this makes it a scientifically-exciting time, it also means that this survey is doomed to be obsolete before it appears. It also means that the survey is going to take the form of an "annotated bibliography" with the intent to provide many pointers to the relevant literature, along with a bit of context.*

As predicted, that survey, which was written for a conference that has not yet even taken place (due to the pandemic), is indeed already obsolete, with several important advances being announced in just the past year. Also, some unfortunate typographical errors and at least one misstatement wormed their way into [**2**]. Thus I offer this updated survey.

## 2. Meta-complexity, MCSP and Kolmogorov Complexity

The focus of complexity theory is to determine how hard problems are. The focus of *meta-complexity* is to determine how hard it is to determine how hard problems are. Some of the most exciting recent developments in complexity theory have been the result of meta-complexity-theoretic investigations.

The Minimum Circuit Size Problem (MCSP) is, quite simply, the problem of determining the circuit complexity of functions. The input consists of a pair $(f, i)$, where $f$ is a bit string of length $N = 2^n$ representing the truth-table of a Boolean function, and $i \in \mathbb{N}$, and the problem is to determine if $f$ has a circuit of size at most $i$.[1] The study of the complexity of MCSP is therefore the canonical meta-complexity-theoretic question. Complexity theoreticians are fond of complaining that the problems they confront (showing that computational problems are hard to compute) are notoriously difficult. But is this really true? Is it hard to show that a particular function is difficult to compute? This question can be made precise by asking about the computational complexity of MCSP. (See also [**55**] for a different approach.)

A small circuit is a short description of a large truth-table $f$; thus it is no surprise that investigations of MCSP have made use of the tools and terminology of Kolmogorov complexity. In order to discuss some of the recent developments, it will be necessary to review some of the different notions, and to establish the notation that will be used throughout the rest of the article.

[1] The terms "circuit" and "size" are intentionally left undefined here. There are many reasonable choices (such as "size" being the number of gates, or the number of wires, or the length of an encoding of the circuit description, or "circuits" consisting only of NAND gates, or allowing threshold gates, etc.) It is conceivable – although seemingly unlikely – that these variants have very different complexity. No reductions among these variants are known.

Let $U$ be a Turing machine. We define $K_U(x)$ to be $\min\{|d| : U(d) = x\}$. Those readers who are familiar with Kolmogorov complexity[2] will notice that the definition here is for what is sometimes called "plain" Kolmogorov complexity, although the notation $K_U(x)$ is more commonly used to denote what is called "prefix-free" Kolmogorov complexity. This is intentional. In this survey, the distinctions between these two notions will be blurred, in order to keep the discussion on a high level. Some of the theorems that will be mentioned below are only known to hold for the prefix-free variant, but the reader is encouraged to ignore these finer distinctions here, and seek the more detailed information in the cited references. For some Turing machines $U$, $K_U(x)$ will not be defined for some $x$, and the values of $K_U(x)$ and $K_{U'}(x)$ can be very different, for different machines $U$ and $U'$. But the beauty of Kolmogorov complexity (and the applicability of the theory it gives rise to) derives from the fact that if $U$ and $U'$ are *universal* Turing machines, then $K_U(x)$ and $K_{U'}(x)$ differ by at most $O(1)$. By convention, we select one particular universal machine $U$ and define $K(x)$ to be equal to $K_U(x)$.

The function $K$ is not computable. The simplest way to obtain a computable function that shares many of the properties of $K$ is to simply impose a time bound, leading to the definition $K^t(x) := \min\{|d| : U(d) = x \text{ in time } t(|x|)\}$ where $t$ is a computable function. Although it is useful in many contexts, $K^t(x)$ does not appear to be closely connected to the circuit size of $x$ (where $x$ is viewed as the truth-table of a function). Thus we will frequently refer to two additional resource-bounded Kolmogorov complexity measures, $\mathsf{Kt}$ and $\mathsf{KT}$.

Levin defined $\mathsf{Kt}(x)$ to be $\min\{|d| + \log t : U(d) = x \text{ in time } t\}$ [**41**]; it has the nice property that it can be used to define the optimal search strategy to use, in searching for accepting computations on a nondeterministic Turing machine. $\mathsf{Kt}(x)$ also corresponds to the circuit size of the function $x$, but not on "normal" circuits. As is shown in [**4**], $\mathsf{Kt}(x)$ is roughly the same as the size of the smallest *oracle* circuit that computes $x$, where the oracle is a complete set for $\mathsf{EXP}$. (An oracle circuit has "oracle gates" in addition to the usual AND, OR, and NOT gates; an oracle gate for oracle $A$ has $k$ wires leading into it, and if those $k$ wires encode a bitstring $y$ of length $k$ where $y$ is in $A$, then the gate outputs 1, otherwise it outputs 0.)

It is clearly desirable to have a version of Kolmogorov complexity that is more closely related to "ordinary" circuit size, instead of oracle circuit size. This is accomplished by defining $\mathsf{KT}(x)$ to be $\min\{|d| + t : U(d, i) = x_i \text{ in time } t\}$. (More precise definitions can be found in [**4, 14**].)

We have now presented a number of different measures $\mathsf{K}_\mu \in \{K, K^t, \mathsf{Kt}, \mathsf{KT}\}$. In order to connect the problem of computing these measures to the framework of complexity classes, it is useful to define corresponding decision problems, as follows: By analogy with $\mathsf{MCSP}$, we can study $\mathsf{K}_\mu$ in place of the "circuit size" measure, and thus obtain various problems of the form $\mathsf{MK}_\mu\mathsf{P} = \{(x, i) : \mathsf{K}_\mu(x) \leq i\}$, such as $\mathsf{MKTP}$, $\mathsf{M}K^t\mathsf{P}$ and $\mathsf{MKtP}$. If $t(n) = n^{O(1)}$, then $\mathsf{M}K^t\mathsf{P}$ is in $\mathsf{NP}$, and several theorems about $\mathsf{MKTP}$ yield corollaries about $\mathsf{M}K^t\mathsf{P}$ in this case. (See, e.g. [**4**]). Similarly, if $t(n) = 2^{n^c}$ for some $c > 0$, then $\mathsf{M}K^t\mathsf{P}$ is in $\mathsf{EXP}$, and several theorems about $\mathsf{MKtP}$ yield corollaries about $\mathsf{M}K^t\mathsf{P}$ for $t$ in this range [**4**].

[2] If the reader is not familiar with Kolmogorov complexity, then we recommend some excellent books on this topic [**43, 22**].

Table 1. List of the main complexity measures and decision problems dealing with Kolmogorov complexity considered here.

| Complexity Measure | Definition | Decision Problem |
|---|---|---|
| $K$ | $\min\{\|d\| : U(d) = x\}$ | MKP |
| $K^t$ | $\min\{\|d\| : U(d) = x$ in time $t(\|x\|)\}$ | M$K^t$P |
| Kt | $\min\{\|d\| + \log t : U(d) = x$ in time $t\}$ | MKtP |
| KT | $\min\{\|d\| + t : U(d, i) = x_i$ in time $t\}$ | MKTP |

In order to highlight some of the recent developments, let us introduce some notation that is somewhat imprecise and which is not used anywhere else, but which will be convenient for our purposes. Let $K^{poly}$ serve as a shorthand for $K^t$ whenever $t = n^{O(1)}$, and similarly let $K^{exp}$ serve as a shorthand for $K^t$ whenever $t = 2^{n^c}$ for some $c > 0$. We will thus be referring to M$K^{poly}$P and M$K^{exp}$P. Doing so will enable us to avoid some confusing notation surrounding the name MinKT, which was introduced by Ko [**40**] to denote the set

$$\mathsf{MinKT} = \{(x, 1^t, 1^i) : \exists d\ [U(d) = x \text{ in at most } t \text{ steps and } |d| \leq i]\}.$$

That is, $(x, i) \in$ M$K^{poly}$P iff $(x, 1^{n^c}, i) \in$ MinKT (where the time bound $t(n) = n^c$). Hence these sets have comparable complexity and results about MinKT can be rephrased in terms of M$K^{poly}$P with only a small loss of accuracy. In particular, some recent important results [**27, 28**] are phrased in terms of MinKT, and as such they deal with $K^{poly}$ complexity, and they are not really very closely connected with the KT measure; the name MinKT was devised more than a decade before KT was formulated. The reader who is interested in the details should refer to the original papers for the precise formulation of the theorems. However, the view presented here is "probably approximately correct".

Frequently, theorems about MCSP and the various MK$_\mu$P problems are stated not in terms of *exactly* computing the circuit size or the complexity of a string, but in terms of *approximating* these values. This is usually presented in terms of two thresholds $\theta_1 < \theta_2$, where the desired solution is to say *yes* if the complexity of $x$ is less than $\theta_1$, and to say *no* if the complexity of $x$ is greater than $\theta_2$, and any answer is allowed if the complexity of $x$ lies in the "gap" between $\theta_1$ and $\theta_2$. In the various theorems that have been proved in this setting, the choice of thresholds $\theta_1$ and $\theta_2$ is usually important, but in this article those details will be suppressed, and all of these approximation problems will be referred to as GapMCSP, GapMKtP, GapMKTP, etc.

At this point, the reader's eyes may be starting to glaze over. It is natural to wonder if we really need to have all of these different related notions. In particular, there does not seem to be much difference between MCSP and MKTP. Most hardness results for MCSP actually hold for GapMCSP, and if the "gap" is large enough, then MKTP is a solution to GapMCSP (and vice-versa). Furthermore it has frequently been the case that a theorem about MCSP was first proved for MKTP and then the result for MCSP was obtained as a corollary. However, there is no efficient reduction known (in either direction) between MCSP and MKTP, and there are some theorems that are currently known to hold only for MKTP, although they are suspected to hold also for MCSP (e.g., [**8, 10, 31, 20**]).[3] Similarly, some of the more intriguing recent developments can only be understood by paying attention to the distinction between different notions of resource-bounded Kolmogorov complexity. Thus it is worth making this investment in defining the various distinct notions.

## 3. Connections to Learning Theory

Certain connections between computational learning theory and Kolmogorov complexity were identified soon after computational learning theory emerged as a field. After all, the goal of computational learning theory is to find a satisfactory (and hence succinct) explanation of a large body of observed data. For instance, in the 1980s and 1990s (and even earlier [**25**]) there was work [**56, 57**] showing that it is NP-hard to find "succinct explanations" that have size somewhat close to the optimal size, if these "explanations" are required to be finite automata or various other restricted formalisms. Ko studied this in a more general setting, allowing "explanations" to be efficient programs (in the setting of time-bounded Kolmogorov complexity).

Thus Ko studied not only the problem of computing $K^{poly}(x)$ (where one can consider $x$ to be a completely-specified Boolean function), but also the problem of finding the smallest description $d$ such that $U(d)$ agrees with a given list of "yes instances" $Y$ and a list of "no instances" $N$ (that is, $x$ can be considered as a partial Boolean function, with many "don't care" instances). Thus, following [**36**], we can call this problem Partial-M$K^{poly}$P. In the setting that is most relevant for computational learning theory, the partial function $x$ is presented compactly as separate lists $Y$ and $N$, rather than as a string of length $2^n$ over the alphabet $\{0, 1, *\}$.

Ko showed in [**40**] that relativizing techniques would not suffice, in order to settle the question of whether M$K^{poly}$P and Partial-M$K^{poly}$P are NP-complete. That is, by giving the universal Turing machine $U$ that defines Kolmogorov complexity access to an oracle $A$, one obtains the problems $\mathsf{M}K^{poly}\mathsf{P}^A$ and $\text{Partial-}\mathsf{M}K^{poly}\mathsf{P}^A$, and these sets can either be $\mathsf{NP}^A$-complete or not, depending on the choice of $A$.

Thus it is noteworthy that it has recently been shown that Partial-MCSP is NP-complete under $\leq_m^{\mathsf{P}}$ reductions [**36**]. (As is usually the case[4], the proof also establishes that Partial-MKTP is NP-complete under $\leq_m^{\mathsf{P}}$ reductions.) One lesson to take from this is that KT and $K^{poly}$ complexity differ from each other in significant ways, since the result of Ko mentioned in the previous paragraph shows that Partial-M$K^{poly}$P, *cannot* be shown to be NP-complete using relativizing techniques. There are other recent examples of related phenomena, which will be discussed below.

There are other strong connections between MCSP and learning theory that have come to light recently. Using MCSP as an oracle (or even using a set that shares

[3] Given the close connection between KT and circuit size, the case can be made that MKTP is a particularly convenient formulation of MCSP. They are suspected to have equivalent complexity, but it seems to be easier to prove theorems about MKTP than MCSP.

[4] In fact, I am not aware of any instance where a theorem has been proved for MCSP and the proof does not carry over to MKTP. As mentioned in the last paragraph of the preceding section, there are some theorems that have been proved for MKTP that are not (yet) known to hold for MCSP.

certain characteristics with $\mathsf{MCSP}$) one can efficiently learn small circuits that do a good job of explaining the data [**15**]. For certain restricted classes of circuits, there are sets in $\mathsf{P}$ that one can use in place of $\mathsf{MCSP}$ to obtain learning algorithms that don't require an oracle [**15**]. This connection has been explored further [**51, 16**].

## 4. Completeness, Hardness, Reducibility

The preceding section mentioned a result about a problem being $\mathsf{NP}$-complete under $\leq^{\mathsf{P}}_{\mathrm{m}}$ reductions. In order to discuss other results about the complexity of $\mathsf{MCSP}$ and related problems it is necessary to go into more detail about different notions of reducibility.

Let $\mathcal{C}$ be either a class of functions or a class of circuits. The classes that will concern us the most are the standard complexity classes $\mathsf{L} \subseteq \mathsf{P} \subseteq \mathsf{NP}$ as well as the circuit classes (both uniform and nonuniform):

$$\mathsf{NC}^0 \subsetneq \mathsf{AC}^0 \subsetneq \mathsf{AC}^0[p] \subsetneq \mathsf{NC}^1 \subseteq \mathsf{P/poly}.$$

We refer the reader to the text by Vollmer [**63**] for background and more complete definitions of these standard circuit complexity complexity classes, as well as for a discussion of uniformity.

We say that $A \leq^{\mathcal{C}}_{\mathrm{m}} B$ if there is a function $f \in \mathcal{C}$ (or $f$ computed by a circuit family in $\mathcal{C}$, respectively) such that $x \in A$ iff $f(x) \in B$. We will make use of $\leq^{\mathsf{P}}_{\mathrm{m}}$,$\leq^{\mathsf{L}}_{\mathrm{m}}$, $\leq^{\mathsf{AC}^0}_{\mathrm{m}}$, $\leq^{\mathsf{NC}^0}_{\mathrm{m}}$, and $\leq^{\mathsf{proj}}_{\mathrm{m}}$ reducibility. This last notion ($\leq^{\mathsf{proj}}_{\mathrm{m}}$), refers to *projections*, which are functions computed by $\mathsf{NC}^0$ circuits that have only NOT gates. That is, in a projection, each output bit is either a constant 0 or 1, or is connected by a wire to an input bit or its negation.

The more powerful notion of Turing reducibility also plays an important role in this work. Here, $\mathcal{C}$ is a complexity class that admits a characterization in terms of Turing machines or circuits, which can be augmented with an "oracle" mechanism, either by providing a "query tape" or "oracle gates". We say that $A \leq^{\mathcal{C}}_{\mathrm{T}} B$ if there is a oracle machine in $\mathcal{C}$ (or a family of oracle circuits in $\mathcal{C}$) accepting $A$, when given oracle $B$. We make use of $\leq^{\mathsf{P/poly}}_{\mathrm{T}}$, $\leq^{\mathsf{RP}}_{\mathrm{T}}$, $\leq^{\mathsf{ZPP}}_{\mathrm{T}}$, $\leq^{\mathsf{BPP}}_{\mathrm{T}}$, $\leq^{\mathsf{P}}_{\mathrm{T}}$,$\leq^{\mathsf{L}}_{\mathrm{T}}$, $\leq^{\mathsf{NC}^1}_{\mathrm{T}}$ and $\leq^{\mathsf{AC}^0}_{\mathrm{T}}$ reducibility; instead of writing $A \leq^{\mathsf{P/poly}}_{\mathrm{T}} B$ or $A \leq^{\mathsf{ZPP}}_{\mathrm{T}} B$, we will sometimes write $A \in \mathsf{P}^B/\mathsf{poly}$ or $A \in \mathsf{ZPP}^B$. Turing reductions that are "nonadaptive" – in the sense that the list of queries that are posed on input $x$ does not depend on the answers provided by the oracle – are called *truth table reductions*. We make use of $\leq^{\mathsf{P}}_{\mathrm{tt}}$ and $\leq^{\mathsf{P/poly}}_{\mathrm{tt}}$ reducibility.

Once again, the reader may protest that this profusion of different notions of reducibility is unjustified and unmotivated. We will return to discuss this objection, after we present some of the hardness and non-hardness results, so that the reader will be in a better position to understand the motivation.

### 4.1. Hardness of MCSP.

The strongest hardness results that are known for the $\mathsf{MK}_\mu\mathsf{P}$ problems in $\mathsf{NP}$ remain the results of [**6**], where it was shown that $\mathsf{MCSP}$, $\mathsf{MKTP}$, and $\mathsf{M}K^{poly}\mathsf{P}$ are all hard for $\mathsf{SZK}$ under $\leq^{\mathsf{BPP}}_{\mathrm{T}}$ reductions. $\mathsf{SZK}$ is the class of problems that have statistical zero knowledge interactive proofs; $\mathsf{SZK}$ contains most of the problems that are assumed to be intractable, in order to build public-key cryptosystems. Thus it is widely assumed that $\mathsf{MCSP}$ and related problems lie outside of $\mathsf{P/poly}$, and cryptographers hope that it requires nearly exponential-sized circuits. $\mathsf{SZK}$ also contains the Graph Isomorphism problem, which is $\leq_{\mathrm{T}}^{\mathsf{RP}}$-reducible to $\mathsf{MCSP}$ and $\mathsf{MKTP}$. In [**8**], Graph Isomorphism (and several other problems) were shown to be $\leq_{\mathrm{T}}^{\mathsf{ZPP}}$ reducible to $\mathsf{MKTP}$; it remains unknown if this also holds for $\mathsf{MCSP}$. In fact, there is no interesting example of a problem $A$ that is not known to be in $\mathsf{NP} \cap \mathsf{coNP}$ that has been shown to be $\leq_{\mathrm{T}}^{\mathsf{ZPP}}$ reducible to $\mathsf{MCSP}$.

Although it is useful to know that every problem in $\mathsf{SZK}$ is "efficiently reducible" (via a $\mathsf{BPP}$ reduction) to $\mathsf{MCSP}$, this does not yield any unconditional lower bounds on the complexity of $\mathsf{MCSP}$, since it is still open whether $\mathsf{BPP} = \mathsf{EXP}$. Thus there is motivation to consider very restrictive reductions:

**Theorem 1.** [**7**] $\mathsf{MKTP}$ *is hard for* $\mathsf{co\text{-}NISZK_L}$ *under non-uniform* $\leq_{\mathrm{m}}^{\mathsf{proj}}$ *reductions. This also holds for* $\mathsf{MKtP}$ *and* $\mathsf{MKP}$.

Here, $\mathsf{co\text{-}NISZK_L}$ is a subclass of $\mathsf{SZK}$ that – like $\mathsf{SZK}$ – contains several problems that are widely believed to be cryptographically hard. It includes the well-known complexity classes $\mathsf{L}$ and $\mathsf{NL}$, as well as the class known as $\mathsf{DET}$: the class of problems $\mathsf{NC}^1$-Turing-reducible to computing the determinant.

Because projections are so computationally weak, this immediately implies that $\mathsf{MKTP}$ is not in $\mathsf{AC}^0[p]$ for any prime $p$. (This was mentioned as an open question in [**1**] (see footnote 2 of [**1**]).) It also implies that $\mathsf{MKTP}$ cannot be computed by $\mathsf{THRESHOLD} \circ \mathsf{MAJORITY}$ circuits of size $2^{n^{o(1)}}$, by appealing to a lower bound proved in [**23**]. It is currently still open whether this latter lower bound holds also for $\mathsf{MCSP}$.

The $\mathsf{AC}^0[p]$ lower bound for $\mathsf{MKTP}$ was first proved in [**10**]. It remained open whether $\mathsf{MCSP}$ was in $\mathsf{AC}^0[p]$ until this was established in [**26**], by showing that the problem of computing the determinant of integer matrices is reducible to $\mathsf{MCSP}$ via non-uniform $\leq_{\mathrm{T}}^{\mathsf{AC}^0}$ reductions. Incidentally, it is no accident that the reductions presented in [**7, 10, 26**] are non-uniform. If one can show that $\mathsf{MCSP}$ or $\mathsf{MKTP}$ is hard for $\mathsf{TC}^0$ under *uniform* $\leq_{\mathrm{T}}^{\mathsf{AC}^0}$ reductions, then one will have shown that $\mathsf{NP} \neq \mathsf{TC}^0$ [**11**]. Of course, most researchers would conjecture that $\mathsf{NP} \neq \mathsf{TC}^0$, and thus this should not be taken as evidence that non-uniformity is essential – only that it is essential given our current inability to prove lower bounds.

**4.2. Negative hardness results.** In the last section, we noted that proving hardness for $\mathsf{MKTP}$ under uniform $\leq_{\mathrm{T}}^{\mathsf{AC}^0}$ reductions will be difficult with our current understanding. This is just one example of what is by now a large collection of results, showing either that $\mathsf{MCSP}$ is *not* hard under a class of reductions, or at least showing that it will be difficult to show that it *is* hard. Table 2 is an updated version of a similar table that appeared in my earlier survey [**1**]. Table 2 presents information about the consequences that will follow if $\mathsf{MCSP}$ is $\mathsf{NP}$-complete (or even if it is hard for certain subclasses of $\mathsf{NP}$). There is some redundancy in the table, since some readers will primarily be interested in the consequences that follow if $\mathsf{MCSP}$ is $\mathsf{NP}$-complete under $\leq_{\mathrm{m}}^{\mathsf{P}}$ reductions, even though that line in the table follows from the lines dealing with hardness for subclasses of $\mathsf{NP}$ under even more powerful reductions. The "???" entry indicates that no consequences are known, if $\mathsf{MCSP}$ is $\mathsf{NP}$-complete under $\leq_{\mathrm{T}}^{\mathsf{P}}$ reductions. The table does not include results about some restricted versions of $\leq_{\mathrm{m}}^{\mathsf{P}}$ reductions, although the theorems of this type that were proved by Kabanets and Cai [**39**] were influential in starting off this line of research. One thing should jump out at the reader from Table 2: All of the conditions listed in Column 3 (with the exception of "FALSE") are widely believed to be true, although they all seem to be far beyond the reach of current proof techniques.

It is significant that neither $\mathsf{MCSP}$ nor $\mathsf{MKTP}$ is $\mathsf{NP}$-complete under $\leq_m^{n^{1/3}}$ reductions, since $\mathsf{SAT}$ and many other well-known problems *are* complete under this very restrictive notion of reducibility – but it would be more satisfying to know whether these problems can be complete under more widely-used reducibilities such as $\leq_{\mathrm{m}}^{\mathsf{AC}^0}$. These sublinear-time reductions are so restrictive, that even the $\mathsf{PARITY}$ problem is not $\leq_m^{n^{1/3}}$-reducible to $\mathsf{MCSP}$ or $\mathsf{MKTP}$.

TABLE 2. Summary of what is known about the consequences of $\mathsf{MCSP}$ being hard for $\mathsf{NP}$ under different types of reducibility. If $\mathsf{MCSP}$ is hard for the class in Column 1 under the reducibility shown in Column 2, then the consequence in Column 3 follows.

| class $\mathcal{C}$ | reductions $\mathcal{R}$ | statement $\mathcal{S}$ | Reference |
|---|---|---|---|
| $\mathsf{TC}^0$ | $\leq_m^{n^{1/3}}$ | FALSE[5] | [**50**] |
| $\mathsf{TC}^0$ | $\leq_{\mathrm{m}}^{\mathsf{AC}^0}$ | $\mathsf{LTH}^6 \not\subseteq \mathsf{io\text{-}SIZE}[2^{\Omega(n)}]$ and $\mathsf{P} = \mathsf{BPP}$ | [**11, 50**] |
| $\mathsf{TC}^0$ | $\leq_{\mathrm{m}}^{\mathsf{AC}^0}$ | $\mathsf{NP} \not\subseteq \mathsf{P/poly}$ | [**11**] |
| $\mathsf{TC}^0$ | $\leq_{\mathrm{T}}^{\mathsf{AC}^0}$ | $\mathsf{NP} \neq \mathsf{TC}^0$ | [**10**] |
| $\mathsf{NC}^1$ | $\leq_{\mathrm{T}}^{\mathsf{AC}^0}$ | $\mathsf{NP} \neq \mathsf{NC}$ | [**10**] |
| $\mathsf{P}$ | $\leq_{\mathrm{m}}^{\mathsf{L}}$ | $\mathsf{PSPACE} \neq \mathsf{P}$ | [**11**] |
| $\mathsf{ZPP}$ | $\leq_{\mathrm{T}}^{\mathsf{L}}$ | $\mathsf{PSPACE} \neq \mathsf{ZPP}$ | implicit in [**24**] |
| $\mathsf{ZPP}$ | $\leq_{\mathrm{tt}}^{\mathsf{P}}$ | $\mathsf{EXP} \neq \mathsf{ZPP}$ | [**24**] |
| $\mathsf{NP}$ | $\leq_{\mathrm{T}}^{\mathsf{AC}^0}$ | $\mathsf{NP} \neq (\mathsf{MA} \cap \mathsf{P/poly})$ | [**10**] |
| $\mathsf{NP}$ | $\leq_{\mathrm{m}}^{\mathsf{P}}$ | $\mathsf{EXP} \neq \mathsf{ZPP}$ | [**50**] |
| $\mathsf{NP}$ | $\leq_{\mathrm{tt}}^{\mathsf{P}}$ | $\mathsf{EXP} \neq \mathsf{ZPP}$ | [**33**] |
| $\mathsf{NP}$ | $\leq_{\mathrm{T}}^{\mathsf{P}}$ | ??? | [**60**] |

I suspect that Theorem 1 holds also for $\mathsf{MCSP}$. Let us pause, to consider one of the obstacles to proving this. The proof of Theorem 1 actually carries over to a version of Gap$\mathsf{MKTP}$ where the "gap" is quite small. Thus one avenue for proving a hardness result for $\mathsf{MCSP}$ had seemed to be to improve the hardness result for $\mathsf{MKTP}$, so that it worked for a much larger "gap". This avenue was subsequently blocked, when it was shown that $\mathsf{PARITY}$ is not $\mathsf{AC}^0$-reducible to Gap$\mathsf{MCSP}$ (or to Gap$\mathsf{MKTP}$) for a moderate-sized "gap" [**12**]. Thus, although it is still open whether $\mathsf{MCSP}$ is $\mathsf{NP}$-complete under $\leq_{\mathrm{m}}^{\mathsf{AC}^0}$ reductions, we now know that Gap$\mathsf{MCSP}$ is not $\mathsf{NP}$-complete under this notion of reducibility.

When a *much* larger "gap" is considered, it was shown in [**10**] that, if cryptographically-secure one-way functions exist, then Gap$\mathsf{MCSP}$ and Gap$\mathsf{MKTP}$ are $\mathsf{NP}$-intermediate in the sense that neither problem is in $\mathsf{P/poly}$, and neither problem is complete for $\mathsf{NP}$ under $\mathsf{P/poly}$-Turing reductions.

We close this section with a discussion of a very powerful notion of reducibility: $\mathsf{SNP}$ reductions. (Informally $A$ is $\mathsf{SNP}$ reducible to $B$ means that $A$ is $(\mathsf{NP} \cap$

[5] The notation "$\leq_m^{n^{1/3}}$" refers to "local reductions" computable in time bounded by the cube root of the input length. This is an important non-hardness result, because $\mathsf{SAT}$ and most familiar $\mathsf{NP}$-complete problems are complete under local reductions computable even in logarithmic time.

[6] $\mathsf{LTH}$ is the linear-time analog of the polynomial hierarchy. Problems in $\mathsf{LTH}$ are accepted by alternating Turing machines that make only $O(1)$ alternations and run for linear time.

$\mathsf{coNP}$)-reducible to $B$.) Hitchcock and Pavan have shown, under the very plausible assumption that $\mathsf{NP} \cap \mathsf{coNP}$ contains problems that require large circuits, that if $\mathsf{MCSP}$ is NP-complete (under the usual $\leq_{\mathrm{m}}^{\mathsf{P}}$ reductions), then it is also complete under $\mathsf{SNP}$ reductions whose queries avoid asking about very small circuit sizes; they are able to use this as a tool to derive additional interesting consequences from the assumption that $\mathsf{MCSP}$ is $\mathsf{NP}$-complete [**33**]. It is interesting to note that, back in the early 1990's, Ko explicitly considered the possibility that computing $\mathsf{M}K^{poly}\mathsf{P}$ might be $\mathsf{NP}$-complete under $\mathsf{SNP}$ reductions [**40**].

**4.3. Completeness in EXP and other classes.** There are problems "similar" to $\mathsf{MCSP}$ that reside in many complexity classes. We can define $\mathsf{MCSP}^A$ to be $\mathsf{MCSP}$ for oracle circuits with $A$-oracle gates. That is, $\mathsf{MCSP}^A = \{(f, i) : f$ has an $A$-oracle circuit of size at most $i\}$. When $A$ is complete for $\mathsf{EXP}$, then $\mathsf{MCSP}^A$ is thought of as being quite similar to $\mathsf{MKtP}$. Both of these problems, along with $\mathsf{M}K^{exp}\mathsf{P}$, are complete for $\mathsf{EXP}$ under $\leq_{\mathrm{tt}}^{\mathsf{P/poly}}$ and $\leq_{\mathrm{T}}^{\mathsf{NP}}$ reductions, and neither is complete for $\mathsf{EXP}$ under $\leq_{\mathrm{tt}}^{\mathsf{P}}$ reductions [**4**].

It is still open whether either of $\mathsf{MKtP}$ or $\mathsf{MCSP}^A$ is in $\mathsf{P}$, and it had been open if $\mathsf{M}K^t\mathsf{P}$ is in $\mathsf{P}$ for "small" exponential functions $t$ such as $t(n) = 2^{n/2}$. But there is recent progress:

**Theorem 2.** [**28**] $\mathsf{M}K^{exp}\mathsf{P}$ *is complete for* $\mathsf{EXP}$ *under* $\leq_{\mathrm{T}}^{\mathsf{ZPP}}$ *reductions.*

This seems to go a long way toward addressing Open Question 3.6 in [**1**].

In contrast to $\mathsf{MKtP}$, we know that $\mathsf{M}K^{exp}\mathsf{P}$ is not in $\mathsf{P}$. In fact, a much stronger result holds. Let $t$ be any superpolynomial function. Then the set of $K^t$-random strings $\{x : K^t(x) < |x|\}$ is *immune* to $\mathsf{P}$ (meaning: it has no infinite subset in $\mathsf{P}$) [**28**]. The proof does not seem to carry over to $\mathsf{Kt}$ complexity, highlighting a significant difference between $\mathsf{Kt}$ and $K^{exp}$.

Although it remains open whether $\mathsf{MKtP} \in \mathsf{P}$, Hirahara [**29**] does show that $\mathsf{MKtP}$ is not in $\mathsf{P}$-uniform $\mathsf{ACC}^0$, and in fact the set of $\mathsf{Kt}$-random strings is immune to $\mathsf{P}$-uniform $\mathsf{ACC}^0$. Furthermore, improved immunity results for the $\mathsf{Kt}$-random strings are in some sense possible *if and only if* better algorithms for $\mathsf{CircuitSAT}$ can be devised for larger classes of circuits [**28**].

Oliveira has defined a randomized version of $\mathsf{Kt}$ complexity, which is conjectured to be nearly the same as $\mathsf{Kt}$, but for which he is able to prove unconditional intractability results [**52**]. Lu and Oliveira also show that a version of the "coding theorem" for Kolmogorov complexity holds for this randomized version of $\mathsf{Kt}$, which is a nice property not known to hold for other versions of resource-bounded Kolmogorov complexity [**48**].

$\mathsf{MCSP}^{\mathsf{QBF}}$ was known to be complete for $\mathsf{PSPACE}$ under $\leq_{\mathrm{T}}^{\mathsf{ZPP}}$ reductions [**4**]. In more recent work, for various subclasses $\mathcal{C}$ of $\mathsf{PSPACE}$, when $A$ is a suitable complete problem for $\mathcal{C}$, then $\mathsf{MCSP}^A$ has been shown to be complete for $\mathcal{C}$ under $\leq_{\mathrm{T}}^{\mathsf{BPP}}$ reductions [**38**]. Crucially, the techniques used by [**38**] (and, indeed, by any of the authors who had proved hardness results for $\mathsf{MCSP}^A$ previously for various $A$) failed to work for any $A$ in the polynomial hierarchy. We will return to this issue in the following section.

In related work, it was shown [**10**] that the question of whether $\mathsf{MKTP}^A$ is hard for $\mathsf{DET}$ under a type of uniform $\mathsf{AC}^0$ reductions is equivalent to the question of whether $\mathsf{DSPACE}(n)$ contains any sets that require exponential-size $A$-oracle circuits. Furthermore, this happens if and only if PARITY reduces to $\mathsf{MKTP}^A$. Note that this condition is *more likely* to be true if $A$ is easy, than if $A$ is complex; it is false if $A$ is complete for PSPACE, and it is probably true if $A = \emptyset$. Thus, although $\mathsf{MKTP}^{\mathsf{QBF}}$ is almost certainly more complex than MKTP (the former is PSPACE-complete, and the latter is in NP), a reasonably-large subclass of P probably reduces to MKTP via these uniform $\mathsf{AC}^0$ reductions, whereas hardly anything $\mathsf{AC}^0$-reduces to $\mathsf{MKTP}^{\mathsf{QBF}}$. The explanation for this is that a uniform $\mathsf{AC}^0$ reduction cannot formulate any useful queries to a complex oracle, whereas it (probably) can do so for a simpler oracle.

**4.4. NP-Hardness.** Recall from the previous section that there were no NP-hardness results known for any problem of the form $\mathsf{MCSP}^A$ where $A$ is in the polynomial hierarchy.

This is still true; however, there is some progress to report. Hirahara has shown that computing the "conditional" complexity $K^{poly}(x|y)$ relative to SAT (i.e., given $(x, y)$, finding the length of the shortest description $d$ such that $U^{\mathsf{SAT}}(d, y) = x$ in time $n^c$) is NP-hard under $\leq_{\mathrm{tt}}^{\mathsf{P}}$ reductions [**28**].

It might be more satisfying to remove the SAT oracle, and have a hardness result for computing $K^{poly}(x|y)$ – but Hirahara [**29**] shows that this can't be shown to be hard for NP (or even hard for ZPP) under $\leq_{\mathrm{tt}}^{\mathsf{P}}$ reductions without first separating EXP from ZPP.

In a similar vein, if one were to show that MCSP or MKTP (or $\mathsf{MCSP}^A$ or $\mathsf{MKTP}^A$ for any set $A \in \mathsf{EXP}$) is hard for NP under $\leq_{\mathrm{tt}}^{\mathsf{P}}$ reductions, then one will have shown that $\mathsf{ZPP} \neq \mathsf{EXP}$ [**28**].

One should be careful how to interpret these results. To illustrate this, let me restate the result above, and provide additional context, for the particular case where $A$ is complete for EXP (in which case the proof carries over to MKtP: the problem of computing Levin's Kt complexity).

(1) If MKtP is hard for NP under $\leq_{\mathrm{tt}}^{\mathsf{P}}$ reductions, then $\mathsf{ZPP} \neq \mathsf{EXP}$ [**28**].
(2) If MKtP is hard for ZPP under $\leq_{\mathrm{tt}}^{\mathsf{P}}$ reductions, then $\mathsf{ZPP} \neq \mathsf{EXP}$ (This follows from the proof given in [**24**], showing the analogous result where MKtP is replaced by MCSP.)
(3) If MKtP is hard for NP under $\leq_{\mathrm{m}}^{\mathsf{P}}$ reductions, then $\mathsf{EXP} = \mathsf{NEXP}$ [**11**].

The second item is a strengthening of the first item; each of the first two items seem to be saying that we should not expect a proof in the near future, showing that MKtP is hard for NP (or even for ZPP) under $\leq_{\mathrm{m}}^{\mathsf{P}}$ reductions, since this would provide the long-awaited proof that EXP is not equal to ZPP. But the third item shows that the "expected" conclusion that $\mathsf{ZPP} \neq \mathsf{EXP}$ follows because of the *extremely unlikely* condition $\mathsf{EXP} = \mathsf{NEXP}$. Thus we should certainly *not* expect that MKtP is NP-hard under $\leq_{\mathrm{m}}^{\mathsf{P}}$ reductions. These results give us no guidance, regarding whether we should expect that MKtP is hard for ZPP under $\leq_{\mathrm{m}}^{\mathsf{P}}$ reductions.[7]

But let us return to the topic of NP-hardness for conditional versions of Kolmogorov complexity.

A different kind of NP-hardness result for conditional Kolmogorov complexity was proved recently by Ilango [**34**]. In [**4**], conditional KT complexity $\mathsf{KT}(x|y)$ was

[7] Of course, under the popular conjecture that $\mathsf{ZPP} = \mathsf{P}$, hardness holds trivially.

studied by making the string $y$ available to the universal Turing machine $U$ as an "oracle". Thus it makes sense to consider a "conditional complexity" version of $\mathsf{MCSP}$ by giving a string $y$ available to a circuit via oracle gates. This problem was formalized and shown to be $\mathsf{NP}$-complete under *randomized* reductions[8][**34**]. This proof was adapted [**5**] to show that $\mathsf{McKTP} = \{(x, y, i) : \mathsf{KT}(x|y) \leq i\}$ is also $\mathsf{NP}$-complete under randomized reductions. Neither of these problems can be shown to be hard for $\mathsf{NP}$ (or even for $\mathsf{ZPP}$) under $\leq^{\mathsf{P}}_{\mathrm{tt}}$ reductions, without first showing $\mathsf{ZPP} \neq \mathsf{EXP}$ (by adapting the proof in [**24**]).

Many of the functions that we compute daily produce more than one bit of output. Thus it makes sense to study the circuit size that is required in order to compute such functions. This problem is called $\mathsf{Multi\text{-}MCSP}$ in [**36**], where it is shown to be $\mathsf{NP}$-complete under randomized reductions. It will be interesting to see how the complexity of this problem varies, as the number of output bits of the functions under consideration shrinks toward one (at which point it becomes $\mathsf{MCSP}$).

It has been known since the 1970's that computing the size of the smallest DNF expression for a given truth-table is $\mathsf{NP}$-complete. (A simple proof, and a discussion of the history can be found in [**9**].) However, it remains unknown what the complexity is of finding the smallest depth-three circuit for a given truth table. (Some very weak intractability results for minimizing constant-depth circuits can be found in [**9**], giving subexponential reductions from the problem of factoring Blum integers.) The first real progress on this front was reported in [**30**], giving an $\mathsf{NP}$-completeness result (under $\leq^{\mathsf{P}}_{\mathrm{m}}$ reductions) for a class of depth three circuits (with MOD gates on the bottom level). Ilango proved that computing the size of the smallest depth-$d$ *formula* for a truth-table lies outside of $\mathsf{AC}^0[p]$ for any prime $p$ [**34**], and he has now followed that up with a proof that computing the size of the smallest depth-$d$ *formula* is $\mathsf{NP}$-complete under randomized quasipolynomial-time reductions [**35**]. Note that a constant-depth circuit can be transformed into a formula with only a polynomial blow-up; thus in many situations we are able to ignore the distinction between circuits and formulas in the constant-depth realm. However, the techniques employed in [**35, 34**] are quite sensitive to small perturbations in the size, and hence the distinction between circuits and formulae is important here. Still, this is dramatic progress on a front where progress has been very slow.

**4.5. Why so many kinds of reducibility?** I was pleased to be invited to give a lecture on Metacomplexity at the 2021 Computational Complexity Conference [**3**]. One of the questions from the audience after the lecture essentially asked: "Why do you bother with so many different types of reducibility?" I do not think that I gave this question a sufficiently clear and compelling answer. Let me try again here.

**Better lower bounds follow from hardness results using less-powerful forms of reducibility.** For instance, the lower bound proved in [**7**], showing that $\mathsf{MKTP}$ requires large $\mathsf{THRESHOLD} \circ \mathsf{MAJORITY}$ circuits of size $2^{n^{o(1)}}$ would not follow if we did not have a $\leq^{\mathsf{proj}}_{\mathrm{m}}$ reduction from a problem in $A \in \mathsf{L}$ to $\mathsf{MKTP}$,

[8] A randomized reduction from $A$ to $B$ is computed by a polynomial-time machine that takes as input a string $x$ and a string $r$ of random bits, such that, with high probability over the choice of $r$, $x \in A$ if and only if $M(x, r) \in B$.

where $A$ is known to require large circuits of this type. (Projections are typically the most restrictive notion of reducibility that is studied – although even in this instance we needed to use *non-uniform* projections, because hardness under uniform projections, or even uniform $\mathsf{AC}^0$ reductions, cannot be established without first separating $\mathsf{NP}$ from $\mathsf{TC}^0$ [**11**].) Similarly, the argument in [**26**] showing that $\mathsf{MCSP} \not\in \mathsf{AC}^0[p]$ required making use of $\leq_{\mathrm{T}}^{\mathsf{AC}^0}$ reducibility. Using a more powerful notion of reducibility would not have yielded the lower bound. And we still don't know if hardness under a more restrictive reducibility holds. Thus, even if you don't care about restrictive reductions, they can still be used as the means to a desirable end.

**On occasion, more powerful forms of reducibility are required, because hardness under more restrictive reducibilities fails to hold.** The problem $\mathsf{MKtP}$ provides an instructive example. It is useful to know that $\mathsf{MKtP}$ is complete for $\mathsf{EXP}$; but the only "efficient" reducibility for which this is known to hold is $\leq_{\mathrm{tt}}^{\mathsf{P/poly}}$. It is provably not complete under the usual $\leq_{\mathrm{m}}^{\mathsf{P}}$ or even $\leq_{\mathrm{tt}}^{\mathsf{P}}$ reducibility [**4**]. It is a significant open question whether it is complete under $\leq_{\mathrm{T}}^{\mathsf{P}}$ reductions. It is known that $\mathsf{MKtP}$ is in $\mathsf{ZPP}$ iff $\mathsf{EXP} = \mathsf{ZPP}$ [**4**], which is the conclusion one would obtain if $\mathsf{MKtP}$ were hard for $\mathsf{EXP}$ under $\leq_{\mathrm{T}}^{\mathsf{ZPP}}$ reductions – but we still do not know if hardness under $\leq_{\mathrm{T}}^{\mathsf{ZPP}}$ reductions holds. (This highlights the importance of Hirahara's proof that $\mathsf{M}K^{exp}\mathsf{P}$ *is* complete for $\mathsf{EXP}$ under $\leq_{\mathrm{T}}^{\mathsf{ZPP}}$ reductions [**28**].) Or consider the conditional $\mathsf{KT}$ problem $\mathsf{McKTP}$. It is useful to know that $\mathsf{McKTP}$ is $\mathsf{NP}$-complete under randomized reductions. If it's complete under $\leq_{\mathrm{m}}^{\mathsf{P}}$ reductions, then $\mathsf{EXP} \neq \mathsf{ZPP}$; if it's *not* complete under $\leq_{\mathrm{m}}^{\mathsf{P}}$ reductions, then $\mathsf{P} \neq \mathsf{NP}$. Thus it seems like we're unlikely to avoid randomized reductions when considering the complexity of this problem, until some of the longstanding questions in complexity are resolved. (There may be reasons to consider whether $\mathsf{McKTP}$ is hard under, say, randomized or nonuniform $\mathsf{AC}^0$ reductions, but this requires some extra work, and thus far there has not been a reason to take this step. In "most" cases, a problem that is hard under $\leq_{\mathrm{m}}^{\mathsf{P/poly}}$ reductions is actually hard under $\leq_{\mathrm{m}}^{\mathsf{AC}^0}$ or even $\leq_{\mathrm{m}}^{\mathsf{proj}}$ reductions, although for $\mathsf{MKTP}$ in particular this is an open question [**7**].)

The general lesson is: It's better to use more restrictive reducibilities, because doing so yields stronger conclusions. But more powerful notions of reducibility are sometimes the only feasible tool available, to draw an important connection about the complexity of a problem.

## 5. Average Case Complexity, One-Way Functions, and Cryptography

Cai and Kabanets gave birth to the modern study of $\mathsf{MCSP}$ in 2000 [**39**], in a paper that was motivated in part by the study of Natural Proofs [**58**], and which called attention to the fact that if $\mathsf{MCSP}$ is easy, then there are no cryptographically-secure one-way functions. In the succeeding decades, there has been speculation about whether the converse implication also holds. That is, can one base cryptography on assumptions about the complexity of $\mathsf{MCSP}$?

First, it should be observed that, in some sense, $\mathsf{MCSP}$ is very easy "on average". For instance the hardness results that we have (such as reducing $\mathsf{SZK}$ to $\mathsf{MCSP}$) show that the "hard instances" of $\mathsf{MCSP}$ are the ones where we want to distinguish between $n$-ary functions that require circuits of size $2^n/n^2$ (the "NO" instances) and those that have circuits of size at most $2^{n/3}$ (the "YES" instances). However, an algorithm that simply says "no" on all inputs will give the correct answer more than 99% of the time. (We will return to this point later in this section.)

Thus Hirahara and Santhanam [**31**] chose to study a different notion of heuristics for $\mathsf{MCSP}$, where algorithms must always give an answer in {Yes, No, I don't know}, where the algorithm never gives an incorrect answer ("*errorless heuristics*"), and the algorithm is said to perform well "on average" if it only seldom answers "I don't know". They were able to show unconditionally that $\mathsf{MCSP}$ is hard on average in this sense for $\mathsf{AC}^0[p]$ for any prime $p$, and to show that certain well-studied hypotheses imply that $\mathsf{MCSP}$ is hard on average.

More recently, Santhanam [**61**] has formulated a conjecture (which would involve too big of a digression to describe more carefully here), which – if true – would imply that a version of $\mathsf{MCSP}$ is hard on average in this sense if and only if cryptographically-secure one-way functions exist. That is, Santhanam's conjecture provides a framework for believing that one can base cryptography on the average-case complexity of $\mathsf{MCSP}$.

But how does the average-case complexity of $\mathsf{MCSP}$ depend on its worst-case complexity? Hirahara [**27**] showed that Gap$\mathsf{MCSP}$ has no solution in $\mathsf{BPP}$ if and only if a version of $\mathsf{MCSP}$ is hard on average. A related result stated in terms of $K^{poly}$ appears in the same paper. These results attracted considerable attention, because prior work had indicated that such worst-case-to-average-case reductions would be impossible to prove using black-box techniques. Additional work has given further evidence that the techniques of [**27**] are inherently non-black-box [**32**].

A flurry of recent activity has shown that the existence of cryptographically-secure one-way functions can indeed be *characterized* in terms of the complexity of computing time-bounded Kolmogorov complexity.

The initial breakthrough was provided by Liu and Pass, who showed that one-way functions exist if and only if $\mathsf{M}K^{poly}\mathsf{P}$ is hard-on-average [**44**] (in the sense of "regular" heuristics, rather than "errorless" heuristics).

Let us digress for a moment, to highlight the significance of this result of Liu and Pass. Although one-way functions are essential for cryptography, the nomination of any particular candidate one-way function has largely been guided more by heuristics, experimentation, and conjecture, instead of a firm theoretical foundation. There had never been a natural example of a computational problem whose complexity is equivalent to the existence of cryptographically-secure one-way functions. (There had long been an "unnatural" example, arising from Levin's "universal one-way function" [**42**]. But it is safe to say that this function, although of theoretical interest, has had little impact on practical cryptography.) In contrast, $\mathsf{M}K^{poly}\mathsf{P}$ has been studied for years, independent of any connection to cryptography. Thus [**44**] provided a new window into the theoretical foundations of cryptography. Furthermore, since Hirahara [**27**] had related the worst-case complexity of $\mathsf{M}K^{poly}\mathsf{P}$ to its average case complexity (albeit only for errorless heuristics), this seems to bring us closer to the goal of basing one-way functions on a worst-case complexity assumption for a problem where we have strong theoretical justification of intractability.

The result of [**44**] relates one-way functions to $\mathsf{M}K^{poly}\mathsf{P}$. What about MKTP? Ren and Santhanam addressed this question, by showing that MKTP is hard-on-average if and only if logspace-computable one-way functions exist [**59**]. Furthermore, this happens if and only if the NP-*complete* problem McKTP (discussed earlier) is hard-on-average [**5**]. In addition, if *any* one-way functions exist (not just those computable in logspace), then McKTP is "somewhat" hard-on-average [**5**]; thereby giving the first example of a "natural" NP-complete problem whose average-case complexity is tightly linked to the existence of cryptographically-secure one-way functions. Liu and Pass [**46**] subsequently provided an alternative definition of conditional time-bounded Kolmogorov complexity (which they also called McKTP), and showed that (a) it is also NP-complete under randomized reductions, and (b) it is hard on average if and only if one-way functions exist.

But NP is not the limit! It turns out that cryptographically-secure one-way functions exist if and only the EXP-*complete* problem MKtP is hard on average [**59, 47**]. Nor do things stop at EXP. Ilango, Ren, and Santhanam subsequently showed that one-way functions exist if and only if the *undecidable* problem MKP is hard on some samplable distribution (and they also provide yet another equivalent characterization, in terms of the average-case complexity of MCSP on a class of "locally-samplable" distributions) [**37**]. This was subsequently generalized again by Liu and Pass [**45**].

This connection between complexity-theoretical considerations and undecidable languages connects well to our next topic:

## 6. Complexity Classes and Noncomputable Complexity Measures

The title of this section is the same as the title of Section 4 of my earlier survey [**1**]. In that section, I described the work that had been done, studying the classes of sets that are reducible to the (non-computable) set of Kolmogorov-random strings $R_K$, and to MKP, including the reasons why it seemed reasonable to conjecture that BPP and NEXP could be characterized in terms of different types of reductions to the Kolmogorov-random strings.

I won't repeat that discussion here, because both of those conjectures have been disproved (barring some extremely unlikely complexity class collapses). Taken together, the papers [**32**], [**29**], and [**28**] give a much better understanding of the classes of languages reducible to the Kolmogorov-random strings.

Previously, it was known that $\mathsf{PSPACE} \subseteq \mathsf{P}^{R_K}$, and $\mathsf{NEXP} \subseteq \mathsf{NP}^{R_K}$. Hirahara [**28**] has now shown $\mathsf{NEXP} \subseteq \mathsf{EXP}^{\mathsf{NP}} \subseteq \mathsf{P}^{R_K}$.

This same paper also gives a surprising answer to Open Question 4.6 of [**1**], in showing that Quasipolynomial-time nonadaptive reductions to $R_K$ suffice to capture NP (and also some other classes in the polynomial hierarchy).

As described in [**1**], when we consider *uniform* reductions to MKP (such as $\leq_{\mathrm{T}}^{\mathsf{P}}$ or $\leq_{\mathrm{T}}^{\mathsf{NP}}$ reductions) that hold regardless of the universal Turing machine that is used in defining Kolmogorov complexity, only subclasses of EXPSPACE result (and when $\leq_{\mathrm{tt}}^{\mathsf{P}}$ reductions are used, one obtains a class between BPP and PSPACE). It is not clear what the true picture is.

Similarly, when one considers *nonuniform* reductions to MKP all computably-enumerable sets are $\leq_{\mathrm{tt}}^{\mathsf{P/poly}}$-reducible to MKP, but no complexity class larger than co-$\mathsf{NISZK_L}$ is known to be $\leq_{\mathrm{m}}^{\mathsf{AC}^0}$ reducible to MKP [**7**]. It seems unlikely that this is is optimal.

## 7. Magnification

Some of the most important and exciting developments relating to MCSP and related problems deal with the emerging study of "hardness magnification". This is the phenomenon whereby seemingly very modest lower bounds can be "amplified" or "magnified" and thereby be shown to imply superpolynomial lower bounds. I was involved in some of the early work in this direction [**13**] (which did not involve MCSP), but much stronger work has subsequently appeared.

It is important to note, in this regard, that lower bounds have been proved for MCSP that essentially match the strongest lower bounds that we have for any problems in NP [**21**]. There is now a significant body of work, showing that slight improvements to those bounds, or other seemingly-attainable lower bounds for GapMKtP or GapMCSP or related problems, would yield dramatic complexity class separations [**19, 18, 17, 16, 62, 54, 53, 49**].

In particular, I'd like to put a spotlight on two theorems. To state the theorems, let $\mathsf{MCSP}[s(n)]$ denote the set of truth tables $f$ of $n$-ary Boolean functions that have circuits of size $\leq s(n)$. That is $\mathsf{MCSP}[s(n)] = \{f : |f| = N = 2^n \wedge (f, s(n)) \in \mathsf{MCSP}\}$.

- $\mathsf{MCSP}[2^{\epsilon n}]$ requires time more than $N^{1.99}$ on any one-tape probabilistic Turing machine [**20**].
- If $\mathsf{MCSP}[2^{\delta n}]$ requires time more than $N^{1.01}$ on any one-tape *deterministic* Turing machine, then $\mathsf{P} \neq \mathsf{NP}$ [**49**].

If it were not the case that $\delta < \epsilon$, this would yield a proof of $\mathsf{P} \neq \mathsf{NP}$.

This would be a good place to survey the field of hardness magnification, except that an excellent survey already appears in [**16**]. Igor Carboni Oliveira has also written some notes entitled "Advances in Hardness Magnification" related to a talk he gave at the Simons Institute in December, 2019, available on his home page. These notes and [**16**] describe in detail the reasons that this approach seems to avoid the Natural Proofs barrier identified in the work of Razborov and Rudich [**58**]. But they also describe some potential obstacles that need to be overcome, before this approach can truly be used to separate complexity classes.

## Acknowledgments

Thanks are due to Rahul Santhanam, for calling attention to some misstatements in an earlier version of this survey [**2**]. I also thank Noah Singer and Harsha Tirumala for helpful discussions.

## References

[1] Eric Allender. The complexity of complexity. In *Computability and Complexity: Essays Dedicated to Rodney G. Downey on the Occasion of his 60th Birthday*, volume 10010 of *Lecture Notes in Computer Science*, pages 79–94. Springer, 2017.

[2] Eric Allender. The new complexity landscape around circuit minimization. In *Proc. 14th International Conference on Language and Automata Theory and*

*Applications (LATA)*, volume 12038 of *Lecture Notes in Computer Science*, pages 3–16. Springer, 2020.

[3] Eric Allender. How much information is in the title of this lecture? (invited lecture). 2021.

[4] Eric Allender, Harry Buhrman, Michal Koucký, Dieter van Melkebeek, and Detlef Ronneburger. Power from random strings. *SIAM Journal on Computing*, 35:1467–1493, 2006.

[5] Eric Allender, Mahdi Cheraghchi, Dimitrios Myrisiotis, Harsha Tirumala, and Ilya Volkovich. One-way functions and partial MCSP. Technical Report TR21-9, Electronic Colloquium on Computational Complexity (ECCC), 2021.

[6] Eric Allender and Bireswar Das. Zero knowledge and circuit minimization. *Information and Computation*, 256:2–8, 2017. Special issue for MFCS '14.

[7] Eric Allender, John Gouwar, Shuichi Hirahara, and Caleb Robelle. Cryptographic hardness under projections for time-bounded Kolmogorov complexity. Technical Report TR21-10, Electronic Colloquium on Computational Complexity (ECCC), 2021.

[8] Eric Allender, Joshua Grochow, Dieter van Melkebeek, Andrew Morgan, and Cristopher Moore. Minimum circuit size, graph isomorphism and related problems. *SIAM Journal on Computing*, 47:1339–1372, 2018.

[9] Eric Allender, Lisa Hellerstein, Paul McCabe, Toniann Pitassi, and Michael E. Saks. Minimizing disjunctive normal form formulas and $\mathrm{AC}^0$ circuits given a truth table. *SIAM Journal on Computing*, 38(1):63–84, 2008.

[10] Eric Allender and Shuichi Hirahara. 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.

[11] Eric Allender, Dhiraj Holden, and Valentine Kabanets. The minimum oracle circuit size problem. *Computational Complexity*, 26(2):469–496, 2017.

[12] Eric Allender, Rahul Ilango, and Neekon Vafa. The non-hardness of approximating circuit size. *Theory Comput. Syst.*, 65(3):559–578, 2021. Special issue for CSR'19.

[13] Eric Allender and Michal Koucký. Amplifying lower bounds by means of self-reducibility. *J. ACM*, 57:14:1 – 14:36, 2010.

[14] Eric Allender, Michal Koucký, Detlef Ronneburger, and Sambuddha Roy. The pervasive reach of resource-bounded Kolmogorov complexity in computational complexity theory. *Journal of Computer and System Sciences*, 77:14–40, 2010.

[15] Marco Carmosino, Russell Impagliazzo, Valentine Kabanets, and Antonina Kolokolova. Learning algorithms from natural proofs. In *31st Conference on Computational Complexity, CCC*, volume 50 of *LIPIcs*, pages 10:1–10:24. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2016.

[16] Lijie Chen, Shuichi Hirahara, Igor Carboni Oliveira, Ján Pich, Ninad Rajgopal, and Rahul Santhanam. Beyond natural proofs: Hardness magnification and locality. In *11th Innovations in Theoretical Computer Science Conference (ITCS)*, volume 151 of *LIPIcs*, pages 70:1–70:48. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2020.

[17] Lijie Chen, Ce Jin, and Ryan Williams. Hardness magnification for all sparse NP languages. In *Symposium on Foundations of Computer Science (FOCS)*, pages 1240–1255, 2019.

[18] Lijie Chen, Ce Jin, and Ryan Williams. Sharp threshold results for computational complexity. Manuscript, 2019.

[19] Lijie Chen, Dylan M. McKay, Cody D. Murray, and R. Ryan Williams. Relations and equivalences between circuit lower bounds and Karp-Lipton theorems. In *34th Computational Complexity Conference (CCC)*, volume 137 of *LIPIcs*, pages 30:1–30:21. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2019.

[20] Mahdi Cheraghchi, Shuichi Hirahara, Dimitrios Myrisiotis, and Yuichi Yoshida. One-tape turing machine and branching program lower bounds for MCSP. In Markus Bläser and Benjamin Monmege, editors, *38th International Symposium on Theoretical Aspects of Computer Science (STACS)*, volume 187 of *LIPIcs*, pages 23:1–23:19. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021.

[21] Mahdi Cheraghchi, Valentine Kabanets, Zhenjian Lu, and Dimitrios Myrisiotis. Circuit lower bounds for MCSP from local pseudorandom generators. *ACM Trans. Comput. Theory*, 12(3):21:1–21:27, 2020.

[22] R. Downey and D. Hirschfeldt. *Algorithmic Randomness and Complexity.* Springer, 2010.

[23] Jürgen Forster, Matthias Krause, Satyanarayana V. Lokam, Rustam Mubarakzjanov, Niels Schmitt, and Hans Ulrich Simon. Relations between communication complexity, linear arrangements, and computational complexity. In *Proc. 21st Foundations of Software Technology and Theoretical Computer Science (FSTTCS)*, volume 2245 of *Lecture Notes in Computer Science*, pages 171–182. Springer, 2001.

[24] Bin Fu. Hardness of sparse sets and minimal circuit size problem. In Donghyun Kim, R. N. Uma, Zhipeng Cai, and Dong Hoon Lee, editors, *Computing and Combinatorics - 26th International Conference, (COCOON)*, volume 12273 of *Lecture Notes in Computer Science*, pages 484–495. Springer, 2020.

[25] E. Mark Gold. Complexity of automaton identification from given data. *Inf. Control.*, 37(3):302–320, 1978.

[26] Alexander Golovnev, Rahul Ilango, Russell Impagliazzo, Valentine Kabanets, Antonina Kolokolova, and Avishay Tal. $\mathrm{AC}^0[p]$ lower bounds against MCSP via the coin problem. In *46th International Colloquium on Automata, Languages, and Programming,(ICALP)*, volume 132 of *LIPIcs*, pages 66:1–66:15. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2019.

[27] Shuichi Hirahara. Non-black-box worst-case to average-case reductions within NP. In *59th IEEE Annual Symposium on Foundations of Computer Science (FOCS)*, pages 247–258, 2018.

[28] Shuichi Hirahara. Unexpected hardness results for Kolmogorov complexity under uniform reductions. In Konstantin Makarychev, Yury Makarychev, Madhur Tulsiani, Gautam Kamath, and Julia Chuzhoy, editors, *Proccedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing (STOC)*, pages 1038–1051. ACM, 2020.

[29] Shuichi Hirahara. Unexpected power of random strings. In *11th Innovations in Theoretical Computer Science Conference, ITCS*, volume 151 of *LIPIcs*, pages 41:1–41:13. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2020.

[30] Shuichi Hirahara, Igor Carboni Oliveira, and Rahul Santhanam. NP-hardness of minimum circuit size problem for OR-AND-MOD circuits. In *33rd Conference on Computational Complexity, CCC*, volume 102 of *LIPIcs*, pages 5:1–5:31. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2018.

[31] Shuichi Hirahara and Rahul Santhanam. On the average-case complexity of MCSP and its variants. In *32nd Conference on Computational Complexity, CCC*, volume 79 of *LIPIcs*, pages 7:1–7:20. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2017.

[32] Shuichi Hirahara and Osamu Watanabe. On nonadaptive reductions to the set of random strings and its dense subsets. In Ding-Zhu Du and Jie Wang, editors, *Complexity and Approximation - In Memory of Ker-I Ko*, volume 12000 of *Lecture Notes in Computer Science*, pages 67–79. Springer, 2020.

[33] John M. Hitchcock and Aduri Pavan. On the NP-completeness of the minimum circuit size problem. In *Conference on Foundations of Software Technology and Theoretical Computer Science (FST&TCS)*, volume 45 of *LIPIcs*, pages 236–245. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2015.

[34] Rahul Ilango. Approaching MCSP from above and below: Hardness for a conditional variant and $\mathrm{AC}^0[p]$. In *11th Innovations in Theoretical Computer Science Conference, ITCS*, volume 151 of *LIPIcs*, pages 34:1–34:26. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2020.

[35] Rahul Ilango. Constant depth formula and partial function versions of MCSP are hard. In *61st IEEE Annual Symposium on Foundations of Computer Science (FOCS)*, pages 424–433. IEEE, 2020.

[36] Rahul Ilango, Bruno Loff, and Igor Carboni Oliveira. NP-hardness of circuit minimization for multi-output functions. In Shubhangi Saraf, editor, *35th Computational Complexity Conference (CCC)*, volume 169 of *LIPIcs*, pages 22:1–22:36. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020.

[37] Rahul Ilango, Hanlin Ren, and Rahul Santhanam. Hardness on any samplable distribution suffices: New characterizations of one-way functions by meta-complexity. Technical Report TR21-82, Electronic Colloquium on Computational Complexity (ECCC), 2021.

[38] R. Impagliazzo, V. Kabanets, and I. Volkovich. The power of natural properties as oracles. In *33rd Conference on Computational Complexity, CCC*, volume 102 of *LIPIcs*, pages 7:1–7:20. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2018.

[39] Valentine Kabanets and Jin-Yi Cai. Circuit minimization problem. In *ACM Symposium on Theory of Computing (STOC)*, pages 73–79, 2000.

[40] Ker-I Ko. On the notion of infinite pseudorandom sequences. *Theor. Comput. Sci.*, 48(3):9–33, 1986.

[41] Leonid A. Levin. Randomness conservation inequalities; information and independence in mathematical theories. *Information and Control*, 61(1):15–37, 1984.

[42] Leonid A. Levin. The tale of one-way functions. *Probl. Inf. Transm.*, 39(1):92–103, 2003.

[43] Ming Li and Paul M. B. Vitányi. *An Introduction to Kolmogorov Complexity and Its Applications, 4th Edition.* Texts in Computer Science. Springer, 2019.

[44] Yanyi Liu and Rafael Pass. On one-way functions and Kolmogorov complexity. In *61st IEEE Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1243–1254. IEEE, 2020.

[45] Yanyi Liu and Rafael Pass. A note on one-way functions and sparse languages. Technical Report TR21-92, Electronic Colloquium on Computational Complexity (ECCC), 2021.

[46] Yanyi Liu and Rafael Pass. On one-way functions from NP-complete problems. Technical Report TR21-59, Electronic Colloquium on Computational Complexity (ECCC), 2021.

[47] Yanyi Liu and Rafael Pass. On the possibility of basing cryptography on EXP $\neq$ BPP. Technical Report TR21-56, Electronic Colloquium on Computational Complexity (ECCC), 2021.

[48] Zhenjian Lu and Igor Carboni Oliveira. An efficient coding theorem via probabilistic representations and its applications. In Nikhil Bansal, Emanuela Merelli, and James Worrell, editors, *48th International Colloquium on Automata, Languages, and Programming (ICALP)*, volume 198 of *LIPIcs*, pages 94:1–94:20. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021.

[49] Dylan M. McKay, Cody D. Murray, and R. Ryan Williams. 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)*, pages 1215–1225, 2019.

[50] Cody Murray and Ryan Williams. On the (non) NP-hardness of computing circuit complexity. *Theory of Computing*, 13(4):1–22, 2017.

[51] Igor Oliveira and Rahul Santhanam. Conspiracies between learning algorithms, circuit lower bounds and pseudorandomness. In *32nd Conference on Computational Complexity, CCC*, volume 79 of *LIPIcs*, pages 18:1–18:49. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2017.

[52] Igor Carboni Oliveira. Randomness and intractability in Kolmogorov complexity. In *46th International Colloquium on Automata, Languages, and Programming,(ICALP)*, volume 132 of *LIPIcs*, pages 32:1–32:14. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2019.

[53] Igor Carboni Oliveira, Ján Pich, and Rahul Santhanam. Hardness magnification near state-of-the-art lower bounds. In *34th Computational Complexity Conference (CCC)*, volume 137 of *LIPIcs*, pages 27:1–27:29. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2019.

[54] Igor Carboni Oliveira and Rahul Santhanam. Hardness magnification for natural problems. In *59th IEEE Annual Symposium on Foundations of Computer Science (FOCS)*, pages 65–76, 2018.

[55] Ján Pich and Rahul Santhanam. Why are proof complexity lower bounds hard? In *Symposium on Foundations of Computer Science (FOCS)*, pages 1305–1324, 2019.

[56] Leonard Pitt and Leslie G. Valiant. Computational limitations on learning from examples. *J. ACM*, 35(4):965–984, 1988.

[57] Leonard Pitt and Manfred K. Warmuth. The minimum consistent DFA problem cannot be approximated within any polynomial. *J. ACM*, 40(1):95–142, 1993.

[58] Alexander Razborov and Steven Rudich. Natural proofs. *Journal of Computer and System Sciences*, 55:24–35, 1997.

[59] Hanlin Ren and Rahul Santhanam. Hardness of KT characterizes parallel cryptography. In Valentine Kabanets, editor, *36th Computational Complexity Conference (CCC)*, volume 200 of *LIPIcs*, pages 35:1–35:58. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021.

[60] Michael Saks and Rahul Santhanam. Circuit lower bounds from np-hardness of MCSP under Turing reductions. In Shubhangi Saraf, editor, *35th Computational Complexity Conference (CCC)*, volume 169 of *LIPIcs*, pages 26:1–26:13. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020.

[61] Rahul Santhanam. Pseudorandomness and the minimum circuit size problem. In *11th Innovations in Theoretical Computer Science Conference (ITCS)*, volume 151 of *LIPIcs*, pages 68:1–68:26. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2020.

[62] Avishay Tal. The bipartite formula complexity of inner-product is quadratic. *Electronic Colloquium on Computational Complexity (ECCC)*, 23:181, 2016.

[63] Heribert Vollmer. *Introduction to Circuit Complexity: A Uniform Approach.* Springer-Verlag New York Inc., 1999.

Rutgers University
New Brunswick
NJ 08854
USA.
allender@cs.rutgers.edu