New Insights on the (Non-)Hardness of Circuit Minimization and Related Problems

Eric Allender¹ and Shuichi Hirahara²

¹ Department of Computer Science, Rutgers University, Piscataway, NJ, USA, allender@cs.rutgers.edu
² Department of Computer Science, The University of Tokyo, Tokyo, Japan, hirahara@is.s.u-tokyo.ac.jp

Abstract

The Minimum Circuit Size Problem (MCSP) and a related problem (MKTP) that deals with time-bounded Kolmogorov complexity are prominent candidates for NP-intermediate status. We show that, under very modest cryptographic assumptions (such as the existence of one-way functions), the problem of approximating the minimum circuit size (or time-bounded Kolmogorov complexity) within a factor of $n^{1-o(1)}$ is indeed NP-intermediate. To the best of our knowledge, these problems are the first natural NP-intermediate problems under the existence of an arbitrary one-way function. Our technique is quite general; we use it also to show that approximating the size of the largest clique in a graph within a factor of $n^{1-o(1)}$ is also NP-intermediate unless NP ⊆ P/poly.

We also prove that MKTP is hard for the complexity class DET under non-uniform NC⁰ reductions. This is surprising, since prior work on MCSP and MKTP had highlighted weaknesses of "local" reductions such as $\leq^p_{NC^0}$. We exploit this local reduction to obtain several new consequences:

- MKTP is not in $AC^0[p]$.
- Circuit size lower bounds are equivalent to hardness of a relativized version $MKTP^A$ of MKTP under a class of uniform $AC^0$ reductions, for a large class of sets $A$.
- Hardness of $MCSP^A$ implies hardness of $MKTP^A$ for a wide class of sets $A$. This is the first result directly relating the complexity of $MCSP^A$ and $MKTP^A$, for any $A$.

1998 ACM Subject Classification F.1.3 Complexity Measures and Classes

Keywords and phrases computational complexity, Kolmogorov complexity, Circuit size

Digital Object Identifier 10.4230/LIPIcs...

1 Introduction

The Minimum Circuit Size Problem (MCSP) has attracted intense study over the years, because of its close connection with the natural proofs framework of Razborov and Rudich [34], and because it is a prominent candidate for NP-intermediate status. It has been known since the work of Ladner [27] that NP-intermediate problems exist if P ≠ NP, but “natural” candidates for this status are rare. Problems such as factoring and Graph Isomorphism are sometimes put forward as candidates, but there are not strong complexity-theoretic arguments for why these problems should not lie in P. We prove that a very weak cryptographic assumption implies that a $n^{1-o(1)}$ approximation for MCSP is NP-intermediate.

* Supported by NSF grant CCF-1555409 (Allender) and JSPS KAKENHI Grant Numbers JP16J06743 (Hirahara).

© Eric Allender and Shuichi Hirahara; licensed under Creative Commons License CC-BY
Leibniz International Proceedings in Informatics

1 Introduction

The Minimum Circuit Size Problem (MCSP) has attracted intense study over the years, because of its close connection with the natural proofs framework of Razborov and Rudich [34], and because it is a prominent candidate for NP-intermediate status. It has been known since the work of Ladner [27] that NP-intermediate problems exist if P ≠ NP, but “natural” candidates for this status are rare. Problems such as factoring and Graph Isomorphism are sometimes put forward as candidates, but there are not strong complexity-theoretic arguments for why these problems should not lie in P. We prove that a very weak cryptographic assumption implies that a $n^{1-o(1)}$ approximation for MCSP is NP-intermediate.

* Supported by NSF grant CCF-1555409 (Allender) and JSPS KAKENHI Grant Numbers JP16J06743 (Hirahara).
MCSP is hard for SZK [5] under BPP reductions, but the situation is quite different, when more restricted notions of reducibility are considered. Recent results [7, 20, 29] have suggested that MCSP might not even be hard for \text{P} under logspace or \text{AC}^0 reductions (although the evidence is still inconclusive).

The input to MCSP consists of a pair \((T, s)\), where \(T\) is a bit string of length \(2^n\) representing the truth-table of an \(m\)-variate Boolean function, and \(s \in \mathbb{N}; (T, s) \in \text{MCSP}\) if there is a circuit computing \(T\) having size at most \(s\). Note that, for different models of circuit (type of gates, allowable fan-in, etc.) and different measures of size (number of gates, number of wires, size of the description of the circuit, etc.) the resulting MCSP problems might have different complexity. No efficient reduction is known between different variants of the problem. However, all prior work on MCSP (such as [4, 5, 7, 9, 20, 21, 22, 25, 29, 36]) applies equally well to any of these variants. MCSP is also closely related to a type of time-bounded Kolmogorov complexity known as \(\text{KT}\), which was defined in [4]. The problem of determining \(\text{KT}\) complexity, formalized as the language \(\text{MKTP} = \{(x, s) : \text{KT}(x) \leq s\}\) has often been viewed as just another equivalent “encoding” of MCSP in this prior work. (In particular, our results mentioned in the paragraphs above apply also to MKTP.) Recently, however, some reductions were presented that are not currently known to apply to MCSP [6, 19].

In this section, we outline the ways in which this paper advances our understanding of MCSP and related problems, while reviewing some of the relevant prior work.

**Hardness is equivalent to circuit size lower bounds.** Significant effort (e.g. [25, 29, 7, 20]) has been made in order to explain why it is so difficult to show \(\text{NP}\)-hardness of MCSP or MKTP. Most of the results along this line showed implications from hardness of MCSP to circuit size lower bounds: If MCSP or MKTP is \(\text{NP}\)-hard under some restricted types of reductions, then a circuit size lower bound (which is quite difficult to obtain via current techniques of complexity theory) follows. For example, if \(\text{MCSP}\) or \(\text{MKTP}\) is hard for \(\text{TC}^0\) under \(\text{Dlogtime-uniform} \leq_{\text{AC}^0}\) reductions, then \(\text{NP} \not\subseteq \text{P/poly}\) and \(\text{DSPACE}(n) \not\subseteq \text{io-SIZE}(2^n)\) [29, 7].

Murray and Williams [29] asked if, in general, circuit lower bounds imply hardness of the circuit minimization problems. We answer their questions affirmatively in certain settings: A stronger lower bound \(\text{DSPACE}(n) \not\subseteq \text{io-SIZE}^{\text{MKTP}}(2^n)\) implies that MKTP is hard for \(\text{DET}\) under logspace-uniform \(\leq_{\text{AC}^0}\) reductions (Theorem 15).

At this point, it is natural to ask if the circuit lower bounds are in fact equivalent to hardness of MKTP. We indeed show that this is the case, when we consider the minimum \textit{oracle} circuit size problem. For an oracle \(A\), \(\text{MCSP}^A\) is the set of pairs \((T, s)\) such that \(T\) is computed by a size-\(s\) circuit that has “oracle gates” for \(A\) in addition to standard AND and OR gates. The related \(\text{MKTP}^A\) problem asks about the time-bounded Kolmogorov complexity of a string, when the universal Turing machine has access to the oracle \(A\). For many oracles \(A\) that are hard for \(\text{PH}\), we show that \(\text{DSPACE}(n) \not\subseteq \text{io-SIZE}^A(2^n)\) for some \(\epsilon > 0\) if and only if \(\text{MKTP}^A\) is hard for \(\text{DET}\) under a certain class of reducibilities (Theorem 17).

That is, it is impossible to prove hardness of \(\text{MKTP}^A\) (under some reducibilities) without proving circuit lower bounds, and vice versa. Our results clearly connect the fact that it is difficult to obtain hardness of \(\text{MKTP}^A\) with the fact that circuit size lower bounds are difficult.

**Hardness under local reductions, and unconditional lower bounds.** Murray and Williams [29] showed that MCSP and MKTP are not hard for \(\text{TC}^0\) under so-called \textit{local} reductions computable in time less than \(\sqrt{n}\) – and thus in particular they are not hard under \(\text{NC}^0\) reductions that are very uniform (i.e., there is no routine computable in time \(t(n) < n^{5-\epsilon}\) that, on input \((n, i)\) outputs the \(O(1)\) queries upon which the \(i\)-th output bit
of such an $\text{NC}^0$ circuit depends). Murray and Williams speculated that this might be a promising first step toward showing that $\text{MCSP}$ is not hard for $\text{NP}$ under $\text{Dlogtime-uniform AC}^0$ reductions, since it follows from [1] that any set that is hard for $\text{TC}^0$ under $\text{P-uniform AC}^0$ reductions is also hard for $\text{TC}^0$ under $\text{P-uniform NC}^0$ reductions. Indeed, the results of Murray and Williams led us to expect that $\text{MCSP}$ and $\text{MKTP}$ are not even hard for $\text{PARITY}$ under non-uniform $\text{NC}^0$ reductions.

Contrary to these expectations, we show that $\text{MKTP}$ is hard not only for $\text{TC}^0$ but even for the complexity class $\text{DET}$ under non-uniform $\text{NC}^0$ reductions (Theorem 13). Consequently, $\text{MKTP}$ is not in $\text{AC}^0[p]$ for any prime $p$.\footnote{Subsequent to our work, a stronger average-case lower bound against $\text{AC}^0[p]$ was proved [19]. The techniques of [19] do not show how to reduce $\text{DET}$, or even smaller classes such as $\text{TC}^0$, to $\text{MKTP}$. Thus our work is incomparable to [19].} Note that it is still not known whether $\text{MCSP}$ or $R_{\text{KT}} = \{x : \text{KT}(x) \geq |x|\}$ is in $\text{AC}^0[p]$. It is known\footnote{Somewhat remarkably, Oliveira and Santhanam [31] have independently shown that $\text{MCSP}$ and $\text{MKTP}$ are hard for $\text{DET}$ under non-uniform $\leq^r_{\text{NC}^0}$ reductions. Their proof relies on self-reducibility properties of the determinant, whereas our proof relies on the fact that Graph Isomorphism is hard for $\text{DET}$ [39]. Their results have the advantage that they apply to $\text{MCSP}$ rather than merely to $\text{MKTP}$, but because it is not known whether $\text{TC}^0 = \text{P}$ they do not obtain unconditional lower bounds, as in Corollary 14.} that neither of these problems is in $\text{AC}^0$. Under a plausible derandomization hypothesis, this non-uniform reduction can be converted into a logspace-uniform $\leq^\text{AC}^0_{\text{tti}}$ reduction that is an AND of $\text{NC}^0$-computable queries. Thus “local” reductions are more effective for reductions to $\text{MKTP}$ than may have been suspected.

Implications among hardness conditions for $\text{MKTP}$ and $\text{MCSP}$. No $\leq^\text{P}_{\text{tt}}$ reductions are known between $\text{MKTP}^A$ or $\text{MCSP}^A$ for any $A$. Although most previous complexity results for one of the problems have applied immediately to the other, via essentially the same proof, there has not been any proven relationship among the problems. For the first time, we show for one of the problems have applied immediately to the other, via essentially the same proof, that all of the then-known reductions to $\text{MCSP}$ or $\text{MKTP}$ are hard for $\text{C}$ under $\leq$ also show that $\text{MCSP}^A$ ($\text{MKTP}^A$) is also hard for $\text{C}$, for every $A$. In addition, they showed an inherent limitation of oracle-independent proofs: They showed that oracle-independent $\leq^\text{P}_{\text{tt}}$-reductions cannot show hardness for any class larger than $\text{P}$.

This motivates the search for reductions that are not oracle-independent. We give a concrete example of a logspace-uniform $\leq^\text{AC}^0_{\text{tti}}$ reduction that (under a plausible complexity assumption) reduces $\text{DET}$ to $\text{MKTP}$. This is not an oracle independent reduction, since $\text{MKTP}^\text{QBF}$ is not hard for $\text{DET}$ under this same class of reductions (Corollary 19).

A clearer picture of how hardness “evolves”. It is instructive to contrast the evolution of the class of problems reducible to $\text{MKTP}^A$ under different types of reductions, as $A$ varies from very easy ($A = \emptyset$) to complex ($A = \text{QBF}$). For this thought experiment, we assume the very plausible hypothesis that $\text{DSPACE}(n) \not\subseteq \text{io-SIZE}(2^{cn})$. Restrictions of $\text{QBF}$ give a useful parameterization for the complexity of $A$. Consider $A$ varying from being complete for each level of $\text{PH}$ (that is, quantified Boolean formulas with $O(1)$ alternations between $\forall$ and $\exists$ quantifiers), to instances of $\text{QBF}$ with log$^\epsilon n$ alternations, then to $O(\log n)$ alternations etc., through to $2^{\log n}$ alternations, and so on, until finally $A = \text{QBF}$. Since $\text{DSPACE}(n) \subseteq \text{P}^\text{QBF}/\text{poly}$, at some point in this evolution we have $\text{DSPACE}(n) \subseteq \text{io-SIZE}^A(2^{cn})$: it is plausible to assume that this doesn’t happen until $A$ has at least log$ n$ quantifier alternations, or more.

At all stages in this evolution $\text{SZK} \subseteq \text{BPP}^\text{MKTP}^A$ [5], until at some point $\text{BPP}^\text{MKTP}^A$
expands to coincide with PSPACE [4]. Also, at all stages in this evolution \(\text{DET} \leq_m^{NC^0} \text{reduces to MKTP}^A\). No larger class is known to \(\leq_m^{NC^0} \text{reduce to MKTP}^A\); even when \(A = \text{QBF}\) we do not know, for instance, if \(\text{NC}^1 \leq_m^{NC^0} \text{reduces to MKTP}^A\). Thus these reductions behave “monotonically”, in the sense that as the complexity of \(A\) increases, the class of problems reducible to \(\text{MKTP}^A\) does not shrink noticeably, and sometimes appears to grow markedly.

The situation is much more intriguing when we consider the uniform class of \(\leq_T^{NC^0}\) reductions that arise from derandomizing the nonuniform \(\leq_m^{NC^0}\) reductions from \(\text{DET}\). At the start, when \(A = \emptyset\), we have \(\text{DET}\) reducing to \(\text{MKTP}^A\), and this is maintained until \(A\) becomes complex enough so that \(\text{DSPACE}(n) \subseteq \text{io-SIZE}^A(2^n)\). At this point, not only does \(\text{DET}\) not reduce to \(\text{MKTP}^A\), but neither does \(\text{PARITY}\) ! (See Theorem 17.)

This helps place the results of [7] in the proper context. In [7] strong evidence was presented against \(\text{MCSP}^{\text{QBF}}\) being hard for \(P\) under \(\leq_L^m\) reductions, and this was taken as indirect evidence that \(\text{MCSP}\) itself should not be hard for \(P\), since \(\text{MCSP} \in \text{NP}\) and thus is much “easier” than the PSPACE-complete problem \(\text{MCSP}^{\text{QBF}}\). However, we expect that \(\text{MCSP}^A\) and \(\text{MKTP}^A\) should behave somewhat similarly to each other, and it can happen that a class can reduce to \(\text{MKTP}\) (Theorem 15) and \(\text{not reduce to MKTP}^A\) for a more powerful oracle \(A\) (Corollary 19).

**Hardness of the Gap problem.** Our new hardness results for \(\text{MKTP}^A\) share with earlier reductions the property that they hold even for “gap” versions of the problem. That is, for some \(\epsilon > 0\), the reduction works correctly for any solution to the promise problem with “yes” instances \(\{(x, s) : \text{KT}^A(x) \leq s\}\) and “no” instances \(\{(x, s) : \text{KT}^A(x) > s + \|x\|^\epsilon\}\). However, we do not know if they carry over to instances with a wider “gap” between the Yes and No instances; earlier hardness results such as those of [4, 9, 5, 36] hold for a much wider gap (such as with the Yes instances having \(\text{KT}(x) < |x|^\epsilon\), and the no instances with \(\text{KT}(x) \geq |x|\)), and this is one reason why they applied both to \(\text{MKTP}\) and to \(\text{MCSP}\). Thus there is interest in whether it is possible to reduce \(\text{MCSP}\) with small “gap” to \(\text{MCSP}\) with large “gap”. If this were possible, then \(\text{MCSP}\) and \(\text{MKTP}\) would be interreducible in some sense.

Earlier work [7] had presented unconditional results, showing that “gap” versions of \(\text{MCSP}\) could not be hard for \(\text{TC}^0\) under \(\leq_{AC^0}^m\) reductions, unless those reductions had large “stretch” (mapping short inputs to long outputs). In Section 4, we show that \(BPP\)-Turing reductions among gap \(\text{MCSP}\) problems require large stretch, unless \(\text{MCSP} \in \text{BPP}\).

**Natural \(\text{NP}\)-intermediate Problems.** In Section 3 we also consider gap \(\text{MCSP}\) problems where the “gap” is quite large (i.e., problems of approximating the minimum circuit size for a truth table of size \(n\) within a factor of \(n^{1-o(1)}\)). Problems of this sort are of interest, because of the role they play in the natural proofs framework of [34], if one is trying to prove circuit lower bounds of size \(2^{o(n)}\). Our Theorem 6 shows that these problems are \(\text{NP}\)-intermediate in the sense that these do not lie in \(\text{P}/\text{poly}\) and are not \(\text{NP}\)-hard under \(\text{P}/\text{poly}\) reductions, under modest cryptographic assumptions (weaker than assuming that factoring or discrete log requires superpolynomial-size circuits, or assuming the existence of a one-way function). To the best of our knowledge, these problems are the first natural \(\text{NP}\)-intermediate problems under the existence of an arbitrary one-way function.

Our new insight on \(\text{MCSP}\) here is that, if the gap problems are \(\text{NP}\)-hard, then \(\text{MCSP}\) is “strongly downward self-reducible”: that is, any instance of \(\text{MCSP}\) of size \(n\) can be reduced to instances of size \(n^\epsilon\). In the past, many natural problems have been shown to be strongly downward self-reducible (see [8]); Our contribution is to show that \(\text{MCSP}\) also has such a property (under the assumption that the gap \(\text{MCSP}\) problems are \(\text{NP}\)-hard). In fact, we also present a similar argument showing that a \(n^{1-o(1)}\) approximation for \(\text{CLIQUE}\) is
NP-intermediate if NP \not\subseteq P/poly.

2 Preliminaries

We assume the reader is familiar with standard DTIME and DSPACE classes. We also occasionally refer to classes defined by time-bounded alternating Turing machines: \(\text{ATIME}(t(n))\), or by simultaneously bounding time and the number of alternations between existential and universal configurations: \(\text{ATIME-ALT}(t(n), a(n))\).

We refer the reader to the text by Vollmer [42] for background and more complete definitions of the standard circuit complexity complexity classes

\[\text{NC}^0 \subset \text{AC}^0 \subset \text{AC}^0[p] \subset \text{TC}^0 \subset \text{NC}^1 \subseteq \text{P}/\text{poly},\]

as well as the standard complexity classes \(L \subseteq P \subseteq \text{NP} \subseteq \text{PH} \subseteq \text{PSPACE}\). Between \(L\) and \(P\) in this list, there is one more class that plays an important role for us: DET is the class of problems that are reducible to the problem of computing the determinant of integer matrices, by \(\text{NC}^1\)-Turing reductions.

This brings us to the topic of reducibility. Let \(\mathcal{C}\) be either a class of functions or a class of circuits. We say that \(A \leq_{\text{m}}^\mathcal{C} B\) 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 \(\leq_{\text{m}}^\text{TC}^0\), \(\leq_{\text{m}}^\text{NC}^0\), and \(\leq_{\text{nc}}^\text{TC}^0\) reducibility. 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 \(A \leq_{\text{T}}^\mathcal{C} B\) 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 \(\leq_{\text{T}}^{\text{P/poly}}\), \(\leq_{\text{T}}^{\text{BPP}}\), \(\leq_{\text{T}}^{\text{D}}\), \(\leq_{\text{T}}^{\text{AC}^0}\) and \(\leq_{\text{nc}}^{\text{TC}^0}\) reducibility; instead of writing \(A \leq_{\text{T}}^{\text{P/poly}} B\) or \(A \leq_{\text{T}}^{\text{BPP}} B\), we will more frequently write \(A \in \text{P}^B/\text{poly}\) or \(A \in \text{BPP}^B\). 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 \(\leq_{\text{tt}}^{\text{AC}^0}\) and \(\leq_{\text{tt}}^{\text{TC}^0}\) reducibility.

Kabanets and Cai [25] sparked renewed interest in \(\text{MCSP}\) and highlighted connections between \(\text{MCSP}\) and more recent progress in derandomization. They introduced a class of reductions to \(\text{MCSP}\), which they called natural reductions. Recall that instances of \(\text{MCSP}\) are of the form \((T, s)\) where \(s\) is a “size parameter”. A \(\leq_{\text{m}}^p\) reduction \(f\) is called natural if \(f(x)\) is of the form \(f(x) = (f_1(x), f_2(|x|))\). That is, the “size parameter” is the same, for all inputs \(x\) of the same length.

The notation \(\text{io-SIZE}(s(n))\) denotes the class of all languages \(A\) such that, for infinitely many lengths \(n\), there is a circuit of size at most \(s(n)\) accepting exactly the strings of length \(n\) in \(A\). (Although this definition can depend upon the precise notion of “circuit size” being considered, every statement that we make using this notation holds using any reasonable notion of “size”.) If \(B\) is a language, then \(\text{io-SIZE}^B(s(n))\) denotes the class of all languages \(A\) such that, for infinitely many lengths \(n\), there is an “oracle circuit” (that is, a circuit that has “oracle gates” in addition to the standard Boolean gates) of size at most \(s(n)\) accepting exactly the strings of length \(n\) in \(A\), when given \(B\) as an oracle.

Whenever circuit families are discussed (either when defining complexity classes, or reducibilities), one needs to deal with the issue of uniformity. For example, the class \(\text{AC}^0\) (corresponding to families \(\{C_n : n \in \mathbb{N}\}\) of unbounded fan-in AND, OR, and NOT gates having size \(n^{O(1)}\) and depth \(O(1)\)) comes in various flavors, depending on the complexity of computing the mapping \(1^n \mapsto C_n\). When this is computable in polynomial time (or
logarithmic space), then one obtains P-uniform AC$^0$ (logspace-uniform AC$^0$, respectively). If no restriction at all is imposed, then one obtains non-uniform AC$^0$. As discussed in [42], the more restrictive notion of Dlogtime-uniform AC$^0$ is frequently considered to be the “right” notion of uniformity to use when discussing small complexity classes such as AC$^0$, AC$^0[p]$ and TC$^0$. If these classes are mentioned with no explicit mention of uniformity, then Dlogtime-uniformity is intended. For uniform NC$^1$ the situation is somewhat more complicated, as discussed in [42]; there is wide agreement that the “correct” definition coincides with ATIME$(O(\log n))$.

There are many ways to define time-bounded Kolmogorov complexity. The definition KT$(x)$ was proposed in [4], and has the advantage that it is polynomially-related to circuit size (when a string $x$ is viewed as the truth-table of a function). KT$(x)$ is the minimum, over all $d$ and $t$, of $|d|+t$, such that the universal Turing machine $U$, on input $(d, i, b)$ can determine in time $t$ if the $i$-th bit of $x$ is $b$. (More formal definitions can be found in [4].)

A promise problem consists of a pair of disjoint subsets $(Y, N)$. A language $A$ is a solution to the promise problem $(Y, N)$ if $Y \subseteq A \subseteq \overline{N}$. A language $B$ reduces to a promise problem via a type of reducibility $\leq_r$ if $B \leq_r A$ for every set $A$ that is a solution to the promise problem.

### 3 GapMCSP

In this section, we consider the “gap” versions of MCSP and MKTP. We focus primarily on MCSP, and for simplicity of exposition we consider the “size” of a circuit to be the number of AND and OR gates of fan-in two. (NOT gates are “free”). The arguments can be adjusted to consider other circuit models and other reasonable measures of “size” as well. Given a truth-table $T$, let $CC(T)$ be the size of the smallest circuit computing $T$, using this notion of “size”.

**Definition 1.** For any function $\epsilon : \mathbb{N} \to (0, 1)$, let Gap$_{MCSP}$ be the approximation problem that, given a truth-table $T$, asks for outputting a value $f(T) \in \mathbb{N}$ such that

$$CC(T) \leq f(T) \leq |T|^{1-\epsilon(|T|)} \cdot CC(T).$$

Note that this approximation problem can be formulated as the following promise problem. (See also [14] for similar comments.)

**Fact 2.** Gap$_{MCSP}$ is polynomial-time Turing equivalent to the following promise problem $(Y, N)$:

$$Y := \{ (T, s) \mid CC(T) < s/|T|^{1-\epsilon(|T|)} \},$$

$$N := \{ (T, s) \mid CC(T) > s-1 \},$$

where $T$ is a truth-table and $s \in \mathbb{N}$.

**Proof.** Given a solution $A$ of Gap$_{MCSP}$, one can compute an approximation $f(T)$ of CC$(T)$ as follows:

$$f(T) := \max\{ s \in \mathbb{N} \mid (T, s) \not\in A \}$$

We claim that $f(T)$ satisfies the approximation guarantee as given in Definition 1. By the definition of $f(T)$, we have $(T, f(T)) \not\in A$, which implies that $(T, f(T)) \not\in Y$, and thus $CC(T) \geq f(T)/|T|^{1-\epsilon(|T|)}$. Similarly, by the definition of $f(T)$, we have $(T, f(T) + 1) \in A$.
which implies that \((T, f(T) + 1) \notin \mathbb{N}\), and thus \(\text{CC}(T) \leq f(T)\). To summarize, we have \(\text{CC}(T) \leq f(T) \leq |T|^{1 - \epsilon(T)}\). CC(T) and thus \(f(T)\) satisfies Definition 1.

On the other hand, suppose that an approximation \(f(T)\) of CC(T) is given. We can define a solution \(A\) of \(\text{Gap}_{\text{MCSP}}\) as \(A := \{ (T, s) \mid f(T) < s \}\). We claim that \(A\) indeed satisfies the promise of \(\text{Gap}_{\text{MCSP}}\). If \((T, s) \in Y\), then \(f(T) \leq |T|^{1 - \epsilon(T)} \cdot \text{CC}(T) < s\) and therefore \((T, s) \in A\). On the other hand, if \((T, s) \in N\), then \(f(T) \geq \text{CC}(T) > s - 1\), which implies \((T, s) \notin A\).

Note that \(\text{Gap}_{\text{MCSP}}\) becomes easier when \(\epsilon\) becomes smaller. If \(\epsilon(n) = o(1)\), then (using the promise problem formulation) it is easy to see that \(\text{Gap}_{\text{MCSP}}\) has a solution in \(\text{DTIME}(2^{\mathcal{O}(n)})\), since the Yes instances have witnesses of length \(|T|^{o(1)}\). However, it is worth emphasizing that, even when \(\epsilon(n) = o(1)\), \(\text{Gap}_{\text{MCSP}}\) is a canonical example of a combinatorial property that is useful in proving circuit size lower bounds of size \(2^{o(n)}\), in the sense of [34]. Thus it is of interest that \(\text{MCSP}\) cannot reduce to \(\text{Gap}_{\text{MCSP}}\) in this regime under very general notions of reducibility, unless \(\text{MCSP}\) itself is easy.

**Theorem 3.** For any polynomial-time-computable nonincreasing \(\epsilon(n) = o(1)\), if \(\text{MCSP} \in \text{BPP}_{\text{Gap}_{\text{MCSP}}}\), then \(\text{MCSP} \in \text{BPP}\).

A new idea is that the \(\text{Gap}_{\text{MCSP}}\) is “strongly downward self-reducible.” We will show that any \(\text{Gap}_{\text{MCSP}}\) instance of length \(n\) is reducible to \(n^{1 - \epsilon}\) \(\text{MCSP}\) instances of length \(n^\epsilon\). To this end, we will exploit the following simple fact.

**Lemma 4.** For a function \(f : \{0, 1\}^n \to \{0, 1\}\), a string \(x \in \{0, 1\}^k\) and \(k \in \mathbb{N}\), let \(f_x : \{0, 1\}^{n-k} \to \{0, 1\}\) be a function defined as \(f_x(y) := f(x, y)\). Then, the following holds:

\[
\max_{x \in \{0, 1\}^k} \text{CC}(f_x) \leq \text{CC}(f) \leq 2^k \cdot \left( \max_{x \in \{0, 1\}^k} \text{CC}(f_x) + 3 \right),
\]

(In other words, \(\max_{x \in \{0, 1\}^k} \text{CC}(f_x)\) gives an approximation of \(\text{CC}(f)\) within a factor of \(2^k\).)

**Proof.** We first claim that \(\max_{x \in \{0, 1\}^k} \text{CC}(f_x) \leq \text{CC}(f)\). Indeed, let \(C\) be a minimum circuit that computes \(f\) and \(x\) be an arbitrary string of length \(k\). For each \(x \in \{0, 1\}^k\), define a circuit \(C_x\) as \(C_x(y) := C(x, y)\) on input \(y \in \{0, 1\}^{n-k}\). Then, since \(C_x\) computes \(f_x\) and the size of \(C_x\) is at most that of \(C\), we have \(\text{CC}(f_x) \leq \text{CC}(f)\).

Next, we claim that \(\text{CC}(f) \leq 2^k \cdot \left( \max_{x \in \{0, 1\}^k} \text{CC}(f_x) + O(1) \right)\). For any \(x \in \{0, 1\}^k\), let \(C_x\) be a minimum circuit that computes \(f_x\). We build a circuit that computes \(f := f_x\) recursively as follows: \(f_z(x, y) = (\neg x_1 \land f_{z0}(x_2, \ldots, x_k, y)) \lor (x_1 \land f_{z1}(x_2, \ldots, x_k, y))\) for any string \(z\) of length less than \(k\), and \(f_x(y) = C_x(y)\) for any \(x \in \{0, 1\}^k\). Since \(\text{CC}(f_x) \leq \text{CC}(f_{z0}) + \text{CC}(f_{z1}) + 3\) we obtain

\[
\text{CC}(f) \leq \sum_{x \in \{0, 1\}^k} C_x(y) + 3 \cdot (2^k - 1)
\]

\[
< 2^k \cdot \left( \max_{x \in \{0, 1\}^k} \text{CC}(f_x) + 3 \right).
\]

**Proof of Theorem 3.** Let \(M\) be an oracle \(\text{BPP}\) Turing machine which reduces \(\text{MCSP}\) to \(\text{Gap}_{\text{MCSP}}\). Let \(|T|^c\) be an upper bound for the running time of \(M\), given a truth-table \(T\), and let \(|T| = 2^n\).

We recursively compute the circuit complexity of \(T\) by the following procedure: Run \(M\) on input \(T\). If \(M\) makes a query \(S\) to the \(\text{Gap}_{\text{MCSP}}\) oracle, then divide \(S\) into
consecutive substrings $S_1, \ldots, S_{2k}$ of length $|S| \cdot 2^{-k}$ such that $S_1 \cdot S_2 \cdots S_{2k} = S$ (where $k$ is a parameter, chosen later, that depends on $|S|$), and compute the circuit complexity of each $S_i$ recursively for each $i \in [2^k]$. Then continue the simulation of $M$, using the value $2^k \cdot (\max_{i \in [2^k]} \text{CC}(S_i) + 3)$ as an approximation to $\text{CC}(S)$.

We claim that the procedure above gives the correct answer. For simplicity, let us first assume that the machine $M$ has zero error probability. It suffices to claim that the simulation of $M$ is correct in the sense that every query of $M$ is answered with a value that satisfies the approximation criteria of $\text{Gap}_{\text{MCSP}}$. Suppose that $M$ makes a query $S$. By the assumption on the running time of $M$, we have $|S| \leq |T|^c = 2^{n \epsilon}$. By Lemma 4, we have

$$\text{CC}(S) \leq 2^k \cdot \left( \max_{i \in [2^k]} \text{CC}(S_i) + 3 \right) \leq 2^k \cdot (\text{CC}(S) + 3).$$

In particular, the estimated value satisfies the promise of $\text{Gap}_{\text{MCSP}}$ if $2^k \cdot (\text{CC}(S) + 3) \leq |S|^{1-\epsilon(|S|)} \cdot \text{CC}(S)$. Since we may assume without loss of generality that $\text{CC}(S) \geq 3$, it suffices to make sure that $2^{k+1} \cdot \text{CC}(S) \leq |S|^{1-\epsilon(|S|)} \cdot \text{CC}(S)$. Let $|S| = 2^m$. Then, in order to satisfy $k + 1 \leq (1 - \epsilon(|S|)) \cdot m$, let us define $k := (1 - \epsilon(|S|)) \cdot m - 1$. For this particular choice of $k$, the estimated value $2^k \cdot (\max_{i \in [2^k]} \text{CC}(S_i) + 3)$ of the circuit complexity of $S$ satisfies the promise of $\text{Gap}_{\text{MCSP}}$, which implies that the reduction $M$ computes the correct answer for $\text{MCSP}$.

Now we analyze the time complexity of the algorithm. Each recursive step makes at most $2^{cn}$ many recursive calls, because there are potentially $2^{cn}$ many queries $S$ of $M$, each of which may produce at most $2^k \leq 2^{cn}$ recursive calls. The length of each truth-table $S_i$ that arises in one of the recursive calls is $|S_i| = |S| \cdot 2^{-k} = 2^{m-k} = 2^{\epsilon(|S|) \cdot m + 1}$. We claim that $|S_i| \leq 2^{1+(n/2)}$ holds for sufficiently large $n$. Let us take $n$ to be large enough so that $\epsilon(2n/2) \leq 1/2c$. If $m \geq n/2$, then $|S_i| \leq 2^{(2^m) \cdot m + 1} \leq 2^{(2^{n/2}) \cdot cn + 1} \leq 2^{1+(n/2)}$. Otherwise, since $m \leq n/2$ and $\epsilon(|S|) < 1$, we obtain $|S_i| \leq 2^{\epsilon(|S|) \cdot m + 1} \leq 2^{1+(n/2)}$. Therefore, on inputs of length $2^n$, each recursive call produces instances of length at most $2^{1+(n/2)}$. The overall time complexity can be estimated as $2^{cn} \cdot 2^{c n/2} \cdot 2^{c n/4} \cdots = 2^{2c n}$ for some constant $c'$ (say, $c' = 3c$), which is a polynomial in the input length $2^n$.

We note that the analysis above works even for randomized reductions that may err with exponentially small probability. Since we have proved that the algorithm runs in polynomial time, the probability that the algorithm makes an error is at most a polynomial times an exponentially small probability, which is still exponentially small probability (by the union bound).

**Remark.** If we drop the assumption that $\epsilon(n)$ be computable, then the proof of Theorem 3 still shows that if $\text{MCSP} \in \text{P}^{\text{Gap}_{\text{MCSP}} / \text{poly}}$ then $\text{MCSP} \in \text{P} / \text{poly}$.

**Corollary 5.** Let $\epsilon(n) = o(1)$. If $\text{Gap}_{\text{MCSP}}$ has no solution in $\text{P} / \text{poly}$ then $\text{Gap}_{\text{MCSP}}$ is not hard for $\text{NP}$ (or even for $\text{MCSP}$) under $\text{P} / \text{poly}$ reductions, and is thus $\text{NP}$-intermediate.

**Proof.** This is immediate from the preceding remark. If $\text{MCSP} \in \text{P}^{\text{Gap}_{\text{MCSP}} / \text{poly}}$ then $\text{MCSP} \in \text{P} / \text{poly}$, which in turn implies that $\text{Gap}_{\text{MCSP}}$ has a solution in $\text{P} / \text{poly}$.

In what follows, we show that the assumption of Corollary 5 is true under very modest cryptographic assumptions. It is known that, for any constant $\epsilon > 0$, $\text{Gap}_{\text{MCSP}}$ is $\text{SZK}$-hard under $\text{P} / \text{poly}$ reductions [5]. Here, we show that if $\text{SZK}$ is not in $\text{P} / \text{poly}$, then for some $\epsilon(n) = o(1)$, $\text{Gap}_{\text{MCSP}}$ has no solution in $\text{P} / \text{poly}$. In fact, we can prove something stronger: If auxiliary-input one-way functions exist, then $\text{Gap}_{\text{MCSP}}$ is not in $\text{P} / \text{poly}$. We now describe auxiliary-input one-way functions.
Usually, the existence of cryptographically-secure one-way functions is considered to be essential for meaningful cryptography. That is, one requires a function \( f \) computed in polynomial time such that, for any algorithm \( A \) computed by polynomial-sized circuits, \( \Pr_x[ f(A(f(x))) = f(x) ] = 1/n^ε(1) \) where \( x \) is chosen uniformly at random from \( \{0,1\}^n \). A weaker notion that has been studied in connection with \( \mathsf{SZK} \) goes by the name auxiliary-input one-way functions. This is an indexed family of functions \( f_y(x) = F(y, x) \), where \( |x| = p(|y|) \) for some polynomial \( p \), and \( F \) is computable in time polynomial in \( |y| \), such that for some infinite set \( I \), for any algorithm\(^3\) \( A \) computed by polynomial-sized circuits, for all \( y \in I \), \( \Pr_x[f_y(A(f_y(x))) = f_y(x)] = 1/n^ε(1) \) where \( n = |y| \) and \( x \) is chosen uniformly at random from \( \{0,1\}^p(n) \). It is known that there are promise problems in \( \mathsf{SZK} \) that have no solution in \( \mathsf{P/poly} \) only if auxiliary-input one-way functions exist. (This is due to \([33]\); a good exposition can be found in \([40, \text{Theorems 7.1 & 7.5}]\), based on earlier work of \([32]\).)

**Theorem 6.** If auxiliary-input one-way functions exist, then there is a function \( ε(n) = o(1) \) such that \( \text{Gap}_n \mathsf{MCSP} \) is \( \mathsf{NP} \)-intermediate. (Namely, \( \text{Gap}_n \mathsf{MCSP} \) has no solution in \( \mathsf{P/poly} \) and \( \text{Gap}_n \mathsf{MCSP} \) is not \( \mathsf{NP} \)-hard under \( \leq_{\mathsf{P/poly}} \) reductions.)

**Remark.** In particular, either one of the following implies that some \( \text{Gap}_n \mathsf{MCSP} \) is \( \mathsf{NP} \)-intermediate, since each implies the existence of auxiliary-input one-way functions:

1. The existence of cryptographically-secure one-way functions.
2. \( \mathsf{SZK} \) is not in \( \mathsf{P/poly} \).

**Proof.** Let \( F(y, x) \) define an auxiliary-input one-way family of functions \( f_y(x) \) where \( |x| = p(|y|) \) for some polynomial \( p \). Let \( S(n) \) be the size of the smallest circuit such that for some \( y \) of length \( n \), \( \Pr_x[f_y(A(f_y(x))) = f_y(x)] \geq 1/S(n) \) where \( n = |y| \) and \( x \) is chosen uniformly at random from \( \{0,1\}^p(n) \). By assumption \( S(n) \) is not bounded by any polynomial. Let \( ε(n) \) be a nondecreasing unbounded function such that \( n^{c_0ε(n^{c_0})} < S(n) \) for infinitely many \( n \), where \( c_0 \) is a constant that we will pick later.

At this point, we make use of some standard derandomization tools, including the \( \mathsf{HILL} \) pseudorandom generator \([18]\), and pseudorandom function generators \([15, 34]\). First, we recall the \( \mathsf{HILL} \) construction, phrased in terms of non-uniform adversaries:

**Theorem 7** (see \([18]\)). Let \( F(y, x) \) be computable uniformly in time polynomial in \( |y| \), and let \( µ : \mathbb{N} \to [0,1] \). For any oracle \( L \) and any oracle circuit \( M \) of size \( s(n) \), there is a size \( (s(n)^O(1)/µ(n^{O(1)})) \) circuit \( N \) such that the following holds for any \( n \) and \( y \): If

\[
\Pr_{[r]=2n}[M^L(y,r)=1] - \Pr_{[x]=n}[M^L(y,G^\mathsf{HILL}_{f_y}(x))=1] \geq µ(n),
\]

then

\[
\Pr_{[x]=n}[F(y,N^L(y,F(y,x)))=F(y,x)] \geq µ(n^{O(1)}/n^{O(1)}),
\]

where \( r \) and \( x \) are chosen uniformly at random. Here \( G^\mathsf{HILL}_{f_y} \) is a pseudorandom generator, where \( G^\mathsf{HILL}_{f_y}(x) \) is computable in time polynomial in \( |y| \), as described in \([18]\).

Theorem 7 states that if there exists a distinguisher with access to an oracle \( L \) that distinguishes the output of \( G^\mathsf{HILL}_{f_y} \) from the uniform distribution, then oracle access to \( L \) suffices to invert \( f_y \) on a significant fraction of the inputs. We now argue that such a distinguisher

\(^3\) We have chosen to define one-way functions in terms of security against non-uniform adversaries. It is also common to use the weaker notion of security against probabilistic polynomial-time adversaries, as in \([40]\).
can be computed by a circuit of size $n^{O(e(n))}$ with oracle gates for \textsc{Gap}_{1/\varepsilon(n)}\textsc{MCSP}, where $e(n)$ is the slow-growing function that we defined earlier.

Let $G : \{0, 1\}^n \rightarrow \{0, 1\}^{2n}$ be a pseudorandom generator mapping strings of length $n$ to strings of length $2n$, constructed from the generator $G_{f_y}^{\text{HILL}}$. Furthermore, let $G_0(x)$ be the first $n$ bits of $G(x)$, and let $G_1(x)$ be the second $n$ bits of $G(x)$, so that $G(x) = G_0(x)G_1(x)$. We now make use of the pseudorandom function generator of Razborov and Rudich [34], with the following parameters.

For any string $w$ of length $k$, let $G_w(x) : \{0, 1\}^n \rightarrow \{0, 1\}^n$ be defined as $G_w(x) = G_{w_1}(G_{w_2}(...(G_{w_n}(x)))...)$, Define $G'_y(x, w)$ to be the first bit of $G_w(x)$, where here the subscript $y$ refers back to the fact that $G$ is defined from $G_{f_y}^{\text{HILL}}$.

Now let $z(x)$ be the truth table of $G'_y(x, w)$ (viewed as a function of $w$). Since $|w| = k$, $|z(x)| = 2^k$. Since $G'_y$ is computed in time polynomial in the length of $x$ and $w$, $\text{CC}(z(x)) < (n + k)^c$ for some constant $c$.

Now, let us choose $k$ to be $(c + 1)e(n) \log n$. It follows that $\text{CC}(z(x)) < (n + (c + 1)e(n) \log n)^c < n^c+1 = (2^{(c+1)e(n) \log n})^{1/\varepsilon(n)} = |z(x)|^{1/\varepsilon(n)}$. That is, from the pseudorandom distribution, we always have $\text{CC}(z(x)) < |z(x)|^{1/\varepsilon(n)}$, whereas a random string has CC complexity at least roughly equal to the length of the string with high probability.

Thus, an oracle gate for any oracle that satisfies the $\text{Gap}_{1/\varepsilon(n)}\textsc{MCSP}$ promise problem can distinguish random functions from the output of the pseudorandom function generator. And [34] shows how to obtain a circuit $L$ of size $n^{O(e(n))}$ such that

$$\left| \Pr_{|y|=2n} [M_L(y, r) = 1] - \Pr_{|x|=n} [M_L(y, G_{f_y}^{\text{HILL}}(x)) = 1] \right| \geq 1/n^{e(n)}.$$ 

By Theorem 7, there are constants $c_1, c_2, c_3, c_4$ and there is a circuit $N$ of size $n^{-c_3\varepsilon(n^2)}$ such that the following holds for any $n$ and $y$:

$$\Pr_{|x|=n} [F(y, N_L(y, F(y, x))) = F(y, x)] \geq n^{-c_3\varepsilon(n^2)}$$

where $x$ is chosen uniformly at random.

Now if we pick $c_0$ to be greater than $\max\{c_1, c_2, c_3, c_4\}$, it follows that $N$ is a circuit of size less than $S(n)$ that inverts $f_y(x)$ with probability greater than $1/S(n)$, contrary to the definition of $S$.

This establishes that no solution to the $\text{Gap}_{1/\varepsilon(n)}\textsc{MCSP}$ promise problem lies in $\text{P/poly}$. By Corollary 5, $\text{Gap}_{1/\varepsilon(n)}\textsc{MCSP}$ is NP-intermediate.

\textbf{Remark.} Observe that Theorem 6 can also be rephrased in terms of \textit{uniform} probabilistic adversaries, if we assume that the one-way functions require time $n^{\varepsilon(n)}$ to invert, for some easy-to-compute function $\varepsilon$.

### 3.1 Other NP-intermediate problems

Although our focus is primarily on \textsc{MCSP}, we observe here that the strongly downward self-reducibility property that we exploited above is fairly common. For instance, it has been noticed previously that \textsc{CLIQUE} also has this property [38, 8]. It appears to be a new observation, however, that this property yields a natural NP-intermediate optimization problem.

\textbf{Definition 8.} For any function $\varepsilon : \mathbb{N} \rightarrow (0, 1)$, let $\text{Gap}_{\varepsilon}\textsc{CLIQUE}$ be the approximation problem that, given an $n$-vertex graph $G$, asks for outputting a value $f(G) \in \mathbb{N}$ such that

$$\omega(G) \leq f(G) \leq n^{1-\varepsilon(n)} \cdot \omega(G).$$
Here, as usual $\omega(G)$ denotes the clique number of $G$: the size of the largest clique in $G$.

\begin{theorem}
NP \not\subseteq P/poly if and only if there is an $\epsilon(n) = o(1)$ such that Gap,$\text{CLIQUE}$ has no solution in $P/poly$ and is not hard for NP under $\leq^T_{P/poly}$ reductions.
\end{theorem}

**Proof.** Assume NP \not\subseteq P/poly. Define $\epsilon(n)$ to be the least $\epsilon$ such that, for all $m \geq n$, there is a circuit of size $n^\epsilon$ that computes a function $f(G)$ (for $m$-vertex graphs $G$) such that $\omega(G) \leq f(G) \leq m^{1-1/\epsilon} \cdot \omega(G)$. If $\epsilon(n) = O(1)$, it follows from [17] that CLIQUE \in P/poly, contrary to assumption. Thus $\epsilon(n) = \omega(1)$.

Let $\epsilon = \epsilon(n) = 1/\epsilon(n)$; thus $\epsilon(n) = o(1)$. It follows immediately from the definition of $\epsilon(n)$ that Gap,$\text{CLIQUE}$ has no solution in $P/poly$.

If we partition the vertices of an $n$-node graph $G$ into $n^{1-\epsilon}$ parts $V_1, \ldots, V_{n^{1-\epsilon}}$ of size at most $\lfloor n^\epsilon \rfloor$, then $\omega(G) \leq (n^{1-\epsilon}) \cdot \max_i \omega(G_i)$, where $G_i$ is the induced subgraph of $G$ with vertices in $V_i$. (See [38, 8] for other applications of this observation.)

Now, precisely as in the proof of Theorem 3, it follows that if CLIQUE were $P/poly$-Turing reducible to Gap,$\text{CLIQUE}$, then CLIQUE \in P/poly, contrary to our assumption. This shows that Gap,$\text{CLIQUE}$ is not NP-hard under $P/poly$ reductions, and thus completes the “only if” direction of the Theorem. (The converse is trivial.)

\section{Reductions among GapMCSPs Require Large Stretch}

In the previous section, we studied Gap$_k$MCSP where $\epsilon(n) = o(1)$. In this section, we focus on the case where $\epsilon$ is a fixed positive constant.

In what follows, we say that a reduction from Gap$_k$MCSP to Gap$_l$MCSP has stretch $n^c$ if, on input $T$, the reduction makes queries of length at most $|T|^c$.

\begin{theorem}
Let $0 < \epsilon < \delta < 1$. If Gap$_k$MCSP is reducible to Gap$_l$MCSP via a randomized Turing reduction of stretch at most $n^c$ for some $c < \delta/\epsilon$, then Gap$_k$MCSP \in BPP.
\end{theorem}

**Proof.** The argument is almost identical to the argument in the preceding section. Given an input to Gap$_k$MCSP, simulate the reduction from Gap$_k$MCSP to Gap$_l$MCSP. As before, if the reduction makes a query $S$, then divide $S$ into consecutive substrings $S_1, \ldots, S_{2^k}$ of length $2^m-k$, where $m$ is defined as $|S| = 2^m$ and $k$ is a parameter chosen later depending on $m$. For each $i \in [2^k]$, recursively solve Gap$_l$MCSP on the instance $S_i$, and let $f(S_i)$ be the answer of the recursive call. Now, we estimate the circuit complexity of $S$ as $2^k \cdot (\max_{i \in [2^k]} f(S_i) + 3)$ and continue the simulation.

We claim the correctness of the simulation for a certain choice of parameter $k = k(m)$. Let $e$ denote the estimated circuit complexity of $S$, that is, $e := 2^k \cdot (\max_{i \in [2^k]} f(S_i) + 3)$. The goal is to show that $e$ satisfies the promise of Gap$_k$MCSP, or equivalently,

$$CC(S) \leq e \leq |S|^{1-\epsilon} \cdot CC(S). \tag{1}$$

We may assume that answers of recursive calls satisfy the promise of Gap$_k$MCSP by induction: that is, $CC(S_i) \leq f(S_i) \leq |S_i|^{1-\delta} \cdot CC(S_i)$. Thus, by Lemma 4, we have

$$e \geq 2^k \cdot \left( \max_{i \in [2^k]} CC(S_i) + 3 \right) \geq CC(S),$$

as required in the first inequality of (1). Now we turn to the second inequality of (1). We
may assume, without loss of generality, that \( e \leq 2^{k+1} \cdot \max_{i \in [2^k]} f(S_i) \). Therefore, we obtain

\[
e \leq 2^{k+1} \cdot \max_{i \in [2^k]} f(S_i)
\leq 2^{k+1} \cdot \max_{i \in [2^k]} |S_i|^{1-\delta} \cdot CC(S_i) \quad \text{(by the promise of Gap}_4\text{MCSP)}
= 2^{k+1}(m-k)(1-\delta) \cdot \max_{i \in [2^k]} CC(S_i)
\leq 2^{k+1}(m-k)(1-\delta) \cdot CC(S) \quad \text{(since } |S_i| = 2^{m-k} \text{)}
\leq |S|^{1-\epsilon} \cdot CC(S),
\]

where the last inequality holds if \( k+1+(m-k)(1-\delta) \leq m \cdot (1-\epsilon) \), that is, \( k \leq m - m\epsilon/\delta - 1/\delta \). Thus we define \( k := m - m\epsilon/\delta - 1/\delta \), which ensures the second inequality of (1).

Now we turn to analysis of the running time of the algorithm. Let \( 2^m \) be the length of the input to the algorithm. By the assumption on the stretch of the reduction, we have \( |S| \leq 2^{m\epsilon} \), that is, \( m \leq m\epsilon \). Therefore, \( |S_i| = 2^{m-k} = 2^{m\epsilon/\delta+1/\delta} \leq 2^{m\epsilon/\delta+1/\delta} \). Since \( \epsilon \delta < 1 \), the algorithm above runs in polynomial time. Indeed, let \( t(N) \) be an upper bound of the running time of the algorithm on inputs of length \( N \) and \( \rho := c\epsilon/\delta < 1 \). We have \( t(N) \leq N^{O(1)} t(N^\rho) \).

Solving this recursive inequality, we obtain \( t(N) = N^{O(1)} \). \( \diamond \)

## 5 Hardness for DET

In this section, we present some of our main contributions. We show that MKTP is hard for DET under \( \leq_m^{NC^0} \) reductions (Theorem 13); prior to this, no variant of MCSP has been shown to be hard for any complexity class under any type of many-one reducibility. The \( \leq_m^{NC^0} \) reduction that we present is nonuniform; we show that hardness under uniform reductions is closely related to lower bounds in circuit complexity, and in some cases we show that circuit lower bounds are equivalent to hardness results under uniform notions of reducibility (Theorem 17). These techniques allow us to prove the first results relating the complexity of MCSP\(^4\) and MKTP\(^4\) problems.

Here is the outline of this section. We will build on a randomized reduction of [6]: It is proved there that there is a ZPP reduction from the rigid\(^4\) graph isomorphism problem to MKTP. Here we modify that construction, to obtain a nonuniform AC\(^0\) reduction (Corollary 12). Combining Torán’s AC\(^0\) reduction [39] from DET to the rigid graph isomorphism as well as the Gap theorem [2], we will show \( DET \leq_m^{NC^0} MKTP \) (Theorem 13).

Next, we will establish that certain circuit size lower bounds are equivalent to the existence of certain uniform AC\(^0\) reductions to MKTP. This will be accomplished, by derandomizing the reduction of [6, Section 3.1]. Using this equivalence as a tool, we then close the section with a series of results presenting consequences of MKTP or MCSP being hard for various complexity classes, under different types of reducibility.

### 5.1 Hardness of MKTP under nonuniform many-one reductions

We now modify the ZPP reduction of [6]. As a first step, we present an “encoder” \( e \) mapping randomly-chosen binary strings to nearly-uniformly random permutations, along with an AC\(^0\) reduction \( f \) that will be central to our construction of a nonuniform AC\(^0\) reduction from the rigid graph isomorphism problem to MKTP:

\(^4\) A graph is rigid if it has no nontrivial automorphisms.
Lemma 11. Let $A$ be any oracle. There is a function $f$ computable in Dlogtime-uniform $\text{AC}^0$ and a function $e$ computable in Dlogtime-uniform $\text{TC}^0$ such that, for any two rigid graphs $G_0, G_1$ with $n$ vertices:

- $\Pr_r[f(G_0, G_1, e(r)) \not\in \text{MKTP}^A] > 1 - \frac{1}{2^{\nu n}}$ if $G_0 \not\equiv G_1$, and
- $\Pr_r[f(G_0, G_1, e(r)) \in \text{MKTP}^A] = 1$ if $G_0 \equiv G_1$.

Proof. We present the proof for $A = \emptyset$; however, it is immediate that the proof carries over for any oracle $A$. The function $f$ is given by the reduction presented in [6, Theorem 1], showing that the Rigid Graph Isomorphism Problem is in $\text{Promise-ZPP}^{\text{MKTP}}$. This reduction takes graphs $G_0$ and $G_1$ as input, and interprets the random coin flip sequence $r$ as a tuple $(w, \Pi)$ where $\Pi$ is a sequence of $t$ random permutations $\pi_1, \ldots, \pi_t$, and $|w| = t$. To the best of our knowledge, there is not any encoding of permutations such that both

- a random string of polynomial length can be viewed as encoding an approximately uniformly random permutation, and
- an $\text{AC}^0$ function can efficiently decode the permutation and apply it to the adjacency matrix of a graph.

To get around this, we will employ a $\text{TC}^0$-computable mapping $e$ from random strings to encodings of permutations. Such mappings have been used before (e.g., [3, 41]), but we provide a detailed exposition here for completeness.

First, note that a random string $s$ of length $n^{\ell'}(\ell' \log n)$ divided into blocks of length $\ell' \log n$ will contain at least $n$ blocks containing distinct entries, with probability $\geq 1 - 2^{-n^{\ell'}}$ (where $\ell'$ depends on $\ell'$).

Thus, with very high probability, a $\text{TC}^0$ routine can, on input $s$, output a sequence $((1, \sigma(1)), (2, \sigma(2)), \ldots, (n, \sigma(n)))$ with the property that $\sigma(i)$ is the contents of the $i$-th distinct block in $s$, and thus $\sigma$ is an injective map $\sigma : [n] \to [n^{\ell'}]$. Now a second $\text{TC}^0$-computable transformation can map $\sigma(i)$ to the number $j = \pi(i)$ such that $\sigma(i)$ is the $j$-th element in a sorted list of the elements $\{\sigma(1), \ldots, \sigma(n)\}$. In this way, a random string $s$ of length $n^{O(1)}$ yields a nearly-uniformly-random permutation $\pi = e(s)$, where $\pi$ is encoded as a sequence of pairs $(i, \pi(i))$, which is an encoding that is amenable to manipulation by $\text{AC}^0$ circuits. (With probability at most $1/2^{n^{\ell'}}$ the string $s$ will not encode a permutation, in which case we define $e(s)$ to be a string of zeros.) Thus the $\text{TC}^0$ function $e(r)$ in the statement of the theorem takes approximately $t + tn^{\ell'}(\ell' \log n)$ bits and produces a string $w$ of length $n$ (where $t$ is a suitably-large polynomial in $n$) and $t$ permutations, appropriately encoded. (The constant $\ell'$ determines the constant $\ell$, as described in the previous paragraph; as $\ell'$ increases, so does $\ell$. We pick $\ell'$ so that $2^{-t/3} + t/2^{n^{\ell'}} < 2^{-4n^2}$.)

As presented in [6], the reduction takes two graphs $G_0$ and $G_1$, along with a random string $r$, and computes the string $w$ and $t$ random permutations (as above), in order to produce a string $x_r = \pi_1(G_{w_1}), \ldots, \pi_t(G_{w_t})$. The proof in [6, Section 3.1] shows that, if $G_0 \equiv G_1$, then $\text{KT}(x_r) \leq (t \log n!) + t/3$.

On the other hand, [6] observes that if $G_0 \not\equiv G_1$ then the entropy of the distribution on strings $x_r$ (assuming $t$ uniformly random permutations and a uniformly-randomly chosen string $w$) is at least $t + t \log(n!)$, and hence the probability that $\text{KT}(x_r) < (t + t \log(n!)) - t/3$ is at most $2^{-t/3}$. In our setting, the permutations are very nearly uniformly random (and it approaches the uniform distribution as $\ell'$ increases), and there is also the possibility that $e(r)$ does not contain the encoding of $t$ permutations, but instead contains a block of zeros. This latter condition arises with probability at most $t/2^{n^{\ell'}}$. Recalling that $2^{-t/3} + t/2^{n^{\ell'}} < 2^{-4n^2}$, we have the following:

- If $G_0 \equiv G_1$, then $\text{KT}(x_r) \leq (t \log n!) + t/3$.
- If $G_0 \not\equiv G_1$, then with probability $> 1 - 2^{-4n^2}$, we have $\text{KT}(x_r) \geq (t \log n!) + 2t/3$. 
We are now ready to define the \( \text{AC}^0 \)-computable function \( f: f(G_0, G_1, e(r)) = (x_r, \theta) \), where \( \theta = t(\log n) + t/2 \) (unless \( e(r) \) contains a block of zeros, indicating failure, in which case \( f(G_0, G_1, e(r)) \) is a string of zeros). Now we observe that \( f \) is computable in \( \text{AC}^0 \). This is because the only real work performed by \( f \) involves permuting a graph. Graphs are encoded as adjacency matrices. Thus, given a graph \( G \) and a permutation \( \pi \), the bit \( (r, s) \) of \( \pi(G) \) is the same as the bit \( (i, j) \) in \( G \), where \( \pi(i) = r \) and \( \pi(j) = s \). That is, position \((r, s)\) in the output is the \( \text{OR}_{r,j} \) (taken over all relevant positions \((i, j)\) in the encoding of \( \pi \)) of \([G_{i,j} \text{ AND } \text{the encoding of } \pi \text{ contains the strings } (i, r) \text{ and } (j, s)]\). This latter condition can easily be checked in \( \text{AC}^0 \).

This establishes that \( f \) has the desired properties.

\begin{Corollary}
Let \( A \) be any oracle. The rigid graph isomorphism problem is reducible to \( \text{MCSP}^A \) via a non-uniform \( \leq_m^{\text{AC}^0} \) reduction.
\end{Corollary}

**Proof.** A standard counting argument shows that there is a value of \( e(r) \) that can be hardwired into the probabilistic reduction of Lemma 11 that works correctly for all pairs \((G_0, G_1)\) of \( n \)-vertex graphs. (Note that the length of the input is \( 2n^2 \), and the error probability is at most \( 1/2^{4n^2} \).)

\begin{Theorem}
Let \( A \) be any oracle. \( \text{DET} \) is reducible to \( \text{MCSP}^A \) via a non-uniform \( \leq_m^{\text{AC}^0} \) reduction. Furthermore, this reduction is “natural” in the sense of [25].
\end{Theorem}

**Proof.** Since \( \text{DET} \) is closed under \( \leq_{\text{TC}^0} \) reductions, it suffices to show that \( \text{MCSP}^A \) is hard under \( \leq_m^{\text{AC}^0} \) reductions, and then appeal to the “Gap” theorem of [2], to obtain hardness under \( \leq_m^{\text{NC}^0} \) reducibility. Torán [39] shows that \( \text{DET} \) is \( \text{AC}^0 \)-reducible to \( \text{GI} \). In fact it is shown in the proofs of Theorem 5.3 and Corollary 5.4 of [39] that \( \text{DET} \) is \( \text{AC}^0 \)-reducible to \( \text{GI} \) via a reduction that produces only pairs of rigid graphs as output. Composing this reduction with the non-uniform \( \text{AC}^0 \) reduction given by Corollary 12 completes the argument.

Since the same threshold \( \theta \) is used for all inputs of the same length, the reduction is “natural”.

An appeal to the circuit lower bounds of Razborov and Smolensky [35, 37] now yields the following corollary:

\begin{Corollary}
\( \text{MCSP}^A \) is not in \( \text{AC}^0[p] \) for any oracle \( A \) and any prime \( p \).
\end{Corollary}

(An alternate proof of this circuit lower bound can be obtained by applying the pseudorandom generator of [13] that has sublinear stretch and is secure against \( \text{AC}^0[p] \); see [19], where a stronger separation from \( \text{AC}^0[p] \) is obtained in this way. Neither our argument nor that of [19] seems easy to extend, to provide a lower bound for \( \text{MCSP} \).

### 5.2 Equivalence between hardness of \( \text{MCSP} \) and circuit lower bounds

The reader may wonder whether the non-uniform reduction can be made uniform under a suitable derandomization hypothesis. We do not know how to obtain a uniform \( \text{AC}^0 \)-many-one reduction, but we can come close, if the oracle \( A \) is not too complex. Recall the definition of ctt-reductions: \( B \leq_{\text{ctt}} C \) if there is a function \( f \in \mathcal{C} \) with the property that \( f(x) \) is a list \( f(x) = (y_1, \ldots, y_m) \), and \( x \in B \) if and only if \( y_j \in C \) for all \( j \). Furthermore, we say that \( f \) is a natural logspace-uniform \( \leq_{\text{ctt}} \)-reduction to \( \text{MCSP} \) if each query \( y_j \) has the same length (and this length depends only on \(|x|\)), and furthermore each \( y_j \) is of the form \((z_j, \theta)\) where the threshold \( \theta \) depends only on \(|x|\).
The following theorem can be viewed as a “partial converse” to results of [29, 7], which say that problems in $\text{LCH} \subseteq \text{E}$ require exponential size circuits if $\text{MCSP}$ or $\text{MKTP}$ is hard for $\text{TC}^0$ under $\text{Dlogtime}$-uniform reductions. That is, the earlier results show that very uniform hardness results imply circuit lower bounds, whereas the next theorem shows that somewhat stronger circuit lower bounds imply uniform hardness results (for a less-restrictive notion of uniformity, but hardness for a larger class). Later on, in Theorem 17, we present a related condition on reductions to $\text{MKTP}^A$ that is equivalent to circuit lower bounds.

**Theorem 15.** Let $A$ be any oracle. If there is some $\epsilon > 0$ such that $\text{DSPACE}(n) \not\subseteq \text{io-SIZE}^{\text{MKTP}^A}(2^n)$, then every language in $\text{DET}$ reduces to $\text{MKTP}^A$ via a natural logspace-uniform reduction.

**Proof.** Let $B \in \text{DET}$. Thus there is an $\text{AC}^0$ reduction $g$ reducing $B$ to the Rigid Graph Isomorphism Problem [39]. Consider the following family of statistical tests $T_x(r)$, indexed by strings $x$:

On input $r$:

- Compute $z = f(g(x), e(r))$, where $f(G_0, G_1, e(r))$ is the function from Lemma 11.
- Accept $r$ if $(x \in B)$ iff $z \in \text{MKTP}^A$.

Since $B \in \text{DET} \subseteq \text{P}$, the test $T_x(r)$ has a polynomial-size circuit with one $\text{MKTP}^A$ oracle gate. (In fact, the statistical test is an $\text{NC}^2$ circuit with one oracle gate.) If $x \in B$, then $T_x$ accepts every string $r$, whereas if $x \not\in B$, $T_x$ accepts most strings $r$.

Klivans and van Melkebeek [26] (building on the work of Impagliazzo and Wigderson [24]) show that, if $\text{DSPACE}(n)$ requires exponential-size circuits from a given class $C$, then there is a hitting set generator computable in logspace that hits all large sets computable by circuits from $C$ that have size $n^k$. In particular, under the given assumption, there is a function $h$ computable in logspace such that $h(0^n) = (r_1, r_2, \ldots, r_{n^\epsilon})$ with the property that, for all strings $x$ of length $n$, there is an element of $h(0^n)$ that is accepted by $T_x$.

Now consider the logspace-uniform $\text{AC}^0$ oracle circuit family, where the circuit for inputs of length $n$ has the strings $e(h(0^n)) = (e(r_1), e(r_2), \ldots, e(r_{n^\epsilon}))$ hardwired into it. On input $x$, the circuit computes the queries $f(g(x), e(r_i))$ for $1 \leq i \leq n^\epsilon$, and accepts if, for all $i$, $f(g(x), e(r_i)) \in \text{MKTP}^A$. Note that if $x \not\in B$, then one of the $r_i$ is accepted by $T_x$, which means that $f(g(x), e(r_i)) \not\in \text{MKTP}^A$; if $x \in B$, then $f(g(x), e(r_i)) \in \text{MKTP}^A$ for all $i$. This establishes that the reduction is correct.

We remark that the hardness assumption $\text{DSPACE}(n) \not\subseteq \text{io-SIZE}^{\text{MKTP}^A}(2^n)$ can probably be weakened (saying that $\text{DSPACE}(n)$ requires large circuits of some restricted sort), since the class of statistical tests that need to be fooled consists only of $\text{NC}^2$ circuits with one oracle gate. On the other hand, Theorem 17 indicates that the hardness assumption that we use is equivalent to the existence of uniform reductions, for certain oracles $A$ — so it is not clear that there is much to be gained by searching for a weaker hardness assumption.

It is also possible to strengthen the hardness assumption, to obtain a stronger conclusion regarding the uniformity condition:

**Corollary 16.** Let $A$ be any oracle. If there is some $\epsilon > 0$ such that the linear-time counting hierarchy $\text{LCH}$ (see [10] for a definition) is not contained in $\text{io-SIZE}^{\text{MKTP}^A}(2^n)$, then every language in $\text{DET}$ reduces to $\text{MKTP}^A$ via a natural ($\text{Dlogtime}$-uniform-$\text{TC}^0$)-uniform reduction.

Since ($\text{Dlogtime}$-uniform-$\text{TC}^0$)-uniform $\text{AC}^0$ is somewhat cumbersome to work with, we concentrate on more familiar uniformity conditions such as ($\text{Dlogtime}$, logspace, $\text{P}$)-uniformity.
in the rest of the paper (although we observe here that Theorem 17 can also be rephrased in terms of the circuit condition of Corollary 16).

Theorem 15 deals with the oracle problem MKTP$^A$, but the most interesting case is the case where $A = \emptyset$, both because the hypothesis seems most plausible in that case, and because MKTP has been studied in connection with MCSP, which has been studied more than the associated circuit problem MCSP$^A$. The hypothesis is false when $A = \text{QBF}$, since the KT$^A$ measure is essentially the same as the KS measure studied in [4], where it is shown that PSPACE $= \text{ZPP}^R_{\text{cc}}$, and thus PSPACE has polynomial-size MKTP$^{\text{QBF}}$-circuits. Strikingly, it is of interest that not only the hypothesis is false in this case – but the conclusion is false as well. (See Corollary 19.)

For certain oracles (and we discuss below how broad this class of oracles is), the existence of uniform reductions is equivalent to certain circuit lower bounds.

**Theorem 17.** Let MKTP$^A \in \mathcal{P}^A/\text{poly}$. Then the following are equivalent:

- PARITY reduces to MKTP$^A$ via a natural logspace-uniform $\leq_{\text{ctt}}^A$-reduction.
- For some $\epsilon > 0$, $\text{DSPACE}(n) \not\subseteq \text{io-SIZE}^A(2^{\epsilon n})$.
- For some $\epsilon > 0$, $\text{DSPACE}(n) \not\subseteq \text{io-SIZE}^{\text{MKTP}^A}(2^{\epsilon n})$.
- DET reduces to MKTP$^A$ via a natural logspace-uniform $\leq_{\text{ctt}}^A$-reduction.

Furthermore, if PARITY reduces to MCSP$^A$ via a natural logspace-uniform $\leq_{\text{ctt}}^A$-reduction, then all of the above hold.

**Proof.** First, we show that the first condition implies the second.

Let $\{C_n : n \in \mathbb{N}\}$ be a logspace-uniform family of oracle circuits computing PARITY, consisting of $\mathcal{AC}^0$ circuitry feeding into oracle gates, which in turn are connected to an AND gate as the output gate. Let the oracle gates in $C_n$ be $g_1, g_2, \ldots, g_{n^c}$. On any input string $x$, let the value fed into gate $g_i$ on input $x$ be $(q_i(x), \theta)$, and recall that, since the reduction is natural, the threshold $\theta$ depends only on $n$, and thus it is a constant in $C_n$.

Now, we appeal to [7, Claim 3.11], and conclude that each MKTP$^{\text{QBF}}$ oracle gate can be replaced by a DNF formula of size at most $n^{O(1)}2^{O(\theta^2 \log \theta)}$. Inserting these DNF formulae into $C_n$ (in place of each oracle gate) results in a circuit of size $n^{O(1)}2^{O(\theta^2 \log \theta)}$ computing PARITY. Let the depth of this circuit be some constant $d$. It follows from [16] that $n^{O(1)}2^{O(\theta^2 \log \theta)} \geq 2^{\Theta(n^{1/4d})}$, and hence that $\theta \geq n^{1/4d}$.

Note that all of the oracle gates $g_i$ must output 1 on input $0^{n-1}1$, and one of the oracle gates $g_{i_0}$ must output 0 on input $0^n$. Thus we have $\text{KT}^A(q_{i_0}(0^n)) \geq \theta \geq n^{1/4d}$. It follows from [4, Theorem 11] that the function with truth-table $q_{i_0}(0^n)$ has no circuit (with oracle gates for $A$) of size less than $(\text{KT}^A(q_{i_0}(0^n)))^{1/3} \geq \theta^{1/3} \geq n^{1/12d}$.

Note that, in order to compute the $j$-th bit of some query $q_i(0^n)$, it suffices to evaluate a logspace-uniform $\mathcal{AC}^0$ circuit where all of the input bits are 0. Since this computation can be done in logspace on input $(0^n1^01^0)$, note that the language $H = \{(n, i, j) : \text{the } j\text{-th bit of query } q_i(0^n) \text{ is } 1\}$ is in linear space. Let $m = |(n, i, j)|$, and let $s(m)$ be the size of the smallest circuit $D_m$ computing $H$ for inputs of length $m$. Hardwire the bits for $n$ and also set the bits for $i$ to $i_0$. The resulting circuit on $|j| < m$ bits computes the function given by $q_{i_0}(0^n)$, and it was observed above that this circuit has size at least $n^{1/20d} \geq 2^{m^{1/20d}}$.

This establishes the first implication. (Note also that a similar argument yields the same conclusion from the assumption that PARITY reduces to MCSP$^A$ via a natural logspace-uniform $\leq_{\text{ctt}}^A$-reduction.)

The assumption that MKTP$^A \in \mathcal{P}^A/\text{poly}$ suffices to show that the second condition implies the third. More formally, we'll consider the contrapositive. Assume that $\text{DSPACE}(n) \not\subseteq \text{io-SIZE}^{\text{MKTP}^A}(2^{\epsilon n})$ for every $\epsilon > 0$. An oracle gate for MKTP$^A$ on inputs of size $m$ can be
replaced by a circuit (with oracle gates for $A$) of size $m^c$ for some constant $c$. Carrying out this substitution in a circuit (with oracle gates for $\text{MKTP}^A$) of size $2^n$ yields a circuit of size at most $2^n + 2^n(2^n)^c$.

Let $\delta > 0$. Then we can pick $\epsilon$ small enough so that $2^{c\epsilon n} + 2^{n(2^{c\epsilon n})} < 2^{\delta n}$, thereby establishing that $\text{DSPACEx}(n) \subseteq \text{io-SIZE}^A(2^{\delta n})$ for every $\delta > 0$. This establishes the second implication.

Theorem 15 establishes that the third condition implies the fourth. The fourth condition obviously implies the first.

To the best of our knowledge, this is the first theorem that has given conditions where the existence of a reduction to $\text{MCSP}^A$ implies the existence of a reduction to $\text{MKTP}^A$. We know of no instance where the implication goes in the opposite direction.

The logspace uniformity condition in Theorem 17 can be replaced by other less-restrictive uniformity conditions. We mention the following example:

**Corollary 18.** Let $\text{MKTP}^A \in P^A/poly$. Then the following are equivalent:

- $\text{PARITY}$ reduces to $\text{MKTP}^A$ via a natural $P$-uniform $\leq_{\text{ctt}}^A$-reduction.
- For some $\epsilon > 0$, $E \not\subseteq \text{io-SIZE}^A(2^{\epsilon n})$.
- For some $\epsilon > 0$, $E \not\subseteq \text{io-SIZE}^{\text{MKTP}^A}(2^{\epsilon n})$.
- $\text{DET}$ reduces to $\text{MKTP}^A$ via a natural $P$-uniform $\leq_{\text{ctt}}^A$-reduction.

Furthermore, if $\text{PARITY}$ reduces to $\text{MCSP}^A$ via a natural $P$-uniform $\leq_{\text{ctt}}^A$-reduction, then all of the above hold.

At this point, we should consider the class of oracles for which Theorem 17 applies. That is, what is the set of oracles $A$ for which $\text{MKTP}^A \in P^A/poly$? First, we observe that this condition holds for any $\text{PSPACE}$-complete set, which yields the following corollary:

**Corollary 19.** $\text{PARITY}$ does not reduce to either $\text{MKTP}^{QBF}$ or $\text{MCSP}^{QBF}$ via a natural logspace-uniform $\leq_{\text{ctt}}^A$-reduction.

As another example of a set for which $\text{MKTP}^A \in P^A/poly$, consider the set $A = \{(M, x, 1^m) : M$ is an alternating Turing machine that accepts $x$, and runs in time at most $m$ and makes at most $\log m$ alternations$\}$. $A$ is complete for the class $\text{ATIME-ALT}(n^{O(1)}, O(\log n))$ under $\leq_{\text{AC}^0}^A$ reductions. It is easy to see that $\text{MKTP}^A \in \text{ATIME-ALT}(n^{O(1)}, O(\log n))$, and thus $\text{MKTP}^A \in P^A$. (Other examples can easily be created in this way, using an even smaller number of alternations.) Note that, for this oracle $A$, it seems plausible that all four conditions in Theorem 17 hold.

Nonetheless, we do grant that this does seem to be a strong condition to place upon the oracle $A$ – and it has even stronger consequences than are listed in Theorem 17. For instance, note that the proof that the first condition in Theorem 17 implies the second relies only on the fact that $\text{PARITY}$ requires large $\text{AC}^0$ circuits. Thus, an identical proof shows that these four conditions are also equivalent to the condition that $\text{PARITY}$ is reducible to $\text{MKTP}^A$ via a natural $\text{ctt}$-reduction where the queries are computed by logspace-uniform $\text{AC}^0[7]$ circuits. (Or you can substitute any other problem and class of mod circuits, where an exponential lower bound is known because of [35, 37].) In fact, as in [7, Lemma 3.10] we can apply random restrictions in a logspace-uniform way (as described in [1]) and obtain a reduction from $\text{PARITY}$ to $\text{MKTP}^A$ where the queries are computed by logspace-uniform $\text{NC}^0$ circuits! That is, for example, $\text{MAJORITY}$ is reducible to $\text{MKTP}^A$ via reductions of this sort computed by logspace-uniform $\text{AC}^0[3]$ circuits if $\text{PARITY}$ is reducible to the same set via reductions where the queries are computed by logspace-uniform $\text{NC}^0$ circuits. We find these implications to be surprising. The “gap” phenomenon that was described in [2]
(showing that completeness under one class of reductions is equivalent to completeness under a more restrictive class of reductions) had not previously been observed to apply to $\text{AC}_0^0[p]$ reducibility.

We want to highlight some contrasts between Theorem 15 and Corollary 19. $\text{MKTP}^{Q\text{BF}}$ is hard for $\text{PSPACE}$ under $\text{ZPP}$-Turing reductions [4], whereas $\text{MKTP}$ is in $\text{NP}$. Thus $\text{MKTP}^{Q\text{BF}}$ appears to be much harder than $\text{MKTP}$. Yet, Theorem 17 shows that, under a plausible hypothesis, the “easier” set $\text{MKTP}$ is hard for $\text{DET}$, whereas the “harder” problem $\text{MKTP}^{Q\text{BF}}$ cannot even be used as an oracle for $\text{PARITY}$ under this same reducibility.

In other words, the (conditional) natural logspace-uniform $\leq_{\text{AC}_0^0}$ reductions from problems in $\text{DET}$ to $\text{MKTP}$ given in Theorem 15 are not “oracle independent” in the sense of [20]. Prior to this work, there had been no reduction to $\text{MCSP}$ or $\text{MKTP}$ that did not work for every $\text{MCSP}_A$ or $\text{MKTP}_A$, respectively.

Prior to this work, it appears that there was no evidence for any variant of $\text{MCSP}$ or $\text{MKTP}$ being hard for a reasonable complexity class under $\leq_{\text{polY}}$ reductions. All prior reductions (such as those in [5, 4, 6]) had been probabilistic and/or non-uniform, or (even under derandomization hypotheses) seemed difficult to implement in $\text{NC}$. But Theorem 17 shows that it is quite likely that $\text{MKTP}$ is hard for $\text{DET}$ under $\leq_{\text{TT}}$ reductions (and even under much more restrictive reductions).

5.3 On the importance of uniformity

Surprisingly (to us), the notion of uniformity appears to be central. In particular, the reader is probably wondering whether the logspace-uniformity condition in Theorem 15 can be improved to Dlogtime-uniformity. One answer is provided by the results of [12], which show that – at a minimum – any such proof would need to involve a different approach than an implementation of the Nisan-Wigderson generator [30], because no set system that satisfies the Nisan-Wigderson requirements can be implemented in Dlogtime-uniform $\text{AC}_0$. However, Theorem 21 below shows that, under a plausible hypothesis, no Dlogtime-uniform approach is possible (at least, for many oracles $A$).

First, we recall Corollary 3.7 of [7], which states that $\text{MKTP}^{Q\text{BF}}$ is not hard for $\text{P}$ under $\leq_{\text{m}}$ reductions unless $\text{PSPACE} = \text{EXP}$. It turns out that this holds even for logspace-Turing reductions.

$\blacktriangleright$ Theorem 20. $\text{MKTP}^{Q\text{BF}}$ is not hard for $\text{P}$ (or $\text{NP}$) under $\leq_{\text{TT}}$ reductions unless $\text{PSPACE} = \text{EXP}$ (or $\text{PSPACE} = \text{NEXP}$, respectively). $\text{MKTP}^{Q\text{BF}}$ is not hard for $\text{PSPACE}$ under $\leq_{\text{TT}}$ reductions. The same holds for $\text{MCSP}^{Q\text{BF}}$.

We include this proof here, both because it improves a Corollary in [7], and because the proof can be viewed as a warm-up for the proof of Theorem 21.

Proof. First, note that $\leq_{\text{m}}$ and $\leq_{\text{TT}}$ reducibilities coincide [28]. Thus assume that $\text{MKTP}^{Q\text{BF}}$ is hard for $\text{P}$ under $\leq_{\text{TT}}$ reductions; we will show that $\text{PSPACE} = \text{EXP}$. (The proof for $\text{MCSP}^{Q\text{BF}}$ is identical, and the variant concerning hardness for $\text{NP}$ is analogous.)

The proof idea is based on [20]: Assume that $\text{P} \subseteq L_{\text{TT}}^{\text{MKTP}^{Q\text{BF}}}$. (Here, $L_{\text{TT}}$ means a $\leq_{\text{TT}}$ reduction.) By standard padding, we obtain $\text{EXP} \subseteq \text{PSPACE}_{\text{TT}}^{\text{MKTP}^{Q\text{BF}}}$. Any query of a $\text{PSPACE}_{\text{TT}}$ machine has low KT$^{Q\text{BF}}$ complexity. Moreover, one can check whether
a string has low $\ KT_{QBF}$ complexity in $\text{PSPACE}$. Combining these two facts, we obtain $\text{EXP} \subseteq \text{PSPACE}_{\text{MKTP}^A}^{\text{QBF}} = \text{PSPACE}$. A formal proof follows.

Let $B \in \text{EXP}$. Let $B' = \{x10^{2^{|x|}} : x \in B\}$ and note that $B' \in \text{P}$. Consider the $\leq_{tt}^A$ reduction that reduces $B'$ to $\text{MKTP}^A$. On any input string $y$, let the $i$-th oracle query be $q_i(y)$. The language $\{(i,j,x) : \text{the } j\text{-th bit of } q_i(x10^{2^{|x|}}) \text{ is } 1\}$ is in $\text{PSPACE}$ and thus is in $\text{P}^{\text{QBF}}$. It follows that $q_i(x10^{2^{|x|}})$ is of the form $(y_i, \theta_i)$, where $\text{KT}_{QBF}(y_i) = |x,i,j|^{O(1)}$. Thus, to evaluate the oracle query $q_i$ on input $x10^{2^{|x|}}$, this $\text{PSPACE}$ computation (on input $x$) suffices: Compute the bits of $\theta_i$; this can be done in $\text{PSPACE}$, since the number of bits in $\theta_i$ is at most $|x|^{O(1)}$, and each bit is computable in $\text{PSPACE}$. If $\theta_i > |x,i,j|^{c}$ (for the appropriate value of $c$), then return “1” since the query $y_i$ certainly has $\text{KT}^A$ complexity less than this. Otherwise, try all descriptions $d$ of length at most $\theta_i$, to determine whether there is some such $d$ for which $U^{\text{QBF}}(d,j)$ is equal to the $j$-th bit of $q_i$ (allowing at most $|x,i,j|^c$ steps for the computation of $U$).

The rest of the $\leq_{tt}^A$ reduction on input $x10^{2^{|x|}}$ can be computed in space $|x|^{O(1)}$, by re-computing the values of the oracle queries, as required.

The unconditional result that $\text{MKTP}^{\text{QBF}}$ is not hard for $\text{PSPACE}$ under $\leq_{tt}^A$ reductions follows along the same lines, choosing $B \in \text{EXPSPACE}$, and leading to the contradiction $\text{EXPSPACE} = \text{PSPACE}$. □

A similar approach yields the following result:

> Theorem 21. Let $\text{NP} \subseteq \text{P}^A/\text{poly}$. If $\text{PSPACE} \not\subseteq \text{PH}^A$, then neither $\text{MKTP}^A$ nor $\text{MCSP}^A$ is hard for $\text{NC}^1$ under Dlogtime-uniform $\leq_{tt}^{\text{AC}^0}$ reductions.

Proof. We present the proof for $\text{MKTP}^A$; the proof for $\text{MCSP}^A$ is identical.

Assume that $\text{MKTP}^A$ is hard for $\text{NC}^1$ under Dlogtime-uniform $\leq_{tt}^{\text{AC}^0}$; we will show that $\text{PSPACE} \not\subseteq \text{PH}^A$. Since we are assuming that $\text{NP} \subseteq \text{P}^A/\text{poly}$ note that we also have $\text{PH} \subseteq \text{P}^A/\text{poly}$.

By the closure properties of $\text{PH}$, it will suffice to show that $\text{ATIME}(n) \not\subseteq \text{PH}^A$.

Let $B \in \text{ATIME}(n)$. Let $B' = \{x10^{2^{|x|}} : x \in B\}$ and note that $B' \in \text{NC}^1$. Consider the oracle family $(C_n)$ that reduces $B'$ to $\text{MKTP}^A$. Let the oracle gates in $C_{2^n+n+1}$ be $g_1, g_2, \ldots, g_r$. On any input string $y$, let the query that is fed into gate $g_i$ be $q_i(y)$. The language $\{2^{|x|} + |x| + 1, i, j, x) : \text{the } j\text{-th bit of } q_i(x10^{2^{|x|}}) \text{ is } 1\}$ is in $\text{PH}$ and thus is in $\text{P}^A/\text{poly}$. It follows that $q_i(x10^{2^{|x|}})$ is of the form $(y_i, \theta_i)$, where $\text{KT}_A^A(y_i) = |x,i,j|^{O(1)}$. Thus, to evaluate oracle gate $g_i$ on input $x10^{2^{|x|}}$, this $\text{PH}^A$ computation (on input $x$) suffices: Compute the bits of $\theta_i$; this can be done in $\text{PH}$, since the number of bits in $\theta_i$ is at most $|x|^{O(1)}$, and each bit is computable in $\text{PH}$. If $\theta_i > |x,i,j|^{c}$ (for the appropriate value of $c$), then return “1” since the query $y_i$ certainly has $\text{KT}^A$ complexity less than this. Otherwise, guess a description $d$ of length at most $\theta_i$, and universally check (for each $j$) that $U^A(d,j)$ is equal to the $j$-th bit of $q_i$ (allowing at most $|x,i,j|^c$ steps for the computation of $U$).

To evaluate the rest of the circuit, note that the unbounded fan-in AND and OR gates that sit just above the oracle gates can also be evaluated in $\text{PH}^A$ (at one level higher in the hierarchy than is required to evaluate the oracle gates). Repeating this process through the remaining $O(1)$ levels of the circuit yields the desired $\text{PH}^A$ algorithm for $B$. □

Remark. The significance of Theorem 21 is best viewed by combining it with Theorem 15. If we choose $A$ to be any $\text{NP}$-complete set, then both of the hypotheses $\text{PSPACE} \not\subseteq \text{PH}^A$ and $\text{SPACE}(n) \not\subseteq \text{io-SIZE}^{\text{MKTP}^A}(2^n)$ are plausible. Thus, for such oracles $A$, under a plausible hypothesis, we have both $\text{MKTP}^A$ is not hard for $\text{NC}^1$ under Dlogtime-uniform $\leq_{tt}^{\text{AC}^0}$ reductions, and $\text{MKTP}^A$ is hard for $\text{DET}$ under logspace-uniform $\leq_{tt}^{\text{AC}^0}$ reductions.
Thus different notions of uniformity are a key part of the puzzle, when trying to understand the hardness of problems such as MKTP and MCSP.

We are even able to extend our approach in some cases, to apply to $\text{AC}^0$-Turing reducibility.

**Theorem 22.** Let $\text{NP}^A \subseteq P^A / \text{poly}$. If $\text{PSPACE} \not\subseteq \text{PH}^A$, then neither $\text{MKTP}^A$ nor $\text{MCSP}^A$ is hard for $\text{NC}^1$ under Dlogtime-uniform $\leq_{T}^{AC^0}$ reductions.

**Proof.** Note that in a circuit computing an $\leq_{T}^{AC^0}$ reduction, there is an “initial” layer of oracle gates, whose queries are computed nonadaptively, while all oracle gates at deeper levels have queries whose values depend upon oracle gates at earlier levels in the circuit. Note also that, under the given assumption $\text{NP}^A \subseteq P^A / \text{poly}$, we can conclude that $\text{PH}^A \subseteq P^A / \text{poly}$.

The proof now proceeds along precisely the same lines as the proof of Theorem 21, which shows that a $\text{PH}^A$ computation can compute the value of each wire that feeds into the “initial” layer of oracle gates. Similarly, as in the proof of Theorem 21, all of the AND, OR, and NOT gates at higher levels can be computed in $\text{PH}^A$, given that the gates at lower levels can be evaluated in $\text{PH}^A$. Thus, we need only show how to deal with oracle gates at deeper levels.

Consider any such oracle gate $g$. On any input string $y$, let the query that is fed into gate $g$ when evaluating the circuit on input $y$ be $q_g(y)$. The language $\{ (2^{|x|} + |x| + 1, g, j, x) : \text{the } j\text{-th bit of } q_g(x10^{2|x|}) \text{ is } 1 \}$ is in $\text{PH}^A$ and thus (by our new assumption) is in $P^A / \text{poly}$. It follows that $q_g(x10^{2|x|})$ is of the form $(y, \theta)$, where $\text{KT}^A(y) = |x, g, j|$ (1). Thus, to evaluate oracle gate $g$ on input $x10^{2|x|}$, this $\text{PH}^A$ computation (on input $x$) suffices: Compute the bits of $\theta$; this can be done in $\text{PH}^A$, since the number of bits in $\theta$ is at most $|x|$ (1), and each bit is computable in $\text{PH}$. If $\theta > |x, g, j|^c$ (for the appropriate value of $c$), then return “1” since the query $y$ certainly has $\text{KT}^A$ complexity less than this. Otherwise, guess a description $d$ of length at most $\theta$, and universally check (for each $j$) that $U^A(d, j)$ is equal to the $j$-th bit of $q_g$ (allowing at most $|x, i, j|^c$ steps for the computation of $U$).

A consequence of Theorem 22 is the following corollary, which has the same flavor of results of the form “$\text{MCSP}$ is hard for class $C$ implies a likely but hard-to-prove consequence” as presented by Murray and Williams [29], but moving beyond the $\leq_{T}^{AC^0}$ reductions considered by them, to the more general $\leq_{T}^{AC^0}$ reductions.

**Corollary 23.** If either of $\text{MKTP}$ or $\text{MCSP}$ is hard for $\text{NC}^1$ under Dlogtime-uniform $\leq_{T}^{AC^0}$ reductions, then $\text{NP} \neq \text{NC}$.

**Proof.** This follows from Theorem 21 when $A = \emptyset$. If $\text{NP} = \text{NC}$, then we have $\text{NP} \subseteq \text{P} / \text{poly}$, and $\text{PH} = \text{NC} \neq \text{PSPACE}$. Thus neither $\text{MKTP}$ nor $\text{MCSP}$ is hard for $\text{NC}^1$ under Dlogtime-uniform $\leq_{T}^{AC^0}$ reductions.

We also present another result in this vein, about $\text{NP}$-completeness. Prior work [29, 7] had obtained stronger consequences from the stronger assumption that $\text{MCSP}$ is $\text{NP}$-complete under Dlogtime-uniform $\leq_{T}^{AC^0}$ reductions.

**Corollary 24.** If either of $\text{MKTP}$ or $\text{MCSP}$ is hard for $\text{NP}$ under Dlogtime-uniform $\leq_{T}^{AC^0}$ reductions, then $\text{NP} \neq \text{MA} \cap \text{P} / \text{poly}$.

**Proof.** If you modify the proof of Theorem 22, replacing $\text{NC}^1$ by $\text{NP}$ and replacing $\text{PSPACE}$ by $\text{NEXP}$, you obtain that, if $\text{NP} \subseteq \text{P} / \text{poly}$, then $\text{NEXP} \neq \text{PH}$ implies that neither $\text{MKTP}$ nor $\text{MCSP}$ is hard for $\text{NP}$ under Dlogtime-uniform $\leq_{T}^{AC^0}$ reductions.

Or, restating this using the same hypothesis as in the statement of the corollary, if $\text{MKTP}$ or $\text{MCSP}$ is hard for $\text{NP}$ under Dlogtime-uniform $\leq_{T}^{AC^0}$, then either $\text{NP} \not\subseteq \text{P} / \text{poly}$.
or $\text{NEXP} = \text{PH}$. Since (NP $\subseteq$ P/poly and NEXP $\subseteq$ P) is equivalent to NEXP $\subseteq$ P/poly, and since NEXP $\subseteq$ P/poly is equivalent to NEXP $= \text{MA}$ [23], we obtain that NP-hardness of MCSP or MKTP implies NP $\not\subseteq$ P/poly or NEXP $= \text{MA}$. (Murray and Williams obtain essentially this same consequence under the stronger assumption that MCSP is complete under $\leq^T_{\text{m}} \text{AC}^0$ reductions, but are also able to show that NEXP $\not\subseteq$ P/poly in this case.)

In either case, we obtain the consequence NP $\neq$ MA $\cap$ P/poly.

We close this section with another variant of Theorem 22, proved via the same technique:

- **Theorem 25.** Let $\text{NP}^A \subseteq \text{P}^A/\text{poly}$. If NEXP $\not\subseteq$ PSPACE$^A$ (or NEXP $\not\subseteq$ EXP$^A$), then neither MKTP$^A$ nor MCSP$^A$ is hard for NP under logspace-uniform $\leq^T_{\text{AC}^0}$ reductions (P-uniform $\leq^T_{\text{AC}^0}$ reductions).

- **Corollary 26.** MKTP$^\text{QBF}$ is not hard for NP under logspace-uniform $\leq^T_{\text{AC}^0}$ reductions (P-uniform $\leq^T_{\text{AC}^0}$ reductions) unless PSPACE $= \text{NEXP}$ (EXP $= \text{NEXP}$, respectively). The same holds for MCSP$^\text{QBF}$.

Although the following corollary discusses $\leq^T_{\text{AC}^0}$ reductions, it also says something about $\leq^T_1$ reducibility. This is because, assuming $\text{DSPACE}(n) \not\subseteq$ io-SIZE$^\text{MKTP}^A(2^n)$, any $\leq^T_1$ reduction to MKTP can be simulated by a logspace-uniform $\leq^T_{\text{AC}^0}$ reduction to MKTP. (To see this, note that, by Theorem 15, MKTP is hard for DET under this class of reductions, and hence each of the logspace-computable (nonadaptive) queries can be computed using oracle gates for MKTP, and similarly the logspace computation that uses the queries can also be simulated using MKTP. Similar observations arise in [11].)

- **Corollary 27.** If either of MKTP or MCSP is hard for NP under logspace-uniform $\leq^T_{\text{AC}^0}$ reductions (P-uniform $\leq^T_{\text{AC}^0}$ reductions), then NP $\not\subseteq$ P/poly or NEXP $= \text{PSPACE}$ (EXP $= \text{NEXP}$, respectively).

### 6 Conclusions and Open Questions

**Conclusions.** At a high level, we have advanced our understanding about MCSP and MKTP in the following two respects:

1. On one hand, under a very weak cryptographic assumption, the problem of approximating MCSP or MKTP is indeed NP-intermediate under general types of reductions when the approximation factor is quite huge. This complements the work of [29] for very restricted reductions.

2. On the other hand, if the gap is small, MKTP is DET-hard under nonuniform NC$^0$ reductions (contrary to previous expectations). This suggests that nonuniform reductions are crucial to understanding hardness of MCSP. While there are many results showing that NP-hardness of MCSP under uniform reductions is as difficult as proving circuit lower bounds, can one show that MCSP is NP-hard under P/poly reductions (without proving circuit lower bounds)?

**Open Questions.** It should be possible to prove unconditionally that MCSP is not in AC$^0[2]$; we conjecture that the hardness results that we are able to prove for MKTP hold also for MCSP.

We suspect that it should be possible to prove more general results of the form “If MCSP$^A$ is hard for class C, then so is MKTP$^A$.” We view Theorem 17 to be just a first step in this direction. One way to prove such a result would be to show that MCSP$^A$ reduces to MKTP$^A$,
but (with a few exceptions such as $A = \text{QBF}$) no such reduction is known. Of course, the case $A = \emptyset$ is the most interesting case.

Is MKTP hard for P? Or for some class between DET and P? Is it more than a coincidence that DET arises both in this investigation of MKTP and in the work of Oliveira and Santhanam on MCSP [31]?

Is there evidence that Gap,MCSP has intermediate complexity when $\epsilon$ is a fixed constant, similar to the evidence that we present for the case when $\epsilon(n) = o(1)$?

Acknowledgments

We thank Ryan Williams, Rahul Santhanam, Salil Vadhan, Marina Knittel, Rahul Ilango, and Prashant Nalini Vasudevan for helpful discussions.

References


