Nondeterministic Direct Product Reductions and the Success Probability of SAT Solvers

Andrew Drucker[*]

Abstract

We give two nondeterministic reductions which yield new direct product theorems (DPTs) for Boolean circuits. In these theorems one assumes that a target function f is mildly hard against *nondeterministic* circuits, and concludes that the direct product $f^{\otimes t}$ is extremely hard against (only polynomially smaller) probabilistic circuits. The main advantage of these results compared with previous DPTs is the strength of the size bound in our conclusion.

As an application, we show that if NP is not in $\mathsf{coNP/poly}$ then, for every PPT algorithm attempting to produce satisfying assigments to Boolean formulas, there are infinitely many instances where the algorithm's success probability is nearly-exponentially small. This furthers a project of Paturi and Pudlák [STOC'10].

Contents

[*]School of Informatics, U. Edinburgh, U.K. Email: `andy.drucker@gmail.com`. This research was conducted as a member of the School of Mathematics, IAS, Princeton, NJ. This material is based upon work supported by the National Science Foundation under agreements Princeton University Prime Award No. CCF-0832797 and Sub-contract No. 00001583. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

1 Introduction

This work contributes to two central areas of study in complexity theory: *hardness amplification* on the one hand, and *the complexity of* NP *search problems* on the other.

1.1 Hardness amplification and direct product theorems

In the general hardness amplification project, we assume that we have identified a function f that is "mildly hard" to compute, for some class $\mathcal{C}$ of resource-bounded algorithms. Our goal is to derive a second function f' that is "extremely hard" to compute, for some possibly-different class $\mathcal{C}'$. In our initial discussion we will focus on the case where $f : \{0,1\}^n \to \{0,1\}^d$, $f' : \{0,1\}^{n'} \to \{0,1\}^{d'}$ are finite functions, and $\mathcal{C}, \mathcal{C}'$ are two sets of probabilistic Boolean circuits, but we note that the project can be studied in other models as well.

The notion of difficulty suggested above can be formalized in two ways (both relevant to our work). Let $p \in [0,1]$. In the *average-case* setting, let us say that f is *p-hard for $\mathcal{C}$* with respect to an input distribution $\mathcal{D}$ if, on an input $\mathbf{x} \sim \mathcal{D}$, every algorithm in $\mathcal{C}$ computes $f(\mathbf{x})$ correctly with probability at most p. In the *worst-case* setting, we say that f is *worst-case p-hard* for a class $\mathcal{C}$ of randomized algorithms if, for every algorithm $C \in \mathcal{C}$, there is an input x such that $\Pr_C[C(x) = f(x)] \leq p$. In either setting, from a "mild" hardness guarantee $p = 1 - \varepsilon$ for $\mathcal{C}$ in computing f, we want to obtain a much stronger bound $p' \ll 1$ for the second class $\mathcal{C}'$ in computing f'.

There are several motivations to pursue hardness amplification. First, the security of most modern cryptographic primitives, such as one-way functions and public-key cryptosystems, inherently requires the existence of computational problems, solvable in NP, which possess a strong average-case hardness guarantee. While the mere existence of hard-on-average problems in NP is not known to be *sufficient* for doing cryptography, a better understanding of the sources of average-case hardness seems necessary for making progress in the foundations of cryptography. Moreover, hardness-amplification techniques in complexity theory have also helped to inspire tools for the *security-amplification* of cryptographic primitives. (See, e.g., [Gol07] for background on the complexity-theoretic underpinnings of modern cryptography and on ideas of security amplification.)

Second, average-case hardness is also inherent in the fundamental concept of *pseudorandomness*: a pseudorandom source is information-theoretically distinguishable from random bits, yet the distinguishing task must be computationally hard-on-average. Techniques of hardness amplification have played a key role in important constructions of pseudorandom generators [HILL99, IW97].

Third, hardness amplification, and in particular the *direct product* approach to amplifying hardness, is interesting in its own right, and helps us to critically examine some of our most basic intuitions about computation, as we will describe.

Given a function f as above and $t \in \mathbb{N}^+$, let $f^{\otimes t} : \{0,1\}^{n \times t} \to \{0,1\}^{d \times t}$, the *$t$-fold direct product of f*, be the function which takes t length-n inputs $(x^1, \ldots, x^t)$ and outputs $(f(x^1), \ldots, f(x^t))$. A *direct product theorem (DPT)* is any result upper-bounding the success bound p' for computing $f^{\otimes t}$ in terms of an assumed success bound p for f (and, possibly, other parameters).

When f is Boolean, the direct product construction can be considered along with the related "t-fold XOR" $f^{\oplus t}(x^1, \ldots, x^t) := \bigoplus f(x^j)$ (i.e., the sum mod 2). An "XOR lemma" is any result upper-bounding the success bound p' for computing $f^{\oplus t}$ in terms of an assumed success bound p for f. The original XOR lemma was stated by Yao in unpublished work, with the first published proof due to Levin [Lev87]; see [GNW11] for more information on the lemma's history and several proofs. Unlike the direct product, the t-fold XOR $f^{\oplus t}$ is itself a Boolean function, which can be advantageous in applications of hardness amplification, but which can also be a disadvantage since this limits its average-case hardness (an algorithm may compute $f^{\oplus t}$ with success probability $1/2$ by guessing a random bit). Several works show how in some settings XOR lemmas may be obtained from DPTs [GL89, GNW11] or vice versa [NRS99, VW08]. We will not prove or use XOR lemmas in this work; we merely point out that their study is often intimately linked with the study of direct product theorems (indeed, XOR lemmas are even referred to as "direct product theorems" in some papers).

The motivation for the direct product construction is as follows. Let $\mathcal{C}_{\leq s}$ be the class of probabilistic Boolean circuits of size at most s. It would *appear* that, if any circuit $C \in \mathcal{C}_{\leq s}$ has success probability at most $p < 1$ in computing f, then any circuit $C' \in \mathcal{C}_{\leq s}$ should have success probability not much more than p^t in computing $f^{\otimes t}$. The intuition here is that combining the t "unrelated" computations should not help much, and simply trying to solve each instance separately would be a nearly-optimal strategy.

This hypothesis can be considered in both the worst-case and the average-case setting; in the latter, if f is p-hard with respect to inputs drawn from $\mathcal{D}$, then it is natural to study the difficulty of computing $f^{\otimes t}$ with t inputs drawn independently from $\mathcal{D}$.[1]

One might even be tempted to make the bolder conjecture that $f^{\otimes t}$ is p^t-hard against circuits in $\mathcal{C}_{\leq t \cdot s}$, but this was shown by Shaltiel to fail badly in the average-case setting [Sha03]. So what kind of DPT is known to hold in the circuit model? A version of the following theorem, with slightly weaker parameters, was proved in [GNW11, first version in '95] ; a tighter argument leading to the

[1] "Derandomized" variants of the scenario, in which the t inputs are not fully independent, have also been studied, and powerful "derandomized" DPTs were obtained, notably in [IW97, IJKW10]. We will not consider these in the present paper. Neither will we consider "XOR lemmas", which analyze a variant of the direct product construction in the case where f is Boolean [GNW11].

bounds given below is described in [Wig97]. In the form of the DPT stated below, the focus is on getting a success probability bound of at most some $\varepsilon > 0$ for $f^{\otimes t}$, where t is chosen accordingly.

Theorem 1.1 (see [GNW11], Lemma 7, and [Wig97], Theorems 2.9, 2.10)**.** *Suppose the Boolean function $f : \{0,1\}^n \to \{0,1\}$ is p-hard for circuits of size s with respect to input distribution $\mathcal{D}$, for some $p < 1$. For an appropriate $t = \Theta\left(\frac{\ln(1/\varepsilon)}{1-p}\right)$, the function $f^{\otimes t}$ is ε-hard with respect to $\mathcal{D}^{\otimes t}$ for circuits with size bounded by s', where*

$$s' \;=\; \Theta\left(\frac{\varepsilon \cdot s}{\ln(1/\varepsilon)}\right) \;.$$

This is a powerful and elegant result, but one whose parameters can be disappointing in many situations. The size bound s' degrades quickly as $\varepsilon \to 0$; if $s \leq \mathrm{poly}(n)$, i.e., if our initial hardness assumption is against circuits of some fixed-polynomial size (and $p = 2/3$, say), then Theorem 1.1 cannot give a success bound of $n^{-\omega(1)}$ against any nontrivial class of circuits. In unpublished work, Steven Rudich has observed that this barrier is inescapable for a certain class of "black-box," relativizing, *deterministic* (or probabilistic) reductions (see [GNW11] for more discussion). The limitations of more general black-box hardness-amplification reductions have been extensively studied, particularly for the case of XOR lemmas and other reductions that produce a Boolean function; Shaltiel and Viola's work [SV10] is one notable contribution which also provides a good guide to this literature.

1.2 Our new direct product theorems

In this work we show that, if we are willing to assume that our starting function f is somewhat hard to compute by *nondeterministic* circuits, then we obtain very strong hardness results for $f^{\otimes t}$ against the class of probabilistic circuits. The direct product theorems we prove have quantitative parameters that are far superior to those in Theorem 1.1.

Our first direct product theorem holds for the worst-case setting. We show:

Theorem 1.2. *Let $f = \{f_n\}$ be a family of Boolean functions on n input bits, and suppose that f is "hard for nondeterministic circuits" in the sense that $f \notin \mathsf{NP/poly} \cap \mathsf{coNP/poly}$.*[2]

Now let $100 \leq t(n) \leq \mathrm{poly}(n)$ be a parameter, and let $\{C_n\}_{n>0}$ be any family of polynomial-size, probabilistic circuits outputting $t(n)$ bits. Then for infinitely many choices of n and $x \in \{0,1\}^{n \times t(n)}$,

$$\Pr[C_n(x) = f_n^{\otimes t(n)}(x)] \;<\; \exp\left(-\Omega(t(n))\right) \;.$$

Like all known DPTs in the circuit setting, this result is proved in its contrapositive form; it follows straightforwardly from our Theorem 4.1. The latter is a *nondeterministic direct product reduction*—a method for transforming a probabilistic circuit that weakly approximates $f_n^{\otimes t(n)}$ into a *nondeterministic* circuit that computes f_n with much greater confidence. In the present reduction, we get a nondeterministic circuit that computes f_n exactly. This transformation incurs only a polynomial blowup in circuit size. The reduction is fully black-box, but is not subject to the limitations identified by Rudich due to its use of nondeterminism.

Our next DPT holds for the average-case setting, and applies to input distributions that are efficiently sampleable.

[2] Here, strictly speaking we mean that the language $L_f := f^{-1}(1)$ is not in $\mathsf{NP/poly} \cap \mathsf{coNP/poly}$.

Theorem 1.3. *Let $\{f_n\}$ be a family of Boolean functions on n input bits. Let $\mathcal{D} = \{\mathcal{D}_n\}$ be a family of input distributions, sampleable by a polynomial-size family of circuits. Let $\delta_n \in [.5, 1]$ be a parameter. Suppose that f is "hard for nondeterministic circuits with respect to $\mathcal{D}$" in the sense that, for all families $\{G_n\}$ of polynomial-size nondeterministic circuits, if n is sufficiently large then*

$$\Pr_{\mathbf{x}\sim\mathcal{D}_n}[G_n(\mathbf{x}) = f_n(\mathbf{x})] \;<\; 1 - \varepsilon_n \;.$$ [3]

Now let $100 \leq t(n) \leq \mathrm{poly}(n)$ be a parameter, and let $\{C_n\}_{n>0}$ be any family of polynomial-size, probabilistic circuits outputting $t(n)$ bits. Assume that $\varepsilon_n > \frac{2^{12}}{t(n)^{1/3}}$.

Then for sufficiently large n and $\mathbf{x} \sim \mathcal{D}_n^{\otimes t(n)}$, we have

$$\Pr[C_n(\mathbf{x}) = f_n^{\otimes t(n)}(\mathbf{x})] \;<\; \exp\left(-\Omega\left(\varepsilon_n^{3/2}\sqrt{t(n)}\right)\right) \;.$$

This result follows easily from our Theorem 6.1, a nondeterministic direct product reduction for sampleable distributions. Our two DPTs above, stated for Boolean functions, are special cases of our general results, in which the functions f_n need not be Boolean; there is no adverse dependence in these results on the range size.

Our nondeterministic direct product reductions are not the first use of nondeterministic reductions in the study of average-case complexity. In particular, previous authors have exploited nondeterminism to give worst-case to average-case reductions for computational problems. In [FL97, first version in '92], Feige and Lund gave a nondeterministic worst-case to average-case reduction for computing the Permanent over large fields. We state one of the resulting theorems on worst-case success probability for 0-1 matrices, which is interesting to compare with ours:

Theorem 1.4 ([FL97], Theorem 3.6)**.** *Suppose there is a $\gamma \in (0, 1)$ and a probabilistic polynomial-time algorithm P such that, for any $n \times n$ input matrix X with 0/1 entries, we have*

$$\Pr[P(X) = \mathrm{perm}_{\mathbb{Z}}(X)] \;\geq 2^{-n^{\gamma}} \;.$$

Then, $\mathsf{P}^{\#\mathsf{P}} = \mathsf{PH} = \mathsf{AM}$*.*

Earlier Amir, Beigel, and Gasarch [ABG03, first version in '90] had shown somewhat weaker results for #SAT, the problem of computing the number of satisfying assignments to a Boolean formula. Thus we have long had a good understanding of the worst-case difficulty against PPT algorithms of #P-complete counting problems. We also have quite strong average-case hardness results for #P, assuming $\mathsf{P}^{\#\mathsf{P}} \neq \mathsf{AM}$ [FL97]. However, #P functions are not believed to be computable with the power of NP, or even PH (this would collapse PH, since $\mathsf{PH} \subsetneq \mathsf{P}^{\#\mathsf{P}}$ [Tod91]). This seems to limit the potential applications of the strong hardness of #P functions, e.g., in cryptography.

As another example of the power of nondeterminism for average-case complexity, we mention a work of Trevisan and Vadhan; in the course of constructing deterministic extractors for efficiently sampleable distributions, they gave a nondeterministic worst-case to average-case reduction for the task of computing an arbitrary low-degree polynomial over a finite field [TV00, Lem. 4.1].

[3] In the most common definition, a nondeterministic circuit $G_n(x)$ is said to *compute* a function $g(x)$ if the following condition holds: $g(x) = 1$ iff there exists some setting of the nondeterministic gates of G_n causing it to accept input x. Our Theorem 1.3 is valid if our initial hardness assumption on f_n is with respect to this definition. However, for this result we actually only require hardness with respect to a more restrictive model of nondeterministic computation: the model of *nondeterministic mapping circuits*, described in Section 2.2.

None of these reductions from previous work proceed through a direct product reduction in our sense. However, [ABG03] considers t-fold direct products $f^{\otimes t}$ and gives complexity upper bounds for functions f such that $f^{\otimes t}$ can be computed using few queries to an oracle; some of these reductions use nondeterminism.

1.3 Application to the success probability of PPT SAT solvers

In a recent work, Paturi and Pudlák [PP10] asked about the achievable worst-case success probability of PPT heuristics for circuit satisfiability. They argue for the importance of this question by observing that many of the known exact algorithms for k-SAT and other NP search problems, which achieve exponential runtimes with an improved exponent over naive search, can be converted to *polynomial-time* search heuristics with a success probability attaining nontrivial advantage over random guessing. Thus, exploring the limitations of PPT search heuristics also illuminates the limitations of a very natural paradigm for exponential-time computation.

Paturi and Pudlák show the following powerful result (a special case of a more general theorem): Suppose there is a $\gamma < 1$ and a PPT algorithm P_{solver} that, when given as input a description of any satisfiable Circuit-SAT instance Ψ with r variables, outputs a satisfying assignment to Ψ with probability at least $q(r) := 2^{-\gamma r}$. Then, there is a deterministic circuit family $\{C_r\}_r$ that succeeds at the same task on r-variable instances of size $n \leq \text{poly}(r)$ with probability 1, and C_r is of size at most 2^{r^μ} for some $\mu < 1$.

In fact, Paturi and Pudlák show the conclusion in their result holds even if the algorithm merely outputs *witnesses* of satisfiability for some NP verifier for Circuit-SAT, with the probability guarantee above. The witness need not be a satisfying assignment. (Our own negative results will not hold in the full generality of this setting. However, all intelligent random guessing algorithms known to this author for witnessing satisfiability, work by producing actual satisfying assignments.)

In this work, we exploit a simple connection between direct product computations for the satisfiability decision problem for Boolean formulas, and the task of producing satisfying assignments to such formulas. The connection is simple enough to describe in a single sentence:

($\star$) If $\psi^1, \ldots, \psi^t$ are formulas, and $s \in [0, t]$ is a correct guess for the number of satisfiable ψ^js, then the 0/1 values $[\psi^1 \in SAT], \ldots, [\psi^t \in SAT]$ can all be inferred given any satisfying assignment to the formula $\Psi^{(s)}$ which asks for satisfying assignments to at least s of the ψ^js.

This observation has been used before in [BH88] for quite different purposes, as we will discuss shortly. Using this connection together with our worst-case DPT (Theorem 4.1), we prove the following result, bounding the achievable success probability of polynomial-time heuristics for SAT solvers under the standard complexity-theoretic assumption that NP is not contained in $\mathsf{coNP/poly}$.

Theorem 1.5. *Let $\gamma \in (0, 1)$. Suppose there is a PPT algorithm P_{solver} that, when given as input a description of a satisfiable 3-CNF formula Φ, of description length $|\langle \Phi \rangle| = N$, outputs a satisfying assignment to Φ with probability at least $q(N) := 2^{-N^\gamma}$.*

Then, $\mathsf{NP} \subseteq \mathsf{coNP/poly}$ (and the Polynomial Hierarchy collapses to Σ_3^p).

In fact, the conclusion would hold even if P_{solver} were a non-uniform polynomial-size circuit family rather than a uniform PPT algorithm.

This theorem is incomparable to the result of Paturi and Pudlák. Their result implies a stronger upper bound for the success probability of SAT solvers, at the cost of assuming that NP has nearly-exponential circuit complexity. While we admire this past work (and it gave the original motivation for our project, although our methods are almost completely different), we also believe that it is valuable to understand how much one can infer about the difficulty of NP problems, starting from assumptions about *polynomial-time computation alone*. The hypothesis that the Polynomial Hierarchy does not collapse to Σ_3^p can be equivalently restated as one such assumption: namely, that there is no polynomial-time procedure that reduces a 4-round game, described by a Boolean circuit, to an equivalent 3-round game with the "existential" player taking the first move (see [Pap94, Chap. 17]).

Essentially the same observation ($\star$) above was used earlier by Buss and Hay [BH88] (see also [Pap94, Chap. 17]) to show the equality of complexity classes $\mathsf{P}_{||}^{\mathsf{NP}} = \mathsf{P}^{\mathsf{NP}[\log]}$; that is, poly$(n)$ non-adaptive queries to an NP oracle are equivalent in power to $O(\log(n))$ adaptive queries, at least for solving decision problems in polynomial time.[4] We are not aware of previous work on hardness amplification using ($\star$). However, many past works have used various connections between direct product theorems and the difficulty of NP search problems. Indeed, cryptography's demand for various types of hard-on-average NP search problems has been a prime motivation for the study of hardness amplification as far back as Yao's seminal work [Yao82], and direct product theorems for NP search problems such as preimage-finding have been an central ingredient in this project (see [Gol07, Chap. 2]). In the modern "hardness-versus-randomness" paradigm [NW94, IW97] for obtaining pseudorandom generators (PRGs) under hardness assumptions about $\mathsf{E} = \mathsf{DTIME}[2^{\mathsf{O(n)}}]$, one important step is to apply a direct product theorem to certain *decision problems* lying in E.[5] Hardness amplification has also been previously applied to NP *decision problems* to obtain hard-on-average NP *search problems*, e.g., in a previous work of ours [Dru11, Thm. 5]; the connection used there was more complicated than in our present work, and proved a much stronger hardness for NP search problems under a rather strong assumption on the exponential-time complexity of NP. Beyond this, a great deal of work has been devoted to amplifying average-case hardness *within* the class of NP decision problems (see [O'D02, BT06]); such works avoid both the direct product construction (which produces a non-Boolean function) and the XOR construction (which may produce a decision problem outside of NP). Finally, Robin Moser and Dominik Scheder [MS] have asked whether the achievable worst-case success probability of producing satisfying assignments to *many satisfiable* SAT instances obeys a DPT-like statement, if we first assume that SAT requires exponential time (so that the worst-case success probability of satisfying a *single* satisfiable instance is exponentially small for PPT algorithms). This question remains open.

1.4 On the power of bounded queries

Let us mention a further application of Theorem 1.5 in structural complexity theory. The complexity class PF^A is defined as the set of all functions $f : \{0,1\}^* \rightarrow \{0,1\}^*$ computable by a polynomial-time algorithm with oracle access to the language A. If $q(n) \leq \text{poly}(n)$ is an efficiently computable integer-valued function, the query-bounded analogue $\mathsf{PF}^{A[q(n)]}$ is the corresponding class, under the restriction that the algorithm makes at most $q(n)$ queries to its oracle on a length-n input.

It is considered likely that for every $k > 0$, the class PF^{SAT} is a proper superset of $\mathsf{PF}^{\text{SAT}[n^k]}$, and even of $\mathsf{PF}^{A[n^k]}$ for an *arbitrary* oracle A. This is known to hold under a quite strong assumption

[4] In the reduction used in Buss and Hay's work, the value s is determined by binary search, whereas our reduction simply makes a random guess for s. Our goal is to output the values $[\psi^1 \in SAT], \ldots, [\psi^t \in SAT]$, whereas in [BH88] the goal is to compute some Boolean function of these values.

[5] This is relevant because every PRG must be a one-way function, and the associated preimage-finding task is an NP search problem which must be hard on average.

called the NP *machine hypothesis* [CP07]. However, it is an open question to prove the statement assuming that the Polynomial Hierarchy is infinite. Under the latter assumption, the best that was known previously [ABG03] was that $\mathsf{PF}^{\mathrm{SAT}} \not\subseteq \mathsf{PF}^{\mathrm{SAT}[q(n)]}$ for $q(n) = O(\log n)$.[6]

Consider the function LEXSAT that, on input a description of a Boolean formula, asks for the lexicographically first satisfying assignment, if any exist (otherwise the output is 0, say). By employing binary search, one may easily compute LEXSAT in $\mathsf{PF}^{\mathrm{SAT}[n]}$, where n is the description length of the input formula. Now suppose that LEXSAT were computable with $n^{1-\varepsilon}$ queries to *any* oracle (not necessarily in NP). Then, we could *randomly guess* the outcomes to the oracle calls, and efficiently produce a satisfying assignment to any satisfiable ψ, with success probability $\geq 2^{-n^{1-\varepsilon}}$. By Theorem 1.5, this would imply that $\mathsf{NP} \subseteq \mathsf{coNP/poly}$. We conclude:

Theorem 1.6. *For any $\varepsilon > 0$ and any oracle A, if $\mathsf{PF}^{\mathrm{SAT}[n]} \subseteq \mathsf{PF}^{A[n^{1-\varepsilon}]}$, then $\mathsf{NP} \subseteq \mathsf{coNP/poly}$.*

The approach described here gives equally strong evidence that LEXSAT is not computable in the analogous *bounded-error* class $\mathsf{BPF}^{A[n^{1-\varepsilon}]}$.

1.5 A derandomized DPT for NP languages

In Section 7 we prove a *derandomized* DPT for languages in NP. In this variant, the instances of our decision problem are not truly independent, but are instead drawn according to the *expander walk* pseudorandom generator of [AKS87]. We give a DPT establishing exponential decay of the success probability of computing $f^{\otimes t}$ under this distribution; the quantitative aspects of this result are comparable to that of Theorem 1.2. We speculate that this derandomized variant may be better-suited to some future applications of our results.

1.6 Material deferred to the full version

In the full version we will provide:

1. A quantitatively-improved version of the DPT for sampleable distributions, following a different strategy which involves *randomly permuting* the indices of the t input instances;

2. Discussion of the relation between item 1 and the open question of Moser and Scheder discussed previously in Section 1.3;

3. A discussion of how the results of [ABG03] results can be used to derive (weak) DPTs for the worst-case setting, via hashing techniques in [VV86, PP10]. This does not yield an alternative proof to our results, but it indicates a further connection between our work and that of [ABG03].

1.7 Our techniques

We describe and analyze two main nondeterministic direct product reductions in this work. While there are major technical differences between them, both begin with the same intuition, which we will describe at a high level here.

Let f be a Boolean function on n input bits, and $\mathcal{D}$ a distribution over inputs to f. Suppose C is a probabilistic circuit that computes $f^{\otimes t}$ with some success probability $q > 2^{-ct}$ on inputs

[6] In fact, if $\mathsf{PH} \neq \Sigma_3^p$, then it was shown in [ABG03] that $\mathsf{PF}^{\mathrm{SAT}[q(n)+1]} \not\subseteq \mathsf{PF}^{\mathrm{A}[q(n)]}$ for every A.

$\overline{\mathbf{x}} = (\mathbf{x}^1, \ldots, \mathbf{x}^t) \sim \mathcal{D}^{\otimes t}$, for some small constant $0 < c \ll 1$. We would like to obtain from C a nondeterministic circuit computing f with high success probability with respect to $\mathcal{D}$. (To prove our worst-case direct product reduction, Theorem 4.1, it will suffice to show how to do this for every $\mathcal{D}$. We can then use the minimax theorem to build a nondeterministic circuit that is correct on every input.)

Say that an execution of C is *j-valid*, for $0 \le j \le t$, if it correctly computes f on its first j inputs. We obviously have

$$\Pr\left[C(\overline{\mathbf{x}}) = f^{\otimes t}(\overline{\mathbf{x}})\right] \;=\; \prod_{j \in [t]} \Pr[j\text{-valid}|(j-1)\text{-valid}] \;>\; 2^{-ct} \;.$$

Thus, for a *typical* choice of index j, $\Pr[j\text{-valid}|(j-1)\text{-valid}] \approx 2^{-c} \approx 1$. This motivates us to choose such an index $j = j^*$, and to *fix* some settings $y^1, \ldots, y^{j^*-1}$ to the first (j^*-1) inputs. Then, by storing the values $f(y^1), \ldots, f(y^{j^*-1})$, we can easily *recognize* a (j^*-1)-valid execution (as specified by a setting to the remaining inputs and to the random bits used by C). Now, given a single input $\mathbf{x} \sim \mathcal{D}$ on which we wish to compute f, we will try to obtain a (j^*-1)-valid execution of C on an input-tuple whose first j^* elements are $y^1, \ldots, y^{j^*-1}, \mathbf{x}$. The idea is that, by our choice of j^*, a "typical" such execution (in which the remaining inputs are drawn from $\mathcal{D}^{\otimes(t-j^*)}$) should also be j^*-valid, and give us the value $f(\mathbf{x})$. This idea essentially follows [GNW11]. In our reduction, however, nondeterminism will allow us to obtain a (j^*-1)-valid execution of C very efficiently, even when such executions are extremely rare; we simply need to "guess and check."

This approach requires care, however, because an execution obtained by nondeterministic guessing need not be a representative sample of the population from which it was drawn. Thus, even if we successfully fix values of $y^1, \ldots, y^{j^*-1}$ and receive an input $\mathbf{x} \sim \mathcal{D}$ such that most (j^*-1)-valid executions are also j^*-valid, we need a way to "kill off" the "atypical" (j^*-1)-valid executions which fail to be j^*-valid.

For this task, a natural idea is to try to apply *random hashing*, a well-established tool for reducing the size of a set and culling atypical elements. The use of randomly selected hash functions for such purposes, in conjunction with nondeterministic guessing, was pioneered by Goldwasser and Sipser [GS86] (with related techniques found in [VV86]).[7] This technique has an important requirement, however: to kill all the "atypical" (j^*-1)-valid executions while simultaneously leaving at least one j^*-valid execution alive, we need to know a good approximation to the *probability* of a (j^*-1)-valid execution, conditioned on $y^1, \ldots, y^{j^*-1}, \mathbf{x}$. We want this probability to be predictable with high accuracy based on $y^1, \ldots, y^{j^*-1}$ alone, without any foreknowledge of the input $\mathbf{x}$, so that a good approximation can be encoded into our final nondeterministic circuit as helpful advice. To summarize, we hope to find and fix inputs $y^1, \ldots, y^{j^*-1}$, such that with high probability over $\mathbf{x} \sim \mathcal{D}$, we have:

(i) $\Pr[j^*\text{-valid}|y^1, \ldots, y^{j^*-1}, \mathbf{x}] \;\approx\; \Pr[(j^*-1)\text{-valid}|y^1, \ldots, y^{j^*-1}, \mathbf{x}]$;

(ii) $\Pr[(j^*-1)\text{-valid}|y^1, \ldots, y^{j^*-1}, \mathbf{x}] \;\approx\; \Pr[(j^*-1)\text{-valid}|y^1, \ldots, y^{j^*-1}]$.

[7] We are aiming to build a nondeterministic circuit, not a probabilistic one; but the eventual plan will be to fix a polynomial number of representative hash functions as non-uniform advice. Let us also mention that hash families were used in Paturi and Pudlák's work [PP10] as well, but in a very different way. Those authors used hash functions to *reduce the amount of randomness* used by a SAT solver having a worst-case success probability guarantee, as a step toward transforming a Circuit-SAT instance into an equivalent instance with *fewer variables*.

In each condition above, we will tolerate a $(1 \pm .01)$ multiplicative error in our approximations.

So how do we choose the values $y^1, \ldots, y^{j^*-1}$? The obvious idea is to choose them as independent samples from $\mathcal{D}$, after selecting j^* uniformly at random. However, this approach may *fail* to guarantee condition (i) above, if the successful direct-product computations of C are "concentrated" in a pathological way. For example, it may be that $C(x^1, \ldots, x^t)$ always outputs $f^{\otimes t}(x^1, \ldots, x^t)$ provided the first input x^1 lies in some "good" set $G \subset \{0,1\}^n$ of probability mass $\approx 2^{-ct}$, while if $x^1 \notin G$, then C simply outputs random guesses. In this case, condition (i) fails for a typical setting $x^1 := y^1$. Also, condition (ii) is only useful if the conditional probabilities involved are nonzero, and this may also fail with high probability.

We address these difficulties in two distinct ways in our two direct product reductions:

- In our worst-case reduction (Theorem 4.1), we assume from the start that our C has a probability $\geq q$ of computing $f^{\otimes t}$ under *every* input. Then, the problem of zero probabilities doesn't arise, and the worst-case success guarantee of C turns out to very usefully constrain the effects of conditioning on $y^1, \ldots, y^{j^*-1} \sim \mathcal{D}$.

- In our average-case reduction, we show how to transform C to a second probabilistic circuit $\tilde{C}$ taking some number $t' \ll t$ of n-bit inputs, and whose success probability is $\geq .5q$ on *almost every* t'-tuple from $\mathcal{D}^{\otimes t'}$. We call this key attribute the *input-confidence property*; it turns out to be nearly as nearly as useful as the worst-case guarantee assumed in the previous case.

  To endow C with the input-confidence property, we regard most of the t input positions as auxiliary sources of randomness, and concentrate on computing f on the remaining t' coordinates. This has the effect of "smoothing out" the success probability over the different possible t'-tuples. In this step and its analysis (which uses Kullback-Leibler divergence) we are strongly influenced by Raz's proof of the Parallel Repetition Theorem [Raz98]. Also, in this transformation, we crucially use that $\mathcal{D}$ is sampleable; we need our transformed circuit to generate its own samples from $\mathcal{D}$ in order to be useful.

Let us rename t' as t in the average-case setting, for uniformity of discussion. In either setting, we are then able to show that choosing $j^*, y^1, \ldots, y^{j^*-1}$ randomly as before ensures conditions (i) and (ii) with high probability. This requires careful work, but ultimately derives from elementary facts about the behavior of random sequences (see Lemma 3.4).

Now, in our average-case direct product reduction for sampleable distributions, we can perform hashing over all possible outcomes to $x^{j^*+1}, \ldots, x^t$, weighted by their likelihood under $\mathcal{D}$. In our *worst-case* direct product reduction, $\mathcal{D}$ may not be efficiently sampleable, which causes an additional challenge. In this setting we will show that in fact, it is adequate to draw $x^{j^*+1}, \ldots, x^t$ independently at random from multisets $S_{j^*+1}, \ldots, S_t$, each obtained by sampling a reasonable (polynomial) number of times from $\mathcal{D}$. These "sparsified" versions of $\mathcal{D}$ can be coded into our nondeterministic circuit. The idea of this sparsification and its analysis are somewhat similar to (and inspired by) a sparsification step from our previous work on instance compression [Dru12, Lem. 6.3].

2 Preliminaries

When we speak of *probabilistic polynomial-time (PPT) algorithms*, we refer to any uniform model of classical computation, e.g., multi-tape Turing machines. We assume familiarity with the basic uniform complexity classes P, NP and coNP and the higher levels Σ_k^p, Π_k^p of the Polynomial Hierarchy PH. (For background on complexity classes, consult [AB09, Pap94].)

For a language $L \subseteq \{0,1\}^*$, we let χ_L denote the characteristic function of L. Let $\chi_L|_{=n} : \{0,1\}^n \to \{0,1\}$ denote its restriction to inputs of length n, and let $L_n := L \cap \{0,1\}^n$. If $f : \{0,1\}^n \to \{0,1\}^d$ is a function and $t \in \mathbb{N}^+$, we let $f^{\otimes t} : \{0,1\}^{n \times t} \to \{0,1\}^{d \times t}$, the *$t$-fold direct product of f*, be defined by

$$f^{\otimes t}(x^1, \ldots, x^t) \ := \ (f(x^1), \ldots, f(x^t)) \ .$$

All probability spaces we consider will be finite. For distributions $\mathcal{D}, \mathcal{D}'$ over a finite set U, we let $\mathcal{D}(u) := \Pr_{\mathbf{u} \sim \mathcal{D}}[\mathbf{u} = u]$, and for $U' \subseteq U$ let $\mathcal{D}(U') := \Pr_{\mathbf{u} \sim \mathcal{D}}[\mathbf{u} \in U']$. Let $\mathrm{supp}(\mathcal{D})$, the *support of* $\mathcal{D}$, be defined as $\mathrm{supp}(\mathcal{D}) := \{u : \mathcal{D}(u) > 0\}$. We let $||\mathcal{D} - \mathcal{D}'||_{\mathrm{stat}} := \frac{1}{2}\sum_{u \in U} |\mathcal{D}(u) - \mathcal{D}'(u)|$ denote the statistical distance between $\mathcal{D}$ and $\mathcal{D}'$. Equivalently,

$$||\mathcal{D} - \mathcal{D}'||_{\mathrm{stat}} \ = \ \max_{U' \subseteq U} |\mathcal{D}(U') - \mathcal{D}'(U')| \ .$$

The statistical distance between two random variables X, X' is defined as the statistical distance between their respective distributions.

We use $\mathcal{D} \otimes \mathcal{D}'$ to denote the distribution over pairs $(\mathbf{u}, \mathbf{u}')$ which independently samples $\mathbf{u} \sim \mathcal{D}$ and $\mathbf{u}' \sim \mathcal{D}'$. We let $\mathcal{D}^{\otimes k}$ denote k independent samples from $\mathcal{D}$. For a finite multiset S, we write $\mathbf{a} \in_r S$ to indicate that random variable $\mathbf{a}$ is sampled uniformly from S (with elements weighted by their multiplicity in S). We let $\mathbf{1}[E]$ denote the $0/1$-valued indicator random variable for an event E.

If S, S' are multisets, we use $S \cup S'$ to indicate multiset union, and similarly for other multiset operations.[8] We let $S^{\times k}$ denote the k-fold Cartesian product of S.

We will appeal to the following form of the Chernoff-Hoeffding bound:

Lemma 2.1. *Suppose $X_1, \ldots, X_k$ are independent random variables in the range $[0,1]$, each satisfying $\mathbb{E}[X_i] = \mu$. Let $X_{\mathrm{avg}} := \frac{1}{k}\sum_{i \in [k]} X_i$. Then for $\varepsilon > 0$,*

$$\Pr\left[X_{\mathrm{avg}} \le \mu - \varepsilon\right] \ \le \ \exp\left(-2\varepsilon^2 k\right) \qquad \textit{and} \qquad \Pr\left[X_{\mathrm{avg}} \ge \mu + \varepsilon\right] \ \le \ \exp\left(-2\varepsilon^2 k\right) \ .$$

2.1 Deterministic and probabilistic Boolean circuits

When we refer to *Boolean circuits,* we will consider the model of Boolean circuits with gates from $\{\wedge, \vee, \neg\}$. The $\wedge, \vee$ gates are of fanin two. We let $\mathrm{size}(C)$ denote the total number of gates in a (deterministic, probabilistic, or nondeterministic) Boolean circuit C, including input gates and all other types of gates. Note that $\mathrm{size}(C)$ is within a factor 2 of the number of wires in C.

Boolean circuits may compute multiple-output functions, as follows. We consider every Boolean circuit C to be equipped with an ordering on some nonempty subset of its gates, call these $g_1^*, \ldots, g_d^*$. We then say that C computes the function which on input x, outputs $(g_1^*(x), \ldots, g_d^*(x))$. We denote this function simply as $C(x)$.

A *probabilistic Boolean circuit* is a circuit C which, in addition to having gates for its regular input variables $x = (x_1, \ldots, x_n)$, has an additional designated set of (fanin-zero) "random" gates $r = (r_1, \ldots, r_m)$. We write $C(x)$ to denote the random variable giving the output of C on input x,

[8] The multiplicity of (s, s') in the Cartesian product $S \times S'$ is equal to the product of the multiplicity of s in S with the multiplicity of s' in S'.

when the random gates are set to uniform random values. We write C^{det} to indicate the underlying deterministic circuit with input gates (x, r). For a deterministic or probabilistic Boolean circuit C, we write

$$C : \{0,1\}^m \to \{0,1\}^d$$

to denote that C takes m regular input bits (not including any random gates), and produces d bits of output.

For a deterministic or probabilistic circuit $C : \{0,1\}^n \to \{0,1\}$, a value $\delta \in [0,1]$, a function $f : \{0,1\}^n \to \{0,1\}^d$, and a distribution $\mathcal{D}$ over $\{0,1\}^n$, we say that C $(1-\delta)$-*computes* f *with respect to* $\mathcal{D}$ if $\Pr_{x\sim\mathcal{D}}[C(x) = f(x)] \geq 1 - \delta$.

A *sampling circuit* is a circuit C with no input gates, but with designated "random" gates r and output gates $g_1^*, \ldots, g_d^*$. We say that C *samples* a distribution $\mathcal{D}$ on $\{0,1\}^d$ if a uniformly random setting to r induces output distribution $\mathcal{D}$. We let $C(r)$ denote the output on the setting r to the random gates.

2.2 Nondeterministic circuits and nondeterministic mappings

An *ordinary nondeterministic circuit* is a Boolean circuit C, accompanied with a specification of three sets of special gates in C:

- a set of input gates $x = (x_1, \ldots, x_n)$;
- a set of fanin-zero "nondeterministic" gates $w = (w_1, \ldots, w_m)$;
- a single "accept/reject" gate g_0^*.

We require that the input and nondeterministic gates be disjoint, but otherwise these sets are allowed to overlap. We say that $C(x, w)$ *accepts* (x, w) if $g_0^*(x, w) = 1$, otherwise we say C *rejects* (x, w). We say that C *recognizes* a set $A \subseteq \{0,1\}^n$, if for all $x \in \{0,1\}^n$,

$$x \in A \iff \exists w : C(x, w) \text{ accepts.}$$

If $\mathfrak{C} = \{C_n(x, w)\}_{n>0}$ is a family of nondeterministic circuits, with C_n having n input gates, we say that $\mathfrak{C}$ *recognizes* a language L if each C_n recognizes L_n. The complexity class $\mathsf{NP/poly}$ is defined as $\{L$: there is an ordinary nondeterministic circuit family $\{C_n\}$ recognizing L, with $\mathrm{size}(C_n) \leq \mathrm{poly}(n)\}$. The class $\mathsf{coNP/poly}$ is defined as $\{L : \overline{L} \in \mathsf{NP/poly}\}$.[9] It appears unlikely that $\mathsf{NP} \subseteq \mathsf{coNP/poly}$, as this would imply a collapse of the Polynomial Hierarchy:

Theorem 2.2 ([Yap83]). *If* $\mathsf{NP} \subseteq \mathsf{coNP/poly}$, *then* $\mathsf{PH} = \Sigma_3^p = \Pi_3^p$.

We will also use a fairly standard model of nondeterministic computation for functions with one or more bits of output (see [BLS84, BLS85], and [HO02, Sec. 3.3 and App. A.14] for background); here we specialize the model to the circuit setting and use somewhat different terminology. A *nondeterministic mapping circuit* is a circuit C which, in addition to the three classes of designated gates described above, also has a set of output gates $g_1^*, \ldots, g_d^*$ for some $d > 0$ (these gates may overlap with the other gate-classes). The *mapping defined by* C, denoted $F_C : \{0,1\}^n \to \mathcal{P}\left(\{0,1\}^d\right)$, is defined as

$$F_C(x) := \{v \in \{0,1\}^d : \exists w \in \{0,1\}^m \text{ such that } C \text{ accepts } (x, w) \text{ and } (g_1^*(x, w), \ldots, g_d^*(x, w)) = v\}.$$

We will use the following obvious fact:

[9] (Here, $\overline{L}$ denotes the complement of L.)

Proposition 2.3. *Let L be a language. Suppose there is a family $\{C_n\}_{n>0}$ of nondeterministic mapping circuits, satisfying*

1. *For every n and $x \in \{0,1\}^n$, $F_{C_n}(x) = \{\chi_L(x)\}$;*
2. $\mathrm{size}(C_n) \leq \mathrm{poly}(n)$.

Then, $L \in \mathsf{NP/poly} \cap \mathsf{coNP/poly}$.

We say that a nondeterministic mapping circuit C $(1-\delta)$-*defines* a function $f : \{0,1\}^n \to \{0,1\}^d$ with respect to input distribution $\mathcal{D}$ if $\Pr_{x \sim \mathcal{D}}[F_C(x) = \{f(x)\}] \geq 1 - \delta$.

2.3 Direct-product solvers

Definition 2.4 (Direct-product solvers)**.** *Let $n, d, t \in \mathbb{N}^+$ be fixed, and let $f : \{0,1\}^n \to \{0,1\}^d$ be a function. Let $C : \{0,1\}^{n\times t} \to \{0,1\}^{d\times t}$ be a probabilistic circuit. Let $q, c \in [0,1]$.*

1. *Let $\overline{\mathcal{D}}$ be a distribution over $\{0,1\}^{n\times t}$. We say that C is a* q-direct-product solver for $f^{\otimes t}$ with respect to $\overline{\mathcal{D}}$ *if the following holds: if we sample $\overline{\mathbf{x}} = (\mathbf{x}^1, \ldots, \mathbf{x}^t) \sim \overline{\mathcal{D}}$, then*
$$\Pr\left[C(\overline{\mathbf{x}}) = (f(\mathbf{x}^1), \ldots, f(\mathbf{x}^t))\right] \;\geq\; q \ ,$$
where the probability is taken over $\overline{\mathbf{x}}$ and over the randomness used by C.

2. *We say that the circuit C is a* worst-case q-direct-product solver for $f^{\otimes t}$ *if it satisfies item 1 above for* every *input distribution $\overline{\mathcal{D}}$ over $\{0,1\}^{n\times t}$. Equivalently, for all $(x^1, \ldots, x^t) \in \{0,1\}^{n\times t}$,*
$$\Pr\left[C(x^1, \ldots, x^t) = (f(x^1), \ldots, f(x^t))\right] \;\geq\; q \ .$$

3. *For any $(x^1, \ldots, x^t) \in \{0,1\}^{n\times t}$, define the* confidence
$$\mathrm{conf}(C; x^1, \ldots, x^t) \;:=\; \Pr\left[C(x^1, \ldots, x^t) = (f(x^1), \ldots, f(x^t))\right] \ .$$
We say that C is a (c,q)-input-confident direct-product solver for $f^{\otimes t}$ with respect to $\overline{\mathcal{D}}$ *if the following holds: if we sample $\overline{\mathbf{x}} = (\mathbf{x}^1, \ldots, \mathbf{x}^t) \sim \overline{\mathcal{D}}$, then*
$$\Pr\left[\mathrm{conf}(C; \overline{\mathbf{x}}) \geq q\right] \;\geq\; c \ .$$
(Note that any such C is also a q'-direct-product solver for $f^{\otimes t}$ with respect to $\overline{\mathcal{D}}$, where $q' := qc$.)

4. *We extend each of the above definitions to* families *of circuits and input distributions, in the natural way. Let $d(n), t(n) : \mathbb{N}^+ \to \mathbb{N}^+$, $q(n) : \mathbb{N}^+ \to [0,1]$ be functions. Let $\mathfrak{C} = \{C_n\}_{n>0}$ be a family of probabilistic circuits $C_n : \{0,1\}^{n\times t(n)} \to \{0,1\}^{d(n)\times t(n)}$. Let $\overline{\mathcal{D}} = \{\overline{\mathcal{D}}_n\}_{n>0}$ be a family of distributions over $\{0,1\}^{n\times t(n)}$.*

   We say that $\mathfrak{C}$ is a $q(n)$-direct-product solver for $f^{\otimes t(n)}$ with respect to $\overline{\mathcal{D}}$ *if for any $n > 0$, C_n is a $q(n)$-direct-product solver for $f^{\otimes t(n)}$ with respect to $\overline{\mathcal{D}}_n$. The definitions in items 2 and 3 are extended to circuit and input-distribution families in an analogous fashion.*

If C is a q-direct-product solver for $f^{\otimes t}$ with respect to some input distribution, then we may non-uniformly fix the random gates of C to obtain a deterministic q-direct-product solver for $f^{\otimes t}$ with respect to the same input distribution. This is a standard observation in the study of average-case complexity. Note, however, that there is no obvious analogue of this transformation for for worst-case direct-product solvers, or for input-confident direct product solvers, that would allow us to derandomize while preserving the quality parameters.

2.4 Hash families and their properties

We now introduce a widely-used class of function families called strongly universal hash families. Let U be a finite set, and let $\mathcal{H}$ be a finite family of "hash functions" $h : U \to \mathbb{F}_2^k$. We say that $\mathcal{H}$ is a *strongly universal hash family* if, for all $u, u' \in U$ with $u \neq v$, and for all $z, z' \in \mathbb{F}_2^k$, we have

$$\Pr_{h \in_r \mathcal{H}}[h(u) = z \ \wedge \ h(u') = z'] \ = \ 2^{-2k} \ .$$

We use the following standard, explicit construction:

Proposition 2.5. *Given $k, \ell > 0$, consider $U := \mathbb{F}_2^\ell$. The family of functions*

$$\mathcal{H}^{\ell,k} \ := \ \left\{ \ h_{A,v} : \mathbb{F}_2^\ell \to \mathbb{F}_2^k \ \right\}_{A \in \mathbb{F}_2^{k\times\ell}, v \in \mathbb{F}_2^k}$$

given by

$$h_{A,v}(x) \ := \ Ax + v \qquad \text{(with addition over } \mathbb{F}_2^k\text{)}$$

is a strongly universal hash family.

Lemma 2.6. *Suppose that $k, \ell > 0$, that $U' \subseteq U = \mathbb{F}_2^\ell$, and that $|U'| = \theta \cdot 2^k$, for some $\theta > 0$. Say we select $(A, v) \in_r \mathbb{F}_2^{k\times\ell} \times \mathbb{F}_2^k$; then,*

$$1 - \theta^{-1} < \ \Pr[\ 0^k \in h_{A,v}(U')\ ] \ \leq \ \theta \ . \tag{1}$$

Proof. Let $U' = \{u_1, \ldots, u_m\}$. For $i \in [m]$, define the indicator variable $X_i := [h_{A,v}(u_i) = 0^k]$. Note that $\mathbb{E}[X_i] = 2^{-k}$. Let $S := \sum_{i\in[m]} X_i$. Then $\Pr[0^k \in h_{A,v}(U')] = \Pr[S \geq 1]$, and by Markov's inequality this is at most $\mathbb{E}[S] = \sum_{i\in[m]} 2^{-k} = \theta$. This proves the upper bound.

For the lower bound, note that $[0^k \notin h_{A,v}(U')]$ implies $S = 0$, so that in this case $|S - \mathbb{E}[S]| = \theta$. By Chebyshev's inequality, this occurs with probability at most $\frac{\mathbb{E}[(S-\mathbb{E}[S])^2]}{\theta^2}$. The strongly universal property implies that the random variables $X_i, X_{i'}$ are pairwise independent, so we have

$$\Pr[0^k \notin h_{A,v}(U')] \ \leq \ \frac{\sum_{i\in[m]} \mathbb{E}[(X_i - 2^{-k})^2]}{\theta^2} \ = \ \frac{\theta \cdot 2^k}{\theta^2} \cdot \left(2^{-k}(1 - 2^{-k})\right) \ < \ \frac{1}{\theta}.$$

This gives the lower bound in the Lemma's statement. □

Corollary 2.7. *Suppose that $k, \ell > 0$ and that $U = \mathbb{F}_2^\ell$. Consider two subsets $U_{(\mathrm{i})}, U_{(\mathrm{ii})} \subseteq U$, with $|U_{(\mathrm{i})}| = \theta \cdot 2^k$ and $|U_{(\mathrm{ii})}| = \theta' \cdot 2^k$. If $(A, v) \in_r \mathbb{F}_2^{k\times\ell} \times \mathbb{F}_2^k$, then we have*

$$\Pr[0^k \in (h_{A,v}(U_{(\mathrm{i})}) \setminus h_{A,v}(U_{(\mathrm{ii})}))] \ \geq \ 1 - \theta^{-1} - \theta',$$

where $h_{A,v}$ is as in Proposition 2.5.

Proof. First we apply the lower bound of Lemma 2.6 with $U' := U_{(\mathrm{i})}$ to find that

$$\Pr[0^k \notin h_{A,v}(U_{(\mathrm{i})})] \;\leq\; \theta^{-1} \;.$$

Next we apply the upper bound of Lemma 2.6 with $U' := U_{(\mathrm{ii})}$ to find that

$$\Pr[0^k \in h_{A,v}(U_{(\mathrm{i})})] \;\leq\; \theta' \;.$$

Taking a union bound completes the proof. □

2.5 A general nondeterministic circuit construction

The following technical lemma, which is slightly complicated to state but conceptually simple, will be useful in our proofs of Theorems 4.1 and 6.1. Readers may wish to defer studying the lemma until it is used in its proper context.

Lemma 2.8. *Let $n, d \in \mathbb{N}^+$, and let $f : \{0,1\}^n \to \{0,1\}^d$ be a function. Let $K, N, T \in \mathbb{N}^+$ be additional parameters, and suppose we have identified several sets and mappings, as follows.*

- *For every $u \in \{0,1\}^n$, there is a set $V_u \subseteq \{0,1\}^N$, partitioned into disjoint subsets $\{V_u^z\}_{z\in\{0,1\}^d}$;*
- *For $i \in [T]$, there is a mapping $h_i^* : \{0,1\}^N \to \{0,1\}^K$;*
- *There is a "favorable" set $\mathrm{Fav} \subseteq \{0,1\}^n$.*

Suppose that there is a deterministic circuit $C_{\mathrm{Vtest}}(w,u) : \{0,1\}^{N+u} \to \{0,1\}^{d+1}$ that determines whether $w \in V_u$ and, if so, which subset V_u^z contains w. Suppose too that, for each $i \in [T]$, there is a circuit $C_{h_i^*}$ of size $O(KN)$ that computes h_i^*.

Say that h_i^* is good *for $u \in \{0,1\}^n$ if*

$$0^K \;\in\; h_i^*\left(V_u^{f(u)}\right) \setminus \left(\bigcup_{z\neq f(u)} h_i^*\left(V_u^z\right)\right) \;.$$

Finally, assume the following condition:

- *For every $u \in \mathrm{Fav}$, there are at least $.6T$ indices $i \in [T]$ such that h_i^* is good for u.*

Then, there exists a nondeterministic mapping circuit $C^\dagger$ taking n input bits, such that for all $u \in \mathrm{Fav}$,

$$F_{C^\dagger}(u) \;=\; \{f(u)\} \;;$$

also, we have $\mathrm{size}(C^\dagger) \leq O((\mathrm{size}(C_{\mathrm{Vtest}})KN) \cdot T)$.

Proof. $C^\dagger$ takes input $u \in \{0,1\}^n$ and has nondeterministic variables

$$\overline{w} \;=\; \left(w^1, \ldots, w^T\right) \;\in\; \{0,1\}^{N\times T} \;.$$

The circuit $C^\dagger(u, \overline{w})$ acts as follows:

1. For each $i \in [T]$, define $z^i \in \{0,1\}^d \cup \{\perp\}$ by
$$z^i \ := \ \begin{cases} z & \text{if } w^i \in V_u^z \text{ and } h_i^*(w^i) = 0^K, \\ \perp & \text{otherwise (i.e., if } w^i \notin V_u \text{ or } h_i^*(w^i) \neq 0^K). \end{cases}$$
2. If there exists a $z \in \{0,1\}^d$ such that at least $.6T$ of the strings z^i are equal to z, C' accepts and outputs z (which is necessarily unique). If there is no such z, C' rejects.

That $C^\dagger$ can be implemented in the desired resource bounds is immediate from our assumptions. To prove correctness of the construction, consider any $u \in \mathrm{Fav}$. By our choice of $h_1^*, \ldots, h_T^*$, there is a set $I \subseteq [T]$ of size at least $.6T$ indices i such that h_i^* is good for u. For each such i, there is a string $\hat{w}^i \in V_u^{f(u)}$ for which $h_i^*(\hat{w}^i) = 0^K$. Define an assignment $\overline{w} = (w^1, \ldots, w^T)$ to the nondeterministic gates of C' by letting
$$w^i \ := \ \begin{cases} \hat{w}^i & \text{if } i \in I, \\ 0^N & \text{otherwise.} \end{cases}$$
(Our use of the value 0^N here is arbitrary.) Observe that in the execution of $C^\dagger(u, \overline{w})$, we have $z^i = f(u)$ for each $i \in I$. Thus, $C^\dagger$ accepts $(u, \overline{w})$ and outputs $f(u)$. This shows $f(u) \in F_{C'}(u)$.

To see that $F_{C'}(u) \subseteq \{f(u)\}$, consider any $z \neq f(u)$. Note that, for any $i \in I$ (for which h_i^* is good for u), we cannot have $z^i = z$ under any assignment to $\overline{w}$. Thus the number of i for which $z^i = z$ is at most $.4T$, so $C^\dagger(u, \overline{w})$ cannot accept with output z. This completes the proof of Lemma 2.8. □

3 Stage-based analysis of direct-product computations

In this section we analyze the behavior of direct-product solvers on inputs $(x^1, \ldots, x^t)$ drawn from a known probability distribution $\overline{D}$ over $\{0,1\}^{n \times t}$. The case where $\overline{D}$ is a t-fold product distribution will be of primary interest to us, although some of our lemmas will apply to non-product input distributions.

3.1 Valid outputs and the α, β sequences

Here we make some definitions that will be of central importance.

Definition 3.1 (j-valid outputs)**.** *Let $f : \{0,1\}^n \to \{0,1\}^d$ be a function, let $(x^1, \ldots, x^t) \in \{0,1\}^{n \times t}$, and let $z = (z_1, \ldots, z_t) \in \{0,1\}^{d \times t}$. For $j \in [t]$, say that z is j-*valid for $(x^1, \ldots, x^t)$, with respect to $f^{\otimes t}$, *if*
$$z_\ell \ = \ f(x^\ell) \ , \quad \textit{for all } \ell \leq j \ .$$
When the target function f and the reference strings $x^1, \ldots, x^t$ are clear from the context, we will simply say that z is j-valid. *Note that if z is j-valid for $(x^1, \ldots, x^t)$ then it is also j'-valid for $j' < j$. By convention, every $z \in \{0,1\}^{d \times t}$ is said to be 0-valid.*

If C is a probabilistic circuit taking a tuple of strings $(x^1, \ldots, x^t)$ as input (with each x^j of equal, predetermined length) and outputting a t-bit string, we say that a particular execution of C on input $(x^1, \ldots, x^t)$ is j-valid if it outputs some bitstring that is j-valid with respect to the inputs. We denote this event simply as $[C(x^1, \ldots, x^t)$ is j-valid $]$.

Definition 3.2 (α, β sequences)**.** *Let $n, t \in \mathbb{N}^+$ and let $f : \{0,1\}^n \to \{0,1\}^d$. Let $C : \{0,1\}^{n\times t} \to \{0,1\}^{d\times t}$ be a probabilistic circuit. Let $\overline{\mathcal{D}}$ be a distribution over $\{0,1\}^{n\times t}$, and let $(\mathbf{x}^1, \ldots, \mathbf{x}^t) \sim \overline{\mathcal{D}}$.*

Define two sequences of random variables

$$\alpha_0, \alpha_1, \ldots, \alpha_t \ , \quad \beta_0, \beta_1, \ldots, \beta_{t-1} \ ,$$

as follows. For $j \in [0, t]$, we let

$$\alpha_j \ := \ \Pr\left[C(\mathbf{x}^1, \ldots, \mathbf{x}^t) \text{ is } j\text{-valid} \,\middle|\, \mathbf{x}^1, \ldots, \mathbf{x}^j \right] \ ,$$

with validity defined with respect to f. In other words, if $(\mathbf{x}^1, \ldots, \mathbf{x}^j) = (x^1, \ldots, x^j)$, then α_j takes on the value

$$\alpha_j \ = \ \Pr\left[C(\mathbf{x}^1, \ldots, \mathbf{x}^t) \text{ is } j\text{-valid} \,\middle|\, (\mathbf{x}^1, \ldots, \mathbf{x}^j) = (x^1, \ldots, x^j) \right] \ ,$$

where the probability is taken over the randomness in $\mathbf{x}^1, \ldots, \mathbf{x}^t$ and in the randomness used by C. Similarly, for $j \in [0, t-1]$, define

$$\beta_j \ := \ \Pr\left[C(\mathbf{x}^1, \ldots, \mathbf{x}^t) \text{ is } j\text{-valid} \,\middle|\, \mathbf{x}^1, \ldots, \mathbf{x}^{j+1} \right] \ .$$

Observe that $\alpha_0 = \beta_0 = 1$. Also, we have $\alpha_j, \beta_j \le 1$ and $\alpha_{j+1} \le \beta_j$.

3.2 A lemma on random sequences

Claim 3.3. *1. The function $\ln(1 + x)$, defined on $(-1, \infty)$, satisfies*

$$\ln(1+x) \ \le \ \begin{cases} x - \frac{x^2}{6} & \text{if } x \in (-1,1) \ , \\ (\ln 2)x & \text{if } x \ge 1 \ . \end{cases}$$

2. Consequently, for all $x \in (-1, \infty)$,

$$\ln(1+x) \ \le \ x - \min\left\{ \frac{x^2}{6}, .3 \right\} \ .$$

Proof. **(1)** We have the Taylor series representation

$$\ln(1+x) \ = \ \sum_{n=1}^{\infty} (-1)^{n+1} \frac{x^n}{n} \ , \qquad \text{valid for } x \in (-1,1) \ .$$

This is an alternating series with terms monotonically decreasing in absolute value, so the Leibniz rule for alternating series tells us that $\ln(1+x) \le x - \frac{x^2}{2} + \frac{x^3}{3}$ for $x \in (-1, 1)$. For such x we have $\frac{x^3}{3} \le \frac{x^2}{3}$, which establishes the first half of item 1.

For the other half, observe that the function $f(x) = \ln(1 + x)$ satisfies

$$f'(x) \ = \ \frac{1}{1+x} \ , \quad f''(x) \ = \ -\frac{1}{(1+x)^2} \ < \ 0 \ ,$$

with these expressions valid over its entire domain $(-1,\infty)$. Define the linear function $g(x) := (\ln 2)x$. We have

$$f(1) \; = \; \ln 2 \; = g(1) \quad \text{and} \quad f'(1) \; = \; \frac{1}{2} \; < \; \ln 2 \; = \; g'(1) \; ;$$

combining this with the fact that $f''(x) < 0$ everywhere implies that $f(x) \leq g(x)$ for $x \geq 1$. This completes the proof of item 1.

(2) From item 1 it immediately follows that for $x \in (-1,\infty)$,

$$\ln(1+x) \; \leq \; x - \min\left\{\frac{x^2}{6}, (1-\ln 2)|x|\right\} \; .$$

The first term in the min is smaller for $x \in (-1,1]$, and for $x \geq 1$ we have $(1-\ln 2)|x| > .3$. This proves item 2. □

Lemma 3.4. *Let $Y_1, Y_2, \ldots, Y_T$ be (possibly dependent) nonnegative random variables satisfying $\mathbb{E}[Y_i] \leq 1$ for $i \in [T]$. Let $Y_{\text{prod}} := \prod_{i\in[T]} Y_i$. Let $\mathbf{i} \in_r [T]$ be chosen independently of $Y_1, \ldots, Y_t$.*

1. *Suppose that there is some $q \in (0,1]$ such that $Y_{\text{prod}} \geq q$ with probability 1. Then,*

$$\Pr[Y_{\mathbf{i}} \in [.99, 1.01]] \; \geq \; 1 - \frac{2^{16}\ln(1/q)}{T} \; .$$

2. *Suppose instead that for some $q \in (0,1]$ and $\zeta \in [0,1]$, we have $\Pr[Y_{\text{prod}} \geq q] \geq 1-\zeta$. Then*

$$\Pr\left[Y_{\mathbf{i}} \in [.99, 1.012]\right] \; \geq \; 1 - \frac{2^{16}\ln(1/q)}{T} - 1.1 \cdot 2^{16}\zeta \; .$$

Proof. **(1)** Let $Z_1, \ldots, Z_T$ be defined by $Z_i := \ln(Y_i)$. Note that Z_i is well-defined since $Y_i > 0$, under our assumption $Y_{\text{prod}} \geq q$ in part 1. Letting $Z_{\text{sum}} := \sum_{i\in[T]} Z_i$, note that $Z_{\text{sum}} = \ln(Y_{\text{prod}})$. Our assumption in part 1 implies that $Z_{\text{sum}} \geq \ln q$. Thus,

$$\sum_{i\in[T]} \mathbb{E}[Z_i] \; = \; \mathbb{E}[Z_{\text{sum}}] \; \geq \; \ln q \; . \tag{2}$$

On the other hand, by applying Claim 3.3, item 2, we find that

$$Z_i \; \leq \; (Y_i - 1) - \min\left\{\frac{(Y_i-1)^2}{6}, .3\right\} \; .$$

Taking expectations and using that $\mathbb{E}[Y_i] \leq 1$,

$$\mathbb{E}[Z_i] \; \leq \; -\mathbb{E}\left[\min\left\{\frac{(Y_i-1)^2}{6}, .3\right\}\right] \; .$$

Let $p_i := \Pr[Y_i \notin [.99, 1.01]]$. Then

$$\mathbb{E}\left[\min\left\{\frac{(Y_i-1)^2}{6}, .3\right\}\right] \; \geq \; p_i \cdot \frac{(.01)^2}{6} \; ,$$

so that

$$\mathbb{E}[Z_i] \;\le\; -\frac{p_i}{2^{16}} \,.$$

Combining this with Eq. (2) gives

$$\sum_{i\in[T]} p_i \;\le\; -2^{16}\ln q \;=\; 2^{16}\ln(1/q) \,,$$

which implies that

$$\Pr_{\mathbf{i}\in_r[T]}[Y_{\mathbf{i}} \notin [.99, 1.01]] \;=\; \frac{1}{T}\sum_{i\in[T]} p_i \;\le\; \frac{2^{16}\ln(1/q)}{T} \,,$$

as was to be shown.

(2) Note that if $\zeta > .001$, the assertion being made is trivial, since probabilities are always nonnegative. So let us assume that $\zeta \in [0, .001]$. Let $(Y'_1, \ldots, Y'_T)$ be random variables jointly distributed as $(Y_1, \ldots, Y_T)$ conditioned on the event $[Y_{\text{prod}} \ge q]$. That is, for any $(y_1, \ldots, y_T) \in \mathbb{R}^T$, $\Pr[(Y'_1, \ldots, Y'_T) = (y_1, \ldots, y_T)] = \Pr[(Y_1, \ldots, Y_T) = (y_1, \ldots, y_T) | Y_{\text{prod}} \ge q]$. Let $c := 1 - \zeta$; our assumption in part 2 implies that $\mathbb{E}[Y_i] \ge c \cdot \mathbb{E}[Y'_i]$, which gives $\mathbb{E}[Y'_i] \le 1/c$.

Now let $Y''_i := cY'_i$; we have $Y''_i > 0$ and $\mathbb{E}[Y''_i] \le 1$. Let $Y''_{\text{prod}} := \prod_{i\in[T]} Y''_i$. We have $Y''_{\text{prod}} \ge c^T q$ always. Thus we may apply item 1 to the sequence $Y''_1, \ldots, Y''_T$ to find that

$$\Pr_{\mathbf{i}\in_r[T]}\left[Y'_{\mathbf{i}} \in \left[\frac{.99}{c}, \frac{1.01}{c}\right]\right] \;=\; \Pr_{\mathbf{i}\in_r[T]}[Y''_{\mathbf{i}} \in [.99, 1.01]] \;\ge\; 1 - \frac{2^{16}\ln\left(\frac{1}{c^T q}\right)}{T} \,. \tag{3}$$

Then it follows from our definitions that

$$\Pr_{\mathbf{i}\in_r[T]}\left[Y_{\mathbf{i}} \in \left[\frac{.99}{c}, \frac{1.01}{c}\right]\right] \;\ge\; c \cdot \Pr_{\mathbf{i}\in_r[T]}\left[Y'_{\mathbf{i}} \in \left[\frac{.99}{c}, \frac{1.01}{c}\right]\right] \,.$$

Next, note that our assumption $c \in [.999, 1]$ implies that $[.99/c, 1.01/c] \subseteq [.99, 1.012]$, and also that $1/c = 1/(1-\zeta) \le 1 + 1.01\zeta$. Using these facts and Eq. (3), we derive the bounds

$$\begin{aligned}
\Pr_{\mathbf{i}\in_r[T]}[Y_{\mathbf{i}} \in [.99, 1.012]] \;&\ge\; \Pr_{\mathbf{i}\in_r[T]}\left[Y_{\mathbf{i}} \in \left[\frac{.99}{c}, \frac{1.01}{c}\right]\right] \\
&\ge\; c \cdot \left(1 - \frac{2^{16}\ln\left(\frac{1}{c^T q}\right)}{T}\right) \\
&\ge\; 1 - \zeta - \frac{2^{16}\ln\left(\frac{1}{c^T q}\right)}{T} \\
&\ge\; 1 - \zeta - \frac{2^{16}\ln\left(\frac{(1+1.01\zeta)^T}{q}\right)}{T} \\
&=\; 1 - \zeta - \frac{2^{16}T \cdot \ln(1 + 1.01\zeta)}{T} - \frac{2^{16}\ln(1/q)}{T} \\
&\ge\; 1 - 1.1 \cdot 2^{16}\zeta - \frac{2^{16}\ln(1/q)}{T} \,,
\end{aligned}$$

where in the last step we used the bound $\ln(1 + x) \le x$. This proves part 2. □

3.3 Behavior of the α, β sequences

Lemma 3.5. *Fix $n, d, t \in \mathbb{N}^+$. Let $f : \{0,1\}^n \to \{0,1\}^d$ be a function, and let $C : \{0,1\}^{n \times t} \to \{0,1\}^{d \times t}$ be a probabilistic circuit. Let $q \in (0,1]$ and $\zeta \in [0,1]$ be given.*

1. *Suppose that C is a $(1-\zeta, q)$-input-confident direct-product solver for $f^{\otimes t}$ with respect to an input distribution $\overline{\mathcal{D}}$ over $\{0,1\}^{n \times t}$.*

   Let $\overline{\mathbf{x}} = (\mathbf{x}^1, \ldots, \mathbf{x}^t) \sim \overline{\mathcal{D}}$. Let $\alpha_0, \ldots, \alpha_t, \beta_0, \ldots, \beta_{t-1}$ be as in Definition 3.2, defined with respect to C and $\overline{\mathcal{D}}$. Let $\mathbf{j} \in_r [t]$ be sampled independently of $\overline{\mathbf{x}}$. Then with probability at least

   $$1 - \frac{2^{16} \ln(1/q)}{t} - 2^{18}\zeta \ ,$$

   we have

   $$\alpha_{\mathbf{j}-1}, \beta_{\mathbf{j}-1} \ > \ 0 \ , \quad \left(\frac{\beta_{\mathbf{j}-1}}{\alpha_{\mathbf{j}-1}}\right) \in [.99, 1.012] \ , \quad \text{and} \quad \left(\frac{\alpha_{\mathbf{j}}}{\beta_{\mathbf{j}-1}}\right) \in [.99, 1] \ . \tag{4}$$

2. *Now suppose instead that C is a worst-case q-direct-product solver for $f^{\otimes t}$. Let V be a finite set and let $\{\overline{\mathcal{D}}_v\}_{v \in V}$ be a set of distributions indexed by V, with each distribution over $\{0,1\}^{n \times t}$.*

   Let $\mathfrak{D}, \mathfrak{D}'$ be two distributions over $V \times [t]$, with the following properties:

   (a) If $(\mathbf{v}, \mathbf{j}) \sim \mathfrak{D}$, then $\mathbf{v}, \mathbf{j}$ are independent and $\mathbf{j}$ is uniform over $[t]$;

   (b) $||\mathfrak{D} - \mathfrak{D}'|| \le \gamma$, for some $\gamma \in [0,1)$.

   Consider the following experiment $\mathbf{Expt}(\mathfrak{D}')$*:*

   (i) Sample $(\mathbf{v}', \mathbf{j}') \sim \mathfrak{D}'$;

   (ii) Sample $\overline{\mathbf{x}} = (\mathbf{x}^1, \ldots, \mathbf{x}^t) \sim \overline{\mathcal{D}}_{\mathbf{v}'}$;

   (iii) Let the sequence $\alpha_0, \ldots, \alpha_t, \beta_0, \ldots, \beta_{t-1}$ as in Definition 3.2 be defined with respect to $\overline{\mathcal{D}}_{\mathbf{v}'}$ and $\overline{\mathbf{x}}$.

   Then with probability at least

   $$1 - \frac{2^{16} \ln(1/q)}{t} - \gamma$$

   over $\mathbf{Expt}(\mathfrak{D}')$*, we have*

   $$\left(\frac{\beta_{\mathbf{j}-1}}{\alpha_{\mathbf{j}-1}}\right) \in [.99, 1.02] \quad \text{and} \quad \left(\frac{\alpha_{\mathbf{j}}}{\beta_{\mathbf{j}-1}}\right) \in [.99, 1] \ . \tag{5}$$

Part 1 of Lemma 3.5 will be applied to prove Theorem 6.1, our DPT for sampleable distributions, and also to prove part 2. Part 2 of the Lemma will be applied in the proof of Theorem 4.1, our DPT for worst-case direct-product solvers.

Proof. **(1)** Let $T := 2t$, and define random variables $Y_1, \ldots, Y_T$ as follows: for each $\ell \in [T]$, if $\ell = 2k+1$ then let

$$Y_\ell := \begin{cases} \beta_k / \alpha_k & \text{if } \alpha_k \neq 0 \ , \\ 1 & \text{otherwise.} \end{cases}$$

If $\ell = 2k$, let

$$Y_\ell \; := \; \begin{cases} \alpha_k/\beta_{k-1} & \text{if } \beta_{k-1} \neq 0 \ , \\ 1 & \text{otherwise.} \end{cases}$$

To illustrate the pattern, if all α_k, β_k are nonzero in some outcome then we have

$$Y_1 \;=\; \left(\frac{\beta_0}{\alpha_0}\right) \;=\; 1 \ , \ Y_2 \;=\; \left(\frac{\alpha_1}{\beta_0}\right) \ , Y_3 \;=\; \left(\frac{\beta_1}{\alpha_1}\right) \ , \ \ldots , \ Y_T \;=\; \left(\frac{\alpha_t}{\beta_{t-1}}\right) \ .$$

Observe that if $\alpha_t > 0$, then all of $\alpha_0, \ldots, \alpha_{t-1}, \beta_0, \ldots, \beta_{t-1}$ are also positive, so that the product $Y_{\text{prod}} := \prod_{\ell \in [T]} Y_\ell$ equals $\alpha_t/\alpha_0 = \alpha_t$. By the definition of α_t and the input-confidence property of C, it follows that

$$\Pr\left[Y_{\text{prod}} \geq q\right] \;\geq\; 1 - \zeta \ .$$

For the even indices, we have $Y_{2k} \leq 1$ always. Also, we claim that $\mathbb{E}[Y_{2k+1}] = 1$. To see this, just observe that for $k \in [t(n)]$ we have the identity $\mathbb{E}\left[\beta_k | \alpha_k\right] = \alpha_k$, which tells us that Y_{2k+1} has expected value 1 conditioned on any nonzero value of α_k; and if we condition on $[\alpha_k = 0]$, then $Y_{2k+1} = 1$ with certainty.

We have verified that the assumptions of Lemma 3.4, part 2 are satisfied by $(Y_1, \ldots, Y_T)$; we infer that if $\mathbf{i} \in_r [T]$,

$$\Pr\left[Y_{\mathbf{i}} \notin [.99, 1.012]\right] \;\leq\; \frac{2^{16} \ln(1/q)}{T} + 1.1 \cdot 2^{16}\zeta \;=\; \frac{2^{15} \ln(1/q)}{t} + 1.1 \cdot 2^{16}\zeta \ .$$

Recall that $T = 2t$ is even. If we instead choose $\hat{\mathbf{i}} \in_r \{1, 3, 5, \ldots, T-1\}$, and then select $\hat{\mathbf{i}}' \in_r \{\hat{\mathbf{i}}, \hat{\mathbf{i}}+1\}$, then $\hat{\mathbf{i}}'$ is uniform over $[T]$ and we get the same bound for $\Pr\left[Y_{\hat{\mathbf{i}}'} \notin [.99, 1.012]\right]$. It follows that

$$\Pr\left[Y_{\hat{\mathbf{i}}} \notin [.99, 1.012] \ \vee \ Y_{\hat{\mathbf{i}}+1} \notin [.99, 1.012]\right] \;\leq\; \frac{2^{16} \ln(1/q)}{t} + 1.1 \cdot 2^{17}\zeta \ .$$

Now, note that $\mathbf{j} := \hat{\mathbf{i}}/2$ is distributed as a uniform element in $[t]$, and that the relations

$$\alpha_{\mathbf{j}-1}, \beta_{\mathbf{j}-1} \;>\; 0 \ , \quad Y_{\hat{\mathbf{i}}} \;=\; \left(\frac{\beta_{\mathbf{j}-1}}{\alpha_{\mathbf{j}-1}}\right) \ , \quad Y_{\hat{\mathbf{i}}+1} \;=\; \left(\frac{\alpha_{\mathbf{j}}}{\beta_{\mathbf{j}-1}}\right)$$

hold whenever $\alpha_t > 0$, which happens with probability at least $1 - \zeta$. Finally, if $\alpha_t > 0$ then $\beta_{\mathbf{j}-1} > 0$ and $\left(\frac{\alpha_{\mathbf{j}}}{\beta_{\mathbf{j}-1}}\right) \leq 1$. So Eq. (4) holds with probability at least

$$1 - \frac{2^{16} \ln(1/q)}{t} - 2^{18}\zeta \ .$$

This proves part 1 of the Lemma.

(2) First, suppose we run the alternative experiment $\mathbf{Expt}(\mathfrak{D})$, which samples $(\mathbf{v}', \mathbf{j}')$ according to $\mathfrak{D}$ rather than $\mathfrak{D}'$. Now, after conditioning upon any outcome $[\mathbf{v}' = v]$ of the first component, the index $\mathbf{j}$ remains uniform over $[t]$ (by property (a) of $\mathfrak{D}$). Also, C is a $(1, q)$-input-confident direct-product solver for $f^{\otimes t}$ with respect to the input distribution $\overline{\mathcal{D}}_v$. Thus we may set $\overline{\mathcal{D}} := \overline{\mathcal{D}}_v$ and $\zeta := 0$, and apply Lemma 3.5, part 1 to find that the probability that Eq. (5) holds is at least $1 - \frac{2^{16} \ln(1/q)}{t}$. Thus in $\mathbf{Expt}(\mathfrak{D})$, Eq. (5) holds with probability at least $1 - \frac{2^{16} \ln(1/q)}{t}$.

Now let $\mathbf{I}, \mathbf{I}'$ be the indicator variables for the events that Eq. (5) holds in $\mathbf{Expt}(\mathfrak{D}), \mathbf{Expt}(\mathfrak{D}')$ respectively. Note that the two experiments are identically defined, except that the first draws a single sample from $\mathfrak{D}$ while the second draws a sample from $\mathfrak{D}'$. Thus, $||\mathbf{I} - \mathbf{I}'||_{\text{stat}} \leq ||\mathfrak{D} - \mathfrak{D}'||_{\text{stat}} \leq \gamma$, using property (b). This proves part 2 of the Lemma. □

3.4 Analysis of worst-case direct-product solvers: the key experiment

Lemma 3.6. *Fix $n, d, t, M \in \mathbb{N}^+$ with $M \geq 2$, and $q \in (0,1], \zeta \in [0,1]$. Let $f : \{0,1\}^n \to \{0,1\}^d$ be a function, and suppose the probabilistic circuit C is a worst-case q-direct-product solver for $f^{\otimes t}$. Let $\mathcal{D}$ be a distribution over $\{0,1\}^n$, and consider the following experiment $\mathbf{Expt}^*(\mathcal{D})$:*

1. *Let $\mathbf{u} \in \{0,1\}^n$ be sampled according to $\mathcal{D}$, and let $\mathbf{j} \in_r [t]$;*
2. *For each $j \in [t]$:*
   - *(i) let $s_j \in_r \{M, M+1, M+2, \ldots, 2M-1\}$;*
   - *(ii) Define a multiset S_j over $\{0,1\}^n$, obtained by drawing s_j independent samples from $\mathcal{D}$;*
   - *(iii) Let $\hat{S}_j := S_j \cup \{\mathbf{u}\}$ if $j = \mathbf{j}$; otherwise let $\hat{S}_j := S_j$;*
   - *(iv) Let $\mathbf{y}^j \in_r S_j$;*
   - *(v) Let $\hat{\mathbf{y}}^j := \mathbf{u}$ if $j = \mathbf{j}$; otherwise let $\hat{\mathbf{y}}^j := \mathbf{y}^j$.*
3. *Define the random variables*

$$\alpha_0, \alpha_1, \ldots, \alpha_t, \quad \beta_0, \beta_1, \ldots, \beta_{t-1}, \quad \hat{\alpha}_0, \hat{\alpha}_1, \ldots, \hat{\alpha}_t, \quad \hat{\beta}_0, \hat{\beta}_1, \ldots, \hat{\beta}_{t-1} \ ,$$

by the rules

$$\alpha_j \ := \ \Pr\left[C(\mathbf{y}^1, \ldots, \mathbf{y}^t) \text{ is } j\text{-valid} \ \middle| \ S_1, S_2, \ldots, S_t, \mathbf{y}^1, \ldots, \mathbf{y}^j \right] \ ,$$

$$\hat{\alpha}_j \ := \ \Pr\left[C(\hat{\mathbf{y}}^1, \ldots, \hat{\mathbf{y}}^t) \text{ is } j\text{-valid} \ \middle| \ \hat{S}_1, \hat{S}_2, \ldots, \hat{S}_t, \hat{\mathbf{y}}^1, \ldots, \hat{\mathbf{y}}^j \right] \ ,$$

$$\beta_j \ := \ \Pr\left[C(\mathbf{y}^1, \ldots, \mathbf{y}^t) \text{ is } j\text{-valid} \ \middle| \ S_1, S_2, \ldots, S_t, \mathbf{y}^1, \ldots, \mathbf{y}^{j+1} \right] \ ,$$

$$\hat{\beta}_j \ := \ \Pr\left[C(\hat{\mathbf{y}}^1, \ldots, \hat{\mathbf{y}}^t) \text{ is } j\text{-valid} \ \middle| \ \hat{S}_1, \hat{S}_2, \ldots, \hat{S}_t, \hat{\mathbf{y}}^1, \ldots, \hat{\mathbf{y}}^{j+1} \right] \ .$$

Then with probability at least $1 - \frac{2^{16}\ln(1/q)}{t} - \frac{1}{M}$, we have

$$\left(\frac{\hat{\beta}_{\mathbf{j}-1}}{\alpha_{\mathbf{j}-1}} \right) \in [.98, 1.02] \quad \text{and} \quad \left(\frac{\hat{\alpha}_{\mathbf{j}}}{\hat{\beta}_{\mathbf{j}-1}} \right) \in [.99, 1] \ . \tag{6}$$

Proof. We aim to apply part 2 of Lemma 3.5 to the sequences $\hat{\alpha}_0, \ldots, \hat{\alpha}_t, \hat{\beta}_0, \ldots, \hat{\beta}_t$. Let $\mathbb{S}, \hat{\mathbb{S}}$ denote the random tuples $(S^1, \ldots, S^t)$ and $(\hat{S}^1, \ldots, \hat{S}^t)$ respectively. Let $\mathfrak{D}$ denote the distribution governing the tuple $(\mathbb{S}, \mathbf{j})$, and let $\mathfrak{D}'$ denote the distribution governing $(\hat{\mathbb{S}}, \mathbf{j})$. Each t-tuple $\overline{B} = (B_1, \ldots, B_t)$ of multisets over $\{0,1\}^n$ naturally defines a distribution $\overline{\mathcal{D}}_{\overline{B}}$ over elements $(\mathbf{z}^1, \ldots, \mathbf{z}^t) \in \{0,1\}^{n \times t}$, namely, the product distribution that independently chooses $\mathbf{z}^j \in_r B_j$ for each j.

The random variable $\mathbf{j}$ is uniform over $[t]$ and independent of $\mathbb{S}$, so condition (a) of Lemma 3.5, part 2 is satisfied by $\mathfrak{D}$. For condition (b), note that $\hat{\mathbb{S}}$ is not fully independent of $\mathbf{j}$. However, we will show that $(\hat{\mathbb{S}}, \mathbf{j})$ is quite close in distribution to $(\mathbb{S}, \mathbf{j})$:

Claim 3.7. $\left|\left|(\hat{S}_1, \ldots, \hat{S}_t, \mathbf{j}) - (S_1, \ldots, S_t, \mathbf{j})\right|\right|_{\mathrm{stat}} \ \le \ \frac{1}{M}$.

Proof. We use a coupling argument. First, we generate a random multiset S_0 consisting of M independent samples from $\mathcal{D}$. Now define a random multiset $\tilde{S}$ by letting

$$\tilde{S} \ := \ \begin{cases} \hat{S}_{\mathbf{j}} & \text{if } s_{\mathbf{j}} \ < \ 2M-1 \ , \\ S_0 & \text{if } s_{\mathbf{j}} \ = \ 2M-1 \ . \end{cases}$$

Note that $|\tilde{S}|$ is uniform over $\{M, M+1, \ldots, 2M-1\}$, and its elements are distributed as independent samples from $\mathcal{D}$. Thus, if we form the random tuple

$$(S_1, \ldots, S_{\mathbf{j}-1}, \tilde{S}, S_{\mathbf{j}+1}, \ldots, S_t, \mathbf{j}) \ ,$$

we see that it is identically distributed to $(S_1, \ldots, S_{\mathbf{j}}, \ldots, S_t, \mathbf{j})$. Also, we have $\tilde{S} \ = \ \hat{S}_{\mathbf{j}}$ unless $s_{\mathbf{j}} = 2M-1$, which happens only with probability $\frac{1}{M}$; and we always have $\hat{S}_j = S_j$ for all $j \neq \mathbf{j}$. This proves our Claim. □

Thus condition (b) is satisfied by $\mathfrak{D}, \mathfrak{D}'$ with $\gamma := \frac{1}{M}$.

Observe that, after conditioning on $\mathbb{S}$, the sequence $(\mathbf{y}^1, \ldots, \mathbf{y}^t)$ sampled in $\mathbf{Expt}^*(\mathcal{D})$ is distributed precisely according to $\overline{\mathcal{D}}_{\mathbb{S}}$. Similarly, after conditioning on $\hat{\mathbb{S}}$, the sequence $(\hat{\mathbf{y}}^1, \ldots, \hat{\mathbf{y}}^t)$ is distributed according to $\overline{\mathcal{D}}_{\hat{\mathbb{S}}}$. We can therefore combine part 2 of Lemma 3.5 with Claim 3.7 to find that, with probability at least $1 - \frac{2^{16}\ln(1/q)}{t} - \frac{1}{M}$ over $\mathbf{Expt}^*(\mathcal{D})$, we have

$$\left(\frac{\hat{\beta}_{\mathbf{j}-1}}{\hat{\alpha}_{\mathbf{j}-1}}\right) \ \in \ [.99, 1.012] \quad \text{and} \quad \left(\frac{\hat{\alpha}_{\mathbf{j}}}{\hat{\beta}_{\mathbf{j}-1}}\right) \ \in \ [.99, 1] \ .$$

Next we will need the following simple but important claim:

Claim 3.8. *With probability 1 we have*

$$\hat{\alpha}_{\mathbf{j}-1} \ = \ \frac{1}{s_{\mathbf{j}}+1} \cdot \hat{\beta}_{\mathbf{j}-1} + \left(\frac{s_{\mathbf{j}}}{s_{\mathbf{j}}+1}\right) \cdot \alpha_{\mathbf{j}-1} \ .$$

Proof. Consider any outcome of $\mathbf{Expt}^*(\mathcal{D})$, which is fully determined by the values of the random variables

$$(S_1, \ldots, S_t, \mathbf{y}^1, \ldots, \mathbf{y}^t, \mathbf{j}, \mathbf{u}) \ = \ (S_1^*, \ldots, S_t^*, y^1, \ldots, y^t, j, u) \ .$$

Under these conditionings, observe that $\hat{\alpha}_{\mathbf{j}-1}$ equals the probability that the output of the computation $C(y^1, \ldots, y^{j-1}, \mathbf{z}^j, \mathbf{z}^{j+1}, \ldots, \mathbf{z}^t)$ is $(j-1)$-valid, where

$$(\mathbf{z}^j, \mathbf{z}^{j+1}, \ldots, \mathbf{z}^t) \ \in_r \ ((S_j^* \cup \{u\}) \times S_{j+1}^* \times \ldots \times S_t^*) \ .$$

This distribution on $(\mathbf{z}^j, \mathbf{z}^{j+1}, \ldots, \mathbf{z}^t)$ can be equivalently realized as follows:

1. First, let $\mathbf{a} \in_r [s_j + 1]$ (noting here that $s_j = |S_j^*|$);

2. If $\mathbf{a} = s_j + 1$, let $\mathbf{z}^j := u$ and sample $(\mathbf{z}^{j+1}, \ldots, \mathbf{z}^t) \in_r (S_{j+1}^* \times \ldots \times S_t^*)$; otherwise choose $(\mathbf{z}^j, \mathbf{z}^{j+1}, \ldots, \mathbf{z}^t) \in_r (S_j^* \times S_{j+1}^* \times \ldots \times S_t^*)$.

On the other hand, $\hat{\beta}_{\mathbf{j}-1}$ equals the probability that $C(y^1, \ldots, y^{j-1}, u, \mathbf{z}^{j+1}, \mathbf{z}^{j+2}, \ldots, \mathbf{z}^t)$ is $(j-1)$-valid, where $(\mathbf{z}^{j+1}, \ldots, \mathbf{z}^t) \in_r (S^*_{j+1} \times \ldots \times S^*_t)$; and $\alpha_{\mathbf{j}-1}$ equals the probability that $C(y^1, \ldots, y^{j-1}, \mathbf{z}^j, \mathbf{z}^{j+1}, \ldots, \mathbf{z}^t)$ is $(j-1)$-valid, where $(\mathbf{z}^j, \ldots, \mathbf{z}^t) \in_r (S^*_j \times \ldots \times S^*_t)$. Combining these facts with our observations about $\hat{\alpha}_{\mathbf{j}-1}$ yields the Claim. □

Now, suppose that

$$\hat{\beta}_{\mathbf{j}-1} \ \geq \ .99 \cdot \hat{\alpha}_{\mathbf{j}-1} \ ,$$

which, as we have seen, occurs with high probability. Using Claim 3.8, this implies that

$$\frac{\hat{\beta}_{\mathbf{j}-1}}{.99} \ \geq \ \frac{1}{s_{\mathbf{j}}+1} \cdot \hat{\beta}_{\mathbf{j}-1} + \left(\frac{s_{\mathbf{j}}}{s_{\mathbf{j}}+1}\right) \cdot \alpha_{\mathbf{j}-1} \ ,$$

so that

$$\left(\frac{1}{.99} - \frac{1}{s_{\mathbf{j}}+1}\right) \cdot \frac{\hat{\beta}_{\mathbf{j}-1}}{\alpha_{\mathbf{j}-1}} \ \geq \ \left(\frac{s_{\mathbf{j}}}{s_{\mathbf{j}}+1}\right) \ ,$$

which simplifies to

$$\frac{\hat{\beta}_{\mathbf{j}-1}}{\alpha_{\mathbf{j}-1}} \ \geq \ \left(\frac{99 s_{\mathbf{j}}}{100 s_{\mathbf{j}}+1}\right) \ .$$

This is greater than .98. By a similar calculation, if $\hat{\beta}_{\mathbf{j}-1} \ \leq \ 1.012 \cdot \hat{\alpha}_{\mathbf{j}-1}$ then

$$\frac{\hat{\beta}_{\mathbf{j}-1}}{\alpha_{\mathbf{j}-1}} \ \leq \ \left(\frac{1012 \cdot s_{\mathbf{j}}}{1000 s_{\mathbf{j}} - 12}\right) \ ,$$

which is less than 1.02 since $s_{\mathbf{j}} \geq 2$. Combining our work, we conclude that with probability at least $1 - \frac{2^{16}\ln(1/q)}{t} - \frac{1}{M}$, Eq. (6) is satisfied. This completes the proof of Lemma 3.6. □

4 The main DPT for worst-case direct-product solvers

In this section, we prove:

Theorem 4.1. *Let $n, d, t \in \mathbb{N}^+$, with $t \geq 100$. Let $q \in (0,1]$, and let $f : \{0,1\}^n \to \{0,1\}^d$ be a function. Suppose there is a probabilistic circuit $C : \{0,1\}^{n \times t} \to \{0,1\}^{d \times t}$, such that C is a worst-case q-direct-product solver for $f^{\otimes t}$. Assume that*

$$q \ \geq \ \exp\left(-\frac{t}{3 \cdot 10^5}\right) \ .$$

Then, there is a nondeterministic mapping circuit C^* with n input bits and d output bits, such that $F_{C^*}(u) = \{f(u)\}$ for every $u \in \{0,1\}^n$, and for which

$$\text{size}(C^*) \ \leq \ \text{poly}(\text{size}(C)) \ .$$

Theorem 1.2 from the Introduction follows from this more general result:

Proof of Theorem 1.2. Let $f = \{f_n\}$ satisfy the hypothesis of Theorem 1.2. Suppose for contradiction's sake that there is a family of probabilistic circuits $\{C_n\}$ of size at most n^k for some $k > 0$, such that for all sufficiently large n and all $x \in \{0,1\}^{n \times t(n)}$,

$$q \ := \ \Pr[C_n(x) = f_n^{\otimes t(n)}(x)] \ \geq \ \exp\left(-\frac{t(n)}{3 \cdot 10^5}\right) \ .$$

Then by applying Theorem 4.1, to sufficiently large values of n, we find that there is a family $\{C_n^*\}$ of nondeterministic mapping circuits on n input bits, each with a single output bit, such that for all $u \in \{0,1\}^n$,

$$F_{C_n^*}(u) \ = \ \{f_n(u)\} \ ,$$

and satisfying

$$\mathrm{size}(C_n^*) \ \leq \mathrm{poly}(\mathrm{size}(C_n)) = \mathrm{poly}(n^k) \ = \mathrm{poly}(n) \ .$$

By Proposition 2.3, we conclude that $f \in \mathsf{NP/poly} \cap \mathsf{coNP/poly}$. This contradicts our initial hypothesis, proving the Theorem. □

Proof of Theorem 4.1. Let $\delta := \frac{10^5 \ln(1/q)}{t}$. Note that $\delta < .49$ by our assumption on q. As our main technical effort in this section, we will prove the following lemma:

Claim 4.2. *For any distribution $\mathcal{D}$ over $\{0,1\}^n$, there is a nondeterministic mapping circuit $C' = C'_{\mathcal{D}}$ that $(1-\delta)$-defines f with respect to $\mathcal{D}$, and for which* $\mathrm{size}(C') \leq \mathrm{size}(C)^a$ *for some $a > 0$.*

We defer the proof of Claim 4.2. Our Theorem follows from this Claim by a standard type of minimax argument (following [Yao77]), which we give next. Consider the following two-player, simultaneous-move, zero-sum game G:

- **Player 1:** Chooses an input $u \in \{0,1\}^n$;
- **Player 2:** Chooses a nondeterministic mapping circuit C' with n input bits and d output bits, for which $\mathrm{size}(C') \leq \mathrm{size}(C)^a$;
- **Payoff to Player 2:** A reward of 1 if $F_{C'}(u) = \{f(u)\}$, or 0 otherwise.

By our Claim, for every mixed strategy $u \sim \mathcal{D}$ Player 1 may use, there is a pure strategy $C'_{\mathcal{D}}$ for Player 2 that gives expected payoff greater than .51 for Player 2. By the minimax theorem, there exists a single mixed strategy $\mathcal{C}$ for Player 2 that achieves expected payoff at least .51 against *every* pure strategy u for Player 1. This is a distribution over circuits of size at most $\mathrm{size}(C)^a$. Fix any $u \in \{0,1\}^n$. By Lemma 2.1, if we take $H = O(n)$ large enough, and sample $C_1, \ldots, C_H$ independently from $\mathcal{C}$, then with probability greater than $1 - 2^{-n}$, we have $F_{C_i}(u) = \{f(u)\}$ for at least $.505 \cdot H$ indices $i \in [H]$. By a union bound, there exists a possible outcome $C_1^*, \ldots, C_H^*$ for which this occurs for every $u \in \{0,1\}^n$.[10]

Let $w^1, \ldots, w^H$ denote the nondeterministic gate-sets for $C_1^*, \ldots, C_H^*$ respectively (their lengths may differ). We define C^*, with input $u \in \{0,1\}^n$ and nondeterministic gates $\overline{w} = (w^1, \ldots, w^H)$, as follows. C^* first evaluates $C_i^*(u, w^i)$ for each $i \in [H]$. If there is some $z \in \{0,1\}^d$ such that at least $.505 \cdot H$ of the circuits C_i^* accept with output value z, then C^* accepts and outputs z; otherwise, C^* rejects. It is immediate from our construction that $F_{C^*}(u) = \{f(u)\}$ for each $u \in \{0,1\}^n$, and clearly we can achieve $\mathrm{size}(C^*) \leq O\left(H \cdot \mathrm{size}(C)^a\right) \leq \mathrm{poly}(\mathrm{size}(C))$.[11] □

[10] We remark that this step is an instance of the "strategy sparsification" technique of [LY94, Alt94].

[11] Recall here that $\mathrm{size}(C) \geq \max\{nt, dt\}$, since we count input and output gates towards the circuit size.

Proof of Claim 4.2. Fix any distribution $\mathcal{D}$ over $\{0,1\}^n$. Our construction of the circuit $C' = C'_{\mathcal{D}}$ will require some preliminary work. First, refer to the experiment $\mathbf{Expt}^*(\mathcal{D})$ of Lemma 3.6, defined with respect to $\mathcal{D}, C, n, d, t, f$, and with $M := \lceil t/\ln(1/q) \rceil$. With the random variables $\alpha_j, \hat{\alpha}_j, \beta_j, \hat{\beta}_j$ as defined in that experiment, let us fix outcomes to the random variables

$$s_1, \ldots, s_t,\ S_1, \ldots, S_t,\ \mathbf{j},\ \mathbf{y}^1, \ldots, \mathbf{y}^t$$

that maximize the probability that Eq. (6) holds, where the probability is now taken over $\mathbf{u} \sim \mathcal{D}$. Let Λ denote the collection of random variables whose values we are fixing, and let $[\Lambda = \lambda]$ denote the particular setting we are making. Let $j^* \in [t]$ denote the fixed outcome to $\mathbf{j}$. (In our circuit construction, we will effectively ignore the values $\mathbf{y}^j$ for $j > j^*$.)

When in $\mathbf{Expt}^*(\mathcal{D})$ we condition on $[\Lambda = \lambda]$, Eq. (6) holds with probability at least $1 - \frac{2^{16}\ln(1/q)}{t} - \frac{1}{M} \geq \frac{(2^{16}+1)\ln(1/q)}{t}$, which is $> 1 - \delta$ by our setting. Also, under our conditioning, $\mathbf{u}$ remains undetermined and is distributed according to $\mathcal{D}$.

Note that our settings determine outcomes to $\alpha_0, \ldots, \alpha_t, \beta_0, \ldots, \beta_{t-1}$. The value $\alpha_{j^*-1} > 0$ in particular will be useful to us in defining our circuit. Abusing notation somewhat, we now let $s_1, \ldots, s_t, S_1, \ldots, S_t, \alpha_0, \ldots, \alpha_t, \beta_0, \ldots, \beta_{t-1}$ denote the fixed outcomes to these variables. For each $j \in [t]$, let

$$S_j \ = \ \{\ y^{j,\ell}\ \}_{\ell \in [s_j]}$$

be an indexing of S_j (with some elements possibly appearing multiple times, according to their multiplicity in S_j). We define a mapping $\ell^* : [t] \to \mathbb{N}^+$ by the relation that, for our outcomes to $\mathbf{y}^1, \ldots, \mathbf{y}^t$, we have

$$\mathbf{y}^j \ = \ y^{j,\ell^*(j)}\ .$$

As another important piece of non-uniform data in our construction, we will need to know the values taken by f on $y^{1,\ell^*(1)}, \ldots, y^{j^*-1,\ell^*(j^*-1)}$. For $j \in [j^* - 1]$, we let

$$\hat{z}^j \ := \ f(y^{j,\ell^*(j)})\ .$$

Next we make some further definitions and observations. Suppose the probabilistic circuit C uses R bits of randomness (we may assume $R > 0$, or else we would have $q = 1$ and the Claim would be a triviality). Recall that $C^{\det}(x^1, \ldots, x^t; r) : \{0,1\}^{n \times t + R} \to \{0,1\}$ denotes C considered as a deterministic circuit with random string r as part of its input. For any string $u \in \{0,1\}^n$, we define a *viable certificate for* u as a tuple

$$w \ = \ (m_{j^*+1}, m_{j^*+2}, \ldots, m_t,\ r) \in [s_{j^*+1}] \times \ldots \times [s_t] \times \{0,1\}^R$$

for which the first $(j^* - 1)$ length-d output blocks of the computation

$$C^{\det}\left(y^{1,\ell^*(1)}, \ldots, y^{j^*-1,\ell^*(j^*-1)},\ u,\ y^{j^*+1,m_{j^*+1}}, \ldots, y^{t,m_t};\ r\right) \tag{7}$$

equal $(\hat{z}^1, \ldots, \hat{z}^{j^*-1})$. For such a w and $z \in \{0,1\}^d$, we say that w is a *viable* z*-certificate for* u if the $(j^*)^{th}$ output block of the computation in Eq. (7) equals z, i.e., if in this computation C makes the "guess" that $f(u)$ equals z.

We fix some natural encoding of $[s_{j^*+1}] \times \ldots \times [s_t] \times \{0,1\}^R$ in which each element w has a unique representation as a binary string in $\{0,1\}^N$; here, we may take $N \leq R + O(t \log_2 M) \leq \mathrm{poly}(\mathrm{size}(C))$. Let $V_u \subseteq \{0,1\}^N$ denote the set of viable certificates for u, and for $z \in \{0,1\}^d$, let $V_u^z \subseteq V_u$ denote the viable z-certificates for u. The sets V_u^z form a partition of V_u.

Claim 4.3. *Let us condition on $[\Lambda = \lambda]$ as above in* $\mathbf{Expt}^*(\mathcal{D})$*. Then,*

1. *For the random variable* $\mathbf{u}$ *over* $\{0,1\}^n$*, the equality*
$$|V_{\mathbf{u}}| \;=\; 2^R \left(\prod_{j=j^*+1}^{t} s_j \right) \cdot \hat{\beta}_{j^*-1} \tag{8}$$
holds with probability 1.

2. *Also, we have the equality*
$$\left| V_{\mathbf{u}}^{f(\mathbf{u})} \right| \;=\; 2^R \left(\prod_{j=j^*+1}^{t} s_j \right) \cdot \hat{\alpha}_{j^*} \ , \tag{9}$$
and therefore
$$\frac{\left| V_{\mathbf{u}}^{f(\mathbf{u})} \right|}{|V_{\mathbf{u}}|} \;=\; \frac{\hat{\alpha}_{j^*}}{\hat{\beta}_{j^*-1}} \ . \tag{10}$$

Proof. **(1)** Condition further on any possible outcome $[\mathbf{u} = u]$ in $\mathbf{Expt}^*(\mathcal{D})$. Together with our prior conditioning $[\Lambda = \lambda]$, this determines the values of $\hat{S}_1, \ldots, \hat{S}_t, \hat{\alpha}_1, \ldots, \hat{\alpha}_t, \hat{\beta}_1, \ldots, \hat{\beta}_t$. Under this conditioning, we see from the definition that

$$\hat{\beta}_{j^*-1} \;=\; \Pr\left[C(\hat{\mathbf{y}}^1, \ldots, \hat{\mathbf{y}}^t) \text{ is } (j^*-1)\text{-valid} \;\middle|\; \hat{S}_1, \hat{S}_2, \ldots, \hat{S}_t, \hat{\mathbf{y}}^1, \ldots, \hat{\mathbf{y}}^{j^*} \right] \tag{11}$$
$$\;=\; \Pr\left[C(y^{1,\ell^*(1)}, \ldots, y^{j^*-1,\ell^*(j^*-1)},\ u,\ \mathbf{v}^{j^*+1}, \ldots, \mathbf{v}^t) \text{ is } (j^*-1)\text{-valid} \ \right] \ , \tag{12}$$

where we sample $(\mathbf{v}^{j^*+1}, \ldots, \mathbf{v}^t) \in_r S_{j^*+1} \times \ldots \times S_t$ (and where validity is with respect to f). Here, $S_{j^*+1}, \ldots, S_t$ are our fixed values under $[\Lambda = \lambda]$, and the probability in Eq. (12) is taken over $\mathbf{v}^{j^*+1}, \ldots, \mathbf{v}^t$ and over the random bits r used by C.

Let us calculate the probability in Eq. (12). The selection of $(\mathbf{v}^{j^*+1}, \ldots, \mathbf{v}^t)$ may be equivalently performed by choosing $(m_{j^*+1}, \ldots, m_t) \in_r [s_{j^*+1}] \times \ldots \times [s_t]$, and setting $\mathbf{v}^j := y^{j,m_j}$ for $j \in \{j^*+1, \ldots, t\}$. There are $\left(\prod_{j=j^*+1}^{t} s_j\right) \cdot 2^R$ possible outcomes to $(m_{j^*+1}, \ldots, m_t, r)$, each one equally likely. The outcomes that cause the computation indicated in Eq. (12) to be (j^*-1)-valid are, under our definition, precisely those for which

$$(m_{j^*+1}, \ldots, m_t, r) \;\in\; V_u \ .$$

Thus, under our conditioning $[\mathbf{u} = u]$ we have

$$\hat{\beta}_{j^*-1} \;=\; \frac{|V_u|}{2^R \left(\prod_{j=j^*+1}^{t} s_j \right)} \ , \qquad \text{i.e.,} \qquad |V_u| \;=\; 2^R \left(\prod_{j=j^*+1}^{t} s_j \right) \hat{\beta}_{j^*-1} \ .$$

As u was an arbitrary outcome to $\mathbf{u}$, we have proved part 1 of the Claim.

(2) Condition again on any possible outcome $[\mathbf{u} = u]$ in $\mathbf{Expt}^*(\mathcal{D})$. Then we have

$$\begin{aligned} \hat{\alpha}_{j^*} &= \Pr\left[C(\hat{\mathbf{y}}^1, \ldots, \hat{\mathbf{y}}^t) \text{ is } j^*\text{-valid} \;\middle|\; \hat{S}_1, \hat{S}_2, \ldots, \hat{S}_t, \hat{\mathbf{y}}^1, \ldots, \hat{\mathbf{y}}^{j^*} \right] && (13) \\ &= \Pr\left[C(y^{1,\ell^*(1)}, \ldots, y^{j^*-1,\ell^*(j^*-1)},\ u,\ \mathbf{v}^{j^*+1}, \ldots, \mathbf{v}^t) \text{ is } (j^*-1)\text{-valid} \;\right], && (14) \end{aligned}$$

where again $(\mathbf{v}^{j^*+1}, \ldots, \mathbf{v}^t) \in_r S_{j^*+1} \times \ldots \times S_t$. Let these $\mathbf{v}^j$ be generated by $(m_{j^*+1}, \ldots, m_t)$ just as in part 1. The outcomes that cause the computation in Eq. (14) to be j^*-valid are exactly those for which the following two conditions hold:

1. $(m_{j^*+1}, \ldots, m_t, r) \in V_u$;
2. The $(j^*)^{th}$ output block of $C^{\det}(y^{1,\ell^*(1)}, \ldots, y^{j^*-1,\ell^*(j^*-1)},\ u,\ \mathbf{v}^{j^*+1}, \ldots, \mathbf{v}^t; r)$ equals $f(u)$.

These outcomes are exactly those for which $(m_{j^*+1}, \ldots, m_t, r) \in V_u^{f(u)}$. Then by a calculation following that in part 1, we can verify that Eq. (9) holds under $[\mathbf{u} = u]$. As u was arbitrary, Eq. (9) holds identically. Combining this with part 1 gives Eq. (10). □

We have chosen the settings $[\Lambda = \lambda]$ so that Eq. (6) holds with high probability over $\mathbf{u} \sim \mathcal{D}$. Using Claim 4.3, this implies that $\left|V_{\mathbf{u}}^{f(u)}\right| \approx |V_{\mathbf{u}}|$ with high probability, i.e., almost all viable certificates for u correctly guess $f(u)$. Furthermore, by both parts of Claim 4.3 and the first condition of Eq. (6), both of $\left|V_{\mathbf{u}}^{f(\mathbf{u})}\right|, |V_{\mathbf{u}}|$ are (with high probability) approximately equal to $\rho := 2^R \left(\prod_{j=j^*+1}^t s_j\right) \alpha_{j^*-1}$; this latter quantity is determined by the setting $[\Lambda = \lambda]$, and does not depend on $\mathbf{u}$.

This motivates our strategy for building a nondeterministic mapping circuit to compute f on an input u sampled from $\mathcal{D}$. First, we choose a random hash function h from a strongly universal hash family with domain $U := \{0,1\}^N$ (identified with $\mathbb{F}_2^N$), and with a range space of size determined by ρ. We consider an element of U "dead" unless it maps to the all-0 vector under h; our aim is to "kill off" all of the viable certificates making incorrect guesses for $f(u)$, while leaving alive some viable certificate that makes a correct guess. Corollary 2.7, combined with our control on the sizes of $|V_{\mathbf{u}}|, \left|V_{\mathbf{u}}^{f(\mathbf{u})}\right|$, makes it possible to ensure this outcome with reasonable success probability. Nondeterminism will then allow us to guess and verify a live, viable certificate.

To make this strategy succeed with the required probability, we will perform repeated trials, selecting multiple hash functions and taking a majority vote over the trials. In the end we will remove the randomness in these trials and apply Lemma 2.8 to obtain our final nondeterministic circuit.

Let

$$K := \lceil \log_2 \rho - 4 \rceil\ ,$$

and let

$$\mathcal{H}^{N,K} \;=\; \{\ \ h_{A,v} : \mathbb{F}_2^N \to \mathbb{F}_2^K\ \ \}_{A \in \mathbb{F}_2^{K \times N}, v \in \mathbb{F}_2^K}$$

be the strongly universal hash family given by Proposition 2.5. Note that $K = O(R + Mt) = O(R + t^2) \le \text{poly}(\text{size}(C))$. Under our setting $[\Lambda = \lambda]$, say that $h_{A,v} \in \mathcal{H}^{N,K}$ is *good for* $u \in \{0,1\}^n$ if

$$0^K \;\in\; h_{A,v}\left(V_u^{f(u)}\right) \setminus \left(\bigcup_{z \neq f(u)} h_{A,v}\left(V_u^z\right) \right)\ .$$

Say that a string $u \in \{0,1\}^n$, contained in the support of $\mathcal{D}$, is *favorable*, and write $u \in \mathrm{Fav}$, if Eq. (6) holds under $[\Lambda = \lambda, \mathbf{u} = u]$. By our choice of λ we have $\Pr_{\mathbf{u} \sim \mathcal{D}}[\mathbf{u} \in \mathrm{Fav}] \geq 1 - \delta$.

Claim 4.4. *Suppose u is favorable. If $(A, v) \in_r \mathbb{F}_2^{K \times N} \times \mathbb{F}_2^K$, then*

$$\Pr[h_{A,v} \textit{ is good for } u] \;>\; .75 \;.$$

Proof. Define the set

$$V_u^{\mathrm{wrong}} \;:=\; \bigcup_{z \neq f(u)} V_u^z \;.$$

Under the conditioning $[\Lambda = \lambda, \mathbf{u} = u]$ in $\mathbf{Expt}^*(\mathcal{D})$, which defines outcomes to $\hat{\beta}_{j^*-1}, \hat{\alpha}_{j^*}$, part 2 of Claim 4.3 tells us that

$$\frac{\left|V_u^{f(u)}\right|}{|V_u|} \;=\; \frac{\hat{\alpha}_{j^*}}{\hat{\beta}_{j^*-1}} \;.$$

As u is favorable, this implies

$$\frac{\left|V_u^{f(u)}\right|}{|V_u|} \;\in\; [.99, 1] \;, \qquad \text{and so} \qquad \frac{|V_u^{\mathrm{wrong}}|}{|V_u|} \;\leq\; .01 \;. \tag{15}$$

Next, part 1 of Claim 4.3 combined with Eq. (6) tells us that

$$\frac{|V_u|}{\rho} \;=\; \frac{|V_u|}{2^R \left(\prod_{j=j^*+1}^{t} s_j\right) \alpha_{j^*-1}} \;=\; \frac{\hat{\beta}_{j^*-1}}{\alpha_{j^*-1}} \;\in\; [.98, 1.02] \;. \tag{16}$$

Define real numbers θ, θ' by the relations

$$|V_u| \;=\; \theta \cdot 2^K, \qquad |V_u^{\mathrm{wrong}}| \;=\; \theta' \cdot 2^K \;.$$

By Eqs. (15)-(16) and our setting $K = \lceil \log_2 \rho - 2 \rceil$, we have the bounds

$$\theta \;\geq\; 8 \cdot .98 \;>\; 7 \;, \qquad \theta \;\leq 16 \cdot 1.02 \;<\; 17 \;, \qquad \theta' \;\leq\; .01\theta \;.$$

We apply Corollary 2.7, with $U := \mathbb{F}_2^N, U_{(\mathrm{i})} := V_u$, and $U_{(\mathrm{ii})} := V_u^{\mathrm{wrong}}$ (there is no requirement that $U_{(\mathrm{i})}, U_{(\mathrm{ii})}$ be disjoint) to find that

$$\Pr_{A,v}\left[0^K \in h_{A,v}\left(V_u\right) \setminus h_{A,v}\left(V_u^{\mathrm{wrong}}\right)\right] \;\geq\; 1 - \theta^{-1} - .1\theta \;>\; .75 \;,$$

where we used the fact that $1 - x^{-1} - .01x > .75$ for $x \in [7, 17]$. Thus $h_{A,v}$ is good for u with probability greater than .75. This proves the Claim. □

Let $T := 40n$. We consider T-tuples

$$\overline{h} \;=\; \left(h_{A^1,v^1}, \ldots, h_{A^T,v^T}\right) \;\in\; \left(\mathcal{H}^{N,K}\right)^{\times T} \;.$$

Suppose we select the functions (A^i, v^i) independently as $(A^i, v^i) \in_r \mathbb{F}_2^{K \times N} \times \mathbb{F}_2^K$. For any $u \in \{0,1\}^n$, let

$$X^+(u) \;:=\; \sum_{i \in [T]} \mathbf{1}\left[h_{A^i,v^i} \text{ is good for } u\right]$$

Fix attention to any favorable u. By using Claim 4.4 and applying Lemma 2.1 to $X^{+}(u)$, we find that with probability at least $1 - \exp(-2(.15)^2 \cdot T) > 1 - 2^{-2n}$,

$$X_{+}(u) \ \geq \ .6T \ . \tag{17}$$

Taking a union bound, we conclude that with probability at least $1 - 2^n \cdot 2^{-2n} > 0$, Eq. (17) holds for *every* favorable $u \in \{0,1\}^n$. Thus there exists a choice

$$\overline{h} \ = \ (h_1^*, \ldots, h_T^*) \ = \ \left(h_{A^1,v^1}, \ldots, h_{A^T,v^T}\right)$$

such that Eq. (17) holds for every $u \in \mathrm{Fav}$.

We are now ready to construct our circuit C' promised in the statement of Claim 4.2, by appealing to Lemma 2.8. First, each hash function h_i^* is determined by the values (N, K) and the pair (A^i, v^i), which can be specified by $O(KN)$ bits. Using this description, we can directly compute $h_i^*(w)$ for a given $w \in \{0,1\}^N$ using $O(KN)$ gates, as needed.

Let us next consider the problem of testing membership in the sets V_u, V_u^z. Our encoding of elements of $[s_{j^*+1}] \times \ldots \times [s_t] \times \{0,1\}^R$ as strings in $\{0,1\}^N$ can be explicitly defined given the values $s_{j^*+1}, \ldots, s_t$, and these are specifiable with $O(t \log_2 M) = O(t \log_2 t)$ bits. The multisets $S_1, \ldots, S_t$ we used, and the distinguished elements $y^{1,\ell^*(1)}, \ldots, y^{t,\ell^*(t)}$, are specifiable with $O(tMn) = O(t^2 n)$ bits; given these sets, we can efficiently determine whether w is a well-formed representative of an element of $[s_{j^*+1}] \times \ldots \times [s_t] \times \{0,1\}^R$ and, if so, map it to the input to $C^{\det}$ it represents under the correspondence presented in Eq. (7). By performing this mapping, evaluating $C^{\det}$ on the resulting input, and comparing its output to the hard-coded values $\hat{z}^1, \ldots, \hat{z}^{j^*-1}$, we can determine which set V_u^z (if any) contains a given $w \in \{0,1\}^N$. This can be performed by a circuit $C_{\mathrm{Vtest}}(w,u)$ with at most $\mathrm{size}(C) + \mathrm{poly}(n + d + t) \leq \mathrm{poly}(\mathrm{size}(C))$ gates.

Thus, we may apply Lemma 2.8 to obtain a nondeterministic mapping circuit $C^{\dagger}$ on n input gates, of size $\mathrm{size}(C^{\dagger}) \leq \mathrm{poly}(\mathrm{size}(C))$, such that $F_{C^{\dagger}}(u) = \{f(u)\}$ for every $u \in \mathrm{Fav}$. Recall that $\Pr_{\mathbf{u} \sim \mathcal{D}}[\mathbf{u} \in \mathrm{Fav}] \geq 1 - \delta$. Thus $C^{\dagger}$ $(1-\delta)$-defines f with respect to $\mathcal{D}$. So we may choose $C^{\dagger}$ as our desired circuit C', finding that $\mathrm{size}(C^{\dagger}) \leq \mathrm{size}(C)^a$ for an appropriately large $a > 0$. This proves Claim 4.2, completing the proof of Theorem 4.1. □

5 The success probability of SAT solvers

For $k \in \mathbb{N}^+$, a *k-CNF* is a Boolean formula ψ of the form $\psi = \bigwedge_i D_i$, where each D_i is a disjunction of exactly k *terms*; here, a term is a literal or negated literal.

In this section we prove:

Theorem 5.1 (Theorem 1.5, restated). *Let $\gamma \in (0,1)$. Suppose there is a PPT algorithm P_{solver} that, when given as input a description of a satisfiable 3-CNF formula Φ, of description length $|\langle \Phi \rangle| = N$, outputs a satisfying assignment to Φ with probability at least $q(N) := 2^{-N^{\gamma}}$.*

Then, $\mathsf{NP} \subseteq \mathsf{coNP/poly}$.

We will need the following straightforward lemma.

Lemma 5.2. *There is a deterministic polynomial-time algorithm M that takes as inputs descriptions of 3-CNF formulas $\psi^1, \psi^2, \ldots, \psi^t$ and a value $s \geq 0$, and outputs a 3-CNF formula $\Psi^{(s)}$ that is satisfiable if and only if at least s of the ψ_j's are satisfiable. Moreover, $\Psi^{(s)}$ contains designated variables $y = (y_1, \ldots, y_t)$ such that for each $j \in [t]$, if $\Psi^{(s)}$ has a satisfying assignment with y_j set to 1, then ψ^j is satisfiable. If ψ^j has m_j clauses, then $\Psi^{(s)}$ has $O\left(t + \sum_{j \in [t]} m_j\right)$ clauses.*

Proof. Consider Boolean strings y of length t. It is a standard fact that for any $s \geq 0$ we can explicitly (in polynomial time) construct a fanin-two Boolean circuit $G^{(s)}(y)$ over $\{\wedge, \vee, \neg\}$ with $O(t)$ gates, that accepts exactly if the Hamming weight $||y||_1$ is at least s.

Next we rename the variables of each ψ^j if necessary to ensure that for $j \neq j'$, ψ^j and $\psi^{j'}$ contain disjoint sets of variables. Let x^j denote the input variables to ψ^j. Then for each j we construct a circuit $H^j(x^j, y_j)$ that accepts exactly if $[y_j = 0 \vee \psi^j(x^j) = 1]$. This H^j can be implemented with $O(m_j)$ gates.

Define a circuit $F^{(s)}(x^1, \ldots, x^t, y)$ which outputs $G^{(s)}(y) \wedge \left(\bigwedge_{j \in [t]} H^j(x^j, y_j)\right)$. Using Cook's reduction again, we derive from $F^{(s)}$ a 3-CNF formula $\Psi^{(s)}(y_1, \ldots, y_t, z_1, \ldots, z_T)$, such that $\Phi^{(s)}(y, \cdot)$ is satisfiable exactly if there are settings to $x^1, \ldots, x^t$ such that $F^{(s)}(x^1, \ldots, x^t, y) = 1$. This is the case exactly if $[||y||_1 \geq s] \wedge [\forall j$ with $y_j = 1$, ψ^j is satisfiable$]$. We have established the correctness of our reduction. The number of clauses in $\Psi^{(s)}$ is bounded by a constant factor times the number of gates in $F^{(s)}$, which is $O\left(t + \sum_{j \in [t]} m_j\right)$, so $\Psi^{(s)}$ obeys the required size bound; and $\Psi^{(s)}$ can be constructed in polynomial time as needed. □

The next lemma connects the task of satisfying 3CNFs to direct-product computations for 3SAT.

Lemma 5.3. *Let P_{solver} be a PPT algorithm that takes as input a description of a 3-CNF formula Φ. Assume that there is a nonincreasing function*

$$q : \mathbb{N} \rightarrow (0, 1] \ ,$$

such that, whenever Φ is a satisfiable 3-CNF of description length N, $P_{\text{solver}}(\langle \Psi \rangle)$ outputs a satisfying assignment to Φ with probability at least $q(N)$.

Then there is a PPT algorithm P_{decider} that takes as input an arbitrary-size list $\langle \langle \psi^1 \rangle, \ldots, \langle \psi^t \rangle \rangle$ of descriptions of 3-CNFs, and outputs a length-t Boolean string $v = (v_1, \ldots, v_t)$, giving guesses for the satisfiability status of each ψ^i, i.e., for the values $\left(\chi_{3\text{SAT}}(\langle \psi^1 \rangle), \ldots, \chi_{3\text{SAT}}(\langle \psi^t \rangle)\right)$.

P_{decider} has the following property: if each ψ^j has description length $|\langle \psi^j \rangle| = n$, then for some $N = O(nt \cdot \log_2(nt))$, we have

$$\Pr\left[(v_1, \ldots, v_t) = \left(\chi_{\text{SAT}}(\langle \psi^1 \rangle), \ldots, \chi_{\text{SAT}}(\langle \psi^t \rangle)\right)\right] \ \geq \ \frac{q(N)}{t+1} \ .$$

Proof. P_{decider} first guesses a value $s \in_r \{0, 1, \ldots, t\}$. It then constructs the formula $\Psi^{(s)}$ defined by $(\psi^1, \ldots, \psi^t, s)$ as in Lemma 5.2, and applies P_{solver} to $\langle \Psi^{(s)} \rangle$. If P_{solver} returns a satisfying assignment to $\Psi^{(s)}$, with setting $(y_1, \ldots, y_t)$ to the y-variables, then P_{decider} outputs $(v_1, \ldots, v_t) := (y_1, \ldots, y_t)$. Otherwise P_{decider} sets $v_1, \ldots, v_t$ arbitrarily.

P_{decider} is clearly polynomial-time. We analyze its success probability when given as input descriptions of 3-CNFs $\psi^1, \ldots, \psi^t$, each of description length n. Let $S \subseteq [t]$ denote the set of indices j for which ψ^j is satisfiable. With probability at least $\frac{1}{t+1}$, P_{decider} sets $s := |S|$. Let us condition on this event. Now $\Psi^{(s)}$ is satisfiable, and (by our guarantee on the y-variables from Lemma 5.2) is satisfiable *only* by assignments for which $||y||_1 \geq s$ while $y_j = 0$ for all $j \notin S$. For such assignments, we have $(y_1, \ldots, y_t) = \left(\chi_{3\text{SAT}}(\langle \psi^1 \rangle), \ldots, \chi_{3\text{SAT}}(\langle \psi^t \rangle)\right)$.

Thus, P_{decider} succeeds provided that P_{solver} finds a satisfying assignment to $\Psi^{(s)}$; by the success property of P_{solver} occurs with probability at least $q(N)$, where we define N as an upper bound on the description length $|\langle \Psi^{(s)} \rangle|$. (Here we are using that $q(\cdot)$ is nonincreasing.) We may take $N = O(nt \cdot \log_2(nt))$, since $\Psi^{(s)}$ has $O(nt)$ clauses. Overall, our success probability is at least $q(N)/(t+1)$. This proves Lemma 5.3. □

Proof of Theorem 5.1. We apply Lemma 5.3 to $P_{\text{solver}}, q(\cdot)$ to obtain a second PPT algorithm P_{decider} as described in that Lemma. Fixing any values of n, t, we can construct a probabilistic Boolean circuit $C_{n,t} : \{0,1\}^{n\times t} \to \{0,1\}^t$ such that on input $(\langle\psi^1\rangle, \ldots, \langle\psi^t\rangle) \in \{0,1\}^{n\times t}$, the circuit $C_{n,t}$ simulates an execution of P_{decider} on input $\langle\langle\psi^1\rangle, \ldots, \langle\psi^t\rangle\rangle$. Here, we may ensure $\text{size}(C_{n,t}) \leq \text{poly}(n+t)$ by using any standard translation of algorithms to circuits. From the property of P_{decider} guaranteed by Lemma 5.3, we find that $C_{n,t}$ is a worst-case q'-direct-product solver for $(\chi_{\text{3SAT,n}})^{\otimes t}$, where

$$q' \;=\; \frac{q(\kappa nt \cdot \log_2(nt))}{t+1} \;=\; 2^{-(\kappa nt \log_2(nt)^{\gamma})^{\gamma} - \log_2(t+1)} \;, \tag{18}$$

for some absolute constant $\kappa > 0$.

Let $\rho := 2\gamma/(1-\gamma)$; we now fix $t := \lceil n^{\rho} \rceil$. Then $(nt \cdot \log_2(nt))^{\gamma} = O\left(n^{(1+\rho)\gamma} \cdot \log_2(nt)^{\gamma}\right) = O\left(n^{\gamma(1+\gamma)/(1-\gamma)} \cdot \log_2(nt)^{\gamma}\right) = o(n^{\rho})$. Also, $\log_2(t+1) = O(\log_2 n) = o(n^{\rho})$. Thus, for sufficiently large n we have

$$(\kappa nt \cdot \log_2(nt))^{\gamma} + \log_2(t+1) < \frac{t}{3 \cdot 10^5} \;,$$

so that, using Eq. (18), we have

$$q' \;\geq 2^{-t/(3\cdot 10^5)} \;\geq \exp\left(\frac{-t}{3\cdot 10^5}\right) \;.$$

We can therefore apply Theorem 4.1 to $C_{n,t}$, with $f := \chi_{\text{3SAT},n}$, to obtain a nondeterministic mapping circuit C^*_n on n input bits, such that $F_{C^*_n}(\langle\psi\rangle) = \{\chi_{\text{3SAT}}(\langle\psi\rangle)\}$ for all formulas ψ of description length n, and for which $\text{size}(C^*) \leq \text{poly}(\text{size}(C_{n,t})) \leq \text{poly}(n+t) \leq \text{poly}_{\gamma}(n)$. It follows from Proposition 2.3 that 3SAT $\in$ $\mathsf{coNP/poly}$. As 3SAT is NP-complete, this proves the Theorem. □

6 The DPT for sampleable distributions

In this section we prove:

Theorem 6.1. *Let $n, d, t \in \mathbb{N}^+$ with $t > 1$. Let $f : \{0,1\}^n \to \{0,1\}^d$, and let $q \in (0,1)$. Let $\mathcal{D}$ be a distribution over $\{0,1\}^n$ sampleable by a probabilistic circuit $C_{\mathcal{D}\text{-samp}}$. Suppose there is a probabilistic circuit $C : \{0,1\}^{n\times t} \to \{0,1\}^t$, such that C is a q-direct-product solver for $f^{\otimes t}$ with respect to $\mathcal{D}^{\otimes t}$.*

Let

$$\varepsilon \;\in\; [1/t, 1)$$

be given. Assume that $\varepsilon > \frac{2^{12}}{t^{1/3}}$. Assume also that

$$q \;\geq\; \exp\left(-\frac{\varepsilon^{3/2}\sqrt{t}}{10^{13}}\right) \;; \tag{19}$$

then, there is a nondeterministic mapping circuit C^*_ε on n input bits that $(1-\varepsilon)$-defines f with respect to $\mathcal{D}$, and such that

$$\mathrm{size}(C^*_\varepsilon) \;\le\; \mathrm{poly}\left(\mathrm{size}(C) + \mathrm{size}(C_{\mathcal{D}\text{-samp}})\right) \;.$$

In the size bound on C^*_ε above, there is no hidden dependence on ε. This result readily implies Theorem 1.3:

Proof of Theorem 1.3. Let $f = \{f_n\}$ satisfy the hypothesis of Theorem 1.3. Suppose for contradiction's sake that there is an infinite set $S \subseteq \mathbb{N}$, and a family of probabilistic circuits $\{C_n\}$ of size at most n^k for some $k > 0$, such that for all $n \in S$ and all $\mathbf{x} \sim \mathcal{D}_n^{\otimes t(n)}$,

$$q \;:=\; \Pr[C_n(\mathbf{x}) = f_n^{\otimes t(n)}(\mathbf{x})] \;\ge\; \exp\left(-\frac{\varepsilon_n^{3/2}\sqrt{t(n)}}{10^8}\right) \;.$$

We have also $\varepsilon_n > \frac{2^{12}}{t(n)^{1/3}}$.

Let $\{C_{\mathrm{samp},n}\}$ be the polynomial-sized sampling circuit family, assumed to exist, for which $C_{\mathrm{samp},n}$ samples $\mathcal{D}_n$. Suppose $\mathrm{size}(C_{\mathrm{samp},n}) \le n^{k'}$. Then by applying Theorem 6.1 to each $n \in S$, we find that there is a family $\{C^*_{n,\varepsilon_n}\}_{n\in S}$ of nondeterministic mapping circuits on n input bits, each with a single output bit; for each $n \in S$, C^*_{n,ε_n} is a circuit that $(1-\varepsilon_n)$-defines f_n with respect to $\mathcal{D}_n$, and satisfies

$$\mathrm{size}(C^*_{n,\varepsilon_n}) \;\le\; \mathrm{poly}(\mathrm{size}(C_n) + \mathrm{size}(C_{\mathrm{samp},n})) \;=\; \mathrm{poly}(n^k + n^{k'}) \;=\; \mathrm{poly}(n) \;.$$

This contradiction to our hypothesis proves the Theorem. □

6.1 A "confidence-building" lemma

Our first step toward proving Theorem 6.1 will be to give a reduction which converts a direct-product solver into an input-confident direct-product solver. This will occupy us in Section 6.1, where our goal is to prove the following lemma.

Lemma 6.2. *Fix $n, d, t \in \mathbb{N}^+$ and $q, \xi \in (0,1)$. Let $\mathcal{D}$ be a distribution over $\{0,1\}^n$, sampleable by a probabilistic circuit $C_{\mathcal{D}\text{-samp}}$ with s non-output gates. Let $f : \{0,1\}^n \to \{0,1\}^d$, and suppose the deterministic circuit C is a q-direct-product solver for $f^{\otimes t}$ with respect to the input distribution $\mathcal{D}^{\otimes t}$ over $\{0,1\}^{n\times t}$.*

Fix any $t' \in [t]$. Let $k := \lfloor t/t' \rfloor$, and let

$$\zeta \;:=\; \min\left(\frac{.6}{1-\xi}\sqrt{\log_2(1/q)/k}\;,\;\frac{1-e^{-1}q^{1/k}}{1-\xi}\right) \;.$$

Assume that $\zeta < 1$. Then there is a probabilistic circuit

$$\tilde{C} : \{0,1\}^{n\times t'} \to \{0,1\}^{t'} \;,$$

satisfying

$$\mathrm{size}(\tilde{C}) \;\le\; \mathrm{size}(C) + st \;,$$

such that $\tilde{C}$ is a $(1-\zeta, \xi q)$-input-confident direct product solver for $f^{\otimes t'}$ with respect to the input distribution $\mathcal{D}^{\otimes t'}$.

Note that the efficiency of this reduction depends on the ease of sampling from $\mathcal{D}$. If $\mathcal{D}$ is the uniform distribution on $\{0,1\}^n$, then for $C_{\mathcal{D}\text{-samp}}$ we may take a circuit all of whose n gates are designated both as random gates and as output gates. Then $s = 0$, and for the circuit $\tilde{C}$ obtained from Lemma 6.2 we have $\text{size}(\tilde{C}) = \text{size}(C)$. The added efficiency of the reduction in such cases is not important for our main results; we merely point it out.

For our work in proving Lemma 6.2 we will need some additional definitions and facts. Suppose B is a finite set, $k > 0$ is an integer, and $\overline{\nu}$ is a (possibly non-product) distribution over $B^{\times k}$. For $i \in [k]$, let $\overline{\nu}^{(i)}$ denote the distribution over B governing the i^{th} coordinate of $\overline{\nu}$. Also, if $A \subseteq B^{\times k}$ is assigned nonzero probability by ν, we let $\overline{\nu}_A$ denote the distribution of a random variable $\mathbf{u} \sim \overline{\nu}$ after conditioning on $[\mathbf{u} \in A]$. If $\overline{\nu}(A) = 0$ then $\overline{\nu}_A$ is left undefined.

We will use the following well-known, non-symmetric measure of difference between random variables (see [CT06] for more information).

Definition 6.3 (KL divergence)**.** *The (binary)* Kullback-Leibler divergence*, or* KL divergence *between two distributions $\mathcal{R}, \mathcal{R}'$, denoted $D_{\text{KL}}(\mathcal{R}||\mathcal{R}')$, is defined as follows. If* $\text{supp}(\mathcal{R}) \subseteq \text{supp}(\mathcal{R}')$*, set*

$$D_{\text{KL}}(\mathcal{R}||\mathcal{R}') \ := \ \sum_{x \in \text{supp}(\mathcal{R})} \mathcal{R}(x) \cdot \log_2\left(\frac{\mathcal{R}(x)}{\mathcal{R}'(x)}\right) \ ;$$

otherwise set $D_{\text{KL}}(\mathcal{R}||\mathcal{R}') := +\infty$.

Note that if $||\mathcal{R} - \mathcal{R}'||_{\text{stat}} = 1$ then $D_{\text{KL}}(\mathcal{R}||\mathcal{R}') = +\infty$. We define the KL divergence $D_{\text{KL}}(Z||Z')$ between two random variables as the divergence between the corresponding distributions.

Fact 6.4. *[Raz98, Special case of Lemma 3.3] Suppose μ is a distribution over a finite set B. Let $k > 0$, and let $\overline{\nu}$ be any distribution over $B^{\times k}$. Then,*

$$D_{\text{KL}}\left(\overline{\nu}||\mu^{\otimes k}\right) \ \geq \ \sum_{i \in [k]} D_{\text{KL}}\left(\overline{\nu}^{(i)}||\mu\right) \ .$$

Fact 6.5. *[Raz98, Lemma 3.5] Let B be a finite set, $k > 0$, and suppose $\overline{\pi}$ is any distribution over $B^{\times k}$. Suppose that $V \subseteq B^{\times k}$ satisfies $\overline{\pi}(B) > 0$. Then,*

$$D_{\text{KL}}\left(\overline{\pi}_A||\overline{\pi}\right) \ = \ -\log_2(\overline{\pi}(A)) \ .$$

The next corollary follows a similar use of Lemmas 6.4 and 6.5 in [Raz98].

Corollary 6.6. *Let μ be a distribution over the finite set B, and $k > 0$. Suppose that $A \subseteq B^{\times k}$ satisfies $\mu^{\otimes k}(A) \geq q > 0$. Let us use the notation $\overline{\nu} := (\mu^{\otimes k})_A$. If we let*

$$\gamma_i \ := \ D_{\text{KL}}\left(\overline{\nu}^{(i)}||\mu\right) \ ,$$

then

$$\frac{1}{k}\sum_{i \in [k]} \gamma_i \ \leq \ \frac{\log_2(1/q)}{k} \ .$$

Proof. First, Lemma 6.5, applied to $\overline{\pi} := \mu^{\otimes k}$, tells us that

$$D_{\text{KL}}\left(\overline{\nu}||\mu^{\otimes k}\right) \ = \ D_{\text{KL}}\left(\overline{\pi}_A||\overline{\pi}\right) \ = \ -\log_2(\mu^{\otimes k}(A)) \ \leq \ \log_2(1/q) \ .$$

Next, Lemma 6.5 tells us that $\sum_{i \in [k]} \gamma_i \leq D_{\text{KL}}\left(\overline{\nu}||\mu^{\otimes k}\right)$. Combining these facts gives the result. □

We will also use the following important relation between KL divergence and statistical distance [CT06] (see Lemma 11.6.1, p. 370).

Lemma 6.7 (Pinsker's inequality, stated for binary KL divergence)**.** *For any random variables Z, Z',*

$$D(Z||Z') \;\geq\; \frac{2}{\ln 2} \cdot ||Z - Z'||^2_{\text{stat}} \ .$$

When $||Z - Z'||_{\text{stat}} \approx 1$, the following bound, due to Vajda (see [FHT03, RW09]), gives a better bound on the divergence than Pinsker's inequality.

Lemma 6.8 (Vajda's inequality, stated for binary KL divergence)**.** *For any random variables Z, Z', let $\Delta := ||Z - Z'||_{\text{stat}}$. If $\Delta < 1$ we have*

$$D(Z||Z') \;\geq\; \frac{1}{\ln 2}\left(\ln\left(\frac{1+\Delta}{1-\Delta}\right) - \frac{2\Delta}{1+\Delta}\right) \;\geq\; \frac{1}{\ln 2}\left(\ln\left(\frac{1}{1-\Delta}\right) - 1\right) \ ,$$

which implies

$$\Delta \;\leq\; 1 - e^{-1}2^{-D(Z||Z')} \ .$$

Lemma 6.9. *Let B be a finite set, and μ a distribution over B. Let $k \geq 2$ be an integer and let $A \subseteq B^{\times k}$. Suppose that A is "large" according to the product measure $\mu^{\otimes k}$; that is, $\mu^{\otimes k}(A) \geq q$ for some $q \in (0, 1)$.*

Consider the following experiment $\mathbf{Expt}^{\dagger}(\mu)$*:*

1. *Sample $\mathbf{b} = (\mathbf{b}^1, \ldots, \mathbf{b}^k) \sim \mu^{\otimes k}$;*
2. *For $i \in [k]$, define τ_i, a random variable in $[0, 1]$ determined by $\mathbf{b}^i$, by*

$$\tau_i \;:=\; \Pr\left[(\mathbf{b}^1, \ldots, \mathbf{b}^k) \in A \middle| \mathbf{b}^i\right] \ .$$

Fix $\xi \in (0, 1)$, and for each $i \in [k]$, let $\zeta_i := \Pr[\tau_i < \xi q]$. Then,

$$\frac{1}{k}\sum_{i\in[k]} \zeta_i \;\leq\; \min\left(\frac{.6}{1-\xi}\sqrt{\frac{\log_2(1/q)}{k}} \ , \ \frac{1}{1-\xi}\left(1 - e^{-1}q^{1/k}\right)\right) \ .$$

In particular, there exists an $i \in [k]$ with $\zeta_i \leq \min\left(\frac{.6}{1-\xi}\sqrt{\frac{\log_2(1/q)}{k}} \ , \ \frac{1}{1-\xi}\left(1 - e^{-1}q^{1/k}\right)\right)$.

Proof. We will prove that for any $i \in [k]$,

$$\zeta_i \;\leq\; \min\left(\frac{.6}{1-\xi}\sqrt{D_{\text{KL}}\left(\overline{\nu}^{(i)}||\mu\right)} \ , \ \frac{1 - e^{-1}2^{-D_{\text{KL}}\left(\overline{\nu}^{(i)}||\mu\right)}}{1-\xi}\right) \ .$$

It will follow that

$$\frac{1}{k}\sum_{i\in[k]} \zeta_i \;\leq\; \frac{.6}{1-\xi}\left(\frac{1}{k}\sum_{i\in[k]}\sqrt{D_{\text{KL}}\left(\overline{\nu}^{(i)}||\mu\right)}\right) \;\leq\; \frac{.6}{1-\xi}\sqrt{\frac{1}{k}\sum_{i\in[k]} D_{\text{KL}}\left(\overline{\nu}^{(i)}||\mu\right)} \;\leq\; \frac{.6}{1-\xi}\sqrt{\frac{\log_2(1/q)}{k}} \ ,$$

where in the last two steps we used Jensen's inequality and Corollary 6.6. Similarly, it will follow that

$$\begin{aligned}
\frac{1}{k}\sum_{i\in[k]}\zeta_i \;&\le\; \frac{1}{1-\xi}\left(1-e^{-1}\cdot\frac{1}{k}\sum_{i\in[k]}2^{-D_{\mathrm{KL}}\left(\overline{\nu}^{(i)}||\mu\right)}\right)\\
&\le\; \frac{1}{1-\xi}\left(1-e^{-1}2^{-\frac{1}{k}\sum_{i\in[k]}D_{\mathrm{KL}}\left(\overline{\nu}^{(i)}||\mu\right)}\right)\\
&\le\; \frac{1}{1-\xi}\left(1-e^{-1}q^{1/k}\right)\;.
\end{aligned}$$

So fix attention to some $i\in[k]$. For notational simplicity, let us assume $i=1$; the other cases are handled identically. Define

$$B^- \;:=\; \left\{b\in B:\Pr_{(\mathbf{b}^2,\ldots,\mathbf{b}^k)\sim\mu^{\otimes(k-1)}}\left[(b,\mathbf{b}^2,\ldots,\mathbf{b}^k)\in A\right]<\xi q\right\}\;,\qquad A' \;:=\; A\cap\{(b^1,\ldots,b^k):b^1\in B^-\}\;,$$

and observe that we have

$$\zeta_1 \;=\; \mu(B^-)\;.$$

Also, it follows from the definition of $\overline{\nu}=(\mu^{\otimes k})_A$ that we have

$$\overline{\nu}^{(1)}(B^-) \;=\; \frac{\mu^{\otimes k}(A')}{\mu^{\otimes k}(A)}\;. \tag{20}$$

The numerator on the right-hand side of Eq. (20) is at most $\mu(B^-)\cdot((1-\xi)q)$ by definition of B^-, while the denominator is at least q, by our assumption on A. Thus,

$$\overline{\nu}^{(1)}(B^-) \;\le\; \xi\cdot\mu(B^-)\;,$$

which implies that

$$||\overline{\nu}^{(1)}-\mu||_{\mathrm{stat}} \;\ge\; (1-\xi)\cdot\mu(B^-)\;. \tag{21}$$

On the other hand, Lemma 6.7 tells us that

$$||\overline{\nu}^{(1)}-\mu||_{\mathrm{stat}} \;\le\; \sqrt{\frac{\ln 2\cdot D_{\mathrm{KL}}\left(\overline{\nu}^{(1)}||\mu\right)}{2}} \;\le\; .6\sqrt{D_{\mathrm{KL}}\left(\overline{\nu}^{(1)}||\mu\right)}\;.$$

Combining this with Eq. (21) gives

$$\zeta_1 \;=\; \mu(B^-) \;\le\; \frac{.6}{1-\xi}\sqrt{D_{\mathrm{KL}}\left(\overline{\nu}^{(1)}||\mu\right)}\;,$$

as claimed.

Similarly, Lemma 6.8 tells us that

$$||\overline{\nu}^{(1)}-\mu||_{\mathrm{stat}} \;\le\; 1-e^{-1}2^{-D_{\mathrm{KL}}\left(\overline{\nu}^{(1)}||\mu\right)}\;,$$

which when combined with Eq. (21) gives

$$\zeta_1 \;\le\; \frac{1-e^{-1}2^{-D_{\mathrm{KL}}\left(\overline{\nu}^{(1)}||\mu\right)}}{1-\xi}\;.$$

This proves Lemma 6.9. □

Proof of Lemma 6.2. First we make a definition. Let $(x^1, \ldots, x^t)$ denote the t blocks of input variables to C, with each x^j consisting of n bits. Given a pair U, V of disjoint subsets of $[t]$, with U nonempty, and given a mapping $\Phi : V \to \{0,1\}^n$ describing an assignment to the blocks $(x^j)_{j \in V}$, define a probabilistic circuit

$$C_{U,V,\Phi} : \{0,1\}^{n \times |U|} \to \{0,1\}^{|U|} \ ,$$

obtained from C, as follows. First, each input block x^j with $j \in V$ is fixed to the assignment $\Phi(j)$. Next, if the designated output gates of C are

$$\{\ g^*_{j,e}\ \}_{j \in [t], e \in [d]} \ ,$$

where $g^*_{j,e}$ tries to compute the e^{th} bit of $f(x^j)$, then the output gates of $C_{U,V,\Phi}$ are $\{g^*_{j,e}\}_{j \in U, e \in [d]}$. Finally, for each of the blocks $(x^j)_{j \in [t] \setminus (U \cup V)}$, we construct a separate copy of $C_{\mathcal{D}\text{-samp}}$, and identify x^j with the output gates of the corresponding copy of $C_{\mathcal{D}\text{-samp}}$. The inputs to each such copy of $C_{\mathcal{D}\text{-samp}}$ are regarded as random gates in $C_{U,V,\Phi}$; the blocks $(x^j)_{j \in U}$ are left as the designated input gates of $C_{U,V,\Phi}$.

Our plan is to take $\tilde{C} := C_{U^*,V^*,\Phi^*}$, for suitably chosen (U^*, V^*, Φ^*). As a first step, note that we may write $t = kt' + \ell$, for some $0 \le \ell < t'$. Set $V^* := \{j : kt' < j < t\}$, a possibly-empty set. For any $\Phi : V \to \{0,1\}^n$, let $q_\Phi \in [0,1]$ be the maximal value such that $C_{[t] \setminus V^*, V^*, \Phi}$ is a q_Φ-direct-product solver for $f^{\otimes(t-\ell)}$ with respect to the input distribution $\mathcal{D}^{\otimes(t-\ell)}$. By averaging over settings to Φ induced by outcomes of $\mathcal{D}^{\otimes \ell}$ to $(x^j)_{j \in V^*}$ and applying our assumption on C, we conclude there exists a Φ such that $q_\Phi \ge q$. Let us fix Φ^* as any such mapping.

Next, for $i \in [k]$, let U_i be the interval $\{(i-1)k + 1, \ldots, (i-1)k + t'\}$, so that $|U_i| = t'$ and the sets $U_1, \ldots, U_k, V^*$ form a partition of $[t]$. We will choose U^* as one of our sets U_i, and will apply Lemma 6.9 to find a choice of i with good properties. Define the finite set $B := \{0,1\}^{n \times t'}$, and the distribution $\mu := \mathcal{D}^{\otimes t'}$ over B. Define

$$A \ := \ \{\overline{x} = (x^1, \ldots, x^{kt'}) \in \{0,1\}^{n \times kt'} : C_{[t] \setminus V^*, V^*, \Phi^*}(\overline{x}) = (f(x^1), \ldots, f(x^{kt'}))\} \ .$$

Note that, as $([t] \setminus V^*) \cup V^* = [t]$, the circuit $C_{[t] \setminus V^*, V^*, \Phi^*}$ is deterministic (no copies of $C_{\mathcal{D}\text{-samp}}$ are introduced), so that A is well-defined. We may regard A as a subset of B^k; by our choice of Φ^* we have

$$\mu^{\otimes k}(A) \ \ge \ q.$$

Lemma 6.9 tells us that there is an $i^* \in [k]$ for which, if we choose $(\mathbf{b}^1, \ldots, \mathbf{b}^k) \sim \mu^{\otimes k}$, then with probability at least $1 - \zeta$, we have

$$\Pr\left[(\mathbf{b}^1, \ldots, \mathbf{b}^k) \in A \middle| \mathbf{b}^{i^*}\right] \ \ge \ \xi q \ .$$

Thus, if we modify $C_{[t] \setminus V^*, V^*, \Phi^*}$ by supplying all blocks $(x^j)_{j \notin U_{i^*} \cup V^*}$ with an independent random sample from $\mathcal{D}$ (not considered as part of the input), and by using $\{g^*_{j,e}\}_{j \in U_{i^*}, e \in [d]}$ as the designated output gates, we obtain a $(1 - \zeta, \xi q)$-input-confident direct-product solver for $f^{\otimes t'}$ with respect to the input distribution $\mathcal{D}^{\otimes t'}$ over the remaining input blocks $(x^j)_{j \in U_{i^*}}$. Now observe that the modification we have just described is precisely implemented by $C_{U_{i^*}, V^*, \Phi^*}$. This circuit has at most $\text{size}(C) + st$ gates, since we have obtained it from C by fixing some input gate values, adding fewer than t copies of $C_{\mathcal{D}\text{-samp}}$ (with output gates of these copies identified with gates in C), and changing the designated type of other gates. This proves Lemma 6.2. □

6.2 A DPT for input-confident direct-product solvers

In the previous section we showed how to endow direct-product solvers with the input-confidence property; in this section we will show how to *exploit* this property. The DPT we show here for input-confident direct-product solvers may also be of interest in its own right. We prove:

Theorem 6.10. *Fix $n, d, t' \in \mathbb{N}^+$ and $\zeta \in [0, 1), q' \in (0, 1]$. Let $\mathcal{D}$ be a distribution over $\{0, 1\}^n$, sampled by the circuit $C_{\mathcal{D}\text{-samp}}$. Let $f : \{0, 1\}^n \to \{0, 1\}^d$. Suppose the probabilistic circuit C is a $(1 - \zeta, q')$-input-confident direct-product solver for $f^{\otimes t'}$ with respect to the input distribution $\mathcal{D}^{\otimes t'}$ over $\{0, 1\}^{n \times t'}$.*

Let $\delta := \frac{2^{16} \ln(1/q')}{t'} + 2^{18}\zeta$. Then there is a nondeterministic mapping circuit $C' : \{0, 1\}^n \to \{0, 1\}^d$ that $(1 - \delta)$-defines f with respect to input distribution $\mathcal{D}$, and such that

$$\text{size}(C') \ \leq \text{poly}(\text{size}(C) + \text{size}(C_{\mathcal{D}\text{-samp}})) \ .$$

Proof. Let $\overline{\mathbf{x}} = (\mathbf{x}^1, \ldots, \mathbf{x}^{t'}) \sim \mathcal{D}^{\otimes t'}$. Let $\alpha_0, \ldots, \alpha_t, \beta_0, \ldots, \beta_{t'-1}$ be as in Definition 3.2, defined with respect to C, f, and $\overline{\mathbf{x}}$. Let $\mathbf{j} \in_r [t']$ be sampled independently of $\overline{\mathbf{x}}$. Now let us fix a $j^* \in [t']$ and settings

$$[\mathbf{j} = j^*, \ \mathbf{x}^1 = y^1, \ldots, \mathbf{x}^{j^*-1} = y^{j^*-1}] \tag{22}$$

that maximize the probability that Eq. (4) holds. Let Λ denote the collection of variables whose values we are setting, and let $[\Lambda = \lambda]$ denote the event described in Eq. (22).[12] By Part 1 of Lemma 3.5, Eq. (4) holds with probability at least $1 - \delta$ after conditioning on $[\Lambda = \lambda]$. Our setting $[\Lambda = \lambda]$ determines the value of $\alpha_{j^*-1} > 0$, but (in general) do not determine $\beta_{j^*-1}, \alpha_{j^*}$. Also, under our conditioning, $\mathbf{x}^{j^*}, \ldots, \mathbf{x}^{t'}$ remain undetermined and are distributed as independent samples from $\mathcal{D}$.

For $j \in [j^* - 1]$, let

$$\hat{z}^j \ := \ f(y^j) \ .$$

Suppose that the circuit C has R random gates, and that the sampling circuit $C_{\mathcal{D}\text{-samp}}$ uses R_{samp} random gates; we may assume $R, R_{\text{samp}} > 0$. For any $u \in \{0, 1\}^n$, we define a *viable certificate for* u as a tuple

$$w \ = \ \left(r^{j^*+1}, \ldots, r^{t'}, \ r\right) \ \in \ \{0, 1\}^{R_{\text{samp}} \times (t' - j^*) + R}$$

for which the first $(j^* - 1)$ length-d output blocks of the computation

$$C^{\text{det}}\left(y^1, \ldots, y^{j^*-1}, \ u, \ C_{\mathcal{D}\text{-samp}}(r^{j^*+1}), \ldots, C_{\mathcal{D}\text{-samp}}(r^{t'}); \ r\right) \tag{23}$$

equal $(\hat{z}^1, \ldots, \hat{z}^{j^*-1})$. Set

$$N \ := \ R_{\text{samp}} \cdot (t' - j^*) + R \ .$$

We let $V_u \subseteq \{0, 1\}^N$ denote the viable certificates for u. For $z \in \{0, 1\}^d$, we say that $w \in V_u$ is a *viable z-certificate for u* if the $(j^*)^{th}$ output block of the computation in Eq. (23) equals z. Let V_u^z denote the viable z-certificates for u.

Claim 6.11. *Let us condition on $[\Lambda = \lambda]$ as above. Then,*

[12] Note, here and in what follows, that our notation indicates a similarity with our work in the proof of Claim 4.2, but that significant differences are also present. For example, our setting $[\Lambda = \lambda]$ here plays an analogous role to the setting $[\Lambda = \lambda]$ in that proof, but the random variables being fixed are different.

1. *Defining the random variable* $\mathbf{u} := \mathbf{x}^{\mathbf{j}}$ *over* $\{0,1\}^n$, *the equality*

$$|V_{\mathbf{u}}| \;=\; 2^N \cdot \beta_{j^*-1} \tag{24}$$

   holds with probability 1.

2. *Also, we have the equality*

$$\left|V_{\mathbf{u}}^{f(\mathbf{u})}\right| \;=\; 2^N \cdot \alpha_{j^*} \;, \tag{25}$$

   and therefore

$$\frac{\left|V_{\mathbf{u}}^{f(\mathbf{u})}\right|}{|V_{\mathbf{u}}|} \;=\; \frac{\alpha_{j^*}}{\beta_{j^*-1}} \;. \tag{26}$$

Proof. **(1)** Condition further on any possible outcome $[\mathbf{u} = u]$. Under this conditioning, we see that

$$\begin{aligned}\beta_{j^*-1} \;&=\; \Pr\left[C(\mathbf{x}^1, \ldots, \mathbf{x}^{t'}) \text{ is } (j^*-1)\text{-valid} \;\middle|\; \mathbf{x}^1, \ldots, \mathbf{x}^{j^*}\right] &(27)\\ &=\; \Pr\left[C(y^1, \ldots, y^{j^*-1},\; u,\; \mathbf{v}^{j^*+1}, \ldots, \mathbf{v}^{t'}) \text{ is } (j^*-1)\text{-valid} \;\right] \;, &(28)\end{aligned}$$

where validity is defined with respect to f, and where we sample $\mathbf{v}^{j^*+1}, \ldots, \mathbf{v}^{t'}$ independently from $\mathcal{D}$. Equivalently, in Eq. (28) we may regard $\mathbf{v}^{j^*+1}, \ldots, \mathbf{v}^{t'}$ as being sampled by independent copies of $C_{\mathcal{D}\text{-samp}}$. Now we may regard the probability in Eq. (28) as being taken over uniform random seeds $r^{j^*+1}, \ldots, r^{t'}$ to $(t' - j^*)$ copies of $C_{\mathcal{D}\text{-samp}}$, and over a uniform setting $r \in \{0,1\}^R$ to the random gates in C.

There are $2^{R_{\text{samp}} \times (t'-j^*) + R}$ equally-likely outcomes to $(r^{j^*+1}, \ldots, r^{t'}, r)$. The outcomes that cause the computation indicated in Eq. (12) to be (j^*-1)-valid are, under our definition, precisely those for which $(r^{j^*+1}, \ldots, r^{t'}, r) \in V_u$. Thus, under our conditioning $[\mathbf{u} = u]$ we have

$$\beta_{j^*-1} \;=\; \frac{|V_u|}{2^{R_{\text{samp}} \times (t'-j^*) + R}} \;=\; \frac{|V_u|}{2^N} \;.$$

This proves part 1 of the Claim.

(2) Condition again on any outcome $[\mathbf{u} = u]$. Under this conditioning, we see that

$$\begin{aligned}\alpha_{j^*} \;&=\; \Pr\left[C(\mathbf{x}^1, \ldots, \mathbf{x}^{t'}) \text{ is } j^*\text{-valid} \;\middle|\; \mathbf{x}^1, \ldots, \mathbf{x}^{j^*}\right] &(29)\\ &=\; \Pr\left[C(y^1, \ldots, y^{j^*-1},\; u,\; \mathbf{v}^{j^*+1}, \ldots, \mathbf{v}^{t'}) \text{ is } j^*\text{-valid} \;\right] \;, &(30)\end{aligned}$$

where we sample $\mathbf{v}^{j^*+1}, \ldots, \mathbf{v}^{t'}$ independently from $\mathcal{D}$; these may again be regarded as sampled by independent copies of $C_{\mathcal{D}\text{-samp}}$, with random gate-sets $r^{j^*+1}, \ldots, r^{t'}$. Again let r denote the random gates of C. The settings to $(r^{j^*+1}, \ldots, r^{t'}, r)$ that cause the computation in Eq. (12) to be j^*-valid are precisely those for which $(r^{j^*+1}, \ldots, r^{t'}, r) \in V_u^{f(u)}$. Thus, conditioned on $[\mathbf{u} = u]$ we have $\alpha_{j^*} = |V_u|/2^N$. This proves part 2. □

Next, let $K := \lceil (N-4) + \log_2(\alpha_{j^*-1}) \rceil$, and let

$$\mathcal{H}^{N,K} \;=\; \left\{ \; h_{A,v} : \mathbb{F}_2^N \to \mathbb{F}_2^K \; \right\}_{A \in \mathbb{F}_2^{K \times N}, v \in \mathbb{F}_2^K}$$

be the hash family given by Proposition 2.5. Under the setting $[\Lambda = \lambda]$, say that $h_{A,v} \in \mathcal{H}^{N,K}$ is *good for* $u \in \{0,1\}^n$ if

$$0^K \;\in\; h_{A,v}\left(V_u^{f(u)}\right) \setminus \left(\bigcup_{z \neq f(u)} h_{A,v}\left(V_u^z\right) \right) \;.$$

Say that a string $u \in \{0,1\}^n$, satisfying $\mathcal{D}(u) > 0$, is *favorable*, and write $u \in \text{Fav}$, if Eq. (4) holds under $[\Lambda = \lambda, \mathbf{x}^{j^*} = u]$. By our choice of λ, we have $\Pr_{\mathbf{u} \sim \mathcal{D}}[\mathbf{u} \in \text{Fav}] \geq 1 - \delta$.

Claim 6.12. *Suppose u is favorable. If $(A, v) \in_r \mathbb{F}_2^{K \times N} \times \mathbb{F}_2^K$, then*

$$\Pr[h_{A,v} \text{ is good for } u] \;>\; .75 \;.$$

Proof. Define

$$V_u^{\text{wrong}} \;:=\; \bigcup_{z \neq f(u)} V_u^z \;.$$

Under the conditioning $[\Lambda = \lambda, \mathbf{x}^{j^*} = u]$, which defines outcomes to $\beta_{j^*-1}, \alpha_{j^*}$, part 2 of Claim 4.3 tells us that

$$\frac{\left|V_u^{f(u)}\right|}{|V_u|} \;=\; \frac{\alpha_{j^*}}{\beta_{j^*-1}} \;.$$

As u is favorable, this gives

$$\frac{\left|V_u^{f(u)}\right|}{|V_u|} \;\in\; [.99, 1] \;, \qquad \text{and so} \qquad \frac{|V_u^{\text{wrong}}|}{|V_u|} \;\leq\; .01 \;.$$

Next we combine part 1 of Claim 6.11 with Eq. (4) to find that

$$\frac{|V_u|}{2^N \cdot \alpha_{j^*-1}} \;=\; \frac{\beta_{j^*-1}}{\alpha_{j^*-1}} \;\in\; [.99, 1.012] \;;$$

we also have $2^K \in [2^{-4} \cdot 2^N \alpha_{j^*-1}, 2^{-3} \cdot 2^N \alpha_{j^*-1}]$, so that

$$\theta \;:=\; \frac{|V_u|}{2^K} \;\in\; [8 \cdot .99, 16 \cdot 1.012] \;\subset\; [7, 17] \qquad \text{and} \qquad \theta' \;:=\; \frac{|V_u^{\text{wrong}}|}{2^K} \;\leq\; .01\theta \;.$$

We apply Corollary 2.7 with $U := \mathbb{F}_2^N, U_{(\text{i})} := V_u$, and $U_{(\text{ii})} := V_u^{\text{wrong}}$; by the same calculations used to prove Claim 4.4, we find that

$$\Pr_{A,v}\left[0^K \in h_{A,v}\left(V_u\right) \setminus h_{A,v}\left(V_u^{\text{wrong}}\right)\right] \;>\; .75 \;.$$

This proves Claim 6.12. □

Let $T := 40n$. Suppose we select T hash functions $(h_{A^1,v^1}, \ldots, h_{A^T,v^T})$ independently, with $h_{A^i,v^i} \in_r \mathcal{H}^{N,K}$. For any $u \in \{0,1\}^n$, let

$$X^+(u) \ := \ \sum_{i \in [T]} \mathbf{1}\left[h_{A^i,v^i} \text{ is good for } u\right] \ .$$

Consider any favorable u. By using Claim 4.4 and applying Lemma 2.1 to $X^+(u)$, we find that with probability at least $1 - \exp(-2(.15)^2 \cdot T) > 1 - 2^{-2n}$,

$$X^+(u) \ \geq \ .6T \ . \tag{31}$$

Then with positive probability, Eq. (31) holds for *every* favorable $u \in \{0,1\}^n$. Thus there exists some choice

$$\overline{h} \ = \ (h_1^*, \ldots, h_T^*) \ = \ \left(h_{A^1,v^1}, \ldots, h_{A^T,v^T}\right)$$

such that Eq. (31) holds for every favorable u.

We can now apply Lemma 2.8, just as in the proof of Claim 4.2. We note that under our current settings, $N, K, T \leq \text{poly}(\text{size}(C) + \text{size}(C_{\mathcal{D}\text{-samp}}))$, and each hash function h_i^* can be evaluated using $O(KN)$ gates. The one novel element is that to check whether a string $w \in \{0,1\}^N$ lies in the set V_u (as defined here), and if so to determine which V_u^z contains it, now requires the evaluation of $C_{\mathcal{D}\text{-samp}}$ on $(t - j^*)$ given random seeds, as in Eq. (23). The total number of gates needed for C_{Vtest} is polynomial in $\text{size}(C) + \text{size}(C_{\mathcal{D}\text{-samp}})$. We obtain a circuit $C^\dagger$ of size $\leq \text{poly}(\text{size}(C) + \text{size}(C_{\mathcal{D}\text{-samp}}))$, such that $F_{C^\dagger}(u) = \{f(u)\}$ for every $u \in \text{Fav}$. As $\Pr_{\mathbf{u} \sim \mathcal{D}}[\mathbf{u} \in \text{Fav}] \geq 1 - \delta$, we conclude that $C^\dagger$ $(1-\delta)$-defines f with respect to $\mathcal{D}$, and is a suitable choice for C'. This proves Theorem 6.10. □

6.3 Proof of Theorem 6.1

Theorem 6.13 (Theorem 6.1, restated)**.** *Let $n, d, t \in \mathbb{N}^+$ with $t > 1$. Let $f : \{0,1\}^n \to \{0,1\}^d$, and let $q \in (0,1)$. Let $\mathcal{D}$ be a distribution over $\{0,1\}^n$ sampleable by a probabilistic circuit $C_{\mathcal{D}\text{-samp}}$. Suppose there is a probabilistic circuit $C : \{0,1\}^{n \times t} \to \{0,1\}^t$, such that C is a q-direct-product solver for $f^{\otimes t}$ with respect to $\mathcal{D}^{\otimes t}$.*

Let $\varepsilon \in (0,1)$ be given, satisfying $\varepsilon > \frac{2^{12}}{t^{1/3}}$. Assume also that

$$q \ \geq \ \exp\left(-\frac{\varepsilon^{3/2}\sqrt{t}}{10^{13}}\right) \ ; \tag{32}$$

then, there is a nondeterministic mapping circuit C_ε^* on n input bits that $(1-\varepsilon)$-defines f with respect to $\mathcal{D}$, and such that

$$\text{size}(C_\varepsilon^*) \ \leq \ \text{poly}\left(\text{size}(C) + \text{size}(C_{\mathcal{D}\text{-samp}})\right) \ .$$

Proof. To dispose of an easy case, suppose first that $\varepsilon t \leq 1$. Then, we have

$$q \ \geq \ \exp\left(-\frac{\varepsilon \cdot (\varepsilon t)^{1/2}}{10^{13}}\right) \ \geq \ \exp\left(-\frac{\varepsilon}{10^{13}}\right) \ > \ 1 - \varepsilon \ ,$$

where in the last step we used that $e^{-x} \geq 1 - x$ for $x \geq 0$. In other words, our success guarantee for C in computing $f^{\otimes t}$ is already at least the desired success guarantee for computing a single instance of f. We non-uniformly fix inputs $x^2, \ldots, x^t$ to C that maximize the probability over $\mathbf{x} \sim \mathcal{D}$ that $C(\mathbf{x}, x^2, \ldots, x^t) = f^{\otimes t}(\mathbf{x}, x^2, \ldots, x^t)$. We obtain the desired circuit C^*_ε as the circuit which outputs just the first d output bits of this computation.

So from now on let us assume $\varepsilon \in [1/t, 1)$. Let us set

$$t' \ := \ \left\lceil \sqrt{(\varepsilon t)} \right\rceil \ , \qquad \xi \ := \ \exp\left(-\frac{\varepsilon^{3/2}\sqrt{t}}{2^{18}}\right) \ .$$

ξ is at most $1/2$ by our assumption $\varepsilon > \frac{2^{12}}{t^{1/3}}$, i.e., $\varepsilon^{3/2}\sqrt{t} > 2^{18}$. Also, from our assumption $\varepsilon \in [1/t, 1)$, we have

$$1 \ \leq t' \ \leq \ \min(t, 2\sqrt{\varepsilon t}) \ .$$

Thus we may apply Lemma 6.2 with our choice of t', ξ, to obtain a probabilistic circuit

$$\tilde{C} : \{0,1\}^{n \times t'} \to \{0,1\}^{t'} \ ,$$

satisfying

$$\text{size}(\tilde{C}) \ \leq \ \text{size}(C) + \text{size}(C_{\mathcal{D}\text{-samp}}) \cdot t \ ,$$

such that $\tilde{C}$ is a $(1-\zeta, \xi q)$-input-confident direct product solver for $f^{\otimes t'}$ with respect to the input distribution $\mathcal{D}^{\otimes t'}$; we have

$$\begin{aligned} \zeta \ &= \ \frac{.6}{1-\xi}\sqrt{\frac{\log_2(1/q)}{\lfloor t/t' \rfloor}} \\ &\leq \ 2\sqrt{\frac{\log_2(1/q)t'}{t}} \\ &< \ 2^{-19}\varepsilon \ , \end{aligned}$$

where we used the fact that $\xi \leq 1/2$ as well as our assumption in Eq. (32). Next, we apply Theorem 6.10 to $\tilde{C}$, with $q' := \xi q$; we obtain a nondeterministic mapping circuit $C' : \{0,1\}^n \to \{0,1\}^d$ that $(1-\delta)$-defines f with respect to input distribution $\mathcal{D}$, where

$$\begin{aligned} \delta \ &= \ \frac{2^{16}}{t'} \ln\left(\frac{1}{\xi q}\right) + 2^{18}\zeta \\ &\leq \ \varepsilon/2 + \varepsilon/2 \ = \ \varepsilon \end{aligned}$$

(here, we again used Eq. (32). Also, as guaranteed by Theorem 6.10, we have

$$\text{size}(C') \ \leq \ \text{poly}(\text{size}(\tilde{C}) + \text{size}(C_{\mathcal{D}\text{-samp}})) \ \leq \ \text{poly}(\text{size}(C) + \text{size}(C_{\mathcal{D}\text{-samp}})) \ .$$

Thus we may take C' as our desired circuit C^*_ε. This proves Theorem 6.1. □

7 A derandomized direct product theorem

7.1 Expander walks and the theorem statement

Thus far, we have focused on the task of computing a function f evaluated on t independent inputs $x^1, \ldots, x^t$. In this section we consider the setting in which the strings x^j are not fully independent, but instead represent the t steps of a random walk on an *expander graph* over vertex set $\{0,1\}^n$. Such a collection of inputs can be sampled using $n + O(t)$ random bits. We will show that, if f is the characteristic function of a language $L \in \mathsf{NP}$ that is mildly hard on average against nondeterministic mapping circuits (with respect to the uniform input distribution), then computing f on these t pseudorandom inputs is extremely hard.

More formally, we will study the well-known *expander-walk generator* of [AKS87]. This is a polynomial-time computable function which, for each $n \geq 1, t \geq 2$, maps a seed

$$w \;=\; (w^1, s^1, s^2, \ldots, s^{t-1}) \;\in \{0,1\}^{n+4(t-1)}$$

to a string

$$\mathrm{GEN}_{n,t}(w) \;=\; (v^1, \ldots, v^t) \;\in\; \{0,1\}^{n\times t} \;,$$

as we will describe next. The behavior of $\mathrm{GEN}_{n,t}$ is defined in terms of a graph $\mathcal{G}_n$ with vertex set $V(\mathcal{G}_n) = \{0,1\}^n$. The graph $\mathcal{G}_n$ is undirected (with self-loops and multiple edges allowed) and k-regular for some $k = O(1)$, with normalized second eigenvalue λ_n at most some fixed constant $\lambda < 1$. The graph family used must be *strongly explicit*, in the sense that there is a polynomial-time algorithm $M_{\text{adj}}(v, s)$ which, given $v \in \{0,1\}^n$ and $s \in \{0,1\}^{\lceil \log_2 k \rceil}$ (considered to represent an integer in $\{1, \ldots, k\}$), outputs the s^{th} neighbor of v in $\mathcal{G}_n$ according to some fixed ordering. By using the classical construction due to Margulis [Mar73], along with explicit eigenvalue bounds due to Gabber and Gallil [GG81], we may obtain such an explicit graph family with $\lambda = .99$ and $k = 16$, so that $\log_2 k = 4$.[13] We fix such a graph family in the definition of our generators $\mathrm{GEN}_{n,t}$ for the remainder of the paper.

The values $v^1, \ldots, v^t$ always represent a walk of length t in $\mathcal{G}_n$. They are defined inductively by setting $v^1 := w^1$ and, for $j > 1$, setting

$$v^j \;:=\; M_{\text{adj}}(v^{j-1}, s^{j-1}) \;.$$

Throughout Section 7, we will freely use $v^j(w)$ to denote the j^{th} vertex output by $\mathrm{GEN}_{n,t}(w)$, and $\overline{v}(w)$ to denote $(v^1(w), \ldots, v^t(w))$; the values n, t will be clear from the context.

Given a language L, an input length n, and a $t \geq 2$, we consider the composed function $(\chi_{L,n}^{\otimes t} \circ \mathrm{GEN}_{n,t}) : \{0,1\}^{n+4(t-1)} \to \{0,1\}^t$ which acts as

$$(\chi_{L,n}^{\otimes t} \circ \mathrm{GEN}_{n,t})(w) \;=\; (\chi_L(v^1(w)), \chi_L(v^2(w)), \ldots, \chi_L(v^t(w))) \;.$$

We study the difficulty of computing $\chi_{L,n}^{\otimes t}$ on inputs drawn from the expander-walk generator, where the circuit is given the seed w as input. Our goal in this section is to prove the following theorem:

Theorem 7.1. *Fix $n \geq 1$, $t \geq 2$. Let L be a language, and suppose $L_n \subseteq \{0,1\}^n$ is recognized by an* ordinary *nondeterministic circuit C_{rec} (see Section 2.2). Suppose also that there is a probabilistic circuit $C : \{0,1\}^{n\times t} \to \{0,1\}^t$ that Q^*-computes $(\chi_{L,n}^{\otimes t} \circ \mathrm{GEN}_{n,t})$ with respect to the uniform distribution on $\{0,1\}^{n+4(t-1)}$.*

[13] We don't attempt to optimize the degree and expansion parameters. The Margulis construction is 8-regular and has vertex set $\mathbb{Z}_m \times \mathbb{Z}_m$ for $m > 1$. If n is even, we take the Margulis graph over $\{0,1\}^n$ and double each edge. If n is odd, we double each vertex v in the Margulis graph over $\{0,1\}^{n-1}$, and connect each copy to both copies of its original neighbors. See [HLW06] for general background on expander graphs, and [HLW06, Sec. 8] for details on the Margulis graphs.

Let $\varepsilon > 0$. If

$$Q^* \ \geq \ \frac{1600}{\varepsilon} \cdot \exp\left(\frac{-\varepsilon^2 t}{2 \cdot 10^9}\right) \ ,$$

then there is a nondeterministic mapping circuit $C^*_\varepsilon : \{0,1\}^n \to \{0,1\}$ that $(1-\varepsilon)$-defines $\chi_{L,n}$ with respect to the uniform distribution on $\{0,1\}^n$, and that satisfies

$$\mathrm{size}(C^*_\varepsilon) \ \leq \ \mathrm{poly}(\mathrm{size}(C) + \mathrm{size}(C_{\mathrm{rec}})) \ .$$

(In the size bound above there is no hidden dependence on ε.)

In Section 7.2 we will prove some useful probabilistic lemmas about expander walks, and in Section 7.3 we will apply them to prove Theorem 7.1.

7.2 Probabilistic analysis of expander walks

To analyze the behavior of our generator, we will use a powerful result known as the "strong Chernoff bound for expander walks" [WX05, WX08, Hea08].

Theorem 7.2. *[Hea08] Let $G = (V, E)$ be a k-regular graph with normalized second eigenvalue $\lambda \in (0,1)$, let $t > 0$, and let $f_1, \ldots, f_t : V \to [0,1]$ have expectations $\mu_1, \ldots, \mu_t$ (over a uniform choice of input $v \in V$). Taking a random walk $v^1, \ldots, v^t$ on G, with uniformly chosen starting vertex,*[14] *we have for all $\theta > 0$,*

$$\Pr\left[\sum_{j\in[t]} f_j(v^j) - \sum_{j\in[t]} \mu_j \geq \theta t\right] \ \leq \ e^{-\frac{\theta^2(1-\lambda)t}{4}} \ .$$

We have the same probability bound for the event $\left[\sum_{j\in[t]} f_j(v^j) - \sum_{j\in[t]} \mu_j \leq -\theta t\right]$.

Our analysis of expander walks on $\mathcal{G}_n$ will focus upon a "good" subset of interest $A \subseteq \{0,1\}^{n+4(t-1)}$. We will establish that if A is "large," then for most indices $j \in [t]$, drawing w uniformly at random and conditioning on the value $v^j(w)$ is unlikely to significantly affect the probability that $w \in A$. For brevity, we will use

$$w \sim \mathcal{W}$$

to denote the uniform distribution $w \in_r \{0,1\}^{n+4(t-1)}$.

Define

$$Q \ := \ \Pr_{w\sim\mathcal{W}}[w \in A] \ = \ \mathcal{W}(A) \tag{33}$$

and, for each $j \in [t]$ and $v \in \{0,1\}^n$, define the conditional probability

$$Q[v,j] \ := \ \Pr_{w\sim\mathcal{W}}[w \in A | v^j(w) = v] \ . \tag{34}$$

Define the "exceptional" sets

$$B_j^+ \ := \ \{v \in \{0,1\}^n : Q[v,j] > 1.01Q\} \ , \qquad B_j^- \ := \ \{v \in \{0,1\}^n : Q[v,j] < .99Q\} \ ,$$

[14] Each v^j in turn is chosen as the neighbor of v^{j-1} along an edge uniformly selected from the edges of v^{j-1}.

and let

$$\zeta_j^+ \;:=\; \frac{|B_j^+|}{2^n} \;, \qquad \zeta_j^- \;:=\; \frac{|B_j^-|}{2^n} \;.$$

Let

$$\zeta_{\mathrm{avg}}^+ \;:=\; \frac{1}{t}\sum_{j\in[t]} \zeta_j^+ \;, \qquad \zeta_{\mathrm{avg}}^- \;:=\; \frac{1}{t}\sum_{j\in[t]} \zeta_j^- \;.$$

Lemma 7.3. *Assume that*

$$Q \;\geq\; \frac{800}{\varepsilon}\cdot \exp\left(-\frac{\varepsilon^2 t}{2.56\cdot 10^8}\right) \;,$$

for some $\varepsilon > 0$. Then, we have

$$\zeta_{\mathrm{avg}}^+ \;\leq\; \varepsilon/4 \qquad \text{and} \qquad \zeta_{\mathrm{avg}}^- \;\leq\; \varepsilon/4 \;.$$

Proof. Let $\mathcal{W}_A$ denote a sample from $\mathcal{W}$ conditioned on landing in A; this is the uniform distribution over A. We let $\mathcal{V}_A^j$ denote the distribution on the j^{th}-step vertex $v^j(w)$ when $w \sim \mathcal{W}_A$.

Claim 7.4. *For each $j \in [t]$,*

$$\mathcal{V}_A^j(B_j^+) - \zeta_j^+ \;\geq\; .01\zeta_j^+ \qquad \text{and} \qquad \zeta_j^- - \mathcal{V}_A^j(B_j^-) \;\geq\; .01\zeta_j^- \;.$$

Proof. We will assume $j = 1$, the other cases being handled identically. Define

$$A^+ \;:=\; \{w \in A : v^1(w) \in B_1^+\} \;.$$

We have

$$\mathcal{V}_A^1(B_1^+) \;=\; \frac{|A^+|}{|A|} \tag{35}$$

By the definition of B_1^+, we have

$$\frac{|A^+|}{2^{n+4(t-1)}} \;\geq\; \frac{|B_1^+|}{2^n}\cdot(1.01Q) \;,$$

while

$$\frac{|A^+|}{2^{n+4(t-1)}} \;=\; Q \;.$$

Thus, Eq. (35) implies

$$\mathcal{V}_A^1(B_1^+) \;\geq\; 1.01\cdot\frac{|B_1^+|}{2^n} \;. \tag{36}$$

This gives the first part of the Claim. For the second part, define

$$A^- \;:=\; \{w \in A : v^1(w) \in B_1^-\} \;.$$

We have

$$\mathcal{V}_A^1(B_1^-) \;=\; \frac{|A^-|}{|A|} \tag{37}$$

From the definition of B_1^-, we see that

$$\frac{|A^-|}{2^{n+4(t-1)}} \;\leq\; \frac{|B_1^-|}{2^n}\cdot(.99Q) \;,$$

while again $\frac{|A|}{2^{n+4(t-1)}} = Q$. Thus, Eq. (37) implies

$$\mathcal{V}_A^1(B_1^-) \ \leq \ .99 \cdot \frac{|B_1^-|}{2^n} \ . \tag{38}$$

This gives the second part, proving the Claim. □

For each $j \in [t]$, define functions $f_j^+, f_j^- : \{0,1\}^n \to \{0,1\}$ by

$$f_j^+(v) \ := \ \mathbf{1}[v \in B_j^+] \ , \qquad f_j^-(v) \ := \ \mathbf{1}[v \in B_j^-] \ .$$

We have

$$\mathbb{E}_{v \in_r \{0,1\}^n}[f_j^+(v)] \ = \ \zeta_j^+ \ , \qquad \mathbb{E}_{v \in_r \{0,1\}^n}[f_j^-(v)] \ = \ \zeta_j^- \ . \tag{39}$$

Given a string $w \in \{0,1\}^{n+4(t-1)}$, define

$$F^+(w) \ := \ \sum_{j \in [t]} f_j^+(v^j(w)) \ , \qquad F^-(w) \ := \ \sum_{j \in [n]} f_j^-(v^j(w)) \ .$$

By Theorem 7.2 and the definition of the generator $\mathrm{GEN}_{n,t}$, for $\theta > 0$ we have

$$\Pr_{w \sim \mathcal{W}}\left[F^+(w) - \sum_{j \in [t]} \zeta_j^+ \geq \theta t\right] \ \leq \ e^{-\frac{\theta^2 (.01) t}{4}} \ , \tag{40}$$

where we used our upper bound $\lambda \leq .99$ on the normalized second eigenvalue of $\mathcal{G}_n$. Similarly,

$$\Pr_{w \sim \mathcal{W}}\left[F^-(w) - \sum_{j \in [t]} \zeta_j^- \leq -\theta t\right] \ \leq \ e^{-\frac{\theta^2 (.01) t}{4}} \ . \tag{41}$$

On the other hand, Claim 7.4 tells us that

$$\mathbb{E}_{w \sim \mathcal{W}_A}[f_j^+(v)] \ \geq \ 1.01 \zeta_j^+ \ , \tag{42}$$

so that, summing,

$$\mathbb{E}_{w \sim \mathcal{W}_A}[F^+(w)] \ \geq \ 1.01 \sum_{j \in [t]} \zeta_j^+ \ . \tag{43}$$

Similarly,

$$\mathbb{E}_{w \sim \mathcal{W}_A}[F^-(w)] \ \leq \ .99 \sum_{j \in [t]} \zeta_j^- \ . \tag{44}$$

Now, a basic calculation shows that, for any random variable X taking values in the interval $[0, t]$, and any $\gamma > 0$, we have

$$\Pr[X \geq (1-\gamma)\mathbb{E}[X]] \ \geq \ \frac{\gamma \cdot \mathbb{E}[X]}{t - (1-\gamma)\mathbb{E}[X]} \ \geq \ \frac{\gamma \cdot \mathbb{E}[X]}{t} \tag{45}$$

and (by Markov's inequality)

$$\Pr[X \leq (1+\gamma)\mathbb{E}[X]] \ \geq \ 1 - \frac{1}{1+\gamma} \ . \tag{46}$$

From Eqs. (43) and (45) we compute that

$$\Pr_{w\sim\mathcal{W}_A}\left[F^+(w)\geq 1.005\cdot\sum_{j\in[t]}\zeta_j^+\right] \;\geq\; \frac{\frac{5}{1010}\mathbb{E}[F^+(w)]}{t}$$
$$\geq\; \frac{5\left(1.01\sum_{j\in[t]}\zeta_j^+\right)}{1010t}$$
$$=\; .005\zeta_{\text{avg}}^+\;. \tag{47}$$

Similarly, from Eqs. (44) and (46) we compute that

$$\Pr_{w\sim\mathcal{W}_A}\left[F^-(w)\leq .995\cdot\sum_{j\in[t]}\zeta_j^+\right] \;\geq\; 1-\frac{.99}{.995} \;>\; .005\;. \tag{48}$$

Combining the definition $Q := \Pr_{w\sim\mathcal{W}}[w\in A]$ with Eq. (47), we find

$$\Pr_{w\sim\mathcal{W}}\left[F^+(w)-\sum_{j\in[t]}\zeta_j^+\geq .005\sum_{j\in[t]}\zeta_j^+\right] \;\geq\; Q\cdot .005\zeta_{\text{avg}}^+ \tag{49}$$

and, using Eq. (47) similarly we obtain

$$\Pr_{w\sim\mathcal{W}}\left[F^-(w)-\sum_{j\in[t]}\zeta_j^-\leq -.005\sum_{j\in[t]}\zeta_j^+\right] \;\geq\; Q\cdot .005\;. \tag{50}$$

Combining Eq. (49) with Eq. (40) under the setting $\theta := \frac{.005}{t}\sum_{j\in[t]}\zeta_j^+ = .005\zeta_{\text{avg}}^+$, we find that

$$.005Q\cdot\zeta_{\text{avg}}^+ \;\leq\; \exp\left(-\frac{\left(.005\zeta_{\text{avg}}^+\right)^2 t}{400}\right)\;,$$

or equivalently,

$$Q \;\leq\; \left(\frac{200}{\zeta_{\text{avg}}^+}\right)\cdot\exp\left(-\frac{(\zeta_{\text{avg}}^+)^2 t}{1.6\cdot 10^7}\right)\;.$$

(We are assuming here that $\zeta_{\text{avg}}^+ > 0$; if $\zeta_{\text{avg}}^+ = 0$ then there is nothing to prove.) Note that the right-hand side above is an decreasing function of ζ_{avg}^+ on $(0,1]$. By our assumption on Q in Lemma 7.3, we find that $\zeta_{\text{avg}}^+ \leq \varepsilon/4$. This proves the first assertion of Lemma 7.3.

Next, combining Eq. (49) with Eq. (40) under the setting $\theta := .005\zeta_{\text{avg}}^-$, we have

$$.005Q \;\leq\; \exp\left(-\frac{\left(.005\zeta_{\text{avg}}^-\right)^2 t}{400}\right)\;,$$

and using our assumption on Q again, this implies $\zeta_{\text{avg}}^- \leq \varepsilon/4$, completing the proof of Lemma 7.3.

□

The next Lemma requires some further setup. Let $A \subseteq \{0,1\}^{n+4(t-1)}$ as in Lemma 7.3, with $\Pr_{w \in_r \{0,1\}^{n+4(t-1)}}[w \in A] = Q$. For each $w \in A$, suppose there is an associated index set

$$\mathrm{Bad}_w \subseteq [t] \ .$$

For $w \notin A$, define $\mathrm{Bad}_w := \emptyset$. For $v \in \{0,1\}^n, j \in [t]$, define the conditional probability

$$Q^\circ[v,j] \ := \ \Pr_{w \sim \mathcal{W}}[w \in A \wedge j \notin \mathrm{Bad}_w | v^j(w) = v] \ . \tag{51}$$

Note that $Q^\circ[v,j] \le Q[v,j]$. Define

$$B_j^\circ \ := \ \{v \in \{0,1\}^n : Q^\circ[v,j] < Q[v,j] - .01Q\} \ ,$$

and set

$$\zeta_j^\circ \ := \ |B_j^\circ|/2^n \ , \qquad \zeta_{\mathrm{avg}}^\circ \ := \ \frac{1}{t}\sum_{j \in [t]} \zeta_j^\circ \ .$$

Lemma 7.5. *Assume that* Bad_w *is "small" for almost all strings* $w \in A$*:*

$$\Pr_{w \sim \mathcal{W}_A}\left[|\mathrm{Bad}_w| > \frac{\varepsilon t}{800}\right] \ \le \ \frac{\varepsilon}{800} \ . \tag{52}$$

Then,

$$\zeta_{\mathrm{avg}}^\circ \ \le \ \varepsilon/4 \ .$$

Proof. For any v, j, we have

$$\begin{aligned} Q^\circ[v,j] \ &\ge \ \Pr_{w \sim \mathcal{W}}[w \in A | v^j(w) = v] - \Pr_{w \sim \mathcal{W}}[j \in \mathrm{Bad}_w | v^j(w) = v] \\ &= \ Q[v,j] - 2^n \cdot \Pr_{w \sim \mathcal{W}}[j \in \mathrm{Bad}_w \wedge v^j(w) = v] \ . \end{aligned} \tag{53}$$

Summing over all v, j and using Eq. (52), along with the fact that $\mathrm{Bad}_w = \emptyset$ for $w \notin A$, we find that

$$\begin{aligned} \sum_{v \in \{0,1\}^n, j \in [t]} (Q[v,j] - Q^\circ[v,j]) \ &\le \ 2^n \sum_{j \in [t]} \Pr_{w \sim \mathcal{W}}[j \in \mathrm{Bad}_w] \\ &= \ 2^n \cdot \mathbb{E}_{w \sim \mathcal{W}}[|\mathrm{Bad}_w|] \\ &\le \ 2^n \cdot Q \cdot \frac{\varepsilon t}{400} \ . \end{aligned} \tag{54}$$

On the other hand, for each j, using the definition of B_j° we have

$$\sum_{v \in \{0,1\}^n} (Q[v,j] - Q^\circ[v,j]) \ \ge \ |B_j^\circ| \cdot (.01Q) \ .$$

Summing this over all j, and combining with Eq. (54), we have

$$.01Q \sum_{j \in [t]} |B_j^\circ| \ \le \ \frac{2^n Q \varepsilon t}{400} \ ,$$

or equivalently,

$$\zeta_{\mathrm{avg}}^\circ \ = \ \frac{1}{t}\sum_{j \in [t]} \zeta_j^\circ \ \le \ \varepsilon/4.$$

□

7.3 Applying the lemmas

Proof of Theorem 7.1. First, we may assume that C is deterministic (by fixing any internal randomness to maximize the success probability). Let $C_1(w), \ldots, C_t(w)$ denote the t bits output by C on input $\overline{v}$. Let $W_{\mathrm{suc}} \subseteq \{0,1\}^{n+4(t-1)}$, the *successful seeds*, be the set of strings w for which

$$C(w) \;=\; (\chi_{L,n}^{\otimes t} \circ \mathrm{GEN}_{n,t})(w) \;.$$

Let $\rho := |L_n|/2^n$. Let $W_{\mathrm{attr}} \subseteq \{0,1\}^{n+4(t-1)}$, the *attractive seeds*, be the set of w which satisfy the following two conditions:

1. The number of indices $j \in [t]$ for which $C_j(w) = 1$ is in the range
$$\left[\left(\rho - \frac{\varepsilon}{1600}\right)t, \left(\rho + \frac{\varepsilon}{1600}\right)t\right] \;;$$
2. For every j such that $C_j(w) = 1$, we also have $\chi_L(v^j(w)) = 1$.

There is no inclusion relation between the sets $W_{\mathrm{suc}}, W_{\mathrm{attr}}$. The idea, however, is that W_{attr} will act as a reasonable *surrogate* for W_{suc}; this surrogate set has the advantage of being efficiently recognizable using nondeterminism.

For any $\overline{v} = (v^1, \ldots, v^t) \in \{0,1\}^{n\times t}$, let

$$\#_L(\overline{v}) \;:=\; |\{j \in [t] : v^j \in L\}| \;.$$

Next, define functions $f_1, \ldots, f_t : \{0,1\}^n \to \{0,1\}$ by letting $f_j(v) := \chi_L(v)$ for all j. Recall that $\mathcal{W}$ denotes the uniform distribution on $\{0,1\}^{n+4(t-1)}$. Applying Theorem 7.2 to these functions with $\theta := \varepsilon/1600$, and using the definition of $\mathrm{GEN}_{n,t}$, we have

$$\Pr_{w\sim\mathcal{W}}\left[|\#_L(\overline{v}(w)) - \rho t| > \frac{\varepsilon t}{1600}\right] \;<\; 2\exp\left(-\frac{(.01)\varepsilon^2 t}{4\cdot(1600)^2}\right) \;<\; 2\exp\left(-\frac{\varepsilon^2 t}{2\cdot 10^9}\right) \;. \tag{55}$$

Define

$$Q \;:=\; \Pr_{w\sim\mathcal{W}}[w \in W_{\mathrm{attr}}] \;.$$

Using Eq. (55) and our largeness assumption on Q^*, we have

$$Q \;\geq\; \Pr_{w\sim\mathcal{W}}[w \in W_{\mathrm{suc}} \cap W_{\mathrm{attr}}] \;>\; Q^* - 2\exp\left(-\frac{\varepsilon^2 t}{2\cdot 10^9}\right) \;>\; Q^*/2 \;.$$

(We note that Q may even be larger than Q^*.) Set

$$A \;:=\; W_{\mathrm{attr}} \;.$$

We have $\Pr_{w\in_r\{0,1\}^N}[w \in A] = Q > Q^*/2$, and from this we verify that the hypothesis of Lemma 7.3 is satisfied. Thus, we have $\zeta^+_{\mathrm{avg}}, \zeta^-_{\mathrm{avg}} \leq \varepsilon/4$, where $\zeta^+_{\mathrm{avg}}, \zeta_{\mathrm{avg}}$ are as defined in Section 7.2.

Next, for each $w \in A$, define the set

$$\mathrm{Bad}_w \;:=\; \{j \in [t] : C_j(w) = 0 \neq \chi_L(v^j(w))\} \;. \tag{56}$$

For $w \notin A$, let $\mathrm{Bad}_w := \emptyset$. Note that for $w \in A$,

$$|\mathrm{Bad}_w| \;\leq\; \#_L(\overline{v}(w)) - \left(\rho - \frac{\varepsilon}{1600}\right) t \;.$$

This is at most $\frac{\varepsilon t}{800}$ provided $\#_L(\overline{v}(w)) \leq \left(\rho + \frac{\varepsilon}{1600}\right) t$, which, by another appeal to Theorem 7.2, occurs with probability greater than $1 - \exp\left(-\frac{\varepsilon^2 t}{2 \cdot 10^9}\right)$ over $w \sim \mathcal{W}$. Thus,

$$\Pr_{w \sim \mathcal{W}_A}\left[|\mathrm{Bad}_w| > \frac{\varepsilon t}{800}\right] \;\leq\; \frac{\Pr_{w\sim\mathcal{W}}\left[|\mathrm{Bad}_w| > \frac{\varepsilon t}{800}\right]}{Q} \;\leq\; Q^{-1}\exp\left(-\frac{\varepsilon^2 t}{2 \cdot 10^9}\right) \;\leq\; \frac{\varepsilon}{800} \;, \qquad (57)$$

using our assumption on Q^* and the fact that $Q \geq Q^*/2$.

With the terms $Q^\circ[v, j], B^\circ_j, \zeta^\circ_j, \zeta^\circ_{\mathrm{avg}}$ as defined in Section 7.2, we have verified that the hypothesis of Lemma 7.5 is satisfied. We apply that Lemma to find that $\zeta^\circ_{\mathrm{avg}} \leq \varepsilon/4$. Combining this with our finding that $\zeta^+_{\mathrm{avg}}, \zeta^-_{\mathrm{avg}} \leq \varepsilon/4$, we conclude that there is an index $j^* \in [t]$ for which

$$\zeta^+_{j^*} + \zeta^-_{j^*} + \zeta^\circ_{j^*} \;\leq\; 3\varepsilon/4 \;.$$

We fix one such value j^*. We are now ready to build our circuit C^*_ε. To do so, we will aim to apply Lemma 2.8. Suppose that C_{rec}, the ordinary nondeterministic circuit recognizing L_n, has $m > 0$ nondeterministic gates. We set

$$N \;:=\; (n + 4(t-1)) + 1 + (m+1)t \;, \qquad K \;:=\; \lceil (N-4) + \log_2 Q \rceil \;.$$

We consider strings $\overline{x} \in \{0,1\}^N$ as having the form

$$\overline{x} \;=\; (w, a, y^0, y^1, y^2, \ldots, y^t) \;,$$

where $w \in \{0,1\}^{n+4(t-1)}$, $a \in \{0,1\}$, and $y^j \in \{0,1\}^m$ for $j \in [0,t]$. Now we define our sets

$$V^b_u \subseteq \{0,1\}^N \;, \qquad u \in \{0,1\}^n \;,\; b \in \{0,1\}$$

as in Lemma 2.8. We let $\overline{x} \in V^1_u$ exactly if $a = 1$ and $C^{\mathrm{det}}_{\mathrm{rec}}(u, y^0) = 1$ (noting that this implies $u \in L$). We let $\overline{x} \in V^0_u$ exactly if the following conditions hold:

1. $a = 0$;
2. $v^{j^*}(w) = u$;
3. $C_{j^*}(w) = 0$;
4. The number of indices $j \in [t]$ such that $C_j(w) = 1$ is in the range
$$\left[\left(\rho - \frac{\varepsilon}{1600}\right)t, \left(\rho + \frac{\varepsilon}{1600}\right)t\right] \;;$$
5. For each $j \in [t]$ for which $C_j(w) = 1$, we have $C^{\mathrm{det}}_{\mathrm{rec}}(u, y^j) = 1$.

Note that conditions 4-5 imply that $w \in A = W_{\mathrm{attr}}$.

The sets V_u^1, V_u^0 are disjoint by construction. It is clear that given a tuple $(\overline{x}, u) \in \{0,1\}^{N+n}$, one can test whether $\overline{x} \in V_u^1 \cup V_u^0$ (and if so, which of the two sets contains $\overline{x}$) using a circuit C_{Vtest} of size $\mathrm{poly}(n + t + m + \mathrm{size}(C_{\mathrm{rec}}) + \mathrm{size}(C)) = \mathrm{poly}(\mathrm{size}(C_{\mathrm{rec}}) + \mathrm{size}(C))$.[15]

Define a set of *favorable* length-n inputs $\mathrm{Fav} \subseteq \{0,1\}^n$ by letting

$$\mathrm{Fav} \;:=\; \{u : Q^{\circ}[u, j^*] \geq .98Q \wedge Q[u, j^*] \leq 1.01Q\} \;. \tag{58}$$

We claim that Fav is large. Suppose that $u \notin B_{j^*}^{+} \cup B_{j^*}^{-} \cup B_{j^*}^{\circ}$. Then, by the definitions, we have

$$Q[u, j^*] \;\in\; [.99Q, 1.01Q] \;, \qquad Q^{\circ}[u, j^*] \;\geq\; Q[u, j^*] - .01Q \;\geq\; .98Q \;,$$

so that $u \in \mathrm{Fav}$. Thus,

$$|\mathrm{Fav}| \;\geq\; 2^n - |B_{j^*}^{+}| - |B_{j^*}^{-}| - |B_{j^*}^{\circ}| \;=\; 2^n(1 - \zeta_{j^*}^{+} - \zeta_{j^*}^{-} - \zeta_{j^*}^{\circ}) \;\geq\; (1 - 3\varepsilon/4)2^n \;.$$

As in our other direct product reductions, we will apply hashing. However, we will slightly modify the approach to fit the present proof. Let

$$N' \;:=\; n + 4(t-1) \;, \qquad K \;:=\; 4t - 8 + \lceil \log_2(Q) \rceil \;,$$

and let

$$\mathcal{H}^{N',K} \;=\; \left\{ \;h_{A,v} : \mathbb{F}_2^{N'} \to \mathbb{F}_2^{K}\; \right\}_{A \in \mathbb{F}_2^{K \times N'}, v \in \mathbb{F}_2^{K}}$$

be the hash family as given by Proposition 2.5. For $A \in \mathbb{F}_2^{K \times N'}, v \in \mathbb{F}_2^K$, define $\hat{h}_{A,v} : \{0,1\}^N \to \{0,1\}^K$ as follows: on input $\overline{x} = (w, a, y^0, y^1, y^2, \ldots, y^t)$,

1. If $a = 0$, let $\hat{h}_{A,v}(\overline{x}) := h_{A,v}(w)$;
2. If $a = 1$, let $\hat{h}_{A,v}(\overline{x}) := 0^K$.

Now fix any $u \in \mathrm{Fav}$, and suppose that $(A, v) \in_r \mathbb{F}_2^{K \times N'} \times \mathbb{F}_2^K$; we will analyze the behavior of the random hash function $\hat{h}_{A,v}$ upon the sets V_u^0, V_u^1.

First, suppose that $u \in \mathrm{Fav} \cap L$. By definition of C_{rec}, there exists a $y \in \{0,1\}^m$ such that $C_{\mathrm{rec}}^{\mathrm{det}}(u, y) = 1$. We verify that by taking $\overline{x} := (w, 1, y, 0^m, \ldots, 0^m)$, we have $\overline{x} \in V_u^1$, and also $\hat{h}_{A,v}(\overline{x}) = 0^K$ with probability 1. Next, define $W_u \subseteq \{0,1\}^{n+4(t-1)}$ by

$$W_u \;:=\; \{w : \; w \text{ appears as the first input block in some } \overline{x} \in V_u^0\} \;.$$

We will upper-bound $|W_u|$. (This set's size, rather than the absolute size of V_u^0, is the relevant quantity for our current hashing experiment.) We have observed previously that any $w \in W_u$ must lie in $A = W_{\mathrm{attr}}$. Consulting our definition of Bad_w from Eq. (56) and items 2-3 from the definition of V_u^0, we see that it must also hold that $j^* \in \mathrm{Bad}_w$.

[15] The only non-uniformity required in the construction of C_{Vtest} are the two integer thresholds needed to verify condition 3 above, which are specifiable with $2\lceil \log_2 t \rceil$ bits.

Recalling that $\mathcal{W}$ denotes the uniform distribution on $\{0,1\}^{n+4(t-1)}$, it follows that

$$\begin{aligned}
|W_u| &\leq 2^{n+4(t-1)} \cdot \Pr_{w \sim \mathcal{W}}[v^{j^*}(w) = u \wedge w \in A \wedge j^* \in \mathrm{Bad}_w] \\
&= 2^{4(t-1)} \cdot \Pr_{w \sim \mathcal{W}}[w \in A \wedge j^* \in \mathrm{Bad}_w | v^{j^*}(w) = u] \\
&= 2^{4(t-1)}(Q[u, j^*] - Q^\circ[u, j^*]) \\
&\leq 2^{4(t-1)}(.02Q[u, j^*]) \\
&\leq 2^{4(t-1)}(.021Q) \ ,
\end{aligned}$$

where in the last three steps we used Eqs. (34), (51) and (58) and the assumption $u \in \mathrm{Fav}$. By our setting to K, we therefore have

$$|W_u| \ \leq \ .021 \cdot 16 \cdot 2^K \ < \ .34 \cdot 2^K \ .$$

By Lemma 2.6, applied with $U' := W_u \subseteq \{0,1\}^{N'}$, we find that

$$\Pr_{A,v}[0^K \in h_{A,v}(W_u)] \ < \ .34 \ .$$

Now if $\hat{h}_{A,v}(\overline{x}) = 0^K$ for some $\overline{x} = (w, a, y^0, \ldots, y^t) \in V_u^0$, we must have $w \in W_u$, $a = 0$, and $h_{A,v}(w) = 0^K$. Thus, we also have

$$\Pr_{A,v}[0^K \in \hat{h}_{A,v}(V_u^0)] \ < \ .34 \ . \tag{59}$$

Next, suppose that $u \in \mathrm{Fav} \cap \overline{L}$. We have already observed that for $u \in \overline{L}$, the set V_u^1 is empty. To analyze the behavior of the random hash function $\hat{h}_{A,v}$ upon V_u^0, we define

$$W_u \ := \ \{w : \ w \text{ appears as the first input block in some } \overline{x} \in V_u^0\}$$

just as in the previous case. This time, however, we will lower-bound $|W_u|$. Consider any $w \in \{0,1\}^{n+4(t-1)}$ for which $[v^{j^*}(w) = u \wedge w \in A]$ holds. Let $J \subseteq [t]$ be the set of indices j for which $C_j(w) = 1$. As $w \in A$, we have $|J| \in [(\rho - \varepsilon/1600)t, (\rho + \varepsilon/1600)t]$, and we have $v^j(w) \in L$ for each $j \in J$ (in particular, this means that $j^* \notin J$). For each $j \in J$, let $y^j \in \{0,1\}^m$ be an assignment for which $C_{\mathrm{rec}}^{\mathrm{det}}(v^j(w), y^j) = 1$; these are guaranteed to exist by the correctness of C_{rec}.

For $j \in [t]$, define $\hat{y}^j := y^j$ if $j \in J$, otherwise $\hat{y}^j := 0^m$. Define $\overline{x} \in \{0,1\}^N$ by

$$\overline{x} \ := \ (w, 0, 0^m, \hat{y}^1, \ldots, \hat{y}^m) \ .$$

It is immediate to check that $\overline{x} \in V_u^0$. Thus $w \in W_u$. We then have

$$\begin{aligned}
|W_u| &\geq 2^{n+4(t-1)} \cdot \Pr_{w \sim \mathcal{W}}[v^{j^*}(w) = u \wedge w \in A] \\
&= 2^{4(t-1)} \cdot \Pr_{w \sim \mathcal{W}}[w \in A | v^{j^*}(w) = u] \\
&= 2^{4(t-1)} Q[u, j^*] \\
&\geq 2^{4(t-1)} \cdot (.98Q) \\
&\geq .98 \cdot 8 \cdot 2^K \ .
\end{aligned}$$

Then by Lemma 2.6, applied with $U' := W_u$, we find that

$$\Pr_{A,v}[0^K \in h_{A,v}(W_u)] \;>\; 1-(7.84)^{-1} \;>\; .87 \ .$$

Similarly to the previous case, it follows that

$$\Pr_{A,v}[0^K \in \hat{h}_{A,v}(V_u^0)] \;>\; .87 \ . \tag{60}$$

Let $T := 300n$. Let us sample T hash functions $(\hat{h}_{A^1,v^1},\ldots,\hat{h}_{A^T,v^T})$ independently, with $(A^i,v^i) \in_r \mathbb{F}_2^{K\times N'} \times \mathbb{F}_2^K$. Say that $\hat{h}_{A^i,v^i}$ is *good for* $u \in \{0,1\}^n$ if

$$0^K \;\in\; \hat{h}_{A^i,v^i}\left(V_u^{\chi_L(u)}\right) \setminus \hat{h}_{A^i,v^i}\left(V_u^{1-\chi_L(u)}\right) \ .$$

Our calculations imply that for every $u \in \mathrm{Fav}$, each individual $\hat{h}_{A^i,v^i}$ is good for u with probability greater than .66, and these events are independent. For any $u \in \{0,1\}^n$, let

$$X^+(u) \;:=\; \sum_{i\in[T]} \mathbf{1}\left[h_{A^i,v^i} \text{ is good for } u\right] \ .$$

Consider any $u \in \mathrm{Fav}$. By using Claim 4.4 and applying Lemma 2.1 to $X^+(u)$, we find that with probability at least $1-\exp(-2(.06)^2\cdot T) > 1-2^{-2n}$,

$$X^+(u) \;\geq\; .6T \ . \tag{61}$$

Then with positive probability, Eq. (61) holds for *every* $u \in \mathrm{Fav}$; so there exists some choice

$$\overline{h} \;=\; (h_1^*,\ldots,h_T^*) \;=\; \left(\hat{h}_{A^1,v^1},\ldots,\hat{h}_{A^T,v^T}\right)$$

such that Eq. (61) holds for every $u \in \mathrm{Fav}$.

Note too that the hash functions $\hat{h}_{A,v}$ are each computable by a circuit of size $O(KN') \leq O(KN)$. We have verified that all of the assumptions of Lemma 2.8 are satisfied, with $f := \chi_{L,n}$; we conclude that there exists a nondeterministic mapping circuit $C^\dagger$ taking n input bits, such that for all $u \in \mathrm{Fav}$, we have $F_{C^\dagger}(u) = \{\chi_L(u)\}$; also, we have

$$\mathrm{size}(C^\dagger) \;\leq\; O((\mathrm{size}(C_{\mathrm{Vtest}})\cdot KNT) \;\leq\; O(\mathrm{poly}(\mathrm{size}(C_{\mathrm{rec}})+\mathrm{size}(C))\cdot KNT) \;\leq\; \mathrm{poly}(\mathrm{size}(C_{\mathrm{rec}})+\mathrm{size}(C)) \ .$$

We take $C_\varepsilon^* := C^\dagger$; as $|\mathrm{Fav}| > (1-\varepsilon)2^n$, this proves Theorem 7.1. □

Acknowledgments

I thank Avi Wigderson for helpful comments, and Robin Moser and Dominik Scheder for discussions of related questions.

References

[AB09] Sanjeev Arora and Boaz Barak. *Computational Complexity: A Modern Approach.* Cambridge University Press, 2009.

[ABG03] Amihood Amir, Richard Beigel, and William I. Gasarch. Some connections between bounded query classes and non-uniform complexity. *Inf. Comput.*, 186(1):104–139, 2003.

[AKS87] Miklós Ajtai, János Komlós, and Endre Szemerédi. Deterministic simulation in LOGSPACE. In *19th ACM STOC*, pages 132–140, 1987.

[Alt94] Ingo Althöfer. On sparse approximations to randomized strategies and convex combinations. *Linear Algebra and its Applications*, 199, Supplement 1(0):339 – 355, 1994.

[BH88] Samuel R. Buss and Louise Hay. On truth-table reducibility to SAT and the difference hierarchy over NP. In *3rd Structure in Complexity Theory Conference*, pages 224–233, 1988.

[BLS84] Ronald V. Book, Timothy J. Long, and Alan L. Selman. Quantitative relativizations of complexity classes. *SIAM J. Comput.*, 13(3):461–487, 1984.

[BLS85] Ronald V. Book, Timothy J. Long, and Alan L. Selman. Qualitative relativizations of complexity classes. *J. Comput. Syst. Sci.*, 30(3):395–413, 1985.

[BT06] Andrej Bogdanov and Luca Trevisan. Average-case complexity. *Foundations and Trends in Theoretical Computer Science*, 2(1), 2006.

[CP07] Richard Chang and Suresh Purini. Bounded queries and the NP machine hypothesis. In *IEEE Conference on Computational Complexity*, pages 52–59, 2007.

[CT06] Thomas M. Cover and Joy A. Thomas. *Elements of Information Theory.* Wiley-Interscience, 2nd edition, 2006.

[Dru11] Andrew Drucker. A PCP characterization of AM. In *ICALP*, pages 581–592, 2011. Full version at http://eccc.hpi-web.de/report/2010/019/.

[Dru12] Andrew Drucker. New limits to classical and quantum instance compression. In *53rd IEEE FOCS*, pages 609–618, 2012. Full version at http://eccc.hpi-web.de/report/2012/112/.

[FHT03] Alexei A. Fedotov, Peter Harremoës, and Flemming Topsøe. Refinements of Pinsker's inequality. *IEEE Transactions on Information Theory*, 49(6):1491–1498, 2003.

[FL97] Uriel Feige and Carsten Lund. On the hardness of computing the permanent of random matrices. *Computational Complexity*, 6(2):101–132, 1997.

[GG81] Ofer Gabber and Zvi Galil. Explicit constructions of linear-sized superconcentrators. *J. Comput. Syst. Sci.*, 22(3):407–420, 1981. Earlier version in FOCS '79.

[GL89] Oded Goldreich and Leonid A. Levin. A hard-core predicate for all one-way functions. In *21st ACM STOC*, pages 25–32, 1989.

[GNW11] Oded Goldreich, Noam Nisan, and Avi Wigderson. On Yao's XOR-lemma. In *Studies in Complexity and Cryptography*, volume 6650 of *Lecture Notes in Computer Science*, pages 273–301. Springer, 2011. Earlier version on ECCC (TR95-050, 1995).

[Gol07] Oded Goldreich. *Foundations of Cryptography: Volume 1, Basic Tools.* Cambridge University Press, 1 edition, 2007.

[GS86] Shafi Goldwasser and Michael Sipser. Private coins versus public coins in interactive proof systems. In *18th ACM STOC*, pages 59–68, 1986.

[Hea08] Alexander Healy. Randomness-efficient sampling within nc^1. *Computational Complexity*, 17(1):3–37, 2008. Earlier version in RANDOM '06.

[HILL99] Johan Håstad, Russell Impagliazzo, Leonid A. Levin, and Michael Luby. A pseudorandom generator from any one-way function. *SIAM J. Comput.*, 28(4):1364–1396, 1999.

[HLW06] Shlomo Hoory, Nathan Linial, and Avi Wigderson. Expander graphs and their applications. *Bull. Amer. Math. Soc.*, 43:439–561, 2006.

[HO02] Lane A. Hemaspaandra and Mitsunori Ogihara. *The Complexity Theory Companion.* Texts in Theoretical Computer Science. Springer, 2002.

[IJKW10] Russell Impagliazzo, Ragesh Jaiswal, Valentine Kabanets, and Avi Wigderson. Uniform direct product theorems: Simplified, optimized, and derandomized. *SIAM J. Comput.*, 39(4):1637–1665, 2010. Earlier version in STOC '08.

[IW97] Russell Impagliazzo and Avi Wigderson. $P = BPP$ if E requires exponential circuits: Derandomizing the XOR lemma. In *29th ACM STOC*, pages 220–229, 1997.

[Lev87] Leonid A. Levin. One-way functions and pseudorandom generators. *Combinatorica*, 7(4):357–363, 1987.

[LY94] Richard J. Lipton and Neal E. Young. Simple strategies for large zero-sum games with applications to complexity theory. In *26th ACM STOC*, pages 734–740, 1994.

[Mar73] G. A. Margulis. Explicit constructions of expanders. *Problemy Peredači Informacii*, 9(4):71–80, 1973.

[MS] Robin Moser and Dominik Scheder. Personal communication.

[NRS99] Noam Nisan, Steven Rudich, and Michael E. Saks. Products and help bits in decision trees. *SIAM J. Comput.*, 28(3):1035–1050, 1999. Earlier version in FOCS '94.

[NW94] Noam Nisan and Avi Wigderson. Hardness vs randomness. *J. Comput. Syst. Sci.*, 49(2):149–167, 1994. Earlier version in FOCS '88.

[O'D02] Ryan O'Donnell. Hardness amplification within NP. In *34th ACM STOC*, pages 751–760, 2002.

[Pap94] Christos H. Papadimitriou. *Computational Complexity.* Addison-Wesley, 1994.

[PP10] Ramamohan Paturi and Pavel Pudlák. On the complexity of circuit satisfiability. In Leonard J. Schulman, editor, *STOC*, pages 241–250. ACM, 2010.

[Raz98] Ran Raz. A parallel repetition theorem. *SIAM J. Comput.*, 27(3):763–803, 1998. Earlier version in STOC '95.

[RW09] Mark D. Reid and Robert C. Williamson. Generalised Pinsker inequalities. In *COLT*, 2009.

[Sha03] Ronen Shaltiel. Towards proving strong direct product theorems. *Computational Complexity*, 12(1-2):1–22, 2003. Earlier version in CCC '01.

[SV10] Ronen Shaltiel and Emanuele Viola. Hardness amplification proofs require majority. *SIAM J. Comput.*, 39(7):3122–3154, 2010.

[Tod91] Seinosuke Toda. PP is as hard as the polynomial-time hierarchy. *SIAM J. Comput.*, 20(5):865–877, 1991.

[TV00] Luca Trevisan and Salil P. Vadhan. Extracting randomness from samplable distributions. In *41st IEEE FOCS*, pages 32–42, 2000.

[VV86] Leslie G. Valiant and Vijay V. Vazirani. NP is as easy as detecting unique solutions. *Theor. Comput. Sci.*, 47(3):85–93, 1986. Earlier version in STOC '85.

[VW08] Emanuele Viola and Avi Wigderson. Norms, XOR lemmas, and lower bounds for polynomials and protocols. *Theory of Computing*, 4(1):137–168, 2008. Earlier version in CCC '07.

[Wig97] Avi Wigderson. Derandomizing BPP, 1997. Lecture notes prepared by Ronen Shaltiel. http://www.math.ias.edu/∼avi/BOOKS/rand.pdf.

[WX05] Avi Wigderson and David Xiao. A randomness-efficient sampler for matrix-valued functions and applications. In *46th IEEE FOCS*, pages 397–406, 2005. See corrections in [WX08].

[WX08] Avi Wigderson and David Xiao. Derandomizing the Ahlswede-Winter matrix-valued Chernoff bound using pessimistic estimators, and applications. *Theory of Computing*, 4(1):53–76, 2008.

[Yao77] Andrew Chi-Chih Yao. Probabilistic computations: Toward a unified measure of complexity (extended abstract). In *18th IEEE FOCS*, pages 222–227, 1977.

[Yao82] Andrew Chi-Chih Yao. Theory and applications of trapdoor functions (extended abstract). In *FOCS*, pages 80–91. IEEE Computer Society, 1982.

[Yap83] Chee-Keng Yap. Some consequences of non-uniform conditions on uniform classes. *Theor. Comput. Sci.*, 26:287–300, 1983.