Electronic Colloquium on Computational Complexity, Report No. 87 (2025)

# Hardness Amplification for Real-Valued Functions

Yunqi Li[*] Prashant Nalini Vasudevan[†]

**Abstract**

Given an integer-valued function $f : \{0,1\}^n \to \{0,1,\ldots,m-1\}$ that is mildly hard to compute on instances drawn from some distribution $D$ over $\{0,1\}^n$, we show that the function $g(x_1,\ldots,x_t) = f(x_1) + \cdots + f(x_t)$ is strongly hard to compute on instances $(x_1,\ldots,x_t)$ drawn from the product distribution $D^t$. We also show the same for the task of approximately computing real-valued functions $f : \{0,1\}^n \to [0,m)$. Our theorems immediately imply hardness self-amplification for several natural problems including Max-Clique and Max-SAT, Approximate #SAT, Entropy Estimation, etc..

## Contents

[*] Department of Computer Science, National University of Singapore. Email: yunqili@comp.nus.edu.sg

[†] Department of Computer Science, National University of Singapore. Email: prashant@comp.nus.edu.sg

ISSN 1433-8092

# 1 Introduction

Hardness amplification is the process of taking a computational problem $\Pi$ and a distribution $D$ of instances over which $\Pi$ is mildly hard, and constructing a problem $\Pi'$ and distribution $D'$ over which $\Pi'$ is much harder. There has been extensive work in the past studying hardness amplification for various computational tasks such as computing Boolean functions [Yao82, Imp95, GNW11, KS03, Kal07], inverting efficient functions [Yao82, GIL+90], distinguishing between distributions [Gei22], deciding languages contained in complexity classes like $\mathsf{NP}$ [O'D04, HVV06, Tre05, GG11, BT06], $\mathsf{EXP}$ [TV07], $\#\mathsf{P}$ [Lip89, CPS99], or $\mathsf{P}$ [BRSV17, GR18, BBB19], solving optimization problems [GK20], for specific interesting or structured problems [AGGS22, HS23, ASS+24], etc..

In this paper, we study hardness amplification for the task of evaluating integer- or real-valued functions. We first describe our setting and results, and then demonstrate various corollaries of our theorems that motivate studying such problems.

**Evaluating Functions.** In our first result, we consider functions $f : \{0,1\}^n \to \mathbb{Z}_m$, where $\mathbb{Z}_m$ denotes the set of integers $\{0, 1, \ldots, m-1\}$[1], and the computational task is to compute $f(x)$ given an input $x \in \{0,1\}^n$. Suppose we are given such an $f$ and a distribution $D$ on $\{0,1\}^n$ over which computing $f$ is $(1-\delta)$-hard – meaning that no small circuit can correctly compute $f(x)$ with probability greater than $(1-\delta)$ when $x$ is drawn from $D$. Our objective is to construct a function $g$ and distribution $D'$ such that computing $g$ is $\eta$-hard over $D'$ for some small $\eta$. Further, we would like $g$ to have the same type as $f$ – to take bit-strings as input and produce integers from a bounded range as output.

For Boolean functions, Yao's XOR Lemma [Yao82] shows that such amplification can be achieved by having $g$ be the XOR of multiple instances of $f$; and similar results are also known if $g$ is the Recursive Majority-of-3 of such instances [O'D04]. We show that in this case of integer-valued functions, having $g$ be the sum (over integers) of multiple instances of $f$ achieves the same. For $t \in \mathbb{N}$, denote by $(\mathsf{SUM}_t \otimes f)$ the function that takes $t$ inputs $x_1, \ldots, x_t \in \{0,1\}^n$, and outputs the sum $\sum_i f(x_i)$.

**Theorem 1.1** (Simplification of Theorem 4.1)**.** *Suppose a function $f : \{0,1\}^n \to \mathbb{Z}_m$ is $(1-\delta)$-hard to compute over a distribution $D$ for circuits of size $s$. Then, for $t \in \mathbb{N}$, the function $(\mathsf{SUM}_t \otimes f)$ is $\left(\frac{2m}{\sqrt{t\delta}}\right)$-hard to compute over the product distribution $D^t$ for circuits of size $\left(\frac{c'm^2}{t^2\delta^2\log(t)}\right) \cdot s$, as long as $t > \frac{cm^2}{\delta}$, where $c$ and $c'$ are some universal constants.*

In a typical application of this theorem (see Section 1.1 for examples), one might take $\delta$ to be a small constant, $m$ to be some polynomially large value in $n$, assume $(1-\delta)$-hardness for $s$ being any arbitrary polynomial in $n$, and set $t$ to be $\omega(m^2)$ but still some polynomial in $n$. The theorem would then imply that $(\mathsf{SUM}_t \otimes f)$ is $1/\mathsf{poly}(n)$-hard for all polynomial-sized circuits.

To place the $O(m/\sqrt{t\delta})$-hardness we obtain in context, observe that it is not possible to show that summation generically amplifies such a function to hardness less than $\Theta(1/\sqrt{t\delta})$. Consider, for example, a hypothetical function that takes values in $\{0,1\}$, is easy to compute on $(1-2\delta)$ fraction of inputs, and on the remaining $2\delta$ is optimally hard (so it is not possible to do better than random guessing). This function is $(1-\delta)$-hard. Given $t$ random inputs from the hard distribution, the hardness comes only from about $\delta t$ of the inputs. And simply guessing randomly on each of these will yield the correct value for the sum of their outputs with probability $\Omega(1/\sqrt{t\delta})$.

[1] We only use $\mathbb{Z}_m$ to denote set without involving any modulo operations.

**Approximating Functions.** In our second result, we extend the above hardness amplification to the task of approximately evaluating bounded real-valued functions. Here we consider functions $f : \{0,1\}^n \to [0,m)$, and the task is, for some approximation parameter $\epsilon \in \mathbb{R}^+$, to compute some value in the range $(f(x)-\epsilon, f(x)+\epsilon)$ given input $x$. We show that summation again amplifies hardness, though with slightly different dependence on the various parameters, and also now depending on the $\epsilon$.

**Theorem 1.2** (Simplification of Theorem 5.1)**.** *Suppose a function $f : \{0,1\}^n \to [0,m)$ is $(1-\delta)$-hard to $\epsilon$-approximate over a distribution $D$ for circuits of size $s$. Then, the function $(\mathsf{SUM}_t \otimes f)$ is $10 \cdot \left(\frac{m}{\epsilon\sqrt{t\delta}}\right)^{1/2}$-hard to $\epsilon$-approximate over the product distribution $D^t$ for circuits of size $\left(\frac{c'm}{\epsilon(t\delta)^{3/2}\log(t)}\right) \cdot s$, as long as $t > \frac{cm^2}{\epsilon^2\delta}$, where $c$ and $c'$ are some universal constants.*

Here too, in the applications we show, parameters are set as described for Theorem 1.1 earlier, with $\epsilon = \Theta(1)$.

**Paper Outline.** In the rest of this section, we describe various corollaries of the above theorems (Section 1.1) and provide an overview of the proofs of these theorems (Section 1.2). In Section 2, we set up the definitions and conventions needed in the rest of the paper. In Section 3, we prove a hardcore lemma for relations that is central to our proofs. In Sections 4 and 5, we state and prove more comprehensive versions of Theorems 1.1 and 1.2, respectively. In Appendix A, we present the statements of our corollaries in more detail and present sketches of their proofs.

## 1.1 Corollaries

Functions mapping bit-strings to integers or real numbers, even within limited ranges, are quite general and capture a variety of natural problems whose complexity is of significant interest – essentially any problem $\Pi$ whose solution $\Pi(x)$ for an instance $x$ is a bounded integer or real number. For such problems, our results roughly say that computing the sum of solutions to $t$ instances is a much harder problem. Such a statement is not particularly meaningful in general, but things become much more interesting if the problem $\Pi$ also happens to admit an *additively homomorphic self-reduction.*

That is, suppose there is an efficient algorithm $R$ such that for any inputs $x_1, \ldots, x_t$, we have $\Pi(R(x_1, \ldots, x_t)) = \sum_i \Pi(x_i)$. In this case, the problem of computing the sum of solutions of $t$ instances can be reduced back to the solving the problem $\Pi$ itself on a single instance. Then, our results can be used to show that mild hardness of $\Pi$ implies strong hardness of $\Pi$ itself, possibly on a different distribution over instances (in what is sometimes referred to as hardness self-amplification). And this requirement is weak enough that many natural and important problems have such self-reductions. Below, we show three examples, each of which is qualitatively distinct from the others.

**Optimization Problems.** Various natural optimization problems can be cast in terms of computing a polynomially bounded integer-valued function of the input, and further be shown to possess simple additively homomorphic self-reductions. For example, consider the Max-Clique problem where, given (the adjacency matrix of) a graph $G$, the task is to compute the size of its largest clique. Given graphs $G_1, \ldots, G_t$, we can create a new graph consisting of one copy of each $G_i$, with edges between every pair of vertices that are not from the same graph. The size of the maximum clique in this composite graph is simply the sum of the maximums in all the $G_i$'s.

Another example is the $\mathsf{MaxSAT}$ problem, where given a CNF formula $\phi$, the task is to find the maximum number of clauses satisfied by any assignment to its variables. Given $t$ formulas $\phi_1, \ldots, \phi_t$

on disjoint sets of variables, the maximum number of clauses of the formula $(\phi_1 \wedge \cdots \wedge \phi_t)$ that can be satisfied is simply the sum of the maximums of all the $\phi_i$'s. Note that both of these problems also happen to be $\mathsf{NP}$-hard. We get the following from Theorem 1.1, following the arguments above.

**Corollary 1.3.** *The following holds for any problem* $\Pi \in \{\mathsf{MaxSAT}, \mathsf{MaxClique}\}$. *If there is a family of distributions on which* $\Pi$ *is* $0.9$*-hard, then there is a family of distributions on which* $\Pi$ *is* $O(n^{-0.49})$*-hard (where* $n$ *is the instance size). Further, if the former family is efficiently sampleable, then so is the latter.*

In these corollaries, we consider the asymptotic hardness of these problems rather than for a fixed input size, which is why we need to consider a family of distributions – one distribution for each value of the instance size parameter $n$ – rather than a single distribution. And by efficiently sampleable, we mean sampleable by a polynomial-sized family of circuits. Similarly, when we just say $\eta$-hard, we mean $\eta$-hard for families of circuits of size any polynomial in the instance size parameter $n$. More detailed and careful statements of all the corollaries are presented in Appendix A, along with sketches of their proofs. These are all asymptotic statements, and so involve applying our theorems (which are stated for arbitrary input lengths and circuit sizes) for all members of families of functions and circuits.

Hardness amplification for optimization problems, including the above examples, was studied in [GK20]. However, they considered the task of actually finding the maximum clique, the maximally satisfying assignment, etc., and their results are incomparable to the corollary above.

**Entropy Estimation.** A natural problem (that has incidentally been of some significance in cryptography [Vad99]) is that of estimating the Shannon entropy of a distribution given its sampling algorithm (say, as a circuit). Given a distribution over $\{0,1\}^m$, its entropy is some real number in the range $[0, m]$, and Shannon entropy is also conveniently additive: for any random variables $X$ and $Y$, we have $H(X,Y) = H(X) + H(Y)$. We cannot use Theorem 1.1 here because the entropy is not integer-valued, but we can use Theorem 1.2 to show hardness amplification for the task of approximately computing the entropy of a given distribution.

In this case, we can in fact go further. A related decision problem, called the Entropy Difference problem, is known to be complete for the complexity class $\mathsf{SZK}$, which consists of problems that possess statistical zero-knowledge proofs [SV03]. In this problem, given sampling algorithms for two distributions $D_0$ and $D_1$, and promised that their entropies are separated by a gap of at least 1, the task is to tell which distribution has larger entropy. If this problem is even mildly average-case hard over some distribution of instances $(D_0, D_1)$, then the task of computing the entropy of distributions to within $\pm 1/2$ is mildly average-case hard for the distribution given by sampling $(D_0, D_1)$ as above and randomly outputting one of the two distributions. These observations, together with Theorem 1.2, give us the following.

**Corollary 1.4.** *If there is a problem in* $\mathsf{SZK}$ *that is* $0.9$*-hard over some family of distributions, then there exists a family of distributions on which* $O(1)$*-approximating Shannon entropy is* $O(n^{-0.24})$*-hard. Further, if the former family of distributions is efficiently sampleable, then so is the latter.*

**Approximate Counting.** Given as input the description of a Non-deterministic Turing Machine $M$ and an input $x$ for it, define $f(M,x)$ to be the number of accepting paths in the execution of $M$ given input $x$. This function captures the defining problem of the complexity class $\#\mathsf{P}$. The same can be done with the $\#\mathsf{P}$-complete problem $\#\mathsf{SAT}$, which is the problem of counting the number of satisfying assignments to a given Boolean formula.

In both these cases, however, the function can take exponentially many values in the instance size, and so trying to apply our theorems would not give meaningful bounds. However, if we instead consider the function $g(M, x) = \log_2(f(M, x))$, this function is real-valued and lies in a polynomially bounded range (as long as the formula is guaranteed to be satisfiable). Further, additive $\pm\varepsilon$ approximations to $g$ are equivalent to multiplicative $2^{\pm\epsilon}$ approximations to $f$. Theorem 1.2 now implies the following.

**Corollary 1.5.** *Suppose there is a family of distributions over satisfiable Boolean formulas on which multiplicatively approximating the number of satisfying assignments to within a factor of* $2$ *is* $0.9$*-hard. Then there is a family of distributions on which the same task is* $O(n^{-0.24})$*-hard (where* $n$ *is the instance size). Further, if the former is efficiently sampleable, then so is the latter.*

## 1.2 Technical Overview

In this section, we give an overview of our analysis of the hardness amplification of summation. We start by looking at hardness amplification of evaluating integer-valued functions (Theorem 1.1), and then describe how to extend this to approximately evaluating real-valued functions (Theorem 1.2).

**Hardness of $\{0,1\}$-valued functions.** We will start by showing something even simpler – hardness amplification for functions that only take two different values. Our techniques here are inspired by ideas in the proof of existing hardness amplification theorems for problems in $\mathsf{NP}$ [O'D04].

Suppose that there is a function $f : \{0,1\}^n \to \{0,1\}$, and a corresponding distribution $H$ over $\{0,1\}^n$, on which the function $f$ is strongly average-case hard; that is, there is some small $\gamma = 1/\mathsf{poly}(n)$ such that for any circuit $C$ of size at most $s$,

$$\Pr_{x \leftarrow H}[C(x) = f(x)] < \frac{1}{2}(1+\gamma),$$

For simplicity, we assume that $f$ is balanced over $H$. That is,

$$\Pr_{x \leftarrow H}[f(x) = 0] = \Pr_{x \leftarrow H}[f(x) = 1]$$

For some $t \in \mathbb{N}$, consider the function $g : \{0,1\}^{tn} \to \mathbb{Z}_{t+1}$, where $g(x_1, \ldots, x_t) = f(x_1) + \cdots + f(x_t)$. In the following, we will show that the average-case hardness of $g$ improves polynomially in $t$. Particularly, for any circuits of size at most approximately $s$, we have:

$$\Pr_{x \leftarrow H^t}[C(x) = g(x)] < \frac{\binom{t}{\frac{t}{2}}}{2^t}\left(1 + \frac{t}{2} \cdot \gamma\right) \tag{1}$$

Before we show this, let us understand the best hardness we can hope to show. A simple algorithm for computing $g$ is to just always output the value that $g$ is most likely to take. Since $f$ is assumed to be balanced over $H$, this value would be $\frac{t}{2}$.

$$\Pr_{x \leftarrow H^t}\left[g(x) = \frac{t}{2}\right] = \frac{\binom{t}{\frac{t}{2}}}{2^t} \approx \Theta\left(\frac{1}{\sqrt{t}}\right).$$

If the function $f$ had been optimally $(1/2)$-hard, then this would also be the best possible algorithm for $g$. What we have is that $f$ is $(1+\gamma)/2$-hard for some small $\gamma$, indicating that $f$ is still almost optimally hard. We essentially show that in this case the above algorithm is still nearly the best possible algorithm $g$.

We start by observing that the hardness of $f$ implies the indistinguishability of the distributions $H$ conditioned on different outputs – $H|_{f(x)=0}$ and $H|_{f(x)=1}$. That is, for any circuit $C$ of size at most $s$,

$$\left| \Pr_{x \leftarrow H}[C(x) = 1 | f(x) = 1] - \Pr_{x \leftarrow H}[C(x) = 1 | f(x) = 0] \right| < \gamma. \tag{2}$$

To see why, suppose that this is not the case. Without loss of generality, there exists a circuit $C$ satisfying

$$\Pr_{x \leftarrow H}[C(x) = 1 | f(x) = 1] - \Pr_{x \leftarrow H}[C(x) = 1 | f(x) = 0] \geq \gamma.$$

Then,

$$\begin{aligned}
\Pr_{x \leftarrow H}[C(x) = f(x)] =& \frac{1}{2} \Pr[C(x) = f(x) | f(x) = 1] + \frac{1}{2} \Pr[C(x) = f(x) | f(x) = 0] \\
=& \frac{1}{2} \Pr[C(x) = 1 | f(x) = 1] + \frac{1}{2} \left(1 - \Pr[C(x) = 1 | f(x) = 0]\right) \\
\geq& \frac{1}{2}(1 + \gamma)
\end{aligned}$$

which leads to a contradiction.

For function $g$, consider the performance of any circuit $\hat{C}$ for computing $g$. We claim that, for any $k \in \mathbb{Z}_t$ and any $v$ in the output range of $\hat{C}$, the following holds:

$$\left| \Pr_{x \leftarrow H^t}[\hat{C}(x) = v | g(x) = k + 1] - \Pr_{x \leftarrow H^t}[\hat{C}(x) = v | g(x) = k] \right| < \gamma. \tag{3}$$

To prove it, assume

$$\left| \Pr_{x \leftarrow H^t}[\hat{C}(x) = v | g(x) = k + 1] - \Pr_{x \leftarrow H^t}[\hat{C}(x) = v | g(x) = k] \right| \geq \gamma. \tag{4}$$

The distribution $x \leftarrow H^t|_{g(x)=k}$ is equivalent to the distribution sampled as follows:

- Independently sample $x_1, \ldots, x_k \leftarrow H|_{f(x)=1}$, and $x_{k+1}, \ldots, x_t \leftarrow H|_{f(x)=0}$ independently
- Sample a uniformly random permutation $\pi$ from all possible permutations over $t$ coordinates
- Output $\pi(x_1, \ldots, x_t)$

Using this observation and the linearity of expectation, (4) implies that there must exist a fixed $(x_1, \ldots, x_k, x_{k+2}, \ldots, x_t)$ and a permutation $\pi$, such that

$$\left| \Pr_{\substack{x \leftarrow H \\ \hat{x} \leftarrow \pi(x_1, \ldots, x_k, x, x_{k+2}, \ldots)}} \left[\hat{C}(\hat{x}) = v | f(x) = 1\right] - \Pr_{\substack{x \leftarrow H \\ \hat{x} \leftarrow \pi(x_1, \ldots, x_k, x, x_{k+2}, \ldots)}} \left[\hat{C}(\hat{x}) = v | f(x) = 0\right] \right| \geq \gamma.$$

Then, a circuit $C : \{0,1\}^n \to \{0,1\}$ can be constructed by taking $x_1, \ldots, x_k, x_{k+2}, \ldots, x_t$ and permutation $\pi$ as non-uniform advice and working as follows: on the input $x \in \{0,1\}^n$, outputs 1 iff $\hat{C}(\pi(x_1, \ldots, x, \ldots, x_t))$ outputs $v$. The size of $C$ is approximately the size of $\hat{C}$, and we have

$$\left| \Pr_{x \leftarrow H}[C(x) = 1 | f(x) = 1] - \Pr_{x \leftarrow H}[C(x) = 1 | f(x) = 0] \right| \geq \gamma,$$

which contradicts the hardness of $f$ as captured by (2).

Based on (3) and a simple telescoping argument, we further obtain, for any $i, j \in \mathbb{Z}_{t+1}$ and any $v$ in the output range of $\hat{C}$,

$$\left| \Pr_{x \leftarrow H^t}[\hat{C}(x) = v | g(x) = i] - \Pr_{x \leftarrow H^t}[\hat{C}(x) = v | g(x) = j] \right| < |i - j| \cdot \gamma. \tag{5}$$

We can now bound the probability that a circuit $\hat{C}$ can correctly compute the function $g$ as:

$$\begin{aligned}
\Pr_{x \leftarrow H^t}[\hat{C}(x) = g(x)] &= \sum_{k=0}^{t} \Pr_{x \leftarrow H^t}[g(x) = k] \Pr_{x \leftarrow H^t}[\hat{C}(x) = k | g(x) = k] \\
&= \sum_{k=0}^{t} \frac{\binom{t}{k}}{2^t} \cdot \Pr_{x \leftarrow H^t}[\hat{C}(x) = k | g(x) = k] \\
&< \sum_{k=0}^{t} \frac{\binom{t}{k}}{2^t} \left( \Pr_{x \leftarrow H^t}\left[\hat{C}(x) = k \,\middle|\, g(x) = \frac{t}{2}\right] + \left|k - \frac{t}{2}\right| \cdot \gamma \right) \\
&\le \frac{\binom{t}{\frac{t}{2}}}{2^t} \cdot \sum_{k=0}^{t} \Pr_{x \leftarrow H^t}\left[\hat{C}(x) = k \,\middle|\, g(x) = \frac{t}{2}\right] + \sum_{k=0}^{t} \frac{\binom{t}{k}}{2^t} \left|k - \frac{t}{2}\right| \cdot \gamma \\
&= \frac{\binom{t}{\frac{t}{2}}}{2^t} \cdot \sum_{k=0}^{t} \Pr_{x \leftarrow H^t}\left[\hat{C}(x) = k \,\middle|\, g(x) = \frac{t}{2}\right] + \frac{1}{2^t} \cdot \frac{t}{2} \cdot \binom{t}{\frac{t}{2}} \cdot \gamma \\
&\le \frac{\binom{t}{\frac{t}{2}}}{2^t} \left(1 + \frac{t}{2} \cdot \gamma\right).
\end{aligned}$$

where the second line follows from the fact that $f$ is balanced over $H$, the third line follows from (5), the fourth line from the maximality of the central binomial co-efficient, the fifth line from computing the sum of the series there, and the last line from the fact that the events in the probability expressions are disjoint.

The above approach to bounding the probability of computing the sum of $t$ independent instances of a function whose value between two possible outputs is strongly hard to decide is at the core of the proofs of our results.

**Reducing to two outputs.** Since our amplification approach is based on the strong indistinguishability of distributions over the pre-image sets of two outputs, for any evaluation problem, we will identify such a pair of indistinguishable pre-image sets based on assumption that the evaluation problem is hard. For simplicity, we will take the distribution over which the problem is hard to be the uniform distribution over $\{0,1\}^n$.

Consider a function $f : \{0,1\}^n \to \mathbb{Z}_m$ that is $(1 - \delta)$-hard for circuits of size $s$. For every $a, b \in \mathbb{Z}_m$, $a \neq b$, we define a computation problem in which we only consider the correctness on inputs whose output belongs to $\{a, b\}$. We formalize the above problem by defining the relations $R_{a,b}$ over $\{0,1\}^n \times \mathbb{Z}_m$:

- If $f(x) \in \{a, b\}$, then $(x, y) \in R_{a,b}$ if and only if $y = f(x)$;
- If $f(x) \notin \{a, b\}$, then $(x, y) \in R_{a,b}$ for every $y \in \mathbb{Z}_m$.

For any $x \in \{0,1\}^n$, denote by $R_{a,b}(x)$ the set of $y \in \mathbb{Z}_m$ such that $(x, y) \in R_{a,b}$. We show that the hardness of $f$ implies that there must exist some $a \neq b \in \mathbb{Z}_m$ and some distribution over their pre-image sets for which it is hard to distinguish whether $f(x)$ is $a$ or $b$. More precisely, we show that there exists a pair $(a, b)$ such that $R_{a,b}$ is $\left(1 - \delta/\binom{m}{2}\right)$-hard for circuits of size $\frac{s}{m^2}$.

To prove this by contradiction, suppose for every $a \neq b \in \mathbb{Z}_m$, there exists a circuit $C_{a,b}$ that satisfies,

$$\Pr_{x \leftarrow \{0,1\}^n}[C_{a,b}(x) \in R_{a,b}(x)] \geq 1 - \frac{\delta}{\binom{m}{2}}.$$

For simplicity, let $C_{b,a} = C_{a,b}$. Then, by combining the $C_{a,b}$'s, we can construct a circuit $C$ as follows:

- Input: $x \in \{0,1\}^n$
- For $i \in \{0, \ldots, m-1\}$
    - If $C_{i,j}(x) = i$ for every $j \neq i$, output $i$
- Output $\perp$

The size of $C$ is approximately $\binom{m}{2} \cdot \frac{s}{m^2} < s$. It is clear that on the input $x$, if every $C_{a,b}$ outputs a value in $R_{a,b}(x)$, then $C(x) = f(x)$. Then, the probability that $C$ agree with $f$ is

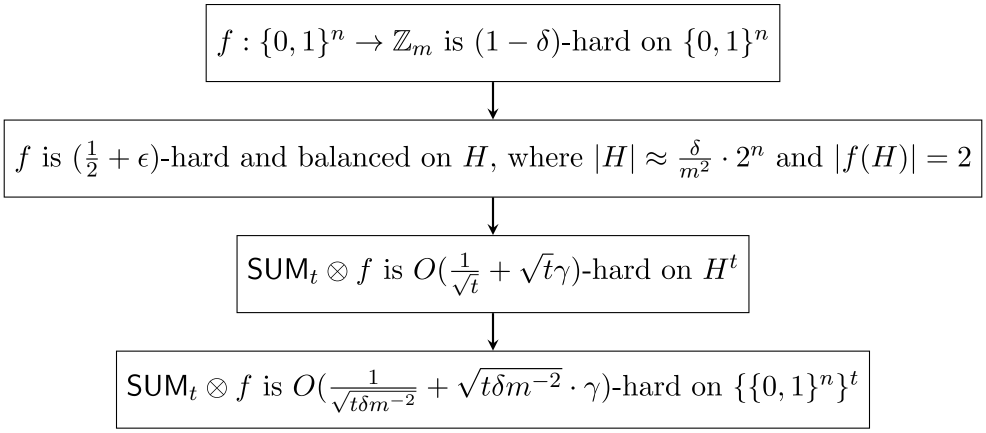
$$\begin{aligned}
\Pr_{x \leftarrow \{0,1\}^n}[C(x) = f(x)] &\geq \Pr_{x \leftarrow \{0,1\}^n}[\forall (a,b), a < b : C_{a,b}(x) \in R_{a,b}(x)] \\
&\geq 1 - \sum_{(a,b), a<b} \Pr_{x \leftarrow \{0,1\}^n}[C_{a,b}(x) \notin R_{a,b}(x)] \\
&\geq 1 - \delta,
\end{aligned}$$

which results in a contradiction. Therefore, there must exist such an $R_{a,b}$ that is $(1 - \delta/\binom{m}{2})$-hard for circuits of size $s/m^2$.

**Amplifying using hardcore sets.** Pick a relation $R_{a,b}$ that has such hardness. As its hardness essentially comes from the hardness of deciding between two possible outputs $a$ and $b$, we can extend existing proofs of the hardcore lemma for Boolean functions (e.g. that of [Imp95]) to obtain a hardcore set[2] for $R_{a,b}$. This is a set $H \subseteq \{0,1\}^n$ of density at least $\delta' = \delta/\binom{m}{2}$ such that the relation $R_{a,b}$ is $(1+\gamma)/2$-hard over random inputs from $H$ for circuits of size roughly $\gamma^2 s/m^2$. Further, we can ensure that all inputs $x \in H$ are such that $f(x) \in \{a, b\}$, and with only a small loss, we can also ensure that this set is balanced between the outputs $a$ and $b$.

The rest of the argument is quite standard. Given $t$ inputs $x_1, \ldots, x_t$ sampled uniformly at random from $\{0,1\}^n$, with high probability roughly at least a $\delta'$ fraction of these will fall in $H$. Looking at just these $\delta' t$ inputs, we are essentially back in the case discussed at the beginning of this overview – that of a function that has two possible outputs, with inputs being sampled from a hard distribution balanced between these outputs. Applying the amplification arguments there to this subset of inputs, we get from (1) that computing the sum of the $f(x_i)$'s for the $x_i$'s that fall in $H$ is roughly $(1/\sqrt{\delta' t} + \sqrt{\delta' t}\gamma)$-hard for circuits of size roughly $\gamma^2 s/m^2$. In order to compute the sum of all the $f(x_i)$'s, the sum corresponding to the above $\delta' t$ inputs needs to be computed. So this hardness carries over to computing $\mathsf{SUM}_t \otimes f$ as well. Setting $\gamma = 1/\delta' t$ now gives us Theorem 1.1. The entire process is as depicted below.

[2] Actually, what we obtain are hardcore distributions, but we assume these are sets in this overview for simplicity.



$f : \{0,1\}^n \to \mathbb{Z}_m$ is $(1-\delta)$-hard on $\{0,1\}^n$

$f$ is $(\frac{1}{2}+\epsilon)$-hard and balanced on $H$, where $|H| \approx \frac{\delta}{m^2} \cdot 2^n$ and $|f(H)| = 2$

$\mathsf{SUM}_t \otimes f$ is $O(\frac{1}{\sqrt{t}} + \sqrt{t}\gamma)$-hard on $H^t$

$\mathsf{SUM}_t \otimes f$ is $O(\frac{1}{\sqrt{t\delta m^{-2}}} + \sqrt{t\delta m^{-2}} \cdot \gamma)$-hard on $\{\{0,1\}^n\}^t$

**Approximating Real-valued Functions.** Our main theorem (Theorem 1.2) is that summation amplifies not just the hardness of computing functions exactly, but also the hardness of additively approximating real-valued functions with bounded range. Our proof of this follows the same high-level structure as that of the above theorem about exactly computing integer-valued functions:

1. Using the mild hardness of $\epsilon$-approximating a function $f : \{0,1\}^n \to [0,m)$, obtain the mild hardness of an approximate "two-output" relation $R_{a,b}$, which corresponds to $\epsilon$-approximating $f(x)$ under the promise that $f(x)$ is close to either $a$ or $b$
2. Show that this mild hardness implies that there is a hardcore set of inputs of noticeable size on which computing $R_{a,b}$ is strongly hard
3. Show that when multiple samples $x_i$ are drawn from this hardcore set, the hardness of $\epsilon$-approximating the sum of the $f(x_i)$'s amplifies as expected, using the fact that these $f(x_i)$'s are all close to either $a$ or $b$
4. Observe that since this hardcore set is of noticeable size, given many uniformly random inputs $x_i$, a noticeable fraction of them are from this hardcore set, and so the above amplified hardness carries over

Before we do any of this, we pick a $d \ll \epsilon$ and partition the space $[0,m)$ into $(m/2d)$ intervals of "radius" $d$, centered at $d$, $3d$, etc.. Earlier, we defined the relations $R_{a,b}$ by looking at every pair of values the output $f(x)$ could take, and essentially ignoring inputs whose outputs were not in $\{a,b\}$. Here we do the same, except with these intervals. For every pair of centers $a$ and $b$ of such intervals, we then define the relation $R_{a,b}$ over $\{0,1\}^n \times [0,m)$ as follows:

- If $f(x) \in [a \pm d)$ or $f(x) \in [b \pm d)$, then $y \in R_{a,b}(x)$ if and only if $|f(x) - y| < \epsilon$.
- Else, $y \in R_{a,b}(x)$ for any $y$.

Suppose $f$ is $(1-\delta)$-hard for circuits of size $s$. Using arguments analogous to those in the integer case, we show that there must exist some pair of intervals such that distinguishing between their pre-images is also mildly hard. That is, there exist centers $a, b \in [0,m)$ such that, for any circuit $C$ of size $\frac{d^2 s}{m^2}$, we have:

$$\Pr_{x \leftarrow \{0,1\}^n}[C(x) \in R_{a,b}(x)] < 1 - \frac{\delta}{\binom{\lceil \frac{m}{2d} \rceil}{2}},$$

This completes the first step mentioned above. The second step is to prove a hardcore lemma for such relations. To do so, we observe that a crucial element that is essentially sufficient for hardcore lemmas is what we call a *majority combiner*. This is a function $M$ that is computable by a small circuit, and has the property that the output of $M(y_1, \dots, y_t)$ is contained in $R_{a,b}(x)$ whenever a majority of the $y_i$'s are contained in $R_{a,b}(x)$. For the $R_{a,b}$'s as defined defined in the integer case, the majority function itself had this property. In the present case, it is not hard to see that the median function has this property. This observation lets us extend the hardcore lemma to these relations.

The fourth step above, being quite generic, is unchanged and follows easily, but the third step turns out to be quite hairy and require careful arguments that take into account the relative sizes of $\epsilon$ and $d$, the gap between $a$ and $b$, etc.. The high-level idea is still the same as the corresponding part of the proof in the integer case. The core there, as captured by (3), was to show that for any circuit $C$ (of a certain size) that takes $t$ inputs $x_1, \dots, x_t$ sampled from the hardcore set, if the number of $x_i$'s with $f(x_i) = a$ is changed by 1, the probability mass placed by $C$ on any given output changes by very little. We show the same here, except that instead of showing this for the probability masses of specific outputs, we need to argue about the masses of intervals of various sizes. This turns out to be the part of the proof that requires the most care, but ultimately works out with some similar parameters. We refer the reader to Section 5 for the details.

# 2 Definitions

## 2.1 Notations

For $m \in \mathbb{N}$, denote the set $\{0, \dots, m-1\}$ by $\mathbb{Z}_m$ (note that this is just a set, not the ring of integers modulo $m$). For $v, \epsilon \in \mathbb{R}$, we use $[v \pm \epsilon)$ to denote the interval $[v - \epsilon, v + \epsilon)$ and use round brackets for open intervals and square brackets for closed intervals.

For distributions $H, G$ over the same domain $\{0,1\}^n$, for any integers $0 \leq k \leq t$, the symbol $\Pi_t(H^k, G^{t-k})$ stands for the following distribution: sample $x_1, \dots, x_k$ from $H$ independently and sample $x_{k+1}, \dots, x_t$ from $G$ independently, sample a permutation $\pi$ over $t$ entries uniformly randomly, and output $\pi(x_1, \dots, x_t)$.

**Functions and relations.** For $n, t \in \mathbb{N}$ and some alphabet $\Sigma, \Sigma'$, given functions $f : \{0,1\}^n \to \Sigma$ and $g : \Sigma^t \to \Sigma'$, denote the function that outputs $g(f(x_1), \dots, f(x_t))$ over input $(x_1, \dots, x_t)$ by $g \otimes f$. For a relation $R \subseteq \mathcal{X} \times \mathcal{Y}$, for any $x \in \mathcal{X}$, we define $R(x) = \{y : y \in \mathcal{Y} \wedge (x, y) \in R\}$.

**Representing real numbers.** We represent real numbers using strings. In each case, the range of relevant real numbers is some $[0, m)$ that will be clear from the context, and the string is to be interpreted as a fixed-point representation of numbers in that range. That is, for any $y \in [0, m)$, $y$ is evaluated as $y_1 \cdot 2^{\lceil \log m \rceil - 1} + y_2 \cdot 2^{\lceil \log m \rceil - 2} + \cdots + y_{\lceil \log m \rceil} \cdot 2^0 + y_{\lceil \log m \rceil + 1} \cdot 2^{-1} + \cdots$, where $y_i \in \{0,1\}$ and $y$ is represented by $(y_1, y_2, \dots)$.

## 2.2 Average-Case Hardness

The average-case hardness of a problem is defined with respect to a distribution over its input domain. We start by formally defining the hardness of evaluating functions.

**Definition 2.1** (Hardness of Evaluating Functions)**.** For any $\delta \in (0,1)$, $n, l, s \in \mathbb{N}$, consider a function $f : \{0,1\}^n \to \Sigma$, where $\Sigma$ is an output domain that can be encoded by $\{0,1\}^l$ and $l = \lceil \log |\Sigma| \rceil$. For a distribution $D$ over $\{0,1\}^n$, $f$ is called *$\delta$-hard on $D$ for circuits of size $s$* if, for any circuit $C : \{0,1\}^n \to \{0,1\}^l$ of size at most $s$, we have

$$\Pr_{x \leftarrow D}[C(x) = f(x)] < \delta.$$

As functions are specific instances of relations, the above definition can be generalized to a broader context.

**Definition 2.2** (Hardness of Satisfying Relations)**.** For any $\delta \in (0,1)$, $n, l, s \in \mathbb{N}$, consider a relation $R \subseteq \{0,1\}^n \times \Sigma$, where $\Sigma$ is an output domain that can be encoded by $\{0,1\}^l$ and $l = \lceil \log |\Sigma| \rceil$. For a distribution $D$ over $\{0,1\}^n$, $R$ is called *$\delta$-hard on $D$ for circuits of size $s$*, if for any circuit $C : \{0,1\}^n \to \{0,1\}^l$ of size at most $s$,

$$\Pr_{x \leftarrow D}[C(x) \in R(x)] < \delta.$$

We introduce the following terms for real-valued functions.

**Definition 2.3.** For a function $f : \{0,1\}^n \to [0,m)$, the approximation problem with distance $d$ is denoted by a relation $R_f^d \subseteq \{0,1\}^n \times \mathbb{R}$, where

$$R_f^d = \{(x,y) : |f(x) - y| < d\}.$$

Similarly, the closed approximation is defined by

$$\hat{R}_f^d = \{(x,y) : |f(x) - y| \leq d\}.$$

**Definition 2.4** (Hardness of Approximating Functions)**.** For any $\delta \in (0,1)$, $\alpha, s \in \mathbb{N}$ and $m, \epsilon \in \mathbb{R}$, consider a function $f : \{0,1\}^n \to [0,m)$. For a distribution $D$ over $\{0,1\}^n$, $f$ is called *$\delta$-hard to approximate on $D$ with accuracy $\alpha$ and distance $\epsilon$ for circuits of size $s$*, if the relation $R \subseteq \{0,1\}^n \times \{0,1\}^\alpha$ is $\delta$-hard on $D$ for circuits of size $s$, where

$$R = \{(x,y) : |f(x) - y| < \epsilon\},$$

and real value $y$ is encoded by a binary of length $\alpha$.

## 3 Hardcore Lemmas

Impagliazzo's hardcore lemma [Imp95] implies the existence of a strongly hard subset within an instance space where the Boolean function is only mildly hard on average. In this section, we first extend the hardcore lemma to a more general setting, for relations with a closure property under majority. Then, we will demonstrate how to transform a hard distribution into a balanced one, to facilitate our subsequent proofs of hardness amplification.

The following definition of density is utilized to measure the flatness of the hardcore distribution obtained, ensuring that it can be reintegrated into the original distribution [AB09, Chapter 19].

**Definition 3.1** (Relative Density)**.** For $\delta \in (0,1]$ and distributions $X, Y$ on $\{0,1\}^n$, $X$ is called *$\delta$-dense* with respect to $Y$, if for any $x \in \{0,1\}^n$, we have

$$\Pr[X = x] \leq \frac{1}{\delta} \cdot \Pr[Y = x].$$

**Claim 3.1.** *If the distribution $X$ has a relative density $\delta$, with respect to $Y$, then there exists another distribution $\bar{X}$, such that $Y = \delta X + (1-\delta)\bar{X}$.*

*Proof.* We proof this by showing the construction of $\bar{X}$. If $\delta = 1$, $X$ and $Y$ are the same distributions. For $\delta \in (0,1)$, consider any $x \in \{0,1\}^n$, let

$$\Pr[\bar{X} = x] = \frac{1}{1-\delta}\left(\Pr[Y = x] - \delta \cdot \Pr[X = x]\right) \in (0,1).$$

We have

$$\sum_{x \in \{0,1\}^n} \Pr[\bar{X} = x] = \frac{1}{1-\delta}\left(\sum_{x \in \{0,1\}^n} \Pr[Y = x] - \delta \cdot \sum_{x \in \{0,1\}^n} \Pr[X = x]\right) = 1.$$

Therefore, $\bar{X}$ is a valid distribution satisfying $Y = \delta X + (1-\delta)\bar{X}$. □

### 3.1 Hardcore Lemma for Relations

The closure property under majority is highly useful for identifying the hardcore distribution of functions or relations. Several prior studies have relied on this closure property to prove the existence of hardcore distribution [Imp95, KS03, Kal07, BHK09]. We begin by formally defining *majority combiner.*

**Definition 3.2** (Majority Combiner)**.** For a relation $R \subseteq \{0,1\}^n \times \Sigma$ and $t \in \mathbb{N}$, a circuit $M : \Sigma^t \to \Sigma$ is called a *majority combiner* for relation $R$ over $t$ coordinates, if for any $x \in \{0,1\}^n$ and any $y_1, \dots, y_t \in \Sigma$, such that $|\{i : i \in \{1,\dots,t\} \wedge y_i \in R(x)\}| > t/2$, we have $M(y_1,\dots,y_t) \in R(x)$.

The key idea behind Impagliazzo's hardcore lemma is that, if for any distribution $H$ with certain density, there always exists a circuit of slightly smaller size that solves the problem with probability more than $\frac{1}{2} + \gamma$, for some $\gamma \in (0,1)$, then we can construct a larger circuit by taking the majority vote of multiple carefully chosen circuits, which can result in a high probability of agreement with function $f$, leading to a contradiction.

**Lemma 3.2** (Extended Hardcore Lemma)**.** *For $n \in \mathbb{N}$, consider a relation $R \subseteq \{0,1\}^n \times \{0,1\}^m$; define $G = \{x : \forall y \in \{0,1\}^m, y \in R(x)\}$. Consider any distribution $D$ over $\{0,1\}^n$. Consider any $\delta \in (0,1)$, $\gamma \in (0,1/2)$, and large enough $s \in \mathbb{N}$. Let $t = \lceil \frac{8\log(2/\gamma\delta)}{\gamma^2} \rceil$ be an integer. If there exists a majority combiner for relation $R$ over $t$ coordinates of size at most $s/2$, and $R$ is $(1-\delta)$-hard on $D$ for circuits of size $s$, then there is a distribution $H$ over $\{0,1\}^n \setminus G$ which is $\delta$-dense with respect to $D$, such that $R$ is $(\frac{1}{2}+\gamma)$-hard on $H$ for circuits of size $\frac{\gamma^2 s}{16\log(2/\gamma\delta)}$.*

**Remark 3.1.** *The best-known parameter for the small circuit size in the lemma is $O(\frac{\gamma^2 s}{\log(1/\delta)})$, whereas the bound we present here is $O(\frac{\gamma^2 s}{\log(2/\gamma\delta)})$. In fact, the proof in [BHK09], which uses a multiplicative weight update method, can be directly adapted to our extended setting. For simplicity, we provide a proof for a slightly weaker bound, which suffices for our purpose.*

We follow the proof in [Imp95, AB09] with some subtle adjustments, and prove the statement via the Min-Max theorem.

*Proof of Lemma 3.2.* For a relation $R$ that is $(1-\delta)$-hard on a distribution $D$, consider a zero-sum game between two players A and B, defined as follows. Player A selects a circuit $C : \{0,1\}^n \to \{0,1\}^m$ of size at most $s' = \frac{\gamma^2 s}{16\log(2/\gamma\delta)}$ to maximize the payoff, while player B chooses a distribution $S$ over $\{0,1\}^n \setminus G$ that is $\delta$-dense with respect to $D$, to minimize the payoff of A. The payoff of player A is calculated by

$$\mathsf{Payoff}(C,S) = \Pr_{x \leftarrow S}[C(x) \in R(x)].$$

Since $R$ is $(1-\delta)$-hard, the following should hold:

$$\Pr_{x \leftarrow D}[x \in G] < 1-\delta \Leftrightarrow \Pr_{x \leftarrow D}[x \notin G] > \delta. \tag{6}$$

Player B's strategy set is non-empty (at least including $D|_{x \notin G}$). For intuition, player A tends to choose a powerful circuit to solve problem $R$ and the hard instances of $R$ would benefit player B more. By the Min-Max theorem, if mixed strategy is allowed, the order of playing will not influence the game value. Suppose that two players use a mixed strategy $D_C$ and $D_S$ correspondingly, the game value is defined as

$$v = \max_{D_C} \min_{D_S} \mathop{\mathbb{E}}_{\substack{C \leftarrow D_C \\ S \leftarrow D_S}} \left[ \Pr_{x \leftarrow S}[C(x) \in R(x)] \right] = \min_{D_S} \max_{D_C} \mathop{\mathbb{E}}_{\substack{C \leftarrow D_C \\ S \leftarrow D_S}} \left[ \Pr_{x \leftarrow S}[C(x) \in R(x)] \right],$$

where $D_C$ is a distribution over all possible choices that A can choose, and $D_S$ is a distribution over all possible distribution $S$. The game value is either at least $\frac{1}{2}+\gamma$ or less than $\frac{1}{2}+\gamma$. We will show $v < \frac{1}{2}+\gamma$, as otherwise it would contradict $(1-\delta)$-hardness of $R$.

Assume that game value $v \geq \frac{1}{2}+\gamma$, then there exists a mixed strategy $D_C$, such that the expected payoff of player A would always be at least $\frac{1}{2}+\gamma$ no matter which $S$ is chosen by player B. Define a bad distribution $B_{D_C}$ as follows,

$$x \leftarrow D|_{\Pr_{C \leftarrow D_C}[C(x) \in R(x)] < \frac{1}{2}(1+\gamma)}.$$

That is, $B_{D_C}$ is the hard distribution $D$ conditioned on the above probability statement. Abusing notation, when saying $x \in B_{D_C}$, it stands for $x \in \mathsf{Supp}(B_{D_C})$. The set $B_{D_C}$ is disjoint with $G$, because for any $x \in G$, for any circuit $C$

$$\Pr[C(x) \in R(x)] = 1 > \frac{1}{2}(1+\gamma).$$

Since we assume that game value $v \geq \frac{1}{2}+\gamma$, for any $S$ with relative density $\delta$ with respect to $D$ over $\{0,1\}^n \setminus G$, we always have the following,

$$\Pr_{\substack{C \leftarrow D_C \\ x \leftarrow S}}[C(x) \in R(x)] \geq \frac{1}{2}+\gamma. \tag{7}$$

Then, we claim that

$$\Pr_{x \leftarrow D}\left[x \in B_{D_C}\right] \leq \delta\left(1-\frac{\gamma}{2}\right).$$

If not, there exists a $\gamma' < \gamma$, such that $\Pr_{x \leftarrow D}[x \in B_{D_C}] = \delta(1-\frac{\gamma'}{2})$. We construct a distribution $S'$ to derive a contradiction: with probability $(1-\frac{\gamma'}{2})$, sample $x$ from $B_{D_C}$ (which is disjoint with $G$); else sample $x$ from $D$ conditioned on $x$ not being in $(B_{D_C} \cup G)$. If $x \in B_{D_C}$, then

$$\Pr[S' = x] = \left(1-\frac{\gamma'}{2}\right) \cdot \Pr[B_{D_C} = x] = \left(1-\frac{\gamma'}{2}\right) \cdot \frac{\Pr[D = x]}{\Pr_{x \leftarrow D}\left[x \in B_{D_C}\right]} = \frac{\Pr[D = x]}{\delta}.$$

For $x \notin B_{D_C}$, we have

$$\Pr[S' = x] = \frac{\gamma'}{2} \cdot \frac{\Pr[D = x]}{\Pr_{x \leftarrow D}\left[x \notin (B_{D_C} \cup G)\right]} = \frac{\gamma'}{2} \cdot \frac{\Pr[D = x]}{\Pr_{x \leftarrow D}\left[x \notin G\right] - \Pr_{x \leftarrow D}\left[x \in B_{D_C}\right]} < \frac{\Pr[D = x]}{\delta},$$

where the last inequality follows from (6). Thus, $S'$ has relative density $\delta$, supported in $\{0,1\}^n \setminus G$.

$$\Pr_{\substack{C\leftarrow D_C\\ x\leftarrow S'}}[C(x)\in R(x)] \le \left(1-\frac{\gamma'}{2}\right)\Pr_{\substack{C\leftarrow D_C\\ x\leftarrow B_{D_C}}}[C(x)\in R(x)] + \frac{\gamma'}{2} < \frac{1}{2}+\gamma,$$

which contradicts the assumption (7).

Let $t = \frac{8\log(2/\gamma\delta)}{\gamma^2}$. According to our hypothesis on $R$, for any large enough $s$, there is a circuit $M$ of size at most $\frac{s}{2}$, such that, for any $x \in \{0,1\}^n$, $M(y_1,\ldots,y_t)\in R(x)$ if the majority of $y_i$ satisfies $y_i \in R(x)$ for $i\in\{1,\ldots,t\}$. Construct a circuit $\hat{C}$, as follows: sample $C_1,\ldots,C_t \leftarrow D_C$ independently, let $\hat{C}(x) = M(C_1(x),\ldots,C_t(x))$, the size of $\hat{C}$ is at most $t\cdot\frac{\gamma^2 s}{16\log(2/\gamma\delta)} + \frac{s}{2} \le s$. By taking Chernoff bound, for any $x \notin B_{D_C}$, the probability that $\hat{C}$ outputs a wrong value is at most $e^{-\gamma^2 t/8}$. Therefore,

$$\begin{aligned}\Pr_{x\leftarrow D}[\hat{C}(x)\in R(x)] &\ge \Pr_{x\leftarrow D}[\hat{C}(x)\in R(x)\,|x\notin B_{D_C}]\Pr_{x\leftarrow D}[x\notin B_{D_C}]\\ &\ge 1-\Pr_{x\leftarrow D}[\hat{C}(x)\notin R(x)|x\notin B_{D_C}] - \Pr_{x\leftarrow D}[x\in B_{D_C}]\\ &\ge 1-e^{-\gamma^2 t/8} - \delta\left(1-\frac{\gamma}{2}\right)\\ &= 1-\delta.\end{aligned}$$

which contradicts the assumption that $R$ is $(1-\delta)$-hard on $D$ for circuit size $s$. Therefore, game value cannot exceed $\frac{1}{2}+\gamma$.

Consequently, there exists a mixed strategy $D_S$, such that for any $C$ with size at most $s'$,

$$\Pr_{\substack{S\leftarrow D_S\\ x\leftarrow S}}[C(x)\in R(x)] < \frac{1}{2}+\gamma.$$

Then, define the hardcore distribution $H$ as follows: sample $S \leftarrow D_S$, $x \leftarrow S$. Since each $S$ is supported in $\{0,1\}^n \setminus G$ and is $\delta$-dense with respect to $D$, and $H$ is a convex combination of $S$'s, $H$ is also supported in $\{0,1\}^n \setminus G$ and has $\delta$-density with respect to $D$. □

## 3.2 Balancing Hardcore Distributions

**Definition 3.3** (Balanced Distribution)**.** For any domain $\Sigma$, given a distribution $X$ on $\{0,1\}^n$ and $y_0, y_1 \in \Sigma$, a relation $R \subseteq \{0,1\}^n \times \Sigma$ is called *balanced* on $X$ around $\{y_0, y_1\}$, if

$$\Pr_{x\leftarrow X}[y_0\in R(x)] = \Pr_{x\leftarrow X}[y_1\in R(x)] = \frac{1}{2} \text{ and } \Pr_{x\leftarrow X}[y_0\in R(x)\wedge y_1\in R(x)] = 0.$$

**Lemma 3.3** (Balanced Hardcore)**.** *For $\gamma\in(0,\frac{1}{2})$, $\delta\in(0,1)$ and $s\in\mathbb{N}$, for a relation $R\subseteq\{0,1\}^n\times\Sigma$ and distributions $H, D$ over $\{0,1\}^n$, suppose that there exist $a,b\in\Sigma$, $a\neq b$, such that*

- *For any $x\in\mathsf{Supp}(H)$, there is exactly one of the following holds: $a\in R(x)$ or $b\in R(x)$.*
- *Letting $D_a$ denote the distribution $x\leftarrow D|_{a\in R(x)\wedge b\notin R(x)}$ and $D_b$ denote the distribution $x\leftarrow D|_{b\in R(x)\wedge a\notin R(x)}$; $D_a, D_b$ has $\delta$-density with respect to $D$.*

*If $H$ is a $\delta$-dense distribution with respect to $D$ and $R$ is $\frac{1}{2}(1+\gamma)$-hard on $H$ for circuits of size $s$, then there is a distribution $H'$ with density $\delta$ with respect to $D$, on which $R$ is balanced around $\{a,b\}$ and $(\frac{1}{2}+\gamma)$-hard for circuits of size $s$.*

*Proof.* Let $p_a = \Pr_{x \leftarrow H}[a \in R(x)]$ and $p_b = \Pr_{x \leftarrow H}[b \in R(x)]$. $R$ is $\frac{1}{2}(1+\gamma)$-hard on $H$, then

$$\frac{1}{2}(1-\gamma) < p_a, p_b < \frac{1}{2}(1+\gamma).$$

Otherwise, there is a circuit that trivially outputs $a$ or $b$ can succeed with probability at least $\frac{1}{2}(1+\gamma)$. Then, construct a distribution $\hat{H}$ by the following steps:

- Let $\hat{p}_a = \frac{1}{\gamma}\left(\frac{1+\gamma}{2} - p_a\right)$ and $\hat{p}_b = \frac{1}{\gamma}\left(\frac{1+\gamma}{2} - p_a\right)$. If $p_a, p_b \in \frac{1}{2}(1 \pm \gamma)$, $\hat{p}_a, \hat{p}_b \in (0,1)$.
- With probability $\hat{p}_a$, sample an instance $x$ from $D_a$ uniformly randomly; with probability $\hat{p}_b$, sample an instance $x$ from $D_b$ uniformly randomly.

In the following, we first show that the distribution $H' = \frac{1}{1+\gamma}H + \frac{\gamma}{1+\gamma}\hat{H}$ is balanced. The support of $H'$ is over $D_a \cup D_b$, then, for any $x \in \mathsf{Supp}(H')$, only one of the following holds: $a \in R(x)$ or $b \in R(x)$.

$$\Pr_{x \leftarrow H'}[a \in R(x)] = \frac{1}{1+\gamma}p_a + \frac{\gamma}{1+\gamma}\hat{p}_a = \frac{1}{2}.$$

Similarly, $\Pr_{x \leftarrow H'}[b \in R(x)] = \frac{1}{2}$. Therefore, $R$ is balanced on $H'$ around $\{a, b\}$.

Since $D_a, D_b$ has $\delta$-density with respect to $D$, for any $x \in \{0,1\}^n$, we have

$$\Pr[\hat{H} = x] \le \max\left\{\hat{p}_a \cdot \frac{\Pr[D = x]}{\delta}, \hat{p}_b \cdot \frac{\Pr[D = x]}{\delta}\right\} < \frac{\Pr[D = x]}{\delta}.$$

Both of $H$ and $\hat{H}$ have $\delta$-density with respect to $D$, since $H'$ is a convex combination of $H$ and $\hat{H}$, $H'$ is $\delta$-dense with respect to $D$.

Consider any circuit $C$ of size $s$,

$$\begin{aligned}
\Pr_{x \leftarrow H'}[C(x) \in R(x)] &= \frac{1}{1+\gamma} \Pr_{x \leftarrow H}[C(x) \in R(x)] + \frac{\gamma}{1+\gamma} \Pr_{x \leftarrow \hat{H}}[C(x) \in R(x)] \\
&\le \frac{1}{1+\gamma} \cdot \frac{1}{2}(1+\gamma) + \frac{\gamma}{1+\gamma} \\
&< \frac{1}{2} + \gamma.
\end{aligned}$$

Therefore, $R$ is $(\frac{1}{2}+\gamma)$-hard on $H'$ for circuits of size $s$. □

# 4 Evaluating Integer-Valued Functions

We now present our hardness amplification result for evaluating integer-valued functions. Given a function $f$, which is somewhat hard to evaluate on average, it is feasible to show that the function $\mathsf{SUM}_t \otimes f$ possesses a strong average-case hardness, where $\mathsf{SUM}_t$ represents the summation function over $t$ coordinates. We state our main theorem below.

**Theorem 4.1.** *For $\delta \in (0,1)$, $m, s, t \in \mathbb{N}$ and a distribution $D$ over $\{0,1\}^n$, for any large enough $s$, consider a function $f : \{0,1\}^n \to \mathbb{Z}_m$ that is $(1-\delta)$-hard on $D$ for circuits of size $s$, define a function $g : (\{0,1\}^n)^t \to \mathbb{Z}_{t \cdot m}$ as follows:*

$$g(x_1, \ldots, x_t) = \sum_{i=1}^{t} f(x_i).$$

*Then, for $\gamma \in (0,1)$, for large enough $s$, $g$ is $\eta$-hard on $D^t$ for circuits of size $s'$, where*

$$\eta = e^{-\mu/4} + \frac{\binom{\mu}{\lfloor \frac{\mu}{2} \rfloor}}{2^\mu}\left(1 + \lceil \frac{\mu}{2} \rceil \gamma\right), \mu = \lceil \frac{t\delta}{m(m-1)} \rceil,$$
$$s' = \frac{\gamma^2 s}{512 m^2 \log(4m^2/\gamma\delta)}.$$

For sufficiently small $\gamma$, the dominant term of $\eta$ is $\frac{\binom{\mu}{\mu/2}}{2^\mu} = \Theta(\frac{1}{\sqrt{\mu}})$. Taking $t$ large enough enables us to establish hardness amplification. To prove it, we will first construct the hardcore distribution for the function $f$, show that summation effectively amplify the hardness on this hard distribution and then generalize the result to the original distribution.

Intuitively, the hardcore distribution of any Boolean-valued function is straightforward, as the output is restricted to either yes or no. However, for integer-valued functions, the structure of a hard set is inherently more complicated. We characterize the hardcore of integer-valued functions by defining a set of new problems, simply considering two values in the output domain and an input value is only considered relevant if its corresponding output matches one of those. We show that there is a pair of values such that the resulting problem is hard. Then, we extract a hardcore from this hard problem, which possesses a good structure corresponding to the original function.

**Lemma 4.2.** *For $\delta \in (0,1)$, $m, s \in \mathbb{N}$ and a distribution $D$ over $\{0,1\}^n$, consider a function $f : \{0,1\}^n \to \mathbb{Z}_m$. For any $a, b \in \mathbb{Z}_m$ and $a \neq b$, define the relation $R_{a,b} \subseteq \{0,1\}^n \times \{0,1\}^{\lceil \log m \rceil}$ as follows:*

- *If $f(x) \in \{a,b\}$, then $(x,y) \in R_{a,b}$ if and only if $y = f(x)$;*
- *If $f(x) \notin \{a,b\}$, then $(x,y) \in R_{a,b}$ for any $y \in \{0,1\}^{\lceil \log m \rceil}$.*

*For $s \gg m^2 \log m$, if $f$ is $(1-\delta)$-hard on $D$ for circuits of size $s$, there exists a pair of $a, b \in \mathbb{Z}_m, a \neq b$, such that $R_{a,b}$ is $\left(1 - \frac{2\delta}{m(m-1)}\right)$-hard on $D$ for circuits of size $\frac{s}{m^2}$.*

This lemma suggests that if the function $f$ is hard to evaluate on average, then there must exist output values $a, b$, such that distinguishing their pre-images is also hard on average. We defer the proof to Section 4.1, and our hardcore construction is shown below.

**Lemma 4.3** (Hardcore for Integer-Valued Functions)**.** *For $\delta, \gamma \in (0,1)$, $m, s \in \mathbb{N}$ and a distribution $D$, consider a function $f : \{0,1\}^n \to \mathbb{Z}_m$, which is $(1-\delta)$-hard on $D$ for circuits of size $s$. If $s$ is sufficient large, there exist $a, b \in \mathbb{Z}_m, a \neq b$ and a $\frac{2\delta}{m(m-1)}$-dense distribution $H$ (with respect to $D$), on which $f$ is balanced around $\{a,b\}$ and $\frac{1}{2}(1+\gamma)$-hard for circuits of size $\frac{\gamma^2 s}{256 m^2 \log(4m^2/\gamma\delta)}$.*

*Proof.* Suppose $f : \{0,1\}^n \to \mathbb{Z}_m$ is $(1-\delta)$-hard on $D$ for circuits of size $s$, by Lemma 4.2, if $s \gg m^2 \log m$, there exists a pair of $a, b \in \mathbb{N}, a \neq b$, such that $R_{a,b}$ is $\left(1 - \frac{2\delta}{m(m-1)}\right)$-hard on $D$ for circuits of size $\frac{s}{m^2}$. This hardness implies that $\Pr_{x \leftarrow D}[f(x) = a] > \frac{2\delta}{m(m-1)}$, then the distribution $D|_{f(x)=a}$ is $\frac{2\delta}{m(m-1)}$-dense with respect to $D$ (and the same holds for $b$).

For relation $R_{a,b}$, the majority gate is a natural choice for the combiner. For some $\gamma \in (0,1)$, let $t = \frac{128 \log(4m^2/\gamma\delta)}{\gamma^2}$ be an integer, if the size of majority-of-$t$ circuits is less than $\frac{s}{2m^2}$, by Lemma 3.2, there is a $\frac{2\delta}{m(m-1)}$-dense hardcore distribution $H'$ (with respect to $D$) over $\{x : f(x) \in \{a,b\}\} \subseteq \{0,1\}^n$, on which $R_{a,b}$ is $(\frac{1}{2} + \frac{\gamma}{4})$-hard for circuits of size $\frac{\gamma^2 s}{256 m^2 \log(4m^2/\gamma\delta)}$.

By Lemma 3.3, we can construct a distribution $H$ with density $\frac{2\delta}{m(m-1)}$ (with respect to $D$), on which $f$ is balanced around $\{a,b\}$ and $\frac{1}{2}(1+\gamma)$-hard for circuits of size $\frac{\gamma^2 s}{256 m^2 \log(4m^2/\gamma\delta)}$. □

We believe that this hardcore distribution exhibits a desirable structure, given that the hardness of evaluating function $f$ on it can be captured by indistinguishability. In the following, we consider the inputs sampled from the hardcore distribution. It is a natural way to amplify the average-case hardness of function $f$, by constructing the function $\mathsf{SUM}_t \otimes f$. If $f$ is hard on distribution $H$ on which there are two possible outputs, then the best algorithm with restricted running time would not perform significantly better than random guessing. Consequently, the almost optimal way for guessing the value of $\mathsf{SUM}_t \otimes f$ on $H^t$ is output the one with the highest probability of occurring.

**Lemma 4.4.** *For $\gamma \in (0,1)$, $m, s, t \in \mathbb{N}$ and $a, b \in \mathbb{Z}_m$, consider a hardcore distribution $H \subseteq \{0,1\}^n$, on which function $f : \{0,1\}^n \to \mathbb{Z}_m$ is balanced around $\{a, b\}$ and $\frac{1}{2}(1+\gamma)$-hard for circuits of size $s$. Define the function $g : (\{0,1\}^n)^t \to \mathbb{Z}_{t\cdot m}$ as follows:*

$$g(x_1, \ldots, x_t) = \sum_{i=1}^{t} f(x_i).$$

*For $k \in \mathbb{N}, 0 < k \leq t$ and any other distribution $G$ over $(\{0,1\}^n)^{t-k}$, for sufficient large $s$, specifically $s \gg \log(t \cdot m)$, the function $g$ is $\eta$-hard on $\Pi_t(H^k, G)$ for circuits of size $\frac{s}{2}$, where*

$$\eta = \frac{\binom{k}{\lfloor \frac{k}{2} \rfloor}}{2^k} \left(1 + \lceil \frac{k}{2} \rceil \gamma\right).$$

This lemma demonstrates that summation can effectively amplify the hardness over the hardcore distribution, for which the proof will be presented in Section 4.2. However, the hardcore lemma only ensures the existence of a hard distribution without guaranteeing efficient sampling. Therefore, to derive a more meaningful hardness result, we will eventually focus on the hardness on the original distribution.

One direct approach is to embed this distribution into the original one with some probability mass parameterized by its relative density. When sampling instances from the original distribution a sufficient number of times, the number of instances sampled from the hard one will concentrate around the expected value. Based on this observation, we proceed to prove our main theorem.

**Theorem 4.1.** *For $\delta \in (0,1)$, $m, s, t \in \mathbb{N}$ and a distribution $D$ over $\{0,1\}^n$, for any large enough $s$, consider a function $f : \{0,1\}^n \to \mathbb{Z}_m$ that is $(1-\delta)$-hard on $D$ for circuits of size $s$, define a function $g : (\{0,1\}^n)^t \to \mathbb{Z}_{t\cdot m}$ as follows:*

$$g(x_1, \ldots, x_t) = \sum_{i=1}^{t} f(x_i).$$

*Then, for $\gamma \in (0,1)$, for large enough $s$, $g$ is $\eta$-hard on $D^t$ for circuits of size $s'$, where*

$$\eta = e^{-\mu/4} + \frac{\binom{\mu}{\lfloor \frac{\mu}{2} \rfloor}}{2^\mu} \left(1 + \lceil \frac{\mu}{2} \rceil \gamma\right), \mu = \lceil \frac{t\delta}{m(m-1)} \rceil,$$
$$s' = \frac{\gamma^2 s}{512 m^2 \log(4m^2/\gamma\delta)}.$$

*Proof.* Theorem 4.1 For a function $f : \{0,1\}^n \to \mathbb{Z}_m$, which is $(1-\delta)$-hard on $D$ for circuits of size $s$, by Lemma 4.3, there exists $a, b \in \mathbb{Z}_m, a \neq b$ and a $\frac{2\delta}{m(m-1)}$-dense distribution $H$ with respect to $D$, such that $f$ is balanced around $\{a, b\}$ and $\frac{1}{2}(1+\gamma)$-hard on $H$ for circuits of size $\hat{s} = \frac{\gamma^2 s}{256 m^2 \log(4m^2/\gamma\delta)}$.

$H$ has density $\hat{\delta} = \frac{2\delta}{m(m-1)}$, then there exists a distribution $G$ over $\{0,1\}^n$, such that $D = \hat{\delta}H + (1-\hat{\delta})G$. For $t \in \mathbb{N}$, we have

$$D^t = \sum_{k=0}^{t} \binom{t}{k} \hat{\delta}^k (1-\hat{\delta})^{t-k} \cdot \Pi_t(H^k, G^{t-k}).$$

Therefore, for any large enough $s \in \mathbb{N}$, for any circuit $C$ of size $s' = \frac{\hat{s}}{2}$, by Lemma 4.4, we have

$$\begin{aligned}
\Pr_{x \leftarrow D^t}[C(x) = g(x)] &= \sum_{k=0}^{t} \binom{t}{k} \cdot \hat{\delta}^k (1-\hat{\delta})^{t-k} \cdot \Pr_{x \leftarrow \Pi_t(H^k, G^{t-k})}[C(x) = g(x)] \\
&\leq \sum_{k=0}^{\mu-1} \binom{t}{k} \cdot \hat{\delta}^k (1-\hat{\delta})^{t-k} + \sum_{k=\mu}^{t} \binom{t}{k} \cdot \hat{\delta}^k (1-\hat{\delta})^{t-k} \cdot \frac{\binom{\mu}{\lfloor \frac{\mu}{2} \rfloor}}{2^\mu} \left(1 + \lceil \frac{\mu}{2} \rceil \gamma\right) \\
&< \sum_{k=0}^{\mu-1} \binom{t}{k} \cdot \hat{\delta}^k (1-\hat{\delta})^{t-k} + \frac{\binom{\mu}{\lfloor \frac{\mu}{2} \rfloor}}{2^\mu} \left(1 + \lceil \frac{\mu}{2} \rceil \gamma\right) \\
&< e^{-\mu/4} + \frac{\binom{\mu}{\lfloor \frac{\mu}{2} \rfloor}}{2^\mu} \left(1 + \lceil \frac{\mu}{2} \rceil \gamma\right),
\end{aligned}$$

where $\mu = \lceil \frac{t\hat{\delta}}{2} \rceil$. The last inequality is obtained by Chernoff bound, where the first term is equivalent to the probability that a binomial distribution with parameter $(n, \hat{\delta})$ samples a value less than $\mu$. □

### 4.1 Proof of Lemma 4.2

**Lemma 4.2.** *For $\delta \in (0,1)$, $m, s \in \mathbb{N}$ and a distribution $D$ over $\{0,1\}^n$, consider a function $f : \{0,1\}^n \to \mathbb{Z}_m$. For any $a, b \in \mathbb{Z}_m$ and $a \neq b$, define the relation $R_{a,b} \subseteq \{0,1\}^n \times \{0,1\}^{\lceil \log m \rceil}$ as follows:*

- *If $f(x) \in \{a, b\}$, then $(x, y) \in R_{a,b}$ if and only if $y = f(x)$;*
- *If $f(x) \notin \{a, b\}$, then $(x, y) \in R_{a,b}$ for any $y \in \{0,1\}^{\lceil \log m \rceil}$.*

*For $s \gg m^2 \log m$, if $f$ is $(1-\delta)$-hard on $D$ for circuits of size $s$, there exists a pair of $a, b \in \mathbb{Z}_m, a \neq b$, such that $R_{a,b}$ is $\left(1 - \frac{2\delta}{m(m-1)}\right)$-hard on $D$ for circuits of size $\frac{s}{m^2}$.*

*Proof.* Assume that, for any $a, b \in \mathbb{Z}_m$, $a < b$, there is a circuit $C_{a,b} : \{0,1\}^n \to \{0,1\}^{\lceil \log m \rceil}$ of size $\frac{s}{m^2}$, such that

$$\Pr_{x \leftarrow D}[C_{a,b}(x) \in R_{a,b}(x)] \geq 1 - \frac{2\delta}{m(m-1)}.$$

Let $C_{b,a} = C_{a,b}$. Then, we can construct a circuit $C$ as follows:

```
• Input: $x \in \{0,1\}^n$
• For $i \in \{0, 1, \dots, m-1\}$:
    – If for every $j \neq i$, $C_{i,j}(x) = i$ holds, return $i$.
• Return $\perp$.
```

During the process, $C$ compares each output of $C_{i,j}(x)$ with $i$, which means there are $\Theta(m^2)$ comparison of $\Theta(\log m)$ bits, so the circuit complexity of $C$ is at most $\binom{m}{2} \cdot \frac{s}{m^2} + c \cdot m^2 \log m$, where $c$ is a constant. If $s \gg m^2 \log m$, the size of $C$ is at most $s$.

By taking the union bound, we have

$$\Pr_{x \leftarrow D}[\exists (a,b), a < b : C_{a,b}(x) \notin R_{a,b}(x)] \leq \sum_{a<b} \Pr_{x \leftarrow D}[C_{a,b}(x) \notin R_{a,b}(x)] \leq \delta.$$

For any input $x$, there exists at most one $i$, such that for every $j \neq i$, $C_{i,j}(x)$ outputs $i$. If not, we have $C_{i,j}(x) = i = j$, which leads to a contradiction.

If every $C_{a,b}(x)$ outputs a correct value in $R_{a,b}(x)$, there exists a unique $i = f(x)$, such that $C_{i,j}(x) \in R_{i,j}(x)$ for every $j \neq i$, then $C$ computes $f(x)$ correctly.

$$\Pr_{x \leftarrow D}[C(x) = f(x)] \geq \Pr_{x \leftarrow D}[\forall (a,b), a < b : C_{a,b}(x) \in R_{a,b}(x)] \geq 1 - \delta,$$

which contradicts the fact that $f$ is $(1-\delta)$-hard for circuits of size $s$. □

## 4.2 Proof of Lemma 4.4

**Lemma 4.4.** *For $\gamma \in (0,1)$, $m, s, t \in \mathbb{N}$ and $a, b \in \mathbb{Z}_m$, consider a hardcore distribution $H \subseteq \{0,1\}^n$, on which function $f : \{0,1\}^n \to \mathbb{Z}_m$ is balanced around $\{a,b\}$ and $\frac{1}{2}(1+\gamma)$-hard for circuits of size $s$. Define the function $g : (\{0,1\}^n)^t \to \mathbb{Z}_{t \cdot m}$ as follows:*

$$g(x_1, \ldots, x_t) = \sum_{i=1}^{t} f(x_i).$$

*For $k \in \mathbb{N}, 0 < k \leq t$ and any other distribution $G$ over $(\{0,1\}^n)^{t-k}$, for sufficient large $s$, specifically $s \gg \log(t \cdot m)$, the function $g$ is $\eta$-hard on $\Pi_t(H^k, G)$ for circuits of size $\frac{s}{2}$, where*

$$\eta = \frac{\binom{k}{\lfloor \frac{k}{2} \rfloor}}{2^k} \left(1 + \lceil \frac{k}{2} \rceil \gamma \right).$$

*Proof.* Consider a hardcore distribution $H$ and a function $f : \{0,1\}^n \to \mathbb{Z}_m$, such that $f$ is balanced around $\{a,b\}$ and $\frac{1}{2}(1+\gamma)$-hard on $H$ for circuits of size $s$. Let $H_a$ denote the distribution $x \leftarrow H|_{f(x)=a}$ and $H_b$ denote $x \leftarrow H|_{f(x)=b}$, we have $H = \frac{1}{2}H_a + \frac{1}{2}H_b$. For any $i, k \in \mathbb{N}$, denote $\Pi(H_a^i, H_b^{k-i})$ by $H_i^k$ Then, consider any $\hat{x} = (\hat{x}_1, \ldots, \hat{x}_{t-k}) \in (\{0,1\}^n)^{t-k}$ and a permutation $\pi$ of $t$ entries, we claim the following fact.

**Claim 4.5.** *If $s \gg \log(t \cdot m)$, for any circuit $C : (\{0,1\}^n)^t \to \{0,1\}^{\lceil \log tm \rceil}$ of size at most $\frac{s}{2}$ and any $i \in \mathbb{Z}_k$, $v \in \mathbb{Z}_{t \cdot m}$, we have*

$$\left| \Pr_{\bar{x} \leftarrow H^k} \left[ C(\pi(\bar{x}, \hat{x})) = v | \bar{x} \in H_{i+1}^k \right] - \Pr_{\bar{x} \leftarrow H^k} \left[ C(\pi(\bar{x}, \hat{x})) = v | \bar{x} \in H_i^k \right] \right| < \gamma.$$

By Claim 4.5 (which is proven below), combined with triangle inequality, for any $i, j \in \mathbb{Z}_k$,

$$\Pr_{\bar{x} \leftarrow H^k} \left[ C(\pi(\bar{x}, \hat{x})) = v | \bar{x} \in H_i^k \right] < \Pr_{\bar{x} \leftarrow H^k} \left[ C(\pi(\bar{x}, \hat{x})) = v | \bar{x} \in H_j^k \right] + |i - j| \gamma.$$

Let $\Delta = \sum_{i=1}^{t-k} f(\hat{x}_i)$. For any circuit $C : (\{0,1\}^n)^t \to \{0,1\}^{\lceil \log tm \rceil}$ of size at most $\frac{s}{2}$,

$$\begin{aligned}
&\Pr_{\bar{x} \leftarrow H^k}\left[C(\pi(\bar{x},\hat{x})) = g(\pi(\bar{x},\hat{x}))\right] \\
&= \sum_{i=0}^{k} \Pr_{\bar{x} \leftarrow H^k}\left[\bar{x} \in H_i^k\right] \Pr_{\bar{x} \leftarrow H^k}\left[C(\pi(\bar{x},\hat{x})) = g(\bar{x},\hat{x}) \,\middle|\, \bar{x} \in H_i^k\right] \\
&= \sum_{i=0}^{k} \Pr_{\bar{x} \leftarrow H^k}\left[\bar{x} \in H_i^k\right] \Pr_{\bar{x} \leftarrow H^k}\left[C(\pi(\bar{x},\hat{x})) = ai + b(k-i) + \Delta \,\middle|\, \bar{x} \in H_i^k\right] \\
&< \frac{1}{2^k} \sum_{i=0}^{k} \binom{k}{i} \left( \Pr_{\bar{x} \leftarrow H^k}\left[C(\pi(\bar{x},\hat{x})) = ai + b(k-i) + \Delta \,\middle|\, \bar{x} \in H_{\lfloor \frac{k}{2} \rfloor}^k\right] + \left| i - \lfloor \frac{k}{2} \rfloor \right| \gamma \right) \\
&\leq \frac{1}{2^k} \left( \binom{k}{\lfloor \frac{k}{2} \rfloor} \sum_{i=0}^{k} \Pr_{\bar{x} \leftarrow H^k}\left[C(\pi(\bar{x},\hat{x})) = ai + b(k-i) + \Delta \,\middle|\, \bar{x} \in H_{\lfloor \frac{k}{2} \rfloor}^k\right] + \gamma \sum_{i=0}^{k} \binom{k}{i} \left| i - \frac{k}{2} \right| \right) \\
&\leq \frac{1}{2^k} \left( \binom{k}{\lfloor \frac{k}{2} \rfloor} + \lceil \frac{k}{2} \rceil \gamma \cdot \binom{k}{\lfloor \frac{k}{2} \rfloor} \right) \\
&\leq \frac{\binom{k}{\lfloor \frac{k}{2} \rfloor}}{2^k} \left( 1 + \lceil \frac{k}{2} \rceil \gamma \right).
\end{aligned}$$

The second last line is obtained by Claim 4.6. Then, for any distribution $G$ over $(\{0,1\}^n)^{t-k}$,

$$\Pr_{\bar{x} \leftarrow \Pi(H^k, G)}\left[C(\bar{x}) = g(\bar{x})\right] \leq \frac{\binom{k}{\lfloor \frac{k}{2} \rfloor}}{2^k} \left( 1 + \lceil \frac{k}{2} \rceil \gamma \right).$$

□

**Claim 4.6.** *For any $t \in \mathbb{N}$,*

$$\sum_{i=0}^{t} \left| i - \frac{t}{2} \right| \binom{t}{i} = \lceil \frac{t}{2} \rceil \cdot \binom{t}{\lfloor \frac{t}{2} \rfloor}.$$

*Proof.* For any $t \in \mathbb{N}$,

$$\begin{aligned}
\sum_{i=0}^{t} \left| i - \frac{t}{2} \right| \binom{t}{i} &= \sum_{i=0}^{\lfloor \frac{t}{2} \rfloor} (t - 2i) \binom{t}{i} = \sum_{i=0}^{\lfloor \frac{t}{2} \rfloor} \left( (t-i) \cdot \frac{t!}{i!(t-i)!} - i \cdot \frac{t!}{i!(t-i)!} \right) \\
&= \sum_{i=0}^{\lfloor \frac{t}{2} \rfloor} t \cdot \binom{t-1}{i} - \sum_{i=1}^{\lfloor \frac{t}{2} \rfloor} t \cdot \binom{t-1}{i-1} = t \cdot \binom{t-1}{\lfloor \frac{t}{2} \rfloor} = \lceil \frac{t}{2} \rceil \cdot \binom{t}{\lfloor \frac{t}{2} \rfloor}.
\end{aligned}$$

□

### 4.2.1 Proof of Claim 4.5

**Claim 4.5.** *If $s \gg \log(t \cdot m)$, for any circuit $C : (\{0,1\}^n)^t \to \{0,1\}^{\lceil \log tm \rceil}$ of size at most $\frac{s}{2}$ and any $i \in \mathbb{Z}_k$, $v \in \mathbb{Z}_{t \cdot m}$, we have*

$$\left| \Pr_{\bar{x} \leftarrow H^k}\left[C(\pi(\bar{x},\hat{x})) = v | \bar{x} \in H_{i+1}^k\right] - \Pr_{\bar{x} \leftarrow H^k}\left[C(\pi(\bar{x},\hat{x})) = v | \bar{x} \in H_i^k\right] \right| < \gamma.$$

*Proof.* Without loss of generality, suppose there exists a circuit $C : (\{0,1\}^n)^t \to \{0,1\}^{\lceil \log tm \rceil}$ of size at most $\frac{s}{2}$ and $i \in \mathbb{Z}_k$, $k \in \mathbb{Z}_{t \cdot m}$, such that

$$\left| \Pr_{\bar{x} \leftarrow H^k} \left[ C(\pi(\bar{x}, \hat{x})) = v | \bar{x} \in H_{i+1}^k \right] - \Pr_{\bar{x} \leftarrow H^k} \left[ C(\pi(\bar{x}, \hat{x})) = v | \bar{x} \in H_i^k \right] \right| \geq \gamma.$$

Then, there must exists a tuple $(x_1, x_2, \ldots, x_{k-1})$ and a permutation $\pi_k$ of $k$ entries, such that

$$\Pr_{x \leftarrow H} \left[ C(\pi(\pi_k(x, x_1, \ldots, x_{k-1}), \hat{x})) = v | x \in H_a \right] - \Pr_{x \leftarrow H} \left[ C(\pi(\pi_k(x, x_1, \ldots, x_{k-1}), \hat{x})) = v | x \in H_b \right] \geq \gamma.$$

Construct a circuit $C'$, implementing $C$ by taking an input of length $n$, along with fixed $\pi, \hat{x}$ and $\pi_k, (x_1, \ldots, x_{k-1}), v$ as the non-uniform advice, outputs $a$ if and only if $C$ outputs $v$ and outputs $b$ otherwise. Then,

$$\left| \Pr_{x \leftarrow H} [C'(x) = a | x \in H_a] - \Pr_{x \leftarrow H} [C'(x) = b | x \in H_b] \right| \geq \gamma.$$

Therefore, the probability that $C'$ correctly compute $f$ is

$$\Pr_{x \leftarrow H} [C'(x) = f(x)] = \frac{1}{2} \Pr[C'(x) = a | x \in H_a] + \frac{1}{2} \Pr[C'(x) = b | x \in H_b] \geq \frac{1}{2}(1 + \gamma),$$

which contradict to $f$ is $\frac{1}{2}(1+\gamma)$-hard on $H$.

□

# 5 Approximating Real-Valued Functions

In this section, we extend our results to real-valued functions. To avoid any precision loss introduced by encoding, we assume that for any open interval of length $\frac{\epsilon}{2}$, there is a value that can be encoded by $\{0,1\}^\alpha$ in the interval. Therefore, for any approximation considered below, we always assume $\alpha > \log(m/\epsilon) + 4$.

**Theorem 5.1.** *For $\delta \in (0,1)$, $m, \epsilon \in \mathbb{R}$, $\alpha, s, t \in \mathbb{N}$, $\alpha > \log(m/\epsilon) + 4$ and a distribution $D$ over $\{0,1\}^n$, consider a function $f : \{0,1\}^n \to [0, m)$ that is $(1-\delta)$-hard to approximate on $D$ with accuracy $\alpha$ and distance $\epsilon$, for circuits of size $s$. For any large enough $t$, define a function $g : (\{0,1\}^n)^t \to [0, t \cdot m)$ as follows:*

$$g(x_1, \ldots, x_t) = \sum_{i=1}^{t} f(x_i).$$

*Then, for $\gamma \in (0,1)$, for any large enough $s$, $g$ is $\eta$-hard to approximate on $D^t$ with accuracy $\alpha'$ and distance $\epsilon$, $\alpha' > \log(t \cdot m/\epsilon) + 4$, for circuits of size $s'$, where*

$$\eta = e^{-\mu/4} + \frac{\binom{\mu}{\frac{\mu}{2}}}{2^\mu} \left( 6 + \frac{\mu}{2}\gamma \right), \mu = \frac{\epsilon}{m}\sqrt{2t\delta},$$
$$s' = \frac{\gamma^2 \epsilon}{256 m \sqrt{2t\delta} \log(8tm^2/\epsilon^2\gamma^2\delta)} \cdot s.$$

When $\gamma$ is small enough, $\eta$ will be dominated by $\frac{\binom{\mu}{\mu/2}}{2^\mu} = \Theta(\frac{1}{\sqrt{\mu}})$. For large enough $t$, we can effectively obtain a function with strong average-case hardness to approximate by taking the summation of multiple copies of $f$.

**Lemma 5.2.** *For $\delta \in (0,1)$, $m, \epsilon \in \mathbb{R}$, $\alpha, s \in \mathbb{N}$, $\alpha > \log(m/\epsilon)+4$ and a distribution $D$ over $\{0,1\}^n$, consider a real-valued function $f : \{0,1\}^n \to [0,m)$. For any $l \in \mathbb{N}$, let $d = \frac{\epsilon}{l}$, which denotes the radius of the partitioned intervals. For any $a, b \in \{d, 3d, \ldots, (2\lceil \frac{m}{2d} \rceil - 1)d\}, a \neq b$, define the relation $R_{a,b} \subseteq \{0,1\}^n \times \{0,1\}^\alpha$ as follows:*

- *If $f(x) \in [a \pm d)$ or $f(x) \in [b \pm d)$, then $(x,y) \in R_{a,b}$ if and only if $y \in (f(x) \pm \epsilon)$;*
- *If $f(x) \notin [a \pm d)$ and $f(x) \notin [b \pm d)$, then $(x,y) \in R_{a,b}$ for any $y \in \{0,1\}^\alpha$.*

*For any integer $l > 1$, for large enough $s$, if $f$ is $(1-\delta)$-hard to approximate on $D$ with accuracy $\alpha$ and distance $\epsilon$ for circuits of size $s$, there exist $a, b \in \{d, 3d, \ldots, (2\lceil \frac{m}{2d} \rceil - 1)d\}$, $b - a > (\frac{3}{2}l - 2)d$, such that $R_{a,b}$ is $(1 - \frac{4d^2\delta}{m^2})$-hard on $D$, for circuits of size $\frac{d^2 s}{m^2}$.*

The proof is deferred to Section 5.1. Following the approach used in the integer case, we proceed with the construction of the hardcore distribution. This hard distribution maintains a good structure, on which $f$ will be balanced and mapped to $[a \pm d)$ or $[b \pm d)$, for some fixed $a, b$, which implies the closed approximation of $f$ with distance $d$ is balanced on $H$ around $\{a, b\}$.

**Lemma 5.3** (Hardcore for Real-Valued Functions)**.** *For $\delta, \gamma \in (0,1)$, $m, \epsilon \in \mathbb{R}$, $\alpha, s \in \mathbb{N}$, $\alpha > \log(m/\epsilon) + 4$ and a distribution $D$ over $\{0,1\}^n$, consider a function $f : \{0,1\}^n \to [0,m)$, which is $(1-\delta)$-hard to approximate $D$ with accuracy $\alpha$ and distance $\epsilon$ for circuits of size $s$. For any integer $l \geq 3$, let $d = \frac{\epsilon}{l}$, there exist $a, b \in \{d, 3d, \ldots, (2\lceil \frac{m}{2d} \rceil - 1)d\}$, $b - a > (\frac{3}{2}l - 2)d$, and a $\frac{4d^2\delta}{m^2}$-dense distribution $H$ (with respect to $D$), on which the closed approximation of $f$ with distance $d$ is balanced around $\{a, b\}$ and the approximation of $f$ with accuracy $\alpha$ and distance $\epsilon$ is $\frac{1}{2}(1+\gamma)$-hard for circuits of size $\frac{\gamma^2 d^2 s}{256 m^2 \log(2m^2/d^2\gamma\delta)}$.*

*Proof.* Suppose $f : \{0,1\}^n \to [0,m)$ is $(1-\delta)$-hard on $D$ for circuits of size $s$, by Lemma 5.2, for integer $l > 1$, $d = \frac{\epsilon}{l}$, if $s$ is sufficiently large, there exist $a, b \in \left\{d, 3d, \ldots, (2\lceil \frac{m}{2d} \rceil - 1)d\right\}$, $b - a > \left(\frac{3}{2}l - 2\right)d$, such that $R_{a,b}$ (as defined in Lemma 5.2) is $\left(1 - \frac{4d^2\delta}{m^2}\right)$-hard on $D$ for circuits of size $\frac{d^2 s}{m^2}$.

For $R_{a,b}$, the majority combiner can be constructed by taking the middle point. By Lemma 3.2, when $s$ is large enough, we have a $\frac{4d^2\delta}{m^2}$-dense distribution $H'$ (with respect to $D$) over $\{x : f(x) \in [a \pm d) \cup [b \pm d)\} \subseteq \{0,1\}^n$, on which $R_{a,b}$ is $(\frac{1}{2} + \frac{\gamma}{4})$-hard for circuits of size $\hat{s} = \frac{\gamma^2 d^2 s}{256 m^2 \log(2m^2/d^2\gamma\delta)}$, as well as the approximation of $f$ with accuracy $\alpha$ and distance $\epsilon$ is hard on $H'$.

If $l \geq 3$, then $b - a > 2d$, the intervals $[a \pm d]$ and $[b \pm d]$ are disjoint. Then, by Lemma 3.3, we can construct a distribution $H$ with density $\frac{4d^2\delta}{m^2}$, on which the closed approximation of $f$ with distance $d$ is balanced around $\{a, b\}$ and the approximation of $f$ with accuracy $\alpha$ and distance $\epsilon$ is $\frac{1}{2}(1+\gamma)$-hard for circuits of size $\hat{s}$. □

Analogously, we prove that summation suffices to achieve amplification on hard distributions.

**Lemma 5.4.** *For $\gamma \in (0,1)$, $m, \epsilon \in \mathbb{R}$ and $\alpha, s, t \in \mathbb{N}$, $\alpha > \log(m/\epsilon) + 4$, for large enough $l \in \mathbb{N}$, let $d = \frac{\epsilon}{l}$, consider a hardcore distribution $H \subseteq \{0,1\}^n$ and $a, b \in \left\{d, 3d, \ldots, (2\lceil \frac{m}{2d} \rceil - 1)d\right\}$, $b - a > \left(\frac{3}{2}l - 2\right)d$, on which the closed approximation of function $f : \{0,1\}^n \to [0,m)$ with distance $d$ is balanced around $\{a, b\}$ and $f$ is $\frac{1}{2}(1+\gamma)$-hard to approximate with accuracy $\alpha$ and distance $\epsilon$ for circuits of size $s$. For any integer $t$, define a function $g : (\{0,1\}^n)^t \to [0, t \cdot m)$ as follows:*

$$g(x_1, \ldots, x_t) = \sum_{i=1}^{t} f(x_i).$$

*For $k \in \mathbb{N}, 0 < k \leq t$ and any other distribution $G$ over $(\{0,1\}^n)^{t-k}$, for any large enough $s$, function $g$ is $\eta$-hard to approximate with accuracy $\alpha'$ and distance $\epsilon$ on $\Pi_t(H^k, G)$ for circuits of size $\frac{s}{2}$, where $\alpha' > \log(t \cdot m/\epsilon) + 4$ and*

$$\eta = \frac{\binom{k}{\frac{k}{2}}}{2^k} \left( \frac{3\sqrt{k}}{l} + 3 + \frac{k}{2}\gamma \right).$$

We postpone the proof to Section 5.2 and now present the proof for Theorem 5.1.

**Theorem 5.1.** *For $\delta \in (0,1)$, $m, \epsilon \in \mathbb{R}$, $\alpha, s, t \in \mathbb{N}$, $\alpha > \log(m/\epsilon) + 4$ and a distribution $D$ over $\{0,1\}^n$, consider a function $f : \{0,1\}^n \to [0,m)$ that is $(1-\delta)$-hard to approximate on $D$ with accuracy $\alpha$ and distance $\epsilon$, for circuits of size $s$. For any large enough $t$, define a function $g : (\{0,1\}^n)^t \to [0, t \cdot m)$ as follows:*

$$g(x_1, \ldots, x_t) = \sum_{i=1}^{t} f(x_i).$$

*Then, for $\gamma \in (0,1)$, for any large enough $s$, $g$ is $\eta$-hard to approximate on $D^t$ with accuracy $\alpha'$ and distance $\epsilon$, $\alpha' > \log(t \cdot m/\epsilon) + 4$, for circuits of size $s'$, where*

$$\eta = e^{-\mu/4} + \frac{\binom{\mu}{\frac{\mu}{2}}}{2^\mu} \left( 6 + \frac{\mu}{2}\gamma \right), \mu = \frac{\epsilon}{m}\sqrt{2t\delta},$$

$$s' = \frac{\gamma^2 \epsilon}{256 m \sqrt{2t\delta} \log(8tm^2/\epsilon^2\gamma^2\delta)} \cdot s.$$

*Proof.* For $\alpha > \log(m/\epsilon) + 4$ and a function $f : \{0,1\} \to [0,m)$, which is $(1-\delta)$-hard for circuits of size $s$, by Lemma 5.3, for $l \in \mathbb{N}$, let $d = \frac{\epsilon}{l}$, there exist $a, b \in \{d, 3d, \ldots, (2\lceil \frac{m}{2d} \rceil - 1)d\}$, $b - a > \left(\frac{3}{2}l - 2\right) d$, and a $\frac{4d^2\delta}{m^2}$-dense distribution $H$ with respect to $D$, such that the closed approximation of $f$ with distance $d$ is balanced around $\{a, b\}$ and that $f$ is $\frac{1}{2}(1+\gamma)$-hard to approximate with accuracy $\alpha$ and distance $\epsilon$ on $H$ for circuits of size $\hat{s} = \frac{\gamma^2 d^2 s}{256 m^2 \log(2m^2/d^2\gamma\delta)}$.

Since $H$ has relative density $\hat{\delta} = \frac{4d^2\delta}{m^2}$, there exists a distribution $G$ over $\{0,1\}^n$, such that $D = \hat{\delta}H + (1-\hat{\delta})G$. For $t \in \mathbb{N}$, we have

$$D^t = \sum_{k=0}^{t} \binom{t}{k} \cdot \hat{\delta}^k (1-\hat{\delta})^{t-k} \cdot \Pi_t(H^k, G^{t-k}).$$

Therefore, for any large enough $s, t \in \mathbb{N}$, for any circuit of size $s' = \frac{\hat{s}}{2}$, by Lemma 5.4, we have

$$\begin{aligned}
\Pr_{x \leftarrow D^t}[C(x) = g(x)] &= \sum_{k=0}^{t} \binom{t}{k} \cdot \hat{\delta}^k (1-\hat{\delta})^{t-k} \cdot \Pr_{x \leftarrow \Pi_t(H^k, G^{t-k})}[C(x) = g(x)] \\
&< \sum_{k=0}^{\mu} \binom{t}{k} \cdot \hat{\delta}^k (1-\hat{\delta})^{t-k} + \frac{\binom{\mu}{\frac{\mu}{2}}}{2^\mu} \left( \frac{3\sqrt{\mu}}{l} + 3 + \frac{\mu}{2}\gamma \right) \\
&\leq e^{-\mu/4} + \frac{\binom{\mu}{\frac{\mu}{2}}}{2^\mu} \left( \frac{3\sqrt{\mu}}{l} + 3 + \frac{\mu}{2}\gamma \right),
\end{aligned}$$

where $\mu = \frac{t\hat{\delta}}{2} = \frac{2td^2\delta}{m^2}$. Let $l = \sqrt{\mu}$, we have

$$\sqrt{\mu} = \sqrt{\frac{2td^2\delta}{m^2}} = \sqrt{\frac{2t\epsilon^2\delta}{l^2m^2}} = \frac{\epsilon}{lm}\sqrt{2t\delta} = l$$

Then, $l = \sqrt{\frac{\epsilon}{m}\sqrt{2t\delta}}$.

$$\mu = \frac{\epsilon}{m}\sqrt{2t\delta}, s' = \frac{\gamma^2\epsilon}{256m\sqrt{2t\delta}\log(8tm^2/\epsilon^2\gamma^2\delta)} \cdot s.$$

□

## 5.1 Proof of Lemma 5.2

**Lemma 5.2.** *For $\delta \in (0,1)$, $m, \epsilon \in \mathbb{R}$, $\alpha, s \in \mathbb{N}$, $\alpha > \log(m/\epsilon)+4$ and a distribution $D$ over $\{0,1\}^n$, consider a real-valued function $f : \{0,1\}^n \to [0,m)$. For any $l \in \mathbb{N}$, let $d = \frac{\epsilon}{l}$, which denotes the radius of the partitioned intervals. For any $a, b \in \{d, 3d, \ldots, (2\lceil\frac{m}{2d}\rceil - 1)d\}, a \neq b$, define the relation $R_{a,b} \subseteq \{0,1\}^n \times \{0,1\}^\alpha$ as follows:*

- *If $f(x) \in [a \pm d)$ or $f(x) \in [b \pm d)$, then $(x,y) \in R_{a,b}$ if and only if $y \in (f(x) \pm \epsilon)$;*
- *If $f(x) \notin [a \pm d)$ and $f(x) \notin [b \pm d)$, then $(x,y) \in R_{a,b}$ for any $y \in \{0,1\}^\alpha$.*

*For any integer $l > 1$, for large enough $s$, if $f$ is $(1-\delta)$-hard to approximate on $D$ with accuracy $\alpha$ and distance $\epsilon$ for circuits of size $s$, there exist $a, b \in \{d, 3d, \ldots, (2\lceil\frac{m}{2d}\rceil - 1)d\}$, $b - a > (\frac{3}{2}l - 2)d$, such that $R_{a,b}$ is $(1 - \frac{4d^2\delta}{m^2})$-hard on $D$, for circuits of size $\frac{d^2s}{m^2}$.*

*Proof.* Suppose that for any $a, b \in \{d, 3d, \ldots, (2\lceil\frac{m}{2d}\rceil - 1)d\}$, $a < b$, there is a circuit $C_{a,b} : \{0,1\}^n \to \{0,1\}^\alpha$ of size $\frac{d^2s}{m^2}$, such that

$$\Pr_{x \leftarrow D}[C_{a,b}(x) \in R_{a,b}(x)] \geq 1 - \frac{4d^2\delta}{m^2}.$$

For simplicity, let $C_{b,a} = C_{a,b}$. Taking a combination of circuits $C_{a,b}$, construct a new circuit $C : \{0,1\}^n \to \{0,1\}^\alpha$ as follows:

- On input $x$, for any $i \in \{d, 3d, \ldots, (2\lceil\frac{m}{2d}\rceil - 1)d\}$ in ascending order:
  - Compute $C_{i,j}(x)$;
  - if $C_{i,j}(x)$ outputs a value in $(i \pm (\epsilon + d))$ for every $j \neq i$, return $\max_{j \neq i}(C_{i,j}(x))$, which is the maximum value among all the outputs given by $C_{i,j}(x)$.
- Return $\perp$ if no such $i$ exists.

If $s$ is large enough, specifically $s \gg \left(\frac{m}{d}\right)^2 \cdot \alpha$, the size of $C$ is approximately $\binom{\lceil\frac{m}{2d}\rceil}{2} \cdot \frac{d^2s}{m^2} \leq s$. The performance of the circuit $C$ is stated as follows.

**Claim 5.5.** *For any $x \in \{0,1\}^n$, if $C_{a,b}(x) \in R_{a,b}(x)$ for any distinct $a, b \in \{d, 3d, \ldots, (2\lceil\frac{m}{2d}\rceil - 1)d\}$, $C(x) \in (f(x) \pm \epsilon)$.*

By Claim 5.5, we have

$$\Pr_{x \leftarrow D}[C(x) \in (f(x) \pm \epsilon)] \geq \Pr_{x \leftarrow D}[\forall (a,b), a < b : C_{a,b}(x) \in R_{a,b}(x)] \geq 1 - \binom{\lceil \frac{m}{2d} \rceil}{2} \cdot \frac{4d^2\delta}{m^2} \geq 1 - \delta.$$

The second inequality is obtained by taking the union bound. It contradicts the fact that $f$ is $(1-\delta)$-hard to approximate with accuracy $\alpha$ and distance $\epsilon$.

In the following, we will prove that the relation $R_{a,b}$ $(a < b)$ is potentially hard only if $b - a > (\frac{3}{2}l - 2)d$. Assume the distance of two centers $b - a \leq (\frac{3}{2}l - 2)d$, construct a circuit $C_{a,b}$ which outputs a value in $(b - (\epsilon - d), a + (\epsilon - d))$, regardless of inputs. Since the interval length is

$$a - b + 2(\epsilon - d) \geq -\left(\frac{3}{2}l - 2\right)d + 2(\epsilon - d) \geq \frac{\epsilon}{2},$$

there exists a value in this interval that can be encoded in $\{0,1\}^\alpha$.

For any input $x$,

- If $f(x) \in [a \pm d)$, $f(x) - \epsilon < a + d - \epsilon < b - (\epsilon - d) < a + (\epsilon - d) < f(x) + \epsilon$
- If $f(x) \in [b \pm d)$, $f(x) - \epsilon < b - (\epsilon - d) < a + (\epsilon - d) < b - d + \epsilon \leq f(x) + \epsilon$.
- Otherwise, any output is in $R_{a,b}(x)$.

Then, the output is guaranteed to have $C_{a,b}(x) \in R_{a,b}(x)$.

Therefore, there exist $a, b \in \{d, 3d, \ldots, (2\lceil \frac{m}{2d} \rceil - 1)d\}$, $b - a > \left(\frac{3}{2}l - 2\right)d$, such that $R_{a,b}$ is $(1 - \frac{4d^2\delta}{m^2})$-hard for circuits of size $\frac{d^2 s}{m^2}$. □

### 5.1.1 Proof of Claim 5.5

**Claim 5.5.** *For any $x \in \{0,1\}^n$, if $C_{a,b}(x) \in R_{a,b}(x)$ for any distinct $a, b \in \{d, 3d, \ldots, (2\lceil \frac{m}{2d} \rceil - 1)d\}$, $C(x) \in (f(x) \pm \epsilon)$.*

*Proof.* We partition the output space into multiple intervals with length $2d$ and define a set relation $R_{a,b}$. For each relation, we focus on the inputs whose outputs by $f$ lie in the corresponding intervals $[a \pm d)$ or $[b \pm d)$. Recall the process of algorithm $C$: for $i \in \{d, 3d, \ldots, (2\lceil \frac{m}{2d} \rceil - 1)d\}$ in ascending order, if for every $j \neq i$, $C_{i,j}(x) \in (i \pm (\epsilon + d))$ holds, then $C$ stops and outputs $\max_{j \neq i}(C_{i,j}(x))$.

Suppose that the algorithm returns when $i = \hat{i}$, then $f(x) \geq \hat{i} - d$. If $f(x) < \hat{i} - d$, there exists $\tilde{i} < \hat{i}$, such that $f(x) \in [\tilde{i} \pm d)$, since we assume the correctness of every $C_{a,b}$, then $C$ should stop when $i = \tilde{i}$, which results in a contradiction.

If $f(x) \in \left[\hat{i} \pm d\right)$, $C_{i,j}(x) \in (f(x) \pm \epsilon)$ for every $j \neq i$, then $C(x) \in (f(x) \pm \epsilon)$.

If $f(x) \geq \hat{i} + d$, suppose $\tilde{i} > \hat{i}$ and $f(x) \in [\tilde{i} \pm d)$, then $C_{\hat{i},\tilde{i}}(x) \in (f(x) \pm \epsilon)$.

$$f(x) - \epsilon < C_{\hat{i},\tilde{i}}(x) \leq C(x) < \hat{i} + d + \epsilon \leq f(x) + \epsilon.$$

□

## 5.2 Proof of Lemma 5.4

**Lemma 5.4.** *For $\gamma \in (0,1)$, $m, \epsilon \in \mathbb{R}$ and $\alpha, s, t \in \mathbb{N}$, $\alpha > \log(m/\epsilon) + 4$, for large enough $l \in \mathbb{N}$, let $d = \frac{\epsilon}{l}$, consider a hardcore distribution $H \subseteq \{0,1\}^n$ and $a, b \in \left\{d, 3d, \ldots, (2\lceil \frac{m}{2d} \rceil - 1)d\right\}$, $b - a > \left(\frac{3}{2}l - 2\right)d$, on which the closed approximation of function $f : \{0,1\}^n \to [0, m)$ with distance*

*$d$ is balanced around $\{a, b\}$ and $f$ is $\frac{1}{2}(1+\gamma)$-hard to approximate with accuracy $\alpha$ and distance $\epsilon$ for circuits of size $s$. For any integer $t$, define a function $g : (\{0,1\}^n)^t \to [0, t\cdot m)$ as follows:*

$$g(x_1, \ldots, x_t) = \sum_{i=1}^{t} f(x_i).$$

*For $k \in \mathbb{N}, 0 < k \leq t$ and any other distribution $G$ over $(\{0,1\}^n)^{t-k}$, for any large enough $s$, function $g$ is $\eta$-hard to approximate with accuracy $\alpha'$ and distance $\epsilon$ on $\Pi_t(H^k, G)$ for circuits of size $\frac{s}{2}$, where $\alpha' > \log(t \cdot m/\epsilon) + 4$ and*

$$\eta = \frac{\binom{k}{\frac{k}{2}}}{2^k}\left(\frac{3\sqrt{k}}{l} + 3 + \frac{k}{2}\gamma\right).$$

*Proof.* For an integer $l$, let $d = \frac{\epsilon}{l}$, consider a hardcore distribution $H \subseteq \{0,1\}^n$ and $a, b \in \left\{d, 3d, \ldots, (2\lceil \frac{m}{2d} \rceil - 1)d\right\}$, $b - a > \left(\frac{3}{2}l - 2\right)d$, such that, the closed approximation of function $f : \{0,1\}^n \to [0, m)$ with distance $d$ is balanced around $\{a, b\}$ on $H$. Denote distribution $x \leftarrow H|_{f(x)\in(a\pm d)}$ by $H_a$ and distribution $x \leftarrow H|_{f(x)\in(b\pm d)}$ by $H_b$. Since $f$ is balanced around $\{a, b\}$ on distribution $H$, $H = \frac{1}{2}H_a + \frac{1}{2}H_b$. The hardness of approximating function $f$ implies the indistinguishability of this two distribution $H_a$ and $H_b$.

For $t \in \mathbb{N}$, let $H_i^t = \Pi_t(H_a^i, H_b^{t-i})$. Then, consider any fixed $\hat{x} = (\hat{x}_1, \ldots, \hat{x}_{t-k}) \in (\{0,1\}^n)^{t-k}$ and any permutation $\pi$ of $t$ coordinates, we have the following fact.

**Claim 5.6.** *For $s, \alpha' \in \mathbb{N}$, such that $s \gg \alpha'$ and $(t\cdot m, \alpha', \epsilon)$ is valid, for any circuit $C : (\{0,1\}^n)^t \to \{0,1\}^{\alpha'}$ of size at most $\frac{s}{2}$, for any $i, j \in \mathbb{N}_{k+1}$, such that $|i - j| = 1$ and any $v, \epsilon' \in [0, t\cdot m), \epsilon' \geq \epsilon$, we have*

$$\Pr_{\substack{\bar{x}\leftarrow H^k \\ \bar{x}'\leftarrow\pi(\bar{x},\hat{x})}}\left[C(\bar{x}') \in (g_t(\bar{x}') + v \pm \epsilon') \,\middle|\, \bar{x} \in H_j^t\right] - \Pr_{\substack{\bar{x}\leftarrow H^k \\ \bar{x}'\leftarrow\pi(\bar{x},\hat{x})}}\left[C(\bar{x}') \in (g_t(\bar{x}') + v + v' \pm (\epsilon' + 2d)) \,\middle|\, \bar{x} \in H_i^t\right] < \gamma$$

*where $v' = (j - i)(a - b)$.*

Let $\Delta = \sum_{i=1}^{t-k} f(\hat{x}_i)$. For any large even $t$, for any circuit $C : (\{0,1\}^n)^t \to \{0,1\}^{\alpha'}$ of size at most $\frac{s}{2}$, the following holds,

$$
\begin{aligned}
&\Pr_{\substack{\bar{x}\leftarrow H^k\\ \bar{x}'\leftarrow\pi(\bar{x},\hat{x})}}\left[C(\bar{x}')\in(g_t(\bar{x}')\pm\epsilon)\right]\\
=&\sum_{i=0}^{k}\Pr_{\substack{\bar{x}\leftarrow H^k\\ \bar{x}'\leftarrow\pi(\bar{x},\hat{x})}}\left[\bar{x}\in H_i^k\right]\cdot\Pr_{\substack{\bar{x}\leftarrow H^k\\ \bar{x}'\leftarrow\pi(\bar{x},\hat{x})}}\left[C(\bar{x}')\in(g_t(\bar{x}')\pm\epsilon)\,\middle|\,\bar{x}\in H_i^k\right]\\
=&\frac{1}{2^k}\sum_{i=0}^{k}\binom{k}{i}\Pr_{\substack{\bar{x}\leftarrow H^k\\ \bar{x}'\leftarrow\pi(\bar{x},\hat{x})}}\left[C(\bar{x}')\in(g_k(\bar{x})+\Delta\pm\epsilon)\,\middle|\,\bar{x}\in H_i^k\right]\\
=&\frac{1}{2^k}\sum_{i=-\frac{k}{2}}^{\frac{k}{2}}\binom{k}{\frac{k}{2}+i}\Pr_{\substack{\bar{x}\leftarrow H^k\\ \bar{x}'\leftarrow\pi(\bar{x},\hat{x})}}\left[C(\bar{x}')\in(g_k(\bar{x})+\Delta\pm\epsilon)\,\middle|\,\bar{x}\in H_{\frac{k}{2}+i}^k\right]\\
<&\frac{1}{2^k}\sum_{i=-\frac{k}{2}}^{\frac{k}{2}}\binom{k}{\frac{k}{2}+i}\left(\Pr_{\substack{\bar{x}\leftarrow H^k\\ \bar{x}'\leftarrow\pi(\bar{x},\hat{x})}}\left[C(\bar{x}')\in(g_k(\bar{x})+i(a-b)+\Delta\pm(\epsilon+2d\,|i|))\,\middle|\,\bar{x}\in H_{\frac{k}{2}}^k\right]+\gamma\cdot|i|\right) \quad (8)\\
\le&\frac{\binom{k}{\frac{k}{2}}}{2^k}\left(\frac{3\sqrt{k}}{l}+3+\frac{k}{2}\gamma\right).
\end{aligned}
$$

The inequality (8) is obtained by using Claim 5.6, we use the probability with a same condition $\bar{x}\in H_{\frac{k}{2}}^k$ to give an upper bound for the original term. The last inequility holds by combining Claim 4.6 and Claim 5.7.

Therefore, for any distribution $G$ over $(\{0,1\}^n)^{t-k}$, we have

$$
\Pr_{\bar{x}\leftarrow\Pi_t(H^k,G)}[C(\bar{x})\in(g_t(\bar{x})\pm\epsilon)]\le\frac{\binom{k}{\frac{k}{2}}}{2^k}\left(\frac{3\sqrt{k}}{l}+3+\frac{k}{2}\gamma\right).
$$

□

**Claim 5.7.** *For large enough $l\in\mathbb{N}$, for any circuit $C$, we have*

$$
\sum_{i=-\frac{k}{2}}^{\frac{k}{2}}\binom{k}{\frac{k}{2}+i}\Pr_{\substack{\bar{x}\leftarrow H^k\\ \bar{x}'\leftarrow\pi(\bar{x},\hat{x})}}\left[C(\bar{x}')\in(g_k(\bar{x})+i(a-b)+\Delta\pm(\epsilon+2d\,|i|))\,\middle|\,\bar{x}\in H_{\frac{k}{2}}^k\right]\le\binom{k}{\frac{k}{2}}\left(\frac{3\sqrt{k}}{l}+3\right),
$$

*where $b-a>\left(\frac{3}{2}l-2\right)d$ and $\epsilon=l\cdot d$.*

*Proof.* Recall that $\epsilon$ denotes the tolerance of the approximation error, and for some integer $l\in\mathbb{N}$, we let $d=\frac{\epsilon}{l}$. Since $a,b$ are the multiples of $d$, let $b-a=l_1\cdot d$, for some positive integer $l_1$. By our assumption, $b-a>\left(\frac{3}{2}l-2\right)d$, thus $l_1>\frac{3}{2}l-2$.

For simplicity, for any integer $i_1,i_2$, let

$$
P(i_1,i_2)=\Pr_{\substack{\bar{x}\leftarrow H^k\\ \bar{x}'\leftarrow\pi(\bar{x},\hat{x})}}\left[C(\bar{x}')\in[g_k(\bar{x})+\Delta+i_1d,g_k(\bar{x})+\Delta+i_2d)\,\middle|\,\bar{x}\in H_{\frac{k}{2}}^k\right].
$$

It is clear that $P(i_1, i_2) + P(i_2, i_3) = P(i_1, i_3)$ for $i_1 < i_2 < i_3$. Note that $\binom{k}{\frac{k}{2}+i} = \binom{k}{\frac{k}{2}-i}$, the left hand side can be upper bounded by

$$\sum_{i=-\frac{k}{2}}^{\frac{k}{2}} \binom{k}{\frac{k}{2}+i} \cdot P(i \cdot l_1 - l - 2\,|i|\,, i \cdot l_1 + l + 2\,|i|).$$

Then, we will try to reorder the sum by taking the property of probability:

$$\begin{aligned} &\sum_{i=-\frac{k}{2}}^{\frac{k}{2}} \binom{k}{\frac{k}{2}+i} \cdot P(i \cdot l_1 - l - 2\,|i|\,, i \cdot l_1 + l + 2\,|i|) \\ =&\sum_{i=-\frac{k}{2}}^{\frac{k}{2}} \binom{k}{\frac{k}{2}+i} \sum_{j=i \cdot l_1 - l - 2|i|}^{i \cdot l_1 + l + 2|i| - 1} P(j, j+1). \end{aligned}$$

To calculate the above, we collect the sum of coefficients corresponding to each $P(j, j+1)$. For each $j$, the term should be

$$\sum_{i=i_f(j)}^{i_c(j)} \binom{k}{\frac{k}{2}+i} P(j, j+1), \tag{9}$$

for some functions $i_f, i_c$. Let $S(j) = \sum_{i=i_f(j)}^{i_c(j)} \binom{k}{\frac{k}{2}+i}$ denote the coefficient of $P(j, j+1)$. Since the summation of all possible $P(j, j+1)$ is at most 1, by the definition of probability, it is feasible to give an upper bound for the entire summation by computing the upper bound for $S(j)$.

For any $i \in [i_f(j), i_c(j)]$, $i$ should satisfy the following:

$$i \cdot l_1 - l - 2\,|i| \le j \le i \cdot l_1 + l + 2\,|i| - 1 \text{ and } -\frac{k}{2} \le i \le \frac{k}{2}.$$

We prove $S(j) = S(-j-1)$ by showing the following. For any $i \in [i_f(j), i_c(j)]$,

$$i \cdot l_1 - l - 2\,|i| \le j \le i \cdot l_1 + l + 2\,|i| - 1 \Leftrightarrow -i \cdot l_1 - l - 2\,|i| \le -j - 1 \le -i \cdot l_1 + l + 2\,|i| - 1.$$

Then, $-i \in [i_f(-j-1), i_c(-j-1)]$, since $\binom{k}{\frac{k}{2}+i} = \binom{k}{\frac{k}{2}-i}$, $S(j) = S(-j-1)$.

Recall that $l_1 > \frac{3}{2}l - 2$, assume $l > 6$, $l_1 - l > 1$. When $j \ge 0$, we necessarily have $i \cdot l_1 + l + 2\,|i| \ge 1$. If there exists a negative $i$ satisfies the inequality, then $i(l_1 - 2) + l \le -(l_1 - 2) + l < 1$, which leads to a contradiction. Therefore,

$$i \cdot l_1 - l - 2i \le j \le i \cdot l_1 + l + 2i - 1,$$

which is equivalent to

$$i_f(j) = \lceil \frac{j - l + 1}{l_1 + 2} \rceil \le i \le \lfloor \frac{j + l}{l_1 - 2} \rfloor = i_c(j).$$

Therefore, we can give an upper bound for $S(j)$,

$$\begin{aligned}
S(j) &= \sum_{i=i_f(j)}^{i_c(j)} \binom{k}{\frac{k}{2}+i} \\
&\le \left(\frac{j+l}{l_1-2} - \frac{j-l+1}{l_1+2} + 1\right)\binom{k}{\frac{k}{2}+i_f(j)} \\
&= \left(\frac{4j+2l\cdot l_1-(l_1-2)}{(l_1-2)(l_1+2)} + 1\right)\binom{k}{\frac{k}{2}+i_f(j)} \\
&\le \left(\frac{4j}{(l_1-2)(l_1+2)} + 3\right)\binom{k}{\frac{k}{2}+i_f(j)}.
\end{aligned}$$

On the other hand, $j$ can be upper bounded in terms of $i_f(j)$, that is

$$\frac{j-l+1}{l_1+2} < i_f(j)+1 \Rightarrow j < (i_f(j)+1)(l_1+2)+l-1 < (i_f(j)+2)(l_1+2).$$

Then, we plug in $i_f(j)$,

$$S(j) \le \left(\frac{4j}{(l_1-2)(l_1+2)} + 3\right)\binom{k}{\frac{k}{2}+i_f(j)} < \left(\frac{4(i_f(j)+2)}{l_1-2} + 3\right)\binom{k}{\frac{k}{2}+i_f(j)}.$$

In the following, for $0 \le i \le \frac{k}{2}$, we denote

$$T(i) = \frac{i+2}{l_1-2}\binom{k}{\frac{k}{2}+i}. \tag{10}$$

It is clear that the maximum value of $S(j)$ is at most the maximum value of $4T(i) + 3\binom{k}{\frac{k}{2}}$, that is

$$\max_j S(j) = \max_{j\ge 0} S(j) \le 4\cdot \max_i T(i) + 3\binom{k}{\frac{k}{2}}.$$

The first equality holds because $S(j) = S(-j-1)$. To find the maximum value of $T(i)$, we compare each pairs of adjacent terms in the sequence.

$$\frac{T(i+1)}{T(i)} = \frac{(i+3)\binom{k}{\frac{k}{2}+i+1}}{(i+2)\binom{k}{\frac{k}{2}+i}} = \frac{(i+3)\left(\frac{k}{2}-i\right)}{(i+2)\left(\frac{k}{2}+i+1\right)}.$$

Then, $T(i+1) > T(i)$ if and only if $i < \frac{\sqrt{k+5}-3}{2}$. We have

$$\max_i T(i) < \frac{\lfloor\frac{\sqrt{k+5}-3}{2}\rfloor + 2}{l_1-2}\binom{k}{\frac{k}{2}}.$$

Therefore, for $k \ge 12$,

$$\max_j S(j) < 4\cdot\frac{\lfloor\frac{\sqrt{k+5}-3}{2}\rfloor + 2}{l_1-2}\binom{k}{\frac{k}{2}} + 3\binom{k}{\frac{k}{2}} < 3\left(\frac{\sqrt{k}}{l}+1\right)\binom{k}{\frac{k}{2}}.$$

□

### 5.2.1 Proof of Claim 5.6

**Claim 5.6.** *For $s, \alpha' \in \mathbb{N}$, such that $s \gg \alpha'$ and $(t\cdot m, \alpha', \epsilon)$ is valid, for any circuit $C : (\{0,1\}^n)^t \to \{0,1\}^{\alpha'}$ of size at most $\frac{s}{2}$, for any $i, j \in \mathbb{N}_{k+1}$, such that $|i-j| = 1$ and any $v, \epsilon' \in [0, t\cdot m), \epsilon' \geq \epsilon$, we have*

$$\Pr_{\substack{\bar{x}\leftarrow H^k\\ \bar{x}'\leftarrow\pi(\bar{x},\hat{x})}}\left[C(\bar{x}') \in (g_t(\bar{x}') + v \pm \epsilon')\,\middle|\,\bar{x} \in H_j^t\right] - \Pr_{\substack{\bar{x}\leftarrow H^k\\ \bar{x}'\leftarrow\pi(\bar{x},\hat{x})}}\left[C(\bar{x}') \in (g_t(\bar{x}') + v + v' \pm (\epsilon' + 2d))\,\middle|\,\bar{x} \in H_i^t\right] < \gamma$$

*where $v' = (j-i)(a-b)$.*

*Proof.* Without loss of generality, suppose $i \in \mathbb{N}_t$ and $j = i+1$. Suppose that there is a circuit $C$ of size at most $\frac{s}{2}$ and $v, \epsilon' \in [0, t\cdot m)$, $\epsilon' \geq \epsilon$, satisfying

$$\Pr_{\substack{\bar{x}\leftarrow H^k\\ \bar{x}'\leftarrow\pi(\bar{x},\hat{x})}}\left[C(\bar{x}') \in (g_t(\bar{x}') + v \pm \epsilon')\,\middle|\,\bar{x} \in H_j^t\right] - \Pr_{\substack{\bar{x}\leftarrow H^k\\ \bar{x}'\leftarrow\pi(\bar{x},\hat{x})}}\left[C(\bar{x}') \in (g_t(\bar{x}') + v + v' \pm (\epsilon' + 2d))\,\middle|\,\bar{x} \in H_i^t\right] \geq \gamma.$$

Then, there must exist a tuple $(x_1, \dots, x_{k-1})$ and a permutation $\pi_k$ of $k$ entries, such that,

$$\begin{aligned}&\Pr_{\substack{x\leftarrow H\\ \bar{x}\leftarrow\pi_k(x_1,\dots,x_{k-1},x)\\ \bar{x}'\leftarrow\pi(\bar{x},\hat{x})}}\left[C(\bar{x}') \in (g_t(\bar{x}') + v \pm \epsilon')\,|x \in H_a\right]\\ -&\Pr_{\substack{x\leftarrow H\\ \bar{x}\leftarrow\pi_k(x_1,\dots,x_{k-1},x)\\ \bar{x}'\leftarrow\pi(\bar{x},\hat{x})}}\left[C(\bar{x}') \in (g_t(\bar{x}') + v + v' \pm (\epsilon' + 2d))\,|x \in H_b\right] \geq \gamma.\end{aligned}$$

In fact, $g_t(\bar{x}') = f(x) + g_{k-1}(x_1, \dots, x_{t-1}) + g_{t-k}(\hat{x})$, let $\Delta = g(\bar{x}') - f(x)$, which is a fixed value independent of $x$. Recall that $\epsilon$ is the tolerance of approximation error and $d$ is the radius of the intervals around $a$ and $b$, while letting $d = \frac{\epsilon}{l}$ for some large enough integer $l$. Define a circuit $C' : \{0,1\}^n \to \{0,1\}^\alpha$ as follows:

1. Input: $x \in \{0,1\}^n$.
2. Compute $y \leftarrow C(\pi(x, \hat{x}))$.
3. If $y \in [a + \Delta + v \pm (\epsilon' + d))$, output a value in $(a \pm \frac{\epsilon}{4})$.
4. Otherwise, output a value in $(b \pm \frac{\epsilon}{4})$.

If $s$ is large enough, the size of $C'$ is less than $s$. In the following, we will show that the circuit $C'$ can approximate function $f$ with a good probability, then result in a contradiction.

For any $x \in H_a$, which means $f(x) \in [a \pm d)$, if $C(\bar{x}')$ output a value $y$ in $(g_t(\bar{x}') + v \pm \epsilon')$ which is equivalent to $(f(x) + \Delta + v \pm \epsilon')$, we necessarily have $y \in [a + \Delta + v \pm (\epsilon' + d))$. For any value $z \in \left(a \pm \frac{\epsilon}{4}\right)$, $|f(x) - z| \leq \frac{\epsilon}{4} + d \leq \epsilon$, then

$$\Pr_{x\leftarrow H}[C'(x) \in (f(x) \pm \epsilon)\,|x \in H_a] \geq \Pr_{\substack{x\leftarrow H\\ \bar{x}\leftarrow\pi_k(x_1,\dots,x_{k-1},x)\\ \bar{x}'\leftarrow\pi(\bar{x},\hat{x})}}\left[C(\bar{x}') \in (g_t(\bar{x}') + v \pm \epsilon')\,|x \in H_a\right].$$

On the other hand, for any $x \in H_b$, $f(x) \in [b \pm d)$, if $C(\bar{x}')$ output a value $y$, such that $y \notin (g_t(\bar{x}') + v + v' \pm (\epsilon' + 2d))$, which is equivalent to $(f(x) + \Delta + v + (a-b) \pm (\epsilon' + 2d))$. The interval above covers the interval $[a + \Delta + v \pm (\epsilon' + d))$, since

$$\begin{aligned}a + \Delta + v + \epsilon' + d &\leq f(x) + \Delta + v + (a-b) + \epsilon' + 2d\\ a + \Delta + v - \epsilon' - d &> f(x) + \Delta + v + (a-b) - \epsilon' - 2d\end{aligned}$$

The circuit $C'$ will output a value in $\left(b \pm \frac{\epsilon}{4}\right)$, then

$$\Pr_{x \leftarrow H}[C'(x) \in (f(x) \pm \epsilon) \,| x \in H_b] \geq \Pr_{\substack{x \leftarrow H \\ \bar{x} \leftarrow \pi_k(x_1, \ldots, x_{k-1}, x) \\ \bar{x}' \leftarrow \pi(\bar{x}, \hat{x})}} \left[C(\bar{x}') \notin (g_t(\bar{x}') + v + v' \pm (\epsilon' + 2d)) \,| x \in H_b\right].$$

Therefore, the probability that $C'$ can successfully approximate function $f$ on $H$ is

$$\begin{aligned}
&\Pr_{x \leftarrow H}[C'(x) \in (f(x) \pm \epsilon)] \\
&= \frac{1}{2} \Pr_{x \leftarrow H}[C'(x) \in (f(x) \pm \epsilon) | x \in H_a] + \frac{1}{2} \Pr_{x \leftarrow H}[C'(x) \in (f(x) \pm \epsilon) | x \in H_b] \\
&\geq \frac{1}{2} \Pr_{\substack{x \leftarrow H \\ \bar{x} \leftarrow \pi_k(x_1, \ldots, x_{k-1}, x) \\ \bar{x}' \leftarrow \pi(\bar{x}, \hat{x})}} \left[C(\bar{x}') \in (g_t(\bar{x}') + v \pm \epsilon') \,| x \in H_a\right] \\
&+ \frac{1}{2} \Pr_{\substack{x \leftarrow H \\ \bar{x} \leftarrow \pi_k(x_1, \ldots, x_{k-1}, x) \\ \bar{x}' \leftarrow \pi(\bar{x}, \hat{x})}} \left[C(\bar{x}') \notin (g_t(\bar{x}') + v + v' \pm (\epsilon' + 2d)) \,| x \in H_b\right]. \\
&\geq \frac{1}{2}(1 + \gamma),
\end{aligned}$$

which contradict to $f$ is $\frac{1}{2}(1 + \gamma)$-hard on $H$. □

# References

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

[AGGS22] Vahid R. Asadi, Alexander Golovnev, Tom Gur, and Igor Shinkar. Worst-case to average-case reductions via additive combinatorics. In Stefano Leonardi and Anupam Gupta, editors, *STOC '22: 54th Annual ACM SIGACT Symposium on Theory of Computing, Rome, Italy, June 20 - 24, 2022*, pages 1566–1574. ACM, 2022.

[ASS+24] Shweta Agrawal, Sagnik Saha, Nikolaj I. Schwartzbach, Akhil Vanukuri, and Prashant Nalini Vasudevan. k-sum in the sparse regime: Complexity and applications. In Leonid Reyzin and Douglas Stebila, editors, *Advances in Cryptology - CRYPTO 2024 - 44th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2024, Proceedings, Part II*, volume 14921 of *Lecture Notes in Computer Science*, pages 315–351. Springer, 2024.

[BBB19] Enric Boix-Adserà, Matthew S. Brennan, and Guy Bresler. The average-case complexity of counting cliques in erdős-rényi hypergraphs. In David Zuckerman, editor, *60th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2019, Baltimore, Maryland, USA, November 9-12, 2019*, pages 1256–1280. IEEE Computer Society, 2019.

[BHK09] Boaz Barak, Moritz Hardt, and Satyen Kale. The uniform hardcore lemma via approximate bregman projections. In Claire Mathieu, editor, *Proceedings of the Twentieth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2009, New York, NY, USA, January 4-6, 2009*, pages 1193–1200. SIAM, 2009.

[BRSV17] Marshall Ball, Alon Rosen, Manuel Sabin, and Prashant Nalini Vasudevan. Average-case fine-grained hardness. In Hamed Hatami, Pierre McKenzie, and Valerie King, editors, *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2017, Montreal, QC, Canada, June 19-23, 2017*, pages 483–496. ACM, 2017.

[BT06] Andrej Bogdanov and Luca Trevisan. On worst-case to average-case reductions for NP problems. *SIAM J. Comput.*, 36(4):1119–1159, 2006.

[CPS99] Jin-yi Cai, Aduri Pavan, and D. Sivakumar. On the hardness of permanent. In Christoph Meinel and Sophie Tison, editors, *STACS 99, 16th Annual Symposium on Theoretical Aspects of Computer Science, Trier, Germany, March 4-6, 1999, Proceedings*, volume 1563 of *Lecture Notes in Computer Science*, pages 90–99. Springer, 1999.

[Gei22] Nathan Geier. A tight computational indistinguishability bound for product distributions. In Eike Kiltz and Vinod Vaikuntanathan, editors, *Theory of Cryptography - 20th International Conference, TCC 2022, Chicago, IL, USA, November 7-10, 2022, Proceedings, Part II*, volume 13748 of *Lecture Notes in Computer Science*, pages 333–347. Springer, 2022.

[GG11] Parikshit Gopalan and Venkatesan Guruswami. Hardness amplification within NP against deterministic algorithms. *J. Comput. Syst. Sci.*, 77(1):107–121, 2011.

[GIL$^+$90] Oded Goldreich, Russell Impagliazzo, Leonid A. Levin, Ramarathnam Venkatesan, and David Zuckerman. Security preserving amplification of hardness. In *31st Annual Symposium on Foundations of Computer Science, St. Louis, Missouri, USA, October 22-24, 1990, Volume I*, pages 318–326. IEEE Computer Society, 1990.

[GK20] Elazar Goldenberg and Karthik C. S. Hardness amplification of optimization problems. In Thomas Vidick, editor, *11th Innovations in Theoretical Computer Science Conference, ITCS 2020, January 12-14, 2020, Seattle, Washington, USA*, volume 151 of *LIPIcs*, pages 1:1–1:13. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020.

[GNW11] Oded Goldreich, Noam Nisan, and Avi Wigderson. On yao's xor-lemma. In Oded Goldreich, editor, *Studies in Complexity and Cryptography. Miscellanea on the Interplay between Randomness and Computation - In Collaboration with Lidor Avigad, Mihir Bellare, Zvika Brakerski, Shafi Goldwasser, Shai Halevi, Tali Kaufman, Leonid Levin, Noam Nisan, Dana Ron, Madhu Sudan, Luca Trevisan, Salil Vadhan, Avi Wigderson, David Zuckerman*, volume 6650 of *Lecture Notes in Computer Science*, pages 273–301. Springer, 2011.

[GR18] Oded Goldreich and Guy N. Rothblum. Counting t-cliques: Worst-case to average-case reductions and direct interactive proof systems. In Mikkel Thorup, editor, *59th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2018, Paris, France, October 7-9, 2018*, pages 77–88. IEEE Computer Society, 2018.

[GV99] Oded Goldreich and Salil P. Vadhan. Comparing entropies in statistical zero knowledge with applications to the structure of SZK. In *Proceedings of the 14th Annual IEEE Conference on Computational Complexity, Atlanta, Georgia, USA, May 4-6, 1999*, page 54. IEEE Computer Society, 1999.

[HS23] Shuichi Hirahara and Nobutaka Shimizu. Hardness self-amplification: Simplified, optimized, and unified. In Barna Saha and Rocco A. Servedio, editors, *Proceedings of the 55th Annual ACM Symposium on Theory of Computing, STOC 2023, Orlando, FL, USA, June 20-23, 2023*, pages 70–83. ACM, 2023.

[HVV06] Alexander Healy, Salil P. Vadhan, and Emanuele Viola. Using nondeterminism to amplify hardness. *SIAM J. Comput.*, 35(4):903–931, 2006.

[Imp95] Russell Impagliazzo. Hard-core distributions for somewhat hard problems. In *36th Annual Symposium on Foundations of Computer Science, Milwaukee, Wisconsin, USA, 23-25 October 1995*, pages 538–545. IEEE Computer Society, 1995.

[Kal07] Satyen Kale. Boosting and hard-core set constructions: a simplified approach. *Electron. Colloquium Comput. Complex.*, TR07-131, 2007.

[KS03] Adam R. Klivans and Rocco A. Servedio. Boosting and hard-core set construction. *Mach. Learn.*, 51(3):217–238, 2003.

[Lip89] Richard J. Lipton. New directions in testing. In Joan Feigenbaum and Michael Merritt, editors, *Distributed Computing And Cryptography, Proceedings of a DIMACS Workshop, Princeton, New Jersey, USA, October 4-6, 1989*, volume 2 of *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, pages 191–202. DIMACS/AMS, 1989.

[O'D04] Ryan O'Donnell. Hardness amplification within np. *J. Comput. Syst. Sci.*, 69(1):68–94, 2004.

[SV03] Amit Sahai and Salil P. Vadhan. A complete problem for statistical zero knowledge. *J. ACM*, 50(2):196–249, 2003.

[Tre05] Luca Trevisan. On uniform amplification of hardness in NP. In Harold N. Gabow and Ronald Fagin, editors, *Proceedings of the 37th Annual ACM Symposium on Theory of Computing, Baltimore, MD, USA, May 22-24, 2005*, pages 31–38. ACM, 2005.

[TV07] Luca Trevisan and Salil P. Vadhan. Pseudorandomness and average-case complexity via uniform reductions. *Comput. Complex.*, 16(4):331–364, 2007.

[Vad99] Salil Pravin Vadhan. *A Study of Statistical Zero-Knowledge Proofs*. PhD thesis, Harvard University, USA, 1999. AAI0801528.

[Yao82] Andrew Chi-Chih Yao. Theory and applications of trapdoor functions (extended abstract). In *23rd Annual Symposium on Foundations of Computer Science, Chicago, Illinois, USA, 3-5 November 1982*, pages 80–91. IEEE Computer Society, 1982.

# A Corollaries

Our motivation for investigating this in the context of general evaluation or approximation problem arises from the average-case hardness of $\mathsf{SZK}$. The complexity class $\mathsf{SZK}$ consists of problems which have statistical zero-knowledge proofs, for which *Entropy Difference* ($\mathsf{ED}$) is a known complete problem [GV99].

**Definition A.1** (Entropy Difference)**.** The promise problem *Entropy Difference* $\mathsf{ED}$ is defined as,

$$\mathsf{ED}_Y = \{(C_0, C_1) : H(C_0) \geq H(C_1) + 1\},$$
$$\mathsf{ED}_N = \{(C_0, C_1) : H(C_0) \leq H(C_1) - 1\},$$

where $C_0, C_1$ are circuits with output length $n$. $H(C)$ denotes the Shannon entropy of the distribution encoded by circuit $C$ – that is the distribution of its outputs when its input is sampled uniformly at random.

Following our approach for hardness amplification and assuming the average-case hardness of $\mathsf{SZK}$, we derive the conclusion that the estimation of Shannon entropy for distributions exhibits strong average-case hardness. The corollary can be formulated as follows. We will use the terms *efficient* or *polynomial-time* alternatively.

**Corollary A.1.** *If there is a promise problem $\Pi \in \mathsf{SZK}$ that is somewhat hard on average, then there exists an efficiently sampleable distribution, on which estimating Shannon entropy is extremely hard on average. In particular, for $\delta : \mathbb{N} \to (0,1)$ and a constant $c \in \mathbb{N}$, if there is an efficient sampler $S$ that on input $1^n$ outputs a circuit $C$ with output length $n$ and $k \in (0, n)$, such that it is $(1 - \delta(n))$-hard to decide $\mathsf{ED}$ on $S$ in polynomial time, then there exists an efficient sampler $S'$ that on input $1^m$ outputs a circuit with output length $m$, on which estimating Shannon entropy is infinitely-often $10 \cdot \left(m^{\frac{c-2}{c+1}} \delta'(m)/8\right)^{-1/4}$-hard in polynomial time, where $\delta'(m) = \delta\left(m^{1/(c+1)}\right)$.*

*Proof Sketch.* Assume there is an $\mathsf{ED}$ instance sampler $S$, such that, for any polynomial-time algorithm $A$,

$$\Pr_{(C_0,C_1) \leftarrow S(1^n)} [A(C_0, C_1) = \mathsf{ED}(C_0, C_1)] < 1 - \delta(n).$$

Then, the estimating of Shannon entropy with distance $\frac{1}{2}$ is $(1 - \frac{\delta(n)}{2})$-hard, that is, for any polynomial-time algorithm $A'$,

$$\Pr_{\substack{(C_0,C_1) \leftarrow S(1^n) \\ b \leftarrow \{0,1\}}} \left[A'(C_b) \in \left(H(C_b) \pm \frac{1}{2}\right)\right] < 1 - \frac{\delta(n)}{2}.$$

We construct an infinitely-often sampler $S'$ as follows: on input parameter $m = n^{c+1}$, sample $(C_{i,0}, C_{i,1}) \leftarrow S(1^n)$ and $(b_1, \ldots, b_{n^c})$ for $(i = 1, \ldots, n^c)$, and outputs $(C_{1,b_1}, \ldots, C_{n^c,b_{n^c}})$. The output length of resulting circuit is $n^{c+1}$. By Theorem 1.2, the approximation on $S'$ with circuit output length $n^{c+1}$ is $10 \cdot \left(n^{c-2}\delta(n)/8\right)^{-1/4}$-hard for polynomial-time algorithms, where $t(n) = n^c$. As $m = n^{c+1}$, Shannon entropy is $10 \cdot \left(m^{\frac{c-2}{c+1}} \delta'(m)/8\right)^{-1/4}$-hard to approximate on $S'$ with distance $\frac{1}{2}$ for polynomial-time algorithm, where $m$ is the output length of the circuit generated by the sampler and $\delta'(m) = \delta\left(m^{1/(c+1)}\right)$. □

Additionally, our result implies the hardness amplification for multiplicatively approximating the problems in $\#\mathsf{P}$ with closure property under multiplication.

**Definition A.2** (Closure under multiplication)**.** For a counting problem $\Pi \in \#\mathsf{P}$, $\Pi$ is called closed under multiplication, if there is an efficient algorithm $\mathsf{Comb}$ such that, taking problem instances $(x_1, x_2, \ldots)$ as input, outputs an instance $x$ satisfying $|x| = |x_1| + |x_2| + \cdots$ and $\Pi(x) = \Pi(x_1) \cdot \Pi(x_2) \cdot \cdots$, where we use $|\cdot|$ to denote the complexity parameter of an instance.

The closure property under multiplication requires an efficient way for combining the instances such that the characteristics of the combined instance can be computed as the product of its components' characteristics. For example, the #SAT problem, a complete problem for #P, is closed under multiplication, where the complexity is parameterized in terms of the number of variables or clauses.

Since our hardness amplification method relies on addition, we take the logarithm of the counting value. To ensure that the logarithm is well-defined, the problem must be total, meaning that for every input instance, the counting value is at least 1.

**Corollary A.2.** *For $\delta : \mathbb{N} \to (0,1)$ and a constant $\epsilon$, if there is total counting problem $\Pi \in \#\mathsf{P}$ which is closed under multiplication and is $(1-\delta(n))$-hard to approximate multiplicatively with ratio $2^{\pm\epsilon}$ on some polynomial-time sampler $S$ for any polynomial-time algorithm, where $n$ is the complexity parameter of $\Pi$, for any constant $c \in \mathbb{N}$, there exists an efficient sampler $S'$, such that $\Pi$ is infinitely-often $O\left((m^{\frac{c-2}{c+1}}\delta'(m))^{-1/4}\right)$-hard to approximate multiplicatively with the same ratio on $S'(1^m)$ for polynomial-time algorithms, where $\delta'(m) = \delta\left(m^{1/(c+1)}\right)$.*

*Proof Sketch.* For simplicity, suppose any instance $x$ generated by $S$ satisfies $1 \leq \Pi(x) \leq 2^n$. Assume there is an efficient sampler $S$, such that, for any (non-uniform) polynomial-time algorithm $A$, we have

$$\Pr_{x \leftarrow S(1^n)}\left[A(x) \in \left(2^{-\epsilon}\cdot\Pi(x), 2^{\epsilon}\cdot\Pi(x)\right)\right] < 1-\delta(n).$$

Let $f(x) = \log\Pi(x)$, it is equivalent to, for any efficient algorithm $A'$,

$$\Pr_{x \leftarrow S(1^n)}\left[A'(x) \in (f(x) \pm \epsilon)\right] < 1-\delta(n).$$

For some constant $c \in \mathbb{N}$, we construct another sample $S'(1^{n^{c+1}})$: sample $x_1, \cdots, x_{n^c} \leftarrow S(1^n)$ independently and output $x \leftarrow \mathsf{Comb}(x_1, \ldots, x_{n^c})$. It is clear that $f(x) = \sum_{i=1}^{n^c} f(x_i)$. By theorem 1.2, the approximation of $f$ on $S'(1^{n^{c+1}})$ is $10 \cdot \epsilon^{-1/2}\left(m^{\frac{c-2}{c+1}}\delta'(m)\right)^{-1/4}$-hard for polynomial-time algorithms. Let $m = n^{c+1}$, it follows that

$$\Pr_{x \leftarrow S'(1^m)}\left[A(x) \in \left(2^{-\epsilon}\cdot\Pi(x), 2^{\epsilon}\cdot\Pi(x)\right)\right] < O\left((m^{\frac{c-2}{c+1}}\delta'(m))^{-1/4}\right)$$

where $\delta'(m) = \delta\left(m^{1/(c+1)}\right)$. □

Beyond the approximation problems mentioned above, we further explore some variants of optimization problems. For instance, while the search version of MaxSAT is a problem to find the optimal assignments to maximize the number of satisfied clauses, we focus on a different version of it, that is to evaluate this maximum value. According to previous study [GK20], the hardness of searching MaxSAT can be amplified. Our work indicates that evaluating MaxSAT also exhibits this property. We refer to this problem as MaxSAT in the following.

**Corollary A.3.** *For $\delta : \mathbb{N} \to (0,1)$, if there exists an instance sampler $S$, on which* MaxSAT *is $(1-\delta(n))$-hard for poly-time algorithms, for any constant $c \in \mathbb{N}$, there exists another sampler $S'$, on which* MaxSAT *is infinitely-often $O\left((m^{\frac{c-2}{c+1}}\delta'(m))^{-1/2}\right)$-hard for poly-time algorithm, where $\delta'(m) = \delta(m^{1/(c+1)})$.*

*Proof Sketch.* Based on sampler $S$, for constant $c \in \mathbb{N}$, construct $S'(1^{n^{c+1}})$: sample $\phi_i(x_{i,1},\ldots)$ independently, for $i \in \left\{1,\ldots,n^{c+1}\right\}$, and output $\phi_1(x_{1,1},\ldots) \wedge \phi_{n^{c+1}}(x_{n^{c+1},1},\ldots)$. By theorem 1.1, the $\mathsf{MaxSAT}$ on $S'(1^{n^{c+1}})$ is $O\left((n^{c-2}\delta(n))^{-1/2}\right)$-hard for polynomial-time algorithms. Let $m = n^{c+1}$, the following holds, for any poly-time algorithm $A$,

$$\Pr_{x \leftarrow S'(1^m)}\left[A(x) = \mathsf{MaxSAT}(x)\right] < O\left((m^{\frac{c-2}{c+1}}\delta'(m))^{-1/2}\right),$$

where $\delta'(m) = \delta\left(m^{1/(c+1)}\right)$. □