Electronic Colloquium on Computational Complexity, Revision 1 of Report No. 49 (2019)

A Tight Parallel-Repetition Theorem for Random-Terminating Interactive Arguments

Itay Berman* Iftach Haitner†‡ Eliad Tsfadia†

April 14, 2019

Abstract

Soundness amplification is a central problem in the study of interactive protocols. While "natural" parallel repetition transformation is known to reduce the soundness error of some special cases of interactive arguments: three-message protocols (Bellare, Impagliazzo, and Naor [FOCS '97]) and public-coin protocols (Håstad, Pass, Wikström, and Pietrzak [TCC '10], Chung and Lu [TCC '10] and Chung and Pass [TCC '15]), it fails to do so in the general case (the above Bellare, Impagliazzo, and Naor; also Pietrzak and Wikström [TCC '07]).

The only known round-preserving approach that applies to the general case of interactive arguments is Haitner's "random-terminating" transform [FOCS '09, SiCOMP '13]. Roughly speaking, a protocol π is first transformed into a new slightly modified protocol $\widetilde{\pi}$, referred as the *random terminating variant* of π, and then parallel repetition is applied. Haitner's analysis shows that the parallel repetition of $\widetilde{\pi}$ does reduce the soundness error at a *weak* exponential rate. More precisely, if π has m rounds and soundness error $1-\varepsilon$, then $\widetilde{\pi}^k$, the k-parallel repetition of $\widetilde{\pi}$, has soundness error $(1-\varepsilon)^{\varepsilon k/m^4}$. Since the security of many cryptographic protocols (e.g., binding) depends on the soundness of a related interactive argument, improving the above analysis is a key challenge in the study of cryptographic protocols.

In this work we introduce a different analysis for the above method, proving that parallel repetition of random terminating protocols reduces the soundness error at a much stronger exponential rate: the soundness error of $\widetilde{\pi}^k$ is $(1-\varepsilon)^{k/m}$, only an m factor from the optimal rate of $(1-\varepsilon)^k$, achievable in public-coin and three-message protocols. We prove the tightness of our analysis by presenting a matching protocol.

Keywords: parallel repetition; interactive argument; smooth KL-divergence

[*] MIT. E-mail:itayberm@mit.edu. Research supported in part by NSF Grants CNS-1413920 and CNS-1350619, and by the Defense Advanced Research Projects Agency (DARPA) and the U.S. Army Research Office under contracts W911NF-15-C-0226 and W911NF-15-C-0236.

[†] School of Computer Science, Tel Aviv University. E-mail:{iftachh@cs.tau.ac.il, eliadtsfadia@gmail.com}. Research supported by ERC starting grant 638121.

[‡] Member of the Check Point Institute for Information Security.

ISSN 1433-8092

Contents

1 Introduction

Hardness amplification is one of the most fascinating questions in the theory of computation. Can we transform a “weak primitive” into a hard one? And if so, can we do that while preserving the additional properties of the original weak primitive? In this paper we focus on better understanding the above question with respect to interactive arguments (also known as computationally sound proofs).

In an interactive proof system, a prover tries to convince a verifier via interaction in the validity of a statement. The basic properties of such proofs are *completeness* and *soundness*: in the former, the prover, typically using additional computational resources or some extra information, convinces the verifier to accept valid statements, while in the latter, a cheating prover (of a certain class) cannot convince the verifier to accept invalid statements. The basic distinction regarding such proof systems is whether the soundness holds unconditionally (i.e., against unbounded provers) or only holds against computationally bounded provers. Interactive proof systems with unconditional soundness are simply called interactive proofs, whereas proof systems in which soundness is only guaranteed to hold against polynomial time provers are called interactive arguments. The latter are the focus of this work. Interactive arguments are fundamental since the security of many cryptographic protocols depends on the soundness of a related interactive argument. In particular, having better means to amplify the hardness of interactive arguments, as discussed below, will help us improve the security of numerous cryptographic protocols.

The question is whether, given a proof system with non-negligible soundness error (a cheating prover can convince the verifier to accept false statements with some non-negligible probability), we can convert it into a new system, of similar properties, with negligible soundness error (the verifier almost never accepts false statements). The most common method to obtain such amplification is via repetition: repeat the protocol many times with independent randomness, and the verifier accepts only if the verifiers of the original protocol accept in *all* executions. Such repetition can be done in two different ways, sequentially (known as *sequential repetition*), where the $(i+1)$ execution of the protocol starts only after the i^{th} execution has finished, or in parallel (known as *parallel repetition*), where all of the executions are simultaneous. Sequential repetition is known to reduce the soundness error in most computational models (cf., Damgärd and Pfitzmann [DP98]), but has the undesired effect of increasing the round complexity of the protocol. Parallel repetition, on the other hand, does preserve the round complexity, and reduces the soundness error for (single-prover) interactive proofs (Goldreich [Gol99]) and two-prover interactive proofs (Raz [Raz98]). Parallel repetition was also shown to reduce the soundness error in three-message arguments ([BIN97]) and public-coin arguments (Håstad, Pass, Wikström, and Pietrzak [Hås+10], Chung and Lu [CL02], and Chung and Pass [CP15]). But, as shown by Bellare, Impagliazzo, and Naor [BIN97], and by Pietrzak and Wikström [PW12], parallel repetition *might not* reduce the soundness error of any interactive argument: using common cryptographic assumptions, Pietrzak and Wikström [PW12] presented an 8-message interactive proof with constant soundness error, whose parallel repetition, for *any* polynomial number of repetitions, still has a constant soundness error (same constant for all k).

Faced with the above barrier, Haitner [Hai13] presented a simple method for transforming any interactive argument π into a slightly modified protocol $\widetilde{\pi}$, such that the parallel repetition of $\widetilde{\pi}$ does reduce the soundness error. Given any m-round interactive protocol $\pi = (\mathrm{P}, \mathrm{V})$, let $\widetilde{\mathrm{V}}$ be the following *random terminating variant* of V: in each round, it flips a coin that takes one with probability $1/m$ and zero otherwise. If the coin outcome is one, it accepts and aborts the execution. Otherwise, it acts as V would, and continues to the next round. At the end of the prescribed execution, if reached, it accepts if and only if V would. Observe that if the original protocol π has soundness error $1-\varepsilon$, then the new protocol $\widetilde{\pi} = (\mathrm{P}, \widetilde{\mathrm{V}})$ has soundness error $1-\varepsilon/4$ (i.e., only slightly closer to one). Haitner [Hai13] proved that the parallel repetition of $\widetilde{\pi}$ does reduce the soundness error (for any protocol π). Specifically, assuming π's soundness error is $1-\varepsilon$, then $\widetilde{\pi}^k$, the k-parallel repetition of π, has soundness error $(1-\varepsilon)^{\varepsilon k/m^4}$.[1] The intuition here is that, by randomly terminating, the verifier prevents a cheating prover from coordinating the different executions of the protocol. Thus, it cannot do much better than acting *independently* in the different executions, yielding an exponential decay in its cheating probability.[2] Turning the above intuition into a formal proof is not that simple; see further details in Section 2. While Haitner's work [Hai13] is a strong feasibility result, the dependency on ε and inverse dependency on m^4 in the soundness error makes the random termination approach impractical for arguments with a weak soundness guarantee or with a large number of rounds. It also lags behind the $(1-\varepsilon)^k$ upper bound achieved by parallel repetition of interactive proofs, and by three-message and public-coin interactive arguments.

We emphasize that parallel repetition of the random-terminating variant of a protocol is the *only* unconditional round-preserving hardness amplification technique we have for arbitrary interactive arguments.[3] For instance, parallel repetition of the random-terminating variants yields the only known proof that constant-round weakly binding statistically hiding commitments imply constant-round fully secure commitments.[4] For additional concrete examples where the above amplification paradigm is used, see [BC12; Chu+13].

1.1 Our Results

Recall that parallel repetition of the random-terminating variant on an interactive argument is the only known (unconditional) round-preserving amplification method for interactive arguments. We present a tight characterization of this amplification method.

Upper bound. Our main result is that parallel repetition of the random termination applied on interactive arguments decreases the soundness error at a much stronger rate than that proven in [Hai13].

[1] As in all known amplifications of computational hardness, and proven to be an inherent limitation (at least to some extent) in [Dod+12], the improvement in the soundness error does not go below negligible. We ignore this subtly in the introduction. We also ignore constant factors in the exponent.

[2] For those seeking further intuition for why random-termination is useful, in Section 8 we show that random-terminating verifiers are immune to the counterexample of [BIN97].

[3] A conditional result proved by Chung and Liu [CL10] is the that fully homomorphic encryption (FHE) can be used to compile any interactive argument into one (with the same soundness error) for which parallel repetition improves the soundness (at the same rate as for public-coin arguments). Since it assumes FHE, which we only know how to build assuming hardness of *learning with errors* [BV14], [CL10], it is applicable only in very restricted settings. In addition, the compiled protocol does not have some of the guarantees the original protocol might have, e.g., fairness. Finally, since it requires homomorphic evaluation of *each* of the protocol's gates, it is highly inefficient (computation-wise).

[4] Using sequential repetitions—the only other alternative—would blow up the round complexity by $1/\delta$ for $\delta < 1$ being the commitment (weak) binding guaranteed (we are omitting an additional logarithmic factor, where the logarithm is over the security parameter).

Theorem 1.1 (main theorem, informal)**.** *Let $\pi = (\mathrm{P}, \mathrm{V})$ be an m-round interactive argument with soundness error $1 - \varepsilon$, let $\widetilde{\mathrm{V}}$ be the random terminating variant of V, and let $\widetilde{\pi}^k$ be the k-parallel repetition of $\widetilde{\pi} = (\mathrm{P}, \widetilde{\mathrm{V}})$. Then, $\widetilde{\pi}^k$ has soundness error $(1 - \varepsilon)^{k/m}$.*

Suppose that we want to get from soundness error $1 - \varepsilon$ to soundness error δ. According to [Hai13], we have to take $m^4 \cdot \log(1/\delta)/\varepsilon^2$ repetitions of $\widetilde{\pi}$, where according to our Theorem 1.1, $m \cdot \log(1/\delta)/\varepsilon$ repetitions suffice. Specifically, for constant-round protocols, our result matches, up to a constant factor, the dream version of parallel repetition for interactive proofs, and public-coin and three-message arguments, and it improves over [Hai13] by a factor of $1/\varepsilon$. For non-constant-round protocols, our result is only an m factor away from the dream version, and this linear dependency in m improves over the quartic dependency in [Hai13].

Theorem 1.1 immediately yields (see [Hai13] for details) the following improvement of the only known round-preserving amplification of statistically hiding commitments. A commitment scheme is *ε-binding* if no efficient cheating committer opens the commitment into two different values with probability larger than ε. A commitment is *statistically hiding* if it does not reveal any significant information about the committed value.

Corollary 1.2 (Amplification of statistically hiding commitment, informal)**.** *Let Com be an m-round, $(1 - \varepsilon)$-binding and statistically hiding commitment scheme, and let $\widetilde{\mathsf{Com}}$ be its variant in which the receiver aborts following each round of the commitment phase and publishes an empty commitment string, with probability $1/m$. Then $\widetilde{\mathsf{Com}}^{m \cdot \log(1/\delta)/\varepsilon}$ is a statistically hiding and δ-binding commitment. Taking $\delta = n^{-\omega(\log n)}$, for n being the security parameter, yields a full-fledged (i.e.,* neg*-binding) statistically hiding and computationally binding commitment scheme.*

The above gives a tight result for constant-round statistically hiding commitments, and drastically improves upon the $m^4 \cdot \log(1/\delta)/\varepsilon^2$ repetitions of $\widetilde{\mathsf{Com}}$ required according to [Hai13].

Lower bound. We complete the picture by showing that the $1/m$ factor in the exponent in Theorem 1.1 is unavoidable.

Theorem 1.3 (lower bound, informal)**.** *Under suitable cryptographic assumptions, for any $m \in \mathbb{N}$ and $\varepsilon \in [0, 1]$, there exists an m-round interactive argument (P, V) with soundness error $1 - \varepsilon$ such that $(\mathrm{P}^k, \widetilde{\mathrm{V}}^k)$ has soundness error at least $(1 - \varepsilon)^{k/m}$.*

Namely, $m \cdot \log(1/\delta)/\varepsilon$ repetitions are required for moving from soundness error $1 - \varepsilon$ to soundness error δ.

Theorem 1.1 easily yields the following lower bound for amplification of statistically hiding commitments.

Corollary 1.4 (Lower bound on amplification of statistically hiding commitment, informal)**.** *Under suitable cryptographic assumptions, for any $m \in \mathbb{N}$ and $\varepsilon \in [0, 1]$ there exists an m-round, $(1 - \varepsilon)$-binding and statistically hiding commitment scheme Com, such that $\widetilde{\mathsf{Com}}^{m \cdot \log(1/\delta)/\varepsilon}$ is* not *$o(\delta)$ binding.*

Our technique, a short overview. Below we give the highlights of our proof for Theorem 1.1. See Section 2 for a detailed overview.

As in all such amplification results, the proof of Theorem 1.1 is via a reduction: given an efficient prover P^{k*} that violates the $(1-\varepsilon)^{k/m}$ soundness error of $\widetilde{\pi}^k$, we construct an efficient prover P^* that violates the $(1-\varepsilon)$ soundness error of $\pi = (\mathrm{P}, \mathrm{V})$. As in Haitner [Hai13], we considered the following cheating prover P^* for making V accept a false statement: P^* uniformly samples $i \sim [k]$, and starts emulating an interaction of $(\mathrm{P}^{k*}, \widetilde{\mathrm{V}}^k)$ with V embedded as the i^{th} verifier. Upon getting the j^{th} message from V, it acts as follows:

1. Samples the messages of the emulated verifiers in the j^{th} round of $(\mathrm{P}^{k*}, \widetilde{\mathrm{V}}^k)$, conditioned that all verifiers accept and the i^{th} verifier halts in the next round.
2. Answers V according to the message sent to the i^{th} verifier in the j^{th} round of the emulated execution of $(\mathrm{P}^{k*}, \widetilde{\mathrm{V}}^k)$.

Namely, the rejection sampling assumes the i^{th} (real) verifier aborts in the beginning of the next round, and thus the sampling can be done efficiently (see Section 2 for further details).

To analyze the success probability P^*, we use the standard (in this line of works) paradigm of *ideal* vs. *real* executions: let Ideal denote the distribution induced by an *accepting* random execution of $(\mathrm{P}^{k*}, \widetilde{\mathrm{V}}^k)$, and show that the distribution of the emulated execution of $(\mathrm{P}^{k*}, \widetilde{\mathrm{V}}^k)$ induced by the above attack (denoted by the Real experiment) is close enough to Ideal. It will then follow that the above attack succeeds with high probability. Haitner [Hai13] bounds the statistical distance between Ideal and Real. Statistical distance, however, seems not to be the right measure to consider in this setting. Specifically, it lacks a chain rule and does not tensor under product distributions, two properties that seem relevant for lower bounding the prover's success probability. So rather, we bound a relaxed variant of their KL-divergence.[5] We first give a high-level overview of the steps in our proof.

First round. For the first round interaction, we show that while the KL-divergence between Ideal and Real might be *huge*, the resulting divergence is small when we ignore carefully defined events in Ideal. We then show that this "smooth" variant of KL-divergence suffices for the proof.

Next rounds. Our first round analysis critically relies on the fact that the position i of the real verifier among the k emulated ones is uniformly chosen by the cheating prover P^*. When analyzing the next rounds, however, the relevant distribution to consider is the position of the real verifier *conditioned* that the interaction so far led to the previous rounds' transcript. It turns out that this conditional distribution might be very far from uniform.

We show that when sampling the transcript according to Ideal, as done when computing the (smooth) KL-divergence between Ideal and Real, the conditional distribution of the index i induces a martingale sequence (this fact holds for any prover strategy that hides the real verifier among the emulated ones). We then show that in our setting, this martingale sequence converges well. It follows that with high probability over Ideal, the distribution of the location i conditioned on the transcripts is "uniform enough" to allow the same approach we take for the first round to go through.

We believe that the above observations will turn out to be useful in analyzing the parallel repetition on other interactive proof systems.

[5] For these reasons, Chung and Pass [CP15] use the standard notion of KL-divergence for bounding the soundness error of parallel repetition of public-coin interactive arguments.

1.2 Related Work

1.2.1 Interactive Arguments

Positive results. Bellare, Impagliazzo, and Naor [BIN97] proved that the parallel repetition of three-message interactive arguments reduces the soundness error at an exponential but not optimal rate. Canetti, Halevi, and Steiner [CHS05] later showed that parallel repetition does achieve an optimal exponential decay in the soundness error for such arguments. Pass and Venkitasubramaniam [PV12] have proved the same for constant-round public-coin arguments. For public-coin arguments of any (polynomial) round complexity, Håstad *et al.* [Hås+10] were the first to show that parallel repetition reduces the soundness error exponentially, but not at an optimal rate. The first optimal analysis of parallel repetition in public-coin arguments was that of Chung and Liu [CL10], who showed that the soundness error of the k repetitions improves to $(1-\varepsilon)^k$. Chung and Pass [CP15] gave an arguably simpler proof for public-coin arguments, via KL-divergence arguments, a result that is the starting point of our analysis (see Section 2). For non-public coin and with any round complexity argument, Haitner [Hai13] introduced the random-terminating variant of a protocol, and proved that the parallel repetition of these variants improves the soundness error at a weak exponential rate. An alternative proof, with essentially the same parameters, was given by [Hås+10]. Their proof holds for $1/m$-*simulatable verifiers* [Hås+10] that contain random-terminating verifiers as a special case.[6] All the above results extend to "threshold verifiers": the parallel repetition is considered accepting if the number of accepting verifiers is above a certain threshold. Our result rather easily extends to such verifiers, but we defer the tedious details to the next version.

Chung and Pass [CP11] proved that full independence of the parallel executions is not necessary to improve the soundness of public-coin arguments, and the verifier can save randomness by carefully correlating the different executions. It is unknown whether similar savings in randomness can be achieved for random-terminating arguments.

Negative results. Bellare, Impagliazzo, and Naor [BIN97] presented for any $k \in \mathbb{N}$, a four-message interactive argument of soundness error $1/2$, whose k-parallel repetition soundness remains $1/2$. Pietrzak and Wikström [PW12] ruled out the possibility that enough repetitions will eventually improve the soundness of an interactive argument. They presented a *single* 8-message argument for which the above phenomenon holds for all polynomial k simultaneously. Both results hold under common cryptographic assumptions.

1.2.2 Two-Prover Interactive Proofs

The techniques used in analyzing parallel-repetition of interactive arguments are closely related to those for analyzing parallel repetition of two-prover one-round games, which we now very briefly describe. In such a game, two unbounded *isolated* provers try to convince a verifier in the validity of a statement. Given a game of soundness error $(1-\varepsilon)$, one might expect the soundness error of its k parallel repetition to be $(1-\varepsilon)^k$, but as in the case of interactive arguments, this turned out to be false [Fei91; FV02; FRS90]. Nonetheless, and although not true for arguments, Raz [Raz98] showed that parallel repetition does achieve an exponential decay for any two-prover one-round game, and

[6] Roughly, a verifier is δ-simulatable if given any partial transcript, the verifier's future messages can be sampled efficiently with probability δ (over its coins), without knowing the internal state of the verifier. Our proof seems to easily extend to $1/m$-simulatable verifiers, but since the only examples for such verifiers are random terminating verifiers, we chose to give our proof in the simpler language of the latter.

in particular reduces the soundness error to $(1-\varepsilon)^{\varepsilon^{O(1)} k/\log s}$, letting s being the provers' answer length. These parameters were later improved by Holenstein [Hol09], and improved further for certain types of games by Rao [Rao11], Dinur and Steurer [DS14], and Moshkovitz [Mos14].

The core challenge in the analysis of parallel repetition of interactive arguments and of two-prover one-round games is very similar: how to simulate a random accepting execution of the proof/game given the verifier message. In interactive arguments, this is difficult since the prover lacks computational power. In two-prover one-round games, the issue is that the two provers cannot communicate. We hope that our new tight understanding of parallel repetition of interactive arguments will turn out to be useful for achieving tighter analysis of parallel repetition of (certain types of) two-prover one-round games.

Paper Organization

We overview the proof of our main theorem (Theorem 1.1) in Section 2. Basic notations, definitions and tools used throughout the paper are given in Section 3. The formal statement of our main theorem and its proof using Lemma 4.9, our main technical lemma, are given in Section 4. The road map towards proving Lemma 4.9 is given in Section 5, and the proof details are given in Sections 6 and 7. Our matching lower bound on the effect of parallel repetition on random-terminating arguments is stated and proved in Section 8. Finally, the missing proofs can be found in Appendix A.

2 Our Technique

In this section we give a high-level overview of the proof of our main result (Theorem 1.1). We start by describing the simpler case of parallel repetition of public-coin arguments, while focusing on bounding a distance measure known as KL-divergence (following Chung and Pass [CP15]). Moving to random-terminating arguments, we explain the reduction of Haitner [Hai13] and present our analysis that bounds a relaxed ("smooth") variant of the KL-divergence.

2.1 Public-Coin Arguments

Let $\pi = (\mathrm{P}, \mathrm{V})$ be an m-round public-coin interactive argument (the verifier simply sends its random coins) with soundness error $1-\varepsilon$, and let $k \in \mathbb{N}$ be such that $(1-\varepsilon)^k$ is noticeable (as we mentioned in Footnote 1, we cannot expect the soundness to get below noticeable). The goal is to show an *optimal* exponential decay of the soundness error when repeating the protocol in parallel, that is, to prove that the soundness error of $\pi^k = (\mathrm{P}^k, \mathrm{V}^k)$, the k-fold repetition of π, is at most $(1-\varepsilon)^k$. As in all such hardness amplification results, the proof is via a reduction: given an efficient prover P^{k^*} violating the $(1-\varepsilon)^k$ soundness error of π^k, we use P^{k^*} to construct an efficient prover P^* that violates the $(1-\varepsilon)$ soundness error of π. More specifically, to interact with V on a false statement, the cheating prover P^* uses P^{k^*} to emulate a winning (all verifiers accept) execution of $(\mathrm{P}^{k^*}, \mathrm{V}^k)$ on the false statement, while embedding the messages of the real interaction as those of one of the k verifiers. Since an all-accepting emulation yields that the embedded real verifier accepts in the real execution, the challenge reduces to showing that such an emulation can be done successfully.

To present and analyze the above reduction, we need to be a bit more formal. Assume for simplicity that P^{k^*} is deterministic. Let $X^{m\times k} = (X_1^k, \ldots, X_m^k)$ be the messages (in this case, random coins) of V^k in a random execution of $(\mathrm{P}^{k^*}, \mathrm{V}^k)$, where $X_{j,i}$ consists of the j^{th} message sent by the i^{th} verifier. Let W be the event that V^k accepts in $(\mathrm{P}^{k^*}, \mathrm{V}^k)$ (namely, in this case W is simply a subset of $\mathrm{Supp}(X^{m \times k})$).

The cheating prover P^* emulates a winning execution of $(\mathrm{P}^{k^*}, \mathrm{V}^k)$ as follows: before interacting with V it uniformly samples $i \sim [k]$; the messages from V would be embedded as the messages of the i^{th} verifier in $(\mathrm{P}^{k^*}, \mathrm{V}^k)$. Upon getting the j^{th} message $x_{j,i}$ from V, it acts as follows:

1. Samples $x_j^k \sim X_j^k|_{X_{<j}^k = x_{<j}^k, X_{j,i} = x_{j,i}, W}$. (Letting $X_{<j}^k = (X_1^k, \ldots, X_{j-1}^k)$ and similarly for $x_{<j}^k$, where the latter denotes the verifiers' messages thus far.)

2. Sends $b_{j,i}$ back to V, for $b_j^k = (b_{j,1}, \ldots, b_{j,k})$ being the message tuple P^{k^*} sends back to V^k in the j^{th} round of $(\mathrm{P}^{k^*}, \mathrm{V}^k)$, induced by x_j^k (recall that P^{k^*} is assumed to be deterministic).

The sampling in Step 1 is done via *rejection sampling*: keep sampling values for $X_{\geq j}^k|_{X_{<j}^k = x_{<j}^k, X_{j,i} = x_{j,i}}$ until W happens and set $x_j^k = X_j^k$. Since V is public-coin, as long as $\Pr[W | X_{<j}^k = x_{<j}^k, X_{j,i} = x_{j,i}]$ does not get too low, such rejection sampling can be done efficiently. For a tuple of messages $x^{m \times k}$, let $\mathrm{Succ}(x^{m \times k})$ be the indicator for the event that $\Pr[W | X_{<j}^k = x_{<j}^k, X_{j,i} = x_{j,i}]$ does not get too low for every $j \in [m]$. Let Real denote the random tuple of messages $X^{m \times k}$ induced by the above execution of $(\mathrm{P}^*, \mathrm{V})$, whose soundness error can now be lower-bounded by $\Pr[\mathrm{Succ}(\mathrm{Real})]$. Thus, showing that $\Pr[\mathrm{Succ}(\mathrm{Real})] > 1 - \varepsilon$ would complete the analysis.

The standard technique to show the above lower-bound is by *change of measure*: describe a different distribution under which Succ occurs with high probability, and bound the difference between that distribution and Real. A natural choice for such a distribution is that of $X^{m \times k}|_W$, which we refer to as Ideal. This is the distribution that would arise if the messages of the real verifier would also have been chosen, as are the messages of the other emulated verifiers, by conditioning on W (and not uniformly at random). Since, by assumption, $\Pr[W] \geq (1 - \varepsilon)^k$ is noticeable, a Markov argument yields that $\Pr[\mathrm{Succ}(\mathrm{Ideal})] \approx 1$, and we will assume it is equal to 1 for the rest of this analysis.

It is left to show that the difference between Real and Ideal is small. Note that up until now we have not specified which measure of difference to use. Indeed, different choices of measure yield different results. Early results in this line of works (e.g., [Hås+10; Hai13]) bounded the *statistical distance* between Ideal and Real.[7] It seems, however, that statistical distance is not the right measure to consider in this setting. Specifically, it lacks a chain rule and does not tensor under product distributions, two properties that seem relevant for lower bounding the prover's success probability. The chain rule can be used to split the transcripts of Ideal and Real per round and analyze their difference on a round basis. Tensorizing under product distributions is useful since the messages of the public-coin verifiers are chosen from a product distribution. The analysis in the above works does suffer from these disadvantages, and as a result they do not achieve optimal exponential decay.

A more suitable choice of measure would seem to be the *Kullback-Leibler divergence* (KL-divergence) between Ideal and Real, denoted by $D(\mathrm{Ideal} \,||\, \mathrm{Real})$.[8] The KL–divergence does have a chain rule and is (appropriately) tensorized under product distributions. Indeed, using the KL-

[7] The *statistical distance* between two distributions P and Q over the same domain $\mathcal{X}$ is defined as $\mathrm{SD}(P, Q) := \max_{\mathcal{S} \subseteq \mathcal{X}} P[\mathcal{S}] - Q[\mathcal{S}]$.

[8] The KL-divergence (also known as *divergence* and *relative entropy*) between two distributions P and Q is defined as $D(P||Q) = \mathrm{E}_{x \sim P} \log \frac{P(x)}{Q(x)}$.

divergence, Chung and Pass [CP15] gave an elegantly simple proof for the optimal exponential decay of the soundness error for public-coin protocols that we review next.[9]

Recall that our goal is to show that $\Pr[\mathrm{Succ}(\mathrm{Real})] > 1-\varepsilon$. The first step is to apply the data-processing inequality for KL-divergence:[10]

$$D(\mathrm{Ideal}\,||\,\mathrm{Real}) \geq D(\mathrm{Bern}(\Pr[\mathrm{Succ}(\mathrm{Ideal})])||\,\mathrm{Bern}(\Pr[\mathrm{Succ}(\mathrm{Real})])) = \log\frac{1}{\Pr[\mathrm{Succ}(\mathrm{Real})]} \tag{1}$$

for $\mathrm{Bern}(p)$ denoting the Bernoulli distribution with parameter p, and where the equality follows since we assumed that $\Pr[\mathrm{Succ}(\mathrm{Ideal})] = 1$. The second step is to upper-bound $D(\mathrm{Ideal}\,||\,\mathrm{Real})$. Chung and Pass [CP15], generalizing over [Raz98] and using the chain-rule for KL-divergence, showed that

$$D(\mathrm{Ideal}\,||\,\mathrm{Real}) \leq \frac{1}{k}\cdot D(X^{m\times k}|_W||X^{m\times k}) \leq \frac{1}{k}\cdot\log\frac{1}{\Pr[W]} \tag{2}$$

The above equations now yield that

$$\Pr[\mathrm{Succ}(\mathrm{Real})] \geq \exp(-D(\mathrm{Ideal}\,||\,\mathrm{Real})) \geq \Pr[W]^{1/k} > 1-\varepsilon \tag{3}$$

where we used that, by assumption, $\Pr[W] > (1-\varepsilon)^k$.

Our proof (see below) adopts the above paradigm to the more complicated setting that arises when analyzing parallel repetition of random-termination arguments. In particular, we bound a *relaxed* variant of the KL-divergence between the Ideal and Real distributions, and show that such a bound suffices for the reduction.

2.2 Random-Terminating Arguments

For arbitrary (non-public coin) arguments, the above analysis fails to hold because of the possible infeasibility of the rejection sampling used by the above attacker for choosing its response in each round. Indeed, such sampling requires finding random coins for the real and emulated verifiers that are consistent with the current transcript. This requires inverting at random the transcript function of the real verifier (i.e., the function mapping the parties' coins to the protocol's transcripts), and for the emulated verifiers (for which the attacker holds one set of consistent coins), it requires finding a second random preimage of the transcript function. Each of these tasks is infeasible assuming one-way functions exist [IL89; Rom90], and indeed the sampling should be infeasible since parallel repetition of arbitrary arguments might not improve the hardness at all [BIN97; PW12]. Random-terminating arguments enable us to bypass the two obstacles above (inverting the real verifier transcript function, and finding a second pre-image for the emulated verifiers).

Let $\pi = (\mathrm{P},\mathrm{V})$ be an (arbitrary) m-round argument and let $\widetilde{\mathrm{V}}$ be the random-terminating variant of V, i.e., at the beginning of each round, $\widetilde{\mathrm{V}}$ halts and accepts with probability $1/m$, and let $k\in\mathbb{N}$ be such that $(1-\varepsilon)^{k/m}$ is noticeable. Let P^{k^*} be an efficient adversary violating the $(1-\varepsilon)^{k/m}$ soundness error of $\widetilde{\pi}^k$ (note that we are no longer aiming for the optimal exponential decay). As in the public-coin case, we use P^{k^*} for constructing an efficient prover P^* violating the $(1-\varepsilon)$ soundness error of π.

[9] An optimal exponential decay for public-coin protocols was already shown by [CL10]. That proof does not use the Ideal vs. Real paradigm, and is harder to follow.

[10] The data-processing inequality for KL-divergence states that for any (possibly random) function F, it holds that $D(P||Q)\geq D(F(P)||F(Q))$.

To present and analyze the reduction, we again need to be a bit more formal. We keep the simplifying assumption that P^{k^*} is deterministic, and further assume without loss of generality that V flips all its coins before the interaction begins. It follows that the random-terminating variant $\widetilde{\mathrm{V}}$ flips a string of coins before the interaction starts, to be used by V, and then flips a single $(1/m, 1-1/m)$ coin before each round, to determine whether it aborts (and accepts) or acts as V would in the current round. Let $(Z^k, X^{m\times k} = (X_1^k, \ldots, X_m^k))$ be the *coins* flipped by $\widetilde{\mathrm{V}}^k$ in a random execution of $(\mathrm{P}^{k^*}, \widetilde{\mathrm{V}}^k)$: Z_i are the coins the i^{th} verifier flips for the use of its internal copy of V, and $X_{j,i}$ is the coin it flips before the j^{th} round to decide whether to halt (set to 0 in case of an abort in a previous round). Let W be the event that V^k accepts $(\mathrm{P}^{k^*}, \widetilde{\mathrm{V}}^k)$ (i.e., W is simply a subset of $\operatorname{Supp}(Z^k, X^{m\times k})$).

Haitner [Hai13] considered the following cheating prover P^* for making V accept a false statement: before interacting with V, it samples uniformly $i \sim [k]$, embeds V as the i^{th} verifier in the emulated interaction $(\mathrm{P}^{k^*}, \mathrm{V}^k)$, and samples $z^k \sim Z^k|_{Z_i = z_i, X_{1,i}=1, W}$, for z_i being the random coins of V. (As explained below, this sampling does *not* require knowing z_i, which is not known to P^*.) Upon getting the j^{th} message from V, it acts as follows:

1. Samples $x_j^k \sim X_j^k|_{Z^k = z^k, X_{<j}^k = x_{<j}^k, X_{j+1,i}=1, W}$.
2. Sends $b_{j,i}$ back to V, for $b_j^k = (b_{j,1}, \ldots, b_{j,k})$ being the message tuple P^{k^*} sends back to V^k in the j^{th} round of $(\mathrm{P}^{k^*}, \mathrm{V}^k)$ induced by $z^k, x_1^k, \ldots, x_j^k$.

Namely, the rejection sampling assumes the real verifier aborts in the beginning of the next round. This yields that the rejection sampling can be carried out efficiently, as long as the conditional winning (all verifiers accept) probability is not too low. Indeed, since the conditioning is on the verifier coins (and not its messages), finding coins for the emulated verifiers boils down to choosing their next round coins uniformly at random. In addition, since the condition is that the real verifier aborts in the beginning of the next round, its random coins have *no* effect on the conditional distribution we aim to sample from, and thus we can sample from this distribution without knowing their value.

As in the public-coin setting, we would like to bound the KL-divergence between the Ideal distribution—that in this case is defined as $Z^k X^{m\times k}|_W$, and the Real distribution—the random tuple $Z^k X^{m\times k}$ induced by a random execution of $(\mathrm{P}^*, \mathrm{V})$. As mentioned above, we were only able to bound a relaxed variant of the KL-divergence between Ideal and Real, and had to consider a relaxed variant of this measure; see details in the next subsection.

2.2.1 Bounding the KL-Divergence between Ideal and Real

Bounding the KL-divergence between Ideal and Real turned to be a much more challenging task than in the public-coin case considered above. First, the conditional distribution used in the rejection sampling is very different than its ideal variant. Therefore, even bounding the KL-divergence of a *single* interacting round is complicated. Second, in the public-coin case it can be assumed without loss of generality that $X^{m\times k}|_W$ is a product distribution—the attacker consists of k independent attackers,[11] an assumption that drastically simplifies the analysis. Unfortunately, this

[11] This is not easy to see at first glance but it implicitly arises by the proof of Chung and Pass [CP15].

simplifying assumption cannot be made for non-public-coin random-terminating arguments.[12] Instead, the attacker may induce complicated non-product distributions Ideal and Real such that the KL-divergence between them is too large to be useful. Fortunately, it turns out that when ignoring the distribution of small probability events over Ideal, the resulting "smooth" KL-divergence is low, and this bound suffices to make the reduction go through.

To illustrate our technique, we focus only on $Z^k = (Z_1, \ldots, Z_k)$—the coins for the internal copies of V, and on $X_1^k = X^k = (X_1, \ldots, X_k)$—the random termination coins for the first round (in particular, $X_i \sim \mathrm{Bern}(1/m)$). The distribution Ideal in this case is $(Z^k X^k|_W)$, and in this explanation we focus only on the "Z-part" of Ideal—$Z^k|_W$ (but as we will see shortly, the "X-part" will be very relevant). The "Z-part" of Real is more complicated. First an index $i \sim [k]$ is drawn and then $z_i \sim Z_i$ is sampled uniformly at random. The rest of Z^k is now drawn from $Z^k|_{Z_i=z_i, X_i=1, W}$. Our goal is to bound the divergence between these two "Z-parts". Actually, for this discussion, we also want to assume for simplicity that Z_i is sampled the same as the rest of Z^k; that is, we consider $Z^k|_{X_i=1,W}$, which we call Real$'$. While Real$'$ is different from Real, the insights as to how to bound the KL-divergence for this distribution carry over to the actual Real distribution. To summarize, our goal is to bound $D(Z^k|_W || Z^k|_{X_I=1,W})$, for I being drawn uniformly from $[k]$.

Our first observation is as follows: conditioned on X^k being some fixed x^k, Z^k is distributed the same under Ideal and Real$'$—both sample from $Z^k|_{X^k=x^k,W}$. The difference between these distributions is thus traced to how X^k is sampled. By the data-processing inequality for KL-divergence, it holds that

$$D(Z^k|_W || Z^k|_{X_I=1,W}) \leq D(X^k|_W || X^k|_{X_I=1,W}) \tag{4}$$

So, instead of bounding the KL-divergence of the "Z-parts", we bound it for the "X-parts", *without* first drawing the "Z-parts".

In the following, fix $x^k \in \mathrm{Supp}(X^k|_W)$ and let $1_{x^k} = \{i \in [k] \colon x_i = 1\}$ denote the set of 1-indexes in x^k. It holds that

$$\begin{aligned} \Pr\Big[X^k = x^k \mid X_I = 1, W\Big] &= \mathrm{E}_{i \sim [k]}\Big[\Pr\Big[X^k = x^k \mid W, X_i = 1\Big]\Big] \\ &= \frac{1}{k} \sum_{i \in 1_{x^k}} \Pr\Big[X^k = x^k \mid W, X_i = 1\Big] \\ &= \frac{1}{k} \sum_{i \in 1_{x^k}} \frac{\Pr\big[X^k = x^k \mid W\big]}{\Pr[X_i = 1 \mid W]}. \end{aligned} \tag{5}$$

Combining the above we get

$$D(Z^k|_W || Z^k|_{X_I=1,W}) \leq \mathrm{E}_{x^k \sim X^k|_W}\left[\log \frac{k}{\sum_{i \in 1_{x^k}} \frac{1}{\Pr[X_i=1|W]}}\right] \tag{6}$$

Our first round analysis focuses on characterizing $\sum_{i \in 1_{x^k}} \frac{1}{\Pr[X_i=1|W]}$ for a random $x^k \sim X^k|_W$. We take the following approach: for $i \in [k]$, let $p_i = \Pr[X_i = 1 \mid W]$, let Y_i be a random variable taking

[12] We actually know that for certain arguments, the attacker can improve its winning probability by correlating between the different verifiers (e.g., see our counterexample in Section 8).

the value $1/p_i$ if $x_i = 1$, and 0 otherwise, for a randomly drawn $x^k \sim X^k|_W$, and let $Y = \sum_{i=1}^{k} Y_i$. Note that the Y_i's are *dependent*, since their distributions are determined by the same $x^k \sim X^k|_W$. It is easy to verify that $\mathrm{E}_{X^k|_W}[Y] = k$.[13] That is, the expected value of the denominator in Equation (6) is equal to the nominator. Let Δ be a random variable measuring how far Y is from its mean; that is, $Y = (1+\Delta) \cdot k$. It follows that $\mathrm{E}_{X^k|_W}[\Delta] = 0$ and that

$$D(Z^k|_W || Z^k|_{X_I=1,W}) \le \mathrm{E}_{X^k|_W}\left[\log \frac{1}{1+\Delta}\right] \tag{7}$$

Naturally, we would like to approximate the logarithm in the above equation with a low-degree polynomial. We can only do that, however, if Δ is far away from -1. In particular, if $\Delta = -1$ (which happens if W allows for none of the verifiers to abort in this round), the above expectation is unbounded. Luckily, it turns out that Δ is far from its expected value 0 under $X^k|_W$ with only small probability. We somehow want to ignore the chance that Δ is far from 0 when bounding the KL-divergence. We would like a *smooth* variant of the KL-divergence.

2.2.2 Smooth KL-Divergence

The KL-divergence between P and Q is a very sensitive distance measure. An event x with $P(x) \gg Q(x)$ might make $D(P||Q)$ huge even if $P(x)$ is tiny (e.g., $P(x) > 0 = Q(x)$ implies $D(P||Q) = \infty$). While in some settings one might care about low probability events, this is not the case in our setting. Recall that our ultimate goal is to use the KL-divergence for a change-of-measure: if $\Pr_P[E]$ is large for some event E, then we would like to argue that $\Pr_Q[E]$ is also large. Since an element x with small $P(x)$ does not contribute much to the probability of E, omitting it still keeps $\Pr_Q[E]$ high and thus we can exclude it from our analysis.

So we need a less sensitive measure that still maps events of high probability in P to events of high probability in Q. A natural attempt would be to define it as $\inf_{P',Q'}\{D(P'||Q')\}$, where the infimum is over all pairs of distributions such that both $\mathrm{SD}(P,P')$ and $\mathrm{SD}(Q,Q')$ are small. This relaxation, however, requires an upper bound on the probability of events with respect to Q, which in our case is the Real distribution. But bounding the probability of events with respect to the Real distribution is exactly what we are trying to do to begin with.

So rather, we take advantage of the asymmetric nature of the KL-divergence to propose a relaxation that only requires upper-bounding events with respect to P, which in our case is the much simpler Ideal distribution.[14]

Assume P and Q are over domain $\mathcal{U}$. The *α-smooth KL-divergence of P and Q* is defined by

$$D^{\alpha}(P||Q) = \inf_{(F_P,F_Q)\in\mathcal{F}}\{D(F_P(P)||F_Q(Q))\}, \tag{8}$$

for $\mathcal{F}$ being the set of randomized function pairs, such that for every $(F_P, F_Q) \in \mathcal{F}$:

[13] Note that $p_i > 0$ for all i since all the verifiers might abort and accept in the first round. In the body of this work we refer to this property as *termination consistent*.

[14] At least syntactically, the notion of smooth KL-divergence we consider here is similar to the distance measure used by the *(coefficients) H-Technique* tool, introduced by Patarin [Pat90], for upper-bounding *statistical distance*. Consider the following alternative definition of statistical distance: $\mathrm{SD}(P,Q) = \mathrm{E}_{x\sim P}\max\{0, 1-\frac{Q(x)}{P(x)}\}$. The H-Technique approach considers a smooth variant of the above formulation: small events with respect to P are ignored. However, while smooth KL-divergence is useful in settings when the actual KL-divergence might be *unbounded*, as in our settings, the above smooth variant of statistical distance is always very close to the actual statistical distance, and as such, it is more of a tool for bounding statistical distance than a measure of interest for its own sake.

1. $\Pr_{x \sim P}[F_P(x) \neq x] \leq \alpha$.
2. $\forall x \in \mathcal{U}$: $\operatorname{Supp}(F_P(x)) \cap \mathcal{U} \subseteq \{x\}$ and $\operatorname{Supp}(F_Q(x)) \cap \mathcal{U} \subseteq \{x\}$.

Note that for any pair $(F_P, F_Q) \in \mathcal{F}$ and an event E over $\mathcal{U}$, it holds that $\Pr_Q[E] \geq \Pr_{F_Q(Q)}[E]$, and $\Pr_{F_P(P)}[E] \geq \Pr_P[E] - \alpha$. Thus, if $\Pr_P[E]$ is high, a bound on $D(F_P(P)||F_Q(Q))$ implies that $\Pr_Q[E]$ is high as well. Namely, large events in P happen with high probability also in Q.

Of course, it might be difficult to bound the KL-divergence for any such pair (F_P, F_Q), since we now must consider also the elements outside $\mathcal{U}$. We leave further details on how to achieve such a bound to the body of this work and steer our attention back to bounding the divergence between Ideal and Real′. In the remainder of this discussion we allow ourselves to assume that some bad events, as long as they occur with small probability under P, are irrelevant.

2.2.3 Bounding the Smooth KL-divergence Between Ideal and Real′

We pick up from Equation (7)—where we derived a bound on the KL-divergence between the "Z-part" of Ideal and that of Real′—with the difference that now we consider the smooth variant of the KL-divergence:

$$D^{\varepsilon}(Z^k|_W||Z^k|_{X_I=1,W}) \leq \mathrm{E}_{X^k|W}\left[\log \frac{1}{1+\Delta}\right] \tag{9}$$

The fact that we are bounding only the smooth KL-divergence essentially allows us to assume that $|\Delta| \leq 1/2$. Using that $-\log(1+x) \leq -x + x^2$ for all $-1/2 \leq x \leq 1/2$,[15] it holds that

$$\begin{aligned} D^{\varepsilon}(Z^k|_W||Z^k|_{X_I=1,W}) &\leq \mathrm{E}_{X^k|_W}\left[-\Delta + \Delta^2\right] \\ &= \mathrm{E}_{X^k|_W}\left[\Delta^2\right], \end{aligned} \tag{10}$$

where we used that $\mathrm{E}_{X^k|_W}[\Delta] = 0$.

So, our goal is to bound $\mathrm{E}_{X^k|_W}\left[\Delta^2\right]$ with some function of $D(X^k|_W||X^k)$. Specifically, we sketch how to derive the following bound:

$$\mathrm{E}_{X^k|_W}\left[\Delta^2\right] \leq \frac{m}{k} \cdot D(X^k|_W||X^k) \tag{11}$$

Before deriving the above inequality, let's use it to show a contradiction. We do so by using the chain rule for KL-divergence and moving back to Real (instead of Real′). Then, Equation (11) implies that

$$D(\text{Ideal}\,||\,\text{Real}) \leq \frac{m}{k} \cdot D(Z^k X^{m \times k}|_W||Z^k X^{m \times k}) \leq \frac{m}{k} \cdot \log \frac{1}{\Pr[W]} \tag{12}$$

Similar calculations to the ones in the public-coin setting (Equation (3)) show that

$$\Pr[\text{Succ}(\text{Real})] \geq \Pr[W]^{m/k} \geq 1 - \varepsilon \tag{13}$$

where we used the assumption that $\Pr[W] \geq (1-\varepsilon)^{k/m}$, and which yields a contradiction. The factor of m difference in the exponent between this bound and the one in Equation (3) (i.e., $\Pr[W]^{1/k}$) is

[15] All logarithms in this paper are natural logarithms.

exactly the reason we must assume that $\Pr[W] \geq (1-\varepsilon)^{k/m}$ (rather than $(1-\varepsilon)^k$ in the public-coin case). This is the cause for the non-optimal exponent in our result (i.e., exponent of k/m rather than k), which we also show is necessary (see Theorem 1.3).

We now proceed to derive Equation (11). In fact, we derive the following weaker bound:

$$\mathrm{E}_{X^k|_W}\left[\Delta^2\right] \leq \frac{m}{k} \cdot \Big(D(X^k|_W||X^k) + 1\Big) \tag{14}$$

Namely, we derive an additional additive loss of m/k, which is actually necessary.[16] To bound the effect of this loss, we assume for now that $k > c \cdot m^2/\varepsilon$ for some large enough constant c; in Section 2.2.5 we explain how to eliminate this assumption. When this loss is accumulated for every round (when using the chain rule), the right-hand side of Equation (12) becomes $\frac{m}{k} \log \frac{1}{\Pr[W]} + \varepsilon/c$. Such a bound still allows us to achieve exponential decay of $(1-\varepsilon)^{\Omega(m/k)}$, albeit with a slightly worse constant in the exponent.

To derive Equation (14), we use the following inequality, due to Donsker and Varadhan [DV83]:[17]

$$\mathrm{E}_P[f(X)] \leq \log \mathrm{E}_Q[\exp(f(X))] + D(P||Q) \tag{15}$$

for any distributions P and Q with $D(P||Q) < \infty$ and any f with $\mathrm{E}_Q[\exp(f(X))] < \infty$. An immediate choice for deriving Equation (14) using the above inequality would be $P = X^k|_W$ and $Q = X^k$. For this choice to work, however, we must show that Δ has super-exponential moment (i.e., $\mathrm{E}[\exp(\Delta^2)] < \infty$) under X^k. Since this moment exists for well-concentrated random variables (i.e., sub-Gaussian random variables), it suffices to argue that Δ is well-concentrated. We prove this concentration under the (simpler) distribution $\prod_{i=1}^k X_i|_W$, the product distribution of the marginals of $X^k|_W$. This suffices to derive Equation (14) since X^k is a product distribution and the chain rule for KL-divergence implies that

$$D(X^k|_W||X^k) \geq D(X^k|_W|| \prod_{i=1}^k X_i|_W) \tag{16}$$

So, we wish to show that Δ is concentrated under $\prod_{i=1}^k X_i|_W$; equivalently, we argue that Y under $\prod_{i=1}^k X_i|_W$ is concentrated. Since under $\prod_{i=1}^k X_i|_W$ the random variable $Y = \sum_{i=1}^k Y_i$ is a sum of *independent* random variables, we can use standard concentration bounds (e.g., Hoeffding's inequality) to show that Δ is concentrated. However, such bounds require the Y_i's to be bounded, and if $p_i = \Pr[X_i = 1|W]$ is very small, then Y_i, which is equal to $1/p_i$ with probability p_i, might be huge. Here again we use the fact that we bound the smooth KL-divergence—we can show (see Section 7 for details) that for most i's, $p_i \approx 1/m$. Thus, we can assume that the index i sampled by the prover is not one of these "bad" indexes—for which $p_i \not\approx 1/m$, and Y would be summed only over non-bad indexes.

Actually, even after the concentration bounds are applied, large values of Δ are not sufficiently concentrated. Specifically, those bounds show that Δ is a sub-exponential random variable, for which the super-exponential moment might not exist (if Δ were sub-Gaussian, such a bound would exist). It turns out that we can avoid the loss in concentration for large Δ using our assumption

[16] If $\Pr[W] = 1$, it holds that $D((X^k|_W)||X^k) = 0$, but the divergence $D(X^k|_W||X^k|_{X_I=1,W})$ roughly equals m/k.

[17] The original theorem by Donsker and Varadhan [DV83] (see Theorem A.2) is stronger; it states the following variational characterization for KL-divergence: $D(P||Q) = \sup_f \mathrm{E}_P[f(X)] - \log \mathrm{E}_Q[\exp(f(X))]$.

that $|\Delta| \leq 1/2$ under $X^k|_W$, and we indeed show that the super-exponential moment of Δ is bounded; that is, $\mathrm{E}_{\prod_{i=1}^k X_i|_W}\left[\exp(\Delta^2/(m/k))||\Delta| \leq 1/2\right] \leq e$. This bound would also suffice to establish Equation (14). We leave further details to the body of this paper.

2.2.4 Bounding the Smooth KL-Divergence Induced by Next Rounds

So far we have only focused on bounding the smooth KL-divergence between the Ideal and Real′ distributions induced by the first round of the protocol. In this part we explain how to extend the first round analysis for the next (non-first) rounds. We bound the smooth KL-divergence between the Ideal and Real′ distributions induced by next rounds by reducing it to the first round case, a reduction that we believe to be of interest for amplification of arbitrary interactive arguments and proofs.

The main challenge for analyzing the non-first rounds is that the distribution of I conditioned on the previous rounds is not necessarily uniform.[18] (Recall that I is the index of the real interaction embedded as one of the k interactions). The uniformity of I was critical for our first round analysis (for instance, in Equations (5) and (6)). When bounding the divergence induced by non-first rounds, however, we do that *conditioned on the previous rounds' coins.* This conditioning might leak information about the value of I, making it non-uniform under the conditioning, and the analysis becomes much more complicated.

One way to tackle the above is to assume that the distribution of I conditioned on previous rounds is uniform, and pay the statistical distance per round between the uniform distribution and the actual (conditioned) distribution of I. This approach was taken by Håstad *et al.* [Hås+10] and Haitner [Hai13], but the cost of moving to the uniform distribution in each round yields a non-optimal bound.

Here we take a more holistic approach to perform the per-round analysis without assuming that I is uniform. In particular, we prove the following fact on the distribution of I conditioned on the previous rounds: with high probability over $z^k x^{m\times k} = (z^k, x_1^k, \ldots, x_m^k) \sim \text{Ideal}$, the following holds for most $i \in [k]$:

$$\forall j \in [m]: \qquad \Pr_{\text{Real}'}\left[I = i \mid Z^k X_{<j}^k = z^k x_{<j}^k\right] \in \Theta(1/k) \tag{17}$$

That is, in all rounds the distribution of I in Real′ under the conditioning is close (up to a constant multiplicative factor) to being uniformly distributed over a very large set of indices. Note that $z^k x^{m\times k}$ is sampled according to Ideal, since we are bounding $D(\text{Ideal}\,||\,\text{Real}')$, in which the previous rounds are sampled according to Ideal, where the conditioning of I is on $\text{Real}'(Z^k X_{<j}^k) = z^k x_{<j}^k$, since we care about the distribution of I in Real′ under the conditioning (note that I is not even defined in Ideal).

The characterization given in Equation (17) is strong enough so that we can employ the strategy we described for the first round in all other rounds. Hence, proving that it holds with high probability over $z^k x^{m\times k} \sim \text{Ideal}$, as we argue below, yields that the smooth KL-divergence between

[18] For instance, let $m = 2$ and assume that if $X_{2,1} = 1$ then the adversary P^{k^*} fails unless $X_{1,i} = 1 \vee X_{2,i} = 1$ for all $i \in [k]$ (i.e., P^{k^*} does not fail in this case only if all the k verifiers abort). Since the probability that all verifiers abort in a uniform execution is much smaller than the assumed winning probability of P^{k^*}, we expect the number of ones in $x_1^k \sim \text{Ideal}_1$ to be $\approx k/2$. On the other hand, a simple calculation yields that the expected number of ones in $x_1^k \sim \text{Real}'_1|_{I=1}$ is $\approx 2k/3$. This means that for a typical $\approx k/2$ ones $x_1^k \sim \text{Ideal}_1$, the probability that $I = 1$ conditioned on $\text{Real}'_1 = x_1^k$ is tiny, much smaller than the $1/k$ probability this event has with respect to a uniform I.

Ideal and Real$'$ is small. The proof of Equation (17) is the main technical part of our paper. To a large extent it is rather general, not limited to the proof system under consideration, and we hope it will find applications in other parallel repetition theorems.

Proving Equation (17). We present a rather general approach for proving Equation (17) that might be of use for other parallel repetition proofs. In particular, we prove the following fact.

Proposition 2.1 (informal)**.** *Let P be a distribution over an m-size tuple $(Y_1, \ldots, Y_m)$ and let $\{E_{j,i}\}_{j\in[m],i\in[k]}$ be a set of (arbitrary) events over P. Let Q be the distribution defined by the following process:*

1. *Sample uniformly $I \sim [k]$.*
2. *For $j = 1$ to m: sample $y_j \sim Y_j|_{Y_{<j}=y_{<j},E_{j,I}}$.*
3. *Output $(y_1, \ldots, y_m)$.*

Finally, let $\alpha_{j,i}(y_{\leq j}) = \prod_{j'=1}^{j} \frac{\Pr_P[E_{j',i}|Y_{\leq j'}=y_{\leq j'}]}{\Pr_P[E_{j',i}|Y_{<j'}=y_{<j'}]}$. Then

- *For all $i \in [k]$: the sequence $\alpha_{0,i} = 1, \alpha_{1,i}(Y_{\leq 1}), \ldots, \alpha_{m,i}(Y_{\leq m})$ is a martingale sequence with respect to P (i.e., $\mathrm{E}_{P_{Y_j|Y_{<j}}}[\alpha_{j,i}(Y_{\leq j}))] = \alpha_{j-1,i}(Y_{<j})$ for all $j \in [m]$).*
- *For all $i \in [k]$, $j \in [m]$ and $y_{\leq j} \in \mathrm{Supp}(Y_{\leq j})$: $\Pr_Q[I = i \mid Y_{\leq j} = y_{\leq j}] = \frac{\alpha_{j,i}(y_{\leq j})}{\sum_{i'=1}^{k} \alpha_{j,i'}(y_{\leq j})}$.*

By letting $P = \text{Ideal}$ (and thus $(Y_1, \ldots, Y_{m+1}) = (Z^k, X_1^k, \ldots, X_m^k)|_W$), and letting $E_{j,i}$ be the event that $X_{j,i} = 1$, we get $Q \equiv \text{Real}'$. Proposition 2.1 characterizes the conditional distribution of I in terms of $\{\alpha_{j,i}\}$. For this choice of P and $\{E_{j,i}\}$, we are able to prove that for most i's the martingale sequence $\alpha_{0,i}, \alpha_{1,i}, \ldots, \alpha_{m,i}$ is well concentrated around its mean (i.e., 1). It follows that for most i's it holds that $\Pr_Q[I = i \mid Y_{\leq j} = y_{\leq j}] \approx 1/k$ holds simultaneously for all $j \in [m]$, and Equation (17) follows.[19]

2.2.5 Small Number of Repetitions

Recall that the analysis above requires the number of repetitions, k, to be at least m^2/ε. In the following we explain how to handle arbitrary numbers of repetitions by reducing the analysis to a variant of the large number of repetitions case. The reduction is applicable to any "natural" hardness amplification proof, and not only the one considered above.

Let $k < m^2/\varepsilon$, and let P^{k^*} be an adversary violating the noticeable $(1-\varepsilon)^{k/m}$ soundness error of $\widetilde{\pi}^k$. Let $\ell = m^2/(\varepsilon k)$, and assume for simplicity that $\ell \in \mathbb{N}$. Consider the "product" cheating prover $\mathrm{P}^{\ell k^*}$ that attacks protocol $\widetilde{\pi}^{k\ell}$ by invoking ℓ independent copies of P^{k^*}, one for each k copies of $\widetilde{\pi}$ in $\widetilde{\pi}^{\ell k}$. It is clear that $\mathrm{P}^{\ell k^*}$ breaks the soundness of $\widetilde{\pi}^{k\ell}$ with probability greater than $(1-\varepsilon)^{\ell k/m}$. This, however, does not immediately result in a contradiction to the large number of repetitions case, since it might be that $(1-\varepsilon)^{\ell k/m}$ is not noticeable (even if $(1-\varepsilon)^{k/m}$ is), and our result requires the success probability to be noticeable. In particular, what fails in the proof for

[19] Actually, for proving Equation (17) we also need to show that for all $j \in [m]$, $\sum_{i'\in\mathcal{B}} a_{j,i'}$ is not too large (namely, not more than $\Theta(k)$), where $\mathcal{B}$ is the (small) set of i's that do have large jumps in their sequence $\alpha_{0,i}, \alpha_{1,i}, \ldots, \alpha_{m,i}$. We leave further details to the actual proof.

not noticeable $(1-\varepsilon)^{\ell k/m}$ is that the rejection sampling in each round might not run in polynomial time. Fortunately, we prove that for the specific product prover $\mathrm{P}^{\ell k^*}$ defined above, the rejection sampling can be done efficiently: since $\mathrm{P}^{\ell k^*}$ invokes ℓ independent copies of P^{k^*}, the rejection sampling can be done *independently* for each copy. By assumption, the probability of breaking the soundness of each copy, i.e., $(1-\varepsilon)^{k/m}$, is noticeable. Thus, each of the ℓ sampling tasks can be carried out in polynomial time, and thus the whole sampling process runs in polynomial time.

3 Preliminaries

3.1 Notation

We use calligraphic letters to denote sets, uppercase for random variables, and lowercase for values and functions. All logarithms considered here are natural logarithms (i.e., in base e). For $a \in \mathrm{R}$ and $b \geq 0$, let $a \pm b$ stand for the interval $[a-b, a+b]$. Given sets $\mathcal{S}_1, \ldots, \mathcal{S}_k$ and k-input function f, let $f(\mathcal{S}_1, \ldots, \mathcal{S}_k) := \{f(x_1, \ldots, x_j) \colon x_i \in \mathcal{S}_i\}$, e.g., $f(1 \pm 0.1) = \{f(x) \colon x \in [.9, 1.1]\}$. For $n \in \mathbb{N}$, let $[n] := \{1, \ldots, n\}$ and $(n) := \{0, \ldots, n\}$.

Let poly denote the set all polynomials, PPT denote for probabilistic polynomial time, and PPTM denote a PPT algorithm (Turing machine). A function $\nu \colon \mathbb{N} \to [0,1]$ is *negligible*, denoted $\nu(n) = \operatorname{neg}(n)$, if $\nu(n) < 1/p(n)$ for every $p \in \operatorname{poly}$ and large enough n. Function ν is *noticeable*, denoted $\nu(n) \geq 1/\operatorname{poly}(n)$, if exists $p \in \operatorname{poly}$ such that $\nu(n) \geq 1/p(n)$ for all n.

We denote by $v^n = (v_1, \ldots, v_n)$ a vector of length n and by $v^{m \times n} = (v_1^n, \ldots, v_m^n)$ a matrix of size $m \times n$. We sometimes write 0^n as the n-bit vector $(0, \ldots, 0)$ (same for 1^n). Given a binary vector $v^n \in \{0,1\}^n$, we sometimes treat v^n as a set and write $1 \in v^n$ (meaning that $v^n \neq 0^n$), and define $1_{v^n} := \{i \in [n] \colon v_i = 1\}$.

3.2 Distributions and Random Variables

A discrete random variable X over $\mathcal{X}$ is sometimes defined by its probability mass function (pmf) P_X (P is an arbitrary symbol). A conditional probability distribution is a function $P_{Y|X}(\cdot|\cdot)$ such that for any $x \in \mathcal{X}$, $P_{Y|X}(\cdot|x)$ is a pmf over $\mathcal{Y}$. The joint pmf P_{XY} can be written the product $P_X P_{Y|X}$, where $(P_X P_{Y|X})(x,y) = P_X(x) P_{Y|X}(y|x) = P_{XY}(xy)$. The marginal pmf P_Y can be written as the composition $P_{Y|X} \circ P_X$, where $(P_{Y|X} \circ P_X)(y) = \sum_{x \in \mathcal{X}} P_{Y|X}(y|x) P_X(x) = P_Y(y)$. We denote by $P_X[W]$ the probability that an event W over P_X occurs, and given a set $\mathcal{S} \subseteq \mathcal{X}$ we define $P_X(\mathcal{S}) = P_X[X \in \mathcal{S}]$. The support of a distribution P over a finite set $\mathcal{X}$, denoted $\operatorname{Supp}(P)$, is defined as $\{x \in \mathcal{X} : P(x) > 0\}$. The *statistical distance* of two distributions P and Q over a finite set $\mathcal{X}$, denoted as $\operatorname{SD}(P,Q)$, is defined as $\max_{\mathcal{S} \subseteq \mathcal{X}} |P(\mathcal{S}) - Q(\mathcal{S})| = \frac{1}{2} \sum_{x \in \mathcal{S}} |P(x) - Q(x)|$.

Given a set $\mathcal{S}$, let $U_{\mathcal{S}}$ denote the uniform distribution over the elements of $\mathcal{S}$, and for $n \in \mathbb{N}$ let $U_n := U_{\{0,1\}^n}$. We sometimes write $x \sim \mathcal{S}$ or $x \leftarrow \mathcal{S}$, meaning that x is uniformly drawn from $\mathcal{S}$. For $p \in [0,1]$, let $\operatorname{Bern}(p)$ be the Bernoulli distribution over $\{0,1\}$, taking the value 1 with probability p. For $n \in \mathbb{N}$ and $p \in [0,1]$, let $\operatorname{Bin}(n,p)$ be the binomial distribution induces by the sum of n independent random variables, each is distributed according to $\operatorname{Bern}(p)$. Given a boolean statement S (e.g., $X \geq 5$), let $\mathbb{1}\{S\}$ be the indicator function that outputs 1 if S is a true statement and 0 otherwise.

We use the following fact.

Claim 3.1. *Let P_{XYZ} be a probability distribution over $\mathcal{X} \times \mathcal{Y} \times \{0,1\}$ such that $P_{Z|X} = \mathrm{Bern}(P_{Y|X}[f(Y)=1])$, for some boolean function $f\colon \mathcal{Y} \to \{0,1\}$. Then $P_{X|Z=1} \equiv P_{X|f(Y)=1}$.*

Namely, $Z=1$ implies that X is distributed as $X|f(Y)=1$.[20]

Proof. Fix $x \in \mathcal{X}$ and compute

$$\begin{aligned}
P_{X|Z}(x|1) &= P_{Z|X}(1|x) \cdot \frac{P_X(x)}{P_Z(1)} \\
&= P_{Y|X=x}[f(Y)=1] \cdot \frac{P_X(x)}{P_Y[f(Y)=1]} \\
&= \sum_{y \in \mathcal{Y}\colon f(y)=1} P_{Y|X}(y|x) \cdot \frac{P_X(x)}{P_Y[f(Y)=1]} \\
&= \sum_{y \in \mathcal{Y}\colon f(y)=1} \frac{P_Y(y)}{P_Y[f(Y)=1]} \cdot P_{X|Y}(x|y) \\
&= \sum_{y \in \mathcal{Y}\colon f(y)=1} P_{Y|f(Y)=1}(y) \cdot P_{X|Y}(x|y) \\
&= \mathrm{E}_{P_{Y|f(Y)=1}}\left[P_{X|Y}(x)\right] \\
&= P_{X|f(Y)}(x|1)
\end{aligned}$$

□

3.2.1 KL-Divergence

Definition 3.2. *The* divergence *(a.k.a. Kullback-Leibler divergence or relative entropy) between two distributions P, Q on a discrete alphabet $\mathcal{X}$ is*

$$D(P||Q) = \sum_{x \in \mathcal{X}} P(x) \log \frac{P(x)}{Q(x)} = \mathrm{E}_{x \sim P} \log \frac{P(x)}{Q(x)},$$

where $0 \cdot \log \frac{0}{0} = 0$ and if there exists $x \in \mathcal{X}$ such that $P(x) > 0 = Q(x)$ then $D(P||Q) = \infty$.

Definition 3.3. *For any $p, q \in [0,1]$ we define $D(p||q) := D(\mathrm{Bern}(p)||\,\mathrm{Bern}(q))$.*

Definition 3.4. *Let P_{XY} and Q_{XY} be two probability distributions over $\mathcal{X} \times \mathcal{Y}$. The* conditional divergence *between $P_{Y|X}$ and $Q_{Y|X}$ is*

$$D(P_{Y|X}||Q_{Y|X}|P_X) = \mathrm{E}_{x \sim P_X}[D(P_{Y|X=x}||Q_{Y|X=x})] = \sum_{x \in \mathcal{X}} P_X(x) D(P_{Y|X=x}||Q_{Y|X=x}).$$

Fact 3.5 (Properties of divergence)**.** *P_{XY} and Q_{XY} be two probability distributions over $\mathcal{X} \times \mathcal{Y}$. It holds that:*

1. *(Information inequality) $D(P_X||Q_X) \geq 0$, with equality holds iff $P_X = Q_X$.*

[20] Note that Z is distributed as $f(Y)$ but is not necessarily equal to $f(Y)$ (i.e., it might be possible to draw X, Y, Z such that $Z \neq f(Y)$). Yet, the distributions $X|Z=1$ and $X|f(Y)=1$ are equal.

2. *(Monotonicity)* $D(P_{XY}||Q_{XY}) \geq D(P_Y||Q_Y)$.
3. *(Chain rule)*
$$D(P_{X_1 \cdots X_n}||Q_{X_1 \cdots X_n}) = \sum_{i=1}^{n} D(P_{X_i|X_{<i}}||Q_{X_i|X_{<i}}|P_{X_{<i}}).$$
If $Q_{X_1 \cdots X_n} = \prod_{i=1}^{n} Q_{X_i}$ *then*
$$D(P_{X_1 \cdots X_n}||Q_{X_1 \cdots X_n}) = D(P_{X_1 \cdots X_n}||P_{X_1}P_{X_2} \cdots P_{X_n}) + \sum_{i=1}^{n} D(P_{X_i}||Q_{X_i}).$$
4. *(Conditioning increases divergence) If* $Q_Y = Q_{Y|X} \circ P_X$ *(and* $P_Y = P_{Y|X} \circ P_X$*), then*
$$D(P_Y||Q_Y) \leq D(P_{Y|X}||Q_{Y|X}|P_X).$$
5. *(Data-processing) If* $Q_Y = P_{Y|X} \circ Q_X$ *(and* $P_Y = P_{Y|X} \circ P_X$*), it holds that*
$$D(P_Y||Q_Y) \leq D(P_X||Q_X).$$

Fact 3.6. *Let X be random variable drawn from P and let W be an event defined over P. It holds that*
$$D\big(P_{X|W}||P_X\big) \leq \log \frac{1}{P[W]}$$

Fact 3.7. *Let X, Y be random variables drawn from either P or Q and let W be an event defined over P. It holds that*
$$\mathrm{E}_{x \sim P_{X|W}} D(P_{Y|X=x}||Q_{Y|X=x}) \leq \frac{1}{P[W]} \cdot D(P_{Y|X}||Q_{Y|X}||P_X).$$

Proof.
$$\begin{aligned}
\mathrm{E}_{x \sim P_{X|W}} D(P_{Y|X=x}||Q_{Y|X=x}) &= \sum_x P_{X|W}(x) D(P_{Y|X=x}||Q_{Y|X=x}) \\
&= \sum_x \frac{P[X=x,W]}{P[W]} D(P_{Y|X=x}||Q_{Y|X=x}) \\
&\leq \sum_x \frac{P_X(x)}{P[W]} D(P_{Y|X=x}||Q_{Y|X=x}) \\
&= \frac{1}{P[W]} \cdot D(P_{Y|X}||Q_{Y|X}||P_X),
\end{aligned}$$
where the inequality follows since $P[X = x, W] \leq P_X(x)$ and $D(\cdot||\cdot) \geq 0$. □

Fact 3.8. *Let X be a random variable over $\mathcal{X}$ drawn form either P_X or Q_X and let $\mathcal{S} \subseteq \mathcal{X}$. It holds that*
$$D(P_{X|X \in \mathcal{S}}||Q_X) \leq \frac{1}{P_X(\mathcal{S})} \cdot \left(D(P_X||Q_X) + \frac{1}{e} + 1\right).$$

Proof. If $D(P_X||Q_X) = \infty$, then the statement holds trivially. Assume that $D(P_X||Q_X) < \infty$ and compute

$$\begin{aligned} D(P_{X|X\in\mathcal{S}}||Q_X) &= \sum_{x\in\mathcal{S}} P_{X|X\in\mathcal{S}}(x)\log\frac{P_{X|X\in\mathcal{S}}(x)}{Q_X(x)} \\ &= \sum_{x\in\mathcal{S}} \frac{P_X(x)}{P_X(\mathcal{S})}\log\frac{P_X(x)/P_X(\mathcal{S})}{Q_X(x)} \\ &= \sum_{x\in\mathcal{S}} \frac{P_X(x)}{P_X(\mathcal{S})}\log\frac{1}{P_X(\mathcal{S})} + \sum_{x\in\mathcal{S}} \frac{P_X(x)}{P_X(\mathcal{S})}\log\frac{P_X(x)}{Q_X(x)}. \end{aligned}$$

To bound the left sum, compute

$$\begin{aligned} \sum_{x\in\mathcal{S}} \frac{P_X(x)}{P_X(\mathcal{S})}\log\frac{1}{P_X(\mathcal{S})} &\leq \sum_{x\in\mathcal{S}} \frac{P_X(x)}{P_X(\mathcal{S})}\cdot\frac{1}{P_X(\mathcal{S})} \\ &\leq \frac{1}{P_X(\mathcal{S})}, \end{aligned}$$

where the first inequality follows since $\log(x) \leq x$ for all x.

To bound the right sum, compute

$$\begin{aligned} \sum_{x\in\mathcal{S}} \frac{P_X(x)}{P_X(\mathcal{S})}\log\frac{P_X(x)}{Q_X(x)} &= \frac{1}{P_X(\mathcal{S})}\left(\sum_{x\in\mathcal{S}} P_X(x)\log\frac{P_X(x)}{Q_X(x)} + \sum_{x\notin\mathcal{S}} P_X(x)\log\frac{P_X(x)}{Q_X(x)} - \sum_{x\notin\mathcal{S}} P_X(x)\log\frac{P_X(x)}{Q_X(x)}\right) \\ &= \frac{1}{P_X(\mathcal{S})}\left(D(P_X||Q_X) - \sum_{x\notin\mathcal{S}} P_X(x)\log\frac{P_X(x)}{Q_X(x)}\right). \end{aligned}$$

The following calculation completes the proof:

$$\begin{aligned} \sum_{x\notin\mathcal{S}} P_X(x)\log\frac{P_X(x)}{Q_X(x)} &= \sum_{x\notin\mathcal{S}} Q_X(x)\frac{P_X(x)}{Q_X(x)}\log\frac{P_X(x)}{Q_X(x)} \\ &\geq \sum_{x\notin\mathcal{S}} Q_X(x)(-e^{-1}) \\ &\geq -e^{-1}, \end{aligned}$$

where the first inequlity holds since $x\log(x) \geq -e^{-1}$ for all $x > 0$. □

Fact 3.9 ([Mul, Implicit in Corollary 3.2 to 3.4])**.** *For any $p \in [0,1]$ it holds that*

1. *$D((1-\delta)p||p) \geq \frac{1}{2}\delta^2 p$ for any $\delta \in [0,1]$.*
2. *$D((1+\delta)p||p) \geq \frac{1}{4}\min\{\delta,\delta^2\}p$ for any $\delta \in [0,\frac{1}{p}-1]$.*

The proof of the following proposition is given in Appendix A.1.

Proposition 3.10. *Let X be a random variable drawn form either P or Q. Assume that $\Pr_P[|X| \leq 1] = 1$ (i.e., if X is drawn from P then $|X| \leq 1$ almost surely) and that there exist $\varepsilon, \sigma^2, K_1, K_2 > 0$ such that $\Pr_Q[|X| \leq 1] \geq 1 - \varepsilon$ and*

$$\Pr_Q[|X| \geq t] \leq K_2 \cdot \exp\left(-\frac{t^2}{K_1\sigma^2}\right) \quad \text{for all } 0 \leq t \leq 1.$$

Then, there exists $K_3 = K_3(K_1, K_2, \varepsilon) > 0$ such that

$$\mathrm{E}_P[X^2] \leq K_3 \cdot \sigma^2 \cdot (D(P||Q) + 1).$$

Smooth KL-divergence. We put forth the following definition of smooth KL-divergence.

Definition 3.11 (α-*smooth* divergence)**.** *Let P and Q be two distributions over a universe $\mathcal{U}$ and let $\alpha \in [0,1]$. The α-*smooth divergence *of P* and *Q, denoted $D^{\alpha}(P||Q)$, is defined as $\inf_{(F_P,F_Q)\in\mathcal{F}}\{D(F_P(P)||F_Q(Q))\}$, for $\mathcal{F}$ being the set of randomized functions pairs such that for every $(F_P, F_Q) \in \mathcal{F}$:*

1. $\Pr_{x\sim P}[F_P(x) \neq x] \leq \alpha$*, where the probability is also over the coins of F_P.*

2. $\forall x \in \mathcal{U}$*:* $\mathrm{Supp}(F_P(x)) \cap \mathcal{U} \subseteq \{x\}$ *and* $\mathrm{Supp}(F_Q(x)) \cap \mathcal{U} \subseteq \{x\}$*.*

As any useful measure, smooth KL-divergence has data-processing properties.

Proposition 3.12 (Data processing of smooth KL-divergence)**.** *Let P and Q be two distributions over a finite universe $\mathcal{U}$, let $\alpha \in [0,1]$ and let H be a randomized function over $\mathcal{U}$ with finite range. Then $D^{\alpha}(H(P)||H(Q)) \leq D^{\alpha}(P||Q)$.*

Proof. Let (F_P, F_Q) be a pair of functions such that

1. $\Pr_{x\sim P}[F_P(x) \neq x] \leq \alpha$, and

2. $\forall x \in \mathcal{U}$: $\mathrm{Supp}(F_P(x)) \cap \mathcal{U} \subseteq \{x\}$ and $\mathrm{Supp}(F_Q(x)) \cap \mathcal{U} \subseteq \{x\}$.

We assume without loss of generality that for both $T \in \{P, Q\}$:

$$\forall x \in \mathcal{U} : \ \mathrm{Supp}(F_T(x)) \cap \mathrm{Supp}(H(x)) \subseteq \{x\}. \tag{18}$$

Indeed, since $F_T(x) \neq x$ implies $F_T(x) \notin \mathcal{U}$, one can add a fixed prefix to the value of $F_T(x)$ when $F_T(x) \neq x$ (same prefix for both $T \in \{P, Q\}$) such that Equation (18) holds (recall that $\mathrm{Supp}(H(\mathcal{U}))$ is finite). Such a change neither effect the properties of F_P and F_Q stated above, nor the value of $D(F_P(P)||F_Q(Q))$.

For $T \in \{P, Q\}$, let $G_T(y)$ be the randomized function defined by the following processes:

a. Sample $x \sim T_{X|H(X)=y}$.

b. Sample $z \sim F_T(x)$.

c. If $z = x$, output y.

Else, output z.

By construction and Equation (18), for both $T \in \{P, Q\}$:

$$\forall y \in H(\mathcal{U}) : \mathrm{Supp}(G_T(y)) \cap H(\mathcal{U}) \subseteq \{y\}. \tag{19}$$

Let $Y_T = H(T)$ and let X_T be the value of x in a random execution of $G_T(Y_T)$. It is clear that $X_T \sim T$. We note that

$$\begin{aligned} \Pr[G_P(Y_P) \neq Y_P] &= \Pr[F_P(X_P) \neq X_P] \\ &= Pr_{x\sim P}[F_P(x) \neq x] \\ &\leq \alpha. \end{aligned} \tag{20}$$

The inequality is by the assumption about F_P.

Consider the randomized function $K(z)$ that outputs $H(z)$ if $z \in \mathcal{U}$, and otherwise outputs z. It holds that

$$\begin{aligned} \Pr[K(F_T(T)) = z] &= \Pr[F_T(T) \in \mathcal{U}] \cdot \Pr[H(F_T(T)) = z | F_T(T) \in \mathcal{U}] \\ &\quad + \Pr[F_T(T) \notin \mathcal{U}] \cdot \Pr[F_T(T) = z | F_T(T) \notin \mathcal{U}] \\ &= \Pr[F_T(T) = T] \cdot \Pr[H(T) = z | F_T(T) = T] \\ &\quad + \Pr[F_T(T) \neq T] \cdot \Pr[F_T(T) = z | F_T(T) \neq T], \end{aligned}$$

where the second inequality follows from the second property of (F_P, F_Q); namely, $F_T(T) \in \mathcal{U} \iff F_T(T) = T$. Similarly,

$$\begin{aligned} \Pr[G_T(H(T)) = z] &= \Pr[F_T(X_T) = X_T] \cdot \Pr[H(X_T) = z | F_T(X_T) = X_T] \\ &\quad + \Pr[F_T(X_T) = X_T] \cdot \Pr[F_T(X_T) = z | F_T(X_T) \neq X_T]. \\ &= \Pr[F_T(T) = T] \cdot \Pr[H(T) = z | F_T(T) = T] \\ &\quad + \Pr[F_T(T) \neq T] \cdot \Pr[F_T(T) = z | F_T(T) \neq T], \end{aligned}$$

where the second inequality holds since $X_T \sim T$. Hence, we have $G_T(H(T)) \equiv K(F_T(T))$. Thus, the data-processing inequality for (standard) KL-divergence implies that

$$\begin{aligned} D(F_P(P) || F_Q(Q)) &\geq D(K(F_P(P)) || K(F_Q(Q))) \\ &= D(G_P(H(P)) || G_Q(H(Q))). \end{aligned} \tag{21}$$

The proof then follows by Properties (19), (20), (21) of G_P and G_Q. □

The following fact states that small smooth KL-divergence guarantees that large events with respect to the left-hand distribution happen with high probability also with respect to the right-hand distribution.

Proposition 3.13. *Let P and Q be two distributions over a universe $\mathcal{U}$. Assume that*

1. $\Pr_{x\sim P}[x \notin \mathcal{S}] \leq \beta$ *and*
2. $D^{\alpha}(P||Q) < \frac{\alpha+\beta}{4}$.

for some $\mathcal{S} \subseteq \mathcal{U}$ and $\alpha, \beta \in [0, 1]$. Then $\Pr_{x\sim Q}[x \notin \mathcal{S}] < 2(\alpha + \beta)$.

Proof. Assume that $\alpha+\beta \leq \frac{1}{2}$, since otherwise the proof trivially holds. By the second assumption, there exist randomized function F_P, F_Q satisfying

a. $D(F_P(P)||F_Q(Q)) < \frac{\alpha+\beta}{4}$ and

b. $\Pr_{x\sim P}[F_P(x) \neq x] \leq \alpha$ and

c. $\forall x \in \mathcal{U}$: $\mathrm{Supp}(F_P(x)) \cap \mathcal{U}, \mathrm{Supp}(F_Q(x)) \cap \mathcal{U} \subseteq \{x\}$.

By Property a of F_P, F_Q along with Fact 3.5(5) (data-processing), it holds that

$$D(\mathbb{1}\{F_P(P) \notin \mathcal{S}\}||\mathbb{1}\{F_Q(Q) \notin \mathcal{S}\}) < \frac{\alpha+\beta}{4} \tag{22}$$

Observe that by Property b and Property c of F_P, and by the assumption that $\Pr_{x\sim P}[x \notin \mathcal{S}] \leq \beta$, it holds that

$$\Pr_{x\sim P}[F_P(x) \notin \mathcal{S}] \leq \Pr_{x\sim P}[F_P(x) \neq x] + \Pr_{x\sim P}[x \notin \mathcal{S}] \leq \alpha+\beta \tag{23}$$

Assume towards a contradiction that $\Pr_{x\sim Q}[F_Q(x) \notin \mathcal{S}] \geq 2(\alpha+\beta)$. Then by Equations (22) and (23) it holds that

$$D(\alpha+\beta||2(\alpha+\beta)) \leq D(\mathbb{1}\{F_P(P) \notin \mathcal{S}\}||\mathbb{1}\{F_Q(Q) \notin \mathcal{S}\}) < \frac{\alpha+\beta}{4},$$

in contradiction to the fact that $D(\alpha+\beta||2(\alpha+\beta)) \geq \frac{\alpha+\beta}{4}$ (follows by Fact 3.9). Hence, we conclude that

$$\Pr_{x\sim Q}[x \notin \mathcal{S}] \leq \Pr_{x\sim Q}[F_Q(x) \notin \mathcal{S}] < 2(\alpha+\beta),$$

as required, where the first inequality follows by Property c of F_Q. □

3.3 Some Concentration Bounds

3.3.1 Sum of Independent Random Variables

Fact 3.14 (Hoeffding's inequality)**.** *Let $X = X_1 + \cdots + X_n$ be the sum of independent random variables such that $X_i \in [a_i, b_i]$. Then for all $t \geq 0$:*

1. $\Pr[X - \mathrm{E}[X] \geq t] \leq \exp\left(-\frac{2t^2}{\sum_{i=1}^n (b_i-a_i)^2}\right)$.

2. $\Pr[|X - \mathrm{E}[X]| \geq t] \leq 2\exp\left(-\frac{2t^2}{\sum_{i=1}^n (b_i-a_i)^2}\right)$.

Fact 3.15 ([CO13, Theorem 5.3])**.** *Let $X \sim \mathrm{Bin}(n,p)$, then for all $t \geq 0$:*

1. $\Pr[X \geq \mathrm{E}[X] + t] \leq \exp\left(-\frac{t^2}{2\left(np+\frac{t}{3}\right)}\right)$.

2. $\Pr[X \leq \mathrm{E}[X] - t] \leq \exp\left(-\frac{t^2}{2np}\right)$.

Fact 3.16 ([CL02, Lemma 2.1])**.** *Let $X_1, \ldots, X_n$ be independent random variables such that $X_i \sim \mathrm{Bern}(p_i)$. For $X = \sum_{i=1}^n b_i X_i$ with $b_i > 0$ we have $\mathrm{E}[X] = \sum_{i=1}^n b_i p_i$ and we define $v = \sum_{i=1}^n b_i^2 p_i$. Then for all $t \geq 0$:*

$$\Pr[|X - \mathrm{E}[X]| \geq t] \leq 2\exp\left(-\frac{t^2}{2(v+bt/3)}\right),$$

for $b = \max\{b_1, b_2, \ldots, b_n\}$.

3.3.2 Martingales

Fact 3.17 ([Das11, Theorem 14.9]). *Let $X_1, \ldots, X_n$ be a martingale sequence with $X_0 = 0$ and $\mathrm{E}\left[X_i^2\right] < \infty$ for all $i \geq 1$. Then, for every $\lambda > 0$, it holds that*

$$\Pr\left[\max_{i \in [n]} |X_i| \geq \lambda\right] \leq \frac{\mathrm{E}\left[D_n^2\right]}{\lambda^2},$$

for $D_n^2 := \sum_{j=1}^{n} (X_i - X_{i-1})^2$.

3.4 Smooth Sampling

Let $X^m = (X_1, \ldots, X_m)$ be a random variable over $\mathcal{U}^m$, and let $\mathcal{S} \subseteq \mathcal{U}^m$ be with $\Pr[X^m \in \mathcal{S}] = \varepsilon$. For $j \in [m]$ and $x^j \in \mathcal{U}^j$, let $v(x^j) = \Pr\left[X^m \in \mathcal{S} | X^j = x^j\right]$, where $X^j = (X_1, \ldots, X_j)$. Consider the following strategy for the task of choosing $(x_1, \ldots, x_m) \in \mathcal{S}$ in rounds, where the value of x_j should be chosen in the j'th round:

Algorithm 3.18 (Sam). *For $j = 1$ to m do:*

```
1. Do until a break occur:
    (a) Sample $(x'_1, \ldots, x'_m) \leftarrow (X^m | X^{j-1} = (x_1, \ldots, x_{j-1}))$.
    (b) Break the loop if $(x'_1, \ldots, x'_m) \in \mathcal{S}$
2. Set $x_j = x'_j$
```

Output $(x_1, \ldots, x_m)$.

It is clear that Sam outputs $(x_1, \ldots, x_m) \in \mathcal{S}$ with probability one. We use the following observation from [Hai13] (implicit in [Hås+10]):

Fact 3.19 ([Hai13, Proposition 2.5]). $\mathrm{E}_{(x_1, \ldots, x_m) \leftarrow \mathrm{Sam}}\left[\frac{1}{v(x_1, \ldots, x_j)}\right] = 1/\varepsilon$.

3.5 Interactive Arguments

Definition 3.20 (Interactive arguments). *A* PPT *protocol* (P, V) *is an* interactive argument *for language* $\mathrm{L} \in \mathrm{NP}$ *with* completeness α *and* soundness error β*, if the following holds:*

- $\Pr[(\mathrm{P}(w), \mathrm{V})(x) = 1] \geq \alpha(|x|)$ *for any* $(x, w) \in R_{\mathrm{L}}$.
- $\Pr[(\mathrm{P}^*, \mathrm{V})(x) = 1] \leq \beta(|x|)$ *for any* PPT P^* *and large enough* $x \notin \mathrm{L}$.

We refer to party P *as the* prover*, and to* V *as the* verifier*.*

Soundness against *non-uniform* provers is analogously defined, and all the results in this paper readily extend to this model.

Since in our analysis we only care about soundness amplification, in the following we fix L to be the empty language, and assume the input to the protocol is just a string of ones, which we refer to as the *security parameter*.

Random-terminating variant.

Definition 3.21 (Random-terminating variant, Haitner [Hai13])**.** *Let* V *be a randomized interactive algorithm, and let* $\delta \in [0,1]$*. The* δ-random-terminating variant *of* V*, denoted* $\widetilde{\mathrm{V}}$*, is defined as follows: algorithm* V *acts exactly as* V *does, but adds the following step at the beginning of each communication round and right after the final interaction round: it tosses an* $(1-\delta,\delta)$ *biased coin (i.e.,* 1 *is tossed with probability* δ*), if the outcome is one then it outputs* 1 *(i.e., accept) and halts. Otherwise, it continues as* V *would.*[21]

Parallel repetition.

Definition 3.22 (Parallel repetition)**.** *Let* (P,V) *be an interactive protocol, and let* $k \in \mathbb{N}$*. We define the* k-parallel-repetition *of* (P,V) *to be the protocol* $(\mathrm{P}^k,\mathrm{V}^k)$ *in which* P^k *and* V^k *execute* k *copies of* (P,V) *in parallel, and at the end of the execution,* V^k *accepts if all copies accept.*

4 The Parallel Repetition Theorem

In this section, we restate Theorem 1.1 and prove it using Lemma 4.9, our main technical lemma. The proof of Lemma 4.9 appears in Section 5, using facts proven in Sections 6 and 7.

Theorem 4.1 (Restatement of Theorem 1.1)**.** *Let* $\pi = (\mathrm{P},\mathrm{V})$ *be an* m*-round interactive argument with soundness error* $1-\varepsilon$*, for* $m = m(n) \in [2, \mathrm{poly}(n)]$ *and* $\varepsilon = \varepsilon(n) \in [1/\mathrm{poly}(n), 1/2]$*. Let* $\widetilde{\mathrm{V}}$ *be the* $1/m$*-random-terminating variant of* V *(according to Definition 3.21), and for* $k = k(n) \leq \mathrm{poly}(n)$*, let* $\widetilde{\pi}^k = (\mathrm{P}^k, \widetilde{\mathrm{V}}^k)$ *be the* k*-parallel repetition of* $\widetilde{\pi} = (\mathrm{P},\widetilde{\mathrm{V}})$ *(according to Definition 3.22). Then,* $\widetilde{\pi}^k$ *has soundness error* $\max\{(1-\varepsilon)^{k/c\cdot m}, \mathrm{neg}(n)\}$ *for some universal constant* $c > 0$*.*

The rest of this section is dedicated to proving Theorem 4.1. We begin with setting the stage for stating Lemma 4.9 by describing our reduction and providing relevant definitions.

Let $\pi = (\mathrm{P},\mathrm{V}), m, \varepsilon$ and k be as in the statement of Theorem 4.1, and assume that there exists a PPT cheating prover P^{k*} and $p \in \mathrm{poly}$ such that for infinity many n's,

$$\Pr\left[(\mathrm{P}^{k*},\widetilde{\mathrm{V}}^k)(1^n) = 1\right] > \max\{(1-\varepsilon)^{\frac{k}{c\cdot m}}, 1/p(n)\}, \tag{24}$$

where $c > 0$ is a constant to be determined by the analysis. We assume for simplicity that P^{k*} is deterministic, the reduction for randomized P^{k*} is done via standard means.

The following discussion is with respect to a fixed $n \in \mathbb{N}$. Assume without loss of generality that $\widetilde{\mathrm{V}}$ chooses the whole randomness of V before the interaction begins. Thus, in the beginning of each round $j \in [m]$, $\widetilde{\mathrm{V}}$ only chooses the random-terminating bit of that round, and at the end of the interaction it chooses the $(m+1)$'th coin. Let $\ell = \ell(n) \in \mathbb{N}$ be a (polynomial) bound on the number of random bits used by V in $\pi(1^n)$. Hence, a partial view of $\widetilde{\mathrm{V}}^k$ in $(\mathrm{P}^{k*},\widetilde{\mathrm{V}}^k)$ is of the form $\mathrm{view} = (z^k, x_1^k, \ldots, x_j^k)$, where $z^k = (z_1,\ldots,z_k) \in \{0,1\}^{k\cdot\ell}$ are the coins of the original V's, and $x_{j'}^k = (x_{j',1},\ldots,x_{j',k}) \in \{0,1\}^k$, for $j' \in [j]$, are the random-terminating coins of all $\widetilde{\mathrm{V}}$'s in round j'. If the i^{th} $\widetilde{\mathrm{V}}$ aborts before round j', we set $x_{j',i} = 0$.

[21] This definition is slightly different than the one appearing in [Hai13] where $\widetilde{\mathrm{V}}$ flips a coin at the end of each communication round (rather than at the beginning of it). Since the coin flipped at the *end* of round j can be seen as it were flipped at the *beginning* of round $j+1$, then up to the first coin used in our variant, both definitions are equivalent. This additional coin is merely used for notation simplification.

$$z^k x^{(m+1)\times k} = \begin{bmatrix} z^k \\ x_1^k \\ x_2^k \\ . \\ . \\ . \\ x_{m+1}^k \end{bmatrix} = \begin{bmatrix} z_1 & z_2 & \dots & z_k \\ x_{1,1} & x_{1,2} & \dots & x_{1,k} \\ x_{2,1} & x_{2,2} & \dots & x_{2,k} \\ . & . & & . \\ . & . & & . \\ . & . & & . \\ x_{m+1,1} & x_{m+1,2} & \dots & x_{m+1,k} \end{bmatrix}$$

Figure 1: A matrix representation of a view. Given a full view $(z^k, x_1^k, \dots, x_{m+1}^k) \in \{0,1\}^{kl+k(m+1)}$, we sometimes write the vectors $(x_1^k, \dots, x_{m+1}^k)$ as an $(m+1)\times k-$size binary matrix $x^{(m+1)\times k}$ whose j^{th} row is x_j^k, and look at $z^k = (z_1, \dots, z_k)$ as the "zero-row" (or "zero-round") coins of the verifiers. We use $j \in [m+1]$ as a row index which represents the round number, and we use $i \in [k]$ as a column index which represents the verifier's index in the k-fold execution. By the above, $x_{j,i} \in \{0,1\}$ represents the value of the random terminating coin taken by the i^{th} verifier at the beginning of the j^{th} round, and $z_i \in \{0,1\}^\ell$ represents the zero-round coins of the i^{th} verifier.

Notation 4.2 (The set $\mathcal{W}$ of all accepting views)**.** *Let $\mathcal{W}$ be the set of all accepting (full) views $z^k x^{(m+1)\times k} \in \{0,1\}^{kl+k(m+1)}$.*

That is, $\mathcal{W}$ is the joint random coins of all $\widetilde{\text{V}}$'s that makes all of them to accept in an execution of $(\text{P}^{k^*}, \widetilde{\text{V}}^k)$. We assume without loss of generality that $\mathcal{W}$ is *termination consistent*:

Definition 4.3. *A set $\mathcal{S} \subseteq \{0,1\}^{k\ell+k(m+1)}$ is called* termination consistent*, if $\{z^k x^{(m+1)\times k} \in \{0,1\}^{k\ell+k(m+1)} \colon \forall i \in [k]\ \exists j \in [m+1]$ s.t. $x_{j,i} = 1\} \subseteq \mathcal{S}$.*

Namely, any view in which all verifiers accept and abort prematurely is (in particular) an accepting view.

We use the multiple-instance prover P^{k^*} to construct a single-instance one P^* that convinces V to accept with probability greater than $1-\varepsilon$. Algorithm P^* selects at the beginning a session $i \in [k]$ uniformly at random, and emulates a random accepting execution of $(\text{P}^{k^*}, \widetilde{\text{V}}^k)$, where V plays the role of the i^{th} verifier in $\widetilde{\text{V}}^k$. Before the interaction with V begins, P^* selects z_{-i} using rejection sampling: it repeatedly samples a random continuation of $(\text{P}^{k^*}, \widetilde{\text{V}}^k)$, conditioned on the event that $x_{1,i} = 1$ (i.e., the i^{th} verifier accepts and aborts at the first round) until it finds an *accepting continuation* (i.e., $\widetilde{\text{V}}^k$ accepts at the end of interaction). Then, P^* sets the random coins z_{-i} according to the corresponding random coins in the accepting continuation. Upon receiving V's j^{th} message $a_{j,i}$, algorithm P^* selects the j^{th} round random-terminating coins $x_{j,-i}$ of the other verifiers, using a similar rejection sampling process: it repeatedly samples a random continuation of $(\text{P}^{k^*}, \widetilde{\text{V}}^k)$ conditioned on the history (i.e., the previous i^{th} verifier's messages $a_{<j,i}$ and the fixed randomness of the other verifiers $z_{-i}, x_{<j,-i}$) and conditioned on the event that $x_{j+1,i} = 1$ (i.e., the i^{th} verifier accepts and aborts at round $j+1$) until it finds an *accepting continuation*. Then, P^* sets the j^{th} round random coins $x_{j,-i}$ according to the corresponding j^{th} round randomness of the accepting continuation, computes the j^{th} round messages $b_j^k = (b_{j,1}, \dots, b_{j,k})$ of P^{k^*} and sends to V the message $b_{j,i}$.

At the formal description of P^* given below, it is assumed that at the beginning V sends to P^* all its random coins, rather than sending a message $a_{j,i}$ in each round j. Hence, P^* does not need to wait for V's messages to arrive, and is only required to send m messages to V. This is merely done for presentation clarity, and the validity of this assumption is explained below.[22]

Algorithm 4.4 (P*)**.**

Input: 1^n. *(In the the following, $k, \ell, m, \varepsilon, p$ are all functions of n)*

Operation:

```
1. Sample $i \leftarrow [k]$.
2. Receive the random coins $z \in \{0,1\}^\ell$ from V.
3. Let $z^k = (z_1, \ldots, z_k) = \mathrm{GetZeroRoundCoins}(i, z)$.
4. Set $\mathrm{view} = z^k$.
5. For $j = 1$ to $m$ do:
   (a) Let $x_j^k = (x_{j,1}, \ldots, x_{j,k}) = \mathrm{GetNextRoundCoins}(\mathrm{view}, i)$.
   (b) Set $\mathrm{view} = (\mathrm{view}, x_j^k)$.
   (c) Send $b_{j,i}$ back to V, where $b_j^k = (b_{j,1}, \ldots, b_{j,k})$ are the messages that $\mathrm{P}^{k^*}$ sends to $\widetilde{\mathrm{V}}^k$ in
       the $j^{\text{th}}$ round of view.
```

Algorithm 4.5 (GetZeroRoundCoins)**.**

Input: an index $i \in [k]$ and a string $z \in \{0,1\}^\ell$.

Operation:

```
1. Do the following $t_0 = \lceil 8 \cdot p/\varepsilon \rceil$ times:
   (a) Sample $\mathrm{view}' = (z^k, x_1^k, \ldots, x_{m+1}^k)$ as $\widetilde{\mathrm{V}}^k$'s view in a random execution of $(\mathrm{P}^{k^*}, \widetilde{\mathrm{V}}^k)$,
       conditioned on $z_i = z$ and $x_{1,i} = 1$.
   (b) If $\mathrm{view}' \in \mathcal{W}$, return $z^k = (z_1, \ldots, z_k)$.
2. Abort the execution.
```

Algorithm 4.6 (GetNextRoundCoins)**.**

Input: a (partial) view of $\widetilde{\mathrm{V}}^k$ — view and an index $i \in [k]$.

Operation:

```
1. Set $j = \mathrm{round}(\mathrm{view}) + 1$.
2. Do the following $t = \lceil 200 \cdot m^2 p/\varepsilon^2 \rceil$ times:
   (a) Sample $\mathrm{view}' = (z^k, x_1^k, \ldots, x_{m+1}^k)$ as $\widetilde{\mathrm{V}}^k$'s view in a random execution of $(\mathrm{P}^{k^*}, \widetilde{\mathrm{V}}^k)$,
       conditioned on $(z^k, x_1^k, \ldots, x_{j-1}^k) = \mathrm{view}$ and $x_{j+1,i} = 1$.
```

[22] As mentioned in Section 2.2, similar description is also used in [Hai13], and the validity follows by similar arguments.

(b) If $\mathrm{view}' \in \mathcal{W}$*, return* $x_j^k = (x_{j,1}, \ldots, x_{j,k})$*.*

3. Abort the execution.

It is clear that P^*'s running time is polynomial in n. We should also make sure that P^* can indeed be executed without receiving V's random coins at Step 2. Note that at the j^{th} round, both GetZeroRoundCoins and GetNextRoundCoins choose view' conditioned on the event that V, the i^{th} verifier of $\widetilde{\mathrm{V}}^k$, aborts at round $j+1$ (where $j = 0$ in case GetZeroRoundCoins is called). Under this conditioning, P^{k^*} only sees the verifier's messages till the j^{th} round. It follows that the test $\mathrm{view}' \in \mathcal{W}$ done in both procedures, can be replaced with following one: let t be the full transcript defined by the messages the emulated verifiers (i.e., indexed different from i) on randomness view', and those of the i^{th} (real) verifier sent in the first j rounds. In such a transcript, the i^{th} verifier has only j messages and it aborts and accepts in round $j+1$. The test is verifying that all verifiers accept in t. Indeed, this test only uses the messages the i^{th} verifier sent till the j^{th} round, and the randomness of the emulated verifiers.

So it is left to analyze the success (cheating) probability of P^*. As describe in Section 2, the analysis of P^*'s success probability is done by relating the distribution induced by a random execution of $(\mathrm{P}^*, \mathrm{V})$, which we refer to as the Real distribution, to idealized variants of this distribution.

In the following let $\widetilde{\text{GetZeroRoundCoins}}$ and $\widetilde{\text{GetNextRoundCoins}}$ be the unbounded variants of these algorithms, respectively — the loop in both procedures runs until a good value of view' is found (i.e., $\mathrm{view}' \in \mathcal{W}$). Observe that both procedures are guaranteed to halt since by assumption $\mathcal{W}$ is termination consistent (Definition 4.3).

The Real and Ideal distributions. Distribution Real over $\{0,1\}^{k\ell + k(m+1)}$ is defined by the value of $(Z^k, X_1^k, \ldots, X_{m+1}^k)$ induced by the following process: let View be the value of view at the end of a random execution of $(\mathrm{P}^*, \mathrm{V})$, and let $(Z^k, X_1^k, \ldots, X_{m+1}^k)$ be $\widetilde{\mathrm{V}}^k$'s view in a random execution of $(\mathrm{P}^{k^*}, \widetilde{\mathrm{V}}^k)$ conditioned on (1) $(Z^k, X_1^k, \ldots, X_m^k) = \mathrm{View}$, (2) $X_{m+1,i} = 0$ and (3) $(Z^k, X_1^k, \ldots, X_{m+1}^k) \in \mathcal{W}$. If under first two conditions $\Pr\left[(Z^k, X_1^k, \ldots, X_{m+1}^k) \in \mathcal{W}\right] = 0$, set $(Z^k, X_1^k, \ldots, X_{m+1}^k) = (\mathrm{View}, 0^k)$.

That is, Real is the view of the emulated execution of $(\mathrm{P}^{k^*}, \widetilde{\mathrm{V}}^k)$ induced by a random execution of $(\mathrm{P}^*, \mathrm{V})$, while adding an imaginary step at the end of the interaction for choosing the coins $\widetilde{\mathrm{V}}^k$ use in its final $m+1$ round. Note that by construction, the $m+1$ random-terminating bits of the i^{th} verifier in Real are all set to zero since in each round $j \in [m]$ we choose X_j^k conditioned on $X_{j+1,i} = 1$ (which implies that $X_{j,i} = 0$) and also $X_{m+1,i}$ is always set to 0. Therefore, the coins of the i^{th} verifier in Real reflects those of a random-terminating verifier $\widetilde{\mathrm{V}}$ that uses the random bits of V in a random execution of $(\mathrm{P}^*, \mathrm{V})$, and never aborts. It follows that

$$\Pr[(\mathrm{P}^*, \mathrm{V}) = 1] \geq \Pr[\mathrm{Real} \in \mathcal{W}] \tag{25}$$

We also use the distribution $\widetilde{\mathrm{Real}}$, defined analogously to Real but with $\widetilde{\text{GetZeroRoundCoins}}$ and $\widetilde{\text{GetNextRoundCoins}}$ taking the role of GetZeroRoundCoins and GetNextRoundCoins in the definition P^*, respectively. The distribution Ideal is defined as P^{k^*}'s view in a random accepting execution of $(\mathrm{P}^{k^*}, \widetilde{\mathrm{V}}^k)$.

As mentioned in Section 2, for the attack of P^* to go through, we not only need to get an accepting view with high probability over $\widetilde{\mathrm{Real}}$, but also need that the index in which P^* embeds the real verifier (i.e., i) takes a "good value". We do that by bounding the smooth KL-divergence (Definition 3.11) between *extensions* of Ideal and $\widetilde{\mathrm{Real}}$ that incorporate this information.

To present our main lemma, we introduce a different formulation of the distributions Ideal and $\widetilde{\mathrm{Real}}$ discussed above.

Definition 4.7 (The distributions R and P, and the event W)**.** *For $k, m, \ell \in \mathbb{N}$ and $\mathcal{W} \subseteq \{0,1\}^{kl} \times \{0,1\}^{(m+1)\times k}$, define $R = R_{Z^k X^{(m+1)\times k}} = R_{Z^k} R_{X^{(m+1)\times k}}$ by $R_{Z^k} = \prod_{i=1}^k R_{Z_i}$, $R_{Z_i} = U_\ell$, $R_{X^{(m+1)\times k}} = \prod_{i=1}^k R_{X_{1,i} X_{2,i} \cdots X_{m+1,i}}$, and $R_{X_{j,i}|X_{<j,i}} = \begin{cases} \mathrm{Bern}(0) & 1 \in X_{<j,i} \\ \mathrm{Bern}(1/m) & o.w. \end{cases}$. Let W be the event over R that $Z^k X^{(m+1)\times k} \in \mathcal{W}$, and let $P = P_{Z^k X^{(m+1)\times k}} = R_{Z^k X^{(m+1)\times k}|W}$.*

It is easy to verify that P and Ideal are the same distribution with respect to the values k, m, ℓ and the set $\mathcal{W}$ described in this section. Indeed, $R_{Z^k X^{(m+1)\times k}}$ denotes the distribution of the random coins of all k verifiers in $\widetilde{\mathrm{V}}^k$. Note that for each $i \in [k]$, the random coins Z_i of the internal verifier V in $\widetilde{\mathrm{V}}_i$ are chosen uniformly over $\{0,1\}^\ell$, and for each round $j \in [m+1]$, the random terminating coin $X_{j,i}$ is chosen according to the Bernoulli distribution with parameter $1/m$ if all previous coins $X_{1,i}, \ldots, X_{j-1,i}$ are equal to zero (otherwise, $X_{j,i}$ is set to zero). Given a full view $Z^k X^{(m+1)\times k}$, the event W denotes whether it is an accepting view (i.e., $Z^k X^{(m+1)\times k} \in \mathcal{W}$). By definition, $R[W] = \Pr\left[(\mathrm{P}^{k*}, \widetilde{\mathrm{V}}^k) = 1\right] > \max\{(1-\varepsilon)^{k/cm}, 1/p\}$.

Similarly, we reformulate the (unbounded) real distribution $\widetilde{\mathrm{Real}}$ as follows:

Definition 4.8 (The distribution Q)**.** *For $k, m, \ell \in \mathbb{N}$ and for a termination consistent set $\mathcal{W} \subseteq \{0,1\}^{kl+k(m+1)}$ (according to Definition 4.3), define $Q = Q_{I, Z^k X^{(m+1)\times k}} = Q_I Q_{Z^k X^{(m+1)\times k}|I}$ by $Q_I = U_{[k]}$, $Q_{Z^k|I} = R_{Z_I} P_{Z_{-I}|Z_I, X_{1,I}=1}$, $Q_{X_j^k|I Z^k X_{<j}^k} = P_{X_j^k|Z^k X_{<j}^k, X_{j+1,I}=1}$, and $Q_{X_{m+1}^k|I Z^k X_{\leq m}^k} = \begin{cases} P_{X_{m+1}^k|Z^k X_{\leq m}^k, X_{m+1,I}=0} & R[W|Z^k X_{\leq m}^k, X_{m+1,I}=0] > 0 \\ 0^k & o.w. \end{cases}$.*

It is easy to verify that indeed $Q_{Z^k X^{(m+1)\times k}}$ and $\widetilde{\mathrm{Real}}$ are the same distribution (with respect to the values of $k, m, \ell, \mathcal{W}$ described in this section). In particular, $\Pr\left[\widetilde{\mathrm{Real}} \in \mathcal{W}\right] = Q_{Z^k X^{(m+1)\times k}}(\mathcal{W})$.

Indeed, Q describes the following random process: First choose a uniform $I \in [k]$ (as done in Step 1 of P^*), then choose the uniform random coins $Z_I \in \{0,1\}^\ell$ (as done in Step 2 of P^*), and then choose Z_{-I} and all $\{X_{j,-I}\}_{j \in [m+1]}$ as done in P^*. By definition, for all $j \in [m]$ it holds that $X_{j+1,I} = 1 \implies X_{j,I} = 0$. In addition, it always holds that $X_{m+1,I} = 0$. Therefore, we always get that $Q_{X_{1,I}, X_{2,I}, \ldots, X_{m+1,I}|I} = 0^{m+1}$, which perfectly simulates V as the i'th verifier since it behaves as $\widetilde{\mathrm{V}}$ conditioned on all random terminating coins to be zero.

The following lemma, proved in Section 5, is the center of our analysis of P^*'s success probability.

Lemma 4.9 (Main lemma)**.** *Let $k, m, \ell \in \mathbb{N}$, let $\varepsilon \in (0, 1/2]$, let $\mathcal{W} \subseteq \{0,1\}^{k\ell + k(m+1)}$ be a termination-consistent set (according to Definition 4.3) and let W, R, P and Q, be the event and distributions from Definitions 4.7 and 4.8 with respect to $\mathcal{W}, m, k, \ell$. Assume $k \geq \lambda \cdot m^2/\varepsilon$ and $R[W] > (1-\varepsilon)^{\frac{k}{\lambda \cdot m}}$ for some universal constant $\lambda > 0$. Then there exist distributions $\widehat{P} = \widehat{P}_{Z^k X^{(m+1)\times k}, B}$ and $\widehat{Q} = \widehat{Q}_{I, Z^k X^{(m+1)k}, B}$, with $\widehat{P}_{Z^k X^{(m+1)\times k}} = P$ and $\widehat{Q}_{I, Z^k X^{(m+1)\times k}} = Q$ such that the following holds:*

1. *$D^{\frac{\varepsilon}{24}}(\widehat{P} || \widehat{Q}_{Z^k X^{(m+1)\times k}, B}) \leq \lambda \cdot \frac{m}{k} \cdot \left(\log \frac{1}{R[W]} + m\right)$.*

2. $\widehat{P}_B(1) \geq 1 - \varepsilon/24$.

3. $\forall (i, z^k x^{(m+1)\times k}) \in \operatorname{Supp}(\widehat{Q}_{I,Z^k X^{(m+1)\times k}|B=1})$:

(a) $R[W|Z_i = z_i, X_{1,i} = 1] \geq R[W]/2$.

(b) $\forall j \in [m+1] : R[W|Z^k X^k_{<j} = z^k x^k_{<j}, X_{j+1,i} = 1] \geq R[W|Z^k X^k_{<j} = z^k x^k_{<j}]/2$.

That is, Lemma 4.9 states the following with respect to the *extensions* $\widehat{P}$ and $\widehat{Q}$ of P and Q: First, the smooth KL-divergence between the distribution $\widehat{P}$ and (a projection of) $\widehat{Q}$ (without the I) is small. Second, the extension bit B is one with high probability over $\widehat{P}$, and that conditioned on this bit to be "on" in $\widehat{Q}$, the (unbounded) attack done in $\widetilde{\text{Real}}$ (as reflected in Q) actually runs in polynomial time.

The following is an immediate corollary of Lemma 4.9.

Corollary 4.10. *Let $\varepsilon, k, m, W, P, Q, \widehat{P}, \widehat{Q}, \lambda$ be as in Lemma 4.9, and assume that $k \geq c \cdot m^2/\varepsilon$ and $R[W] > (1-\varepsilon)^{\frac{k}{c\cdot m}}$ for $c = 128 \cdot \lambda$. Then $D^{\frac{\varepsilon}{24}}(\widehat{P}||\widehat{Q}_{Z^k X^{(m+1)\times k},B}) < \varepsilon/32$.*

Proof. Since $R[W] > (1-\varepsilon)^{\frac{k}{c\cdot m}} > (1-\varepsilon)^{\frac{k}{\lambda\cdot m}}$, we can apply Lemma 4.9 (1) to obtain that

$$\begin{aligned} D^{\frac{\varepsilon}{24}}(\widehat{P}||\widehat{Q}_{Z^k,X^{(m+1)\times k},B}) &< \frac{\lambda m}{k} \cdot \left(\log \frac{1}{(1-\varepsilon)^{\frac{k}{cm}}} + m\right) \\ &\leq \frac{\lambda m}{k} \cdot \left(2\varepsilon \cdot \frac{k}{cm} + m\right) \\ &= 2\varepsilon\frac{\lambda}{c} + \frac{\lambda m^2}{k}, \\ &< \frac{\varepsilon}{32}. \end{aligned} \tag{26}$$

The first inequality holds since $R[W] > (1-\varepsilon)^{\frac{k}{c\cdot m}}$, the second one holds since $1 - \varepsilon \geq e^{-2\varepsilon}$ for $\varepsilon \in [0, 1/2]$ and the last one holds since $k \geq 128\lambda \cdot m^2/\varepsilon$ and since $c = 128\lambda$. □

In the next section we use Lemma 4.9 for proving the main theorem, while assuming—like Lemma 4.9 does—that the number of repetitions is sufficiently large (i.e., $k \geq c \cdot m^2/\varepsilon$ for the universal constant c of Corollary 4.10). In Section 4.2 we prove the main theorem for the case that $k < c \cdot m^2/\varepsilon$, via a reduction to the large k case.

4.1 Proving Theorem 4.1 for Large Number of Repetitions

Assume $k \geq c \cdot m^2/\varepsilon$ (for the constant c of Corollary 4.10). We start by proving the following simple claim, which states that in P, all the values $\{R[W|Z^k X^k_{<j}]\}_{j\in[m]}$ are large enough with high probability.

Claim 4.11. *Let $\mathcal{S} = \{z^k x^{(m+1)\times k} \in \{0,1\}^{k\ell + k(m+1)} \colon \forall j \in [m].\ R[W|(Z^k X^k_{<j}) = z^k x^k_{<j}] \geq \varepsilon \cdot R[W]/24m\}$. Then $P_{Z^k X^{(m+1)\times k}}(\mathcal{S}) \geq 1 - \varepsilon/24$.*

Proof. By Fact 3.19, it holds that $\mathrm{E}_{P_{Z^k X^k_{<j}}}\left[\frac{1}{R[W|Z^k X^k_{<j}]}\right] = \frac{1}{R[W]}$ for every $j \in [m]$. Thus, the proof follows by Markov inequality and union bound. □

At this point, we proved that P and Q are close enough by *smooth* divergence (Lemma 4.9(1)), and we proved that in P all the values $\{R[W|Z^k X^k_{<j}]\}_{j=1}^m$ are large enough with high probability (Claim 4.11). In addition, note that by definition P always produces $Z^k X^{(m+1)\times k} \in \mathcal{W}$. Therefore, we can deduce by Proposition 3.13 that in Q we also have $Z^k X^{(m+1)\times k} \in \mathcal{W}$ and large enough values of $\{R[W|Z^k X^k_{<j}]\}_{j=1}^m$ with high probability. Using Items 2 and 3 of Lemma 4.9, we actually can deduce that the above is true even for the values $\{R[W|Z^k X^k_{<j}, X_{j+1,I} = 1]\}_{j=1}^m$. The formal result of the above informal plan is state in the following corollary.

Corollary 4.12. *Assume that $R[W] > (1-\varepsilon)^{\frac{k}{c \cdot m}}$, where c is the constant from Corollary 4.10, and let*

$$\begin{aligned}\mathcal{T} = \{(i, z^k x^{(m+1)\times k}) \in [k] \times \{0,1\}^{k\ell + k(m+1)} \colon & \left(z^k x^{(m+1)\times k} \in \mathcal{W}\right),\\ & (R[W|Z_i = z_i, X_{1,i} = 1] \geq R[W]/2),\\ & \left(\forall j \in [m].\ R[W|(Z^k X^k_{<j}) = z^k x^k_{<j}, X_{j+1,i} = 1] \geq \varepsilon \cdot R[W]/48m\right)\}\end{aligned}$$

Then $Q_{I, Z^k X^{(m+1)\times k}}(\mathcal{T}) > 1 - \varepsilon/4$.

Proof. In the following, let $\mathcal{S}$ be the set from Claim 4.11 and let

$$\widehat{\mathcal{S}} = (\mathcal{W} \cap \mathcal{S}) \times \{1\}. \tag{27}$$

Note that by Claim 4.11 and Lemma 4.9(2,3) and by the fact that $P(\mathcal{W}) = 1$, it holds that

$$\widehat{P}(\widehat{\mathcal{S}}) > 1 - \varepsilon/12. \tag{28}$$

In addition, by Corollary 4.10 it holds that

$$D^{\frac{\varepsilon}{24}}(\widehat{P} || \widehat{Q}_{Z^k X^{(m+1)\times k}, B}) < \varepsilon/32 \tag{29}$$

Therefore, we can apply Proposition 3.13 on $\widehat{P}$ and $\widehat{Q}$ with $\alpha = \frac{\varepsilon}{24}$, $\beta = \frac{\varepsilon}{12}$ and the set $\widehat{\mathcal{S}}$ to obtain that

$$\widehat{Q}_{Z^k X^{(m+1)\times k}, B}(\widehat{\mathcal{S}}) > 1 - \varepsilon/4, \tag{30}$$

and we conclude that

$$\begin{aligned} Q(\mathcal{T}) &= \widehat{Q}_{I, Z^k X^{(m+1)\times k}}(\mathcal{T})\\ &\geq \widehat{Q}_{Z^k X^{(m+1)\times k}, B}(\widehat{\mathcal{S}})\\ &> 1 - \varepsilon/4, \end{aligned}$$

as required, where the first inequality holds since Lemma 4.9(3) yields that for any $z^k x^{(m+1)\times k} \in \mathcal{W} \cap \mathcal{S}$ and any $i \in \mathrm{Supp}(\widehat{Q}_{I|(Z^k X^{(m+1)\times k}) = z^k x^{(m+1)\times k}, B=1})$ we have $(i, z^k x^{(m+1)\times k}) \in \mathcal{T}$.

□

The proof of Theorem 4.1 in the case $k \geq c \cdot m^2/\varepsilon$, given below, follows Corollary 4.12.

Proof of Theorem 4.1 for $k \geq c \cdot m^2/\varepsilon$. Let $(\mathrm{P}, \mathrm{V}), m = m(n), \varepsilon = \epsilon(n), k = k(n)$ be as in the statement of Theorem 4.1 and assume towards a contradiction the existence of a polynomial-time adversarial prover P^{k^*} and a polynomial p such that Equation (24) holds for infinity many n's, where c (the constant from the theorem statement) is set to the constant c of Corollary 4.12. In the following, fix such value of n and assume that $k \geq c \cdot m^2/\varepsilon$. Let $\mathcal{W}$ be the set of all accepting (full) views (see Notation 4.2), let P^* be the adversarial prover described in Algorithm 4.4, let Real, $\widetilde{\text{Real}}$ and Ideal be the distributions induced by Algorithm 4.4, and let P and Q be distributions from Definitions 4.7 and 4.8, respectively.

In the following, let $\mathcal{T}$ be the set from Corollary 4.12 and let T be the event over $Q_{I,Z^k X^{(m+1)\times k}}$ that $(I, Z^k X^{(m+1)\times k}) \in \mathcal{T}$. By Corollary 4.12,

$$Q[T] > 1 - \varepsilon/4 \tag{31}$$

Since $R[W] > 1/p$, Equation (31) yields that with probability $1 - \varepsilon/4$ over $(i, z^k x^{(m+1)\times k}) \sim Q$ (i.e., according to $\widetilde{\text{Real}}$ with I), the event T happens, yielding that $1/R[W|Z_i = z_i, X_{1,i} = 1] \leq 2p$ and $\{1/R[W|Z^k X^k_{<j} = z^k x^k_{<j}, X_{j+1,i} = 1]\}_{j\in[m]}$ are all at most $48mp/\varepsilon$. In particular, conditioned on T, the expected number of sampling attempts in $\widetilde{\text{GetNextRoundCoins}}$ for each round $j \in [m]$ (which equals to $1/R[W|(Z^k X^k_{<j}) = z^k x^k_{<j}, X_{j+1,i} = 1])$ is at most $48mp/\varepsilon$. Therefore, by Markov inequality and a union bound, conditioned on T, with probability less than $\varepsilon/4$ over a random execution of Algorithm 4.4 (with $\widetilde{\text{GetZeroRoundCoins}}$ and $\widetilde{\text{GetNextRoundCoins}}$), there exists $j \in [m]$ such that the j^{th} call to $\widetilde{\text{GetNextRoundCoins}}$ fails to find accepting continuation after t $(= \lceil 200 \cdot m^2 p/\varepsilon^2 \rceil)$ sampling attempts. In addition, conditioned on T, the expected number of sampling attempts in $\widetilde{\text{GetZeroRoundCoins}}$ is $1/R[W|Z_i = z_i, X_{1,i} = 1] \leq 2p$. Therefore, by Markov inequality we have that conditioned on T, the probability that $\widetilde{\text{GetZeroRoundCoins}}$ fails after t_0 $(= \lceil 8 \cdot p/\varepsilon \rceil)$ rounds is at most $\varepsilon/4$.

In the following, given a random execution of Algorithm 4.4 (with $\widetilde{\text{GetZeroRoundCoins}}$ and $\widetilde{\text{GetNextRoundCoins}}$), we denote by A_0 the event that $\widetilde{\text{GetZeroRoundCoins}}$ finds an accepting continuation within t_0 sampling attempts and let A be the event that each of the m calls to $\widetilde{\text{GetNextRoundCoins}}$ finds an accepting continuation within t sampling attempts. By combining all parts of above analysis, we obtain that

$$\begin{aligned}
\Pr[\neg A_0 \vee \neg A] &\leq \Pr[\neg T] + \Pr[\neg A_0 \mid T] + \Pr[\neg A \mid T] \\
&< \varepsilon/4 + \varepsilon/4 + \varepsilon/4 \\
&= 3\varepsilon/4.
\end{aligned}$$

In words, this means that with probability at least $1 - 3\varepsilon/4$ over a random execution of Algorithm 4.4 (with $\widetilde{\text{GetZeroRoundCoins}}$ and $\widetilde{\text{GetNextRoundCoins}}$), $\widetilde{\text{GetZeroRoundCoins}}$ finds an accepting continuation within t_0 sampling attempts and each of the m calls to $\widetilde{\text{GetNextRoundCoins}}$ finds an accepting continuation within t sampling attempts. Observe that the above also holds over a random execution of Algorithm 4.4 with GetZeroRoundCoins and GetNextRoundCoins (i.e., $A_0 \wedge A$ happens with the same probability over Real, which means that it does not abort prematurely). Since $\text{Real}\,|_{A_0 \wedge A} \equiv \widetilde{\text{Real}}|_{A_0 \wedge A}$, we obtain that

$$\mathrm{SD}(\text{Real}, \widetilde{\text{Real}}) \leq \Pr[\neg A_0 \vee \neg A] < 3\varepsilon/4 \tag{32}$$

Finally, observe that Corollary 4.12 yields (in particular) that $Q_{Z^k X^{(m+1)\times k}}(\mathcal{W}) = \Pr\left[\widetilde{\text{Real}} \in \mathcal{W}\right] > 1 - \varepsilon/4$ and we conclude that

$$\Pr[(\mathrm{P}^*, \mathrm{V}) = 1] \geq \Pr[\text{Real} \in \mathcal{W}] \geq \Pr\left[\widetilde{\text{Real}} \in \mathcal{W}\right] - \mathrm{SD}(\text{Real}, \widetilde{\text{Real}}) > 1 - \varepsilon,$$

in contradiction to the soundness property of (P, V). □

4.2 Handling Small Number of Repetitions

In this section we complete the proof of Theorem 4.1 by proving it for small number of repetition using a reduction to the many repetitions case. The rather long and technical reduction follows the intuition given in Section 2.2.5, and a first time reader may prefer to skip it and move to the proof of the main lemma given in Section 5.

In the following let $(\mathrm{P}, \mathrm{V}), m = m(n), \varepsilon = \varepsilon(n), k' = k'(n)$ be as in the statement of Theorem 4.1 (replacing k with k') and assume that there exists a polynomial-time adversarial prover $\mathrm{P}^{k'*}$ and a polynomial p such that

$$\Pr\left[(\mathrm{P}^{k'*}, \widetilde{\mathrm{V}}^{k'})(1^n) = 1\right] > \max\left((1-\varepsilon)^{\frac{k'}{c \cdot m}}, \frac{1}{p(n)}\right), \tag{33}$$

for infinity many n's, where c is the universal constant from Corollary 4.12. In the following, fix a value of n such that Equation (33) holds and $k' < c \cdot m^2/\varepsilon$, and let $k = k' \cdot r$ for $r = \lceil c \cdot m^2/\varepsilon \rceil$. We first use the adversarial prover $\mathrm{P}^{k'*}$ (against $\widetilde{\mathrm{V}}^{k'}$) to construct an adversarial prover P^{k*} (against $\widetilde{\mathrm{V}}^{k}$) as follows: P^{k*} divides the set of k verifiers into r sets, each of size k', and executes $\mathrm{P}^{k'*}$ on each set (independently). By Equation (33) it holds that

$$\Pr\left[(\mathrm{P}^{k*}, \widetilde{\mathrm{V}}^{k})(1^n) = 1\right] > \left((1-\varepsilon)^{\frac{k'}{c \cdot m}}\right)^r = (1-\varepsilon)^{\frac{k}{c \cdot m}} \tag{34}$$

We now use P^{k*} to construct P^* that convinces V with probability greater than $1 - \varepsilon$. The construction is very similar to the one described in Algorithm 4.4, but there is an important difference. In Algorithm 4.4, in order to find an accepting continuation (both in GetZeroRoundCoins and GetNextRoundCoins), it was suffice to use $t_0, t \leq \mathrm{poly}(n)$ sampling attempts that make Equation (32) to hold, since we assumed that $\Pr\left[(\mathrm{P}^{k*}, \widetilde{\mathrm{V}}^{k})(1^n) = 1\right] \geq 1/p(n)$ for some polynomial p. Here, $\Pr\left[(\mathrm{P}^{k*}, \widetilde{\mathrm{V}}^{k})(1^n) = 1\right]$ might be negligible, so the same construction does not work. Yet, since P^{k*} consists of r independent copies of $\mathrm{P}^{k'*}$ and since $\Pr\left[(\mathrm{P}^{k'*}, \widetilde{\mathrm{V}}^{k'})(1^n) = 1\right] \geq 1/p$, algorithm P^* can find an accepting continuation by searching in each copy separately and using only $\mathrm{poly}(n)$ sampling attempts in each copy.

Formally, P^* has the same structure of Algorithm 4.4, but uses modified variants of GetZeroRoundCoins and GetNextRoundCoins that searches for accepting continuation in each copy. The formal definitions of the modified procedures GetZeroRoundCoins and GetNextRoundCoins appear at Algorithms 4.13 and 4.14, respectively. In the following, we write a partial view of $(\mathrm{P}^{k*}, \widetilde{\mathrm{V}}^{k})$ in the form view $= (z^k = (z_1^{k'}, \ldots, z_r^{k'}), x_1^k = (x_{1,1}^{k'}, \ldots, x_{1,r}^{k'}), \ldots, x_j^k = (x_{j,1}^{k'}, \ldots, x_{j,r}^{k'}))$ and for $s \in [r]$ we denote by view$[s] = (z_s^{k'}, x_{1,s}^{k'}, \ldots, x_{m+1,s}^{k'})$ the partial view of the

s'th part of verifiers $\widetilde{\mathrm{V}}^k[s] = (\widetilde{\mathrm{V}}_{k'(s-1)+1}, \ldots, \widetilde{\mathrm{V}}_{k's})$. In addition, we denote by $\mathcal{W}'$ the set of all accepting views $(z^{k'}, x_1^{k'}, \ldots, x_{m+1}^{k'}) \in \{0,1\}^{k'l+k'(m+1)}$ of $(\mathrm{P}^{k'^*}, \widetilde{\mathrm{V}}^{k'})$, and by $\mathcal{W} = \mathcal{W}'^r$ the set of all accepting views $(z^k, x_1^k, \ldots, x_{m+1}^k) \in \{0,1\}^{kl+k(m+1)}$ of $(\mathrm{P}^{k*}, \widetilde{\mathrm{V}}^k)$.

Algorithm 4.13 (GetZeroRoundCoins, redefined)**.**

Input: an index $i \in [k]$ and a string $z \in \{0,1\}^\ell$.

Operation:

```
1. Let $s_i = \lceil i/k' \rceil \in [r]$ and $i' = i - k'(s_i - 1) \in [k']$.
2. For $s = 1$ to $r$:
   (a) Do the following $t_0 = \lceil 8pr/\varepsilon \rceil$ times:
       i. Choose $z^{k'} x^{(m+1)\times k'}$ as $\widetilde{\mathrm{V}}^{k'}$'s view in a random execution of $(\mathrm{P}^{k'^*}, \widetilde{\mathrm{V}}^{k'})$. If $s = s_i$, do the above choosing conditioned on $z_{i'} = z$ and $x_{1,i'} = 1$.
       ii. If $z^{k'} x^{(m+1)\times k'} \in \mathcal{W}'$, set $z_{s'}^{k'} = z^{k'}$ and go to the next iteration of the outer loop.
   (b) Abort the execution.
3. Return $z^k = (z_1^{k'}, \ldots, z_r^{k'})$.
```

Algorithm 4.14 (GetNextRoundCoins, redefined)**.**

Input: a (partial) view *of $\widetilde{\mathrm{V}}^k$ and an index $i \in [k]$.*

Operation:

```
1. Let $s_i = \lceil i/k' \rceil \in [r]$ and $i' = i - k'(s_i - 1) \in [k']$.
2. Set $j = \mathrm{round}(\mathrm{view}) + 1$.
3. For $s = 1$ to $r$:
   (a) Do the following $t = \lceil 4 \cdot 10^6 m^2 r^2 p/\varepsilon^4 \rceil$ times:
       i. Choose $z^{k'} x^{(m+1)\times k'}$ as $\widetilde{\mathrm{V}}^{k'}$'s view in a random execution of $(\mathrm{P}^{k'^*}, \widetilde{\mathrm{V}}^{k'})$ conditioned on $z^{k'} x_{<j}^{k'} = \mathrm{view}[s]$. If $s = s_i$, do the above choosing conditioned on $x_{j+1,i'} = 1$.
       ii. If $z^{k'} x^{(m+1)\times k'} \in \mathcal{W}'$, set $x_{j,s}^{k'} = x_j^{k'}$ and go to the next iteration of the outer loop.
   (b) Abort the execution.
4. Return $(x_{j,1}^{k'}, \ldots, x_{j,r}^{k'})$.
```

We start by redefining the real and ideal distributions. Let $\widetilde{\text{GetZeroRoundCoins}}$, $\widetilde{\text{GetNextRoundCoins}}$ be the "unbounded variants" of the new definitions of GetZeroRoundCoins and GetNextRoundCoins, respectively, and let Real and $\widetilde{\text{Real}}$ be the distributions induced by Algorithm 4.4 with the new GetZeroRoundCoins and GetNextRoundCoins. The key observation is that the $\widetilde{\text{Real}}$ which is induced by Algorithm 4.4 with the old variants of GetZeroRoundCoins and GetNextRoundCoins (Algorithms 4.5 and 4.6) has the same distribution as $\widetilde{\text{Real}}$ with the new variants (Algorithms 4.13 and 4.14). This equality simply holds by the fact that P^{k^*} executes r independent copies of $\mathrm{P}^{k'^*}$.

In the following, let W,R,P and Q be the event and distributions defined in Definitions 4.7 and 4.8, respectively, and we denote by R' and P' the distribution R and P (respectively) from Definition 4.7 with respect to k' and $\mathcal{W}'$. First, since $\mathcal{W} = \mathcal{W}'^r$, it holds that $R[W] = R'[W]^r$ and for any $z^k x^{(m+1)\times k} \in \{0,1\}^{kl+(m+1)k}$ where $z^k = (z_1^{k'}, \ldots, z_r^{k'})$ and $x_j^k = (x_{j,1}^{k'}, \ldots, x_{j,r}^{k'})$ it holds that

$$P_{Z^k}(z^k) = \prod_{s=1}^{r} P'_{Z^{k'}}(z_s^{k'}) \tag{35}$$

and for $j \in [m+1]$:

$$P_{X_j^k|Z^k X_{<j}^k}(x_j^k|z^k x_{<j}^k) = \prod_{s=1}^{r} P'_{X_j^{k'}|Z_j^{k'} X_{<j}^{k'}}(x_{j,s}^{k'}|z_s^{k'} x_{<j,s}^{k'}) \tag{36}$$

Second, by the above observation about $\widetilde{\mathrm{Real}}$, it holds that $\widetilde{\mathrm{Real}} \equiv Q_{Z^k X^{(m+1)\times k}}$. Since $k \geq c \cdot m^2/\varepsilon$, we now can apply Lemma 4.9 on P and Q to deduce that $\widetilde{\mathrm{Real}} \in \mathcal{W}$ with high probability. However, this is not enough since we still need to figure out what is the probability that $\mathrm{Real} \in \mathcal{W}$. In other words, we need to bound the probability that GetZeroRoundCoins or GetNextRoundCoins (Algorithms 4.13 and 4.14) abort prematurely. We do so by showing that with high probability, the expected number of sampling attempts in each part of GetZeroRoundCoins or GetNextRoundCoins is bounded.

As first step, the following claim state that with high probability over $z^k x^{(m+1)\times k} \sim P_{Z^k X^{(m+1)\times k}}$, all values $\{R[W|(Z^k X_{<j}^k) = z^k x_{<j}^k]\}_j$ are “close enough” to their expected value $R[W]$, and all the internal values $\{R'[W|(Z^{k'} X_{<j}^{k'}) = z_s^{k'} x_{j,s}^{k'}]\}_{j,s}$ which captures most of the expected number of sampling attempts of GetNextRoundCoins, are bounded.

Claim 4.15. *Let $d = 72m/\varepsilon$, let $d' = r \cdot d$ and let*

$$\begin{aligned}\mathcal{S} = \{&(z^k = (z_1^{k'}, \ldots, z_r^{k'}), x_1^k = (x_{1,1}^{k'}, \ldots, x_{1,r}^{k'}), \ldots, x_{m+1}^k = (x_{m+1,1}^{k'}, \ldots, x_{m+1,r}^{k'})) \in \{0,1\}^{kl+k(m+1)}: \\ &\Big(\forall j \in [m].\ R[W|(Z^k X_{<j}^k) = z^k x_{<j}^k] \in [R[W]/d, d \cdot R[W]]\Big) \wedge \\ &\Big(\forall j \in [m]\ \forall s \in [r].\ R'[W|(Z^{k'} X_{<j}^{k'}) = z_s^{k'} x_{j,s}^{k'}] \geq R'[W]/d'\Big)\}.\end{aligned}$$

Then $P_{Z^k X^{(m+1)\times k}}(\mathcal{S}) \geq 1 - \varepsilon/24$.

Proof. We write $\mathcal{S} = \mathcal{S}_1 \cap \mathcal{S}_2 \cap \mathcal{S}_3$ where $\mathcal{S}_1$ is defined by only considering the lower bound of the first condition in $\mathcal{S}$ (i.e., $\geq R[W]/d$), $\mathcal{S}_2$ is defined by only considering the upper bound of the first condition (i.e., $\leq d \cdot R[W]$) and $\mathcal{S}_3$ is defined by only considering the second condition. We now handle each set separately.

By Fact 3.19 it holds that $\mathrm{E}_{P_{Z^k X_{<j}^k}}\left[\frac{1}{R[W|Z^k X_{<j}^k]}\right] = \frac{1}{R[W]}$ for every $j \in [m]$. Therefore, by Markov inequality and union bound we obtain that

$$P_{Z^k X^{(m+1)\times k}}(\mathcal{S}_1) \geq 1 - \varepsilon/72 \tag{37}$$

Next, note that $\mathrm{E}_{P_{Z^k X^k_{<j}}}\left[R[W|Z^k X^k_{<j}]\right] = R[W]$ for every $j \in [m]$. Again, by Markov inequality and union bound we obtain that

$$P_{Z^k X^{(m+1)\times k}}(\mathcal{S}_2) \geq 1 - \varepsilon/72 \tag{38}$$

Finally, observe that for any $j \in [m]$ and $s \in [r]$, it holds that $\mathrm{E}_{z^k x^k_{<j} \sim P_{Z^k X^k_{<j}}}\left[\frac{1}{R'[W|(Z^{k'} X^{k'}_{<j}) = z^{k'}_s x^{k'}_{<j,s}]}\right] = \mathrm{E}_{P'_{Z^{k'} X^{k'}_{<j}|W}}\left[\frac{1}{R'[W|Z^{k'} X^{k'}_{<j}]}\right] = \frac{1}{R'[W]}$, where the last equality holds by Fact 3.19. Hence, by Markov inequality and union bound we obtain that

$$P_{Z^k X^{(m+1)\times k}}(\mathcal{S}_3) \geq 1 - \varepsilon/72 \tag{39}$$

and we conclude that $P_{Z^k X^{(m+1)\times k}}(\mathcal{S}) \geq 1 - \varepsilon/24$ by Equations (37) to (39). □

As a corollary of Lemma 4.9, Corollary 4.10, and Claim 4.15, we now prove that with high probability over $(i, z^k x^{(m+1)\times k}) \sim Q$, we have bounded expected number of sampling attempts in each of the $m \cdot r$ iterations of GetNextRoundCoins.

Corollary 4.16. *Assume that $R[W] > (1-\varepsilon)^{\frac{k}{c \cdot m}}$, where c is the constant from Corollary 4.10, and let*

$$\begin{aligned}
\mathcal{T} = \{(i, z^k = (z^{k'}_1, \ldots, z^{k'}_r), x^k_1 = (x^{k'}_{1,1}, \ldots, x^{k'}_{1,r}), \ldots, x^k_{m+1} = (x^{k'}_{m+1,1}, \ldots, x^{k'}_{m+1,r})) \in [k] \times \{0,1\}^{kl + k(m+1)} :\\
\quad \left(z^k x^{(m+1)\times k} \in \mathcal{W}\right) \wedge\\
\quad \left(R'[W|Z_{i'} = z_i, X_{1,i'} = 1] \geq R'[W]/2\right) \wedge\\
\quad \left(\forall j \in [m]\ \forall s \in [r] \setminus s_i.\ R'[W|(Z^{k'} X^{k'}_{<j}) = z^{k'}_s x^{k'}_{<j,s}] \geq \varepsilon \cdot R'[W]/72mr\right) \wedge\\
\quad \left(\forall j \in [m].\ R'[W|(Z^{k'} X^{k'}_{<j}) = z^{k'}_{s_i} x^{k'}_{<j,s_i}, X_{j+1,i'} = 1] \geq \varepsilon^3 \cdot R'[W]/10^6 mr\right)\},
\end{aligned}$$

where $s_i = \lceil i/k' \rceil \in [r]$ and $i' = i - k'(s-1) \in [k']$. Then $Q_{i, Z^k X^{(m+1)\times k}}(\mathcal{T}) \geq 1 - \varepsilon/4$.

Proof. Let $\mathcal{S}$ be the set from Claim 4.15, let

$$\widehat{\mathcal{S}} = (\mathcal{W} \cap \mathcal{S}) \times \{1\},$$

and recall that $k \geq n \cdot m^2/\varepsilon$ and that $R[W] > (1-\varepsilon)^{\frac{k}{c \cdot m}}$ where c is the constant from Corollary 4.10. By Claim 4.15 and Lemma 4.9(2) and by the fact that $P_{Z^k X^{(m+1)\times k}}(\mathcal{W}) = 1$, it holds that

$$\widehat{P}_{Z^k X^{(m+1)\times k}, B}(\widehat{\mathcal{S}}) > 1 - \varepsilon/12.$$

In addition, by Corollary 4.10 it holds that

$$D^{\frac{\varepsilon}{24}}(\widehat{P}_{Z^k X^{(m+1)\times k}, B} || \widehat{Q}_{Z^k X^{(m+1)\times k}, B}) < \varepsilon/32$$

Therefore, we can apply Proposition 3.13 on $\widehat{P}$ and $\widehat{Q}$ with $\alpha = \frac{\varepsilon}{24}$, $\beta = \frac{\varepsilon}{12}$ and the set $\widehat{\mathcal{S}}$ to obtain that

$$\widehat{Q}_{Z^k X^{(m+1)\times k}, B}(\widehat{\mathcal{S}}) > 1 - \varepsilon/4. \tag{40}$$

In the following, fix $z^k x^{(m+1)\times k} \in \mathcal{W} \cap \mathcal{S}$ and $i \in \operatorname{Supp}(\widehat{Q}_{I|(Z^k X^{(m+1)\times k})=z^k x^{(m+1)\times k},B=1})$. First, observe that

$$\begin{aligned}
R'[W]^{r-1} \cdot R'[W|Z_{i'} = z_i, X_{1,i'} = 1] &= R[W|Z_i = z_i, X_{1,i} = 1]\\
&\geq R[W]/2\\
&= R'[W]^r/2
\end{aligned}$$

$$\implies R'[W|Z_{i'} = z_i, X_{1,i'} = 1] \geq R'[W]/2, \tag{41}$$

where the inequality holds by Lemma 4.9(3). Second, for any $j \in [m]$ it holds that

$$\begin{aligned}
\frac{R[W]}{2d} &\leq R[W|(Z^k X^k_{<j}) = z^k x^k_{<j}, X_{j+1,i} = 1]\\
&= R'[W|(Z^{k'} X^{k'}_{<j}) = z^{k'}_{s_i} x^{k'}_{<j,s_i}, X_{j+1,i'} = 1] \cdot \prod_{s\in[r]\setminus\{s_i\}} R'[W|(Z^{k'} X^{k'}_{<j}) = z^{k'}_s x^{k'}_{<j,s}]\\
&= R'[W|(Z^{k'} X^{k'}_{<j}) = z^{k'}_{s_i} x^{k'}_{<j,s_i}, X_{j+1,i'} = 1] \cdot \frac{R[W|(Z^k X^k_{<j}) = z^k x^k_{<j}]}{R'[W|(Z^{k'} X^{k'}_{<j}) = z^{k'}_{s_i} x^{k'}_{<j,s_i}]}\\
&\leq R'[W|(Z^{k'} X^{k'}_{<j}) = z^{k'}_{s_i} x^{k'}_{<j,s_i}, X_{j+1,i'} = 1] \cdot \frac{d \cdot R[W]}{R'[W]/d'},
\end{aligned}$$

where d and d' are the values from Claim 4.15. The first inequality holds since $z^k x^{(m+1)\times k} \in \mathcal{S}$ and since $R[W|(Z^k X^k_{<j}) = z^k x^k_{<j}, X_{j+1,i} = 1] \geq R[W|(Z^k X^k_{<j}) = z^k x^k_{<j}]/2$ (Lemma 4.9(3)) and the last one simply holds by the fact that $z^k x^{(m+1)\times k} \in \mathcal{S}$. Therefore, we deduce that

$$\forall j \in [m].\ R'[W|(Z^{k'} X^{k'}_{<j}) = z^{k'}_{s_i} x^{k'}_{<j,s_i}, X_{j+1,i'} = 1] \geq \frac{R'[W]}{2d^2 d'} > \frac{\varepsilon^3 \cdot R'[W]}{10^6 \cdot mr}. \tag{42}$$

In addition, since $z^k x^{(m+1)\times k} \in \mathcal{S}$. it holds that

$$\forall j \in [m]\ \forall s \in [r].\ R'[W|(Z^{k'} X^{k'}_{<j}) = z^{k'}_s x^{k'}_{j,s}] \geq R'[W]/d' = \frac{\varepsilon \cdot R'[W]}{72mr}, \tag{43}$$

and we deduce from Equations (40) to (43) that

$$\begin{aligned}
&\forall z^k x^{(m+1)\times k} \in \mathcal{W} \cap \mathcal{S}\ \forall i \in \operatorname{Supp}(\widehat{Q}_{I|(Z^k X^{(m+1)\times k})=z^k x^{(m+1)\times k},B=1}).\\
&\qquad (i, z^k x^{(m+1)\times k}) \in \mathcal{T}.
\end{aligned} \tag{44}$$

Hence, we conclude that

$$\begin{aligned}
Q_{I,Z^k X^{(m+1)\times k}}(\mathcal{T}) &= \widehat{Q}_{I,Z^k X^{(m+1)\times k}}(\mathcal{T})\\
&\geq \widehat{Q}_{Z^k X^{(m+1)\times k},B}(\widehat{\mathcal{S}})\\
&> 1 - \varepsilon/4,
\end{aligned}$$

as required, where the first inequality holds by Equation (44) and the second one by Equation (40). □

The proof of Theorem 4.1 for small number of repetitions, given below, follows Corollary 4.16.

Proof of Theorem 4.1 for Small Number of Repetitions. Let $(\mathrm{P}, \mathrm{V}), m, \varepsilon, k'$ be as in the statement of Theorem 4.1 (replacing k with k') and assume towards a contradiction the existence of a polynomial-time adversarial prover $\mathrm{P}^{k'^*}$ and a polynomial p such that Equation (33) holds infinity many n, where c (the constant from the theorem statement) is set to the constant c of Corollary 4.10. In the following we fix a value of n such that Corollary 4.10 holds and assume that $k' < c \cdot m^2/\varepsilon$.

In the following, let $\ell = \ell(n)$ be a (polynomial) bound on the number of random coins used by V, let $k = k' \cdot r$ for $r = \lceil c \cdot m^2/\varepsilon \rceil$ and let P^{k^*} be the adversarial prover (against $\widetilde{\mathrm{V}}^{k'}$) that divides the set of k verifiers into r sets, each of size k', and executes $\mathrm{P}^{k'^*}$ on each set (independently).

Let P^* be the adversarial prover (against V) described in Algorithm 4.4 with the new variants of GetZeroRoundCoins and GetNextRoundCoins (Algorithm 4.13 and Algorithm 4.13, respectively), let Real, $\widetilde{\text{Real}}$ and Ideal be distributions induced by P^*, let $\mathcal{W}$ be the set of all accepting (full) views of $(\mathrm{P}^{k^*}, \widetilde{\mathrm{V}}^{k})$, let $\mathcal{W}'$ be the set of all accepting (full) views of $(\mathrm{P}^{k'^*}, \widetilde{\mathrm{V}}^{k'})$, let R,P and Q be the distributions from Definitions 4.7 and 4.8 with respect to m,ℓ,k and $\mathcal{W}$ and let R',P' and Q' be distributions from Definitions 4.7 and 4.8 with respect to m,ℓ,k' and $\mathcal{W}'$.

In the following, let $\mathcal{T}$ be the set from Corollary 4.16 and let T be the event over $Q_{I,Z^kX^{(m+1)\times k}}$ that $(I, Z^kX^{(m+1)\times k}) \in \mathcal{T}$. By Corollary 4.12 it holds that

$$Q[T] > 1 - \varepsilon/4 \tag{45}$$

Since $R[W] > 1/p$, Equation (45) yields that with probability at least $1 - \varepsilon/4$ over $(i, z^kx^{(m+1)\times k}) \sim Q_{I,Z^kX^{(m+1)\times k}}$ (i.e., over $\widetilde{\text{Real}}$), T happens which yields that $1/R'[W|Z_{i'} = z_i, X_{1,i'} = 1] \leq 2p$ (i.e., the expected number of sampling attempts in the s_i'th iteration of GetZeroRoundCoins is bounded) and $\{1/R'[W|(Z^{k'}X^{k'}_{<j}) = z^{k'}_s x^{k'}_{<j,s}]\}_{j\in[m],s\in[r]\setminus\{s_i\}} \leq 72mrp/\varepsilon$ (i.e., all expected number of sampling attempts in each round $j \in [m]$ and each iteration $s \neq s_i$ of Algorithm 4.14 are bounded) and $\{1/R'[W|(Z^{k'}X^{k'}_{<j}) = z^{k'}_{s_i}x^{k'}_{<j,s_i}, X_{j+1,i'} = 1]\}_{j=1}^{m} \leq 10^6m^2rp/\varepsilon^3$ (i.e., all expected number of sampling attempts in the s_i'th iteration of each round $j \in [m]$ are bounded). By Markov inequality and union bound, conditioned on T, the probability that there exists a round $j \in [m]$ and an iteration $s \in [r]$ such that GetNextRoundCoins (the unbounded variant of Algorithm 4.14) exceeds $t = \lceil 4 \cdot 10^6m^2r^2p/\varepsilon^4 \rceil$ number of sampling attempts is at most $\varepsilon/4$. Moreover, note the expected number of sampling attempts in each iteration $s \neq s_i$ of Algorithm 4.13 is $1/R'[W] \leq p$ and recall that T implies that $1/R'[W|Z_{i'} = z_i, X_{1,i'} = 1] \leq 2p$. Therefore, conditioned on T, we obtain by Markov inequality and union bound that the probability there exists an iteration $s \in [r]$ such that GetZeroRoundCoins (the unbounded variant of Algorithm 4.13) exceeds $t_0 = \lceil 8pr/\varepsilon \rceil$ number of sampling attempts is at most $\varepsilon/4$.

In the following, given a random execution of Algorithm 4.4 (with GetZeroRoundCoins and GetZeroRoundCoins, the unbounded variants of Algorithms 4.13 and 4.14), we denote by A_0 the event that GetZeroRoundCoins finds an accepting continuation within t_0 sampling attempts in each iteration $s \in [r]$ and let A be the event that each of the m calls to GetNextRoundCoins finds an accepting continuation within t sampling attempts in each iteration $s \in [r]$. By combining all parts of above analysis, we obtain that

$$\begin{aligned}\Pr[\neg A_0 \vee \neg A] &\leq \Pr[T] + \Pr[\neg A_0 \mid T] + \Pr[\neg A \mid T] \\ &< \varepsilon/4 + \varepsilon/4 + \varepsilon/4 \\ &= 3\varepsilon/4\end{aligned}$$

Since $\mathrm{Real}\,|_{A_0 \wedge A} \equiv \widetilde{\mathrm{Real}}|_{A_0 \wedge A}$, we obtain that

$$\mathrm{SD}(\mathrm{Real}, \widetilde{\mathrm{Real}}) \leq \Pr[\neg A_0 \vee \neg A] < 3\varepsilon/4 \tag{46}$$

Finally, observe that Corollary 4.16 yields (in particular) that $\Pr\left[\widetilde{\mathrm{Real}} \in \mathcal{W}\right] > 1 - \varepsilon/4$ and we conclude that

$$\Pr[(\mathrm{P}^*, \mathrm{V}) = 1] \geq \Pr[\mathrm{Real} \in \mathcal{W}] \geq \Pr\left[\widetilde{\mathrm{Real}} \in \mathcal{W}\right] - \mathrm{SD}(\mathrm{Real}, \widetilde{\mathrm{Real}}) > 1 - \varepsilon,$$

in contradiction to the soundness property of (P, V). □

5 The Extensions of P and Q

In this section, we give the structure and a sketch of the proof of Lemma 4.9, while most of the technical details appear in Sections 6 and 7.

Rather than presenting the extensions $\widehat{P}$ and $\widehat{Q}$ of the type stated in Lemma 4.9 and prove that their smooth KL-divergence is small, we define many-bit variants of these extensions and bound their smooth KL-divergence. Lemma 4.9 then follows by a data-processing argument. Moving to many-bit extensions is useful, since the additional bits, essentially one bit per round, enable us to apply the chain rule of KL-divergence more easily for bounding their smooth KL-divergence.

The structure of this section is as follows. In Section 5.1 we give a many-bit form of Lemma 4.9, Lemma 5.3, and use it for proving Lemma 4.9. In Section 5.2, we define various functions and sets that will be crucial to the proof of Lemma 5.3. We explain these definitions by sketching the proof for the divergence-bound part of Lemma 5.3. In Section 5.3, we define—using the aforementioned functions and sets—the many-bit extensions required by Lemma 5.3. In Section 5.4, we state two major properties of these extensions (proven in Sections 6 and 7) and use those properties to derive Lemma 5.3.

5.1 A Many-bit Variant of Lemma 4.9

In this section we state a many-bit variant form of Lemma 4.9 that we find easier to work with, and show that it implies Lemma 4.9. In addition, to make the analysis of the last round similar to previous rounds, we add an additional "row" to the distribution R defined in previous section. In this section, we use the following definitions which are equivalent to Definitions 4.7 and 4.8.

Definition 5.1 (The distributions R and P, and the event W, revisited). *For $k, m, \ell \in \mathbb{N}$ and $\mathcal{W} \subseteq \{0,1\}^{kl+k(m+1)}$, define $R = R_{Z^k X^{(m+2)\times k}} = R_{Z^k} R_{X^{(m+2)\times k}}$ by $R_{Z^k} = \prod_{i=1}^k R_{Z_i}$, $R_{Z_i} = U_\ell$, $R_{X^{(m+2)\times k}} = \prod_{i=1}^k R_{X_{1,i}X_{2,i}\cdots X_{m+2,i}}$, and $R_{X_{j,i}|X_{<j,i}} = \begin{cases}\mathrm{Bern}(0) & 1 \in X_{<j,i} \\ \mathrm{Bern}(1/m) & o.w.\end{cases}$. Let W be an event over R that $Z^k X^{(m+1)\times k} \in \mathcal{W}$. Finally, define $P = P_{Z^k X^{(m+1)\times k}} = R_{Z^k X^{(m+1)\times k}|W}$.*

Namely, the only difference from Definition 4.7 is that now R has also an $(m+2)$'th row X^k_{m+2}. Yet, it is easy to verify that the distribution of $R_{Z^kX^{(m+1)\times k}}$ (i.e., without the $(m+2)$'th row) and $P_{Z^kX^{(m+1)\times k}}$ are equal to the ones in Definition 4.7.

Definition 5.2 (The distribution Q, revisited)**.** *For $k,m,\ell\in\mathbb{N}$ and for a termination consistent set $\mathcal{W}\subseteq\{0,1\}^{kl+k(m+1)}$ (according to Definition 4.3), define $Q=Q_{I,Z^kX^{(m+1)\times k}}=Q_IQ_{Z^kX^{(m+1)\times k}|I}$ by $Q_I=U_{[k]}$, $Q_{Z^k|I}=R_{Z_I}P_{Z_{-I}|Z_I,X_{1,I}=1}$, $Q_{X^k_j|IZ^kX^k_{<j}}=P_{X^k_j|Z^kX^k_{<j},X_{j+1,I}=1}$, and $Q_{X^k_{m+1}|IZ^kX^k_{\le m}}=$*

$$\begin{cases} P_{X^k_{m+1}|Z^kX^k_{\le m},X_{m+2,I}=1} & R[W|Z^kX^k_{\le m},X_{m+2,I}=1]>0 \\ 0^k & o.w. \end{cases}.$$

Namely, the only difference from Definition 4.8 is how we define $Q_{X^k_{m+1}|IZ^kX^k_{\le m}}$: In Definition 4.8 we defined it using $P_{X^k_{m+1}|Z^kX^k_{\le m},X_{m+1,I}=0}$ while in Definition 5.2 we defined it using $P_{X^k_{m+1}|Z^kX^k_{\le m},X_{m+2,I}=1}$. Yet, observe that by definition of R and P in Definition 5.1, both definitions are equivalent since

$$P_{X^k_{m+1}|Z^kX^k_{\le m},X_{m+2,I}=1}\equiv P_{X^k_{m+1}|Z^kX^k_{\le m},X_{m+1,I}=0,X_{m+2,I}=1}\equiv P_{X^k_{m+1}|Z^kX^k_{\le m},X_{m+1,I}=0}$$

where the first equivalence holds since $X_{m+2,I}=1\implies X_{m+1,I}=0$, and the second one holds since given $Z^kX^k_{\le m}X_{m+1,I}$, the event W in R is independent of $X_{m+2,I}$.

Lemma 5.3. *Let $k,m,\ell\in\mathbb{N}$, let $\varepsilon\in(0,1/2]$, let $\mathcal{W}\subseteq\{0,1\}^{k\ell+k(m+1)}$ be a termination-consistent set (according to Definition 4.3) and let W, R, P and Q, be the event and distributions from Definitions 5.1 and 5.2 with respect to $\mathcal{W},m,k,\ell$, respectively. Assume $k\ge\lambda\cdot m^2/\varepsilon$ and $R[W]>(1-\varepsilon)^{\frac{k}{\lambda\cdot m}}$ for some universal constant $\lambda>0$. Then there exist distributions $\widehat{P}=\widehat{P}_{B_0,Z^k,B_1,X^k_1,\ldots,B_{m+1},X^k_{m+1}}$ and $\widehat{Q}=\widehat{Q}_{I,B_0,Z^k,B_1,X^k_1,\ldots,B_{m+1},X^k_{m+1}}$ with $\widehat{P}_{Z^kX^{(m+1)\times k}}=P$ and $\widehat{Q}_{I,Z^kX^{(m+1)\times k}}=Q$ and with $\operatorname{Supp}(\widehat{P}_{B_j}),\operatorname{Supp}(\widehat{Q}_{B_j})\subseteq\{0,1\}$ for $j\in(m+1)$, such that the following holds:*

1. *$D^{\frac{\varepsilon}{24}}(\widehat{P}||\widehat{Q}_{B_0,Z^k,B_1,X^k_1,\ldots,B_{m+1},X^k_{m+1}})\le\frac{\lambda m}{k}\cdot\left(\log\frac{1}{R[W]}+m\right)$.*
2. *$\widehat{P}_{B^{m+2}}(1^{m+2})\ge 1-\varepsilon/24$, for $B^{m+2}=B_0,\ldots,B_{m+1}$.*
3. *$\forall(i,z^kx^{(m+1)\times k})\in\operatorname{Supp}(\widehat{Q}_{I,Z^kX^{(m+1)\times k}|B^{m+2}=1^{m+2}})$:*
   - *(a) $R[W|Z_i=z_i,X_{1,i}=1]\ge R[W]/2$.*
   - *(b) $\forall j\in[m+1]: R[W|Z^kX^k_{<j}=z^kx^k_{<j},X_{j+1,i}=1]\ge R[W|Z^kX^k_{<j}=z^kx^k_{<j}]/2$.*

That is, the extensions above have $m+2$ additional bits, essentially one per round, rather than a single additional bit in Lemma 4.9. The logical conjunction (i.e., And) of these bits takes the role of the single bit in the extensions considered in Lemma 4.9.

Lemma 5.3 yields Lemma 4.9 via the data-processing property of the smooth KL-divergence.

Proof of Lemma 4.9. Let $\widehat{P}$ and $\widehat{Q}$ be the distributions guaranteed by Lemma 5.3. Let $\widehat{P}'_{Z^k,X^{(m+1)\times k},B}=(\widehat{P}_{Z^k,X^{(m+1)\times k}|B^{m+2}}T_{B|B^{m+2}})\circ\widehat{P}_{B^{m+2}}$ for $T_{B|B^{m+2}=B_0,\ldots,B_{m+1}}=\prod_{j=0}^{m+1}B_j$, and $\widehat{Q}'_{I,Z^kX^{(m+1)k},B}=(\widehat{Q}_{I,Z^kX^{(m+1)k}|B^{m+2}}T_{B|B^{m+2}})\circ\widehat{Q}_{B^{m+2}}$. We show that $\widehat{P}'$ and $\widehat{Q}'$ have the properties required in Lemma 4.9.

The data-processing property of smooth KL-divergence (Proposition 3.12) and Lemma 5.3(1), yield that

$$D^{\frac{\varepsilon}{24}}(\widehat{P}'||\widehat{Q}'_{Z^k,X^{(m+1)k},B}) \leq \frac{\lambda m}{k} \cdot \left(\log \frac{1}{R[W]} + m\right). \tag{47}$$

Lemma 5.3(2) yields that

$$\widehat{P}'_B(1) \geq 1 - \varepsilon/24. \tag{48}$$

Finally, Lemma 5.3(3) yields that for every $\forall(i, z^k x^{(m+1)\times k}) \in \mathrm{Supp}(\widehat{Q}'_{I,Z^k X^{(m+1)\times k}|B=1})$:

1. $R[W|Z_i = z_i, X_{1,i} = 1] \geq R[W]/2$.
2. $\forall j \in [m+1] : R[W|Z^k X^k_{<j} = z^k x^k_{<j}, X_{j+1,i} = 1] \geq R[W|Z^k X^k_{<j} = z^k x^k_{<j}]/2$.

□

5.2 Definitions and Motivating Discussion

Let R,P and Q as defined in Definitions 5.1 and 5.2. For $j \in [m+1]$, $i \in [k]$ and $z^k x^{(m+1)\times k} \in \mathrm{Supp}(P_{Z^k X^{(m+1)\times k}})$, consider the definitions appear in Tables 1 and 2.

Table 1: Measurements.

Definition	*Value*
$\rho_{0,i}$	$m \cdot P_{X_{1,i}}(1) - 1$
$\rho_{j,i}(z^k x^k_{<j})$	$P_{X_{j+1,i} \mid Z^k X^k_{<j}}(1 \mid z^k x^k_{<j}) / \left(\frac{1}{m}(1 - \frac{1}{m})\right) - 1$
$\beta_{j,i}(z^k x^k_{<j})$ (for $j \geq 2$)	$\frac{P_{X_{j,i} \mid Z^k X^k_{<j}}(1 \mid z^k x^k_{<j})}{P_{X_{j,i} \mid Z^k X^k_{<j-1}}(1 \mid z^k x^k_{<j-1})} - 1$
$\alpha_{0,i}(z)$	$\frac{R_{Z_i}(z)}{P_{Z_i \mid X_{1,i}=1}(z)} \cdot \mathbb{1}\{(i,z) \in \mathcal{D}\}$
$\alpha_{j,i}(z^k x^k_{<j})$	$\frac{R_{Z_i}(z_i)}{P_{Z_i}(z_i)} \cdot \frac{P_{X_{1,i} \mid Z^k}(1 \mid z^k)}{P_{X_{1,i} \mid Z_i}(1 \mid z_i)} \cdot \prod_{j'=2}^{j}(1 + \beta_{j',i}(z^k x^k_{<j'}))$
$\delta_0(z^k x^k_1)$	$\left(\sum_{i \in 1_{x^k_1}} \frac{\mathbb{1}\{(i,z) \in \mathcal{D}\}}{P_{Z_i X_{1,i}}(z_i 1)}\right) / \lvert\mathcal{D}\rvert - 1 = \left(\sum_{i \in 1_{x^k_1}} \frac{\alpha_{0,i}(z_i)}{P_{X_{1,i}}(1)}\right) / \left(\lvert\mathcal{D}\rvert / 2^\ell\right) - 1$
$\delta_j(x^k_{j+1}; z^k x^k_{<j})$	$\left(\sum_{i \in \mathcal{G}_{z^k x^k_{<j}} \bigcap 1_{x^k_{j+1}}} \frac{\alpha_{j,i}(z^k x^k_{<j})}{P_{X_{j+1,i} \mid Z^k X^k_{<j}}(1 \mid z^k x^k_{<j})}\right) / \left(\sum_{i \in \mathcal{G}_{z^k x^k_{<j}}} \alpha_{j,i}(z^k x^k_{<j})\right) - 1$

In order to explain the rather complex definitions in Tables 1 and 2 and why we actually need to use smooth extensions, we give a rather detailed proof sketch (more accurately, an attempt proof sketch) for the divergence-bound part of Lemma 5.3. Specifically, we try to bound the divergence between $P_{Z^k X^{(m+1)\times k}}$ and $Q_{Z^k X^{(m+1)\times k}}$; that is, to show that

$$D(P_{Z^k X^{(m+1)\times k}}||Q_{Z^k X^{(m+1)\times k}}) \leq O\left(\frac{m}{k} \cdot (D(P_{Z^k X^{(m+1)\times k}}||R_{Z^k X^{(m+1)\times k}}) + m)\right). \tag{49}$$

Since $D(P_{Z^k X^{(m+1)\times k}}||R_{Z^k X^{(m+1)\times k}}) \leq \log(1/R[W])$ (Fact 3.6), establishing the bound in Equation (49) would indeed show the divergence-bound part of Lemma 5.3. Furthermore, recall that

Table 2: Sets.

Definition	*Value*
$\mathcal{I}_{x^k_{<j}}$	$\{i \in [k] \colon x_{1,i} = x_{2,i} = \cdots = x_{j-1,i} = 0\}$
$\mathcal{G}$	$\{i \in [k] \colon \lvert\rho_{0,i}\rvert \le 0.1\}$
$\mathcal{G}_{z^k x^k_{<j}}$	$\{i \in \mathcal{G}_{z^k x^k_{<j-1}} \colon \left(\left\lvert\rho_{j,i}(z^k x^k_{<j})\right\rvert \le 0.1\right) \wedge \left(\alpha_{j,i}(z^k x^k_{<j}) \in [0.01, 10]\right)\}$ where we denote $\mathcal{G}_{z^k x^k_{<0}} = \mathcal{G}$
$\mathcal{Z}_i$	$\{z \in \{0,1\}^\ell \colon P_{Z_i \mid X_{1,i}=1}(z) \in (1 \pm 0.1) \cdot 2^{-\ell}\}$
$\mathcal{D}$	$\{(i,z) \in [k] \times \{0,1\}^\ell \colon (i,z) \in \mathcal{G} \times \mathcal{Z}_i\}$

in the public-coin case, Chung and Pass [CP15] bound the divergence between P (the Ideal distribution) and Q (the $\widetilde{\text{Real}}$ distributions) with $\frac{1}{k} \cdot D(P_{Z^k X^{m\times k}} || R_{Z^k X^{m\times k}})$ (we abuse notation to fit their result to the current discussion). Our bound on the exponential decay of the soundness error (Theorem 4.1) is $\Omega(k/m)$—as oppose to the optimal decay of $\Omega(k)$ in the public-coin case—comes exactly from the difference between the coefficients of the divergence in Equation (49) and in the the public-coin bound (i.e., m/k vs. $1/k$).

The first step to prove Equation (49) would naturally be to apply the chain rule for divergence:

$$D(P_{Z^k X^{(m+1)\times k}} || Q_{Z^k X^{(m+1)\times k}}) = D(P_{Z^k} || Q_{Z^k}) + \sum_{j=1}^{m+1} D(P_{X^k_j \mid Z^k X^k_{<j}} || Q_{X^k_j \mid Z^k X^k_{<j}} \mid P_{Z^k X^k_{<j}}).$$

In this sketch we focus on bounding the divergence for a fixed round $1 \le j \le m+1$. The sketch for the zero round (i.e., Z^k) is similar, and at the end we shortly explain the differences.

Let's take a closer look at the j'th round of the $\widetilde{\text{Real}}$ distribution. In that round, the prover P^* samples the coins of the internal verifiers conditioned on the external verifier, which is located at index i chosen at the start of the execution, aborting in the $j+1$ round. Importantly, however, we are interested in the distribution of the coins of the verifiers, not in that of the index i. More formally, we are concerned with $Q_{X^k_j \mid Z^k X^k_{<j}}$, and not with $Q_{X^k_j \mid I Z^k X^k_{<j}}$, where we also condition on I. It holds that

$$\begin{aligned} Q_{X^k_j \mid Z^k X^k_{<j}} &= P_{X^k_j \mid Z^k X^k_{<j}, X_{j+1,I}=1} \circ Q_{I \mid Z^k X^k_{<j}} \\ &= P_{X^k_j \mid Z^k X^k_{<j} X^k_{j+1}} \circ P_{X^k_{j+1} \mid Z^k X^k_{<j}, X_{j+1,I}=1} \circ Q_{I \mid Z^k X^k_{<j}}. \end{aligned}$$

Namely, the distribution of round j of the $\widetilde{\text{Real}}$ distribution can be described as follows: first draw an index I conditioned on the transcript so far, then draw the $j+1$ round conditioned on the transcript and that its I^{th} location is equal 1 (i.e., aborts), and finally draw the j'th round conditioned on the transcript and the $j+1$ round. Recall that by conditioning that the I^{th} verifier aborts in round $j+1$, we are guaranteed that this verifier does not abort in round j. The distribution P can also be naturally described in the terms of the $j+1$ round:

$$P_{X^k_j \mid Z^k X^k_{<j}} = P_{X^k_j \mid Z^k X^k_{<j} X^k_{j+1}} \circ P_{X^k_{j+1} \mid Z^k X^k_{<j}}.$$

Now, the data-processing inequality for divergence yields that

$$D(P_{X^k_j \mid Z^k X^k_{<j}} || Q_{X^k_j \mid Z^k X^k_{<j}} \mid P_{Z^k X^k_{<j}}) \le D(P_{X^k_{j+1} \mid Z^k X^k_{<j}} || Q'_{X^k_{j+1} \mid Z^k X^k_{<j}} \mid P_{Z^k X^k_{<j}}),$$

for $Q'_{X^k_{j+1}|Z^k X^k_{<j}} = P_{X^k_{j+1}|Z^k X^k_{<j}, X_{j+1,I}=1} \circ Q_{I|Z^k X^k_{<j}}$.

So, we have transforms our question for round j to a different question for round $j+1$—what is the divergence between choosing the $j+1$ round according to P given a partial transcript up to round $j-1$, to choosing the same round also condition on the I index being 1, where I is chosen according to $Q_{I|Z^k X^k_{<j}}$? This is the reason that many of the definitions in Tables 1 and 2 take x^k_{j+1} into account.

To answer this question we need to better understand $Q_{I|Z^k X^k_{<j}}$. With no prior transcript, Q_I is simply uniform on the set of indexes $[k]$. However, conditioned on a transcript $z^k x^k_{<j}$, $Q_{I|Z^k X^k_{<j}}$ puts more weight on indexes that are likely to be 1 in round $j+1$ of P. How this likelihood changes from conditioning on the previous $j-2$ rounds to conditioning on the previous $j-1$ rounds is measured by $\beta_{i,j}(z^k x^k_{<j})$. The total likelihood changes that accumulated from all previous rounds is measured by $\alpha_{j,i}(z^k x^k_{<j})$. So, $Q_{I|Z^k X^k_{<j}}$ puts more weight on indexes with high $\alpha_{j,i}(z^k x^k_{<j})$. This high-level intuition is formalized in the next claim (this claim, as well as all others in this sketch, is proven in Appendix A.3).

Claim 5.4. *Let $j \in [m+1]$ and $\tau = (z^k x^k_{<j}) \in \operatorname{Supp}(P_{Z^k X^k_{<j}})$. Then, for every $i \in \mathcal{G}_\tau$ it holds that*

$$Q_{I|Z^k X^k_{<j}, I \in \mathcal{G}_\tau}(i|z^k x^k_{<j}) = \frac{\alpha_{j,i}(z^k x^k_{<j})}{\sum_{i' \in \mathcal{G}_\tau} \alpha_{j,i'}(z^k x^k_{<j})}$$

For now, think of the set $\mathcal{G}_\tau$ in the above claim as $\mathcal{I}_{x^k_{<j}}$—the set of active indexes in round j; namely, the verifiers that have not aborted yet. Since in Q (the $\widetilde{\text{Real}}$ distribution) the external verifier never aborts (it is the original verifier V, and not the random terminating verifier $\widetilde{\text{V}}$), a verifier that aborted cannot be the external verifier; that is, it holds that $Q_{I|Z^k X^k_{<j}}(i|z^k x^k_{<j}) = 0$ for every $i \notin \mathcal{I}_{x^k_{<j}}$, and thus $Q_{I|Z^k X^k_{<j}} = Q_{I|Z^k X^k_{<j}, I \in \mathcal{I}_{X^k_{<j}}}$. We will circle back to the set $\mathcal{G}_\tau$ later in this sketch.

Using Claim 5.4 we can now give an exact measurement for the ratio between the pmfs of P and Q, which turns out to also depend on the probability of a given index being 1 in the $j+1$ round.

Claim 5.5. *Let $j \in [m+1]$, let $\tau = (z^k x^k_{<j}) \in \operatorname{Supp}(P_{Z^k X^k_{<j}})$, and let $Q'_{X^k_{j+1}|Z^k X^k_{<j}} = P_{X^k_{j+1}|Z^k X^k_{<j} X_{j+1,I}=1} \circ Q_{I|Z^k X^k_{<j}, I \in \mathcal{G}_\tau}$. Then, for every $x^k_{j+1} \in \operatorname{Supp}(P_{X^k_{j+1}|(Z^k X^k_{<j})=\tau})$ with $1_{x^k_{j+1}} \cap \mathcal{G}_\tau \neq \emptyset$, it holds that*

$$\frac{P_{X^k_{j+1}|Z^k X^k_{<j}}(x^k_{j+1}|\tau)}{Q'_{X^k_{j+1}|Z^k X^k_{<j}}(x^k_{j+1}|\tau)} = \frac{\sum_{i \in \mathcal{G}_\tau} \alpha_{j,i}(\tau)}{\sum_{i \in 1_{x^k_{j+1}} \cap \mathcal{G}_\tau} \frac{\alpha_{j,i}(\tau)}{p_i(\tau)}},$$

for $p_i(\tau) = P_{X_{j+1,i}|Z^k X^k_{<j}}(1|\tau)$.

Fix some previous transcript $\tau = (z^k x^k_{<j})$. Rearranging the above equation, we have that

$$\frac{Q'_{X^k_{j+1}|Z^k X^k_{<j}}(x^k_{j+1}|\tau)}{P_{X^k_{j+1}|Z^k X^k_{<j}}(x^k_{j+1}|\tau)} = \sum_{i \in 1_{x^k_{j+1}} \cap \mathcal{G}_\tau} \frac{Q_{I|Z^k X^k_{<j}, I \in \mathcal{G}_\tau}(i|\tau)}{p_i(\tau)}.$$

As a sanity check, let's see what happens to this ratio when W does not change the random coins' distribution (i.e., $R_{Z^k X^{(m+1)\times k}} = P$). We expect there to be roughly k/m ones in x^k_{j+1} (that many verifiers are expected to abort in round $j+1$). For each such index i, it would hold that $Q_{I|Z^kX^k_{<j},I\in\mathcal{G}_\tau}(i|\tau) \approx 1/k$ and $p_i(\tau) \approx 1/m$. Hence, the above ratio is roughly 1, which is what we would expect. Another interpretation for the above ratio is given in the following expectation.

$$\frac{Q'_{X^k_{j+1}|Z^kX^k_{<j}}(x^k_{j+1}|\tau)}{P_{X^k_{j+1}|Z^kX^k_{<j}}(x^k_{j+1}|\tau)} \propto \mathop{\mathrm{E}}_{i\sim Q_{I|Z^kX^k_{<j},I\in\mathcal{G}_\tau\cap 1_{x^k_{j+1}}}}\left[\frac{1}{p_i(\tau)}\right].$$

Namely, choose a random 1-index in x^k_{j+1} according to Q, and measure how likely it is for the verifier in that index to abort in Q (which happens with probability 1 since Q sets that verifier to abort in round $j+1$) vs. how likely it aborts in P (which is $p_i(\tau)$).

Using Claim 5.5, our goal has now become to bound

$$D(P_{X^k_{j+1}|(Z^kX^k_{<j})=\tau}||Q'_{X^k_{j+1}|(Z^kX^k_{<j})=\tau}) = \mathop{\mathrm{E}}_{x^k_{j+1}\sim P_{X^k_{j+1}|(Z^kX^k_{<j})=\tau}}\left[\log\frac{\sum_{i\in\mathcal{G}_\tau}\alpha_{j,i}(\tau)}{\sum_{i\in 1_{x^k_{j+1}}\cap\mathcal{G}_\tau}\frac{\alpha_{j,i}(\tau)}{p_i(\tau)}}\right].$$

The next claim shows how to interpret the denominator in the above expectation as a sum of random variables, whose expected value is exactly the nominator.

Claim 5.6. *Let* $j\in[m+1]$, *let* $\tau=(z^kx^k_{<j})\in\mathrm{Supp}(P_{Z^kX^k_{<j}})$, *and let* X^k_{j+1} *be drawn from* $P_{X^k_{j+1}|(Z^kX^k_{<j})=\tau}$ *or from* $\prod_{i=1}^k P_{X_{j+1,i}|(Z^kX^k_{<j})=\tau}$.[23] *Let* $Y=\sum_{i\in\mathcal{G}_\tau}Y_i$, *for* $Y_i=\frac{\alpha_{j,i}(\tau)}{P_{X^k_{j+1,i}|Z^kX^k_{<j}}(1|\tau)}$ *if* $X_{j+1,i}=1$ *and* $Y_i=0$ *otherwise.*

It holds that

$$\mathrm{E}_{P_{X^k_{j+1}|(Z^kX^k_{<j})=\tau}}[Y] = \mathrm{E}_{\prod_{i=1}^k P_{X_{j+1,i}|(Z^kX^k_{<j})=\tau}}[Y] = \sum_{i\in\mathcal{G}_\tau}\alpha_{j,i}(\tau).$$

Let $\Delta = \delta_j(X^k_{j+1};\tau)$, where X^k_{j+1} is drawn from either $P_{X^k_{j+1}|(Z^kX^k_{<j})=\tau}$ or $\prod_{i=1}^k P_{X_{j+1,i}|(Z^kX^k_{<j})=\tau}$. The definition of δ_j implies that Δ is a random variable that measures how far Y is from its expected value; that is, $Y=(1+\Delta)\cdot\sum_{i\in\mathcal{G}_\tau}\alpha_{j,i}(\tau)$. It follows that

$$D(P_{X^k_{j+1}|(Z^kX^k_{<j})=\tau}||Q'_{X^k_{j+1}|(Z^kX^k_{<j})=\tau}) = \mathrm{E}_{P_{X^k_{j+1}|(Z^kX^k_{<j})=\tau}}\left[\log\frac{1}{1+\Delta}\right].$$

Naturally, we would like to approximate $\log\left(\frac{1}{1+\Delta}\right)$ with a low-degree polynomial. To do so, however, we need a bound on the value of Δ. This bound (among other things that we will see ahead) is exactly what the $(m+2)$-extensions will give us—they'll guarantee that $|\Delta|\leq 1/2$ with high

[23] $\prod_{i=1}^k P_{X_{j+1,i}|(Z^kX^k_{<j})=\tau}$ is the product distribution of the marginals of $P_{X^k_{j+1}|(Z^kX^k_{<j})=\tau}$.

probability under P. Roughly, we would get that

$$\begin{aligned} D(P_{X^k_{j+1}|(Z^k X^k_{<j})=\tau} || Q'_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}) &\lesssim D(P_{X^k_{j+1}|(Z^k X^k_{<j})=\tau, |\Delta|\leq 1/2} || Q'_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}) + O\Big(\frac{m}{k}\Big) \\ &\approx \mathrm{E}\bigg[\log \frac{1}{1+\Delta}\bigg| |\Delta| \leq 1/2\bigg] + O\Big(\frac{m}{k}\Big) \\ &\leq \mathrm{E}\big[-\Delta + \Delta^2 \big| |\Delta| \leq 1/2\big] + O\Big(\frac{m}{k}\Big), \end{aligned}$$

where the above expectation is over $P_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}$. Since Δ measures how far Y is from its expected value, it follows that $\mathrm{E}[\Delta] = 0$. This, however, does not hold when we also condition on $|\Delta| \leq 1/2$. But, since we are guaranteed (from the extension) that $|\Delta| \leq 1/2$ with high probability, we would be able to show that $\mathrm{E}[-\Delta||\Delta| \leq 1/2] \leq O(m/k)$.

We are left with the expected value of Δ^2. We ignore the condition on $|\Delta| \leq 1/2$ in this proof sketch (handling this condition follows again from the guarantee that $|\Delta| \leq 1/2$ with high probability and is fairly technical, so we defer this case to the formal proof). Instead, we would like to show that

$$\mathrm{E}\big[\Delta^2\big] \leq O\Big(\frac{m}{k} \cdot \Big(D(P_{X^k_{j+1}|(Z^k X^k_{<j})=\tau} || R_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}) + 1\Big)\Big). \tag{50}$$

Combining Equation (50) with the previous bounds we established and applying the chain rule once more would yield Equation (49) (ignoring the zero round).

To show that Equation (50) holds, we would use Proposition 3.10, which requires that Δ is well concentrated under $R_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}$. It would in fact be easier to show that Δ is well-concentrated under a different distribution: $P^{\Pi}_{X^k_{j+1}|(Z^k X^k_{<j})=\tau} = \prod_{i=1}^{k} P_{X_{j+1,i}|(Z^k X^k_{<j})=\tau}$. Showing this would suffice, since $R_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}$ is a product distribution, so the chain rule for divergence yields that

$$D(P_{X^k_{j+1}|(Z^k X^k_{<j})=\tau} || R_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}) \geq D(P_{X^k_{j+1}|(Z^k X^k_{<j})=\tau} || P^{\Pi}_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}).$$

Why is Δ well-concentrated under $P^{\Pi}_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}$? First, note that by Claim 5.6, the expected value of Δ under $P^{\Pi}_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}$ is 0 as well. So instead of arguing that Δ is well-concentrated around 0, we argue that $Y = \sum_{i \in \mathcal{G}_\tau} Y_i$ is well concentrated around its mean. Importantly, the random variables Y_i's are now, under $P^{\Pi}_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}$, *independent*. Hence, to bound how far Y is from its mean we can use standard concentration bounds, such as Hoeffding's inequality (Fact 3.14) or Fact 3.16. Such bounds, however, require that the Y_i's are bounded. We again use the extension to ensure that the Y_i's are indeed bounded.

Finally, we consider the definition of the set $\mathcal{G}_\tau$ from Table 2. That definition guarantees that $Y_i \leq O(m)$ for every $i \in \mathcal{G}_\tau$. Indeed, for every such i, we have that $\alpha_{j,i}(\tau) \in \Theta(1)$ and that $p_i(\tau) \geq \Omega(1/m)$. Our extension will now guarantee that the index I chosen by Q belongs to the set $\mathcal{G}_\tau$ and that $|\mathcal{G}_\tau| \geq \Omega(k)$. Using these properties, Fact 3.16 indeed yields the required concentration bound.

This concludes the proof sketch for the j'th round. The proof for the zero round is similar, but differ in the following major manner—when we condition on $X_{j+1,i} = 1$, the definition of P implies that $X_{j,i} = 0$. In the first round, this does not hold, and conditioned on $X_{1,i} = 1$, the coins Z_i are still uniform. Instead of applying the data-processing inequality to consider the divergence of the $j+1$ round, in the zero round we apply the monotonicity property of divergence to consider the divergence of both the zero and the first round. In particular, the ratio between P and Q distributions include both the zero and the first round (in round j, as shown by Claim 5.5, this ratio depends only on the $j+1$ round). This is evident in the definitions of $\alpha_{0,i}$ and δ_0 in Table 1. This also implies a change in the random variable Y, as given in the next claim (analogous to Claim 5.6).

Claim 5.7. *Let $Z^k X_1^k$ be drawn from $P_{Z^k X_1^k}$ or from $\prod_{i=1}^k P_{Z_i X_{1,i}}$.*[24] *Let $Y = \sum_{i \in [k]} Y_i$, for $Y_i = \frac{\alpha_{0,i}(z_i)}{P_{X_{1,i}}(1)}$ if $X_{1,i} = 1$ and $Y_i = 0$ otherwise.*

It holds that

$$\mathrm{E}_{P_{Z^k X_1^k}}[Y] = \mathrm{E}_{\prod_{i=1}^k P_{Z_i X_{1,i}}}[Y] = \frac{|\mathcal{D}|}{2^\ell}.$$

Finally, since Y takes into account the zero and the first round, arguing that it is concentrated around its mean is more complicated, and we leave the details to the formal proof.

This concludes the proof sketch. The formal proofs of the claims in this sketch appear in Appendix A.3. We now proceed to define the $m+2$ extensions $\widehat{P}$ and $\widehat{Q}$.

5.3 The Extensions

In this section we define the two extensions $\widehat{P}$ and $\widehat{Q}$ of the P and Q (respectively), as required for proving Lemma 5.3.

Recall from the proof sketch in Section 5.2 that the extensions should guarantee the following properties: (1) the probability that $|\Delta| \leq 1/2$ in round $j+1$ is high given any transcript τ up to round $j-1$; (2) the size of $\mathcal{G}_\tau$ is $\Omega(k)$; and (3) the index chosen by Q is in $\mathcal{G}_\tau$.

With these goals in mind, we now formally define the following two extensions. After the definitions we state and prove their important properties.

Definition 5.8 ($\widehat{P}$)**.** *Let $\widehat{P}_{B_0, Z^k, B_1, X_1^k, \ldots, B_{m+1}, X_{m+1}^k} = P_{Z^k X^{(m+1) \times k}} \widehat{P}_{B_0 | Z^k X_1^k} \prod_{j=1}^{m+1} \widehat{P}_{B_j | Z^k X_{\leq j}^k}$ be defined as follows:*

1. $\widehat{P}_{B_0 | Z^k X_1^k} = \widehat{P}_{B_0 | B_0^{\text{cur}} B_0^{\text{hist}} B_0^{\text{indx}}} \circ \widehat{P}_{B_0^{\text{cur}} | Z^k X_1^k} \widehat{P}_{B_0^{\text{hist}}} \widehat{P}_{B_0^{\text{indx}}}$, *where*
   (a) $\widehat{P}_{B_0^{\text{cur}} | Z^k X_1^k} = \mathbb{1}\{\left|\delta_0(Z^k X_1^k)\right| \leq \frac{1}{2}\}$
   (b) $\widehat{P}_{B_0^{\text{hist}}} = \mathbb{1}\{|\mathcal{D}| \geq k \cdot 2^{\ell-1}\} \cdot \mathbb{1}\{\mathrm{E}_{P_{Z^k X_1^k}}\left[\widehat{P}_{B_0^{\text{cur}} | Z^k X_1^k}(0)\right] \leq \frac{m}{k^2}\}$
   (c) $\widehat{P}_{B_0^{\text{indx}}} = \mathbb{1}\{(I, Z_I) \in \mathcal{D}\} \circ Q_{I, Z_I}$
   (d) $\widehat{P}_{B_0 | B_0^{\text{cur}} B_0^{\text{hist}} B_0^{\text{indx}}} = B_0^{\text{cur}} \cdot B_0^{\text{hist}} \cdot B_0^{\text{indx}}$.
2. $\widehat{P}_{B_j | Z^k X_{\leq j}^k} = \widehat{P}_{B_j | B_j^{\text{cur}} B_j^{\text{hist}} B_j^{\text{indx}}} \circ \widehat{P}_{B_j^{\text{cur}} | Z^k X_{\leq j}^k} \widehat{P}_{B_j^{\text{hist}} | Z^k X_{<j}^k} \widehat{P}_{B_j^{\text{indx}} | Z^k X_{<j}^k}$ *for $j \in [m+1]$, where*
   (a) $\widehat{P}_{B_j^{\text{cur}} | Z^k X_{\leq j}^k} = \mathrm{Bern}\Big(P_{X_{j+1}^k | Z^k X_{\leq j}^k}\left[\left|\delta_j(X_{j+1}^k; Z^k X_{<j}^k)\right| \leq \frac{1}{2}\right]\Big)$
   (b) $\widehat{P}_{B_j^{\text{hist}} | Z^k X_{<j}^k} = \mathbb{1}\{\left|\mathcal{G}_{Z^k X_{<j}^k}\right| \geq \frac{k}{10}\} \cdot \mathbb{1}\{\mathrm{E}_{P_{X_j^k | Z^k X_{<j}^k}}\left[\widehat{P}_{B_j^{\text{cur}} | Z^k X_{\leq j}^k}(0)\right] \leq \frac{m}{k^2}\}$

[24] $\prod_{i=1}^k P_{Z_i X_{1,i}}$ is the product distribution of the marginals of $P_{Z^k X_1^k}$.

(c) $\widehat{P}_{B_j^{\mathrm{indx}}|Z^k X_{<j}^k} = \mathbb{1}\{I \in \mathcal{G}_{Z^k X_{<j}^k}\} \circ Q_{I|Z^k X_{<j}^k, I \in \mathcal{G}_{Z^k X_{<j-1}^k}}$

(d) $\widehat{P}_{B_j|B_j^{\mathrm{cur}} B_j^{\mathrm{hist}} B_j^{\mathrm{indx}}} = B_j^{\mathrm{cur}} \cdot B_j^{\mathrm{hist}} \cdot B_j^{\mathrm{indx}}$.

Definition 5.9 ($\widehat{Q}$)**.** *Let* $\widehat{Q}_{I,B_0,Z^k,B_1,X_1^k,\ldots,B_{m+1},X_{m+1}^k} = Q_I Q_{Z^k X^{(m+1)\times k}|I} \widehat{Q}_{B_0|I,Z^k X_1^k} \prod_{j=1}^{m+1} \widehat{Q}_{B_j|I,Z^k X_{<j}^k}$ *be defined as follows:*

1. $\widehat{Q}_{B_0|I,Z^k X_1^k} = \widehat{P}_{B_0|B_0^{\mathrm{cur}} B_0^{\mathrm{hist}} B_0^{\mathrm{indx}}} \circ \widehat{Q}_{B_0^{\mathrm{cur}}} \widehat{Q}_{B_0^{\mathrm{hist}}} \widehat{Q}_{B_0^{\mathrm{indx}}|I,Z_I}$, *where*

   (a) $\widehat{Q}_{B_0^{\mathrm{cur}}} = \widehat{P}_{B_0^{\mathrm{cur}}|Z^k X_1^k} \circ \widehat{P}_{Z^k X_1^k}$

   (b) $\widehat{Q}_{B_0^{\mathrm{hist}}} = \widehat{P}_{B_0^{\mathrm{hist}}}$

   (c) $\widehat{Q}_{B_0^{\mathrm{indx}}|I,Z_I} = \mathbb{1}\{(I, Z_I) \in \mathcal{D}\}$.

2. $\widehat{Q}_{B_j|I,Z^k X_{<j}^k} = \widehat{P}_{B_j|B_j^{\mathrm{cur}} B_j^{\mathrm{hist}} B_j^{\mathrm{indx}}} \circ \widehat{Q}_{B_j^{\mathrm{cur}}|Z^k X_{<j}^k} \widehat{Q}_{B_j^{\mathrm{indx}}|I,Z^k X_{<j}^k} \widehat{Q}_{B_j^{\mathrm{hist}}|Z^k X_{<j}^k}$ *for* $j \in [m+1]$, *where*

   (a) $\widehat{Q}_{B_j^{\mathrm{cur}}|Z^k X_{<j}^k} = \widehat{P}_{B_j^{\mathrm{cur}}|Z^k X_{\leq j}^k} \circ \widehat{P}_{X_j^k|Z^k X_{<j}^k}$

   (b) $\widehat{Q}_{B_j^{\mathrm{hist}}|Z^k X_{<j}^k} = \widehat{P}_{B_j^{\mathrm{hist}}|Z^k X_{<j}^k}$

   (c) $\widehat{Q}_{B_j^{\mathrm{indx}}|I,Z^k X_{<j}^k} = \mathbb{1}\{I \in \mathcal{G}_{Z^k X_{<j}^k}\}$.

A few words about these definitions are in order. Note that the bits B_j^{cur} and B_j^{hist} are related to the distribution P, while the bit B_j^{indx} is related to the distribution Q. We define all bits in both experiments so that the distribution of B_j will be identical under both extensions. The bit B_j^{hist} meant to guarantee that $\mathcal{G}_\tau$ is of size $\Omega(k)$ and that the probability that $|\Delta| \leq 1/2$ is high. This bit depends only on the transcript so far (i.e., the "history"), and in particular is independent of round j. On the other hand, the bit B_j^{cur} does depend on round j (i.e., the "current" round) and we will see ahead that conditioning on $B_j^{\mathrm{cur}} = 1$ means that indeed $|\Delta| \leq 1/2$ (not just with high probability). Finally, the bit B_j^{indx} meant to guarantee that the index I chosen by Q belongs to $\mathcal{G}_\tau$.

We summarize the properties of the two extensions in the next claim.

Claim 5.10. *It holds that*

1. ***Round zero:***

   (a) $\widehat{P}_{Z^k X_1^k|B_0=1} = P_{Z^k X_1^k||\delta_0(Z^k X_1^k)|\leq 1/2}$.

   (b) $\widehat{Q}_{Z^k X_1^k|B_0=1} = P_{Z^k X_1^k|I,Z_I,X_{1,I}=1} \circ Q_{IZ_I|IZ_I \in \mathcal{D}}$.

   (c) $\widehat{P}_{B_0} = \widehat{Q}_{B_0}$.

2. ***Round*** $1 \leq j \leq m+1$***:***

   (a) $\widehat{P}_{X_j^k|Z^k X_{<j}^k, B_0 B_{\leq j} = 1^{j+1}} = P_{X_j^k|Z^k X_{<j}^k X_{j+1}^k} \circ P_{X_{j+1}^k|Z^k X_{<j}^k, \left|\delta_j(X_{j+1}^k; Z^k X_{<j}^k)\right| \leq 1/2}$.

   (b) $\widehat{Q}_{X_j^k|Z^k X_{<j}^k, B_0 B_{\leq j} = 1^{j+1}} = P_{X_j^k|Z^k X_{<j}^k X_{j+1}^k} \circ Q'_{X_{j+1}^k|Z^k X_{<j}^k}$ *for*

$$Q'_{X_{j+1}^k|Z^k X_{<j}^k} = P_{X_{j+1}|Z^k X_{<j}^k, X_{j+1,I}=1} \circ Q_{I|Z^k X_{<j}^k, I \in \mathcal{G}_{Z^k X_{<j}^k}},$$

(c) For every $z^k x^k_{<j} \in \operatorname{Supp}(\widehat{P}_{Z^k X^k_{<j}|(B_0 B_{<j})=1^j})$ *it holds that*

$$\widehat{P}_{B_j|(Z^k X^k_{<j})=(z^k x^k_{<j}),(B_0 B_{<j})=1^j} = \widehat{Q}_{B_j|(Z^k X^k_{<j})=(z^k x^k_{<j}),(B_0 B_{<j})=1^j}.$$

Proof. We prove the statement for a fixed $1 \leq j \leq m+1$. The proof for round zero follows from similar arguments.

The proofs of Items 2a to 2c follow merely from the definitions. However, the abundant of random variables might make it difficult to verify the correctness of the statements, so we explicitly prove them.

Proving (2a): First, observe that conditioned on $Z^k X^k_{<j}$, it holds that X^k_j is independent of $B_0, B_1, \ldots, B_{j-1}, B^{\text{hist}}_j, B^{\text{indx}}_j$ under $\widehat{P}$. Namely,

$$\widehat{P}_{X^k_j|Z^k X^k_{<j}, B_0 B_{\leq j}=1^{j+1}} = \widehat{P}_{X^k_j|Z^k X^k_{<j}, B^{\text{cur}}_j=1}.$$

Now, applying Claim 3.1 with the random variables $X = X^k_j|Z^k X^k_{<j}$, $Y = X^k_{j+1}|Z^k X^k_{<j}$ and $f(X^k_{j+1}; Z^k X^k_{<j}) = \mathbb{1}\{|\delta_j(X^k_{j+1}; Z^k X^k_{<j}) \leq 1/2\}$, all under $\widehat{P}$, yields that

$$\begin{aligned}\widehat{P}_{X^k_j|Z^k X^k_{<j}, B^{\text{cur}}_j=1} &= \widehat{P}_{X^k_j|Z^k X^k_{<j} X^k_{j+1}} \circ \widehat{P}_{X^k_{j+1}|Z^k X^k_{<j}, |\delta(X^k_{j+1}; Z^k X^k_{<j})| \leq 1/2} \\ &= P_{X^k_j|Z^k X^k_{<j} X^k_{j+1}} \circ P_{X^k_{j+1}|Z^k X^k_{<j}, |\delta_j(X^k_{j+1}; Z^k X^k_{<j})| \leq 1/2},\end{aligned}$$

where the second equality follows from the definition of $\widehat{P}$.

Proving (2b): First, observe that conditioned on $Z^k X^k_{<j}$, it holds that X^k_j is independent of $B^{\text{hist}}_0, B^{\text{cur}}_0, \ldots, B^{\text{hist}}_j, B^{\text{cur}}_j$ under $\widehat{Q}$. If we condition on I as well, then X^k_j is also independent of $B^{\text{indx}}_0, \ldots, B^{\text{indx}}_j$. Thus,

$$\begin{aligned}\widehat{Q}_{X^k_j|Z^k X^k_{<j}, B_0 B_{\leq j}=1^{j+1}} &= \widehat{Q}_{X^k_j|Z^k X^k_{<j}, (B^{\text{indx}}_0 B^{\text{indx}}_{\leq j})=1^{j+1}} \\ &= \widehat{Q}_{X^k_j|I Z^k X^k_{<j}, (B^{\text{indx}}_0 B^{\text{indx}}_{\leq j})=1^{j+1}} \circ \widehat{Q}_{I|Z^k X^k_{<j}, (B^{\text{indx}}_0 B^{\text{indx}}_{\leq j})=1^{j+1}} \\ &= \widehat{Q}_{X^k_j|I Z^k X^k_{<j}} \circ \widehat{Q}_{I|Z^k X^k_{<j}, (B^{\text{indx}}_0 B^{\text{indx}}_{\leq j})=1^{j+1}}.\end{aligned}$$

By definition, it holds that $\mathcal{G}_{Z^k X^k_{<j}} \subseteq \mathcal{G}_{Z^k X^k_{<j'}}$ for every $j' < j$. Hence, it holds that

$$\begin{aligned}\widehat{Q}_{I|Z^k X^k_{<j}, (B^{\text{indx}}_0 B^{\text{indx}}_{\leq j})=1^{j+1}} &= \widehat{Q}_{I|Z^k X^k_{<j}, B^{\text{indx}}_j=1} \\ &= Q_{I|Z^k X^k_{<j}, I \in \mathcal{G}_{Z^k X^k_{<j}}}.\end{aligned}$$

Furthermore, the definition of Q yields that for $i \in \mathcal{G}_{Z^k X^k_{<j}}$, it holds that

$$\begin{aligned}\widehat{Q}_{X^k_j|(I Z^k X^k_{<j})=(i z^k x^k_{<j})} &= Q_{X^k_j|I Z^k X^k_{<j}=(i z^k x^k_{<j})} \\ &= P_{X^k_j|(Z^k X^k_{<j})=(z^k x^k_{<j}), X_{j+1,i}=1} \\ &= P_{X^k_j|(Z^k X^k_{<j})=(z^k x^k_{<j}), X^k_j} \circ P_{X^k_{j+1}|(Z^k X^k_{<j})=(z^k x^k_{<j}), X_{j+1,i}=1}.\end{aligned}$$

In particular, note the above equality holds also for $j = m+1$. Indeed, if $I \in \mathcal{G}_{Z^k X^k_{\leq m}}$, then $P_{X_{m+2,i}|Z^k X^k_{\leq m}}(1|z^k x^k_{\leq m}) > 0$, and thus also $R[W|(Z^k X^k_{\leq m}) = (z^k x^k_{\leq m}), X_{m+2,i} = 1]$. Combining the above three equations completes the proof of the second statement.

Proving (2c): That $\widehat{P}_{B_j^{\text{hist}}|Z^kX^k_{<j}B_0B_{<j}} = \widehat{Q}_{B_j^{\text{hist}}|Z^kX^k_{<j}B_0B_{<j}}$ and $\widehat{P}_{B_j^{\text{cur}}|Z^kX^k_{<j}B_0B_{<j}} = \widehat{Q}_{B_j^{\text{cur}}|Z^kX^k_{<j}B_0B_{<j}}$ follows immediately from definition. For B_j^{indx}, the same arguments we used in the proof of the previous item yield that

$$\begin{aligned}
\widehat{Q}_{B_j^{\text{indx}}|Z^kX^k_{<j},(B_0B_{<j})=1^j} &= \widehat{Q}_{B_j^{\text{indx}}|Z^kX^k_{<j},(B_0^{\text{indx}}B_{<j}^{\text{indx}})=1^j}\\
&= \mathbb{1}\{I \in \mathcal{G}_{Z^kX^k_{<j}}\} \circ \widehat{Q}_{I|Z^kX^k_{<j},(B_0^{\text{indx}}B_{<j}^{\text{indx}})=1^j}\\
&= \mathbb{1}\{I \in \mathcal{G}_{Z^kX^k_{<j}}\} \circ Q_{I|Z^kX^k_{<j},I\in\mathcal{G}_{Z^kX^k_{<j}}}\\
&= \widehat{P}_{B_j^{\text{indx}}|Z^kX^k_{<j}}\\
&= \widehat{P}_{B_j^{\text{indx}}|Z^kX^k_{<j},(B_0B_{<j})=1^j}.
\end{aligned}$$

□

5.4 Proving Lemma 5.3

The proof of Lemma 5.3 is divided into two parts. In the first part we prove that conditioned on all the extensions bits being equal to 1, the divergence between $\widehat{P}$ and $\widehat{Q}$ is sufficiently small. In the second part we show that the probability that the extensions bits are all 1 in $\widehat{P}$ is high.

To enforce the conditioning on all bits equal 1, we use the following function.

Definition 5.11 (f_{cut})**.** *Let $f_{cut}\colon \{0,1\}^{\ell k+(m+1)k+(m+2)} \to \{0,1,\perp\}^{\ell k+(m+1)k+(m+2)}$ to be the function that cuts its input $(b_0z^k, b_1x_1^k, \ldots, b_{m+1}x_{m+1}^k) \in \{0,1\}^{\ell k+(m+1)k+(m+2)}$ after the first bit b_j that equals to 0. Formally*

1. *If $(b_0, b_1, \ldots, b_m, b_{m+1}) = 1^{m+2}$, then $f_{cut}(b_0z^k, b_1x_1^k, \ldots, b_{m+1}x_{m+1}^k) = (b_0z^k, b_1x_1^k, \ldots, b_{m+1}x_{m+1}^k)$.*
2. *Else, let $j \in \{0, \ldots, m+1\}$ be the first index with $b_j = 0$. Then*
   (a) *If $j = 0$, $f_{cut}(b_0z^k, b_1x_1^k, \ldots, b_{m+1}x_{m+1}^k) = (b_0, \perp^{\ell k+(m+1)k+m+1})$.*
   (b) *Else, $f_{cut}(b_0z^k, b_1x_1^k, \ldots, b_{m+1}x_{m+1}^k) = (b_0z^k, b_1x_1^k, \ldots, b_{j-1}x_{j-1}^k, b_j, \perp^{(m-j+2)k+(m-j+1)}$).*

The following two lemmata prove the two aforementioned parts and are the main technical part of our work. Lemma 5.12 is proven in Section 6 and Lemma 5.13 is proven in Section 7.

Lemma 5.12. *There exists two universal constants $\lambda, \lambda' > 0$ such that the following holds: Let $k, m, \ell \in \mathbb{N}$, let $\mathcal{W} \subseteq \{0,1\}^{kl+k(m+1)}$ be a termination-consistent set (according to Definition 4.3) and let W, R, $\widehat{P}$ and $\widehat{Q}$ be the event and distributions from Definitions 5.1, 5.8 and 5.9, respectively, and let f_{cut} be the function from Definition 5.11. Assume that $\widehat{P}_{B^{m+2}}(1^{m+2}) \geq 1/2$ and that $k \geq \lambda \cdot m$, then*

$$D\Big(f_{cut}(\widehat{P}_{B_0Z^k,B_1X_1^k,\ldots,B_{m+1}X_{m+1}^k})||f_{cut}(\widehat{Q}_{B_0Z^k,B_1X_1^k,\ldots,B_{m+1}X_{m+1}^k})\Big) \leq \frac{\lambda' m}{k} \cdot \Big(\log \frac{1}{R[W]} + m\Big).$$

Lemma 5.13. *For any constant $\lambda > 0$ there exist constants $\lambda', \lambda'' > 0$ such that the following holds: Let $k, m, \ell \in \mathbb{N}$, let $\varepsilon \in (0, 1/2]$, let $\mathcal{W} \subseteq \{0,1\}^{kl+k(m+1)}$ be a termination-consistent set (according to Definition 4.3) and let W, R and $\widehat{P}$ be the event and distributions from Definitions 5.1 and 5.8 respectively, for the above $k, m, \ell, \mathcal{W}$. Assume $k \geq \lambda' \cdot m^2/\varepsilon$ and $R[W] \geq (1-\varepsilon)^{\frac{k}{\lambda'' \cdot m}}$, then $\widehat{P}_{B^{m+2}}(1^{m+2}) \geq 1 - \varepsilon/\lambda$.*

Using the above lemmata, we are ready to prove Lemma 5.3.

Proof of Lemma 5.3. Let $\widehat{P}_{B_0 Z^k, B_1 X_1^k, \ldots, B_{m+1} X_{m+1}^k}$ and $\widehat{Q}_{B_0 Z^k, B_1 X_1^k, \ldots, B_{m+1} X_{m+1}^k}$ be the distributions from Definitions 5.8 and 5.9, respectively, let f_{cut} be the function from Definition 5.11 and let $\lambda = \max\{c_1, c_1', c_2, c_2'\}$, where c_1, c_1' are the constants λ, λ' from Lemma 5.12 and c_2, c_2' are the constants $\lambda'(24), \lambda''(24)$ from Lemma 5.13 (with respect to $\lambda = 24$). First, observe that by Lemma 5.13 it holds that

$$\widehat{P}_{B^{m+2}}(1^{m+2}) = \Pr_{y \sim \widehat{P}_{B_0 Z^k, B_1 X_1^k, \ldots, B_{m+1} X_{m+1}^k}}[f_{cut}(y) = y] \geq 1 - \varepsilon/24 \tag{51}$$

and along with Lemma 5.12 we obtain that

$$D^{\frac{\varepsilon}{24}}(\widehat{P}_{B_0 Z^k, B_1 X_1^k, \ldots, B_{m+1} X_{m+1}^k} || \widehat{Q}_{B_0 Z^k, B_1 X_1^k, \ldots, B_{m+1} X_{m+1}^k}) \leq \frac{\lambda m}{k} \cdot \left(\log \frac{1}{R[W]} + m\right) \tag{52}$$

Second, observe that by the definition of $\widehat{Q}$, it holds that $\forall z^k x^{(m+1)\times k} \in \{0,1\}^{k\ell + k(m+1)}$ and $\forall i \in \mathrm{Supp}(\widehat{Q}_{I|Z^k X^{(m+1)\times k}, B^{m+2} = 1^{m+2}})$,

$$P_{Z_i|X_{1,i}=1}(z_i) \geq (1-0.1) \cdot 2^{-\ell} \text{ and } P_{X_{1,i}}(1) \geq \frac{1-0.1}{m}$$

$$\begin{aligned} \implies R[W|Z_i = z_i, X_{1,i} = 1] &= R[W] \cdot \frac{P_{X_{1,i}}(1) \cdot P_{Z_i|X_{1,i}=1}(z_i)}{R_{X_{1,i}}(1) \cdot R_{Z_i|X_{1,i}=1}(z_i)} \\ &\geq R[W] \cdot (1-0.1)^2 \\ &\geq R[W]/2 \end{aligned} \tag{53}$$

and

$$\forall j \in [m+1]: \;\; P_{X_{j+1,i}|(Z^k X^k_{<j}) = z^k x^k_{<j}}(1) \geq \frac{1-0.1}{m}(1 - \frac{1}{m}).$$

$$\begin{aligned} \implies \forall j \in [m+1]: \;\; & R[W|(Z^k X^k_{<j}) = z^k x^k_{<j}, X_{j+1,i} = 1] \\ &= R[W|(Z^k X^k_{<j}) = z^k x^k_{<j}] \cdot \frac{P_{X_{j+1,i}|(Z^k X^k_{<j}) = z^k x^k_{<j}}(1)}{R_{X_{j+1,i}|(Z^k X^k_{<j}) = z^k x^k_{<j}}(1)} \\ &\geq R[W|(Z^k X^k_{<j}) = z^k x^k_{<j}] \cdot (1-0.1) \\ &\geq R[W|(Z^k X^k_{<j}) = z^k x^k_{<j}]/2 \end{aligned} \tag{54}$$

The proof then follows by Equations (51) to (54). □

6 Bounding the Smooth KL-Divergence of $\widehat{P}$ and $\widehat{Q}$

In this section, we prove Lemma 5.12. That is, we prove that there exist two universal constants $\lambda, \lambda' > 0$ such that if $k \geq \lambda \cdot m$ then

$$D(f_{cut}(\widehat{P}_{B_0Z^k,B_1X_1^k,\dots,B_{m+1}X_{m+1}^k})||f_{cut}(\widehat{Q}_{B_0Z^k,B_1X_1^k,\dots,B_{m+1}X_{m+1}^k})) \leq \lambda' \cdot \frac{m}{k} \cdot \left(\log\frac{1}{R[W]} + m\right). \tag{55}$$

Let $k, m, \ell \in \mathbb{N}$ with $m \geq 2$ and $k \geq \lambda \cdot m$ for $\lambda \geq 1$ to be determined by the analysis. Let

$$P^{cut}_{B_0Z^k,B_1X_1^k,\dots,B_{m+1}X_{m+1}^k} = f_{cut}(\widehat{P}_{B_0Z^k,B_1X_1^k,\dots,B_{m+1}X_{m+1}^k}),$$

and let Q^{cut} be analogously defined with $\widehat{Q}$. Our first step is to apply the chain rule for divergence (Fact 3.5(3)):

$$\begin{aligned}
&D(f_{cut}(\widehat{P}_{B_0Z^k,B_1X_1^k,\dots,B_{m+1}X_{m+1}^k})||f_{cut}(\widehat{Q}_{B_0Z^k,B_1X_1^k,\dots,B_{m+1}X_{m+1}^k})) \\
&= D(P^{cut}_{B_0Z^k,B_1X_1^k,\dots,B_{m+1}X_{m+1}^k}||Q^{cut}_{B_0Z^k,B_1X_1^k,\dots,B_{m+1}X_{m+1}^k}) \\
&= D(P^{cut}_{B_0Z^k}||Q^{cut}_{B_0Z^k}) + \sum_{j=1}^{m+1} D(P^{cut}_{B_jX_j^k|B_0Z^kB_{<j}X_{<j}^k}||Q^{cut}_{B_jX_j^k|B_0Z^kB_{<j}X_{<j}^k}|P^{cut}_{B_0Z^kB_{<j}X_{<j}^k}).
\end{aligned} \tag{56}$$

The proof now follows from the next two claims.

Claim 6.1 (Round zero)**.** *There exists a universal constant $C_0 > 0$ such that*

$$D(P^{cut}_{B_0Z^k}||Q^{cut}_{B_0Z^k}) \leq C_0 \cdot \frac{m}{k} \cdot \Big(D(P_{Z^kX_1^k}||R_{Z^kX_1^k}) + 1\Big).$$

Claim 6.2 (Rounds 1 to $m+1$)**.** *There exists a universal constant $C_0 > 0$ such that*

$$\begin{aligned}
&D(P^{cut}_{B_jX_j^k|B_0Z^kB_{<j}X_{<j}^k}||Q^{cut}_{B_jX_j^k|B_0Z^kB_{<j}X_{<j}^k}|P^{cut}_{B_0Z^kB_{<j}X_{<j}^k}) \\
&\leq C \cdot \frac{m}{k} \cdot \Big(D(P_{X_{j+1}^k|Z^kX_{<j}^k}||R_{X_{j+1}^k|Z^kX_{<j}^k}|P_{Z^kX_{<j}^k}) + 1\Big).
\end{aligned}$$

We prove Claims 6.1 and 6.2 below, but first we use them to derive Equation (55). Since conditioning increases divergence (Fact 3.5(4)), it holds that

$$D(P_{X_{j+1}^k|Z^kX_{<j}^k}||R_{X_{j+1}^k|Z^kX_{<j}^k}|P_{Z^kX_{<j}^k}) \leq D(P_{X_{j+1}^k|Z^kX_{\leq j}^k}||R_{X_{j+1}^k|Z^kX_{\leq j}^k}|P_{Z^kX_{\leq j}^k}).$$

(We added a conditioning on X_j^k as well.) Plugging Claims 6.1 and 6.2 into Equation (56) and setting $\lambda' = C_0 + 2C$ yields that

$$
\begin{aligned}
&D(f_{cut}(\widehat{P}_{B_0 Z^k, B_1 X^k_1, \ldots, B_{m+1} X^k_{m+1}}) || f_{cut}(\widehat{Q}_{B_0 Z^k, B_1 X^k_1, \ldots, B_{m+1} X^k_{m+1}}))\\
&\le C_0 \cdot \frac{m}{k} \cdot \Big(D(P_{Z^k X^k_1} || R_{Z^k X^k_1}) + 1 \Big) + \sum_{j=1}^{m+1} C \cdot \frac{m}{k} \cdot \Big(D(P_{X^k_{j+1} | Z^k X^k_{\le j}} || R_{X^k_{j+1} | Z^k X^k_{\le j}} | P_{Z^k X^k_{\le j}}) + 1 \Big)\\
&\le \lambda' \cdot \frac{m}{k} \cdot \left(D(P_{Z^k X^k_1} || R_{Z^k X^k_1}) + \sum_{j=1}^{m+1} D(P_{X^k_{j+1} | Z^k X^k_{\le j}} || R_{X^k_{j+1} | Z^k X^k_{\le j}} | P_{Z^k X^k_{\le j}}) + m \right)\\
&= \lambda' \cdot \frac{m}{k} \cdot (D(P_{Z^k X^{(m+2)\times k}} || R_{Z^k X^{(m+2)\times k}}) + m)\\
&\le \lambda' \cdot \frac{m}{k} \cdot \left(\log \frac{1}{R[W]} + m \right),
\end{aligned}
$$

where the equality follows from another application of the chain rule for divergence (Fact 3.5(3)), and the last inequality follows from Fact 3.6. This completes the proof of Lemma 5.12.

The rest of this section is dedicated to proving Claims 6.1 and 6.2. The proofs of both claims share similar structure and insights. Since it is conceptually (slightly) easier, we begin with proving Claim 6.2, which we do in Section 6.1. In Section 6.2 we prove Claim 6.1.

6.1 Round 1 to $m+1$, Proving Claim 6.2

Fix a round $j \in [m+1]$. Our goal in this section is to prove Claim 6.2. Thats is, to show that there exists $C > 0$ such that

$$
\begin{aligned}
&D(P^{cut}_{B_j X^k_j | B_0 Z^k B_{<j} X^k_{<j}} || Q^{cut}_{B_j X^k_j | B_0 Z^k B_{<j} X^k_{<j}} | P^{cut}_{B_0 Z^k B_{<j} X^k_{<j}})\\
&\le C \cdot \frac{m}{k} \cdot \Big(D(P_{X^k_{j+1} | Z^k X^k_{<j}} || R_{X^k_{j+1} | Z^k X^k_{<j}} | P_{Z^k X^k_{<j}}) + 1 \Big).
\end{aligned} \tag{57}
$$

As a first step we apply the chain rule for divergence (Fact 3.5(3)) to get that

$$
\begin{aligned}
&D(P^{cut}_{B_j X^k_j | B_0 Z^k B_{<j} X^k_{<j}} || Q^{cut}_{B_j X^k_j | B_0 Z^k B_{<j} X^k_{<j}} | P^{cut}_{B_0 Z^k B_{<j} X^k_{<j}})\\
&= D(P^{cut}_{B_j | B_0 Z^k B_{<j} X^k_{<j}} || Q^{cut}_{B_j | B_0 Z^k B_{<j} X^k_{<j}} | P^{cut}_{B_0 Z^k B_{<j} X^k_{<j}})\\
&\quad + D(P^{cut}_{X^k_j | Z^k X^k_{<j} B_0 B_{\le j}} || Q^{cut}_{X^k_j | Z^k X^k_{<j} B_0 B_{\le j}} | P^{cut}_{Z^k X^k_{<j} B_0 B_{\le j}})\\
&= D(P^{cut}_{X^k_j | Z^k X^k_{<j} B_0 B_{\le j}} || Q^{cut}_{X^k_j | Z^k X^k_{<j} B_0 B_{\le j}} | P^{cut}_{Z^k X^k_{<j} B_0 B_{\le j}}),
\end{aligned}
$$

where the second equality follows since $P^{cut}_{B_j | B_0 Z^k B_{<j} X^k_{<j}} = Q^{cut}_{B_j | B_0 Z^k B_{<j} X^k_{<j}}$ (follows from Claim 5.10(2c) that shows that $\widehat{P}_{B_j | (Z^k X^k_{<j}) = (z^k x^k_{<j}), (B_0 B_{<j}) = 1^j} = \widehat{Q}_{B_j | (Z^k X^k_{<j}) = (z^k x^k_{<j}), (B_0 B_{<j}) = 1^j}$ and since, by definition, $B_j = \perp$ under both P^{cut} and Q^{cut} if $B_{j'} = 0$ for some $j' < j$). Moreover, again by definition, if $B_{j'} = 0$ for some $j \le j$, then $X^k_j = \perp$ under both P^{cut} and Q^{cut}. The definition of conditional divergence now yields that

$$
\begin{aligned}
&D(P^{cut}_{X^k_j | Z^k X^k_{<j} B_0 B_{\le j}} || Q^{cut}_{X^k_j | Z^k X^k_{<j} B_0 B_{\le j}} | P^{cut}_{Z^k X^k_{<j} B_0 B_{\le j}})\\
&\le D(P^{cut}_{X^k_j | Z^k X^k_{<j}, B_0 B_{\le j} = 1^{j+1}} || Q^{cut}_{X^k_j | Z^k X^k_{<j}, B_0 B_{\le j} = 1^{j+1}} | P^{cut}_{Z^k X^k_{<j} | B_0 B_{\le j} = 1^{j+1}})\\
&= D(\widehat{P}_{X^k_j | Z^k X^k_{<j}, B_0 B_{\le j} = 1^{j+1}} || \widehat{Q}_{X^k_j | Z^k X^k_{<j}, B_0 B_{\le j} = 1^{j+1}} | \widehat{P}_{Z^k X^k_{<j} | B_0 B_{\le j} = 1^{j+1}}),
\end{aligned} \tag{58}
$$

where the last equality follows the definition of f_{cut}.

In the rest of this section we bound the right-hand side term in Equation (58). Using Claim 5.10 and the data-processing inequality for divergence (Fact 3.5(5)), it holds that

$$\begin{aligned}
&D(\widehat{P}_{X_j^k|Z^kX_{<j}^k,B_0B_{\le j}=1^{j+1}}||\widehat{Q}_{X_j^k|Z^kX_{<j}^k,B_0B_{\le j}=1^{j+1}}|\widehat{P}_{Z^kX_{<j}^k|B_0B_{\le j}=1^{j+1}})\\
&\le D(P_{X_{j+1}^k|Z^kX_{<j}^k,|\delta_j(X_{j+1}^k;Z^kX_{<j}^k)|\le 1/2}||Q'_{X_{j+1}^k|Z^kX_{<j}^k}|\widehat{P}_{Z^kX_{<j}^k|B_0B_{\le j}=1^{j+1}}),
\end{aligned}$$

for $Q'_{X_{j+1}^k|Z^kX_{<j}^k} = P_{X_{j+1}|Z^kX_{<j}^k,X_{j+1,I}=1} \circ Q_{I|Z^kX_{<j}^k,I\in\mathcal{G}_{Z^kX_{<j}^k}}$.

The proof of Claim 6.2 immediately follows from the next claim.

Claim 6.3. *There exists a universal constant $C > 0$ such that*

$$\begin{aligned}
&D(P_{X_{j+1}^k|Z^kX_{<j}^k,|\delta_j(X_{j+1}^k;Z^kX_{<j}^k)|\le 1/2}||Q'_{X_{j+1}^k|Z^kX_{<j}^k}|\widehat{P}_{Z^kX_{<j}^k|B_0B_{\le j}=1^{j+1}})\\
&\le C\cdot\frac{m}{k}\cdot\Big(D(P_{X_{j+1}^k|Z^kX_{<j}^k}||R_{X_{j+1}^k|Z^kX_{<j}^k}|P_{Z^kX_{<j}^k})+1\Big).
\end{aligned}$$

Proof. Fix $\tau = (z^k, x_{<j}^k) \in \mathrm{Supp}(\widehat{P}_{Z^kX_{<j}^k|B_0B_{\le j}=1^{j+1}})$. Our first step is to observe that since τ is fixed such that $B_0B_{\le j} = 1^{j+1}$, the additional conditioning on $|\delta_j(X_{j+1}^k;Z^kX_{<j}^k)| \le 1/2$ does not change the distribution of X_{j+1}^k under P by much. In particular, the definition of $\widehat{P}$ (Definition 5.8) yields that

$$\begin{aligned}
P_{X_{j+1}^k|(Z^kX_{<j}^k)=\tau}[|\delta_j(X_{j+1}^k;\tau)| \le 1/2] &= \mathrm{E}_{P_{X_j^k|(Z^kX_{<j}^k)=\tau}}\left[P_{X_{j+1}^k|(Z^kX_{<j}^k)=\tau,X_j^k}[|\delta_j(X_{j+1}^k;\tau)| \le 1/2]\right] \qquad (59)\\
&= \mathrm{E}_{P_{X_j^k|(Z^kX_{<j}^k)=\tau}}[\widehat{P}_{B_j^{\mathrm{cur}}|Z^kX_{\le j}^k}(1)]\\
&\ge 1-\frac{m}{k^2},
\end{aligned}$$

where the last inequality holds since $B_j^{\mathrm{hist}} = 1$. To ease the notation, let $P_{X_{j+1}^k|\tau,|\delta|\le 1/2} = P_{X_{j+1}^k|(Z^kX_{<j}^k)=\tau,|\delta_j(X_{j+1}^k;Z^kX_{<j}^k)|\le 1/2}$. It follows that

$$\begin{aligned}
&D(P_{X_{j+1}^k|\tau,|\delta|\le 1/2}||Q'_{X_{j+1}^k|(Z^kX_{<j}^k)=\tau}) \qquad (60)\\
&= \mathop{\mathrm{E}}_{x_{j+1}^k\sim P_{X_{j+1}^k|\tau,|\delta|\le 1/2}} \log\frac{P_{X_{j+1}^k|\tau,|\delta|\le 1/2}(x_{j+1}^k)}{Q'_{X_{j+1}^k|Z^kX_{<j}^k}(x_{j+1}^k|\tau)}\\
&= \mathop{\mathrm{E}}_{x_{j+1}^k\sim P_{X_{j+1}^k|\tau,|\delta|\le 1/2}} \log\frac{P_{X_{j+1}^k|Z^kX_{<j}^k}(x_{j+1}^k|\tau)/P_{X_{j+1}^k|Z^kX_{<j}^k}[|\delta_j(X_{j+1}^k;\tau)| \le 1/2|Z^kX_{<j}^k=\tau]}{Q'_{X_{j+1}^k|Z^kX_{<j}^k}(x_{j+1}^k|\tau)}\\
&= \log\frac{1}{P_{X_{j+1}^k|Z^kX_{<j}^k}[|\delta_j(X_{j+1}^k;\tau)| \le 1/2|Z^kX_{<j}^k=\tau]} + \mathop{\mathrm{E}}_{x_{j+1}^k\sim P_{X_{j+1}^k|\tau,|\delta|\le 1/2}} \log\frac{P_{X_{j+1}^k|Z^kX_{<j}^k}(x_{j+1}^k|\tau)}{Q'_{X_{j+1}^k|Z^kX_{<j}^k}(x_{j+1}^k|\tau)}\\
&\le \frac{2m}{k^2} + \mathop{\mathrm{E}}_{x_{j+1}^k\sim P_{X_{j+1}^k|\tau,|\delta|\le 1/2}} \log\frac{P_{X_{j+1}^k|Z^kX_{<j}^k}(x_{j+1}^k|\tau)}{Q'_{X_{j+1}^k|Z^kX_{<j}^k}(x_{j+1}^k|\tau)}\\
&\le \frac{m}{k} + \mathop{\mathrm{E}}_{x_{j+1}^k\sim P_{X_{j+1}^k|\tau,|\delta|\le 1/2}} \log\frac{\sum_{i\in\mathcal{G}_\tau}\alpha_{j,i}(\tau)}{\sum_{i\in 1_{x_{j+1}^k}\cap\mathcal{G}_\tau}\frac{\alpha_{j,i}(\tau)}{p_i(\tau)}},
\end{aligned}$$

where the first inequality follows from Equation (59) and since $\frac{1}{1-x} \leq e^{2x}$ for all $0 < x \leq 0.5$, and the last equality follows since $k \geq m \geq 2$ and from applying Claim 5.5 with $\mathcal{J} = \mathcal{G}_\tau$ (recall that we defined in Claim 5.5 that $p_i(\tau) = P_{X_{j+1,i}|Z^k X^k_{<j}}(1|\tau)$).

Our next step is to use the following claim — proved below — which is where the crux of the argument lies.

Claim 6.4. *There exists a constant $C' > 0$ such that*

$$\mathrm{E}_{x^k_{j+1} \sim P_{X^k_{j+1}|\tau,|\delta| \leq 1/2}} \log \frac{\sum_{i \in \mathcal{G}_\tau} \alpha_{j,i}(\tau)}{\sum_{i \in 1_{x^k_{j+1}} \cap \mathcal{G}_\tau} \frac{\alpha_{j,i}(\tau)}{p_i(\tau)}} \leq C' \cdot \frac{m}{k} \cdot \Big(D(P_{X^k_{j+1}|(Z^k X^k_{<j})=\tau} || R_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}) + 1 \Big). \tag{61}$$

We now proceed to complete the proof of Claim 6.3. Note that Claim 6.4 does not immediately suffice in order to establish Claim 6.3. The reason is that in order to get $D(P_{X^k_{j+1}|Z^k X^k_{<j}, \delta_j(X^k_{j+1};Z^k X^k_{<j}) \leq 1/2} || Q'_{X^k_{j+1}|Z^k X^k_{<j}} | \widehat{P}_{Z^k X^k_{<j}|B_0 B_{\leq j} = 1^{j+1}})$ from the left-hand side of Equation (60) we need to take expectation over $\widehat{P}_{Z^k X^k_{<j}|B_0 B_{\leq j} = 1^{j+1}}$. However, to get $D(P_{X^k_{j+1}|Z^k X^k_{<j}} || R_{X^k_{j+1}|Z^k X^k_{<j}} | P_{Z^k X^k_{<j}})$ from the right-hand side of Equation (61), we need to take expectation over $P_{Z^k X^k_{<j}}$. We use Fact 3.7 to handle this issue.

Set $C = 2C' + 1$. Equation (60) and Claim 6.4 yield that

$$\begin{aligned}
&D(P_{X^k_{j+1}|Z^k X^k_{<j}, \delta_j(X^k_{j+1};Z^k X^k_{<j}) \leq 1/2} || Q'_{X^k_{j+1}|Z^k X^k_{<j}} | \widehat{P}_{Z^k X^k_{<j}|B_0 B_{\leq j} = 1^{j+1}}) \\
&= \mathrm{E}_{\tau \sim \widehat{P}_{Z^k X^k_{<j}|B_0 B_{\leq j} = 1^{j+1}}} D(P_{X^k_{j+1}|(Z^k X^k_{<j})=\tau, \delta_j(X^k_{j+1};Z^k X^k_{<j}) \leq 1/2} || Q'_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}) \\
&\leq \mathrm{E}_{\tau \sim \widehat{P}_{Z^k X^k_{<j}|B_0 B_{\leq j} = 1^{j+1}}} \left[\frac{m}{k} + C' \cdot \frac{m}{k} \cdot \Big(D(P_{X^k_{j+1}|(Z^k X^k_{<j})=\tau} || R_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}) + 1 \Big) \right] \\
&\leq \frac{m}{k} + C' \cdot \frac{m}{k} \cdot \left(\frac{1}{\widehat{P}_{B_0 B_{\leq j}}(1^{j+1})} \cdot D(P_{X^k_{j+1}|Z^k X^k_{<j}} || R_{X^k_{j+1}|Z^k X^k_{<j}} | P_{Z^k X^k_{<j}}) + 1 \right) \\
&\leq C \cdot \frac{m}{k} \cdot \Big(D(P_{X^k_{j+1}|Z^k X^k_{<j}} || R_{X^k_{j+1}|Z^k X^k_{<j}} | P_{Z^k X^k_{<j}}) + 1 \Big),
\end{aligned}$$

where the second inequality follows from Fact 3.7 and since $\widehat{P}_{Z^k X^{m \times k}} = P_{Z^k X^{m \times k}}$, and the last inequality follows since by assumption $\widehat{P}_{B_0 B_{\leq j}}(1^{j+1}) \geq 1/2$ and by the setting of C. This completes the proof of Claim 6.3. □

Proof of Claim 6.4. First, we lower-bound the right-hand side of Equation (61). Note that by Definition 5.1, $X_{j+1,i}$ and $X_{j+1,i'}$ are independent for $i \neq i'$; that is, $R_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}$ can be written as a product distribution $R_{X^k_{j+1}|(Z^k X^k_{<j})=\tau} = \prod_{i=1}^k R_{X_{j+1,i}|(Z^k X^k_{<j})=\tau}$. Thus, by chain rule of divergence (Fact 3.5(3)) it holds that

$$D(P_{X^k_{j+1}|(Z^k X^k_{<j})=\tau} || R_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}) \geq D(P_{X^k_{j+1}|(Z^k X^k_{<j})=\tau} || P^{\Pi}_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}), \tag{62}$$

where $P^{\Pi}_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}$ is the product distribution of the marginals of $P_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}$; that is $P^{\Pi}_{X^k_{j+1}|(Z^k X^k_{<j})=\tau} = \prod_{i=1}^k P_{X^k_{j+1,i}|(Z^k X^k_{<j})=\tau}$.

Next, we upper-bound the left-hand side of Equation (61). At this point we recall the setting of Claim 5.6. For $i \in \mathcal{G}_\tau$ and $x^k_{j+1} \in \mathcal{X}^k$ let $f_i(x^k_{j+1}) = \alpha_{j,i}(\tau)/p_i(\tau)$ if $x^k_{j+1,i} = 1$ and 0 otherwise. Let $Y = \sum_{i \in \mathcal{G}_\tau} Y_i$, where the Y_i's are random variables defined as $Y_i = f_i(X^k_{j+1})$ and X^k_{j+1} is drawn either from $P_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}$ or $P^\Pi_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}$. Note that in the former case, the Y_i's are *dependent*, whereas in the latter case they are *independent*. This observation will play a crucial role ahead. Let $\Delta = \delta_j(X^k_{j+1};\tau)$, where again X^k_{j+1} is drawn either from $P_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}$ or $P^\Pi_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}$. The definition of δ_0 (see Table 1) yields that $Y = (1+\Delta)\cdot \sum_{i \in \mathcal{G}_\tau} \alpha_{j,i}(\tau)$. We can now upper-bound the left-hand side of Equation (61) as

$$
\begin{aligned}
\mathrm{E}_{x^k_{j+1} \sim P_{X^k_{j+1}|\tau, |\delta| \le 1/2}} \log \frac{\sum_{i \in \mathcal{G}_\tau} \alpha_{j,i}(\tau)}{\sum_{i \in 1_{x^k_{j+1}} \cap \mathcal{G}_\tau} \frac{\alpha_{j,i}(\tau)}{p_i(\tau)}} &= \mathrm{E}_{P_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}} \left[\log \frac{\sum_{i \in \mathcal{G}_\tau} \alpha_{j,i}(\tau)}{Y} \middle| |\Delta| \le 1/2 \right] \\
&= \mathrm{E}_{P_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}} \left[\log \frac{1}{1+\Delta} \middle| |\Delta| \le 1/2 \right] \\
&\le \mathrm{E}_{P_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}} \left[-\Delta + \Delta^2 \middle| |\Delta| \le 1/2 \right],
\end{aligned}
$$

where the inequality follows since $-\log(1+x) \le -x + x^2$ for all $-1/2 \le x \le 1/2$.

The proof of Claim 6.4 immediately follows form the next two claims that bound the expected values of $-\Delta$ and Δ^2.

Claim 6.5. *The exists $C_1 > 0$ such that*

$$
\mathrm{E}_{P_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}} [-\Delta | |\Delta| \le 1/2] \le C_1 \cdot \frac{m}{k}.
$$

Claim 6.6. *The exists $C_2 > 0$ such that*

$$
\mathrm{E}_{P_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}} \left[\Delta^2 \middle| |\Delta| \le 1/2 \right] \le C_2 \cdot \frac{m}{k} \cdot \left(D(P_{X^k_{j+1}|(Z^k X^k_{<j})=\tau} || P^\Pi_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}) + 1 \right).
$$

Claims 6.5 and 6.6 are proven in Sections 6.1.1 and 6.1.2, respectively. □

6.1.1 Proving Claim 6.5

A key fact toward proving Claim 6.5 is that the expected value of Y under $P_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}$ is exactly $\sum_{i \in \mathcal{G}_\tau} \alpha_{j,i}(\tau)$. Indeed, this is exactly the statement of Claim 5.6. Since $Y = (1+\Delta)\cdot \sum_{i \in \mathcal{G}_\tau} \alpha_{j,i}(\tau)$, the random variable Δ in fact measures how far Y is from its expectation. It follows that $\mathrm{E}_{P_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}}[\Delta] = 0$.

Assume that $\mathrm{E}_{P_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}}[\Delta | |\Delta| \le 1/2] < 0$, since otherwise the claim holds trivially. We use the following claim

Claim 6.7. *It holds that $\delta_j(x^k_{j+1}; z^k x^k_{<j}) \le 3000 \cdot m$, for every $j \in [m]$ and all $(z^k, x^k_{<j}, x^k_{j+1}) \in$ $\mathrm{Supp}(P_{Z^k X^k_{<j} X^k_{j+1}})$.*

Proof. By the definition of $\mathcal{G}_{z^k x^k_{<j}}$, it follows that for every $i \in \mathcal{G}_{z^k x^k_{<j}}$, it holds that $\alpha_{j,i}(z^k x^k_{<j}) \in [0.01, 10]$, and that

$$\begin{aligned} P_{X_{j+1,i}|Z^k X^k_{<j}}(1|z^k x^k_{<j}) &\geq 0.9 \cdot \frac{1}{m} \cdot \left(1 - \frac{1}{m}\right) \\ &\geq \frac{1}{3m}, \end{aligned} \tag{63}$$

where the second inequality holds by the assumption that $m \geq 2$. Thus,

$$\begin{aligned} \delta_j(x^k_{j+1}; z^k x^k_{<j}) &= \frac{\left(\sum_{i \in \mathcal{G}_{z^k x^k_{<j}} \bigcap 1_{x^k_{j+1}}} \frac{\alpha_{j,i}(z^k x^k_{<j})}{P_{X_{j+1,i}|Z^k X^k_{<j}}(1|z^k x^k_{<j})}\right)}{\left(\sum_{i \in \mathcal{G}_{z^k x^k_{<j}}} \alpha_{j,i}(z^k x^k_{<j})\right)} - 1 \\ &\leq \frac{\left|\mathcal{G}_{z^k x^k_{<j}}\right| \cdot 30 \cdot m}{\left|\mathcal{G}_{z^k x^k_{<j}}\right|/100} \\ &= 3000 \cdot m. \end{aligned}$$

□

Using that $\Delta \leq 3000 \cdot m$ and that $P_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}\left[|\Delta| \leq \frac{1}{2}\right] \geq 1 - \frac{m}{k^2}$ (Equation (59)), it follows that

$$\begin{aligned} 0 &= \mathrm{E}_{P_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}}[\Delta] \\ &= P_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}[|\Delta| \leq 1/2] \cdot \mathrm{E}_{P_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}}[\Delta||\Delta| \leq 1/2] \\ &\quad + P_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}[|\Delta| > 1/2] \cdot \mathrm{E}_{P_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}}[\Delta||\Delta| > 1/2] \\ &\leq \left(1 - \frac{m}{k^2}\right) \cdot \mathrm{E}_{P_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}}[\Delta||\Delta| \leq 1/2] + 3000 \cdot m \cdot \frac{m}{k^2} \\ &\leq \frac{1}{2} \cdot \mathrm{E}_{P_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}}[\Delta||\Delta| \leq 1/2] + 3000 \cdot \frac{m}{k}, \end{aligned} \tag{64}$$

where the last inequality holds since, by assumption, $k \geq m \geq 2$, so $m/k^2 \leq 1/2$ and $m^2/k^2 \leq m/k$. Setting $C_1 = 6000$ and rearranging the above equation complete the proof of the claim.

6.1.2 Proving Claim 6.6

To prove Claim 6.6 we would like to use Proposition 3.10. To do so, we need to show that Δ is well concentrated under $P^{\Pi}_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}$. This is where we use that the Y_i's are independent under $P^{\Pi}_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}$. Indeed, for $0 \leq t \leq 1$, Fact 3.16 yields that

$$\begin{aligned} P^{\Pi}_{X_{j+1}|(Z^k X^{<j})=\tau}[|\Delta| \geq t] &= P^{\Pi}_{X_{j+1}|(Z^k X^{<j})=\tau}[|Y - \mathrm{E}[Y]| \geq \mathrm{E}[Y] \cdot t] \\ &\leq 2 \exp\left(-\frac{(\mathrm{E}[Y] \cdot t)^2}{2(v + b \cdot \mathrm{E}[Y] \cdot t/3)}\right), \end{aligned}$$

for $b_i = \alpha_{j,i}(\tau)/p_i(\tau)$, $v = \sum_{i \in \mathcal{G}_\tau} b_i^2 p_i(\tau)$ and $b = \max\{b_i \colon i \in \mathcal{G}_\tau\}$, where the above expectation is taken over $P^{\Pi}_{X_{j+1}|(Z^k X^{<j})=\tau}$. Here again we use that τ was chosen condition that $B_j^{\text{hist}} = 1$. By Definition 5.8, it holds that $|\mathcal{G}_\tau| \geq k/10$, and for every $i \in \mathcal{G}_\tau$ it also holds that $\alpha_{j,i}(\tau) \in [0.01, 10]$ and $p_i(\tau) \geq 1/3m$ (Equation (63)). Claim 5.6 shows that $\mathrm{E}_{P^{\Pi}_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}}[Y] = \sum_{i \in \mathcal{G}_\tau} \alpha_{j,i}(\tau)$. It follows that $k/1000 \leq \mathrm{E}[Y] \leq 10k$, $v \leq 3 \cdot 10^2 \cdot mk$ and $b \leq 30m$. Plugging into the above equation, we have that

$$
\begin{aligned}
P^{\Pi}_{X_{j+1}|(Z^k X^{<j})=\tau}[|\Delta| \geq t] &\leq 2 \exp\left(-\frac{(k/1000 \cdot t)^2}{2(3 \cdot 10^2 \cdot mk + 30m \cdot 10k \cdot t/3)}\right) \\
&\leq 2 \exp\left(-\frac{t^2}{K_1 \cdot (m/k)}\right),
\end{aligned}
$$

where the second inequality follows since $t \leq 1$ and by setting K_1 to be large enough constant.

In the following, we set the constant λ of Lemma 5.12 to be $4K_1$. Since, by assumption, $k \geq \lambda m \geq 4K_1 m$ the above inequality implies that $P^{\Pi}_{X_{j+1}|(Z^k X^{<j})=\tau}[|\Delta| \geq 1] \leq 1/2$. Proposition 3.10 now yields that there exists a constant $K_2 > 0$ such that

$$
\begin{aligned}
&\mathrm{E}_{P_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}}\left[\Delta^2 \middle| |\Delta| \leq 1/2\right] \\
&\leq K_2 \cdot \frac{m}{k} \cdot \left(D(P_{X^k_{j+1}|(Z^k X^k_{<j})=\tau, |\delta_j(X^k_{j+1};\tau)| \leq 1/2} || P^{\Pi}_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}) + 1\right).
\end{aligned}
$$

To proof is completed by removing the condition on $|\delta(X^k_{j+1};\tau)| \leq 1/2$ from $P_{X^k_{j+1}|(Z^k X^k_{<j})=\tau, |\delta(X^k_{j+1};\tau)| \leq 1/2}$ via Fact 3.8. Formally, Fact 3.8 yields that

$$
\begin{aligned}
&D(P_{X^k_{j+1}|(Z^k X^k_{<j})=\tau, |\delta_j(X^k_{j+1};\tau)| \leq 1/2} || P^{\Pi}_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}) \\
&\leq \frac{1}{P_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}\left[|\Delta| \leq \frac{1}{2}\right]} \left(D(P_{X^k_{j+1}|(Z^k X^k_{<j})=\tau} || P^{\Pi}_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}) + \frac{1}{e} + 1\right).
\end{aligned}
$$

Recall that (Equation (59)) $P_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}\left[|\Delta| \leq \frac{1}{2}\right] \geq 1 - \frac{m}{k^2} \geq 1/2$, where the latter follows since $k \geq m \geq 2$. Setting $C_2 = 2(1 + 1/e)K_2$ completes the proof.

6.2 Round Zero, Proving Claim 6.1

Our goal in this section is to prove that there exists $C_0 > 0$ such that

$$
D(P^{cut}_{B_0 Z^k} || Q^{cut}_{B_0 Z^k}) \leq C_0 \cdot \frac{m}{k} \cdot \left(D(P_{Z^k X^k_1} || R_{Z^k X^k_1}) + 1\right). \tag{65}
$$

First, observe that if $|\mathcal{D}| < k \cdot 2^{\ell-1}$ or $\widehat{P}_{B_0^{\text{cur}}}(1) = P_{Z^k X^k_1}[|\delta_0(Z^k X^k_1)| \leq 1/2] < 1 - \frac{m}{k^2}$, then $B_0^{\text{hist}} = 0$ (and $B_0 = 0$) under both $\widehat{P}$ and $\widehat{Q}$, and thus $D(P^{cut}_{B_0 Z^k} || Q^{cut}_{B_0 Z^k}) = 0$. Henceforth, we assume that

$$
|\mathcal{D}| \geq k \cdot 2^{\ell-1} \qquad \text{and} \qquad P_{Z^k X^k_1}[|\delta_0(Z^k X^k_1)| \leq 1/2] \geq 1 - \frac{m}{k^2}. \tag{66}
$$

Next, similar arguments to those used to derive to Equation (58) yield that

$$\begin{aligned}D(P^{cut}_{B_0Z^k}||Q^{cut}_{B_0Z^k}) &\leq D(\widehat{P}_{Z^k|B_0=1}||\widehat{Q}_{Z^k|B_0=1})\\ &\leq D(\widehat{P}_{Z^kX_1^k|B_0=1}||\widehat{Q}_{Z^kX_1^k|B_0=1})\\ &\leq D(P_{Z^kX_1^k||\delta_0(Z^kX_1^k)|\leq 1/2}||Q'_{Z^kX_1^k}),\end{aligned}$$

where the second inequality follows from the monotonicity of divergence (Fact 3.5(2)), and the last inequality follows from Claim 5.10, letting $Q'_{Z^kX_1^k} = P_{Z^kX_1^k|I,Z_I,X_{1,I}=1} \circ Q_{IZ_I|IZ_I\in\mathcal{D}}$. Hence, to prove Claim 6.1 it suffices to prove the following claim, which we do below.

Claim 6.8. *There exists a universal constant* $C_0 > 0$ *such that*

$$D(P_{Z^kX_1^k||\delta_0(Z^kX_1^k)|\leq 1/2}||Q'_{Z^kX_1^k}) \leq C_0 \cdot \frac{m}{k} \cdot \Big(D(P_{Z^kX_1^k}||R_{Z^kX_1^k}) + 1\Big).$$

Proof of Claim 6.8. The structure of this proof is similar to that of the proofs of Claims 6.3 and 6.4 and throughout this proof we point to arguments used before in those proofs.

First, using that $P_{Z^kX_1^k}[|\delta_0(Z^kX_1^k)| \leq 1/2] \geq 1 - \frac{m}{k^2}$ (Equation (66)) and by similar arguments we used to derive Equation (60) it holds that

$$D(P_{Z^kX_1^k||\delta_0(Z^kX_1^k)|\leq 1/2}||Q'_{Z^kX_1^k}) \leq \frac{m}{k} + \mathop{\mathrm{E}}_{z^kx_1^k\sim P_{Z^kX_1^k||\delta_0(Z^kX_1^k)|\leq 1/2}} \log\frac{P_{Z^kX_1^k}(z^kx_1^k)}{Q'_{z^kX_1^k}(z^kx_1^k)}. \tag{67}$$

In the rest of the proof we show that there exists $C_0' > 0$ such that

$$\mathop{\mathrm{E}}_{z^kx_1^k\sim P_{Z^kX_1^k|\big|\delta_0(Z^kX_1^k)\big|\leq 1/2}} \log\frac{P_{Z^kX_1^k}(z^kx_1^k)}{Q'_{z^kX_1^k}(z^kx_1^k)} \leq C_0' \cdot \frac{m}{k} \cdot \Big(D(P_{Z^kX_1^k}||R_{Z^kX_1^k}) + 1\Big). \tag{68}$$

The proof of Claim 6.8 would then follow by taking $C_0 = 2 \cdot C_0'$.[25]

As in the proof of Claim 6.4, the first step is to lower-bound the right-hand side of Equation (68) using the product distribution of the marginals. Specifically, the chain rule for divergence (Fact 3.5(3)) yields that

$$D(P_{Z^kX_1^k}||R_{Z^kX_1^k}) \geq D(P_{Z^kX_1^k}||P^{\Pi}_{Z^kX_1^k}),$$

for $P^{\Pi}_{Z^kX_1^k} = \prod_{i=1}^k P_{Z_iX_{1,i}}$.

Our second step, again as in the proof of Claim 6.4, it to upper-bound the left-hand side of

[25] Note the difference from round j: Claim 6.4 — the analogous claim in round j to Equation (68) — did not immediately implies the proof of Claim 6.3 — the analogous claim in round j to Claim 6.8. The reason is that in round j we had to take into consideration the distribution of the previous transcript τ, which does not exists for round zero.

Equation (68). By the definition of δ_0 (see Table 1), it holds that

$$\begin{aligned}
Q'_{z^kX_1^k}(z^kx_1^k) &= \sum_{i=1}^{k} Q_{IZ_I|IZ_I\in\mathcal{D}}(i,z_i)\cdot P_{Z^kX_1^k|Z_iX_{1,i}}(z^kx_1^k|z_i,1)\\
&= \frac{1}{|\mathcal{D}|}\cdot\sum_{i=1}^{k}\mathbb{1}\{(i,z_i)\in\mathcal{D}\}\cdot P_{Z^kX_1^k|Z_iX_{1,i}}(z^kx_1^k|z_i,1)\\
&= \frac{1}{|\mathcal{D}|}\cdot\sum_{i\in 1_{x_1^k}}\mathbb{1}\{(i,z_i)\in\mathcal{D}\}\cdot P_{Z^kX_1^k|Z_iX_{1,i}}(z^kx_1^k|z_i,1)\\
&= \frac{1}{|\mathcal{D}|}\cdot\sum_{i\in 1_{x_1^k}}\mathbb{1}\{(i,z_i)\in\mathcal{D}\}\cdot\frac{P_{Z^kX_1^k}(z^kx_1^k)}{P_{Z_iX_{1,i}}(z_i1)}\\
&= P_{Z^kX_1^k}(z^kx_1^k)\cdot(1+\delta_0(z^kx_1^k)),
\end{aligned}$$

where the third equality holds since $P_{Z^kX_1^k|Z_iX_{1,i}}(z^kx_1^k|z_i,1)=0$ for every $i\notin 1_{x_1^k}$. Let $\Delta=\delta_0(Z^kX_1^k)$, where $Z^kX_1^k$ are drawn either from $P_{Z^kX_1^k}$ or $P^{\Pi}_{Z^kX_1^k}$. It follows that

$$\begin{aligned}
&\mathop{\mathrm{E}}_{z^kx_1^k\sim P_{Z^kX_1^k|\left|\delta_0(Z^kX_1^k)\right|\le 1/2}}\left[\log\frac{P_{Z^kX_1^k}(z^kx_1^k)}{Q'_{z^kX_1^k}(z^kx_1^k)}\right]\\
&= \mathop{\mathrm{E}}_{z^kx_1^k\sim P_{Z^kX_1^k|\left|\delta_0(Z^kX_1^k)\right|\le 1/2}}\left[\log\frac{1}{1+\delta_0(z^kx_1^k)}\right]\\
&= \mathop{\mathrm{E}}_{P_{Z^kX_1^k}}\left[\log\frac{1}{1+\Delta}\middle||\Delta|\le 1/2\right]\\
&\le \mathop{\mathrm{E}}_{P_{Z^kX_1^k}}\left[-\Delta+\Delta^2\middle||\Delta|\le 1/2\right],
\end{aligned}$$

where the inequality follows since $-\log(1+x)\le -x+x^2$ for all $-1/2\le x\le 1/2$.

We conclude the proof of Claim 6.8, and thus also of Claim 6.1, by proving the next two claims, analogous to Claims 6.5 and 6.6.

Claim 6.9. *The exists $C_1>0$ such that*

$$\mathrm{E}_{P_{Z^kX_1^k}}[-\Delta||\Delta|\le 1/2]\le C_1\cdot\frac{m}{k}.$$

Claim 6.10. *The exists $C_2>0$ such that*

$$\mathrm{E}_{P_{Z^kX_1^k}}\left[\Delta^2\middle||\Delta|\le 1/2\right]\le C_2\cdot\frac{m}{k}\cdot\Big(D(P_{Z^kX_1^k}||P^{\Pi}_{Z^kX_1^k})+1\Big).$$

Claims 6.9 and 6.10 are proven in Sections 6.2.1 and 6.2.2 respectively. Both proofs use the setting of Claim 5.7, which we now recall. For $i\in[k]$ let $p_i=P_{X_{1,i}}(1)$, and for $z^kx_1^k\in\{0,1\}^{\ell k}\times\{0,1\}^k$ let $f_i(z^kx_1^k)=\alpha_{0,i}(z_i)/p_i$ if $x_{1,i}^k=1$ and 0 otherwise. Let $Y=\sum_{i\in[k]}Y_i$, where the Y_i's are random variables defined as $Y_i=f_i(Z^kX_1^k)$ and $Z^kX_1^k$ are drawn either from $P_{Z^kX_1^k}$ or $P^{\Pi}_{Z^kX_1^k}$.

As it was the case in the proof Claim 6.4, that the Y_i's are independent under $P^{\Pi}_{Z^k X_1^k}$ will play a crucial role ahead. Finally, note that $Y = (1+\Delta) \cdot \frac{|\mathcal{D}|}{2^\ell}$.

The proof of Claim 6.8 follows immediately from Claims 6.9 and 6.10. □

6.2.1 Proving Claim 6.9

A key fact toward proving Claim 6.9 is that the expected value of Y under $P_{Z^k X_1^k}$ is exactly $\frac{|\mathcal{D}|}{2^\ell}$. Indeed, this is exactly the statement of Claim 5.7. Since $Y = (1+\Delta) \cdot \frac{|\mathcal{D}|}{2^\ell}$, the random variable Δ in fact measures how far Y is from its expectation. It follows that $\mathrm{E}_{P_{Z^k X_1^k}}[\Delta] = 0$.

Recall that by the assumptions we made in Equation (66), it holds that $|\mathcal{D}| \geq k \cdot 2^{\ell-1}$ and $P_{Z^k X_1^k}[|\Delta| \leq 1/2] \geq 1 - \frac{m}{k^2}$. We use the following claim.

Claim 6.11. *If $|\mathcal{D}| \geq k \cdot 2^{\ell-1}$, then $\delta_0(z^k x_1^k) \leq 6 \cdot m$, for every $z^k x_1^k \in \mathrm{Supp}(P_{Z^k X_1^k})$.*

Proof. Let $z^k x_1^k \in \mathrm{Supp}(P_{Z^k X_1^k})$. Assume that $(i, z_i) \in \mathcal{D}$. If follows that $i \in \mathcal{G}$ and $z_i \in \mathcal{Z}_i$. Since $i \in \mathcal{G}$, it follows that $|\rho_{0,1}| \leq 0.1$, which implies that $P_{X_{1,i}}(1) \geq 0.9/m$. And since $z_i \in \mathcal{Z}_i$, it follows that $P_{Z_i|X_{1,i}}(z_i|1) \geq 0.9 \cdot 2^{-\ell} \geq 2^{-(\ell+1)}$. Putting this together, we have that

$$\begin{aligned}
\delta_0(z^k x_1^k) &= \frac{\sum_{i \in 1_{x_1^k}} \frac{\mathbb{1}\{(i,z_i)\in\mathcal{D}\}}{P_{Z_i X_{1,i}}(z_i 1)}}{|\mathcal{D}|} - 1 \\
&\leq \frac{\sum_{i \in 1_{x_1^k}} \frac{\mathbb{1}\{(i,z_i)\in\mathcal{D}\}}{(0.9/m)\cdot 2^{-(\ell+1)}}}{|\mathcal{D}|} \\
&\leq \frac{3 \cdot k \cdot 2^\ell \cdot m}{|\mathcal{D}|}.
\end{aligned}$$

The proof now follows from the assumption that $|\mathcal{D}| \geq k \cdot 2^{\ell-1}$. □

Using Claim 6.11 and calculations similar using to those in Equation (64) complete the proof of the claim.

6.2.2 Proving Claim 6.10

As in the proof of Claim 6.6, we would like to show that Δ is well-concentrated under the product distribution $P^{\Pi}_{Z^k X_1^k}$. Showing this, however, requires more delicate analysis than in the aforementioned proof.

We rely on the following observation regarding the random variables Y_i's under $P^{\Pi}_{Z^k X_1^k}$. By definition, Y_i is chosen according to the underlying distribution $P_{Z_i X_{i,1}}$, where Z_i and $X_{i,1}$ are dependent. However, Y_i is not zero only if $X_{i,1} = 1$, and if $X_{i,1} = 1$, the value of Y_i depends only on Z_i. Thus, we can decouple the underlying distribution to a product distribution in which Z_i and $X_{1,i}$ are independent: we first choose whether Y_i is zero according to $P_{X_{1,i}}$ and then, assuming it is not zero, choose the value Y_i gets, according to $P_{Z_i|X_{1,i}=1}$. Formally, for $y > 0$ it holds that

$$\begin{aligned}
P_{Z_i X_{i,1}}[Y_i = y] &= P_{Z_i X_{i,1}}[X_{1,i} = 1 \wedge \alpha_{0,i}(Z_i) = y \cdot p_i] \\
&= P_{X_{1,i}}(1) \cdot P_{Z_i|X_{1,i}=1}[\alpha_{0,i}(Z_i) = y \cdot p_i] \\
&= P'_{Z_i X_{1,i}}[Y_i = y],
\end{aligned}$$

where we define $P'_{Z_i X_{1,i}} = P_{X_{1,i}} \cdot P_{Z_i|X_{1,i}=1}$. It is also easy to see that $P_{Z_i X_{i,1}}[Y_i = 0] = P'_{Z_i X_{1,i}}[Y_i = 0]$. We conclude that Y, and thus also Δ, has the same distribution under $P^{\Pi}_{Z^k X_1^k}$ and under $P'_{Z^k X_1^k} := \prod_{i=1}^k P'_{Z_i X_{i,1}}$. It will be easier to see that Δ is well concentrated under the latter distribution.

Let $A = \sum_{i=1}^k A_i$, where $A_1, \ldots, A_k$ are random variables defined as $A_i = \alpha_{0,i}(Z_i)$ and Z_i is drawn from $P'_{Z_i} = P_{Z_i|X_{1,i}=1}$. Let $\mu = |\mathcal{D}|/2^{\ell}$. For $0 < t \leq 1$, it holds that

$$\begin{aligned}
P^{\Pi}_{Z^k X_1^k}[|\Delta| \geq t] &= P^{\Pi}_{Z^k X_1^k}[|Y - \mu| \geq t\mu] \\
&= P'_{Z^k X_1^k}[|Y - \mu| \geq t\mu] \\
&= P'_{Z^k X_1^k}[|Y - \mu - A + A| \geq t\mu] \\
&\leq P'_{Z^k X_1^k}[|Y - A| + |A - \mu| \geq t\mu] \\
&\leq P'_{Z^k X_1^k}[|A - \mu| \geq t\mu/2] + P'_{Z^k X_1}[|Y - A| \geq t\mu/2] \\
&= P'_{Z^k}[|A - \mu| \geq t\mu/2] + P'_{Z^k X_1}[|Y - A| \geq t\mu/2]. \qquad (69)
\end{aligned}$$

We bound each term in Equation (69) separately. For the left-hand side term, we use Hoeffding's inequality. Indeed, similar calculations to those in the proof of Claim 5.7 show that $\mathrm{E}_{P'_{Z^k}}[A] = \mu$. Furthermore, the definitions of $\alpha_{0,i}(Z_i)$ and $\mathcal{D}$ (see Tables 1 and 2) yield that $A_i \in [0, 2]$ almost surely . Hoeffding's inequality (Fact 3.14) now gives the following bound:

$$\begin{aligned}
P'_{Z^k X_1^k}[|A - \mu| \geq t\mu/2] &\leq 2\exp\left(-\frac{(t\mu/2)^2}{2^2 \cdot k}\right) \qquad (70) \\
&\leq 2\exp\left(-\frac{t^2 k}{64}\right),
\end{aligned}$$

where the second inequality follows since $|\mathcal{D}| \geq k \cdot 2^{\ell-1}$ (Equation (66)), which implies that $\mu \geq k/2$.

To bound the right-hand side term in Equation (69), we use Fact 3.16. By the definition of $P'_{Z^k X_1^k}$, it holds that

$$P'_{Z^k X_1^k}[|Y - A| \geq t\mu/2] = \mathrm{E}_{z^k \sim P'_{Z^k}} P'_{X_1^k}[|Y - A| \geq t\mu/2 \mid A_1 = \alpha_{0,1}(z_1), \ldots, A_k = \alpha_{0,k}(z_k)].$$

Fix any $z^k \in \mathrm{Supp}(P'_{Z^k})$ and let $\alpha_i = \alpha_{0,i}(z_i)$. Note that condition on $A_i = \alpha_i$, the random variable Y_i is equal to α_i/p_i with probability $p_i = P_{X_{1,i}}(1)$ and 0 otherwise. Equivalently, $Y = \sum_{i=1}^k b_i Y'_i$ for $b_i = \alpha_i/p_i$ and $Y'_i \sim \mathrm{Bern}(p_i)$. Thus, $\mathrm{E}[Y] = \sum_{i=1}^k b_i p_i = \sum_{i=1}^k \alpha_i$. Let $v = \sum_{i=1}^k b_i^2 p_i = \sum_{i=1}^k \alpha_i^2/p_i$. As we argued above, it holds that $\alpha_i \leq 2$. Also, for i with $\alpha_i > 0$, it holds that $p_i \geq 0.9/m$ (if $\alpha_i > 0$, it must be the case that $(i, z_i) \in \mathcal{D}$, which implies that $i \in \mathcal{G}$, which means that $|\rho_{0,i}| \leq 0.1$). Hence, $v \leq 5km$ and $b = \max\{b_1, \ldots, b_k\} \leq 3m$. Letting $a = \sum_{i=1}^{k} \alpha_i$, Proposition 3.10 yields that:

$$\begin{aligned}
P'_{X_1^k}[|Y - A| \geq t\mu/2 \mid A_1 = \alpha_1, \ldots, A_k = \alpha_k] &= P'_{X_1^k}[|Y - a| \geq t\mu/2] \\
&\leq 2\exp\left(-\frac{(t\mu/2)^2}{2(v + bt\mu/6)}\right) \\
&\leq 2\exp\left(-\frac{(tk/4)^2}{2(5km + 3tkm/6)}\right) \\
&\leq 2\exp\left(-\frac{(tk/4)^2}{2(5km + km)}\right) \\
&= 2\exp\left(-\frac{t^2}{192 \cdot (m/k)}\right),
\end{aligned}$$

where the second inequality follows since $k/2 \leq \mu \leq k$, and the last inequality follows since $t \leq 1$. Since the above bound holds for any fixing of $z^k \in \mathrm{Supp}(P'_{Z^k})$, by taking expectation over P'_{Z^k}, we get the following bound:

$$P'_{Z^k X_1^k}[|Y - A| \geq tk/2] = 2\exp\left(-\frac{t^2}{192 \cdot (m/k)}\right). \tag{71}$$

Finally, plugging Equations (70) and (71) into Equation (69) yields that

$$\begin{aligned}
P^{\Pi}_{Z^k X_1^k}[|\Delta| \geq t] &\leq 2\exp\left(-\frac{t^2 k}{64}\right) + 2\exp\left(-\frac{t^2}{192 \cdot (m/k)}\right) \\
&\leq K_2 \cdot \exp\left(-\frac{t^2}{K_1 \cdot (m/k)}\right),
\end{aligned}$$

where the last inequality holds for $K_2 = 4$ and large enough K_1.

Since, by assumption, $k \geq \lambda m = 4K_1 m$ (we previously set $\lambda = 4K_1$), the above inequality implies that $P^{\Pi}_{Z^k X_1^k}[|\Delta| \geq 1] \leq 1/2$. Proposition 3.10 now yields that there exists a constant $K_3 > 0$ such that

$$\mathrm{E}_{P_{Z^k X_1^k}}\left[\Delta^2 \middle| |\Delta| \leq 1/2\right] \leq K_3 \cdot \frac{m}{k} \cdot \left(D(P_{Z^k X_1^k | |\Delta| \leq 1/2} || P^{\Pi}_{Z^k X_1^k}) + 1\right).$$

To proof is completed by removing the conditioning on $|\Delta| \leq 1/2$ from $P_{Z^k X_1^k | |\Delta| \leq 1/2}$ via Fact 3.8. Formally, Fact 3.8 yields that

$$\begin{aligned}
&D(P_{Z^k X_1^k | |\Delta| \leq 1/2} || P^{\Pi}_{Z^k X_1^k}) \\
&\leq \frac{1}{P_{Z^k X_1^k}\left[|\Delta| \leq \frac{1}{2}\right]} \left(D(P_{Z^k X_1^k} || P^{\Pi}_{Z^k X_1^k}) + \frac{1}{e} + 1\right).
\end{aligned}$$

Recall that $P_{Z^k X_1^k}[|\Delta| \leq 1/2] \geq 1 - \frac{m}{k^2} \geq 1/2$ (Equation (66)), where the latter follows since $k \geq m \geq 2$. Setting $C_2 = 2(1 + 1/e)K_3$ completes the proof.

7 Bounding the Probability of Failure in $\widehat{P}$

In this section, we prove Lemma 5.13, restated for convenience below.

Lemma 7.1 (Restatement of Lemma 5.13)**.** *For any constant $\lambda > 0$ there exist constants $\lambda', \lambda'' > 0$ such that the following holds: Let $k, m, \ell \in \mathbb{N}$, let $\varepsilon \in (0, 1/2]$, let $\mathcal{W} \subseteq \{0,1\}^{kl+k(m+1)}$ be a termination-consistent set (according to Definition 4.3) and let W, R and $\widehat{P}$ be the event and distributions from Definitions 5.1 and 5.8 respectively, for the above $k, m, \ell, \mathcal{W}$. Assume $k \geq \lambda' \cdot m^2/\varepsilon$ and $R[W] \geq (1-\varepsilon)^{\frac{k}{\lambda'' \cdot m}}$, then $\widehat{P}_{B^{m+2}}(1^{m+2}) \geq 1 - \varepsilon/\lambda$.*

In the following, let $\varepsilon, k, m, \ell, \mathcal{W}, W, R, \widehat{P}$ be as in Lemma 5.13 and let P and Q be the distributions from Definitions 4.7 and 4.8 (respectively) with respect to $k, m, \ell, \mathcal{W}$.

In Section 7.1 we state Lemma 7.2 which captures the heart of the proof of Lemma 5.13. In Section 7.2 we prove Lemma 5.13 using Lemma 7.2 and in Section 7.3 we prove Lemma 7.2.

7.1 Bounding the Number of Bad Columns in P

In order to give a formal statement for our main lemma, we broadly use the definitions of $\{\rho_{j,i}\}_{j=0}^{m+1}$, $\{\beta_{j,i}\}_{j=2}^{m+1}$, $\{\alpha_{j,i}\}_{j=0}^{m+1}$, $\{\delta_j\}_{j=0}^{m+1}$ given in Table 1 (Section 5) and the definitions of $\{\mathcal{I}_{x^k_{<j}}\}_{j=1}^{m+1}$, $\mathcal{G}$, $\{\mathcal{G}_{z^k x^k_{<j}}\}_{j=1}^{m+1}$, $\mathcal{Z}_i$, $\mathcal{D}$ given in Table 2 (Section 5), and in addition we define new sets and variables (Tables 3 to 5) which are also broadly used, and an intuition for their purpose is given below.

The following definitions are with respect to some fixing of $j \in [m+1]$ and $\tau_j = z^k x^k_{<j} \in \operatorname{Supp}(P_{Z^k X^k_{<j}})$.

$$Z^k X^{(m+1)\times k} | (Z^k X^k_{<j} = \tau_j) = \begin{bmatrix} z^k \\ x_1^k \\ x_2^k \\ \cdot \\ \cdot \\ x_{j-1}^k \\ X_j^k \\ \cdot \\ \cdot \\ X_{m+1}^k \end{bmatrix} = \begin{bmatrix} z_1 & z_2 & \dots & z_k \\ x_{1,1} & x_{1,2} & \dots & x_{1,k} \\ x_{2,1} & x_{2,2} & \dots & x_{2,k} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ x_{j-1,1} & x_{j-1,2} & \dots & x_{j-1,k} \\ X_{j,1} & X_{j,2} & \dots & X_{j,k} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ X_{m+1,1} & X_{m+1,2} & \dots & X_{m+1,k} \end{bmatrix}$$

Figure 2: A matrix representation of the random coins $Z^k X^{(m+1)\times k}$ at the beginning of round j conditioned on $Z^k X^k_{<j} = \tau_j$ for some $j \in [m+1]$ and $\tau_j = z^k x^k_{<j} \in \operatorname{Supp}(P_{Z^k X^k_{<j}})$ (lowercase letter represents a fixed value and an uppercase for a radnom variable which hasn't been determined yet).

First, in Table 3 we define $\gamma_{j,i}(\tau_j)$ which measures how much $P_{X_{j,i}|Z^k X^k_{<j}}(1|\tau_j)$ is far from $1/m$ (note that this is different from $\rho_{j,i}(\tau_j)$ which measures the probability according to the next round bit $X_{j+1,i}$ and not according to the current round's bit $X_{j,i}$). Next, we split the set of "good" columns $\mathcal{G}_{\tau_j}$ (defined in Table 2) into the sets $\mathcal{G}^{\rho}_{\tau_j}$ and $\mathcal{G}^{\alpha}_{\tau_j}$ that satisfy $\mathcal{G}_{\tau_j} = \mathcal{G}^{\rho}_{\tau_j} \cap \mathcal{G}^{\alpha}_{\tau_j} \cap \mathcal{G}$ ($\mathcal{G}$ is also defined in Table 2) and define a similar set $\mathcal{G}^{\gamma}_{\tau_j}$ with respect to the $\{\gamma_{j,i}\}$ measurements (see Table 4 for formal definitions). In addition, we define $u^{\gamma}_i(\tau_j), u^{\rho}_i(\tau_j), u^{\alpha}_i(\tau_j)$ that outputs the first

round $j' \in [j]$ (with respect to a column $i \in [k]$) which has unexpected large jump in the value of the measurement. Note that if $1 \in x_{<j',i}$ (i.e., the i^{th} verifier is not active at the beginning of round j') then by definition, $\gamma_{j',i} = \rho_{j',i} = -1$ since $X_{j,i} = X_{j+1,i} = 0$ (with probability 1) in this case. Therefore, we define it as follows: $u_i^{\gamma}(\tau_j)$ outputs the first round $j' \in [j]$ such that $1 \notin x_{<j',i}$ (equivalently, $i \in \mathcal{I}_{x^k_{<j'}}$ meaning that i is "active" at round j) but still has an unexpected large jump in the value of $\left|\gamma_{j',i}\right|$, where in case no such j' exists it outputs ∞. Similarly, we define u_i^{ρ} and u_i^{α} for the $\rho_{j',i}$ and $\alpha_{j',i}$ measurements (respectively), and define u_i to be the first round $j' \in [j]$ which has large jump in the value of (at least) one of the measurements: $\gamma_{j',i}$, $\rho_{j',i}$ or $\alpha_{j',i}$. Finally, for $\nu \in \{\gamma, \rho, \alpha\}$ we define $\text{jumps}^{\nu}(\tau_j)$ to be the number of columns $i \in [k]$ which have large jumps in the $\{\nu_{j,i}\}$'s measurements (i.e., with $u_i^{\nu}(\tau_j) < \infty$) and define $\text{jumps}(\tau_j)$ to be the number of columns $i \in [k]$ with a jump in any of the measurement (i.e., with $u_i(\tau_j) < \infty$). See Table 5 for the formal definitions.

Table 3: The $\gamma_{j,i}$ measurement

Definition	*Value*
$\gamma_{j,i}(\tau_j)$	$m \cdot P_{X_{j,i}\mid Z^k X^k_{<j}}(1\mid\tau_j) - 1$

Table 4: the typical columns for each measurement

Definition	*Value*
$\mathcal{G}^{\gamma}_{\tau_j}$	$\{i \in [k] \colon \forall j' \in [j]. \left|\gamma_{j',i}\right| \leq 0.1\}$
$\mathcal{G}^{\rho}_{\tau_j}$	$\{i \in [k] \colon \forall j' \in [j]. \left|\rho_{j',i}\right| \leq 0.1\}$
$\mathcal{G}^{\alpha}_{\tau_j}$	$\{i \in [k] \colon \forall j' \in [j]. \alpha_{j',i} \in [0.01, 10]\}$

An important observation of the above is that the following holds:

(a) $\mathcal{G}_{\tau_j} = \mathcal{G}^{\rho}_{\tau_j} \cap \mathcal{G}^{\alpha}_{\tau_j} \cap \mathcal{G}$.

(b) $\forall \nu \in \{\gamma, \rho, \alpha\}.\ i \in \mathcal{G}^{\nu}_{\tau_j} \iff \left(i \in \mathcal{I}_{x^k_{<j}}\right) \wedge (u_i^{\nu}(\tau_j) = \infty)$.

(c) $\left(i \in \mathcal{I}_{x^k_{<j}} \cap \mathcal{G}\right) \wedge (u_i(\tau_j) = \infty) \iff i \in \mathcal{G}^{\gamma}_{\tau_j} \cap \mathcal{G}^{\rho}_{\tau_j} \cap \mathcal{G}^{\alpha}_{\tau_j} \cap \mathcal{G} \implies i \in \mathcal{G}_{\tau_j}$.

(d) $\left|\mathcal{G}_{\tau_j}\right| \geq \left|\mathcal{I}_{x^k_{<j}}\right| - (k - |\mathcal{G}|) - \text{jumps}(\tau_j)$.

Note that we can interpret (c) as follows: if we have a column $i \in [k]$ which is "active" (i.e. $i \in \mathcal{I}_{x^k_{<j}}$, or equivalently, $1 \notin x_{<j,i}$), and it belongs to $\mathcal{G}$ — the set of "good" columns at the beginning, and it has no unexpected jump (i.e., $u_i(\tau_j) = \infty$), then it holds that $i \in \mathcal{G}_{\tau_j}$ (i.e., i is a "good" column in round j). In addition, note that (d) simply follows by (c) since $\left|\mathcal{I}_{x^k_{<j}} \cap \mathcal{G}\right| \geq \left|\mathcal{I}_{x^k_{<j}}\right| - (k - |\mathcal{G}|)$.

Using the above definitions, we can finally state our main lemma of this section.

Lemma 7.2. *[Bounding the number of bad columns in P] For any constant $\lambda > 0$, there exists a constant $\lambda' > 0$ such that the following holds: let $k, m, \ell, \mathcal{W}, \varepsilon$ be as in Lemma 5.13, let P be the* *distribution from Definition 4.7, let $\mathcal{G}, \mathcal{D}$ be the sets from Table 2 and let* jumps *be the function from Table 5. Assume that at least one of the following holds:*

1. $|\mathcal{D}| \le (1 - \varepsilon/\lambda)k \cdot 2^{\ell}$, *or*
2. $\mathrm{E}_P\left[\mathrm{jumps}(Z^k X^{(m+1)\times k})\right] \ge \varepsilon k/\lambda$,

then $R[W] \le (1-\varepsilon)^{\frac{k}{\lambda' \cdot m}}$.

Namely, Lemma 7.2 implies the following: if $R[W]$ is high enough, then most of the pairs $(i, z_i) \in [k] \times \{0,1\}^{\ell}$ must be "good" (i.e., in $\mathcal{D}$), and in expectation over P, most of the columns $i \in [k]$ should not have large jumps during the execution, (i.e., $\mathrm{E}_P\left[\mathrm{jumps}(Z^k X^{(m+1)\times k})\right]$ should be small).

Lemma 7.2 is used in Section 7.2 to prove Lemma 5.13, and in Section 7.3 we prove Lemma 7.2.

Table 5: first rounds with untypical measurement.

Definition	*Value*
$u_i^{\lvert\gamma\rvert>c}(\tau_j)$	$\begin{cases} \infty & \forall j' \in [j]: \ \left(\lvert\gamma_{j',i}\rvert \le c\right) \vee \left(1 \in x_{<j',i}\right) \\ \min\{j' \in [j] \colon \left(\lvert\gamma_{j',i}\rvert > c\right) \wedge \left(1 \notin x_{<j',i}\right)\} & \text{Otherwise} \end{cases}$
$u_i^{\gamma}(\tau_j)$	$u_i^{\lvert\gamma\rvert>0.1}(\tau_j)$
$u_i^{\lvert\rho\rvert>c}(\tau_j)$	$\begin{cases} \infty & \forall j' \in [j]: \ \left(\lvert\rho_{j',i}\rvert \le c\right) \vee \left(1 \in x_{<j',i}\right) \\ \min\{j' \in [j] \colon \left(\lvert\rho_{j',i}\rvert > c\right) \wedge \left(1 \notin x_{<j',i}\right)\} & \text{Otherwise} \end{cases}$
$u_i^{\rho}(\tau_j)$	$u_i^{\lvert\rho\rvert>0.1}(\tau_j)$
$u_i^{\alpha}(\tau_j)$	$\begin{cases} \infty & \forall j' \in [j]: \left(\alpha_{j',i} \in [0.01, 10]\right) \vee \left(1 \in x_{<j',i}\right) \\ \min\{j' \in [j] \colon \left(\alpha_{j',i} \notin [0.01, 10]\right) \wedge \left(1 \notin x_{<j',i}\right)\} & \text{Otherwise} \end{cases}$
$u_i(\tau_j)$	$\min\{u_i^{\gamma}(\tau_j), u_i^{\rho}(\tau_j), u_i^{\alpha}(\tau_j)\}$
$\mathrm{jumps}^{\gamma}(\tau_j)$	$\sum_{i=1}^{k} \mathbb{1}\{u_i^{\gamma}(\tau_j) < \infty\}$
$\mathrm{jumps}^{\rho}(\tau_j)$	$\sum_{i=1}^{k} \mathbb{1}\{u_i^{\rho}(\tau_j) < \infty\}$
$\mathrm{jumps}^{\alpha}(\tau_j)$	$\sum_{i=1}^{k} \mathbb{1}\{u_i^{\alpha}(\tau_j) < \infty\}$
$\mathrm{jumps}(\tau_j)$	$\sum_{i=1}^{k} \mathbb{1}\{u_i(\tau_j) < \infty\}$

7.2 Proving Lemma 5.13 Using Lemma 7.2

In this section we prove Lemma 5.13 by showing that if k and $R[W]$ are large enough, then $\widehat{P}_{B^{m+2}}(1^{m+2})$ must be close to 1. Recall that by the definition of $\widehat{P}$ (defined in Definition 5.8), each bit B_j equals to the product $B_j^{\mathrm{hist}} \cdot B_j^{\mathrm{indx}} \cdot B_j^{\mathrm{cur}}$. In the following, we extend the distribution of $\widehat{P}$ by separating the bits B_j^{hist} into two new bits $B_j^{\mathrm{large\_set}}$ and $B_j^{\mathrm{exp\_cur}}$ such that

$\widehat{P}_{B_j^{\text{hist}}|B_j^{\text{large\_set}},B_j^{\text{exp\_cur}}} = B_j^{\text{large\_set}} \cdot B_j^{\text{exp\_cur}}$. We do so by defining $\widehat{P}_{B_0^{\text{large\_set}}} = \mathbb{1}\{|\mathcal{D}| \geq k \cdot 2^{\ell-1}\}$ and $\widehat{P}_{B_0^{\text{exp\_cur}}} = \mathbb{1}\{\mathrm{E}_{P_{Z^k X_1^k}}\left[\widehat{P}_{B_0^{\text{cur}}|Z^k X_1^k}(0)\right] \leq \frac{m}{k^2}\}$, and for $j \in [m+1]$ we define $\widehat{P}_{B_j^{\text{large\_set}}|Z^k X_{<j}^k} = \mathbb{1}\{\left|\mathcal{G}_{Z^k X_{<j}^k}\right| \geq \frac{k}{10}\}$ and $\widehat{P}_{B_j^{\text{exp\_cur}}|Z^k X_{<j}^k} = \mathbb{1}\{\mathrm{E}_{P_{X_j^k|Z^k X_{<j}^k}}\left[\widehat{P}_{B_j^{\text{cur}}|Z^k X_{\leq j}^k}(0)\right] \leq \frac{m}{k^2}\}$.

In order to prove Lemma 5.13, we handle each type of bit separately. In Section 7.2.1 we handle the $B_j^{\text{large\_set}}$ bits, in Section 7.2.2 we hande the B_j^{indx} bits, and in Section 7.2.3 we handle the B_j^{cur} and $B_j^{\text{exp\_cur}}$ bits. Finally, in Section 7.2.4 we collect all parts and deduce the proof of Lemma 5.13.

7.2.1 The Large-Set Bits

Before handling the "large-set" bits, we first prove the following simple claim which state that the set of active verifiers $\mathcal{I}_{X^{(m+1)\times k}}$ is large.

Claim 7.3. *There exists a universal constant $\lambda > 0$ such that for any $q \in (0,1)$ the following holds: If $P\left[|\mathcal{I}_{X^{(m+1)\times k}}| \leq \frac{k}{9}\right] \geq q$, then $R[W] \leq \frac{1}{q} \cdot e^{-k/\lambda}$.*

Proof. Assume $P\left[|\mathcal{I}_{X^{(m+1)\times k}}| \leq \frac{k}{9}\right] \geq q$ for some $q \in (0,1)$. Observe that the distribution of $|\mathcal{I}_{X^{(m+1)\times k}}|$ when $X^{(m+1)\times k}$ is drawn from $R_{X^{(m+1)\times k}}$ is exactly $\mathrm{Bin}(k, (1-\frac{1}{m})^{m+1})$. Since $(1-\frac{1}{m})^{m+1} \geq \frac{1}{8}$ for $m \geq 2$, Hoeffding's inequality (Fact 3.14) yields that

$$\begin{aligned} R\left[|\mathcal{I}_{X^{(m+1)\times k}}| \leq \frac{k}{9}\right] &\leq \Pr[\mathrm{Bin}(k, 1/8) \leq k/9] \\ &\leq e^{-k/\lambda}, \end{aligned}$$

for some universal constant $\lambda > 0$, and we conclude that

$$R[W] \leq \frac{R\left[|\mathcal{I}_{X^{(m+1)\times k}}| \leq \frac{k}{9}\right]}{P\left[|\mathcal{I}_{X^{(m+1)\times k}}| \leq \frac{k}{9}\right]} \leq \frac{1}{q} \cdot e^{-k/\lambda}$$

as required. □

In addition, we prove that if $R[W]$ is high enough and if k is large enough, then the probability (over P) that $|\mathcal{G}_{Z^k X^{(m+1)\times k}}| \geq \frac{k}{10}$ is high.

Claim 7.4. *For any constant $\lambda > 0$, there exists constants $\lambda', \lambda'' > 0$ such that the following holds: If $P[|\mathcal{G}_{Z^k X^{(m+1)\times k}}| \geq \frac{k}{10}] \leq 1 - \varepsilon/\lambda$ and $k \geq \lambda'/\varepsilon$, then $R[W] \leq (1-\varepsilon)^{\frac{k}{\lambda'' \cdot m}}$.*

Proof. Assume that $P[|\mathcal{G}_{Z^k X^{(m+1)\times k}}| \geq \frac{k}{10}] \leq 1 - \varepsilon/\lambda$ for some constant $\lambda > 0$. Note that by definition, for any fixed $Z^k X^{(m+1)\times k}$ it holds that

$$|\mathcal{G}_{Z^k X^{(m+1)\times k}}| \geq |\mathcal{I}_{X^{(m+1)\times k}}| - (k - |\mathcal{G}|) - \mathrm{jumps}(Z^k X^{(m+1)\times k}) \tag{72}$$

By assumption, one of the following items must hold:

1. $|\mathcal{G}| \leq 0.999k$, or

2. $P\left[|\mathcal{I}_{Z^k X^{(m+1)\times k}}| \leq \frac{k}{9}\right] \geq \varepsilon/2\lambda$, or

3. $P\left[\mathrm{jumps}(Z^k X^{(m+1)\times k}) \geq 0.001k\right] \geq \varepsilon/2\lambda$.

If Item 1 holds, then we deduce from Lemma 7.2(1) that $R[W] \leq (1-\varepsilon)^{\frac{k}{c \cdot m}}$, where c is the constant $\lambda' = \lambda'(1000)$ of Lemma 7.2 (note that $|\mathcal{D}| \leq |\mathcal{G}| \cdot 2^{\ell}$). If Item 2 holds, then we deduce from Claim 7.3 that $R[W] \leq \frac{2\lambda}{\varepsilon} \cdot e^{-k/c'} \leq (1-\varepsilon)^{\frac{k}{2c'}}$, where c' is the universal constant λ' of Claim 7.3, and the second inequality holds by choosing the claim's constant λ' to be large enough such that $k > \lambda'/\varepsilon$ implies it. If Item 3 holds, then in particular it holds that

$$\mathrm{E}_P\left[\mathrm{jumps}(Z^k X^{(m+1)\times k})\right] \geq \frac{\varepsilon k}{2000\lambda}$$

Hence, we deduce from Lemma 7.2(2) that $R[W] \leq (1-\varepsilon)^{\frac{k}{c'' \cdot m}}$ where c'' is the constant $\lambda' = \lambda'(2000\lambda)$ of Lemma 7.2. By setting the claim's constant $\lambda'' = \max\{c, 2c', c''\}$, the proof follows. □

As a corollary of Lemma 7.2 and Claim 7.4, it holds that if k and $R[W]$ are large enough, then the probability of failure (over $\widehat{P}$) in the "large_set" bits is low.

Corollary 7.5. *For any constant $\lambda > 0$, there exists constants $\lambda', \lambda'' > 0$ such that the following holds: If $\widehat{P}_{B_0^{\mathrm{large\_set}},\ldots,B_{m+1}^{\mathrm{large\_set}}}(1^{m+2}) \leq 1 - \varepsilon/\lambda$ and $k \geq \lambda'/\varepsilon$, then $R[W] \leq (1-\varepsilon)^{\frac{k}{\lambda'' \cdot m}}$.*

Proof. Assume that $\widehat{P}_{B_0^{\mathrm{large\_set}},\ldots,B_{m+1}^{\mathrm{large\_set}}}(1^{m+2}) \leq 1-\varepsilon/\lambda$ for some constant $\lambda > 0$. If $\widehat{P}_{B_0^{\mathrm{large\_set}}}(1) = 0$, then $|\mathcal{D}| \leq k \cdot 2^{\ell-1}$ and the proof follows by Lemma 7.2(1). Otherwise, $\widehat{P}_{B_0^{\mathrm{large\_set}}}(1) = 1$ and therefore, $\widehat{P}_{B_1^{\mathrm{large\_set}},\ldots,B_{m+1}^{\mathrm{large\_set}}}(1^{m+2}) \leq 1 - \varepsilon/\lambda$. Since $\widehat{P}_{Z^k X^{(m+1)\times k}} \equiv P$ and since $\widehat{P}_{B_0^{\mathrm{large\_set}},\ldots,B_{m+1}^{\mathrm{large\_set}}|Z^k X^{(m+1)\times k}}(1^{m+2}) = \mathbb{1}\{|\mathcal{G}_{Z^k X^{m\times k}}| \geq \frac{k}{10}\} \geq \mathbb{1}\{|\mathcal{G}_{Z^k X^{(m+1)\times k}}| \geq \frac{k}{10}\}$ (for any fixed $Z^k X^{(m+1)\times k}$), we deduce that $P[|\mathcal{G}_{Z^k X^{(m+1)\times k}}| \geq \frac{k}{10}] \leq 1-\varepsilon/\lambda$ and the proof follows by Claim 7.4. □

7.2.2 The Index Bits

In order to bound the probability of failure (over $\widehat{P}$) in the "index" bits, we make use of the following two claims. The proof of the first claim appears in Corollary 7.24.

Claim 7.6. *For any constant $\lambda > 0$ there exists a constant $\lambda' > 0$ such that if $\mathrm{E}_P\left[\sum_{i=1}^{k}\sum_{j=1}^{m+1} \gamma_{j,i} \cdot \mathbb{1}\{\gamma_{j,i} > 1\}\right] \geq \varepsilon k/\lambda$ for $\gamma_{j,i} = \gamma_{j,i}(Z^k X^{(m+1)\times k})$, then $R[W] \leq (1-\varepsilon)^{\frac{k}{\lambda' \cdot m}}$.*

Claim 7.7. *For any constant $\lambda > 0$ there exists a constant $\lambda' > 0$ such that if $\mathrm{E}_P\left[\sum_{i=1}^{k}\sum_{j=1}^{m+1} (1+\gamma_{j,i}) \cdot \mathbb{1}\{u_i = j\}\right] \geq \varepsilon k/\lambda$ for $\gamma_{j,i} = \gamma_{j,i}(Z^k X^k_{<j})$ and $u_i = u_i(Z^k X^{(m+1)\times k})$, then $R[W] \leq (1-\varepsilon)^{\frac{k}{\lambda' \cdot m}}$.*

Proof. Observe that

$$\begin{aligned}
&\mathrm{E}_P\left[\sum_{i=1}^{k}\sum_{j=1}^{m+1}(1+\gamma_{j,i})\cdot \mathbb{1}\{u_i=j\}\right]\\
&=\mathrm{E}_P\left[\sum_{i=1}^{k}\sum_{j=1}^{m+1}(1+\gamma_{j,i})\cdot \mathbb{1}\{u_i=j\}\cdot\left(\mathbb{1}\{\gamma_{j,i}\le 1\}+\mathbb{1}\{\gamma_{j,i}>1\}\right)\right]\\
&\le 2\cdot\mathrm{E}_P\left[\sum_{i=1}^{k}\sum_{j=1}^{m+1}\mathbb{1}\{u_i=j\}\right]+2\cdot\mathrm{E}_P\left[\sum_{i=1}^{k}\sum_{j=1}^{m+1}\gamma_{j,i}\cdot\mathbb{1}\{\gamma_{j,i}>1\}\right]\\
&=2\cdot\mathrm{E}_P\left[\mathrm{jumps}(Z^kX^{(m+1)\times k})\right]+2\cdot\mathrm{E}_P\left[\sum_{i=1}^{k}\sum_{j=1}^{m+1}\gamma_{j,i}\cdot\mathbb{1}\{\gamma_{j,i}>1\}\right],
\end{aligned}$$

By assumption, at least one of the following items must holds:

1. $\mathrm{E}_P\left[\mathrm{jumps}(Z^kX^{(m+1)\times k})\right]\ge\frac{\varepsilon}{4\lambda}$, or

2. $\mathrm{E}_P\left[\sum_{i=1}^{k}\sum_{j=1}^{m+1}\gamma_{j,i}\cdot\mathbb{1}\{\gamma_{j,i}>1\}\right]\ge\frac{\varepsilon}{4\lambda}$.

If Item 1 holds, then Lemma 7.2(2) implies that $R[W]\le(1-\varepsilon)^{\frac{k}{c\cdot m}}$, where $c>0$ is the constant $\lambda'=\lambda'(4\lambda)>0$ of Lemma 7.2. If Item 2 holds then Claim 7.6 implies that $R[W]\le(1-\varepsilon)^{\frac{k}{c'\cdot m}}$, where $c'>0$ is the constant $\lambda'=\lambda'(4\lambda)>0$ of Claim 7.6. Hence, the proof follows by setting $\lambda'=\max\{c,c'\}$. □

As a corollary of Claim 7.7, if k and $R[W]$ are large enough, then the probability of failure (over $\widehat{P}$) in the "index" bits is low.

Corollary 7.8. *For any constant $\lambda>0$, there exists constants $\lambda',\lambda''>0$ such that the following holds: If $\widehat{P}_{B_0^{\mathrm{indx}},\ldots,B_{m+1}^{\mathrm{indx}}}(1^{m+2})\le 1-\varepsilon/\lambda$ and $k\ge\lambda'/\varepsilon$, then $R[W]\le(1-\varepsilon)^{\lambda''\cdot k/m}$.*

Proof. Assume that $\widehat{P}_{B_0^{\mathrm{indx}},\ldots,B_{m+1}^{\mathrm{indx}}}(1^{m+2})\le 1-\varepsilon/\lambda$ for some constant $\lambda>0$. If $\widehat{P}_{B_0^{\mathrm{indx}}}(0)\ge\frac{\varepsilon}{2\lambda}$, then $|\mathcal{D}|\le(1-\frac{\varepsilon}{2\lambda})\cdot k\cdot 2^{\ell}$ and by Lemma 7.2(1) we deduce that $R[W]\le(1-\varepsilon)^{\frac{k}{c\cdot m}}$, where $c>0$ is the constant $\lambda'=\lambda'(2\lambda)>0$ of Lemma 7.2. Otherwise, it holds that $\widehat{P}_{B_1^{\mathrm{indx}},\ldots,B_{m+1}^{\mathrm{indx}}}(1^{m+2})<1-\frac{\varepsilon}{2\lambda}$. Observe that for any fixing of $Z^kX^{(m+1)\times k}$ with $|\mathcal{G}_{Z^kX^{(m+1)\times k}}|\ge\frac{k}{10}$ and for any $j\in[m+1]$, it holds that

$$\begin{aligned}
\widehat{P}_{B_j^{indx}|Z^k X^k_{<j}}(0) &= \Pr_{i \sim Q_{I|Z^k X^k_{<j}, I \in \mathcal{G}_{j-1}}}[i \notin \mathcal{G}_j] \\
&= \frac{\sum_{i \in \mathcal{G}_{j-1} \setminus \mathcal{G}_j} \alpha_{j,i}}{\sum_{i' \in \mathcal{G}_{j-1}} \alpha_{j,i'}} \\
&= \frac{\sum_{i \in \mathcal{G}_{j-1} \setminus \mathcal{G}_j} \alpha_{j-1,i} \cdot \frac{P_{X_{j,i}|Z^k X^k_{<j'}}(1)}{P_{X_{j,i}|Z^k X^k_{<j-1}}(1)}}{\sum_{i' \in \mathcal{G}_{j-1}} \alpha_{j,i'}} \\
&\leq \frac{\sum_{i \in \mathcal{G}_{j-1} \setminus \mathcal{G}_j} 10 \cdot \frac{P_{X_{j,i}|Z^k X^k_{<j'}}(1)}{\frac{1-0.1}{m}(1-\frac{1}{m})}}{0.01 \cdot |\mathcal{G}_j|} \\
&\leq 25000 \cdot \frac{m}{k} \cdot \sum_{i \in \mathcal{G}_{j-1} \setminus \mathcal{G}_j} P_{X_{j,i}|Z^k X^k_{<j'}}(1) \\
&= 25000 \cdot \frac{1}{k} \cdot \sum_{i=1}^{k} (1 + \gamma_{j,i}) \cdot \mathbb{1}\{u_i = j\},
\end{aligned} \tag{73}$$

where we let $\mathcal{G}_{j-1} = \mathcal{G}_{Z^k X^k_{<j-1}}$ and $\mathcal{G}_j = \mathcal{G}_{Z^k X^k_{<j}}$. The second equality in (73) holds by Claim 5.4, the first inequality holds since $i \in \mathcal{G}_{j-1} \implies a_{j-1,i} \in [0.01, 10], |\rho_{j-1,i}| \leq 0.1$ and since $\sum_{i' \in \mathcal{G}_{j-1}} \alpha_{j,i'} \geq \sum_{i' \in \mathcal{G}_j} \alpha_{j,i'} \geq 0.01 \cdot |\mathcal{G}_j|$, and the last inequality holds since $|\mathcal{G}_j| \geq |\mathcal{G}_{Z^k X^{(m+1) \times k}}| \geq \frac{k}{10}$ and since $m \geq 2$. Therefore, by assumption we deduce that

$$\begin{aligned}
\frac{\varepsilon}{2\lambda} &\leq \widehat{P}_{B_1^{\text{indx}}, \ldots, B_{m+1}^{\text{indx}}}[\exists j \in [m+1] \text{ s.t. } B_j^{\text{indx}} = 0] \\
&\leq \sum_{j=1}^{m+1} \widehat{P}_{B_j^{\text{indx}}}(0) \\
&= \mathrm{E}_P\left[\sum_{j=1}^{m+1} \widehat{P}_{B_j^{\text{indx}}|Z^k X^k_{<j}}(0)\right] \\
&\leq \mathrm{E}_P\left[\sum_{j=1}^{m+1} \widehat{P}_{B_j^{\text{indx}}|Z^k X^k_{<j}}(0) \mid |\mathcal{G}_{Z^k X^{(m+1) \times k}}| \geq \frac{k}{10}\right] + P\left[|\mathcal{G}_{Z^k X^{(m+1) \times k}}] \geq \frac{k}{10}\right| \\
&\leq 25000 \cdot \frac{1}{k} \cdot \mathrm{E}_P\left[\sum_{i=1}^{k} \sum_{j=1}^{m+1} (1 + \gamma_{j,i}) \cdot \mathbb{1}\{u_i = j\}\right] + P\left[|\mathcal{G}_{Z^k X^{(m+1) \times k}}] \geq \frac{k}{10}\right|,
\end{aligned}$$

where the last inequality holds by Equation (73). Hence, one of the above two item must hold:

1. $\mathrm{E}_P\left[\sum_{i=1}^{k} \sum_{j=1}^{m+1} (1 + \gamma_{j,i}) \cdot \mathbb{1}\{u_i = j\}\right] \geq \frac{\varepsilon k}{10^5 \cdot \lambda}$, or
2. $P\left[|\mathcal{G}_{Z^k X^{(m+1) \times k}}] \geq \frac{k}{10}\right| \geq \frac{\varepsilon}{4\lambda}$.

If Item 1 holds, then Claim 7.7 implies that $R[W] \leq (1-\varepsilon)^{\frac{\varepsilon k}{c' \cdot m}}$ where c' is the constant $\lambda' = \lambda'(10^5 \cdot \lambda)$ of Claim 7.7. If Item 2 holds, then by setting the constant λ' of the claim to the constant $\lambda' = \lambda'(4\lambda)$

of Claim 7.4, we obtain that Claim 7.4 implies that $R[W] \leq (1-\varepsilon)^{\frac{\varepsilon k}{c''\cdot m}}$ where c'' is the constant $\lambda'' = \lambda''(4\lambda)$ of Claim 7.4. The proof then follows by setting the constant λ'' of the corollary to $\lambda'' = \max\{c, c', c''\}$. □

7.2.3 The Current-Round Bits

In this section we handle the B_j^{cur} and $B_j^{\mathrm{exp\_cur}}$ bits. Assuming that $R[W]$ is large enough, the following claim states that if $B_j^{\mathrm{large\_set}} = 1$ (i.e., the set of"good" columns $\mathcal{G}_{Z^k X^k_{<j}}$ is large) then $B_j^{\mathrm{exp\_cur}} = 1$ (i.e., the probability that $|\delta_j| > 0.5$ is small).

Claim 7.9. *There exists two constants $\lambda, \lambda' > 0$ such that the following holds: If $k \geq \lambda \cdot m^2$ and $\exists j \in (m+1)$ such that $\widehat{P}_{B_j^{\mathrm{large\_set}}, B_j^{\mathrm{exp\_cur}}}(1,0) > 0$, then $R[W] \leq (1-\varepsilon)^{\frac{k}{\lambda'\cdot m}}$.*

Proof. We separately handle two cases: $j = 0$ and $j \in [m+1]$.

The case $j = 0$: In this case, it holds that $|\mathcal{D}| \geq k \cdot 2^{\ell-1}$ (in particular, $|\mathcal{G}| \geq \frac{k}{2}$), and that

$$P_{Z^k X_1^k}\left[\left|\delta_0(Z^k X_1^k)\right| > 0.5\right] > \frac{m}{k^2}. \tag{74}$$

and recall that

$$\delta_0(z^k x_1^k) = \left(\sum_{i \in 1_{x_1^k}} \frac{\alpha_{0,i}(z_i)}{P_{X_{1,i}}(1)}\right) / \left(|\mathcal{D}|/2^\ell\right) - 1$$

In the following, we define

1. $\delta_0^X(x_1^k; z^k) = \left(\sum_{i \in 1_{x_1^k}} \frac{\alpha_{0,i}(z_i)}{P_{X_{1,i}}(1)}\right) / \left(\sum_{i=1}^k \alpha_{0,i}(z_i)\right) - 1$,
2. $\delta_0^Z(z^k) = \left(\sum_{i=1}^k \alpha_{0,i}(z_i)\right) / \left(|\mathcal{D}|/2^\ell\right) - 1 = \left(\sum_{i=1}^k \frac{\mathbb{1}\{(i,z) \in \mathcal{D}\}}{P_{Z_i | X_{1,i}=1}(z_i)}\right) / |\mathcal{D}| - 1$.

and observe that

$$\begin{aligned}
\delta_0 &= \left(\left(1 + \delta_0^X\right) \cdot \sum_{i=1}^k \alpha_{0,i}\right) / \left(|\mathcal{D}|/2^\ell\right) - 1 \\
&= \left(\left(1 + \delta_0^X\right) \cdot \left(1 + \delta_0^Z\right) \cdot |\mathcal{D}|/2^\ell\right) / \left(|\mathcal{D}|/2^\ell\right) - 1 \\
&= \delta_0^X + \delta_0^Z + \delta_0^X \cdot \delta_0^Z
\end{aligned} \tag{75}$$

Therefore, by Equations (74) and (75), one of the following must holds

1. $P_{Z^k X_1^k}\left[\left|\delta_0^X(X_1^k; Z^k)\right| > 0.2\right] > \frac{m}{2k^2}$, or
2. $P_{Z^k}\left[\left|\delta_0^Z(Z^k)\right| > 0.2\right] > \frac{m}{2k^2}$

Note that the sum $\sum_{i=1}^{k} \frac{\mathbb{1}\{(i,z)\in\mathcal{D}\}}{P_{Z_i|X_{1,i}=1}(z_i)}$ when z^k is drawn from R_{Z^k} is a sum of k independent random variable, where

$$\begin{aligned}
\mathrm{E}_{z^k\sim R_{Z^k}}\left[\sum_{i=1}^{k} \frac{\mathbb{1}\{(i,z)\in\mathcal{D}\}}{P_{Z_i|X_{1,i}=1}(z_i)}\right] &= \sum_{z\in\{0,1\}^\ell}\sum_{i=1}^{k} 2^{-\ell}\cdot \frac{\mathbb{1}\{(i,z)\in\mathcal{D}\}}{P_{Z_i|X_{1,i}=1}(z_i)} \\
&\in \frac{1}{1\pm 0.1}\cdot \sum_{z\in\{0,1\}^\ell}\sum_{i=1}^{k}\mathbb{1}\{(i,z)\in\mathcal{D}\} \\
&\subseteq (0.9, 1.15)\cdot|\mathcal{D}| \qquad (76)
\end{aligned}$$

and the i^{th} variable is bounded in the interval $[0, \frac{1}{1-0.1}\cdot 2^\ell] \subseteq [0, 1.15\cdot 2^\ell]$. Therefore,

$$\begin{aligned}
&\Pr_{z^k\sim R_{Z^k}}\left[\left|\delta_0^Z(z^k)\right| > 0.2\right] \\
&= \Pr_{z^k\sim R_{Z^k}}\left[\left|\sum_{i=1}^{k}\frac{\mathbb{1}\{(i,z)\in\mathcal{D}\}}{P_{Z_i|X_{1,i}=1}(z_i)} - |\mathcal{D}|\right| > 0.2\cdot|\mathcal{D}|\right] \\
&\leq \Pr_{z^k\sim R_{Z^k}}\left[\left|\sum_{i=1}^{k}\frac{\mathbb{1}\{(i,z)\in\mathcal{D}\}}{P_{Z_i|X_{1,i}=1}(z_i)} - \mathrm{E}_{z^k\sim R_{Z^k}}\left[\sum_{i=1}^{k}\frac{\mathbb{1}\{(i,z)\in\mathcal{D}\}}{P_{Z_i|X_{1,i}=1}(z_i)}\right]\right| > 0.05\cdot|\mathcal{D}|\right] \\
&\leq 2\cdot\exp\!\left(-\frac{2\cdot(0.05\cdot|\mathcal{D}|)^2}{k\cdot(1.15\cdot 2^\ell)^2}\right) \\
&\leq 2\cdot\exp\!\left(-\frac{k}{2\cdot 10^3 m}\right) \qquad (77)
\end{aligned}$$

where the first inequality holds by Equation (76), the second one by Fact 3.14 (Hoeffding's inequality) and the last one holds since $|\mathcal{D}| \geq k\cdot 2^{\ell-1}$.

In the following, fix z^k with $\left|\delta_0^Z(z^k)\right| \leq 0.2 \implies \left(\sum_{i=1}^{k}\alpha_{0,i}(z_i)\right)/\left(k\cdot 2^{\ell-1}/2^\ell\right) - 1 \geq -0.2 \implies \sum_{i=1}^{k}\alpha_{0,i}(z_i) \geq 0.4k$. Note that the sum $\sum_{i\in 1_{x_1^k}}\frac{\alpha_{0,i}(z_i)}{P_{X_{1,i}}(1)}$ when x_1^k is drawn from $R_{X_1^k}$ is a sum of k independent random variables, where the i^{th} variable (which corresponds to $\mathbb{1}\{x_1^k = 1\}\cdot\frac{\alpha_{0,i}(z_i)}{P_{X_{1,i}}(1)}$) is distributed according to $b_i\cdot\mathrm{Bern}(1/m)$ for $b_i = \frac{\alpha_{0,i}(z_i)}{P_{X_{1,i}}(1)} \in \frac{\alpha_{0,i}(z_i)}{(1\pm 0.1)\cdot 1/m} \subseteq (0.9, 1.15)\cdot m\cdot\alpha_{0,i}(z_i)$. Therefore,

$$\mathrm{E}_{x_1^k\sim R_{X_1^k}}\left[\sum_{i\in 1_{x_1^k}}\frac{\alpha_{0,i}(z_i)}{P_{X_{1,i}}(1)}\right] \in \frac{1}{1\pm 0.1}\cdot\sum_{i=1}^{k}\alpha_{0,i}(z_i) \subseteq (0.9, 1.15)\cdot\sum_{i=1}^{k}\alpha_{0,i}(z_i) \qquad (78)$$

and we obtain that

$$\begin{aligned}
&\Pr_{x_1^k \sim R_{X_1^k}}\left[\left|\delta_0^X(x_1^k; z^k)\right| > 0.2\right]\\
&= \Pr_{x_1^k \sim R_{X_1^k}}\left[\left|\sum_{i \in 1_{x_1^k}} \frac{\alpha_{0,i}(z_i)}{P_{X_{1,i}}(1)} - \sum_{i=1}^{k} \alpha_{0,i}(z_i)\right| > 0.2 \cdot \sum_{i=1}^{k} \alpha_{0,i}(z_i)\right]\\
&\leq \Pr_{x_1^k \sim R_{X_1^k}}\left[\left|\sum_{i \in 1_{x_1^k}} \frac{\alpha_{0,i}(z_i)}{P_{X_{1,i}}(1)} - \mathrm{E}_{x_1^k \sim R_{X_1^k}}\left[\sum_{i \in 1_{x_1^k}} \frac{\alpha_{0,i}(z_i)}{P_{X_{1,i}}(1)}\right]\right| > 0.05 \cdot \sum_{i=1}^{k} \alpha_{0,i}(z_i)\right]\\
&\leq 2\exp\left(-\frac{(0.05 \cdot \sum_{i=1}^{k} \alpha_{0,i}(z_i))^2}{2(\sum_{i=1}^{k} b_i^2/m + \max\{b_i\} \cdot 0.05 \cdot \sum_{i=1}^{k} \alpha_{0,i}(z_i)/3)}\right)\\
&\leq 2\exp\left(-\frac{k}{10^4 m}\right) \qquad (79)
\end{aligned}$$

where the first inequality holds by Equation (78), the second one holds by Fact 3.16 and the third one holds since $\max\{b_i\} \leq 2m$ and $\sum_{i=1}^{k} \alpha_{0,i}(z_i) \geq 0.4k$.

Using Equations (77) and (79), we conclude that

$$\begin{aligned}
R_{Z^k X_1^k}\left[\left|\delta_0(Z^k X_1^k)\right| > 0.5\right] &\leq R_{Z^k}\left[\left|\delta_0^Z(Z^k)\right| > 0.2\right] + R_{Z^k X_1^k \mid |\delta_0^Z(Z^k)| \leq 0.2}\left[\left|\delta_0^X(X_1^k; Z^k)\right| > 0.2\right]\\
&\leq 4 \cdot \exp\left(-\frac{k}{10^4 m}\right),
\end{aligned}$$

$$\implies R[W] \leq \frac{R_{Z^k X_1^k}\left[\left|\delta_0(Z^k X_1^k)\right| > 0.5\right]}{P_{Z^k X_1^k}\left[\left|\delta_0(Z^k X_1^k)\right| > 0.5\right]} \leq \frac{4 \cdot \exp\left(-\frac{k}{10^4 m}\right)}{m/k^2} \leq (1-\varepsilon)^{\frac{k}{2 \cdot 10^4 m}},$$

where the last inequality holds by choosing the constant λ' of the claim to be large enough such that $k \geq \lambda' \cdot m^2$ implies it.

The case $j \in [m+1]$: In this case, it holds that

$$P_{Z^k X_{<j}^k}\left[\left|\mathcal{G}_{Z^k X_{<j}^k}\right| \geq k/10 \wedge P_{X_{j+1}^k \mid Z^k X_{<j}^k}\left[\left|\delta_j(X_{j+1}^k; Z^k X_{<j}^k)\right| > 0.5\right] > \frac{m}{k^2}\right] > 0 \qquad (80)$$

In particular, there exists $z^k x_{<j}^k \in \mathrm{Supp}(P_{Z^k X_{<j}^k})$ that satisfy both conditions. In the following, fix such $z^k x_{<j}^k$. Recall that

$$\left(1 + \delta_j(x_{j+1}^k; z^k x_{<j}^k)\right) \cdot \sum_{i \in \mathcal{G}_{z^k x_{<j}^k}} \alpha_{j,i} = \sum_{i \in \mathcal{G}_{z^k x_{<j}^k} \bigcap 1_{x_{j+1}^k}} \frac{\alpha_{j,i}}{P_{X_{j+1,i} \mid Z^k X_{<j}^k}(1 \mid z^k x_{<j}^k)}$$

where $\alpha_{j,i} = \alpha_{j,i}(z^k x^k_{<j})$ is according to Table 1. Therefore, it holds that

$$\begin{aligned}
&\Pr_{x^k_{j+1}\sim P_{X^k_{j+1}|Z^kX^k_{<j}}(\cdot|z^kx^k_{<j})}\left[\left|\delta_j(x^k_{j+1};z^kx^k_{<j})\right| > \frac{1}{2}\right] \\
&= \Pr_{x^k_{j+1}\sim P_{X^k_{j+1}|Z^kX^k_{<j}}(\cdot|z^kx^k_{<j})}\left[\sum_{i\in\mathcal{S}\bigcap 1_{x^k_{j+1}}}\frac{\alpha_i}{p_i} \notin (1\pm 0.5)\sum_{i\in\mathcal{S}}\alpha_i\right] \\
&> \frac{m}{k^2}
\end{aligned} \tag{81}$$

where we denote $\mathcal{S} = \mathcal{G}_{z^kx^k_{<j}}$ (recall that $|\mathcal{S}| \geq k/10$), $\alpha_i = \alpha_{j,i}(z^kx^k_{<j}) \in [0.01, 10]$ and $p_i = P_{X_{j+1,i}|Z^kX^k_{<j}}(1|z^kx^k_{<j}) \in (1\pm 0.1)\cdot\frac{1}{m}(1-\frac{1}{m})$. Observe that when taking $x^k_{j+1} \sim R_{X^k_{j+1}|Z^kX^k_{<j}}(\cdot|z^kx^k_{<j})$ (i.e., without the conditioning on W), the term $\sum_{i\in\mathcal{S}\bigcap 1_{x^k_{j+1}}}\frac{\alpha_i}{p_i}$ is a sum of $|\mathcal{S}| \geq k/10$ independent random variables, where the element that corresponds to $i \in \mathcal{S}$ is distributed according to $b_i \cdot \text{Bern}(\frac{1}{m}(1-\frac{1}{m}))$ for $b_i = \frac{\alpha_i}{p_i} \in \frac{1}{1\pm 0.1}\cdot\frac{\alpha_i}{\frac{1}{m}(1-\frac{1}{m})}$. Therefore,

$$\mathrm{E}_{x^k_{j+1}\sim R_{X^k_{j+1}|Z^kX^k_{<j}}(\cdot|z^kx^k_{<j})}\left[\sum_{i\in\mathcal{S}\bigcap 1_{x^k_{j+1}}}\frac{\alpha_i}{p_i}\right] \in \frac{1}{1\pm 0.1}\cdot\sum_{i\in\mathcal{S}}\alpha_i \subseteq (0.9, 1.15)\cdot\sum_{i\in\mathcal{S}}\alpha_i \tag{82}$$

and it holds that

$$\begin{aligned}
&\Pr_{x^k_{j+1}\sim R_{X^k_{j+1}|Z^kX^k_{<j}}(\cdot|z^kx^k_{<j})}\left[\left|\delta_j(x^k_{j+1};z^kx^k_{<j})\right| > 0.5\right] \\
&= \Pr_{x^k_{j+1}\sim R_{X^k_{j+1}|Z^kX^k_{<j}}(\cdot|z^kx^k_{<j})}\left[\left|\sum_{i\in\mathcal{S}\bigcap 1_{x^k_{j+1}}}\frac{\alpha_i}{p_i}\right| \notin (1\pm 0.5)\cdot\sum_{i\in\mathcal{S}}\alpha_i\right] \\
&\leq \Pr_{x^k_{j+1}\sim R_{X^k_{j+1}|Z^kX^k_{<j}}(\cdot|z^kx^k_{<j})}\left[\left|\sum_{i\in\mathcal{S}\bigcap 1_{x^k_{j+1}}}\frac{\alpha_i}{p_i} - \mathrm{E}_{x^k_{j+1}\sim R_{X^k_{j+1}|Z^kX^k_{<j}}(\cdot|z^kx^k_{<j})}\left[\sum_{i\in\mathcal{S}\bigcap 1_{x^k_{j+1}}}\frac{\alpha_i}{p_i}\right]\right| > 0.35\cdot\sum_{i\in\mathcal{S}}\alpha_i\right] \\
&\leq 2\exp\left(-\frac{0.35^2\cdot(\sum_{i\in\mathcal{S}}\alpha_i)^2}{2\left(\sum_{i\in\mathcal{S}}\frac{\alpha_i^2}{p_i^2}\cdot\frac{1}{m}(1-\frac{1}{m}) + 0.1\cdot\max_{i\in\mathcal{S}}\{\frac{\alpha_i}{p_i}\}\cdot\sum_{i\in\mathcal{S}}\alpha_i\right)}\right) \\
&\leq 2\exp\left(-\frac{0.35^2\cdot(\sum_{i\in\mathcal{S}}\alpha_i)^2}{2\left(300m\cdot\sum_{i\in\mathcal{S}}\alpha_i + 30m\cdot\sum_{i\in\mathcal{S}}\alpha_i\right)}\right) \\
&\leq 2\exp\left(-\frac{k}{6\cdot 10^6 m}\right),
\end{aligned} \tag{83}$$

where the first inequality holds by Equation (82), the second one holds by Fact 3.16 and the last one holds since $\sum_{i\in\mathcal{S}}\alpha_i \geq 0.01\cdot|S| \geq k/10^3$.

Finally, by Equations (81) and (83), we conclude that

$$R[W] \leq \frac{\Pr_{x_{j+1}^k \sim R_{X_{j+1}^k | Z^k X_{<j}^k}(\cdot | z^k x_{<j}^k)}\left[\left|\delta_j(x_{j+1}^k; z^k x_{<j}^k)\right| > 0.5\right]}{\Pr_{x_{j+1}^k \sim P_{X_{j+1}^k | Z^k X_{<j}^k}(\cdot | z^k x_{<j}^k)}\left[\left|\delta_j(x_{j+1}^k; z^k x_{<j}^k)\right| > 0.5\right]} \leq \frac{2\exp\left(-\frac{k}{6 \cdot 10^6 m}\right)}{m/k^2} \leq (1-\varepsilon)^{\frac{k}{10^7 m}},$$

where the last inequality holds by choosing the constant λ' of the claim to be large enough such that $k \geq \lambda' \cdot m^2$ implies it (recall that $\varepsilon \in [0, \frac{1}{2}]$). □

As a simple corollary of Claim 7.9, if k and $R[W]$ are large enough, then the probability of failure (over $\widehat{P}$) in the "expected current" bits is low.

Corollary 7.10. *For any constant $\lambda > 0$ there exists constants $\lambda', \lambda'' > 0$ such that if $\widehat{P}_{B_0^{\text{exp\_cur}}, \ldots, B_{m+1}^{\text{exp\_cur}}}(1^{m+2}) \leq 1 - \varepsilon/\lambda$ and $k \geq \lambda' \cdot m^2/\varepsilon$, then $R[W] \leq (1-\varepsilon)^{\frac{k}{\lambda'' \cdot m}}$.*

Proof. Assume that $\widehat{P}_{B_0^{\text{exp\_cur}}, \ldots, B_{m+1}^{\text{exp\_cur}}}(1^{m+2}) \leq 1 - \varepsilon/\lambda$ for some constant $\lambda > 0$. By Claim 7.9, we can focus on the case that $\widehat{P}_{B_0^{\text{exp\_cur}}, \ldots, B_{m+1}^{\text{exp\_cur}} | B_0^{\text{large\_set}}, \ldots, B_{m+1}^{\text{large\_set}}}(1^{m+2} | 1^{m+2}) = 1$. Note that

$$\widehat{P}_{B_0^{\text{large\_set}}, \ldots, B_{m+1}^{\text{large\_set}}}(1^{m+2}) \leq \frac{\widehat{P}_{B_0^{\text{exp\_cur}}, \ldots, B_{m+1}^{\text{exp\_cur}}}(1^{m+2})}{\widehat{P}_{B_0^{\text{exp\_cur}}, \ldots, B_{m+1}^{\text{exp\_cur}} | B_0^{\text{large\_set}}, \ldots, B_{m+1}^{\text{large\_set}}}(1^{m+2} | 1^{m+2})} \leq 1 - \varepsilon/\lambda$$

Therefore, the proof follows by Corollary 7.5. □

The above yields that the probability of failure in the "current" bits is also low.

Corollary 7.11. *For any constant $\lambda > 0$ there exists constants $\lambda', \lambda'' > 0$ such that if $\widehat{P}_{B_0^{\text{cur}}, \ldots, B_{m+1}^{\text{cur}}}(1^{m+2}) \leq 1 - \varepsilon/\lambda$ and $k \geq \lambda' \cdot m^2/\varepsilon$, then $R[W] \leq (1-\varepsilon)^{\frac{k}{\lambda'' \cdot m}}$.*

Proof. Assume that $\widehat{P}_{B_0^{\text{cur}}, \ldots, B_{m+1}^{\text{cur}}}(1^{m+2}) \leq 1 - \varepsilon/\lambda$ for some constant $\lambda > 0$. Note that

$$\begin{aligned}
\widehat{P}_{B_0^{\text{exp\_cur}}, \ldots, B_{m+1}^{\text{exp\_cur}}}(1^{m+2}) &\leq \frac{\widehat{P}_{B_0^{\text{cur}}, \ldots, B_{m+1}^{\text{cur}}}(1^{m+2})}{\widehat{P}_{B_0^{\text{cur}}, \ldots, B_{m+1}^{\text{cur}} | B_0^{\text{exp\_cur}}, \ldots, B_{m+1}^{\text{exp\_cur}}}(1^{m+2} | 1^{m+2})} \\
&\leq \frac{1 - \varepsilon/\lambda}{1 - (m+2) \cdot \frac{m}{k^2}} \\
&\leq 1 - \frac{\varepsilon}{2\lambda},
\end{aligned}$$

where the last inequality holds by choosing the constant λ' of the corollary to be large enough such that $k \geq \lambda' \cdot m^2/\varepsilon$ implies it. The proof then follows by Corollary 7.10. □

As a corollary of Corollaries 7.5 and 7.10, if k and $R[W]$ are large enough, then the probability of failure (over $\widehat{P}$) in the "history" bits is low.

Corollary 7.12. *For any constant $\lambda > 0$ there exists constants $\lambda', \lambda'' > 0$ such that if $\widehat{P}_{B_0^{\text{hist}}, \ldots, B_{m+1}^{\text{hist}}}(1^{m+2}) \leq 1 - \varepsilon/\lambda$ and $k \geq \lambda' \cdot m^2/\varepsilon$, then $R[W] \leq (1-\varepsilon)^{\frac{k}{\lambda'' \cdot m}}$.*

Proof. Immediately follows by Corollaries 7.5 and 7.10 since $B_j^{\text{hist}} = B_j^{\text{large\_set}} \cdot B_j^{\text{exp\_cur}}$. □

7.2.4 Putting It Together

The proof of Lemma 5.13 is now trivially holds by the previous sections.

Lemma 7.13 (Restatement of Lemma 5.13)**.** *For any constant $\lambda > 0$ there exist constants $\lambda', \lambda'' > 0$ such that the following holds: Let $k, m, \ell \in \mathbb{N}$, let $\varepsilon \in (0, 1/2]$, let $\mathcal{W} \subseteq \{0,1\}^{kl+k(m+1)}$ be a termination-consistent set (according to Definition 4.3) and let W, R and $\widehat{P}$ be the event and distributions from Definitions 5.1 and 5.8 respectively, for the above $k, m, \ell, \mathcal{W}$. Assume $k \geq \lambda' \cdot m^2/\varepsilon$ and $R[W] \geq (1-\varepsilon)^{\frac{k}{\lambda'' \cdot m}}$, then $\widehat{P}_{B^{m+2}}(1^{m+2}) \geq 1 - \varepsilon/\lambda$.*

Proof. Let $k, m, \ell, \varepsilon, \mathcal{W}, W, R, \widehat{P}$ as in Lemma 5.13 and assume that $\widehat{P}_{B^{m+2}}(1^{m+2}) < 1 - \varepsilon/\lambda$ for some constant $\lambda > 0$. Since $B_j = B_j^{\mathrm{cur}} \cdot B_j^{\mathrm{hist}} \cdot B_j^{\mathrm{indx}}$, at least one of the following must hold:

1. $\widehat{P}_{B_0^{\mathrm{cur}}, \ldots, B_{m+1}^{\mathrm{cur}}}(1^{m+2}) < 1 - \frac{\varepsilon}{3\lambda}$, or
2. $\widehat{P}_{B_0^{\mathrm{hist}}, \ldots, B_{m+1}^{\mathrm{hist}}}(1^{m+2}) < 1 - \frac{\varepsilon}{3\lambda}$, or
3. $\widehat{P}_{B_0^{\mathrm{indx}}, \ldots, B_{m+1}^{\mathrm{indx}}}(1^{m+2}) < 1 - \frac{\varepsilon}{3\lambda}$.

The proof then immediately follows by Corollaries 7.8, 7.11 and 7.12. □

7.3 Proving Lemma 7.2

In this section, we prove Lemma 7.2, restated for convenience below.

Lemma 7.2. *[Bounding the number of bad columns in P] For any constant $\lambda > 0$, there exists a constant $\lambda' > 0$ such that the following holds: let $k, m, \ell, \mathcal{W}, \varepsilon$ be as in Lemma 5.13, let P be the distribution from Definition 4.7, let $\mathcal{G}, \mathcal{D}$ be the sets from Table 2 and let* jumps *be the function from Table 5. Assume that at least one of the following holds:*

1. *$|\mathcal{D}| \leq (1 - \varepsilon/\lambda)k \cdot 2^\ell$, or*
2. *$\mathrm{E}_P\left[\mathrm{jumps}(Z^k X^{(m+1)\times k})\right] \geq \varepsilon k/\lambda$,*

then $R[W] \leq (1-\varepsilon)^{\frac{k}{\lambda' \cdot m}}$.

In the following, fix $k, m, \ell, \varepsilon, \mathcal{W}, W, R, P, \mathcal{G}, \mathcal{D}$ as in Lemma 7.2, and let $\mathrm{jumps}^\gamma, \mathrm{jumps}^\rho, \mathrm{jumps}^\alpha$ the function from Table 5. The main components of Lemma 7.2's proof are divided into Claims 7.14 to 7.16, proven separately in Sections 7.3.1 to 7.3.3, respectively.

Claim 7.14. *For any constant $\lambda > 0$ there exists a constant $\lambda' > 0$ such that if $|\mathcal{D}| \leq (1-\varepsilon/\lambda)k \cdot 2^\ell$, then $R[W] \leq (1-\varepsilon)^{\frac{k}{\lambda' \cdot m}}$.*

Claim 7.15. *For any constant $\lambda > 0$ there exists a constants $\lambda' > 0$ such that if $\mathrm{E}_P\left[\mathrm{jumps}^\nu(Z^k X^{(m+1)\times k})\right] \geq \varepsilon k/\lambda$ for some $\nu \in \{\gamma, \rho\}$, then $R[W] \leq (1-\varepsilon)^{\frac{k}{\lambda' \cdot m}}$.*

Claim 7.16. *For any constant $\lambda > 0$, there exists a constant $\lambda' > 0$ such that if $\mathrm{E}_P\left[\mathrm{jumps}^\alpha(Z^k X^{(m+1)\times k})\right] \geq \varepsilon k/\lambda$, then $R[W] \leq (1-\varepsilon)^{\frac{k}{\lambda' \cdot m}}$.*

The proof of Lemma 7.2 now trivially follows by Claims 7.14 to 7.16.

Proof of Lemma 7.2. Let $k, m, \ell, \varepsilon, \mathcal{W}, W, R, P$ as in Lemma 7.2 and assume that at least one of the following holds for some constant $\lambda > 0$:

1. $|\mathcal{D}| \leq (1 - \varepsilon/\lambda)k \cdot 2^{\ell}$, or
2. $\mathrm{E}_P\left[\mathrm{jumps}(Z^k X^{(m+1)\times k})\right] \geq \varepsilon k/\lambda$,

If Item 1 holds then the proof follows by Claim 7.14. Note that by definition of jumps, it holds that $\mathrm{jumps}(\tau_j) \leq \sum_{\nu \in \{\gamma,\rho,\alpha\}} \mathrm{jumps}^{\nu}(\tau_j)$ for any input τ_j. Therefore, if Item 2 holds then there exists $\nu \in \{\gamma, \rho, \alpha\}$ such that $\mathrm{E}_P\left[\mathrm{jumps}^{\nu}(Z^k X^{(m+1)\times k})\right] \geq \frac{\varepsilon k}{3\lambda}$. If the above holds for $\nu \in \{\gamma, \rho\}$, then the proof follows by Claim 7.15, and if it holds for $\nu = \alpha$, then the proof follows by Claim 7.16. □

7.3.1 Proving Claim 7.14

Before proving Claim 7.14, we start with a simple claim that connects the $\{\rho_{0,i}\}$'s measurements with $R[W]$.

Claim 7.17. *It holds that*

$$\log \frac{1}{R[W]} \geq \frac{1}{4m} \cdot \sum_{i=1}^{k} \min\{|\rho_{0,i}|, \rho_{0,i}^2\}$$

Proof. Compute

$$\begin{aligned}
\log \frac{1}{R[W]} &\geq D\left(P_{X_1^k} || R_{X_1^k}\right) = D\left(P_{X_1^k} || \prod_{i=1}^{k} R_{X_{1,i}}\right) \\
&\geq \sum_{i=1}^{k} D\left(P_{X_{1,i}} || R_{X_{1,i}}\right) = \sum_{i=1}^{k} D\left(\frac{1+\rho_{0,i}}{m} || \frac{1}{m}\right) \\
&\geq \frac{1}{4m} \cdot \sum_{i=1}^{k} \min\{|\rho_{0,i}|, \rho_{0,i}^2\},
\end{aligned}$$

where the first inequality holds by Fact 3.6, the second one holds by Fact 3.5 (the product case of chain rule) and the last one by Fact 3.9. □

As a corollary of Claim 7.17, we obtain a lower bound on $|\mathcal{G}|$ in case $R[W]$ is high enough.

Corollary 7.18. *For any constant $\lambda > 0$ there exists a constant $\lambda' > 0$ such that if $|\mathcal{G}| \leq (1-\varepsilon/\lambda)k$, then $R[W] \leq (1-\varepsilon)^{\frac{k}{\lambda' \cdot m}}$.*

Proof. Assume that $|\mathcal{G}| \leq (1 - \varepsilon/\lambda)k$ for some constant $\lambda > 0$. Then it holds that

$$\begin{aligned}
\log \frac{1}{R[W]} &\geq \frac{1}{4m} \cdot \sum_{i=1}^{k} \min\{|\rho_{0,i}|, \rho_{0,i}^2\} \\
&\geq \frac{1}{4m} \cdot \sum_{i \in [k] \setminus \mathcal{G}} \min\{|\rho_{0,i}|, \rho_{0,i}^2\} \\
&\geq \frac{0.01 \cdot (k - |\mathcal{G}|)}{4m} \geq \frac{\varepsilon k}{400 \cdot m}
\end{aligned}$$

$$\implies R[W] \le e^{-\frac{\varepsilon k}{400\cdot m}} \le (1-\varepsilon)^{\frac{\varepsilon k}{800\cdot m}},$$

where the first inequality holds by Claim 7.17 and the third one holds since $i \notin \mathcal{G} \implies |\rho_{0,i}| > 0.1$. $\square$

The last claim we need in order to prove Claim 7.14 gives a lower bound on the average size of the sets $\{\mathcal{Z}_i\}_{i\in[k]}$ (defined in Table 2) in case $R[W]$ is high enough.

Claim 7.19. *For any constants $\lambda > 0$ there exists a constant $\lambda' > 0$ such that if $\mathrm{E}_{i\leftarrow\mathcal{G}}\left[|\mathcal{Z}_i|/2^\ell\right] \le 1-\varepsilon/\lambda$ then $R[W] \le (1-\varepsilon)^{\frac{k}{\lambda'\cdot m}}$.*

Proof. Assume that $\mathrm{E}_{i\leftarrow\mathcal{G}}\left[|\mathcal{Z}_i|/2^\ell\right] \le 1-\varepsilon/\lambda$ for some constant $\lambda > 0$. If $|\mathcal{G}| < k/2$ then the proof immediately follows by Corollary 7.18. Therefore, in the following we assume that $|\mathcal{G}| \ge k/2$. Observe that

$$\begin{aligned}
\log\frac{1}{R[W]} &\ge D\Big(P_{Z^k X_1^k}||R_{Z^k X_1^k}\Big) = D\left(P_{Z^k X_1^k}||\prod_{i=1}^{k} R_{Z_i X_{1,i}}\right)\\
&\ge \sum_{i=1}^{k} D\big(P_{Z_i X_{1,i}}||R_{Z_i X_{1,i}}\big) \ge \sum_{i\in\mathcal{G}} D\big(P_{Z_i X_{1,i}}||R_{Z_i X_{1,i}}\big)\\
&\ge \sum_{i\in\mathcal{G}} \frac{1+\rho_{0,i}}{m}\cdot D\Big(P_{Z_i|X_{1,i}=1}||R_{Z_i}\Big)\\
&\ge \frac{0.9}{m}\cdot\sum_{i\in\mathcal{G}} D\Big(P_{Z_i|X_{1,i}=1}||R_{Z_i}\Big) \qquad (84)
\end{aligned}$$

where the first inequality holds by Fact 3.6 and the second one by Fact 3.5 (the product case of chain rule). In the following, let $\bar{\mathcal{Z}}_i^+ = \{z \in \{0,1\}^\ell : P_{Z_i|X_{1,i}=1}(z) > (1+0.1)\cdot 2^{-\ell}\}$ and $\bar{\mathcal{Z}}_i^- = \{z \in \{0,1\}^\ell : P_{Z_i|X_{1,i}=1}(z) < (1-0.1)\cdot 2^{-\ell}\}$, and observe that $\bar{\mathcal{Z}}_i^+ \bigcup \bar{\mathcal{Z}}_i^- = \{0,1\}^\ell \setminus \mathcal{Z}_i$. Therefore, by assumption it holds that $\mathrm{E}_{i\leftarrow\mathcal{G}}\left[\left|\bar{\mathcal{Z}}_i^+\right|/2^\ell\right] \ge \frac{\varepsilon}{2\lambda}$ or $\mathrm{E}_{i\leftarrow\mathcal{G}}\left[\left|\bar{\mathcal{Z}}_i^-\right|/2^\ell\right] \ge \frac{\varepsilon}{2\lambda}$. If the first bound holds, then by Equation (84) we obtain that

$$\begin{aligned}
\log\frac{1}{R[W]} &\ge \sum_{i\in\mathcal{G}} \frac{0.9}{m}\cdot D\Big(P_{Z_i|X_{1,i}=1}(\bar{\mathcal{Z}}_i^+)||R_{Z_i}(\bar{\mathcal{Z}}_i^+)\Big)\\
&> \sum_{i\in\mathcal{G}} \frac{0.9}{m}\cdot D\Big((1+0.1)\cdot\left|\bar{\mathcal{Z}}_i^+\right|/2^\ell||\left|\bar{\mathcal{Z}}_i^+\right|/2^\ell\Big)\\
&\ge \frac{0.9\cdot 0.1^2}{4m}\cdot\sum_{i\in\mathcal{G}}\left|\bar{\mathcal{Z}}_i^+\right|/2^\ell\\
&= \frac{0.009}{4m}\cdot|\mathcal{G}|\cdot\mathrm{E}_{i\leftarrow\mathcal{G}}\left[\left|\bar{\mathcal{Z}}_i^+\right|/2^\ell\right]\\
&\ge \frac{\varepsilon k}{1800\cdot m}
\end{aligned}$$

$$\implies R[W] \le e^{-\frac{\varepsilon k}{1800\cdot m}} \le (1-\varepsilon)^{\frac{\varepsilon k}{1800\cdot m}},$$

where the first inequality holds from Equation (84) by Fact 3.5 (data-processing), the third one holds by Fact 3.9, the fourth one holds since $|\mathcal{G}| \geq k/2$ and $\mathrm{E}_{i \leftarrow \mathcal{G}}\left[\left|\bar{\mathcal{Z}}_i^+\right|/2^\ell\right] \geq \frac{\varepsilon}{2\lambda}$ and the last one holds since $\varepsilon \in [0, \frac{1}{2}]$. Otherwise, the second bound holds and we obtain that

$$\begin{aligned}
\log \frac{1}{R[W]} &\geq \sum_{i \in \mathcal{G}} \frac{0.9}{m} \cdot D\Big(P_{Z_i|X_{1,i}=1}(\bar{\mathcal{Z}}_i^-)||R_{Z_i}(\bar{\mathcal{Z}}_i^-)\Big) \\
&> \sum_{i \in \mathcal{G}} \frac{0.9}{m} \cdot D\Big((1-0.1) \cdot \left|\bar{\mathcal{Z}}_i^-\right|/2^\ell || \left|\bar{\mathcal{Z}}_i^-\right|/2^\ell\Big) \\
&\geq \frac{0.9 \cdot 0.1^2}{4m} \cdot \sum_{i \in \mathcal{G}} \left|\bar{\mathcal{Z}}_i^-\right|/2^\ell \\
&= \frac{0.009}{4m} \cdot |\mathcal{G}| \cdot \mathrm{E}_{i \leftarrow \mathcal{G}}\Big[\left|\bar{\mathcal{Z}}_i^-\right|/2^\ell\Big] \\
&\geq \frac{\varepsilon k}{1800 \cdot m}
\end{aligned}$$

$$\implies R[W] \leq e^{-\frac{\varepsilon k}{1800 \cdot m}} \leq (1-\varepsilon)^{\frac{\varepsilon k}{3600 \cdot m}}$$

□

The proof of Claim 7.14 now trivially follows by Corollary 7.18 and Claim 7.19.

Claim 7.20 (Restatement of Claim 7.14)**.** *For any constant $\lambda > 0$ there exists a constant $\lambda' > 0$ such that if $|\mathcal{D}| \leq (1-\varepsilon/\lambda)k \cdot 2^\ell$, then $R[W] \leq (1-\varepsilon)^{\frac{k}{\lambda' \cdot m}}$.*

Proof. Assume that $|\mathcal{D}| \leq (1-\varepsilon/\lambda)k \cdot 2^\ell$ for some constant $\lambda > 0$ and recall that $\mathcal{D} = \{(i,z) \in [k] \times \{0,1\}^\ell \colon (i,z) \in \mathcal{G} \times \mathcal{Z}_i\}$. Compute

$$\begin{aligned}
1 - \varepsilon/\lambda &\geq \frac{|\mathcal{D}|}{k \cdot 2^\ell} \\
&= \Pr_{(i,z) \leftarrow [k] \times \{0,1\}^\ell}[(i,z) \in \mathcal{G} \times \mathcal{Z}_i] \\
&= \frac{|\mathcal{G}|}{k} \cdot \mathrm{E}_{i \leftarrow \mathcal{G}}\left[\frac{|\mathcal{Z}_i|}{2^\ell}\right].
\end{aligned}$$

Therefore, it must holds that $\frac{|\mathcal{G}|}{k} \leq 1 - \frac{\varepsilon}{2\lambda}$ or $\mathrm{E}_{i \leftarrow \mathcal{G}}\left[\frac{|\mathcal{Z}_i|}{2^\ell}\right] \leq 1 - \frac{\varepsilon}{2\lambda}$ and we conclude from Corollary 7.18 and Claim 7.19 that $R[W] \leq (1-\varepsilon)^{\frac{k}{\lambda' m}}$ by choosing $\lambda' = \max\{c, c'\}$ where c is the constant $\lambda'(2\lambda)$ of Corollary 7.18 and c' is the constant $\lambda'(2\lambda)$ of Claim 7.19. □

7.3.2 Proving Claim 7.15

Before proving Claim 7.15, we first state and prove some useful facts about the $\{\gamma_{j,i}\}$ and $\{\rho_{j,i}\}$ measurements when drawing $Z^k X^{(m+1) \times k}$ from P (done in Sections 7.3.2 and 7.3.2, respectively), and the proof of Claim 7.15 which follows from these facts is given in Section 7.3.2.

Facts About the $\{\gamma_{j,i}\}$ measurements The following claim connects the jumps in the measurements $\{\gamma_{j,i}\}_{j\in[m+1],i\in[k]}$ (over P) with $R[W]$.

Claim 7.21. *It holds that*

$$\log\frac{1}{R[W]}\geq\frac{1}{4m}\cdot\mathrm{E}_P\left[\sum_{i=1}^{k}\sum_{j=1}^{m+1}\min\{|\gamma_{j,i}|,\gamma_{j,i}^2\}\cdot\mathbb{1}\{1\notin X_{<j,i}\}\right],$$

where $\gamma_{j,i}=\gamma_{j,i}(Z^kX^k_{<j})$.

Proof. Compute

$$\begin{aligned}\log\frac{1}{R[W]}&\geq D(P_{Z^kX^{(m+1)\times k}}||R_{Z^kX^{(m+1)\times k}})\\&\geq\sum_{j=1}^{m+1}\mathrm{E}_{P_{Z^kX^k_{<j}}}\left[D\Big(P_{X^k_j|Z^kX^k_{<j}}||R_{X^k_j|Z^kX^k_{<j}}\Big)\right]\\&=\sum_{j=1}^{m+1}\mathrm{E}_{P_{Z^kX^k_{<j}}}\left[D\left(P_{X^k_j|Z^kX^k_{<j}}||\prod_{i=1}^{k}R_{X_{j,i}|Z^kX^k_{<j}}\right)\right]\\&\geq\sum_{i=1}^{k}\sum_{j=1}^{m+1}\mathrm{E}_{P_{Z^kX^k_{<j}}}\left[D\Big(P_{X_{j,i}|Z^kX^k_{<j}}||R_{X_{j,i}|Z^kX^k_{<j}}\Big)\right]\\&=\sum_{i=1}^{k}\sum_{j=1}^{m+1}\mathrm{E}_{P_{Z^kX^k_{<j}}}\left[D\Big(\frac{1+\gamma_{j,i}}{m}||\frac{1}{m}\Big)\cdot\mathbb{1}\{1\notin X_{<j,i}\}\right]\\&\geq\frac{1}{4m}\cdot\sum_{i=1}^{k}\sum_{j=1}^{m+1}\mathrm{E}_{P_{Z^kX^k_{<j}}}\left[\min\{|\gamma_{j,i}|,\gamma_{j,i}^2\}\cdot\mathbb{1}\{1\notin X_{<j,i}\}\right]\\&=\frac{1}{4m}\cdot\mathrm{E}_P\left[\sum_{i=1}^{k}\sum_{j=1}^{m+1}\min\{|\gamma_{j,i}|,\gamma_{j,i}^2\}\cdot\mathbb{1}\{1\notin X_{<j,i}\}\right],\end{aligned}$$

where the first inequality holds by Fact 3.6, the second one holds by the chain-rule property of KL-Divergence (Fact 3.5(3)), the third one holds by the product case of chain-rule (Fact 3.5(3)) and the last one holds by Fact 3.9. □

As a first corollary of Claim 7.21, we obtain an upper bound on the sum of squares of "small" jumps in the values of $\{\gamma_{j,i}\}_{j\in[m+1],i\in[k]}$ (over P) in case $R[W]$ is high enough.

Corollary 7.22. *For any constant $\lambda>0$ there exists a constant $\lambda'>0$ such that if $\mathrm{E}_P\left[\sum_{i=1}^{k}\sum_{j=1}^{m+1}\gamma_{j,i}^2\cdot\mathbb{1}\{1\notin X_{<j,i}\}\cdot\mathbb{1}\{\gamma_{j,i}\leq 1\}\right]\geq\varepsilon k/\lambda$ for $\gamma_{j,i}=\gamma_{j,i}(Z^kX^k_{<j})$, then $R[W]\leq(1-\varepsilon)^{\frac{k}{\lambda'\cdot m}}$.*

Proof. Immediately follows by Claim 7.21. □

As a second corollary of Claim 7.21, we obtain an upper bound on the sum of "large" jumps in the values of $\{\gamma_{j,i}\}_{j\in[m+1],i\in[k]}$ (over P) in case $R[W]$ is high enough.

Corollary 7.23. *For any constants $\lambda > 0$ and $c \in (0,1)$ there exists a constant $\lambda' > 0$ such that if one of the following holds:*

1. $\mathrm{E}_P\left[\sum_{i=1}^{k}\sum_{j=1}^{m+1}|\gamma_{j,i}| \cdot \mathbb{1}\{1 \notin X_{<j,i}\} \cdot \mathbb{1}\{|\gamma_{j,i}| > c\}\right] \geq \varepsilon k/\lambda$, *or*

2. $\mathrm{E}_P\left[\sum_{i=1}^{k}\mathbb{1}\{u_i^{|\gamma|>c} < \infty\}\right] \geq \varepsilon k/\lambda$,

for $\gamma_{j,i} = \gamma_{j,i}(Z^k X^k_{<j})$ *and* $u_i^{|\gamma|>c} = u_i^{|\gamma|>c}(Z^k X^{(m+1)\times k})$, *then* $R[W] \leq (1-\varepsilon)^{\frac{k}{\lambda' \cdot m}}$.

Proof. If Item 1 holds, the proof follows by Claim 7.21 and by the assumption that $\varepsilon \in [0, \frac{1}{2}]$, since for any $i \in [k]$, $j \in [m+1]$ and $\tau_j = z^k x^k_{<j} \in \mathrm{Supp}(P_{Z^k X^k_{<j}})$ it holds that

$$\min\{|\gamma_{j,i}(\tau_j)|, \gamma_{j,i}(\tau_j)^2\} \cdot \mathbb{1}\{1 \notin X_{<j,i}\} \geq c \cdot |\gamma_{j,i}(\tau_j)| \cdot \mathbb{1}\{1 \notin X_{<j,i}\} \cdot \mathbb{1}\{|\gamma_{j,i}(\tau_j)| > c\}$$

If Item 2 holds, the proof follows by Item 1 since for any $z^k x^{(m+1)\times k} \in \mathrm{Supp}(P)$ it holds that

$$\begin{aligned}
\mathbb{1}\{u_i^{|\gamma|>c}(z^k x^{(m+1)\times k}) < \infty\} &= \sum_{j=1}^{m+1} \mathbb{1}\{u_i^{|\gamma|>c}(z^k x^k_{<j}) = j\} \\
&\leq \frac{1}{c} \cdot \sum_{j=1}^{m+1} \left|\gamma_{j,i}(z^k x^k_{<j})\right| \cdot \mathbb{1}\{u_i^{|\gamma|>c}(z^k x^k_{<j}) = j\} \\
&\leq \frac{1}{c} \cdot \sum_{j=1}^{m+1} \left|\gamma_{j,i}(z^k x^k_{<j})\right| \cdot \mathbb{1}\{1 \notin X_{<j,i}\} \cdot \mathbb{1}\{\left|\gamma_{j,i}(z^k x^k_{<j})\right| > c\}
\end{aligned}$$

□

As a trivial corollary of Corollary 7.23, we now prove Claim 7.6.

Corollary 7.24 (restatement of Claim 7.6)**.** *For any constant $\lambda > 0$ there exists a constant $\lambda' > 0$ such that if $\mathrm{E}_P\left[\sum_{i=1}^{k}\sum_{j=1}^{m+1}\gamma_{j,i} \cdot \mathbb{1}\{\gamma_{j,i} > 1\}\right] \geq \varepsilon k/\lambda$ for $\gamma_{j,i} = \gamma_{j,i}(Z^k X^{(m+1)\times k})$, then $R[W] \leq (1-\varepsilon)^{\frac{k}{\lambda' \cdot m}}$.*

Proof. Immediately follows by Corollary 7.23(1) with respect to $c = 1$. □

Facts About the $\{\rho_{j,i}\}$ measurements The following claim connects the jumps in the measurements $\{\rho_{j,i}\}_{j\in[m+1],i\in[k]}$ (over P) with $R[W]$.

Claim 7.25. *It holds that*

$$\log\frac{1}{R[W]} \geq \frac{1}{4m}(1 - \frac{1}{m}) \cdot \max\{S_{even}, S_{odd}\},$$

where $S_\nu := \mathrm{E}_P\left[\sum_{i=1}^{k}\sum_{j\in[m+1]\bigcap\mathbb{N}_\nu}\min\{|\rho_{j,i}|, \rho_{j,i}^2\} \cdot \mathbb{1}\{1 \notin X_{<j,i}\}\right]$ *for* $\nu \in \{even, odd\}$ *and* $\rho_{j,i} = \rho_{j,i}(Z^k X^k_{<j})$.

Proof. Fix $\nu \in \{even, odd\}$ and compute

$$\begin{aligned}
\log \frac{1}{R[W]} &\geq D(P_{Z^k X^{(m+1)\times k}} || R_{Z^k X^{(m+1)\times k}}) \\
&\geq \sum_{j \in [m+1] \cap \mathbb{N}_\nu} \mathrm{E}_{P_{Z^k X^k_{<j}}} \left[D\Big(P_{X^k_j X^k_{j+1} | Z^k X^k_{<j}} || R_{X^k_j X^k_{j+1} | Z^k X^k_{<j}} \Big) \right] \\
&\geq \sum_{j \in [m+1] \cap \mathbb{N}_\nu} \mathrm{E}_{P_{Z^k X^k_{<j}}} \left[D\Big(P_{X^k_{j+1} | Z^k X^k_{<j}} || R_{X^k_{j+1} | Z^k X^k_{<j}} \Big) \right] \\
&= \sum_{j \in [m+1] \cap \mathbb{N}_\nu} \mathrm{E}_{P_{Z^k X^k_{<j}}} \left[D\left(P_{X^k_{j+1} | Z^k X^k_{<j}} || \prod_{i=1}^{k} R_{X_{j+1,i} | Z^k X^k_{<j}} \right) \right] \\
&\geq \sum_{i=1}^{k} \sum_{j \in [m+1] \cap \mathbb{N}_\nu} \mathrm{E}_{P_{Z^k X^k_{<j}}} \left[D\Big(P_{X_{j+1,i} | Z^k X^k_{<j}} || R_{X_{j+1,i} | Z^k X^k_{<j}} \Big) \right] \\
&= \sum_{i=1}^{k} \sum_{j \in [m+1] \cap \mathbb{N}_\nu} \mathrm{E}_{P_{Z^k X^k_{<j}}} \left[D\left(\frac{1+\rho_{j,i}}{m}(1-\frac{1}{m}) || \frac{1}{m}(1-\frac{1}{m}) \right) \cdot \mathbb{1}\{1 \notin X_{<j,i}\} \right] \\
&\geq \sum_{i=1}^{k} \sum_{j \in [m+1] \bigcap \mathbb{N}_\nu} \mathrm{E}_{P_{Z^k X^k_{<j}}} \left[\frac{1}{4m}(1-\frac{1}{m}) \cdot \min\{|\rho_{j,i}|, \rho^2_{j,i}\} \cdot \mathbb{1}\{1 \notin X_{<j,i}\} \right] \\
&= \frac{1}{4m}(1-\frac{1}{m}) \cdot S_\nu,
\end{aligned}$$

where the first inequality holds by Fact 3.6, the second one holds by the chain-rule property of KL-Divergence (Fact 3.5(3)), the fourth holds by the product case of chain-rule (Fact 3.5(3)) and the last one holds by Fact 3.9. □

As a first corollary of Claim 7.25, we obtain an upper bound on the sum of squares of "small" jumps in the values of $\{\rho_{j,i}\}_{j \in [m+1], i \in [k]}$ (over P) in case $R[W]$ is high enough.

Corollary 7.26. *For any constant $\lambda > 0$ there exists a constant $\lambda' > 0$ such that if $\mathrm{E}_P\left[\sum_{i=1}^{k}\sum_{j=1}^{m+1} \rho^2_{j,i} \cdot \mathbb{1}\{1 \notin X_{<j,i}\} \cdot \mathbb{1}\{\rho_{j,i} \leq 1\}\right] \geq \varepsilon k/\lambda$ for $\rho_{j,i} = \rho_{j,i}(Z^k X^k_{<j})$, then $R[W] \leq (1-\varepsilon)^{\frac{k}{\lambda' \cdot m}}$.*

Proof. Assume that $\mathrm{E}_P\left[\sum_{i=1}^{k}\sum_{j=1}^{m+1} \rho^2_{j,i} \cdot \mathbb{1}\{1 \notin X_{<j,i}\} \cdot \mathbb{1}\{\rho_{j,i} \leq 1\}\right] \geq \varepsilon k/\lambda$ for some constant $\lambda > 0$. Since for any $i \in [k]$, $j \in [m+1]$ and $\tau_j = z^k x^k_{<j} \in \mathrm{Supp}(P_{Z^k X^k_{<j}})$ it holds that

$$\min\{|\rho_{j,i}(\tau_j)|, \rho^2_{j,i}(\tau_j)\} \cdot \mathbb{1}\{1 \notin X_{<j,i}\} \geq \rho^2_{j,i}(\tau_j) \cdot \mathbb{1}\{1 \notin X_{<j,i}\} \cdot \mathbb{1}\{\rho_{j,i}(\tau_j) \leq 1\},$$

our assumption yields that there exists $\nu \in \{even, odd\}$ such that $S_\nu := \mathrm{E}_P\left[\sum_{i=1}^{k}\sum_{j \in [m+1] \bigcap \mathbb{N}_\nu} \min\{|\rho_{j,i}|, \rho^2_{j,i}\} \cdot \mathbb{1}\{1 \notin X_{<j,i}\}\right] \geq \frac{\varepsilon k}{2\lambda}$. The proof then immediately follows by Claim 7.25 and by the assumption that $\varepsilon \in [0, \frac{1}{2}]$. □

As a second corollary of Claim 7.25, we obtain an upper bound on the sum of "large" jumps in the values of $\{\rho_{j,i}\}_{j \in [m+1], i \in [k]}$ (over P) in case $R[W]$ is high enough.

Corollary 7.27. *For any constants $\lambda > 0$ and $c \in (0,1)$ there exists a constant $\lambda' > 0$ such that if one of the following holds:*

1. $\sum_{i=1}^{k}\sum_{j=1}^{m+1} \mathrm{E}_{P_{Z^k X^k_{<j}}}[|\rho_{j,i}| \cdot \mathbb{1}\{1 \notin X_{<j,i}\} \cdot \mathbb{1}\{|\rho_{j,i}| > c\}] \geq \varepsilon k/\lambda$*, or*

2. $\mathrm{E}_{P_{Z^k X^{(m+1)\times k}}}\left[\sum_{i=1}^{k} \mathbb{1}\{u_i^{|\rho|>c} < \infty\}\right] \geq \varepsilon k/\lambda$*,*

for $\rho_{j,i} = \rho_{j,i}(Z^k X^k_{<j})$ and $u_i^{|\rho|>c} = u_i^{|\rho|>c}(Z^k X^{m\times k})$, then $R[W] \leq (1-\varepsilon)^{\frac{k}{\lambda' \cdot m}}$.

Proof. If Item 1 holds, then there exists $\nu \in \{even, odd\}$ with

$$\sum_{i=1}^{k}\sum_{j\in[m+1]\bigcap \mathbb{N}_\nu} \mathrm{E}_{P_{Z^k X^k_{<j}}}[|\rho_{j,i}| \cdot \mathbb{1}\{1 \notin X_{<j,i}\} \cdot \mathbb{1}\{|\rho_{j,i}| > c\}] \geq \frac{\varepsilon k}{2\lambda},$$

and the proof follows by Claim 7.25 and by the assumption that $\varepsilon \in [0, \frac{1}{2}]$, since for any $i \in [k]$, $j \in [m+1]$ and $\tau_j \in \mathrm{Supp}(P_{Z^k X^k_{<j}})$ it holds that

$$\min\{|\rho_{j,i}(\tau_j)|, \rho_{j,i}^2(\tau_j)\} \cdot \mathbb{1}\{1 \notin X_{<j,i}\} \geq c \cdot |\rho_{j,i}(\tau_j)| \cdot \mathbb{1}\{1 \notin X_{<j,i}\} \cdot \mathbb{1}\{|\rho_{j,i}(\tau_j)| > c\}.$$

If Item 2 holds, then the proof follows by Item 1 since for any $z^k x^{(m+1)\times k} \in \mathrm{Supp}(P)$ it holds that

$$\begin{aligned}
\mathbb{1}\{u_i^{|\rho|>c}(z^k x^{(m+1)\times k}) < \infty\} &= \sum_{j=1}^{m+1} \mathbb{1}\{u_i^{|\rho|>c}(z^k x^k_{<j}) = j\} \\
&\leq \frac{1}{c} \cdot \sum_{j=1}^{m+1} \left|\rho_{j,i}(z^k x^k_{<j})\right| \cdot \mathbb{1}\{u_i^{|\rho|>c}(z^k x^k_{<j}) = j\} \\
&\leq \frac{1}{c} \cdot \sum_{j=1}^{m+1} \left|\rho_{j,i}(z^k x^k_{<j})\right| \cdot \mathbb{1}\{1 \notin X_{<j,i}\} \cdot \mathbb{1}\{\left|\rho_{j,i}(z^k x^k_{<j})\right| > c\}
\end{aligned}$$

□

Putting it Together We are finally ready to prove Claim 7.15

Claim 7.28 (Restatement of Claim 7.15)**.** *For any constant $\lambda > 0$ there exists a constants $\lambda' > 0$ such that if $\mathrm{E}_P\left[\mathrm{jumps}^\nu(Z^k X^{(m+1)\times k})\right] \geq \varepsilon k/\lambda$ for some $\nu \in \{\gamma, \rho\}$, then $R[W] \leq (1-\varepsilon)^{\frac{k}{\lambda' \cdot m}}$.*

Proof. Recall that $\mathrm{jumps}^\nu(\tau) = \sum_{i=1}^{k} \mathbb{1}\{u_i^{|\nu|>0.1}(\tau) < \infty\}$, for any $\nu \in \{\gamma, \rho\}$ and $\tau \in \mathrm{Supp}(P)$. Therefore the proof immediately follows by Corollary 7.23(2) and Corollary 7.27(2). □

7.3.3 Proving Claim 7.16

In this section we prove Claim 7.16, restated for convenience below.

Claim 7.29 (Restatement of Claim 7.16)**.** *For any constant $\lambda > 0$, there exists a constant $\lambda' > 0$ such that if $\mathrm{E}_P\left[\mathrm{jumps}^\alpha(Z^k X^{(m+1)\times k})\right] \geq \varepsilon k/\lambda$, then $R[W] \leq (1-\varepsilon)^{\frac{k}{\lambda' \cdot m}}$.*

Proving Claim 7.16 is the most challenging part in the proof of Lemma 7.2. Unlike the $\{\gamma_{j,i}\}$ and $\{\rho_{j,i}\}$ measurements which are directly connected to $R[W]$ (as we proved in Claims 7.21 and 7.25), the connection between the $\{\alpha_{j,i}\}$ measurements and $R[W]$ is less clear. Recall that the values $\{\alpha_{j,i}\}$ comes from the change in the distribution of I in Q given a history $Z^k X^k_{<j}$, as stated in Claim 5.4:

$$Q_{I|Z^k X^k_{<j}, I \in \mathcal{G}_\tau}(i|z^k x^k_{<j}) = \frac{\alpha_{j,i}(z^k x^k_{<j})}{\sum_{i' \in \mathcal{G}_\tau} \alpha_{j,i'}(z^k x^k_{<j})}.$$

Proving Claim 7.16 requires a very deep understanding of these measurements, and therefore, we start by presenting the high level plan of this complicated part.

High-Level Plan The goal of this section is to understand the distribution of $Q_{I|Z^k X^k_{<j}}$ for every $j \in [m+1]$ when $Z^k X^k_{<j}$ is drawn from $P_{Z^k X^k_{<j}}$. The main idea for proving Claim 7.16 is to show that in expectation (over P), the distributions $\{Q_{I|Z^k X^k_{<j}}\}_{j=1}^{m+1}$ might behave badly over a small set of columns (i.e., columns $i \in [k]$ which has large "jumps" in their $\alpha_{j,i}$ value for some $j \in [m+1]$), but conditioned on the event that I is not in the "bad" set, it remains close to uniform over the "good" columns. Informally, Claim 7.16 states that in expectation over P, $(1 - o(\varepsilon))k$ of the columns $i \in [k]$ are "good" which means that they have $\alpha_{j,i} \in [0.01, 10]$ for all $j \in [m+1]$. Intuitively, this means that by taking uniformly $I \leftarrow [k]$ at the beginning (as done in Q), we hit a potential "bad" column only with probability $o(\varepsilon)$, and conditioned on hitting the "good" set, the distribution of $Q_{I|Z^k X^k_{<j}}$ remains "close enough" to uniform over the "good" set of columns (Claim 5.4). Now, recall that

$$\alpha_{j,i} = \frac{R_{Z_i}(z_i)}{P_{Z_i}(z_i)} \cdot \frac{P_{X_{1,i}|Z^k}(1|z^k)}{P_{X_{1,i}|Z_i}(1|z_i)} \cdot \prod_{j'=2}^{j} \Big(1 + \beta_{j',i}(z^k x^k_{<j'})\Big). \tag{85}$$

In Section 7.3.3 we handle the first two terms of (85) which captures the effect of choosing $z^k \sim P_{Z^k}$ on the distribution $Q_{I|Z^k = z^k}$. This is done by showing (using standard arguments) that if $R[W]$ is high enough, then in expectation (over $z^k \sim P_{Z^k}$), most columns $i \in [k]$ (all but $o(\varepsilon k)$) have $\frac{R_{Z_i}(z_i)}{P_{Z_i}(z_i)} \approx 1$ and $\frac{P_{X_{1,i}|Z^k}(1|z^k)}{P_{X_{1,i}|Z_i}(1|z_i)} \approx 1$. In Section 7.3.3 we handle the complex part of the proof by showing that if $R[W]$ is high enough, then in expectation (over $z^k x^{(m+1)\times k} \sim P$), most active columns $i \in [k]$ (all but $o(\varepsilon k)$) have values $\{\prod_{j'=2}^{j}(1 + \beta_{j',i})\}_{j \in [m+1]}$ bounded between two constants (inside the interval $[0.01, 10]$), where the above product captures the effect of choosing $x^k_{<j} \sim P_{X^k_{<j}|Z^k = z^k}$ on $Q_{I|(Z^k X^k_{<j}) = z^k x^k_{<j}}$ for any fixing of z^k. We now focus on giving the high level parts of the ideas in Section 7.3.3. Given $\tau_j = \tau_{j-1} x^k_{j-1} = z^k x^k_{<j}$, recall that

$$\beta_{j,i}(\tau_j) = \frac{P_{X_{j,i}|Z^k X^k_{<j}}(1|\tau_j)}{P_{X_{j,i}|Z^k X^k_{<j-1}}(1|\tau_{j-1})} - 1$$

and observe that

$$\mathrm{E}_{P_{X^k_{j-1}|Z^k X^k_{<j-1}}(\cdot|\tau_{j-1})}\Big[\beta_{j,i}(\tau_{j-1} X^k_{j-1})\Big] = \frac{\mathrm{E}_{P_{X^k_{j-1}|Z^k X^k_{<j-1}}(\cdot|\tau_{j-1})}\Big[P_{X_{j,i}|Z^k X^k_{<j}}(1|\tau_{j-1} X^k_{j-1})\Big]}{P_{X_{j,i}|Z^k X^k_{<j-1}}(1|\tau_{j-1})} - 1 = 0.$$

Namely, for every $i \in [k]$, the sequence $\{\beta_{j,i}\}_{j=2}^{m+1}$ is a martingale difference sequence with respect to $\{P_{X^k_{j-1}|Z^k X^k_{<j-1}}\}_{j=2}^{m+1}$ for any fixing of Z^k. Therefore, if we could prove that for most active columns $i \in [k]$ (all but $o(\varepsilon k)$) it holds that $\mathrm{E}_P\left[\sum_{j=2}^{m+1} \beta_{j,i}^2\right] \leq o(\varepsilon)$, then we could apply Fact 3.17 for obtaining that in expectation over P, there are at least $(1-o(\varepsilon))k$ columns $i \in [k]$ in which all their partial sums $\{\sum_{j'=2}^{j} \beta_{j',i}\}_{j=2}^{m+1}$ are bounded in an interval of the form $[-O(1), O(1)]$. For such columns, we could bound the values $\{\prod_{j'=2}^{j}(1+\beta_{j',i})\}_{j\in[m+1]}$ since $\prod_{j'=2}^{j}(1+\beta_{j',i}) \approx \exp\left(\sum_{j'=2}^{j} \beta_{j',i}\right)$ (assuming that all values $\{\beta_{j,i}\}_{j=2}^{m+1}$ are small). The problem is that the above claim is incorrect. Namely, even if $R[W] = 1$ (i.e., $P = R_{Z^k X^{(m+1)\times k}}$), still we expect to have at least $\Omega(k)$ columns with $\mathrm{E}_P\left[\sum_{j=2}^{m+1} \beta_{j,i}^2\right] \geq \Omega(1)$. In order to see it, fix $j \in [m+1]$ and $\tau_j = z^k x^k_{<j}$ with $1 \notin x^k_{<j-1}$ (i.e., active) and observe that in this degenerate case where $R[W] = 1$ (denote as the "Uniform" case and denote its $\beta_{j,i}$ by $\beta^U_{j,i}$), we have

$$\begin{aligned}
\beta^U_{j,i}(\tau_j) &= \frac{R_{X_{j,i}|Z^k X^k_{<j}}(1|\tau_j)}{R_{X_{j,i}|Z^k X^k_{<j-1}}(1|\tau_{j-1})} - 1 \\
&= \frac{\begin{cases} \frac{1}{m} & x_{j-1,i} = 0 \\ 0 & x_{j-1,i} = 1 \end{cases}}{\frac{1}{m}(1-\frac{1}{m})} - 1 \\
&= \begin{cases} \frac{1}{m-1} & x_{j-1,i} = 0 \\ -1 & x_{j-1,i} = 1, \end{cases}
\end{aligned}$$

Namely, as long there is no value 1 in the past (i.e., $1 \notin x_{<j-1,i}$ for the j^{th} element), the next element is -1 w.p. $\frac{1}{m}$ and $\frac{1}{m-1}$ otherwise. Since we expected that at least $\Omega(k)$ of the columns $i \in [k]$ have $x_{\leq m+1,i} = 0^{m+1}$, these sequences have $\sum_{j=2}^{m+1}(\beta^U_{j,i})^2 \geq \Omega(1)$, and therefore, not bounded by $o(\varepsilon)$. Yet, this sequences still behave nicely in a sense that the values $\{\prod_{j'=2}^{j}(1+\beta^U_{j',i})\}_{j=2}^{m+1} = \{(1+\frac{1}{m-1})^{j-1}\}_{j=2}^{m+1}$ are always bounded in the interval $[1,4]$ in case $x_{\leq m+1,i} = 0^{m+1}$. Back to the general case where $R[W] \leq 1$, the above observation leads us to explore the sequences $\{\widehat{\beta}_{j,i}\}$ for $\widehat{\beta}_{j,i} = \beta_{j,i} - \beta^U_{j,i}$ and prove that if $R[W]$ is high enough, then for most active columns $i \in [k]$ we have $\mathrm{E}_P\left[\sum_{j=2}^{m+1} \widehat{\beta}_{j,i}^2\right] \leq o(\varepsilon)$. The first problem is that now this is not necessarily a martingale difference sequence anymore. Therefore, we transform it into a martingale by defining $\widehat{\beta}_{j,i} = \beta_{j,i} - \beta^U_{j,i} + \mu^U_{j-1,i}$ where $\mu^U_{j-1,i}(\tau_{j-1}) = \mathrm{E}_{P_{X^k_{j-1}|Z^k X^k_{<j-1}}(\cdot|\tau_{j-1})}\left[\beta^U_{j,i}(\tau_{j-1} X^k_{j-1})\right]$. The second problem is that in the general case, there might be large jumps in the value of $\beta_{j,i}$ (i.e., $\beta_{j,i}$ might be larger than 1 and even $\approx m$). In order to see why this is a problem, consider the case where it always holds that the values $\{\rho_{j,i}\}$ are zeros, and therefore, if $\beta_{j,i} = \frac{m}{m-1} \cdot \frac{1+\gamma_{j,i}}{1+\rho_{j-1,i}} - 1 = \frac{m}{m-1}(\gamma_{j,i} - \frac{1}{m}) >> 1$ then $\beta_{j,i} \approx \gamma_{j,i}$. Hence, if we could prove that high enough $R[W]$ implies $\mathrm{E}\left[\sum_{i=1}^{k}\sum_{j=1}^{m+1} \gamma_{j,i}^2 \cdot \mathbb{1}\{\gamma_{j,i} > 1\}\right] < o(\varepsilon k)$, then we could handle the $\beta_{j,i}^2$'s in case of large jumps. However, the above bound is incorrect and by Claim 7.6 we only know that high enough $R[W]$ implies $\mathrm{E}\left[\sum_{i=1}^{k}\sum_{j=1}^{m+1} \gamma_{j,i} \cdot \mathbb{1}\{\gamma_{j,i} > 1\}\right] < o(\varepsilon k)$ (i.e., we loose the squares in the large jumps case). We solve this issue by cutting the large jumps and defining $\widehat{\beta}_{j,i} = \beta_{j,i} \cdot \mathbb{1}\{\gamma_{j,i} \leq 1\} + \xi_{j-1,i} - \beta^U_{j,i} + \mu^U_{j-1,i}$ where $\xi_{j-1,i}(\tau_{j-1}) =$

$\mathrm{E}_{x^k_{j-1} \sim P_{X^k_{j-1}|Z^k X^k_{<j-1}}(\cdot|\tau_{j-1})}\left[\beta_{j,i}(\tau_{j-1}x^k_{j-1}) \cdot \mathbb{1}\{\gamma_{j,i}(\tau_{j-1}x^k_{j-1}) > 1\}\right]$ is added in order to preserve the martingale property of these sequences. Finally, by Claim 7.15 and Corollary 7.35, we actually expect that if $R[W]$ is high enough, then for most active columns $i \in [k]$ (all but $o(\varepsilon k)$) there are no jumps in the values of $\{\gamma_{j,i}\}$, $\{\rho_{j,i}\}$ and $\{\xi_{j,i}\}$ and in our analysis we use it by zeroing the sequence $\{\widehat{\beta}_{j,i}\}_{j=2}^{m+1}$ in some round j if there was some large jump in one of measurements of the first $j-1$ rounds (denote this "bad" event by $\mathrm{good}_{j-1,i} = 0$). Moreover, since we do not expect such jumps for most active columns, then it can be shown that for such good column $i \in [k]$, the sequence $\{\widehat{\beta}_{j,i}\}_{j=2}^{m+1}$ which we finally can bound using a fact about martingales, is close enough to the desired sequence $\{\beta_{j,i}\}_{j=2}^{m+1}$ and the proof follows.

Round Zero The following claim states that if $R[W]$ is high enough, then in expectation (over $z^k \sim P_{Z^k}$), most columns $i \in [k]$ (all but $o(\varepsilon k)$) have $\frac{R_{Z_i}(z_i)}{P_{Z_i}(z_i)} \approx 1$.

Claim 7.30. *For every two constants $\lambda > 0$ and $c \in (0,1)$ there exists a constant $\lambda' > 0$ such that if $\mathrm{E}_{z^k \sim P_{Z^k}}\left[\sum_{i=1}^k \mathbb{1}\{P_{Z_i}(z_i) \notin (1 \pm c) \cdot R_{Z_i}(z_i)\}\right] > \varepsilon k/\lambda$, then $R[W] \leq (1-\varepsilon)^{k/\lambda'}$.*

Proof. We first handle the case $\mathrm{E}_{z^k \sim P_{Z^k}}\left[\sum_{i=1}^k \mathbb{1}\{P_{Z_i}(z_i) > (1+c) \cdot R_{Z_i}(z_i)\}\right] > \frac{\varepsilon k}{2\lambda}$. Let $p_i := \Pr_{z \sim P_{Z_i}}[P_{Z_i}(z) > (1+c) \cdot R_{Z_i}(z)]$ and $q_i := \Pr_{z \sim R_{Z_i}}[P_{Z_i}(z) > (1+c) \cdot R_{Z_i}(z)]$. Recall that by assumption, $\sum_{i=1}^k p_i \geq \frac{\varepsilon k}{2\lambda}$ and observe that for any $i \in [k]$ it holds that $q_i \leq \frac{p_i}{1+c}$. The proof then follows since

$$\begin{aligned}
\log \frac{1}{R[W]} &\geq D(P_{Z^k}||R_{Z^k}) = D\left(P_{Z^k}||\prod_{i=1}^k R_{Z_i}\right) \\
&\geq \sum_{i=1}^k D(P_{Z_i}||R_{Z_i}) \geq \sum_{i=1}^k D(p_i||q_i) \\
&\geq \sum_{i=1}^k D\left((1+c)\frac{p_i}{1+c}||\frac{p_i}{1+c}\right) \\
&\geq \frac{c^2}{4} \cdot \sum_{i=1}^k p_i \geq c^2 \cdot \frac{\varepsilon k}{8\lambda}
\end{aligned}$$

$$\implies R[W] \leq e^{-c^2 \cdot \frac{\varepsilon k}{8\lambda}} \leq (1-\varepsilon)^{\varepsilon k/\left(16\lambda/c^2\right)},$$

where the first inequality holds by Fact 3.6, the second and third one holds by Fact 3.5 (the product case of chain-rule and data-processing, respectively), and the one before last holds by Fact 3.9.

Otherwise, it holds that $\mathrm{E}_{z^k \sim P_{Z^k}}\left[\sum_{i=1}^k \mathbb{1}\{P_{Z_i}(z_i) < (1-c) \cdot R_{Z_i}(z_i)\}\right] > \frac{\varepsilon k}{2\lambda}$. In this case we define $p_i := \Pr_{z \sim P_{Z_i}}[P_{Z_i}(z) < (1-c) \cdot R_{Z_i}(z)]$ and $q_i := \Pr_{z \sim R_{Z_i}}[P_{Z_i}(z) < (1-c) \cdot R_{Z_i}(z)]$ and note that $p_i \le (1-c)q_i$ and $\sum_{i=1}^k q_i \ge \sum_{i=1}^k p_i \ge \frac{\varepsilon k}{2\lambda}$. The proof then follows since

$$\begin{aligned}\log\frac{1}{R[W]} &\ge \sum_{i=1}^k D(P_{Z_i}||R_{Z_i}) \ge \sum_{i=1}^k D(p_i||q_i)\\ &\ge \sum_{i=1}^k D((1-c)q_i||q_i) \ge \frac{c^2}{2}\cdot\sum_{i=1}^k q_i\\ &\ge c^2\cdot\frac{\varepsilon k}{4\lambda}\end{aligned}$$

$$\implies R[W] \le e^{-c^2\cdot\frac{\varepsilon k}{4\lambda}} \le (1-\varepsilon)^{k/\left(8\lambda/c^2\right)}$$

□

The following claim states that if $R[W]$ is high enough, then in expectation (over $z^k \sim P_{Z^k}$), most columns $i \in [k]$ (all but $o(\varepsilon k)$) have $\frac{P_{X_{1,i}|Z^k}(1|z^k)}{P_{X_{1,i}|Z_i}(1|z_i)} \approx 1$

Claim 7.31. *For every two constants $\lambda > 0$ and $c \in (0,1)$ there exists a constant $\lambda' > 0$ such that if $\mathrm{E}_{P_{Z^k}}\left[\sum_{i=1}^k \mathbb{1}\{P_{X_{1,i}|Z_i}(1) \notin \frac{1\pm c}{m}\}\right] \ge \varepsilon k/\lambda$, then $R[W] \le (1-\varepsilon)^{\frac{k}{\lambda'\cdot m}}$.*

Proof. Compute

$$\begin{aligned}\log\frac{1}{R[W]} &\ge D\Big(P_{Z^k X_1^k}||R_{Z^k X_1^k}\Big) = D\left(P_{Z^k X_1^k}||\prod_{i=1}^k R_{Z_i X_{1,i}}\right)\\ &\ge \sum_{i=1}^k D\big(P_{Z_i X_{1,i}}||R_{Z_i X_{1,i}}\big) \ge \sum_{i=1}^k \mathrm{E}_{P_{Z_i}}\left[D\Big(P_{X_{1,i}|Z_i}||R_{X_{1,i}|Z_i}\Big)\right]\\ &\ge \sum_{i=1}^k \mathrm{E}_{P_{Z_i}}\left[D\Big(P_{X_{1,i}|Z_i}||R_{X_{1,i}|Z_i}\Big)\cdot\mathbb{1}\{P_{X_{1,i}|Z_i}(1)\notin\frac{1\pm c}{m}\}\right]\\ &\ge \frac{c^2}{4m}\cdot\mathrm{E}_{P_{Z_i}}\left[\sum_{i=1}^k \mathbb{1}\{P_{X_{1,i}|Z_i}(1)\notin\frac{1\pm c}{m}\}\right]\\ &\ge c^2\cdot\frac{\varepsilon k}{4\lambda\cdot m}\end{aligned}$$

$$\implies R[W] \le e^{-c^2\cdot\frac{\varepsilon k}{4\lambda\cdot m}} \le (1-\varepsilon)^{\frac{k}{(8\lambda/c^2)\cdot m}},$$

where the first inequality holds by Fact 3.6, the second and third ones hold by Fact 3.5 (chain-rule) and the one before last holds by Fact 3.9 since $R_{X_{1,i}|Z_i}(1) = \frac{1}{m}$. □

Table 6: Additional Measurements.

Definition	*Value*
$\xi_{j,i}(\tau_j)$	$\mathrm{E}_{x^k_{j-1} \sim P_{X^k_{j-1} \mid Z^k X^k_{<j-1}}(\cdot \mid \tau_{j-1})}\left[\beta_{j,i}(\tau_{j-1}x^k_{j-1}) \cdot \mathbb{1}\{\gamma_{j,i}(\tau_{j-1}x^k_{j-1}) > 1\}\right]$
$\beta^U_{j,i}(\tau_j)$	$\begin{cases} \frac{1}{m-1} & x_{j-1,i} = 0 \\ -1 & x_{j-1,i} = 1 \end{cases}$
$\mu^U_{j,i}(\tau_j)$	$\mathrm{E}_{x^k_{j-1} \sim P_{X^k_{j-1} \mid Z^k X^k_{<j-1}}(\cdot \mid \tau_{j-1})}\left[\beta^U_{j,i}(\tau_{j-1}x^k_{j-1})\right]$
$\mathrm{good}_{j,i}(\tau_j)$	$\mathbb{1}\{i \in \mathcal{G}^{\gamma}_{\tau_j} \cap \mathcal{G}^{\rho}_{\tau_j}\} \cdot \mathbb{1}\{\xi_{j,i} \leq 0.1\}$
$\widehat{\beta}_{j,i}(\tau_j)$	$\begin{cases} 0 & \mathrm{good}_{j-1,i} = 0 \\ \beta_{j,i} \cdot \mathbb{1}\{\gamma_{j,i} \leq 1\} + \xi_{j-1,i} - \beta^U_{j,i} + \mu^U_{j-1,i} & \text{Otherwise} \end{cases}$

Rounds 1 **to** $m+1$ As mentioned in Section 7.3.3, the goal of this section is to prove that if $R[W]$ is high enough, then for most active columns $i \in [k]$ (all but $o(\varepsilon k)$) it holds that the values $\{\prod_{j'=2}^{j}(1+\beta_{j',i})\}_{j=2}^{m+1}$ are bounded between two constants, and then using Section 7.3.3 we deduce Claim 7.16. In Table 6 we present the formal definitions of the new variables that are mentioned in Section 7.3.3.

The following claim states basic facts about the new variables.

Claim 7.32 (Measurements' Properties)**.** *For any $\tau_j = \tau_{j-1}x^k_{j-1} = z^k x^k_{<j} \in \mathrm{Supp}(P_{Z^k X^k_{<j}})$ it holds that*

1. $1 \notin x_{<j-1,i} \implies \mu_{j-1,i}(\tau_{j-1}) = -\frac{\gamma_{j-1,i}(\tau_{j-1})}{m-1}$.
2. $\mathrm{E}_{P_{X^k_{j-1}|Z^k X^k_{<j-1}}(\cdot|\tau_{j-1})}\left[\widehat{\beta}_{j,i}(\tau_{j-1}X^k_{j-1})\right] = 0.$
3. $\left|\widehat{\beta}_{j,i}(\tau_j)\right| \leq 7.$
4. $\gamma_{j,i}(\tau_j) > 1, |\rho_{j-1,i}(\tau_{j-1})| \leq 0.1 \implies \beta_{j,i}(\tau_j) \in (0.8\gamma_{j,i}, 4\gamma_{j,i})$.
5. $1 \notin x_{<j,i}, \gamma_{j,i} \leq 1 \implies \gamma_{j,i}(\tau_j) = \frac{m-1}{m}(1+\rho_{j-1,i})\left(\widehat{\beta}_{j,i} + \frac{\gamma_{j-1,i}}{m-1} - \xi_{j-1,i}\right) + \rho_{j-1,i}$.
6. $1 \notin x_{<j,i}, \gamma_{j,i} \leq 1, |\rho_{j-1,i}|, \xi_{j,i} \leq 0.1 \implies \gamma^2_{j,i} \leq \frac{1}{10}\widehat{\beta}^2_{j,i} - \gamma^2_{j-1,i} - \xi_{j-1,i} - 3\rho^2_{j-1,i}$

Proof. For property 1, compute

$$\begin{aligned} \mu^U_{j-1,i}(\tau_{j-1}) &= -1 \cdot P_{X^k_{j-1}|Z^k X^k_{<j-1}}(1|\tau_{j-1}) + \frac{1}{m-1} \cdot P_{X^k_{j-1}|Z^k X^k_{<j-1}}(0|\tau_{j-1}) \\ &= -\frac{1+\gamma_{j-1,i}(\tau_{j-1})}{m} + \frac{1}{m-1} \cdot \left(1 - \frac{1+\gamma_{j-1,i}(\tau_{j-1})}{m}\right) \\ &= -\frac{\gamma_{j-1,i}(\tau_{j-1})}{m-1}. \end{aligned} \tag{86}$$

For property 2, observe that if $\mathrm{good}_{j-1,i} = 0$ then $\widehat{\beta}_{j,i} = 0$ by definition, and otherwise it holds that

$$\begin{aligned}
&\mathrm{E}_{x_{j-1}^k \sim P_{X_{j-1}^k | Z^k X_{<j-1}^k}(\cdot|\tau)} \left[\widehat{\beta}_{j,i}(\tau_{j-1} x_{j-1}^k)\right] \\
&= \mathrm{E}_{x_{j-1}^k} \left[\beta_{j,i} \cdot \mathbb{1}\{\gamma_{j,i} \le 1\} + \xi_{j-1,i} - \beta_{j,i}^U + \mu_{j-1,i}^U\right] \\
&= \mathrm{E}_{x_{j-1}^k}[\beta_{j,i}] \cdot \mathrm{Pr}_{x_{j-1}^k}[\gamma_{j,i} \le 1] + \mathrm{E}_{x_{j-1}^k}[\beta_{j,i}] \cdot \mathrm{Pr}_{x_{j-1}^k}[\gamma_{j,i} > 1] - \mathrm{E}_{x_{j-1}^k}\left[\beta_{j,i}^U\right] + \mathrm{E}_{x_{j-1}^k}\left[\beta_{j,i}^U\right] \\
&= \mathrm{E}_{x_{j-1}^k \sim P_{X_{j-1}^k | Z^k X_{<j}^k}(\cdot|\tau_{j-1})} \left[\beta_{j,i}(\tau_{j-1} x_{j-1}^k)\right] \\
&= \frac{\mathrm{E}_{x_{j-1}^k \sim P_{X_{j-1}^k | Z^k X_{<j-1}^k}(\cdot|\tau_{j-1})} \left[P_{X_{j,i}|Z^k X_{<j}^k}(1|\tau_{j-1} x_{j-1}^k)\right]}{P_{X_{j,i}|Z^k X_{<j-1}^k}(1|\tau_{j-1})} - 1 \\
&= 0
\end{aligned}$$

For property 3, recall that if $\mathrm{good}_{j-1,i}(\tau_{j-1}) = 0$ then $\widehat{\beta}_{j,i}(\tau_j) = 0$ and otherwise

$$\begin{aligned}
\left|\widehat{\beta}_{j,i}(\tau_j)\right| &\le |\beta_{j,i}| \cdot \mathbb{1}\{\gamma_{j,i} \le 1\} + |\xi_{j-1,i}| + \left|\beta_{j,i}^U\right| + \left|\mu_{j-1,i}^U\right| \\
&\le \frac{m}{m-1} \cdot \frac{1+\gamma_{j,i}}{1+\rho_{j-1,i}} \cdot \mathbb{1}\{\gamma_{j,i} \le 1\} + \xi_{j-1,i} + 2 \\
&\le 2 \cdot \frac{2}{1-0.1} + 0.1 + 2 \\
&\le 7
\end{aligned}$$

For property 4, recall that $\gamma_{j,i} > 1$ and $\rho_{j-1,i} \le 0.1$. The upper bound holds since

$$\begin{aligned}
\beta_{j,i} &= \frac{m}{m-1} \cdot \frac{1+\gamma_{j,i}}{1+\rho_{j-1,i}} - 1 \\
&\le 2 \cdot \frac{1+\gamma_{j,i}}{1-0.1} - 1 < 2.5\gamma_{j,i} + 1.5 < 4\gamma_{j,i}
\end{aligned}$$

and the lower bound holds since

$$\begin{aligned}
\beta_{j,i} &= \frac{m}{m-1} \cdot \frac{1+\gamma_{j,i}}{1+\rho_{j-1,i}} - 1 \\
&\ge \frac{1+\gamma_{j,i}}{1+0.1} - 1 > 0.9\gamma_{j,i} - 0.1 > 0.8\gamma_{j,i}
\end{aligned}$$

For property 5, compute

$$\begin{aligned}
\gamma_{j,i}(\tau_j) &= \frac{m-1}{m}(1+\rho_{j-1,i})(1+\beta_{j,i}) - 1 \\
&= \frac{m-1}{m}(1+\rho_{j-1,i})(1+\widehat{\beta}_{j,i} - \xi_{j-1,i} + \frac{1}{m-1} + \frac{\gamma_{j-1,i}}{m-1}) - 1 \\
&= \frac{m-1}{m}(\widehat{\beta}_{j,i} - \xi_{j-1,i} + \frac{\gamma_{j-1,i}}{m}) + \frac{m-1}{m}\rho_{j-1,i}(1+\widehat{\beta}_{j,i} - \xi_{j-1,i} + \frac{1}{m-1} + \frac{\gamma_{j-1,i}}{m-1}) \\
&= \frac{m-1}{m}(1+\rho_{j-1,i})\left(\widehat{\beta}_{j,i} + \frac{\gamma_{j-1,i}}{m-1} - \xi_{j-1,i}\right) + \rho_{j-1,i}
\end{aligned}$$

For property 6, compute

$$\begin{aligned}
\gamma_{j,i}(\tau_j)^2 &= \left(\frac{m-1}{m}(1+\rho_{j-1,i})\widehat{\beta}_{j,i} + \big((1+\rho_{j-1,i})\cdot\frac{\gamma_{j-1,i}}{m} - \frac{m-1}{m}(1+\rho_{j-1,i})\xi_{j-1,i} + \rho_{j-1,i}\big)\right)^2\\
&\geq \frac{1}{2}\left(\frac{m-1}{m}(1+\rho_{j-1,i})\widehat{\beta}_{j,i}\right)^2 - \left((1+\rho_{j-1,i})\cdot\frac{\gamma_{j-1,i}}{m} - \frac{m-1}{m}(1+\rho_{j-1,i})\xi_{j-1,i} + \rho_{j-1,i}\right)^2\\
&\geq \frac{1}{10}\widehat{\beta}^2_{j,i} - 3\cdot\left(\frac{(1+0.1)^2}{m^2}\gamma^2_{j-1,i} + (1+0.1)^2\xi^2_{j-1,i} + \rho^2_{j-1,i}\right)\\
&\geq \frac{1}{10}\widehat{\beta}^2_{j,i} - \gamma^2_{j-1,i} - \xi_{j-1,i} - 3\rho^2_{j-1,i},
\end{aligned}$$

where the first inequality holds by the fact that $(a+b)^2 \geq \frac{1}{2}a^2 - b^2$, the second inequality holds by the fact that $(a+b+c)^2 \leq 3(a^2+b^2+c^2)$ and by the bound $m \geq 2$ and $|\rho_{j-1,i}| \leq 0.1$, and the last one holds since $m \geq 2$ and $0 \leq \xi_{j,i} \leq 0.1$. □

The following claim connects between the measurements $\{\xi_{j,i}\}_{j,i}$ to $R[W]$.

Claim 7.33. *It holds that*

$$\log\frac{1}{R[W]} \geq \frac{1}{16m}\sum_{i=1}^{k}\sum_{j=1}^{m}\mathrm{E}_{P_{Z^k X^k_{<j}}}[\xi_{j,i}\cdot\mathbb{1}\{|\rho_{j,i}| \leq 0.1\}],$$

for $\xi_{j,i} = \xi_{j,i}(Z^k X^k_{<j})$ and $\rho_{j,i} = \rho_{j,i}(Z^k X^k_{<j})$.

Proof. Compute

$$\begin{aligned}
\log\frac{1}{R[W]} &\geq \frac{1}{4m}\cdot\sum_{i=1}^{k}\sum_{j=2}^{m+1}\mathrm{E}_{P_{Z^k X^k_{<j}}}[\gamma_{j,i}\cdot\mathbb{1}\{\gamma_{j,i} > 1\}]\\
&\geq \frac{1}{4m}\cdot\sum_{i=1}^{k}\sum_{j=2}^{m+1}\mathrm{E}_{P_{Z^k X^k_{<j-1}}}\left[\mathbb{1}\{|\rho_{j-1,i}| \leq 0.1\}\cdot\mathrm{E}_{P_{X^k_{j-1}|Z^k X^k_{<j-1}}}[\gamma_{j,i}\cdot\mathbb{1}\{\gamma_{j,i} > 1\}]\right]\\
&\geq \frac{1}{16m}\sum_{i=1}^{k}\sum_{j=2}^{m+1}\mathrm{E}_{P_{Z^k X^k_{<j-1}}}\left[\mathbb{1}\{|\rho_{j-1,i}| \leq 0.1\}\cdot\mathrm{E}_{P_{X^k_{j-1}|Z^k X^k_{<j-1}}}[\beta_{j,i}\cdot\mathbb{1}\{\gamma_{j,i} > 1\}]\right]\\
&= \frac{1}{16m}\sum_{i=1}^{k}\sum_{j=2}^{m+1}\mathrm{E}_{P_{Z^k X^k_{<j-1}}}[\xi_{j-1,i}\cdot\mathbb{1}\{|\rho_{j-1,i}| \leq 0.1\}]\\
&= \frac{1}{16m}\sum_{i=1}^{k}\sum_{j=1}^{m}\mathrm{E}_{P_{Z^k X^k_{<j}}}[\xi_{j,i}\cdot\mathbb{1}\{|\rho_{j,i}| \leq 0.1\}],
\end{aligned}$$

where the first inequality follows by Claim 7.21 and the fact that $\gamma_{j,i} > 1 \implies 1 \notin X_{<j,i}$, and the third one by Claim 7.32(4). □

As a first corollary of Claim 7.33, we obtain the following.

Corollary 7.34. *For any constant $\lambda > 0$ there exists a constant $\lambda' > 0$ such that if $\mathrm{E}_P\left[\sum_{i=1}^k \sum_{j=1}^m \xi_{j,i} \cdot \mathbb{1}\{|\rho_{j,i}| \leq 0.1\}\right] \geq \varepsilon k/\lambda$ for $\xi_{j,i} = \xi_{j,i}(Z^k X^k_{<j})$ and $\rho_{j,i} = \rho_{j,i}(Z^k X^k_{<j})$, then $R[W] \leq (1-\varepsilon)^{\frac{k}{\lambda' \cdot m}}$.*

Proof. Immediately follows by Claim 7.33. □

As a second corollary of Claim 7.33, we obtain that if $R[W]$ is high enough, then most columns $i \in [k]$ have bounded sum $\sum_{j=1}^m \xi_{j,i}$ in expectation over P.

Corollary 7.35. *For any constants $\lambda > 0$ and $c \in (0,1)$ there exists a constant $\lambda' > 0$ such that if $\mathrm{E}_P\left[\sum_{i=1}^k \mathbb{1}\{\sum_{j=1}^m \xi_{j,i} > c\}\right] \geq \varepsilon k/\lambda$ for $\xi_{j,i} = \xi_{j,i}(Z^k X^k_{<j})$, then $R[W] \leq (1-\varepsilon)^{\frac{k}{\lambda' \cdot m}}$.*

Proof. Assume that $\mathrm{E}_P\left[\sum_{i=1}^k \mathbb{1}\{\sum_{j=1}^m \xi_{j,i} > c\}\right] \geq \varepsilon k/\lambda$ for some constant $\lambda > 0$. Observe that

$$\begin{aligned}
&\mathrm{E}_P\left[\sum_{i=1}^k \mathbb{1}\{\sum_{j=1}^m \xi_{j,i} > c\}\right] \\
&= \mathrm{E}_P\left[\sum_{i=1}^k \mathbb{1}\{\sum_{j=1}^m \xi_{j,i} > c\} \cdot \mathbb{1}\{u_i^\rho = \infty\}\right] + \mathrm{E}_P\left[\sum_{i=1}^k \mathbb{1}\{\sum_{j=1}^m \xi_{j,i} > c\} \cdot \mathbb{1}\{u_i^\rho < \infty\}\right],
\end{aligned}$$

where $u_i^\rho = u_i^\rho(Z^k X^{(m+1)\times k})$. If $\mathrm{E}_P\left[\sum_{i=1}^k \mathbb{1}\{\sum_{j=1}^m \xi_{j,i} > c\} \cdot \mathbb{1}\{u_i^\rho < \infty\}\right] > \frac{\varepsilon k}{2\lambda}$ then in particular, $\mathrm{E}_P\left[\mathrm{jumps}^\rho(Z^k X^{(m+1)\times k})\right] = \mathrm{E}_P\left[\sum_{i=1}^k \mathbb{1}\{u_i^\rho < \infty\}\right] > \frac{\varepsilon k}{2\lambda}$ and the proof follows by Claim 7.15. Otherwise, $\mathrm{E}_P\left[\sum_{i=1}^k \mathbb{1}\{\sum_{j=1}^m \xi_{j,i} > c\} \cdot \mathbb{1}\{u_i^\rho = \infty\}\right] \geq \frac{\varepsilon k}{2\lambda}$. Compute

$$\begin{aligned}
\log \frac{1}{R[W]} &\geq \frac{1}{16m} \cdot \mathrm{E}_P\left[\sum_{i=1}^k \sum_{j=1}^m \xi_{j,i} \cdot \mathbb{1}\{|\rho_{j,i}| \leq 0.1\}\right] \\
&\geq \frac{1}{16m} \cdot \mathrm{E}_P\left[\sum_{i=1}^k \mathbb{1}\{\sum_{j=1}^m \xi_{j,i} > c\} \cdot \mathbb{1}\{u_i^\rho = \infty\} \cdot \sum_{j=1}^m \xi_{j,i} \cdot \mathbb{1}\{|\rho_{j,i}| \leq 0.1\}\right] \\
&= \frac{1}{16m} \cdot \mathrm{E}_P\left[\sum_{i=1}^k \mathbb{1}\{\sum_{j=1}^m \xi_{j,i} > c\} \cdot \mathbb{1}\{u_i^\rho = \infty\} \cdot \sum_{j=1}^m \xi_{j,i}\right] \\
&\geq \frac{c}{16m} \cdot \mathrm{E}_P\left[\sum_{i=1}^k \mathbb{1}\{\sum_{j=1}^m \xi_{j,i} > c\} \cdot \mathbb{1}\{u_i^\rho = \infty\}\right] \\
&\geq c \cdot \frac{\varepsilon k}{32\lambda \cdot m} \implies R[W] \leq e^{-c \cdot \frac{\varepsilon k}{32 m \lambda}} \leq (1-\varepsilon)^{\frac{\varepsilon k}{(32\lambda/c)\cdot m}}
\end{aligned}$$

where the first inequality holds by Claim 7.33 and the last one hold since $\varepsilon \in [0, \frac{1}{2}]$. □

The following claim is the heart of this section. It states that if $R[W]$ is high enough, then in expectation (over P), the sum of squares of all sequences' elements (Namely, $\sum_{i=1}^k \sum_{j=2}^{m+1} \widehat{\beta}_{j,i}^2$) is at most $o(\varepsilon k)$. This later yields that for a typical column $i \in [k]$ we expect that $\sum_{j=2}^{m+1} \widehat{\beta}_{j,i}^2 \leq o(\varepsilon)$ and then the ideas of Section 7.3.3 follows.

Claim 7.36. *For any constant $\lambda > 0$ there exists a constant $\lambda' > 0$ such that if* $\mathrm{E}_P\left[\sum_{i=1}^{k}\sum_{j=2}^{m+1}\widehat{\beta}_{j,i}^2\right] \geq \varepsilon k/\lambda$ *for* $\widehat{\beta}_{j,i} = \widehat{\beta}_{j,i}(Z^k X_{<j}^k)$*, then* $R[W] \leq (1-\varepsilon)^{\frac{k}{\lambda'\cdot m}}$.

Proof. Assume that $\mathrm{E}_P\left[\sum_{i=1}^{k}\sum_{j=2}^{m+1}\widehat{\beta}_{j,i}^2\right] \geq \varepsilon k/\lambda$ for some constant $\lambda > 0$. If $\mathrm{E}_P\left[\sum_{i=1}^{k}\sum_{j=2}^{m+1}\widehat{\beta}_{j,i}^2 \cdot \mathbb{1}\{\gamma_{j,i} > 1\}\right] \geq \frac{\varepsilon k}{2\lambda}$ then the proof follows since

$$\begin{aligned}
\log\frac{1}{R[W]} &\geq \mathrm{E}_P\left[\sum_{i=1}^{k}\sum_{j=1}^{m+1}\frac{\min\{|\gamma_{j,i}|, \gamma_{j,i}^2\}}{4m}\cdot\mathbb{1}\{1\notin x_{<j,i}\}\right]\\
&\geq \mathrm{E}_P\left[\sum_{i=1}^{k}\sum_{j=1}^{m+1}\frac{\gamma_{j,i}}{4m}\cdot\mathbb{1}\{\gamma_{j,i} > 1\}\right]\\
&\geq \frac{1}{196m}\cdot\mathrm{E}_P\left[\sum_{i=1}^{k}\sum_{j=1}^{m+1}\widehat{\beta}_{j,i}^2\cdot\mathbb{1}\{\gamma_{j,i} > 1\}\right]\\
&\geq \frac{\varepsilon k}{392\lambda\cdot m} \implies R[W] \leq e^{-\frac{\varepsilon k}{392\lambda\cdot m}} \leq (1-\varepsilon)^{\frac{\varepsilon k}{392\lambda\cdot m}},
\end{aligned}$$

where the first inequality holds by Claim 7.21, the third one holds since $\left|\widehat{\beta}_{j,i}\right| \leq 7$ (property 3 of Claim 7.32) and the last one holds since $\varepsilon \in [0, \frac{1}{2}]$. Otherwise, it holds that

$$\begin{aligned}
&\mathrm{E}_P\left[\sum_{i=1}^{k}\sum_{j=2}^{m+1}\widehat{\beta}_{j,i}^2\cdot\mathbb{1}\{\gamma_{j,i} \leq 1\}\right]\\
&= \mathrm{E}_P\left[\sum_{i=1}^{k}\sum_{j=2}^{m+1}\widehat{\beta}_{j,i}^2\cdot\mathbb{1}\{X_{j-1,i} = 1\}\right] + \mathrm{E}_P\left[\sum_{i=1}^{k}\sum_{j=2}^{m+1}\widehat{\beta}_{j,i}^2\cdot\mathbb{1}\{1\notin X_{<j,i}\}\cdot\mathbb{1}\{\gamma_{j,i}\leq 1\}\right]\\
&\geq \frac{\varepsilon k}{2\lambda}
\end{aligned} \tag{87}$$

Now, observe that

$$\begin{aligned}
&\mathrm{E}_P\left[\sum_{i=1}^{k}\sum_{j=2}^{m+1}\widehat{\beta}_{j,i}^2\cdot\mathbb{1}\{X_{j-1,i}=1\}\right]\\
&=\mathrm{E}_P\left[\sum_{i=1}^{k}\sum_{j=2}^{m+1}\widehat{\beta}_{j,i}^2\cdot\mathbb{1}\{X_{j-1,i}=1\}\cdot\mathbb{1}\{\mathrm{good}_{j-1,i}=1\}\right]\\
&=\mathrm{E}_P\left[\sum_{i=1}^{k}\sum_{j=2}^{m+1}(\xi_{j-1,i}-\frac{\gamma_{j-1,i}}{m-1})^2\cdot\mathbb{1}\{\mathrm{good}_{j-1,i}=1\}\right]\\
&\leq\mathrm{E}_P\left[\sum_{i=1}^{k}\sum_{j=2}^{m+1}2(\xi_{j-1,i}^2+\frac{\gamma_{j-1,i}^2}{(m-1)^2})\cdot\mathbb{1}\{\mathrm{good}_{j-1,i}=1\}\right]\\
&\leq\mathrm{E}_P\left[\sum_{i=1}^{k}\sum_{j=1}^{m-1}\xi_{j,i}\cdot\mathbb{1}\{|\rho_{j,i}|\leq 0.1\}\right]+2\cdot\mathrm{E}_P\left[\sum_{i=1}^{k}\sum_{j=1}^{m-1}\gamma_{j,i}^2\cdot\mathbb{1}\{1\notin X_{<j,i}\}\cdot\mathbb{1}\{\gamma_{j,i}\leq 1\}\right], \qquad (88)
\end{aligned}$$

where the first inequality holds by the fact that $(a+b)^2 \leq 2(a^2+b^2)$, and the last one holds since $\mathrm{good}_{j-1,i}=1 \implies |\gamma_{j-1,i}|, |\rho_{j-1,i}|, \xi_{j-1,i} \leq 0.1$ and since $m \geq 2$ and $\xi_{j-1,i} \geq 0$. Therefore, if $\mathrm{E}_P\left[\sum_{i=1}^{k}\sum_{j=2}^{m+1}\widehat{\beta}_{j,i}^2\cdot\mathbb{1}\{X_{j-1,i}=1\}\right] \geq \frac{\varepsilon k}{4\lambda}$, then at least one of the terms in (88) must be $\geq \frac{\varepsilon k}{8\lambda}$ and the proof follows by Corollaries 7.22 and 7.34. Otherwise, it holds by Equation (87) that

$\mathrm{E}_P\left[\sum_{i=1}^{k}\sum_{j=2}^{m+1}\widehat{\beta}_{j,i}^2 \cdot \mathbb{1}\{1 \notin X_{<j,i}\} \cdot \mathbb{1}\{\gamma_{j,i} \leq 1\}\right] \geq \frac{\varepsilon k}{4\lambda}$. Compute

$$
\begin{aligned}
&\log \frac{1}{R[W]} \\
&\geq \mathrm{E}_P\left[\sum_{i=1}^{k}\sum_{j=1}^{m+1} \frac{\min\{|\gamma_{j,i}|, \gamma_{j,i}^2\}}{4m} \cdot \mathbb{1}\{1 \notin X_{<j,i}\}\right] \\
&\geq \frac{1}{4m} \cdot \mathrm{E}_P\left[\sum_{i=1}^{k}\sum_{j=1}^{m+1} \gamma_{j,i}^2 \cdot \mathbb{1}\{1 \notin X_{<j,i}\} \cdot \mathbb{1}\{\gamma_{j,i} \leq 1\} \cdot \mathbb{1}\{\mathrm{good}_{j-1,i} = 1\}\right] \\
&\geq \frac{1}{4m} \cdot \mathrm{E}_P\left[\sum_{i=1}^{k}\sum_{j=2}^{m+1} (\frac{1}{10}\widehat{\beta}_{j,i}^2 - \gamma_{j-1,i}^2 - \xi_{j-1,i} - 3\rho_{j-1,i}^2) \cdot \mathbb{1}\{1 \notin X_{<j,i}\} \cdot \mathbb{1}\{\gamma_{j,i} \leq 1\} \cdot \mathbb{1}\{\mathrm{good}_{j-1,i} = 1\}\right] \\
&\geq \frac{1}{160m}\mathrm{E}_P\left[\sum_{i=1}^{k}\sum_{j=2}^{m+1} \widehat{\beta}_{j,i}^2 \cdot \mathbb{1}\{1 \notin X_{<j,i}\} \cdot \mathbb{1}\{\gamma_{j,i} \leq 1\}\right] \qquad (89) \\
&- \frac{1}{4m} \cdot \mathrm{E}_P\left[\sum_{i=1}^{k}\sum_{j=1}^{m} \gamma_{j,i}^2 \cdot \mathbb{1}\{1 \notin X_{<j,i}\} \cdot \mathbb{1}\{\gamma_{j,i} \leq 1\}\right] \\
&- \frac{3}{4m} \cdot \mathrm{E}_P\left[\sum_{i=1}^{k}\sum_{j=1}^{m} \rho_{j,i}^2 \cdot \mathbb{1}\{1 \notin X_{<j,i}\} \cdot \mathbb{1}\{\rho_{j,i} \leq 1\}\right] \\
&- \frac{1}{4m} \cdot \mathrm{E}_P\left[\sum_{i=1}^{k}\sum_{j=1}^{m} \xi_{j,i} \cdot \mathbb{1}\{|\rho_{j,i}| \leq 0.1\}\right],
\end{aligned}
$$

where the first inequality holds by Claim 7.21, the second one holds since $\mathrm{good}_{j-1,i} = 1 \implies |\gamma_{j-1,i}| \leq 0.1$ and the third one holds by Claim 7.32 (property 6) since $\mathrm{good}_{j-1,i} = 1 \implies |\rho_{j-1,i}|, \xi_{j-1,i} \leq 0.1$. By assumption, the first term in Equation (89) is at least $\frac{\varepsilon k}{4\lambda}$. Therefore, there are two options: The first option is that the sum of terms in (89)$\geq \frac{\varepsilon k}{8\lambda} \implies R[W] \leq e^{-\frac{\varepsilon k}{8\lambda}} \leq (1-\varepsilon)^{\frac{\varepsilon k}{16\lambda}}$. The second option is that at least one of the negative terms in (89) has absolute value $\geq \frac{\varepsilon k}{24\lambda}$, and then the proof follows by Corollaries 7.22, 7.26 and 7.34. □

The following claim focuses on "good" columns, i.e., columns $i \in [k]$ with bounded sums $\{\sum_{j'=2}^{j}\widehat{\beta}_{j',i}\}_{j=2}^{m+1}$ and with small values of $\{\gamma_{j,i}\}_{j=1}^{m+1}$, $\{\rho_{j,i}\}_{j=1}^{m+1}$ and $\{\sum_{j'=1}^{j}\xi_{j',i}\}_{j=1}^{m}$. For these columns, the claim connects the sums $\{\sum_{j'=2}^{j}\widehat{\beta}_{j',i}\}_{j=2}^{m+1}$ into the required products $\{\prod_{j'=2}^{j}(1+\beta_{j',i})\}_{j=2}^{m+1}$ by showing that they are indeed bounded in an interval of constants. Along with assuming that the first two terms of $\alpha_{j,i}$ are ≈ 1, the claim concludes that for such columns it holds that the values of $\{\alpha_{j,i}\}_{j=1}^{m+1}$ are indeed bounded.

Claim 7.37. *There exists a constant $c \in (0, 0.1)$ such that for any $z^k x^{(m+1)\times k} \in \mathrm{Supp}(P_{Z^k X^{(m+1)\times k}})$ and $i \in [k]$, it holds that $i \in \mathcal{G}^{\alpha}_{z^k x^{(m+1)\times k}}$ if all the following conditions hold:*

1. $\frac{R_{Z_i}(z_i)}{P_{Z_i}(z_i)} \in 1 \pm c$, *and*

2. $\frac{P_{X_{1,i}|Z^k}(1|z^k)}{P_{X_{1,i}|Z_i}(1|z_i)} \in 1 \pm c$, *and*

3. $i \in \mathcal{G}^{\gamma}_{z^k x^{(m+1)\times k}} \bigcap \mathcal{G}^{\rho}_{z^k x^{(m+1)\times k}}$, *and*

4. $\sum_{j=1}^{m} \xi_{j,i}(z^k x^k_{<j}) \leq c$, *and*

5. $\sum_{j=2}^{m+1} \widehat{\beta}^2_{j,i}(z^k x^k_{<j}) \leq c$, *and*

6. $\max\{\left|\sum_{j'=2}^{j} \widehat{\beta}_{j',i}(z^k x^k_{<j})\right|\}_{j=2}^{m+1} \leq c$.

Proof. Fix $j \in [m+1]$ and recall that

$$\alpha_{j,i} = \frac{R_{Z_i}(z_i)}{P_{Z_i}(z_i)} \cdot \frac{P_{X_{1,i}|Z^k}(1|z^k)}{P_{X_{1,i}|Z_i}(1|z_i)} \cdot \prod_{j'=2}^{j}(1+\beta_{j',i})$$

By assumption, it holds that $\left|\gamma_{j'-1,i}\right|, \left|\rho_{j'-1,i}\right|, \sum_{j'=2}^{j} \xi_{j'-1,i} \leq 0.1$ for any $j' \in [j] \setminus \{1\}$. In particular, this yields that for any such j' it holds that

a. $\widehat{\beta}_{j',i} = \beta_{j',i} + \xi_{j'-1,i} - \beta^U_{j',i} + \mu_{j'-1,i}$.

b. $\beta^U_{j',i} = \frac{1}{m-1}$.

c. $\beta_{j',i} = \frac{1+\gamma_{j',i}}{1+\rho_{j'-1,i}} \cdot \frac{m}{m-1} - 1 \geq \frac{0.9}{1.1} \cdot \frac{m}{m-1} - 1 \geq -0.2$.

Using the above observations, we prove that $\alpha_{j,i} \in [0.01, 10]$. Note that the upper bound holds since

$$\begin{aligned}
\alpha_{j,i} &\leq (1+c)^2 \cdot e^{\sum_{j'=2}^{j} \beta_{j',i}} \\
&= (1+c)^2 \cdot e^{\sum_{j'=2}^{j}(\widehat{\beta}_{j',i} - \xi_{j'-1,i} + \beta^U_{j',i} - \mu^U_{j'-1,i})} \\
&\leq (1+c)^2 \cdot e^{c - 0 + \frac{j-1}{m-1} + \frac{0.1\cdot(j-1)}{m-1}} \\
&\leq (1+c)^2 \cdot e^{c+2.2}
\end{aligned}$$

and the lower bound holds since

$$\begin{aligned}
\alpha_{j,i} &\geq (1-c)^2 \cdot e^{\sum_{j'=1}^{j} \beta_{j',i}} \cdot e^{-\sum_{j'=1}^{j} \beta^2_{j',i}} \\
&= (1-c)^2 \cdot e^{\sum_{j'=2}^{j}(\widehat{\beta}_{j',i} - \xi_{j'-1,i} + \beta^U_{j',i} - \mu^U_{j'-1,i})} \cdot e^{-0.6\cdot\sum_{j'=1}^{j}(\widehat{\beta}_{j',i} - \xi_{j'-1,i} + \beta^U_{j',i} - \mu^U_{j'-1,i})^2} \\
&\geq (1-c)^2 \cdot e^{-c-c+\frac{j-1}{m-1} - \frac{0.1\cdot(j-1)}{m-1}} \cdot e^{0.6\cdot\left(-6\sum_{j'=1}^{j}\left(\widehat{\beta}^2_{j',i} + \xi^2_{j'-1,i} + (\frac{\gamma_{j'-1,i}}{m-1})^2\right) - 2\sum_{j'=1}^{j}(\beta^U_{j',i})^2\right)} \\
&\geq (1-c)^2 \cdot e^{-2c} \cdot e^{-4\left(c + c^2 + (\frac{0.1}{m-1})^2\cdot(j-1)\right) - 4} \\
&= (1-c)^2 \cdot e^{-6c-4c^2-4.08},
\end{aligned}$$

where the first inequality holds by the fact that $1 + x \geq e^{x-0.6x^2}$ for $x \geq -0.2$, the second one holds by the fact that $(a+b+c+d)^2 \leq 2\left((a+b+c)^2 + d^2\right) \leq 6(a^2+b^2+c^2) + 2d^2$ and the last one holds since $\sum_{j'=2}^{j} \widehat{\beta}^2_{j',i} \leq c$ and $\sum_{j'=1}^{j} \xi^2_{j',i} \leq \sum_{j=1}^{m} \xi_{j,i} \leq c$ and $\sum_{j'=1}^{j}(\beta^U_{j',i})^2 \leq \frac{m}{(m-1)^2} \leq 2$ and $(\frac{0.1}{m-1})^2 \cdot (j-1) \leq \frac{0.01m}{(m-1)^2} \leq 0.02$. By taking $c = 0.01$ we obtain that $\alpha_{j,i} \in [0.01, 10]$, as required. □

As a corollary of all the claims of this section, we are finally ready to prove Claim 7.16.

Putting it Together

Corollary 7.38 (Restatement of Claim 7.16)**.** *For any constant $\lambda > 0$, there exists a constant $\lambda' > 0$ such that if* $\mathrm{E}_P\big[\mathrm{jumps}^{\alpha}(Z^k X^{(m+1)\times k})\big] \geq \varepsilon k/\lambda$*, then* $R[W] \leq (1-\varepsilon)^{\frac{k}{\lambda'\cdot m}}$*.*

Proof. Let c be the constant from Claim 7.37. Observe that Claim 7.37 implies that

$$\begin{aligned}
\mathbb{1}\{u_i^{\alpha} < \infty\} \leq \mathbb{1}\{\frac{R_{Z_i}(z_i)}{P_{Z_i}(z_i)} \notin 1 \pm c\} + \mathbb{1}\{\frac{P_{X_{1,i}|Z^k}(1|z^k)}{P_{X_{1,i}|Z_i}(1|z_i)} \notin 1 \pm c\}\\
+ \mathbb{1}\{u^{|\gamma|>0.1} < \infty\} + \mathbb{1}\{u^{|\rho|>0.1} < \infty\} + \mathbb{1}\{\sum_{j=1}^{m} \xi_{j,i} > c\}\\
+ \mathbb{1}\{\sum_{j=2}^{m+1} \widehat{\beta}_{j,i}^2 > c\} + \mathbb{1}\{\max\{\left|\sum_{j'=2}^{j} \widehat{\beta}_{j',i}\right|\}_{j=2}^{m+1} > c\}
\end{aligned}$$

Therefore, by assumption (recall that $\mathrm{jumps}^{\alpha}(Z^k X^{(m+1)\times k}) = \sum_{i=1}^{k} \mathbb{1}\{u_i^{\alpha} < \infty\}$), when summing over $i \in [k]$ and taking expectation over P, the sum of all the right side terms is at least $\frac{\varepsilon k}{\lambda}$. If one of the first five terms have expected sum $\geq \frac{\varepsilon k}{10\lambda}$, then the proof follows by Claims 7.30 and 7.31 and Corollaries 7.23, 7.27 and 7.35. Otherwise, it holds that

$$\mathrm{E}_P\left[\sum_{i=1}^{k}\left(\mathbb{1}\{\sum_{j=2}^{m+1} \widehat{\beta}_{j,i}^2 > c\} + \mathbb{1}\{\max\{\left|\sum_{j'=2}^{j} \widehat{\beta}_{j,i}\right|\}_{j=1}^{m+1} > c\}\right)\right] \geq \frac{\varepsilon k}{2\lambda} \tag{90}$$

For $i \in [k]$, let $q_i = \mathrm{E}_P\left[\sum_{j=2}^{m+1} \widehat{\beta}_{j,i}^2\right]$. Note that Claim 7.32 (property 2) yields that the sequence $\{\widehat{\beta}_{j,i}(Z^k X_{<j}^k)\}_{j=2}^{m+1}$ is a martingale difference sequence with respect to $\{P_{X_j^k|Z^k X_{<j}^k}\}_{j=1}^{m}$ (for any fixing of Z^k). Therefore, Fact 3.17 yields that $P\left[\max\{\left|\sum_{j'=2}^{j} \widehat{\beta}_{j,i}\right|\}_{j=1}^{k} > c\right] \leq q_i/c^2$ which implies that

$$\mathrm{E}_P\left[\mathbb{1}\{\max\{\left|\sum_{j'=2}^{j} \widehat{\beta}_{j,i}\right|\}_{j=2}^{m+1} > c\}\right] \leq q_i/c^2. \tag{91}$$

Moreover, by Markov inequality, it holds that $P\left[\sum_{j=2}^{m+1} \widehat{\beta}_{j,i}^2(Z^k X_{<j}^k) > c\right] \leq q_i/c$ which implies that

$$\mathrm{E}_P\left[\mathbb{1}\{\sum_{j=2}^{m+1} \widehat{\beta}_{j,i}^2 > c\}\right] \leq q_i/c \tag{92}$$

Hence, Equations (90) to (92) yields that

$$\begin{aligned}
(1/c + 1/c^2)\sum_{i=1}^{k} q_i \geq \mathrm{E}_P\left[\sum_{i=1}^{k}\left(\mathbb{1}\{\sum_{j=2}^{m+1} \widehat{\beta}_{j,i}^2 > c\} + \mathbb{1}\{\max\{\left|\sum_{j'=2}^{j} \widehat{\beta}_{j,i}\right|\}_{j=1}^{m+1} > c\}\right)\right]\\
\geq \frac{\varepsilon k}{2\lambda}\\
\implies \mathrm{E}_P\left[\sum_{j=2}^{m+1}\sum_{i=1}^{k} \widehat{\beta}_{j,i}^2\right] = \sum_{i=1}^{k} q_i \geq \frac{\varepsilon k}{2\lambda \cdot (1/c + 1/c^2)}
\end{aligned}$$

and the proof follows by Claim 7.36. □

8 Lower Bound

In this section we present the counterexample that proves Theorem 1.3. In Section 8.1 we start by showing how random termination helps to beat [BIN97]'s counterexample, and in Section 8.2 we restate and prove Theorem 1.3 using a variant of [BIN97]'s protocol.

8.1 Random Termination Beats Counterexample of [BIN97]

In this section we exemplify the power of random termination, showing that the counterexample of [BIN97] does not apply to random-terminating verifiers. We do so by presenting [BIN97]'s counterexample against k repetitions and see how random termination helps in this case. The protocol is described below.

Protocol 8.1 ([BIN97]'s Protocol $\pi = (\mathrm{P}, \mathrm{V})$)**.**

Common input: Public key pk .

Prover's private input: Secret key sk.

Operation:

1. *Round* 1*:*
   (a) V *uniformly samples* $b \leftarrow \{0,1\}$ *and* $r \leftarrow \{0,1\}^n$*, and sends* $B = \mathrm{Enc}_{pk}(b,r)$ *to* P*.*
   (b) P *computes* $(b,r) = \mathrm{Dec}_{sk}(B)$ *and for any* $i \in [k-1]$*, it uniformly samples* $b'_i \in \{0,1\}$ *and* $r'_i \in \{0,1\}^n$ *conditioned on* $b = \oplus_{i=1}^{k-1} b'_i$*. Then it computes* $C_i = \mathrm{Enc}_{pk}(b'_i, r'_i)$*, and sends* $(C_1, \ldots, C_{k-1})$ *to* V*.*
2. *Round* 2*:*
   (a) V *sends* (b,r) *to* P*.*
   (b) P *sends* $\big((b'_1, r'_1), \ldots, (b'_{k-1}, r'_{k-1})\big)$ *to* V*.*
3. *At the end:* V *accepts iff* $b = \oplus_{i=1}^{k-1} b'_i$*, and for any* $i \in [k-1]$*:* $C_i = \mathrm{Enc}_{pk}(b'_i, r'_i)$ *and* $B \neq C_i$*.*

Intuitively, assuming the cryptosystem is CCA2-secure, if a single instance of the protocol is run, then a prover without access to sk can only convince the honest verifier with probability $1/2$, since it must commit itself to a guess $\oplus_{i=1}^{k-1} b'_i$ of b before receiving (b,r). On the other hand, if k instances of the protocol are run in parallel, then a cheating prover can send the tuple $(C_1, \ldots, C_{k-1}) = (B_1, \ldots, B_{i-1}, B_{i+1}, \ldots, B_k)$ to V_i and then either all verifier instances accept or all verifier instances fail, the first event occurring with probability at least $1/2$.

Let's look now on a k instances that run in parallel of the protocol $\pi = (\mathrm{P}, \widetilde{\mathrm{V}})$, where $\widetilde{\mathrm{V}}$ is the random-terminating variant of V (note that this protocol has only two rounds, and therefore, a random terminating bit takes one with probability $1/2$). First, we expect that $\approx k/2$ of the verifiers abort at the first round, and with high probability at least $k/4$ of the verifiers remain active (assume that k is large enough). For a cheating prover, aborting at the first round is not an issue since it can completely simulate the aborted verifiers. However, even if a single verifier V_i

aborts at the second round, then the attack presented above completely fail since the prover has no way to reveal (b_i, r_i), needed for the other verifiers. Note that the attack do succeed in case non of the verifiers abort at the second round, but the probability of this to happen is at most $2^{-k/4}$.

8.2 Proving Theorem 1.3

In this section, we restate and prove Theorem 1.3.

Theorem 8.2 (Restatement of Theorem 1.3)**.** *Assume the existence of CCA2-secure public-key cryptosystem. Then for every $m = m(n) \in [2, \mathrm{poly}(n)]$ and $\varepsilon = \varepsilon(n) \in [1/\mathrm{poly}(n), 1/3]$ and $k = k(n) \in [m/\varepsilon, \mathrm{poly}(n)]$, there exists an m-round interactive argument (P, V) with soundness error $1-\varepsilon$ such that $(\mathrm{P}^k, \widetilde{\mathrm{V}}^k)$ has soundness error of at least $(1-\varepsilon)^{c \cdot k/m}$ for some universal constant $c > 0$, where $\widetilde{\mathrm{V}}$ is the $1/m$-random-terminating variant of V (according to Definition 3.21) and $(\mathrm{P}^k, \widetilde{\mathrm{V}}^k)$ denotes the k-parallel repetition of $(\mathrm{P}, \widetilde{\mathrm{V}})$ (according to Definition 3.22).*[26]

In the following, fix large enough n and fix m, ε, k as in the theorem statements, and let $\mathrm{CS} = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ be a CCA2-secure public-key cryptosystem. Consider the following m-round variant (P, V) of [BIN97]'s protocol:

Protocol 8.3 (The counterexample protocol $\pi = (\mathrm{P}, \mathrm{V})$)**.**

Common input: Security parameter 1^n and Public key pk .

Prover's private input: Secret key sk.

Operation:

1. *Round 1:*
   (a) *V flips a coin that takes one with probability $1 - 3\varepsilon$ and zero otherwise.*
   If the coin outcome is one, V sends $\perp$ to P, accepts and the protocol terminates.
   Else, V uniformly samples $b \leftarrow \{0, 1\}$ and $r \leftarrow \{0, 1\}^n$, and sends $B = \mathrm{Enc}_{pk}(b, r)$ to P.

   (b) *P computes $(b, r) = \mathrm{Dec}_{sk}(B)$ and for any $i \in [k-1]$, it uniformly samples $b'_i \in \{0, 1\}$ and $r'_i \in \{0, 1\}^n$ conditioned on $b = \oplus_{i=1}^{k-1} b'_i$. Then it computes $C_i = \mathrm{Enc}_{pk}(b'_i, r'_i)$, and sends $(C_1, \ldots, C_{k-1})$ to V.*

2. *Round 2:*
   (a) *V sends (b, r) to P.*

   (b) *P sends $\big((b'_1, r'_1), \ldots, (b'_{k-1}, r'_{k-1})\big)$ to V.*

3. *Rounds 3 to m: parties exchange dummy messages.*

4. *At the end: V accepts iff $b = \oplus_{i=1}^{k-1} b'_i$, and for every $i \in [k-1]$: $C_i = \mathrm{Enc}_{pk}(b'_i, r'_i)$ and $B \neq C_i$.*

[26] Assuming the existence of collision-free family of hash functions and CCA2-secure cryptosystem with respect to superpolynomial adversaries, one can adopt the techniques used in [PW12] for constructing a single protocol (P, V) such that for any polynomial bounded k, $(\mathrm{P}^k, \widetilde{\mathrm{V}}^k)$ has soundness error of at least $(1 - \varepsilon)^{c \cdot k/m}$. This, however, is beyond the scope of this paper.

Namely, Protocol 8.3 first transforms [BIN97]'s two-rounds protocol, of soundness error $1/2 + \mathrm{neg}(n)$, into an m-round protocol with soundness error $1 - \varepsilon$, by flipping a coin at Step 1a (for increasing the soundness error) and adding dummy rounds at the end for increasing the number of rounds (Step 3).[27]

We first note that soundness error of π is indeed low.

Claim 8.4. *The soundness error of $\pi(1^n)$ is at most $1 - \varepsilon$.*

Proof. Let P^* be some efficient cheating prover and let T be the event over a random execution of $(\mathrm{P}^*, \mathrm{V})$ that the outcome of the $(1-3\varepsilon, 3\varepsilon)$ bit (flipped by V at Step 1a) is 0 (i.e., V does not abort). Conditioned on T, P^* must commit itself to a guess $\oplus_{i=1}^{k-1} b_i'$ before receiving (b, r). Since the encryption scheme is CCA2-secure (which implies non-malleability), we obtain that

$$\Pr_{(pk,sk)\leftarrow \mathrm{Gen}(1^n)}[(\mathrm{P}^*, \mathrm{V})(1^n, pk) = 1 \mid T] \le 1/2 + \mathrm{neg}(n),$$

and hence

$$\begin{aligned}\Pr_{(pk,sk)\leftarrow \mathrm{Gen}(1^n)}[(\mathrm{P}^*, \mathrm{V})(1^n) = 1] &\le \Pr[\neg T] + \Pr[T] \cdot \Pr_{(pk,sk)\leftarrow \mathrm{Gen}(1^n)}[(\mathrm{P}^*, \mathrm{V})(1^n, pk) = 1 \mid T] \\ &\le 1 - 3\varepsilon + 3\varepsilon \cdot (1/2 + \mathrm{neg}(n)) \\ &\le 1 - \varepsilon.\end{aligned}$$

□

So it is left to show that the soundness error of the k parallel repetition of the random terminating variant of π is high. Let $\widetilde{\mathrm{V}}$ and $(\mathrm{P}^k, \widetilde{\mathrm{V}}^k)$ be as in the theorem statement with respect to (P, V) (Protocol 8.3) and assume without loss of generality that $\widetilde{\mathrm{V}}$ sends $\perp$ to the prover right after flipping a termination coin with outcome one. Consider the following cheating prover P^{k^*}:

Algorithm 8.5 (Cheating prover P^{k^*})**.**

Input: *Security parameter 1^n.*

Operation:

1. *Upon receiving a k-tuple $(a_1, \ldots, a_k)$ from $\widetilde{\mathrm{V}}^k = (\widetilde{\mathrm{V}}_1, \ldots, \widetilde{\mathrm{V}}_k)$, let $\mathcal{S} = \{i \in [k] \colon a_i \ne \perp\}$ (the set of active verifiers) and for $i \notin \mathcal{S}$ sample uniformly $b_i \leftarrow \{0,1\}$ and $r_i \leftarrow \{0,1\}^n$. Then for any $i \in \mathcal{S}$ send $(a_1', \ldots, a_{i-1}', a_{i+1}', \ldots, a_k')$ to $\widetilde{\mathrm{V}}_i$, where $a_j' = \begin{cases} a_j & j \in \mathcal{S} \\ \mathrm{Enc}_{pk}(b_j, r_j) & o.w \end{cases}$.*
2. *If at least one verifier in $\mathcal{S}$ sends $\perp$ (after aborting at the second round), fail and abort. Otherwise, upon receiving (b_i, r_i) for all $i \in \mathcal{S}$, send the tuple $((b_1, r_1), \ldots, (b_{i-1}, r_{i-1}), (b_{i+1}, r_{i+1}), \ldots, (b_k, r_k))$ to $\widetilde{\mathrm{V}}_i$.*

Namely, P^{k^*} performs [BIN97]'s attack on the verifiers that remain active after the first round. The attack, however, can only be performed if none of these active verifiers abort in the second round. Yet, we show that the probability for this to happen is high enough. The following claim conclude the proof of Theorem 8.2.

[27] As in [BIN97; PW12], the soundness error holds with respect to a prover without access to sk.

Claim 8.6. *Let ε, m, k as in the theorem statement, let (P, V) be Protocol 8.3 and let P^{k^*} be the cheating prover described in Algorithm 8.5 (with respect to k). Then*

$$\Pr_{(pk,sk)\leftarrow \mathrm{Gen}(1^n)}\left[(\mathrm{P}^{k^*}, \widetilde{\mathrm{V}}^k)(1^n, pk) = 1\right] \geq (1-\varepsilon)^{14\cdot k/m}.$$

Proof. Fix pk and let L be the random variable that denotes the value of $|\mathcal{S}|$ (the number of active verifiers after the first round) in a random execution of $(\mathrm{P}^{k^*}, \widetilde{\mathrm{V}}^k)(1^n, pk)$. Note that each verifier aborts with probability greater than $1 - 3\varepsilon$ at the first round (it can abort by the $(1-3\varepsilon, 3\varepsilon)$ coin or by the $(1/m, 1-1/m)$ random-terminating coin). Therefore, $\mathrm{E}[L] \leq 3\varepsilon k$ and we obtain by Markov's inequality that $\Pr[L \leq 6\varepsilon k] \geq 1/2$. Let G be the event that none of the verifiers abort at the second round. Note that

$$\begin{aligned}\Pr[G] &\geq \Pr[L \leq 6\varepsilon k] \cdot \Pr[G | L \leq 6\varepsilon k] \\ &\geq 1/2 \cdot (1-1/m)^{6\varepsilon k} \\ &\geq 1/2 \cdot \exp(-12\varepsilon k/m).\end{aligned} \tag{93}$$

The second inequality holds since $1 - x \geq e^{-2x}$ for $x \in [0, 1/2]$. In addition, observe that

$$\begin{aligned}\Pr\left[(\mathrm{P}^{k^*}, \widetilde{\mathrm{V}}^k)(1^n, pk) = 1 \mid G\right] &\geq \Pr_{(b_1,\ldots,b_k)\leftarrow\{0,1\}^k}\left[\oplus_{i=1}^k b_i = 0\right] - \mathrm{neg}(n) \\ &= 1/2 - \mathrm{neg}(n)\end{aligned} \tag{94}$$

and we conclude by Equations (93) and (94) that

$$\begin{aligned}\Pr\left[(\mathrm{P}^{k^*}, \widetilde{\mathrm{V}}^k)(1^n, pk) = 1\right] &\geq \Pr[G] \cdot \Pr\left[(\mathrm{P}^{k^*}, \widetilde{\mathrm{V}}^k)(1^n, pk) = 1 \mid G\right] \\ &\geq 1/2 \cdot \exp(-12\varepsilon k/m) \cdot (1/2 - \mathrm{neg}(n)) \\ &\geq \exp(-14\varepsilon k/m) \\ &\geq (1-\varepsilon)^{14k/m}.\end{aligned}$$

The penultimate inequality holds since we assumed that $k \geq m/\varepsilon$, and the last one since $1 + x \leq e^x$ for any $x \in \mathbb{R}$. □

Acknowledgment

We thank Chris Brzuska, Or Ordentlich and Yury Polyanskiy for very useful discussions.

References

[BC12] N. Bitansky and A. Chiesa, "Succinct arguments from multi-prover interactive proofs and their efficiency benefits," in *Annual Cryptology Conference*, 2012, pp. 255–272 (cit. on p. 2).

[BIN97] M. Bellare, R. Impagliazzo, and M. Naor, "Does parallel repetition lower the error in computationally sound protocols?" In *38th Annual Symposium on Foundations of Computer Science, FOCS '97, Miami Beach, Florida, USA, October 19-22, 1997*, 1997, pp. 374–383 (cit. on pp. 1, 2, 5, 8, 95–97).

[BV14] Z. Brakerski and V. Vaikuntanathan, "Efficient fully homomorphic encryption from (standard) lwe," *Journal of the ACM*, vol. 43, no. 2, pp. 831–871, 2014 (cit. on p. 2).

[CHS05] R. Canetti, S. Halevi, and M. Steiner, "Hardness amplification of weakly verifiable puzzles," in *Theory of Cryptography, Second Theory of Cryptography Conference, TCC 2005*, 2005, pp. 17–33 (cit. on p. 5).

[Chu+13] K.-M. Chung, R. Ostrovsky, R. Pass, and I. Visconti, "Simultaneous resettability from one-way functions," in *2013 IEEE 54th Annual Symposium on Foundations of Computer Science*, 2013, pp. 60–69 (cit. on p. 2).

[CL02] F. Chung and L. Lu, "Connected components in random graphs with given expected degree sequences," 2002. [Online]. Available: https://link.springer.com/content/pdf/10.1007/PL00012580.pdf (cit. on pp. 1, 22).

[CL10] K. Chung and F. Liu, "Parallel repetition theorems for interactive arguments," in *Theory of Cryptography, Sixth Theory of Cryptography Conference, TCC 2010*, 2010, pp. 19–36 (cit. on pp. 2, 5, 8).

[CO13] A. Coja-Oghlan, "Probabilistic combinatorics," 2013. [Online]. Available: https://www.math.uni-frankfurt.de/~acoghlan/probcomb.pdf (cit. on p. 22).

[CP11] K.-M. Chung and R. Pass, "The randomness complexity of parallel repetition," in *Proceedings of the 52nd Annual Symposium on Foundations of Computer Science (FOCS)*, 2011, pp. 658–667 (cit. on p. 5).

[CP15] K. Chung and R. Pass, "Tight parallel repetition theorems for public-coin arguments using kl-divergence," in *Theory of Cryptography, 11th Theory of Cryptography Conference, TCC 2015*, 2015, pp. 229–246 (cit. on pp. 1, 4–6, 8, 9, 41).

[Das11] A. DasGupta, *Probability for Statistics and Machine Learning. Chapter 14: Discrete Time Martingales and Concentration Inequalities*. 2011. [Online]. Available: https://www.researchgate.net/publication/226263860_Discrete_Time_Martingales_and_Concentration_Inequalities (cit. on p. 23).

[Dod+12] Y. Dodis, A. Jain, T. Moran, and D. Wichs, "Counterexamples to hardness amplification beyond negligible," in *Theory of Cryptography, 8th Theory of Cryptography Conference, TCC 2012*, 2012, pp. 476–493 (cit. on p. 2).

[DP98] I. B. Damgärd and B. Pfitzmann, "Sequential iteration arguments and an efficientzero-knowledge argument for NP," in *Annual International Colloquium on Automata, Languages and Programming (ICALP)*, 1998, pp. 772–783 (cit. on p. 1).

[DS14] I. Dinur and D. Steurer, "Analytical approach to parallel repetition," in *Symposium on Theory of Computing, STOC 2014, New York, NY, USA, May 31 - June 03, 2014*, 2014, pp. 624–633 (cit. on p. 6).

[Duc16] J. Duchi, "Lecture notes for statistics 311/electrical engineering 377," 2016. [Online]. Available: https://stanford.edu/class/stats311/Lectures/full_notes.pdf (cit. on p. 102).

[DV83] M. D. Donsker and S. R. S. Varadhan, "Asymptotic evaluation of certain markov process expectations for large time. iv," *Communications on Pure and Applied Mathematics*, vol. 36, no. 2, pp. 183–212, 1983 (cit. on p. 13).

[Fei91] U. Feige, "On the success probability of the two provers in one-round proof systems," in *Proceedings of the Sixth Annual Structure in Complexity Theory Conference, Chicago, Illinois, USA, June 30 - July 3, 1991*, 1991, pp. 116–123 (cit. on p. 5).

[FRS90] L. Fortnow, J. Rompel, and M. Sipser, "Errata for on the power of multi-prover interactive protocols," in *Proceedings: Fifth Annual Structure in Complexity Theory Conference, Universitat Politècnica de Catalunya, Barcelona, Spain, July 8-11, 1990*, 1990, pp. 318–319 (cit. on p. 5).

[FV02] U. Feige and O. Verbitsky, "Error reduction by parallel repetition - A negative result," *Combinatorica*, vol. 22, no. 4, pp. 461–478, 2002 (cit. on p. 5).

[Gol99] O. Goldreich, *Modern Cryptography, Probabilistic Proofs and Pseudorandomness.* Springer, 1999 (cit. on p. 1).

[Hai13] I. Haitner, "A parallel repetition theorem for any interactive argument," *SIAM J. Comput.*, vol. 42, no. 6, pp. 2487–2501, 2013. DOI: 10.1137/100810630. [Online]. Available: https://doi.org/10.1137/100810630 (cit. on pp. 1–7, 9, 14, 23, 24, 26).

[Hol09] T. Holenstein, "Parallel repetition: Simplification and the no-signaling case," *Theory of Computing*, vol. 5, no. 1, pp. 141–172, 2009 (cit. on p. 6).

[Hås+10] J. Håstad, R. Pass, D. Wikström, and K. Pietrzak, "An efficient parallel repetition theorem," in *Theory of Cryptography, Sixth Theory of Cryptography Conference, TCC 2010*, 2010, pp. 1–18 (cit. on pp. 1, 5, 7, 14, 23).

[IL89] R. Impagliazzo and M. Luby, "One-way functions are essential for complexity based cryptography," in *Proceedings of the 30th Annual Symposium on Foundations of Computer Science (FOCS)*, 1989, pp. 230–235 (cit. on p. 8).

[Mos14] D. Moshkovitz, "Parallel repetition from fortification," in *55th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2014, Philadelphia, PA, USA, October 18-21, 2014*, 2014, pp. 414–423 (cit. on p. 6).

[Mul] W. Mulzer, *Chernoff bounds*. [Online]. Available: https://page.mi.fu-berlin.de/mulzer/notes/misc/chernoff.pdf (cit. on p. 19).

[Pat90] J. Patarin, "Pseudorandom permutations based on the DES scheme," in *EUROCODE '90, International Symposium on Coding Theory and Applications, Udine, Italy, November 5-9, 1990, Proceedings*, 1990, pp. 193–204. DOI: 10.1007/3-540-54303-1_131. [Online]. Available: https://doi.org/10.1007/3-540-54303-1_131 (cit. on p. 11).

[PV12] R. Pass and M. Venkitasubramaniam, "A parallel repetition theorem for constant-round arthur-merlin proofs," *TOCT*, vol. 4, no. 4, 10:1–10:22, 2012 (cit. on p. 5).

[PW12] K. Pietrzak and D. Wikström, "Parallel repetition of computationally sound protocols revisited," *Journal of Cryptology*, vol. 25, no. 1, pp. 116–135, 2012 (cit. on pp. 1, 5, 8, 96, 97).

[PW17] Y. Polyanskiyi and Y. Wu, "Lecture notes on information theroy," 2017. [Online]. Available: http://people.lids.mit.edu/yp/homepage/data/itlectures_v5.pdf (cit. on p. 101).

[Rao11] A. Rao, "Parallel repetition in projection games and a concentration bound," *SIAM J. Comput.*, vol. 40, no. 6, pp. 1871–1891, 2011 (cit. on p. 6).

[Raz98] R. Raz, "A parallel repetition theorem," *SIAM J. Comput.*, vol. 27, no. 3, pp. 763–803, 1998 (cit. on pp. 1, 5, 8).

[Rom90] J. Rompel, "One-way functions are necessary and sufficient for secure signatures," in *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing (STOC)*, 1990, pp. 387–394 (cit. on p. 8).

[Ver10] R. Vershynin, "Introduction to the non-asymptotic analysis of random matrices," *ArXiv e-prints*, Nov. 2010. arXiv: 1011.3027 [math.PR]. [Online]. Available: https://arxiv.org/abs/1011.3027 (cit. on p. 102).

A Missing Proofs

A.1 Proof of Proposition 3.10

Proposition A.1 (Restatement of Proposition 3.10)**.** *Let X be a random variable drawn form either P or Q. Assume that $\Pr_P[|X| \leq 1] = 1$ (i.e., if X is drawn from P then $|X| \leq 1$ almost surely) and that there exist $\varepsilon, \sigma^2, K_1, K_2 > 0$ such that $\Pr_Q[|X| \leq 1] \geq 1 - \varepsilon$ and*

$$\Pr_Q[|X| \geq t] \leq K_2 \cdot \exp\left(-\frac{t^2}{K_1 \sigma^2}\right) \quad \text{for all } 0 \leq t \leq 1.$$

Then, there exists $K_3 = K_3(K_1, K_2, \varepsilon) > 0$ such that

$$\mathrm{E}_P[X^2] \leq K_3 \cdot \sigma^2 \cdot (D(P||Q) + 1).$$

Note that for $\sigma \geq 1$, the statement is trivial, and thus not interesting. We would use this proposition when $\sigma \ll 1$.

Proof. Assume that $\sigma^2 \leq 1$ and that $D(P||Q) < \infty$, since otherwise the statement is trivial. We use the following two fundamental theorems. The first theorem gives a variational characterization for divergence that is useful for bounding expected values of random variables.

Theorem A.2 (Donsker-Varadhan; cf. [PW17, Theorem 3.5])**.** *Let P and Q be probability measures on $\mathcal{X}$ and let $\mathcal{C}$ denote the set of functions $f\colon \mathcal{X} \to \mathbb{R}$ such that $\mathrm{E}_Q[\exp(f(X))] < \infty$. If $D(P||Q) < \infty$, then*

$$D(P||Q) = \sup_{f \in \mathcal{C}} \mathrm{E}_P[f(X)] - \log \mathrm{E}_Q[\exp(f(X))].$$

In particular, for every $f \in \mathcal{C}$, it holds that

$$\mathrm{E}_P[f(X)] \leq \log \mathrm{E}_Q[\exp(f(X))] + D(P||Q).$$

The second theorem is the super-exponential moment characterization condition for sub-Gaussianity.

Theorem A.3 (Sub-Gaussian characterization; cf. [Duc16, Theorem 3.10][28])**.** *Let X be a random variable and $\sigma^2 > 0$ be a constant. Assume that there exist $K_1', K_2' > 0$ such that*

$$\Pr[|X| \geq t] \leq K_2' \cdot \exp\left(-\frac{t^2}{K_1'\sigma^2}\right) \quad \textit{for all } t \geq 0.$$

Then, there exists $K_3' = K_3'(K_1', K_2')$ such that

$$\mathrm{E}\left[\exp\left(\frac{X^2}{K_3'\sigma^2}\right)\right] \leq e.$$

We would like to apply the above theorems to derive the proof. However, under the Q distribution X is not sub-Gaussian, since its concentration bound apply only for $0 \leq t \leq 1$. Instead, we let $\mathcal{W} = [0, 1]$, $K_2' = K_2/(1-\varepsilon)$ and observe that

$$\Pr_Q[|X| \geq t \mid |X| \in \mathcal{W}] \leq K_2' \cdot \exp\left(-\frac{t^2}{K_1\sigma^2}\right) \quad \text{for all } t \geq 0.$$

Indeed, for $t > 1$ this inequality holds trivially. For $0 \leq t \leq 1$, it holds that

$$\begin{aligned}\Pr_Q[|X| \geq t \mid |X| \in \mathcal{W}] &\leq \frac{\Pr_Q[|X| \geq t]}{\Pr_Q[|X| \in \mathcal{W}]}\\ &\leq \frac{\Pr_Q[|X| \geq t]}{1-\varepsilon}\\ &\leq K_2' \cdot \exp\left(-\frac{t^2}{K_1\sigma^2}\right),\end{aligned}$$

where the second inequality follows from the assumption of the proposition and since $\sigma^2 \leq 1$, and the third inequality again follows from the assumption of the proposition.

Let $K_3 = K_3'(K_1, K_2')$ from the statement of Theorem A.3. Furthermore, note that $D(P_X||Q_{X|(|X|\in\mathcal{W})}) < \infty$, since $D(P_X||Q_X) < \infty$ and $|X| \in \mathcal{W}$ under P almost surely. Using Theorems A.2 and A.3, it follows that

$$\begin{aligned}\frac{1}{K_2\sigma^2}\mathrm{E}_P[X^2] &\leq \log \mathrm{E}_Q[\exp(X^2/(K_2\sigma^2))||X| \in \mathcal{W}] + D(P_X||Q_{X|(|X|\in\mathcal{W})})\\ &\leq \log e + D(P_X||Q_{X|(|X|\in\mathcal{W})}).\end{aligned}$$

Finally, the proposition follows since

$$\begin{aligned}D(P_X||Q_{X|(|X|\in\mathcal{W})}) &= \mathrm{E}_{x\sim P_X} \log \frac{P_X(x)}{Q_X(x)/\Pr_Q[|X| \in \mathcal{W}]}\\ &= D(P_X||Q_X) + \log(\Pr_Q[|X| \in \mathcal{W}])\\ &\leq D(P_X||Q_X),\end{aligned}$$

where in the first equality we again used that $|x| \in \mathcal{W}$ for every $x \in \mathrm{Supp}(P_X)$, so $\Pr_Q[X = x \wedge |X| \in \mathcal{W}] = Q_X(x)$ for any such x. □

[28] While the statement of [Duc16, Theorem 3.10] explicitly take $K_2' = 2$ and require that X's mean is zero, it is easy to see how to modify the proof to work with any constant K_2' and that the proof of this part does not actually use that X has a zero mean. For example, see [Ver10, Lemma 5.5] that uses $K_2' = e$ and does not assume that X has zero mean.

A.2 Proof of Proposition 2.1

Proposition A.4 (Restatement of Proposition 2.1)**.** *Let $m, k \in \mathbb{N}$, let $P = P_{Y_1,\ldots,Y_m}$ be a distribution and let $\{E_{j,i}\}_{j\in[m],i\in[k]}$ be a set of events over P. Let $Q = Q_{I,Y_1,\ldots,Y_m} = Q_I \cdot \prod_{j=1}^m Q_{Y_j|Y_{<j},I}$ be the distribution such that Q_I is a distribution over $[k]$ and for $j \in [m]$: $Q_{Y_j|Y_{<j},I} = \begin{cases} P_{Y_j|Y_{<j},E_{j,I}} & P[E_{j,I} \mid Y_{<j}] > 0 \\ \perp & o.w \end{cases}$. Assume that for any $j \in [m]$, $i \in [k]$ and $y_{\leq j} \in \operatorname{Supp}(Q_{Y_{\leq j}})$ it holds that $P[E_{j,i} \mid Y_{<j} = y_{<j}] > 0$, and let $\alpha_{j,i}(y_{\leq j}) = Q[I = i] \cdot \prod_{j'=1}^{j} \frac{P[E_{j',i}|Y_{\leq j'}=y_{\leq j'}]}{P[E_{j',i}|Y_{<j'}=y_{<j'}]}$.[29] Then*

- *For all $i \in [k]$: the sequence $\{\alpha_{j,i}(Y_{\leq j})\}_{j=0}^m$, where Y_j is drawn from $P_{Y_j|Y_{<j}}$, is a martingale sequence.*
- *For all $i \in [k]$, $j \in [m]$ and $y_{\leq j} \in \operatorname{Supp}(Y_{\leq j})$: $Q[I = i \mid Y_{\leq j} = y_{\leq j}] = \frac{\alpha_{j,i}(y_{\leq j})}{\sum_{i'=1}^k \alpha_{j,i'}(y_{\leq j})}$.*

Proof. For the first item, fix $i \in [k]$, $j \in [m]$, $y_{<j} \in \operatorname{Supp}(P_{Y_{<j}})$ and compute

$$\begin{aligned}
\mathrm{E}_{y_j \sim P_{Y_j|Y_{<j}=y_{<j}}}[\alpha_{j,i}(y_{\leq j})] &= \mathrm{E}_{y_j \sim P_{Y_j|Y_{<j}=y_{<j}}}\left[Q[I=i] \cdot \prod_{j'=1}^{j} \frac{P[E_{j',i} \mid Y_{\leq j'} = y_{\leq j'}]}{P[E_{j',i} \mid Y_{<j'} = y_{<j'}]}\right] \\
&= Q[I=i] \cdot \prod_{j'=1}^{j-1} \frac{P[E_{j',i} \mid Y_{\leq j'} = y_{\leq j'}]}{P[E_{j',i} \mid Y_{<j'} = y_{<j'}]} \cdot \frac{\mathrm{E}_{y_j \sim P_{Y_j|Y_{<j}=y_{<j}}}\left[P[E_{j',i} \mid Y_{\leq j'} = y_{\leq j'}]\right]}{P[E_{j',i} \mid Y_{<j'} = y_{<j'}]} \\
&= Q[I=i] \cdot \prod_{j'=1}^{j-1} \frac{P[E_{j',i} \mid Y_{\leq j'} = y_{\leq j'}]}{P[E_{j',i} \mid Y_{<j'} = y_{<j'}]} \cdot 1 \\
&= \alpha_{j-1,i}(y_{<j})
\end{aligned}$$

We now focus on the second item. In the following, fix $j \in [m]$, $i \in [k]$ and $y_{\leq j} \in \operatorname{Supp}(Q_{Y_{\leq j}})$. Note that for any $i' \in [k]$ it holds that

$$\begin{aligned}
\frac{Q[Y_{\leq j} = y_{\leq j} \mid I = i']}{Q[Y_{\leq j} = y_{\leq j} \mid I = i]} &= \prod_{j'=1}^{j} \frac{Q[Y_{j'} = y_{j'} \mid Y_{<j'} = y_{<j'}, I = i']}{Q[Y_{j'} = y_{j'} \mid Y_{<j'} = y_{<j'}, I = i]} \\
&= \prod_{j'=1}^{j} \frac{P[Y_{j'} = y_{j'} \mid Y_{<j'} = y_{<j'}, E_{j',i'}]}{P[Y_{j'} = y_{j'} \mid Y_{<j'} = y_{<j'}, E_{j',i}]} \\
&= \prod_{j'=1}^{j} \frac{\frac{P[E_{j',i'}|Y_{<=j'}=y_{<=j'}]\cdot P[Y_{j'}=y_{j'}|Y_{<j'}=y_{<j'}]}{P[E_{j',i'}|Y_{<j'}=y_{<j'}]}}{\frac{P[E_{j',i}|Y_{<=j'}=y_{<=j'}]\cdot P[Y_{j'}=y_{j'}|Y_{<j'}=y_{<j'}]}{P[E_{j',i}|Y_{<j'}=y_{<j'}]}} \\
&= \frac{Q[I=i]}{Q[I=i']} \cdot \frac{\alpha_{j,i'}(y_{\leq j})}{\alpha_{j,i}(y_{\leq j})}, \qquad (95)
\end{aligned}$$

[29] In case I is sampled uniformly over $[k]$ in Q, we get the same weights $\{\alpha_{j,i}\}$ as presented in Proposition 2.1 up to a multiplicative factor of $1/k$ which can be ignored.

Therefore, we conclude that

$$\begin{aligned}
Q[I = i \mid Y_{\leq j} = y_{\leq j}] &= Q[I = i] \cdot \frac{Q[Y_{\leq j} = y_{\leq j} \mid I = i]}{Q[Y_{\leq j} = y_{\leq j}]} \\
&= Q[I = i] \cdot \frac{Q[Y_{\leq j} = y_{\leq j} \mid I = i]}{Q[I = i'] \cdot \sum_{i'=1}^{k} Q[Y_{\leq j} = y_{\leq j} | I = i']} \\
&= \frac{1}{\sum_{i'=1}^{k} \frac{Q[I=i']}{Q[I=i]} \cdot \frac{Q[Y_{\leq j}=y_{\leq j}|I=i']}{Q[Y_{\leq j}=y_{\leq j}|I=i]}} \\
&= \frac{1}{\sum_{i'=1}^{k} \frac{\alpha_{j,i'}(y_{\leq j})}{\alpha_{j,i}(y_{\leq j})}} \\
&= \frac{\alpha_{j,i}(y_{\leq j})}{\sum_{i'=1}^{k} \alpha_{j,i'}(y_{\leq j})},
\end{aligned}$$

where the one before last equality holds by Equation (95). □

A.3 Deferred Proofs from Section 5.2

We give the formal proofs for the claim in the proof sketch in Section 5.2.

Claim 5.4. *Let $j \in [m+1]$ and $\tau = (z^k x^k_{<j}) \in \mathrm{Supp}(P_{Z^k X^k_{<j}})$. Then, for every $i \in \mathcal{G}_\tau$ it holds that*

$$Q_{I|Z^k X^k_{<j}, I \in \mathcal{G}_\tau}(i | z^k x^k_{<j}) = \frac{\alpha_{j,i}(z^k x^k_{<j})}{\sum_{i' \in \mathcal{G}_\tau} \alpha_{j,i'}(z^k x^k_{<j})}$$

Proof. In the following, for $i \in [k]$, $j \in [m]$ and $z^k x^{m \times k} \in \mathrm{Supp}(P)$ we define

- $\alpha_i^{(Z)}(z^k) = \frac{P_{Z_i}(z_i)}{P_{Z_i|W}(z_i)} \cdot \frac{P_{X_{1,i}|Z^k W}(1|z^k)}{P_{X_{1,i}|Z_i W}(1|z_i)}$, and
- $\alpha_{j,i}^{(X)}(z^k x^k_{<j}) = \prod_{j'=1}^{j-1} \frac{P_{X_{j+1,i}|Z^k X^k_{\leq j}}(1|z^k x^k_{\leq j})}{P_{X_{j+1,i}|Z^k X^k_{\leq j-1}}(1|z^k x^k_{\leq j-1})}$,

and observe that $\alpha_{j,i}(z^k x^k_{<j}) = \alpha_i^{(Z)}(z^k) \cdot \alpha_{j,i}^{(X)}(z^k x^k_{<j})$.

In the following, fix j, $\tau = (z^k x^k_{<j})$ and i as in the claim statement.

Observe that for any $i' \in \mathcal{G}_\tau$, it holds that

$$
\begin{aligned}
\frac{Q_{Z^k|I}(z^k|i)}{Q_{Z^k|I}(z^k|i')} &= \frac{P_{Z_i}(z_i) \cdot P_{Z_{-i}|Z_i X_{1,i} W}(z_{-i}|z_i 1)}{P_{Z_{i'}}(z_{i'}) \cdot P_{Z_{-i'}|Z_{i'} X_{1,i'} W}(z_{-i'}|z_{i'} 1)}\\
&= \frac{P_{Z_{-i}|Z_i X_{1,i} W}(z_{-i}|z_i 1)}{P_{Z_{-i'}|Z_{i'} X_{1,i'} W}(z_{-i'}|z_{i'} 1)}\\
&= \frac{P_{Z_{i'}|X_{1,i'} W}(z_{i'}|1)}{P_{Z_i|X_{1,i} W}(z_i|1)} \cdot \frac{P_{Z^k|X_{1,i} W}(z^k|1)}{P_{Z^k|X_{1,i'} W}(z^k|1)}\\
&= \frac{\frac{P_{X_{1,i'}|Z_{i'} W}(1|z_{i'}) \cdot P_{Z_{i'}|W}(z_{i'})}{P_{X_{1,i'}|W}(1)}}{\frac{P_{X_{1,i}|Z_i W}(1|z_i) \cdot P_{Z_i|W}(z_i)}{P_{X_{1,i}|W}(1)}} \cdot \frac{\frac{P_{X_{1,i}|Z^k W}(1|z^k)}{P_{X_{1,i}|W}(1)}}{\frac{P_{X_{1,i'}|Z^k W}(1|z^k)}{P_{X_{1,i'}|W}(1)}}\\
&= \frac{\frac{P_{Z_i}(z_i)}{P_{Z_i|W}(z_i)} \cdot \frac{P_{X_{1,i}|Z^k W}(1|z^k)}{P_{X_{1,i}|Z_i W}(1|z_i)}}{\frac{P_{Z_{i'}}(z_{i'})}{P_{Z_{i'}|W}(z_{i'})} \cdot \frac{P_{X_{1,i'}|Z^k W}(1|z^k)}{P_{X_{1,i'}|Z_{i'} W}(1|z_{i'})}}\\
&= \frac{\alpha_i^{(Z)}(z^k)}{\alpha_{i'}^{(Z)}(z^k)} \qquad (96)
\end{aligned}
$$

The above implies that

$$
\begin{aligned}
Q_{I|Z^k, I \in \mathcal{G}_\tau}(i|z^k) &= Q_{I|I \in \mathcal{G}_\tau}(i) \cdot \frac{Q_{Z^k|I}(z^k|i)}{Q_{Z^k|I \in \mathcal{G}_\tau}(z^k)}\\
&= \frac{1}{|\mathcal{G}_\tau|} \cdot \frac{Q_{Z^k|I}(z^k|i)}{\frac{1}{|\mathcal{G}_\tau|} \cdot \sum_{i' \in \mathcal{G}_\tau} Q_{Z^k|I}(z^k|i')}\\
&= \frac{1}{\sum_{i' \in \mathcal{G}_\tau} \frac{Q_{Z^k|I}(z^k|i')}{Q_{Z^k|I}(z^k|i)}}\\
&= \frac{\alpha_i^{(Z)}(z^k)}{\sum_{i' \in \mathcal{G}_\tau} \alpha_{i'}^{(Z)}(z^k)} \qquad (97)
\end{aligned}
$$

We now use Proposition A.4 where let $\widetilde{P}$ be the P of Proposition A.4 and let $\widetilde{Q}$ be Q of Proposition A.4 which are defined as follows: $\widetilde{P}_{Y_1,\ldots,Y_m} = P_{X_1,\ldots,X_m|Z^k=z^k}$, $E_{j,i}$ is the event $X_{j+1,i} = 1$ and $\widetilde{Q}_I = Q_{I|Z^k=z^k, I \in \mathcal{G}_\tau}$. Note that by the above definition it holds that $\widetilde{Q}_{I,Y_1,\ldots Y_m} \equiv Q_{I,X_1,\ldots,X_m|Z^k=z^k, I \in \mathcal{G}_\tau}$, and that

$$
\begin{aligned}
\widetilde{\alpha}_{j-1,i}(x^k_{<j}) &= Q_{I|Z^k, I \in \mathcal{G}_\tau}(i|z^k) \cdot \alpha_{j,i}^{(X)}(z^k x^k_{<j})\\
&= \frac{\alpha_i^{(Z)}(z^k)}{\sum_{i' \in \mathcal{G}_\tau} \alpha_{i'}^{(Z)}(z^k)} \cdot \alpha_{j,i}^{(X)}(z^k x^k_{<j})\\
&= \frac{\alpha_{j,i}(z^k x^k_{<j})}{\sum_{i' \in \mathcal{G}_\tau} \alpha_{i'}^{(Z)}(z^k)}, \qquad (98)
\end{aligned}
$$

where we let $\widetilde{\alpha}_{j,i}$ be the $\alpha_{j,i}$ of Proposition A.4. Hence,

$$\begin{aligned}
Q_{I|Z^k X^k_{<j}, I \in \mathcal{G}_\tau}(i|z^k x^k_{<j}) &= \widetilde{Q}_{I|Y_{\leq j-1}}(i|x^k_{<j}) \\
&= \frac{\widetilde{\alpha}_{j-1,i}(x^k_{<j})}{\sum_{i' \in \mathcal{G}_\tau} \widetilde{\alpha}_{j-1,i'}(x^k_{<j})} \\
&= \frac{\alpha_{j,i}(z^k x^k_{<j})}{\sum_{i' \in \mathcal{G}_\tau} \alpha_{j,i'}(z^k x^k_{<j})},
\end{aligned}$$

where the one before last equality holds by Proposition A.4 and the last one by Equation (98). □

Claim 5.5. *Let $j \in [m+1]$, let $\tau = (z^k x^k_{<j}) \in \operatorname{Supp}(P_{Z^k X^k_{<j}})$, and let $Q'_{X^k_{j+1}|Z^k X^k_{<j}} = P_{X^k_{j+1}|Z^k X^k_{<j} X_{j+1,I}=1} \circ Q_{I|Z^k X^k_{<j}, I \in \mathcal{G}_\tau}$. Then, for every $x^k_{j+1} \in \operatorname{Supp}(P_{X^k_{j+1}|(Z^k X^k_{<j})=\tau})$ with $1_{x^k_{j+1}} \cap \mathcal{G}_\tau \neq \emptyset$, it holds that*

$$\frac{P_{X^k_{j+1}|Z^k X^k_{<j}}(x^k_{j+1}|\tau)}{Q'_{X^k_{j+1}|Z^k X^k_{<j}}(x^k_{j+1}|\tau)} = \frac{\sum_{i \in \mathcal{G}_\tau} \alpha_{j,i}(\tau)}{\sum_{i \in 1_{x^k_{j+1}} \cap \mathcal{G}_\tau} \frac{\alpha_{j,i}(\tau)}{p_i(\tau)}},$$

for $p_i(\tau) = P_{X_{j+1,i}|Z^k X^k_{<j}}(1|\tau)$.

Proof. Fix $(z^k, x^k_{<j}, x^k_{j+1}) \in \operatorname{Supp}(P_{Z^k X^k_{<j} X^k_{j+1}|W})$ with $1_{x^k_{j+1}} \cap \mathcal{G}_\tau \neq \emptyset$. By definition, it holds that

$$\begin{aligned}
Q'_{X^k_{j+1}|Z^k X^k_{<j}}(x^k_{j+1}|z^k, x^k_{<j}) &= \sum_{i \in \mathcal{G}_\tau} Q_{I|Z^k X^k_{<j}, I \in \mathcal{G}_\tau}(i|z^k, x^k_{<j}) \cdot P_{X^k_{j+1}|Z^k X^k_{<j} X_{j+1,i},W}(x^k_{j+1}|z^k, x^k_{<j}, 1) \\
&= \sum_{i \in 1_{x^k_{j+1}} \cap \mathcal{G}_\tau} Q_{I|Z^k X^k_{<j}, I \in \mathcal{G}_\tau}(i|z^k, x^k_{<j}) \cdot P_{X^k_{j+1}|Z^k X^k_{<j} X_{j+1,i},W}(x^k_{j+1}|z^k, x^k_{<j}, 1),
\end{aligned}$$

where the second equality holds since if $x_{j+1,i} = 0$ then $P_{X^k_{j+1}|Z^k X^k_{<j}, X_{j+1,i},W}(x^k_{j+1}|z^k, x^k_{<j}, 1) = 0$. Claim 5.4 now yields that

$$\begin{aligned}
Q'_{X_{j+1}|Z^k X^{<j}}(x_{j+1}|z^k, x^{<j}) &= \sum_{i \in 1_{x_{j+1}} \cap \mathcal{G}_\tau} \frac{\alpha_{j,i}(z^k x^k_{<j})}{\sum_{i' \in \mathcal{G}_\tau} \alpha_{j,i'}(z^k x^k_{<j})} \cdot P_{X^k_{j+1}|Z^k X^k_{<j}, X_{j+1,i},W}(x^k_{j+1}|z^k, x^k_{<j}, 1) \\
&= \sum_{i \in 1_{x_{j+1}} \cap \mathcal{G}_\tau} \frac{\alpha_{j,i}(z^k x^k_{<j})}{\sum_{i' \in \mathcal{G}_\tau} \alpha_{j,i'}(z^k x^k_{<j})} \cdot \frac{P_{X^k_{j+1}|Z^k X^k_{<j} W}(x^k_{j+1}|z^k, x^k_{<j})}{P_{X_{j+1,i}|Z^k X^k_{<j} W}(1|z^k, x^k_{<j})}.
\end{aligned}$$

It follows that

$$\begin{aligned}
\frac{P_{X^k_{j+1}|Z^k X^k_{<j} W}(x^k_{j+1}|z^k, x^k_{<j})}{Q'_{X^k_{j+1}|Z^k X^k_{<j}}(x^k_{j+1}|z^k, x^k_{<j})} &= \frac{P_{X^k_{j+1}|Z^k X^k_{<j} W}(x^k_{j+1}|z^k, x^k_{<j})}{\sum_{i \in 1_{x_{j+1}} \cap \mathcal{G}_\tau} \frac{\alpha_{j,i}(z^k x^k_{<j})}{\sum_{i' \in \mathcal{G}_\tau} \alpha_{j,i'}(z^k x^k_{<j})} \cdot \frac{P_{X^k_{j+1}|Z^k X^k_{<j} W}(x^k_{j+1}|z^k, x^k_{<j})}{P_{X_{j+1,i}|Z^k X^k_{<j} W}(1|z^k, x^k_{<j})}} \\
&= \frac{\sum_{i' \in \mathcal{G}_\tau} \alpha_{j,i'}(z^k x^k_{<j})}{\sum_{i \in 1_{x_{j+1}} \cap \mathcal{G}_\tau} \frac{\alpha_{j,i}(z^k x^k_{<j})}{p_i(z^k, x^{<j})}}.
\end{aligned}$$

□

Claim 5.6. *Let $j \in [m+1]$, let $\tau = (z^k x^k_{<j}) \in \mathrm{Supp}(P_{Z^k X^k_{<j}})$, and let X^k_{j+1} be drawn from $P_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}$ or from $\prod_{i=1}^k P_{X_{j+1,i}|(Z^k X^k_{<j})=\tau}$.*[30] *Let $Y = \sum_{i \in \mathcal{G}_\tau} Y_i$, for $Y_i = \frac{\alpha_{j,i}(\tau)}{P_{X^k_{j+1,i}|Z^k X^k_{<j}}(1|\tau)}$ if $X_{j+1,i} = 1$ and $Y_i = 0$ otherwise.*

It holds that

$$\mathrm{E}_{P_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}}[Y] = \mathrm{E}_{\prod_{i=1}^k P_{X_{j+1,i}|(Z^k X^k_{<j})=\tau}}[Y] = \sum_{i \in \mathcal{G}_\tau} \alpha_{j,i}(\tau).$$

Proof. Fix $j \in [m+1]$ and $\tau = (z^k x^k_{<j}) \in \mathrm{Supp}(P_{Z^k X^k_{<j}|W})$. Compute

$$\begin{aligned}
\mathrm{E}_{P_{X^k_{j+1}|(Z^k X^k_{<j})=\tau,W}}[Y] &= \sum_{i \in \mathcal{G}_\tau} \mathrm{E}_{P_{X^k_{j+1,i}|(Z^k X^k_{<j})=\tau,W}}[Y_i] \\
&= \sum_{i \in \mathcal{G}_\tau} \mathrm{E}_{x_{j+1,i} \sim P_{X^k_{j+1,i}|(Z^k X^k_{<j})=\tau,W}} \frac{a_{j,i}(\tau)}{P_{X^k_{j+1,i}|Z^k X^k_{<j} W}(1|\tau)} \cdot \mathbb{1}\{x_{j+1,i} = 1\} \\
&= \sum_{i \in \mathcal{G}_\tau} P_{X^k_{j+1,i}|Z^k X^k_{<j} W}(1|\tau) \cdot \frac{a_{j,i}(\tau)}{P_{X^k_{j+1,i}|Z^k X^k_{<j} W}(1|\tau)} \\
&= \sum_{i \in \mathcal{G}_\tau} a_{j,i}(\tau),
\end{aligned}$$

where the first equality follows from linearity of expectation and third equality holds since $P_{X^k_{j+1,i}|Z^k X^k_{<j} W}(1|\tau) > 0$ for every $i \in \mathcal{G}_\tau$ (follows from the condition that $|\rho_{j,i}(\tau)| \leq 0.1$). Finally, observe that the very same computation also yields that the expected value of Y under $\prod_{i=1}^k P_{X_{j+1,i}|(Z^k X^k_{<j})=\tau,W}$ is also $\sum_{i \in \mathcal{G}_\tau} a_{j,i}(\tau)$. □

Claim 5.7. *Let $Z^k X^k_1$ be drawn from $P_{Z^k X^k_1}$ or from $\prod_{i=1}^k P_{Z_i X_{1,i}}$.*[31] *Let $Y = \sum_{i \in [k]} Y_i$, for $Y_i = \frac{\alpha_{0,i}(z_i)}{P_{X_{1,i}}(1)}$ if $X_{1,i} = 1$ and $Y_i = 0$ otherwise.*

It holds that

$$\mathrm{E}_{P_{Z^k X^k_1}}[Y] = \mathrm{E}_{\prod_{i=1}^k P_{Z_i X_{1,i}}}[Y] = \frac{|\mathcal{D}|}{2^\ell}.$$

[30] $\prod_{i=1}^k P_{X_{j+1,i}|(Z^k X^k_{<j})=\tau}$ is the product distribution of the marginals of $P_{X^k_{j+1}|(Z^k X^k_{<j})=\tau}$.

[31] $\prod_{i=1}^k P_{Z_i X_{1,i}}$ is the product distribution of the marginals of $P_{Z^k X^k_1}$.

Proof. Compute

$$\begin{aligned}
\mathrm{E}_{P_{Z^k X_1^k|W}}[Y] &= \sum_{i\in[k]} \mathrm{E}_{P_{Z_i X_{1,i}|W}}[Y_i] \\
&= \sum_{i\in[k]} \mathrm{E}_{z_i x_{1,i} \sim P_{Z_i X_{1,i}|W}} \frac{a_{0,i}(z_i)}{P_{X_{1,i}|W}(1)} \cdot \mathbb{1}\{x_{1,i}=1\} \\
&= \sum_{i\in[k], z_i\in\{0,1\}^\ell} P_{X_{1,i}|W}(1) P_{Z_i|X_{1,i}W}(z_i|1) \cdot \frac{a_{0,i}(z_i)}{P_{X_{1,i}|W}(1)} \\
&= \sum_{i\in[k], z_i\in\{0,1\}^\ell} P_{Z_i|X_{1,i}W}(z_i|1) \cdot \frac{P_{Z_i}(z_i)}{P_{Z_i|X_{1,i}W}(z_i|1)} \cdot \mathbb{1}\{(i,z_i)\in\mathcal{D}\}, \\
&= \sum_{i\in[k], z_i\in\{0,1\}^\ell} P_{Z_i}(z_i) \cdot \mathbb{1}\{(i,z_i)\in\mathcal{D}\}, \\
&= \frac{|\mathcal{D}|}{2^\ell},
\end{aligned}$$

where the first equality follows from linearity of expectation, and the third and forth equalities hold since $\mathcal{W}$ is termination consistent, so the transcript in which all the verifiers terminate in round 1 belongs to $\mathcal{W}$, regardless of the value of the random coins z^k; that is, $P_{X_{1,i}|W}(1) > 0$ and $P_{Z_i|X_{1,i}W}(z_i|1) > 0$ for every $i \in [k]$ and $z_i \in \{0,1\}^\ell$. Since $Y = (1+\Delta)\cdot\frac{|\mathcal{D}|}{2^\ell}$, the random variable Δ in fact measures how far Y is from its expectation. It follows that $\mathrm{E}_{P_{Z^k X_1^k|W}}[\Delta] = 0$. Finally, observe that the very same computation also yields that the expected value of Y under $\prod_{i=1}^k P_{Z_i X_{1,i}|W}$ is also $\frac{|\mathcal{D}|}{2^\ell}$. □