A Parallel Repetition Theorem for Any Interactive Argument

Iftach Haitner*

August 10, 2009

Abstract

The question of whether or not parallel repetition reduces the soundness error is a fundamental question in the theory of protocols. While parallel repetition reduces (at an exponential rate) the error in interactive proofs and (at a weak exponential rate) in special cases of interactive arguments (e.g., 3-message protocols — Bellare, Impagliazzo and Naor [FOCS '97], and public-coin protocols — Håstad, Pass, Pietrzak and Wikström [Manuscript '08]), Bellare et al. gave an example of interactive arguments for which parallel repetition does not reduce the soundness error at all.

We show that by slightly modifying *any* interactive argument, in a way that preserves its completeness and only slightly deteriorates its soundness, we get a protocol for which parallel repetition *does* reduce the error at a weak exponential rate. In this modified version, the verifier flips at the beginning of each round an $(1-\frac{1}{4m},\frac{1}{4m})$ biased coin (i.e., 1 is tossed with probability $1/4m$), where m is the round complexity of the (original) protocol. If the coin is one, the verifier halts the interaction and accepts, otherwise it sends the same message that the original verifier would. At the end of the protocol (if reached), the verifier accepts if and only if the original verifier would.

1 Introduction

In an interactive proof, a prover P is trying to convince the verifier V in the validity of some statement. Typically, P has some advantage over V, such as additional computational resources or some extra information (e.g., an NP witness that validates the claim). The two basic properties we would like such protocols to have are *completeness* and *soundness*. The completeness means that P convinces V to accept *valid* statements, and the soundness means that no cheating prover (of a certain class) can convince V to accept *invalid* statements. More generally, (P,V) has completeness β if for any valid statement x, V accepts in $(\mathrm{P},\mathrm{V})(x)$ with probability at least β (where P typically gets an advice $w(x)$ as an additional input). Where V has soundness $1-\varepsilon$ with respect to a given class of algorithms, if no malicious P^* from this class can convince V to accept an invalid statement with probability greater than ε. The bound ε is typically called the *soundness error* of the protocol.

The basic distinction one may make about the soundness of a given protocol, is whether it holds unconditionally (i.e., even an all-powerful prover cannot break the soundness) or that it only holds against computationally bounded (uniform, or non-uniform) provers. Protocols with unconditional soundness are called *interactive proofs*, whereas protocols with the weaker type of soundness are called *interactive arguments*. In this work we focus on computationally bounded provers. In particular, we consider polynomial-time provers.

A common paradigm for constructing protocols with low soundness error, is to start by constructing a protocol with noticeable soundness error, and then manipulate the original protocol in a certain way that decreases its soundness error while keeping its completeness high. The most natural such manipulation that comes to mind, is to use repetition. Namely, to repeat the protocol many times (with independent randomness), where the verifier accepts only if the verifiers (of the original protocol) accept in all executions. The above repetition can be done in essentially two different ways: sequentially (known as *sequential repetition*),

*Microsoft Research, New England Campus. E-mail: iftach@microsoft.com.

where the $(i+1)$ execution of the protocol is only started after the i'th execution is finished, or in parallel (known as *parallel repetition*), where all the executions are done simultaneously.

Sequential repetition is known to reduce the soundness error at an exponential rate in most computational models (cf., [DP98]). Unfortunately, sequential repetition has the undesired effect of increasing the round complexity. Parallel repetition on the other hand, does preserve the round complexity, and for the case of interactive proofs, it also reduces the soundness error at an exponential rate [Gol99]. Unfortunately, as shown by Bellare, Impagliazzo and Naor [BIN97], in the case of interactive arguments parallel repetition might not reduce the soundness error at all.

Let us be more precise about the latter statement. Parallel repetition does reduce the soundness error in the case of 3-message protocol ([BIN97, CHS, IJK06]) and in the case of public-coin verifiers ([PV07, HPPW08]), see Section 1.3 for more details. On the negative side, for any $k \in \mathbb{N}$ [BIN97] presented an 8-message protocol with soundness error $\frac{1}{2}$, whose k-parallel repetition soundness remains $\frac{1}{2}$. Recently, Pietrzak and Wikström [PW07] gave an example of a single protocol for which the above phenomena holds for all polynomial k simultaneously.[1] Moreover, both results extend to 4-message protocols, assuming a rather natural limitation about the soundness proof.

1.1 Our Result

We present a simple method for transforming any efficient interactive argument whose soundness error is bounded away from one, into an efficient interactive argument with the same number of rounds and negligible soundness error. Given an m-round interactive protocol (P, V), we define the ***random-termination*** variant of V, denoted by $\widetilde{\mathrm{V}}$, as follows: through the interaction with P algorithm $\widetilde{\mathrm{V}}$ acts exactly as V does, but with the following additional step: at the end of each round, $\widetilde{\mathrm{V}}$ tosses an $(1 - 1/4m, 1/4m)$ biased coin (i.e., 1 is tossed with probability $1/4m$). If the outcome of the coin is 1, then $\widetilde{\mathrm{V}}$ accepts the interaction and halts. Otherwise, $\widetilde{\mathrm{V}}$ proceeds as V does (where in particular, at the end of the protocol, if reached, $\widetilde{\mathrm{V}}$ accepts iff V does). Note that the completeness of $(\mathrm{P}, \widetilde{\mathrm{V}})$ is at least as high as the completeness of (P, V), where the soundness of $\widetilde{\mathrm{V}}$ is at least $(1 - \frac{1}{4m})^m \cdot \alpha \geq \frac{3}{4} \cdot \alpha$, given that the soundness of V is at least α.

In the following we refer to $(\mathrm{P}, \widetilde{\mathrm{V}})$ as the random-termination variant of (P, V). Our main contribution is stated in the following theorem.

Theorem 1.1 (informal)**.** *Parallel repetition of the random-termination variant of* any *interactive argument, reduces the soundness error at a weak exponential rate.*[2]

We note that our result holds with respect to any interactive protocol that can be cast as an interactive argument. For instance, our result yields a round-preserving binding amplification for computationally binding commitment schemes.[3] Our result also extends to the more general threshold case, where the prover in the k-fold repetition is only required to make $t < k$ of the verifiers accept.

1.2 Our Technique

Let (P, V) be an interactive argument with soundness error ε and let $(\mathrm{P}^{(k)}, \mathrm{V}^{(k)})$ be its k'th parallel repetition. We show that if (P, V) is a random-termination variant of some protocol, then any efficient strategy $\mathrm{P}^{(k)*}$

[1] Both negative results hold under common cryptographic assumptions.

[2] We are using a rather relaxed interpretation of weak exponential rate, meaning that the soundness error is bounded by $\max\{\mathrm{neg}, \exp(-\mathrm{poly}(\frac{1-\varepsilon}{m}) \cdot k\}$, where m is the round complexity of the protocol and ε is the soundness error of the original protocol. See Theorem 3.2 for the exact statement.

[3] Given a weakly binding commitment (S, R), consider the protocol (P, V) where P and V play the role of S and R in a random commit stage of (S, R) respectively. Following the commit stage, P sends two strings to the V, and V outputs "1" iff the strings are valid decommitments to different values. The weakly binding property of (S, R) yields that the soundness error of (P, V) is noticeably far from one. Thus, Theorem 1.1 yields that the parallel repetition of the random-termination variant of (P, V), has negligible soundness error. It follows that the parallel repetition of the random-termination variant of (S, R) is strongly binding.

that breaks the soundness of $(\mathrm{P}^{(k)}, \mathrm{V}^{(k)})$ with "too high" probability ε_k, implies an *efficient* algorithm P^* that breaks the soundness of (P, V) with probability higher than ε. As a warm up, we start by presenting such strategy for the parallel repetition of public-coin protocols (with no random-termination), and then explain how to adapt this strategy the random-termination case.

Public-coin protocols In the following we loosely follow the approach presented by [HPPW08]. In order to interact with V, algorithm P^* emulates a random execution of $(\mathrm{P}^{(k)^*}, \mathrm{V}^{(k)})$, where the "real" V plays the role of the i^*'th V, for i^* that is chosen at random from $[k]$, and P^* emulates the execution of the other $(k-1)$ verifiers and of $\mathrm{P}^{(k)^*}$. In the j'th round, P^* acts as follows: upon receiving the j'th message from V, it samples at random a value $M_j = (M_{j,1}, \ldots, M_{j,k})$ for the j'th messages of emulated verifiers, and evaluates their "quality" α_{M_j} — the probability that $\mathrm{P}^{(k)^*}$ makes $\mathrm{V}^{(k)}$ accept conditioned on the current transcript and on M_j. In order to do so, P^* samples many random continuations of the protocol, and measures the fraction of accepting ones (i.e., where all the verifiers accept). If the estimated value of α_{M_j} is higher than some threshold β_j (e.g., $\beta_j = (1 - \frac{j}{4m}) \cdot \varepsilon_k$, where we recall that ε_k is the success probability of $\mathrm{P}^{(k)^*}$), then P^* sends $M^j_{i^*}$ back to the real V. In addition, P^* sets the state of the emulated verifiers and $\mathrm{P}^{(k)^*}$ according to M_j. P^* keeps sampling random values for M_j until a good value is found, or until n/ε_k unsuccessful attempts, where in the latter case it aborts. We note that V accepts whenever P^* does not abort.[4]

The proof that P^* breaks the soundness of $(\mathrm{P}^*, \mathrm{V})$ with high probability, goes by showing that conditioned on P^* not aborting in the j'th round, the probability that P^* abort in the $j+1$ round is small. For proving the above, it suffices to show that $\mathrm{P}^{(k)^*}$'s conditional success probability after getting the $j+1$ message from the real verifier, is not much smaller than α_{M_j}. While in the worst case the latter probability might be arbitrarily small (and in particular, much smaller than α_{M_j}), using a result of Raz [Raz98] one can show that for most values of i^*, this conditional probability is with high probability close to α_{M_j}.

Random-termination protocols When one tries to adopt the above strategy for non public-coin protocols, he should first decide what the values of M_j and α_{M_j} stand for in this case. The first (and the more natural) option, is to choose M_j at random from the j'th *messages* of the emulated verifier that are consistent with the current *transcript*, and let α_{M_j} be the probability that $\mathrm{P}^{(k)^*}$ makes $\mathrm{V}^{(k)}$ accept conditioned on M_j and on the current transcript. The very same argument we used above for the public-coin case, yields that P^* makes V accepts with high probability also in this settings. The problem is, however, that the above strategy is not necessarily efficient. (Indeed, the task of sampling M_j and of estimating α_{M_j} using the above strategy, are essentially the task of finding a random preimage of an arbitrary function).[5]

The way we adopt the public-coin strategy for the non public-coin case is different. We assume without loss of generality that the random (private) coins that V is using in each round are chosen uniformly at random from $\{0,1\}^t$ (for some value of t that might depend on the round). In each round, P^* chooses M_j uniformly random from $\{0,1\}^{t\cdot(k-1)}$, and estimates the value of α_{M_j} defined as the probability that $\mathrm{P}^{(k)^*}$ makes $\mathrm{V}^{(k)}$ accept, conditioned on the random coins flipped by all the verifiers (emulated and real) till now, and that the random coins of the emulated verifiers in the j'th round are set to M_j. Upon finding a good value for M_j (i.e., the estimation of α_{M_j} is at least β_j), P^* fixes the random coins of the emulated verifiers in the j'th round to M_j, and sends the message that $\mathrm{P}^{(k)^*}$ sends to the i^* verifier in the j'th round to V (given this fixing). As in the case of former approach, it follows that P^* makes V accepts with high probability.

[4] [HPPW08] use a different (and somewhat less intuitive) strategy for evaluating the quality of M_j, which significantly simplifies the analysis of P^* success probability (see Section 2.3 for more details). The sampling method of the cheating prover for random-termination verifiers described in Section 3, is a variant of their approach.

[5] We mention that the proofs of all interactive argument protocols for which parallel repetition is known to reduce soundness, follow (implicitly or explicitly) the above strategy. Indeed, such proofs were only given for protocols for which the above sampling strategy can be carried efficiently: public-coin protocol [HPPW08], with extensions to protocols in which the last message of the verifier (which contains its decision bit) is not necessarily efficiently samplable: 3-message protocols [BIN97] and "extendable and simulatable" verifiers [HPPW08].

On a first look, the above approach does not look very promising, as in general no strategy (even not an unbounded one) can evaluate α_{M_j}.[6] Interestingly, we show that a close variant of the above strategy can be implemented efficiently for any random-termination verifier.

Let V be a random-termination verifier and assume without loss of generality that it chooses all but its decision bits (the bits uses for deciding whether or not to terminate the executions) before the interaction starts. In order to approximate the value of α_{M_j}, P^* samples the future random coins of all the verifiers conditioned that the real verifier's decision bit in the end of the j'th round is one (i.e., it decides to halt in the end of the j'th round). Sampling in this case is very easy, since the real verifier sends no further messages, and the future random coins for the emulated verifiers (under any conditioning) are simply uniform random strings. The obvious problem with the above approach is that by adding this additional conditioning we might reduce the success probability of P^*. We prove that the latter does not happen for most choices of i^*, by proving the following stronger statement: for a given $i^* \in [k]$, consider the distribution that a random execution of $(\mathrm{P}^*, \widetilde{\mathrm{V}})$ described above induces on the value of $(M_1 \ldots, M_m)$ with respect to to this choice of i^* (hereafter, the "real" distribution). For such i^*, we also consider the "ideal" version of the above distribution. In this version, P^* has access to the random coins of the i^* verifier, and uses them for approximating the values of α_{M_j} well. Our main technical contribution is showing that for most values of $i^* \in [k]$ (i.e., for $(1 - (\frac{m}{k})^{\Omega(1)})$ fraction of them), the above distributions are statistically close.

Bounding the distance between the ideal and real distributions Let $k \geq m \cdot n^2$. For concreteness, we consider the distribution of M_1 induced by the first round of the protocol, given an arbitrary fixing of the real verifier random coins. We say that $i^* \in [k]$ has ***global effect***, if by conditioning that the i^*'th verifier halts at the end of the first round, we significantly change the probability that P^* finds a good value for M_1 in a single first round iteration. We say that i^* has ***local effect*** on some value of M_1, if by conditioning on the i^* verifier halting at the end of the first round, we significantly change the value of α_{M_1} (recall that α_{M_1} was defined as the success probability ${\mathrm{P}^{(k)}}^*$, conditioned that the emulated verifiers random coins in the first round are set to M_1).

We first show that the fraction of local effect indices is small for every value of M_1. Assume that the number of local effect indices on some value of M_1 is larger than $m \cdot n$. Further, assume for simplicity that by conditioning on half of these indices, we reduce the value of α_{M_1} significantly. In this case, at least one of these local high effect verifiers halts in almost every random continuation of the protocol (recall that any of the verifiers halts with probability $1/4m$). This means that the value of α_{M_1} should have been smaller than what we assume it is. A similar proof also show that the number of global effect indices is small.

In the following we assume for simplicity that every index has local effect only on a small portion of the possible values for M_1, and let i^* be an index with no global effect. It is easy to verify that the following holds in a random first round iteration of P^* with such choice of i^*: the probability that P^* picks a good value for M_1 (P^* estimates that $\alpha_{M_1} > \beta_1$) and i^* *does not have* local large effect on, is much larger than the probability that P^* picks a good value for M_1 that i^* *has* local large effect on. It follows that the probability that such choice of i^* induces on most value of M_1, is close to the probability in which each M_1 is drawn with probability $\frac{\alpha_{M_1}}{\mathsf{E}_{M_1}[\alpha_{M_1}]}$. Namely, the distribution induced by i^* is close to the real distribution.

1.3 Related Work

Babai and Moran [BM88] showed that parallel repetition reduces the soundness error of Arthur-Merlin protocols, whereas Goldreich [Gol99, Appendix C.1] showed that the same holds with respect to interactive proofs. Parallel repetition is also known to reduce the error in the important case of two-prover interactive proofs [Raz98] (in all the above cases the soundness error reduces at exponential rate).

[6] The random coins that the real verifier chooses in the j'th round, might only affect the transcript on a later round. Therefore, the transcript of the protocol in the j'th round might not contain the required information for estimating α_{M_j} (recall that the value of α_{M_j} is determined by the random coined that were already flipped by the verifiers, and not by the transcript).

Bellare, Impagliazzo and Naor [BIN97] showed that parallel repetition of 3-message interactive arguments reduces the soundness error at weak exponential rate. For two-message protocols, Canetti et al. [CHS] gave a proof with better parameters, and Impagliazzo et al. [IJK06] showed that the same holds with respect to the threshold case. For public-coin protocols, Pass and Venkitasubramaniam [PV07] gave a parallel repetition theorem for constant-round protocols, whereas recently Håstad et al. [HPPW08] extended this result to a polynomial number of rounds. The result of [HPPW08] generalizes to "extendable and simulatable" verifiers, which essentially means that it is feasible to sample a random continuation of the verifier's actions, given a partial transcript of the protocol. All the latter protocols reduce the soundness error at a weak exponential rate. Recently, Haitner et al. [HRVW] showed a round-preserving binding amplification of a specific (weak) computational binding commitment. The random-termination verifier we introduce here, is inspired by their construction. Finally, the phenomena that by changing the verifier to send less information in a single execution (thus increasing the soundness error), we reduce the soundness error when repeating the protocol in parallel, is a reminisce of the work (in the context of two-prover protocols) of Feige and Kilian [FK94].

1.4 Paper Organization

We present the notations and formal definitions used in this paper in Section 2, where our main result is formally stated and proved in Section 3.

2 Preliminaries

For $\alpha, \beta > 0$, let $(\alpha \pm \beta) := [\alpha - \beta, \alpha + \beta]$. We use calligraphic letters to denote sets, capital letters for random variable, and lower case letters for values. We use superscripts to denote tuples, e.g., $X^n := (X_1, \ldots, X_n)$ and $x^n := (x_1, \ldots x_n)$. We write $x \xleftarrow{R} \mathcal{X}$ to indicate that x is selected according to the uniform distribution over $\mathcal{X}$.

We let U_n be the uniform distribution over $\{0,1\}^n$. Given a set $\mathcal{S}$ and $p \in (0,1]$, we let $U_{\mathcal{S}}^p$ be the distribution induced on $2^{\mathcal{S}}$ by independently selecting each of the elements of $\mathcal{S}$ with probability p. For $i \in \mathcal{S}$, let the distribution $U_{\mathcal{S},i=1}^p$ [resp., $U_{\mathcal{S},i=0}^p$] be the distribution $U_{\mathcal{S}}^p$ conditioned that i is selected [resp., not selected]. The statistical difference of two distributions P_X^1 and P_X^2 over $\mathcal{X}$, denoted by $\left\|\mathsf{P}_X^1 - \mathsf{P}_X^2\right\|$, is defined as $\frac{1}{2}\sum_{x\in\mathcal{X}} \left|\mathsf{P}_X^1(x) - \mathsf{P}_X^2(x)\right| = \max_{\mathcal{X}'\subseteq\mathcal{X}}\{\mathsf{P}_X^1(\mathcal{X}') - \mathsf{P}_X^2(\mathcal{X}')\}$. Given a set $\mathcal{X}'$, we let $\left\|\mathsf{P}_X^1 - \mathsf{P}_X^2\right\|_{\mathcal{X}'} = \frac{1}{2}\cdot\sum_{x\in\mathcal{X}\setminus\mathcal{X}'} \left|\mathsf{P}_X^1(x) - \mathsf{P}_X^2(x)\right|$ and let $\left\|\mathsf{P}_X^1 - \mathsf{P}_X^2\right\|_{\overline{\mathcal{X}'}} = \left\|\mathsf{P}_X^1 - \mathsf{P}_X^2\right\|_{\mathcal{X}\setminus\mathcal{X}'}$. When bounding the statistical difference of two distributions, we often use the following proposition (whose straight forward proof is given in the appendix).

Proposition 2.1. *Let P^1 and P^2 be two distributions over $\mathcal{X}$ and let $\mathcal{X}' \subseteq \mathcal{X}$, then*

$$\left\|\mathsf{P}^1 - \mathsf{P}^2\right\| \leq \mathsf{P}^1(\overline{\mathcal{X}'}) + 2\cdot\left\|\mathsf{P}^1 - \mathsf{P}^2\right\|_{\mathcal{X}'}.$$

The following proposition plays an important in the proof of Theorem 3.2.[7]

Proposition 2.2. *Let $X_1, \ldots, X_k$ be independent random variables and let W be a Boolean random variable, then for any $\varepsilon > 0$ it holds that*

$$\mathsf{Pr}_{i\xleftarrow{R}[k], x\xleftarrow{R}X_i}\left[\mathsf{Pr}[W \mid X_i = x] \notin (1\pm\varepsilon)\cdot\mathsf{Pr}[W]\right] \leq \frac{2}{\varepsilon}\cdot\sqrt{\frac{-\log\mathsf{Pr}[W]}{k}}.$$

Proof. We assume without loss of generality that $\mathsf{Pr}[W] > 0$. For $i \in [k]$, let P_{X_i} be the probability distribution induced by X_i, and let $\mathcal{S}_i^- = \{x \in \mathrm{Supp}(X_i) \colon \mathsf{Pr}[W \mid X_i = x] < (1-\varepsilon)\cdot\mathsf{Pr}[W]\}$ and $\mathcal{S}_i^+ =$

[7] In [Hai09, Lemma 2.3] we prove a variant of Proposition 2.2, which yields a slightly stronger variant of Theorem 3.2 (the number of repetitions is proportional to m^8 rather than to m^{10}). For the sake of simplicity and self containment, however, we have preferred to use here Proposition 2.2, whose proof is significantly simpler.

$\{x \in \mathrm{Supp}(X_i)\colon \mathsf{Pr}[W \mid X_i = x] > (1+\varepsilon)\cdot \mathsf{Pr}[W]\}$. Since $\left\|\mathsf{P}_{X_i|W} - \mathsf{P}_{X_i}\right\| \geq \frac{1}{2}\cdot\left|\mathsf{P}_{X_i|W}(\mathcal{S}_i^-) - \mathsf{P}_{X_i}(\mathcal{S}_i^-)\right| + \frac{1}{2}\cdot\left|\mathsf{P}_{X_i|W}(\mathcal{S}_i^+) - \mathsf{P}_{X_i}(\mathcal{S}_i^+)\right| \geq \frac{\varepsilon}{2}\cdot\mathsf{P}_{X_i}(\mathcal{S}_i^- \cup \mathcal{S}_i^+)$, it follows that

$$\mathsf{Pr}_{i\xleftarrow{R}[k],x\xleftarrow{R}X_i}\left[\mathsf{Pr}[W \mid X_i = x] \notin (1\pm\varepsilon)\cdot\mathsf{Pr}[W]\right] \leq \frac{1}{k}\cdot\sum_{i\in[k]}\mathsf{P}_{X_i}(\mathcal{S}_i^- \cup \mathcal{S}_i^+) \leq \frac{2}{\varepsilon\cdot k}\cdot\sum_{i\in[k]}\left\|\mathsf{P}_{X_i|W} - \mathsf{P}_{X_i}\right\|.$$

The proof is concluded by the following Lemma due to Holenstein (simplifying a lemma of [Raz98]).

Lemma 2.3. *([Hol07, Equation 8]) Let $\mathsf{P}_{X^k} := \mathsf{P}_{X_1}\cdots\mathsf{P}_{X_k}$ be a probability distribution over $\mathcal{X}^k$ and let W be an event in the same probability space, then*

$$\sum_{i=1}^{k}\left\|\mathsf{P}_{X_i|W} - \mathsf{P}_{X_i}\right\| \leq \sqrt{-k\cdot\log\mathsf{Pr}[W]}.$$

□

2.1 Interactive Arguments

An interactive argument for a language $L \subseteq \{0,1\}^*$, is an interactive protocol between the prover P and the verifier V. The parties get as common input a security parameter 1^n and an element $x \in \{0,1\}^*$, and the prover might get an additional private input $w(x)$ (e.g., witness). We assume for simplicity that V speaks first, where each round of the protocol consists of exchange of two message, from V to P and back. We say that V is an $m(n)$-round verifier, if $m(n)$ bounds V's number of rounds in any execution $(\mathrm{P}^*,\mathrm{V})(1^n,x)$, for any value of P^* and x.

The protocol (P,V) has completeness $\beta(n)$, if for every $x \in L$, there exits $w \in \{0,1\}^*$ such that $\mathsf{Pr}(\mathrm{P}(w),\mathrm{V})(1^n,x) \neq 1] \leq \beta(n)$. The verifier V has soundness error $\varepsilon(n)$ against uniform [resp., non-uniform] adversaries, if for any $x \notin L$ and any uniform [resp., non-uniform] PPT P^*, it holds that $\mathsf{Pr}(\mathrm{P}^*,\mathrm{V})(1^n,x) = 1] \leq \varepsilon(n)$.

2.2 Random-termination Verifiers

Definition 2.4. *[random-termination verifiers] Let V be a verifier of an m-round protocol. The* random-termination variant of V*, denoted as $\widetilde{\mathrm{V}}$, acts exactly as V does, but with the following additional steps: at the end of each round, $\widetilde{\mathrm{V}}$ tosses an $(1-1/4m, 1/4m)$ biased coin (i.e., 1 is tossed with probability $1/4m$), if the outcome of the coin is 1, then $\widetilde{\mathrm{V}}$ accepts and halts (where otherwise, it continues as V does).*

2.3 Smooth Sampler

Let $X^m = (X_1,\ldots,X_m)$ be a random variable and let $\varepsilon > 0$. We consider the following m-round game between Challenger and Sampler. In the i'th round, Challenger sends to Sampler a description of an event E_i, and Sampler response with x_i. Sampler wins if $(x_1,\ldots,x_m) \in E_m$. In order to make the game fair, we require that $\mathsf{Pr}_{X^m}[E_1] \geq \varepsilon$, and that for each $i > 1$ the event E_i is as good for Sampler as E_{i-1} was. Namely, $\mathsf{Pr}_{X^m|x_1,\ldots,x_{i-1}}[E_i] \geq \mathsf{Pr}_{X^m|x_1,\ldots,x_{i-1}}[E_{i-1}]$.

The above game is an abstraction of the game presented in Section 1.2 between P^* and V, where V (the Challenger) defines the new events by sending its random coins in every round, and the goal of P^* (the Sampler) is to select random coins for the emulated verifiers that (via interacting with the emulated $\mathrm{P}^{(k)^*}$) make the real verifier accept.

A straight forward wining strategy for the Sampler, which we call here the "threshold sampler", is to maintain the property that at the end of each round $\mathsf{Pr}_{X^m|x_1,\ldots,x_i}[E_i] \geq (1-\frac{i}{2m})\cdot\varepsilon$. This strategy can be implemented by sampling many candidates for x_i, till one with the above property is found. The value of $\mathsf{Pr}_{X^m|x_1,\ldots,x_i}[E_i]$ is approximated via sampling many tuples $(x'_{i+1},\ldots,x'_m) \xleftarrow{R} (X_{i+1},\ldots,X_m)$, and counting

the number of tuples $(x_1, \ldots, x_i, x'_{i+1}, \ldots, x'_m) \in E_i$. (Note that this is essentially the approach we have taken in Section 1.2).

In the following we present a different strategy for Sampler, which we call here the "smooth sampler", that was used by [HPPW08] for proving their parallel repetition theorem. While the success probability induced by this smooth sampler is not as good as that of the threshold one, its main advantage is that the analysis of its success probability is easier, in the setting where Challenger is allowed to give E_i's such that $\mathsf{Pr}_{X^m|x_1,\ldots,x_{i-1}}[E_i]$ is (slightly) smaller than what it should be. The reason being that in each round, the smooth sampler selects each x_i with probability that is proportional to $\mathsf{Pr}_{X^m|x_1,\ldots,x_i}[E_i]$. It follows a small change in the value of $\mathsf{Pr}_{X^m|x_1,\ldots,x_i}[E_i]$, might cause only a small change in the sampler winning probability. This should be compared to the threshold sampler, where only x_i's whose conditional probabilities is greater than some threshold are considered (and thus a small change in the value of $\mathsf{Pr}_{X^m|x_1,\ldots,x_{i-1}}[E_i]$, might have large effect on the sampler winning probability). In the following we define the smooth sampler, and then prove that it wins with high probability.

Algorithm 2.5 (smooth sampler)**.** Sampler.

Parameter: $t \in \mathbb{N}$.

Operation:

For $i = 1$ *to* m *do:*

1. *Get the description of* E_i *from* Challenger.
2. *Do the following for* tm/ε *times:*
   (a) *Let* $(x_i, \ldots, x_m) \leftarrow (X_i, \ldots, X_m)$.
   (b) *If* $(x_1, \ldots, x_m) \in E_i$, *break.*
3. *Send* x_i *to* Challenger.

Claim 2.6. Sampler *wins any (valid)* Challenger *with probability at least* $1 - \frac{1}{t}$.

Proof. (implicit in [HPPW08]) Let Sampler_∞ be the "infinite" version of Sampler — the loop that starts in Line 2.(a) is done till a break occurs, and let $Y_1, \ldots, Y_m$ be the value of $(x_1, \ldots, x_m)$ as sent to Challenger in a random execution of Sampler_∞. Note that Sampler_∞ wins with probability 1. For $(x_1, \ldots, x_i)$, let $v(x_1, \ldots, x_i) = \mathsf{E}_{X^m|(X_1,\ldots,X_i)=(x_1,\ldots,x_i)}[E_i]$. Using induction and the guarantee that $\mathsf{Pr}_{X^m|x_1,\ldots,x_{i-1}}[E_i] \geq \mathsf{Pr}_{X^m|x_1,\ldots,x_{i-1}}[E_{i-1}]$, we get that

$$\mathsf{Pr}[(Y_1, \ldots, Y_i) = (x_1, \ldots, x_i)] \geq \mathsf{Pr}[(X_1, \ldots, X_i) = (x_1, \ldots, x_i)] \cdot \frac{v(x_1, \ldots, x_i)}{\varepsilon} \tag{1}$$

Let T_i be the expected running time of Sampler_∞ in the i'th round, it follows that

$$T_i = \mathsf{E}_{Y_1,\ldots,Y_i}[1/v(Y_1, \ldots, Y_i)] \leq \frac{1}{\varepsilon} \cdot \mathsf{E}_{X_1,\ldots,X_i}[v(X_1, \ldots, X_i)/v(X_1, \ldots, X_i)] = \frac{1}{\varepsilon}.$$

Hence, $\mathsf{Pr}[\text{Sampler wins}] = 1 - \mathsf{Pr}[\exists i \in [m] \colon T_i > tm/\varepsilon] \geq 1 - \frac{1}{t}$. □

3 Parallel Repetition Theorem for Random-termination Protocols

In this section we formalize and prove Theorem 1.1. We start by proving the following lemma relating the soundness of the k'th parallel repetition of the random-termination variant of a verifier to that of the original verifier.

Lemma 3.1. *For every m-round verifier there exists an oracle-aided algorithm P^* such that the following holds: let $x \in \{0,1\}^*$, $n \in \mathbb{N}$, $n^5 \cdot m^{10} \leq k \in \mathrm{poly}(n)$ and $t \in [k]$. Then for any strategy $\mathrm{P}^{(k)^*}$ for which $\varepsilon_k := \mathsf{Pr}[$at least t verifiers accept in$(\mathrm{P}^{(k)^*}, \widetilde{\mathrm{V}}^{(k)})(1^n, x)] > 2^{-n/2}$, it holds that*

$$\mathsf{Pr}[(\mathrm{P}^{*\mathrm{P}^{(k)^*}}(t), \mathrm{V})(1^n, x) = 1] > \frac{2t-k}{k} - O(m \cdot k^{-\frac{1}{5}}).$$ [8]

The running time of P^* is bounded by $O(m^2 \cdot k^{6/5} \cdot T_{\mathrm{P}^{(k)^*}}/\varepsilon_k)$, where $T_{\mathrm{P}^{(k)^*}}$ is an upper bound on the execution time of $(\mathrm{P}^{(k)^*}, \widetilde{\mathrm{V}}^{(k)})(1^n, x)$.

Before proving Lemma 3.1, we first use it for proving the following restatement of Theorem 1.1.

Theorem 3.2 (restatement of Theorem 1.1)**.** *Let V be an efficient $m(n)$-round verifier, let $x \in \{0,1\}^*$, $n^5 \cdot m^{10} \leq k(n) \in \mathrm{poly}(n)$ and $t(n) \in [k(n)]$. Assume that $\mathsf{Pr}[(\mathrm{P}^*, \mathrm{V})(1^n, x) = 1] \leq \varepsilon(n)$ for any uniform [resp., non-uniform] PPT P^*, that $\delta(n) := \frac{2t(n)-k(n)}{k(n)} - \varepsilon(n) > \frac{1}{p(n)}$ for some $p \in \mathrm{poly}$ and that $k(n)$ and $\delta(n)$ are polynomial-time computable [resp., arbitrary] functions. Then the following holds for any uniform [resp., non-uniform] PPT $\mathrm{P}^{(k)^*}$*

$$\mathsf{Pr}[\text{at least } t(n) \text{ verifiers accept in}(\mathrm{P}^{(k)^*}, \widetilde{\mathrm{V}}^{(k)})(1^n, x)] \leq \max\{\mathrm{neg}(n), \exp(-(\frac{\delta(n)}{m})^5 \cdot k(n))\}.$$

Proof. We give the proof for the non-uniform case, where the proof of the uniform case follows essentially the very same lines. Assume towards a contradiction the existence of a non-uniform algorithm $\mathrm{P}^{(k)^*}$ that violates the statement of Theorem 1.1 with respect to parameters k and t. Let $C > 0$ be the implicit constant in the term $O(m \cdot k^{-\frac{1}{5}})$ given in Lemma 3.1 and let $k' \in O(m^5/\delta(n)^5)$ be the first multiple of k stratifying $C \cdot m \cdot k^{-\frac{1}{5}} < \delta(n)/2$. Lemma 3.2 yields that for $t' = \frac{k'}{k} \cdot t$ and any (non uniform) PPT $\mathrm{P}^{(k')^*}$, it holds that $\varepsilon^{\mathrm{P}^{(k')^*}}_{k',t'}(n) := \mathsf{Pr}[$at least $t'(n)$ verifiers accept in$(\mathrm{P}^{(k')^*}, \widetilde{\mathrm{V}}^{(k')})(1^n, x)] \in \mathrm{neg}(n)$.

Consider the following implementation of $\mathrm{P}^{(k')^*}$: this cheating prover interacts with $\widetilde{\mathrm{V}}^{(k')}$ on x by invoking k'/k copies of $\mathrm{P}^{(k)^*}$. Namely, $\mathrm{P}^{(k')^*}$ partitions the verifiers in $\widetilde{\mathrm{V}}^{(k')}$ into groups of size k and acts as $\mathrm{P}^{(k)^*}$ against each of this groups. It follows that $\varepsilon^{\mathrm{P}^{(k')^*}}_{k',t'}(n) \geq \exp(-(\frac{\delta(n)}{m})^5 \cdot k(n))^{k'/k(n)} = \exp(-(\frac{\delta(n)}{m})^5 \cdot k') \in O(\exp(-C))$, deriving a contradiction. □

Proof. (of Lemma 3.1) We assume for simplicity that $\mathrm{P}^{(k)^*}$ is deterministic, since the only effect of handling randomized $\mathrm{P}^{(k)^*}$ would be in complicating notations. (Alternatively, once can reduce the randomized case to the deterministic one by finding (via sampling) "good" random coins). We omit 1^n and x from our notations whenever their values are clear from the context.

Let $\mathrm{len} \in \mathbb{N}$ be a bound on the number of random coins used by V, in any interaction on security parameter 1^n. We assume without loss of generality that the partial view of $\widetilde{\mathrm{V}}^{(k)}$ in an interaction with $\mathrm{P}^{(k)^*}$ is of the form $\mathrm{view} = (r^k, \mathcal{S}_1, \ldots, \mathcal{S}_\ell)$, where $r^k \in \{0,1\}^{k \cdot \mathrm{len}}$ denotes the random coins of the k embedded V's inside $\widetilde{\mathrm{V}}^{(k)}$ and $\mathcal{S}_j$ (for $j \in \{2, \ldots, \ell\}$) denotes the indices of those verifiers that decided to halt at the end of the $(j-1)$ round. (Since $\mathrm{P}^{(k)^*}$ is deterministic, we omit the messages its sends from $\widetilde{\mathrm{V}}^{(k)}$'s view). We let $\mathrm{view}_j = (r^k, \mathcal{S}_1, \ldots, \mathcal{S}_j)$, let $\mathcal{S}_j(\mathrm{view})$ be the value of the entry '$\mathcal{S}_j$' in view, and let $r^k(\mathrm{view})$ be the value of the entry 'r^k' in view. We let $\mathcal{S}_{\leq j}(\mathrm{view}) := \bigcup_{j'=1}^{j} \mathcal{S}_{j'}(\mathrm{view})$ and $\mathcal{S}_{>j}(\mathrm{view}) := [k] \setminus \mathcal{S}_{\leq j}(\mathrm{view})$. Finally, we let $\mathrm{round}(\mathrm{view} = (r^k, \mathcal{S}_1, \ldots, \mathcal{S}_\ell)) := \ell$ and set $\mathrm{round}(\perp) := 0$.

In order to simplify notations, we start by describing an algorithm $\widehat{\mathrm{P}}$ that given V's random coins as input, makes V accept with high probability. It will clear be from the description of $\widehat{\mathrm{P}}$, however, that it can

[8] By considering a random termination variant of V that halts in each round with probability $\frac{1}{mn}$ (rather than $\frac{1}{4m}$) and $k > m^{10}n^{15}$, the term $\frac{2t-k}{k} - O(m \cdot k^{-\frac{1}{5}})$ can be replace with $\frac{t-k}{k} - O(m \cdot k^{-\frac{1}{15}})$.

be implemented without using this knowledge of V's coins. Algorithm $\widehat{\mathrm{P}}$ follows rather closely the intuition given in Section 1.2, where the main difference is that in order to choose the emulated verifiers random coins, we are using a variant of the "smooth sampler" described in Section 2.3, rather than the threshold approach we described in the introduction. In the following we say that $\widetilde{\mathrm{V}}^{(k)}$ accepts, if at least t of the $\widetilde{\mathrm{V}}$'s accept in the end of the interaction, and set $\mu = k^{-1/5}$.

Algorithm 3.3. $\widehat{\mathrm{P}}$.

Oracle: ${\mathrm{P}^{(k)}}^*$.

Input *A string* $r \in \{0,1\}^{\mathrm{len}}$.

Operation:

1. *Choose* $i^* \in [k]$ *uniformly at random and set* view $=\perp$.
2. *For* $j = 1$ *to* m *do:*
   (a) *Get the message* q^j *from* V.
   (b) *Set* view $= \mathrm{GetNextView}^{{\mathrm{P}^{(k)}}^*}(\mathrm{view}, i^*, r)$.
   (c) *Send* $a^j_{i^*}$ *to* V, *where* a^j *is the message that* ${\mathrm{P}^{(k)}}^*$ *sends to* $\widetilde{\mathrm{V}}$ *in the* j*'th round of* view.

Algorithm 3.4. GetNextView.

Oracle: ${\mathrm{P}^{(k)}}^*$

Input: $\widetilde{\mathrm{V}}^{(k)}$*'s view —* view, *an index* $i^* \in [k] \cup \perp$ *and a string* $r \in \{0,1\}^{\mathrm{len}} \cup \perp$.

Operation:

1. *Let* round $=$ round(view) $+ 1$, *and do the following for* $\frac{m}{\mu \cdot \varepsilon_k}$ *times:*
   (a) *Choose a random value* view′ *for a complete view of* $\widetilde{\mathrm{V}}^{(k)}$ *in* $({\mathrm{P}^{(k)}}^*, \widetilde{\mathrm{V}}^{(k)})$, *conditioned on* $\mathrm{view}'_{\mathrm{round}-1} = \mathrm{view}$, *on* $i^* \in \mathcal{S}_{\mathrm{round}+1}(\mathrm{view}')$ *and on one of the following conditions:*
      i. *If* view $=\perp$, *on* $r^k(\mathrm{view}')_{i^*} = r$.
      ii. *Otherwise, on* $i^* \notin \mathcal{S}_{\mathrm{round}}(\mathrm{view}')$.
   (b) *If* $\widetilde{\mathrm{V}}^{(k)}$ *accepts in* view′, *return* $\mathrm{view}'_{\mathrm{round}}$.
2. *Abort the execution.*

We assume that $\widehat{\mathrm{P}}$ outputs the value of (view, i^*) at the end of the execution (we set this value to $\perp$ if $\widehat{\mathrm{P}}$ aborts), and let $\mathsf{P}^0_{\mathrm{View},I^*}$ be the output distribution of $\widehat{\mathrm{P}}$ induced by an execution of $(\widehat{\mathrm{P}}(U_{\mathrm{len}}), \mathrm{V}(U_{\mathrm{len}}))$. We say that $\mathrm{Emb}(\widetilde{\mathrm{V}}_i)$ accepts in view $= (r^k, \mathcal{S}_1, \ldots, \mathcal{S}_m)$, if the embedded V inside $\widetilde{\mathrm{V}}_i$ does. We are interested in the probability over $\mathsf{P}^0_{\mathrm{View},I^*}$ that $\mathrm{Emb}(\widetilde{\mathrm{V}}_{I^*})$ accepts in View, for lower bounding this probability we introduce the following family of experiments $\{\mathrm{Exp}^\ell\}_{\ell \in [m]}$.

Experiment 3.5. Exp^ℓ.

1. *Set* view $=\perp$.
2. *For* $j = 1$ *to* ℓ *do:*
   set view $= \mathrm{GetNextView}^{{\mathrm{P}^{(k)}}^*}(\mathrm{view}, \perp, \perp)$ *(where we define that if* GetNextView *is called with* $i^* = \perp$, *then it does the sampling of Line* 1.(*a*) *without the conditioning on* i^**.)*

3. *Select uniformly at random* $i^* \in \mathcal{S}_{>\ell}(\text{view})$.

4. *For* $j = \ell + 1$ *to* m *do:*

   set $\text{view} = \text{GetNextView}^{\mathrm{P}^{(k)*}}(\text{view}, i^*, \perp)$.

5. *Output* (view, i^*).

Let $\mathsf{P}^{\ell}_{\text{View},I^*}$ be the output distribution of Exp^{ℓ} (where in case Exp^{ℓ} aborts, we set its output to $\perp$). The proof of Theorem 3.2 follows by the next two claims.

Claim 3.6. $\mathsf{P}^{m}_{\text{View},I^*}(\text{Emb}(\widetilde{\mathrm{V}}_{I^*})$ *accepts in* $\text{View}) \geq \frac{2t-k}{k} - O(\mu)$.

Claim 3.7. $\left\|\mathsf{P}^{0}_{\text{View},I^*} - \mathsf{P}^{m}_{\text{View},I^*}\right\| \in O(m \cdot \mu)$.

Before proving the above claims, let us first use them for proving Theorem 3.2. By Claim 3.7 and Claim 3.6, we have that $\widehat{\mathrm{P}}$ makes V accept with probability $\frac{2t-k}{k} - O(m\mu)$. Note that $\widehat{\mathrm{P}}$ calls $\text{GetNextView}(\text{view}, i^*, r)$ only *after* receiving the first $\text{round}(\text{view}) + 1$ messages from V, where knowing these messages suffices for the computation of $\text{GetNextView}(\text{view}, i^*, r)$. Hence, the proof of Theorem 3.2 follows by letting P^* act as $\widehat{\mathrm{P}}$ while using the messages it gets from V rather than the knowledge of r. □

Proof. (of Claim 3.6) Note that algorithm $\widehat{\mathrm{P}}$ acts in Exp^m exactly as Sampler from Algorithm 2.5, with respect to $X^m = (X_1, \ldots, X_{m+1})$ taken as the value of $(r^k, \mathcal{S}_2, \ldots, \mathcal{S}_{m+1})$ in a random execution of $(\mathrm{P}^{(k)*}, \widetilde{\mathrm{V}}^{(k)})$, and $E_1 = E_2 = \ldots, E_{m+1}$ defined as the event that $\widetilde{\mathrm{V}}^{(k)}$ accepts in $\text{view} = (X_1, \ldots, X_{m+1})$. Hence, Claim 2.6 yields that

$$\mathsf{P}^{m}_{\text{View},I^*}(\perp) \leq \mu \cdot \frac{m+1}{m} \in O(\mu) \tag{2}$$

For $\text{view} = (r^k, \mathcal{S}_1, \ldots, \mathcal{S}_m)$, let $\text{Acc}(\text{view}) = \{i \in \mathcal{S}_{>m}(\text{view})\colon \text{Emb}(\widetilde{\mathrm{V}}_{I^*})$ accepts in $\text{view}\}$ and let W be the event that $\widehat{\mathrm{P}}$ does not aborts in Exp^m and $\frac{|\text{Acc}(\text{View})|}{|\mathcal{S}_{>m}(\text{View})|} < \frac{2t-k}{k}$. We complete the proof by showing that the probability of W is bounded by $O(\mu)$. Let View_{m+1} be the value of the first accepting view′ sampled in the $m+1$ call to GetNextView done in the execution of Exp^m (where we set it to $\perp$ if no such called occurred). We note that if the output of Exp^m is $(\text{View}, I^*) \neq \perp$, then $\text{Acc}(\text{View}) + \mathcal{S}_{\leq m+1}(\text{View}_{m+1}) \geq t$. Hoeffding's inequality yields that $\mathsf{P}^{m}_{\text{View},I^*}(\text{View}_{m+1} \neq \perp \wedge \mathcal{S}_{\leq m+1}(\text{View}_{m+1}) > k/2) \in O(\mu)$, and we conclude that

$$\begin{aligned}
&\mathsf{P}^{m}_{\text{View},I^*}\Big(\frac{|\text{Acc}(\text{View})|}{|\mathcal{S}_{>m}(\text{View})|} < \frac{t-(k/2)}{k/2}\Big) \\
&\leq \mathsf{P}^{m}_{\text{View},I^*}\Big(\frac{t-|\mathcal{S}_{\leq m+1}(\text{View}_{m+1})|}{k-|\mathcal{S}_{\leq m}(\text{View})|} < \frac{t-(k/2)}{k/2}\Big) \\
&\leq \mathsf{P}^{m}_{\text{View},I^*}\Big(\frac{t-|\mathcal{S}_{\leq m+1}(\text{View}_{m+1})|}{k-|\mathcal{S}_{\leq m+1}(\text{View}_{m+1})|} < \frac{t-(k/2)}{k/2}\Big) \\
&\in O(\mu).
\end{aligned}$$

□

Proof. (of Claim 3.7) Given a $\text{view} = (r^k, \mathcal{S}_1, \ldots, \mathcal{S}_j)$, let $k(\text{view}) = |\mathcal{S}_{>j}(\text{view})|$ and identify the indices in $\mathcal{S}_{>j}(\text{view})$ with the set $[k(\text{view})]$. Using induction and Hoeffding's inequality, we have that

$$\mathsf{P}^{m}_{\text{View},I^*}(k(\text{View}) < k/2 \wedge \text{View} \neq \perp) \in O(2^{-n/2}) \tag{3}$$

Let $\alpha(\text{view}) = \mathsf{P}^m_{\text{View},I^*}(\overline{\perp} \mid \text{View}_j = \text{view})$. Since Exp^m makes at most $\frac{m^2}{\mu \cdot k}$ random samplings, it follows that

$$\mathsf{P}^m_{\text{View},I^*}(\exists j \in [m] \colon \alpha(\text{View}_j) < 2^{-n} \wedge \text{View} \neq \perp) \in O(2^{-n/4}) \tag{4}$$

Finally, let $\text{Typical} = \{(\text{view}, i) \in \text{Supp}(\mathsf{P}^m_{\text{View},I^*}) \setminus \{\perp\} \colon k(\text{view}) \geq k/2 \wedge \ \forall j \in [m] \qquad \alpha(\text{view}_j) \geq 2^{-n}\}$. Equations (2), (3) and (4) yield that

$$\mathsf{P}^m_{\text{View},I^*}(\overline{\text{Typical}}) \leq O(2^{-n/2}) + O(2^{-n/4}) + O(\mu) \in O(\mu) \tag{5}$$

and we conclude the proof of Claim 3.7 using the following claim:

Claim 3.8. *For every $\ell \in \{0, \ldots, m-1\}$ it holds that $\left\|\mathsf{P}^{\ell+1}_{\text{View},I^*} - \mathsf{P}^{\ell}_{\text{View},I^*}\right\|_{\text{Typical}} \in O(\mu)$.*

Hence,

$$\begin{aligned}
&\left\|\mathsf{P}^m_{\text{View},I^*} - \mathsf{P}^0_{\text{View},I^*}\right\| \\
&\leq \quad \mathsf{P}^m_{\text{View},I^*}(\overline{\text{Typical}}) + 2 \cdot \sum_{\ell=0}^{m-1} \left\|\mathsf{P}^{\ell+1}_{\text{View},I^*} - \mathsf{P}^{\ell}_{\text{View},I^*}\right\|_{\text{Typical}} \\
&\in \quad O(\mu) + O(m \cdot \mu) \in O(m \cdot \mu).
\end{aligned}$$

where the first inequality follows by Proposition 2.1, and second inequality follows by (5) and Claim 3.8. □

Proof. (of Claim 3.8) We prove the case of $\ell \in [m-1]$ and describe later how to adjust the proof for the case of $\ell = 0$. Since the only difference between $\mathsf{P}^{\ell+1}_{\text{View},I^*}$ and $\mathsf{P}^{\ell}_{\text{View},I^*}$ is in the $\ell+1$ call to GetNextView and in the method applied for choosing I^*, it suffices to bound the statistical distance between the following distributions for every non aborting $\text{view} = (r^k, \mathcal{S}_1, \ldots, \mathcal{S}_\ell)$, for which $k_\ell = k(\text{view}) \geq k/2$ and $\alpha_\ell = \alpha(\text{view}) \geq 2^{-n}$.

- $\mathsf{D}^0_{I^*,S} := \left(I^* \xleftarrow{\text{R}} \mathcal{S}_{>\ell}(\text{view}), S = \mathcal{S}_{\ell+1}(\text{GetNextView}(\text{view}, I^*, \perp)\right)$
- $\mathsf{D}^1_{I^*,S} := \left(S = \mathcal{S}_{\ell+1}(\text{GetNextView}(\text{view}, \perp, \perp)), I^* \xleftarrow{\text{R}} S\right)$

where the above distributions take the value $\perp$ in case that GetNextView aborts. In the following we prove the existence of a set $\mathcal{T} \subseteq [k_\ell] \times 2^{[k_\ell]}$ such that the following hold:

1. $\mathsf{D}^1_{I^*,S}(\overline{\mathcal{T}}) \in O(\mu)$, and
2. for every $(i, \mathcal{S}) \in T$, it holds that $\mathsf{D}^1_{I^*,S}(i, \mathcal{S}) \in (1 \pm O(\mu)) \cdot \mathsf{D}^0_{I^*,S}(i, \mathcal{S})$.

The existence of $\mathcal{T}$ concludes the proof of Claim 3.8, since Proposition 2.1 yields that

$$\left\|\mathsf{D}^1_{I^*,S} - \mathsf{D}^0_{I^*,S}\right\| \leq \mathsf{D}^1_{I^*,S}(\overline{T}) + 2 \cdot \left\|\mathsf{D}^1_{I^*,S} - \mathsf{D}^0_{I^*,S}\right\|_T \in O(\mu).$$

Let $p = 1/4m$. For $\mathcal{S} \subseteq [k_\ell]$, let $\delta(\mathcal{S})$ be the probability that $\widetilde{\text{V}}^{(k)}$ accepts in a random continuation of $(\text{P}^{(k)*}, \widetilde{\text{V}}^{(k)})$, conditioned on view and on $\mathcal{S}_{\ell+1} = \mathcal{S}$ (i.e., $\delta(\mathcal{S}) = \alpha(\text{view}, \mathcal{S})$). Similarly, for $\mathcal{Y} \subseteq [k_\ell] \setminus \mathcal{S}$ let $\delta(\mathcal{S}, \mathcal{Y})$ be the above probability where we also condition on $\mathcal{S}_{\ell+2} = \mathcal{Y}$. The distribution $\mathsf{D}^1_{I^*,S}$ can be now described as the output of the following process: repeat till success for at most $\frac{m}{\mu \cdot k}$ times — select $S \xleftarrow{\text{R}} U^p_{[k_\ell]}$ and $I^* \xleftarrow{\text{R}} [k_\ell] \setminus S$, and output (I^*, S) with probability $\delta(S)$. Similarly, the following process describes $\mathsf{D}^0_{I^*,S}$: select $I^* \xleftarrow{\text{R}} [k_\ell]$ and repeat till success for at most $\frac{m}{\mu \cdot k}$ times — select $S \xleftarrow{\text{R}} U^p_{[k_\ell],i=0}$ and $Y \xleftarrow{\text{R}} U^p_{[k_\ell]\setminus S,i=1}$, and output (I^*, S) with probability $\delta(S, Y)$.

Let $\text{TypicalSets} := \{\mathcal{S} \subseteq [k_\ell] \colon \delta(S) \geq 2^{-2n} \wedge |S| \in (1 \pm \mu) \cdot k_\ell\}$. Let $\text{GlobalEffect} := \{i \in [k_\ell] \colon \delta(S = U^p_{[k_\ell],i=0}, U^p_{[k_\ell]\setminus S,i=1}) \notin (1 \pm \mu) \cdot \alpha_\ell\}$ (i.e., $i \in \text{GlobalEffect}$ if by conditioning that $i \in \mathcal{S}_{\ell+2}$, one significantly

effects the probability that $\widetilde{\mathrm{V}}^{(k)}$ accepts in a random continuation of $(\mathrm{P}^{(k)^*}, \widetilde{\mathrm{V}}^{(k)})$ conditioned on view). Finally, let LocalEffect $:= \{(i,S)\colon \delta(\mathcal{S}, U^p_{[k_\ell]\setminus\mathcal{S},i=1}) \notin (1\pm\mu)\cdot\delta(\mathcal{S})\}$ (i.e., $(i,S) \in$ LocalEffect if by conditioning that $i \in \mathcal{S}_{\ell+2}$, one significantly effects the probability that $\widetilde{\mathrm{V}}^{(k)}$ accepts in a random continuation of $(\mathrm{P}^{(k)^*}, \widetilde{\mathrm{V}}^{(k)})$ conditioned on view and $\mathcal{S}_{\ell+1} = S$). We define the set $\mathcal{T}$ as $\{(i,S) \in [k_\ell] \times 2^{[k_\ell]}\colon \mathcal{S} \in \text{TypicalSets} \wedge i \notin \text{GlobalEffect} \wedge (i,S) \notin \text{LocalEffect}\}$. Note that for every $\mathcal{S} \in$ TypicalSets and $i \in ([k_\ell]\setminus\mathcal{S})$ it holds that

$$\begin{aligned}
\mathsf{D}^1_{I^*,S}(i,\mathcal{S}) &= \mathsf{D}^1_{I^*,S}(S=\mathcal{S})\cdot\mathsf{D}^1_{I^*,S}(i,\mathcal{S}\mid S=\mathcal{S}) \\
&= \mathsf{D}^1_{I^*,S}(S=\mathcal{S}\mid\not\perp)\cdot(1-\mathsf{D}^1_{I^*,S}(\perp))\cdot\frac{1}{|\mathcal{S}|} \\
&= \frac{\mathsf{Pr}_{U^p_{[k_\ell]}}[\mathcal{S}]\cdot\delta(\mathcal{S})}{\alpha_\ell}\cdot(1-2^{-\Omega(n)})\cdot\frac{1}{|\mathcal{S}|} \\
&\in \frac{\mathsf{Pr}_{U^p_{[k_\ell]}}[\mathcal{S}]\cdot\delta(\mathcal{S})}{\alpha_\ell}\cdot(1\pm O(\mu))\cdot\frac{1}{(1-p)\cdot k_\ell},
\end{aligned}$$

where the last equality follows since $\mathsf{D}^1_{I^*,S}(\perp) \le (1-\alpha_\ell)^{\frac{m}{\mu\cdot\varepsilon_k}} \in 2^{-\Omega(n)}$. On the other hand, the following holds for every $(i,\mathcal{S}) \notin$ LocalEffect where $i \notin$ GlobalEffect,

$$\begin{aligned}
\mathsf{D}^0_{I^*,S}(i,\mathcal{S}) &= \mathsf{D}^0_{I^*,S}(I^*=i)\cdot\mathsf{D}^0_{I^*,S}(i,\mathcal{S}\mid I^*=i) \\
&= \frac{1}{n}\cdot\mathsf{D}^0_{I^*,S}(i,\mathcal{S}\mid I^*=i\mid\not\perp)\cdot(1-\mathsf{D}^0_{I^*,S}(\perp\mid I^*=i)) \\
&= \frac{1}{n}\cdot\frac{\mathsf{Pr}_{U^p_{[k_\ell],i=0}}[\mathcal{S}]\cdot\delta(\mathcal{S},U^p_{[k_\ell]\setminus S,i=1})}{\delta(S=U^p_{[k_\ell],i=0},U^p_{[k_\ell]\setminus S,i=1})}\cdot(1-2^{-\Omega(n)}) \\
&\in (1\pm O(\mu))\cdot\frac{1}{n}\cdot\frac{\mathsf{Pr}_{U^p_{[k_\ell],i=0}}[\mathcal{S}]\cdot\delta(\mathcal{S})}{\alpha_\ell} \\
&\in (1\pm O(\mu))\cdot\frac{1}{n}\cdot\frac{1}{(1-p)\cdot k_\ell}\cdot\frac{\mathsf{Pr}_{U^p_{[k_\ell]}}[\mathcal{S}]\cdot\delta(\mathcal{S})}{\alpha_\ell},
\end{aligned}$$

where the second equation holds since $\mathsf{D}^0_{I^*,S}(\perp\mid I^*=i) < (1-\frac{\alpha_\ell}{2})^{\frac{m}{\mu\cdot\varepsilon_k}} \in 2^{-\Omega(n)}$ for every $i \notin$ GlobalEffect, and the first ' $\in$' is immediate by the definitions of GlobalEffect and LocalEffect. Since for $i \in \mathcal{S}$ it holds that $\mathsf{D}^0_{I^*,S}(i,\mathcal{S}) = \mathsf{D}^1_{I^*,S}(i,\mathcal{S}) = 0$, it follows that $\mathsf{D}^0_{I^*,S}(i,\mathcal{S}) \in 1\pm O(\mu))\cdot\mathsf{D}^1_{I^*,S}(i,\mathcal{S})$ for every $(i,\mathcal{S}) \in \mathcal{T}$. In the following we prove that $\mathsf{D}^0_{I^*,S}(i,\mathcal{S})(\overline{\mathcal{T}})$ is small.

By Hoeffding's inequality (recall that $k_\ell > k/2 \in O(n^5\cdot m^{10})$) we have that $\mathsf{Pr}_{U^p_{[k_\ell]}}(\mathcal{S}) < 2^{-n}$ for every $\mathcal{S} \in [k_\ell]$ with $|\mathcal{S}| \notin (1\pm\mu)\cdot k_\ell$. Hence, for every set $\mathcal{S} \in (2^{[k_\ell]} \setminus \text{TypicalSets})$ it holds that $\mathsf{Pr}_{U^p_{[k_\ell]}}(\mathcal{S})\cdot\delta(\mathcal{S}) \in O(2^{-n/2})$, and therefore

$$\begin{aligned}
\mathsf{D}^1_{I^*,S}(S\notin\text{TypicalSets}) &= \mathsf{D}^1_{I^*,S}(\perp) + \mathsf{D}^1_{I^*,S}(S\in(2^{[k_\ell]}\setminus\text{TypicalSets})) \qquad (6)\\
&\in \frac{O(2^{-n/2})}{\alpha_\ell} + 2^{-\Omega(n)} \in O(\mu)
\end{aligned}$$

Consider the random variables $S \overset{\mathrm{R}}{\leftarrow} U^p_{[k_\ell]}$, $Y \overset{\mathrm{R}}{\leftarrow} U^p_{[k_\ell]\setminus S}$ and $X_1 = (B_{1,1}, B_{1,2}), \ldots, X_{k_\ell} = (B_{k_\ell,1}, B_{k_\ell,2})$, where $B_{i,1} = 1$ iif $i \in S$, and $B_{i,2} = 1$ iif $i \in Y$. Let W be the random variable that takes the value 1 iff $\widetilde{\mathrm{V}}^{(k)}$ accepts in a random continuation of $(\mathrm{P}^{(k)^*}, \widetilde{\mathrm{V}}^{(k)})$ conditioned on view, $\mathcal{S}_{\ell+1} = S$ and $\mathcal{S}_{\ell+2} = Y$, Proposition 2.2

yields that

$$\begin{aligned}
&\mathsf{Pr}_{i\xleftarrow{R}[k_\ell]}\big[\mathsf{Pr}[W \mid X_i = (0,1)] \notin (1 \pm \mu)\cdot \mathsf{Pr}[W]\big] \qquad (7)\\
&\leq \frac{1}{(1-p)\cdot p}\cdot \mathsf{Pr}_{i\xleftarrow{R}[k_\ell],x\xleftarrow{R}X_i}\big[\mathsf{Pr}[W \mid X_i = x]\\
&\quad \notin (2 \pm \mu)\cdot \mathsf{Pr}[W]\big]\\
&\leq \frac{1}{(1-p)\cdot}\cdot\frac{2}{\mu}\cdot\sqrt{\frac{-\log \mathsf{Pr}[W]}{k_\ell}}
\end{aligned}$$

It follows that $|\text{GlobalEffect}| \in O(k_\ell \cdot \mu)$ and therefore

$$\mathsf{D}^1_{I^*,S}(I^* \in \text{GlobalEffect} \wedge S \in \text{TypicalSets}) \leq \frac{|\text{GlobalEffect}|}{|\mathcal{S}|} \in O(\mu) \qquad (8)$$

Consider now the following random variables defined with respect to a fixed set $\mathcal{S} \subseteq [k_\ell]$: $Y \xleftarrow{R} U^p_{[k_\ell]\setminus\mathcal{S}}$ and $X_1,\ldots,X_{k_\ell-|\mathcal{S}|}$, where $X_i = 1$ iif the i'th element of $[k_\ell]\setminus\mathcal{S}$ is in Y. Let W be the random variable that takes the value 1 iff $\widetilde{\mathrm{V}}^{(k)}$ accepts in a random continuation of $(\mathrm{P}^{(k)^*},\widetilde{\mathrm{V}}^{(k)})$ conditioned on view, $\mathcal{S}_{\ell+1} = \mathcal{S}$ and $\mathcal{S}_{\ell+2} = Y$, Proposition 2.2 yields that

$$\begin{aligned}
&\mathsf{Pr}_{i\xleftarrow{R}[k_\ell-|\mathcal{S}|]}\big[\mathsf{Pr}[W \mid X_i = 1] \notin (1 \pm \mu)\cdot \mathsf{Pr}[W]\big]\\
&\leq \frac{1}{p}\cdot \mathsf{Pr}_{i\xleftarrow{R}[k_\ell-|\mathcal{S}|],x\xleftarrow{R}X_i}\big[\mathsf{Pr}[W \mid X_i = x] \notin (1 \pm \mu)\cdot \mathsf{Pr}[W]\big]\\
&\leq \frac{2}{p\cdot\mu}\cdot\sqrt{\frac{-\log \mathsf{Pr}[W]}{k_\ell-|\mathcal{S}|}}.
\end{aligned}$$

It follows that for every $\mathcal{S}$ with $\delta(\mathcal{S}) > 2^{-n}$, it holds that $|\{i \in \mathcal{S}\colon (i,\mathcal{S}) \in \text{LocalEffect}\}| \in O(\mu)\cdot(k_\ell - |\mathcal{S}|)$. Hence,

$$\mathsf{D}^1_{I^*,S}((I^*,S) \in \text{LocalEffect} \wedge S \in \text{TypicalSets}) \in \sum_{\mathcal{S}\in\text{TypicalSets}} \mathsf{D}^1_{I^*,S}(S = \mathcal{S})\cdot O(\mu) \in O(\mu) \qquad (9)$$

We conclude that $\mathsf{D}^1_{I^*,S}(\overline{\mathcal{T}}) = \mathsf{D}^1_{I^*,S}(\overline{\text{TypicalSets}}) + \mathsf{D}^1_{I^*,S}((I^*,S) \in \text{GlobalEffect} \wedge S \in \text{TypicalSets}) + \mathsf{D}^1_{I^*,S}((I^*,S) \in \text{LocalEffect} \wedge S \in \text{TypicalSets}) \in O(\mu)$.

The case $\ell = 0$ The proof of this case follows very closely the proof for $\ell > 0$ given above. In the following we only describe the differences between these proofs. As in the case of $\ell > 0$, it suffices to prove that the following distributions are statistically close.

- $\mathsf{D}^0_{I^*,R^k} := (I^* \xleftarrow{R} [k], R^k = r^k(\text{GetNextView}(\bot, I^*, \bot))$
- $\mathsf{D}^1_{I^*,R^k} := \big(R^k = r^k(\text{GetNextView}(\bot,\bot,\bot)), I^* \xleftarrow{R} [k]\big)$

For $r^k \in \{0,1\}^{k\cdot\text{len}}$, let $\delta(r^k)$ be the probability that $\widetilde{\mathrm{V}}^{(k)}$ accepts in a random execution of $(\mathrm{P}^{(k)^*},\widetilde{\mathrm{V}}^{(k)})$, conditioned that the $\widetilde{\mathrm{V}}^{(k)}$ random coins are equal to r^k. For $\mathcal{Y} \subseteq [k]$, let $\delta(r^k,\mathcal{Y})$ be the above probability where we also condition on $\mathcal{S}_2 = \mathcal{Y}$.

Given $r^k \in \{0,1\}^{k\cdot\text{len}}$, we sometimes view r^k as composed of k blocks of length len and denote its i'th block by $r^k_{B(i)}$. Similarly, we let the random variable $U_{k\cdot\text{len},B(i)=r}$ be uniformly distributed over

$\{0,1\}^{k\cdot \text{len}}$ conditioned that the i'th block is equal to r. We continue by letting TypicalCoins $:= \{r^k \in \{0,1\}^{k\cdot\text{len}} \colon \delta(r^k) \geq 2^{-n}\}$, GlobalEffect $:= \{(i,r) \in [k] \times \{0,1\}^{\text{len}} \colon \delta(U_{k\cdot\text{len},B(i)=r}, U^p_{[k],i=1}) \notin (1 \pm \mu)\cdot\varepsilon_k\}$, and LocalEffect $:= \{(i,r^k) \colon \delta(r^k, U^p_{[k],i=1}) \notin (1\pm\mu)\cdot\delta(r^k)\}$. Finally, we let $\mathcal{T} := \{(i,r^k) \in [k] \times \{0,1\}^{k\cdot\text{len}} \colon r^k \in \text{TypicalCoins} \wedge (i, r^k_{B(i)}) \notin \text{GlobalEffect} \wedge (i,r^k) \notin \text{LocalEffect}\}$.

It is easy to verify that $\mathsf{D}^0_{I^*,R^k}(i,r^k) \in (1\pm O(\mu))\cdot \mathsf{D}^1_{I^*,R^k}(i,r^k)$ for every $(i,r^k) \in \mathcal{T}$, and that $\mathsf{D}^1_{I^*,R^k}(R^k \notin \text{TypicalCoins}) \in O(\mu)$. Moreover, a very similar argument to the one used in the case $\ell > 0$, yields that $\mathsf{D}^1_{I^*,R^k}(\text{LocalEffect}) \in O(\mu)$. Hence, it is left to prove that $\mathsf{D}^1_{I^*,R^k}((I^*, R^k_{B(I^*)}) \in \text{GlobalEffect}) \in O(\mu)$. a very similar argument to that used in the proof of (7) yields that

$$\mathsf{Pr}_{i\xleftarrow{R}[k],r\xleftarrow{R}\{0,1\}^{\text{len}}}\left[\delta(U_{k\cdot\text{len},B(i)=r}, U^p_{[k],i=1})] \notin (1\pm\mu)\cdot\varepsilon_k\right] \in O(\mu) \tag{10}$$

Namely, $\mathsf{Pr}_{i\xleftarrow{R}[k],r\xleftarrow{R}\{0,1\}^{\text{len}}}[(i,r) \in \text{GlobalEffect}] \in O(\mu)$, where the same lines also yield that

$$\mathsf{Pr}_{i\xleftarrow{R}[k],r\xleftarrow{R}\{0,1\}^{\text{len}}}\left[\delta(U_{k\cdot\text{len},B(i)=r}, U^p_{[k]})] \notin (1\pm\mu)\cdot\varepsilon_k\right] \in O(\mu) \tag{11}$$

The above equation yields that $\mathsf{Pr}_{i\xleftarrow{R}[k],r\xleftarrow{R}\{0,1\}^{\text{len}}}[(i,r) \in \text{GlobalEffect}'] \in O(\mu)$, where GlobalEffect$'$ $:= \{(i,r) \in [k] \times \{0,1\}^{\text{len}} \colon \delta(U_{k\cdot\text{len},B(i)=r}, U^p_{[k]}) \notin (1\pm\mu)\cdot\varepsilon_k\}$ (i.e., the difference comparing to GlobalEffect$'$, is that we do not condition on $i \in \mathcal{S}_2$). Hence,

$$\begin{aligned}&\mathsf{E}_{i\xleftarrow{R}[k],r^k\xleftarrow{R}\{0,1\}^{k\cdot\text{len}}}\left[((i,r^k_{B(i)}) \notin \text{GlobalEffect} \cup \text{GlobalEffect}')\cdot\delta(r^k)\right]\\ &\quad\geq (1-O(\mu))\cdot(1-\mu)\cdot\varepsilon_k > (1-O(\mu))\cdot\varepsilon_k.\end{aligned}$$

We conclude that

$$\begin{aligned}&\mathsf{D}^1_{I^*,R^k}((I^*,R^k_{B(I^*)}) \in \text{GlobalEffect})\\ &\leq\quad \mathsf{D}^1_{I^*,R^k}((I^*,R^k_{B(I^*)}) \in \text{GlobalEffect} \cup \text{GlobalEffect}') \in O(\mu).\end{aligned}$$

□

Acknowledgment

I am very thankful to Oded Goldreich, Thomas Holenstein, Tal Moran, Rafael Pass, Omer Reingold,, Alex Samorodnitsky and Salil Vadhan for very useful discussions.

References

[BIN97] Mihir Bellare, Russell Impagliazzo, and Moni Naor. Does parallel repetition lower the error in computationally sound protocols? In *Proceedings of the 37th Annual Symposium on Foundations of Computer Science (FOCS)*, 1997.

[BM88] László Babai and Shlomo Moran. Arthur-Merlin games: A randomized proof system and a hierarchy of complexity classes. *Journal of Computer and System Sciences*, 36:254–276, 1988.

[CHS] Ran Canetti, Shai Halevi, and Michael Steiner. Hardness amplification of weakly verifiable puzzles. In *Theory of Cryptography, Second Theory of Cryptography Conference (TCC)*.

[DP98] Ivan B. Damgård and Birgit Pfitzmann. Sequential iteration arguments and an efficient zero-knowledge argument for NP. In *ICALP: Annual International Colloquium on Automata, Languages and Programming*, 1998.

[FK94] Uriel Feige and Joe Kilian. Two prover protocols: low error at affordable rates. In *Proceedings of the 26th Annual ACM Symposium on Theory of Computing (STOC)*, 1994.

[Gol99] Oded Goldreich. *Modern Cryptography, Probabilistic Proofs and Pseudorandomness*. Springer-Verlag, 1999.

[Hai09] Iftach Haitner. A parallel repetition theorem for any interactive argument. Technical report, 2009. ECCC, TR09-027, Revision 1.

[Hol07] Thomas Holenstein. Parallel repetition: simplifications and the no-signaling case. In *Proceedings of the 39th Annual ACM Symposium on Theory of Computing (STOC)*. ACM Press, 2007.

[HPPW08] Johan Håstad, Rafael Pass, Krzysztof Pietrzak, and Douglas Wikström. An efficient parallel repetition theorem. Unpublished manuscript, 2008.

[HRVW] Iftach Haitner, Omer Reingold, Salil Vadhan, and Hoeteck Wee. Inaccessible entropy. In *Proceedings of the 41st Annual ACM Symposium on Theory of Computing (STOC)*.

[IJK06] Russell Impagliazzo, Ragesh Jaiswal, and Ragesh Kabanets. Approximately list-decoding direct product codes and uniform hardness amplification. In *Proceedings of the 46th Annual Symposium on Foundations of Computer Science (FOCS)*, 2006.

[PV07] Rafael Pass and Muthuramakrishnan Venkitasubramaniam. An efficient parallel repetition theorem for arthur-merlin games. In *Proceedings of the 39th Annual ACM Symposium on Theory of Computing (STOC)*, 2007.

[PW07] Krzysztof Pietrzak and Douglas Wikström. Parallel repetition of computationally sound protocols revisited. In *Theory of Cryptography, Fourth Theory of Cryptography Conference (TCC)*, 2007.

[Raz98] Ran Raz. A parallel repetition theorem. *Journal of the ACM*, 27(3):763–803, 1998. Preliminary version in *STOC'95*.

A Omitted Proofs

Proof. (of Proposition 2.1) Note that

$$\begin{aligned}
&\left\|\mathsf{P}^1 - \mathsf{P}^2\right\|_{\mathcal{X}'} \\
&= \frac{1}{2} \cdot \Big(\sum_{x \in \mathcal{X}' : \mathsf{P}^1(x) \geq \mathsf{P}^2(x)} (\mathsf{P}^1(x) - \mathsf{P}^2(x)) \\
&+ \sum_{x \in \mathcal{X}' : \mathsf{P}^1(x) < \mathsf{P}^2(x)} (\mathsf{P}^2(x) - \mathsf{P}^1(x)) \Big) \\
&\geq \frac{1}{2} \cdot \Big(\sum_{x \in \mathcal{X}' : \mathsf{P}^1(x) \geq \mathsf{P}^2(x)} (\mathsf{P}^1(x) - \mathsf{P}^2(x)) \\
&+ \sum_{x \in \mathcal{X}' : \mathsf{P}^1(x) < \mathsf{P}^2(x)} (\mathsf{P}^1(x) - \mathsf{P}^2(x)) \Big) \\
&= \frac{1}{2}(\mathsf{P}^1(\mathcal{X}') - \mathsf{P}^2(\mathcal{X}')) = \frac{1}{2}(\mathsf{P}^2(\overline{\mathcal{X}'}) - \mathsf{P}^1(\overline{\mathcal{X}'})).
\end{aligned}$$

It follows that $\mathsf{P}^2(\overline{\mathcal{X}'}) \leq 2 \cdot \left\|\mathsf{P}^1 - \mathsf{P}^2\right\|_{\mathcal{X}'} + \mathsf{P}^1(\overline{\mathcal{X}'})$, and therefore

$$\begin{aligned}
&\left\|\mathsf{P}^1 - \mathsf{P}^2\right\| \\
&= \frac{1}{2} \cdot \big(\sum_{x \in \mathcal{X}'} \left|\mathsf{P}^1(x) - \mathsf{P}^2(x)\right| + \sum_{x \in \overline{\mathcal{X}}} \left|\mathsf{P}^1(x) - \mathsf{P}^2(x)\right| \big) \\
&\leq \frac{1}{2} \cdot (\mathsf{P}^1(\overline{\mathcal{X}'}) + \mathsf{P}^2(\overline{\mathcal{X}'})) + \left\|\mathsf{P}^1 - \mathsf{P}^2\right\|_{\mathcal{X}'} \\
&\leq \frac{1}{2} \cdot (\mathsf{P}^1(\overline{\mathcal{X}'}) + \mathsf{P}^1(\overline{\mathcal{X}'}) \\
&+ 2 \cdot \left\|\mathsf{P}^1 - \mathsf{P}^2\right\|_{\mathcal{X}'}) + \left\|\mathsf{P}^1 - \mathsf{P}^2\right\|_{\mathcal{X}'} \\
&\leq \mathsf{P}^1(\overline{\mathcal{X}'}) + 2 \cdot \left\|\mathsf{P}^1 - \mathsf{P}^2\right\|_{\mathcal{X}'} .
\end{aligned}$$

□