Computational Complexity Implications of Secure Coin-Flipping

by

Aristeidis Tentes

A dissertation submitted in partial fulfillment

of the requirements for the degree of

Doctor of Philosophy

Department of Computer Science

New York University

September, 2014

Professor Yevgeniy Dodis

Dedication

This thesis is dedicated to my family for their endless support through the difficult times. To my mother Lia, my father Giannis and my sister Maraki.

Acknowledgements

First of all I would like to thank my advisor, Yevgeniy Dodis, for giving me the chance to explore the world of research and cryptography specifically. His enthusiasm has always been inspiring. Moreover, I want to thank him a lot for being always helpful and giving me a complete freedom. Special thanks to a person who helped me and taught me a lot about research and this is Iftach Haitner. I really feel grateful to have met him both as a researcher and a friend. I also want to thank who served as supervisors either in my undergrad, Efstathios Zachos and Aris Pagourtzis, or in my internships, Krszysztof Pietrzak and Vladimir Kolesnikof. Moreover, I would also like to thank George Kollios.

I also want to thank colleagues and friends that I met during my studies. First of all Vasilleios Gkatzelis and his wife Maria Christoforaki. Other people I want to thank are Preyas Popat, Petros Mol, Adriana Lopez-Alt, Andreas Goebel, Vasilis Zikas. Very special thanks to Itay Berman for all the support, the difficult but also happy times we went through.

I also want to thank my friends from my homecountry for their continuing support: Ilias Iliopoulos, Diomidis Ntountounakis, Sotiris Papageorgiou, Michalis Symseridis, Kostas Theodoropoulos and Sarantis Zanakis.

Last but not least I want to thank a special person, whose name I will not mention.

Abstract

Modern Cryptography is based on computational intractability assumptions, e.g., Factoring, Discrete Logarithm, Diffie-Helman etc. However, since an assumption might be proven incorrect, there has been a lot of focus in order to construct cryptographic primitives based on the possibly most minimal assumption. The most popular minimal assumption, which is implied by the existence of almost all cryptographic primitives, is the existence of One Way Functions. Coin-Flipping protocols are known to be implied by One-Way Functions, however, a complete characterization of the inverse direction is not known. There was even speculation that weak notions of Coin Flipping Protocols might be strictly weaker than One Way Functions. In this thesis we show that even very weak notions of Coin Flipping protocols do imply One Way Functions.

In particular we show that the existence of a coin-flipping protocol safe against *any* non-trivial constant bias (e.g., .499) implies the existence of One Way Functions. This improves upon a recent result of Haitner and Omri [FOCS '11], who proved this implication for protocols with bias $\frac{\sqrt{2}-1}{2} - o(1) \approx .207$. Unlike the former result result, our result also holds for *weak* coin-flipping protocols.

Contents

Dedication **iv**

Acknowledgements **v**

Abstract **vi**

List of Figures **ix**

1 Introduction **1**

1.1 Our Result 2

1.2 Related Results 3

1.3 Our Techniques 5

2 Preliminaries **17**

2.1 Notations 17

2.2 Two-Party Protocols 18

2.3 Coin-Flipping Protocols 22

2.4 One-Way Functions and Distributional One-Way Functions 24

2.5 Two Inequalities 28

3 The Biased-Continuation Attack **29**

3.1 Biased Continuation 29

3.2 Basic Observations About $\mathsf{A}^{(i)}$ 33

3.3 Optimal Valid Attacks 35
3.4 Dominated Measures 37
3.5 Warmup — Proof Attempt Using a (Single) Dominated Measure . . 44
3.6 Back to the Proof — Sequence of Alternating Dominated Measures 49
3.7 Improved Analysis Using Alternating Dominated Measures 59
3.8 Proving Lemma 3.7.1 61
3.9 Additional Properties of the Biased-Continuation Attack 84

4 The Real Attack **88**
4.1 Attacking Coin Flipping Protocols Using (Imperfect) Function Inverters 88
4.2 The Approximated Biased Continuation Attack 89
4.3 Visiting Unbalanced Nodes is Unlikely 93
4.4 Approximated Biased-Continuation Attack on Pruned Protocols . . 103
4.5 The Pruning-in-the-Head Attacker 113
4.6 Main Theorem - Constructing the Efficient Attacker 119

Appendix **126**

A Missing Proofs **127**
A.1 Proving Lemma 2.5.1 127
A.2 Proving Lemma 2.5.2 129

Bibliography **1**

List of Figures

1.1 Coin-flipping protocol Π. The label of an internal node (i.e., partial transcript) denotes the name of the party controlling it (i.e., the party that sends the next message given this partial transcript), and that of a leaf (i.e., full transcript) denotes its value — the parties' common output once reaching this leaf. Finally, the label on an edge leaving a node u to node u' denotes the probability that a random execution of Π visits u' once in u. Note that $\mathsf{OPT}_{\mathsf{A}}(\Pi) = 1$ and $\mathsf{OPT}_{\mathsf{B}}(\Pi) = 1 - \alpha_1$. The A-dominated set $\mathcal{S}^{\mathsf{A}}$ in this case consists of the single 1-leaf to the left of the root. The conditional protocol Π' is the protocol rooted in the node to the right of the root (of Π), and the B'-dominated set $\mathcal{S}^{\mathsf{B}}$ consists of the single 0-leaf to the left of the root of Π'. 12

3.1 Example for a coin flipping protocol is given to the left, and for calculating its A-dominated measure is given to the right. 40

3.2 The conditional protocol $\Pi_{(\mathsf{B},0)} = \Pi|\neg M^{\mathsf{A}}_{\Pi}$ of Π from Figure 3.1a. Dashed Edges are such that their edge distribution has changed. Note that due to this change, the leaf 00 (the leftmost leaf, signal by thick border) is *inaccessible* in $\Pi_{(\mathsf{B},0)}$. The B-dominated measure of $\Pi_{(\mathsf{B},0)}$ assign value of 1 to the leaf 010, and value of 0 to all other leaves. 59

Chapter 1

Introduction

A central focus of modern cryptography has been to investigate the weakest possible assumptions under which various cryptographic primitives exist. This direction of research has been quite fruitful, and minimal assumptions are known for a wide variety of primitives. In particular, it has been shown that one-way functions (i.e., easy to compute but hard to invert) imply pseudorandom generators, pseudorandom functions, symmetric-key encryption/message authentication, commitment schemes, and digital signatures [GGM84, GGM86, HILL99, HNO+09, Nao91, NY89, GL89, Rom90], where one-way functions were also shown to be implied by each of these primitives [IL89].

An important exception to the above successful characterization, however, is the case of coin-flipping (-tossing) protocols. A coin-flipping protocol [Blu81] allows the honest parties to jointly flip an unbiased coin, where even a cheating (efficient) party cannot bias the outcome of the protocol by very much. Specifically, a coin-flipping protocol is δ-bias if no efficient cheating party can make the common output to be 1, or to be 0, with probability greater than $\frac{1}{2} + \delta$. While one-way functions are known to imply negligible-bias coin-flipping protocols [Blu81, Nao91, HILL99], the other direction is less clear. Impagliazzo and Luby [IL89] showed that $\Theta\left(1/\sqrt{m}\right)$-bias coin-flipping protocols imply one-way functions, where

m is the number of rounds in the protocol.[1] Recently, Maji et. al. [MPS10] extended the above for $(\frac{1}{2} - 1/\operatorname{poly}(n))$-bias *constant-round* protocols, where n is the security parameter. And more recently, Haitner and Omri [HO11] have shown the above implication holds for $(\frac{\sqrt{2}-1}{2} - o(1) \approx 0.207)$-bias coin-flipping protocols (of arbitrary round complexity). No such implications were known for any other choice of parameters, and in particular for protocols with bias greater than $\frac{\sqrt{2}-1}{2}$ with super-constant round complexity.

1.1 Our Result

In this work, we make progress towards answering the question of whether coin-flipping protocols also imply one-way functions. We show that (even weak) coin-flipping protocols, safe against any non-trivial bias (e.g., 0.4999), do in fact imply such functions. We note that unlike [HO11], but like [IL89, MPS10], our result also applies to the so-called *weak coin-flipping protocols* (see Section 2.3 for the formal definition of strong and weak coin-flipping protocols). Specifically, we prove the following theorem.

Theorem 1.1.1 (informal)**.** *For any $c > 0$, the existence of a $(\frac{1}{2} - c)$-bias coin-flipping protocol (of any round complexity) implies the existence of one-way functions.*

Note that $\frac{1}{2}$-bias coin-flipping protocol requires no assumption (i.e., one party flips a coin and announces the result to the other party). So our result is tight as long as constant biases (i.e., independent of the security parameter) are concerned.

[1] In the original paper, only $\frac{1}{2} + \operatorname{neg}(m)$ was stated, where the above term follows the proof technique hinted at the original paper and the result by Cleve [CI93].

To prove Theorem 1.1.1, we observe a connection between the success probability of the best (valid) attacks in a two-party game (i.e., chess) and the success of the biased-continuation attack of [HO11] in winning this game (see more in Section 1.3). The scope of this interesting connection seems to extend beyond the question in the focus of this paper, and we hope that it will find additional implications.

1.2 Related Results

As mentioned above, [IL89] showed that negligible-bias coin-flipping protocols imply one-way functions. Maji et.al. [MPS10] proved the same for $(\frac{1}{2} - o(1))$-bias yet constant-round protocols. Finally, Haitner and Omri [HO11] showed that the above implication holds for $\frac{\sqrt{2}-1}{2} - o(1) \approx 0.207$)-bias (strong) coin-flipping protocols (of arbitrary round complexity). Results of weaker complexity implications are also known.

Zachos [Zac86] has shown that non-trivial (i.e., $(\frac{1}{2} - o(1))$-bias), constant-round coin-flipping protocols imply that NP $\not\subseteq$ BPP, where Maji et.al. [MPS10] proved the same implication for $(\frac{1}{4} - o(1))$-bias coin-flipping protocols of arbitrary round complexity. Finally, it is well known that the existence of non-trivial coin-flipping protocols implies that PSPACE $\not\subseteq$ BPP. Apart from [HO11], all the above results extend to weak coin-flipping protocols. See Table 1.1 for a summary of the above results.

Information theoretic coin-flipping protocols (i.e., whose security holds against all-powerful attackers) were shown to exist in the quantum world; Mochon [Moc07]

[1] Only holds for *strong* coin-flipping protocols.

Implication	*Protocol type*	*Paper*
Existence of OWFs	$(\frac{1}{2} - c)$-bias, for some $c > 0$	**This work**
Existence of OWFs	$(\frac{\sqrt{2}-1}{2} - o(1))$-bias	[HO11][2]
Existence of OWFs	$(\frac{1}{2} - o(1))$-bias, *constant round*	[MPS10]
Existence of OWFs	Negligible bias	[IL89]
NP $\not\subseteq$ BPP	$(\frac{1}{4} - o(1))$-bias	[MPS10]
NP $\not\subseteq$ BPP	$(\frac{1}{2} - o(1))$-bias, *constant round*	[Zac86]
PSPACE $\not\subseteq$ BPP	Non-trivial	Folklore

Table 1.1: Results summary.

presented an ε-bias quantum weak coin-flipping protocol for any $\varepsilon > 0$. Chailloux et.al. [CK09] presented a $\left(\frac{\sqrt{2}-1}{2} - \varepsilon\right)$-bias quantum strong coin-flipping protocol for any $\varepsilon > 0$ (this bias was shown in [Kit03] to be tight). A key step in [CK09] is a reduction from strong to weak coin-flipping protocols, which holds also in the classical world.

A related line of work considers *fair* coin-flipping protocols. In this setting the honest party is required to always output a bit, whatever the other party does. In particular, a cheating party might bias the output coin just by aborting. We know that one-way functions imply fair $(1/\sqrt{m})$-bias coin-flipping protocols [ABC$^+$85, Cle86], where m is the round complexity of the protocol, and this quantity is known to be tight for $O(m/\log m)$-round protocols with fully black-box reductions [DSLMM11]. Oblivious transfer, on the other hand, implies fair $1/m$-bias protocols [MNS09, BOO10] (this bias was shown in [Cle86] to be tight).

1.3 Our Techniques

The following is a rather elaborate, high-level description of the ideas underlying our proof.

That the existence of a given (cryptographic) primitive implies the existence of one-way functions is typically proven by looking at the *primitive core function* — an efficiently computable function (not necessarily unique) whose inversion on uniformly chosen outputs implies breaking the security of the primitive.[3] For private-key encryption, for instance, a possible core function is the mapping from the inputs of the encryption algorithm (i.e., message, secret key, and randomness) into the ciphertexts. Assuming that one has defined such a core function for a given primitive, then, by definition, this function should be one-way. So it all boils down to finding, or proving the existence of, such a core function for the primitive under consideration. For a *non-interactive* primitive, finding such a core function is typically easy. In contrast, for an *interactive* primitive, finding such a core function, or functions is, at least in many settings, a much more involved task. The reason is that in order to break an interactive primitive, the attacker typically has to invert a given function on many different outputs, where these outputs are chosen *adaptively* by the attacker, after seeing the answers to the previous queries. As a result, it is very challenging to find a single function, or even finitely many functions, whose output distribution (on uniformly chosen input) matches the distribution of the attacker's queries.[4]

[3] For the sake of this informal discussion, inverting a function on a given value means returning a *uniformly* chosen preimage of this value.

[4] If the attacker makes *constant* number of queries, one can overcome the above difficulty by defining a set of core functions $f_1, \ldots, f_k$, where f_1 is the function defined by the primitive, f_2 is the function defined by the attacker after making the first inversion call, and so on. Since the evaluation time of f_{i+1} is polynomial in the evaluation time of f_i (since evaluating f_{i+1} requires

What seems as the only plausible candidate to serve as the core function of a coin-flipping protocol is its *transcript function*: the function that maps the parties' randomness into the resulting protocol transcript (i.e., the transcript produced by executing the protocol with this randomness). In order to bias the output of an m-round coin-flipping protocol by more than $O(\frac{1}{\sqrt{m}})$, a super-constant number of adaptive inversions of the transcript function seems necessary. Yet, we managed to prove that the transcript function is the core function of any (constant-bias) coin-flipping protocol. This is done by designing an adaptive attacker for any such protocol, whose query distribution is "not too far" from the output distribution of the transcript function (when invoked on uniform inputs). Since our attacker, described below, is not only adaptive, but also defined in a recursive manner, proving it possesses the aforementioned property is one of the major challenges we had to deal with.

In what follows, we give a high-level overview of our attacker that ignores computational issues (i.e., assumes it has a perfect inverter for any function). We then explain how to adjust this attacker to work with the inverter of the protocol's transcript function.

Optimal Valid Attacks and The Biased-Continuation Attack

The crux of our approach lies in an interesting connection between the optimal attack on a coin-flipping protocol and the, more feasible, *recursive biased-continuation* attack. The latter attack recursively applies the biased-continuation attack used by [HO11] to achieve their constant-bias attack (called there, the

a call to an inverter of f_i), this approach fails miserably for attackers of super-constant query complexity.

random-continuation attack) and is the basis of our efficient attack (assuming one-way functions do not exist) on coin-flipping protocols.

Let $\Pi = (\mathsf{A}, \mathsf{B})$ be a coin-flipping protocol (i.e., the common output of the honest parties is a uniformly chosen bit). In this discussion we restrict ourselves to analyzing attacks that when carried out by the left-hand side party, i.e., A, are used to bias the outcome towards one, and when carried out by the right-hand side party, i.e., B, are used to bias the outcome towards zero. Analogous statements hold for opposite attacks (i.e., attacks carried out by A and used to bias towards zero, and attacks carried out by B and used to bias towards one). The optimal valid attacker $\mathcal{A}$ carry out the *best* attack A can employ (using unbounded power) to bias the protocol towards *one*, while sending *valid* messages — ones that could have been sent by the honest party. The optimal valid attacker $\mathcal{B}$ carry out the best attack B can employ to bias the protocol towards *zero* is analogously defined. Since coin-flipping protocol is a zero-sum game, for any such protocol the expected outcome of $(\mathcal{A}, \mathcal{B})$ is either zero or one. As a first step, we give a lower bound on the success probability of the recursive biased-continuation attack carried out by the party winning the aforementioned zero-sum game. As this lower bound might not be sufficient for our goal (it might be less that constant) — and this is a crucial point in the description below — our analysis takes additional steps to give an arbitrarily-close-to-one lower bound on the success probability of the recursive biased-continuation attack carried out by *some* party, which may or may not be the same party winning the zero-sum game.[5]

[5]That the identity of the winner in $(\mathcal{A}, \mathcal{B})$ cannot be determined by the recursive biased-continuation attack is crucial. Since we show that the latter attack can be efficiently approximated assuming one-way functions do not exist, the consequences of giving up this information would be profound. It would mean that we can estimate the optimal attack (which is implemented in PSPACE) using only the assumption that one-way functions do not exist.

Assume that $\mathcal{A}$ is the winning party when playing against $\mathcal{B}$. Since $\mathcal{A}$ sends only valid messages, it follows that the expected outcome of $(\mathsf{A}, \mathcal{B})$, i.e., honest A against the optimal attacker for B, is larger than zero (since A might send the optimal messages "by mistake"). Let $\mathsf{OPT}_{\mathsf{A}}(\Pi)$ be the expected outcome of the protocol $(\mathcal{A}, \mathsf{B})$ and let $\mathsf{OPT}_{\mathsf{B}}(\Pi)$ be 1 minus the expected outcome of the protocol $(\mathsf{A}, \mathcal{B})$. The above observation yields that $\mathsf{OPT}_{\mathsf{A}}(\Pi) = 1$, while $\mathsf{OPT}_{\mathsf{B}}(\Pi) = 1 - \alpha < 1$. This gives rise to the following question: *what gives $\mathcal{A}$ an advantage over $\mathcal{B}$?*

We show that if $\mathsf{OPT}_{\mathsf{B}}(\Pi) = 1 - \alpha$, then there exists an α-dense set $\mathcal{S}^{\mathsf{A}}$ of 1-transcripts, full transcripts in which the parties' common output is 1,[6] that are "dominated by A". The A-dominated set has an important property — its density is "immune" to any action B might take, even if B is employing its optimal attack; specifically, the following holds:

$$\Pr_{\langle \mathsf{A},\mathsf{B} \rangle}\left[\mathcal{S}^{\mathsf{A}}\right] = \Pr_{\langle \mathsf{A},\mathcal{B} \rangle}\left[\mathcal{S}^{\mathsf{A}}\right] = \alpha, \tag{1.1}$$

where $\langle \Pi' \rangle$ samples a random full transcript of protocol Π'. It is easy to be convinced that the above holds in case A controls the root of the tree and has a 1-transcript as a direct descendant; see Figure 1.1 for a concrete example. The proof of the general case can be found in Chapter 3. Since the A-dominated set is B-immune, a possible attack for $\mathcal{A}$ is to go towards this set. Hence, what seems like a feasible adversarial attack for A is to mimic $\mathcal{A}$'s attack by hitting the A-dominated set with high probability. It turns out that the biased-continuation attack of [HO11] does exactly that.

The biased-continuation attacker $\mathsf{A}^{(1)}$, taking the role of A in Π and trying to bias the output of Π towards one, is defined as follows: given that the partial

[6] Throughout, we assume without loss of generality that the protocol's transcripts determines the common output of the parties.

transcript is trans, algorithm $\mathsf{A}^{(1)}$ samples a pair of random coins $(r_{\mathsf{A}}, r_{\mathsf{B}})$ that is consistent with trans and leads to a 1-transcript, and then acts as the honest A on the random coins r_{A}, given the transcript trans. In other words, $\mathsf{A}^{(1)}$ takes the first step of a random continuation of (A, B) leading to a 1-transcript. (The attacker $\mathsf{B}^{(1)}$, taking the role of B and trying to bias the outcome towards zero, is analogously defined.) [HO11] showed that for any coin-flipping protocol, if either A or B carries out the biased-continuation attack towards one, the outcome of the protocol will be biased towards one by $\frac{\sqrt{2}-1}{2}$ (when interacting with the honest party).[7] Our basic attack employs the above biased-continuation attack recursively. Specifically, for $i > 1$ we consider the attacker $\mathsf{A}^{(i)}$ that takes the first step of a random continuation of $(\mathsf{A}^{(i-1)}, \mathsf{B})$ leading to a 1-transcript, letting $\mathsf{A}^{(0)} \equiv \mathsf{A}$. The attacker $\mathsf{B}^{(i)}$ is analogously defined. Our analysis takes a different route from that of [HO11], whose approach is only applicable for handling bias up to $\frac{\sqrt{2}-1}{2}$ and cannot be applied to weak coin-flipping protocols.[8] Instead, we analyze the probability of the biased-continuation attacker to hit the dominated set we introduced above.

Let trans be a 1-transcript of Π in which all messages are sent by A. Since $\mathsf{A}^{(1)}$ picks a random 1-transcript, and B cannot force $\mathsf{A}^{(1)}$ to diverge from this transcript, the probability to produce trans under an execution of $(\mathsf{A}^{(1)}, \mathsf{B})$ is *doubled* with respect to this probability under an execution of (A, B) (assuming the expected outcome of (A, B) is $1/2$). The above property, that B cannot force $\mathsf{A}^{(1)}$ to diverge

[7] They show that the same holds for the analogous attackers carry out the biased-continuation attack towards zero.

[8] A key step in the analysis of [HO11] is to consider the "all-cheating protocol" $(\mathsf{A}^{(1),1}, \mathsf{B}^{(1),1})$, where $\mathsf{A}^{(1),1}$ plays against $\mathsf{B}^{(1),1}$ and they both carry out the biased-continuation attack trying to bias the outcome towards one. Since, and this is easy to versify, the expected outcome of $(\mathsf{A}^{(1),1}, \mathsf{B}^{(1),1})$ is one, using symmetry one can show that the expected outcome of either $(\mathsf{A}^{(1),1}, \mathsf{B})$ or $(\mathsf{A}, \mathsf{B}^{(1),1})$ is at least $\frac{1}{\sqrt{2}}$, yielding a bias of $\frac{1}{\sqrt{2}} - \frac{1}{2}$. As mentioned in [HO11], symmetry cannot be used to prove a bias larger than $\frac{1}{\sqrt{2}} - \frac{1}{2}$.

from a transcript, is in fact the B-immune property of the A-dominated set. A key point we make is to generalize the above argument to show that for the α-dense A-dominated set $\mathcal{S}^{\mathsf{A}}$ (exists assuming that $\mathsf{OPT}_{\mathsf{B}}(\Pi) = 1 - \alpha < 1$), it holds that:

$$\Pr_{\langle \mathsf{A}^{(1)}, \mathsf{B} \rangle} \left[\mathcal{S}^{\mathsf{A}} \right] \geq \frac{\alpha}{\mathsf{val}(\Pi)}, \tag{1.2}$$

where $\mathsf{val}(\Pi')$ is the expected outcome of Π'. Namely, in $(\mathsf{A}^{(1)}, \mathsf{B})$ the probability of hitting the set $\mathcal{S}^{\mathsf{A}}$ of 1-transcripts is larger by a factor of at least $\frac{1}{\mathsf{val}(\Pi)}$ than the probability of hitting this set in the original protocol Π. Again, it is easy to be convinced that the above holds in case A controls the root of the tree and has a 1-transcript as a direct descendant; see Figure 1.1 for a concrete example. The proof of the general case can be found in Chapter 3.

Consider now the protocol $(\mathsf{A}^{(1)}, \mathsf{B})$. In this protocol, the probability of hitting the set $\mathcal{S}^{\mathsf{A}}$ is at least $\frac{\alpha}{\mathsf{val}(\Pi)}$, and clearly the set $\mathcal{S}^{\mathsf{A}}$ remains B-immune. Hence, we can apply Equation (1.2) again, to deduce that

$$\Pr_{\langle \mathsf{A}^{(2)}, \mathsf{B} \rangle} \left[\mathcal{S}^{\mathsf{A}} \right] = \Pr_{\langle (\mathsf{A}^{(1)})^{(1)}, \mathsf{B} \rangle} \left[\mathcal{S}^{\mathsf{A}} \right] \geq \frac{\Pr_{\langle \mathsf{A}^{(1)}, \mathsf{B} \rangle} \left[\mathcal{S}^{\mathsf{A}} \right]}{\mathsf{val}(\mathsf{A}^{(1)}, \mathsf{B})} \geq \frac{\alpha}{\mathsf{val}(\Pi) \cdot \mathsf{val}(\mathsf{A}^{(1)}, \mathsf{B})}. \tag{1.3}$$

Continuing it for κ iterations yields that

$$\mathsf{val}(\mathsf{A}^{(\kappa)}, \mathsf{B}) \geq \Pr_{\langle \mathsf{A}^{(\kappa)}, \mathsf{B} \rangle} \left[\mathcal{S}^{\mathsf{A}} \right] \geq \frac{\alpha}{\prod_{i=0}^{\kappa-1} \mathsf{val}(\mathsf{A}^{(i)}, \mathsf{B})}. \tag{1.4}$$

So, modulo some cheating,[9] it seems that we are in good shape. Taking, for example, $\kappa = \log(\frac{1}{\alpha}) / \log(\frac{1}{0.9})$, Equation (1.4) yields that $\mathsf{val}(\mathsf{A}^{(\kappa)}, \mathsf{B}) > 0.9$. Namely, if we assume that $\mathcal{A}$ has an advantage over $\mathcal{B}$, then by recursively applying

[9] The actual argument is somewhat more complicated than the one given above. To ensure the above argument holds we need to consider measures over the 1-transcripts (and not sets). In addition, while (the measure variant of) Equation (1.3) is correct, deriving it from Equation (1.2) takes some additional steps.

the biased-continuation attack for A enough times, we arbitrarily bias the expected output of the protocol towards one. Unfortunately, if this advantage (i.e., $\alpha = (1 - \mathsf{OPT}_{\mathsf{B}}(\Pi))$) is very small, which is the case in typical examples, the number of recursions required might be linear in the protocol depth (or even larger). Given the recursive nature of the above attack, the running time of the described attacker is *exponential*. To overcome this obstacle, we consider not only the dominated set, but additional sets that are "close to" being dominated. Informally speaking, a 1-transcript belongs to the A-dominated set if it can be generated by an execution of $(\mathcal{A}, \mathsf{B})$. In other words, the probability, over B's coins, that a transcript generated by a random execution of $(\mathcal{A}, \mathsf{B})$ belongs to the A-dominated set is one. We define a set of 1-transcripts that does not belong to the A-dominated set to be "close to" A-dominated if there is an (unbounded) attacker $\widehat{\mathcal{A}}$, such that the probability, over B's coins, that a transcript generated by a random execution of $(\widehat{\mathcal{A}}, \mathsf{B})$ belongs to the set is close to one. These sets are formally defined via the notion of conditional protocols, discussed next.

Conditional Protocols Let $\Pi = (\mathsf{A}, \mathsf{B})$ be a coin-flipping protocol in which there exists an A-dominated set $\mathcal{S}^{\mathsf{A}}$ of density $\alpha > 0$. Consider the "conditional" protocol $\Pi' = (\mathsf{A}', \mathsf{B}')$, resulting from conditioning on not hitting the set $\mathcal{S}_{\mathsf{A}}$. Namely, the message distribution of Π' is that induced by a random execution of Π that does not generate transcripts in $\mathcal{S}_{\mathsf{A}}$. See Figure 1.1 for a concrete example. We note that the protocol Π' might not be efficiently computable (even if Π is), but this does not bother us, since we only use it as a thought experiment.

We have effectively removed all the 1-transcripts dominated by A (the set $\mathcal{S}^{\mathsf{A}}$ must contain all such transcripts; otherwise $\mathsf{OPT}_{\mathsf{B}}(\Pi)$ would be smaller than $1-\alpha$).

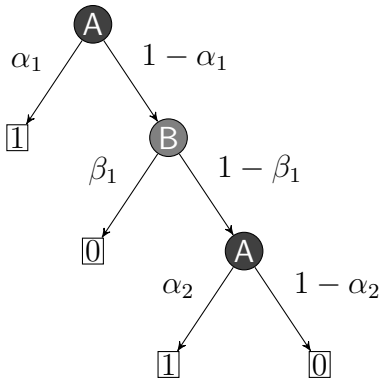


Figure 1.1: Coin-flipping protocol Π. The label of an internal node (i.e., partial transcript) denotes the name of the party controlling it (i.e., the party that sends the next message given this partial transcript), and that of a leaf (i.e., full transcript) denotes its value — the parties' common output once reaching this leaf. Finally, the label on an edge leaving a node u to node u' denotes the probability that a random execution of Π visits u' once in u. Note that $\mathsf{OPT}_{\mathsf{A}}(\Pi) = 1$ and $\mathsf{OPT}_{\mathsf{B}}(\Pi) = 1 - \alpha_1$. The A-dominated set $\mathcal{S}^{\mathsf{A}}$ in this case consists of the single 1-leaf to the left of the root. The conditional protocol Π' is the protocol rooted in the node to the right of the root (of Π), and the B'-dominated set $\mathcal{S}^{\mathsf{B}}$ consists of the single 0-leaf to the left of the root of Π'.

Thus, the expected outcome of $(\mathcal{A}', \mathcal{B}')$ is zero. Therefore, $\mathsf{OPT}_{\mathsf{B}'}(\Pi') = 1$ and $\mathsf{OPT}_{\mathsf{A}'}(\Pi') = 1 - \beta < 1$. It follows from this crucial observation that there exists a B'-dominated $\mathcal{S}^{\mathsf{B}}$ of density β, over the 0-transcripts of Π'. Applying a similar argument to that used for Equation (1.4) yields that for large enough κ, the biased-continuation attacker $\mathsf{B}'^{(\kappa)}$, playing the role of B', succeeds in biasing the outcome of Π' toward zero, where κ is proportional to $\log(\frac{1}{\beta})$. Moreover, if α is small, the above yields that $\mathsf{B}^{(\kappa)}$ is doing almost equally well in the original protocol Π. If β is also small, we can now consider the conditional protocol Π'', obtained by conditioning Π' on not hitting the B'-dominated set, and so on.

By iterating the above process enough times, the A-dominated sets cover all the 1-transcripts, and the B-dominated sets cover all the 0-transcripts.[10] Assume

[10]When considering measures and not sets, as done in the actual proof, this covering property

that in the above iterated process, the density of the A-dominated sets is the first to go beyond $\varepsilon > 0$. It can be shown — and this a key technical contribution of this paper — that it is almost as good as if the density of the *initial* set $\mathcal{S}_{\mathsf{A}}$ was ε.[11] We conclude that for any $\varepsilon > 0$, there exists a constant κ such that $\mathsf{val}(\mathsf{A}^{(\kappa)}, \mathsf{B}) > 1 - \varepsilon$.[12]

Using the Transcript Inverter

We have seen above that for any constant ε, by recursively applying the biased-continuation attack for constantly many times, we get an attack that biases the outcome of the protocol by $\frac{1}{2} - \varepsilon$. The next thing is to implement the above attack *efficiently*, under the assumption that one-way functions do not exist. Given a partial transcript u of protocol Π, we wish to return a uniformly chosen full transcript of Π that is consistent with u and the common outcome it induces is one. Biased continuation can be reduced to the task of finding *honest continuation*: returning a uniformly chosen full transcript of Π that is consistent with u. Assuming honest continuations can be done for the protocol, biased-continuation can also be done by calling the honest continuation many times, until transcript whose output is one is obtained. The latter can be done efficiently, as long as the value of the partial transcript u — the expected outcome of the protocol conditioned on u, is not too low. (If it is too low, too much time might pass before a full transcript leading to one is obtained.) Ignoring this low value problem, and noting that hon-

is not trivial.

[11] More accurately, let $\widetilde{\mathcal{S}}^{\mathsf{A}}$ be the union of these 1-transcript sets and let $\widetilde{\alpha}$ be the density of $\widetilde{\mathcal{S}}^{\mathsf{A}}$ in Π. Then $\mathsf{val}(\mathsf{A}^{(\kappa)}, \mathsf{B}) \geq \Pr_{\langle \mathsf{A}^{(\kappa)}, \mathsf{B} \rangle}\left[\widetilde{\mathcal{S}}^{\mathsf{A}}\right] \geq \frac{\widetilde{\alpha}}{\prod_{i=0}^{\kappa-1} \mathsf{val}(\mathsf{A}^{(i)}, \mathsf{B})}$.

[12] The assumption that the density of the A-dominated sets is the first to go beyond $\varepsilon > 0$ is independent of the assumption that $\mathcal{A}$ wins in the zero-sum game $(\mathcal{A}, \mathcal{B})$. Specifically, the fact that $\mathsf{A}^{(\kappa)}$ succeeds in biasing the protocol does not guarantee that $\mathcal{A}$ is the winner of $(\mathcal{A}, \mathcal{B})$.

est continuation of a protocol can be reduced to inverting the protocol's transcript function, all we need to do to implement $\mathsf{A}^{(i)}$ is to invert the transcript functions of the protocols $(\mathsf{A},\mathsf{B}),(\mathsf{A}^{(1)},\mathsf{B}),\ldots,(\mathsf{A}^{(i-1)},\mathsf{B})$. Furthermore, noting that the attackers $\mathsf{A}^{(1)},\ldots,\mathsf{A}^{(i-1)}$ are *stateless*, it suffices to have the ability to invert *only* the transcript function of (A,B).

So attacking a coin-flipping protocol Π boils down to inverting the transcript function f_Π of Π, and making sure we are not doing that on low value transcripts. Assuming one-way functions do not exist, there exists an efficient inverter Inv for f_Π that is guaranteed to work well when invoked on random outputs of f_Π (i.e., when f_Π is invoked on the uniform distribution. Nothing is guaranteed for distributions far from uniform). By the above discussion, algorithm Inv implies an efficient approximation of $\mathsf{A}^{(i)}$, as long as the partial transcripts attacked by $\mathsf{A}^{(i)}$ are neither *low-value* nor *unbalanced* (by low-value transcript we mean that the expected outcome of the protocol conditioned on the transcript is low; by unbalanced transcript we mean that its density with respect to $(\mathsf{A}^{(i)},\mathsf{B})$ is not to far from its density with respect to (A,B)). Unlike [HO11], we failed to prove (and we believe that it is untrue) that the queries of $\mathsf{A}^{(i)}$ obey these two conditions with sufficiently high probability, and thus we cannot simply argue that $\mathsf{A}^{(i)}$ has an efficient approximation, assuming one-way functions do not exist. Fortunately, we managed to prove the above for the "pruned" variant of $\mathsf{A}^{(i)}$, defined below.

Unbalanced and low value transcripts Before defining our final attacker, we relate the problem of unbalanced transcripts to that of low-value transcripts. We say that a (partial) transcript u is γ-*unbalanced*, if the probability that u is visited with respect to a random execution of $(\mathsf{A}^{(1)},\mathsf{B})$, is at least γ times larger than

with respect to a random execution of (A, B). Furthermore, we say that a (partial) transcript u is δ-*small*, if the expected outcome of (A, B), conditioned on visiting u, is at most δ. We prove (a variant of) the following statement. For any $\delta > 0$ and $\gamma > 1$, there exists c that depends on δ, such that

$$\Pr_{\ell \leftarrow \langle \mathsf{A}^{(1)}, \mathsf{B} \rangle} [\ell \text{ has a } \gamma\text{-unbalanced prefix but no } \delta\text{-small prefix}] \leq \frac{1}{\gamma^c}. \qquad (1.5)$$

Namely, as long as $(\mathsf{A}^{(1)}, \mathsf{B})$ does not visit low-value transcripts, it is only at low risk to significantly deviate (in a multiplicative sense) from the distribution induced by (A, B). Equation (1.5) naturally extends to recursive biased-continuation attacks. It also has an equivalent form for the attacker $\mathsf{B}^{(1)}$, trying to bias the protocol towards zero, with respect to δ-high transcripts — the expected outcome of Π, conditioned on visiting the transcript, is at least $1 - \delta$.

The pruning attacker At last we are ready to define our final attacker. To this end, for protocol $\Pi = (\mathsf{A}, \mathsf{B})$ we define its δ-*pruned variant* $\Pi_\delta = (\mathsf{A}_\delta, \mathsf{B}_\delta)$, where $\delta \in (0, \frac{1}{2})$, as follows. As long as the execution does not visit a δ-low or δ-high transcripts, the parties act as in Π. Once a δ-low transcript is visited, only the party B sends messages, and it does so according to the distribution induced by Π. If a δ-high transcript is visited (and has no δ-low prefix), only the party A sends messages, and again it does so according to the distribution induced by Π.

Since the transcript distribution induced by Π_δ is the same as of Π, protocol Π_δ is also a coin-flipping protocol. We also note that Π_δ can be implemented efficiently assuming one-way functions do not exist (simply use the inverter of Π's transcript function to estimate the value of a given transcript). Finally, by Equation (1.5), $\mathsf{A}_\delta^{(i)}$ (i.e., recursive biased-continuation attacks for Π_δ) can be efficiently implemented, since there are *no* low-value transcripts where A needs to send the

next message. (Similarly, $\mathsf{B}_\delta^{(i)}$ can be efficiently implemented since there are no high-value transcripts where B needs to send the next message.)

It follows that for any constant $\varepsilon > 0$, there exists constant κ such that either the expected outcome of $(\mathsf{A}_\delta^{(\kappa)}, \mathsf{B}_\delta)$ is a least $1 - \varepsilon$, or the expected outcome of $(\mathsf{A}_\delta, \mathsf{B}_\delta^{(\kappa)})$ is at most ε. Assume for concreteness that it is the former case. We define our pruning attacker $\mathsf{A}^{(\kappa,\delta)}$ as follows. When playing against B, the attacker $\mathsf{A}^{(\kappa,\delta)}$ acts like $\mathsf{A}_\delta^{(\kappa)}$ would when playing against B_δ. Namely, the attacker pretends that it is in the δ-pruned protocol Π_δ. But once a low or high value transcript is reached, $\mathsf{A}^{(\kappa,\delta)}$ acts *honestly* in the rest of the execution (like A would).

It follows that until a low or high value transcript has been reached for the first time, the distribution of $(\mathsf{A}^{(\kappa,\delta)}, \mathsf{B})$ is the same as that of $(\mathsf{A}_\delta^{(\kappa)}, \mathsf{B}_\delta)$. Once a δ-low transcript is reached, the expected outcome of both $(\mathsf{A}^{(\kappa,\delta)}, \mathsf{B})$ and $(\mathsf{A}_\delta^{(\kappa)}, \mathsf{B}_\delta)$ is δ, but when a δ-high transcript is reached, the expected outcome of $(\mathsf{A}^{(\kappa,\delta)}, \mathsf{B})$ is $(1 - \delta)$ (since it plays like A would), where the expected outcome of $(\mathsf{A}_\delta^{(\kappa)}, \mathsf{B}_\delta)$ is at most one. All in all, the expected outcome of $(\mathsf{A}^{(\kappa,\delta)}, \mathsf{B})$ is δ-close to that of $(\mathsf{A}_\delta^{(\kappa)}, \mathsf{B}_\delta)$, and thus the expected outcome of $(\mathsf{A}^{(\kappa,\delta)}, \mathsf{B})$ is at least $1 - \varepsilon - \delta$. Since ε and δ are arbitrary constants, we have established an efficient attacker to bias the outcome of Π by a value that is an arbitrary constant close to one.

Chapter 2

Preliminaries

2.1 Notations

We use calligraphic letters to denote sets, uppercase for random variables and functions, lowercase for values, boldface for vectors, and sans-serif (e.g., A) for algorithms (i.e., Turing Machines). All logarithms considered here are in base two, where $\circ$ denotes string concatenation. Let $\mathbb{N}$ denote the set of natural numbers, where 0 is considered as a natural number, i.e., $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$. For $n \in \mathbb{N}$, let $(n) = \{0, \ldots, n\}$ and if n is positive let $[n] = \{1, \cdots, n\}$, where $[0] = \emptyset$. For $a \in \mathbb{R}$ and $b \geq 0$, let $[a \pm b]$ stand for the interval $[a-b, a+b]$, $(a \pm b]$ for $(a-b, a+b]$ etc. For a non-empty string $t \in \{0,1\}^*$ and $i \in [|t|]$, let t_i be the i'th bit of t, and for $i, j \in [|t|]$ such that $i < j$, let $t_{i,\ldots,j} = t_i \circ t_{i+1} \circ \ldots \circ t_j$. The empty string is denoted by λ, and for a non-empty string, let $t_{1,\ldots,0} = \lambda$. We let poly denote the set all polynomials and let PPTM denote a probabilistic algorithm that runs in *strictly* polynomial time. Give a PPTM algorithm A we let $\mathsf{A}(u; r)$ be an execution of A on input u given randomness r. A function $\nu \colon \mathbb{N} \mapsto [0,1]$ is *negligible*, denoted $\nu(n) = \text{neg}(n)$, if $\nu(n) < 1/p(n)$ for every $p \in \text{poly}$ and large enough n.

Given a random variable X, we write $x \leftarrow X$ to indicate that x is selected according to X. Similarly, given a finite set $\mathcal{S}$, we let $s \leftarrow \mathcal{S}$ denote that s is

selected according to the uniform distribution on $\mathcal{S}$. We adopt the convention that when the same random variable occurs several times in an expression, all occurrences refer to a single sample. For example, $\Pr[f(X) = X]$ is defined to be the probability that when $x \leftarrow X$, we have $f(x) = x$. We write U_n to denote the random variable distributed uniformly over $\{0,1\}^n$. The support of a distribution D over a finite set $\mathcal{U}$, denoted $\mathrm{Supp}(D)$, is defined as $\{u \in \mathcal{U} : D(u) > 0\}$. The *statistical distance* of two distributions P and Q over a finite set $\mathcal{U}$, denoted as $\mathrm{SD}(P,Q)$, is defined as $\max_{\mathcal{S}\subseteq\mathcal{U}} |P(\mathcal{S}) - Q(\mathcal{S})| = \frac{1}{2}\sum_{u\in\mathcal{U}} |P(u) - Q(u)|$.

A *measure* is a function $M\colon \Omega \mapsto [0,1]$. The support of M over a set Ω, denoted $\mathrm{Supp}(M)$, is defined as $\{\omega \in \Omega\colon M(\omega) > 0\}$. A measure M over Ω is the *zero measure* if $\mathrm{Supp}(M) = \emptyset$.

2.2 Two-Party Protocols

The following discussion is restricted to no-input (possibly randomized), two-party protocols, where each message consists of a *single* bit. We do not assume, however, that the parties play in turns (i.e., the same party might send two consecutive messages), but only that the protocol's transcript uniquely determines which party is playing next (i.e., the protocol is well defined). In an m-round protocol, the parties interact for exactly m rounds. The tuple of the messages sent so far in any partial execution of a protocol is called the *(communication) transcript* of this execution.

We write that a protocol Π is equal to (A,B), when A and B are the interactive Turing Machines that control the left and right hand side party respectively, of the interaction according to Π. For a party C interacting according to Π, let $\overline{\mathsf{C}}_\Pi$ be the

other party in Π, where in case Π is clear from the context, we simply write $\overline{\mathsf{C}}$.

If A, B are deterministic, then by $\mathrm{trans}(\mathsf{A}, \mathsf{B})$, we denote the uniquely defined transcript, namely the bits sent by both parties in the order of appearance, when these parties run the protocol.

Binary Trees

Definition 2.2.1 (binary trees)**.** *For $m \in \mathbb{N}$, let $\mathcal{T}^m$ be the complete directed binary tree of height m. We naturally identify the vertices of $\mathcal{T}^m$ with binary strings: the root is denoted by the empty string λ, and the the left-hand side and right-hand side children of a non-leaf node u, are denoted by $u0$ and $u1$ respectively.*

- *Let $\mathcal{V}(\mathcal{T}^m)$, $\mathcal{E}(\mathcal{T}^m)$, $\mathsf{root}(\mathcal{T}^m)$ and $\mathcal{L}(\mathcal{T}^m)$ denote the vertices, edges, root and leaves of $\mathcal{T}^m$ respectively.*

- *For $u \in \mathcal{V}(\mathcal{T}^m) \setminus \mathcal{L}(\mathcal{T}^m)$, let $\mathcal{T}^m_u$ be the subtree of $\mathcal{T}^m$ rooted at u.*

- *For $u \in \mathcal{V}(\mathcal{T}^m)$, let $\mathsf{desc}_m(u)$ [resp., $\overline{\mathsf{desc}}_m(u)$] be the descendants of u in $\mathcal{T}^m$ including u [resp., excluding u], and for $\mathcal{U} \subseteq \mathcal{V}(\mathcal{T}^m)$ let $\mathsf{desc}_m(\mathcal{U}) = \bigcup_{u \in \mathcal{U}} \mathsf{desc}_m(u)$ and $\overline{\mathsf{desc}}_m(\mathcal{U}) = \bigcup_{u \in \mathcal{U}} \overline{\mathsf{desc}}_m(u)$.*

- *The frontier of a set $\mathcal{U} \subseteq \mathcal{V}(\mathcal{T}^m)$, denoted by $\mathsf{frnt}(\mathcal{U})$, is defined as $\mathcal{U} \setminus \overline{\mathsf{desc}}_m(\mathcal{U})$.*

When m is clear from the context, it is typically omitted from the above notation.

Protocol Trees

We naturally identify a (possibly partial) transcript of a m-round, single-bit message protocol with a rooted path in $\mathcal{T}^m$. That is, the transcript $t \in \{0,1\}^m$ is identified with the path $\lambda, t_1, t_{1,2}, \ldots, t$.

Definition 2.2.2 (tree representation of a protocol)**.** *We make use of the following definitions with respect to an m-round protocol $\Pi = (\mathsf{A}, \mathsf{B})$, and $\mathsf{C} \in \{\mathsf{A}, \mathsf{B}\}$.*

- *Let* round$(\Pi) = m$*, let $\mathcal{T}(\Pi) = \mathcal{T}^m$ and for $X \in \{\mathcal{V}, \mathcal{E}, \mathsf{root}, \mathcal{L}\}$ let $X(\Pi) = X(\mathcal{T}(\Pi))$.*

- *The* edge distribution *induced by a protocol Π, is the function $e_\Pi \colon \mathcal{E}(\Pi) \mapsto [0,1]$ defined as $e_\Pi(u,v)$ being the probability that the transcript of a random execution of Π visits v, conditioned that it visits u.*

- *For $u \in \mathcal{V}(\Pi)$, let $\mathsf{v}_\Pi(u) = e_\Pi(\lambda, u_1) \cdot e_\Pi(u_1, u_{1,2}) \cdot \ldots \cdot e_\Pi(u_{1,\ldots,|u|-1}, u)$, and let the* l*eavesdistribution induced by Π be the distribution $\langle\Pi\rangle$ over $\mathcal{L}(\Pi)$, defined by $\langle\Pi\rangle(u) = \mathsf{v}_\Pi(u)$.*

- *The party that sends the next message on transcript u, is said to control u, and we denote this party by $\mathsf{cntrl}_\Pi(u)$. Let $\mathcal{C}\mathsf{trl}_\Pi^{\mathsf{C}} = \{u \in \mathcal{V}(\Pi) \colon \mathsf{cntrl}_\Pi(u) = \mathsf{C}\}$.*

  Let $\mathsf{cntrl}'_\Pi(u)$ be 0 if $\mathsf{cntrl}_\Pi(u) = \mathsf{A}$, and 1 otherwise. The leaf-control distribution *over $\mathcal{L}(\Pi) \times \{0,1\}^m$, denoted by $[\Pi]$, is $(\ell, \mathsf{cntrl}'_\Pi(\ell_1), \mathsf{cntrl}'_\Pi(\ell_{1,2}) \ldots, \mathsf{cntrl}'_\Pi(\ell))_{\ell \leftarrow \langle\Pi\rangle}$.*

Note that every function $e \colon \mathcal{E}(\mathcal{T}^m) \mapsto [0,1]$ with $e(u, u0) + e(u, u1) = 1$ for every $u \in \mathcal{V}(\mathcal{T}^m) \setminus \mathcal{L}(\mathcal{T}^m)$ with $\mathsf{v}(u) > 0$, along with a controlling scheme (who is active in each node), defines a two party, m-round, single-bit message protocol

(the resulting protocol might be inefficient). This observation allows us to consider the protocols induced by subtrees of $\mathcal{T}(\Pi)$.

The analysis done in Chapter 3 naturally gives rise to functions over binary trees, that do not corresponds to any two parties execution. We identify the "protocols" induced by such functions by the special symbol $\perp$. We let $\mathrm{E}_{\langle\perp\rangle}[f] = 0$, for any real-value function f.

Definition 2.2.3 (sub-protocols)**.** *Let Π be a protocol and let $u \in \mathcal{V}(\Pi)$. Let $(\Pi)_u$ denotes the the protocol induced by the function e_Π on the subtree of $\mathcal{T}(\Pi)$ rooted at u, in case such protocol exists,*[1] *and let $(\Pi)_u = \perp$, otherwise.*

When convenient, we remove the parentheses from notation, and simply write Π_u. Two sub-protocols of interest are Π_0 and Π_1, induced by e_Π and the trees rooted at the left-hand side and right-hand side descendants of $\mathsf{root}(\mathcal{T})$. For a measure $M\colon \mathcal{L}(\Pi) \mapsto [0,1]$ and $u \in \mathcal{V}(\Pi)$, let $(M)_u\colon \mathcal{L}(\Pi_u) \mapsto [0,1]$ be the restricted measure induced by M on the sub-protocol Π_u. Namely, for any $\ell \in \mathcal{L}(\Pi_u)$, $(M)_u(\ell) = M(\ell)$.

Tree Value

Definition 2.2.4 (tree value)**.** *Let Π a two-party protocol, in which at the end of any of its executions the parties output the* same *real value. Let $\chi_\Pi\colon \mathcal{L}(\Pi) \mapsto \mathbb{R}$ be the* common output *function of Π, where $\chi_\Pi(\ell)$ being the common output of the parties in an execution ending in ℓ.*[2] *Let $\mathsf{val}(\Pi) = \mathrm{E}_{\langle\Pi\rangle}[\chi_\Pi]$, and for $x \in \mathbb{R}$ let $\mathcal{L}_x(\Pi) = \{\ell \in \mathcal{L}(\Pi)\colon \chi_\Pi(\ell) = x\}$.*

[1] Namely, the protocol Π_u, is the protocol Π conditioned on u being the transcript of the first $|u|$ rounds.

[2] Since condition on u, the random coins of the parties are in a product distribution, under the above assumption the common output is indeed a function of u.

The following immediate fact states that the expected value of a measure, whose support is a subset of the 1-leaves of some protocol, is always smaller than the value of that protocol.

Fact 2.2.5. *Let* Π *be a protocol and let* M *be a measure over* $\mathcal{L}_1(\Pi)$*, then* $\mathrm{E}_{\langle\Pi\rangle}[M] \leq \mathsf{val}(\Pi)$*.*

Protocol with Common Inputs

We sometimes would like to apply the above terminology to a protocol $\Pi = (\mathsf{A}, \mathsf{B})$ whose parties get a common security parameter 1^n. This is formally done by considering the protocol $\Pi_n = (\mathsf{A}_n, \mathsf{B}_n)$, where C_n is the algorithm derived by of "hardwiring" 1^n into the code of C.

2.3 Coin-Flipping Protocols

In a coin-flipping protocol two parties interact and in the end they have a common output bit. Ideally, this bit should be random and no cheating party should be able to bias its outcome to neither direction (if the other party remains honest). For interactive, probabilistic algorithms A and B, and $x \in \{0,1\}^*$, let $\mathrm{out}(\mathsf{A}, \mathsf{B})(x)$ denotes parties' output, on common input x.

Definition 2.3.1 ((strong) coin-flipping)**.** *A PPT protocol* (A, B) *is a* δ-bias coin-flipping protocol*, if the following holds.*

Correctness: $\Pr[\mathrm{out}(\mathsf{A}, \mathsf{B})(1^n) = (0,0)] = \Pr[\mathrm{out}(\mathsf{A}, \mathsf{B})(1^n) = (1,1)] = \frac{1}{2}$.

Security: $\Pr[\mathrm{out}(\mathsf{A}^*, \mathsf{B})(1^n) = (*, c)], \Pr[\mathrm{out}(\mathsf{A}, \mathsf{B}^*)(1^n) = (c, *)] \leq \frac{1}{2} + \delta(n)$*, for any PPTM's* A^* *and* B^**, bit* $c \in \{0,1\}$ *and large enough* n*.*

Sometimes, e.g., if the parties have (a priori known) opposite preferences, an even weaker definition of coin-flipping protocols is of interest.

Definition 2.3.2 (weak coin-flipping)**.** *A PPT protocol* (A, B) *is a* weak δ-bias coin-flipping protocol*, if the following holds.*

Correctness: Same as in Definition 2.3.1.

Security: There exist bits $c_{\mathsf{A}} \neq c_{\mathsf{B}} \in \{0,1\}$ *such that*

$$\Pr[\text{out}(\mathsf{A}^*, \mathsf{B})(n) = c_{\mathsf{A}}], \Pr[\text{out}(\mathsf{A}, \mathsf{B}^*)(n) = c_{\mathsf{B}}] \leq \frac{1}{2} + \delta(n)$$

for any PPTM's A^* *and* B^**, and large enough* n*.*

Remark 2.3.3. *Our result still holds when replacing the value* $\frac{1}{2}$ *in the correctness requirement above, with any constant in* $(0,1)$*. It also holds for protocols in which, with some small probability, the parties are not in agreement regarding the protocol's outcome, or even might output values that are not bits.*

In the the rest of the paper we restrict our attention to m-round single-bit message coin-flipping protocols, where $m = m(n)$ is a function of the protocol's security parameter. Given such protocol $\Pi = (\mathsf{A}, \mathsf{B})$, we assume that the common output of the protocol (i.e., the coin), is efficiently computable from a (full) transcript of the protocol. (It is easy to see that these assumptions are without loss of generality).

2.4 One-Way Functions and Distributional One-Way Functions

A one-way function (OWF) is an efficiently computable function whose inverse cannot be computed on average by any PPTM.

Definition 2.4.1. *A polynomial-time computable function* $f\colon \{0,1\}^n \mapsto \{0,1\}^{\ell(n)}$ *is* o*ne-way, if*

$$\Pr_{x\leftarrow\{0,1\}^n;y=f(x)}\left[\mathsf{A}(1^n,y)\in f^{-1}(y)\right]=\mathrm{neg}(n)$$

for any PPTM A*.*

A seemingly weaker definition is that of a distributional OWF. Such a function is easy to compute, but, roughly speaking, it is hard to compute uniformly random preimages of random images.

Definition 2.4.2. *A polynomial-time computable* $f\colon \{0,1\}^n \mapsto \{0,1\}^{\ell(n)}$ *is* d*istributional one-way, if* $\exists p\in \mathrm{poly}$ *such that*

$$\mathrm{SD}\left((x,f(x))_{x\leftarrow\{0,1\}^n},(\mathsf{A}(f(x)),f(x))_{x\leftarrow\{0,1\}^n}\right)\geq\frac{1}{p(n)}$$

for any PPTM A *and large enough* n*.*

Clearly, any one-way function is also a distributional one-way function. While the other implication is not necessarily always true, [IL89] showed that the existence of distributional one-way functions implyies that of (standard) one-way functions. In particular, [IL89] proved that if one-way functions do not exist, then any efficiently computable function has an inverter of the following form.

Definition 2.4.3 (γ-inverter)**.** *An algorithm* Inv *is a* γ-inverter *of* $f\colon \mathcal{D} \mapsto \mathcal{R}$*, if the following holds.*

$$\Pr_{x\leftarrow\mathcal{D};y=f(x)}\left[\mathrm{SD}\left((y,x')_{x'\leftarrow f^{-1}(y)},(y,\mathsf{Inv}(y))\right)\geq\gamma\right]\leq\gamma.$$

Lemma 2.4.4 ([IL89, Lemma 1])**.** *Assume one-way functions do not exit, then for any polynomial-time computable function* $f\colon\{0,1\}^n\mapsto\{0,1\}^{\ell(n)}$ *and* $p\in\mathrm{poly}$*, there exists a PPTM algorithm* Inv *such the that the following holds for infinitely many* n*'s. On security parameter* 1^n*, algorithm* Inv *is a* $1/p(n)$*-inverter of* f_n *(i.e.,* f *restricted to* $\{0,1\}^n$*).*

Note that nothing is guaranteed when invoking a good inverter (i.e., a γ-inverter for some small γ) on an *arbitrary distribution*. Yet, the following lemma yields that if the distribution in consideration is "not too different" from the output distribution of f, then such good inverters are useful.

Lemma 2.4.5. *Let* f *and* g *be two randomized functions over the same domain* $\mathcal{D}$*, and let* $\{D_i\}_{i\in[k]}$ *be a set of distributions over* $\mathcal{D}$ *such that for some* $a\geq 0$ *it holds that* $\mathrm{E}_{d\leftarrow D_i}[\mathrm{SD}(f(d),g(d))]\leq a$ *for every* $i\in[k]$*. Let* A *be a* k*-query oracle-aided algorithm that only makes queries in* $\mathcal{D}\cup\{\bot\}$*. For* $i\in[k]$*, let* F_i *be the probability distribution of the* i*'th query to* f *in a random execution of* A^f*, and let* $Q=(Q_1,\ldots,Q_k)$ *be the random variable of the queries of* A^f *in such a random execution (in case the* i*'th query was* $\bot$*, we also set its reply to* $\bot$*).*

Assume $\Pr_{(q_1,\ldots,q_k)\leftarrow Q}\left[\exists i\in[k]\colon q_i\neq\bot\wedge F_i(q_i)>\lambda\cdot D_i(q_i)\right]\leq b$ *for some* $\lambda,b\geq 0$*, then* $\mathrm{SD}\left(\mathsf{A}^f,\mathsf{A}^g\right)\leq b+ka\lambda$*.*

For proving Lemma 2.4.5, we use the following fact.

Proposition 2.4.6. *For every two distributions P and Q over as set $\mathcal{D}$ there exists a distribution $R_{P,Q}$ over $\mathcal{D} \times \mathcal{D}$, such that the following holds:*

1. $(R_{P,Q})_1 \equiv P$ *and* $(R_{P,Q})_2 \equiv Q$*, where* $(R_{P,Q})_b$ *is the projection of* $R_{P,Q}$ *into its b'th coordinate.*

2. $\Pr_{(x_1,x_2)\leftarrow R_{P,Q}}[x_1 \neq x_2] = \mathrm{SD}(P,Q)$.

Proof. For every $x \in \mathcal{D}$, let $M(x) = \min\{P(x), Q(x)\}$, let $M_P(x) = P(x) - M(x)$ and $M_Q(x) = Q(x) - M(x)$. The distribution $R_{P,Q}$ is defined by the following procedure. With probability $\mu = \sum_{x\in\mathcal{D}} M(x)$, sample an element x according to M (i.e., x is return with probability $\frac{M(x)}{\mu}$), and return (x,x), otherwise return (x_P, x_Q) where x_P is sampled according to M_P and x_Q is sampled according to M_Q. It is clear that $\Pr_{(x_1,x_2)\leftarrow R_{P,Q}}[x_1 \neq x_2] = \mathrm{SD}(P,Q)$. It also holds that

$$\begin{aligned}(R_{P,Q})_1(x) &= \mu \cdot \frac{M(x)}{\mu} + (1-\mu)\cdot\frac{M_P(x)}{\mu_P} \\ &= M(x) + M_P(x) \\ &= P(x),\end{aligned}$$

where $\mu_P := \sum_{x\in\mathcal{D}} M_P = (1-\mu)$. Namely, $(R_{P,Q})_1 \equiv P$. The proof that $(R_{P,Q})_2 \equiv Q$ is analogous.

□

Proof of Lemma 2.4.5. Using Proposition 2.4.6 and standard argument, it holds that $\mathrm{SD}\left(\mathsf{A}^f, \mathsf{A}^g\right)$ is at most the probability that the following experiment aborts.

Experiment 2.4.7.

1. *Start emulating a random execution of* A.

2. Do until A *halts:*

a) Let q *be the next query of* $\mathsf{A}(r)$.

b) if $q = \perp$ *give* $\perp$ *to* A *as the oracle answer and continue.*

c) Otherwise, sample $(a_1, a_2) \leftarrow R_{f(q),g(q)}$.

d) If $a_1 = a_2$, *give* a_1 *to* A *as the oracle answer.*

Otherwise, abort.

Letting $\mathrm{SD}(f(\perp), g(\perp)) = 0$ and setting $\mathcal{S}_i = \{q : q \in \mathrm{Supp}(F_i) \wedge F_i(q) \leq \lambda \cdot D_i(q)\}$ for $i \in [k]$, we conclude that

$$
\begin{aligned}
\mathrm{SD}\left(\mathsf{A}^f, \mathsf{A}^g\right) &\leq \Pr_{(q_1,\ldots,q_k)\leftarrow Q}\left[\exists i \in [k] \colon q_i \notin \mathcal{S}_i \cup \{\perp\}\right] \\
&\quad + \Pr_{(q_1,\ldots,q_k)\leftarrow Q}\left[\left(\exists i \in [k] : a_1 \neq a_2 \text{ where } (a_1, a_2) \leftarrow R_{f(q_i),g(q_i)}\right) \wedge (\forall \in [k] : q_i \in \mathcal{S}_i)\right] \\
&\leq \delta + \sum_{i\in[k]} \sum_{q\in\mathcal{S}_i} F_i(q) \cdot \Pr\left[a_1 \neq a_2 \text{ where } (a_1, a_2) \leftarrow R_{f(q),g(q)}\right] \\
&\leq \delta + \sum_{i\in[k]} \sum_{q\in\mathcal{S}_i} F_i(q) \cdot \mathrm{SD}(f(q), g(q)) \\
&\leq \delta + \sum_{i\in[k]} \sum_{q\in\mathrm{Supp}(D_i)} \lambda \cdot D_i(q) \cdot \mathrm{SD}(f(q), g(q)) \\
&\leq \delta + \lambda \sum_{i\in[k]} \mathrm{E}_{q\leftarrow D_i}[\mathrm{SD}(f(q), g(q))] \\
&\leq \delta + k\lambda\alpha,
\end{aligned}
$$

Where the third inequality follows from Proposition 2.4.6 and the fourth form the definition of the sets S_i. □

2.5 Two Inequalities

We make use of following technical lemmata, whose proofs are given in Appendix A.

Lemma 2.5.1. *Let $x, y \in [0,1]$ and $a_1, \ldots, a_k, b_1, \ldots, b_k \in (0,1]$. Then for any $p_0, p_1 \geq 0$ with $p_0 + p_1 = 1$, it holds that*

$$p_0 \cdot \frac{x^{k+1}}{\prod_{i=1}^{k} a_i} + p_1 \cdot \frac{y^{k+1}}{\prod_{i=1}^{k} b_i} \geq \frac{(p_0 x + p_1 y)^{k+1}}{\prod_{i=1}^{k} (p_0 a_i + p_1 b_i)}. \tag{2.1}$$

Lemma 2.5.2. *For every $\delta \in (0, \frac{1}{2}]$, there exists $\alpha = \alpha(\delta) \in (0,1]$ such that for every $x \geq \delta$*

$$\lambda \cdot a_1^{1+\alpha} \cdot (2 - a_1 \cdot x) + a_2^{1+\alpha} \cdot (2 - a_2 \cdot x) \leq (1 + \lambda) \cdot (2 - x) \tag{2.2}$$

for every $\lambda, y \geq 0$ with $\lambda y \leq 1$, where $a_1 = 1 + y$ and $a_2 = 1 - \lambda y$.

Chapter 3

The Biased-Continuation Attack

3.1 Biased Continuation

In this section we describe an attack to bias any (coin-flipping) protocol (in the following we typically omit the term "coin-flipping", since we only consider such protocols). The described attack, however, might be impossible to implement efficiently (even when assuming one-way functions do not exist). Specifically, we assume access to an ideal sampling algorithm to sample a *uniform* preimage of *any* output of the functions in consideration. Our actual attack, subject of Section 4.1, tries to mimic the behaviour of this attack while being efficiently implemented (assuming one-way functions do not exist).

The following discussion is restricted to (coin-flipping) protocols whose parties always output the same bit as their common output, and this bit is determined by the protocol's transcript. In all protocols considered in this section, the messages are bits. In addition, the protocols in consideration have no inputs (neither private nor common), and in particular no security parameter is involved.[1]. Recall that $\perp$ stands for a canonical invalid/udenfined protocol, and that $\mathrm{E}_{\langle\perp\rangle}[f] = 0$, for any real value function f. (We refer the reader to Chapter 2 for a discussion on the

[1]In Section 4.1, we make use of these input-less protocols by "hardwiring" the security parameter of the protocols in consideration.

conventions and assumptions used above.)

For concreteness, the attackers described below taking the left-hand side party of the protocol (i.e., A), are trying to bias the common output of the protocol towards one where the attackers taking the right-hand side party (i.e., B) are trying to bias the common output towards zero. All statements have analogues ones with respect to the opposite attack goals.

Let $\Pi = (\mathsf{A}, \mathsf{B})$ be a protocol. The *iterated biased-continuation attack* described below applies recursively the *biased-continuation attack* introduced by **(author?)** [HO11].[2] The biased-continuation attacker $\mathsf{A}_{\Pi}^{(1)}$ – playing the role of A – works as follows: in each of A's turns, $\mathsf{A}_{\Pi}^{(1)}$ picks a random continuation of Π, whose output it induces is equal one, and plays the current turn accordingly. The i'th biased-continuation attacker $\mathsf{A}_{\Pi}^{(i)}$, formally described below, uses the same strategy but the random continuation taken is of the protocol $(\mathsf{A}_{\Pi}^{(i-1)}, \mathsf{B})$.

Moving to the formal discussion, for a protocol $\Pi = (\mathsf{A}, \mathsf{B})$, let $\mathsf{BiasedCont}_{\Pi}$ be the following algorithm.

Algorithm 3.1.1 ($\mathsf{BiasedCont}_{\Pi}$)**.**

Input: $u \in \mathcal{V}(\Pi) \setminus \mathcal{L}(\Pi)$ *and a bit* $b \in \{0, 1\}$

Operation:

1. *Choose* $\ell \leftarrow \langle \Pi \rangle$ *conditioned that*

   a) $\ell \in \mathsf{desc}(u)$*, and*

   b) $\chi_{\Pi}(\ell) = b$.[3]

2. *Return* $\ell_{|u|+1}$.

[2] Called the "random continuation attack" in [HO11].

[3] In case no such ℓ exists, the algorithm returns an arbitrary leaf in $\mathsf{desc}(u)$.

Let $\mathsf{A}_{\Pi}^{(0)} \equiv \mathsf{A}$, and for integer $i > 0$ define:

Algorithm 3.1.2 ($\mathsf{A}_{\Pi}^{(i)}$)**.**

Oracle: $\mathsf{BiasedCont}_{(\mathsf{A}^{(i-1)},\mathsf{B})}$

Input: transcript $u \in \{0,1\}^*$.

Operation:

1. *If* $u \in \mathcal{L}(\Pi)$*, output* $\chi_\Pi(u)$ *and halt.*
2. *Set* $\mathsf{msg} = \mathsf{BiasedCont}_{(\mathsf{A}_{\Pi}^{(i-1)},\mathsf{B})}(u, 1)$.
3. *Send* msg *to* B.
4. *If* $u' = u \circ \mathsf{msg} \in \mathcal{L}(\Pi)$*, output* $\chi_\Pi(u')$.[4]

Adversary $\mathsf{B}_{\Pi}^{(i)}$ attacking towards zero is analogously defined. Specifically, changing the call $\mathsf{BiasedCont}_{(\mathsf{A}_{\Pi}^{(i-1)},\mathsf{B})}(u, 1)$ in Algorithm 3.1.2 to $\mathsf{BiasedCont}_{(\mathsf{A},\mathsf{B}_{\Pi}^{(i-1)})}(u, 0)$.[5]

It is relatively easy to show that the more recursions $\mathsf{A}_{\Pi}^{(i)}$ and $\mathsf{B}_{\Pi}^{(i)}$ do, the closer their success probability to that of an all powerful adversary, who can either bias the outcome to zero or to one. The important point of the following theorem is that for any $\varepsilon > 0$ there exists a *global* constant $\kappa = \kappa(\varepsilon)$ (i.e., independent

[4]For the mere purpose of biassing B's output, there is no need for $\mathsf{A}^{(i)}$ to output anything. Yet, doing that helps us to simplify our recursion definitions (specifically, we use the fact that in $(\mathsf{A}^{(i)}, \mathsf{B})$ the parties always have the same output).

[5]The subscript Π is added to the notation (i.e., $\mathsf{A}_{\Pi}^{(i)}$), since the biased-continuation attack for A depends not only on the definition of the party A, but also on the definition of B, the other party in the protocol.

of the underlying protocol), for which either $\mathsf{A}_{\Pi}^{(\kappa)}$ or $\mathsf{B}_{\Pi}^{(\kappa)}$ succeeds in its attack with probability at least $1-\varepsilon$. This fact gets crucial when trying to efficiently implement these adversaries (see Section 4.1), as each recursion call might induce a polynomial blowup in the running time of the adversary. Since κ is constant (for a constant ε), the recursive attacker is still efficient.

Theorem 3.1.3 (main theorem, ideal version)**.** *For every $\varepsilon \in (0, \frac{1}{2}]$ there exists an integer $\kappa = \kappa(\varepsilon) \geq 0$ such that for every protocol $\Pi = (\mathsf{A}, \mathsf{B})$, either $\mathsf{val}(\mathsf{A}_{\Pi}^{(\kappa)}, \mathsf{B}) > 1-\varepsilon$ or $\mathsf{val}(\mathsf{A}, \mathsf{B}_{\Pi}^{(\kappa)}) < \varepsilon$.*

The rest of this section is dedicated for proving the above theorem.

In what follows, we typically omit the subscript Π from the notation of the above attackers. Towards proving Theorem 3.1.3 we show a strong (and somewhat surprising) connection between iterated biased-continuation attacks on a given protocol, and the optimal valid attack one this protocol. The latter is the best (unbounded) attack on this protocol, which sends only valid messages (one that could have been sent by the honest party). Towards this goal we define sequences of a measures over the leaves (i.e., transcripts) of the protocol, connect these measures to the optimal attack, and then relate the success of the iterated biased-continuation attacks to these measures.

In the following we first observe some basic properties of the iterated biased-continuation attack. Next, we define the optimal valid attack, define a simple measure with respect to this attack, and prove, as a warm-up, the performance of iterated biased-continuation attacks on this measure. After arguing why considering the latter measure does not suffice, we define a sequence of measures, and then state, in Section 3.7, a property of this sequence that yields Theorem 3.1.3

as a corollary. The main body of this section deals with proving Section 3.7,

3.2 Basic Observations About $\mathsf{A}^{(i)}$

We make two basic observations regarding the iterated biased-continuation attack. The first gives expression to the edge distribution this attack induces. The second is that this attack is stateless. We'll use these observations in the following sections, however, the reader might want to skip their straightforward proofs for now.

Recall that at each internal node of its control, $\mathsf{A}^{(1)}$ picks a random continuation to one. Put it differently, $\mathsf{A}^{(1)}$, after seeing a transcript u, biases the probability of sending, e.g., 0 to B proportionally to the relative chance of having output one among all honest executions of the protocol, which are consistent with transcript $u \circ 0$, to those with transcript u. The behavior of $\mathsf{A}^{(i)}$ is analogues where $\mathsf{A}^{(i-1)}$ replaces the role of A in the above discussion. Formally, we have the following fact.

Claim 3.2.1. *Let $\Pi = (\mathsf{A}, \mathsf{B})$ be a protocol and let $\mathsf{A}^{(j)}$ be according to Algorithm 3.1.2, then*

$$e_{(\mathsf{A}^{(i)},\mathsf{B})}(u, ub) = e_{\Pi}(u, ub) \cdot \frac{\prod_{j=0}^{i-1} \mathsf{val}((\mathsf{A}^{(j)}, \mathsf{B})_{ub})}{\prod_{j=0}^{i-1} \mathsf{val}((\mathsf{A}^{(j)}, \mathsf{B})_{u})},$$ [6]

for any $i \in \mathbb{N}$, A-controlled $u \in \mathcal{V}(\Pi)$ and $b \in \{0, 1\}$.

This claim is a straightforward generalization of the proof of [HO11, Lemma 12]. Yet, for the purposes of completeness and giving an example of using our notations, a full proof is given below.

[6] Recall that for a protocol Π and a partial transcript u, we let $e_{\Pi}(u, ub)$ stands for the probability that the party controlling u sends b as the next message, conditioning that u is the transcript of the execution thus far.

Proof. The proof is by induction on i. For $i = 0$, recall that $\mathsf{A}^{(0)} \equiv \mathsf{A}$, and hence $e_{(\mathsf{A}^{(0)},\mathsf{B})}(u, ub) = e_{\Pi}(u, ub)$, as required.

Assume the claim holds for $i-1$, and we want to compute $e_{(\mathsf{A}^{(i)},\mathsf{B})}(u, ub)$. The definition of Algorithm 3.1.2 yields that for any positive $i \in \mathbb{N}$, it holds that

$$\begin{aligned} e_{(\mathsf{A}^{(i)},\mathsf{B})}(u, ub) &= \Pr_{\ell \leftarrow \langle \mathsf{A}^{(i-1)},\mathsf{B} \rangle}\left[\ell_{|u|+1} = b \mid \ell \in \mathsf{desc}(u) \wedge \chi_{\left(\mathsf{A}^{(i-1)},\mathsf{B}\right)}(\ell) = 1\right] \text{ [7]} \quad (3.1) \\ &= \frac{\Pr_{\ell \leftarrow \langle \mathsf{A}^{(i-1)},\mathsf{B} \rangle}\left[\ell_{|u|+1} = b \wedge \chi_{\left(\mathsf{A}^{(i-1)},\mathsf{B}\right)}(\ell) = 1 \mid \ell \in \mathsf{desc}(u)\right]}{\Pr_{\ell \leftarrow \langle \mathsf{A}^{(i-1)},\mathsf{B} \rangle}\left[\chi_{\left(\mathsf{A}^{(i-1)},\mathsf{B}\right)}(\ell) = 1 \mid \ell \in \mathsf{desc}(u)\right]} \\ &= e_{(\mathsf{A}^{(i-1)},\mathsf{B})}(u, ub) \cdot \frac{\mathsf{val}((\mathsf{A}^{(i-1)}, \mathsf{B})_{ub})}{\mathsf{val}((\mathsf{A}^{(i-1)}, \mathsf{B})_{u})}, \end{aligned}$$

where the last equality is by a simple chain rule, i.e., since

$$\begin{aligned} e_{(\mathsf{A}^{(i-1)},\mathsf{B})}(u, ub) &= \Pr_{\ell \leftarrow \langle \mathsf{A}^{(i-1)},\mathsf{B} \rangle}\left[\ell_{|u|+1} = b \mid \ell \in \mathsf{desc}(u)\right], \text{ and} \\ \mathsf{val}((\mathsf{A}^{(i-1)}, \mathsf{B})_{ub}) &= \Pr_{\ell \leftarrow \langle \mathsf{A}^{(i-1)},\mathsf{B} \rangle}\left[\chi_{\left(\mathsf{A}^{(i-1)},\mathsf{B}\right)}(\ell) = 1 \mid \ell \in \mathsf{desc}(u) \wedge \ell_{|u|+1} = b\right]. \end{aligned}$$

The proof in concluded by plugin the induction hypothesis into Equation (3.1).

□

The following observation enable us to use induction when analyzing the power of the $\mathsf{A}^{(i)}$.

Proposition 3.2.2. *For every protocol $\Pi = (\mathsf{A}_{\Pi}, \mathsf{B}_{\Pi})$, $i \in \mathbb{N}$ and $b \in \{0,1\}$, it holds that $\left(\mathsf{A}_{\Pi}^{(i)}, \mathsf{B}\right)_b$ and $\left(\mathsf{A}_{\Pi_b}^{(i)}, \mathsf{B}_{\Pi_b}\right)$ are the same protocol, where $\Pi_b = (\mathsf{A}_{\Pi_b}, \mathsf{B}_{\Pi_b})$*

Proof. Immediately follows from $\mathsf{A}_{\Pi}^{(i)}$ being stateless. □

Remark 3.2.3. *Note that the party B_{Π_b}, defined by the sub-protocol Π_b (specifically, by the edge distribution of the subtree $\mathcal{T}(\Pi_b)$) might not have an efficient*

[7] Recall that for a protocol Π, we let $\langle \Pi \rangle$ stands for the leaf distribution of Π.

implementation, even if B *has. For the sake of the arguments we make in this section, however, we only care that* B_{Π_b} *is well defined.*

3.3 Optimal Valid Attacks

When consider the optimal adversaries for a given protocol, we restrict ourselves to valid attackers. Informally, on each of its turns, a valid attacker sends a message from the set of possible replies that the honest party might choose given the transcript so far.

Definition 3.3.1 (optimal valid adversary)**.** *Let* $\Pi = (\mathsf{A}, \mathsf{B})$ *be a protocol. A deterministic algorithm* A' *playing the role of* A *in* Π *is in* $\mathcal{A}^*$*, if* $\mathsf{v}_\Pi(u) = 0 \implies \mathsf{v}_{(\mathsf{A}',\mathsf{B})}(u) = 0$ *for any* $u \in \mathcal{V}(\Pi)$*. The class* $\mathcal{B}^*$ *is analogously defined. Let* $\mathsf{OPT}_\mathsf{A}(\Pi) = \max_{\mathsf{A}' \in \mathcal{A}^*} \{\mathsf{val}(\mathsf{A}', \mathsf{B})\}$ *and* $\mathsf{OPT}_\mathsf{B}(\Pi) = \max_{\mathsf{B}' \in \mathcal{B}^*} \{1 - \mathsf{val}(\mathsf{A}, \mathsf{B}')\}$.

The following fact is immediate.

Proposition 3.3.2. *Let* $\Pi = (\mathsf{A}, \mathsf{B})$ *be a protocol and let* $u \in \mathcal{V}(\Pi)$*. Then,*

$$\mathsf{OPT}_\mathsf{A}(\Pi_u) = \begin{cases} \chi_\Pi(u) & u \in \mathcal{L}(\Pi); \\ \max\{\mathsf{OPT}_\mathsf{A}(\Pi_{ub}) \colon e_\Pi(u, ub) > 0\}, & u \notin \mathcal{L}(\Pi) \\ \qquad \textit{and } u \textit{ is controlled by } \mathsf{A}; & \\ e_\Pi(u, u0) \cdot \mathsf{OPT}_\mathsf{A}(\Pi_{u0}) + e_\Pi(u, u1) \cdot \mathsf{OPT}_\mathsf{A}(\Pi_{u1}), & u \notin \mathcal{L}(\Pi) \\ \qquad \textit{and } u \textit{ is controlled by } \mathsf{B}, & \end{cases}$$

and the analog conditions hold for $\mathsf{OPT}_\mathsf{B}(\Pi_u)$.[8]

The following holds true for any (bit value) protocol.

[8]Recall that for a (possible partial) transcript u, Π_u is the protocol Π, conditioned that $u_1, \ldots, u_{|u|}$ were that first $|u|$ messages.

Proposition 3.3.3. *Let* $\Pi = (\mathsf{A}, \mathsf{B})$ *be a protocol with* $\mathsf{val}(\Pi) \in [0,1]$*, then either* $\mathsf{OPT}_{\mathsf{A}}(\Pi)$ *or* $\mathsf{OPT}_{\mathsf{B}}(\Pi)$ *(but not both) is equal to* 1*.*

The somewhat surprising part is that *only* one party has a winning valid strategy. Assume for simplicity that $\mathsf{OPT}_{\mathsf{A}}(\Pi) = 1$. Since A might accidently act like the optimal winning adversary, it follows that for any valid strategy B' for B there is a positive probability over the random choices of the honest A that the outcome is *not* zero. Namely, it holds that $\mathsf{OPT}_{\mathsf{B}}(\Pi) < 1$. The formal proof follows a straightforward induction on the protocol's round complexity.

Proof of Proposition 3.3.3. The proof is by induction on the round complexity of Π. Assume that $\mathrm{round}(\Pi) = 0$ and let ℓ be the only node in $\mathcal{T}(\Pi)$. In case $\chi_{\Pi}(\ell) = 1$ the proof follows since $\mathsf{OPT}_{\mathsf{A}}(\Pi) = 1$ and $\mathsf{OPT}_{\mathsf{B}}(\Pi) = 0$. In the complementary case, i.e., $\chi_{\pi}(\ell) = 0$ the proof follows since $\mathsf{OPT}_{\mathsf{A}}(\Pi) = 0$ and $\mathsf{OPT}_{\mathsf{B}}(\Pi) = 1$.

Assume that the lemma holds for m-round protocols and that $\mathrm{round}(\Pi) = m+1$. In case $e_{\Pi}(\lambda, b) = 1$[9] for some $b \in \{0,1\}$, since Π is a protocol, it holds that $e_{\Pi}(\lambda, 1-b) = 0$. Hence, by Proposition 3.3.2 it holds that $\mathsf{OPT}_{\mathsf{A}}(\Pi) = \mathsf{OPT}_{\mathsf{A}}(\Pi_b)$ and $\mathsf{OPT}_{\mathsf{B}}(\Pi) = \mathsf{OPT}_{\mathsf{B}}(\Pi_b)$, regardless of the party controlling $\mathsf{root}(\Pi)$. The proof follows from the induction hypothesis.

In case $e_{\Pi}(\lambda, b) \notin \{0,1\}$ for both $b \in \{0,1\}$, the proof splits according to the following complementary cases.

$\mathsf{OPT}_{\mathsf{B}}(\Pi_0) < 1$ and $\mathsf{OPT}_{\mathsf{B}}(\Pi_1) < 1$. The induction hypothesis yields that $\mathsf{OPT}_{\mathsf{A}}(\Pi_0) = 1$ and $\mathsf{OPT}_{\mathsf{A}}(\Pi_1) = 1$. Proposition 3.3.2 now yields that $\mathsf{OPT}_{\mathsf{B}}(\Pi) < 1$ and $\mathsf{OPT}_{\mathsf{A}}(\Pi) = 1$, regardless of the party controlling $\mathsf{root}(\Pi)$.

[9] Recall that λ is the string representation of the root of $\mathcal{T}(\Pi)$.

$\mathsf{OPT}_{\mathsf{B}}(\Pi_0) = 1$ **and** $\mathsf{OPT}_{\mathsf{B}}(\Pi_1) = 1$**.** The induction hypothesis yields that $\mathsf{OPT}_{\mathsf{A}}(\Pi_0) < 1$ and $\mathsf{OPT}_{\mathsf{A}}(\Pi_1) < 1$. Proposition 3.3.2 now yields that $\mathsf{OPT}_{\mathsf{B}}(\Pi) = 1$ and $\mathsf{OPT}_{\mathsf{A}}(\Pi) < 1$, regardless of the party controlling $\mathsf{root}(\Pi)$.

$\mathsf{OPT}_{\mathsf{B}}(\Pi_0) = 1$ **and** $\mathsf{OPT}_{\mathsf{B}}(\Pi_1) < 1$**.** The induction hypothesis yields that $\mathsf{OPT}_{\mathsf{A}}(\Pi_0) < 1$ and $\mathsf{OPT}_{\mathsf{A}}(\Pi_1) = 1$. In case A controls $\mathsf{root}(\Pi)$, Proposition 3.3.2 yields that $\mathsf{OPT}_{\mathsf{A}}(\Pi) = 1$ and $\mathsf{OPT}_{\mathsf{B}}(\Pi) < 1$. In case B controls $\mathsf{root}(\Pi)$, Proposition 3.3.2 yields that $\mathsf{OPT}_{\mathsf{A}}(\Pi) < 1$ and $\mathsf{OPT}_{\mathsf{B}}(\Pi) = 1$. Hence, the proof follows.

$\mathsf{OPT}_{\mathsf{B}}(\Pi_0) < 1$ and $\mathsf{OPT}_{\mathsf{B}}(\Pi_1) = 1$. The proof follows arguments similar to the previous case.

□

In the next sections we show the connection between the optimal valid adversary and iterated biased-continuation attacks, by connecting them both to a specific measure over the protocol's leaves, called here the "dominated measure" of a protocol.

3.4 Dominated Measures

Consider the following measure over the protocol's leaves.

Definition 3.4.1 (dominated measures)**.** *The* A-dominated measure *of protocol* $\Pi = (\mathsf{A}, \mathsf{B})$*, denoted* M^{A}_{Π}*, is a measure over* $\mathcal{L}(\Pi)$ *defined as* $M^{\mathsf{A}}_{\Pi}(\ell) = \chi_{\Pi}(\ell)$ *in*

case $\text{round}(\Pi) = 0$*, and otherwise recursively defined by:*

$$M_{\Pi}^{\mathsf{A}}(\ell) = \begin{cases} 0, & e_{\Pi}(\lambda, \ell_1) = 0;^{10} \\ M_{\Pi_{\ell_1}}^{\mathsf{A}}(\ell_{2,\ldots,|\ell|}), & e_{\Pi}(\lambda, \ell_1) = 1; \\ M_{\Pi_{\ell_1}}^{\mathsf{A}}(\ell_{2,\ldots,|\ell|}), & e_{\Pi}(\lambda, \ell_1) \notin \{0,1\} \\ & \wedge(\mathsf{A} \textit{ controls } \mathsf{root}(\Pi) \vee \mathsf{Smaller}_{\Pi}(\ell_1)); \\ \frac{\mathrm{E}_{\langle \Pi_{1-\ell_1} \rangle}\left[M_{\Pi_{1-\ell_1}}^{\mathsf{A}}\right]}{\mathrm{E}_{\langle \Pi_{\ell_1} \rangle}\left[M_{\Pi_{\ell_1}}^{\mathsf{A}}\right]} \cdot M_{\Pi_{\ell_1}}^{\mathsf{A}}(\ell_{2,\ldots,|\ell|}), & \textit{otherwise.} \end{cases},$$

where $\mathsf{Smaller}_{\Pi}(\ell_1) = 1$ *if* $\mathrm{E}_{\langle \Pi_{\ell_1} \rangle}\left[M_{\Pi_{\ell_1}}^{\mathsf{A}}\right] \leq \mathrm{E}_{\langle \Pi_{1-\ell_1} \rangle}\left[M_{\Pi_{1-\ell_1}}^{\mathsf{A}}\right]$*. Finally, we let* $M_{\perp}^{\mathsf{A}}$ *be the zero measure.*

The B-dominated measure *of protocol* Π*, denoted* M_{Π}^{B}*, is analogously defined, except that* $M_{\Pi}^{\mathsf{B}}(\ell) = 1 - \chi_{\Pi}(\ell)$ *in case* $\text{round}(\Pi) = 0$*.*

The following key observation justifies the name of the above measures.

Lemma 3.4.2. *Let* $\Pi = (\mathsf{A}, \mathsf{B})$ *be a protocol and let* M_{Π}^{A} *be its* A*-dominated measure, then* $\mathsf{OPT}_{\mathsf{B}}(\Pi) = 1 - \mathrm{E}_{\langle \Pi \rangle}\left[M_{\Pi}^{\mathsf{A}}\right]$*.*

In particular, since $\mathsf{OPT}_{\mathsf{A}}(\Pi) = 1$ iff $\mathsf{OPT}_{\mathsf{B}}(\Pi) < 1$ (Proposition 3.3.2), it holds that $\mathsf{OPT}_{\mathsf{A}}(\Pi) = 1$ iff $\mathrm{E}_{\langle \Pi \rangle}\left[M_{\Pi}^{\mathsf{A}}\right] > 0$.

The proof of Lemma 3.4.2 is given below. For the intuitive explanation, note that in case A controls the root, the expected value of the A-dominated measure is the weighted average of the measures of the sub-protocols Π_0 and Π_1 (according to the edge distributions). Where in case B controls the root, the expected value is that of the lowest measure of the same sub-protocols. Hence, in both cases the A-dominated measure "captures" the behaviour of the optimal adversary for B.

[10] Recall that for transcript ℓ, ℓ_1 stands for the first messages sent in ℓ.

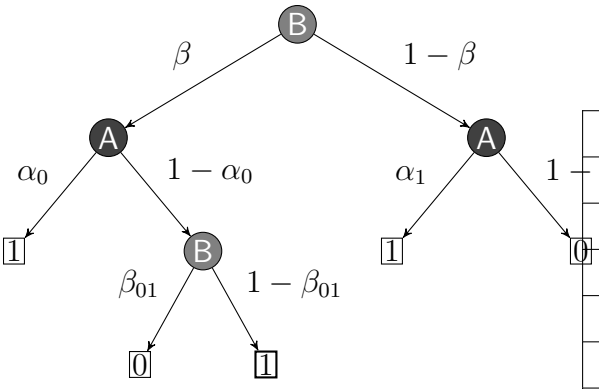
Example 3.4.3. *Before continuing with the formal proof, we believe the reader might find the following concrete example useful. Let* $\Pi = (\mathsf{A}, \mathsf{B})$ *be the protocol described in Figure 3.1a and assume for the sake of this example that* $\alpha_0 < \alpha_1$*. The* A*-dominated measures of* Π *and its sub-protocols are given in Figure 3.1b.*

We would like to highlight some points regarding the calculations of the A*-dominated measures. The first point we note is that* $M^{\mathsf{A}}_{\Pi_{011}}(011) = 1$ *but* $M^{\mathsf{A}}_{\Pi_{01}}(011) = 0$*. Namely, the* A*-dominated measure of the sub-protocol* Π_{011} *assign the leaf represented by the string* 011 *with the value* 1*, while the* A*-dominated measure of the sub-protocol* Π_{01} *(for which* Π_{011} *is a sub-protocol) assign the same leaf with the value* 0*. This follows since* $\mathrm{E}_{\langle \Pi_{010} \rangle}\left[M^{\mathsf{A}}_{\Pi_{010}}\right] = 0$ *and* $\mathrm{E}_{\langle \Pi_{011} \rangle}\left[M^{\mathsf{A}}_{\Pi_{011}}\right] = 1$*, which yield that* $\mathsf{Smaller}_{\Pi_{01}}(1) = 0$ *(recall that* $\mathsf{Smaller}_{\Pi'}(b) = 0$ *iff the expected value of the* A*-dominated measure of* Π'_b *is larger than that of the* A*-dominated measure of* Π'_{1-b}*). Hence, Definition 3.4.1 with respect to* Π_{01} *now yields that*

$$\begin{aligned} M^{\mathsf{A}}_{\Pi_{01}}(011) &= \frac{\mathrm{E}_{\langle \Pi_{010} \rangle}\left[M^{\mathsf{A}}_{\Pi_{010}}\right]}{\mathrm{E}_{\langle \Pi_{011} \rangle}\left[M^{\mathsf{A}}_{\Pi_{011}}\right]} \cdot M^{\mathsf{A}}_{\Pi_{011}}(011) \\ &= \frac{0}{1} \cdot 1 = 0. \end{aligned}$$

The second point we note is that $M^{\mathsf{A}}_{\Pi_1}(10) = 1$ *but* $M^{\mathsf{A}}_{\Pi}(10) = \frac{\alpha_0}{\alpha_1}$ *(recall that we assumed that* $\alpha_0 < \alpha_1$*, so* $\frac{\alpha_0}{\alpha_1} < 1$*). This follows similar arguments to the previous point; it holds that* $\mathrm{E}_{\langle \Pi_0 \rangle}\left[M^{\mathsf{A}}_{\Pi_0}\right] = \alpha_0$ *and* $\mathrm{E}_{\langle \Pi_1 \rangle}\left[M^{\mathsf{A}}_{\Pi_1}\right] = \alpha_1$*, which yields that* $\mathsf{Smaller}_{\Pi}(1) = 0$ *(since* $\alpha_0 < \alpha_1$*). Definition 3.4.1 with respect to* Π *now yields that*

$$\begin{aligned} M^{\mathsf{A}}_{\Pi}(10) &= \frac{\mathrm{E}_{\langle \Pi_0 \rangle}\left[M^{\mathsf{A}}_{\Pi_0}\right]}{\mathrm{E}_{\langle \Pi_1 \rangle}\left[M^{\mathsf{A}}_{\Pi_1}\right]} \cdot M^{\mathsf{A}}_{\Pi_1}(10) \\ &= \frac{\alpha_0}{\alpha_1} \cdot 1 = \frac{\alpha_0}{\alpha_1}. \end{aligned}$$



(a) Protocol $\Pi = (\mathsf{A}, \mathsf{B})$. The label of an internal node denotes the name of the party controlling it, and that of a leaf denotes its value. The label on an edge leaving a node u to node u' denotes the probability that a random execution of Π visits u' once in u. Finally, all nodes are represented as strings from the root of Π, even when considering sub-protocols (e.g., the string representations of the leaf with the thick borders is 011).

	Leaves				
measures	00	010	011	10	11
$M^{\mathsf{A}}_{\Pi_{00}}$	1				
$M^{\mathsf{A}}_{\Pi_{010}}$		0			
$M^{\mathsf{A}}_{\Pi_{011}}$			1		
$M^{\mathsf{A}}_{\Pi_{01}}$		0	0		
$M^{\mathsf{A}}_{\Pi_{0}}$	1	0	0		
$M^{\mathsf{A}}_{\Pi_{10}}$				1	
$M^{\mathsf{A}}_{\Pi_{11}}$					0
$M^{\mathsf{A}}_{\Pi_{1}}$				1	0
M^{A}_{Π}	1	0	0	α_0/α_1	0

(b) Calculating the A-dominated measure of Π. The A-dominated measure of a sub-protocol Π_u, is only defined over the leaves in the subtree $\mathcal{T}(\Pi_u)$.

Figure 3.1: Example for a coin flipping protocol is given to the left, and for calculating its A-dominated measure is given to the right.

The third and final point we note is the implication of Lemma 3.4.2 for this protocol. By the assumption that $\alpha_0 < \alpha_1$ it holds that $\mathsf{OPT}_{\mathsf{B}}(\Pi) = 1 - \alpha_0$. Independently, let us calculate the expected value of the A-dominated measure. Since $\mathrm{Supp}\left(M^{\mathsf{A}}_{\Pi}\right) = \{00, 01\}$, it holds that

$$\begin{aligned}
\mathrm{E}_{\langle\Pi\rangle}\left[M^{\mathsf{A}}_{\Pi}\right] &= \mathsf{v}_{\Pi}(00) \cdot M^{\mathsf{A}}_{\Pi}(00) + \mathsf{v}_{\Pi}(10) \cdot M^{\mathsf{A}}_{\Pi}(10) \\
&= \beta \cdot \alpha_0 \cdot 1 + (1-\beta) \cdot \alpha_1 \cdot \frac{\alpha_0}{\alpha_1} \\
&= \alpha_0.
\end{aligned}$$

Hence, $\mathrm{E}_{\langle\Pi\rangle}\left[M^{\mathsf{A}}_{\Pi}\right] = 1 - \mathsf{OPT}_{\mathsf{B}}(\Pi)$.

Towards proving Lemma 3.4.2, we first notice that the definition of M^{A}_{Π} assures three important properties.

Proposition 3.4.4. *Let* Π *be a protocol with* $e_{\Pi}(\lambda, b) \notin \{0,1\}$ *for both* $b \in \{0,1\}$. *Then*

1. *(*A*-maximal)* A *controls* $\mathsf{root}(\Pi) \implies \left(M^{\mathsf{A}}_{\Pi}\right)_b \equiv M^{\mathsf{A}}_{\Pi_b}$ *for both* $b \in \{0,1\}$.[11]

2. *(*B*-minimal)* B *controls* $\mathsf{root}(\Pi) \implies \left(M^{\mathsf{A}}_{\Pi}\right)_b \equiv \begin{cases} M^{\mathsf{A}}_{\Pi_b}, \mathsf{Smaller}_{\Pi}(b) = 1; \\ \frac{\mathrm{E}_{\langle \Pi_{1-b} \rangle}\left[M^{\mathsf{A}}_{\Pi_{1-b}}\right]}{\mathrm{E}_{\langle \Pi_b \rangle}\left[M^{\mathsf{A}}_{\Pi_b}\right]} \cdot M^{\mathsf{A}}_{\Pi_b}, \textit{else.} \end{cases}$

3. *(*B*-immune)* B *controls* $\mathsf{root}(\Pi) \implies \mathrm{E}_{\langle \Pi_0 \rangle}\left[\left(M^{\mathsf{A}}_{\Pi}\right)_0\right] = \mathrm{E}_{\langle \Pi_1 \rangle}\left[\left(M^{\mathsf{A}}_{\Pi}\right)_1\right]$.

Namely, in case A controls $\mathsf{root}(\Pi)$, the A-*maximal* property of M^{A}_{Π} (the A-dominated measure of Π) assures that the restrictions of this measure to the sub-protocols of Π are the A-dominated measures of these sub-protocols. In the complementary case, i.e., B controls $\mathsf{root}(\Pi)$, the B-*minimal* property of M^{A}_{Π} assures that for at least one sub-protocol of Π, the restriction of this measure to this sub-protocol is equal to the A-dominated measure of the sub-protocol. Moreover, the B-*immune* property of M^{A}_{Π} assures that the expected values of the measures derived by restrict M^{A}_{Π} to the sub-protocols of Π are equal (and hence, they are also equal to the expected value of M^{A}_{Π}).

Proof of Proposition 3.4.4. The proof of Items 1 and 2 immediately follows Definition 3.4.1.

Towards proving Item 3, assume B controls $\mathsf{root}(\Pi)$. In case $\mathsf{Smaller}_{\Pi}(0) = \mathsf{Smaller}_{\Pi}(1) = 1$, the proof again follows immediately from Definition 3.4.1. In

[11] Recall that for a measure $M \colon \mathcal{L}(\Pi) \mapsto [0,1]$ and a bit b, $(M)_b$ is the measure induced by M when restricted to $\mathcal{L}(\Pi_b) \subseteq \mathcal{L}(\Pi)$.

the complementary case, i.e., $\mathsf{Smaller}_{\Pi}(b) = 0$ and $\mathsf{Smaller}_{\Pi}(1-b) = 1$ for some $b \in \{0,1\}$, it holds that

$$\begin{aligned}
\mathrm{E}_{\langle \Pi_b \rangle}\left[\left(M_{\Pi}^{\mathsf{A}}\right)_b\right] &= \mathrm{E}_{\langle \Pi_b \rangle}\left[\frac{\mathrm{E}_{\langle \Pi_{1-b} \rangle}\left[M_{\Pi_{1-b}}^{\mathsf{A}}\right]}{\mathrm{E}_{\langle \Pi_b \rangle}\left[M_{\Pi_b}^{\mathsf{A}}\right]} \cdot M_{\Pi_b}^{\mathsf{A}}\right] \\
&= \frac{\mathrm{E}_{\langle \Pi_{1-b} \rangle}\left[M_{\Pi_{1-b}}^{\mathsf{A}}\right]}{\mathrm{E}_{\langle \Pi_b \rangle}\left[M_{\Pi_b}^{\mathsf{A}}\right]} \cdot \mathrm{E}_{\langle \Pi_b \rangle}\left[M_{\Pi_b}^{\mathsf{A}}\right] \\
&= \mathrm{E}_{\langle \Pi_{1-b} \rangle}\left[M_{\Pi_{1-b}}^{\mathsf{A}}\right] \\
&= \mathrm{E}_{\langle \Pi_{1-b} \rangle}\left[\left(M_{\Pi}^{\mathsf{A}}\right)_{1-b}\right],
\end{aligned}$$

where the first and last equalities follow the B-minimal property of M_{Π}^{A} (Proposition 3.4.4(2)). □

We are now ready to prove Lemma 3.4.2.

Proof of Lemma 3.4.2. The proof is by induction on the round complexity of Π.

Assume that $\mathrm{round}(\Pi) = 0$ and let ℓ be the only node in $\mathcal{T}(\Pi)$. In case $\chi_{\Pi}(\ell) = 1$, then by Definition 3.4.1 it holds that $M_{\Pi}^{\mathsf{A}}(\ell) = 1$, implying that $\mathrm{E}_{\langle \Pi \rangle}\left[M_{\Pi}^{\mathsf{A}}\right] = 1$. The proof follows since in this case, by Proposition 3.3.3, $\mathsf{OPT}_{\mathsf{B}}(\Pi) = 0$. In the complementary case, i.e., $\chi(\ell) = 0$, by Definition 3.4.1 it holds that $M_{\Pi}^{\mathsf{A}}(\ell) = 0$, implying that $\mathrm{E}_{\langle \Pi \rangle}\left[M_{\Pi}^{\mathsf{A}}\right] = 0$. The proof follows since in this case, by Proposition 3.3.3, $\mathsf{OPT}_{\mathsf{B}}(\Pi) = 1$.

Assume that the lemma holds for m-round protocols and that $\mathrm{round}(\Pi) = m+1$. For $b \in \{0,1\}$ let $\alpha_b := \mathrm{E}_{\langle \Pi_b \rangle}\left[M_{\Pi_b}^{\mathsf{A}}\right]$. The induction hypothesis yields that $\mathsf{OPT}_{\mathsf{B}}(\Pi_b) = 1 - \alpha_b$ for both $b \in \{0,1\}$. In case $e_{\Pi}(\lambda, b) = 1$ for some $b \in \{0,1\}$ (which also means that $e_{\Pi}(\lambda, 1-b) = 0$), the proof follows since Proposition 3.3.2 yields that $\mathsf{OPT}_{\mathsf{B}}(\Pi) = \mathsf{OPT}_{\mathsf{B}}(\Pi_b) = 1 - \alpha_b$, where Definition 3.4.1 yields that $\mathrm{E}_{\langle \Pi \rangle}\left[M_{\Pi}^{\mathsf{A}}\right] = \mathrm{E}_{\langle \Pi_b \rangle}\left[M_{\Pi_b}^{\mathsf{A}}\right] = \alpha_b$.

Assume $e_{\Pi}(\lambda, b) \notin \{0,1\}$ for both $b \in \{0,1\}$ and let $p := e_{\Pi}(\lambda, 0)$. The proof splits according to who controls the root of Π.

A controls $\mathsf{root}(\Pi)$. Definition 3.4.1 yields that

$$\begin{aligned}
\mathrm{E}_{\langle \Pi \rangle}\left[M_{\Pi}^{\mathsf{A}}\right] &= p \cdot \mathrm{E}_{\langle \Pi_0 \rangle}\left[\left(M_{\Pi}^{\mathsf{A}}\right)_0\right] + (1-p) \cdot \mathrm{E}_{\langle \Pi_1 \rangle}\left[\left(M_{\Pi}^{\mathsf{A}}\right)_1\right] \\
&= p \cdot \mathrm{E}_{\langle \Pi_0 \rangle}\left[M_{\Pi_0}^{\mathsf{A}}\right] + (1-p) \cdot \mathrm{E}_{\langle \Pi_1 \rangle}\left[M_{\Pi_1}^{\mathsf{A}}\right] \\
&= p \cdot \alpha_0 + (1-p) \cdot \alpha_1,
\end{aligned}$$

where the second equality follows the A-maximal property of $M_{\Pi_b}^{\mathsf{A}}$ (Proposition 3.4.4(1)). Using Proposition 3.3.2 we conclude that

$$\begin{aligned}
\mathsf{OPT}_{\mathsf{B}}(\Pi) &= p \cdot \mathsf{OPT}_{\mathsf{B}}(\Pi_0) + (1-p) \cdot \mathsf{OPT}_{\mathsf{B}}(\Pi_1) \\
&= p \cdot (1-\alpha_0) + (1-p) \cdot (1-\alpha_1) \\
&= 1 - (p \cdot \alpha_0 + (1-p) \cdot \alpha_1) \\
&= 1 - \mathrm{E}_{\langle \Pi \rangle}\left[M_{\Pi}^{\mathsf{A}}\right].
\end{aligned}$$

B controls $\mathsf{root}(\Pi)$. We assume that $\alpha_0 \leq \alpha_1$ (the complementary case is analogous). Proposition 3.3.2 and the induction hypothesis yield that $\mathsf{OPT}_{\mathsf{B}}(\mathsf{A}, \mathsf{B}) = 1 - \alpha_0$. Hence, it is left to show that $\mathrm{E}_{\langle \Pi \rangle}\left[M_{\Pi}^{\mathsf{A}}\right] = \alpha_0$. Note that the assumption that $\alpha_0 \leq \alpha_1$ yields that $\mathsf{Smaller}_{\Pi}(0) = 1$. Thus, by the B-minimal property of M_{Π}^{A} (Proposition 3.4.4(2)), it holds that $\left(M_{\Pi}^{\mathsf{A}}\right)_0 \equiv M_{\Pi_0}^{\mathsf{A}}$. It follows that $\mathrm{E}_{\langle \Pi_0 \rangle}\left[\left(M_{\Pi}^{\mathsf{A}}\right)_0\right] = \alpha_0$, and the B-immune property of M_{Π}^{A} (Proposition 3.4.4(3)) yields that $\mathrm{E}_{\langle \Pi_1 \rangle}\left[\left(M_{\Pi}^{\mathsf{A}}\right)_1\right] = \alpha_0$. To conclude the proof com-

pute,

$$\begin{aligned}
\mathrm{E}_{\langle \Pi \rangle}\left[M_{\Pi}^{\mathsf{A}}\right] &= p \cdot \mathrm{E}_{\langle \Pi_0 \rangle}\left[\left(M_{\Pi}^{\mathsf{A}}\right)_0\right] + (1-p) \cdot \mathrm{E}_{\langle \Pi_1 \rangle}\left[\left(M_{\Pi}^{\mathsf{A}}\right)_1\right] \\
&= p \cdot \alpha_0 + (1-p) \cdot \alpha_0 \\
&= \alpha_0.
\end{aligned}$$

□

Lemma 3.4.2 shows a connection between optimal attacks and the dominated measure. In the next section we show that the iterated biased-continuation attack also has a connection to the dominated measure. Unfortunately, this connection does not seem to suffice for our goal. In Section 3.6 we generalize the dominated measure described above to a sequence of (alternating) dominated measures, where in Section 3.7 we use this new notion to prove that the iterated biased continuation is indeed a good attack.

3.5 Warmup — Proof Attempt Using a (Single) Dominated Measure

As mentioned above, the approach described in this section falls too short to serve our goals. Yet, we describe it here as a detailed overview for the more complicated proof, given in in following sections (with respect to sequence of dominated measures). Specifically, we sketch the proof of the following lemma, relates the performance of the iterate biased-continuation attack, $\mathsf{A}^{(k)}$, running on some protocol Π, to the performance of the optimal (valid) adversary playing the role of B in the same protocol. The proof, see below, is done via the A-dominated measure

of Π defined above.[12]

Lemma 3.5.1. *Let $\Pi = (\mathsf{A}, \mathsf{B})$ be a protocol with $\mathsf{val}(\Pi) > 0$, let $k \in \mathbb{N}$ and let $\mathsf{A}^{(k)}$ be according to Algorithm 3.1.2, then*

$$\mathsf{val}(\mathsf{A}^{(k)}, \mathsf{B}) \geq \frac{1 - \mathsf{OPT}_{\mathsf{B}}(\Pi)}{\prod_{i=0}^{k-1} \mathsf{val}(\mathsf{A}^{(i)}, \mathsf{B})}.$$

The proof of the above lemma is a direct implication of the next lemma.

Lemma 3.5.2. *Let $\Pi = (\mathsf{A}, \mathsf{B})$ be a protocol with $\mathsf{val}(\Pi) > 0$, let $k \in \mathbb{N}$ and let $\mathsf{A}^{(k)}$ be according to Algorithm 3.1.2, then*

$$\mathrm{E}_{\langle \mathsf{A}^{(k)}, \mathsf{B} \rangle}\left[M_{\Pi}^{\mathsf{A}}\right] \geq \frac{\mathrm{E}_{\langle \Pi \rangle}\left[M_{\Pi}^{\mathsf{A}}\right]}{\prod_{i=0}^{k-1} \mathsf{val}(\mathsf{A}^{(i)}, \mathsf{B})}.$$

Proof of Lemma 3.5.1. Immediately follows Lemmas 3.4.2 and 3.5.2 and Fact 2.2.5. □

We begin by sketching the proof of the following lemma, which is a special case of Lemma 3.5.2. Later we say how to generalize the below proof to derive Lemma 3.5.2.

Lemma 3.5.3. *Let $\Pi = (\mathsf{A}, \mathsf{B})$ be a protocol with $\mathsf{val}(\Pi) > 0$ and let $\mathsf{A}^{(1)}$ be according to Algorithm 3.1.2, then $\mathrm{E}_{\langle \mathsf{A}^{(1)}, \mathsf{B} \rangle}\left[M_{\Pi}^{\mathsf{A}}\right] \geq \frac{\mathrm{E}_{\langle \Pi \rangle}\left[M_{\Pi}^{\mathsf{A}}\right]}{\mathsf{val}(\Pi)}$.*

Sketch. The proof is by induction on the round complexity of Π. The base case (i.e., $\mathrm{round}(\Pi) = 0$) is straightforward. Assume that the lemma holds for m-round protocols and that $\mathrm{round}(\Pi) = m + 1$. For $b \in \{0, 1\}$ let $\alpha_b := \mathrm{E}_{\langle \Pi_b \rangle}\left[M_{\Pi_b}^{\mathsf{A}}\right]$ and let $p := e_{\Pi}(\lambda, 0)$.

[12] Formal proof of Lemma 3.5.1 follows its stronger variant, Lemma 3.7.1, introduced in Section 3.7.

In case $\mathsf{root}(\Pi)$ is controlled by A, the A-maximal property of M^{A}_{Π} (Proposition 3.4.4(1)) yields that $\mathrm{E}_{\langle \Pi \rangle}\left[M^{\mathsf{A}}_{\Pi}\right] = p \cdot \alpha_0 + (1-p) \cdot \alpha_1$. It holds that

$$\begin{aligned}\mathrm{E}_{\left\langle \mathsf{A}^{(1)},\mathsf{B} \right\rangle}\left[M^{\mathsf{A}}_{\Pi}\right] &= e_{\left(\mathsf{A}^{(1)},\mathsf{B}\right)}(\lambda,0) \cdot \mathrm{E}_{\left\langle \left(\mathsf{A}^{(1)},\mathsf{B}\right)_0 \right\rangle}\left[\left(M^{\mathsf{A}}_{\Pi}\right)_0\right] + e_{\left(\mathsf{A}^{(1)},\mathsf{B}\right)}(\lambda,1) \cdot \mathrm{E}_{\left\langle \left(\mathsf{A}^{(1)},\mathsf{B}\right)_1 \right\rangle}\left[\left(M^{\mathsf{A}}_{\Pi}\right)_1\right] \qquad (3.2)\\ &= p \cdot \frac{\mathsf{val}(\Pi_0)}{\mathsf{val}(\Pi)} \cdot \mathrm{E}_{\left\langle \left(\mathsf{A}^{(1)},\mathsf{B}\right)_0 \right\rangle}\left[\left(M^{\mathsf{A}}_{\Pi}\right)_0\right] + (1-p) \cdot \frac{\mathsf{val}(\Pi_1)}{\mathsf{val}(\Pi)} \cdot \mathrm{E}_{\left\langle \left(\mathsf{A}^{(1)},\mathsf{B}\right)_1 \right\rangle}\left[\left(M^{\mathsf{A}}_{\Pi}\right)_1\right],\end{aligned}$$

where the second equality follows Claim 3.2.1. Since $\mathsf{A}^{(1)}$ is stateless (Proposition 3.2.2), we can write Equation (3.2) as

$$\mathrm{E}_{\left\langle \mathsf{A}^{(1)},\mathsf{B} \right\rangle}\left[M^{\mathsf{A}}_{\Pi}\right] = p \cdot \frac{\mathsf{val}(\Pi_0)}{\mathsf{val}(\Pi)} \cdot \mathrm{E}_{\left\langle \mathsf{A}^{(1)}_{\Pi_0},\mathsf{B}_{\Pi_0} \right\rangle}\left[\left(M^{\mathsf{A}}_{\Pi}\right)_0\right] + (1-p) \cdot \frac{\mathsf{val}(\Pi_1)}{\mathsf{val}(\Pi)} \cdot \mathrm{E}_{\left\langle \mathsf{A}^{(1)}_{\Pi_1},\mathsf{B}_{\Pi_1} \right\rangle}\left[\left(M^{\mathsf{A}}_{\Pi}\right)_1\right] \qquad (3.3)$$

The A-maximal property of M^{A}_{Π} and Equation (3.3) yield that

$$\mathrm{E}_{\left\langle \mathsf{A}^{(1)},\mathsf{B} \right\rangle}\left[M^{\mathsf{A}}_{\Pi}\right] = p \cdot \frac{\mathsf{val}(\Pi_0)}{\mathsf{val}(\Pi)} \cdot \mathrm{E}_{\left\langle \mathsf{A}^{(1)}_{\Pi_0},\mathsf{B}_{\Pi_0} \right\rangle}\left[M^{\mathsf{A}}_{\Pi_0}\right] + (1-p) \cdot \frac{\mathsf{val}(\Pi_1)}{\mathsf{val}(\Pi)} \cdot \mathrm{E}_{\left\langle \mathsf{A}^{(1)}_{\Pi_1},\mathsf{B}_{\Pi_1} \right\rangle}\left[M^{\mathsf{A}}_{\Pi_1}\right] \qquad (3.4)$$

Applying the induction hypothesis on the right-hand side of Equation (3.4) yields that

$$\begin{aligned}\mathrm{E}_{\left\langle \mathsf{A}^{(1)},\mathsf{B} \right\rangle}\left[M^{\mathsf{A}}_{\Pi}\right] &\geq p \cdot \frac{\mathsf{val}(\Pi_0)}{\mathsf{val}(\Pi)} \cdot \frac{\alpha_0}{\mathsf{val}(\Pi_0)} + (1-p) \cdot \frac{\mathsf{val}(\Pi_1)}{\mathsf{val}(\Pi)} \cdot \frac{\alpha_1}{\mathsf{val}(\Pi_1)}\\ &= \frac{p \cdot \alpha_0 + (1-p) \cdot \alpha_1}{\mathsf{val}(\Pi)}\\ &= \frac{\mathrm{E}_{\langle \Pi \rangle}\left[M^{\mathsf{A}}_{\Pi}\right]}{\mathsf{val}(\Pi)},\end{aligned}$$

which concludes the proof for the case that A controls $\mathsf{root}(\Pi)$.

In case $\mathsf{root}(\Pi)$ is controlled by B, and assuming that $\alpha_0 \leq \alpha_1$ (the complementary case is analogous), it holds that $\mathsf{Smaller}_{\Pi}(0) = 1$. Thus, by the B-minimal property of M^{A}_{Π} (Proposition 3.4.4(2)), it holds that $\left(M^{\mathsf{A}}_{\Pi}\right)_0 \equiv M^{\mathsf{A}}_{\Pi_0}$ and

$\left(M_{\Pi}^{\mathsf{A}}\right)_1 \equiv \frac{\alpha_0}{\alpha_1} M_{\Pi_1}^{\mathsf{A}}$. Hence, the B-immune property of M_{Π}^{A} (Proposition 3.4.4(3)) yields that $\mathrm{E}_{\langle \Pi \rangle}\left[M_{\Pi}^{\mathsf{A}}\right] = \alpha_0$. In addition, since B controls $\mathsf{root}(\Pi)$, the edge distribution of the edges $(\lambda, 0)$ and $(\lambda, 1)$ has not changed. It holds that

$$\begin{aligned}
\mathrm{E}_{\left\langle \mathsf{A}^{(1)}, \mathsf{B} \right\rangle}\left[M_{\Pi}^{\mathsf{A}}\right] &= p \cdot \mathrm{E}_{\left\langle \left(\mathsf{A}^{(1)}, \mathsf{B}\right)_0 \right\rangle}\left[\left(M_{\Pi}^{\mathsf{A}}\right)_0\right] + (1-p) \cdot \mathrm{E}_{\left\langle \left(\mathsf{A}^{(1)}, \mathsf{B}\right)_1 \right\rangle}\left[\left(M_{\Pi}^{\mathsf{A}}\right)_1\right] \qquad (3.5) \\
&= p \cdot \mathrm{E}_{\left\langle \mathsf{A}^{(1)}_{\Pi_0}, \mathsf{B}_{\Pi_0} \right\rangle}\left[\left(M_{\Pi}^{\mathsf{A}}\right)_0\right] + (1-p) \cdot \mathrm{E}_{\left\langle \mathsf{A}^{(1)}_{\Pi_1}, \mathsf{B}_{\Pi_1} \right\rangle}\left[\left(M_{\Pi}^{\mathsf{A}}\right)_1\right] \\
&= p \cdot \mathrm{E}_{\left\langle \mathsf{A}^{(1)}_{\Pi_0}, \mathsf{B}_{\Pi_0} \right\rangle}\left[M_{\Pi_0}^{\mathsf{A}}\right] + (1-p) \cdot \mathrm{E}_{\left\langle \mathsf{A}^{(1)}_{\Pi_1}, \mathsf{B}_{\Pi_1} \right\rangle}\left[\frac{\alpha_0}{\alpha_1} M_{\Pi_1}^{\mathsf{A}}\right] \\
&= p \cdot \mathrm{E}_{\left\langle \mathsf{A}^{(1)}_{\Pi_0}, \mathsf{B}_{\Pi_0} \right\rangle}\left[M_{\Pi_0}^{\mathsf{A}}\right] + (1-p) \cdot \frac{\alpha_0}{\alpha_1} \cdot \mathrm{E}_{\left\langle \mathsf{A}^{(1)}_{\Pi_1}, \mathsf{B}_{\Pi_1} \right\rangle}\left[M_{\Pi_1}^{\mathsf{A}}\right],
\end{aligned}$$

where the second equality follows since $\mathsf{A}^{(1)}$ is stateless (Proposition 3.2.2). Applying the induction hypothesis on the right-hand side of Equation (3.5) yields that

$$\begin{aligned}
\mathrm{E}_{\left\langle \mathsf{A}^{(1)}, \mathsf{B} \right\rangle}\left[M_{\Pi}^{\mathsf{A}}\right] &\geq p \cdot \frac{\alpha_0}{\mathsf{val}(\Pi_0)} + (1-p) \cdot \frac{\alpha_0}{\alpha_1} \cdot \frac{\alpha_1}{\mathsf{val}(\Pi_1)} \\
&= \alpha_0 \left(\frac{p}{\mathsf{val}(\Pi_0)} + \frac{1-p}{\mathsf{val}(\Pi_1)} \right) \\
&\geq \frac{\mathrm{E}_{\langle \Pi \rangle}\left[M_{\Pi}^{\mathsf{A}}\right]}{\mathsf{val}(\Pi)},
\end{aligned}$$

which concludes the proof for the case that A controls $\mathsf{root}(\Pi)$, and where the last equality holds since

$$\frac{p}{\mathsf{val}(\Pi_0)} + \frac{1-p}{\mathsf{val}(\Pi_1)} \geq \frac{1}{\mathsf{val}(\Pi)} \qquad (3.6)$$

□

The proof of Lemma 3.5.2 follows similar arguments to the ones used above for proving Lemma 3.5.3.[13] Informally, we proved Lemma 3.5.3 by showing that $\mathsf{A}^{(1)}$

[13]The proof sketch given for Lemma 3.5.3 is almost a formal proof. It only lacks dealing with the base case and the extreme cases in which $e_{\Pi}(\lambda, b) = 1$ for some $b \in \{0, 1\}$.

"puts" more weight on the dominated measure, than what A does. A natural step is to consider $\mathsf{A}^{(2)}$, and to see if it puts more weight on the dominated measure than what $\mathsf{A}^{(1)}$ does. It turns out that one can turn this intuitive argument into a formal proof, and prove Lemma 3.5.1 by repeating this procedure with respect to many iterated biased-continuation attacks.[14]

The shortcoming of Lemma 3.5.1. Given a protocol $\Pi = (\mathsf{A}, \mathsf{B})$, we are interested in the minimal value of κ for which $\mathsf{A}^{(\kappa)}$ biases the value of protocol towards one with probability at least 0.9 (as a concrete example). Following Lemma 3.5.1, it suffices to find a value κ such that

$$\mathsf{val}(\mathsf{A}^{(\kappa)}, \mathsf{B}) \geq \frac{1 - \mathsf{OPT}_{\mathsf{B}}(\Pi)}{\prod_{i=0}^{\kappa-1} \mathsf{val}(\mathsf{A}^{(i)}, \mathsf{B})} \geq 0.9 \tag{3.7}$$

Using worse case analysis, it suffices to find κ such that $(1 - \mathsf{OPT}_{\mathsf{B}}(\Pi))/(0.9)^{\kappa} \geq 0.9$, where the latter dictates that

$$\kappa \geq \frac{\log\left(\frac{1}{1-\mathsf{OPT}_{\mathsf{B}}(\Pi)}\right)}{\log\left(\frac{1}{0.9}\right)} \tag{3.8}$$

Recall that our ultimate goal is to implement an *efficient* attack on any coin-flipping protocol, under the mere assumption that one-way functions do not exist. Specifically, we would like to do so by given an efficient version of the iterated biased-continuation attack. For the very least, this requires the protocols in consideration by the iterated attack (i.e., $(\mathsf{A}^{(1)}, \mathsf{B}), \ldots, (\mathsf{A}^{(\kappa-1)}, \mathsf{B})$) to be efficient comparing to the basic protocol. The latter efficiency restriction together with the recursive definition of $\mathsf{A}^{(i)}$, dictates κ (the number of iterations) to be constant.

Unfortunately, the above discussion tells that in case in case $\mathsf{OPT}_{\mathsf{B}}(\Pi) \in 1 - o(1)$, we need take $\kappa \in \omega(1)$, yielding an inefficient attack.

[14]The main additional complication in the proof of Lemma 3.5.1, is that the simple argument used to derive Equation (3.6), is replaced with a the more general argument, described in Lemma 2.5.1.

3.6 Back to the Proof — Sequence of Alternating Dominated Measures

Let $\Pi = (\mathsf{A}, \mathsf{B})$ be a protocol and let M be a measure over the leaves of Π. Consider the variant of Π whose parties act identically like in Π, but with the following tweak: when the execution reaches a leaf ℓ, the protocol restarts with probability $M(\ell)$. Namely, a random execution of the resulting (possibly inefficient) protocol, is distributed like a random execution of Π, conditioned on not "hitting" the measure M.[15] The above is formally captured by the definition below.

Conditional protocols.

Definition 3.6.1 (conditional protocols)**.** *Let Π be an m-message protocol and let M be a measure over $\mathcal{L}(\Pi)$ with $\mathrm{E}_{\langle\Pi\rangle}[M] < 1$. The m-message, M-*conditional protocol of Π*, denoted $\Pi|\neg M$, is defined by the color function $\chi_{(\Pi|\neg M)} \equiv \chi_\Pi$, and the edge distribution function $e_{(\Pi|\neg M)}$ defined by*

$$e_{(\Pi|\neg M)}(u, ub) = \begin{cases} 0, & \mathrm{E}_{\langle\Pi_u\rangle}[M] = 1;^{16} \\ e_\Pi(u, ub) \cdot \frac{1-\mathrm{E}_{\langle\Pi_{ub}\rangle}[M]}{1-\mathrm{E}_{\langle\Pi_u\rangle}[M]}, & \textit{otherwise.} \end{cases},$$

for every $u \in \mathcal{V}(\Pi) \setminus \mathcal{L}(\Pi)$ and $b \in \{0,1\}$. The controlling scheme of the protocol $\Pi|\neg M$ is the same as in Π.

In case $\mathrm{E}_{\langle\Pi\rangle}[M] = 1$ or $\Pi = \perp$, we set $\Pi|\neg M = \perp$.

The next proposition shows that the M-conditional protocol is indeed a protocol. It also shows a relation between the leaves distributions of the M-conditional

[15] For concreteness, one might like to consider the case where M is a set.

[16] Note that this case does not affect the resulting protocol, and is defined only to simply future discussion.

protocol and the original protocol. Using this relation we conclude that the set of possible transcripts of the M-conditional protocol is a subset the original protocol's possible transcripts and that in case M gives value of 1 to some transcript, then this transcript is inaccessible by the M-conditional protocol.

Proposition 3.6.2. *Let Π be a protocol and let M be a measure over $\mathcal{L}(\Pi)$ with $\mathrm{E}_{\langle\Pi\rangle}[M] < 1$, then*

1. $\forall u \in \mathcal{V}(\Pi) \setminus \mathcal{L}(\Pi)\colon \quad \mathsf{v}_{(\Pi|\neg M)}(u) > 0 \implies e_{(\Pi|\neg M)}(u, u0) + e_{(\Pi|\neg M)}(u, u1) = 1;$
2. $\forall \ell \in \mathcal{L}(\Pi)\colon \quad \mathsf{v}_{(\Pi|\neg M)}(\ell) = \mathsf{v}_{\Pi}(\ell) \cdot \dfrac{1 - M(\ell)}{1 - \mathrm{E}_{\langle\Pi\rangle}[M]};$
3. $\forall \ell \in \mathcal{L}(\Pi)\colon \quad \mathsf{v}_{(\Pi|\neg M)}(\ell) > 0 \implies \mathsf{v}_{\Pi}(\ell) > 0;$ *and*
4. $\forall \ell \in \mathcal{L}(\Pi)\colon \quad M(\ell) = 1 \implies \mathsf{v}_{(\Pi|\neg M)}(\ell) = 0.$

Proof. The first two items immediately follows from Definition 3.6.1. The last two items follows the second item. □

In addition to the above properties, Definition 3.6.1 guarantees the following "locality" property of the M-conditional protocol.

Proposition 3.6.3. *Let Π be a protocol and let M be a measure over $\mathcal{L}(\Pi)$, then $(\Pi|\neg M)_u = \Pi_u|\neg(M)_u$ for every $u \in \mathcal{V}(\Pi) \setminus \mathcal{L}(\Pi)$.*

Proof. Immediately follows from Definition 3.6.1. □

Proposition 3.6.3 helps us to apply induction on conditional protocols. Specifically, we use it to prove the following lemma, which relates the dominated measure conditional protocol with the optimal (valid) attack.

Lemma 3.6.4. *Let $\Pi = (\mathsf{A}, \mathsf{B})$ be a protocol with $\mathsf{val}(\Pi) < 1$, then $\mathsf{OPT}_{\mathsf{B}}\left(\Pi|\neg M^{\mathsf{A}}_{\Pi}\right) = 1$.*

Proof. First, observe that by assuming that $\mathsf{val}(\Pi) < 1$, Definition 3.4.1 yields that $\mathrm{E}_{\langle \Pi \rangle}\left[M_{\Pi}^{\mathsf{A}}\right] < 1$, and hence $\Pi|\neg M_{\Pi}^{\mathsf{A}} \neq \perp$ (i.e., is a protocol). The rest of the proof is by induction on the round complexity of Π.

Assume that $\mathrm{round}(\Pi) = 0$ and let ℓ be the only node in $\mathcal{T}(\Pi)$. Since it is assumed that $\mathsf{val}(\Pi) < 1$, it must be the case that $\chi_{\Pi}(\ell) = 0$. The proof follows since $M_{\Pi}^{\mathsf{A}}(\ell) = 0$, and thus $\Pi|\neg M_{\Pi}^{\mathsf{A}} = \Pi$, and since $\mathsf{OPT}_{\mathsf{B}}(\Pi) = 1$.

Assume the lemma holds for m-round protocols and that $\mathrm{round}(\Pi) = m + 1$. In case $e_{\Pi}(\lambda, b) = 1$ for some $b \in \{0, 1\}$, Definition 3.4.1 yields that $\left(M_{\Pi}^{\mathsf{A}}\right)_b = M_{\Pi_b}^{\mathsf{A}}$. Moreover, Definition 3.6.1 yields that $e_{\left(\Pi|\neg M_{\Pi}^{\mathsf{A}}\right)}(\lambda, b) = 1$. It holds that

$$\begin{aligned}
\mathsf{OPT}_{\mathsf{B}}\left(\Pi|\neg M_{\Pi}^{\mathsf{A}}\right) &= \mathsf{OPT}_{\mathsf{B}}\left(\left(\Pi|\neg M_{\Pi}^{\mathsf{A}}\right)_b\right) \\
&= \mathsf{OPT}_{\mathsf{B}}\left(\Pi_b|\neg\left(M_{\Pi}^{\mathsf{A}}\right)_b\right) \\
&= \mathsf{OPT}_{\mathsf{B}}\left(\Pi_b|\neg M_{\Pi_b}^{\mathsf{A}}\right) \\
&= 1,
\end{aligned} \tag{3.9}$$

where the first equality follows Proposition 3.3.2, the second follows Proposition 3.6.3, and the last equality follows the induction hypothesis.

In the complementary case, i.e., $e_{\Pi}(\lambda, b) \notin \{0, 1\}$ for both $b \in \{0, 1\}$, the proof splits according to who controls the roof of Π.

A controls $\mathsf{root}(\Pi)$. The assumption that $\mathsf{val}(\Pi) < 1$ dictates that $\mathsf{val}(\Pi_0) < 1$ or $\mathsf{val}(\Pi_1) < 1$. Consider the following complimentary cases.

$\mathsf{val}(\Pi_0), \mathsf{val}(\Pi_1) < 1$**:** Proposition 3.3.2 yields that

$$\begin{aligned}
&\mathsf{OPT}_{\mathsf{B}}\left(\Pi|\neg M^{\mathsf{A}}_{\Pi}\right)\\
&= e_{\left(\Pi|\neg M^{\mathsf{A}}_{\Pi}\right)}(\lambda,0)\cdot \mathsf{OPT}_{\mathsf{B}}\left(\left(\Pi|\neg M^{\mathsf{A}}_{\Pi}\right)_0\right) + e_{\left(\Pi|\neg M^{\mathsf{A}}_{\Pi}\right)}(\lambda,1)\cdot \mathsf{OPT}_{\mathsf{B}}\left(\left(\Pi|\neg M^{\mathsf{A}}_{\Pi}\right)_1\right)\\
&= e_{\left(\Pi|\neg M^{\mathsf{A}}_{\Pi}\right)}(\lambda,0)\cdot \mathsf{OPT}_{\mathsf{B}}\left(\Pi_0|\neg\left(M^{\mathsf{A}}_{\Pi}\right)_0\right) + e_{\left(\Pi|\neg M^{\mathsf{A}}_{\Pi}\right)}(\lambda,1)\cdot \mathsf{OPT}_{\mathsf{B}}\left(\Pi_1|\neg\left(M^{\mathsf{A}}_{\Pi}\right)_1\right)\\
&= e_{\left(\Pi|\neg M^{\mathsf{A}}_{\Pi}\right)}(\lambda,0)\cdot \mathsf{OPT}_{\mathsf{B}}\left(\Pi_0|\neg M^{\mathsf{A}}_{\Pi_0}\right) + e_{\left(\Pi|\neg M^{\mathsf{A}}_{\Pi}\right)}(\lambda,1)\cdot \mathsf{OPT}_{\mathsf{B}}\left(\Pi_1|\neg M^{\mathsf{A}}_{\Pi_1}\right)\\
&= 1,
\end{aligned}$$

where the first equality follows Proposition 3.3.2, the second follows Proposition 3.6.3, the third follows by the A-maximal property of M^{A}_{Π} (Proposition 3.4.4(1)), and last equality follows the induction hypothesis.

$\mathsf{val}(\Pi_0) < 1$**,** $\mathsf{val}(\Pi_1) = 1$**:** By Definition 3.6.1, it holds that

$$\begin{aligned}
e_{\left(\Pi|\neg M^{\mathsf{A}}_{\Pi}\right)}(\lambda,1) &= e_{\Pi}(\lambda,1)\cdot\frac{1-\mathrm{E}_{\langle\Pi_1\rangle}\left[\left(M^{\mathsf{A}}_{\Pi}\right)_1\right]}{1-\mathrm{E}_{\langle\Pi\rangle}\left[M^{\mathsf{A}}_{\Pi}\right]}\\
&= e_{\Pi}(\lambda,1)\cdot\frac{1-\mathrm{E}_{\langle\Pi_1\rangle}\left[M^{\mathsf{A}}_{\Pi_1}\right]}{1-\mathrm{E}_{\langle\Pi\rangle}\left[M^{\mathsf{A}}_{\Pi}\right]}\\
&= 0,
\end{aligned}$$

where the second equality follows the A-maximal property of M^{A}_{Π}, and the last equality follows since $\mathsf{val}(\Pi_1) = 1$, which yields that $\mathrm{E}_{\langle\Pi_1\rangle}\left[M^{\mathsf{A}}_{\Pi_1}\right] = 1$. Since $\Pi|\neg M^{\mathsf{A}}_{\Pi}$ is a protocol (Proposition 3.6.2), it holds that $e_{\left(\Pi|\neg M^{\mathsf{A}}_{\Pi}\right)}(\lambda,0) = 1$. The proof now follows Equation (3.9).

$\mathsf{val}(\Pi_0) = 1$**,** $\mathsf{val}(\Pi_1) < 1$**:** The proof in analogous to the previous case.

B **controls** $\mathsf{root}(\Pi)$**.** Assume for simplicity that $\mathsf{Smaller}_{\Pi}(0) = 1$, namely that $\mathrm{E}_{\langle\Pi_0\rangle}\left[M^{\mathsf{A}}_{\Pi_0}\right] \leq \mathrm{E}_{\langle\Pi_1\rangle}\left[M^{\mathsf{A}}_{\Pi_1}\right]$ (the other case is analogous). First, observe that it

must hold that $\mathsf{val}(\Pi_0) < 1$ (otherwise, it holds that $\mathrm{E}_{\langle \Pi_0 \rangle}\left[M^{\mathsf{A}}_{\Pi_0}\right] = \mathrm{E}_{\langle \Pi_1 \rangle}\left[M^{\mathsf{A}}_{\Pi_1}\right] = 1$, which yields that $\mathsf{val}(\Pi_1) = 1$, and thus $\mathsf{val}(\Pi) = 1$). Hence, $\mathrm{E}_{\langle \Pi_0 \rangle}\left[M^{\mathsf{A}}_{\Pi_0}\right] < 1$, and Definition 3.6.1 yields that $e_{\left(\Pi|\neg M^{\mathsf{A}}_{\Pi}\right)}(\lambda, 0) > 0$. By Proposition 3.3.2, it holds that

$$\begin{aligned}
\mathsf{OPT}_{\mathsf{B}}\left(\Pi|\neg M^{\mathsf{A}}_{\Pi}\right) &\geq \mathsf{OPT}_{\mathsf{B}}\left(\left(\Pi|\neg M^{\mathsf{A}}_{\Pi}\right)_0\right) \\
&= \mathsf{OPT}_{\mathsf{B}}\left(\Pi_0|\neg\left(M^{\mathsf{A}}_{\Pi}\right)_0\right) \\
&= \mathsf{OPT}_{\mathsf{B}}\left(\Pi_0|\neg M^{\mathsf{A}}_{\Pi_0}\right) \\
&= 1,
\end{aligned}$$

where the second equality follows Proposition 3.6.3, the third follows the B-minimal property of M^{A}_{Π} (Proposition 3.4.4(2)), and the last equality follows the induction hypothesis. □

Let $\Pi = (\mathsf{A}, \mathsf{B})$ be a protocol in which an optimal adversary playing the role of A biases the outcome towards one with probability one. Lemma 3.6.4 shows that in the conditional protocol $\Pi_{(\mathsf{B},0)} := \Pi|\neg M^{\mathsf{A}}_{\Pi}$, an optimal adversary playing the role of B can bias the outcome towards zero with probability one. Repeating this procedure with respect to $\Pi_{(\mathsf{B},0)}$ results in the protocol $\Pi_{(\mathsf{A},1)} := \Pi_{(\mathsf{B},0)}|\neg M^{\mathsf{A}}_{\Pi_{(\mathsf{B},0)}}$, in which again an optimal adversary playing the role of A can bias the outcome towards one with probability one. This procedure is formally put in Definition 3.6.6.

Dominated measures sequence. Given a protocol (A, B), we use the simple ordering over the pairs $\{(\mathsf{C}, j)\}_{(\mathsf{C},j)\in\{\mathsf{A},\mathsf{B}\}\times\mathbb{Z}}$.

Notation 3.6.5. *Let* (A, B) *be a protocol. For* $j \in \mathbb{Z}$ *let* $\mathsf{pred}(\mathsf{A}, j) = (\mathsf{B}, j - 1)$ *and* $\mathsf{pred}(\mathsf{B}, j) = (\mathsf{A}, j)$*, and let* succ *be the inverse operation of* pred *(i.e.,* $\mathsf{succ}(\mathsf{pred}(\mathsf{C}, j)) = (\mathsf{C}, j)$*). For pairs* $(\mathsf{C}, j), (\mathsf{C}', j') \in \{\mathsf{A}, \mathsf{B}\} \times \mathbb{Z}$*, we write*

- (C, j) *is* less equal than (C', j') *, denoted* $(\mathsf{C}, j) \preceq (\mathsf{C}', j')$*, if* $\exists \{(\mathsf{C}_1, j_1), \ldots, (\mathsf{C}_n, j_n)\}$ *such that* $(\mathsf{C}, j) = (\mathsf{C}_1, j_1)$*,* $(\mathsf{C}', j') = (\mathsf{C}_n, j_n)$ *and* $(\mathsf{C}_i, j_i) = \mathsf{pred}(\mathsf{C}_{i+1}, j_{i+1})$ *for any* $i \in [n-1]$*.*

- (C, j) *is* less than (C', j')*, denoted* $(\mathsf{C}, j) \prec (\mathsf{C}', j')$*, if* $(\mathsf{C}, j) \preceq (\mathsf{C}', j')$ *and* $(\mathsf{C}, j) \neq (\mathsf{C}', j')$*.*

Finally, for $(\mathsf{C}, j) \succeq (\mathsf{A}, 0)$*, let* $[(\mathsf{C}, j)] := \{(\mathsf{C}', j') \colon (\mathsf{A}, 0) \preceq (\mathsf{C}', j') \preceq (\mathsf{C}, j)\}$*.*

Definition 3.6.6. *(dominated measures sequence) For a protocol* $\Pi = (\mathsf{A}, \mathsf{B})$ *and* $(\mathsf{C}, j) \in \{\mathsf{A}, \mathsf{B}\} \times \mathbb{N}$*, the protocol* $\Pi_{(\mathsf{C},j)}$ *is defined by*

$$\Pi_{(\mathsf{C},j)} = \begin{cases} \Pi, & (\mathsf{C}, j) = (\mathsf{A}, 0); \\ \Pi_{(\mathsf{C}',j')=\mathsf{pred}(\mathsf{C},j)} | \neg \left(M^{\mathsf{C}'}_{\Pi_{(\mathsf{C}',j')}} \right), & \textit{otherwise.}^{17} \end{cases}$$

Define the (C, j) dominated measures sequence of Π*, denoted* (C, j)-$\mathsf{D}MS(\Pi)$*, by* $\left\{ M^{\mathsf{C}'}_{\Pi_{(\mathsf{C}',j')}} \right\}_{(\mathsf{C}',j') \in [(\mathsf{C},j)]}$*. Finally, for* $z \in \mathbb{N}$*, let* $L^{\mathsf{C},z}_{\Pi} \equiv \sum_{j=0}^{z} M^{\mathsf{C}}_{\Pi_{(\mathsf{C},j)}} \prod_{t=0}^{j-1} \left(1 - M^{\mathsf{C}}_{\Pi_{(\mathsf{C},t)}}\right)$*.*

We show that $L^{\mathsf{A},z}_{\Pi}$ is a measure (i.e., its range is $[0,1]$) and that its support is a subset of the 1-leaves of Π. We also give an explicit expression for its expected value (analogous to the expected value of M^{A}_{Π} given in Lemma 3.4.2).

Lemma 3.6.7. *Let* $\Pi = (\mathsf{A}, \mathsf{B})$ *be a protocol, let* $z \in \mathbb{N}$ *and let* $L^{\mathsf{A},z}_{\Pi}$ *be as in Definition 3.6.6. It holds that*

1. $L^{\mathsf{A},z}_{\Pi}$ *is a measure over* $\mathcal{L}_1(\Pi)$*:*

   a) $L^{\mathsf{A},z}_{\Pi}(\ell) \in [0,1]$ *for every* $\ell \in \mathcal{L}(\Pi)$*, and*

[17] Note that in case $\mathrm{E}_{\langle \Pi_{(\mathsf{C},j)} \rangle} \left[M^{\mathsf{C}}_{\Pi_{(\mathsf{C},j)}} \right] = 1$, Definition 3.6.1 yields that $\Pi_{\mathsf{succ}(\mathsf{C},j)} = \perp$. In fact, since we defined $\perp | \neg M = \perp$ for any measure M (also in Definition 3.6.1), it follows that $\Pi_{(\mathsf{C}',j')} = \perp$ for any $(\mathsf{C}', j') \succ (\mathsf{C}, j)$.

b) $\text{Supp}\left(L_{\Pi}^{\mathsf{A},z}\right) \subseteq \mathcal{L}_1(\Pi)$.

2. $\mathrm{E}_{\langle\Pi\rangle}\left[L_{\Pi}^{\mathsf{A},z}\right] = \sum_{j=0}^{z} \alpha_j \cdot \prod_{t=0}^{j-1}(1-\beta_t)(1-\alpha_t)$, *where* $\alpha_j = 1 - \mathsf{OPT}_{\mathsf{B}}\left(\Pi_{(\mathsf{A},j)}\right)$, $\beta_j = 1 - \mathsf{OPT}_{\mathsf{A}}\left(\Pi_{(\mathsf{B},j)}\right)$ *and* $\mathsf{OPT}_{\mathsf{A}}(\perp) = \mathsf{OPT}_{\mathsf{B}}(\perp) = 1$.

Proof. We prove the above two items separately.

Proof of Item 1. Let $\ell \in \mathcal{L}_0(\Pi)$. Since $M^{\mathsf{A}}_{\Pi_{(\mathsf{A},j)}}(\ell) = 0$ for every $j \in (z)$, it holds that $L_{\Pi}^{\mathsf{A},z}(\ell) = 0$. Let $\ell \in \mathcal{L}_1(\Pi)$. Since $L_{\Pi}^{\mathsf{A},z}(\ell)$ is a sum of non negative numbers, it follows that its value is non negative. It is left to argue that $L_{\Pi}^{\mathsf{A},z}(\ell) \leq 1$. Since $M^{\mathsf{A}}_{\Pi_{(\mathsf{A},z)}}$ is a measure, note that $M^{\mathsf{A}}_{\Pi_{(\mathsf{A},z)}}(\ell) \leq 1$. Thus

$$
\begin{aligned}
L_{\Pi}^{\mathsf{A},z}(\ell) &= \sum_{j=0}^{z} M^{\mathsf{A}}_{\Pi_{(\mathsf{A},j)}}(\ell) \cdot \prod_{t=0}^{j-1}\left(1 - M^{\mathsf{A}}_{\Pi_{(\mathsf{A},t)}}(\ell)\right) \\
&\leq \prod_{t=0}^{z-1}\left(1 - M^{\mathsf{A}}_{\Pi_{(\mathsf{A},t)}}(\ell)\right) + \sum_{j=0}^{z-1} M^{\mathsf{A}}_{\Pi_{(\mathsf{A},j)}}(\ell) \cdot \prod_{t=0}^{j-1}\left(1 - M^{\mathsf{A}}_{\Pi_{(\mathsf{A},t)}}(\ell)\right) \\
&= \left(\sum_{\mathcal{I}\subseteq(z-1)} (-1)^{|\mathcal{I}|} \cdot \prod_{t\in\mathcal{I}} M^{\mathsf{A}}_{\Pi_{(\mathsf{A},t)}}(\ell)\right) \\
&+ \sum_{j=0}^{z-1} M^{\mathsf{A}}_{\Pi_{(\mathsf{A},j)}}(\ell) \cdot \left(\sum_{\mathcal{I}\subseteq(j-1)} (-1)^{|\mathcal{I}|} \cdot \prod_{t\in\mathcal{I}} M^{\mathsf{A}}_{\Pi_{(\mathsf{A},t)}}(\ell)\right) \\
&= \left(\sum_{\mathcal{I}\subseteq(z-1)} (-1)^{|\mathcal{I}|} \cdot \prod_{t\in\mathcal{I}} M^{\mathsf{A}}_{\Pi_{(\mathsf{A},t)}}(\ell)\right) \\
&+ \left(\sum_{\emptyset\neq\mathcal{I}\subseteq(z-1)} (-1)^{|\mathcal{I}|+1} \cdot \prod_{t\in\mathcal{I}} M^{\mathsf{A}}_{\Pi_{(\mathsf{A},t)}}(\ell)\right) \\
&= 1.
\end{aligned}
$$

Proof of Item 2. By linearity of expectation, it suffice to prove that

$$\mathrm{E}_{\langle \Pi \rangle}\left[M^{\mathsf{A}}_{\Pi_{(\mathsf{A},j)}} \cdot \prod_{t=0}^{j-1}\left(1 - M^{\mathsf{A}}_{\Pi_{(\mathsf{A},t)}}\right)\right] = \alpha_j \cdot \prod_{t=0}^{j-1}(1-\beta_t)(1-\alpha_t) \tag{3.10}$$

for any $j \in (z)$. Fix $j \in (z)$. In case $\Pi_{(\mathsf{A},j)} = \perp$, then by Definition 3.4.1 it holds that $M^{\mathsf{A}}_{\Pi_{(\mathsf{A},j)}}$ is the zero measure, and both sides of Equation (3.10) equal 0.

In the following we assume that $\Pi_{(\mathsf{A},j)} \neq \perp$. We first note that $\mathrm{E}_{\langle \Pi_{(\mathsf{C},t)} \rangle}\left[M^{\mathsf{C}}_{\Pi_{(\mathsf{C},t)}}\right] < 1$ for any $(\mathsf{C},t) \in [\mathsf{pred}(\mathsf{A},j)]$ (otherwise, it must be that $\Pi_{(\mathsf{A},j)} = \perp$). Thus, Lemma 3.4.2 yields that $\alpha_t, \beta_t < 1$ for every $t \in (j-1)$. Hence, recursively applying Proposition 3.6.2(2) yields that

$$\mathsf{v}_{\left(\Pi_{(\mathsf{A},j)}\right)}(\ell) = \mathsf{v}_{\Pi}(\ell) \cdot \prod_{t=0}^{j-1} \frac{1 - M^{\mathsf{A}}_{\Pi_{(\mathsf{A},t)}}(\ell)}{1-\alpha_t} \cdot \frac{1 - M^{\mathsf{B}}_{\Pi_{(\mathsf{B},t)}}(\ell)}{1-\beta_t} \tag{3.11}$$

for every $\ell \in \mathcal{L}(\Pi)$. Moreover, for $\ell \in \mathrm{Supp}\left(\Pi_{(\mathsf{A},j)}\right)$, i.e., $\mathsf{v}_{\left(\Pi_{(\mathsf{A},j)}\right)}(\ell) > 0$, we can manipulate Equation (3.11) to get that

$$\mathsf{v}_{\Pi}(\ell) = \mathsf{v}_{\left(\Pi_{(\mathsf{A},j)}\right)}(\ell) \cdot \prod_{t=0}^{j-1} \frac{1-\alpha_t}{1 - M^{\mathsf{A}}_{\Pi_{(\mathsf{A},t)}}(\ell)} \cdot \frac{1-\beta_t}{1 - M^{\mathsf{B}}_{\Pi_{(\mathsf{B},t)}}(\ell)} \tag{3.12}$$

for every $\ell \in \mathrm{Supp}\left(\Pi_{(\mathsf{A},j)}\right)$.

It follows that

$$
\begin{aligned}
&\mathrm{E}_{\langle\Pi\rangle}\left[M^{\mathsf{A}}_{\Pi_{(\mathsf{A},j)}}\cdot\prod_{t=0}^{j-1}\left(1-M^{\mathsf{A}}_{\Pi_{(\mathsf{A},t)}}\right)\right]\\
&=\sum_{\ell\in\mathcal{L}(\Pi)}\mathsf{v}_{\Pi}(\ell)\cdot\left(M^{\mathsf{A}}_{\Pi_{(\mathsf{A},j)}}(\ell)\cdot\prod_{t=0}^{j-1}\left(1-M^{\mathsf{A}}_{\Pi_{(\mathsf{A},t)}}(\ell)\right)\right)\\
&=\sum_{\ell\in\mathrm{Supp}\left(\Pi_{(\mathsf{A},j)}\right)\cap\mathcal{L}_1(\Pi)}\mathsf{v}_{\Pi}(\ell)\cdot\left(M^{\mathsf{A}}_{\Pi_{(\mathsf{A},j)}}(\ell)\cdot\prod_{t=0}^{j-1}\left(1-M^{\mathsf{A}}_{\Pi_{(\mathsf{A},t)}}(\ell)\right)\right)\\
&=\sum_{\ell\in\mathrm{Supp}\left(\Pi_{(\mathsf{A},j)}\right)\cap\mathcal{L}_1(\Pi)}\mathsf{v}_{\left(\Pi_{(\mathsf{A},j)}\right)}(\ell)\cdot\prod_{t=0}^{j-1}\frac{1-\alpha_t}{1-M^{\mathsf{A}}_{\Pi_{(\mathsf{A},t)}}(\ell)}\cdot\frac{1-\beta_t}{1-M^{\mathsf{B}}_{\Pi_{(\mathsf{B},t)}}(\ell)}\\
&\quad\cdot\left(M^{\mathsf{A}}_{\Pi_{(\mathsf{A},j)}}(\ell)\cdot\prod_{t=0}^{j-1}\left(1-M^{\mathsf{A}}_{\Pi_{(\mathsf{A},t)}}(\ell)\right)\right)\\
&=\sum_{\ell\in\mathrm{Supp}\left(\Pi_{(\mathsf{A},j)}\right)\cap\mathcal{L}_1(\Pi)}\mathsf{v}_{\left(\Pi_{(\mathsf{A},j)}\right)}(\ell)\cdot M^{\mathsf{A}}_{\Pi_{(\mathsf{A},j)}}(\ell)\cdot\prod_{t=0}^{j-1}\left(1-\alpha_j\right)\left(1-\beta_j\right)\\
&=\alpha_j\cdot\prod_{t=0}^{j-1}(1-\beta_t)(1-\alpha_t),
\end{aligned}
$$

concluding the proof. The second equality follows since Definition 3.4.1 yields that $M^{\mathsf{A}}_{\Pi_{(\mathsf{A},j)}}(\ell)=0$ for any $\ell\notin\mathrm{Supp}\left(\Pi_{(\mathsf{A},j)}\right)\cap\mathcal{L}_1(\Pi)$, the third equality follows by Equation (3.12) and the forth equality follows since $M^{\mathsf{B}}_{\Pi_{(\mathsf{B},t)}}(\ell)=0$ for every $\ell\in\mathcal{L}_1(\Pi)$ and $t\in(j-1)$.

□

Example 3.6.8. *Once again we consider the protocol* Π *from Figure 3.1a. In Figure 3.2 we present the conditional protocol* $\Pi_{(\mathsf{B},0)}=\Pi|\neg M^{\mathsf{A}}_{\Pi}$*, namely the protocol derived when protocol* Π *is conditioned not to "hit" the* A*-dominated measure of* Π*. We would like to highlight some points regarding this conditional protocol.*

The first point we note is the changes in the edges distribution. Considering the root of Π_0 *(i.e., the node* 0*), then according to the calculations in Figure 3.1b,*

it holds that $\mathrm{E}_{\langle \Pi_{00} \rangle}\left[M_{\Pi}^{\mathsf{A}}\right] = M_{\Pi}^{\mathsf{A}}(00) = 1$ *and that* $\mathrm{E}_{\langle \Pi_{0} \rangle}\left[M_{\Pi}^{\mathsf{A}}\right] = \alpha_0$*. Hence, Definition 3.6.1 yields that*

$$\begin{aligned} e_{\left(\Pi|\neg M_{\Pi}^{\mathsf{A}}\right)}(0,00) &= \alpha_0 \cdot \frac{1 - \mathrm{E}_{\langle \Pi_{00} \rangle}\left[M_{\Pi}^{\mathsf{A}}\right]}{1 - \mathrm{E}_{\langle \Pi_{0} \rangle}\left[M_{\Pi}^{\mathsf{A}}\right]} \\ &= \alpha_0 \cdot \frac{0}{1 - \alpha_0} \\ &= 0. \end{aligned}$$

Note that the above change makes the leaf 00 *inaccessible in* $\Pi_{(\mathsf{B},0)}$*. This occurs since* $M_{\Pi}^{\mathsf{A}}(00) = 1$ *and follows Proposition 3.6.2. Similar calculations yield the changes in the edge distribution of the edges leaving the root of* Π_1 *(i.e., the node* 1*).*

The second point we note is that the conditional protocol is in fact a protocol. Namely, that for every node, the sum of the edge distribution of the edges leaving it is one. This is easily seen from Figure 3.2 and again follows Proposition 3.6.2.

The third point we note is that the edges distribution of the root of Π *does not change at all. This follows Definition 3.6.1 and the fact that*

$$\mathrm{E}_{\langle \Pi_{0} \rangle}\left[M_{\Pi}^{\mathsf{A}}\right] = \mathrm{E}_{\langle \Pi_{1} \rangle}\left[M_{\Pi}^{\mathsf{A}}\right] = \mathrm{E}_{\langle \Pi \rangle}\left[M_{\Pi}^{\mathsf{A}}\right] = \alpha_0.$$

The forth point we note is that in the conditional protocol, optimal valid adversary playing the role of B *can bias the outcome towards zero with probability one. Namely,* $\mathsf{OPT}_{\mathsf{B}}\left(\Pi|\neg M_{\Pi}^{\mathsf{A}}\right) = 1$*. Such adversary will send* 0 *as the first message,* A *must send* 1 *as the next message, and then the adversary will send* 0*. The outcome of this interaction is the value of the leaf* 010*, which is* 0*. This follows Lemma 3.6.4.*

Using dominated measures sequences we manage to give an improved bound for the success probability of the iterated biased-continuation attacks (comparing to

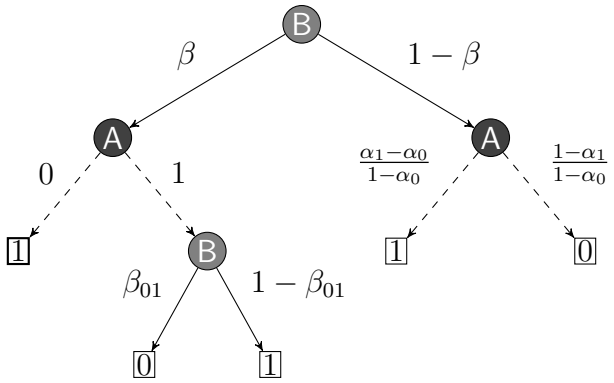


Figure 3.2: The conditional protocol $\Pi_{(\mathsf{B},0)} = \Pi|\neg M^{\mathsf{A}}_{\Pi}$ of Π from Figure 3.1a. Dashed Edges are such that their edge distribution has changed. Note that due to this change, the leaf 00 (the leftmost leaf, signal by thick border) is *inaccessible* in $\Pi_{(\mathsf{B},0)}$. The B-dominated measure of $\Pi_{(\mathsf{B},0)}$ assign value of 1 to the leaf 010, and value of 0 to all other leaves.

the bound of Lemma 3.5.3, which uses a single dominated measure). The improved analysis yields that constant iteration of biased-continuation attack is successful in biassing the protocol to arbitrary constant close to either 0 or 1.

3.7 Improved Analysis Using Alternating Dominated Measures

We are finally ready to state two main lemmas, whose proofs – given in the next two sections – are the main technical contribution of Chapter 3, and then show how to use them from proving Theorem 3.1.3.

The first lemma is analogous to Lemma 3.5.1, but applied on the sequence of the dominated measures, and not just on a single dominated measure.

Lemma 3.7.1. *For a protocol* $\Pi = (\mathsf{A}, \mathsf{B})$ *with* $\mathsf{val}(\Pi) > 0$ *and* $z \in \mathbb{N}$*, it holds that*

$$\mathsf{val}(\mathsf{A}^{(k)}, \mathsf{B}) \geq \mathrm{E}_{\langle \mathsf{A}^{(k)}, \mathsf{B} \rangle}\left[L_{\Pi}^{\mathsf{A},z}\right] \geq \frac{\mathrm{E}_{\langle \Pi \rangle}\left[L_{\Pi}^{\mathsf{A},z}\right]}{\prod_{i=0}^{k-1} \mathsf{val}(\mathsf{A}^{(i)}, \mathsf{B})} \cdot \left(1 - \sum_{j=0}^{z-1} \beta_j\right)^k$$

for every $k \in \mathbb{N}$*, where* $\beta_j = 1 - \mathsf{OPT}_{\mathsf{A}}\left(\Pi_{(\mathsf{B},j)}\right)$*, letting* $\mathsf{OPT}_{\mathsf{A}}(\perp) = 1$*.*

In words, Lemma 3.7.1 states that the iterated biased-continuation attacker biases the outcome of the protocol by a similar bound given in Lemma 3.5.1, but applied with respect to $L_{\Pi}^{\mathsf{A},z}$, instead of M_{Π}^{A} in Lemma 3.5.1. This is helpful since the expected value of $L_{\Pi}^{\mathsf{A},z}$ is strictly larger than that of M_{Π}^{A}. However, since $L_{\Pi}^{\mathsf{A},z}$ is defined in with respect to sequence of conditional protocols, we must "pay" the term $\left(1 - \sum_{j=0}^{z-1} \beta_j\right)^k$ in order to get this bound in the original protocol.

The following lemma states that Lemma 3.7.1 provides a sufficient bound. Specifically, it shows that taking long enough sequence of conditional protocols, the expected value of the measure $L_{\Pi}^{\mathsf{A},z}$ is sufficiently large, while keeping the payment term mentioned above sufficiently small.

Lemma 3.7.2. *Let* $\Pi = (\mathsf{A}, \mathsf{B})$ *be a protocol. Then for every* $c \in (0, \frac{1}{2}]$ *there exists* $z = z(c, \Pi) \in \mathbb{N}$ *(possibly exponential large) such that:*

1. $\mathrm{E}_{\langle \Pi \rangle}\left[L_{\Pi}^{\mathsf{A},z}\right] \geq c \cdot (1 - 2c)$ *and* $\sum_{j=0}^{z-1} \beta_j < c$*; or*
2. $\mathrm{E}_{\langle \Pi \rangle}\left[L_{\Pi}^{\mathsf{B},z}\right] \geq c \cdot (1 - 2c)$ *and* $\sum_{j=0}^{z} \alpha_j < c$*,*

where $\alpha_j = 1 - \mathsf{OPT}_{\mathsf{B}}\left(\Pi_{(\mathsf{A},j)}\right)$ *and* $\beta_j = 1 - \mathsf{OPT}_{\mathsf{A}}\left(\Pi_{(\mathsf{B},j)}\right)$*.*

To derive Theorem 3.1.3, we take long enough sequence of the dominated measures so that its accumulated weight is sufficiently large. Furthermore, the weight of the dominated measures precedes the final dominated measure in the sequence is

small (otherwise, we would have taken shorter sequence), so the parties are "missing" these measures with high probability. The formal proof of Theorem 3.1.3 is given next, and the proofs of Lemmas 3.7.1 and 3.7.2 are given in Sections 3.8 and 3.8 respectively.

Proving Theorem 3.1.3.

Proof of Theorem 3.1.3. In case $\mathsf{val}(\Pi) = 0$, Theorem 3.1.3 trivially holds. Assume that $\mathsf{val}(\Pi) > 0$, let z be the minimum integer guaranteed by Lemma 3.7.2 for $c = \varepsilon/2$ and let $\kappa = \left\lceil \frac{\log\left(\frac{2}{\varepsilon}\right)}{\log\left(\frac{1-\varepsilon/2}{1-\varepsilon}\right)} \right\rceil$.

In case z satisfies Item 1 of Lemma 3.7.2, assume towards a contradiction that $\mathsf{val}(\mathsf{A}^{(\kappa)}, \mathsf{B}) \leq 1 - \varepsilon$. Lemma 3.7.1 yields that

$$\begin{aligned}
\mathsf{val}(\mathsf{A}^{(\kappa)}, \mathsf{B}) &\geq \frac{\mathrm{E}_{\langle \Pi \rangle}\left[L_{\Pi}^{\mathsf{A},z}\right]}{\prod_{i=0}^{\kappa-1} \mathsf{val}(\mathsf{A}^{(i)}, \mathsf{B})} \cdot \left(1 - \sum_{j=0}^{z-1} \beta_j\right)^{\kappa} \\
&> \frac{\varepsilon(1-\varepsilon)}{2} \cdot \left(\frac{1-\varepsilon/2}{1-\varepsilon}\right)^{\kappa} \\
&\geq 1 - \varepsilon,
\end{aligned}$$

and a contradiction is derived.

In case z satisfies Item 2 of Lemma 3.7.2, analogous argument to the above yields that $\mathsf{val}(\mathsf{A}, \mathsf{B}^{(\kappa)}) \leq \varepsilon$. □

3.8 Proving Lemma 3.7.1

The proof of Lemma 3.7.1 is an easy implication of Lemma 3.6.7 and the following key lemma, defined with respect to sequences of *submeasures* of the dominated measure.

Definition 3.8.1. *(dominated submeasures sequence) For a protocol* $\Pi = (\mathsf{A}, \mathsf{B})$*, a pair* $(\mathsf{C}^*, j^*) \in \{\mathsf{A}, \mathsf{B}\} \times \mathbb{N}$ *and* $\boldsymbol{\eta} = \left\{\eta_{(\mathsf{C},j)} \in [0,1]\right\}_{(\mathsf{C},j)\in[(\mathsf{C}^*,j^*)]}$*, define the protocol* $\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)}$ *by*

$$\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)} := \begin{cases} \Pi, & (\mathsf{C},j) = (\mathsf{A},0); \\ \widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C}',j')=\mathsf{pred}(\mathsf{C},j)} | \neg \left(\widehat{M}^{\Pi,\boldsymbol{\eta}}_{(\mathsf{C}',j')}\right), & \textit{otherwise.} \end{cases},$$

where $\widehat{M}^{\Pi,\boldsymbol{\eta}}_{(\mathsf{C}',j')} \equiv \eta_{(\mathsf{C}',j')} \cdot M^{\mathsf{C}'}_{\Pi^{\boldsymbol{\eta}}_{(\mathsf{C}',j')}}$*. For* $(\mathsf{C},j) \in [(\mathsf{C}^*,j^*)]$*, define the* $(\mathsf{C},j,\boldsymbol{\eta})$-dominated measures sequence of Π*, denoted* $(\mathsf{C},j,\boldsymbol{\eta})$-$\mathsf{D}MS(\Pi)$*, as* $\left\{\widehat{M}^{\Pi,\boldsymbol{\eta}}_{(\mathsf{C}',j')}\right\}_{(\mathsf{C}',j')\in[(\mathsf{C},j)]}$*, and let* $\widehat{\mu}^{\Pi,\boldsymbol{\eta}}_{(\mathsf{C},j)} = \mathrm{E}_{\left\langle \widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)} \right\rangle}\left[\widehat{M}^{\Pi,\boldsymbol{\eta}}_{(\mathsf{C},j)}\right]$.[18]

Finally, let $\widehat{L}^{\mathsf{C},\boldsymbol{\eta}}_{\Pi} \equiv \sum_{j\colon (\mathsf{C},j)\in[(\mathsf{C}^*,j^*)]} \widehat{M}^{\Pi,\boldsymbol{\eta}}_{(\mathsf{C},j)} \cdot \prod_{t=0}^{j-1}\left(1 - \widehat{M}^{\Pi,\boldsymbol{\eta}}_{(\mathsf{C},t)}\right)$.

Lemma 3.8.2. *Let* $\Pi = (\mathsf{A},\mathsf{B})$ *be a protocol with* $\mathsf{val}(\Pi) > 0$*, let* $z \in \mathbb{N}$ *and let* $\boldsymbol{\eta} = \left\{\eta_{(\mathsf{C},j)} \in [0,1]\right\}_{(\mathsf{C},j)\in[(\mathsf{A},z)]}$*. For* $j \in (z)$ *let* $\alpha_j = \widehat{\mu}^{\Pi,\boldsymbol{\eta}}_{(\mathsf{A},j)}$*, and for* $j \in (z-1)$ *let* $\beta_j = \widehat{\mu}^{\Pi,\boldsymbol{\eta}}_{(\mathsf{B},j)}$*. Then*

$$\mathrm{E}_{\left\langle \mathsf{A}^{(k)},\mathsf{B}\right\rangle}\left[\widehat{L}^{\mathsf{A},\boldsymbol{\eta}}_{\Pi}\right] \geq \frac{\sum_{j=0}^{z} \alpha_j \cdot \prod_{t=0}^{j-1}(1-\beta_t)^{k+1}(1-\alpha_t)}{\prod_{i=0}^{k-1}\mathsf{val}(\mathsf{A}^{(i)},\mathsf{B})}$$

for any positive $k \in \mathbb{N}$*.*

The proof of Lemma 3.8.2 is given below, but we first use it for proving Lemma 3.7.1.

Proof of Lemma 3.7.1. Let $\eta_{(\mathsf{C},j)} = 1$ for every $(\mathsf{C},j) \in [(\mathsf{A},z)]$ and let $\boldsymbol{\eta} = \left\{\eta_{(\mathsf{C},j)}\right\}_{(\mathsf{C},j)\in[(\mathsf{A},z)]}$. It follows that $\widehat{L}^{\mathsf{A},\boldsymbol{\eta}}_{\Pi} \equiv L^{\mathsf{A},z}_{\Pi}$. Applying Lemma 3.8.2 yields that

$$\mathrm{E}_{\left\langle \mathsf{A}^{(k)},\mathsf{B}\right\rangle}\left[L^{\mathsf{A},z}_{\Pi}\right] \geq \frac{\sum_{j=0}^{z} \alpha_j \cdot \prod_{t=0}^{j-1}(1-\beta_t)^{k+1}(1-\alpha_t)}{\prod_{i=0}^{k-1}\mathsf{val}(\mathsf{A}^{(i)},\mathsf{B})} \tag{3.13}$$

[18]Note that for $\boldsymbol{\eta} = (1,1,1,\ldots,1)$, Definition 3.8.1 coincides with Definition 3.6.6.

where $\alpha_j = \widehat{\mu}^{\Pi,\boldsymbol{\eta}}_{(\mathsf{A},j)}$ and $\beta_j = \widehat{\mu}^{\Pi,\boldsymbol{\eta}}_{(\mathsf{B},j)}$. Multiplying the j'th summand of the right hand side of Equation (3.13) by $\prod_{t=j}^{z-1}(1-\beta_j)^k \leq 1$ yields that

$$\begin{aligned} \mathrm{E}_{\langle \mathsf{A}^{(k)},\mathsf{B}\rangle}\left[L^{\mathsf{A},z}_{\Pi}\right] &\geq \frac{\sum_{j=0}^{z}\alpha_j \cdot \prod_{t=0}^{j-1}(1-\beta_t)(1-\alpha_t)}{\prod_{i=0}^{k-1}\mathsf{val}(\mathsf{A}^{(i)},\mathsf{B})} \cdot \prod_{t=0}^{z-1}(1-\beta_t)^k \qquad (3.14)\\ &\geq \frac{\sum_{j=0}^{z}\alpha_j \cdot \prod_{t=0}^{j-1}(1-\beta_t)(1-\alpha_t)}{\prod_{i=0}^{k-1}\mathsf{val}(\mathsf{A}^{(i)},\mathsf{B})} \cdot \left(1-\sum_{t=0}^{z-1}\beta_t\right)^k \end{aligned}$$

where the second inequality follows since $\beta_j \geq 0$ and $(1-x)(1-y) \geq 1-(x+y)$ for any $x, y \geq 0$. By Lemma 3.4.2 and the definition of $\boldsymbol{\eta}$ it follows that $\widehat{\mu}^{\Pi,\boldsymbol{\eta}}_{(\mathsf{A},j)} = 1 - \mathsf{OPT}_{\mathsf{B}}\left(\Pi_{(\mathsf{A},j)}\right)$ and $\widehat{\mu}^{\Pi,\boldsymbol{\eta}}_{(\mathsf{B},j)} = 1 - \mathsf{OPT}_{\mathsf{A}}\left(\Pi_{(\mathsf{B},j)}\right)$. Hence, plugin Lemma 3.6.7 into Equation (3.14) yields that

$$\mathrm{E}_{\langle \mathsf{A}^{(k)},\mathsf{B}\rangle}\left[L^{\mathsf{A},z}_{\Pi}\right] \geq \frac{\mathrm{E}_{\langle \Pi\rangle}\left[L^{\mathsf{A},z}_{\Pi}\right]}{\prod_{i=0}^{k-1}\mathsf{val}(\mathsf{A}^{(i)},\mathsf{B})} \cdot \left(1-\sum_{t=0}^{z-1}\beta_t\right)^k \qquad (3.15)$$

Finally, the proof is concluded, since by Lemma 3.6.7 and Fact 2.2.5 it immediately follows that $\mathsf{val}(\mathsf{A}^{(k)},\mathsf{B}) \geq \mathrm{E}_{\langle \mathsf{A}^{(k)},\mathsf{B}\rangle}\left[L^{\mathsf{A},z}_{\Pi}\right]$. □

Proving Lemma 3.8.2

Proof of Lemma 3.8.2. In the following we fix a protocol Π, real vector $\boldsymbol{\eta} = \left\{\eta_{(\mathsf{C},j)}\right\}_{(\mathsf{C},j)\in[(\mathsf{A},z)]}$ and a positive integer k. We also assume for simplicity that $\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{A},z)}$ is not the undefined protocol, i.e., $\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{A},z)} \neq \perp$.[19] The proof is by induction on the round complexity of Π.

Base case. Assume $\mathrm{round}(\Pi) = 0$ and let ℓ be the only node in $\mathcal{T}(\Pi)$. For $j \in (z)$, Definition 3.8.1 yields that $\chi_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{A},j)}}(\ell) = \chi_{\Pi}(\ell) = 1$, where the last equality holds

[19] In case this assumption does not hold, let $z' \in (z-1)$ be the largest index such that $\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{A},z')} \neq \perp$, and let $\boldsymbol{\eta}' = \left\{\eta_{(\mathsf{C},j)}\right\}_{(\mathsf{C},j)\in[(\mathsf{A},z')]}$. It follows Definition 3.4.1 that $\widehat{M}^{\Pi,\boldsymbol{\eta}}_{(\mathsf{A},j)}$ is the zero measure for any $z' < j \leq z$, and thus $\widehat{L}^{\Pi,\boldsymbol{\eta}'}_{\mathsf{A}} \equiv \widehat{L}^{\Pi,\boldsymbol{\eta}}_{\mathsf{A}}$. Moreover, noticing that $\alpha_j = 0$ for any $z' < j \leq z$ suffices for validating the assumption.

since, by assumption, $\mathsf{val}(\Pi) > 0$. It follows Definition 3.4.1 that $M^{\mathsf{A}}_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{A},j)}}(\ell) = 1$ and Definition 3.8.1 that $\widehat{M}^{\Pi,\boldsymbol{\eta}}_{(\mathsf{A},j)}(\ell) = \eta_{(\mathsf{A},j)}$. Hence, it holds that $\alpha_j = \eta_{(\mathsf{A},j)}$. Similarly, for $j \in (z-1)$ it holds that $\widehat{M}^{\Pi,\boldsymbol{\eta}}_{(\mathsf{B},j)}(\ell) = 0$ and thus $\beta_j = 0$. Clearly, $\left(\mathsf{A}^{(k)}, \mathsf{B}\right) = \Pi$ and $\mathsf{val}(\mathsf{A}^{(i)}, \mathsf{B}) = 1$ for every $i \in [k-1]$. We conclude that

$$\begin{aligned}
\mathrm{E}_{\langle \mathsf{A}^{(k)},\mathsf{B}\rangle}\left[\widehat{L}^{\Pi,\boldsymbol{\eta}}_{\mathsf{A}}\right] =& \mathrm{E}_{\langle \Pi\rangle}\left[\widehat{L}^{\Pi,\boldsymbol{\eta}}_{\mathsf{A}}\right] \\
=& \sum_{j=0}^{z} \widehat{M}^{\Pi,\boldsymbol{\eta}}_{(\mathsf{A},j)}(\ell) \cdot \prod_{t=0}^{j-1}\left(1 - \widehat{M}^{\Pi,\boldsymbol{\eta}}_{(\mathsf{A},t)}(\ell)\right) \\
=& \sum_{j=0}^{z} \eta_{(\mathsf{A},j)} \cdot \prod_{t=0}^{j-1}\left(1 - \eta_{(\mathsf{A},t)}\right) \\
=& \sum_{j=0}^{z} \alpha_j \cdot \prod_{t=0}^{j-1}(1-\alpha_t) \\
=& \frac{\sum_{j=0}^{z} \alpha_j \prod_{t=0}^{j-1}(1-\beta_t)^{k+1}(1-\alpha_t)}{\prod_{i=0}^{k-1} \mathsf{val}(\mathsf{A}^{(i)}, \mathsf{B})}.
\end{aligned}$$

Induction step. Assume the lemma holds for m-round protocols and that $\mathrm{round}(\Pi) = m+1$. The proof takes the following steps: (1) defines two real vectors $\boldsymbol{\eta_0}$ and $\boldsymbol{\eta_1}$ such that the restriction of $\widehat{L}^{\Pi,\boldsymbol{\eta}}_{\mathsf{A}}$ to Π_0 and Π_1 is equal to $\widehat{L}^{\Pi_0,\boldsymbol{\eta_0}}_{\mathsf{A}}$ and $\widehat{L}^{\Pi_1,\boldsymbol{\eta_1}}_{\mathsf{A}}$ respectively; (2) Applies the induction hypothesis on the two latter measures; (3) In case A controls $\mathsf{root}(\Pi)$, uses the properties of $\mathsf{A}^{(k)}$ – as put in Claim 3.2.1 – to derive the lemma, whereas in case B controls $\mathsf{root}(\Pi)$, derives the lemma from Lemma 2.5.1.

All claims given in the context of this proof are proven in Section 3.8. We defer handling the case that $e_\Pi(\lambda, b) \in \{0,1\}$ for some $b \in \{0,1\}$ for later and assume for now that $e_\Pi(\lambda,0), e_\Pi(\lambda,1) \in (0,1)$. The real vectors $\boldsymbol{\eta_0}$ and $\boldsymbol{\eta_1}$ are defined as follows.

Definition 3.8.3. *Let* $\boldsymbol{\eta_b} = \left\{\eta^b_{(\mathsf{C},j)}\right\}_{(\mathsf{C},j)\in[(\mathsf{A},z)]}$, *where for* $(\mathsf{C},j) \in [(\mathsf{A},z)]$ *and* $b \in \{0,1\}$, *let*

$$\eta^b_{(\mathsf{C},j)} = \begin{cases} 0 & e_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)}}(\lambda,b) = 0; \\ \eta_{(\mathsf{C},j)} & e_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)}}(\lambda,b) = 1; \\ \eta_{(\mathsf{C},j)} & e_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)}}(\lambda,b) \notin \{0,1\} \wedge (\mathsf{C} \textit{ controls } \mathsf{root}(\Pi) \vee \mathsf{Smaller}_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)}}(b)); \\ \frac{\xi^{1-b}_{(\mathsf{C},j)}}{\xi^{b}_{(\mathsf{C},j)}} \cdot \eta_{(\mathsf{C},j)} & \textit{otherwise;} \end{cases},$$

where $\xi^b_{(\mathsf{C},j)} = \mathrm{E}_{\left\langle\left(\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)}\right)_b\right\rangle}\left[M^{\mathsf{C}}_{\left(\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)}\right)_b}\right]$ *and* $\mathsf{Smaller}_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)}}(b) = 1$ *if* $\xi^b_{(\mathsf{C},j)} \leq \xi^{1-b}_{(\mathsf{C},j)}$.[20]

Given the real vector $\boldsymbol{\eta_b}$, consider the dominated submeasure sequence $\boldsymbol{\eta_b}$ induces on the sub-protocol Π_b. At a first look, the relation of this submeasure sequence to the dominated submeasure sequence $\boldsymbol{\eta}$ induces on Π, is unclear; yet, we manage to prove the following key observation.

Claim 3.8.4. *It holds that* $\widehat{L}^{\Pi_b,\boldsymbol{\eta}_b}_{\mathsf{A}} \equiv \left(\widehat{L}^{\Pi,\boldsymbol{\eta}}_{\mathsf{A}}\right)_b$ *for both* $b \in \{0,1\}$.

Namely, taking $(\mathsf{A},z,\boldsymbol{\eta_b})$-D$MS\,(\Pi_b)$ – the dominated submeasures defined with respect to Π_b and $\boldsymbol{\eta_b}$ – and combining it to the measure $\widehat{L}^{\Pi_b,\boldsymbol{\eta_b}}_{\mathsf{A}}$, results in the same measure as taking $(\mathsf{A},z,\boldsymbol{\eta})$-D$MS\,(\Pi)$ – the dominated submeasures defined with respect to Π and $\boldsymbol{\eta}$ – combine it to the measure $\widehat{L}^{\Pi,\boldsymbol{\eta}}_{\mathsf{A}}$ and restrict the latter to Π_b.

Given the above fact, we can use our induction hypothesis on the sub-protocols Π_0 and Π_1 with respect to the real vectors $\boldsymbol{\eta_0}$ and $\boldsymbol{\eta_1}$, respectively. For $b \in \{0,1\}$ and $j \in (z)$, let $\alpha^b_j := \mu^{\Pi_b,\boldsymbol{\eta_b}}_{(\mathsf{A},j)}$ $(:= \mathrm{E}_{\left\langle\left(\widehat{\Pi}_b\right)^{\boldsymbol{\eta_b}}_{(\mathsf{A},j)}\right\rangle}\left[\widehat{M}^{\Pi_b,\boldsymbol{\eta_b}}_{(\mathsf{A},j)}\right])$, and for $j \in (z-1)$ let

[20]Note that the definition of η^b follows the same lines of the definition of the dominated measure (given in Definition 3.4.1).

$\beta_j^b := \mu_{(\mathsf{B},j)}^{\Pi_b,\boldsymbol{\eta_b}}$. Assuming that $\mathsf{val}(\Pi_1) > 0$, then

$$\mathrm{E}_{\left\langle \left(\mathsf{A}^{(k)},\mathsf{B}\right)_1 \right\rangle}\left[\left(\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}}\right)_1\right] = \mathrm{E}_{\left\langle \mathsf{A}_{\Pi_1}^{(k)},\mathsf{B}_{\Pi_1} \right\rangle}\left[\widehat{L}_{\mathsf{A}}^{\Pi_1,\boldsymbol{\eta_1}}\right] \geq \frac{\sum_{j=0}^{z} \alpha_j^1 \prod_{t=0}^{j-1}(1-\beta_t^1)^{k+1}(1-\alpha_t^1)}{\prod_{i=0}^{k-1} \mathsf{val}\left(\left(\mathsf{A}^{(i)},\mathsf{B}\right)_1\right)} \tag{3.16}$$

where the equality holds by Proposition 3.2.2 and Claim 3.8.4, and the inequality by the induction hypothesis. Similarly, if $\mathsf{val}(\Pi_0) > 1$, then

$$\mathrm{E}_{\left\langle \left(\mathsf{A}^{(k)},\mathsf{B}\right)_0 \right\rangle}\left[\left(\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}}\right)_0\right] = \mathrm{E}_{\left\langle \mathsf{A}_{\Pi_0}^{(k)},\mathsf{B}_{\Pi_0} \right\rangle}\left[\widehat{L}_{\mathsf{A}}^{\Pi_0,\boldsymbol{\eta_0}}\right] \geq \frac{\sum_{j=0}^{z} \alpha_j^0 \prod_{t=0}^{j-1}(1-\beta_t^0)^{k+1}(1-\alpha_t^0)}{\prod_{i=0}^{k-1} \mathsf{val}\left(\left(\mathsf{A}^{(i)},\mathsf{B}\right)_0\right)} \tag{3.17}$$

In the following we use the fact that at least the dominated submeasure sequence of one of sub-protocols is at least as long as the submeasure sequence of the protocol itself. Specifically, we show the following.

Definition 3.8.5. *For $b \in \{0,1\}$ let $z^b = \min\left\{\left\{j \in (z) \colon \alpha_j^b = 1 \vee \beta_j^b = 1\right\} \cup \{z\}\right\}$.*

Assuming without loss of generality (and throughout the proof of the lemma) that $z^1 \leq z^0$, we have the following claim (proved in Section 3.8).

Claim 3.8.6. *Assume that $z^1 \leq z^0$, then $z^0 = z$.*

We are now ready to prove the lemma by separately considering which party controls the root of Π.

A controls $\mathsf{root}(\Pi)$ and $\mathsf{val}(\Pi_0), \mathsf{val}(\Pi_1) > 0$. Under these assumptions, we can apply the induction hypothesis on both subtrees (namely, to use Equa-

tions (3.16) and (3.17)). Let $p = e_{\Pi}(\lambda, 0)$. Compute

$$\begin{aligned}
&\mathrm{E}_{\langle \mathsf{A}^{(k)},\mathsf{B}\rangle}\left[\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}}\right] && (3.18)\\
&= e_{\left(\mathsf{A}^{(k)},\mathsf{B}\right)}(\lambda,0)\cdot \mathrm{E}_{\langle \left(\mathsf{A}^{(k)},\mathsf{B}\right)_0\rangle}\left[\left(\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}}\right)_0\right] + e_{\left(\mathsf{A}^{(k)},\mathsf{B}\right)}(\lambda,1)\cdot \mathrm{E}_{\langle \left(\mathsf{A}^{(k)},\mathsf{B}\right)_1\rangle}\left[\left(\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}}\right)_1\right]\\
&= p\cdot\frac{\prod_{i=0}^{k-1}\mathsf{val}\left(\left(\mathsf{A}^{(i)},\mathsf{B}\right)_0\right)}{\prod_{i=0}^{k-1}\mathsf{val}\left(\mathsf{A}^{(i)},\mathsf{B}\right)}\cdot \mathrm{E}_{\langle \left(\mathsf{A}^{(k)},\mathsf{B}\right)_0\rangle}\left[\left(\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}}\right)_0\right]\\
&\quad + (1-p)\cdot\frac{\prod_{i=0}^{k-1}\mathsf{val}\left(\left(\mathsf{A}^{(i)},\mathsf{B}\right)_1\right)}{\prod_{i=0}^{k-1}\mathsf{val}(\mathsf{A}^{(i)},\mathsf{B})}\cdot \mathrm{E}_{\langle \left(\mathsf{A}^{(k)},\mathsf{B}\right)_1\rangle}\left[\left(\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}}\right)_1\right]\\
&\geq p\cdot\frac{\prod_{i=0}^{k-1}\mathsf{val}\left(\left(\mathsf{A}^{(i)},\mathsf{B}\right)_0\right)}{\prod_{i=0}^{k-1}\mathsf{val}\left(\mathsf{A}^{(i)},\mathsf{B}\right)}\cdot\frac{\sum_{j=0}^{z}\alpha_j^0\prod_{t=0}^{j-1}(1-\beta_t^0)^{k+1}(1-\alpha_t^0)}{\prod_{i=0}^{k-1}\mathsf{val}\left(\left(\mathsf{A}^{(i)},\mathsf{B}\right)_0\right)}\\
&\quad + (1-p)\cdot\frac{\prod_{i=0}^{k-1}\mathsf{val}\left(\left(\mathsf{A}^{(i)},\mathsf{B}\right)_1\right)}{\prod_{i=0}^{k-1}\mathsf{val}(\mathsf{A}^{(i)},\mathsf{B})}\cdot\frac{\sum_{j=0}^{z}\alpha_j^1\prod_{t=0}^{j-1}(1-\beta_t^1)^{i+1}(1-\alpha_t^1)}{\prod_{i=0}^{k-1}\mathsf{val}\left(\left(\mathsf{A}^{(i)},\mathsf{B}\right)_1\right)}\\
&= \frac{p\cdot\left(\sum_{j=0}^{z}\alpha_j^0\prod_{t=0}^{j-1}(1-\beta_t^0)^{k+1}(1-\alpha_t^0)\right)}{\prod_{i=0}^{k-1}\mathsf{val}(\mathsf{A}^{(i)},\mathsf{B})} && (3.19)\\
&+ \frac{(1-p)\cdot\left(\sum_{j=0}^{z}\alpha_j^1\prod_{t=0}^{j-1}(1-\beta_t^1)^{k+1}(1-\alpha_t^1)\right)}{\prod_{i=0}^{k-1}\mathsf{val}(\mathsf{A}^{(i)},\mathsf{B})}
\end{aligned}$$

where the second equality follows Claim 3.2.1 and the third inequality follows Equations (3.16) and (3.17).

Our next step is to establish a connection between the above $\left\{\alpha_j^0,\alpha_j^1\right\}_{j\in(z)}$ and $\left\{\beta_j^0,\beta_j^1\right\}_{j\in(z-1)}$ to $\{\alpha_j\}_{j\in(z)}$ and $\{\beta_j\}_{j\in(z-1)}$ (appearing in the lemma's statement). We prove the following claims.

Claim 3.8.7. *In case* A *controls* $\mathsf{root}(\Pi)$*, it holds that* $\beta_j^0 = \beta_j$ *for every* $j \in (z-1)$ *and* $\beta_j^1 = \beta_j$ *for every* $j \in (z^1-1)$*.*

Intuitively (Section 3.8 for the formal proof), the fact that $\beta_j^0 = \beta_j^1 = \beta_j$ for $j \in (z^1-1)$ is a direct implication of Proposition 3.4.4, whereas the fact that

$\beta_j^0 = \beta_j$ for every $z^1 \leq j \leq z-1$ is of technical nature, and formally proved in Section 3.8.

Claim 3.8.8. *In case* A *controls* $\mathsf{root}(\Pi)$ *and* $z^1 < z$*, it holds that* $\alpha_{z^1}^1 = 1$.

Intuitively, (again, Section 3.8 for the formal proof), by Claim 3.8.7 it follows that as long as an undefined protocol was not reached in one of the sub-protocols, then $\beta_j^0 = \beta_j^1 = \beta_j$. Assuming that $z^1 < z$ and $\beta_{z^1}^1 = 1$, it would have followed that $\beta_{z^1} = 1$, and an undefined protocol is reached in the original protocol before z, a contradiction to our assumption.

Claims 3.8.7 and 3.8.8 and Equation (3.18) yield that

$$\mathrm{E}_{\langle \mathsf{A}^{(k)},\mathsf{B}\rangle}\left[\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}}\right] \geq \frac{\sum_{j=0}^{z}\prod_{t=0}^{j-1}(1-\beta_t)^{k+1}\Big(p\cdot\alpha_j^0\prod_{t=0}^{j-1}(1-\alpha_t^0)\Big)}{\prod_{i=0}^{k-1}\mathsf{val}(\mathsf{A}^{(i)},\mathsf{B})} \tag{3.20}$$

$$+\frac{\sum_{j=0}^{z}\prod_{t=0}^{j-1}(1-\beta_t)^{k+1}\Big((1-p)\cdot\alpha_j^1\cdot\prod_{t=0}^{j-1}(1-\alpha_t^1)\Big)}{\prod_{i=0}^{k-1}\mathsf{val}(\mathsf{A}^{(i)},\mathsf{B})} \tag{3.21}$$

The proof of this case is concluded by plugin the next claim into Equation (3.20).

Claim 3.8.9. *In case* A *controls* $\mathsf{root}(\Pi)$ *it holds that*

$$\alpha_j\cdot\prod_{t=0}^{j-1}(1-\alpha_t) = p\cdot\alpha_j^0\cdot\prod_{t=0}^{j-1}(1-\alpha_t^0) + (1-p)\cdot\alpha_j^1\cdot\prod_{t=1}^{j-1}(1-\alpha_t^1)$$

for any $j \in (z)$.

Claim 3.8.9 is proved in Section 3.8, but informally it holds since the probability of visiting the left-hand [resp., right-hand] sub-protocol in the conditional protocol $\widehat{\Pi}_{(\mathsf{A},j)}^{\boldsymbol{\eta}}$ (in which α_j is defined) is $p\cdot\prod_{t=0}^{j-1}(1-\alpha_t^0)/\prod_{t=0}^{j-1}(1-\alpha_t)$ [resp.,

$(1-p)\cdot\prod_{t=0}^{j-1}(1-\alpha_t^1)/\prod_{t=0}^{j-1}(1-\alpha_t)]$. Since α_j is defined to be the expected value of some measure in the above conditional protocol, its value is a linear combination of α_j^0 and α_j^1, with the coefficient being the above probabilities.

A controls $\mathsf{root}(\Pi)$ and $\mathsf{val}(\Pi_0) > \mathsf{val}(\Pi_1) = 0$. Under these assumptions, we can still use the induction hypothesis for the left-hand sub-protocol Π_0, where for right-hand sub-protocol Π_1, we argue the following.

Claim 3.8.10. *In case* $\mathsf{val}(\Pi_1) = 0$*, it holds that* $\left(\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}}\right)_1 \equiv 0$.[21]

Intuitively, Claim 3.8.10 holds since according to Claim 3.8.4 we can simply argue that $\widehat{L}_{\mathsf{A}}^{\Pi_1,\boldsymbol{\eta_1}}$ is the zero measure, and this holds since the latter measure is a combination of A-dominated measures, all of which are the zero measure in a zero-value protocol.

Using Claim 3.8.10, and similar to Equation (3.18), we deduce

$$\begin{aligned}
&\mathrm{E}_{\langle \mathsf{A}^{(k)},\mathsf{B}\rangle}\left[\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}}\right] \qquad (3.22)\\
&= e_{\left(\mathsf{A}^{(k)},\mathsf{B}\right)}(\lambda,0)\cdot \mathrm{E}_{\langle (\mathsf{A}^{(k)},\mathsf{B})_0\rangle}\left[\left(\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}}\right)_0\right] + e_{\left(\mathsf{A}^{(k)},\mathsf{B}\right)}(\lambda,1)\cdot \mathrm{E}_{\langle (\mathsf{A}^{(k)},\mathsf{B})_1\rangle}\left[\left(\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}}\right)_1\right]\\
&\geq p\cdot\frac{\prod_{i=0}^{k-1}\mathsf{val}\left(\left(\mathsf{A}^{(i)},\mathsf{B}\right)_0\right)}{\prod_{i=0}^{k-1}\mathsf{val}\left(\mathsf{A}^{(i)},\mathsf{B}\right)}\cdot\frac{\sum_{j=0}^{z}\alpha_j^0\prod_{t=0}^{j-1}(1-\beta_t^0)^{k+1}(1-\alpha_t^0)}{\prod_{i=0}^{k-1}\mathsf{val}\left((\mathsf{A}^{(i)},\mathsf{B})_0\right)}\\
&= \frac{p\cdot\left(\sum_{j=0}^{z}\alpha_j^0\prod_{t=0}^{j-1}(1-\beta_t^0)^{k+1}(1-\alpha_t^0)\right)}{\prod_{i=0}^{k-1}\mathsf{val}(\mathsf{A}^{(i)},\mathsf{B})}.
\end{aligned}$$

Using similar argument to that of Equation (3.20), combining Claim 3.8.7 and Equation (3.22) yields that

$$\mathrm{E}_{\langle \mathsf{A}^{(k)},\mathsf{B}\rangle}\left[\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}}\right] \geq \frac{\sum_{j=0}^{z}\prod_{t=0}^{j-1}(1-\beta_t)^{k+1}\left[p\cdot\alpha_j^0\prod_{t=0}^{j-1}(1-\alpha_t^0)\right]}{\prod_{i=0}^{k-1}\mathsf{val}(\mathsf{A}^{(i)},\mathsf{B})} \qquad (3.23)$$

[21] I.e., $\left(\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}}\right)_1$ is the zero measure.

The proof of this case is concluded by plugin the next claim (proved in Section 3.8) into Claim 3.8.9, and plugin the result into Equation (3.23).

Claim 3.8.11. *In case* $\mathsf{val}(\Pi_1) = 0$*, it holds that* $\alpha_j^1 = 0$ *for every* $j \in (z)$*.*

A controls $\mathsf{root}(\Pi)$ and $\mathsf{val}(\Pi_1) > \mathsf{val}(\Pi_0) = 0$. The proof of the lemma under these assumptions is analogous to the previous case.

We have concluded the proof for cases in which A controls $\mathsf{root}(\Pi)$, and now proceed to prove the cases in which B controls $\mathsf{root}(\Pi)$. Roughly speaking, A and B switched roles, and claims true before regarding β_j are now true for α_j, and viceversa. Additional significant difference to the above cases is that the probabilities of visiting the left- and right-hand side sub-protocols does not change when the biassed-continuation attack plays the role of A (namely, they remain p and $1-p$ respectively). Instead, we derive the lemma by using a convex type argument stated in Lemma 2.5.1.

B controls $\mathsf{root}(\Pi)$ and $\mathsf{val}(\Pi_0), \mathsf{val}(\Pi_1) > 0$. In this case Equations (3.16) and (3.17) hold.

Compute,

$$\begin{aligned}
&\mathrm{E}_{\langle \mathsf{A}^{(k)}, \mathsf{B} \rangle} \left[\widehat{L}_{\mathsf{A}}^{\Pi, \boldsymbol{\eta}} \right] && (3.24)\\
&= p \cdot \mathrm{E}_{\langle (\mathsf{A}^{(k)}, \mathsf{B})_0 \rangle} \left[\left(\widehat{L}_{\mathsf{A}}^{\Pi, \boldsymbol{\eta}} \right)_0 \right] + (1-p) \cdot \mathrm{E}_{\langle (\mathsf{A}^{(k)}, \mathsf{B})_1 \rangle} \left[\left(\widehat{L}_{\mathsf{A}}^{\Pi, \boldsymbol{\eta}} \right)_1 \right] \\
&\geq p \cdot \frac{\sum_{j=0}^{z} \alpha_j^0 \prod_{t=0}^{j-1} (1-\beta_t^0)^{k+1} (1-\alpha_t^0)}{\prod_{i=0}^{k-1} \mathsf{val}\left((\mathsf{A}^{(i)}, \mathsf{B})_0 \right)} && (3.25)\\
&+ (1-p) \cdot \frac{\sum_{j=0}^{z} \alpha_j^1 \prod_{t=0}^{j-1} (1-\beta_t^1)^{k+1} (1-\alpha_t^1)}{\prod_{i=0}^{k-1} \mathsf{val}\left((\mathsf{A}^{(i)}, \mathsf{B})_1 \right)},
\end{aligned}$$

where the inequality follows Equations (3.16) and (3.17). In case B controls $\mathsf{root}(\Pi)$ we can prove the next claims (proved in Section 3.8), analogous to Claims 3.8.7 and 3.8.8.

Claim 3.8.12. *In case* B *controls* $\mathsf{root}(\Pi)$*, it holds that* $\alpha_j^0 = \alpha_j$ *for every* $j \in (z)$ *and that* $\alpha_j^1 = \alpha_j$ *for every* $j \in (z^1)$*.*

Claim 3.8.13. *In case* B *controls* $\mathsf{root}(\Pi)$ *and* $z^1 < z$*, it holds that* $\beta_{z^1}^1 = 1$*.*

Claim 3.8.12 and Equation (3.24) yield that

$$\begin{aligned} &\mathrm{E}_{\langle \mathsf{A}^{(k)},\mathsf{B}\rangle}\left[\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}}\right] \qquad (3.26)\\ &\geq \sum_{j=0}^{z} \alpha_j \prod_{t=0}^{j-1}(1-\alpha_t)\left(p\cdot\frac{\prod_{t=0}^{j-1}(1-\beta_t^0)^{k+1}}{\prod_{i=0}^{k-1}\mathsf{val}\left((\mathsf{A}^{(i)},\mathsf{B})_0\right)} + (1-p)\cdot\frac{\prod_{t=0}^{j-1}(1-\beta_t^1)^{k+1}}{\prod_{i=0}^{k-1}\mathsf{val}\left((\mathsf{A}^{(i)},\mathsf{B})_1\right)}\right) \end{aligned}$$

Applying the convex type inequality given in Lemma 2.5.1 for each summand in the right-hand side of Equation (3.26) with respect to $x = \prod_{t=0}^{j-1}(1-\beta_t^0)$, $y = \prod_{t=0}^{j-1}(1-\beta_t^1)$, $a_i = \mathsf{val}(\mathsf{A}^{(i-1)},\mathsf{B}_0)$, $b_i = \mathsf{val}(\mathsf{A}^{(i-1)},\mathsf{B}_1)$, $p_0 = p$ and $p_1 = 1-p$, and plugin Equation (3.26) yields that

$$\mathrm{E}_{\langle \mathsf{A}^{(k)},\mathsf{B}\rangle}\left[\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}}\right] \qquad (3.27)$$

$$\geq \frac{\sum_{j=0}^{z}\alpha_j\prod_{t=0}^{j-1}(1-\alpha_t)\left(p\cdot\prod_{t=0}^{j-1}(1-\beta_t^0)+(1-p)\cdot\prod_{t=0}^{j-1}(1-\beta_t^1)\right)^{k+1}}{\prod_{i=0}^{k-1}\left(p\cdot\mathsf{val}\left((\mathsf{A}^{(i)},\mathsf{B})_0\right)+(1-p)\cdot\mathsf{val}\left((\mathsf{A}^{(i)},\mathsf{B})_1\right)\right)} \qquad (3.28)$$

We conclude the proof of this case by observing that for every $i \in (k-1)$ it holds that $\mathsf{val}\left(\mathsf{A}^{(i)},\mathsf{B}\right) = p\cdot\mathsf{val}\left(\left(\mathsf{A}^{(i)},\mathsf{B}\right)_0\right) + (1-p)\cdot\mathsf{val}\left(\left(\mathsf{A}^{(i)},\mathsf{B}\right)_1\right)$, and using the next claim (proved in Section 3.8), analogous to Claim 3.8.9.

Claim 3.8.14. *In case* B *controls* $\mathsf{root}(\Pi)$*, it holds that*

$$\prod_{t=0}^{j-1}(1-\beta_t) = p \cdot \prod_{t=0}^{j-1}(1-\beta_t^0) + (1-p) \cdot \prod_{t=0}^{j-1}(1-\beta_t^1)$$

B controls $\mathsf{root}(\Pi)$ and $\mathsf{val}(\Pi_0) > \mathsf{val}(\Pi_1) = 0$. In this case, Claims 3.8.7 and 3.8.12 yield that $\alpha_j = 0$ for any $j \in (z^1)$. Hence, it suffices to prove that

$$\mathrm{E}_{\langle \mathsf{A}^{(k)},\mathsf{B}\rangle}\left[\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}}\right] \geq \frac{\sum_{j=z^1+1}^{z} \alpha_j \prod_{t=0}^{j-1}(1-\beta_t)^{k+1}(1-\alpha_t)}{\prod_{i=0}^{k-1} \mathsf{val}(\mathsf{A}^{(i)},\mathsf{B})} \tag{3.29}$$

Thus, the proof immediately follows in case $z^1 = z$, and in the following we assume that $z^1 < z$.

Similar to Equation (3.24), compute

$$\mathrm{E}_{\langle \mathsf{A}^{(k)},\mathsf{B}\rangle}\left[\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}}\right] = p \cdot \mathrm{E}_{\langle (\mathsf{A}^{(k)},\mathsf{B})_0\rangle}\left[\left(\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}}\right)_0\right] + (1-p) \cdot \mathrm{E}_{\langle (\mathsf{A}^{(k)},\mathsf{B})_1\rangle}\left[\left(\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}}\right)_1\right] \tag{3.30}$$

$$\geq p \cdot \frac{\sum_{j=0}^{z} \alpha_j^0 \prod_{t=0}^{j-1}(1-\beta_t^0)^{k+1}(1-\alpha_t^0)}{\prod_{i=0}^{k-1} \mathsf{val}\left((\mathsf{A}^{(i)},\mathsf{B})_0\right)},$$

where the inequality follows Equation (3.17) and Claim 3.8.10. Claim 3.8.12 now yields

$$\mathrm{E}_{\langle \mathsf{A}^{(k)},\mathsf{B}\rangle}\left[\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}}\right] \geq \sum_{j=0}^{z} \alpha_j \prod_{t=0}^{j-1}(1-\alpha_t) \cdot \frac{p \cdot \prod_{t=0}^{j-1}(1-\beta_t^0)^{k+1}}{\prod_{i=0}^{k-1} \mathsf{val}\left((\mathsf{A}^{(i)},\mathsf{B})_0\right)} \tag{3.31}$$

where Claim 3.8.12 yields

$$\mathrm{E}_{\langle \mathsf{A}^{(k)},\mathsf{B}\rangle}\left[\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}}\right] \geq \sum_{j=z^1+1}^{z} \alpha_j \prod_{t=0}^{j-1}(1-\alpha_t) \cdot \frac{p \cdot \prod_{t=0}^{j-1}(1-\beta_t^0)^{k+1}}{\prod_{i=0}^{k-1} \mathsf{val}\left((\mathsf{A}^{(i)},\mathsf{B})_0\right)} \tag{3.32}$$

Multiplying both the numerator and the denominator for every summand of Equation (3.32) with p^k yields

$$\mathrm{E}_{\langle \mathsf{A}^{(k)},\mathsf{B}\rangle}\left[\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}}\right] \geq \sum_{j=z^1+1}^{z} \alpha_j \prod_{t=0}^{j-1}(1-\alpha_t) \cdot \frac{\left(p \cdot \prod_{t=0}^{j-1}(1-\beta_t^0)\right)^{k+1}}{\prod_{i=0}^{k-1} p \cdot \mathsf{val}\left((\mathsf{A}^{(i)},\mathsf{B})_0\right)} \tag{3.33}$$

Equation (3.29), and hence the proof of this case, is derived by observing that $\mathsf{val}(\mathsf{A}^{(i)}, \mathsf{B}) = p \cdot \mathsf{val}\left(\left(\mathsf{A}^{(i)}, \mathsf{B}\right)_0\right)$ for every $i \in (k-1)$,[22] and plugin Claim 3.8.13 combined with Claim 3.8.14 into Equation (3.33).

B controls $\mathsf{root}(\Pi)$ and $\mathsf{val}(\Pi_1) > \mathsf{val}(\Pi_0) = 0$. Analogous to Claim 3.8.11, it holds that $\alpha_j^0 = 0$ for every $j \in (z)$. Claim 3.8.12 yields that $\alpha_j = 0$ for every $j \in (z)$. The proof of this case trivially follows since

$$\frac{\sum_{j=0}^{z} \alpha_j \prod_{t=0}^{j-1}(1-\beta_t)^{k+1}(1-\alpha_t)}{\prod_{i=0}^{k-1} \mathsf{val}(\mathsf{A}^{(i)}, \mathsf{B})} = 0.$$

The above case analysis concludes the proof of the lemma when assuming that $e_{\Pi}(\lambda, b) \notin \{0,1\}$ for both $b \in \{0,1\}$. Assume that $e_{\Pi}(\lambda, b) = 1$ for some $b \in \{0,1\}$. Since, by assumption, $\mathsf{val}(\Pi) > 0$, it follows that $\mathsf{val}(\Pi_b) > 0$. Moreover, the definition of conditional protocol (Definition 3.6.1) yields that $e_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)}}(\lambda, b) = 1$ and $e_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)}}(\lambda, 1-b) = 0$ for any $(\mathsf{C}, j) \in [(\mathsf{A}, z)]$ (regardless of which party controls $\mathsf{root}(\Pi)$). By defining $\boldsymbol{\eta}_{\mathbf{b}} = \boldsymbol{\eta}$, the definition of the dominated measure (Definition 3.4.1) yields that $\alpha_j = \alpha_j^b$ for every $j \in (z)$ and that $\beta_j = \beta_j^b$ for every $j \in (z-1)$. The proof of this case immediately follows from the induction hypothesis on Π_b. □

Missing Proofs

This section is dedicated to proving deferred statements used during the proof of Lemma 3.8.2. The context in which the following claims are proved is defined according to the proof of the lemma. Specifically, we assume a fixed protocol Π, fixed real vector $\boldsymbol{\eta} = \left(\eta_{(\mathsf{A},0)}, \eta_{(\mathsf{B},0)}, \ldots, \eta_{(\mathsf{B},z-1)}, \eta_{(\mathsf{A},z)}\right)$ and a fixed positive integer

[22] Recall that in case $\mathsf{val}\left(\mathsf{A}, \mathsf{B}\right) = 0$, then $\mathsf{val}\left(\mathsf{A}^{(i)}, \mathsf{B}\right) = 0$ for every $i \in \mathbb{N}$.

k. We also assume that $\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{A},z)} \neq \perp$, $z^1 \leq z^0$ and $e_\Pi(\lambda, b) \in (0,1)$ for both $b \in \{0,1\}$. Recall that we defined two real vectors $\boldsymbol{\eta_0}$ and $\boldsymbol{\eta_1}$ (Definition 3.8.3), and for $b \in \{0,1\}$ we defined $\alpha^b_j := \mu^{\Pi_b,\boldsymbol{\eta_b}}_{(\mathsf{A},j)}$ $(:= \mathrm{E}_{\left\langle (\widehat{\Pi_b})^{\boldsymbol{\eta_b}}_{(\mathsf{A},j)} \right\rangle}\left[\widehat{M}^{\Pi_b,\boldsymbol{\eta_b}}_{(\mathsf{A},j)}\right])$ for $j \in (z)$, and $\beta^b_j := \mu^{\Pi_b,\boldsymbol{\eta_b}}_{(\mathsf{B},j)}$, for $j \in (z-1)$.

We begin by showing the next fact, underlying many of the claims to follow.

Proposition 3.8.15. *For $b \in \{0,1\}$ and $(\mathsf{C},j) \in [(\mathsf{A},z)]$, it holds that*

1. $\left(\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)}\right)_b = \left(\widehat{\Pi_b}\right)^{\boldsymbol{\eta_b}}_{(\mathsf{C},j)}$*; and*

2. $\left(\widehat{M}^{\Pi,\boldsymbol{\eta}}_{(\mathsf{C},j)}\right)_b \equiv \widehat{M}^{\Pi_b,\boldsymbol{\eta_b}}_{(\mathsf{C},j)}$.

Namely, the restriction of $\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)}$ (the (C,j)'th conditional protocol with respect to Π and $\boldsymbol{\eta}$) to its b'th subtree, is equal to the (C,j)'th conditional protocol defined with respect to Π_b (b'th subtree of Π) and $\boldsymbol{\eta_b}$. Moreover, the result of multiplying the C-dominated measure of $\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)}$ by $\eta_{(\mathsf{C},j)}$, and then restricting it to the subtree $\left(\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)}\right)_b$, is equivalent to multiplying the C-dominated measure of $\left(\widehat{\Pi_b}\right)^{\boldsymbol{\eta_b}}_{(\mathsf{C},j)}$ by $\eta^b_{(\mathsf{C},j)}$.[23]

Proof of Proposition 3.8.15. The proof is by induction on the ordered pairs $[(\mathsf{A},z)]$.

Base case. Recall that the first pair of $[(\mathsf{A},z)]$ is $(\mathsf{A},0)$. Definition 3.8.1 yields that $\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{A},0)} = \Pi$ and that $\left(\widehat{\Pi_b}\right)^{\boldsymbol{\eta_b}}_{(\mathsf{A},0)} = \Pi_b$, yielding that Item 1 holds for $(\mathsf{A},0)$. Where by Definition 3.4.1 and the assumption that $e_\Pi(\lambda,b) \in (0,1)$ for both $b \in \{0,1\}$, it

[23]Note that Item 1 is not immediate. Protocol $\left(\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)}\right)_b$ is a restriction of a protocol defined on the root of the Π, whereas $\left(\widehat{\Pi_b}\right)^{\boldsymbol{\eta_b}}_{(\mathsf{C},j)}$ is a protocol define on the root of Π_b.

holds that

$$\left(\widehat{M}^{\Pi,\boldsymbol{\eta}}_{(\mathsf{A},0)}\right)_b \equiv \left(\eta_{(\mathsf{A},0)} \cdot M^{\mathsf{A}}_{\Pi}\right)_b \equiv \begin{cases} \eta_{(\mathsf{A},0)} \cdot M^{\mathsf{A}}_{\Pi_b} & \mathsf{A} \text{ controls } \mathsf{root}(\Pi) \vee \mathsf{Smaller}_{\Pi}(b)\,; \\ \eta_{(\mathsf{A},0)} \cdot \frac{\xi^{1-b}_{(\mathsf{A},0)}}{\xi^{b}_{(\mathsf{A},0)}} \cdot M^{\mathsf{A}}_{\Pi_b} & \text{otherwise,} \end{cases}$$

and the proof that Item 2 holds for $(\mathsf{A}, 0)$ follows by Definition 3.8.3.

Induction step. Fix $(\mathsf{C}, j) \in [(\mathsf{A}, z)]$ and assume the claim holds for $\mathsf{pred}(\mathsf{C}, j)$. Using the induction hypothesis we first prove Item 1 for (C, j). Next, using the fact that Item 1 holds for (C, j), we prove Item 2.

Proving Item 1. By Definition 3.8.1, it holds that

$$\begin{aligned} \left(\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)}\right)_b &= \left(\widehat{\Pi}^{\boldsymbol{\eta}}_{\mathsf{pred}(\mathsf{C},j)} | \neg \left(\widehat{M}^{\Pi,\boldsymbol{\eta}}_{\mathsf{pred}(\mathsf{C},j)}\right)\right)_b \\ &= \left(\widehat{\Pi}^{\boldsymbol{\eta}}_{\mathsf{pred}(\mathsf{C},j)}\right)_b | \neg \left(\widehat{M}^{\Pi,\boldsymbol{\eta}}_{\mathsf{pred}(\mathsf{C},j)}\right)_b \\ &= \left(\widehat{\Pi_b}\right)^{\boldsymbol{\eta_b}}_{\mathsf{pred}(\mathsf{C},j)} | \neg \left(\widehat{M}^{\Pi_b,\boldsymbol{\eta_b}}_{\mathsf{pred}(\mathsf{C},j)}\right) \\ &= \left(\widehat{\Pi_b}\right)^{\boldsymbol{\eta_b}}_{(\mathsf{C},j)}, \end{aligned}$$

where the third equality follows from the induction hypothesis.

Proving Item 2. Similarly to the base case, Definition 3.4.1 yields that

$$\left(\widehat{M}^{\Pi,\boldsymbol{\eta}}_{(\mathsf{C},j)}\right)_b \equiv \begin{cases} 0 & e_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)}}(\lambda, b) = 0; \\ \eta_{(\mathsf{C},j)} \cdot M^{\mathsf{C}}_{\left(\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)}\right)_b} & e_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)}}(\lambda, b) = 1; \\ \eta_{(\mathsf{C},j)} \cdot M^{\mathsf{C}}_{\left(\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)}\right)_b} & e_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)}}(\lambda, b) \notin \{0,1\} \wedge \\ & \left(\mathsf{C} \text{ controls } \mathsf{root}(\Pi) \vee \mathsf{Smaller}_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)}}(b)\right); \\ \eta_{(\mathsf{C},j)} \cdot \frac{\xi^{1-b}_{(\mathsf{C},j)}}{\xi^{b}_{(\mathsf{C},j)}} \cdot M^{\mathsf{C}}_{\left(\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)}\right)_b} & \text{otherwise,} \end{cases}$$

and the proof follows by Item 1 and Definition 3.8.3.

□

Recall, see the proof of Lemma 3.8.2, that the reals α_j^b and β_j^b were defined to be the expected values of the (A, j)'th and (B, j)'th dominated measures in the sequence $(\mathsf{A}, z, \boldsymbol{\eta}_{\mathbf{b}})$-D$MS\left(\Pi_b\right)$, respectively. Following Proposition 3.8.15, we can view α_j^b and β_j^b in the context $(\mathsf{A}, z, \boldsymbol{\eta})$-D$MS\left(\Pi\right)$.

Proposition 3.8.16. *For both $b \in \{0,1\}$, it holds that*

1. $\alpha_j^b = \mathrm{E}_{\left\langle \left(\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{A},j)}\right)_b \right\rangle}\left[\left(\widehat{M}^{\Pi,\boldsymbol{\eta}}_{(\mathsf{A},j)}\right)_b\right]$ *for every* $j \in (z)$*; and*
2. $\beta_j^b = \mathrm{E}_{\left\langle \left(\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{B},j)}\right)_b \right\rangle}\left[\left(\widehat{M}^{\Pi,\boldsymbol{\eta}}_{(\mathsf{B},j)}\right)_b\right]$ *for every* $j \in (z-1)$.

Proof. Immediately follows Proposition 3.8.15. □

Proposition 3.8.16 allows us to use Proposition 3.4.4 in order to analyze the connections between α_j^0 and α_j^1 to α_j, and similarly between β_j^0 and β_j^1 to β_j. Towards this goal, we analyze the edge distribution of the conditional protocols defined in the process generating the measure sequence $(\mathsf{A}, z, \boldsymbol{\eta})$-D$MS\left(\Pi\right)$.

Proposition 3.8.17. *The following holds for both $b \in \{0,1\}$.*

1. A *controls* $\mathsf{root}(\Pi) \implies$
   a) $e_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{A},j)}}(\lambda, b) = e_{\Pi}(\lambda, b) \cdot \frac{\prod_{t=0}^{j-1}\left(1-\alpha_t^b\right)}{\prod_{t=0}^{j-1}(1-\alpha_t)}$ *for all* $j \in (z)$.
   b) $e_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{B},j)}}(\lambda, b) = e_{\Pi}(\lambda, b) \cdot \frac{\prod_{t=0}^{j}\left(1-\alpha_t^b\right)}{\prod_{t=0}^{j}(1-\alpha_t)}$ *for all* $j \in (z-1)$.
2. B *controls* $\mathsf{root}(\Pi) \implies$
   a) $e_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{A},j)}}(\lambda, b) = e_{\Pi}(\lambda, b) \cdot \frac{\prod_{t=0}^{j-1}\left(1-\beta_t^b\right)}{\prod_{t=0}^{j-1}(1-\beta_t)}$ *for all* $j \in (z)$.
   b) $e_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{B},j)}}(\lambda, b) = e_{\Pi}(\lambda, b) \cdot \frac{\prod_{t=0}^{j-1}\left(1-\beta_t^b\right)}{\prod_{t=0}^{j-1}(1-\beta_t)}$ *for all* $j \in (z-1)$.

Proof. We prove Item 1 using induction on the ordered pairs $[(\mathsf{A}, z)]$. The proof of Item 2 is analogous.

Base case. The proof follows since according to Definition 3.8.1, it holds that $\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{A},0)} = \Pi$.

Induction step. Fix $(\mathsf{C}, j) \in [(\mathsf{A}, z)]$ and assume the claim holds for $\mathsf{pred}(\mathsf{C}, j)$. The proof splits according to which party C is.

Case $\mathsf{C} = \mathsf{A}$. In case $e_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{B},j-1)}}(\lambda, b) = 0$, Definition 3.6.1 yields that $e_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{A},j)}}(\lambda, b) = 0$. The proof follows since, by the induction hypothesis, it holds that

$$e_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{A},j)}}(\lambda, b) = e_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{B},j-1)}}(\lambda, b) = e_{\Pi}(\lambda, b) \cdot \frac{\prod_{t=0}^{j-1}\left(1 - \alpha_t^b\right)}{\prod_{t=0}^{j-1}\left(1 - \alpha_t\right)}.$$

In the complementary case, i.e., $e_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{B},j-1)}}(\lambda, b) > 0$, Proposition 3.4.4 and Definition 3.4.1 yield that $\beta_{j-1} = \beta^b_{j-1}$. It must be the case that $\beta_{j-1} = \beta^b_{j-1} < 1$, since otherwise, according to Definition 3.8.1, it holds that $\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{A},j)} = \perp$, a contradiction to the assumption that $\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{A},z)} \neq \perp$. The proof follows since in this case Definition 3.6.1 and Proposition 3.8.16 yield that

$$\begin{aligned} e_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{A},j)}}(\lambda, b) &= e_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{B},j-1)}}(\lambda, b) \cdot \frac{1 - \beta^b_{j-1}}{1 - \beta_{j-1}} \\ &= e_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{B},j-1)}}(\lambda, b) \\ &= e_{\Pi}(\lambda, b) \cdot \frac{\prod_{t=0}^{j-1}\left(1 - \alpha_t^b\right)}{\prod_{t=0}^{j-1}\left(1 - \alpha_t\right)}, \end{aligned}$$

where the last equality follows the induction hypothesis.

Case $\mathsf{C} = \mathsf{B}$. It must be that case that $\alpha_j < 1$, since otherwise, similarly to the previous case and according to Definition 3.8.1, it holds that $\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{B},j)} = \perp$, a contradiction to the assumption that $\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{A},z)} \neq \perp$. The proof follows since in

this case Definition 3.6.1 and Proposition 3.8.16 yield that

$$\begin{aligned} e_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{B},j)}}(\lambda,b) &= e_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{A},j)}}(\lambda,b)\cdot\frac{1-\alpha_j^b}{1-\alpha_j} \\ &= e_{\Pi}(\lambda,b)\cdot\frac{\prod_{t=0}^{j-1}\left(1-\alpha_t^b\right)}{\prod_{t=0}^{j-1}\left(1-\alpha_t\right)}\cdot\frac{1-\alpha_j^b}{1-\alpha_j} \\ &= e_{\Pi}(\lambda,b)\cdot\frac{\prod_{t=0}^{j}\left(1-\alpha_t^b\right)}{\prod_{t=0}^{j}\left(1-\alpha_t\right)}, \end{aligned}$$

where the second equality follows the induction hypothesis.

□

Using the above propositions, we now turn our focus to proving the claims in the proof of Lemma 3.8.2. To ease reading and tracking their proofs, we cluster claims according to the context of the proof of Lemma 3.8.2.

Proving Claims 3.8.4 and 3.8.6.

Proof of Claim 3.8.4. For $b\in\{0,1\}$ it holds that

$$\begin{aligned} \widehat{L}_{\mathsf{A}}^{\Pi_b,\boldsymbol{\eta}_{\mathbf{b}}} &\equiv \sum_{j=0}^{z}\widehat{M}_{(\mathsf{A},j)}^{\Pi_b,\boldsymbol{\eta}_{\mathbf{b}}}\cdot\prod_{t=0}^{j-1}\left(1-\widehat{M}_{(\mathsf{A},t)}^{\Pi_b,\boldsymbol{\eta}_{\mathbf{b}}}\right) \\ &\equiv \sum_{j=0}^{z}\left(\widehat{M}_{(\mathsf{A},j)}^{\Pi,\boldsymbol{\eta}}\right)_b\cdot\prod_{t=0}^{j-1}\left(1-\left(\widehat{M}_{(\mathsf{A},t)}^{\Pi,\boldsymbol{\eta}}\right)_b\right) \\ &\equiv \left(\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}}\right)_b, \end{aligned}$$

where the second equality follows Proposition 3.8.15. □

Proof of Claim 3.8.6. Assume towards a contradiction that $z^0<z$. By the definition of z^0 (Definition 3.8.5) and the definition of conditional protocols (Definition 3.6.1), it follows that $\left(\widehat{\Pi_0}\right)^{\boldsymbol{\eta_0}}_{(\mathsf{A},z^0+1)}=\perp$. Since (by assumption) $z^1\leq z^0$, it also holds that $\left(\widehat{\Pi_1}\right)^{\boldsymbol{\eta_1}}_{(\mathsf{A},z^0+1)}=\perp$. Hence, Proposition 3.8.15 yields that

$\left(\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{A},z^0+1)}\right)_0, \left(\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{A},z^0+1)}\right)_1 = \perp$. Namely, the restrictions of the function describing $\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{A},z^0+1)}$ to the subtrees $\mathcal{T}(\Pi_0)$ and $\mathcal{T}(\Pi_1)$, do not correspond to any two-party execution. Hence, the aforementioned function does not correspond to a two-party execution (over $\mathcal{T}(\Pi)$), in contradiction to the assumption that $\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{A},z)} \neq \perp$. □

Proving Claims 3.8.7 to 3.8.9. The following proofs relay on the next observation. As long as $\alpha^b_j < 1$ and $\beta^b_j < 1$, Proposition 3.8.17 assures that there is a positive probability to visiting both the left and the right subtree of the (C, j)'th conditional protocol.

Proof of Claim 3.8.8. Assume that A controls $\mathsf{root}(\Pi)$ and that $z^1 < z$. Assume toward a contradiction that $\alpha^1_{z^1} < 1$. Since $z^1 \leq z^0$ (by assumption) it follows that $\alpha^0_{z^1} < 1$ as well. The definition of z^1 (Definition 3.8.5) yields that $\beta^1_{z^1} = 1$. However, Proposition 3.8.17 yields that $e_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{B},j)}}(\lambda, b) \in (0,1)$ for both $b \in \{0,1\}$, and thus Propositions 3.4.4 and 3.8.16 yield that $\beta_{z^1} = 1$. Now, Definition 3.8.1 yield that $\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{A},z^1+1)} = \perp$, a contradiction to the assumption that $\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{A},z)} \neq \perp$. □

Proof of Claim 3.8.7. For $j \in (z^1 - 1)$, it holds that $e_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{B},j)}}(\lambda, b) \in (0,1)$ for both $b \in \{0,1\}$. Thus, $\beta^0_j = \beta^1_j = \beta_j$ is a direct implication of Propositions 3.4.4 and 3.8.15.

For $z^1 \leq z - 1$, Claim 3.8.8 and Proposition 3.8.17 yield that $e_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{B},j)}}(\lambda, 0) = 1$. Since, by Definition 3.8.3, it holds that $\eta_{(\mathsf{B},j)} = \eta^0_{(\mathsf{B},j)}$, Definition 3.4.1 and Proposition 3.8.15 yield that $\beta^0_j = \beta_j$. □

Proof of Claim 3.8.9. The proof immediately follows Propositions 3.8.16 and 3.8.17.

□

Proving Claims 3.8.10 and 3.8.11.

Proof of Claim 3.8.10. By Definition 3.4.1 it holds that $\widehat{M}^{\Pi_1,\boldsymbol{\eta_1}}_{(\mathsf{A},j)} \equiv 0$ for every $j \in (z)$. Definition 3.8.1 yields that $\widehat{L}^{\Pi_1,\boldsymbol{\eta_1}}_{\mathsf{A}} \equiv 0$. The proof follows Claim 3.8.4. □

Proof of Claim 3.8.11. Follows similar arguments to the above proof of Claim 3.8.10, together with Proposition 3.8.16. □

Proving Claims 3.8.12 to 3.8.14. The proofs of the rest of the claims stated in the proof of Lemma 3.8.2 are analogous to claims proved above. Specifically, Claim 3.8.12 is analogous to Claim 3.8.7, Claim 3.8.13 is analogous to Claim 3.8.8, and Claim 3.8.14 is analogous to Claim 3.8.9.

Proving Lemma 3.7.2

Lemma 3.7.2 immediately follows by the next lemma.

Lemma 3.8.18. *For every protocol* Π*, there exists* $(\mathsf{C}, j) \in \{\mathsf{A}, \mathsf{B}\} \times \mathbb{N}$ *such that*

$$\mathrm{E}_{\langle \Pi_{(\mathsf{C},j)} \rangle} \left[M^{\mathsf{C}}_{\Pi_{(\mathsf{C},j)}} \right] = 1.$$

The proof of Lemma 3.8.18 is given below, but first we use it to derive Lemma 3.7.2.

Proof of Lemma 3.7.2. Let z be the minimal integer such that $\sum_{j=0}^{z} \alpha_j \geq c$ or $\sum_{j=0}^{z} \beta_j \geq c$. Note that such z guaranteed to exists by Lemma 3.8.18 and since by Lemma 3.4.2 it holds that $\alpha_j = \mathrm{E}_{\langle \Pi_{(\mathsf{A},j)} \rangle} \left[M^{\mathsf{A}}_{\Pi_{(\mathsf{A},j)}} \right]$ and $\beta_j = \mathrm{E}_{\langle \Pi_{(\mathsf{B},j)} \rangle} \left[M^{\mathsf{B}}_{\Pi_{(\mathsf{B},j)}} \right]$. The proof splits to the following cases.

Case $\sum_{j=0}^{z}\alpha_j \geq c$. By the choice of z it holds that $\sum_{j=0}^{z-1}\alpha_j < c$ and $\sum_{j=0}^{z-1}\beta_j < c$.

Lemma 3.6.7 yields that

$$\begin{aligned}
\mathrm{E}_{\langle\Pi\rangle}\left[L_{\Pi}^{\mathsf{A},z}\right] &= \sum_{j=0}^{z}\alpha_j\prod_{t=0}^{j-1}(1-\beta_t)(1-\alpha_t) \\
&\geq \left(\sum_{j=0}^{z}\alpha_j\right)\cdot\left(1-\sum_{j=0}^{z-1}\beta_j\right)\cdot\left(1-\sum_{j=0}^{z-1}\alpha_j\right) \\
&\geq c\cdot(1-2c),
\end{aligned}$$

where the first inequality follows by multiplying the j'th summand by $\prod_{t=j}^{z-1}(1-\beta_t)(1-\alpha_t) \leq 1$ and both inequalities follows since $(1-x)(1-y) \geq 1-(x+y)$ for any $x, y \geq 0$. Hence, z satisfies Item 1.

Case $\sum_{j=0}^{z}\alpha_j < c$. By the choice of z it holds that $\sum_{j=0}^{z}\beta_j \geq c$ and $\sum_{j=0}^{z-1}\beta_j < c$.

Similar arguments to the previous case show that z satisfies Item 2.

□

Towards proving Lemma 3.8.18 we prove that there is always a leaf for which the value of the dominated measure is 1.

Claim 3.8.19. *Let Π be a protocol with $\mathsf{OPT}_{\mathsf{A}}(\Pi) = 1$. Then there exists $\ell \in \mathcal{L}_1(\Pi)$ such that $M_{\Pi}^{\mathsf{A}}(\ell) = 1$.*

Proof. The proof is by induction on the round complexity of Π.

Assume that $\mathrm{round}(\Pi) = 0$ and let ℓ be the only node in $\mathcal{T}(\Pi)$. Since $\mathsf{OPT}_{\mathsf{A}}(\Pi) > 0$, it must be the case that $\chi_{\Pi}(\ell) = 1$. The proof follows since Definition 3.4.1 yields that $M_{\Pi}^{\mathsf{A}}(\ell) = 1$.

Assume that $\mathrm{round}(\Pi) = m+1$ and that the lemma holds for m-round protocols. In case $e_{\Pi}(\lambda, b) = 1$ for some $b \in \{0,1\}$, then by Proposition 3.3.2 it holds

that $\mathsf{OPT}_{\mathsf{A}}(\Pi_b) = \mathsf{OPT}_{\mathsf{A}}(\Pi) = 1$. This allows to apply the induction hypothesis on Π_b, which yields that there exists $\ell \in \mathcal{L}_1(\Pi_b)$ such that $M^{\mathsf{A}}_{\Pi_b}(\ell) = 1$. In this case, according to Definition 3.4.1, $M^{\mathsf{A}}_{\Pi}(\ell) = M^{\mathsf{A}}_{\Pi_b}(\ell) = 1$, and the proof follows.

In the following we assume that $e_{\Pi}(\lambda, b) \in (0, 1)$ for any $b \in \{0, 1\}$. We conclude the proof using the following case analysis.

A controls $\mathsf{root}(\Pi)$. According to Proposition 3.3.2, there exists $b \in \{0, 1\}$ such that $\mathsf{OPT}_{\mathsf{A}}(\Pi_b) = \mathsf{OPT}_{\mathsf{A}}(\Pi) = 1$. This allows to apply the induction hypothesis on Π_b, which yields that there exists $\ell \in \mathcal{L}_1(\Pi_b)$ such that $M^{\mathsf{A}}_{\Pi_b}(\ell) = 1$. The A-maximal property of M^{A}_{Π} (Proposition 3.4.4(1)) yields that $M^{\mathsf{A}}_{\Pi}(\ell) = M^{\mathsf{A}}_{\Pi_b}(\ell) = 1$, and the proof for this case follows.

B controls $\mathsf{root}(\Pi)$. According to Proposition 3.3.2, $\mathsf{OPT}_{\mathsf{A}}(\Pi_b) = \mathsf{OPT}_{\mathsf{A}}(\Pi) = 1$ for both $b \in \{0, 1\}$. This allows to apply the induction hypothesis on Π_0 and Π_1, which yields that there exists $\ell_0 \in \mathcal{L}_1(\Pi_0)$ and $\ell_1 \in \mathcal{L}_1(\Pi_1)$ such that $M^{\mathsf{A}}_{\Pi_0}(\ell_0) = 1$ and $M^{\mathsf{A}}_{\Pi_1}(\ell_1) = 1$. The B-minimal property of M^{A}_{Π} (Proposition 3.4.4(2)) yields that there exists $b \in \{0, 1\}$ such that $M^{\mathsf{A}}_{\Pi}(\ell_b) = M^{\mathsf{A}}_{\Pi_b}(\ell_b) = 1$ (the bit b for which $\mathsf{Smaller}_{\Pi}(b) = 1$), and the proof for this case follows.

This concludes the case analysis and the proof follows. □

We can now derive Lemma 3.8.18. Intuitively, Claim 3.8.19 and Proposition 3.4.4 yield that the number of possible transcripts of $\Pi_{(\mathsf{C},j)}$ is shrinking as (C, j) grows. Specifically, at least one possible transcript of $\Pi_{(\mathsf{A},j)}$ whose output is 1 (the transcript represented by the leaf guarantee to exists from Claim 3.8.19) is *not* a possible transcript of $\Pi_{(\mathsf{B},j)}$. Similarly, at least one possible transcript of $\Pi_{(\mathsf{B},j-1)}$ whose output is 0 is not a possible transcript of $\Pi_{(\mathsf{A},j)}$. Since the number

of possible transcripts of Π is finite (though might be exponentially large), there exists $j \in \mathbb{N}$ such that either all possible transcripts $\Pi_{(\mathsf{A},j)}$ output 1 or all possible transcripts of $\Pi_{(\mathsf{B},j)}$ output 0. The expected value of the A-dominated measure of $\Pi_{(\mathsf{A},j)}$ or the B-dominated measure of $\Pi_{(\mathsf{B},j)}$ will be 1. The formal proof is given next.

Proof of Lemma 3.8.18. Assume towards a contradiction that $\mathrm{E}_{\langle \Pi_{(\mathsf{C},j)} \rangle}\left[M^{\mathsf{C}}_{\Pi_{(\mathsf{C},j)}}\right] < 1$ for every $(\mathsf{C},j) \in \{\mathsf{A},\mathsf{B}\} \times \mathbb{N}$. It follows that $\Pi_{(\mathsf{C},j)} \neq \bot$ for every such (C,j). For a pair $(\mathsf{C},j) \in \{\mathsf{A},\mathsf{B}\} \times \mathbb{N}$ recursively define $\mathcal{L}_{(\mathsf{C},j)} := \mathcal{L}_{\mathsf{pred}(\mathsf{C},j)} \cup \mathcal{S}_{(\mathsf{C},j)}$, where $\mathcal{S}_{(\mathsf{C},j)} := \left\{\ell \in \mathcal{L}(\Pi)\colon M^{\mathsf{C}}_{\Pi_{(\mathsf{C},j)}}(\ell) = 1\right\}$ and $\mathcal{L}_{(\mathsf{B},-1)} := \emptyset$. The following claim (proved below) shows two properties of $\mathcal{S}_{(\mathsf{C},j)}$.

Claim 3.8.20. *It holds that $\mathcal{S}_{(\mathsf{C},j)} \neq \emptyset$ and $\mathcal{L}_{\mathsf{pred}(\mathsf{C},j)} \cap \mathcal{S}_{(\mathsf{C},j)} = \emptyset$ for every $(\mathsf{C},j) \succeq (\mathsf{B},0)$.*

Claim 3.8.20 yields that $\left|\mathcal{L}_{(\mathsf{C},j)}\right| > \left|\mathcal{L}_{\mathsf{pred}(\mathsf{C},j)}\right|$ for every $(\mathsf{C},j) \succeq (\mathsf{B},0)$, a contradiction to the fact that $\mathcal{L}_{(\mathsf{C},j)} \subseteq \mathcal{L}(\Pi)$ for every (C,j). □

Proof of Claim 3.8.20. Let $(\mathsf{C},j) \succeq (\mathsf{B},0)$. By Lemma 3.6.4 it holds that $\mathsf{OPT}_{\mathsf{C}}\left(\Pi_{(\mathsf{C},j)}\right) = 1$.[24] Hence, Claim 3.8.19 yields that $\mathcal{S}_{(\mathsf{C},j)} \neq \emptyset$.

Towards proving the second property, let $\ell' \in \mathcal{L}_{\mathsf{pred}(\mathsf{C},j)}$, and let $(\mathsf{C}',j') \in [\mathsf{pred}(\mathsf{C},j)]$ such that $\ell' \in \mathcal{S}_{(\mathsf{C}',j')}$. By the definition of $\mathcal{S}_{(\mathsf{C}',j')}$, it holds that $M^{\mathsf{C}'}_{\Pi_{(\mathsf{C}',j')}}(\ell') = 1$. By Proposition 3.6.2 it holds that $\ell' \notin \mathrm{Supp}\left(\left\langle \Pi_{(\mathsf{C}'',j'')} \right\rangle\right)$ for every $(\mathsf{C}'',j'') \succ (\mathsf{C}',j')$. Since $(\mathsf{C},j) \succ \mathsf{pred}(\mathsf{C},j) \succeq (\mathsf{C}',j')$, it holds that $\ell' \notin \mathrm{Supp}\left(\left\langle \Pi_{(\mathsf{C},j)} \right\rangle\right)$. By Definition 3.4.1 it holds that $M^{\mathsf{C}}_{\Pi_{(\mathsf{C},j)}}(\ell) = 0$ for every $\ell \notin \mathrm{Supp}\left(\left\langle \Pi_{(\mathsf{C},j)} \right\rangle\right)$, and thus $\ell' \notin \mathcal{S}_{(\mathsf{C},j)}$. Hence, $\mathcal{L}_{\mathsf{pred}(\mathsf{C},j)} \cap \mathcal{S}_{(\mathsf{C},j)} = \emptyset$. □

[24] Note that this might not hold for $\Pi_{(\mathsf{A},0)} = \Pi$. Namely, it might be the case that $\mathsf{OPT}_{\mathsf{B}}(\Pi) = 1$. In this case M^{A}_{Π} is the zero measure, $\Pi_{(\mathsf{B},0)} = \Pi$ and $\mathcal{S}_{(\mathsf{A},0)} = \emptyset$.

3.9 Additional Properties of the Biased-Continuation Attack

Robustness

The following lemma states that, under a certain condition, by applying the biased-continuation attack on similar protocols, one does not make them too far apart.

Lemma 3.9.1. *Let* $\Pi = (\mathsf{A}, \mathsf{B})$ *and* $\Pi' = (\mathsf{C}, \mathsf{D})$ *be two* m*-round protocols such that* $\mathrm{SD}([\Pi], [\Pi']) \leq \alpha$*. let* $\delta \in (0, \frac{1}{2}]$ *and let* $c = c(\delta)$ *from Lemma 4.3.1. Then*

$$\mathrm{SD}\left(\left[\mathsf{A}^{(1)}, \mathsf{B}\right], \left[\mathsf{C}^{(1)}, \mathsf{D}\right]\right) \leq \frac{2 \cdot m \cdot \gamma}{\delta'} \cdot \left(\alpha + \Pr_{\langle \mathsf{A},\mathsf{B} \rangle}\left[\mathsf{desc}\left(\mathcal{S}\mathsf{mall}_{\Pi}^{\delta',\mathsf{A}} \cup \mathcal{S}\mathsf{mall}_{\Pi'}^{\delta',\mathsf{C}}\right)\right]\right) + \frac{4}{\gamma^c},$$

for every $\delta' \geq \delta$ *and* $\gamma \geq 1$*, where* $\mathsf{A}^{(1)}$ *and* $\mathsf{C}^{(1)}$ *are as defined in Algorithm 3.1.2.*[25]

Proof. In order to prove this lemma we will use Lemma 2.4.5. The corresponding function f will be the function implied by the leaf chosen by $\mathsf{BiasedCont}_{\Pi}$ and g the one implied by the leaf chosen by $\mathsf{BiasedCont}_{\Pi'}$, where both in addition output the controlling scheme of the corresponding leaf. For every $i \in [m]$ let D_i be the distribution over the pairs (u, b), where u is node of level i whose distribution is the one implied by $\langle \mathsf{A}, \mathsf{B} \rangle$ and b is a bit equal 1 with probability $\mathsf{val}(\Pi_u)$. For our purposes we have to give an upper bound on $\mathrm{E}_{u \leftarrow D_i}[\mathrm{SD}(f(u), g(u))]$ for every $i \in [m]$. However, if we set

1. for a node u, $\Delta_u = \mathsf{val}(\Pi'_u) - \mathsf{val}(\Pi_u)$,

[25] Recall that $[\Pi]$, is the transcript and controlling path (i.e., which party sent each of the messages), induced by a random execution of Π, as defined in Definition 2.2.2.

2. for a protocol Π and a node u, $[\Pi]_u$ to be a distribution where any pair (ℓ, x) is drawn according to $[\Pi]$ conditioning on $\ell_{1\ldots i} = u$ and

3. for a leaf ℓ, x^ℓ and y^ℓ to be the controlling schemes associated with ℓ in protocol Π and Π' respectively.

4. for every node u, $\mathcal{S}_u$ to be the set of all leaves ℓ, such that $\ell \in \mathsf{desc}(u)$ and with $\chi_\Pi(\ell) = \chi_{\Pi'}(\ell) = 1$ (remember by the assumption we made in the beginning of this section this is equivalent to $\ell_m = 1$) and $\Pr_{[\mathsf{A},\mathsf{B}]_u}\left[(\ell, x^\ell)\right] \geq \Pr_{[\mathsf{C},\mathsf{D}]_u}\left[(\ell, y^\ell)\right]$

$$\mathrm{E}_{u\leftarrow D_i}[\mathrm{SD}(f(u),g(u))] = \sum_{u\in\{0,1\}^i} D_i(u)\cdot \mathrm{SD}(f(u),g(u))$$

$$= \sum_{u\in\{0,1\}^i} D_i(u)\cdot\left(\sum_{\ell\in\mathcal{S}_u}\Pr_{[\mathsf{A},\mathsf{B}]_u}\left[(\ell,x^\ell)|\chi_\Pi(\ell)=1\right]-\sum_{\ell\in\mathcal{S}_u}\Pr_{[\mathsf{C},\mathsf{D}]_u}\left[(\ell,y^\ell)|\chi_{\Pi'}(\ell)=1\right]\right)$$

$$= \sum_{u\in\{0,1\}^i} D_i(u)\cdot\left(\frac{\sum_{\ell\in\mathcal{S}_u}\Pr_{[\mathsf{A},\mathsf{B}]_u}\left[(\ell,x^\ell)\right]}{\mathsf{val}(\Pi_u)}-\frac{\sum_{\ell\in\mathcal{S}_u}\Pr_{[\mathsf{C},\mathsf{D}]_u}\left[(\ell,y^\ell)\right]}{\mathsf{val}(\Pi'_u)}\right)$$

$$= \sum_{u\in\{0,1\}^i} D_i(u)\cdot\left(\frac{\sum_{\ell\in\mathcal{S}_u}\Pr_{[\mathsf{A},\mathsf{B}]_u}\left[(\ell,x^\ell)\right]}{\mathsf{val}(\Pi_u)}-\frac{\sum_{\ell\in\mathcal{S}_u}\Pr_{[\mathsf{C},\mathsf{D}]_u}\left[(\ell,y^\ell)\right]}{\mathsf{val}(\Pi_u)+\Delta_u}\right)$$

$$= \sum_{u\in\{0,1\}^i\wedge\Delta_u\le 0} D_i(u)\cdot\left(\frac{\sum_{\ell\in\mathcal{S}_u}\Pr_{[\mathsf{A},\mathsf{B}]_u}\left[(\ell,x^\ell)\right]}{\mathsf{val}(\Pi_u)}-\frac{\sum_{\ell\in\mathcal{S}_u}\Pr_{[\mathsf{C},\mathsf{D}]_u}\left[(\ell,y^\ell)\right]}{\mathsf{val}(\Pi_u)+\Delta_u}\right)$$

$$+ \sum_{u\in\{0,1\}^i\wedge\Delta_u>0} D_i(u)\cdot\left(\frac{\sum_{\ell\in\mathcal{S}_u}\Pr_{[\mathsf{A},\mathsf{B}]_u}\left[(\ell,x^\ell)\right]}{\mathsf{val}(\Pi_u)}-\frac{\sum_{\ell\in\mathcal{S}_u}\Pr_{[\mathsf{C},\mathsf{D}]_u}\left[(\ell,y^\ell)\right]}{\mathsf{val}(\Pi_u)+\Delta_u}\right)$$

$$\le \sum_{u\in\{0,1\}^i\setminus\mathcal{S}\mathsf{mall}_\Pi^{\delta',\mathsf{C}}\wedge\Delta_u\le 0}\frac{D_i(u)}{\mathsf{val}(\Pi'_u)}\cdot\left(\sum_{\ell\in\mathcal{S}_u}\Pr_{[\mathsf{A},\mathsf{B}]_u}\left[(\ell,x^\ell)\right]-\sum_{\ell\in\mathcal{S}_u}\Pr_{[\mathsf{C},\mathsf{D}]_u}\left[(\ell,y^\ell)\right]\right)$$

$$+ \sum_{u\in\{0,1\}^i\setminus\mathcal{S}\mathsf{mall}_{\Pi'}^{\delta',\mathsf{A}}\wedge\Delta_u>0}\frac{D_i(u)}{\mathsf{val}(\Pi_u)}\cdot\left(\sum_{\ell\in\mathcal{S}_u}\Pr_{[\mathsf{A},\mathsf{D}]_u}\left[(\ell,y^\ell)\right]-\sum_{\ell\in\mathcal{S}_u}\Pr_{[\mathsf{C},\mathsf{D}]_u}\left[(\ell,y^\ell)\right]\right)$$

$$+\sum_{u\in\{0,1\}^i} D_i(u)\cdot\Delta_u$$

$$+\Pr_{\langle\mathsf{A},\mathsf{B}\rangle}\left[\mathsf{desc}\left(\mathcal{S}\mathsf{mall}_\Pi^{\delta',\mathsf{A}}\cup\mathcal{S}\mathsf{mall}_{\Pi'}^{\delta',\mathsf{C}}\right)\right]$$

$$\le \frac{\mathrm{SD}([\Pi],[\Pi'])}{\delta'}+\mathrm{SD}([\Pi],[\Pi'])+\Pr_{\langle\mathsf{A},\mathsf{B}\rangle}\left[\mathsf{desc}\left(\mathcal{S}\mathsf{mall}_\Pi^{\delta',\mathsf{A}}\cup\mathcal{S}\mathsf{mall}_{\Pi'}^{\delta',\mathsf{C}}\right)\right]$$

$$\le \frac{2\alpha}{\delta'}+\Pr_{\langle\mathsf{A},\mathsf{B}\rangle}\left[\mathsf{desc}\left(\mathcal{S}\mathsf{mall}_\Pi^{\delta',\mathsf{A}}\cup\mathcal{S}\mathsf{mall}_{\Pi'}^{\delta',\mathsf{C}}\right)\right],$$

where the third equality follows from the definition of $\mathsf{BiasedCont}_{\Pi_b}$, which chooses a leaf conditioned on its value being 1 and the inequality follows from the fact that for $0\le a\le b$ and $c\ge 0$ it holds $\frac{a}{b}\ge\frac{a-c}{b-c}$.

Moreover, notice that if we set F_i to be the distribution of the i'th query of $\mathsf{A}^{(1)}$ to $\mathsf{BiasedCont}$, we can see (setting Q to be the random variable of the queries of $\mathsf{A}^{(1)}$ of a random execution of $(\mathsf{A}^{(1)}, \mathsf{B})$) that

$$\begin{aligned}
&\Pr_{(q_1,\ldots,q_k)\leftarrow Q}\left[\exists i \in [k]\colon q_i \neq \perp \wedge F_i(q_i) > \frac{\gamma}{\delta'} \cdot D_i(q_i)\right] \\
&\quad = \Pr_{\langle \mathsf{A}^{(1)},\mathsf{B}\rangle}\left[\mathsf{desc}\left(\mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi} \cup \mathcal{S}\mathsf{mall}^{\delta',\mathsf{A}}_{\Pi}\right)\right] \\
&\quad \leq \Pr_{\langle \mathsf{A}^{(1)},\mathsf{B}\rangle}\left[\mathsf{desc}\left(\mathcal{S}\mathsf{mall}^{\delta',\mathsf{A}}_{\Pi}\right)\right] + \frac{2}{\gamma^c} \\
&\quad \leq \gamma \cdot \Pr_{\langle \mathsf{A},\mathsf{B}\rangle}\left[\mathsf{desc}\left(\mathcal{S}\mathsf{mall}^{\delta',\mathsf{A}}_{\Pi}\right)\right] + \frac{4}{\gamma^c}
\end{aligned}$$

where the first inequality follows from Lemma 4.3.1 and the second from Proposition 4.3.3(1).

Putting things together after applying Lemma 2.4.5 with $k := m$, $a := \frac{2\alpha}{\delta'} + \Pr_{\langle \mathsf{A},\mathsf{B}\rangle}\left[\mathsf{desc}\left(\mathcal{S}\mathsf{mall}^{\delta',\mathsf{A}}_{\Pi} \cup \mathcal{S}\mathsf{mall}^{\delta',\mathsf{C}}_{\Pi'}\right)\right]$, $\lambda := \frac{\gamma}{\delta'}$ and $b := \gamma \cdot \Pr_{\langle \mathsf{A},\mathsf{B}\rangle}\left[\mathsf{desc}\left(\mathcal{S}\mathsf{mall}^{\delta',\mathsf{A}}_{\Pi}\right)\right] + \frac{4}{\gamma^c}$ we derive (a stronger version of) the lemma. □

Chapter 4

The Real Attack

4.1 Attacking Coin Flipping Protocols Using (Imperfect) Function Inverters

In Chapter 3 we showed that for any constant $\varepsilon \in (0, \frac{1}{2}]$ there exists some constant $\kappa = \kappa(\varepsilon)$ such that carrying out κ iterations of the biased-continuation attack biases any coin-flipping protocol by $1 - \varepsilon$. Implementing this attack requires, however, access to a sampling algorithm, denoted BiasedCont (Algorithm 3.1.1), which we don't know how to efficiently implement assuming OWFs do not exist. Our goal in this section is to show that access to an approximation of the sampling algorithm suffices to bias any coin-flipping protocol. Though we couldn't prove that carrying out the bias-continuation attack successfully biases any coin-flipping protocol (and believe it is not true), we manage to prove it for a variant of the above attack.

In the rest of the section we prove our main theorem: assuming OWFs do not exist, then there exists an efficient attacker that successfully biases any coin-flipping protocol. We begin by defining an approximation of the sampling algorithm BiasedCont, which can be efficiently implemented assuming OWFs do not

exist. We then define the approximated biases-continuation attacker, that carries out the iterated biases-continuation attack using oracle access to the approximated samling algorithm. We show that there exist two sets of transcripts, $\mathcal{U}\mathsf{nBal}$ and $\mathcal{S}\mathsf{mall}$, such that if the probability of the original protocol to generate transcripts within these sets is small, the biased-continuation attacker still does well (i.e., successfully biases any coin-flipping protocol). Next, we show that, in fact, the biased-continuation attacker still does well when only the probability of the original protocol to generate a transcript within $\mathcal{S}\mathsf{mall}$ is small. We then define a variant of the original protocol, the pruned protocol, which cannot generate transcript within $\mathcal{S}\mathsf{mall}$, and thus the biased-continuation attacker does well when attacking this protocol. Our last step before proving our main theorem is to use the pruned protocol to define the Pruning-in-the-Head attacker, which if some condition is met, does well for all protocols. The main theorem is proven by slightly tweaking the Pruning-in-the-Head attacker, to ensure the above condition is met.

4.2 The Approximated Biased Continuation Attack

The biased-continuation attacker of Chapter 3 was given an oracle access to an ideal biased-continuator, $\mathsf{BiasedCont}$ (Algorithm 3.1.1). Unfortunately, we do not know how to efficiently implement this algorithm, even when assuming OWFs do not exist. Hence, we need to define a relaxation of this algorithm that can be efficiently implemented assuming OWFs do not exist.

Definition 4.2.1 (approximated biased-continuator)**.** *Algorithm* $\widetilde{\mathsf{BiasedCont}}$ *is a*

(ξ, δ)-biased-continuator *for* Π*, if the following hold.*

$Pr_{\ell \leftarrow \langle \Pi \rangle}[\exists i \in [m] \colon \mathrm{SD}\left(\widetilde{\mathsf{BiasedCont}}(\ell_{1,\ldots,i}, 1), \mathsf{BiasedCont}(\ell_{1,\ldots,i}, 1)\right) > \xi \wedge \mathsf{val}(\Pi_{\ell_{1,\ldots,i}}) > \delta] \leq \xi$

and

$Pr_{\ell \leftarrow \langle \Pi \rangle}[\exists i \in [m] \colon \mathrm{SD}\left(\widetilde{\mathsf{BiasedCont}}(\ell_{1,\ldots,i}, 0), \mathsf{BiasedCont}(\ell_{1,\ldots,i}, 0)\right) > \xi \wedge \mathsf{val}(\Pi_{\ell_{1,\ldots,i}}) < 1 - \delta] \leq \xi$,

where BiasedCont *is as in Algorithm 3.1.1.*

The approximated biased-continuation attacker is identical to the biased-continuation attacker, except it is given an oracle access to the approximated biased-continuator.

Algorithm 4.2.2 ($\mathsf{A}_{\Pi}^{(1,\widetilde{\mathsf{BiasedCont}})}$)**.**

Oracle: $\widetilde{\mathsf{BiasedCont}}$.

Input: $u \in \{0,1\}^*$.

Operation:

1. *If* $u \in \mathcal{L}(\Pi)$*, output* $\chi_\Pi(u)$ *and halt.*
2. *Set* $\mathsf{msg} = \widetilde{\mathsf{BiasedCont}}(u, 1)$.
3. *Send* msg *to* B.
4. *If* $u' = u \circ \mathsf{msg} \in \mathcal{L}(\Pi)$*, output* $\chi_\Pi(u')$.

Adversary $\mathsf{B}_{\Pi}^{(1,\widetilde{\mathsf{BiasedCont}})}$ is defined analogously, where the only difference is that the second argument in the call to $\widetilde{\mathsf{BiasedCont}}$ is 0. In the rest of the section we focus on attackers playing the role of A and trying to bias the protocol towards 1.

Our goal is to bound the difference between the biased-continuation attacker and its approximated variant. Intuitively, if the statistical distance of the answers of $\mathsf{BiasedCont}$ and $\widetilde{\mathsf{BiasedCont}}$ is small, then so would be the difference between the attackers. Definition 4.2.1, however, does not always guarantee such small statistical distance. Specifically, there is no such guarantee for low-value and high-value transcripts.

Definition 4.2.3 (low-value and high-value nodes)**.** *For a protocol* $\Pi = (\mathsf{A}, \mathsf{B})$ *and* $\delta \in [0,1]$*, let*

- $\mathcal{S}\mathsf{mall}_{\Pi}^{\delta} = \{u \in \mathcal{V}(\Pi) \setminus \mathcal{L}(\Pi) : \mathsf{val}(\Pi_u) \leq \delta\}$*, and*
- $\mathcal{L}\mathsf{arge}_{\Pi}^{\delta} = \{u \in \mathcal{V}(\Pi) \setminus \mathcal{L}(\Pi) : \mathsf{val}(\Pi_u) \geq 1 - \delta\}$.

For $\mathsf{C} \in \{\mathsf{A}, \mathsf{B}\}$*, let* $\mathcal{S}\mathsf{mall}_{\Pi}^{\delta,\mathsf{C}} = \mathcal{S}\mathsf{mall}_{\Pi}^{\delta} \cap \mathcal{C}\mathsf{trl}_{\Pi}^{\mathsf{C}}$ *and similarly* $\mathcal{L}\mathsf{arge}_{\Pi}^{\delta,\mathsf{C}} = \mathcal{L}\mathsf{arge}_{\Pi}^{\delta} \cap \mathcal{C}\mathsf{trl}_{\Pi}^{\mathsf{C}}$.[1]

Moreover, even for transcripts that are not low-value or high-value, Definition 4.2.1 only guarantees small statistical distance between the answers of $\mathsf{BiasedCont}$ and $\widetilde{\mathsf{BiasedCont}}$ when queried on transcripts chosen according to the honest distribution of leaves, $\langle\Pi\rangle$. However, the queries the biased-continuation attacker makes might be chosen from a different distribution, making some transcripts much likely to be asked than before. We call such transcripts "unbalanced".

Definition 4.2.4 (unbalanced nodes)**.** *For a protocol* $\Pi = (\mathsf{A}, \mathsf{B})$ *and* $\gamma \geq 1$*, let* $\mathcal{U}\mathsf{nBal}_{\Pi}^{\gamma} = \left\{u \in \mathcal{V}(\Pi) \colon \mathsf{v}_{(\mathsf{A}^{(1)},\mathsf{B})}(u) \geq \gamma \cdot \mathsf{v}_{(\mathsf{A},\mathsf{B})}(u)\right\}$*, where* $\mathsf{A}^{(1)}$ *is as in Algorithm 3.1.2 and* v *as in Definition 2.2.2.*

[1] Recall that $\mathcal{C}\mathsf{trl}_{\Pi}^{\mathsf{C}}$ denotes the nodes in $\mathcal{T}(\Pi)$ controlled by the party C.

Consider an execution of $(\mathsf{A}^{(1,\widetilde{\mathsf{BiasedCont}})}, \mathsf{B})$. Such execution asks $\widetilde{\mathsf{BiasedCont}}$ for continuations of transcripts under A's control, leading to 1-leaves. Hence, as long as this execution does not generate low-value transcripts under A's control or unbalanced transcripts, we expect the approximated biased-continuation attacker to do almost as well as its ideal variant. This is formally put in the following lemma.

Lemma 4.2.5. *Let $\Pi = (\mathsf{A}, \mathsf{B})$ be a m-round protocol and let $\delta \in (0, \frac{1}{2}]$. Then for every $\gamma \geq 1$ it holds that*

$$\mathrm{SD}\left(\left[\mathsf{A}^{(1)}, \mathsf{B}\right], \left[\mathsf{A}^{(1,\widetilde{\mathsf{BiasedCont}})}, \mathsf{B}\right]\right) \leq m \cdot \gamma \cdot \left(2\xi + \Pr_{\langle \mathsf{A},\mathsf{B}\rangle}\left[\mathsf{desc}(\mathcal{S}\mathsf{mall}_{\Pi}^{\delta,\mathsf{A}})\right]\right) + \Pr_{\langle \mathsf{A}^{(1)},\mathsf{B}\rangle}\left[\mathsf{desc}\left(\mathcal{U}\mathsf{nBal}_{\Pi}^{\gamma}\right)\right],$$ [2]

where $\widetilde{\mathsf{BiasedCont}}$ is a (ξ, δ)-biased-continuator for Π according to Definition 4.2.1.

Proof. The lemma is proven by applying Lemma 2.4.5. The corresponding functions f and g will be the output of $\mathsf{BiasedCont}$ and $\widetilde{\mathsf{BiasedCont}}$ respectively (in case the query is $\perp$, the output will also be $\perp$). For every $i \in [m]$, let D_i be the distribution over $\{\mathcal{V}(\Pi) \times \{1\}\} \cup \{\perp\}$ set to $(\ell_{1,\ldots,i}, 1)$, where $\ell \leftarrow \langle \Pi \rangle$ in case $\ell_{1,\ldots,i} \in \mathcal{C}\mathsf{trl}_{\Pi}^{\mathsf{A}}$; and set to $\perp$ otherwise. The definition of $\widetilde{\mathsf{BiasedCont}}$ as a (ξ, δ')-continuator guarantees that for every $i \in [m]$, it holds that

$$\mathrm{E}_{d \leftarrow D_i}\left[\mathrm{SD}(f(d), g(d))\right] \leq 2\xi + \Pr_{\langle \mathsf{A},\mathsf{B}\rangle}\left[\mathsf{desc}(\mathcal{S}\mathsf{mall}_{\Pi}^{\delta,\mathsf{A}})\right].$$

[2] Recall that for a protocol Π, $[\Pi]$ denotes the leaf-control distribution, which samples a leaf according to $\langle \Pi \rangle$, and outputs the party controlling each ancestor of that leaf (see Definition 2.2.2). Moreover, for $\mathcal{S} \subseteq \mathcal{V}(\Pi)$, $\mathsf{desc}(\mathcal{S})$ stands for the set of leaves which have an ancestor in $\mathcal{S}$.

Moreover, let H^{O} be an oracle-aided algorithm define as follows: randomly execute $(\mathsf{A}^{(1,\mathsf{O})},\mathsf{B})$; when this execution reaches a node u, call $\mathsf{O}(u,1)$ in case u controlled by A and call $\mathsf{O}(\perp)$ otherwise; output the leaf at the end of this execution, together with its controlling scheme.

It follows that $\mathrm{SD}\left(\left[\mathsf{A}^{(1)},\mathsf{B}\right],\left[\mathsf{A}^{(1,\widetilde{\mathsf{BiasedCont}})},\mathsf{B}\right]\right)=\mathrm{SD}\left(\mathsf{H}^{f},\mathsf{H}^{g}\right)$. Let F_i to be the distribution of the i'th query to f in a random execution of H^{f}, and let Q to be the random variable of the queries of H^{f} in such a random execution.[3] It holds that

$$\Pr_{(q_1,\ldots,q_m)\leftarrow Q}\left[\exists i\in[m]\colon q_i\neq\perp\wedge F_i(q_i)>\gamma\cdot D_i(q_i)\right]=\Pr_{\langle\mathsf{A}^{(1)},\mathsf{B}\rangle}\left[\mathsf{desc}\left(\mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi}\right)\right].$$

Applying Lemma 2.4.5 with $k:=m$, $a:=2\xi+\Pr_{\langle\mathsf{A},\mathsf{B}\rangle}\left[\mathsf{desc}(\mathcal{S}\mathsf{mall}^{\delta,\mathsf{A}}_{\Pi})\right]$, $\lambda:=\gamma$ and $b:=\Pr_{\langle\mathsf{A}^{(1)},\mathsf{B}\rangle}\left[\mathsf{desc}\left(\mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi}\right)\right]$ yields the lemma. □

In the rest of this section we show how to guarantee that the probability of hitting the sets of unbalanced and low-value transcripts is small. Our first step is to relate these two sets – if a transcript is unbalanced, it is likely that it has a low-value prefix.

4.3 Visiting Unbalanced Nodes is Unlikely

Consider a node $u\in\mathcal{V}(\Pi)$ of some protocol $\Pi=(\mathsf{A},\mathsf{B})$. We want to see when u becomes unbalanced. Taking the edge distribution of $\left(\mathsf{A}^{(1)},\mathsf{B}\right)$, given in Claim 3.2.1, we get

$$\frac{\mathsf{v}_{(\mathsf{A}^{(1)},\mathsf{B})}(u)}{\mathsf{v}_{(\mathsf{A},\mathsf{B})}(u)}=\prod_{i\in\mathcal{C}^{\mathsf{A}}_{u}}\frac{\mathsf{val}(\Pi_{u_1,\ldots,i+1})}{\mathsf{val}(\Pi_{u_1,\ldots,i})},\tag{4.1}$$

[3]Informally, ignoring the $\perp$ queries, F_i is the distribution of the i'th query of $\mathsf{A}^{(1)}$ to $\mathsf{BiasedCont}$, and Q is the random variable of the queries of $\mathsf{A}^{(1)}$ of a random execution of $(\mathsf{A}^{(1)},\mathsf{B})$

where $i \in \mathcal{C}_u^{\mathsf{A}}$ iff $u_{1,\ldots,i}$ is controlled by A. Hence, for u to become unbalanced, one of the terms of the product of the right-hand side of Equation (4.1) must be large. This happens when the denominator of that term is small, i.e., when u has a low-value ancestor controlled by A.

The following key lemma formulates the above intuition, and shows that the biased-continuation attacker does not biased the original distribution of the attacked protocol by too much, unless it has previously visited a low-value node. To prove it we use a technical calculus fact, given in Lemma 2.5.2.

Lemma 4.3.1. *Let $\Pi = (\mathsf{A}, \mathsf{B})$ be a protocol and let $\mathsf{A}^{(1)}$ be as in Algorithm 3.1.2. Then for every $\delta \in (0, \frac{1}{2}]$, there exists a constant $c = c(\delta) > 0$ such that for every $\delta' \geq \delta$ and every $\gamma > 1$.*

$$\Pr_{\langle \mathsf{A}^{(1)}, \mathsf{B} \rangle} \left[\mathsf{desc}\left(\mathcal{U}\mathsf{nBal}_{\Pi}^{\gamma} \setminus \overline{\mathsf{desc}}\left(\mathcal{S}\mathsf{mall}_{\Pi}^{\delta', \mathsf{A}} \right) \right) \right] \leq \frac{2}{\gamma^c}.^{4}$$

Proof. We prove the lemma in the following three steps:

(1) We prove that for any such δ there exists $c > 0$, such that for every $\gamma > 1$ it holds that

$$\Pr_{\langle \mathsf{A}^{(1)}, \mathsf{B} \rangle} \left[\mathsf{desc}\left(\mathcal{U}\mathsf{nBal}_{\Pi}^{\gamma} \setminus \mathsf{desc}\left(\mathcal{S}\mathsf{mall}_{\Pi}^{\delta, \mathsf{A}} \right) \right) \right] \leq \frac{2 - \mathsf{val}(\Pi)}{\gamma^c}. \tag{4.2}$$

Note that Equation (4.2) only considers descendants of $\mathcal{S}\mathsf{mall}_{\Pi}^{\delta, \mathsf{A}}$, and not proper descendants, as the lemma stated.

(2) We show that if $\gamma > 1$, then

$$\mathsf{desc}\left(\mathcal{U}\mathsf{nBal}_{\Pi}^{\gamma} \setminus \overline{\mathsf{desc}}\left(\mathcal{S}\mathsf{mall}_{\Pi}^{\delta, \mathsf{A}} \right) \right) \subseteq \mathsf{desc}\left(\mathcal{U}\mathsf{nBal}_{\Pi}^{\gamma} \setminus \mathsf{desc}\left(\mathcal{S}\mathsf{mall}_{\Pi}^{\delta, \mathsf{A}} \right) \right).$$

[4] Recall that $\langle \Pi \rangle$, is the transcript induced by a random execution of Π, where $\mathsf{desc}(u)$ and $\overline{\mathsf{desc}}(u)$ are the descendants and the proper descendants of u as defined in Definition 2.2.1.

(3) Then we show that if $\delta' > \delta$, then $\mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi} \setminus \overline{\mathsf{desc}}\left(\mathcal{S}\mathsf{mall}^{\delta',\mathsf{A}}_{\Pi}\right) \subseteq \mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi} \setminus \overline{\mathsf{desc}}\left(\mathcal{S}\mathsf{mall}^{\delta,\mathsf{A}}_{\Pi}\right)$.

Combining the above steps yields (a stronger version of) the lemma.

Proof of (1): Fix some $\delta \in (0, \frac{1}{2}]$ and set $c := \alpha(\delta)$ from Lemma 2.5.2. The proof is by induction on the round complexity of Π.

Assume $\mathrm{round}(\Pi) = 0$ and let ℓ be the single leaf of Π. Note that if $\gamma > 1$, then $\ell \notin \mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi}$, and hence the set $\mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi}$ is empty. Thus, for every $\delta > 0$,

$$\Pr_{\langle \mathsf{A}^{(1)},\mathsf{B}\rangle}\left[\mathsf{desc}\left(\mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi} \setminus \mathsf{desc}(\mathcal{S}\mathsf{mall}^{\delta,\mathsf{A}}_{\Pi})\right)\right] = \Pr_{\langle \mathsf{A}^{(1)},\mathsf{B}\rangle}[\emptyset] = 0 \leq \frac{2 - \mathsf{val}(\mathsf{A},\mathsf{B})}{\gamma^c}.$$

Assume that Equation (4.2) holds for m-round protocols and that $\mathrm{round}(\Pi) = m + 1$. In case $e_{(\mathsf{A},\mathsf{B})}(\lambda, b) = 1$ for some $b \in \{0,1\}$, it holds that

$$\begin{aligned}
&\Pr_{\langle \mathsf{A}^{(1)},\mathsf{B}\rangle}\left[\mathsf{desc}\left(\mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi} \setminus \mathsf{desc}(\mathcal{S}\mathsf{mall}^{\delta,\mathsf{A}}_{\Pi})\right)\right] \\
&= \Pr_{\langle (\mathsf{A}^{(1)},\mathsf{B})_b\rangle}\left[\mathsf{desc}\left(\mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi_b} \setminus \mathsf{desc}(\mathcal{S}\mathsf{mall}^{\delta,\mathsf{A}}_{\Pi_b})\right)\right] \\
&= \Pr_{\langle \mathsf{A}^{(1)}_{\Pi_b},\mathsf{B}_{\Pi_b}\rangle}\left[\mathsf{desc}\left(\mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi_b} \setminus \mathsf{desc}(\mathcal{S}\mathsf{mall}^{\delta,\mathsf{A}}_{\Pi_b})\right)\right],
\end{aligned}$$

where the second equality follows Proposition 3.2.2. The proof now follows the induction hypothesis.

Assume $e_{(\mathsf{A},\mathsf{B})}(\lambda, b) \notin \{0,1\}$ for both $b \in \{0,1\}$, and let $p = e_{(\mathsf{A},\mathsf{B})}(\lambda, 0)$. The proof splits according to who controls the root of Π.

B controls $\mathsf{root}(\Pi)$. We first prove that

$$\mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi} \setminus \mathsf{desc}\left(\mathcal{S}\mathsf{mall}^{\delta,\mathsf{A}}_{\Pi}\right) \tag{4.3}$$

$$= \left(\mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi_0} \setminus \mathsf{desc}\left(\mathcal{S}\mathsf{mall}^{\delta,\mathsf{A}}_{\Pi_0}\right)\right) \cup \left(\mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi_1} \setminus \mathsf{desc}\left(\mathcal{S}\mathsf{mall}^{\delta,\mathsf{A}}_{\Pi_1}\right)\right). \tag{4.4}$$

Indeed, let $u \in \mathcal{V}(\Pi)$. First, note that since B controls $\mathsf{root}(\Pi)$ it holds that $e_{(\mathsf{A}^{(1)},\mathsf{B})}(\lambda, b) = e_{(\mathsf{A},\mathsf{B})}(\lambda, b)$, and thus if $u \neq \mathsf{root}(\Pi)$, it holds that $u \in \mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi}$ if and only if $u \in \mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi_b}$. Assume $u \in \mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi} \setminus \mathsf{desc}\left(\mathcal{S}\mathsf{mall}^{\delta,\mathsf{A}}_{\Pi}\right)$. Since $\gamma > 1$, it holds that $u \neq \mathsf{root}(\Pi)$, and thus $u \in \mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi_b}$. Moreover, it follows that $u_1, \ldots, u_{1,\ldots,|u|} \notin \mathcal{S}\mathsf{mall}^{\delta,\mathsf{A}}_{\Pi_b}$, and thus $u \in \mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi_b} \setminus \mathsf{desc}\left(\mathcal{S}\mathsf{mall}^{\delta,\mathsf{A}}_{\Pi_b}\right)$. For the other direction, assume $u \in \mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi_0} \setminus \mathsf{desc}\left(\mathcal{S}\mathsf{mall}^{\delta,\mathsf{A}}_{\Pi_b}\right)$. As argued before, it holds that $u \in \mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi}$. Moreover, if follows that $u_1, \ldots, u_{1,\ldots,|u|} \notin \mathcal{S}\mathsf{mall}^{\delta,\mathsf{A}}_{\Pi_b}$, and since B controls $\mathsf{root}(\Pi)$, it also holds that $\mathsf{root}(\Pi) \notin \mathcal{S}\mathsf{mall}^{\delta,\mathsf{A}}_{\Pi_b}$. Hence, $u \in \mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi} \setminus \mathsf{desc}\left(\mathcal{S}\mathsf{mall}^{\delta,\mathsf{A}}_{\Pi}\right)$. This complete the proof of Equation (4.3).

We write

$$
\begin{aligned}
&\Pr_{\langle \mathsf{A}^{(1)},\mathsf{B}\rangle}\left[\mathsf{desc}\left(\mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi} \setminus \mathsf{desc}\left(\mathcal{S}\mathsf{mall}^{\delta,\mathsf{A}}_{\Pi}\right)\right)\right] \\
&= e_{(\mathsf{A}^{(1)},\mathsf{B})}(\lambda, 0) \cdot \Pr_{\langle (\mathsf{A}^{(1)},\mathsf{B})_0\rangle}\left[\mathsf{desc}\left(\mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi_0} \setminus \mathsf{desc}(\mathcal{S}\mathsf{mall}^{\delta,\mathsf{A}}_{\Pi_0})\right)\right] \\
&\quad + e_{(\mathsf{A}^{(1)},\mathsf{B})}(\lambda, 1) \cdot \Pr_{\langle (\mathsf{A}^{(1)},\mathsf{B})_1\rangle}\left[\mathsf{desc}\left(\mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi_1} \setminus \mathsf{desc}(\mathcal{S}\mathsf{mall}^{\delta,\mathsf{A}}_{\Pi_1})\right)\right] \\
&= p \cdot \Pr_{\langle \mathsf{A}^{(1)}_{\Pi_0},\mathsf{B}_{\Pi_0}\rangle}\left[\mathsf{desc}\left(\mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi_0} \setminus \mathsf{desc}(\mathcal{S}\mathsf{mall}^{\delta,\mathsf{A}}_{\Pi_0})\right)\right] \\
&\quad + (1-p) \cdot \Pr_{\langle \mathsf{A}^{(1)}_{\Pi_1},\mathsf{B}_{\Pi_1}\rangle}\left[\mathsf{desc}\left(\mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi_1} \setminus \mathsf{desc}(\mathcal{S}\mathsf{mall}^{\delta,\mathsf{A}}_{\Pi_1})\right)\right] \\
&\leq p \cdot \frac{2 - \mathsf{val}(\Pi_0)}{\gamma^c} + (1-p) \cdot \frac{2 - \mathsf{val}(\Pi_1)}{\gamma^c} \\
&= \frac{2 - \mathsf{val}(\Pi)}{\gamma^c},
\end{aligned}
$$

where the first equality follows Equation (4.3), the second equality follows Proposition 3.2.2, and the inequality follows from the induction hypothesis.

A controls $\mathsf{root}(\Pi)$. In case $\mathsf{val}(\Pi) \leq \delta$, it holds that $\mathsf{root}(\Pi) \in \mathcal{S}\mathsf{mall}^{\delta,\mathsf{A}}_{\Pi}$. Therefore, $\mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi} \setminus \mathsf{desc}\left(\mathcal{S}\mathsf{mall}^{\delta,\mathsf{A}}_{\Pi}\right) = \emptyset$ and the proof follows similar argument as in the base case.

In the complementary case, i.e., $\mathsf{val}(\Pi) > \delta$, assume without loss of generality that $\mathsf{val}(\Pi_0) \geq \mathsf{val}(\Pi) \geq \mathsf{val}(\Pi_1) > 0$, where the case that $\mathsf{val}(\Pi_1) = 0$ is handled later. For $b \in \{0,1\}$, let $\gamma_b := \frac{\mathsf{val}(\Pi)}{\mathsf{val}(\Pi_b)} \cdot \gamma$. By Claim 3.2.1, for $u \in \mathcal{V}(\Pi)$ with $u \neq \mathsf{root}(\Pi)$ and $b = u_1$, it holds that

$$\frac{\mathsf{v}_{(\mathsf{A}^{(1)},\mathsf{B})}(u)}{\mathsf{v}_{(\mathsf{A},\mathsf{B})}(u)} = \frac{e_{(\mathsf{A},\mathsf{B})}(\lambda, b)}{e_{(\mathsf{A}^{(1)},\mathsf{B})}(\lambda, b)} \cdot \frac{\mathsf{v}_{(\mathsf{A}^{(1)},\mathsf{B})_b}(u)}{\mathsf{v}_{(\mathsf{A},\mathsf{B})_b}(u)} = \frac{\mathsf{val}(\Pi_b)}{\mathsf{val}(\Pi)} \cdot \frac{\mathsf{v}_{(\mathsf{A}^{(1)},\mathsf{B})_b}(u)}{\mathsf{v}_{(\mathsf{A},\mathsf{B})_b}(u)}.$$

Thus, $u \in \mathcal{U}\mathsf{nBal}_{\Pi}^{\gamma}$ if and only if $u \in \mathcal{U}\mathsf{nBal}_{\Pi_b}^{\gamma_b}$. Hence, using also the fact that $\mathsf{root}(\Pi) \notin \mathcal{S}\mathsf{mall}_{\Pi}^{\delta,\mathsf{A}}$ (since we assumed $\mathsf{val}(\Pi) > \delta$), similar arguments used to prove Equation (4.3) yields that

$$\mathcal{U}\mathsf{nBal}_{\Pi}^{\gamma} \setminus \mathsf{desc}\left(\mathcal{S}\mathsf{mall}_{\Pi}^{\delta,\mathsf{A}}\right) \tag{4.5}$$

$$= \left(\mathcal{U}\mathsf{nBal}_{\Pi_0}^{\gamma_0} \setminus \mathsf{desc}\left(\mathcal{S}\mathsf{mall}_{\Pi_0}^{\delta,\mathsf{A}}\right)\right) \cup \left(\mathcal{U}\mathsf{nBal}_{\Pi_1}^{\gamma_1} \setminus \mathsf{desc}\left(\mathcal{S}\mathsf{mall}_{\Pi_1}^{\delta,\mathsf{A}}\right)\right). \tag{4.6}$$

Moreover, we can write

$$\begin{aligned}
&\Pr_{\left\langle(\mathsf{A}^{(1)},\mathsf{B})_b\right\rangle}\left[\mathsf{desc}\left(\mathcal{U}\mathsf{nBal}_{\Pi_b}^{\gamma_b} \setminus \mathsf{desc}(\mathcal{S}\mathsf{mall}_{\Pi_b}^{\delta,\mathsf{A}})\right)\right] \qquad (4.7)\\
&= \Pr_{\left\langle\mathsf{A}_{\Pi_b}^{(1)},\mathsf{B}_{\Pi_b}\right\rangle}\left[\mathsf{desc}\left(\mathcal{U}\mathsf{nBal}_{\Pi_1}^{\gamma} \setminus \mathsf{desc}(\mathcal{S}\mathsf{mall}_{\Pi_1}^{\delta,\mathsf{A}})\right)\right]\\
&\leq \frac{2 - \mathsf{val}(\Pi_b)}{\gamma_b^c}\\
&= \left(\frac{\mathsf{val}(\Pi_b)}{\mathsf{val}(\Pi)}\right)^c \cdot \frac{2 - \mathsf{val}(\Pi_b)}{\gamma^c},
\end{aligned}$$

where the first equality follows Proposition 3.2.2, and the inequality follows the induction hypothesis in case $\gamma_b > 1$, and the fact that $\frac{2-\mathsf{val}(\Pi_b)}{\gamma_b^c} \geq 1$

otherwise. We have that

$$\begin{aligned}
&\Pr_{\langle \mathsf{A}^{(1)},\mathsf{B}\rangle}\left[\mathsf{desc}\left(\mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi}\setminus\mathsf{desc}\left(\mathcal{S}\mathsf{mall}^{\delta,\mathsf{A}}_{\Pi}\right)\right)\right]\\
&=e_{(\mathsf{A}^{(1)},\mathsf{B})}(\lambda,0)\cdot\Pr_{\langle (\mathsf{A}^{(1)},\mathsf{B})_0\rangle}\left[\mathsf{desc}\left(\mathcal{U}\mathsf{nBal}^{\gamma_0}_{\Pi_0}\setminus\mathsf{desc}\left(\mathcal{S}\mathsf{mall}^{\delta,\mathsf{A}}_{\Pi_0}\right)\right)\right]\\
&\quad+e_{(\mathsf{A}^{(1)},\mathsf{B})}(\lambda,1)\cdot\Pr_{\langle (\mathsf{A}^{(1)},\mathsf{B})_1\rangle}\left[\mathsf{desc}\left(\mathcal{U}\mathsf{nBal}^{\gamma_1}_{\Pi_1}\setminus\mathsf{desc}\left(\mathcal{S}\mathsf{mall}^{\delta,\mathsf{A}}_{\Pi_1}\right)\right)\right]\\
&\leq p\cdot\left(\frac{\mathsf{val}(\Pi_0)}{\mathsf{val}(\Pi)}\right)^{1+c}\cdot\frac{2-\mathsf{val}(\Pi_0)}{\gamma^c}+(1-p)\cdot\left(\frac{\mathsf{val}(\Pi_1)}{\mathsf{val}(\Pi)}\right)^{1+c}\cdot\frac{2-\mathsf{val}(\Pi_1)}{\gamma^c},
\end{aligned}$$

where the equality follows Equation (4.5), and the inequality follows Equation (4.7) together with Claim 3.2.1. Setting $\frac{\mathsf{val}(\Pi_0)}{\mathsf{val}(\Pi)}:=1+y$, $x:=\mathsf{val}(\Pi)$ and $\lambda:=\frac{p}{1-p}$ and noticing that $\lambda y=\left(\frac{\mathsf{val}(\Pi_0)}{\mathsf{val}(\Pi)}-1\right)\cdot\frac{p}{1-p}=\frac{p\cdot\mathsf{val}(\Pi_0)-p\cdot\mathsf{val}(\Pi)}{\mathsf{val}(\Pi)-p\cdot\mathsf{val}(\Pi)}\leq\frac{p\cdot\mathsf{val}(\Pi_0)}{\mathsf{val}(\Pi)}\leq 1$, we can use Lemma 2.5.2 and have the following inequality (after multiplying by $\frac{1-p}{\gamma^c}$), which completes the proof for the case that $\mathsf{val}(\Pi_1)>0$:

$$\begin{aligned}
p\cdot\left(\frac{\mathsf{val}(\Pi_0)}{\mathsf{val}(\Pi)}\right)^{1+c}\cdot\frac{2-\mathsf{val}(\Pi_0)}{\gamma^c}+(1-p)\cdot\left(\frac{\mathsf{val}(\Pi_1)}{\mathsf{val}(\Pi)}\right)^{1+c}\cdot\frac{2-\mathsf{val}(\Pi_1)}{\gamma^c}&\\
\leq\frac{2-\mathsf{val}(\Pi)}{\gamma^c}.&
\end{aligned}$$

It is left to argue for the case that $\mathsf{val}(\Pi_1)=0$. In this case, according to Claim 3.2.1, is holds that $e_{(\mathsf{A}^{(1)},\mathsf{B})}(\lambda,0)=1$ and $e_{(\mathsf{A}^{(1)},\mathsf{B})}(\lambda,1)=0$. Hence, there are no unbalanced nodes in Π_1, i.e., $\mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi}\setminus\mathsf{desc}\left(\mathcal{S}\mathsf{mall}^{\delta,\mathsf{A}}_{\Pi}\right)\cap\mathcal{V}(\Pi_1)=\emptyset$. As before, let $\gamma_0:=\frac{\mathsf{val}(\Pi)}{\mathsf{val}(\Pi_0)}\cdot\gamma=p\cdot\gamma$. Similar arguments used to prove Equation (4.5) yields that

$$\mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi}\setminus\mathsf{desc}\left(\mathcal{S}\mathsf{mall}^{\delta,\mathsf{A}}_{\Pi}\right)=\mathcal{U}\mathsf{nBal}^{\gamma_0}_{\Pi_0}\setminus\mathsf{desc}\left(\mathcal{S}\mathsf{mall}^{\delta,\mathsf{A}}_{\Pi_0}\right)$$

It holds that

$$\begin{aligned}
&\Pr_{\langle \mathsf{A}^{(1)},\mathsf{B}\rangle}\left[\mathsf{desc}\left(\mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi}\setminus \mathsf{desc}\left(\mathcal{S}\mathsf{mall}^{\delta,\mathsf{A}}_{\Pi}\right)\right)\right]\\
&= e_{(\mathsf{A}^{(1)},\mathsf{B})}(\lambda,0)\cdot \Pr_{\langle (\mathsf{A}^{(1)},\mathsf{B})_0\rangle}\left[\mathsf{desc}\left(\mathcal{U}\mathsf{nBal}^{\gamma_0}_{\Pi_0}\setminus \mathsf{desc}\left(\mathcal{S}\mathsf{mall}^{\delta,\mathsf{A}}_{\Pi_0}\right)\right)\right]\\
&\leq \left(\frac{1}{p}\right)^{1+c}\cdot\frac{2-\mathsf{val}(\Pi_0)}{\gamma^c}.
\end{aligned}$$

Applying Lemma 2.5.2 with the same parameters as above, completes the proof.

Proof of (2): We prove the statement by showing that in case $\gamma > 1$ it holds that

$$\mathsf{frnt}\left(\mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi}\setminus \overline{\mathsf{desc}}\left(\mathcal{S}\mathsf{mall}^{\delta,\mathsf{A}}_{\Pi}\right)\right)\subseteq \mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi}\setminus \mathsf{desc}\left(\mathcal{S}\mathsf{mall}^{\delta,\mathsf{A}}_{\Pi}\right).^{5}$$

Let $u\in \mathsf{frnt}\left(\mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi}\setminus \overline{\mathsf{desc}}\left(\mathcal{S}\mathsf{mall}^{\delta,\mathsf{A}}_{\Pi}\right)\right)$. It holds that for every $i\in(|u|-1)$, it holds that $u_{1\ldots i}\notin \mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi}\cup\mathcal{S}\mathsf{mall}^{\delta,\mathsf{A}}_{\Pi}$ (note that this includes the root). We complete the proof by showing that $u\notin\mathcal{S}\mathsf{mall}^{\delta,\mathsf{A}}_{\Pi}$.

Since $\gamma>1$, it must be the case that $u\neq\mathsf{root}(\Pi)$. Hence, u has a parent in $\mathcal{T}(\Pi)$, and let w denote this parent. Since $w\notin\mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi}$, it holds that $\mathsf{v}_{(\mathsf{A}^{(1)},\mathsf{B})}(w)<\gamma\cdot\mathsf{v}_{(\mathsf{A},\mathsf{B})}(w)$. We write

$$\begin{aligned}
\gamma\cdot\mathsf{v}_{(\mathsf{A},\mathsf{B})}(w)\cdot e_{(\mathsf{A}^{(1)},\mathsf{B})}(w,u) &> \mathsf{v}_{(\mathsf{A}^{(1)},\mathsf{B})}(w)\cdot e_{(\mathsf{A}^{(1)},\mathsf{B})}(w,u)\\
&= \mathsf{v}_{(\mathsf{A}^{(1)},\mathsf{B})}(u)\\
&\geq \gamma\cdot\mathsf{v}_{(\mathsf{A},\mathsf{B})}(u)\\
&= \gamma\cdot\mathsf{v}_{(\mathsf{A},\mathsf{B})}(w)\cdot e_{(\mathsf{A},\mathsf{B})}(w,u).
\end{aligned}$$

[5]Recall that for a set $\mathcal{S}\subset\mathcal{V}(\Pi)$, $\mathsf{frnt}\,(\mathcal{S})$ stands the frontier of $\mathcal{S}$, i.e., the set of nodes belong to $\mathcal{S}$, whose ancestors do not belong to $\mathcal{S}$.

Hence, $e_{(\mathsf{A},\mathsf{B})}(w,u) < e_{(\mathsf{A}^{(1)},\mathsf{B})}(w,u)$. It follows that A controls w. By Claim 3.2.1, it holds that $e_{(\mathsf{A}^{(1)},\mathsf{B})}(w,u) = e_{(\mathsf{A},\mathsf{B})}(w,u) \cdot \frac{\mathsf{val}(\Pi_u)}{\mathsf{val}(\Pi_w)}$, and thus $\mathsf{val}(\Pi_u) > \mathsf{val}(\Pi_w)$. But since $w \notin \mathcal{S}\mathsf{mall}_{\Pi}^{\delta,\mathsf{A}}$, it holds that $\mathsf{val}(\Pi_w) > \delta$, and hence $\mathsf{val}(\Pi_u) > \delta$, as required.

Proof of (3): Note that for every $\delta' \geq \delta$ it holds that $\mathcal{S}\mathsf{mall}_{\Pi}^{\delta,\mathsf{A}} \subseteq \mathcal{S}\mathsf{mall}_{\Pi}^{\delta',\mathsf{A}}$. Hence, $\mathcal{U}\mathsf{nBal}_{\Pi}^{\gamma} \setminus \overline{\mathsf{desc}}(\mathcal{S}\mathsf{mall}_{\Pi}^{\delta',\mathsf{A}}) \subseteq \mathcal{U}\mathsf{nBal}_{\Pi}^{\gamma} \setminus \overline{\mathsf{desc}}(\mathcal{S}\mathsf{mall}_{\Pi}^{\delta,\mathsf{A}})$, and the proof follows.

□

The above lemma allows us to argue that if the probability of hitting low-value nodes is small, then the biased-continuation attacker does not change the leaves distribution by much. Consider the process in which a transcript u is generated by $(\mathsf{A}^{(1)},\mathsf{B})$. If this process first generates an unbalanced node, then the probability of hitting u is bounded by Lemma 4.3.1. If it first generates a low-value node, then the probability of hitting u is bounded by the probability of hitting low-value nodes. If neither of the above cases apply, then u is a balanced transcript, and the probability of hitting it can be bounded by the probability of (A,B) hitting u.

Formally, the above intuition is captured in the next lemma.

Corollary 4.3.2. *Let $\Pi = (\mathsf{A},\mathsf{B})$ be an m-round protocol, let $\mathcal{S} \subseteq \mathcal{V}(\Pi)$, let $\delta \in (0,\frac{1}{2}]$ and let $c = c(\delta)$ from Lemma 4.3.1.*

Then, for every $\delta' \geq \delta$ and every $\gamma > 1$, it holds that

$$\Pr_{\langle \mathsf{A}^{(1)},\mathsf{B}\rangle}\left[\mathsf{desc}\left(\mathcal{S}\right)\right] \leq \gamma \cdot \Pr_{\langle \mathsf{A},\mathsf{B}\rangle}\left[\mathsf{desc}\left(\left(\mathcal{S} \cup \mathcal{S}\mathsf{mall}_{\Pi}^{\delta',\mathsf{A}}\right) \setminus \mathsf{desc}\left(\mathcal{U}\mathsf{nBal}_{\Pi}^{\gamma}\right)\right)\right] + \frac{2}{\gamma^c}.$$

Proof. Fix $\delta' \geq \delta$, $\gamma > 1$. We start by showing that

$$\mathsf{desc}\left(\mathcal{S}\right) \subseteq \mathsf{desc}\left(\left(\mathsf{frnt}\left(\mathcal{S}\right) \cup \mathcal{S}\mathsf{mall}_{\Pi}^{\delta',\mathsf{A}}\right) \setminus \mathsf{desc}\left(\mathcal{U}\mathsf{nBal}_{\Pi}^{\gamma}\right)\right) \tag{4.8}$$

$$\cup \mathsf{desc}\left(\mathcal{U}\mathsf{nBal}_{\Pi}^{\gamma} \setminus \overline{\mathsf{desc}}\left(\mathcal{S}\mathsf{mall}_{\Pi}^{\delta',\mathsf{A}}\right)\right). \tag{4.9}$$

Let $u \in \mathsf{desc}(\mathcal{S})$ and let $v \in \mathsf{frnt}(\mathcal{S})$ such that $u \in \mathsf{desc}(v)$. If $v \in \mathsf{desc}\left(\mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi} \setminus \overline{\mathsf{desc}}\left(\mathcal{S}\mathsf{mall}^{\delta',\mathsf{A}}_{\Pi}\right)\right)$ we are done. Hence, assume that $v \notin \mathsf{desc}\left(\mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi} \setminus \overline{\mathsf{desc}}\left(\mathcal{S}\mathsf{mall}^{\delta',\mathsf{A}}_{\Pi}\right)\right)$. If $v \in \mathsf{desc}\left(\mathcal{S}\mathsf{mall}^{\delta',\mathsf{A}}_{\Pi}\right)$, and letting $w \in \mathsf{frnt}\left(\mathcal{S}\mathsf{mall}^{\delta',\mathsf{A}}_{\Pi}\right)$ such that $v \in \mathsf{desc}(w)$, then it must be that $w \notin \mathsf{desc}(\mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi})$, since otherwise it would follow that $v \in \mathsf{desc}\left(\mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi} \setminus \overline{\mathsf{desc}}\left(\mathcal{S}\mathsf{mall}^{\delta',\mathsf{A}}_{\Pi}\right)\right)$. Hence, it this case, it holds that $v \in \mathsf{desc}\left(\mathcal{S}\mathsf{mall}^{\delta',\mathsf{A}}_{\Pi} \setminus \mathsf{desc}(\mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi})\right)$. If $v \notin \mathsf{desc}\left(\mathcal{S}\mathsf{mall}^{\delta',\mathsf{A}}_{\Pi}\right)$, then it must be that $v \notin \mathsf{desc}(\mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi})$, since otherwise it would follow that $v \in \mathsf{desc}\left(\mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi} \setminus \overline{\mathsf{desc}}\left(\mathcal{S}\mathsf{mall}^{\delta',\mathsf{A}}_{\Pi}\right)\right)$. Hence, in this case, it holds that $u \in \mathsf{desc}(\mathcal{S} \setminus \mathsf{desc}(\mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi}))$. This concludes the proof of Equation (4.8).

We get

$$\begin{aligned}\Pr_{\langle \mathsf{A}^{(1)},\mathsf{B}\rangle}[\mathsf{desc}(\mathcal{S})] &\leq \Pr_{\langle \mathsf{A}^{(1)},\mathsf{B}\rangle}\left[\mathsf{desc}\left(\left(\mathsf{frnt}(\mathcal{S}) \cup \mathcal{S}\mathsf{mall}^{\delta',\mathsf{A}}_{\Pi}\right) \setminus \mathsf{desc}(\mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi})\right)\right] \\ &\quad + \Pr_{\langle \mathsf{A}^{(1)},\mathsf{B}\rangle}\left[\mathsf{desc}\left(\mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi} \setminus \overline{\mathsf{desc}}\left(\mathcal{S}\mathsf{mall}^{\delta',\mathsf{A}}_{\Pi}\right)\right)\right] \\ &\leq \gamma \cdot \Pr_{\langle \mathsf{A},\mathsf{B}\rangle}\left[\mathsf{desc}\left(\left(\mathcal{S} \cup \mathcal{S}\mathsf{mall}^{\delta',\mathsf{A}}_{\Pi}\right) \setminus \mathsf{desc}(\mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi})\right)\right] + \frac{2}{\gamma^c},\end{aligned}$$

where the first inequality follows Equation (4.8) and the second inequality follows the definition of $\mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi}$ (Definition 4.2.4) and Lemma 4.3.1. □

In the rest of the section we need bounds for some special cases of the above corollary, given in the next proposition.

Proposition 4.3.3. *Let $\Pi = (\mathsf{A}, \mathsf{B})$ be an m-round protocol, let $\delta \in (0, \frac{1}{2}]$ and let $c = c(\delta)$ from Lemma 4.3.1. Then the following holds for any $\delta' \geq \delta$:*

1. *For any $\gamma > 1$ it holds that*

$$\Pr_{\langle \mathsf{A}^{(1)},\mathsf{B}\rangle}\left[\mathsf{desc}\left(\mathcal{S}\mathsf{mall}^{\delta',\mathsf{A}}_{\Pi}\right)\right] \leq \gamma \cdot \Pr_{\langle \mathsf{A},\mathsf{B}\rangle}\left[\mathsf{desc}\left(\mathcal{S}\mathsf{mall}^{\delta',\mathsf{A}}_{\Pi}\right)\right] + \frac{2}{\gamma^c}.$$

and

$$\Pr_{\langle \mathsf{A}^{(1)},\mathsf{B}\rangle}\left[\mathsf{desc}\left(\mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi}\right)\right] \leq \gamma \cdot \Pr_{\langle \mathsf{A},\mathsf{B}\rangle}\left[\mathsf{desc}\left(\mathcal{S}\mathsf{mall}^{\delta',\mathsf{A}}_{\Pi}\right)\right] + \frac{2}{\gamma^{c}}.$$

2. *Let* $\mathcal{S} \subseteq \mathcal{V}(\Pi)$ *with* $\Pr_{\langle \mathsf{A},\mathsf{B}\rangle}\left[\mathsf{desc}\left(\mathcal{S}\right)\right] \leq \alpha$*. If* $\mathcal{S}\mathsf{mall}^{\delta',\mathsf{A}}_{\Pi} = \emptyset$*, then for every* $k \in \mathbb{N}$ *and any* $\gamma_1, \ldots, \gamma_k > 1$ *it holds that*

$$\Pr_{\langle \mathsf{A}^{(k)},\mathsf{B}\rangle}\left[\mathsf{desc}\left(\mathcal{S}\right)\right] \leq \alpha \cdot \prod_{i=1}^{k}\gamma_i + 2 \cdot \sum_{i=1}^{k}\frac{\cdot \prod_{j=i+1}^{k}\gamma_j}{\gamma_i^{c}} := \phi^{\mathsf{Bal}}(\alpha, \delta', \boldsymbol{\gamma}).$$

Proof. Item 1 follows by applying Corollary 4.3.2 with respect to sets $\mathsf{desc}\left(\mathcal{S}\mathsf{mall}^{\delta',\mathsf{A}}_{\Pi}\right)$ and $\mathsf{desc}\left(\mathcal{U}\mathsf{nBal}^{\gamma}_{\Pi}\right)$. Item 2 follows by induction and Corollary 4.3.2. □

The above proposition bounds the probability of hitting unbalanced nodes by using the probability of hitting A-controlled low-value nodes. Recall that in Section 4.2 we showed that the approximated biased-continuation attacker does almost as well as biased-continuation attacker, if the probability of hitting unbalanced and A-controlled low-value nodes is small. Hence, using the above proposition, we can now argue that the approximated biased-continuation attacker does well if the probability of hitting A-controlled low-value nodes is small.

Corollary 4.3.4. *Let* $\Pi = (\mathsf{A}, \mathsf{B})$ *be a* m*-round protocol, let* $\delta \in (0, \frac{1}{2}]$ *and let* $c = c(\delta)$ *from Lemma 4.3.1. Then for every* $\gamma \geq 1$ *it holds that*

$$\mathrm{SD}\left(\left[\mathsf{A}^{(1)}, \mathsf{B}\right], \left[\mathsf{A}^{(1,\widetilde{\mathsf{BiasedCont}})}, \mathsf{B}\right]\right) \leq 2 \cdot m \cdot \gamma \cdot \left(\xi + \Pr_{\langle \mathsf{A},\mathsf{B}\rangle}\left[\mathsf{desc}(\mathcal{S}\mathsf{mall}^{\delta,\mathsf{A}}_{\Pi})\right]\right) + \frac{2}{\gamma^{c}},$$

where $\widetilde{\mathsf{BiasedCont}}$ *is a* (ξ, δ)*-biased-continuator for* Π *according to Definition 4.2.1.*

Proof. Follows immediately from Lemma 4.2.5 and Proposition 4.3.3. □

Unfortunately, there might be protocols for which the probability of hitting A-controlled low-value nodes is large. Hence, the above corollary does not suffice to argue that the approximated biased-continuation attacker successfully biases any protocol. However, given any protocol, we can define a pruned variant of it, such that the probability of hitting A-controlled low-value nodes is indeed small. Thus, the above corollary shows that the biased-continuation attacker successfully biases the above variant. The definition of the pruned variant and the analysis of it is given in the next section.

4.4 Approximated Biased-Continuation Attack on Pruned Protocols

We are now ready to define the pruned variant of a protocol. Recall that Lemma 4.3.1 shows that in case the protocol has no low value node that are in A's control, biased-continuation attack does not change the leaves distribution by much. For a protocol $\Pi = (\mathsf{A}, \mathsf{B})$, the pruned variant of Π will keep the leaves distribution intact, while changing the controlling scheme of the protocol – for low value nodes it will give the control to B, and for high value nodes it will give the control to A. Hence, Lemma 4.3.1 assures that biased continuation will not change the leaves distribution of the pruned protocol by much.

We give both ideal and approximated variants.

Pruning Protocols

Ideally Pruned Protocols

Definition 4.4.1 (the pruned variant of a protocol)**.** *Let* $\Pi = (\mathsf{A}, \mathsf{B})$ *be a* m*-round protocol and let* $\delta \in (0,1)$*. In the* δ-pruned variant of Π*, denoted by* $\Pi^{[\delta]} = \left(\mathsf{A}_{\Pi}^{[\delta]}, \mathsf{B}_{\Pi}^{[\delta]}\right)$*, the parties follow the protocol* Π*, where* $\mathsf{A}_{\Pi}^{[\delta]}$ *and* $\mathsf{B}_{\Pi}^{[\delta]}$ *take the roles of* A *and* B *respectively, with the following exception occurring the* first time *the protocol's transcript* u *is in* $\mathcal{S}\mathsf{mall}_{\Pi}^{\delta} \cup \mathcal{L}\mathsf{arge}_{\Pi}^{\delta}$*:*

If $u \in \mathcal{L}\mathsf{arge}_{\Pi}^{\delta}$ *set* $\mathsf{C} = \mathsf{A}_{\Pi}^{[\delta]}$*, otherwise set* $\mathsf{C} = \mathsf{B}_{\Pi}^{[\delta]}$*. The party* C *takes control of the node* u*, samples a leaf* $\ell \leftarrow \langle \Pi \rangle$ *conditioned on* $\ell_{1,\ldots,|u|} = u$*, and then, bit by bit, sends* $\ell_{|u|+1,\ldots,m}$ *to the other party.*[6]

Namely, for the first time the value of the protocol is close to either 1 or 0, the party who is interested in this value (i.e., A^{δ} for one, and B^{δ} for zero), is taking control and deciding the outcome (without changing the value of the protocol). Hence, the protocol is effectively pruned at these leaves (each such node is effectively a parent of two leaves).

Approximately Pruned Protocols

Definition 4.4.2 (Approximated honest continuation)**.** *Algorithm* $\widetilde{\mathsf{HonCont}}$ *is a* ξ-Honest continuator *for* Π*, if*
$\Pr_{\ell \leftarrow \langle \Pi \rangle}\left[\exists i \in [m] \colon \mathrm{SD}\left(\widetilde{\mathsf{HonCont}}(\ell_{1,\ldots,i}), \mathsf{HonCont}(\ell_{1,\ldots,i})\right) > \xi\right] \leq \xi$*, where* $\mathsf{HonCont}(u)$*, for* $u \in \mathcal{V}(\Pi)$*, returns* $\ell \leftarrow \langle \Pi_u \rangle$*.*

[6]Note that in the pruned protocol, the parties turns might not alternate (i.e., the same party might sends several consecutive bits), even if they do alternate in the original protocol. Rather, the protocol's control scheme (determining what party is active at a given point) is ia function of the protocol's transcript and the original protocol scheme. Such schemes are consistent with the ones considered in the previous sections.

Definition 4.4.3 (Approximated estimator)**.** *An Algorithm* $\widetilde{\mathsf{Est}}$ *is a* (ξ,δ)-estimator *for an* m*-round protocol* Π*, if it is deterministic and* $\Pr_{\ell\leftarrow\langle\Pi\rangle}\left[\exists i\in[m]\colon\ \left|\widetilde{\mathsf{Est}}(\ell_{1,\ldots,i})-\mathsf{val}(\Pi_{\ell_{1,\ldots,i}})\right|>\delta\right]\leq\xi$.

The approximately pruned protocol is the oracle variant of the above protocol.

Definition 4.4.4. *Let* Π *be a protocol,* $\delta\in[0,1]$ *and let* $\widetilde{\mathsf{Est}}$ *be a deterministic real value algorithm. Let*

- $\widetilde{\mathcal{S}\mathsf{mall}}_{\Pi}^{\delta,\widetilde{\mathsf{Est}}}=\left\{u\in\mathcal{V}(\Pi)\colon\widetilde{\mathsf{Est}}(u)\leq\delta\right\}$.
- $\widetilde{\mathcal{L}\mathsf{arge}}_{\Pi}^{\delta,\widetilde{\mathsf{Est}}}=\left\{u\in\mathcal{V}(\Pi)\colon\widetilde{\mathsf{Est}}(u)\geq1-\delta\right\}$.

Definition 4.4.5 (the approximately pruned variant of a protocol)**.** *Let* $\Pi=(\mathsf{A},\mathsf{B})$ *be a* m*-round protocol, let* $\delta_1<\delta_2\in(0,1)$*, let* $\widetilde{\mathsf{HonCont}}$ *be an algorithm, and let* $\widetilde{\mathsf{Est}}$ *and be a deterministic real value algorithm. Let* $\mathcal{F}=\mathsf{frnt}\left(\widetilde{\mathcal{L}\mathsf{arge}}_{\Pi}^{\delta,\widetilde{\mathsf{Est}}}\cup\widetilde{\mathcal{S}\mathsf{mall}}_{\Pi}^{\delta,\widetilde{\mathsf{Est}}}\right)$*. The* $(\delta,\widetilde{\mathsf{Est}},\widetilde{\mathsf{HonCont}})$-approximately pruned variant of Π*, denoted* $\Pi^{[\delta,\widetilde{\mathsf{Est}},\widetilde{\mathsf{HonCont}}]}=\left(\mathsf{A}_{\Pi}^{[\delta,\widetilde{\mathsf{Est}},\widetilde{\mathsf{HonCont}}]},\mathsf{B}_{\Pi}^{[\delta,\widetilde{\mathsf{Est}},\widetilde{\mathsf{HonCont}}]}\right)$*, is defined as follows. For* $u\in\mathcal{V}(\Pi)\setminus\mathsf{desc}\left(\mathcal{F}\right)$*, the party* $\mathsf{cntrl}_{\Pi}(u)$ *sends the bit* $\widetilde{\mathsf{HonCont}}(u)_{|u|+1}$ *to the other party. For* $u\in\mathcal{F}$*,* C *stores* $\mathrm{state}=\widetilde{\mathsf{HonCont}}(w)$ *and for every* $w\in\mathsf{desc}\left(\mathcal{F}\right)$*,* C *sends* $\mathrm{state}_{|w|+1}$*, where*

$$\mathsf{C}=\begin{cases}\mathsf{A}, & u\in\mathsf{desc}\left(\widetilde{\mathcal{L}\mathsf{arge}}_{\Pi}^{\delta,\widetilde{\mathsf{Est}}}\setminus\mathsf{desc}\left(\widetilde{\mathcal{S}\mathsf{mall}}_{\Pi}^{\delta,\widetilde{\mathsf{Est}}}\right)\right)\\ \mathsf{B}, & u\in\mathsf{desc}\left(\widetilde{\mathcal{S}\mathsf{mall}}_{\Pi}^{\delta,\widetilde{\mathsf{Est}}}\setminus\mathsf{desc}\left(\widetilde{\mathcal{L}\mathsf{arge}}_{\Pi}^{\delta,\widetilde{\mathsf{Est}}}\right)\right)\end{cases}$$

Namely, until reaching a node in $\widetilde{\mathcal{S}\mathsf{mall}}_{\Pi}^{\delta,\widetilde{\mathsf{Est}}}\cup\widetilde{\mathcal{L}\mathsf{arge}}_{\Pi}^{\delta,\widetilde{\mathsf{Est}}}$, the parties act like in Π (same party sends each message), but using the oracle $\widetilde{\mathsf{HonCont}}$ instead of their random coins, which make them stateless. Once hitting a node in $\widetilde{\mathcal{S}\mathsf{mall}}_{\Pi}^{\delta,\widetilde{\mathsf{Est}}}\cup\widetilde{\mathcal{L}\mathsf{arge}}_{\Pi}^{\delta,\widetilde{\mathsf{Est}}}$ for the first time, the control moves (and stays with) A in case $u\in$

$\widetilde{\mathcal{L}\mathsf{arge}}_{\Pi}^{\delta,\widetilde{\mathsf{Est}}}$, or with B in case $u \in \widetilde{\mathcal{S}\mathsf{mall}}_{\Pi}^{\delta,\widetilde{\mathsf{Est}}}$. The party taking the control, stores the response from the oracle $\widetilde{\mathsf{HonCont}}$ and sends bit by bit all the remaining bits as directed by this stored value (notice that it also sends the bits that would have been sent by the other party).

The next lemma states that if there are not too many nodes with values close to the point of pruning, and the oracle given to the parties are close to their ideal version, then the approximate pruned variant of the protocol is close to ideal one.

Definition 4.4.6. *For a protocol* Π, $\xi \in (0,1)$, $\delta \in (0, \frac{1}{2}]$, *let*

$$\mathcal{N}\mathsf{eigh}_{\Pi}^{\delta,\xi} = \{u \in \mathcal{V}(\Pi) \colon \mathsf{val}(\Pi_u) \in (\delta \pm \xi] \vee \mathsf{val}(\Pi_u) \in [1-\delta \pm \xi)\}\,,$$

and let $\mathsf{neigh}_{\Pi}(\delta,\xi) = \Pr_{\langle\Pi\rangle}\left[\mathsf{desc}\left(\mathcal{N}\mathsf{eigh}_{\Pi}^{\delta,\xi}\right)\right]$.

Lemma 4.4.7. *Let* $\Pi = (\mathsf{A},\mathsf{B})$ *be* m*-round protocol, let* $\bar{\xi} \in (0,1)$ *and let* $\delta,\xi \in (0,\frac{1}{2}]$. *Assume that* $\widetilde{\mathsf{Est}}$ *is a deterministic* $(\bar{\xi},\xi)$*-estimator for* Π *and that* $\widetilde{\mathsf{HonCont}}$ *is a* ξ'*-honest continuator for* Π *according to Definitions 4.4.2 and 4.4.3, then*

$$\mathrm{SD}\left(\left[\mathsf{A}_{\Pi}^{[\delta]},\mathsf{B}_{\Pi}^{[\delta]}\right],\left[\mathsf{A}_{\Pi}^{[\delta,\widetilde{\mathsf{Est}},\widetilde{\mathsf{HonCont}}]},\mathsf{B}_{\Pi}^{[\delta,\widetilde{\mathsf{Est}},\widetilde{\mathsf{HonCont}}]}\right]\right) \leq \mathsf{neigh}_{\Pi}(\delta,\xi) + \bar{\xi} + 2\cdot m\cdot \xi'.$$

Proof. In the first step we show that

$$d_1 := \mathrm{SD}\left(\left[\mathsf{A}_{\Pi}^{[\delta]},\mathsf{B}_{\Pi}^{[\delta]}\right],\left[\mathsf{A}_{\Pi}^{[\delta,\widetilde{\mathsf{Est}},\mathsf{HonCont}]},\mathsf{B}_{\Pi}^{[\delta,\widetilde{\mathsf{Est}},\mathsf{HonCont}]}\right]\right) \leq \mathsf{neigh}_{\Pi}(\delta,\xi) + \bar{\xi}.$$

Let $\mathcal{F}\mathsf{ail}_{\Pi}^{\xi,\widetilde{\mathsf{Est}}} = \left\{u \in \mathcal{V}(\Pi) \colon \left|\mathsf{val}(\Pi_u) - \widetilde{\mathsf{Est}}(u)\right| > \xi\right\}$). Since $\widetilde{\mathsf{Est}}$ is a $(\bar{\xi},\xi)$-estimator for Π, it holds that $\mathsf{fail}_{\Pi}^{\widetilde{\mathsf{Est}}}(\xi) := \Pr_{\langle\Pi\rangle}\left[\mathsf{desc}\left(\mathcal{F}\mathsf{ail}_{\Pi}^{\xi,\widetilde{\mathsf{Est}}}\right)\right] \leq \bar{\xi}$, and let $\mathcal{N}\mathsf{eigh}_{\Pi}^{\delta,\xi}$ and $\mathsf{neigh}_{\Pi}(\delta,\xi)$ be according to Definition 4.4.6.

Note that both $\left(\mathsf{A}_{\Pi}^{[\delta]},\mathsf{B}_{\Pi}^{[\delta]}\right)$ and $\left(\mathsf{A}_{\Pi}^{[\delta,\widetilde{\mathsf{Est}},\mathsf{HonCont}]},\mathsf{B}_{\Pi}^{[\delta,\widetilde{\mathsf{Est}},\mathsf{HonCont}]}\right)$ randomly executes Π. The former diverts from this execution in case it reaches a node u such that

$u \in \mathcal{S}\mathsf{mall}_{\Pi}^{\delta} \cup \mathcal{L}\mathsf{arge}_{\Pi}^{\delta}$, where the latter diverts in case $u \in \widetilde{\mathcal{S}\mathsf{mall}}_{\Pi}^{\delta,\widetilde{\mathsf{Est}}} \cup \widetilde{\mathcal{L}\mathsf{arge}}_{\Pi}^{\delta,\widetilde{\mathsf{Est}}}$. Claim 4.4.8 shows that if $u \notin \mathcal{N}\mathsf{eigh}_{\Pi}^{\delta,\xi} \cup \mathcal{F}\mathsf{ail}_{\Pi}^{\xi,\widetilde{\mathsf{Est}}}$, both protocols diverts at the same point, both call for $\mathsf{HonCont}(u)$ to determined the rest of the execution, and both give the control to the same party. Thus, it holds that

$$\begin{aligned} d_1 &\leq \Pr_{\langle \Pi \rangle}\left[\mathsf{desc}\left(\mathcal{N}\mathsf{eigh}_{\Pi}^{\delta,\xi}\right) \cup \mathsf{desc}\left(\mathcal{F}\mathsf{ail}_{\Pi}^{\xi,\widetilde{\mathsf{Est}}}\right)\right] \\ &\leq \Pr_{\langle \Pi \rangle}\left[\mathsf{desc}\left(\mathcal{N}\mathsf{eigh}_{\Pi}^{\delta,\xi}\right)\right] + \Pr_{\langle \Pi \rangle}\left[\mathsf{desc}\left(\mathcal{F}\mathsf{ail}_{\Pi}^{\xi,\widetilde{\mathsf{Est}}}\right)\right] \\ &= \mathsf{neigh}_{\Pi}(\delta,\xi) + \bar{\xi}. \end{aligned}$$

In the next step we conclude the proof by using Lemma 2.4.5 to show that

$$d_2 := \mathrm{SD}\left(\left[\mathsf{A}_{\Pi}^{[\delta,\widetilde{\mathsf{Est}},\mathsf{HonCont}]}, \mathsf{B}_{\Pi}^{[\delta,\widetilde{\mathsf{Est}},\mathsf{HonCont}]}\right], \left[\mathsf{A}_{\Pi}^{[\delta,\widetilde{\mathsf{Est}},\widetilde{\mathsf{HonCont}}]}, \mathsf{B}_{\Pi}^{[\delta,\widetilde{\mathsf{Est}},\widetilde{\mathsf{HonCont}}]}\right]\right) \leq 2 \cdot m \cdot \xi'.$$

Let $\mathsf{E}^{\mathsf{HonCont}}$ [resp., $\mathsf{E}^{\widetilde{\mathsf{HonCont}}}$] be an oracle-aided algorithm that randomly executes $\left(\mathsf{A}_{\Pi}^{[\delta,\widetilde{\mathsf{Est}},\mathsf{HonCont}]}, \mathsf{B}_{\Pi}^{[\delta,\widetilde{\mathsf{Est}},\mathsf{HonCont}]}\right)$ [resp., $\left(\mathsf{A}_{\Pi}^{[\delta,\widetilde{\mathsf{Est}},\widetilde{\mathsf{HonCont}}]}, \mathsf{B}_{\Pi}^{[\delta,\widetilde{\mathsf{Est}},\widetilde{\mathsf{HonCont}}]}\right)$] while answering the oracle calls to $\mathsf{HonCont}$ [resp., $\widetilde{\mathsf{HonCont}}$] with calls to its own oracle, and outputs the resulting leaf and the controlling scheme of this execution. Hence, now it suffices to bound $\mathrm{SD}\left(\mathsf{E}^{\mathsf{HonCont}}, \mathsf{E}^{\widetilde{\mathsf{HonCont}}}\right)$. Applying Lemma 2.4.5 with respect to $k := m$, $D_i := \langle \mathsf{A}, \mathsf{B} \rangle$ for every $i \in [m]$, $a := 2 \cdot \xi$, $\lambda := 1$ and $b := 0$ yields that

$$d_2 = \mathrm{SD}\left(\mathsf{E}^{\mathsf{HonCont}}, \mathsf{E}^{\widetilde{\mathsf{HonCont}}}\right) \leq 2 \cdot m \cdot \xi'$$

□

Claim 4.4.8. *Let $u \in \mathcal{V}(\Pi)$ such that $u \notin \mathcal{N}\mathsf{eigh}_{\Pi}^{\delta,\xi} \cup \mathcal{F}\mathsf{ail}_{\Pi}^{\xi,\widetilde{\mathsf{Est}}}$, then*

- $u \in \mathcal{S}\mathsf{mall}_{\Pi}^{\delta} \iff u \in \widetilde{\mathcal{S}\mathsf{mall}}_{\Pi}^{\delta,\widetilde{\mathsf{Est}}}$; *and*
- $u \in \mathcal{L}\mathsf{arge}_{\Pi}^{\delta} \iff u \in \widetilde{\mathcal{L}\mathsf{arge}}_{\Pi}^{\delta,\widetilde{\mathsf{Est}}}$.

Proof. We prove for the first case, where the proof for the second case is analogous.

Assume $u \in \mathcal{S}\mathsf{mall}_{\Pi}^{\delta}$. Then by definition it holds that $\mathsf{val}(\Pi_u) \leq \delta$. Since $u \notin \mathcal{N}\mathsf{eigh}_{\Pi}^{\delta,\xi}$, it holds that $\mathsf{val}(\Pi_u) \leq \delta - \xi$. Now, since $u \notin \mathcal{F}\mathsf{ail}_{\Pi}^{\xi,\widetilde{\mathsf{Est}}}$, it holds that $\widetilde{\mathsf{Est}}(u) \leq \delta$, and thus $u \in \widetilde{\mathcal{S}\mathsf{mall}}_{\Pi}^{\delta,\widetilde{\mathsf{Est}}}$.

Assume $u \notin \mathcal{S}\mathsf{mall}_{\Pi}^{\delta}$. Then by definition it holds that $\mathsf{val}(\Pi_u) > \delta$. Since $u \notin \mathcal{N}\mathsf{eigh}_{\Pi}^{\delta,\xi}$, it holds that $\mathsf{val}(\Pi_u) > \delta + \xi$. Now, since $u \notin \mathcal{F}\mathsf{ail}_{\Pi}^{\xi,\widetilde{\mathsf{Est}}}$, it holds that $\widetilde{\mathsf{Est}}(u) > \delta$, and thus $u \notin \widetilde{\mathcal{S}\mathsf{mall}}_{\Pi}^{\delta,\widetilde{\mathsf{Est}}}$. □

The above lemma bounds the difference between the approximate pruned variant and the pruned variant of the protocol with the probability of hitting nodes that their value is close to the point of pruning. We next argue that if we allow small diversion from this point of punning, this probability is small.

Proposition 4.4.9. *Let Π be m-round protocol, let $\delta \in (0, \frac{1}{2}]$ and let $\xi \in (0,1)$. If $\xi \leq \frac{\delta^2}{16m^2}$, then there exists $\delta' \in [\frac{\delta}{2}, \delta]$ such that $\mathsf{neigh}_{\Pi}(\delta', \xi) \leq m \cdot \sqrt{\xi}$, where $\delta' = \delta/2 + j \cdot 2\xi$ with $j \in \mathcal{J} := \left\{0, 1, \ldots, \left\lceil m/\sqrt{\xi} \right\rceil\right\}$.*

Proof. For $i \in [m]$, let $\mathcal{N}\mathsf{eigh}_{\Pi}^{\delta,\xi,i} = \left\{u \in \mathcal{V}(\Pi) \colon u \in \mathcal{N}\mathsf{eigh}_{\Pi}^{\delta,\xi} \wedge |u| = i\right\}$. It holds that

$$\begin{aligned}\Pr_{\langle\Pi\rangle}\left[\mathsf{desc}\left(\mathcal{N}\mathsf{eigh}_{\Pi}^{\delta,\xi}\right)\right] &\leq \Pr_{\langle\Pi\rangle}\left[\mathsf{desc}\left(\cup_{i\in[m]}\mathcal{N}\mathsf{eigh}_{\Pi}^{\delta,\xi,i}\right)\right] \\ &\leq \sum_{i=1}^{m} \Pr_{\langle\Pi\rangle}\left[\mathsf{desc}\left(\mathcal{N}\mathsf{eigh}_{\Pi}^{\delta,\xi,i}\right)\right] \qquad (4.10)\end{aligned}$$

Fix $i \in [m]$ and let $n(i) = \left|\left\{j \in \mathcal{J} \colon \Pr_{\langle\Pi\rangle}\left[\mathsf{desc}\left(\mathcal{N}\mathsf{eigh}_{\Pi}^{\delta/2+j\cdot 2\xi,\xi,i}\right)\right] > \sqrt{\xi}\right\}\right|$. Since for every $j \neq j' \in \mathcal{J}$ it holds that $\mathcal{N}\mathsf{eigh}_{\Pi}^{\delta/2+j\cdot 2\xi,\xi,i} \cap \mathcal{N}\mathsf{eigh}_{\Pi}^{\delta/2+j'\cdot 2\xi,\xi,i} = \emptyset$, it follows that $n(i) < 1/\sqrt{\xi}$. Hence,

$$\sum_{i=1}^{m} n(i) < \frac{m}{\sqrt{\xi}} < |\mathcal{J}|\,.$$

Thus, $\exists j \in \mathcal{J}$ such that $\Pr_{\langle \Pi \rangle}\left[\mathsf{desc}\left(\mathcal{N}\mathsf{eigh}_{\Pi}^{\delta',\xi,i}\right)\right] \leq \sqrt{\xi}$ for any $i \in [m]$, where $\delta' = \delta/2 + j \cdot 2\xi$. Plugging it in Equation (4.10), yields that $\mathsf{neigh}_{\Pi}(\delta', \xi) = \Pr_{\langle \Pi \rangle}\left[\mathsf{desc}\left(\mathcal{N}\mathsf{eigh}_{\Pi}^{\delta',\xi}\right)\right] \leq m \cdot \sqrt{\xi}$. □

Approximated biased continuation attack does well on pruned protocols

To simplify notation for every $\delta \in [0,1]$ let $\widetilde{\mathsf{A}}^{\delta}$ be $\mathsf{A}_{\Pi}^{[\delta,\widetilde{\mathsf{Est}},\widetilde{\mathsf{HonCont}}]}$ and let $\widetilde{\mathsf{B}}^{\delta}$ be analogously defined.

The next lemma shows that Approximated Biased Continuation attack on an approximated pruned protocol performs almost as good as Biased Continuation Attack on the ideally pruned protocol (where there is no sampling error and every A controlled low value node is pruned).

Notation 4.4.10 (iterated approximated attacker)**.** *Let $\Pi = (\mathsf{A}, \mathsf{B})$ be a protocol and $\xi, \delta \in [0,1]$. For every $i \in \mathbb{N}$ let $\mathsf{A}_{\Pi}^{(i,\xi,\delta)} \equiv \left(\mathsf{A}_{\Pi}^{(i-1,\xi,\delta)}\right)^{\left(1,\widetilde{\mathsf{BiasedCont}}_{\left(\mathsf{A}_{\Pi}^{(i-1,\xi,\delta)},\mathsf{B}\right)}\right)}$ (see Lemma 4.2.5), where $\widetilde{\mathsf{BiasedCont}}_{\left(\mathsf{A}_{\Pi}^{(i-1,\xi,\delta)},\mathsf{B}\right)}$ is a (ξ,δ)-Biased Continuator as in Definition 4.2.1 and $\mathsf{A}_{\Pi}^{(0,\xi,\delta)} \equiv \mathsf{A}$.*

Lemma 4.4.11 (iterated attack)**.** *Let $\Pi_1 = (\mathsf{A}, \mathsf{B})$ and $\Pi_2 = (\mathsf{C}, \mathsf{D})$ be two m-round protocols, let $\delta \in (0, \frac{1}{2}]$, let $c = c(\delta)$ from Lemma 4.3.1. Assume that*

1. $\mathrm{SD}\left([\Pi_1], [\Pi_2]\right) \leq \alpha$.
2. *$\delta' \in [\delta, \frac{1}{4}]$ is such that $\mathsf{desc}\left(\mathcal{S}\mathsf{mall}_{\Pi_2}^{2\delta'}\right) \cap \mathcal{C}\mathsf{trl}_{\Pi_2}^{\mathsf{C}} = \emptyset$.*

Then $\mathrm{SD}\left(\left[\mathsf{A}_{\Pi_1}^{(i,\delta',\xi)}, \mathsf{B}\right], \left[\mathsf{C}_{\Pi_2}^{(i)}, \mathsf{D}\right]\right) \leq \phi^{\mathsf{lt}}(m, \alpha, \xi, \delta', \boldsymbol{\gamma})$ for any $i \in \mathbb{N}$ and $\gamma_1, \ldots, \gamma_i >$

1, *where*

$$\phi^{\mathsf{It}}(m,\alpha,\xi,\delta',(\gamma_1,\ldots,\gamma_i)) := \alpha\cdot\frac{8^i\cdot m^i\cdot\prod_{t=1}^{i}\gamma_t}{\delta'^{2i}}+\xi\cdot\sum_{j=1}^{i}\frac{8^j\cdot m^j\cdot\prod_{t=1}^{j}\gamma_t}{\delta'^{2j}} + 6\cdot\sum_{j=1}^{i}\frac{8^{i-j}\cdot m^{i-j}\cdot\prod_{t=j+1}^{i}\gamma_t}{\delta'^{2(i-j)}\cdot\gamma_j^c}.$$

The proof of the above lemma, easily follows from the single attack stated and proved in Section 4.4.

Proof. Note that for any $i\in\mathbb{N}$ and any $u\in\mathcal{V}(\Pi_2)$, it holds that $\mathsf{val}(\left(\mathsf{C}^{(i+1)},\mathsf{D}\right)_u)\geq\mathsf{val}(\left(\mathsf{C}^{(i)},\mathsf{D}\right)_u)$. Namely, the value of every node can only increases when applying biased-continuation attack towards 1. It follows that $\mathsf{desc}\left(\mathcal{S}\mathsf{mall}^{2\delta'}_{\left(\mathsf{C}^{(i)},\mathsf{D}\right)}\right)\cap\mathcal{C}\mathsf{trl}^{\mathsf{C}}_{\left(\mathsf{C}^{(i)},\mathsf{D}\right)}=\emptyset$ for every $i\in\mathbb{N}$. The proof now follows a straightforward recursion formula based on Lemma 4.4.14. □

Corollary 4.4.12. *Assume the conditions of Lemma 4.4.11. Then for every $\varepsilon>0$ and $j\in[i]$ if $\gamma_j=\left(\frac{48\cdot i}{\delta'^2}\cdot\frac{m}{\varepsilon}\cdot\gamma_{j+1}\right)^{\frac{i}{c}}$ with $\gamma_{i+1}=1$, it holds*

$$\phi^{\mathsf{It}}(m,\alpha,\xi,\delta',\boldsymbol{\gamma})\leq(\alpha+2\cdot\xi)\cdot\left(\frac{48\cdot i}{\delta'^2}\cdot\frac{m}{\varepsilon}\right)^{\left(\frac{i}{c}\right)^i}+\varepsilon$$

The next proposition bounds the running time of the above attacker.

Proposition 4.4.13. *Let Π be m-round protocol, let $\delta\in(0,\frac{1}{2}]$ and let $\xi\in[0,\delta/2]$. Assume that the running time of Π is T_Π, then the running time of $\mathsf{A}^{(i,\delta,\xi)}_\Pi$ is*

$$T^{\Pi,\delta,\xi}_{\mathsf{Pru}}(i) := O\left(\left(\frac{m+\ln\left(\frac{1}{\xi}\right)}{2\xi^2}+\frac{\ln\left(\frac{1}{\xi}\right)}{\ln\left(\frac{1}{1-\delta}\right)}\right)^i\cdot m^{2^i}\cdot T_\Pi\right)$$

Proof. Consider a single call to $\mathsf{A}^{(i,\delta,\xi)}_\Pi$. In this call it might call $\widetilde{\mathsf{Est}}$ and $\widetilde{\mathsf{BiasedCont}}$ for m times. The running time of $\widetilde{\mathsf{Est}}$ is $T_{\widetilde{\mathsf{Est}}}:=O\left(\frac{m+\ln\left(\frac{1}{\xi}\right)}{2\xi^2}\right)$, where the running

time of $\widetilde{\mathsf{BiasedCont}}$ is $T_{\mathsf{BC}} = O\left(\frac{\ln\left(\frac{1}{\xi}\right)}{\ln\left(\frac{1}{1-\delta}\right)}\right)$. Is also might call $\mathsf{A}_{\Pi}^{(i-1,\delta,\xi)}$. Counting for m possible turns of $\mathsf{A}_{\Pi}^{(i,\delta,\xi)}$, we get the following recursion

$$T_{\mathsf{Pru}}^{\Pi,\delta,\xi}(i) = O\left(\left(T_{\widetilde{\mathsf{Est}}} + T_{\mathsf{BC}}\right) \cdot m^2 \cdot T_{\mathsf{Pru}}^{\Pi,\delta,\xi}(i-1)\right),$$

where $T_{\mathsf{Pru}}^{\Pi,\delta,\xi}(0) = T_{\Pi}$. The proof follows by solving the above recursion. □

Analyzing a single attack

Lemma 4.4.14 (single attack)**.** *Let $\Pi_1 = (\mathsf{A}, \mathsf{B})$ and $\Pi_2 = (\mathsf{C}, \mathsf{D})$ be two m-round protocols, let $\delta \in (0, \frac{1}{2}]$, let $c = c(\delta)$ from Lemma 4.3.1. Assume that*

1. $\mathrm{SD}\left([\Pi_1], [\Pi_2]\right) \leq \alpha$.
2. *$\delta' \in [\delta, \frac{1}{4}]$ is such that $\mathsf{desc}\left(\mathcal{S}\mathsf{mall}_{\Pi_2}^{2\delta'}\right) \cap \mathcal{C}\mathsf{trl}_{\Pi_2}^{\mathsf{C}} = \emptyset$.*

Then for every (ξ, δ')-biased continuator for Π, $\widetilde{\mathsf{BiasedCont}}$ (see Definition 4.2.1) with $\xi \in [0, \delta'/2]$ and every $\gamma > 1$ it holds that

$$\mathrm{SD}\left(\left[\mathsf{A}_{\Pi_1}^{(1,\widetilde{\mathsf{BiasedCont}})}, \mathsf{B}\right], \left[\mathsf{C}_{\Pi_2}^{(1)}, \mathsf{D}\right]\right) \leq \frac{8 \cdot m \cdot \gamma \cdot (\alpha + \xi)}{\delta'^2} + \frac{6}{\gamma^c}.$$

Proof of Lemma 4.4.14. In order to apply Lemma 3.9.1 (robustness lemma) we have to bound $\Pr_{\langle \mathsf{A},\mathsf{B}\rangle}\left[\mathsf{desc}\left(\mathcal{S}\mathsf{mall}_{\Pi}^{\delta',\mathsf{A}} \cup \mathcal{S}\mathsf{mall}_{\Pi'}^{\delta',\mathsf{C}}\right)\right]$ and by condition 2 it is equal to bounding $\Pr_{\langle \mathsf{A},\mathsf{B}\rangle}\left[\mathsf{desc}\left(\mathcal{S}\mathsf{mall}_{\Pi}^{\delta',\mathsf{A}}\right)\right]$.

Let $\mathcal{S} = \left\{\ell \in \mathsf{desc}\left(\mathcal{S}\mathsf{mall}_{\Pi}^{\delta',\mathsf{A}}\right) : \ell_{|\ell|} = 1\right\}$[7] Let $\beta = \Pr_{\langle \mathsf{A},\mathsf{B}\rangle}\left[\mathsf{desc}\left(\mathcal{S}\mathsf{mall}_{\Pi}^{\delta',\mathsf{A}}\right)\right]$ and $\beta' = \Pr_{\langle \mathsf{C},\mathsf{D}\rangle}\left[\mathsf{desc}\left(\mathcal{S}\mathsf{mall}_{\Pi}^{\delta',\mathsf{A}}\right)\right]$. Since $\mathrm{SD}\left(\langle \mathsf{A},\mathsf{B}\rangle, \langle \mathsf{C},\mathsf{D}\rangle\right) \leq \alpha$ (which is implied by the assumption that $\mathrm{SD}\left([\mathsf{A},\mathsf{B}], [\mathsf{C},\mathsf{D}]\right) \leq \alpha$), it follows that $\beta' > \beta - \alpha$ and also

[7] Recall that we assume the last message of the transcript is the common output bit.

$\Pr_{\langle \mathsf{C},\mathsf{D}\rangle}[\mathsf{desc}(\mathcal{S})] - \Pr_{\langle \mathsf{A},\mathsf{B}\rangle}[\mathsf{desc}(\mathcal{S})] \leq \alpha$. However, by the definition of $\mathcal{S}$ it follows that $\Pr_{\langle \mathsf{A},\mathsf{B}\rangle}[\mathsf{desc}(\mathcal{S})] \leq \beta \cdot \delta'$ and that $\Pr_{\langle \mathsf{C},\mathsf{D}\rangle}[\mathsf{desc}(\mathcal{S})] \geq \beta' \cdot 2\delta'$. Now we have

$$\begin{aligned}
\alpha &\geq \Pr_{\langle \mathsf{C},\mathsf{D}\rangle}[\mathsf{desc}(\mathcal{S})] - \Pr_{\langle \mathsf{A},\mathsf{B}\rangle}[\mathsf{desc}(\mathcal{S})] \\
&\geq 2\beta' \cdot \delta' - \beta \cdot \delta' \\
&\geq 2(\beta - \alpha) \cdot \delta' - \beta \cdot \delta' \\
&\geq \beta \cdot \delta' - 2\alpha \cdot \delta' \\
&\geq \beta \cdot \delta' - \alpha
\end{aligned}$$

where the last equality follows the assumption and the fact that $\delta' \leq 1/2$. The above implies that $\Pr_{\langle \mathsf{A},\mathsf{B}\rangle}\left[\mathsf{desc}\left(\mathcal{S}\mathsf{mall}_{\Pi}^{\delta',\mathsf{A}}\right)\right] = \beta \leq \frac{2\alpha}{\delta}$.

Now let $\gamma > 1$. First we can apply Lemma 3.9.1 and derive

$$\begin{aligned}
\mathrm{SD}\left(\left[\mathsf{A}_{\Pi_1}^{(1)}, \mathsf{B}\right], \left[\mathsf{C}_{\Pi_2}^{(1)}, \mathsf{D}\right]\right) &\leq \frac{2 \cdot m \cdot \gamma}{\delta'} \cdot (\alpha + \frac{2\alpha}{\delta'}) + \frac{4}{\gamma^c} \\
&\leq \frac{6 \cdot m \cdot \alpha \cdot \gamma}{\delta'^2} + \frac{4}{\gamma^c}
\end{aligned}$$

Now we can apply Lemma 4.2.5 and have

$$\mathrm{SD}\left(\left[\mathsf{A}_{\Pi_1}^{(1)}, \mathsf{B}\right], \left[\mathsf{A}_{\Pi_1}^{(1,\widetilde{\mathsf{BiasedCont}})}, \mathsf{B}\right]\right) \leq m \cdot \gamma \cdot (2\xi + \frac{2\alpha}{\delta'}) + \frac{2}{\gamma^c}$$

Finally, combining the last two inequalities and using triangle inequality we have:

$$\mathrm{SD}\left(\left[\mathsf{A}_{\Pi_1}^{(1,\widetilde{\mathsf{BiasedCont}})}, \mathsf{B}\right], \left[\mathsf{C}_{\Pi_2}^{(1)}, \mathsf{D}\right]\right) \leq \frac{8 \cdot m \cdot \gamma \cdot (\alpha + \xi)}{\delta'^2} + \frac{6}{\gamma^c}.$$

□

4.5 The Pruning-in-the-Head Attacker

The following attacker successfully applies the pruning attacker of Section 4.4 on *arbitrary* protocols. In particular, on a protocol for which the assumptions required for proving the success probability of the pruning attacker, see Lemma 4.4.11, do not hold. To do that, it prunes the initial protocol before applying the pruning attacker, while making sure not to attack pruned transcripts, i.e., low-value and high-value transcripts.

Algorithm 4.5.1 ($\mathsf{A}_{\Pi}^{(i,\delta,\xi,\ state)}$)**.**

Oracles: $\widetilde{\mathsf{HonCont}}$ *and* $\widetilde{\mathsf{Est}}$ *(the latter is deterministic).*

Input: transcript $u \in \{0,1\}^*$.

State: state *set at the beginning to* $\perp$

Operation:

1. *If* $u \in \mathcal{L}(\Pi)$*, output* $\chi_{\Pi}(u)$ *and halt.*
2. *Let* $\widetilde{\Pi} = \Pi^{[2\delta,\widetilde{\mathsf{Est}},\widetilde{\mathsf{HonCont}}]}$.
3. *At round* r *set* msg *as follows.*
   - *In case* state $\neq\perp$*, set* $\mathsf{msg} :=$ state$_r$.
   - *In case* state $=\perp$ *and* $u \in \widetilde{\mathcal{S}\mathsf{mall}}_{\Pi}^{2\delta,\widetilde{\mathsf{Est}}} \cup \widetilde{\mathcal{L}\mathsf{arge}}_{\Pi}^{2\delta,\widetilde{\mathsf{Est}}}$*, let* $\ell \leftarrow \widetilde{\mathsf{HonCont}}(u)$*, set* state $:= \ell$ *and* $\mathsf{msg} :=$ state$_r$.
   - *Else set* $\mathsf{msg} := \mathsf{A}_{\widetilde{\Pi}}^{(i,\delta,2\xi)}(u)$ *(see Notation 4.4.10).*
4. *Send* msg *to* B.
5. *If* $u' = u \circ \mathsf{msg} \in \mathcal{L}(\Pi)$*, output* $\chi_{\Pi}(u')$.

The next lemma, proven in Section 4.5 states that in case protocol Π does not have many nodes whose value is close to 2δ, then the above algorithm mimics that of the ideal attacker for the ideal pruned protocol well.

Lemma 4.5.2. *Let Π be m-round protocol, let $\delta \in (0, \frac{1}{2}]$ and let $c = c(\delta)$ from Lemma 4.3.1. It holds that*

$$\mathsf{val}\left(\mathsf{A}_{\Pi}^{(i,\delta',\xi,\mathrm{state})}, \mathsf{B}\right) \geq \mathsf{val}\left(\left(\mathsf{A}_{\Pi}^{[2\delta']}\right)^{(i)}, \mathsf{B}_{\Pi}^{[2\delta']}\right) - 3\delta' - 9 \cdot \phi^{\mathsf{lt}}(m, \mathsf{neigh}_{\Pi}(2\delta', 2\xi) + 7 \cdot m \cdot \xi, 2 \cdot \xi, \delta', \boldsymbol{\gamma}),$$

for every $\delta' \in [\delta, \frac{1}{2}]$, every $\xi \in [0, \delta'/2]$, every $i \in \mathbb{N}$ and every $\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_i)$, all larger than 1, where $\widetilde{\mathsf{HonCont}}$ is ξ-honest continuator and $\widetilde{\mathsf{Est}}$ is a $(2\xi, \delta)$-estimator for Π. Moreover, ϕ^{lt} is as in Lemma 4.4.11 and neigh as in Definition 4.4.6.

We also bound the running time of the above attacker,

Proposition 4.5.3. *Let $\Pi = (\mathsf{A}, \mathsf{B})$ be m-round protocol let $\delta \in [0, \frac{1}{4}]$ and let $\xi \in [0, \delta/2]$. Assume that the running time of $\widetilde{\mathsf{Inv}}$ is $T_{\widetilde{\mathsf{Inv}}}$, then the running time of $\mathsf{A}_{\Pi}^{(i,\delta,\xi,\ \mathrm{state})}$ is*

$$T_{\mathsf{final}}^{\delta,\xi,\widetilde{\mathsf{Inv}}}(i) := O\left(m^{2^i+3} \cdot \left(\frac{m + \ln\left(\frac{1}{2\xi}\right)}{4\xi^2} + \frac{\ln\left(\frac{1}{2\xi}\right)}{\ln\left(\frac{1}{1-\delta}\right)}\right)^i \cdot \left(\frac{m + \ln\left(\frac{1}{\xi}\right)}{2\xi^2}\right) \cdot T_{\widetilde{\mathsf{Inv}}}\right)$$

Proof. Consider a single call to $\mathsf{A}_{\Pi}^{(i,\delta,\xi,state)}$. It is easy to verify that the dominant term of this running ti,e is the call to $\mathsf{A}_{\widetilde{\Pi}}^{(i,\delta,2\xi)}$ on the protocol $\widetilde{\Pi} = \left(\mathsf{A}_{\Pi}^{[2\delta,\widetilde{\mathsf{Est}},\widetilde{\mathsf{HonCont}}]}, \mathsf{B}_{\Pi}^{[2\delta,\widetilde{\mathsf{Est}},\widetilde{\mathsf{HonCont}}]}\right)$. Note that the running time of Π is $T_{\widetilde{\Pi}} = O\left(m \cdot T_{\widetilde{\mathsf{Inv}}} \cdot \left(\frac{m+\ln\left(\frac{1}{\xi}\right)}{\xi^2}\right)\right)$. Plugging in $T_{\mathsf{Pru}}^{\widetilde{\Pi},\delta,2\xi}(i)$ from Proposition 4.4.13 and considering m possible rounds $\mathsf{A}_{\Pi}^{(i,\delta,\xi,state)}$ might run complete the proof. □

Analysis of the Pruning-in-the-Head Attack

Proof of Lemma 4.5.2. In order to prove this lemma we will define five hybrids $\mathsf{H}_0, \ldots, \mathsf{H}_4$. The first hybrid H_0 has as output the output bit of a random execution of $\left(\mathsf{A}_{\Pi}^{(i,\delta',\xi,state)}, \mathsf{B}\right)$, while the last hybrid H_5 that of a random execution of $\left(\left(\mathsf{A}_{\Pi}^{[2\delta']}\right)^{(i)}, \mathsf{B}_{\Pi}^{[2\delta']}\right)$. Then we will give a bound of the statistical distance between the hybrids and by triangle inequality we will conclude proving the lemma. Let us define the hybrids one by one.

- $\mathsf{H}_\mathbf{0}$: As already mentioned, this hybrid is equal to the random variable of the output of a random execution of $\left(\mathsf{A}_{\Pi}^{(i,\delta',\xi,state)}, \mathsf{B}\right)$.

- $\mathsf{H}_\mathbf{1}$: In order to define this hybrid let us first define the following sets. Let

  $$\mathcal{F}\mathsf{ail}^{\xi,\widetilde{\mathsf{HonCont}}} = \mathsf{frnt}\left(\left\{u \in \mathcal{V}(\Pi)\colon \mathrm{SD}\left(\widetilde{\mathsf{HonCont}}(u), \mathsf{HonCont}(u)\right) > \xi\right\}\right)$$

  and

  $$\mathcal{F}\mathsf{ail}^{\widetilde{\mathsf{Est}}} = \mathsf{frnt}\left(\left\{u \in \mathcal{V}(\Pi)\colon \mathsf{val}(\Pi_u) < 1 - 3\delta' \wedge \widetilde{\mathsf{Est}}(u) > 1 - 2\delta'\right\}\right)$$

  .

  Let $\mathcal{F}\mathsf{ail} = \mathcal{F}\mathsf{ail}^{\xi,\widetilde{\mathsf{HonCont}}} \cup \mathcal{F}\mathsf{ail}^{\widetilde{\mathsf{Est}}}$ and $\mathcal{E} = \mathsf{frnt}\left(\widetilde{\mathcal{S}\mathsf{mall}}_{\Pi}^{2\delta',\widetilde{\mathsf{Est}}} \cup \widetilde{\mathcal{L}\mathsf{arge}}_{\Pi}^{2\delta',\widetilde{\mathsf{Est}}}\right) \setminus \mathcal{F}\mathsf{ail}$. This hybrid is the same as the previous one up to a point where the protocol $\left(\mathsf{A}_{\Pi}^{(i,\delta',\xi,state)}, \mathsf{B}\right)$ reaches a node $u \in \mathcal{E}$. Then for every $w \in \mathsf{desc}(u)$, both parties act like $\left(\mathsf{A}_{\widetilde{\Pi}}^{(i,\delta',2\xi)}, \widetilde{\mathsf{B}}\right)$, where
  $\widetilde{\Pi} = (\widetilde{\mathsf{A}}, \widetilde{\mathsf{B}}) = \left(\mathsf{A}_{\Pi}^{[2\delta',\widetilde{\mathsf{Est}},\widetilde{\mathsf{HonCont}}]}, \mathsf{B}_{\Pi}^{[2\delta',\widetilde{\mathsf{Est}},\widetilde{\mathsf{HonCont}}]}\right)$.

- $\mathsf{H}_\mathbf{2}$: In this hybrid both parties act everywhere like $\left(\mathsf{A}_{\widetilde{\Pi}}^{(i,\delta',2\xi)}, \widetilde{\mathsf{B}}\right)$ except for nodes $u \in \mathsf{desc}\left(\mathsf{frnt}\left(\mathcal{F}\mathsf{ail}\right) \setminus \mathsf{desc}\left(\widetilde{\mathcal{S}\mathsf{mall}}_{\Pi}^{2\delta',\widetilde{\mathsf{Est}}} \cup \widetilde{\mathcal{L}\mathsf{arge}}_{\Pi}^{2\delta',\widetilde{\mathsf{Est}}}\right)\right)$, where both parties act like $\left(\mathsf{A}_{\Pi}^{(i,\delta',\xi,state)}, \mathsf{B}\right)$.

- $\mathsf{H_3}$: This hybrid is equal to the random variable of the output of a random execution of $\left(\mathsf{A}_{\widetilde{\Pi}}^{(i,\delta',2\xi)}, \widetilde{\mathsf{B}}\right)$.

- $\mathsf{H_4}$: This hybrid is equal to the random variable of the output of a random execution of $\left(\left(\mathsf{A}_{\Pi}^{[2\delta']}\right)^{(i)}, \mathsf{B}_{\Pi}^{[2\delta']}\right)$.

Claim 4.5.4. $\mathrm{SD}(\mathsf{H}_0, \mathsf{H}_1) \leq 3\delta' + 2\xi$.

Proof. Now let $v(u) = \mathsf{val}\left(\left(\mathsf{A}_{\Pi}^{(i,\delta',\xi,state)}, \mathsf{B}\right)_u\right)$ and $\widetilde{v}(u) = \mathsf{val}\left(\left(\mathsf{A}_{\widetilde{\Pi}}^{(i,\delta',2\xi)}, \widetilde{\mathsf{B}}\right)_u\right)$. The proof of the claim follows by giving an upper bound on $v(u) - \widetilde{v}(u)$ for any node $u \in \mathcal{E}$.

$u \in \mathcal{E} \cap \widetilde{\mathcal{S}\mathsf{mall}}_{\Pi}^{2\delta',\widetilde{\mathsf{Est}}}$**:** By Algorithm 4.5.1, it holds that $v(u) = \mathrm{E}[\widetilde{\mathsf{HonCont}}(u)_m]$.[8] Since $u \notin \mathcal{F}\mathsf{ail}^{\xi,\widetilde{\mathsf{HonCont}}}$, it follows that $|v(u) - \mathsf{val}(\Pi_u)| \leq \xi$.

By Definition 4.4.5, it holds that $\widetilde{v}(u) = \mathrm{E}[\widetilde{\mathsf{HonCont}}(u)_m]$. It again follows that $|\widetilde{v}(u) - \mathsf{val}(\Pi_u)| \leq \xi$, and the proof follows.

$u \in \mathcal{E} \cap \widetilde{\mathcal{L}\mathsf{arge}}_{\Pi}^{2\delta',\widetilde{\mathsf{Est}}}$**:** Since $u \notin \mathcal{F}\mathsf{ail}^{\widetilde{\mathsf{Est}}}$, if holds that $\mathsf{val}(\Pi_u) \geq 1 - 3\delta'$, and thus $v(u) \geq 1 - 3\delta' - \xi$. The proof follows since $\widetilde{v}(u) \leq 1$.

$u \in \mathcal{L}(\Pi)$**:** It holds that $v(u) = \widetilde{v}(u) = \chi_{\Pi}(u)$.

□

Claim 4.5.5. $\mathrm{SD}(\mathsf{H}_1, \mathsf{H}_2) \leq m \cdot \xi$.

Proof. By the definition of $\widetilde{\mathsf{HonCont}}$ and since $\mathsf{H}_0, \mathsf{H}_1$ only differ in nodes outside $\mathcal{F}\mathsf{ail}$, specifically outside $\mathcal{F}\mathsf{ail}^{\xi,\widetilde{\mathsf{HonCont}}}$ and the fact that there are at most m rounds we conclude that the statistical difference is at most $m \cdot \xi$. □

[8] in case A controls u this is immediate. In case A controls u, note that in the first time it is A's turn it makes the same call to the inverter. Since the random coins of the parties are in product distribution, the outcome is a valid transcript.

Claim 4.5.6.

$$\mathrm{SD}(\mathsf{H}_2, \mathsf{H}_3) \leq 2 \cdot \phi^{\mathsf{Bal}}(\mathsf{neigh}_{\Pi}(2\delta', 2\xi) + 7 \cdot m \cdot \xi, 2\delta', \boldsymbol{\gamma}) + 2 \cdot \phi^{\mathsf{It}}(m, \mathsf{neigh}_{\Pi}(2\delta', 2\xi) + 4 \cdot m \cdot \xi, 2\xi, \delta', \boldsymbol{\gamma}).$$

Proof. These two hybrids only differ when the protocol reaches a node $u \in \mathcal{F}\mathsf{ail}$. Therefore the statistical distance is bounded by
$\Pr_{\left\langle \mathsf{A}_{\widetilde{\Pi}}^{(i,\delta',2\xi)}, \widetilde{\mathsf{B}} \right\rangle} \left[\mathsf{desc}(\mathcal{F}\mathsf{ail})\right] \leq \Pr_{\left\langle \mathsf{A}_{\widetilde{\Pi}}^{(i,\delta',2\xi)}, \widetilde{\mathsf{B}} \right\rangle} \left[\mathsf{desc}(\mathcal{F}\mathsf{ail}^{\xi,\widetilde{\mathsf{HonCont}}})\right]$
$+\Pr_{\left\langle \mathsf{A}_{\widetilde{\Pi}}^{(i,\delta',2\xi)}, \widetilde{\mathsf{B}} \right\rangle} \left[\mathsf{desc}\left(\mathcal{F}\mathsf{ail}^{\widetilde{\mathsf{Est}}} \setminus \mathsf{desc}\left(\mathcal{F}\mathsf{ail}^{\xi,\widetilde{\mathsf{HonCont}}}\right)\right)\right]$. The claim will follow from the next claim.

Claim 4.5.7. *Let $\mathcal{F}$ be a frontier. Assume that $\Pr_{\langle \mathsf{A},\mathsf{B} \rangle}\left[\mathsf{desc}\left(\mathcal{F}\right)\right] \leq \alpha$ and that $\mathcal{F} \cap \overline{\mathsf{desc}}\left(\mathcal{F}\mathsf{ail}^{\xi,\widetilde{\mathsf{HonCont}}}\right) = \emptyset$, then it holds that*

$$\Pr_{\left\langle \mathsf{A}_{\widetilde{\Pi}}^{(i,\delta',2\xi)}, \widetilde{\mathsf{B}} \right\rangle}\left[\mathsf{desc}\left(\mathcal{F}\right)\right] \leq \phi^{\mathsf{Bal}}(\alpha + \mathsf{neigh}_{\Pi}(2\delta', 2\xi) + 5 \cdot m \cdot \xi, 2\delta', \boldsymbol{\gamma}) + \phi^{\mathsf{It}}(m, \mathsf{neigh}_{\Pi}(2\delta', 2\xi) + 4 \cdot m \cdot \xi, 2\xi, \delta', \boldsymbol{\gamma}).$$

Proof. Let H^{O} a process that emulates random execution of $\left(\mathsf{A}_{\Pi}^{[2\delta',\widetilde{\mathsf{Est}},\mathsf{O}]}, \mathsf{B}_{\Pi}^{[2\delta',\widetilde{\mathsf{Est}},\mathsf{O}]}\right)$, halts when reaching a node in $\mathcal{F} \cup \mathcal{F}\mathsf{ail}^{\xi,\widetilde{\mathsf{HonCont}}}$ or when the execution ends and outputs the transcript of the execution. Note that
$\Pr_{\langle \mathsf{A},\mathsf{B} \rangle}\left[\mathsf{desc}\left(\mathcal{F}\right)\right]$ [resp., $\Pr_{\left\langle \widetilde{\mathsf{A}},\widetilde{\mathsf{B}} \right\rangle}\left[\mathsf{desc}\left(\mathcal{F}\right)\right]$] is equal to the probability that $\mathsf{H}^{\mathsf{HonCont}}$ [resp., $\mathsf{H}^{\widetilde{\mathsf{HonCont}}}$] outputs a transcript in $\mathcal{F}$, as by assumption $\mathcal{F} \cap \overline{\mathsf{desc}}\left(\mathcal{F}\mathsf{ail}^{\xi,\widetilde{\mathsf{HonCont}}}\right) = \emptyset$. Observing that H makes at most m oracles queries and none of them is in $\mathcal{F}\mathsf{ail}^{\xi,\widetilde{\mathsf{HonCont}}}$, together with the fact that $\widetilde{\mathsf{HonCont}}$ is a ξ-honest continuator of Π as shown in Claim 4.6.3 and a standard hybrid argument yield that

$$\mathrm{SD}\left(\mathsf{H}^{\mathsf{HonCont}}, \mathsf{H}^{\widetilde{\mathsf{HonCont}}}\right) \leq m \cdot \xi \tag{4.11}$$

It follows that $\Pr_{\left\langle \widetilde{\mathsf{A}},\widetilde{\mathsf{B}} \right\rangle}\left[\mathsf{desc}\left(\mathcal{F}\right)\right] \leq \alpha + m \cdot \xi$. In order to ease notation, let $(\mathsf{C}, \mathsf{D}) = \left(\mathsf{A}_{\Pi}^{[2\delta']}, \mathsf{B}_{\Pi}^{[2\delta']}\right)$. Since we assume that $\widetilde{\mathsf{Est}}$ is 2ξ-estimator for Π, Lemma 4.4.7 yields

that

$$\begin{aligned}\Pr_{\langle \mathsf{C},\mathsf{D}\rangle}\left[\mathsf{desc}\left(\mathcal{F}\right)\right] &\leq \alpha + m\cdot\xi + \mathsf{neigh}_{\Pi}(2\delta',2\xi) + 2\xi + 2\cdot m\cdot\xi \qquad (4.12)\\ &= \alpha + \mathsf{neigh}_{\Pi}(2\delta',2\xi) + 5\cdot m\cdot\xi.\end{aligned}$$

Applying Proposition 4.3.3(2) with respect to (C,D)

$$\Pr_{\left\langle \mathsf{C}^{(i)},\mathsf{D}\right\rangle}\left[\mathsf{desc}\left(\mathcal{F}\right)\right] \leq \phi^{\mathsf{Bal}}(\alpha + \mathsf{neigh}_{\Pi}(2\delta',2\xi) + 5\cdot m\cdot\xi, 2\delta', \boldsymbol{\gamma}). \qquad (4.13)$$

Applying Lemma 4.4.11 with respect to $\Pi_1 = \left(\widetilde{\mathsf{A}},\widetilde{\mathsf{B}}\right)$ and $\Pi_2 = (\mathsf{C},\mathsf{D})$, yields that

$$\begin{aligned}\Pr_{\left\langle \mathsf{A}_{\widetilde{\Pi}}^{(i,\delta',2\xi)},\widetilde{\mathsf{B}}\right\rangle}\left[\mathsf{desc}\left(\mathcal{F}\right)\right] \leq\ & \phi^{\mathsf{Bal}}(\alpha + \mathsf{neigh}_{\Pi}(2\delta',2\xi) + 5\cdot m\cdot\xi, 2\delta', \boldsymbol{\gamma})\\ &+ \phi^{\mathsf{It}}(m, \mathsf{neigh}_{\Pi}(2\delta',2\xi) + 4\cdot m\cdot\xi, 2\xi, \delta', \boldsymbol{\gamma}).\end{aligned}$$

□

However, notice that by definition $\Pr_{\left\langle \mathsf{A}_{\widetilde{\Pi}}^{(i,\delta',2\xi)},\widetilde{\mathsf{B}}\right\rangle}\left[\mathsf{desc}\left(\mathcal{F}\mathsf{ail}^{\xi,\widetilde{\mathsf{HonCont}}}\right)\right] \leq \xi$ and $\Pr_{\left\langle \mathsf{A}_{\widetilde{\Pi}}^{(i,\delta',2\xi)},\widetilde{\mathsf{B}}\right\rangle}\left[\mathsf{desc}\left(\mathcal{F}\mathsf{ail}^{\widetilde{\mathsf{Est}}} \setminus \mathsf{desc}\left(\mathcal{F}\mathsf{ail}^{\xi,\widetilde{\mathsf{HonCont}}}\right)\right)\right] \leq \Pr_{\left\langle \mathsf{A}_{\widetilde{\Pi}}^{(i,\delta',2\xi)},\widetilde{\mathsf{B}}\right\rangle}\left[\mathsf{desc}\left(\mathcal{F}\mathsf{ail}^{\widetilde{\mathsf{Est}}}\right)\right] \leq 2\cdot\xi$. Moreover, notice that by definition neither of these two sets intersects with $\overline{\mathsf{desc}}\left(\mathcal{F}\mathsf{ail}^{\xi,\widetilde{\mathsf{HonCont}}}\right)$ and applying the above claim the proof follows. □

Claim 4.5.8. $\mathrm{SD}(\mathsf{H}_3,\mathsf{H}_4) \leq \phi^{\mathsf{It}}(m, \mathsf{neigh}_{\Pi}(2\delta',2\xi) + 4\cdot m\cdot\xi, 2\xi, \delta', \boldsymbol{\gamma})$

Proof. This is straightforward from Lemmas 4.4.7 and 4.4.11. □

Putting everything together we derive

$$\begin{aligned}\mathrm{SD}(\mathsf{H}_0,\mathsf{H}_4) \leq\ & 3\delta' + (3+m)\cdot\xi\\ &+ 2\cdot\phi^{\mathsf{Bal}}(\mathsf{neigh}_{\Pi}(2\delta',2\xi) + 7\cdot m\cdot\xi, 2\delta', \boldsymbol{\gamma})\\ &+ 3\cdot\phi^{\mathsf{It}}(m, \mathsf{neigh}_{\Pi}(2\delta',2\xi) + 4\cdot m\cdot\xi, 2\xi, \delta', \boldsymbol{\gamma}),\end{aligned}$$

and the lemma follows, by noticing that both $\phi^{\mathsf{Bal}}(\mathsf{neigh}_{\Pi}(2\delta', 2\xi) + 7 \cdot m \cdot \xi, 2\delta', \boldsymbol{\gamma})$ and $\phi^{\mathsf{It}}(m, \mathsf{neigh}_{\Pi}(2\delta', 2\xi) + 4 \cdot m \cdot \xi, 2\xi, \delta', \boldsymbol{\gamma})$ are at most $\phi^{\mathsf{It}}(m, \mathsf{neigh}_{\Pi}(2\delta', 2\xi) + 7 \cdot m \cdot \xi, 2\xi, \delta', \boldsymbol{\gamma})$. □

4.6 Main Theorem - Constructing the Efficient Attacker

Definition 4.6.1 (Protocol inverter)**.** *Algorithm* $\widetilde{\mathsf{Inv}}$ *is a* ξ-inverter *for* Π *if* $Pr_{\ell \leftarrow \langle \Pi \rangle}[\exists i \in [m] \colon \mathrm{SD}\left(\mathrm{trans}\left(\mathsf{A}(\ell_{1,\ldots,i}; r_{\mathsf{A}}), \mathsf{B}(\ell_{1,\ldots,i}; r_{\mathsf{B}})\right)_{(r_{\mathsf{A}}, r_{\mathsf{B}}) \leftarrow \widetilde{\mathsf{Inv}}(\ell_{1\ldots,i})}, \mathsf{HonCont}(\ell_{1,\ldots,i})\right) > \xi] \leq \xi$. *where* $\mathsf{HonCont}$ *is as in Definition 4.4.2.*[9]

Reductions

We give some simple reduction between the previously defined tools and a Protocol Inverter.

From inversion to honest continuation

Algorithm 4.6.2 ($\widetilde{\mathsf{HonCont}}^{\widetilde{\mathsf{Inv}}}_{(\mathsf{A},\mathsf{B})}$)**.**

Oracle: algorithm $\widetilde{\mathsf{Inv}}$ *whose domain is in* $\{0,1\}^*$.

Input: transcript $u \in \{0,1\}^*$.

Operation:

1. *Set* $(r_{\mathsf{A}}, r_{\mathsf{B}}) \leftarrow \widetilde{\mathsf{Inv}}(u)$.
2. *Return* $(\mathrm{trans}(\mathsf{A}(r_{\mathsf{A}}), \mathsf{B}(r_{\mathsf{B}}))(u))_{|u|+1,\ldots,m}$.

[9] Recall that $\mathsf{A}(u; r)$ is an execution of A on input u with randomness r and trans is the transcript as defined in Section 2.2.

Claim 4.6.3. *Assume that* $\widetilde{\mathsf{Inv}}$ *is* ξ*-inverter for* Π*. Then* $\widetilde{\mathsf{HonCont}}$ *of Algorithm 4.6.2 is* ξ*-honest continuator for* Π*.*

Proof. Immediately follows definition. □

From honest continuation to estimation

Algorithm 4.6.4 ($\widetilde{\mathsf{Est}}^{(\xi,\mathsf{O})}$)**.**

Parameters: $\xi \in [0,1]$.

Input: transcript $u \in \{0,1\}^*$.

Oracle: algorithm O *returning values in* $\{0,1\}^{m-|u|-1}$.

Operation:

1. *Set* $sum = 0$ *and* $s = \left\lceil \frac{\ln\left(\frac{2^{m+2}}{\xi}\right)}{2\cdot\xi^2} \right\rceil$.
2. *For* $i = 1$ *to* s*:*
   a) *Let* b *be the last bit of* $\mathsf{O}(u)$.
   b) $sum = sum + b$.
3. *Return* sum/s.

Claim 4.6.5. *Let* Π *be an* m*-round protocol and let* $\alpha, \xi \in (0,1)$*. Assume that* $\widetilde{\mathsf{HonCont}}$ *is a* α*-honest continuator for* Π*, then* $\widetilde{\mathsf{Est}}^{(\xi,\widetilde{\mathsf{HonCont}})}$ *is* $(\alpha+\xi)$*-estimator for* Π *making* $\left\lceil \frac{\ln\left(\frac{2^{m+2}}{\xi}\right)}{2\cdot\xi^2} \right\rceil$ *calls to* $\widetilde{\mathsf{HonCont}}$.

Proof. Immediately follows from the fact that $\widetilde{\mathsf{HonCont}}$ is a α-honest continuator for Π and Claim 4.6.6. □

Claim 4.6.6. *Let Π be an m-round protocol, let $\alpha, \xi \in (0,1)$ and let $\widetilde{\mathsf{HonCont}}$ be an algorithm. Then for any $u \in \mathcal{V}(\Pi)$ it holds that* $\Pr\left[\left|\widetilde{\mathsf{Est}}(u) - \widetilde{\mathsf{HonCont}}(\Pi_u)\right| > \xi\right] \leq \xi/2^{m+1}$.

In order to prove Claim 4.6.6, we use the following fact derived from Hoeffding's bound.

Fact 4.6.7 (sampling)**.** *Let $X_1, \ldots, X_m \in [0,1]$ be independent and identically distributed boolean random variables and let $\mu = \mathrm{E}[X_i]$. If $m \geq \frac{\ln\left(\frac{2}{\delta}\right)}{2 \cdot \varepsilon^2}$, then*

$$\Pr\left[\left|\frac{1}{m}\sum_{i=1}^{m} X_i - \mu\right| \geq \varepsilon\right] \leq \delta.$$

Proof of Claim 4.6.6. Fix some $u \in \mathcal{V}(\Pi)$, let $\mu = \Pr\left[\widetilde{\mathsf{HonCont}}(u)_{\left|\widetilde{\mathsf{HonCont}}(u)\right|} = 1\right]$ and let $\widetilde{\mu} = \widetilde{\mathsf{Est}}^{(\xi,\widetilde{\mathsf{HonCont}})}(u)$. Plugging $\varepsilon = \xi$ and $\delta = \xi/2^{m+1}$ in Fact 4.6.7 now yields that

$$\Pr\left[|\widetilde{\mu} - \mu| > \xi\right] \leq \frac{\xi}{2^{m+1}}$$

□

From honest continuation to biased continuation

Algorithm 4.6.8 ($\widetilde{\mathsf{BiasedCont}}^{(\delta,\xi,\mathsf{O})}$)**.**

Input: transcript $u \in \{0,1\}^*$ and bit $b \in \{0,1\}$.

Oracle: algorithm O returning values in $\{0,1\}^{m-|u|-1}$.

Operation:

1. *For* $i = 1$ *to* $\left\lceil \frac{\log \xi}{\log(1-\delta)} \right\rceil$*:*

   a) *Let* s *be the last bit of* $\mathsf{O}(u)$.

   b) *If* $s = b$ *return* $\mathsf{O}(u)$.

2. *Return* $\perp$.

Claim 4.6.9. *Let* Π *be an* m*-round protocol and let* $\xi, \delta \in (0,1)$*. Assume that* $\widetilde{\mathsf{HonCont}}$ *is a* α*-honest continuator for* Π*, then* $\widetilde{\mathsf{BiasedCont}}^{(\delta,\xi,\widetilde{\mathsf{HonCont}})}$ *is a* $((t+2)\cdot \alpha + \xi, \delta)$*-biased continuator for* Π*, where* $t = \left\lceil \frac{\log \xi}{\log(1-\delta)} \right\rceil$.

Proof. We prove for the case that the second input of the algorithm is 1 (i.e., the algorithm is trying to find a continuation of the protocol that ends with 1), where the proof for the case that the second input of the algorithm is 0 is analogous. Fix $u \in \mathcal{V}(\Pi)$ with $\mathsf{val}(\Pi_u) \geq \delta$ and let $\mathsf{HonCont}$ be as in Definition 4.4.2. It is not difficult to verify that $\mathrm{SD}\left(\widetilde{\mathsf{BiasedCont}}^{(\delta,\xi,\mathsf{HonCont})}(u,1), \mathsf{BiasedCont}(u,1)\right) \leq \Pr\left[\widetilde{\mathsf{BiasedCont}}^{(\delta,\xi,\mathsf{HonCont})}(u,1) = \perp\right]$ Moreover, it holds that

$$\begin{aligned}
\Pr\left[\widetilde{\mathsf{BiasedCont}}^{(\delta,\xi,\mathsf{HonCont})}(u,1) = \perp\right] &= \left(\Pr\left[\mathsf{HonCont}(u)_{|\mathsf{HonCont}(u)|} = 0\right]\right)^t \\
&\leq (1-\delta)^t \\
&\leq \xi,
\end{aligned}$$

where the last inequality follows the choice of t.

Assume in addition that $\mathrm{SD}\left(\mathsf{HonCont}(u), \widetilde{\mathsf{HonCont}}(u)\right) \leq \alpha$. A standard hybrid argument shows that

$$\mathrm{SD}\left(\widetilde{\mathsf{BiasedCont}}^{(\delta,\xi\mathsf{HonCont})}(u,1), \widetilde{\mathsf{BiasedCont}}^{(\delta,\xi\widetilde{\mathsf{HonCont}})}(u,1)\right) \leq (t+1)\cdot\alpha$$

According to Definition 4.2.1 it holds that
$\Pr_{\ell\leftarrow\langle\Pi\rangle}\left[\exists i\in[m]\colon \mathrm{SD}\left(\widetilde{\mathsf{HonCont}}(\ell_{1,\ldots,i}), \mathsf{HonCont}(\ell_{1,\ldots,i})\right) > \alpha\right] \leq \alpha$, and the proof follows. □

Honest Continuation for Stateless Protocols

For stateless protocols (i.e., the parties maintain no state), providing (perfect) honest continuation is immediate.

Algorithm 4.6.10 ($\widetilde{\mathsf{HonCont}}_\Pi$)**.**

Parameters: protocol $\Pi = (\mathsf{A},\mathsf{B})$.

Input: transcript $u \in \{0,1\}^*$.

Operation:

1. *Choose uniformly at random coins* r_A *and* r_B *for the parties* A *and* B *respectively.*
2. *Return* $(\mathrm{trans}(\mathsf{A}(r_\mathsf{A}),\mathsf{B}(r_\mathsf{B}))(u))_{|u|+1,\ldots,m}$.

Claim 4.6.11. *Assume that* Π *is stateless, then* $\widetilde{\mathsf{HonCont}}_\Pi$ *of Algorithm 4.6.10 is* 0*-honest continuator for* Π.

Proof. Immediate. □

Main Theorem

We are finally ready to state and prove our main result – the existence of any constant bias coin-flipping protocol implies the existence of one-way functions.

Theorem 4.6.12 (main theorem, restatement of Theorem 1.1.1)**.** *Assume one-way functions do not exist. Then for any PPT coin-flipping protocol* $\Pi = (\mathsf{A}, \mathsf{B})$ *and* $\varepsilon > 0$*, there exist PPTM's* $\mathcal{A}$ *and* $\mathcal{B}$ *such that the following holds for infinitely many* n*'s.*

1. $(\mathcal{A}(1), \mathsf{B}) \geq 1 - \varepsilon$ *or* $(\mathsf{A}, \mathcal{B}(0)) \leq \varepsilon$*, and*
2. $(\mathcal{A}(0), \mathsf{B}) \leq \varepsilon$ *or* $(\mathsf{A}, \mathcal{B}(1)) \geq 1 - \varepsilon$*.*

Proof. Let $m(n) = \text{round}((\mathsf{A}, \mathsf{B})(1^n))$, and let $\rho_{\mathsf{A}}(n)$ and $\rho_{\mathsf{B}}(n)$ respectively, be the (maximal) number of random bits used by A and B on common input 1^n. By the assumption that Π is probabilistic polynomial time protocol, it follows that $m(n) \in \text{poly}(n)$. Consider the function f_Π over $1^* \times \{0,1\}^{\rho_{\mathsf{A}}(n)} \times \{0,1\}^{\rho_{\mathsf{B}}(n)} \times [m(n)]$, defined by

$$f_\Pi(1^n, r_{\mathsf{A}}, r_{\mathsf{B}}, i) = 1^n, \text{trans}((\mathsf{A}(r_{\mathsf{A}}), \mathsf{B}(r_{\mathsf{B}}))(1^n))_{1,\ldots,i} \tag{4.14}$$

In the following we remove Π from the subscript of f_Π and let $\widetilde{\mathsf{Inv}}_f$ be the ξ-inverter of f for some $\xi = 1/\text{poly}(n)$ to be determined by the analysis and for every n within an infinite size index set $\mathcal{I} \subseteq \mathbb{N}$, guaranteed to exists by Lemma 2.4.4.

In the rest of the proof we focus on proving the first case of the theorem, where the second can be proven symmetrically. Let Π_n be the variant of the protocol Π when the parties are given the security parameter 1^n. Set $\delta = \varepsilon/12$ and for every $n \in \mathcal{I}'$, let $\delta'_n \in [\delta/2, \delta]$ be such that

$\mathsf{neigh}_{\Pi_n}(2\delta'_n, 2\xi(n)) \leq m(n) \cdot \sqrt{2\xi(n)}$, guaranteed to exist from Proposition 4.4.9. Let κ such that $\mathsf{val}\left(\left(\mathsf{A}_{\Pi_n}^{[2\delta'_n,1-2\delta'_n]}\right)^{(\kappa)}, \mathsf{B}_{\Pi_n}^{[2\delta'_n,1-2\delta'_n]}\right) > 1-\varepsilon/2$ or $\mathsf{val}\left(\mathsf{A}_{\Pi_n}^{[2\delta'_n,1-2\delta'_n]}, \left(\mathsf{B}_{\Pi_n}^{[2\delta'_n,1-2\delta'_n]}\right)^{(\kappa)}\right) < \varepsilon/2$, guaranteed to exist for every $n \in \mathcal{I}$ from Theorem 3.1.3. Assume without loss of generality that there exists an infinite set $\mathcal{I}' \subseteq \mathcal{I}$ such that

$$\mathsf{val}\left(\left(\mathsf{A}_{\Pi_n}^{[2\delta'_n,1-2\delta'_n]}\right)^{(\kappa)}, \mathsf{B}_{\Pi_n}^{[2\delta'_n,1-2\delta'_n]}\right) > 1-\varepsilon/2 \tag{4.15}$$

for every $n \in \mathcal{I}'$. Let $c = c(\delta/2)$ from Lemma 4.3.1. Note that the bound attained by Lemma 4.3.1 holds for any $\delta' \geq \delta$ as well. Let $\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_\kappa)$ be such that $\gamma_i \in \mathrm{poly}(n)$, to be determined by the analysis, and let $\boldsymbol{\gamma}_n = (\gamma_1(n), \ldots, \gamma_\kappa(n))$. We recall that $\kappa \in \mathbb{N}$ is *constant* depending only on ε from Theorem 3.1.3, and not a function of n.

The settings of parameters above guarantee that the term in **??** is in $o(1)$. Applying Lemma 4.5.2 yields that

$$\begin{aligned}\mathsf{val}\left(\mathsf{A}_{\Pi_n}^{(\kappa,\delta'_n,\xi(n),\widetilde{\mathsf{Inv}}_f(n))}, \mathsf{B}_{\Pi_n}\right) &\geq \mathsf{val}\left(\left(\mathsf{A}_{\Pi_n}^{[2\delta'_n,1-2\delta'_n]}\right)^{(i)}, \mathsf{B}_{\Pi_n}^{[2\delta'_n,1-2\delta'_n]}\right) - 3\delta' - o(1) \\ &\geq 1 - \frac{\varepsilon}{2} - \frac{\varepsilon}{4} - o(1),\end{aligned} \tag{4.16}$$

where $\widetilde{\mathsf{Inv}}_f(n)$ is the variant of $\widetilde{\mathsf{Inv}}_f$ when restricted to inputs starting with 1^n. Our final adversary $\mathsf{A}'(1)$, on input 1^n, checks all possible candidates for δ'_n from Proposition 4.4.9, estimate the value of $\left(\mathsf{A}_{\Pi_n}^{(\kappa,\delta'_n,\xi(n),\widetilde{\mathsf{Inv}}_f(n))}, \mathsf{B}_{\Pi_n}\right)$ by running the latter for polynomial many times (this will only add exponentially small additive error) and find δ'_n such that

$$\mathsf{val}\left(\mathsf{A}_{\Pi_n}^{(\kappa,\delta'_n,\xi(n),state)}, \mathsf{B}_{\Pi_n}\right) \geq 1 - \varepsilon - o(1), \tag{4.17}$$

for any $n \in \mathcal{I}'$. The last step is to argue about the running time of $\mathcal{A}(1)$. By the setting of parameters above, the facts that κ is constant (i.e., independent of n) and that $T_{\widetilde{\mathsf{Inv}}_{f(n)}} \in \mathrm{poly}(n)$, by Proposition 4.5.3 it holds that $T_{\mathsf{final}}^{\delta'_n,\xi(n),\widetilde{\mathsf{Inv}}_{f(n)}}(\kappa) \in \mathrm{poly}(n)$. Since there are only $\mathrm{poly}(n)$ possibilities for setting δ'_n, it follows that the running time of $\mathcal{A}(1)$ is also is $\mathrm{poly}(n)$. $\square$

Appendix A

Missing Proofs

A.1 Proving Lemma 2.5.1

Lemma A.1.1 (Restatement of Lemma 2.5.1)**.** *Let* $x, y \in [0,1]$ *and* $a_1, \ldots, a_k, b_1, \ldots, b_k \in (0,1]$*. Then for any* $p_0, p_1 \geq 0$ *with* $p_0 + p_1 = 1$*, it holds that*

$$p_0 \cdot \frac{x^{k+1}}{\prod_{i=1}^{k} a_i} + p_1 \cdot \frac{y^{k+1}}{\prod_{i=1}^{k} b_i} \geq \frac{(p_0 x + p_1 y)^{k+1}}{\prod_{i=1}^{k} (p_0 a_i + p_1 b_i)}. \tag{A.1}$$

Proof. The lemma easily follows if one of the following holds: (1) $p_0 = 1, p_1 = 0$; (2) $p_0 = 0, p_1 = 1$; and (3) $x = y = 0$. Assuming $1 > p_0, p_1 > 0$ and $x + y > 0$, dividing Equation (A.1) by its right hand side (which is always positive) gives

$$p_0 \cdot \frac{\left(\frac{x}{(p_0 x + p_1 y)}\right)^{k+1}}{\prod_{i=1}^{k} \frac{a_i}{p_0 a_i + p_1 b_i}} + p_1 \cdot \frac{\left(\frac{y}{(p_0 x + p_1 y)}\right)^{k+1}}{\prod_{i=1}^{k} \frac{b_i}{p_0 a_i + p_1 b_i}} \geq 1. \tag{A.2}$$

Define the following variable changes.

$$z = \frac{p_0 x}{p_0 x + p_1 y} \qquad c_i = \frac{p_0 a_i}{p_0 a_i + p_1 b_i} \quad \text{for } 1 \leq i \leq k.$$

It follows that

$$1 - z = \frac{p_1 y}{p_0 x + p_1 y} \qquad 1 - c_i = \frac{p_1 b_i}{p_0 a_i + p_1 b_i} \quad \text{for } 1 \leq i \leq k.$$

Note that $0 \leq z \leq 1$ and that $0 < c_i < 1$ for every $1 \leq i \leq k$. Plugging the above into Equation (A.2), it remains to show that

$$\frac{z^{k+1}}{\prod_{i=1}^{k} c_i} + \frac{(1-z)^{k+1}}{\prod_{i=1}^{k}(1-c_i)} \geq 1 \tag{A.3}$$

for all $0 \leq z \leq 1$ and $0 < c_i < 1$. Equation (A.3) immediately follows for $z = 0, 1$, and in the rest of the proof we show that it also holds for $z \in (0,1)$. Define $f(z, c_1, \ldots, c_k) := \frac{z^{k+1}}{\prod_{i=1}^{k} c_i} + \frac{(1-z)^{k+1}}{\prod_{i=1}^{k}(1-c_i)} - 1$. Equation (A.3) follows by showing that $f(z, c_1, \ldots, c_k) \geq 0$ for all $z \in (0,1)$ and $0 < c_i < 1$. Taking the partial derivative with respect to c_i for $1 \leq i \leq k$, it holds that

$$\frac{\partial}{\partial c_i} f = -\frac{z^{k+1}}{c_i^2 \prod_{\substack{1 \leq j \leq k \\ j \neq i}} c_j} + \frac{(1-z)^{k+1}}{(1-c_i)^2 \prod_{\substack{1 \leq j \leq k \\ j \neq i}} (1-c_j)}.$$

Fixed $0 \leq z \leq 1$, and let $f_z(c_1, \ldots, c_k) = f(z, c_1, \ldots, c_k)$. If $c_1 = \ldots = c_k = z$, then for every $1 \leq i \leq k$ it holds that $\frac{\partial}{\partial c_i} f_z(c_1, \ldots, c_k) = \frac{\partial}{\partial c_i} f(z, c_1, \ldots, c_k) = 0$. Hence, f_z has a local extremum at $(c_1, \ldots, c_k) = (z, \ldots, z)$. Taking the second partial derivative with respect to c_i for $1 \leq i \leq k$, it holds that

$$\frac{\partial^2}{\partial c_i} f = \frac{2z^{k+1}}{c_i^3 \prod_{\substack{1 \leq j \leq k \\ j \neq i}} c_j} + \frac{2(1-z)^{k+1}}{(1-c_i)^3 \prod_{\substack{1 \leq j \leq k \\ j \neq i}} (1-c_j)} > 0,$$

and thus, $(c_1, \ldots, c_k) = (z, \ldots, z)$ is a local minimum of f_z.

The next step is to show that $(c_1, \ldots, c_k) = (z, \ldots, z)$ is a global minimum of f_z. This is done by showing that f_z is convex when $0 < c_i < 1$. Indeed, consider the function $-\ln(x)$. This is a convex function in for $0 < x < 1$. Thus the function $\sum_{i=1}^{k} -\ln(c_i)$, which is a sum of convex functions, is also convex. Moreover, consider the function e^x. This is a convex function for any x. Hence, the function $e^{\sum_{i=1}^{k} -\ln(c_i)} = \frac{1}{\prod_{i=1}^{k} c_i}$, which is a composition of two convex functions, is also convex for $0 < c_i < 1$. Since z is fixed, the function $\frac{z^{k+1}}{\prod_{i=1}^{k} c_i}$ is also convex.

Similar argument shows that $\frac{(1-z)^{k+1}}{\prod_{i=1}^{k}(1-c_i)}$ is also convex for $0 < c_i < 1$. This yields that f_z, which is a sum of two convex functions, is convex. It is known that a local minimum of a convex function is also a global minimum for that function [**?** , Therorem A, Chapter V], and thus $(z, \ldots, z)$ is a global minimum of f_z.

Let $z', c'_1, \ldots, c'_k \in (0, 1)$. Since $(z', \ldots, z')$ is a global minimum of $f_{z'}$, it holds that $f(z', z', \ldots, z') = f_{z'}(z', \ldots, z') \leq f_{z'}(c'_1, \ldots, c'_k) = f(z', c'_1, \ldots, c'_k)$. But $f(z', z', \ldots, z') = 0$, and thus $f(z', c'_1, \ldots, c'_k) \geq 0$. This shows that Equation (A.3) holds, and the proof is concluded. □

A.2 Proving Lemma 2.5.2

Lemma A.2.1 (Restatement of Lemma 2.5.2)**.** *For every $\delta \in (0, \frac{1}{2}]$, there exists $\alpha = \alpha(\delta) \in (0, 1]$ such that for every $x \geq \delta$*

$$\lambda \cdot a_1^{1+\alpha} \cdot (2 - a_1 \cdot x) + a_2^{1+\alpha} \cdot (2 - a_2 \cdot x) \leq (1 + \lambda) \cdot (2 - x) \tag{A.4}$$

for every $\lambda, y \geq 0$ with $\lambda y \leq 1$, where $a_1 = 1 + y$ and $a_2 = 1 - \lambda y$.

Proof. Fix $\delta \in (0, \frac{1}{2}]$. Rearranging the terms of Equation (A.4), one can equivalently prove that for some $\alpha \in (0, 1]$, it holds that

$$x \cdot (1 + \lambda - \lambda \cdot (1 + y)^{2+\alpha} - (1 - \lambda y)^{2+\alpha}) \tag{A.5}$$

$$\leq 2 \cdot (1 + \lambda - \lambda \cdot (1 + y)^{1+\alpha} - (1 - \lambda y)^{1+\alpha}) \tag{A.6}$$

for all x, λ and y in the proper range. Note that the above trivially holds, regardless of the choice of $\alpha \in (0, 1]$, in case $\lambda y = 0$ (both sides of the inequality are 0). In the following we show that for the cases $\lambda y = 1$ and $\lambda y \in (0, 1)$, Equation (A.5) holds for any small enough choice of α. Hence, the proof follows by taking the small enough α for which the above cases holds simultaneously.

$\lambda y = 1$**:** Let $z = \frac{1}{\lambda} + 1 = y + 1 > 1$. Plugging in Equation (A.5), we need to find $\alpha_h \in (0, 1]$ for which it holds that

$$x \cdot \left(1 + \frac{1}{z-1} - \frac{z^{2+\alpha}}{z-1}\right) \leq 2 \cdot \left(1 + \frac{1}{z-1} - \frac{z^{1+\alpha}}{z-1}\right) \tag{A.7}$$

for for all $z > 1$ and $\alpha \in (0, \alpha_h)$. Equivalently, by multiplying both sides by $\frac{z-1}{z}$ – which, since $z > 1$, is always positive – it suffices to find $\alpha_h \in (0, 1]$ for which it holds that

$$x \cdot (1 - z^{1+\alpha}) \leq 2 \cdot (1 - z^{\alpha}) \tag{A.8}$$

for all $z > 1$ and $\alpha \in (0, \alpha_h)$.

Since $1 - z^{1+\alpha} < 0$ for all $\alpha \geq 0$ and $z > 1$, and letting $h_\alpha(z) := \frac{z^\alpha - 1}{z^{1+\alpha} - 1}$, proving Equation (A.8) is equivalent to finding $\alpha_h \in (0, 1]$ such that

$$\delta \geq \sup_{z>1} \{2 \cdot h_\alpha(z)\} = 2 \cdot \sup_{z>1} \{h_\alpha(z)\} \tag{A.9}$$

for all $z > 1$ and $\alpha \in (0, \alpha_h)$.

Consider the function

$$h(w) := \sup_{z>1} \{h_w(z)\}, \tag{A.10}$$

Claim A.2.2 states that $\lim_{w \to 0^+} h(w) = 0$ (i.e., $h(w)$ approaches 0 when w approaches 0 from the positive side), and hence $2 \cdot \lim_{w \to 0^+} h(w) = 0$. The proof of Equation (A.9), and thus the proof of this part, follows since there is now small enough $\alpha_h < 1$ for which $x \geq 2 \cdot h(\alpha)$ for every $\alpha \in (0, \alpha_h]$ and $x \geq \delta$.

$\lambda y \in (0, 1)$**:** Consider the function

$$g(\alpha, \lambda, y) := 1 + \lambda - \lambda \cdot (1 + y)^{2+\alpha} - (1 - \lambda y)^{2+\alpha} \tag{A.11}$$

Claim A.2.3 states that for $\alpha \geq 0$, the function g is negative over the given range of λ and y. This allows us to complete the proof by finding $\alpha \in (0, 1]$ for which

$$\delta \geq 2 \cdot \sup_{\lambda, y > 0, \lambda y < 1} \left\{ f_\alpha(\lambda, y) := \frac{1 + \lambda - \lambda \cdot (1+y)^{1+\alpha} - (1-\lambda y)^{1+\alpha}}{1 + \lambda - \lambda \cdot (1+y)^{2+\alpha} - (1-\lambda y)^{2+\alpha}} \right\} \tag{A.12}$$

Consider the function

$$f(w) := \sup_{\lambda, y > 0, \lambda y < 1} \{ f_w(\lambda, y) \}, \tag{A.13}$$

Claim A.2.4 states that $\lim_{w \to 0^+} h(w) = 0$, and hence $(1+\delta) \cdot \lim_{w \to 0^+} h(w) = 0$. The proof of Equation (A.12), and thus the proof of this part, follows since there is now small enough $\alpha_f < 1$ for which $x \geq 2 \cdot h(\alpha)$ for every $\alpha \in (0, \alpha_f]$ and $x \geq \delta$.

By setting $\alpha_{\min} = \min \{\alpha_h, \alpha_f\}$, it follows that $x \geq h(\alpha), f(\alpha)$ for any $\alpha \in (0, \alpha_{\min})$ and $x \geq \delta$, concluding the the proof of the claim. □

Claim A.2.2. $\lim_{w \to 0^+} h(w) = 0$.

Proof. Simple calculations show that for fixed w, the function $h_w(z)$ is decreasing in the interval $(1, \infty)$. Indeed, fix some $w > 0$, and consider the derivative of h_w

$$\begin{aligned} h'_w(z) &= \frac{w z^{w-1}(z^{1+w} - 1) - (1+w) z^w (z^w - 1)}{(z^{1+w} - 1)^2} \\ &= \frac{-z^{w-1}(z^{1+w} - (1+w)z + w)}{(z^{1+w} - 1)^2} \end{aligned} \tag{A.14}$$

Let $p(z) := z^{1+w} - (1+w)z + w$. Taking the derivative of p and equaling it to 0, we have that

$$\begin{aligned} p'(z) = (1+w)z^w - (1+w) = 0 \\ \iff z = 1 \end{aligned} \tag{A.15}$$

Since $p''(1) = (1+w)w > 0$ for all $w > 0$, it holds that $z = 1$ is the minimum of p in $[1, \infty)$. Since $p(1) = 0$, it holds that $p(a) > 0$ for every $a \in (1, \infty)$. Thus, $h'_w(z) < 0$, and $h_w(z)$ is decreasing in the interval $(1, \infty)$. The latter fact yields that

$$\begin{aligned}
\lim_{w \to 0^+} h(w) &= \lim_{w \to 0^+} \sup_{z > 1} h_w(z) \\
&= \lim_{w \to 0^+} \lim_{z \to 1^+} \frac{z^w - 1}{z^{1+w} - 1} \\
&= \lim_{w \to 0^+} \lim_{z \to 1^+} \frac{w z^{w-1}}{(1+w) z^w} \\
&= \lim_{w \to 0^+} \frac{w}{1+w} \\
&= 0,
\end{aligned}$$

where the third equality holds by L'Hôpital's rule. □

Claim A.2.3. *For all $\alpha \geq 0$ and $\lambda, y > 0$ with $\lambda y < 1$, it holds that $g(\alpha, \lambda, y) < 0$.*

Proof. Fix $\lambda, y > 0$ with $\lambda y \leq 1$ and let $f(x) := g(x, \lambda, y)$. We first prove that f is strictly decreasing in the range $[0, \infty)$, and then show that $f(0) < 0$. Yielding that $g(\alpha, \lambda, y) < 0$ for the given range of parameters. Taking the derivative of f, we have that

$$f'(x) = -\lambda \cdot (1+y)^{2+x} \cdot \ln(1+y) + (1-\lambda y)^{2+x} \cdot \ln(1-\lambda y), \tag{A.16}$$

and since $\ln(1-\lambda y) < 0$, it holds that f' is a negative function. Hence, f is strictly decreasing, and takes its (unique) maximum over $[0, \infty)$ at 0. We conclude the proof noting that $f(0) = -\lambda \cdot y^2 \cdot (1+\lambda) < 0$. □

Claim A.2.4. $\lim_{w \to 0^+} f(w) = 0$.

Proof. Assume towards a contradiction that the claim does not holds. It follows that there exist $\varepsilon > 0$ and an infinite sequence $\{w_i\}_{i\in\mathbb{N}}$ such that $\lim_{i\to\infty} w_i = 0$ and $f(w_i) \geq \varepsilon$ for every $i \in \mathbb{N}$. Hence, there exists an infinite sequence of pairs $\{(\lambda_i, y_i)\}_{i\in\mathbb{N}}$, such that for every $i \in \mathbb{N}$ it holds that $f(w_i) = f_{w_i}(\lambda_i, y_i) \geq \varepsilon$, $\lambda_i, y_i > 0$ and $\lambda_i y_i \leq 1$.

In case $\{\lambda_i\}_{i\in\mathbb{N}}$ is not bounded from above, we focus on a subsequence of $\{(\lambda_i, y_i)\}$ in which λ_i converges to ∞, and let $\lambda^* = \infty$. Similarly, in case $\{y_i\}_{i\in\mathbb{N}}$ is not bounded from above, we focus on a subsequence of $\{(\lambda_i, y_i)\}$ in which y_i converges to ∞, and let $y^* = \infty$. Otherwise, by the Bolzano-Weierstrass Theorem, there exists a subsequence of $\{(\lambda_i, y_i)\}$ in which both λ_i and y_i converge to some real values. We let λ^* and y^* be these values.

The rest of the proof splits according to the values of λ^* and y^*. In each case we focus on the subsequence of $\{(w_i, \lambda_i, y_i)\}$ that converges to $(0, \lambda^*, y^*)$, and show that $\lim_{i\to\infty} f_{w_i}(\lambda_i, y_i) = 0$, in contradiction to the above assumption.

$y^* = \infty$: First note that the assumption $y^* = \infty$ and the fact that $\lambda_i y_i \leq 1$ for every i, yield that $\lambda^* = 0$.

For $c \in [0, 1)$, the Taylor's expansion with Lagrange remainder over the interval $[0, c]$ yields that

$$(1-c)^t = 1 - tc + \frac{t(t-1)(1-s)^{t-2}}{2}c^2 \tag{A.17}$$

for some $s \in (0, c)$. Consider the function

$$g(t, \lambda, y) := 1 + \lambda - \lambda \cdot (1+y)^t - (1-\lambda y)^t \tag{A.18}$$

Equation (A.17) yields that

$$g(t,\lambda_i,y_i) = 1+\lambda_i-\lambda_i\cdot(1+y_i)^t - \left(1-t\lambda_i y_i + \frac{t(t-1)(1-s_i)^{t-2}}{2}\lambda_i^2 y_i^2\right) \tag{A.19}$$
$$= \lambda_i\left(1-(1+y_i)^t + ty - \frac{t(t-1)(1-s_i)^{t-2}}{2}\lambda_i y_i^2\right)$$

for every index i and some $s_i \in (0,\lambda_i y_i)$. We conclude that

$$\begin{aligned}
\lim_{i\to\infty} f_{w_i}(\lambda_i,y_i) &= \lim_{i\to\infty}\frac{g(1+w_i,\lambda_i,y_i)}{g(2+w_i,\lambda_i,y_i)}\\
&= \lim_{i\to\infty}\frac{1-(1+y_i)^{1+w_i}+(1+w_i)y_i - \frac{(1+w_i)w_i(1-s_i)^{w_i-1}}{2}\lambda_i y_i^2}{1-(1+y_i)^{2+w_i}+(2+w_i)y_i - \frac{(2+w_i)(1+w_i)(1-s_i)^{w_i}}{2}\lambda_i y_i^2}\\
&= \lim_{i\to\infty}\frac{\frac{1}{(1+y_i)^{2+w_i}} - \frac{(1+y_i)^{1+w_i}}{(1+y_i)^{2+w_i}} + \frac{(1+w_i)y_i}{(1+y_i)^{2+w_i}} - \frac{(1+w_i)w_i(1-s_i)^{w_i-1}\lambda_i y_i^2}{2(1+y_i)^{2+w_i}}}{\frac{1}{(1+y_i)^{2+w_i}} - 1 + \frac{(2+w_i)y_i}{(1+y_i)^{2+w_i}} - \frac{(2+w_i)(1+w_i)(1-s_i)^{w_i}\lambda_i y_i^2}{2(1+y_i)^{2+w_i}}}\\
&= 0.
\end{aligned}$$

$\lambda^* = \infty$: Note that the assumption $\lambda^* = \infty$ yields that $y^* = 0$. For $c \in [0,1)$, the Taylor's expansion with Lagrange remainder over the interval $[0,c]$ yields that that

$$(1-c)^t = 1 - tc + \frac{t(t-1)}{2}c^2 - \frac{t(t-1)(t-2)(1-s)^{t-3}}{6}c^3, \tag{A.20}$$

for some $s \in (0,c)$, and

$$(1+c)^t = 1 + tc + \frac{t(t-1)}{2}c^2 + \frac{t(t-1)(t-2)(1+s')^{t-3}}{6}c^3, \tag{A.21}$$

for some $s' \in (0,c)$.

Applying Equations (A.20) and (A.21) for the function g of Equation (A.18), yields that

$$
\begin{aligned}
& g(t,\lambda_i,y_i) && \text{(A.22)}\\
& = \widetilde{g}(t,\lambda_i,y_i,s_i,s_i') \\
& := 1+\lambda_i-\lambda_i\left(1+ty+\frac{t(t-1)}{2}y_i^2+\frac{t(t-1)(t-2)(1+s_i')^{t-3}}{6}y_i^3\right) \\
& \quad -\left(1-t\lambda_i y_i+\frac{t(t-1)}{2}\lambda_i^2y_i^2+\frac{t(t-1)(t-2)(1-s_i)^{t-3}}{6}\lambda_i^3y_i^3\right) \\
& = -\frac{\lambda_i^2y_i^2}{6}\Big(\frac{3t(t-1)}{\lambda_i}+\frac{t(t-1)(t-2)(1+s_i')^{t-3}y_i}{\lambda_i} && \text{(A.23)}\\
& + 3t(t-1)+t(t-1)(t-2)(1-s_i)^{t-3}\lambda_i y_i\Big)
\end{aligned}
$$

for large enough index i and some $s_i \in (0,\lambda_i y_i)$ and $s_i' \in (0,y_i)$. We conclude that

$$
\begin{aligned}
& \lim_{i\to\infty} f_{w_i}(\lambda_i,y_i) \\
& = \lim_{i\to\infty}\frac{g(1+w_i,\lambda_i,y_i)}{g(2+w_i,\lambda_i,y_i)} \\
& = \lim_{i\to\infty}\frac{\widetilde{g}(1+w_i,\lambda_i,y_i,s_i,s_i')}{\widetilde{g}(2+w_i,\lambda_i,y_i,s_i,s_i')} \\
& = 0,
\end{aligned}
$$

where the before to last equality holds since $\lambda_i y_i \le 1$ for every i, and hence the last term of the numerator and denominator goes to 0 when $i\to\infty$.

$\lambda^*, y^* > 0$: It holds that

$$
\begin{aligned}
\lim_{i\to\infty} f_{w_i}(\lambda_i,y_i) &= \lim_{i\to\infty}\frac{1+\lambda_i-\lambda_i\cdot(1+y_i)^{1+w_i}-(1-\lambda_i y_i)^{1+w_i}}{1+\lambda_i-\lambda_i\cdot(1+y_i)^{2+w_i}-(1-\lambda_i y_i)^{2+w_i}} \\
&= \frac{1+\lambda^*-\lambda^*(1+y^*)-(1-\lambda^*y^*)}{1+\lambda^*-\lambda^*(1+y^*)^2-(1-\lambda^*y^*)^2} \\
&= 0.
\end{aligned}
$$

$\lambda^* = 0$ and $y^* > 0$: Equations (A.17) and (A.19) yields that

$$\begin{aligned}\lim_{i\to\infty} f_{w_i}(\lambda_i, y_i) &= \lim_{i\to\infty} \frac{1-(1+y_i)^{1+w_i}+(1+w_i)y_i - \frac{(1+w_i)w_i(1-s_i)^{w_i-1}}{2}\lambda_i y_i^2}{1-(1+y_i)^{2+w_i}+(2+w_i)y_i - \frac{(2+w_i)(1+w_i)(1-s_i)^{w_i}}{2}\lambda_i y_i^2} \\ &= \frac{1-(1+y^*)+y^*}{1-(1+y^*)^2+2y^*} \\ &= 0.\end{aligned}$$

$y^* = 0$: Rearranging Equation (A.22) yields that the following holds for large enough index i.

$$\begin{aligned}& g(t, \lambda_i, y_i) && \text{(A.24)} \\ &= \widetilde{g}(t, \lambda_i, y_i, s_i, s_i') \\ &= -\frac{\lambda_i y_i^2}{6}(3t(t-1) + t(t-1)(t-2)(1+s_i')^{t-3} y_i + 3t(t-1)\lambda_i && \text{(A.25)} \\ &+ t(t-1)(t-2)(1-s_i)^{t-3}\lambda_i^2 y_i)\end{aligned}$$

for some $s_i \in (0, \lambda_i y_i)$ and $s_i \in (0, y_i)$. Giving this formulation it is easy to see that

$$\begin{aligned}\lim_{i\to\infty} f_{w_i}(\lambda_i, y_i) &= \lim_{i\to\infty} \frac{\widetilde{g}(1+w_i, \lambda_i, y_i, s_i, s_i')}{\widetilde{g}(2+w_i, \lambda_i, y_i, s_i, s_i')} \\ &= \frac{0}{6+6\lambda^*} \\ &= 0.\end{aligned}$$

The above holds since every term in numerator goes to 0 and the terms $3(2+w_i)(1+w_i)$ in the denominator goes to 6.

This conclude the case analysis, and thus the proof of the claim. □

Bibliography

[ABC+85] B. Averbuch, M. Blum, B. Chor, S. Goldwasser, and S. Micali. How to implement Bracha's $O(\log n)$ Byzantine agreement algorithm, 1985. Unpublished manuscript.

[Blu81] Manuel Blum. Coin flipping by telephone. In *Advances in Cryptology – CRYPTO '81*, pages 11–15, 1981.

[BOO10] Amos Beimel, Eran Omri, and Ilan Orlov. Protocols for multiparty coin toss with dishonest majority. In *Advances in Cryptology – CRYPTO 2010*, pages 538–557, 2010.

[CI93] Richard Cleve and Russell Impagliazzo. Martingales, collective coin flipping and discrete control processes (extended abstract). `http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.51.1797`, 1993.

[CK09] A. Chailloux and I. Kerenidis. Optimal quantum strong coin flipping. In *Proceedings of the 50th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 527–533, 2009.

[Cle86] Richard Cleve. Limits on the security of coin flips when half the processors are faulty. In *Proceedings of the 18th Annual ACM Symposium on Theory of Computing (STOC)*, pages 364–369, 1986.

[DSLMM11] Dana Dachman-Soled, Yehuda Lindell, Mohammad Mahmoody, and Tal Malkin. On the black-box complexity of optimally-fair coin tossing. In *Theory of Cryptography, 8th Theory of Cryptography Conference, TCC 2011*, volume 6597, pages 450–467, 2011.

[GGM84] Oded Goldreich, Shafi Goldwasser, and Silvio Micali. On the cryptographic applications of random functions. In *Advances in Cryptology – CRYPTO '84*, pages 276–288, 1984.

[GGM86] Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions. *Journal of the ACM*, pages 792–807, 1986.

[GL89] Oded Goldreich and Leonid A. Levin. A hard-core predicate for all one-way functions. In *Proceedings of the 21st Annual ACM Symposium on Theory of Computing (STOC)*, pages 25–32, 1989.

[HILL99] Johan Håstad, Russell Impagliazzo, Leonid A. Levin, and Michael Luby. A pseudorandom generator from any one-way function. *SIAM Journal on Computing*, pages 1364–1396, 1999.

[HNO+09] Iftach Haitner, Minh Nguyen, Shien Jin Ong, Omer Reingold, and Salil Vadhan. Statistically hiding commitments and statistical zero-knowledge arguments from any one-way function. *SIAM Journal on Computing*, 39(3):1153–1218, 2009.

[HO11] Iftach Haitner and Eran Omri. Coin Flipping with Constant Bias Implies One-Way Functions. In *Proceedings of the 52nd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 110–119,

2011.

[IL89] Russell Impagliazzo and Michael Luby. One-way functions are essential for complexity based cryptography. In *Proceedings of the 30th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 230–235, 1989.

[Kit03] A. Y. Kitaev. Quantum coin-flipping. Presentation at the 6th workshop on quantum information processing (qip 2003), 2003.

[MNS09] Tal Moran, Moni Naor, and Gil Segev. An optimally fair coin toss. In *Theory of Cryptography, 6th Theory of Cryptography Conference, TCC 2009*, pages 1–18, 2009.

[Moc07] Carlos Mochon. Quantum weak coin flipping with arbitrarily small bias. arXiv:0711.4114, 2007.

[MPS10] Hemanta K. Maji, Manoj Prabhakaran, and Amit Sahai. On the Computational Complexity of Coin Flipping. In *Proceedings of the 51st Annual Symposium on Foundations of Computer Science (FOCS)*, pages 613–622, 2010.

[Nao91] Moni Naor. Bit commitment using pseudorandomness. *Journal of Cryptology*, pages 151–158, 1991.

[NY89] Moni Naor and Moti Yung. Universal one-way hash functions and their cryptographic applications. In *Proceedings of the 21st Annual ACM Symposium on Theory of Computing (STOC)*, pages 33–43, 1989.

[Rom90] John Rompel. One-way functions are necessary and sufficient for secure signatures. In *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing (STOC)*, pages 387–394, 1990.

[Zac86] Stathis Zachos. Probabilistic Quantifiers, Adversaries, and Complexity Classes: An Overview. In *Proceedings of the First Annual IEEE Conference on Computational Complexity*, pages 383–400, 1986.