Fair Coin Flipping: Tighter Analysis and the Many-Party Case

Niv Buchbinder* Iftach Haitner†‡ Nissan Levi† Eliad Tsfadia†

February 19, 2018

Abstract

In a multi-party *fair* coin-flipping protocol, the parties output a common (close to) unbiased bit, even when some corrupted parties try to bias the output. In this work we focus on the case of arbitrary number of corrupted parties. Cleve [19] [STOC 1986] has shown that in *any* such m-round coin-flipping protocol, the corrupted parties can bias the honest parties' common output bit by $\Theta(1/m)$. For more than two decades, however, the best known coin-flipping protocol was the one of Awerbuch, Blum, Chor, Goldwasser, and Micali [10] [Manuscript 1985], who presented a t-party, m-round protocol with bias $\Theta(t/\sqrt{m})$. This was changed by the breakthrough result of Moran, , Naor, and Segev [43] [TCC 2009, Journal of Cryptology 2016], who constructed an m-round, *two*-party coin-flipping protocol with optimal bias $\Theta(1/m)$. Recently, Haitner and Tsfadia [33] [STOC 14] constructed an m-round, *three*-party coin-flipping protocol with bias $O(\log^3 m/m)$. Still for the case of more than three parties, the best known protocol remained the $\Theta(t/\sqrt{m})$-bias protocol of [10].

We make a step towards eliminating the above gap, presenting a t-party, m-round coin-flipping protocol, with bias $O(\frac{t^4 \cdot 2^t \cdot \sqrt{\log m}}{m^{1/2+1/(2^{t-1}-2)}})$. This improves upon the $\Theta(t/\sqrt{m})$-bias protocol of [10] for any $t \leq \frac{1}{2} \cdot \log\log m$, and in particular for $t \in O(1)$, it is a $1/m^{\frac{1}{2}+\Theta(1)}$-bias protocol. For the three-party case, it is an $O(\sqrt{\log m}/m)$-bias protocol, improving over the $O(\log^3 m/m)$-bias protocol of [33].

Our protocol generalizes that of [33], by presenting an appropriate "defense protocols" for the remaining parties to interact in, in the case that some parties abort or caught cheating ([33] only presented a two-party defense protocol, which limits their final protocol to handle three parties). We prove the fairness of the new protocol by presenting a new paradigm for analyzing fairness of coin-flipping protocols; the claimed fairness is proved by mapping the set of adversarial strategies that try to bias the honest parties outcome in the protocol to the set of the feasible solutions of a linear program. The gain each strategy achieves is the value of the corresponding solution. We then bound the the optimal value of the linear program by constructing a feasible solution to its dual.

Keywords: coin-flipping; fair computation; stopping time problems

*Statistics and Operations Research, Tel Aviv university. E-mail:niv.buchbinder@gmail.com.

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

‡Member of the Israeli Center of Research Excellence in Algorithms (ICORE) and the Check Point Institute for Information Security.

Contents

1 Introduction

In a multi-party *fair* coin-flipping protocol, the parties wish to output a common (close to) unbiased bit, even though some of the parties may be corrupted and try to bias the output. More formally, such protocols should satisfy the following two properties: first, when all parties are honest (i.e., follow the prescribed protocol), they all output the *same* bit, and this bit is unbiased (i.e., uniform over $\{0,1\}$). Second, even when some parties are corrupted (i.e., collude and arbitrarily deviate from the protocol), the remaining parties should still output the *same* bit, and this bit should not be too biased (i.e., its distribution should be close to uniform over $\{0,1\}$). We emphasize that unlike weaker variants of coin-flipping protocol known in the literature, the honest parties should **always** output a common bit, regardless of what the corrupted parties do, and in particular they are not allowed to abort if a cheat was detected.

When a majority of the parties are honest, efficient and *completely* fair coin-flipping protocols are known as a special case of secure multi-party computation with an honest majority [15].[1] However, when there is no honest majority, the situation is more complex.

Negative results. Cleve [19] showed that for *any* efficient two-party m-round coin-flipping protocol, there exists an efficient adversarial strategy to bias the output of the honest party by $\Theta(1/m)$. This lower bound extends to the multi-party case, with no honest majority, via a simple reduction.

Positive results. Awerbuch, Blum, Chor, Goldwasser, and Micali [10] showed, that if one-way functions exist, a simple m-round majority protocol can be used to derive a t-party coin-flipping protocol with bias $\Theta(t/\sqrt{m})$.[2]

For more than two decades, Awerbuch et al.'s protocol was the best known fair coin-flipping protocol (without honest majority), under *any* hardness assumption and for *any* number of parties. In their breakthrough result, Moran, , Naor, and Segev [43] constructed an m-round, *two*-party coin-flipping protocol with optimal bias of $\Theta(1/m)$. In a subsequent work, Beimel, Omri, and Orlov [12] extended the result of [43] for the multi-party case in which *less than* $\frac{2}{3}$ of the parties can be corrupted. More specifically, for any $\ell < \frac{2}{3} \cdot t$, they presented an m-round, t-party protocol, with bias $\frac{2^{2^{\ell-t}}}{m}$ against (up to) ℓ corrupted parties. Recently, Haitner and Tsfadia [33] constructed an m-round, *three*-party coin-flipping protocol with bias $O(\log^3 m/m)$ against two corruptions. In a subsequent work, Alon and Omri [4] presented for any $t \in O(1)$, an m-round, t-party coin-flipping protocol, with bias $O(\log^3 m/m)$ against $\ell < 3t/4$ corrupted parties. All the above results hold under the assumption that oblivious transfer protocols exist.

Yet, for the case of more than three parties (and unbounded number of corruptions), the best known protocol was the $\Theta(t/\sqrt{m})$-bias protocol of [10].

1.1 Our Result

Our main result is a new multi-party coin flipping protocol.

[1] Throughout, we assume a broadcast channel is available to the parties. By [21], broadcast channel is necessary for fair coin-flipping protocol secure against third, or more, corruptions.

[2] The result of Awerbuch et al. [10] was never published, and it is contributed to them by Cleve [19] who analyzed the two-party case. Cleve [19] analysis extends to the many party case in a straightforward manner. The protocol of [19] is using family of trapdoor permutations, but the latter were merely used to construct commitment schemes, which we currently know how to construct from any one-way function [35, 36, 44].

Theorem 1.1 (main theorem, informal)**.** *Assuming the existence of oblivious transfer protocols, then for any $m = m(n) \leq \text{poly}(n)$ and $t = t(n) \leq \frac{1}{2}\log\log m$, there exists an m-round, t-party coin-flipping protocol, with bias $O(\frac{t^4 \cdot 2^t \cdot \sqrt{\log m}}{m^{1/2+1/(2^{t-1}-2)}})$ (against $t-1$ corrupted parties).*

The above protocol improves upon the $\Theta(t/\sqrt{m})$-bias protocol of Awerbuch et al. [10] for any $t \leq \frac{1}{2} \cdot \text{loglog}\, m$. For $t \in O(1)$, this yields an $1/m^{\frac{1}{2}+\Theta(1)}$-bias protocol. For the three-party case, the above yields an $O(\sqrt{\log m}/m)$-bias protocol, improving over the the $O(\log^3 m/m)$-bias protocol of Haitner and Tsfadia [33].

We analyze the new protocol by presenting a new paradigm for analyzing fairness of coin-flipping protocols. We upper bound the bias of the protocol by upper-bounding the value of a linear program that *characterizes it*: there exists an onto mapping from the set of adversarial strategies that try to bias the honest parties outcome in the protocol, to the set of the program's feasible solutions, such that the gain a strategy achieves is, essentially, the value of the solution of the program it is mapped to. See Section 1.3 for more details.

1.2 The New Multi-Party Fair Coin-Flipping Protocol

Our fair-flipping protocol follows the paradigm of Haitner and Tsfadia [33]. In the following we focus on efficient *fail-stop* adversaries: ones that follow the protocol description correctly and their only adversarial action is abort prematurely (forcing the remaining parties to decide on their common output without them). Compiling a protocol secure against such fail-stop adversaries into a protocol of the same bias that is secure against *any* efficient adversary, can be done using standard cryptographic tools. We also assume the parties can *securely compute with abort* any efficient functionality — The only information a party obtains from such a computation is its local output (might be a different output per party). The order of which the outputs are given by such functionality, however, is arbitrary. In particular, a "rushing" party that aborts after obtaining its own output, prevents the remaining parties to get their outputs. For every efficient functionality, a constant-round protocol that securely compute it with abort can be constructed using *oblivious transfer* protocol.

The protocol of Haitner and Tsfadia [33] enhances the basic majority coin-flipping protocol of Awerbuch et al. [10] with *defense protocols* for the remaining parties to interact in, if some of the parties abort. We consider the following generalization of the [33] m-round protocol for arbitrary number of parties. The functionality $\mathsf{Defense}$ and the sub-protocols $\{\Pi^{t'}\}_{t'<t}$ used in the protocol are specified later.

Protocol 1.2 ($\widehat{\Pi}^t = (\mathsf{P}_1, \mathsf{P}_2, \ldots, \mathsf{P}_t)$)**.**

For $i = 1$ to m:

1. *Every (proper) subset of parties $\mathcal{Z} \subsetneq \{\mathsf{P}_1, \mathsf{P}_2, \ldots, \mathsf{P}_t\}$ securely compute $\mathsf{Defense}^{|\mathcal{Z}|}()$. Let $\mathsf{share}^{\#z,\mathcal{Z}}$ be the output party P_z received from this call.*

2. *The parties securely compute $\mathsf{Coin}()$ that returns a common uniform $\{-1, 1\}$ coin c_i.*[3]

Output: All parties output $\mathsf{sign}(\sum_{i=1}^{m} c_i)$.

Abort: Let $\mathcal{Z} \subsetneq \{\mathsf{P}_1, \ldots, \mathsf{P}_t\}$ be the remaining (non-aborting) parties. To decide on a common output, the parties in $\mathcal{Z}$ interact in the "defense" protocol $\Pi^{|\mathcal{Z}|}$, where party P_z private input is $\mathsf{share}^{\#z,\mathcal{Z}}$. If $\mathcal{Z} = \{\mathsf{P}_z\}$ (i.e., only a single non-aborting party remained), the party P_z outputs $\mathsf{share}^{\#z,\mathcal{Z}}$.

Note that for odd value of m, the common output in an all-honest execution is a uniform bit. To instantiate the above protocol one needs to define the functionality $\mathsf{Defense}^{t'}$ and the protocol $\Pi^{t'}$, for all $t' < t$. But first let's discuss whether we need these functionality and protocols at all. That is, why not simply instruct the remaining parties to re-toss the coin c_i if some parties abort in Step 2 of the i'th round. This is essentially the vanilla protocol of Awerbuch et al. [10], and it is not hard to get convinced that a malicious (fail-stop) party can bias the output of the protocol by $\Theta(1/\sqrt{m})$. To see that, note that the sum of m unbiased $\{-1, 1\}$ coins is roughly uniform over $[-\sqrt{m}, \sqrt{m}]$. In particular, the probability that the sum is in $\{-1, 1\}$ is $\Theta(1/\sqrt{m})$. It follows that if a party aborts after seeing in Step 2 of the first round that $c_1 = 1$, and by that causing the remaining parties to re-toss c_1, it biases the final outcome of the protocol towards 0 by $\Theta(1/\sqrt{m})$.

To improve upon this $1/\sqrt{m}$ barrier, [33] have defined $\mathsf{Defense}$ such that the expected outcome of $\Pi^{t'}(\mathsf{Defense}(1^{t'}))$ equals $\delta_i = \Pr\left[\mathsf{sign}(\sum_j c_j) = 1 | c_1, \ldots, c_i\right]$ for every t'. Namely, the expected outcome of the remaining parties has *not changed*, if some parties abort in Step 2 of the protocol.[4] The above correlation of the defense values returned by $\mathsf{Defense}$ in Step 1 and the value of c_i returned by Coin in Step 2, however, yields that they give some information about c_i, and thus the (only) weak point of the protocol has shifted to Step 1. Specifically, the bias achieved by aborting in Step 1 of round i is the difference between δ_{i-1}, the expected value of the protocol given the coins $c_1, \ldots, c_{i-1}$ flipped in the previous rounds, and the expected outcome of the protocol given these coins and the defense values given to the corrupted parties in Step 1. If done properly, only limited information about c_i is revealed in Step 1, and thus attacking there is not as effective as attacking in Step 2 of the vanilla (no defense) protocol.

For $t = 2$, [33] have set the defense for the remaining party to be a bit b_i that is set to 1 with probability δ_i. Namely, if a party aborts in Step 2 of the i'th round, the other party output 1 with probability δ_i, and 0 otherwise. Since $\mathrm{E}[b_i] = \delta_i$, attacking in Step 2 (in any round) of the protocol is useless. Moreover, since b_i only leaks "limited information" about δ_i (and thus about c_i), it is possible to show that attacking in Step 1 (in any round) biases the protocol by $(\delta_i - \delta_{i-1})^2$ (to compare to the $(\delta_i - \delta_{i-1})$ bias achieved in Step 2 of the vanilla protocol). These

[3] In the actual implementation of the protocol, see Section 3, in round i Coin returns $(m + 1 - i)^2$ coins.

[4] The above definition requires $\mathsf{Defense}$ to share a (secret) state with Coin, since both functionalities are defined with respect to the same coin c_i. This non-standard requirement is only for the sake of presentation, and in the actual protocol we replace it with stateless functionalities that share, and maintain, their "state" by secret sharing it between the parties. See Section 3.

observations yield (see Section 1.3) that the protocol's bias is $\text{polylog}(m)/m$.[5] Generalizing the above for even $t = 3$, however, is non-trivial. The defense values of the remaining parties should allow them to interact in a *fair* protocol Π^2 of expected outcome δ_i. Being fair, protocol Π^2 should contain a defense mechanism of its own to avoid one of the remaining parties to bias its outcome by too much (this was not an issue in the the case $t = 1$, in which there is only one remaining party). Yet, [33] managed to find such an implementation of the Defense functionality and Π^2 that yield a $\text{polylog}(m)/m$-bias protocol.[6] The rather complicated approach use by [33], however, was very tailored for the case that defense sub-protocol Π^2 is a two-party protocol. In particular, it critically relies on the fact that in a two-party protocol there is no defense sub-protocol (rather, the remaining party decides on its output by its own). We take a very different approach to implement the Defense functionality and its accompanied defense protocol $\Pi^{t'}$.[7]

Algorithm 1.3 (The Defense functionality)**.**

Input: $1^{t'}$

//Recall that $c_1, \ldots, c_{i-1}$ are the coins flipped in the previous rounds, c_i is the coin to be output in this round call to Coin*, and* $\delta_i = \Pr\left[\mathsf{sign}(\sum_j c_j) = 1 | c_1, \ldots, c_i\right]$.

1. *Let $\delta'_i = \delta_i + Noise$, where $Noise$ is random variable of expectation 0.*
2. *Let $\mathsf{share}^{\#1}, \ldots, \mathsf{share}^{\#t'}$ be t'-out-of-t' secret sharing of δ'_i.[8] Return $\mathsf{share}^{\#i}$ to the i'th party.*

Namely, Defense computes a noisy version of δ_i and secret-share the result between the calling parties.

Protocol 1.4 ($\Pi^{t'} = (\mathsf{P}_1, \mathsf{P}_2, \ldots, \mathsf{P}_{t'})$)**.**

Input: Party P_z's input is $\mathsf{share}^{\#z}$.

1. *Each party P_z sends its input $\mathsf{share}^{\#z}$ to the other parties, and all parties set $\delta' = \bigoplus_{z=1}^{t'} \mathsf{share}^{\#z}$.*
2. *Continue as the δ'-biased version of Protocol $\widehat{\Pi}^{t'}$:*
   - Coin *sets the coin c_i to be 1 with probability $1/2+\varepsilon$ (rather than $1/2$), for $\varepsilon \in [-1, 1]$ being the value such that δ' is the probability that the sum of m independent $(1/2 + \varepsilon)$-biased $\{-1, 1\}$ coins is positive.*
   - *The definition of* Defense *is changed accordingly to reflect this change in the bias of the coins.*

[5] More precisely, this bound was proved for the weighted variant of the above protocol, where in round i the functionality Coin returns the sum of $m - i + 1$ independent coins. See Section 3.

[6] The analysis we employ in this paper, see Section 1.3, shows that the bias of (a simple variant of) the [33] protocols is actually $\sqrt{\log m}/m$.

[7] For subsets of size two, we are still using the mechanism of [33] that handles such subsets better. We ignore this subtlety for the sake of the introduction.

[8] I.e., $\{\mathsf{share}^{\#i}\}$ are uniform strings conditioned on $\bigoplus_{i=1}^{t'} \mathsf{share}^{\#i} = \delta'_i$. (We assume for simplicity that δ'_i has a short binary representation.)

Since $\mathrm{E}[Noise] = 0$, the expected outcome of $\Pi^{t'}(\mathsf{Defense}(1^{t'}))$ is indeed δ_i. Note that since the corrupted parties can use their shares to reconstruct the value of δ'_i sampled in the all-corrupted calls to $\mathsf{Defense}$ (those calls made by subsets in which all parties are corrupted), the values returned by $\mathsf{Defense}$ do leak some information about δ_i, and thus about the coin c_i. But if $Noise$ is "noisy enough" (i.e., high enough variance), then δ'_i does not leak too much information about δ_i. Hence, by taking noisy enough $Noise$, we make $\widehat{\Pi}^t$ robust against a single abort (this is similar to the two-party protocol). On its second abort, however, an attacker is actually attacking the above sub-protocol $\Pi^{t'}$, which provides the attacker a very effective attack opportunity: the attacker who is first to reconstruct $\delta' = \delta'_i$, can choose to abort and by that make the remaining parties to continue with an execution whose expected outcome is δ_i. Hence, it can bias the protocol's outcome by $\delta_i - \delta'_i$. If δ'_i is with high probability far from δ_i, this makes the resulting protocol unfair. A partial solution for this problem is to defend the reconstruction of δ' in a similar way to how we defend the reconstruction of the coin c_i; before reconstruction the value of δ', call (a variant of) $\mathsf{Defense}$ to defend the parties in the case an abort happens in the reconstruction step. As in the two-party protocol we mentioned before, the use of $\mathsf{Defense}$ reduces the bias from $\delta_i - \delta'_i$ to $(\delta_i - \delta'_i)^2$. This limitation dictates us to choose $Noise$ of bounded variance. But when using such a $Noise$ function, we are no longer in the situation where δ'_i does not leak significant information about δ_i, making the protocol $\widehat{\Pi}^t$ vulnerable to aborting attacks. The solution is to choose a variance of $Noise$ that compromises between these two contradicting requirements. For not too large t, the right choice of parameters yields a protocol of the claimed biased, significantly improving over the $(1/\sqrt{m})$-bias vanilla protocol.

1.3 Proving Fairness via Linear Program

The security of Protocol 1.2 described in the previous section, can be reduced to the value of the appropriate *online binomial game*, first considered by [33].

Online binomial games. An m-round online-binomial game is a game between the (honest, randomized) challenger and an all-powerful player. The game is played for m rounds. At round i, the challenger tosses an independent $\{-1, 1\}$ coin c_i. The final outcome of the game is set to one if the overall sum of the coins is positive. Following each round, the challenger sends the player some information (i.e., *hint*) about the outcome of the coins tossed until this round. After getting the hint, the player decides whether to *abort*, or to continue playing. If aborts, the game stops and the player is rewarded with δ_{i-1} — the probability that the output of the game is one given coins $c_1, \ldots, c_{i-1}$. If never aborted, the player is rewarded with the (final) outcome of the game.[9] The bias of an m-round game G_m, denoted $\mathsf{Bias}(\mathsf{G}_m)$, is the advantage the *best* all-powerful player achieves over the passive (non-aborting) player, namely its expected reward minus $\frac{1}{2}$.

The connection between such line Binomial games and the coin-flipping protocols $\widehat{\Pi}^t$ described in the previous section is rather straightforward. Recall that an adversary controlling some of the parties in an execution of Protocol $\widehat{\Pi}^t$ gains nothing by aborting in Step 2, and thus we can assume without loss of generality that it only aborts, if ever, at Step 1 of some rounds.[10] Recall that the

[9] A different and somewhat more intuitive way to think about the game is as follows. In each round, after getting the hint, the player can instruct the challenger to *re-toss* the current round coin, but it can only do that at most once during the duration of the game. After the game ends, the player is rewarded with its final outcome.

[10] Actually, in an inner sub-protocols $\Pi^{t'}$ the attacker can also aborts in the steps where δ' is reconstructed. But

gain achieved from aborting in Step 1 of round i is the difference between δ_{i-1}, here the expected outcome of the protocol given the coins $c_1, \ldots, c_{i-1}$ flipped in the previous rounds, and the expected outcome of the protocol given these coins and the defense values given to the corrupted parties in Step 1. It follows that the maximal bias obtained by a *single* abort, is exactly the bias of the online binomial game, in which the hints are set to the defense values of the corrupted parties. The biased achieved by t aborts in the protocol, is at most t times the bias of the corresponding game.

Bounding online binomial games via a linear program. Upperbounding the bias of even a rather simple binomial game is not easy.[11] Specifically, it is non-trivial to take advantage of the fact that the player does not know beforehand which round will yield him the largest gain. A pessimistic approach, taken in [33], is to consider non-adaptive players that can only abort in a predetermined round, and then upperbound general players using a union bound. This approach effectively assumes the player is told the round it is best to abort, and as we prove here misses the right bound by a polylog factor. We take a different approach. The idea is to map the set of all possible strategies of the game into feasible solutions to a linear formulation. The bias each strategy achieves is equal to the objective value of the corresponding solution. We then use duality to bound the maximal value of the LP. Interestingly, we also prove the other direction: each feasible solution to the LP corresponds to a possible strategy of the game. This shows that bounding the value of the linear formulation is actually equivalent to bounding the value of the best strategy in the game.

The intuition of the linear formulation is simple. For a given binomial game we consider all possible states. Specifically, each state u is characterized by the the current round, i, the sum of coins tossed so far (in the first $i-1$ rounds), b, and the hint h given to the strategy. We use the notation $u = \langle i, b, h \rangle$. For state u, let p_u be the probability that the game visits state u. For two state u and v, let $p_{v|u}$ be the probability that the game visits v given that it visits state u. We write $u < v$, to indicate that the round of v is strictly larger than the round of u. For a state v, let c_v be the expected outcome of the game given that the strategy aborts at v. Given a strategy S, let a_v^{S} be the marginal probability that the strategy aborts at state v. It is easy to see that the bias achieved by strategy S can be written as:

$$\mathsf{Bias}_m(\mathsf{S}) = \sum_{v \in \mathcal{U}} a_v^{\mathsf{S}} \cdot c_v - \frac{1}{2}$$

Next, we build a linear formulation whose variables are the marginal probabilities a_v, capturing the probability that a strategy aborts at state v. One clear constraint on the variables is that the variables a_v are non-negative. Another obvious constraint is that a_v can never be larger than p_v, the probability that the game visits state v. A more refined constraint is $a_v + \sum_{u|u<v} a_u \cdot p_{v|u} \leq p_v$. Intuitively, this constraint stipulates that the marginal probability of aborting at state v plus the probability that the game visits v and the strategy aborted in a state $u < v$, cannot exceed the probability that the game visits v. We prove that this is indeed a valid constraint for any strategy and also that any solution that satisfies this constraint can be mapped to a valid strategy. As all our

bounding the effect of such aborts is rather simple, comparing to those done is Step 1, and we ignore such aborts from the current discussion.

[11] Our problem fits in the well-studied area of *stopping-time problems*, where the goal is to upperbound the value of the optimal stopping strategy.

constraints and the objective function are linear, this gives us a linear program that characterizes all strategies.

Formulating the linear program is just the first step. Although there are many methods for solving (exactly) a specific linear program, we are interested in (bounding) the *asymptotic* behavior of the optimal solution of the program as a function of m. To bound the solution we construct an asymptotic feasible solution to the dual program. This gives (by weak duality) an upper bound on the optimal bias obtained by any strategy.

1.4 Additional Related Work

Cleve and Impagliazzo [20] showed that in the *fail-stop model* any two-party m-round coin-flipping protocol has bias $\Omega(1/\sqrt{m})$; adversaries in this model are computationally unbounded, but they must follow the instructions of the protocol, except for being allowed to abort prematurely. Dachman-Soled et al. [22] showed that the same holds for $o(n/\log n)$-round protocols in the random-oracle model — the parties have oracle access to a uniformly chosen function over n bit strings.

There is a vast literature concerning coin-flipping protocols with weaker security guarantees. Most notable among these are protocols that are *secure with abort*. According to this security definition, if a cheat is detected or if one of the parties aborts, the remaining parties are not required to output anything. This form of security is meaningful in many settings, and it is typically much easier to achieve; assuming one-way functions exist, secure-with-abort protocols of negligible bias are known to exist against any number of corrupted parties [17, 34, 45]. To a large extent, one-way functions are also necessary for such coin-flipping protocols [16, 31, 38, 41].

Coin-flipping protocols were also studied in a variety of other models. Among these are collective coin-flipping in the *perfect information model*: parties are computationally unbounded and all communication is public [5, 14, 24, 47, 48], and protocols based on physical assumptions, such as quantum computation [2, 6, 7] and tamper-evident seals [42].

Perfectly fair coin-flipping protocols (i.e., zero bias) are a special case of protocols for *fair* secure function evaluation (SFE). Intuitively, the security of such protocols guarantees that when the protocol terminates, either everyone receives the (correct) output of the functionality, or no one does. While Cleve [19]'s result yields that some functions do not have fair SFE, it was recently shown that many interesting function families do have (perfectly) fair SFE [29, 8, 9].

1.5 Open Problems

Finding the the optimal bias t-party coin-flipping protocol for $t > 2$, remained the main open question in this area. While the gap between the upper and lower bound for the three-party case is now quite small (i.e., $O(\sqrt{\log m})$ factor), the gap for $t > 3$ is still rather large, and for $t > \log\log m/2$ the best protocol remained the $t/\sqrt{m}$-bias protocol of [10].

Acknowledgment

We thank Eran Omri for very useful discussions.

Paper Organization

Notations and the definitions used throughout the paper are given in Section 2. Our coin-flipping protocol along with its security proof are given in Section 3. The proofs given in Section 3 use the bounds given in Section 4 on the change knowing the defense values has on the expected output off the protocol, and the new bounds on the bias of online binomial games given in Section 5. Missing proofs can be found in Appendix A.

2 Preliminaries

2.1 Notation

We use calligraphic letters to denote sets, uppercase for random variables and functions, lowercase for values, boldface for vectors and capital boldface for matrices. All logarithms considered here are in base two. For a vector v, we denote its i-th entry by v_i or $v[i]$. For $a \in \mathbb{R}$ and $b \geq 0$, let $a \pm b$ stand for the interval $[a-b, a+b]$. Given sets $\mathcal{S}_1, \ldots, \mathcal{S}_k$ and k-input function f, let $f(\mathcal{S}_1, \ldots, \mathcal{S}_k) := \{f(x_1, \ldots, x_j) \colon x_i \in \mathcal{S}_i\}$, e.g., $f(1 \pm 0.1) = \{f(x) \colon x \in [.9, 1.1]\}$. For $n \in \mathbb{N}$, let $[n] := \{1, \ldots, n\}$ and $(n) := \{0, \ldots, n\}$. Given a vector $v \in \{-1,1\}^*$, let $w(v) := \sum_{i \in [|v|]} v_i$. Given a vector $v \in \{-1,1\}^*$ and a set of indexes $\mathcal{I} \subseteq [|v|]$, let $v_{\mathcal{I}} = (v_{i_1}, \ldots, v_{i_{|\mathcal{I}|}})$ where $i_1, \ldots, i_{|\mathcal{I}|}$ are the ordered elements of $\mathcal{I}$. We let the XOR of two integers, stands for the *bitwise* XOR of their bit representations, and we let $\mathsf{sign} \colon \mathbb{R} \mapsto \{0,1\}$ be the function that outputs one on non-negative input and zero otherwise.

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

Distributions. Given a distribution D, we write $x \leftarrow D$ to indicate that x is selected according to D. Similarly, given a random variable X, we write $x \leftarrow X$ to indicate that x is selected according to X. Given a finite set $\mathcal{S}$, we let $s \leftarrow \mathcal{S}$ denote that s is selected according to the uniform distribution on $\mathcal{S}$. 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 $\max_{\mathcal{S} \subseteq \mathcal{U}} |P(\mathcal{S}) - Q(\mathcal{S})| = \frac{1}{2} \sum_{u \in \mathcal{U}} |P(u) - Q(u)|$.

For $\delta \in [0,1]$, let $\mathcal{B}er(\delta)$ be the Bernoulli probability distribution over $\{0,1\}$, taking the value 1 with probability δ and 0 otherwise. For $\varepsilon \in [-1,1]$, let $\mathcal{C}_\varepsilon$ be the Bernoulli probability distribution over $\{-1,1\}$, taking the value 1 with probability $\frac{1}{2}(1+\varepsilon)$ and -1 otherwise. For $n \in \mathbb{N}$ and $\varepsilon \in [-1,1]$, let $\mathcal{C}_{n,\varepsilon}$ be the binomial distribution induced by the sum of n independent random variables, each distributed according to $\mathcal{C}_\varepsilon$. For $n \in \mathbb{N}$, $\varepsilon \in [-1,1]$ and $k \in \mathbb{Z}$, let $\widehat{\mathcal{C}}_{n,\varepsilon}(k) := \Pr_{x \leftarrow \mathcal{C}_{n,\varepsilon}}[x \geq k] = \sum_{t=k}^{n} \mathcal{C}_{n,\varepsilon}(t)$. For $n \in \mathbb{N}$ and $\delta \in [0,1]$, let $\widehat{\mathcal{C}}_n^{-1}(\delta)$ be the value $\varepsilon \in [-1,1]$ with $\widehat{\mathcal{C}}_{n,\varepsilon}(0) = \delta$. For $n \in \mathbb{N}$, $\ell \in [n]$ and $p \in \{-n, \ldots, n\}$, define the hyper-geometric probability distribution $\mathcal{HG}_{n,p,\ell}$ by $\mathcal{HG}_{n,p,\ell}(k) := \Pr_{\mathcal{I}}[w(v_{\mathcal{I}}) = k]$, where $\mathcal{I}$ is an ℓ-size set uniformly chosen from $[n]$ and $v \in \{-1,1\}^n$ with $w(v) = p$. Let $\widehat{\mathcal{HG}}_{n,p,\ell}(k) := \Pr_{x \leftarrow \mathcal{HG}_{n,p,\ell}}[x \geq k] = \sum_{t=k}^{\ell} \mathcal{HG}_{n,p,\ell}(t)$. Let $\Phi \colon \mathbb{R} \mapsto (0,1)$ be the cumulative distribution function of the standard normal distribution, defined by $\Phi(x) := \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-\frac{t^2}{2}} dt$. Finally, for $n \in \mathbb{N}$ and $i \in [n]$, let $\ell_n(i) := (n+1-i)^2$ and $\mathsf{sum}_n(i) := \sum_{j=i}^{n} \ell_n(j)$. We summarize the different notations used throughout the paper in the following tables.

Table 1: Basic functions.

Definition	*Input Range*	*Output value*
$[n]$	$n \in \mathbb{N}$	$\{1, \ldots, n\}$
(n)	$n \in \mathbb{N}$	$\{0, \ldots, n\}$
$\ell_n(i)$	$n \in \mathbb{N}$, $i \in [n]$	$(n+1-i)^2$
$\mathsf{sum}_n(i)$	$n \in \mathbb{N}$, $i \in [n]$	$\sum_{j=i}^{n} \ell_n(j)$
$w(v)$	$v \in \{-1,1\}^*$	$\sum_{i \in \mathcal{I}} v_i$
$v_{\mathcal{I}}$	$v \in \{-1,1\}^*$, $\mathcal{I} \subseteq [\lvert v \rvert]$ and $i_1, \ldots, i_{\lvert\mathcal{I}\rvert}$ are the ordered elements of $\mathcal{I}$	$(v_{i_1}, \ldots, v_{i_{\lvert\mathcal{I}\rvert}})$
$a \pm b$	$a \in \mathbb{R}$, $b \geq 0$	$[a-b, a+b]$
$\mathsf{sign}(x)$	$x \in \mathbb{R}$	1 for $x \geq 0$ and 0 otherwise.

Table 2: Distributions.

Distribution	*Input Range*	*Description*
$\mathcal{B}er(\delta)$	$\delta \in [0,1]$	1 with probability δ and 0 otherwise.
$\mathcal{C}_\varepsilon$	$\varepsilon \in [-1,1]$	1 with probability $\frac{1}{2}(1+\varepsilon)$ and -1 otherwise
$\mathcal{C}_{n,\varepsilon}$	$n \in \mathbb{N}$, $\varepsilon \in [-1,1]$	sum of n independent $\mathcal{C}_\varepsilon$ random variables
$\mathcal{HG}_{n,p,\ell}$	$n \in \mathbb{N}$, $p \in \{-n, \ldots, n\}$, $\ell \in [n]$	The value of $w(v_{\mathcal{I}})$ where $\mathcal{I}$ is an ℓ-size set uniformly chosen from $[n]$ and $v \in \{-1,1\}^n$ with $w(v) = p$

Table 3: Distributions related functions.

Definition	*Input Range*	*Output value*
$\Phi(x)$	$x \in \mathbb{R}$	$\frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-\frac{t^2}{2}} dt$
$\mathcal{C}_{n,\varepsilon}(k)$	$n \in \mathbb{N}$, $\varepsilon \in [-1,1]$, $k \in \mathbb{Z}$	$\Pr_{x \leftarrow \mathcal{C}_{n,\varepsilon}}[x = k]$
$\widehat{\mathcal{C}}_{n,\varepsilon}(k)$	$n \in \mathbb{N}$, $\varepsilon \in [-1,1]$, $k \in \mathbb{Z}$	$\Pr_{x \leftarrow \mathcal{C}_{n,\varepsilon}}[x \geq k]$
$\widehat{\mathcal{C}}_n^{-1}(\delta)$	$n \in \mathbb{N}$, $\delta \in [0,1]$	The value $\varepsilon \in [-1,1]$ with $\widehat{\mathcal{C}}_{n,\varepsilon}(0) = \delta$
$\mathcal{HG}_{n,p,\ell}(k)$	$n \in \mathbb{N}$, $p \in \{-n, \ldots, n\}$, $\ell \in [n]$, $k \in \mathbb{Z}$	$\Pr_{x \leftarrow \mathcal{HG}_{n,p,\ell}}[x = k]$
$\widehat{\mathcal{HG}}_{n,p,\ell}(k)$	$n \in \mathbb{N}$, $p \in \{-n, \ldots, n\}$, $\ell \in [n]$, $k \in \mathbb{Z}$	$\Pr_{x \leftarrow \mathcal{HG}_{n,p,\ell}}[x \geq k]$

2.2 Facts About the Binomial Distribution

Fact 2.1 (Hoeffding's inequality for $\{-1,1\}$)**.** *Let $n, t \in \mathbb{N}$ and $\varepsilon \in [-1,1]$. Then*

$$\Pr_{x \leftarrow \mathcal{C}_{n,\varepsilon}}[|x - \varepsilon n| \geq t] \leq 2e^{-\frac{t^2}{2n}}.$$

Proof. Immediately follows by [37]. □

The following proposition is proven in [32].

Proposition 2.2. *Let $n \in \mathbb{N}$, $t \in \mathbb{Z}$ and $\varepsilon \in [-1,1]$ be such that $t \in \mathrm{Supp}(\mathcal{C}_{n,\varepsilon})$, $|t| \leq n^{\frac{3}{5}}$ and $|\varepsilon| \leq n^{-\frac{2}{5}}$. Then*

$$\mathcal{C}_{n,\varepsilon}(t) \in (1 \pm \mathsf{error}) \cdot \sqrt{\frac{2}{\pi}} \cdot \frac{1}{\sqrt{n}} \cdot e^{-\frac{(t-\varepsilon n)^2}{2n}},$$

for $\mathsf{error} = \xi \cdot (\varepsilon^2 |t| + \frac{1}{n} + \frac{|t|^3}{n^2} + \varepsilon^4 n)$ *and a universal constant* ξ.

The following propositions are proven in Appendix A.2.

Proposition 2.3. *Let $n \in \mathbb{N}$, $\varepsilon \in [-1,1]$ and let $\mu := \mathrm{E}_{x \leftarrow \mathcal{C}_{n,\varepsilon}}[x] = \varepsilon \cdot n$. Then for every $k > 0$ it holds that*

1. $\mathrm{E}_{x \leftarrow \mathcal{C}_{n,\varepsilon} | |x-\mu| \leq k}\left[(x-\mu)^2\right] \leq \mathrm{E}_{x \leftarrow \mathcal{C}_{n,\varepsilon}}\left[(x-\mu)^2\right] \leq n$.
2. $\mathrm{E}_{x \leftarrow \mathcal{C}_{n,\varepsilon} | |x-\mu| \leq k}\left[|x-\mu|\right] \leq \mathrm{E}_{x \leftarrow \mathcal{C}_{n,\varepsilon}}\left[|x-\mu|\right] \leq \sqrt{n}$.

Proposition 2.4. *Let $n, n' \in \mathbb{N}$, $k \in \mathbb{Z}$, $\varepsilon \in [-1,1]$ and $\lambda > 0$ be such that $n \leq n'$, $|k| \leq \lambda \cdot \sqrt{n \log n}$, $|\varepsilon| \leq \lambda \cdot \sqrt{\frac{\log n}{n}}$, and let $\delta = \widehat{\mathcal{C}}_{n,\varepsilon}(k)$. Then*

$$\widehat{\mathcal{C}}^{-1}_{n'}(\delta) \in \frac{\varepsilon n - k}{\sqrt{n \cdot n'}} \pm \mathsf{error},$$

for $\mathsf{error} = \varphi(\lambda) \cdot \frac{\log^{1.5} n}{\sqrt{n \cdot n'}}$ *and a universal function* φ.

2.3 Facts About the Hypergeometric Distribution

Fact 2.5 (Hoeffding's inequality for hypergeometric distribution)**.** *Let $\ell \leq n \in \mathbb{N}$, and $p \in \mathbb{Z}$ with $|p| \leq n$. Then*

$$\Pr_{x \leftarrow \mathcal{HG}_{n,p,\ell}}\left[|x-\mu| \geq t\right] \leq e^{-\frac{t^2}{2\ell}},$$

for $\mu = \mathrm{E}_{x \leftarrow \mathcal{HG}_{n,p,\ell}}[x] = \frac{\ell \cdot p}{n}$.

Proof. Immediately follows by [49, Equations (10),(14)]. □

The following propositions are proven in Appendix A.3.

Proposition 2.6. *Let $n \in \mathbb{N}$, $\ell \in [\lfloor \frac{n}{2} \rfloor]$, $p, t \in \mathbb{Z}$ and $\lambda > 0$ be such that $|p| \leq \lambda \cdot \sqrt{n \log n}$, $|t| \leq \lambda \cdot \sqrt{\ell \log \ell}$ and $t \in \mathrm{Supp}(\mathcal{HG}_{n,p,\ell})$. Then*

$$\mathcal{HG}_{n,p,\ell}(t) = (1 \pm \mathsf{error}) \cdot \sqrt{\frac{2}{\pi}} \cdot \frac{1}{\sqrt{\ell(1-\frac{\ell}{n})}} \cdot e^{-\frac{(t-\frac{p\ell}{n})^2}{2\ell(1-\frac{\ell}{n})}},$$

for $\mathsf{error} = \varphi(\lambda) \cdot \frac{\log^{1.5} \ell}{\sqrt{\ell}}$ *and a universal function* φ.

Proposition 2.7. *Let $n \in \mathbb{N}$, $\ell \in [\lfloor \frac{n}{2} \rfloor]$, $p, k \in [n]$ and $\lambda > 0$ be such that $|p| \leq \lambda \cdot \sqrt{n \log n}$ and $|k| \leq \lambda \cdot \sqrt{\ell \log \ell}$. Then*

$$\widehat{\mathcal{HG}}_{n,p,\ell}(k) \in \Phi\left(\frac{k - \frac{p \cdot \ell}{n}}{\sqrt{\ell(1 - \frac{\ell}{n})}}\right) \pm \mathsf{error},$$

where $\mathsf{error} = \varphi(\lambda) \cdot \frac{\log^{1.5} \ell}{\sqrt{\ell}}$ *for some universal function φ.*

Proposition 2.8. *Let $n \in \mathbb{N}$, $\ell \in [\lfloor \frac{n}{2} \rfloor]$, $p, k \in [n]$ and $\lambda > 0$ be such that $|p| \leq \lambda \cdot \sqrt{n \log n}$ and $|k| \leq \lambda \cdot \sqrt{\ell \log \ell}$ and let $\delta = \widehat{\mathcal{HG}}_{n,p,\ell}(k)$. Then for every $m \geq \ell$ it holds that*

$$\widehat{\mathcal{C}}_m^{-1}(\delta) \in \frac{\frac{p \cdot \ell}{n} - k}{\sqrt{m \cdot \ell(1 - \frac{\ell}{n})}} \pm \mathsf{error},$$

where $\mathsf{error} = \varphi(\lambda) \cdot \frac{\log^{1.5} \ell}{\sqrt{m \cdot \ell}}$ *for some universal function φ.*

2.4 Multi-Party Computation

2.4.1 Protocols

To keep the discussion simple, in the following we focus on no private input protocols. A t-party protocol is defined using t Turing Machines (TMs) $\mathsf{P}_1, \ldots, \mathsf{P}_t$, having the security parameter 1^κ as their common input. In each round, the parties broadcast and receive messages on a broadcast channel. At the end of protocol, each party outputs some binary string. The parties communicate in a synchronous network, using only a broadcast channel: when a party broadcasts a message, all other parties see *the same* message. This ensures some consistency between the information the parties have. There are no private channels and all the parties see all the messages, and can identify their sender. We do not assume simultaneous broadcast. It follows that in each round, some parties might hear the messages sent by the other parties before broadcasting their messages. We assume that if a party aborts, it first broadcasts the message Abort to the other parties, and without loss of generality only does so at the end of a round in which it is supposed to send a message. A protocol is *efficient*, if its parties are PPTM, and the protocol's number of rounds is a computable function of the security parameter.

This work focuses on efficient protocols, and on malicious, static (i.e., non-adaptive) PPT adversaries for such protocols. An adversary is allowed to corrupt some subset of the parties; before the beginning of the protocol, the adversary corrupts a subset of the parties that from now on may arbitrarily deviate from the protocol. Thereafter, the adversary sees the messages sent to the corrupted parties and controls their messages. We also consider the so called *fail-stop* adversaries. Such adversaries follow the prescribed protocol, but might abort prematurely. Finally, the honest parties follow the instructions of the protocol to its completion.

2.4.2 The Real vs. Ideal Paradigm

The security of multi-party computation protocols is defined using the *real* vs. *ideal* paradigm [18, 26]. In this paradigm, the *real-world model*, in which protocols is executed is compared to

an *ideal model* for executing the task at hand. The latter model involves a trusted party whose functionality captures the security requirements of the task. The security of the real-world protocol is argued by showing that it "emulates" the ideal-world protocol, in the following sense: for any real-life adversary A, there exists an ideal-model adversary (also known as simulator) $\mathbb{A}$ such that the global output of an execution of the protocol with A in the real-world model is distributed similarly to the global output of running $\mathbb{A}$ in the ideal model. The following discussion is restricted to random, no-input functionalities. In addition, to keep the presentation simple, we limit our attention to uniform adversaries.[12]

The Real Model. Let π be an t-party protocol and let A be an adversary controlling a subset $\mathcal{C} \subseteq [t]$ of the parties. Let $\mathrm{REAL}_{\pi,\mathsf{A},\mathcal{C}}(\kappa)$ denote the output of A (i.e., without loss of generality its view: its random input and the messages it received) and the outputs of the honest parties, in a random execution of π on common input 1^κ. Recall that an adversary is *fail stop*, if until they abort, the parties in its control follow the prescribed protocol (in particular, they property toss their private random coins). We call an execution of π with such a fail-stop adversary, a fail-stop execution.

The Ideal Model. Let f be a t-output functionality. If f gets a security parameter (given in unary), as its first input, let $f_\kappa(\cdot) = f(1^\kappa, \cdot)$. Otherwise, let $f_\kappa = f$. An ideal execution of f with respect to an adversary $\mathbb{A}$ controlling a subset $\mathcal{C} \subseteq [t]$ of the "parties" and a security parameter 1^κ, denoted $\mathrm{IDEAL}_{f,\mathbb{A},\mathcal{C}}(\kappa)$, is the output of the adversary $\mathbb{A}$ and that of the trusted party, in the following experiment.

Experiment 2.9.

1. *The trusted party sets $(y_1, \ldots, y_t) = f_\kappa(X)$, where X is a uniform element in the domain of f_κ, and sends $\{y_i\}_{i\in\mathcal{C}}$ to $\mathbb{A}(1^\kappa)$.*
2. *$\mathbb{A}(1^\kappa)$ sends the message* Continue/ Abort *to the trusted party, and locally outputs some value.*
3. *The trusted party outputs $\{o_i\}_{i\in[t]\setminus\mathcal{C}}$, for o_i being y_i if $\mathbb{A}$ instructs* Continue*, and $\perp$ otherwise.*

An adversary $\mathbb{A}$ is non-aborting, if it never sends the Abort message.

α-secure computation. The following definitions adopts the notion of α-secure computation [13, 28, 40] for our restricted settings.

Definition 2.10 (α-secure computation)**.** *An efficient t-party protocol π computes a t-output functionality f in a α-*secure *manner [resp., against fail-stop adversaries], if for every $\mathcal{C} \subsetneq [t]$ and every [resp., fail-stop]* PPT *adversary A controlling the parties indexed by $\mathcal{C}$,*[13] *there exists a* PPT *$\mathbb{A}$ controlling the same parties, such that*

$$\mathrm{SD}\left(\mathrm{REAL}_{\pi,\mathsf{A},\mathcal{C}}(\kappa), \mathrm{IDEAL}_{f,\mathbb{A},\mathcal{C}}(\kappa)\right) \leq \alpha(\kappa),$$

[12] All results stated in this paper, straightforwardly extend to the non-uniform settings.

[13] The requirement that $\mathcal{C}$ is a *strict* subset of $[t]$, is merely for notational convinced.

for large enough κ. A protocol securely compute a functionality f, if it computes f in a $\mathrm{neg}(\kappa)$*-secure manner. The protocol π computes f in a* simultaneous α-secure *manner, if the above is achieved by a* non-aborting $\mathbb{A}$.

Note that being simultaneous α-secure is a very strong requirement, as it dictates that the cheating real adversary has no way to prevent the honest parties from getting their part of the output, and this should be achieved with no simultaneous broadcast mechanism.

2.4.3 Fair Coin-Flipping Protocols

Definition 2.11 (α-fair coin-flipping)**.** *For $t \in \mathbb{N}$ let* $\mathsf{CoinFlip}_t$ *be the t-output functionality from $\{0,1\}$ to $\{0,1\}^t$, defined by* $\mathsf{CoinFlip}_t(b) = b \dots b$ *(t times). A t-party protocol π is α-*fair coin-flipping protocol*, if it computes* $\mathsf{CoinFlip}_t$ *in a* simultaneous α-secure *manner.*

Proving fairness. Haitner and Tsfadia [32] gave an alternative characterization of fair coin-flipping protocols against fail-stop adversaries. Specifically, Lemma 2.15 below reduces the task of proving fairness of a coin-flipping protocol, against fail-stop adversaries, to proving the protocol is correct: the honest parties always output the same bit, and this bit is uniform in an all honest execution, and to proving the protocol is unbiased: a fail-stop adversary cannot bias the output of the honest parties by too much.

Definition 2.12 (correct coin-flipping protocols)**.** *A protocol is a* correct coin flipping*, if*

- *When interacting with an fails-stop adversary controlling a subset of the parties, the honest parties* always *output the same bit, and*
- *The common output in a random* honest *execution of π, is uniform over $\{0,1\}$.*

Given a partial view of a fail-stop adversary, we are interesting in the expected outcome of the parties, conditioned on this and the adversary making no further aborts.

Definition 2.13 (view value)**.** *Let π be a protocol in which the honest parties always output the same bit value. For a partial view v of the parties in a fail-stop execution of π, let $\mathsf{C}_\pi(v)$ denote the parties' full view in an* honest *execution of π conditioned on v (i.e., all parties that do not abort in v act honestly in $\mathsf{C}_\pi(v)$). Let $\mathsf{val}_\pi(v) = \mathrm{E}_{v' \leftarrow \mathsf{C}_\pi(v)}[\mathrm{out}(v')]$, where $\mathrm{out}(v')$ is the common output of the non-aborting parties in v'.*

Finally, a protocol is unbiased, if no fail-stop adversary can bias the common output of the honest parties by too much.

Definition 2.14 (α-unbiased coin-flipping protocols, [32].)**.** *A t-party, m-round protocol π is α-*unbiased*, if the following holds for every fail-stop adversary A controlling the parties indexed by a subset $\mathcal{C} \subset [t]$ (the corrupted parties). Let V be the corrupted parties' view in a random execution of π in which A controls those parties, and let I_j be the index of the j'th round in which A sent an abort message (set to $m+1$, if no such round). Let V_i be the prefix of V at the end of the i'th round, letting V_0 being the empty view, and let V_i^- be the prefix of V_i with the i'th round abort messages (if any) removed. Then*

$$\left| \mathop{\mathrm{E}}_{V} \left[\sum_{j \in |\mathcal{C}|} \mathsf{val}(V_{I_j}) - \mathsf{val}(V_{I_j}^-) \right] \right| \leq \alpha,$$

where $\mathsf{val} = \mathsf{val}_\pi$ is according to Definition 2.13.

Lemma 2.15 ([32], Lemma 2.18)**.** *Let π be a correct, α-unbiased coin-flipping protocol with $\alpha(\kappa) \leq \frac{1}{2} - \frac{1}{p(\kappa)}$, for some $p \in \text{poly}$, then π is a $(\alpha(\kappa)+\text{neg}(\kappa))$-secure coin-flipping protocol against fail-stop adversaries.*

2.4.4 Oblivious Transfer

Definition 2.16. *The $\binom{1}{2}$ oblivious transfer (*OT *for short) functionality, is the two-output functionality f over $\{0,1\}^3$, defined by $f(\sigma_0, \sigma_1, i) = ((\sigma_0, \sigma_1), (\sigma_i, i))$.*

Protocols the securely compute OT, are known under several hardness assumptions (cf., [3, 23, 25, 30, 39, 46]).

2.4.5 f-Hybrid Model

Let f be a t-output functionality. The f-hybrid model is identical to the real model of computation discussed above, but in addition, each t-size subset of the parties involved, has access to a trusted party realizing f. It is important to emphasize that the trusted party realizes f in a *non*-simultaneous manner: it sends a random output of f to the parties in an arbitrary order. When a party gets its part of the output, it instructs the trusted party to either continue sending the output to the other parties, or to send them the abort symbol (i.e., the trusted party "implements" f in a perfect non-simultaneous manner). All notions given in Sections 2.4.2 and 2.4.3 naturally extend to the f-hybrid model, for any functionality f. In addition, the proof of Lemma 2.15 straightforwardly extends to this model. We also make use of the following known fact.

Fact 2.17. *Let f be a polynomial-time computable functionality, and assume there exists a t-party, m-round, α-fair coin-flipping protocol in the f-hybrid model, making at most k calls to f, were t, m, α and k, are function of the security parameter κ. Assuming there exist a protocol for securely computing* OT*, then there exists a t-party, $(O(k \cdot t^2) + m)$-round, $(\alpha + \text{neg}(\kappa))$-fair coin-flipping protocol (in the real world).*

Proof. Since f is a polynomial-time computable and since we assume the existence of a protocol for securely computing OT, there exists a constant-round protocol π_f for securely computing f: a constant-round protocol for f that is secure against semi-honest adversaries follows by Beaver et al. [11] (assuming OT), and the latter protocol can be compiled into a $O(t^2)$-round protocol that securely computes f, against arbitrary malicious adversaries, using the techniques of Goldreich et al. [27] (assuming one-way functions, that follows by the existence of OT). Let π be a t-party, m-round, α-fair coin-flipping protocol in the f-hybrid model. Canetti [18] yields that by replacing the trusted party for computing f used in π with the protocol π_f, we get an $(O(k \cdot t^2) + m)$-round, $(\alpha + \text{neg})$-fair coin-flipping protocol. □

3 The Many-Party Coin-Flipping Protocol

In Section 3.1, the many-party coin-flipping protocol is defined in an hybrid model. The security of the latter protocol is analyzed in Section 3.2. The (real model) many-party coin-flipping protocol is defined and analyzed in Section 3.3.

3.1 The Hybrid-Model Protocol

The coin-flipping protocol described below follows the high-level description given in the introduction. The main difference is that the number of coins flipped is every round is not one, but a decreasing function of the round index. This asymmetry, also done in [32], prevents the last rounds from having too high influence on the final outcome.

The protocols below are defined in an hybrid model in which the parties get joint oracle access to several ideal functionalities. We assume the following conventions about the model: all functionalities are guaranteed to function correctly, but do not guarantee fairness: an adversary can abort, and thus preventing the honest parties from getting their output, *after* seeing the outputs of the corrupted parties in its control. We assume identified abort: when a party aborts, its identity is revealed to all other parties. We also assume that when the parties make *parallel* oracle calls, a party that aborts in one of these calls is forced to abort in all of them.

The protocols defined below will not be efficient, even in the hybrid model, since the parties are required to hold real numbers (which apparently have infinite presentation), we handle this inefficiency when defining the (efficient) real world protocol in Section 3.3.

Protocol $\widehat{\Pi}$ defined next is our (hybrid model) coin-flipping protocol to be called.

This protocol is merely a wrapper for protocol Π: the parties first correlate their private inputs using an oracle to the $\mathsf{Defense}$ functionality, and then interact in Π with these inputs (protocol Π and the functionality $\mathsf{Defense}$ are defined below). For $m, t \in \mathbb{N}$, the t-party, $O(m \cdot t)$-round protocol $\widehat{\Pi}^t_m$ is defined as follows.

Protocol 3.1 ($\widehat{\Pi}^t_m = (\widehat{\mathsf{P}}_1, \ldots, \widehat{\mathsf{P}}_t)$)**.**

Oracle: $\mathsf{Defense}$.

Protocol's description:

1. *Let $\delta^{\#1}, \ldots, \delta^{\#t}$ be t-out-of-t shares of $\frac{1}{2}$.*
2. *Let $\ell = t$ be the defense-quality parameter.*
3. *For every $\emptyset \neq \mathcal{Z} \subseteq [t]$ (in parallel), the parties jointly call $\mathsf{Defense}(1^m, 1^t, 1^\ell, \mathcal{Z}, \delta^{\#1}, \ldots, \delta^{\#t})$, where 1^m, 1^t, 1^ℓ, and $\mathcal{Z}$ are common inputs, and input $\delta^{\#k}$ is provided by party P_k. Let $\delta^{\#z,\mathcal{Z}}$ be the output of party $\widehat{\mathsf{P}}_z$ returned by this call.*
4. *The parties interact in $\Pi^t_m = (\mathsf{P}_1, \mathsf{P}_2, \ldots, \mathsf{P}_t)$ with common input 1^ℓ. Party $\widehat{\mathsf{P}}_z$ plays the role of P_z with private input $\{\delta^{\#z,\mathcal{Z}}\}_{\emptyset \neq \mathcal{Z} \subseteq [t]}$.*

Abort (during step 2): If there is a single remaining party, it outputs an unbiased bit. Otherwise, the remaining parties interact in $\widehat{\Pi}^{t'}_m(1^\ell)$ for $t' < t$ being the number of the remaining parties.

3.1.1 Protocol Π^r_m

When defining Π^r_m, we make a distinction whether the number of parties is two or larger. We let Π^2_m be the two-party protocol Π^{HT}_m, which is a variant of the of two-party protocol of [33] defined in Section 3.1.5. For the many-party case (three parties or more), we use the newly defined protocol given below. This distinction between the two-party and many-party cases is made for improving the bias of the final protocol, and all is well-defined if we would have used the protocol below also

for the two-party case (on the first read, we encourage the reader to assume that this is indeed the case). See Remark 3.27 for the benefit of using the the [33] protocol for the two-party case. ‘

For $m, r \leq t \in \mathbb{N}$, the r-party, $O(m{\cdot}r)$-round protocol Π_m^r is defined as follows (the functionalities $\mathsf{Defense}$ and Coin the protocol uses are defined in Sections 3.1.2 and 3.1.3, respectively).

Protocol 3.2 ($\Pi_m^r = (\mathsf{P}_1, \mathsf{P}_2, \ldots, \mathsf{P}_r)$ (for $r > 2$))**.**

Oracles: $\mathsf{Defense}$*, and* Coin*.*

Common input: defense-quality parameter 1^ℓ*.*

P_z*'s inputs:* $\{\delta^{\#z,\mathcal{Z}}\}_{\emptyset \neq \mathcal{Z} \subseteq [r]}$*.*[14]

Protocol's description:

1. *For every* $\emptyset \neq \mathcal{Z} \subsetneq [r]$ *(in parallel), the parties jointly call* $\mathsf{Defense}(1^m, 1^r, 1^\ell, \mathcal{Z}, \delta^{\#1,[r]}, \ldots, \delta^{\#r,[r]})$*, where* $1^m, 1^r, 1^\ell, \mathcal{Z}$ *are common inputs, and input* $\delta^{\#k,[r]}$ *is provided by party* P_k*.*
   - *For all* $z \in \mathcal{Z}$*, party* P_z *updates* $\delta^{\#z,\mathcal{Z}}$ *to the value it received from this call.*
2. *Each party* P_z *sends* $\delta^{\#z,[r]}$ *to the other parties.*
   - *All parties set* $\delta = \bigoplus_{z=1}^r \delta^{\#z,[r]}$*.*
3. *For* $i = 1$ *to* m*:*
   (a) *The parties jointly call* $\mathsf{Coin}(1^m, 1^r, \delta, c_1, \ldots, c_{i-1})$*.*
      - *For* $z \in \mathcal{Z}$*, let* $(c_i^{\#z}, \delta_i^{\#z})$ *be the output of party* P_z *returned by* Coin*.*

   (b) *For every* $\emptyset \neq \mathcal{Z} \subsetneq [r]$ *(in parallel), the parties jointly call* $\mathsf{Defense}(1^m, 1^r, 1^\ell, \mathcal{Z}, \delta_i^{\#1}, \ldots, \delta_i^{\#r})$*, where* $1^m, 1^r, 1^\ell, \mathcal{Z}$ *are common inputs, and the input* $\delta_i^{\#k}$ *is provided by party* P_k*.*
      - *For* $z \in \mathcal{Z}$*, party* P_z *updates* $\delta^{\#z,\mathcal{Z}}$ *to the value it received from this call.*

   (c) *Each party* P_z *sends* $c_i^{\#z}$ *to the other parties.*
      - *All parties set* $c_i = \bigoplus_{z=1}^r c_i^{\#z}$*.*

Output: All parties output $\mathsf{sign}(\sum_{i=1}^m c_i)$*.*

Abort: Let $\emptyset \neq \mathcal{Z} \subsetneq [r]$ *be the indices of the remaining parties. If* $\mathcal{Z} = \{z_k\}$*, then the party* P_k *outputs* $\delta^{\#k,\{k\}}$*. Otherwise (*$|\mathcal{Z}| \geq 2$*), assume for ease of notation that* $\mathcal{Z} = [h]$ *for some* $h \in [r-1]$*. To decide on a common output, the parties interact in* $\Pi_m^h = (\mathsf{P}'_1, \ldots, \mathsf{P}'_h)$ *with common input* 1^ℓ*, where party* P_z *plays the role of* P'_z *with private input* $\{\delta^{\#z,\mathcal{Z}'}\}_{\emptyset \neq \mathcal{Z}' \subseteq \mathcal{Z}}$*.*

That is at Step 1, the parties use $\mathsf{Defense}$ to be instructed what to do if some parties aborts in the reconstruction of the value of δ that happens at Step 2. If Step 1 ends successfully (no aborts), then the expected outcome of the protocol is guaranteed to be δ, even if some parties abort in he reconstruction of δ done in Step 2 (but no further aborts). If an abort occurs in this Step 1, then

[14] The type of $\delta^{\#z,\mathcal{Z}}$ varies according to $|\mathcal{Z}|$. For $|\mathcal{Z}| = 1$, $\delta^{\#z,\mathcal{Z}}$ is simply a $\{0,1\}$ bit, for $|\mathcal{Z}| > 2$ it is a share of $|\mathcal{Z}|$-out-of$|\mathcal{Z}|$ secret share of a number in $[0,1]$, and for $|\mathcal{Z}| = 2$ it has a more complex structure. See Section 3.1.3 for details.

the remaining parties use their inputs to interact in a protocol whose expected outcome is δ', for δ' being the input in the call to Defense that generated the parties' input. The key point is that even though δ might be rather far from δ', the corrupted parities who only holds parties information about δ (i.e., the output of Defense), cannot exploit this gap too effectively.

A similar thing happens when flipping each of the coins c_i. The parties first use Coin and Defense to get shares of the new coin c_i and to get instructed what to do if some parties abort in the reconstruction of c_i. If Step 3b ends successfully, then the expected outcome of the protocol is $\delta_i = \Pr\left[\mathsf{sign}(\sum_{i=1}^{m} c_i) = 1 \mid c_1, \ldots, c_i\right]$, even if some parties abort in the reconstruction of c_i (but no further aborts). If an abort occurs in Step 3b, then the remaining parties use their inputs to interact in a protocol whose expected outcome is δ_{i-1}. Also in this case, the corrupted parities cannot exploit the gap between δ_i and δ_{i-1} too effectively.

We note that in the recursive invocations done in the protocol when abort happens, the number of interacting parties in the new protocol is smaller. We also note that since all calls to the Defense functionality taken is Step 1 / Step 3b are done in *parallel*, the resulting protocol has indeed $O(r \cdot m)$ rounds.

Finally, the role of the input parameter ℓ is to optimize the information the calls to Defense leak through the execution of the protocol (including its sub-protocols executions that take place when aborts happen). Recall (see discussion in the introduction) that on one hand, we would like Defense to leak as little information as possible, to prevent an effective attack of the current execution of the protocol. For instance, the value return by Defense in Step 1, should not give too much information about the value of δ. On the other hand, a too hiding Defense will make an interaction done in a sub-protocol, happens if an abort happens, less secure. Parameter ℓ is set to t in the parent call to the protocol done from the t-party protocol $\widehat{\Pi}^t$ and is kept to this value throughout the different sub-protocol executions, enables us to find the optimal balance between these contradicting requirements. See Section 3.1.3 for details.

3.1.2 The Coin Functionality

Functionality Coin performs the (non fair) coin-flipping operation done inside the main loop of Π. It outputs shares of the i-th round's coin c_i, and also shares for the value of expected outcome of the protocol given c_i.[15]

Recall that $\mathcal{B}er(\delta)$ is the Bernoulli probability distribution over $\{0, 1\}$ that assigns probability δ to 1, that $\mathcal{C}_\varepsilon$ is the Bernoulli probability distribution over $\{-1, 1\}$ that assigns probability $\frac{1}{2}(1 + \varepsilon)$ to 1, that $\mathcal{C}_{n,\varepsilon}(k) = \Pr\left[\sum_{i=1}^{n} x_i = k\right]$ for x_i's that are i.i.d according to $\mathcal{C}_\varepsilon$, and $\widehat{\mathcal{C}}_{n,\varepsilon}(k) = \Pr_{x \leftarrow \mathcal{C}_{n,\varepsilon}}\left[x \geq k\right]$. Also recall that $\widehat{\mathcal{C}}_n^{-1}(\delta)$ is the value $\varepsilon \in [-1, 1]$ with $\widehat{\mathcal{C}}_{n,\varepsilon}(0) = \delta$, that $\ell_m(i) = (m + 1 - i)^2$ (i.e., the number of coins tossed at round i), and that $\mathsf{sum}_m(i) = \sum_{j=i}^{n} \ell_m(j)$ (i.e., the

[15] This redundancy in the functionality description, i.e., the shares of coins can be used to compute the the second part of the output, simplifies the presentation of the protocol.

number of coins tossed after round i).

Algorithm 3.3 (Coin)**.**

Input: Parameters 1^m *and* 1^r, $\delta \in [0,1]$, *and coins* $c_1, \ldots, c_{i-1}$.

Operation:

1. *Let* $\varepsilon = \widehat{\mathcal{C}}^{-1}_{\mathsf{sum}_m(1)}(\delta)$.
2. *Sample* $c_i \leftarrow \mathcal{C}_{\ell_m(i),\varepsilon}$.
3. *Let* $\delta_i = \widehat{\mathcal{C}}_{\mathsf{sum}_m(i+1),\varepsilon}(-\sum_{j=1}^{i} c_j)$
4. *Sample* r *uniform strings* $\mathsf{share}^{\#1}, \ldots, \mathsf{share}^{\#r}$ *conditioned on* $(c_i, \delta_i) = \bigoplus_{i=1}^{r} \mathsf{share}^{\#i}$, *and return party* P_i *the share* $\mathsf{share}^{\#i}$.

3.1.3 The Defense Functionality

The Defense functionality is used by protocol Π to "defend" the remaining parties when some corrupted parties abort. When invoked with a subset $\mathcal{Z} \subsetneq [r]$ and $\delta \in [0,1]$, it produces the inputs the parties in $\mathcal{Z}$ need in order to collaborate and produce a δ-biased bit — expected value is δ.

As with protocols Π^r_m, we make a distinction whether $r = 2$ (r is the number of parties that call Defense) or $r > 2$. In the former case, we use a simple variant of the [33] defense functionality defined in Section 3.1.5. For all other values, we use the functionality defined below. (Also in this case, we encourage the first-time reader to ignore this subtlety, and assume we use the new definition for all cases.)

Algorithm 3.4 (Defense functionality for $r > 2$)**.**

Input: Parameters 1^m, 1^r, 1^ℓ, *set* $\mathcal{Z} \subseteq [r]$ *and shares* $\{\delta^{\#z}\}_{z\in[r]}$.

Operation: Return $\widetilde{\mathsf{Defense}}(1^m, 1^r, 1^\ell, \mathcal{Z}, \bigoplus_{z\in[r]} \delta^{\#z})$

Namely, Defense just reconstructs δ and calls $\widetilde{\mathsf{Defense}}$ defined below.

Algorithm 3.5 ($\widetilde{\mathsf{Defense}}$)**.**

Input: Parameter 1^m, 1^r, 1^ℓ, *set* $\mathcal{Z} = \{z_1, \ldots, z_k\} \subsetneq [r]$, *and* $\delta \in [0,1]$.

Operation:

1. *If* $|\mathcal{Z}| = 1$, *let* $o_1 \leftarrow \mathcal{C}_\delta$.
2. *If* $|\mathcal{Z}| = 2$, *let* $(o_1, o_2) = \widetilde{\mathsf{Defense}}^{\mathsf{HT}}(1^m, \delta)$.
3. *If* $|\mathcal{Z}| > 2$,
   (a) *Let* $\delta' = \mathsf{Noise}(1^m, 1^\ell, |\mathcal{Z}|, \delta)$.
   (b) *Sample* $|\mathcal{Z}|$ *uniform shares* $o_1, \ldots, o_k$ *such that* $\delta' = \bigoplus_{i=1}^{k} o_k$.
4. *Return* o_i *to party* P_{z_i}, *and* $\perp$ *to the other parties.*

It is clear that for the case $|\mathcal{Z}| = 1$, the expected value of the output bit of the party in $\mathcal{Z}$ is indeed δ. Since the expected value of δ' output by $\mathsf{Noise}(\cdot, \delta)$, see below, it δ, it is not hard to see that the same holds also for the case $|\mathcal{Z}| > 2$. Finally, thought somewhat more difficult to verify, the above also holds for the case $|\mathcal{Z}| = 2$ (see Section 3.1.5).

3.1.4 The Noise Functionality

The Noise functionality, invoked by $\widetilde{\mathsf{Defense}}$, takes as input $\delta \in [0,1]$ and returns a "noisy version" of it δ' (i.e., expected value is δ). The amount of noise used is determined by the defense-quality parameter ℓ that reflects the number of players that interact in the parent protocol $\widehat{\Pi}^t$, the number of parties that will use the returned value in their sub-protocol $|\mathcal{Z}|$, and the round complexity of the protocol m.

Definition 3.6 (α-factors)**.** *For $m \geq 1$, $\ell \geq 2$ and $2 \leq k \leq \ell$, let $\alpha(m,\ell,k) = m^{\frac{2^{\ell-3}}{2^{\ell-2}-1} \cdot \frac{2^{k-2}-1}{2^{k-3}}}$.*

Algorithm 3.7 (Noise)**.**

Input: Parameter 1^m, 1^ℓ and 1^k, and $\delta \in [0,1]$.

Operation:

1. *Let $\alpha = \alpha(m,\ell,k)$ and $\varepsilon = \widehat{\mathcal{C}}^{-1}_{\mathsf{sum}_m(1)}(\delta)$.*
2. *Sample $\bar{\mathbf{b}} \leftarrow (\mathcal{C}_\varepsilon)^{\alpha \cdot \mathsf{sum}_m(1)}$.*
3. *Let $\delta' = \Pr_{\mathcal{X} \subseteq [\alpha \cdot \mathsf{sum}_m(1)], |\mathcal{X}| = \mathsf{sum}_m(1)} \left[\sum_{x \in X} \bar{\mathbf{b}}[x] > 0\right]$.*[16]
4. *Output δ'.*

Namely, Noise sample a vector $\bar{\mathbf{b}}$ of $\alpha \cdot \mathsf{sum}_m(1)$ ε-biased coins. The value of δ' is then determined as the probability to get a positive sum, when sampling $\mathsf{sum}_m(1)$-size subset of coins from $\bar{\mathbf{b}}$.

3.1.5 The Protocol of Haitner and Tsfadia

In this section we define the two-party protocol Π^2 and the functionality $\widetilde{\mathsf{Defense}}^{\mathsf{HT}}$. For clarity, in this subsection we name protocol Π^2 by Π^{HT}.

Protocol Π^{HT} and functionality $\widetilde{\mathsf{Defense}}^{\mathsf{HT}}$ defined below are close variants for those used by Haitner and Tsfadia [33] for construction their three-party coin-flipping protocol. For an elaborated discussion of the ratio underlying the following definitions, see [32].

Protocol Π^{HT}. The two-party m-round protocol Π^{HT}_m is defined as follows (the functionality $\mathsf{RoundDefense}^{\mathsf{HT}}$ used by the protocol is defined below). Recall that for $\ell \in \mathbb{N}$, $h(\ell) = \lceil \log \ell \rceil + 1$ is the number of bits it takes to encode an integer in $[-\ell, \ell]$.

[16] I.e., δ' is the probability that when sampling $\mathsf{sum}_m(1)$ coins from $\bar{\mathbf{b}}$, their sum is positive.

Protocol 3.8 ($\Pi_m^{\mathsf{HT}} = (\mathsf{P}_1, \mathsf{P}_2)$)**.**

Common input: round parameter 1^m.

Oracles: $\mathsf{RoundDefense}^{\mathsf{HT}}$.

P_z*'s input:* $\mathbf{c}^{\#\mathbf{z}} \in \{0,1\}^{m \times h(m)}$, $d^z \in \{0,1\}$, *and* $\mathbf{b}^{\#\mathbf{z},\mathbf{1}}, \mathbf{b}^{\#\mathbf{z},\mathbf{2}} \in \{0,1\}^{2 \cdot \mathsf{sum}_m(1)}$.

Protocol's description:

1. *For* $i = 1$ *to* m*:*
   (a) *The parties jointly call* $\mathsf{RoundDefense}^{\mathsf{HT}}(1^m, c_1, \ldots, c_{i-1}, \mathbf{c}^{\#\mathbf{1}}[i], \mathbf{c}^{\#\mathbf{2}}[i], \mathbf{b}^{\#\mathbf{1},\mathbf{1}}, \mathbf{b}^{\#\mathbf{1},\mathbf{2}}, \mathbf{b}^{\#\mathbf{2},\mathbf{1}}, \mathbf{b}^{\#\mathbf{2},\mathbf{2}})$, *where* $(1^m, c_1, \ldots, c_{i-1})$ *is the common input, and* $(\mathbf{c}^{\#\mathbf{z}}[i], \mathbf{b}^{\#\mathbf{z},\mathbf{1}}, \mathbf{b}^{\#\mathbf{z},\mathbf{2}})$ *is provided by the party* P_z.
   - *For all* $z \in \{1,2\}$, *party* P_z *updates* d^z *to the value it received from this call.*

   (b) P_1 *sends* $\mathbf{c}^{\#\mathbf{1}}[i]$ *to* P_2, *and* P_2 *sends* $\mathbf{c}^{\#\mathbf{2}}[i]$ *to* P_1.
   - *Both parties set* $c_i = \mathbf{c}^{\#\mathbf{1}}[i] \oplus \mathbf{c}^{\#\mathbf{2}}[i]$.
2. *Both parties output* $\mathsf{sign}(\sum_{i=1}^m c_i)$.

Abort: The remaining party P_z *outputs* d^z.

That is, the parties get correlated shares for the rounds' coins, and they reveal them in the main loop at Step 1b. Prior to revealing them, the parties call the $\mathsf{RoundDefense}^{\mathsf{HT}}$ functionality to get a defense value in case the other party aborts during the coin reconstruction.

Algorithm 3.9 ($\mathsf{RoundDefense}^{\mathsf{HT}}$)**.**

Input: Parameter 1^m, *coins* $c_1, \ldots, c_{i-1}$, *and shares* $\mathbf{c}^{\#\mathbf{1}}[i], \mathbf{c}^{\#\mathbf{2}}[i] \in \{0,1\}^{h(m)}$ *and* $\mathbf{b}^{\#\mathbf{1},\mathbf{1}}, \mathbf{b}^{\#\mathbf{2},\mathbf{1}}, \mathbf{b}^{\#\mathbf{1},\mathbf{2}}, \mathbf{b}^{\#\mathbf{2},\mathbf{2}} \in \{-1,1\}^{2 \cdot \mathsf{sum}_m(1)}$.

Operation:

1. *Let* $\mathbf{b}^{\mathbf{1}} = \mathbf{b}^{\#\mathbf{1},\mathbf{1}} \oplus \mathbf{b}^{\#\mathbf{2},\mathbf{1}}$, $\mathbf{b}^{\mathbf{2}} = \mathbf{b}^{\#\mathbf{1},\mathbf{2}} \oplus \mathbf{b}^{\#\mathbf{2},\mathbf{2}}$ *and* $c_i = \mathbf{c}^{\#\mathbf{1}}[i] \oplus \mathbf{c}^{\#\mathbf{2}}[i]$.
2. *For both* $z \in \{1,2\}$*: sample a random* $(\mathsf{sum}_m(i+1))$*-size subset* $\mathcal{W}^z \subset [2 \cdot \mathsf{sum}_m(1)]$, *and set* d^z *to one if* $\sum_{j=1}^i c_j + \sum_{w \in \mathcal{W}^z} \mathbf{b}^{\mathbf{z}}[w] \geq 0$, *and to zero otherwise.*
3. *Return* d^z *to party* P_z.

Namely, to generate a defense value d_z for P_z, $\mathsf{RoundDefense}^{\mathsf{HT}}$ samples $(\mathsf{sum}_m(i+1))$-coins from the vector $\mathbf{b}^{\mathbf{z}}$, adds them to the coin $c_1, \cdots, c_i$ and set d_z to the sign of this sum.

The $\widetilde{\mathsf{Defense}}^{\mathsf{HT}}$ functionality. This functionality prepares the inputs for the parties that interact in Π^{HT}.

Recall that for $n \in \mathbb{N}$ and $\varepsilon \in [-1,1]$, $\mathcal{C}_{n,\varepsilon}$ is the binomial distribution induced by the sum of n independent random ± 1 coins, taking the value 1 with probability $\frac{1}{2}(1+\varepsilon)$, and -1 otherwise.

Algorithm 3.10 ($\widetilde{\mathsf{Defense}}^{\mathsf{HT}}$)**.**

Input: Parameter 1^m *and* $\delta \in [0,1]$.

Operation:

1. *Let* $\varepsilon = \widehat{\mathcal{C}}^{-1}_{\mathsf{sum}_m(1)}(\delta)$.
2. *For* $z \in \{1,2\}$*: sample* $\mathbf{b^z} \leftarrow (\mathcal{C}_\varepsilon)^{2\cdot \mathsf{sum}_m(1)}$.
3. *For* $z \in \{1,2\}$*: sample a random* $(\mathsf{sum}_m(1))$*-size subset* $\mathcal{I}^z \subset [2 \cdot \mathsf{sum}_m(1)]$*, and set* d^z *to one if* $w(\mathbf{b^z}_{\mathcal{I}^z}) \geq 0$*, and to zero otherwise.*
4. *Let* $\mathbf{c} = (c_1, \ldots, c_m)$ *where for* $i \in [m]$*,* $c_i \leftarrow \mathcal{C}_{\ell_m(i),\varepsilon}$.
5. *Sample two uniform shares* $\mathbf{c^{\#1}}, \mathbf{c^{\#2}}$ *with* $\mathbf{c^{\#1}} \oplus \mathbf{c^{\#2}} = \mathbf{c}$*. For both* $z \in \{1,2\}$*, sample two uniform shares* $\mathbf{b^{\#1,z}}, \mathbf{b^{\#2,z}}$ *with* $\mathbf{b^{\#1,z}} \oplus \mathbf{b^{\#2,z}} = \mathbf{b^z}$.
6. *Return:* $((\mathbf{c^{\#z}}, \mathbf{b^{\#z,1}}, \mathbf{b^{\#z,2}}, d^z))_{z\in\{1,2\}}$.

Namely, at Step 1, $\widetilde{\mathsf{Defense}}^{\mathsf{HT}}(\delta)$ calculates $\varepsilon \in [-1,1]$ for which the probability that the sum of $\mathsf{sum}_m(1)$ independent ε-bias coins is positive, is δ. Then, $\widetilde{\mathsf{Defense}}^{\mathsf{HT}}$ uses this ε to sample the rounds' coins c_i, to be used in the two-party protocol Π^{HT}_m, and the vectors that are used by $\mathsf{RoundDefense}^{\mathsf{HT}}$ to give defense values in every round of the loop of Π^{HT}_m.

3.2 Security Analysis of the Hybrid-Model Protocol

In this section we prove the following theorem, stating that Protocol 3.1 cannot be biased much by a fail-stop adversary.

Theorem 3.11. *Fix some integer function* $t' = t'(m)$ *such that* $t' \leq \frac{1}{2}\log\log m$*. For integers* $m \equiv 1 \bmod 12$ *and* $t = t'(m)$*, protocol* $\widehat{\Pi}^t_m$ *is a* $(t \cdot m)$*-round,* t*-party,* $O\left(\frac{t\cdot 2^t \cdot \sqrt{\log m}}{m^{1/2+1/(2^{t-1}-2)}}\right)$*-fair, coin-flipping protocol, against unbounded fail-stop adversaries, in the* $(\mathsf{Defense}, \mathsf{Coin})$*-hybrid model.*

We prove Theorem 3.11 in Section 3.2.4, but first introduce the main tools and concepts used for this proof. *Leakage from two-step boolean process* used to bound attack in Step 1, is presented in Section 3.2.1. *Binomial games* used to bound an attack inside the loop of Protocol 3.2, are introduced in Section 3.2.2. Finally, in Section 3.2.3 we note several simple facts about the protocol.

3.2.1 Leakage from Two-Step Boolean Processes

Our main tool for analyzing the effect of an abort in Step 1 of protocol Π^r_m, for $r > 2$, is bounding the leakage from the relevant "two-step boolean process". A two-step boolean process is a pair of jointly-distributed random variables (A, B), where B is over $\{0,1\}$ and A is over an arbitrary domain $\mathcal{A}$. It is instructive to think that the process' first step is choosing A, and its second step is to choose B as a random function of A. A leakage function f for a two-step process (A, B) is

simply a randomized function over the support of A. We will be interested in bounding by how much the expected outcome of B changes when $f(A)$ is leaked. This change is captured via the notion of prediction advantage.

Definition 3.12 (prediction advantage)**.** *For a two-step process* $\mathsf{P} = (A, B)$ *and a leakage function* f *for* P*, define the* prediction advantage $\Gamma_{\mathsf{P},f}$ *by* $\Gamma_{\mathsf{P},f}(h) = |\Pr[B = 1] - \Pr[B = 1 \mid f(A) = h]|$.

We now define the notions of an hypergeometric process, and of vector leakage function. As we shall see later on, the boolean process that induced in Item 1 of protocol Π^r_m, can be viewed as such a hypergeometric process, coupled to a vector leakage function.

Definition 3.13 (vector leakage function)**.** *Let* s, α *be integers. A randomized function* f *is a* (s, α)-vector leakage function *for the two-step Boolean process* (A, B)*, if on input* $a \in \mathrm{Supp}(A)$*, it outputs a vector in* $\{-1, 1\}^{\alpha \cdot s}$ *according to* $(\mathcal{C}_\varepsilon)^{\alpha \cdot s}$*, for* $\varepsilon = \widehat{\mathcal{C}}_s^{-1}(\mathrm{E}[B \mid A = a])$.

Definition 3.14 (Hypergeometric process)**.** *Let* $s, \beta \in \mathbb{N}$ *and* $\delta \in [0, 1]$*. An* (s, β, δ)-hypergeometric process *is the two-step Boolean process* (A, B) *defined by*

1. $A = \widehat{\mathcal{HG}}_{\beta \cdot s, w(v), s}(0)$*, for* $v \leftarrow (\mathcal{C}_\varepsilon)^{\beta \cdot s}$ *and* $\varepsilon = \widehat{\mathcal{C}}_s^{-1}(\delta)$.
2. $B \leftarrow \mathcal{B}er(A)$,

In Section 3.2.4 we use the following lemma to bound the gain an adversary can achieve by aborting at Step 1 of Π^r_m. The proof is given in Section 4.

Lemma 3.15. *Assume* $s, \alpha, \beta \in \mathbb{N}$ *and* $\delta \in [0, 1]$*, satisfy*

1. $2 \leq \alpha < \beta \leq s$,
2. $\frac{\alpha + \sqrt{s}}{s} \cdot \log^2 s \leq 10^{-5} \cdot \sqrt{\frac{\alpha}{\beta}}$*, and*
3. $\sqrt{\frac{\alpha}{\beta}} \cdot \log s \leq \frac{1}{100}$.

Let $\mathsf{P} = (A, B)$ *be a* (s, β, δ)*-hypergeometric process according to Definition 3.14 , let* f *be an* (s, α)*-vector leakage function for* P *according to Definition 3.13, and let* $\Gamma_{\mathsf{P},f}$ *be according to Definition 3.12. Then, there exists a universal constant* $\lambda > 0$ *such that*

$$\Pr_{h \leftarrow f(A)}\left[\Gamma_{\mathsf{P},f}(h) > \lambda \cdot \sqrt{\log s} \cdot \frac{\sqrt{\alpha}}{\beta}\right] \leq \frac{1}{s^2}.$$

3.2.2 Online-Binomial Games

Our main tool for analyzing the effect an abort in the main loop of the protocol has, is bounding the bias of the relevant "online-binomial games". Following the informal discussion given in Section 1, we give here a formal definition of such games. While in the introduction we referred to a very narrow notion of binomial game, here we cover a wider class of games, letting the challenger to toss many, possibly biased, coins in each round.

Definition 3.16 (online-binomial game)**.** *Let* $m \in \mathbb{N}$*,* $\varepsilon \in [-1, 1]$*, and* f *be a randomized function over* $[m] \times \mathbb{Z} \times \mathbb{Z}$*. The* m-round online binomial game $\mathsf{G}_{m,\varepsilon,f}$ *is the random variable* $\mathsf{G}_{m,\varepsilon,f} = \{C_1, \ldots, C_m, f\}$*, where for every* $i \in [m]$*,* $C_i \leftarrow \mathcal{C}_{(m-i+1)^2,\varepsilon}$*. We refer to each* C_i *as the* i'th round coins*, and to* f *as the* hint *function.*

We will be interested in bounding by how much the outcome of such a game can be biased.

Definition 3.17 (The bias of $G_{m,\varepsilon,f}$)**.** *Let* $\mathsf{G} = \mathsf{G}_{m,\varepsilon,f} = \{C_1, \ldots, C_m, f\}$ *be an* m*-round online binomial game. For* $i \in \{1, \ldots, m\}$*, let* $S_i = \sum_{j=1}^{i} C_j$*, letting* $S_0 = 0$*. For* $i \in \{1, \ldots, m\}$*, let* $H_i = f(i, S_{i-1}, C_i)$*, let* $\delta_i(b) = \Pr[S_m \geq 0 \mid S_{i-1} = b]$*, let* $\delta_i(b, h) = \Pr[S_m \geq 0 \mid S_{i-1} = b,\ H_i = h]$*, let* $O_i = \delta_i(S_{i-1}, H_i)$*, and let* $O_i^- = \delta_i(S_{i-1})$*. Let also* $O_{m+1} = O_{m+1}^- = 1$ *if* $S_m \geq 0$*, and let* $O_{m+1} = O_{m+1}^- = 0$ *if* $S_m < 0$*.*

For an algorithm B*, let* I *be the first round in which* B *outputs* 1 *in the following* m*-round process: in round* i*, algorithm* B *is getting input* (S_{i-1}, H_i) *and outputs a* $\{0,1\}$*-value. Let* $I = m+1$ *if* B *never outputs a one. The* bias B gains in G *is defined by*

$$\mathsf{Bias}_{\mathsf{B}}(\mathsf{G}) = \left| \mathrm{E}\left[O_I - O_I^-\right] \right|$$

The bias of G *is defined by* $\mathsf{Bias}_{m,\varepsilon,f} = \mathsf{Bias}(\mathsf{G}) = \max_{\mathsf{B}}\{\mathsf{Bias}_{\mathsf{B}}(\mathsf{G})\}$*, where the maximum is over* all *possible algorithms* B*.*

Namely, in the i'th round the algorithm B is getting the sum of the coins flipped up to previous round - S_{i-1}, and a "hint" $H_i = f(i, S_{i-1}, C_i)$. If the B decides to abort, it get rewarded by $|\delta_i(S_{i-1}, H_i) - \delta_i(S_{i-1})|$. Hence, B's "goal" is to find the round in which the above gain is maximized.

In the proof of Theorem 3.11, we use the following two lemmas (proven in Section 5).

Definition 3.18 (Vector hint)**.** *For* $m, \ell \in \mathbb{N}$ *and* $\varepsilon \in [-1, 1]$*, define the random function* $f^{\mathsf{vec}}_{m,\varepsilon,\ell} \colon [m] \times \mathbb{Z} \times \mathbb{Z} \mapsto \{-1,1\}^\ell$ *as follows: on input* (i, b, c)*, it calculates* $\delta = \widehat{\mathcal{C}}_{\mathsf{sum}_m(i+1),\varepsilon}(-b-c)$*, and* $\varepsilon := \widehat{\mathcal{C}}^{-1}_{\mathsf{sum}_m(1)}(\delta)$*, and returns a random sample from* $(\mathcal{C}_\varepsilon)^\ell$*.*

Lemma 3.19. *For* $m \in \mathbb{N}$*,* $k \in [m]$*,* $\varepsilon \in [-1, 1]$*, and* $f = f^{\mathsf{vec}}_{m,\varepsilon,k\cdot\mathsf{sum}_m(1)}$*, let* G *be the binomial game* $\mathsf{G}_{m,\varepsilon,f}$ *according to Definition 3.16. Assuming that* $k \leq \frac{m}{\log^6 m}$*, it holds that* $\mathsf{Bias}_{\mathsf{G}} \in O(\frac{\sqrt{k}}{m} \cdot \sqrt{\log m})$*.*

Definition 3.20 (hypergeometric hint)**.** *For* $m \in \mathbb{N}$*, and an integer* $p \in [-2\cdot\mathsf{sum}_m(1), 2\cdot\mathsf{sum}_m(1)]$*, define the random function* $f^{\mathsf{hyp}}_{m,p} \colon [m] \times \mathbb{Z} \times \mathbb{Z} \mapsto \{-1, 1\}$ *as follow: on input* (i, b, c) *outputs* 1 *with probability* $\widehat{\mathcal{HG}}_{2\cdot\mathsf{sum}_m(1),p,\mathsf{sum}_m(i+1)}(-b-c)$ *and* -1 *otherwise.*

Lemma 3.21. *Let* $m \in \mathbb{N}$*,* $\varepsilon \in [-1, 1]$*, and let* p *be integer in* $[-2\cdot\mathsf{sum}_m(1), 2\cdot\mathsf{sum}_m(1)]$*. Assume that* $|p| \leq \lambda \cdot \sqrt{\log m \cdot \mathsf{sum}_m(1)}$ *for some constant* λ*, and let* $f = f^{\mathsf{hyp}}_{m,p}$*. Let* G *be the binomial game* $\mathsf{G}_{m,\varepsilon,f}$ *according to Definition 3.16, then* $\mathsf{Bias}_{\mathsf{G}} \in O(\frac{\sqrt{\log m}}{m})$*.*

3.2.3 Basic Observations about Protocol 3.1

The following simple facts are used within the proof of Theorem 3.11. We start with a simple observation regarding the outcome of the Defense functionality.

Fact 3.22. *Let* $m \geq 1$*,* $r > 2$*,* $\ell \in \mathbb{N}$*,* $\delta \in [0, 1]$ *and* $\mathcal{Z} = (z_1, \ldots, z_{|\mathcal{Z}|}) \subseteq [r]$*, and let* $S = (S_1, \ldots, S_r) = \widetilde{\mathsf{Defense}}(1^m, 1^r, 1^\ell, \mathcal{Z}, \delta)$*. Let* $\mathsf{outcome}(S)$ *be the outcome of a non-aborting execution of protocol* $\Pi_m^{|\mathcal{Z}|}$ *on common input* 1^ℓ*, and the* j*'th party private input is set to* S_{z_j}*. Then for every* $\mathcal{B} \subset [r]$ *with* $\mathcal{Z} \not\subset \mathcal{B}$ *and for every* $\mathbf{s} \in \mathrm{Supp}(S^{\mathcal{B}} = \{S_z\}_{z\in\mathcal{B}})$*, it holds that* $\mathrm{E}\left[\mathsf{outcome}(S) \mid S^{\mathcal{B}} = \mathbf{s}\right] = \delta$*.*

Namely, in an honest interaction that follows an abort, the expected outcome of the interaction is δ, for δ being the input in the last call to $\widetilde{\mathsf{Defense}}$ that happened before the abort. The latter holds, even conditioned on the partial information held by the corrupted parties.

Proof. Assume without loss of generality that $\mathcal{B} = \{2, \ldots, r\}$, and that $\mathcal{Z} = \{1, \ldots, |\mathcal{Z}|\}$. Consider an honest execution of protocol $\Pi_m^{|\mathcal{Z}|}$, in which party P_z for $z \in \mathcal{Z}$ start with private inputs S_j for $1 \leq j \leq |\mathcal{Z}|$.[17] Let $\mathbf{s} = (s_2, \ldots, s_r) \in \mathrm{Supp}(S^{\mathcal{B}})$.

By construction of $\mathsf{Defense}$ functionality, and specifically since it breaks the output into random shares, it holds that $\mathrm{E}\left[\bigoplus_{i=1}^{|\mathcal{Z}|} S_i \mid S^{\mathcal{B}} = s\right] = \delta$. Writing it a bit differently:

$$\mathop{\mathrm{E}}_{S_1}\left[S_1 \oplus s_2 \oplus \ldots \oplus s_{|\mathcal{Z}|}\right] = \delta \tag{1}$$

By construction of Protocol 3.2, it holds that

$$\mathrm{E}\left[\mathsf{outcome}(S) \mid S_1, \ldots, S_{|\mathcal{Z}|}\right] = S_1 \oplus \ldots \oplus S_{|\mathcal{Z}|} \tag{2}$$

Putting it together we get:

$$\begin{aligned}
\mathrm{E}\left[\mathsf{outcome}(S) \mid S^{\mathcal{B}} = s\right] &= \mathrm{E}\left[\mathsf{outcome}(S) \mid S_2 = s_2, \ldots, S_r = s_r\right] \\
&= \mathop{\mathrm{E}}_{S_1}\left[\mathrm{E}\left[\mathsf{outcome}(S) \mid S_1, S_2 = s_2, \ldots, S_r = s_r\right]\right] \\
&= \mathop{\mathrm{E}}_{S_1}\left[S_1 \oplus s_2 \oplus \ldots \oplus s_{|\mathcal{Z}|}\right] \\
&= \delta,
\end{aligned}$$

as required. □

We remind the reader that the α-factors are: $\alpha(m, \ell, k) = m^{\frac{2^{\ell-3}}{2^{\ell-2}-1} \cdot \frac{2^{k-2}-1}{2^{k-3}}}$ (see Definition 3.6). The following fact states some basic properties of the α-factors.

Fact 3.23. *Let $m \geq 1$ and $\ell \geq 2$ be two integers, and denote for simplicity $\alpha_k = \alpha(m, \ell, k)$. It holds that*

1. $\alpha_{\ell-1} = m^{1 - \frac{1}{2^{\ell-2}-1}}$.
2. $\alpha_2 = 1$.
3. $\frac{\sqrt{\alpha_2}}{\alpha_3} = \ldots = \frac{\sqrt{\alpha_{\ell-3}}}{\alpha_{\ell-2}} = \frac{\sqrt{\alpha_{\ell-2}}}{\alpha_{\ell-1}} = \frac{\sqrt{\alpha_{\ell-1}}}{m} = \frac{1}{m^{\frac{1}{2} + \frac{1}{2^{\ell-1}-2}}}$.

Proof. Immediate by definition. □

[17] The parties that participate in this execution have more inputs for the case that some of them will abort later on. Since, however, we are interested in an honest execution, those additional inputs can be ignored.

3.2.4 Proving Theorem 3.11

Proof of Theorem 3.11. By construction, in an all-honest execution the parties output a uniform bit, so it left to prove that the protocol cannot be biased by too much by fail-stop adversaries.

Let A be a fail-stop adversary controlling the parties $\{\widehat{\mathsf{P}}_z\}_{z\in\mathcal{C}}$ for some $\mathcal{C} \subsetneq [t]$. Let V be the (joint) view of the parties controlled by A, let V_i is the prefix of V at the end of round i, and V_i^- be the prefix of V_i with the i'th round abort messages (if any) removed. Let $\mathsf{val}(v)$ be the expected outcome of an honest (non-aborting) execution of the protocol by the parties that do not abort in v, conditioned on v (see Definition 2.13). We assume without loss of generality that if A instructs a corrupted party to abort at a given round, it does so *after* seeing the honest parties' messages of that round.

For $k \in [t-1]$, let I_k be the k-th aborting communication round (that is, the k'th round in which at least one party aborts). Letting $I_k = \perp$ if less than k aborting rounds happen, and let $V_\perp = V_\perp^-$. By Lemma 2.15, to prove the theorem it is sufficient to show that:

$$\left|\mathop{\mathrm{E}}_{V}\left[\sum_{k=1}^{t-1}\mathsf{val}(V_{I_k}) - \mathsf{val}(V_{I_k}^-)\right]\right| \le O\left(\frac{t\cdot 2^t\cdot\sqrt{\log m}}{m^{1/2+1/(2^{t-1}-2)}}\right). \tag{3}$$

Since

$$\left|\mathop{\mathrm{E}}_{V}\left[\sum_{k=1}^{t-1}\mathsf{val}(V_{I_k}) - \mathsf{val}(V_{I_k}^-)\right]\right| = \left|\sum_{k=1}^{t-1}\mathop{\mathrm{E}}_{V}\left[\mathsf{val}(V_{I_k}) - \mathsf{val}(V_{I_k}^-)\right]\right| \le \sum_{k=1}^{t-1}\left|\mathop{\mathrm{E}}_{V}\left[\mathsf{val}(V_{I_k}) - \mathsf{val}(V_{I_k}^-)\right]\right|,$$

it suffices to show that

$$\left|\mathop{\mathrm{E}}_{V}\left[\mathsf{val}(V_{I_k}) - \mathsf{val}(V_{I_k}^-)\right]\right| \le O\left(\frac{2^t\cdot\sqrt{\log m}}{m^{1/2+1/(2^{t-1}-2)}}\right) \tag{4}$$

for every $1 \le k \le t-1$.

Fix $1 \le k \le t-1$. The k'th abort can occur in one of the following places:

- In Step 3 of the parent protocol $\widehat{\Pi}_m^t$ (can only happen for $k = 1$).
- During the execution of protocol Π_m^r, for some $r \le t$.

Since by construction aborting in Step 3 gives nothing to the adversary, it is left to prove that Equation (4) holds for aborting done during an execution of Π_m^r.

Let $R = R(k)$ be the number of active parties when the k'th abort occur (that means that it occurs during the execution of Π_m^R). We show that for any value of $r \in \{2,\ldots,t\}$, it holds that

$$\left|\mathop{\mathrm{E}}_{V|R=r}\left[\mathsf{val}(V_{I_k}) - \mathsf{val}(V_{I_k}^-)\right]\right| \le O\left(\frac{2^t\cdot\sqrt{\log m}}{m^{1/2+1/(2^{t-1}-2)}}\right) \tag{5}$$

and Equation (4) will follow.

Let $I = I_k$. For $r \in \{2,\ldots,t\}$, we condition till the end of the proof on $R = r$. We distinguish between the case $r > 2$ case, and $r = 2$.

The case $r > 2$. Recall that protocol Π_m^r has five step: Step 1, Step 2, Step 3a, Step 3b, and Step 3c. We let $\mathcal{S} = \{1, 2, 3a, 3b, 3c\}$, and let $T \in \mathcal{S}$ to be the step executed in round I. Applying complete expectation on the left side of Equation (5), we get that (we remind the reader that with let $I_k = I$, and we fixed some value of r):

$$\left|\mathop{\mathrm{E}}_{V}\left[\mathsf{val}(V_I) - \mathsf{val}(V_I^-)\right]\right| = \sum_{j \in \mathcal{S}} \left|\mathop{\mathrm{E}}_{V|T=j}\left[\mathsf{val}(V_I) - \mathsf{val}(V_I^-)\right]\right| \cdot \Pr\left[T = j\right] \tag{6}$$

In the following we prove that for $t \in \{2, 3a, 3c\}$ it holds that

$$\mathsf{val}(V_I|_{T=t}) = \mathsf{val}(V_I^-|_{T=t}), \tag{7}$$

that for $t = 1$ it holds that

$$\left|\mathrm{E}\left[\mathsf{val}(V_I) - \mathsf{val}(V_I^-) \mid T = 1\right]\right| \cdot \Pr\left[T = 1\right] \leq O\left(\frac{2^t \cdot \sqrt{\log m}}{m^{1/2+1/(2^{t-1}-2)}}\right), \tag{8}$$

and that for $t = 3b$ it holds that

$$\left|\mathrm{E}\left[\mathsf{val}(V_I) - \mathsf{val}(V_I^-) \mid T = 3b\right]\right| \cdot \Pr\left[T = 3b\right] \leq O\left(\frac{2^t \cdot \sqrt{\log m}}{m^{1/2+1/(2^{t-1}-2)}}\right). \tag{9}$$

Putting Equation (7), Equation (8), and Equation (9), in Equation (6), yields that $\left|\mathrm{E}_V\left[\mathsf{val}(V_I) - \mathsf{val}(V_I^-)\right]\right| \leq O\left(\frac{2^t \cdot \sqrt{\log m}}{m^{1/2+1/(2^{t-1}-2)}}\right)$, proving Equation (5).

The following random variables are define with respect to this interaction of Π_m^r. Let Δ be the value of δ calculated in Step 2, set to $\perp$ if an abort occurred before this round (i.e., $T < 2$), and let Δ_{def} be the value of the parameter δ in the last call to $\widetilde{\mathsf{Defense}}$ before I (by definition, such a call is guaranteed to exist).

By Fact 3.22, it holds that

$$\mathsf{val}(V_I) = \Delta_{\mathsf{def}} \tag{10}$$

Proving Equation (7). We prove separately for every $t \in \{2, 3a, 3c\}$.

$t = 2$**:** By construction, in case of no abort, the expected outcome of the protocol at the end of Step 2 is Δ, namely $\mathsf{val}(V_I^-|_{T=2}) = \Delta$. Since by construction $\Delta = \Delta_{\mathsf{def}}$, Equation (10) yields that $\mathsf{val}(V_I|_{T=2}) = \mathsf{val}(V_I^-|_{T=2})$.

$t = 3a$**:** Since c_i and δ_i are shared using an r-out-of-r secret sharing schemes, V_I contains *no information* about c_i and δ_i. Thus, $\mathsf{val}(V_I^-) = \mathsf{val}(V_{I-1})$. If I is the very first round to reach Step 3a (i.e., we are in the first round of the loop), then by construction $\mathsf{val}(V_{I-1}) = \Delta = \Delta_{\mathsf{def}}$. Otherwise (not the first round in the loop), by definition $\mathsf{val}(V_{I-1}) = \Pr\left[\mathsf{sign}(\sum_{i=1}^m c_i) = 1 \mid V_{I-1}\right]$, which by construction is also equal to Δ_{def}. Hence, by Equation (10), $\mathsf{val}(V_I) = \mathsf{val}(V_I^-)$.

$t = 3c$**:** Follows by an analogues argument to that used for proving the case $t = 2$.

Proving Equation (8). In the following we condition on $V_{I-1} = v'$ for some $v' \in \mathrm{Supp}(V_{I-1})|_{T=1}$.

Let M be the messages that the corrupted parties receive during the execution of Item 1. We assume without loss of generality that M contains also the vectors of coins sampled in Step 2 of functionality Noise (happened by the joint call to $\mathsf{Defense}$ done in this round) that was used to generate the defense values (i.e., the messages) of the corrupted parties.[18] We remind the reader that Δ_{def} is the value of the δ parameter passed to the last call of $\mathsf{Defense}$. By construction, Δ_{def} is a deterministic function of V_{I-1}. Since we conditioned on $V_{I-1} = v'$, we conclude that Δ_{def} has a fixed value, denote this value by δ_{def}.

The proof follow by the next claim (proven below).

Claim 3.24. *It holds that*

$$\Pr_{n \leftarrow M}\left[\left|\delta_{\mathsf{def}} - \mathrm{E}\left[\Delta \mid M = n\right]\right| > \lambda \cdot \frac{\sqrt{2^r \cdot \alpha_{r-1}}}{\alpha_r} \cdot \sqrt{\log m}\right] \leq \frac{1}{m^2}.$$

Namely, with high probability, after the adversary sees the messages of Step 1, the value of Δ is not far from δ_{def}. It follows that

$$\begin{aligned}
\mathop{\mathrm{E}}_{V_I|T=1}\left[\mathsf{val}(V_I) - \mathsf{val}(V_I^-)\right] &= \mathop{\mathrm{E}}_{V_I|T=1}\left[\mathsf{val}(V_I)\right] - \mathop{\mathrm{E}}_{V_I|T=1}\left[\mathsf{val}(V_I^-)\right] && (11)\\
&= \delta_{\mathsf{def}} - \mathop{\mathrm{E}}_{V_I|T=1}\left[\mathsf{val}(V_I^-)\right] && (12)\\
&= \delta_{\mathsf{def}} - \mathop{\mathrm{E}}_{V_I|T=1}\left[\mathrm{E}\left[\Delta \mid V_I\right]\right] && (13)\\
&= \mathop{\mathrm{E}}_{V_I|T=1}\left[\delta_{\mathsf{def}} - \mathrm{E}\left[\Delta \mid V_I\right]\right]\\
&= \mathop{\mathrm{E}}_{M|T=1}\left[\delta_{\mathsf{def}} - \mathrm{E}\left[\Delta \mid M\right]\right]
\end{aligned}$$

Equation (12) holds by Fact 3.22. Equation (13) holds since conditioned on $T = 1$, $\mathsf{val}(V_I^-) = \mathrm{E}\left[\Delta \mid V_I\right]$. Applying triangle inequality to Equation (11), and multipling it by $\Pr\left[T = 1\right]$, it holds that

$$\left|\mathop{\mathrm{E}}_{V_I|T=1}\left[\mathsf{val}(V_I) - \mathsf{val}(V_I^-)\right]\right| \cdot \Pr\left[T = 1\right] \leq \mathop{\mathrm{E}}_{M|T=1}\left[\left|\delta_{\mathsf{def}} - \mathrm{E}\left[\Delta \mid M\right]\right|\right] \cdot \Pr\left[T = 1\right]$$

Continuing the evaluation, it holds that

$$\begin{aligned}
\mathop{\mathrm{E}}_{N|T=1}\left[\left|\delta_{\mathsf{def}} - \mathrm{E}\left[\Delta \mid N\right]\right|\right] \cdot \Pr\left[T = 1\right] &\leq \mathop{\mathrm{E}}_{N}\left[\left|\delta_{\mathsf{def}} - \mathrm{E}\left[\Delta \mid N\right]\right|\right]\\
&= \sum_{n \in \mathrm{Supp}(N)} \left|\delta_{\mathsf{def}} - \mathrm{E}\left[\Delta \mid N = n\right]\right| \cdot \Pr\left[N = n\right],
\end{aligned}$$

Applying Claim 3.24 to previous inequality yields that

$$\mathop{\mathrm{E}}_{M|T=1}\left[\left|\delta_{\mathsf{def}} - \mathrm{E}\left[\Delta \mid M\right]\right|\right] \cdot \Pr\left[T = 1\right] \leq 1 \cdot \frac{1}{m^2} + \lambda \cdot \frac{\sqrt{2^r \cdot \alpha_{r-1}}}{\alpha_r} \cdot \sqrt{\log m} \qquad (14)$$

[18] An adversary that can bias the protocol without this additional information, can be emulated by an adversary that get this additional information.

for some universal constant λ. Finally, since $\frac{\sqrt{2^r \cdot \alpha_{r-1}}}{\alpha_r} \leq \frac{\sqrt{2^r \cdot \alpha_{\ell-1}}}{m} = \frac{\sqrt{2^r}}{m^{\frac{1}{2}+\frac{1}{2^{\ell-1}-2}}}$ (Fact 3.23), we conclude that

$$\left| \mathop{\mathrm{E}}_{V_I|T=1} \left[\mathsf{val}(V_I) - \mathsf{val}(V_I^-) \right] \right| \cdot \Pr\left[T = 1\right] \leq O\left(\frac{2^r \cdot \sqrt{\log m}}{m^{1/2+1/\left(2^{\ell-1}-2\right)}} \right) = O\left(\frac{2^t \cdot \sqrt{\log m}}{m^{1/2+1/\left(2^{\ell-1}-2\right)}} \right),$$

which is the same as Equation (8).

Proving Equation (9). We prove Equation (9) in the following claim.

Claim 3.25. $\left| \mathrm{E}\left[\mathsf{val}(V_I) - \mathsf{val}(V_I^-) \ \mid \ T = 3b \right] \right| \cdot \Pr\left[T = 3b\right] \leq O\left(\frac{2^t \cdot \sqrt{\log m}}{m^{1/2+1/(2^{\ell-1}-2)}} \right)$.

The case of $r = 2$. The proof of this case follows similar lines to that of [32, Thm 3.10], using the new bound for binomial game given in Lemma 3.21, instead of the bound used in [32]. Details below.

We prove $\Pi_m^2 = \Pi_m^{\mathsf{HT}}$ is secured against an abort action. By construction, A can abort either in Step 1a (i.e., during the call to $\mathsf{RoundDefense}^{\mathsf{HT}}$), or in Step 1b (i.e., during the reconstruction of the coin). We let $T \in \{1a, 1b\}$ to be the step executed in round I. Applying complete expectation on the left side of Equation (5), we get that :

$$\left| \mathop{\mathrm{E}}_{V} \left[\mathsf{val}(V_I) - \mathsf{val}(V_I^-) \right] \right| = \sum_{j \in \{1a, 1b\}} \left| \mathop{\mathrm{E}}_{V|T=j} \left[\mathsf{val}(V_I) - \mathsf{val}(V_I^-) \right] \right| \cdot \Pr\left[T = j\right] \tag{15}$$

Similar lines to that used to analyze abort in Step 3c of protocol Π_m^r with $r > 2$, yield that conditioned on $T = 1b$, it holds that $\mathrm{E}\left[\mathsf{val}(V_I)\right] = \mathrm{E}\left[\mathsf{val}(V_I^-)\right]$. Putting it in Equation (15), we get:

$$\left| \mathop{\mathrm{E}}_{V} \left[\mathsf{val}(V_I) - \mathsf{val}(V_I^-) \right] \right| = \left| \mathop{\mathrm{E}}_{V|T=1a} \left[\mathsf{val}(V_I) - \mathsf{val}(V_I^-) \right] \right| \cdot \Pr\left[T = 1a\right]$$

Hence, the following finishes the proof of the theorem

$$\left| \mathop{\mathrm{E}}_{V|T=1a} \left[\mathsf{val}(V_I) - \mathsf{val}(V_I^-) \right] \right| \cdot \Pr\left[T = 1a\right] \leq O\left(\frac{2^t \cdot \sqrt{\log m}}{m^{1/2+1/(2^{t-1}-2)}} \right) \tag{16}$$

let P be the sum of all entries of the vector $\mathbf{b^1}$ (sampled at Step 2 of $\widetilde{\mathsf{Defense}}^{\mathsf{HT}}$) during the last execution of $\widetilde{\mathsf{Defense}}^{\mathsf{HT}}$. [19] Let $\tau = 12 \cdot \sqrt{\log m \cdot \mathsf{sum}_m(1)}$. It holds that,

$$\left| \mathrm{E}\left[\mathsf{val}(V_I) - \mathsf{val}(V_I^-) \ \mid \ T = 1a \right] \right| \cdot \Pr\left[T = 1a\right] =$$

$$\left| \mathrm{E}\left[\mathsf{val}(V_I) - \mathsf{val}(V_I^-) \ \mid |P| > \tau, T = 1a \right] \right| \cdot \Pr\left[|P| > \tau \ \mid \ T = 1a\right] \cdot \Pr\left[T = 1a\right] + \tag{17}$$

$$\left| \mathrm{E}\left[\mathsf{val}(V_I) - \mathsf{val}(V_I^-) \ \mid |P| \leq \tau, T = 1a \right] \right| \cdot \Pr\left[|P| \leq \tau \ \mid \ T = 1a\right] \cdot \Pr\left[T = 1a\right] \tag{18}$$

[19] Using the notations from Section 2.1, we can define P to be: $P = w(\mathbf{b^1})$.

The term from Line 17 contains in it $\Pr\left[|P| > \tau \;\middle|\; T = 1a\right] \cdot \Pr\left[T = 1a\right]$ which is bounded by $\Pr\left[|P| > \tau\right]$. By Hoeffding's inequality,

$$\Pr\left[|P| > \tau\right] \leq \Pr\left[\left|P - 2\varepsilon \cdot \mathsf{sum}_m(1)\right| > 4 \cdot \sqrt{\log m \cdot \mathsf{sum}_m(1)}\right] \leq \frac{1}{m}. \tag{19}$$

The term from Line 18 satisfies:

$$\left|\mathrm{E}\left[\mathsf{val}(V_I) - \mathsf{val}(V_I^-) \;\middle|\; |P| \leq \tau, T = 1a\right]\right| \cdot \Pr\left[|P| \leq \tau \;\middle|\; T = 1a\right] \cdot \Pr\left[T = 1a\right] \leq$$
$$\left|\mathrm{E}\left[\mathsf{val}(V_I) - \mathsf{val}(V_I^-) \;\middle|\; |P| \leq \tau, T = 1a\right]\right| \cdot \Pr\left[T = 1a \;\middle|\; |P| \leq \tau\right]$$

Hence, in order to prove Equation (16) (and finish the proof), we prove the following:

Claim 3.26.

$$\left|\mathrm{E}\left[\mathsf{val}(V_I) - \mathsf{val}(V_I^-) \;\middle|\; |P| \leq \tau, T = 1a\right]\right| \cdot \Pr\left[T = 1a \mid |P| \leq \tau\right] \leq O\left(\frac{2^t \cdot \sqrt{\log m}}{m^{1/2+1/(2^{t-1}-2)}}\right)$$

□

Remark 3.27 (On the setting of the α-factors and using the protocol of [32] for the two-party sub-protocol.)**.** *Following the notations from the proof of Theorem 3.11, let Δ be the value of δ calculated in Step 2 of protocol Π_m^r. Let $\alpha_k = \alpha(m, t, k)$ (i.e., as in Fact 3.23). By construction, $\alpha_r \cdot \mathsf{sum}_m(1)$ is the number (independent, possibly biases) coins used in Step 2 of the* Noise *functionality to determined the value of Δ, and (roughly) $\alpha_{r-1} \cdot \mathsf{sum}_m(1)$ coins are used in by the* Defense *functionality at Step 1 of protocol Π_m^r. It can be shown that (roughly):*

1. *Aborting at Step 3b of Π_m^t, gains bias $\frac{\sqrt{\alpha_{t-1}}}{m}$.*
2. *Aborting at Step 1 of protocol Π_m^r for $2 \leq r < t$, gains bias $\frac{\sqrt{\alpha_{r-1}}}{\alpha_r}$.*

and there are no other attacking opportunities.

Since protocol Π_m^2 (i.e., protocol Π_m^{HT}) uses $\Theta(\mathsf{sum}_m(1))$ coins, by the above observation about the α's it holds that $\alpha_2 = 1$. Optimizing the choice of α's to minimize the bias they yield according to Item 1 and Item 2, yields the following equation:

$$\left(\frac{\sqrt{\alpha_2}}{\alpha_3} =\right) \frac{1}{\alpha_3} = \frac{\sqrt{\alpha_3}}{\alpha_4} = \ldots = \frac{\sqrt{\alpha_{t-2}}}{\alpha_{t-1}} = \frac{\sqrt{\alpha_{t-1}}}{m} \tag{20}$$

Assume that instead of using protocol Π^{HT} in the two players case, we would have used protocol Π_m^r (Protocol 3.2) with $r = 2$. Now an adversary has an additional attacking opportunity (at Step 1 of protocol Π_2^r), which gains bias $\frac{\sqrt{\alpha_1}}{\alpha_2} = \frac{1}{\alpha_2}$.

As a result, when optimizing the parameters of the new protocol, Equation (20) changes to

$$\frac{1}{\alpha_2} = \frac{\sqrt{\alpha_2}}{\alpha_3} = \ldots = \frac{\sqrt{\alpha_{t-2}}}{\alpha_{t-1}} = \frac{\sqrt{\alpha_{t-1}}}{m} \tag{21}$$

Consider for instance the case of four players (i.e., $t = 4$). When of using Π^{HT} (as we actually do), Equation (20) becomes $\frac{1}{\alpha_3} = \frac{\sqrt{\alpha_3}}{m}$, implying that $\alpha_3 = m^{2/3}$. This yields roughly an overall bias of $\frac{1}{m^{2/3}}$. When using Protocol 3.2 also for the case $r = 2$, Equation (21) becomes $\frac{1}{\alpha_2} = \frac{\sqrt{\alpha_2}}{\alpha_3} = \frac{\sqrt{\alpha_3}}{m}$, implying that $\alpha_2 = m^{4/7}$, yielding roughly an overall bias of $\frac{1}{m^{4/7}}$.

Proving Claim 3.24

Proof of Claim 3.24. Define the two-step process (see Section 3.2.1 for an introduction about leakage from two-step boolean processes) $P = (A, B)$, for $A = \Delta$, and $B = \mathcal{B}er(A)$, and define a leakage function f for P by $f(a) = M|_{A=a}$ (i.e., the messages received by the corrupted parties at round s^1). By definition, $\delta_{\mathsf{def}} - \Pr[\Delta = 1 \mid M = n] = \Gamma_{P,f}(m)$ for every $n \in \mathrm{Supp}(M)$. Hence, it is left to prove that

$$\Pr_{n \leftarrow M}\left[|\Gamma_{P,f}(n)| > \lambda \cdot \frac{\sqrt{2^r \cdot \alpha_{r-1}}}{\alpha_r} \cdot \sqrt{\log m}\right] \leq \frac{1}{m^2}. \tag{22}$$

Let $P' = (A', B')$ be a $\langle \mathsf{sum}_m(1), \alpha_r, \delta_{\mathsf{def}} \rangle$-hypergeometric process (see Definition 3.14), and let f' be a $(\mathsf{sum}_m(1), 2^r \cdot \alpha_{r-1})$-vector leakage function (see Definition 3.13) for P'. By construction, it holds that $P \equiv P'$ (i.e., the two random variables are distributed the same). We remind the reader that we assume that M contains also the vectors of coins sampled at Step 2 in the Noise algorithm, and that the messages that the corrupted parties get are a random function of those vectors. Hence, for every $a \in \mathrm{Supp}(A)$, $f(a)$ is a concatenation of $f'(a)$ and some random function of $f(a)$. Thus (see Proposition 4.11), for proving Equation (22) it suffices to show that

$$\Pr_{h \leftarrow f'(A')}\left[\left|\Gamma_{P',f'}(h)\right| > \lambda \cdot \frac{\sqrt{2^r \cdot \alpha_{r-1}}}{\alpha_r} \cdot \sqrt{\log m}\right] \leq \frac{1}{m^2} \tag{23}$$

We prove the above equation by applying Lemma 3.15 for the hypergeometric process (A', B') with the vector leakage function f', and parameters $s = \mathsf{sum}_m(1)$, $\beta = \alpha_r$ and $\alpha = 2^r \cdot \alpha_{r-1}$. Note that the first and third conditions of Lemma 3.15 trivially holds for this choice of parameters, whereas the second condition holds since $\frac{\log^2 s}{\sqrt{s}} = o(\sqrt{\frac{\alpha}{\beta}})$ and since $\frac{\alpha}{s} \cdot \log^2 s = o(\sqrt{\frac{\alpha}{\beta}})$ for $r \leq t = o(\log m)$. Therefore, Lemma 3.15 yields that

$$\Pr_{h \leftarrow f'(A')}\left[\left|\Gamma_{P',f'}(h)\right| > \lambda' \sqrt{\log s} \cdot \frac{\sqrt{\alpha}}{\beta}\right] \leq \frac{1}{s^2},$$

for some universal constant $\lambda' > 0$. We conclude that

$$\Pr_{h \leftarrow f'(A')}\left[\left|\Gamma_{P',f'}(h)\right| > 2\lambda' \sqrt{\log m} \cdot \frac{\sqrt{2^r \cdot \alpha_{r-1}}}{\alpha_r}\right] \leq \frac{1}{s^2} \leq \frac{1}{m^2},$$

and the proof of the claim follows. □

Proving Claim 3.25.

Proof of Claim 3.25. Assume towards a contradiction that:

$$\left|\mathrm{E}\left[\mathsf{val}(V_I) - \mathsf{val}(V_I^-) \;\mid\; T = 3b\right]\right| \cdot \Pr[T = 3b] = \omega\left(\frac{2^t \cdot \sqrt{\log m}}{m^{1/2+1/(2^{\ell-1}-2)}}\right) \tag{24}$$

Let Δ be the value of δ calculated in Step 2 of Π_m^r, and let $\mathcal{E} = \widehat{\mathcal{C}}^{-1}_{\mathsf{sum}_m(1)}(\Delta)$. Note that $\mathcal{E}$ is the bias of the coins tossed in the main loop of Π_m^r.

Since

$$\left|\mathrm{E}\left[\mathsf{val}(V_I) - \mathsf{val}(V_I^-) \;\mid\; T = 3b\right]\right| \cdot \Pr\left[T = 3b\right] =$$
$$\sum_{\varepsilon \in \mathrm{Supp}(\mathcal{E})} \left|\mathrm{E}\left[\mathsf{val}(V_I) - \mathsf{val}(V_I^-) \;\mid\; \mathcal{E} = \varepsilon, T = 3b\right]\right| \cdot \Pr\left[\mathcal{E} = \varepsilon \mid T = 3b\right] \cdot \Pr\left[T = 3b\right] =$$
$$\sum_{\varepsilon \in \mathrm{Supp}(\mathcal{E})} \left|\mathrm{E}\left[\mathsf{val}(V_I) - \mathsf{val}(V_I^-) \;\mid\; \mathcal{E} = \varepsilon, T = 3b\right]\right| \cdot \Pr\left[T = 3b \mid \mathcal{E} = \varepsilon\right] \cdot \Pr\left[\mathcal{E} = \varepsilon\right],$$

Equation (24) yields that

$$\left|\mathrm{E}\left[\mathsf{val}(V_I) - \mathsf{val}(V_I^-) \;\mid\; \mathcal{E} = \varepsilon', T = 3b\right]\right| \cdot \Pr\left[T = 3b \mid \mathcal{E} = \varepsilon'\right] = \omega\left(\frac{2^t \cdot \sqrt{\log m}}{m^{1/2+1/\left(2^{\ell-1}-2\right)}}\right) \tag{25}$$

for some $\varepsilon' \in \mathrm{Supp}(\mathcal{E})$.

Let $\tilde{r}_{\mathsf{A}}$ and $\tilde{r}_h$ be a fixing of A and the honest party respectively, that cause the protocol to reach the main loop of Π_m^r with $\mathcal{E} = \varepsilon'$. Let $\beta = \left|\mathrm{E}\left[\mathsf{val}(V_I) - \mathsf{val}(V_I^-) \;\mid\; \mathcal{E} = \varepsilon', T = 3b\right]\right| \cdot \Pr\left[T = 3b \mid \mathcal{E} = \varepsilon'\right]$ — the gain of the adversary A, conditioned on $\mathcal{E} = \varepsilon'$.

Let $f = f^{\mathsf{vec}}_{m,\varepsilon',2^r\cdot\alpha_{r-1}\cdot\mathsf{sum}_m(1)}$ be according to Definition 3.18, let $\mathsf{G} = \mathsf{G}_{m,\varepsilon,f}$ be a binomial game with vector hint according to *Definition* 3.16 and let Bias be according to Definition 3.17. We next show that $\beta \leq \mathsf{Bias}(\mathsf{G})$. Observe that the assumption $r < \frac{1}{2}\log\log m$ implies that $2^r \cdot \alpha_{r-1} < \frac{m}{\log^6 m}$. Hence, we can apply Lemma 3.19 and together with Fact 3.23 it holds that

$$\beta \leq \mathsf{Bias}(\mathsf{G}) \leq O(\frac{\sqrt{2^r \cdot \alpha_{r-1}}}{m} \cdot \sqrt{\log m}) = O\left(\frac{\sqrt{2^r} \cdot \sqrt{\log m}}{m^{\frac{1}{2}+\frac{1}{2^{\ell-1}-2}}}\right) = O\left(\frac{2^t \cdot \sqrt{\log m}}{m^{1/2+1/\left(2^{\ell-1}-2\right)}}\right),$$

contradicting Equation (25).

To show that $\beta \leq \mathsf{Bias}(\mathsf{G})$, we define a player B for the game G, that achieves bias β.

Algorithm 3.28 (player B)**.**

Operation:

1. *Start emulating an execution of protocol $\widehat{\Pi}_m^t(1^\ell)$, with A controlling parties $\mathsf{P}_1, \ldots, \mathsf{P}_{t-1}$, where A uses randomness $\tilde{r}_{\mathsf{A}}$, and the honest party P_t uses randomness $\tilde{r}_h$ until the main loop of Π_m^r is reached. (If not reached, B never aborts.) From that point, continue the execution randomly using fresh new randomness.*

2. *For $i = 1$ to m:*

   (a) *Let (s_{i-1}, h_i) be the i'th message sent by the challenger.*

   (b) *If $i > 1$, emulate Step 3c: let $c_{i-1} = s_i - s_{i-1}$ and set $c_{i-1}^{\#r}$ such that $c_{i-1} = \bigoplus_{z\in[r]} c_{i-1}^{\#z}$. Emulate the reconstruction of c_{i-1}, letting $c_{i-1}^{\#r}$ be the message of the honest party.*

   (c) *Emulate Step 3a: send the corrupted parties $2 \cdot (r-1)$ random strings $(c_i^{\#1}, \delta_i^{\#1}, \ldots, c_i^{\#r-1}, \delta_i^{\#r-1})$ as the answers of Coin.*

(d) *Emulate Step 3b: emulate the parallel calls to* Defense *using the hint* h_i.

Recall that the Defense *functionality is merely a deterministic wrapper for the* $\widetilde{\mathsf{Defense}}$ *functionality, and the latter, in turn, is a wrapper to the* Noise *functionality. Hence, it suffices to shows how to use* h_i *for emulating these calls to* Noise. *The* Noise *functionality uses* $\alpha_{r-1} \cdot \mathsf{sum}_m(1)$ *independent* $\mathcal{C}_{\varepsilon'}$*-biased coins per call, and there are at most* 2^r *such calls. Also note that hint* h_i *is a vector of* $2^r \cdot \alpha_{r-1} \cdot \mathsf{sum}_m(1)$ *entries of independent from* $\mathcal{C}_{\varepsilon'}$.

Thus to emulate this step, the samples in h_i *for these samples needed by* Noise.

- *If* A *aborts at this step, output* 1 *(i.e., abort at round* i*). Otherwise, output* 0 *(i.e., continue to next round).*

By construction, A's view in the above emulation has the same distribution as in the execution of Protocol 3.1, condition on $\mathcal{E} = \varepsilon'$. Recall that the bias of B for a binomial game $\mathsf{G} = \mathsf{G}_{m,\varepsilon',f}$ is defined by $\mathsf{Bias}_{\mathsf{B}}(\mathsf{G}) = \mathrm{E}\left[\left|O_I - O_I^-\right|\right]$, where I is the aborting round of B (m+1 if no abort occurred), $O_i = \delta_i(S_{i-1}, H_i)$, and $O_i^- = \delta_i(S_{i-1})$ for $i \in [m]$, and for $i = m+1$ it holds that $O_{m+1} = O_{m+1}^-$. Also recall that S_j is the sum of coins tossed up to round j, $\delta_i(s_{i-1})$ is the expected outcome of the binomial game given $S_{i-1} = s_{i-1}$, and $\delta_i(s_{i-1}, h_i)$ is the expected outcome of the binomial game given $S_{i-1} = s_{i-1}$ and the hint in round i is h_i. By above notations, and since $O_{m+1} = O_{m+1}^-$, we can write: $\mathsf{Bias}_{\mathsf{B}}(\mathsf{G}) = |\mathrm{E}\left[\delta_I(S_{I-1}) - \delta_I(S_{I-1}, H_I) \;\mid\; I \neq m+1\right]| \cdot \Pr\left[I \neq m+1\right]$. By construction, $\mathsf{val}(V_I) = \delta_I(S_{I-1})$, $\mathsf{val}(V_I^-) = \delta_I(S_{I-1}, H_I)$, and $T = 3b$ if and only if $I \neq m+1$. It follows that $\mathsf{Bias}_{m,\varepsilon',f}(\mathsf{B}) = \left|\mathrm{E}\left[\mathsf{val}(V_I) - \mathsf{val}(V_I^-) \;\mid\; \mathcal{E} = \varepsilon', T = 3b\right]\right| \cdot \Pr\left[T = 3b \mid \mathcal{E} = \varepsilon'\right] = \beta$. Since $\mathsf{Bias}(\mathsf{G}) = \max_{\mathsf{B}}\{\mathsf{Bias}_{\mathsf{B}}(\mathsf{G})\}$, we conclude that $\beta \leq \mathsf{Bias}(\mathsf{G})$. □

Proving Claim 3.26.

Proof of Claim 3.26. This proof follows the same line as the proof of Claim 3.25, so we omit several details. Starting as in the proof of Claim 3.25, we assume toward contradiction that:

$$\left|\mathrm{E}\left[\mathsf{val}(V_I) - \mathsf{val}(V_I^-) \;\mid T = 1a, |P| \leq \tau\right]\right| \cdot \Pr\left[T = 1a \mid |P| \leq \tau\right] = \Omega\left(\frac{2^t \cdot \sqrt{\log m}}{m^{1/2+1/(2^{t-1}-2)}}\right) \tag{26}$$

Let Δ_{def} be the δ parameter passed to the last call to $\widetilde{\mathsf{Defense}}^{\mathsf{HT}}$, and let $\mathcal{E} = \widehat{\mathcal{C}}^{-1}_{\mathsf{sum}_m(1)}(\Delta_{\mathsf{def}})$ (i.e., $\mathcal{E}$ is the last ε calculated in Step 1 of $\widetilde{\mathsf{Defense}}^{\mathsf{HT}}$). Note that the Π^{HT} can be thought as a majority protocol of $\mathcal{E}$-biased coins. As in the proof of Claim 3.25, it is guaranteed that there exists $\varepsilon' \in \mathrm{Supp}(\mathcal{E})$, and $p' \in \mathrm{Supp}(P)$, $-\tau \leq p' \leq \tau$, for which:

$$\left|\mathrm{E}\left[\mathsf{val}(V_I) - \mathsf{val}(V_I^-) \;\mid\; T = 1a, \mathcal{E} = \varepsilon', P = p'\right]\right| \cdot \Pr\left[T = 1a \mid \mathcal{E} = \varepsilon', P = p'\right] = \Omega\left(\frac{2^t \cdot \sqrt{\log m}}{m^{1/2+1/(2^{\ell-1}-2)}}\right) \tag{27}$$

Let $\tilde{r}_{\mathsf{A}}$, and $\tilde{r}_h$ be a possible randomness' values such that when adversary A uses $\tilde{r}_{\mathsf{A}}$, and the honest party uses $\tilde{r}_h$, the protocol reaches Π_m^{HT} with $\mathcal{E} = \varepsilon'$, and $P = p'$. Let $\beta = \left|\mathrm{E}\left[\mathsf{val}(V_I) - \mathsf{val}(V_I^-) \;\mid\; T = 1a, \mathcal{E} = \varepsilon', P = p'\right]\right| \cdot \Pr\left[T = 1a \mid \mathcal{E} = \varepsilon', P = p'\right]$, the gain of the adversary A, conditioned on $\mathcal{E} = \varepsilon'$, and $P = p'$.

Let $f = f^{\mathsf{hyp}}_{m,p'}$ be according to Definition 3.20, let $\mathsf{G} = \mathsf{G}_{m,\varepsilon',f}$ be a binomial game with hypergeometric hint according to *Definition* 3.16, and let Bias be according to Definition 3.17. In the following, we show that $\beta \leq \mathsf{Bias}(\mathsf{G})$. Assuming that, by Lemma 3.21, we get that

$$\beta \leq \mathsf{Bias}(\mathsf{G}) \leq O(\frac{\sqrt{\log m}}{m}) = O\left(\frac{2^t \cdot \sqrt{\log m}}{m^{1/2+1/(2^{\ell-1}-2)}}\right)$$

Contradicting Equation (27).

As in the proof for Claim 3.25, to show that $\beta \leq \mathsf{Bias}(\mathsf{G})$, we define a player B for the game G, that achieves bias β.

Algorithm 3.29 (Player B)**.**

Operation:

1. *Start emulating an execution of protocol* $\widehat{\Pi}^t_m(1^\ell)$*, with* A *controlling parties* $\mathsf{P}_1, \ldots, \mathsf{P}_{t-1}$*, where* A *uses randomness* $\tilde{r}_{\mathsf{A}}$ *, and the honest party* P_t *uses randomness* $\tilde{r}_h$ *until the main loop of* Π^{HT}_m *is reached. (If not reached,* B *never aborts.) From that point, continue the execution randomly using fresh new randomness.*

2. *For* $i = 1$ *to* m*:*

   (a) *Let* (s_{i-1}, h_i) *be the* i*'th message sent by the challenger.*

   (b) *If* $i > 1$*, emulate Step 1b: let* $c_{i-1} = s_i - s_{i-1}$ *and set* $c^{\#1}_{i-1}$ *such that* $c_{i-1} = c^{\#1}_{i-1} \oplus c^{\#2}_{i-1}$*. Emulate the reconstruction of* c_{i-1}*, letting* $c^{\#2}_{i-1}$ *be the message of the honest party.*

   (c) *Emulate Step 1a: emulate the call to* $\mathsf{RoundDefense}^{\mathsf{HT}}$ *by sending* h_i *to party* P_1*.*

   - *If* A *aborts at this step, output* 1 *(i.e., abort at round* i*). Otherwise, output* 0 *(i.e., continue to next round).*

By construction of strategy B, A's view in the above emulation has the same distribution as in his view in the execution of Protocol 3.8, condition on $\mathcal{E} = \varepsilon'$, and on $P = p'$. Using the very same argument that was use at the end of the proof of Claim 3.25 we conclude that $\mathsf{Bias}_{m,\varepsilon',f}(\mathsf{B}) = \beta$. Since $\mathsf{Bias}(\mathsf{G}) = \max_{\mathsf{B}}\{\mathsf{Bias}_{\mathsf{B}}(\mathsf{G})\}$, we conclude that $\beta \leq \mathsf{Bias}(\mathsf{G})$. □

3.3 Proof of Main Theorem

In this section we prove our main result: the existence of an $O(m)$-round, t-party coin-flipping protocol, in the real (non-hybrid) model, that is $O(\frac{t^4 \cdot 2^t \cdot \sqrt{\log m}}{m^{1/2+1/(2^{t-1}-2)}})$-fair.

Theorem 3.30 (Main theorem — many-party, fair coin flipping)**.** *Assuming protocols for securely computing* OT *exist, then for any polynomially bounded, polynomial-time computable, integer functions* $m = m(\kappa)$ *and* $t = t(\kappa) \leq \frac{1}{2}\log\log m$*, there exists a* t*-party,* m*-round,* $O(\frac{t^4 \cdot 2^t \cdot \sqrt{\log m}}{m^{1/2+1/(2^{t-1}-2)}})$*-fair, coin-flipping protocol.*

Proof of Theorem 3.30. We compile our hybrid protocol defined in Section 3.1 into the desired real-world protocol. The main part of the proof is showing how to modify the $O(m't')$-round, t'-party hybrid protocol $\widehat{\Pi}^{t'}_{m'}$ (see Protocol 3.1), for arbitrary integers m' and t', into a form that allows

this compilation. This modification involves several steps, all using standard techniques. In the following we fix m' and t', and let $\widehat{\Pi} = \widehat{\Pi}^{t'}_{m'}$.

First modification is that $\widehat{\Pi}$ (through protocol Π) uses real numbers. Specifically, the parties keep the value of δ, which is a real number in $[0,1]$, and also keep shares for such values. We note that the value of δ is always set to the probability that when sampling some k ε-biased $\{-1,1\}$-coins, the bias is at least $b \in \mathbb{Z}$. Where in turn, ε is the value such that the sum of n ε-biased coins, is positive with probability δ', for some δ' whose value is already held by the parties. It follows that δ has short description given the value of δ' (i.e., the values of k and b), and thus all δ have short descriptions.

Second modification is to modify the functionalities used by the protocol as oracles into ones that are polynomial-time computable in m' and $2^{t'}$, without hurting the security of the protocol. By inspection, the only calculation that need to be treated is the calculations done in Step 1 of Coin, Step 1 in Noise, and Step 1 in $\widetilde{\mathsf{Defense}}^{\mathsf{HT}}$. To be concrete, we focus on the calculation of $\varepsilon = \widehat{\mathcal{C}}^{-1}_{\mathsf{sum}_m(1)}(\delta)$ for some $\delta \in [0,1]$ done in Coin. Via sampling, for any $p \in \text{poly}$, one can efficiently estimate ε by a value $\widetilde{\varepsilon}$ such that $|\varepsilon - \widetilde{\varepsilon}| \leq \frac{1}{p(m)}$ with save but negligible probability in m. Since ε is merely used for sampling $q(m) \in \text{poly}$ ε-bias $\{-1,1\}$ coins, it follows that statistical distance between the parties' views in random execution of $\widehat{\Pi}^t_m$ and the efficient variant of $\widehat{\Pi}^t_m$ that uses the above estimation, is at most $\frac{q(m)}{p(m)} + \text{neg}(m)$ which is in $O(1/m)$ for large enough p. It follows that Theorem 3.11 also holds with respect to the above efficient implementation of Coin.

Next modification is to make all the oracles call made by the parties to be sequential (i.e., one after the other). To do that we merely replace the parallel calls to $\mathsf{Defense}$ done in Step 1 and Step 3b of Protocol 3.2, with a single call per step. This done by modifying $\mathsf{Defense}$ to get as input the inputs provided by the parties for *all* parallel calls, compute the answer of each of this calls, and return the answers in an aggregated manner to the parties. Since our hybrid model dictates that a single abort in one of the parallel calls to $\mathsf{Defense}$ aborts all calls, it is clear that this change does not effect the correctness and security of protocol $\widehat{\Pi}$.

Last modification it to make the protocol secure against arbitrary adversaries (not only fail-stop ones). Using information-theoretic one-time message authentication codes (cf., [43]), the functionalities Coin, $\mathsf{Defense}$ and protocol $\widehat{\Pi}$ can be compiled into functionalities and protocol that maintain the same correctness, essentially the same efficiency, and the resulting protocol is $(\gamma + \text{neg}(m'))$-fair against *arbitrary* adversaries, assuming the protocol γ-fair against fail-stop adversaries.

Then next step is to define an hybrid-model protocol whose characteristic are functions of the security parameter κ. Let $\widetilde{m} = \widetilde{m}(\kappa) = \lceil m(\kappa)/c \cdot t(\kappa)^3 \rceil - a$, for $c > 0$ to be determined by the analysis, and $a \in \{0, \ldots, 11\}$ is the value such that $\widetilde{m}(\kappa) - a \equiv 1 \bmod 12$.[20] Consider the $O(t \cdot \widetilde{m})$-round, t-party, polynomial-time protocol $\widetilde{\Pi}$ in the $(\mathsf{Coin}, \mathsf{Defense})$-hybrid-model, that on input κ, the parties act as in $\widehat{\Pi}^t_{\widetilde{m}}(1^t)$. Theorem 3.11 and the above observations yields the $\widetilde{\Pi}$ is a $\gamma(\kappa) := \left(O\left(\frac{t \cdot 2^t \cdot \sqrt{\log \widetilde{m}}}{\widetilde{m}^{1/2+1/(2^{t-1}-2)}} \right) = O\left(\frac{t^4 \cdot 2^t \cdot \sqrt{\log m}}{m^{1/2+1/(2^{t-1}-2)}} \right) \right)$-fair in the $(\mathsf{Defense}, \mathsf{Coin})$-hybrid model.

Note that $\widetilde{\Pi}$ makes sequential calls to the oracles, and that since $t(\kappa) \leq \frac{1}{2} \log \log m$, protocol $\widetilde{\Pi}$ runs in polynomial time.

We are finally able to present the real model protocol. Assuming protocols for securely computing OT exist, there exists (see Fact 2.17) an $O(t^3 \widetilde{m} + t \cdot \widetilde{m})$-round, t-party, polynomial-time protocol $\breve{\Pi}$ correct coin-flipping protocol, that is $(\gamma(\kappa) + \text{neg}(\kappa))$-fair in the *standard model*. By

[20] Note that the total number of coins, $\frac{\widetilde{m}(\widetilde{m}+1)(2\widetilde{m}+1)}{6}$, is odd for $\widetilde{m} \equiv 1 \bmod 12$.

choosing c in the definition of $\widetilde{m}$ large enough, we have that the protocol has (at most) m rounds, yielding that $\breve{\Pi}$ is $O\left(\frac{t^4 \cdot 2^t \cdot \sqrt{\log m}}{m^{1/2+1/(2^{t-1}-2)}}\right)$-fair. $\square$

4 Leakage from Two-Step Boolean Processes

In this section we give bounds on the advantage one gains in predicting the outcome of certain types of Boolean random variables, when some information has "leaked". These bounds play a critical role in the analysis of the coin-flipping protocol presented in Section 3. Specifically, they are used to prove Claim 3.24 that bounds the gain from aborting in the first round of Protocol 3.2, and to prove Lemmas 3.19 and 3.21 that bounds the bias of the online binomial games (which, in turn, captures the bias obtained by aborting in the main loop of Protocols 3.2 and 3.8).

The types of random processes and leakage functions considered in this section are given in Section 4.1, where the bounds on the prediction gain for different types of random variables and leakage functions are given in Section 4.2.

4.1 Two-step Processes and Leakage Functions

Two-step Boolean processes are defined in Section 4.1.1 and the leakage functions we care about are defined in Section 4.1.2.[21]

4.1.1 Two-step Boolean Process

A two-step Boolean process is a pair of jointly-distributed random variables (A, B), where A is over an arbitrary domain $\mathcal{A}$ and B is Boolean (i.e., over $\{0, 1\}$). It is instructive to think that the process' first step is choosing A, and its second step is to choose B as a random function of A. Jumping ahead, the leakage functions we considered are limited to be functions of A (i.e., of the process' "state" after its first step). We focus on several types of such Boolean two-step processes.

Binomial process. Recall that $\mathcal{C}_\varepsilon$ is the Bernoulli probability distribution over $\{-1, 1\}$ taking the value 1 with probability $\frac{1}{2} \cdot (1 + \varepsilon)$, and that $\mathcal{C}_{n,\varepsilon}$ is the probability distribution defined by $\mathcal{C}_{n,\varepsilon}(k) = \Pr_{(x_1,\ldots,x_n)\leftarrow(\mathcal{C}_\varepsilon)^n}\left[\sum_{i=1}^n x_i = k\right]$.

Definition 4.1 (Binomial process)**.** *Let $m \in \mathbb{N}$, $i \in [m]$, $\ell\colon \mathbb{N} \mapsto \mathbb{N}$, $b \in \mathbb{Z}$ and $\varepsilon \in [-1, 1]$. An $(m, i, \ell, b, \varepsilon)$-*binomial process *is the two-step Boolean process (A, B) defined by*

1. $A = C_i$.
2. $B = \mathsf{sign}(b + A + \sum_{j=i+1}^m C_j)$,

where C_j, for $j \in \{i, \ldots, m\}$, is an independent random variable sampled according to $\mathcal{C}_{\ell(j),\varepsilon}$.

Namely, in the first step C_i is sampled, and the second step returns one if the value of C_i plus a predetermined value b and the sum $C_{i+1}, \ldots, C_m$ is non-negative. With the proper choice of parameters, the two-step binomial process captures the random process that happens in the execution of Protocols 3.2 and 3.8.

[21] Some of the definitions given below were already given in Section 3, and they recalled below for the reader convenience.

Hypergeometric process. Recall that $\mathcal{B}er(\delta)$ is the Bernoulli probability distribution over $\{0,1\}$ taking the value 1 with probability δ and 0 otherwise, that $\mathcal{HG}_{n,p,\ell}$ is the hyper-geometric probability distribution defined by $\mathcal{HG}_{n,p,\ell}(k) = \Pr_{\mathcal{I}\subset[n],|\mathcal{I}|=\ell}[w(v_{\mathcal{I}}) = k]$, where $v \in \{-1,1\}^n$ is an arbitrary vector with $w(v) = \sum_{i=1}^{n} v_i = p$, and that $\widehat{\mathcal{HG}}_{n,p,\ell}(k) = \Pr_{x\leftarrow\mathcal{HG}_{n,p,\ell}}[x \geq k] = \sum_{t=k}^{\ell} \mathcal{HG}_{n,p,\ell}(t)$. Finally, recall that $\widehat{\mathcal{C}}_{n,\varepsilon}(k) := \Pr_{x\leftarrow\mathcal{C}_{n,\varepsilon}}[x \geq k]$ and that $\widehat{\mathcal{C}}_n^{-1}(\delta)$ is the value $\varepsilon \in [-1,1]$ with $\widehat{\mathcal{C}}_{n,\varepsilon}(0) = \delta$.

Definition 4.2 (Hypergeometric process – Restatement of Definition 3.14)**.** *Let $s, \beta \in \mathbb{N}$ and $\delta \in [0,1]$. An (s,β,δ)-*hypergeometric process *is the two-step Boolean process (A,B) defined by*

1. *$A = \widehat{\mathcal{HG}}_{\beta\cdot s, w(v), s}(0)$, for $v \leftarrow (\mathcal{C}_\varepsilon)^{\beta\cdot s}$ and $\varepsilon = \widehat{\mathcal{C}}_s^{-1}(\delta)$.*
2. *$B \leftarrow \mathcal{B}er(A)$,*

Namely, A is set to the probability that a random s-size subset of this vector contains more ones than zeros, and B is one with probability A. This two-step process captures the random process that happens in Step 1 of Protocol 3.2.

4.1.2 Leakage Functions

A leakage function f for a two-step process (A,B) is simply a randomized function over $\mathrm{Supp}(A)$. We will later consider the advantage in predicting the outcome of B gained from knowing $f(A)$. That is, we will measure the difference between $\mathrm{E}[B]$ and $\mathrm{E}[B \mid f(A) = h]$, for a given "hint" (leakage) $h \in \mathrm{Supp}(f(A))$. In the following we define several such leakage functions. The choice of the second and third leakage functions considered below might seems somewhat arbitrary, but these are the functions one need to consider when analyzing Protocols 3.2 and 3.8.

All-information leakage. The all-information leakage function simply leaks the whole state of the process.

Definition 4.3 (all-information leakage function)**.** *A function f is* an all-information leakage function *for a two-step Boolean process (A,B), if $f(a) = a$ for every $a \in \mathrm{Supp}(A)$.*

Vector leakage.

Definition 4.4 (vector leakage function – Restatement of Definition 3.13)**.** *Let s, α be integers. A randomized function f is a (s,α)-*vector leakage function *for the two-step Boolean process (A,B), if on input $a \in \mathrm{Supp}(A)$, it outputs a vector in $\{-1,1\}^{\alpha\cdot s}$ according to $(\mathcal{C}_\varepsilon)^{\alpha\cdot s}$, for $\varepsilon = \widehat{\mathcal{C}}_s^{-1}(\mathrm{E}[B \mid A = a])$.*

Namely, the probability that the sum of s bits taken from the output of $f(a)$ is positive, is exactly $\Pr[B = 1 \mid A = a]$.

Hypergeometric leakage.

Definition 4.5 (hypergeometric leakage function)**.** *Let $m \in \mathbb{N}$, $i \in [m]$, $\ell\colon \mathbb{N} \mapsto \mathbb{N}$, $b \in \mathbb{Z}$ and $p \in [-2\cdot\hat{\ell}(1), 2\cdot\hat{\ell}(1)]$, for $\hat{\ell}(t) := \sum_{j=t}^{m} \ell(j)$. A randomized function f is a (m,i,ℓ,b,p)-*hypergeometric leakage function *for the two-step process (A,B) with $\mathrm{Supp}(A) \subseteq \mathbb{Z}$, if on input $a \in \mathrm{Supp}(A)$, $f(a) = b + a + t$, for $t \leftarrow \mathcal{HG}_{2\cdot\hat{\ell}(1),p,\hat{\ell}(i+1)}$.*

Namely, an hypergeometric leakage function *masks* the state of the process with an hypergeometric noise.

4.1.3 Prediction Advantage

We will be interested in bounding the difference in the expected outcome of B when $f(A)$ leaks. This change is captured via the notion of prediction advantage.

Definition 4.6 (prediction advantage – Restatement of Definition 3.12)**.** *For a two-step process* $\mathsf{P} = (A, B)$ *and a leakage function* f *for* P*, define the* prediction advantage $\Gamma_{\mathsf{P},f}$ *by* $\Gamma_{\mathsf{P},f}(h) = |\Pr[B = 1] - \Pr[B = 1 \mid f(A) = h]|$.

The goal of the following section is to bound the prediction advantage $\Gamma_{\mathsf{P},f}$ in several processes with leakage functions. The bounds given in this section are used for proving the security of Protocols 3.2 and 3.8.

4.2 Bounding Prediction Advantage

We give bounds on the prediction advantage in several combinations of two-step Boolean processes and leakage functions. The bounds are stated in Section 4.2.1. In Sections 4.2.3, 4.2.4 and 4.2.7 we develop tools for proving such bounds, and the proofs of the stated bounds are given in Sections 4.2.5, 4.2.6, 4.2.8 and 4.2.9. The choice of parameters we considered below are somewhat arbitrary, but these are the parameters needed when analyzing the security of Protocols 3.2 and 3.8.

In the following recall that $\ell_m(i) = (m - i + 1)^2$ and that $\mathsf{sum}_m(i) = \sum_{j=i}^{m} \ell_m(i)$.

4.2.1 The Bounds

Bound on binomial process with all-Information leakage.

Lemma 4.7. *Assume* $m \in \mathbb{N}$*,* $i \in [m]$*,* $b \in \mathbb{Z}$ *and* $\varepsilon \in [-1, 1]$*, satisfy*

1. $|\varepsilon| \leq 4 \cdot \sqrt{\frac{\log m}{\mathsf{sum}_m(1)}}$,
2. $i \in [m - \left\lfloor m^{\frac{1}{8}} \right\rfloor]$*, and*
3. $|b + \varepsilon \cdot \mathsf{sum}_m(i)| \leq 4 \cdot \sqrt{\log m \cdot \mathsf{sum}_m(i)}$.
4. $-(b + 1) \in \mathrm{Supp}(\mathcal{C}_{\mathsf{sum}_m(i),\varepsilon})$.[22]

Let $\mathsf{P} = (A = C_i, B)$ *be an* $\big(m, i, \ell_m, b, \varepsilon\big)$*-binomial process according to Definition 4.1, let* f *be an all-information leakage function for* P *according to Definition 4.3, and let* $\Gamma_{\mathsf{P},f}$ *be according to Definition 4.6. Then, there exists a set* $\mathcal{H} \subseteq \mathrm{Supp}(f(C_i))$ *such that*

1. $\Pr[f(C_i) \notin \mathcal{H}] \leq \frac{1}{m^2}$*, and*

[22] We see b as a valid bias of the first $i - 1$ rounds of our coin flipping protocol, i.e., satisfy the condition that $b + 1$ and $\mathsf{sum}_m(i)$ has the same parity (recall that the first $i - 1$ rounds has $\mathsf{sum}_m(1) - \mathsf{sum}_m(i)$ coins and that $\mathsf{sum}_m(1)$ is odd). By assuming that b is not too large (condition 3), the above is equivalent to condition 4.

2. $\Gamma_{\mathsf{P},f}(h) \leq \lambda \cdot \sqrt{\ell_m(i)} \cdot \sqrt{\log m} \cdot \Pr\left[\sum_{j=i}^{m} C_j = -(b+1)\right]$, *for every* $h \in \mathcal{H}$ *and a universal constant* $\lambda > 0$.

In words, the above lemma (and also the following Lemmas 4.8 and 4.9) states that we can bound the prediction advantage $\Gamma_{\mathsf{P},f}$ for "typicall" leakages, using the value of $\Pr\left[\sum_{j=i}^{m} C_j = -(b+1)\right]$. Jumping ahead, such a bound on binomial process, together with Lemma 5.24 which is the main result of Section 5, is used for analyzing our coin-flipping protocol. See the proofs of Lemma 5.25 and Lemma 5.26 for more details (which are restatements of Lemma 3.19 and Lemma 3.21, respectively).

Bound on binomial process with hypergeometric leakage.

Lemma 4.8. *Assume* $m \in \mathbb{N}$, $i \in [m]$, $b \in \mathbb{Z}$, $\varepsilon \in [-1, 1]$, $\lambda > 0$ *and* $p \in [-2 \cdot \mathsf{sum}_m(1), 2 \cdot \mathsf{sum}_m(1)]$, *satisfy*

1. $|p| \leq \lambda \cdot \sqrt{\log m \cdot \mathsf{sum}_m(1)}$,
2. $|\varepsilon| \leq 4 \cdot \sqrt{\frac{\log m}{\mathsf{sum}_m(1)}}$,
3. $i \in [m - \left\lfloor m^{\frac{1}{8}} \right\rfloor]$, *and*
4. $|b + \varepsilon \cdot \mathsf{sum}_m(i)| \leq 4 \cdot \sqrt{\log m \cdot \mathsf{sum}_m(i)}$.
5. $-(b+1) \in \mathrm{Supp}(\mathcal{C}_{\mathsf{sum}_m(i),\varepsilon})$.

Let $\mathsf{P} = (A = C_i, B)$ *be a* $(m, i, \ell_m, b, \varepsilon)$*-binomial process according to Definition 4.1, let* f *be an* (m, i, ℓ_m, b, p)*-hypergeometric leakage function for* P *according to Definition 4.5, and let* $\Gamma_{\mathsf{P},f}$ *be according to Definition 4.6. Then, there exists a set* $\mathcal{H} \subseteq \mathrm{Supp}(f(C_i))$ *such that*

1. $\Pr[f(C_i) \notin \mathcal{H}] \leq \frac{1}{m^2}$, *and*
2. *for every* $h \in \mathcal{H}$*:*
   (a) $\Pr\left[|C_i| > 7\sqrt{\log m \cdot \ell_m(i)} \mid f(C_i) = h\right] \leq \frac{\gamma}{m^{12}}$, *for a universal constant* $\gamma > 0$.
   (b) $\Gamma_{\mathsf{P},f}(h) \leq \varphi(\lambda) \cdot \sqrt{\log m} \cdot \sqrt{\frac{\ell_m(i)}{m-i+1}} \cdot \Pr\left[\sum_{j=i}^{m} C_j = -(b+1)\right]$, *for a universal function* $\varphi \colon \mathbb{R}^+ \to \mathbb{R}^+$.

Bound on binomial process with vector leakage.

Lemma 4.9. *Assume* $s, \alpha \in \mathbb{N}$, $m \in \mathbb{N}$, $i \in [m]$, $b \in \mathbb{Z}$ *and* $\varepsilon \in [-1, 1]$ *satisfy*

1. $|\varepsilon| \leq 4\sqrt{\frac{\log m}{\mathsf{sum}_m(1)}}$,
2. $i \in [m - \left\lfloor m^{\frac{1}{8}} \right\rfloor]$,
3. $|b + \varepsilon \cdot \mathsf{sum}_m(i)| \leq 4 \cdot \sqrt{\log m \cdot \mathsf{sum}_m(i)}$,
4. $-(b+1) \in \mathrm{Supp}(\mathcal{C}_{\mathsf{sum}_m(i),\varepsilon})$,

5. $s \geq \mathsf{sum}_m(1)$, *and*

6. $\sqrt{\frac{\alpha}{m-i}} \cdot \log m \leq \frac{1}{100}$,

Let $\mathsf{P} = (A = C_i, B)$ *be a* $\big(m, i, \ell_m, b, \varepsilon\big)$*-binomial process according to Definition 4.1, let* f *be an* $\big(s, \alpha\big)$*-vector leakage function for* P *according to Definition 4.4, and let* $\Gamma_{\mathsf{P},f}$ *be according to Definition 4.6. Then, there exists a set* $\mathcal{H} \subseteq \mathrm{Supp}(f(C_i))$ *such that*

1. $\Pr\left[f(C_i) \notin \mathcal{H}\right] \leq \frac{1}{m^2}$, *and*

2. *for every* $h \in \mathcal{H}$,

   (a) $\Pr\left[|C_i| > 7\sqrt{\log m \cdot \ell_m(i)} \mid f(C_i) = h\right] \leq \frac{\gamma}{m^{12}}$, *for a universal constant* $\gamma > 0$.

   (b) $\Gamma_{\mathsf{P},f}(h) \leq \lambda \cdot \sqrt{\log m \cdot \alpha} \cdot \sqrt{\frac{\ell_m(i)}{m-i+1}} \cdot \Pr\left[\sum_{j=i}^{m} C_j = -(b+1)\right]$, *for a universal constant* $\lambda > 0$.

Bound on hypergeometric process with vector leakage.

Lemma 4.10. *Assume* $s, \alpha, \beta \in \mathbb{N}$ *and* $\delta \in [0,1]$, *satisfy*

1. $2 \leq \alpha < \beta \leq s$,

2. $\frac{\alpha+\sqrt{s}}{s} \cdot \log^2 s \leq 10^{-5} \cdot \sqrt{\frac{\alpha}{\beta}}$, *and*

3. $\sqrt{\frac{\alpha}{\beta}} \cdot \log s \leq \frac{1}{100}$.

Let $\mathsf{P} = (A, B)$ *be a* $\big(s, \beta, \delta\big)$*-hypergeometric process according to Definition 4.2 , let* f *be an* $\big(s, \alpha\big)$*-vector leakage function for* P *according to Definition 4.4, and let* $\Gamma_{\mathsf{P},f}$ *be according to Definition 4.6. Then, there exists a universal constant* $\lambda > 0$ *such that*

$$\Pr_{h \leftarrow f(A)}\left[\Gamma_{\mathsf{P},f}(h) > \lambda \cdot \sqrt{\log s} \cdot \frac{\sqrt{\alpha}}{\beta}\right] \leq \frac{1}{s^2}.$$

4.2.2 Data Processing on the Leakage

The following proposition shows that given access to a (randomize) function of the leakage cannot improve the prediction quality.

Proposition 4.11. *Let* $\mathsf{P} = (A, B)$ *be a two-step process and let* f *and* f' *be two leakage functions for* P. *Assume there exists randomize function* g *over the range of* f *such that* $f'(a) = f(a) \circ g(f(a))$ *for every* $a \in \mathrm{Supp}(A)$, *where the randomness of* g *is independent of* f *and* P. *Then, for every* $\gamma \in [0,1]$, *it holds that*

$$\Pr_{h \leftarrow f(A)}\left[\Gamma_{\mathsf{P},f}(h) > \gamma\right] = \Pr_{h' \leftarrow f'(A)}\left[\Gamma_{\mathsf{P},f'}(h') > \gamma\right].$$

Proof. Let $\gamma \in [0,1]$. Compute

$$\begin{aligned}
\Pr_{h' \leftarrow f'(A)}\left[\Gamma_{\mathsf{P},f'}(h') > \gamma\right] &= \Pr_{h \leftarrow f(A), h'' \leftarrow g(h)}\left[\Gamma_{\mathsf{P},f'}(h \circ h'') > \gamma\right] \\
&= \Pr_{h \leftarrow f(A), h'' \leftarrow g(h)}\left[\left|\Pr\left[B=1\right] - \Pr\left[B=1 \mid f'(A) = h \circ h''\right]\right| > \gamma\right] \\
&= \Pr_{h \leftarrow f(A), h'' \leftarrow g(h)}\left[\left|\Pr\left[B=1\right] - \Pr\left[B=1 \mid f(A) = h, g(h) = h''\right]\right| > \gamma\right] \\
&= \Pr_{h \leftarrow f(A)}\left[\left|\Pr\left[B=1\right] - \Pr\left[B=1 \mid f(A) = h\right]\right| > \gamma\right] \\
&= \Pr_{h \leftarrow f(A)}\left[\Gamma_{\mathsf{P},f}(h) > \gamma\right].
\end{aligned} \tag{28}$$

The penultimate equation holds since $\Pr\left[B=1 \mid f(A)=h, g(h)=h''\right] = \Pr\left[B=1 \mid f(A)=h\right]$. □

4.2.3 Expressing Prediction Advantage using Ratio

In this section we develop a general tool for bounding the prediction advantage $\Gamma_{\mathsf{P},f}$ of a process $\mathsf{P} = (A,B)$ with leakage function f. Informally, we reduce the task of bounding the prediction advantage into evaluating the "ratio" of P with f, where ratio (defined below) is a useful measurement on how much the distribution of A changes when $f(A)$ is given.

Definition 4.12. *Let $\mathsf{P} = (A,B)$ be a two-step process and let f be a leakage function for P. For $h \in \mathrm{Supp}(f(A))$, $\mathcal{A}^* \subseteq \mathrm{Supp}(A)$ and $a \in \mathcal{A}^*$, define*

$$\mathsf{ratio}_{h,\mathcal{A}^*}(a) = \frac{\Pr\left[A=a \mid f(A)=h, A \in \mathcal{A}^*\right]}{\Pr\left[A=a \mid A \in \mathcal{A}^*\right]}$$

Namely, $\mathsf{ratio}_{h,\mathcal{A}^*}(a)$ measures the change (in multiplicative term) of the probability that $A=a$, due to the knowledge of h, assuming that A is in some "typical" set (i.e., $A \in \mathcal{A}^*$).

An alternative and equivalent definition of ratio is stated below.

Definition 4.13. *Let $\mathsf{P} = (A,B)$ be a two-step process and let f be a leakage function for P. For $h \in \mathrm{Supp}(f(A))$, $\mathcal{A}^* \subseteq \mathrm{Supp}(A)$ and $a \in \mathcal{A}^*$, define*

$$\mathsf{ratio}_{h,\mathcal{A}^*}(a) = \frac{\Pr\left[f(A)=h \mid A=a\right]}{\Pr\left[f(A)=h \mid A \in \mathcal{A}^*\right]}$$

As the next claim states, the above two definitions of ratio are indeed equivalent.

Claim 4.14. *Definitions 4.12 and 4.13 are equivalent.*

Proof. Let $\mathsf{ratio}_{h,\mathcal{A}^*}(a)$ be according to Definition 4.13. A simple calculation yields that

$$\begin{aligned}
\mathsf{ratio}_{h,\mathcal{A}^*}(a) &= \frac{\Pr\left[f(A)=h \mid A=a\right]}{\Pr\left[f(A)=h \mid A \in \mathcal{A}^*\right]} \\
&= \frac{\Pr\left[A=a \mid f(A)=h\right]}{\Pr\left[A=a\right]} \cdot \frac{\Pr\left[A \in \mathcal{A}^*\right]}{\Pr\left[A \in \mathcal{A}^* \mid f(A)=h\right]}
\end{aligned} \tag{29}$$

Since $a \in \mathcal{A}^*$, it follows that

$$\Pr\left[A=a \mid A \in \mathcal{A}^*\right] = \frac{\Pr\left[A=a\right]}{\Pr\left[A \in \mathcal{A}^*\right]} \tag{30}$$

and

$$\Pr\left[A = a \mid A \in \mathcal{A}^*, f(A) = h\right] = \frac{\Pr\left[A = a \mid f(A) = h\right]}{\Pr\left[A \in \mathcal{A}^* \mid f(A) = h\right]} \tag{31}$$

We conclude that

$$\mathsf{ratio}_{h,\mathcal{A}^*}(a) = \frac{\Pr\left[A = a \mid A \in \mathcal{A}^*\right]}{\Pr\left[A = a \mid A \in \mathcal{A}^*, f(A) = h\right]},$$

as required. □

The following lemma allows us to bound the prediction advantage $\Gamma_{\mathsf{P},f}$ of a process P with a leakage function f, using its *ratio* and a "small" additive term.

Lemma 4.15. *Let $\mathsf{P} = (A, B)$ be a two-step process and let f be a leakage function for P. Then, for every $h \in \mathrm{Supp}(f(A))$ and $\mathcal{A}^* \subseteq \mathrm{Supp}(A)$, it holds that*

$$\Gamma_{\mathsf{P},f}(h) \leq \mathop{\mathrm{E}}_{a \leftarrow A \mid a \in \mathcal{A}^*}\left[\left|\Pr\left[B = 1\right] - \Pr\left[B = 1 \mid A = a\right]\right| \cdot \left|1 - \mathsf{ratio}_{h,\mathcal{A}^*}(a)\right|\right] + \mathsf{tail}_{h,\mathcal{A}^*},$$

for $\mathsf{tail}_{h,\mathcal{A}^*} = 2 \cdot \left(\Pr\left[a \notin \mathcal{A}^*\right] + \Pr\left[a \notin \mathcal{A}^* \mid f(A) = h\right]\right)$.

Proof. Let $p = \Pr[A \in \mathcal{A}^*]$, let $q = 1 - p$, let $p_h = \Pr[A \in \mathcal{A}^* \mid f(A) = h]$, let $q_h = 1 - p_h$, let $p' = \Pr[B = 1 \mid A \notin \mathcal{A}^*]$ and let $p'' = \Pr[B = 1 \mid f(A) = h, a \notin \mathcal{A}^*]$. Note that

$$\begin{aligned}
&\Pr[B = 1] \\
&= p \cdot \Pr[B = 1 \mid A \in \mathcal{A}^*] + q \cdot \Pr[B = 1 \mid A \notin \mathcal{A}^*] \\
&= p \cdot \mathop{\mathrm{E}}_{a \leftarrow A \mid a \in \mathcal{A}^*}[\Pr[B = 1 \mid A = a]] + q \cdot p' \\
&= p \cdot \mathop{\mathrm{E}}_{a \leftarrow A \mid a \in \mathcal{A}^*}[\Pr[B = 1 \mid A = a]] + q \cdot p' \\
&= p_h \cdot \mathop{\mathrm{E}}_{a \leftarrow A \mid a \in \mathcal{A}^*}[\Pr[B = 1 \mid A = a]] + (p - p_h) \cdot \mathop{\mathrm{E}}_{a \leftarrow A \mid a \in \mathcal{A}^*}[\Pr[B = 1 \mid A = a]] + q \cdot p'.
\end{aligned} \tag{32}$$

In addition, note that

$$\begin{aligned}
&\Pr[B = 1 \mid f(A) = h] \\
&= p_h \cdot \Pr[B = 1 \mid f(A) = h, a \in \mathcal{A}^*] + q_h \cdot \Pr[B = 1 \mid f(A) = h, a \notin \mathcal{A}^*] \\
&= p_h \cdot \frac{\Pr[B = 1 \wedge f(A) = h \mid a \in \mathcal{A}^*]}{\Pr[f(A) = h \mid a \in \mathcal{A}^*]} + q_h \cdot p'' \\
&= p_h \cdot \frac{\mathrm{E}_{a \leftarrow A \mid a \in \mathcal{A}^*}\left[\Pr[B = 1 \wedge f(A) = h \mid A = a]\right]}{\Pr[f(A) = h \mid a \in \mathcal{A}^*]} + q_h \cdot p'' \\
&= p_h \cdot \frac{\mathrm{E}_{a \leftarrow A \mid a \in \mathcal{A}^*}\left[\Pr[B = 1 \mid A = a] \cdot \Pr[f(A) = h \mid A = a]\right]}{\Pr[f(A) = h \mid a \in \mathcal{A}^*]} + q_h \cdot p'' \\
&= p_h \cdot \mathop{\mathrm{E}}_{a \leftarrow A \mid a \in \mathcal{A}^*}\left[\Pr[B = 1 \mid A = a] \cdot \frac{\Pr[f(A) = h \mid A = a]}{\Pr[f(A) = h \mid a \in \mathcal{A}^*]}\right] + q_h \cdot p'' \\
&= p_h \cdot \mathop{\mathrm{E}}_{a \leftarrow A \mid a \in \mathcal{A}^*}\left[\Pr[B = 1 \mid A = a] \cdot \mathsf{ratio}_{h,\mathcal{A}^*}(a)\right] + q_h \cdot p''.
\end{aligned} \tag{33}$$

Combing Equations (32) and (33) yields that

$$\begin{aligned}
\Gamma_{\mathsf{P},f}(h) &= |\Pr[B=1] - \Pr[B=1 \mid f(A)=h]| \\
&\le p_h \cdot \left| \mathop{\mathrm{E}}_{a \leftarrow A | a \in \mathcal{A}^*} [\Pr[B=1 \mid A=a] \cdot (1 - \mathsf{ratio}_{h,\mathcal{A}^*}(a))] \right| + |p - p_h| + q + q_h \\
&= p_h \cdot \left| \mathop{\mathrm{E}}_{a \leftarrow A | a \in \mathcal{A}^*} [(\Pr[B=1 \mid A=a] - \Pr[B=1]) \cdot (1 - \mathsf{ratio}_{h,\mathcal{A}^*}(a))] \right| + |p - p_h| + q + q_h \\
&\le \left| \mathop{\mathrm{E}}_{a \leftarrow A | a \in \mathcal{A}^*} [(\Pr[B=1 \mid A=a] - \Pr[B=1]) \cdot (1 - \mathsf{ratio}_{h,\mathcal{A}^*}(a))] \right| + |q - q_h| + q + q_h \\
&\le \mathop{\mathrm{E}}_{a \leftarrow A | a \in \mathcal{A}^*} [|\Pr[B=1 \mid A=a] - \Pr[B=1]| \cdot |1 - \mathsf{ratio}_{h,\mathcal{A}^*}(a)|] + 2 \cdot (q + q_h).
\end{aligned}$$

The second equality holds by the following calculation

$$\begin{aligned}
&\mathop{\mathrm{E}}_{a \leftarrow A | a \in \mathcal{A}^*} [\Pr[B=1 \mid A=a] \cdot (1 - \mathsf{ratio}_{h,\mathcal{A}^*}(a))] \\
&= \left| \mathop{\mathrm{E}}_{a \leftarrow A | a \in \mathcal{A}^*} [(\Pr[B=1] + \Pr[B=1 \mid A=a] - \Pr[B=1]) \cdot (1 - \mathsf{ratio}_{h,\mathcal{A}^*}(a))] \right| \\
&= \mathop{\mathrm{E}}_{a \leftarrow A | a \in \mathcal{A}^*} [\Pr[B=1] \cdot (1 - \mathsf{ratio}_{h,\mathcal{A}^*}(a))] + \mathop{\mathrm{E}}_{a \leftarrow A | a \in \mathcal{A}^*} [(\Pr[B=1 \mid A=a] - \Pr[B=1]) \cdot (1 - \mathsf{ratio}_{h,\mathcal{A}^*}(a))] \\
&= \Pr[B=1] \cdot (1 - \mathop{\mathrm{E}}_{a \leftarrow A | a \in \mathcal{A}^*} [\mathsf{ratio}_{h,\mathcal{A}^*}(a)]) + \mathop{\mathrm{E}}_{a \leftarrow A | a \in \mathcal{A}^*} [(\Pr[B=1 \mid A=a] - \Pr[B=1]) \cdot (1 - \mathsf{ratio}_{h,\mathcal{A}^*}(a))] \\
&= \mathop{\mathrm{E}}_{a \leftarrow A | a \in \mathcal{A}^*} [\Pr[B=1] \cdot (1-1)] + \mathop{\mathrm{E}}_{a \leftarrow A | a \in \mathcal{A}^*} [(\Pr[B=1 \mid A=a] - \Pr[B=1]) \cdot (1 - \mathsf{ratio}_{h,\mathcal{A}^*}(a))] \\
&= \mathop{\mathrm{E}}_{a \leftarrow A | a \in \mathcal{A}^*} [(\Pr[B=1 \mid A=a] - \Pr[B=1]) \cdot (1 - \mathsf{ratio}_{h,\mathcal{A}^*}(a))] .
\end{aligned}$$

□

4.2.4 Bounding Prediction Advantage for Binomial Processes

In this section we develop tools for bounding the prediction advantage $\Gamma_{\mathsf{P},f}$ of a binomial process P with respect to an arbitrary leakage f. In Sections 4.2.5, 4.2.6 and 4.2.8, we use these tools to bound the prediction advantage of binomial process with respect to specific leakage functions.

The following lemma, proven in Section 4.2.4, is our first tool for bounding the prediction advantage of a binomial process $(A = C_i, B)$ with arbitrary leakage. The lemma uses ratio, defined in Definition 4.13, and states that an appropriate upper-bound on $|1 - \mathsf{ratio}|$ yields an upper-bound on the prediction advantage. This tool is used in Sections 4.2.6 and 4.2.8 for bounding the prediction advantage with hypergeometric and vector leakage, respectively.

Lemma 4.16. *Let $m \in \mathbb{N}$, $i \in [m]$, $b \in \mathbb{Z}$ and $\varepsilon \in [-1, 1]$ and assume that $i \in [m - \left\lfloor m^{\frac{1}{8}} \right\rfloor]$, that $|\varepsilon| \le 4 \cdot \sqrt{\frac{\log m}{\mathsf{sum}_m(1)}}$, that $-(b+1) \in \mathrm{Supp}(\sum_{j=i}^{m} C_j)$ and that $|b + \varepsilon \cdot \mathsf{sum}_m(i)| \le 4\sqrt{\log m \cdot \mathsf{sum}_m(i)}$. Let $\mathsf{P} = (C_i, B)$ be a $(m, i, \ell_m, b, \varepsilon)$-binomial process according to Definition 4.1, let f be a leakage function for P, let $\Gamma_{\mathsf{P},f}$ be according to Definition 4.6 and let $\mathcal{C}_i^* := \{c \in \mathrm{Supp}(C_i) \mid |\sigma(c)| \le 6 \cdot \sqrt{\log m \cdot \ell_m(i)}\}$ for $\sigma(c) := c - \mathrm{E}_{c' \leftarrow C_i}[c'] = c - \varepsilon \cdot \ell_m(i)$. Let $h \in \mathrm{Supp}(f(C_i))$ be such that*

1. $\Pr[C_i \notin \mathcal{C}_i^* \mid f(C_i) = h] \le \frac{1}{m^{12}}$, *and*

2. $|1 - \mathsf{ratio}_h(c)| \leq \gamma \cdot \frac{|\sigma(c)| + \sqrt{\ell_m(i)}}{\sqrt{\mathsf{sum}_m(i)}}$ *for every* $c \in \mathcal{C}_i^*$

for $\mathsf{ratio}_h = \mathsf{ratio}_{h,\mathcal{C}_i^*}$ *being according to Definition 4.13. Then*

$$\Gamma_{\mathsf{P},f}(h) \leq \lambda \cdot (\gamma + 1) \cdot \sqrt{\frac{\ell_m(i)}{m - i + 1}} \cdot \Pr\left[\sum_{j=i}^{m} C_j = -(b+1)\right]$$

for a universal constant $\lambda > 0$.

Namely, in order to bound the prediction advantage, it is enough to bound the value of $|1 - \mathsf{ratio}|$ for the set of "typical" coins $\mathcal{C}_i^*$.

The next lemma, proven in Section 4.2.4, is our second tool for bounding the prediction advantage of a binomial process $(A = C_i, B)$. This tool is used directly in Section 4.2.5 for bounding the prediction advantage with all-information leakage and is one of the main building blocks for proving Lemma 4.16.

Lemma 4.17. *Let* $m \in \mathbb{N}$, $i \in [m]$, $b \in \mathbb{Z}$ *and* $\varepsilon \in [-1, 1]$ *and assume that* $i \in [m - \lfloor m^{\frac{1}{8}} \rfloor]$, *that* $|\varepsilon| \leq 4 \cdot \sqrt{\frac{\log m}{\mathsf{sum}_m(1)}}$, *that* $-(b+1) \in \mathrm{Supp}(\sum_{j=i}^{m} C_j)$ *and that* $|b + \varepsilon \cdot \mathsf{sum}_m(i)| \leq 4 \cdot \sqrt{\log m \cdot \mathsf{sum}_m(i)}$. *Let* $\mathsf{P} = (C_i, B)$ *be a* $(m, i, \ell_m, b, \varepsilon)$*-binomial process according to Definition 4.1 and let* $\mathcal{C}_i^*$ *and* σ *be as defined in Lemma 4.16. Then, for every* $c \in \mathcal{C}_i^*$ *it holds that*

$$|\Pr[B = 1] - \Pr[B = 1 \mid C_i = c]| \leq \lambda \cdot \left(|\sigma(c)| + \sqrt{\ell_m(i)}\right) \cdot \Pr\left[\sum_{j=i}^{m} C_j = -(b+1)\right]$$

for a universal constant $\lambda > 0$.

Namely, the above lemma bounds the expectation change of B, given a "typical" value for C_i.

Proving Lemma 4.16.

Proof of Lemma 4.16. In the following we assume without loss of generality that m is larger than a universal constant determined by the proof (otherwise, the proof is trivially holds by choosing large enough λ). Assume $h \in \mathrm{Supp}(f(C_i))$ satisfies assumptions 1 and 2 of Lemma 4.16. Since $|b + \varepsilon \cdot \mathsf{sum}_m(i)| \leq 4\sqrt{\log m \cdot \mathsf{sum}_m(i)}$, Proposition 2.2 yields that

$$\begin{aligned} \Pr\left[\sum_{j=i}^{m} C_j = -(b+1)\right] &\geq \frac{1}{\sqrt{\mathsf{sum}_m(i)}} \cdot e^{-\frac{(b+1+\varepsilon \cdot \mathsf{sum}_m(i))^2}{2 \cdot \mathsf{sum}_m(i)}} \\ &\geq \frac{1}{m^{10}} \end{aligned} \tag{34}$$

Therefore, by Hoeffding's inequality (Fact 2.1) and assumption 1 on h, it holds that

$$\frac{2(\Pr[C_i \notin \mathcal{C}_i^*] + \Pr[C_i \notin \mathcal{C}_i^* \mid f(A) = h])}{\Pr\left[\sum_{j=i}^{m} C_j = -(b+1)\right]} \leq \frac{\frac{4}{m^{12}}}{\frac{1}{m^{10}}} = \frac{4}{m^2} \tag{35}$$

It follows that

$$\begin{aligned}
&\frac{\Gamma_{\mathsf{P},f}(h)}{\Pr\left[\sum_{j=i}^{m} C_j = -(b+1)\right]} \\
&\leq \mathop{\mathrm{E}}_{c \leftarrow C_i | c \in \mathcal{C}_i^*}\left[\frac{|\Pr[B=1] - \Pr[B=1 \mid C_i = c]|}{\Pr\left[\sum_{j=i}^{m} C_j = -(b+1)\right]} \cdot |1 - \mathsf{ratio}_h(c)|\right] + \frac{4}{m^2} \\
&\leq \mathop{\mathrm{E}}_{c \leftarrow C_i | c \in \mathcal{C}_i^*}\left[\lambda'\left(|\sigma(c)| + \sqrt{\ell_m(i)}\right) \cdot \gamma \cdot \frac{|\sigma(c)| + \sqrt{\ell_m(i)}}{\sqrt{\mathsf{sum}_m(i)}}\right] + \frac{4}{m^2} \\
&\leq \lambda' \cdot \gamma \cdot \mathop{\mathrm{E}}_{c \leftarrow C_i | c \in \mathcal{C}_i^*}\left[\frac{|\sigma(c)|^2 + 2|\sigma(c)|\sqrt{\ell_m(i)} + \ell_m(i)}{\sqrt{\mathsf{sum}_m(i)}}\right] + \frac{4}{m^2} \\
&\leq 4\lambda' \cdot \gamma \cdot \frac{\ell_m(i)}{\sqrt{\mathsf{sum}_m(i)}} + \frac{4}{m^2} \\
&\leq 4\lambda' \cdot \gamma \cdot \sqrt{\frac{\ell_m(i)}{m-i+1}} + \frac{4}{m^2} \\
&\leq 4(\lambda' \cdot \gamma + 1) \cdot \sqrt{\frac{\ell_m(i)}{m-i+1}}
\end{aligned}$$

for λ' being the constant guaranteed in Lemma 4.17. The first inequality holds by Lemma 4.15 and by Equation (35), the seconds one by Lemma 4.17 and assumption 2 on h, the fourth one by Proposition 2.3 and the fifth one holds since $\mathsf{sum}_m(i) \leq (m-i+1) \cdot \ell_m(i)$. □

Proving Lemma 4.17.

Proof of Lemma 4.17. In the following we assume without loss of generality that m is larger than a universal constant to be determined by the proof (otherwise, the proof is trivially holds by choosing large enough λ). Since $|b + \varepsilon \cdot \mathsf{sum}_m(i)| \leq 4\sqrt{\log m \cdot \mathsf{sum}_m(i)}$ and since m is large, Proposition 2.2 yields that

$$\Pr\left[\sum_{j=i}^{m} C_j = -(b+1)\right] \geq \frac{1}{m^{10}}$$

Therefore, by Hoeffding's inequality (Fact 2.1), it holds that

$$\frac{\Pr[C_i \notin \mathcal{C}_i^*]}{\Pr\left[\sum_{j=i}^{m} C_j = -(b+1)\right]} \leq \frac{\frac{1}{m^{12}}}{\frac{1}{m^{10}}} = \frac{1}{m^2} \tag{36}$$

We use the following claim (proven in the next section).

Claim 4.18. *For every $c, c' \in \mathcal{C}_i^*$, it holds that*

$$\left|\Pr[B=1 \mid C_i = c] - \Pr\left[B=1 \mid C_i = c'\right]\right| \leq \lambda' \cdot \left(|\sigma(c)| + \left|\sigma(c')\right|\right) \cdot \Pr\left[\sum_{j=i}^{m} C_j = -(b+1)\right]$$

for a universal constant $\lambda' > 0$.

Fix $c \in \mathcal{C}_i^*$ and compute

$$\begin{aligned}
&\frac{|\Pr[B=1] - \Pr[B=1 \mid C_i = c]|}{\Pr\left[\sum_{j=i}^m C_j = -(b+1)\right]} \\
&\leq \mathop{\mathrm{E}}_{c' \leftarrow C_i}\left[\frac{|\Pr[B=1 \mid C_i = c'] - \Pr[B=1 \mid C_i = c]|}{\Pr\left[\sum_{j=i}^m C_j = -(b+1)\right]}\right] \\
&\leq \mathop{\mathrm{E}}_{c' \leftarrow C_i \mid c' \in \mathcal{C}_i^*}\left[\frac{|\Pr[B=1 \mid C_i = c'] - \Pr[B=1 \mid C_i = c]| + \Pr[C_i \notin \mathcal{C}_i^*]}{\Pr\left[\sum_{j=i}^m C_j = -(b+1)\right]}\right] \\
&\leq \mathop{\mathrm{E}}_{c' \leftarrow C_i \mid c' \in \mathcal{C}_i^*}\left[\lambda' \cdot (|\sigma(c)| + |\sigma(c')|)\right] + \frac{1}{m^2} \\
&\leq \lambda' \cdot \sqrt{\ell_m(i)} + \lambda' \cdot |\sigma(c)| + \frac{1}{m^2} \\
&\leq (\lambda' + 1) \cdot \left(\sqrt{\ell_m(i)} + \lambda' \cdot |\sigma(c)|\right).
\end{aligned}$$

The third inequality holds by Claim 4.18 and eq. (36), and the fourth one by Proposition 2.3. □

Proving Claim 4.18.

Proof of Claim 4.18. We consider two cases.

The case $|b + \varepsilon \cdot \mathsf{sum}_m(i+1)| \leq \sqrt{\mathsf{sum}_m(i+1)}$. In this case, it holds that

$$\begin{aligned}
\Pr\left[\sum_{j=i}^m C_j = -(b+1)\right] &= \widehat{\mathcal{C}}_{\mathsf{sum}_m(i+1),\varepsilon}(-(b+1)) \\
&\geq \frac{1}{2} \cdot \frac{1}{\sqrt{\mathsf{sum}_m(i+1)}} \cdot e^{-\frac{(-b-1-\varepsilon \cdot \mathsf{sum}_m(i+1))^2}{2 \cdot \mathsf{sum}_m(i+1)}} \\
&\geq \frac{1}{2} \cdot \frac{1}{\sqrt{\mathsf{sum}_m(i+1)}} \cdot e^{-1},
\end{aligned} \tag{37}$$

where the first inequality holds by Proposition 2.2. In addition, it holds that

$$\begin{aligned}
\left|\Pr[B=1 \mid C_i = c] - \Pr\left[B=1 \mid C_i = c'\right]\right| &= \left|\widehat{\mathcal{C}}_{\mathsf{sum}_m(i+1),\varepsilon}\big(-(b+c)\big) - \widehat{\mathcal{C}}_{\mathsf{sum}_m(i+1),\varepsilon}\big(-(b+c')\big)\right| \\
&\leq \frac{|\sigma(c) - \sigma(c')|}{\sqrt{\mathsf{sum}_m(i+1)}} \\
&\leq \frac{|\sigma(c)| + |\sigma(c')|}{\sqrt{\mathsf{sum}_m(i+1)}},
\end{aligned} \tag{38}$$

where the first inequality also holds by Proposition 2.2. Combining Equations (37) and (38) yields that

$$\frac{|\Pr[B=1 \mid C_i = c] - \Pr[B=1 \mid C_i = c']|}{\Pr\left[\sum_{j=i}^m C_j = -(b+1)\right]} \leq 2e \cdot (|\sigma(c)| + |\sigma(c')|) \tag{39}$$

The case $|b+\varepsilon\cdot\mathsf{sum}_m(i+1)| > \sqrt{\mathsf{sum}_m(i+1)}$. Assume for simplicity that $b+\varepsilon\cdot\mathsf{sum}_m(i+1) > \sqrt{\mathsf{sum}_m(i+1)}$ (the case $b+\varepsilon\cdot\mathsf{sum}_m(i+1) \le -\sqrt{\mathsf{sum}_m(i+1)}$ follows by an analogues arguments). In addition, we assume without loss of generality that $|c| \ge |c'|$. Note that for every c'' with $|c''| \le |c|$, it holds that

$$\begin{aligned}
\Pr\left[\sum_{j=i+1}^{m} C_j = -(b+c'')\right] &= \widehat{\mathcal{C}}_{\mathsf{sum}_m(i+1),\varepsilon}(-(b+c'')) \qquad (40)\\
&\le \frac{1}{\sqrt{\mathsf{sum}_m(i+1)}}\cdot e^{-\frac{(-b-c''-\varepsilon\cdot\mathsf{sum}_m(i+1))^2}{2\cdot\mathsf{sum}_m(i+1)}}\\
&\le \frac{1}{\sqrt{\mathsf{sum}_m(i+1)}}\cdot e^{-\frac{(-b+|c|-\varepsilon\cdot\mathsf{sum}_m(i+1))^2}{2\cdot\mathsf{sum}_m(i+1)}}\\
&\le 2\cdot\widehat{\mathcal{C}}_{\mathsf{sum}_m(i+1),\varepsilon}(-(b-|c|))\\
&= 2\cdot\Pr\left[\sum_{j=i+1}^{m} C_j = -(b-|c|)\right].
\end{aligned}$$

The first and third inequalities holds by Proposition 2.2 and the second inequality holds since $|c''| \le |c| < \sqrt{\mathsf{sum}_m(i+1)} < b+\varepsilon\cdot\mathsf{sum}_m(i+1)$.

Therefore,

$$\begin{aligned}
&\frac{\Pr\left[\sum_{j=i}^{m} C_j = -(b+1)\right]}{|\Pr[B=1 \mid C_i=c] - \Pr[B=1 \mid C_i=c']|}\\
&\ge \frac{\Pr\left[\sum_{j=i}^{m} C_j = -(b+1) \mid C_i \in \mathcal{C}_i^*\right]\cdot\Pr[C_i\in\mathcal{C}_i^*]}{|\Pr[B=1 \mid C_i=c] - \Pr[B=1 \mid C_i=c']|}\\
&\ge \frac{1}{2}\cdot\mathop{\mathrm{E}}_{c''\leftarrow C_i|c''\in\mathcal{C}_i^*}\left[\frac{\Pr\left[\sum_{j=i}^{m} C_j = -(b+1) \mid C_i = c''\right]}{|\Pr[B=1 \mid C_i=c] - \Pr[B=1 \mid C_i=c']|}\right]\\
&\ge \frac{1}{2}\cdot\mathop{\mathrm{E}}_{c''\leftarrow C_i|c''\in\mathcal{C}_i^*}\left[\frac{\Pr\left[\sum_{j=i+1}^{m} C_j = -(b+c''+1)\right]}{|c-c'|\cdot\Pr\left[\sum_{j=i+1}^{m} C_j = -(b-|c|)\right]}\right]\\
&\ge \frac{1}{2\big(|\sigma(c)|+|\sigma(c')|\big)}\cdot\mathop{\mathrm{E}}_{c''\leftarrow C_i|c''\in\mathcal{C}_i^*}\left[\frac{\Pr\left[\sum_{j=i+1}^{m} C_j = -(b+c''+1)\right]}{\Pr\left[\sum_{j=i+1}^{m} C_j = -(b-|c|)\right]}\right]\\
&\ge \frac{1}{4(|\sigma(c)|+|\sigma(c')|)}\cdot\mathop{\mathrm{E}}_{c''\leftarrow C_i|c''\in\mathcal{C}_i^*}\left[\frac{\exp\left(-\frac{(-b-c''-1-\varepsilon\cdot\mathsf{sum}_m(i+1))^2}{2\cdot\mathsf{sum}_m(i+1)}\right)}{\exp\left(-\frac{(-b+|c|-\varepsilon\cdot\mathsf{sum}_m(i+1))^2}{2\cdot\mathsf{sum}_m(i+1)}\right)}\right]\\
&= \frac{\mathrm{E}_{c''\leftarrow C_i|c''\in\mathcal{C}_i^*}\left[\exp\left(-\frac{(c''+1)^2+2b(c''+1)+2(c''+1)\cdot\varepsilon\cdot\mathsf{sum}_m(i+1)-c^2+2|c|b+2|c|\cdot\varepsilon\cdot\mathsf{sum}_m(i+1)}{2\cdot\mathsf{sum}_m(i+1)}\right)\right]}{4(|\sigma(c)|+|\sigma(c')|)}\\
&\ge \frac{1}{4e\cdot(|\sigma(c)|+|\sigma(c')|)}.
\end{aligned}$$

The third inequality holds by Equation (40), the fifth one by Proposition 2.2, and the last one since the expression in the exponent is smaller than one (note that $|c|, |c''| \leq 6 \cdot \sqrt{\log m \cdot \ell_m(i+1)} + \varepsilon \cdot \ell_m(i) \leq 7 \cdot \sqrt{\log m \cdot \ell_m(i+1)}$). We conclude that

$$\frac{|\Pr[B = 1 \mid C_i = c] - \Pr[B = 1 \mid C_i = c']|}{\Pr\left[\sum_{j=i}^{m} C_j = -(b+1)\right]} \leq 4e \cdot (|\sigma(c)| + |\sigma(c')|),$$

as required. □

4.2.5 A Bound on Binomial Process with All-Information Leakage

In this section we prove Lemma 4.7. Let $m \in \mathbb{N}$, $i \in [m]$, $b \in \mathbb{Z}$ and $\varepsilon \in [-1, 1]$ that satisfy the assumptions of Lemma 4.7. We assume without loss of generality that m is larger than some universal constant and we focus on the $(m, i, \ell_m, b, \varepsilon)$-binomial process $\mathsf{P} = (A = C_i, B)$ (according to Definition 4.1) with all-information leakage function f. Let $\mathcal{C}_i^* := \{c \in \mathrm{Supp}(C_i) \mid |\sigma(c)| \leq 6 \cdot \sqrt{\log m \cdot \ell_m(i)}\}$ for $\sigma(c) := c - \mathrm{E}_{c' \leftarrow C_i}[c'] = c - \varepsilon \cdot \ell_m(i)$.

Proof of Lemma 4.7. Let $\mathcal{H} = \mathcal{C}_i^*$. By Fact 2.1 (Hoeffding's inequality), it holds that

$$\Pr[f(C_i) \notin \mathcal{H}] = \Pr[C_i \notin \mathcal{C}_i^*] \leq \frac{1}{m^2}. \tag{41}$$

Fix $c \in \mathcal{C}_i^*$. Since $f(C_i) = C_i$, Lemma 4.17 yields that there exists some universal constant $\lambda' > 0$ such that

$$\begin{aligned} \frac{|\Pr[B = 1] - \Pr[B = 1 \mid f(C_i) = c]|}{\Pr\left[\sum_{j=i}^{m} C_j = -(b+1)\right]} &\leq \lambda' \cdot \left(|\sigma(c)| + \sqrt{\ell_m(i)}\right) \\ &\leq 7\lambda' \cdot \sqrt{\ell_m(i)} \cdot \sqrt{\log m}, \end{aligned} \tag{42}$$

where the second inequality holds since $|\sigma(c)| \leq 6 \cdot \sqrt{\log m \cdot \ell_m(i)}$. The proof follows by Equations (41) and (42). □

4.2.6 Bound on Binomial Process with Hypergeometric Leakage

In this section we prove Lemma 4.8. Let $m \in \mathbb{N}$, $i \in [m]$, $b \in \mathbb{Z}$, $\varepsilon \in [-1, 1]$, $p \in [-2 \cdot \mathsf{sum}_m(1), 2 \cdot \mathsf{sum}_m(1)]$ and $\lambda > 0$ that satisfy the assumptions of Lemma 4.8. In the following, we assume without loss of generality that m is larger than some universal constant (we can choose γ and φ to be large enough on small values of m), and we focus on the $(m, i, \ell_m, b, \varepsilon)$-binomial process $\mathsf{P} = (A = C_i, B)$ with (m, i, ℓ_m, b, p)-hypergeometric leakage function f. We let $\mathcal{C}_i^* := \{c \in \mathrm{Supp}(C_i) \mid |\sigma(c)| \leq 6 \cdot \sqrt{\log m \cdot \ell_m(i)}\}$ for $\sigma(c) := c - \mathrm{E}_{c' \leftarrow C_i}[c'] = c - \varepsilon \cdot \ell_m(i)$, and $\mathcal{H}^* := \{h \in \mathrm{Supp}(f(C_i)) \mid |h - b| \leq (\lambda + 4) \cdot \sqrt{\log m \cdot \mathsf{sum}_m(i)}\}$.

The following proposition, which wraps the main analysis of this section, bounds how much $\mathsf{ratio}_h(a)$ can be far from 1.

Proposition 4.19. *For every $h \in \mathcal{H}^*$ and $c \in \mathcal{C}_i^*$, it holds that*

$$|1 - \mathsf{ratio}_h(c)| \leq \varphi(\lambda) \cdot \sqrt{\log m} \cdot \frac{|\sigma(c)| + \sqrt{\ell_m(i)}}{\sqrt{\mathsf{sum}_m(i)}},$$

for some universal function $\varphi \colon \mathbb{R}^+ \to \mathbb{R}^+$.

Proof. Fix $h = b + t \in \mathcal{H}^*$ and $c \in \mathcal{C}_i^*$. Compute

$$\begin{aligned}
\frac{1}{\mathsf{ratio}_h(c)} &= \frac{\Pr\left[f(A) = b + t \mid C_i \in \mathcal{C}_i^*\right]}{\Pr\left[f(A) = b + t \mid C_i = c\right]} \qquad (43)\\
&= \mathop{\mathrm{E}}_{c' \leftarrow C_i \mid c' \in \mathcal{C}_i^*}\left[\frac{\mathcal{HG}_{2\cdot\mathsf{sum}_m(1),p,\mathsf{sum}_m(i+1)}(t-c')}{\mathcal{HG}_{2\cdot\mathsf{sum}_m(1),p,\mathsf{sum}_m(i+1)}(t-c)}\right]\\
&\in \mathop{\mathrm{E}}_{c' \leftarrow C_i \mid c' \in \mathcal{C}_i^*}\left[e^{\frac{(t-c-\frac{p\cdot\mathsf{sum}_m(i+1)}{2\cdot\mathsf{sum}_m(1)})^2-(t-c'-\frac{p\cdot\mathsf{sum}_m(i+1)}{2\cdot\mathsf{sum}_m(1)})^2}{2\cdot\mathsf{sum}_m(i+1)\cdot(1-\frac{\mathsf{sum}_m(i+1)}{2\cdot\mathsf{sum}_m(1)})}}\right]\cdot\left(1 \pm 4\varphi'(\lambda)\cdot\frac{\log^{1.5} m}{\sqrt{\mathsf{sum}_m(i+1)}}\right)\\
&= \mathop{\mathrm{E}}_{c' \leftarrow C_i \mid c' \in \mathcal{C}_i^*}\left[e^{\frac{2(c'-c)\cdot(t-\frac{p\cdot\mathsf{sum}_m(i+1)}{2\cdot\mathsf{sum}_m(1)})+c^2-c'^2}{2\cdot\mathsf{sum}_m(i+1)\cdot(1-\frac{\mathsf{sum}_m(i+1)}{2\cdot\mathsf{sum}_m(1)})}}\right]\cdot\left(1 \pm 4\varphi'(\lambda)\cdot\frac{\log^{1.5} m}{\sqrt{\mathsf{sum}_m(i+1)}}\right)\\
&= \mathop{\mathrm{E}}_{c' \leftarrow C_i \mid c' \in \mathcal{C}_i^*}\left[e^{\frac{2\left(\sigma(c')-\sigma(c)\right)\cdot(t-\frac{p\cdot\mathsf{sum}_m(i+1)}{2\cdot\mathsf{sum}_m(1)})+\sigma(c)^2-\sigma(c')^2+2\cdot\left(\sigma(c)-\sigma(c')\right)\cdot\varepsilon\cdot\ell_m(i)}{2\cdot\mathsf{sum}_m(i+1)\cdot(1-\frac{\mathsf{sum}_m(i+1)}{2\cdot\mathsf{sum}_m(1)})}}\right]\cdot\left(1 \pm 4\varphi'(\lambda)\cdot\frac{\log^{1.5} m}{\sqrt{\mathsf{sum}_m(i+1)}}\right)
\end{aligned}$$

where the third transition follows by Proposition 2.6 where φ' is the function from it. Since $|\sigma(c)|, |\sigma(c')| \le 6\sqrt{\log m \cdot \ell_m(i)}$, $|t| \le (\lambda+4)\sqrt{\log m \cdot \mathsf{sum}_m(i)}$, $|p| \le \lambda\sqrt{\log m \cdot \mathsf{sum}_m(1)}$ and $i \in [m - \lfloor m^{\frac{1}{8}} \rfloor]$, it holds that $\left|\frac{2\left(\sigma(c')-\sigma(c)\right)\cdot(t-\frac{p\cdot\mathsf{sum}_m(i+1)}{2\cdot\mathsf{sum}_m(1)})+\sigma(c)^2-\sigma(c')^2+2\cdot\left(\sigma(c)-\sigma(c')\right)\cdot\varepsilon\cdot\ell_m(i)}{2\cdot\mathsf{sum}_m(i+1)\cdot(1-\frac{\mathsf{sum}_m(i+1)}{2\cdot\mathsf{sum}_m(1)})}\right| < 1$. Therefore,

$$\begin{aligned}
&\mathop{\mathrm{E}}_{c' \leftarrow C_i \mid c' \in \mathcal{C}_i^*}\left[e^{\frac{2\left(\sigma(c')-\sigma(c)\right)\cdot(t-\frac{p\cdot\mathsf{sum}_m(i+1)}{2\cdot\mathsf{sum}_m(1)})+\sigma(c)^2-\sigma(c')^2+2\cdot\left(\sigma(c)-\sigma(c')\right)\cdot\varepsilon\cdot\ell_m(i)}{2\cdot\mathsf{sum}_m(i+1)\cdot(1-\frac{\mathsf{sum}_m(i+1)}{2\cdot\mathsf{sum}_m(1)})}}\right] \qquad (44)\\
&\in \left(1 \pm \mathop{\mathrm{E}}_{c' \leftarrow C_i \mid c' \in \mathcal{C}_i^*}\left[\frac{4\cdot|\sigma(c')-\sigma(c)|\cdot\left|t-\frac{p\cdot\mathsf{sum}_m(i+1)}{2\cdot\mathsf{sum}_m(1)}\right| + 2\left|\sigma(c)^2-\sigma(c')^2\right| + 4\cdot|\sigma(c)-\sigma(c')|\cdot\varepsilon\cdot\ell_m(i)}{\mathsf{sum}_m(i+1)}\right]\right)\\
&\in \left(1 \pm \frac{4\cdot\left(|\sigma(c)|+\sqrt{\ell_m(i)}\right)\cdot(3\lambda+4)\sqrt{\log m\cdot\mathsf{sum}_m(i+1)} + 2\cdot\sigma(c)^2 + 2\cdot\ell_m(i) + \left(|\sigma(c)|+\sqrt{\ell_m(i)}\right)\cdot 1}{\mathsf{sum}_m(i+1)}\right)\\
&\in \left(1 \pm (12\lambda+17)\cdot\sqrt{\log m}\cdot\frac{|\sigma(c)|+\sqrt{\ell_m(i)}}{\sqrt{\mathsf{sum}_m(i+1)}}\right)
\end{aligned}$$

where the first transition holds since $e^a \in 1 \pm 2|a|$ for every $a \in [-1,1]$ and the second one holds by Proposition 2.3 and by the bound on $|p|$, $|t|$ and $|\varepsilon|$. Combining Equations (43) and (44) yields that

$$\begin{aligned}
\frac{1}{\mathsf{ratio}_h(c)} &\in \left(1 \pm (12\lambda+17)\cdot\sqrt{\log m}\cdot\frac{|\sigma(c)|+\sqrt{\ell_m(i)}}{\sqrt{\mathsf{sum}_m(i+1)}}\right)\cdot\left(1 \pm 4\varphi'(\lambda)\cdot\frac{\log^{1.5} m}{\sqrt{\mathsf{sum}_m(i+1)}}\right)\\
&\in \left(1 \pm (12\lambda+18)\cdot\sqrt{\log m}\cdot\frac{|\sigma(c)|+\sqrt{\ell_m(i)}}{\sqrt{\mathsf{sum}_m(i+1)}}\right)
\end{aligned}$$

Since $(12\lambda+18)\cdot\sqrt{\log m}\cdot\frac{|\sigma(c)|+\sqrt{\ell_m(i)}}{\sqrt{\mathsf{sum}_m(i+1)}}<0.5$ and since $\frac{1}{1\pm a}\in 1\pm 2a$ for every $a\in(-0.5,0.5)$, we conclude that

$$|1-\mathsf{ratio}_h(c)|\leq(24\lambda+36)\cdot\sqrt{\log m}\cdot\frac{|\sigma(c)|+\sqrt{\ell_m(i)}}{\sqrt{\mathsf{sum}_m(i+1)}},$$

as required. □

The following proposition combines the analysis done in Proposition 4.19 with the main tool of Section 4.2.4 in order to bound the expectation change of B.

Proposition 4.20. *For every $h\in\mathcal{H}^*$ such that $\Pr\left[C_i\notin\mathcal{C}_i^*\mid f(C_i)=h\right]\leq\frac{1}{m^{12}}$, it holds that*

$$\frac{\left|\Pr\left[B=1\right]-\Pr\left[B=1\mid f(C_i)=h\right]\right|}{\Pr\left[\sum_{j=i}^m C_j=-(b+1)\right]}\leq\varphi(\lambda)\sqrt{\log m}\cdot\sqrt{\frac{\ell_m(i)}{m-i+1}},$$

for some universal function $\varphi\colon\mathbb{R}^+\to\mathbb{R}^+$.

Proof. The proof immediately follows by Proposition 4.19 and Lemma 4.16. □

We are finally ready for proving Lemma 4.8.

Proof of Lemma 4.8.

Proof. Let $\mathcal{H}:=\{h\in\mathcal{H}^*\mid\Pr\left[C_i\notin\mathcal{C}_i^*\mid f(C_i)=h\right]\leq\frac{1}{m^{12}}\}$. Assume by contradiction that $\Pr_{h\leftarrow f(C_i)}\left[\Pr\left[C_i\notin\mathcal{C}_i^*\mid f(C_i)=h\right]>\frac{1}{m^{12}}\right]>\frac{1}{2m^2}$. Then

$$\begin{aligned}
&\Pr\left[C_i\notin\mathcal{C}_i^*\right]\\
&\quad\geq\Pr_{h\leftarrow f(C_i)}\left[C_i\notin\mathcal{C}_i^*\mid\Pr\left[C_i\notin\mathcal{C}_i^*\mid f(C_i)=h\right]>\frac{1}{m^{12}}\right]\cdot\Pr_{h\leftarrow f(C_i)}\left[\Pr\left[C_i\notin\mathcal{C}_i^*\mid f(C_i)=h\right]>\frac{1}{m^{12}}\right]\\
&\quad\geq\frac{1}{m^{12}}\cdot\frac{1}{2m^2}\\
&\quad=\frac{1}{2m^{14}},
\end{aligned}$$

In contradiction to Hoeffding's inequality (Fact 2.1). Hence,

$$\Pr_{h\leftarrow f(C_i)}\left[\Pr\left[C_i\notin\mathcal{C}_i^*\mid f(C_i)=h\right]>\frac{1}{m^{12}}\right]\leq\frac{1}{2m^2},\tag{45}$$

In addition, it holds that

$$\begin{aligned}
\Pr\left[f(C_i)\notin\mathcal{H}^*\right]&=\Pr_{h\leftarrow f(C_i)}\left[|h-b|>(\lambda+4)\sqrt{\log m\cdot\mathsf{sum}_m(i)}\right]\qquad(46)\\
&=\Pr_{t\leftarrow\mathcal{HG}_{2\mathsf{sum}_m(1),p,\mathsf{sum}_m(i+1)}}\left[|C_i+t|>(\lambda+4)\sqrt{\log m\cdot\mathsf{sum}_m(i)}\right]\\
&\leq\Pr_{t\leftarrow\mathcal{HG}_{2\mathsf{sum}_m(1),p,\mathsf{sum}_m(i+1)}}\left[|C_i+t|>(\lambda+4)\sqrt{\log m\cdot\mathsf{sum}_m(i)}\mid C_i\in\mathcal{C}_i^*\right]+\Pr\left[C_i\notin\mathcal{C}_i^*\right]\\
&\leq\Pr_{t\leftarrow\mathcal{HG}_{2\mathsf{sum}_m(1),p,\mathsf{sum}_m(i+1)}}\left[|t|>(\lambda+3)\sqrt{\log m\cdot\mathsf{sum}_m(i)}\right]+\frac{1}{4m^2}\\
&\leq\Pr_{t\leftarrow\mathcal{HG}_{2\mathsf{sum}_m(1),p,\mathsf{sum}_m(i+1)}}\left[\left|t-\frac{\mathsf{sum}_m(i+1)\cdot p}{\mathsf{sum}_m(1)}\right|>3\sqrt{\log m\cdot\mathsf{sum}_m(i)}\right]+\frac{1}{4m^2}\\
&\leq\frac{1}{2m^2}.
\end{aligned}$$

The second inequality holds since $|C_i| \leq 7\sqrt{\log m \cdot \ell_m(i)} \leq \sqrt{\log m \cdot \mathsf{sum}_m(i+1)}$ and by Hoeffding's inequality (Fact 2.1), the third on holds since $\left|\frac{\mathsf{sum}_m(i+1)\cdot p}{\mathsf{sum}_m(1)}\right| \leq \lambda\sqrt{\log m \cdot \mathsf{sum}_m(i+1)}$ and the last one holds by Fact 2.5 (Hoeffding's inequality for hypergeometric distribution).

Combining Equations (45) and (46) yields that

$$\Pr\left[f(C_i) \notin \mathcal{H}\right] \leq \frac{1}{m^2}. \tag{47}$$

In addition, note that for every $h \in \mathcal{H}$ it holds that

$$\begin{aligned}\Pr\left[|C_i| > 7\sqrt{\log m \cdot \ell_m(i)} \mid f(C_i) = h\right] &= \Pr\left[|C_i| > 7\sqrt{\log m \cdot \ell_m(i)} \mid f(C_i) = h\right] \\ &\leq \Pr\left[|\sigma(C_i)| > 6\sqrt{\log m \cdot \ell_m(i)} \mid f(C_i) = h\right] \\ &= \Pr\left[C_i \notin \mathcal{C}_i^* \mid f(C_i) = h\right] \\ &\leq \frac{1}{m^{12}},\end{aligned} \tag{48}$$

where the first inequality holds since $|C_i - \sigma(C_i)| = \varepsilon \cdot \ell_m(i) < \sqrt{\log m \cdot \ell_m(i)}$ and the last inequality holds by the definition of $\mathcal{H}$. The rest of proof immediately follows by Equation (47), Equation (48) and by Proposition 4.20. □

4.2.7 Bounding the Ratio for Processes with Vector Leakage

In this section, we prove the following lemma which states a general property about the ratio function, defined in Section 4.2.3, for any process $\mathsf{P} = (A, B)$ with a vector leakage function f. This property, together with Lemma 4.15, will be used for proving Lemmas 4.9 and 4.10.

Lemma 4.21. *Let $s, \alpha \in \mathbb{N}$, let (A, B) be a two-step process, let f be an (s, α)-vector leakage function for (A, B) according to Definition 3.18, and let ratio be according to Definition 4.13. Then, for every $h \in \mathrm{Supp}(f(A))$, $\mathcal{A}^* \subseteq \mathrm{Supp}(A)$ and $a \in \mathcal{A}^*$, it holds that*

$$\frac{1}{\mathsf{ratio}_{h,\mathcal{A}^*}(a)} \in \mathop{\mathrm{E}}_{a' \leftarrow A \mid a' \in \mathcal{A}^*}\left[e^{(\varepsilon_{a'} - \varepsilon_a)\cdot\left(w(h) - \frac{\varepsilon_{a'}+\varepsilon_a}{2}\cdot\alpha\cdot s\right)}\right] \cdot (1 \pm \mathsf{error}),$$

for $\varepsilon_a := \widehat{\mathcal{C}}_s^{-1}(\Pr[B = 1 \mid A = a])$ and $\mathsf{error} := \max_{a', a'' \in \mathcal{A}^*, z \in \pm\left|\varepsilon_{a'}^4 - \varepsilon_{a''}^4\right|}\left|e^{\frac{\varepsilon_{a'}^3 - \varepsilon_{a''}^3}{3}\cdot w(h) + z\cdot\alpha\cdot s} - 1\right|$.

Proof. Note that for every $a \in \mathrm{Supp}(A)$ and $h \in \mathrm{Supp}(f(A))$, it holds that

$$\begin{aligned}\Pr\left[f(A) = h \mid A = a\right] &= \Pr\left[f(a) = h\right] \\ &= 2^{-\alpha\cdot s} \cdot (1 + \varepsilon_a)^{\frac{1}{2}(\alpha\cdot s + w(h))} \cdot (1 - \varepsilon_a)^{\frac{1}{2}(\alpha\cdot s - w(h))} \\ &\in 2^{-\alpha\cdot s} \cdot e^{\left(\varepsilon_a - \frac{\varepsilon_a^2}{2} + \frac{\varepsilon_a^3}{3} \pm \varepsilon_a^4\right)\cdot\frac{1}{2}(\alpha\cdot s + w(h))} \cdot e^{\left(-\varepsilon_a - \frac{\varepsilon_a^2}{2} - \frac{\varepsilon_a^3}{3} \pm \varepsilon_a^4\right)\cdot\frac{1}{2}(\alpha\cdot s - w(h))} \\ &= 2^{-\alpha\cdot s} \cdot e^{\varepsilon_a\cdot w(h) - \frac{\varepsilon_a^2}{2}\cdot\alpha\cdot s} \cdot e^{\frac{\varepsilon_a^3}{3}\cdot w(h) \pm \varepsilon_a^4\cdot\alpha\cdot s},\end{aligned} \tag{49}$$

where the third transition holds by the Taylor series $\ln(1 + x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \ldots$.

Hence

$$\begin{aligned}
\frac{1}{\mathsf{ratio}_h(a)} &= \frac{\Pr\left[f(A)=h \mid A\in\mathcal{A}^*\right]}{\Pr\left[f(A)=h \mid A=a\right]} \\
&= \mathop{\mathrm{E}}_{a'\leftarrow A|a'\in\mathcal{A}^*}\left[\frac{\Pr\left[f(A)=h' \mid A=a'\right]}{\Pr\left[f(A)=h \mid A=a\right]}\right] \\
&\in \mathop{\mathrm{E}}_{a'\leftarrow A|a'\in\mathcal{A}^*}\left[e^{(\varepsilon_{a'}-\varepsilon_a)\cdot w(h)-\frac{\varepsilon_{a'}^2-\varepsilon_a^2}{2}\cdot\alpha\cdot s}\cdot e^{\frac{\varepsilon_{a'}^3-\varepsilon_a^3}{3}\cdot w(h)\pm\left|\varepsilon_{a'}^4-\varepsilon_a^4\right|\cdot\alpha\cdot s}\right] \\
&= \mathop{\mathrm{E}}_{a'\leftarrow A|a'\in\mathcal{A}^*}\left[e^{(\varepsilon_{a'}-\varepsilon_a)\cdot\left(w(h)-\frac{\varepsilon_{a'}+\varepsilon_a}{2}\cdot\alpha\cdot s\right)}\cdot\left(1+\left(e^{\frac{\varepsilon_{a'}^3-\varepsilon_a^3}{3}\cdot w(h)\pm\left|\varepsilon_{a'}^4-\varepsilon_a^4\right|\cdot\alpha\cdot s}-1\right)\right)\right] \\
&\in \mathop{\mathrm{E}}_{a'\leftarrow A|a'\in\mathcal{A}^*}\left[e^{(\varepsilon_{a'}-\varepsilon_a)\cdot\left(w(h)-\frac{\varepsilon_{a'}+\varepsilon_a}{2}\cdot\alpha\cdot s\right)}\right]\cdot\left(1\pm\mathsf{error}\right),
\end{aligned} \tag{50}$$

where the third transition holds by Equation (49). □

4.2.8 Bound on Binomial Process with Vector Leakage

In this section we prove Lemma 4.9. Let $s,\alpha\in\mathbb{N}$, $m\in\mathbb{N}$, $i\in[m]$, $b\in\mathbb{Z}$ and $\varepsilon\in[-1,1]$ that satisfy the assumptions of Lemma 4.9. In the following, we assume that m is larger than some universal constant (we can choose γ and φ to be large enough on small values of m), and we focus on the $(m,i,\ell_m,b,\varepsilon)$-binomial process $(A=C_i,B)$ with (s,α)-vector leakage function f. We let $\mathcal{C}_i^* := \{c\in\mathrm{Supp}(C_i) \mid |\sigma(c)|\le 6\cdot\sqrt{\log m\cdot\ell_m(i)}\}$ for $\sigma(c) := c-\mathrm{E}_{c'\leftarrow C_i}[c'] = c-\varepsilon\cdot\ell_m(i)$, and $\mathcal{H}^* := \{h\in\mathrm{Supp}(f(C_i)) \mid |\sigma(h)|\le 4\cdot\sqrt{\log m\cdot\alpha\cdot s}\}$ for $\sigma(h) := w(h)-\mathrm{E}_{c\leftarrow C_i,h'\leftarrow f(c)}[w(h')] = w(h)-\mathrm{E}_{c\leftarrow C_i}[\varepsilon_c]\cdot\alpha\cdot s$, where $\varepsilon_c=\widehat{\mathcal{C}}_s^{-1}(\Pr[B=1\mid C_i=c])$.

The following proposition, which wraps the main analysis of this section, bounds how much $\mathsf{ratio}_h(a)$ can be far from one.

Proposition 4.22. *For every $h\in\mathcal{H}^*$ and $c\in\mathcal{C}_i^*$, it holds that*

$$|1-\mathsf{ratio}_h(c)|\le\lambda\sqrt{\log m\cdot\alpha}\cdot\frac{|\sigma(c)|+\sqrt{\ell_m(i)}}{\sqrt{\mathsf{sum}_m(i)}},$$

for some universal constant $\lambda>0$.

Proof. Fix $h\in\mathcal{H}^*$ and $c\in\mathcal{C}_i^*$. By Lemma 4.21, it holds that

$$\frac{1}{\mathsf{ratio}_h(c)}\in\mathop{\mathrm{E}}_{c'\leftarrow C_i|c'\in\mathcal{C}_i^*}\left[e^{(\varepsilon_{c'}-\varepsilon_c)\cdot\left(w(h)-\frac{\varepsilon_{c'}+\varepsilon_c}{2}\cdot\alpha\cdot s\right)}\right]\cdot(1\pm\mathsf{error}),$$

where $\mathsf{error}=\max_{c',c''\in\mathcal{C}_i^*,z\in\pm\left|\varepsilon_{c'}^4-\varepsilon_{c''}^4\right|}\left|e^{\frac{\varepsilon_{c'}^3-\varepsilon_{c''}^3}{3}\cdot w(h)+z\cdot\alpha\cdot s}-1\right|$.

Since $\varepsilon_{c'}=\widehat{\mathcal{C}}_s^{-1}(\Pr[B=1\mid C_i=c'])$ for every $c'\in\mathcal{C}_i^*$, Proposition 2.4 yields that

$$\varepsilon_{c'}\in\frac{\varepsilon\cdot\mathsf{sum}_m(i+1)+b+c'}{\sqrt{s\cdot\mathsf{sum}_m(i+1)}}\pm\frac{\log^2 m}{2\cdot\sqrt{s\cdot\mathsf{sum}_m(i+1)}}, \tag{51}$$

for every $c' \in \mathcal{C}_i^*$, which yields that

$$\begin{aligned} |\varepsilon_{c'}| &\leq \frac{|\varepsilon| \cdot \mathsf{sum}_m(i+1) + |b| + |c'|}{\sqrt{s \cdot \mathsf{sum}_m(i+1)}} + \frac{\log^2 m}{2 \cdot \sqrt{s \cdot \mathsf{sum}_m(i+1)}} \\ &\leq 10 \cdot \sqrt{\frac{\log m}{s}}, \end{aligned} \tag{52}$$

where the second inequality holds by the bound on $|\varepsilon|, |b|$ (assumptions 1 and 3 of Lemma 4.9) and by the bound on $|c'|$. Therefore, for every $c', c'' \in \mathcal{C}_i^*$ and $z \in \pm \left|\varepsilon_{c'}^4 - \varepsilon_{c''}^4\right|$, it holds that

$$\begin{aligned} &\left|\frac{\varepsilon_{c'}^3 - \varepsilon_{c''}^3}{3} \cdot w(h) + z \cdot \alpha \cdot s\right| \\ &\leq \frac{|\varepsilon_{c'}|^3 + |\varepsilon_{c''}|^3}{3} \cdot w(h) + |z| \cdot \alpha \cdot s \\ &\leq \frac{2000}{3} \cdot \frac{\log^{1.5} m}{s^{1.5}} \cdot \left(10 \cdot \sqrt{\frac{\log m}{s}} \cdot \alpha \cdot s + 4\sqrt{\log m \cdot \alpha \cdot s}\right) + 20000 \cdot \frac{\log^2 m}{s^2} \cdot \alpha \cdot s \\ &\leq 30000 \cdot \log^2 m \cdot \frac{\alpha}{s} \\ &\leq 1. \end{aligned} \tag{53}$$

The second inequality holds by the bounds on $|\varepsilon_{c'}|$, $|\varepsilon_{c''}|$ and $|w(h)|$, and the last one by assumptions 5 and 6 of Lemma 4.9 and by assuming that m is larger than some universal constant. This yields that

$$\begin{aligned} \mathsf{error} &= \max_{c', c'' \in \mathcal{C}_i^*, z \in \pm\left|\varepsilon_{c'}^4 - \varepsilon_{c''}^4\right|} \left| e^{\frac{\varepsilon_{c'}^3 - \varepsilon_{c''}^3}{3} \cdot w(h) + z \cdot \alpha \cdot s} - 1 \right| \\ &\leq \max_{c', c'' \in \mathcal{C}_i^*, z \in \pm\left|\varepsilon_{c'}^4 - \varepsilon_{c''}^4\right|} 2 \cdot \left|\frac{\varepsilon_{c'}^3 - \varepsilon_{c''}^3}{3} \cdot w(h) + z \cdot \alpha \cdot s\right| \\ &\leq 60000 \cdot \log^2 m \cdot \frac{\alpha + \sqrt{s}}{s}, \end{aligned} \tag{54}$$

where the first inequality holds since $e^a \in 1 \pm 2|a|$ for every $a \in [-1, 1]$ and the second one holds by Equation (53).

In addition, note that

$$\begin{aligned} w(h) &= \mathop{\mathrm{E}}_{c' \leftarrow C_i}[\varepsilon_{c'}] \cdot \alpha \cdot s + \sigma(h) \\ &\in \mathop{\mathrm{E}}_{c' \leftarrow C_i}[\varepsilon_{c'}] \cdot \alpha \cdot s \pm 4 \cdot \sqrt{\log m \cdot \alpha \cdot s} \\ &= \frac{\varepsilon \cdot \mathsf{sum}_m(i+1) + b + \varepsilon \cdot \ell_m(i)}{\sqrt{s \cdot \mathsf{sum}_m(i+1)}} \cdot \alpha \cdot s \pm \frac{\log^2 m}{2 \cdot \sqrt{s \cdot \mathsf{sum}_m(i+1)}} \pm 4 \cdot \sqrt{\log m \cdot \alpha \cdot s} \\ &\in \sqrt{\frac{s}{\mathsf{sum}_m(i+1)}} \cdot \left(\frac{\varepsilon \cdot \mathsf{sum}_m(i+1) + b + \varepsilon \cdot \ell_m(i)}{s} \cdot \alpha \cdot s \pm 5 \cdot \sqrt{\log m \cdot \mathsf{sum}_m(i+1) \cdot \alpha}\right), \end{aligned} \tag{55}$$

where the second equality holds by Equation (51). Therefore, for every $c' \in \mathcal{C}_i^*$, it holds that

$$
\begin{aligned}
&(\varepsilon_{c'} - \varepsilon_c) \cdot \left(w(h) - \frac{\varepsilon_{c'} + \varepsilon_c}{2} \cdot \alpha \cdot s \right) \qquad (56)\\
&\in \frac{c' - c \pm \log^2 m}{\sqrt{s \cdot \mathsf{sum}_m(i+1)}} \cdot \left(w(h) - \frac{2\varepsilon \cdot \mathsf{sum}_m(i+1) + 2b + c + c' \pm \log^2 m}{2\sqrt{s \cdot \mathsf{sum}_m(i+1)}} \cdot \alpha \cdot s \right)\\
&= \frac{\sigma(c') - \sigma(c) \pm \log^2 m}{\mathsf{sum}_m(i+1)} \cdot \left(\sqrt{\frac{\mathsf{sum}_m(i+1)}{s}} \cdot w(h) - \frac{2\varepsilon \cdot \mathsf{sum}_m(i+1) + 2b + c + c' \pm \log^2 m}{2s} \cdot \alpha \cdot s \right)\\
&\subseteq \frac{\sigma(c') - \sigma(c) \pm \log^2 m}{\mathsf{sum}_m(i+1)} \cdot \left(\pm 5 \cdot \sqrt{\log m \cdot \mathsf{sum}_m(i+1) \cdot \alpha} - \frac{1}{2} \left(\sigma(c) + \sigma(c') \pm \log^2 m \right) \cdot \alpha \right)\\
&\subseteq \frac{\sigma(c') - \sigma(c) \pm \log^2 m}{\mathsf{sum}_m(i+1)} \cdot \left(\pm 5 \cdot \sqrt{\log m \cdot \mathsf{sum}_m(i+1) \cdot \alpha} \pm 4 \cdot \sqrt{\log m \cdot \ell_m(i)} \cdot \alpha \right)\\
&\subseteq \frac{\sigma(c') - \sigma(c) \pm \log^2 m}{\sqrt{\mathsf{sum}_m(i+1)}} \cdot \left(\pm 5 \cdot \sqrt{\log m \cdot \alpha} \pm 4 \cdot \frac{\alpha \cdot \sqrt{\log m}}{\sqrt{m-i}} \right)\\
&\subseteq \frac{\sigma(c') - \sigma(c) \pm \log^2 m}{\sqrt{\mathsf{sum}_m(i+1)}} \cdot \left(\pm 9 \cdot \sqrt{\log m \cdot \alpha} \right),
\end{aligned}
$$

where the first transition holds by Equation (51), the third one holds by Equation (55), the fourth one holds since $c, c' \in \mathcal{C}_i^*$ and the fifth one holds since $\mathsf{sum}_m(i+1) \leq (m-i) \cdot \ell_m(i)$.

By the bounds on $|\sigma(c)|, |\sigma(c')|, |\varepsilon_c|, |\varepsilon_{c'}|$ and by assumption 6 of Lemma 4.9, it holds that

$$
\left| (\varepsilon_{c'} - \varepsilon_c) \cdot \left(w(h) - \frac{\varepsilon_{c'} + \varepsilon_c}{2} \cdot \alpha \cdot s \right) \right| \leq 1,
$$

for every $c' \in \mathcal{C}_i^*$. Hence,

$$
\begin{aligned}
\frac{1}{\mathsf{ratio}_h(c)} &\in \mathop{\mathrm{E}}_{c' \leftarrow C_i | c' \in \mathcal{C}_i^*} \left[e^{(\varepsilon_{c'} - \varepsilon_c) \cdot \left(w(h) - \frac{\varepsilon_{c'} + \varepsilon_c}{2} \cdot \alpha \cdot s \right)} \right] \cdot (1 \pm \mathsf{error}) \qquad (57)\\
&\subseteq \mathop{\mathrm{E}}_{c' \leftarrow C_i | c' \in \mathcal{C}_i^*} \left[1 \pm 18 \cdot \frac{|\sigma(c)| + |\sigma(c')| + \log^2 m}{\sqrt{\mathsf{sum}_m(i+1)}} \cdot \sqrt{\log m \cdot \alpha} \right] \cdot (1 \pm \mathsf{error})\\
&\subseteq \left(1 \pm 18 \cdot \frac{|\sigma(c)| + \sqrt{\ell_m(i)} + \log^2 m}{\sqrt{\mathsf{sum}_m(i+1)}} \cdot \sqrt{\log m \cdot \alpha} \right) \cdot \left(1 \pm 60000 \cdot \log^2 m \cdot \frac{\alpha}{s} \right)\\
&\subseteq \left(1 \pm 19 \cdot \frac{|\sigma(c)| + \sqrt{\ell_m(i)}}{\sqrt{\mathsf{sum}_m(i+1)}} \cdot \sqrt{\log m \cdot \alpha} \right),
\end{aligned}
$$

where the second transition holds by Equation (56) and since $e^a \in 1 \pm 2|a|$ for every $a \in [-1, 1]$, the third one holds by Proposition 2.3 and the last one holds by assumptions 2, 5, 6 of Lemma 4.9 and by assuming that m is larger than some universal constant, which yields that $\sqrt{\frac{\ell_m(i)}{\mathsf{sum}_m(i)}} \geq \sqrt{\frac{1}{m-i}} = \omega(\log^2 m \cdot \frac{\alpha + \sqrt{s}}{s})$

By assumption 6 of Lemma 4.9 and since $c \in \mathcal{C}_i^*$ and $\frac{1}{1 \pm a} \subseteq 1 \pm 2a$ for every $a \in (-0.5, 0.5)$, we deduce from Equation (57) that

$$
\mathsf{ratio}_h(c) \in \left(1 \pm 38 \sqrt{\log m \cdot \alpha} \cdot \frac{|\sigma(c)| + \sqrt{\ell_m(i)}}{\sqrt{\mathsf{sum}_m(i+1)}} \right). \qquad (58)
$$

Thus

$$|1 - \mathsf{ratio}_h(c)| \leq 38\sqrt{\log m \cdot \alpha} \cdot \frac{|\sigma(c)| + \sqrt{\ell_m(i)}}{\sqrt{\mathsf{sum}_m(i+1)}}$$

□

The following proposition combines the analysis done in Proposition 4.22 with the main tool of Section 4.2.4 in order to bound the expectation change of B.

Proposition 4.23. *For every $h \in \mathcal{H}^*$ such that $\Pr[C_i \notin \mathcal{C}_i^* \mid f(C_i) = h] \leq \frac{1}{m^{12}}$, it holds that*

$$\frac{|\Pr[B = 1] - \Pr[B = 1 \mid f(C_i) = h]|}{\Pr\left[\sum_{j=i}^{m} C_j = -(b+1)\right]} \leq \lambda\sqrt{\log m \cdot \alpha} \cdot \sqrt{\frac{\ell_m(i)}{m - i + 1}}$$

Proof. The proof immediately follows by Proposition 4.22 and Lemma 4.16. □

We are finally ready for proving Lemma 4.9.

Proving Lemma 4.9.

Proof. Let $\mathcal{H} := \{h \in \mathcal{H}^* \mid \Pr[C_i \notin \mathcal{C}_i^* \mid f(C_i) = h] \leq \frac{1}{m^{12}}\}$. Using similar arguments as in the proof of Lemma 4.8, it holds that

$$\Pr_{h \leftarrow f(C_i)}\left[\Pr[C_i \notin \mathcal{C}_i^* \mid f(C_i) = h] > \frac{1}{m^{12}}\right] \leq \frac{1}{2m^2}, \tag{59}$$

In addition, Hoeffding's inequality (Fact 2.1) yields that

$$\Pr[f(C_i) \notin \mathcal{H}^*] \leq \frac{1}{2m^2} \tag{60}$$

Therefore, we conclude from Equations (59) and (60) that

$$\Pr[f(C_i) \notin \mathcal{H}] \leq \frac{1}{m^2} \tag{61}$$

In addition, as proven in Lemma 4.8, for every $h \in \mathcal{H}$ it holds that

$$\Pr\left[|C_i| > 7\sqrt{\log m \cdot m} \mid f(C_i) = h\right] \leq \frac{1}{m^{12}}, \tag{62}$$

The proof now follows by Equations (61) and (62) and Proposition 4.23. □

4.2.9 Bound on Hypergeometric Process with Vector Leakage

In this section we prove Lemma 4.10. Let $s, \alpha, \beta \in \mathbb{N}$ and $\delta \in [0,1]$ that satisfy the assumptions of Lemma 4.10, assume that $\delta \in [\frac{1}{s^4}, 1 - \frac{1}{s^4}]$ and let $\varepsilon := \widehat{\mathcal{C}}_s^{-1}(\delta)$ (note that by Fact 2.1, $|\varepsilon| \leq 4\sqrt{\frac{\log s}{s}}$). We assume without loss of generality that s is larger than some universal constant (otherwise, the proof trivially holds by taking large enough λ).

Let (A, B) be a (s, β, δ)-hypergeometric process with (s, α)-vector leakage function f, as defined in Definition 4.4.

Let $\mathcal{V}^* = \{v \in \{-1,1\}^{\beta \cdot s} \mid |\sigma(v)| \leq 4\sqrt{\log s \cdot \beta \cdot s}\}$, for $\sigma(v) := w(v) - \mathrm{E}_{v' \leftarrow (\mathcal{C}_\varepsilon)^{\beta \cdot s}}[w(v')] = w(v) - \varepsilon \cdot \beta \cdot s$, let $\mathcal{A}^* := \bigcup_{v \in \mathcal{V}^*} \{\widehat{\mathcal{HG}}_{\beta \cdot s, w(v), s}(0)\}$ and let $\mathcal{H}^* := \{h \in \mathrm{Supp}(f(A)) \mid |\sigma(h)| \leq 4 \cdot \sqrt{\log s \cdot \alpha \cdot s}\}$, for $\sigma(h) := w(h) - \mathrm{E}_{a \leftarrow A, h \leftarrow f(A) | A = a}[w(h)] = w(h) - \mathrm{E}_{a \leftarrow A}[\varepsilon_a] \cdot \alpha \cdot s$ for $\varepsilon_a := \widehat{\mathcal{C}}_s^{-1}(\Pr[B = 1 \mid A = a])$. In addition, for $a \in \mathcal{A}^*$, let $w(a)$ be the value $w \in \mathbb{Z}$ with $a = \widehat{\mathcal{HG}}_{\beta \cdot s, w, s}(0)$ and we let $\sigma(a) = w(a) - \varepsilon \cdot \beta \cdot s$ (note that by definition, $|\sigma(a)| \leq 4\sqrt{\log s \cdot \beta \cdot s}$ for every $a \in \mathcal{A}^*$).

Proving Lemma 4.10 is done by bounding $\Gamma_{\mathsf{P},f}(h)$ for "typical" values of h. The first step (Proposition 4.24) is to bound $|\Pr[B = 1] - \Pr[B = 1 \mid A = a]|$ for "typical" values of h. The second step (Proposition 4.25) is to bound $|1 - \mathsf{ratio}_h(a)|$ for "typical" values of a and h. Then, Proposition 4.26 combines the two step using Lemma 4.15 in order to achieve the desired bound on $\Gamma_{\mathsf{P},f}(h)$.

Proposition 4.24. *For every $a \in \mathcal{A}^*$, it holds that*

$$|\Pr[B = 1] - \Pr[B = 1 \mid A = a]| \leq \frac{\sigma(a) + 2\sqrt{\beta \cdot s}}{\beta \cdot \sqrt{s}}.$$

Proof. Note that for every $a' \in \mathcal{A}^*$, it holds that $\Pr[B = 1 \mid A = a'] = a' = \widehat{\mathcal{HG}}_{\beta \cdot s, w(a'), s}(0)$. Therefore, by Proposition 2.7 it holds that

$$\begin{aligned} \Pr\left[B = 1 \mid A = a'\right] &\in \Phi\left(\frac{-\frac{w(a') \cdot s}{\beta \cdot s}}{\sqrt{s(1 - \frac{s}{\beta \cdot s})}}\right) \pm \varphi(4) \cdot \frac{\log^{1.5} s}{\sqrt{s}} \\ &= \Phi\left(-\frac{w(a')}{\beta \cdot \sqrt{s \cdot (1 - \frac{1}{\beta})}}\right) \pm \varphi(4) \cdot \frac{\log^{1.5} s}{\sqrt{s}} \end{aligned} \tag{63}$$

for every $a' \in \mathcal{A}^*$. This yields that

$$\begin{aligned}
&|\Pr[B=1] - \Pr[B=1 \mid A=a]| \\
&= \mathop{\mathrm{E}}_{a' \leftarrow A}[\Pr[B=1 \mid A=a] - \Pr[B=1 \mid A=a]] \\
&\leq \mathop{\mathrm{E}}_{a' \leftarrow A}\left[\left|\Phi\left(-\frac{w(a')}{\beta \cdot \sqrt{s}}\right) - \Phi\left(-\frac{w(a)}{\beta \cdot \sqrt{s}}\right)\right|\right] + 2\varphi(4) \cdot \frac{\log^{1.5} s}{\sqrt{s}} \\
&\leq \mathop{\mathrm{E}}_{a' \leftarrow A}\left[\left|\int_{\frac{w(a)}{\beta \cdot \sqrt{s}}}^{\frac{w(a')}{\beta \cdot \sqrt{s}}} e^{-\frac{t^2}{2}} dt\right|\right] + 2\varphi(4) \cdot \frac{\log^{1.5} s}{\sqrt{s}} \\
&\leq \mathop{\mathrm{E}}_{a' \leftarrow A}\left[\left|\frac{w(a')}{\beta \cdot \sqrt{s}} - \frac{w(a)}{\beta \cdot \sqrt{s}}\right|\right] + 2\varphi(4) \cdot \frac{\log^{1.5} s}{\sqrt{s}} \\
&= \mathop{\mathrm{E}}_{a' \leftarrow A}\left[\left|\frac{\sigma(a')}{\beta \cdot \sqrt{s}} - \frac{\sigma(a)}{\beta \cdot \sqrt{s}}\right|\right] + 2\varphi(4) \cdot \frac{\log^{1.5} s}{\sqrt{s}} \\
&\leq \mathop{\mathrm{E}}_{a' \leftarrow A}\left[\frac{|\sigma(a)| + |\sigma(a')|}{\beta \cdot \sqrt{s}}\right] + 2\varphi(4) \cdot \frac{\log^{1.5} s}{\sqrt{s}} \\
&= \frac{|\sigma(a)| + \mathrm{E}_{v \leftarrow (\mathcal{C}_\varepsilon)^{\beta \cdot s}}[|\sigma(v)|]}{\beta \cdot \sqrt{s}} + 2\varphi(4) \cdot \frac{\log^{1.5} s}{\sqrt{s}} \\
&\leq \frac{|\sigma(a)| + 2\sqrt{\beta \cdot s}}{\beta \cdot \sqrt{s}}.
\end{aligned}$$

The second transition holds by Equation (63), the penultimate one holds since $\mathrm{E}_{a' \leftarrow A}[|\sigma(a')|] = \mathrm{E}_{v \leftarrow (\mathcal{C}_\varepsilon)^{\beta \cdot s}}[|\sigma(v)|]$ and the last one by Proposition 2.3. □

The following proposition, which wraps the main analysis of this section, bounds how much $\mathsf{ratio}_h(a)$ can be far from 1.

Proposition 4.25. *For every $h \in \mathcal{H}^*$ and $a \in \mathcal{A}^*$, it holds that*

$$|1 - \mathsf{ratio}_h(a)| \leq \lambda \sqrt{\log s \cdot \frac{\alpha}{\beta}} \cdot \frac{|\sigma(a)| + \sqrt{\beta \cdot s}}{\sqrt{\beta \cdot s}},$$

for some universal constant $\lambda > 0$.

Proof. By Lemma 4.21 it holds that

$$\frac{1}{\mathsf{ratio}_h(a)} \in \mathop{\mathrm{E}}_{a' \leftarrow A | a' \in \mathcal{A}^*}\left[e^{(\varepsilon_{a'} - \varepsilon_a) \cdot \left(w(h) - \frac{\varepsilon_{a'} + \varepsilon_a}{2} \cdot \alpha \cdot s\right)}\right] \cdot (1 \pm \mathsf{error}),$$

for $\mathsf{error} = \max_{a', a'' \in \mathcal{A}^*, z \in \pm |\varepsilon_{a'}^4 - \varepsilon_{a''}^4|} \left|e^{\frac{\varepsilon_{a'}^3 - \varepsilon_{a''}^3}{3} \cdot w(h) + z \cdot \alpha \cdot s} - 1\right|$. Recall that $\varepsilon_{a'} = \widehat{\mathcal{C}}_s^{-1}(\Pr[B=1 \mid A=a'])$, for every $a' \in \mathcal{A}^*$, where $\Pr[B=1 \mid A=a'] = a' = \widehat{\mathcal{HG}}_{\beta \cdot s, w(a'), s}(0)$. Therefore, Proposition 2.8 yields that

$$\begin{aligned}
\varepsilon_{a'} &\in \frac{\frac{w(a') \cdot s}{\beta \cdot s}}{\sqrt{s \cdot s \cdot (1 - \frac{s}{\beta \cdot s})}} \pm \frac{\log^2 s}{2s} \\
&= \frac{w(a')}{\beta \cdot s \cdot \sqrt{1 - \frac{1}{\beta}}} \pm \frac{\log^2 s}{2s},
\end{aligned} \tag{64}$$

for every $a' \in \mathcal{A}^*$, which yields that

$$\begin{aligned} |\varepsilon_{a'}| &\leq \frac{|w(a')|}{\beta \cdot s} + \frac{\log^2 s}{s} \\ &= \frac{|\varepsilon \cdot \beta \cdot s + \sigma(a')|}{\beta \cdot s} + \frac{\log^2 s}{s} \\ &\leq 10 \cdot \sqrt{\frac{\log s}{s}}, \end{aligned} \tag{65}$$

where the second inequality holds by the bound on $|\varepsilon|$ and $|\sigma(a')|$. Therefore, for every $a', a'' \in \mathcal{A}^*$ and $z \in \pm \left|\varepsilon_{a'}^4 - \varepsilon_{a''}^4\right|$, it holds that

$$\begin{aligned} \left|\frac{\varepsilon_{a'}^3 - \varepsilon_{a''}^3}{3} \cdot w(h) + z \cdot \alpha \cdot s\right| &\leq \frac{|\varepsilon_{a'}|^3 + |\varepsilon_{a''}|^3}{3} \cdot w(h) + |z| \cdot \alpha \cdot s \\ &\leq \frac{2000}{3} \cdot \frac{\log^{1.5} s}{s^{1.5}} \cdot \left(10 \cdot \sqrt{\frac{\log s}{s}} \cdot \alpha \cdot s + 4\sqrt{\log s \cdot \alpha \cdot s}\right) + 20000 \cdot \frac{\log^2 s}{s^2} \cdot \alpha \cdot s \\ &\leq 2700 \cdot \frac{\log^2 s}{\sqrt{s}} + 27000 \cdot \log^2 s \cdot \frac{\alpha}{s} \\ &\leq 27000 \cdot \log^2 s \cdot \frac{\alpha + \sqrt{s}}{s} \\ &\leq 1, \end{aligned} \tag{66}$$

where the second inequality holds by the bounds on $|\varepsilon_{a'}|$, $|\varepsilon_{a''}|$ and $|w(h)|$, and the last one holds by assumption 2. This yields that

$$\begin{aligned} \mathsf{error} &= \max_{a', a'' \in \mathcal{A}^*, z \in \pm\left|\varepsilon_{a'}^4 - \varepsilon_{a''}^4\right|} \left| e^{\frac{\varepsilon_{a'}^3 - \varepsilon_{a''}^3}{3} \cdot w(h) + z \cdot \alpha \cdot s} - 1 \right| \\ &\leq \max_{a', a'' \in \mathcal{A}^*, z \in \pm\left|\varepsilon_{a'}^4 - \varepsilon_{a''}^4\right|} 2 \cdot \left| \frac{\varepsilon_{a'}^3 - \varepsilon_{a''}^3}{3} \cdot w(h) + z \cdot \alpha \cdot s \right| \\ &\leq 54000 \cdot \log^2 s \cdot \frac{\alpha + \sqrt{s}}{s}, \end{aligned} \tag{67}$$

where the first inequality holds since $e^a \in 1 \pm 2|a|$ for every $a \in [-1, 1]$, and the second one holds by Equation (66).

In addition, note that

$$\begin{aligned} w(h) &= \mathop{\mathrm{E}}_{a' \leftarrow A}[\varepsilon_{a'}] \cdot \alpha \cdot s + \sigma(h) \\ &\in \mathop{\mathrm{E}}_{a' \leftarrow A}[\varepsilon_{a'}] \cdot \alpha \cdot s \pm 4 \cdot \sqrt{\log s \cdot \alpha \cdot s} \\ &\in \left(\frac{\mathrm{E}_{a' \leftarrow A}[w(a')]}{\beta \cdot s \cdot \sqrt{1 - \frac{1}{\beta}}} \pm \frac{\log^2 s}{s}\right) \cdot \alpha \cdot s \pm 4 \cdot \sqrt{\log s \cdot \alpha \cdot s} \\ &\in \left(\frac{\varepsilon \cdot \beta \cdot s \pm 4\sqrt{\log s \cdot \beta \cdot s}}{\beta \cdot s \cdot \sqrt{1 - \frac{1}{\beta}}} \pm \frac{\log^2 s}{s}\right) \cdot \alpha \cdot s \pm 4 \cdot \sqrt{\log s \cdot \alpha \cdot s} \end{aligned} \tag{68}$$

where the third equality holds by Equation (64). Therefore, for every $a' \in \mathcal{A}^*$, it holds that

$$
\begin{aligned}
&(\varepsilon_{a'} - \varepsilon_a) \cdot \left(w(h) - \frac{\varepsilon_{a'} + \varepsilon_a}{2} \cdot \alpha \cdot s \right) \qquad (69)\\
&\in \frac{w(a)' - w(a) \pm \beta \cdot \log^2 s}{\beta \cdot s \cdot \sqrt{1 - \frac{1}{\beta}}} \cdot \left(w(h) - \frac{w(a) + w(a') \pm \beta \cdot \log^2 s}{2 \cdot \beta \cdot s \cdot \sqrt{1 - \frac{1}{\beta}}} \cdot \alpha \cdot s \right)\\
&\in \frac{\sigma(a)' - \sigma(a) \pm \beta \cdot \log^2 s}{\beta \cdot s \cdot \sqrt{1 - \frac{1}{\beta}}} \cdot \left(\frac{\sigma(a) + \sigma(a') \pm \beta \cdot \log^2 s}{2 \cdot \beta \cdot s \cdot \sqrt{1 - \frac{1}{\beta}}} \cdot \alpha \cdot s \pm 4 \cdot \sqrt{\log s \cdot \alpha \cdot s} \right)\\
&\in \frac{\sigma(a)' - \sigma(a) \pm \beta \cdot \log^2 s}{\beta \cdot s \cdot \sqrt{1 - \frac{1}{\beta}}} \cdot \left(\frac{\pm 9 \cdot \sqrt{\log s \cdot \beta \cdot s}}{2 \cdot \beta \cdot \sqrt{1 - \frac{1}{\beta}}} \cdot \alpha \pm 4 \cdot \sqrt{\log s \cdot \alpha \cdot s} \right)\\
&\in \frac{\sigma(a)' - \sigma(a) \pm \beta \cdot \log^2 s}{\beta \cdot s \cdot \sqrt{1 - \frac{1}{\beta}}} \cdot \left(\pm \frac{\alpha}{\beta} \cdot 5 \cdot \sqrt{\log s \cdot \beta \cdot s} \pm 4 \cdot \sqrt{\log s \cdot \alpha \cdot s} \right)\\
&\in \frac{\sigma(a)' - \sigma(a) \pm \beta \cdot \log^2 s}{\beta \cdot s} \cdot \left(\pm 8 \cdot \sqrt{\log s \cdot \alpha \cdot s} \right)\\
&= \frac{\sigma(a)' - \sigma(a) \pm \beta \cdot \log^2 s}{\sqrt{\beta \cdot s}} \cdot \left(\pm 8 \cdot \sqrt{\log s \cdot \frac{\alpha}{\beta}} \right),
\end{aligned}
$$

where the first transition holds by Equation (64), the second one holds by Equation (68) and the third one holds since $a, a' \in \mathcal{A}^*$.

By the bounds on $|\sigma(a)|, |\sigma(a')|$ and by assumption 3, it holds that

$$
\left| (\varepsilon_{a'} - \varepsilon_a) \cdot \left(w(h) - \frac{\varepsilon_{a'} + \varepsilon_a}{2} \cdot \alpha \cdot s \right) \right| \leq 1,
$$

for every $a' \in \mathcal{A}^*$. Hence,

$$
\begin{aligned}
\frac{1}{\mathsf{ratio}_h(a)} &\in \mathop{\mathrm{E}}_{a' \leftarrow A | a' \in \mathcal{A}^*} \left[e^{(\varepsilon_{a'} - \varepsilon_a) \cdot \left(w(h) - \frac{\varepsilon_{a'} + \varepsilon_a}{2} \cdot \alpha \cdot s \right)} \right] \cdot (1 \pm \mathsf{error}) \qquad (70)\\
&\in \mathop{\mathrm{E}}_{a' \leftarrow A | a' \in \mathcal{A}^*} \left[1 \pm 16 \cdot \frac{|\sigma(a)| + |\sigma(a')| + \beta \cdot \log^2 s}{\sqrt{\beta \cdot s}} \cdot \sqrt{\log s \cdot \frac{\alpha}{\beta}} \right] \cdot (1 \pm \mathsf{error})\\
&\in \left(1 \pm 16 \cdot \frac{|\sigma(a)| + \sqrt{\beta \cdot s} + \beta \cdot \log^2 s}{\sqrt{\beta \cdot s}} \cdot \sqrt{\log s \cdot \frac{\alpha}{\beta}} \right) \cdot \left(1 \pm 54000 \cdot \log^2 s \cdot \frac{\alpha + \sqrt{s}}{s} \right)\\
&\in \left(1 \pm 18 \cdot \frac{|\sigma(a)| + \sqrt{\beta \cdot s}}{\sqrt{\beta \cdot s}} \cdot \sqrt{\log s \cdot \frac{\alpha}{\beta}} \right),
\end{aligned}
$$

where the second transition holds by Equation (69) and since $e^a \in 1 \pm 2|a|$ for every $a \in [-1, 1]$, the third one holds by Proposition 2.3 and the last one holds by assumptions 2 and 3.

By assumption 3 and since $a \in \mathcal{A}^*$ and $\frac{1}{1 \pm a} \subseteq 1 \pm 2a$ for every $a \in (-0.5, 0.5)$, we deduce from Equation (70) that

$$
\mathsf{ratio}_h(a) \in \left(1 \pm 36 \cdot \frac{|\sigma(a)| + \sqrt{\beta \cdot s}}{\sqrt{\beta \cdot s}} \cdot \sqrt{\log s \cdot \frac{\alpha}{\beta}} \right). \qquad (71)
$$

Thus

$$|1 - \mathsf{ratio}_h(a)| \leq 36\sqrt{\log s \cdot \frac{\alpha}{\beta}} \cdot \frac{|\sigma(a)| + \sqrt{\beta \cdot s}}{\sqrt{\beta \cdot s}}$$

□

The following proposition combines Proposition 4.24 and Proposition 4.25 in order to achieve a bound on the prediction advantage $\Gamma_{\mathsf{P},f}(h)$ for "typical" values of h.

Proposition 4.26. *For every $h \in \mathcal{H}^*$ such that $\Pr[A \notin \mathcal{A}^* \mid f(A) = h] \leq \frac{1}{s^2}$, it holds that*

$$\Gamma_{\mathsf{P},f}(h) \leq \lambda\sqrt{\log s} \cdot \frac{\sqrt{\alpha}}{\beta},$$

for a universal constant $\lambda > 0$.

Proof. Compute

$$\begin{aligned}
\Gamma_{\mathsf{P},f}(h) &\leq \mathop{\mathrm{E}}_{a \leftarrow \mathcal{A}^*}\left[|\Pr[B = 1] - \Pr[B = 1 \mid A = a]| \cdot |1 - \mathsf{ratio}_h(a)|\right] + \frac{2}{s^2} \\
&\leq \mathop{\mathrm{E}}_{a \leftarrow \mathcal{A}^*}\left[\left(\frac{|\sigma(a)| + 2\sqrt{\beta \cdot s}}{\beta \cdot \sqrt{s}}\right) \cdot \left(\lambda'\sqrt{\log s \cdot \frac{\alpha}{\beta}} \cdot \frac{|\sigma(a)| + \sqrt{\beta \cdot s}}{\sqrt{\beta \cdot s}}\right)\right] + \frac{2}{s^2} \\
&= \lambda'\sqrt{\log s} \cdot \frac{\sqrt{\alpha}}{\beta} \cdot \mathop{\mathrm{E}}_{a \leftarrow \mathcal{A}^*}\left[\frac{|\sigma(a)|^2 + 3\,|\sigma(a)| \cdot \sqrt{\beta \cdot s} + 2 \cdot \beta \cdot s}{\beta \cdot s}\right] + \frac{2}{s^2} \\
&= \lambda'\sqrt{\log s} \cdot \frac{\sqrt{\alpha}}{\beta} \cdot \mathop{\mathrm{E}}_{v \leftarrow (\mathcal{C}_\varepsilon)^{\beta \cdot s}}\left[\frac{|\sigma(v)|^2 + 3\,|\sigma(v)| \cdot \sqrt{\beta \cdot s} + 2 \cdot \beta \cdot s}{\beta \cdot s}\right] + \frac{2}{s^2} \\
&\leq \lambda'\sqrt{\log s} \cdot \frac{\sqrt{\alpha}}{\beta} \cdot 6 + \frac{2}{s^2} \\
&\leq 7\lambda'\sqrt{\log s} \cdot \frac{\sqrt{\alpha}}{\beta}.
\end{aligned}$$

The first inequality holds by Lemma 4.15 and since $\Pr[A \notin \mathcal{A}^* \mid f(A) = h] \leq \frac{1}{s^2}$ and $\Pr[A \notin \mathcal{A}^*] \leq \frac{1}{s^2}$ by Fact 2.1 (Hoeffding's inequality), the second one holds by Propositions 4.24 and 4.25, and the third one holds by Proposition 2.3. □

We are finally ready to prove Lemma 4.10.

Proving Lemma 4.10.

Proof of Lemma 4.10. We divide the proof into two case

Case $\delta \notin [\frac{1}{s^4}, 1 - \frac{1}{s^4}]$. Assume that $\delta \in [0, \frac{1}{s^4}]$, where the proof of the case $\delta \in [1 - \frac{1}{s^4}, 1]$ is analogous. Assume by contradiction that

$$\Pr_{h \leftarrow f(A)}\left[\Gamma_{\mathsf{P},f}(h) > \frac{1}{s}\right] > \frac{1}{s^2} \tag{72}$$

Therefore,

$$\begin{aligned}
2\delta &= \Pr[B=1] + \mathop{\mathrm{E}}_{h\leftarrow f(A)}[\Pr[B=1 \mid f(A)=h]] \\
&\geq \mathop{\mathrm{E}}_{h\leftarrow f(A)}[|\Pr[B=1] - \Pr[B=1 \mid f(A)=h]|] \\
&\geq \frac{1}{s^3},
\end{aligned}$$

in contradiction to the assumption that $\delta \in [0, \frac{1}{s^4}]$. The proof immediately follows by Equation (72) since $\frac{1}{s} < \frac{\sqrt{\alpha}}{\beta}$ by assumption 1 of Lemma 4.10.

Case $\delta \in [\frac{1}{s^4}, 1-\frac{1}{s^4}]$**.** Let $\mathcal{H} := \{h \in \mathcal{H}^* \mid \Pr[A \notin \mathcal{A}^* \mid f(A)=h] \leq \frac{1}{s^2}\}$. Assume by contradiction that $\Pr_{h\leftarrow f(A)}\left[\Pr[A \notin \mathcal{A}^* \mid f(A)=h] > \frac{1}{s^2}\right] > \frac{1}{2s^2}$. Then

$$\begin{aligned}
&\Pr[A \notin \mathcal{A}^*] \\
&\geq \Pr_{h\leftarrow f(A)}\left[A \notin \mathcal{A}^* \mid \Pr[A \notin \mathcal{A}^* \mid f(A)=h] > \frac{1}{s^2}\right] \cdot \Pr_{h\leftarrow f(A)}\left[\Pr[A \notin \mathcal{A}^* \mid f(A)=h] > \frac{1}{s^2}\right] \\
&\geq \frac{1}{s^2} \cdot \frac{1}{2s^2} = \frac{1}{2s^4},
\end{aligned}$$

In contradiction to Hoeffding's inequality (Fact 2.1). Hence,

$$\Pr_{h\leftarrow f(A)}\left[\Pr[A \notin \mathcal{A}^* \mid f(A)=h] > \frac{1}{s^2}\right] \leq \frac{1}{2s^2} \tag{73}$$

It follows that

$$\Pr[f(A) \notin \mathcal{H}] \leq \Pr[f(A) \notin \mathcal{H}^*] + \Pr_{h\leftarrow f(A)}\left[\Pr[A \notin \mathcal{A}^* \mid f(A)=h] > \frac{1}{s^2}\right] \leq \frac{1}{s^2},$$

where the last inequality hold by Equation (73) and Fact 2.1 (Hoeffding's inequality). The proof now follows by Proposition 4.26. □

5 Bounding Online-Binomial Games via Linear Programs

In this section we show how to bound online binomial games via a linear programming. In Section 5.1 we give additional notations and facts related to an online Binomial games (hereafter, a Binomial game). In Section 5.2 we present a linear program whose feasible solution set characterizes all valid strategies for an adversary. In Section 5.4 we construct a feasible dual solution that bounds the binomial game that is relevant for our work.

5.1 Facts About Binomial Games

We first restate the following definitions from Section 3.2.2.

Definition 5.1 (online binomial games – Restatement of Definition 3.16)**.** *Let $m \in \mathbb{N}$, $\varepsilon \in [-1,1]$, and f be a randomized function over $[m] \times \mathbb{Z} \times \mathbb{Z}$. The m-*round online binomial game *$\mathsf{G}_{m,\varepsilon,f}$ is the random variable $\mathsf{G}_{m,\varepsilon,f} = \{C_1, \ldots, C_m, f\}$, where for every $i \in [m]$, $C_i \leftarrow \mathcal{C}_{(m-i+1)^2,\varepsilon}$. We refer to each C_i as the i'*th round coins*, and to f as the* hint *function.*

Definition 5.2 (game bias – Restatement of Definition 3.17)**.** *Let* $\mathsf{G} = \mathsf{G}_{m,\varepsilon,f} = \{C_1, \ldots, C_m, f\}$ *be an* m*-round online binomial game. For* $i \in \{1, \ldots, m\}$*, let* $S_i = \sum_{j=1}^{i} C_j$*, letting* $S_0 = 0$*. For* $i \in \{1, \ldots, m\}$*, let* $H_i = f(i, S_{i-1}, C_i)$*, let* $\delta_i(b) = \Pr[S_m \geq 0 \mid S_{i-1} = b]$*, let* $\delta_i(b, h) = \Pr[S_m \geq 0 \mid S_{i-1} = b,\ H_i = h]$*, let* $O_i = \delta_i(S_{i-1}, H_i)$*, and let* $O_i^- = \delta_i(S_{i-1})$*. Let also* $O_{m+1} = O_{m+1}^- = 1$ *if* $S_m \geq 0$*, and let* $O_{m+1} = O_{m+1}^- = 0$ *if* $S_m < 0$*.*

For an algorithm B*, let* I *be the first round in which* B *outputs* 1 *in the following* m*-round process: in round* i*, algorithm* B *is getting input* (S_{i-1}, H_i) *and outputs a* $\{0,1\}$*-value. Let* $I = m + 1$ *if* B *never outputs a one. The* bias B gains in G *is defined by*

$$\mathsf{Bias}_{\mathsf{B}}(\mathsf{G}) = \left| \mathrm{E}\left[O_I - O_I^-\right] \right|$$

The bias of G *is defined by* $\mathsf{Bias}_{m,\varepsilon,f} = \mathsf{Bias}(\mathsf{G}) = \max_{\mathsf{B}}\{\mathsf{Bias}_{\mathsf{B}}(\mathsf{G})\}$*, where the maximum is over* all *possible algorithms* B*.*

Let $\mathsf{G}_{m,\varepsilon,f} = \{C_1, \ldots, C_m, f\}$ be a Binomial game. In the following it will convenient to identify a round of the game by the number of rounds left until the game ends. Thus, referring the i-th round of G_m, as *level* $m - i + 1$. For any level $\ell \in [m]$, let $D_\ell = C_{m-\ell+1}$, and let $\mathsf{rem}(\ell) = (\ell - 1)^2 + \ldots + 1^2 = O(\ell^3)$ be the remaining coins when at level ℓ.

We define two types of events/states. A *no-hint state* $\langle \ell, b \rangle$ corresponds to the event that $S_{m-\ell} = b$. A *with-hint state* $\langle \ell, b, h \rangle$ corresponds to the event that $\langle \ell, b \rangle$ happens and $H_{m-\ell+1} = h$. In some cases, we abuse notation and refer to state $u = \langle \ell, b, h \rangle$ as the tuple (ℓ, b, h). For a set of states S, let $\Pr[S]$ be $\Pr\left[\bigcup_{u \in S} u\right]$. For a *with-hint state* $u = \langle \ell, b, h \rangle$ or *no-hint state* $u = \langle \ell, b \rangle$, let ℓ be the *level* of u, and b be the *offset* of u. For two states u, v, we write $u < v$ to indicate that u occurred in an earlier round. For a *with-hint state* $u = \langle \ell, b, hint \rangle$, let $u^- = \langle \ell, b \rangle$ be the corresponding *no-hint state* . For *no-hint state* $u = \langle \ell, b \rangle$, u^- is the same as u.

The final *no-hint state* $\langle 0, b \rangle$ is referred to as a f_b. In particular, $f_{\text{-}1}$ be the final state with *offset* -1. Let F^{pos} be the set of all *final states* with positive *offset* . Let $\widehat{V}$ be the union of all *with-hint state* and final states. Given some state u (*with-hint state* or *no-hint state*), let $c_u := \Pr[F^{pos} \mid u^-]$, and $v_u := \Pr[F^{pos} \mid u]$.

The following proposition allows us to focus on *stateless* deterministic algorithms.

Definition 5.3 (stateless online algorithm)**.** *A an online algorithm is* stateless*, if on input* x *it replies with* $f(x)$ *for some predetermined randomized function* f *(i.e., same function for all inputs, independent of previous inputs it answered). We sometimes refer to stateless online algorithms as strategies.*

Proposition 5.4. *For any online-binomial binomial game* G*, it holds that* $\mathsf{Bias}(\mathsf{G}) = \max_{\mathsf{T}}\{\mathsf{Bias}_{\mathsf{T}}(\mathsf{G})\}$*, where the maximum is over* all *possible deterministic stateless online algorithms* T*.*

Proof. For any algorithm B it holds that:

$$\mathsf{Bias}_{\mathsf{B}}(\mathsf{G}) = \left| \mathrm{E}\left[O_I - O_I^-\right] \right| = \max(\mathrm{E}\left[O_I - O_I^-\right], \mathrm{E}\left[O_I^- - O_I\right])$$

In the following proof we assume without loss of generality that all algorithms B under consideration are *positively aimed*, so for such algorithms $\mathrm{E}\left[O_I - O_I^-\right] \geq 0$, and hence $\mathsf{Bias}_{\mathsf{B}}(\mathsf{G}) = \mathrm{E}\left[O_I - O_I^-\right]$. The case where $\mathrm{E}\left[O_I - O_I^-\right] \leq 0$, is similar.

We start with putting a few notations. For $i \in [m]$, $b \in \mathrm{Supp}(S_{i-1})$ and $h \in \mathrm{Supp}(H_i)$, let $\langle i, b, h\rangle$ be the event that $S_{i-1} = b$, and $H_i = h$. We refer to $\langle i, b, h\rangle$ as an i-th round state.[23] For $i \in [m]$, a vector of integers $\mathbf{c} = (c_1, \ldots, c_{i-1})$, a vector of hints $\mathbf{h} = \langle h_1, \ldots, h_{i-1}\rangle$, and h_i a hint, let $\langle i, \mathbf{c}, \mathbf{h}, h_i\rangle$ be the event that $(C_1 \ldots, C_{i-1}) = (c_1, \ldots, c_{i-1})$ and $(H_1, \ldots, H_i) = (h_1, \ldots, h_i)$. We refer to $\langle i, \mathbf{c}, \mathbf{h}, h_i\rangle$ as an i-th round *augmented-state*. Namely, an augmented-state have the entire history of the coins and hints of previous rounds, and the hint of current round. For an augmented-state $s = \langle i, \mathbf{c}, \mathbf{h}, h_i\rangle$, let $\lfloor s \rfloor$ be the corresponding state, that is $\lfloor s \rfloor = \langle i, \mathsf{sum}(c), h_i\rangle$, where $\mathsf{sum}(c)$ is simply the sum of all $\mathbf{c}$'s entries. For $i \in [m]$, let $\mathcal{S}\mathsf{tate}_i$ be the set of all i-th round states, and let $\mathcal{A}\mathsf{ugState}_i$ be all the i-th round augmented-states.

The next step is to extend Definition 5.2, and define the bias of an algorithm that starts "playing" in some specific augmented-state/state of the binomial game G. For an algorithm B and a j-th round state/augmented-state s, define the *bias* B *gains in* G *when started in* s as follows. Using the same notations and terminology as in Definition 5.2, define I_j to be the minimal round greater or equal to j in which algorithm B outputs 1, letting $I_j = m + 1$, if no such round exists. the *bias* B *gains in* G *when started in* s is:

$$\mathsf{Bias}_{\mathsf{B}}(s) = \left|\mathrm{E}\left[O_{I_j} - O^-_{I_j} \mid s\right]\right|.$$

Namely, this is the bias B gains in a game in which the augmented-state/state $s = \langle j, \cdots\rangle$ happened, and it is only allowed to abort at step j or after.

Consider the function opt that given a triplet (i, b, h) as input, where $1 \le i \le m$, $b \in \mathrm{Supp}(S_{i-1})$ and $h \in \mathrm{Supp}(H_i)$, outputs a value in $[0, 1]$ according to the following recursive definition:

$$\mathsf{opt}(i, b, h) = \begin{cases} \max(\delta_m(b) - \delta_m(b, h)\ , 0) & i = m, \\ \max(\delta_i(b) - \delta_i(b, h), \sum_{b', h'} \mathsf{opt}(i + 1, b', h') \cdot \Pr\left[\langle i + 1, b', h'\rangle \mid \langle i, b, h\rangle\right]) & i < m. \end{cases}$$

For a state $u = \langle i, b, h\rangle$, let $\mathsf{opt}(u)$ stands for $\mathsf{opt}(i, b, h)$.

The following claim states that starting from an augmented-state s, the best possible bias that can be achieved by an algorithm is $\mathsf{opt}(\lfloor s \rfloor)$

Claim 5.5. *For an augmented-state $s = \langle i, \mathbf{c}, \mathbf{h}, h\rangle$ and algorithm B, it holds that*

$$\mathsf{Bias}_{\mathsf{B}}(s) \le \mathsf{opt}(\lfloor s \rfloor).^{24} \tag{74}$$

Proof. Fix an algorithm B. The proof is by induction on i, starting from $i = m$. Let $s = \langle m, \mathbf{c}, \mathbf{h}, h\rangle$ be an m-th round augmented-state. Conditioned that B aborts at round $i = m$, the bias it gains is $\delta_m(\mathsf{sum}(c)) - \delta_m(\mathsf{sum}(c), h)$. Conditioned that B does not aborts at round m, the bias it gains is 0. Since, by definition, B gains nothing in the game started in s conditioned it aborted before round m, it follows $\mathsf{Bias}_{\mathsf{B}}(s) \le \mathsf{opt}(i, \mathsf{sum}(c), h)$.

Assume that Equation (74) holds for all i-th round augmented-states. Let $s = \langle i - 1, \mathbf{c}, \mathbf{h}, h\rangle$ be an $(i - 1)$-th round augmented-state. Conditioned that B aborts at round i, the bias it gains is

[23] This definition of state, done for notational convince, overrides previous definition of state, and holds only for this proof (previous definition of state was $\langle \ell, b, h\rangle$, where ℓ is the level, i.e., the number of rounds till the end of the game).

[24] I.e., $\mathsf{Bias}_{\mathsf{B}}(s) \le \mathsf{opt}(i, \mathsf{sum}(c), h))$.

$\delta_{i-1}(\mathsf{sum}(c)) - \delta_{i-1}(\mathsf{sum}(c), h) \leq \mathsf{opt}(i-1, \mathsf{sum}(c), h)$. Conditioned that B does not abort at round i or earlier, it holds that

$$\begin{aligned}
\mathsf{Bias}_{\mathsf{B}}(s) &= \sum_{s' \in \mathcal{A}\mathsf{ugState}_i} \mathsf{Bias}_{\mathsf{B}}(s') \cdot \Pr\left[s' \mid s\right] && (75)\\
&= \sum_{s' \in \mathcal{A}\mathsf{ugState}_i} \mathsf{Bias}_{\mathsf{B}}(s') \cdot \Pr\left[\lfloor s' \rfloor \mid \lfloor s \rfloor\right] && (76)\\
&\leq \sum_{s' \in \mathcal{S}\mathsf{tate}_i} \mathsf{opt}(\lfloor s' \rfloor) \cdot \Pr\left[\lfloor s' \rfloor \mid \lfloor s \rfloor\right] && (77)\\
&= \mathsf{opt}(\lfloor s \rfloor) && (78)
\end{aligned}$$

Equation (75) is immediate by the definition of Bias. Equation (76) holds since if s' is an i-th round augmented-state, and s is an $(i-1)$-th round augmented-state, then $\Pr[s' \mid s] = \Pr[\lfloor s' \rfloor \mid \lfloor s \rfloor]$. Equation (77) is by the induction hypothesis, and Equation (78) is by the definition of opt. □

The following claim bounds the bias of a game, using the opt function.

Claim 5.6. *It holds that*

$$\mathsf{Bias}(G) \leq \mathrm{E}\left[\mathsf{opt}(1, 0, H_1)\right].$$

Proof. Let B be an algorithm, and let $\langle 1, h\rangle = \langle 1, \emptyset, \emptyset, h\rangle$ be a first's round augmented-state. By definition, it holds that

$$\mathsf{Bias}_{\mathsf{B}}(G) = \mathrm{E}\left[\mathsf{Bias}_{\mathsf{B}}(\langle 1, H_1\rangle)\right] \tag{79}$$

By Claim 5.5, and the fact that $\lfloor \langle 1, h\rangle \rfloor = \langle 1, 0, h\rangle$, we get:

$$\mathsf{Bias}_{\mathsf{B}}(G) = \mathrm{E}\left[\mathsf{Bias}_{\mathsf{B}}(\langle 1, H_1\rangle)\right] \leq \mathrm{E}\left[\mathsf{opt}(1, 0, H_1)\right].$$

Since the above holds for any algorithm B, we concludes that $\mathsf{Bias}(G) \leq \mathrm{E}\left[\mathsf{opt}(1, 0, H_1)\right]$. □

To conclude the proof, we show that there exists a deterministic strategy (i.e., a *stateless algorithm*) T that achieves the above bound, that is: $\mathsf{Bias}_{\mathsf{T}}(\mathsf{G}) = \mathrm{E}\left[\mathsf{opt}(1, 0, H_1)\right]$. Consider the following strategy.

Algorithm 5.7 (Greedy)**.**

Input: Round $i \in [m]$, sum of previous coins $b \in \mathrm{Supp}(S_{i-1})$, and hint $h \in \mathrm{Supp}(H_i)$.

Operation:

1. *if* $(\delta_i(b) - \delta_i(b, h) \geq \mathsf{opt}(i, b, h))$
   return 1.
2. *otherwise*
   return 0.

The next claim is a major step towards proving that the strategy Greedy achieves the optimal bias.

Claim 5.8. *For every state $s = \langle i, b, h\rangle$, it holds that* $\mathsf{Bias}_{\mathsf{Greedy}}(s) = \mathsf{opt}(s)$.

Proof. We prove by induction on $i \in [m]$, starting from $i = m$. Let $b \in S_{m-1}$, and let $h_m \in \mathrm{Supp}(H_m)$. If $\delta_m(b) - \delta_m(b, h) \leq 0$, then by definition of opt it holds that $\mathsf{opt}(m, b, h) = 0$. By construction of Greedy we get that $\mathsf{Greedy}(m, b, h) = 0$, hence also $\mathsf{Bias}_{\mathsf{Greedy}}(s) = 0$. If on the other hand $\delta_m(b) - \delta_m(b, h) > 0$, then by definition of opt it holds that $\mathsf{opt}(m, b, h) = \delta_m(b) - \delta_m(b, h)$. By construction of Greedy we get that $\mathsf{Greedy}(m, b, h) = 1$, hence also $\mathsf{Bias}_{\mathsf{Greedy}}(s) = \delta_m(b) - \delta_m(b, h)$, and the base case of the induction follows.

Assume the claim holds for all $(i + 1)$-th round states. Let $s = \langle i, b, h\rangle$ be an i-th round state. If $\delta_i(b) - \delta_i(b, h) < \mathsf{opt}(i, b, h)$, then by construction $\mathsf{Greedy}(i, b, h) = 0$. Hence,

$$\begin{aligned}
\mathsf{Bias}_{\mathsf{Greedy}}(s) &= \sum_{n \in \mathcal{S}\mathsf{tate}_{i+1}} \mathsf{Bias}_{\mathsf{Greedy}}(n) \cdot \Pr[n \mid s] \\
&= \sum_{n \in \mathcal{S}\mathsf{tate}_{i+1}} \mathsf{opt}(n) \cdot \Pr[n \mid s] && (80) \\
&= \mathsf{opt}(s) && (81)
\end{aligned}$$

Equation (80) is by the induction hypothesis, and Equation (81) is by the definition of the opt function.

If on the other hand $\delta_i(b) - \delta_i(b, h) \geq \mathsf{opt}(i, b, h)$, then $\mathsf{Greedy}(i, b, h) = 1$. Hence, $\mathsf{Bias}_{\mathsf{Greedy}}(s) = \delta_i(b) - \delta_i(b, h)$. Thus, by definition, it holds that $\mathsf{opt}(s) = \delta_i(b) - \delta_i(b, h)$, concluding the proof. □

By definition, for a strategy T it holds that

$$\mathsf{Bias}_{\mathsf{T}}(G) = \mathrm{E}\left[\mathsf{Bias}_{\mathsf{T}}(\langle 1, 0, H_1\rangle)\right]$$

Applying it to strategy Greedy, and using Claim 5.8, we dedcuce that

$$\mathsf{Bias}_{\mathsf{Greedy}}(G) = \mathrm{E}\left[\mathsf{Bias}_{\mathsf{Greedy}}(\langle 1, 0, H_1\rangle)\right] = \mathrm{E}\left[\mathsf{opt}(1, 0, H_1)\right].$$

To conclude, the bias achieved by Greedy is the optimal bias, and since Greedy is a deterministic stateless algorithm, the claim follows. □

In the following when bounding the bias a player B gains in an online binomial game, we assume without loss of generality that B it is stateless, and refer to such player as a strategy. We remark, that the following proof does not assume that B is deterministic. We first define the final state in which strategy T stops.

Definition 5.9 (Abort state)**.** *For a strategy* T*, let* U_{T} *be the* with-hint state *in which the strategy* T *aborts, or the* final state *that the game reached if no abort occurs.*

$$U_{\mathsf{T}} = \begin{cases} \langle \ell, b, h\rangle & \textit{if} \quad I_{\mathsf{T}} = m - \ell + 1, S_{m-\ell} = b, H_{m-\ell+1=h} \\ \langle 0, b\rangle & \textit{if} \quad I_{\mathsf{T}} = m + 1, S_m = b \end{cases}$$

Claim 5.10 (bias of strategy)**.** *For a* strategy T*, it holds that*

$$\mathsf{Bias}_{\mathsf{T}} = \sum_{u \in \widehat{V}} (c_u - v_u) \cdot \Pr[U_{\mathsf{T}} = u]$$

(P) $\max \sum_{v\in\widehat{V}} a_v \cdot (c_v - v_v)$		(D) $\min \sum_{u\in\widehat{V}} y_u \cdot \Pr[u]$	
s.t.		s.t.	
$a_v + \sum_{u\|u<v} a_u \cdot \Pr[v\|u] \le \Pr[v]$	$\forall v \in \widehat{V}$	$y_u + \sum_{v\|u<v} y_v \cdot \Pr[v\|u] \ge c_u - v_u$	$\forall u \in \widehat{V}$
$a_v \ge 0$	$\forall v \in \widehat{V}$	$y_u \ge 0$	$\forall u \in \widehat{V}$

Figure 1: Linear program and its dual for the Binomial game $\mathsf{G}_{m,\varepsilon,f}$

Proof.

$$\begin{aligned}
\mathsf{Bias}_{\mathsf{T}} &= \mathrm{E}\left[\delta_{I_{\mathsf{T}}}(S_{I_{\mathsf{T}}-1}) - \delta_{I_{\mathsf{T}}}(S_{I_{\mathsf{T}}-1}, H_{I_{\mathsf{T}}})\right] \\
&= \sum_{i=1}^{m}\sum_{b}\sum_{h}(\delta_i(b) - \delta_i(b,h)) \cdot \Pr\left[I_{\mathsf{T}} = i, S_{i-1} = b, H_i = h\right] \\
&= \sum_{i=1}^{m}\sum_{b}\sum_{h}(\Pr\left[S_m \ge 0 \mid S_{i-1} = b\right] - \Pr\left[S_m \ge 0 \mid S_{i-1} = b, H_i = h\right]) \cdot \Pr\left[U_{\mathsf{T}} = \langle i, b, h\rangle\right] \\
&= \sum_{u\in\widehat{V}}(c_u - v_u) \cdot \Pr\left[U_{\mathsf{T}} = u\right]
\end{aligned}$$

□

5.2 The Linear Program

In this section we present a linear program which we show characterizes *all* possible strategies S of the adversary in the binomial game. The linear program captures not only deterministic strategies, but any strategy, including probabilistic strategies. Thus, finding the best strategy for the adversary is equivalent to finding the optimal solution to the linear program. The linear program and its dual appear in Figure 1. The primal LP has variables a_v for every *with-hint state* v that represent the probability that the strategy aborts at state v. The LP is, of course, specific for each family of binomial games under consideration (with its specific states, number of rounds etc.). The following two lemmas show that the linear program exactly characterizes all feasible strategies for the adversary.

Lemma 5.11 (Strategy to LP solution)**.** *Let T be an adversarial strategy for the m-round binomial game $\mathsf{G}_{m,\varepsilon,f}$. For any $v \in \widehat{V}$ let a_v^{T} be the probability that the strategy aborts at state v, where probability is taken over the randomness of both the game and possibly the strategy (formally, $a_v^{\mathsf{T}} = \Pr\left[U_{\mathsf{T}} = v\right]$) . Then, a_v^{T} is a feasible solution to the linear program. Moreover, the objective value $\sum_{v\in\widehat{V}} a_v^{\mathsf{T}} \cdot (c_v - v_v)$ is the bias obtained by strategy T.*

Proof. Let T be an m-round strategy. Obviously, $a_v^{\mathsf{T}} \ge 0$. Using Claim 5.10, we have:

$$\mathsf{Bias}_{\mathsf{T}} = \sum_{v\in\widehat{V}} a_v^{\mathsf{T}} \cdot (c_v - v_v)$$

Next, we prove that for every states $u < v$, given that u occurred, the events: v, and $U_{\mathsf{T}} = u$, are independent. Formally:

$$\Pr\left[v \mid U_{\mathsf{T}} = u, u\right] = \Pr\left[v \mid u\right] \tag{82}$$

Assume u belong to the i-th round, and v belong to the j-th round, and denote: $u = \langle m - i + 1, b_u, h_u \rangle$ and $v = \langle m - j + 1, b_v, h_v \rangle$. Given that the game visits $u = \langle m - i + 1, b_u, h_u \rangle$, the random variables $C_1, \ldots, C_i$ as well as the hints at rounds 1 to i are constants. In this case the event that the adversary decides to terminate at round u ($U_\mathsf{T} = u$) depends only on the random coins tossed by the adversary. On the other hand, given that the game visits u, the event that the game visits $v = \langle m - j + 1, b_v, h_v \rangle$ depends on the random variables $C_i, \ldots, C_j$ (note, however, that the random variable C_i depends on the hint at round i and therefore on the state u). Since the above two random sources are disjoint, we conclude that the events are independent. Thus, we have:

$$\begin{aligned}
\Pr[v] &\geq \sum_{u \leq v} \Pr[v \mid U_\mathsf{T} = u] \cdot \Pr[U_\mathsf{T} = u] && (83)\\
&= \sum_{u \leq v} \Pr[v \mid U_\mathsf{T} = u, u] \cdot \Pr[U_\mathsf{T} = u] && (84)\\
&= \sum_{u \leq v} \Pr[v \mid u] \cdot a_u^\mathsf{T} && (85)\\
&= a_v^\mathsf{T} + \sum_{u < v} a_u^\mathsf{T} \cdot \Pr[v|u]
\end{aligned}$$

Inequality (83) follows by total probability on disjoint events (without the probability that T does not abort until v's round). Equality (84) is due that the event $U_\mathsf{T} = u$ is contained in u. Equality (85) is due Equation (82). Thus, the variables satisfy the main constraint.

□

Lemma 5.12 (LP solution to strategy)**.** *Let a_v for $v \in \widehat{V}$ be a feasible solution to (P). Let T be a strategy that aborts at state v with probability $\frac{a_v}{\Pr[v] - \sum_{u<v} a_u \cdot \Pr[v|u]}$ whenever the execution gets to state v and T did not abort in any previous state. Then, T is a valid strategy that achieves bias of $\sum_{v \in \widehat{V}} a_v \cdot (c_v - v_v)$.*

Proof. Let $\mathsf{T}(v) = \frac{a_v}{\Pr[v] - \sum_{u<v} a_u \cdot \Pr[v|u]}$. First, by the constraints of (P) $0 \leq \mathsf{T}(v) \leq 1$ and so the strategy define a valid conditional probability of stopping at state v. We prove by induction on the rounds that the strategy aborts at every state v with probability a_v. This immediately implies (from Claim 5.10) that the strategy has bias $\sum_{v \in \widehat{V}} a_v \cdot (c_v - v_v)$. For the first round the probability that the game visits v is $\Pr[v]$. Hence, the strategy aborts with probability $\Pr[v] \cdot \frac{a_v}{\Pr[v] - \sum_{u<v} a_u \cdot \Pr[v|u]} = \Pr[v] \cdot \frac{a_v}{\Pr[v]} = a_v$. For an arbitrary state v at round k we have,

$$\begin{aligned}
&\Pr[\mathsf{T} \text{ aborts at } v] = \mathsf{T}(v) \cdot \Pr[\text{game visits state } v \text{ and did not abort at any } u < v]\\
&= \mathsf{T}(v) \cdot \left(\Pr[\text{game visits state } v] - \sum_{u<v} \Pr[\text{game visits } v | S \text{ aborts at } u] \Pr[S \text{ aborts at } u] \right) && (86)\\
&= \mathsf{T}(v) \cdot \left(\Pr[\text{game visits state } v] - \sum_{u<v} \Pr[\text{game visits } v | \text{game visits } u] \Pr[S \text{ aborts at } u] \right) && (87)\\
&= \mathsf{T}(v) \cdot \left(\Pr[v] - \sum_{u<v} a_u \cdot \Pr[v|u] \right) = a_v && (88)
\end{aligned}$$

Equality (86) follows by total probability on disjoint events. Enequality (87) follows since given that the game visits u, the probability that the strategy aborts on state u is independent of the event that the game visits v (that depends on coins that are tossed at later rounds. Finally, Equality (88) follows by the induction hypothesis.

□

The following lemma is a direct implication of Lemma 5.11 along with weak duality.

Lemma 5.13 (Bound the Game Value)**.** *Let $\mathsf{G} = \mathsf{G}_{m,\varepsilon,f}$ be some Binomial game. Let $\{y_u \mid u \in \widehat{V}\}$ be a feasible solution to the dual LP (D) induced by G. Then,*

$$\mathsf{Bias}_{m,\varepsilon,f} \leq \sum_{u \in \widehat{V}} \Pr[u] \cdot y_u$$

Proof. Consider the primal-dual LPs defined in Figure 1. By Weak duality theorem the value of any feasible solution to the (D) is an upper bound on the value of any feasible solution to (P). By Lemma 5.11 for any positively aimed strategy T and any feasible solution $\{y_u \mid u \in \widehat{V}\}$ for (D),

$$\mathsf{Bias}_{\mathsf{T}} = \sum_{v \in \widehat{V}} a_v^{\mathsf{T}} \cdot (c_v - v_v) \leq \sum_{u \in \widehat{V}} y_u \cdot \Pr[u] \tag{89}$$

Thus, $\mathsf{Bias}_{m,\varepsilon,f} \leq \sum_{u \in \widehat{V}} \Pr[u] \cdot y_u$. □

5.3 Useful Tools

In this section we develop several useful tools, that are later used to analyze the dual-LP. We start with the intuitive claim that states that the best possible hint is the result of current coins.

Claim 5.14 (best possible hint)**.** *Let $\mathsf{G}_{m,\varepsilon,f} = \{C_1, \ldots, C_m, f\}$ be an m-round online Binomial game, where $f \colon [m] \times \mathbb{Z} \times \mathbb{Z} \to \mathcal{H}$. Let $\mathsf{G}' = \mathsf{G}'_{m,\varepsilon,f'}$ be the m-round online Binomial game, that uses the function f', where $f' : [m] \times \mathbb{Z} \times \mathbb{Z} \to \mathcal{H} \cup \{-\ell^2, \ldots, \ell^2\}$ is defined as follows:*

$$f'(i,b,z) = \begin{cases} z & \text{For } z \in Z' \subset Z \text{ [25]} \\ f(i,b,z) & \text{For } z \in Z \setminus Z' \end{cases}$$

Let $\{y_u\}_{u \in \widehat{V'}}$ be a feasible solution for the dual LP, induced by G'. Then there exist a feasible solution $\{x_u\}_{u \in \widehat{V}}$ for the dual LP induced by G, such that,

$$\sum_{u \in \widehat{V'}} \Pr[u] \cdot y_u = \sum_{u \in \widehat{V}} \Pr[u] \cdot x_u \tag{90}$$

Proof of Claim 5.14. The following proves the claim for a hint function f', that agrees with f on all *no-hint states* except of one. That is, $f'(i,b,z) = f(i,b,z)$ for all Z except one coordinate. The validity for any f' will follow by easy induction. So assume that f agree with f', on all *no-hint states* , except from $\langle \ell', b' \rangle$, and for every $z \in \mathbb{Z}$, $f'(\ell', b', z) = z$. Denote by $\langle \ell, b \rangle^+ := \{\langle \ell, b, h \rangle \mid h \in \mathcal{H}\}$ that is the set of all *with-hint states* with corresponding *no-hint state* : $\langle \ell, b \rangle$. We define the the solution for the dual-LP induced by G, to be:

$$x_u = \begin{cases} \sum_{i=-\ell^2}^{\ell^2} \quad y_{\langle \ell', b', i \rangle} \cdot \Pr[D_{\ell'} = i \mid u] & \text{if} \quad u = \langle \ell', b', h \rangle, h \in \mathcal{H} \\ y_u & \text{otherwise} \end{cases}$$

We start by proving that the target function has the same value in both LPs. Indeed for every $u = \langle \ell, b, h \rangle$, where $\langle \ell, b \rangle \neq \langle \ell', b' \rangle$, we have $\Pr[u] \cdot y_u = \Pr[u] \cdot x_u$, hence those states contribute the same to the sums in Equation (90). We calculate:

$$\begin{aligned}
\sum_{h \in \mathcal{H}} \Pr\left[\langle \ell', b', h \rangle\right] \cdot x_u &= \sum_{h \in \mathcal{H}} \Pr\left[\langle \ell', b', h \rangle\right] \cdot \sum_{i=-\ell^2}^{\ell^2} y_{\langle \ell', b', i \rangle} \cdot \Pr\left[D_{\ell'} = i \mid \langle \ell', b', h \rangle\right] \\
&= \sum_{i=-\ell^2}^{\ell^2} y_{\langle \ell', b', i \rangle} \cdot \sum_{h \in \mathcal{H}} \Pr\left[\langle \ell', b', h \rangle\right] \cdot \Pr\left[D_{\ell'} = i \mid \langle \ell', b', h \rangle\right] \\
&= \sum_{i=-\ell^2}^{\ell^2} y_{\langle \ell', b', i \rangle} \cdot \Pr\left[\langle \ell', b' \rangle, D_{\ell'} = i\right]
\end{aligned}$$

So we conclude that states of the type $\langle \ell', b', \cdot \rangle$ contribute the same to the sums in Equation (90), hence Equation (90) follows.

Next, we prove the that $\{x_u\}_{u \in \widehat{V}}$ is a feasible solution for the dual-LP induced by G. Constraints relevant to states $\langle \ell, b, h \rangle$, with $\ell < \ell'$, or $\ell = \ell'$, and $b \neq b'$, are trivially satisfied because they look the same in the LP induced by G'. Consider now states of the form $\langle \ell', b', h \rangle$:

$$\begin{aligned}
& x_{\langle \ell', b', h \rangle} + \sum_{v > \langle \ell', b', h \rangle} x_v \cdot \Pr\left[v \mid \langle \ell', b', h \rangle\right] \\
&= \sum_{i=-\ell^2}^{\ell^2} y_{\langle \ell', b', i \rangle} \cdot \Pr\left[D_{\ell'} = i \mid \langle \ell', b', h \rangle\right] + \sum_{v > \langle \ell', b', h \rangle} y_v \cdot \Pr\left[v \mid \langle \ell', b', h \rangle\right] \\
&= \sum_{i=-\ell^2}^{\ell^2} y_{\langle \ell', b', i \rangle} \cdot \Pr\left[D_{\ell'} = i \mid \langle \ell', b', h \rangle\right] + \\
&\qquad + \sum_{v > \langle \ell', b', h \rangle} y_v \cdot \sum_{i=-\ell^2}^{\ell^2} \Pr\left[v \mid D_{\ell'} = i, \langle \ell', b', h \rangle\right] \cdot \Pr\left[D_{\ell'} = i \mid \langle \ell', b', h \rangle\right] \\
&= \sum_{i=-\ell^2}^{\ell^2} \Big(y_{\langle \ell', b', i \rangle} \cdot \Pr\left[D_{\ell'} = i \mid \langle \ell', b', h \rangle\right] + \\
&\qquad + \Pr\left[D_{\ell'} = i \mid \langle \ell', b', h \rangle\right] \cdot \sum_{v > \langle \ell', b', h \rangle} y_v \cdot \Pr\left[v \mid D_{\ell'} = i, \langle \ell', b', h \rangle\right] \Big)
\end{aligned} \tag{91}$$

Continuing from Equation (91) we get

$$
\begin{aligned}
&= \sum_{i=-\ell^2}^{\ell^2} \Pr\left[D_{\ell'} = i \mid \langle \ell', b', h\rangle\right] \cdot \left(y_{\langle \ell', b', i\rangle} + \sum_{v > \langle \ell', b', h\rangle} y_v \cdot \Pr\left[v \mid D_{\ell'} = i, \langle \ell', b', h\rangle\right] \right) \\
&= \sum_{i=-\ell^2}^{\ell^2} \Pr\left[D_{\ell'} = i \mid \langle \ell', b', h\rangle\right] \cdot \left(y_{\langle \ell', b', i\rangle} + \sum_{v > \langle \ell', b', h\rangle} y_v \cdot \Pr\left[v \mid D_{\ell'} = i, \langle \ell', b'\rangle\right] \right) \qquad (92) \\
&= \sum_{i=-\ell^2}^{\ell^2} \Pr\left[D_{\ell'} = i \mid \langle \ell', b', h\rangle\right] \cdot \left(y_{\langle \ell', b', i\rangle} + \sum_{v > \langle \ell', b', i\rangle} y_v \cdot \Pr\left[v \mid D_{\ell'} = i, \langle \ell', b'\rangle\right] \right) \\
&\geq \sum_{i=-\ell^2}^{\ell^2} \Pr\left[D_{\ell'} = i \mid \langle \ell', b', h\rangle\right] \cdot \left(\Pr\left[F^{pos} \mid \langle \ell', b'\rangle\right] - \Pr\left[F^{pos} \mid \langle \ell', b'\rangle, D_{\ell'} = i\right] \right) \qquad (93) \\
&= \Pr\left[F^{pos} \mid \langle \ell', b'\rangle\right] \cdot \sum_{i=-\ell^2}^{\ell^2} \Pr\left[D_{\ell'} = i \mid \langle \ell', b', h\rangle\right] - \\
&\qquad - \sum_{i=-\ell^2}^{\ell^2} \Pr\left[F^{pos} \mid \langle \ell', b', h\rangle, D_{\ell'} = i\right] \cdot \Pr\left[D_{\ell'} = i \mid \langle \ell', b', h\rangle\right] \qquad (94) \\
&= \Pr\left[F^{pos} \mid \langle \ell', b'\rangle\right] - \Pr\left[F^{pos} \mid \langle \ell', b', h\rangle\right]
\end{aligned}
$$

Where Equality (92), and Equality (94) we used the fact that $\Pr\left[v \mid D_{\ell'} = i, \langle \ell', b'\rangle\right] = \Pr\left[v \mid D_{\ell'} = i, \langle \ell', b', h\rangle\right]$ (Intuitively, once we know the value of $D_{\ell'}$, the hint h gives us no more information), and in Inequality (93) we use the feasibility of the solution $\{y_u\}_{u \in \widehat{V'}}$. The feasibility for states $\langle \ell, b', h\rangle$ for $\ell > \ell'$ involves same kind of computation, and we omit it. □

Recall that S is a set of states. In the following we abuse notation and write $\Pr[S]$ instead of $\Pr\left[\bigcup_{u \in S} u\right]$.

Claim 5.15 (low profit states)**.** *Let $\delta > 0$ be a positive constant. Let S be a set of* with-hint states *such that $S \subset \{u = \langle \ell, b, h\rangle \mid c_u - v_u \leq \delta \ , \ \ell \neq 0\}$. Then, there are values y_u ($u \in S$) such that $\sum_{u \in S} y_u \cdot \Pr[u] \leq \delta \cdot \Pr[S]$ and for every state $u \in S$: $y_u + \sum_{v \in S \ : \ v > u} y_v \cdot \Pr[v|u] \geq c_u - v_u$.*

Proof. Fix some δ, and S. Denote by S^i, all the states from S, that belong to level i. Define y_u to be:

$$
y_u = \begin{cases} \delta & \text{if } u \in S^1 \\ \delta \cdot \Pr[\overline{S^{i-1}}, \ldots, \overline{S^1} \mid u] & \text{if } u \in S^i \text{ for } i > 1 \end{cases}
$$

Where $\overline{S^i}$ are all states that are not in S^i. Take some state $u \in S^i$. We have:

$$
\begin{aligned}
y_u + \sum_{v \in S \ : \ v > u} y_v \cdot \Pr[v|u] &= \delta \cdot \Pr[\overline{S^{i-1}}, \ldots, \overline{S^1} \mid u] + \sum_{j<i} \sum_{v \in S^j} \delta \cdot \Pr[\overline{S^{j-1}}, \ldots, \overline{S^1} \mid v] \cdot \Pr[v|u] \\
&= \delta \cdot (\Pr[\overline{S^{i-1}}, \ldots, \overline{S^1} \mid u] + \sum_{j<i} \Pr[S^j, \overline{S^{j-1}}, \ldots, \overline{S^1} \mid u]) \\
&= \delta \geq c_u - v_u
\end{aligned}
$$

Also we have:

$$\begin{aligned}
\sum_{u\in S}\Pr[u]\cdot y_u &= \sum_{i=1}^{m}\sum_{u\in S^i}\delta\cdot\Pr[\overline{S^{i-1}},\ldots,\overline{S^1}\mid u]\cdot\Pr[u]\\
&= \sum_{i=1}^{m}\sum_{u\in S^i}\delta\cdot\Pr[u,\overline{S^{i-1}},\ldots,\overline{S^1}]\\
&= \sum_{i=1}^{m}\delta\cdot\Pr[S^i,\overline{S^{i-1}},\ldots,\overline{S^1}]\\
&= \delta\cdot\Pr[S^m\cup\ldots\cup S^1]\\
&= \delta\cdot\Pr[S]
\end{aligned}$$

□

Claim 5.16 ($\frac{1}{m}$-profit states)**.** *Let* $\mathsf{G}_{m,\varepsilon,f}=\{C_1,\ldots,C_m,f\}$ *be an* m*-round online Binomial game with* $|\varepsilon|\le\frac{4\cdot\sqrt{\log m}}{m\sqrt{m}}$*, and for every* $\langle i,b\rangle\in[m,\mathbb{Z}]$*, such that* $|b+\varepsilon\cdot\mathsf{rem}(\ell)|\ge 4\sqrt{\log m\cdot\mathsf{rem}(\ell)}$*, and every* $z\in\mathbb{Z}$*,* $f(i,b,z)=z$ [26]*. Let* $S:=S_{pos}\cup S_{neg}$ *the set of states such that,*

$$\begin{aligned}
S_{pos} &:= \{\langle\ell,b,h\rangle\ :\ b+\varepsilon\cdot\mathsf{rem}(\ell)\ge 4\sqrt{\log m\cdot\mathsf{rem}(\ell)}\ ,\ -\sqrt{\log m\cdot\mathsf{rem}(\ell)}\le h\}\\
S_{neg} &:= \{\langle\ell,b,h\rangle\ :\ b+\varepsilon\cdot\mathsf{rem}(\ell)\le -4\sqrt{\log m\cdot\mathsf{rem}(\ell)}\ ,\ h\le\sqrt{\log m\cdot\mathsf{rem}(\ell)}\}
\end{aligned}$$

Then for every $u\in S$ *we have:*

$$c_u-v_u=O(\frac{1}{m})$$

Proof. We prove that claim for $u\in S_{pos}$. The case of $u\in S_{neg}$ can be done similarly. Let $u=\langle\ell,b,h\rangle\in S_{pos}$ be such a state. For $\ell\in[m]$, let $X_\ell=D_{\ell-1}+\ldots+D_1$ (informally, X_ℓ is the sum of the remaining coins to be toss after level ℓ). Finally, let $\mathsf{HBound}:=\sqrt{\log m\cdot\mathsf{rem}(\ell)}$. We have:

$$\begin{aligned}
c_u-v_u &= \Pr[X_\ell+D_\ell>-b]-\Pr[X_\ell+h>-b]\\
&= \sum_i\Pr[X_\ell+i>-b]\cdot\Pr[D_\ell=i]-\sum_i\Pr[X_\ell+h>-b]\cdot\Pr[D_\ell=i]\\
&= \sum_i(\Pr[X_\ell+i>-b]-\Pr[X_\ell+h>-b])\cdot\Pr[D_\ell=i]\\
&\le \sum_i(1-\Pr[X_\ell>-(b+h)])\cdot\Pr[D_\ell=i]\\
&= \sum_i(\Pr[X_\ell\le-(b+h)])\cdot\Pr[D_\ell=i]\\
&\le \Pr[X_\ell\le-(b-\mathsf{HBound})]\\
&= \Pr[X_\ell-\varepsilon\cdot\mathsf{rem}(\ell)\le-(b-\mathsf{HBound}+\varepsilon\cdot\mathsf{rem}(\ell))]\\
&\le 2\cdot e^{-\frac{((b+\varepsilon\cdot\mathsf{rem}(\ell))-\mathsf{HBound})^2}{2\cdot\mathsf{rem}(\ell)}}
\end{aligned}$$

[26] For such $\langle i,b\rangle$, f output current round coins.

Where the final inequality follows by Fact 2.1. We will show that,

$$e^{-\frac{((b+\varepsilon\cdot\mathsf{rem}(\ell))-\mathsf{HBound})^2}{2\cdot\mathsf{rem}(\ell)}} \leq \frac{1}{m}$$

Simplifying, we get that we should show that,

$$2\cdot\mathsf{rem}(\ell)\cdot\log m + 2(b+\varepsilon\cdot\mathsf{rem}(\ell))\cdot\mathsf{HBound} \leq (b+\varepsilon\cdot\mathsf{rem}(\ell))^2 + \mathsf{HBound}^2 \tag{95}$$

To conclude we prove that:

$$2\cdot\mathsf{rem}(\ell)\cdot\log m + 2(b+\varepsilon\cdot\mathsf{rem}(\ell))\cdot\mathsf{HBound} \leq (b+\varepsilon\cdot\mathsf{rem}(\ell))^2$$

The above holds since: $\mathsf{HBound} = \sqrt{\log m\cdot\mathsf{rem}(\ell)} \leq \frac{1}{4}\cdot(b+\varepsilon\cdot\mathsf{rem}(\ell))$, hence $2(b+\varepsilon\cdot\mathsf{rem}(\ell))\cdot\mathsf{HBound} \leq \frac{1}{2}\cdot(b+\varepsilon\cdot\mathsf{rem}(\ell))^2$. Also since $2\sqrt{\log m\cdot\mathsf{rem}(\ell)} \leq b+\varepsilon\cdot\mathsf{rem}(\ell)$, we get that $2\log m\cdot\mathsf{rem}(\ell) \leq \frac{1}{2}\cdot(b+\varepsilon\cdot\mathsf{rem}(\ell))^2$, so Inequality (95) holds. □

Claim 5.17 (Trivially Stisfaction)**.** *Let $u = \langle\ell, b, h\rangle$ be a non* final state *. Let $\{y_v\}_{v\in\widehat{V}}$ be any assignment to the dual variables, where for each $v \in F^{pos}$, $y_v \geq 1$, and $y_u \geq c_u - v_u$. Then the dual constraint of state u, is satisfied. That is:*

$$y_u + \sum_{v:\ v>u} y_v\cdot\Pr[v|u] \geq c_u - v_u$$

Proof. Immediately from $y_u \geq c_u - v_u$. □

Claim 5.18 (marginal states)**.** *Let $\mathsf{G}_{m,\varepsilon,f} = \{C_1,\ldots,C_m,f\}$ be an m-round online Binomial game such that $|\varepsilon| \leq \frac{4\sqrt{\log m}}{m\sqrt{m}}$. Let $S := \{u = \langle\ell,b,h\rangle\ :\ |b+\varepsilon\cdot\mathsf{rem}(\ell)| \geq 4\sqrt{\log m\cdot\mathsf{rem}(\ell)}\}$. Then, there exists an assignment of values y_u for $u \in S$, that satisfies:*

$$\sum_{u\in S} y_u\cdot\Pr[u] \leq O(\frac{1}{m}) \tag{96}$$

$$y_u + \sum_{v\in S\ :\ v>u} y_v\cdot\Pr[v|u] \geq c_u - v_u \qquad \forall u\in S \tag{97}$$

Proof. By Claim 5.14 it enough to prove the claim for the case that the hint function f simply output the coins of current state. Define the following sets:

$$\begin{aligned}
S_{pos} &:= \{u = \langle\ell,b,h\rangle\ :\ b+\varepsilon\cdot\mathsf{rem}(\ell) \geq 4\sqrt{\log m\cdot\mathsf{rem}(\ell)},\ h \geq -\sqrt{\log m\cdot\mathsf{rem}(\ell)}\}\\
A_{pos} &:= \{u = \langle\ell,b,h\rangle\ :\ b+\varepsilon\cdot\mathsf{rem}(\ell) \geq 4\sqrt{\log m\cdot\mathsf{rem}(\ell)},\ h < -\sqrt{\log m\cdot\mathsf{rem}(\ell)}\}\\
S_{neg} &:= \{u = \langle\ell,b,h\rangle\ :\ b+\varepsilon\cdot\mathsf{rem}(\ell) \leq -4\sqrt{\log m\cdot\mathsf{rem}(\ell)},\ h \leq \sqrt{\log m\cdot\mathsf{rem}(\ell)}\}\\
A_{neg} &:= \{u = \langle\ell,b,h\rangle\ :\ b+\varepsilon\cdot\mathsf{rem}(\ell) \leq -4\sqrt{\log m\cdot\mathsf{rem}(\ell)},\ h > \sqrt{\log m\cdot\mathsf{rem}(\ell)}\}
\end{aligned}$$

Obviously $S = S_{pos}\cup S_{neg}\cup A_{pos}\cup A_{neg}$. Also note that S_{pos}, and S_{neg}, are the same as in Claim 5.16. We prove the claim for every $u \in A_{pos}\cup S_{pos}$. The proof for $S_{neg}\cup A_{neg}$ can be done similarly. Start with S_{pos}. We define y_u for $u \in S_{pos}$, according to Claim 5.15, with $\delta = O(\frac{1}{m})$. By Claim 5.16 we

know that for each $u \in S_{pos}$, $c_u - v_u \leq O(\frac{1}{m})$. For $u \in A_{pos}$, define $y_u := c_u - v_u$. By Claim 5.17, Equation (97) holds. It is left to prove Equation (96) where summation is over A_{pos}.

We start with lower bounding the following expression:

$$\begin{aligned}
\sqrt{\log m \cdot \mathsf{rem}(\ell)} + \varepsilon \cdot \ell^2 &\geq \sqrt{\log m \cdot \mathsf{rem}(\ell)} - |\varepsilon| \cdot \ell^2 \\
&\geq \sqrt{\log m \cdot \mathsf{rem}(\ell)} - \frac{4\sqrt{\log m}}{m\sqrt{m}} \cdot \ell^2 \\
&\geq \sqrt{\log m} \cdot (\sqrt{\mathsf{rem}(\ell)} - 4\sqrt{\ell}) \\
&\geq \sqrt{\log m} \cdot \ell^{1.25} \qquad (98)
\end{aligned}$$

Before we continue, recall that for a set of *with-hint states* W, $W^- := \{u^- \mid u \in W\}$, and W^ℓ is the set of W that are in level ℓ. For every $\langle \ell, b \rangle \in A^-_{pos}$, the following holds:

$$\begin{aligned}
\Pr\left[\langle \ell, b, h \rangle \in A^\ell_{pos} \mid \langle \ell, b \rangle\right] &= \Pr\left[D_\ell < -\sqrt{\log m \cdot \mathsf{rem}(\ell)}\right] \\
&= \Pr\left[D_\ell - \varepsilon \cdot \ell^2 < -(\sqrt{\log m \cdot \mathsf{rem}(\ell)} + \varepsilon \cdot \ell^2)\right] \\
&\leq 2 \cdot e^{-\frac{(\sqrt{\log m \cdot \mathsf{rem}(\ell)} + \varepsilon \ell^2)^2}{2\ell^2}} \qquad (99) \\
&\leq 2 \cdot e^{-\frac{(\sqrt{\log m} \cdot \ell^{1.25})^2}{2\ell^2}} \qquad (100) \\
&= 2 \cdot e^{-\frac{1}{2} \cdot \log(m) \cdot \sqrt{\ell}} \\
&\leq \frac{2}{m} \cdot e^{-\frac{\sqrt{\ell}}{2}} \qquad (101)
\end{aligned}$$

Where Inequality (99) follows by Fact 2.1, and Inequality (100) follows by Equation (98).

Now we perform our final calculation:

$$\begin{aligned}
\sum_{u \in A_{pos}} \Pr[u] \cdot y_u &= \sum_{u \in A_{pos}} \Pr[u] \cdot (c_u - v_u) \\
&\leq \sum_{u \in A_{pos}} \Pr[u] \\
&= \sum_{\langle \ell, b \rangle \in A^-_{pos}} \sum_{h < -\sqrt{\log m \cdot \mathsf{rem}(\ell)}} \Pr\left[\langle \ell, b, h \rangle\right] \qquad (102) \\
&= \sum_{\langle \ell, b \rangle \in A^-_{pos}} \sum_{h < -\sqrt{\log m \cdot \mathsf{rem}(\ell)}} \Pr[\langle \ell, b, h \rangle | \langle \ell, b \rangle] \cdot \Pr\left[\langle \ell, b \rangle\right] \\
&= \sum_{\langle \ell, b \rangle \in A^-_{pos}} \Pr[\langle \ell, b, h \rangle \in A_{pos} | \langle \ell, b \rangle] \cdot \Pr\left[\langle \ell, b \rangle\right] \\
&= \sum_{\ell} \sum_{\langle \ell, b \rangle \in (A^\ell_{pos})^-} \Pr[\langle \ell, b, h \rangle \in A^\ell_{pos} | \langle \ell, b \rangle)] \cdot \Pr\left[\langle \ell, b \rangle\right] \\
&\leq \sum_{\ell} \sum_{\langle \ell, b \rangle \in (A^\ell_{pos})^-} \frac{1}{m} \cdot e^{-\frac{\sqrt{\ell}}{2}} \cdot \Pr\left[\langle \ell, b \rangle\right] \qquad (103)
\end{aligned}$$

$$\leq \frac{1}{m} \cdot \sum_{\ell} e^{-\frac{\sqrt{\ell}}{2}} \cdot \sum_{\langle \ell, b \rangle \in (A^{\ell}_{pos})^{-}} \Pr\left[\langle \ell, b \rangle\right]$$
$$\leq \frac{1}{m} \cdot \sum_{\ell} e^{-\frac{\sqrt{\ell}}{2}} \cdot 1$$
$$= O(\frac{1}{m})$$

Where Equality (102) is simply by the definition of A_{pos}, and Inequality (103) is due Equation (101)

□

Claim 5.19 (final rounds 8)**.** *Let $\mathsf{G}_{m,\varepsilon,f} = \{C_1, \ldots, C_m, f\}$ be an m-round online Binomial game with $|\varepsilon| \leq \frac{4\sqrt{\log m}}{m\sqrt{m}}$. Let $S := \{u = \langle \ell, b, h \rangle \ : \ \ell \leq \sqrt[8]{m}\}$. Then there exists an assignment of values y_u for $u \in S$, that satisfies:*

$$\sum_{u \in S} y_u \cdot \Pr[u] \leq O(\frac{1}{m}) \tag{104}$$

$$y_u + \sum_{v \in S \ : \ v > u} y_v \cdot \Pr[v|u] \geq c_u - v_u \qquad \forall u \in S \tag{105}$$

Proof. Let $u = \langle \ell, b, h \rangle \in S$. By Claim 5.18 we may assume that

$$-4\sqrt{\log m \cdot \mathsf{rem}(\ell)} \leq b + \varepsilon \cdot \mathsf{rem}(\ell) \leq 4\sqrt{\log m \cdot \mathsf{rem}(\ell)}$$

For $u \in S$ we set $y_u = c_u - v_u$. By Claim 5.17 we know that Equation (105) holds. To prove Equation (104), we calculate:

$$\sum_{u \in S'} y_u \cdot \Pr[u] = \sum_{\ell \leq \sqrt[8]{m}} \sum_{b} (c_u - v_u) \cdot \Pr\left[\langle \ell, b \rangle\right]$$
$$\leq \sum_{\ell \leq \sqrt[8]{m}} \sum_{b} \Pr\left[\langle \ell, b \rangle\right]$$
$$= O(\frac{1}{m\sqrt{m}} \cdot \sqrt{\log m \cdot \mathsf{rem}(\sqrt[8]{m})} \cdot \sqrt[8]{m}) \leq O(\frac{1}{m})$$

□

Lemma 5.20. *Let $\mathsf{G}_{m,\varepsilon,f} = \{C_1, \ldots, C_m, f\}$ be an m-round online Binomial game with $|\varepsilon| \leq 4\sqrt{\frac{\log m}{\mathsf{sum}_m(1)}}$ and a hint function f that simply output currents round coins. Let $S := \{\langle \ell, b, h \rangle \ : \ |b + \varepsilon \cdot \mathsf{rem}(\ell)| \leq 4\sqrt{\log m \cdot \mathsf{rem}(\ell)}, \ m^{\frac{1}{8}} \leq \ell\}$. Then, for every $\langle \ell, b \rangle \in S^{-}$, there exists a set $\mathcal{H}_{\ell,b}$ such that the following two conditions hold:*

1. $$\sum_{h \notin \mathcal{H}_{\ell,b}} \Pr\left[\langle \ell, b, h \rangle \mid \langle \ell, b \rangle\right] \leq \frac{1}{m^2}$$

2. *For every $u = \langle \ell, b, h \rangle$ where $h \in \mathcal{H}_{\ell,b}$, the following holds:*

$$c_u - v_u \leq \lambda \cdot \ell \cdot \sqrt{\log(m)} \cdot \Pr\left[f_{-1} \mid u\right]$$

for some universal constant $\lambda > 0$.

Proof. Let $\langle \ell, b \rangle \in S^-$, let $i = m - \ell + 1$, let (A, B) be the variables of a $\big(m, i, b, \varepsilon\big)$-binomial two-step process (as defined in Definition 4.1) and let g be an all-information hint function for (A, B) (as defined in Definition 4.3). Since m, i, b and ε satisfy all the conditions of Lemma 4.7, it holds that there exists a set $\mathcal{H}_{\ell,b} \subseteq \mathrm{Supp}(f(A))$ such that

1. $\Pr\left[g(A) \notin \mathcal{H}_{\ell,b}\right] \leq \frac{1}{m^2}$
2. For every $h \in \mathcal{H}_{\ell,b}$,

$$\frac{\left|\Pr\left[B = 1\right] - \Pr\left[B = 1 \mid g(A) = h\right]\right|}{\Pr\left[\sum_{j=i}^{m} C_j = -(b+1)\right]} \leq \lambda \cdot \sqrt{\ell_m(i)} \cdot \sqrt{\log m},$$

   for some universal constant $\lambda > 0$.

The proof follows since $c_u - v_u = \left|\Pr\left[B = 1\right] - \Pr\left[B = 1 \mid g(A) = h\right]\right|$, $\Pr\left[f_{-1} \mid u\right] = \Pr\left[\sum_{j=i}^{m} C_j = -(b+1)\right]$ and since $\sqrt{\ell_m(i)} = \ell$. □

Claim 5.21 (final rounds)**.** *Let $\mathsf{G}_{m,\varepsilon,f} = \{C_1, \ldots, C_m, f\}$ be an m-round online Binomial game with $|\varepsilon| \leq \frac{4\sqrt{\log m}}{m\sqrt{m}}$. Let $S := \{u = \langle \ell, b, h \rangle \ : \ \ell \leq \gamma\}$ where $\gamma \in [m]$. Then, there exists an assignment to the variables y_u for $u \in S \cup \{f_{-1}\}$ that satisfies:*

$$\sum_{u \in S} y_u \cdot \Pr[u] \leq O(\frac{1}{m}) \tag{106}$$

$$y_{f_{-1}} \leq O(\gamma \cdot \sqrt{\log m}) \tag{107}$$

$$y_u + \sum_{v \in S \cup \{f_{-1}\} \ : \ v > u} y_v \cdot \Pr[v|u] \geq c_u - v_u \qquad \forall u \in S \tag{108}$$

Proof. By Claim 5.14 it enough to prove the claim for the case that the hint function f simply outputs the coins of current state. By Claim 5.18, and Claim 5.19 we can assume that the set S is actually: $S' := \{u = \langle \ell, b, h \rangle \ : \ m^{\frac{1}{8}} \leq \ell \leq \gamma \ , \ |b + \varepsilon \cdot \mathsf{rem}(\ell)| \leq 4\sqrt{\log m \cdot \mathsf{rem}(\ell)}\}$.

Next, by Lemma 5.20, we get that for every $\langle \ell, b \rangle \in S^-$, there exists a set $\mathcal{H}_{\ell,b}$ such that the following two conditions hold:

1. $$\sum_{h \notin \mathcal{H}_{\ell,b}} \Pr\left[\langle \ell, b, h \rangle \mid \langle \ell, b \rangle\right] \leq \frac{1}{m^2} \tag{109}$$

2. For every $u = \langle \ell, b, h \rangle$ where $h \in \mathcal{H}_{\ell,b}$, the following holds:

$$c_u - v_u \leq \lambda \cdot \ell \cdot \sqrt{\log(m)} \cdot \Pr\left[f_{-1} \mid u\right] \tag{110}$$

where λ is some universal constant.

Let,

$$\begin{aligned} L :=& \{u = \langle \ell, b, h \rangle \in S' \mid h \notin \mathcal{H}_{\ell,b},\ c_u - v_u > 0\ \} \\ \bar{L} :=& \{u = \langle \ell, b, h \rangle \in S' \mid h \in \mathcal{H}_{\ell,b}\} \end{aligned}$$

The assignment of values y_u for $u \in S' \cup \{f_{-1}\}$ is as follows. For state f_{-1} define $y_{f_{-1}} = \lambda \cdot \gamma \cdot \sqrt{\log m}$. For $u \in L$, define $y_u = c_u - v_u$. For all other states u, define $y_u = 0$. Equation (107) is satisfied trivially. To prove that Equation (106) holds we recall that L^ℓ is the set of all the states in L from level ℓ. We have:

$$\begin{aligned} \sum_{u \in L} \Pr[u] \cdot y_u &= \sum_{u \in L} \Pr[u] \cdot (c_u - v_u) \\ &\leq \sum_{u \in L} \Pr[u] \\ &= \sum_{\langle \ell, b \rangle \in L^-} \sum_{h \notin \mathcal{H}_{\ell,b}} \Pr\left[\langle \ell, b, h \rangle\right] \\ &= \sum_{\langle \ell, b \rangle \in L^-} \sum_{h \notin \mathcal{H}_{\ell,b}} \Pr\left[\langle \ell, b \rangle\right] \cdot \Pr\left[\langle \ell, b, h \rangle \mid \langle \ell, b \rangle\right] \\ &= \sum_{\langle \ell, b \rangle \in L^-} \Pr\left[\langle \ell, b \rangle\right] \sum_{h \notin \mathcal{H}_{\ell,b}} \Pr\left[\langle \ell, b, h \rangle \mid \langle \ell, b \rangle\right] \\ &\leq \sum_{\langle \ell, b \rangle \in L^-} \Pr\left[\langle \ell, b \rangle\right] \cdot \frac{1}{m^2} \qquad (111) \\ &= \frac{1}{m^2} \sum_{\ell} \sum_{\langle \ell, b \rangle \in (L^\ell)^-} \Pr\left[\langle \ell, b \rangle\right] \\ &\leq \frac{1}{m^2} \sum_{\ell} 1 = \frac{1}{m^2} \cdot m = O(\frac{1}{m}) \end{aligned}$$

Where Inequality (111) follows by Inequality (109). Thus, we conclude that Equation (106) holds.

We next prove the feasibility of this solution, for states in S' (Equation (108)). For states $u \in L$ it's immediate from Claim 5.17. For states $u \in \bar{L}$ we calculate:

$$\begin{aligned} c_u - v_u &\leq \lambda \cdot \ell \cdot \sqrt{\log(m)} \cdot \Pr\left[f_{-1} \mid u\right] \\ &\leq \lambda \cdot \gamma \cdot \sqrt{\log m} \cdot \Pr\left[f_{-1} \mid u\right] \\ &\leq y_{f_{-1}} \cdot \Pr\left[f_{-1} \mid u\right] \\ &\leq y_u + \sum_{v:\ v > u} y_v \cdot \Pr\left[v \mid u\right] \end{aligned}$$

Where the first Inequality follows by Inequality (110). □

Claim 5.22 (big ε)**.** *Let* $\mathsf{G}_{m,\varepsilon,f} = \{C_1, \ldots, C_m, f\}$ *be an* m*-round online Binomial game with* $|\varepsilon| \geq \frac{4\sqrt{\log m}}{m\sqrt{m}}$*. Then, there are values* y_u *(for* $u \in \hat{V}$*) such that,* $\sum_{u \in \hat{V}} y_u \cdot \Pr[u] \leq O(\frac{1}{m})$*, and for every state* $u \in S$*:* $y_u + \sum_{v \in \hat{V} \,:\, v > u} y_v \cdot \Pr[v|u] \geq c_u - v_u$*.*

Proof. We prove for $\varepsilon \geq \frac{4\sqrt{\log m}}{m\sqrt{m}}$. The proof for $\varepsilon \leq -\frac{4\sqrt{\log m}}{m\sqrt{m}}$ is equivalent. First, we have that,

$$\varepsilon^2 \cdot \mathsf{rem}(m) \geq (\frac{4\sqrt{\log m}}{m\sqrt{m}})^2 \cdot \mathsf{rem}(m) \geq 16 \cdot \log m \cdot \frac{\mathsf{rem}(m)}{m^3} \geq 4 \cdot \log m \tag{112}$$

Let F^{neg} be the union of all *final states* with negative *offset* . We have:

$$\begin{aligned}
\Pr\left[F^{neg}\right] &= \Pr\left[S_m \leq 0\right] = \Pr\left[S_m - \varepsilon \cdot \mathsf{rem}(m) \leq -\varepsilon \cdot \mathsf{rem}(m)\right] \\
&\leq \Pr\left[|S_m - \varepsilon \cdot \mathsf{rem}(m)| \geq \varepsilon \cdot \mathsf{rem}(m)\right] && (113) \\
&\leq 2 \cdot e^{-\frac{(\varepsilon \cdot \mathsf{rem}(m))^2}{2 \cdot \mathsf{rem}(m)}} \\
&\leq 2 \cdot e^{-\frac{1}{2} \cdot \varepsilon^2 \cdot \mathsf{rem}(m)} \\
&\leq 2 \cdot e^{-2 \log m} = \frac{2}{m^2} && (114)
\end{aligned}$$

Where Inequality (113) is by Fact 2.1, and Inequality (114) is by Equation (112). We conclude that $\Pr\left[F^{neg}\right] \leq \frac{2}{m^2}$.

Next we prove that $\Pr\left[\exists u \colon \Pr\left[F^{neg} \mid u\right] \geq \frac{1}{m}\right] \leq \frac{2}{m}$, where by "$\exists u \colon \Pr\left[F^{neg} \mid u\right] \geq \frac{1}{m}$" we mean the event that the game reaches a state u, such that $\Pr\left[F^{neg} \mid u\right] \geq \frac{1}{m}$. Assume to the contrary that $\Pr\left[\exists u \colon \Pr\left[F^{neg} \mid u\right] \geq \frac{1}{m}\right] > \frac{2}{m}$. We get:

$$\begin{aligned}
\Pr\left[F^{neq}\right] &\geq \Pr\left[F^{neq} \;\middle|\; \exists u \colon \Pr\left[F^{neg} \mid u\right] \geq \frac{1}{m}\right] \cdot \Pr\left[\exists u \colon \Pr\left[F^{neg} \mid u\right] \geq \frac{1}{m}\right] \\
&> \Pr\left[F^{neq} \;\middle|\; \exists u \colon \Pr\left[F^{neg} \mid u\right] \geq \frac{1}{m}\right] \cdot \frac{2}{m} \\
&\geq \frac{1}{m} \cdot \frac{2}{m} = \frac{2}{m^2}
\end{aligned}$$

Contradicting Inequality (114).

Denote $S := \{u \mid v_u < 1 - \frac{1}{m}\}$. The above calculation shows that $\Pr\left[S\right] \leq \frac{2}{m}$. Obviously for every $u \in S$, we have $c_u - v_u \leq \frac{1}{m}$. Define a solution for the dual LP as follow:

- For $u \notin S$, define y_u by Claim 5.15 with $\delta = \frac{1}{m}$.
- For $u \in S$, define y_u by Claim 5.15 with $\delta = 1$.

By Claim 5.15, the above solution is feasible. Also by the same claim, and the fact that $\Pr\left[S\right] \leq \frac{2}{m}$ we get that $\sum_u y_u \cdot \Pr[u] \leq O(\frac{1}{m})$ and thus the claim follows. □

5.4 Solving the Dual LP

By the preceding discussion in Section 5.2 any feasible solution to the dual linear program in Figure 1 upper bounds the profit of any adversary. In this section we construct a feasible dual solution with the desired properties.

Lemma 5.23. *[Solving the Dual LP - Big ε] Let $\mathsf{G}_{m,\varepsilon,f} = \{C_1, \ldots, C_m, f\}$ be some m-round online Binomial game, and assume $|\varepsilon| \geq 4\sqrt{\frac{\log m}{\mathsf{sum}_m(1)}}$ then $\mathsf{Bias}(\mathsf{G}) = O(\frac{1}{m})$.*

Proof of Lemma 5.23. By Lemma 5.13, it is enough to show a feasible solution $\{y_u\}$, of the dual-LP such that: $\sum_{u \in \widehat{V}} \Pr[u] \cdot y_u = O(\frac{1}{m})$. Since $|\varepsilon| > \frac{4\sqrt{\log m}}{m\sqrt{m}}$ it follows immediately from Claim 5.22. □

Lemma 5.24. *[Solving the Dual LP] Let $\mathsf{G}_{m,\varepsilon,f} = \{C_1, \ldots, C_m, f\}$ be an m-round online Binomial game, and assume $|\varepsilon| < 4\sqrt{\frac{\log m}{\mathsf{sum}_m(1)}}$. Let $\tau \in [m]$ be such that $\frac{\tau}{\sqrt{m}} \cdot \log^3(m) < 1$ and let*

$$S := \left\{ \langle \ell, b \rangle \ : \ |b + \varepsilon \cdot \mathsf{rem}(\ell)| \leq 4\sqrt{\log m \cdot \mathsf{rem}(\ell)}, \ \ell \geq \max\left(\left\lfloor m^{\frac{1}{8}} \right\rfloor, \tau^2 \log^3(m) \right), b + 1 \equiv \mathsf{rem}(\ell) \ (mod\ 2) \right\}$$

Assume that for every $\langle \ell, b \rangle \in S$, there exists a set $\mathcal{H}_{\ell,b}$ (of hints) such that the following conditions hold:

1. $$\sum_{h \notin \mathcal{H}_{\ell,b}} \Pr\left[\langle \ell, b, h \rangle \mid \langle \ell, b \rangle \right] \leq \frac{1}{m^2} \tag{115}$$

2. *For every $u = \langle \ell, b, h \rangle$, where $\langle \ell, b \rangle \in S$ and $h \in \mathcal{H}_{\ell,b}$, the following two condition holds:*

   (a)
   $$c_u - v_u \leq \lambda' \cdot \tau \cdot \sqrt{m \log m} \cdot \Pr\left[f_{-1} \mid u^- \right] \tag{116}$$
   where λ' is some universal constant.

   (b)
   $$\Pr\left[D_\ell > 9 \cdot \sqrt{\ell \cdot \log m} \ \mid \ \langle \ell, b, h \rangle \right] \leq \frac{\lambda''}{m^{12}} \tag{117}$$
   where λ'' is some universal constant.

Then $\mathsf{Bias}(\mathsf{G}) = O(\frac{\tau \cdot \sqrt{\log m}}{m})$.

Proof of Lemma 5.24. By Lemma 5.13, it is enough to show a feasible solution $\{y_u\}$, of the dual-LP such that: $\sum_{u \in \widehat{V}} \Pr[u] \cdot y_u = O(\frac{\tau\sqrt{\log m}}{m})$. We define the set S' as follows:

$$S' := \left\{ \langle \ell, b \rangle \ \mid \ |b + \varepsilon \cdot \mathsf{rem}(\ell)| \leq 4\sqrt{\log m \cdot \mathsf{rem}(\ell)}, \ \ell \geq \tau \cdot \sqrt{m}, \ b + 1 \equiv \mathsf{rem}(\ell) \ (mod\ 2) \right\}$$

Since $\frac{\tau}{\sqrt{m}} \cdot \log^3(m) < 1$, it follows that $\tau \cdot \log^3(m) < \sqrt{m}$. Hence if $\ell \geq \tau \cdot \sqrt{m}$, it implies that $\ell \geq \tau \cdot \sqrt{m} \geq \tau^2 \cdot \log^3(m)$, and so $\ell \geq \max\left(\left\lfloor m^{\frac{1}{8}} \right\rfloor, \tau^2 \log^3(m) \right)$. Hence we conclude that $S' \subseteq S$, and for the rest of the proof we use the properties guaranteed for S only for the states in S'.

We define the solution for the dual LP as follow:

1. For non final states $u = \langle \ell, b, h \rangle$, with: $\ell \leq \tau \cdot \sqrt{m}$, define y_u according to Claim 5.21 where $\gamma = \tau \cdot \sqrt{m}$.

2. For $u = f_{\text{-}1}$ (the *final state* with $b =$ -1) define $y_{f_{-1}}$ according to Claim 5.21 where $\gamma = \tau \cdot \sqrt{m}$, with the following enhancement. By (Equation (107)) we knows that

$$y_{f_{-1}} \leq O(\tau \cdot \sqrt{m} \cdot \sqrt{\log m}) \tag{118}$$

   Let λ be a constant s.t. $y_{f_{-1}} \leq \lambda \cdot \tau \cdot \sqrt{m} \cdot \sqrt{\log m})$. Define $\lambda^{\max} := \max(\lambda, \lambda', \lambda'')$. We define $y_{f_{-1}}$ to be $y_{f_{-1}} = \lambda^{\max} \cdot \tau \cdot \sqrt{m} \cdot \sqrt{\log m}$.[27]

3. For non final states $u = \langle \ell, b, h \rangle$, with: $\ell \geq \tau \cdot \sqrt{m}$, $\langle \ell, b \rangle \in S'$, and $h \notin \mathcal{H}_{\ell,b}$, and $c_u - v_u > 0$, take $y_u = c_u - v_u$.

4. For non final states $u = \langle \ell, b, h \rangle$, with: $\ell \geq \tau \cdot \sqrt{m}$, $\langle \ell, b \rangle \notin S'$, define y_u, according to Claim 5.18.

5. for all other states u in $\widehat{V}$, take $y_u = 0$.

We start by proving that:

$$\sum_{u \in \widehat{V}} \Pr[u] \cdot y_u = O(\frac{\tau \cdot \sqrt{\log m}}{m}) \tag{119}$$

By Proposition 2.2:

$$\Pr[f_{\text{-}1}] \cdot y_{f_{\text{-}1}} = O(\Pr[f_{\text{-}1}] \cdot \tau \cdot \sqrt{m} \cdot \sqrt{\log m}) = O(\frac{\tau \cdot \sqrt{\log m}}{m}) \tag{120}$$

By Claim 5.21, and by Claim 5.18, states u defined in case 2 or 4, contribute to the sum $O(\frac{1}{m})$. So, it remains to deal with states of the case 3. Define

$$L := \{u = \langle \ell, b, h \rangle \mid \langle \ell, b \rangle \in S', h \notin \mathcal{H}_{\ell,b},\ c_u - v_u > 0\ \}$$

[27] Since we only enlarged the value of $y_{f_{-1}}$ guaranteed to exist by Claim 5.21, we know that all levels up to $\gamma = \tau \cdot \sqrt{m}$ are covered.

Recall that L^ℓ is the set of all the states in L from level ℓ. We have:

$$\begin{aligned}
\sum_{u\in L}\Pr[u]\cdot y_u &= \sum_{u\in L}\Pr[u]\cdot(c_u - v_u)\\
&\le \sum_{u\in L}\Pr[u]\\
&= \sum_{\langle\ell,b\rangle\in L^-}\ \sum_{h\notin\mathcal{H}_{\ell,b}}\Pr\left[\langle\ell,b,h\rangle\right]\\
&= \sum_{\langle\ell,b\rangle\in L^-}\ \sum_{h\notin\mathcal{H}_{\ell,b}}\Pr\left[\langle\ell,b\rangle\right]\cdot\Pr\left[\langle\ell,b,h\rangle \mid \langle\ell,b\rangle\right]\\
&= \sum_{\langle\ell,b\rangle\in L^-}\Pr\left[\langle\ell,b\rangle\right]\sum_{h\notin\mathcal{H}_{\ell,b}}\Pr\left[\langle\ell,b,h\rangle \mid \langle\ell,b\rangle\right]\\
&\le \sum_{\langle\ell,b\rangle\in L^-}\Pr\left[\langle\ell,b\rangle\right]\cdot\frac{3}{m^2} \qquad (121)\\
&= \frac{3}{m^2}\sum_{\ell}\ \sum_{\langle\ell,b\rangle\in(L^\ell)^-}\Pr\left[\langle\ell,b\rangle\right]\\
&\le \frac{3}{m^2}\sum_{\ell}1 = \frac{3}{m^2}\cdot m = O(\frac{1}{m}) \qquad (122)
\end{aligned}$$

Where Inequality (121) is due to Equation (115). Combining Equation (122), and Equation (120), we conclude that Equation (119) holds.

We move now to prove the feasibility of our solution. For that, we need to show that for every state u, the following holds:

$$y_u + \sum_{v:\ v>u} y_v\cdot\Pr[v|u] \ge c_u - v_u$$

We divide the proof into 5 types of states u:

1. Final states: For final states u, with positive or negative *offset* we have $c_u - v_u = 0$, so the constraint holds.

2. For non final states $u = \langle\ell,b,h\rangle$, with $\ell \le \tau\cdot\sqrt{m}$: the feasibility follows immediately from Claim 5.21.

3. For non final states $u = \langle\ell,b,h\rangle$, with: $\ell \ge \tau\cdot\sqrt{m}$, and $\langle\ell,b\rangle \notin S'$, feasibility follows from Claim 5.18.

4. For non final states $u = \langle\ell,b,h\rangle$, with: $\ell \ge \tau\cdot\sqrt{m}$, $\langle\ell,b\rangle \in S'$, $h \notin \mathcal{H}_{i,b}$, and $c_u - v_u > 0$: follows immediately from Claim 5.17.

5. For non final states $u = \langle\ell,b,h\rangle$, with: $\ell \ge \tau\cdot\sqrt{m}$, $\langle\ell,b\rangle \in S'$, $h \in \mathcal{H}_{i,b}$, and $c_u - v_u > 0$, we prove below.

Consider some state $u = \langle\ell,b,h\rangle$ as defined in the case 5. We first prove that there exist a constant ν, such that $\Pr\left[f_{-1} \mid u^-\right] \le \nu\cdot\Pr\left[f_{-1} \mid u\right]$.

$$
\begin{aligned}
\Pr\left[f_{-1} \mid u\right] &= \sum_i \Pr\left[f_{-1} \mid \langle \ell, b\rangle, D = i\right] \cdot \Pr\left[D = i \mid u\right] \\
&\geq \sum_{|i| \leq 9 \cdot \sqrt{\ell \cdot \log(m)}} \Pr\left[f_{-1} \mid \langle \ell, b\rangle, D = i\right] \cdot \Pr\left[D = i \mid u\right] \\
&= \sum_{|i| \leq 9 \cdot \sqrt{\ell \cdot \log(m)}} \Pr\left[X = -(b+i)\right] \cdot \Pr\left[D = i \mid u\right] \\
&\geq \sum_{|i| \leq 9 \cdot \sqrt{\ell \cdot \log(m)}} \nu \cdot \Pr\left[X + D = -b\right] \cdot \Pr\left[D = i \mid u\right] \qquad (123) \\
&= \sum_{|i| \leq 9 \cdot \sqrt{\ell \cdot \log(m)}} \nu \cdot \Pr\left[f_{-1} \mid \langle \ell, b\rangle\right] \cdot \Pr\left[D = i \mid u\right] \\
&= \nu \cdot \Pr\left[f_{-1} \mid \langle \ell, b\rangle\right] \cdot \sum_{|i| \leq 9 \cdot \sqrt{\ell \cdot \log(m)}} \Pr\left[D = i \mid u\right] \\
&\geq \frac{1}{2} \cdot \nu \cdot \tilde{\lambda} \cdot \Pr\left[f_{-1} \mid u^-\right] \qquad (124)
\end{aligned}
$$

Where Inequality (123) is because $\nu \cdot \Pr\left[X + D = -b\right] \leq \Pr\left[X = -(b+i)\right]$ for some constant ν, and every i such that $|i| \leq 9 \cdot \sqrt{\ell \cdot \log(m)}$. Inequality (124) is due to Equation (117).

We have:

$$
\begin{aligned}
y_u + \sum_{v:\ v > u} y_v \cdot \Pr\left[v \mid u\right] &\geq y_{f_{-1}} \cdot \Pr\left[f_{-1} \mid u\right] \\
&= \nu \cdot y_{f_{-1}} \cdot \Pr\left[f_{-1} \mid u^-\right] \\
&= \lambda' \cdot \tau \cdot \sqrt{m} \cdot \sqrt{\log m} \cdot \Pr\left[f_{-1} \mid u^-\right] \\
&\geq c_u - v_u \qquad (125)
\end{aligned}
$$

Where Inequality (125) is due to Equation (116). □

5.5 Bounding Vector and Hypergeometric Games

A main tool for this section is Lemma 5.24, proved in previous section. We use Lemma 5.24 together with the tools of Section 4 to prove Lemma 3.19 and Lemma 3.21.

Lemma 5.25. *[Restatement of Lemma 3.19] For $m \in \mathbb{N}$, $k \in [m]$, $\varepsilon \in [-1, 1]$, and $f = f^{\mathsf{vec}}_{m,\varepsilon,k \cdot \mathsf{sum}_m(1)}$, let G be the binomial game $\mathsf{G}_{m,\varepsilon,f}$ according to Definition 5.1. Assuming that $k \leq \frac{m}{\log^6 m}$, it holds that $\mathsf{Bias}_{\mathsf{G}} \in O(\frac{\sqrt{k}}{m} \cdot \sqrt{\log m})$.*

Proof. If $|\varepsilon| > 4\sqrt{\frac{\log m}{\mathsf{sum}_m(1)}}$, the proof immediately follows by Lemma 5.23. Therefore, we assume that $|\varepsilon| \leq 4\sqrt{\frac{\log m}{\mathsf{sum}_m(1)}}$. Let S be as defined in Lemma 5.24, with respect to $\tau = \sqrt{k}$ and $\mathsf{G} = \mathsf{G}_{m,\varepsilon,f}$ for $f = f^{\mathsf{vec}}_{m,\varepsilon,k \cdot \mathsf{sum}_m(1)}$, as defined in Definition 3.18. Namely, f on input (i, b, c) calculates $\delta = \widehat{\mathcal{C}}_{\mathsf{sum}_m(i+1),\varepsilon}(-b-c)$ and outputs a random sample from $(\mathcal{C}_\varepsilon)^{k \cdot \mathsf{sum}_m(1)}$, for $\varepsilon := \widehat{\mathcal{C}}^{-1}_{\mathsf{sum}_m(1)}(\delta)$.

In the following, let $\langle \ell, b\rangle \in S^-$, let $i = m - \ell + 1$, let $s = \mathsf{sum}_m(1)$, let $(A = C_i, B)$ be the variables of a (m, i, b, ε)-binomial two-step process (as defined in Definition 4.1) and let g be a (s, k)-vector leakage function for (A, B) (as defined in Definition 4.4). Since m,i,b,s,ε and $\alpha = k$ satisfy all the conditions of Lemma 4.9, the lemma yields that there exists $\mathcal{H}_{\ell,b} \subseteq \{-1, 1\}^{k\cdot\mathsf{sum}_m(1)}$ such that

1. $\Pr\left[g(A) \notin \mathcal{H}_{\ell,b}\right] \leq \frac{1}{m^2}$
2. For every $h \in \mathcal{H}_{\ell,b}$,
   (a) $\Pr\left[|C_i| > 9\sqrt{\log m \cdot \ell_m(i)} \mid g(A) = h\right] \leq \frac{\lambda}{m^{12}}$, for some universal constant $\lambda > 0$.
   (b) $\left|\Pr\left[B = 1\right] - \Pr\left[B = 1 \mid g(A) = h\right]\right| \leq \lambda'\sqrt{\log m \cdot k} \cdot \sqrt{\frac{\ell_m(i)}{m-i+1}} \cdot \Pr\left[\sum_{j=i}^{m} C_j = -(b+1)\right]$, for some universal constant $\lambda' > 0$.

By doing the translations from the notations of Section 5 to the notations of Section 4, we get that $\sum_{h\notin\mathcal{H}_{\ell,b}} \Pr\left[\langle \ell, b, h\rangle \mid \langle \ell, b\rangle\right] = \Pr\left[g(A) \notin \mathcal{H}_{\ell,b}\right] \leq \frac{1}{m^2}$ and for every $u = \langle \ell, b, h\rangle$,

* $c_u - v_u = \Pr\left[B = 1\right] - \Pr\left[B = 1 \mid g(A) = h\right]$,
* $\Pr\left[f_{-1} \mid u^-\right] = \Pr\left[\sum_{j=i}^{m} C_j = -(b+1)\right]$,
* $\Pr\left[D_\ell > 9 \cdot \sqrt{\ell \cdot \log m} \;\mid\; \langle \ell, b, h\rangle\right] = \Pr\left[C_i > 9 \cdot \sqrt{\log m \cdot \ell_m(i)} \mid g(A) = h\right]$.

Therefore, combining these equalities with properties 2a and 2b of $\mathcal{H}_{\ell,b}$, together with the fact that $\sqrt{\frac{\ell_m(i)}{m-i+1}} \leq \sqrt{m}$, yields that

(a) $\Pr\left[D_\ell > 9 \cdot \sqrt{\ell \cdot \log m} \;\mid\; \langle \ell, b, h\rangle\right] \leq \frac{\lambda}{m^2}$, and

(b) $|c_u - v_u| \leq \lambda'\sqrt{k} \cdot \sqrt{m \log m} \cdot \Pr\left[f_{-1} \mid u^-\right]$,

for every $u = \langle \ell, b, h\rangle$ with $h \in \mathcal{H}_{\ell,b}$. In summary, we proved that for every $\langle \ell, b\rangle \in S^-$ there exists a set $\mathcal{H}_{\ell,b}$ that satisfy the three conditions of Lemma 5.24 with $\tau = \sqrt{k}$. Therefore, applying Lemma 5.24 yields that $\mathsf{Bias}_{\mathsf{G}} \in O(\frac{\sqrt{k}}{m} \cdot \sqrt{\log m})$, as required. □

Lemma 5.26. *[Restatement of Lemma 3.21] Let $m \in \mathbb{N}$, $\varepsilon \in [-1, 1]$, and let p be integer in $[-2 \cdot \mathsf{sum}_m(1), 2 \cdot \mathsf{sum}_m(1)]$. Assume that $|p| \leq \lambda \cdot \sqrt{\log m \cdot \mathsf{sum}_m(1)}$ for some constant λ, and let $f = f^{\mathsf{hyp}}_{m,p}$. Let G be the binomial game $\mathsf{G}_{m,\varepsilon,f}$ according to Definition 5.1, then $\mathsf{Bias}_{\mathsf{G}} \in O(\frac{\sqrt{\log m}}{m})$.*

Proof. If $|\varepsilon| > 4\sqrt{\frac{\log m}{\mathsf{sum}_m(1)}}$, the proof immediately follows by Lemma 5.23. Therefore, we assume that $|\varepsilon| \leq 4\sqrt{\frac{\log m}{\mathsf{sum}_m(1)}}$.

Let G' be the binomial game $\mathsf{G}_{m,\varepsilon,f'}$ according to Definition 5.1, where f' is a random function that on input (i, b, c), samples t according to $\mathcal{HG}_{2\cdot\mathsf{sum}_m(1),p,\mathsf{sum}_m(i+1)}$ and outputs $b + c + t$. Recall that $f^{\mathsf{hyp}}_{m,p}$, defined in Definition 3.20, is a random function that on input (i, b, c), outputs 1 with probability $\widehat{\mathcal{HG}}_{2\cdot\mathsf{sum}_m(1),p,\mathsf{sum}_m(i+1)}(-b-c)$ and -1 otherwise. Note that $f^{\mathsf{hyp}}_{m,p} = f'' \circ f'$ for f'' that on input $z \in \mathbb{Z}$ output 1 if $z \geq 0$ and -1 otherwise. Therefore, since $f^{\mathsf{hyp}}_{m,p}$ is just a function on the output of f', it is enough to bound $\mathsf{Bias}_{\mathsf{G}'}$ (Lemma 4.3 of [32]).

In the following, let S be as defined in Lemma 5.24, with respect to $\tau = 1$ and G', let $\langle \ell, b \rangle \in S^-$, let $i = m - \ell + 1$, let $(A = C_i\, B)$ be the variables of a $\big(m, i, b, \varepsilon\big)$-binomial two-step process (as defined in Definition 4.1) and let g be a $\big(m, i, b, p\big)$-hypergeometric leakage function for (A, B) (as defined in Definition 4.5). Since m, i, b, ε, p and λ satisfy all the conditions of Lemma 4.8, the lemma yields that there exists a set $\mathcal{H}_{\ell,b}$ such that

1. $\Pr\left[g(A) \notin \mathcal{H}_{\ell,b}\right] \leq \frac{1}{m^2}$
2. For every $h \in \mathcal{H}_{\ell,b}$,
   (a) $\Pr\left[|C_i| > 9\sqrt{\log m \cdot \ell_m(i)} \mid g(A) = h\right] \leq \frac{\lambda'}{m^{12}}$, for some universal constant $\lambda' > 0$.
   (b) $\left|\Pr\left[B = 1\right] - \Pr\left[B = 1 \mid g(A) = h\right]\right| \leq \varphi(\lambda)\sqrt{\log m} \cdot \sqrt{\frac{\ell_m(i)}{m-i+1}} \cdot \Pr\left[\sum_{j=i}^{m} C_j = -(b+1)\right]$, for some universal function $\varphi\colon \mathbb{R}^+ \to \mathbb{R}^+$.

By doing the translations from the notations of Section 5 to the notations of Section 4 (as done in Lemma 5.25) and by combining the above properties of $\mathcal{H}_{\ell,b}$ together with the fact that $\sqrt{\frac{\ell_m(i)}{m-i+1}} \leq \sqrt{m}$, we get that

(a) $\Pr\left[D_\ell > 9 \cdot \sqrt{\ell \cdot \log m} \;\mid\; \langle \ell, b, h \rangle\right] \leq \frac{\lambda'}{m^2}$, and

(b) $|c_u - v_u| \leq \varphi(\lambda) \cdot \sqrt{m \log m} \cdot \Pr\left[f_{-1} \mid u^-\right]$,

for every $u = \langle \ell, b, h \rangle$ with $h \in \mathcal{H}_{\ell,b}$. In summary, we proved that for every $\langle \ell, b \rangle \in S^-$ there exists a set $\mathcal{H}_{\ell,b}$ that satisfy the three conditions of Lemma 5.24 with $\tau = 1$. Therefore, applying Lemma 5.24 yields that $\mathsf{Bias}_{\mathsf{G}'} \in O(\frac{\sqrt{\log m}}{m})$, as required. □

References

[1] Abramowitz, M. and Stegun, I. A., editors. *Handbook of Mathematical Functions*. Dover Publications, 1964.

[2] D. Aharonov, A. Ta-Shma, U. Vazirani, and A. C. Yao. Quantum bit escrow. In *STOC: ACM Symposium on Theory of Computing (STOC)*, 2000.

[3] W. Aiello, Y. Ishai, and O. Reingold. Priced oblivious transfer: How to sell digital goods. In *Advances in Cryptology – EUROCRYPT 2001*, 2001.

[4] B. Alon and E. Omri. Almost-optimally fair multiparty coin-tossing with nearly three-quarters malicious. Cryptology ePrint Archive, Report 2016/800, 2016. http://eprint.iacr.org/2016/800.

[5] N. Alon and M. Naor. Coin-flipping games immune against linear-sized coalitions. *SIAM Journal on Computing*, pages 46–54, 1993.

[6] A. Ambainis. A new protocol and lower bounds for quantum coin flipping. *J. Comput. Syst. Sci.*, 68(2):398–416, 2004.

[7] A. Ambainis, H. Buhrman, Y. Dodis, and H. Röhrig. Multiparty quantum coin flipping. In *Proceedings of the 18th Annual IEEE Conference on Computational Complexity*, pages 250–259, 2004.

[8] G. Asharov. Towards characterizing complete fairness in secure two-party computation. In *Theory of Cryptography - 11th Theory of Cryptography Conference, TCC 2014, San Diego, CA, USA, February 24-26, 2014. Proceedings*, pages 291–316, 2014. doi: 10.1007/978-3-642-54242-8_13.

[9] G. Asharov, A. Beimel, N. Makriyannis, and E. Omri. Complete characterization of fairness in secure two-party computation of boolean functions. In *Theory of Cryptography - 12th Theory of Cryptography Conference, TCC 2015, Warsaw, Poland, March 23-25, 2015, Proceedings, Part I*, pages 199–228, 2015.

[10] B. Awerbuch, M. Blum, B. Chor, S. Goldwasser, and S. Micali. How to implement brachas o (log n) byzantine agreement algorithm. 1985.

[11] D. Beaver, S. Micali, and P. Rogaway. The round complexity of secure protocols. In *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing (STOC)*, pages 503–513, 1990.

[12] A. Beimel, E. Omri, and I. Orlov. Protocols for multiparty coin toss with dishonest majority. In *Advances in Cryptology – CRYPTO 2010*, volume 6223, pages 538–557, 2010.

[13] A. Beimel, Y. Lindell, E. Omri, and I. Orlov. $1/p$-secure multiparty computation without honest majority and the best of both worlds. In *Advances in Cryptology – CRYPTO 2011*, pages 277–296, 2011.

[14] M. Ben-Or and N. Linial. Collective coin flipping. *ADVCR: Advances in Computing Research*, 5, 1989.

[15] M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation. In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing (STOC)*, 1988.

[16] I. Berman, I. Haitner, and A. Tentes. Coin flipping of any constant bias implies one-way functions. In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing (STOC)*, pages 817–836, 2014.

[17] M. Blum. How to exchange (secret) keys. *ACM Transactions on Computer Systems*, 1983.

[18] R. Canetti. Security and composition of multiparty cryptographic protocols. *Journal of Cryptology*, 13(1):143–202, 2000.

[19] R. Cleve. Limits on the security of coin flips when half the processors are faulty. In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing (STOC)*, pages 364–369, 1986.

[20] R. Cleve and R. Impagliazzo. Martingales, collective coin flipping and discrete control processes. Manuscript, 1993. URL https://pdfs.semanticscholar.org/7c7f/244d2ef064d75b3d23c88472ee1226461695.pdf.

[21] R. Cohen, I. Haitner, E. Omri, and L. Rotem. Characterization of secure multiparty computation without broadcast. pages 596–616, 2016.

[22] D. Dachman-Soled, Y. Lindell, M. Mahmoody, and T. Malkin. On the black-box complexity of optimally-fair coin tossing. In *tcc11*, pages 450–467, 2011.

[23] S. Even, O. Goldreich, and A. Lempel. A randomized protocol for signing contracts. *Communications of the ACM*, 28(6):637–647, 1985.

[24] U. Feige. Noncryptographic selection protocols. In *Proceedings of the 40th Annual Symposium on Foundations of Computer Science (FOCS)*, 1999.

[25] C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the 40th Annual ACM Symposium on Theory of Computing (STOC)*, pages 197–206, 2008.

[26] O. Goldreich. *Foundations of Cryptography – VOLUME 2: Basic Applications*. Cambridge University Press, 2004.

[27] O. Goldreich, S. Micali, and A. Wigderson. How to play any mental game or a completeness theorem for protocols with honest majority. In *Proceedings of the 19th Annual ACM Symposium on Theory of Computing (STOC)*, pages 218–229, 1987.

[28] S. D. Gordon and J. Katz. Partial fairness in secure two-party computation. In *Advances in Cryptology – EUROCRYPT 2011*, pages 157–176, 2010.

[29] S. D. Gordon, C. Hazay, J. Katz, and Y. Lindell. Complete fairness in secure two-party computation. *Journal of the ACM*, 58(6):24, 2011.

[30] I. Haitner. Implementing oblivious transfer using collection of dense trapdoor permutations. In *Theory of Cryptography, First Theory of Cryptography Conference, TCC 2004*, pages 394–409, 2004.

[31] I. Haitner and E. 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.

[32] I. Haitner and E. Tsfadia. An almost-optimally fair three-party coin-flipping protocol. `www.cs.tau.ac.il/~iftachh/papers/3PartyCF/QuasiOptimalCF_Full.pdf`. Manuscript. Preliminary version in *STOC '14*.

[33] I. Haitner and E. Tsfadia. An almost-optimally fair three-party coin-flipping protocol. In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing (STOC)*, pages 817–836, 2014.

[34] I. Haitner, M. Nguyen, S. J. Ong, O. Reingold, and S. Vadhan. Statistically hiding commitments and statistical zero-knowledge arguments from any one-way function. *SIAM Journal on Computing*, pages 1153–1218, 2009.

[35] I. Haitner, O. Reingold, S. Vadhan, and H. Wee. Inaccessible entropy. In *Proceedings of the 41st Annual ACM Symposium on Theory of Computing (STOC)*, pages 611–620, 2009.

[36] J. Håstad, R. Impagliazzo, L. A. Levin, and M. Luby. A pseudorandom generator from any one-way function. *SIAM Journal on Computing*, pages 1364–1396, 1999.

[37] W. Hoeffding. Probability inequalities for sums of bounded random variables, 1963.

[38] R. Impagliazzo and M. Luby. One-way functions are essential for complexity based cryptography. In *Proceedings of the 30th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 230–235, 1989.

[39] Y. Kalai. Smooth projective hashing and two-message oblivious transfer. In *Advances in Cryptology – EUROCRYPT 2005*, 2005.

[40] J. Katz. On achieving the "best of both worlds" in secure multiparty computation. In *Proceedings of the 37th Annual ACM Symposium on Theory of Computing (STOC)*, pages 11–20, 2007.

[41] H. K. Maji, M. Prabhakaran, and A. Sahai. On the Computational Complexity of Coin Flipping. In *Proceedings of the 51th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 613–622, 2010.

[42] T. Moran and M. Naor. Basing cryptographic protocols on tamper-evident seals. In *ICALP: Annual International Colloquium on Automata, Languages and Programming*, 2005.

[43] T. Moran, , M. Naor, and G. Segev. An optimally fair coin toss. *Journal of Cryptology*, 29(3): 491–513, 2016. ISSN 1432-1378. doi: 10.1007/s00145-015-9199-z. URL http://dx.doi.org/10.1007/s00145-015-9199-z.

[44] M. Naor. Bit commitment using pseudorandomness. *Journal of Cryptology*, pages 151–158, 1991.

[45] M. Naor. Bit commitment using pseudorandomness. *Journal of Cryptology*, pages 151–158, 1991.

[46] M. Naor and B. Pinkas. Efficient oblivious transfer protocols. In *SODA*, pages 448–457, 2001.

[47] A. Russell and D. Zuckerman. Perfect information leader election in log* n + 0 (1) rounds. In *Proceedings of the 39th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 576–583, 1999.

[48] M. Saks. A robust noncryptographic protocol for collective coin flipping. *SIJDM: SIAM Journal on Discrete Mathematics*, 2, 1989.

[49] M. Scala. Hypergeometric tail inequalities: ending the insanity. *arXiv preprint arXiv:1311.5939*, 2009.

A Missing Proofs

This section contains missing proofs for statement given in Sections 2.2 and 2.3.

A.1 Properties of Bell-Like Distributions

This section proves useful properties of "bell-like" distributions, which in particular gives useful properties on the binomial and hypergeometric distributions.

Recall that for $a \in \mathbb{R}$ and $b \geq 0$, $a \pm b$ denotes for the interval $[a-b, a+b]$, and that given sets $\mathcal{S}_1, \ldots, \mathcal{S}_k$ and k-input function f, $f(\mathcal{S}_1, \ldots, \mathcal{S}_k) = \{f(x_1, \ldots, x_j) \colon x_i \in \mathcal{S}_i\}$, e.g., $f(1 \pm 0.1) = \{f(x) \colon x \in [.9, 1.1]\}$.

Definition A.1 (bell-like distributions)**.** *For $r \in \mathbb{N}$, $v \in [1, r]$, $\lambda > 0$ and $\xi > 0$, we say that a distribution $\mathcal{D}$ is a (r, v, λ, ξ)-bell-like distribution if*

1. $|\mu| \leq \lambda \cdot \sqrt{v \log v}$ *where* $\mu := \mathrm{E}_{t \leftarrow \mathcal{D}}[t]$.
2. $\Pr_{t \leftarrow \mathcal{D}}[|t - \mu| \geq a] \leq 2 \cdot e^{-\frac{a^2}{2v}}$ *[Hoeffding's Inequality].*
3. $\mathcal{D}(t) = 0$ *for every* $t \in \mathbb{Z}$ *with* $\frac{r+t}{2} \notin (r)$.
4. $\mathcal{D}(t) \in (1 \pm \xi \cdot \frac{\log^{1.5} v}{\sqrt{v}}) \cdot \sqrt{\frac{2}{\pi}} \cdot \frac{1}{\sqrt{v}} \cdot e^{-\frac{(t-\mu)^2}{2v}}$ *for every* $t \in \mathbb{Z}$ *with* $|t| \leq \lambda \cdot \sqrt{v \log v}$ *and* $\frac{r+t}{2} \in (r)$.

In the following, let $r \in \mathbb{N}$, $v \in [1, r]$, $\lambda \geq 1$ and $\xi > 0$ and let $\mathcal{D}$ be a (r, v, λ, ξ)-bell-like distribution with (according to Definition A.1) and let $\mu := \mathrm{E}_{t \leftarrow \mathcal{D}}[t]$. In the following, we make some observations regards $\mathcal{D}$.

Recall that the function $\Phi \colon \mathbb{R} \mapsto (0, 1)$ defined as $\Phi(x) := \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-\frac{t^2}{2}} dt$ is the cumulative distribution function of the standard normal distribution.

Fact A.2 ([1])**.** *For $x \geq 0$ it holds that*

$$\sqrt{\frac{2}{\pi}} \cdot \frac{e^{-\frac{x^2}{2}}}{x + \sqrt{x^2 + 4}} \leq \Phi(x) \leq \sqrt{\frac{2}{\pi}} \cdot \frac{e^{-\frac{x^2}{2}}}{x + \sqrt{x^2 + \frac{8}{\pi}}}.$$

Proposition A.3. *Let $v \in \mathbb{N}$, $\mu \in \mathbb{Z}$ and $k, \ell \in \mathbb{Z}$ be such that $\ell \geq k \geq \frac{\mu}{2}$. Then*

$$\left| \sum_{t=k}^{\ell} e^{-\frac{(2t-\mu)^2}{2v}} - \int_k^\ell e^{-\frac{(2t-\mu)^2}{2v}} dt \right| \leq e^{-\frac{(2k-\mu)^2}{2v}}.$$

Proof. See [32]. □

The following proposition states the connection between a bell-like distribution and the normal distribution.

Proposition A.4. *For every $k \in \mathbb{Z}$ with $|k| < \lambda \cdot \sqrt{v \log v}$, it holds that*

$$\widehat{\mathcal{D}}(k) \in \Phi(\frac{k - \mu}{\sqrt{v}}) \pm \mathsf{error},$$

where $\mathsf{error} = \varphi(\xi) \cdot \frac{\log^{1.5} v}{\sqrt{v}} \cdot e^{-\frac{(k-\mu)^2}{2v}}$ *for* $\varphi(\xi) = 4\xi + 5$.

Proof. Assume for simplicity that r and k are both even, where the proofs of the other cases are analogous. Let $\ell = \ell(\lambda, v) := 4 \cdot \lceil \lambda\sqrt{v \log v} \rceil < 5\lambda \cdot \sqrt{v \log v}$. We start by handling the case $k \geq \mu$. It holds that

$$\begin{aligned}
\sum_{t=k}^{\ell} \mathcal{D}(t) &= \sum_{t=\frac{k}{2}}^{\frac{\ell}{2}} \mathcal{D}(2t) \\
&\in \sum_{t=\frac{k}{2}}^{\frac{\ell}{2}} \sqrt{\frac{2}{\pi}}(1 \pm \xi \cdot \frac{\log^{1.5} v}{\sqrt{v}}) \cdot \frac{1}{\sqrt{v}} \cdot e^{-\frac{(2t-\mu)^2}{2v}} \\
&\subseteq (1 \pm \xi \cdot \frac{\log^{1.5} v}{\sqrt{v}}) \cdot A(v, k, \lambda),
\end{aligned} \tag{126}$$

letting $A(v, k, \lambda) := \sum_{t=\frac{k}{2}}^{\frac{\ell}{2}} \sqrt{\frac{2}{\pi}} \cdot \frac{1}{\sqrt{v}} \cdot e^{-\frac{(2t-\mu)^2}{2v}}$. The first transition holds by property 3 of $\mathcal{D}$ and the second one by property 4 of $\mathcal{D}$.

Compute

$$\begin{aligned}
A(v, k, \lambda) &= \sum_{t=\frac{k}{2}}^{\frac{\ell}{2}} \sqrt{\frac{2}{\pi}} \cdot \frac{1}{\sqrt{v}} \cdot e^{-\frac{(2t-\mu)^2}{2v}} \\
&\in \int_{\frac{k}{2}}^{\frac{\ell}{2}} \sqrt{\frac{2}{\pi}} \cdot \frac{1}{\sqrt{v}} \cdot e^{-\frac{(2t-\mu)^2}{2v}} dt \pm \frac{1}{\sqrt{v}} \cdot e^{-\frac{(k-\mu)^2}{2v}} \\
&= \int_{\frac{k-\mu}{\sqrt{v}}}^{\frac{\ell-\mu}{\sqrt{v}}} \frac{1}{\sqrt{2\pi}} \cdot e^{-\frac{x^2}{2}} dx \pm \frac{1}{\sqrt{v}} \cdot e^{-\frac{(k-\mu)^2}{2v}} \\
&= \Phi(\frac{k-\mu}{\sqrt{v}}) - \Phi(\frac{\ell-\mu}{\sqrt{v}}) \pm \frac{1}{\sqrt{v}} \cdot e^{-\frac{(k-\mu)^2}{2v}} \\
&\subseteq \Phi(\frac{k-\mu}{\sqrt{v}}) \pm \frac{1}{v^{4\lambda^2}} \pm \frac{1}{\sqrt{v}} \cdot e^{-\frac{(k-\mu)^2}{2v}} \\
&\subseteq \Phi(\frac{k-\mu}{\sqrt{v}}) \pm \frac{2}{\sqrt{v}} \cdot e^{-\frac{(k-\mu)^2}{2v}},
\end{aligned} \tag{127}$$

where the second transition holds by Proposition A.3 (and since $k \geq \mu$), the third one holds by letting $x = \frac{2t-\mu}{\sqrt{v}}$, the fifth one holds by Fact A.2 together with property 1 of $\mathcal{D}$ which yields that $\Phi(\frac{\ell-\mu}{\sqrt{v}}) \leq \Phi(3\lambda\sqrt{\log v}) \leq \frac{1}{v^{4\lambda^2}}$, and the last one holds since $\frac{1}{\sqrt{v}} \cdot e^{-\frac{(k-\mu)^2}{2v}} \geq \frac{1}{v^{2\lambda^2+\frac{1}{2}}} \geq \frac{1}{v^{4\lambda^2}}$.

Applying Equation (127) on Equation (126) yields that

$$\begin{aligned}
\sum_{t=k}^{\ell} \mathcal{D}(t) &\in (1 \pm \xi \cdot \frac{\log^{1.5} v}{\sqrt{v}}) \cdot (\Phi(\frac{k-\mu}{\sqrt{v}}) \pm \frac{2}{\sqrt{v}} \cdot e^{-\frac{(k-\mu)^2}{2v}}) \\
&= \Phi(\frac{k-\mu}{\sqrt{v}}) \pm \xi \cdot \frac{\log^{1.5} v}{\sqrt{v}} \cdot \Phi(\frac{k-\mu}{\sqrt{v}}) \pm 2 \cdot \xi \cdot \frac{\log^{1.5} v}{v} \cdot e^{-\frac{(k-\mu)^2}{2v}} \pm \frac{2}{\sqrt{v}} \cdot e^{-\frac{(k-\mu)^2}{2v}} \\
&\subseteq \Phi(\frac{k-\mu}{\sqrt{v}}) \pm (3\xi + 2) \cdot \frac{\log^{1.5} v}{\sqrt{v}} \cdot e^{-\frac{(k-\mu)^2}{2v}},
\end{aligned} \tag{128}$$

We conclude that

$$\begin{aligned}\widehat{\mathcal{D}}(k) &= \sum_{t=k}^{n} \mathcal{D}(t) \\ &= \sum_{t=k}^{\ell} \mathcal{D}(t) + \Pr_{x \leftarrow \mathcal{D}}[x > \ell] \\ &\in \sum_{t=k}^{\ell} \mathcal{D}(t) \pm \frac{2}{v^{4\lambda^2}} \\ &\subseteq \left(\Phi(\frac{k-\mu}{\sqrt{v}}) \pm (3\xi+2) \cdot \frac{\log^{1.5} v}{\sqrt{v}} \cdot e^{-\frac{(k-\mu)^2}{2v}}\right) \pm \frac{2}{v^{4\lambda^2}} \\ &\subseteq \Phi(\frac{k-\mu}{\sqrt{v}}) \pm (3\xi+4) \cdot \frac{\log^{1.5} v}{\sqrt{v}} \cdot e^{-\frac{(k-\mu)^2}{2v}},\end{aligned} \tag{129}$$

where the third transition holds by property 2 of $\mathcal{D}$ and the fourth one holds by Equation (128). It is left to handle the case $k < \mu$. For such k, it holds that

$$\begin{aligned}\widehat{\mathcal{D}}(k) &= 1 - (\widehat{-\mathcal{D}})(-k) + \mathcal{D}(k) \\ &\in 1 - (\widehat{-\mathcal{D}})(-k) + (1 \pm \xi \cdot \frac{\log^{1.5} v}{\sqrt{v}}) \cdot \sqrt{\frac{2}{\pi}} \cdot \frac{1}{\sqrt{v}} \cdot e^{-\frac{(k-\mu)^2}{2v}} \\ &\subseteq \left(1 - \Phi(\frac{-k+\mu}{\sqrt{v}}) \pm (3\xi+4) \cdot \frac{\log^{1.5} v}{\sqrt{v}} \cdot e^{-\frac{(k-\mu)^2}{2v}}\right) + (1 \pm \xi \cdot \frac{\log^{1.5} v}{\sqrt{v}}) \cdot \sqrt{\frac{2}{\pi}} \cdot \frac{1}{\sqrt{v}} \cdot e^{-\frac{(k-\mu)^2}{2v}} \\ &\subseteq \Phi(\frac{k-\mu}{\sqrt{v}}) \pm (4\xi+5) \cdot \frac{\log^{1.5} v}{\sqrt{v}} \cdot e^{-\frac{(k-\mu)^2}{2v}},\end{aligned} \tag{130}$$

where the second transition holds by property 4 of $\mathcal{D}$ and the third one holds by Equation (129) applied to $-\mathcal{D}$ and $-k$ (The distribution $-\mathcal{D}$, which defined as $-\mathcal{D}(t) = \mathcal{D}(-t)$, is also a (r, v, c, ξ)-bell-like distribution). □

Proposition A.5. *Let $n \in \mathbb{N}$, $\delta \in [0,1]$ and $\lambda > 0$ be such that $\delta \in (\frac{1}{n^\lambda}, 1 - \frac{1}{n^\lambda})$. Then,*

$$\widehat{\mathcal{C}}_n^{-1}(\delta) \in -\frac{\Phi^{-1}(\delta)}{\sqrt{n}} \pm \mathsf{error}$$

for $\mathsf{error} = \varphi(\lambda) \cdot \frac{\log^{1.5} n}{n}$ *and a universal function φ.*

Proof. See [32]. □

Proposition A.6. *Let $\delta = \widehat{\mathcal{D}}(k)$ for some $k \in \mathbb{Z}$ with $|k| < \lambda \cdot \sqrt{v \log v}$. Assuming $e^{-4\xi'(\xi'+\lambda) \cdot \frac{\log^3 v}{\sqrt{v}}} \geq \frac{1}{2}$, it holds that*

$$\Phi^{-1}(\delta) \in \frac{k-\mu}{\sqrt{v}} \pm \mathsf{error},$$

for $\mathsf{error} = (8\xi + 10) \cdot \frac{\log^{1.5} v}{\sqrt{v}}$.

Proof. Let $\xi' = 4\xi + 5$, let $\Delta := 2\xi' \cdot \log^{1.5} v$ and let $k_0 := k - \mu$.

We prove that $\Phi(\frac{k_0+\Delta}{\sqrt{v}}) \leq \delta \leq \Phi(\frac{k_0-\Delta}{\sqrt{v}})$, which yields the required bound since Φ is monotonic decreasing. We focus on the upper bound, whereas the lower bound can be proven analogously. Since

$$\frac{\Delta}{\sqrt{v}} \cdot e^{-\frac{k_0^2}{2v}} \geq \xi' \cdot \frac{\log^{1.5} v}{\sqrt{v}} \cdot e^{-\frac{k_0^2}{2v}} \tag{131}$$

and

$$\begin{aligned} \frac{\Delta}{\sqrt{v}} \cdot e^{-\frac{(k_0-\Delta)^2}{2v}} &= \frac{\Delta}{\sqrt{v}} \cdot e^{-\frac{k_0^2}{2v}} \cdot e^{\frac{2k_0\Delta-\Delta^2}{2v}} \\ &\geq \frac{\Delta}{\sqrt{v}} \cdot e^{-\frac{k_0^2}{2v}} \cdot e^{-4\xi'(\xi'+\lambda)\cdot\frac{\log^3 v}{\sqrt{v}}} \\ &\geq \frac{\Delta}{\sqrt{v}} \cdot e^{-\frac{k_0^2}{2v}} \cdot \frac{1}{2} \\ &= \xi' \cdot \frac{\log^{1.5} v}{\sqrt{v}} \cdot e^{-\frac{k_0^2}{2v}}, \end{aligned} \tag{132}$$

it follows that

$$\begin{aligned} \delta &\leq \Phi(\frac{k_0}{\sqrt{v}}) + \xi' \cdot \frac{\log^{1.5} v}{\sqrt{v}} \cdot e^{-\frac{k_0^2}{2v}} \\ &\leq \Phi(\frac{k_0}{\sqrt{v}}) + \frac{\Delta}{\sqrt{v}} \cdot \min(e^{-\frac{k_0^2}{2v}}, e^{-\frac{(k_0-\Delta)^2}{2v}}) \\ &\leq \Phi(\frac{k_0}{\sqrt{v}}) + \int_{\frac{k_0-\Delta}{\sqrt{v}}}^{\frac{k_0}{\sqrt{v}}} e^{-\frac{t^2}{2}}\, dt \\ &= \Phi(\frac{k_0}{\sqrt{v}} - \frac{\Delta}{\sqrt{v}}), \end{aligned} \tag{133}$$

where the first inequality holds by Proposition A.4 and the second one by Equation (131) and Equation (132). □

Proposition A.7. *Let $\delta = \widehat{\mathcal{D}}(k)$ for some $k \in \mathbb{Z}$ with $|k| < \lambda \cdot \sqrt{v \log v}$. Assume*

1. $v \geq 16$
2. $\max(\lambda, \xi') \cdot \frac{\log^2 v}{\sqrt{v}} < \frac{1}{8}$
3. $e^{-4\xi'(\xi'+\lambda)\cdot\frac{\log^3 v}{\sqrt{v}}} \geq \frac{1}{2}$,

where $\xi' = 4\xi + 5$ and φ' is the function from Proposition A.5. Then

$$\widehat{\mathcal{C}}_n^{-1}(\delta) \in \frac{\mu - k}{\sqrt{n \cdot v}} \pm \mathsf{error},$$

for $\mathsf{error} = \left(\varphi'(2\lambda^2 + 1) + 2\xi'\right) \cdot \frac{\log^{1.5} v}{\sqrt{n \cdot v}}$.

Proof. In order to use Proposition A.5, we first prove that $\delta \in (\frac{1}{v^{2\lambda^2+1}}, 1 - \frac{1}{v^{2\lambda^2+1}}) \subseteq (\frac{1}{n^{2\lambda^2+1}}, 1 - \frac{1}{n^{2\lambda^2+1}})$. Let $k_0 := k - \mu$. For simplicity, we assume $k_0 \geq 0$, whereas the case $k_0 < 0$ holds by symmetry. Compute

$$\begin{aligned}
\delta &\in \Phi(\frac{k_0}{\sqrt{v}}) \pm \xi' \cdot \frac{\log^{1.5} v}{\sqrt{v}} \cdot e^{-\frac{k_0^2}{2v}} \\
&\subseteq \left(\frac{1}{\frac{k_0}{\sqrt{v}} + \sqrt{\frac{k_0^2}{v} + 4} \pm 2} \pm \xi' \cdot \frac{\log^{1.5} v}{\sqrt{v}} \right) \cdot e^{-\frac{k_0^2}{2v}}, \\
&\subseteq \frac{1 \pm \frac{1}{2}}{\frac{k_0}{\sqrt{v}} + \sqrt{\frac{k_0^2}{v} + 4} \pm 2} \cdot e^{-\frac{k_0^2}{2v}} \\
&\subseteq (\frac{1}{8\lambda \cdot \sqrt{\log v} \cdot v^{2c^2}}, \frac{3}{4}) \\
&\subseteq (\frac{1}{v^{2\lambda^2+1}}, 1 - \frac{1}{v^{2\lambda^2+1}})
\end{aligned} \tag{134}$$

where the first transition holds by Proposition A.4, the second one holds by Fact A.2, the third one holds by condition 2 and since $k_0 \leq 2\lambda \cdot \sqrt{v \log v}$, the fourth one also holds since $k_0 \leq 2\lambda \cdot \sqrt{v \log v}$ and the last one holds by conditions 1 and 2.

Finally, it holds that

$$\begin{aligned}
\widehat{\mathcal{C}}_n^{-1}(\delta) &\in -\frac{\Phi^{-1}(\delta)}{\sqrt{n}} \pm \varphi'(2\lambda^2 + 1) \cdot \frac{\log^{1.5} n}{n} \\
&\subseteq -\frac{\left(\frac{k-\mu}{\sqrt{v}} \pm 2\xi' \cdot \frac{\log^{1.5} v}{\sqrt{v}}\right)}{\sqrt{n}} \pm \varphi'(2\lambda^2 + 1) \cdot \frac{\log^{1.5} n}{n} \\
&\subseteq \frac{\mu - k}{\sqrt{n \cdot v}} \pm \left(\varphi'(2\lambda^2 + 1) + 2\xi'\right) \cdot \frac{\log^{1.5} v}{\sqrt{n \cdot v}},
\end{aligned} \tag{135}$$

where the first transition holds by Proposition A.5, the second one by Proposition A.6 and the last one holds since $n \geq v$. □

A.2 Facts about binomial distribution

Recall that for $n \in \mathbb{N}$ and $\varepsilon \in [-1, 1]$, we let $\mathcal{C}_{n,\varepsilon}$ be the binomial distribution induced by the sum of n independent random variables over $\{-1, 1\}$, each takes the value 1 with probability $\frac{1}{2}(1 + \varepsilon)$ and -1 otherwise.

Proposition A.8. *[Restatement of Proposition 2.3] Let $n \in \mathbb{N}$, $\varepsilon \in [-1, 1]$ and let $\mu := \mathrm{E}_{x \leftarrow \mathcal{C}_{n,\varepsilon}}[x] = \varepsilon \cdot n$. Then for every $k > 0$ it holds that*

1. $\mathrm{E}_{x \leftarrow \mathcal{C}_{n,\varepsilon} | |x-\mu| \leq k}\left[(x - \mu)^2\right] \leq \mathrm{E}_{x \leftarrow \mathcal{C}_{n,\varepsilon}}\left[(x - \mu)^2\right] \leq n$.
2. $\mathrm{E}_{x \leftarrow \mathcal{C}_{n,\varepsilon} | |x-\mu| \leq k}\left[|x - \mu|\right] \leq \mathrm{E}_{x \leftarrow \mathcal{C}_{n,\varepsilon}}\left[|x - \mu|\right] \leq \sqrt{n}$.

Proof. The right inequality in Item 1 holds since

$$\begin{aligned}\mathop{\mathrm{E}}_{x\leftarrow\mathcal{C}_{n,\varepsilon}}\left[(x-\mu)^2\right] &= \mathop{\mathrm{E}}_{x\leftarrow\mathcal{C}_{n,\varepsilon}}\left[x^2\right] - 2\mu\cdot\mathop{\mathrm{E}}_{x\leftarrow\mathcal{C}_{n,\varepsilon}}[x] + \mu^2\\ &= \mathrm{Var}_{x\leftarrow\mathcal{C}_{n,\varepsilon}}[x]\\ &= n\cdot(1-\varepsilon^2)\\ &\le n,\end{aligned}$$

where the right inequality in Item 2 holds since $\mathrm{E}_{x\leftarrow\mathcal{C}_{n,\varepsilon}}[|x-\mu|] \le \sqrt{\mathrm{E}_{x\leftarrow\mathcal{C}_{n,\varepsilon}}[(x-\mu)^2]}$.

The left inequality in Item 2 holds since

$$\begin{aligned}&\mathop{\mathrm{E}}_{x\leftarrow\mathcal{C}_{n,\varepsilon}}[|x-\mu|]\\ &= \Pr_{x\leftarrow\mathcal{C}_{n,\varepsilon}}[|x-\mu|\le k]\cdot\mathop{\mathrm{E}}_{x\leftarrow\mathcal{C}_{n,\varepsilon}||x-\mu|\le k}[|x-\mu|] + \Pr_{x\leftarrow\mathcal{C}_{n,\varepsilon}}[|x-\mu|>k]\cdot\mathop{\mathrm{E}}_{x\leftarrow\mathcal{C}_{n,\varepsilon}||x-\mu|>k}[|x-\mu|]\\ &\ge \Pr_{x\leftarrow\mathcal{C}_{n,\varepsilon}}[|x-\mu|\le k]\cdot\mathop{\mathrm{E}}_{x\leftarrow\mathcal{C}_{n,\varepsilon}||x-\mu|\le k}[|x-\mu|] + \Pr_{x\leftarrow\mathcal{C}_{n,\varepsilon}}[|x-\mu|>k]\cdot\mathop{\mathrm{E}}_{x\leftarrow\mathcal{C}_{n,\varepsilon}||x-\mu|\le k}[|x-\mu|]\\ &= \mathop{\mathrm{E}}_{x\leftarrow\mathcal{C}_{n,\varepsilon}||x-\mu|\le k}[|x-\mu|],\end{aligned}$$

where the left inequality in Item 1 holds analogously to the above calculation. □

Fact A.9. *[Restatement of Fact 2.1 (Hoeffding's inequality)] Let $n, t \in \mathbb{N}$ and $\varepsilon \in [-1,1]$. Then*

$$\Pr_{x\leftarrow\mathcal{C}_{n,\varepsilon}}[|x-\varepsilon n|\ge t] \le 2e^{-\frac{t^2}{2n}}.$$

Proposition A.10. *[Restatement of Proposition 2.2] Let $n \in \mathbb{N}$, $t \in \mathbb{Z}$ and $\varepsilon \in [-1,1]$ be such that $t \in \mathrm{Supp}(\mathcal{C}_{n,\varepsilon})$, $|t| \le n^{\frac{3}{5}}$ and $|\varepsilon| \le n^{-\frac{2}{5}}$. Then*

$$\mathcal{C}_{n,\varepsilon}(t) \in (1\pm\mathsf{error})\cdot\sqrt{\frac{2}{\pi}}\cdot\frac{1}{\sqrt{n}}\cdot e^{-\frac{(t-\varepsilon n)^2}{2n}},$$

for $\mathsf{error} = \xi\cdot(\varepsilon^2|t| + \frac{1}{n} + \frac{|t|^3}{n^2} + \varepsilon^4 n)$ and a universal constant ξ.

Proposition A.11. *[Restatement of Proposition 2.4] Let $n, n' \in \mathbb{N}$, $k \in \mathbb{Z}$, $\varepsilon \in [-1,1]$ and $\lambda > 0$ be such that $n \le n'$, $|k| \le \lambda\cdot\sqrt{n\log n}$, $|\varepsilon| \le \lambda\cdot\sqrt{\frac{\log n}{n}}$, and let $\delta = \widehat{\mathcal{C}}_{n,\varepsilon}(k)$. Then*

$$\widehat{\mathcal{C}}^{-1}_{n'}(\delta) \in \frac{\varepsilon n - k}{\sqrt{n\cdot n'}} \pm \mathsf{error},$$

for $\mathsf{error} = \varphi(\lambda)\cdot\frac{\log^{1.5} n}{\sqrt{n\cdot n'}}$ and a universal function φ.

Proof. Let φ' be the function from Proposition A.10, and let φ'' be the function from Proposition A.5. By Fact A.9 and Proposition A.10 and using the proposition's bounds, it follows that $\mathcal{C}_{n,\varepsilon}$ is a $(n, n, \lambda, \varphi'(\lambda))$-bell-like distribution according to Definition A.1. Note that there exists a function $\vartheta\colon \mathbb{R}^+ \mapsto \mathbb{N}$ such that conditions 1, 2 and 3 of Proposition A.5 holds for every $n \ge \vartheta(\lambda)$. In the following we focus on $n \ge \vartheta(\lambda)$, where smaller n's are handled by setting the value of $\varphi(\lambda)$ to be large enough on these values. Now we can apply Proposition A.7 to get that

$$\widehat{\mathcal{C}}^{-1}_{n'}(\delta) \in \frac{\varepsilon n - k}{\sqrt{n\cdot n'}} \pm \varphi''(\lambda)\cdot\frac{\log^{1.5} n}{\sqrt{n\cdot n'}},$$

as required. □

A.3 Facts About the Hypergeometric Distribution

Recall that for a vector $v \in \{-1,1\}^*$ we let $w(v) := \sum_{i\in[|\mathcal{I}|]} v_i$, and given a set of indexes $\mathcal{I} \subseteq [|v|]$, we let $v_{\mathcal{I}} = (v_{i_1}, \ldots, v_{i_{|\mathcal{I}|}})$ where $i_1, \ldots, i_{|\mathcal{I}|}$ are the ordered elements of $\mathcal{I}$. In addition, recall that for $n \in \mathbb{N}$, $\ell \in [n]$, and an integer $p \in [-n, n]$, we define the hypergeometric probability distribution $\mathcal{HG}_{n,p,\ell}$ by $\mathcal{HG}_{n,p,\ell}(k) := \Pr_{\mathcal{I}}[w(v_{\mathcal{I}}) = k]$, where $\mathcal{I}$ is an ℓ-size set uniformly chosen from $[n]$ and $v \in \{-1,1\}^n$ with $w(v) = p$.

Fact A.12 (Hoeffding's inequality for hypergeometric distribution)**.** *Let $\ell \le n \in \mathbb{N}$, and $p \in \mathbb{Z}$ with $|p| \le n$. Then*

$$\Pr_{x\leftarrow\mathcal{HG}_{n,p,\ell}}[|x-\mu| \ge t] \le e^{-\frac{t^2}{2\ell}},$$

for $\mu = \mathrm{E}_{x\leftarrow\mathcal{HG}_{n,p,\ell}}[x] = \frac{\ell\cdot p}{n}$.

Proof. Immediately follows by [49, Equations (10),(14)]. □

We use the following estimation of an almost-central binomial coefficients.

Proposition A.13. *Let $n \in \mathbb{N}$ and $t \in \mathbb{Z}$ be such that $|t| \le n^{\frac{3}{5}}$ and $\frac{n+t}{2} \in (n)$. Then*

$$\binom{n}{\frac{n+t}{2}} \cdot 2^{-n} \in (1 \pm \mathsf{error}) \cdot \sqrt{\frac{2}{\pi}} \cdot \frac{1}{\sqrt{n}} \cdot e^{-\frac{t^2}{2n}},$$

for $\mathsf{error} = \xi \cdot (\frac{|t|^3}{n^2} + \frac{1}{n})$ and a universal constant ξ.

Proof. See [32]. □

The following claim calculates $\mathcal{HG}_{n,p,\ell}(t)$ using an almost-central binomial coefficients.

Claim A.14. *Let $n \in \mathbb{N}$, $\ell \in [n]$, $p, t \in \mathbb{Z}$ be such that $|p| \le n^{\frac{3}{5}}$, $|t| \le \ell^{\frac{3}{5}}$ and $t \in \mathrm{Supp}(\mathcal{HG}_{n,p,\ell})$. Then*

$$\mathcal{HG}_{n,p,\ell}(t) = \frac{\binom{\ell}{\frac{\ell+t}{2}} \cdot \binom{n-\ell}{\frac{(n-\ell)+(p-t)}{2}}}{\binom{n}{\frac{n+p}{2}}}$$

Proof. By definition it holds that

$$\mathcal{HG}_{n,p,\ell}(t) = \frac{\binom{\frac{n+p}{2}}{\frac{\ell+t}{2}} \cdot \binom{\frac{n-p}{2}}{\frac{\ell-t}{2}}}{\binom{n}{\ell}} \tag{136}$$

Compute

$$\begin{aligned}\mathcal{HG}_{n,p,\ell}(t) &= \frac{(\frac{n+p}{2})!}{(\frac{\ell+t}{2})!(\frac{(n+p)-(\ell+t)}{2})!} \cdot \frac{(\frac{n-p}{2})!}{(\frac{\ell-t}{2})!(\frac{(n-p)-(\ell-t)}{2})!} \cdot \frac{\ell!(n-\ell)!}{n!} \\ &= \frac{\binom{\ell}{\frac{\ell+t}{2}} \cdot \binom{n-\ell}{\frac{(n-\ell)+(p-t)}{2}}}{\binom{n}{\frac{n+p}{2}}},\end{aligned}$$

as required. □

The following propositions gives an estimation for the hypergeometric probability $\mathcal{HG}_{n,p,\ell}(t)$ using the almost central binomial coefficients' estimation done in Proposition A.13.

Proposition A.15. *Let $n \in \mathbb{N}$, $\ell \in [\lfloor \frac{n}{2} \rfloor]$, $p, t \in \mathbb{Z}$ be such that $|p| \leq \frac{1}{4}n^{\frac{3}{5}}$, $|t| \leq \frac{1}{4}\ell^{\frac{3}{5}}$ and $t \in \mathrm{Supp}(\mathcal{HG}_{n,p,\ell})$. Then*

$$\mathcal{HG}_{n,p,\ell}(t) = (1 \pm \mathsf{error}) \cdot \sqrt{\frac{2}{\pi}} \cdot \frac{1}{\sqrt{\ell(1-\frac{\ell}{n})}} \cdot e^{-\frac{(t-\frac{p\ell}{n})^2}{2\ell(1-\frac{\ell}{n})}},$$

for $\mathsf{error} = \xi \cdot (\frac{1}{\ell} + \frac{|t|^3}{\ell^2} + \frac{|p|^3}{n^2})$ and a universal constant ξ.

Proof. Let ξ' be the constant from Proposition A.13. In the following we focus on $n \geq 1000(1+\xi'^2)$, smaller n's are handled by setting the value of ξ to be large enough on these values. Compute

$$\begin{aligned}
\mathcal{HG}_{n,p,\ell}(t) &= \frac{\binom{\ell}{\frac{\ell+t}{2}} \cdot \binom{n-\ell}{\frac{(n-\ell)+(p-t)}{2}}}{\binom{n}{\frac{n+p}{2}}} \qquad (137)\\
&= \frac{\left((1 \pm \xi' \cdot (\frac{1}{\ell} + \frac{|t|^3}{\ell^2})) \cdot \sqrt{\frac{2}{\pi}} \cdot \frac{1}{\sqrt{\ell}} \cdot e^{-\frac{t^2}{2\ell}}\right) \cdot \left((1 \pm \xi' \cdot (\frac{1}{n-\ell} + \frac{|p-t|^3}{(n-\ell)^2})) \cdot \sqrt{\frac{2}{\pi}} \cdot \frac{1}{\sqrt{n-\ell}} \cdot e^{-\frac{(p-t)^2}{2(n-\ell)}}\right)}{(1 \pm \xi' \cdot (\frac{1}{n} + \frac{|p|^3}{n^2})) \cdot \sqrt{\frac{2}{\pi}} \cdot \frac{1}{\sqrt{n}} \cdot e^{-\frac{p^2}{2n}}}\\
&= (1 \pm \mathsf{error}') \cdot \frac{\left(\sqrt{\frac{2}{\pi}} \cdot \frac{1}{\sqrt{\ell}} \cdot e^{-\frac{t^2}{2\ell}}\right) \cdot \left(\sqrt{\frac{2}{\pi}} \cdot \frac{1}{\sqrt{n-\ell}} \cdot e^{-\frac{(p-t)^2}{2(n-\ell)}}\right)}{\sqrt{\frac{2}{\pi}} \cdot \frac{1}{\sqrt{n}} \cdot e^{-\frac{p^2}{2n}}}\\
&= (1 \pm \mathsf{error}') \cdot \sqrt{\frac{2}{\pi}} \cdot \frac{1}{\sqrt{\ell(1-\frac{\ell}{n})}} \cdot e^{-\frac{t^2}{2\ell} - \frac{(p-t)^2}{2(n-\ell)} + \frac{p^2}{n}}\\
&= (1 \pm \mathsf{error}') \cdot \sqrt{\frac{2}{\pi}} \cdot \frac{1}{\sqrt{\ell(1-\frac{\ell}{n})}} \cdot e^{\frac{-t^2(1-\frac{\ell}{n}) - (p-t)^2 \cdot \frac{\ell}{n} + p^2 \cdot \frac{\ell}{n}(1-\frac{\ell}{n})}{2\ell(1-\frac{\ell}{n})}}\\
&= (1 \pm \mathsf{error}') \cdot \sqrt{\frac{2}{\pi}} \cdot \frac{1}{\sqrt{\ell(1-\frac{\ell}{n})}} \cdot e^{-\frac{(t-\frac{p\ell}{n})^2}{2\ell(1-\frac{\ell}{n})}},
\end{aligned}$$

for $\mathsf{error}' = 8(\xi' + \xi'^2) \cdot (\frac{1}{\ell} + \frac{|t|^3}{\ell^2} + \frac{1}{n-\ell} + \frac{|p-t|^3}{(n-\ell)^2} + \frac{1}{n} + \frac{|p|^3}{n^2})$. In the second transition, the evaluation of $\binom{n-\ell}{\frac{(n-\ell)+(p-t)}{2}}$ using Proposition A.13 holds since $|p-t| \leq \frac{1}{2}n^{\frac{3}{5}} \leq (\frac{1}{2}n)^{\frac{3}{5}} \leq (n-\ell)^{\frac{3}{5}}$. By letting $\mathsf{error} = \xi \cdot (\frac{1}{\ell} + \frac{|t|^3}{\ell^2} + \frac{|p|^3}{n^2})$ for $\xi = 40(\xi' + \xi'^2)$, we conclude that

$$\mathcal{HG}_{n,p,\ell}(t) = (1 \pm \mathsf{error}) \cdot \sqrt{\frac{2}{\pi}} \cdot \frac{1}{\sqrt{\ell(1-\frac{\ell}{n})}} \cdot e^{-\frac{(t-\frac{p\ell}{n})^2}{2\ell(1-\frac{\ell}{n})}}, \qquad (138)$$

as required. □

I case we have tighter bound on $|n|$ and $|t|$, we get the following estimation.

Proposition A.16. *Let $n \in \mathbb{N}$, $\ell \in [\lfloor \frac{n}{2} \rfloor]$, $p, t \in \mathbb{Z}$ and $\lambda > 0$ be such that $|p| \leq \lambda \cdot \sqrt{n \log n}$, $|t| \leq \lambda \cdot \sqrt{\ell \log \ell}$ and $t \in \mathrm{Supp}(\mathcal{HG}_{n,p,\ell})$. Then*

$$\mathcal{HG}_{n,p,\ell}(t) = (1 \pm \mathsf{error}) \cdot \sqrt{\frac{2}{\pi}} \cdot \frac{1}{\sqrt{\ell(1 - \frac{\ell}{n})}} \cdot e^{-\frac{(t - \frac{p\ell}{n})^2}{2\ell(1 - \frac{\ell}{n})}},$$

for $\mathsf{error} = \varphi(\lambda) \cdot \frac{\log^{1.5} \ell}{\sqrt{\ell}}$ *and a universal function* φ.

Proof. There exists a function $\vartheta \colon \mathbb{R}^+ \mapsto \mathbb{N}$ such that $\frac{1}{4}\ell^{\frac{3}{5}} > \lambda \cdot \sqrt{\ell \log \ell}$ for every $\ell \geq \vartheta(\lambda)$. In the following we focus on $\ell \geq \max(\vartheta(\lambda), 10)$, where smaller ℓ's are handled by setting the value of $\varphi(\lambda)$ to be large enough on these values. Let ξ be the constant from Proposition A.15. Note that

$$\xi \cdot (\frac{1}{\ell} + \frac{|t|^3}{\ell^2} + \frac{|p|^3}{n^2}) \leq \xi \cdot (2\lambda^3 + 1) \cdot \frac{\log^{1.5} \ell}{\sqrt{\ell}} \tag{139}$$

Thus, the proposition holds by Proposition A.15 and by setting $\varphi(\lambda) := \xi \cdot (2\lambda^3 + 1)$. □

Proposition A.17. *[Restatement of Proposition 2.7] Let $n \in \mathbb{N}$, $\ell \in [\lfloor \frac{n}{2} \rfloor]$, $p, k \in [n]$ and $\lambda > 0$ be such that $|p| \leq \lambda \cdot \sqrt{n \log n}$ and $|k| \leq \lambda \cdot \sqrt{\ell \log \ell}$. Then*

$$\widehat{\mathcal{HG}}_{n,p,\ell}(k) \in \Phi\left(\frac{k - \frac{p \cdot \ell}{n}}{\sqrt{\ell(1 - \frac{\ell}{n})}}\right) \pm \mathsf{error},$$

where $\mathsf{error} = \varphi(\lambda) \cdot \frac{\log^{1.5} \ell}{\sqrt{\ell}}$ *for some universal function* φ.

Proof. Let φ' be the function from Proposition A.16. By Fact A.12 and Proposition A.16 and using the proposition's bounds, it follows that $\mathcal{HG}_{n,p,\ell}$ is a $(\ell, \ell(1 - \frac{\ell}{n}), \lambda, \varphi'(\lambda))$-bell-like distribution according to Definition A.1. Therefore, by Proposition A.4 it follows that

$$\widehat{\mathcal{HG}}_{n,p,\ell}(k) \in \Phi\left(\frac{k - \frac{p \cdot \ell}{n}}{\sqrt{\ell(1 - \frac{\ell}{n})}}\right) \pm (4\varphi'(\lambda) + 5) \cdot \frac{\log^{1.5} \ell}{\sqrt{\ell}},$$

as required. □

Proposition A.18. *[Restatement of Proposition 2.8] Let $n \in \mathbb{N}$, $\ell \in [\lfloor \frac{n}{2} \rfloor]$, $p, k \in [n]$ and $\lambda > 0$ be such that $|p| \leq \lambda \cdot \sqrt{n \log n}$ and $|k| \leq \lambda \cdot \sqrt{\ell \log \ell}$ and let $\delta = \widehat{\mathcal{HG}}_{n,p,\ell}(k)$. Then for every $m \geq \ell$ it holds that*

$$\widehat{\mathcal{C}}_m^{-1}(\delta) \in \frac{\frac{p \cdot \ell}{n} - k}{\sqrt{m \cdot \ell(1 - \frac{\ell}{n})}} \pm \mathsf{error},$$

where $\mathsf{error} = \varphi(\lambda) \cdot \frac{\log^{1.5} \ell}{\sqrt{m \cdot \ell}}$ *for some universal function* φ.

Proof. Let φ' be the function from Proposition A.16, and let φ'' be the function from Proposition A.5. By Fact A.12 and Proposition A.16 and using the proposition's bounds, it follows that $\mathcal{HG}_{n,p,\ell}$ is a $(\ell, \ell(1-\frac{\ell}{n}), \lambda, \varphi'(\lambda))$-bell-like distribution according to Definition A.1. Note that there exists a function $\vartheta\colon \mathbb{R}^+ \mapsto \mathbb{N}$ such that conditions 1, 2 and 3 of Proposition A.5 hold for every $\ell \geq \vartheta(\lambda)$ (with respect to $v := \ell(1-\frac{\ell}{n})$ and $\xi := \varphi'(\lambda)$). In the following we focus on $\ell \geq \vartheta(\lambda)$, where smaller ℓ's are handled by setting the value of $\varphi(\lambda)$ to be large enough on these values. Now we can apply Proposition A.7 to get that

$$\widehat{\mathcal{C}}_m^{-1}(\delta) \in \frac{\frac{p\cdot\ell}{n} - k}{\sqrt{m\cdot v}} \pm \left(\varphi''(2\lambda^2+1) + 2\cdot\left(4\varphi'(\lambda)+5\right)\right)\cdot\frac{\log^{1.5}\ell}{\sqrt{m\cdot\ell}},$$

as required. □