An Almost-Optimally Fair Three-Party Coin-Flipping Protocol[*]

Iftach Haitner[†]   Eliad Tsfadia[†]

May 5, 2021

Abstract

In a multiparty *fair* coin-flipping protocol, the parties output a common (close to) unbiased bit, even when some corrupted parties try to bias the output. Cleve [STOC 1986] has shown that in the case of dishonest majority (i.e., at least half of the parties can be corrupted), in *any* m-round coin-flipping protocol the corrupted parties can bias the honest parties' common output bit by $\Omega(\frac{1}{m})$. For more than two decades the best known coin-flipping protocols against dishonest majority had bias $\Theta(\frac{\ell}{\sqrt{m}})$, where ℓ is the number of corrupted parties. This was changed by a recent breakthrough result of Moran et al. [TCC 2009], who constructed an m-round, *two*-party coin-flipping protocol with optimal bias $\Theta(\frac{1}{m})$. In a subsequent work, Beimel et al. [Crypto 2010] extended this result to the multiparty case in which *less than* $\frac{2}{3}$ of the parties can be corrupted. Still for the case of $\frac{2}{3}$ (or more) corrupted parties, the best known protocol had bias $\Theta(\frac{\ell}{\sqrt{m}})$. In particular, this was the state of affairs for the natural three-party case.

We make a step towards eliminating the above gap, presenting an m-round, three-party coin-flipping protocol, with bias $\frac{O(\log^3 m)}{m}$. Our approach (which we also apply for the two-party case) does not follow the "threshold round" paradigm used in the work of Moran et al. and Beimel et al., but rather is a variation of the majority protocol of Cleve, used to obtain the aforementioned $\Theta(\frac{\ell}{\sqrt{m}})$-bias protocol.

Keywords: coin-flipping; protocols; fairness; fair computation

Contents

1   Introduction

In a multi-party *fair* coin-flipping (-tossing) protocol, the parties output a common (close to) unbiased bit, even though some corrupted parties 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 output a common bit, regardless of what the corrupted parties do. In particular, they are not allowed to abort if a cheat was noticed.

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 [13].[1] When an honest majority is not guaranteed, however, the situation is more complex.

Negative results.   Cleve [17] showed that for *any* efficient two-party m-round coin-flipping protocol, there exists an efficient adversary to bias the output of the honest party by $\Theta(1/m)$, and that the lower bound extends to the multi-party case via a simple reduction.

Positive results.   Assuming one-way functions exist, Cleve [17] showed that a simple m-round majority protocol can be used to derive a t-party coin-flipping protocol with bias $\Theta(\frac{\ell}{\sqrt{m}})$ (against dishonest majority), where ℓ is the number of corrupted parties. For more than two decades, Cleve's protocol was the best known fair coin-flipping protocol (without honest majority), under *any* hardness assumption, and for *any* number of parties. In a recent breakthrough result, Moran et al. [41] constructed an m-round, *two*-party coin-flipping protocol with optimal bias of $\Theta(\frac{1}{m})$. The result holds for any parameter $m \in \mathbb{N}$, and under the assumption that oblivious transfer protocols exist. In a subsequent work, Beimel et al. [10] extended the result of [41] 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.

Still for the case of $\frac{2}{3}$ (or more) corrupted parties, the best known protocol was the $\Theta(\frac{\ell}{\sqrt{m}})$-bias majority protocol of [17]. In particular, this was the state of affairs for the natural three-party case (where two parties are corrupt).

1.1   Our Result

We present an almost-optimally fair, three-party coin-flipping protocol.

Theorem 1.1 (main theorem, informal). *Assuming the existence of oblivious transfer protocols,[2] then for any $m \in \mathbb{N}$ there exists an m-round, three-party coin-flipping protocol, with bias $\frac{O(\log^3 m)}{m}$ (against one, or two, corrupted parties).*

---

[1]Throughout, we assume a broadcast channel is available to the parties. By [19], broadcast channel is necessary for fair coin-flipping protocol secure against third, or more, corruptions.

[2]It is enough to assume the existence of a constant-round secure-with-abort protocol, which is a weaker assumption. However, we chose to assume OT for simplifying the main theorem.

That is, no efficient algorithm can makes the (expected) outcome of the protocol to deviate from $\frac{1}{2}$ by more than $\frac{O(\log^3 m)}{m}$. As a building block towards constructing our three-party protocol, we present an alternative construction for two-party, almost-optimally fair coin-flipping protocols. Our approach does not follow the "threshold round" paradigm used in [41, 10], but rather is a variation of the aforementioned $\Theta(\frac{\ell}{\sqrt{m}})$-bias, coin-flipping protocol of [17].

1.2 Additional Related Work

Cleve and Impagliazzo [18] showed that in the *fail-stop model*,[3] any two-party m-round coin-flipping protocol has bias $\Omega(\frac{1}{\sqrt{m}})$; 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. [20] 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 [15, 34, 42]. To a large extent, one-way functions are also necessary for such coin-flipping protocols [14, 31, 36, 39].

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 [4, 12, 22, 44, 45], and protocols based on physical assumptions, such as quantum computation [2, 5, 6] and tamper-evident seals [40].

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 [17]'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, 7, 8].

1.3 Our Techniques

The following is a high-level description of the ideas underlying our three-party fair coin flipping protocol.[4] We start by describing the two-party protocol of Moran et al. [41] (hereafter the MNS protocol), and explain why natural extensions of their approach (such as the one used in [10]) fall short when it comes to constructing three-party fair protocols. We next explain our new approach for two-party protocols, and then extend this approach to three parties.

Throughout, we assume without loss of generality that if a corrupted party aborts in a given round, it sends an abort message to all other parties at the *end* of this round (after seeing the messages sent by the non-aborting parties). To keep the discussion simple, we focus on security against polynomially bounded fail-stop adversaries — ones that follow the prescribed protocol, but

---

[3]In this model, the parties are assumed to have unbounded computation power, cannot deviate from the prescribed protocol, but are allowed to prematurely abort their execution.

[4]We restrict the discussion to the intuitive game-base definition of fairness — the goal of the adversary is to make the honest party to output some bit b with probability as further away from $\frac{1}{2}$ as possible. Discission of the more standard Real/Ideal definition of fairness, in which we prove our result, is given in Section 2.6.

might abort prematurely. Achieving this level of security is the heart of the matter, since (assuming one-way functions exist) there exists a round-preserving reduction from protocols secure against fail-stop adversaries into protocols of full-fledged security [26].[5]

1.3.1 The Two-Party MNS Protocol

For $m \in \mathbb{N}$, the $(2m)$-round, two-party MNS protocol $(\mathsf{P}_0, \mathsf{P}_1)$ is defined as follows.[6] Following a common paradigm for fair multi-party computations [10, 28, 38], the protocol starts by the two parties using oblivious transfer (OT) to securely compute the following "share generating" random function.

Algorithm 1.2 (share generating function SharesGen).

Input: Round parameter 1^m.

Operation:

1. *Uniformly sample $c \leftarrow \{0,1\}$ and $i^* \leftarrow [m]$ $(= \{1, \ldots, m\})$.*

2. *For $i = 1$ to m, let*

    (a) $(d_i^0, d_i^1) = \begin{cases} \text{uniform } \textit{sample from } \{0,1\}^2, & i < i^* - 1 \\ (c,c), & \textit{otherwise.} \end{cases}$

    (b) $c_i = \begin{cases} \bot, & i < i^* \\ c, & \textit{otherwise.} \end{cases}$

3. *Split each of the $3m$ values $d_1^0, d_1^1, \ldots, d_m^0, d_m^1, c_1, \ldots, c_m$ into two "shares," using a 2-out-of-2 secret sharing scheme, and output the two sets of shares.*

Protocol 1.3 $((\mathsf{P}_0, \mathsf{P}_1))$.

Common input: round parameter 1^m.

Initial step: The parties securely compute $\mathsf{SharesGen}(1^m)$, where each party gets one set of shares.

Main loop: For $i = 1$ to m, do

   (a) P_0 *sends to* P_1 *its share of* d_i^1, *and* P_1 *sends to* P_0 *its share of* d_i^0.

   - P_0 *reconstructs the value of* d_i^0, *and* P_1 *reconstructs the value of* d_i^1.

   (b) *Each party sends to the other party its share of* c_i.

   - *Both parties reconstruct the value of* c_i.

Output: The parties output c_i, for the first i for which $c_i \neq \bot$.

---

[5]Note that by restricting the parties to being fail-stop, we do not reduce the setting to the fail-stop model, since the parties considered here are computationally bounded.

[6]The protocol described below is a close variant of the original MNS protocol, which serves our presentation better. The difference is the addition of phase (b), in both the share generating function and the protocol, which does not exists in the original protocol.

Abort: If P_0 *aborts, party* P_1 *outputs the value of* d_i^1 *for the* maximal $i \in [m]$ *for which it has reconstructed this value. If there is no such* i, P_1 *outputs a uniform bit. (The case that* P_1 *aborts is analogously defined).*

We start with few observations regarding the secure computation of $\mathsf{SharesGen}(1^m)$ done in the above protocol.

- The computation of $\mathsf{SharesGen}(1^m)$ is *not* fair: the parties get their parts of the output (i.e., their shares) in an *arbitrary* manner. Specifically, the corrupted party might prematurely abort after learning its part of the output, preventing the other party from getting its part.

- Since $\mathsf{SharesGen}(1^m)$ is efficient, assuming OT protocols exist, an (unfair) secure computation of $\mathsf{SharesGen}(1^m)$ exists.

- Ignoring negligible terms (due to the imperfection of secure computation using OT), the output of each party (when seen on its own) is a set of uniform strings. In particular, it contains *no information* about the other party's shares, or about the values of c and i^*.

  By construction, a party outputs a uniform bit if the other party aborts before the end of the secure computation phase. Hence, it makes no sense for a party to abort during this phase.

- Given the above observation, it is instructive to pretend that at the first step of the protocol, the output of a random execution of $\mathsf{SharesGen}(1^m)$ was given to the parties by an *honest dealer*.

Note that in each round of the above protocol, both honest parties send their messages without waiting for the other party's message. Hence, the above protocol is symmetric with respect to the parties' role. However, since we assume no simultaneous channel (which would have trivialized the whole question), the corrupted party can postpone sending its message until it gets the message of the honest party, and then decide whether to send its message for this round or abort.

Security of the protocol. At least on the intuitive level, the security proof of the above protocol is rather simple. Since the protocol is symmetric, we assume for concreteness that P_0 is corrupted and tries to bias the expected output of P_1 away from $\frac{1}{2}$. The following random variables are defined with respect to a random execution of $(\mathsf{P}_0, \mathsf{P}_1)$: let V be the view of the corrupted P_0, right after sending the abort message, and let V^- be the view V without this abort message. For a view v, let $\mathsf{val}(v)$, the view *value*, be defined as the expected outcome of P_1 conditioned that P_0's view is v, assuming no further aborts (i.e., if P_0 is not aborting in v, then it acts honestly till the end of the protocol). It is not hard to verify that the bias obtained by P_0 (toward 0 or 1) is *exactly* the expected value of $|\mathsf{val}(V) - \mathsf{val}(V^-)|$.[7]

It is also easy to see that by aborting in round (i, b) (i.e., phase (b) of round i), for some $i \in [m]$, party P_0 gains nothing (i.e., $\mathsf{val}(V) = \mathsf{val}(V^-)$), where the (i, j)'th round of the execution stands for the j'th step of the i'th loop in the execution. A slightly more complicated math yields that by aborting in round (i, a), party P_0 only gains $\Theta(\frac{1}{m})$ bias. It follows that the maximal bias obtained by a fail-stop strategy for P_0 is $\Theta(\frac{1}{m})$.

---

[7]The expected value of $|\mathsf{val}(V) - \mathsf{val}(V^-)|$ actually captures the security of the protocol in a stronger sense, characterizing the so-called α-security of the protocol according to the Real/Ideal paradigm. See proof in Section 2.7.

Fairness via defense. Let us present a different view of the MNS protocol. Consider a variant of this protocol without the d_i's. Namely, the parties reconstruct $c_1, \ldots, c_m$ one at a time, until they reach $c_i \neq \perp$. When an abort occurs, the remaining party outputs an unbiased coin if it has not yet reconstructed c, and outputs c otherwise. It is easy to see that an aborting attacker can bias the output of the other party in this degenerate variant by $\frac{1}{4}$; that is, it simply waits until it reconstructs c and then aborts for biasing the other party's output towards $1 - c$.

The role of "defense" values $(d_i^0, d_i^1), \ldots, (d_m^0, d_m^1)$ is to prevent such an attack; if a party aborts after reconstructing c, the other party is guaranteed to output c as well. The problem is, however, that the defense values themselves might cause a problem: a corrupted party might abort after reconstructing its defense value for the i'th round (and not only after reconstructing c_i). Indeed, by aborting in these rounds, a corrupted party does gain a bias, but only $\Theta(\frac{1}{m})$.

On extending the MNS protocol for the three-party case. We next explain why the approach of MNS does not seem to be useful for constructing fair, three-party coin-flipping protocols.

In a three-party fair coin-flipping protocol, one should deal with two, possibly non-simultaneous, aborts. In particular, after P_0 aborts, the remaining pair of parties $\{\mathsf{P}_1, \mathsf{P}_2\}$ should interact in a two-party protocol to agree on their common coin. Since one of $\{\mathsf{P}_1, \mathsf{P}_2\}$ might be also corrupted, this two-party protocol needs to be a fair coin-flipping protocol as well. Assuming P_0 aborts in round i, the expected outcome of this two-party protocol should be equal (up to an additive difference of $\Theta(\frac{1}{m})$) to the expected outcome of the three party protocol assuming no aborts, from P_0's point of view, *after* getting the i'th round messages. Otherwise, P_0, by aborting after seeing the messages sent by $\{\mathsf{P}_1, \mathsf{P}_2\}$ in this round, can bias the outcome of the other parties by more than $\Theta(\frac{1}{m})$.

Consider the following natural extension of MNS protocol to a three-party protocol. The value of $c_1, \ldots, c_m$ are as in the two-party protocol (now shared between the three parties). The defense values are not bits, but rather two vectors of shares for the two remaining parties (different shares for each possible pair), to enable them to interact in some fair two-party coin-flipping protocol if the third party aborts. Assume that in the i'th round of the "outer" three-party protocol, the value of c_i is one (i.e., $c_i = c = 1$), and consider the two-party protocol executed by the remaining parties, if a party aborts in this round. The outcome of the remaining party in the case of a premature abort in this underlying two-party protocol should be also one. Otherwise, two corrupted parties can mount the following two-phase attack: first aborting in the outer three-party protocol after seeing $c_i = 1$, and then prematurely aborting in the inner two-party protocol, knowing that the other party will output something that is far from one. Now, assume that in the i'th round of the "outer" three-party protocol, the value of c_i is $\perp$ (i.e., $i < i^*$), and consider again the two-party protocol executed by the remaining parties if party aborts in this round. It is easy to see that expected outcome of this two-party protocol should be close to $\frac{1}{2}$ (i.e., unbiased). Thus, the defense values, to be constructed by each party during the execution of this two-party protocol, cannot all be of the same value.

But the above restrictions on the two-party protocol defense values, ruin the security of the outer three-party protocol; in each round i, two corrupted (and thus colluding) parties can reconstruct the *whole* two-party execution that they should engage in if the other (in this case, the honest) party aborts in this round. By checking whether the defense values of this two-party execution are all ones (indicating that $c = 1$), all zeros (indicating that $c = 0$), or mixed (indicating that $c_i = \perp$), they get enough information for biasing the output of the protocol by a constant value.

What fails the above three-party protocol, is that during its execution the expected outcome

of the protocol given a player's view might change by a constant (say from $\frac{1}{2}$ to 1). As we argued above, the (long) defense values reconstructed *before* each round in the three-party protocol have to contain many (i.e., m) samples drawn according to the value of the protocol at the *end* of the round. It follows that two corrupted parties might extrapolate, at the *beginning* of such a round, the value of protocol when this round *ends*, thus rendering the protocol insecure.

To conclude, due to the restrictions described above which comes from the large jump in the game value of MNS, extending it into three-party protocol seems unlikely.

1.3.2 Our Two-Party Protocol

Given the above understanding, our first step is to construct a two-party coin-flipping protocol, whose value only changes *slightly* (i.e., smoothly) between consecutive rounds. In the next section we use a *hiding* variant of such a smooth coin-flipping protocol as a building block for constructing an (almost) optimally fair three-party protocol.

Consider the $\Theta(\frac{1}{\sqrt{m}})$-bias coin-flipping protocol of Cleve [17]: in each round $i \in [m]$, the parties reconstruct the value of a coin $c_i \in \{-1,1\}$, and the final outcome is set to $\mathsf{sign}(\sum_{i\in[m]} c_i)$. Since the value of $\sum c_i$ is close to being uniform over $[-\sqrt{m}, \sqrt{m}]$, the value of the first coin c_1 changes the protocol's value by $\Theta(\frac{1}{\sqrt{m}})$. This sounds like a good start toward achieving a smooth coin-flipping protocol.

The protocol. As in MNS protocol, the parties start by securely computing a share generating function, and then use its outputs to slowly reconstruct the output of the protocol.

Let $\mathcal{B}er(\delta)$ be the Bernoulli distribution over $\{0,1\}$, taking the value one with probability δ and zero otherwise.

We next describe (a simplified variant of) our share generating function and use it to describe our two-party protocol.

Algorithm 1.4 (share generating function TwoPartySharesGen).

Input: Round parameter 1^m.

Operation:

1. *For $z \in \{0,1\}$, sample $d_0^z \leftarrow \{0,1\}$.*

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

   (a) *Sample $c_i \leftarrow \{-1,1\}$.*

   (b) *For $z \in \{0,1\}$, sample $d_i^z \leftarrow \mathcal{B}er(\delta_i)$, for $\delta_i = \Pr\left[\sum_{j=1}^m c_j \geq 0 \mid c_1, \ldots, c_i\right]$.[8]*

3. *Split each of the $3m$ values $d_1^0, d_1^1, \ldots, d_m^0, d_m^1, c_1, \ldots, c_m$ into two "shares", using a 2-out-of-2 secret sharing scheme, to create two sets of shares: $\mathbf{s}^{\#\mathbf{0}}$ and $\mathbf{s}^{\#\mathbf{1}}$.*

4. *Output $(d_0^0, \mathbf{s}^{\#\mathbf{0}}), (d_0^1, \mathbf{s}^{\#\mathbf{1}})$.*

Protocol 1.5 ($\pi_2 = (\mathsf{P}_0^2, \mathsf{P}_1^2)$)**.**

---

[8]δ_i is the probability that the protocol's output is one, given the value of the "coins" $c_1 \ldots, c_i$ (and assuming no abort).

6

Common input: round parameter 1^m.

Initial step: The parties securely compute $\mathsf{TwoPartySharesGen}(1^m)$. *Let* $(d_0^i, \mathbf{s}^{\#\mathbf{i}})$ *be the local output of* P_i^2.

Main loop: For $i = 1$ to m, do

    (a) P_0^2 sends to P_1^2 its share of d_i^1, and P_1^2 sends to P_0^2 its share of d_i^0.

      • *P_0^2 reconstructs the value of d_i^0, and P_1^2 reconstructs the value of d_i^1.*

    (b) Each party sends to the other party its share of c_i.

      • *Both parties reconstruct the value of c_i.*

Output: Both parties output one if $\sum_{j=1}^m c_j \geq 0$, and zero otherwise.

Abort: If P_0^2 aborts, party P_1^2 outputs the value of d_i^1, for the maximal $i \in [m]$ for which it has reconstructed this value (note that by construction such an i always exists).

    The case that P_1^2 aborts is analogously defined.

Namely, the parties interact in a majority protocol, where in the i'th round, they reconstruct, in an unfair manner, the i'th coin (i.e., c_i). If a party aborts, the remaining party outputs a defense value given to it by the honest dealer (implemented via the secure computation of $\mathsf{TwoPartySharesGen}$).

A few remarks are in place. First, we will only define the protocol for odd values of m. Hence, $\sum_{j=1}^m c_j \neq 0$, and the protocol's output is a uniform bit when played by the honest parties. Second, if P_0^2 aborts in the first round, the party P_1^2 could simply output a uniform bit. We make P_0^2 output d_0^1, since this be useful when the two-party protocol will be later used as part of the three-party protocol. Finally, one can define the above protocol without exposing the coins c_i's to the parties (in this case, the honest parties output (d_m^0, d_m^1) as the final outcome). We do expose the coins to make the analysis of the protocol easier to follow.

Security of the protocol. Note that the defense value given in round (i, a) (i.e., step a of the i'th loop) is distributed according to the expected outcome of the protocol, conditioned on the value of the coin to *be given* in round (i, b). These defense values make aborting in round (i, b), for any value of i, harmless. So it is left to argue that aborting in round (i, a), for any value of i, is not too harmful either. Intuitively, this holds since the defense value reconstructed in round (i, a) is only a noisy signal about the value of c_i.

Since the protocol is symmetric, we assume for concreteness that the corrupted party is P_0^2. Similar to the analysis of the MNS protocol sketched above, it suffices to bound the value of $|\mathsf{val}(V) - \mathsf{val}(V^-)|$.

Assume that P_0^2 aborts in round (i, b). By construction, $\mathsf{val}(V^-) = \delta_i$. Since, the defense of P_1^2 in round (i, b) is sampled according to $\mathcal{B}er(\delta_i)$, it is also the case that $\mathsf{val}(V) = \delta_i$.

Assume now that P_0^2 aborts in round (i, a). By construction, $\mathsf{val}(V) = \delta_{i-1}$. Note that V^- does contains some information about δ_i, i.e., a sample from $\mathcal{B}er(\delta_i)$, and thus $\mathsf{val}(V^-)$ is typically different from $\mathsf{val}(V)$. Yet, since V^- contains only a sample from $\mathcal{B}er(\delta_i)$, a noisy signal for the actual value of δ_i, we manage to prove the following.

$$\left| \mathsf{val}(V) - \mathsf{val}(V^-) \right| = \mathrm{E}\left[\frac{(\delta_i - \delta_{i-1})^2}{\delta_{i-1}} \mid \delta_{i-1} \right] \tag{1}$$

If P_0^2 aborts in the first rounds, Equation (1) yields that $|\mathsf{val}(V) - \mathsf{val}(V^-)| = O(\frac{1}{m})$ since by the "smoothness" of the protocol (i.e., the value of the game does not change drastically between consecutive rounds) it follows that $\left|\frac{\delta_i - \delta_{i-1}}{\delta_{i-1}}\right| \in O(\frac{1}{\sqrt{m}})$. The problem is, however, that with probability $\Theta(\frac{1}{\sqrt{m}})$, the sum of $c_1, \ldots, c_{m-1}$ is exactly zero. Hence, with this probability, the final coin changes the protocol's value by $\frac{1}{2}$. Therefore, the bias obtained by P_0^2 that just wait to the last round to abort is $\Theta(\frac{1}{\sqrt{m}})$.

We overcome the above problem by using a *weighted* majority variant of the protocol. In the first round the parties reconstruct m-coins (in a single shot), reconstruct $(m-1)$ coins in the second round, and so on, until in the very last round only a single coin is reconstructed. Now the value of $\sum c_i$ (now each c_i is an integer) is close to being uniform over $[-m, m]$, and the last round determines the outcome only with probability $\Theta(\frac{1}{m})$ (versus $\Theta(\frac{1}{\sqrt{m}})$ in the unweighted version). Other rounds also enjoy a similar smoothness property. See Section 3 for more details.

1.3.3 Our Three-Party Protocol

We start by applying a generic approach, introduced by Beimel et al. [10], to try and extend our fair two-party protocol into a three-party one. We explain why this approach falls short, and present a variant of our two-party protocol for which the generic approach does yield the desired three-party protocol. To keep the presentation simple, the two-party protocol we use is the *non*-weighted variant of our two-party protocol (the actual implementation uses the aforementioned weighted protocol).

In this first attempt protocol, the three parties interact in the following variant of the two-party protocol π_2 described in Protocol 1.5. The parties start by (securely) computing ThreePartySharesGen(1^m) defined below.

For $\delta \in [0, 1]$, let TwoPartySharesGen($1^m, \delta$) be the following variant of TwoPartySharesGen defined above: (1) the "coin" c_i takes the value 1 with probability $\frac{1}{2} + \varepsilon$ and -1 otherwise (and not a uniform coin over $\{-1, 1\}$ as in TwoPartySharesGen), where ε is set to the number such that $\Pr\left[\sum_{i=1}^m c_i \geq 0\right] = \delta$; (2) the initial defense values d_0^0 and d_0^1 are sampled according to $\mathcal{Ber}(\delta)$ (and not $\mathcal{Ber}(\frac{1}{2})$ as in TwoPartySharesGen).

Algorithm 1.6 (share generating function ThreePartySharesGen)**.**

Input: Round parameter 1^m.

Operation:

1. *For $i = 1$ to m,*

   (a) *Sample $c_i \leftarrow \{-1, 1\}$.*

   (b) *For each pair of the three parties, generate shares for an execution of π_2, by calling TwoPartySharesGen$(1^m, \delta_i)$ for $\delta_i = \Pr\left[\sum_{j=1}^m c_j \geq 0 \mid c_1, \ldots, c_i\right]$.*

2. *Split the values of $c_1, \ldots, c_m$ and the defense values into three set of shares using a 3-out-of-3 secret sharing scheme, and output the three sets.*

Protocol 1.7 ($\pi_3 = (P_0^3, P_1^3, P_2^3)$)**.**

Common input: round parameter 1^m.

Initial step: The parties securely compute $\mathsf{ThreePartySharesGen}(1^m)$, *where each party gets one set of shares.*

Main loop: For $i = 1$ *to* m, *do*

    (a) Each party sends to the other parties its share of their defense values.

- *Each pair* $(\mathsf{P}_z^3, \mathsf{P}_{z'}^3)$ *of the parties reconstructs a pair of two sets of shares* $d_i^{z,z'} = ((d_i^{z,z'})_z, (d_i^{z,z'})_{z'})$, *to serve as input for an execution of the two-party protocol if the third party aborts (i.e.,* P_z^3 *reconstructs* $(d_i^{z,z'})_z$, *and* $\mathsf{P}_{z'}^3$ *reconstructs* $(d_i^{z,z'})_{z'}$*).*

    (b) Each party sends the other parties its share of c_i.

- *All parties reconstruct the value of* c_i.

Output: The parties output one if $\sum_{j=1}^{m} c_j \geq 0$, *and zero otherwise.*

Abort: • *If* P_0^3 *aborts, the parties* P_1^3 *and* P_2^3 *use the shares of* $d_i^{1,2}$, *for the* maximal $i \in [m]$ *that has been reconstructed, to interact in* π^2 *(starting right after the share reconstruction phase). If no such* i *exists, the parties interact in the (full, unbiased) two-party protocol* π^2.

        The case that P_1^3 *or* P_2^3 *aborts is analogously defined.*

- *If two parties abort in the same round, the remaining party acts as if one party has only aborted in the very beginning of the two-party protocol.*

Similar to the analysis for the two-party protocol sketched above, it suffices to show that the defense values reconstructed by a pair of corrupted parties in round (i, a) (i.e., the inputs for the two-party protocols) do not give too much information about the value of δ_i — the expected outcome of the three-party protocol conditioned on the coins reconstructed at round (i, b). Note that once two corrupted parties are given these defense values, which happens in round (i, a), they can *immediately* reconstruct the whole two-party execution induced by them. This two-party execution effectively contains $\Theta(m)$ *independent* samples from $\mathcal{B}er(\delta_i)$: one sample is given explicitly as the final output of the execution, and the value of $2m$ additional samples can be extrapolated from the $2m$ defense values given to the two parties. Many such independent samples can be used to reveal the value of δ_i just by looking at the sum of those $2m$ samples, and guess its value according to it.[9] Hence, in round (i, a), two corrupted parties can rush and use the above information to bias the outcome of the three-party protocol by $\Theta(|\delta_i - \delta_{i-1}|) \in \Omega(\frac{1}{\sqrt{m}})$.

We solve this issue using a *hiding* variant of the two-party shares generating function — a function that leaks only *limited* information about the value of δ_i. See details in Section 3.

1.4 Open Problems

The existence of an optimally fair three-party coin-flipping protocol (without the $\text{poly}(\log m)$ factor) is still an interesting open question. A more fundamental question is whether there exist fair coin-flipping protocols for more than three parties (against any number of corrupted parties). A question

---

[9]This can be done by the following process: If the sum is greater than $2m \cdot \delta_{i-1}$, guess that $c_i = 1$. Otherwise, guess that $c_i = -1$. Since $|\delta_i - \delta_{i-1}| \in \Omega(\frac{1}{\sqrt{m}})$, it follows by Hoeffding inequality [35] that the guess is good with probability $\frac{1}{2} + \Theta(1)$. Similarly, it can be shown that the same problem also holds in the weighted variant of the protocol which mentioned in the security proof of Protocol 1.5

of a larger scope, is to find $1/m$-fair protocol for other many-party functionality, as done by Gordon and Katz [27] for two-party functionalities. In particular, can one harness our three-party protocol for this aim.

Finally, some of the proofs we give for bounding the values of the Binomial games, which are in sense equivalent to bounding the bias of our coin-flipping protocols, are long and tedious. Finding simpler proofs would be a good service, and might yield tighter bounds and increase our understanding of these protocols.

Paper Organization

General notations and definitions used throughout the paper are given in Section 2. We also state there (Section 2.7.1) a new game-based definition of fair coin-flipping protocols, which is equivalent to the standard real/ideal definition. Our coin-flipping protocols, along with their security proofs, are given in Section 3. The security proofs of Section 3 use bounds on the value of several types of online-binomial games, these bounds are proven in Section 4. 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 $a \in \mathbb{R}$ 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 $f(\mathcal{S}_1, \ldots, \mathcal{S}_k) := \{f(x_1, \ldots, x_j) : x_i \in \mathcal{S}_i\}$, e.g., $f(1 \pm 0.1) = \{f(x) : x \in [.9, 1.1]\}$. 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 bits.

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 $p \in$ poly and large enough n.

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.[10] 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 $\widehat{\mathcal{C}}_{n,\varepsilon}(k) :=$

---

[10]Notice the slight change in notation comparing to the those used in the introduction.

$\Pr_{x \leftarrow \mathcal{C}_{n,\varepsilon}}[x \geq k] = \sum_{t=k}^{n} \mathcal{C}_{n,\varepsilon}(t)$. 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 $p \in \{-n, \dots, n\}$, 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 $w(v) = p$. 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 $\ell_n(i) := n + 1 - i$ 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
$[n]$	$n \in \mathbb{N}$	$\{1, \dots, n\}$
(n)	$n \in \mathbb{N}$	$\{0, \dots, n\}$
$\ell_n(i)$	$n \in \mathbb{N}$, $i \in [n]$	$n + 1 - i$
$\mathsf{sum}_n(i)$	$n \in \mathbb{N}$, $i \in [n]$	$\sum_{j=i}^{n} \ell_n(j)$
$\Phi(x)$	$x \in \mathbb{R}$	$\frac{1}{\sqrt{2\pi}} \int_x^{\infty} e^{-\frac{t^2}{2}} dt$
$w(v)$	$v \in \{-1,1\}^*$	$\sum_{i \in \mathcal{I}} v_i$
$v_{\mathcal{I}}$	$v \in \{-1,1\}^*$, $\mathcal{I} \subseteq [|v|]$ and $i_1, \dots, i_{|\mathcal{I}|}$ are the ordered elemets of $\mathcal{I}$	$(v_{i_1}, \dots, v_{i_{|\mathcal{I}|}})$
$\mathrm{SD}(P,Q)$	distributions P and Q over a finite set $\mathcal{U}$	$\frac{1}{2} \sum_{u \in \mathcal{U}} |P(u) - Q(u)|$
$\mathrm{Supp}(D)$	distributions D over a finite set $\mathcal{U}$	$\{u \in \mathcal{U} : D(u) > 0\}$
$a \pm b$	$a \in \mathbb{R}$, $b \geq 0$	$[a - b, a + b]$

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: Other Functions.

Definition	Input Range	Output value
$\mathcal{C}_{n,\varepsilon}(k)$	$n \in \mathbb{N},\ \varepsilon \in [-1,1],\ k \in \mathbb{Z}$	$\Pr_{x \leftarrow \mathcal{C}_{n,\varepsilon}}[x=k]$
$\widehat{\mathcal{C}}_{n,\varepsilon}(k)$	$n \in \mathbb{N},\ \varepsilon \in [-1,1],\ k \in \mathbb{Z}$	$\Pr_{x \leftarrow \mathcal{C}_{n,\varepsilon}}[x \geq k]$
$\widehat{\mathcal{C}}_n^{-1}(\delta)$	$n \in \mathbb{N},\ \delta \in [0,1]$	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 Basic Inequalities

The following proposition is proved in Appendix A.1.

Proposition 2.1. *Let $n \in \mathbb{N}$, $\alpha > 0$, $k \in [n]$ and let $\{p_j\}_{j=k}^n$ be a set of non-negative numbers such that $\sum_{j=i}^n p_j \leq \alpha \cdot (n+1-i)$ for every $i \in \{k, k+1, \ldots, n\}$. Then $\sum_{j=k}^n \frac{p_j}{(n+1-j)} \leq \alpha \cdot \sum_{j=k}^n \frac{1}{(n+1-j)}$.*

2.3 Facts About the Binomial Distribution

Fact 2.2 (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 [35]. $\qquad\square$

Fact 2.3. *Let $n \in \mathbb{N}$ and $\varepsilon \in [-\frac{1}{\sqrt{n}}, \frac{1}{\sqrt{n}}]$. Then $\mathrm{E}_{x \leftarrow \mathcal{C}_{n,\varepsilon}}[x^2] \leq 2n$ and $\mathrm{E}_{x \leftarrow \mathcal{C}_{n,\varepsilon}}[|x|] \leq \sqrt{2n}$.*

Proof. A simple calculation yields that $\mathrm{E}_{x \leftarrow \mathcal{C}_{n,\varepsilon}}[x^2] = n(1-\varepsilon^2) + \varepsilon^2 n^2$, which is smaller than $2n$ by the bound on ε. The second bound holds since $\mathrm{E}_{x \leftarrow \mathcal{C}_{n,\varepsilon}}[|x|] \leq \sqrt{\mathrm{E}_{x \leftarrow \mathcal{C}_{n,\varepsilon}}[x^2]}$. $\qquad\square$

The following propositions are proved in Appendix A.2.

Proposition 2.4. *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 error $= \xi \cdot (\varepsilon^2 |t| + \frac{1}{n} + \frac{|t|^3}{n^2} + \varepsilon^4 n)$ *and a universal constant* ξ.

Proposition 2.5. *Let* $n \in \mathbb{N}$, $t, x, x' \in \mathbb{Z}$, $\varepsilon \in [-1, 1]$ *and* $\lambda > 0$ *be such that* $t{-}x, t{-}x' \in \text{Supp}(\mathcal{C}_{n,\varepsilon})$, $|x|, |x'|, |t| \leq \lambda \cdot \sqrt{n \log n}$ *and* $|\varepsilon| \leq \lambda \cdot \sqrt{\frac{\log n}{n}}$, *then*

$$\frac{\mathcal{C}_{n,\varepsilon}(t - x')}{\mathcal{C}_{n,\varepsilon}(t - x)} \in (1 \pm \text{error}) \cdot \exp \left(\frac{-2 \cdot (t - \varepsilon n) \cdot x + x^2 + 2 \cdot (t - \varepsilon n) \cdot x' - x'^2}{2n} \right),$$

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

Proposition 2.6. *Let* $n \in \mathbb{N}$, $k, k' \in \mathbb{Z}$ *and* $\varepsilon \in [-1, 1]$, *where* n *is larger than a universal constant,* $|k|, |k'| \leq n^{\frac{3}{5}}$ *and* $|\varepsilon| \leq n^{-\frac{2}{5}}$. *Then*

$$\left| \widehat{\mathcal{C}}_{n,\varepsilon}(k) - \widehat{\mathcal{C}}_{n,\varepsilon}(k') \right| \leq \frac{|k - k'|}{\sqrt{n}}.$$

Proposition 2.7. *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*

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

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

Proposition 2.8. *Let* $n \in \mathbb{N}$, *integer* $i \in [n - \lfloor \log^{2.5} n \rfloor]$, $x, \beta, \beta', \alpha, \alpha' \in \mathbb{Z}$, $\varepsilon \in [-1, 1]$, $\mathcal{S} \subseteq \mathbb{Z}$ *and* $\lambda > 0$ *such that* $|\alpha|, |\alpha'| \leq \sqrt{\lambda \cdot \text{sum}_n(i) \cdot \log n}$, $|\beta|, |\beta'| \leq 1$, $\mathcal{S} \subseteq [-\sqrt{\lambda \cdot \ell_n(i) \cdot \log n}, \sqrt{\lambda \cdot \ell_n(i) \cdot \log n}]$, $x \in \mathcal{S}$, $|\varepsilon| \leq \sqrt{\lambda \cdot \frac{\log n}{\text{sum}_n(i)}}$ *and* $\text{E}_{x' \leftarrow \mathcal{C}_{\ell_n(i),\varepsilon} | x' \in \mathcal{S}} [|x'|] \leq \text{E}_{x' \leftarrow \mathcal{C}_{\ell_n(i),\varepsilon}} [|x'|]$. *Then*

$$\underset{x' \leftarrow \mathcal{C}_{\ell_n(i),\varepsilon} | x' \in \mathcal{S}}{\text{E}} \left[\exp \left(\frac{\alpha \cdot x + \beta \cdot x^2 + \alpha' \cdot x' + \beta' \cdot x'^2}{\text{sum}_n(i + 1)} \right) \right] \in 1 \pm \varphi(\lambda) \cdot \sqrt{\frac{\log n}{\ell_n(i)}} \left(1 + \frac{|x|}{\sqrt{\ell_n(i)}} \right).$$

for a universal function φ.

2.4   Facts About the Hypergeometric Distribution

Fact 2.9 (Hoeffding's inequality for hypergeometric distribution)**.** *Let* $\ell \leq n \in \mathbb{N}$, *and* $p \in \mathbb{Z}$ *with* $|p| \leq n$. *Then*

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

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

Proof. Immediately follows by [46, Equations (10),(14)]. $\square$

The following proposition is proved in Appendix A.3.

Proposition 2.10. *Let $n \in \mathbb{N}$, $p, t \in \mathbb{Z}$ be such that $|p|, |t| \leq n^{\frac{3}{5}}$ and $t \in \mathrm{Supp}(\mathcal{HG}_{2n,p,n})$. Then*

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

for $\mathsf{error} = \xi \cdot \left(\frac{n + |p|^3 + |t|^3}{n^2}\right)$ and a universal constant ξ.

Proposition 2.11. *Let $n \in \mathbb{N}$, $p, t, x, x' \in \mathbb{Z}$ and $\lambda > 0$ be such that $t - x, t - x' \in \mathrm{Supp}(\mathcal{HG}_{2n,p,n})$ and $|p|, |t|, |x|, |x'| \leq \lambda \cdot \sqrt{n \log n}$. Then*

$$\frac{\mathcal{HG}_{2n,p,n}(t - x')}{\mathcal{HG}_{2n,p,n}(t - x)} \in (1 \pm \mathsf{error}) \cdot \exp\left(\frac{-2(t - \frac{p}{2})x + x^2 + 2(t - \frac{p}{2})x' - x'^2}{n}\right),$$

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

2.5 Multi-Party Protocols

The following discussion is restricted to no private input protocols (such restricted protocols suffice for our needs).

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 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.

2.6 The Real vs. Ideal Paradigm

The security of multi-party computation protocols is defined using the *real* vs. *ideal* paradigm [16, 24]. 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.[11]

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 2.12.

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 $\mathsf{Continue}/\mathsf{Abort}$ 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 $\mathsf{Continue}$, and $\perp$ otherwise.*

. . . .

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

2.6.1 α-Secure Computation

The following definitions adopts the notion of α-secure computation [11, 27, 38] for our restricted settings.

Definition 2.13 (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 $\mathcal{C}$,[12] there exists a PPT $\mathbb{A}$ controlling the same parties, such that*

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

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 $\mathsf{simultaneous}$ α-secure manner, if the above is achieved by a non-aborting $\mathbb{A}$.

---

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

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

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.

2.7 Fair Coin-Flipping Protocols

Definition 2.14 (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.*

2.7.1 Proving Fairness

The following lemma 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 2.15 (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 2.16 (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 2.17 (α-unbiased coin-flipping protocols). *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 $\mathcal{C} \subset [t]$. Let V be the view of the corrupted parties controlled by A in a random execution of π, 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 2.16.

The following is an alternative characterization of fair coin-flipping protocols (against fail-stop adversaries).

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.*

Proof. Let A be a PPT fail-stop adversary controlling a subset $\mathcal{C} \subsetneq [t]$ of the parties. The ideal-world adversary $\mathbb{A}$ is defined as follows.

Algorithm 2.19 ($\mathbb{A}$).

Input: 1^κ.

Operation: Upon receiving $\{y_i = b\}_{i \in \mathcal{C}}$ from the trusted party, for some $b \in \{0, 1\}$, do:

1. *Keep sampling uniformly at random coins for the parties of π and for A, on security parameter κ, until the honest parties' common output in the resulting execution is b. Abort after $\kappa \cdot p(\kappa)$ failed attempts.*

2. *Output A's output in the above sampled execution.*

Let D_κ be the distribution of the honest parities common output, in a random execution of $\pi(1^\kappa)$, in which A controls the parties indexed by $\mathcal{C}$. Assume for a moment that the trusted party chooses its output on security parameter κ, according to D_κ (and not uniformly at random). Assume further that $\mathbb{A}$ keeps sampling in Step 1 until good coins are found. Under these assumptions, it is immediate that $\mathbb{A}$ is a *perfect* ideal variant simulator for A, i.e., $\text{REAL}_{\pi,\mathsf{A},\mathcal{C}}(\kappa) \equiv \text{IDEAL}_{f,\mathbb{A},\mathcal{C}}(\kappa)$ for every κ. We complete the proof showing that $\text{SD}(D_\kappa, U) \leq \alpha(\kappa)$, where U is the uniform distribution over $\{0, 1\}$. This yields that $\text{SD}(\text{REAL}_{\pi,\mathsf{A},\mathcal{C}}(\kappa), \text{IDEAL}_{f,\mathbb{A},\mathcal{C}}(\kappa)) \leq \alpha(\kappa)$ assuming no abort in Step 1. Since, by assumption, $\alpha(\kappa) \leq \frac{1}{2} - \frac{1}{p(\kappa)}$, such aborts happens only with negligible probability, it will follow that $\text{SD}(\text{REAL}_{\pi,\mathsf{A},\mathcal{C}}(\kappa), \text{IDEAL}_{f,\mathbb{A},\mathcal{C}}(\kappa)) \leq \alpha(\kappa) + \text{neg}(\kappa)$.

Let val, V, V_i, V_i^- and I_j be as in Definition 2.17 with respect to algorithm A, subset $\mathcal{C}$ and protocol π. We prove by induction on $\ell \in |\mathcal{C}|$ that $\mathrm{E}\left[\mathsf{val}(V_{I_\ell})\right] = \frac{1}{2} + \beta_\ell$, for $\beta_\ell = \sum_{j \in [\ell]} \mathrm{E}\left[\mathsf{val}(V_{I_j}) - \mathsf{val}(V_{I_j}^-)\right]$. Since no abort occurs after the $|\mathcal{C}|$'th aborting round, it follows that $\mathrm{E}\left[\mathsf{val}(V)\right] = \frac{1}{2} + \beta_{|\mathcal{C}|}$. Since π is α-unbiased, it follows that $\mathrm{E}\left[\mathsf{val}(V)\right] \in [\frac{1}{2} \pm \alpha(\kappa)]$, and therefore $\text{SD}(D_\kappa, U) \leq \alpha(\kappa)$.

The base case (i.e., $\ell = 0$) holds by the correctness of π. Assume for $0 \leq \ell < |\mathcal{C}|$. Since no additional aborts messages were sent in $V_{I_{\ell+1}}^-$ beside the ones sent V_{I_ℓ}, it holds that

$$\mathrm{E}\left[\mathsf{val}(V_{I_{\ell+1}}^-)\right] = \mathrm{E}\left[\mathsf{val}(V_{I_\ell})\right] \tag{2}$$

It follows that

$$\begin{aligned}
\mathrm{E}\left[\mathsf{val}(V_{I_{\ell+1}})\right] &= \mathrm{E}\left[\mathsf{val}(V_{I_{\ell+1}}^-)\right] + \mathrm{E}\left[\mathsf{val}(V_{I_{\ell+1}}) - \mathsf{val}(V_{I_{\ell+1}}^-)\right] \\
&= \mathrm{E}\left[\mathsf{val}(V_{I_\ell})\right] + \mathrm{E}\left[\mathsf{val}(V_{I_{\ell+1}}) - \mathsf{val}(V_{I_{\ell+1}}^-)\right] \\
&= \left(\frac{1}{2} + \sum_{j \in [\ell]} \mathrm{E}\left[\mathsf{val}(V_{I_j}) - \mathsf{val}(V_{I_j}^-)\right]\right) + \mathrm{E}\left[\mathsf{val}(V_{I_{\ell+1}}) - \mathsf{val}(V_{I_{\ell+1}}^-)\right] \\
&= \frac{1}{2} + \sum_{j \in [\ell+1]} \mathrm{E}\left[\mathsf{val}(V_{I_j}) - \mathsf{val}(V_{I_j}^-)\right].
\end{aligned}$$

The second equality holds by Equation (2) and the third one by the induction hypothesis. $\square$

2.8 Oblivious Transfer

Definition 2.20. *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, 21, 23, 30, 37, 43]).

2.9 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 2.6 and 2.7 naturally extend to the f-hybrid model, for any functionality f. In addition, the proof of Lemma 2.18 straightforwardly extends to this model.

We make use of the following known fact.

Fact 2.21. *Let f be a polynomial-time computable functionality, and assume there exists a $k \in O(1)$-party, m-round, α-fair coin-flipping protocol in the f-hybrid model, making at most t calls to f. Assuming there exist protocols for securely computing OT, then there exists a k-party, $(O(t)+m)$-round, $(\alpha + \text{neg})$-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. [9] (assuming OT), and the latter protocol can be compiled into a constant-round protocol that securely computes f, against arbitrary malicious adversaries, using the techniques of Goldreich et al. [25] (assuming one-way functions, that follows by the existence of OT). Let π be a k-party, m-round, α-fair coin-flipping protocol in the f-hybrid model. Canetti [16] yields that by replacing the trusted party for computing f used in π with the protocol π_f, we get an $(O(t) + m)$-round, $(\alpha + \text{neg})$-fair coin-flipping protocol. $\square$

3 The Protocols

The following protocols follows the high-level description given in Section 1.3.

3.1 Two-Party Protocol

We start with defining a coin-flipping protocol whose parties get (correlated) shares as input, then describe the functionality for generating these shares, and finally explain how to combine the two into a (no input) coin-flipping protocol.

3.1.1 The Basic Two-Party Protocol

Protocol 3.1 ($\Pi_m^2 = (\mathsf{P}_0^2, \mathsf{P}_1^2)$).

Common input: round parameter 1^m.

P_z^2*'s input:* $\mathbf{c}^{\#\mathbf{z}} \in \{0,1\}^{m \times \lceil \log m \rceil}$ *and* $\mathbf{d}^{0,\#\mathbf{z}}, \mathbf{d}^{1,\#\mathbf{z}} \in \{0,1\}^{m+1}$.

Protocol's description:

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

   (a) P_0^2 *sends* $\mathbf{d}^{1,\#\mathbf{0}}[i]$ *to* P_1^2, *and* P_1^2 *sends* $\mathbf{d}^{0,\#\mathbf{1}}[i]$ *to* P_0^2.
   - *For $z \in \{0,1\}$, party P_z^2 set $d_i^z = \mathbf{d}^{\mathbf{z},\#\mathbf{0}}[i] \oplus \mathbf{d}^{\mathbf{z},\#\mathbf{1}}[i]$.*
   (b) P_0^2 *sends* $\mathbf{c}^{\#\mathbf{0}}[i]$ *to* P_1^2, *and* P_1^2 *sends* $\mathbf{c}^{\#\mathbf{1}}[i]$ *to* P_0^2.
   - *Both parties set $c_i = \mathbf{c}^{\#\mathbf{0}}[i] \oplus \mathbf{c}^{\#\mathbf{1}}[i]$.*

2. *Both parties output 1 if $\sum_{i=1}^m c_i \geq 0$, and 0 otherwise.*

Abort: If the other party aborts, the remaining party P_z^2 outputs d_i^z, for the maximal $i \in [m]$ for which it has reconstructed this value. In case no such i exists, P_z^2 outputs $\mathbf{d}^{\mathbf{z},\#\mathbf{z}}[m+1]$.

To keep the above description symmetric, in Step 1a and in Step 1b, both parties are supposed to send messages. This is merely for notational convince, and one might assume that the parties send their messages in an arbitrary order.

3.1.2 Two-Party Shares Generator

We now define the share-generating function of our two-party coin-flipping protocol. For future use, we describe a parameterized variant of this function that gets, in addition to the round parameter, also the desired expected outcome of the protocol. Our two-party protocol will call this function with expected outcome $\frac{1}{2}$.

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 $\mathcal{C}_\varepsilon$ is the Bernoulli probability distribution over $\{-1,1\}$, taking the value 1 with probability $\frac{1}{2}(1 + \varepsilon)$ and -1 otherwise,[13] 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 that $\widehat{\mathcal{C}}_{n,\varepsilon}(k) = \Pr_{x \leftarrow \mathcal{C}_{n,\varepsilon}}[x \geq k]$. Also recall that $\widehat{\mathcal{C}}_n^{-1}(\delta)$ is the value $\varepsilon \in [-1,1]$ with $\widehat{\mathcal{C}}_{n,\varepsilon}(0) = \delta$, and that $\ell_n(i) = n + 1 - i$ and $\mathsf{sum}_n(i) = \sum_{j=i}^n \ell_n(j)$. Finally, for $z \in \{0,1\}$ let $\overline{z} = z + 1 \bmod 2$.

Algorithm 3.2 (TwoPartySharesGen).

Input: round parameter 1^m and $\delta \in [0,1]$.

Operation:

1. *For $z \in \{0,1\}$: sample $d_{m+1}^{z,\#z} \leftarrow \mathcal{B}er(\delta)$. Set $d_{m+1}^{z,\#\overline{z}}$ arbitrarily.*

2. *Let $\varepsilon = \widehat{\mathcal{C}}_{\mathsf{sum}_m(1)}^{-1}(\delta)$.[14]*

---

[13]Notice the slight change in notation compared to those used in the introduction.

[14]Note that $\widehat{\mathcal{C}}_{\mathsf{sum}_m(1)}^{-1}(\frac{1}{2}) = 0$ if $\mathsf{sum}_m(1)$ is odd.

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

    (a) *Sample $c_i \leftarrow \mathcal{C}_{\ell_m(i),\varepsilon}$.*

    (b) *Sample $c_i^{\#0} \leftarrow \{0,1\}^{\lceil \log m \rceil}$ and set $c_i^{\#1} = c_i \oplus c_i^{\#0}$.*

    (c) *For $z \in \{0,1\}$:*

        i. *Sample $d_i^z \leftarrow \mathcal{B}er(\widehat{\mathcal{C}}_{\mathsf{sum}_m(i+1),\varepsilon}(-\sum_{j=1}^{i} c_j))$.*

        ii. *Sample $d_i^{z,\#0} \leftarrow \{0,1\}$, and set $d_i^{z,\#1} = d_i^z \oplus d_i^{z,\#0}$.*

4. *Output $(\mathbf{s}^{\#0}, \mathbf{s}^{\#1})$, where $\mathbf{s}^{\#z} = (\mathbf{c}^{\#z}, \mathbf{d}^{0,\#z}, \mathbf{d}^{1,\#z})$, for $\mathbf{c}^{\#z} = (c_1^{\#z}, \ldots, c_m^{\#z})$ and $\mathbf{d}^{z,\#z'} = (d_1^{z,\#z'}, \ldots, d_{m+1}^{z,\#z'})$.*

3.1.3 The Final Two-Party Protocol

For $m \in \mathbb{N}$, our two-party, $(2m)$-round, $\frac{O(\log^3 m)}{m}$-fair coin-flipping protocol $\widehat{\Pi}_m^2$, is defined as follows.

Protocol 3.3 $(\widehat{\Pi}_m^2 = (\widehat{\mathsf{P}}_0^2, \widehat{\mathsf{P}}_1^2))$.

Oracle: an oracle $\tilde{o}$ computing $\mathsf{TwoPartySharesGen}_{\frac{1}{2}} = \mathsf{TwoPartySharesGen}(\cdot, \frac{1}{2})$.

Common input: round parameter 1^m.

Protocol's description:

1. *The two parties use the oracle $\tilde{o}$ to compute $\mathsf{TwoPartySharesGen}_{\frac{1}{2}}(1^m)$. Let $\mathbf{s_0}$ and $\mathbf{s_1}$ be the outputs of $\widehat{\mathsf{P}}_0^2$, and $\widehat{\mathsf{P}}_1^2$ respectively.*

2. *In case the other party aborts, the remaining party outputs a uniform coin.*

3. *Otherwise, the two parties interact in an execution of $\Pi_m^2 = (\mathsf{P}_0^2, \mathsf{P}_1^2)$, where $\widehat{\mathsf{P}}_z^2$ plays the role of P_z^2 with private input $\mathbf{s_z}$.*

3.1.4 Main Theorems for Two-Party Protocols

The following theorem states that Protocol 3.3 is an almost-optimally fair, two-party coin-flipping protocol, in the $\mathsf{TwoPartySharesGen}_{\frac{1}{2}}$-hybrid model.

Theorem 3.4. *For $m \equiv 1 \bmod 4$, the protocol $\widehat{\Pi}_m^2$ is a $(2m)$-round, two-party, $O(\frac{\log^3 m}{m})$-fair coin-flipping protocol against unbounded fail-stop adversaries, in the $\mathsf{TwoPartySharesGen}_{\frac{1}{2}}$-hybrid model.*

Theorem 3.4 is proven in Section 3.1.6 using the the bound on online-binomial games described in Section 3.1.5, but we first use it to deduce an almost-optimal two-party fair coin-flipping protocol, in the real (non-hybrid) model.

Theorem 3.5 (Main theorem — two-party, fair coin flipping). *Assuming protocols for securely computing OT exist, then for any polynomially bounded, polynomial-time computable, integer function m, there exists an m-round, $\frac{O(\log^3 m)}{m}$-fair, two-party coin-flipping protocol.*

Proof. Define the integer function $\widetilde{m}$ by $\widetilde{m}(\kappa) = \lfloor m(\kappa)/3 \rfloor - a$, where $a \in \{0, 1, 2, 3\}$ is the value such that $\lfloor m(\kappa)/3 \rfloor - a \equiv 1 \bmod 4$. Note that both the functionality $\mathsf{TwoPartySharesGen}_{\frac{1}{2}}(1^{\widetilde{m}(\kappa)})$ and the protocol $\widehat{\Pi}^2_{\widetilde{m}(\kappa)}$ are polynomial-time computable in κ, and that $\widehat{\Pi}^2_{\widetilde{m}(\kappa)}$ has $2 \cdot \widetilde{m}(\kappa)$ rounds. Using information-theoretic one-time message authentication codes (cf., [41]), the functionality $\mathsf{TwoPartySharesGen}_{\frac{1}{2}}(1^{\widetilde{m}(\kappa)})$ and protocol $\widehat{\Pi}^2_{\widetilde{m}(\kappa)}$ can be compiled into functionality $\widetilde{\mathsf{TwoPartySharesGen}}_{\frac{1}{2}}(1^{\widetilde{m}(\kappa)})$ and protocol $\widetilde{\Pi}^2_{\widetilde{m}(\kappa)}$ that maintains essentially the same efficiency as the original pair, protocol $\widetilde{\Pi}^2_{\widetilde{m}(\kappa)}$ maintain the same round complexity, and $\widetilde{\Pi}^2_{\widetilde{m}(\kappa)}$ is $\left(\frac{O(\log^3 \widetilde{m}(\kappa))}{\widetilde{m}(\kappa)} + \mathrm{neg}(\kappa) \right)$-fair against *arbitrary* unbounded adversaries, in the $\mathsf{TwoPartySharesGen}_{\frac{1}{2}}$-hybrid model.

Assuming protocols for securely computing OT exist, Fact 2.21 yields that there exists an $(2\widetilde{m}(\kappa) + O(1))$-round, two-party, polynomial-time protocol that is $\left(\frac{O(\log^3 \widetilde{m}(\kappa))}{\widetilde{m}(\kappa)} + \mathrm{neg}(\kappa) \right)$-fair, in the *standard model*. For large enough κ, the latter protocol obtains the parameters stated in the theorem (the theorem trivially holds for small values of κ, i.e., smaller than some universal constant) $\qquad\square$

3.1.5 Online Binomial Games

Our main tool for proving Theorem 3.4 are bounds on the bias of online-binomial games, defined below, that we prove in Section 4.

In a *online binomial game*, independent random variables $X_1 \ldots, X_m$ are independently sampled, and the game outcome (or value) is set to one if $\sum_{i=1}^m X_i \geq 0$, and to zero otherwise. At round i, the value of X_{i-1} is given to the *attacker*, with some auxiliary information (i.e., hint) H_i about the value of X_i. The attacker can abort, and in this case it gains the expected outcome of the game, conditioned on the values of $X_1, \ldots, X_{i-1}$ (but not on the additional information). If it never aborts, it gains the game outcome. The goal of the attacker is to use the hint value to *bias* its expected gain away from the game expected outcome. For instance, in the simple form of the game where the X_i's are unbiased $\{-1, 1\}$ bits and $H_i = X_i$, the game expected outcome is $1/2$, and it is not hard to see that the expected gain of the attacker who aborts on the first round in which $H_i = X_i = 1$, is $1/2 + \Theta(1/\sqrt{m})$. Namely, such an attacker bias the game by $\Theta(1/\sqrt{m})$.

We are concerned with the weighted version of the above games in which the X_i's are *sums* of biased $\{-1, 1\}$ random variables. Specially, X_i is the sum of $\ell_m(i) = m - i + 1$ coins. We will also allow the games to have an initial offset: a fixed value (i.e., *offset*) X_0 is added to the coins sum. Such online binomial games are useful abstractions to understand the power of fail-stop adversaries trying to violate the fairness of the coin-flipping protocols considered in this section, and the results presented below play a central role in their security proofs.

We start with formally defining online-binomial games and the bias of such games.

Definition 3.6 (online binomial games). *For $m \in \mathbb{N}$, $t \in \mathbb{Z}$, $\varepsilon \in [-1, 1]$ and a randomized (hint) function f, the* online game $\mathsf{G}_{f, m, \varepsilon, t}$ *is the set of the following random variables. Let $Y_0 = X_0 = t$, and for $i \in [m]$,*

- X_i *is sampled according to* $\mathcal{C}_{\ell_m(i), \varepsilon}$.

- $Y_i = \sum_{j=0}^i X_j$ *and* $H_i = f(i, Y_i)$.

21

- $O_i = \mathsf{o}_i(Y_{i-1}, H_i)$ and $O_i^- = \mathsf{o}_i(Y_{i-1})$, for $\mathsf{o}_i(y) = \Pr[Y_m \geq 0 \mid Y_{i-1} = y]$ and $\mathsf{o}_i(y,h) = \Pr[Y_m \geq 0 \mid Y_{i-1} = y, H_i = h]$, respectively.

Let $O_{m+1} = O_{m+1}^- = 1$ if $Y_m \geq 0$, and $O_{m+1} = O_{m+1}^- = 0$ otherwise.
We let $\mathsf{G}_{f,m,\varepsilon} = \mathsf{G}_{f,m,\varepsilon,0}$.

Namely, O_i is the expected output of the game given Y_{i-1}, the coins flipped in the first $i-1$ rounds, and the hint H_i about Y_i, and O_i^- is this value given only Y_{i-1}. Consider an attacker who is getting at round i the values of Y_{i-1} and H_i, and decides whether to abort and gain O_i^-, or to continue to next round. If it never aborts, it gains O_{m+1}. The goal of an attacker is to abort in the round that *maximize* the gap between O_i and O_i^-. This is an equivalent task to maximizing the difference between the adversary's expected gain and the game's expected outcome (which is the expected gain of a never-aborting attacker).

Definition 3.7 (game bias). *Let m, t, ε, f and $\mathsf{G} = \mathsf{G}_{f,m,\varepsilon,t} = \{X_i, Y_i, H_i, O_i, O_i^-\}$ be as in Definition 3.6. 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 (i, Y_{i-1}, H_i) and outputs a 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 $\mathsf{Bias}(\mathsf{G}) = \max_\mathsf{B}\{\mathsf{Bias}_\mathsf{B}(\mathsf{G})\}$, where the maximum is over all possible algorithms B.

We give upper bounds for the security of three different types of online-binomial games that we call *simple*, *hypergeometric* and *vector* games. The first type of online-binomial game (i.e., simple game) is used for proving Theorem 3.4 whereas the other types (*hypergeometric* and *vector* games) are used later in Section 3.2 for proving the fairness of our three-party protocol.

Definition 3.8 (simple game). *For $m \in \mathbb{N}$, $\varepsilon \in [-1, 1]$ and a randomized function f, the game $\mathsf{G}_{f,m,\varepsilon}$ is called "simple game" if f on input (i, y) outputs 1 with probability $\mathsf{o}_{i+1}(y)$ $(= \widehat{\mathcal{C}}_{\mathsf{sum}_m(i+1),\varepsilon}(-y))$, and zero otherwise.*

Namely, in the simple game, the value of f is sampled according to the expected value of the game.

Lemma 3.9. *Let $m \in \mathbb{N}$, let $\varepsilon \in [-1, 1]$ and let f be the randomized function such that $\mathsf{G}_{f,m,\varepsilon}$ is a simple game according to Definition 3.8. Then $\mathsf{Bias}(\mathsf{G}_{f,m,\varepsilon}) \leq \frac{\xi \cdot \log^3 m}{m}$, for some universal constant ξ.*

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 $w(v) = p$ (recall that $w(v) = \sum_{j \in [|v|]} v[j]$ and that $v_\mathcal{I} = (v_{j_1}, \ldots, v_{j_{|\mathcal{I}|}})$ where $j_1, \ldots, j_{|\mathcal{I}|}$ are the ordered elements of $\mathcal{I}$) and recall that $\widehat{\mathcal{HG}}_{n,p,\ell}(k) := \Pr_{x \leftarrow \mathcal{HG}_{n,p,\ell}}[x \geq k] = \sum_{t=k}^{\ell} \mathcal{HG}_{n,p,\ell}(t)$.

Definition 3.10 (hypergeometric game). *For $m \in \mathbb{N}$, $\varepsilon \in [-1, 1]$, $\lambda > 0$ and a randomized function f, the game $\mathsf{G}_{f,m,\varepsilon}$ is called "λ-hypergeometric game" if there exists $p \in [-m, m]$, with $|p| \leq \lambda \cdot \sqrt{\log m \cdot \mathsf{sum}_m(1)}$, such that f on input (i, y) outputs 1 with probability $\widehat{\mathcal{HG}}_{2\cdot\mathsf{sum}_m(1),p,\mathsf{sum}_m(i+1)}(-y)$ and zero otherwise.*

Namely, in the above game, the value of f is not sampled according to the expected value of the game, as done in the simple game above, but rather from a skewed version of it, obtained by replacing the Binomial distribution used by the game, with an Hypergeometric distribution.

Lemma 3.11. *Let $m \in \mathbb{N}$, let $\varepsilon \in [-1, 1]$, let $\lambda > 0$ and let f be a randomized function such that $\mathsf{G}_{f,m,\varepsilon}$ is an λ-hypergeometric game according to Definition 3.10. Then $\mathsf{Bias}(\mathsf{G}_{f,m,\varepsilon}) \leq \frac{\varphi(\lambda) \cdot \log^3 m}{m}$ for some universal function φ.*

Recall that for $n \in \mathbb{N}$ and $\delta \in [0, 1]$ we let $\widehat{\mathcal{C}}_n^{-1}(\delta)$ be the value $\varepsilon \in [-1, 1]$ with $\widehat{\mathcal{C}}_{n,\varepsilon}(0) = \delta$.

Definition 3.12 (vector game). *For $m \in \mathbb{N}$, $\varepsilon \in [-1, 1]$, $\lambda \in \mathbb{N}$ and a randomized function f, the game $\mathsf{G}_{f,m,\varepsilon}$ is called "λ-vector game" if f on input (i, y) outputs a string in $\{-1, 1\}^{\lambda \cdot \mathsf{sum}_m(1)}$, where each of entries takes the value 1 with probability $\widehat{\mathcal{C}}_{\mathsf{sum}_m(1)}^{-1}(\delta)$ for $\delta = \mathsf{o}_{i+1}(y) (= \widehat{\mathcal{C}}_{\mathsf{sum}_m(i+1),\varepsilon}(-y))$.*

In the last game, the function f outputs a vector (i.e., a string), and not a bit as in the previous games. The distribution from which the vector is drawn, however, is very related to the expected value of the game.

Lemma 3.13. *Let $m \in \mathbb{N}$, let $\lambda > 0$ and let f be a randomized function such that $\mathsf{G}_{f,m,\varepsilon=0}$ is an λ-vector game according to Definition 3.12. Then $\mathsf{Bias}(\mathsf{G}_{f,m,\varepsilon=0}) \leq \frac{\varphi(\lambda) \cdot \log^3 m}{m}$ for some universal function φ.*

The proof of the above lemmas are given in Sections 4.3 to 4.5. In addition, we make use of the following lemma which asserts that if the expected value of an online-binomial game is almost determined, then there is no much room for an attacker to gain much bias.

Lemma 3.14. *Let $\mathsf{G}_{f,m,\varepsilon,t} = \{X_i, Y_i, H_i, O_i, O_i^-\}$ be according to Definition 3.6. Assume that $O_1^- \notin [\frac{1}{m^2}, 1 - \frac{1}{m^2}]$, then $\mathsf{Bias}(\mathsf{G}_{f,m,\varepsilon,t}) \leq \frac{2}{m}$.*

The proof of Lemma 3.14 is given in Section 4.1.

3.1.6 Proving Theorem 3.4

Proof of Theorem 3.4. Fix $m \equiv 1 \mod 4$. By construction, the honest parties in $\widehat{\Pi}_m^2$ always output the same bit, where under the assumption about m, it holds that $\mathsf{sum}_m(1)$, the total number of coins flipped, is odd. It follows that the common output of a random honest execution of $\widehat{\Pi}_m^2$, is a uniform bit. Namely, protocol $\widehat{\Pi}_m^2$ is correct according to Definition 2.15.

We assume without loss of generality that if a party aborts in the i'th round, it does so by sending the message Abort, after seeing the other party message of that round.

Let the (i, j)'th round in a random execution of $\widehat{\Pi}_m^2$, for $(i, j) \in (m) \times \{a, b\}$, stands for the j'th step of the i'th loop in the execution. Letting $(0, a)$ being the zero round (i.e., before the call to $\mathsf{TwoPartySharesGen}_{\frac{1}{2}}$ is made) and $(0, b)$ denote the round where the call to $\mathsf{TwoPartySharesGen}_{\frac{1}{2}}$ is made.

Let $z \in \{0, 1\}$ and let A be a fail-stop adversary controlling $\widehat{\mathsf{P}}_z^2$. Let V be $\widehat{\mathsf{P}}_z^2$'s view in a random execution of $\widehat{\Pi}_m^2$. For $\mathbf{r} = (i, j) \in (m) \times \{a, b\}$, let $V_\mathbf{r}$ be $\mathbf{r}$'th round prefix of V, and let $V_\mathbf{r}^-$ be the value of $V_\mathbf{r}$ with the abort message sent in the $\mathbf{r}$'th round (if any) removed. Finally, let I be the round in which A sent the abort message, letting $I = (m, b)$, in case no abort occurred.

23

In the following we show that

$$\left| \mathrm{E} \left[\mathsf{val}(V_I) - \mathsf{val}(V_I^-) \right] \right| \leq \frac{\xi \cdot \log^3 m}{m}, \tag{3}$$

for some universal (independent of m) constant $\xi \geq 0$, where $\mathsf{val}(v)$ is the expected outcome of an honest (non aborting) execution of the parties that do no abort in v, conditioned on v (see Definition 2.16).

Since Equation (3) holds for any $m \equiv 1 \bmod 4$ and any fail-stop adversary A, protocol $\widehat{\Pi}_m^2$ is $\frac{\xi \log^3 m}{m}$-biased according to Definition 2.17. Since, see above, $\widehat{\Pi}_m^2$ is correct according to Definition 2.15, the proof of the theorem follows by Lemma 2.18.

So it is left to prove Equation (3). Notice that the next rounds shares held by $\widehat{\mathsf{P}}_z^2$ (when playing the role of P_z^2) at the end of round (i, b) (i.e., $\mathbf{c}^{\#\mathbf{z}}{}_{i+1,\dots,m}$, $\mathbf{d}^{0,\#\mathbf{z}}{}_{i+1,\dots,m+1}$ and $\mathbf{d}^{1,\#\mathbf{z}}{}_{i+1,\dots,m+1}$), are uniformly chosen strings from $\widehat{\mathsf{P}}_z^2$'s point of view. In particular, these shares contains no information about the expected output of the protocol, or the other party's action in case of future aborts. It follows that $\mathsf{val}(V_{0,b}) = \frac{1}{2}$ (recall that $V_{0,b}$ is $\widehat{\mathsf{P}}_z^2$'s view after getting its part of $\mathsf{TwoPartySharesGen}_{\frac{1}{2}}$'s output). We also note that by construction, in case $\widehat{\mathsf{P}}_z^2$ aborts during the call to $\mathsf{TwoPartySharesGen}_{\frac{1}{2}}$ (and in this case the honest party gets no value from the functionality), then the honest party outputs a uniform bit. Namely, $\mathsf{val}(V_{(0,b)}^-) = \frac{1}{2}$. Hence, the adversary A gains *nothing* by aborting during the call to $\mathsf{TwoPartySharesGen}_{\frac{1}{2}}$, and in the following we assume without loss of generality that A only aborts (if any) during the execution of the embedded execution of $\Pi_m^2 = (\mathsf{P}_0^2, \mathsf{P}_1^2)$.

In the rest of the proof we separately consider the case $I = (\cdot, a)$ and the case $I = (\cdot, b)$. We conclude the proof showing that the first type of aborts might help A to gain $\frac{O(\log^3 m)}{m}$ advantage, where the second type give him *nothing*.

Since both steps are symmetric, we assume for concreteness that A controls P_0^2.

$I = (\cdot, b)$. In case $I = (i, b)$, the adversary's view V_I contains the value of $(c_1, \dots, c_i)$ sampled by $\mathsf{TwoPartySharesGen}_{\frac{1}{2}}$, and some random function of these values, i.e., the shares of the next rounds it got from $\mathsf{TwoPartySharesGen}_{\frac{1}{2}}$, which are uniform strings from his point of view, and the shares used till this round, which are random function of $(c_1, \dots, c_i)$. Hence, the expected outcome of the protocol given A's view is $\delta_i := \widehat{\mathcal{C}}_{\mathsf{sum}_m(i),0}\left(-\sum_{j=1}^i c_j \right)$. By construction, however, the expected outcome of P_1^2 in case P_0^2 aborts in round (i, b), is also δ_i. Hence, the adversary gains nothing (i.e., $\mathsf{val}(V_i) = \mathsf{val}(V_i^-)$), by aborting in these steps.

$I = (\cdot, a)$. Since A gains nothing by aborting at Step 1b of the loop, we assume without loss of generality that A only aborts at Step 1a of the loop, and the proof by the next claim (proven below).

Claim 3.15. *Assuming A only aborts at Step 1a of the loop in Π_m^2, then*

$$\left| \mathrm{E} \left[\mathsf{val}(V_I) - \mathsf{val}(V_I)^- \right] \right| \leq \frac{\xi \cdot \log^3 m}{m},$$

for some universal (independent of m) constant $\xi \geq 0$.

Claim 3.15 yields that the overall bias A gains, which equals to $\left| \mathrm{E} \left[\mathsf{val}(V_I) - \mathsf{val}(V_I)^- \right] \right|$, is bounded by $\frac{\xi \cdot \log^3 m}{m}$, for some universal constant $\xi \geq 0$.

$\square$

Proving Claim 3.15 We prove the claim via reduction to online-binomial game, described in Section 3.1.5. The proof immediately follows from the following claim and Lemma 3.9.

Claim 3.16. *Assuming* A *only aborts at Step 1a of the loop in* Π_m^2, *then*

$$\left| \mathrm{E}\left[\mathsf{val}(V_I) - \mathsf{val}(V_I)^- \right] \right| \le \mathsf{Bias}(\mathsf{G}_{f,m,0}),$$

where $\mathsf{G}_{f,m,0}$ *is a simple online-binomial game according to Definition 3.8 and* $\mathsf{Bias}(\cdot)$ *is according to Definition 3.7.*

Proof of Claim 3.16. We prove that an attacker for the coin-flipping protocol of the type considered in this claim, i.e., one that only aborts in Step 1a of the loop in Π_m^2 and achieves bias α, yields a player for the simple binomial game (described in Section 3.1.5) that achieves the same bias. Thus, the bound on the former attacker follows from the bound on the latter one.

Let $\mathsf{G} = \mathsf{G}_{f,m,0} = \{X_i, Y_i, H_i, O_i, O_i^-\}$ be the simple binomial game as defined in Definition 3.8 and recall that in this game, f is the randomized function that on input (i, y) outputs 1 with probability $\widehat{\mathcal{C}}_{\mathsf{sum}_m(i+1),\varepsilon}(-y)$, and zero otherwise. Now, consider the player B for G that emulates interaction with A in $\Pi_m^2 = (\mathsf{P}_0^2, \mathsf{P}_1^2)$, where A controls P_0^2. The emulation goes as follows:

Algorithm 3.17 (Player B for the simple game)**.**

Operation:

1. *Choose uniformly* $\mathbf{c}^{\#0} \leftarrow \{0,1\}^{m \times \lceil \log m \rceil}$ *and* $\mathbf{d}^{0,\#0}, \mathbf{d}^{1,\#0} \leftarrow \{0,1\}^{m+1}$ *and set* $\mathbf{s_0} = \{\mathbf{c}^{\#0}, \mathbf{d}^{0,\#0}, \mathbf{d}^{1,\#0}\}$ *as input for* P_0^2 *in* Π_m^2.

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

    (a) *Receive input* (i, Y_{i-1}, H_i) *from the game* G.

    (b) *If* $i > 1$, *emulate a sending of* $\mathbf{c}^{\#1}[i-1]$ *from* P_1^2 *to* P_0^2 *at step* $(i-1, b)$ *of* Π_m^2, *where* $\mathbf{c}^{\#1}[i-1] := X_{i-1} \oplus \mathbf{c}^{\#0}[i-1]$ *(recall that* $X_{i-1} := Y_{i-1} - Y_{i-2}$ *according to Definition 3.6).*

    (c) *Emulate a sending of* $\mathbf{d}^{0,\#1}[i]$ *from* P_1^2 *to* P_0^2 *at step* (i, a) *of* Π_m^2, *where* $\mathbf{d}^{0,\#1}[i] := H_i \oplus \mathbf{d}^{0,\#0}[i]$. *If* A *aborts at this step, output 1 (abort at round i). Otherwise, output 0 (continue to next round).*

Note that by the definition of f, the set of G's variables $(X_1, \ldots, X_m, H_1, \ldots, H_m)$ has the same distribution as the set of Π_m^2's variables $(c_1, \ldots, c_m, d_1^0, \ldots, d_m^0)$ where the parties' inputs are sampled according to $\mathsf{TwoPartySharesGen}_{\frac{1}{2}}$. Therefore, A's view in the emulation done by B, is distributed exactly the same as its view when interacting with honest P_1^2 in Π_m^2; in both cases, the only meaningful information it gets is the revelation of these values. Since B aborts at round i of G (i.e outputs 1) iff A aborts at round (i, a) of Π_m^2, it follows that

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

as required. □

3.2 Three-Party Protocol

As done in Section 3.1, we start with defining a three-party coin-flipping protocol whose parties get (correlated) shares as input, then describe the functionality for generating these shares, and finally explain how to combine the two into a (no input) coin-flipping protocol.

3.2.1 The Basic Three-Party Protocol

Protocol 3.18 $(\Pi_m^3 = (\mathsf{P}_0^3, \mathsf{P}_1^3, \mathsf{P}_2^3))$.

Common input: round parameter 1^m.

P_z^3*'s input:* $\mathbf{c}^{\#\mathbf{z}} \in \{0,1\}^{m \times \lceil \log m \rceil}$ *and* $\mathbf{D}^{(\mathbf{z}',\mathbf{z}''),\#\mathbf{z}} \in \{0,1\}^{m \times (m \cdot \lceil \log m \rceil + 2(m+1))}$*, for all* $z' \neq z'' \in \{0,1,2\}$.

Protocol's description:

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

    (a) *For all $z_s, z_r, z_o \in \{0,1,2\}$ with $z_r \notin \{z_s, z_o\}$, party $\mathsf{P}_{z_s}^3$ sends $\mathbf{D}^{(\mathbf{z_r},\mathbf{z_o}),\#\mathbf{z_s}}[i]$ to $\mathsf{P}_{z_r}^3$.*

    - *For all $z \neq z' \in \{0,1,2\}$, party P_z^3 sets $\mathbf{d_i^{(\mathbf{z},\mathbf{z}')}} = \bigoplus_{z'' \in \{0,1,2\}} \mathbf{D}^{(\mathbf{z},\mathbf{z}'),\#\mathbf{z}''}[i]$.*

    (b) *For all $z \in \{0,1,2\}$, party P_z^3 sends $\mathbf{c}^{\#\mathbf{z}}[i]$ to the other parties.*

    - *All parties set $c_i = \mathbf{c}^{\#\mathbf{0}}[i] \oplus \mathbf{c}^{\#\mathbf{1}}[i] \oplus \mathbf{c}^{\#\mathbf{2}}[i]$.*

Output: All parties output 1 if $\sum_{i=1}^m c_i \geq 0$, and 0 otherwise.

Abort:

One party aborts: Let $z < z' \in \{0,1,2\}$ be the indices of the remaining parties, and let $i \in [m]$ be the maximal $i \in [m]$ for which both P_z^3 and $\mathsf{P}_{z'}^3$ have reconstructed $\mathbf{d_i^{(\mathbf{z},\mathbf{z}')}}$ and $\mathbf{d_i^{(\mathbf{z}',\mathbf{z})}}$, respectively. Set i to $\perp$ in case no such index exists. To decide on a common output, P_z^3 and $\mathsf{P}_{z'}^3$ interact in the following two-party protocol.

$i = \perp$: P_z^3 and $\mathsf{P}_{z'}^3$ interact in $\widehat{\Pi}_m^2$.

$i \neq \perp$: P_z^3 and $\mathsf{P}_{z'}^3$ interact in $\Pi_m^2 = (\mathsf{P}_0^2, \mathsf{P}_1^2)$, where P_z^3 with input $\mathbf{d_i^{(\mathbf{z},\mathbf{z}')}}$ plays the role of P_0^2, and $\mathsf{P}_{z'}^3$ with input $\mathbf{d_i^{(\mathbf{z}',\mathbf{z})}}$ plays the role of P_1^2.

Two parties abort (in the same round): Let P_z^3 be the remaining party and for an arbitrary $z' \neq z \in \{0,1,2\}$, let $i \in [m]$ be the maximal index for which P_z^3 have reconstructed $\mathbf{d_i^{(\mathbf{z}',\mathbf{z})}}$, set to $\perp$ in case no such index exists.

$i = \perp$: P_z^3 outputs a uniform bit.

$i \neq \perp$: The remaining party P_z^3 acts as if $\mathsf{P}_{z'}^3$ has only aborted at the very beginning of the following two-party protocol: P_z^3 "interact" with $\mathsf{P}_{z'}^3$, in $(\mathsf{P}_0^2, \mathsf{P}_1^2)$, where P_z^3 with input $\mathbf{d_i^{(\mathbf{z}',\mathbf{z})}}$ plays the role of P_0^2 in case $z < z'$ and as P_1^2 otherwise.[15]

---

[15] The latter protocol is well defined, since when aborting right at the beginning, $\mathsf{P}_{z'}^3$ does not send any message.

Namely, at Step (a) the parties help each other to reconstruct inputs for the two-party protocol Π_m^2. More specifically, each pair of parties reconstructs two inputs (shares) for an execution of Π_m^2, one input for each party in the pair. In case a party aborts, the remaining parties use the above inputs for interacting in Π_m^2. In Step (b) the parties help each other to reconstruct the round coins (i.e., c_i).

Note that the above protocol has $4m$ rounds (in case one party abort at the end of the outer three-party protocols). While it is possible to reduce this number to $2m$ (to match the two-party case), we chose to present the somewhat simpler protocol given above.

3.2.2 Hiding Two-Party Shares Generator

As mentioned in Section 1.3, we construct a *hiding* variant HidTwoPartySharesGen of the two-party share-generating function TwoPartySharesGen. The construction is done by modifying the way the defense values (given to the parties in the three-party protocol) are sampled. On input $\delta \in [0,1]$, HidTwoPartySharesGen first draws $\Theta(m^2)$ independent samples from $\mathcal{C}_\varepsilon$ for $\varepsilon = \widehat{\mathcal{C}}^{-1}_{\mathsf{sum}_m(1)}(\delta)$, and then uses these samples via a simple derandomization technique for drawing the $\Theta(m)$ defense values given in the three-party protocol.

Roughly, these $\Theta(m^2)$ values sampled by HidTwoPartySharesGen give about the same information as a *constant* number of independent samples from $\mathcal{B}er(\delta)$ would, unlike the non-hiding TwoPartySharesGen which gives about the same information as $\Theta(m)$ independent samples from $\mathcal{B}er(\delta)$. As mentioned in Section 1.3, these $\Theta(m)$ samples can be used to bias the outcome by $\Omega(\frac{1}{\sqrt{m}})$, which makes HidTwoPartySharesGen crucial for the fairness of our protocol.

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 $\mathcal{I}$.

Algorithm 3.19 (HidTwoPartySharesGen)**.**

Input: Round parameter 1^m and $\delta \in [0,1]$.

Operation:

1. *Let $\varepsilon = \widehat{\mathcal{C}}^{-1}_{\mathsf{sum}_m(1)}(\delta)$.*

2. *For $z \in \{0,1\}$: sample a random vector $v^z \in \{-1,1\}^{2 \cdot \mathsf{sum}_m(1)}$, where each coordinate is independently drawn from $\mathcal{C}_\varepsilon$.*

3. *For $z \in \{0,1\}$: sample a random $(\mathsf{sum}_m(1))$-size subset $\mathcal{I}^z \subset [2 \cdot \mathsf{sum}_m(1)]$, and set $d_{m+1}^{z, \#z}$ to one if $w(v_{\mathcal{I}^z}^z) \geq 0$, and to zero otherwise. Set $d_{m+1}^{z, \#\overline{z}}$ arbitrarily.*

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

    (a) *Sample $c_i \leftarrow \mathcal{C}_{\ell_m(i), \varepsilon}$.*

    (b) *Sample $c_i^{\#0} \leftarrow \{0,1\}^{\lceil \log m \rceil}$, and set $c_i^{\#1} = c_i \oplus c_i^{\#0}$.*

    (c) *For $z \in \{0,1\}$:*

    i. *Sample a random $(\mathsf{sum}_m(i+1))$-size subset $\mathcal{I}^z \subset [2 \cdot \mathsf{sum}_m(1)]$, and set d_i^z to one if $\sum_{j=1}^i c_j + w(v_{\mathcal{I}^z}^z) \geq 0$, and to zero otherwise.*

    ii. *Sample $d_i^{z, \#0} \leftarrow \{0,1\}$, and set $d_i^{z, \#1} = d_i^z \oplus d_i^{z, \#0}$.*

5. Output $(\mathbf{s}^{\#\mathbf{0}}, \mathbf{s}^{\#\mathbf{1}})$, where $\mathbf{s}^{\#\mathbf{z}} = (\mathbf{c}^{\#\mathbf{z}}, \mathbf{d}^{\mathbf{0},\#\mathbf{z}}, \mathbf{d}^{\mathbf{1},\#\mathbf{z}})$, for $\mathbf{c}^{\#\mathbf{z}} = (c_1^{\#z}, \ldots, c_m^{\#z})$ and $\mathbf{d}^{\mathbf{z},\#\mathbf{z}'} = (d_1^{z,\#z'}, \ldots, d_{m+1}^{z,\#z'})$.

Namely, rather then sampling the defense values in Step 4(c)i *independently* (as done in its non-hiding variant TwoPartySharesGen), the defense values used by HidTwoPartySharesGen in the different rounds, are correlated via the vectors v^0 and v^1 (v^z is used for the defense values of the party P_z^2). Note, however, that each round defense value on *its own*, has exactly the same distribution as in TwoPartySharesGen.

3.2.3 Three-Party Shares Generator

Using the above two-party shares generator, our three-party shares generator is defined as follows.

Algorithm 3.20 (ThreePartySharesGen)**.**

Input: round parameter 1^m.

Operation:

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

   (a) *Sample* $c_i \leftarrow \mathcal{C}_{\ell_m(i),0}$.

   (b) *Sample* $(c_i^{\#0}, c_i^{\#1}) \leftarrow (\{0,1\}^{\lceil \log m \rceil})^2$, *and set* $c_i^{\#2} = c_i \oplus c_i^{\#0} \oplus c_i^{\#1}$.

   (c) *Let* $\delta_i = \widehat{\mathcal{C}}_{\mathsf{sum}_m(i+1),0}(-\sum_{j=1}^i c_j)$.

   (d) *For* $z < z' \in \{0,1,2\}$:

   i. *Sample* $(\mathbf{s}_i^{(\mathbf{z},\mathbf{z}')}, \mathbf{s}_i^{(\mathbf{z}',\mathbf{z})}) \leftarrow \mathsf{HidTwoPartySharesGen}(1^m, \delta_i)$.

   ii. *Sample* $(\mathbf{s}_i^{(\mathbf{z},\mathbf{z}'),\#\mathbf{0}}, \mathbf{s}_i^{(\mathbf{z},\mathbf{z}'),\#\mathbf{1}}, \mathbf{s}_i^{(\mathbf{z}',\mathbf{z}),\#\mathbf{0}}, \mathbf{s}_i^{(\mathbf{z}',\mathbf{z}),\#\mathbf{1}}) \leftarrow (\{0,1\}^{m\cdot\lceil \log m \rceil + 2(m+1)})^4$.
   Set $\mathbf{s}_i^{(\mathbf{z},\mathbf{z}'),\#\mathbf{2}} = \mathbf{s}_i^{(\mathbf{z},\mathbf{z}')} \oplus \mathbf{s}_i^{(\mathbf{z},\mathbf{z}'),\#\mathbf{0}} \oplus \mathbf{s}_i^{(\mathbf{z},\mathbf{z}'),\#\mathbf{1}}$ *and* $\mathbf{s}_i^{(\mathbf{z}',\mathbf{z}),\#\mathbf{2}} = \mathbf{s}_i^{(\mathbf{z}',\mathbf{z})} \oplus \mathbf{s}_i^{(\mathbf{z}',\mathbf{z}),\#\mathbf{0}} \oplus \mathbf{s}_i^{(\mathbf{z}',\mathbf{z}),\#\mathbf{1}}$.

2. *Output* $(\mathbf{S}^{\mathbf{0}}, \mathbf{S}^{\mathbf{1}}, \mathbf{S}^{\mathbf{2}})$, *where* $\mathbf{S}^{\mathbf{z}} = (\mathbf{c}^{\#\mathbf{z}}, \mathbf{D}^{(0,1),\#\mathbf{z}}, \mathbf{D}^{(0,2),\#\mathbf{z}}, \mathbf{D}^{(1,0),\#\mathbf{z}}, \mathbf{D}^{(1,2),\#\mathbf{z}}, \mathbf{D}^{(2,0),\#\mathbf{z}}, \mathbf{D}^{(2,1),\#\mathbf{z}})$, *for* $\mathbf{c}^{\#\mathbf{z}} = (c_1^{\#z}, \ldots, c_m^{\#z})$ *and* $\mathbf{D}^{(\mathbf{z}',\mathbf{z}''),\#\mathbf{z}} = (\mathbf{s}_1^{(\mathbf{z}',\mathbf{z}''),\#\mathbf{z}}, \ldots, \mathbf{s}_{\mathbf{m}}^{(\mathbf{z}',\mathbf{z}''),\#\mathbf{z}})$.

3.2.4 The Final Three-Party Protocol

For $m \in \mathbb{N}$, our three-party, $3m$-round, $\frac{O(\log^3 m)}{m}$-fair coin-flipping protocol Π_m^3 is defined as follows.

Protocol 3.21 $(\widehat{\Pi}_m^3 = (\widehat{\mathsf{P}}_0^3, \widehat{\mathsf{P}}_1^3, \widehat{\mathsf{P}}_2^3))$**.**

Input: round parameter 1^m.

Oracle: Oracle $\tilde{o}_2$ *and* $\tilde{o}_3$ *for computing* $\mathsf{TwoPartySharesGen}_{\frac{1}{2}}$ *and* $\mathsf{ThreePartySharesGen}$ *respectively.*

Protocol's description:

1. *The three parties using the oracle* $\tilde{o}_3$ *to securely compute* $\mathsf{ThreePartySharesGen}(1^m)$. *Let* S_0, S_1, *and* S_2 *be the outputs obtained by* $\widehat{\mathsf{P}}_0^3$, $\widehat{\mathsf{P}}_1^3$ *and* $\widehat{\mathsf{P}}_2^3$ *respectively.*

2. *In case one party aborts, the remaining parties use oracle* $\tilde{o}_2$ *to interact in* $\widehat{\Pi}_m^2$ *(Protocol 3.3).*

3. *In case two parties aborts, the remaining party outputs a uniform bit.*

4. *Otherwise, the three parties interact in $\Pi_m^3 = (\mathsf{P}_0^3, \mathsf{P}_1^3, \mathsf{P}_2^3)$, where $\widehat{\mathsf{P}}_z^3$ plays the role of P_z^3 with private input S_z.*

3.2.5 Main Theorems for Three-Party Protocols

Theorem 3.22. *For $m \equiv 1 \bmod 4$, protocol $\widehat{\Pi}_m^3$ is a $(4m)$-round, three-party, $O(\frac{\log^3 m}{m})$-fair, coin-flipping protocol, against unbounded fail-stop adversaries, in the $(\mathsf{TwoPartySharesGen}_{\frac{1}{2}}, \mathsf{ThreePartySharesGen})$-hybrid model.*

As in the two-party case, we deduce the following result.

Theorem 3.23 (Main theorem — three-party, fair coin flipping). *Assuming protocols for securely computing OT exist, then for any polynomially bounded, polynomial-time computable, integer function m, there exists an m-round, $\frac{O(\log^3 m)}{m}$-fair, three-party coin-flipping protocol.*

Proof. The only issue one should take care of in the current proof, which does not occur in the proof of Theorem 3.5, is that the function $\mathsf{HidTwoPartySharesGen}$, called by $\mathsf{ThreePartySharesGen}$, and in particular calculating the value of $\widehat{\mathcal{C}}_{\mathsf{sum}_m(1)}^{-1}(\delta)$, is not necessarily polynomial-time computable. (This issue was not a problem in the proof of Theorem 3.5, since $\widehat{\mathcal{C}}_{\mathsf{sum}_m(1)}^{-1}(\cdot)$ is only called there with $\delta = \frac{1}{2}$, and in this case its output is simply 0). Note, however, that after $\mathsf{HidTwoPartySharesGen}$ calculates $\varepsilon = \widehat{\mathcal{C}}_{\mathsf{sum}_m(1)}^{-1}(\delta)$, it merely uses ε for sampling $5 \cdot \mathsf{sum}_m(1)$ independent samples from $\mathcal{C}_\varepsilon$. Hence, one can efficiently estimate ε by a value $\widetilde{\varepsilon}$ (via binary search),[16] such that $|\varepsilon - \widetilde{\varepsilon}| < \frac{1}{m^5}$, which yields that the statistical distance of $5 \cdot \mathsf{sum}_m(1)$ independent samples from $\mathcal{C}_\varepsilon$, from $5 \cdot \mathsf{sum}_m(1)$ independent samples from $\mathcal{C}_{\widetilde{\varepsilon}}$, is bounded by $\frac{1}{m^2}$. It follows that there exists a polynomial-time computable function $\widetilde{\mathsf{ThreePartySharesGen}}$, such that protocol $\widehat{\Pi}_m^3$ given in Protocol 3.21, is a $(4m)$-round, $\left(\frac{O(\log^3 m)}{m} + \frac{m}{m^2}\right)$-fair, three-party coin-flipping protocol, against unbounded fail-stop adversaries, in the $(\mathsf{TwoPartySharesGen}_{\frac{1}{2}}, \widetilde{\mathsf{ThreePartySharesGen}})$-hybrid model. The proof continues like the proof of Theorem 3.5. $\square$

Proving Theorem 3.22. We advise to reader to read first the proof of Theorem 3.4.

Proof of Theorem 3.22. Fix $m \equiv 1 \bmod 4$. As in the proof of Theorem 3.4, it holds that protocol $\widehat{\Pi}_m^3$ is correct according to Definition 2.15. Also as in the proof of Theorem 3.4, we assume without loss of generality that if a party aborts in the i'th round, it does so by sending the message Abort, and after seeing the other parties' message of that round.

Let the (p, i, j)'th round in a random execution of $\widehat{\Pi}_m^3$, for $(p, i, j) \in \{\mathsf{outer}, \mathsf{inner}\} \times (m) \times \{a, b\}$, stands for the j'th step of the i'th loop in the execution of the $\widehat{\Pi}_m^3$, where $p = \mathsf{outer}$ means that this is a step of the outer execution of $\widehat{\Pi}_m^3$, and $p = \mathsf{inner}$ means that this is a step of the inner execution

---

[16] The binary search on a value $\widetilde{\varepsilon} \in [-1, 1]$ is done by sampling $x \leftarrow \mathcal{C}_{m^{11}, \widetilde{\delta} - \frac{1}{2}}$ (for $\widetilde{\delta} = \widehat{\mathcal{C}}_{\mathsf{sum}_m(1), \widetilde{\varepsilon}}(0)$) and guessing if $\widetilde{\varepsilon}$ is bigger, smaller or close enough to ε according to whether x is bigger, smaller or inside the range $(\delta - \frac{1}{2}) \cdot m^{11} \pm m^6$, respectively. By Hoeffding Inequality (Fact 2.2), all the guesses are good with probability $1 - \mathsf{neg}(m)$ and the binary search outputs $\widetilde{\varepsilon}$ such that $|\varepsilon - \widetilde{\varepsilon}| \leq \left|\delta - \widetilde{\delta}\right| \leq \frac{1}{m^5}$.

of Π_m^2 (whose execution starts in case a party aborts). We let $(\mathsf{outer}, 0, a)$ be the zero round, let $(\mathsf{outer}, 0, b)$ denote the round where the call to ThreePartySharesGen is made, and let $(\mathsf{inner}, 0, b)$ be the zero round in the inner execution of Π_m^2.

Let A be a fail-stop adversary controlling the parties $\{\widehat{\mathsf{P}}_z^3\}_{z \in \mathcal{C}}$, for some $\mathcal{C} \subsetneq \{0, 1, 2\}$. Let V be the view of A in a random execution of $\widehat{\Pi}_m^3$, in which A controls the parties indexed by $\mathcal{C}$. For $\mathbf{r} \in \{\mathsf{outer}, \mathsf{inner}\} \times (m) \times \{a, b\}$, let $V_{\mathbf{r}}$ be the $\mathbf{r}$'th round prefix of V, and let $V_{\mathbf{r}}^-$ be the value of $V_{\mathbf{r}}$ with the $\mathbf{r}$'th round abort messages (if any) removed. Finally, let I_1 and I_2 be the rounds in which A sent an abort message, letting $I_k = (\mathsf{outer}, m, b)$ in case less than k aborts happen. In the following we show that for both $k \in \{1, 2\}$, it holds that

$$\left| \mathrm{E}\left[\mathsf{val}(V_{I_k}) - \mathsf{val}(V_{I_k}^-) \right] \right| \leq \frac{\xi \cdot \log^3 m}{m} \tag{4}$$

for some universal (independent of m) constant $\xi \geq 0$, where $\mathsf{val}(v)$ is the expected outcome of an honest (non aborting) execution of the parties that do not abort in v, conditioned on v (see Definition 2.16). Since Equation (4) holds for any $m \equiv 1 \mod 4$ and any fail-stop adversary A, the proof of the theorem follows by Lemma 2.18.

So it is left to prove Equation (4). By construction, the only non-redundant information in A's view at the end of round (i, b) is the coins constructed by the parties at the end of this round. In particular, it holds that $\mathsf{val}(V_{\mathsf{outer},0,b}) = \frac{1}{2}$. By construction, in case two parties abort during the call to ThreePartySharesGen, the remaining party outputs one with probability $\frac{1}{2}$. In case one party aborts, the remaining parties interact in the unbiased protocol $\widehat{\Pi}_m^2$. In both cases, it holds that $\mathsf{val}(V_{\mathsf{outer},0,b}^-) = \frac{1}{2}$. Taken the security of protocol $\widehat{\Pi}_m^2$ (proven in Theorem 3.4) into account, we can assume without loss of generality that A only aborts (if any) during the embedded execution of $\Pi_m^3 = (\mathsf{P}_0^3, \mathsf{P}_1^3, \mathsf{P}_2^3)$.

In the rest of the proof we separately bound the case $k = 1$ and $k = 2$. Note that I_1 is of the form $(\mathsf{outer}, \cdot, \cdot)$, where I_2, unless equals (outer, m, b), is of the form $(\mathsf{inner}, \cdot, \cdot)$ (i.e., the first abort is in the outer three-party protocol, and the second, if any, is in the inner two-party protocol).

First abort. We separately consider the case $I_1 = (\mathsf{outer}, \cdot, a)$ and the case $I_1 = (\mathsf{outer}, \cdot, b)$. We conclude the proof, of this part, showing that the first type of aborts might help A to gain $\frac{O(\log^3 m)}{m}$ advantage, where the second type give him *nothing*.

Case $I_1 = (\mathsf{outer}, \cdot, b)$. Assume that $I_1 = (\mathsf{outer}, i, b)$ for some $i \in [m]$. The view of A at this point (i.e., V_{I_1}) contains the value of $(c_1, \ldots, c_i)$, and some random function of these values, i.e., the shares of the next rounds it got from ThreePartySharesGen, which are uniform strings from his point of view, and the shares used till this round, which are random function of $(c_1, \ldots, c_i)$. Hence, $\mathsf{val}(V_{I_1}^-) = \delta_i := \widehat{\mathcal{C}}_{\mathsf{sum}_m(i+1),0}\left(-\sum_{j=1}^i c_j \right)$. By construction, δ_i is also the expected outcome of the remaining parties, in case an abort message was sent in this round. Namely, $\mathsf{val}(V_{I_1}) = \delta_i$. Hence, the adversary gains nothing (i.e., $\mathsf{val}(V_{I_1}) = \mathsf{val}(V_{I_1}^-)$), by aborting in this round.

Case $I_1 = (\mathsf{outer}, \cdot, a)$. Since A's first abort at Step 1b of the loop gains nothing, we assume without loss of generality that A's first abort is at Step 1a of the loop. We use the following claim, proof given below, for bounding the effect of such abort.

Claim 3.24. *Assuming* A*'s first abort is only at Step 1a of the loop in* Π_m^3*, it follows that*

$$\left| \mathrm{E} \left[\mathsf{val}(V_{I_1}) - \mathsf{val}(V_{I_1})^- \right] \right| \leq \frac{\xi \cdot \log^3 m}{m},$$

for some universal (independent of m) constant $\xi \geq 0$.

Claim 3.24 yields that the overall bias A's first abort gains, which equals to $|\mathrm{E}\left[\mathsf{val}(V_{I_1}) - \mathsf{val}(V_{I_1})^-\right]|$, is bounded by $\frac{\xi \cdot \log^3 m}{m}$, for some universal constant $\xi \geq 0$.

Second abort. We assume without loss of generality that $I_2 = (\mathsf{inner}, \cdot, \cdot)$ (i.e., a second abort occurred). Assume $I_1 = (\mathsf{out}, j, \cdot)$ and let ε be the value of $\widehat{\mathcal{C}}_m^{-1}(\delta_j)$ computed by HidTwoPartySharesGen on input δ_j, for generating the shares of the two-party protocol.

The following proof is similar to analysis of the two-party protocol Π_m^2, done in the proof of Theorem 3.4, but with few differences. We separately consider the case $I_2 = (\mathsf{inner}, \cdot, a)$ and the case $I_2 = (\mathsf{inner}, \cdot, b)$. We conclude the proof showing that the first type of aborts might help A to gain $\frac{O(\log^3 m)}{m}$ advantage, where the second type give him *nothing*.

Case $I_2 = (\mathsf{inner}, \cdot, b)$**.** Assume $I_2 = (\mathsf{inner}, i, b)$. The view of A at this point (i.e., V_{I_2}) contains the value of $(c_1, \ldots, c_i)$ sampled by HidTwoPartySharesGen, and some random function of these values, i.e., the shares of the next rounds it got from HidTwoPartySharesGen, which are uniform strings from his point of view, and the shares used till this round, which are random function of $(c_1, \ldots, c_i)$. Hence,

$$\mathsf{val}(V_{I_2}^-) = \delta_i := \widehat{\mathcal{C}}_{\mathsf{sum}_m(i+1),\varepsilon} \left(-\sum_{j=1}^{i} c_j \right)$$

By construction, δ_i is also the expected outcome of the remaining party, in case an abort message was sent in this round. It follows that $\mathsf{val}(V_{I_2}) = \delta_i$, and the adversary gains nothing (i.e., $\mathsf{val}(V_{I_2}) = \mathsf{val}(V_{I_2}^-)$), by aborting in this round.

The above point needs is somewhat subtle and deserves some justification. Note that the output of the remaining party P_z^2 is not directly sampled from $\mathcal{B}er(\delta_i)$, as in the case of protocol $\widehat{\Pi}_m^2$ considered in the proof of Theorem 3.4. Rather, a $(2 \cdot \mathsf{sum}_m(1))$-size vector v^z is sampled according to $\mathcal{C}_\varepsilon$ (see Algorithm 3.19). Then, the output of the remaining party is set to one if $\sum_{j=1}^{i} c_j + w(v_{\mathcal{I}^z}^z) \geq 0$, and to zero otherwise, where $\mathcal{I}^z$ is random $(\mathsf{sum}_m(i+1))$-size subset of $[2 \cdot \mathsf{sum}_m(1)]$. Yet, by construction, since V_{I_2} does not contain any extra information about the remaining party's vector v^z, it follows that

$$\mathsf{val}(V_{I_2}) = \mathrm{Pr}_{v^z \leftarrow (\mathcal{C}_\varepsilon)^{2 \cdot \mathsf{sum}_m(1)}, \mathcal{I}^z \subset [2 \cdot \mathsf{sum}_m(1)]} \left[\sum_{j=1}^{i} c_j + w(v_{\mathcal{I}^z}^z) \geq 0 \right] \tag{5}$$

$$= \mathrm{Pr}_{u \leftarrow (\mathcal{C}_\varepsilon)^{\mathsf{sum}_m(i+1)}} \left[\sum_{j=1}^{i} c_j + w(u) \geq 0 \right]$$

$$= \delta_i.$$

Case $I_2 = (\mathsf{inner}, \cdot, a)$. Since A's second abort at Step 1b of the loop gains nothing, we assume without loss of generality that A's second abort is at Step 1a of the loop. We use the following claim, proof given below, for bounding the effect of such abort.

Claim 3.25. *Assuming A's second abort is only at Step 1a of the loop in Π_m^2, it follows that*

$$\left| \mathrm{E}\left[\mathsf{val}(V_{I_2}) - \mathsf{val}(V_{I_2})^- \right] \right| \leq \frac{\xi \cdot \log^3 m}{m},$$

for some universal (independent of m) constant $\xi \geq 0$.

Claim 3.25 yields that the overall bias A's second abort gains, which equals to $|\mathrm{E}\left[\mathsf{val}(V_{I_2}) - \mathsf{val}(V_{I_2})^-\right]|$, is bounded by $\frac{\xi \cdot \log^3 m}{m}$, for some universal constant $\xi \geq 0$. $\qquad\square$

It is left to prove Claims 3.24 and 3.25. Similarly to the proof of Claim 3.15, we prove these claims via reductions to online-binomial games, described in Section 3.1.5.

Proving Claim 3.24 The proof immediately follows from the following claim and Lemma 3.13.

Claim 3.26. *Assuming A's first abort is only at Step 1a of the loop in Π_m^3, then*

$$\left| \mathrm{E}\left[\mathsf{val}(V_{I_1}) - \mathsf{val}(V_{I_1})^- \right] \right| \leq \mathsf{Bias}(\mathsf{G}_{f,m,0}),$$

where $\mathsf{G}_{f,m,0}$ is a 9-vector game according to Definition 3.12 and $\mathsf{Bias}(\cdot)$ is according to Definition 3.7.

Proof of Claim 3.26. We prove that an attacker for the coin-flipping protocol of the type considered in this claim, i.e., one that achieves bias α from his first abort at Step 1a of the loop in Π_m^3, yields a player for the vector binomial game (described in Section 3.1.5) that achieves the same bias. Thus, the bound on the former attacker follows from the bound on the latter one.

Recall that A controls the parties $\{\mathsf{P}_z^3\}_{z \in \mathcal{C}}$ in Π_m^3 and assume without loss of generality that $\mathcal{C} = \{0, 1\}$. Consider the 9-vector binomial game $\mathsf{G} = \mathsf{G}_{f,m,0} = \{X_i, Y_i, H_i, O_i, O_i^-\}$ as defined in Definition 3.12 and recall that in this game, f is the randomized function that on input (i, y) outputs a string in $\{-1, 1\}^{9 \cdot \mathsf{sum}_m(1)}$, where each of entries takes the value 1 with probability $\widehat{\mathcal{C}}_{\mathsf{sum}_m(1)}^{-1}(\delta)$ for $\delta = \widehat{\mathcal{C}}_{\mathsf{sum}_m(i+1),0}(-y)$. Now, consider the player B for G that emulates interaction with A in $\Pi_m^3 = (\mathsf{P}_0^3, \mathsf{P}_1^3, \mathsf{P}_2^3)$, where A controls P_0^3 and P_1^3. The emulation goes as follows:

Algorithm 3.27 (Player B for the vector game)**.**

Operation:

1. *For $z \in \{0, 1\}$, choose $\mathbf{S}^\mathbf{z} = (\mathbf{c}^{\#\mathbf{z}}, \mathbf{D}^{(0,1),\#\mathbf{z}}, \mathbf{D}^{(0,2),\#\mathbf{z}}, \mathbf{D}^{(1,0),\#\mathbf{z}}, \mathbf{D}^{(1,2),\#\mathbf{z}}, \mathbf{D}^{(2,0),\#\mathbf{z}}, \mathbf{D}^{(2,1),\#\mathbf{z}})$ $\leftarrow \{0, 1\}^{m \times \lceil \log m \rceil + 6 \times m \times (m \times \lceil \log m \rceil + 2(m+1))}$ as inputs for P_0^3 and P_1^3 in $\Pi_m^3 = (\mathsf{P}_0^3, \mathsf{P}_1^3, \mathsf{P}_2^3)$.*

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

   (a) *Receive input (i, Y_{i-1}, H_i) from the game G (recall that $H_i \in \{-1, 1\}^{9 \cdot \mathsf{sum}_m(1)}$).*

   (b) *If $i > 1$, emulate a sending of $\mathbf{c}^{\#\mathbf{2}}[i-1]$ from P_2^3 to the other parties at step $(i-1, b)$ of Π_m^3, where $\mathbf{c}^{\#\mathbf{2}}[i-1] := X_{i-1} \oplus \mathbf{c}^{\#\mathbf{0}}[i-1] \oplus \mathbf{c}^{\#\mathbf{1}}[i-1]$ (recall that $X_{i-1} := Y_{i-1} - Y_{i-2}$ according to Definition 3.6).*

(c) *Emulate a sending of* $\mathbf{D}^{(0,1),\#2}[i]$ *and* $\mathbf{D}^{(0,2),\#2}[i]$ *from* P_2^3 *to* P_0^3, *and emulate a sending of* $\mathbf{D}^{(1,0),\#2}[i]$ *and* $\mathbf{D}^{(1,2),\#2}[i]$ *from* P_2^3 *to* P_1^3 *at step* (i,a) *of* Π_m^3, *where*

  i. $(\mathbf{D}^{(0,1),\#2}[i], \mathbf{D}^{(1,0),\#2}[i])$ *is set to the output of* HidTwoPartySharesGen *where* v^z *at Step 2 of* HidTwoPartySharesGen *is set to* $\{H_i[2z\cdot\mathsf{sum}_m(1)], \dots, H_i[4z\cdot\mathsf{sum}_m(1)-1]\}$ *for* $z \in \{0,1\}$, *and* c_i *at Step 4a is set to* $H_i[4\cdot\mathsf{sum}_m(1)-1+i]$ *for* $i \in [m]$.

  ii. *For* $z \in \{0,1\}$, *choose a random* $(\mathsf{sum}_m(1))$-*size subset* $\mathcal{W}^z \subset \{H_i[(5+2z)\cdot\mathsf{sum}_m(1)], \dots, H_i[(7+2z)\cdot\mathsf{sum}_m(1)-1]\}$, *choose uniformly* $\mathbf{D}^{(z,2),\#2}[i] \leftarrow \{0,1\}^{m\cdot\lceil\log m\rceil+(m+1)}$, *and change the last bit of* $\mathbf{D}^{(z,2),\#2}[i]$ *to* 1 *if* $\sum_{w\in\mathcal{W}^z} w \geq 0$ *and to* 0 *otherwise.*

  If P_0^3 *or* P_1^3 *aborts at this step, output* 1 *(abort at round* i*). Otherwise, output* 0 *(continue to next round).*

Note that by the definition of f, the set of B's emulation variables $(X_1,\dots,X_m,\{\mathbf{D}^{(\mathbf{z},\mathbf{z}')}\}_{z\in\{0,1\},z\neq z'})$ has the same joint distribution as the set of Π_m^3's variables $(c_1,\dots,c_m,\{\mathbf{D}^{(\mathbf{z},\mathbf{z}')}\}_{z\in\{0,1\},z\neq z'})$, where the parties' inputs are sampled according to ThreePartySharesGen. Therefore, A's view in the emulation done by B, is distributed exactly the same as its view when interacting with honest P_2^3 in Π_m^3; in both cases, the only meaningful information it gets is the revelation of these values. In addition, note that B aborts at round i of G (i.e outputs 1) iff A's first aborts is at round (i,a) of Π_m^3.

For concluding the analysis, let g be the function that on input $H_i \in \{-1,1\}^{9\cdot\mathsf{sum}_m(1)}$, outputs $\{\mathbf{D}^{(\mathbf{z},\mathbf{z}')}\}_{z\in\{0,1\},z\neq z'}$ as described in Step 2c, and let B' be an attacker for $\mathsf{G}_{g\circ f,m,0}$ that operates just like B, only that it gets the output of $g \circ f$ directly instead of constructing the output as B does at Step 2c. It follows that

$$\mathsf{Bias}_{\mathsf{B}'}(\mathsf{G}_{g\circ f,m,0}) = \left| \mathrm{E}\left[\mathsf{val}(V_{I_1}) - \mathsf{val}(V_{I_1})^-\right] \right|, \tag{6}$$

We conclude that

$$\left| \mathrm{E}\left[\mathsf{val}(V_{I_1}) - \mathsf{val}(V_{I_1})^-\right] \right| = \mathsf{Bias}_{\mathsf{B}'}(\mathsf{G}_{g\circ f,m,0}) \tag{7}$$
$$\leq \mathsf{Bias}(\mathsf{G}_{g\circ f,m,0})$$
$$\leq \mathsf{Bias}(\mathsf{G}_{f,m,0}).$$

$\square$

Proving Claim 3.25 The proof immediately follows from the following claim and Lemma 3.11.

Claim 3.28. *Assuming* A*'s second abort is only at Step 1a of the loop in* Π_m^2 *and that* $\mathsf{Bias}(\mathsf{G}_{f,m,\varepsilon}) \leq \alpha(m)$ *for any* $\varepsilon \in [-1,1]$ *and for any randomized function* f *of a* 12-*hypergeometric game, as defined in Definition 3.10. Then*

$$\left| \mathrm{E}\left[\mathsf{val}(V_{I_2}) - \mathsf{val}(V_{I_2})^-\right] \right| \leq \alpha(m) + \frac{2}{m}.$$

Proof of Claim 3.25. We prove that an attacker for the coin-flipping protocol of the type considered in this claim, i.e., one that achieves bias α from his second abort at Step 1a of the loop in Π_m^2,

yields a player for the hypergeometric binomial game (described in Definition 3.10) that achieves the same bias. Thus, the bound on the former attacker follows from the bound on the latter one.

Assume without loss of generality that A controls P_0^2 in Π_m^2 after the first abort, and recall that the parties' inputs are sampled according to $\mathsf{HidTwoPartySharesGen}(\delta)$ for some $\delta \in [0,1]$. Let $\varepsilon = \widehat{\mathcal{C}}_{\mathsf{sum}_m(1)}^{-1}(\delta)$ and let $p = w(v^0)$ where v^0 is the vector that has been sampled in Step 2 of $\mathsf{HidTwoPartySharesGen}$. Consider the binomial game $\mathsf{G} = \mathsf{G}_{f_p,m,\varepsilon} = \{X_i, Y_i, H_i, O_i, O_i^-\}$ as defined in Definition 3.6 where f_p is the randomized function that on input (i,y) outputs 1 with probability $\delta_p = \widehat{\mathcal{HG}}_{2\cdot\mathsf{sum}_m(1),p,\mathsf{sum}_m(i+1)}(-y)$ and zero otherwise (i.e hypergeometric game). Let B be the player described in the proof of Claim 3.15 at Algorithm 3.17, and let B' be the player for G which operates as B, where the only difference is that at step 1 it chooses $\mathbf{d}^{0,\#0}[m+1]$ according to $\mathcal{Ber}(\delta_p)$ instead of uniformly over $\{0,1\}$ as B does. By the definition of f_p, the set of G's variables $(X_1, \ldots, X_m, H_1, \ldots, H_m)$ has the same distribution as the set of Π_m^2's variables $(c_1, \ldots, c_m, d_1^0, \ldots, d_m^0)$ after A's first abort.

Therefore, after the first abort, A's view in the emulation done by B, is distributed exactly the same as its view when interacting with honest with honest P_1^2 in Π_m^2; in both cases, the only meaningful information A' gets is the revelation of these values together with the value of $\mathbf{d}^{0,\#0}[m+1]$, which is distributed the same in both cases. Since B' aborts at round i of G (i.e outputs 1) iff A aborts at round (i,a) of Π_m^2, it follows that

$$\mathop{\mathrm{E}}_{\delta,p}\left[\mathsf{Bias}_{\mathsf{B}'}(\mathsf{G})\right] = \left|\mathrm{E}\left[\mathsf{val}(V_{I_2}) - \mathsf{val}(V_{I_2})^-\right]\right|, \tag{8}$$

where $\mathsf{Bias}_{\mathsf{B}'}(\mathsf{G})$ is according to Definition 3.7 and the expectation is on the values of δ and p which are being set after A's first abort. Note that by the definition of ε it holds that $O_1^- = \delta$, where O_1^- is according to Definition 3.6. Therefore, in case $\delta \notin [\frac{1}{m^2}, 1 - \frac{1}{m^2}]$, Lemma 3.14 tells us that $\mathsf{Bias}_{\mathsf{B}'}(\mathsf{G}) \leq \frac{1}{m}$. Assuming that $\delta \in [\frac{1}{m^2}, 1 - \frac{1}{m^2}]$, Hoeffding inequality (Fact 2.2) yields that $|\varepsilon| < 4 \cdot \sqrt{\frac{\log m}{\mathsf{sum}_m(1)}}$. Therefore, since p is distributed according to $\mathcal{C}_{2\mathsf{sum}_m(1),\varepsilon}$, it follows that

$$\Pr\left[|p| > 12\sqrt{\log m \cdot \mathsf{sum}_m(1)} \mid \delta \in [\frac{1}{m^2}, 1 - \frac{1}{m^2}]\right] \tag{9}$$
$$\leq \Pr\left[|p - 2\varepsilon \cdot \mathsf{sum}_m(1)| > 4\sqrt{\log m \cdot \mathsf{sum}_m(1)} \mid \delta \in [\frac{1}{m^2}, 1 - \frac{1}{m^2}]\right]$$
$$\leq \frac{1}{m},$$

where the second inequality holds again by Hoeffding inequality. We conclude that

$$\left|\mathrm{E}\left[\mathsf{val}(V_{I_2}) - \mathsf{val}(V_{I_2})^-\right]\right| = \mathop{\mathrm{E}}_{\delta,p}\left[\mathsf{Bias}_{\mathsf{B}'}(\mathsf{G})\right] \tag{10}$$
$$\leq \mathop{\mathrm{E}}_{\delta,p}\left[\mathsf{Bias}_{\mathsf{B}'}(\mathsf{G}) \mid \delta \in [\frac{1}{m^2}, 1 - \frac{1}{m^2}]\right] + \frac{1}{m}$$
$$\leq \mathop{\mathrm{E}}_{\delta,p}\left[\mathsf{Bias}_{\mathsf{B}'}(\mathsf{G}) \mid \delta \in [\frac{1}{m^2}, 1 - \frac{1}{m^2}] \bigwedge |p| \leq 12\sqrt{\log m \cdot \mathsf{sum}_m(1)}\right] + \frac{2}{m}$$
$$\leq \alpha(m) + \frac{2}{m},$$

where the last inequality holds by the assumption. $\qquad\square$

4 Bounds for Online-Binomial Games

In the following section we focus on online-binomial games, as defined in Section 3.1.5. In Section 4.1 we state two basic tools for bounding the bias of such games, in Section 4.2 we develop our main tool for bounding the bias of such games and in Sections 4.3-4.5 we prove Lemmas 3.9, 3.11 and 3.13.

Recall that $\mathcal{C}_\varepsilon$ is the Bernoulli probability distribution over $\{-1, 1\}$, taking the value 1 with probability $\frac{1}{2}(1 + \varepsilon)$ and -1 otherwise, that $\mathcal{C}_{n,\varepsilon}$ is the binomial distribution induced by the sum of n independent random variables, each distributed according to $\mathcal{C}_\varepsilon$, and that $\ell_m(i) = m + 1 - i$ and $\mathsf{sum}_m(i) = \sum_{j=i}^m \ell_m(j)$.

We recall the following definitions from Section 3.1.5.

Definition 4.1 (online binomial games – Restatement of Definition 3.6)**.** *For $m \in \mathbb{N}$, $t \in \mathbb{Z}$, $\varepsilon \in [-1, 1]$ and a randomized (hint) function f, the* online game $\mathsf{G}_{f,m,\varepsilon,t}$ *is the set of the following random variables. Let $Y_0 = X_0 = t$, and for $i \in [m]$,*

- *X_i is sampled according to $\mathcal{C}_{\ell_m(i),\varepsilon}$.*

- *$Y_i = \sum_{j=0}^i X_j$ and $H_i = f(i, Y_i)$.*

- *$O_i = \mathsf{o}_i(Y_{i-1}, H_i)$ and $O_i^- = \mathsf{o}_i(Y_{i-1})$, for $\mathsf{o}_i(y) = \Pr[Y_m \geq 0 \mid Y_{i-1} = y]$ and $\mathsf{o}_i(y, h) = \Pr[Y_m \geq 0 \mid Y_{i-1} = y, H_i = h]$, respectively.*

Let $O_{m+1} = O_{m+1}^- = 1$ if $Y_m \geq 0$, and $O_{m+1} = O_{m+1}^- = 0$ otherwise.
We let $\mathsf{G}_{f,m,\varepsilon} = \mathsf{G}_{f,m,\varepsilon,0}$.

Definition 4.2 (game bias – Restatement of Definition 3.7)**.** *Let m, t, ε, f and $\mathsf{G} = \mathsf{G}_{f,m,\varepsilon,t} = \{X_i, Y_i, H_i, O_i, O_i^-\}$ be as in Definition 4.1. 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 (i, Y_{i-1}, H_i) and outputs a 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 $\mathsf{Bias}(\mathsf{G}) = \max_\mathsf{B}\{\mathsf{Bias}_\mathsf{B}(\mathsf{G})\}$, where the maximum is over* all *possible algorithms B.*

4.1 Basic Tools

We present two basic tools for bounding a game bias. The first tool asserts that the game bias can only decrease when applying a random function to the hint.

Lemma 4.3. *For randomized functions f and g, $m \in \mathbb{N}$, $\varepsilon \in [-1, 1]$ and $t \in \mathbb{Z}$, let $\mathsf{G}_{f,m,\varepsilon,t}$ and $\mathsf{G}_{g \circ f,m,\varepsilon,t}$ be according to Definition 4.1. It holds that $\mathsf{Bias}(\mathsf{G}_{g \circ f,m,\varepsilon,t}) \leq \mathsf{Bias}(\mathsf{G}_{f,m,\varepsilon,t})$.*

Proof. Let $\{Y_i\}_{i=0}^m$ be distributed as in $\mathsf{G}_{f,m,\varepsilon,t}$ (according to Definition 4.1), let $\tau = g \circ f$ and let B^τ be the algorithm with $\mathsf{Bias}_{\mathsf{B}^\tau}(\mathsf{G}_{\tau,m,\varepsilon,t}) = \mathsf{Bias}(\mathsf{G}_{\tau,m,\varepsilon,t})$. Let B^f be the algorithm for $\mathsf{G}_{f,m,\varepsilon,t}$ that emulates an execution of B^τ in $\mathsf{G}_{\tau,m,\varepsilon,t}$. Namely, B^f on input (i, y, h) emulates a sending of

$(i, y, g(h))$ from the game $\mathsf{G}_{\tau,m,\varepsilon,t}$ to B^τ and outputs B^τ's output. Let I be the first round on which B^τ outputs one in $\mathsf{G}_{\tau,m,\varepsilon,t}$, let $H_i^f = f(i, Y_i)$ and let $H_i^\tau = \tau(i, Y_i)$. It follows that

$\mathsf{Bias}(\mathsf{G}_{\tau,m,\varepsilon,t})$

$= \mathsf{Bias}_{\mathsf{B}^\tau}(\mathsf{G}_{\tau,m,\varepsilon,t})$

$= \left| \underset{i \leftarrow I}{\mathrm{E}} \left[\underset{y \leftarrow Y_{i-1}, h \leftarrow H_i^\tau | I=i}{\mathrm{E}} [\Pr\left[Y_m \geq 0 \mid Y_{i-1} = y, H_i^\tau = h\right] - \Pr\left[Y_m \geq 0 \mid Y_{i-1} = y\right]] \right] \right|$

$= \left| \underset{i \leftarrow I}{\mathrm{E}} \left[\underset{y \leftarrow Y_{i-1}, h \leftarrow H_i^\tau | I=i}{\mathrm{E}} \left[\underset{h' \leftarrow H_i^f | Y_{i-1}=y, H_i^\tau = h}{\mathrm{E}} \left[\Pr\left[Y_m \geq 0 \mid Y_{i-1} = y, H_i^f = h'\right] - \Pr\left[Y_m \geq 0 \mid Y_{i-1} = y\right] \right] \right] \right] \right|$

$= \left| \underset{i \leftarrow I}{\mathrm{E}} \left[\underset{y \leftarrow Y_{i-1}, h' \leftarrow H_i^f | I=i}{\mathrm{E}} \left[\Pr\left[Y_m \geq 0 \mid Y_{i-1} = y, H_i^f = h'\right] - \Pr\left[Y_m \geq 0 \mid Y_{i-1} = y\right] \right] \right] \right|$

$= \mathsf{Bias}_{\mathsf{B}^f}(\mathsf{G}_{f,m,\varepsilon,t})$

$\leq \mathsf{Bias}(\mathsf{G}_{f,m,\varepsilon,t}),$

where the last equality holds since I also describes the first output on which B^f outputs one in $\mathsf{G}_{f,m,\varepsilon,t}$. $\square$

The second tool is a restatement of Lemma 3.14. It asserts that if the expected value of a game is almost determined, then there is mo much room for an attacker to gain much bias.

Lemma 4.4. *[Restatement of Lemma 3.14]* Let $\mathsf{G}_{f,m,\varepsilon,t} = \{X_i, Y_i, H_i, O_i, O_i^-\}$ *be according to Definition 4.1. Assume that $O_1^- \notin [\frac{1}{m^2}, 1 - \frac{1}{m^2}]$, then* $\mathsf{Bias}(\mathsf{G}_{f,m,\varepsilon,t}) \leq \frac{2}{m}$.

Proof. We prove the case $O_1^- \leq \frac{1}{m^2}$, where the other case is analogues. By a simple averaging argument, it holds that

$$\Pr\left[\exists i \in [m]: O_i^- > \frac{1}{m}\right] \leq \frac{1}{m} \tag{11}$$

Consider the game $\mathsf{G}_{g,m,\varepsilon,t}$ for $g(i,y) = y$. By the above, $\mathsf{Bias}(\mathsf{G}_{g,m,\varepsilon,t}) \leq \frac{2}{m}$. Hence, Lemma 4.3 yields that the same also holds for $\mathsf{G}_{f,m,\varepsilon,t}$. $\square$

4.2 Main Tool — Expressing Game Bias using Ratio

In this section, we develop our main tool for bounding the bias of online-binomial games. Informally, we reduce the task of bounding the bias of a game into evaluating the "ratio" of the game, where ratio (defined below) is a useful game-depend measurement on how much the distribution of X_i is far from the distribution of $X_i \mid H_i$.

Definition 4.5. *Let $\mathsf{G}_{f,m,\varepsilon} = \{X_i, Y_i, H_i, O_i, O_i^-\}$ be according to Definition 4.1 and let $\mathcal{X}_i := \{x \in \mathrm{Supp}(X_i): |x| \leq 4 \cdot \sqrt{\log m \cdot \ell_m(i)}\}$. For $i \in [m]$, $y \in \mathrm{Supp}(Y_{i-1})$, $x \in \mathrm{Supp}(X_i)$ and $h \in \mathrm{Supp}(H_i)$, define*

$$\mathsf{ratio}_{i,y,h}(x) = \frac{\Pr\left[X_i = x \mid Y_{i-1} = y, H_i = h, X_i \in \mathcal{X}_i\right]}{\Pr\left[X_i = x \mid Y_{i-1} = y, X_i \in \mathcal{X}_i\right]}.$$

Namely, $\mathsf{ratio}_{i,y,h}(x)$ measures the change (in multiplicative term) of the probability $X_i = x$, due to the knowledge of h, assuming that X_i is typical (i.e., $X_i \in \mathcal{X}_i$).

The following lemma states that an appropriate upper-bound on $\left|1 - \mathsf{ratio}_{i,Y_{i-1},H_i}\right|$ for any "interesting" round i, yields an upper-bound on the game bias.

Lemma 4.6. *[main tool: expressing game bias using ratio] Let* $\mathsf{G} = \mathsf{G}_{f,m,\varepsilon} = \{X_i, Y_i, H_i, O_i, O_i^-\}$ *be according to Definition 4.1, and let* ratio *be according to Definition 4.5. Assume that for every* $i \in [m - \lfloor \log^{2.5} m \rfloor]$ *and* $y \in \mathcal{Y}_{i-1} := \{y \in \mathrm{Supp}(Y_{i-1}): |y + \varepsilon \cdot \mathsf{sum}_m(i)| \le 4\sqrt{\log m \cdot \mathsf{sum}_m(i)}\}$, *there exist* $\lambda > 0$ *and a set* $\mathcal{H}_{i,y}$ *such that:*

1. $\Pr\left[H_i \notin \mathcal{H}_{i,y} \mid Y_{i-1} = y\right] \le \frac{1}{m^2}$, *and*

2. $\left|1 - \mathsf{ratio}_{i,y,h}(x)\right| \le \lambda \cdot \sqrt{\frac{\log m}{\ell_m(i+1)}} \cdot \left(\frac{|x|}{\sqrt{\ell_m(i)}} + 1\right)$ *for every* $(x, h) \in \mathcal{X}_i \times \mathcal{H}'_{i,y}$,

for $\mathcal{H}'_{i,y} = \mathcal{H}_{i,y} \bigcap \mathrm{Supp}(H_i \mid Y_{i-1} = y, X_i \in \mathcal{X}_i)$. *Then*

$$\mathsf{Bias}(\mathsf{G}) \le \varphi(\lambda) \cdot \frac{\log^3 m}{m}$$

for a universal function φ.

In the following we fix f, m, ε, we let $\mathsf{G} = \mathsf{G}_{f,m,\varepsilon} = \{X_i, Y_i, H_i, O_i, O_i^-\}$ be according to Definition 4.1, and for $i \in [m]$, we let $\mathcal{X}_i$ be according to Definition 4.5 and $\mathcal{Y}_{i-1}$ be according to Lemma 4.6. We assume without loss of generality that m is larger than some universal constant and that $|\varepsilon| \le 4\sqrt{\frac{\log m}{\mathsf{sum}_m(1)}}$ (Otherwise, Hoeffding's inequality (Fact 2.2) yields that $O_1^- \notin [\frac{1}{m^2}, 1 - \frac{1}{m^2}]$ and the proof follows by Lemma 4.4).

The following sub-lemmas are the main building blocks for proving Lemma 4.6. The first one (proved in Section 4.2.1) states that an appropriate bound of each round bias, yields a bound on the game bias.

Lemma 4.7. *Assume that for every* $i \in [m - \lfloor \log^{2.5} m \rfloor]$ *and* $y \in \mathcal{Y}_{i-1}$, *there exists* $\lambda > 0$ *and a set* $\widehat{\mathcal{H}}_{i,y} \subseteq \mathrm{Supp}(H_i \mid Y_{i-1} = y)$ *such that*

1. $\Pr\left[H_i \notin \widehat{\mathcal{H}}_{i,y} \mid Y_{i-1} = y\right] \le \frac{3}{m^2}$, *and*

2. $\left|\mathsf{o}_i(y) - \mathsf{o}_i(y, h)\right| \le \lambda \cdot \frac{\sqrt{\log m}}{\ell_m(i+1)}$ *for every* $h \in \widehat{\mathcal{H}}_{i,y}$.

Then

$$\mathsf{Bias}(\mathsf{G}) \le \varphi(\lambda) \cdot \frac{\log^3 m}{m}$$

for a universal function φ.

The following lemma (proved in Section 4.2.2) relates the bias that can be obtained in a given round, to the ratio function.

Lemma 4.8. *For* $i \in [m]$, $y \in \mathrm{Supp}(Y_{i-1})$ *and* $h \in \mathrm{Supp}(H_i \mid Y_{i-1} = y, X_i \in \mathcal{X}_i)$, *it holds that*

$$\left|\mathsf{o}_i(y) - \mathsf{o}_i(y, h)\right| \le \mathop{\mathrm{E}}_{x \leftarrow X_i \mid x \in \mathcal{X}_i} \left[\left|\mathsf{o}_{i+1}(y + x) - \mathsf{o}_{i+1}(y)\right| \cdot \left|1 - \mathsf{ratio}_{i,y,h}(x)\right|\right] + 2 \cdot (q + q_h),$$

37

for $q = \Pr[X_i \notin \mathcal{X}_i]$ and $q_h = \Pr[X_i \notin \mathcal{X}_i \mid Y_{i-1} = y, H_i = h]$.[17]

Intuitively, the above tells that if H_i is unlikely to tell much information about X_i, reflected by $\mathsf{ratio}_{i,y,H_i}(X_i)$ being close to one, then the bias of round i is small.

We will also use the following two simple facts. The first one states some useful properties of the sets $\mathcal{X}_i$'s.

Claim 4.9. *The following holds for every $i \in [m]$.*

1. $\Pr\left[X_i \notin \mathcal{X}_i\right] < \frac{1}{m^3}$,

2. $\mathrm{E}_{x \leftarrow X_i | x \in \mathcal{X}_i}\left[|x|\right] < \mathrm{E}_{x \leftarrow X_i}\left[|x|\right]$,

3. $\mathrm{E}_{x \leftarrow X_i | x \in \mathcal{X}_i}\left[x^2\right] < \mathrm{E}_{x \leftarrow X_i}\left[x^2\right]$.

Proof. For Item 1, compute

$$\Pr\left[X_i \notin \mathcal{X}_i\right]$$
$$= \Pr\left[|X_i| > 4\sqrt{\log m \cdot \ell_m(i)}\right]$$
$$< \Pr\left[|X_i - \varepsilon \cdot \ell_m(i)| > 3 \cdot \sqrt{\log m \cdot \ell_m(i)}\right]$$
$$\leq 2 \cdot \exp\left(-\frac{3^2 \cdot \log m \cdot \ell_m(i)}{2 \cdot \ell_m(i)}\right)$$
$$< \frac{1}{m^3},$$

where the first inequality holds since $|\varepsilon| \leq 4\sqrt{\frac{\log m}{\mathsf{sum}_m(1)}}$ yields that $|\varepsilon| \cdot \ell_m(i) < \sqrt{\log m \cdot \ell_m(i)}$ and the second inequality holds by Hoeffding's inequality (Fact 2.2).

For Item 2, compute

$$\mathrm{E}_{x \leftarrow X_i}\left[|x|\right] = \Pr_{x \leftarrow X_i}\left[X_i \in \mathcal{X}_i\right] \cdot \mathrm{E}_{x \leftarrow X_i | x \in \mathcal{X}_i}\left[|x|\right] + \Pr_{x \leftarrow X_i}\left[X_i \notin \mathcal{X}_i\right] \cdot \mathrm{E}_{x \leftarrow X_i | x \notin \mathcal{X}_i}\left[|x|\right]$$
$$> \Pr_{x \leftarrow X_i}\left[X_i \in \mathcal{X}_i\right] \cdot \mathrm{E}_{x \leftarrow X_i | x \in \mathcal{X}_i}\left[|x|\right] + \Pr_{x \leftarrow X_i}\left[X_i \notin \mathcal{X}_i\right] \cdot \mathrm{E}_{x \leftarrow X_i | x \in \mathcal{X}_i}\left[|x|\right]$$
$$= \mathrm{E}_{x \leftarrow X_i | x \in \mathcal{X}_i}\left[|x|\right],$$

where the inequality holds since $\mathrm{E}_{x \leftarrow X_i | x \notin \mathcal{X}_i}\left[|x|\right] > 4\sqrt{\log m \cdot \ell_m(i)} \geq \mathrm{E}_{x \leftarrow X_i | x \in \mathcal{X}_i}\left[|x|\right]$. The proof of Item 3 is analogous to the above. $\square$

The second claim bounds the change of the expected game value in a single round.

Claim 4.10. *For $i \in [m - \lfloor \log^{2.5} m \rfloor]$, $x \in \mathcal{X}_i$ and $y \in \mathcal{Y}_{i-1}$, it holds that*

$$|\mathsf{o}_{i+1}(y + x) - \mathsf{o}_{i+1}(y)| \leq \frac{|x|}{\sqrt{\mathsf{sum}_m(i+1)}}.$$

Proof. Note that $|x|, |y + x| \leq 5 \cdot \sqrt{\log m \cdot \mathsf{sum}_m(i)} < \mathsf{sum}_m(i)^{\frac{3}{5}}$, that $|\varepsilon| \leq 4\sqrt{\frac{\log m}{\mathsf{sum}_m(1)}} < \mathsf{sum}_m(i)^{-\frac{2}{5}}$ and that $|\mathsf{o}_{i+1}(y + x) - \mathsf{o}_{i+1}(y)| = \left|\widehat{\mathcal{C}}_{\mathsf{sum}_m(i+1),\varepsilon}(-y - x) - \widehat{\mathcal{C}}_{\mathsf{sum}_m(i+1),\varepsilon}(-y)\right|$. Therefore, the proof immediately follows by Proposition 2.6. $\square$

---

[17]It can be easily shown that $\mathsf{o}_i(y) - \mathsf{o}_i(y, h) = \mathrm{E}_{x \leftarrow X_i}[(\mathsf{o}_{i+1}(y+x) - \mathsf{o}_{i+1}(y)) \cdot (1 - \frac{\Pr[X_i = x | Y_{i-1} = y, H_i = h]}{\Pr[X_i = x | Y_{i-1} = y]})]$. However, Lemma 4.8 allows us to ignore "non-typical" x's.

Putting it together.

Proof of Lemma 4.6. Let $i \in [m - \lfloor \log^{2.5} m \rfloor]$, $y \in \mathcal{Y}_{i-1}$ and $\mathcal{H}_{i,y}$ be the set that satisfies assumptions 1 and 2 of Lemma 4.6, let $\mathcal{H}'_{i,y} = \mathcal{H}_{i,y} \bigcap \mathrm{Supp}(H_i \mid Y_{i-1} = y, X_i \in \mathcal{X}_i)$ and let $\widehat{\mathcal{H}}_{i,y} = \{h \in \mathcal{H}'_{i,y} \mid \Pr[X_i \notin \mathcal{X}_i \mid Y_{i-1} = y, H_i = h] \le \frac{1}{m}\}$. We first show that $\Pr\left[H_i \notin \widehat{\mathcal{H}}_{i,y} \mid Y_{i-1} = y\right] \le \frac{3}{m^2}$. Next, we use Lemma 4.8 for bounding $|\mathsf{o}_i(y,h) - \mathsf{o}_i(y)|$ for every $h \in \widehat{\mathcal{H}}_{i,y}$ and the proof will follow by Lemma 4.7.

For the first part, let $\mathcal{S}_{i,y} = \{h \in \mathrm{Supp}(H_i) \mid \Pr[X_i \notin \mathcal{X}_i \mid Y_{i-1} = y, H_i = h] \le \frac{1}{m}\}$ and assume by contradiction that $\Pr[H_i \notin \mathcal{S}_{i,y} \mid Y_{i-1} = y] > \frac{1}{m^2}$. It follows that

$$
\begin{aligned}
\Pr[X_i \notin \mathcal{X}_i] &= \Pr[X_i \notin \mathcal{X}_i \mid Y_{i-1} = y] \\
&\ge \Pr[X_i \notin \mathcal{X}_i \mid Y_{i-1} = y, H_i \notin \mathcal{S}_{i,y}] \cdot \Pr[H_i \notin \mathcal{S}_{i,y} \mid Y_{i-1} = y] \\
&> \frac{1}{m} \cdot \frac{1}{m^2} \\
&= \frac{1}{m^3},
\end{aligned}
$$

In contradiction to Item 1 of Claim 4.9. Therefore,

$$
\Pr[H_i \notin \mathcal{S}_{i,y} \mid Y_{i-1} = y] \le \frac{1}{m^2}. \tag{12}
$$

In addition, note that

$$
\Pr[H_i \notin \mathrm{Supp}(H_i \mid Y_{i-1} = y, X_i \in \mathcal{X}_i) \mid Y_{i-1} = y] \le \Pr[X_i \notin \mathcal{X}_i] \le \frac{1}{m^2}. \tag{13}
$$

Using simple union bound, we conclude from Equations (12) and (13) that

$$
\Pr\left[H_i \notin \widehat{\mathcal{H}}_{i,y} \mid Y_{i-1} = y\right] \le \Pr[H_i \notin \mathcal{H}_{i,y} \mid Y_{i-1} = y] + \frac{2}{m^2} \le \frac{3}{m^2}, \tag{14}
$$

where the second inequality holds by assumption 1 of Lemma 4.6.

For the second part, note that for every $h \in \widehat{\mathcal{H}}_{i,y}$ it holds that

$$
|\mathsf{o}_i(y,h) - \mathsf{o}_i(y)| \le \operatorname*{E}_{x \leftarrow X_i | x \in \mathcal{X}_i} \left[|\mathsf{o}_{i+1}(y+x) - \mathsf{o}_{i+1}(y)| \cdot |1 - \mathsf{ratio}_{i,y,h}(x)| \right] + \frac{4}{m} \tag{15}
$$

$$
\le \operatorname*{E}_{x \leftarrow X_i | x \in \mathcal{X}_i} \left[\frac{|x|}{\sqrt{\mathsf{sum}_m(i+1)}} \cdot \left(\lambda \cdot \sqrt{\frac{\log m}{\ell_m(i+1)}} \left(\frac{|x|}{\sqrt{\ell_m(i)}} + 1 \right) \right) \right] + \frac{4}{m}
$$

$$
= \operatorname*{E}_{x \leftarrow X_i | x \in \mathcal{X}_i} \left[\frac{|x|}{\sqrt{\frac{1}{2}\ell_m(i)\ell_m(i+1)}} \cdot \left(\lambda \cdot \sqrt{\frac{\log m}{\ell_m(i+1)}} \left(\frac{|x|}{\sqrt{\ell_m(i)}} + 1 \right) \right) \right] + \frac{4}{m}
$$

$$
= \frac{\sqrt{2}\lambda \cdot \sqrt{\log m}}{\ell_m(i+1)} \cdot \operatorname*{E}_{x \leftarrow X_i | x \in \mathcal{X}_i} \left[\frac{x^2}{\ell_m(i)} + \frac{|x|}{\sqrt{\ell_m(i)}} \right] + \frac{4}{m}
$$

$$
\le \frac{\sqrt{2}\lambda \cdot \sqrt{\log m}}{\ell_m(i+1)} \cdot \left(\frac{2 \cdot \ell_m(i)}{\ell_m(i)} + \frac{\sqrt{2 \cdot \ell_m(i)}}{\sqrt{\ell_m(i)}} \right) + \frac{4}{m}
$$

$$
\le \frac{(5\lambda + 4) \cdot \sqrt{\log m}}{\ell_m(i+1)}.
$$

39

The first inequality holds by Lemma 4.8 (recalling Item 1 of Claim 4.9 and that $\Pr[X_i \notin \mathcal{X}_i \mid Y_{i-1} = y, H_i = h] \leq \frac{1}{m}$ by the definition of $\widehat{\mathcal{H}}_{i,y}$). The second inequality holds by Claim 4.10 and by assumption 2 of Lemma 4.6. The third inequality holds by Fact 2.3 (recalling Items 2 and 3 of Claim 4.9).

In conclusion, we proved that for every $i \in [m - \lfloor \log^{2.5} m \rfloor]$ and $y \in \mathcal{Y}_{i-1}$, the set $\widehat{\mathcal{H}}_{i,y}$ satisfies the constrains of Lemma 4.7. Hence, Lemma 4.7 yields that $\mathsf{Bias}(\mathsf{G}) \leq \varphi(5\lambda + 4) \cdot \frac{\log^3 m}{m}$, for some universal function φ, as required. □

4.2.1 Proving Lemma 4.7

We will use the following facts. The first claim yields that if $Y_{i-1} \notin \mathcal{Y}_{i-1}$ (i.e., $|Y_{i-1}|$ is untypically large), then the expected value of the game at round i is almost determined.

Claim 4.11. *For every $i \in [m]$ and $y \in \mathrm{Supp}(Y_{i-1}) \setminus \mathcal{Y}_{i-1}$, it holds that*

$$\Pr\left[\sum_{j=i}^{m} X_j \geq -y\right] \notin \left[\frac{1}{m^2}, 1 - \frac{1}{m^2}\right].$$

Proof. Let $Z_i := \sum_{j=i}^{m} X_j$. We assume that $y + \varepsilon \cdot \mathsf{sum}_m(i) \leq 0$, where the proof of the case $y + \varepsilon \cdot \mathsf{sum}_m(i) > 0$ is analogous. Note that since $y \notin \mathcal{Y}_{i-1}$, then $-(y + \varepsilon \cdot \mathsf{sum}_m(i)) > 4\sqrt{\log m \cdot \mathsf{sum}_m(i)}$, and since Z_i is distributed according to $\mathcal{C}_{\mathsf{sum}_m(i),\varepsilon}$, then $\mathrm{E}[Z_i] = \varepsilon \cdot \mathsf{sum}_m(i)$. Therefore, Hoeffding's inequality (Fact 2.2) yields that

$$\begin{aligned}
\Pr[Z_i \geq -y] &= \Pr[Z_i - \varepsilon \cdot \mathsf{sum}_m(i) \geq -(y + \varepsilon \cdot \mathsf{sum}_m(i))] \\
&\leq \Pr\left[Z_i - \varepsilon \cdot \mathsf{sum}_m(i) \geq 4\sqrt{\log m \cdot \mathsf{sum}_m(i)}\right] \\
&\leq 2 \cdot \exp\left(-\frac{16 \cdot \mathsf{sum}_m(i) \log m}{2 \cdot \mathsf{sum}_m(i)}\right) \\
&< \frac{1}{m^2}.
\end{aligned}$$

□

We associate the following events with G. For $i \in [m]$, let E_i be the event that $Y_{i-1} \in \mathcal{Y}_{i-1}$ and for $i \in (m)$ let $L_i = E_1 \bigcap E_2 \bigcap \ldots \bigcap E_i \bigcap \neg E_{i+1}$, letting $E_{m+1} = \emptyset$. In words, E_i is the event that $|Y_{i-1}|$ is not large, and L_i is the event that i is the minimal index such that $|Y_i|$ is large (where L_m is the event that all the Y_i's are not large). Note that $\{L_j\}_{j \in (m)}$ are disjoint events and that $\Pr\left[\bigcup_{j \in (m)} L_j\right] = 1$. We use the following fact.

Claim 4.12. *For integer $i \in [\frac{m}{2}, m]$, it holds that $\Pr[E_i] \leq \frac{12 \cdot \ell_m(i)\sqrt{\log m}}{m}$.*

40

Proof. Note that Y_{i-1} is the outcome of $\mathsf{sum}_m(1) - \mathsf{sum}_m(i)$ coins. Compute

$$\mathsf{sum}_m(1) - \mathsf{sum}_m(i) = \frac{1}{2} \left(\ell_m(1)(\ell_m(1) + 1) - \ell_m(i)(\ell_m(i) + 1) \right) \tag{16}$$

$$= \frac{1}{2} \left(m(m+1) - (m - i + 1)(m - i + 2) \right)$$

$$\geq \frac{1}{2} \left(m(m+1) - (\frac{m}{2} + 1)(\frac{m}{2} + 2) \right)$$

$$\geq \frac{m^2}{4}.$$

Proposition 2.4 yields that the probability Y_{i-1} equals a given value in $\mathcal{Y}_{i-1}$ is at most $\frac{1}{\sqrt{(\mathsf{sum}_m(1) - \mathsf{sum}_m(i))}} \leq \frac{2}{m}$ (recall that we only care about large enough m). Since $|\mathcal{Y}_{i-1}| < 8\sqrt{\mathsf{sum}_m(i) \log m}$, it follows that

$$\Pr[E_i] \leq 8\sqrt{\mathsf{sum}_m(i) \log m} \cdot \frac{2}{m}$$

$$= \frac{16\sqrt{\mathsf{sum}_m(i) \log m}}{m}$$

$$= \frac{16\sqrt{\frac{1}{2} \cdot \ell_m(i)(\ell_m(i) + 1) \log m}}{m}$$

$$\leq \frac{12 \cdot \ell_m(i)\sqrt{\log m}}{m}.$$

$\square$

The following claim bounds the sum $\sum_{j=i}^{m} \Pr[L_j]$ for every integer $i \in [\frac{m}{2}, m]$.

Claim 4.13. *For integer $i \in [\frac{m}{2}, m]$, it holds that $\sum_{j=i}^{m} \Pr[L_j] \leq \frac{12 \cdot \ell_m(i)\sqrt{\log m}}{m}$.*

Proof. Since $\{L_j\}_{j=0}^{m}$ are disjoint events and since $\bigcup_{j=i}^{m} L_j \subseteq E_i$, it follows that

$$\sum_{j=i}^{m} \Pr[L_j] = \Pr[\bigcup_{j=i}^{m} L_i] \leq \Pr[E_i] \leq \frac{12 \cdot \ell_m(i)\sqrt{\log m}}{m},$$

where the last inequality holds by Claim 4.12. $\square$

Putting it together.

Proof of Lemma 4.7. Let B be an algorithm and let B' be the algorithm that operates like B with the following difference: if B aborts (i.e., output 1) at round i, and $i > m - \log^{2.5} m$ or $i \geq i'$, for i' being the minimal index with $\overline{E_{i'}}$, then B' does not abort, and outputs 0's till the end of the game. Combining Claims 4.11 and 4.12 and Lemma 4.4 yields that

$$|\mathsf{Bias}_{\mathsf{B}}(\mathsf{G}) - \mathsf{Bias}_{\mathsf{B}'}(\mathsf{G})| \leq \frac{1}{m} + \frac{12 \cdot \log^3 m}{m} \tag{17}$$

Let B'' be the strategy that acts like B', but does not abort (even if B' does) in rounds $\{i, \ldots, m\}$, for i being the minimal index with $H_i \notin \widehat{\mathcal{H}}_{i, Y_{i-1}}$ and let $I'' = I(\mathsf{G}, \mathsf{B}'')$ be according to Definition 4.2.

Since we assume that $\Pr\left[H_i \notin \widehat{\mathcal{H}}_{i,y} \mid Y_{i-1} = y\right] \leq \frac{3}{m^2}$ for every $i \in [m - \lfloor \log^{2.5} m \rfloor]$ and $y \in \mathcal{Y}_{i-1}$, a simple averaging argument yields that

$$|\mathsf{Bias}_{\mathsf{B}'}(\mathsf{G}) - \mathsf{Bias}_{\mathsf{B}''}(\mathsf{G})| \leq \Pr\left[\exists i \in [m - \lfloor \log^{2.5} m \rfloor]: Y_{i-1} \in \mathcal{Y}_{i-1} \wedge H_i \notin \widehat{\mathcal{H}}_{i,Y_{i-1}}\right] \leq \frac{3}{m}. \quad (18)$$

Let $J \in (m)$ be the index for which L_J happens (i.e., J is the minimal index such that $Y_J \notin \mathcal{Y}_J$). The definition of B'' yields that $I'' \leq J$, $I'' \leq m - \log^{2.5} m$, $Y_{I''-1} \in \mathcal{Y}_{I''-1}$ and $H_{I''} \in \widehat{\mathcal{H}}_{I'',Y_{I''-1}}$. Since, by assumption, $|\mathsf{o}_i(y) - \mathsf{o}_i(y,h)| \leq \lambda \cdot \frac{\sqrt{\log m}}{\ell_m(i+1)}$ for every $i \in [m - \lfloor \log^{2.5} m \rfloor]$, $y \in \mathcal{Y}_{i-1}$ and $h \in \widehat{\mathcal{H}}_{i,y}$, it follows that

$$\left|O_{I''}^- - O_{I''}\right| = |\mathsf{o}_{I''}(Y_{I''-1}) - \mathsf{o}_{I''}(Y_{I''-1}, H_{I''})| \leq \lambda \cdot \frac{\sqrt{\log m}}{\ell_m(I'' + 1)} \leq \lambda \cdot \frac{\sqrt{\log m}}{\ell_m(J + 1)}. \quad (19)$$

We conclude that

$$
\begin{aligned}
\mathsf{Bias}_{\mathsf{B}''}(\mathsf{G}) &= \left|\mathop{\mathrm{E}}_{i \leftarrow I''}\left[O_i^- - O_i\right]\right| \quad &(20)\\
&\leq \mathop{\mathrm{E}}_{i \leftarrow I''}\left[\left|O_i^- - O_i\right|\right] \\
&\leq \sum_{i=0}^{m-1} \Pr[L_i] \cdot \frac{\lambda \cdot \sqrt{\log m}}{\ell_m(i+1)} \\
&\leq \lambda \cdot \sqrt{\log m} \cdot \left(\sum_{i=0}^{\lceil \frac{m}{2} \rceil - 1} \frac{\Pr[L_i]}{\ell_m(i+1)} + \sum_{i=\lceil \frac{m}{2} \rceil}^{m-1} \frac{\Pr[L_i]}{\ell_m(i+1)}\right) \\
&\leq \lambda \cdot \sqrt{\log m} \cdot \left(\frac{1}{\ell_m(\lceil \frac{m}{2} \rceil)} + \frac{12 \cdot \sqrt{\log m}}{m} \cdot \sum_{i=\lceil \frac{m}{2} \rceil}^{m-1} \frac{1}{\ell_m(i+1)}\right) \\
&\leq \lambda \cdot \sqrt{\log m} \cdot \left(\frac{2}{m} + \frac{12 \cdot \sqrt{\log m}}{m} \cdot \sum_{i=\lceil \frac{m}{2} \rceil}^{m-1} \frac{1}{m-i}\right) \\
&\leq \lambda \cdot \sqrt{\log m} \cdot \left(\frac{2}{m} + \frac{12 \cdot \log^{1.5} m}{m}\right) \\
&\leq 13\lambda \cdot \frac{\log^2 m}{m}.
\end{aligned}
$$

The fourth inequality holds by Claim 4.13 and Proposition 2.1, and the one before last inequality holds since $\sum_{i=1}^{\lfloor \frac{m}{2} \rfloor} \frac{1}{i} \leq \log m$. Hence, $\mathsf{Bias}(\mathsf{G}) \leq 13\lambda \cdot \frac{\log^2 m}{m} + \frac{4}{m} + \frac{12 \cdot \log^3 m}{m} \leq (13\lambda + 13)\frac{\log^3 m}{m}$. $\quad\square$

4.2.2 Proving Lemma 4.8

The following claim states a more convenient, yet equivalent, expression for the ratio function.

Claim 4.14. *For $x \in \mathcal{X}_i$, $y \in \mathrm{Supp}(Y_{i-1})$ and $h \in \mathrm{Supp}(H_i \mid Y_{i-1} = y, X_i \in \mathcal{X}_i)$, it holds that*

$$\mathsf{ratio}_{i,y,h}(x) = \frac{\Pr[H_i = h \mid Y_{i-1} = y, X_i = x]}{\Pr[H_i = h \mid Y_{i-1} = y, X_i \in \mathcal{X}_i]}.$$

Proof. A simple calculation yields that

$$\frac{\Pr\left[H_i = h \mid Y_{i-1} = y, X_i = x\right]}{\Pr\left[H_i = h \mid Y_{i-1} = y, X_i \in \mathcal{X}_i\right]} = \frac{\Pr\left[X_i = x \mid Y_{i-1} = y, H_i = h\right]}{\Pr\left[X_i = x \mid Y_{i-1} = y\right]} \cdot \frac{\Pr\left[X_i \in \mathcal{X}_i \mid Y_{i-1} = y\right]}{\Pr\left[X_i \in \mathcal{X}_i \mid Y_{i-1} = y, H_i = h\right]} \tag{21}$$

Since $x \in \mathcal{X}_i$, it follows that

$$\Pr\left[X_i = x \mid Y_{i-1} = y, X_i \in \mathcal{X}_i\right] = \frac{\Pr\left[X_i = x \mid Y_{i-1} = y\right]}{\Pr\left[X_i \in \mathcal{X}_i \mid Y_{i-1} = y\right]} \tag{22}$$

and

$$\Pr\left[X_i = x \mid Y_{i-1} = y, X_i \in \mathcal{X}_i, H_i = h\right] = \frac{\Pr\left[X_i = x \mid Y_{i-1} = y, H_i = h\right]}{\Pr\left[X_i \in \mathcal{X}_i \mid Y_{i-1} = y, H_i = h\right]} \tag{23}$$

We conclude that

$$\frac{\Pr\left[H_i = h \mid Y_{i-1} = y, X_i = x\right]}{\Pr\left[H_i = h \mid Y_{i-1} = y, X_i \in \mathcal{X}_i\right]} = \frac{\Pr\left[X_i = x \mid Y_{i-1} = y, X_i \in \mathcal{X}_i\right]}{\Pr\left[X_i = x \mid Y_{i-1} = y, X_i \in \mathcal{X}_i, H_i = h\right]} = \mathsf{ratio}_{i,y,h}(x).$$

$\square$

We now ready to prove Lemma 4.8.

Proof of Lemma 4.8. Let $p = \Pr[X_i \in \mathcal{X}_i] = 1 - q$ and $p_h = \Pr[X_i \in \mathcal{X}_i \mid Y_{i-1} = y, H_i = h] = 1 - q_h$. Then,

$$\begin{aligned}
\mathsf{o}_i(y) &= \Pr[Y_m \geq 0 \mid Y_{i-1} = y] \tag{24}\\
&= p \cdot \Pr[Y_m \geq 0 \mid Y_{i-1} = y, X_i \in \mathcal{X}_i] + q \cdot \Pr[Y_m \geq 0 \mid Y_{i-1} = y, X_i \notin \mathcal{X}_i]\\
&= p \cdot \mathop{\mathrm{E}}_{x \leftarrow X_i \mid x \in \mathcal{X}_i} [\Pr[Y_m \geq 0 \mid Y_{i-1} = y, X_i = x]] + q \cdot p',\\
&= p \cdot \mathop{\mathrm{E}}_{x \leftarrow X_i \mid x \in \mathcal{X}_i} [\mathsf{o}_{i+1}(y + x)] + q \cdot p',\\
&= p_h \cdot \mathop{\mathrm{E}}_{x \leftarrow X_i \mid x \in \mathcal{X}_i} [\mathsf{o}_{i+1}(y + x)] + (p - p_h) \cdot \mathop{\mathrm{E}}_{x \leftarrow X_i \mid x \in \mathcal{X}_i} [\mathsf{o}_{i+1}(y + x)] + q \cdot p',
\end{aligned}$$

for $p' = \Pr[Y_m \geq 0 \mid Y_{i-1} = y, X_i \notin \mathcal{X}_i]$. In addition,

$$\begin{aligned}
\mathsf{o}_i(y, h) &= \Pr[Y_m \geq 0 \mid Y_{i-1} = y, H_i = h] \tag{25}\\
&= p_h \cdot \Pr[Y_m \geq 0 \mid Y_{i-1} = y, H_i = h, X_i \in \mathcal{X}_i] + q_h \cdot \Pr[Y_m \geq 0 \mid Y_{i-1} = y, H_i = h, X_i \notin \mathcal{X}_i]\\
&= p_h \cdot \frac{\Pr[Y_m \geq 0 \wedge H_i = h \mid Y_{i-1} = y, X_i \in \mathcal{X}_i]}{\Pr[H_i = h \mid Y_{i-1} = y, X_i \in \mathcal{X}_i]} + q_h \cdot p''\\
&= p_h \cdot \frac{\mathrm{E}_{x \leftarrow X_i \mid x \in \mathcal{X}_i} [\Pr[Y_m \geq 0 \wedge H_i = h \mid Y_{i-1} = y, X_i = x]]}{\Pr[H_i = h \mid Y_{i-1} = y, X_i \in \mathcal{X}_i]} + q_h \cdot p''\\
&= p_h \cdot \frac{\mathrm{E}_{x \leftarrow X_i \mid x \in \mathcal{X}_i} [\Pr[Y_m \geq 0 \mid Y_{i-1} = y, X_i = x] \cdot \Pr[H_i = h \mid Y_{i-1} = y, X_i = x]]}{\Pr[H_i = h \mid Y_{i-1} = y, X_i \in \mathcal{X}_i]} + q_h \cdot p''\\
&= p_h \cdot \mathop{\mathrm{E}}_{x \leftarrow X_i \mid x \in \mathcal{X}_i} \left[\mathsf{o}_{i+1}(y + x) \cdot \frac{\Pr[H_i = h \mid Y_{i-1} = y, X_i = x]}{\Pr[H_i = h \mid Y_{i-1} = y, X_i \in \mathcal{X}_i]}\right] + q_h \cdot p''\\
&= p_h \cdot \mathop{\mathrm{E}}_{x \leftarrow X_i \mid x \in \mathcal{X}_i} [\mathsf{o}_{i+1}(y + x) \cdot \mathsf{ratio}_{i,y,h}(x)] + q_h \cdot p'',
\end{aligned}$$

43

for $p'' = \Pr[Y_m \geq 0 \mid Y_{i-1} = y, H_i = h, X_i \notin \mathcal{X}_i]$, where the last equality holds by Claim 4.14. Combing Equations (24) and (25) yields that

$$|\mathsf{o}_i(y) - \mathsf{o}_i(y,h)|$$

$$\leq p_h \cdot \left| \operatorname*{E}_{x \leftarrow X_i | x \in \mathcal{X}_i} [\mathsf{o}_{i+1}(y+x) \cdot (1 - \mathsf{ratio}_{i,y,h}(x))] \right| + |p - p_h| + q + q_h$$

$$\leq \left| \operatorname*{E}_{x \leftarrow X_i | x \in \mathcal{X}_i} [(\mathsf{o}_{i+1}(y+x) - \mathsf{o}_{i+1}(y)) \cdot (1 - \mathsf{ratio}_{i,y,h}(x))] \right| + |q - q_h| + q + q_h$$

$$\leq \operatorname*{E}_{x \leftarrow X_i | x \in \mathcal{X}_i} [|\mathsf{o}_{i+1}(y+x) - \mathsf{o}_{i+1}(y)| \cdot |1 - \mathsf{ratio}_{i,y,h}(x)|] + 2 \cdot (q + q_h),$$

where the second inequality holds since

$$\left| \operatorname*{E}_{x \leftarrow X_i | x \in \mathcal{X}_i} [\mathsf{o}_{i+1}(y+x) \cdot (1 - \mathsf{ratio}_{i,y,h}(x))] \right|$$

$$\leq \left| \operatorname*{E}_{x \leftarrow X_i | x \in \mathcal{X}_i} [(\mathsf{o}_{i+1}(y) + \mathsf{o}_{i+1}(y+x) - \mathsf{o}_{i+1}(y)) \cdot (1 - \mathsf{ratio}_{i,y,h}(x))] \right|$$

$$\leq \left| \operatorname*{E}_{x \leftarrow X_i | x \in \mathcal{X}_i} [\mathsf{o}_{i+1}(y) \cdot (1 - \mathsf{ratio}_{i,y,h}(x))] \right| + \left| \operatorname*{E}_{x \leftarrow X_i | x \in \mathcal{X}_i} [(\mathsf{o}_{i+1}(y+x) - \mathsf{o}_{i+1}(y)) \cdot (1 - \mathsf{ratio}_{i,y,h}(x))] \right|$$

$$= \left| \mathsf{o}_{i+1}(y) \cdot (1 - \operatorname*{E}_{x \leftarrow X_i | x \in \mathcal{X}_i} [\mathsf{ratio}_{i,y,h}(x)]) \right| + \left| \operatorname*{E}_{x \leftarrow X_i | x \in \mathcal{X}_i} [(\mathsf{o}_{i+1}(y+x) - \mathsf{o}_{i+1}(y)) \cdot (1 - \mathsf{ratio}_{i,y,h}(x))] \right|$$

$$= \left| \operatorname*{E}_{x \leftarrow X_i | x \in \mathcal{X}_i} [\mathsf{o}_{i+1}(y) \cdot (1 - 1)] \right| + \left| \operatorname*{E}_{x \leftarrow X_i | x \in \mathcal{X}_i} [(\mathsf{o}_{i+1}(y+x) - \mathsf{o}_{i+1}(y)) \cdot (1 - \mathsf{ratio}_{i,y,h}(x))] \right|$$

$$= \left| \operatorname*{E}_{x \leftarrow X_i | x \in \mathcal{X}_i} [(\mathsf{o}_{i+1}(y+x) - \mathsf{o}_{i+1}(y)) \cdot (1 - \mathsf{ratio}_{i,y,h}(x))] \right|.$$

$\square$

4.3 Bounding the Simple Binomial Game

In this section we prove Lemma 3.9 restated below.

Definition 4.15 (simple game – Restatement of Definition 3.8). *For $m \in \mathbb{N}$, $\varepsilon \in [-1, 1]$ and a randomized function f, the game $\mathsf{G}_{f,m,\varepsilon}$ is called "simple game" if f on input (i, y) outputs 1 with probability $\mathsf{o}_{i+1}(y)$ $(= \widehat{\mathcal{C}}_{\mathsf{sum}_m(i+1),\varepsilon}(-y))$, and zero otherwise.*

Lemma 4.16 (Restatement of Lemma 3.9). *Let $m \in \mathbb{N}$, let $\varepsilon \in [-1, 1]$ and let f be the randomized function such that $\mathsf{G}_{f,m,\varepsilon}$ is a simple game according to Definition 4.15. Then $\mathsf{Bias}(\mathsf{G}_{f,m,\varepsilon}) \leq \frac{\xi \cdot \log^3 m}{m}$, for some universal constant ξ.*

Proof. We view the function f as the composition $g \circ \tau$, where $\tau(i, y)$ outputs $y + t$, for $t \leftarrow \mathcal{C}_{\mathsf{sum}_m(i+1),\varepsilon}$, and $g(y + t)$ outputs 1 if $y + t \geq 0$, and zero otherwise. Using Lemma 4.3, for bounding the value of $\mathsf{G}_{f,m,\varepsilon}$ it suffices to bound that of $\mathsf{G}_{\tau,m,\varepsilon}$. We would also like to assume that $|\varepsilon| \leq 4\sqrt{\frac{\log m}{\mathsf{sum}_m(1)}}$. Indeed, if this is not the case, then $O_1^- \notin [\frac{1}{m^2}, 1 - \frac{1}{m^2}]$, and the proof follows by Lemma 4.4. Therefore, in the following we assume that $|\varepsilon| \leq 4\sqrt{\frac{\log m}{\mathsf{sum}_m(1)}}$.

In the following, we fix $i \in [m - \lfloor \log^{2.5} m \rfloor]$ and $y \in \mathcal{Y}_{i-1}$, where $\mathcal{Y}_{i-1}$ is according to Lemma 4.6. Let

$$\mathcal{H}_{i,y} = \{ h \in \mathbb{Z} \colon |h - y| \leq 8 \cdot \sqrt{\log m \cdot \mathsf{sum}_m(i)} \}, \tag{26}$$

Since $(H_i - y)$ is distributed according to $\mathcal{C}_{\mathsf{sum}_m(i),\varepsilon}$ (given that $Y_{i-1} = y$) and since $|\varepsilon \cdot \mathsf{sum}_m(i)| \leq 4 \cdot \sqrt{\log m \cdot \mathsf{sum}_m(i)}$, Hoeffding's inequality yields that

$$
\begin{aligned}
\Pr\left[H_i \notin \mathcal{H}_{i,y} \mid Y_{i-1} = y\right] &= \Pr\left[|H_i - y| > 8 \cdot \sqrt{\log m \cdot \mathsf{sum}_m(i)} \mid Y_{i-1} = y\right] \tag{27} \\
&\leq \Pr\left[|(H_i - y) - \varepsilon \cdot \mathsf{sum}_m(i)| > 4 \cdot \sqrt{\log m \cdot \mathsf{sum}_m(i)} \mid Y_{i-1} = y\right] \\
&\leq 2 \cdot \exp\left(-\frac{16 \cdot \mathsf{sum}_m(i)\log m}{2 \cdot \mathsf{sum}_m(i)}\right) \\
&\leq \frac{1}{m^2}.
\end{aligned}
$$

Fix $h = y + t \in \mathcal{H}'_{i,y} := \mathcal{H}_{i,y} \bigcap \mathrm{Supp}(H_i \mid Y_{i-1} = y, X_i \in \mathcal{X}_i)$, and let $t_0 = t - \varepsilon \cdot \mathsf{sum}_m(i)$. Note that $|t_0| = |t - \varepsilon \cdot \mathsf{sum}_m(i)| = |h - y - \varepsilon \cdot \mathsf{sum}_m(i)| \leq |h - y| + |\varepsilon \cdot \mathsf{sum}_m(i)| \leq 12\sqrt{\mathsf{sum}_m(i)\log m}$. In addition, note that since $y + t \in \mathcal{H}'_{i,y}$, there exists $x_0 \in \mathcal{X}_i$ such that $t - x_0 \in \mathrm{Supp}(\mathcal{C}_{\mathsf{sum}_m(i+1),\varepsilon})$, where $\mathcal{X}_i$ is according to Definition 4.5. Therefore, we can deduce that $t - x \in \mathrm{Supp}(\mathcal{C}_{\mathsf{sum}_m(i+1),\varepsilon})$ for every $x \in \mathcal{X}_i$. The latter holds since $|t - x| \leq |t| + |x| < (8 + 4) \cdot \sqrt{\log m \cdot \mathsf{sum}_m(i)} < \mathsf{sum}_m(i+1)$ (recalling that $i \in [m - \lfloor \log^{2.5} m \rfloor]$ for large m) and since x has the same parity as x_0 (all the elements of $\mathcal{X}_i$ has the same parity since $\mathcal{X}_i \subseteq \mathrm{Supp}(X_i)$).

Fix $x \in \mathcal{X}_i$ and compute

$$
\begin{aligned}
\frac{1}{\mathsf{ratio}_{i,y,h}(x)} &= \frac{\Pr[H_i = y + t \mid Y_{i-1} = y, X_i \in \mathcal{X}_i]}{\Pr[H_i = y + t \mid Y_{i-1} = y, X_i = x]} \tag{28} \\
&= \mathop{\mathrm{E}}_{x' \leftarrow X_i \mid x' \in \mathcal{X}_i}\left[\frac{\mathcal{C}_{\mathsf{sum}_m(i+1),\varepsilon}(t - x')}{\mathcal{C}_{\mathsf{sum}_m(i+1),\varepsilon}(t - x)}\right] \\
&\in \mathop{\mathrm{E}}_{x' \leftarrow X_i \mid x' \in \mathcal{X}_i}\left[\exp\left(\frac{-2 \cdot t_0 \cdot x + x^2 + 2 \cdot t_0 \cdot x' - x'^2}{2 \cdot \mathsf{sum}_m(i+1)}\right)\right] \cdot \left(1 \pm \xi_1 \cdot \frac{\log^{1.5} m}{\sqrt{\mathsf{sum}_m(i+1)}}\right) \\
&\subseteq \left(1 \pm \xi_2 \cdot \sqrt{\frac{\log m}{\ell_m(i+1)}}\left(1 + \frac{|x|}{\sqrt{\ell_m(i)}}\right)\right) \cdot \left(1 \pm \xi_1 \cdot \frac{\log^{1.5} m}{\sqrt{\mathsf{sum}_m(i+1)}}\right) \\
&\subseteq 1 \pm \xi_3 \cdot \sqrt{\frac{\log m}{\ell_m(i+1)}}\left(1 + \frac{|x|}{\sqrt{\ell_m(i)}}\right),
\end{aligned}
$$

for some constants $\xi_1, \xi_2, \xi_3 \in \mathbb{R}^+$ (independent of the game). The first transition holds by Claim 4.14, the third one by Proposition 2.5, and the fourth one by Proposition 2.8.

Recalling that $i \leq m - \log^{2.5} m$, it follows that

$$\xi_3 \cdot \sqrt{\frac{\log m}{\ell_m(i+1)}} \cdot \left(1 + \frac{|x|}{\sqrt{\ell_m(i)}}\right) \in O\left(\frac{\log m}{\sqrt{\ell_m(i+1)}}\right) \in o(1) \tag{29}$$

Since $\frac{1}{1\pm z} \subseteq 1 \pm 2z$ for every $z \in (-0.5, 0.5)$, we deduce from Equation (28) that

$$\mathsf{ratio}_{i,y,h}(x) \in 1 \pm 2\xi_3 \cdot \sqrt{\frac{\log m}{\ell_m(i+1)}} \cdot \left(1 + \frac{|x|}{\sqrt{\ell_m(i)}}\right) \tag{30}$$

and thus

$$|1 - \mathsf{ratio}_{i,y,h}(x)| \leq 2\xi_3 \cdot \sqrt{\frac{\log m}{\ell_m(i+1)}} \cdot \left(1 + \frac{|x|}{\sqrt{\ell_m(i)}}\right) \tag{31}$$

Finally, since the above holds for every $i \leq m - \log^{2.5} m$, $y \in \mathcal{Y}_{i-1}$, $h \in \mathcal{H}_{i,y}$ and $x \in \mathcal{X}_i$, and recalling Equation (27), we can apply Lemma 4.6 to get that $\mathsf{Bias}(\mathsf{G}_{\tau,m,\varepsilon}) \leq \xi \cdot \frac{\log^3 m}{m}$, for some universal constant $\xi > 0$. $\qquad\square$

4.4 Bounding the Hypergeometric Binomial Game

In this section we prove Lemma 3.11 restated below. 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 $w(v) = p$ (recall that $w(v) = \sum_{j \in [|v|]} v[j]$ and that $v_{\mathcal{I}} = (v_{j_1}, \ldots, v_{j_{|\mathcal{I}|}})$ where $j_1, \ldots, j_{|\mathcal{I}|}$ are the ordered elements of $\mathcal{I}$) and recall that $\widehat{\mathcal{HG}}_{n,p,\ell}(k) := \Pr_{x \leftarrow \mathcal{HG}_{n,p,\ell}}[x \geq k] = \sum_{t=k}^{\ell} \mathcal{HG}_{n,p,\ell}(t)$.

Definition 4.17 (hypergeometric game – Restatement of Definition 3.10). *For $m \in \mathbb{N}$, $\varepsilon \in [-1, 1]$, $\lambda > 0$ and a randomized function f, the game $\mathsf{G}_{f,m,\varepsilon}$ is called "λ-hypergeometric game" if there exists $p \in [-m, m]$, with $|p| \leq \lambda \cdot \sqrt{\log m \cdot \mathsf{sum}_m(1)}$, such that f on input (i, y) outputs 1 with probability $\widehat{\mathcal{HG}}_{2 \cdot \mathsf{sum}_m(1), p, \mathsf{sum}_m(i+1)}(-y)$ and zero otherwise.*

Lemma 4.18 (Restatement of Lemma 3.11). *Let $m \in \mathbb{N}$, let $\varepsilon \in [-1, 1]$, let $\lambda > 0$ and let f be a randomized function such that $\mathsf{G}_{f,m,\varepsilon}$ is an λ-hypergeometric game according to Definition 4.17. Then $\mathsf{Bias}(\mathsf{G}_{f,m,\varepsilon}) \leq \frac{\varphi(\lambda) \cdot \log^3 m}{m}$ for some universal function φ.*

Proof. We view the function f as $g \circ \tau$, for $\tau(i, y)$ being the output of the following process. A random subset $\mathcal{I}$ of size $2 \cdot \mathsf{sum}_m(i+1)$ is uniformly chosen from $[2 \cdot \mathsf{sum}_m(1)]$, where the output of τ is set to $(w(v_{\mathcal{I}}), y+t)$, for $v \in \{-1, 1\}^{2 \cdot \mathsf{sum}_m(1)}$ with $w(v) = p$ and for $t \leftarrow \mathcal{HG}_{2\mathsf{sum}_m(i+1), w(v, \mathcal{I}), \mathsf{sum}_m(i+1)}$. The function g on input (p', y') outputs one if $y' \geq 0$, and zero otherwise. Since $\Pr[g \circ \tau(i, y) = 1] = \Pr[f(i, y) = 1]$, by Lemma 4.3 it suffices to bound the bias of the game $\mathsf{G}_{\tau,m,\varepsilon}$. In addition, as in the proof of Lemma 4.16, we can assume without loss of generality that $|\varepsilon| \leq 4\sqrt{\frac{\log m}{\mathsf{sum}_m(1)}}$. Fix $i \in [m - \lfloor \log^{2.5} m \rfloor]$ and $y \in \mathcal{Y}_{i-1}$, where $\mathcal{Y}_{i-1}$ is according to Lemma 4.6. Let

$$\mathcal{H}_{i,y} = \{(p', y') \in \mathbb{Z}^2 \colon |p'|, |y' - y| \leq (\lambda + 8)\sqrt{\log m \cdot \mathsf{sum}_m(i+1)}\},$$

Since $H_i = (p', y+t)$ for $p' \leftarrow \mathcal{HG}_{2\mathsf{sum}_m(1), p, 2\mathsf{sum}_m(i+1)}$ and $t \leftarrow \mathcal{C}_{\ell_m(i), \varepsilon} + \mathcal{HG}_{2\mathsf{sum}_m(i+1), p', \mathsf{sum}_m(i+1)}$

(given that $Y_{i-1} = y$), it follows that

$$\Pr\left[|H_i[0]| > (\lambda + 8)\sqrt{\log m \cdot \mathsf{sum}_m(i+1)}\right]$$

$$\leq \Pr\left[\left|H_i[0] - \frac{p \cdot \mathsf{sum}_m(i+1)}{\mathsf{sum}_m(1)}\right| > 8\sqrt{\log m \cdot \mathsf{sum}_m(i+1)}\right]$$

$$\leq \exp\left(-\frac{64 \cdot \mathsf{sum}_m(i+1)\log m}{2 \cdot \mathsf{sum}_m(i+1)}\right)$$

$$\leq \frac{1}{m^4},$$

where the second inequality holds by Hoeffding's inequality for hypergeometric distribution (Fact 2.9). In addition, given that $H_i[0] = p'$ for $|p'| \leq (\lambda + 8)\sqrt{\log m \cdot \mathsf{sum}_m(i+1)}$, it holds that $\left(H_i[1] - (y + X_i)\right)$ is distributed according to $\mathcal{HG}_{2\mathsf{sum}_m(i+1),p',\mathsf{sum}_m(i+1)}$. This yields that

$$\Pr\left[|H_i[1] - y| > (\lambda + 8)\sqrt{\log m \cdot \mathsf{sum}_m(i+1)} \mid Y_{i-1} = y\right]$$

$$\leq \Pr\left[|H_i[1] - (y + X_i)| > (\lambda + 7)\sqrt{\log m \cdot \mathsf{sum}_m(i+1)} \mid Y_{i-1} = y\right]$$

$$\leq \Pr\left[\left|(H_i[1] - (y + X_i)) - \frac{p'}{2}\right| > 3\sqrt{\log m \cdot \mathsf{sum}_m(i+1)} \mid Y_{i-1} = y\right]$$

$$\leq \exp\left(-\frac{9 \cdot \mathsf{sum}_m(i+1)\log m}{2 \cdot \mathsf{sum}_m(i+1)}\right)$$

$$\leq \frac{1}{m^4}.$$

The first inequality holds since $|X_i| \leq \ell_m(i) < \sqrt{\log m \cdot \mathsf{sum}_m(i+1)}$, the second one holds since $\frac{|p'|}{2} < \frac{\lambda+8}{2}\sqrt{\log m \cdot \mathsf{sum}_m(i+1)}$, and the third one by Hoeffding's inequality for hypergeometric distribution (Fact 2.9). It follows that

$$\Pr\left[H_i \notin \mathcal{H}_{i,y} \mid Y_{i-1} = y\right] \leq \frac{1}{m^4} + \frac{1}{m^4} < \frac{1}{m^2} \tag{32}$$

Fix $h = (p', y + t) \in \mathcal{H}'_{i,y} := \mathcal{H}_{i,y} \bigcap \mathrm{Supp}(H_i \mid Y_{i-1} = y, X_i \in \mathcal{X}_i)$, where $\mathcal{X}_i$ is according to Definition 4.5. Note that by the same arguments introduced in the analogous case in Section 4.3, it holds that $t - x \in \mathrm{Supp}(\mathcal{HG}_{2\mathsf{sum}_m(i+1),p',\mathsf{sum}_m(i+1)})$ for every $x \in \mathcal{X}_i$.

Fix $x \in \mathcal{X}_i$ and compute

$$\frac{1}{\mathsf{ratio}_{i,y,h}(x)} = \frac{\Pr[H_i = (p', y + t) \mid Y_{i-1} = y, X_i \in \mathcal{X}_i]}{\Pr[H_i = (p', y + t) \mid Y_{i-1} = y, X_i = x]} \tag{33}$$

$$= \mathop{\mathrm{E}}_{x' \leftarrow X_i \mid x' \in \mathcal{X}_i}\left[\frac{\mathcal{HG}_{2\mathsf{sum}_m(i+1),p',\mathsf{sum}_m(i+1)}(t - x')}{\mathcal{HG}_{2\mathsf{sum}_m(i+1),p',\mathsf{sum}_m(i+1)}(t - x)}\right]$$

$$\in \mathop{\mathrm{E}}_{x' \leftarrow X_i \mid x' \in \mathcal{X}_i}\left[\exp\left(\frac{-2(t - \frac{p'}{2})x + x^2 + 2(t - \frac{p'}{2})x' - x'^2}{\mathsf{sum}_m(i+1)}\right)\right] \cdot \left(1 \pm \varphi_1(\lambda) \cdot \frac{\log^{1.5} m}{\sqrt{\mathsf{sum}_m(i+1)}}\right)$$

$$\subseteq \left(1 \pm \varphi_2(\lambda)\sqrt{\frac{\log m}{\ell_m(i+1)}}\left(1 + \frac{|x|}{\sqrt{\ell_m(i)}}\right)\right) \cdot \left(1 \pm \varphi_1(\lambda) \cdot \frac{\log^{1.5} m}{\sqrt{\mathsf{sum}_m(i+1)}}\right)$$

$$\subseteq 1 \pm \varphi_3(\lambda)\sqrt{\frac{\log m}{\ell_m(i+1)}}\left(1 + \frac{|x|}{\sqrt{\ell_m(i)}}\right),$$

47

for some functions $\varphi_1, \varphi_2, \varphi_3 \colon \mathbb{R}^+ \mapsto \mathbb{R}^+$ (independent of the game). The first transition holds by Claim 4.14, the third one by Proposition 2.11 and the fourth one by Proposition 2.8.

Recalling that $i \leq m - \log^{2.5} m$, it follows that

$$\varphi_3(\lambda) \cdot \sqrt{\frac{\log m}{\ell_m(i+1)}} \cdot \left(1 + \frac{|x|}{\sqrt{\ell_m(i)}}\right) \in o(1) \tag{34}$$

Since $\frac{1}{1 \pm z} \subseteq 1 \pm 2z$ for every $z \in (-0.5, 0.5)$, we deduce from Equation (33) that

$$\mathsf{ratio}_{i,y,h}(x) \in 1 \pm 2\varphi_3(\lambda) \sqrt{\frac{\log m}{\ell_m(i+1)}} \cdot \left(1 + \frac{|x|}{\sqrt{\ell_m(i)}}\right) \tag{35}$$

and thus

$$|1 - \mathsf{ratio}_{i,y,h}(x)| \leq 2\varphi_3(\lambda) \sqrt{\frac{\log m}{\ell_m(i+1)}} \cdot \left(1 + \frac{|x|}{\sqrt{\ell_m(i)}}\right) \tag{36}$$

Finally, since the above holds for every $i \leq m - \log^{2.5} m$, $y \in \mathcal{Y}_{i-1}$, $h \in \mathcal{H}_{i,y}$ and $x \in \mathcal{X}_i$, and recalling Equation (32), we can apply Lemma 4.6 to get that $\mathsf{Bias}(\mathsf{G}_{\tau,m,\varepsilon}) \leq \varphi(\lambda) \cdot \frac{\log^3 m}{m}$, for some universal function $\varphi \colon \mathbb{R}^+ \mapsto \mathbb{R}^+$. $\qquad\square$

4.5 Bounding the Vector Binomial Game

In this section we prove Lemma 3.13 restated below. Recall that for $n \in \mathbb{N}$ and $\delta \in [0,1]$ we let $\widehat{\mathcal{C}}_n^{-1}(\delta)$ be the value $\varepsilon \in [-1,1]$ with $\widehat{\mathcal{C}}_{n,\varepsilon}(0) = \delta$.

Definition 4.19 (vector game – Restatement of Definition 3.12). *For $m \in \mathbb{N}$, $\varepsilon \in [-1,1]$, $\lambda \in \mathbb{N}$ and a randomized function f, the game $\mathsf{G}_{f,m,\varepsilon}$ is called "λ-vector game" if f on input (i, y) outputs a string in $\{-1,1\}^{\lambda \cdot \mathsf{sum}_m(1)}$, where each of entries takes the value 1 with probability $\widehat{\mathcal{C}}_{\mathsf{sum}_m(1)}^{-1}(\delta)$ for $\delta = \mathsf{o}_{i+1}(y) (= \widehat{\mathcal{C}}_{\mathsf{sum}_m(i+1),\varepsilon}(-y))$.*

Lemma 4.20 (Restatement of Lemma 3.13). *Let $m \in \mathbb{N}$, let $\lambda > 0$ and let f be a randomized function such that $\mathsf{G}_{f,m,\varepsilon=0}$ is an λ-vector game according to Definition 4.19. Then $\mathsf{Bias}(\mathsf{G}_{f,m,\varepsilon=0}) \leq \frac{\varphi(\lambda) \cdot \log^3 m}{m}$ for some universal function φ.*

Proof. For $i \in [m]$ and $y \in \mathbb{Z}$, let $\varepsilon_i(y) := \widehat{\mathcal{C}}_{\mathsf{sum}_m(1)}^{-1}(\mathsf{o}_{i+1}(y))$ (recall that $\mathsf{o}_{i+1}(y) = \widehat{\mathcal{C}}_{\mathsf{sum}_m(i+1),0}(-y)$) and let $q = \lambda \cdot \mathsf{sum}_m(1)$. Fix $i \in [m - \lfloor \log^{2.5} m \rfloor]$ and $y \in \mathcal{Y}_{i-1}$, where $\mathcal{Y}_{i-1}$ is according to Lemma 4.6. Note that

$$\Pr[f(i,y) = v] = 2^{-q} \cdot (1 + \varepsilon_i(y))^{\frac{q}{2} + \frac{w(v)}{2}} \cdot (1 - \varepsilon_i(y))^{\frac{q}{2} - \frac{w(v)}{2}} \tag{37}$$

for every $v \in \{-1,1\}^q$. Let

$$\mathcal{H}_{i,y} = \{v \in \{-1,1\}^q \colon |w(v)| \leq \sqrt{d \cdot \log m \cdot q}\}, \tag{38}$$

for $d = d(\lambda)$ to be determined by the analysis. In the following we let $s_i = \mathsf{sum}_m(i+1) \cdot \mathsf{sum}_m(1)$. Since m is large, Proposition 2.7 yields that $\varepsilon_i(y+x) \in \frac{y+x}{\sqrt{s_i}} \pm \frac{\log^2 m}{\sqrt{s_i}}$ for every $x \in \mathrm{Supp}(X_i)$.

48

Since $y \in \mathcal{Y}_{i-1}$, it follows that $|y| \leq 4\sqrt{\log m \cdot \mathsf{sum}_m(i)}$. Therefore, $\left|\frac{y+x}{\sqrt{s_i}}\right| \leq \frac{4\sqrt{\log m \cdot \mathsf{sum}_m(i)} + \ell_m(i)}{\sqrt{\mathsf{sum}_m(i+1)\cdot\mathsf{sum}_m(1)}} \leq \frac{5\sqrt{\log m \cdot \mathsf{sum}_m(i)}}{\sqrt{\mathsf{sum}_m(i+1)\cdot\mathsf{sum}_m(1)}} \leq \frac{6\sqrt{\log m}}{\sqrt{\mathsf{sum}_m(1)}} = \sqrt{\frac{36\lambda \cdot \log m}{q}}$, and thus, $|\varepsilon_i(y+x)| \leq (36\lambda + 1) \cdot \sqrt{\frac{\log m}{q}}$ for every $x \in \mathrm{Supp}(X_i)$. By setting $d = (5 + 72\lambda)^2$, Hoeffding's bound yields that the following holds for every $x \in \mathrm{Supp}(X_i)$.

$$
\begin{aligned}
&\Pr\left[H_i \notin \mathcal{H}_{i,y} \mid Y_i = y + x\right] \\
&= \Pr_{z \leftarrow \mathcal{C}_{q,\varepsilon_i(y+x)}}\left[|z| > \sqrt{d \cdot \log m \cdot q}\right] \\
&\leq \Pr_{z \leftarrow \mathcal{C}_{q,\varepsilon_i(y+x)}}\left[|z - 2q \cdot \varepsilon_i(y+x)| > \sqrt{d \cdot \log m \cdot q} - 2q \cdot \varepsilon_i(y+x)\right] \\
&\leq \Pr_{z \leftarrow \mathcal{C}_{q,\varepsilon_i(y+x)}}\left[|z - 2q \cdot \varepsilon_i(y+x)| > \sqrt{d \cdot \log m \cdot q} - 2 \cdot (36\lambda + 1) \cdot \sqrt{\log m \cdot q}\right] \\
&= \Pr_{z \leftarrow \mathcal{C}_{q,\varepsilon_i(y+x)}}\left[|z - 2q \cdot \varepsilon_i(y+x)| > 3 \cdot \sqrt{\log m \cdot q}\right] \\
&\leq \frac{1}{m^2}.
\end{aligned}
$$

Thus,

$$
\Pr\left[H_i \notin \mathcal{H}_{i,y} \mid Y_{i-1} = y\right] = \operatorname*{E}_{x \leftarrow X_i}\left[\Pr\left[H_i \notin \mathcal{H}_{i,y} \mid Y_i = y + x\right]\right] \leq \frac{1}{m^2} \tag{39}
$$

Fix $x \in \mathcal{X}_i$ and $v \in \mathcal{H}'_{i,y} := \mathcal{H}_{i,y} \bigcap \mathrm{Supp}(H_i \mid Y_{i-1} = y, X_i \in \mathcal{X}_i)$, where $\mathcal{X}_i$ is as defined in Lemma 4.6. Compute

$$
\begin{aligned}
\Pr[H_i = v \mid Y_i = y + x] &= 2^{-q} \cdot (1 + \varepsilon_i(y + x))^{\frac{q}{2} + \frac{w(v)}{2}} (1 - \varepsilon_i(y + x))^{\frac{q}{2} - \frac{w(v)}{2}} \tag{40} \\
&= 2^{-q} \cdot (1 - \varepsilon_i^2(y + x))^{\frac{q}{2} - \frac{w(v)}{2}} (1 + \varepsilon_i(y + x))^{w(v)}
\end{aligned}
$$

Since $1 + z \leq e^z$ for $z \in \mathbb{R}$, it holds that

$$
\Pr[H_i = v \mid Y_i = y + x] \leq 2^{-q} \cdot \exp\left(-\varepsilon_i^2(y + x) \cdot (\frac{q}{2} - \frac{w(v)}{2}) + \varepsilon_i(y + x) \cdot w(v)\right) \tag{41}
$$

Since m is large, Proposition 2.7 yields that $\varepsilon_i(y + x) \in (-\frac{1}{2}, \frac{1}{2})$. Using the inequality $1 + z \geq e^{z - z^2}$ for $z \in (-\frac{1}{2}, \frac{1}{2})$, we deduce that

$$
\begin{aligned}
\Pr[H_i = v \mid Y_i = y + x] &\geq 2^{-q} \cdot e^{(-\varepsilon_i^2(y+x) - \varepsilon_i^4(y+x))(\frac{q}{2} - \frac{w(v)}{2})} \cdot e^{(\varepsilon_i(y+x) - \varepsilon_i^2(y+x)) \cdot w(v)} \tag{42} \\
&= 2^{-q} \cdot e^{-\varepsilon_i^2(y+x) \cdot (\frac{q}{2} - \frac{w(v)}{2})} \cdot e^{\varepsilon_i(y+x) \cdot w(v)} \cdot e^{-\varepsilon_i^4(y+x) \cdot (\frac{q}{2} - \frac{w(v)}{2}) - \varepsilon_i^2(y+x) \cdot w(v)} \\
&\geq 2^{-q} \cdot \exp\left(-\varepsilon_i^2(y + x) \cdot (\frac{q}{2} - \frac{w(v)}{2}) + \varepsilon_i(y + x) \cdot w(v)\right) \cdot (1 - \mathsf{error}(x)),
\end{aligned}
$$

for

$$
\mathsf{error}(x) := \left|1 - \exp\left(-\varepsilon_i^4(y + x) \cdot (\frac{q}{2} - \frac{w(v)}{2}) - \varepsilon_i^2(y + x) \cdot w(v)\right)\right| \tag{43}
$$

49

Using Equations (41) and (42), we can now write

$$\Pr[H_i = v \mid Y_i = y + x] \in 2^{-q} \cdot \exp\left(-\varepsilon_i^2(y+x) \cdot (\frac{q}{2} - \frac{w(v)}{2}) + \varepsilon_i(y+x) \cdot w(v)\right)(1 \pm \mathsf{error}(x)) \tag{44}$$

Let $x' \in \mathcal{X}_i$, and assume without loss of generality that $\mathsf{error}(x) \geq \mathsf{error}(x')$. We show next that $\mathsf{error}(x) \in o(1)$. Hence, since $\frac{1 \pm z}{1 \pm z} \subseteq 1 \pm 4z$ for every $z \in [0, \frac{1}{2}]$, it holds that

$$\frac{\Pr[H_i = v \mid Y_i = y + x']}{\Pr[H_i = v \mid Y_i = y + x]} \tag{45}$$

$$\in \frac{\exp\left(-\varepsilon_i^2(y+x') \cdot (\frac{q}{2} - \frac{w(v)}{2}) + \varepsilon_i(y+x') \cdot w(v)\right)}{\exp\left(-\varepsilon_i^2(y+x)(\frac{q}{2} - \frac{w(v)}{2}) + \varepsilon_i(y+x) \cdot w(v)\right)} \cdot (1 \pm 4 \cdot \mathsf{error}(x))$$

$$= \exp\left((\varepsilon_i(y+x) - \varepsilon_i(y+x'))\left[(\varepsilon_i(y+x) + \varepsilon_i(y+x'))(\frac{q}{2} - \frac{w(v)}{2}) - w(v)\right]\right)(1 \pm 4 \cdot \mathsf{error}(x))$$

$$\subseteq \exp\left((\frac{x - x'}{\sqrt{s_i}} \pm \frac{\log^2 m}{\sqrt{s_i}})\left[(\frac{2y + x + x'}{\sqrt{s_i}} \pm \frac{\log^2 m}{\sqrt{s_i}}) \cdot (\frac{q}{2} - \frac{w(v)}{2}) - w(v)\right]\right) \cdot (1 \pm 4 \cdot \mathsf{error}(x))$$

$$\subseteq \exp\left(\frac{x - x' \pm \log^2 m}{\mathsf{sum}_m(i+1)} \cdot \left[\frac{2y + x + x' \pm \log^2 m}{\mathsf{sum}_m(1)} \cdot (\frac{q}{2} - \frac{w(v)}{2}) \pm \sqrt{\frac{\mathsf{sum}_m(i+1)}{\mathsf{sum}_m(1)}} \cdot w(v)\right]\right) \cdot (1 \pm 4 \cdot \mathsf{error}(x)),$$

and therefore,

$$\frac{\Pr[H_i = v \mid Y_i = y + x']}{\Pr[H_i = v \mid Y_i = y + x]} \in \exp\left((\frac{x - x'}{\mathsf{sum}_m(i+1)} \pm \frac{\log^2 m}{\mathsf{sum}_m(i+1)}) \cdot \alpha\right) \cdot (1 \pm 4 \cdot \mathsf{error}(x)) \tag{46}$$

for some $\alpha \in (\frac{2y+x+x'}{\mathsf{sum}_m(1)} \pm \frac{\log^2 m}{\mathsf{sum}_m(1)}) \cdot (\frac{q}{2} - w(v)) \pm \sqrt{\frac{\mathsf{sum}_m(i+1)}{\mathsf{sum}_m(1)}} \cdot w(v)$. The third transition of the previous calculation holds by Proposition 2.7. By taking large enough $d' = d'(\lambda) > 0$, we can bound $|\alpha|$ and $\mathsf{error}(x)$ by

$$|\alpha| \leq d' \cdot \sqrt{\log m \cdot \mathsf{sum}_m(i+1)} \tag{47}$$

and

$$\mathsf{error}(x) = \left|1 - \exp\left(-\varepsilon_i^4(y+x)(\frac{q}{2} - \frac{w(v)}{2}) - \varepsilon_i^2(y+x) \cdot w(v)\right)\right|$$

$$\leq \max\left(\left|1 - \exp\left(-\left(\frac{y+x}{\sqrt{s_i}} \pm \frac{\log^2 m}{\sqrt{s_i}}\right)^4 (\frac{q}{2} - \frac{w(v)}{2}) - \left(\frac{y+x}{\sqrt{s_i}} \pm \frac{\log^2 m}{\sqrt{s_i}}\right)^2 w(v)\right)\right|\right)$$

$$\leq 1 - \exp\left(-\left(3 \cdot \sqrt{\frac{\log m}{\mathsf{sum}_m(1)}}\right)^4 \cdot (\lambda + 1) \cdot \mathsf{sum}_m(1) - \left(3 \cdot \sqrt{\frac{\log m}{\mathsf{sum}_m(1)}}\right)^2 \cdot \sqrt{d \cdot \mathsf{sum}_m(1) \cdot \log m}\right)$$

$$\leq 1 - (1 - \frac{d' \cdot \log^{1.5} m}{\sqrt{\mathsf{sum}_m(1)}})$$

$$= d' \cdot \frac{\log^{1.5} m}{\sqrt{\mathsf{sum}_m(1)}},$$

where the second transition holds by Proposition 2.7 and the first inequality holds by the bounds on $|y|$, $|x|$ and $|w(v)|$. Since $\frac{\log^2 m}{\mathsf{sum}_m(i+1)} \cdot \alpha \in o(1)$ and since $e^y \in 1 \pm 2y$ for $y \in (-0.5, 0.5)$, it follows that

$$\exp\left(\frac{\log^2 m}{\mathsf{sum}_m(i+1)} \cdot \alpha\right) \tag{48}$$

$$\leq 1 + 2 \cdot \frac{\log^2 m}{\mathsf{sum}_m(i+1)} \cdot \alpha$$

$$\leq 1 + 2 \cdot \frac{\log^2 m}{\mathsf{sum}_m(i+1)} \cdot d' \cdot \sqrt{\log m \cdot \mathsf{sum}_m(i+1)}$$

$$\leq 1 + 2d' \cdot \frac{\log^{2.5} m}{\sqrt{\mathsf{sum}_m(i+1)}}.$$

Therefore, Equation (46) yields that

$$\frac{\Pr[H_i = v \mid Y_i = y + x']}{\Pr[H_i = v \mid Y_i = y + x]} \in \exp\left(\frac{x - x'}{\mathsf{sum}_m(i+1)} \cdot \alpha\right) \cdot \left(1 \pm \frac{\log^3 m}{\sqrt{\mathsf{sum}_m(i+1)}}\right) \tag{49}$$

and thus

$$\frac{1}{\mathsf{ratio}_{i,y,v}(x)} = \frac{\Pr[H_i = v \mid Y_{i-1} = y, X_i \in \mathcal{X}_i]}{\Pr[H_i = v \mid Y_{i-1} = y, X_i = x]} \tag{50}$$

$$= \mathop{\mathrm{E}}_{x' \leftarrow X_i | x' \in \mathcal{X}_i}\left[\frac{\Pr[H_i = v \mid Y_i = y + x']}{\Pr[H_i = v \mid Y_i = y + x]}\right]$$

$$\in \mathop{\mathrm{E}}_{x' \leftarrow X_i | x' \in \mathcal{X}_i}\left[\exp\left(\frac{\alpha(x - x')}{\mathsf{sum}_m(i+1)}\right) \cdot \left(1 \pm \frac{\log^3 m}{\mathsf{sum}_m(i+1)}\right)\right]$$

$$\subseteq \left(1 \pm \varphi_1(d) \cdot \sqrt{\frac{\log m}{\ell_m(i+1)}} \cdot (1 + \frac{|x|}{\sqrt{\ell_m(i)}})\right) \cdot \left(1 \pm \frac{\log^3 m}{\mathsf{sum}_m(i+1)}\right)$$

$$\subseteq 1 \pm \varphi_2(d) \sqrt{\frac{\log m}{\ell_m(i+1)}} \cdot (1 + \frac{|x|}{\sqrt{\ell_m(i)}}),$$

for some universal functions $\varphi_1, \varphi_2 \colon \mathbb{R}^+ \mapsto \mathbb{R}^+$. The first transition holds by Claim 4.14, the third one by Equation (49) and the fourth one by Proposition 2.8. Recalling that $i \leq m - \log^{2.5} m$, it follows that

$$\sqrt{\frac{\log m}{\ell_m(i+1)}} \cdot (1 + \frac{|x|}{\sqrt{\ell_m(i)}}) \in o(1) \tag{51}$$

Since $\frac{1}{1 \pm z} \subseteq 1 \pm 2z$ for every $z \in (-0.5, 0.5)$, we deduce from Equation (50) that

$$\mathsf{ratio}_{i,y,v}(x) \in 1 \pm 2\varphi_2(d) \cdot \sqrt{\frac{\log m}{\ell_m(i+1)}} \cdot (1 + \frac{|x|}{\sqrt{\ell_m(i)}}) \tag{52}$$

$$= 1 \pm \varphi_3(\lambda) \cdot \sqrt{\frac{\log m}{\ell_m(i+1)}} \cdot (1 + \frac{|x|}{\sqrt{\ell_m(i)}}),$$

51

where $\varphi_3(\lambda) = 2 \cdot \varphi_2(d(\lambda))$. Thus

$$|1 - \mathsf{ratio}_{i,y,v}(x)| \le \varphi_3(\lambda) \cdot \sqrt{\frac{\log m}{\ell_m(i+1)}} \cdot (1 + \frac{|x|}{\sqrt{\ell_m(i)}}) \tag{53}$$

Finally, since the above holds for every $i \le m - \log^{2.5} m$, $y \in \mathcal{Y}_{i-1}$, $v \in \mathcal{H}_{i,y}$ and $x \in \mathcal{X}_i$, and recalling Equation (39), we can apply Lemma 4.6 to get that $\mathsf{Bias}(\mathsf{G}_{f,m,\varepsilon}) \le \varphi(\lambda) \cdot \frac{\log^3 m}{m}$, for some universal function $\varphi \colon \mathbb{R}^+ \mapsto \mathbb{R}^+$. $\qquad\square$

Acknowledgment

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] N. Alon and M. Naor. Coin-flipping games immune against linear-sized coalitions. *SIAM Journal on Computing*, pages 46–54, 1993.

[5] A. Ambainis. A new protocol and lower bounds for quantum coin flipping. *J. Comput. Syst. Sci.*, 68(2):398–416, 2004.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] M. Ben-Or and N. Linial. Collective coin flipping. *ADVCR: Advances in Computing Research*, 5, 1989.

[13] 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.

[14] 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.

[15] M. Blum. How to exchange (secret) keys. *ACM Transactions on Computer Systems*, 1983.

[16] R. Canetti. Security and composition of multiparty cryptographic protocols. *Journal of Cryptology*, 13(1):143–202, 2000.

[17] 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.

[18] R. Cleve and R. Impagliazzo. Martingales, collective coin flipping and discrete control processes. Manuscript, 1993. URL https://pdfs.semanticscholar.org/7c7f/244d2ef064d75b3d23c88472ee1226461695.pdf.

[19] R. Cohen, I. Haitner, E. Omri, and L. Rotem. Characterization of secure multiparty computation without broadcast. In *Theory of Cryptography, 13th Theory of Cryptography Conference, TCC 2016a*, pages 596–616, 2016.

[20] 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.

[21] S. Even, O. Goldreich, and A. Lempel. A randomized protocol for signing contracts. *Communications of the ACM*, 28(6):637–647, 1985.

[22] U. Feige. Noncryptographic selection protocols. In *Proceedings of the 40th Annual Symposium on Foundations of Computer Science (FOCS)*, 1999.

[23] 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.

[24] O. Goldreich. *Foundations of Cryptography – VOLUME 2: Basic Applications*. Cambridge University Press, 2004.

[25] O. Goldreich, S. Micali, and A. Wigderson. How to play any mental game or a complete-ness theorem for protocols with honest majority. In *Proceedings of the 19th Annual ACM Symposium on Theory of Computing (STOC)*, pages 218–229, 1987.

[26] O. Goldreich, S. Micali, and A. Wigderson. Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. *Journal of the ACM*, pages 691–729, 1991. Preliminary version in *FOCS'86*.

[27] S. D. Gordon and J. Katz. Partial fairness in secure two-party computation. In *Advances in Cryptology – EUROCRYPT 2011*, pages 157–176, 2010.

[28] S. D. Gordon, C. Hazay, J. Katz, and Y. Lindell. Complete fairness in secure two-party computation. In *Proceedings of the 38th Annual ACM Symposium on Theory of Computing (STOC)*, pages 413–422, 2008.

[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. In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing (STOC)*, pages 817–836, 2014.

[33] I. Haitner and E. Tsfadia. An almost-optimally fair three-party coin-flipping protocol. *SIAM Journal on Computing*, 46(2):479–542, 2017.

[34] I. Haitner, M. Nguyen, S. J. Ong, O. Reingold, and S. Vadhan. Statistically hiding commit-ments and statistical zero-knowledge arguments from any one-way function. *SIAM Journal on Computing*, pages 1153–1218, 2009.

[35] W. Hoeffding. Probability inequalities for sums of bounded random variables, 1963.

[36] R. Impagliazzo and M. Luby. One-way functions are essential for complexity based cryptog-raphy. In *Proceedings of the 30th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 230–235, 1989.

[37] Y. Kalai. Smooth projective hashing and two-message oblivious transfer. In *Advances in Cryptology – EUROCRYPT 2005*, 2005.

[38] J. Katz. On achieving the "best of both worlds" in secure multiparty computation. In *Pro-ceedings of the 37th Annual ACM Symposium on Theory of Computing (STOC)*, pages 11–20, 2007.

[39] 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.

[40] T. Moran and M. Naor. Basing cryptographic protocols on tamper-evident seals. In *ICALP: Annual International Colloquium on Automata, Languages and Programming*, 2005.

[41] T. Moran, M. Naor, and G. Segev. An optimally fair coin toss. *Journal of Cryptology*, 29(3): 491–513, 2016.

[42] M. Naor. Bit commitment using pseudorandomness. *Journal of Cryptology*, pages 151–158, 1991.

[43] M. Naor and B. Pinkas. Efficient oblivious transfer protocols. In *SODA*, pages 448–457, 2001.

[44] 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.

[45] M. Saks. A robust noncryptographic protocol for collective coin flipping. *SIJDM: SIAM Journal on Discrete Mathematics*, 2, 1989.

[46] M. Scala. Hypergeometric tail inequalities: ending the insanity. *arXiv preprint arXiv:1311.5939*, 2009.

A   Missing Proofs

This section contains missing proofs for statements given in Sections 2.2 to 2.4.

A.1   Basic Inequalities

Proposition A.1 (Restatement of Proposition 2.1)**.** *Let $n \in \mathbb{N}$, $\alpha > 0$, $k \in [n]$ and let $\{p_j\}_{j=k}^n$ be a set of non-negative numbers such that $\sum_{j=i}^n p_j \le \alpha \cdot (n+1-i)$ for every $i \in \{k, k+1, \dots, n\}$. Then $\sum_{j=k}^n \frac{p_j}{(n+1-j)} \le \alpha \cdot \sum_{j=k}^n \frac{1}{(n+1-j)}$.*

Proof. We prove the proposition by showing that for every set $\mathcal{S} = \{p_j\}_{j=k}^n$ satisfying the proposition's constrains, it holds that $\mathsf{val}(\mathcal{S}) := \sum_{j=k}^n \frac{p_j}{(n+1-j)} \le \sum_{j=k}^n \frac{\alpha}{(n+1-j)}$. Let $\mathcal{S} = \{p_j\}_{j=k}^n$ be a set that satisfying the proposition's constrains with maximal $\mathsf{val}(\mathcal{S})$. Assume not all elements of $\mathcal{S}$ equal α, and let $i^* \in \{k, k+1, \dots, n\}$ be the largest index such that $p_{i^*} \ne \alpha$. By the proposition's constrains, it follows that $\sum_{j=i^*}^n p_j \le \alpha \cdot (n+1-i^*)$. Since $\sum_{j=i^*+1}^n p_j = \alpha \cdot (n-i^*)$, it follows that $p_{i^*} + \alpha(n-i^*) \le \alpha \cdot (n+1-i^*)$, and thus $p_{i^*} \le \alpha$. Since we assume $p_{i^*} \ne \alpha$, it follows that $p_{i^*} < \alpha$.

Assume $i^* = k$, then by changing p_{i^*} to α, we get a set $\mathcal{S}'$ with $\mathsf{val}(\mathcal{S}') > \mathsf{val}(\mathcal{S})$ that fulfills the proposition's constrains, in contradiction to the maximality of $\mathcal{S}$.

Assume $i^* > k$ and let $\delta = \alpha - p_{i^*} > 0$. Let $\mathcal{S}' = \{p_j'\}_{j=k}^n$ defined by

$$
p_j' = \begin{cases} p_j + \delta, & j = i^*, \\ p_j - \delta, & j = i^* - 1, \\ p_j, & \text{otherwise.} \end{cases}
$$

Note that $\mathcal{S}'$ fulfills proposition's constrains, and

$$\text{val}(\mathcal{S}') = \sum_{j=k}^{n} \frac{p_j'}{n-j+1} = \sum_{j=k}^{n} \frac{p_j}{n-j+1} + \frac{\delta}{n-i^*+1} - \frac{\delta}{n-i^*+2} > \sum_{j=k}^{n} \frac{p_j}{n-j+1} = \text{val}(\mathcal{S}),$$

in contraction to the maximality of $\mathcal{S}$. $\qquad\square$

A.2   Facts About the Binomial Distribution

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, $f(\mathcal{S}_1, \ldots, \mathcal{S}_k) = \{f(x_1, \ldots, x_j) : x_i \in \mathcal{S}_i\}$, e.g., $f(1 \pm 0.1) = \{f(x) : x \in [.9, 1.1]\}$.

We use the following estimation of the binomial coefficient.

Proposition A.2. *Let $n \in \mathbb{N}$ and $t \in \mathbb{Z}$ be such that $|t| \leq n^{\frac{3}{5}}$ and $\frac{n+t}{2} \in (n)$. Then*

$$\binom{n}{\frac{n+t}{2}} \cdot 2^{-n} \in (1 \pm \text{error}) \cdot \sqrt{\frac{2}{\pi}} \cdot \frac{1}{\sqrt{n}} \cdot e^{-\frac{t^2}{2n}},$$

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

Proof. In the following we focus on $n \geq 200$, smaller n's are handled by setting the value of ξ to be large enough on these values. We also assume that n and t are even, the proof of the odd case is analogous. Let $m := \frac{n}{2} \geq 100$ and $k := \frac{t}{2}$. Stirling's formula states that for every $\ell \in \mathbb{N}$ it holds that $1 \leq \frac{\ell!}{\sqrt{2\pi\ell} \cdot (\frac{\ell}{e})^{\ell}} \leq e^{\frac{1}{12\ell}}$ which implies $\ell! \in (1 \pm \frac{1}{\ell})\sqrt{2\pi\ell} \cdot \ell^{\ell} \cdot e^{-\ell}$. Compute

$$\binom{2m}{m+k} = \frac{(2m)!}{(m+k)!(m-k)!}$$

$$\in \frac{(1 \pm \frac{1}{2m})\sqrt{2\pi \cdot 2m}(2m)^{2m}e^{-2m}}{(1 \pm \frac{1}{m+k})\sqrt{2\pi(m+k)}(m+k)^{m+k}e^{-(m+k)} \cdot (1 \pm \frac{1}{m-k})\sqrt{2\pi(m-k)}(m-k)^{m-k}e^{-(m-k)}}$$

$$\subseteq \frac{\sqrt{2\pi \cdot 2m}(2m)^{2m}e^{-2m}}{\sqrt{2\pi(m+k)}(m+k)^{m+k}e^{-(m+k)} \cdot \sqrt{2\pi(m-k)}(m-k)^{m-k}e^{-(m-k)}} \cdot (1 \pm \frac{20}{m})$$

$$= \frac{(2m)^{2m+\frac{1}{2}}}{\sqrt{2\pi} \cdot (m+k)^{m+k+\frac{1}{2}} \cdot (m-k)^{m-k+\frac{1}{2}}} \cdot (1 \pm \frac{20}{m})$$

$$= 2^{2m} \cdot \frac{1}{\sqrt{\pi m} \cdot (1 + \frac{k}{m})^{m+k+\frac{1}{2}} \cdot (1 - \frac{k}{m})^{m-k+\frac{1}{2}}} \cdot (1 \pm \frac{20}{m})$$

$$= 2^{2m} \cdot \frac{1}{\sqrt{\pi m} \cdot (1 - \frac{k^2}{m^2})^{m-k+\frac{1}{2}} \cdot (1 + \frac{k}{m})^{2k}} \cdot (1 \pm \frac{20}{m}),$$

where the third transition holds by the bound on m and k which yields $\frac{(1 \pm \frac{1}{m})}{(1 \pm \frac{1}{m+k})(1 \pm \frac{1}{m-k})} \subseteq (1 \pm \frac{20}{m})$.

Since $1 + x \in e^{x \pm x^2}$ for $x \in (-0.5, 0.5)$, it follows that

$$\binom{n}{\frac{n+t}{2}} \cdot 2^{-n} = \binom{2m}{m+k} \cdot 2^{-2m} \tag{54}$$

$$\in \frac{1}{\sqrt{\pi m} \cdot e^{(-\frac{k^2}{m^2} \pm \frac{k^4}{m^4})(m-k+\frac{1}{2})} \cdot e^{(\frac{k}{m} \pm \frac{k^2}{m^2}) \cdot 2k}} \cdot (1 \pm \frac{20}{m})$$

$$= \frac{1}{\sqrt{\pi m}} \cdot e^{-\frac{k^2}{m}} \cdot e^{-\frac{k^3}{m^2} \pm \frac{3|k|^3}{m^2} + \frac{k^2}{2m^2} \pm \frac{k^4}{m^4}(m-k+\frac{1}{2})} \cdot (1 \pm \frac{20}{m})$$

$$\subseteq \frac{1}{\sqrt{\pi m}} \cdot e^{-\frac{k^2}{m}} \cdot e^{\pm \frac{5|k|^3}{m^2}} \cdot (1 \pm \frac{20}{m})$$

$$\subseteq \frac{1}{\sqrt{\pi m}} \cdot e^{-\frac{k^2}{m}} \cdot (1 \pm \frac{10|k|^3}{m^2}) \cdot (1 \pm \frac{20}{m})$$

$$\subseteq \frac{1}{\sqrt{\pi}} \cdot (1 \pm 20 \cdot (\frac{|k|^3}{m^2} + \frac{1}{m})) \cdot \frac{1}{\sqrt{m}} \cdot e^{-\frac{k^2}{m}},$$

$$\subseteq \sqrt{\frac{2}{\pi}} \cdot (1 \pm 40 \cdot (\frac{|t|^3}{n^2} + \frac{1}{n})) \cdot \frac{1}{\sqrt{n}} \cdot e^{-\frac{t^2}{2n}}$$

where the third transition holds by the bounds on m and k, and the fourth one holds since $\frac{4|k|^3}{m^2} < 1$ and since $e^x \in 1 \pm 2x$ for every $|x| < 1$. $\square$

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. The following proposition uses the previous estimation for the binomial coefficient for achieving an estimation for the binomial probability $\mathcal{C}_{n,\varepsilon}(t) := \Pr_{x \leftarrow \mathcal{C}_{n,\varepsilon}}[x = t]$.

Proposition A.3 (Restatement of Proposition 2.4)**.** *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.

Proof. In the following we focus on $n \ge 200$, smaller n's are handled by setting the value of ξ to be large enough on these values. Let ξ_1 be the universal constant from Proposition A.2. Compute

$$\mathcal{C}_{n,\varepsilon}(t) = \binom{n}{\frac{n+t}{2}} 2^{-n} (1+\varepsilon)^{\frac{n+t}{2}} (1-\varepsilon)^{\frac{n-t}{2}} \tag{55}$$

$$\in \sqrt{\frac{2}{\pi}} (1 \pm \xi_1 \cdot (\frac{|t|^3}{n^2} + \frac{1}{n})) \cdot \frac{1}{\sqrt{n}} \cdot e^{-\frac{t^2}{2n}} \cdot (1-\varepsilon^2)^{\frac{n-t}{2}} (1+\varepsilon)^t,$$

where the second transition holds by Proposition A.2. Since $1 + x \in e^{x \pm x^2}$ for $x \in (-0.5, 0.5)$, it

follows that:

$$\mathcal{C}_{n,\varepsilon}(t) \in \sqrt{\frac{2}{\pi}}(1 \pm \xi_1 \cdot (\frac{|t|^3}{n^2} + \frac{1}{n})) \cdot \frac{1}{\sqrt{n}} \cdot e^{-\frac{t^2}{2n}} \cdot e^{(-\varepsilon^2 \pm \varepsilon^4) \cdot \frac{n-t}{2}} e^{(\varepsilon \pm \varepsilon^2)t}$$

$$\subseteq \sqrt{\frac{2}{\pi}}(1 \pm \xi_1 \cdot (\frac{|t|^3}{n^2} + \frac{1}{n})) \cdot \frac{1}{\sqrt{n}} \cdot e^{-\frac{t^2}{2n} - \frac{\varepsilon^2 n}{2} + \varepsilon t} \cdot e^{\pm(2\varepsilon^2|t| + \frac{\varepsilon^4 n}{2})}$$

$$\subseteq \sqrt{\frac{2}{\pi}}(1 \pm \xi_1 \cdot (\frac{|t|^3}{n^2} + \frac{1}{n})) \cdot \frac{1}{\sqrt{n}} \cdot e^{-\frac{(t-\varepsilon n)^2}{2n}} (1 \pm 4 \cdot (\varepsilon^2 |t| + \varepsilon^4 n))$$

$$\subseteq \sqrt{\frac{2}{\pi}}(1 \pm \xi \cdot (\varepsilon^2 |t| + \frac{|t|^3}{n^2} + \frac{1}{n} + \varepsilon^4 n)) \cdot \frac{1}{\sqrt{n}} \cdot e^{-\frac{(t-\varepsilon n)^2}{2n}},$$

where $\xi = 4\xi_1 + 4$. Note that since $e^x \in 1 \pm 2x$ for every $|x| < 1$, and since $2\varepsilon^2 |t| + \frac{\varepsilon^4 n}{2} < 2n^{-\frac{1}{5}} + \frac{1}{2}n^{-\frac{3}{5}} < 1$, it follows that $e^{\pm(2\varepsilon^2|t| + \frac{\varepsilon^4 n}{2})} \subseteq 1 \pm 4 \cdot (\varepsilon^2 |t| + \varepsilon^4 n)$ which yields the third transition. In addition, note that $\frac{|t|^3}{n^2} + \frac{1}{n} < n^{-\frac{1}{5}} + \frac{1}{n} < 1$, which implies the last transition. $\square$

Using the above estimation for the binomial probability, the following proposition estimate the relation between two binomial probabilities.

Proposition A.4 (Restatement of Proposition 2.5). *Let $n \in \mathbb{N}$, $t, x, x' \in \mathbb{Z}$, $\varepsilon \in [-1, 1]$ and $\lambda > 0$ be such that $t - x, t - x' \in \mathrm{Supp}(\mathcal{C}_{n,\varepsilon})$, $|x|, |x'|, |t| \leq \lambda \cdot \sqrt{n \log n}$ and $|\varepsilon| \leq \lambda \cdot \sqrt{\frac{\log n}{n}}$, then*

$$\frac{\mathcal{C}_{n,\varepsilon}(t - x')}{\mathcal{C}_{n,\varepsilon}(t - x)} \in (1 \pm \mathsf{error}) \cdot \exp\left(\frac{-2 \cdot (t - \varepsilon n) \cdot x + x^2 + 2 \cdot (t - \varepsilon n) \cdot x' - x'^2}{2n}\right),$$

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

Proof. Let ξ be the constant from Proposition A.3. There exists a function $\vartheta \colon \mathbb{R}^+ \mapsto \mathbb{N}$ such that $n^{\frac{3}{5}} > 2\lambda \cdot \sqrt{n \log n}$ and $\xi \cdot (\lambda^4 + 10\lambda^3 + 1) \cdot \frac{\log^{1.5} n}{\sqrt{n}} < \frac{1}{2}$ for every $n \geq \vartheta(\lambda)$. In the following we focus on $n \geq \vartheta(\lambda)$, where smaller n's are handled by setting the value of $\varphi(\lambda)$ to be large enough on these values. Let $\varphi(\lambda) := 4 \cdot \xi \cdot (\lambda^4 + 10\lambda^3 + 1)$. It follows that

$$\frac{\mathcal{C}_{n,\varepsilon}(t - x')}{\mathcal{C}_{n,\varepsilon}(t - x)} \in \frac{\left(1 \pm \xi \cdot (\varepsilon^2 |t - x'| + \frac{1}{n} + \frac{|t-x'|^3}{n^2} + \varepsilon^4 n)\right) \cdot \sqrt{\frac{2}{\pi}} \cdot \frac{1}{\sqrt{n}} \cdot e^{-\frac{(t-\varepsilon n - x')^2}{2n}}}{\left(1 \pm \xi \cdot (\varepsilon^2 |t - x| + \frac{1}{n} + \frac{|t-x|^3}{n^2} + \varepsilon^4 n)\right) \cdot \sqrt{\frac{2}{\pi}} \cdot \frac{1}{\sqrt{n}} \cdot e^{-\frac{(t-\varepsilon n - x)^2}{2n}}}$$

$$\subseteq \frac{\left(1 \pm \xi \cdot (\lambda^4 + 10\lambda^3 + 1) \cdot \frac{\log^{1.5} n}{\sqrt{n}}\right) \cdot e^{-\frac{(t-\varepsilon n - x')^2}{2n}}}{\left(1 \pm \xi \cdot (\lambda^4 + 10\lambda^3 + 1) \cdot \frac{\log^{1.5} n}{\sqrt{n}}\right) \cdot e^{-\frac{(t-\varepsilon n - x)^2}{2n}}}$$

$$\subseteq (1 \pm \varphi(\lambda) \cdot \frac{\log^{1.5} n}{\sqrt{n}}) \cdot \exp\left(\frac{(t - \varepsilon n - x)^2}{2n} - \frac{(t - \varepsilon n - x')^2}{2n}\right)$$

$$= (1 \pm \varphi(\lambda) \cdot \frac{\log^{1.5} n}{\sqrt{n}}) \cdot \exp\left(\frac{-2 \cdot (t - \varepsilon n) \cdot x + x^2 + 2 \cdot (t - \varepsilon n) \cdot x' - x'^2}{2n}\right),$$

where the first transition holds by Proposition A.3, the second one holds by the bounds on $|t|$, $|x|$, $|x'|$ and $|\varepsilon|$, and the third one holds since $\frac{1 \pm y}{1 \pm y} \subseteq 1 \pm 4y$ for every $y \in [0, \frac{1}{2}]$. $\square$

Recall that for $n \in \mathbb{N}$ and $k \in \mathbb{Z}$ we let $\widehat{\mathcal{C}}_{n,\varepsilon}(k) := \Pr_{x \leftarrow \mathcal{C}_{n,\varepsilon}}[x \geq k] = \sum_{t \geq k} \mathcal{C}_{n,\varepsilon}(t)$. Assuming that n is larger than some universal constant, the following proposition gives a useful bound on the probability of the event that a binomial distribution is in a certain range of value.

Proposition A.5 (Restatement of Proposition 2.6). *Let $n \in \mathbb{N}$, $k, k' \in \mathbb{Z}$ and $\varepsilon \in [-1, 1]$, where n is larger than a universal constant, $|k|, |k'| \leq n^{\frac{3}{5}}$ and $|\varepsilon| \leq n^{-\frac{2}{5}}$. Then*

$$\left| \widehat{\mathcal{C}}_{n,\varepsilon}(k) - \widehat{\mathcal{C}}_{n,\varepsilon}(k') \right| \leq \frac{|k - k'|}{\sqrt{n}}.$$

Proof. By Proposition A.3, for every $t \in \mathbb{Z}$ with $|t| \leq n^{\frac{3}{5}}$, it holds that

$$\mathcal{C}_{n,\varepsilon}(t) \in (1 \pm 0.1) \cdot \sqrt{\frac{2}{\pi}} \cdot \frac{1}{\sqrt{n}} \cdot e^{-\frac{(t - \varepsilon n)^2}{2n}},$$

and therefore

$$\mathcal{C}_{n,\varepsilon}(t) \leq \frac{1}{\sqrt{n}} \cdot e^{-\frac{(t - \varepsilon n)^2}{2n}} \leq \frac{1}{\sqrt{n}}.$$

Assume without loss of generality that $k' \geq k$, it holds that $\widehat{\mathcal{C}}_{n,\varepsilon}(k) - \widehat{\mathcal{C}}_{n,\varepsilon}(k') = \sum_{t=k}^{k'} \mathcal{C}_{n,\varepsilon}(t)$, which by the bound above, is at most $\frac{(k'-k)}{\sqrt{n}}$. $\square$

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. The following fact and proposition are the first steps towards estimating the value of $\widehat{\mathcal{C}}_{n,\varepsilon}(k)$ in Proposition A.8.

Fact A.6 ([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.7. *Let $n \in \mathbb{N}$, $\varepsilon \in (-1, 1)$ and $k, k' \in \mathbb{Z}$ be such that $k' \geq k \geq \frac{\varepsilon n}{2}$. Then*

$$\left| \sum_{t=k}^{k'} e^{-\frac{(2t - \varepsilon n)^2}{2n}} - \int_k^{k'} e^{-\frac{(2t - \varepsilon n)^2}{2n}} dt \right| \leq e^{-\frac{(2k - \varepsilon n)^2}{2n}}.$$

Proof. Consider the function $f(t) = e^{-\frac{(2t - \varepsilon n)^2}{2n}}$. The function f obtains its maximum at $t = \frac{\varepsilon n}{2}$ and is monotonic decreasing in $[\frac{\varepsilon n}{2}, \infty)$. In particular, it is decreasing in $[k, \infty)$. Since $\sum_{t=k}^{k'} f(t)$ is an upper Darboux sum of f with respect to $\{k, k+1, \ldots, k'+1\}$, it holds that $\int_k^{k'} f(t) dt \leq \int_k^{k'+1} f(t) dt \leq \sum_{t=k}^{k'} f(t)$. In addition, since $\sum_{t=k+1}^{k'} f(t)$ is a lower Darboux sum of f with respect to $\{k, k+1, \ldots, k'\}$, it holds that $\sum_{t=k}^{k'} f(t) \leq \int_k^{k'} f(t) dt + f(k)$. The proof follows, since the difference between the above sums is at most $f(k) = e^{-\frac{(2k - \varepsilon n)^2}{2n}}$. $\square$

We are now ready for estimating $\widehat{\mathcal{C}}_{n,\varepsilon}(k)$ using the function Φ.

Proposition A.8. *Let $n \in \mathbb{N}$, $k \in \mathbb{Z}$, $\varepsilon \in [-1, 1]$ and $\lambda > 0$ be such that $|\varepsilon| \leq \lambda \cdot \sqrt{\frac{\log n}{n}}$ and $|k| < \lambda \cdot \sqrt{n \log n}$. Then*

$$\widehat{\mathcal{C}}_{n,\varepsilon}(k) \in \Phi(\frac{k - \varepsilon n}{\sqrt{n}}) \pm \mathsf{error},$$

for $\mathsf{error} = \varphi(\lambda) \cdot \frac{\log^{1.5} n}{\sqrt{n}} \cdot e^{-\frac{(k-\varepsilon n)^2}{2n}}$ *and a universal function* φ.

Proof. Without loss of generality, assume that $\lambda \geq 4$. Note that there exists a function $\vartheta \colon \mathbb{R}^+ \mapsto \mathbb{N}$ such that $n^{\frac{3}{5}} > 5\lambda \cdot \sqrt{n \log n}$ for every $n \geq \vartheta(\lambda)$. In the following we focus on $n \geq \vartheta(\lambda)$, where smaller n's are handled by setting the value of $\varphi(\lambda)$ to be large enough on these values. We also assume for simplicity that n and k are both even, where the proofs of the other cases are analogous. Let ξ_1 be the constant defined in Proposition A.3, and let $\ell := 4 \cdot \lceil \lambda \sqrt{n \log n} \rceil < 5\lambda \cdot \sqrt{n \log n}$. We start by handling the case $k \geq \varepsilon n$. It holds that

$$\sum_{t=k}^{\ell} \mathcal{C}_{n,\varepsilon}(t) = \sum_{t=\frac{k}{2}}^{\frac{\ell}{2}} \mathcal{C}_{n,\varepsilon}(2t) \tag{56}$$

$$\in \sum_{t=\frac{k}{2}}^{\frac{\ell}{2}} \sqrt{\frac{2}{\pi}} (1 \pm \xi_1 \cdot (\varepsilon^2 |2t| + \frac{|2t|^3}{n^2} + \frac{1}{n} + \varepsilon^4 n)) \cdot \frac{1}{\sqrt{n}} e^{-\frac{(2t - \varepsilon n)^2}{2n}}$$

$$\subseteq \sum_{t=\frac{k}{2}}^{\frac{\ell}{2}} \sqrt{\frac{2}{\pi}} (1 \pm \varphi'(\lambda) \cdot \frac{\log^{1.5} n}{\sqrt{n}}) \cdot \frac{1}{\sqrt{n}} e^{-\frac{(2t - \varepsilon n)^2}{2n}}$$

$$\subseteq (1 \pm \varphi'(\lambda) \cdot \frac{\log^{1.5} n}{\sqrt{n}}) \cdot A(n, k, \varepsilon, \lambda),$$

letting $\varphi'(\lambda) := \xi_1 \cdot (\lambda^4 + 1034\lambda^3 + 1)$ and $A(n, k, \varepsilon, \lambda) := \sum_{t=\frac{k}{2}}^{\frac{\ell}{2}} \sqrt{\frac{2}{\pi}} \cdot \frac{1}{\sqrt{n}} \cdot e^{-\frac{(2t - \varepsilon n)^2}{2n}}$. The first transition holds since even n yields that $\mathcal{C}_{n,\varepsilon}(j) = 0$ for every odd j, the second one holds by Proposition A.3 and the third one holds by the bounds on ℓ, ε and k.

Compute

$$A(n, k, \varepsilon, \lambda) = \sum_{t=\frac{k}{2}}^{\frac{\ell}{2}} \sqrt{\frac{2}{\pi}} \cdot \frac{1}{\sqrt{n}} \cdot e^{-\frac{(2t-\varepsilon n)^2}{2n}} \tag{57}$$

$$\in \int_{\frac{k}{2}}^{\frac{\ell}{2}} \sqrt{\frac{2}{\pi}} \cdot \frac{1}{\sqrt{n}} \cdot e^{-\frac{(2t-\varepsilon n)^2}{2n}} dt \pm \frac{1}{\sqrt{n}} \cdot e^{-\frac{(k-\varepsilon n)^2}{2n}}$$

$$= \int_{\frac{k-\varepsilon n}{\sqrt{n}}}^{\frac{\ell-\varepsilon n}{\sqrt{n}}} \frac{1}{\sqrt{2\pi}} \cdot e^{-\frac{x^2}{2}} dx \pm \frac{1}{\sqrt{n}} \cdot e^{-\frac{(k-\varepsilon n)^2}{2n}}$$

$$= \Phi(\frac{k-\varepsilon n}{\sqrt{n}}) - \Phi(\frac{\ell-\varepsilon n}{\sqrt{n}}) \pm \frac{1}{\sqrt{n}} \cdot e^{-\frac{(k-\varepsilon n)^2}{2n}}$$

$$\subseteq \Phi(\frac{k-\varepsilon n}{\sqrt{n}}) \pm \frac{1}{n^{4c^2}} \pm \frac{1}{\sqrt{n}} \cdot e^{-\frac{(k-\varepsilon n)^2}{2n}}$$

$$\subseteq \Phi(\frac{k-\varepsilon n}{\sqrt{n}}) \pm \frac{2}{\sqrt{n}} \cdot e^{-\frac{(k-\varepsilon n)^2}{2n}},$$

where the second transition holds by Proposition A.7 (and since $k \geq \varepsilon n$), the third one holds by letting $x = \frac{2t-\varepsilon n}{\sqrt{n}}$, the fifth one holds by Fact A.6 which yields that $\Phi(\frac{\ell-\varepsilon n}{\sqrt{n}}) \leq \Phi(3\lambda\sqrt{\log n}) \leq \frac{1}{n^{4c^2}}$, and the last one holds since $\frac{1}{\sqrt{n}} \cdot e^{-\frac{(k-\varepsilon n)^2}{2n}} \geq \frac{1}{n^{2\lambda^2 + \frac{1}{2}}} \geq \frac{1}{n^{4\lambda^2}}$. Applying Equation (57) on Equation (56) yields that

$$\sum_{t=k}^{\ell} \mathcal{C}_{n,\varepsilon}(t) \in (1 \pm \varphi'(\lambda) \cdot \frac{\log^{1.5} n}{\sqrt{n}}) \cdot (\Phi(\frac{k-\varepsilon n}{\sqrt{n}}) \pm \frac{2}{\sqrt{n}} \cdot e^{-\frac{(k-\varepsilon n)^2}{2n}}) \tag{58}$$

$$= \Phi(\frac{k-\varepsilon n}{\sqrt{n}}) \pm \varphi'(\lambda) \cdot \frac{\log^{1.5} n}{\sqrt{n}} \cdot \Phi(\frac{k-\varepsilon n}{\sqrt{n}}) \pm 2 \cdot \varphi'(\lambda) \cdot \frac{\log^{1.5} n}{n} \cdot e^{-\frac{(k-\varepsilon n)^2}{2n}} \pm \frac{2}{\sqrt{n}} \cdot e^{-\frac{(k-\varepsilon n)^2}{2n}}$$

$$\subseteq \Phi(\frac{k-\varepsilon n}{\sqrt{n}}) \pm \varphi''(\lambda) \cdot \frac{\log^{1.5} n}{\sqrt{n}} \cdot e^{-\frac{(k-\varepsilon n)^2}{2n}},$$

letting $\varphi''(\lambda) := 3 \cdot \varphi'(\lambda) + 2$. We conclude that

$$\widehat{\mathcal{C}}_{n,\varepsilon}(k) = \sum_{t=k}^{n} \mathcal{C}_{n,\varepsilon}(t) \tag{59}$$

$$= \sum_{t=k}^{\ell} \mathcal{C}_{n,\varepsilon}(t) + \Pr_{x \leftarrow \mathcal{C}_{n,\varepsilon}}[x > \ell]$$

$$\in \sum_{t=k}^{\ell} \mathcal{C}_{n,\varepsilon}(t) \pm \frac{1}{n^{4c^2}}$$

$$\subseteq \left(\Phi(\frac{k-\varepsilon n}{\sqrt{n}}) \pm \varphi''(\lambda) \cdot \frac{\log^{1.5} n}{\sqrt{n}} \cdot e^{-\frac{(k-\varepsilon n)^2}{2n}} \right) \pm \frac{1}{n^{4\lambda^2}}$$

$$\subseteq \Phi(\frac{k-\varepsilon n}{\sqrt{n}}) \pm (\varphi''(\lambda) + 1) \cdot \frac{\log^{1.5} n}{\sqrt{n}} \cdot e^{-\frac{(k-\varepsilon n)^2}{2n}},$$

61

where the third transition holds by Hoeffding's inequality (Fact 2.2) and the fourth one holds by Equation (58).

It is left to handle the case $k < \varepsilon n$. For such k, it holds that

$$\widehat{\mathcal{C}}_{n,\varepsilon}(k) = 1 - \widehat{\mathcal{C}}_{n,-\varepsilon}(-k) + \mathcal{C}_{n,\varepsilon}(k) \tag{60}$$

$$\in 1 - \widehat{\mathcal{C}}_{n,-\varepsilon}(-k) \pm \frac{1}{\sqrt{n}} \cdot e^{-\frac{(k-\varepsilon n)^2}{2n}}$$

$$\subseteq \left(1 - \Phi(\frac{-k+\varepsilon n}{\sqrt{n}}) \pm (\varphi''(\lambda)+1) \cdot \frac{\log^{1.5} n}{\sqrt{n}} \cdot e^{-\frac{(k-\varepsilon n)^2}{2n}}\right) \pm \frac{1}{\sqrt{n}} \cdot e^{-\frac{(k-\varepsilon n)^2}{2n}}$$

$$\subseteq \Phi(\frac{k-\varepsilon n}{\sqrt{n}}) \pm (\varphi''(\lambda)+2) \cdot \frac{\log^{1.5} n}{\sqrt{n}} \cdot e^{-\frac{(k-\varepsilon n)^2}{2n}},$$

where the second transition holds by evaluating the value of $\mathcal{C}_{n,\varepsilon}(k)$ using Proposition A.3 and the third one holds by Equation (59) applied to $-k$ and $-\varepsilon$. $\qquad\square$

Recall that for $n \in \mathbb{N}$ and $\delta \in [0, 1]$ we let $\widehat{\mathcal{C}}_n^{-1}(\delta)$ be the value $\varepsilon \in [-1, 1]$ with $\widehat{\mathcal{C}}_{n,\varepsilon}(0) = \delta$. The following proposition gives an estimation for $\widehat{\mathcal{C}}_n^{-1}(\delta)$ using Proposition A.8.

Proposition A.9. *Let $n \in \mathbb{N}$, $\delta \in [0, 1]$ and $\lambda > 0$ be such that $\delta \in (\frac{1}{n^c}, 1 - \frac{1}{n^c})$. 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. Let $\varphi' \colon \mathbb{R}^+ \mapsto \mathbb{R}^+$ be the function from Proposition A.8, and let $\varphi(\lambda) := 6 \cdot \varphi'(\sqrt{2\lambda}+1)+1$. There exists a function $\vartheta \colon \mathbb{R}^+ \mapsto \mathbb{N}$ such that the two conditions

1. $\min(2\lambda, \lambda^2) \cdot \log n > 1$

2. $\max(\sqrt{2\lambda}, \frac{1}{\sqrt{2\lambda}}) \cdot \max(\varphi^2(\lambda), 1) \cdot \frac{\log^2 n}{\sqrt{n}} < \frac{1}{8}$

holds for every $n \geq \vartheta(\lambda)$. In the following we focus on $n \geq \vartheta(\lambda)$, where smaller n's are handled by setting the value of $\varphi(c)$ to be large enough on these values. Let $x := \Phi^{-1}(\delta)$ and $\Delta := \varphi(\lambda) \cdot \frac{\log^{1.5} n}{\sqrt{n}}$, and let $\varepsilon^+ := -\frac{x}{\sqrt{n}} + \frac{\Delta}{\sqrt{n}}$ and $\varepsilon^- := -\frac{x}{\sqrt{n}} - \frac{\Delta}{\sqrt{n}}$. We prove that $\varepsilon^- < \widehat{\mathcal{C}}_n^{-1}(\delta) < \varepsilon^+$, yielding the required bound. For simplicity, we focus on the upper bound, whereas the lower bound can be proven analogously.

Since $\delta \in (\frac{1}{n^\lambda}, 1 - \frac{1}{n^\lambda})$, it follows by Fact A.6 and condition 1 that $|x| \leq \sqrt{2\lambda \cdot \log n}$ and hence, using condition 2 it follows that $|\varepsilon^+| < (\sqrt{2\lambda}+1) \cdot \sqrt{\frac{\log n}{n}}$. Therefore, Proposition A.8 yields that

$$\widehat{\mathcal{C}}_{n,\varepsilon^+}(0) \in \Phi(-\varepsilon^+ \cdot \sqrt{n}) \pm \varphi'(\sqrt{2\lambda}+1) \cdot \frac{\log^{1.5} n}{\sqrt{n}} \cdot e^{-\frac{\varepsilon^{+2} \cdot n}{2}} \tag{61}$$

$$= \Phi(x - \Delta) \pm \varphi'(\sqrt{2\lambda}+1) \cdot \frac{\log^{1.5} n}{\sqrt{n}} \cdot e^{-\frac{(x-\Delta)^2}{2}}$$

$$= \delta + \frac{1}{\sqrt{2\pi}} \cdot \int_{x-\Delta}^{x} e^{-\frac{t^2}{2}} dt \pm \varphi'(\sqrt{2\lambda}+1) \cdot \frac{\log^{1.5} n}{\sqrt{n}} \cdot e^{-\frac{(x-\Delta)^2}{2}}.$$

62

Note that

$$e^{-\frac{(x-\Delta)^2}{2}} - e^{-\frac{x^2}{2}} = (1 - e^{\frac{-2\Delta x + \Delta^2}{2}}) \cdot e^{-\frac{(x-\Delta)^2}{2}} \tag{62}$$

$$= (1 - e^{-2\Delta(\frac{x}{2} - \frac{\Delta}{4})}) \cdot e^{-\frac{(x-\Delta)^2}{2}}$$

$$\in (1 - e^{\pm 2\Delta \cdot \sqrt{2\lambda \cdot \log n}}) \cdot e^{-\frac{(x-\Delta)^2}{2}}$$

$$\subseteq \pm 4\Delta \cdot \sqrt{2\lambda \cdot \log n} \cdot e^{-\frac{(x-\Delta)^2}{2}},$$

where the third transition holds since $|x|, \Delta < \sqrt{2\lambda \cdot \log n}$, and the fourth one holds by the bound on Δ and using condition 2 since $e^y \in 1 \pm 2|y|$ for $y \in (-1, 1)$. Therefore,

$$\int_{x-\Delta}^{x} e^{-\frac{t^2}{2}} dt \in \Delta \cdot [\min(e^{-\frac{(x-\Delta)^2}{2}}, e^{-\frac{x^2}{2}}), \max(e^{-\frac{(x-\Delta)^2}{2}}, e^{-\frac{x^2}{2}})] \tag{63}$$

$$\in \Delta \cdot e^{-\frac{(x-\Delta)^2}{2}} \cdot (1 \pm 4\Delta \cdot \sqrt{2\lambda \cdot \log n}).$$

Applying Equation (63) on Equation (61) yields that

$$\widehat{\mathcal{C}}_{n,\varepsilon^+}(0) - \delta \in \frac{1}{\sqrt{2\pi}} \cdot \Delta \cdot e^{-\frac{(x-\Delta)^2}{2}} \cdot (1 \pm 4\Delta \cdot \sqrt{2\lambda \cdot \log n}) \pm \varphi'(\sqrt{2\lambda} + 1) \cdot \frac{\log^{1.5} n}{\sqrt{n}} \cdot e^{-\frac{(x-\Delta)^2}{2}}$$

$$= \frac{1}{\sqrt{2\pi}} \cdot \left(\Delta \pm \left(4\Delta^2 \cdot \sqrt{2\lambda \cdot \log n} + \sqrt{2\pi} \cdot \varphi'(\sqrt{2\lambda} + 1) \cdot \frac{\log^{1.5} n}{\sqrt{n}}\right)\right) \cdot e^{-\frac{(x-\Delta)^2}{2}}.$$

By the definition of φ and Δ, and using condition 2, it follows that

$$4\Delta^2 \cdot \sqrt{2\lambda \cdot \log n} + \sqrt{2\pi} \cdot \varphi'(\sqrt{2\lambda} + 1) \cdot \frac{\log^{1.5} n}{\sqrt{n}}$$

$$= 4\Delta \cdot \sqrt{2\lambda} \cdot \varphi(\lambda) \cdot \frac{\log^2 n}{\sqrt{n}} + \frac{\sqrt{2\pi}}{6}(\varphi(\lambda) - 1) \cdot \frac{\log^{1.5} n}{\sqrt{n}}$$

$$< 4\Delta \cdot \frac{1}{8} + \frac{1}{2}\Delta$$

$$= \Delta,$$

and thus, $\widehat{\mathcal{C}}_{n,\varepsilon^+}(0) > \delta$, as required. $\qquad\square$

In order to use Proposition A.9 with $\delta = \widehat{\mathcal{C}}_{n,\varepsilon}(k)$, the following proposition first estimate the value of $\Phi^{-1}(\delta)$.

Proposition A.10. *Let* $n \in \mathbb{N}$, $k \in \mathbb{Z}$, $\varepsilon \in [-1, 1]$ *and* $\lambda > 0$ *be such that* $|k| \le \lambda \cdot \sqrt{n \log n}$, $|\varepsilon| \le \lambda \cdot \sqrt{\frac{\log n}{n}}$, *and let* $\delta = \widehat{\mathcal{C}}_{n,\varepsilon}(k)$. *Then,*

$$\Phi^{-1}(\delta) \in \frac{k - \varepsilon n}{\sqrt{n}} \pm \mathsf{error},$$

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

Proof. Let $\varphi' \colon \mathbb{R}^+ \mapsto \mathbb{R}^+$ be the function from Proposition A.8, let $\Delta := 2\varphi'(\lambda) \cdot \log^{1.5} n$ and let $k_0 := k - \varepsilon n$. Note that there exists a function $\vartheta \colon \mathbb{R}^+ \mapsto \mathbb{N}$ such that $e^{-4\varphi'(\lambda)(\varphi'(\lambda)+\lambda)\cdot\frac{\log^3 n}{\sqrt{n}}} \geq \frac{1}{2}$ for every $n \geq \vartheta(\lambda)$. In the following we focus on $n \geq \vartheta(\lambda)$, where smaller n's are handled by setting the value of $\varphi(\lambda)$ to be large enough on these values.

We prove that $\Phi(\frac{k_0+\Delta}{\sqrt{n}}) \leq \delta \leq \Phi(\frac{k_0-\Delta}{\sqrt{n}})$, 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

$$\frac{\Delta}{\sqrt{n}} \cdot e^{-\frac{k_0^2}{2n}} \geq \varphi'(\lambda) \cdot \frac{\log^{1.5} n}{\sqrt{n}} \cdot e^{-\frac{k_0^2}{2n}} \tag{64}$$

and

$$\begin{aligned}
\frac{\Delta}{\sqrt{n}} \cdot e^{-\frac{(k_0-\Delta)^2}{2n}} &= \frac{\Delta}{\sqrt{n}} \cdot e^{-\frac{k_0^2}{2n}} \cdot e^{\frac{2k_0\Delta-\Delta^2}{2n}} \tag{65}\\
&\geq \frac{\Delta}{\sqrt{n}} \cdot e^{-\frac{k_0^2}{2n}} \cdot e^{-4\varphi'(\lambda)(\varphi'(\lambda)+\lambda)\cdot\frac{\log^3 n}{\sqrt{n}}}\\
&\geq \frac{\Delta}{\sqrt{n}} \cdot e^{-\frac{k_0^2}{2n}} \cdot \frac{1}{2}\\
&= \varphi'(\lambda) \cdot \frac{\log^{1.5} n}{\sqrt{n}} \cdot e^{-\frac{k_0^2}{2n}},
\end{aligned}$$

it follows that

$$\begin{aligned}
\delta &\leq \Phi(\frac{k_0}{\sqrt{n}}) + \varphi'(\lambda) \cdot \frac{\log^{1.5} n}{\sqrt{n}} \cdot e^{-\frac{k_0^2}{2n}} \tag{66}\\
&\leq \Phi(\frac{k_0}{\sqrt{n}}) + \frac{\Delta}{\sqrt{n}} \cdot \min(e^{-\frac{k_0^2}{2n}}, e^{-\frac{(k_0-\Delta)^2}{2n}})\\
&\leq \Phi(\frac{k_0}{\sqrt{n}}) + \int_{\frac{k_0-\Delta}{\sqrt{n}}}^{\frac{k_0}{\sqrt{n}}} e^{-\frac{t^2}{2}} dt\\
&= \Phi(\frac{k_0}{\sqrt{n}} - \frac{\Delta}{\sqrt{n}}),
\end{aligned}$$

where the first inequality holds by Proposition A.8 and the second one by Equation (64) and Equation (65). □

We are now ready for estimating the value of $\widehat{\mathcal{C}}_{n'}^{-1}(\delta)$ for $\delta = \widehat{\mathcal{C}}_{n,\varepsilon}(k)$ and for some $n' \geq n$.

Proposition A.11 (Restatement of Proposition 2.7)**.** *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*

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

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

Proof. Let φ_1 be the function from Proposition A.8, φ_2 be the function from Proposition A.9, φ_3 be the function from Proposition A.10 and let $\varphi(\lambda) := \varphi_2(2\lambda^2 + 1) + \varphi_3(\lambda)$. There exists a function $\vartheta \colon \mathbb{R}^+ \mapsto \mathbb{N}$ such that the two conditions

1. $\min(\lambda, 1) \cdot \log n > 4$

2. $\max(\lambda, \varphi_1(\lambda)) \cdot \frac{\log^2 n}{\sqrt{n}} < \frac{1}{8}$

holds for every $n \geq \vartheta(\lambda)$. In the following we focus on $n \geq \vartheta(\lambda)$, where smaller n's are handled by setting the value of $\varphi(c)$ to be large enough on these values. In order to use Proposition A.9, we first prove that $\delta \in (\frac{1}{n^{2\lambda^2+1}}, 1 - \frac{1}{n^{2\lambda^2+1}})$. Let $k_0 := k - \varepsilon n$. For simplicity, we assume $k_0 \geq 0$, whereas the case $k_0 < 0$ holds by symmetry. Compute

$$\delta \in \Phi\left(\frac{k_0}{\sqrt{n}}\right) \pm \varphi_1(\lambda) \cdot \frac{\log^{1.5} n}{\sqrt{n}} \cdot e^{-\frac{k_0^2}{2n}} \tag{67}$$

$$\subseteq \left(\frac{1}{\frac{k_0}{\sqrt{n}} + \sqrt{\frac{k_0^2}{n} + 4} \pm 2} \pm \varphi_1(\lambda) \cdot \frac{\log^{1.5} n}{\sqrt{n}}\right) \cdot e^{-\frac{k_0^2}{2n}},$$

$$\subseteq \frac{1 \pm \frac{1}{2}}{\frac{k_0}{\sqrt{n}} + \sqrt{\frac{k_0^2}{n} + 4} \pm 2} \cdot e^{-\frac{k_0^2}{2n}}$$

$$\subseteq \left(\frac{1}{8\lambda \cdot \sqrt{\log n} \cdot n^{2\lambda^2}}, \frac{3}{4}\right)$$

$$\subseteq \left(\frac{1}{n^{2\lambda^2+1}}, 1 - \frac{1}{n^{2\lambda^2+1}}\right)$$

where the first transition holds by Proposition A.8, the second one holds by Fact A.6, the third one holds by condition 2 and since $k_0 \leq 2\lambda \cdot \sqrt{n \log n}$, the fourth one also holds since $k_0 \leq 2\lambda \cdot \sqrt{n \log n}$ and the last one holds by conditions 1 and 2.

Finally, it holds that

$$\widehat{\mathcal{C}}_{n'}^{-1}(\delta) \in -\frac{\Phi^{-1}(\delta)}{\sqrt{n'}} \pm \varphi_2(2\lambda^2 + 1) \cdot \frac{\log^{1.5}(n')}{n'} \tag{68}$$

$$\subseteq -\frac{\left(\frac{k - \varepsilon n}{\sqrt{n}} \pm \varphi_3(\lambda) \cdot \frac{\log^{1.5} n}{\sqrt{n}}\right)}{\sqrt{n'}} \pm \varphi_2(2\lambda^2 + 1) \cdot \frac{\log^{1.5}(n')}{n'}$$

$$\subseteq \frac{\varepsilon n - k}{\sqrt{n \cdot n'}} \pm \varphi(\lambda) \cdot \frac{\log^{1.5} n}{\sqrt{n \cdot n'}},$$

where the first transition holds by Proposition A.9, the second one by Proposition A.10 and the last one holds since $n \leq n'$. $\square$

For the following two propositions, recall that for $n \in \mathbb{N}$ and $i \in [n]$ we let $\ell_n(i) = n - i + 1$ and $\mathsf{sum}_n(i) = \sum_{j=i}^{n} \ell_n(i) = \frac{1}{2} \cdot \ell_n(i)(\ell_n(i) + 1)$. The following proposition is the main step towards proving Proposition 2.8.

Proposition A.12. *Let $n \in \mathbb{N}$, integer $i \in [n - \lfloor \log^{2.5} n \rfloor]$, $x, \beta, \alpha \in \mathbb{Z}$, $\varepsilon \in [-1, 1]$ and $\lambda > 0$ be such that $|\alpha| \leq \sqrt{\lambda \cdot \mathsf{sum}_n(i) \cdot \log n}$, $|x| \leq \sqrt{\lambda \cdot \ell_n(i) \cdot \log n}$, $|\beta| \leq 1$ and $|\varepsilon| \leq \sqrt{\lambda \cdot \frac{\log n}{\mathsf{sum}_n(i)}}$. Then*

$$\exp\left(\frac{\alpha \cdot x + \beta \cdot x^2}{\mathsf{sum}_n(i+1)}\right) \in 1 \pm \varphi(\lambda) \cdot \frac{\sqrt{\log n} \cdot |x|}{\ell_n(i)},$$

for a universal function φ.

Proof. Assume that $n \geq 4$. By taking the maximum possible values of $|\alpha|$, $|\beta|$ and $|x|$ it follows that

$$\left| \frac{\alpha \cdot x + \beta \cdot x^2}{\mathsf{sum}_n(i+1)} \right| \leq \frac{\sqrt{\lambda \cdot \mathsf{sum}_n(i) \cdot \log n} \cdot \sqrt{\lambda \cdot \ell_n(i) \cdot \log n} + \lambda \cdot \ell_n(i) \cdot \log n}{\mathsf{sum}_n(i+1)} \tag{69}$$

$$= \lambda \cdot \frac{\sqrt{2(n - i + 2)}}{n - i} \cdot \log n + 2\lambda \cdot \frac{\log n}{n - i}$$

$$\leq 2\lambda \cdot \frac{\log n}{\sqrt{n - i}} + 2\lambda \cdot \frac{\log n}{n - i}$$

$$\leq 2\lambda \cdot \frac{1}{\log^{0.25} n} + 2\lambda \cdot \frac{1}{\log^{1.5} n},$$

where the second inequality holds since $\frac{n-i+2}{n-i} < 2$. Therefore, there exists a function $\vartheta \colon \mathbb{R}^+ \mapsto \mathbb{N}$ such that $\left| \frac{\alpha \cdot x + \beta \cdot x^2}{\mathsf{sum}_n(i+1)} \right| < 1$ for every $n \geq \vartheta(\lambda)$. In the following we focus on $n \geq \vartheta(\lambda)$, where smaller n's are handled by setting the value of $\varphi(\lambda)$ to be large enough on these values. Since $e^y \in 1 \pm 2\,|y|$ for $y \in [-1, 1]$, it follows that

$$\exp\left(\frac{\alpha \cdot x + \beta \cdot x^2}{\mathsf{sum}_n(i+1)}\right) \in 1 \pm 2 \cdot \left| \frac{\alpha \cdot x + \beta \cdot x^2}{\mathsf{sum}_n(i+1)} \right|$$

$$\subseteq 1 \pm 4 \cdot \left| \frac{\alpha \cdot x + \beta \cdot x^2}{\mathsf{sum}_n(i)} \right|$$

$$\subseteq 1 \pm 4 \cdot \left(\frac{|\alpha| \cdot |x| + |\beta| \cdot x^2}{\mathsf{sum}_n(i)} \right)$$

$$\subseteq 1 \pm 4 \cdot \left(\frac{\sqrt{\lambda \cdot \mathsf{sum}_n(i) \cdot \log n} \cdot |x| + x^2}{\mathsf{sum}_n(i)} \right)$$

$$\subseteq 1 \pm 4 \cdot \left(\sqrt{\frac{\lambda \cdot \log n}{\mathsf{sum}_n(i)}} \cdot |x| + \frac{\sqrt{\lambda \cdot \ell_n(i) \cdot \log n}}{\mathsf{sum}_n(i)} \cdot |x| \right)$$

$$= 1 \pm 4 \cdot \left(\sqrt{\frac{\lambda \cdot \log n}{\frac{1}{2}\ell_n(i)(\ell_n(i) + 1)}} \cdot |x| + \frac{\sqrt{\lambda \cdot \ell_n(i) \cdot \log n}}{\frac{1}{2}\ell_n(i)(\ell_n(i) + 1)} \cdot |x| \right)$$

$$\subseteq 1 \pm 8 \cdot \sqrt{\frac{\lambda \cdot \log n}{\ell_n(i)}} \left(\frac{|x|}{\sqrt{\ell_n(i)}} + \frac{|x|}{\ell_n(i)} \right)$$

$$\subseteq 1 \pm 16\sqrt{\lambda} \cdot \frac{\sqrt{\log n} \cdot |x|}{\ell_n(i)},$$

where the second transitions holds since $\frac{\mathsf{sum}_n(i)}{\mathsf{sum}_n(i+1)} < 2$, the fourth one holds by taking the maximum possible values of $|\alpha|$ and $|\beta|$ and fifth one by taking the maximum possible value of $|x|$. $\qquad \square$

Using the above fact, we can prove Proposition 2.8.

Proposition A.13 (Restatement of Proposition 2.8). *Let $n \in \mathbb{N}$, integer $i \in [n - \lfloor \log^{2.5} n \rfloor]$, $x, \beta, \beta', \alpha, \alpha' \in \mathbb{Z}$, $\varepsilon \in [-1, 1]$, $\mathcal{S} \subseteq \mathbb{Z}$ and $\lambda > 0$ such that $|\alpha|, |\alpha'| \leq \sqrt{\lambda \cdot \mathsf{sum}_n(i) \cdot \log n}$, $|\beta|, |\beta'| \leq 1$, $\mathcal{S} \subseteq [-\sqrt{\lambda \cdot \ell_n(i) \cdot \log n}, \sqrt{\lambda \cdot \ell_n(i) \cdot \log n}]$, $x \in \mathcal{S}$, $|\varepsilon| \leq \sqrt{\lambda \cdot \frac{\log n}{\mathsf{sum}_n(i)}}$ and $\mathrm{E}_{x' \leftarrow \mathcal{C}_{\ell_n(i),\varepsilon} | x' \in \mathcal{S}} [|x'|] \leq \mathrm{E}_{x' \leftarrow \mathcal{C}_{\ell_n(i),\varepsilon}} [|x'|]$. Then*

$$\mathop{\mathrm{E}}_{x' \leftarrow \mathcal{C}_{\ell_n(i),\varepsilon} | x' \in \mathcal{S}} \left[\exp \left(\frac{\alpha \cdot x + \beta \cdot x^2 + \alpha' \cdot x' + \beta' \cdot x'^2}{\mathsf{sum}_n(i+1)} \right) \right] \in 1 \pm \varphi(\lambda) \cdot \sqrt{\frac{\log n}{\ell_n(i)}} \left(1 + \frac{|x|}{\sqrt{\ell_n(i)}} \right).$$

for a universal function φ.

Proof. Let φ' be the function from Proposition A.12. Compute

$$
\begin{aligned}
& \mathop{\mathrm{E}}_{x' \leftarrow \mathcal{C}_{\ell_n(i),\varepsilon} | x' \in \mathcal{S}} \left[\exp \left(\frac{\alpha \cdot x + \beta \cdot x^2 + \alpha' \cdot x' + \beta' \cdot x'^2}{\mathsf{sum}_n(i+1)} \right) \right] \\
&= \exp \left(\frac{\alpha \cdot x + \beta \cdot x^2}{\mathsf{sum}_n(i+1)} \right) \cdot \mathop{\mathrm{E}}_{x' \leftarrow \mathcal{C}_{\ell_n(i),\varepsilon} | x' \in \mathcal{S}} \left[\left(\frac{\alpha' \cdot x' + \beta' \cdot x'^2}{\mathsf{sum}_n(i+1)} \right) \right] \\
&\in \left(1 \pm \varphi'(\lambda) \cdot \frac{\sqrt{\log n} \cdot |x|}{\ell_n(i)} \right) \cdot \mathop{\mathrm{E}}_{x' \leftarrow \mathcal{C}_{\ell_n(i),\varepsilon} | x' \in \mathcal{S}} \left[1 \pm \varphi'(\lambda) \cdot \frac{\sqrt{\log n} \cdot |x'|}{\ell_n(i)} \right] \\
&= \left(1 \pm \varphi'(\lambda) \cdot \frac{\sqrt{\log n} \cdot |x|}{\ell_n(i)} \right) \cdot \left(1 \pm \varphi'(\lambda) \cdot \frac{\sqrt{\log n} \cdot \mathrm{E}_{x' \leftarrow \mathcal{C}_{\ell_n(i),\varepsilon} | x' \in \mathcal{S}} [|x'|]}{\ell_n(i)} \right) \\
&\subseteq \left(1 \pm \varphi'(\lambda) \cdot \frac{\sqrt{\log n} \cdot |x|}{\ell_n(i)} \right) \cdot \left(1 \pm 2\varphi'(\lambda) \cdot \sqrt{\frac{\log n}{\ell_n(i)}} \right) \\
&\subseteq 1 \pm 4(\varphi'(\lambda) + \varphi'(\lambda)^2) \cdot \sqrt{\frac{\log n}{\ell_n(i)}} \cdot \left(1 + \frac{|x|}{\sqrt{\ell_n(i)}} \right),
\end{aligned}
$$

where the second transition holds by Proposition A.12 and the fourth one holds by Fact 2.3. $\qquad\square$

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 $w(v) = p$. The following proposition gives an estimation for the hypergeometric probability $\mathcal{HG}_{2n,p,n}(t)$ using the binomial coefficient's estimation done in Proposition A.2.

Proposition A.14 (Restatement of Proposition 2.10). *Let $n \in \mathbb{N}$, $p, t \in \mathbb{Z}$ be such that $|p|, |t| \leq n^{\frac{3}{5}}$ and $t \in \mathrm{Supp}(\mathcal{HG}_{2n,p,n})$. Then*

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

for $\mathsf{error} = \xi \cdot \left(\frac{n + |p|^3 + |t|^3}{n^2} \right)$ and a universal constant ξ.

Proof. Let ξ_1 be the constant from Proposition A.2 and let $\omega := \frac{p}{2}$. In the following we focus on $n \geq 1000(1 + \xi_1^2)$, smaller n's are handled by setting the value of ξ to be large enough on these values. Note that for any vector $v \in \{-1, 1\}^{2n}$ with $w(v) = p$, the number of ones in v is $n + \omega$. It follows that

$$\mathcal{HG}_{2n,p,n}(t) = \frac{\binom{n+\omega}{\frac{n+t}{2}} \cdot \binom{n-\omega}{\frac{n-t}{2}}}{\binom{2n}{n}} \tag{70}$$

$$= \frac{\binom{n+\omega}{\frac{n+\omega}{2} + \frac{t-\omega}{2}} \cdot \binom{n-\omega}{\frac{n-\omega}{2} - \frac{t-\omega}{2}}}{\binom{2n}{n}}$$

$$\in \frac{\sqrt{\frac{2}{\pi}}(1 \pm \xi_1 \cdot (\frac{1}{n} + \frac{|t-\omega|^3}{n^2}))\frac{1}{\sqrt{n+\omega}}e^{-\frac{(t-\omega)^2}{2(n+\omega)}} \cdot \sqrt{\frac{2}{\pi}} \cdot (1 \pm \xi_1 \cdot (\frac{1}{n} + \frac{|t-\omega|^3}{n^2}))\frac{1}{\sqrt{n-\omega}}e^{-\frac{(t-\omega)^2}{2(n-\omega)}}}{\sqrt{\frac{2}{\pi}} \cdot (1 \pm \xi_1 \cdot \frac{1}{n})\frac{1}{\sqrt{2n}}}$$

$$\subseteq \sqrt{\frac{2}{\pi}} \cdot (1 \pm \xi_2 \cdot (\frac{1}{n} + \frac{|t-\omega|^3}{n^2})) \cdot A(n, t, \omega),$$

where the third transition holds by Proposition A.2, $\xi_2 := 8 \cdot (\xi_1 + \xi_1^2)$ and $A(n, t, \omega) := \sqrt{2n} \cdot \frac{1}{\sqrt{n+\omega}}e^{-\frac{(t-\omega)^2}{2(n+\omega)}} \cdot \frac{1}{\sqrt{n-\omega}}e^{-\frac{(t-\omega)^2}{2(n-\omega)}}$. Compute

$$A(n, t, \omega) = \sqrt{\frac{2}{n}} \cdot \frac{n}{\sqrt{n+\omega} \cdot \sqrt{n-\omega}} \cdot e^{-\frac{(t-\omega)^2}{2(n+\omega)}} \cdot e^{-\frac{(t-\omega)^2}{2(n-\omega)}} \tag{71}$$

$$= \sqrt{\frac{2}{n}} \cdot \frac{1}{\sqrt{1 - \frac{\omega^2}{n^2}}} \cdot e^{-\frac{(t-\omega)^2}{n}} \cdot e^{-(t-\omega)^2(\frac{1}{2(n+\omega)} + \frac{1}{2(n-\omega)} - \frac{1}{n})}$$

$$\in \sqrt{\frac{2}{n}} \cdot \left(1 \pm 2 \cdot \frac{\omega^2}{n^2}\right) \cdot e^{-\frac{(t-\omega)^2}{n}} \cdot e^{-\frac{(t-\omega)^2\omega^2}{n(n^2-\omega^2)}}$$

$$\subseteq \sqrt{\frac{2}{n}} \cdot e^{-\frac{(t-\omega)^2}{n}} \cdot \left(1 \pm 2 \cdot \frac{\omega^2}{n^2}\right) \cdot \left(1 \pm 2 \cdot \frac{(t-\omega)^2\omega^2}{n(n^2-\omega^2)}\right)$$

$$\subseteq \sqrt{\frac{2}{n}} \cdot e^{-\frac{(t-\omega)^2}{n}} \cdot \left(1 \pm 4 \cdot (\frac{(t-\omega)^2\omega^2}{n^3} + \frac{\omega^2}{n^2})\right),$$

where the third transition holds since $\frac{1}{\sqrt{1-x}} \in 1 \pm 2x$ for $x \in [0, \frac{1}{4}]$, and the fourth one holds since $e^x \in 1 \pm 2x$ for $|x| < 1$.

We conclude from Equations (70) and (71) that

$$\mathcal{HG}_{2n,p,n}(t) \in \sqrt{\frac{2}{\pi}} \cdot (1 \pm \xi_3 \cdot (\frac{n + |\omega|^3 + |t|^3}{n^2})) \cdot \sqrt{\frac{2}{n}} \cdot e^{-\frac{(t-\omega)^2}{n}}$$

$$\in (1 \pm \xi \cdot (\frac{n + |p|^3 + |t|^3}{n^2})) \cdot \frac{2}{\sqrt{\pi \cdot n}} \cdot e^{-\frac{(t-\frac{p}{2})^2}{n}},$$

where $\xi_3 := 16 \cdot (1 + \xi_2)$ and $\xi := 8 \cdot \xi_3$. $\qquad\square$

Using the above estimation for the hypergeometric probability, the following proposition estimates the relation between two hypergeometric probabilities.

Proposition A.15 (Restatement of Proposition 2.11)**.** *Let $n \in \mathbb{N}$, $p, t, x, x' \in \mathbb{Z}$ and $\lambda > 0$ be such that $t - x, t - x' \in \mathrm{Supp}(\mathcal{HG}_{2n,p,n})$ and $|p|, |t|, |x|, |x'| \leq \lambda \cdot \sqrt{n \log n}$. Then*

$$\frac{\mathcal{HG}_{2n,p,n}(t - x')}{\mathcal{HG}_{2n,p,n}(t - x)} \in (1 \pm \mathsf{error}) \cdot \exp\left(\frac{-2(t - \frac{p}{2})x + x^2 + 2(t - \frac{p}{2})x' - x'^2}{n}\right),$$

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

Proof. Let ξ be the constant from Proposition A.14. There exists a function $\vartheta \colon \mathbb{R}^+ \mapsto \mathbb{N}$ such that $n^{\frac{3}{5}} > 2\lambda \cdot \sqrt{n \log n}$ and $\xi \cdot (10\lambda^3 + 1) \cdot \frac{\log^{1.5} n}{\sqrt{n}} < \frac{1}{2}$ for every $n \geq \vartheta(\lambda)$. In the following we focus on $n \geq \vartheta(\lambda)$, where smaller n's are handled by setting the value of $\varphi(\lambda)$ to be large enough on these values. Let $\varphi(\lambda) := 4 \cdot \xi \cdot (10\lambda^3 + 1)$. It follows that

$$\frac{\mathcal{HG}_{2n,p,n}(t - x')}{\mathcal{HG}_{2n,p,n}(t - x)} \in \frac{\left(1 \pm \xi \cdot \frac{n + |p|^3 + |t - x'|^3}{n^2}\right) \cdot \frac{2}{\sqrt{\pi \cdot n}} \cdot e^{-\frac{(t - \frac{p}{2} - x')^2}{n}}}{\left(1 \pm \xi \cdot \frac{n + |p|^3 + |t - x'|^3}{n^2}\right) \cdot \frac{2}{\sqrt{\pi \cdot n}} \cdot e^{-\frac{(t - \frac{p}{2} - x)^2}{n}}}$$

$$\subseteq \frac{\left(1 \pm \xi \cdot (10\lambda^3 + 1) \cdot \frac{\log^{1.5} n}{\sqrt{n}}\right) \cdot e^{-\frac{(t - \frac{p}{2} - x')^2}{n}}}{\left(1 \pm \xi \cdot (10\lambda^3 + 1) \cdot \frac{\log^{1.5} n}{\sqrt{n}}\right) \cdot e^{-\frac{(t - \frac{p}{2} - x)^2}{n}}}$$

$$\subseteq (1 \pm \varphi(\lambda) \cdot \frac{\log^{1.5} n}{\sqrt{n}}) \cdot \exp\left(\frac{(t - \frac{p}{2} - x)^2}{n} - \frac{(t - \frac{p}{2} - x')^2}{n}\right)$$

$$= (1 \pm \varphi(\lambda) \cdot \frac{\log^{1.5} n}{\sqrt{n}}) \cdot \exp\left(\frac{-2 \cdot (t - \frac{p}{2}) \cdot x + x^2 + 2 \cdot (t - \frac{p}{2}) \cdot x' - x'^2}{n}\right),$$

where the first transition holds by Proposition A.14, the second one holds by the bounds on $|t|, |x|$, $|x'|$ and $|p|$, and the third one holds since $\frac{1 \pm y}{1 \pm y} \subseteq 1 \pm 4y$ for every $y \in [0, \frac{1}{2}]$. $\square$