Estimating Gaps in Martingales and Applications to Coin-Tossing: Constructions & Hardness

Hamidreza Amini Khorasgani
Department of Computer Science, Purdue University, IN, USA
haminikh@purdue.edu

Hemanta K. Maji
Department of Computer Science, Purdue University, IN, USA
hmaji@purdue.edu

Tamalika Mukherjee
Department of Computer Science, Purdue University, IN, USA
tmukherj@purdue.edu

Abstract

Consider the representative task of designing a distributed coin-tossing protocol for n processors such that the probability of heads is $X_0 \in [0,1]$, and an adversary can reset one processor to change the distribution of the final outcome. For $X_0 = 1/2$, in the non-cryptographic setting, no adversary can deviate the probability of the outcome of the well-known Blum's "majority protocol" by more than $\frac{1}{\sqrt{2\pi n}}$, i.e., it is $\frac{1}{\sqrt{2\pi n}}$ insecure. For computationally bounded adversaries and any $X_0 \in [0,1]$, the protocol of Moran, Naor, and Segev (2009) is only $O\left(\frac{1}{n}\right)$ insecure.

In this paper, we study discrete-time martingales $(X_0, X_1, \ldots, X_n)$ such that $X_i \in [0,1]$, for all $i \in \{0,\ldots,n\}$, and $X_n \in \{0,1\}$. These martingales are commonplace in modeling stochastic processes like coin-tossing protocols in the non-cryptographic setting mentioned above. In particular, for any $X_0 \in [0,1]$, we construct martingales that yield $\frac{1}{2}\sqrt{\frac{X_0(1-X_0)}{n}}$ insecure coin-tossing protocols with n-bit communication; irrespective of the number of bits required to represent the output distribution. Note that for sufficiently small X_0, we achieve higher security than Moran et al.'s protocol even against computationally unbounded adversaries. For $X_0 = 1/2$, our protocol requires only 40% of the processors to achieve the same security as the majority protocol.

The technical heart of our paper is a new inductive technique that uses geometric transformations to precisely account for the large gaps in these martingales. For any $X_0 \in [0,1]$, we show that there exists a stopping time τ such that

$$\mathbb{E}\left[|X_\tau - X_{\tau-1}|\right] \geqslant \frac{2}{\sqrt{2n-1}} \cdot X_0(1-X_0)$$

The inductive technique simultaneously constructs martingales that demonstrate the optimality of our bound, i.e., a martingale where the gap corresponding to any stopping time is small. In particular, we construct optimal martingales such that *any* stopping time τ has

$$\mathbb{E}\left[|X_\tau - X_{\tau-1}|\right] \leqslant \frac{1}{\sqrt{n}} \cdot \sqrt{X_0(1-X_0)}$$

Our lower-bound holds for all $X_0 \in [0,1]$; while the previous bound of Cleve and Impagliazzo (1993) exists only for positive constant X_0. Conceptually, our approach only employs elementary techniques to analyze these martingales and entirely circumvents the complex probabilistic tools inherent to the approaches of Cleve and Impagliazzo (1993) and Beimel, Haitner, Makriyannis, and Omri (2018).

By appropriately restricting the set of possible stopping-times, we present representative applications to constructing distributed coin-tossing/dice-rolling protocols, discrete control processes, fail-stop attacking coin-tossing/dice-rolling protocols, and black-box separations.

2012 ACM Subject Classification Mathematics of computing → Markov processes; Security and privacy → Information-theoretic techniques; Security and privacy → Mathematical foundations of cryptography

Keywords and phrases Discrete-time Martingale, Coin-tossing and Dice-rolling Protocols, Discrete Control Processes, Fair Computation, Black-box Separation

Funding The research effort is supported in part by an NSF CRII Award CNS–1566499, an NSF SMALL Award CNS–1618822 (REUs CNS–1724673 and CNS–1833916), the IARPA HECTOR project, MITRE Innovation Program Academic Cybersecurity Research Award, a Center for Science of Information (CSoI) Seed Fund, and a Purdue Research Foundation (PRF) Award.

Contents

1 Introduction

A Representative Motivating Application. Consider a distributed protocol for n processors to toss a coin, where processor i broadcasts her message in round i. At the end of the protocol, all processors reconstruct the common outcome from the public transcript. When all processors are honest, the probability of the final outcome being 1 is X_0 and the probability of the final outcome being 0 is $1 - X_0$, i.e., the final outcome is a *bias-X_0 coin*. Suppose there is an adversary who can (adaptively) choose to *restart* one of the processors; otherwise her presence is innocuous. Our objective is to design bias-X_0 coin-tossing protocols with low communication complexity such that the adversary cannot change the distribution of the final outcome significantly.

The Majority Protocol. Against computationally unbounded adversaries, (essentially) the only known protocol is the well-known majority protocol [11, 6, 14] for $X_0 = 1/2$. The majority protocol requests one uniformly random bit from each processor and the final outcome is the majority of these n bits. An adversary can alter the probability of the final outcome being 1 by $\frac{1}{\sqrt{2\pi n}}$, i.e., the majority protocol is $\frac{1}{\sqrt{2\pi n}}$ insecure.

To construct a bias-X_0 coin, where X_0 has a t-bit binary representation, we compose t majority protocols in parallel. This protocol has $t \cdot n$-bit communication complexity and continues to be $\frac{1}{\sqrt{2\pi n}}$ insecure. If X_0 does not have a t-bit binary representation (for example, say, $X_0 = 1/3$, $X_0 = 1/\mathrm{e}$, or $X_0 = 1/n$) then we construct a bias-X_0' coin, where X_0' is the t-bit truncation of X_0. This protocol has $t \cdot n$-communication complexity and is $\frac{1}{2^{t+1}} + \frac{1}{\sqrt{2\pi n}}$ insecure. That is, we must have $t = \Omega(\log n)$ for the protocol to be $O\left(\frac{1}{\sqrt{n}}\right)$ insecure.

Alternatively, we can partition the processors into t groups and each group generates one bit using the majority protocol. This protocol has n-bit communication and $\frac{1}{2^{t+1}} + \frac{\sqrt{t}}{\sqrt{2\pi n}}$ insecurity. However, this protocol shall reduce the security of the protocol by $t = \Omega(\log n)$ factor, which is not desirable.

The MNS Protocol. Against computationally bounded adversaries, for any $X_0 \in [0, 1]$, Moran, Naor, and Segev [29] construct a bias-X_0 coin that is $O\left(\frac{1}{n}\right)$ insecure with linear communication complexity (based on general MPC with linear communication complexity [2]).

Our New Protocol. We shall prove a general martingale result in this paper that yields the following result as a corollary. For any $X_0 \in [0, 1]$, there exists an n-bit bias-X_0 coin-tossing protocol in the non-cryptographic setting that is $\frac{1}{2}\sqrt{\frac{X_0(1-X_0)}{n}}$ insecure; irrespective of the number of bits required to represent X_0. In the sequel, we highlight some consequences of our result. For sufficiently small X_0, our coin-tossing protocol is more secure than the MNS protocol [29] even in the non-cryptographic setting. For example, when $X_0 = \frac{1}{n^{1+2\varepsilon}}$ and $\varepsilon \geqslant 0$ is any constant, our bias-X_0 protocol is $\frac{1}{2 \cdot n^{1+\varepsilon}}$ insecure.[1] The solutions using the "majority protocol" as discussed above have $\Omega(n \lg n)$ communication complexity and $O(1/\sqrt{n})$ insecurity; a significantly worse solution. Next, for $X_0 = 1/2$, our protocol uses only 625 processors to reduce the insecurity to, say, 1%; while the majority protocol requires 1592 processors. In general, building upon these protocols, we construct any ω-faceted dice-rolling functionality (the final outcome is distributed over the set $\{0, 1, \ldots, \omega - 1\}$) with n-bit communication that is $\frac{d^{3/2}}{4\sqrt{n}}$ insecure, where $d = \lceil \lg \omega \rceil$.

A Representative Application of Dice-Rolling. Consider a distributed *leader election*

[1] It is evident that any adversary cannot decrease the probability of output being 1 by $X_0 = \frac{1}{n^{1+2\varepsilon}}$. Furthermore, in our protocol, no adversary can increase the probability of the output being 1 by $\frac{1}{n^{1+\varepsilon}}$ as well.

protocol for n processors where the probability of a processor being elected the leader is proportional to its computational power. Because, a faster processor is more likely to have the additional bandwidth to accommodate the overhead of performing the tasks of the leader. We do not want an adversary to *significantly change* the probability of the leader belonging to any (proper) subset of the processors by restarting at most one processor. This task corresponds to a distributed dice-rolling protocol with $\omega = n$. The complexity of representing the distribution of the final outcome (roughly) depends on the ratio of the minimum to the maximum computational power of the processors. If this ratio is $\ll 1/\text{poly}(n)$, then the solutions using the "majority protocol" discussed above shall require $t \gg \log n$. Consequently, their communication complexity or insecurity is not sufficiently small. Our protocols, on the other hand, use n-bit communication and are $\frac{(\lg n)^{3/2}}{4\sqrt{n}}$ insecure.

Formal Framework: Martingales. Martingales are natural models for several stochastic processes. Intuitively, martingales correspond to a gradual release of information about an event. A priori, we know that the probability of the event is X_0. For instance, in a distributed n-party coin-tossing protocol the outcome being 1 is the event of interest. A discrete-time martingale $(X_0, X_1, \ldots, X_n)$ represents the gradual release of information about the event over n time-steps.[2]

For intuition, we can assume that X_i represents the probability that the outcome of the coin-tossing protocol is 1 after the first i parties have broadcast their messages. Martingales have the unique property that if we compute the expected value of X_j, for $j > i$, at the end of time-step i, it is identical to the value of X_i. In this paper we shall consider martingales where, at the end of time-step n, we know for sure whether the event of interest has occurred or not. That is, we have $X_n \in \{0, 1\}$.

A *stopping time* τ represents a time step $\in \{1, 2, \ldots, n\}$ where we stop the evolution of the martingale. The test of whether to stop the martingale at time-step i is a function only of the information revealed so far. Furthermore, this stopping time need *not* be a constant. That is, for example, different transcripts of the coin-tossing protocol potentially have different stopping times.

Our Martingale Problem Statement. The inspiration of our approach is best motivated using a two-player game between, namely, the *martingale designer* and the *adversary*. Fix n and X_0. The martingale designer presents a martingale $\mathcal{X} = (X_0, X_1, \ldots, X_n)$ to the adversary and the adversary finds a stopping time τ that maximizes the following quantity.

$$\mathbb{E}\left[|X_\tau - X_{\tau-1}|\right]$$

Intuitively, the adversary demonstrates the most severe *susceptibility* of the martingale by presenting the corresponding stopping time τ as a witness. The martingale designer's objective is to design martingales that have less susceptibility. Our research uses a geometric approach to inductively provide tight bounds on the least susceptibility of martingales for all $n \geqslant 1$ and $X_0 \in [0, 1]$, that is, the following quantity.

$$C_n(X_0) := \inf_{\mathcal{X}} \sup_{\tau} \mathbb{E}\left[|X_\tau - X_{\tau-1}|\right]$$

This precise study of $C_n(X_0)$, for general $X_0 \in [0, 1]$, is motivated by natural applications in discrete process control as illustrated by the representative motivating problem. This paper, for representative applications of our results, considers n-processor distributed protocols and

[2] For the introduction, we do not explicitly mention the underlying filtration for brevity. The proofs, however, clearly mention the underlying filtration.

2-party n-round protocols. The stopping time witnessing the highest susceptibility shall translate into appropriate adversarial strategies.

1.1 Our Contributions

We prove the following general martingale theorem.

▶ **Theorem 1.** *Let $(X_0, X_1, \ldots, X_n)$ be a discrete-time martingale such that $X_i \in [0,1]$, for all $i \in \{1, \ldots, n\}$, and $X_n \in \{0,1\}$. Then, the following bound holds.*

$$\sup_{\text{stopping time } \tau} \mathbb{E}\left[|X_\tau - X_{\tau-1}|\right] \geqslant C_n(X_0),$$

where $C_1(X) = 2X(1-X)$, and, for $n > 1$, we obtain C_n from C_{n-1} recursively using the geometric transformation defined in Figure 7.

Furthermore, for all $n \geqslant 1$ and $X_0 \in [0,1]$, there exists a martingale $(X_0, \ldots, X_n)$ (w.r.t. to the coordinate exposure filtration[3] for $\{0,1\}^n$) such that for any stopping time τ, it has $\mathbb{E}\left[|X_\tau - X_{\tau-1}|\right] = C_n(X_0)$.

Intuitively, given a martingale, an adversary can identify a stopping time where the expected gap in the martingale is at least $C_n(X_0)$. Moreover, there exists a martingale that realizes the lower-bound in the tightest manner, i.e., all stopping times τ have identical susceptibility.

Next, we estimate the value of the function $C_n(X)$.

▶ **Lemma 2.** *For $n \geqslant 1$ and $X \in [0,1]$, we have*

$$\frac{2}{\sqrt{2n-1}} \cdot X(1-X) =: L_n(X) \leqslant C_n(X) \leqslant U_n(X) := \frac{1}{\sqrt{n}} \cdot \sqrt{X(1-X)}$$

In the sequel, we highlight applications of Theorem 1 to protocol constructions and hardness of computation results using these estimates.

▶ Remark 3 (Protocol Constructions). The optimal martingales naturally translate into n-bit distributed coin-tossing and multi-faceted dice rolling protocols.

1. Corollary 11: For all $X_0 \in [0,1]$, there exists an n-bit distributed bias-X_0 coin-tossing protocol for n processors with the following security guarantee. Any (computationally unbounded) adversary who follows the protocol honestly and resets at most one of the processors during the execution of the protocol can change the probability of an outcome by at most $\frac{1}{2\sqrt{n}} \cdot \sqrt{X_0(1-X_0)}$. Section 1 discusses the comparison of this construction with existing algorithms.
2. Corollary 12: A distributed ω-faceted dice-rolling protocol helps n processors agree on a symbol from the set $\{0, 1, \ldots, \omega-1\}$. For an arbitrary distribution of the final outcome over the set $\{0, 1, \ldots, \omega-1\}$, we present an n-bit protocol where any adversary can change the probability of any subset of outcomes by at most $\frac{d^{3/2}}{4\sqrt{n}}$, where $d = \lceil \lg \omega \rceil$.

Observe that the communication complexity of all our constructions are independent of the complexity of representing the distribution of the final outcome.

▶ Remark 4 (Hardness of Computation Results). The lower-bound on the maximum susceptibility helps demonstrate hardness of computation results. For $X_0 = 1/2$, [15] proved that we encounter $|X_\tau - X_{\tau-1}| \geqslant \frac{1}{32\sqrt{n}}$ with probability $\frac{1}{5}$. In other words, their bound guarantees

[3] The coordinate exposure filtration reveals one bit at a time of the final outcome.

that the expected gap in the martingale is at least $\frac{1}{160\sqrt{n}}$, which is significantly smaller than our bound $\frac{1}{2\sqrt{2n}}$.

Hardness of computation results relying on [15] (and its extensions) work only for constant $0 < X_0 < 1$. However, our lower-bound holds for all $X_0 \in [0,1]$; for example, even when $1/\text{poly}(n) \leqslant X_0 \leqslant 1 - 1/\text{poly}(n)$. Consequently, we extend existing hardness of computation results using our more general lower-bound.

1. Theorem 13 extends the fail-stop attack of [15] on 2-party bias-X_0 coin-tossing protocols (in the information-theoretic commitment hybrid). For any $X_0 \in [0,1]$, a fail-stop adversary can change the probability of the final outcome of any 2-party bias-X_0 coin-tossing protocol by $\geqslant \frac{\sqrt{2}}{12\sqrt{n+1}} \cdot X_0(1-X_0)$. This result is useful to demonstrate black-box separations results.
2. Corollary 17 extends the black-box separation results of [16, 23, 17] separating (appropriate restrictions of) 2-party bias-X_0 coin tossing protocols from one-way functions. We illustrate a representative new result that follows as a consequence of Corollary 17. For constant $X_0 \in (0,1)$, [16, 23, 17] rely on (the extensions of) [15] to show that it is highly unlikely that there exist 2-party bias-X_0 coin tossing protocols using one-way functions in a black-box manner achieving $o(1/\sqrt{n})$ *unfairness* [22]. Note that when $X_0 = 1/n$, there are secure 2-party coin tossing protocols with $1/2n$ unfairness (based on Corollary 11) even in the non-cryptographic setting. Previous results cannot determine the limits to the unfairness of 2-party bias-$1/n$ fair coin-tossing protocols that use one-way functions in a black-box manner. Our black-box separation result (refer to Corollary 17) implies that it is highly unlikely to construct bias-$1/n$ coin using one-way functions in a black-box manner with $< \frac{\sqrt{2}}{12 \cdot n^{3/2}}$ unfairness. In general, our black-box separation results also extend to a dice-rolling functionality where the bound on the unfairness is independent of the complexity of describing the output distribution.
3. Corollary 18 and Corollary 19 extend [15]'s result on influencing discrete control processes.

Finally, Theorem 20 demonstrates the versatility of our geometric approach by measuring large L_2-norm gaps in martingales. Study of the large gaps in martingales using the L_2-norm turns out useful for obtaining the upper bound on $C_n(X)$ in Lemma 2.

1.2 Prior Approaches to the General Martingale Problem

Note that the martingale starts from X_0 and ends with $X_n \in \{0,1\}$. Therefore, there exists a round i where the gap in the martingale is at least $\frac{\min\{X_0, 1-X_0\}}{n}$. The entire non-triviality arises due to the objective of demonstrating a $\approx \frac{1}{\sqrt{n}}$ gap in the martingale instead of $\approx \frac{1}{n}$ gap. Additionally, it is essential that the stopping time τ *not* be restricted to being constant. Because, there exist martingales such that, for all constant stopping times τ, the expected gap is only $\approx \frac{1}{n}$ (see Figure 1 for such an example). Burkholder's inequalities are a major tool for martingale analysis. (One form of) Burkholder's inequality states that for $1 < p < \infty$, there exists constant c_1 and c_2 such that the following identity holds

$$c_1 \mathbb{E}\left[\left|\sum_{i=1}^{n} (X_i - X_{i-1})^2\right|^{p/2}\right] \leqslant \mathbb{E}\left[|X_n|^p\right] \leqslant c_2 \mathbb{E}\left[\left|\sum_{i=1}^{n} (X_i - X_{i-1})^2\right|^{p/2}\right]$$

The right-side of the inequality can be used to obtain a lower bound on the average change in the martingale. Since, $X_n \in \{0, 1\}$, note that we have $\mathbb{E}\left[|X_n|^p\right] = X_0$. So, we conclude that

$$X_0 \leqslant c_2 \mathbb{E}\left[\left|\sum_{i=1}^{n} (X_i - X_{i-1})^2\right|^{p/2}\right]$$

However, it is *unclear* how to use this form of the inequality to deduce lower-bounds of the form $\Omega(1/\sqrt{n})$, which is the focus of our work. We know that the stopping time τ cannot be a constant, so averaging arguments seem ineffective (see Figure 1). Therefore, the use of Burkholder-type inequalities or other square function inequalities in our context is not evident.

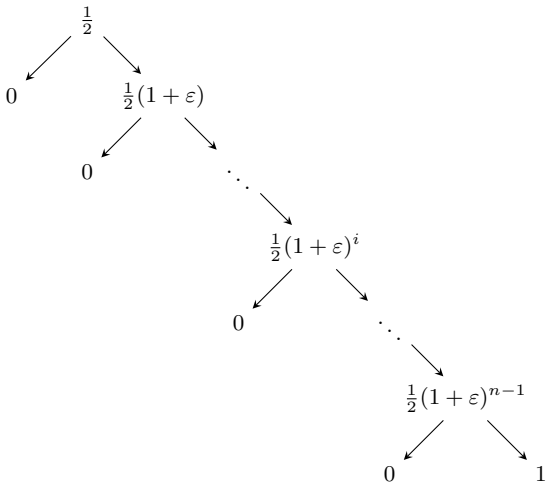

Figure 1 Here, $\varepsilon = 2^{1/n} - 1$ and $\mathbb{E}[|X_i - X_{i-1}|] = 2 \cdot \frac{\varepsilon(1+\varepsilon)^{i-1}}{2(1+\varepsilon)^i} = \frac{\varepsilon}{1+\varepsilon} = 1 - 2^{-1/n} \approx O(\frac{1}{n})$.

Prior works approach this problem as a negation of the Azuma's inequality. Azuma-Hoeffding inequality [7, 25] states that if $|X_i - X_{i-1}| = o(1/\sqrt{n})$, for all $i \in \{1, \ldots, n\}$, then, essentially, $|X_n - X_0| = o(1)$ with probability 1, i.e., the final information X_n remains close to the a priori information X_0. However, $X_n \in \{0, 1\}$, in particular, implies that the final information X_n is significantly different from the a priori information X_0. So, the initial constraint "for all $i \in \{1, \ldots, n\}$ we have $|X_i - X_{i-1}| = o(1/\sqrt{n})$" must be violated. What is the probability of this violation? For $X_0 = 1/2$, Cleve and Impagliazzo [15] proved that there exists a round i such that $|X_i - X_{i-1}| \geqslant \frac{1}{32\sqrt{n}}$ with probability $1/5$. We emphasize that the round i is a random variable and not a constant. Recently, in an independent work, Beimel et al. [8] demonstrate an identical bound for *weak martingales* (that have some additional properties), which is used to model multi-party coin-tossing protocols.

For the upper-bound, on the other hand, Doob's martingale corresponding to the majority protocol is the only known martingale for $X_0 = 1/2$. Martingales that have small gaps corresponding to any stopping time are relatively unknown.

2 Preliminaries

We denote the *arithmetic mean* of two numbers as $\text{A.M.}(x, y) := \frac{x+y}{2}$. The *geometric mean* of two numbers is denoted by $\text{G.M.}(x, y) := \sqrt{x \cdot y}$ and the *harmonic mean* of two numbers is denoted by $\text{H.M.}(x, y) := \left(\left(x^{-1} + y^{-1}\right)/2\right)^{-1}$.

Martingales and Related Definitions. The *conditional expectation* of a random variable X with respect to an event $\mathcal{E}$ denoted by $\mathbb{E}[X|\mathcal{E}]$, is defined as $\mathbb{E}[X\,\mathbb{1}_{\mathcal{E}}]/\Pr[\mathcal{E}]$. For a discrete random variable Y, the conditional expectation of X with respect to Y, denoted by $\mathbb{E}[X|Y]$, is a random variable that takes value $\mathbb{E}[X|Y=y]$ with probability $\Pr[Y=y]$ where $\mathbb{E}[X|Y=y]$ denotes the conditional expectation of X with respect to the event $\{\omega \in \Omega | Y(\omega) = y\}$.
Let $\Omega = \Omega_1 \times \Omega_2 \times \cdots \times \Omega_n$ denote a sample space and $(E_1, E_2, \ldots, E_n)$ be a joint distribution defined over Ω such that for each $i \in \{1, \ldots, n\}$, E_i is a random variable over Ω_i. Let $X = \{X_i\}_{i=0}^n$ be a sequence of random variables defined over Ω. We say that X_j is $E_1, \ldots, E_j$ measurable if there exists a function $g_j \colon \Omega_1 \times \Omega_2 \times \cdots \times \Omega_j \to \mathbb{R}$ such that $X_j = g_j(E_1, \ldots, E_j)$. Let $X = \{X_i\}_{i=0}^n$ be a discrete-time martingale sequence with respect to the sequence $E = \{E_i\}_{i=1}^n$. This statement implies that for each $i \in \{0, 1, \ldots, n\}$, we have

$$\mathbb{E}\left[X_{i+1} | E_1, E_2, \ldots, E_i\right] = X_i$$

Note that the definition of martingale implies X_i to be $E_1, \ldots, E_i$ measurable for each $i \in \{1, \ldots, n\}$ and X_0 to be constant. In the sequel, we shall use $\{X = \{X_i\}_{i=0}^n, E = \{E_i\}_{i=1}^n\}$ to denote a martingale sequence where for each $i = 1, \ldots, n$, $X_i \in [0, 1]$, and $X_n \in \{0, 1\}$. However, for brevity, we use $(X_0, X_1, \ldots, X_n)$ to denote a martingale. Given a function $f \colon \Omega_1 \times \Omega_2 \times \cdots \times \Omega_n \to \mathbb{R}$, if we define the random variable $Z_i := \mathbb{E}\left[f(E_1, \ldots, E_n) | E_1, \ldots, E_i\right]$ for each $i \in \{0, 1, \ldots, n\}$, then it is observed that $Z = \{Z_i\}_{i=0}^n$ is a martingale with respect to $\{E_i\}_{i=1}^n$. This martingale is called *Doob's martingale*.

The random variable $\tau \colon \Omega \to \{0, 1, \ldots, n\}$ is called a stopping time if for each $k \in \{1, 2, \ldots, n\}$, the occurrence or non-occurrence of the event $\{\tau \leqslant k\} = \{\omega \in \Omega | \tau(\omega) \leqslant k\}$ depends only on the values of random variables $E_1, E_2, \ldots, E_k$ or equivalently the random variable $\mathbb{1}_{\{\tau \leqslant k\}}$ is $E_1, \ldots, E_k$ measurable. Let $\mathcal{S}(X, E)$ denote the set of all stopping time random variables over the martingale sequence $\{X = \{X_i\}_{i=0}^n, E = \{E_i\}_{i=1}^n\}$. For $\ell \in \{1, 2\}$, we define the *score* of a martingale sequence (X, E) with respect to a stopping time τ in L_ℓ-norm as the following quantity.

$$\text{score}_\ell(X, E, \tau) := \mathbb{E}\left[|X_\tau - X_{\tau-1}|^\ell\right]$$

We define the *max stopping time* as the stopping time that maximizes the score

$$\tau_{\max}(X, E, \ell) := \text{argmax}_{\ \tau \in \mathcal{S}(X,E)} \text{score}_\ell(X, E, \tau)$$

and the (corresponding) max-score as

$$\text{max-score}_\ell(X, E) := \mathbb{E}\left[|X_{\tau_{\max}} - X_{\tau_{\max}-1}|^\ell\right]$$

Let $A_n(x^*)$ denote the set of all discrete time martingales $\{X = \{X_i\}_{i=0}^n, E = \{E_i\}_{i=1}^n\}$ such that $X_0 = x^*$ and $X_n \in \{0, 1\}$. We define *optimal score* as

$$\text{opt}_n(x^*, \ell) := \inf_{(X,E) \in A_n(x^*)} \text{max-score}_\ell(X, E)$$

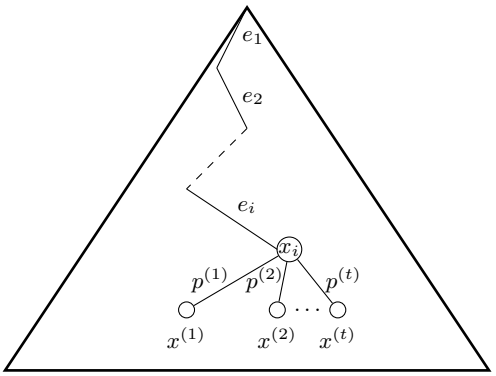

Figure 2 Interpreting a general martingale as a tree.

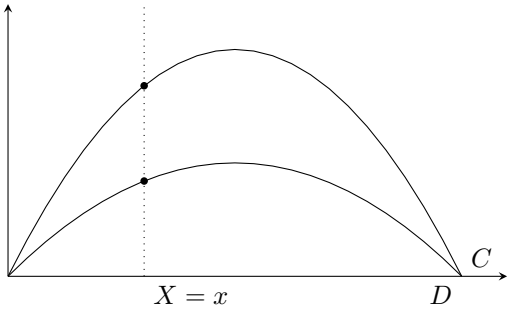

Figure 3 Intuition for a curve C being above another curve D, represented by $C \succcurlyeq D$.

Representing a Martingale as a Tree. A discrete time martingale sequence $X = \{X_i\}_{i=0}^n$ defined over a sample space $\Omega = \Omega_1 \times \cdots \times \Omega_n$, can be represented by a tree of depth n (see Figure 2). For $i = 0, \ldots, n$, any node at depth i has $|\Omega_{i+1}|$ children. In fact, for each i, the edge between a node at depth i and a child at depth $(i+1)$ corresponds to a possible outcome that E_{i+1} can take from the set $\Omega_{i+1} = \{x^{(1)}, \ldots, x^{(t)}\}$.

Each node v at depth i is represented by a unique path from root to v like $(e_1, e_2, \ldots, e_i)$, which corresponds to the event $\{\omega \in \Omega | E_1(\omega) = e_1, \ldots, E_i(\omega) = e_i\}$. Specifically, each path from root to a leaf in this tree, represents a unique outcome in the sample space Ω.

Each edge between the node $(e_1, \ldots, e_i)$ and the node $(e_1, \ldots, e_i, e_{i+1})$, is labeled by $\mathbb{P}\left[E_{i+1} = e_{i+1} | E_1 = e_1, \ldots, E_{i-1} = e_{i-1}\right]$, which is the probability of observing edge e_{i+1} (or equivalently, observing the node $(e_1, \ldots, e_i, e_{i+1})$ at time $(i+1)$ conditioned on reaching the node $(e_1, \ldots, e_i)$ at time i). Moreover, each node $(e_1, \ldots, e_{i+1})$ is labeled by $X_{i+1}(e_1, \ldots, e_{i+1})$, which, according to the definition of martingale, satisfies

$$\begin{aligned}\mathbb{E}\left[X_{i+1} | E_1 = e_1 \ldots, E_i = e_i\right] &= \sum_{e_{i+1} \in \Omega_{i+1}} X_{i+1}(e_1, \ldots, e_{i+1}) \mathbb{P}\left[E_{i+1} = e_{i+1} | E_1 = e_1, \ldots, E_i = e_i\right] \\ &= \left(X_i | E_1 = e_1 \ldots, E_i = e_i\right)\end{aligned}$$

Intuitively, the label assigned to each node is equal to the average of its children's labels, where each child is weighted by the conditional probability assigned to the edge between that node and the child.

Any subset of nodes in a tree that has the property that none of them is an ancestor of any other, is called an *anti-chain*. If we use our tree-based notation to represent a node v, i.e., the sequence of edges $e_1, \ldots, e_i$ corresponding to the path from root to v, then any prefix-free subset of nodes is an anti-chain. Any anti-chain that is not a proper subset of another anti-chain is called a *maximal anti-chain*. A stopping time in a martingale corresponds to a *unique* maximal anti-chain in the martingale tree.

Geometric Definitions and Relations. Consider curves C and D defined by the zeroes of $Y = f(X)$ and $Y = g(X)$, respectively, where $X \in [0, 1]$. We restrict to curves C and D such that each one of them have exactly one intersection with $X = x$, for any $x \in [0, 1]$. Then, we say C is *above* D, represented by $C \succcurlyeq D$, if, for each $x \in [0, 1]$, we have $f(x) \geqslant g(x)$.

3 Large Gaps in Martingales: A Geometric Approach

This section presents a high-level overview of our proof strategy. In the sequel, we shall assume that we are working with discrete-time martingales $(X_0, X_1, \ldots, X_n)$ such that $X_n \in \{0, 1\}$.

Given a martingale $(X_0, \ldots, X_n)$, its *susceptibility* is represented by the following quantity

$$\sup_{\text{stopping time } \tau} \mathbb{E}\left[|X_\tau - X_{\tau-1}|\right]$$

Intuitively, if a martingale has high susceptibility, then it has a stopping time such that the gap in the martingale while encountering the stopping time is large. Our objective is to characterize the *least susceptibility* that a martingale $(X_0, \ldots, X_n)$ can achieve. More formally, given n and X_0, characterize

$$C_n(X_0) := \inf_{(X_0,\ldots,X_n)} \sup_{\text{stopping time } \tau} \mathbb{E}\left[|X_\tau - X_{\tau-1}|\right]$$

Our approach is to proceed by induction on n to exactly characterize the curve $C_n(X)$, and our argument naturally constructs the best martingale that achieves $C_n(X_0)$.

1. We know that the base case is $C_1(X) = 2X(1 - X)$ (see Figure 4 for this argument).
2. Given the curve $C_{n-1}(X)$, we identify a geometric transformation T (see Figure 7) that defines the curve $C_n(X)$ from the curve $C_{n-1}(X)$. Subsection 3.1 summarizes the proof of this inductive step that crucially relies on the geometric interpretation of the problem, which is one of our primary technical contributions. Furthermore, for any $n \geqslant 1$, there exist martingales such that its susceptibility is $C_n(X_0)$.
3. Finally, Subsection 3.2 proves that the curve $C_n(X)$ lies above the curve $L_n(X) := \frac{2}{\sqrt{2n-1}} X(1-X)$ and below the curve $U_n(X) := \frac{1}{\sqrt{n}}\sqrt{X(1-X)}$.

3.1 Proof of Theorem 1

Our objective is the following.

1. Given an arbitrary martingale (X, E), find the maximum stopping time in this martingale, i.e., the stopping time $\tau_{\max}(X, E, 1)$.
2. For any depth n and bias X_0, construct a martingale that achieves the max-score. We refer to this martingale as *optimal* martingale. A priori, this martingale need not be unique. However, we shall see that for each X_0, it is (essentially) a unique martingale.

We emphasize that even if we are only interested in the exact value of $C_n(X_0)$ for $X_0 = 1/2$, it is unavoidable to characterize $C_{n-1}(X)$, for all values of $X \in [0, 1]$. Because, in a martingale $(X_0 = 1/2, X_1, \ldots, X_n)$, the value of X_1 can be arbitrary. So, without a precise characterization of the value $C_{n-1}(X_1)$, it is not evident how to calculate the value of $C_n(X_0 = 1/2)$. Furthermore, understanding $C_n(X_0)$, for all $X_0 \in [0, 1]$, yields entirely new applications for our result.

Base Case of $n = 1$. For a martingale (X_0, X_1) of depth $n = 1$, we have $X_1 \in \{0, 1\}$. Thus, without loss of generality, we assume that E_1 takes only two values (see Figure 4). Then, it is easy to verify that the max-score is always equal to $2X_0(1 - X_0)$.

This score is witnessed by the stopping time $\tau = 1$. So, we conclude that $\text{opt}_1(X_0, 1) = C_1(X_0) = 2X_0(1 - X_0)$

Inductive Step. $n = 2$ (For Intuition). For simplicity, let us consider finite martingales, i.e., the sample space Ω_i of the random variable E_i is finite. Suppose that the root $X_0 = x$ in the corresponding martingale tree has t children with values $x^{(1)}, x^{(2)}, \ldots, x^{(t)}$, and the probability of choosing the j-th child is $p^{(j)}$, where $j \in \{1, \ldots, t\}$ (see Figure 5).

Given a martingale (X_0, X_1, X_2), the adversary's objective is to find the stopping time τ that maximizes the score $\mathbb{E}\left[|X_\tau - X_{\tau-1}|\right]$. If the adversary chooses to stop at $\tau = 0$, then the score $\mathbb{E}\left[|X_\tau - X_{\tau-1}|\right] = 0$, which is not a good strategy. So, for each j, the adversary chooses whether to stop at the child $x^{(j)}$, or continue to a stopping time in the sub-tree rooted at $x^{(j)}$. The adversary chooses the stopping time based on which of these two strategies yield a better score. If the adversary stops the martingale at child j, then the contribution of this decision to the score is $p^{(j)}\left|x^{(j)} - x\right|$. On the other hand, if she does not stop at child j, then the contribution from the sub-tree is guaranteed to be $p^{(j)}C_1(x^{(j)})$. Overall, from the j-th child, an adversary obtains a score that is at least $p^{(j)} \max\left\{\left|x^{(j)} - x\right|, C_1(x^{(j)})\right\}$.

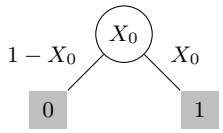

Figure 4 Base Case for Theorem 1. Note

$$C_1(X_0) = \inf_{(X_0,X_1)} \sup_{\tau} \mathbb{E}\left[|X_\tau - X_{\tau-1}|\right]$$

The optimal stopping time is shaded and its score is $X_0(1 - X_0) + (1 - X_0)X_0$.

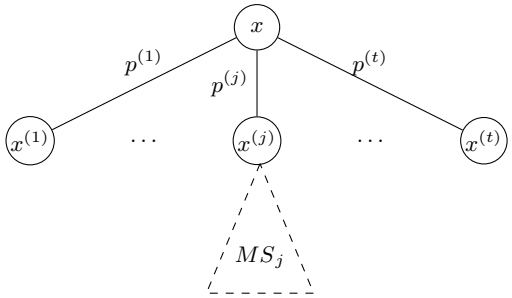

Figure 5 Inductive step for Theorem 1. MS_j represents the max-score of the sub-tree of depth $n - 1$ whose rooted at $x^{(j)}$. For simplicity, the subtree of $x^{(j)}$ is only shown here.

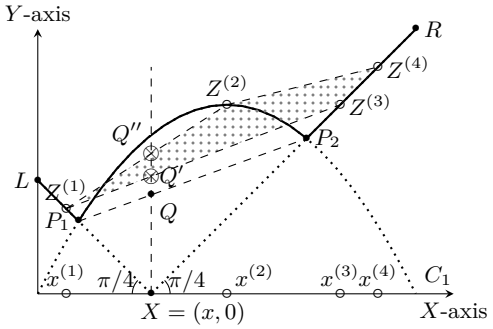

Figure 6 Intuitive summary of the inductive step for $n = 2$.

Let $h^{(j)} := \max\left\{\left|x^{(j)} - x\right|, C_1(x^{(j)})\right\}$. We represent the points $Z^{(j)} = (x^{(j)}, h^{(j)})$ in a two dimensional plane. Then, clearly all these points lie on the solid curve defined by $\max\left\{|X - x|, C_1(X)\right\}$, see Figure 6.

Since (X, E) is a martingale, we have $x = \sum_{j=1}^{t} p^{(j)}x^{(j)}$ and the adversary's strategy for finding $\tau_{\max}$ gives us max-score$_1(X, E) = \sum_{j=1}^{t} p^{(j)}h^{(j)}$. This implies that the $(x, \text{max-score}_1(X, E)) = \sum_{j=1}^{t} p^{(j)}Z^{(j)}$. So, the point in the plane giving the adversary the maximum score for a tree of depth $n = 2$ with bias $X_0 = x$ lies in the *intersection* of the convex hull of the points $Z^{(1)}, \ldots, Z^{(t)}$, and the line $X = x$. Let us consider the martingale defined in Figure 6 as a concrete example. Here $t = 4$, and the points $Z^{(1)}, Z^{(2)}, Z^{(3)}, Z^{(4)}$ lie on $\max\left\{|X - x|, C_1(X)\right\}$. The martingale designer specifies the probabilities $p^{(1)}, p^{(2)}, p^{(3)}$, and $p^{(4)}$, such that $p^{(1)}x^{(1)} + \ldots + p^{(4)}x^{(4)} = x$. These probabilities are not represented in

Given. A curve C defined by the zeroes of the equation $Y = f(X)$, where $X \in [0,1]$.
Definition of the Transform. The transform of C, represented by $T(C)$, is the curve defined by the zeroes of the equation $Y = g(X)$, where, for $x \in [0,1]$, the value of $g(x)$ is defined below.

1. Let $x_S(x) \in [0,1]$ be a solution of the equation $X + f(X) = x$.
2. Let $x_L(x) \in [0,1]$ be a solution of the equation $X - f(X) = x$.
3. Then $g(x) := \text{H.M.}(y^{(1)}, y^{(2)})$, where $y^{(1)} = f(x_S(x))$, $y^{(2)} = f(x_L(x))$, and $\text{H.M.}(y^{(1)}, y^{(2)})$ represents the harmonic mean of $y^{(1)}$ and $y^{(2)}$.

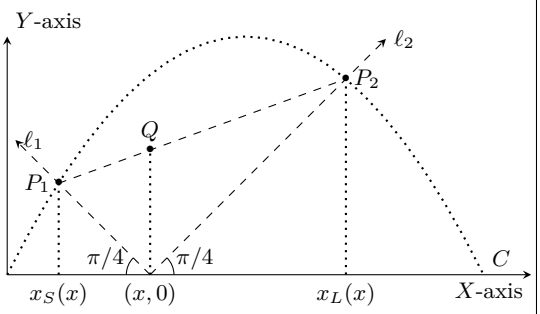

Figure 7 Definition of transform of a curve C, represented by $T(C)$. The locus of the point Q (in the right figure) defines the curve $T(C)$.

Figure 6. Note that the point $\left(p^{(1)}x^{(1)} + \cdots + p^{(4)}x^{(4)}, p^{(1)}h^{(1)} + \cdots + p^{(4)}h^{(4)}\right)$ representing the score of the adversary is the point $p^{(1)}Z^{(1)} + \cdots + p^{(4)}Z^{(4)}$. This point lies inside the convex hull of the points $Z^{(1)}, \ldots, Z^{(4)}$ and on the line $X = p^{(1)}x^{(1)} + \cdots + p^{(4)}x^{(4)} = x$. The exact location depends on $p^{(1)}, \ldots, p^{(4)}$. The point Q' is the point with minimum height. Observe that the height of the point Q' is at least the height of the point Q. So, in any martingale, the adversary shall find a stopping time that scores more than (the height of) the point Q. On the other hand, the martingale designer's objective is to reduce the score that an adversary can achieve. So, the martingale designer chooses $t = 2$, and the two points $Z^{(1)} = P_1$ and $Z^{(2)} = P_2$ to construct the optimum martingale. We apply this method for each $x \in [0,1]$ to find the corresponding point Q. That is, the *locus of the point* Q, for $x \in [0,1]$, yields the curve $C_2(X)$. Note that the height of Q is the harmonic-mean of the heights of P_1 and P_2.

This property inspires the definition of the geometric transformation T, see Figure 7. Applying T on the curve $C_1(X)$ yields the curve $C_2(X)$ for which we have $C_2(x) = \text{opt}_2(x,1)$.

General Inductive Step. Note that a similar approach works for general $n = d \geqslant 2$. Fix X_0 and $n = d \geqslant 2$. We assume that the adversary can compute $C_{d-1}(X_1)$, for any $X_1 \in [0,1]$.

Suppose the root in the corresponding martingale tree has t children with values $x^{(1)}, x^{(2)}, \ldots, x^{(t)}$, and the probability of choosing the j-th child is $p^{(j)}$ (see Figure 5). Let $(X^{(j)}, E^{(j)})$ represent the martingale associated with the sub-tree rooted at $x^{(j)}$.

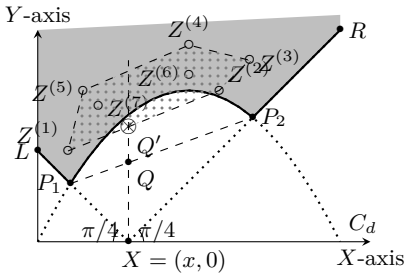

Figure 8 Intuitive Summary of the inductive argument. Our objective is to pick the set of points $\{Z^{(1)}, Z^{(2)} \ldots\}$ in the gray region to minimize the length of the intercept XQ' of their (lower) convex hull on the line $X = x$. Clearly, the unique optimal solution corresponds to including both P_1 and P_2 in the set.

For any $j \in \{1, \ldots, t\}$, the adversary can choose to stop at the child j. This decision will contribute $\left|x^{(j)} - x\right|$ to the score with weight $p^{(j)}$. On the other hand, if she continues to the subtree rooted at $x^{(j)}$, she will get at least a contribution of max-score$_1(X^{(j)}, E^{(j)})$ with weight $p^{(j)}$.

Therefore, the adversary can obtain the following contribution to her score

$$p^{(j)} \max\left\{\left|x^{(j)} - x\right|, C_{d-1}(x^{(j)})\right\}$$

Similar to the case of $n = 2$, we define the points $Z^{(1)}, \ldots, Z^{(t)}$. For $n > 2$, there is one difference from the $n = 2$ case. The point $Z^{(j)}$ need not *lie on the solid curve*, but it can lie on or above it, i.e., they lie in the gray area of Figure 8. Note that a suboptimal martingale designer can produce martingales with suboptimal scores, i.e., above the solid curve. For $n = 1$ it happens to be the case that there is (effectively) only one martingale that the martingale designer can design (the optimal tree). The adversary obtains a score that is at least the height of the point Q', which is at least the height of Q. On the other hand, the martingale designer can choose $t = 2$, and $Z^{(1)} = P_1$ and $Z^{(2)} = P_2$ to define the optimum martingale. Again, the locus of the point Q is defined by the curve $T(C_{d-1})$. Appendix A provides further details of the proof.

So, by induction, we have proved that $C_n(X) = T^{n-1}(C_1(X))$. Additionally, note that, during induction, in the optimum martingale, we always have $\left|x^{(0)} - x\right| = C_{n-1}(x^{(0)})$ and $\left|x^{(1)} - x\right| = C_{n-1}(x^{(1)})$. Intuitively, the decision to stop at $x^{(j)}$ or continue to the subtree rooted at $x^{(j)}$ has identical consequence. So, by induction, *all stopping times* in the optimum martingale have score $C_n(x)$.

3.2 Estimation of $C_n(X)$: Proof of Lemma 2

In this section, we prove Lemma 2, which tightly estimates the curve C_n.

Recall that we defined $L_n(X) = \frac{2}{\sqrt{2n-1}} X(1-X)$ and $U_n(X) = \frac{1}{\sqrt{n}}\sqrt{X(1-X)}$. Our objective is to inductively prove that $U_n \succcurlyeq C_n \succcurlyeq L_n$. To this end, we define the curve $G_n := a_n X(1-X)$ where $a_1 = 2$ and $a_{n+1} = 2\left(\frac{\sqrt{a_n^2+1}-1}{a_n}\right)$. Notice that $G_1(X) = L_1(X)$ for all $X \in [0,1]$. Moreover, it follows from Lemma 10 that $a_n \geqslant \frac{2}{\sqrt{2n-1}}$, and so $G_n \succcurlyeq L_n$ (Observe that since we do not have a closed form for G_n, we use L_n as a lower bound).

Proof. Since $G_n \succcurlyeq L_n$, it is sufficient to prove by induction that $U_n \succcurlyeq C_n \succcurlyeq G_n$.

Base Case of $n = 1$. Since, $C_1(X) = G_1(X) = 2X(1-X)$, it is obvious that $C_1 \succcurlyeq G_1$. Moreover, we know that $U_1(X) = \sqrt{X(1-X)}$. It is easy to verify that $U_1(X) \geqslant C_1(X)$ for all $X \in [0,1]$ which is equivalent to $U_1 \succcurlyeq C_1$.

Inductive Argument. Suppose we have $U_n \succcurlyeq C_n \succcurlyeq G_n$. Then, we have $T(U_n) \succcurlyeq T(C_n) \succcurlyeq T(G_n)$ (by Claim 5). Note that $C_{n+1} = T(C_n)$. We shall prove that $T(G_n) \succcurlyeq G_{n+1}$, and $U_{n+1} \succcurlyeq T(U_n)$ (refer to Claim 6 and Claim 8) respectively. Consequently, it follows that $U_{n+1} \succcurlyeq C_{n+1} \succcurlyeq G_{n+1}$. Figure 9 pictorially summarizes this argument.

◀

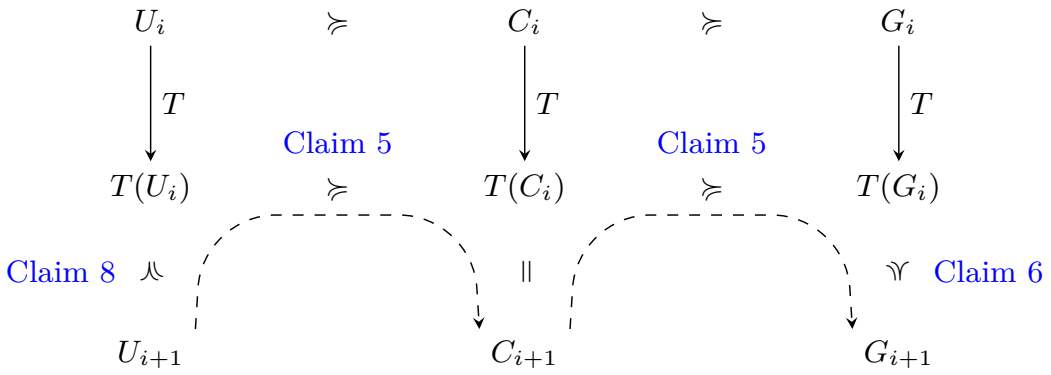

Figure 9 The outline of the inductive proof demonstrating that if the curves U_i and G_i sandwich the curve C_i, then the curves U_{i+1} and G_{i+1} sandwich the curve C_{i+1}. Recall that the notation "$A \succcurlyeq B$" implies that the curve A lies on-or-above the curve B.

A crucial property of convex upwards curves that we use in our proof is the following. Suppose we have $C \succcurlyeq D$, where C and D are two convex upwards curves above the axis $Y = 0$ defined in the domain $X \in [0, 1]$ containing the points $(0, 0)$ and $(1, 0)$. Then, we have $T(C) \succcurlyeq T(D)$. This result is formalized in Claim 5 and Figure 10 summarizes the intuition.

▷ Claim 5. Let C and D be concave downward curves in the domain $X \in [0, 1]$, and both curves C and D are above the axis $Y = 0$ and contain the points $(0, 0)$ and $(1, 0)$. Let C and D be curves such that $C \succcurlyeq D$ in the domain $X \in [0, 1]$, then the curve $T(C) \succcurlyeq T(D)$.

Proof. See Figure 10.
Observe that if the curves C and D are identical, then the result holds. So, let us assume that C and D are not identical. Note that if we have two distinct concave curves C and D such that $C \succcurlyeq D$ then these two curves cannot intersect at any additional point in the domain $(0, 1)$. Fix $x \in (0, 1)$. Let $Q_C = (x, y_C)$ be the intersection of the curve $T(C)$ with the line $X = x$. Similarly, let y_D be the intersection of the curve $T(D)$ with the line $X = x$. Let P be the point $(x, 0)$. Let ℓ_0 be the ray starting at P with slope 135-degrees. Let ℓ_1 be the ray starting at P with slope 45-degrees. Let ℓ_0 intersect the curves D and C at L_D and L_C, respectively. And, let ℓ_1 intersect the curves D and C at R_D and R_C, respectively. Observe in the triangles $\Delta P L_C R_C$ and $\Delta P L_D R_D$ the line segment $L_C R_C$ does not intersect with the line segment $L_D R_D$. Otherwise, if the line segments $L_C R_C$ intersects with $L_D R_D$, then the distinct concave curves C and D intersect at some point with X-coordinate in $(0, 1)$ as well (a contradiction).
Therefore, we have $L_C R_C \succcurlyeq L_D R_D$. Note that y_C is the intersection of $L_C R_C$ with $X = x$, and y_D is the intersection of $L_D R_D$ with $X = x$. So, we have $y_C \succcurlyeq y_D$. ◀

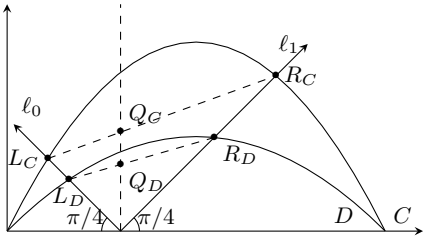

Figure 10 Summary of the proof of Claim 5.

In the following claim, we show that the transformation of a curve whose characteristics are specified below, will be "above" the curve itself.

▷ Claim 6. Let F_n be the curve above $Y = 0$ defined by the zeros of the equation $Y = f_n X(1-X)$, where $f_1 > 0$ and $f_{n+1} = 2\left(\frac{\sqrt{f_n^2+1}-1}{f_n}\right)$ for all $n \geqslant 1$. Then, we have $T(F_n) \succcurlyeq F_{n+1}$.

Proof. For each k, the curve F_k is a concave downward curve that contains the points $(0,0)$ and $(1,0)$, so based on Claim 7, for each k, the curve $T(F_k)$ is also concave downward and contains the points $(0,0)$ and $(1,0)$.

Let us fix $x \in [0,1]$ and let $x_0 \in [0,1]$ denotes the smaller root of the two roots of the equation $x^* + f_n x^*(1-x^*) = x$ and let y_0 be the value $f_n x_0(1-x_0)$. Moreover, let $x_1 \in [0,1]$ denotes the larger root of the two roots of the equation $x^* - f_n x^*(1-x^*) = x$ and let y_1 be the value $f_n x_1(1-x_1)$. So, we have

$$x_0 = \frac{(f_n+1) - \sqrt{(f_n+1)^2 - 4xf_n}}{2f_n}$$

and

$$\begin{aligned} y_0 &= \frac{\left(f_n+1-\sqrt{(f_n+1)^2-4xf_n}\right)\left(f_n-1+\sqrt{(f_n+1)^2-4xf_n}\right)}{4f_n} \\ &= \frac{f_n^2 - 1 - (f_n+1)^2 + 4xf_n + 2\sqrt{(f_n+1)^2-4xf_n}}{4f_n} \\ &= \frac{(2x-1)f_n - 1 + \sqrt{(f_n+1)^2-4xf_n}}{2f_n} \end{aligned}$$

and since $F_n(x) = F_n(1-x)$ (i.e. F_n is a symmetric curve around $\frac{1}{2}$), y_1 can be found by replacing x with $1-x$ in the formula that we found for y_0.

$$\begin{aligned} y_1 &= \frac{(2(1-x)-1)f_n - 1 + \sqrt{(f_n+1)^2-4(1-x)f_n}}{2f_n} \\ &= \frac{(1-2x)f_n - 1 + \sqrt{(f_n-1)^2+4xf_n}}{2f_n} \end{aligned}$$

To prove the claim, it suffices to show that the harmonic mean of y_0 and y_1 is at least equal to $f_{n+1}x(1-x)$. We make the substitution $x = 1/2 - z$ and we need to consider only $z \in [0, 1/2]$ because as mentioned earlier the curves are symmetric around the line $X = 1/2$.

From this substitution, we get

$$\begin{aligned}
y_0 &= \frac{-2zf_n - 1 + \sqrt{f_n^2 + 1 + 4zf_n}}{2f_n} \\
&= \frac{\left(f_n^2 + 1 + 4zf_n\right) - (1 + 2zf_n)^2}{2f_n\left(\sqrt{f_n^2 + 1 + 4zf_n} + (1 + 2zf_n)\right)} \\
&= \frac{(1 - 4z^2)}{2f_n} \cdot \frac{f_n^2}{\sqrt{f_n^2 + 1 + 4zf_n} + (1 + 2zf_n)} \\
y_1 &= \frac{2zf_n - 1 + \sqrt{f_n^2 + 1 - 4zf_n}}{2f_n} \\
&= \frac{(1 - 4z^2)}{2f_n} \cdot \frac{f_n^2}{\sqrt{f_n^2 + 1 - 4zf_n} + (1 - 2zf_n)} \\
\ell &:= f_{n+1}x(1 - x) \\
&= \frac{(1 - 4z^2)}{2f_n}\left(\sqrt{f_n^2 + 1} - 1\right)
\end{aligned}$$

So, we need to prove the following

$$\begin{aligned}
& & \text{H.M.}\,(y_0, y_1) &\geqslant \ell \\
\iff & & \text{H.M.}\left(\frac{2f_n}{1 - 4z^2} \cdot y_0, \frac{2f_n}{1 - 4z^2} \cdot y_1\right) &\geqslant \frac{2f_n}{1 - 4z^2} \cdot \ell \\
\iff & \text{H.M.}\left(\frac{f_n^2}{\sqrt{f_n^2 + 1 + 4zf_n} + (1 + 2zf_n)}, \frac{f_n^2}{\sqrt{f_n^2 + 1 - 4zf_n} + (1 - 2zf_n)}\right) &&\geqslant \sqrt{f_n^2 + 1} - 1 \\
\iff & \text{A.M.}\left(\frac{\sqrt{f_n^2 + 1 + 4zf_n} + (1 + 2zf_n)}{f_n^2}, \frac{\sqrt{f_n^2 + 1 - 4zf_n} + (1 - 2zf_n)}{f_n^2}\right) &&\leqslant \frac{1}{\sqrt{f_n^2 + 1} - 1} \\
\iff & & \text{A.M.}\left(\sqrt{f_n^2 + 1 + 4zf_n}, \sqrt{f_n^2 + 1 - 4zf_n}\right) + 1 &\leqslant \sqrt{f_n^2 + 1} + 1
\end{aligned}$$

In above, we used the fact that for any a, b, $\text{H.M.}(a, b) = \frac{2ab}{a+b} = \frac{1}{\frac{\frac{1}{a} + \frac{1}{b}}{2}} = \frac{1}{\text{A.M.}(a,b)}$. The last inequality is correct due to RMS-AM inequality. This completes the proof of the claim. ◀

In the following claim, we show that the geometric transformation T preserves some characteristics of the curve it is transforming - specifically if the original curve was concave downward and symmetric around $\frac{1}{2}$ then the new curve obtained will also retain these properties.

▷ Claim 7. Suppose the curve C which is concave downward in the interval $X \in [0, 1]$ and symmetric around $\frac{1}{2}$, and the points $(0, 0)$ and $(1, 0)$ lie on it - is given. Suppose the curve F is a curve defined by applying transformation T, defined in Figure 7, on curve C. Then, F has the same properties i.e. F is also concave downward, symmetric around $\frac{1}{2}$, and contains the points $(0, 0)$ and $(1, 0)$.

Proof. Since C is symmetric around $\frac{1}{2}$, the point (x, y) lies on the curve if and only if the point $(1 - x, y)$ lies on the curve. Suppose that the curve C is defined by the zeros of the equation $Y = f(X)$ and the curve $T(C)$ is defined by the zeros of the equation $Y = g(X)$. Then, according to the definition of the transformation T, $g(x) = \text{H.M.}(y^{(1)}, y^{(2)})$ where $y^{(1)} = f(x^{(1)})$ and $y^{(2)} = f(x^{(2)})$ where $x^{(1)}$ is the solution of $X + f(X) = x$ and $x^{(2)}$ is the

solution of $X - f(X) = x$. Note that since $f(x) = f(1-x)$, we have that $1 - x^{(1)}$ is the solution of $X - f(X) = 1 - x$ and $1 - x^{(2)}$ is the solution of the equation $X + f(X) = 1 - x$. Similarly, since $f(1 - x^{(1)}) = f(x^{(1)}) = y^{(1)}$ and $f(1 - x^{(2)}) = f(x^{(2)}) = y^{(2)}$, it follows that $g(1-x) = \text{H.M.}(y^{(2)}, y^{(1)}) = g(x)$ which implies that $T(C)$ is symmetric around $\frac{1}{2}$. For $x = 0$ or $x = 1$, $y^{(1)}$ or $y^{(2)}$ is 0 and so $g(1) = g(0) = 0$.

We provide a geometric proof to show that F is concave downwards and use Figure 11 as illustration. We know that a curve is concave downward in an interval if and only if the line that joins any two points of the curve is below the curve. Let us fix $x_1 \leqslant x_3$ in $[0, 1]$, see Figure 11. The height of points H_1, H_2, H_3 are respectively the value of $T(C)$ at points x_1, x_2, x_3 respectively. Our goal is to show that H_2 is above the segment H_1H_3 for any choice of x_2. Observe that, H_2 lies on the segment P_2Q_2. Since C is concave down, the segment P_2Q_2 is above the segment F_1F_2. Note that we are fixing x_1 and x_3 and allowing x_2 to change between x_1 and x_3. Then, we see that the segment F_1F_2 changes from P_1Q_1 to P_3Q_3 and is always above the segment H_1H_3. ◀

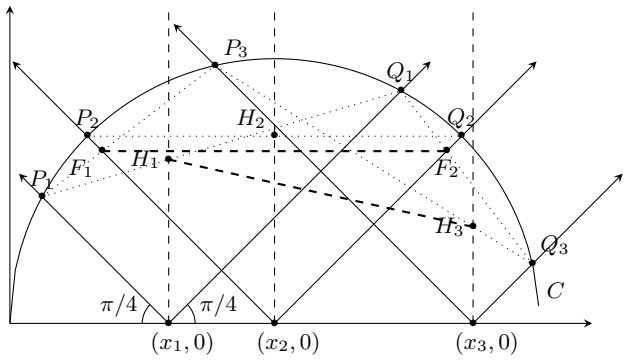

Figure 11 Intuition underlying Claim 7.

▷ Claim 8. Let U_n be defined by the zeros of the curve $Y = u_n\sqrt{X(1-X)}$, where $u_n > 0$ for all $n \geqslant 1$ and $X \in [0, 1]$. Then, we have $U_{n+1} \succcurlyeq T(U_n)$.

Proof. Let x_0 be the smaller of the two roots of the equation $x_0 + u_n\sqrt{x_0(1-x_0)} = x$, and x_1 be the larger of the two roots of the equation $x + u_n\sqrt{x_1(1-x_1)} = x_1$. So, we have

$$x_0 = \frac{(2x + u_n^2) - u_n\sqrt{u_n^2 - 4x^2 + 4x}}{2(1 + u_n^2)}$$

Now, let $y_0 = u_n\sqrt{x_0(1-x_0)}$. Then, we have

$$y_0 = u_n \frac{\sqrt{\left((2x + u_n^2) - u_n\sqrt{u_n^2 - 4x^2 + 4x}\right)\left((2 - 2x + u_n^2) + u_n\sqrt{u_n^2 - 4x^2 + 4x}\right)}}{2(1 + u_n^2)}$$

We substitute $x = 1/2 - z$ and need to consider only $z \in [0, 1/2]$ because the curves are symmetric around the line $X = 1/2$. From this substitution, we have

$$y_0 = u_n \frac{\sqrt{\left((1 + u_n^2 - 2z) - u_n\sqrt{u_n^2 + 1 - 4z^2}\right)\left((1 + u_n^2 + 2z) + u_n\sqrt{u_n^2 + 1 - 4z^2}\right)}}{2(1 + u_n^2)}$$

Now, the expression of $y_1 = u_n\sqrt{x_1(1-x_1)}$ is

$$y_1 = u_n \frac{\sqrt{\left((1+u_n^2+2z) - u_n\sqrt{u_n^2+1-4z^2}\right)\left((1+u_n^2-2z) + u_n\sqrt{u_n^2+1-4z^2}\right)}}{2(1+u_n^2)}$$

Note that $u_{n+1}\sqrt{x(1-x)} = \frac{u_n}{\sqrt{u_n^2+1}}\sqrt{\frac{1}{4}-z^2}$. So, to prove the claim, we need to prove that

$$\begin{aligned} & \text{H.M.}(y_0, y_1) \leqslant \frac{u_n}{\sqrt{u_n^2+1}}\sqrt{\frac{1}{4}-z^2} \\ \iff \qquad & \text{H.M.}\left(\frac{2(1+u_n^2)}{u_n}\cdot y_0, \frac{2(1+u_n^2)}{u_n}\cdot y_1\right) \leqslant \sqrt{(u_n^2+1)(1-4z^2)} \end{aligned}$$

The final inequality follows from the HM-GM inequality and the following simplifications

$$\left((1+u_n^2+2z) + u_n\sqrt{u_n^2+1-4z^2}\right)\left((1+u_n^2+2z) - u_n\sqrt{u_n^2+1-4z^2}\right) = (u_n^2+1)(1+2z)^2$$
$$\left((1+u_n^2-2z) + u_n\sqrt{u_n^2+1-4z^2}\right)\left((1+u_n^2-2z) - u_n\sqrt{u_n^2+1-4z^2}\right) = (u_n^2+1)(1-2z)^2$$

This observation completes the proof. ◀

The following mathematical result is used in the proof of Lemma 10.

▶ **Lemma 9.** *For $x \geqslant 0$, we have $\frac{1}{4\left(\sqrt{x+1}-\sqrt{x}\right)^2} \leqslant x + \frac{1}{2}$.*

Proof.

$$\begin{aligned} & \frac{1}{4\left(\sqrt{x+1}-\sqrt{x}\right)^2} \leqslant x + \frac{1}{2} \\ \iff \qquad & \left(\frac{\sqrt{x+1}+\sqrt{x}}{2}\right)^2 \leqslant x + \frac{1}{2} = \frac{(x+1)+x}{2} \\ \iff \qquad & \left(\frac{\sqrt{x+1}+\sqrt{x}}{2}\right) \leqslant \sqrt{\frac{(\sqrt{x+1})^2+(\sqrt{x})^2}{2}} \\ \iff \qquad & \text{A.M.}\left(\sqrt{x+1}, \sqrt{x}\right) \leqslant \text{R.M.S.}\left(\sqrt{x+1}, \sqrt{x}\right) \end{aligned}$$

The last inequality follows from the RMS-AM inequality. ◀

▶ **Lemma 10.** *Suppose a sequence $a_1, a_2, \ldots$ is given such that $a_{n+1} = 2\left(\frac{\sqrt{a_n^2+1}-1}{a_n}\right)$, then*

$$a_n \geqslant \frac{1}{\sqrt{\frac{1}{a_1^2} + \frac{n-1}{2}}}$$

Proof. Let $b_j := \frac{1}{a_j^2}$, so $a_j = \frac{1}{\sqrt{b_j}}$. Now, it follows from $a_{j+1} = 2\left(\frac{\sqrt{a_j^2+1}-1}{a_j}\right)$ that $b_{j+1} = \frac{1}{4\left(\sqrt{b_j+1}-\sqrt{b_j}\right)^2}$ and according to Lemma 9, $b_{j+1} \leqslant b_j + \frac{1}{2}$ for $j \geqslant 1$. Therefore,

$$\begin{aligned} \sum_{j=1}^{n-1} b_{j+1} \leqslant \sum_{j=1}^{n-1}\left(b_j + \frac{1}{2}\right) \implies b_n \leqslant b_1 + \frac{n-1}{2} &= \frac{1}{a_1^2} + \frac{n-1}{2} \\ \implies a_n \geqslant \frac{1}{\sqrt{\frac{1}{a_1^2} + \frac{n-1}{2}}} & \end{aligned}$$

◀

4 Application 1 : Distributed Coin-Tossing Protocol

We consider constructing distributed n-processor coin-tossing protocols where the i-th processor broadcasts her message in the i-th round. Motivated by efficiency considerations, we study this problem in the non-cryptographic setting.

The only protocol known for this problem exists for $X_0 = 1/2$ using the incredibly elegant "majority protocol" [11, 6, 14]. The i-th processor broadcasts her one random bit in round i. The final outcome of the protocol is the majority of the n outcomes, and an adversary can bias the final outcome by $\frac{1}{\sqrt{2\pi n}}$ by restarting a processor once [14].

We construct distributed n-party bias-X_0 coin-tossing protocols, for any $X_0 \in [0,1]$, and our new protocol for $X_0 = 1/2$ is more robust to restarting attacks than this majority protocol. Fix $X_0 \in [0,1]$ and $n \geqslant 1$. Consider the optimal martingale $(X_0, X_1, \ldots, X_n)$ guaranteed by Theorem 1. The susceptibility corresponding to any stopping time is $= C_n(X_0) \leqslant U_n(X_0) = \frac{1}{\sqrt{n}}\sqrt{X_0(1-X_0)}$. Note that we can construct an n-party coin-tossing protocol where the i-th processor broadcasts the i-th message, and the corresponding Doob's martingale is identical to this optimal martingale. An adversary who can restart a processor once biases the outcome of this protocol by at most $\frac{1}{2}C_n(X_0)$, this is discussed in Section 6.

▶ **Corollary 11** (Distributed Coin-tossing Protocols). *For every $X_0 \in [0,1]$ and $n \geqslant 1$ there exists an n-party bias-X_0 coin-tossing protocol such that any adversary who can restart a processor once causes the final outcome probability to deviate by $\leqslant \frac{1}{2}C_n(X_0) \leqslant \frac{1}{2}U_n(X_0) = \frac{1}{2\sqrt{n}}\sqrt{X_0(1-X_0)}$.*

For $X_0 = 1/2$, our new protocol's outcome can be changed by $\frac{1}{4\sqrt{n}}$, which is less than the $\frac{1}{\sqrt{2\pi n}}$ deviation of the majority protocol. However, we do not know whether there exists a *computationally efficient* algorithm implementing the coin-tossing protocols corresponding to the optimal martingales.

Next, we reduce a distributed dice-rolling protocol for an arbitrary ω-faceted dice to a sequence of distributed coin-tossing protocols. The reduction shall perform a binary search of depth $d = \lceil \lg \omega \rceil$ using distributed coin-tossing protocols among n/d processors for each binary search. For example, in the first phase, the first n/d processors shall determine whether the outcome is $< \omega/2$ or not. An adversary can deviate the outcome in this phase by $\leqslant \frac{1}{2}C_{n/d}(X_0) \leqslant \frac{1}{2}U_{n/d}(X_0) \leqslant \frac{1}{4\sqrt{n/d}}$. Using union bound over d binary searches, the upper-bound to the deviation is $\leqslant \frac{d^{3/2}}{4\sqrt{n}}$. We emphasize that this reduction crucially relies on the fact that the distributed bias-X_0 coin-tossing protocol exists for any $X_0 \in [0,1]$. Otherwise, the depth of a naïve binary search shall depend on the maximum number of bits required to represent the probabilities of every outcome of the ω-faceted dice-roll.

▶ **Corollary 12** (Distributed Dice-rolling Protocols). *For any ω-faceted dice-rolling functionality, and $n \geqslant 1$ there exists an n-party protocol for this functionality such that any adversary who can restart a processor once can cause the probability of any subset of outcomes to deviate by $\leqslant \frac{d^{3/2}}{4\sqrt{n}}$, where $d = \lceil \lg \omega \rceil$.*

For future research, we propose investigating the construction of dice-rolling protocols via *vector-valued* martingales that minimize "large gaps."

5 Application 2: Fail-stop Attacks on Coin-tossing/Dice-rolling Protocols

A *two-party n-round bias-X_0 coin-tossing protocol* is an interactive protocol between two parties who send messages in alternate rounds, and X_0 is the probability of the coin-tossing protocol's outcome being heads. *Fair computation* ensures that even if one of the parties aborts during the execution of the protocol, the other party outputs a (randomized) heads/tails outcome. This requirement of guaranteed output delivery is significantly stringent, and Cleve [14] demonstrated a computationally efficient attack strategy that alters the output-distribution by $O(1/n)$, i.e., any protocol is $O(1/n)$ unfair. Defining fairness and constructing fair protocols for general functionalities has been a field of highly influential research [21, 22, 9, 5, 3, 28, 4]. This interest stems primarily from the fact that fairness is a desirable attribute for secure-computation protocols in real-world applications. However, designing fair protocol even for simple functionalities like (bias-1/2) coin-tossing is challenging both in the two-party and the multi-party setting. In the multi-party setting, several works [6, 10, 1] explore fair coin-tossing where the number of adversarial parties is a constant fraction of the total number of parties. For a small number of parties, like the two-party and the three-party setting, constructing such protocols have been extremely challenging even in the cryptographic setting [29, 24, 13]. These constructions (roughly) match Cleve's $O(1/n)$ lower-bound in the computational setting.

In the non-cryptographic setting, Cleve and Impagliazzo [15] exhibited that any two-party n-round bias-1/2 coin-tossing protocol are $\frac{1}{2560\sqrt{n}}$ unfair. In particular, their adversary is a fail-stop adversary who follows the protocol honestly except aborting prematurely. In the information-theoretic commitment-hybrid, there are two-party n-round bias-1/2 coin-tossing protocols that have $\approx 1/\sqrt{n}$ unfairness [11, 6, 14]. This bound matches the lower-bound of $\Omega(1/\sqrt{n})$ by Cleve and Impagliazzo [15]. It seems that it is necessary to rely on strong computational hardness assumptions or use these primitives in a non-black box manner to beat the $1/\sqrt{n}$ bound [16, 23, 17, 8].

We generalize the result of Cleve and Impagliazzo [15] to all 2-party n-round bias-X_0 coin-tossing protocols (and improve the constants by two orders of magnitude). For $X_0 = 1/2$, our fail-stop adversary changes the final outcome probability by $\geqslant \frac{1}{24\sqrt{2}} \cdot \frac{1}{\sqrt{n+1}}$.

▶ **Theorem 13** (Fail-stop Attacks on Coin-tossing Protocols). *For any two-party n-round bias-X_0 coin-tossing protocol, there exists a fail-stop adversary that changes the final outcome probability of the honest party by at least $\frac{1}{12}C'_n(X_0) \geqslant \frac{1}{12}L'_n(X_0) := \frac{1}{12}\sqrt{\frac{2}{n+1}}X_0(1-X_0)$, where $C'_1(X) := X(1-X)$ and $C'_n(X) := T^{n-1}(C'_1(X))$.*

Before proving the above theorem, we provide some insight into our approach. Let $\Pi = \langle A, B\rangle$ be an n-round bias-X_0 coin-tossing protocol between Alice and Bob. Without loss of generality, assume that Alice sends messages in rounds $1, 3, \ldots$, and Bob sends messages in rounds $2, 4, \ldots$. The random variable $(E_1, \ldots, E_i)$ represents the partial transcript of the protocol at the end of round i. The random variable X_i represents the expected probability of heads at the end of the protocol execution conditioned on the current partial transcript at the end of round i. Note that $(X = (X_i)_{i=0}^n, E = (E_i)_{i=1}^n)$ is a Doob's martingale.

We construct fail-stop adversaries only. Suppose Alice has to send the message in round $(i+1)$ (i.e., i is even), but she aborts. Then, the *defense* D_i is the probability of Bob outputting heads. Similarly, suppose Bob is supposed to send the message in round $(i+1)$ (i.e., i is odd), but he aborts. Then, we define D_i as the probability of Alice outputting heads. Note that D_i is $(E_1, \ldots, E_i)$ measurable. In other words, the defense of round i is a

function only of the partial transcript at the end of that round.

The high-level idea of our construction of a good fail-stop attack is the following. We shall use a stopping time τ to identify appropriate partial transcripts of Π to abort. Suppose we have already generated a partial transcript $(e_1, \ldots, e_i)$ (refer Figure 2), and the next messages that are possible are $e_{i+1} \in \Omega_{i+1}$. Suppose τ stops the martingale at $e_{i+1} = e^{(j)}$. Note that $X_{i+1} = x^{(j)}$ is the probability of heads conditioned on the transcript Π being $(e_1, \ldots, e_i, e_{i+1} = e^{(j)})$. Further, the defense of the other party is D_i.

If i is even, then Alice is supposed to send the $(i+1)$-th message. So, the stopping time τ is indicating Alice to abort if the message in the next round she plans to send is $e^{(j)}$. Suppose $x^{(j)} \leqslant D_i$. Then, if Alice aborts when her next message is $e^{(j)}$, then she is increasing the probability of heads by $p^{(j)} \left| x^{(j)} - D_i \right|$.

So, the conclusion is the following. If i is even and $x^{(j)} \leqslant D_i$ then the advice of τ will be *helpful* to an adversarial Alice who is interested in increasing the probability of heads, say A^+. If $x^{(j)} > D_i$, then the advice of τ will be helpful to an adversarial Alice who is interested in reducing the probability of heads, say A^-. Similarly, when i is odd, the advice of τ is useful to either B^+ or B^-.

Specialized Stopping Time. For this discussion, let us consider Figure 7. Note that if X_1 is very small (that is, $X_1 < x_S(x)$) or X_1 is very large (that is, $X_1 > x_L(x)$), then the adversary aborts. Furthermore, if X_1 is close to X_0 (that is, $X_1 \in [x_S(x), x_L(x)]$), then the adversary does not abort and recursively constructs the optimum stopping time. In particular (refer to Figure 5 and Figure 6) if there exists $x^{(j)}$ and $x^{(j')}$ such that $x^{(j)} < x_S(x)$ and $x^{(j')} > x_L(x)$ then the adversary aborts in both these two cases. This step is crucial to arguing that the point Q' is higher than the point Q in Figure 6, which, in turn, is key to the transformation definition.

However, if a stopping time stops the martingale at high as well as low values of X_i then it is not evident how to to translate the susceptibility corresponding to this stopping time into output-bias achieved by a fail-stop adversary. So, we restrict to *specialized stopping times* with the following property (we use Figure 7 for reference in the following definition).

Fix n and X_0. Pick any $i = n - d$ and fix $E_1 = e_1, \ldots, E_i = e_i$. Let $x = (X_i | E_1 = e_1, \ldots, E_i = e_i)$.

- Either, the specialized stopping time stops for all $X_{i+1} < x_S(x)$ and recursively stops $X_{i+1} \geqslant x_S(x)$ later, or
- The specialized stopping time stops all $X_{i+1} > x_L(x)$ and recursively stops $X_{i+1} \leqslant x_L(x)$ later.

Now, it is not evident whether specialized stopping times also have high susceptibility.

▶ **Theorem 14.** *Let $(X_0, X_1, \ldots, X_n)$ be a discrete-time martingale such that $X_i \in [0, 1]$, for all $i \in \{1, \ldots, n\}$, and $X_n \in \{0, 1\}$. Then, the following bound holds.*

$$\sup_{\text{specialized stopping time } \tau} \mathbb{E}\left[|X_\tau - X_{\tau-1}|\right] \geqslant C'_n(X_0),$$

where $C'_1(X) := X(1 - X)$ and $C'_n(X) := T^{n-1}(C'_1(X))$.

Let us start with the base case $n = 1$. Note that a specialized stopping time cannot stop the martingale at both low and high X_1. So, we consider stopping times $\tau \colon \Omega \to \{1, \ldots, n, \infty\}$, where $\tau = \infty$ for a full transcript indicates that the adversary did not abort. Note that a specialized stopping time can either stop the martingale when $X_1 = 0$ or $X_1 = 1$. In either of these two cases, the susceptibility is $C'_1(X_0) = X_0(1 - X_0)$.

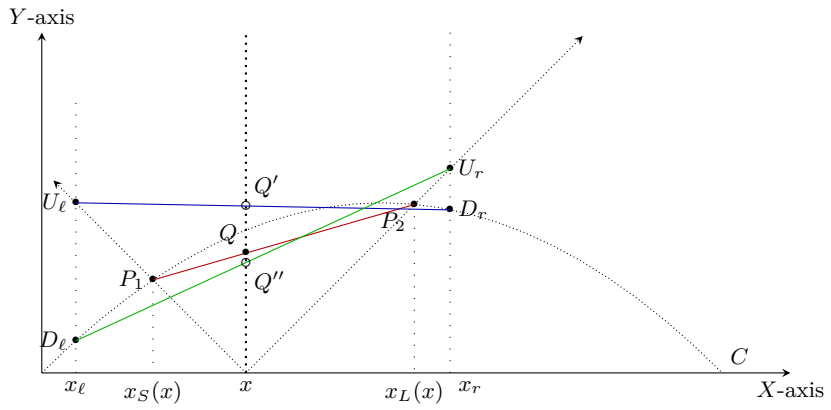

Figure 12 Intuition of the geometric transformation when restricted to specialized stopping times. The intersection of $X = x$ with lines $U_\ell D_r, P_1P_2$ and $D_\ell U_r$ are the points $Q^{'}, Q$ and $Q^{''}$ respectively. Note that in this figure, node x has only two children x_ℓ and x_r

For $n \geqslant 2$, we show that the recursive definition of the transform T continues to hold even for specialized stopping time (refer Figure 12 for intuition). Note that the adversary chooses the stopping time that achieves the highest susceptibility. So, the maximum height of Q' and Q'' in Figure 12 is greater than the height of Q. We emphasize that this proof crucially relies on the fact that $C'_{n-1}(X)$ lies below the curve $Y = \min\{X, 1-X\}$. So, our result holds because $C'_1(X)$ lies below the curve $Y = \min\{X, 1-X\}$. Subsection 5.2 presents the full proof.

Finally, we translate the susceptibility of a specialized stopping time into output-bias that a fail-stop adversary can enforce. Subsection 5.1 provides the full proof of Theorem 13.

5.1 Detailed Discussion of Our Fail-stop Attack and Proofs

Given a stopping time τ we shall associate the following score with it

$$S'(\tau) := \sum_{i=1}^{n+1} \mathbb{E}_{x\in\Omega}\left|\mathbb{E}[(X_i - D_{i-1})\mathbb{1}_{\tau=i}|E_1(x), E_2(x), \ldots, E_{i-1}(x)]\right|$$

Intuitively, this score correctly accounts for the increase and decrease in the probability of heads in every round i. [4]

We need the following claim

▷ Claim 15. If $0 \leqslant x^{(\ell)} \leqslant x_0 \leqslant x \leqslant 1$, (where x_0 is the solution of equation $x - x_0 = C'_d(x_0)$ in $[0,1]$), $x - D \geqslant \frac{2}{3}\left(x - x^{(\ell)}\right) \geqslant 0$, and $x - x^{(\ell)} \geqslant C'_d(x^{(l)})$ then $x - D \geqslant \frac{1}{3}C'_{d+1}(x)$.

If $0 \leqslant x \leqslant x_1 \leqslant x^{(r)} \leqslant 1$ (where x_1 is the solution of equation $x_1 - x = C'_d(x_1)$ in $[0,1]$), $D - x \geqslant \frac{2}{3}\left(x^{(r)} - x\right) \geqslant 0$, and $\left(x^{(r)} - x\right) \geqslant C'_d(x^{(r)})$ then $D - x \geqslant \frac{1}{3}C'_{d+1}(x)$.

[4] The score is slightly pessimistic, which, we argue, is also necessary. Note that our expression is of the form $\left|\mathbb{E}\left[(X_i - D_{i-1})\mathbb{1}_{\tau=i}|\ldots\right]\right|$. One might naïvely consider using the expression $\mathbb{E}\left[|X_i - D_{i-1}|\,\mathbb{1}_{\tau=i}|\ldots\right]$ instead. However, there is an issue. Suppose the stopping time stops the martingale for all children of X_i. This strategy causes the outcome to deviate by $|X_i - D_i|$, and our expression correctly accounts for it (because $\mathbb{E}[X_{i+1}] = X_i$). However, the alternative expression accounts for it incorrectly. Basically, the alternative expression might not be translatable into a deviation of outcome by a fail-stop attacker.

Proof. We prove the first statement. Since for each n, $C_n'(x) = C_n'(1-x)$, the second part is implied by the first part by replacing $x, D, x^{(\ell)}$ with $1-x, 1-D, x^{(r)} = 1-x^{(\ell)}$.

In order to show the first part, it is sufficient to show that $\frac{2}{3}(x - x^{(\ell)}) \geqslant \frac{1}{3}C_{d+1}'(x)$.

We know that

$$\frac{C_{d+1}'(x)}{3} = \frac{2}{3} \cdot \frac{y_0 y_1}{y_0 + y_1} = \frac{2}{3} \cdot \frac{(x - x_0)(x_1 - x)}{(x_1 - x_0)}$$

We also know that

$$x - x^{(\ell)} \geqslant x - x_0$$

and

$$x_1 - x_0 \geqslant x_1 - x$$

Combining the above two relations we have

$$\begin{aligned}
(x - x^{(\ell)})(x_1 - x_0) &\geqslant (x - x_0)(x_1 - x) \\
(x - x^{(\ell)}) &\geqslant \frac{(x - x_0)(x_1 - x)}{(x_1 - x_0)} \\
\frac{2}{3}(x - x^{(\ell)}) &\geqslant \frac{1}{3} \cdot \frac{2(x - x_0)(x_1 - x)}{(x_1 - x_0)} \\
\frac{2}{3}(x - x^{(\ell)}) &\geqslant \frac{1}{3}C_{d+1}'(x) \\
x - D \geqslant \frac{2}{3}(x - x^{(\ell)}) &\geqslant \frac{1}{3}C_{d+1}'(x)
\end{aligned}$$

This completes the proof of our claim. ◀

We will use specialized stopping time defined in Section 5 to construct a stopping time for our fail-stop adversary. More formally, given a stopping time τ_1 from Theorem 14 such that $\sup_{\tau_1} \mathbb{E}\left[|X_{\tau_1} - X_{\tau_1 - 1}|\right] \geqslant C_n'(X_0)$, there exists a stopping time τ_2 such that $S'(\tau_2) \geqslant \frac{1}{3}C_n'(X_0)$.

Proof. The proof will proceed by induction on n.

1. Base Case: For $n = 1$, see Figure 13.

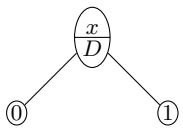

Figure 13 Base Case for Theorem 13

   Recall that $C_1'(x) = x(1-x)$. We have two cases
   - If $D \geqslant x$, we define τ_2 as the stopping time that stops only at 0. Then, $D(1-x) \geqslant x(1-x) \geqslant \frac{1}{3}x(1-x) \geqslant \frac{1}{3}C_1'(x)$.
   - If $D < x$, we define τ_2 as the stopping time that stops only at 1. Then $(1-D)x \geqslant x(1-x) \geqslant \frac{1}{3}x(1-x) \geqslant \frac{1}{3}C_1'(x)$

2. Assume the claim is true for $n = d$, see Figure 14. For each edge $\left(x, x^{(j)}\right)$, if $|x - x^{(j)}| \geqslant C_d'\left(x^{(j)}\right)$, then mark the edge. Let

$$\texttt{Marked} := \{j : |x - x^{(j)}| \geqslant C_d'(x^{(j)})$$

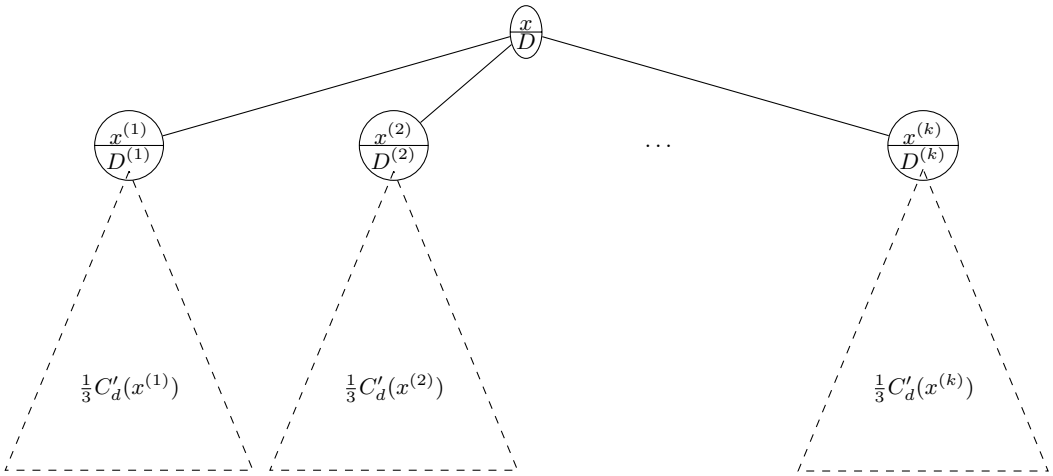

Figure 14 Inductive Hypothesis of Theorem 13

.

Without loss of generality, we assume that the nodes are *in-order*. Denote $\texttt{Left} := \{j : x^{(j)} \leqslant x\} \bigcap \texttt{Marked}$ and $\texttt{Right} := \{j : x^{(j)} \geqslant x\} \bigcap \texttt{Marked}$. We analyze three possible cases

- *Case 1.* No edges are marked. This means that for all j, $|x - x^{(j)}| \leqslant C'_d\left(x^{(j)}\right)$. The adversarial strategy is to recurse on the underlying subtrees. The overall deviation in this case is given by

$$\sum_j p^{(j)} C'_d\left(x^{(j)}\right) \geqslant C'_{d+1}\left(\sum_j p^{(j)} x^{(j)}\right) = C'_{d+1}(x) \geqslant \frac{C'_{d+1}(x)}{3}$$

- *Case 2.* There exists a marked edge j such that $D \leqslant \frac{x+2x^{(j)}}{3}$ and $x \geqslant x^{(j)}$ or $D \geqslant \frac{x+2x^{(j)}}{3}$ and $x^{(j)} \geqslant x$. The adversarial strategy is to abort at the parent.
  Suppose $D \leqslant \frac{x+2x^{(j)}}{3}$ and $x \geqslant x^{(j)}$, then $x - D \geqslant \frac{2}{3}(x - x^{(j)})$, the rest follows from Claim 15. If $D \geqslant \frac{x+2x^{(j)}}{3}$ and $x^{(j)} \geqslant x$, then $D - x \geqslant \frac{2}{3}(x^{(j)} - x)$ and the rest again follows from Claim 15.
- If *Case 1* and *Case 2* are not satisfied, then $\texttt{Marked}$ is not empty but for any marked edge j that $x \geqslant x^{(j)}$, we have $D > \frac{x+2x^{(j)}}{3}$ and for any marked edge j that $x \leqslant x^{(j)}$, we have $D < \frac{x+2x^{(j)}}{3}$. Note that since $\texttt{Marked}$ is not empty, at least one of the two sets $\texttt{Left}$ and $\texttt{Right}$ is not empty. Two cases can happen:
  - *Case 3.1* Both $\texttt{Left}$ and $\texttt{Right}$ are non-empty.
    Then there exist ℓ^* and r^* such that $\frac{x+2x^{(\ell^*)}}{3} < D < \frac{x+2x^{(r^*)}}{3}$ where $\ell^* := \max_\ell \texttt{Left}$ and $r^* := \min_r \texttt{Right}$. There are two sub-cases in this scenario :
    - *Case 3.1.1* $\frac{x+2x^{(\ell^*)}}{3} < D \leqslant x$.
      The adversarial strategy is to follow the strategy of τ_1. If the strategy of τ_1 is to abort on left marked edges and recurse on the rest, then we have the following analysis:
      For any $\ell \in \texttt{Left}$, $\ell \leqslant \ell^*$, and we have

$$D - x^{(\ell)} > \frac{x + 2x^{(\ell^*)}}{3} - x^{(\ell)} = \frac{x - x^{(\ell)} + 2(x^{(\ell^*)} - x^{(\ell)})}{3} \geqslant \frac{x - x^{(\ell)}}{3} > \frac{C'_d(x^{(\ell)})}{3}$$

The total deviation from aborting on the left marked edges is given by

$$\sum_{\ell \in \texttt{Left}} p^{(\ell)}(D - x^{(\ell)}) \geqslant \sum_{\ell \in \texttt{Left}} p^{(\ell)} \frac{x - x^{(\ell)}}{3} \geqslant \sum_{\ell \in \texttt{Left}} p^{(\ell)} \frac{C_d^{'}(x^{(\ell)})}{3}$$

The total deviation from recursing on the right edges and unmarked edges is given by

$$\sum_{k \notin \texttt{Marked}} p^{(k)} \frac{C_d^{'}(x^{(k)})}{3} + \sum_{r \in \texttt{Right}} p^{(r)} \frac{C_d^{'}(x^{(r)})}{3}$$

The overall deviation is

$$\begin{aligned}
&\sum_{\ell \in \texttt{Left}} p^{(\ell)}(D - x^{(\ell)}) + \sum_{r \in \texttt{Right}} p^{(r)} \frac{C_d^{'}(x^{(r)})}{3} + \sum_{k \notin \texttt{Marked}} p^{(k)} \frac{C_d^{'}(x^{(k)})}{3} \\
&\geqslant \sum_{\ell \in \texttt{Left}} p^{(\ell)} \frac{x - x^{(\ell)}}{3} + \sum_{r \in \texttt{Right}} p^{(r)} \frac{C_d^{'}(x^{(r)})}{3} + \sum_{k \notin \texttt{Marked}} p^{(k)} \frac{C_d^{'}(x^{(k)})}{3} \\
&\geqslant \frac{C_{d+1}^{'}(x)}{3}
\end{aligned}$$

In above, the last inequality holds due to the fact that τ_1 is a specialized stopping time and martingale aborts on left marked edges and recurses on the rest which is exactly what τ_1 suggests.

If the strategy of τ_1 is to abort on the right marked edges and recurse on the rest, then we have the following analysis:

For any $r \in \texttt{Right}$ such that $r \geqslant r^*$, we have

$$x^{(r)} - D > x^{(r)} - x > C_d^{'}(x^{(r)}) > \frac{C_d^{'}(x^{(r)})}{3}$$

The total deviation from aborting on the right marked edges is given by

$$\sum_{r \in \texttt{Right}} p^{(r)}(x^{(r)} - D) \geqslant \sum_{r \in \texttt{Right}} p^{(r)} \frac{x^{(r)} - x}{3} \geqslant \sum_{r \in \texttt{Right}} p^{(r)} \frac{C_d^{'}(x^{(r)})}{3}$$

The total deviation from recursing on the left edges and unmarked edges is given by

$$\sum_{k \notin \texttt{Marked}} p^{(k)} \frac{C_d^{'}(x^{(k)})}{3} + \sum_{l \in \texttt{Left}} p^{(l)} \frac{C_d^{'}(x^{(l)})}{3}$$

The overall deviation is

$$\begin{aligned}
&\sum_{r \in \texttt{Right}} p^{(r)}(x^{(r)} - D) + \sum_{\ell \in \texttt{Left}} p^{(l)} \frac{C_d^{'}(x^{(l)})}{3} + \sum_{k \notin \texttt{Marked}} p^{(k)} \frac{C_d^{'}(x^{(k)})}{3} \\
&\geqslant \sum_{r \in \texttt{Right}} p^{(r)} \frac{x^{(r)} - x}{3} + \sum_{\ell \in \texttt{Left}} p^{(\ell)} \frac{C_d^{'}(x^{(\ell)})}{3} + \sum_{k \notin \texttt{Marked}} p^{(k)} \frac{C_d^{'}(x^{(k)})}{3} \\
&\geqslant \frac{C_{d+1}^{'}(x)}{3}
\end{aligned}$$

In above, the last inequality holds due to the fact that τ_1 is a specialized stopping time and martingale aborts on right marked edges and recurses on the rest which is exactly what τ_1 suggests.

- *Case 3.1.2.* $x < D < \frac{x+2x^{(r^*)}}{3}$.
  The adversarial strategy is the same as above : Follow the strategy of τ_1. The analysis is almost identical to the one above due to symmetry.

- *Case 3.2.* Either `Left` or `Right` is empty.
  The adversarial strategy is to abort at all marked edges and recurse on all unmarked edges.
  Suppose `Right` is empty, then $\frac{x+2x^{(\ell^*)}}{3} < D < x$ where $\ell^* := \max_\ell$ `Left`. The analysis is the same as in *Case 3.1.1.* If `Left` is empty then the analysis is the same as *Case 3.1.2.* ◀

The above proof shows that $S'(\tau_2) \geqslant \frac{1}{3}C'_n(X_0)$. In order to estimate $C'_n(X_0)$, we define $L'_n(X) = \sqrt{\frac{2}{n+1}}X(1-X)$ and claim that $C'_n(X) \succcurlyeq L'_n(X)$.

To prove our claim, we define the curve $G'_n(X) := a'_n X(1-X)$ such that $a'_1 = 1$ and $a'_{n+1} = 2\left(\frac{\sqrt{a'^2_n+1}-1}{a'_n}\right)$ for $n \geqslant 1$ and we prove by induction that $C'_n \succcurlyeq G'_n$ for all n as below: (analogous to the one shown for Lemma 2)

Base Case of $n = 1$. Since, $C'_1(X) = G'_1(X) = X(1-X)$, it is obvious that $C'_1 \succcurlyeq G'_1$.

Inductive Argument. Suppose we have $C'_n \succcurlyeq G'_n$. Then, we have $T(C'_n) \succcurlyeq T(G'_n)$ (by Claim 5). Note that $C'_{n+1} = T(C'_n)$. We know that $T(G'_n) \succcurlyeq G'_{n+1}$ (refer to Claim 6). Consequently, it follows that $C'_{n+1} \succcurlyeq G'_{n+1}$.

So far, we have proved that $C'_n \succcurlyeq G'_n$ for all n. Recall that $G'_n(X) := a'_n X(1-X)$ such that $a'_1 = 1$ and $a'_{n+1} = 2\left(\frac{\sqrt{a'^2_n+1}-1}{a'_n}\right)$. Now, by using Lemma 10, we conclude that $a'_n \geqslant \sqrt{\frac{2}{n+1}}$. Thus, $C'_n \succcurlyeq L'_n$. Now we can say that $S'(\tau_2) \geqslant \frac{1}{3}C'_n(X_0) \geqslant \frac{1}{3}L'_n(X_0)$. Further, any contribution to this score is attributable to one of the following four interactions: (1) $\langle A^+, B\rangle$ (i.e., adversarial Alice increasing the probability of heads by aborting), (2) $\langle A^-, B\rangle$, (3) $\langle A, B^+\rangle$, and (4) $\langle A, B^-\rangle$. By an averaging argument, this implies that one of the parties can deviate the outcome of the other party by at least $\frac{1}{12}L'_n(X_0)$. This concludes our proof of Theorem 13.

Similar to the previous section, Theorem 13 extends to ω-faceted dice-rolling protocols by considering any subset $S \subseteq \{0, 1, \ldots, \omega-1\}$ of outcomes, and considering the final outcome being in S as the interesting event for the martingale.

5.2 Discussion of Specialized Stopping Time - Proof of Theorem 14

Before proving the theorem, we define the sequence of functions $\{g_n\}_{n=1}^{\infty}$ recursively. Let $A_n(X_0)$ be the set of all martingales $X = (X_0, X_1, \ldots, X_n)$ such that for each $0 \leqslant i \leqslant n-1$, $X_i \in [0,1]$ and $X_n \in \{0,1\}$. We define

$$g_1(X_0) := \inf_{X \in A_1(X_0)} \sup_{\tau \in \mathcal{F}_1(X_0,X_1)} \mathbb{E}|X_\tau - X_{\tau-1}|$$

where $\mathcal{F}_1(X_0, X_1) := \{\tau_1, \tau_2\}$ and τ_1 is an stopping time defined on martingale (X_0, X_1) such that $\tau_1(X_0, X_1) = 1$ if $X_1 = 0$ and $\tau_1(X_0, X_1) = \infty$ if $X_1 = 1$; and $\tau_2(X_0, X_1) = 1$ if $X_1 = 1$ and $\tau_2(X_0, X_1) = \infty$ if $X_1 = 0$. Note that $\mathcal{F}_1(X_0, X_1)$ represents the set of all specialized stopping times in martingale (X_0, X_1). $A_1(X_0)$ consists of only one martingale and $\mathbb{E}|X_{\tau_1} - X_{\tau_1-1}| = \mathbb{E}|X_{\tau_2} - X_{\tau_2-1}| = X_0(1-X_0)$ which implies that $g_1(X_0) = X_0(1-X_0)$. We define

$$g_n(X_0) := \inf_{X \in A_n(X_0)} \sup_{\tau \in \mathcal{F}_n(X_0,X_1,\ldots,X_n)} \mathbb{E}|X_\tau - X_{\tau-1}|$$

where $\mathcal{F}_n(X_0, X_1, \ldots, X_n)$ denotes the set of all specialized stopping times like τ defined on martingale $X = (X_0, X_1, \ldots, X_n)$ which could be one of the following two cases:

Suppose $X_0 = x$ and $X_1 = x^*$. Then, let $x_0 \in [0,1]$ be the solution of equation $x - x_0 = g_{n-1}(x_0)$ and $x_1 \in [0,1]$ be the solution of equation $x_1 - x = g_{n-1}(x_1)$.

1. For all $x^* \leqslant x_0$, $\tau(x, x^*, X_2, \ldots, X_n) = 1$ and for all $x^* > x_0$, $\tau(x, x^*, X_2, \ldots, X_n) = 1 + \tau^{'}(x^*, X_2, \ldots, X_n)$ for some $\tau^{'} \in \mathcal{F}_{n-1}(x^*, X_2, \ldots, X_n)$. This corresponds to the case that the specialized stopping time stops for all $x^* \leqslant x_0$ and recursively stops for all $x^* \geqslant x_0$ later.
2. For all $x^* \geqslant x_1$, $\tau(x, x^*, X_2, \ldots, X_n) = 1$ and for all $x^* < x_1$, $\tau(x, x^*, X_2, \ldots, X_n) = 1 + \tau^{'}(x^*, X_2, \ldots, X_n)$ for some $\tau^{'} \in \mathcal{F}_{n-1}(x^*, X_2, \ldots, X_n)$. This corresponds to the case that the specialized stopping time stops for all $x^* \geqslant x_1$ and recursively stops for all $x^* \leqslant x_1$ later.

To prove Theorem 14, it suffices to prove the following claim.

▷ Claim 16. Let $C'_1(x) = x(1-x)$ and the curve C'_n is achieved by applying transformation T on the curve C'_{n-1} i.e. $C'_n = T\left(C'_{n-1}\right)$. Then, we have $g_n(x) = C'_n(x)$ for any $x \in [0,1]$.

We first describe the intuitive idea behind the proof and then give a technical proof afterwards.
Proof Sketch. We use induction on n to prove the claim. For $n = 1$ and for each $x \in [0,1]$, we have $g_1(x) = x(1-x) = C'_1(x)$. Now, we assume that for each $x \in [0,1]$, $g_n(x) = C'_n(x)$. Since $C'_{n+1}(X) = T\left(C'_n(X)\right)$, it suffices to prove that $g_{n+1}(X) = T\left(g_n(X)\right)$ because it implies that $g_{n+1}(X) = T\left(g_n(X)\right) = T\left(C'_n(X)\right) = C'_{n+1}(X)$. Let us consider martingale $(X_0, X_1, \ldots, X_n, X_{n+1})$ where $X_0 = x$ and $X_1 \in \{x^{(1)}, \ldots, x^{(t)}\}$. According to the induction hypothesis, the adversary is guaranteed to get $g_n(x^{(j)}) = C'_n(x^{(j)})$ as the score in any martingale of depth n if she chooses an appropriate stopping time in $\mathcal{F}_n(x^{(j)}, X_2, \ldots, X_{n+1})$. We define left marked edges as the set $\{j : x^{(j)} \leqslant x \text{ and } |x - x^{(j)}| \geqslant C^{'}_n(x^{(j)})\}$ and right marked edges as the set $\{j : x^{(j)} \geqslant x \text{ and } |x - x^{(j)}| \geqslant C^{'}_n(x^{(j)})\}$. Now, to prove that $g_{n+1}(X) = T\left(g_n(X)\right)$ it suffices to show that in any arbitrary martingale in $A_{n+1}(x)$, the maximum score that could be achieved by either stopping the martingale at only left marked edges at time 1 or stopping the martingale at only right marked edges at time 1, is always guaranteed to be greater than or equal to $T(g_n(x)) = T(C'_n(x)) = C'_{n+1}(x)$. In Figure 12, we are considering a martingale $(x, X_1, \ldots, X_n, X_{n+1})$ such that X_1 can take only two values either x_l or x_r with probabilities p_l and p_r respectively. Note that $x_l \leqslant x_S(x)$ and $x_L(x) \leqslant x_r$. Any specialized stopping time τ either stops at x_l and continues at x_r or stops at x_r and continues at x_l. Here, the curve C'_n represents the points $(x, g_n(x))$ for $0 \leqslant x \leqslant 1$. According to the induction hypothesis, in martingale $(x_l, X_2, \ldots, X_n)$, the score $g_n(x_l)$ is guaranteed to be achieved (so the contribution of score when martingale doesn't stop at this edge is $p_l g_n(x_l)$) but if martingale stops at time 1 at edge (x, x_l), then the contribution of score for this edge is $p_l|x - x_l|$. A similar thing can be said about x_r. We can observe that while the point $Q^{''}$ (which is the intersection of line $D_l U_r$ with line $X = x$ and its height corresponds to the score achieved when martingale stops at x_r and continues at x_l) lies below the point $Q = (x, g_{n+1}(x))$ (which is the intersection of line P_1P_2 with line $X = x$ and its height corresponds to $T(g_n(x))$), the point $Q^{'}$ (which is the intersection of line $U_l D_r$ with line $X = x$ and its height corresponds to the score achieved by stopping martingale at x_l and allowing it to continue at x_r) is above the point Q. Observe that the maximum of the two scores achieved in these two strategies is always greater than or equal to $T(g_n(x))$. Moreover, if x_S is chosen as x_l and x_L is chosen as x_r, then $Q = Q^{'} = Q^{''}$ and the value $T(C'_n)(x)$ can be achieved for some martingale. This means that $g_{n+1}(x) = T(g_n(x)) = T(C'_n(x)) = C'_{n+1}(x)$ for any $x \in [0,1]$.

5.3 Black-box Separation Results

Gordon and Katz [22] introduced the notion of $1/p$-*unfair secure computation* for a fine-grained study of fair computation of functionalities. In this terminology, Theorem 13 states that $\frac{c}{\sqrt{n+1}}X_0(1-X_0)$-unfair computation of a bias-X_0 coin is impossible for any positive constant $c < \frac{\sqrt{2}}{12}$ and $X_0 \in [0,1]$.

Cleve and Impagliazzo's result [15] states that $\frac{c}{\sqrt{n}}$-unfair secure computation of the bias-1/2 coin is impossible for any positive constant $c < \frac{1}{2560}$. This result on the hardness of computation of fair coin-tossing was translated into black-box separations results. These results [16, 23, 17], intuitively, indicate that it is unlikely that $\frac{c}{\sqrt{n}}$-unfair secure computation of the bias-1/2 coin exists, for $c < \frac{1}{2560}$, relying solely on the black-box use of one-way functions. We emphasize that there are several restrictions imposed on the protocols that [16, 23, 17] consider; detailing all of which is beyond the scope of this draft. The problem in its full generality remains open. Substituting the result of [15] by Theorem 13, extends the results of [16, 23, 17] to general bias-X_0 coin-tossing protocols.

▶ **Corollary 17** (Informal: Black-box Separation). *For any $X_0 \in [0,1]$ and positive constant $c < \frac{\sqrt{2}}{12}$, the existence of $\frac{c}{\sqrt{n+1}}X_0(1-X_0)$-unfair computation protocol for a bias-X_0 coin is black-box separated from the existence of one-way functions (restricted to the classes of protocols considered by [16, 23, 17]).*

This black-box separation result extends to an arbitrary 2-party ω-faceted dice-rolling functionality. Let $S^* \subset \{0,1,\ldots,\omega-1\}$ be the subset of outcomes that maximizes $X_S(1-X_S)$, where X_S is the probability of the outcome being in S. Then, for any positive constant $c < \frac{\sqrt{2}}{12}$, the existence of $\frac{c}{\sqrt{n+1}}X_{S^*}(1-X_{S^*})$-unfair computation protocol for this ω-faceted dice rolling functionality is black-box separated from the existence of one-way functions.

6 Application 3 : Influencing Discrete Control Processes

Lichtenstein et al. [27] considered the problem of an adversary influencing the outcome of a stochastic process through mild interventions. For example, an adversary attempts to bias the outcome of a distributed n-processor coin-tossing protocol, where, in the i-th round, the processor i broadcasts her message. This model is also used to characterize randomness sources that are adversarially influenced, for example, [32, 26, 34, 30, 31, 33, 20, 18, 19, 12].

Consider the sample space $\Omega = \Omega_1 \times \Omega_2 \times \cdots \times \Omega_n$ and a joint distribution $(E_1,\ldots,E_n)$ over the sample space. We have a function $f\colon \Omega \to \{0,1\}$ such that $\mathbb{E}\left[f(E_1,\ldots,E_n)\right] = X_0$. This function represents the protocol that determines the final outcome from the public transcript. The filtration, at time-step i, reveals the value of the random variable E_i to the adversary. We consider the corresponding Doob's martingale $(X_0, X_1, \ldots, X_n)$. Intuitively, X_i represents the probability of $f(E_1,\ldots,E_n) = 1$ conditioned on the revealed values $(E_1 = e_1,\ldots,E_i = e_i)$. The adversary is allowed to intervene only once. She can choose to intervene at time-step i, reject the current sample $E_i = e_i$, and substitute it with a fresh sample from E_i. This intervention is identical to *restarting* the i-th processor if the adversary does not like her message. Note that this intervention changes the final outcome by

$$(X_{i-1}|E_1 = e_1,\ldots,E_{i-1} = e_{i-1}) - (X_i|E_1 = e_1,\ldots,E_i = e_i)$$

We shall use a stopping time τ to represent the time-step where an adversary decides to intervene. However, for some $(E_1 = e_1,\ldots,E_n = e_n)$ the adversary may not choose to intervene. Consequently, we consider stopping times $\tau\colon \Omega \to \{1,\ldots,n,\infty\}$, where the

stopping time being ∞ corresponds to the event that the adversary did not choose to intervene. In the Doob martingale discussed above, as a direct consequence of Theorem 1, there exists a stopping time τ^* with susceptibility $\geqslant C_n(X_0)$. Note that susceptibility measures the expected (unsigned) magnitude of the deviation, if an adversary intervenes at τ^*. Some of these contributions to susceptibility shall increase the probability of the final outcome being 1, and the remaining shall decrease the probability of the final outcome being 1. By an averaging argument, there exists a stopping time $\tau\colon \Omega \to \{1,\ldots,n,\infty\}$ that biases the outcome of f by at least $\geqslant \frac{1}{2}C_n(X_0)$, whence the following corollary.

▶ **Corollary 18** (Influencing Discrete Control Processes). *Let $\Omega_1,\ldots,\Omega_n$ be arbitrary sets, and $(E_1,\ldots,E_n)$ be a joint distribution over the set $\Omega := \Omega_1 \times \cdots \times \Omega_n$. Let $f\colon \Omega \to \{0,1\}$ be a function such that $\mathbb{P}\left[f(E_1,\ldots,E_n)=1\right] = X_0$. Then, there exists an adversarial strategy of intervening once to bias the probability of the outcome away from X_0 by $\geqslant \frac{1}{2}C_n(X_0) \geqslant \frac{1}{2}L_n(X_0) = \frac{1}{\sqrt{2n-1}}X_0(1-X_0)$.*

The previous result of [15] applies only to $X_0 = 1/2$ and they ensure a deviation of $1/320\sqrt{n}$. For $X_0 = 1/2$, our result ensures a deviation of (roughly) $1/4\sqrt{2n} \approx 1/5.66\sqrt{n}$.

6.1 Influencing Multi-faceted Dice-rolls

Corollary 18 generalizes to the setting where $f\colon \Omega \to \{0,1,\ldots,\omega-1\}$, i.e., the function f outputs an arbitrary ω-faceted dice roll. In fact, we quantify the deviation in the probability of any subset $S \subseteq \{0,1,\ldots,\omega-1\}$ of outcomes caused by an adversary intervening once.

▶ **Corollary 19** (Influencing Multi-faceted Dice-Rolls). *Let $\Omega_1,\ldots,\Omega_n$ be arbitrary sets, and $(E_1,\ldots,E_n)$ be a joint distribution over the set $\Omega := \Omega_1 \times \cdots \times \Omega_n$. Let $f\colon \Omega \to \{0,1,\ldots,\omega-1\}$ be a function with $\omega \geqslant 2$ outcomes, $S \subseteq \{0,1,\ldots,\omega-1\}$ be any subset of outcomes, and $\mathbb{P}\left[f(E_1,\ldots,E_n) \in S\right] = X_0$. Then, there exists an adversarial strategy of intervening once to bias the probability of the outcome being in S away from X_0 by $\geqslant \frac{1}{2}C_n(X_0) \geqslant \frac{1}{2}L_n(X_0) = \frac{1}{\sqrt{2n-1}}X_0(1-X_0)$.*

Corollary 18 and Corollary 19 are equivalent to each other. Clearly Corollary 18 is a special case of Corollary 19. Corollary 19, in turn, follows from Corollary 18 by considering "$f(E_1,\ldots,E_n) \in S$" as the interesting event for the martingale. We state these two results separately for conceptual clarity and ease of comparison with the prior work.

7 Application 4 : L_2 Gaps and their Tightness

In Section 3 we measured the gaps in martingales using the L_1-norm, here, we extend this analysis to gaps in martingales using the L_2-norm. To begin, let us fix X_0 and n. We change the definition of susceptibility to

$$\sup_{\text{stopping time } \tau} \mathbb{E}\left[(X_\tau - X_{\tau-1})^2\right]$$

Our objective is to characterize the martingale that is least susceptible

$$D_n(X_0) := \inf_{(X_0,\ldots,X_n)} \sup_{\text{stopping time } \tau} \mathbb{E}\left[(X_\tau - X_{\tau-1})^2\right]$$

Given. A curve D defined by the zeroes of the equation $Y = f(X)$, where $X \in [0,1]$.
Definition of the Transform. The transform of D, represented by $T'(D)$, is the curve defined by the zeroes of the equation $Y = g(X)$, where, for $x \in [0,1]$, the value of $g(x)$ is defined below.

1. Let $x_S(x), x_L(x) \in [0,1]$ be the two solutions of $f(X) = (X-x)^2$.
2. Then $g(x) := \text{G.M.}(y^{(1)}, y^{(2)})$, where $y^{(1)} = f(x_S(x))$, $y^{(2)} = f(x_L(x))$, and $\text{G.M.}(y^{(1)}, y^{(2)})$ represents the geometric mean of $y^{(1)}$ and $y^{(2)}$

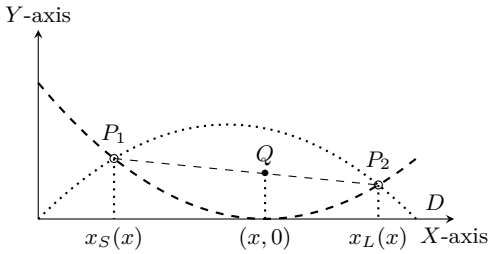

Figure 15 Definition of transform of a curve D, represented by $T'(D)$. The locus of the point Q (in the right figure) defines the curve $T'(D)$.

▶ **Theorem 20.** *Let $(X_0, X_1, \ldots, X_n)$ be a discrete-time martingale such that $X_n \in \{0,1\}$. Then, the following bound holds.*

$$\sup_{\text{stopping time } \tau} \mathbb{E}\left[(X_\tau - X_{\tau-1})^2\right] \geqslant D_n(X_0) := \frac{1}{n} X_0(1-X_0)$$

Furthermore, for all $n \geqslant 1$ and $X_0 \in [0,1]$, there exists a martingale $(X_0, \ldots, X_n)$ such that for any stopping time τ, it has $\mathbb{E}\left[(X_\tau - X_{\tau-1})^2\right] = D_n(X_0)$.

Proof. We shall proceed by induction on n.
Base Case $n = 1$**.** Note that in this case (see Figure 4) the optimal stopping time is $\tau = 1$.

$$\text{opt}_1(X_0, 2) = D_1(X_0) = (1-X_0)X_0^2 + X_0(1-X_0)^2 = X_0(1-X_0)$$

General Inductive Step. Let us fix $X_0 = x$ and $n = d \geqslant 2$. We proceed analogous to the argument in Section 3. The adversary can either decide to stop at the child j (see Figure 5 for reference) or continue to the subtree rooted at it to find a better stopping time.

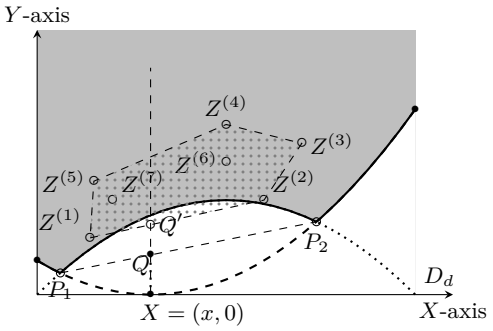

Figure 16 Intuitive Summary of the inductive argument. Our objective is to pick the set of points $\{Z^{(1)}, Z^{(2)} \ldots\}$ in the gray region to minimize the length of the intercept XQ' of their (lower) convex hull on the line $X = x$. Clearly, the unique optimal solution corresponds to including both P_1 and P_2 in this set.

Overall, the adversary gets the following contribution from the j-th child

$$\max\left\{(x^{(j)} - x)^2, D_{d-1}(x^{(j)})\right\}$$

The adversary obtains a score that is at least the height of Q in Figure 16. Further, a martingale designer can choose $t = 2$, and $Z^{(1)} = P_1$ and $Z^{(2)} = P_2$ to define the optimal

martingale. Similar to Theorem 1, the scores corresponding to all possible stopping times in the optimal martingale are identical.

We can argue that the height of Q is the geometric-mean of the heights of P_1 and P_2. This observation defines the geometric transformation T' in Figure 15. For this transformation, we demonstrate that $D_n(X_0) = \frac{1}{n}X_0(1-X_0)$ is the solution to the recursion $D_n = {T'}^{n-1}(D_1)$ in Claim 21. ◀

▷ Claim 21. Let D_1 be the curve defined as the zeros of the equation $Y = X(1-X)$ and for $n > 1$, D_n is obtained as applying the transformation T', defined in Figure 15, to the curve D_{n-1}. We claim that for each $x \in [0,1]$, $D_n(x) = d_n x(1-x)$ where $d_n = \frac{1}{n}$.

Proof. We use induction on n to prove that for each $x \in [0,1]$, we have $D_n(x) = d_n x(1-x)$ where $d_n = \frac{1}{n}$. Base case $n = 1$, is obvious. Now, assuming that $D_n(x) = d_n x(1-x)$ where $d_n = \frac{1}{n}$, we will prove that $D_{n+1}(x) = d_{n+1}x(1-x)$ where $d_{n+1} = \frac{1}{n+1}$. Let's fix $x \in [0,1]$ and let x_0 and x_1 be respectively the smaller and larger root of the equation $d_n x^*(1-x^*) = (x-x^*)^2$. Then we have:

$$x_0 = \frac{(2x+d_n) - \sqrt{d_n^2 + 4d_n x(1-x)}}{2(1+d_n)}$$

$$x_1 = \frac{(2x+d_n) + \sqrt{d_n^2 + 4d_n x(1-x)}}{2(1+d_n)}$$

Let $y_0 = d_n x_0(1-x_0)$ and $y_1 = d_n x_1(1-x_1)$, then we have the following relations:

$$y_0 = d_n \times \frac{(2x+d_n) - \sqrt{d_n^2 + 4d_n x(1-x)}}{2(1+d_n)} \times \frac{(2(1-x)+d_n) + \sqrt{d_n^2 + 4d_n x(1-x)}}{2(1+d_n)}$$

$$y_1 = d_n \times \frac{(2x+d_n) + \sqrt{d_n^2 + 4d_n x(1-x)}}{2(1+d_n)} \times \frac{(2(1-x)+d_n) - \sqrt{d_n^2 + 4d_n x(1-x)}}{2(1+d_n)}$$

Now, according to the definition of transformation T' in Figure 15, we have $D_{n+1}(x) = \sqrt{y_0 y_1}$ and:

$$\begin{aligned}
\sqrt{y_0 y_1} &= \frac{d_n}{4(1+d_n)^2} \times \sqrt{\left((2x+d_n)^2 - \left(d_n^2 + 4d_n x(1-x)\right)\right)\left(\left(2(1-x)+d_n\right)^2 - \left(d_n^2 + 4d_n x(1-x)\right)\right)} \\
&= \frac{d_n}{4(1+d_n)^2} \times \sqrt{\left(4x^2(1+d_n)\right)\left(4(1-x)^2(1+d_n)\right)} = \frac{d_n}{1+d_n}x(1-x) = \frac{\frac{1}{n}}{1+\frac{1}{n}}x(1-x) \\
&= \frac{1}{n+1}x(1-x)
\end{aligned}$$

◀

Note that, for any martingale $(X_0, \ldots, X_n)$ with $X_n \in \{0,1\}$, we have $\mathbb{E}\left[\sum_{i=1}^{n}(X_i - X_{i-1})^2\right] = \mathbb{E}\left[X_n^2 - X_0^2\right] = X_0(1-X_0)$. Therefore, by an averaging argument, there exists a round i such that $\mathbb{E}\left[(X_i - X_{i-1})^2\right] \geqslant \frac{1}{n}X_0(1-X_0)$. Theorem 20 proves the existence of a martingale that achieves the lower-bound even for non-constant stopping times. This result provides a technique to obtain the upper-bound to $C_n(X)$ in Lemma 2.

7.1 Alternate Proof for $U_{n+1} \succcurlyeq T(U_n)$

Proof. Recall that we defined D_n as the zeros of the curve $Y = \frac{1}{n}X(1-X)$. Since U_n is defined by the zeros of the curve $Y = \sqrt{\frac{1}{n}X(1-X)}$, by squaring the Y-values for U_n, we can obtain the curve D_n. This is illustrated in Figure 17. Denote points on curve U_n as $P_1 := (x_0, y_0)$, $P_2 := (x_1, y_1)$ and points on curve D_n as $P_1' := (x_0, y_0')$, $P_2' := (x_1, y_1')$. In the left-hand figure, let $\alpha := x - x_0$ and $\beta := x_1 - x$, then $y_0 = \alpha$ and $y_1 = \beta$ and $Q = H.M.(\alpha, \beta)$. After squaring, in the right-hand figure $Q = (H.M.(\alpha, \beta))^2$. Note by definition of the transformation T', we have that $Q' = G.M.(\alpha^2, \beta^2)$. We show that $G.M.(\alpha^2, \beta^2) \geqslant (H.M.(\alpha, \beta))^2$ as follows

$$
\begin{aligned}
& G.M.(\alpha^2, \beta^2) \geqslant \big(H.M.(\alpha, \beta)\big)^2 \\
\iff \quad & \Big(G.M.(\alpha^2, \beta^2)\Big)^{1/2} \geqslant H.M.(\alpha, \beta) \\
\iff \quad & G.M.(\alpha, \beta) \geqslant H.M.(\alpha, \beta),
\end{aligned}
$$

which is true by the standard $G.M. \geqslant H.M.$ inequality. Now recall that the locus of the point Q' defines the curve $T'(D_n) = D_{n+1}$ (From Claim 21) and we know that $D_{n+1} = U_{n+1}^2$. Also, after squaring the Y-axis, the locus of the point Q defines the curve $T^2(U_n)$, therefore we have just shown that $U_{n+1}^2 \succcurlyeq T^2(U_n)$, which means that $U_{n+1} \succcurlyeq T(U_n)$. ◀

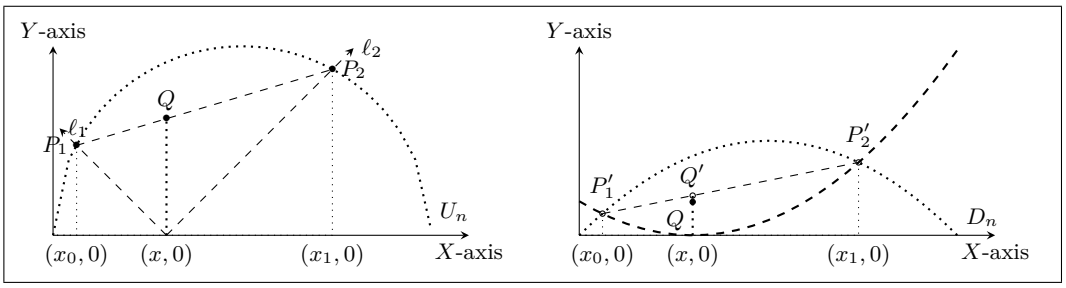

Figure 17 Intuitive summary of the Proof of Claim 8. In the left-hand figure, we have U_n and the locus of the point Q defines the curve $T(U_n)$. Recall that D_n is defined by the zeros of the curve $Y = \frac{1}{n}X(1-X)$. Intuitively we can say that $D_n = (U_n)^2$. By squaring the Y-axis in the left-hand figure, we get the right-hand figure. Since $D_{n+1} = T^{'}(D_n)$ (From Claim 21) , and the locus of the point Q' defines this curve, we only need to show that Q' is always above Q in the right-hand figure in order to prove our original claim.

References

1 Bar Alon and Eran Omri. Almost-optimally fair multiparty coin-tossing with nearly three-quarters malicious. In Martin Hirt and Adam D. Smith, editors, *TCC 2016-B: 14th Theory of Cryptography Conference, Part I*, volume 9985 of *Lecture Notes in Computer Science*, pages 307–335, Beijing, China, October 31 – November 3, 2016. Springer, Heidelberg, Germany. doi:10.1007/978-3-662-53641-4_13.

2 Benny Applebaum, Ivan Damgård, Yuval Ishai, Michael Nielsen, and Lior Zichron. Secure arithmetic computation with constant computational overhead. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology – CRYPTO 2017, Part I*, volume 10401 of *Lecture Notes in Computer Science*, pages 223–254, Santa Barbara, CA, USA, August 20–24, 2017. Springer, Heidelberg, Germany. doi:10.1007/978-3-319-63688-7_8.

3 Gilad Asharov. Towards characterizing complete fairness in secure two-party computation. In Yehuda Lindell, editor, *TCC 2014: 11th Theory of Cryptography Conference*, volume 8349 of *Lecture Notes in Computer Science*, pages 291–316, San Diego, CA, USA, February 24–26, 2014. Springer, Heidelberg, Germany. doi:10.1007/978-3-642-54242-8_13.

4 Gilad Asharov, Amos Beimel, Nikolaos Makriyannis, and Eran Omri. Complete characterization of fairness in secure two-party computation of Boolean functions. In Yevgeniy Dodis and Jesper Buus Nielsen, editors, *TCC 2015: 12th Theory of Cryptography Conference, Part I*, volume 9014 of *Lecture Notes in Computer Science*, pages 199–228, Warsaw, Poland, March 23–25, 2015. Springer, Heidelberg, Germany. doi:10.1007/978-3-662-46494-6_10.

5 Gilad Asharov, Yehuda Lindell, and Tal Rabin. A full characterization of functions that imply fair coin tossing and ramifications to fairness. In Amit Sahai, editor, *TCC 2013: 10th Theory of Cryptography Conference*, volume 7785 of *Lecture Notes in Computer Science*, pages 243–262, Tokyo, Japan, March 3–6, 2013. Springer, Heidelberg, Germany. doi:10.1007/978-3-642-36594-2_14.

6 Baruch Awerbuch, Manuel Blum, Benny Chor, Shafi Goldwasser, and Silvio Micali. How to implement bracha's O(log n) byzantine agreement algorithm. *Unpublished manuscript*, 1985.

7 Kazuoki Azuma. Weighted sums of certain dependent random variables. *Tohoku Math. J. (2)*, 19(3):357–367, 1967. URL: https://doi.org/10.2748/tmj/1178243286, doi:10.2748/tmj/1178243286.

8 Amos Beimel, Iftach Haitner, Nikolaos Makriyannis, and Eran Omri. Tighter bounds on multi-party coin flipping via augmented weak martingales and differentially private sampling. In *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 838–849. IEEE, 2018.

9 Amos Beimel, Yehuda Lindell, Eran Omri, and Ilan Orlov. $1/p$-Secure multiparty computation without honest majority and the best of both worlds. In Phillip Rogaway, editor, *Advances in Cryptology – CRYPTO 2011*, volume 6841 of *Lecture Notes in Computer Science*, pages 277–296, Santa Barbara, CA, USA, August 14–18, 2011. Springer, Heidelberg, Germany. doi:10.1007/978-3-642-22792-9_16.

10 Amos Beimel, Eran Omri, and Ilan Orlov. Protocols for multiparty coin toss with dishonest majority. In Tal Rabin, editor, *Advances in Cryptology – CRYPTO 2010*, volume 6223 of *Lecture Notes in Computer Science*, pages 538–557, Santa Barbara, CA, USA, August 15–19, 2010. Springer, Heidelberg, Germany. doi:10.1007/978-3-642-14623-7_29.

11 Manuel Blum. How to exchange (secret) keys (extended abstract). In *15th Annual ACM Symposium on Theory of Computing*, pages 440–447, Boston, MA, USA, April 25–27, 1983. ACM Press. doi:10.1145/800061.808775.

12 Carl Bosley and Yevgeniy Dodis. Does privacy require true randomness? In Salil P. Vadhan, editor, *TCC 2007: 4th Theory of Cryptography Conference*, volume 4392 of *Lecture Notes in Computer Science*, pages 1–20, Amsterdam, The Netherlands, February 21–24, 2007. Springer, Heidelberg, Germany. doi:10.1007/978-3-540-70936-7_1.

13 Niv Buchbinder, Iftach Haitner, Nissan Levi, and Eliad Tsfadia. Fair coin flipping: Tighter analysis and the many-party case. In Philip N. Klein, editor, *28th Annual ACM-SIAM*

Symposium on Discrete Algorithms, pages 2580–2600, Barcelona, Spain, January 16–19, 2017. ACM-SIAM. doi:10.1137/1.9781611974782.170.

14 Richard Cleve. Limits on the security of coin flips when half the processors are faulty (extended abstract). In *18th Annual ACM Symposium on Theory of Computing*, pages 364–369, Berkeley, CA, USA, May 28–30, 1986. ACM Press. doi:10.1145/12130.12168.

15 Richard Cleve and Russell Impagliazzo. Martingales, collective coin flipping and discrete control processes (extended abstract), 1993.

16 Dana Dachman-Soled, Yehuda Lindell, Mohammad Mahmoody, and Tal Malkin. On the black-box complexity of optimally-fair coin tossing. In Yuval Ishai, editor, *TCC 2011: 8th Theory of Cryptography Conference*, volume 6597 of *Lecture Notes in Computer Science*, pages 450–467, Providence, RI, USA, March 28–30, 2011. Springer, Heidelberg, Germany. doi:10.1007/978-3-642-19571-6_27.

17 Dana Dachman-Soled, Mohammad Mahmoody, and Tal Malkin. Can optimally-fair coin tossing be based on one-way functions? In Yehuda Lindell, editor, *TCC 2014: 11th Theory of Cryptography Conference*, volume 8349 of *Lecture Notes in Computer Science*, pages 217–239, San Diego, CA, USA, February 24–26, 2014. Springer, Heidelberg, Germany. doi:10.1007/978-3-642-54242-8_10.

18 Yevgeniy Dodis, Shien Jin Ong, Manoj Prabhakaran, and Amit Sahai. On the (im)possibility of cryptography with imperfect randomness. In *45th Annual Symposium on Foundations of Computer Science*, pages 196–205, Rome, Italy, October 17–19, 2004. IEEE Computer Society Press. doi:10.1109/FOCS.2004.44.

19 Yevgeniy Dodis, Krzysztof Pietrzak, and Bartosz Przydatek. Separating sources for encryption and secret sharing. In Shai Halevi and Tal Rabin, editors, *TCC 2006: 3rd Theory of Cryptography Conference*, volume 3876 of *Lecture Notes in Computer Science*, pages 601–616, New York, NY, USA, March 4–7, 2006. Springer, Heidelberg, Germany. doi:10.1007/11681878_31.

20 Yevgeniy Dodis and Joel Spencer. On the (non)universality of the one-time pad. In *43rd Annual Symposium on Foundations of Computer Science*, pages 376–387, Vancouver, British Columbia, Canada, November 16–19, 2002. IEEE Computer Society Press. doi:10.1109/SFCS.2002.1181962.

21 S. Dov Gordon, Carmit Hazay, Jonathan Katz, and Yehuda Lindell. Complete fairness in secure two-party computation. In Richard E. Ladner and Cynthia Dwork, editors, *40th Annual ACM Symposium on Theory of Computing*, pages 413–422, Victoria, British Columbia, Canada, May 17–20, 2008. ACM Press. doi:10.1145/1374376.1374436.

22 S. Dov Gordon and Jonathan Katz. Partial fairness in secure two-party computation. In Henri Gilbert, editor, *Advances in Cryptology – EUROCRYPT 2010*, volume 6110 of *Lecture Notes in Computer Science*, pages 157–176, French Riviera, May 30 – June 3, 2010. Springer, Heidelberg, Germany. doi:10.1007/978-3-642-13190-5_8.

23 Iftach Haitner, Eran Omri, and Hila Zarosim. Limits on the usefulness of random oracles. In Amit Sahai, editor, *TCC 2013: 10th Theory of Cryptography Conference*, volume 7785 of *Lecture Notes in Computer Science*, pages 437–456, Tokyo, Japan, March 3–6, 2013. Springer, Heidelberg, Germany. doi:10.1007/978-3-642-36594-2_25.

24 Iftach Haitner and Eliad Tsfadia. An almost-optimally fair three-party coin-flipping protocol. In David B. Shmoys, editor, *46th Annual ACM Symposium on Theory of Computing*, pages 408–416, New York, NY, USA, May 31 – June 3, 2014. ACM Press. doi:10.1145/2591796.2591842.

25 Wassily Hoeffding. Probability inequalities for sums of bounded random variables. *Journal of the American Statistical Association*, 58(301):13–30, 1963. URL: https://www.tandfonline.com/doi/abs/10.1080/01621459.1963.10500830, arXiv:https://www.tandfonline.com/doi/pdf/10.1080/01621459.1963.10500830, doi:10.1080/01621459.1963.10500830.

26 Claire Kenyon, Yuval Rabani, and Alistair Sinclair. Biased random walks, lyapunov functions, and stochastic analysis of best fit bin packing (preliminary version). In Éva Tardos, editor,

7th Annual ACM-SIAM Symposium on Discrete Algorithms, pages 351–358, Atlanta, Georgia, USA, January 28–30, 1996. ACM-SIAM.

27 David Lichtenstein, Nati Linial, and Michael Saks. Some extremal problems arising from discrete control processes. 9:269–287, 09 1989.

28 Nikolaos Makriyannis. On the classification of finite boolean functions up to fairness. In *International Conference on Security and Cryptography for Networks*, pages 135–154. Springer, 2014.

29 Tal Moran, Moni Naor, and Gil Segev. An optimally fair coin toss. In Omer Reingold, editor, *TCC 2009: 6th Theory of Cryptography Conference*, volume 5444 of *Lecture Notes in Computer Science*, pages 1–18. Springer, Heidelberg, Germany, March 15–17, 2009. doi:10.1007/978-3-642-00457-5_1.

30 Noam Nisan. Extracting randomness: how and why-a survey. In *ccc*, page 44. IEEE, 1996.

31 Noam Nisan and Amnon Ta-Shma. Extracting randomness: A survey and new constructions. *J. Comput. Syst. Sci.*, 58(1):148–173, 1999.

32 Aravind Srinivasan and David Zuckerman. Computing with very weak random sources. In *35th Annual Symposium on Foundations of Computer Science*, pages 264–275, Santa Fe, New Mexico, November 20–22, 1994. IEEE Computer Society Press. doi:10.1109/SFCS.1994.365688.

33 Luca Trevisan and Salil P. Vadhan. Extracting randomness from samplable distributions. In *41st Annual Symposium on Foundations of Computer Science*, pages 32–42, Redondo Beach, CA, USA, November 12–14, 2000. IEEE Computer Society Press. doi:10.1109/SFCS.2000.892063.

34 David Zuckerman. Simulating bpp using a general weak random source. *Algorithmica*, 16(4-5):367–391, 1996.

A More Technical Proof of Theorem 1

▷ Claim 22. For each $d \geqslant 1$, let C_d denote a curve over $X \in [0,1]$ that includes all points $(x, \mathrm{opt}_d(x,1))$. Let T be the transformation defined in Figure 7. Then, $C_d = T^{d-1}(C_1)$ where T^0 denotes the identity transformation and T^k denotes the transformation achieved by composing T with itself k times. Moreover, for every depth d, there exists a martingale of bias x whose max-score in L_1-norm is equal to $\mathrm{opt}_d(x,1)$ and for each $i = 1, \ldots, n$, $|\Omega_i| = 2$.

Proof. Let C_1 be the curve defined by the zeros of the equation $Y = 2X(1-X)$ such that $Y \geqslant 0$. Let C_{d+1} be the curve obtained by applying the transformation T on C_d.
Let $X' = \{X' = \{X'_i\}_{i=0}^n, E' = \{E'_i\}_{i=1}^n\}$ be a martingale over the sample space $\Omega' = \Omega'_1 \times \cdots \times \Omega'_n$ such that for each $i \in [n]$, $\Omega'_i = \{0,1\}, E'_i(0) = l, E'_i(1) = r, X'_0 = x$, for each $(e_1, e_2, \ldots, e_{n-1}) \in \{l,r\}^{n-1}$, $X'_n(e_1, \ldots, e_{n-1}, l) = 0$ and $X'_n(e_1, \ldots, e_{n-1}, r) = 1$, for each $i \in \{1, \ldots, n-1\}$, $X'_i(e_1, e_2, \ldots, e_{i-1}, l)$ is the X coordinate of the interception of the line $Y = -X + X'_{i-1}(e_1, \ldots, e_{i-1})$ and the curve C_{n-i}, and $X'_i(e_1, e_2, \ldots, e_{i-1}, r)$ is the X coordinate of the interception of the line $Y = X - X'_{i-1}(e_1, \ldots, e_{i-1})$ and the curve C_{n-i}. Moreover, for each $(e_1, e_2, \ldots, e_{i-1}) \in \{l,r\}^{i-1}$,

$$\Pr[l | E'_1 = e_1, \ldots, E'_{i-1} = e_{i-1}] = \frac{X'_i(e_1, \ldots, e_{i-1}, r) - X'_{i-1}(e_1, \ldots, e_{i-1})}{X'_i(e_1, \ldots, e_{i-1}, r) - X'_i(e_1, \ldots, e_{i-1}, l)}$$

and

$$\Pr[r | E'_1 = e_1, \ldots, E'_{i-1} = e_{i-1}] = \frac{X'_{i-1}(e_1, \ldots, e_{i-1}) - X'_i(e_1, \ldots, e_{i-1}, l)}{X'_i(e_1, \ldots, e_{i-1}, r) - X'_i(e_1, \ldots, e_{i-1}, l)}$$

We claim that for each martingale $\{X = \{X_i\}_{i=1}^n, E = \{E_i\}_{i=1}^n\}$ with respect to the sample space $\Omega = \Omega_1 \times \cdots \times \Omega_n$, we have $\text{max-score}_1(X, E) \geqslant \text{max-score}_1(X', E')$ and so $\mathrm{opt}_d(x,1) = \text{max-score}_1(X', E')$.
We prove our claim by induction on the depth of the martingale i.e. n.
For the base case $n = 1$, suppose $\Omega_1 = \{1, \ldots, t\}$, $E_1(j) = e_1^{(j)}$. Without loss of generality, we assume that $X_1(e_1^{(1)}) \leqslant X_1(e_1^{(2)}) \cdots \leqslant X_1(e_1^{(t)})$. Then there exist $p^{(1)}, \ldots, p^{(n)}$ such that $x = \sum_{j=1}^t p^{(j)} X_1(e_1^{(j)})$ and $\sum_{j=1}^t p^{(j)} = 1$. In this case, since $X_1(e_1^{(j)})$ is 0 or 1, there exists some s such that $x = \sum_{j=s+1}^t p^{(j)}$ and

$$\text{max-score}_1(X, E) = (p^{(1)} + \cdots + p^{(s)})x + (p^{(s+1)} + \cdots + p^{(t)})(1-x) = 2x(1-x)$$

But, the maximum score of a martingale (X, E) with respect to $\Omega_1 = \{0,1\}$ such that $\Pr[0] = x$ and $\Pr[1] = 1 - x$ is also $2x(1-x)$.
Suppose that the claim is true for depth d, and we want to prove it for the depth $d+1$.
Suppose that the martingale $\{X = \{X_i\}_{i=0}^{d+1}, E = \{E_i\}_{i=1}^{d+1}\}$ over $\Omega = \Omega_1 \times \Omega_2 \times \cdots \times \Omega_{d+1}$ is given such that $\Omega_1 = \{1, \ldots, t\}$ and for each $j \in \Omega_1$, $E_1(j) = e_1^{(j)}$.

Note that for each $j \in \{1, 2, \ldots, t\}$, we define the martingale $\{V^{(j)} = \{V_i^{(j)}\}_{i=0}^d, E^{(j)} = \{E_i^{(j)}\}_{i=2}^{d+1}\}$ over $\Omega_2 \times \cdots \times \Omega_{d+1}$ where $V_i^{(j)}(e_2, \ldots, e_{d+1}) := X_{i+1}(e_1^{(j)}, e_2, \ldots, e_{d+1})$ is a martingale of depth d. Observe that for any j and any value of $V_0 = X_1(e_1^{(j)})$, there exists an stopping time $\tau_{max}^{(j)}(V^{(j)}, E^{(j)}) : \Omega_2 \times \cdots \times \Omega_{d+1} \to \{2, \ldots, n\}$ that maximizes the score of the martingale $(V^{(j)}, E^{(j)})$. Now, note that $\tau_{max}(X, E)(e_1^{(j)}, e_2, \ldots, e_{d+1})$ equals 1 (which means that the martingale stops at time 1) when

$$|X_0 - X_1(e_1^{(j)})| \geqslant \text{max-score}_1(V^{(j)}, E^{(j)})$$

or equals $\tau_{max}^{(j)}(V^{(j)}, E^{(j)})(e_2, \ldots, e_{d+1})$ when

$$|X_0 - X_1(e_1^{(j)})| \leqslant \text{max-score}_1(V^{(j)}, E^{(j)})$$

Let us define $B_j := \max(\text{max-score}_1(V^{(j)}, E^{(j)}), |X_0 - X_1(e_1^{(j)})|)$. We represent each point $Z^{(j)} =: (X_1(e_1^{(j)}), B_j)$ in a plane, see Figure 8. In this plane, for each point (x, y), the value y represents the score of a stopping time in a martingale whose average is x (the first value that the martingale takes). Since X is a martingale, we have $X_0 = \sum_{j=1}^{t} p^{(j)} X_1(e_1^{(j)})$. It also follows from the definition of B_j that

$$\text{max-score}_1(X, E) = \sum_{j=1}^{t} \Pr[E_1 = j] B_j = \sum_{j=1}^{t} p^{(j)} B_j.$$

Therefore, we have

$$(X_0, \text{max-score}_1(X, E)) = \sum_{j=1}^{t} p^{(j)} (X_1(e_1^{(j)}), B_j) = \sum_{j=1}^{t} p^{(j)} Z^{(j)}.$$

Consequently, the point $(X_0, \text{max-score}_1(X, E))$ lies on the intersection of the line $X = X_0$ and the convex hull of the points $Z^{(1)}, \ldots, Z^{(t)}$ (Note that the argument is true even if we assume that t is not finite).

It follows from the inductive hypothesis that for each j, there exists a martingale of depth d, $\{X'^{(j)} = \{X_i'^{(j)}\}_{i=1}^{d+1}, E'^{(j)} = \{E_i'^{(j)}\}_{i=2}^{d+1}\}$ over $\Omega_2' \times \cdots \times \Omega_{d+1}'$ such that $X_1'^{(j)} = X_1(e_1^{(j)})$ and for each $i \in \{2, \ldots, d+1\}$, $|\Omega_i'| = 2$ and $\text{max-score}_1(X', E') = \text{opt}_d(X_1'^{(j)}, 1) = \text{opt}_d(X_1(e_1^{(j)}))$. Therefore, $\text{max-score}_1(V^{(j)}, E^{(j)}) \geqslant \text{opt}_d(X_1(e_1^{(j)}), 1)$. This implies that

$$B_j \geqslant \max(\text{opt}_d(X_1(e_1^{(j)}), 1), |X_0 - X_1(e_1^{(j)})|)$$

that means the points $Z^{(1)}, \ldots, Z^{(t)}$ lie above the curve defined by the zeros of the equation $Y = \max(\text{opt}_d(X, 1), |X_0 - X|) = \max(C_d(X), |X - X_0|)$. Note that according to the inductive hypothesis, C_d (the zeros of the equation $Y = \text{opt}_d(X, 1)$) is equal to the curve $T^{d-1}(C_1)$ which is concave downward as a consequence of Claim 7. Thus, the intersection of the line $X = X_0$ and the convex hull of the points $Z^{(1)}, \ldots, Z^{(t)}$ is above the point $Q = (x, C_{d+1}(x))$, see Figure 8. Moreover, by choosing $t = 2$ and $Z^{(1)} = P_1$ and $Z^{(2)} = P_2$, the score $T(C_d)(x)$ (point Q) can be achieved. But, note that according to the inductive hypothesis, the points P_1 and P_2 can be achieved by the martingale $\{X'^{(j)} = \{X_i'^{(j)}\}_{i=1}^{d+1}, E'^{(j)} = \{E_i'^{(j)}\}_{i=2}^{d+1}\}$. This shows that the martingale of depth $d + 1$ with optimal score is achieved when for each $i \in \{1, \ldots, d+1\}$, $|\Omega_i| = 2$. Also as mentioned earlier, the height of the point Q is $T(C_d)(x)$ and according to induction hypothesis, $C_d(x) = T^{d-1}(C_1)(x)$, so $\text{opt}_{d+1}(x, 1) = T^d(C_1)(x)$. ◀