# Martingales, Collective Coin Flipping and Discrete Control Processes

(Extended Abstract)

Richard Cleve*

Department of Computer Science
The University of Calgary
Calgary, Alberta, Canada T2N 1N4
E-mail: cleve@cpsc.ucalgary.ca

Russell Impagliazzo†

Computer Science and Engineering
University of California, San Diego
La Jolla, CA 92093, U.S.A.
E-mail: russell@cs.ucsd.edu

November, 1993

**Abstract**

We show that for *any* martingale $X_0, X_1, \ldots, X_n$ with $X_0 = \frac{1}{2}$ and $X_n \in \{0,1\}$,

$$\Pr[\exists i \in \{1,\ldots,n\}, |X_i - X_{i-1}| > \tfrac{1}{32\sqrt{n}}] > \tfrac{1}{5}.$$

In other words, if information is released concerning the status of an event with *a priori* probability $\frac{1}{2}$ in $n$ "press releases" (the last of which reveals either that the event happened or did not happen) then there is at least a constant probability that one of the press releases changes the conditional probability of the event by $\Omega(1/\sqrt{n})$. This is related to (but is not a direct consequence of) the "martingale tail inequality" of Azuma (1967) and Heoffding (1963).

During the execution of a multiparty protocol (or game), the evolution of the information of its participants can be modeled as a martingale. Consequently, our result has implications concerning the security/robustness of protocols. In particular, for an $r$-round protocol, with probability $\Omega(1)$, there is some round where one player can predict the final outcome with probability $\Omega(1/\sqrt{r})$ greater than the others. We illustrate consequences of this in two specific settings: collective-coin flipping and discrete control processes.

In particular, we show that, for any $r$-round two-party collective coin-flipping protocol in a model where envelopes (bit commitments) are provided as a primitive, there must be one player that can bias the outcome of the other player by $\Omega(1/\sqrt{r})$—and there is a specific protocol which shows that this lower bound is tight (previous results only imply a lower bound of $\Omega(1/r)$). Also, by a straightforward reduction from the $m$-party case to the 2-party case, for any $m$-party $r$-round collective coin-flipping protocol, there is a coalition of $\lceil \frac{m}{2} \rceil$ players that can bias the output of the remaining players by $\Omega(1/m^2\sqrt{r})$.

We also show that a one-sided version of a result of Lichtenstein *et al.* (1989) concerning discrete control processes holds in a much more general setting: the domain can be extended from $\{0,1\}^n$ with the uniform distribution to an arbitrary cartesian product of $n$ sets with an arbitrary distribution.

*Research supported in part by NSERC of Canada. Work partially done while a Postdoctoral Fellow at the International Computer Science Institute, Berkeley.

†Work partially done while an NSERC Postdoctoral Fellow, Computer Science Department, University of Toronto.

# 1 Introduction

A *martingale* is a sequence of random variables that arises when information about some event is revealed in $n$ stages, where partial information is revealed at each stage. (A formal definition of a martingale is given in Section 2.)

One area where martingales arise naturally is as a model of the evolution of knowledge during the execution of a multiparty protocol (or game). For example, suppose that, at the termination of some protocol, a specific event either occurs or does not occur. For each party, consider her expectation of the event occurring after the $i^{\text{th}}$ round of the protocol. This is a sequence of random variables $X_0, X_1, \ldots$ ($X_0$ for the *a priori* expectation, and $X_i$ for the expectation after the $i^{\text{th}}$ round). This sequence is a martingale—regardless of the specifics of the protocol.

Aspnes and Waart (1992) proposed a protocol for "randomized consensus" and used the theory of martingales in the proof its correctness. Our approach in the present paper is to use martingales to prove "lower bounds" for protocols (i.e. to show that within a certain number of rounds, some specific protocol problems *cannot* be solved by *any* protocol).

Our main result is that for *any* martingale $X_0, X_1, \ldots, X_n$ with $X_0 = \frac{1}{2}$ and $X_n \in \{0, 1\}$,

$$\Pr[\exists i \in \{1, \ldots, n\}, |X_i - X_{i-1}| > \tfrac{1}{32\sqrt{n}}] > \tfrac{1}{5}.$$

This complements the martingale tail inequality of Azuma (1967) and Heoffding (1963) (Theorem 1, in Section 2), where there is an absolute bound on $|X_i - X_{i-1}|$ for all $i \in \{1, \ldots, n\}$ and the probability that $|X_n - X_0|$ is "large" is bounded above. It should be noted that, by simply expressing Theorem 1 in its contrapositive form (with appropriate parameters), one cannot directly deduce more than $\Pr[\exists i \in \{1, \ldots, n\}, |X_i - X_{i-1}| > \frac{1}{32\sqrt{n}}] > 0$. To obtain an $\Omega(1)$ lower bound on this probability is more difficult.

Our methodology is, roughly, as follows. We distinguish between the "steps" that are larger than some $\frac{c}{\sqrt{n}}$ and those that are smaller. The complication that arises is that the neither the small steps taken alone nor the large steps taken alone are martingales, and thus are more difficult to analyze separately. In our analysis, we show that the small steps taken alone are a "biased" martingale, and, provided that the "cumulative bias" is sufficienlty small, a version of Theorem 1 that takes the bias into account applies. In the case where the "cumulative bias" is not small enough, we establish a linear relationship between the bias at each stage and the probability that a large step will be taken in the next stage. If the cumulative bias is large then a "poisson-like" phenomenon occurs, resulting in a lower bound on the probability of at least one large step occurring.

It is noteworthy that the following two properties *cannot* be claimed about martingales. Firstly, "$\exists i \in \{1, \ldots, n\}$, $|X_i - X_{i-1}|$" cannot be replaced by "$\exists i \in \{1, \ldots, n\}$, $X_i - X_{i-1}$" in the above inequality (i.e. the "large" gap may only be possible in one direction). In particular, there exists a specific martingale $X_0, X_1, \ldots, X_n$ with $X_0 = \frac{1}{2}$ and $X_n \in \{0, 1\}$, such that $X_i - X_{i-1} \leq \frac{1}{2n}$ for all $i \in \{1, \ldots, n\}$ with probability 1. Secondly, "$\exists i \in \{1, \ldots, n\}$, $|X_i - X_{i-1}|$" cannot be replaced by "$\frac{1}{n}\sum_{i=1}^{n} |X_i - X_{i-1}|$" (i.e. "maximum step size" cannot be replaced by "average step size") in the above inequality. In particular, there exists a specific martingale $X_0, X_1, \ldots, X_n$ with $X_0 = \frac{1}{2}$ and $X_n \in \{0, 1\}$, such that $\frac{1}{n}\sum_{i=1}^{n} |X_i - X_{i-1}| = \frac{1}{2n}$ with probability 1.

In Section 2, we define martingales and state the martingale tail inequality of Azuma (1967) and Hoeffding (1963). In Section 3, we prove our main result about martingales. In Section 4, we explain the applications of the result to collective coin flipping protocols. In Section 5, we explain the applications of the result to discrete control processes.

## 2 Martingales: Definitions and a Previous Result

**Definition:** A sequence of random variables $X_0, X_1, \ldots, X_n$ is a *martingale* if, for all $i \in \{1, \ldots, n\}$,

$$\mathrm{E}[X_i | X_0, \ldots, X_{i-1}] = X_{i-1}.$$

If $X_0, X_1, \ldots, X_n$ is a martingale then the sequence $Y_1, \ldots, Y_n$, defined as

$$Y_i = X_i - X_{i-1},$$

is the corresponding *martingale difference sequence*. Martingale difference sequences are characterized by the property that, for all $i \in \{1, \ldots, n\}$,

$$\mathrm{E}[Y_i | Y_1, \ldots, Y_{i-1}] = 0.$$

The following result, due to Azuma (1967) and Hoeffding (1963), is often referred to as the "Martingale Tail Inequality," or "Azuma's Inequality."

**Theorem 1 (Azuma 1967; Hoeffding 1963):** *Suppose that the martingale difference sequence $Y_1, \ldots, Y_n$ satisfies $|Y_i| \leq s$ for $i = 1, \ldots, n$. Then, for all $\lambda > 0$,*

$$\Pr\left[\left|\sum_{i=1}^{n} Y_i\right| \geq \lambda s\sqrt{n}\right] \leq 2e^{-\lambda^2/2}.$$

## 3 New Result About Martingales

**Theorem 2:** *Let $X_0, X_1, \ldots, X_n$ be any martingale distribution such that $X_0 = \frac{1}{2}$ and $X_n \in \{0, 1\}$. Then, for any $c > 0$, and any $\delta$ such that $0 < \delta < \frac{1}{2}$,*

$$\Pr\left[\max_{i \in \{1,\ldots,n\}} |X_i - X_{i-1}| > \frac{c}{\sqrt{n}}\right] > 1 - 2e^{-\delta^2/8c^2} - e^{-1/2+\delta}.$$

*In particular, setting $c = \frac{1}{32}$ and $\delta = \frac{1}{4}$,*

$$\Pr\left[\max_{i \in \{1,\ldots,n\}} |X_i - X_{i-1}| > \frac{1}{32\sqrt{n}}\right] > \frac{1}{5}.$$

The proof of Theorem 1 will be established by a series of lemmas. Throughout, we use the following definitions. The sequence $X_0, X_1, \ldots, X_n$ is an arbitrary martingale such that $X_0 = \frac{1}{2}$ and $X_n \in \{0, 1\}$ (this also implies that $X_1, \ldots, X_{n-1} \in [0, 1]$). Let $Y_1, \ldots, Y_n$ be the corresponding martingale difference sequence. That is, for all $i \in \{1, \ldots, n\}$,

$$Y_i = X_i - X_{i-1}.$$

Let $c > 0$ and $\delta \in (0, \frac{1}{2})$ be constants. For each $i \in \{1, \ldots, n\}$, define the following random variables:

$$\begin{aligned} W_i &= \begin{cases} 1 & \text{if } |Y_i| \leq \frac{c}{\sqrt{n}} \\ 0 & \text{otherwise} \end{cases} \\ S_i &= W_i \cdot Y_i \\ L_i &= \overline{W_i} \cdot Y_i \\ B_i &= \mathrm{E}[S_i | Y_1, \ldots, Y_{i-1}]. \end{aligned}$$

The sequence $S_1, \ldots, S_n$ represents the "small steps" of the martingale and the sequence $L_1, \ldots, L_n$ represents the "large steps." Note that neither $S_1, \ldots, S_n$ nor $L_1, \ldots, L_n$ are, in general, martingale difference sequences. For $i \in \{1, \ldots, n\}$, the random variable $B_i$ may be thought of as the "conditional bias" of $S_i$. To prove Theorem 2, it is sufficient to upper bound the quantity

$$\Pr[W_1 \wedge \cdots \wedge W_n].$$

**Lemma 3:**

$$\Pr\left[W_1 \wedge \cdots \wedge W_n\right] \leq \Pr\left[\left|\sum_{i=1}^{n}(S_i - B_i)\right| \geq \delta\right] + \Pr\left[\left|\sum_{i=1}^{n} B_i\right| \geq \frac{1}{2} - \delta \wedge W_1 \wedge \cdots \wedge W_n\right].$$

**Proof:** The conditions given for the above random variables imply that

$$\frac{1}{2} = \left|\sum_{i=1}^{n} Y_i\right| \leq \left|\sum_{i=1}^{n} S_i\right| + \left|\sum_{i=1}^{n} L_i\right| \leq \left|\sum_{i=1}^{n}(S_i - B_i)\right| + \left|\sum_{i=1}^{n} B_i\right| + \left|\sum_{i=1}^{n} L_i\right|.$$

Therefore,

$$\Pr\left[\left|\sum_{i=1}^{n}(S_i - B_i)\right| \geq \delta\right] + \Pr\left[\left|\sum_{i=1}^{n} B_i\right| + \left|\sum_{i=1}^{n} L_i\right| \geq \frac{1}{2} - \delta\right] \geq 1.$$

Also, since $W_i = 1$ implies $L_i = 0$ (for all $i \in \{1, \ldots, n\}$),

$$\begin{aligned} &\Pr\left[\left|\sum_{i=1}^{n} B_i\right| + \left|\sum_{i=1}^{n} L_i\right| \geq \frac{1}{2} - \delta\right] \\ &= \Pr\left[\left|\sum_{i=1}^{n} B_i\right| \geq \frac{1}{2} - \delta \wedge W_1 \wedge \cdots \wedge W_n\right] + \Pr\left[\left|\sum_{i=1}^{n} B_i\right| + \left|\sum_{i=1}^{n} L_i\right| \geq \frac{1}{2} - \delta \wedge \overline{(W_1 \wedge \cdots \wedge W_n)}\right] \\ &\leq \Pr\left[\left|\sum_{i=1}^{n} B_i\right| \geq \frac{1}{2} - \delta \wedge W_1 \wedge \cdots \wedge W_n\right] + \Pr\left[\overline{W_1} \vee \cdots \vee \overline{W_n}\right]. \end{aligned}$$

The result follows from these two latter inequalities.□

We shall upper bound the two terms in the right side of the inequality in Lemma 3 separately.

**Lemma 4:**

$$\Pr\left[\left|\sum_{i=1}^{n}(S_i - B_i)\right| \geq \delta\right] < 2e^{-\delta^2/8c^2}.$$

**Proof:** First, we establish that $S_1 - B_1, \ldots, S_n - B_n$ is a martingale difference sequence. This is because, for each $i \in \{1, \ldots, n\}$, $S_1 - B_1, \ldots, S_{i-1} - B_{i-1}$ is determined by $Y_1, \ldots, Y_{i-1}$ and

$$\begin{aligned}
\mathrm{E}[S_i - B_i | Y_1, \ldots, Y_{i-1}] &= \mathrm{E}[S_i | Y_1, \ldots, Y_{i-1}] - \mathrm{E}[B_i | Y_1, \ldots, Y_{i-1}] \\
&= \mathrm{E}[S_i | Y_1, \ldots, Y_{i-1}] - \mathrm{E}[\mathrm{E}[S_i | Y_1, \ldots, Y_{i-1}] | Y_1, \ldots, Y_{i-1}] \\
&= \mathrm{E}[S_i | Y_1, \ldots, Y_{i-1}] - \mathrm{E}[S_i | Y_1, \ldots, Y_{i-1}] \\
&= 0.
\end{aligned}$$

Secondly, for all $i \in \{1, \ldots, n\}$, $|S_i| \leq \frac{c}{\sqrt{n}}$ and $|B_i| \leq \frac{c}{\sqrt{n}}$, which implies that $|S_i - B_i| \leq \frac{2c}{\sqrt{n}}$. Therefore, applying Theorem 1 (with $s = \frac{2c}{\sqrt{n}}$ and $\lambda = \frac{\delta}{2c}$),

$$\Pr\left[\left|\sum_{i=1}^{n}(S_i - B_i)\right| \geq \delta\right] = \Pr\left[\left|\sum_{i=1}^{n}(S_i - B_i)\right| \geq \left(\frac{\delta}{2c}\right)\left(\frac{2c}{\sqrt{n}}\right)\sqrt{n}\right] < 2e^{-\delta^2/8c^2},$$

as required.□

**Lemma 5:** *For all $i \in \{1, \ldots, n\}$,*

$$\mathrm{E}\left[\overline{W_i}\middle| Y_1, \ldots, Y_{i-1}\right] \geq |B_i|.$$

**Proof:** For all $i \in \{1, \ldots, n\}$, since $Y_i = W_i \cdot Y_i + \overline{W_i} \cdot Y_i$,

$$\mathrm{E}\left[\overline{W_i} \cdot Y_i\middle| Y_1, \ldots, Y_{i-1}\right] + \mathrm{E}\left[W_i \cdot Y_i | Y_1, \ldots, Y_{i-1}\right] = \mathrm{E}\left[Y_i | Y_1, \ldots, Y_{i-1}\right] = 0.$$

Also, for each $i \in \{1, \ldots, n\}$, since $|Y_i| \leq 1$,

$$\begin{aligned}
\mathrm{E}\left[\overline{W_i}\middle| Y_1, \ldots, Y_{i-1}\right] &\geq \mathrm{E}\left[\overline{W_i} \cdot |Y_i|\middle| Y_1, \ldots, Y_{i-1}\right] \\
&\geq \left|\mathrm{E}\left[\overline{W_i} \cdot Y_i\middle| Y_1, \ldots, Y_{i-1}\right]\right| \\
&= \left|\mathrm{E}\left[W_i \cdot Y_i\middle| Y_1, \ldots, Y_{i-1}\right]\right| \\
&= \left|\mathrm{E}\left[S_i\middle| Y_1, \ldots, Y_{i-1}\right]\right| \\
&= |B_i|. \square
\end{aligned}$$

**Lemma 6:** *Let $A_1, \ldots, A_n$ be an arbitrary sequence of random variables, and, for each $i \in \{1, \ldots, n\}$, let $D_i$ be a $\{0,1\}$-valued random variable (i.e. an event) whose value is completely determined by the values of $A_1, \ldots, A_i$. For each $i \in \{1, \ldots, n\}$, let $C_i = \mathrm{E}[D_i | A_1, \ldots, A_{i-1}]$. Then, for any real number $r$,*

$$\Pr\left[\sum_{i=1}^{n} C_i \geq r \wedge \overline{D_1} \wedge \cdots \wedge \overline{D_n}\right] \leq e^{-r}.$$

**Proof:** The proof is by induction on $n$. Note that $C_1 = \mathrm{E}[D_1]$ is a constant. Therefore

$$\Pr\left[C_1 \geq r \wedge \overline{D_1}\right] \leq \begin{cases} \mathrm{E}\left[\overline{D_1}\right] \leq 1 - r \leq e^{-r} & \text{if } C_1 \geq r \\ 0 < e^{-r} & \text{if } C_1 < r. \end{cases}$$

This establishes the result when $n = 1$. Now, when $n > 1$, we have

$$\begin{aligned}
&\Pr\left[\sum_{i=1}^{n} C_i \geq r \wedge \overline{D_1} \wedge \cdots \wedge \overline{D_n}\right] \\
&= \Pr\left[\overline{D_1}\right] \cdot \Pr\left[\sum_{i=2}^{n} C_i \geq r - C_1 \wedge \overline{D_2} \wedge \cdots \wedge \overline{D_n} \middle| \overline{D_1}\right] \\
&\leq (1 - C_1) \cdot \sup_{\substack{a_1 \\ D_1(a_1)=0}} \Pr\left[\sum_{i=2}^{n} C_i \geq r - C_1 \wedge \overline{D_2} \wedge \cdots \wedge \overline{D_n} \middle| A_1 = a_1\right].
\end{aligned}$$

For any value of $a_1$, by applying the lemma inductively on the $n-1$ length sequences $A_2, \ldots, A_n$, $D_2, \ldots, D_n$, and $C_2, \ldots, C_n$, where the distributions are conditional on $A_1 = a_1$, we obtain

$$\Pr\left[\sum_{i=2}^{n} C_i \geq r - C_1 \wedge \overline{D_2} \wedge \cdots \wedge \overline{D_n} \middle| A_1 = a_1\right] \leq e^{-(r-C_1)}.$$

Therefore,

$$\Pr\left[\sum_{i=1}^{n} C_i \geq r \wedge \overline{D_1} \wedge \cdots \wedge \overline{D_n}\right] \leq (1 - C_1) \cdot e^{-(r-C_1)} \leq e^{-C_1} \cdot e^{-(r-C_1)} = e^{-r},$$

which completes the proof.□

**Lemma 7:**

$$\Pr\left[\left|\sum_{i=1}^{n} B_i\right| \geq \frac{1}{2} - \delta \wedge W_1 \wedge \cdots \wedge W_n\right] \leq e^{-1/2+\delta}.$$

**Proof:** Applying Lemma 6, with $A_1, \ldots, A_n$ set to $Y_1, \ldots, Y_n$ (respectively), $D_1, \ldots, D_n$ set to $\overline{W_1}, \ldots, \overline{W_n}$ (respectively), and $C_i = \mathrm{E}\left[\overline{W_i} \middle| Y_1, \ldots, Y_n\right]$ for each $i \in \{1, \ldots, n\}$, we obtain

$$\Pr\left[\sum_{i=1}^{n} C_i \geq \frac{1}{2} - \delta \wedge W_1 \wedge \cdots \wedge W_n\right] \leq e^{-(1/2-\delta)}.$$

Also, by Lemma 5, we have $C_i \geq |B_i|$ for each $i \in \{1, \ldots, n\}$, so

$$\Pr\left[\left|\sum_{i=1}^{n} B_i\right| \geq \frac{1}{2} - \delta \wedge W_1 \wedge \cdots \wedge W_n\right] \leq \Pr\left[\sum_{i=1}^{n} C_i \geq \frac{1}{2} - \delta \wedge W_1 \wedge \cdots \wedge W_n\right].$$

The result follows.□

**Proof of Theorem 2:** This clearly follows by combining Lemmas 3, 4, and 7.□

# 4 Applications to Collective Coin Flipping Protocols

In this section, we show that for any $r$-round two-party collective coin-flipping protocol in a model where envelopes (bit commitments) are provided as a primitive, there must be one player that can bias the outcome of the other player by $\Omega(1/\sqrt{r})$. Since there is a protocol that can be implemented

in this model for which the bias cannot be more than $O(1/\sqrt{r})$, the above lower bound is tight. As far as we know, the best lower bound that can be derived from previous techniques is $\Omega(1/r)$ (Cleve, 1986).

These results carry over to case of $m$-party $r$-round collective coin-flipping protocols with envelopes (by a straightforward reduction of the $m$-party case to the 2-party case). The result is that there is always a coalition of $\lceil \frac{m}{2} \rceil$ players that can bias the output of the remaining players by $\Omega(1/m^2\sqrt{r})$.

### 4.1 Basic Definitions

(Several "collective coin flipping" scenarios have been proposed in the literature—see Ben-Or and Linial (1989) and Chor and Dwork (1989) for surveys.)

Define an *(r-round two-party) bit selection scheme* as a pair of interacting probabilistic Turing machines $(A, B)$ that send messages back and forth in $r$ rounds, where a round consists of $A$ sending a message to $B$ followed by $B$ sending a mesage to $A$. After $(A, B)$ is run, both $A$ and $B$ output one-bit values $a$ and $b$ (respectively). Moreover, even if $A$ is replaced by $A'$, an arbitrary Turing machine, and $(A', B)$ is run, $B$ outputs some bit $b$ (and a similar condition holds whenever $B$ is replaced by $B'$).

Call a bit selection scheme a *collective coin flipping protocol* if, whenever $(A, B)$ in run, $a = b$ and $\Pr[a = 0] = \Pr[a = 1] = \frac{1}{2}$. (There are more general notions of a collective coin flipping protocol, that permits a small probability of $a \neq b$ occurring and a small bias of the distributions. We address these in the final paper.)

We are interested in how much bias an adversarial $A'$ can impose on $B$'s output $b$, when $(A', B)$ is executed, as well as the complementary bias for an adversarial $B'$. Informally, the "security" of a protocol $(A, B)$ is related to how robust the distribution of its output is when it is run with some adversarial $A'$ or $B'$. In a secure protocol, no adversarial player can impose a large bias.

Four basic models that we consider are the following.

**Information Theoretic Model:** No limit on the computational power of the Turing machines.

**Cryptographic Model:** The protocol is paramaterized by a number $n$ (the "security parameter") and the Turing machines must run in time polynomial in $n$. (Thus, cryptographic tools such as one-way and trapdoor functions are potentially applicable.)

**Envelope Model:** There is no limit on the computational power of the Turing machines, but it is assumed that there is a *built-in* primitive that permits bit-commitments to be made. In a bit-commitment, a player may, at some round, commit to the value of some bit to the other player. This process reveals no information about the value of the bit; however, at a later round, the player has the option of decommiting the value of this bit, thereby revealing its value to the other player. The important feature of commit/decommit is that, after committing a specific value $x$, a player cannot later decommit to a different value than $x$.

**Fail-Stop Model:** There is no limit on the computational power of the Turing machines, but an adversarial $A'$ or $B'$ can only deviate from the protocol by quitting early. By quitting early, we mean, from some round onwards, sending only null messages back to the other player. Thus the execution of, say, $A'$ may always be viewed as an exact simulation of $A$, combined with an arbitrary computation on the side to determine at each round whether (presumably according to some strategy) to quit at that particular round or not.

The fail-stop model is stronger than the envelope model by the following.

**Claim 8:** *Any collective coin flipping protocol $(A, B)$ in the envelope model may be simulated by a collective coin flipping protocol $(A^*, B^*)$ in the fail-stop model, preserving security in the following sense. If an adversarial $A^{*\prime}$ can impose a bias on $b^*$ when $(A^{*\prime}, B^*)$ is executed then there is an adversarial $A'$ that can impose the same bias on $b$ when $(A', B)$ is executed. A similar condition holds for an adversarial $B^{*\prime}$.*

We do not prove this formally in this abstract. The idea behind the proof is that bit-commitment is trivial to implement in the fail-stop model: to commit the value $x$, a player can simply announce to the other player that he has committed to some value (without revealing the value). At a later round, if the protocol dictates, he can reveal $x$, but he cannot reveal a value different from $x$, because this would entail deviating from the protocol.

### 4.2 Previous Results

A straightforward argument shows that, in the information theoretic model, essentially no security is attainable. For any collective coin flipping protocol $(A, B)$, either there exists an $A'$ such that, whenever $(A', B)$ is run, $b = 1$, or there exists a $B'$ such that, whenever $(A, B')$ is run, $a = 0$. This implies that, in this model, any collective coin flipping protocol can be biased by $\frac{1}{2}$.

In the cryptographic model, assuming that one-way functions exist, there is a simple $r$-round protocol (Cleve, 1986) for which the the maximum bias possible is $O(1/\sqrt{r})$. This protocol uses an implementation of bit-commitment based on one-way functions. Also, there is a proof that in this model any protocol $(A, B)$ can be biased by $\Omega(1/r)$.

For the envelope model, the cryptographic upper and lower bounds can be adapted to apply. Thus, there is a protocol $(A, B)$ for which the maximum bias possible is $O(1/\sqrt{r})$, and, for any protocol, an adversarial player can impose a bias of $\Omega(1/r)$. (In the next subsection, we use Theorem 2 to improve the lower bound to $\Omega(1/\sqrt{r})$, thereby matching the upper bound.)

### 4.3 New Result

In view of Claim 8, to prove a lower bound in the envelope model, it suffices to prove the lower bound in the fail-stop model.

**Theorem 9:** *Let $(A, B)$ be any $r$-round collective coin flipping protocol in the fail-stop model. Then there is either: an adversarial $A'$ such that, when $(A', B)$ is executed, $b$ is biased by $\frac{1}{2560}\frac{1}{\sqrt{2r}} \in \Omega(1/\sqrt{r})$ in some direction; or there is an adversarial $B'$ such that, when $(A, B')$ is executed, $a$ is biased by $\frac{1}{2560}\frac{1}{\sqrt{2r}} \in \Omega(1/\sqrt{r})$ in some direction.*

**Proof:** Let $X$ and $Y$ denote the random strings that $A$ and $B$ use (respectively) to make their random choices (the underlying probability space consists of all possible pairs $(X, Y)$). Let $M_1, M_2, \ldots, M_{2r}$ denote the messages that are sent when $(A, B)$ is executed (at round $i$, $A$ sends $M_{2i-1}$ to $B$ and $B$ sends $M_{2i}$ to $A$). Let $C$ be the output of $(A, B)$, when run to completion. Define $C_1, C_2, \ldots, C_{2r}$ as follows. For $i \in \{1, 2, \ldots, r\}$, $C_{2i-1}$ is the output of $B$ when $A$ quits at round $i$, and $C_{2i}$ is the output of $A$ when $B$ quits at round $i$. Note that all these quantities are functions of $(X, Y)$.

Define the random variables $P_0, P_1, \ldots, P_{2r}$ as follows. For $j \in \{0, 1, \ldots, 2r\}$,

$$P_j(X, Y) = \mathrm{E}_{(X', Y')}[C(X', Y') | (M_1, \ldots, M_j)(X', Y') = (M_1, \ldots, M_j)(X, Y)].$$

Intuitively, $P_j$ is the expected final value of the protocol $(A, B)$, conditioned on the values of the first $j$ messages exchanged by the parties.

Note that $P_0, P_1, \ldots, P_{2r}$ is a martingale, and, since $(A, B)$ is a collective coin flipping protocol, we must have $P_0 = \frac{1}{2}$ and $P_{2r} \in \{0, 1\}$. Therefore Theorem 2 applies and, with probability greater than $\frac{1}{5}$, there exists a $j \in \{1, \ldots, 2r\}$, such that $|P_j - P_{j-1}| > \frac{1}{32\sqrt{2r}}$.

Define the random variables $Q_1, \ldots, Q_{2r}$ as follows. For $j \in \{0, 1, \ldots, 2r\}$,

$$Q_j(X, Y) = \mathrm{E}_{(X', Y')}[C_j(X', Y') | (M_1, \ldots, M_{j-1})(X', Y') = (M_1, \ldots, M_{j-1})(X, Y)].$$

Intuitively, $Q_j$ is the expected value output by the other party if one party quits right after $M_{j-1}$ was sent, conditioned on the values of the first $j-1$ messages exchanged by the parties.

Since, for all $j \in \{1, \ldots, 2r\}$, $|P_j - Q_j| + |Q_j - P_{j-1}| \geq |P_j - P_{j-1}|$, we may express the event that there exists a $j \in \{1, \ldots, 2r\}$ such that $|P_j - P_{j-1}| > \frac{1}{32\sqrt{2r}}$ as the union of these eight events:

$G_{A,0}$ : $\exists i \in \{1, \ldots, r\}$ such that $P_{2i-1} - Q_{2i-1} > \frac{1}{64\sqrt{2r}}$

$G_{A,1}$ : $\exists i \in \{1, \ldots, r\}$ such that $P_{2i-1} - Q_{2i-1} < -\frac{1}{64\sqrt{2r}}$

$G_{B,0}$ : $\exists i \in \{1, \ldots, r\}$ such that $P_{2i} - Q_{2i} > \frac{1}{64\sqrt{2r}}$

$G_{B,1}$ : $\exists i \in \{1, \ldots, r\}$ such that $P_{2i} - Q_{2i} < -\frac{1}{64\sqrt{2r}}$

$H_{A,0}$ : $\exists i \in \{1, \ldots, r\}$ such that $P_{2i-2} - Q_{2i-1} > \frac{1}{64\sqrt{2r}}$

$H_{A,1}$ : $\exists i \in \{1, \ldots, r\}$ such that $P_{2i-2} - Q_{2i-1} < -\frac{1}{64\sqrt{2r}}$

$H_{B,0}$ : $\exists i \in \{1, \ldots, r\}$ such that $P_{2i-1} - Q_{2i} > \frac{1}{64\sqrt{2r}}$

$H_{B,1}$ : $\exists i \in \{1, \ldots, r\}$ such that $P_{2i-1} - Q_{2i} < -\frac{1}{64\sqrt{2r}}$

Since

$$\Pr[G_{A,0} \vee G_{A,1} \vee G_{B,0} \vee G_{B,1} \vee H_{A,0} \vee H_{A,1} \vee H_{B,0} \vee H_{B,1}] > \tfrac{1}{5},$$

at least one of these eight events must occur with probability greater than $(\frac{1}{8})(\frac{1}{5}) = \frac{1}{40}$.

Suppose $\Pr[G_{A,0}] > \frac{1}{40}$. Then consider the following adversarial $A'$: simulate $A$ until a round $i$ occurs where $P_{2i-1} - Q_{2i-1} > \frac{1}{64\sqrt{2r}}$ (these quantities can be determined with the information that $A$ has in round $i$) in which case quit. When $(A', B)$ is executed, $\Pr[b = 0] > \frac{1}{2} + \frac{1}{40}\frac{1}{64\sqrt{2r}}$, so the bias that $A'$ imposes is $\frac{1}{2560\sqrt{2r}} \in \Omega(1/\sqrt{r})$. The cases corresponding to $G_{A,1}$, $G_{B,0}$, $G_{B,1}$ are handled similarly (each yielding an $A'$ or $B'$ that can impose a bias in some direction). The case where $\Pr[H_{A,0}] > \frac{1}{40}$ is also similar. Here, define the adversarial $A''$: simulate $A$ until a round $i$ occurs where $P_{2i-2} - Q_{2i-1} > \frac{1}{64\sqrt{2r}}$ in which case quit. (Note that, in this case, $A''$ does not consider $P_{2i-1}$, even though he has sufficient information to do so.) The cases corresponding to $H_{A,1}$, $H_{B,0}$, $H_{B,1}$ are also handled similarly. □

## 5 Applications to Discrete Control Processes

In this section, we present a sketch of a generalization of a result of Lichtenstein *et al.* (1989), concerning the robustness of $n$-stage "discrete control processes."

## 5.1 Previous Definitions and Results

Lichtenstein *et al.* (1989) proposed an abstract model of a "discrete control process" that can be defined in the following way. Let $f : \{0,1\}^n \to \{0,1\}$ be a function, and let $d = |f^{-1}(1)|/2^n$. Clearly, if $(X_1, \ldots, X_n) \in \{0,1\}^n$ is sampled according to the uniform distribution then $\Pr[f(X_1, \ldots, X_n) = 1] = d$. Now, suppose that a "player" (who may be regarded as an adversary or an ally, depending on your point of view) can "intervene" during the generation of $(X_1, \ldots, X_n) \in \{0,1\}^n$ in the following way. There are $n$ stages, and at the $i$-th stage, the player (who knows $f$) sees the values of $X_1, \ldots, X_{i-1}$, and, based on this, has the option to *intervene* at this stage by determining the value of $X_i$. Questions that Lichtenstein *et al.* address are (for an arbitrary $f : \{0,1\}^n \to \{0,1\}$, and $k \in \{1, \ldots, n\}$):

1. What is the maximum amount by which the player can bias the value of $\Pr[f(X_1, \ldots, X_n) = 1]$ away from $d$, given that the total number of interventions allowed is $k$?

2. Given $\delta \in (0, \frac{1}{2})$, what is the expected number of interventions that the player requires to impose a bias of $\delta$ on $\Pr[f(X_1, \ldots, X_n) = 1]$?

Lichtenstein *et al.* investigate both of these questions in detail. Their results are based on combinatorial arguments in extremal set theory. One particular consequence of their results is the following.

**Theorem 10 (Lichtenstein *et al.* 1989):** *For any function $f : \{0,1\}^n \to \{0,1\}$ for which $|f^{-1}(1)|/2^n = \frac{1}{2}$, there is a strategy with which the player can bias $\Pr[f(X_1, \ldots, X_n) = 1]$ away from $\frac{1}{2}$ by $\Omega(1/\sqrt{n})$ (and this bias can be imposed in either direction).*

## 5.2 New Definitions and Result

A discrete control process can be generalized in two ways. First, the domain of $f$ can be generalized from $\{0,1\}^n$ to the cartesian product of any $n$ sets $S_1 \times \cdots \times S_n$. For example, suppose $f : (\{0,1\}^n)^n \to \{0,1\}$ and $|f^{-1}(1)|/2^{n^2} = \frac{1}{2}$. (In this setting, an intervention would be for an entire $n$-bit block.) It is not clear whether any of the results of Lichtenstein *et al.* carry over in this case. A second way of generalizing the problem is to change the distribution on the domain from the uniform distribution to an arbitrary distribution. For example, suppose $f : \{0,1\}^n \to \{0,1\}$ and $(X_1, \ldots, X_n) \in \{0,1\}^n$ is generated according to an arbitrary distribution such that, according to that distribution, $\Pr[f(X_1, \ldots, X_n) = 1] = \frac{1}{2}$. Here, since $X_1, \ldots, X_n$ are not independently distributed, we have to be precise about how an intervention at stage $i$ affects the distribution of $X_{i+1}, \ldots, X_n$. A natural definition is to assume that $X_1, \ldots, X_n$ are generated sequentially in the following way. For each $i \in \{1, \ldots, n\}$, once $X_1, \ldots, X_{i-1}$ have been determined as $x_1, \ldots, x_{i-1}$ (respectively), $X_i$ is generated (assuming no intervention at stage $i$) according to the conditional probability $\Pr[X_i = 1 | X_1, \ldots, X_{i-1} = x_1, \ldots, x_{i-1}]$. It is also not clear whether any of the results of Lichtenstein *et al.* carry over for this case.

We consider a generalization of a discrete control process that includes both of the above generalizations. Let $S_1, \ldots, S_n$ be arbitrary sets, $f : S_1 \times \cdots \times S_n \to \{0,1\}$, and Pr be an arbitrary probability distribution on $S_1 \times \cdots \times S_n$. Suppose that $\Pr[f(X_1, \ldots, X_n) = 1] = \frac{1}{2}$. The generation of $(X_1, \ldots, X_n) \in S_1 \times \cdots \times S_n$ can be partitioned into $n$ stages, where, at the $i$-th stage, assuming $X_1, \ldots, X_{i-1}$ have been determined as $x_1, \ldots, x_{i-1}$ (respectively), $X_i$ is generated according to the conditional probability $\Pr[X_i = 1 | X_1, \ldots, X_{i-1} = x_1, \ldots, x_{i-1}]$. Suppose that a player can *intervene* in the following way. After the $i$-th stage, the player can request a "retake" of the generation of

$X_i$. (That is, *after* the $i$-th stage, upon seeing the values of $X_1, \ldots, X_i$, the player can request to rewind the process back to the *beginning* of the $i$-th stage and have $X_i$ resampled.) Note that this is a *weaker* notion of an intervention than the one considered by Lichtenstein *et al.* (since it does not permit the player to completely determine $X_i$). From Theorem 2, the following can be proven.

**Theorem 11:** *Let $S_1, \ldots, S_n$ be arbitrary sets, $f : S_1 \times \cdots \times S_n \to \{0,1\}$, and* Pr *be an arbitrary probability distribution on $S_1 \times \cdots \times S_n$ such that $\Pr[f(X_1, \ldots, X_n) = 1] = \frac{1}{2}$. Then there exists a strategy with which the player can bias $\Pr[f(X_1, \ldots, X_n) = 1]$ away from $\frac{1}{2}$ by $\frac{1}{320\sqrt{n}} \in \Omega(1/\sqrt{n})$ in some direction.*

**Proof (Sketch):** Since the player's knowledge of $\Pr[f(X_1, \ldots, X_n) = 1]$ through the stages is a martingale, Theorem 2 applies, and, there must be *some* direction for which a gap of size $\frac{1}{32\sqrt{n}}$ occurs with probability $> \frac{1}{10}$. The player's strategy is to intervene when such a gap occurs.□

It is noteworthy that the one-sidedness in the above theorem cannot be eliminated.

## References


Alon, N. and M. Naor (1993), "Coin-Flipping Games Immune Against Linear-Sized Coalitions," *SIAM J. Comput.*, Vol. 22, No. 2, pp. 403–417. (Preliminary version in *Proc. 31st Ann. IEEE Symp. on Foundations of Computer Sci.*, pp. 46–54, 1990.)

Aspnes, J. and O. Waarts (1992), "Randomized Consensus in Expected $O(n \log^2 n)$ Operations Per Processor," *Proc. 33rd Ann. IEEE Symp. on Foundations of Computer Sci.*, pp. 137–146.

Azuma, K. (1967), "Weighted Sums of Certain Dependent Random Variables," *Tôkuku Math. J.*, Vol. 19, pp. 357–367.

Ben-Or, M. and N. Linial (1989), "Collective Coin Flipping," in *Advances in Computing Research 5: Randomness and Computation*, S. Micali (Ed.), JAI Press, Greenwich, CT. (Preliminary version: "Collective Coin Flipping, Robust Voting Schemes and Minimal Banzhaf Values," *Proc. 26th Ann. IEEE Symp. on Foundations of Computer Sci.*, pp. 408–416, 1985.)

Blum, M. (1982), "Coin Flipping by Telephone: a Protocol for Solving Impossible Problems", *Spring COMPCON Conf.*, pp. 133–137.

Broder, A. and D. Dolev (1984), "Flipping Coins in Many Pockets," *Proc. 25th Ann. IEEE Symp. on Foundations of Computer Sci.*, pp. 157–170.

Chor, B. and C. Dwork (1989), "Randomization in Byzantine Agreement," in *Advances in Computing Research 5: Randomness and Computation*, S. Micali (Ed.), JAI Press, Greenwich, CT.

Cleve, R. (1986), "Limits on the Security of Coin Flips When Half the Processors are Faulty," *Proc. 18th Ann. ACM Symp. on Theory of Comput.*, pp. 364–369.

Heoffding, W. (1963), "Probability Inequalities for Sums of Bounded Random Variables," *J. Amer. Statist. Assoc.*, Vol. 58, pp. 13–30.

Kahn, J, G. Kalai, and N. Linial (1988), "The Influence of Variables on Boolean Functions," *Proc. 29th Ann. IEEE Symp. on Foundations of Computer Sci.*, pp. 68–80.

Lichtenstein, D., N. Linial, and M. Saks (1989), "Some Extremal Problems Arising from Discrete Control Processes," *Combinatorica*, Vol. 9, No. 3, pp. 269–287.

Saks, M. (1989), "A Robust Noncryptographic Protocol for Collective Coin Flipping," *SIAM J. Disc. Math.*, Vol. 2, No. 2, pp. 240–244.