A Representative Motivating Application

Distributed A Representative Motivating Application

Distributed Rolling Protocol.

- n Processes with access to a Broadcast Channel
- At time t ∈ {1, . . . , n}, the processor i broadcasts her message
- All processors agree on the same outcome at the end of the protocol
- The outcome is distributed uniformly over X0, X1, . . .

Adversarial Model.

Adversary can restart (at most) one processor before she broadcasts her message

Research Directions.

1. Given a protocol π, what is the maximum adversarial deviation in the outcome?
2. Which optimum protocol π∗ minimizes the adversarial deviation?

Modeling: Discrete-time Martingales

Sequence of random variables X = (X0, X1, . . .) releases information about the occurrence of an event over an n press releases
The value of Xt represents the probability that an event of interest occurs, conditioned on the first t messages

Property of Martingales.

Conditioned on the first t messages, the expected outcome in the future j > i is identical to the expected outcome now

Our Special Martingales.

Final event either occurs or not, i.e., Xn ∈ {0, 1}

Stopping Time τ.

Random variable indicating the time of adversarial interference
- Decision to stop the martingale at time i is a function only of the first t messages
- Stoping time τ need not be a constant

For example, different transcripts of a coin-tossing protocol are potentially stopped at different times

Our Martingale Problem Formulation

Game between the Martingale Designer and the Adversary

- Martingale Designer presents a martingale X to the Adversary
- Adversary identifies the worst susceptibility in the martingale X by identifying the corresponding stopping time τ as witness

Martingale Designers’s objective is to construct the martingale with the least “worst susceptibility”

Definition. susceptibility(τ, ρ) = E[|Xτ − Xρ|]

Problem Formalization. Characterize

\[
\min_X \max_\tau \text{susceptibility}(X, \tau)
\]

Find the optimum martingale

\[
\min_X \max_\tau \text{susceptibility}(X, \tau)
\]

Perspective

- Martingale X starts at X0 and ends at Xn ∈ {0, 1}
- Therefore, there exists a constant stopping time τ such that

\[
\text{susceptibility}(X, \tau) \geq \frac{\min_{i=0}^{n} |X_i - X_0|}{n}
\]

- For non-constant stopping times how large is the worst susceptibility?

Answer. [5] proved \(\frac{1}{\sqrt{n}}\) for X0 = 1/2

Prior Approaches

Azuma-Hoeffding Inequality. When \(X_i = X_i−1 + o(1/\sqrt{i})\), for all i ∈ {1, . . . , n} then, nearly always (Xn − X0) = o(1) (that is, Xn ∈ [0, 1]). So, \(|X_i − X_i−1| = o(1/\sqrt{i})\) somewhere

Beimel et al. [2] extend this bound to weak martingales (with additional properties useful to model multi-party coin-tossing protocols)

Our Results

- Main Theorem. Given a martingale, the Adversary can identify stopping time τ, where:

\[
\max \text{susceptibility}(X, \tau) \geq Cn(X)
\]

- Technique. Use geometric transformations to inductively define Cn(X)

Our Work

- Involves martingales and martingale susceptibility
- Our work focuses on the adversarial deviation

Application

- Influencing Discrete Control Processes

Problem Statement. Adversary influences outcome of a stochastic process by intervening only once [9]

Previous Result. For X0 = 1/2, deviation of \(\frac{1}{\sqrt{n}}\) by [5]

Our Result. For X0 = 1/2, deviation of \(\frac{1}{\sqrt{n}}\). In general, for any X0 ∈ [0, 1], deviation of \(\frac{1}{\sqrt{n}} X_0(1 − X_0)\)

- Fail Stop Attacks on Coin-Tossing & Dice-Rolling Protocols

Problem Statement. Two-party n-round bias-X0 coin-tossing protocol in non-cryptographic setting

Previous Result. For X0 = 1/2, deviation of \(\frac{1}{\sqrt{n}}\) by [5]

Our Result. For X0 = 1/2, deviation of \(\frac{1}{\sqrt{n}}\). In general, for any X0 ∈ [0, 1], deviation by \(\frac{1}{\sqrt{n}} X_0(1 − X_0)\)

- Distributed Coin-Tossing Protocols

Problem Statement. Distributed n-processor coin-tossing protocol in the Broadcast Channel (non-cryptographic setting)

Previous Result. Only protocol known for X0 = 1/2, the “Majority protocol” [3, 4] has deviation of \(\frac{1}{\sqrt{n}}\) by [4]

Our Result. For X0 = 1/2, our optimum protocol’s outcome deviates by at most \(\frac{1}{\sqrt{n}}\). In general, for any X0 ∈ [0, 1], outcome deviates by \(\frac{1}{\sqrt{n}} X_0(1 − X_0)\)

Black-box Separation Results

Previous Result. Unlikely that \(\frac{1}{\sqrt{n}}\) fair computation of the 1/2-coins exists, for c < \(\frac{1}{\sqrt{n}}\) relying solely on the black-box use of one-way functions [7, 8, 6]

Our Result. For any X0 ∈ [0, 1], unlikely that \(\frac{1}{\sqrt{n}} X_0(1 − X_0)\) fair computation of the X0-coins exists, for c < \(\frac{1}{\sqrt{n}}\) relying solely on the black-box use of one-way functions

References