Response to Epsen's “Games with zero-knowledge signaling”

Ryan Muldoon
Department of Philosophy
University of Pennsylvania

Outline

- Cryptography and Steganography
- Repeated Games of Incomplete Information
- Applications of these new games
- Some limitations
- Potential future directions

Cryptography and Steganography

- Cryptography and Steganography study the strategic hiding and revealing of information
- Cryptography obscures the message, while Steganography hides that there even is a message
- Senders want content of messages to be revealed only to those that they choose

Zero-knowledge proofs

- 3 conditions: Soundness, Completeness, Zero-Knowledge
- Soundness: If the statement is false, a cheating prover can't convince a verifier that it is true
- Completeness: If the statement is true, a verifier will be convinced
- Zero-knowledge: A cheating verifier can't learn any information beyond that the message is true
- Cave example

Connections to Game Theory

- Zero-knowledge proofs are interactive proof systems, so designed for multiple parties
- Both cryptography and steganography trade in strategic information revelation
- Repeated games where there is the possibility of private information have a need for methods of revealing it or demonstrating possession
- In games in which players have types or statuses, and strategies are dependent on the status of the other player, a way of reliably conveying the information would be valuable

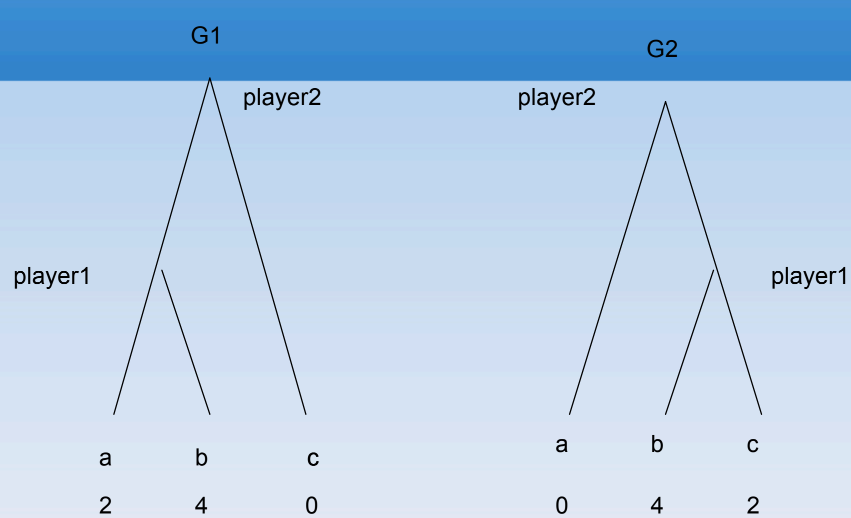
Repeated games of incomplete information

- AMS studied games with secret information
- The analysis was meant to provide an understanding of how and when such information should be revealed so as to be maximally beneficial to the knowledgeable player
- AMS noted that most strategic interactions are ongoing, not just one-shot
- In these 2-player, positive sum games, players may not know their own or the other player's payoffs

Epsen's contribution

- Rather than looking at revelation of information, Epsen looks at games in which *possession of information is revealed*
- *So the existence of secret information is no longer secret, but it remains concealed*
- *Class of games: repeated games where player 1 is either informed or uninformed, player 2 is uninformed of the actual game, but has a belief of how likely it is that player 1 knows the game. Perfect information about what the terminal node of the game was.*
- *Using the history of the terminal nodes allows us to construct a zero-knowledge proof of player 1's status*

Example game



Applications of these games

- Hobbes' Foole: can leverage private knowledge of which game is being played to take advantage of other agents
- Markets
  - Efficient Market Hypothesis leads to No-Trade Theorem
  - Introduction of “noise traders”
  - Rational traders hide themselves as noise traders to avoid No-Trade conclusion

First (minor) difficulty

- Conceptual question: In our example game, was there an intentional proof?
  - The Prover isn't trying to prove anything, just wants to keep Verifier in the dark about the game payoffs
  - Within this class of games, behavior seems to be driven purely by Prover's interest in keeping Verifier ignorant
  - Verifier's proof of Prover's status doesn't affect Verifier's gameplay

Other small difficulty

- In conclusion, Epsen notes that extensions to social networks might offer cases where players can only learn of a player's status by playing with them
- This isn't the case for most network arrangements, as long as we keep the assumption of perfect information of histories
- This can be confounded if the distribution of informed players is not random, or if there is not perfect information of histories

Main contribution

- The particular result that Epsen has is not the most important part of his work – it is the conceptual move of drawing from the extensive literature in cryptography and trying to generate cryptographic results within the confines of a game, not relying on external features (like winking in a poker game)

Extensions

- Zero-knowledge proofs were designed for authentication systems. Any games in which collective action is in everyone's interest but is risky to undertake should benefit from means of authentication
- However, a more fruitful approach might be to follow Ahn, Hopper and Langford 2006 and leverage covert two-party computation.
- covert two-party computation allows both parties to collaborate iff they are both willing, but neither party is aware of the attempt at computation unless it is successful
- Minimally, many communication protocols can be hidden in moves of a game