Pretty Good Strategies To Cast Your Vote Securely

Wojtek Jamroga

University of Luxembourg & Polish Academy of Sciences

Knowledge Representation and Multiagent Systems Conventicle
UNSW Sydney, 13th of May 2024

Research supported by: Fonds National de la Recherche Luxembourg NCBR National Centre for Research and Development

Outline

Secure Voting

Secure Voting

- **Secure voting procedures** should satisfy a number of requirements
- Ballot secrecy, vote anonymity, coercion-resistance, ...

Secure Voting

- **Secure voting procedures** should satisfy a number of requirements
- Ballot secrecy, vote anonymity, coercion-resistance, ...
- In particular, the voter should get no receipt to show the coercer how she voted (receipt-freeness)

Secure E-Voting

When the vote is cast electronically:

- Ballot secrecy and vote anonymity require that the vote is encrypted before it is sent

Secure E-Voting

When the vote is cast electronically:

- Ballot secrecy and vote anonymity require that the vote is encrypted before it is sent
- Receipt-freeness implies that the voter does not get the unencrypted vote

Secure E-Voting

When the vote is cast electronically:

- Ballot secrecy and vote anonymity require that the vote is encrypted before it is sent
- Receipt-freeness implies that the voter does not get the unencrypted vote
- How can the voter make sure that the encryption is correct?

Secure E-Voting

When the vote is cast electronically:

- Ballot secrecy and vote anonymity require that the vote is encrypted before it is sent
- Receipt-freeness implies that the voter does not get the unencrypted vote
- How can the voter make sure that the encryption is correct?
  $\rightsquigarrow$ **Benaloh challenge**

Benaloh Challenge

Procedure:

1. The voter chooses a value of the vote (e.g., a candidate)
2. The device commits to an encryption
3. The voter decides whether to cast the vote (without opening) or audit the encryption and spoil the vote
4. Repeat any number of times until the vote is cast

Benaloh Challenge

Intuition:

A corrupt machine might be eventually caught red-handed.

Benaloh Challenge

Intuition:

A corrupt machine might be eventually caught red-handed.

In the long run, it doesn't pay off for the perpetrator to rig the encryption device.

Benaloh Challenge

Intuition:

A corrupt machine might be eventually caught red-handed.

In the long run, it doesn't pay off for the perpetrator to rig the encryption device.

This is a **game-theoretic argument**!

Outline

Game-Theoretic Analysis of Benaloh Challenge

- **[Culnane & Teague 2016]**: very nice analysis, BC as an inspection game

Game-Theoretic Analysis of Benaloh Challenge

- **[Culnane & Teague 2016]**: very nice analysis, BC as an inspection game
- Two players: the voter vs. the corrupt device serving the interests of the perpetrator
- The voter chooses $n_{cast} \in \{1, \ldots, n_{max}\}$
- The device selects $n_{cheat} \in \{1, \ldots, n_{max} + 1\}$

Game-Theoretic Analysis of Benaloh Challenge

Payoff table:

	Voter payoff $u_V(n_{cast}, n_{cheat})$	Device payoff $u_D(n_{cast}, n_{cheat})$	Comment
$n_{cast} < n_{cheat}$	$-(n_{cast} - 1)c_{audit} + Succ_V$	0	Voter votes as intended
$n_{cast} = n_{cheat}$	$-(n_{cast} - 1)c_{audit} - Fail_V$	$Succ_D$	Device successfully cheats
$n_{cast} > n_{cheat}$	$-n_{cheat} \cdot c_{audit}$	$-Fail_D$	Voter catches cheating device

Game-Theoretic Analysis of Benaloh Challenge

Claims (CC & VT 2016):

1. In deterministic Nash equilibrium strategies, the voter casts right away, and the device immediately cheats. Thus, only randomized strategies of the voter make sense

Game-Theoretic Analysis of Benaloh Challenge

Claims (CC & VT 2016):

1. In deterministic Nash equilibrium strategies, the voter casts right away, and the device immediately cheats. Thus, only randomized strategies of the voter make sense
2. The same happens for randomized strategies with a bounded number of steps. Thus, only infinite audit strategies make sense

Game-Theoretic Analysis of Benaloh Challenge

Claims (CC & VT 2016):

1. In deterministic Nash equilibrium strategies, the voter casts right away, and the device immediately cheats. Thus, only randomized strategies of the voter make sense
2. The same happens for randomized strategies with a bounded number of steps. Thus, only infinite audit strategies make sense
3. In an infinite Benaloh game, there is no natural Nash equilibrium strategy for the voter

Game-Theoretic Analysis of Benaloh Challenge

Claims (CC & VT 2016):

1. In deterministic Nash equilibrium strategies, the voter casts right away, and the device immediately cheats. Thus, only randomized strategies of the voter make sense
2. The same happens for randomized strategies with a bounded number of steps. Thus, only infinite audit strategies make sense
3. In an infinite Benaloh game, there is no natural Nash equilibrium strategy for the voter

Thus, the voter has no natural rational strategies in Benaloh challenge.

Game-Theoretic Analysis of Benaloh Challenge

Claims (CC & VT 2016):

1. In deterministic Nash equilibrium strategies, the voter casts right away, and the device immediately cheats. Thus, only randomized strategies of the voter make sense (correct)
2. The same happens for randomized strategies with a bounded number of steps. Thus, only infinite audit strategies make sense
3. In an infinite Benaloh game, there is no natural Nash equilibrium strategy for the voter (correct)

Thus, the voter has no natural rational strategies in Benaloh challenge.

Game-Theoretic Analysis of Benaloh Challenge

Claims (CC & VT 2016):

1. In deterministic Nash equilibrium strategies, the voter casts right away, and the device immediately cheats. Thus, only randomized strategies of the voter make sense (correct)
2. The same happens for randomized strategies with a bounded number of steps. Thus, only infinite audit strategies make sense (......?)
3. In an infinite Benaloh game, there is no natural Nash equilibrium strategy for the voter (correct)

Thus, the voter has no natural rational strategies in Benaloh challenge.

Game-Theoretic Analysis of Benaloh Challenge

Claims (CC & VT 2016):

1. In deterministic Nash equilibrium strategies, the voter casts right away, and the device immediately cheats. Thus, only randomized strategies of the voter make sense (correct)
2. The same happens for randomized strategies with a bounded number of steps. Thus, only infinite audit strategies make sense (......?)
3. In an infinite Benaloh game, there is no natural Nash equilibrium strategy for the voter (correct)

Thus, the voter has no natural rational strategies in Benaloh challenge.

?

Game-Theoretic Analysis of Benaloh Challenge

Claims (CC & VT 2016):

1. In deterministic **Nash equilibrium** strategies, the voter casts right away, and the device immediately cheats. Thus, only randomized strategies of the voter make sense (correct)
2. The same happens for randomized strategies with a bounded number of steps. Thus, only infinite audit strategies make sense (......?)
3. In an infinite Benaloh game, there is no natural Nash equilibrium strategy for the voter (correct)

Thus, the voter has no natural rational strategies in Benaloh challenge.

?

Outline

Backward Induction

Claim (CC & VT 2016):

In a finite Benaloh game, backward induction produces the following strategy profile:

1. The voter casts her vote immediately
2. The device always cheats right away.

Thus, the voter always gets cheated.

Backward Induction

Claim (CC & VT 2016):

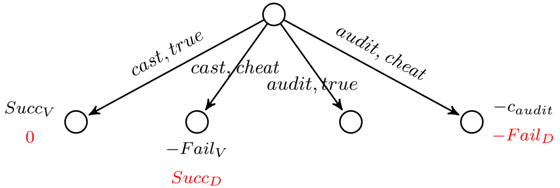
In a finite Benaloh game, backward induction produces the following strategy profile:

1. The voter casts her vote immediately
2. The device always cheats right away.

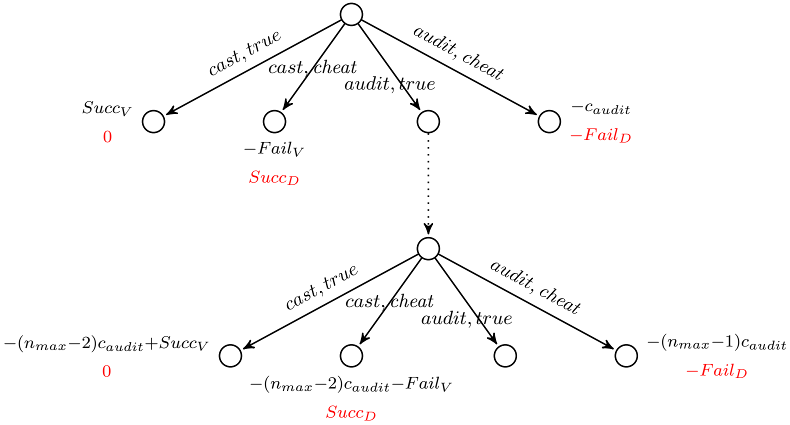
Thus, the voter always gets cheated.

However, to see how backward induction works, we first need to switch to an extensive form game.

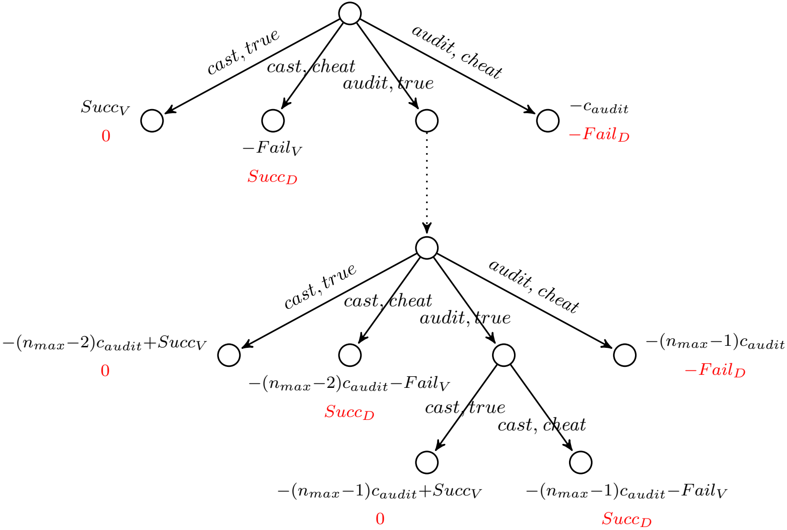
Game Tree for Benaloh Challenge



Game Tree for Benaloh Challenge



Game Tree for Benaloh Challenge

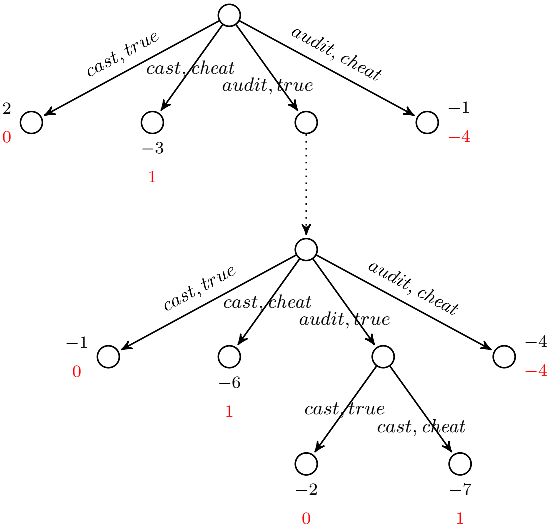


For the Sake of Presentation...

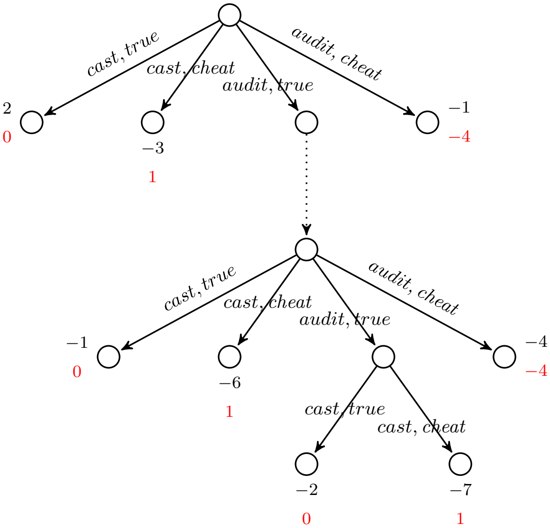
Let's fix example values of the parameters:

- $n_{max} = 5$ (at most 4 audits before casting)
- $Succ_D = 1$ and $Fail_D = 4$ (the perpetrator fears failure 4 times more than he values success)
- $Succ_V = 2$ and $Fail_V = 3$ (the voter loses slightly more by getting cheated than she gains by casting successfully)
- $c_{audit} = 1$ (the cost of audit is half of the gain from a successful vote)

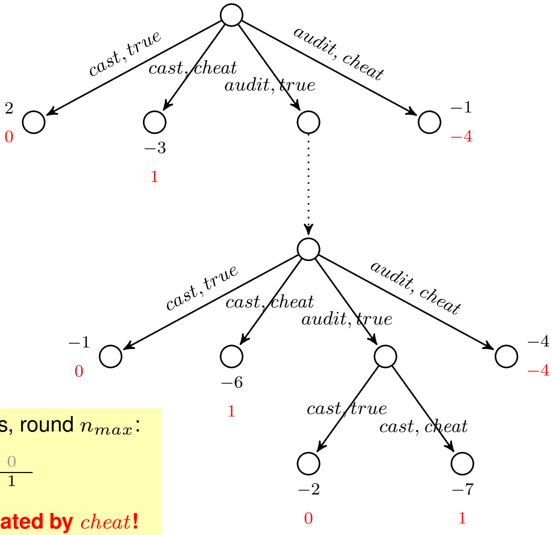
Game Tree for Benaloh Challenge (Example)



Backward Induction in Benaloh Challenge



Backward Induction in Benaloh Challenge

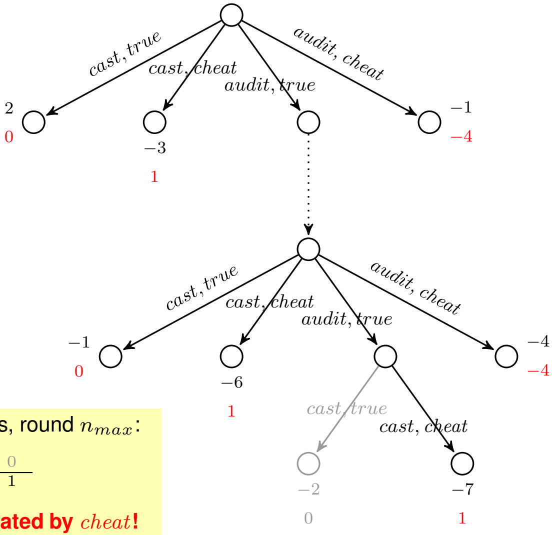


Device choices, round n_{max}:

$true$	0
$cheat$	1

$true$ **is dominated by** $cheat$**!**

Backward Induction in Benaloh Challenge

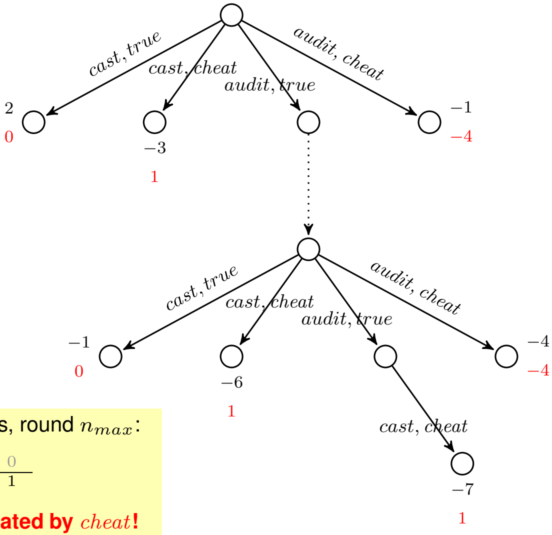


Device choices, round n_{max}:

$true$	0
$cheat$	1

$true$ **is dominated by** $cheat$**!**

Backward Induction in Benaloh Challenge

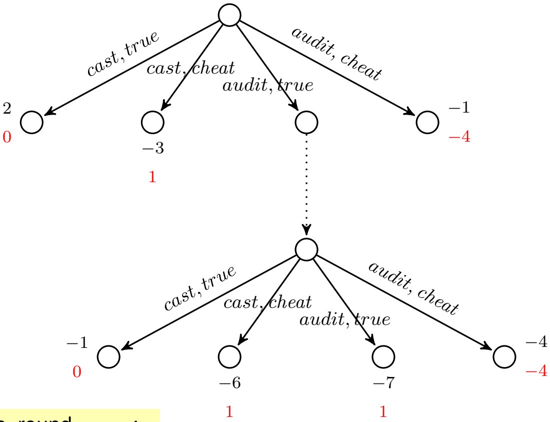


Device choices, round n_{max}:

$true$	0
$cheat$	1

$true$ is dominated by $cheat$!

Backward Induction in Benaloh Challenge

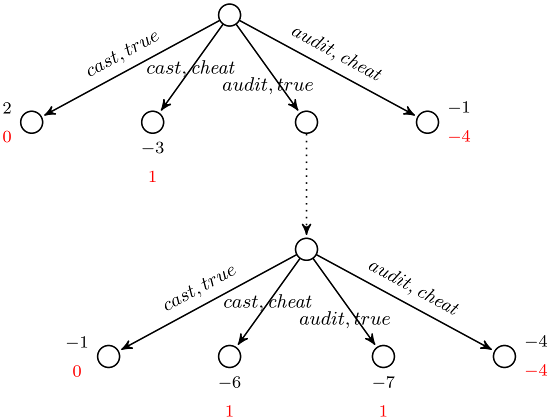


Device choices, round n_{max}:

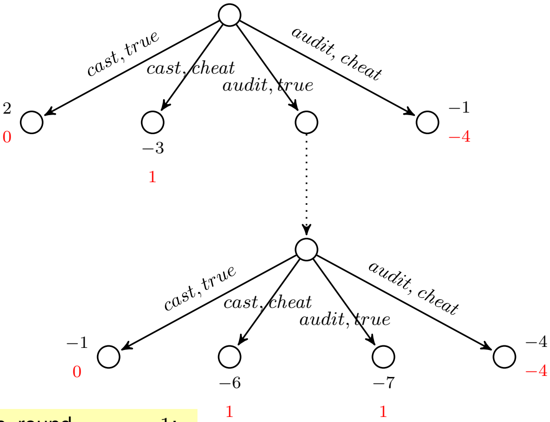
$true$	0
$cheat$	1

$true$ **is dominated by** $cheat$**!**

Backward Induction in Benaloh Challenge



Backward Induction in Benaloh Challenge

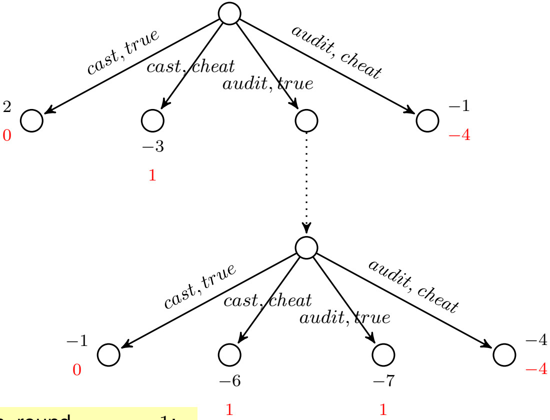


Device choices, round $n_{max} - 1$:

$true$	0	1
$cheat$	1	-4

None dominates the other one!

Backward Induction in Benaloh Challenge

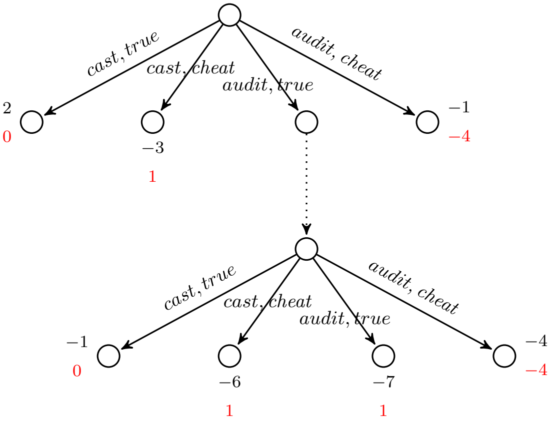


Voter's choices, round $n_{max} - 1$:

cast	-1	-6
audit	-7	-4

None dominates the other one!

Backward Induction in Benaloh Challenge



Backward induction stops here!

Thus, looking at finite audit strategies might make sense!

Nash Equilibria in Finite Randomized Strategies

Theorem (Nash equilibrium in finite Benaloh games)

The mixed voting strategy $s_V = [p_1^V, \cdots, p_{n_{max}}^V]$ is a part of Nash equilibrium iff, for every $n \in \{1, \dots, n_{max}\}$:

$$\mathbf{p_n^V} = \frac{\mathbf{(1-R)R^{n-1}}}{\mathbf{1-R^{n_{max}}}}, \qquad \text{where } R = \frac{Succ_D}{Succ_D + Fail_D}.$$

Alternatively: the behavioral voting strategy $b_V = [b_1^V, \cdots, b_{n_{max}}^V]$ is a part of Nash equilibrium iff, for every $n \in \{1, \dots, n_{max}\}$:

$$\mathbf{b_n^V} = \frac{\mathbf{1-R}}{\mathbf{1-R^{n_{max}-n+1}}}, \qquad \text{where } R = \frac{Succ_D}{Succ_D + Fail_D}.$$

Nash Equilibria in Finite Randomized Strategies

In our example, the behavioral NE strategy is

$$b_V = [0.8, 0.801, 0.81, 0.83, 1].$$

That is, the voter:

1. casts immediately with probability 0.8,
2. else audits, again, and casts with probability 0.801,
3. else audits, randomizes again, and casts with probability 0.81,
4. else audits, randomizes again, and casts with probability 0.83,
5. else audits, and finally casts with probability 1.

Nash Equilibria in Finite Randomized Strategies

In our example, the behavioral NE strategy is

$$b_V = [0.8, 0.801, 0.81, 0.83, 1].$$

That is, the voter:

1. casts immediately with probability 0.8,
2. else audits, again, and casts with probability 0.801,
3. else audits, randomizes again, and casts with probability 0.81,
4. else audits, randomizes again, and casts with probability 0.83,
5. else audits, and finally casts with probability 1.

That doesn't seem easy to execute...
Can we make the voter's life easier?

Making Things Easy for the Voter

Let's make things simple and very, very finite: $n_{max} = 2$

$\rightsquigarrow$ The voter is allowed to audit at most once!

Making Things Easy for the Voter

Let's make things simple and very, very finite: $n_{max} = 2$

$\rightsquigarrow$ The voter is allowed to audit at most once!

Then, the unique NE strategy for the voter is:

1. Cast immediately with probability $p = \frac{Succ_D + Fail_D}{2Succ_D + Fail_D}$,
2. Otherwise audit first and cast in the second round.

Making Things Easy for the Voter

Let's make things simple and very, very finite: $n_{max} = 2$

$\rightsquigarrow$ The voter is allowed to audit at most once!

Then, the unique NE strategy for the voter is:

1. Cast immediately with probability $p = \frac{Succ_D + Fail_D}{2Succ_D + Fail_D}$,
2. Otherwise audit first and cast in the second round.

In our example: cast immediately with probability $\frac{5}{6}$, otherwise audit first and cast in the second round.

Towards Simple and Natural Audit Strategies

Moreover, we can often assume that $Fail_D \gg Succ_D$.
Then, p is close 1.

The voter should almost always cast immediately!

Towards Simple and Natural Audit Strategies

Moreover, we can often assume that $Fail_D \gg Succ_D$.
Then, p is close 1.

The voter should **almost** always cast immediately!

Towards Simple and Natural Audit Strategies

Moreover, we can often assume that $Fail_D \gg Succ_D$.
Then, p is close 1.

The voter should **almost** always cast immediately!

Looks like a simple strategy

Audit Strategies Can Be Simple, But Are They Good Enough?

NE audit strategies for $n_{max} = 2$ are reasonably simple, but what are the players' payoffs?

Audit Strategies Can Be Simple, But Are They Good Enough?

NE audit strategies for $n_{max} = 2$ are reasonably simple, but what are the players' payoffs?

In our example:

$$u_V(s_V, s_D) = -\frac{7}{6} \qquad\qquad u_D(s_V, s_D) = \frac{1}{6}\ .$$

Audit Strategies Can Be Simple, But Are They Good Enough?

NE audit strategies for $n_{max} = 2$ are reasonably simple, but what are the players' payoffs?

In our example:

$$\mathbf{u_V(s_V, s_D) = -\frac{7}{6}} \qquad\qquad u_D(s_V, s_D) = \frac{1}{6}\ .$$

Audit Strategies Can Be Simple, But Are They Good Enough?

NE audit strategies for $n_{max} = 2$ are reasonably simple, but what are the players' payoffs?

In our example:

$$\mathbf{u_V(s_V, s_D) = -\frac{7}{6}} \qquad\qquad u_D(s_V, s_D) = \frac{1}{6}\,.$$

The voter's payoff is negative!

Thus, a considerate election authority should **ban Benaloh challenge** for the good of the voter

Audit Strategies Can Be Simple, But Are They Good Enough?

NE audit strategies for $n_{max} = 2$ are reasonably simple, but what are the players' payoffs?

In our example:

$$\mathbf{u_V(s_V, s_D) = -\frac{7}{6}} \qquad u_D(s_V, s_D) = \frac{1}{6}\ .$$

The voter's payoff is negative!

Thus, a considerate election authority should **ban Benaloh challenge** for the good of the voter

Well, should it really...?

Outline

Are Benaloh and Nash a Good Match?

- The voter does have simple and intuitive NE strategies in Benaloh challenge after all...
- ...however, they don't seem to benefit him/her

Are Benaloh and Nash a Good Match?

- The voter does have simple and intuitive NE strategies in Benaloh challenge after all...
- ...however, they don't seem to benefit him/her

Big question:

Is Nash equilibrium the **right solution concept** to capture the players' deliberation in Benaloh games?

Are Benaloh and Nash a Good Match?

- Nash equilibrium captures the outcome of mutual long-run adaptation of players to each others' strategies
- Inherently symmetric!

Are Benaloh and Nash a Good Match?

- Nash equilibrium captures the outcome of mutual long-run adaptation of players to each others' strategies
- Inherently symmetric!
- [Culnane & Teague 2016]: the device can use ML techniques to profile the voter and learn his/her strategy
  $\rightsquigarrow$ information asymmetry in favor of the device

Are Benaloh and Nash a Good Match?

- Nash equilibrium captures the outcome of mutual long-run adaptation of players to each others' strategies
- Inherently symmetric!
- [Culnane & Teague 2016]: the device can use ML techniques to profile the voter and learn his/her strategy
  $\rightsquigarrow$ information asymmetry in favor of the device
- GT fact: this kind of asymmetry can be exploited by the voter
  $\rightsquigarrow$ **Stackelberg equilibrium**

Nash vs. Stackelberg

- Stackelberg equilibrium captures the outcome in games where one player (the *leader*) exposes her strategy first, and the other players play their best response

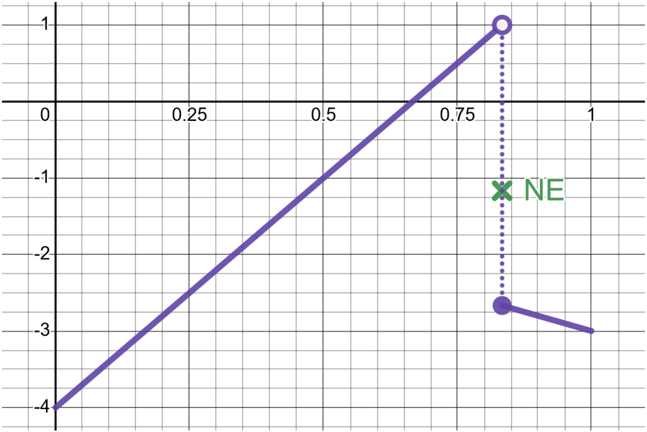
Nash vs. Stackelberg

- Stackelberg equilibrium captures the outcome in games where one player (the *leader*) exposes her strategy first, and the other players play their best response
- Applicability of Stackelberg: the leader must be able to
  1. either complete her strategy before the other players start,
  2. or believably commit to her strategy in advance,
  3. or make her strategy known beforehand in some other way.

Nash vs. Stackelberg

- Stackelberg equilibrium captures the outcome in games where one player (the *leader*) exposes her strategy first, and the other players play their best response
- Applicability of Stackelberg: the leader must be able to
  1. either complete her strategy before the other players start,
  2. or believably commit to her strategy in advance,
  3. or make her strategy known beforehand in some other way.
- GT fact: Stackelberg equilibrium often obtains a better payoff for the leader than Nash equilibrium

Pretty Good Strategies against Best Response



Pretty Good Strategies against Best Response

Theorem (Stackelberg equilibrium in simple Benaloh games)

The following properties hold for the Benaloh game with $n_{max} = 2$:

1. There is no Stackelberg equilibrium for V in randomized strategies.
2. The Stackelberg value of the game is $SVal_V = \frac{Succ_D(Succ_V - Fail_V - c_{audit}) + Fail_D Succ_V}{2Succ_D + Fail_D}$.
3. $SVal_V > Eu_V(p^V_{NE}, p^D_{NE})$, where (p^V_{NE}, p^D_{NE}) is the Nash equilibrium.
4. If $Fail_D \gg Succ_D$ and $Succ_V \geq aFail_V$ for a fixed $a > 0$, then $SVal_V > 0$.

Pretty Good Strategies against Best Response

In plain words...

In the simple Benaloh game:

1. Stackelberg equilibrium in randomized strategies does not exist.
2. However, the Stackelberg optimum can be approximated by the voter arbitrarily close, promising **payoff** that is **positive** and **strictly higher than NE**.

Outline

Takeaway Advice

1. Using Benaloh challenge can be practical and beneficial to the rational voter

Takeaway Advice

1. Using Benaloh challenge can be practical and beneficial to the rational voter
2. Putting a limit on the number of allowed audits makes things easier for the voter.

   Considerate election authority might design the voting system so that each voter can audit the vote encryption at most once.

Takeaway Advice

1. Using Benaloh challenge can be practical and beneficial to the rational voter
2. Putting a limit on the number of allowed audits makes things easier for the voter.

   Considerate election authority might design the voting system so that each voter can audit the vote encryption at most once.
3. The voters should not try to adapt to the strategy of the attacker, the way Nash equilibrium prescribes.

   Instead, they should stick to **auditing the votes with a fixed low frequency**, thus approximating the Stackelberg optimum and putting the attacker on the defensive

Takeaway Advice

And...

Using game theory is tricky

$\rightsquigarrow$ easy to do your models wrong!

Takeaway Advice

And...

Using game theory is tricky

$\rightsquigarrow$ easy to do your models and metamodels wrong!


Questions?