Are Some Voters More Equal Than Others?

Discussions and work in progress on formalisation

Hugo Jonker

in collaboration with Ben Smyth

Elections

Elections:

a way to establish the preference of a group,
based on the preferences of the individual members.

Elections

Elections:

a way to establish the preference of a group,
based on the preferences of the individual members.

1. Collect individual preferences.

Elections

Elections:

a way to establish the preference of a group,
based on the preferences of the individual members.

1. Collect individual preferences.
2. Derive group preference.

Elections

Elections:

a way to establish the preference of a group,
based on the preferences of the individual members.

1. **Collect individual preferences**.
2. Derive group preference.

Are all voters equal?

- Who votes first?
- Who votes last?

Shouldn’t matter, but:

Are all voters equal?

- Who votes first?
- Who votes last?

Shouldn’t matter, but:

- Last voter knows 2 major parties are precisely tied.
  $\Longrightarrow$ last voter can determine winner.
- Eurovision song festival voting: why vote for a losing party?

Are all voters equal?

- Who votes first?
- Who votes last?

Shouldn’t matter, but:

- Last voter knows 2 major parties are precisely tied.
  $\Longrightarrow$ last voter can determine winner.
- Eurovision song festival voting: why vote for a losing party?

Elections should be **fair**.

Intuition

Fairness $=$ each participant has equal “opportunity”.

In other fields:

Intuition

Fairness = each participant has equal “opportunity”.

In other fields:

- **computation:**
  every path must occur in an infinite computation.
- **contract signing:**
  Either all or none of the parties receive a signed document.
- **two-party exchange:**
  Either both items change owner, or neither does.

Fairness in voting

- A voting system doesn't confer any advantage upon any voter.

Fairness in voting

- A voting system doesn't confer any advantage upon any voter.
- A voting system doesn't allow any voter an advantage.

Fairness in voting

- A voting system doesn't confer any advantage upon any voter.

- A voting system doesn't allow any voter an advantage.
- No pulling out (cf. [FOO92]).

Fairness in voting

- A voting system doesn't confer any advantage upon any voter.
- A voting system doesn't allow any voter an advantage.
- No pulling out (cf. [FOO92]).
- All voters have "similar" information about how their vote affects the result.

Fairness in voting

- A voting system doesn't confer any advantage upon any voter.
- A voting system doesn't allow any voter an advantage.
- No pulling out (cf. [FOO92]).
- All voters have "similar" information about how their vote affects the result.
- All voters know in advance how to obtain the advantage.

Fairness in voting

- A voting system doesn't confer any advantage upon any voter.

- A voting system doesn't allow any voter an advantage.
- No pulling out (cf. [FOO92]).

- All voters have "similar" information about how their vote affects the result.
- All voters know in advance how to obtain the advantage.

Each voter has specific, partial control over the result.
Fairness is broken when a voter can exercise control beyond this.

Control: "+1"? can vary per voter?

Examples for discussion

Discussion: ballot independence

Situation 1 (*copy ballot*):

Submit a copy of another voter's filled in ballot.

- You can vote the same as someone.
- Privacy problem? fairness problem?

Discussion: ballot independence

Situation 1 (*copy ballot*):

Submit a copy of another voter's filled in ballot.

- You can vote the same as someone.
- Privacy problem? fairness problem?

Situation 2 (*vote unlike someone*):

Submit a modified copy of another voter's filled in ballot.

- You can vote unlike someone.
- Privacy problem? Fairness problem?

Discussion: aborting a vote

Situation 3 (*change your mind*):

If voting occurs in > 1 *phase, don't participate in last phase.*

- You can cancel your vote.
- When is this a fairness problem?

Existing formalisations

KRS05: secrecy in ProVerif

[KR05]: to verify [FOO92].

- no one can learn vote v before opening phase.
  Standard ProVerif secrecy check of vote variable v.
- no one can guess v before opening phase. $\phi \approx_s \nu v.\phi$ – ProVerif check.

\+ automatic checking

\- copying/modifying ballot not caught

\- contents of vote $\stackrel{?}{\Longrightarrow}$ no early results

BRS07: no early results

[BRS07]: to verify [FOO92].

$$\neg\text{resultAnnounced} \implies \bigwedge_{a \in Ag} L_a(\bigwedge_{b \neq a, c \in \mathcal{C}} vote_b(c)).$$

Before results, no one can exclude any choice by any other voter.

+ knowledge based reasoning
+ straightforward definition
- how to apply
- fairness $>$ knowing no ballots

TMT08: votes in the open

[TMT$^+$08]: case study of [FOO92].

$$\nu X.\, \wedge_{c \in \mathcal{C}} (\langle x.(x_i - X_s \rhd X_r : v).y \looparrowright \varepsilon \rangle tt \rightarrow \langle x.d(T).y.(x_i - X_s \rhd X_r : v).z \looparrowright x.d(T).y.z \rangle X))$$

If a vote can be determined, then there must have been a phase boundary earlier in the protocol.

- “normalized” protocol
- non-intuitive language
- guessing attacks not caught
- ballot exposure $\neq$ fairness

BHM08: don't re-use the vote

[BHM08]: general def of "soundness", applied to [JCJ05].

Every eligible voter votes once.

- $t = t1 \cdot \text{start}(id) \cdot t2$.
- Eligibility: $\text{start}(id) \notin t1 \cdot t2$.
- One vote: $\text{newid}(id) \in t1$. (event by id manager).

\+ simple, straightforward def

\- limited to "soundness" / accuracy + democracy

Towards formalising fairness

Observation

If the result is unaffected, fairness is not harmed.

Initial idea

1. before voting, voter observes trace t;
2. t can be extrapolated to full run with and without voter;
3. For all such possible extrapolations: determine result;

Fairness: $\exists c\colon \forall t \in Tr(with)\colon \exists t' \in Tr(without)\colon c =$ result$(t) -$ result$(t') \wedge t \approx t'$.

Problems

- Constant = 1,2,3,. . .
- Difference between two results constant necessary? Sufficient?
- What if no one votes after voter? Or a variable number?

Idea stubs

Possible definitions of fairness:

a.i. Result occurs > 1 **before** casting, not possible **after**:
$\Longrightarrow$ fairness violated.

Idea stubs

Possible definitions of fairness:

a.i. Result occurs > 1 **before** casting, not possible **after**:
$\Longrightarrow$ fairness violated.

a.ii. Distribution of result changed by > 1 (vote) after casting:
$\Longrightarrow$ fairness violated.

Idea stubs

Possible definitions of fairness:

a.i. Result occurs > 1 **before** casting, not possible **after**:
$\Longrightarrow$ fairness violated.

a.ii. Distribution of result changed by > 1 (vote) after casting:
$\Longrightarrow$ fairness violated.

b.i. For every voter, the effect should be the same.

Idea stubs

Possible definitions of fairness:

a.i. Result occurs > 1 **before** casting, not possible **after**:
$\Longrightarrow$ fairness violated.

a.ii. Distribution of result changed by > 1 (vote) after casting:
$\Longrightarrow$ fairness violated.

b.i. For every voter, the effect should be the same.

b.ii. For every voter, the effect should be the same:
A change of 1 vote.

Idea stubs

Possible definitions of fairness:

a.i. Result occurs > 1 **before** casting, not possible **after**:
$\Longrightarrow$ fairness violated.

a.ii. Distribution of result changed by > 1 (vote) after casting:
$\Longrightarrow$ fairness violated.

b.i. For every voter, the effect should be the same.

b.ii. For every voter, the effect should be the same:
A change of 1 vote.

c. The voting system does not influence the vote.

Idea stubs

Possible definitions of fairness:

a.i. Result occurs > 1 **before** casting, not possible **after**:
$\Longrightarrow$ fairness violated.

a.ii. Distribution of result changed by > 1 (vote) after casting:
$\Longrightarrow$ fairness violated.

b.i. For every voter, the effect should be the same.

b.ii. For every voter, the effect should be the same:
A change of 1 vote.

c. The voting system does not influence the vote.

d. No pulling out (problem in FOO).

Conclusions

- Fairness is necessary for fair voting systems, ...
- ...and we can formally express something,...
- ... but do we know what fairness is?

Conclusions

- Fairness is necessary for fair voting systems, ...
- ...and we can formally express something,...
- ... but do we know what fairness is?

Thank you for your attention.

Questions/comments?

References

[BHM08] M. Backes, C. Hriţcu, and M. Maffei. Automated verification of remote electronic voting protocols in the applied pi-calculus. In Proc. 21st IEEE Computer Security Foundations Symposium, pages 195–209. IEEE Computer Society, 2008.

[BRS07] A. Baskar, R. Ramanujam, and S. P. Suresh. Knowledge-based modelling of voting protocols. In Proc. 11th Conference on Theoretical Aspects of Rationality and Knowledge, pages 62–71. ACM, 2007.

[FOO92] A. Fujioka, T. Okamoto, and K. Ohta. A practical secret voting scheme for large scale elections. In Advances in Cryptology – AUSCRYPT '92, volume 718 of LNCS, pages 244–251. Springer, 1992.

[JCJ05] A. Juels, D. Catalano, and M. Jakobsson. Coercion-resistant electronic elections. In Proc. 2005 ACM Workshop on Privacy in the Electronic Society, pages 61–70. ACM, 2005.

[KR05] S. Kremer and M. Ryan. Analysis of an electronic voting protocol in the applied pi calculus. In Proc. 14th European Symposium on Programming, volume 3444 of LNCS, pages 186–200. Springer, 2005.

[TMT+08] Mehdi Talbi, Benjamin Morin, Valérie Viet Triem Tong, Adel Bouhoula, and