Are Some Voters More Equal Than Others?

Discussions and work in progress on formalisation

Hugo Jonker

in collaboration with Ben Smyth
Elections:

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

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

1. Collect individual preferences.
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:

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.  
  \[ \implies \text{last voter can determine winner.} \]

- 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.  
  $\implies$ last voter can determine winner.

- Eurovision song festival voting: why vote for a losing party?

Elections should be **fair**.
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.
A voting system doesn’t confer any advantage upon any voter.
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
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
[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 \( \Rightarrow \) no early results
BRS07: no early results

[\text{BRS07}]: to verify [\text{FOO92}].

\[ \neg \text{resultAnnounced} \implies \bigwedge_{a \in Ag} L_a(\bigwedge_{b \neq a, c \in C} \text{vote}_b(c)). \]

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

+ knowledge based reasoning
+ straightforward definition
- how to apply
- fairness $\succ$ knowing no ballots
TMT08: votes in the open

\([\text{TMT}^+08]\): case study of \([\text{FOO}92]\).

\[\nu X. \land_{c \in C} (\langle x. (x_i - X_s \triangleright X_r : v).y \leftrightarrow \varepsilon \rangle tt \rightarrow \\
\langle x.d(T).y.(x_i - X_s \triangleright X_r : v).z \leftrightarrow x.d(T).y.z \rangle X)\]

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 ≠ 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
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:** $\exists c: \forall t \in Tr(with): \exists t' \in Tr(without): c = \text{result}(t) - \text{result}(t') \land t \approx t'$.
Problems

- Constant = 1, 2, 3, …
- Difference between two results constant necessary? Sufficient?
- What if no one votes after voter? Or a variable number?
Possible definitions of fairness:

a.i. Result occurs $> 1$ before casting, not possible after:
→ fairness violated.
Idea stubs

Possible definitions of fairness:

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

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

a.i. Result occurs \( \geq 1 \) before casting, not possible after:

\[ \implies \text{fairness violated.} \]

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

a.ii. Distribution of result changed by \( \geq 1 \) (vote) after casting:

\[ \implies \text{fairness violated.} \]
Possible definitions of fairness:

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

a.ii. Distribution of result changed by $> 1$ (vote) after casting: 
    $\implies$ 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.
Possible definitions of fairness:

a.i. Result occurs $\geq 1$ before casting, not possible after:
   $\Rightarrow$ fairness violated.

a.ii. Distribution of result changed by $> 1$ (vote) after casting:
   $\Rightarrow$ 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.
Possible definitions of fairness:

a.i. Result occurs \(\geq 1\) before casting, not possible after:
\[\implies\text{ fairness violated.}\]

a.ii. Distribution of result changed by \(\geq 1\) (vote) after casting:
\[\implies\text{ fairness violated.}\]

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


