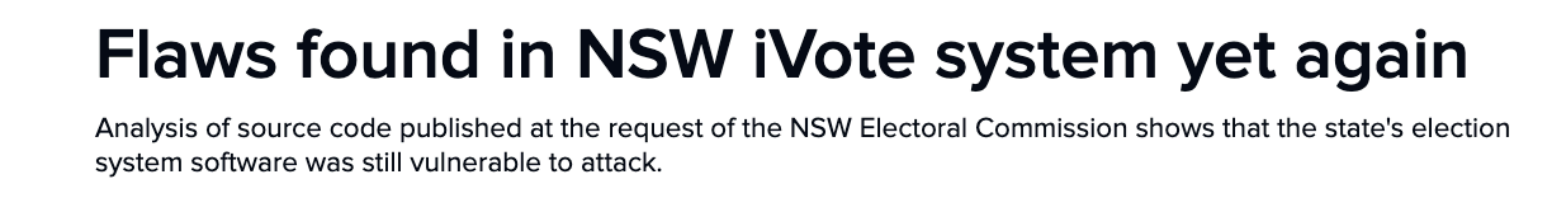
Formal Verification for Correct and Secure Software

Mukesh Tiwari,
University of Cambridge,
Cambridge

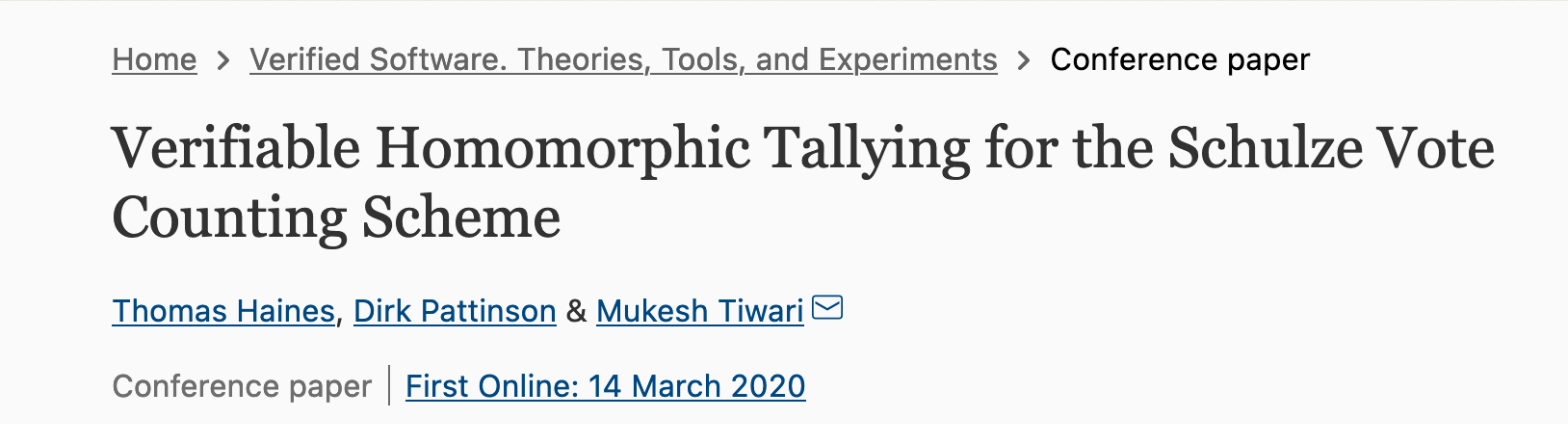
UNIVERSITY OF
CAMBRIDGE

Developing Correct Software is Hard



Flaws found in NSW iVote system yet again

Analysis of source code published at the request of the NSW Electoral Commission shows that the state's election system software was still vulnerable to attack.

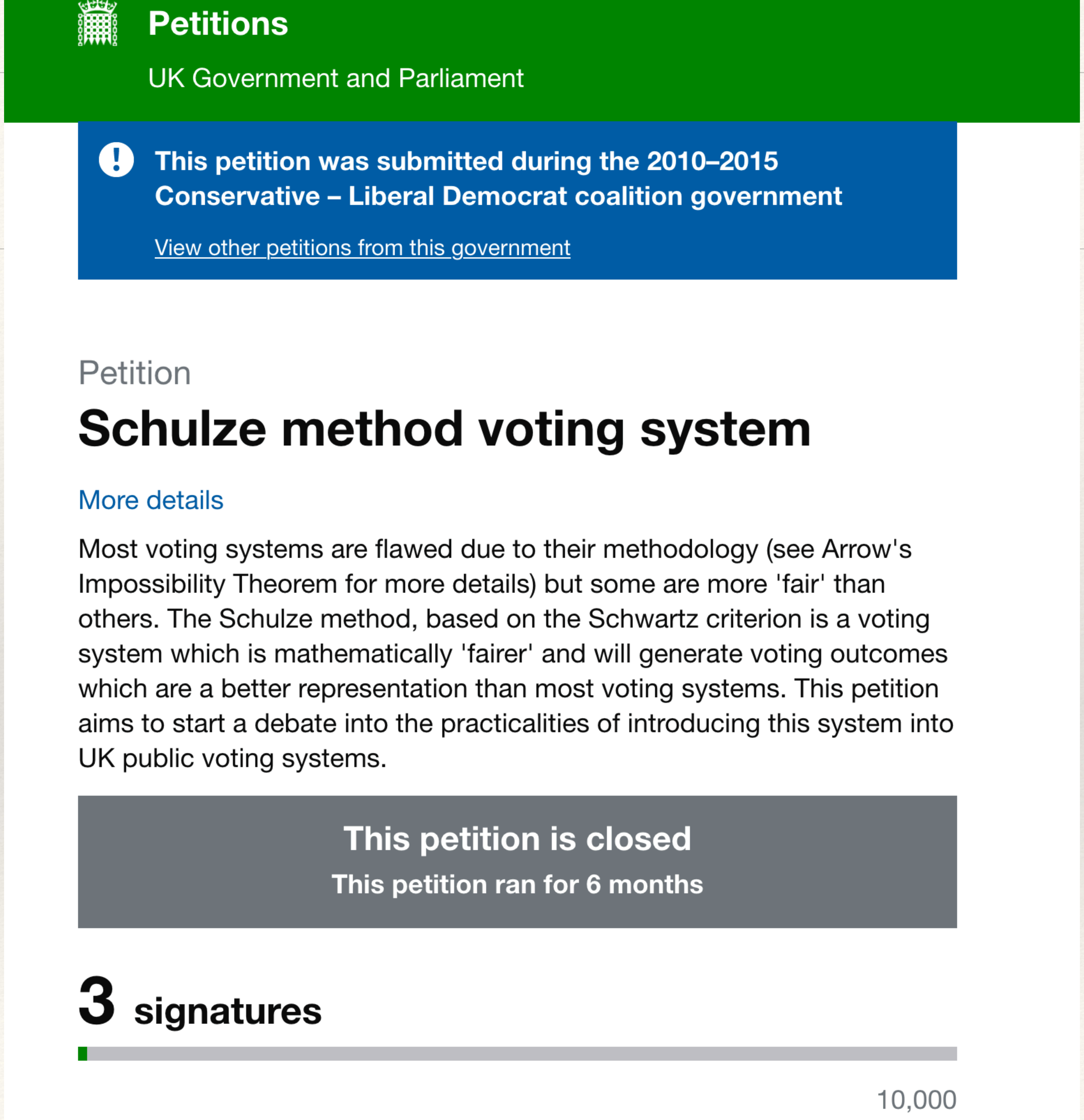


Home › Verified Software. Theories, Tools, and Experiments › Conference paper

Verifiable Homomorphic Tallying for the Schulze Vote Counting Scheme

Thomas Haines, Dirk Pattinson & Mukesh Tiwari

Conference paper | First Online: 14 March 2020



Petitions

UK Government and Parliament

This petition was submitted during the 2010–2015 Conservative – Liberal Democrat coalition government

View other petitions from this government

Petition

Schulze method voting system

More details

Most voting systems are flawed due to their methodology (see Arrow's Impossibility Theorem for more details) but some are more 'fair' than others. The Schulze method, based on the Schwartz criterion is a voting system which is mathematically 'fairer' and will generate voting outcomes which are a better representation than most voting systems. This petition aims to start a debate into the practicalities of introducing this system into UK public voting systems.

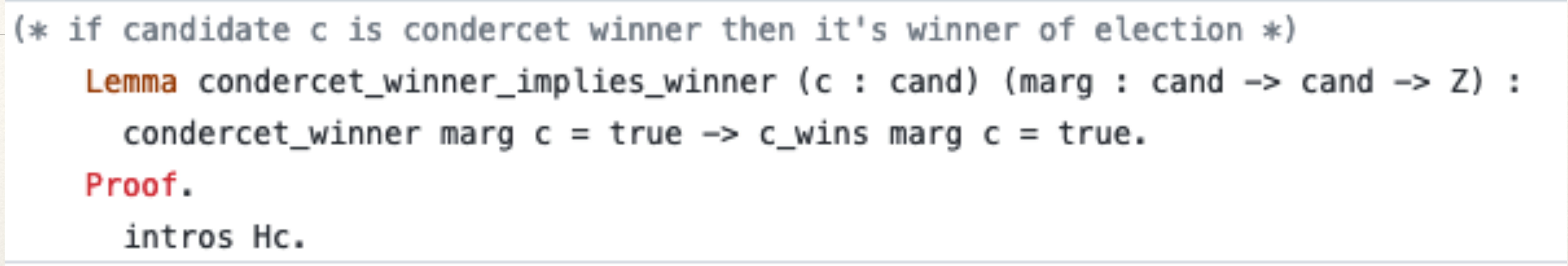
This petition is closed

This petition ran for 6 months

3 signatures

10,000

If there is a Condorcet winner, then Schulze method elects it



```
(* if candidate c is condercet winner then it's winner of election *)
  Lemma condercet_winner_implies_winner (c : cand) (marg : cand -> cand -> Z) :
    condercet_winner marg c = true -> c_wins marg c = true.
  Proof.
    intros Hc.
```

A	1
B	2
C	3

Ballot

A is the Condorcet Winner