Automated Verification for Functional and Relational Properties of Voting Rules [COMSOC 2016]

Bernhard Beckert, Thorsten Borner, Michael Kirsten, Till Neuber, and Mattias Ulbrich

Motivation
- Voting rules often required (e.g., by constitution) to fulfil axiomatic properties
- Design of voting rules with desired properties non-trivial and error-prone
- Growing complexity with rise of electronic voting increases vulnerability
- Solution: Computer-aided verification for trustworthy voting rules

Relational Specification: Coupling Evaluations
- Technique for proving relational (inter-profile) properties, e.g., anonymity
- Relational properties consider two ballot profiles and election outcomes

Separate Evaluations

Coupling Evaluations

Example

\[ \max_{c_{SBP}} \sum_{i=1}^{n} R_{c_i} = \max_{c_{SBP}} \sum_{i=1}^{n} B_{c_i} \]

Example

\[ \text{result1} = \text{result2} \]

Often enables short and concise specifications (only differences)
- Critical point for making verification feasible!

Relational Verification: Examples

Verification using Bounded Model Checking (Tool: CBMC)
- Run-times for 9 candidates in seconds

Verification using Deductive Theorem Proving (Tool: KeY)
- Anonymity Prop.: Indifference to renaming and permutation of voters
- Plurality Rule: Single choice, candidate with plurality of votes is elected
- Concise specifications useable for BMC ⇒ Guidance for SAT-solver

Verifying Voting Rules
- Formalisation: Rules as imperative algorithms (C / Java), properties in FOL
- Established verification techniques: Key and CBMC
- Deductive Theorem Proving and Bounded Model Checking (BMC)

Functional Specication: Exploiting Symmetries
- Already established symmetry, target: functional (intra-profile) property
- Functional property considers elections individually, e.g., majority criterion
- Symmetry example: Anonymity, operation is ballot permutation

Symmetric profiles have minimal elements
- Symmetry properties infer symmetry-breaking predicates (SBPs)
- Reduces search space (to \( \% \)) using SBP as precondition
- Example for anonymity: Check only sorted (by candidate) profiles

Functional Verification: Example

Verification using Bounded Model Checking (Tool: CBMC)
- Run-times for 9 candidates in seconds

- Majority Criterion: If candidate \( \gamma \) has majority, \( \gamma \) must be elected
- Plurality Rule: Single choice, candidate with plurality of votes is elected

General Approach for Functional Verification
- Verification Task: Does voting rule \( V \) satisfy property \( P \)?
- Conjecture: \( V \) satisfies symmetry property 5.

General Approach
1. Verify \( S \) for \( V \) using relational techniques
2. Verify \( V \) satisfies property \( P \) only for subset \( \%, \%
3. Prove that \( \% \) spans all possible profiles (independent of \( \% \)
4. Prove that \( 5 \)-operations preserve property \( P \) (independent of \( \% \)

Conclusion
- General approach: Verification of functional axiomatic properties
- Feasibility demonstrated on multiple well-known results