Logic verification

What it is

- Formal characterization of software behavior within a carefully restricted scope
- Proof that this behavior conforms to specified assertions (i.e., votes are counted correctly)
- Complements [falsification] testing

Why it is

- TGDC Resolution #29-05, “Ensuring Correctness of Software Code”
- Higher level of assurance than functional testing alone
- Clarify objectives of source code review

Where it is

- Draft VVSG2 Sec. 4.2.3.2 / 4.2.3.3

How it works

- Vendor specifies pre- and post-conditions for each module
- Vendor proves assertions regarding tabulation correctness
- Testing authority reviews, checks the math, and issues findings
  - Pre- and post-conditions correctly characterize the software
  - The assertions are satisfied

Issues

- Training required
- Limited scope = limited assurance; unlimited scope = impracticable
- Overlaps with security reviews

Discussion