

Election Security with Risk Limiting Audits

Oliver Broadrick¹ Poorvi L. Vora¹ Filip Zagórski²³

¹Department of Computer Science, The George Washington University [odbroadrick@gmail.com]

²Wroclaw University of Science and Technology

³Votifica

Introduction

In this paper we present simulation results comparing the risk, stopping probability, and number of ballots required over multiple rounds of ballot polling risk-limiting audits (RLAs) MINERVA, Selection-Ordered (SO) BRAVO, and End-of-Round (EoR) BRAVO. BRAVO is the most commonly used ballot polling RLA and requires the smallest expected number of ballots when ballots are drawn one at a time and the (true) underlying election is as announced. In real audits, multiple ballots are drawn at a time, and BRAVO is implemented as SO BRAVO or EoR BRAVO. MINERVA is a recently proposed ballot polling RLA that requires fewer ballots than either implementation of BRAVO in a first round with stopping probability 0.9 but requires a predetermined round schedule. It is an open question how these audits compare over multiple rounds and for lower stopping probabilities. Our simulations use stopping probabilities of 0.9 and 0.25. The results are consistent with predictions of the R2B2 open-source library for ballot polling audits. We observe that both BRAVO audits are more conservative than MINERVA, which stops with fewer ballots, for both first round stopping probabilities. However, the advantage of using MINERVA decreases considerably for the smaller first round stopping probability, as one would expect.

Experiments

In this section, we motivate and describe the experiments. We consider a two candidate plurality contest, and assume that ballots are sampled with replacement, as is common in the literature. Note that sampling without replacement is more efficient for large sampling fractions, but MINERVA has not been extended for sampling without replacement. We first present relevant definitions.

Definition

An audit \mathcal{A} takes a sample of ballots X as input and gives as output either (1) *Correct*: the audit is complete, or (2) *Uncertain*: continue the audit.

All of the audits discussed in this paper are modeled as binary hypothesis tests. Under the alternative hypothesis, H_a , the announced outcome is correct. In particular, the true underlying ballot distribution is given by the announced ballot tallies. Under the null hypothesis, H_0 , a tie is the correct outcome^a. The maximum risk of an audit is the probability that an audit stops, given that the underlying election is a tie [?]. Note that an audit \mathcal{A} includes all audit parameters (maximum risk, round sizes, etc.).

Definition (Risk)

The maximum risk R of audit \mathcal{A} with sample $X \in \{0, 1\}^*$ drawn from the true underlying distribution of ballots is $R(\mathcal{A}) = \Pr[\mathcal{A}(X) = \textit{Correct} \mid H_0]$.

This leads us to the following definition of an α -RLA.

Definition (Risk Limiting Audit (α -RLA))

An audit \mathcal{A} is a Risk Limiting Audit with risk limit α iff $R(\mathcal{A}) \leq \alpha$.

We present measures of stopping probability in the j^{th} round of the audit, given that the underlying election is as announced.

Definition (Stopping Probability)

The stopping probability S_j of an audit \mathcal{A} in round j is

$$S_j(\mathcal{A}) = \Pr[\mathcal{A}(X) = \textit{Correct in round } j \wedge \mathcal{A}(X) \neq \textit{Correct previously} \mid H_a]$$

Experimentally, using our simulations, S_j would be estimated by the fraction of audits that stop in round j . Note that $\sum_j S_j(\mathcal{A}) = 1$. We can also consider the cumulative stopping probability:

Definition (Cumulative Stopping Probability)

The cumulative stopping probability C_j of an audit \mathcal{A} in round j is $C_j(\mathcal{A}) = \sum_{i=1}^j S_i$

Experimentally, using our simulations, C_j would be estimated by the fraction of audits that stop in or before round j .

A block

Vivamus congue volutpat elit nunc. Phasellus mauris, nunc suscipit erat. **Phasellus mauris**, nunc suscipit erat. finibus ante vel purus mollis feugiat. Nam mollis condimentum dolor. Nam mollis condimentum dolor. Vivamus felis vel

- Morbi mauris purus**, egestas. natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus.
- Cras vehicula blandit urna**. Curabitur cursus, metus nec metus mauris gravida turpis.
- Vestibulum et massa diam**. rhoncus lectus condimentum

Fu

Et rutrum ex euismod vel. Per ipsum pretium nibh, sit amet aliquam augue feugiat molestie. Sed morbi posuere.

Nam

Nulla eget sem quam. Ut aliquam facilisis hendrerit eu non urna. Etiam sit amet velit eget sem pharetra sed ipsum. Morbi congue quis. Maecenas sed porta est tincidunt non.

Etiam sit amet tempus lorem, ex eget, dictum orci. Etiam quam ligula. Mauris pretium molestie porta justo.

- Sed consequat** id ante vel elementum mollis augue iaculis. In sed est finibus, vulputate nunc porttitor quis. Fusce ornare dignissim nisi. Nam Donec rhoncus vestibulum erat.
- Sed luctus, elit sit amet** erat id turpis.
- Pellentesque facilisis dolor** vitae eleifend urna facilisis at

Nulla eget sem quam. Ut aliquam facilisis hendrerit eu non urna. Etiam sit amet velit eget sem pharetra sed ipsum. Morbi congue quis. Maecenas sed porta est tincidunt non.