Election Security with Risk-Limiting Audits

THE GEORGE WASHINGTON UNIVERSITY WASHINGTON, DC

Oliver Broadrick[1] Poorvi L. Vora[1] Filip Zagórski[23]

[1]Department of Computer Science, The George Washington University [odbroadrick@gmail.com] [2]Wroclaw University of Science and Technology [3]Votifica

THE GEORGE WASHINGTON UNIVERSITY WASHINGTON, DC

Abstract

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.

Introduction

Definition: Audit

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.

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 $R(\mathcal{A}) = \Pr[\mathcal{A}(X) = Correct \mid H_0]$.

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

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

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: The cumulative stopping probability C_j of an audit $\mathcal{A}$ in round j is $C_j(\mathcal{A}) = \sum_{i=1}^{j} S_j$ Experimentally, using our simulations, C_j would be estimated by the fraction of audits that stop in or before round j. Finally, we are also interested in the probability that an audit will stop in round j given that it did not stop earlier: The conditional stopping probability of an audit $\mathcal{A}$ in round j is

$$\chi_j(\mathcal{A}) = \Pr[\mathcal{A}(X) = Correct\ in\ round\ j \mid H_a \wedge \mathcal{A}(X) \neq Correct\ previo$$

Experimentally, using our simulations, χ_j would be estimated by the ratio of the audits that stop in round j to those that "entered" round j, i.e. those that did not stop before round j. We simulated audits for a risk limit of 10% (as in [?] and [?]) using margins from the 2020 US Presidential election, limiting ourselves to pairwise margins for the two main candidates of 0.05 or larger. Note that both Bravo and Minerva can be extended for multiple-candidate, multiple-winner plurality contests by performing pairwise tests between the winners and the losers [?, ?]. Therefore, the two candidate plurality contest is a general case, and these simulations provide insight for multiple-candidate and multiple-winner contests too. Round sizes increase

Stopping Probability

Finally, we are also interested in the probability that an audit will stop in round j given that it did not stop earlier: The conditional stopping probability of an audit $\mathcal{A}$ in round j is

$$\chi_j(\mathcal{A}) = \Pr[\mathcal{A}(X) = Correct\text{in round } j \mid H_a \wedge \mathcal{A}(X) \neq Correct\ previous$$

Experimentally, using our simulations, χ_j would be estimated by the ratio of the audits that stop in round j to those that "entered" round j, i.e. those that did not stop before round j.

Fusce aliquam magna velit

Et rutrum ex euismod vel. Pellentesque ultricies, velit in fermentum vestibulum, lectus nisi pretium nibh, sit amet aliquam lectus augue vel velit. Suspendisse rhoncus massa porttitor augue feugiat molestie. Sed molestie ut orci nec malesuada. Sed ultricies feugiat est fringilla posuere.

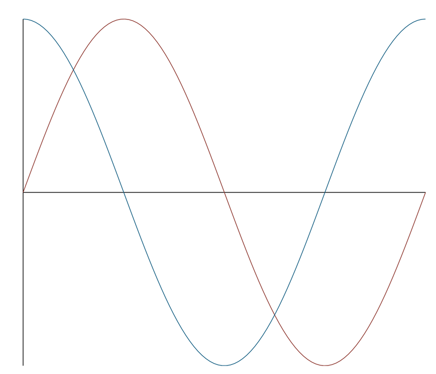

Figure 1. Another figure caption.

Nam cursus consequat egestas

Nulla eget sem quam. Ut aliquam volutpat nisi vestibulum convallis. Nunc a lectus et eros facilisis hendrerit eu non urna. Interdum et malesuada fames ac ante *ipsum primis* in faucibus. Etiam sit amet velit eget sem euismod tristique. Praesent enim erat, porta vel mattis sed, pharetra sed ipsum. Morbi commodo condimentum massa, *tempus venenatis* massa hendrerit quis. Maecenas sed porta est. Praesent mollis interdum lectus, sit amet sollicitudin risus tincidunt non.

Etiam sit amet tempus lorem, aliquet condimentum velit. Donec et nibh consequat, sagittis ex eget, dictum orci. Etiam quis semper ante. Ut eu mauris purus. Proin nec consectetur ligula. Mauris pretium molestie ullamcorper. Integer nisi neque, aliquet et odio non, sagittis porta justo.

- **Sed consequat** id ante vel efficitur. Praesent congue massa sed est scelerisque, elementum mollis augue iaculis.
  - In sed est finibus, vulputate nunc gravida, pulvinar lorem. In maximus nunc dolor, sed auctor eros porttitor quis.
  - Fusce ornare dignissim nisi. Nam sit amet risus vel lacus tempor tincidunt eu a arcu.
  - Donec rhoncus vestibulum erat, quis aliquam leo gravida egestas.
- **Sed luctus, elit sit amet** dictum maximus, diam dolor faucibus purus, sed lobortis justo erat id turpis.
- **Pellentesque facilisis dolor in leo** bibendum congue. Maecenas congue finibus justo, vitae eleifend urna facilisis at.

Nulla eget sem quam. Ut aliquam volutpat nisi vestibulum convallis. Nunc a lectus et eros facilisis hendrerit eu non urna. Interdum et malesuada fames ac ante *ipsum primis* in faucibus. Etiam sit amet velit eget sem euismod tristique. Praesent enim erat, porta vel mattis sed, pharetra sed ipsum. Morbi commodo condimentum massa, *tempus venenatis* massa hendrerit quis. Maecenas sed porta est. Praesent mollis interdum lectus, sit amet sollicitudin risus tincidunt non.

A block containing some math

Nullam non est elit. In eu ornare justo. Maecenas porttitor sodales lacus, ut cursus augue sodales ac.

$$\int_{-\infty}^{\infty} e^{-x^2}\,dx = \sqrt{\pi}$$

Interdum et malesuada fames $\{1, 4, 9, \ldots\}$ ac ante ipsum primis in faucibus. Cras eleifend dolor eu nulla suscipit suscipit. Sed lobortis non felis id vulputate.

A heading inside a block

Praesent consectetur mi $x^2 + y^2$ metus, nec vestibulum justo viverra nec. Proin eget nulla pretium, egestas magna aliquam, mollis neque. Vivamus dictum $\mathbf{u}^\intercal\mathbf{v}$ sagittis odio, vel porta erat congue sed. Maecenas ut dolor quis arcu auctor porttitor.

Another heading inside a block

Sed augue erat, scelerisque a purus ultricies, placerat porttitor neque. Donec $P(y \mid x)$ fermentum consectetur $\nabla_x P(y \mid x)$ sapien sagittis egestas. Duis eget leo euismod nunc viverra imperdiet nec id justo.

Nullam vel erat at velit convallis laoreet

Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Phasellus libero enim, gravida sed erat sit amet, scelerisque congue diam. Fusce dapibus dui ut augue pulvinar iaculis.

First column	Second column	Third column	Fourth
Foo	13.37	384,394	α
Bar	2.17	1,392	β
Baz	3.14	83,742	δ
Qux	7.59	974	γ

Table 1. A table caption.

Donec quis posuere ligula. Nunc feugiat elit a mi malesuada consequat. Sed imperdiet augue ac nibh aliquet tristique. Aenean eu tortor vulputate, eleifend lorem in, dictum urna. Proin auctor ante in augue tincidunt tempor. Proin pellentesque vulputate odio, ac gravida nulla posuere efficitur. Aenean at velit vel dolor blandit molestie. Mauris laoreet commodo quam, non luctus nibh ullamcorper in. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos.

Nulla varius finibus volutpat. Mauris molestie lorem tincidunt, iaculis libero at, gravida ante. Phasellus at felis eu neque suscipit suscipit. Integer ullamcorper, dui nec pretium ornare, urna dolor consequat libero, in feugiat elit lorem euismod lacus. Pellentesque sit amet dolor mollis, auctor urna non, tempus sem.

Providence

Providence is great! Efficient like Minerva but flexible like BRAVO.

Simulations

Look, Providence does pretty ok!

References