THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Ballot Polling Risk-Limiting Audit Providence

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

[1]Department of Computer Science, The George Washington University [2]University of Wrocław [3]Votifica

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Original Contributions

A Risk-Limiting Audit (RLA) is a statistical election tabulation audit with a rigorous error guarantee: viewed as a binary hypothesis test with the null hypothesis being that the announced election outcome is incorrect, its Type I error is bounded above, whatever the true election tally.

We present RLA Providence. [2]

1. Proof that Providence is an RLA and resistant to an adversary who can choose next round sizes after knowing the current sample.
2. Simulations of Providence, Minerva, SO BRAVO, and EoR BRAVO which show that Providence uses number of ballots similar to those of Minerva, both fewer than either version of BRAVO.
3. Results and analysis from the use of Providence in a pilot audit in Rhode Island.
4. A model of workload that includes the overhead effort of each round and the overhead effort of retrieving a storage unit of ballots; simulations that illustrate the use of this model to compare the different types of ballot polling audits and to plan an audit with minimal workload.
5. An analysis of round size as a function of the maximum acceptable probability of a misleading audit sample.
6. Open source implementation of Providence and audit planning tools. The implementation of Providence has been integrated as an option in Arlo.

Risk-Limiting Audits

- A risk-limiting audit (RLA) draws paper ballots in rounds, stopping if a rigorous statistical criterion is satisfied, or proceeding to a full hand count. If the announced outcome of the election is erroneous, an RLA will detect the error with high, predetermined minimum probability.
- 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.
- The maximum risk R of audit $\mathcal{A}$ with sample $X \in \{0,1\}^*$ drawn from the true underlying distribution of ballots is
$$R(\mathcal{A}) = \Pr[\mathcal{A}(X) = Correct \mid H_0],$$
where H_0 is the null hypothesis: the true underlying election is a tie.
- An audit $\mathcal{A}$ is a Risk-Limiting Audit with risk limit α iff
$$R(\mathcal{A}) \leq \alpha.$$

Existing Ballot Polling RLAs

BRAVO [3]

- In the two candidate case is an instance of Wald's classic Sequential Probability Ratio Test (SPRT)
- Most efficient RLA when the stopping condition is checked after each ballot is drawn (ballot-by-ballot)
- In real audits, decisions are taken after many ballots are drawn (round-by-round), and BRAVO is implemented as:
  - Selection-Ordered (SO) BRAVO, where ballot selection order is retained, and the decisions are taken as though the audit were ballot-by-ballot
  - End-of-Round (EoR) BRAVO, where the decision using the BRAVO stopping rule is taken once, after the entire round of ballots is drawn

Minerva [5,4]

- Recent RLA designed for round-by-round use
- Known to be risk-limiting if all round sizes are predetermined, before the audit begins
- In a first round chosen to give a 0.90 probability of stopping, Minerva requires
  - 50% as many ballots as EoR BRAVO
  - 70-80% as many ballots as SO BRAVO
- For smaller stopping probability rounds, the benefit of Minerva decreases (i.e. as the audit approaches the ballot-by-ballot case) [1]

Adversarial Round Sizes

Definition [Weakly Round-Choosing Adversary]

A *weakly* round-choosing adversary may choose the first and consequent round sizes as a pre-determined function of audit parameters. That is, the j^{th} round size is a function
$$n_j(\alpha, p_a, p_0, \text{ballot\_manifest})$$
determined before the audit begins.

The following audits are resistant to a weakly round-choosing adversary:

- EoR BRAVO
- SO BRAVO
- Minerva

Definition [Strongly Round-Choosing Adversary]

A strongly round-choosing adversary may choose any round size as any function of audit parameters and all preceding samples. That is, the first round size is a function
$$n_1(\alpha, p_a, p_0, ballot\_manifest),$$
and for all rounds $j \geq 2$, the round size is a function
$$n_j(\alpha, p_a, p_0, \text{ballot\_manifest}, k_{j-1}, n_{j-1})$$
The functions n_j, $j \geq 1$ may be chosen at any time before the j^{th} round begins.

The following audits are resistant to a strongly round-choosing adversary:

- EoR BRAVO
- SO BRAVO

The following audits may be vulnerable to a strongly round-choosing adversary:

- Minerva

This means that Minerva audits can't be used in RLAs where future round sizes are chosen based on previous samples; predetermined round schedules are required.

Providence

- The efficiency of Minerva is great, but it lacks the flexibility of BRAVO in choosing round sizes based on previous samples.
- Providence is our novel RLA which has the efficiency of Minerva and the flexibility of BRAVO.
- For alternative hypothesis H_a that the election is truly as announced and null hypothesis H_0 that the true election is a tie, BRAVO has the stopping condition that for k cumulative ballots for the winner and n cumulative sampled ballots,
$$\sigma(k, n, p_a, p_0) \triangleq \frac{\Pr[K = k \mid H_a, n]}{\Pr[K = k \mid H_0, n]} \geq \frac{1}{\alpha}.$$
- Minerva has the stopping condition that in round j with cumulative winner ballots k_j and round sizes $\bar{n}_j = n_1, n_2, \ldots, n_j$
$$\tau_j(k_j, \bar{n}_j, p_a, p_0) \triangleq \frac{\Pr[K_j \geq k_j \wedge \mathcal{A}_{i<j}(X) \neq Correct \mid H_a, \bar{n}_j]}{\Pr[K_j \geq k_j \wedge \mathcal{A}_{i<j}(X) \neq Correct \mid H_0, \bar{n}_j]} \geq \frac{1}{\alpha}.$$
Testing this stopping condition requires computationaly expensive convolutions.
- The Providence stopping condition uses ideas from both BRAVO and Minerva and requires no convolution to test:
$$\omega_j(k_{j-1}, k_j, n_{j-1}, n_j, p_a, p_0) \triangleq \sigma(k_{j-1}, n_{j-1}, p_a, p_0) \cdot \tau_1(k_j, n_j, p_a, p_0) \geq \frac{1}{\alpha}.$$

Resistance against an adversary

Providence is resistant to both a *weakly round-choosing adversary* and a *strongly round-choosing adversary.*

Simulations

We provide proofs for theoretical properties of Providence, but we also run simulations to learn about its behavior and validate properties.

Simulations:

- 2020 Presidential Contest (states with a pairwise margin at least 0.05)
- Risk limit $\alpha = 0.1$
- 10^4 trials per state assuming H_a (i.e. p as reported)
- 10^4 trials per state assuming H_0 (i.e. $p = 0.5$)
- 5 rounds
- Round sizes chosen to each give stopping probability of 0.9, conditioned on the current sample (except Minerva which uses first round size to achieve 0.9 stopping probability and then a multiplier of 1.5)

Risk

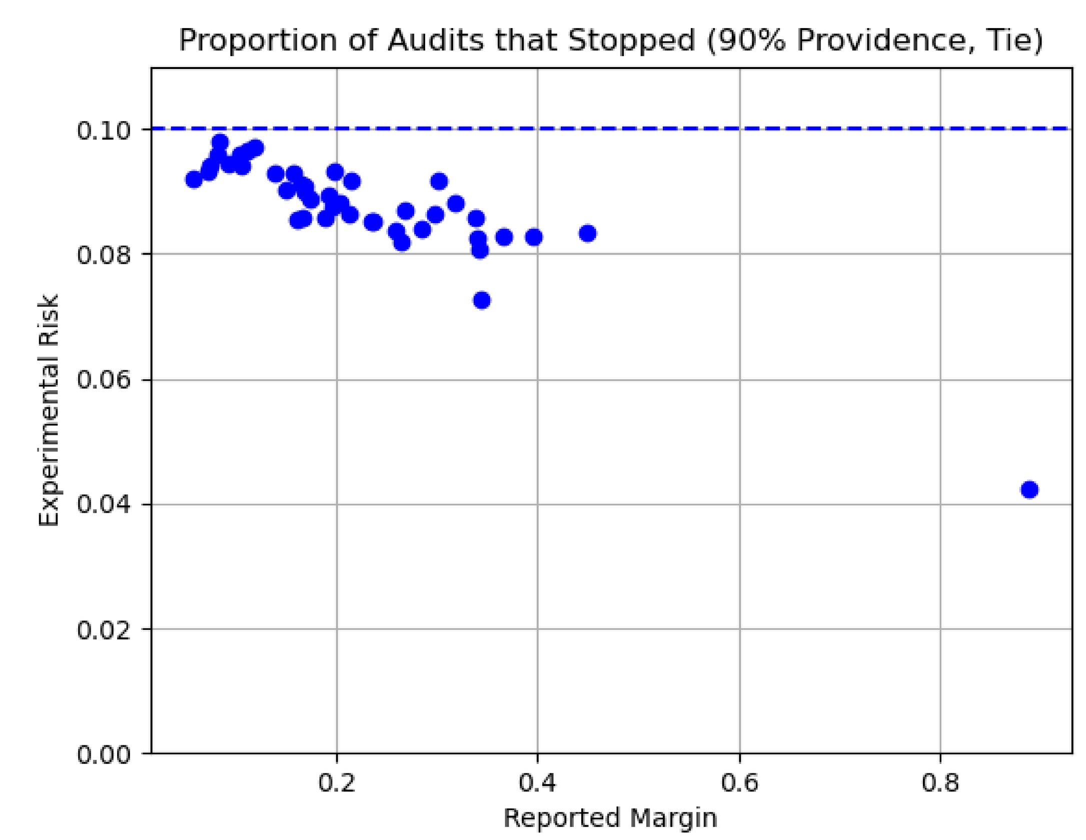

Figure 1. The proportion of simulated Providence audits – assuming the null hypothesis that the underlying margin is a tie – that stopped during any of the five rounds for margins from the 2020 US Presidential contest.

Stopping Probability

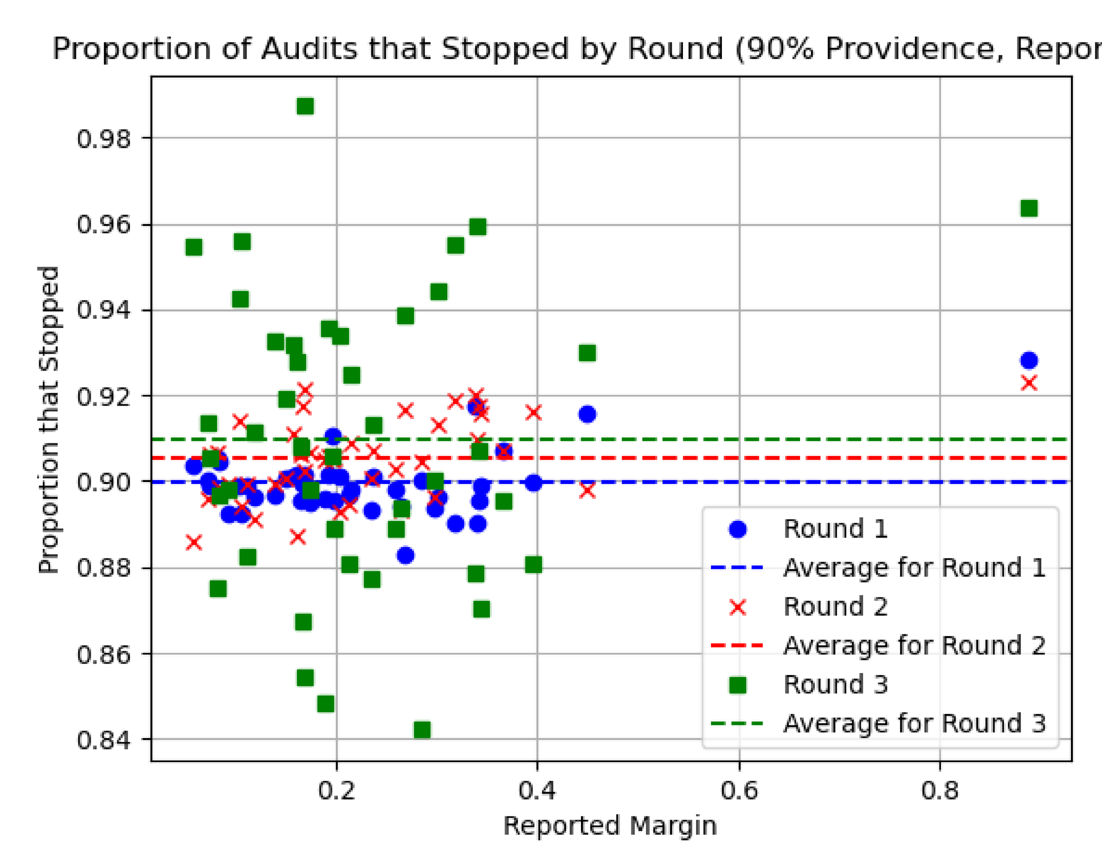

Figure 2. The proportion of simulated Providence audits – assuming the alternative hypothesis that the reported margin is correct – that stopped during rounds 1, 2, and 3, for margins from the 2020 US Presidential contest.

Number of Ballots

US 2020 Presidential Contest in Texas with margin 0.057

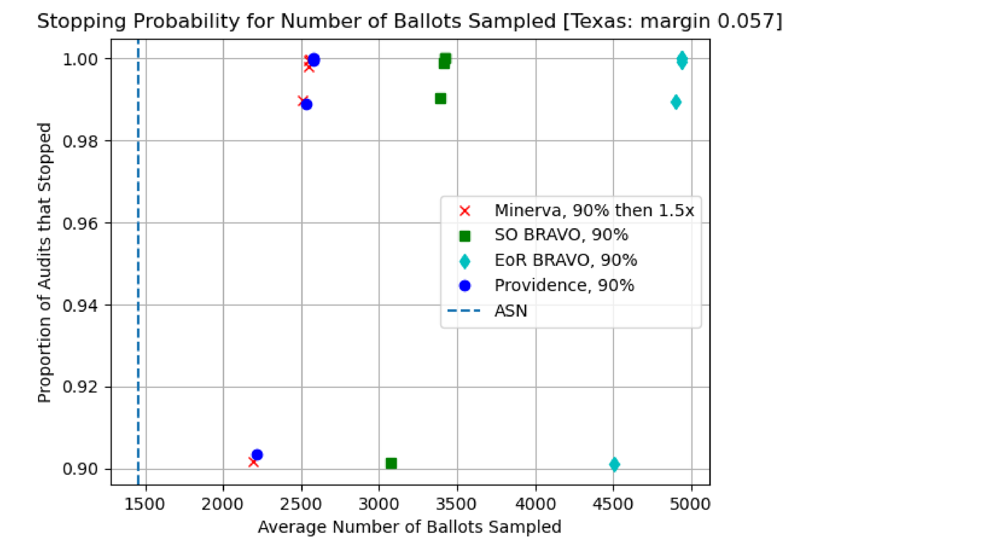

Figure 3. Cumulative fraction of audits that stopped as a function of average number of sampled ballots for the state of Texas with margin $.057$ with first round stopping probability $\chi_1 = 0.9$. Providence, Minerva with multiplier 1.5, and both implementations of BRAVO are included.

Providence Pilot

In February 2022, The Rhode Island Board of Elections hosted a public pilot Providence RLA which passed (met the risk limit) in the first round.

Figure 4. Professor Vora tosses her random-seed-generating 10-sided die, in a roll she dedicated to election officials everywhere. The standing people from left to right are (1) Miguel Nunez, Rhode Island Deputy Director of Elections, (2) Professor Vora, and (3) Mark Lindeman, Verified Voting Director.

References

[1] Oliver Broadrick, Sarah Morin, Grant McClearn, Neal McBurnett, Poorvi L. Vora, and Filip Zagórski. Simulations of ballot polling risk-limiting audits. In *Seventh Workshop on Advances in Secure Electronic Voting, in Association with Financial Crypto*, 2022.

[2] Oliver Broadrick, Poorvi L. Vora, and Filip Zagórski. Providence: a flexible round-by-round risk-limiting audit. In 32^{nd} *USENIX Security Symposium*, 2023.

[3] Mark Lindeman, Philip B Stark, and Vincent S Yates. BRAVO: Ballot-polling risk-limiting audits to verify outcomes. In *EVT/WOTE*, 2012.

[4] Filip Zagórski, Grant McClearn, Sarah Morin, Neal McBurnett, and Poorvi L. Vora. The Athena class of risk-limiting ballot polling audits. *CoRR*, abs/2008.02315, 2020.

[5] Filip Zagórski, Grant McClearn, Sarah Morin, Neal McBurnett, and Poorvi L. Vora. Minerva– an efficient risk-limiting ballot polling audit. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 3059–3076. USENIX Association, August 2021.

odbroadrick@gmail.com