DP-SPRT: Differentially Private Sequential Testing

Thomas Michel, Debabrota Basu, Emilie Kaufmann

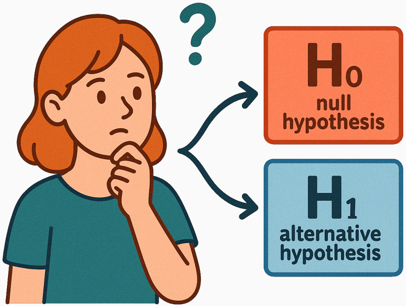
Scool Team, Inria Center of the University of Lille

Sequential Hypothesis Testing

The Problem: We observe samples $X_1, X_2, \ldots$ sequentially from distribution f_θ

Goal: Test $H_0 : \theta = \theta_0$ vs $H_1 : \theta = \theta_1$ with as few samples as possible

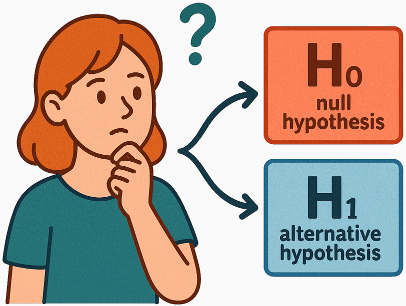
Constraints: False positive probability $\leq \alpha$, false negative probability $\leq \beta$



Sequential Hypothesis Testing

The Problem: We observe samples $X_1, X_2, \ldots$ sequentially from distribution f_θ

Goal: Test $H_0 : \theta = \theta_0$ vs $H_1 : \theta = \theta_1$ with as few samples as possible
Constraints: False positive probability $\leq \alpha$, false negative probability $\leq \beta$



When do we need to test ?

- Clinical Trials
- A/B Testing
- Fraud Detection

In RL and Control:

- Model Validation
- Constraints Satisfaction

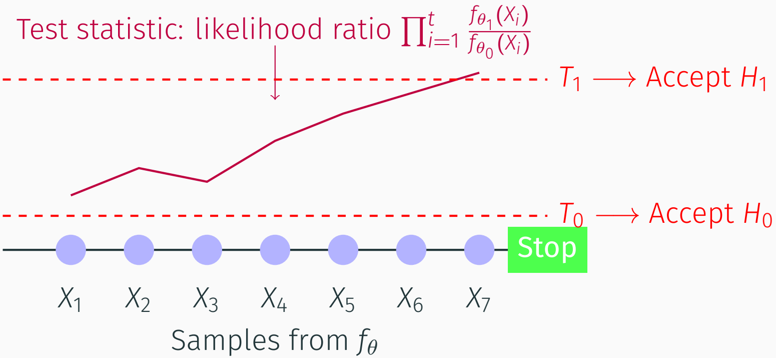
Sequential Probability Ratio Test

The Problem: We observe samples $X_1, X_2, \ldots$ sequentially from distribution f_θ

Goal: Test $H_0 : \theta = \theta_0$ vs $H_1 : \theta = \theta_1$ with as few samples as possible

Constraints: False positive probability $\leq \alpha$, false negative probability $\leq \beta$

Sequential Probability Ratio Test (SPRT) (Wald, 1945):



Sequential Probability Ratio Test

The Problem: We observe samples $X_1, X_2, \ldots$ sequentially from distribution f_θ

Goal: Test $H_0 : \theta = \theta_0$ vs $H_1 : \theta = \theta_1$ with as few samples as possible
Constraints: False positive probability $\leq \alpha$, false negative probability $\leq \beta$

Why Sequential?

- **Efficiency**: Stop as soon as you have enough evidence
- **Optimality**: SPRT minimizes expected sample size
- **Real-time**: Make decisions as data arrives

The Privacy Problem: A Medical Trial

Scenario: Testing if new drug works better than placebo

H_0: Drug success rate = 30% (Same as placebo) vs H_1: Drug success rate = 70%

Each patient outcome: $X_i \in \{0, 1\}$ (failure/success)

The Privacy Problem: A Medical Trial

Scenario: Testing if new drug works better than placebo

H_0: Drug success rate = 30% (Same as placebo) vs H_1: Drug success rate = 70%

Each patient outcome: $X_i \in \{0, 1\}$ (failure/success)

Question: What was patient 7's outcome? **Success (1) or Failure (0)?**

The Privacy Problem: A Medical Trial

Scenario: Testing if new drug works better than placebo

H_0: Drug success rate = 30% (Same as placebo) vs H_1: Drug success rate = 70%

Each patient outcome: $X_i \in \{0, 1\}$ (failure/success)

Question: What was patient 7's outcome? **Success (1) or Failure (0)?**

The stopping decision reveals patient 7 had a SUCCESS!

Privacy violation: Patient 7's medical outcome is leaked by our decision to stop

Privacy in Sequential Decisions

Clinical Trial

- Testing new drug vs placebo
- Stopping pattern reveals:
  - Treatment effectiveness
  - Patient responses

A/B Testing

- Users see different versions
- When we conclude reveals:
  - User behavior
  - Conversion rates

Fraud Detection

- Monitor transactions
- Alert timing reveals:
  - Transaction patterns
  - Detection methods

Core Problem: When we stop reveals what we observed

Differential Privacy

Neighboring Datasets: Two datasets D, D' are neighboring if they differ by exactly one record.

Differential Privacy (Dwork, Roth, et al., 2014): A randomized mechanism $\mathcal{M}$ is DP if for any neigboring datasets D and D' and for any events S:

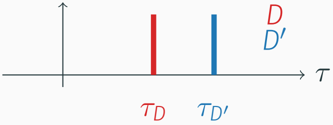
$$\varepsilon\text{-DP:} \quad \log\left(\frac{\mathbb{P}[\mathcal{M}(D) \in S]}{\mathbb{P}[\mathcal{M}(D') \in S]}\right) \leq \varepsilon$$

$$(\alpha, \varepsilon)\text{-Rényi DP:} \quad D_\alpha(\mathcal{M}(D) \| \mathcal{M}(D')) \leq \varepsilon$$

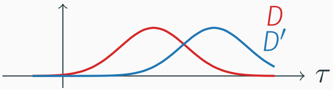
where D_α is the Rényi divergence of order $\alpha > 1$.

Stopping Time Distributions

Deterministic Algorithm



Private Algorithm



Privacy adds randomness to mask the stopping decision pattern

Our Method: DP-SPRT

DP-SPRT Algorithm (blue = privacy additions to SPRT):

Input: Hypotheses θ_0, θ_1, error probabilities α, β, noise distributions $\mathcal{D}_Z, \mathcal{D}_Y$, correction function $C(n, x)$, error allocation γ

1. Sample threshold noise $Z \sim \mathcal{D}_Z$
2. **For** $n = 1, 2, 3, \ldots$ **do**
3. Sample query noise $Y_n \sim \mathcal{D}_Y$
4. Compute noisy average $\bar{X}_n = \frac{1}{n} \sum_{i=1}^{n} X_i + \frac{Y_n}{n}$
5. Compute noisy threshold $\hat{T}_0^n = \mu_0 + \frac{\mathrm{KL}(\nu_{\theta_0}, \nu_{\theta_1}) - \log(1/(\gamma\beta))/n}{\theta_1 - \theta_0} - C(n, (1-\gamma)\beta) - \frac{Z}{n}$
6. Compute noisy threshold $\hat{T}_1^n = \mu_1 - \frac{\mathrm{KL}(\nu_{\theta_1}, \nu_{\theta_0}) - \log(1/(\gamma\alpha))/n}{\theta_1 - \theta_0} + C(n, (1-\gamma)\alpha) + \frac{Z}{n}$
7. **If** noisy average $\bar{X}_n$ is below noisy threshold $\hat{T}_0^n$ **then** Halt and accept $\mathcal{H}_0$
8. **Else if** noisy average $\bar{X}_n$ is above noisy threshold $\hat{T}_1^n$ **then** Halt and accept $\mathcal{H}_1$

DP-SPRT: Privacy

Table: Comparison of DP-SPRT instantiations

	Laplace Noise	Gaussian Noise
Noise distributions	$Y_n \sim \mathrm{Lap}(4/\varepsilon)$ $Z \sim \mathrm{Lap}(2/\varepsilon)$	$Y_n \sim \mathcal{N}(0, \sigma_Y^2)$ $Z \sim \mathcal{N}(0, \sigma_Z^2)$
Privacy guarantee	ε-Differential Privacy	$(\alpha, \varepsilon(\alpha))$-RDP
Correction function $C(n, x)$	$\frac{6 \log(n^s \zeta(s)/x)}{n\varepsilon}$	$\frac{\sqrt{2(\sigma_Y^2+\sigma_Z^2) \log(n^s \zeta(s)/2)}}{n}$

- **Exact error control**: $\mathbb{P}_{\theta_0}(\text{reject } H_0) \leq \alpha$, $\mathbb{P}_{\theta_1}(\text{accept } H_0) \leq \beta$
- **Theoretical calibration**: No empirical tuning required
- **Privacy amplification**: Enhanced with subsampling in high-privacy regimes

Near-Optimal Sample Complexity (DP-SPRT with Laplace noise)

Lower Bound (any ε-DP test):

$$\mathbb{E}[\tau] \geq \frac{\log(1/\beta)}{\min(\mathrm{KL}(\nu_{\theta_0}, \nu_{\theta_1}), \varepsilon \cdot \mathrm{TV}(\nu_{\theta_0}, \nu_{\theta_1}))} \tag{1}$$

Sample Complexity Upper Bound (Laplace Noise):

$$\mathbb{E}[\tau] \lesssim \max\left(\frac{\log(1/\beta)}{\mathrm{KL}(\nu_{\theta_0}, \nu_{\theta_1})}, \frac{(\theta_1 - \theta_0)\log(1/\beta)}{\varepsilon \cdot \mathrm{KL}(\nu_{\theta_0}, \nu_{\theta_1})} \right) \tag{2}$$

For Bernoulli distributions, we have

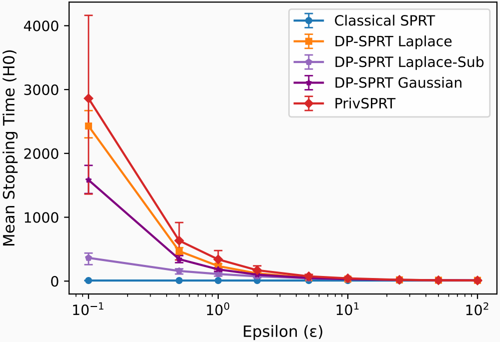
$$\frac{\mathrm{KL}(\nu_{\theta_0}, \nu_{\theta_1})}{\theta_1 - \theta_0} \xrightarrow[\theta_1 \to \theta_0]{} \mathrm{TV}(\nu_{\theta_0}, \nu_{\theta_1})$$

DP-SPRT with Laplace noise is near-optimal

Experimental Results: Performance Comparison

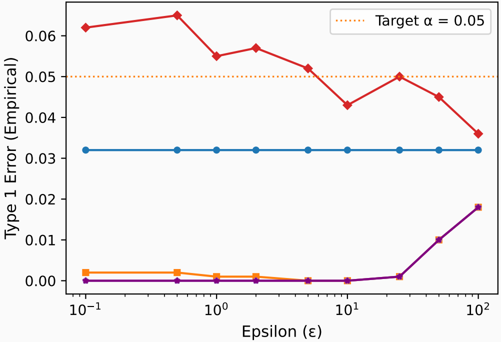
Setup: Bernoulli($p_0 = 0.3$) vs Bernoulli($p_1 = 0.7$), $\alpha = \beta = 0.05$, 1000 trials

Sample Complexity vs Privacy Level



On average, **DP-SPRT variants outperform** PrivSPRT (Zhang, Mei, and Cummings, 2022) across privacy levels

Error Control Comparison



All DP-SPRT variants guarantee error control, while PrivSPRT can violate error targets due to empirical tuning

Conclusion

Privacy:

- Real-world applications **NEED** privacy (regulations, competition, ethics)
- Sequential decisions leak sensitive information

Conclusion

Privacy:

- Real-world applications NEED privacy (regulations, competition, ethics)
- Sequential decisions leak sensitive information

Our Contributions:

1. **First theoretically calibrated** private sequential test with guaranteed error control
2. **Near-optimal sample complexity** matching lower bounds up to a constant in some regimes
3. **Practical implementation** with no empirical tuning required, low variance in stopping times, and subsampling amplification in high-privacy regimes

Conclusion

Privacy:

- Real-world applications NEED privacy (regulations, competition, ethics)
- Sequential decisions leak sensitive information

Our Contributions:

1. **First theoretically calibrated** private sequential test with guaranteed error control
2. **Near-optimal sample complexity** matching lower bounds up to a constant in some regimes
3. **Practical implementation** with no empirical tuning required, low variance in stopping times, and subsampling amplification in high-privacy regimes

Thank you! Questions?

References

Dwork, Cynthia, Aaron Roth, et al. (2014). **"The algorithmic foundations of differential privacy".** In: *Foundations and Trends® in Theoretical Computer Science* 9.3–4, pp. 211–407.

Wald, A. (1945). **"Sequential Tests of Statistical Hypotheses".** In: *Annals of Mathematical Statistics* 16(2), pp. 117–186.

Zhang, Wanrong, Yajun Mei, and Rachel Cummings (2022). **"Private Sequential Hypothesis Testing for Statisticians: Privacy, Error Rates, and Sample Size".** In: *AISTATS*.