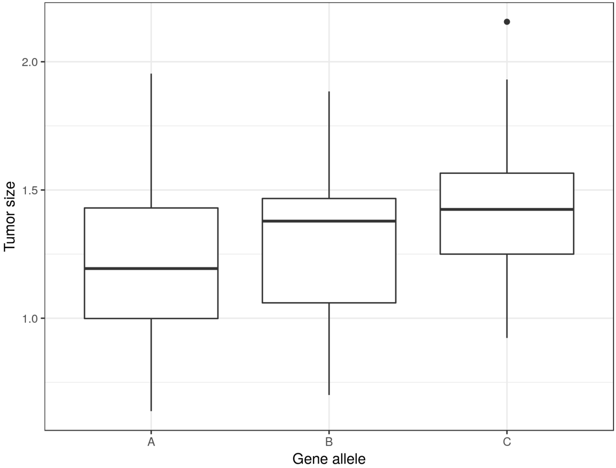
Improved Differentially Private Analysis of Variance

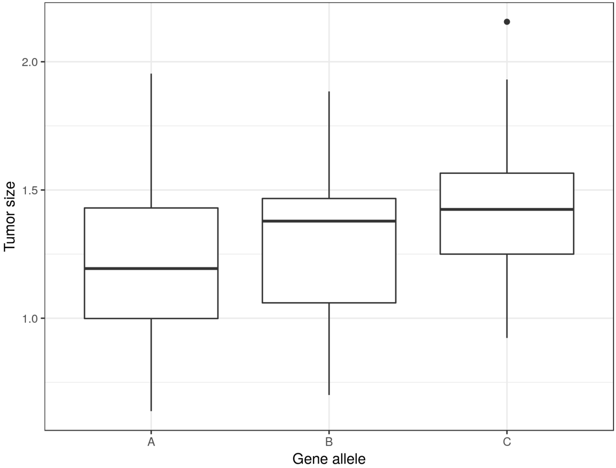
Marika Swanberg Ira Globus-Harris Iris Griffith
Anna Ritz Andrew Bray Adam Groce

Reed College

Observed Data, $n = 30$



Observed Data, $n = 30$



Are gene allele and tumor size dependent?

Metric for dependency

$$F\text{-test} = \frac{\text{Variation between groups}}{\text{In-group variation}}$$

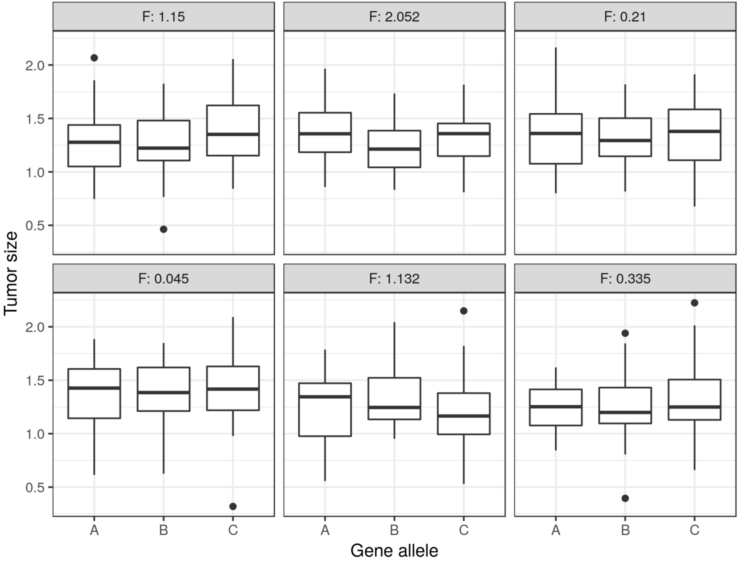
Metric for dependency

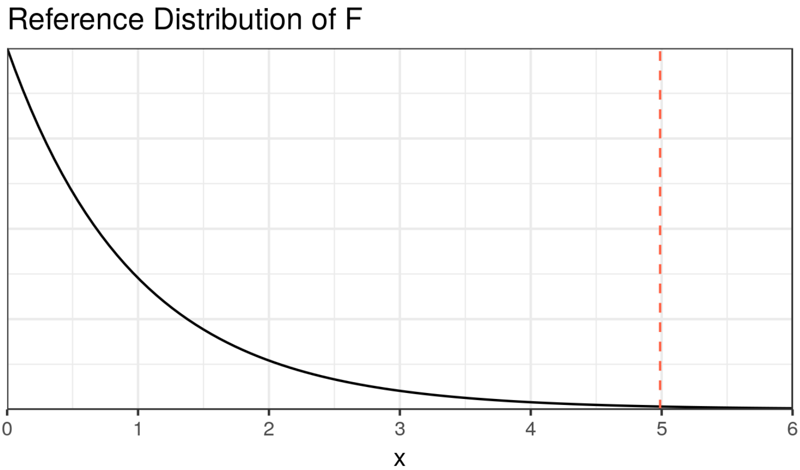
$$F\text{-test} = \frac{\text{Variation between groups}}{\text{In-group variation}}$$

$$SSA(D) = \sum_{j=1}^{k} n_j(\bar{y}_j - \bar{y})^2/(k-1)$$

$$SSE(D) = \sum_{i=1}^{n} (y_i - \bar{y}_{c_i})^2/(n-k)$$

Simulate Random Data





Now do we think our data supports independence of gene allele and tumor size?

Why is F-test optimal?

Why is F-test optimal?

High probability of indicating dependence when variables <u>are</u> dependent . . .

Why is F-test optimal?

High probability of indicating dependence when variables are dependent . . .

. . . even when dataset is small.

Why is F-test optimal?

High probability of indicating dependence when variables are dependent ...

... even when dataset is small.

Definition (Power)

The **power** of a hypothesis test is the probability it rejects H_0. It depends on the alternate distribution H_A and n.

Why is F-test optimal?

High probability of indicating dependence when variables are dependent . . .

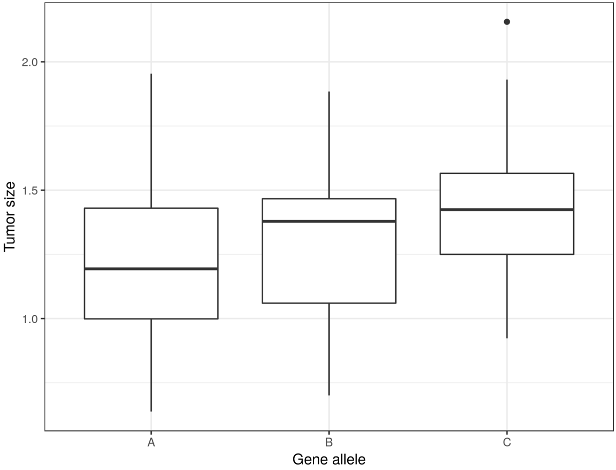
. . . even when dataset is small.

Definition (Power)

The **power** of a hypothesis test is the probability it rejects H_0. It depends on the alternate distribution H_A and n.

Goal of any test statistic is achieving high power*.

Observed Data, $n = 30$



What if we want to keep this data private?

Differential privacy [DMNS06]

Definition

Two databases are **neighboring** if they differ only in the data of one individual.

Differential privacy [DMNS06]

Definition

Two databases are **neighboring** if they differ only in the data of one individual.

Definition

A query f is ε-**differentially private** if for all neighboring databases D, D' and all output sets S

$$\Pr[f(D) \in S] \leq e^{\varepsilon} \Pr[f(D') \in S].$$

Properties of differential privacy [DMNS06]

Theorem (Post-processing)

If f is ε-differentially private then for any (randomized) function g, then if $h(D) = g(f(D)$, h is also ε-differentially private.

Properties of differential privacy [DMNS06]

Theorem (Post-processing)

If f is ε-differentially private then for any (randomized) function g, then if $h(D) = g(f(D)$, h is also ε-differentially private.

Theorem (Composition)

If f is ε_1-differentially private and g is ε_2-differentially private then if $h(D) = (g(D), f(D))$, h is $(\varepsilon_1 + \varepsilon_2)$-differentially private.

Laplace mechanism

Definition (Sensitivity)

The sensitivity Δf of a deterministic, real-valued function f on databases is the maximum over all pairs of neighboring D, D' of $|f(D) - f(D')|$.

Laplace mechanism

Definition (Sensitivity)

The sensitivity Δf of a deterministic, real-valued function f on databases is the maximum over all pairs of neighboring D, D' of $|f(D) - f(D')|$.

Theorem (Laplace Mechanism)

Given any deterministic, real-valued function f on databases, define $\widehat{f}$ as

$$\widehat{f}(D) = f(D) + Y,$$

where $Y \leftarrow \mathrm{Lap}(\Delta f/\varepsilon)$. The Laplace mechanism is ε-differentially private.

Related Works

Other work on private hypothesis testing:

Related Works

Other work on private hypothesis testing:

- Asymptotic analysis [WZ10, Smith11, CKMSU19]

Related Works

Other work on private hypothesis testing:

- Asymptotic analysis [WZ10, Smith11, CKMSU19]
- Chi-squared test (difference of discrete distributions) [VS09, FSU11, JS13, USF13, WLK15, GLRV16, RK17]

Related Works

Other work on private hypothesis testing:

- Asymptotic analysis [WZ10, Smith11, CKMSU19]
- Chi-squared test (difference of discrete distributions) [VS09, FSU11, JS13, USF13, WLK15, GLRV16, RK17]
- Other tests:

Related Works

Other work on private hypothesis testing:

- Asymptotic analysis [WZ10, Smith11, CKMSU19]
- Chi-squared test (difference of discrete distributions) [VS09, FSU11, JS13, USF13, WLK15, GLRV16, RK17]
- Other tests:
  - Binomial data [AS18] (Proven optimal!)

Related Works

Other work on private hypothesis testing:

- Asymptotic analysis [WZ10, Smith11, CKMSU19]
- Chi-squared test (difference of discrete distributions) [VS09, FSU11, JS13, USF13, WLK15, GLRV16, RK17]
- Other tests:
  - Binomial data [AS18] (Proven optimal!)
  - Difference of two means [OHK15, DNLI18]

Related Works

Other work on private hypothesis testing:

- Asymptotic analysis [WZ10, Smith11, CKMSU19]
- Chi-squared test (difference of discrete distributions) [VS09, FSU11, JS13, USF13, WLK15, GLRV16, RK17]
- Other tests:
  - Binomial data [AS18] (Proven optimal!)
  - Difference of two means [OHK15, DNLI18]
  - Linear regression [BRMC17, Sheffet17]

Related Works

Other work on private hypothesis testing:

- Asymptotic analysis [WZ10, Smith11, CKMSU19]
- Chi-squared test (difference of discrete distributions) [VS09, FSU11, JS13, USF13, WLK15, GLRV16, RK17]
- Other tests:
  - Binomial data [AS18] (Proven optimal!)
  - Difference of two means [OHK15, DNLI18]
  - Linear regression [BRMC17, Sheffet17]

Earlier work is often missing:

Related Works

Other work on private hypothesis testing:

- Asymptotic analysis [WZ10, Smith11, CKMSU19]
- Chi-squared test (difference of discrete distributions) [VS09, FSU11, JS13, USF13, WLK15, GLRV16, RK17]
- Other tests:
  - Binomial data [AS18] (Proven optimal!)
  - Difference of two means [OHK15, DNLI18]
  - Linear regression [BRMC17, Sheffet17]

Earlier work is often missing:

- Rigorous p-value computations

Related Works

Other work on private hypothesis testing:

- Asymptotic analysis [WZ10, Smith11, CKMSU19]
- Chi-squared test (difference of discrete distributions) [VS09, FSU11, JS13, USF13, WLK15, GLRV16, RK17]
- Other tests:
  - Binomial data [AS18] (Proven optimal!)
  - Difference of two means [OHK15, DNLI18]
  - Linear regression [BRMC17, Sheffet17]

Earlier work is often missing:

- Rigorous p-value computations
- Power analysis

Unique Challenges of Private Hypothesis Testing

- How to compute p-value?

Unique Challenges of Private Hypothesis Testing

- How to compute p-value?
  - Reference distribution is no longer closed-form

Unique Challenges of Private Hypothesis Testing

- How to compute p-value?
  - Reference distribution is no longer closed-form
  - Solution: simulate it
- Lots of tricky details

Unique Challenges of Private Hypothesis Testing

- How to compute p-value?
  - Reference distribution is no longer closed-form
  - Solution: simulate it
- Lots of tricky details
  - Ex: negative private estimates of standard deviation because of negative noise?

Unique Challenges of Private Hypothesis Testing

- How to compute *p*-value?
  - Reference distribution is no longer closed-form
  - Solution: simulate it
- Lots of tricky details
  - Ex: negative private estimates of standard deviation because of negative noise?
  - Solution: ask the statistician

Unique Challenges of Private Hypothesis Testing

- How to compute p-value?
  - Reference distribution is no longer closed-form
  - Solution: simulate it
- Lots of tricky details
  - Ex: negative private estimates of standard deviation because of negative noise?
  - Solution: ask the statistician
- Low statistical power

Unique Challenges of Private Hypothesis Testing

- How to compute p-value?
  - Reference distribution is no longer closed-form
  - Solution: simulate it
- Lots of tricky details
  - Ex: negative private estimates of standard deviation because of negative noise?
  - Solution: ask the statistician
- Low statistical power
  - Need a lot of data/impractical

Unique Challenges of Private Hypothesis Testing

- How to compute p-value?
  - Reference distribution is no longer closed-form
  - Solution: simulate it
- Lots of tricky details
  - Ex: negative private estimates of standard deviation because of negative noise?
  - Solution: ask the statistician
- Low statistical power
  - Need a lot of data/impractical
  - Main point of improvement

Private ANOVA [CBRG18]

Assume data is on the $[0, 1]$ interval.

Private ANOVA [CBRG18]

Assume data is on the $[0, 1]$ interval.

Theorem

SSE has sensitivity bounded by 7.

Private ANOVA [CBRG18]

Assume data is on the $[0, 1]$ interval.

Theorem

SSE has sensitivity bounded by 7.

$$\widehat{SSE}(D) = SSE(D) + \mathrm{Lap}(7/\varepsilon)$$

Private ANOVA [CBRG18]

Assume data is on the $[0, 1]$ interval.

Theorem

SSE has sensitivity bounded by 7.

$$\widehat{SSE}(D) = SSE(D) + \mathrm{Lap}(7/\varepsilon)$$

Theorem

SSA has sensitivity bounded by $9 + 5/n$.

Private ANOVA [CBRG18]

Assume data is on the $[0, 1]$ interval.

Theorem

SSE has sensitivity bounded by 7.

$$\widehat{SSE}(D) = SSE(D) + \mathrm{Lap}(7/\varepsilon)$$

Theorem

SSA has sensitivity bounded by $9 + 5/n$.

$$\widehat{SSA}(D) = SSA(D) + \mathrm{Lap}\left(\frac{9 + 5/n}{\varepsilon}\right)$$

Private ANOVA [CBRG18]

$$\widehat{F}(D) = \frac{\widehat{SSA}(D)/(k-1)}{\widehat{SSE}(D)/(n-k)}$$

Private ANOVA [CBRG18]

$$\widehat{F}(D) = \frac{\widehat{SSA}(D)/(k-1)}{\widehat{SSE}(D)/(n-k)}$$

Problem: The reference distribution is a mess.

Private ANOVA [CBRG18]

$$\widehat{F}(D) = \frac{\widehat{SSA}(D)/(k-1)}{\widehat{SSE}(D)/(n-k)}$$

Problem: The reference distribution is a mess.

- Simulate it.

Private ANOVA [CBRG18]

$$\widehat{F}(D) = \frac{\widehat{SSA}(D)/(k-1)}{\widehat{SSE}(D)/(n-k)}$$

Problem: The reference distribution is a mess.

- Simulate it.

Problem: The reference distribution is no longer scale free.

Private ANOVA [CBRG18]

$$\widehat{F}(D) = \frac{\widehat{SSA}(D)/(k-1)}{\widehat{SSE}(D)/(n-k)}$$

Problem: The reference distribution is a mess.

- Simulate it.

Problem: The reference distribution is no longer scale free.

- Luckily, $\widehat{SSE}$ is a variance estimate.

Private ANOVA [CBRG18]

$$\widehat{F}(D) = \frac{\widehat{SSA}(D)/(k-1)}{\widehat{SSE}(D)/(n-k)}$$

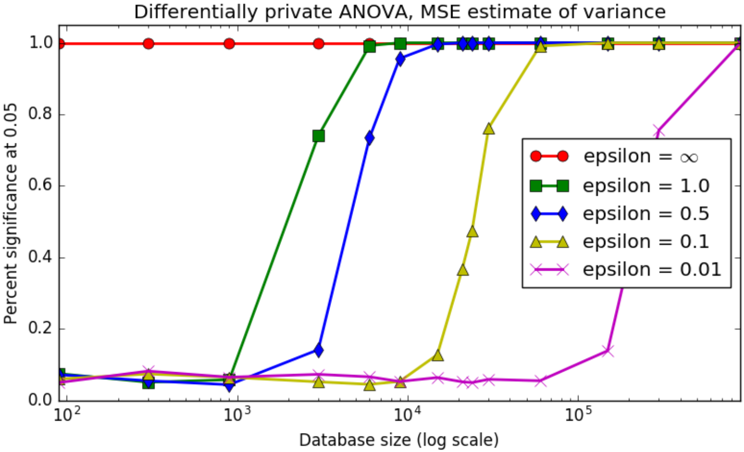
Problem: The reference distribution is a mess.

- Simulate it.

Problem: The reference distribution is no longer scale free.

- Luckily, $\widehat{SSE}$ is a variance estimate.
- Empirically checked: good enough, type 1 error rate bounded by α

Private ANOVA [CBRG18]



Improving ANOVA [SHGRGB19]

Create a new test statistic!

Improving ANOVA [SHGRGB19]

Create a new test statistic!

$$SSA(D) = \sum_{j=1}^{k} n_j(\bar{y}_j - \bar{y})^2 \Longrightarrow SA(D) = \sum_{j=1}^{k} n_j|\bar{y}_j - \bar{y}|$$

$$SSE(D) = \sum_{i=1}^{n} (y_i - \bar{y}_{c_i})^2 \Longrightarrow SE(D) = \sum_{i=1}^{n} |y_i - \bar{y}_{c_i}|$$

$$F(D) = \frac{SSA(D)/(k-1)}{SSE(D)/(n-k)} \Longrightarrow F_1(D) = \frac{SA(D)/(k-1)}{SE(D)/(n-k)}$$

Improving ANOVA [SHGRGB19]

Create a new test statistic!

$$SSA(D) = \sum_{j=1}^{k} n_j(\bar{y}_j - \bar{y})^2 \Longrightarrow SA(D) = \sum_{j=1}^{k} n_j|\bar{y}_j - \bar{y}|$$

$$SSE(D) = \sum_{i=1}^{n}(y_i - \bar{y}_{c_i})^2 \Longrightarrow SE(D) = \sum_{i=1}^{n} |y_i - \bar{y}_{c_i}|$$

$$F(D) = \frac{SSA(D)/(k-1)}{SSE(D)/(n-k)} \Longrightarrow F_1(D) = \frac{SA(D)/(k-1)}{SE(D)/(n-k)}$$

The new F_1 statistic has:

Improving ANOVA [SHGRGB19]

Create a new test statistic!

$$SSA(D) = \sum_{j=1}^{k} n_j(\bar{y}_j - \bar{y})^2 \implies SA(D) = \sum_{j=1}^{k} n_j|\bar{y}_j - \bar{y}|$$

$$SSE(D) = \sum_{i=1}^{n}(y_i - \bar{y}_{c_i})^2 \implies SE(D) = \sum_{i=1}^{n} |y_i - \bar{y}_{c_i}|$$

$$F(D) = \frac{SSA(D)/(k-1)}{SSE(D)/(n-k)} \implies F_1(D) = \frac{SA(D)/(k-1)}{SE(D)/(n-k)}$$

The new F_1 statistic has:

- Lower sensitivity (3 for SE, 4 for SA)

Improving ANOVA [SHGRGB19]

Create a new test statistic!

$$SSA(D) = \sum_{j=1}^{k} n_j(\bar{y}_j - \bar{y})^2 \Longrightarrow SA(D) = \sum_{j=1}^{k} n_j|\bar{y}_j - \bar{y}|$$

$$SSE(D) = \sum_{i=1}^{n} (y_i - \bar{y}_{c_i})^2 \Longrightarrow SE(D) = \sum_{i=1}^{n} |y_i - \bar{y}_{c_i}|$$

$$F(D) = \frac{SSA(D)/(k-1)}{SSE(D)/(n-k)} \Longrightarrow F_1(D) = \frac{SA(D)/(k-1)}{SE(D)/(n-k)}$$

The new F_1 statistic has:

- Lower sensitivity (3 for SE, 4 for SA)
- Much higher typical value

Improving ANOVA [SHGRGB19]

Making F_1 private

Improving ANOVA [SHGRGB19]

Making F_1 private

1. Use Laplace mechanism as in [CBRG18]

Improving ANOVA [SHGRGB19]

Making F_1 private

1. Use Laplace mechanism as in [CBRG18]
2. Simulate reference distribution for computing p-value
   - Problem: need standard deviation

Improving ANOVA [SHGRGB19]

Making F_1 private

1. Use Laplace mechanism as in [CBRG18]
2. Simulate reference distribution for computing p-value
   - Problem: need standard deviation
3. Private estimate of standard deviation:
   - Allocate some of epsilon budget?

Improving ANOVA [SHGRGB19]

Making F_1 private

1. Use Laplace mechanism as in [CBRG18]
2. Simulate reference distribution for computing p-value
   - Problem: need standard deviation
3. Private estimate of standard deviation:
   - Allocate some of epsilon budget? Makes power worse

Improving ANOVA [SHGRGB19]

Making F_1 private

1. Use Laplace mechanism as in [CBRG18]
2. Simulate reference distribution for computing p-value
   - Problem: need standard deviation
3. Private estimate of standard deviation:
   - Allocate some of epsilon budget? Makes power worse
   - Solution: derive an unbiased estimator for σ

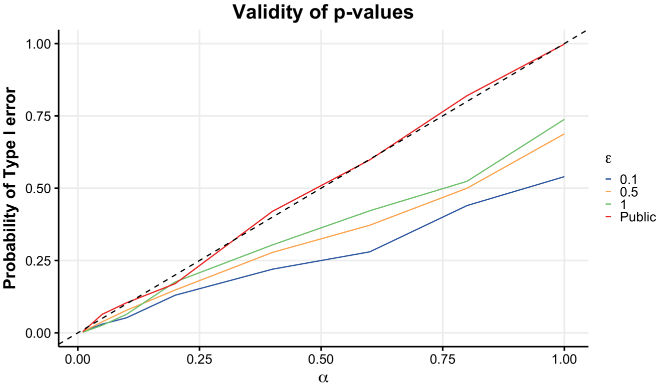
Improving ANOVA [SHGRGB19]

Making F_1 private

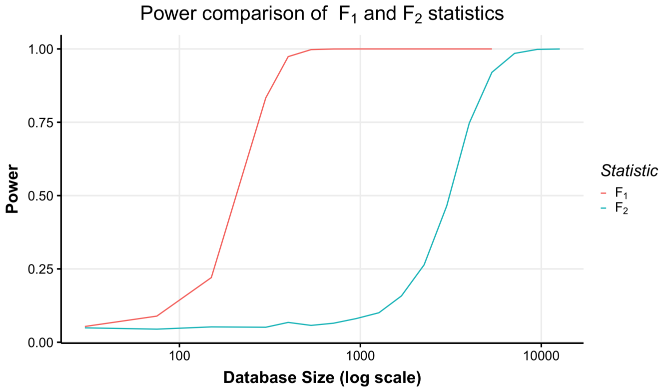
1. Use Laplace mechanism as in [CBRG18]
2. Simulate reference distribution for computing p-value
   - Problem: need standard deviation
3. Private estimate of standard deviation:
   - Allocate some of epsilon budget? Makes power worse
   - Solution: derive an unbiased estimator for σ

$$\hat{\sigma} = \sqrt{\pi/2} \cdot \frac{\widehat{SE}}{(N-k)}$$

Validity of p-values



Power of F_1 test



Power comparision at $\varepsilon = 1$. F achieves 80% power with 4500 observations. F_1 requires 300.

Further Optimization

New Developments [CKSBG19]

Kruskal-Wallis test analogous to F-test

New Developments [CKSBG19]

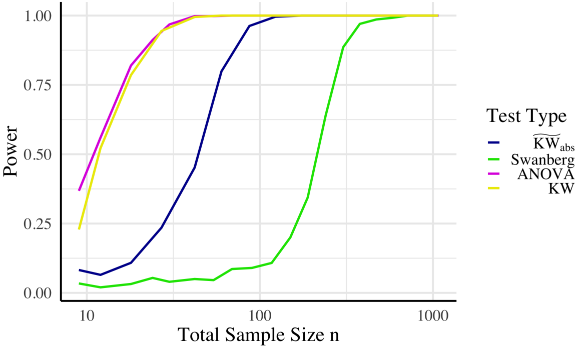
Kruskal-Wallis test analogous to F-test

Modified KW test, similar methods as [SHGRGB19]

New Developments [CKSBG19]

Kruskal-Wallis test analogous to F-test

Modified KW test, similar methods as [SHGRGB19]

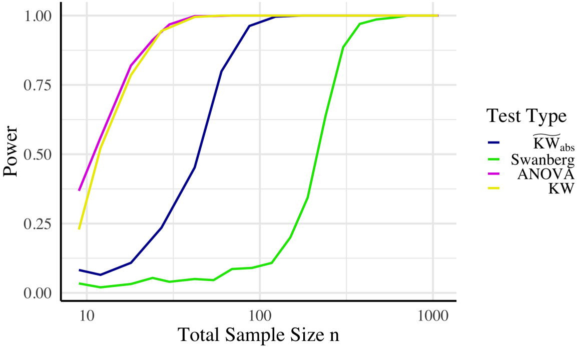


For 80% power, need only 23% as much data as F_1 ([SHGRGB19]) . . .

New Developments [CKSBG19]

Kruskal-Wallis test analogous to F-test

Modified KW test, similar methods as [SHGRGB19]



For 80% power, need only 23% as much data as F_1 ([SHGRGB19]) . . . and about 1-2% as much data as F_2 ([CBRG18])

Thank you