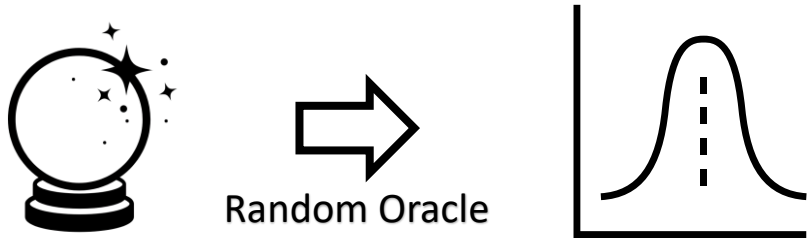
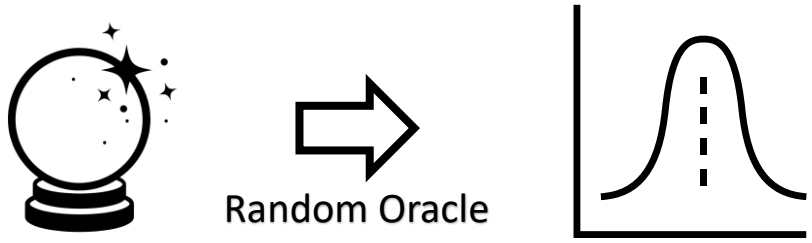
How to Sample a Discrete Gaussian (and more) from a Random Oracle

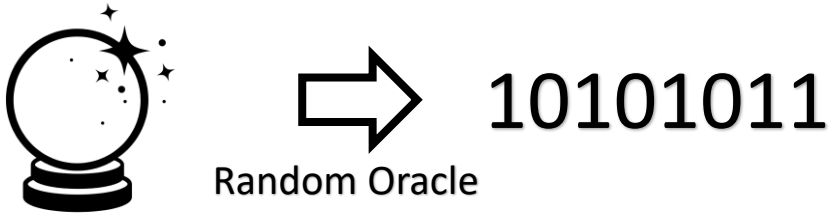
George Lu Brent Waters

Random Oracles to Structured Distributions

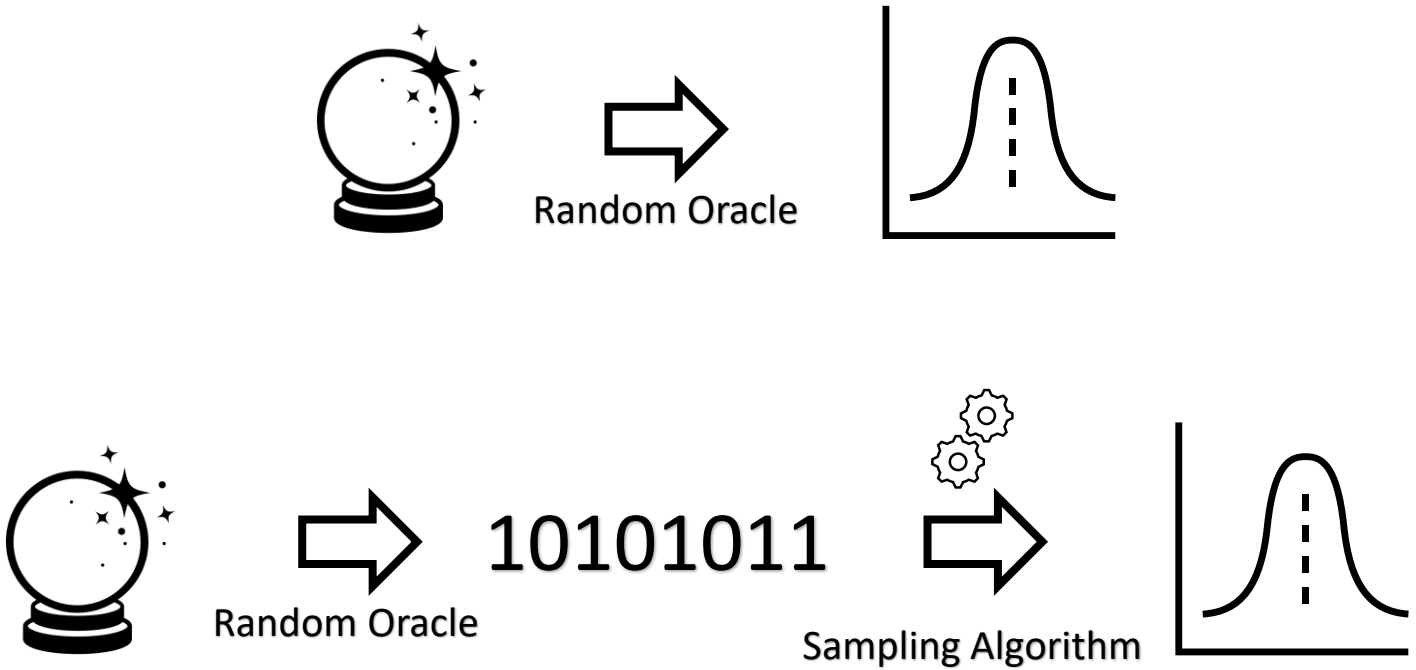


Random Oracles to Structured Distributions

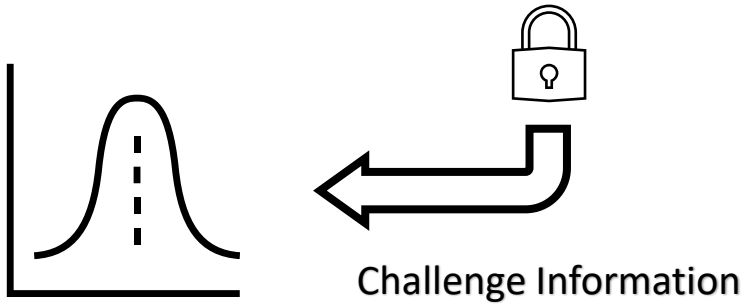




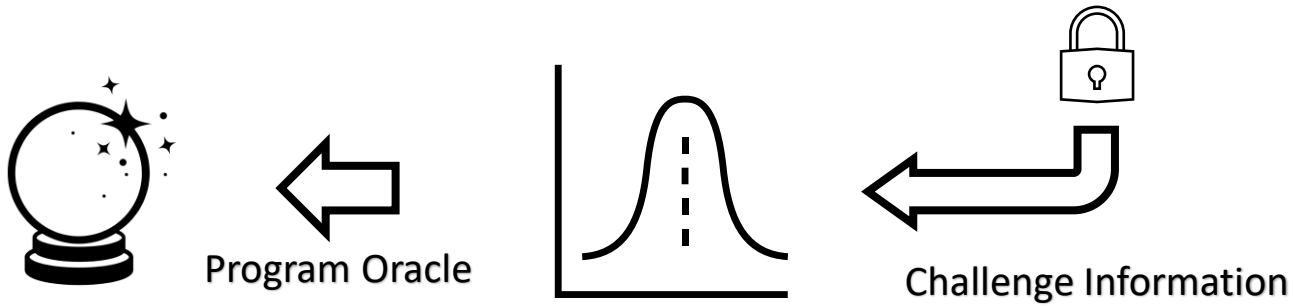
Random Oracles to Structured Distributions



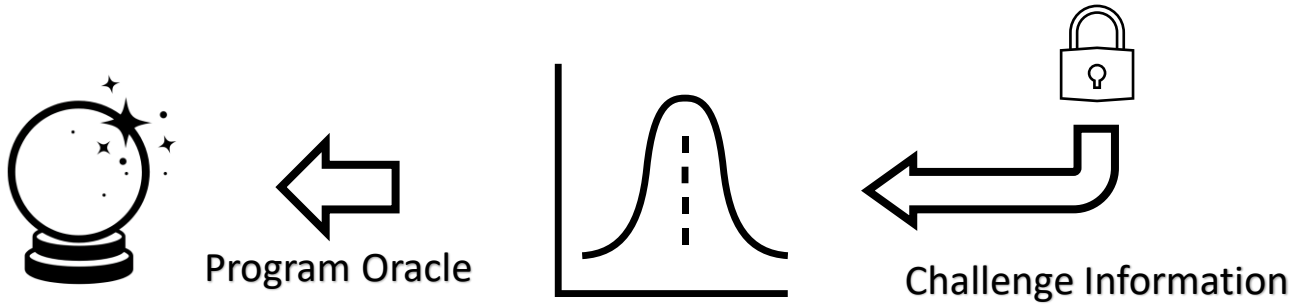
Random Oracles to Structured Distributions

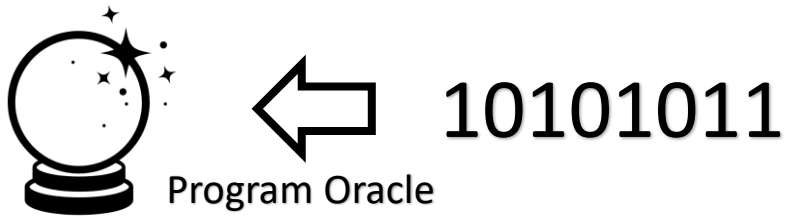


Random Oracles to Structured Distributions

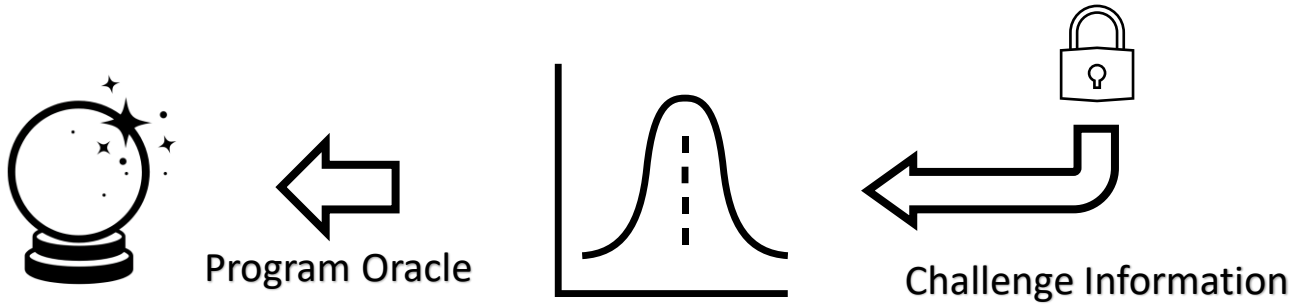


Random Oracles to Structured Distributions

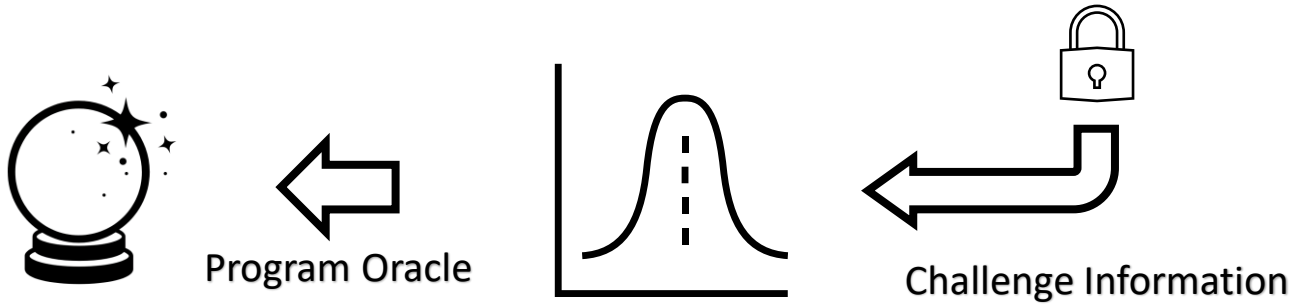


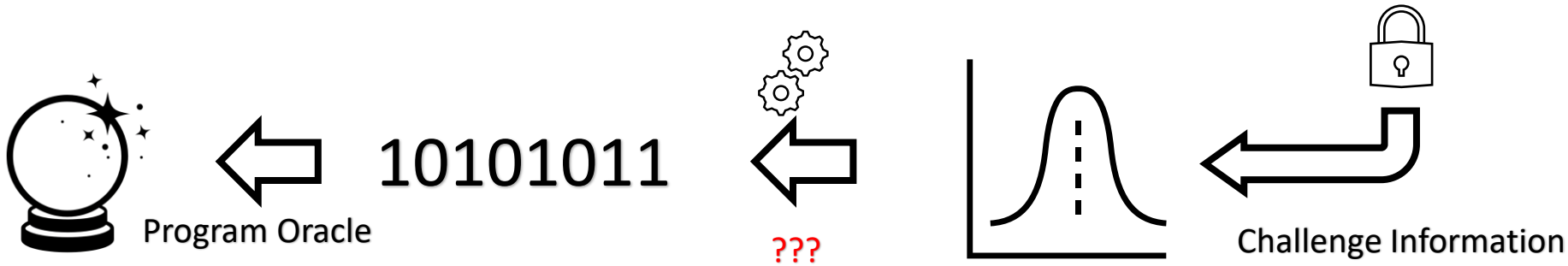


Random Oracles to Structured Distributions



Random Oracles to Structured Distributions





Prior Works

Prior Works

- Random Oracles to Groups
  - RSA Full domain hash
  - Hash-to-Point on Elliptic Curves

Prior Works

- Random Oracles to Groups
  - RSA Full domain hash
  - Hash-to-Point on Elliptic Curves
- Indifferentiability [MRH04]

Prior Works

- Random Oracles to Groups
  - RSA Full domain hash
  - Hash-to-Point on Elliptic Curves
- Indifferentiability [MRH04]
- Universal Samplers [HJKSWZ16]

Lattice-Based Random Oracle Schemes

Lattice-Based Random Oracle Schemes

- Homomorphic ABE [BCTW16]
- Multi-Authority ABE [DKW21]
- Broadcast Encryption* [AWY20]

*uniform random public parameters

Lattice-Based Random Oracle Schemes

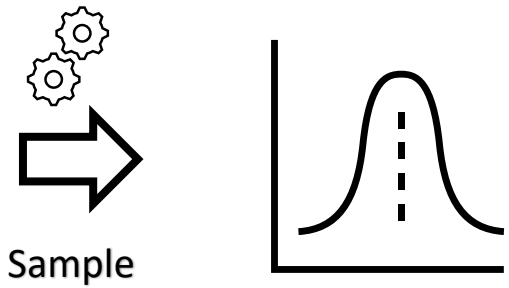
- Homomorphic ABE [BCTW16]
- Multi-Authority ABE [DKW21]
- Broadcast Encryption* [AWY20]

- Ad-hoc workarounds!

*uniform random public parameters

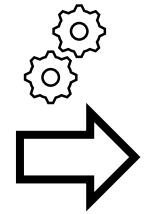
Explainability - Reverse Sampling

10101011

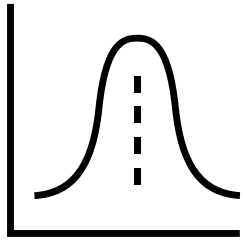


Explainability - Reverse Sampling

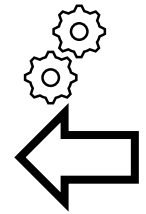
10101011



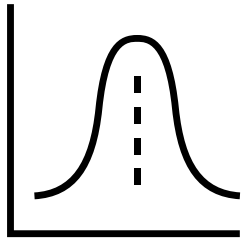
Sample



10101011

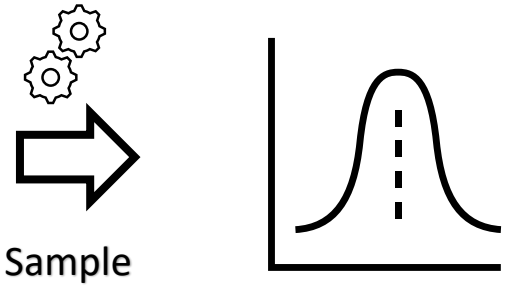


Explain

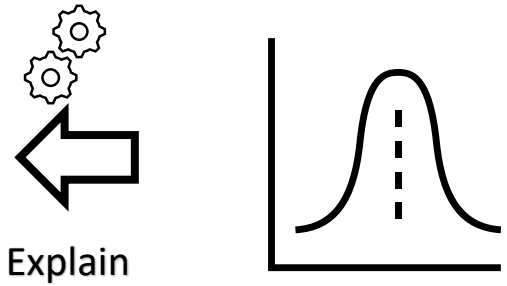


Explainability - Reverse Sampling

10101011



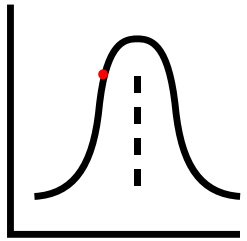
10101011



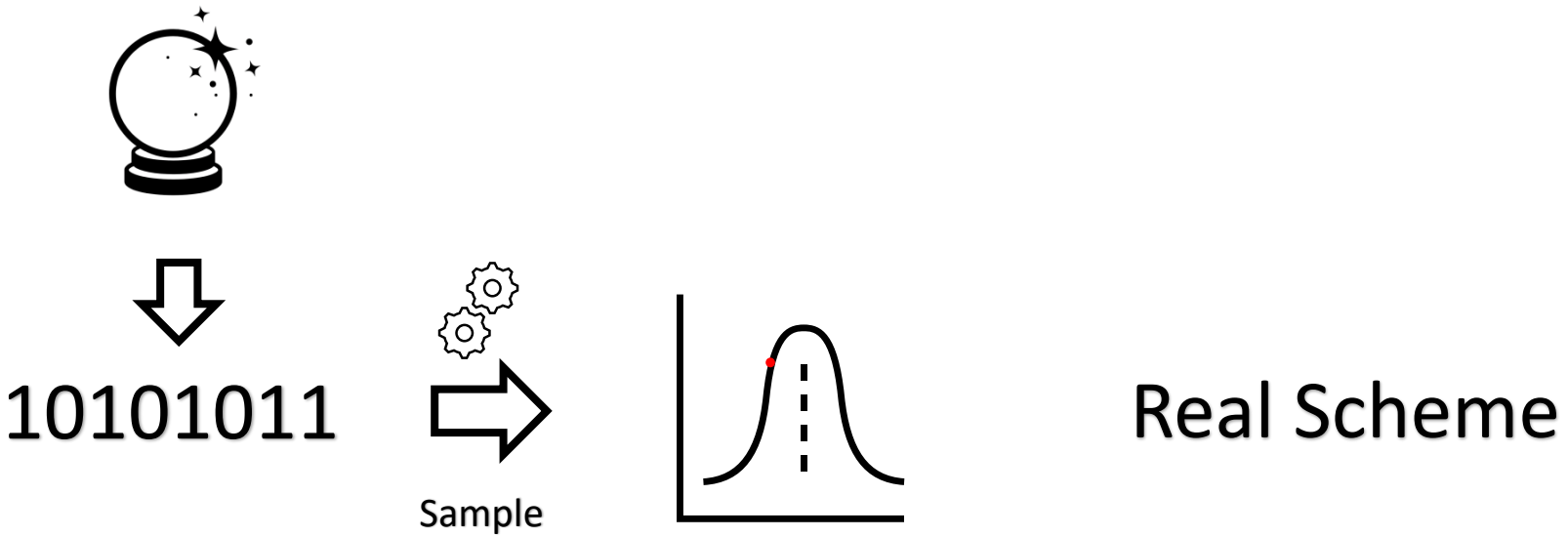
$$\text{Sample}(\text{Explain}(\text{y})) = y$$

Explainability - Reverse Sampling

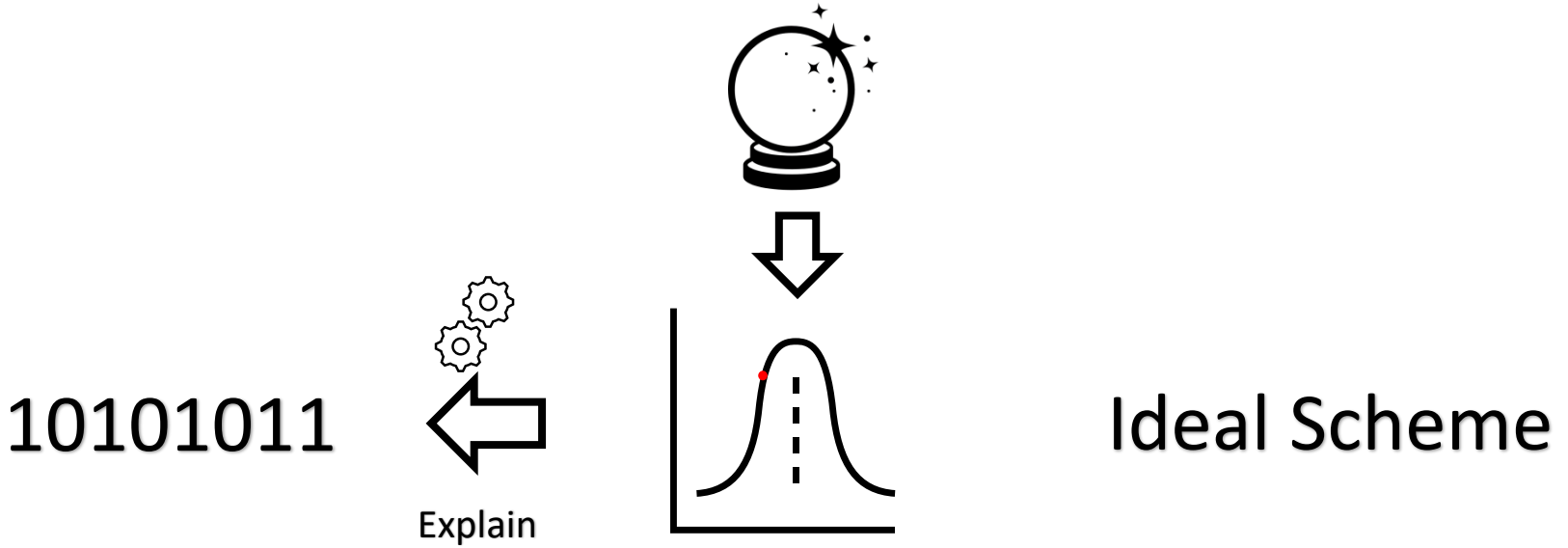
10101011



Explainability - Reverse Sampling



Explainability - Reverse Sampling



Explainability

Distribution 1

$$r \leftarrow \{0,1\}^n$$
$$x \leftarrow \mathsf{Sample}(r)$$

Distribution 2

$$r' \leftarrow \{0,1\}^n$$
$$x \leftarrow \mathsf{Sample}(r')$$
$$r \leftarrow \mathsf{Explain}(1^\kappa, x)$$

Explainability

Distribution 1

$$r \leftarrow \{0,1\}^n$$

$$x \leftarrow \mathsf{Sample}(r)$$

$$(r, x)$$

Distribution 2

$$r' \leftarrow \{0,1\}^n$$

$$x \leftarrow \mathsf{Sample}(r')$$

$$r \leftarrow \mathsf{Explain}(1^\kappa, x)$$

$$(r, x)$$

Explainability

Distribution 1

$$r \leftarrow \{0,1\}^n$$
$$x \leftarrow \mathsf{Sample}(r)$$

Distribution 2

$$r' \leftarrow \{0,1\}^n$$
$$x \leftarrow \mathsf{Sample}(r')$$
$$r \leftarrow \mathsf{Explain}(1^\kappa, x)$$

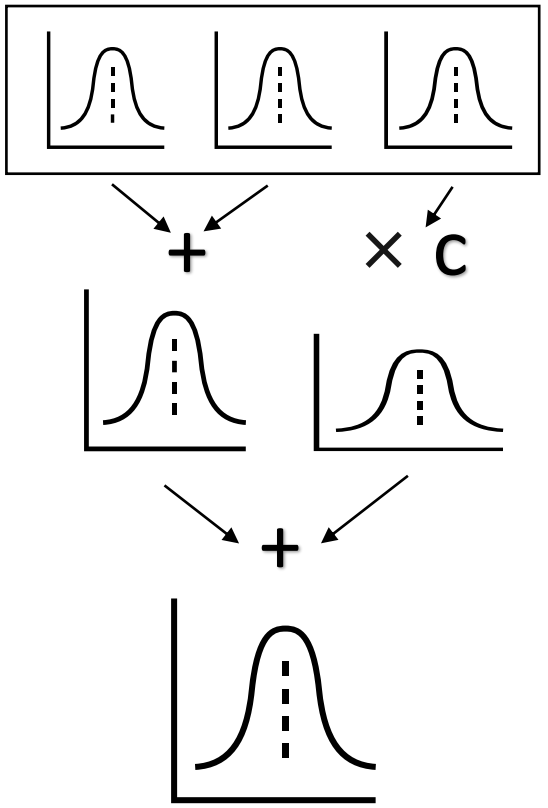
$$(r, x) \approx_{\frac{1}{\kappa}} (r, x)$$

Statistical Distance

Result 1

Explaining the Miccancio-Walter ’17 Discrete Gaussian Sampler

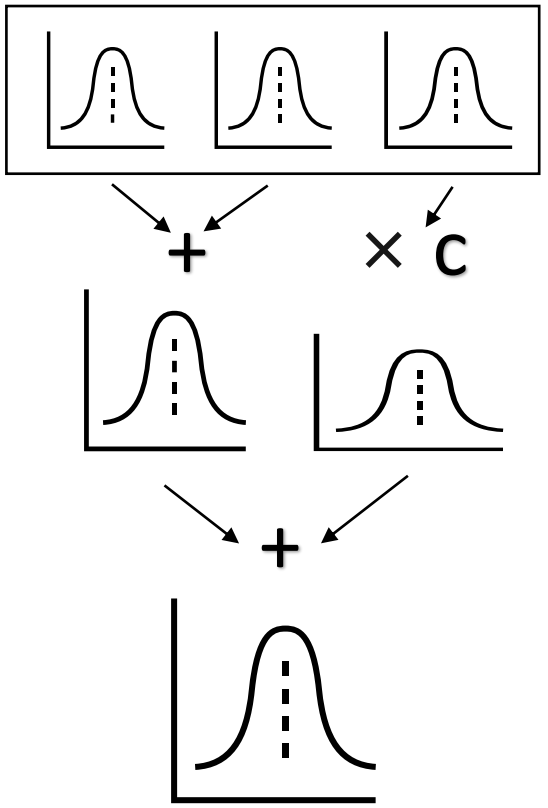
Miccancio-Walter ‘17 Sampler



Offline Phase – Generate ‘Small’ Discrete Gaussian Sample

Online Phase – Combine linear combinations of Small Samples based on μ, σ

Miccancio-Walter ‘17 Sampler

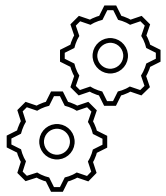


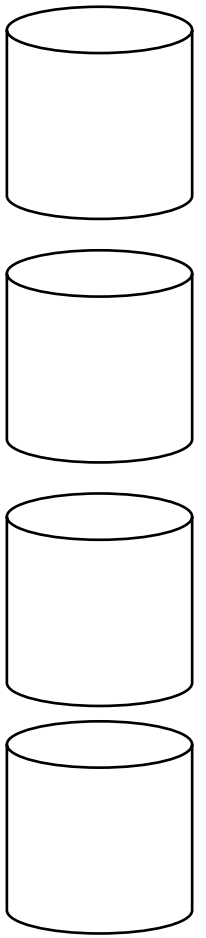
<u>Offline Phase – Generate ‘Small’ Discrete Gaussian Sample</u>

Online Phase – Combine linear combinations of Small Samples based on μ, σ

Explaining Polynomial Range Samplers

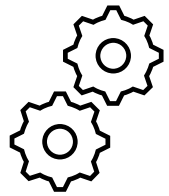
$$\mathsf{Explain}(y) \rightarrow \mathsf{Sample}(r)$$

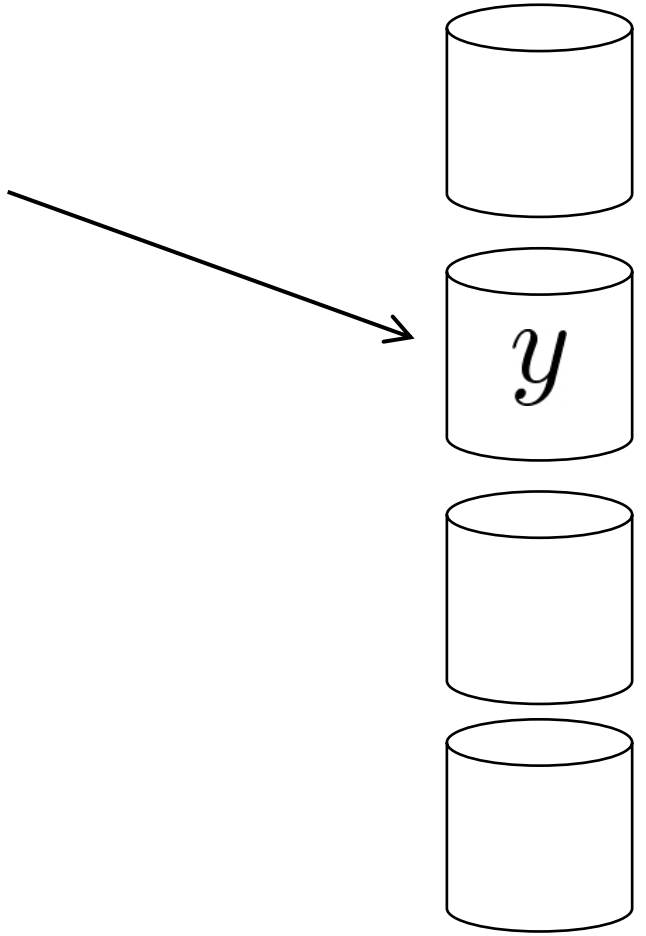




Explaining Polynomial Range Samplers

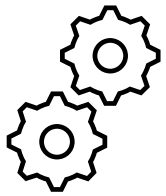
$\mathsf{Explain}(y) \rightarrow \mathsf{Sample}(r)$

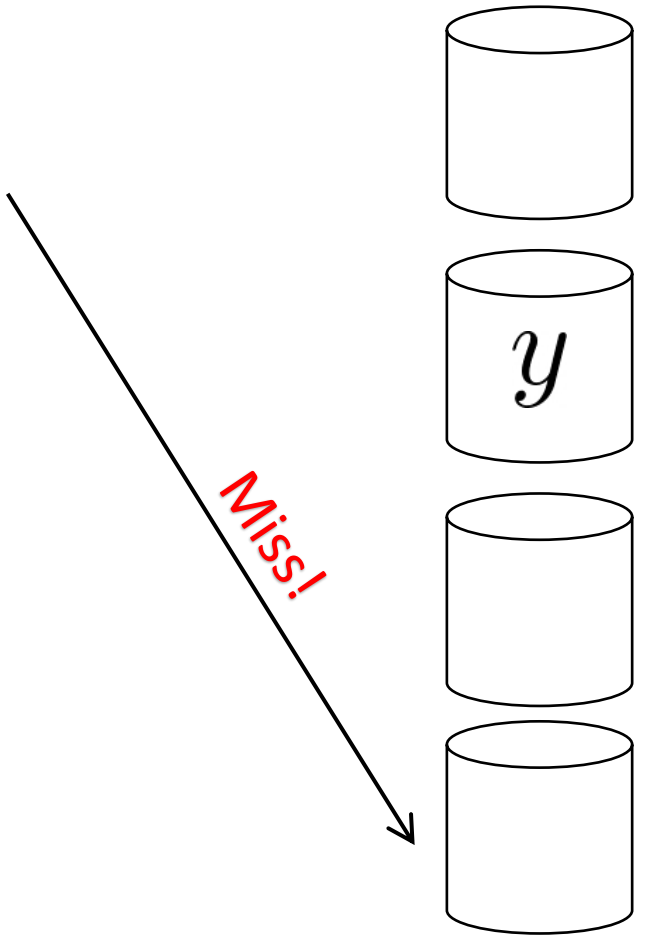




Explaining Polynomial Range Samplers

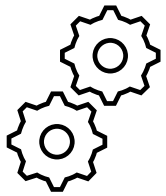
$\mathsf{Explain}(y) \rightarrow \mathsf{Sample}(r_0)$

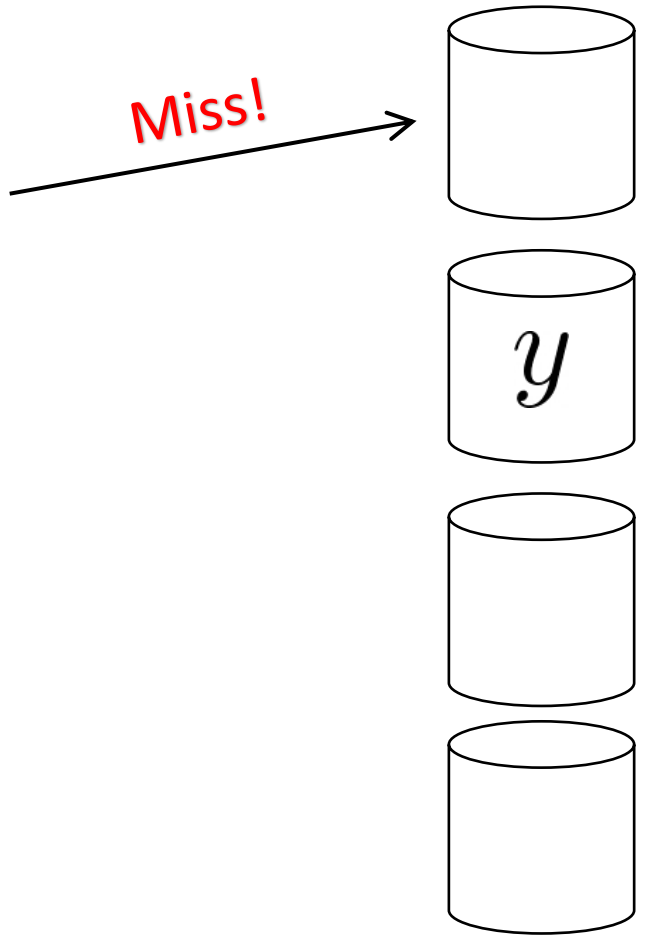




Explaining Polynomial Range Samplers

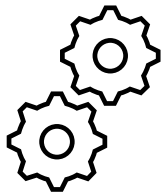
$\mathsf{Explain}(y) \rightarrow \mathsf{Sample}(r_1)$

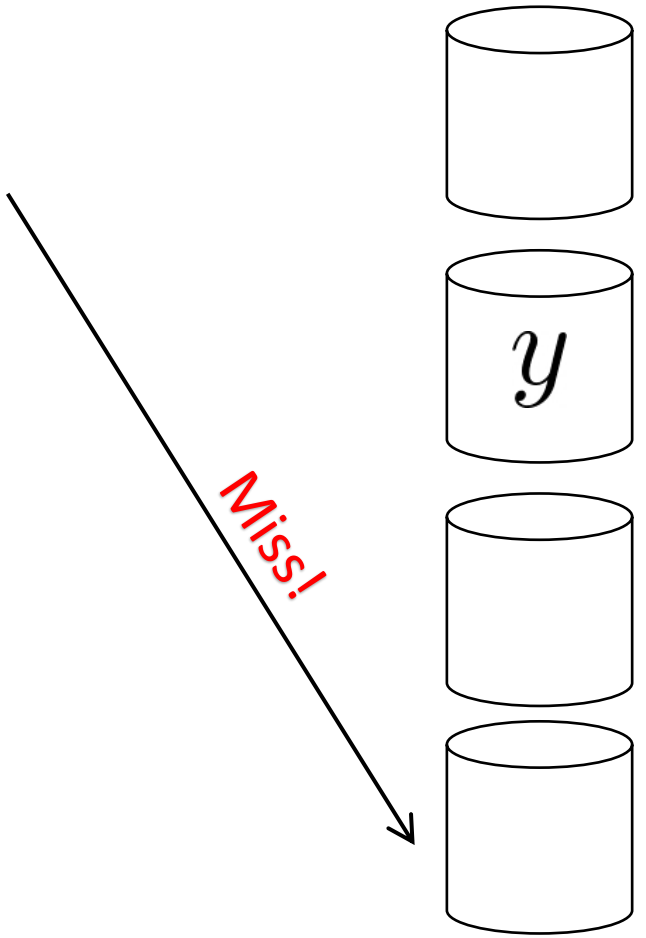




Explaining Polynomial Range Samplers

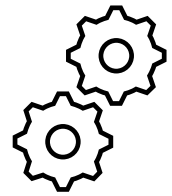
$\mathsf{Explain}(y) \rightarrow \mathsf{Sample}(r_2)$

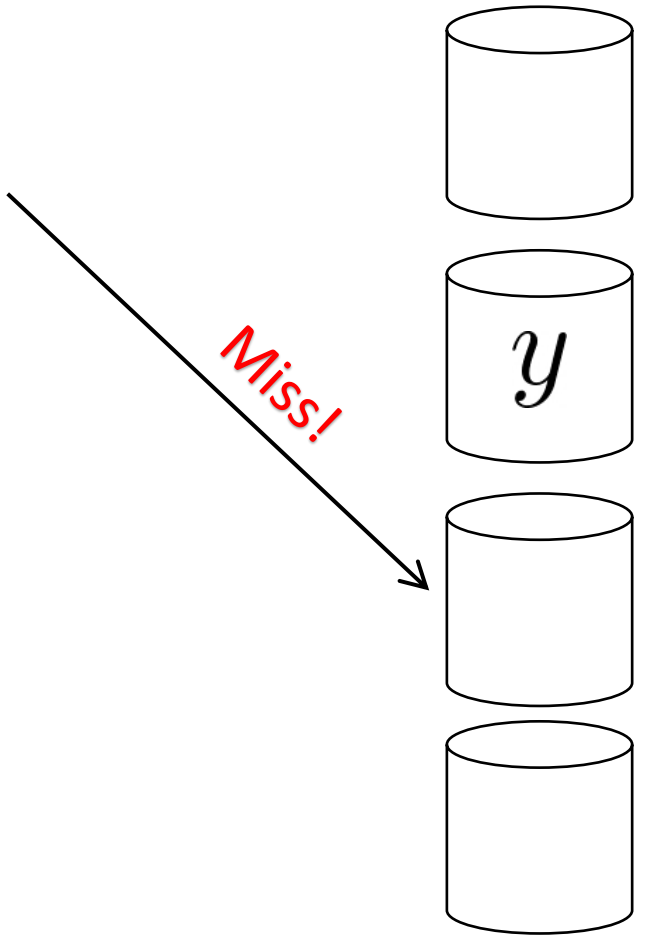




Explaining Polynomial Range Samplers

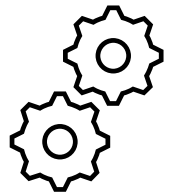
$\mathsf{Explain}(y) \rightarrow \mathsf{Sample}(r_3)$

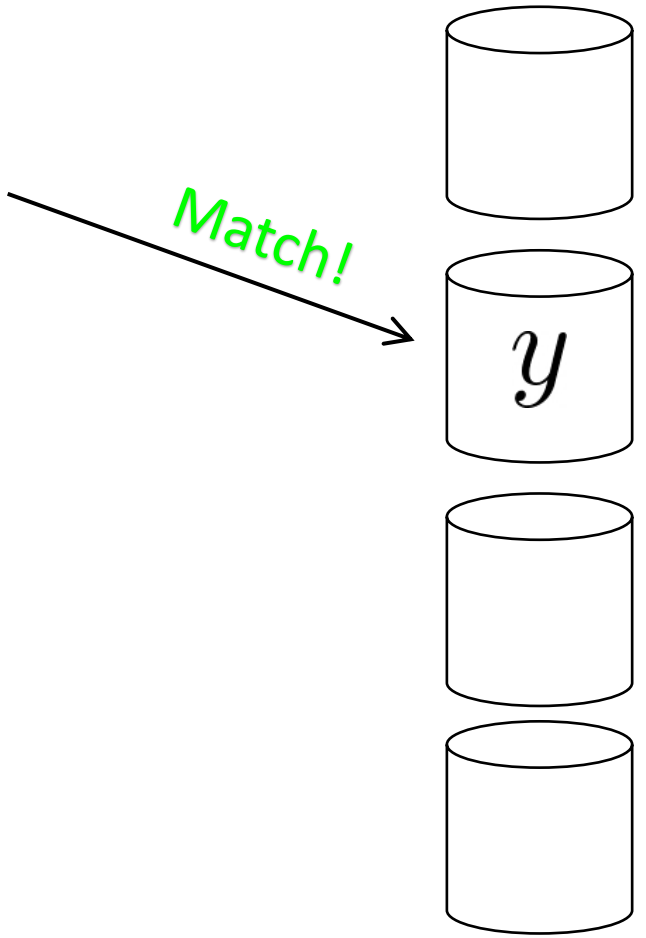




Explaining Polynomial Range Samplers

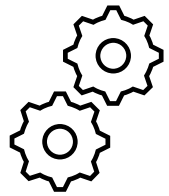
$\mathsf{Explain}(y) \rightarrow \mathsf{Sample}(r_4)$

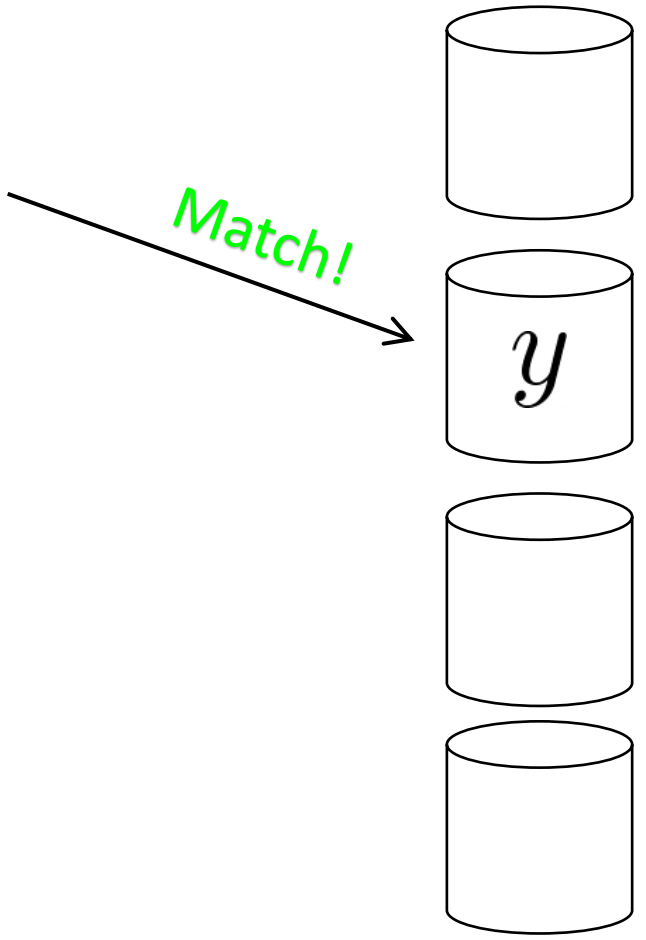




Explaining Polynomial Range Samplers

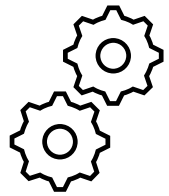
$\mathsf{Explain}(y) \rightarrow \mathsf{Sample}(\underline{r_4})$

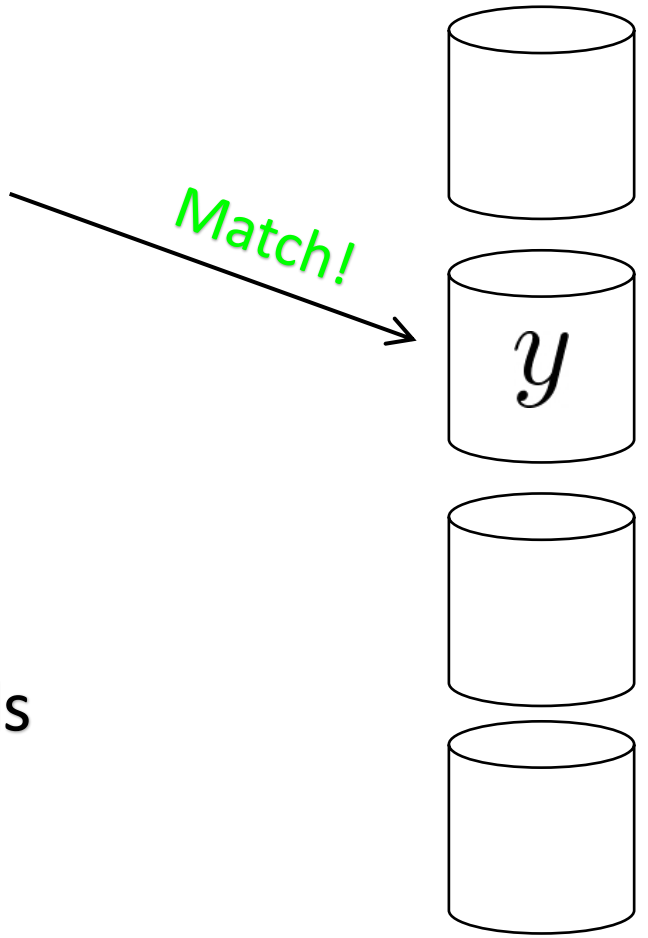




Explaining Polynomial Range Samplers

$\mathsf{Explain}(y) \rightarrow \mathsf{Sample}(\underline{r_4})$





$\kappa \cdot (|range(\mathsf{Sample}(\cdot))| - 1)$ Trials

Result 2

Generic Explainability through Heavy Element Samplers

Result 2

- Encompasses a wide range of mathematical distributions
  - Gaussian
  - Geometric
  - Gamma
  - Poisson
  - Any distribution with monotonic[+] probability density

    …
- Converts non-explainable sampler to explainable one

[+]or decomposable into polynomially many monotonic intervals

Explaining Larger Range Distributions

Explaining Larger Range Distributions

- Sampling Function

  SampleOld(r)

Explaining Larger Range Distributions

- Sampling Function
  SampleOld(r)

Any DG Sampler – ex: MW17

Explaining Larger Range Distributions

- Sampling Function

  SampleOld(r)

- Probability Density function

  PDF(y)

  - Output *proportional* to probability of occurring

Any DG Sampler – ex: MW17

Explaining Larger Range Distributions

- Sampling Function

  SampleOld(r)

- Probability Density function

  PDF(y)

  - Output *proportional* to probability of occurring

Any DG Sampler – ex: MW17

$$e^{-\frac{(x-\mu)^2}{2\sigma^2}}$$

Explaining Larger Range Distributions

- Sampling Function

  SampleOld(r)

- Probability Density function

  PDF(y)

  - Output *proportional* to probability of occurring

- Heavy Element Sampler

  $\{\text{SampleUniform}(p, r), \text{ExplainUniform}(1^\kappa, p, r)\}$

  - Samples uniform element above probability density threshold p
  - Explainable

Any DG Sampler – ex: MW17

$$e^{-\frac{(x-\mu)^2}{2\sigma^2}}$$

Explaining Larger Range Distributions

- Sampling Function

  SampleOld(r)

- Probability Density function

  PDF(y)

  - Output *proportional* to probability of occurring

- Heavy Element Sampler

  $\{\text{SampleUniform}(p, r), \text{ExplainUniform}(1^\kappa, p, r)\}$

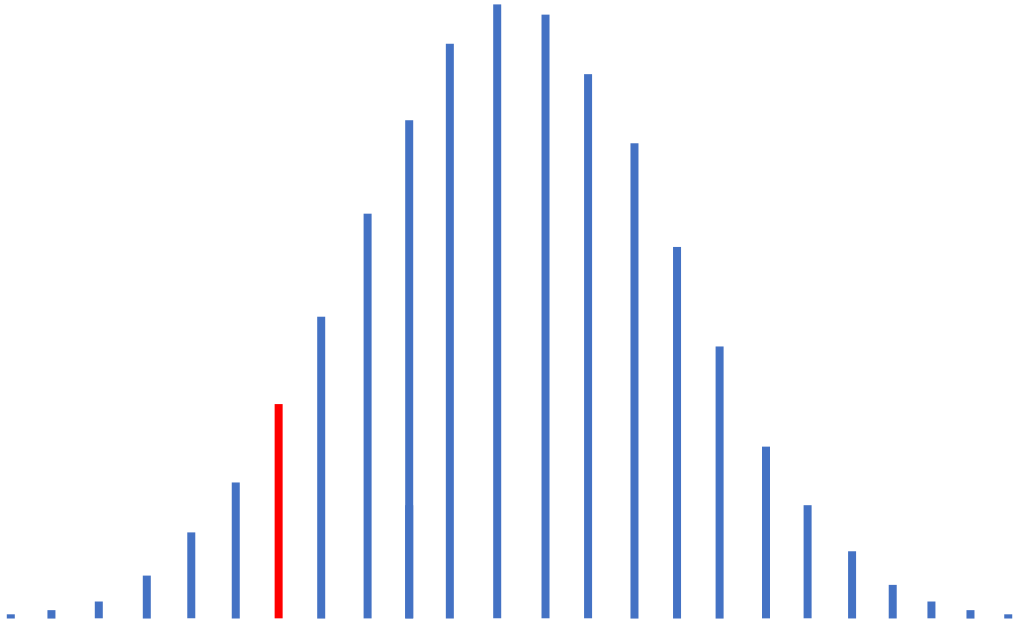
  - Samples uniform element above probability density threshold p
  - Explainable

Any DG Sampler – ex: MW17

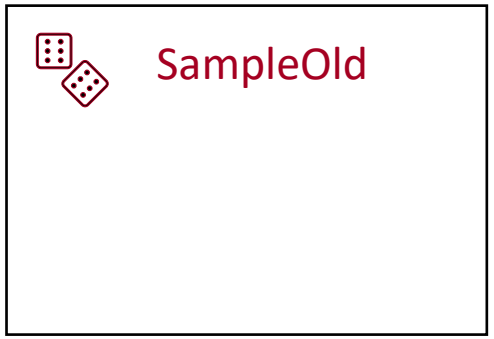
$$e^{-\frac{(x-\mu)^2}{2\sigma^2}}$$

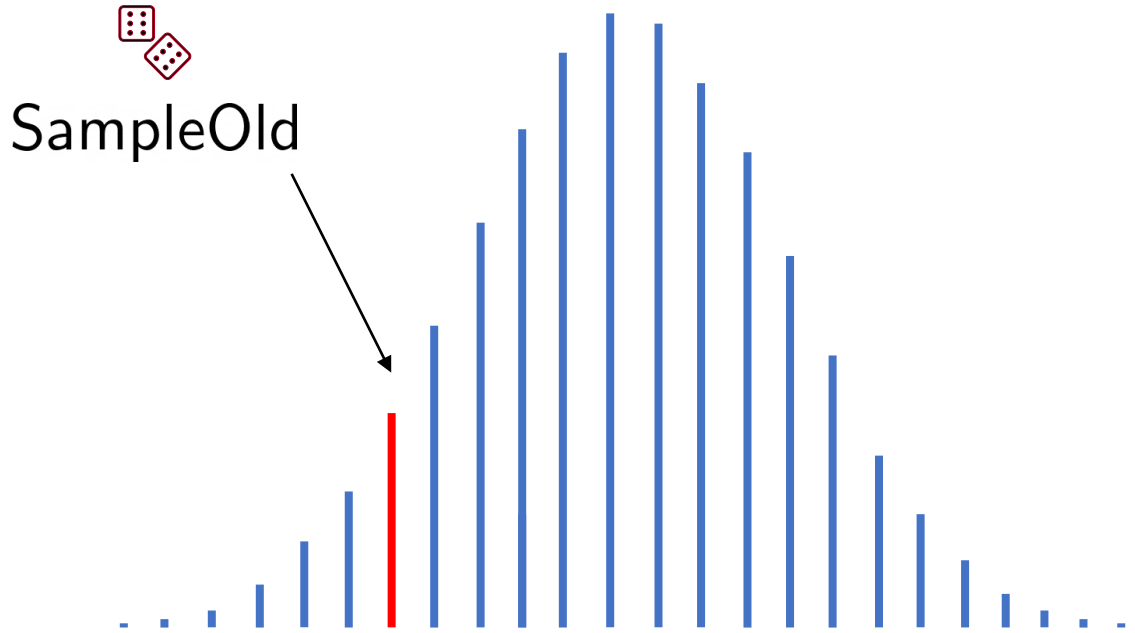
$$\left[\mu - \sqrt{-2\sigma^2 \ln p}, \mu + \sqrt{-2\sigma^2 \ln p}\right]$$

Large Range Sampler



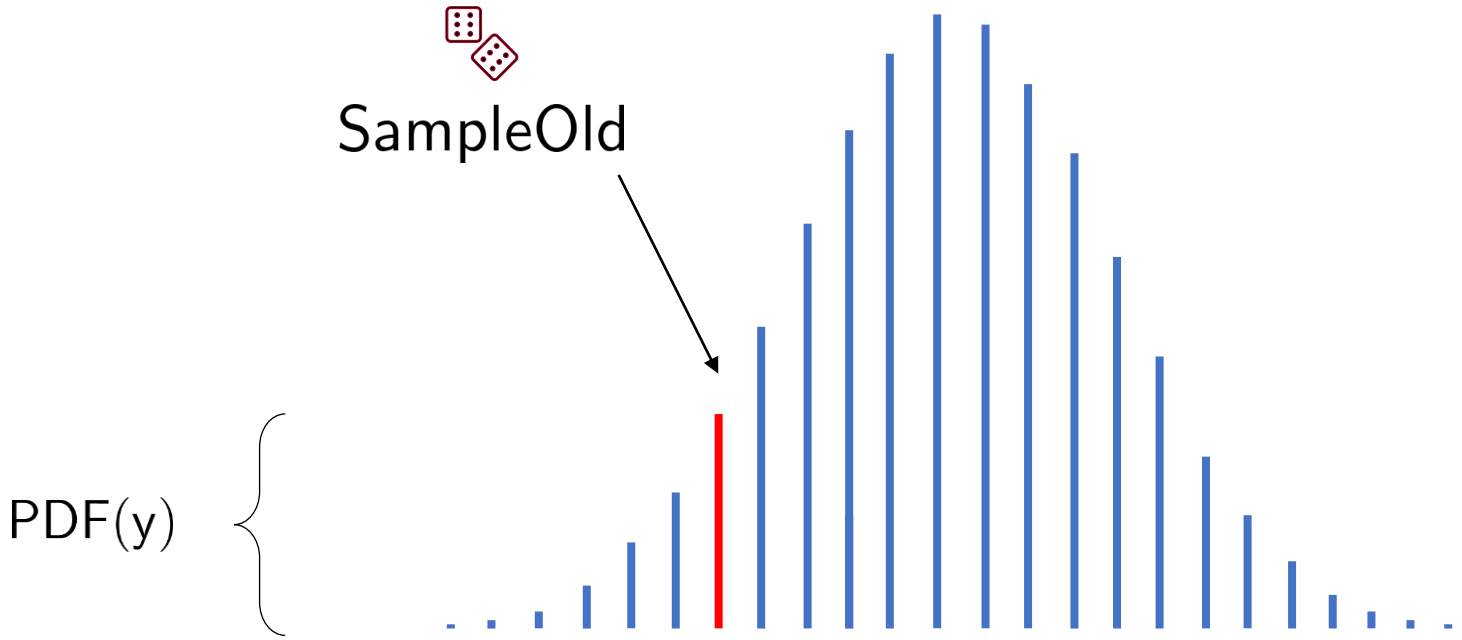
Large Range Sampler





Large Range Sampler

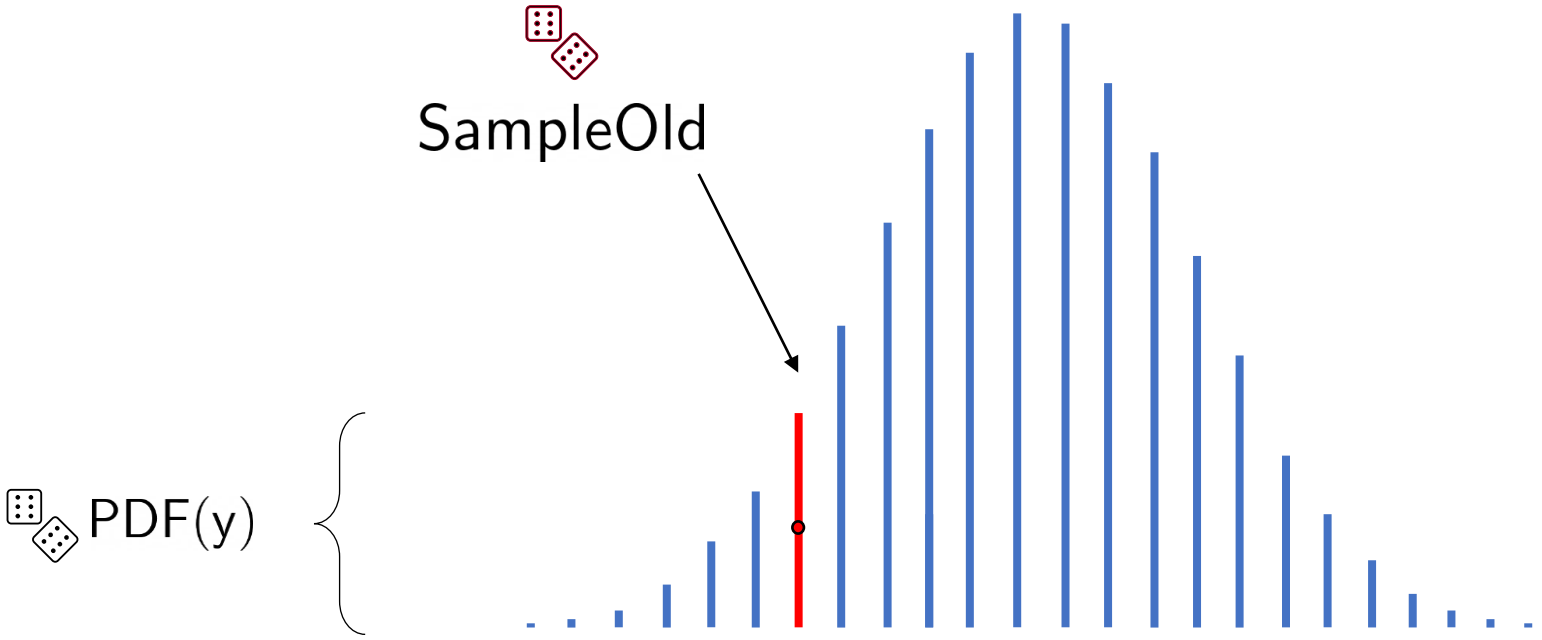
SampleOld



Large Range Sampler

SampleOld

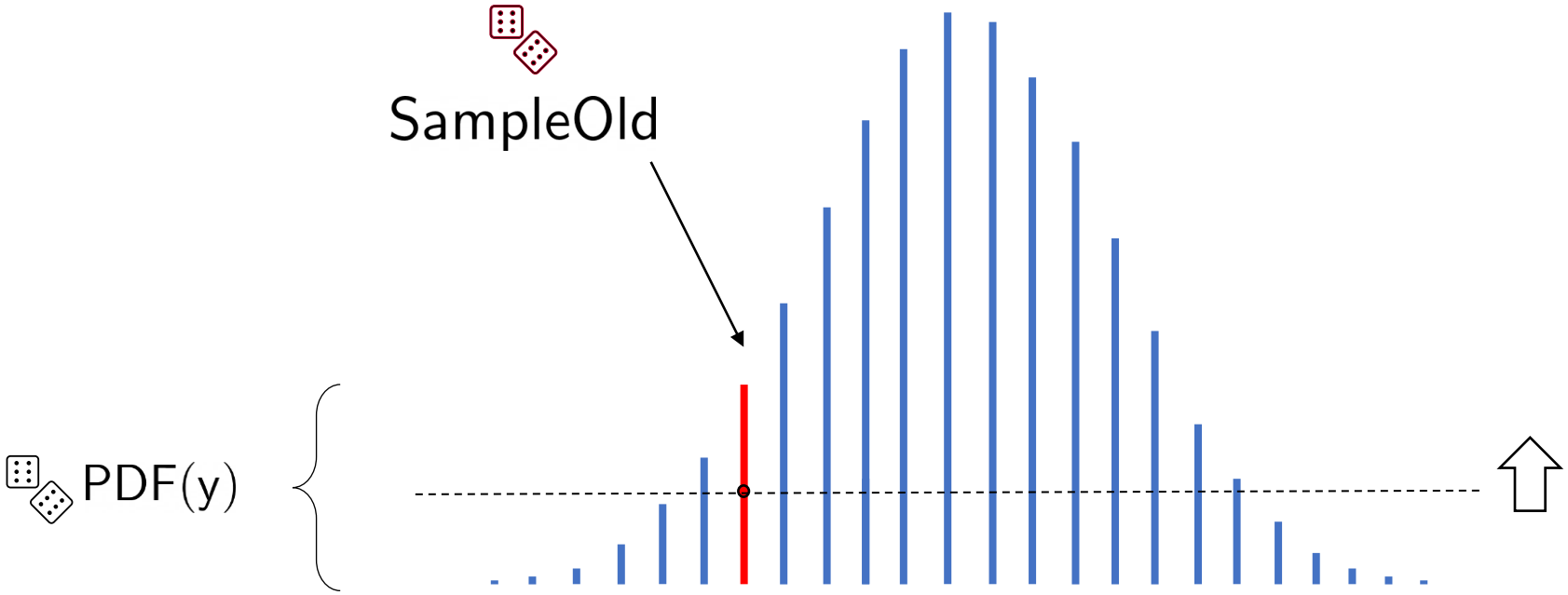
Threshold p



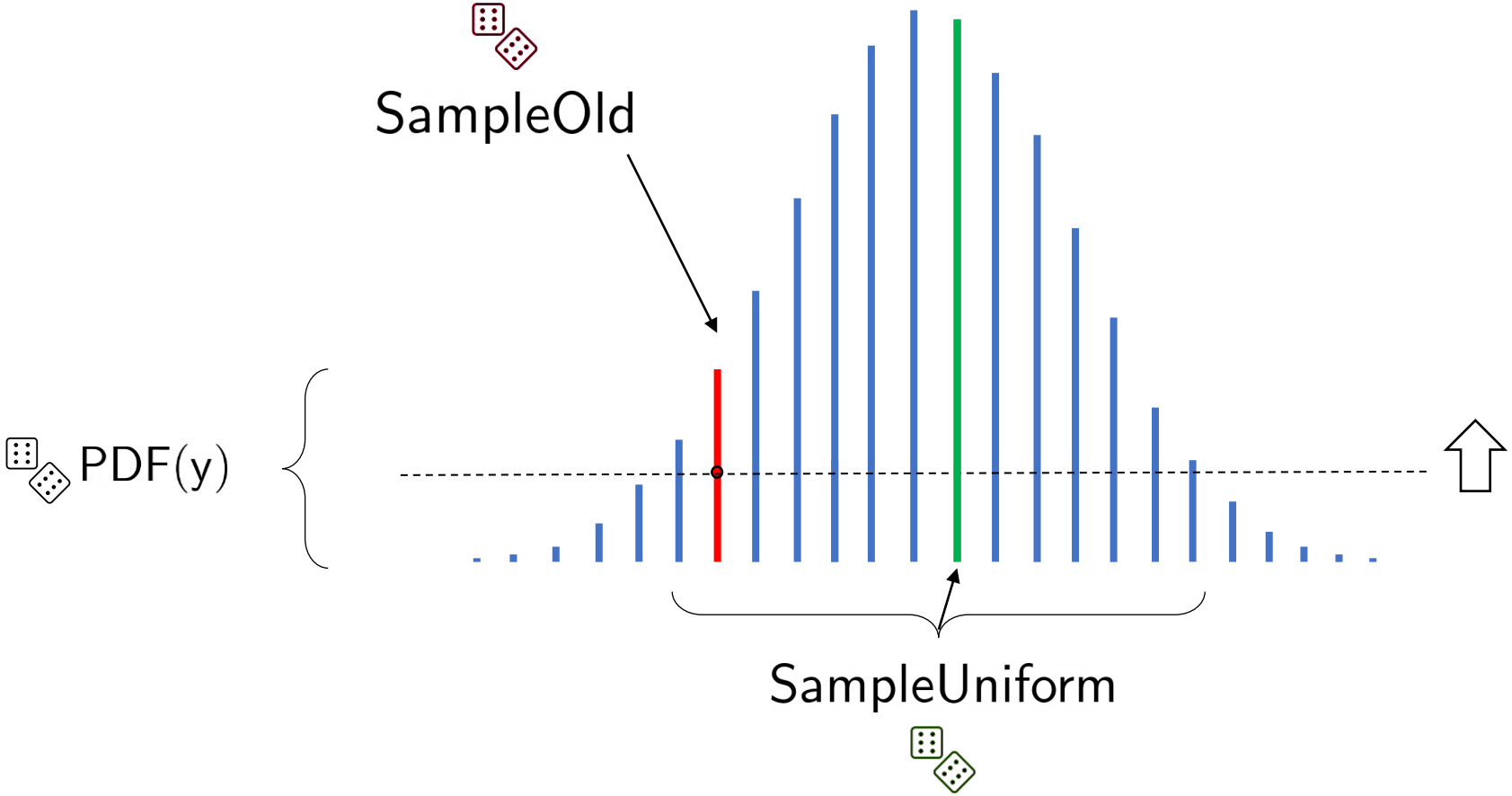
Large Range Sampler

SampleOld

Threshold p



Large Range Sampler

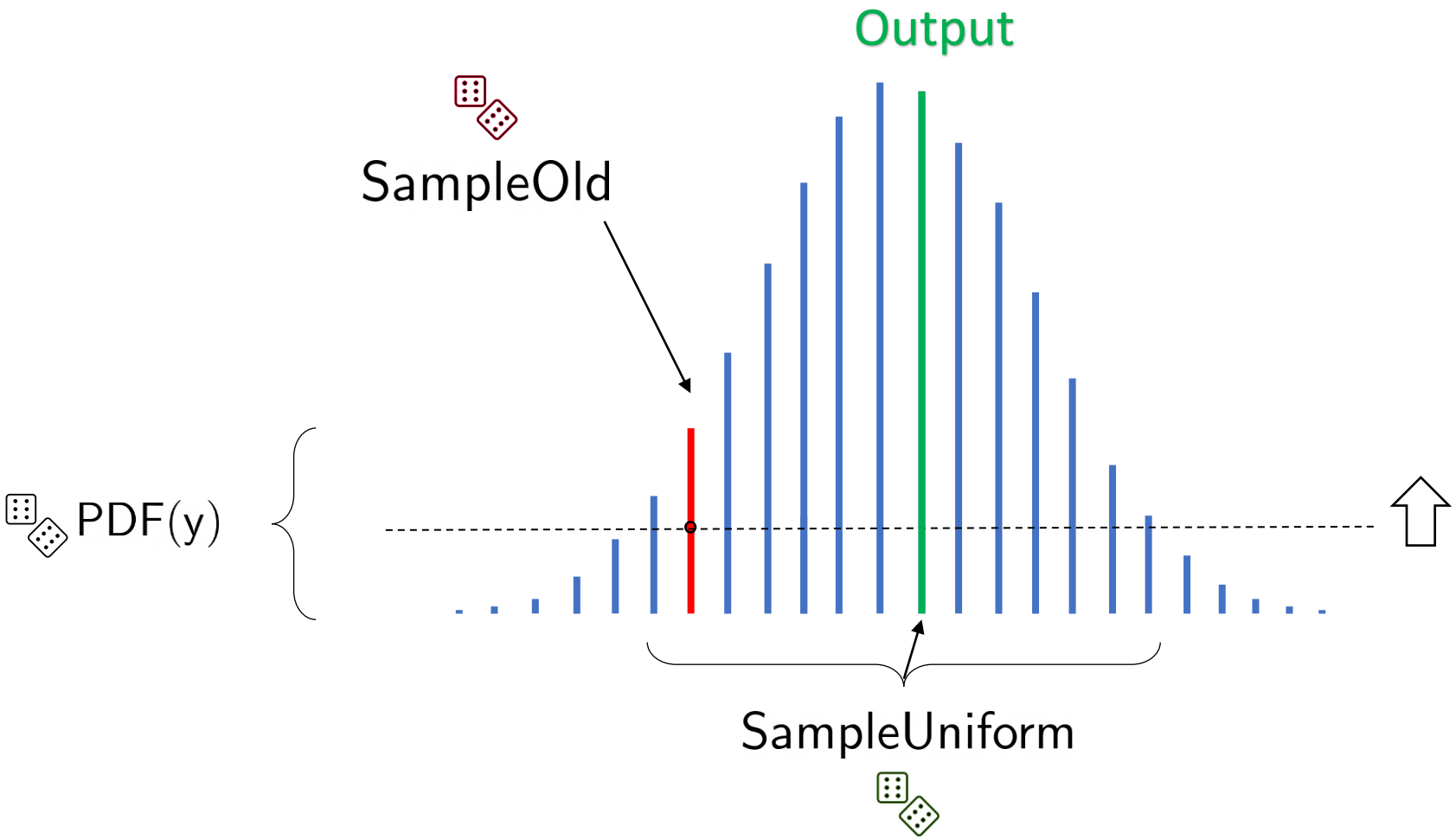


SampleOld

Threshold p

SampleUniform

Large Range Sampler

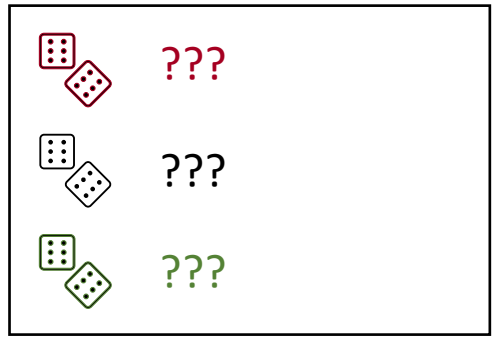


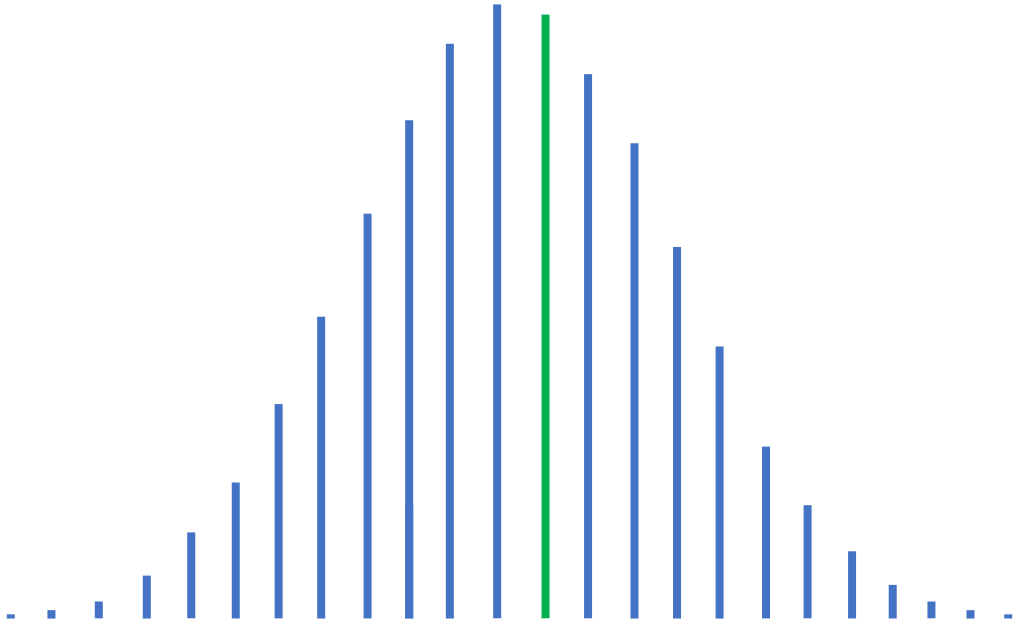
SampleOld

Threshold p

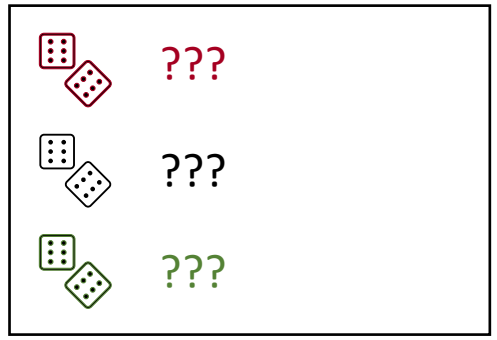
SampleUniform

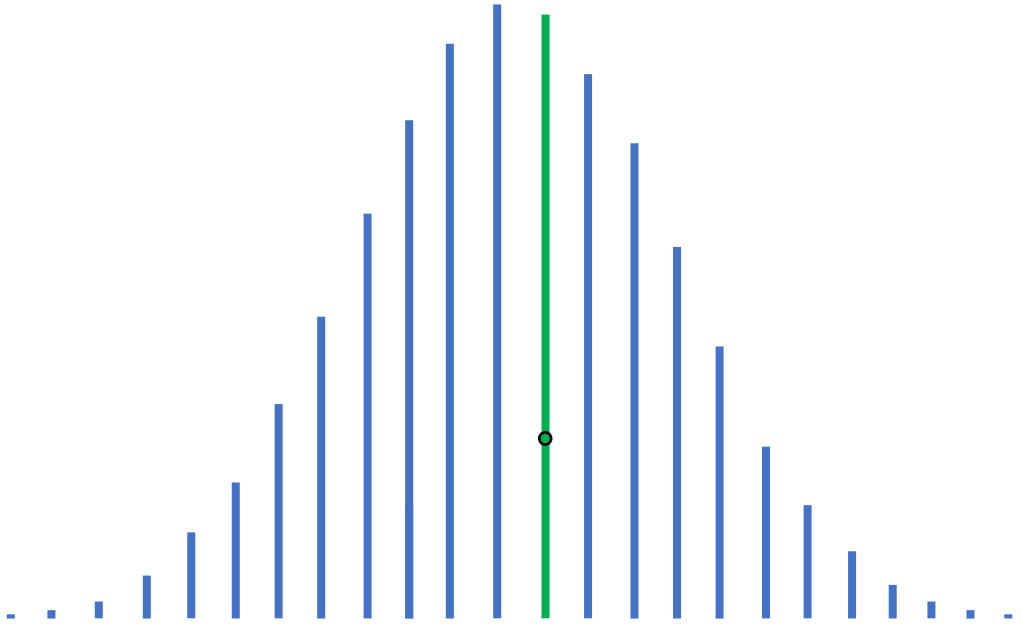
Large Range Explainer



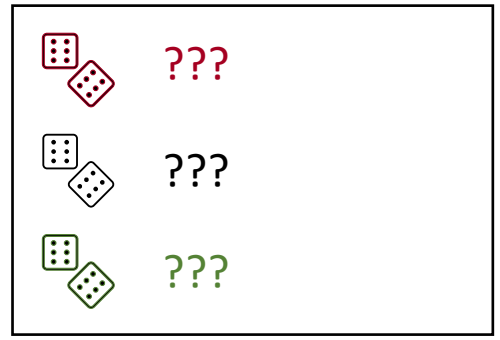


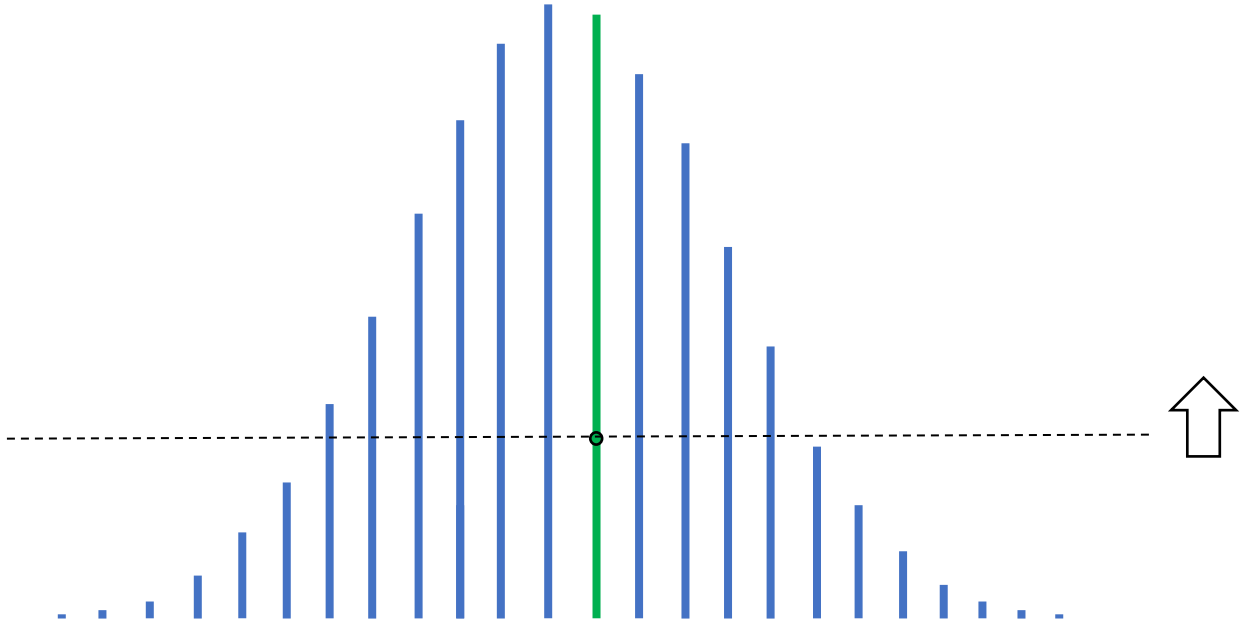
Large Range Explainer



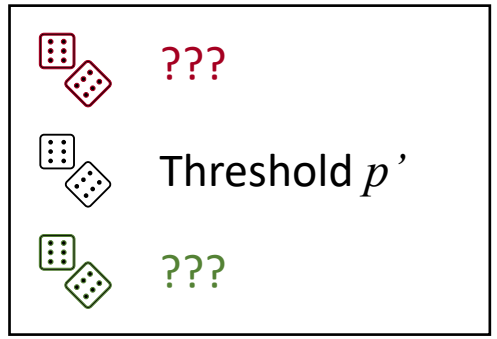


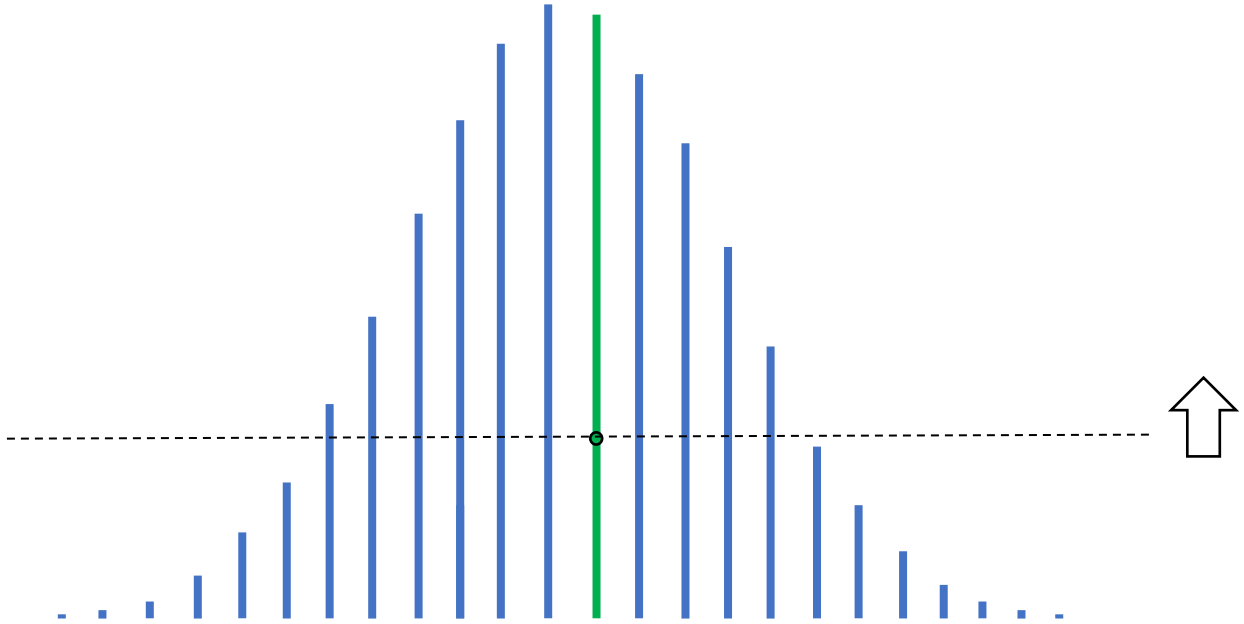
Large Range Explainer



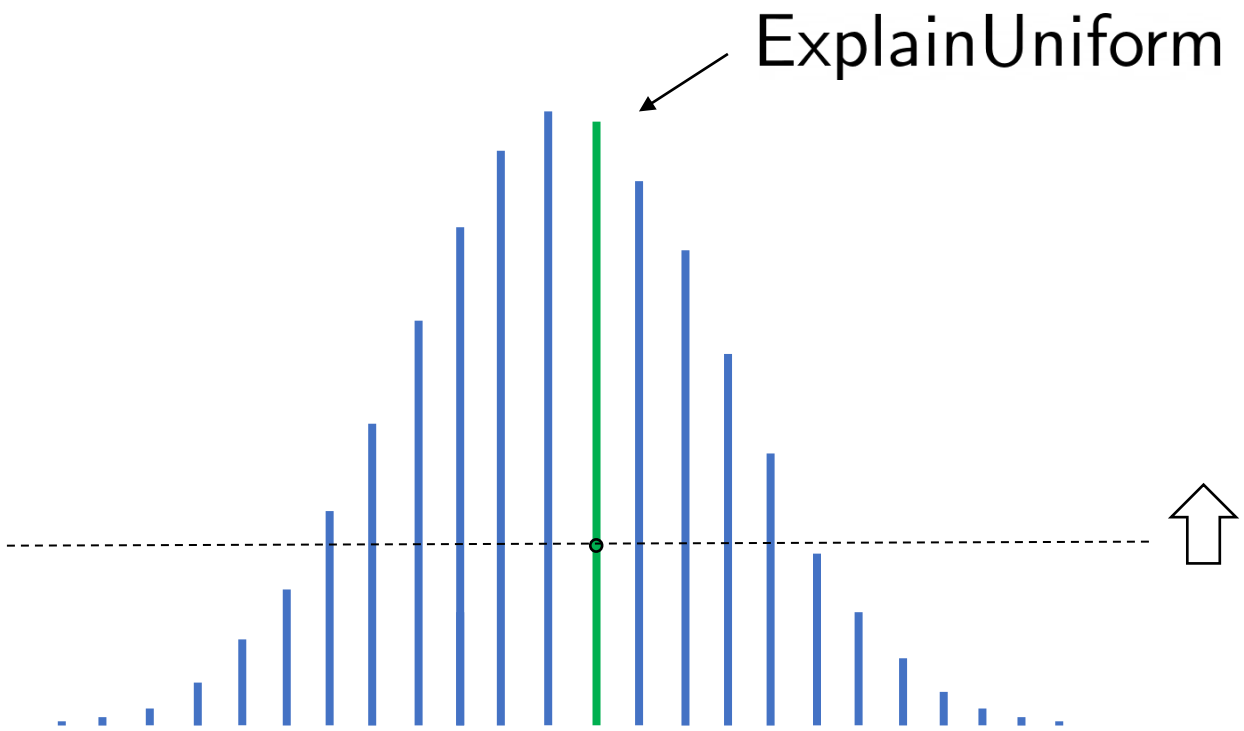


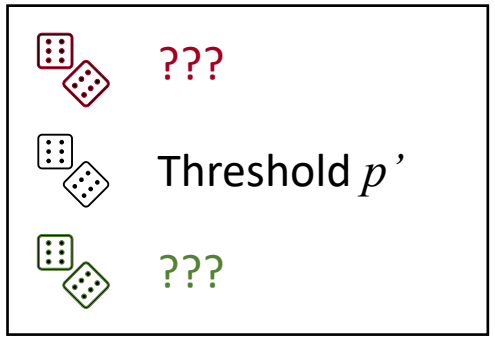
Large Range Explainer



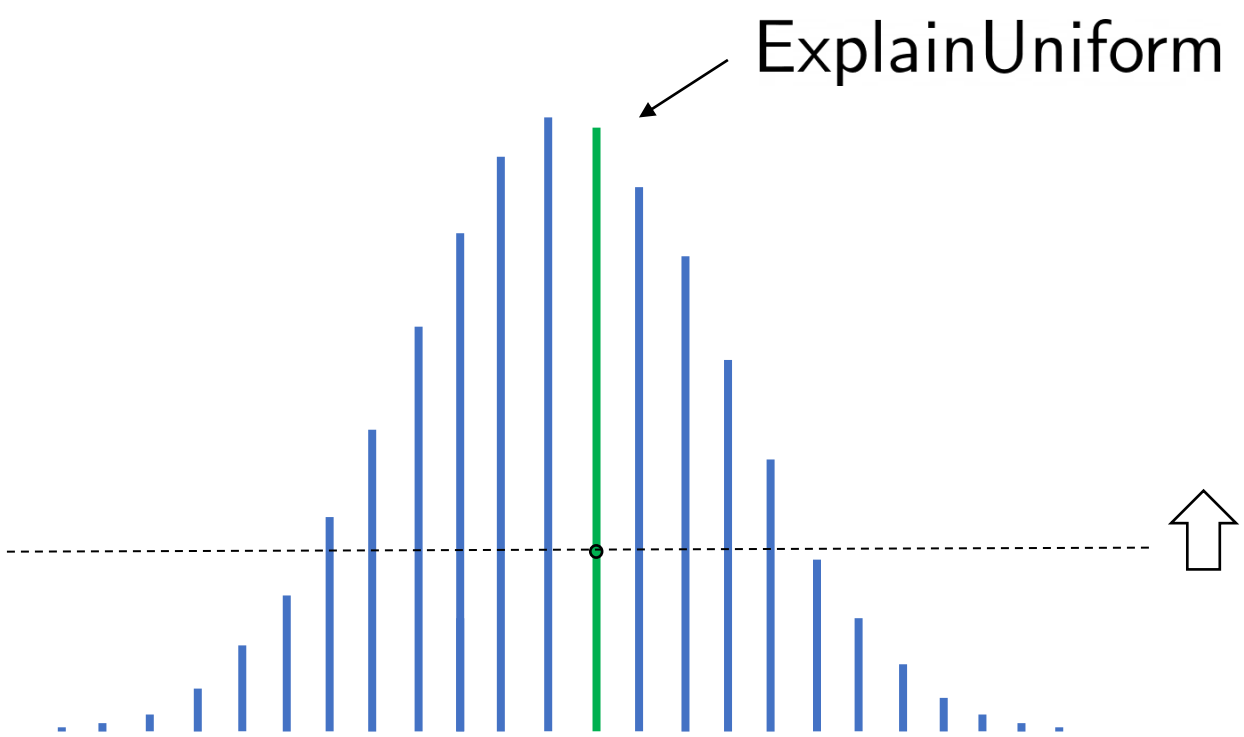


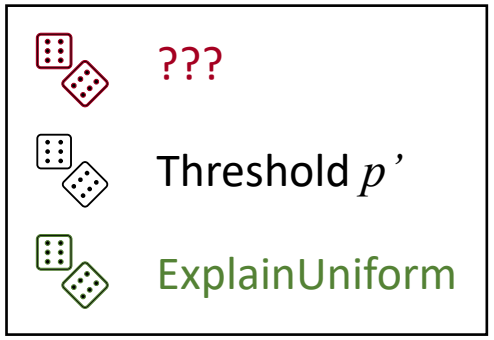
Large Range Explainer



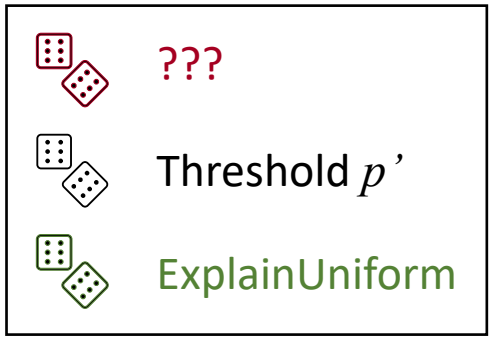


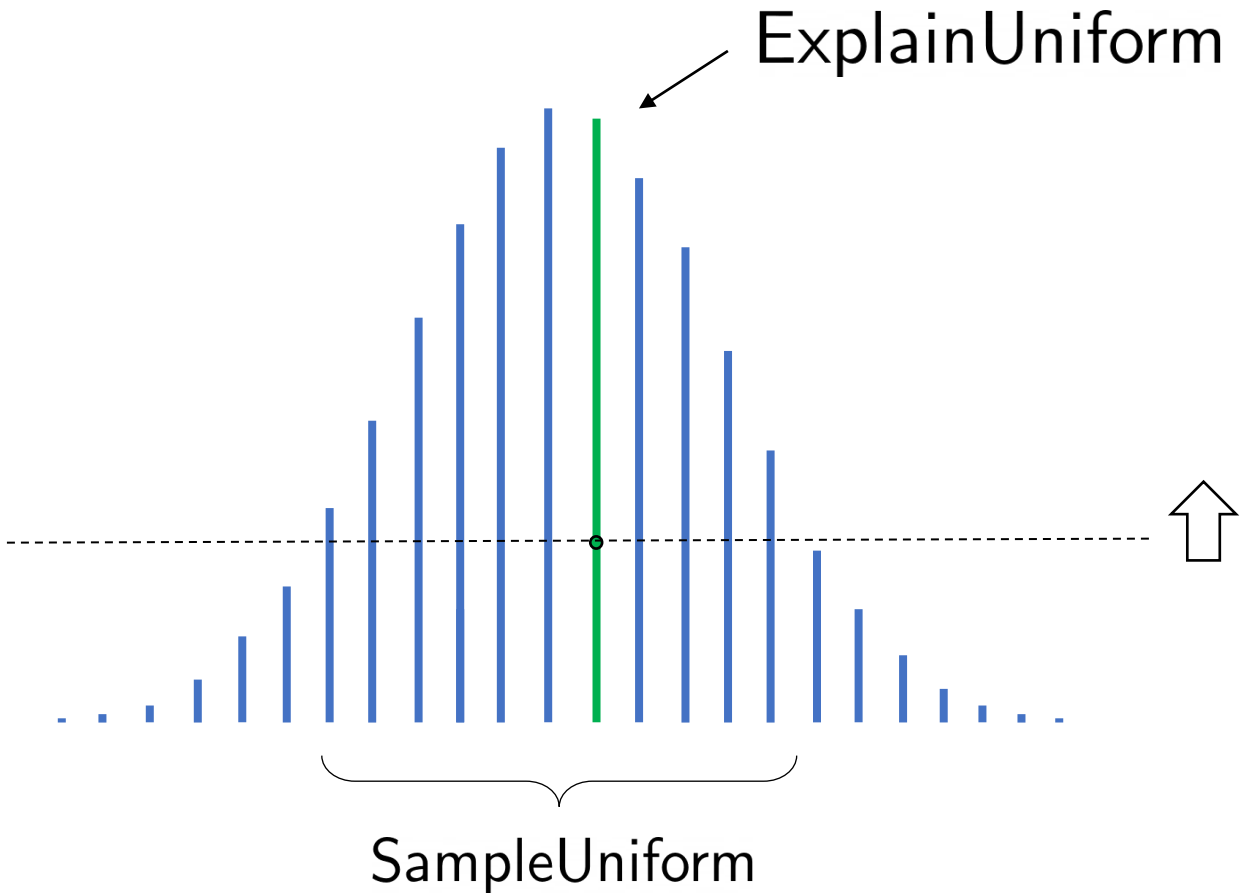
Large Range Explainer



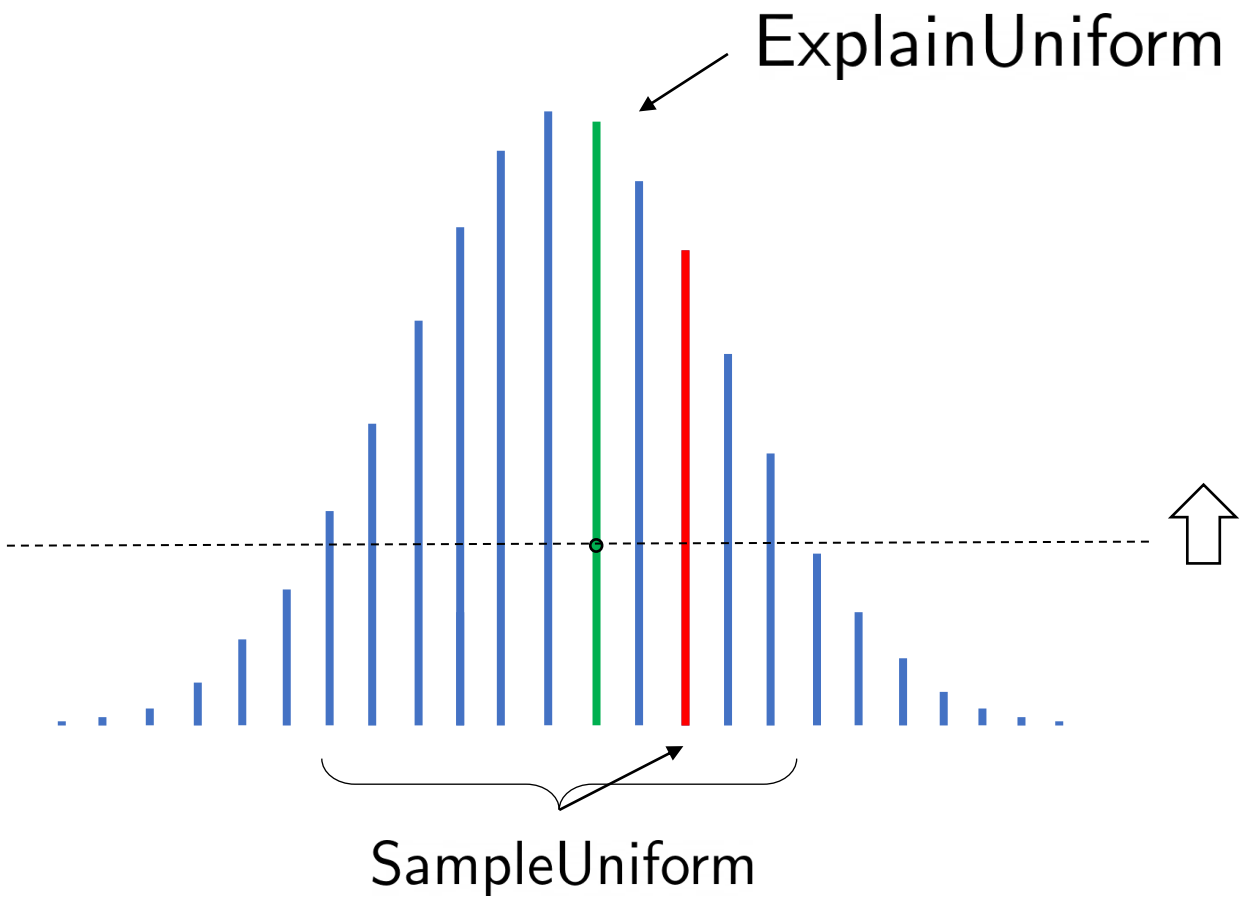


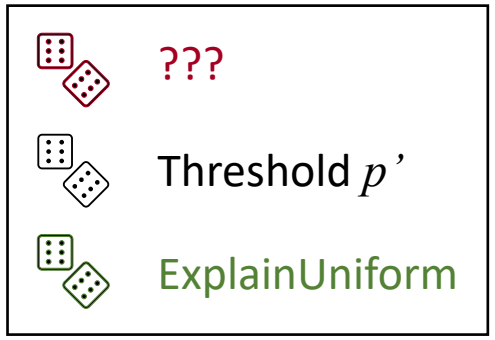
Large Range Explainer



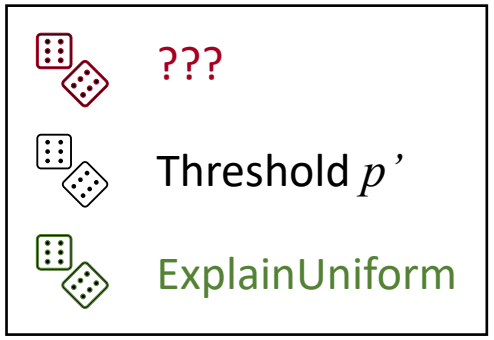


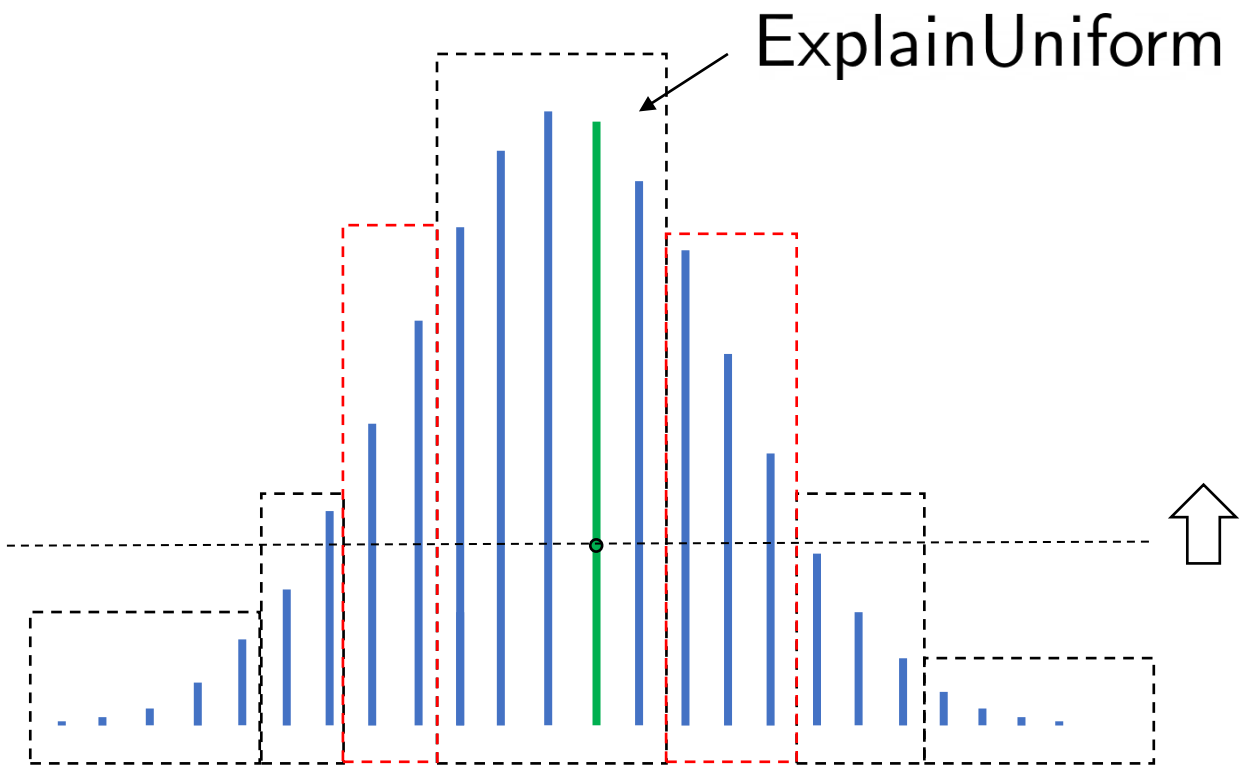
Large Range Explainer



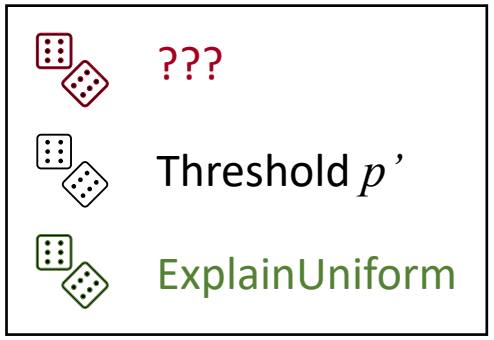


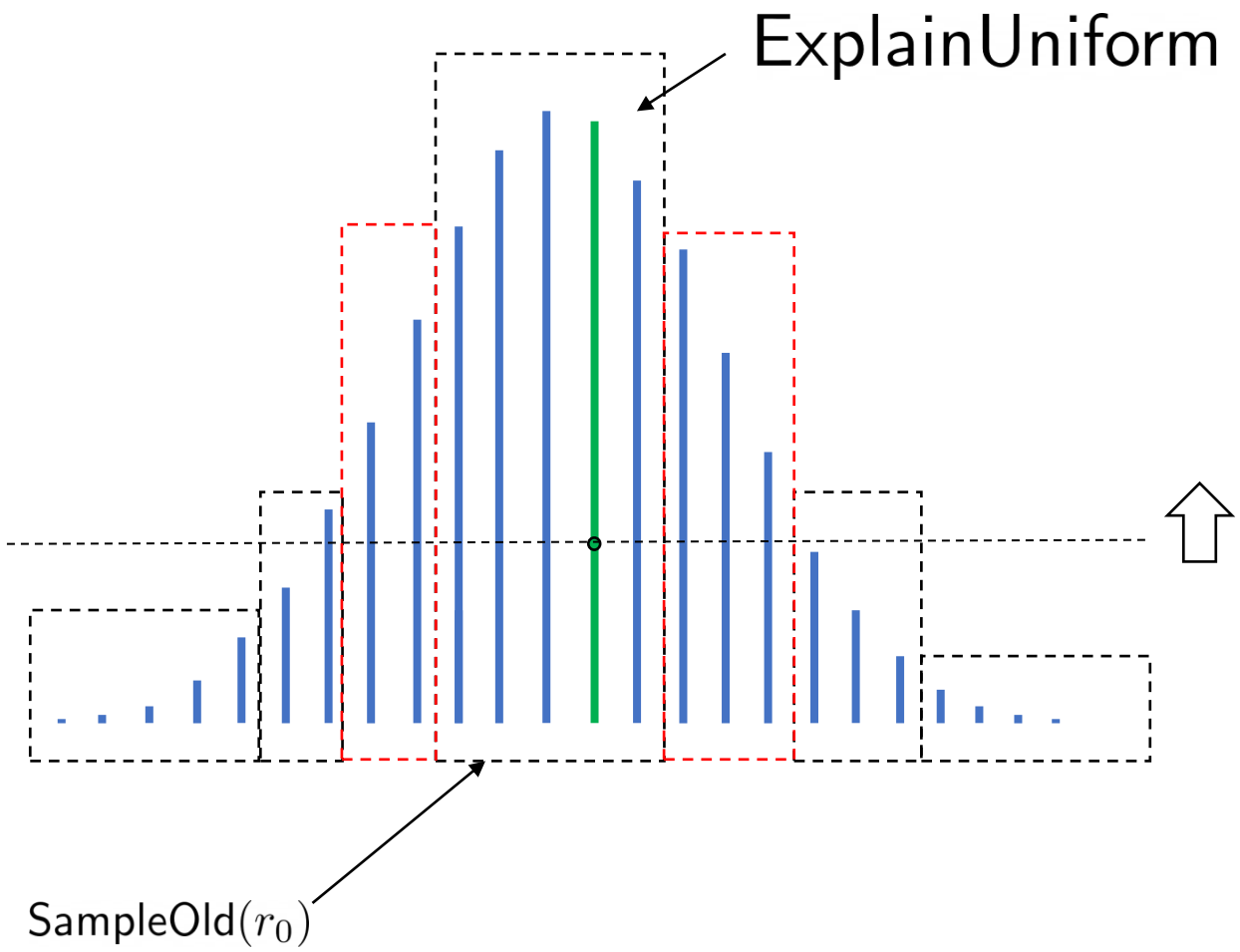
Large Range Explainer



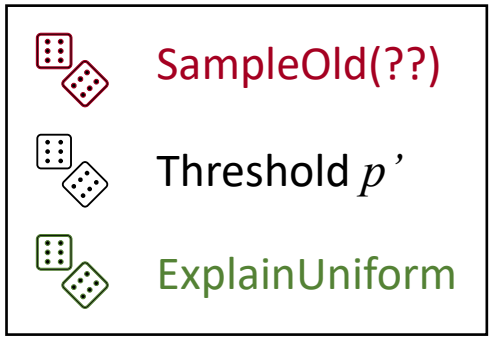


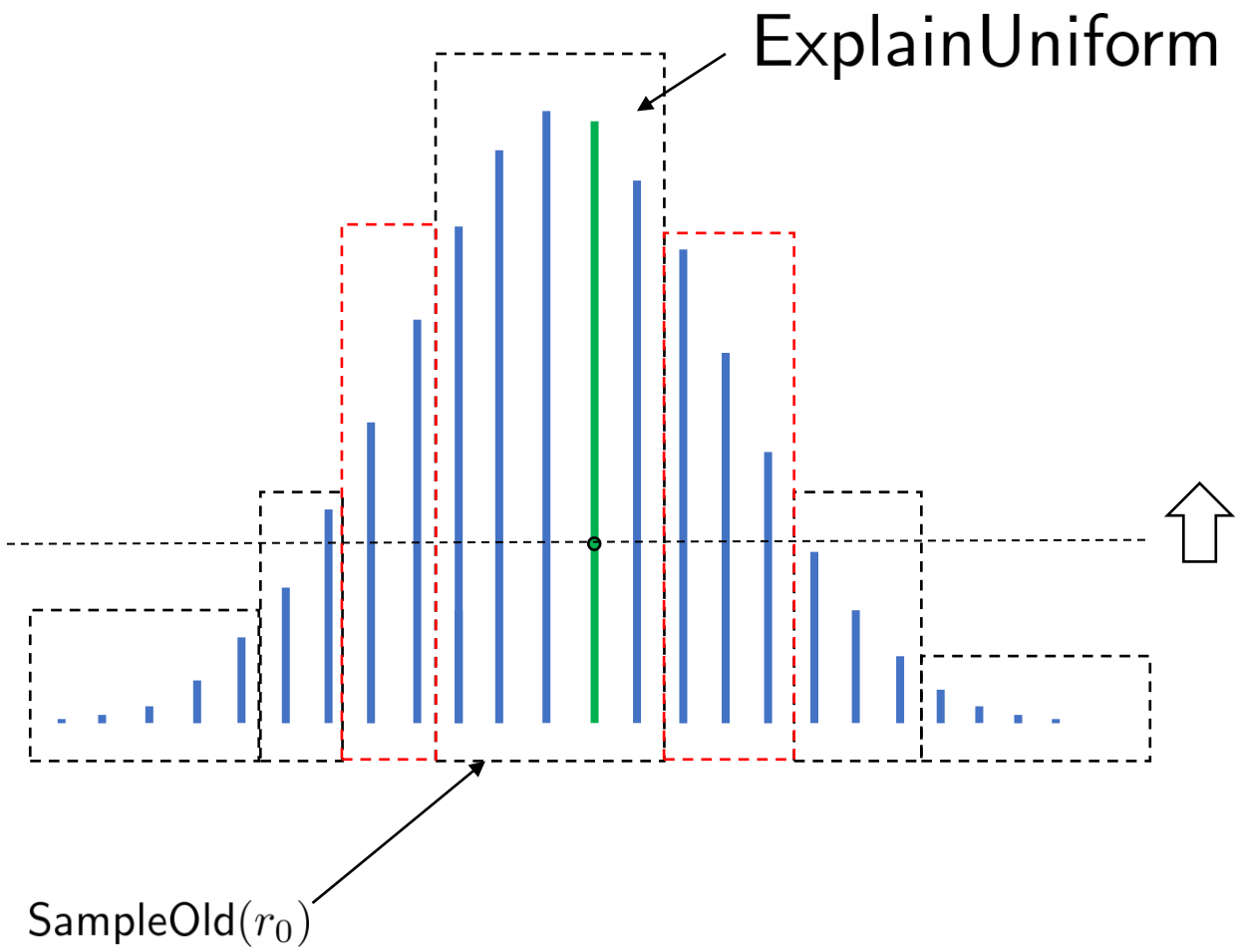
Large Range Explainer



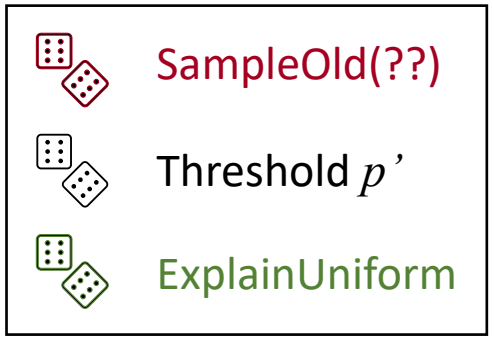


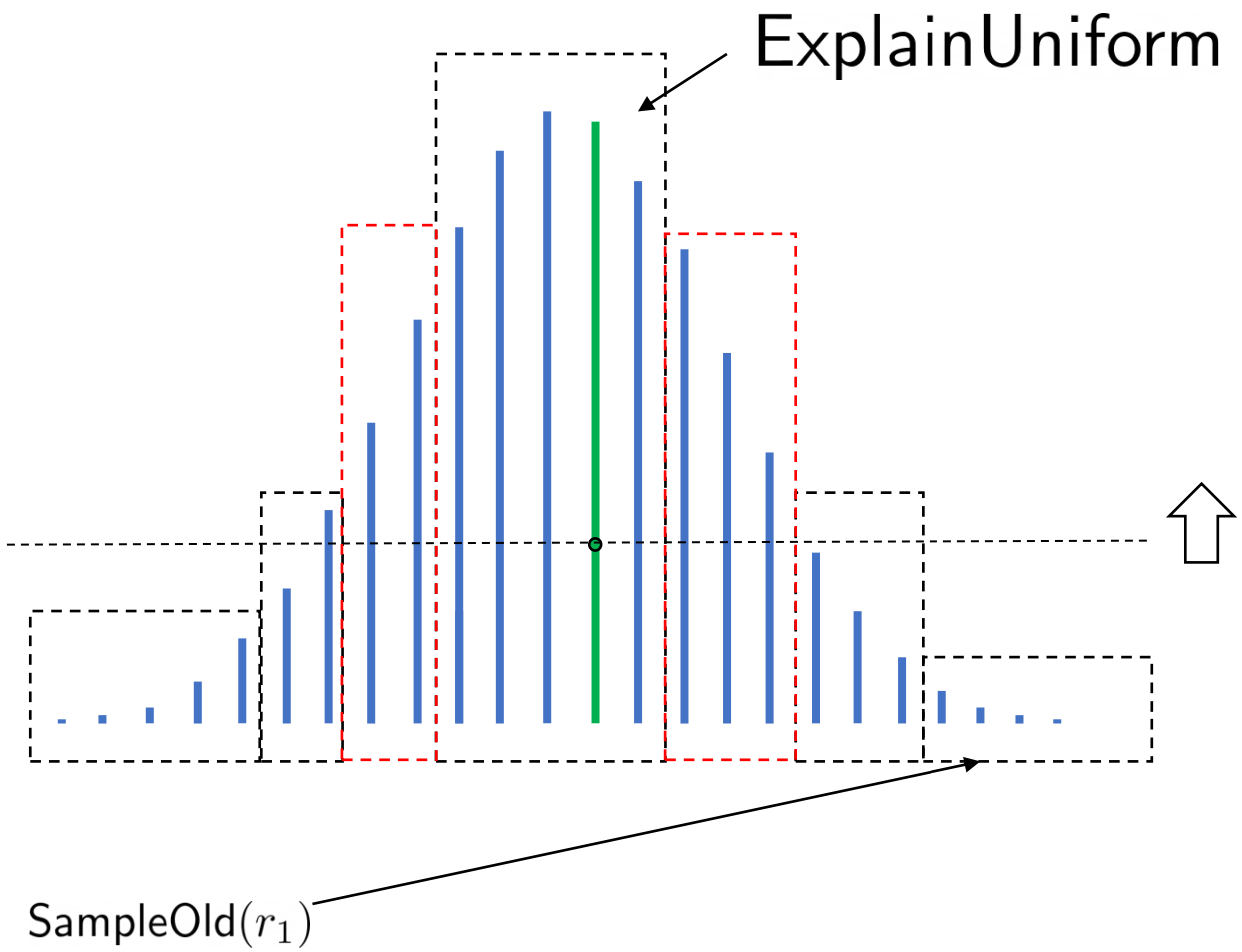
Large Range Explainer



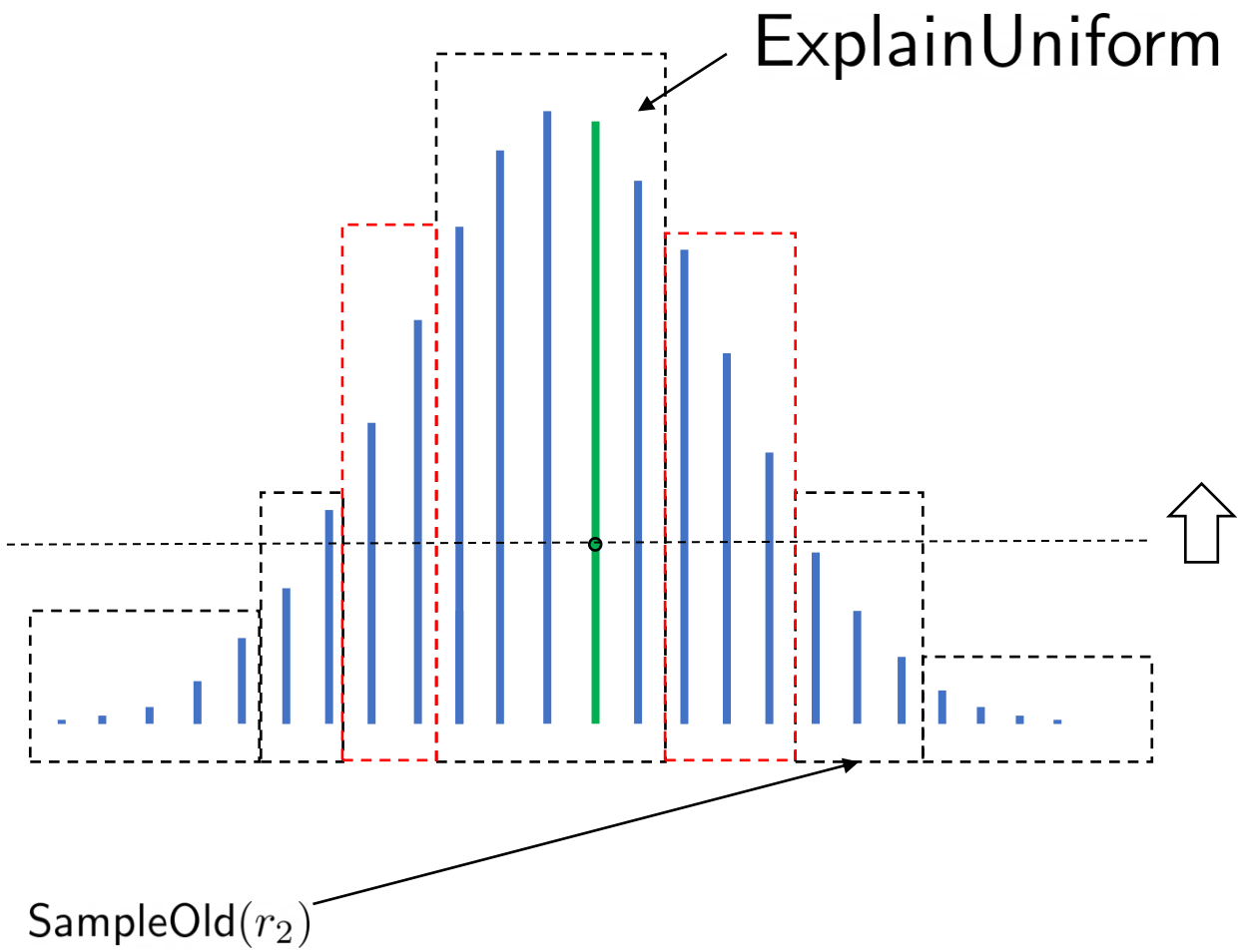


Large Range Explainer





Large Range Explainer

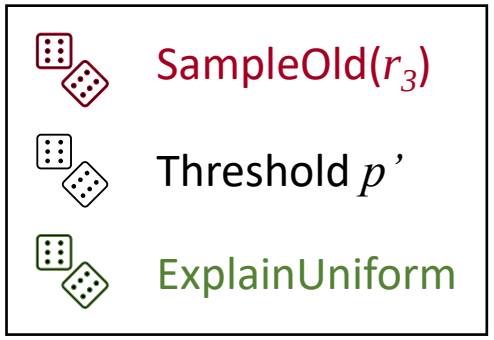


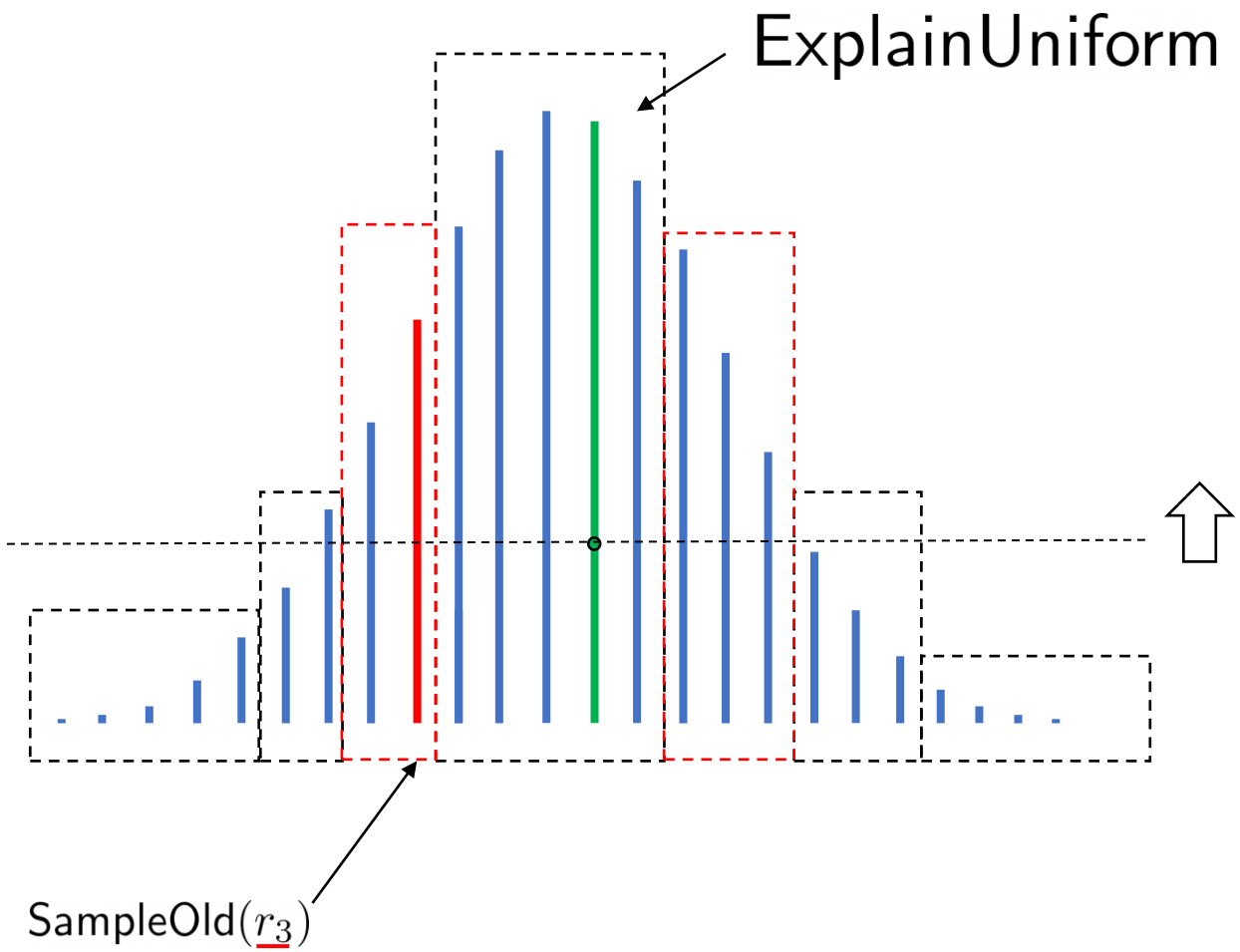
SampleOld(??)

Threshold p'

ExplainUniform

Large Range Explainer





Thank you!