Preserving Properties via Fooling Analysis Algorithms

- We want to sample random variables $\mathbf{e}_1, \ldots, \mathbf{e}_n$ using a small amount of randomness while preserving

- Consider the simple algorithm parameterized by x

- $s \leftarrow 0$

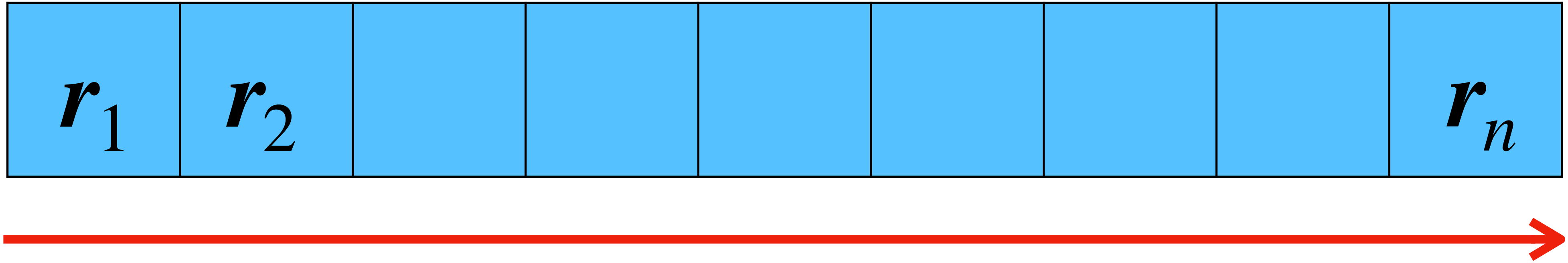
- For $i = 1, \ldots, n$:

- $s \leftarrow \max(s, |x_i| \cdot g(\boldsymbol{r}_i)^{-1/p})$

- Preserve the distribution of the output of this small space algorithm

$$\max(\mathbf{e}_1^{-1/p}\,|\,x_1\,|\,,\ldots,\mathbf{e}_n^{-1/p}\,|\,x_n\,|\,)\equiv\mathbf{e}^{-1/p}F_p^{1/p}$$

Close in TV distance suffices



r_1
r_2
r_n

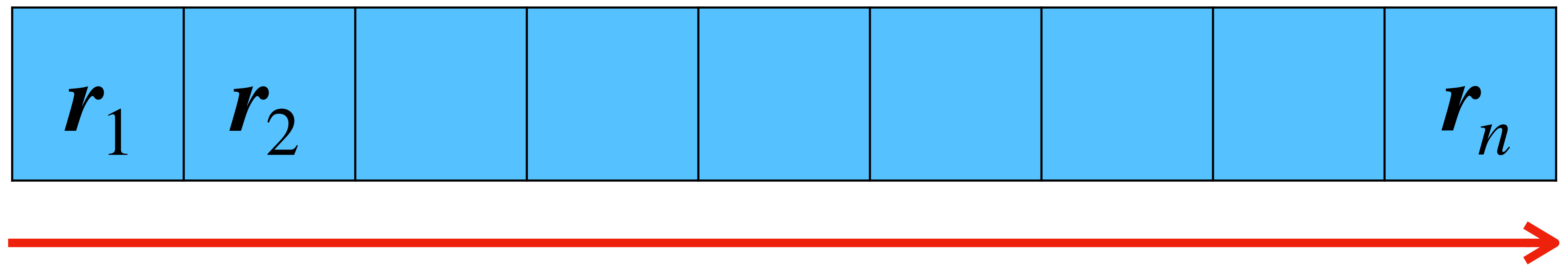
If $\boldsymbol{r}_i$ is a block of uniform random bits, $g(\boldsymbol{r}_i)$ has exponential distribution.

Preserving Properties via Fooling Analysis Algorithms

- We want to sample random variables $\mathbf{e}_1, \ldots, \mathbf{e}_n$ using a small amount of randomness while preserving

$$\max(\mathbf{e}_1^{-1/p} |x_1|, \ldots, \mathbf{e}_n^{-1/p} |x_n|) \equiv \mathbf{e}^{-1/p} F_p^{1/p}$$

- Consider the simple algorithm parameterized by x
  - $s \leftarrow 0$
  - For $i = 1, \ldots, n$:
    - $s \leftarrow \max(s, |x_i| \cdot g(\boldsymbol{r}_i)^{-1/p})$



If $\boldsymbol{r}_i$ is a block of uniform random bits, $g(\boldsymbol{r}_i)$ has exponential distribution.

- Preserve the distribution of the output of this small space algorithm

Derandomizing using Nisan's PRG