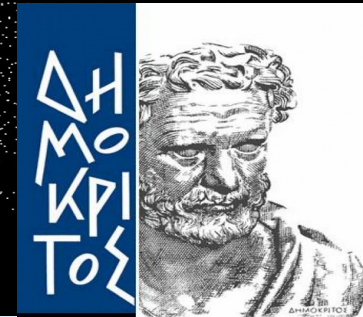


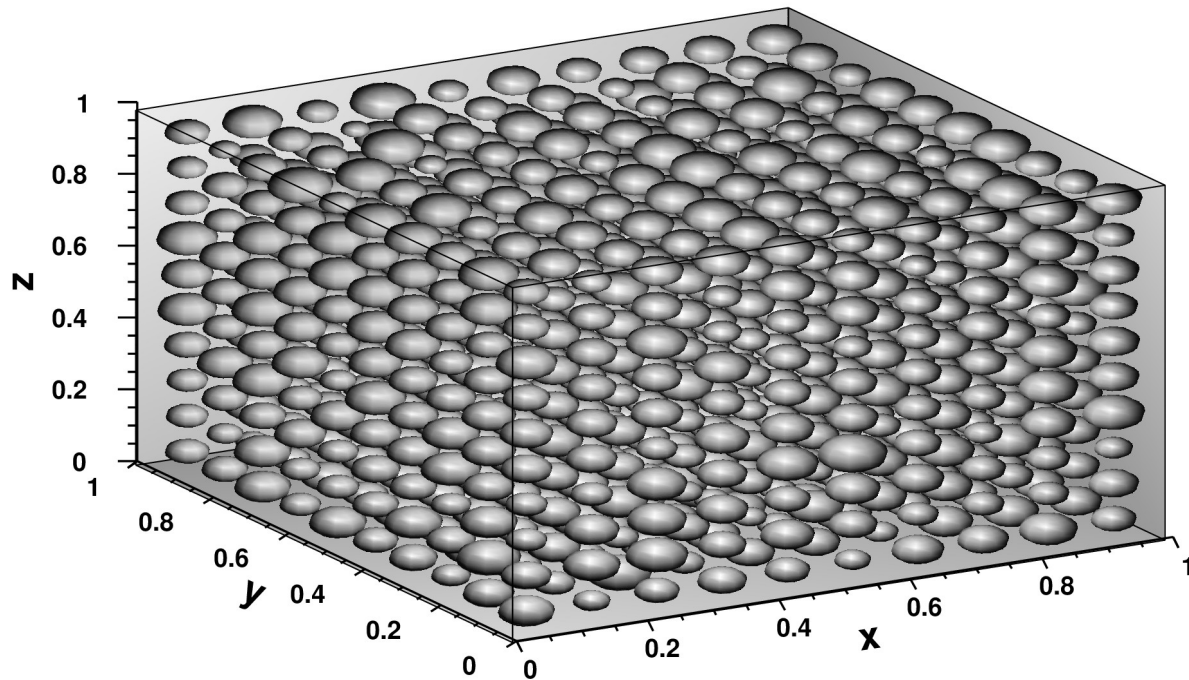
# Statistical tests for MIXMAX RNG

**Gevorg Karyan**

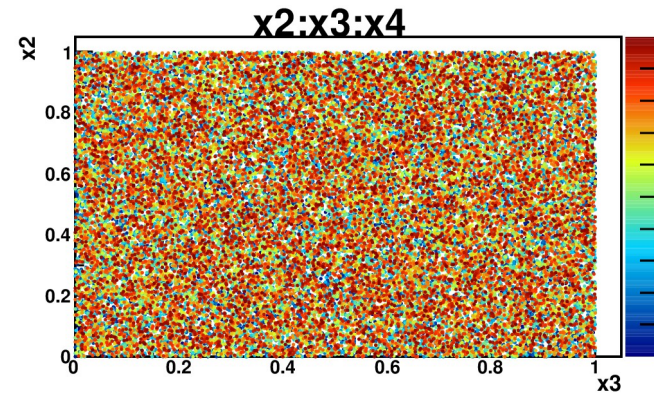
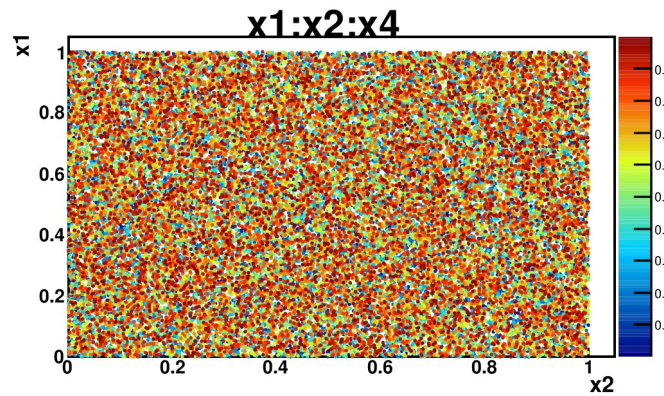
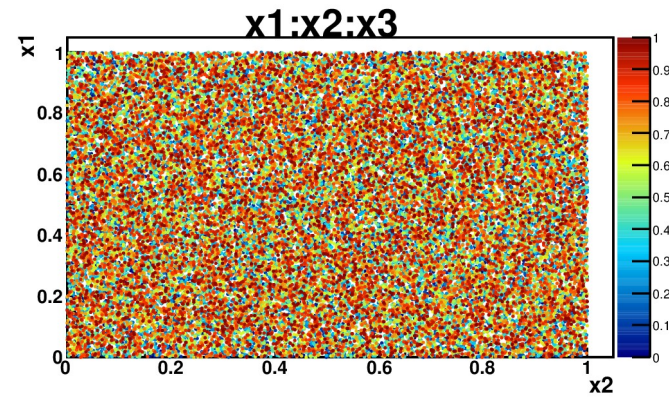
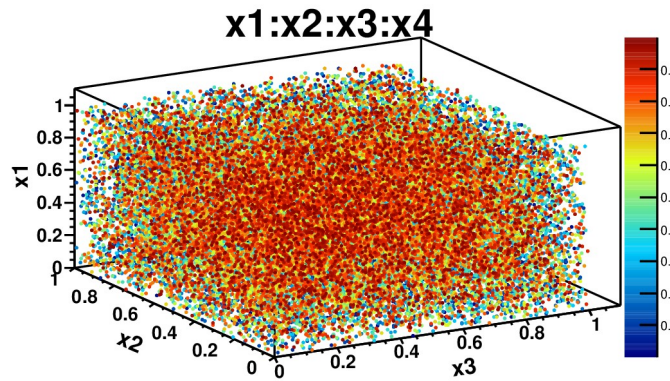
**Alikhanyan National Science Laboratory  
N.C.S.R. Demokritos**



# Are there obvious patterns?

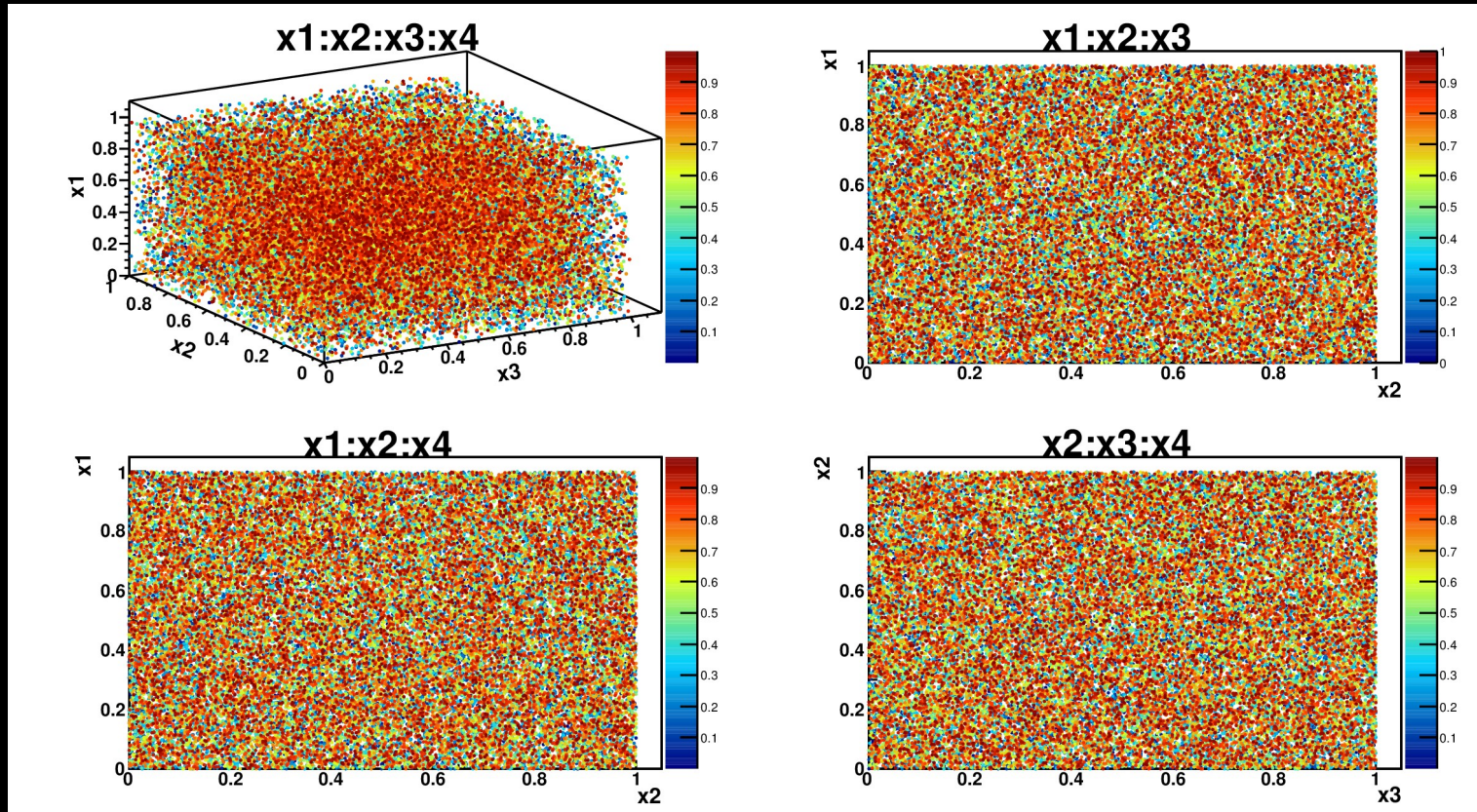


# Are there obvious patterns?





# Are there obvious patterns?



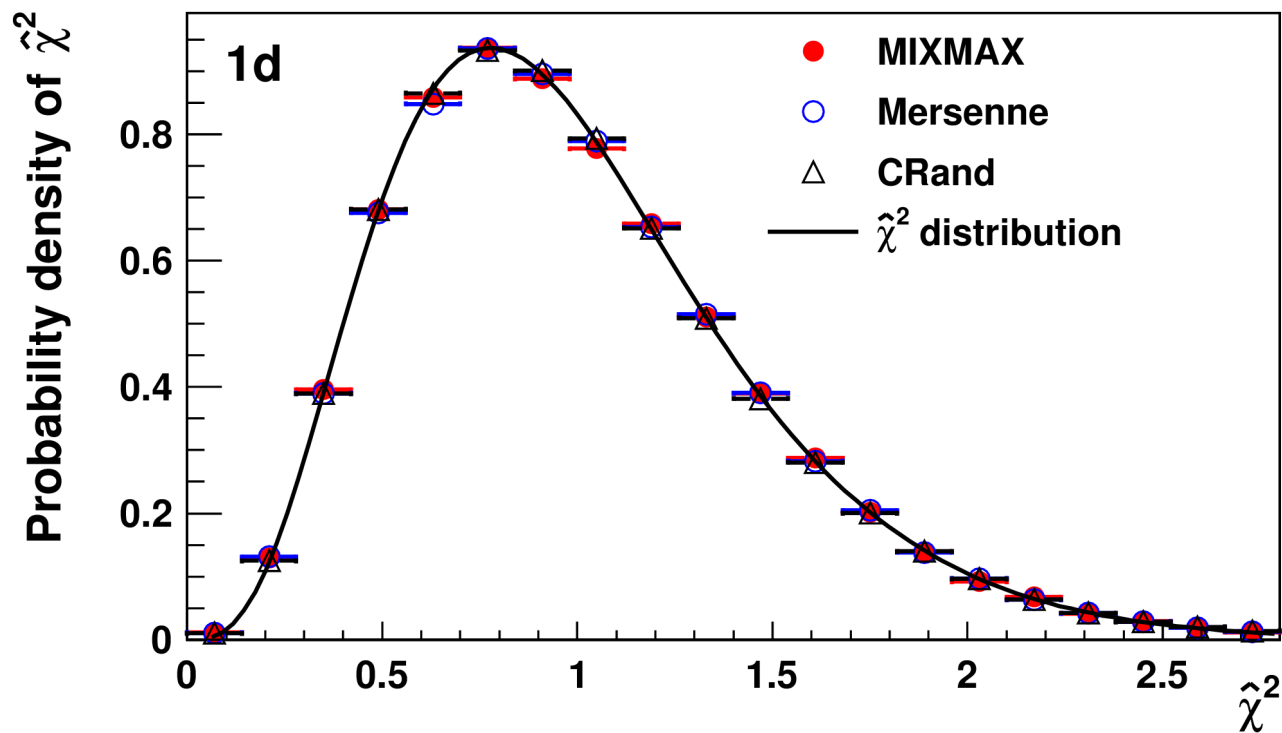
**No obvious patterns. But detailed studies are needed.**

# $\chi^2$ test

$$\chi^2 = \sum_{i=1}^N \frac{(\mathbf{x}_i - \bar{\mathbf{x}})^2}{\bar{\mathbf{x}}}, \quad \bar{\mathbf{x}} = K \frac{1}{N}$$

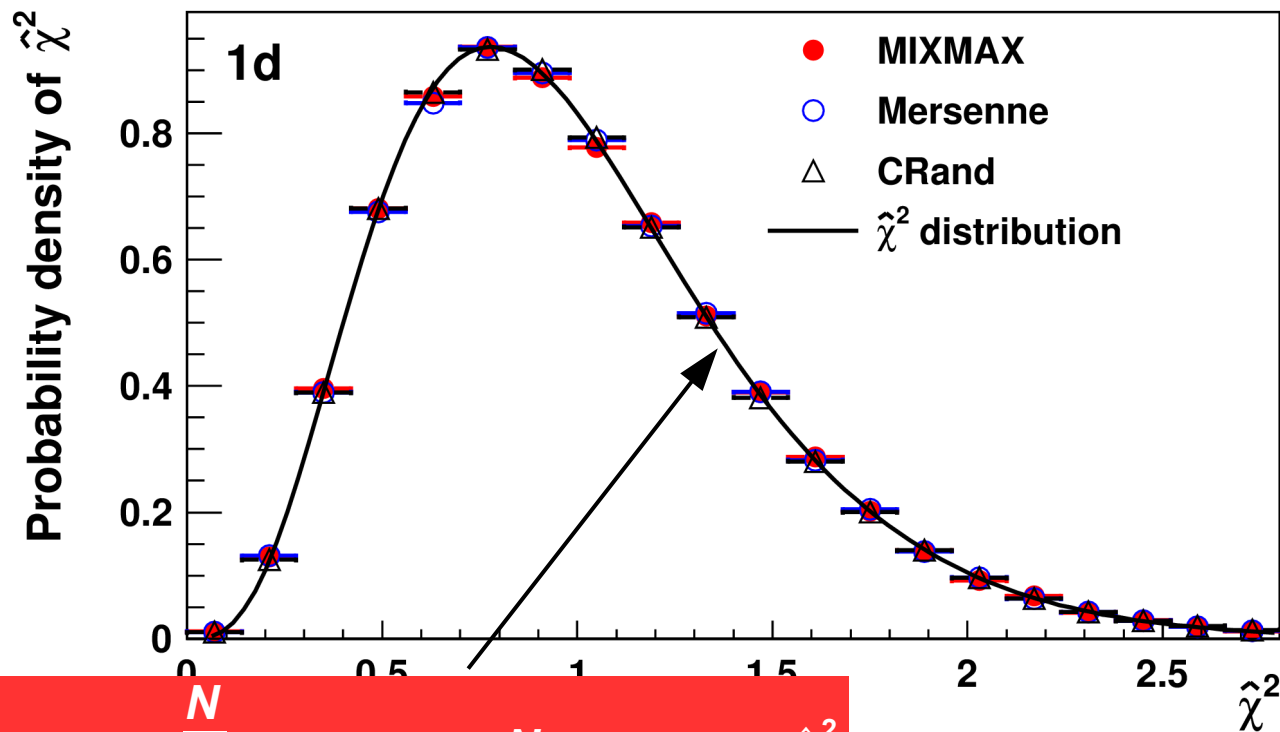
$$\hat{\chi}^2 = \frac{\chi^2}{N - 1}$$

# $\chi^2$ test



# $\chi^2$ test

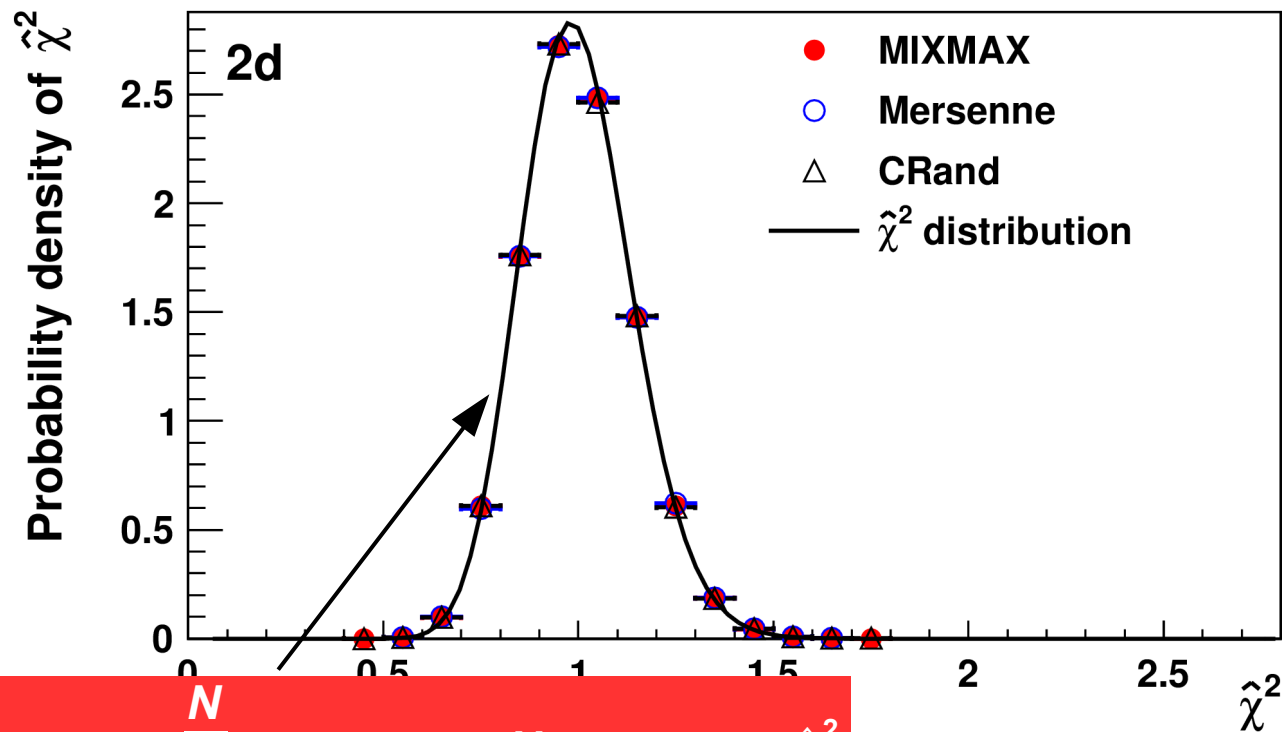
$N = 9$



$$f(\hat{\chi}^2) = \frac{N^{\frac{N}{2}}}{\Gamma\left(\frac{N}{2}\right) 2^{\frac{N}{2}}} (\hat{\chi}^2)^{\left(\frac{N}{2}-1\right)} e^{-N \frac{\hat{\chi}^2}{2}}$$

# $\chi^2$ test

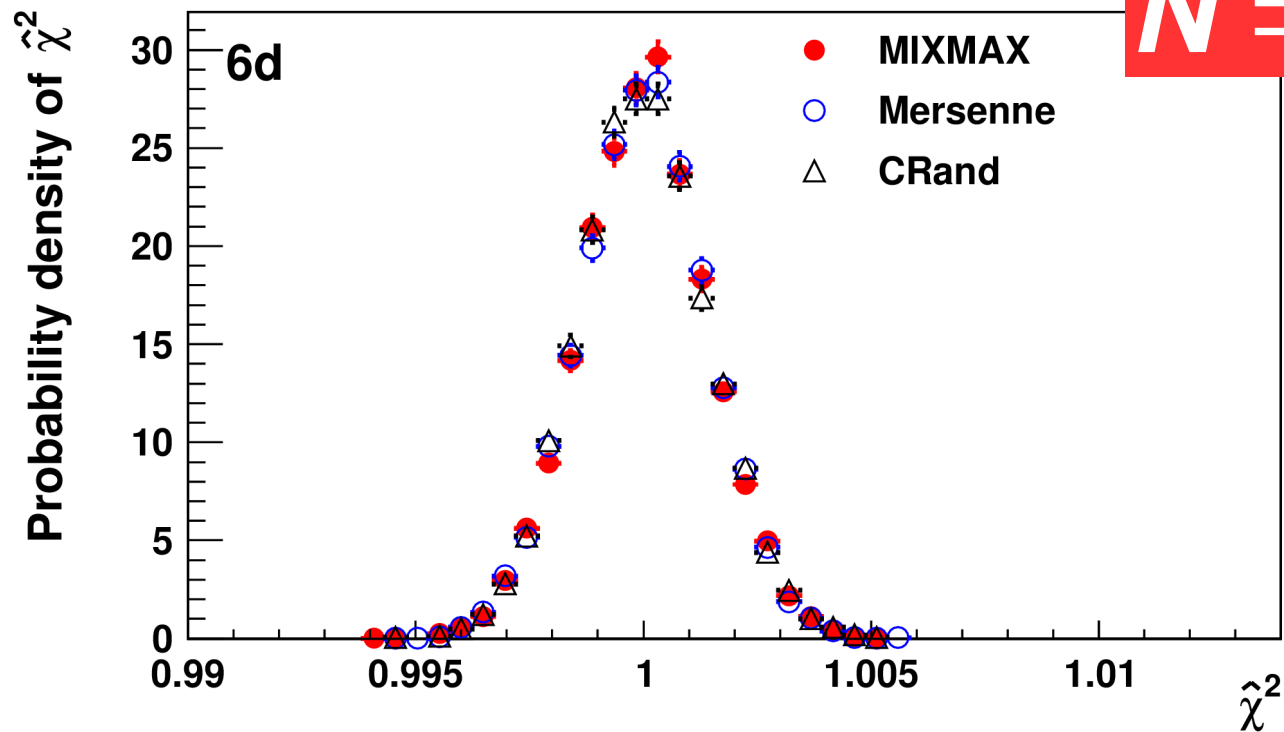
**$N = 99$**



$$f(\hat{\chi}^2) = \frac{N^{\frac{N}{2}}}{\Gamma\left(\frac{N}{2}\right) 2^{\frac{N}{2}}} (\hat{\chi}^2)^{\left(\frac{N}{2}-1\right)} e^{-N \frac{\hat{\chi}^2}{2}}$$



# $\chi^2$ test

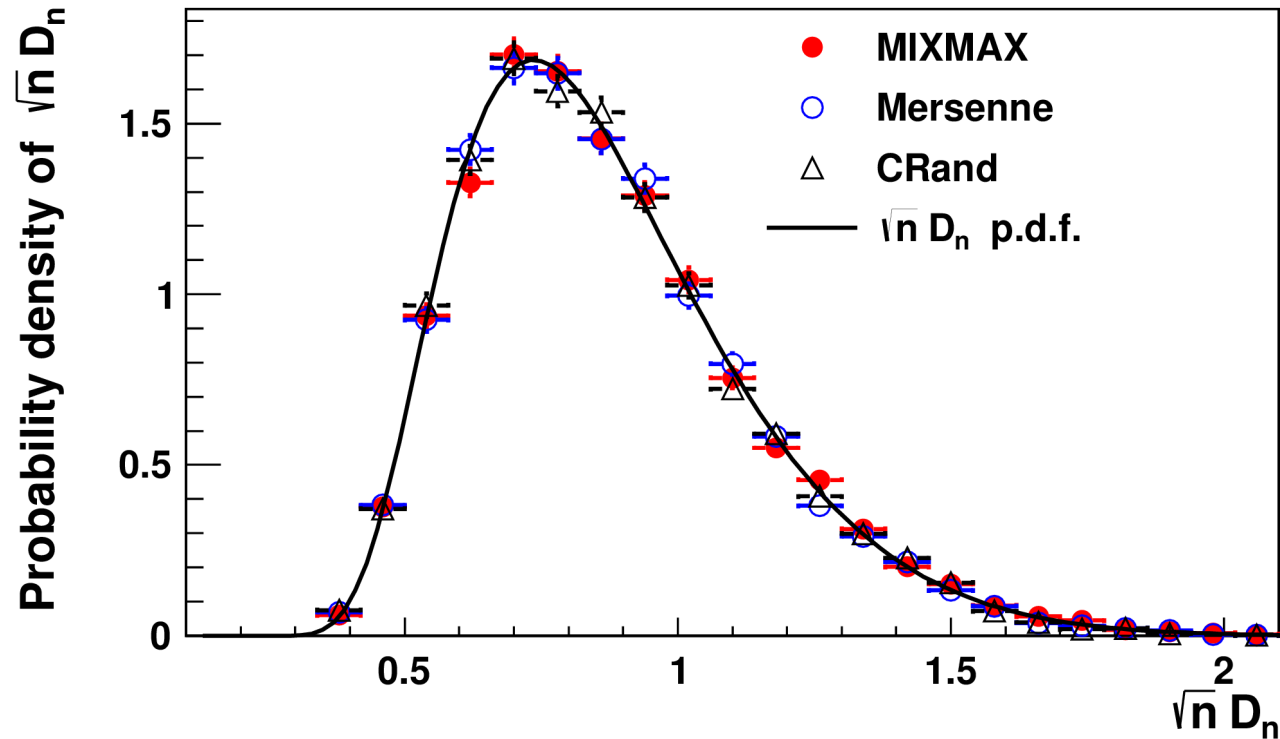


# Kolmogorov-Smirnov test

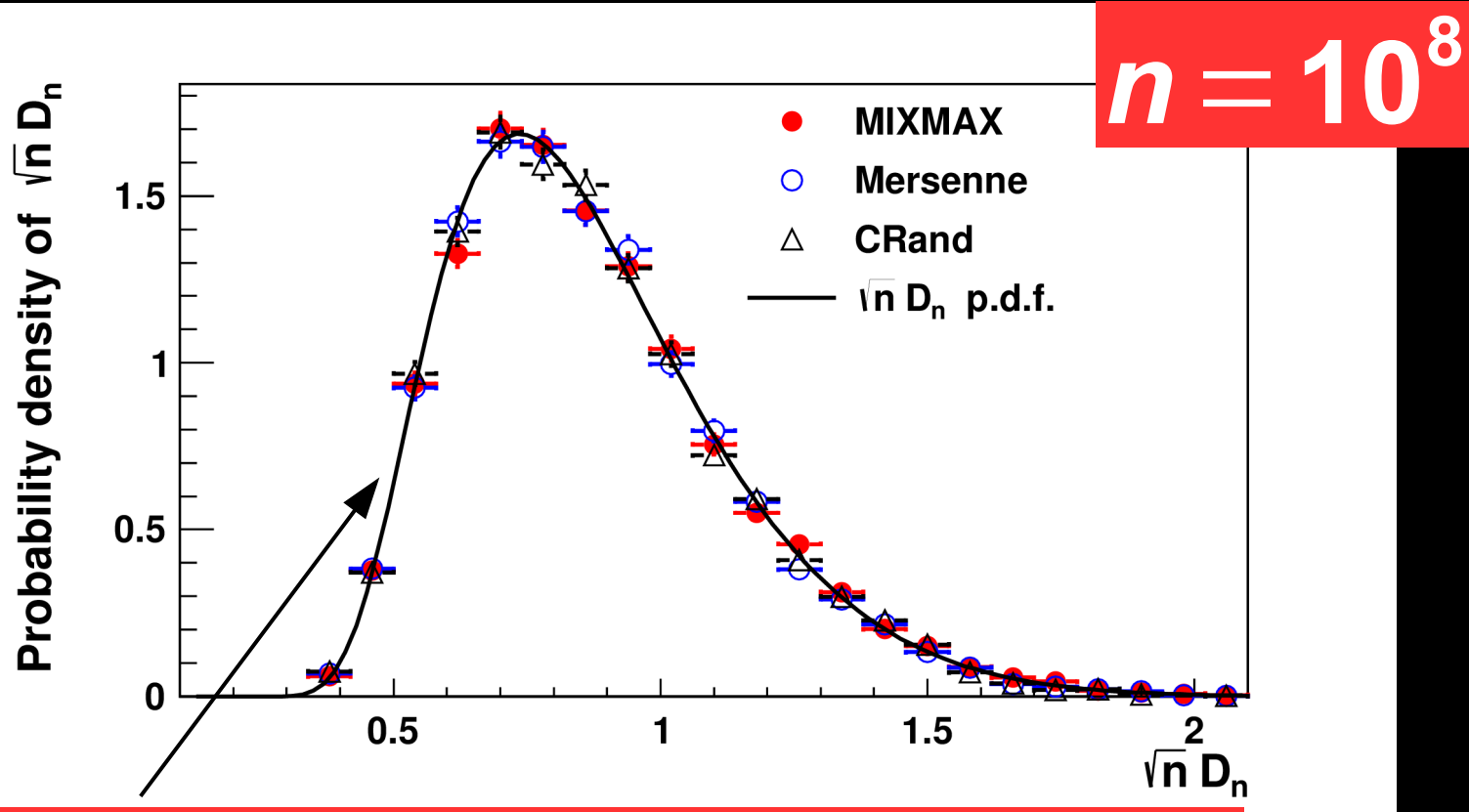
$$\lim_{n \rightarrow \infty} \Pr (\sqrt{n} D_n \leq X) = 1 - 2 \sum_{i=1}^{\infty} (-1)^{i-1} e^{-2 i^2 X^2}$$

$$D_n = \max |F_n(x) - F(x)|$$

# Kolmogorov-Smirnov test

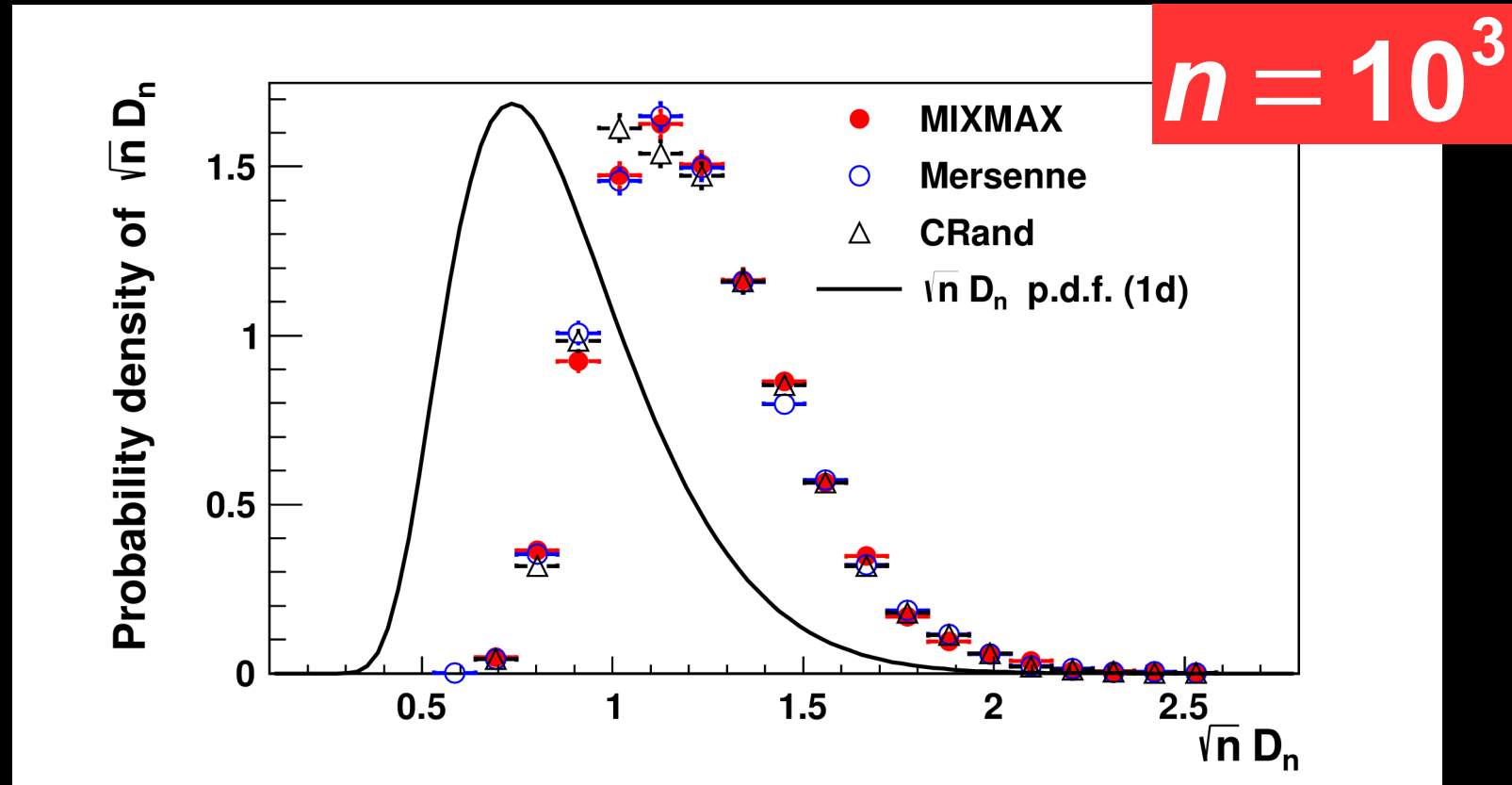


# Kolmogorov-Smirnov test



$$f(\sqrt{n} D_n) = 8 \sum_{i=1}^{100} (-1)^{i-1} i^2 (\sqrt{n} D_n) e^{-2i^2 (\sqrt{n} D_n)^2}$$

# Kolmogorov-Smirnov test (2d)



$$Pr(\sqrt{n} D_n \leq X, \sqrt{n} D_n \leq Y)$$



# **TestU01: empirical testing of RNG**

**A C library for empirical testing of  
random number generators.  
(L'ecuyer, Simard )**

# TestU01: empirical testing of RNG

```
===== Summary results of BigCrush =====  
  
Version:      TestU01 1.2.3  
Generator:    Ranlux24  
Number of statistics: 160  
Total CPU time: 32:37:16.39  
  
All tests were passed
```

# TestU01: empirical testing of RNG

```
===== Summary results of BigCrush =====  
  
Version:      TestU01 1.2.3  
Generator:    Ranlux24  
Number of statistics: 160  
Total CPU time: 32:37:16.39  
  
All tests were passed
```

# TestU01: empirical testing of RNG

## ===== ===== Summary results of BigCrush =====

**Version:** TestU01 1.2.3

**Generator:** Ranlux48

**Number of statistics:** 160

**Total CPU time:** 58:34:03.71

The following tests gave p-values outside [0.001, 0.9990]:

(eps means a value  $< 1.0e-300$ ):

(eps1 means a value  $< 1.0e-15$ ):

Test	p-value
82 LempelZiv, r = 0	0.9991

All other tests were passed

# TestU01: empirical testing of RNG

===== Summary results of BigCrush =====

Version: TestU01 1.2.3

Generator: Mersenne Twister(ROOT)

Number of statistics: 160

Total CPU time: 03:39:58.32

The following tests gave p-values outside [0.001, 0.9990]:

(eps means a value  $< 1.0e-300$ ):

(eps1 means a value  $< 1.0e-15$ ):

Test	p-value
79 RandomWalk1 H (L=10000, r=15)	1 - 7.8e-5
80 LinearComp, r = 0	1 - eps1
81 LinearComp, r = 29	1 - eps1

-----  
All other tests were passed



# TestU01: empirical testing of RNG

===== Summary results of BigCrush =====

Version: TestU01 1.2.3

Generator: Mersenne Twister(ROOT)

Number of statistics: 160

Total CPU time: 03:39:58.32

The following tests gave p-values outside [0.001, 0.9990]:

(eps means a value  $< 1.0e-300$ ):

(eps1 means a value  $< 1.0e-15$ ):

Test	p-value
79 RandomWalk1 H (L=10000, r=15)	1 - 7.8e-5
80 LinearComp, r = 0	1 - eps1
81 LinearComp, r = 29	1 - eps1

All other tests were passed

# TestU01: empirical testing of RNG

```
===== Summary results of BigCrush =====  
  
Version:      TestU01 1.2.3  
Generator:    MIXMAX  
Number of statistics: 160  
Total CPU time: 03:35:34.15  
  
All tests were passed
```

# TestU01: empirical testing of RNG

```
===== Summary results of BigCrush =====  
  
Version:      TestU01 1.2.3  
Generator:    MIXMAX  
Number of statistics: 160  
Total CPU time: 03:35:34.15  
  
All tests were passed
```

# Outlook

- **MIXMAX passes all tests available in TestU01.**
- **Quite fast and user friendly generator.**
- **More studies (i.e. spectral test, multivariate Kolmogorov test, ...) are ongoing.**

# Backup



