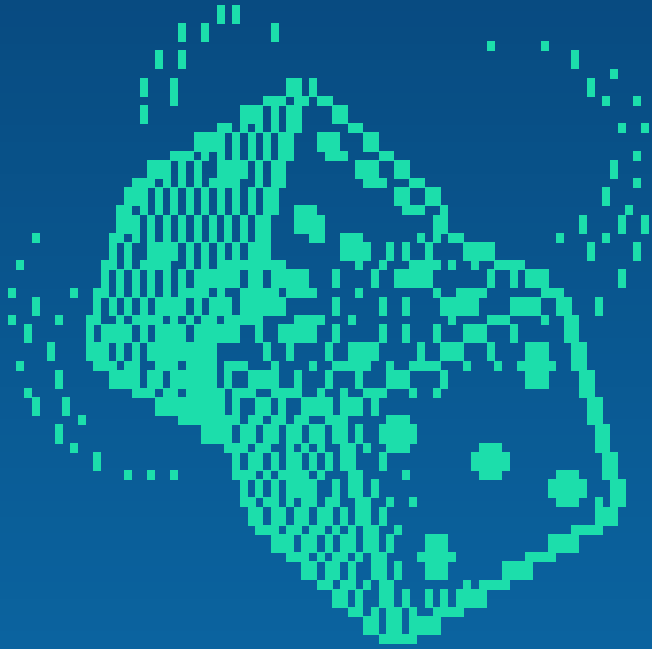


Entropy based Tests for Randomness and Applications to Cryptographic Generators



Stefan Wegenkittl

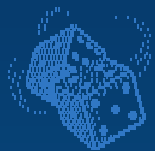
PLAB-Group of Prof. Peter Hellekalek

Dept. of Mathematics

University of Salzburg

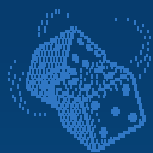
Stefan.Wegenkittl@sbg.ac.at

<http://random.mat.sbg.ac.at>



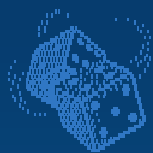
New Challenges for Empirical Testing

- (Pseudo)randomness: (Monte Carlo)
typical correlations: repetitive structures



New Challenges for Empirical Testing

- (Pseudo)randomness: (Monte Carlo)
typical correlations: repetitive structures
- (Pseudo)randomness: (Cryptography)
typical correlations: much broader range of defects



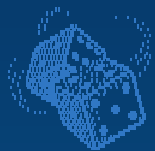
New Challenges for Empirical Testing

- (Pseudo)randomness: (Monte Carlo)
typical correlations: repetitive structures
- (Pseudo)randomness: (Cryptography)
typical correlations: much broader range of defects

⇒ wanted:

universal tests that can detect
any systematic deviation from randomness

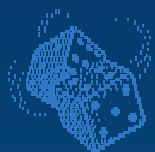
? cost of universality



Why Entropy

Entropy is



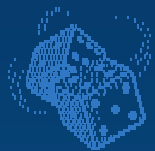


Why Entropy

Entropy is



- well understood concept for measuring randomness

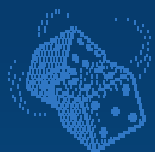


Why Entropy

Entropy is



- well understood concept for measuring randomness
- applicable to finite sequences

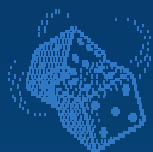


Why Entropy

Entropy is



- well understood concept for measuring randomness
- applicable to finite sequences
- related to cryptographic security

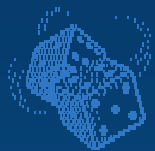


Why Entropy

Entropy is



- well understood concept for measuring randomness
- applicable to finite sequences
- related to cryptographic security
- related to established tests for randomness in Monte Carlo



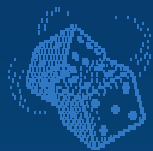
Interpretation

Interpretation: Per-Bit Entropy

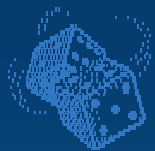
$$\frac{1}{\log_2 (\text{size of state space})} \cdot \text{Entropy}$$

of a cryptographic source

is equal to factor by which effective keysize is reduced

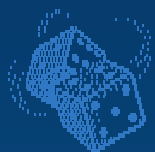


How to apply Entropy based tests



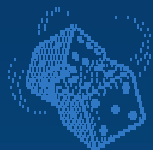
How to apply Entropy based tests

- different test principles (return times, frequencies)



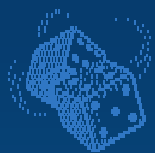
How to apply Entropy based tests

- different test principles (return times, frequencies)
- how to parameterize?



How to apply Entropy based tests

- different test principles (return times, frequencies)
- how to parameterize?
- what can we expect?

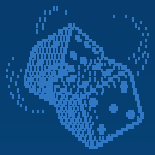


How to apply Entropy based tests

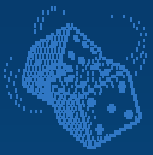
- different test principles (return times, frequencies)
- how to parameterize?
- what can we expect?
- correlations between tests?

Question:

Entropy based testing **universal**, i.e. **no other tests are required?**



Entropy Primer

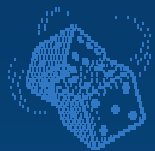


Entropy of Ergodic Prozesses

The scaled **logarithm of the probability of a random path** of length n converges to a limit

$$-\frac{1}{n} \log (P[\text{random Path}]) \xrightarrow{\text{a.s.}} H \dots \text{Entropy}$$

(Shannon-McMillan-Breimann)

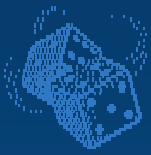


Order κ Markov Chains

The process $X = (X_i)_{i \geq 0}$, $X_i \in \mathcal{A} := \{1, 2, \dots, m\}$ is a

homogenous Markov-Chain of order κ

iff

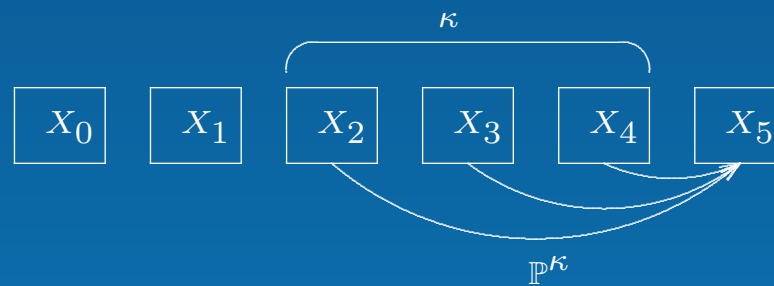


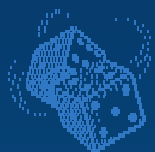
Order κ Markov Chains

The process $X = (X_i)_{i \geq 0}$, $X_i \in \mathcal{A} := \{1, 2, \dots, m\}$ is a
 homogenous Markov-Chain of order κ

iff

$$P[X_i = a_i | X_{i-1} = a_{i-1}, \dots, X_0 = a_0] = p_{a_{i-\kappa}, \dots, a_{i-1}, a_i}$$



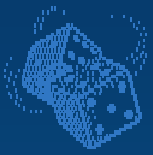


Ergodic Order κ Markov Chains

If transition probabilities

$$\mathbb{P}^{\kappa} = \left(p_{a_{i-\kappa}, \dots, a_{i-1}, a_i} \right)_{\mathbf{a} \in \mathcal{A}^{(\kappa+1)}}$$

define an irreducible and aperiodic chain,



Ergodic Order κ Markov Chains

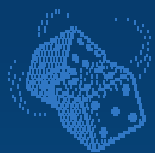
If transition probabilities

$$\mathbb{P}^{\kappa} = \left(p_{a_{i-\kappa}, \dots, a_{i-1}, a_i} \right)_{\mathbf{a} \in \mathcal{A}^{(\kappa+1)}}$$

define an irreducible and aperiodic chain,

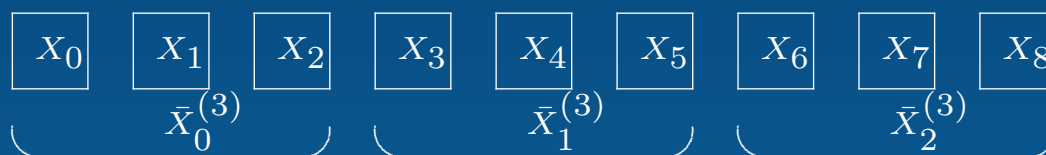
there exists a unique **stable distribution**

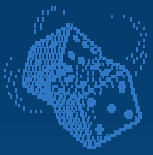
$$\left(\pi_{a_1, \dots, a_{\kappa}}^{(\kappa)} \right)_{\mathbf{a} \in \mathcal{A}^{\kappa}} \quad \text{with} \quad \pi^{(\kappa)} = \pi^{(\kappa)} \cdot \mathbb{P}^{\kappa}$$



Derived Processes of Order κ Chains

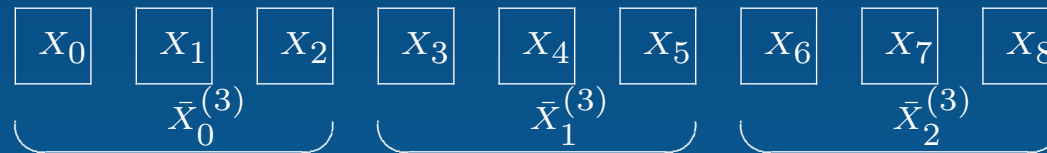
$$\bar{X}_i^{(r)} = (X_{r \cdot i}, \dots, X_{r \cdot i + r - 1}) \dots \text{non-overlapping } r\text{-tuples}$$



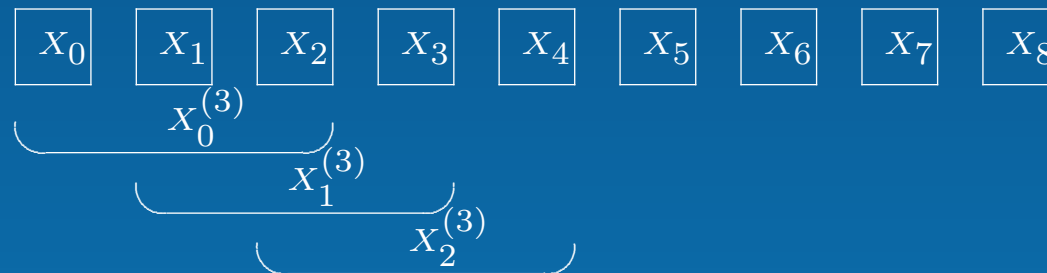


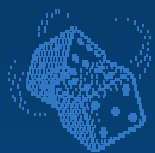
Derived Processes of Order κ Chains

$$\bar{X}_i^{(r)} = (X_{r \cdot i}, \dots, X_{r \cdot i + r - 1}) \dots \text{non-overlapping } r\text{-tuples}$$



$$X_i^{(r)} = (X_i, \dots, X_{i+r-1}) \dots \text{overlapping } r\text{-tuples}$$

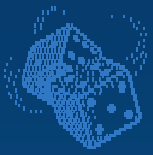




Derived Processes of Order κ Chains (ii)

If $r > \kappa$, the process of overlapping r tuples

$(X_i^{(r)})_{i \geq 0}$ becomes ordinary (order 1) chain



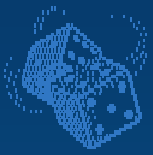
Derived Processes of Order κ Chains (ii)

If $r > \kappa$, the process of overlapping r tuples

$(X_i^{(r)})_{i \geq 0}$ becomes ordinary (order 1) chain

with stable distribution

$$\pi_{a_1, \dots, a_r}^{(r)} = \pi_{a_1, \dots, a_\kappa}^{(\kappa)} \cdot \prod_{l=\kappa+1}^r p_{a_{l-\kappa}, a_{l-\kappa+1}, \dots, a_l}$$

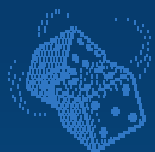


Entropy of Order κ Chains

For $r > \kappa$ Birkhoff's theorem gives

$$H = H(\mathcal{A}, \mathbb{P}^{\kappa}) = - \sum_{\mathbf{a} \in \mathcal{A}^r} \pi_{\mathbf{a}}^{(r)} \log_2 \underbrace{\left(\frac{\pi_{\mathbf{a}}^{(r)}}{\pi_{\mathbf{a}'}^{(r-1)}} \right)}_{\text{prob. of last step}}$$

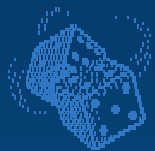
with $\mathbf{a}' = (a_1, \dots, a_{r-1})$.



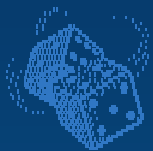
Entropy of Order 1 Chains

For ordinary chains, this gives:

$$H(\mathcal{A}, \mathbb{P}) = - \sum_{i \in \mathcal{A}} \pi_i \sum_{j \in \mathcal{A}} p_{ij} \log_2 p_{ij}$$



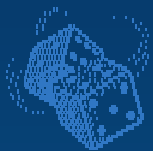
Computing Entropy of Chains



Using stable distributions: Chain Rule

For $r > \kappa$

$$H(\mathcal{A}, \mathbb{P}^{\kappa}) = H(\pi^{(r)}) - H(\pi^{(r-1)}),$$



Using stable distributions: Chain Rule

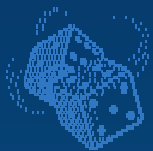
For $r > \kappa$

$$H(\mathcal{A}, \mathbb{P}^{\kappa}) = H(\pi^{(r)}) - H(\pi^{(r-1)}),$$

where

$$H(\pi^{(r)}) = - \sum_{\mathbf{a} \in \mathcal{A}^r} \pi_{\mathbf{a}}^{(r)} \log_2 \pi_{\mathbf{a}}^{(r)}$$

is the Entropy of the distribution $\pi^{(r)}$

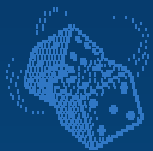


Using Return Times - Overlapping Case

Let

$$T^{(r)} = \min \left\{ i \geq r : X_i^{(r)} = X_0^{(r)} \right\}$$

be the first (overlapping) **return time** of order r .



Using Return Times - Overlapping Case

Let

$$T^{(r)} = \min \left\{ i \geq r : X_i^{(r)} = X_0^{(r)} \right\}$$

be the first (overlapping) **return time** of order r .

Wyner & Ziv:

$$\frac{\log_2 \left(T^{(r)} \right)}{r} \xrightarrow{p} H, \text{ as } r \rightarrow \infty$$

Pointwise Theorem: Ornstein, Weiss

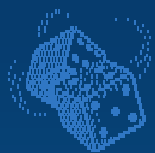


Using Return Times - Non-Overlapping Case

Let

$$\bar{T}^{(r)} = \min \left\{ i \geq 1 : \bar{X}_i^{(r)} = \bar{X}_0^{(r)} \right\}$$

be the first (non-overlapping) return time of order r .



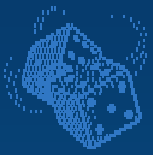
Expected Non-Overlapping Return Times

If $r \geq \kappa$,

$$E \left[\bar{T}^{(r)} \mid \bar{X}_0^{(r)} = \mathbf{a} \right] = \frac{1}{\pi_{\mathbf{a}}^{(r)}}, \quad \mathbf{a} \in \mathcal{A}^r$$

and, consequently,

$$E \left[\bar{T}^{(r)} \right] = m^r$$



Expected Non-Overlapping Return Times

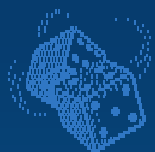
If $r \geq \kappa$,

$$E \left[\bar{T}^{(r)} \mid \bar{X}_0^{(r)} = \mathbf{a} \right] = \frac{1}{\pi_{\mathbf{a}}^{(r)}}, \quad \mathbf{a} \in \mathcal{A}^r$$

and, consequently,

$$E \left[\bar{T}^{(r)} \right] = m^r$$

$E[\cdot]$ contains no information on chain!

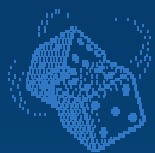


Expected Logarithm of Return Times

Thus: use $E[\log_2(\cdot)]$

Maurer, similar to Willems:

$$\frac{E[\log_2(\bar{T}^{(r)})]}{r} \rightarrow H$$

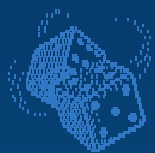


Expected Logarithm of Return Times (ii)

Speed of convergence: Let

$$E(r) = (r - 1) \cdot H(\mathcal{A}, \mathbb{P}^{\kappa}) + H(\pi^{(r)}),$$

then



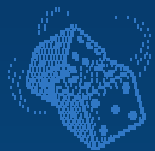
Expected Logarithm of Return Times (ii)

Speed of convergence: Let

$$E(r) = (r - 1) \cdot H(\mathcal{A}, \mathbb{P}^{\kappa}) + H(\pi^{(r)}),$$

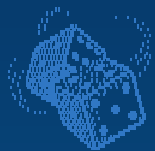
then

$$\lim_{r \rightarrow \infty} \left(E \left[\log_2 \left(\bar{T}^{(r)} \right) \right] - E(r) \right) = \frac{\gamma}{\ln(2)}$$



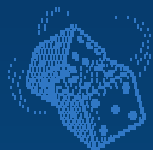
Summary

- Entropy well defined for order κ chains
- **Compute** by either



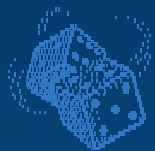
Summary

- Entropy well defined for order κ chains
- **Compute** by either
 - **stable distribution of overlapping tuples and chain rule**

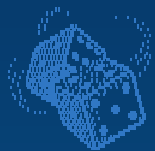


Summary

- Entropy well defined for order κ chains
- **Compute** by either
 - **stable distribution of overlapping tuples and chain rule**
 - **expected logarithm of return time of non-overlapping tuples**



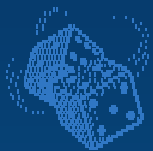
Tests for Randomness based on Entropy



Tests for Randomness based on Entropy

H_0 : X is i.i.d. uniform on \mathcal{A}

H_1 : X is not H_0 but stationary, ergodic chain



Tests for Randomness based on Entropy

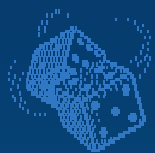
H_0 : X is i.i.d. uniform on \mathcal{A}

H_1 : X is not H_0 but stationary, ergodic chain

Idea: given realization

$$x = (x_0, x_1, \dots, x_{n-1})$$

estimate Entropy H (or related property) of X



Tests for Randomness based on Entropy

H_0 : X is i.i.d. uniform on \mathcal{A}

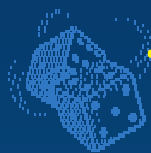
H_1 : X is not H_0 but stationary, ergodic chain

Idea: given realization

$$x = (x_0, x_1, \dots, x_{n-1})$$

estimate Entropy H (or related property) of X

Reject H_0 if result unlikely under H_0 .

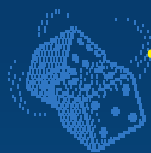


Tests for Randomness based on Entropy (ii)

Universality:

$$H_0: H = \log_2(m)$$

$$H_1: H < \log_2(m)$$



Tests for Randomness based on Entropy (ii)

Universality:

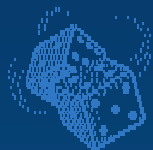
$$H_0: H = \log_2(m)$$

$$H_1: H < \log_2(m)$$

Estimator of H will be able to

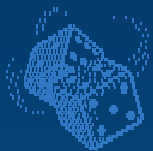
detect any possible deviation from H_0

provided n is large enough.



Construction of Entropy Tests

Goal: estimate Entropy

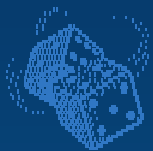


Tests based on relative frequency

Let

$$\hat{\pi}_{\mathbf{a}}^{(r)} = \frac{1}{n} \# \left\{ 0 \leq i < n : \bar{X}_i^{(r)} = \mathbf{a} \right\}$$

then $\hat{\pi}_{\mathbf{a}}^{(r)}$ is unbiased consistent estimator for $\pi_{\mathbf{a}}^{(r)}$



Tests based on relative frequency

Let

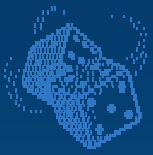
$$\hat{\pi}_{\mathbf{a}}^{(r)} = \frac{1}{n} \# \left\{ 0 \leq i < n : \bar{X}_i^{(r)} = \mathbf{a} \right\}$$

then $\hat{\pi}_{\mathbf{a}}^{(r)}$ is unbiased consistent estimator for $\pi_{\mathbf{a}}^{(r)}$

Apply Chain-Rule: For $r > \kappa$,

$$\hat{H}_f := H(\hat{\pi}^{(r)}) - H(\hat{\pi}^{(r-1)})$$

is asymptotically unbiased consistent estimator for H .



Tests based on relative frequency (ii)

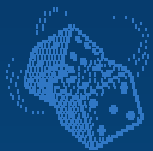
Normalization:

$$\text{dense} : 2n(\log_2(m) - \hat{H}_f) \xrightarrow{d} \chi_{m^r - m^{r-1}}^2, \text{ as } n \rightarrow \infty$$

$$\text{sparse} : \frac{\hat{H}_f - \mu}{\sigma} \xrightarrow{d} N(0, 1) \text{ as } n, r \rightarrow \infty, \frac{m^r}{n} \rightarrow \lambda$$

r . . . dimension of test

m . . . granularity



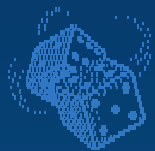
Tests based on relative frequency (iii)

Examples for H_f :

Approx. Entropy Pincus et. al., NIST battery: discrete case, which is equivalent to \hat{H}_f

Modified ApEn Ruhkin, asymptotically and practically equivalent to \hat{H}_f

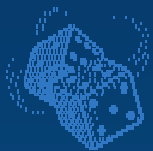
Overlapping I-Divergence Wegenkittl: connection to serial testing



Tests based on relative frequency (iv)

H_f belongs to the class of **Power-Divergence Tests** :

- statistical goodness-of-fit tests
- various likelihood functions
- statistically equivalent in dense case
- very efficient in sparse case (L'Ecuyer, Simard, Wegenkittl)



Tests based on relative frequency (ψ)

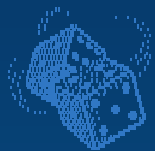
Standard overlapping serial test (Pearson, Good): let

$$\psi^{(r)} := n \sum_{\mathbf{a} \in \mathcal{A}^r} \frac{(\hat{\pi}_{\mathbf{a}}^{(r)} - \pi_{\mathbf{a}}^{(r)})^2}{\pi_{\mathbf{a}}^{(r)}}$$

and put

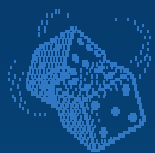
$$\hat{\chi} = \psi^{(r)} - \psi^{(r-1)} \xrightarrow{d} \chi_{m^r - m^{r-1}}^2$$

Examples: **Monkey Tests in Diehard, Serial test in NIST**



Tests based on relative frequency (vi)

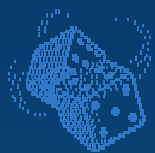
Universality: If X is an order κ Markov chain
and provided $r > \kappa$,



Tests based on relative frequency (vi)

Universality: If X is an order κ Markov chain
and provided $r > \kappa$,

\hat{H}_f is able to detect any deviation from H_0



Tests based on relative frequency (vii)

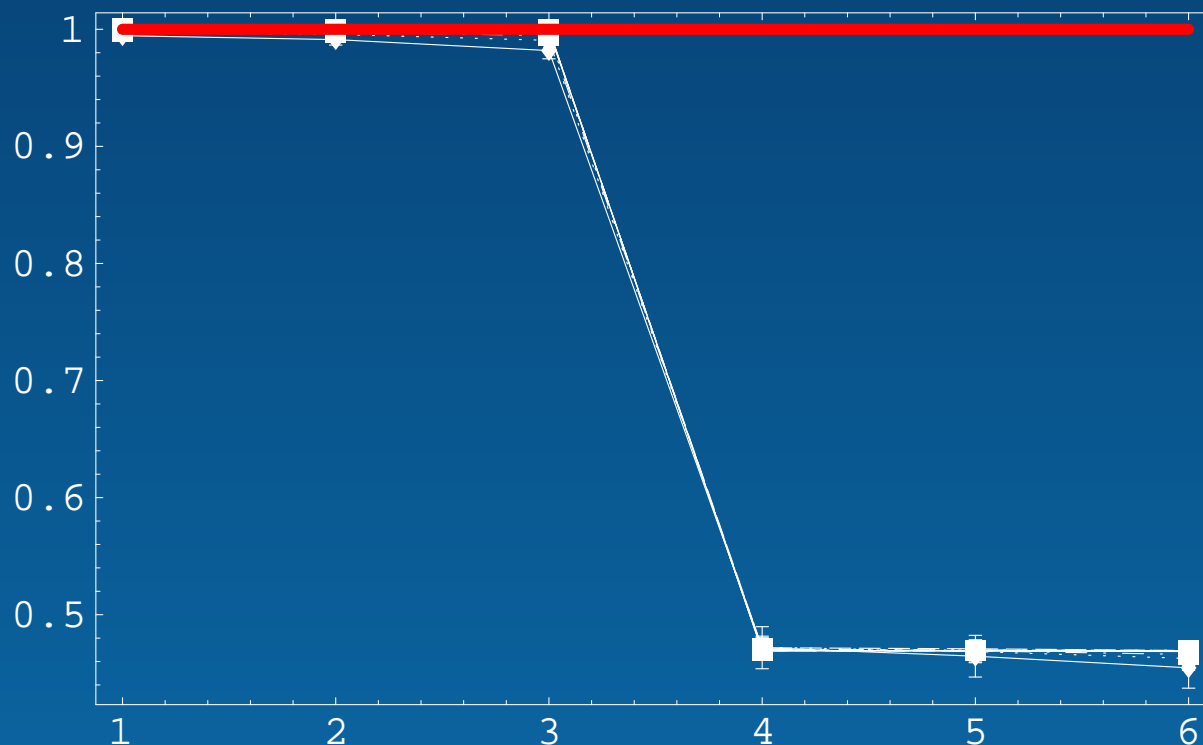
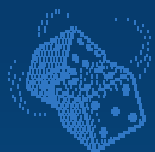


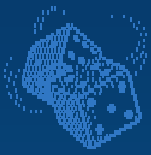
Fig. 1: Samples of \hat{H}_f for an order-3 chain with $H = 0.469$



Tests based on return times

Maurer: estimate $E[\log_2(\bar{T}^{(r)})]$ by

$$\hat{H}_r := \frac{1}{r \cdot n} \sum_{i=Q+1}^{Q+n} \log_2 T(i),$$



Tests based on return times

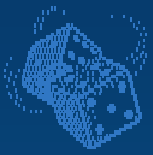
Maurer: estimate $E[\log_2(\bar{T}^{(r)})]$ by

$$\hat{H}_r := \frac{1}{r \cdot n} \sum_{i=Q+1}^{Q+n} \log_2 T(i),$$

with (letting $\bar{X}_{-1}^{(r)} := \bar{X}_i^{(r)}$)

$$T(i) = \min \left\{ 1 \leq j \leq i + 1 : \bar{X}_{i-j}^{(r)} = \bar{X}_i^{(r)} \right\}$$

Q . . . warm-up, initialization



Tests based on return times (ii)

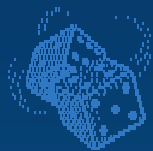
Normalization: compute (tables available)

$E[\hat{H}_r]$ (rather easy)

$V[\hat{H}_r]$ (rather complicated, only approx. available)

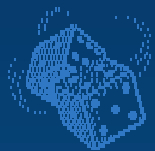
under H_0 , then

$$\frac{\hat{H}_r - E[\cdot]}{\sqrt{V[\cdot]}} \xrightarrow{d} N[0, 1]$$



Tests based on return times (iii)

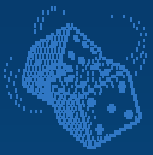
Universality: Maurer: $E [\log_2 (\bar{T}^{(r)})]$ detects any significant deviation from truly random bit source



Tests based on return times (iii)

Universality: Maurer: $E [\log_2 (\bar{T}^{(r)})]$ detects any significant deviation from truly random bit source

! case $r \rightarrow \infty$ is clear



Tests based on return times (iii)

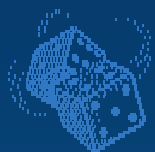
Universality: Maurer: $E [\log_2 (\bar{T}^{(r)})]$ detects any significant deviation from truly random bit source

! case $r \rightarrow \infty$ is clear

? also true for $r \in \mathbb{N}$ fixed

For any fixed $r \in \mathbb{N}$, we do not estimate H but only related property.

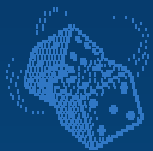
Is this property sensitive to H_1 ?



Tests based on return times (vii)

Some precomputed values of $E[\log_2(\cdot)]$ for $m = 2$

r	$E[r \cdot \hat{H}_r]$	$E[\hat{H}_r] - \frac{\gamma}{r \cdot \ln(2)}$
1	0.73265	1.5654
2	1.53744	1.1851
3	2.40161	1.0781
4	3.31122	1.0360
5	4.25343	1.0172
6	5.21771	1.0084



Tests based on return times (viii)

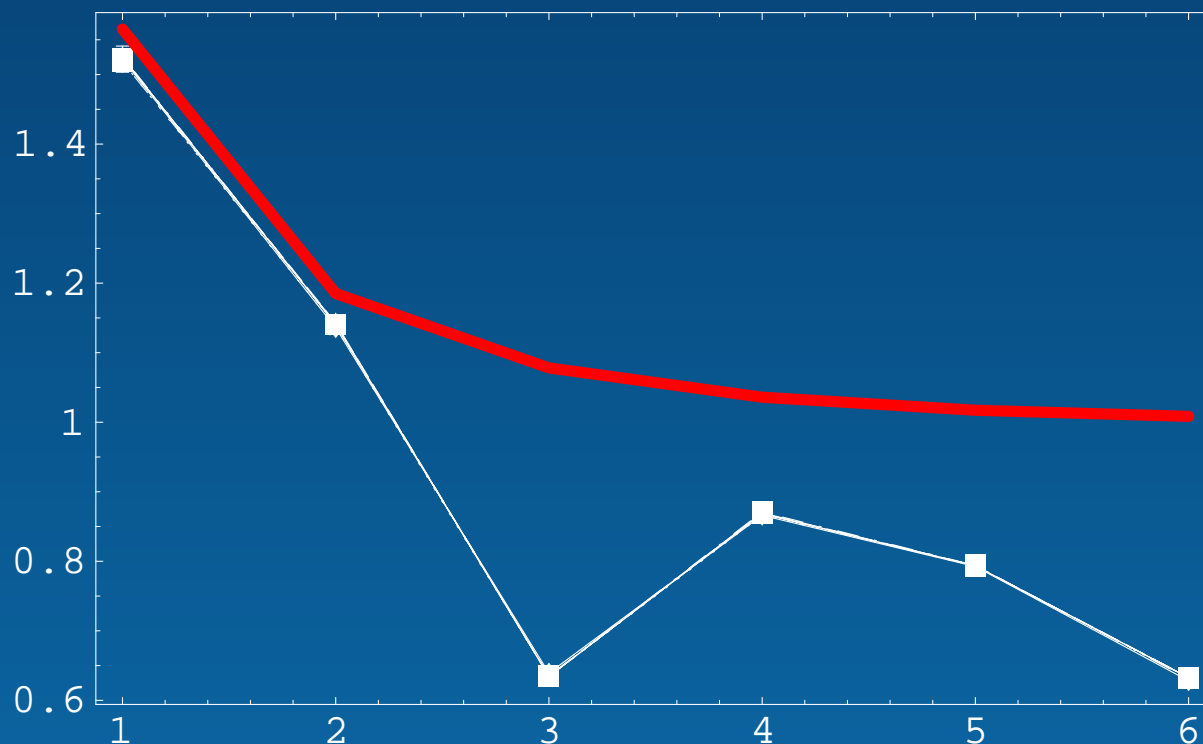
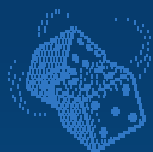


Fig. 2: Samples of \hat{H}_r for an order-3 chain with $H = 0.469$

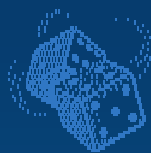


Summary

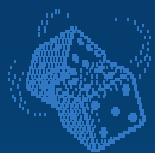
3 Types of Tests:

- Return Time based: **Universal Test**
- Relative Frequency based:
 - a) **Approximate Entropy**, I-Divergence
 - b) **Serial Test**, Monkey Test

Wegenkittl (IEEE 2002, PhD. Thesis): a) \approx b)



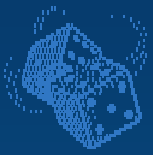
Return Time vs. Frequency: Sample Study



Return Time vs. Frequency: Sample Study

Idea: Simulate order κ chain with non-maximal Entropy

Vary “memory” κ of chain and “dimension” r of test

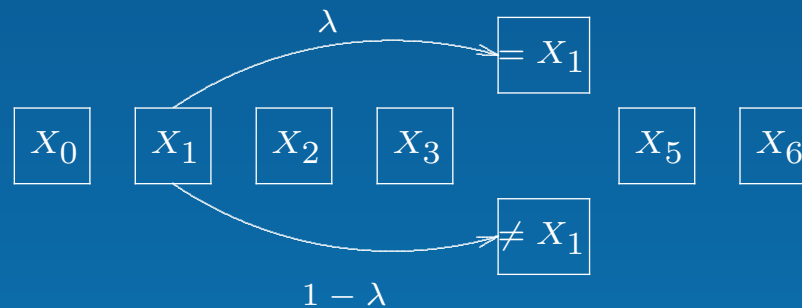


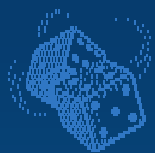
Sample Study: Defective Source

Let $m = 2$ (binary source) and

$$\tilde{\mathbb{P}} = (\tilde{p}_{ij})_{ij \in \mathcal{A}^2} = \begin{pmatrix} \lambda & 1 - \lambda \\ 1 - \lambda & \lambda \end{pmatrix}$$

and define transition probabilities $p_{a_{i-\kappa}, \dots, a_{i-1}, a_i} = \tilde{p}_{a_{i-\kappa} a_i}$

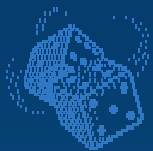




Defective Source Analysis

Then, for the chain $(\mathcal{A}, \mathbb{P}^\kappa(\lambda))$

- equidistribution on \mathcal{A}^κ is the stable distribution
- $H(\text{stable distribution}) = 1$, consequently
- $H(\mathcal{A}, \mathbb{P}^\kappa) = H(\lambda, 1 - \lambda) < 1 \Leftrightarrow \lambda \neq \frac{1}{2}$



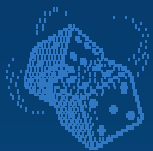
Defective Source Analysis

Then, for the chain $(\mathcal{A}, \mathbb{P}^\kappa(\lambda))$

- equidistribution on \mathcal{A}^κ is the stable distribution
- $H(\text{stable distribution}) = 1$, consequently
- $H(\mathcal{A}, \mathbb{P}^\kappa) = H(\lambda, 1 - \lambda) < 1 \Leftrightarrow \lambda \neq \frac{1}{2}$

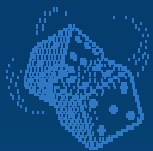
Some values of $H(\mathcal{A}, \mathbb{P}^\kappa)$:

λ	0.5	0.49	0.4	0.25	0.1
$H(\mathcal{A}, \mathbb{P}^\kappa)$	1.0	0.999711	0.970951	0.811278	0.468996



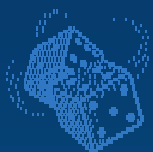
Sensitivity of \hat{H}_f and $\hat{\chi}$

- $\pi^{(r)}$ is equidistribution for all $r \leq \kappa$
- so that \hat{H}_f and $\hat{\chi}$ will not be able to see any defect until $r > \kappa$
- **but** (Chain Rule) \hat{H}_f (and $\hat{\chi}$) will see defect **for all** $r > \kappa$



Sensitivity of \hat{H}_r

- \hat{H}_r should be sensible to $\lambda \neq 1/2$ for all $r \geq 1$.
- is there any dependency on r with respect to fixed κ ?



Example revisited

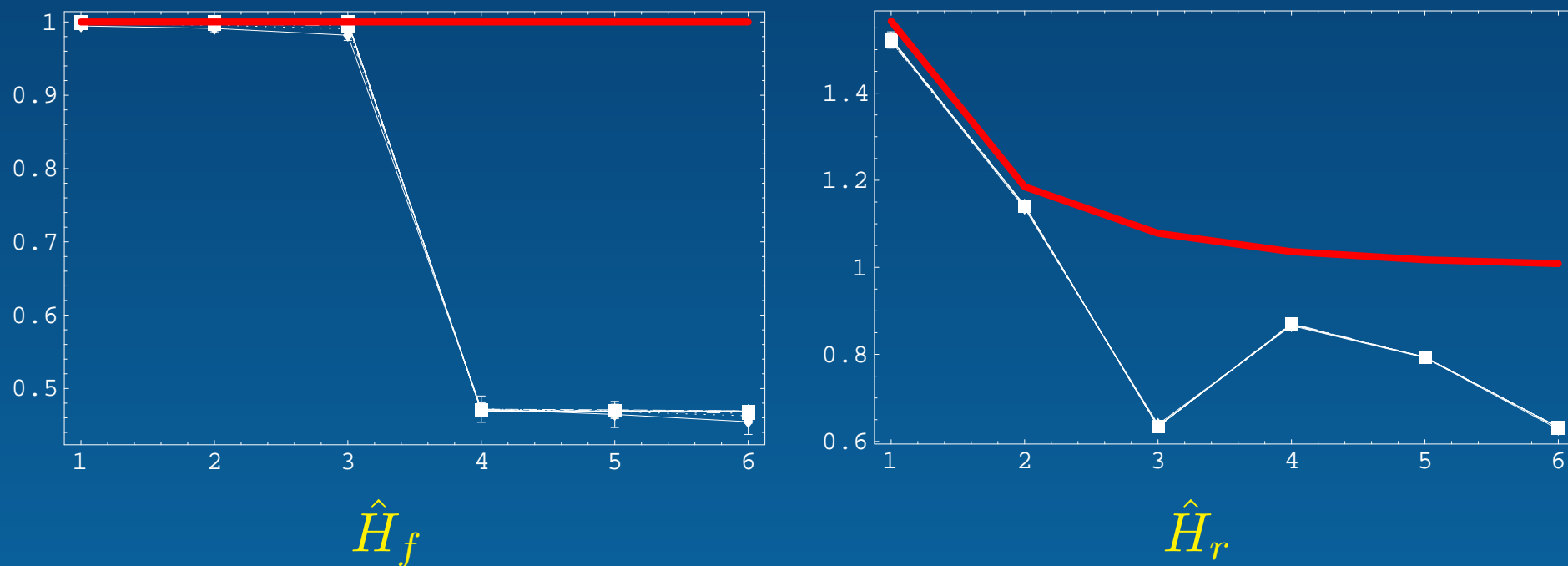
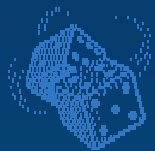


Fig. 3: Samples of \hat{H}_f and \hat{H}_r for $(\mathcal{A}, \mathbb{P}^3(1/2 - 0.4))$ with $H = 0.469$

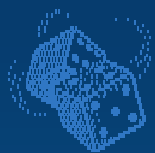


Speaking of samplesizes

In our setup,

ApEn and Serial Test use $\approx n$ samples,

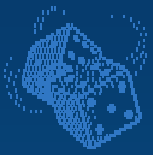
Universal Test uses $\approx n \cdot r$ samples plus warm-up



Speaking of samplesizes (ii)

$\log_2(n)$ needed to be able to detect Entropy defect (at 1% level of significance using $\hat{\chi}$):

r	1	2	4	8	12	16
$H = 0.999711$	15	15	16	19	23	27
$H = 0.468995$	4	4	5	8	12	16



Test Setup and Visualization

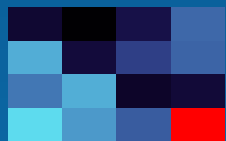
Compute 2-sided p-values according to given asymptotics

\hat{H}_f : dense case with χ^2 distribution

$\hat{\chi}$: dense case with χ^2 distribution

\hat{H}_r : normal distribution

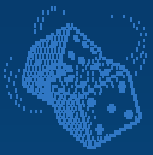
Repeat each test 16 times and arrange results into small rectangle:



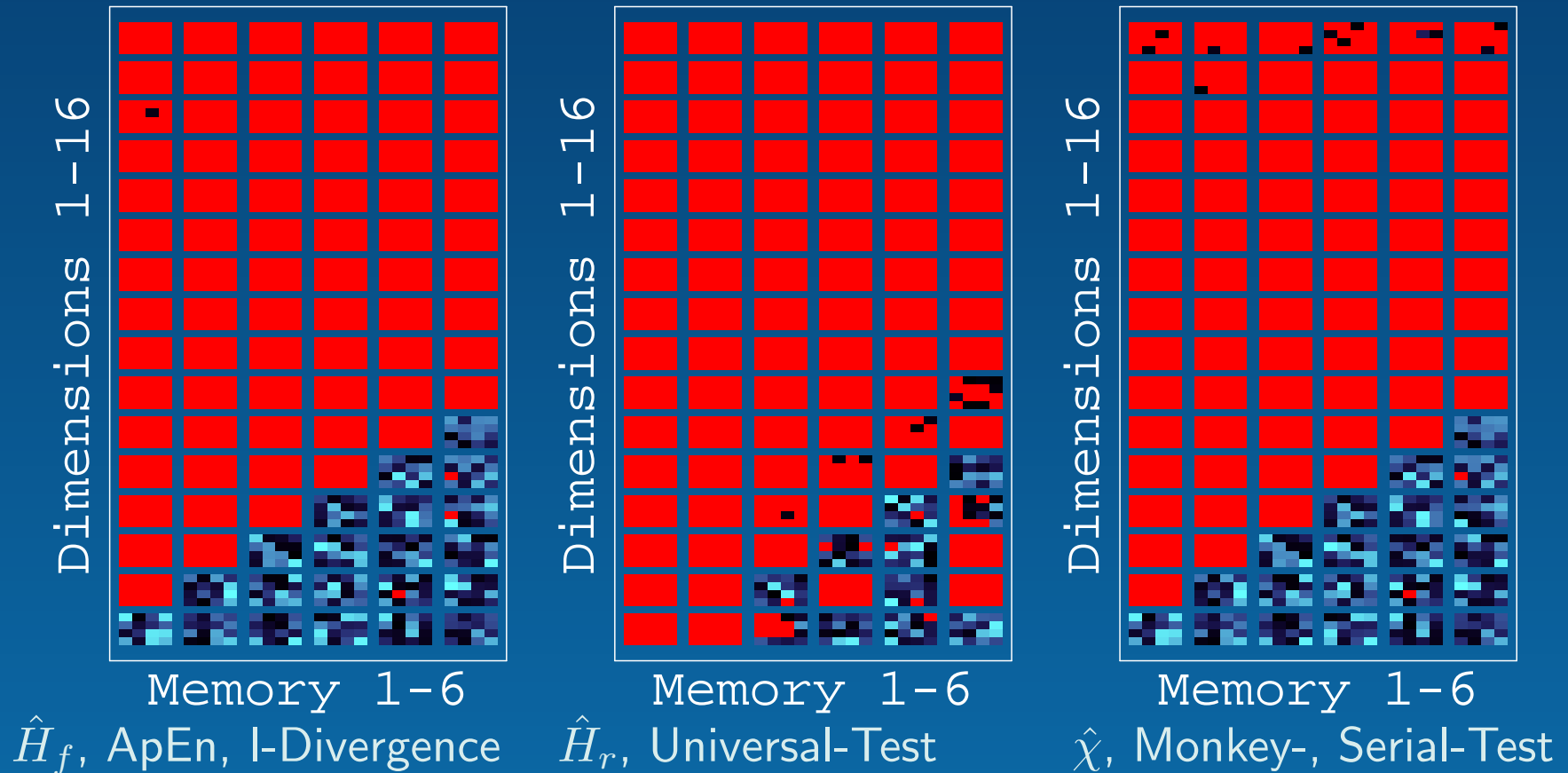
scale:



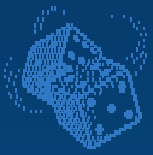
Red color indicates significance at 1% level.



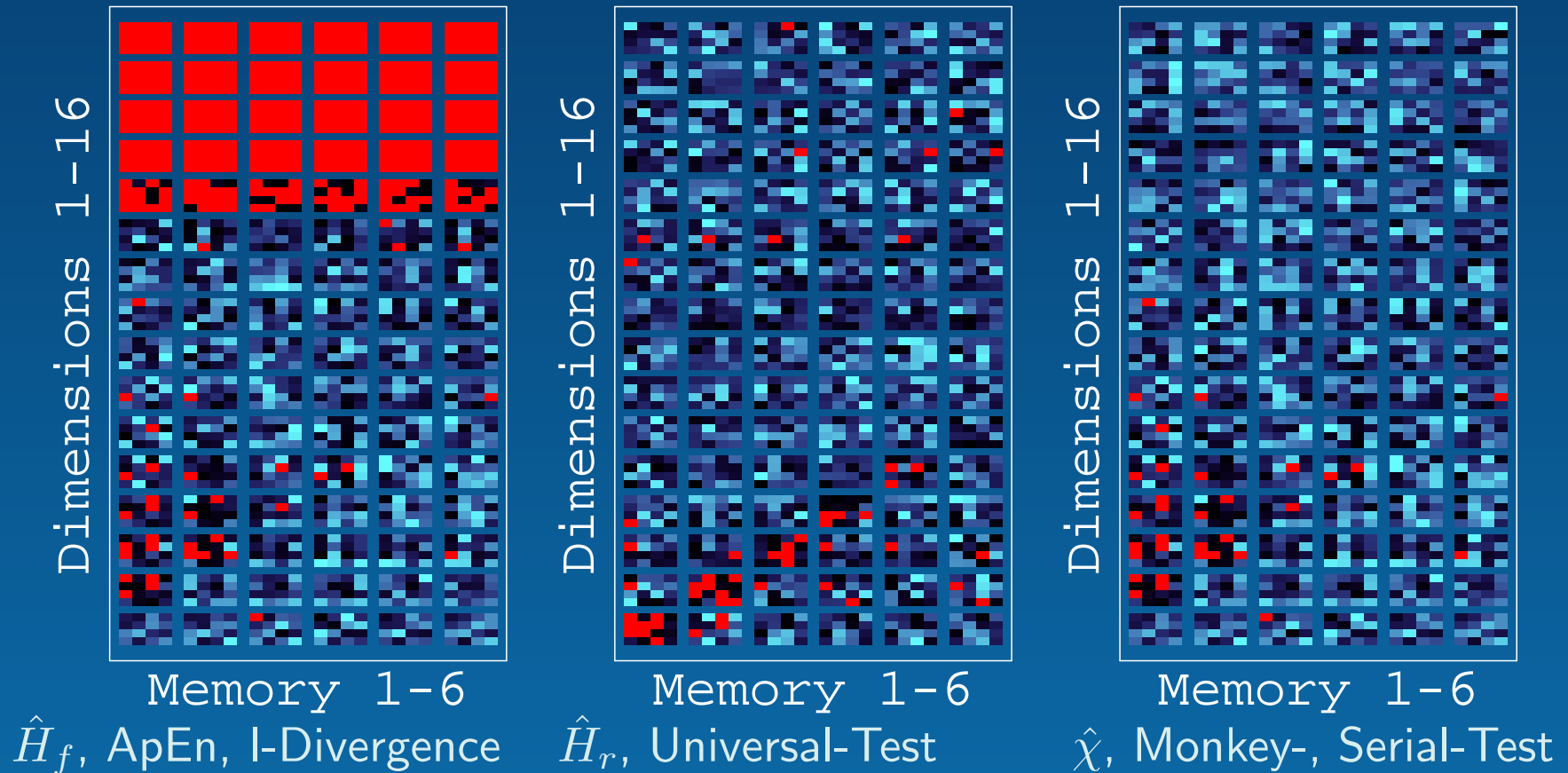
Easy case: $\lambda = 0.4, H = 0.970951$



Parameters: $n = 2^{14}, 1 \leq \kappa \leq 6, 1 \leq r \leq 16$



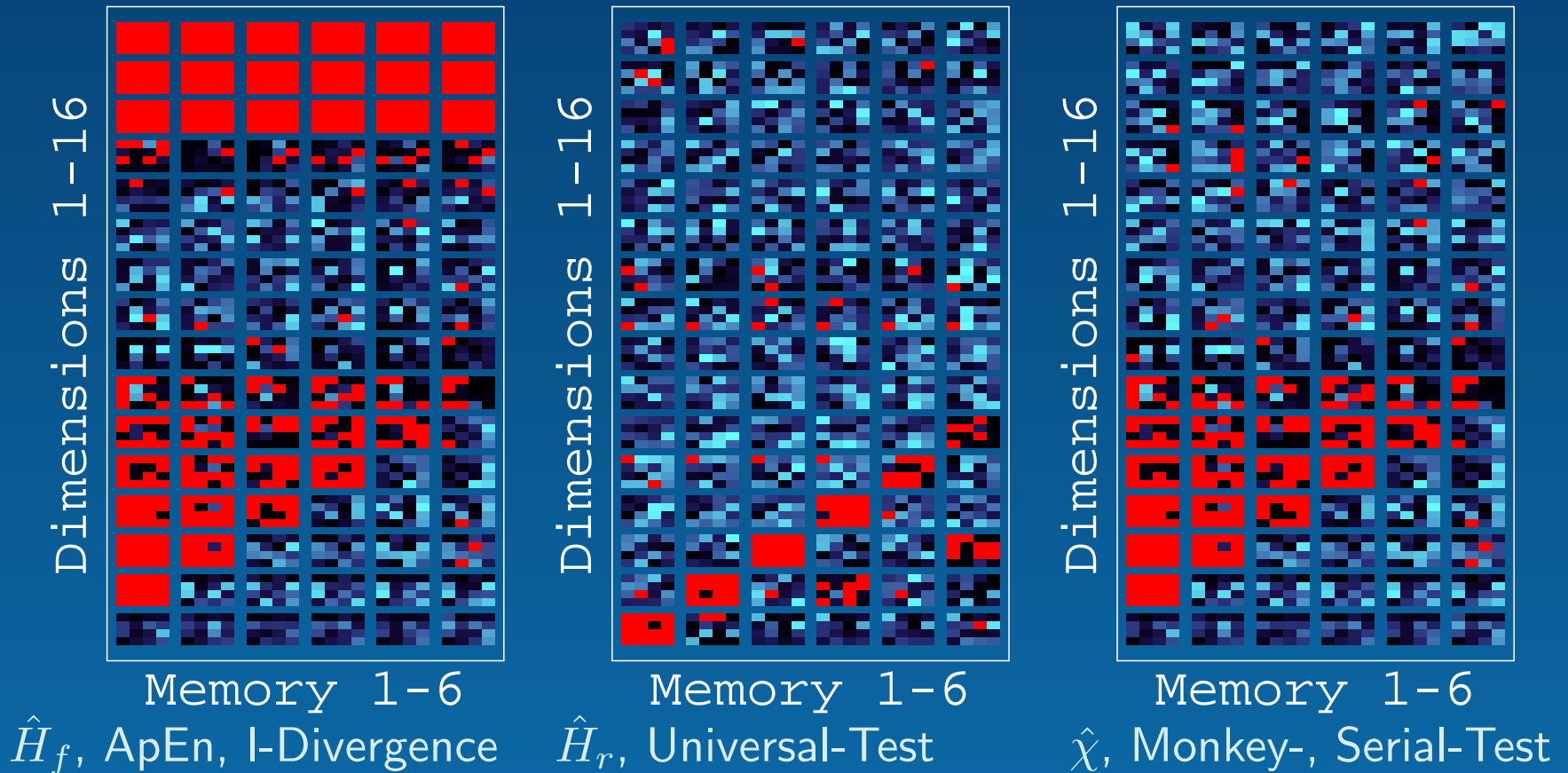
Hard case: $\lambda = 0.5$, $H = 1$, n too small



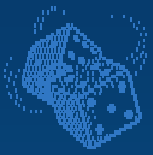
Parameters: $n = 2^{14}$, $1 \leq \kappa \leq 6$, $1 \leq r \leq 16$



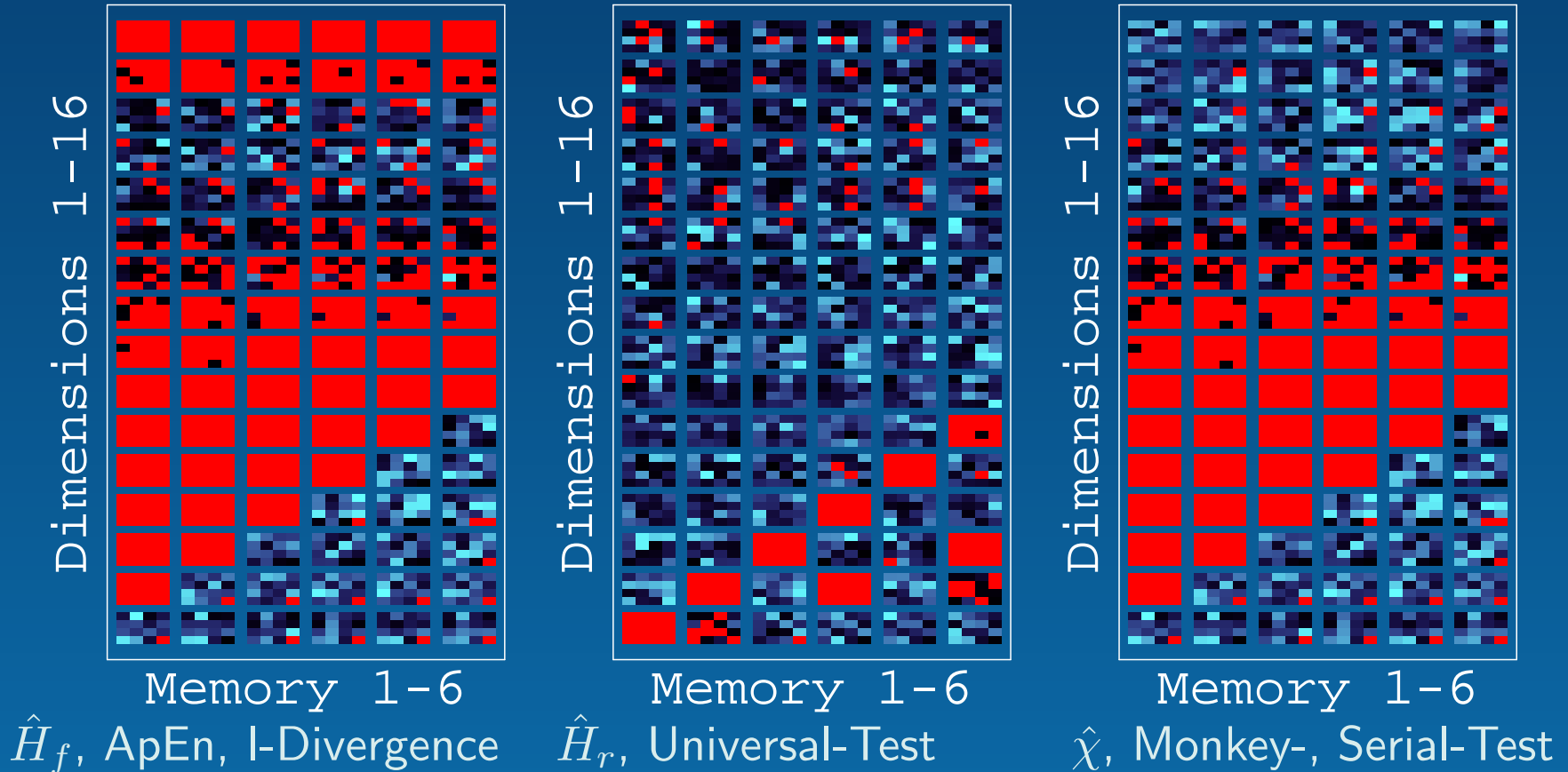
Hard case: $\lambda = 0.49$, $H = 0.999711$, n still small



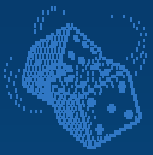
Parameters: $n = 2^{16}$, $1 \leq \kappa \leq 6$, $1 \leq r \leq 16$



Hard case: $\lambda = 0.49$, $H = 0.999711$, n o.k.



Parameters: $n = 2^{18}$, $1 \leq \kappa \leq 6$, $1 \leq r \leq 16$



Summary: Degrees of Universality

special purpose

multi purpose

universal

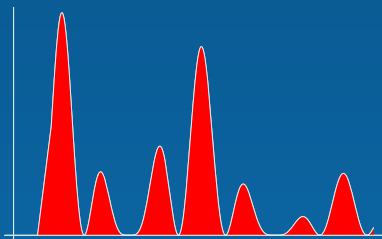
e.g. POKER TEST

UNIVERSAL TEST

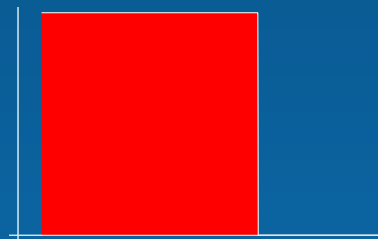
vary DIMENSION

SERIAL TEST

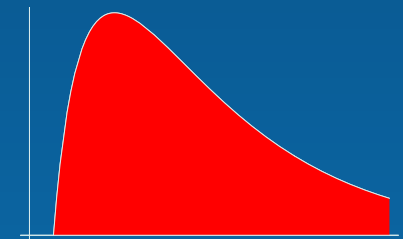
vary DIMENSION, RESOLUTION



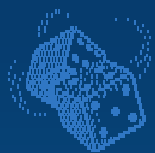
irregular



$r > \kappa$



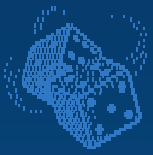
$r \in \mathbb{R}$



Summary: Correlation between Tests

Ability to detect H_1 :

- ApEn and Serial Tests: **similar, good results** if r large enough
- Universal Test: good results if r “correct” (critical!)



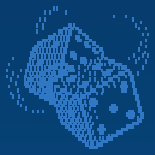
Summary: Correlation between Tests

Ability to detect H_1 :

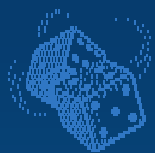
- ApEn and Serial Tests: **similar, good results** if r large enough
- Universal Test: good results if r “correct” (critical!)

Handling:

- Serial Tests: well understood, fast convergence
- ApEn is easy to interpret



Serial Tests in Applications

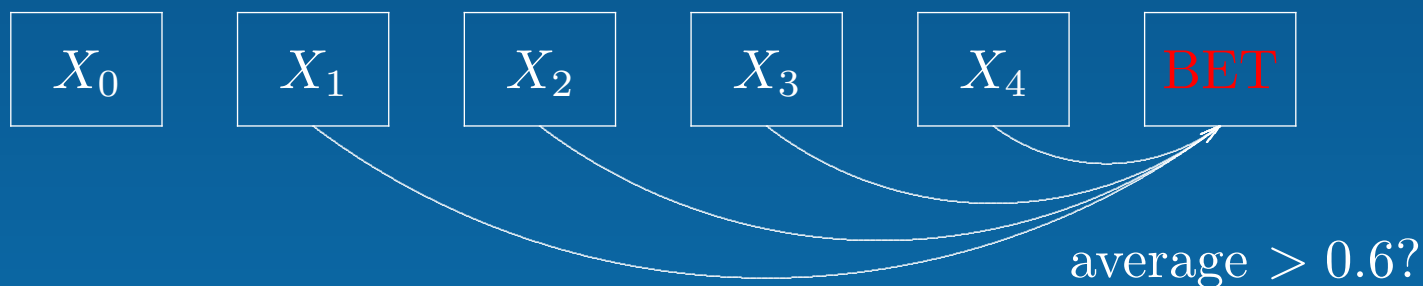


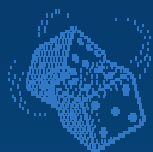
Dimension Reduction: Gambling Tests

Need $r \in 1 \dots 256$ (generating keys for cryptosystems)

Technique of **Gambling Tests** (Wegenkittl 2000):

reduce test dimension, preserve typical RNG correlations





Application: RNG241 of PDH

Study: Hardware Generators in Serial Tests

Example: RNG241

PDH International, Inc.

Precision Digital Hardware

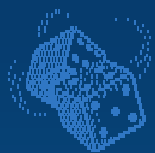
1250 E. Hallandale Beach Blvd. PH2

Hallandale FL 33009, USA

www.pdhint.com

E-mail: contact@pdhint.com





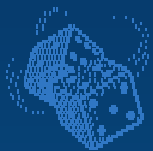
Application: RNG241 of PDH (ii)

radioactive α -decay RNG hardware
1 Kbps naturally perfect entropy
unaffected by external noise



plug & play serial-port box
integrated software solutions





Application: RNG241 of PDH (iii)

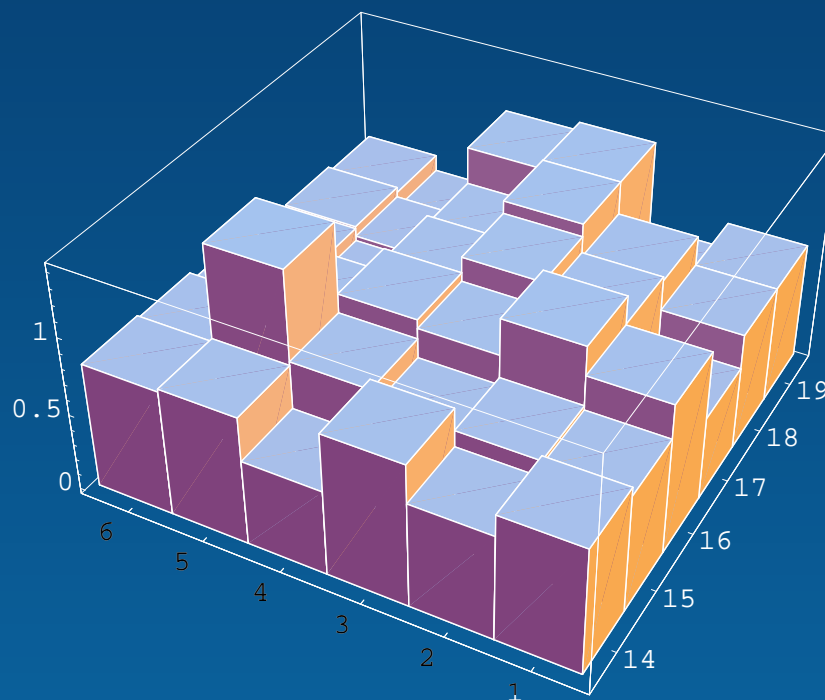
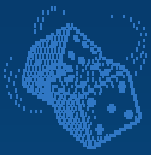


Fig. 4: Load Test: Each bar denotes the value of a single Kolmogorov-Smirnov statistic on 32 repetitions of the Load Test. Axes: dimension $s \in \{1, \dots, 6\}$ and the dual logarithm of the level-one sample size ranging from 14 to 19.



Application: RNG241 of PDH (iv)

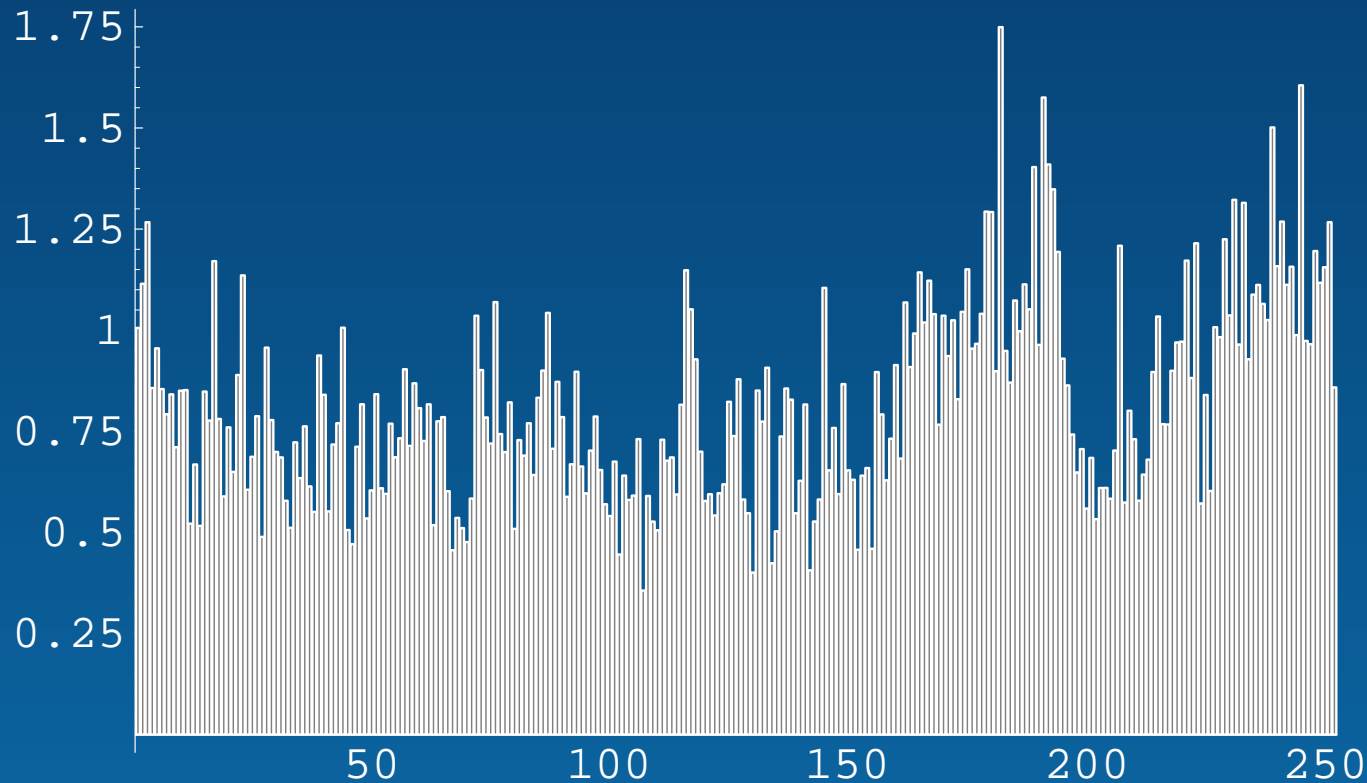
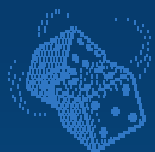


Fig. 5: A plot of the values of the Kolmogorov-Smirnov statistic for the Gambling Test with memory sizes $\lambda \in \{5, \dots, 256\}$



Application: RNG241 of PDH (v)

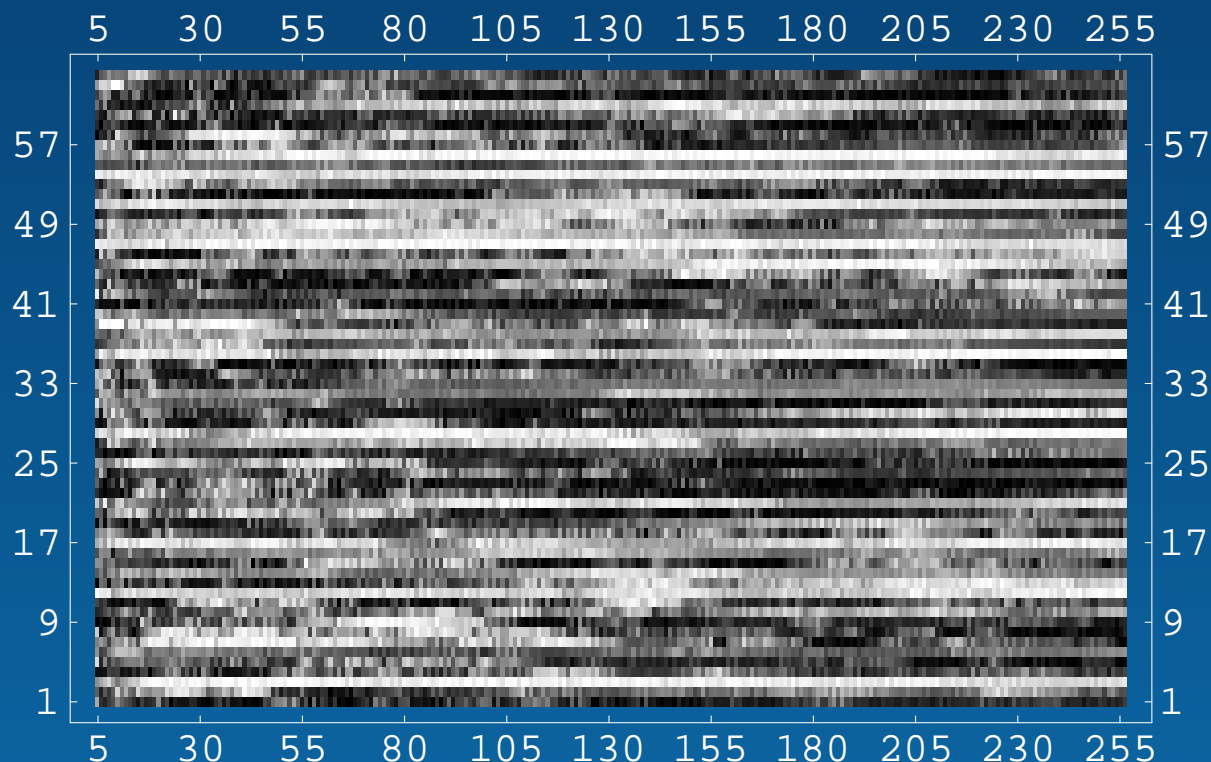
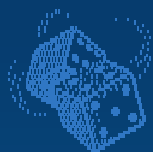


Fig. 6: Single Gambling Tests. Memory size $\lambda \in \{5, \dots, 256\}$, 64 independent samples of upper-tail probabilities of the Gambling Test.



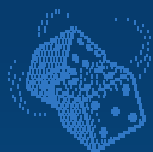
The End

Contact:

Stefan.Wegenkittl@sbg.ac.at

<http://random.mat.sbg.ac.at/team/ste.html>

Slides on web server.



Links and References

References

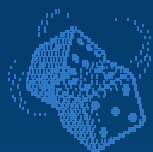
- [1] S. Wegenkittl. Monkeys, gambling, and return times: Assessing pseudorandomness. In P.A. Farrington, H.B. Nembhard, D.T. Sturrock, and G.W. Evans, editors, *Proceedings of the 1999 Winter Simulation Conference*, pages 625–631. IEEE Press, 1999.
- [2] S. Wegenkittl. Entropy estimators and serial tests for ergodic chains. *IEEE Transactions on Information Theory*, **47**(6):2480–2489, Sep 2001.
- [3] S. Wegenkittl. Gambling tests for pseudorandom number generators. *Mathematics and Computers in Simulation*, 55(1–3):281–288, 2001.
- [4] S. Wegenkittl. A generalized ϕ -divergence for asymptotically multivariate normal models, 2002. To appear in *Journal of Multivariate Analysis*, Vol. 84, No. 1, 2003, available via IDEALFirst.
- [5] S. Wegenkittl and M. Matsumoto. Getting rid of correlations among pseudorandom numbers: Discarding versus tempering. *ACM Trans. Modeling and Computer Simulation*, **9**(3):282–294, 1999.
- [6] S. Wegenkittl, “Generalized ϕ -Divergence and Frequency Analysis in Markov Chains,”



Ph.D. thesis, Universität Salzburg, Österreich, 1998, HTML version:
<http://random.mat.sbg.ac.at>

- [7] P. L'Ecuyer, R. Simard, and S. Wegenkittl, "Sparse serial tests of uniformity for random number generators," Accepted for publication in SISC, 2002.
- [8] H. Leeb and S. Wegenkittl, "Inversive and linear congruential pseudorandom number generators in empirical tests.," *ACM Trans. Modeling and Computer Simulation*, vol. **7**, no. 2, pp. 272–286, 1997.
- [9] S. Wegenkittl, "The PLAB picturebook: Load tests and ultimate load tests, part I," Report no. 1, PLAB – reports, University of Salzburg, 1997.
- [10] P. Hellekalek, "Good random number generators are (not so) easy to find," *Mathematics and Computers in Simulation*, vol. **46**, pp. 485–505, 1998.
- [11] U.M. Maurer, "A universal statistical test for random bit generators," *J. Cryptology*, vol. **5**, pp. 89–105, 1992.
- [12] I. Csiszár, "Eine informationstheoretische Ungleichung und ihre Anwendung auf den Beweis der Ergodizität von Markoffschen Ketten," *Magyar Tud. Akad. Mat. Kutató Int. Közl*, vol. **8**, pp. 85–108, 1963.
- [13] K. Pearson, "On the criterion that a given system of deviations from the probable in the case of a correlated system of variables is such that it can be reasonably supposed to have arisen from random sampling.," *Philos. Magazine Series*, vol. **50**, no. 5, pp. 157–172, 1900.

- [14] S. Kullback and R. Leibler, “On information and sufficiency,” *Ann. Math. Statist.*, vol. 22, pp. 79–86, 1951.
- [15] I. J. Good, “The serial test for sampling numbers and other tests for randomness,” *Proc. Cambridge Philosophical Society*, vol. 49, pp. 276–284, 1953.
- [16] G. Marsaglia, “A current view of random number generators,” in *Computer Science and Statistics: The Interface*, L. Billard, Ed. 1985, pp. 3–10, Elsevier Science Publishers B.V.
- [17] G.H. Choe and D.H. Kim, “The probability distribution of the first return time,” Submitted for publication, 1999.
- [18] A. Wyner and J. Ziv, “Some asymptotic properties of the entropy of stationary ergodic data source with applications to data compression,” *IEEE Trans. Information Theory*, vol. 35, pp. 1250–1258, 1989.
- [19] D. Ornstein and B. Weiss, “Entropy and data compression schemes,” *IEEE Trans. Information Theory*, vol. 39, pp. 78–93, 1993.
- [20] J. S. Coron and D. Naccache, “An Accurate Evaluation of Maurer’s Universal Test,” in *Proceedings of Selected Areas in Cryptography 98*. 1998, Lecture Notes in Computer Science 1556, pp. 57–71, Springer.
- [21] G.H. Choe and D.H. Kim, “Average convergence rate of the first return time,” Submitted for publication, 1999.



Jumpstation

- New Challenges for Empirical Testing
- Entropy Primer
- Computing Entropy
- Tests for Randomness based on Entropy
- Construction of Tests
- Sample Study
- Results of Study
- Correlation between Tests
- Application to Cryptographic Generator
- Links and References