Report of Entropy estimates based on NIST SP 800-90B non-IID track

2023-Aug-06 09:10:02.331252

1 Identification information

1.1 Identification of acquisition data from entropy source

Table 1 Identification information of acquisition data from entropy source

URL of the acquisition data	`https://github.com/usnistgov/SP800-90B_EntropyAssessment/blob/master/bin/biased-random-bits.bin`
SHA-256 hash value of the acquisition data [hex]	`481cdac6 e2d65d45 656c2123 4125eaf2 6df18a49 037f15ff d40002b3 5e547586`

- Name of the submitter of the acquisition data :
- Brief explanation of the acquisition data (or entropy source) :

1.2 Identification of analysis environment

Table 2 Identification information of analysis environment

Analysis tool	Name	Another entropy estimation tool with extensions
	Versioning information	1.0.50
	built as	64-bit application
	built by	Intel C++ Compiler (`__INTEL_LLVM_COMPILER`: 20230200)
	linked libraries	Boost C++ 1.82.0
Analysis environment	Hostname	[redacted]
	CPU information	AMD Ryzen [redacted]
	Physical memory size	[redacted] MiB
	OS information	Windows 10 or greater 64-bit
	Username	[redacted]

1.3 Identification of analysis conditions

Table 3 Identification information of analysis conditions

Number of samples	1000000
Bits per sample	1

1.4 Identification of analysis method

NIST SP 800-90B [1] 6.3 with corrections [2] is applied

2 Executive summary

2.1 Numerical results of min-entropy estimates based on non-IID track

Table 4 Numerical results

Estimator	$H_{\text{bitstring}}$ [a] [bit / 1 - bit]	Notes to $H_{\text{bitstring}}$
The Most Common Value Estimate	0.0286331	see 3.1
The Collision Estimate	0.0285138	see 3.2
The Markov Estimate	0.029123	see 3.3
The Compression Estimate	0.0177666	see 3.4
The t-Tuple Estimate	0.0264893	see 3.5
The Longest Repeated Substring (LRS) Estimate	0.0558814	see 3.6
Multi Most Common in Window Prediction Estimate	0.0286349	see 3.7
The Lag Prediction Estimate	0.0405998	see 3.8
The MultiMMC Prediction Estimate	0.0286346	see 3.9
The LZ78Y Prediction Estimate	0.028635	see 3.10
The intial entropy source estimate [bit / 1 -bit] $H_I = H_{\text{bitstring}}$	0.0177666	

[a] Entropy estimate of the sequential dataset [source: NIST SP 800-90B [1] 3.1.3]

2.2 Visual comparison of min-entropy estimates from binary samples

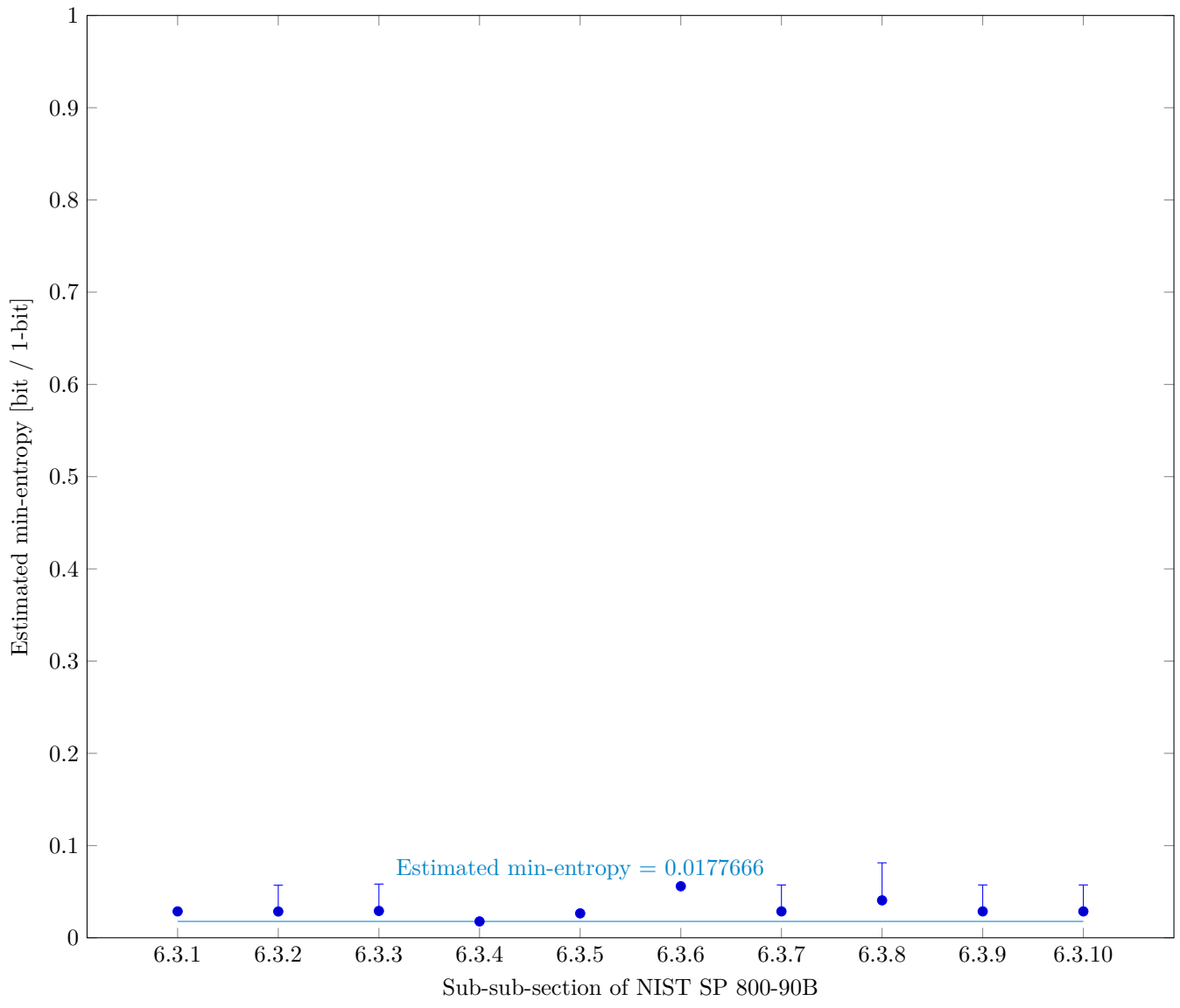

Fig. 1 Estimated Min-Entropy using §6.3 of NIST SP 800-90B

3 Detailed results of analysis from original samples

3.1 The Most Common Value Estimate (NIST SP 800-90B Section 6.3.1)

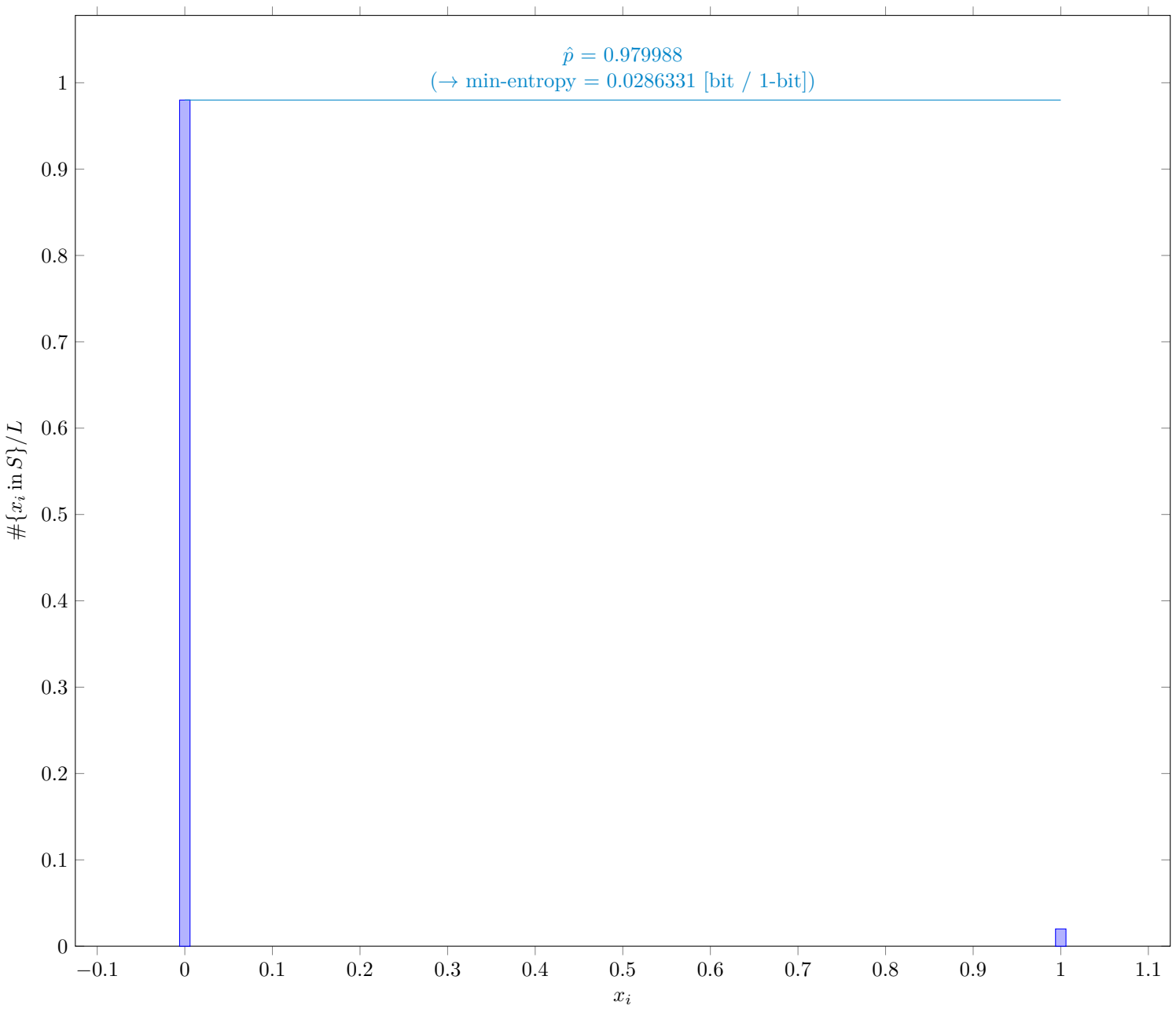

Fig. 2 Distribution of x_i

3.1.1 Supplemental information for traceability

Table 5 Supplemental information for traceability (NIST SP 800-90B Section 6.3.1)

Symbol	Value
mode	979988
$\hat{p}$	0.979988
p_u	0.980349

3.2 The Collision Estimate (NIST SP 800-90B Section 6.3.2)

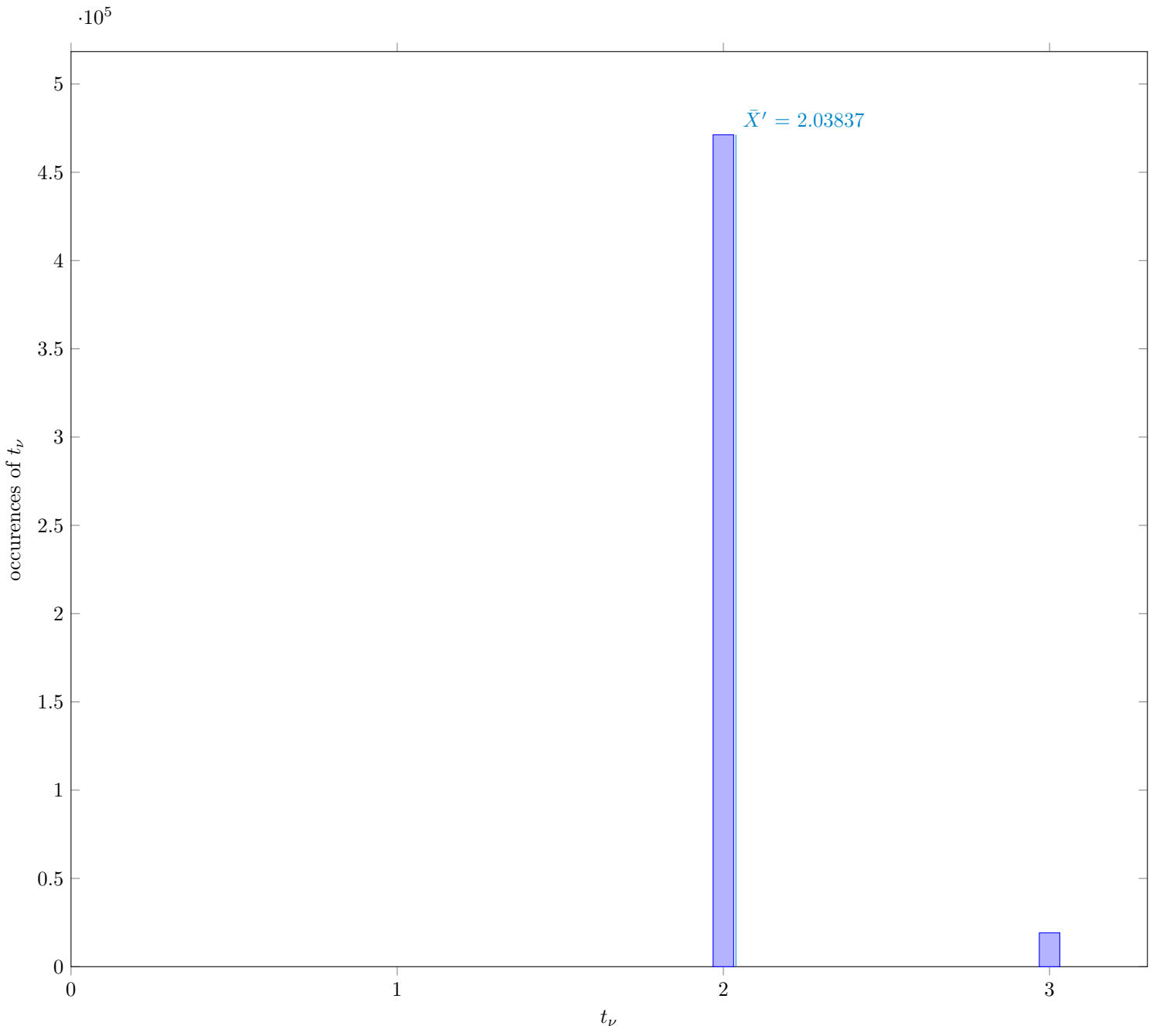

Fig. 3 Distribution of intermediate value t_ν

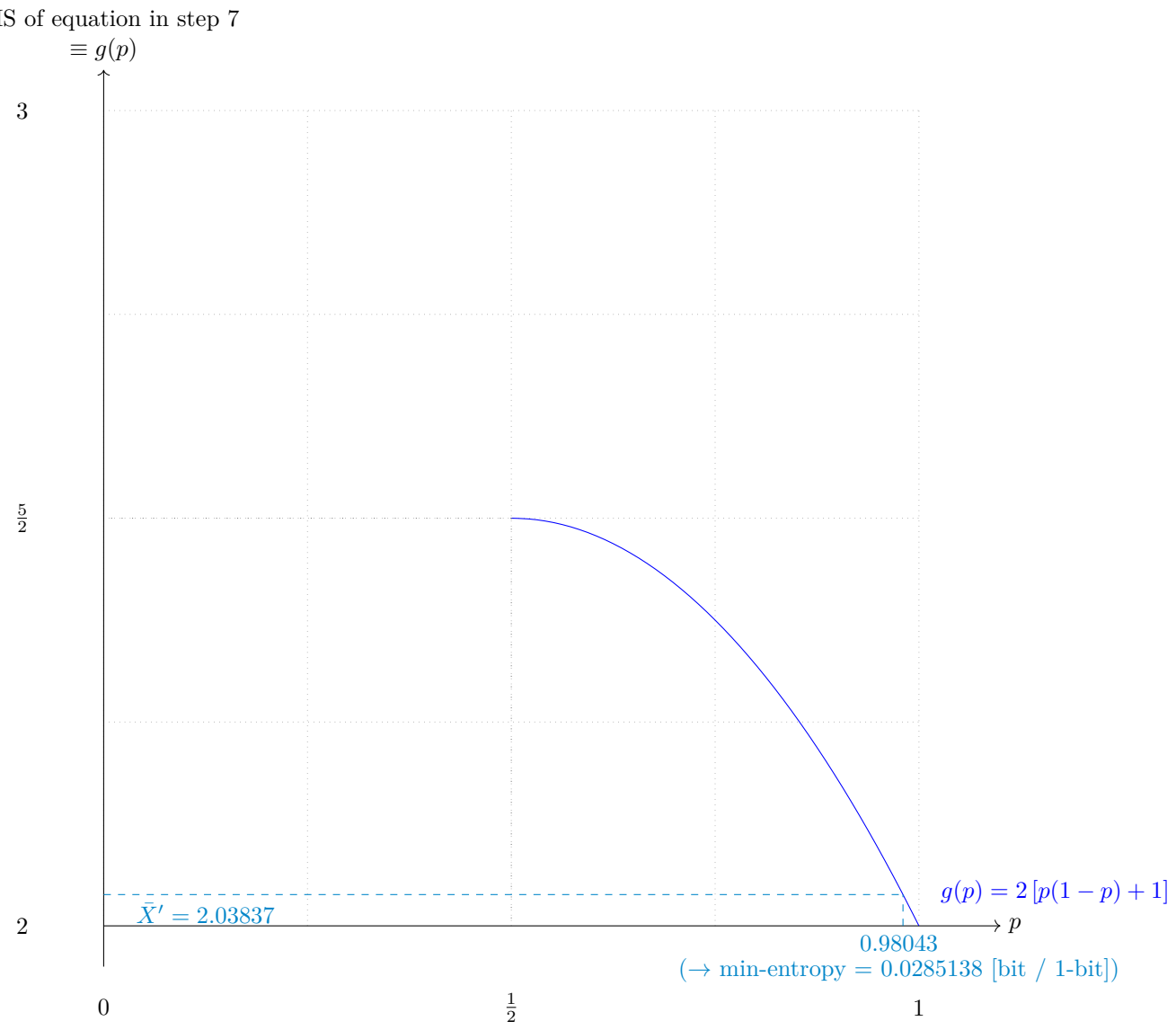

Fig. 4 Solution to the equation in step 7

3.2.1 Supplemental information for traceability

Table 6 Supplemental information for traceability (NIST SP 800-90B Section 6.3.2)

Symbol	Value
p	0.98043
$\bar{X}$	2.03909
$\bar{X}'$	2.03837
$\hat{\sigma}$	0.193803

3.3 The Markov Estimate (NIST SP 800-90B Section 6.3.3)

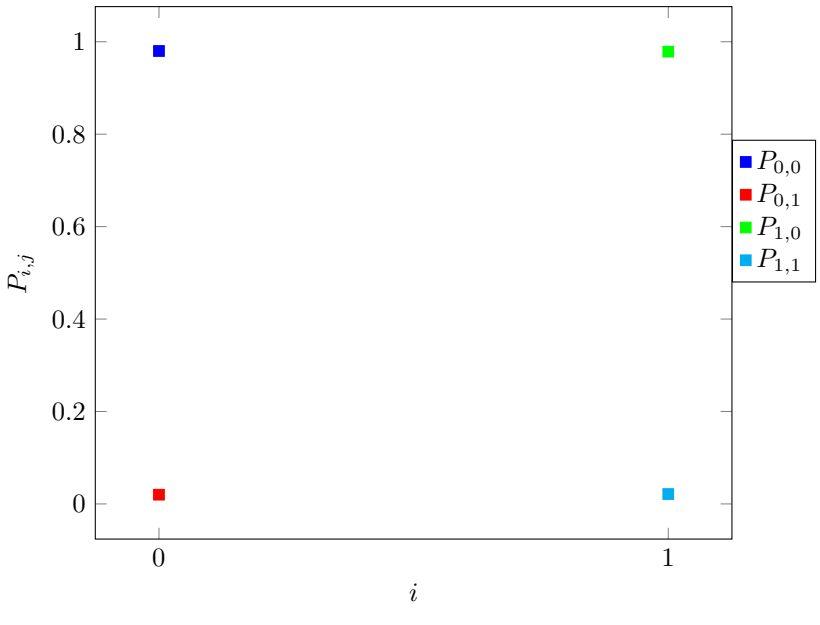

Fig. 5 Transition probability $P_{i,j}$ of §6.3.3 of NIST SP 800-90B

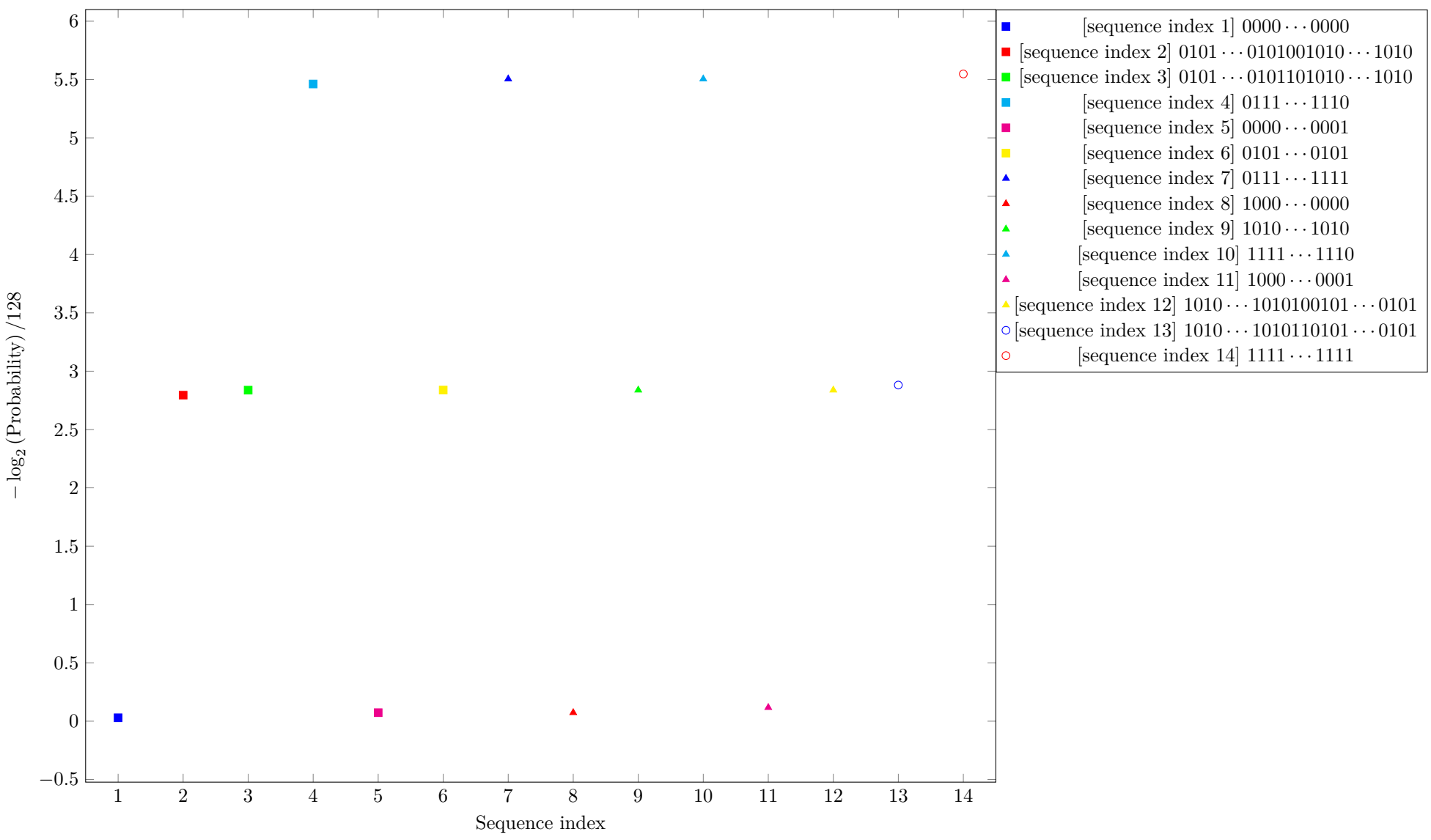

Fig. 6 Estimated Min-Entropy using §6.3.3 of NIST SP 800-90B

3.4 The Compression Estimate (NIST SP 800-90B Section 6.3.4)

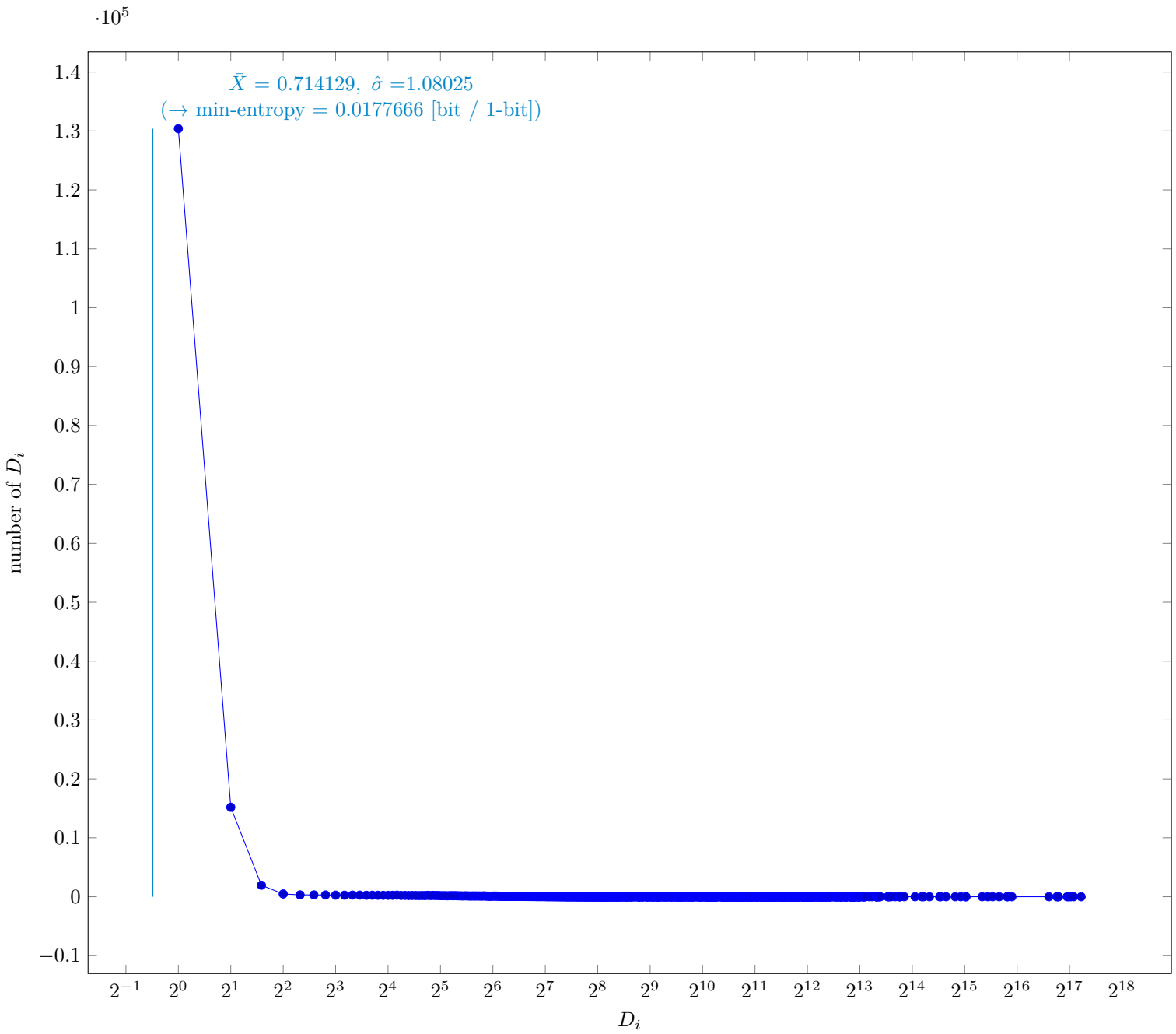

Fig. 7 Distribution of intermediate value D_i

3.4.1 Supplemental information for traceability

Table 7 Supplemental information for traceability (NIST SP 800-90B Section 6.3.4)

Symbol	Value
p	0.928775
$\bar{X}$	0.714129
$\hat{\sigma}$	1.08025
$\bar{X}'$	0.707292

3.5 The t-tuple Estimate (NIST SP 800-90B Section 6.3.5)

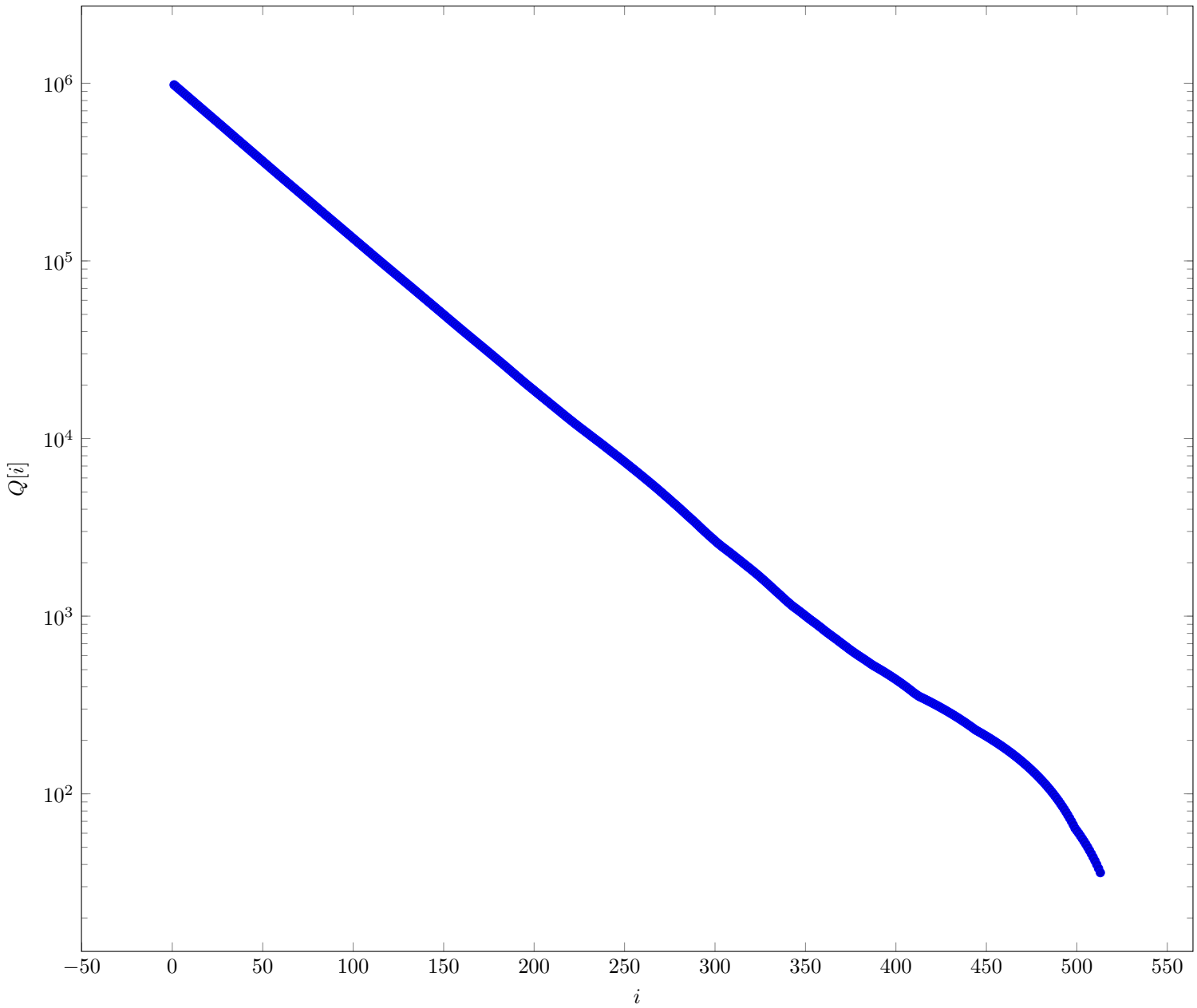

Fig. 8 Intermediate value $Q[i]$ in §6.3.5 of NIST SP 800-90B

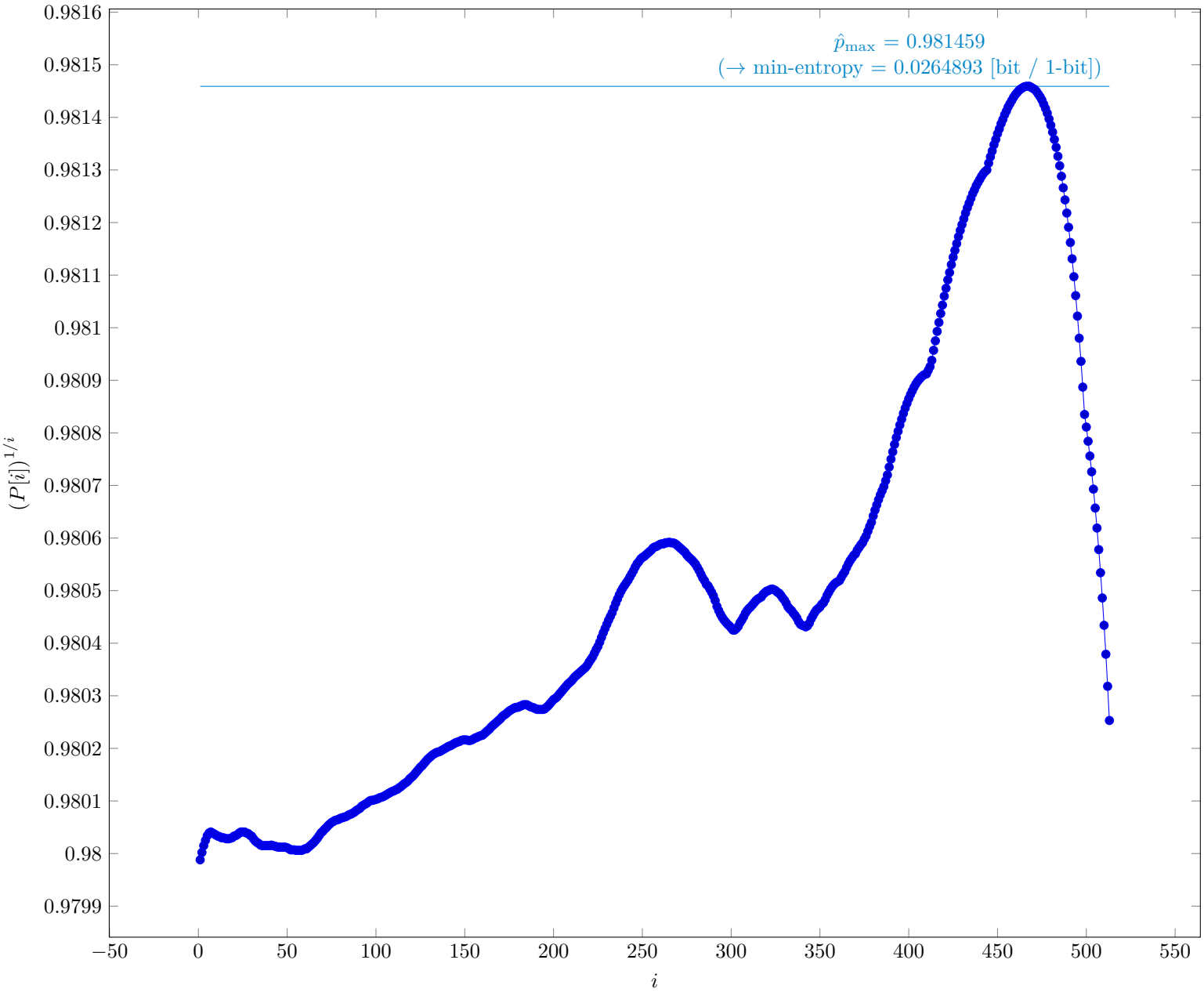

Fig. 9 $P[i]^{1/i}$ in §6.3.5 of NIST SP 800-90B

3.5.1 Supplemental information for traceability

Table 8 Supplemental information for traceability (NIST SP 800-90B Section 6.3.5)

Symbol	Value
t	513
$\hat{p}_{\max}$	0.981459
p_u	0.981807

3.6 The LRS Estimate (NIST SP 800-90B Section 6.3.6)

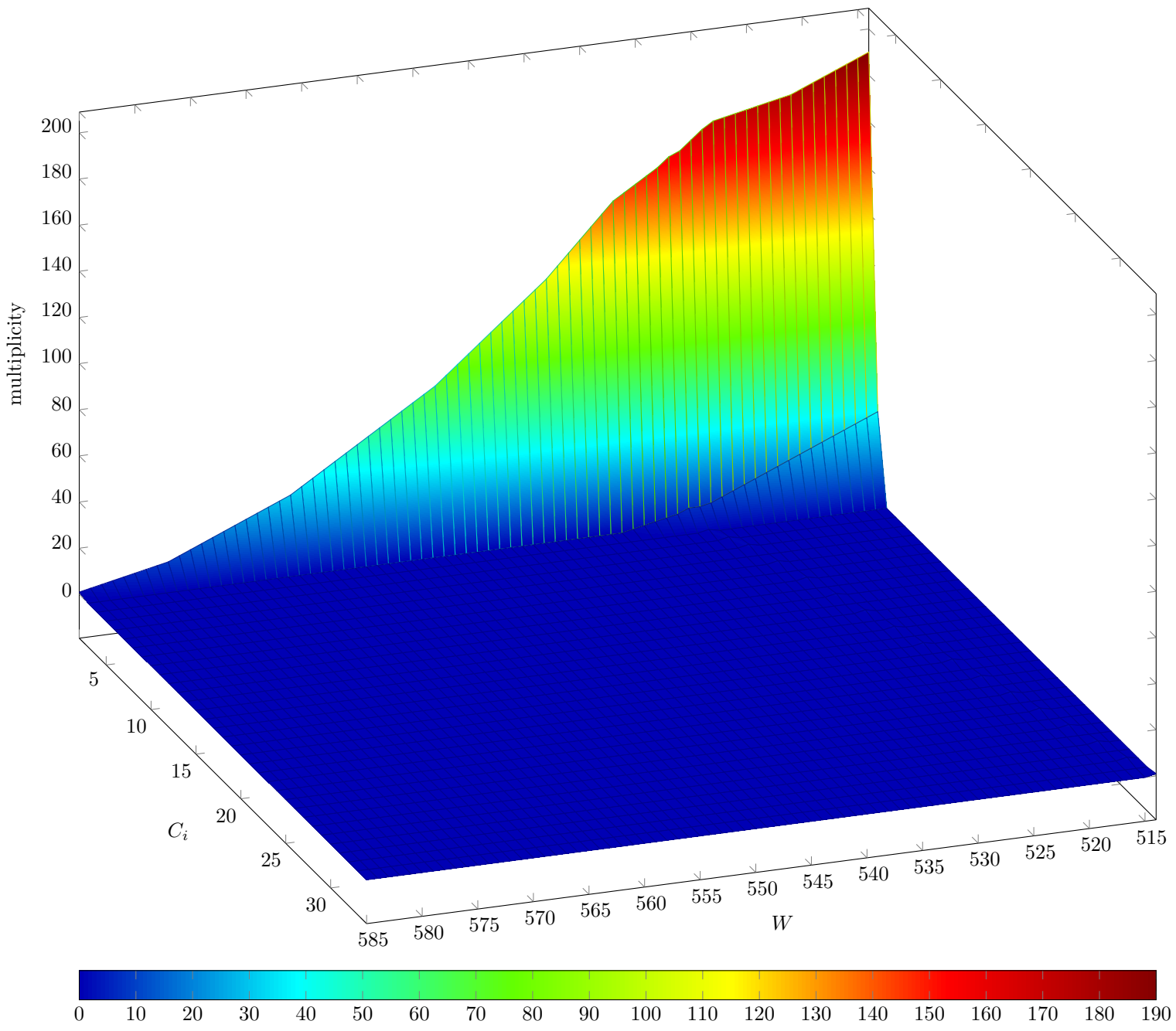

Fig. 10 Estimated W-tuple collision probability in Step 3 of §6.3.6 of NIST SP 800-90B

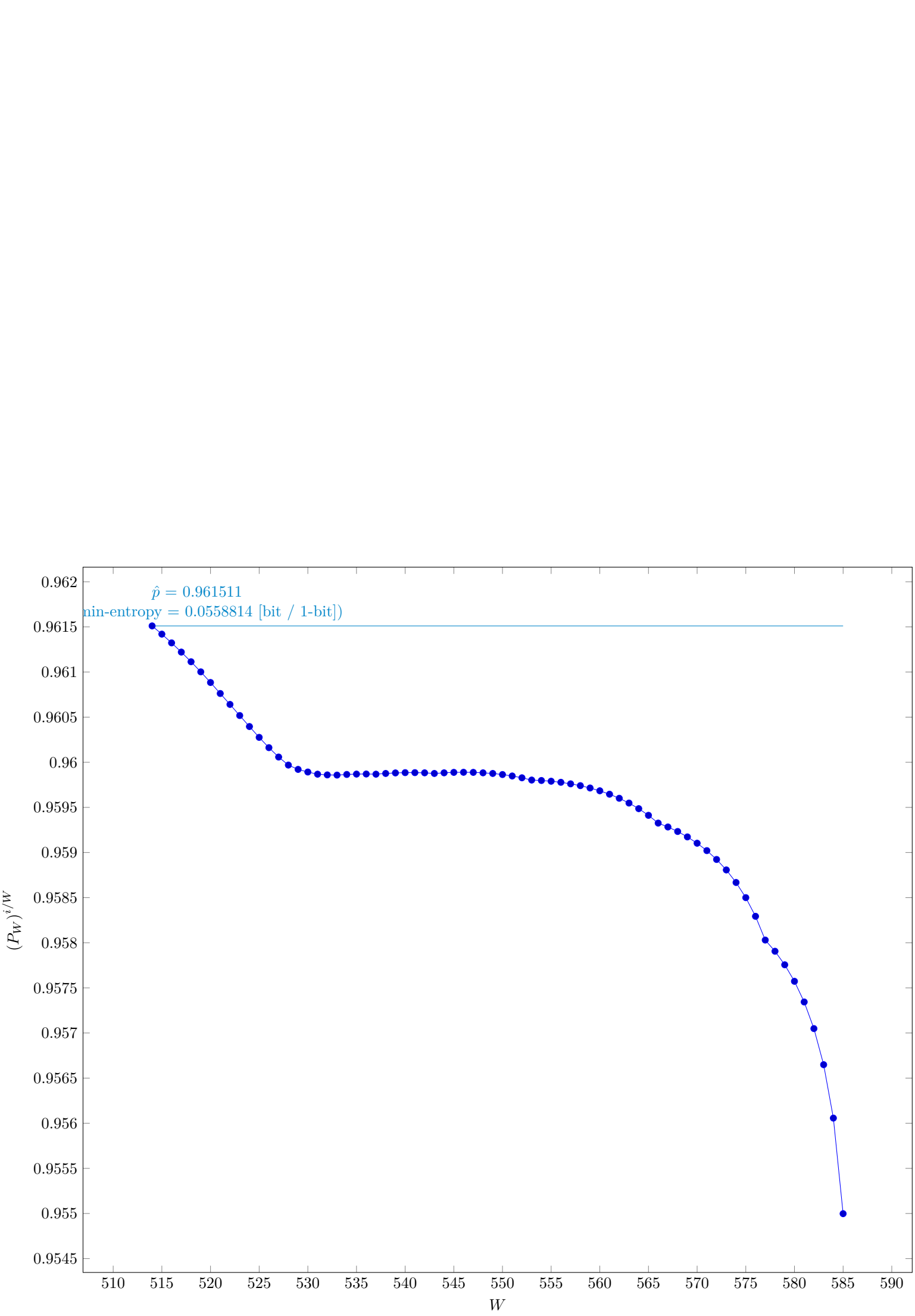

Fig. 11 Estimated average collision probability per string symbol in Step 3 of §6.3.6 of NIST SP 800-90B

3.6.1 Supplemental information for traceability

Table 9 Supplemental information for traceability (NIST SP 800-90B Section 6.3.6)

Symbol	Value
u	514
v	585
$\hat{p}$	0.961511
p_u	0.962007

3.7 Multi Most Common in Window Prediction Estimate (NIST SP 800-90B Section 6.3.7)

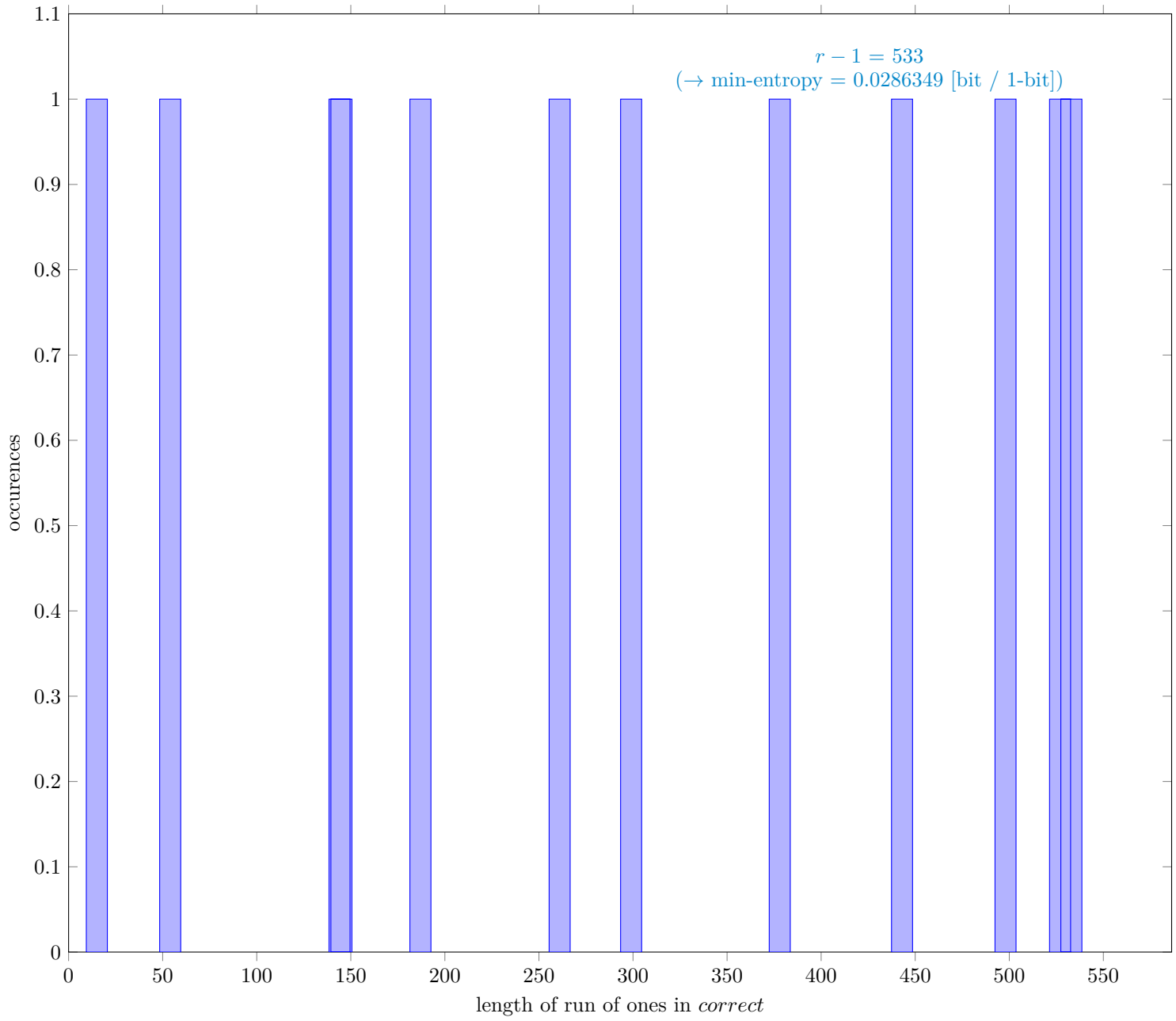

Fig. 12 Distribution of *correct*

3.7.1 Supplemental information for traceability

Table 10 Supplemental information for traceability (NIST SP 800-90B Section 6.3.7)

Symbol	Value
N	999937
C	979925
P_{global}	0.979987
P'_{global}	0.980347
r	534
P_{local}	0.972635

3.8 Lag Prediction Estimate (NIST SP 800-90B Section 6.3.8)

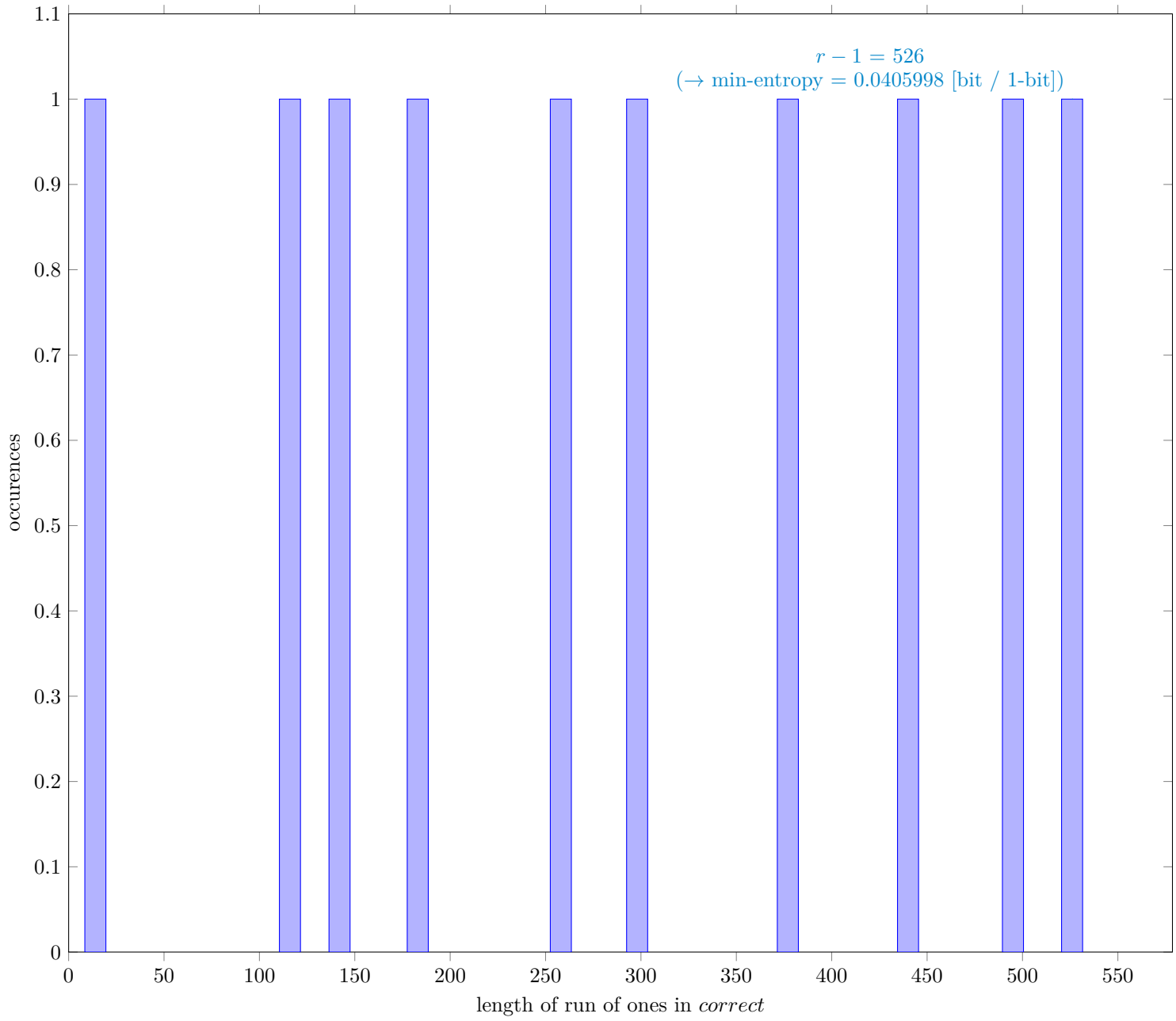

Fig. 13 Distribution of *correct*

3.8.1 Supplemental information for traceability

Table 11 Supplemental information for traceability (NIST SP 800-90B Section 6.3.8)

Symbol	Value
N	999999
C	959838
P_{global}	0.959839
P'_{global}	0.960345
r	527
P_{local}	0.972251

3.9 The MultiMMC Prediction Estimate (NIST SP 800-90B Section 6.3.9)

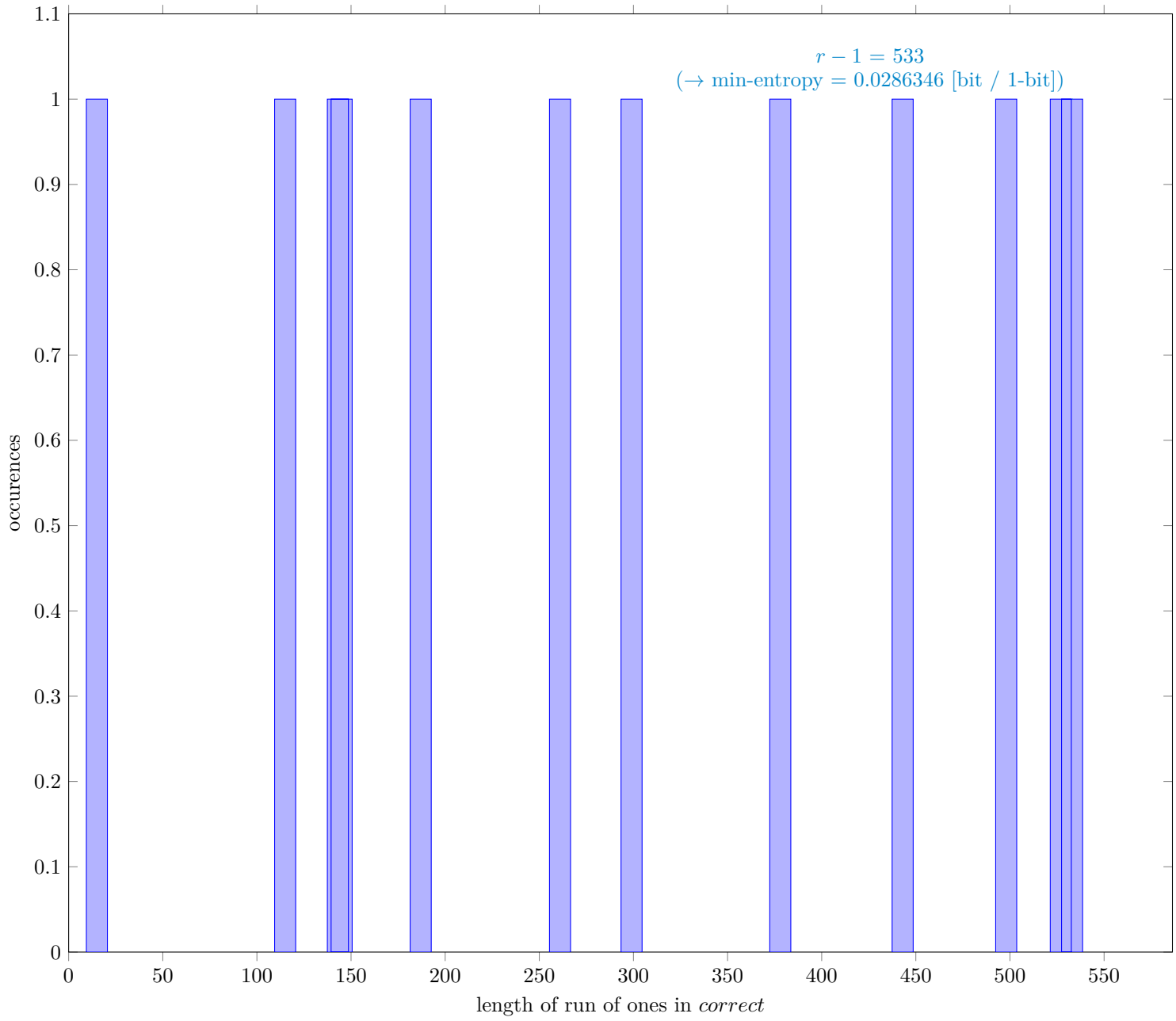

Fig. 14 Distribution of *correct*

3.9.1 Supplemental information for traceability

Table 12 Supplemental information for traceability (NIST SP 800-90B Section 6.3.9)

Symbol	Value
N	999998
C	979985
P_{global}	0.979987
P'_{global}	0.980348
r	534
P_{local}	0.972635

3.10 The LZ78Y Prediction Estimate (NIST SP 800-90B Section 6.3.10)

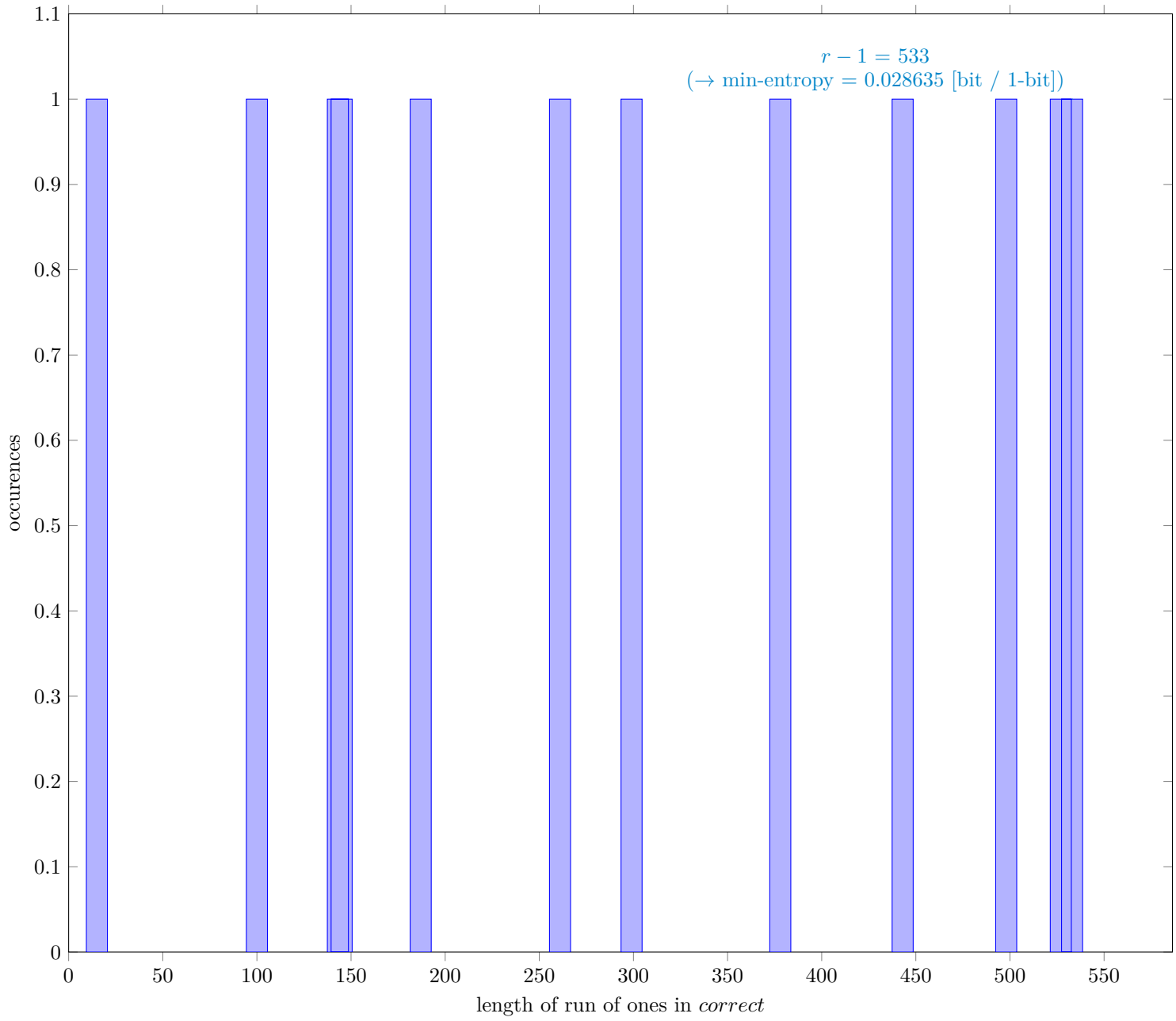

Fig. 15 Distribution of *correct*

3.10.1 Supplemental information for traceability

Table 13 Supplemental information for traceability (NIST SP 800-90B Section 6.3.10)

Symbol	Value
N	999983
C	979970
P_{global}	0.979987
P'_{global}	0.980347
r	534
P_{local}	0.972635

3 References

[1] Meltem Sönmez Turan, Elaine Barker, John Kelsey, Kerry A. McKay, Mary L. Baish, Mike Boyle *Recommendation for the Entropy Sources Used for Random Bit Generation*, NIST Special Publication 800-90B, Jan. 2018 `https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90B.pdf`

[2] G. Sakurai, *Proposed list of corrections for NIST SP 800-90B 6.3 Estimators*, Dec. 2022 `https://github.com/g-g-sakura/AnotherEntropyEstimationTool/blob/main/documentation/ProposedListOfCorrections_SP800-90B.pdf`