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

2023-Jan-03 00:12:14.578246

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/truerand_8bit.bin`

- 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	1.0.37
Analysis environment	Hostname	[redacted]
	CPU information	AMD Ryzen [redacted]
	Physical memory size	[redacted] MB
	OS information	Windows 10 or greater
	Username	[redacted]

1.3 Identification of analysis conditions

Table 3 Identification information of analysis conditions

Number of samples	1000000
Bits per sample	8
Byte to bit conversion	Most Significant bit (MSb) first

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_{original} [a]	$H_{\text{bitstring}}$ [b]
	[bit / 8 - bit]	[bit / 1 - bit]
The Most Common Value Estimate	7.86512	0.998199
The Collision Estimate	—	0.95841
The Markov Estimate	—	0.999439
The Compression Estimate	—	0.904233
The t-Tuple Estimate	7.86512	0.933569
The Longest Repeated Substring (LRS) Estimate	7.9392	0.998671
Multi Most Common in Window Prediction Estimate	7.98858	0.999563
The Lag Prediction Estimate	7.93976	0.998402
The MultiMMC Prediction Estimate	7.92681	0.99966
The LZ78Y Prediction Estimate	7.91928	0.998465
The intial entropy source estimate [bit / 8 - bit] $H_I = \min(H_{\text{original}}, 8 \times H_{\text{bitstring}})$	7.23386	

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

[b] An additional entropy estimation (per bit) for the non-binary sequential dataset [see NIST SP 800-90B 3.1.3]

2.2 Visual comparison of min-entropy estimates from original samples

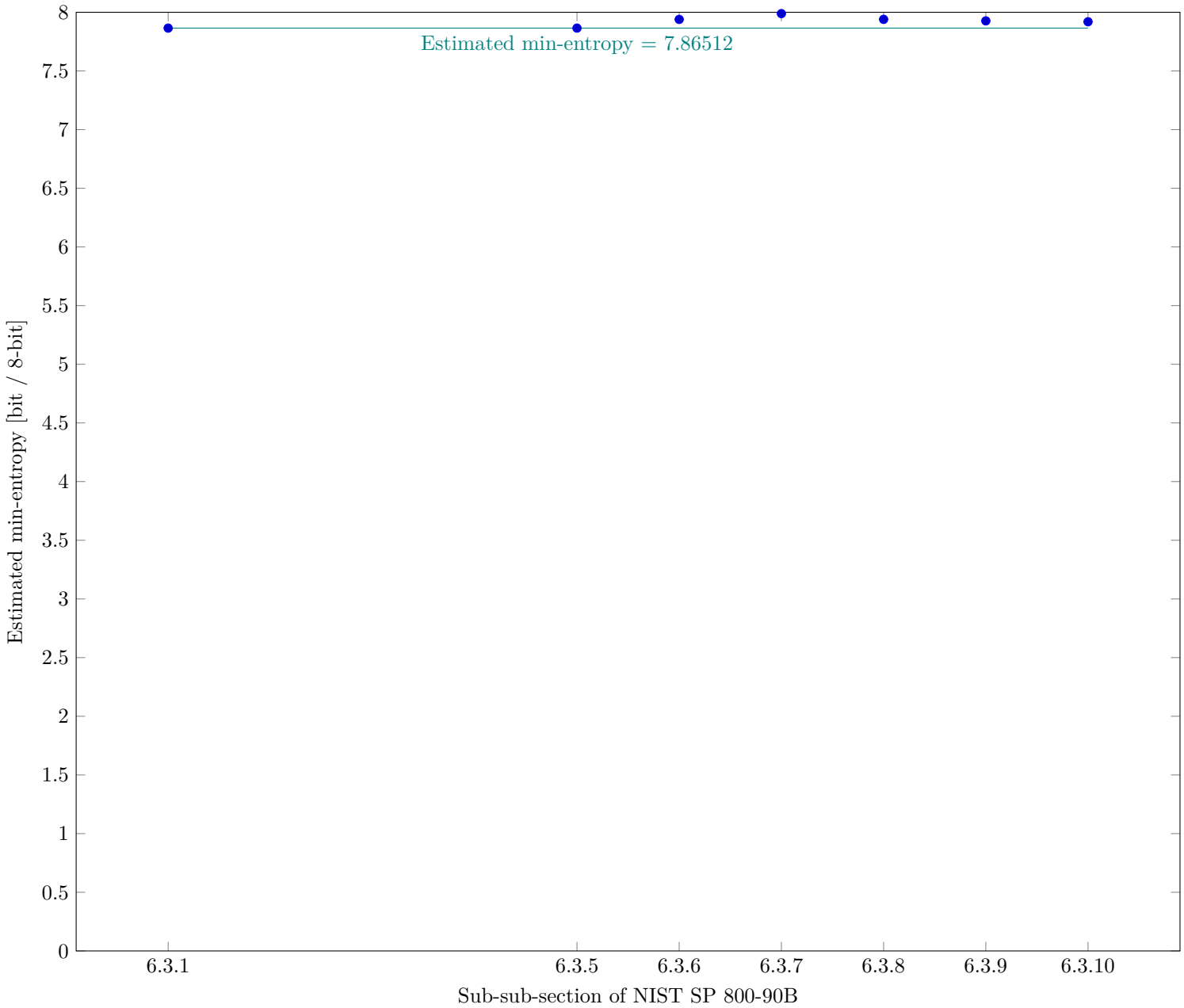


Fig. 1 Estimated Min-Entropy using §6.3 of NIST SP 800-90B

2.3 Visual comparison of min-entropy estimates by interpreting each sample as bitstring

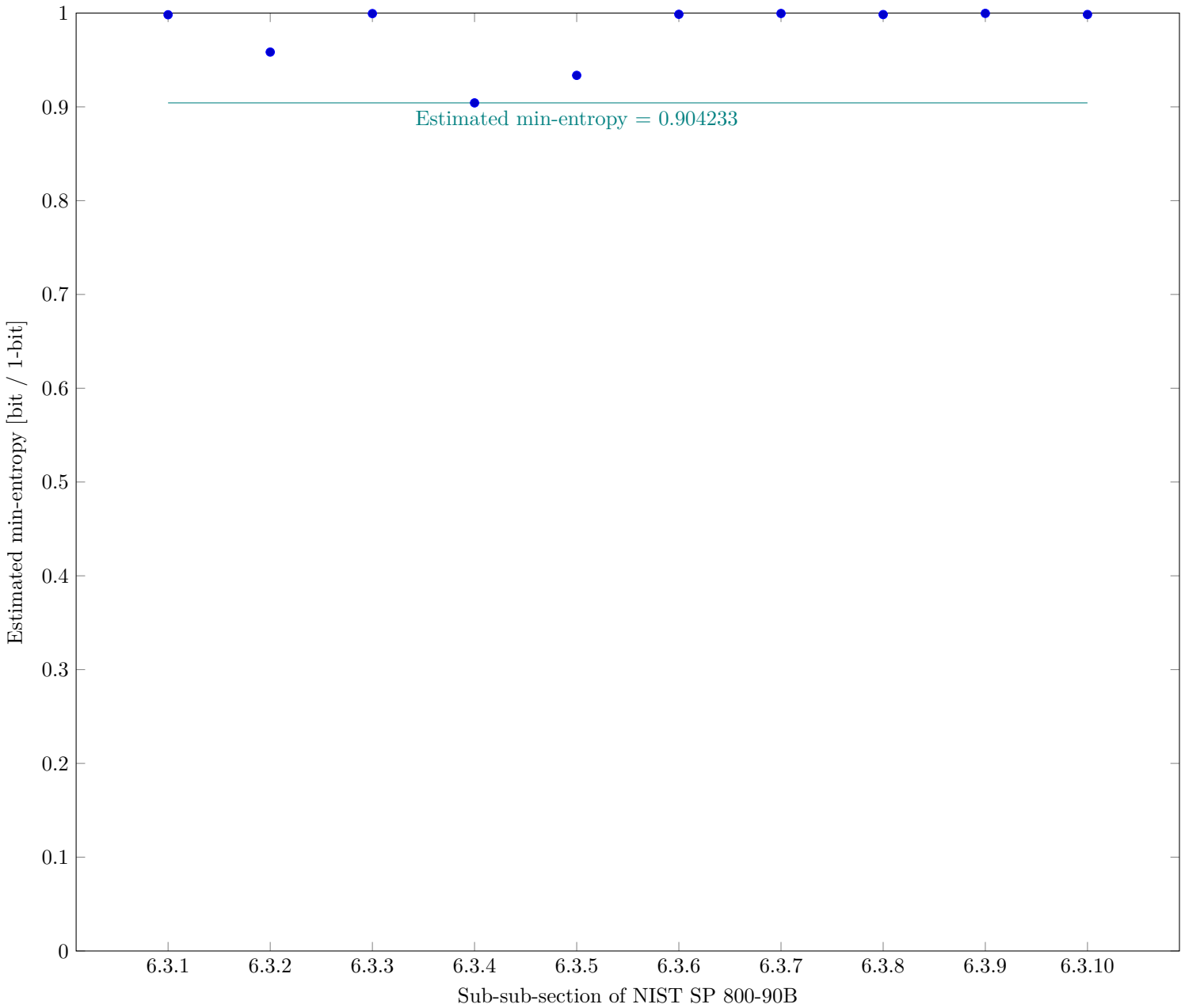
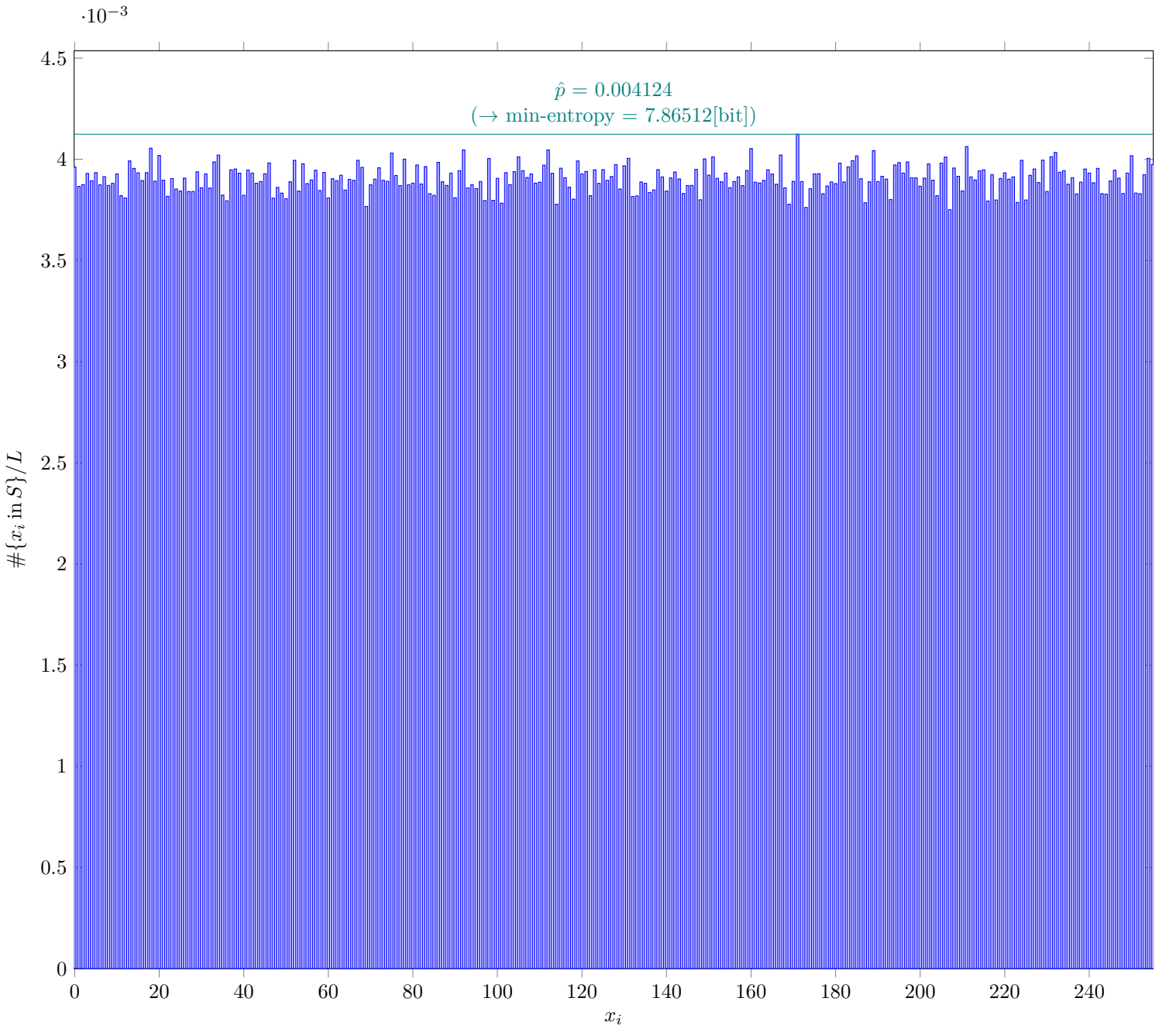


Fig. 2 Estimated Min-Entropy using §6.3 of NIST SP 800-90B

3 Detailed results of analysis from original samples

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



3.1.1 Supplemental information for traceability

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

Symbol	Value
mode	4124
$\hat{p}$	0.004124
p_u	0.00428907

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

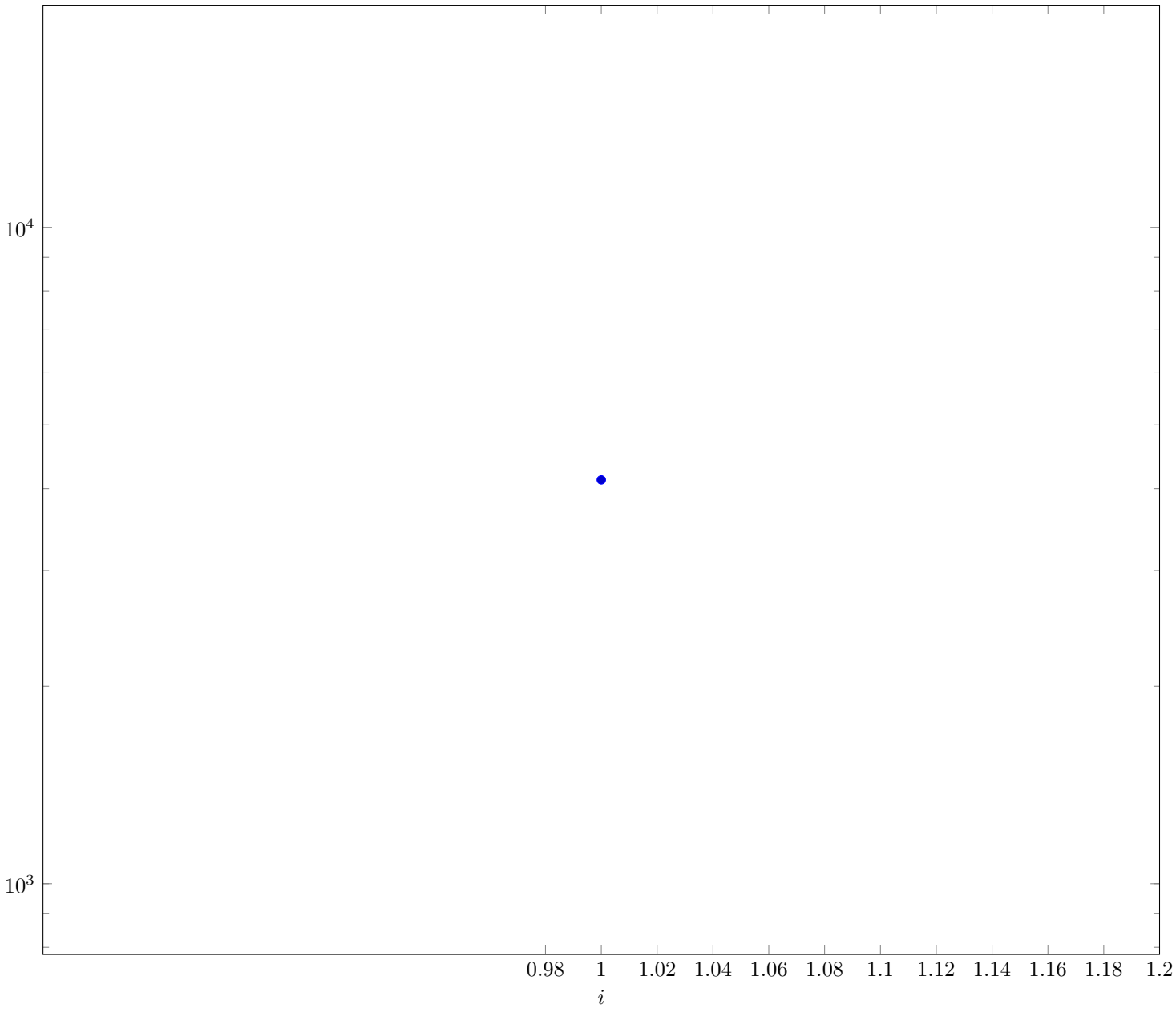


Fig. 3 Intermediate value $Q[i]$ in §6.3.5 of NIST SP 800-90B

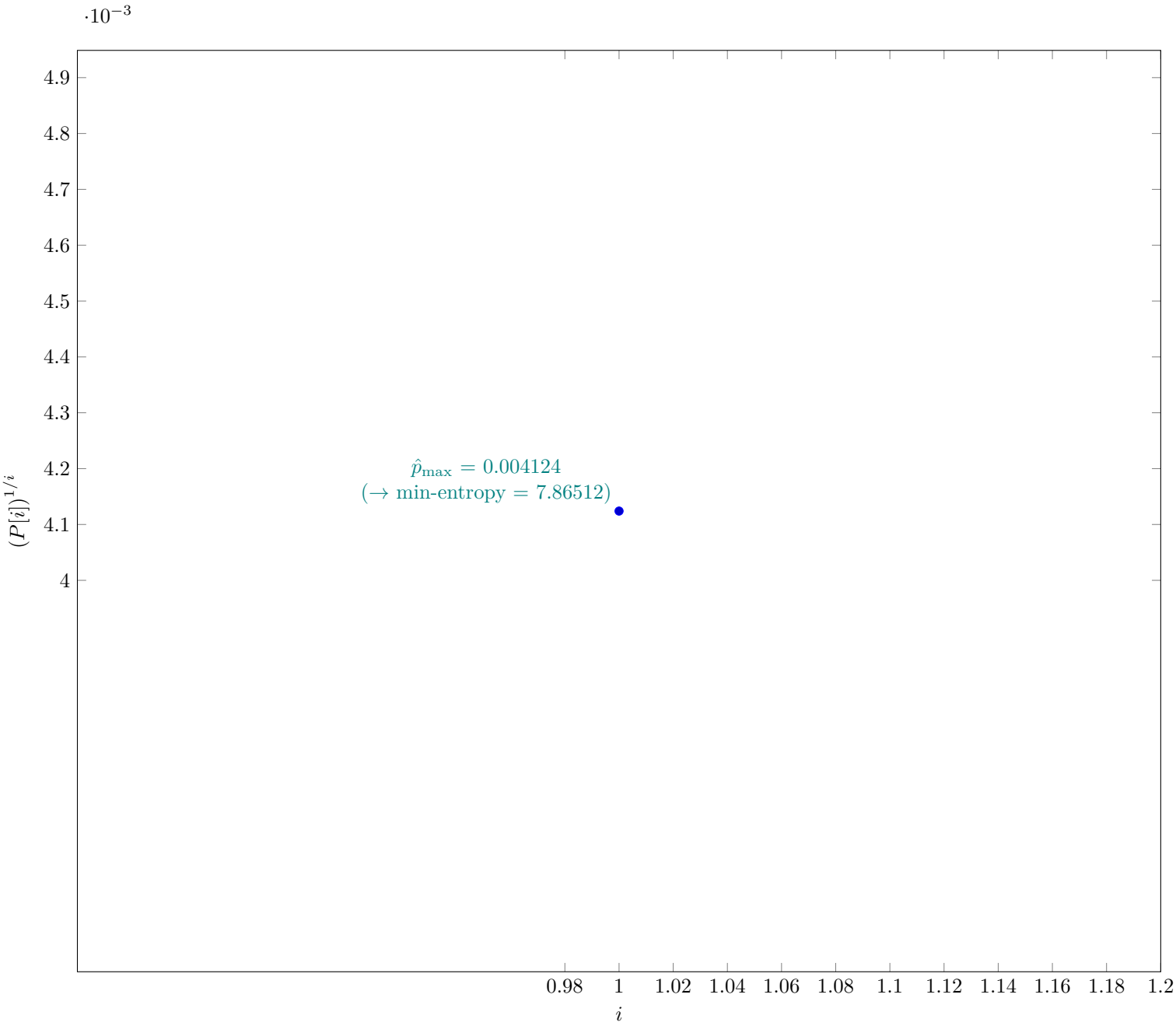


Fig. 4 $P[i]^{1/i}$ in §6.3.5 of NIST SP 800-90B

3.2.1 Supplemental information for traceability

Table 6 Supplemental information for traceability (NIST SP 800-90B Section 6.3.5)

Symbol	Value
t	1
$\hat{p}_{\max}$	0.004124
p_u	0.00428907

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

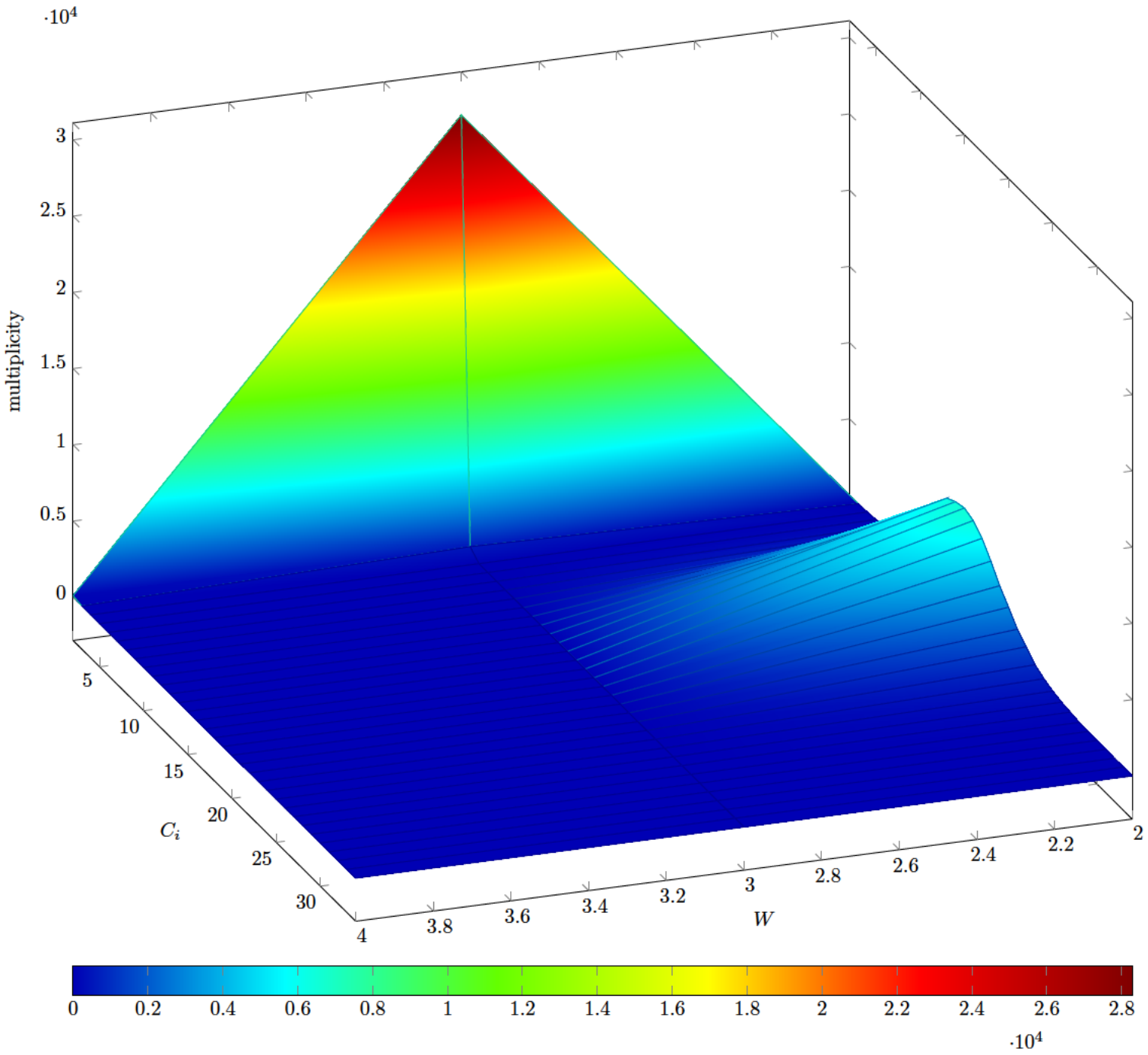


Fig. 5 Estimated W-tuple collision probability in Step 3 of §6.3.6 of NIST SP 800-90B

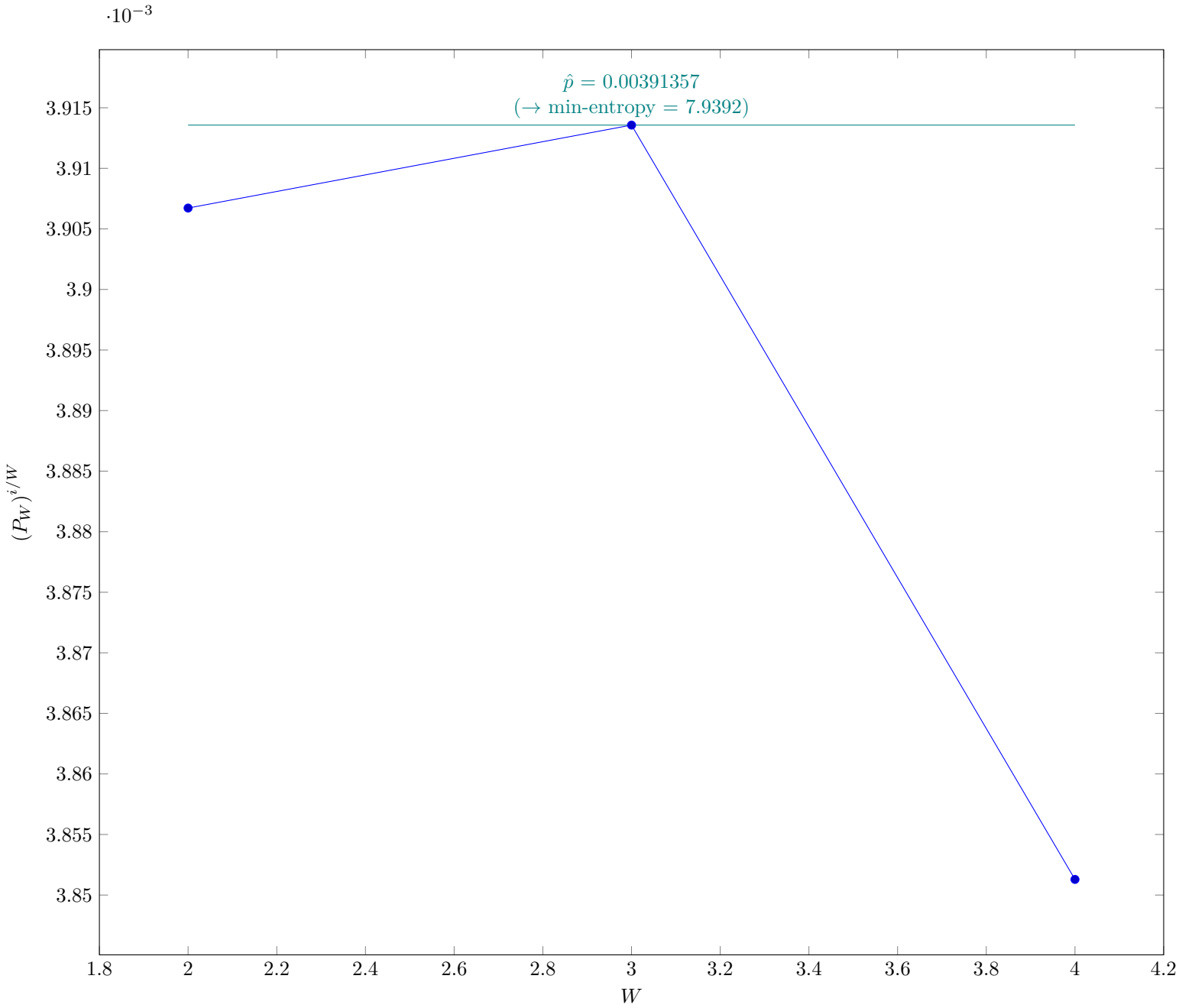


Fig. 6 Estimated average collision probability per string symbol in Step 3 of §6.3.6 of NIST SP 800-90B

3.3.1 Supplemental information for traceability

Table 7 Supplemental information for traceability (NIST SP 800-90B Section 6.3.6)

Symbol	Value
u	2
v	4
$\hat{p}$	0.00391357
p_u	0.00407439

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

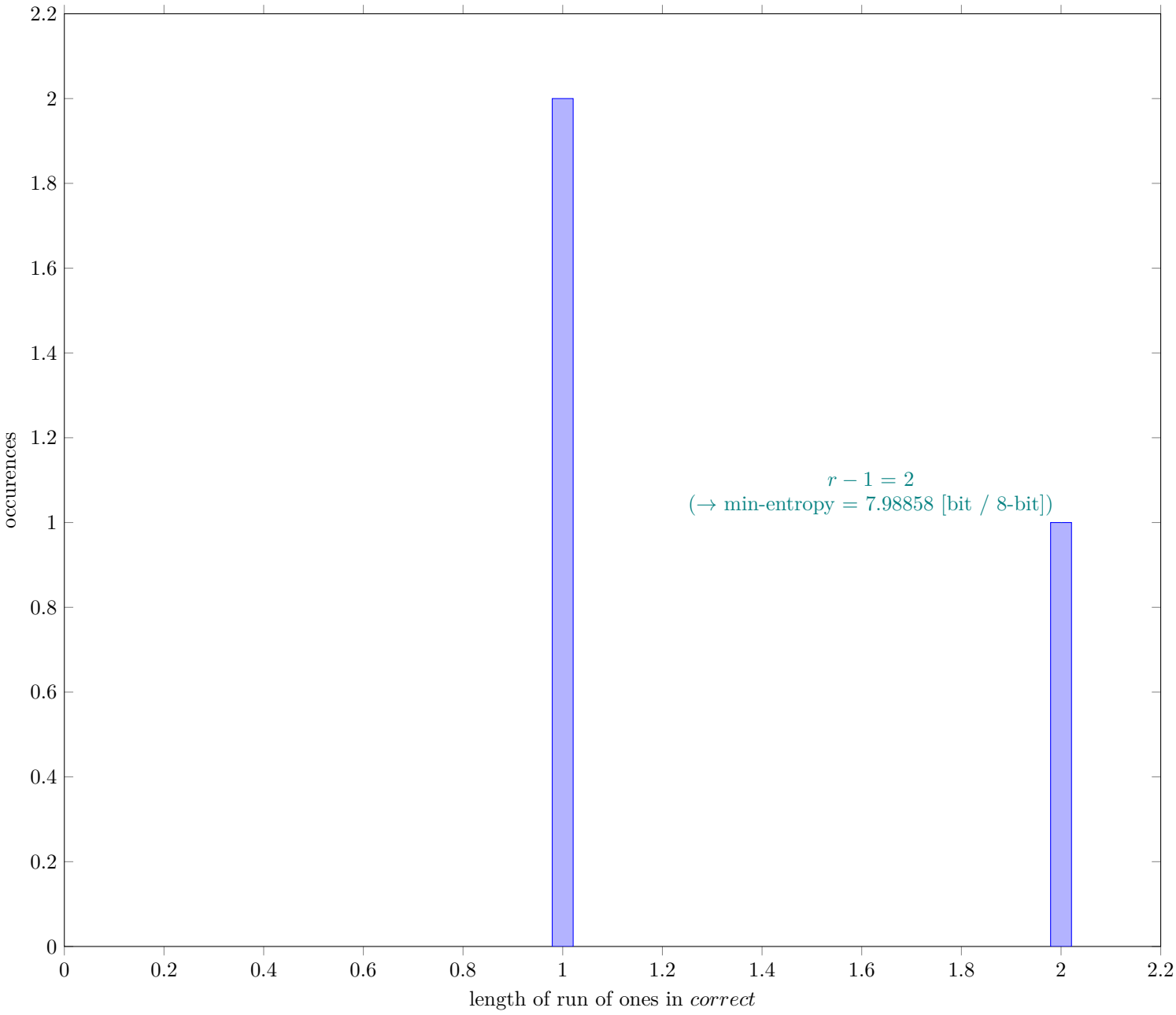


Fig. 7 Distribution of *correct*

3.4.1 Supplemental information for traceability

Table 8 Supplemental information for traceability (NIST SP 800-90B Section 6.3.7)

Symbol	Value
N	999937
C	3779
P_{global}	0.00377924
P'_{global}	0.00393729
r	3
P_{local}	0.00215965

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

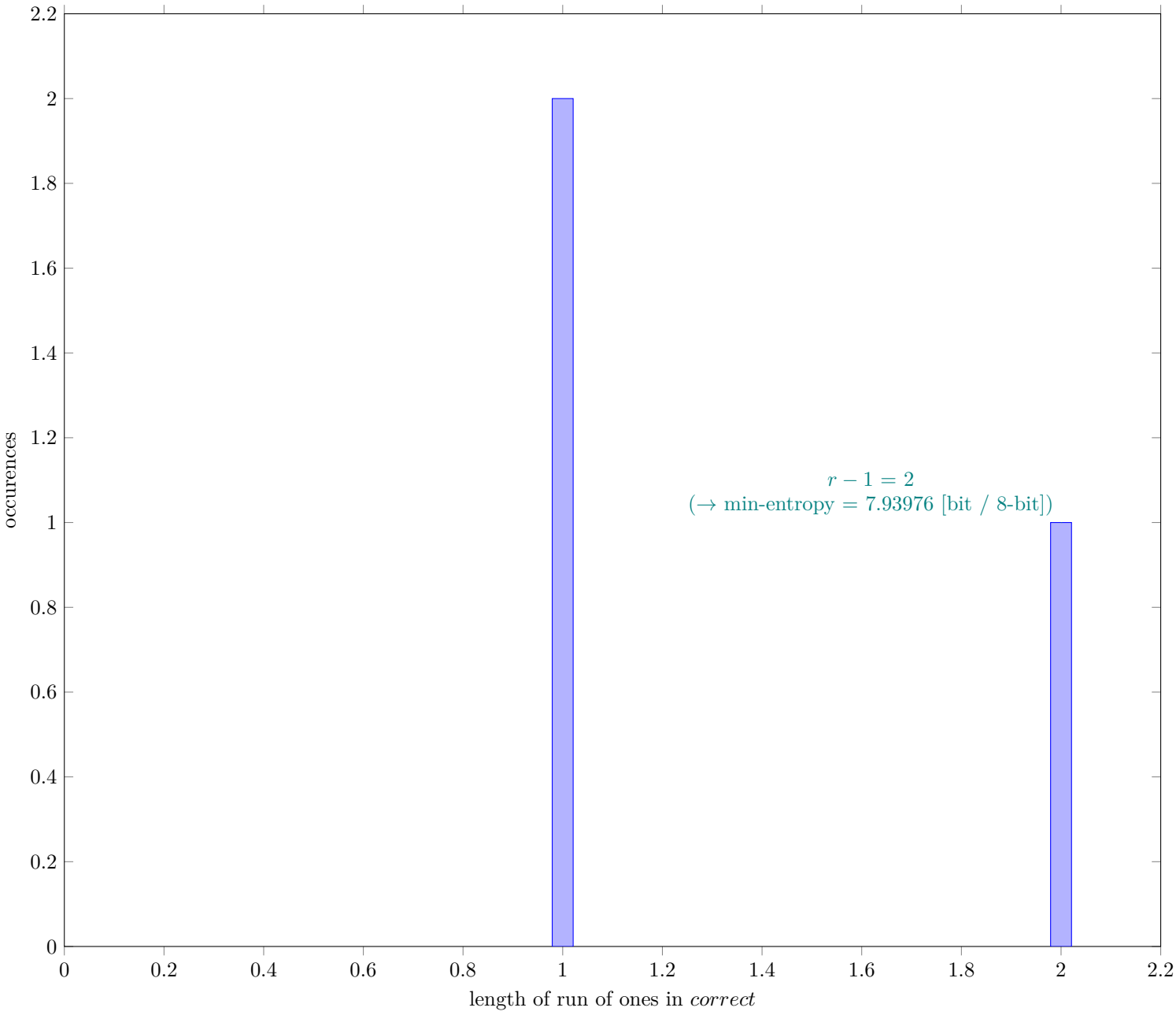


Fig. 8 Distribution of *correct*

3.5.1 Supplemental information for traceability

Table 9 Supplemental information for traceability (NIST SP 800-90B Section 6.3.8)

Symbol	Value
N	999999
C	3912
P_{global}	0.003912
P'_{global}	0.0040728
r	3
P_{local}	0.0021596

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

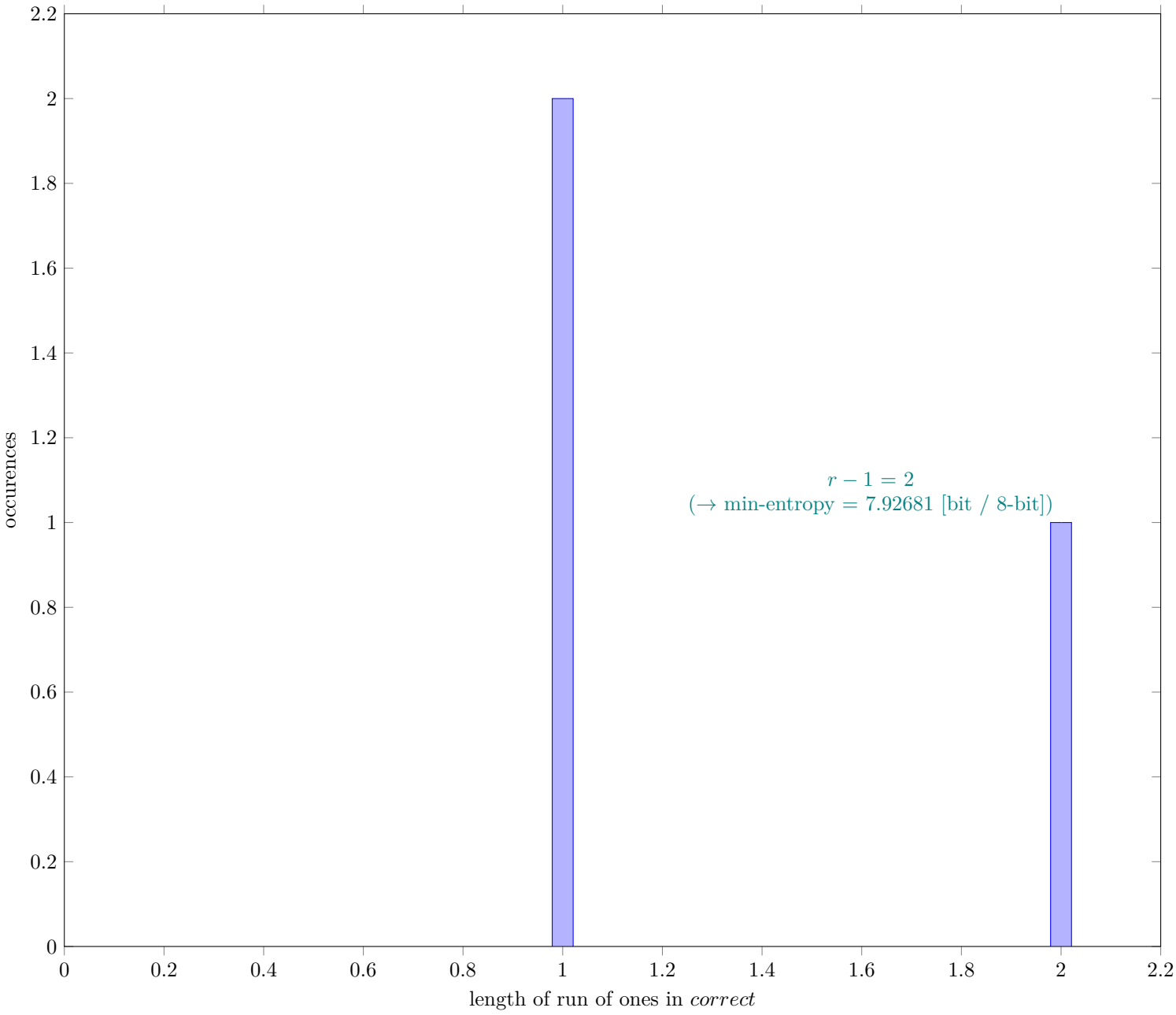


Fig. 9 Distribution of *correct*

3.6.1 Supplemental information for traceability

Table 10 Supplemental information for traceability (NIST SP 800-90B Section 6.3.9)

Symbol	Value
N	999998
C	3948
P_{global}	0.00394801
P'_{global}	0.00410954
r	3
P_{local}	0.0021596

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

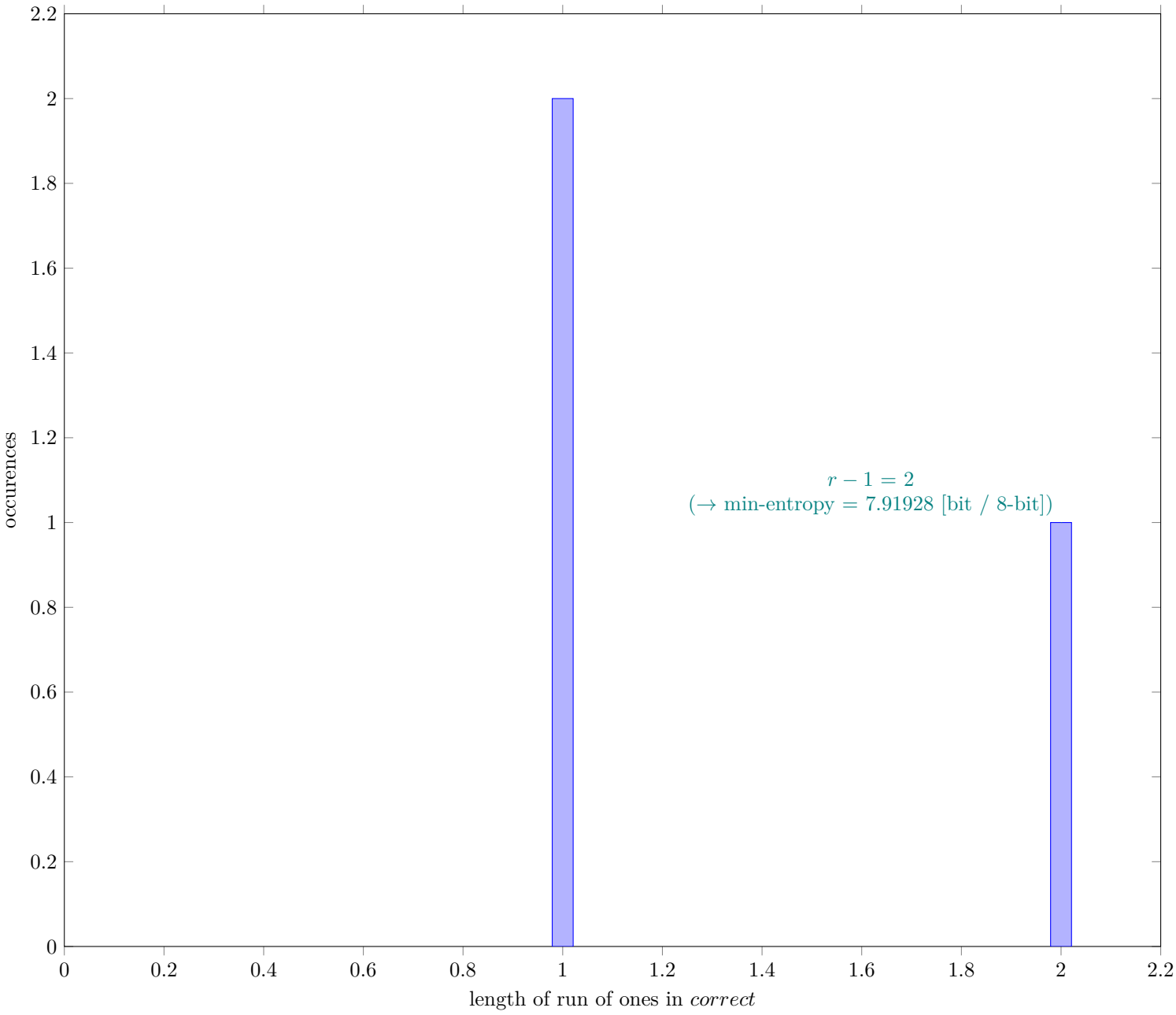


Fig. 10 Distribution of *correct*

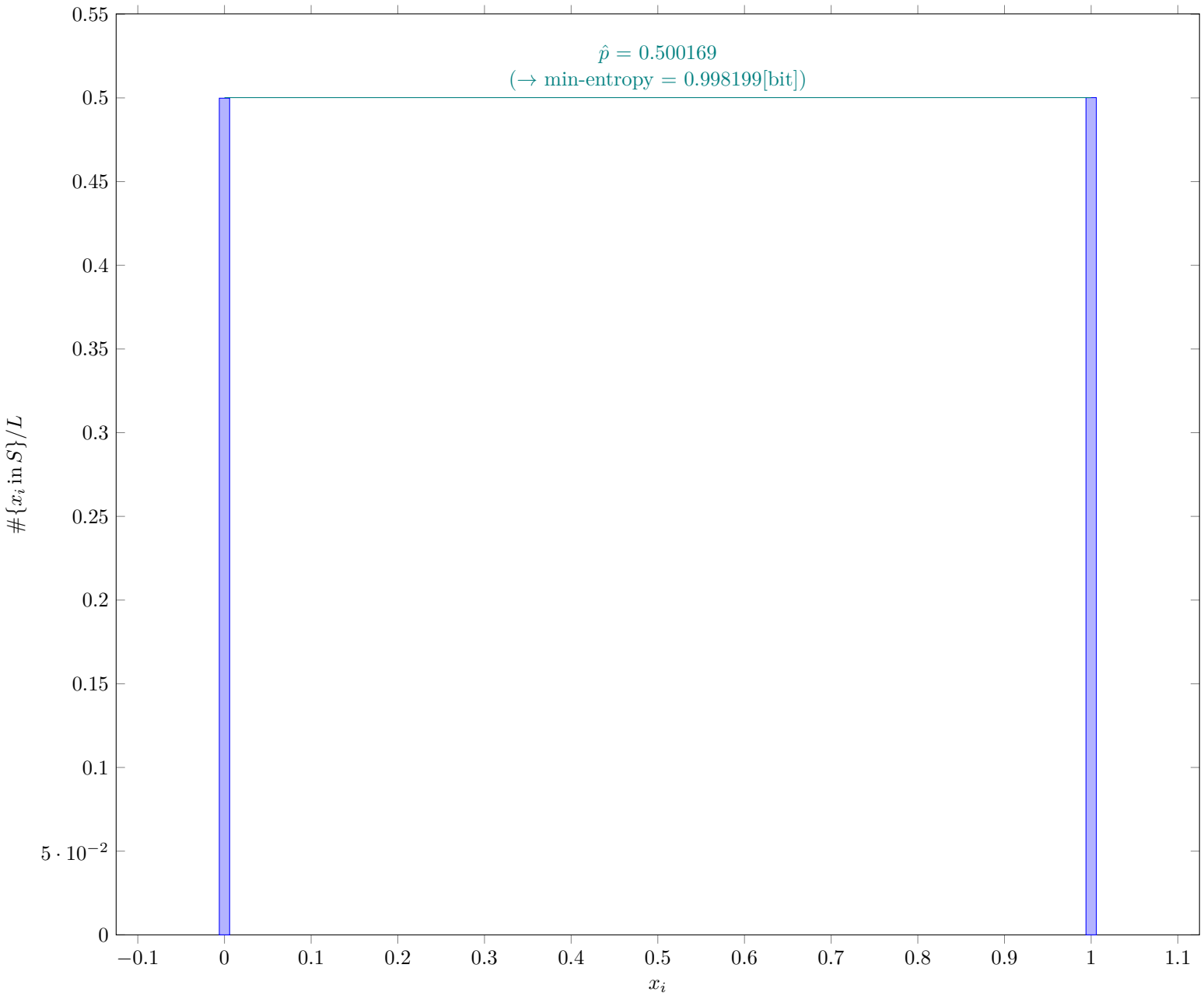
3.7.1 Supplemental information for traceability

Table 11 Supplemental information for traceability (NIST SP 800-90B Section 6.3.10)

Symbol	Value
N	999983
C	3969
P_{global}	0.00396907
P'_{global}	0.00413103
r	3
P_{local}	0.00215961

4 Detailed results of analysis by interpreting each sample as bitstrings

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

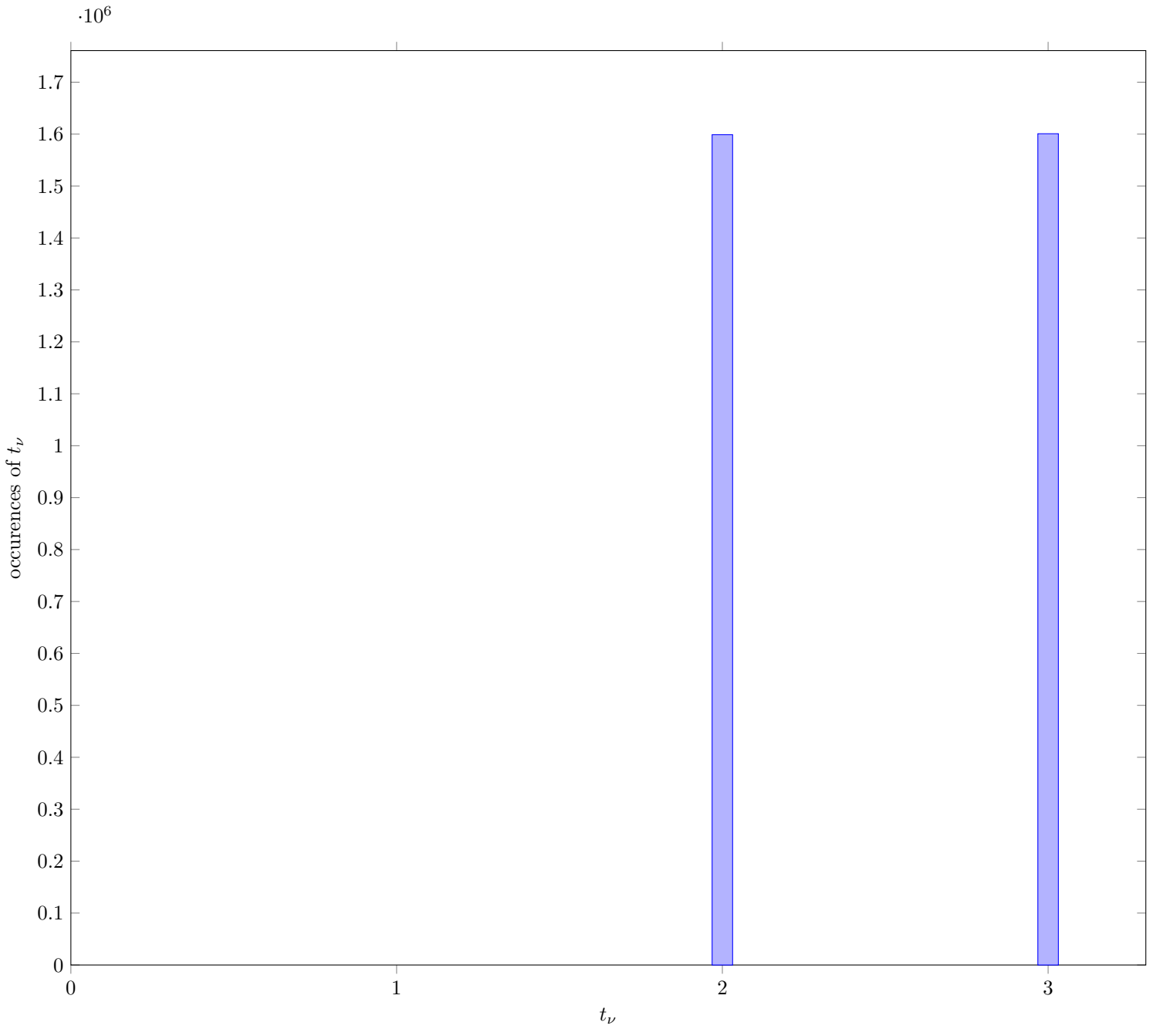


4.1.1 Supplemental information for traceability

Table 12 Supplemental information for traceability (NIST SP 800-90B Section 6.3.1)

Symbol	Value
mode	4001353
$\hat{p}$	0.500169
p_u	0.500624

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



4.2.1 Supplemental information for traceability

Table 13 Supplemental information for traceability (NIST SP 800-90B Section 6.3.2)

Symbol	Value
p	0.514624
$\bar{X}$	2.50029
$\bar{X}'$	2.49957

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

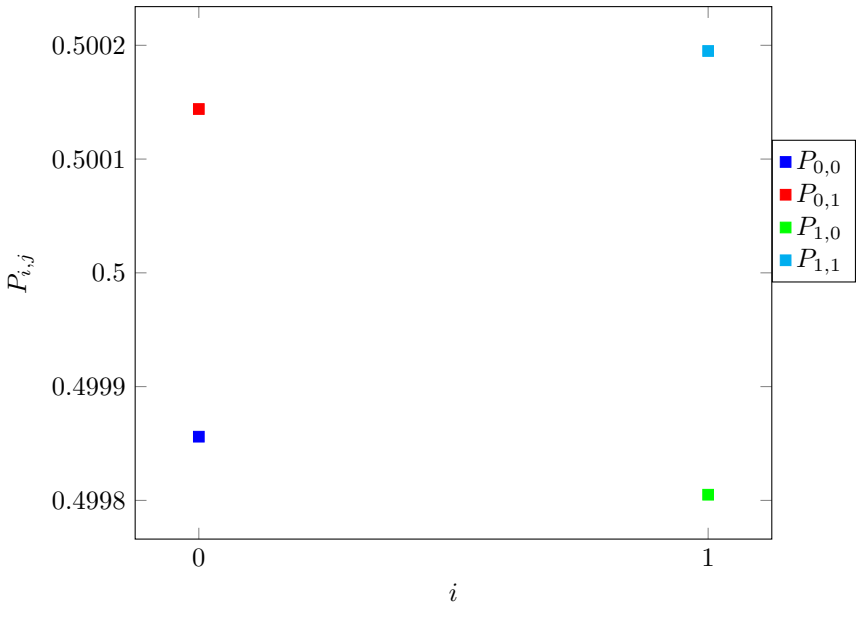


Fig. 11 Transition probability $P_{i,j}$ of §6.3.3 of NIST SP 800-90B

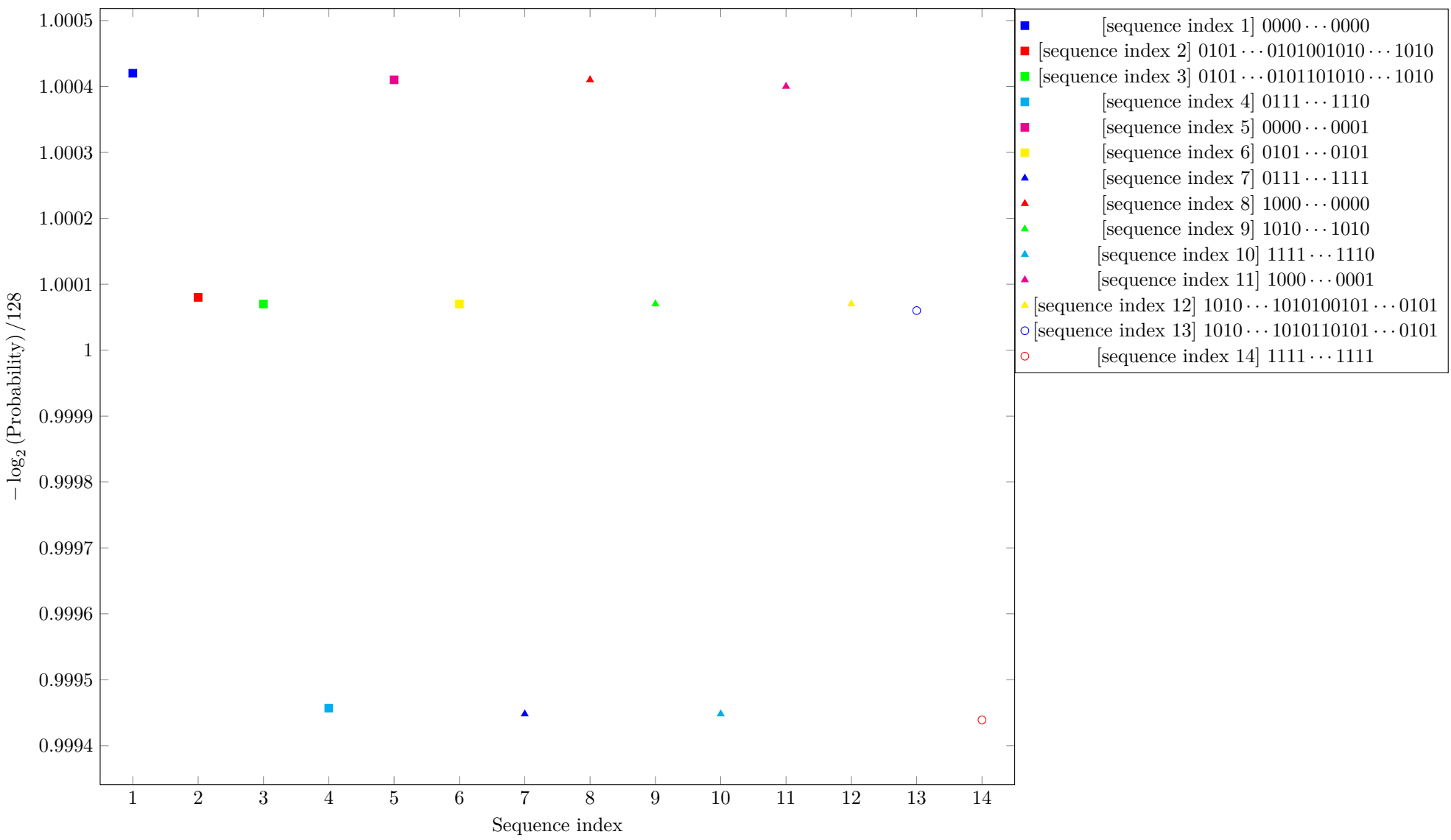
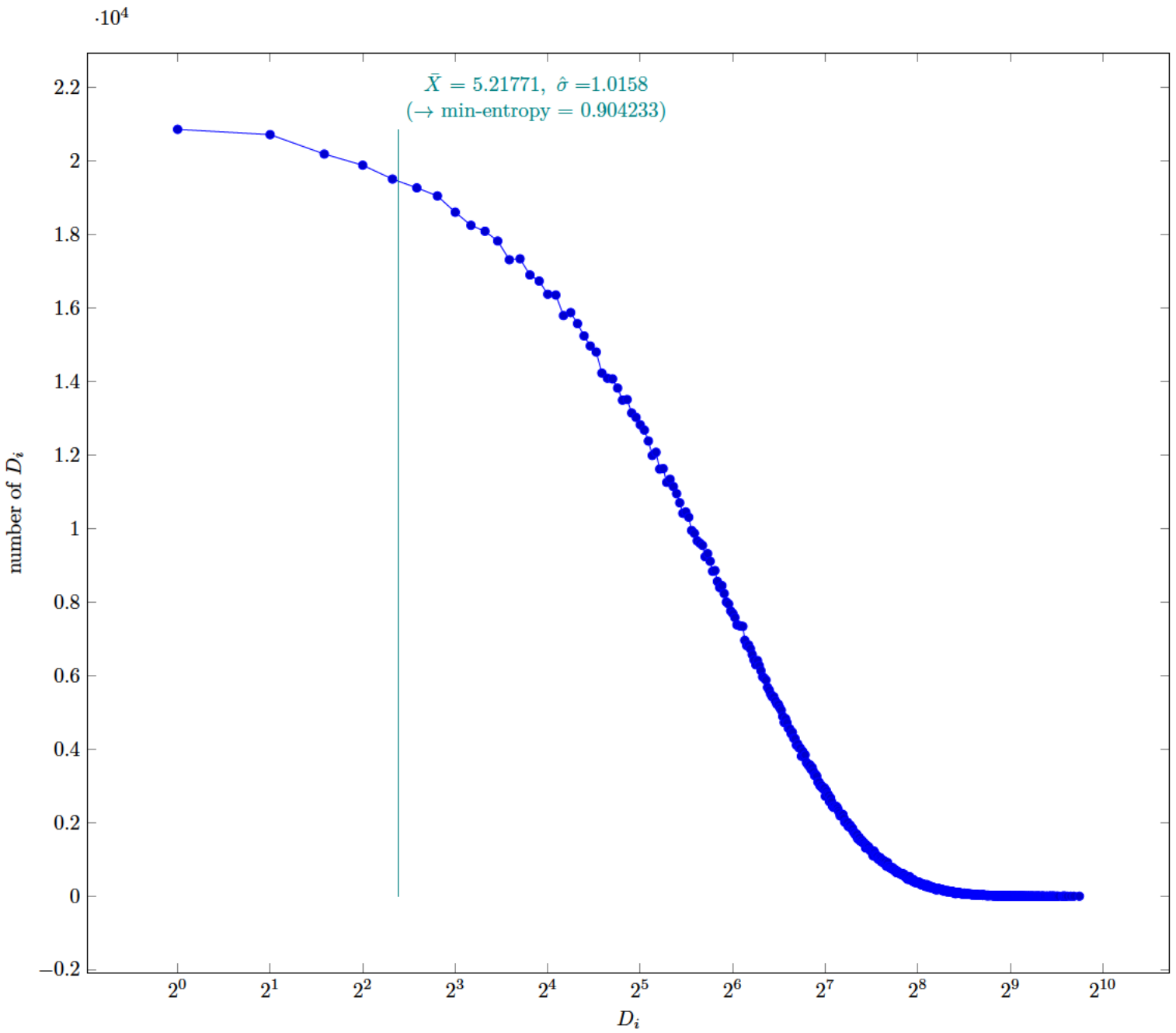


Fig. 12 Estimated Min-Entropy using §6.3.3 of NIST SP 800-90B

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



4.4.1 Supplemental information for traceability

Table 14 Supplemental information for traceability (NIST SP 800-90B Section 6.3.4)

Symbol	Value
p	0.0232698
$\bar{X}$	5.21771
$\hat{\sigma}$	1.0158
$\bar{X}'$	5.21545

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

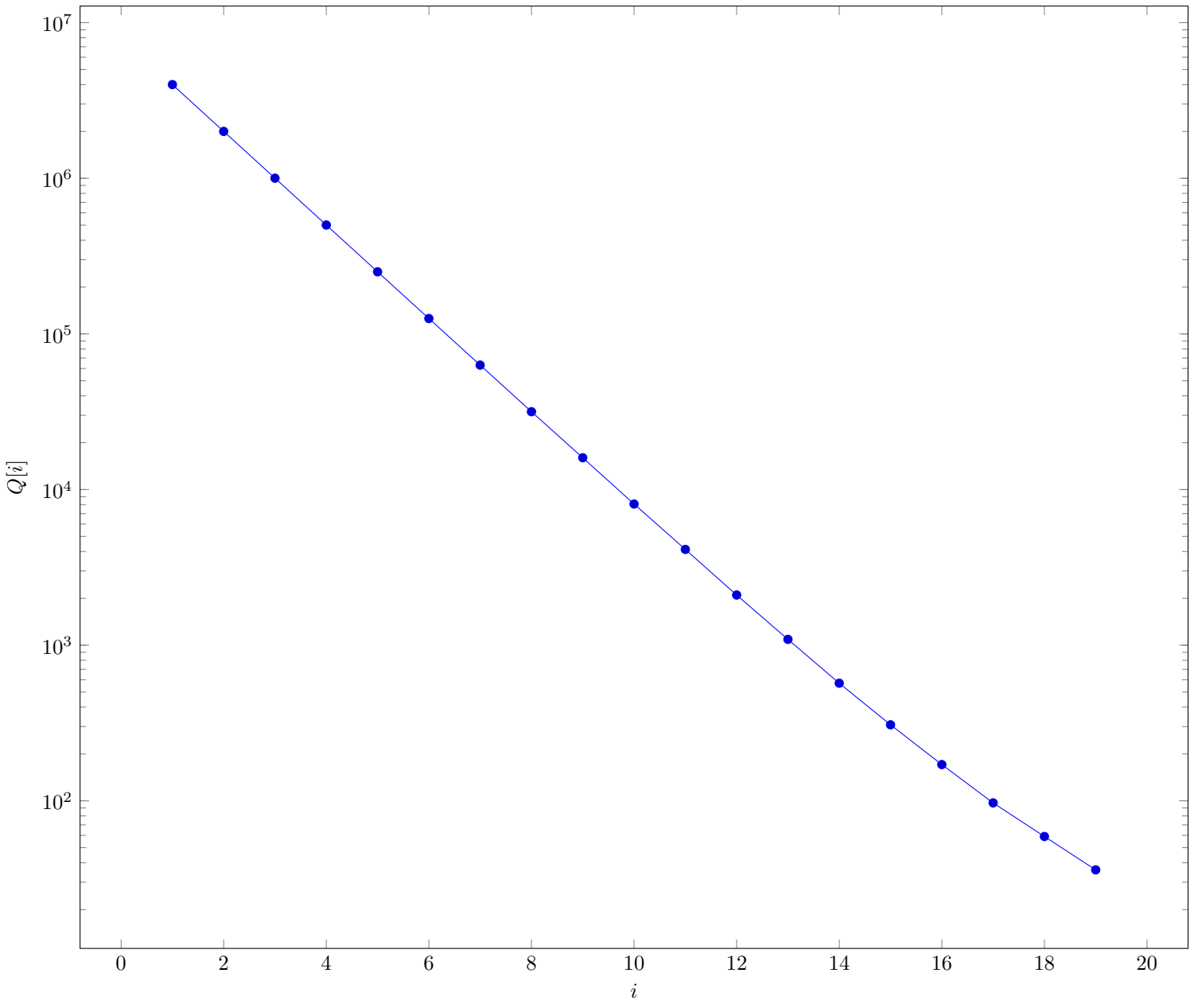


Fig. 13 Intermediate value $Q[i]$ in §6.3.5 of NIST SP 800-90B

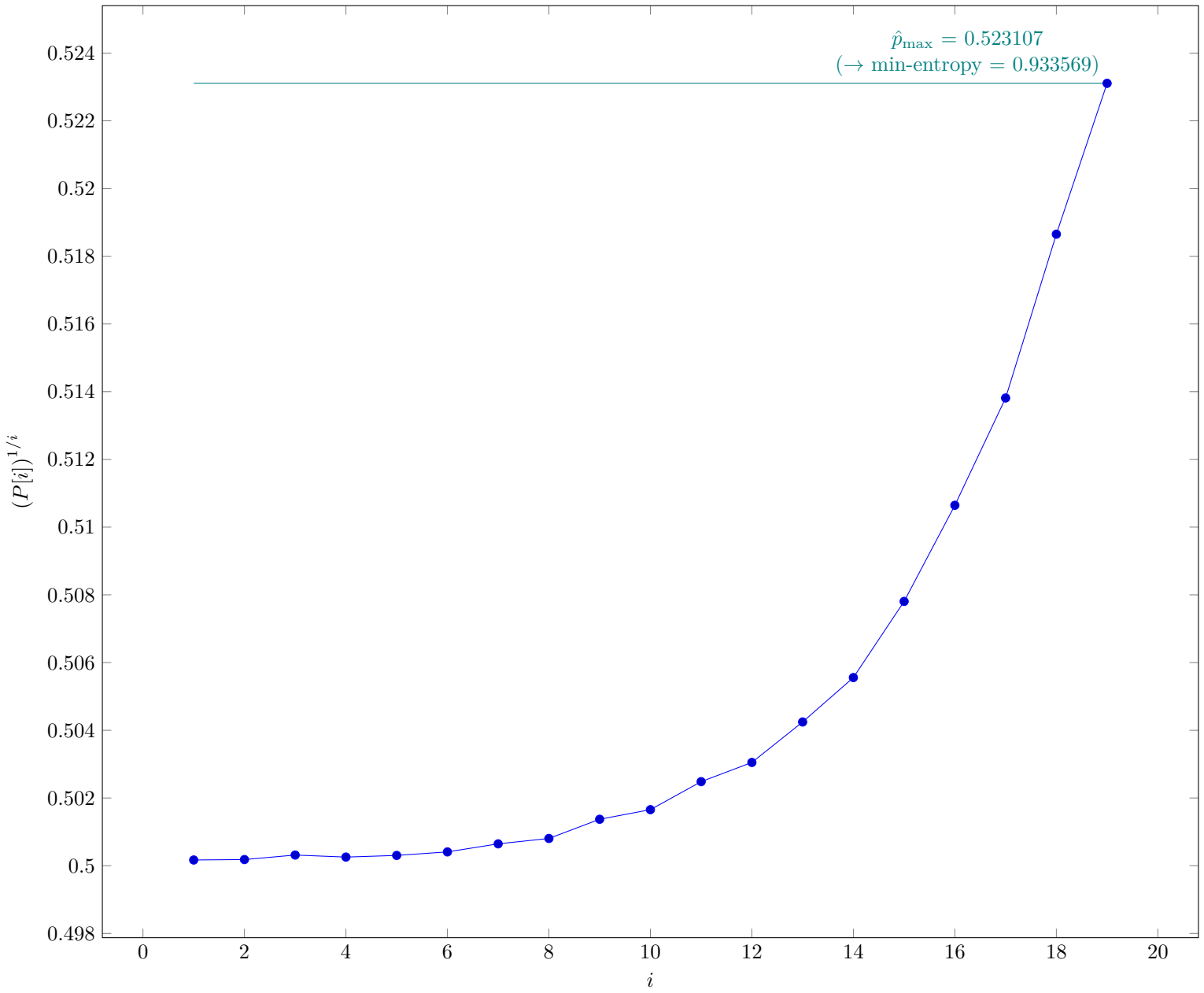


Fig. 14 $P[i]^{1/i}$ in §6.3.5 of NIST SP 800-90B

4.5.1 Supplemental information for traceability

Table 15 Supplemental information for traceability (NIST SP 800-90B Section 6.3.5)

Symbol	Value
t	19
$\hat{p}_{\max}$	0.523107
p_u	0.523561

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

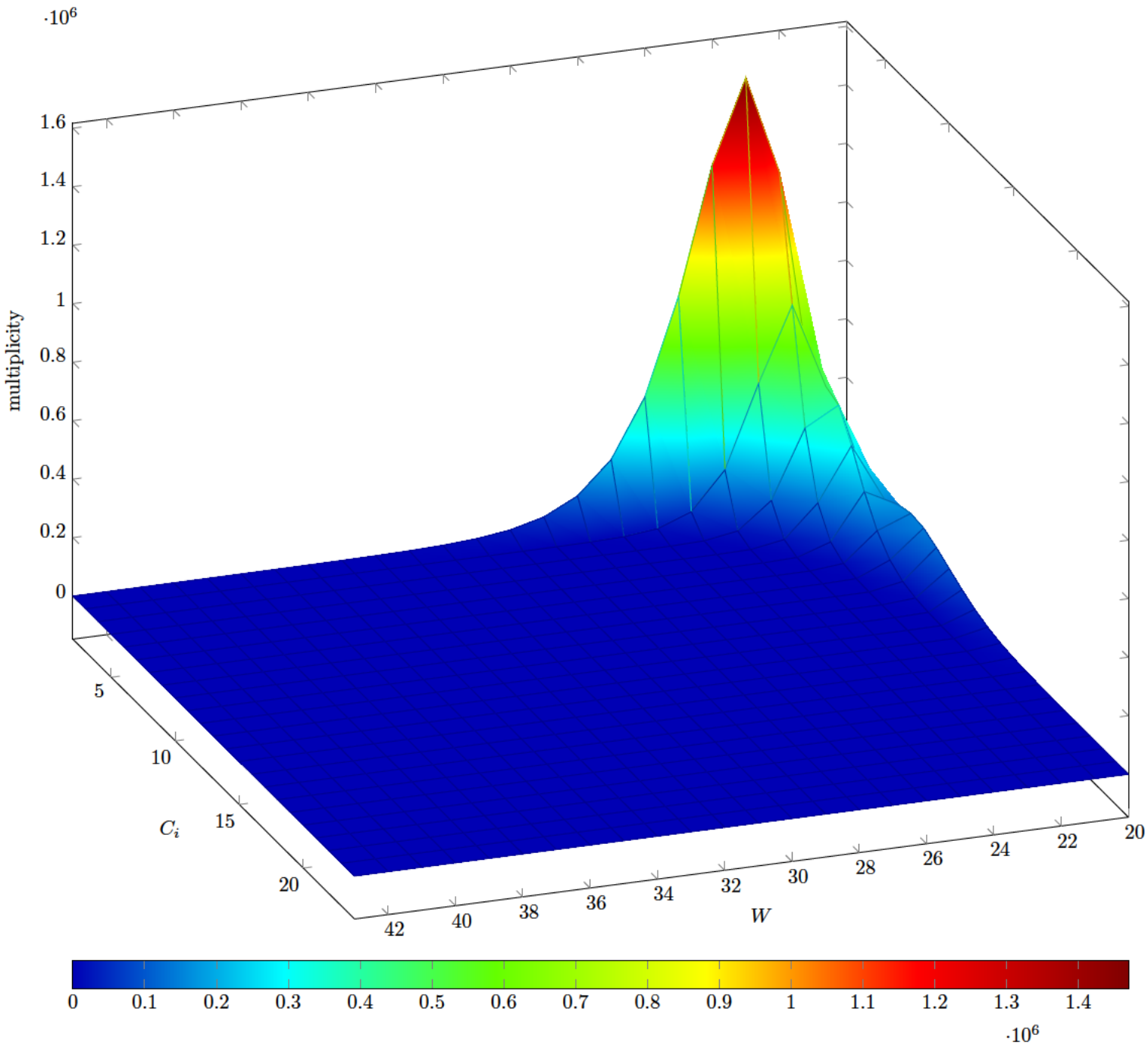


Fig. 15 Estimated W-tuple collision probability in Step 3 of §6.3.6 of NIST SP 800-90B

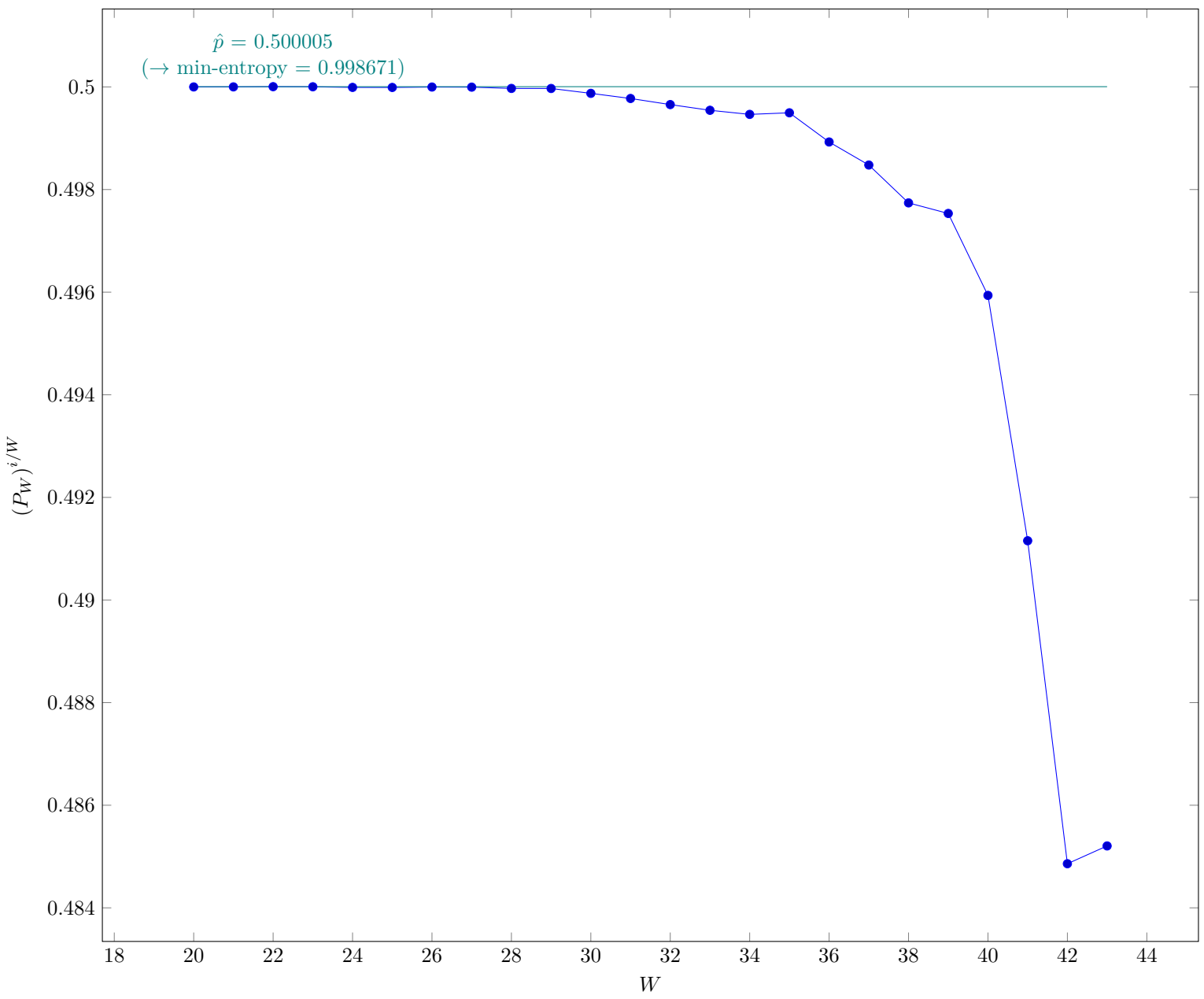


Fig. 16 Estimated average collision probability per string symbol in Step 3 of §6.3.6 of NIST SP 800-90B

4.6.1 Supplemental information for traceability

Table 16 Supplemental information for traceability (NIST SP 800-90B Section 6.3.6)

Symbol	Value
u	20
v	43
$\hat{p}$	0.500005
p_u	0.500461

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

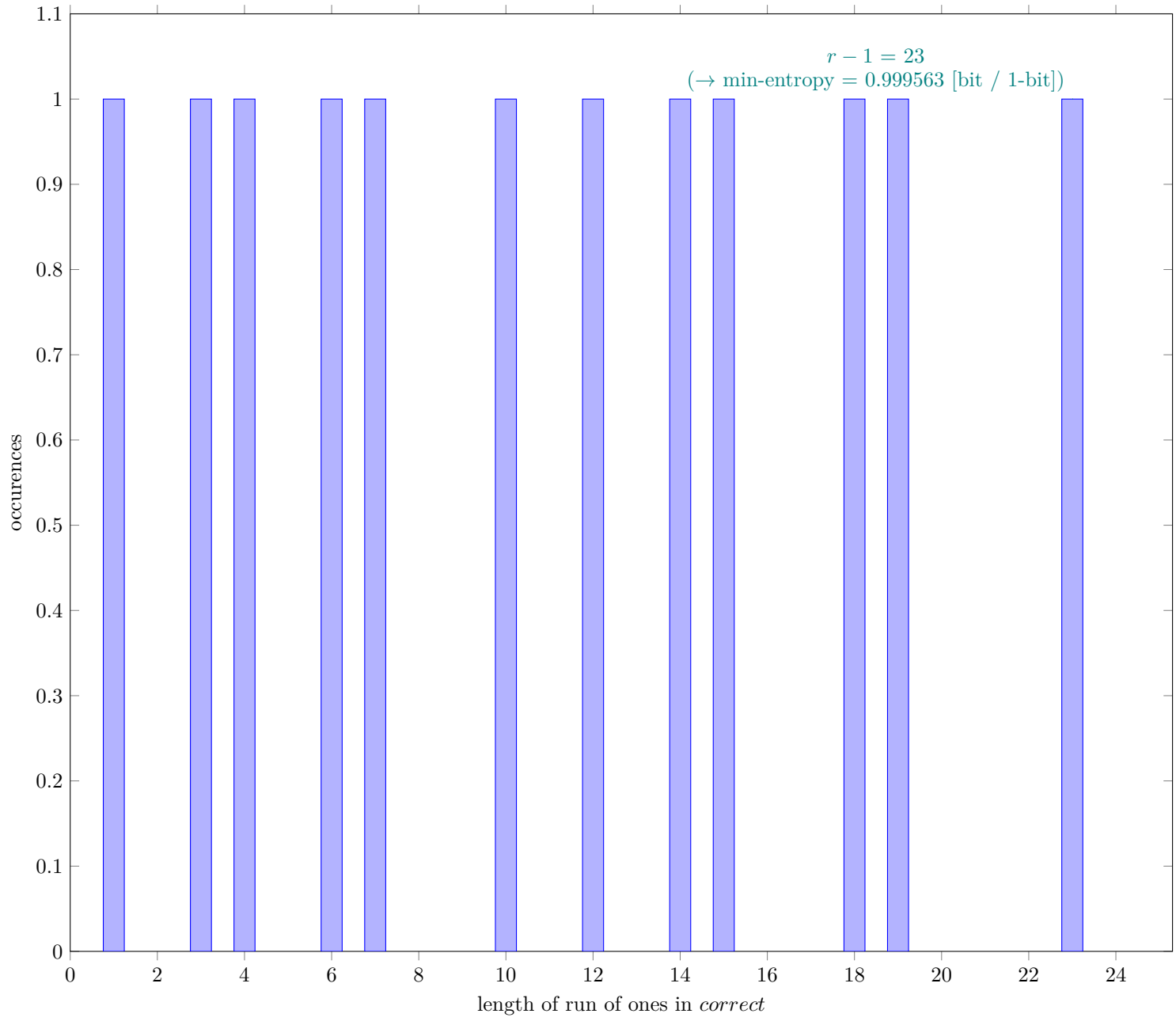


Fig. 17 Distribution of *correct*

4.7.1 Supplemental information for traceability

Table 17 Supplemental information for traceability (NIST SP 800-90B Section 6.3.7)

Symbol	Value
N	7999937
C	3997538
P_{global}	0.499696
P'_{global}	0.500152
r	24
P_{local}	0.436006

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

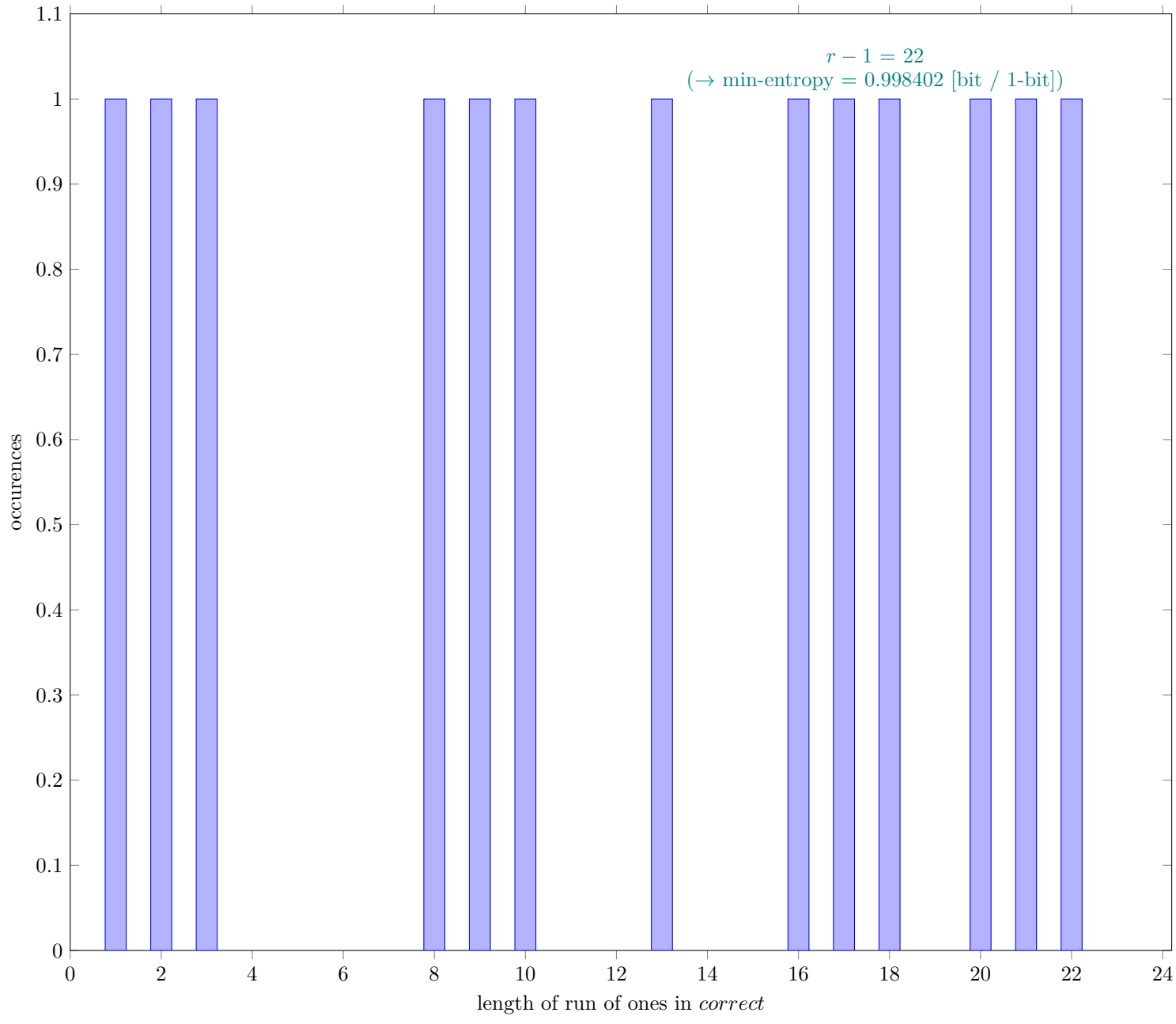


Fig. 18 Distribution of *correct*

4.8.1 Supplemental information for traceability

Table 18 Supplemental information for traceability (NIST SP 800-90B Section 6.3.8)

Symbol	Value
N	7999999
C	4000791
P_{global}	0.500099
P'_{global}	0.500554
r	23
P_{local}	0.42004

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

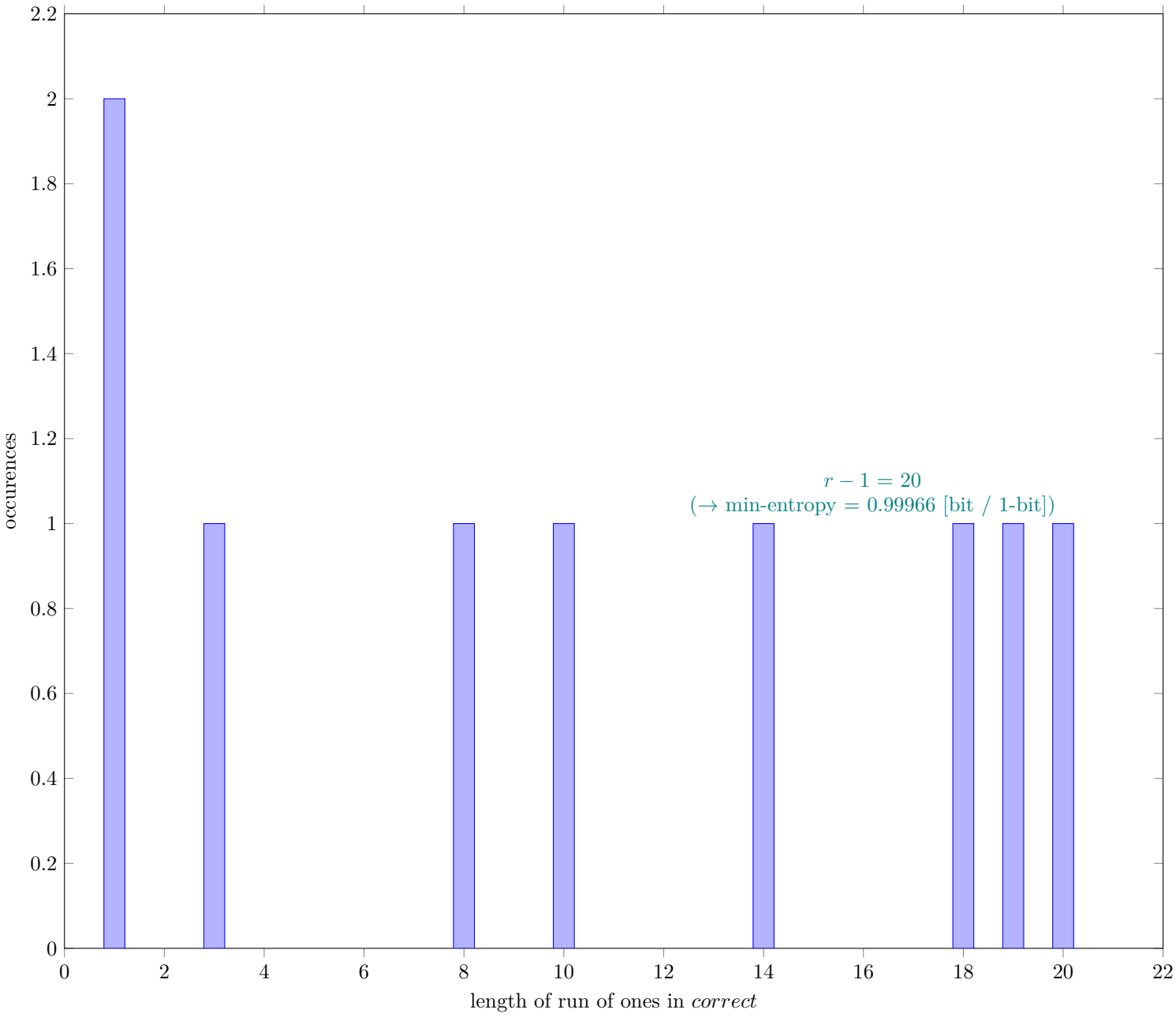


Fig. 19 Distribution of *correct*

4.9.1 Supplemental information for traceability

Table 19 Supplemental information for traceability (NIST SP 800-90B Section 6.3.9)

Symbol	Value
N	7999998
C	3997298
P_{global}	0.499662
P'_{global}	0.500118
r	21
P_{local}	0.385677

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

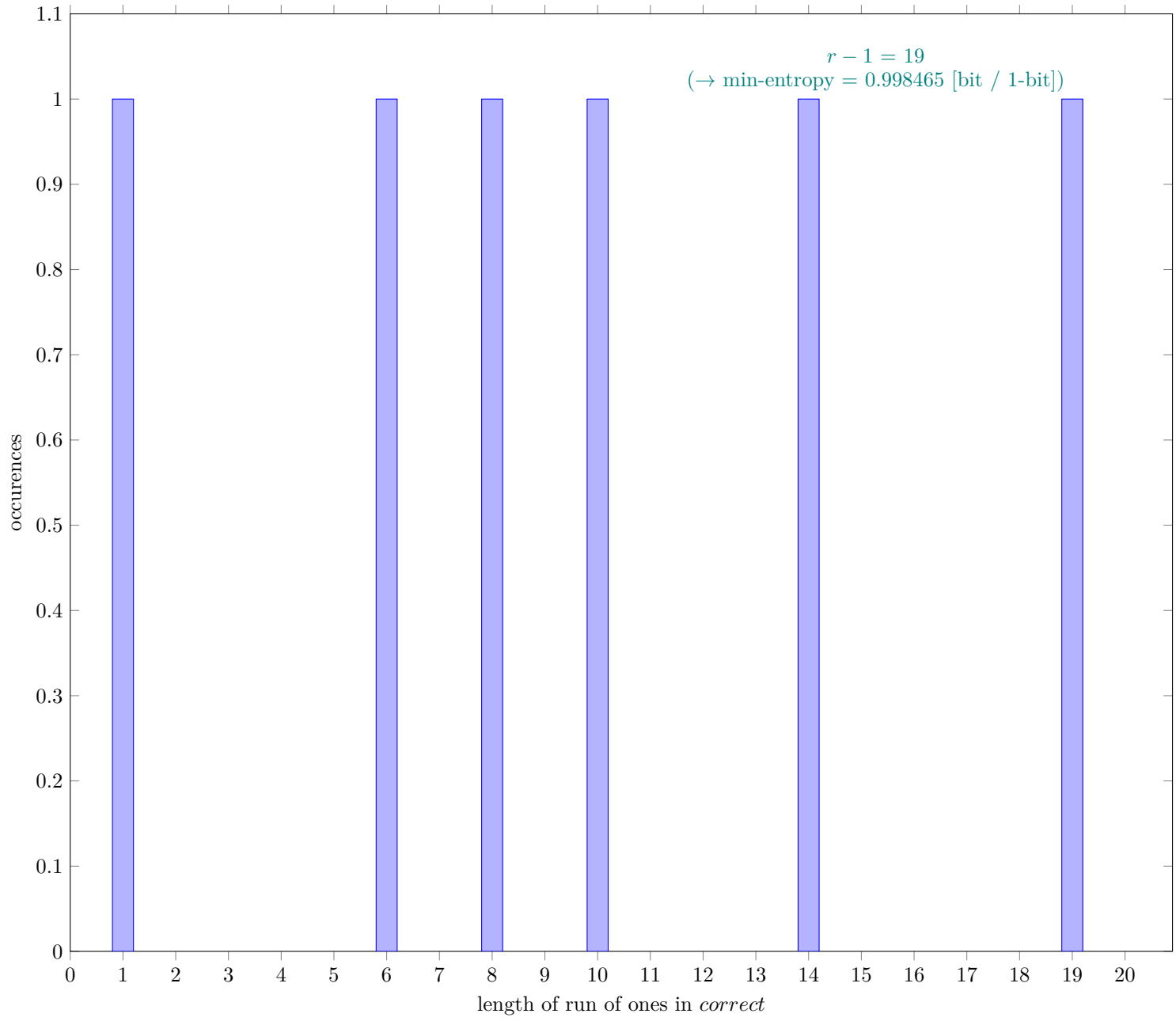


Fig. 20 Distribution of *correct*

4.10.1 Supplemental information for traceability

Table 20 Supplemental information for traceability (NIST SP 800-90B Section 6.3.10)

Symbol	Value
N	7999983
C	4000606
P_{global}	0.500077
P'_{global}	0.500532
r	20
P_{local}	0.36719

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

[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`