

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

2023-Jan-02 23:20:41.427722

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/ringOsc-nist.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	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	$H_{\text{bitstring}}^a$
	(/ 1 - bit)
The Most Common Value Estimate	0.993514
The Collision Estimate	0.126446
The Markov Estimate	0.257979
The Compression Estimate	0.159323
The t-Tuple Estimate	0.201709
The Longest Repeated Substring (LRS) Estimate	0.365799
Multi Most Common in Window Prediction Estimate	0.290519
The Lag Prediction Estimate	0.251067
The MultiMMC Prediction Estimate	0.251069
The LZ78Y Prediction Estimate	0.251073
The intial entropy source estimate (/ 1-bit) $H_I = H_{\text{bitstring}}$	0.126446
^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

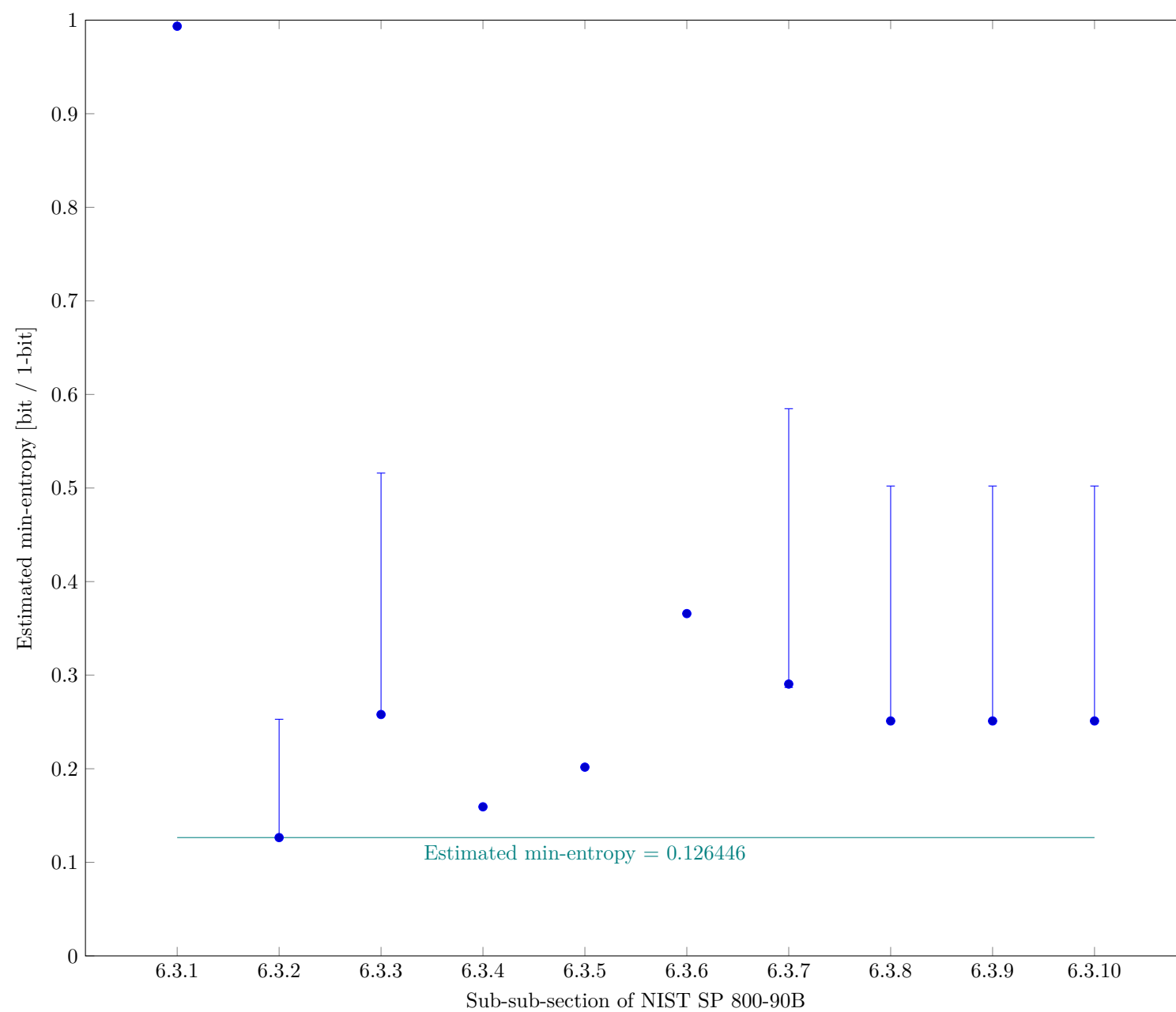
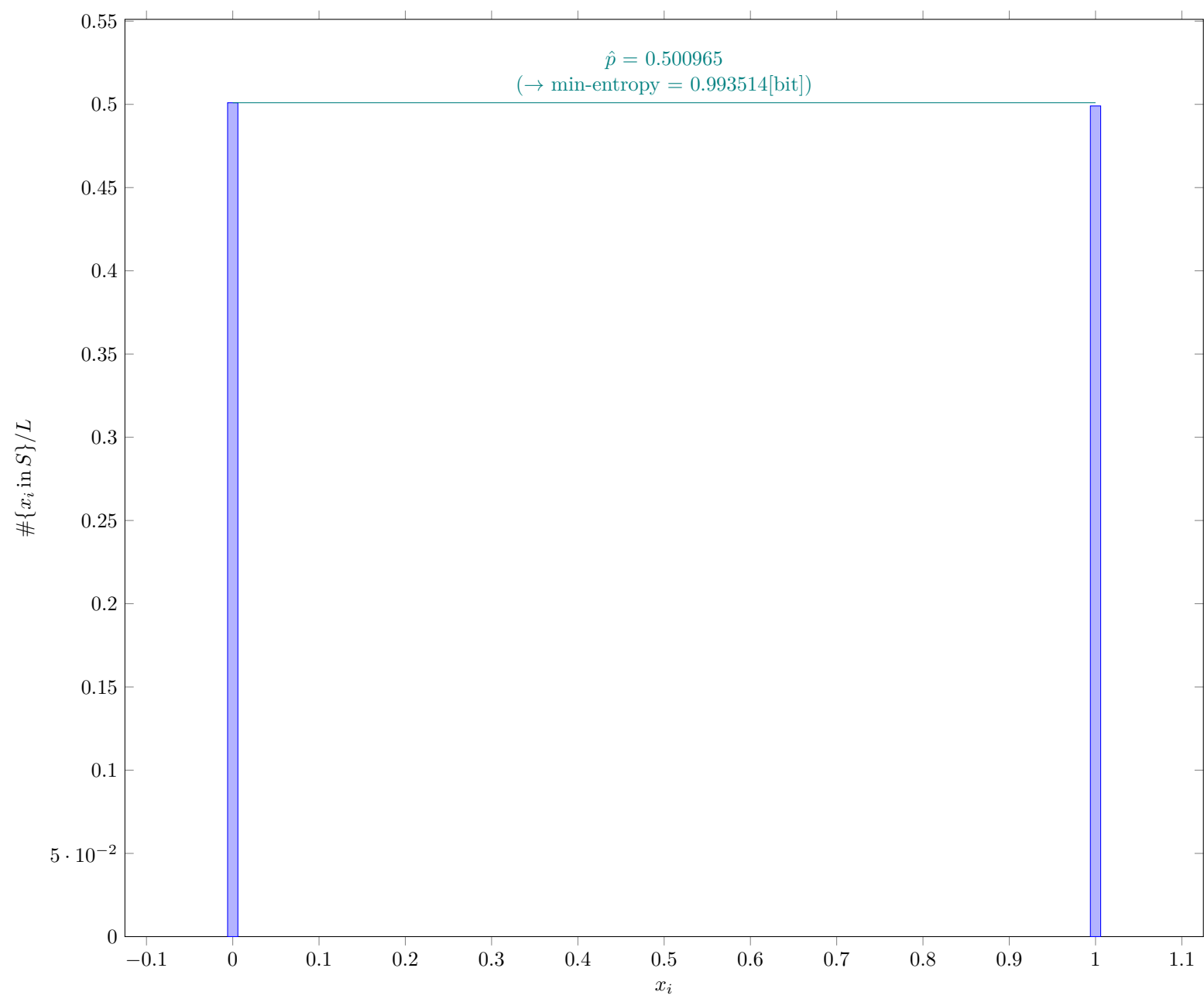


Fig. 1 Estimated Min-Entropy using §6.3 of NIST SP 800-90B

3 Detailed results of analysis from original samples

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

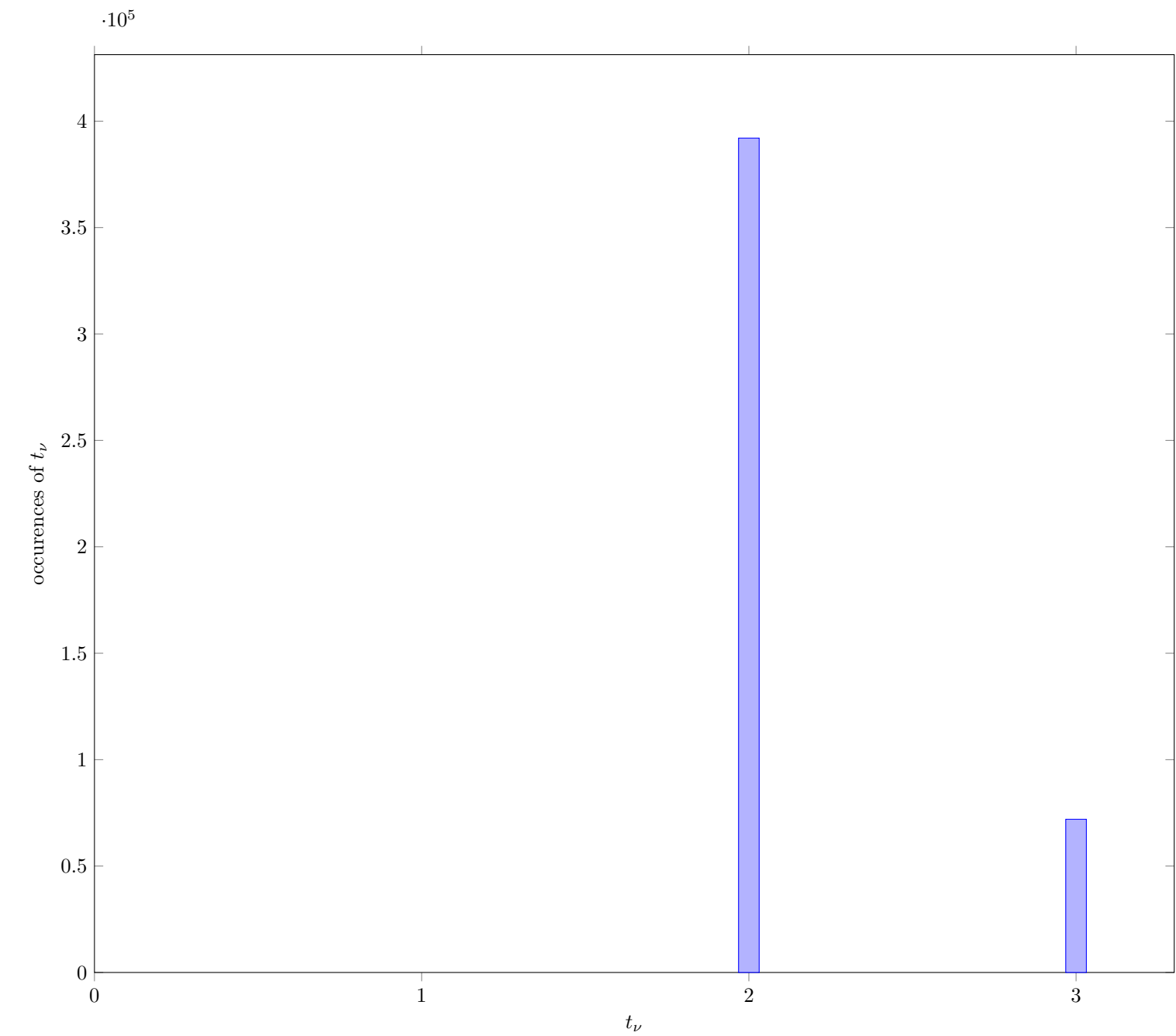


3.1.1 Supplemental information for traceability

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

Symbol	Value
mode	500965
\hat{p}	0.500965
p_u	0.502253

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



3.2.1 Supplemental information for traceability

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

Symbol	Value
p	0.916086
\bar{X}	2.15511
\bar{X}'	2.15375

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

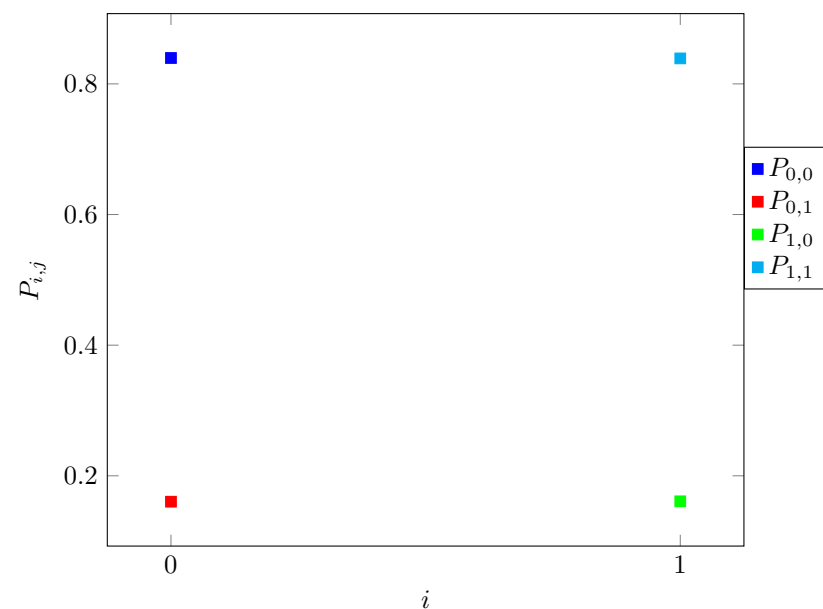


Fig. 2 Transition probability $P_{i,j}$ of §6.3.3 of NIST SP 800-90B

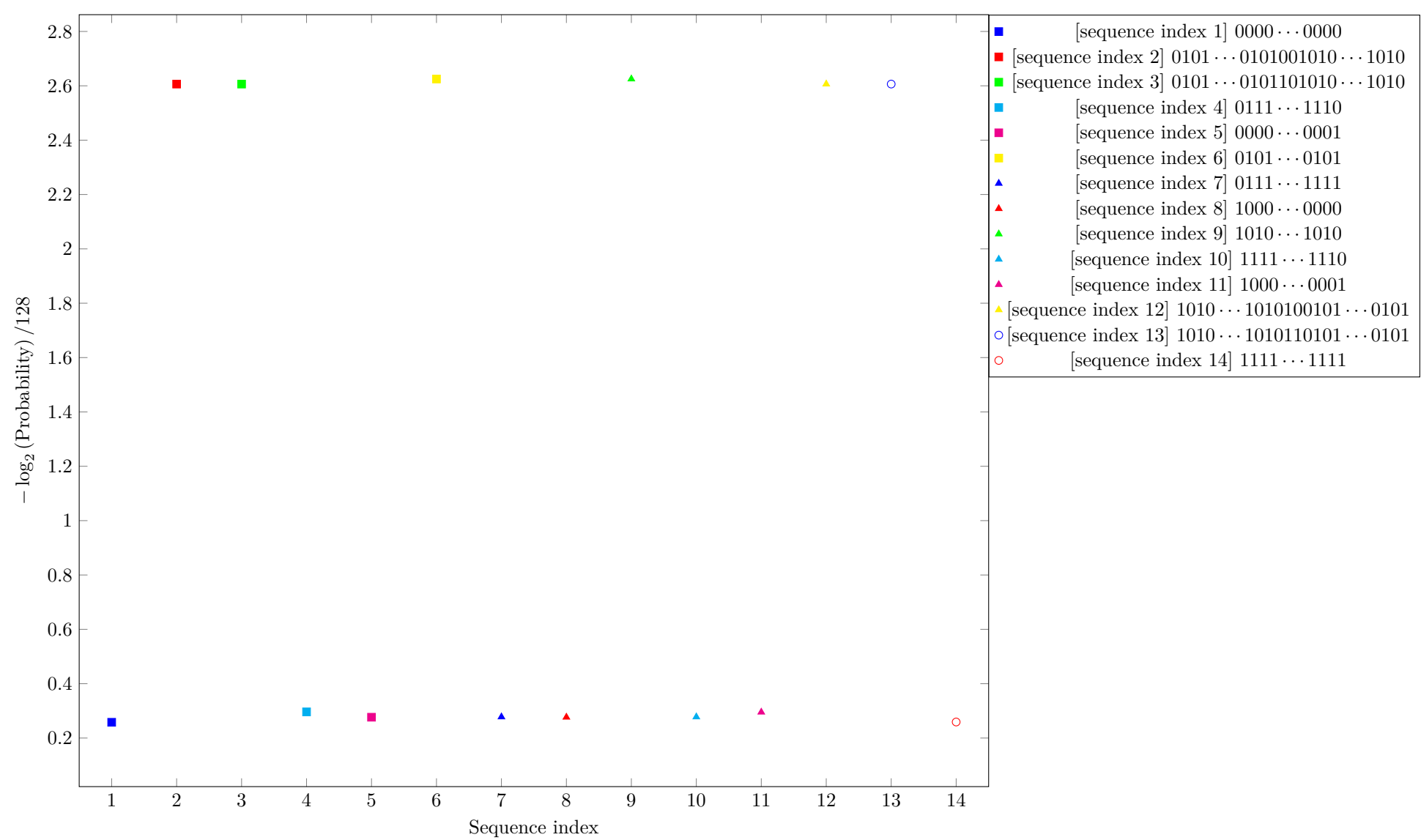
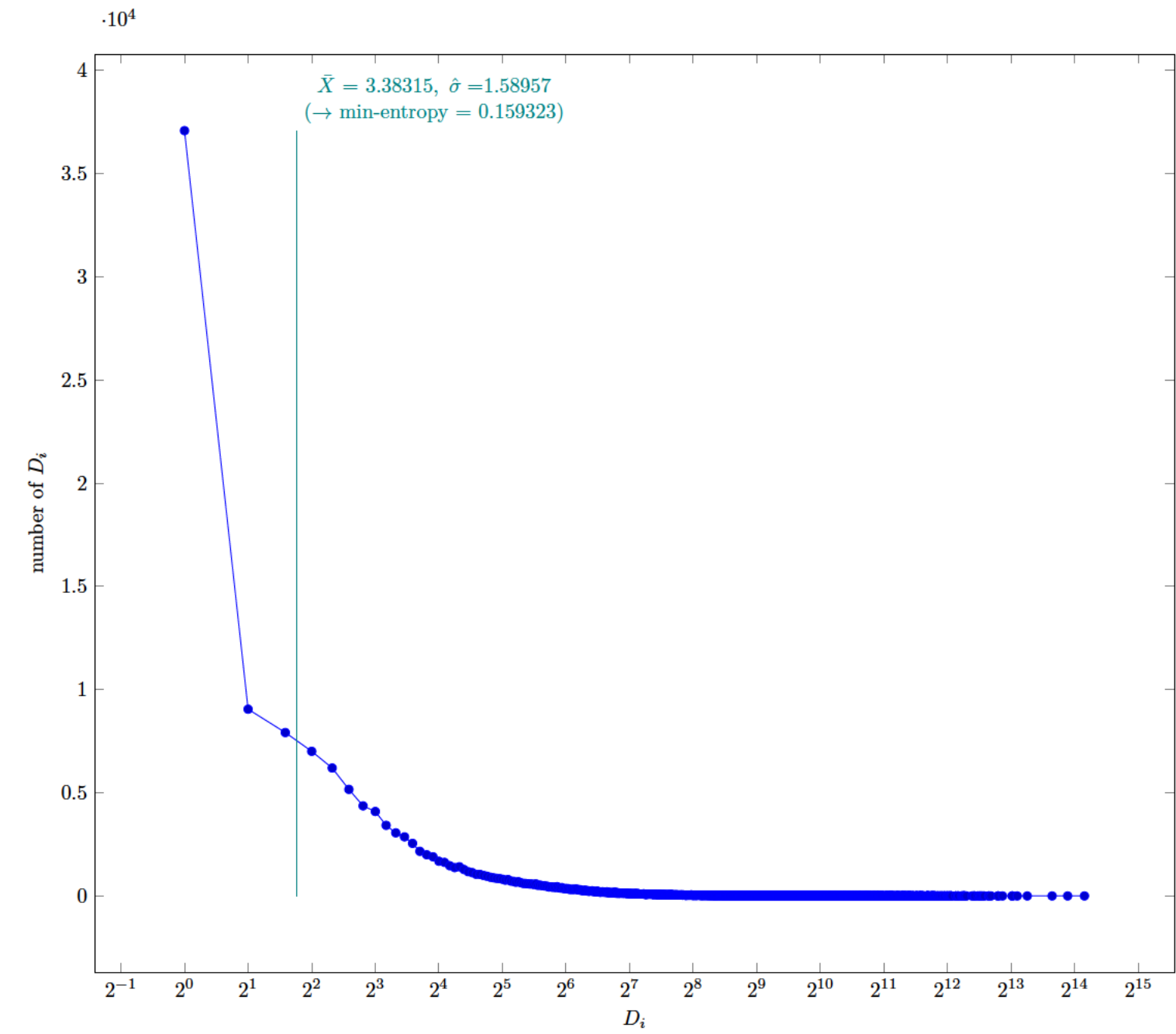


Fig. 3 Estimated Min-Entropy using §6.3.3 of NIST SP 800-90B

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



3.4.1 Supplemental information for traceability

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

Symbol	Value
p	0.515507
\bar{X}	3.38315
$\hat{\sigma}$	1.58957
\bar{X}'	3.37309

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

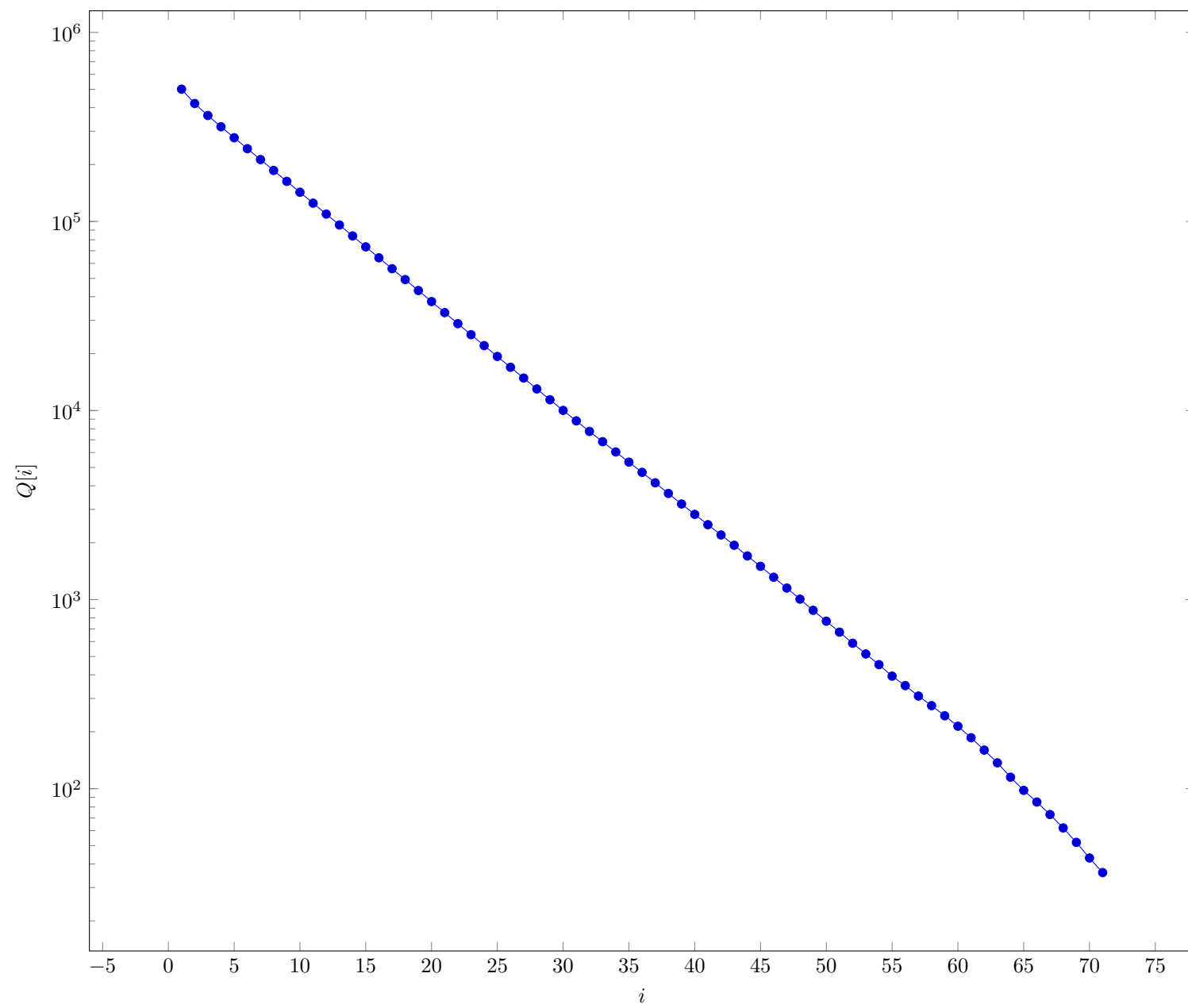


Fig. 4 Intermediate value $Q[i]$ in §6.3.5 of NIST SP 800-90B

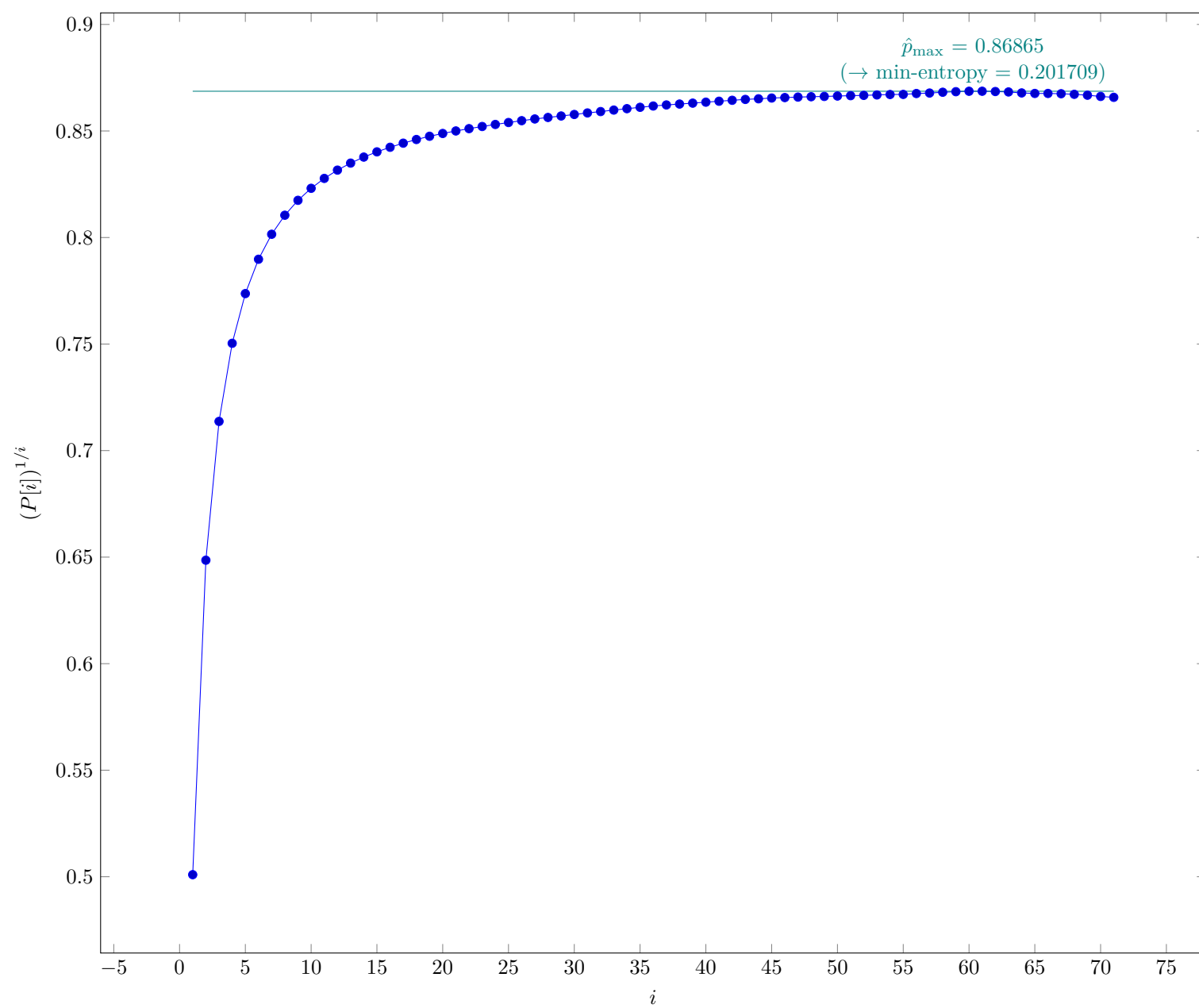


Fig. 5 $P[i]^{1/i}$ in §6.3.5 of NIST SP 800-90B

3.5.1 Supplemental information for traceability

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

Symbol	Value
t	71
\hat{p}_{\max}	0.86865
p_u	0.86952

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

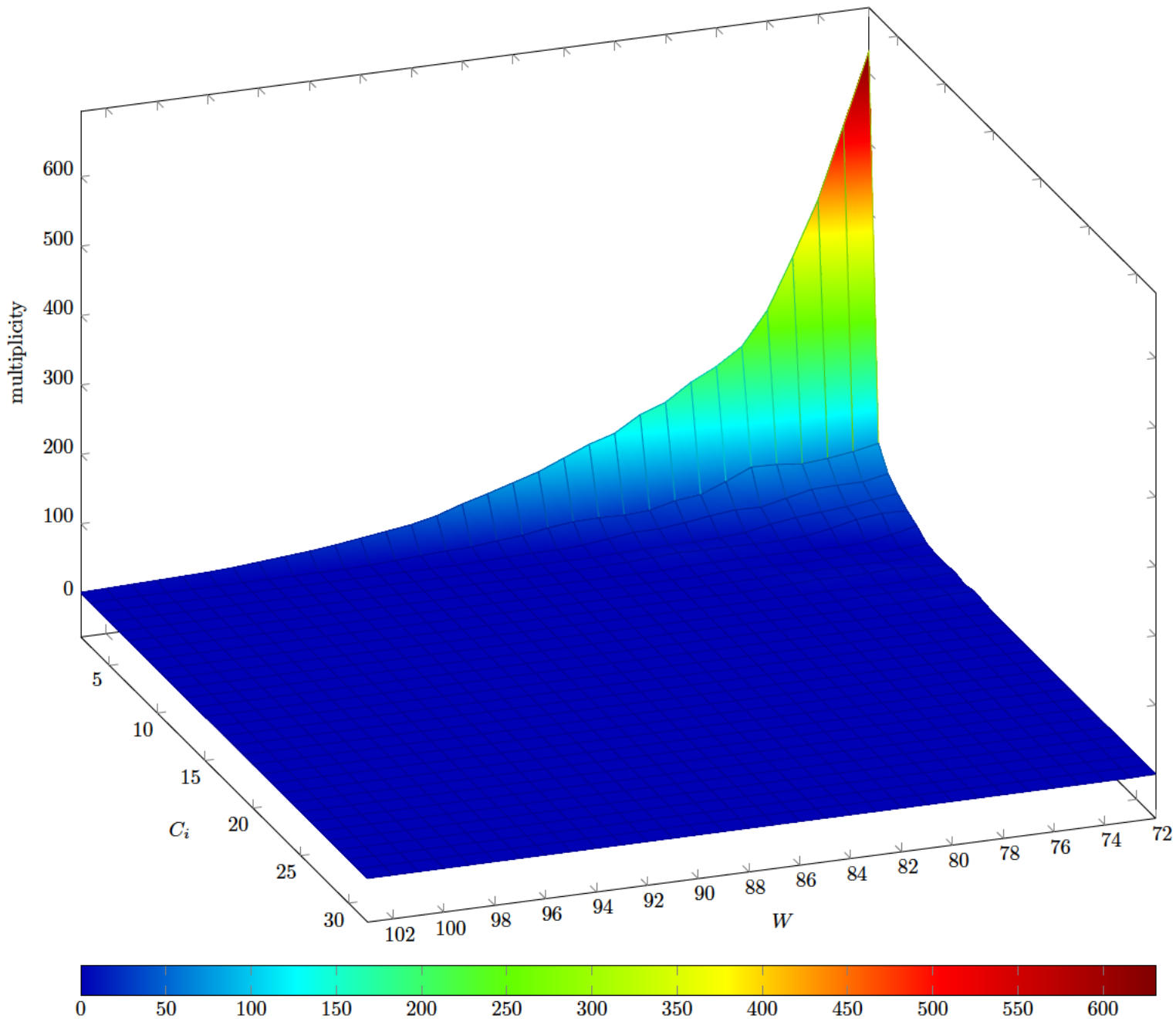


Fig. 6 Estimated W -tuple collision probability in Step 3 of §6.3.6 of NIST SP 800-90B

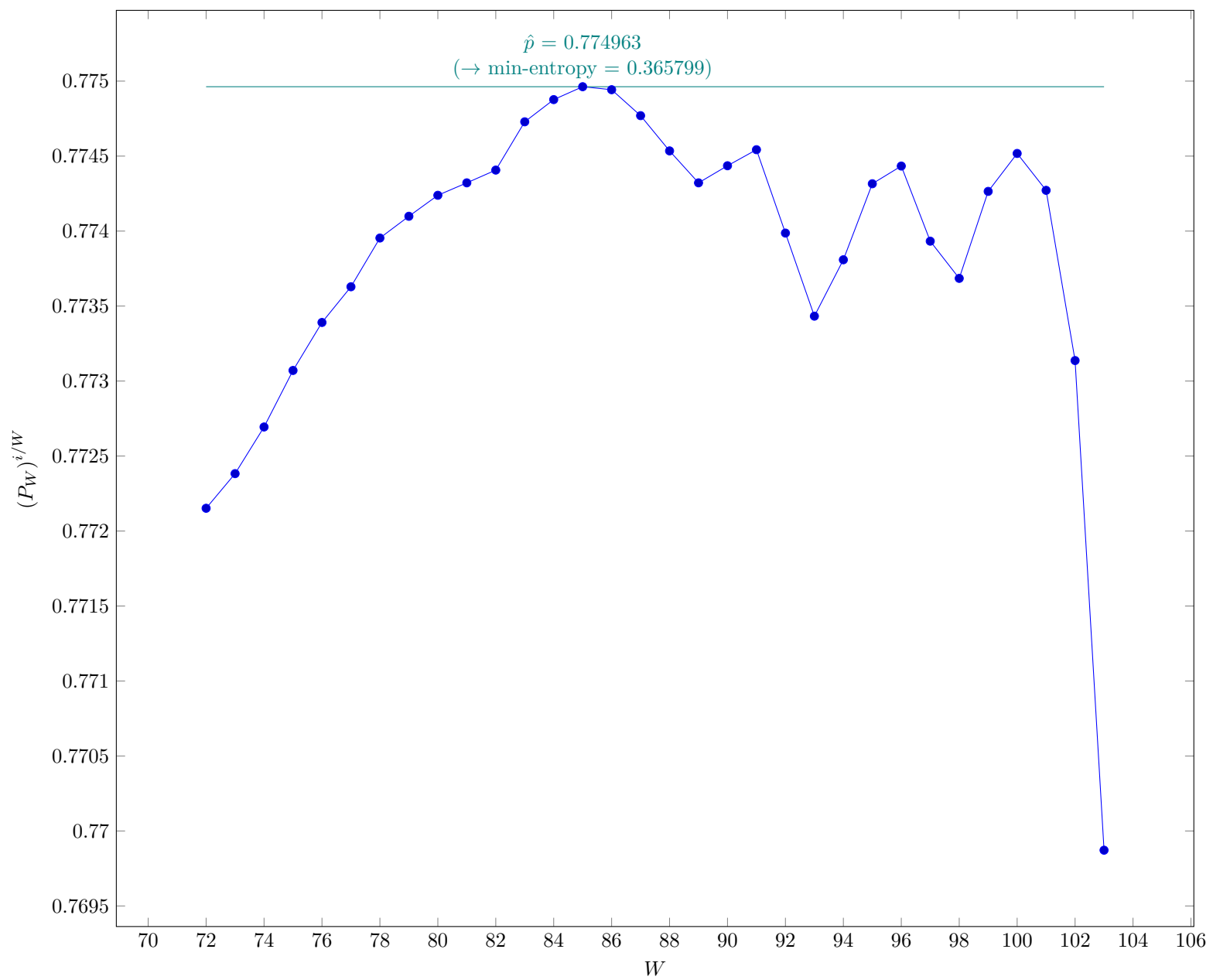


Fig. 7 Estimated average collision probability per string symbol in Step 3 of §6.3.6 of NIST SP 800-90B

3.6.1 Supplemental information for traceability

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

Symbol	Value
u	72
v	103
\hat{p}	0.774963
p_u	0.776039

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

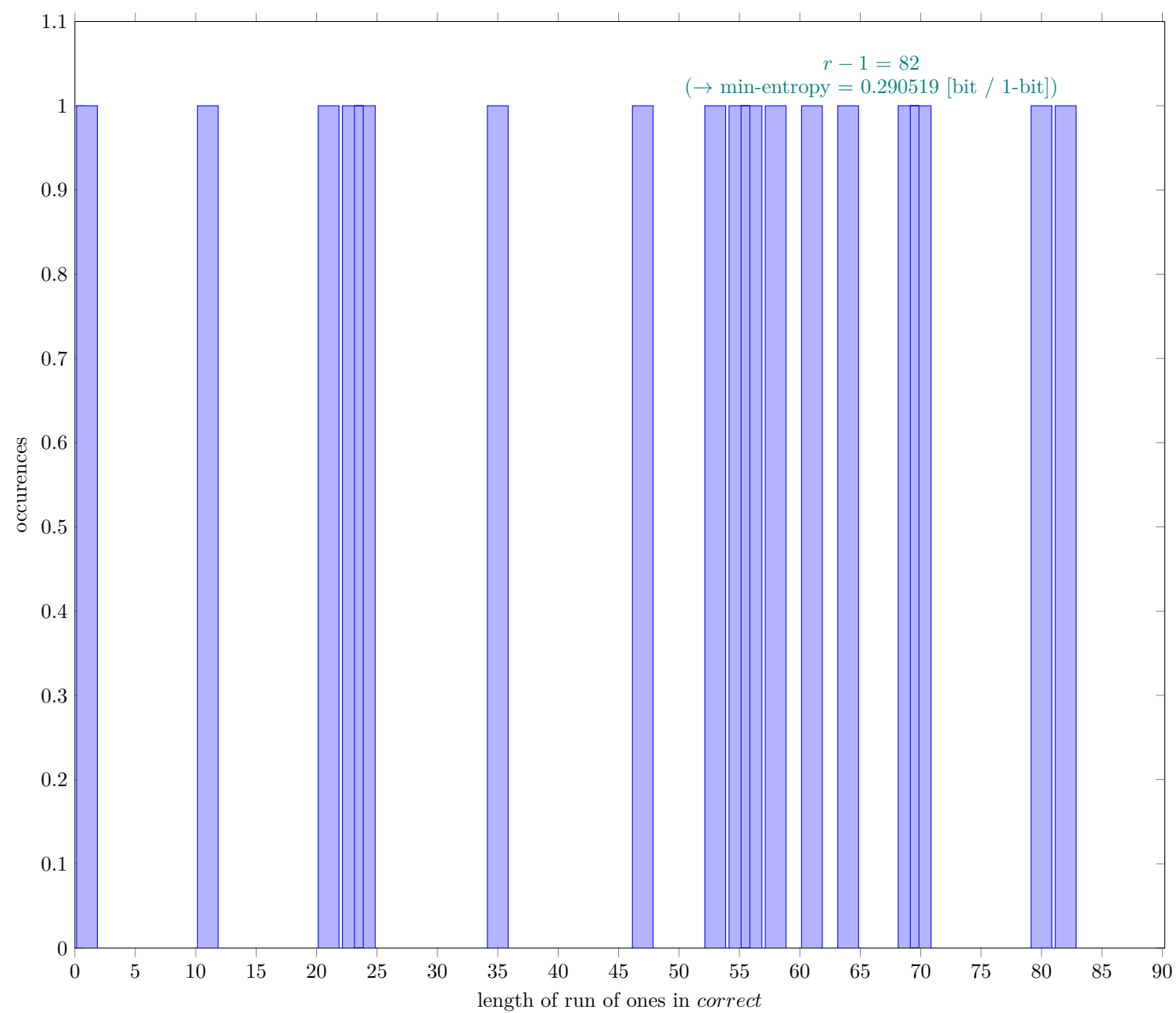


Fig. 8 Distribution of *correct*

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	561973
P_{global}	0.562008
P'_{global}	0.563286
r	83
P_{local}	0.817608

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

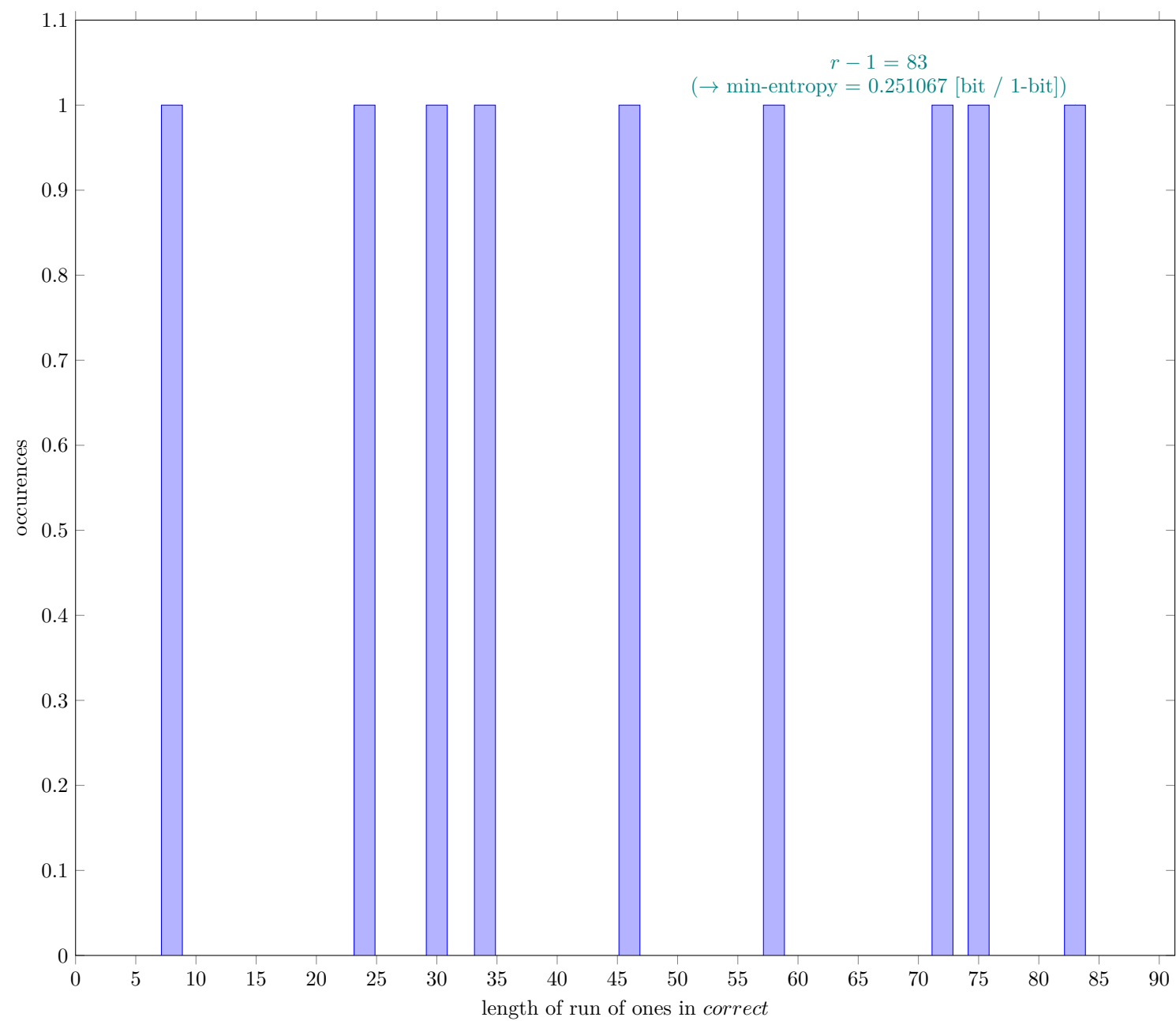


Fig. 9 Distribution of *correct*

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	839328
P_{global}	0.839329
P'_{global}	0.840275
r	84
P_{local}	0.819681

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

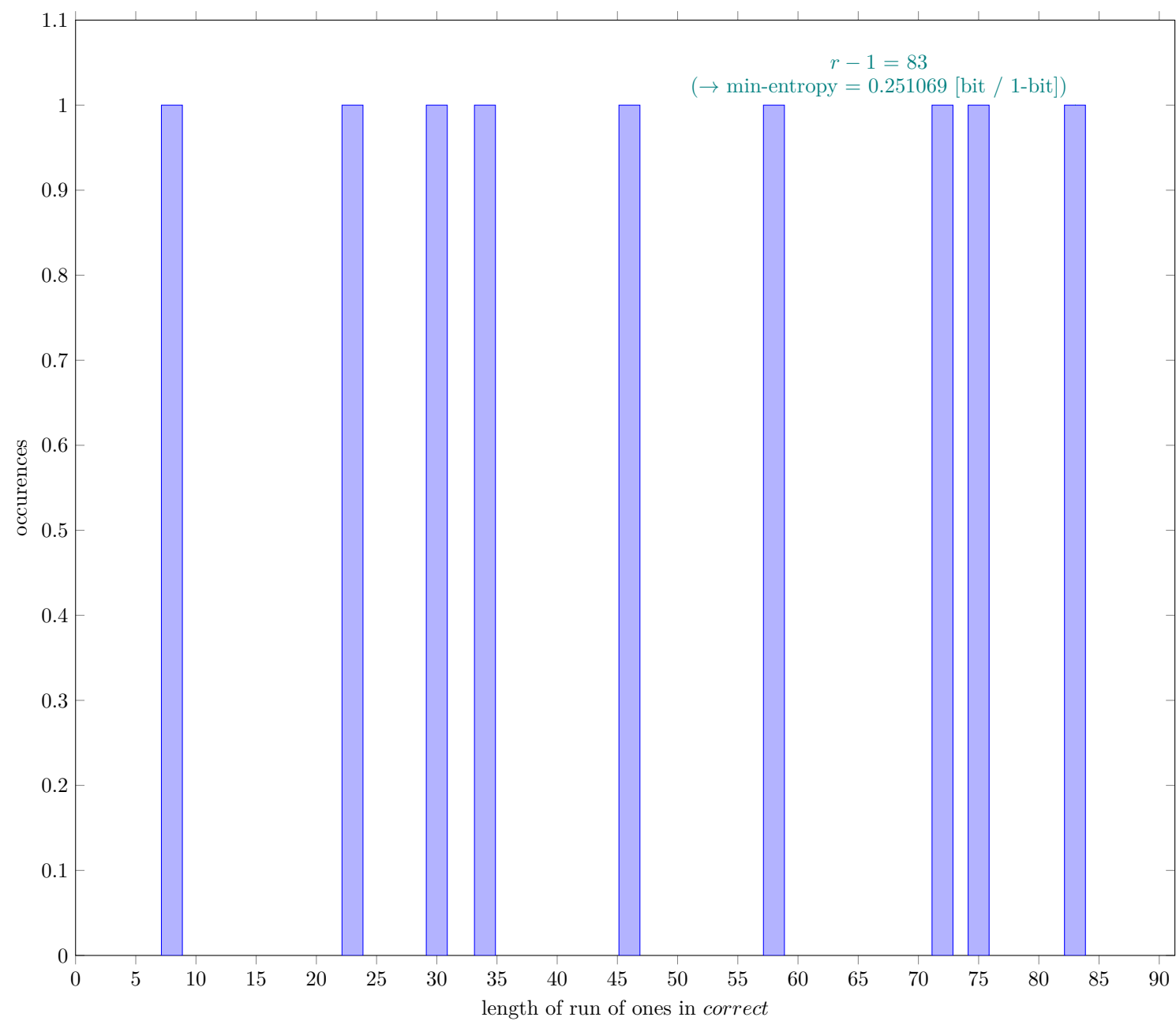


Fig. 10 Distribution of *correct*

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	839326
P_{global}	0.839328
P'_{global}	0.840274
r	84
P_{local}	0.819681

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

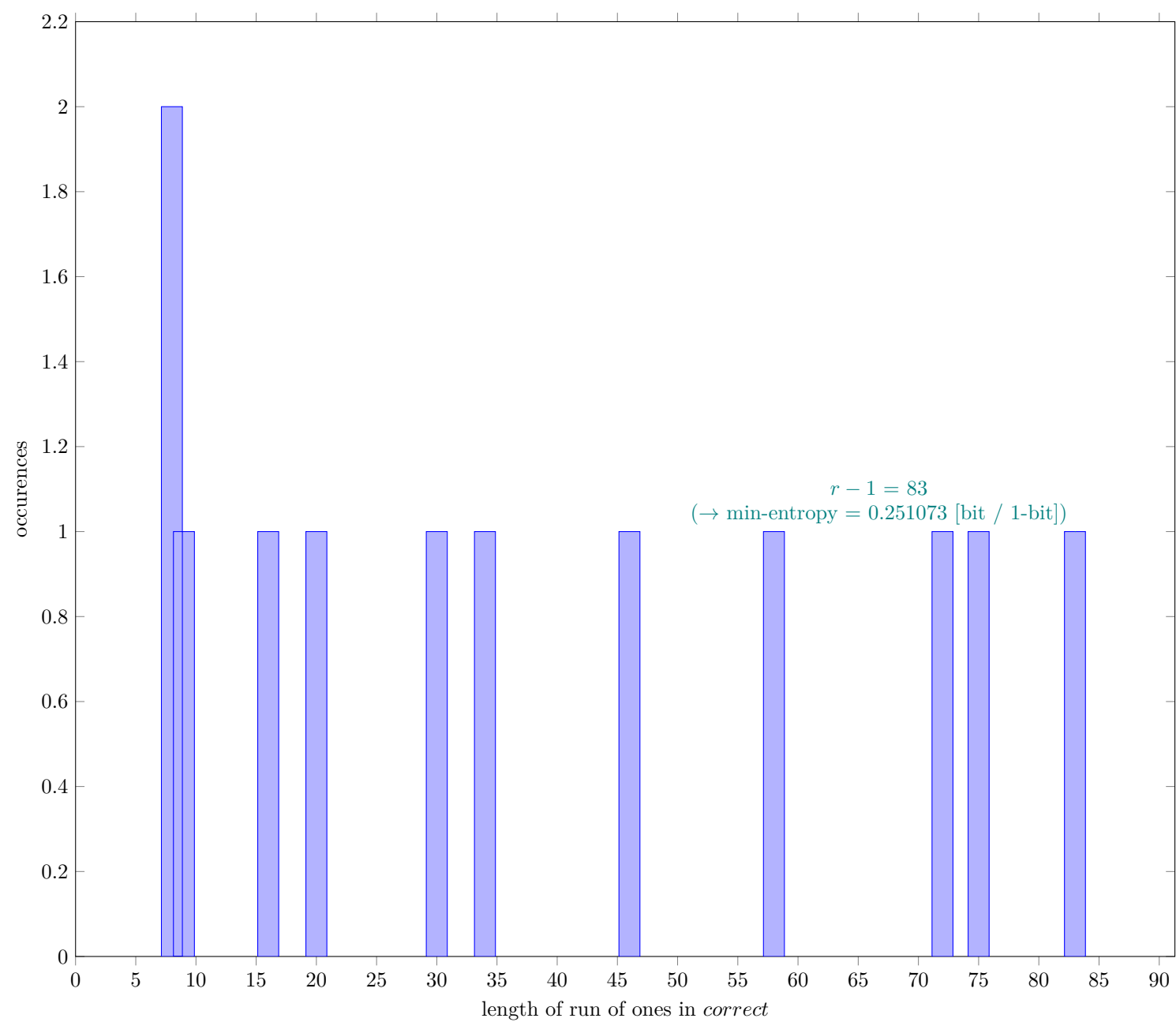


Fig. 11 Distribution of *correct*

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	839311
P_{global}	0.839325
P'_{global}	0.840271
r	84
P_{local}	0.819681

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