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

2023-Jan-03 00:09:42.139978

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/normal.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	5.62216	0.996315
The Collision Estimate	—	1
The Markov Estimate	—	0.993793
The Compression Estimate	—	0.512512
The t-Tuple Estimate	5.52912	0.772906
The Longest Repeated Substring (LRS) Estimate	6.10504	0.828399
Multi Most Common in Window Prediction Estimate	5.66817	1
The Lag Prediction Estimate	6.10622	0.997707
The MultiMMC Prediction Estimate	5.67576	0.676758
The LZ78Y Prediction Estimate	5.677	0.992461
The intial entropy source estimate [bit / 8 - bit] $H_I = \min(H_{\text{original}}, 8 \times H_{\text{bitstring}})$	4.1001	

[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

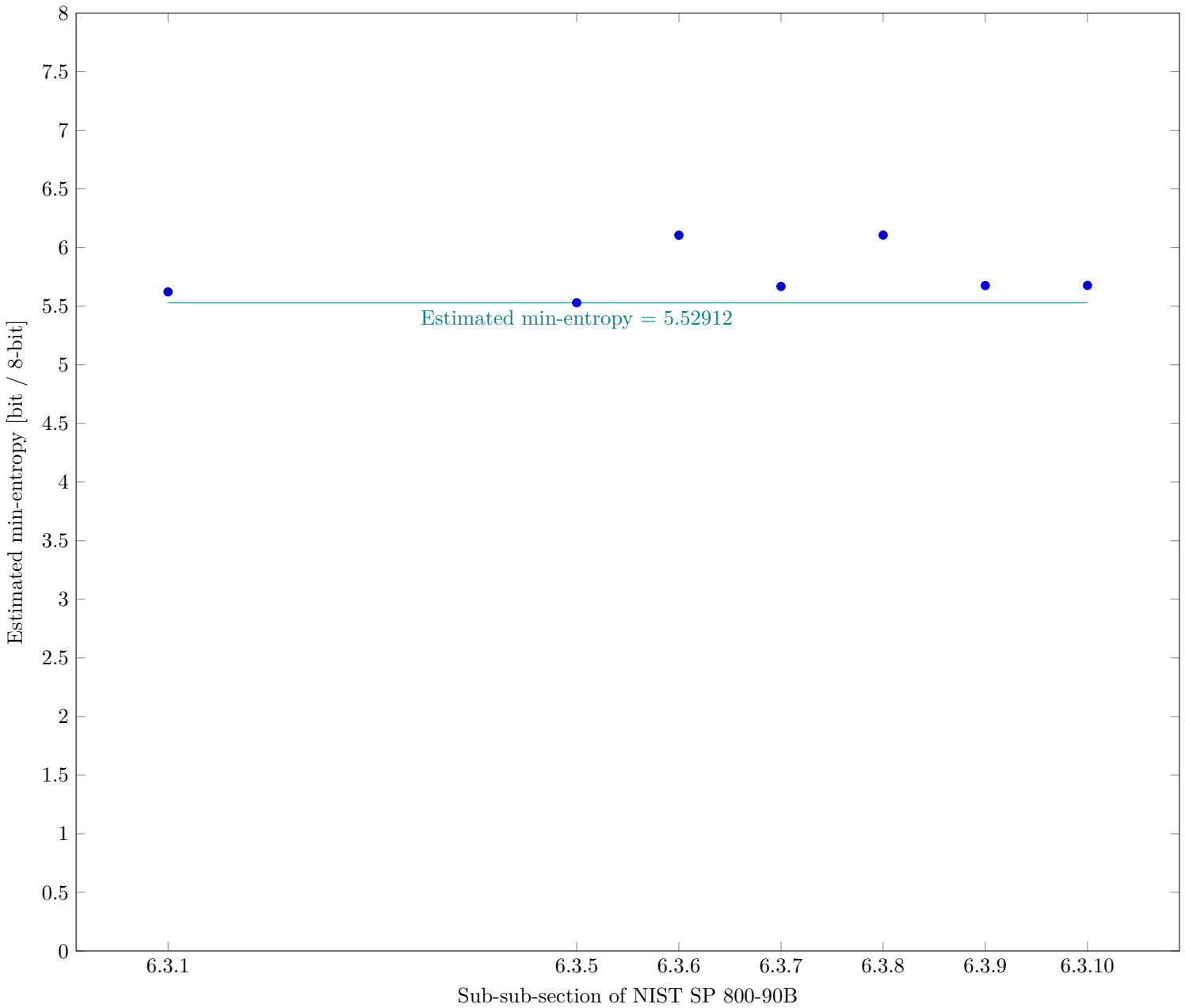


Fig. 1 Estimated Min-Entropy using §6.3 of NIST SP 800-90B

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

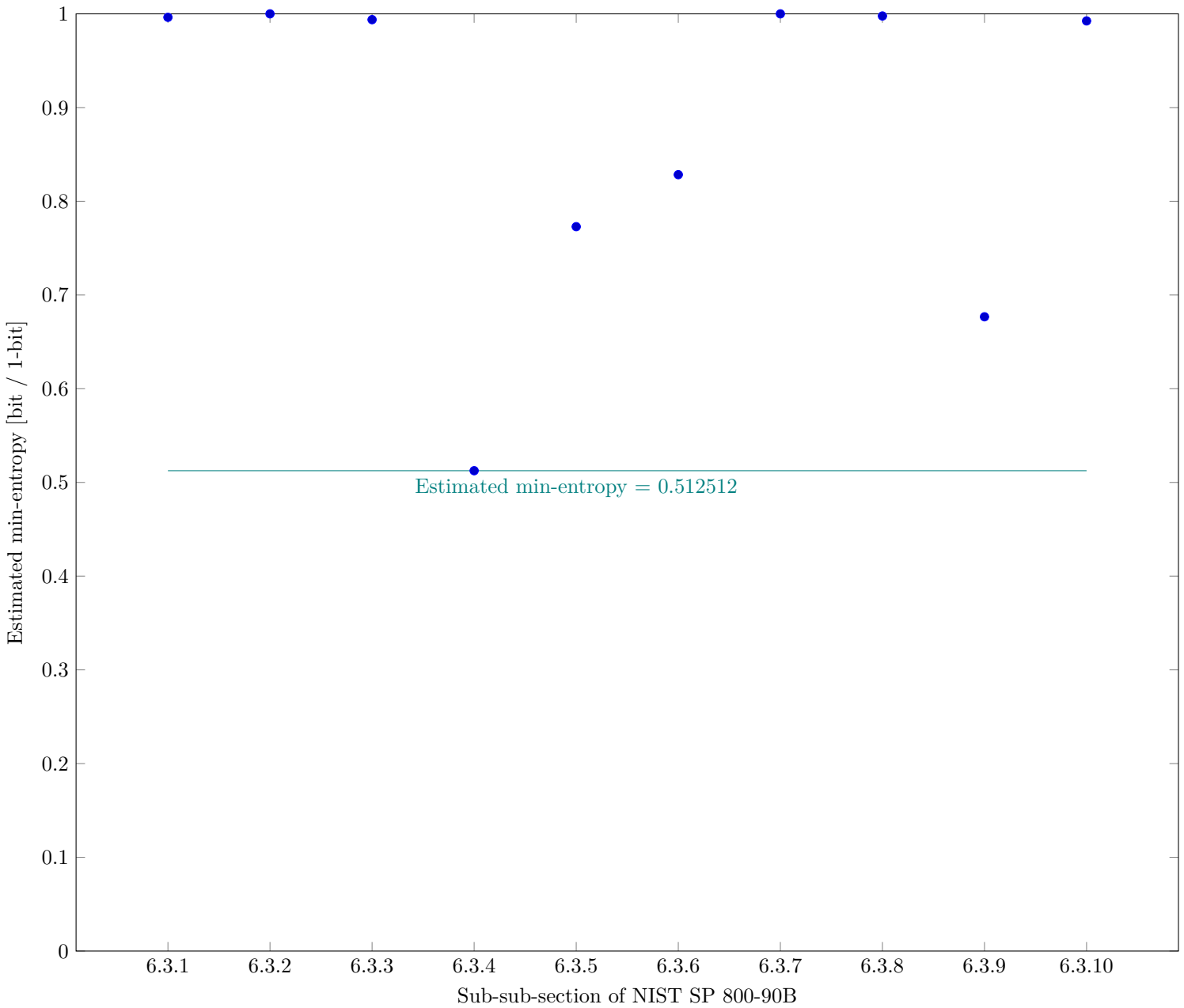
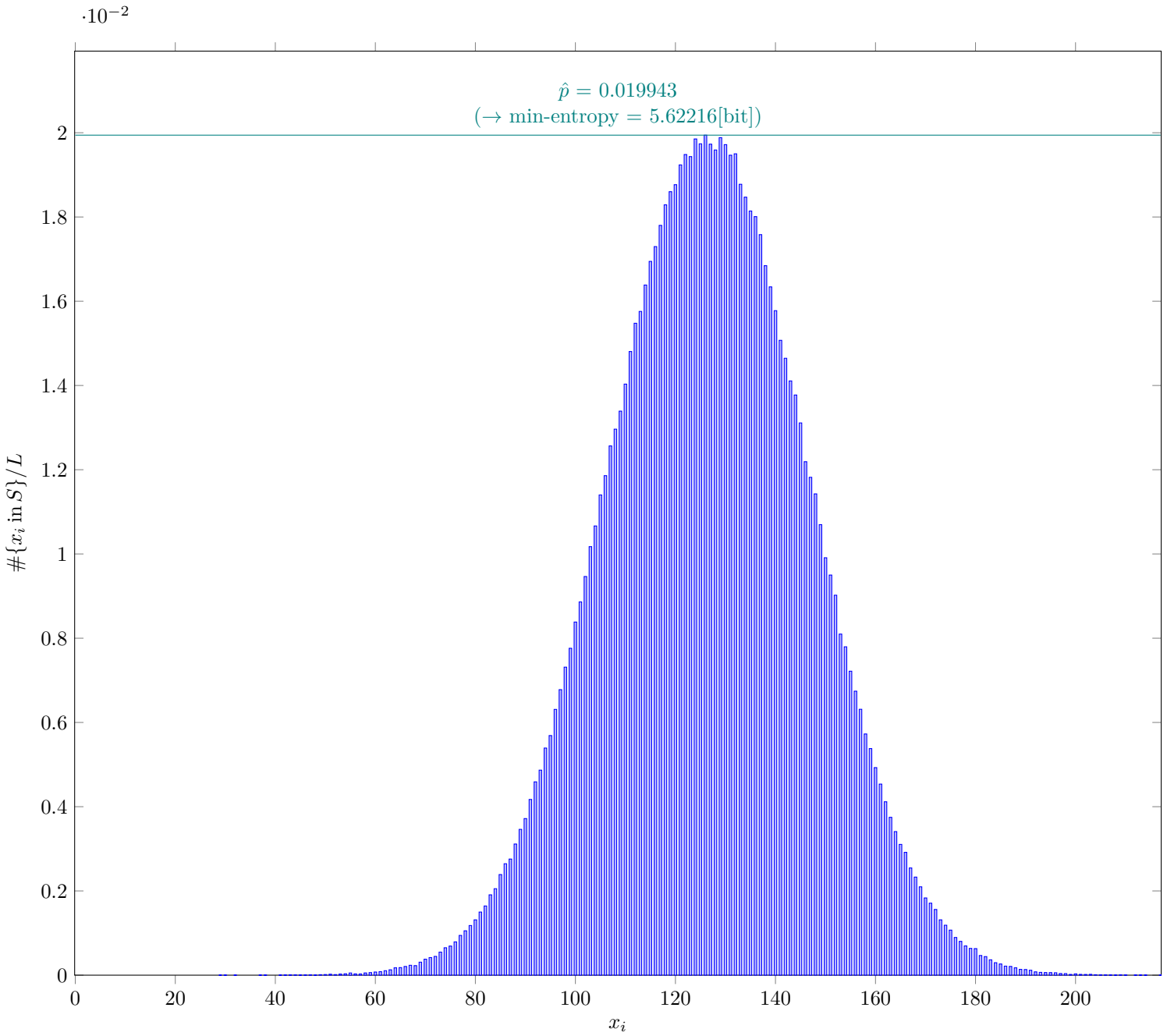


Fig. 2 Estimated Min-Entropy using §6.3 of NIST SP 800-90B

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	19943
$\hat{p}$	0.019943
p_u	0.0203031

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

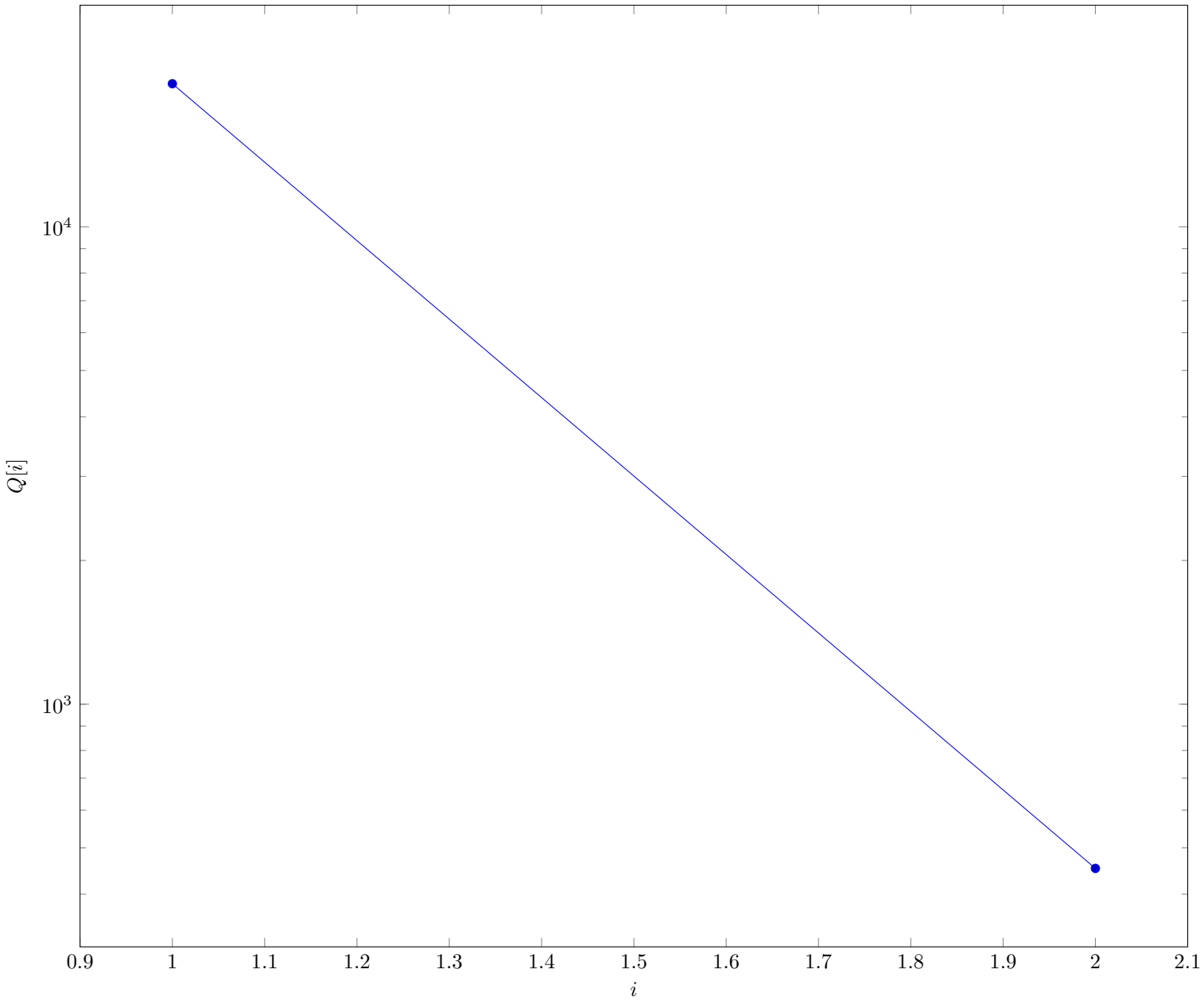


Fig. 3 Intermediate value $Q[i]$ in §6.3.5 of NIST SP 800-90B

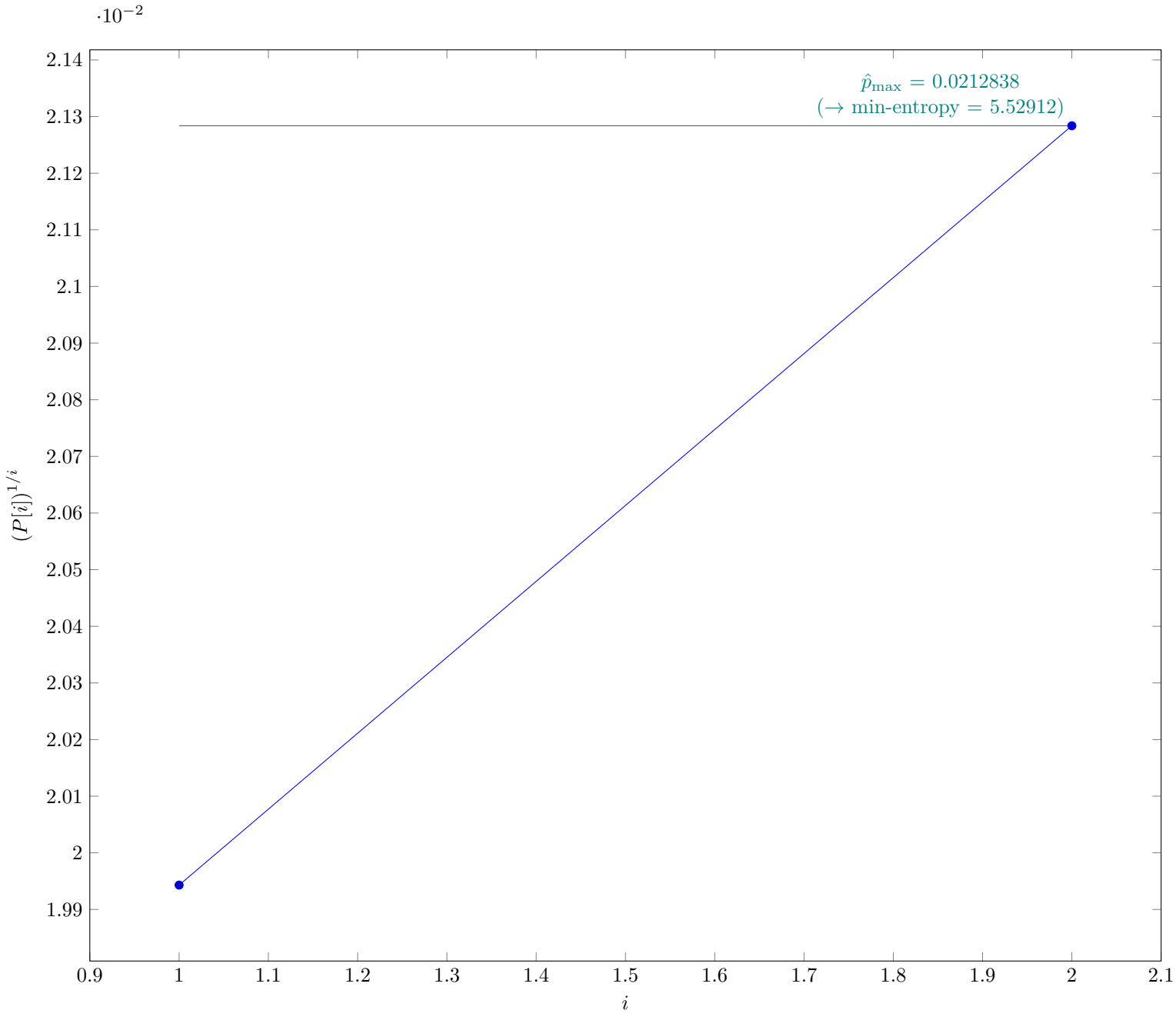


Fig. 4 $P[i]^{1/i}$ in §6.3.5 of NIST SP 800-90B

3.2.1 Supplemental information for traceability

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

Symbol	Value
t	2
$\hat{p}_{\max}$	0.0212838
p_u	0.0216556

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

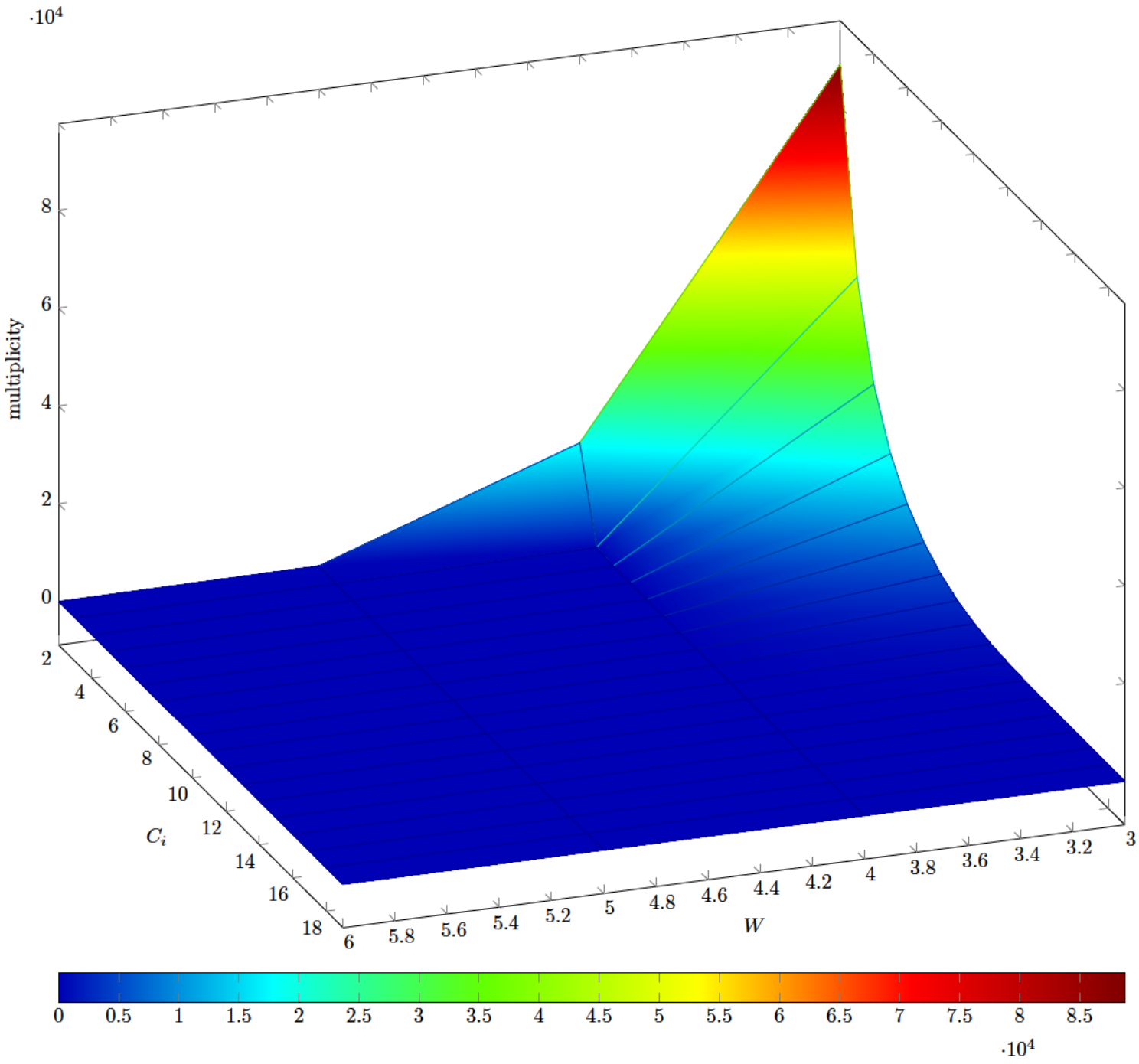


Fig. 5 Estimated W-tuple collision probability in Step 3 of §6.3.6 of NIST SP 800-90B

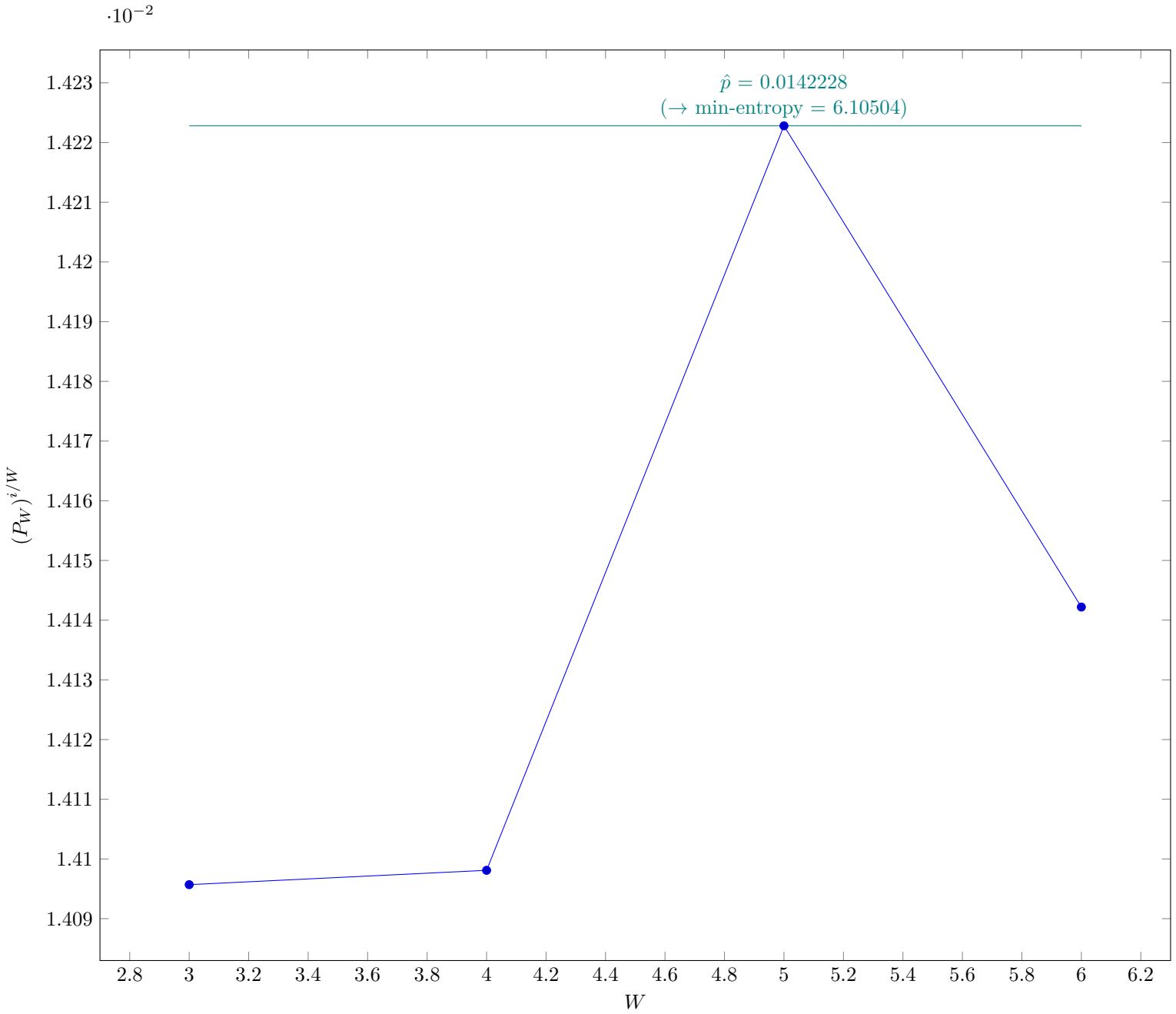


Fig. 6 Estimated average collision probability per string symbol in Step 3 of §6.3.6 of NIST SP 800-90B

3.3.1 Supplemental information for traceability

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

Symbol	Value
u	3
v	6
$\hat{p}$	0.0142228
p_u	0.0145278

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

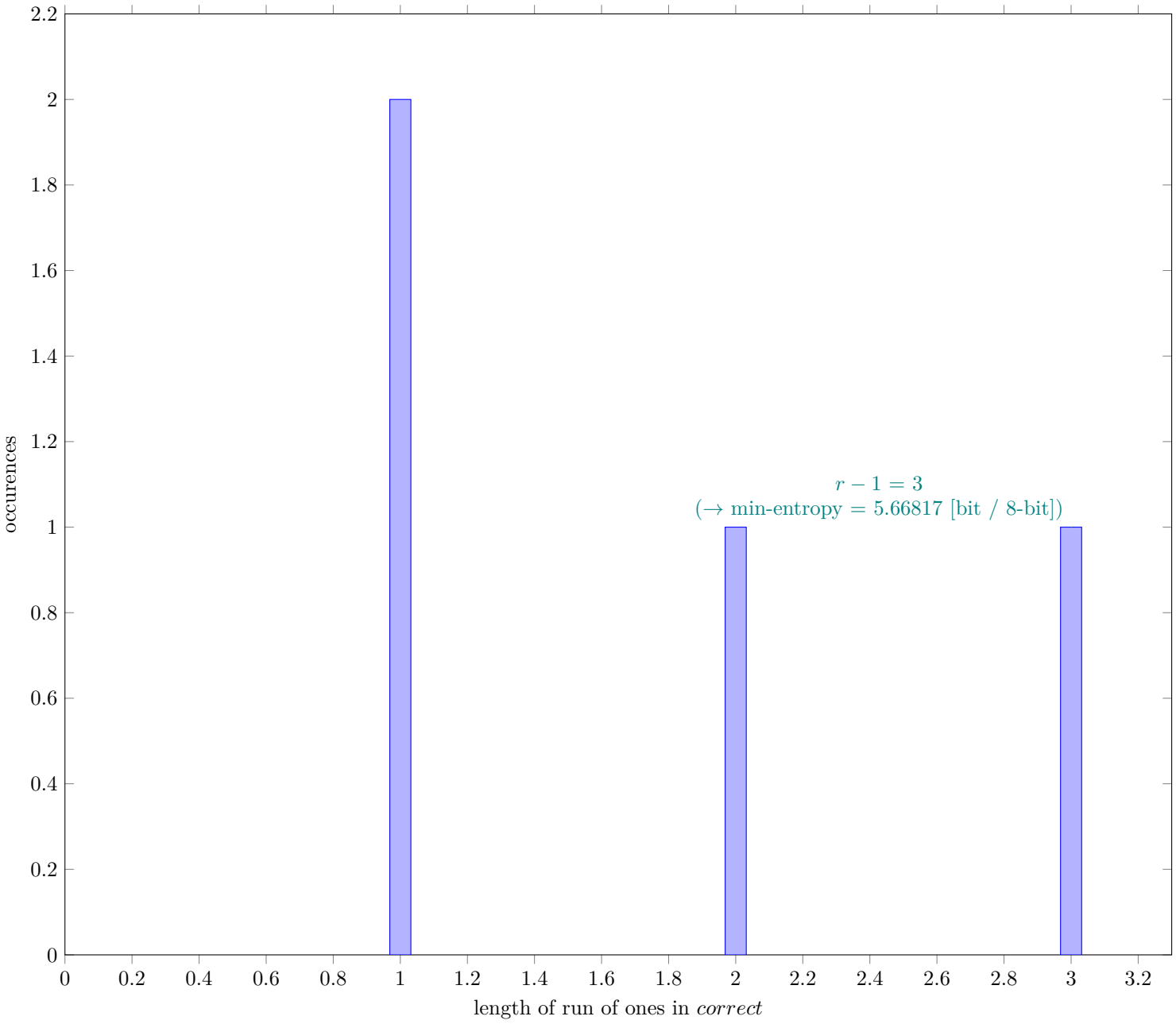


Fig. 7 Distribution of *correct*

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	19310
P_{global}	0.0193112
P'_{global}	0.0196657
r	4
P_{local}	0.010038

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

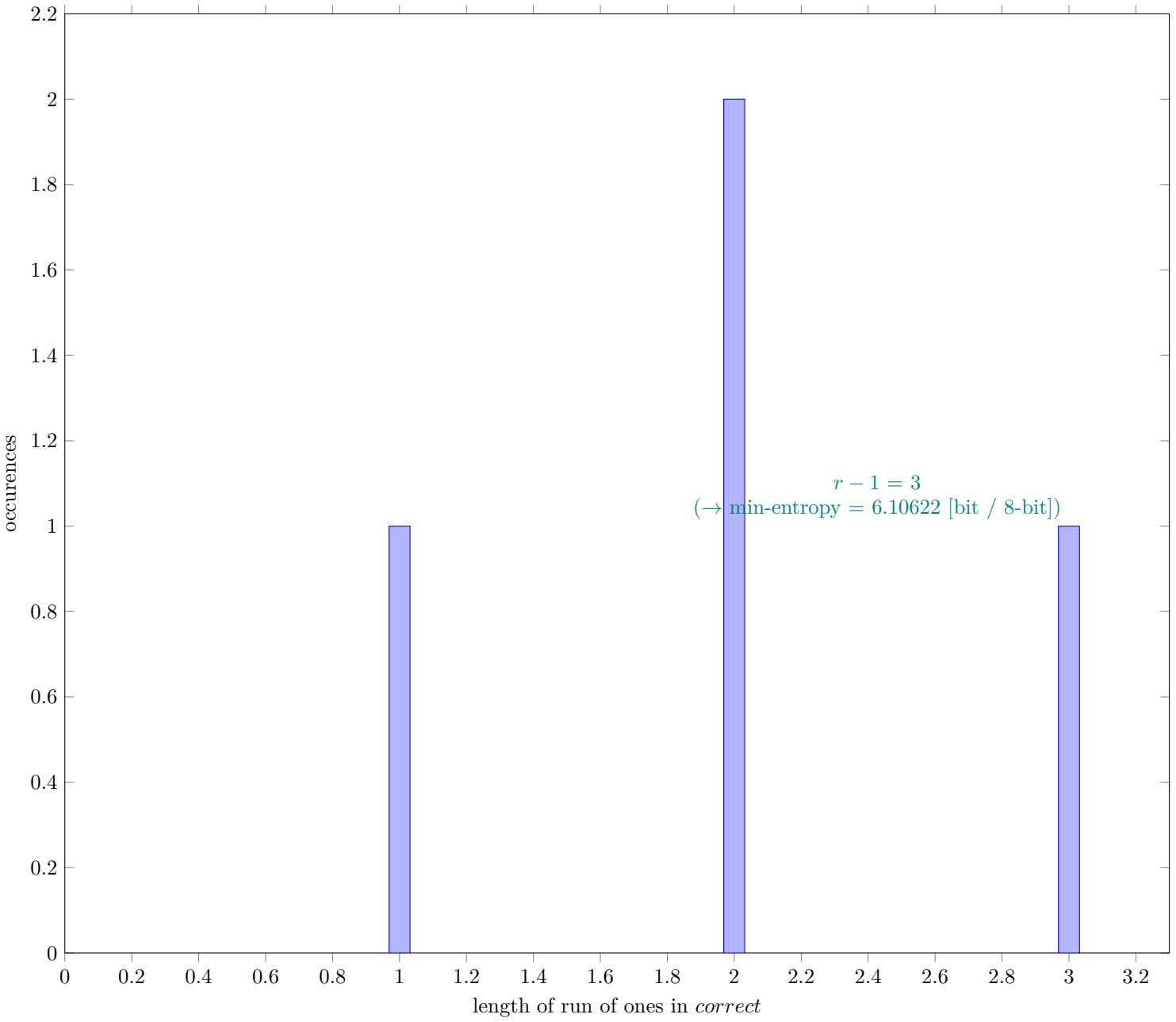


Fig. 8 Distribution of *correct*

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	14211
P_{global}	0.014211
P'_{global}	0.0145159
r	4
P_{local}	0.0100379

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

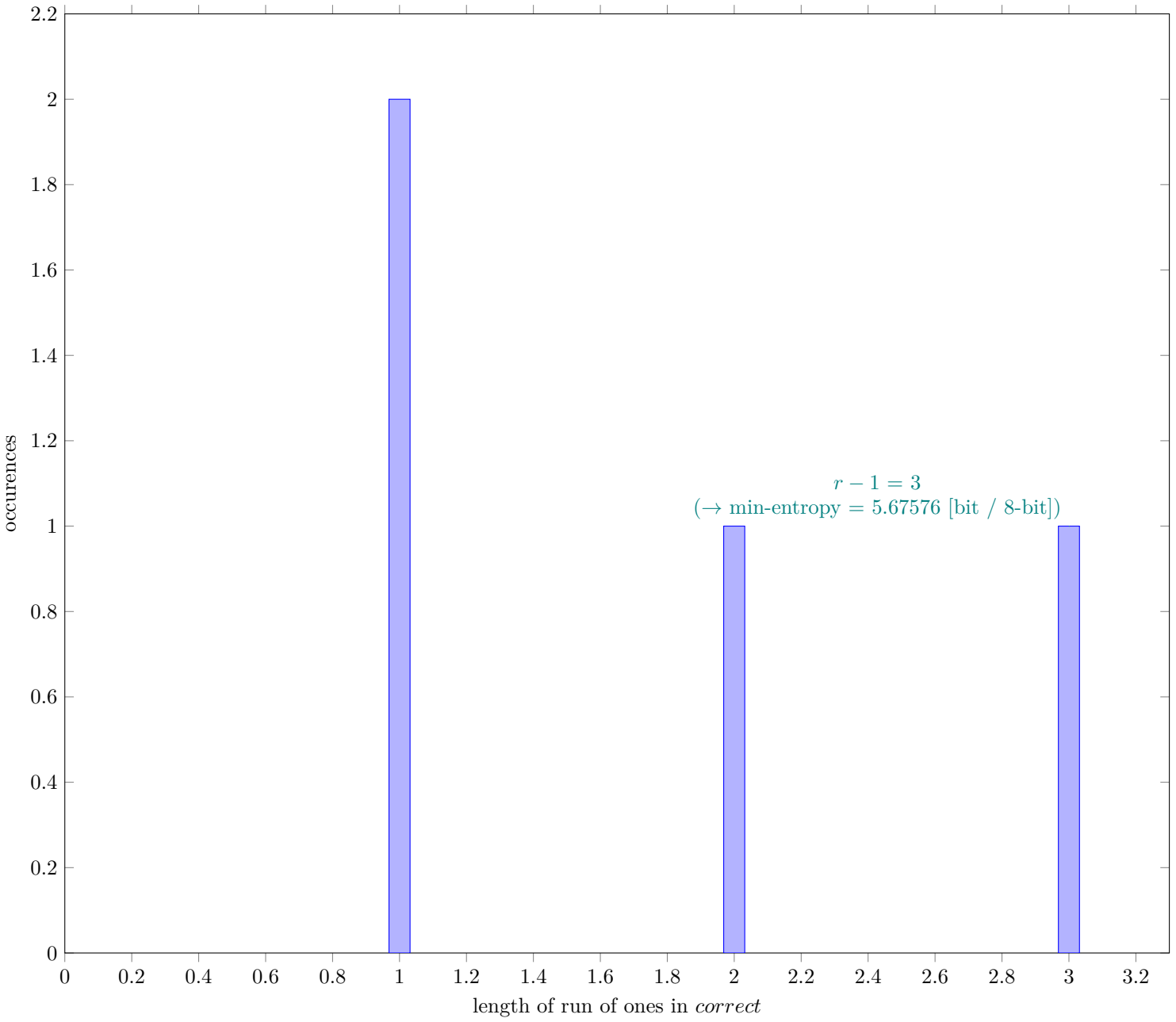


Fig. 9 Distribution of *correct*

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	19209
P_{global}	0.019209
P'_{global}	0.0195626
r	4
P_{local}	0.0100379

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

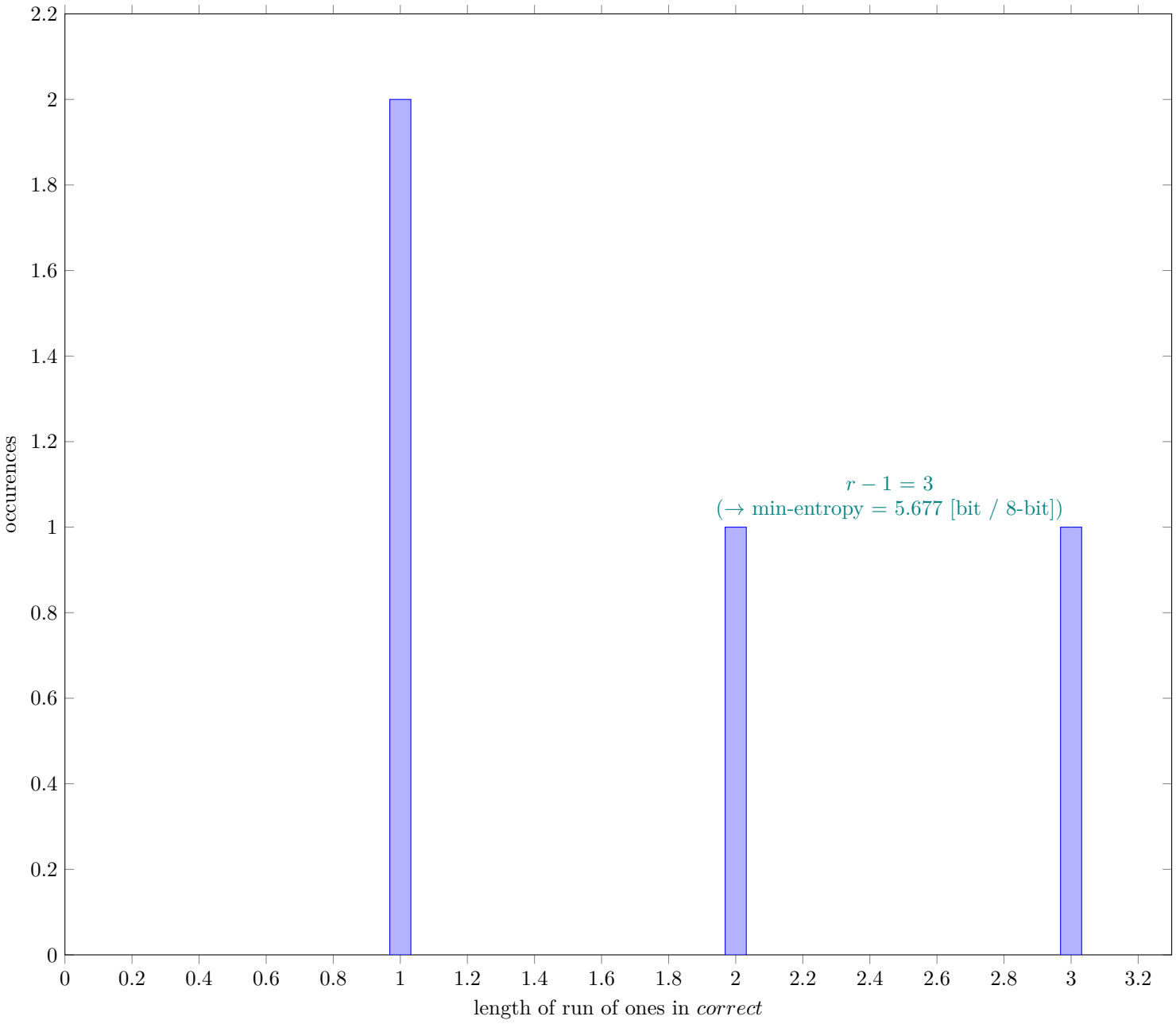


Fig. 10 Distribution of *correct*

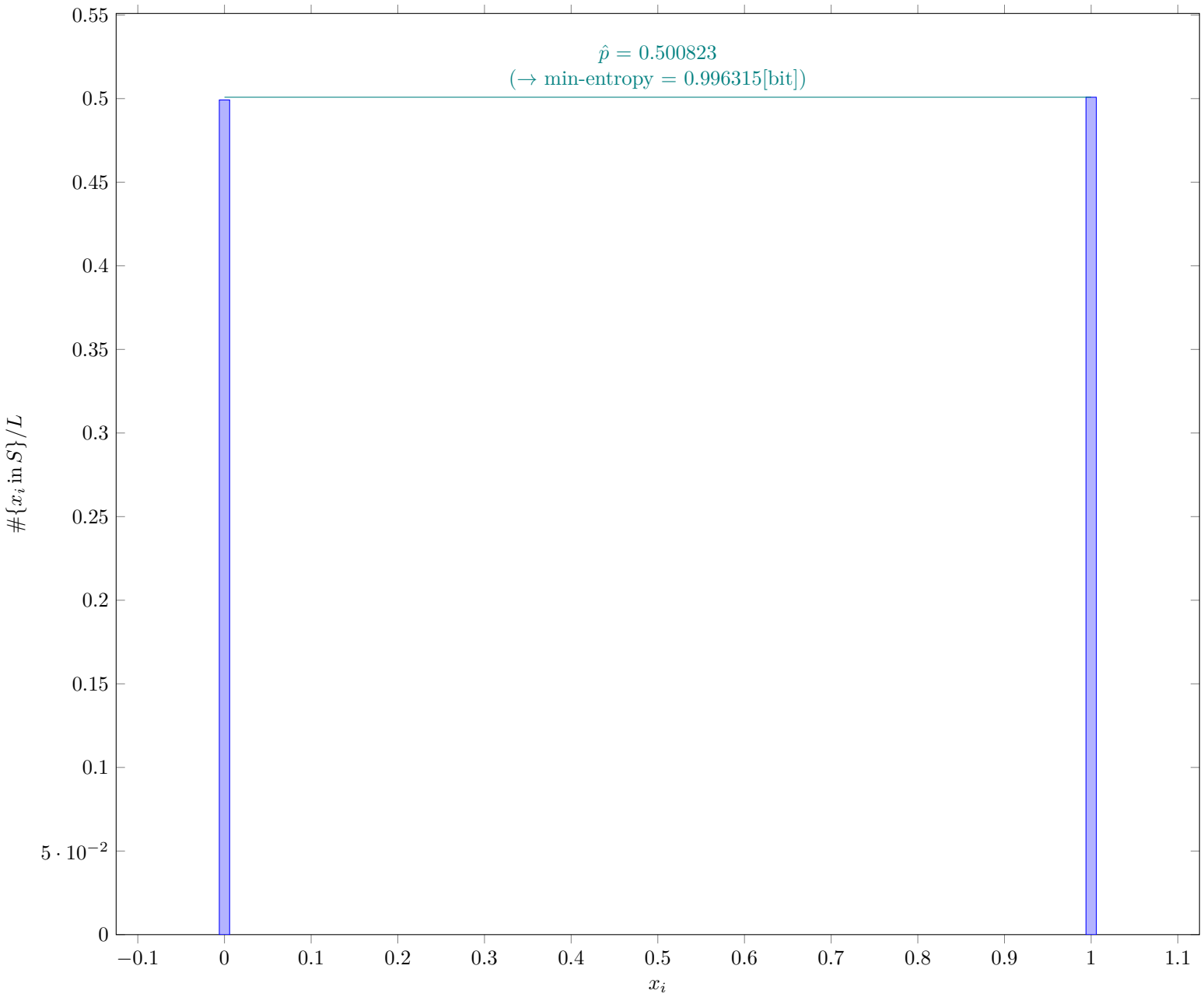
3.7.1 Supplemental information for traceability

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

Symbol	Value
N	999983
C	19192
P_{global}	0.0191923
P'_{global}	0.0195457
r	4
P_{local}	0.0100379

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)

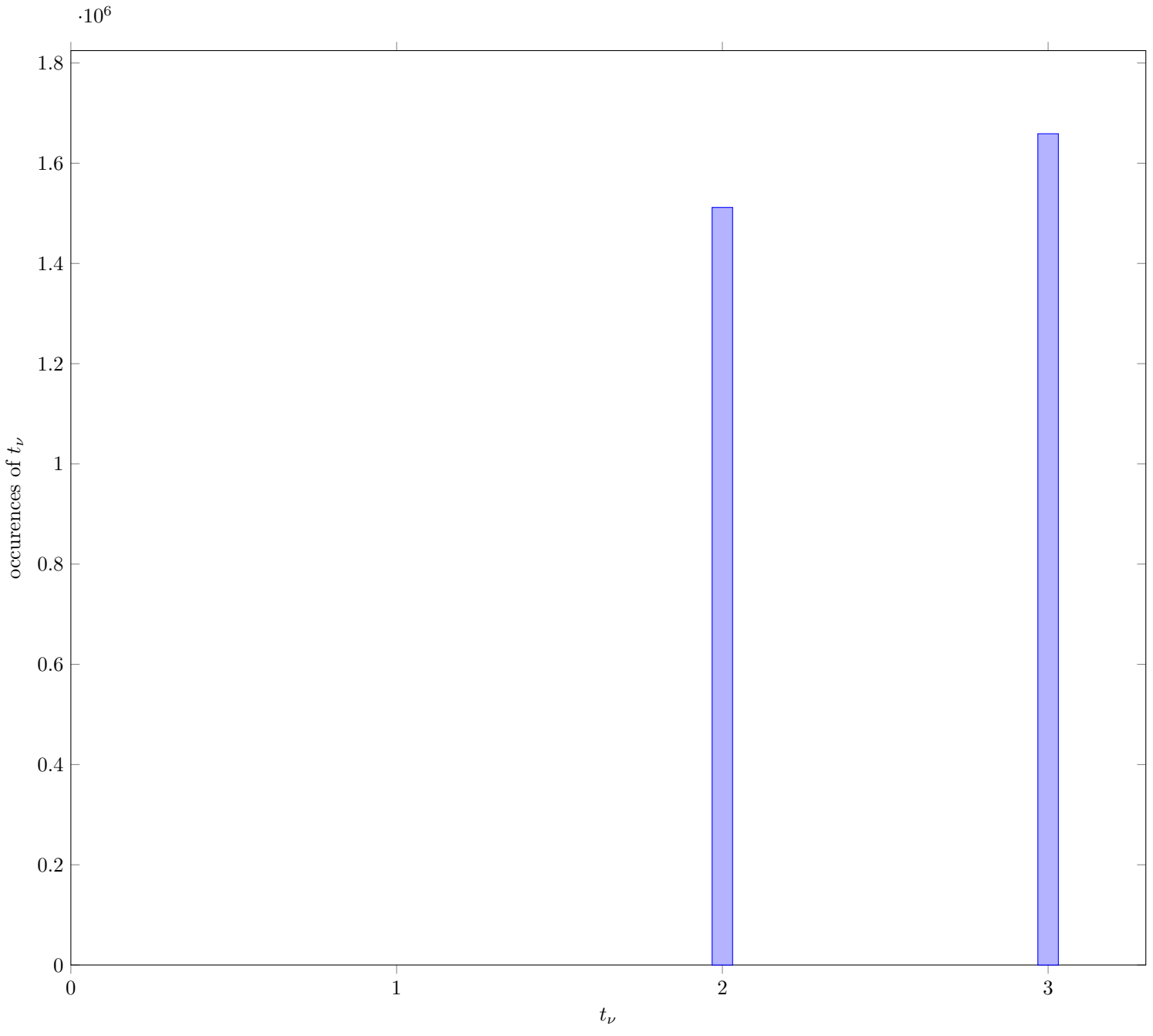


4.1.1 Supplemental information for traceability

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

Symbol	Value
mode	4006586
$\hat{p}$	0.500823
p_u	0.501279

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	0.5
$\bar{X}$	2.52319
$\bar{X}'$	2.52247

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

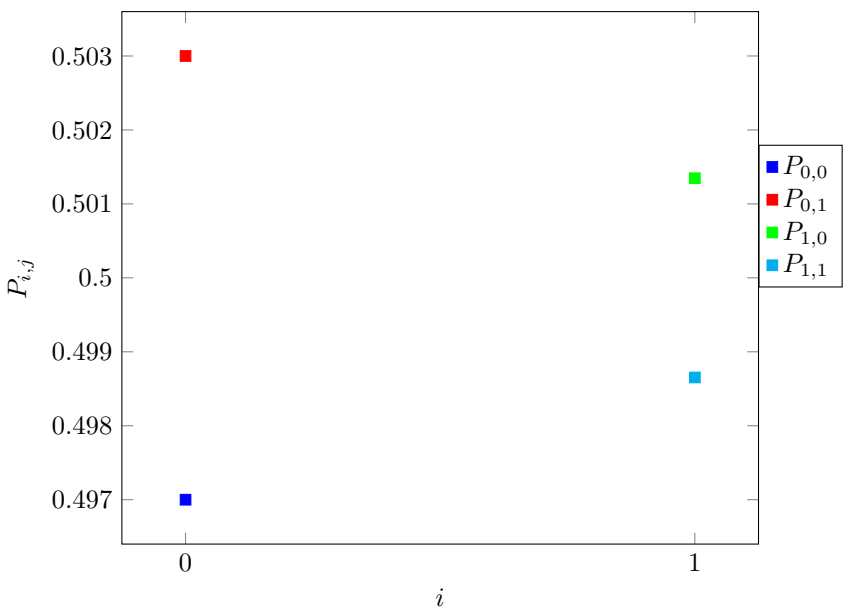


Fig. 11 Transition probability $P_{i,j}$ of §6.3.3 of NIST SP 800-90B

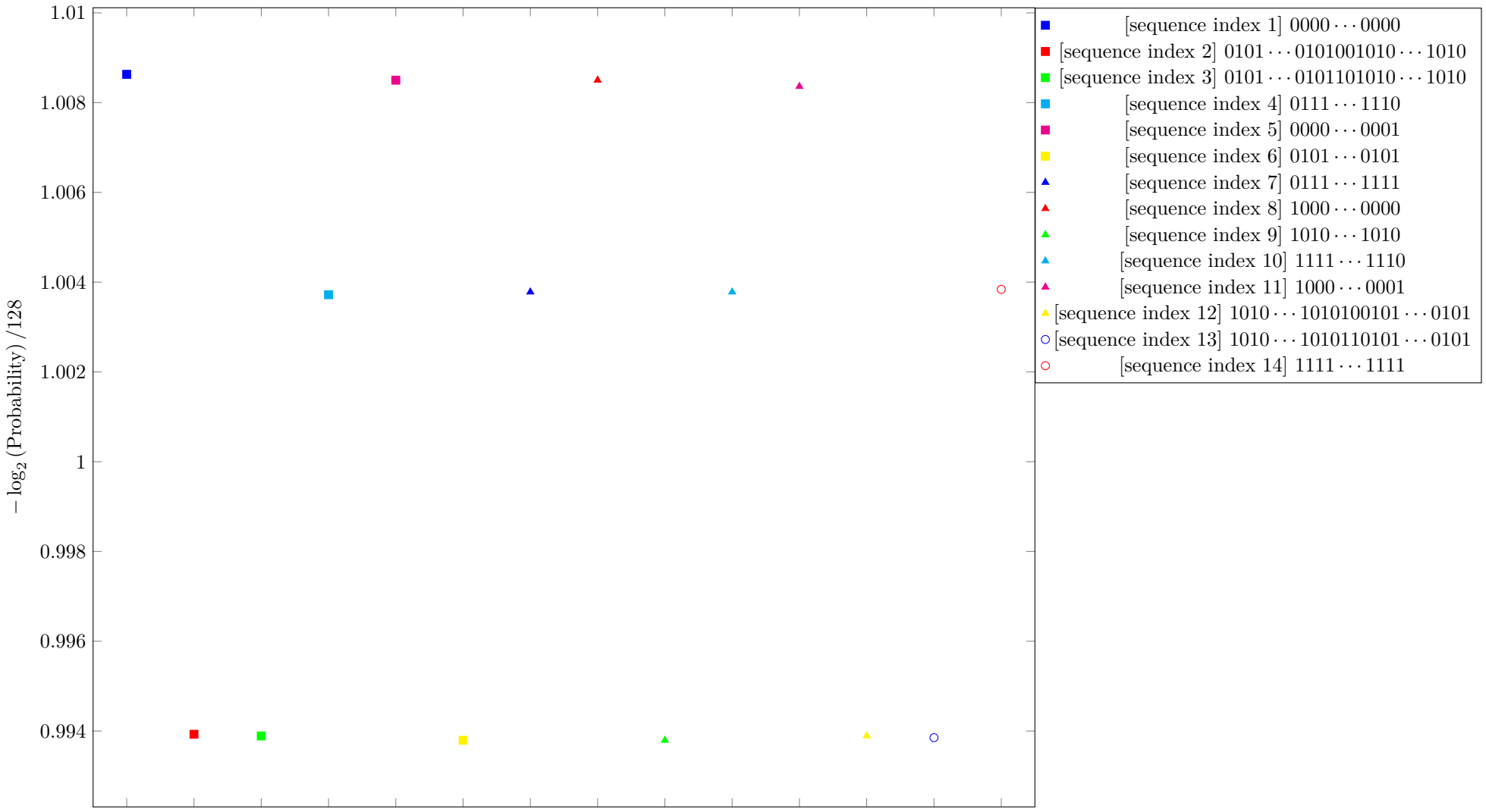
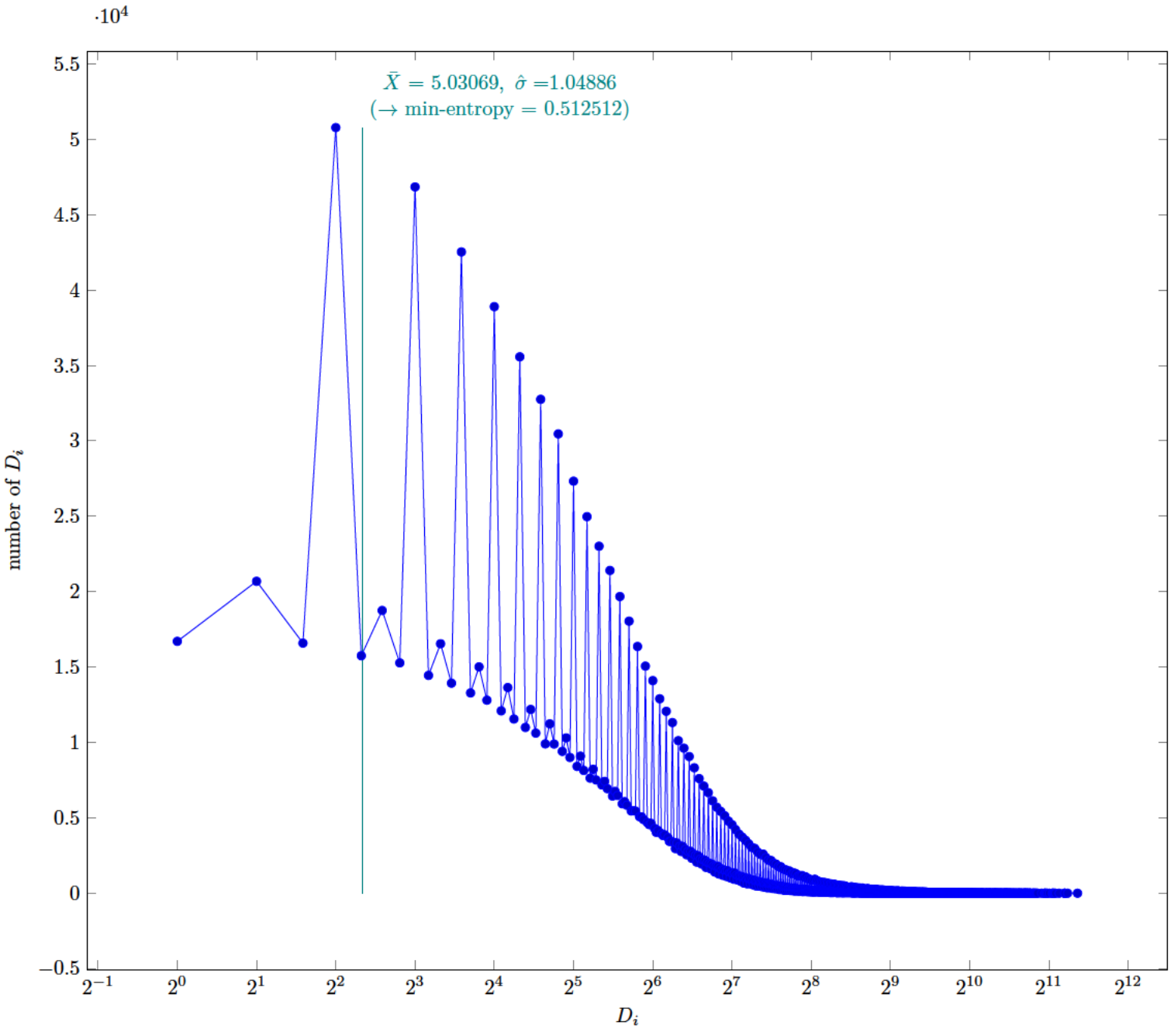


Fig. 12 Estimated Min-Entropy using §6.3.3 of NIST SP 800-90B

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	0.118662
$\bar{X}$	5.03069
$\hat{\sigma}$	1.04886
$\bar{X}'$	5.02835

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

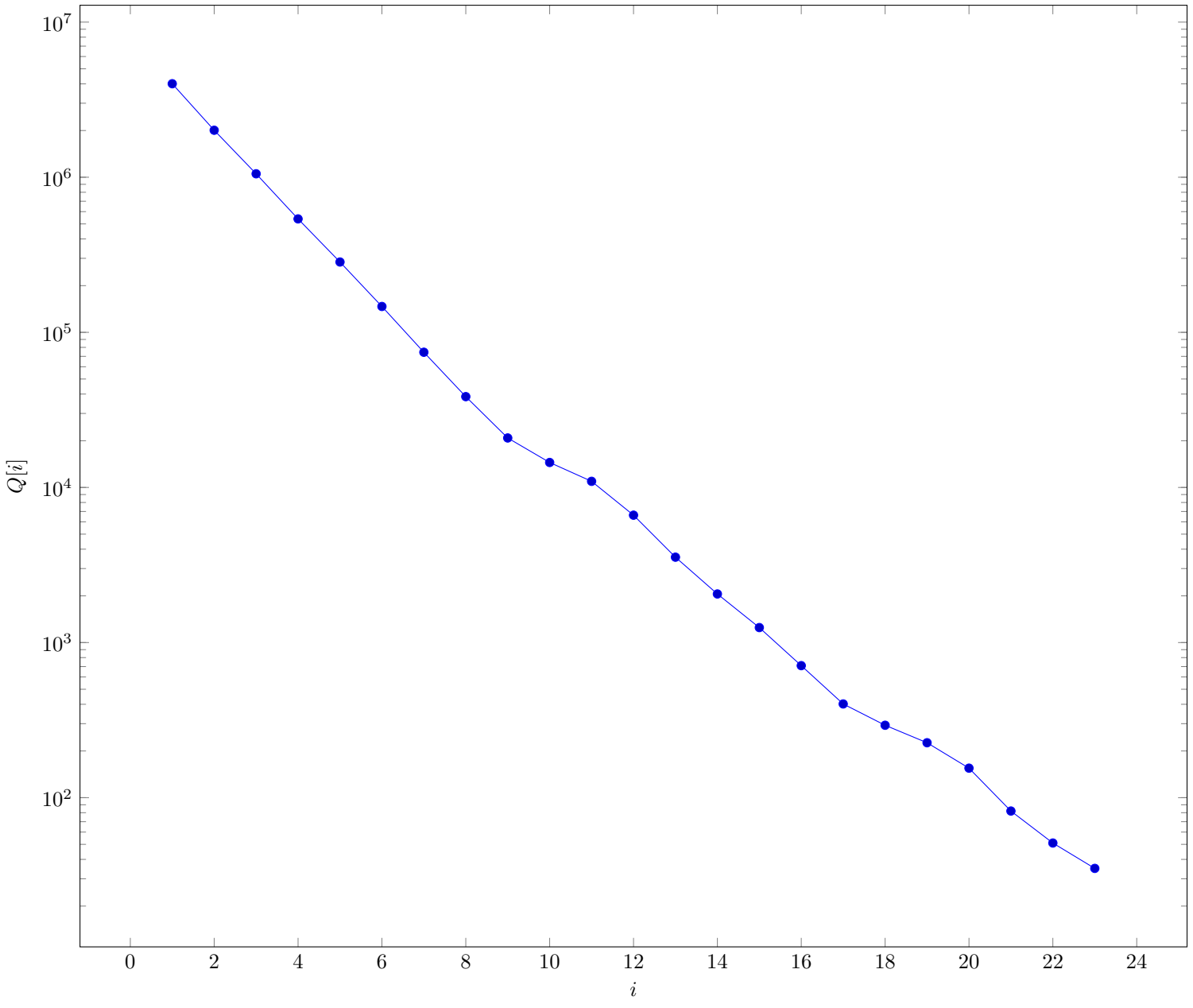


Fig. 13 Intermediate value $Q[i]$ in §6.3.5 of NIST SP 800-90B

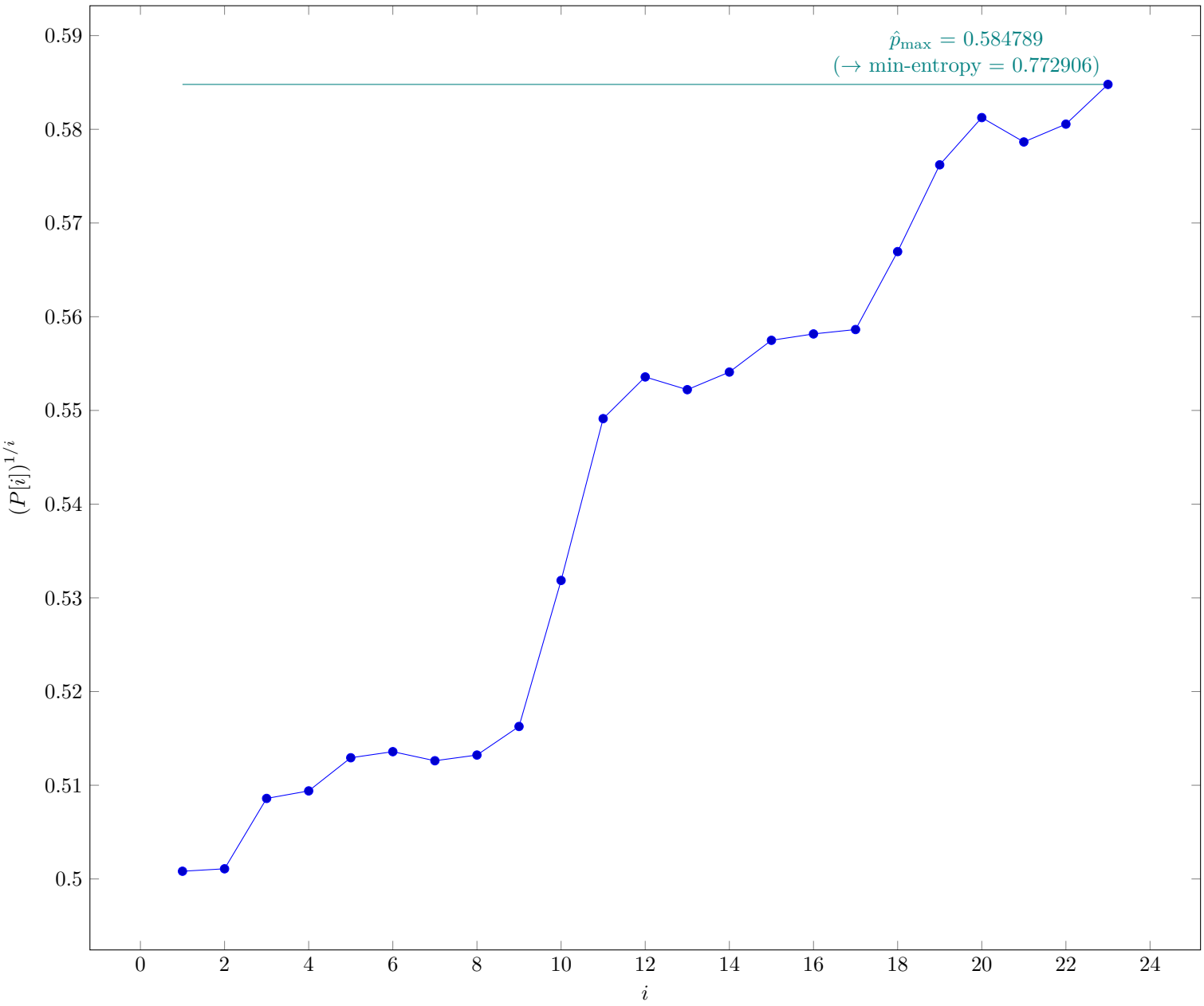


Fig. 14 $P[i]^{1/i}$ in §6.3.5 of NIST SP 800-90B

4.5.1 Supplemental information for traceability

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

Symbol	Value
t	23
$\hat{p}_{\max}$	0.584789
p_u	0.585238

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

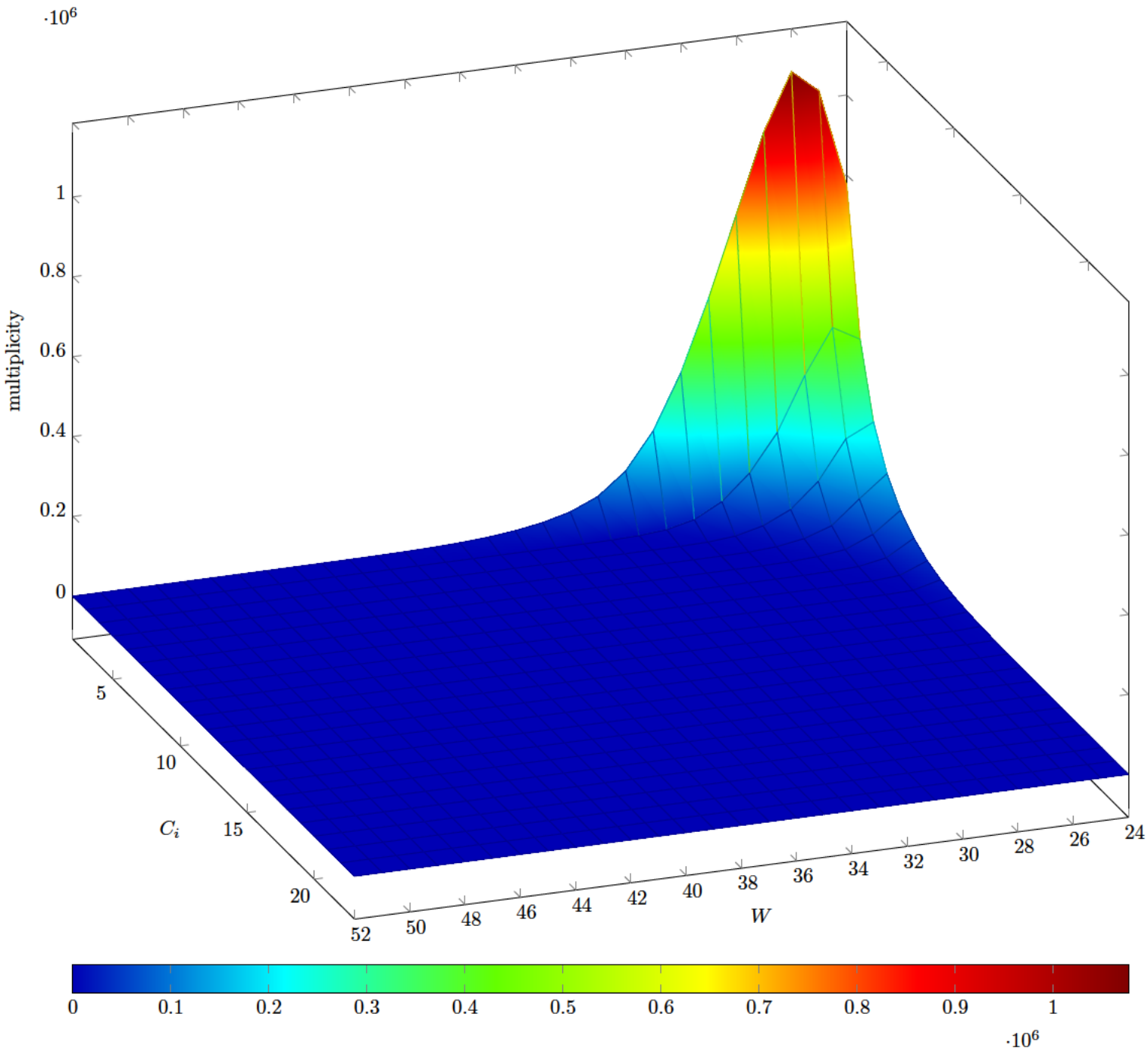


Fig. 15 Estimated W-tuple collision probability in Step 3 of §6.3.6 of NIST SP 800-90B

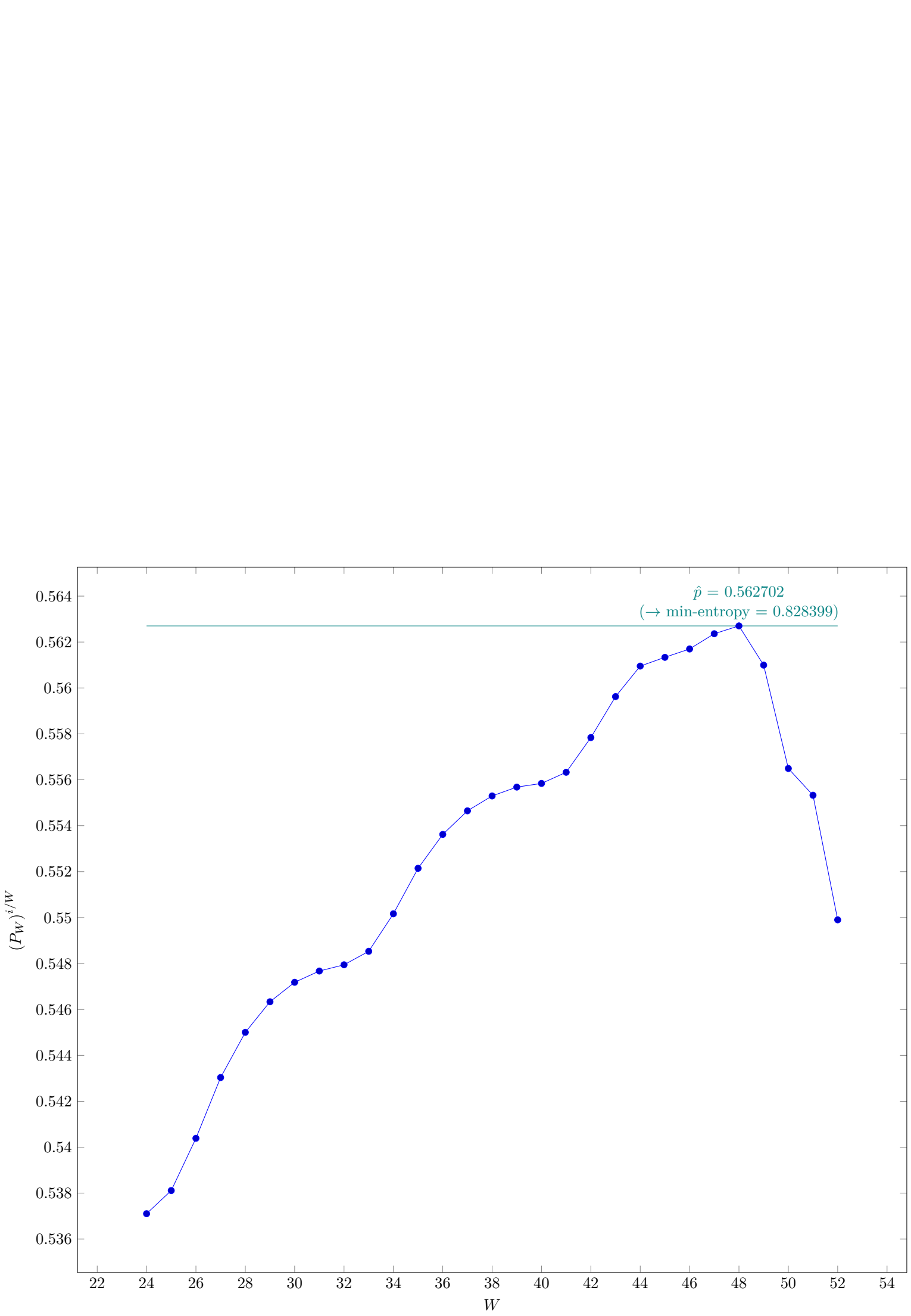


Fig. 16 Estimated average collision probability per string symbol in Step 3 of §6.3.6 of NIST SP 800-90B

4.6.1 Supplemental information for traceability

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

Symbol	Value
u	24
v	52
$\hat{p}$	0.562702
p_u	0.563154

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

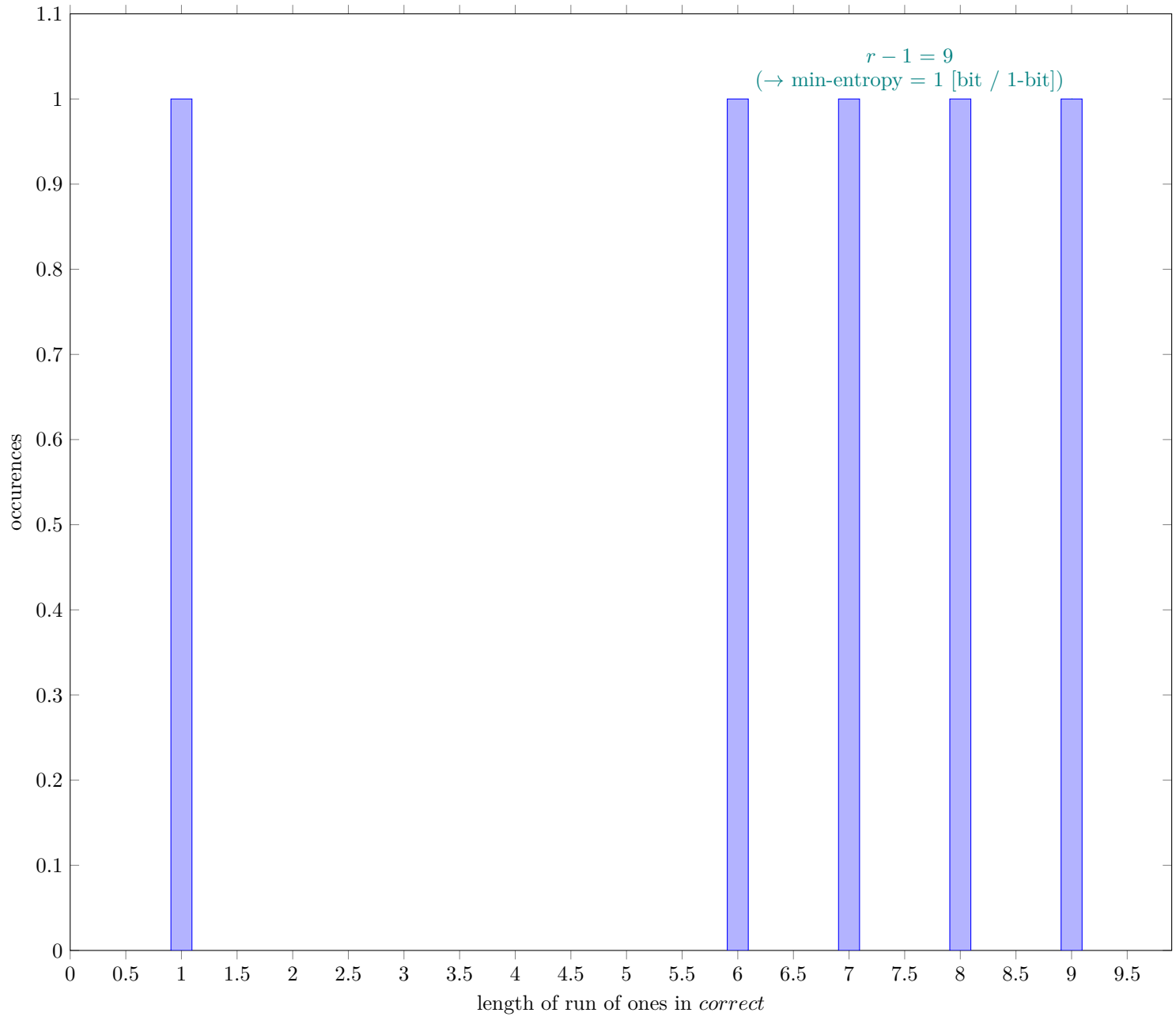


Fig. 17 Distribution of *correct*

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	3996310
P_{global}	0.499543
P'_{global}	0.499998
r	10
P_{local}	0.130614

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

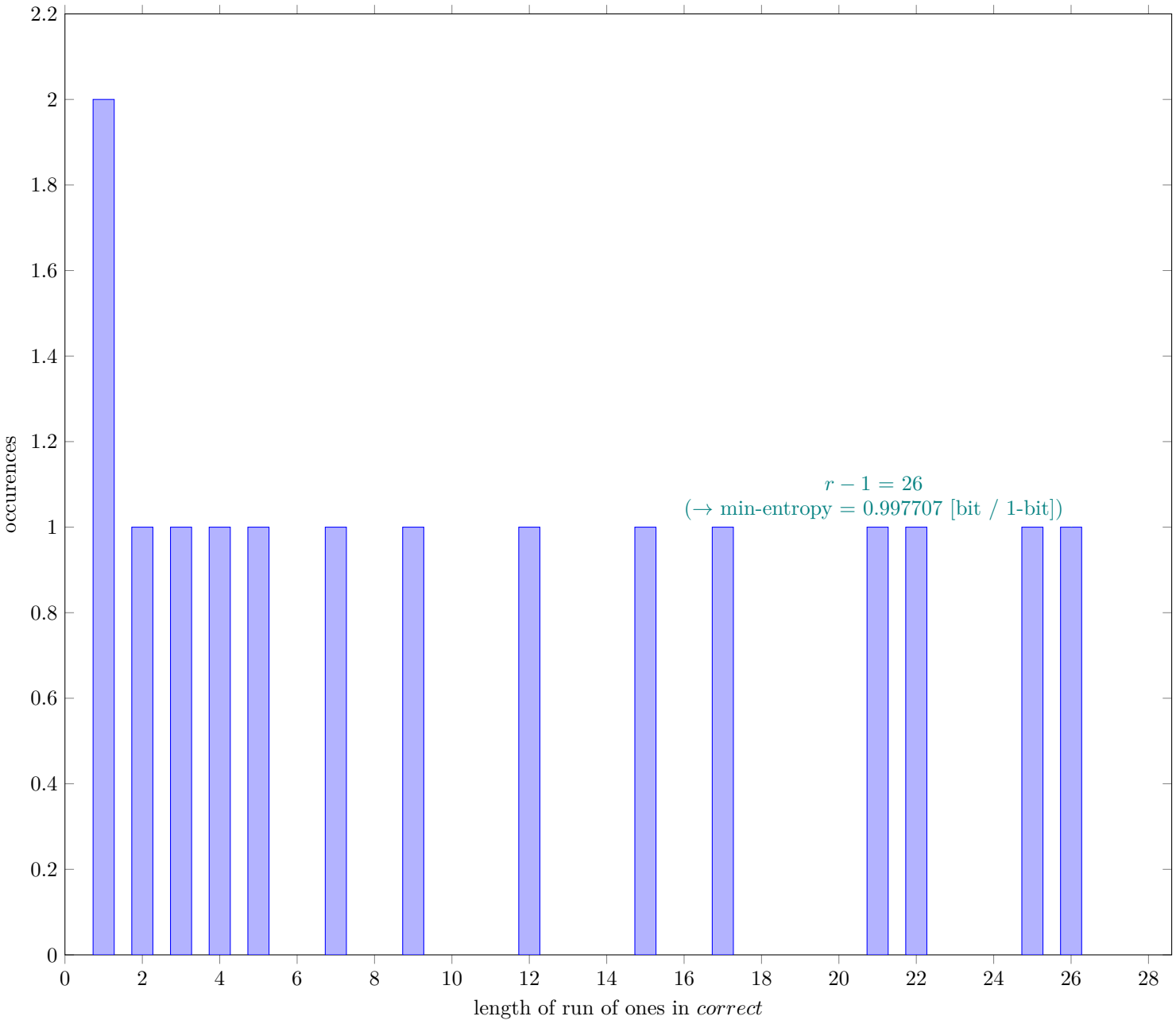


Fig. 18 Distribution of *correct*

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	4002718
P_{global}	0.50034
P'_{global}	0.500795
r	27
P_{local}	0.479558

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

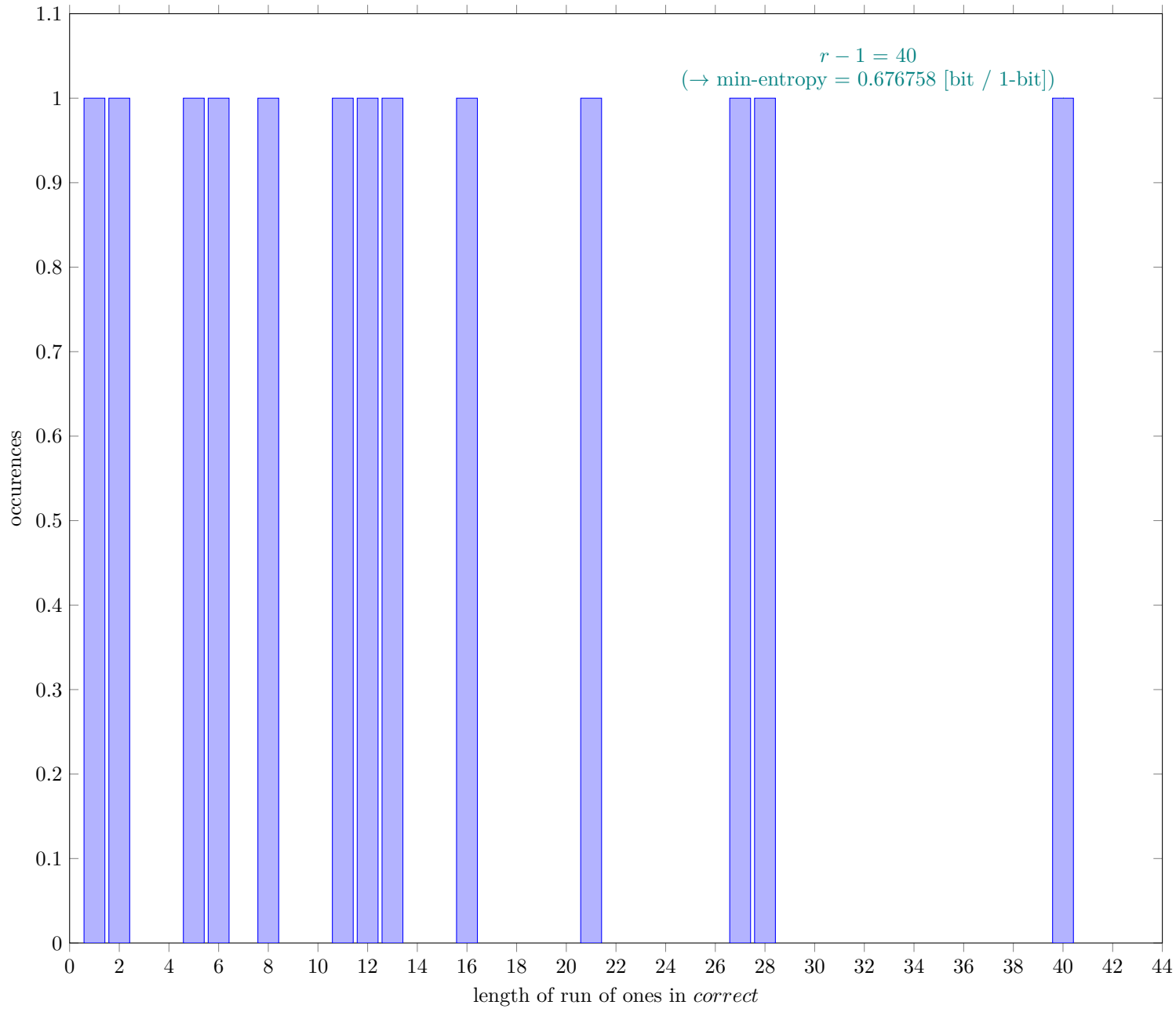


Fig. 19 Distribution of *correct*

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	5001029
P_{global}	0.625129
P'_{global}	0.62557
r	41
P_{local}	0.621134

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

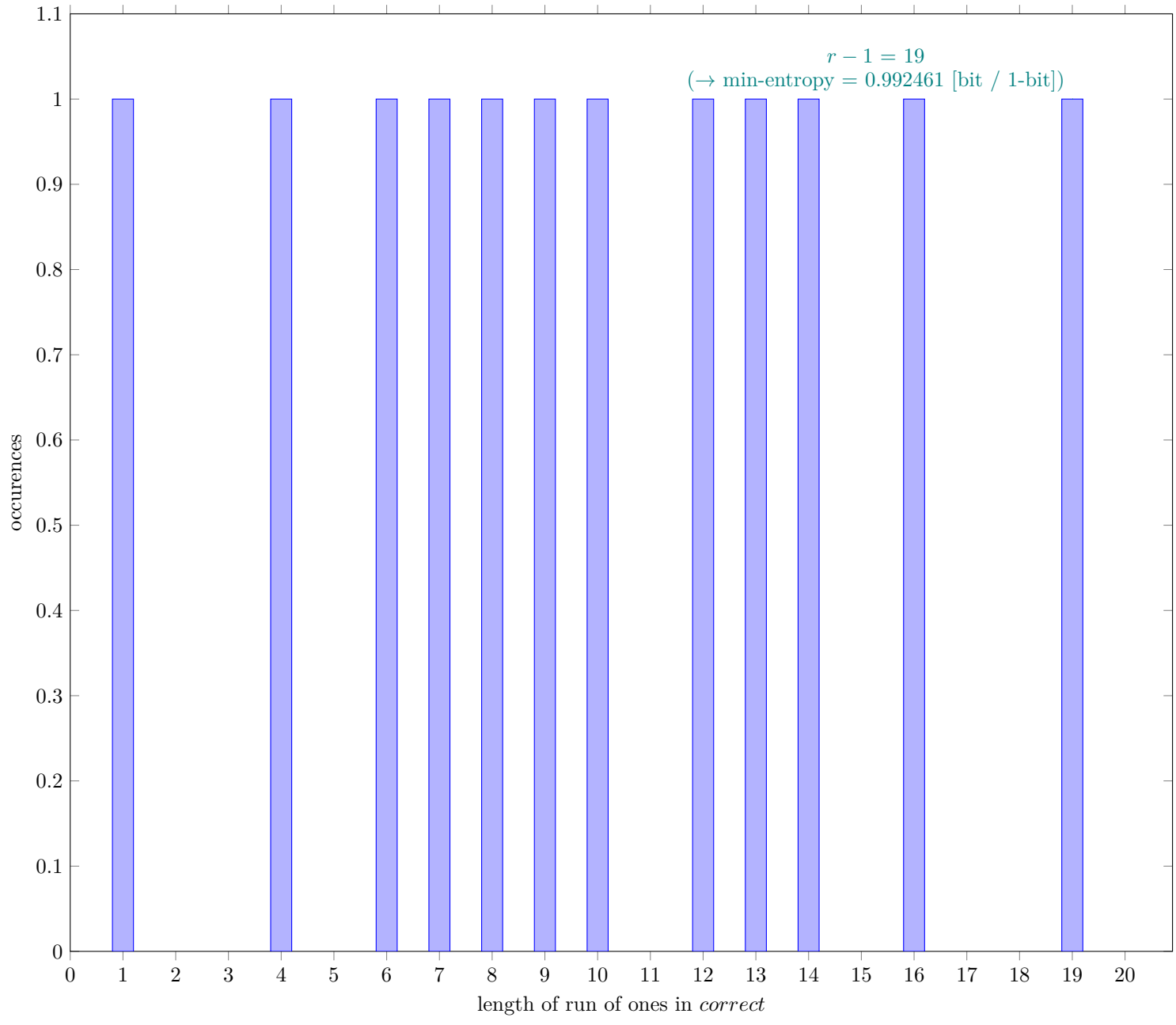


Fig. 20 Distribution of *correct*

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	4017307
P_{global}	0.502164
P'_{global}	0.50262
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`