Test report of based on BSI AIS 20 / AIS 31

2024-Nov-23 18:50:33.586091

1 Identification information

1.1 Identification information of input data

- Filename of input data : See Annex A.1.
- Name of the submitter of the input data :
- Brief explanation of the input data :

1.2 Identification of analysis environment

Table 1 Identification information of analysis environment

Analysis tool	Name	Another AIS 20/AIS 31 test tool
	Versioning information	3.0.0
	built as	64-bit application
	built by	Visual Studio 2019 version 16.11 (`_MSC_FULL_VER`: 192930157)
	linked libraries	Boost C++ 1.86.0
	with	OpenMP disabled
Analysis environment	Hostname	[redacted]
	CPU information	Intel(R) Core(TM) i5-[redacted]
	Physical memory size	[redacted] MiB
	OS name	Microsoft Windows 11 Pro
	OS version	10.0.22631 N/A Build 22631
	System type	64-bit
	Username	[redacted]

1.3 Identification of analysis conditions

Table 2 Identification information of analysis conditions

Bits per sample	8
Byte to bit conversion	Least Significant bit (LSb) first

1.4 Identification of analysis method

Black Box Test Suite T_{irn} of BSI AIS 20 / AIS 31 [1] with corrections [2] is applied.

2 Executive summary

2.1 Test results based on BSI AIS 20 / AIS 31

Table 3 Test results

	1-st trial		2-nd trial	
Tests	Pass / Fail	Notes	Pass / Fail	Notes
Test T1 (monobit test)	Fail	see 3.1.1	Pass	see 3.1.2
Test T2 (poker test)	Pass	see 3.2.1	Pass	see 3.2.2
Test T3 (MultiMMC Prediction Estimate)	Pass	see 3.3.1	Pass	see 3.3.3
Test T4 (LZ78Y Prediction Estimate)	Pass	see 3.4.1	Pass	see 3.4.3
Overall test result	Pass			

3 Detailed information of tests for given input data

3.1 Test T1 (monobit test)

3.1.1 Supplemental information for traceability for the 1st trial

Table 4 Supplemental information for traceability (Test T1) for the 1-st trial

Symbol	Value
$t_{IRN(1)}$	98

3.1.2 Supplemental information for traceability for the 2nd trial

Table 5 Supplemental information for traceability (Test T1) for the 2-nd trial

Symbol	Value
$t_{IRN(1)}$	10055

3.2 Test T2 (poker test)

3.2.1 Supplemental information for traceability for the 1st trial

Table 6 Supplemental information for traceability (Test T2) for the 1-st trial

Symbol	Value
$t_{IRN(2)}$	20.7424

3.2.2 Supplemental information for traceability for the 2nd trial

Table 7 Supplemental information for traceability (Test T2) for the 2-nd trial

Symbol	Value
$t_{IRN(2)}$	12.64

3.3 The MultiMMC Prediction Estimate (Test T3)

3.3.1 Distribution of *correct* for the 1st trial

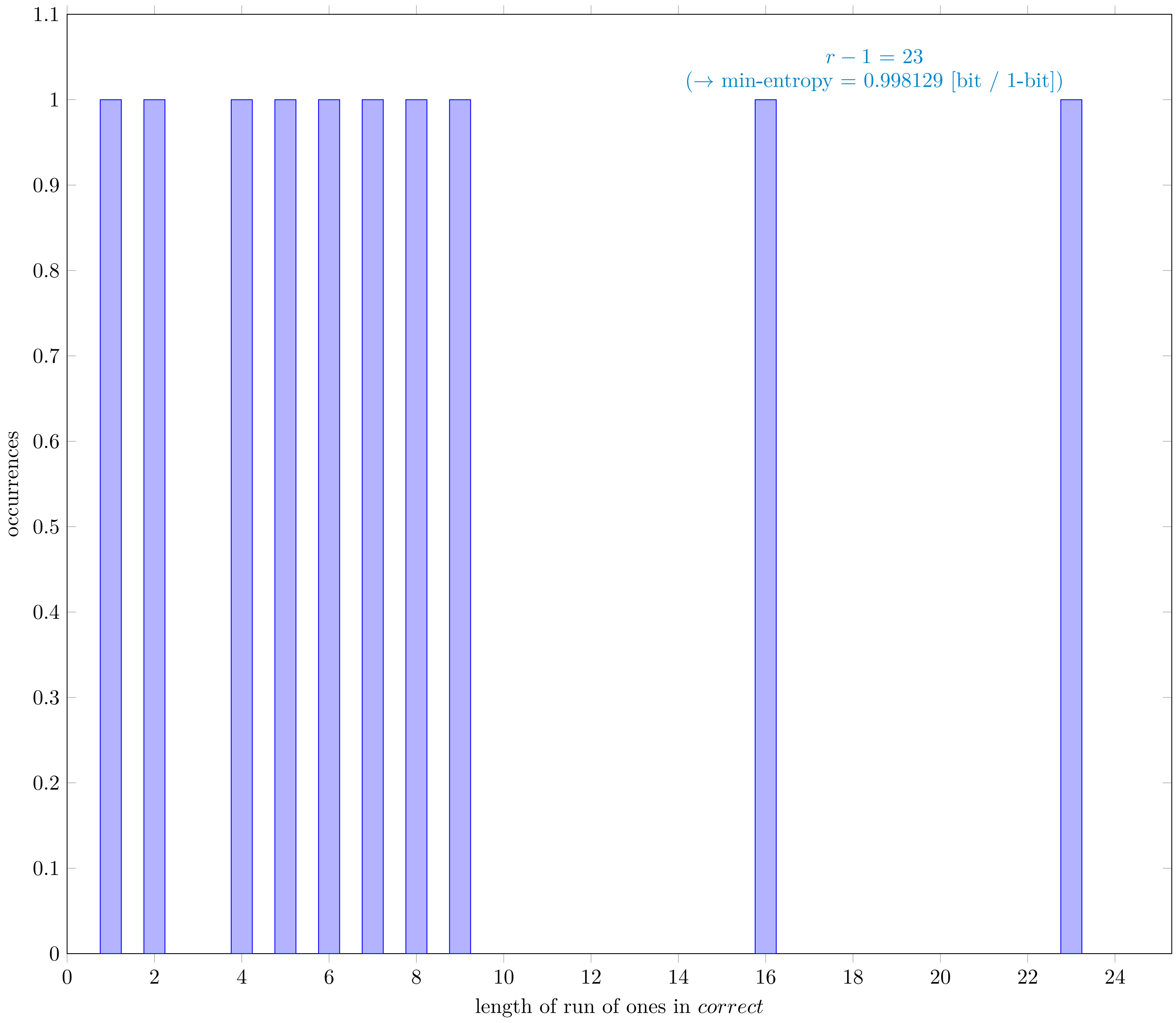

Fig. 1 Distribution of *correct*

3.3.2 Supplemental information for traceability for the 1st trial

Table 8 Supplemental information for traceability (NIST SP 800-90B Section 6.3.9)for the 1-st trial

Symbol	Value
N	999998
C	499360
P_{global}	0.499361
P'_{global}	0.500649
r	24
P_{local}	0.476964

3.3.3 Distribution of *correct* for the 2nd trial

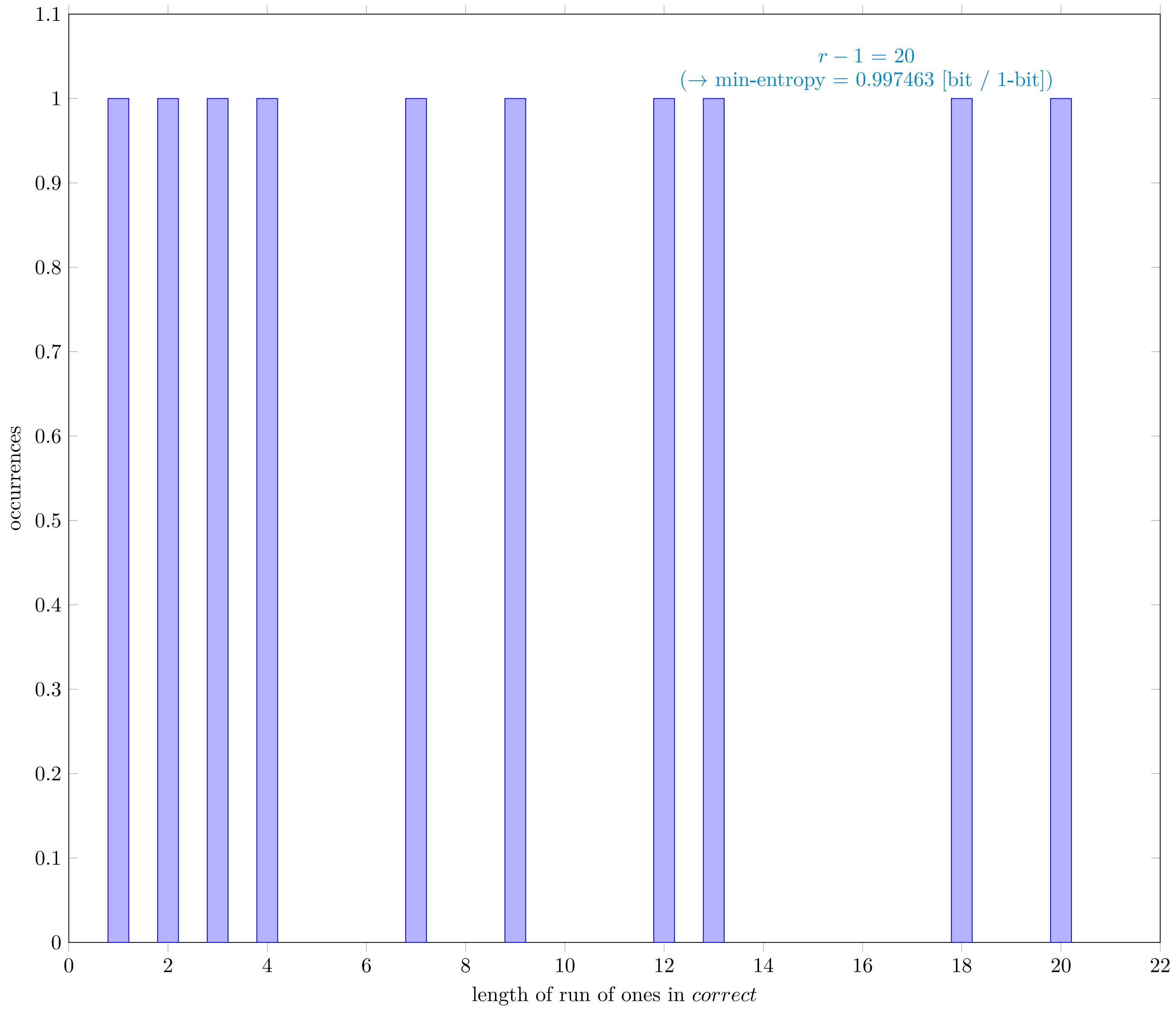

Fig. 2 Distribution of *correct*

3.3.4 Supplemental information for traceability for the 2nd trial

Table 9 Supplemental information for traceability (NIST SP 800-90B Section 6.3.9)for the 2-nd trial

Symbol	Value
N	999998
C	499591
P_{global}	0.499592
P'_{global}	0.50088
r	21
P_{local}	0.427245

3.4 The LZ78Y Prediction Estimate (Test T4)

3.4.1 Distribution of *correct* for the 1st trial

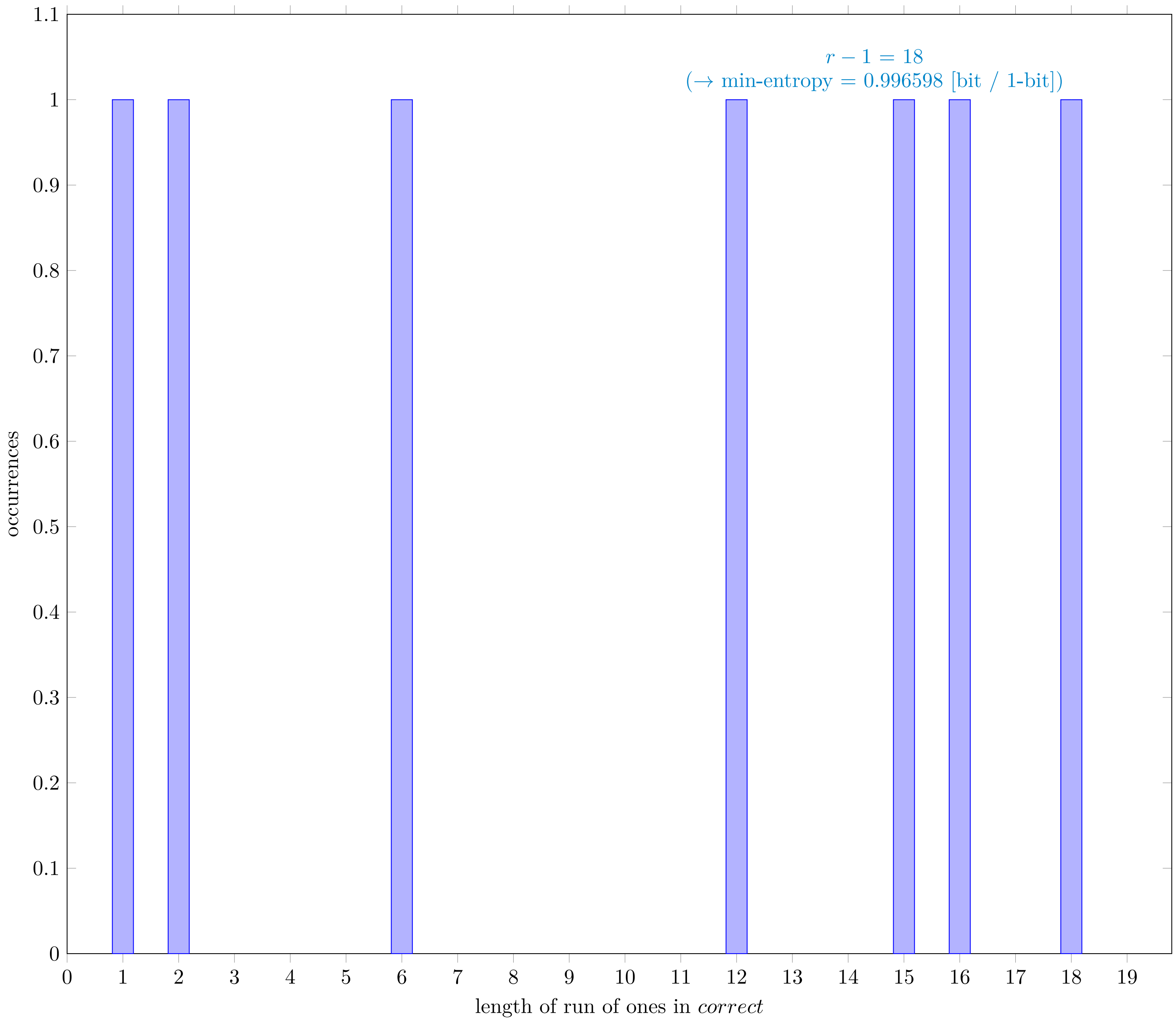

Fig. 3 Distribution of *correct*

3.4.2 Supplemental information for traceability for the 1st trial

Table 10 Supplemental information for traceability (NIST SP 800-90B Section 6.3.10)for the 1-st trial

Symbol	Value
N	999983
C	499884
P_{global}	0.499892
P'_{global}	0.50118
r	19
P_{local}	0.389347

3.4.3 Distribution of *correct* for the 2nd trial

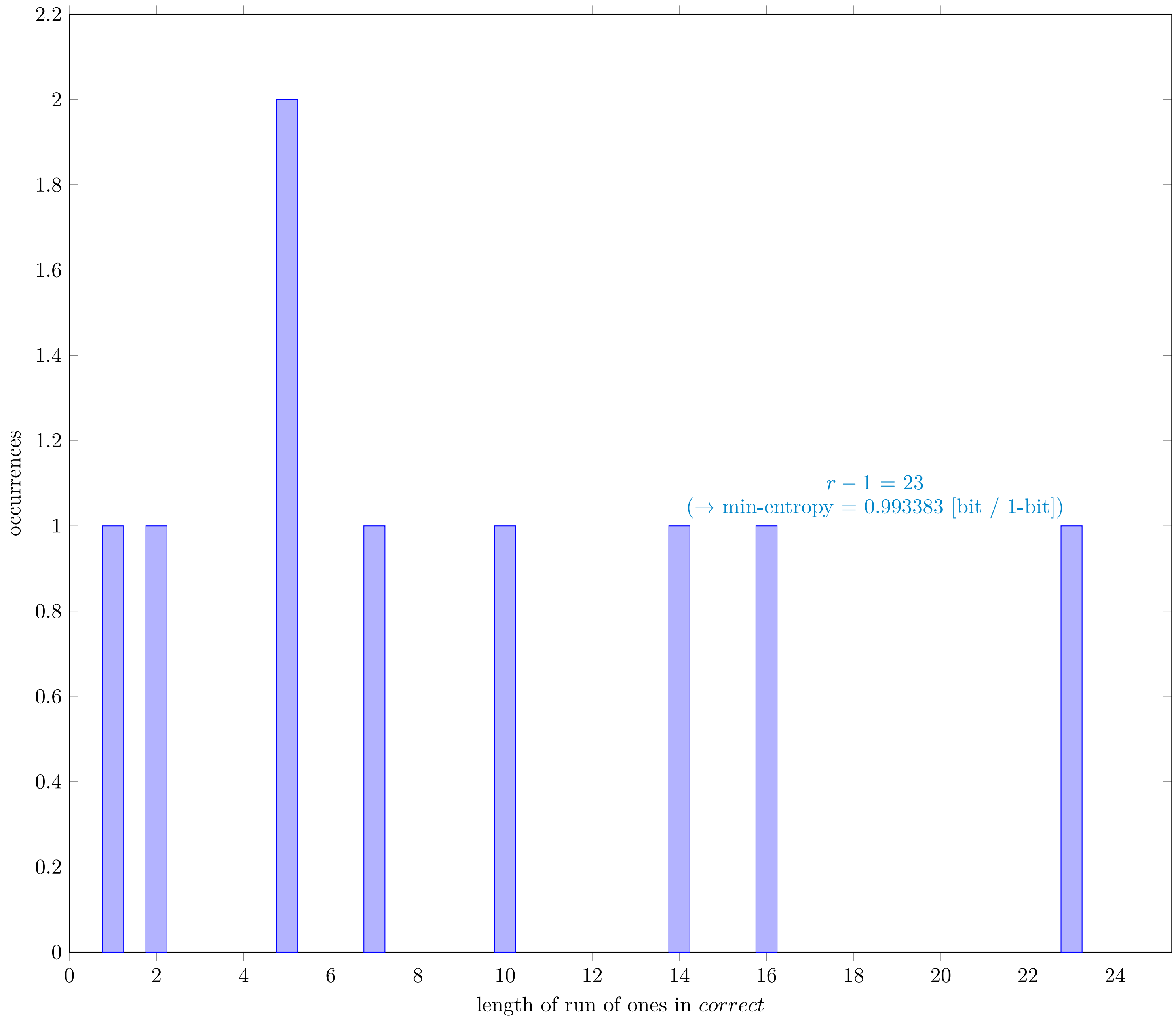

Fig. 4 Distribution of *correct*

3.4.4 Supplemental information for traceability for the 2nd trial

Table 11 Supplemental information for traceability (NIST SP 800-90B Section 6.3.10)for the 2-nd trial

Symbol	Value
N	999983
C	501002
P_{global}	0.501011
P'_{global}	0.502298
r	24
P_{local}	0.476965

A Identification information

A.1 Identification of input data

Table 12: Identification information of input data

No	Item	Value
1	Path to the input data for Tests T1 through T4	[redacted]"v3_sample_input_data_for_T1-T4.bin"
	SHA-256 hash value of the input data for Tests T1 through T4[hex]	a3b04689 c5512355 ba82b434 ea389f77 fd2883e2 b49d6c1b 479788b3 622dfdc1
	Last write time	2024-Nov-17 11:22:52

end of the table

A References

[1] Matthias Peter and Werner Schindler. *A Proposal for Functionality Classes for Random Number Generators*, Version 3.0 (September 10, 2024), `https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Certification/Interpretations/AIS_31_Functionality_classes_for_random_number_generators_e_2024.pdf?__blob=publicationFile&v=3`

[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`