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

2025-Sep-28 07:02:08.652208

## 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_1bit.bin` |
| SHA-256 hash value of the acquisition data [hex] | `f9ea8832 af4c4205 f518845b 26446580 0921688f c2c4d566 fbc08766 4aeb2313` |

- 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 | 1.1.5 |
| | built as | 64-bit application |
| | built by | Intel C++ Compiler ( `__INTEL_LLVM_COMPILER`: 20250200 ) |
| | linked libraries | Boost C++ 1.89.0 |
| 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 | `10.0.26100 N/A Build 26100` |
| | System type | 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 |
| Use Longest Common Prefix[*1] for 6.3.5 and 6.3.6 | True |

[*1] See [3] and [4]

## 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 | 0.995043 | see 3.1 |
| The Collision Estimate | 0.900935 | see 3.2 |
| The Markov Estimate | 0.998486 | see 3.3 |
| The Compression Estimate | 0.829677 | see 3.4 |
| The t-Tuple Estimate | 0.914226 | see 3.5 |
| The Longest Repeated Substring (LRS) Estimate | 0.985818 | see 3.6 |
| Multi Most Common in Window Prediction Estimate | 0.996972 | see 3.7 |
| The Lag Prediction Estimate | 0.998292 | see 3.8 |
| The MultiMMC Prediction Estimate | 0.99666 | see 3.9 |
| The LZ78Y Prediction Estimate | 0.99705 | see 3.10 |
| The intial entropy source estimate [bit / 1 -bit] $H_I = H_{\text{bitstring}}$ | 0.829677 | |

[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

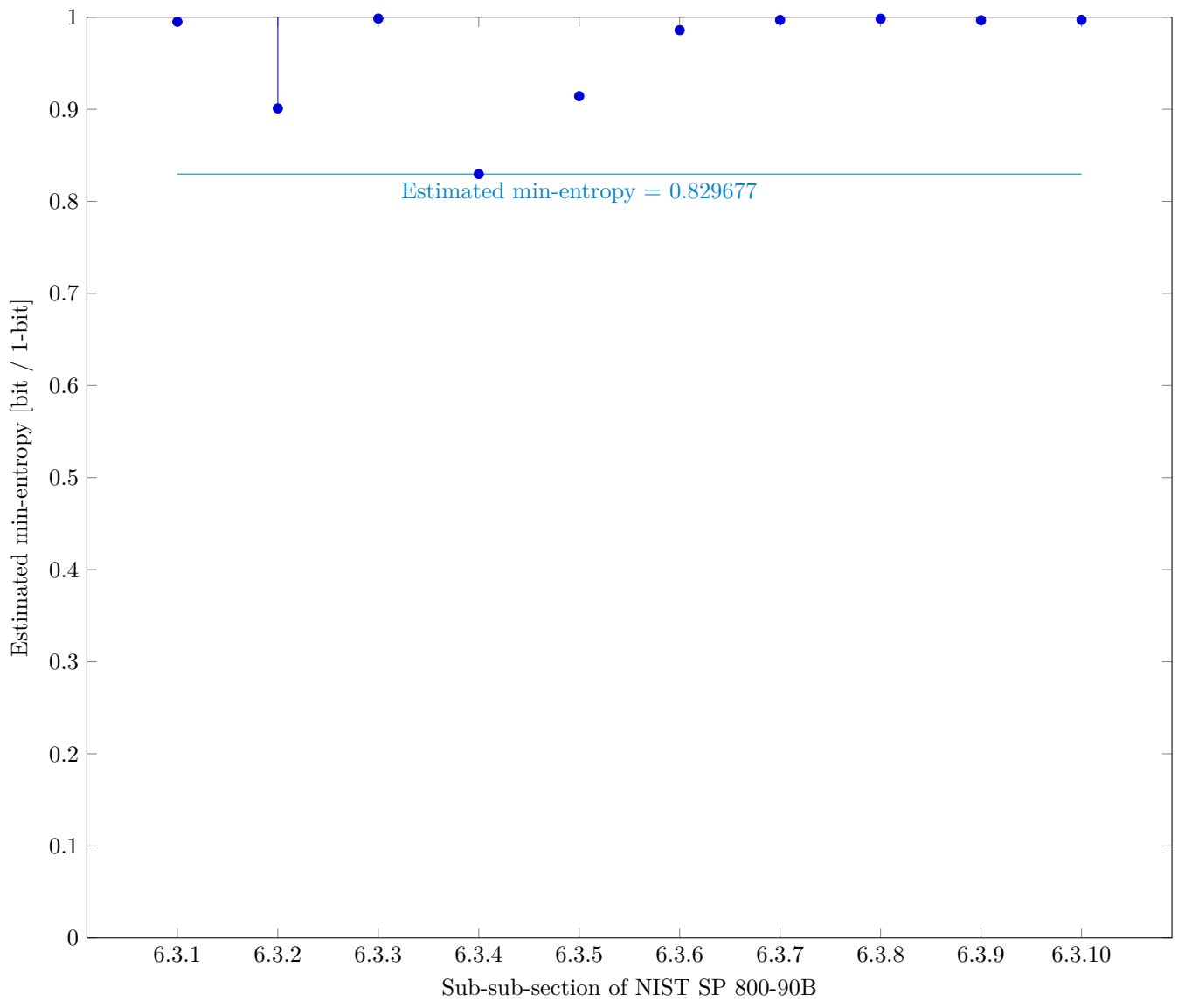


Fig. 1 Estimated Min-Entropy using §6.3 of NIST SP 800-90B

# 3 Detailed results of analysis from original samples

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

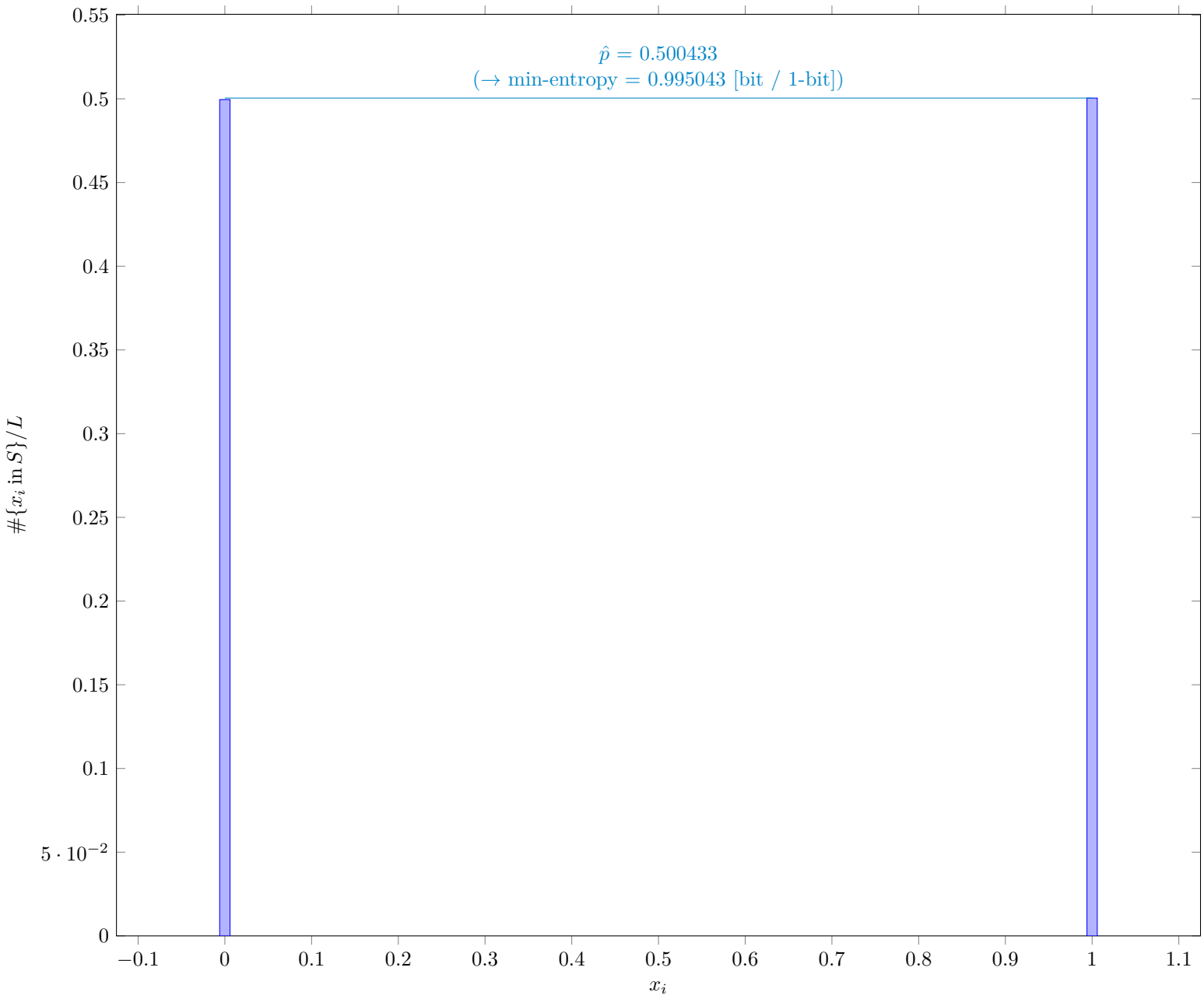


Fig. 2 Distribution of $x_i$

### 3.1.1 Supplemental information for traceability

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

| Symbol | Value |
|---|---|
| mode | 500433 |
| $\hat{p}$ | 0.500433 |
| $p_u$ | 0.501721 |

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

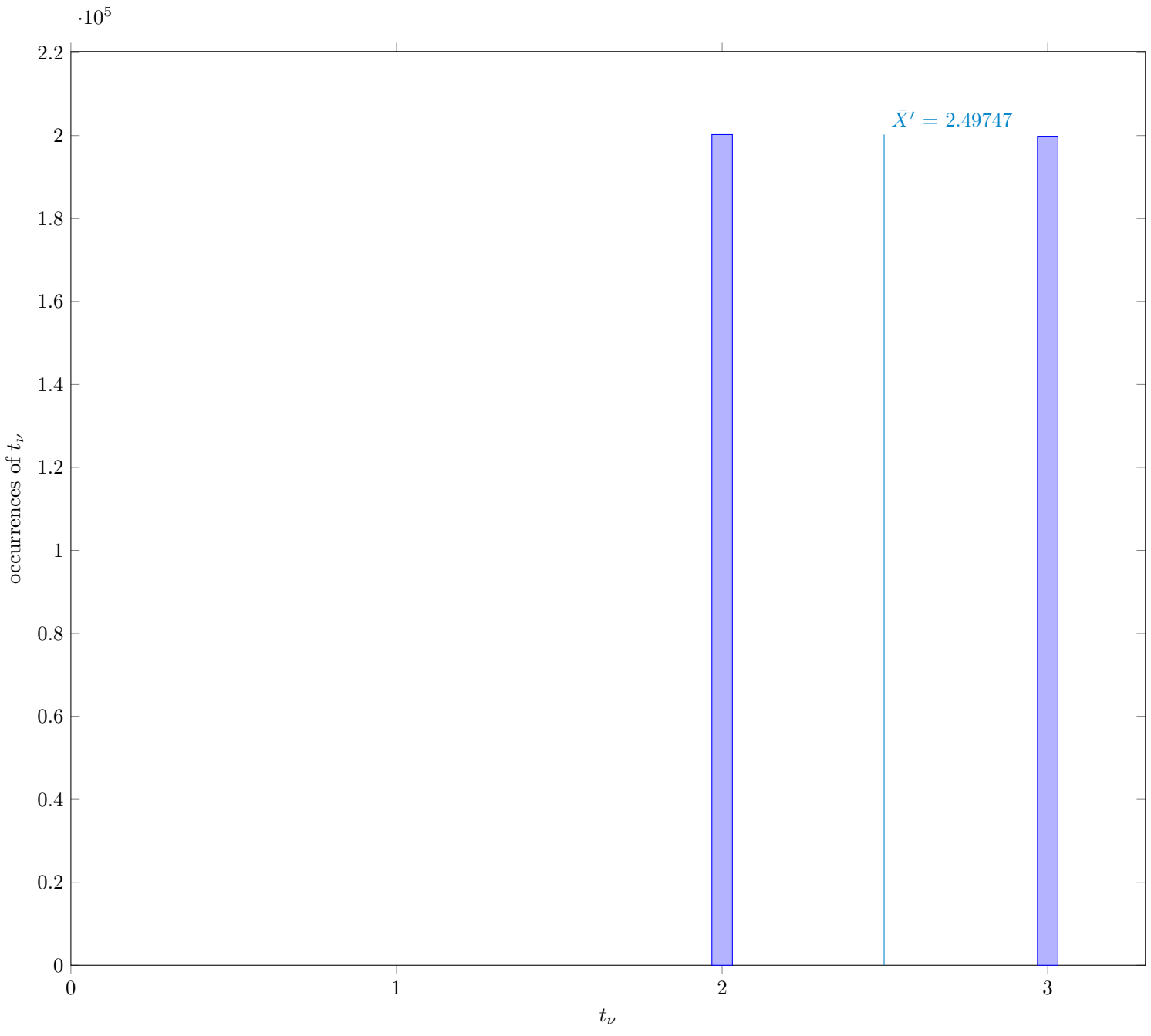


Fig. 3 Distribution of intermediate value $t_\nu$

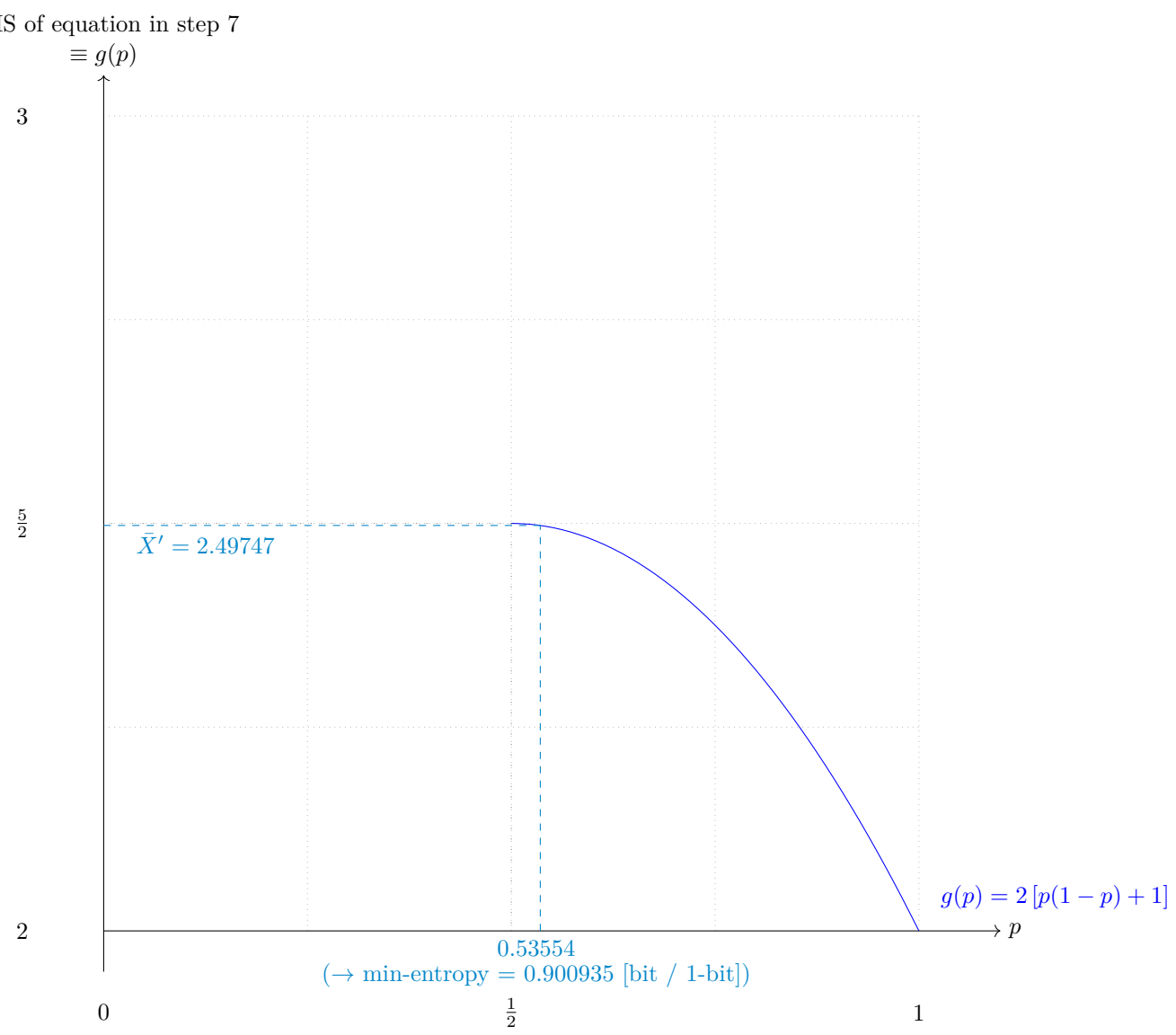


Fig. 4 Solution to the equation in step 7

### 3.2.1 Supplemental information for traceability

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

| Symbol | Value |
|---|---|
| $p$ | 0.53554 |
| $\bar{X}$ | 2.49951 |
| $\bar{X}'$ | 2.49747 |
| $\hat{\sigma}$ | 0.5 |

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

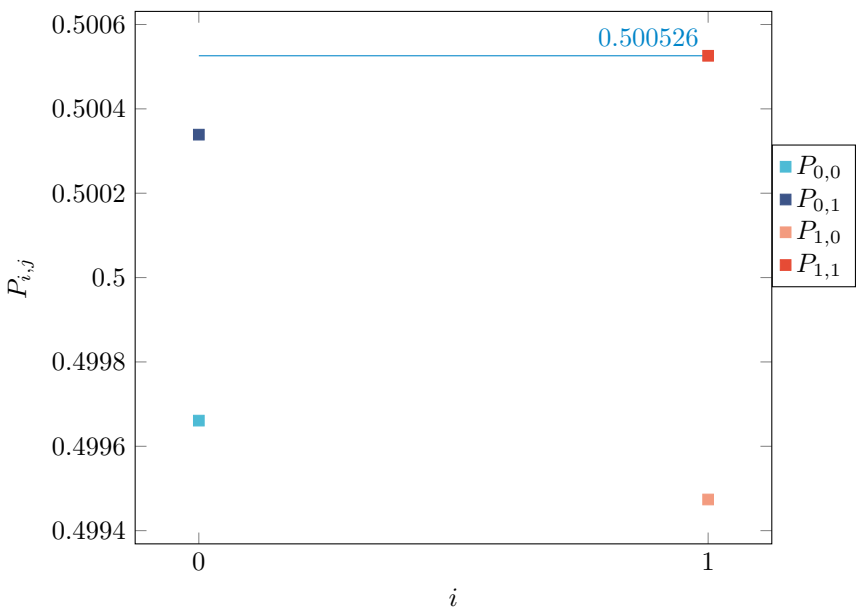


Fig. 5 Transition probability $P_{i,j}$ of §6.3.3 of NIST SP 800-90B

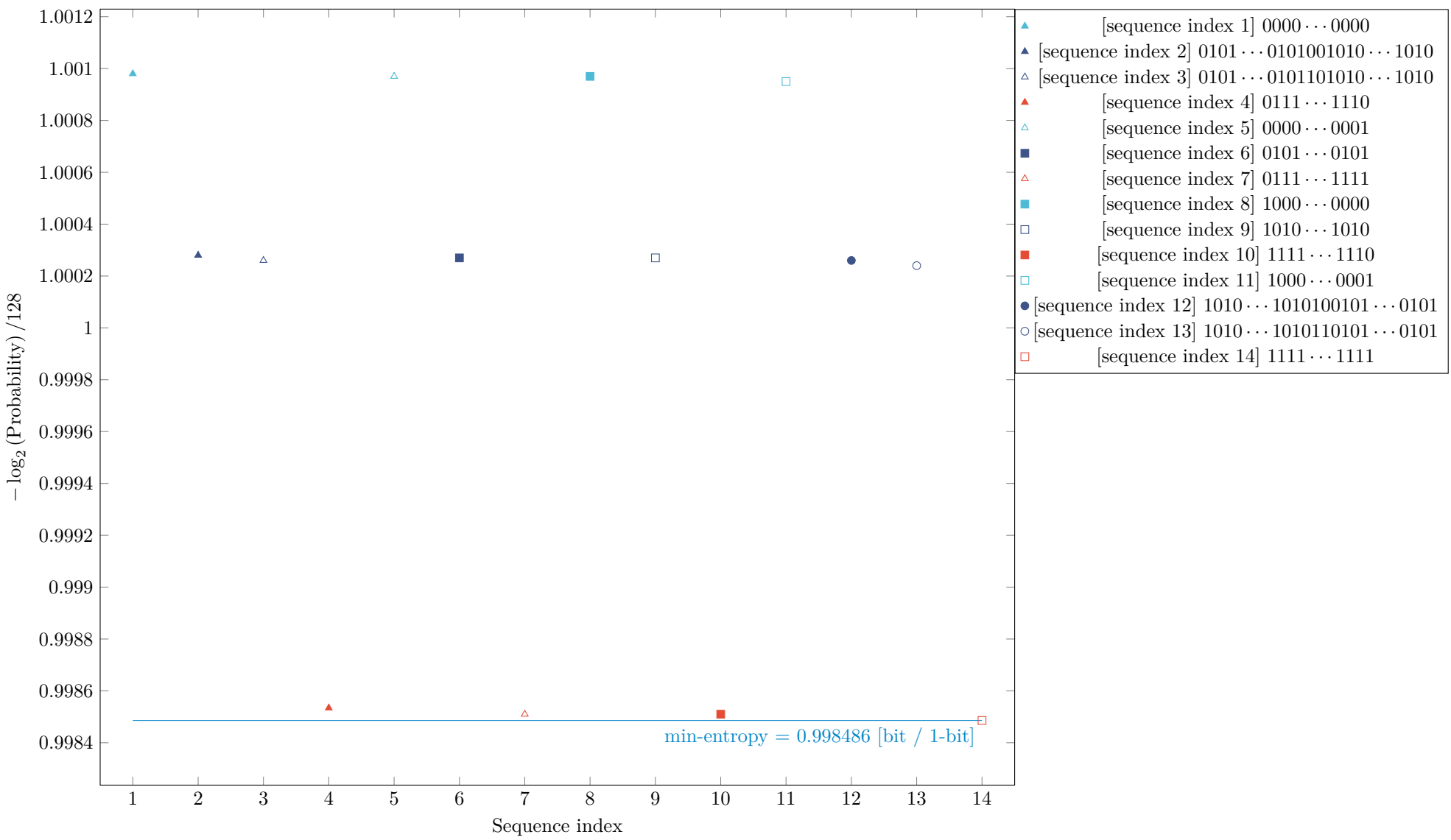


Fig. 6 Estimated Min-Entropy using §6.3.3 of NIST SP 800-90B

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

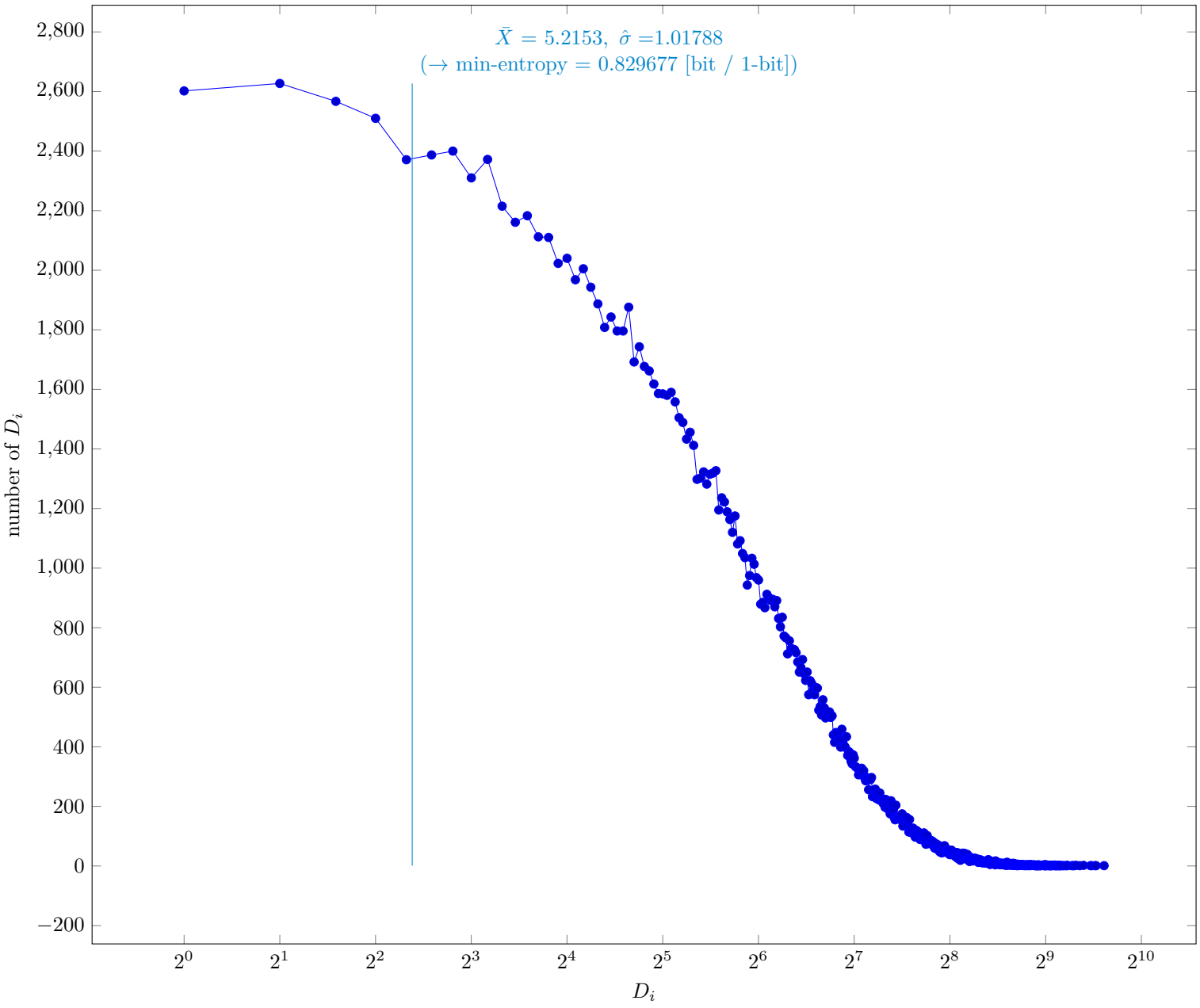


Fig. 7 Distribution of intermediate value $D_i$

### 3.4.1 Supplemental information for traceability

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

| Symbol | Value |
|---|---|
| $p$ | 0.0317288 |
| $\bar{X}$ | 5.2153 |
| $\hat{\sigma}$ | 1.01788 |
| $\bar{X}'$ | 5.20886 |

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

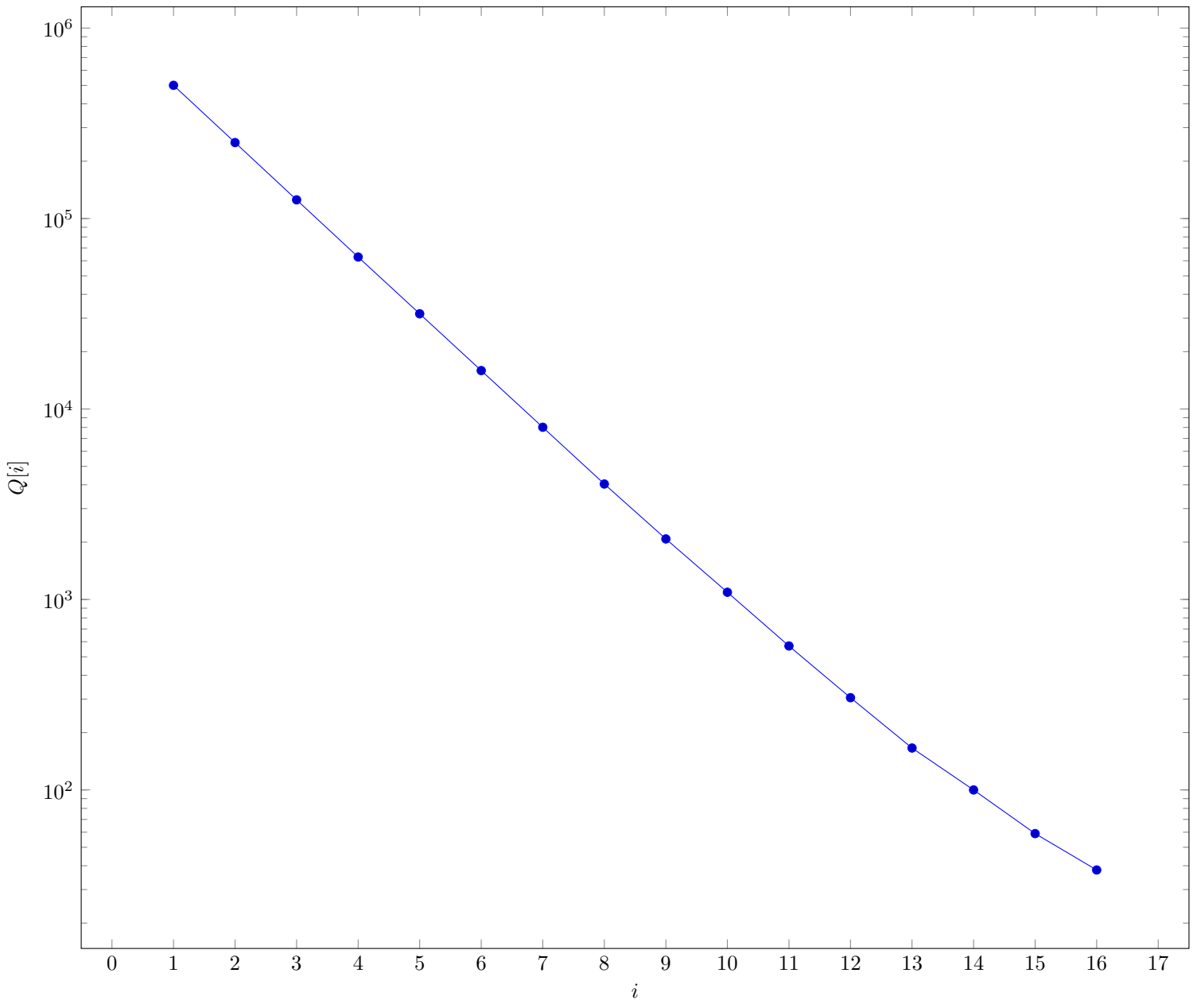


Fig. 8 Intermediate value $Q[i]$ in §6.3.5 of NIST SP 800-90B

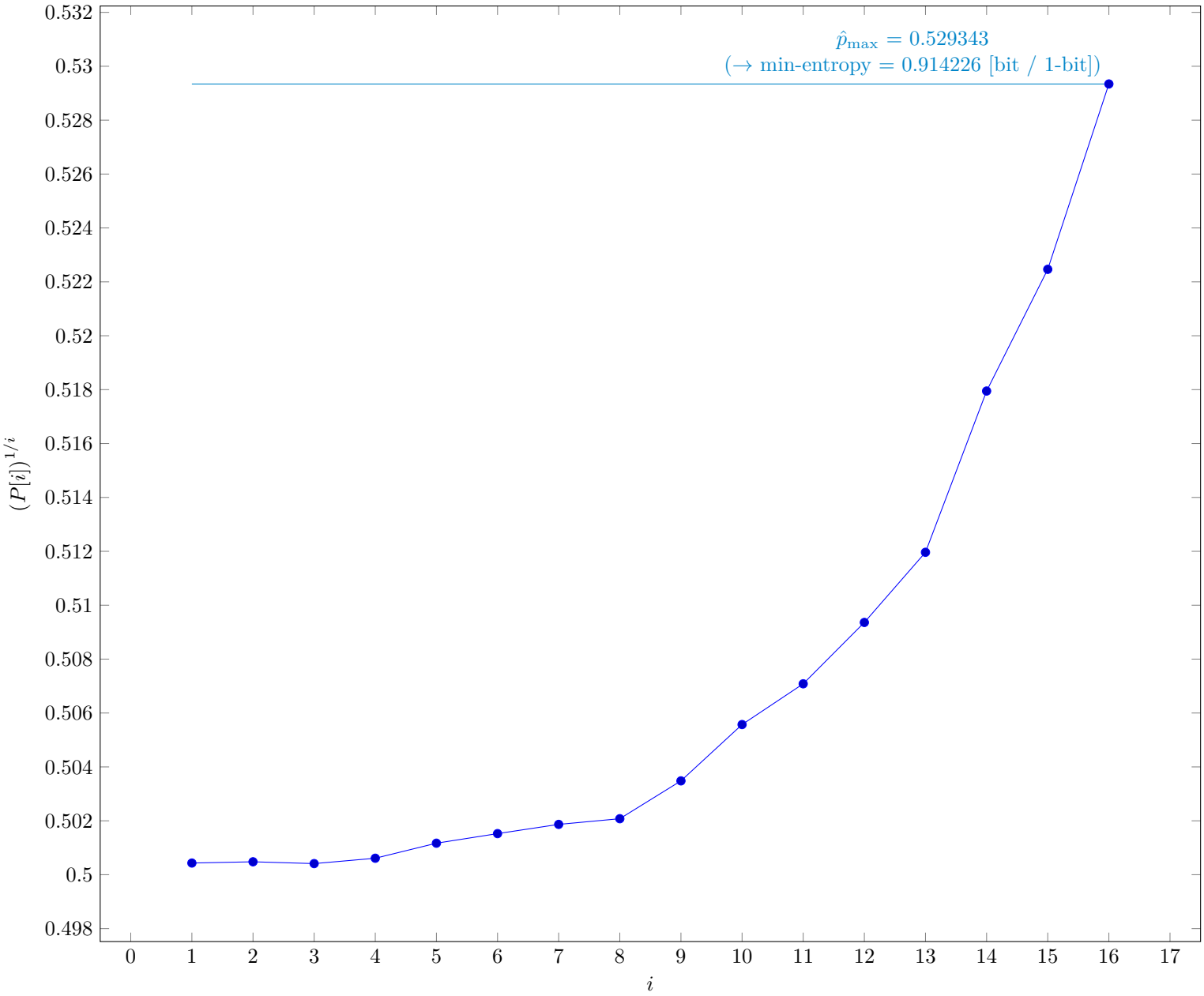


Fig. 9 $P[i]^{1/i}$ in §6.3.5 of NIST SP 800-90B

### 3.5.1 Supplemental information for traceability

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

| Symbol | Value |
|---|---|
| $t$ | 16 |
| $\hat{p}_{\max}$ | 0.529343 |
| $p_u$ | 0.530628 |

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

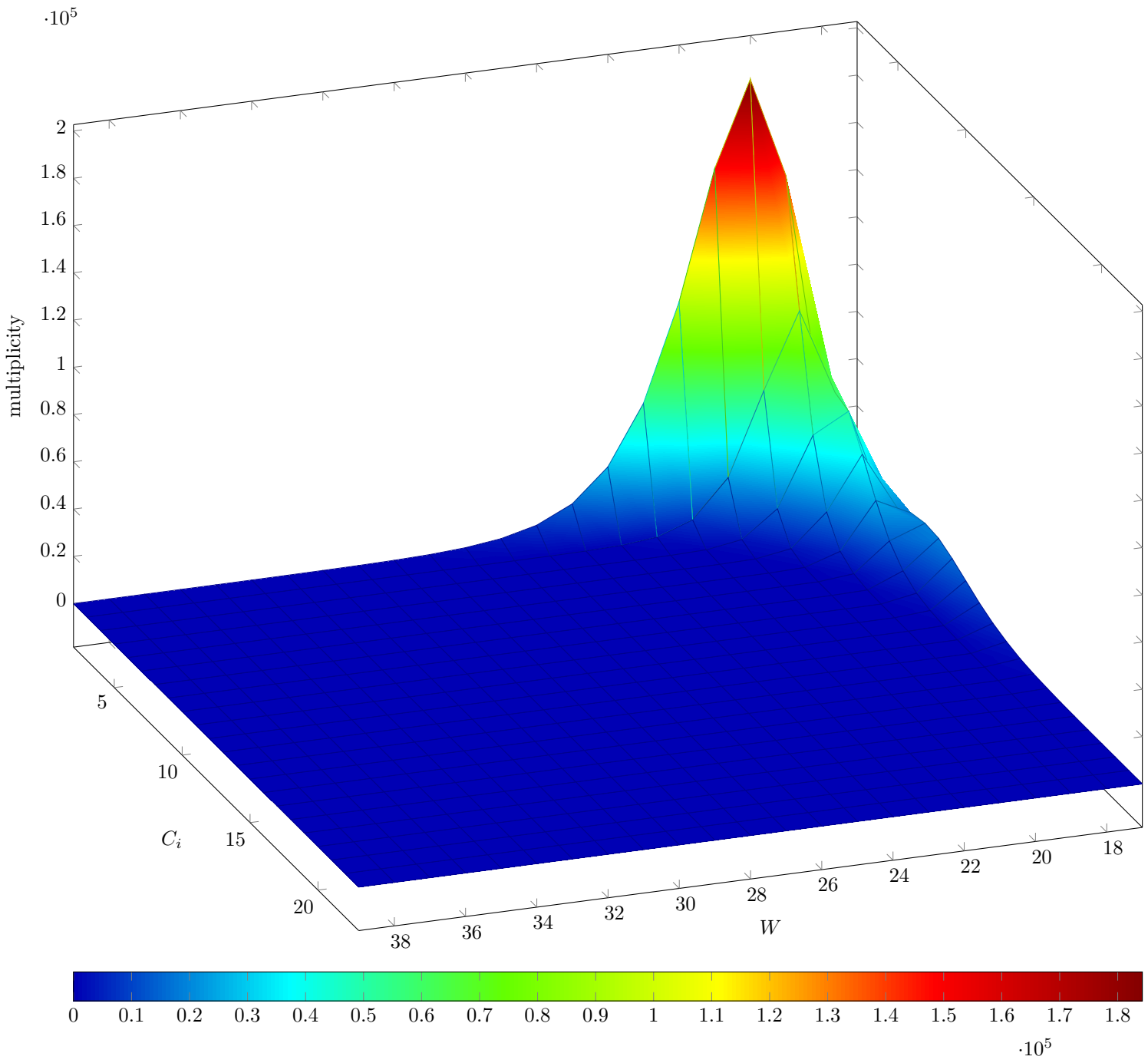


Fig. 10 Estimated $W$-tuple collision probability in Step 3 of §6.3.6 of NIST SP 800-90B

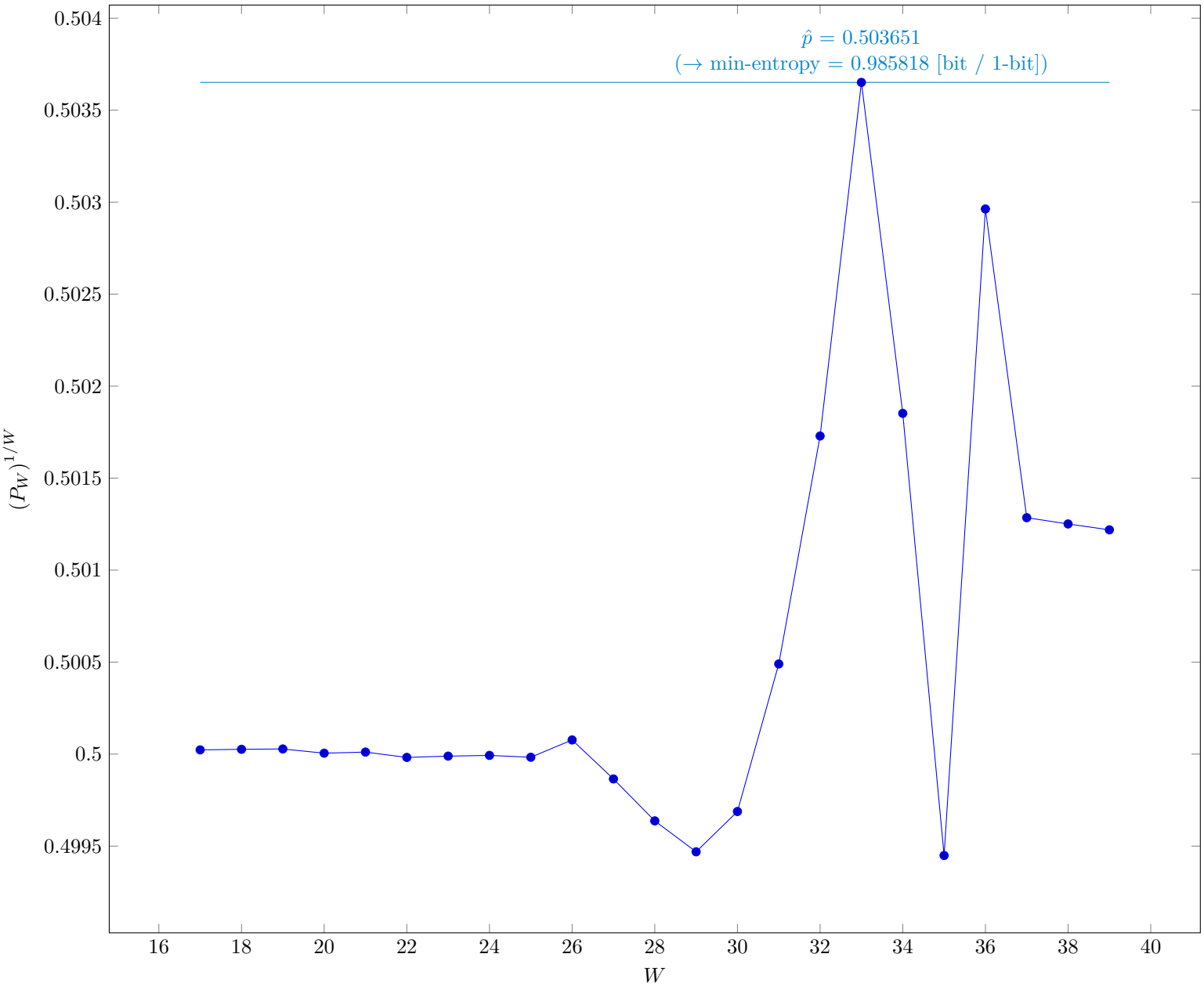


Fig. 11 Estimated average collision probability per string symbol in Step 3 of §6.3.6 of NIST SP 800-90B

### 3.6.1 Supplemental information for traceability

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

| Symbol | Value |
|---|---|
| $u$ | 17 |
| $v$ | 39 |
| $\hat{p}$ | 0.503651 |
| $p_u$ | 0.504939 |

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

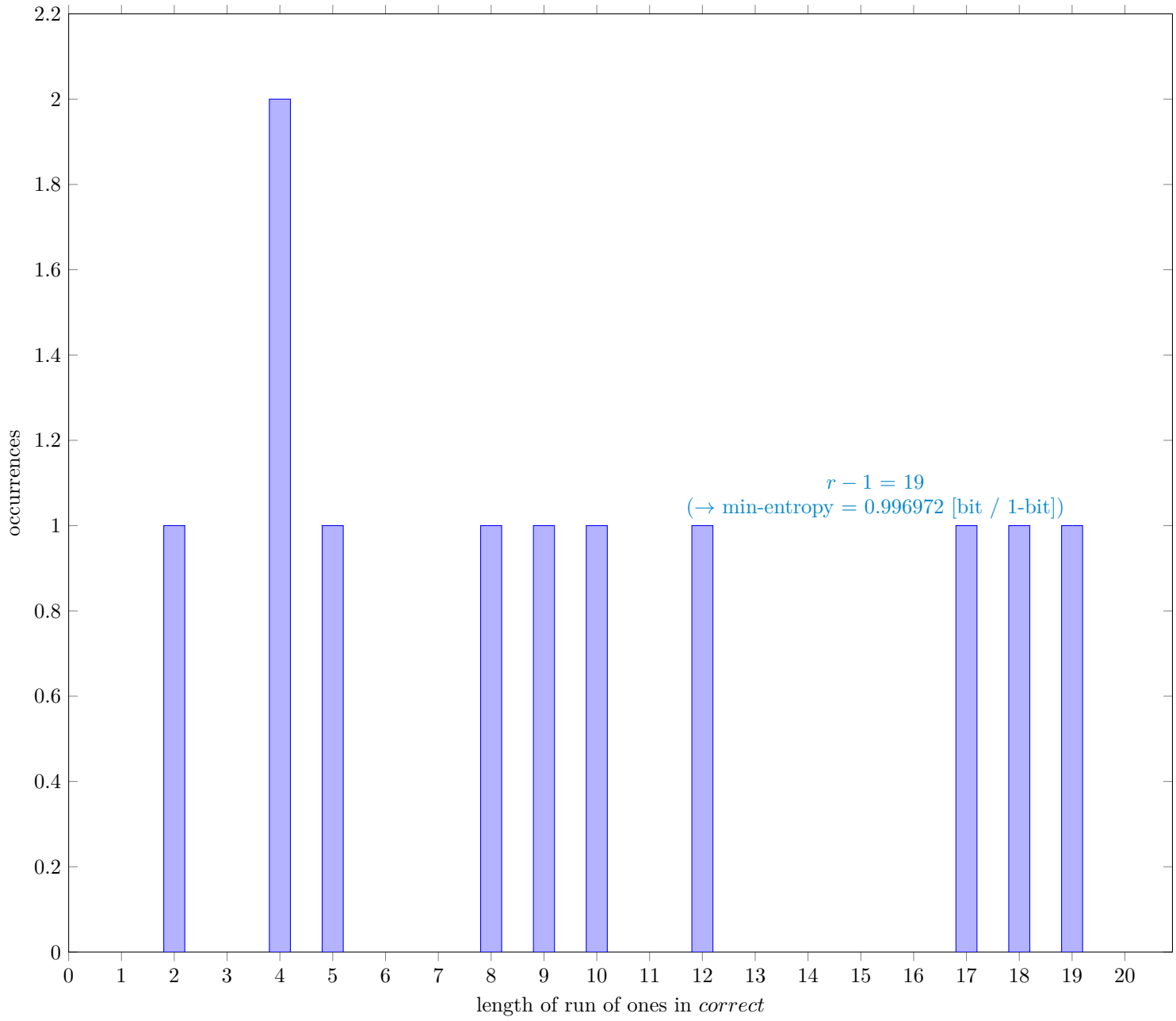


Fig. 12 Distribution of *correct*

### 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 |
| $C$ | 499731 |
| $P_{\text{global}}$ | 0.499762 |
| $P'_{\text{global}}$ | 0.50105 |
| $r$ | 20 |
| $P_{\text{local}}$ | 0.408813 |

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

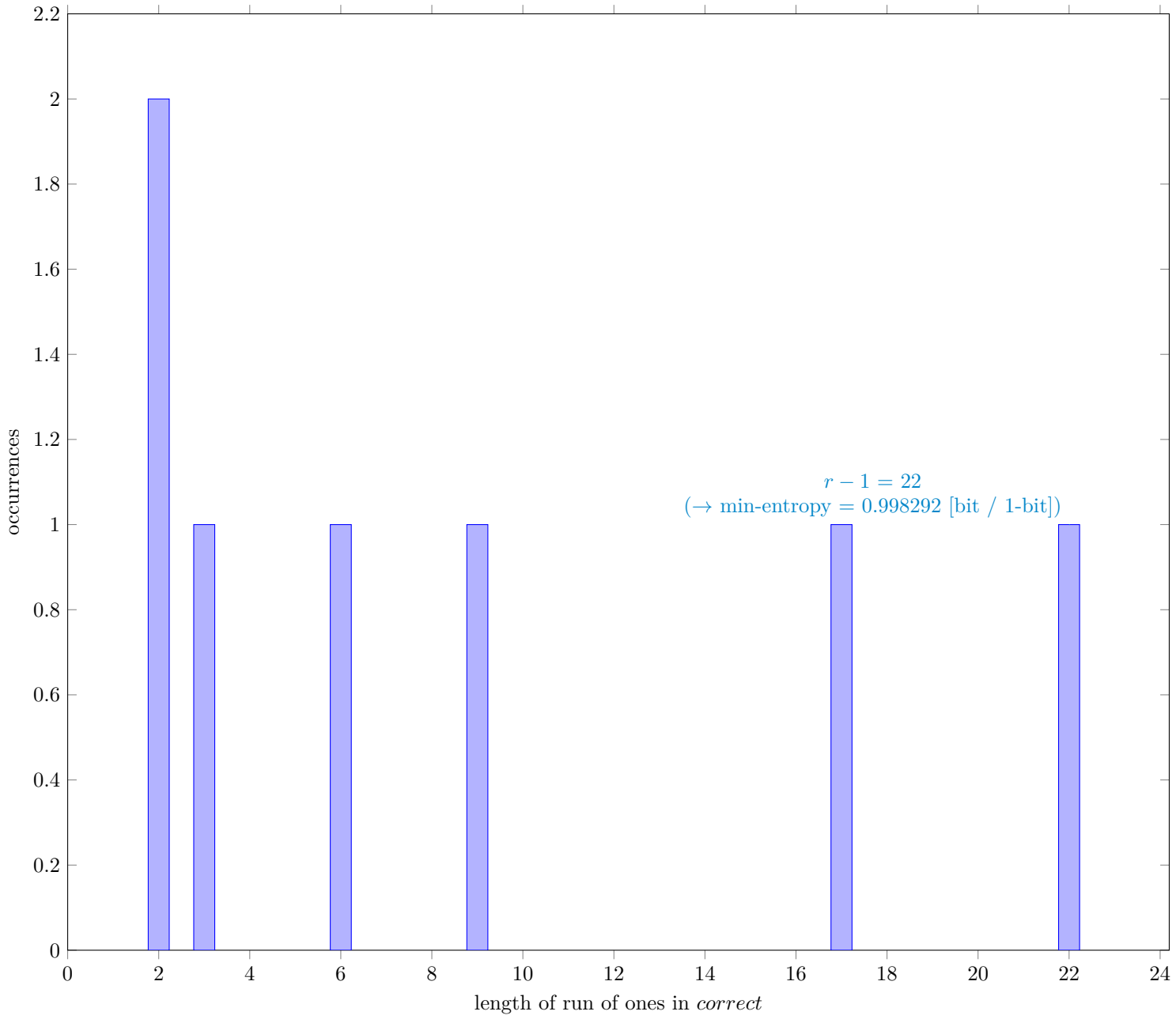


Fig. 13 Distribution of *correct*

#### 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 |
| $C$ | 499304 |
| $P_{\text{global}}$ | 0.499304 |
| $P'_{\text{global}}$ | 0.500592 |
| $r$ | 23 |
| $P_{\text{local}}$ | 0.461263 |

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

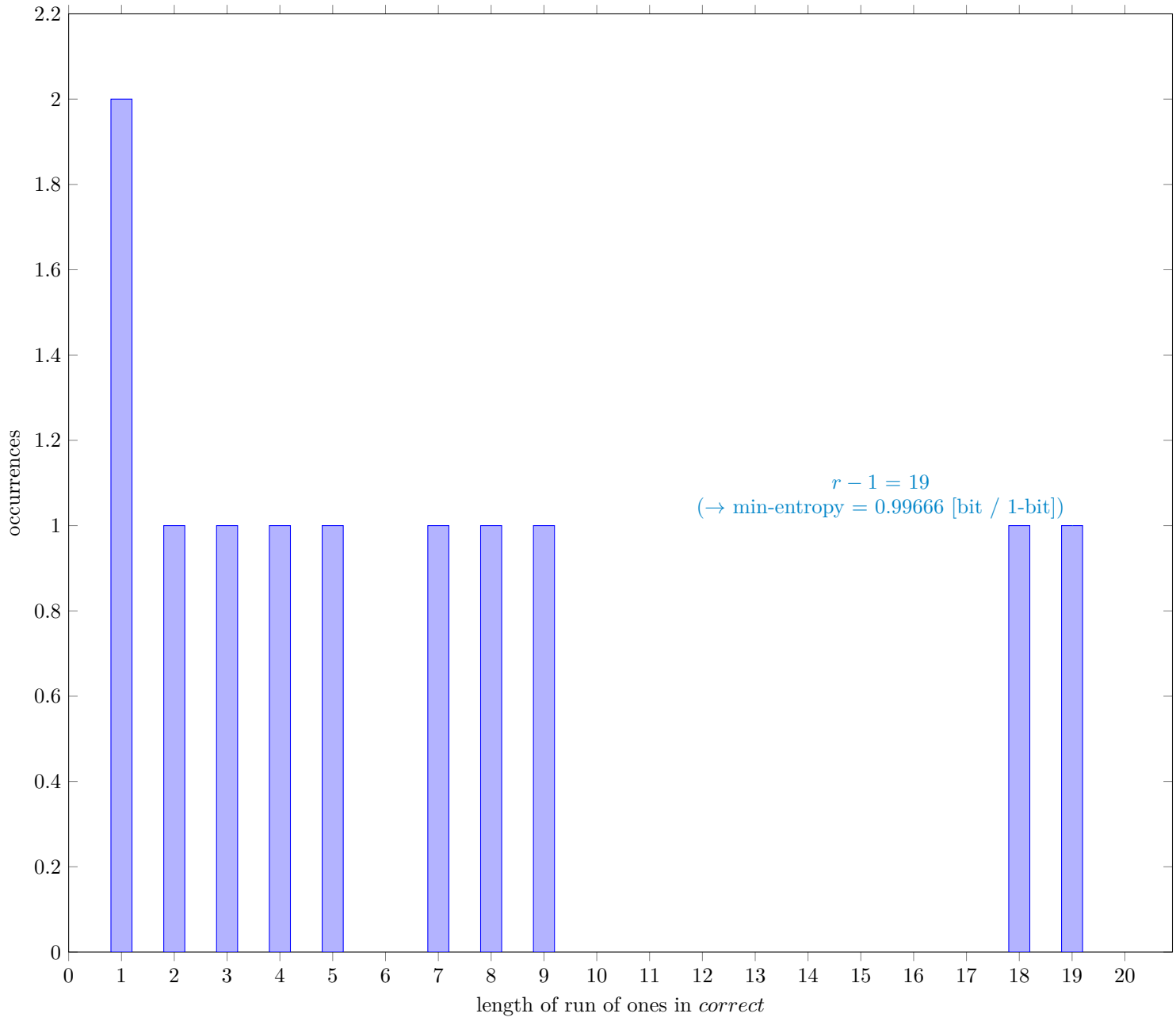


Fig. 14 Distribution of *correct*

### 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 |
| $C$ | 499870 |
| $P_{\text{global}}$ | 0.499871 |
| $P'_{\text{global}}$ | 0.501159 |
| $r$ | 20 |
| $P_{\text{local}}$ | 0.408812 |

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

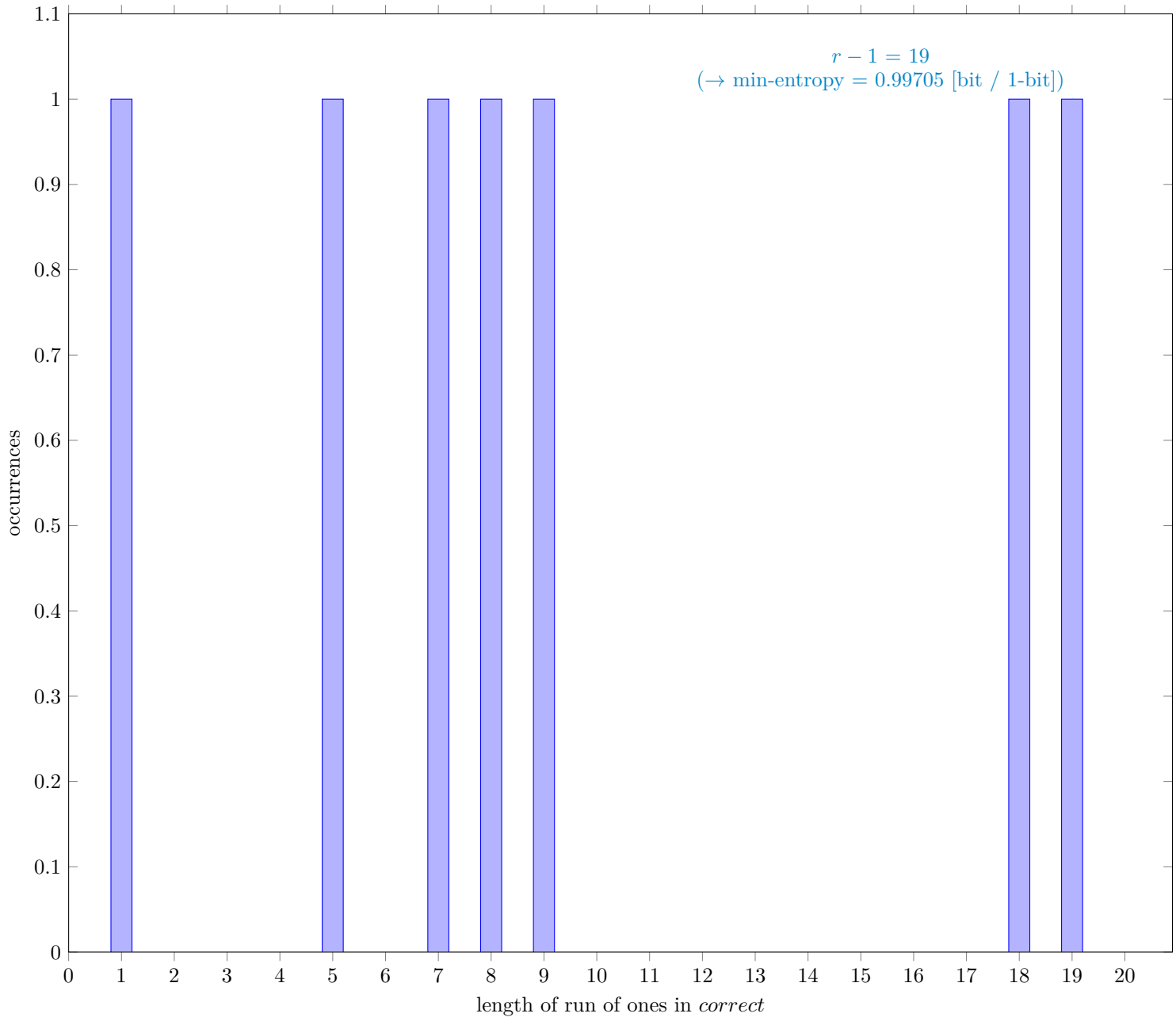


Fig. 15 Distribution of *correct*

#### 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 |
| $C$ | 499727 |
| $P_{\text{global}}$ | 0.499735 |
| $P'_{\text{global}}$ | 0.501023 |
| $r$ | 20 |
| $P_{\text{local}}$ | 0.408812 |

## 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`

[3] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest and Clifford Stein, *Introduction to Algorithms (fourth edition)*, The MIT Press. `https://mitpress.mit.edu/9780262046305/introduction-to-algorithms/`

[4] G. Sakurai, *ImplementationNotes for entropy estimation based on NIST SP800-90B non-IID track*, Sep. 2025 `https://github.com/g-g-sakura/AnotherEntropyEstimationTool/blob/main/documentation/SP800-90B_EntropyEstimate_ImplementationNotes.pdf`