擬似乱数生成系の検定方法に関する調査報告書

平成16年12月

東京理科大学理工学部電気電子情報工学科

金子研究室

第1章　はじめに

乱数は，情報セキュリティシステムにおいて，各種のプロトコルや秘密鍵の種として用いられ，その安全性は，システムの安全性に影響を持つ．乱数の安全性として，過去の乱数系列から未来の乱数系列を推定できないこと（前方予測不可能性）及び，乱数の種を推定できないこと（後方予測不可能性）が要求される．これらの予測不可能性を，発生した乱数系列から計算される統計量のランダム性を検定して判断する方法が乱数検定法である．乱数検定法で合格することは，安全な乱数であるための必要条件である．

乱数生成器の適否を判断する統計的検定法として，米国商務省標準技術局（NIST）が公開しているNIST Special Publication 800-22[1, 2]（以下SP 800-22と略記）がある．これは，乱数生成器の出力2元乱数系列を統計的手法で検定し，“ 著しく偏った乱数 ”を発生する様な乱数生成器を不適と判断する手法である．同じく，乱数の適否を統計的に判断する検定法としてDIEHARDも知られている[27]．これらの検定法は何れも，理想の乱数の統計的振る舞いを理論的に想定し，与えられた乱数列の統計量と比較する事で検定を行う．SP 800-22（Ver.1.5）は，16種類の検定法，189個の試験からなっているが，その内のDFT検定，Lempel-Ziv圧縮検定に関し，疑問点の指摘が学会で行われている[3, 4, 5]．

本報告書ではSP 800-22の16種類の検定法に対し，その背景の理論分布と，実際の試験値の分布を実験的に比較し，検定法の理論的根拠の妥当性を調査した．結果として，DFT検定，Lempel-Ziv圧縮検定では，理論分布と試験値の分布に大きな違いが有ること．近似エントロピー検定において，推奨パラメータの一部においては，理論分布からの乖離が見られることがわかった．

第2章　SP 800-22の概要

NIST SP800-22[1, 2] は，米国商務省標準技術局 NIST（National Institute of Standards and Technology）が公開している乱数の統計試験ツールである．共通鍵ブロック暗号 AES（Advanced Encryption Standard）の選定時には，暗号文出力への乱数検定法として利用された．また，複数の標本系列による乱数生成器の検定法まで規定していることも特徴の一つである．

2.1　検定項目

SP800-22 においては，2 元乱数系列から検定量を抽出する方法で大別して，次の 16 種類の検定法がある．

1. 頻度検定　Frequency (Monobit) Test
2. ブロック単位の頻度検定　Frequency Test within a Block
3. 連検定　Runs Test
4. ブロック単位の最長連検定　Test for the Longest Run of Ones in a Block
5. 2 値行列ランク検定　Binary Matrix Rank Test
6. DFT 検定　Discrete Fourier Transform (Spectral) Test
7. 重なりの無いテンプレート適合検定　Non-overlapping Template Matching Test
8. 重なりのあるテンプレート適合検定　Overlapping Template Matching Test
9. Maurer の「ユニバーサル統計量」検定　Maurer's Universal Statistical Test
10. Lempel-Ziv 圧縮検定　Lempel-Ziv Compression Test
11. 線形複雑度検定　Linear Complexity Test
12. 系列頻度検定　Serial Test
13. 近似エントロピー検定　Approximate Entropy Test

14. 累積和検定　Cumulative Sums (Cusum) Test

15. ランダム回遊検定　Random Excursions Test

16. 変形ランダム回遊検定　Random Excursions Variant Test

2.2　検定の流れ

NIST の検定では，各検定ごとに p-value が得られる．p-value とは，検定で出力される統計量の正規分布もしくは，カイ 2 乗分布において，それよりも偏った統計量が発生する確率を表したものである．p-value < 0.01 の時に良い乱数ではないと判断する．

各検定では，複数の標本系列 (NIST では 1000 程度を推奨) に対し検定を行い，

1. p-value の一様性

2. p-value が 0.01 より大きくなる割合

から乱数列の評価を行う．1. では、得られた p-value が区間 $[0, 1)$ で一様に分布しているかどうかを調べるために，$[0, 1)$ を 10 の区間に分割し，分割した区間ごとの頻度が一様になっているかどうかをカイ 2 乗検定により得られた p-value が 0.0001 以上ならば，乱数列は良い乱数であると判断する．また，2. では，標本の数を m とした時，0.01 以上となる p-value の数の割合が

$$0.99 \pm 3\sqrt{\frac{0.99 \times 0.01}{m}} \tag{2.1}$$

の範囲に入っている場合は，乱数列は良い乱数であると判断する．

第3章　SP 800-22の各種検定法及びGenerator-Using SHA-1を使った理論分布との比較

本章では，NIST のプログラムに付随されている乱数生成器：Generator-Using SHA-1 を理想乱数源と仮定することにより，SP 800-22 の 16 種類の検定法に対し，その背景の理論分布と，実際の試験値の分布を実験的に比較し，検定法の理論的根拠の妥当性を調査した結果を示す.

3.1 頻度検定

3.1.1 目的

頻度検定は、乱数列の 0 と 1 の割合がおおよそ同じになっているか調べるものである。

3.1.2 記号の定義

ε ：0 と 1 からなる乱数列

n ：乱数列の長さ

S_n ：正規分布統計量

3.1.3 推奨パラメータ

乱数長 n は $n \geq 100$ を満たすようにとる。

3.1.4 検定方法

Step1 0 と 1 からなる乱数列 $\varepsilon = (\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_n)$ を、(3.1) 式を用いて"-1" と"+1" からなる系列 $X = (X_1, X_2, \cdots, X_n)$ に変換する。

$$X_i = 2\varepsilon_i - 1 \qquad (1 \leq i \leq n) \tag{3.1}$$

Step2

$$S_n = X_1 + X_2 + \cdots + X_n \tag{3.2}$$

を計算する。

Step3 S_n は平均 $\mu = 0$、分散 $\sigma^2 = n$ の正規分布に従うので、S_n が棄却域に入るかどうかを (3.3) 式で計算される $p\text{-}value$ の値を用いて決定する。$p\text{-}value$ の値が 0.01 以上なら入力乱数はランダムであるとする。

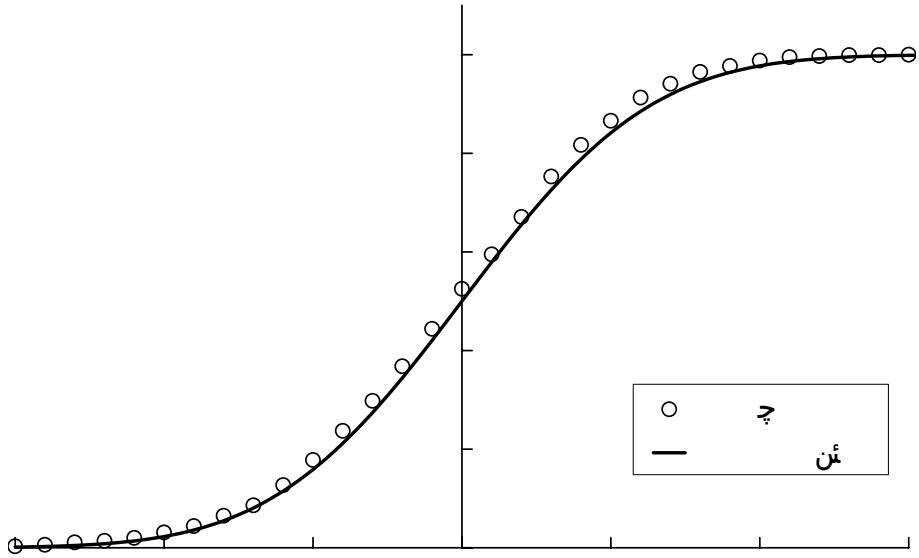
$$p\text{-}value = \mathbf{erfc}\left(\frac{|S_n|}{\sqrt{2n}}\right) \tag{3.3}$$

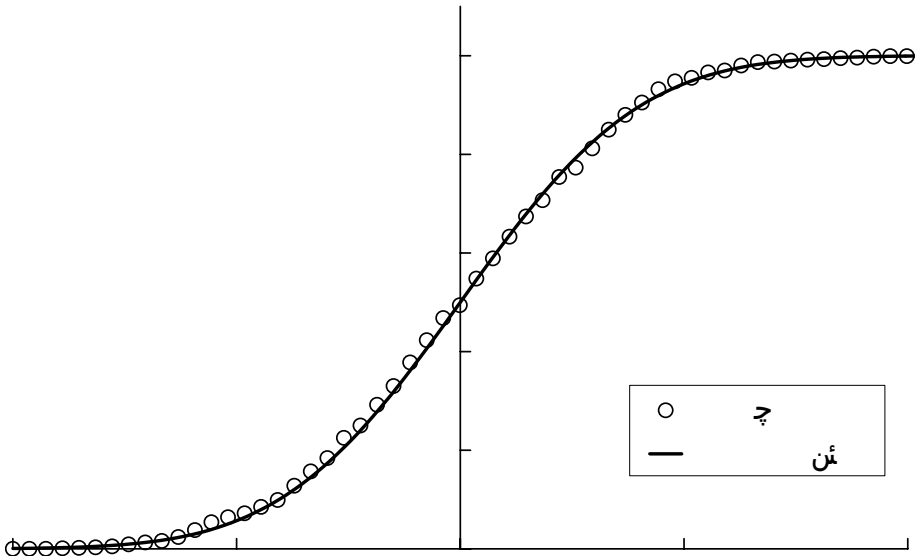
3.1.5 理論背景

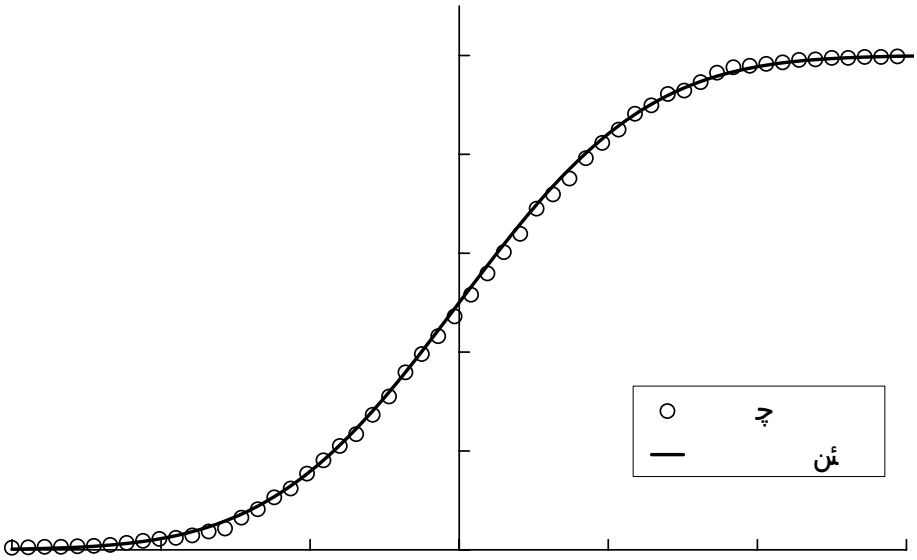
De Moivre-Laplace theorem により、S_n は平均0、分散 n の正規分布に従う。本検定は、S_n が正規分布に従うことを用いて、乱数列の 0 と 1 の割合がおおよそ同じになっているかを評価している。NIST SP800-22 で採用されている他の検定を行うときは、本検定に合格していることが前提条件となっている。

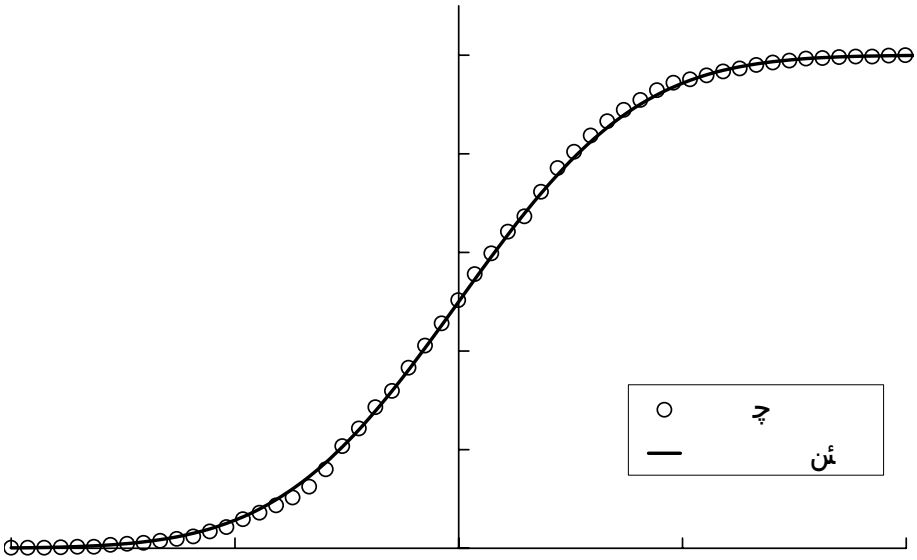
3.1.6 S_n の分布と理論分布の比較

乱数長 $n = 100$、$1,000$、$10,000$、$100,000$、$1,000,000$ の場合について、(3.2) 式で与えられる S_n が平均 $\mu = 0$、分散 $\sigma^2 = n$ の正規分布に従うかどうか、計算機実験を行った結果を図 3.1 に示す。なお、乱数生成器として NIST のプログラムに付随している G Using SHA-1 を使用し、標本系列数は 1000 とした。


چ
ئن


چ
ئن


چ
ئن


چ
ئن

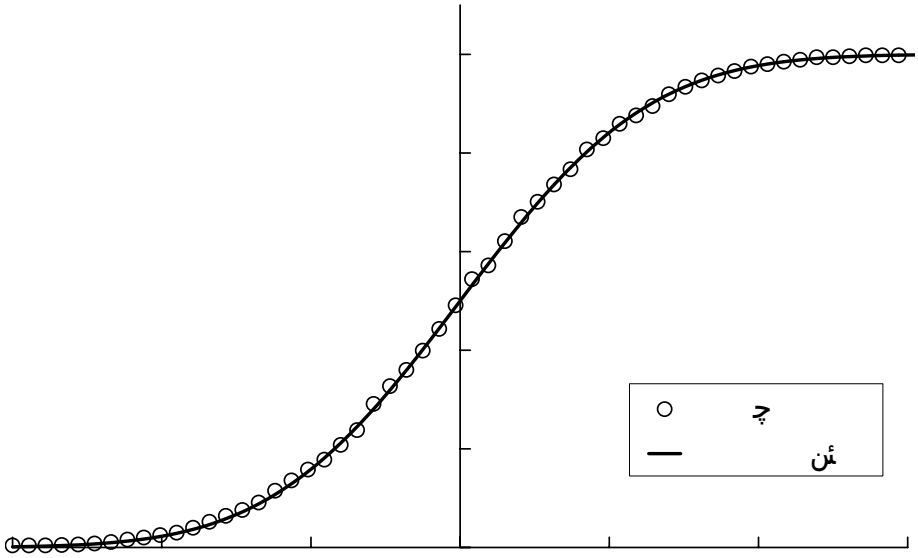


図 3.1: S_n の実測累積確率分布と理論正規分布の分布関数の比較

3.1.7　考察

推奨パラメータの範囲で実験を行い、基になる理論分布とほぼ合致していることが確認された。

3.2 ブロック単位の頻度検定

3.2.1 目的

ブロック単位の頻度検定はM ビットのブロックの中に現れる 1 の数が理想値である M/2 となっているかを確認する。

3.2.2 記号の定義

M:各ブロックの長さ
n:乱数のビット長
ε:0 と 1 からなる乱数列 $\varepsilon = (\varepsilon_1, \varepsilon_2, \cdots \varepsilon_n)$
$\chi^2(obs)$:M ビット中に現れる 1 の数が理想値である M/2 とどれほど合致しているかを表す χ^2 統計量

3.2.3 推奨パラメータ

NIST は乱数のビット長を 100 以上とし、$M \geq 20, M > 0.01n, N < 100$ という値を推奨している。

3.2.4 検定方法

Step1

入力乱数列を $N = \lfloor n/M \rfloor$ 個の重なりのないブロックに分ける。この時、使われなかったビットは廃棄する。

Step2

以下の式から $1 \leq i \leq N$ について i 番目のブロックにおける 1 の比率 π_i を計算する。

$$\pi_i = \frac{\sum_{j=1}^{M} \varepsilon_{(i-1)M+j}}{M} \tag{3.4}$$

Step3

χ^2 統計量を以下の式で計算する。

$$\chi^2(obs) = 4M \sum_{i=1}^{N} (\pi_i - \frac{1}{2})^2 \tag{3.5}$$

Step4

統計量 χ^2(obs) が χ^2 分布に従うと仮定し、統計量 χ^2(obs) の値が χ^2 分布の棄却域 (危険率 0.01) に入るかどうかを、P-value という以下の式

$$P - value = \mathbf{igamc}(\frac{N}{2}, \frac{\chi^2(obs)}{2}) \tag{3.6}$$

で計算される値を用いて決定する。P-value の値が 0.01 以上ならば入力乱数はランダムであるとする。

3.2.5 理論背景

このテストは重なりのないブロック毎に 1 の現れる頻度が理想的な値である 50 %からどれほど離れているかを検定するものである。P-value の値が小さければ 0 と 1 との比率が 1 対 1 から大きく離れているということである。
この検定において元の入力乱数は長さ M ビットの N 個のブロックに分けられる。ここで各ブロックにおける 1 の比率を π_i とし、式 (3.5) から求める統計量は自由度 N の χ^2 分布に従う。

3.2.6 統計量 $\chi^2(obs)$ と χ^2 分布との比較

以下に実際に実験を行い得られた統計量と理論値とを比較した結果を図示する。NIST は統計量が自由度 N の χ^2 分布に従うとしている。実験には NIST のプログラムに付随した G Using SHA-1 を使用し、標本数は 1000 本で行った。

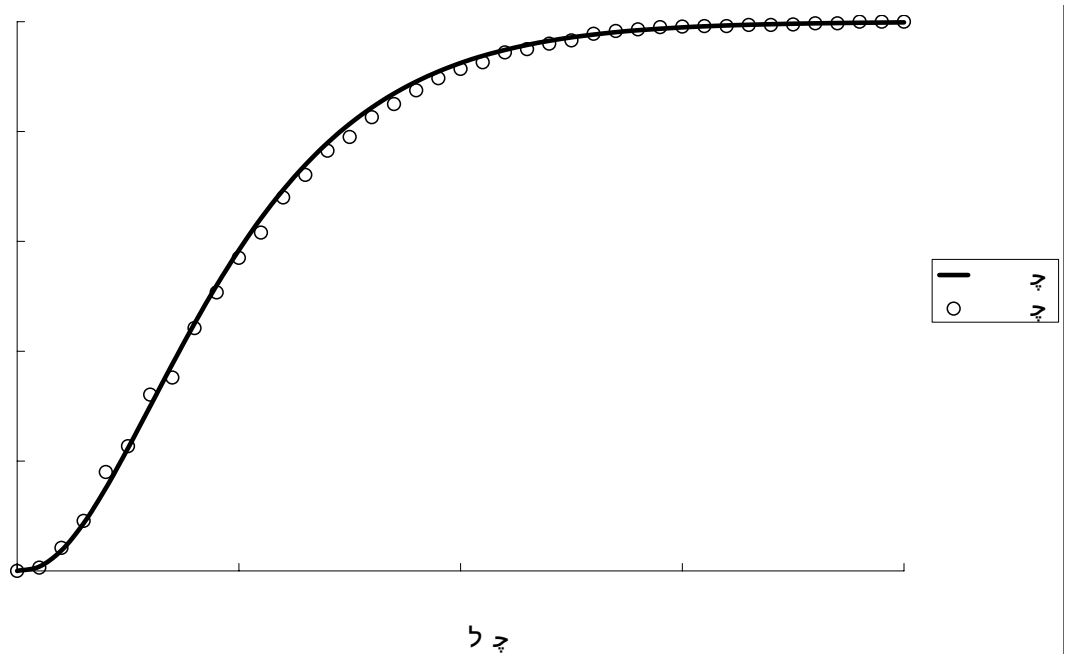


図 1:n=100 M=20 N=5

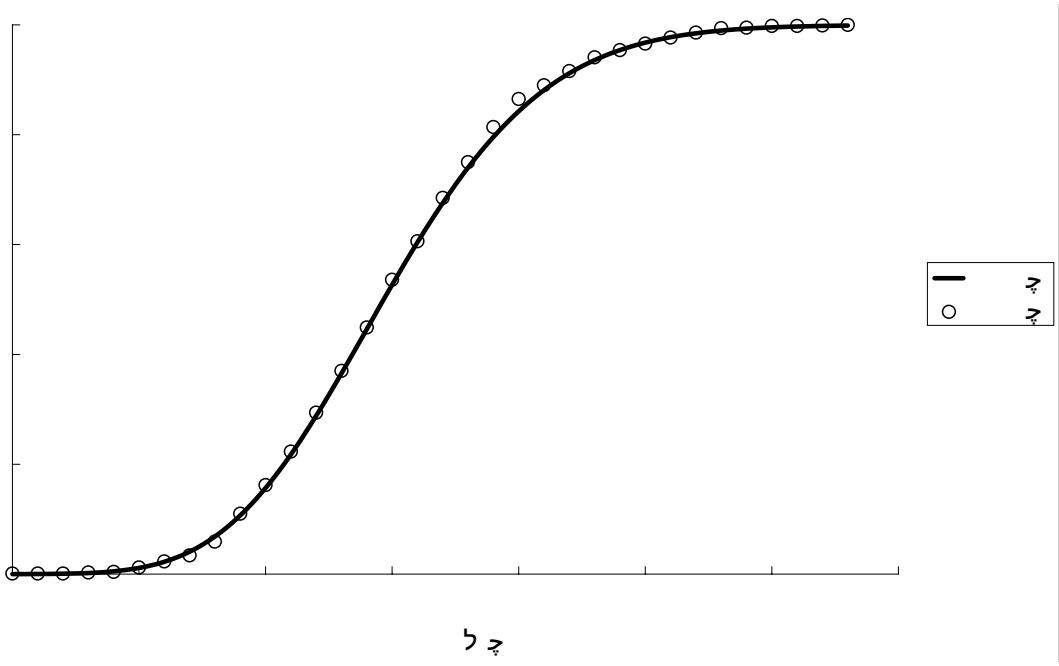


図 2:n=1,000 M=20 N=50

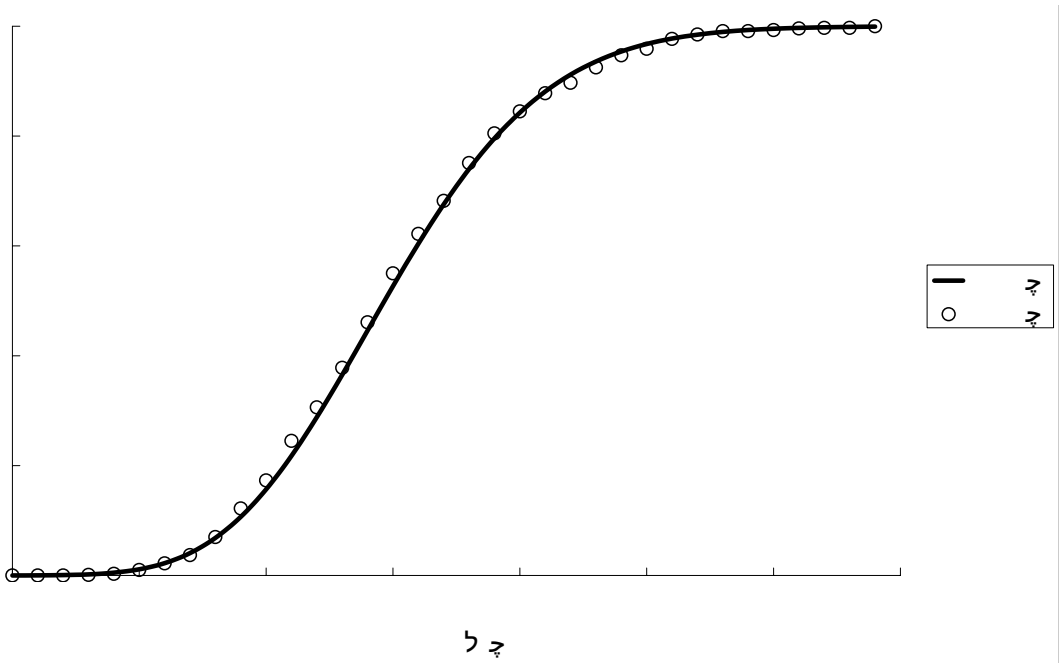


図 3:n=10,000 M=200 N=50

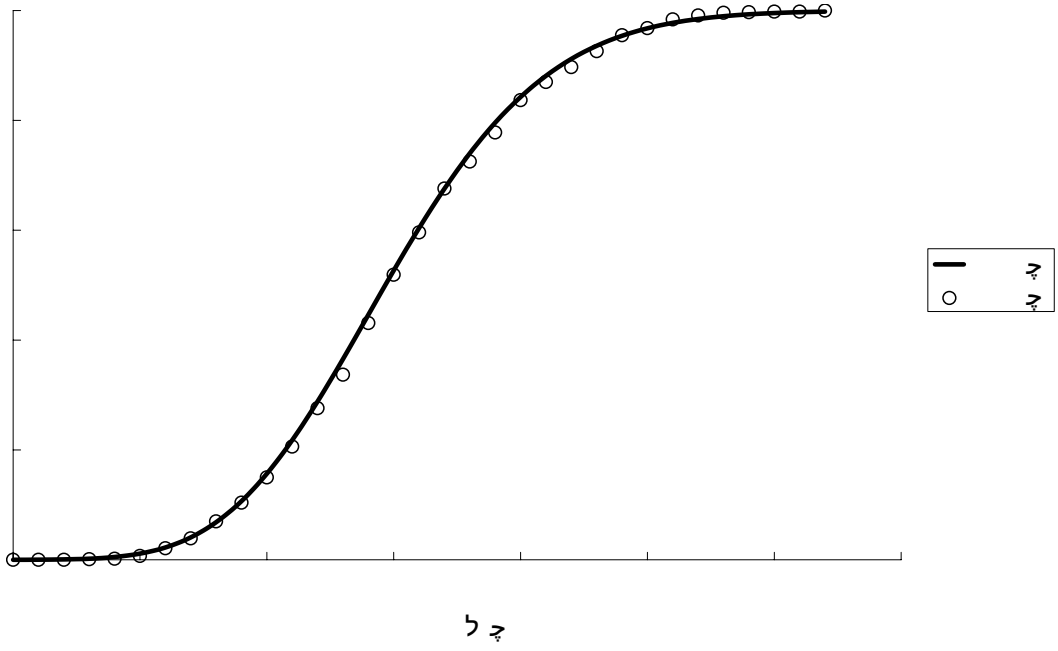


図 4:n=100,000 M=2000 N=50

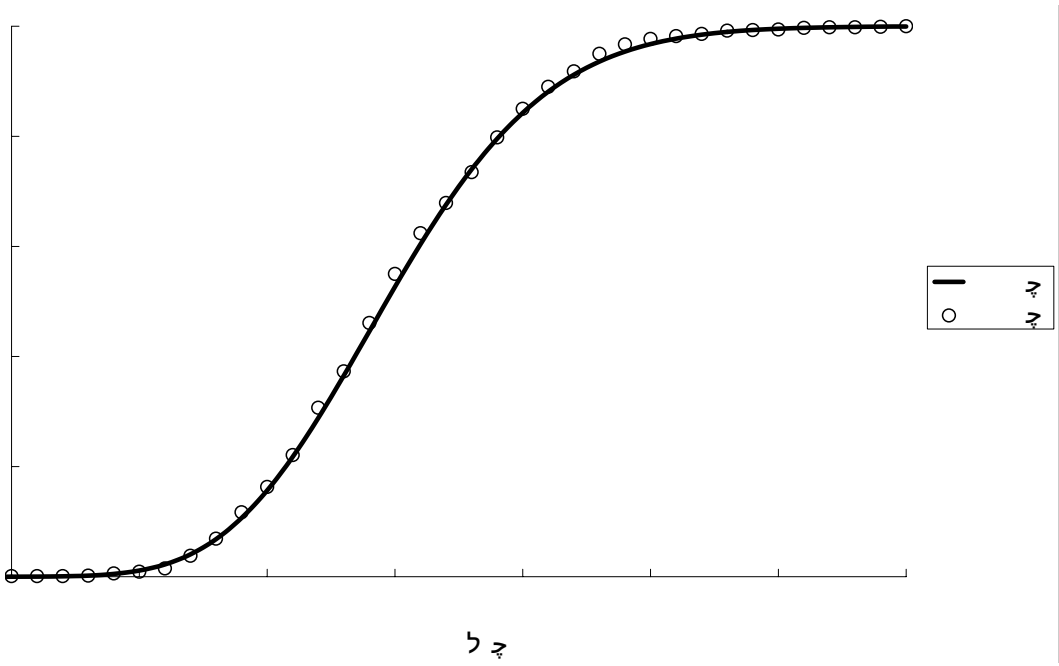


図 5:n=1,000,000 M=20000 N=50

3.2.7 考察

推奨パラメータの範囲で実験を行い、基になる理論分布とほぼ合致していることが確認された。

3.3 連検定

3.3.1 目的

連検定とは連の個数を求めその数の偏りを調べるものである。ここで、連とは同じ数字が連続してつながったものである。つまり長さ k の連とは k-1 個の同一ビットから成り、その前後のビットが異なる部分列である。

3.3.2 記号の定義

n　：乱数列の長さ
ε　：“ 0 ”と“ 1 ”からなる乱数列（ε=ε_1,ε_2,$\cdots$,ε_n）
$V_n(obs)$　：正規分布統計量

3.3.3 推奨パラメータ

NIST は乱数長 n を 100bit 以上となるように推奨している。

3.3.4 検定方法

Step1　入力乱数列の“ 1 ”の比率 π の値を次の式で計算する。

$$\pi = \frac{\sum_{j=1}^{n} \varepsilon_j}{n} \tag{3.7}$$

Step2　Runs Test に合格するかどうか決める。
もし $|\pi - \frac{1}{2}| \geq \tau$ ならば、検定を行う必要はない（すなわち、Frequency test が不合格の場合、Runs Test は行わない)。検定を行わないならば、出力は 0 とする。これは Frequency test により π は 1/2 に近づくということを示している。
この検定において、$\tau = \frac{2}{\sqrt{n}}$ と定義する。

Step3　確率変数 $V_n(obs)$ を下記の計算式で計算する。

$$V_n(obs) = \{\sum_{k=1}^{n-1} r(k)\} + 1 \tag{3.8}$$

ここで、$\varepsilon_k = \varepsilon_{k+1}$ なら $r(k)$=0、$\varepsilon_k \neq \varepsilon_{k+1}$ なら $r(k)$=1 となる。
つまり、(3.8) 式は“ 0 ”から“ 1 ”,“ 1 ”から“ 0 ”への変換点の個数を求めてそれに 1 を足したものであり、$V_n(obs)$ は乱数列nビットにおける連の総数である。

Step4　確率変数 $V_n(obs)$ が標準正規分布に従うと仮定し、確率変数 $V_n(obs)$ の値が標準正規分布の棄却域（危険率 0.01）に入るかどうかを、$P-value$ という以下の式：

$$P-value = erfc\{\frac{|V_n(obs)-2n\pi(1-\pi)|}{2\sqrt{2n}\pi(1-\pi)}\} \tag{3.9}$$

で計算される値を用いて決定する。$P-value$ の値が 0.01 以上ならば入力乱数はランダムであるとする。

3.3.5　理論背景

確率変数 V_n の分布は、中心極限定理より平均 μ:$2n\pi(1-\pi)$、分散 σ^2:$2\sqrt{n}\pi(1-\pi)$ の正規分布になり次式で表わされる。

$$\lim_{n\to\infty} P\Big(\frac{V_n-2n\pi(1-\pi)}{2\sqrt{n}\pi(1-\pi)} \le z\Big) = \Phi(z) \tag{3.10}$$

ここで、

$$\Phi(z) = \int_{-\infty}^{z} \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}} dx \tag{3.11}$$

は標準正規分布の累積分布関数であり、確率変数 V_n の分布は正規分布に従う。

また、NIST では $\Phi(z)$ のかわりに、誤差関数

$$erfc(z) = \int_{z}^{\infty} \frac{2}{\sqrt{\pi}} e^{-x^2} dx \tag{3.12}$$

を用いているため、

$$P-value = erfc(\frac{z}{\sqrt{2}}) \tag{3.13}$$

となり、(3.9) 式のように求めることが出来る。

3.3.6　確率変数 $V_n(obs)$ と標準正規分布との比較

乱数長 n が 100,1000,10^4,10^5,10^6bit の場合で、確率変数 $V_n(obs)$ が正規分布に従うかどうか、シミュレーション実験を行った結果を以下に示す。なお、全ての測定は乱数生成アルゴリズムとして NIST のプログラムに付随している G-Using SHA-1 を使用し、標本数を 1000 とした。

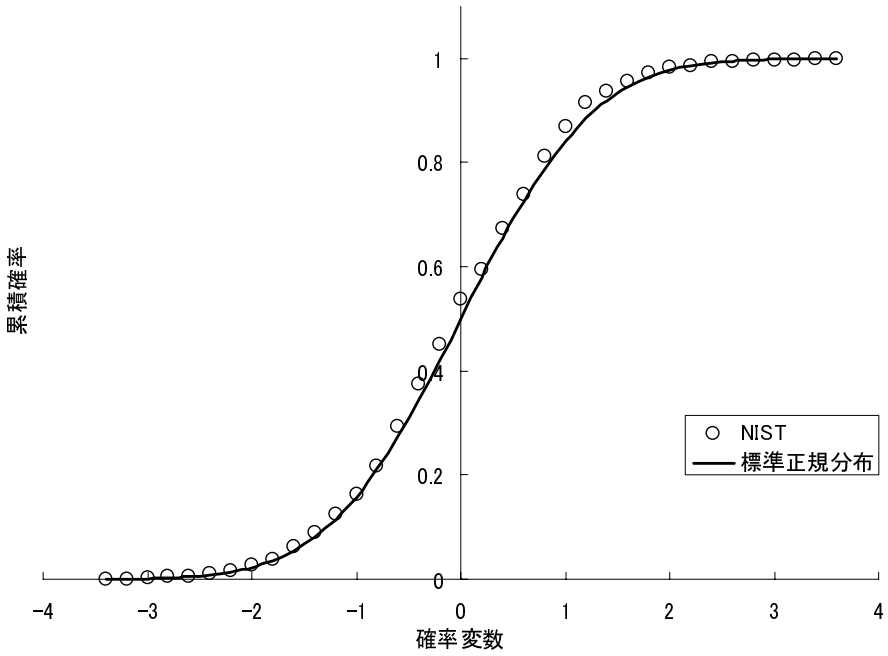


図 3.2: n=100bit

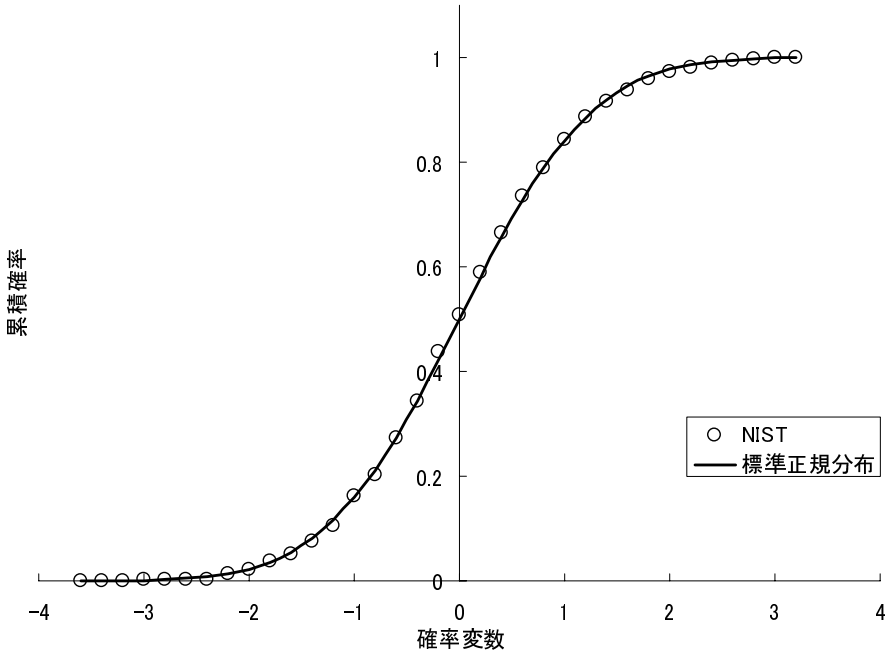


図 3.3: n=1000bit

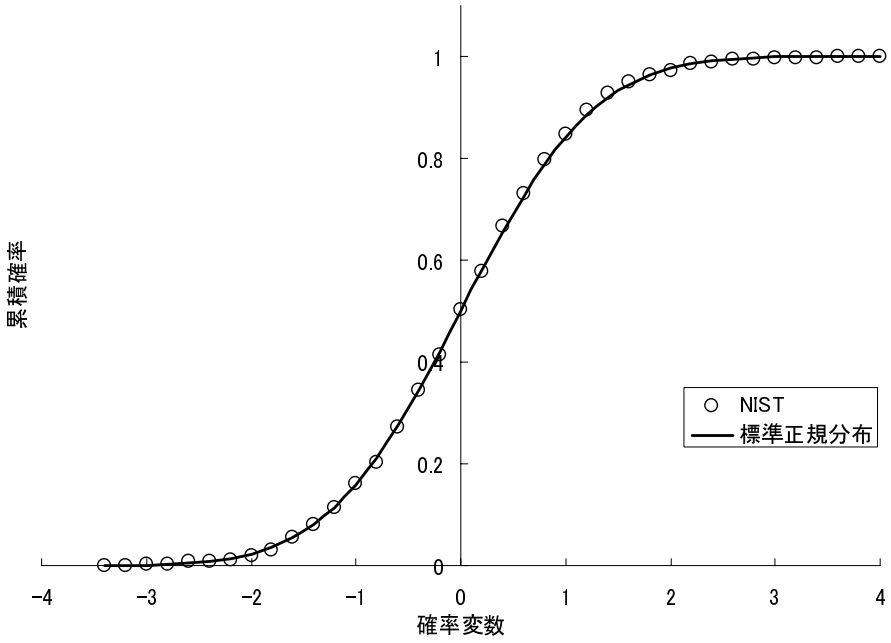


図 3.4: n=10^4bit

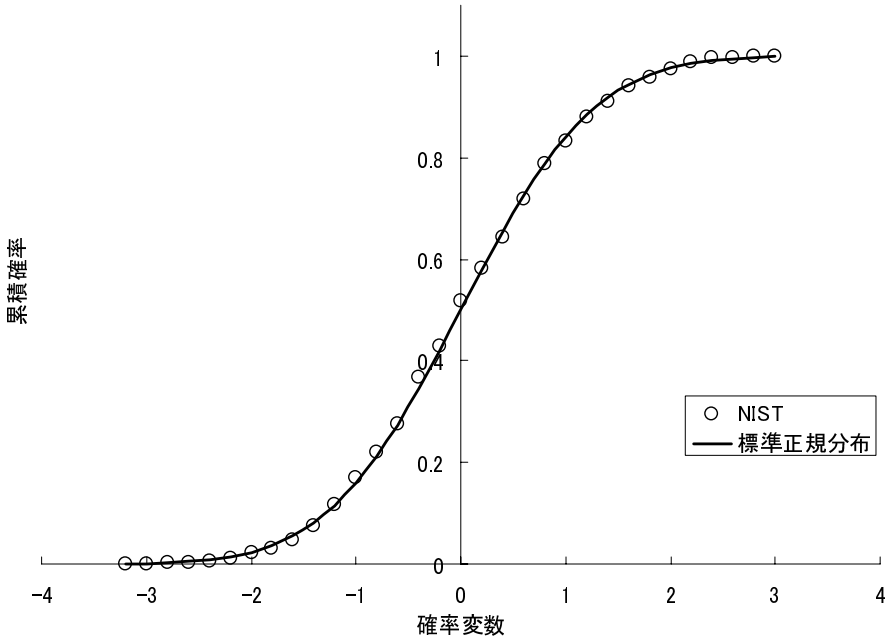


図 3.5: n=10^5bit

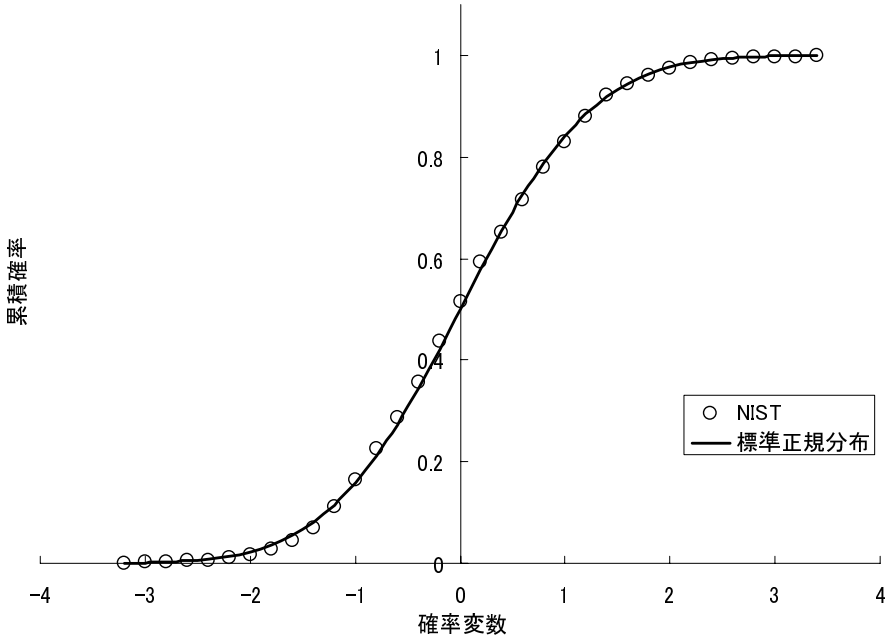


図 3.6: n=10^6bit

3.3.7 考察

推奨パラメータの範囲で実験を行い、基になる理論分布とほぼ合致していることが確認された。

3.4 ブロック単位の最長連検定

3.4.1 目的

ブロック単位の最長連検定とは乱数列を長さ M ビットのブロックに分割し、ブロックの最長連の長さに応じて各部分列をクラス分けし、その度数をカイ２乗検定にて検定し最長連の長さの偏りを調べるものである。

3.4.2 記号の定義

n　：ビット列の長さ
ε　：“０”と“１”からなる乱数列（ε=ε_1,ε_2,$\cdots$,ε_n）
M　：ブロックの長さ（乱数列の長さによって決まる。表 1 を参照。）

n の範囲	M
$128 \leq n < 6272$	8
$6272 \leq n < 750000$	128
$750000 \leq n$	10^4

表 1：M の値を定める n の範囲

N　：ブロックの数
$\chi^2(obs)$　：カイ２乗統計量

3.4.3 推奨パラメータ

NIST は乱数長 n を 128bit 以上となるように推奨している。

3.4.4 検定方法

Step1　入力した乱数列 n を長さ M のブロックに分割する。$N = \lfloor \frac{n}{M} \rfloor$
Step2　各ブロックの“１”の最長連の長さによって、表 2 に従いクラス分けし、その頻度 ν_i を求める。

ν_i	M=8	M=128	M=10^4
ν_0	$\leq$1	$\leq$4	$\leq$10
ν_1	2	5	11
ν_2	3	6	12
ν_3	$\geq$4	7	13
ν_4		8	14
ν_5		$\geq$9	15
ν_6			$\geq$16

表2：各々の M における ν_i の振分け

Step3　統計量 $\chi^2(obs)$ を次の計算式で計算する。

$$\chi^2(obs) = \sum_{i=0}^{K} \frac{(\nu_i - N\pi_i)^2}{N\pi_i} \tag{3.14}$$

ここで、K , π_i の値は、表3にしたがって決められる。

M	K	π_i
8	3	ν_0 ; π_0=0.2148
		ν_1 ; π_1=0.3672
		ν_2 ; π_2=0.2305
		ν_3 ; π_3=0.1875
128	5	ν_0 ; π_0=0.1174
		ν_1 ; π_1=0.2430
		ν_2 ; π_2=0.2493
		ν_3 ; π_3=0.1752
		ν_4 ; π_4=0.1027
		ν_5 ; π_5=0.1124
10^4	6	ν_0 ; π_0=0.0882
		ν_1 ; π_1=0.2092
		ν_2 ; π_2=0.2483
		ν_3 ; π_3=0.1933
		ν_4 ; π_4=0.1208
		ν_5 ; π_5=0.0675
		ν_6 ; π_6=0.0727

表3：M に対する K , π_i の値

Step4　確率変数 $\chi^2(obs)$ がカイ2乗分布に従うと仮定し、確率変数 $\chi^2(obs)$ の値がカイ2乗分布の棄却域（危険率0.01）に入るかどうかを、$P-value$ という以下の式：

$$P - value = igamc\{\frac{K}{2}, \frac{\chi^2(obs)}{2}\} \tag{3.15}$$

で計算される値を用いて決定する。$P-value$ の値が0.01以上ならば入力乱数はランダムであるとする。

3.4.5　理論背景

ν は最長連の長さによって $K+1$ のクラスにわける度数である。分割されたそれぞれのブロックについて、最長連の長さの値が ν_0〜ν_K のどこに属するかを判定しカウントしていく。

長さ M の数列に r 個の“ 1 ”と $M-r$ 個の“ 0 ”がある場合、頻度 ($\nu \leq$ m) の発生確率を次式で表わすことができる。ここで、m は最長連の長さ、$U = min\left(M-r+1, \left[\frac{M-j(m+1)}{M-r}\right]\right)$ である。

$$P(\nu \leq m|r) = \frac{1}{\begin{pmatrix} M \\ r \end{pmatrix}} \sum_{j=0}^{U} (-1)^j \begin{pmatrix} M-r+1 \\ j \end{pmatrix} \begin{pmatrix} M-j(m+1) \\ M-r \end{pmatrix}$$

$$P(\nu \leq m) = \sum_{r=0}^{M} \left(\begin{array}{c} M \\ r \end{array} \right) P(\nu \leq m|r) \frac{1}{2^M} \tag{3.16}$$

それぞれのクラスの頻度の理論値は (3.16) 式から求められ、表３のように表わすことができる。

統計量 χ^2 は実測値 ν と理論値 π より (3.14) 式となり、これは自由度 K のカイ２乗分布に近づく。また、カイ２乗分布に基づいて検定が行われる場合、$P-value$ は次式のようになる。

$$igamc\left(\frac{K}{2}, \frac{\chi^2(obs)}{2}\right) = \frac{1}{\Gamma(\frac{K}{2}) \cdot 2^{\frac{K}{2}}} \int_{\chi^2(obs)}^{\infty} e^{-\frac{u}{2}} \cdot u^{\frac{K}{2}-1} du \tag{3.17}$$

3.4.6 実測値 ν と理論値 π との比較

各クラスの発生確率の理論値は表 3 である。実験により求められた頻度 ν_i をブロック数 N で割ったもの $\nu' = \frac{\nu_i}{N}$ を図3.7〜3.9 に示す。実験は乱数長 n が 128, 8192, 10^6bit に対し行い、乱数生成器は NIST のプログラムに付属の G-Using SHA-1 を使用した。

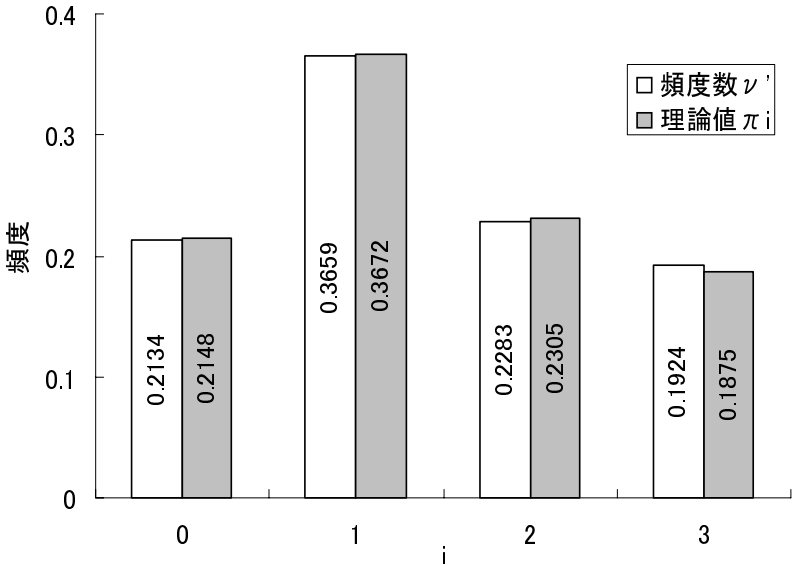


図 3.7: n=128bit

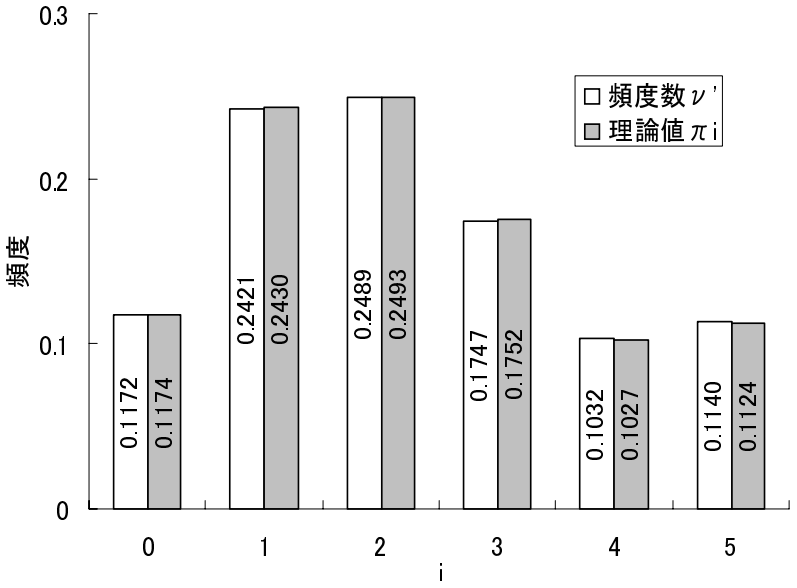


図 3.8: n=8192bit

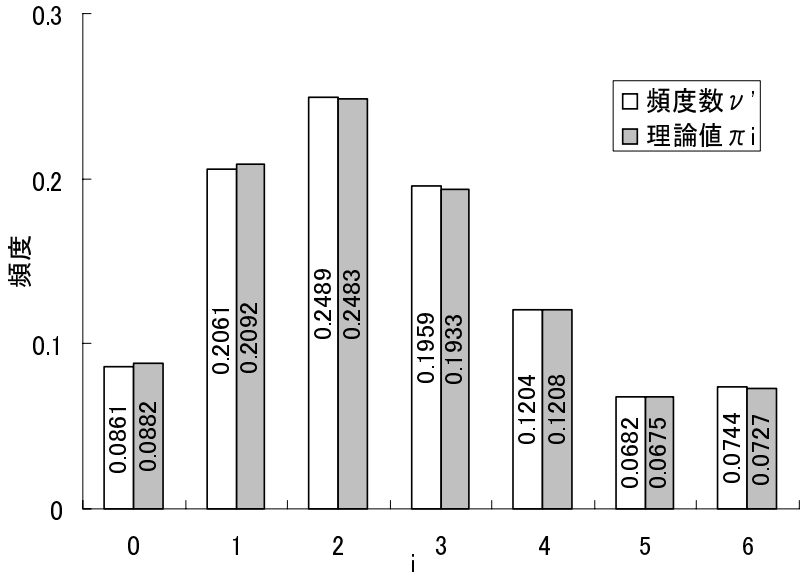


図 3.9: n=10^6bit

3.4.7 確率変数 $\chi^2(obs)$ とカイ２乗分布との比較

乱数長 n が 128 , 8192 , 10^6bit の場合で、確率変数 $\chi^2(obs)$ がカイ２乗分布に従うかどうか実験を行った結果を以下に示す。また、全ての測定は乱数生成アルゴリズムとして NIST のプログラムに付随している G-Using SHA-1 を使用し、標本数を 1000 とした。

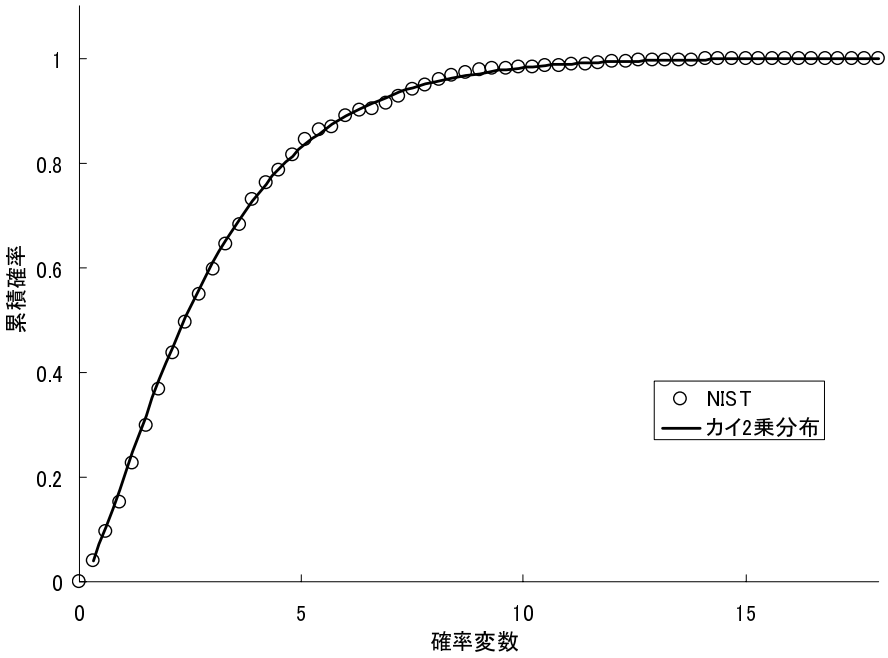


図 3.10: n=100bit

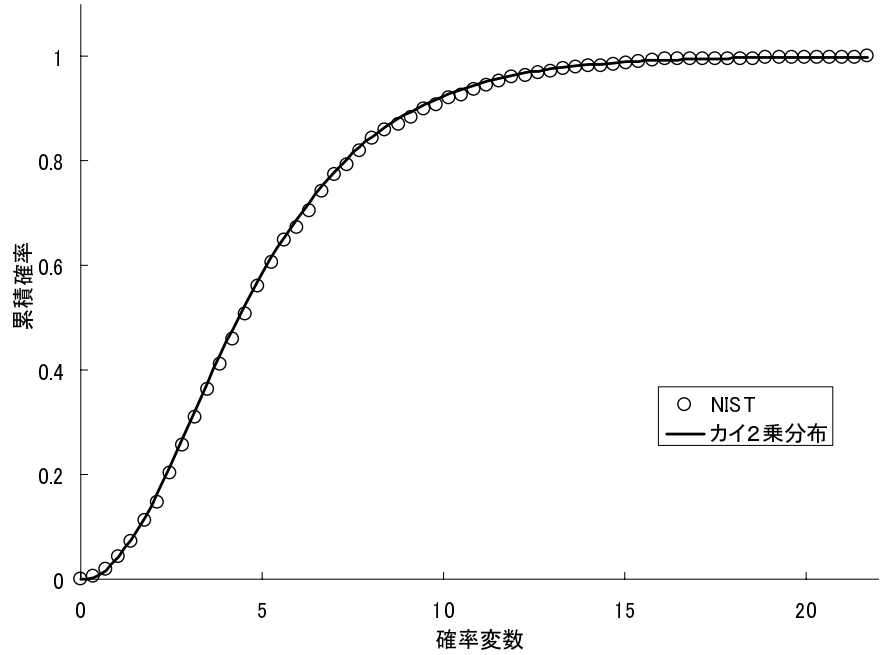


図 3.11: n=8192bit

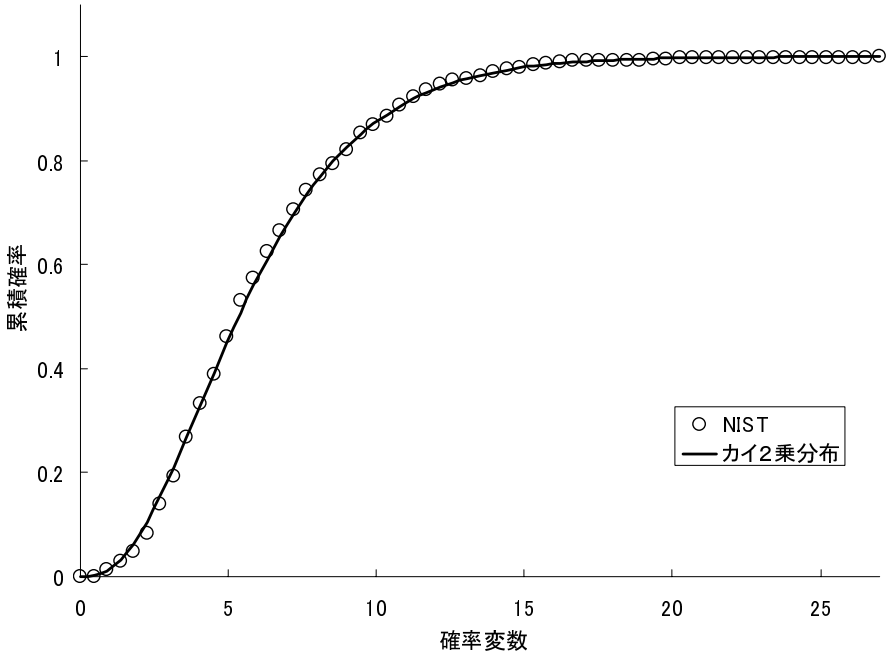


図 3.12: n=10^6bit

3.4.8 考察

推奨パラメータの範囲で実験を行い、基になる理論分布とほぼ合致していることが確認された。

3.5　2 値行列ランク検定

3.5.1　目的

2 値行列ランク検定は乱数列から作った行列のランクの偏りを調べる。

3.5.2　記号の定義

n:乱数の長さ
ε:0 と 1 からなる乱数列 $\varepsilon = (\varepsilon_1, \varepsilon_2, \cdots \varepsilon_n)$
M:作成する行列の行の数。この検定では M=32 が与えられている。
Q:作成する行列の列の数。この検定では Q=32 が与えられている。
$\chi^2(obs)$:測定されたランクの値が理想値とどれほど合致しているかを表す χ^2 統計量

3.5.3　推奨パラメータ

NIST は乱数のビット長を 38912bit 以上にするとしている。

3.5.4　検定方法

Step1

入力乱数列を $N = \left\lfloor \frac{n}{MQ} \right\rfloor$ 個の長さ M·Q ビットのブロックに分ける。使わなかったビットは廃棄する。
各ブロックについて連続する Q ビットの系列を先頭から順番に行列の各行として M×Q の行列を作る。

Step2

各行列についてランク $R_l (1 \leq l \leq N)$ を求める。

Step3

以下のように定義する。
$F_M : R_l = M$ となる行列の数
$F_M - 1 : R_l = M - 1$ となる行列の数
$N - F_M - F_{M-1}$:残りの行列の数

Step4

χ^2 統計量を以下の式で計算する。

$$\chi^2(obs) = \frac{(F_M - 0.2888N)^2}{0.2888N} + \frac{(F_{M-1} - 0.5776N)^2}{0.5776N} + \frac{(N - F_M - F_{M-1} - 0.1336N)^2}{0.1336N} \tag{3.18}$$

Step5

統計量 χ^2(obs) が χ^2 分布に従うと仮定し、統計量 χ^2(obs) の値が χ^2 分布の棄却域 (危険率 0.01) に入るかどうかを、P-value という以下の式

$$P - value = e^{-\chi^2(obs)/2} \tag{3.19}$$

で計算される値を用いて決定する。P-value の値が 0.01 以上ならば入力乱数はランダムであるとする。

3.5.5 理論背景

ランダムであるかどうかを検定する方法のひとつとして入力乱数から作る行列の線形従属性をチェックすることがある。
この検定は Kovalenko [9], また Marsaglia と Tsay [10] による結果に基づいている。この結果とは $M \times Q$ のランダムな 2 値行列のランクが値 $r = 0, 1, 2, \cdots, m$ をとる確率は

$$p_r = 2^{r(Q+M-r)-MQ} \prod_{i=1}^{r-1} \frac{(1-2^{i-Q})(1-2^{i-M})}{1-2^{i-r}} \tag{3.20}$$

で与えられるというものである。この検定では M と N がともに 32 という値が与えられており、この値を用いると

$$p_M \approx \prod_{j=1}^{\infty} [1 - \frac{1}{2^j}] = 0.2888\ldots \tag{3.21}$$

$$p_{M-1} \approx 2p_m \approx 0.5776\ldots \tag{3.22}$$

$$p_{M-2} \approx \frac{4p_M}{9} \approx 0.1284\ldots \tag{3.23}$$

となる。ここで $M \geq 10$ の時、他の確率はとても小さく (≤ 0.05) なる。元の数列から $N = \left\lfloor \frac{n}{MQ} \right\rfloor$ 個の行列を作成したとすると、それら N 個の行列のランクが M のもの、M-1 のもの、M-2 を超えないものの 3 パターンに分類し、それぞれの個数を $F_M, F_{M-1}, N - F_M - FM - 1$ と定義する。
そして式 (3.18) で表される統計量 $\chi^2(obs)$ が自由度 2 の χ^2 分布に従うと仮定し χ^2 検定を行う。

3.5.6 統計量 $\chi^2(\mathrm{obs})$ と χ^2 分布との比較

以下に実際に実験を行い得られた統計量と理論値とを比較した結果を図示する。NIST は統計量が自由度 2 の χ^2 分布に従うとしている。実験には NIST のプログラムに付随した G Using SHA-1 を使用し、標本数は 1000 本で行った。

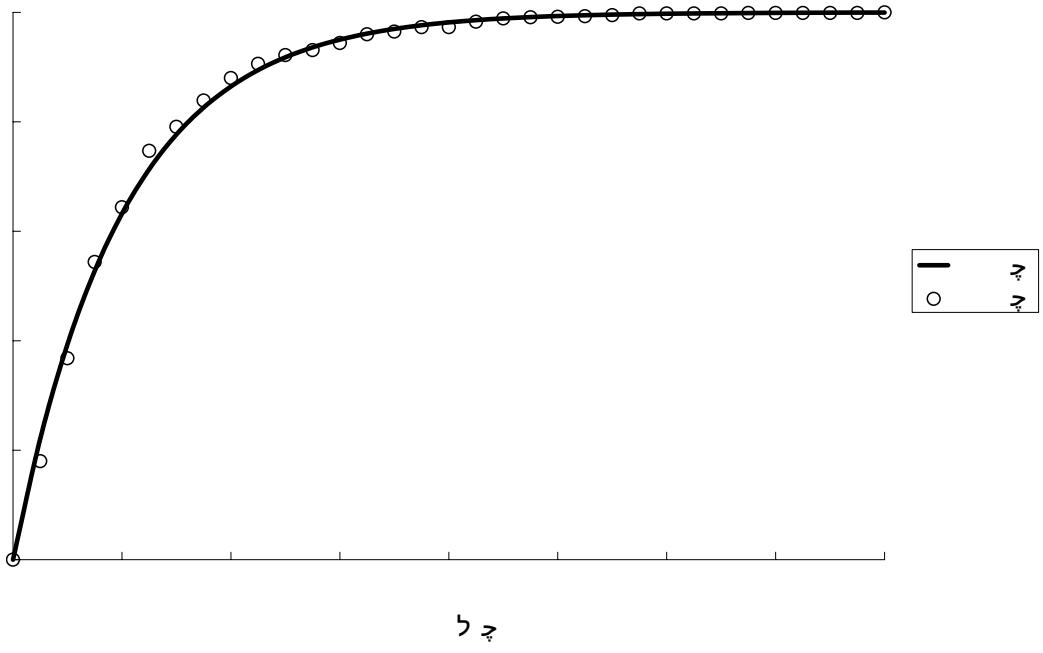


図 1:38912bit

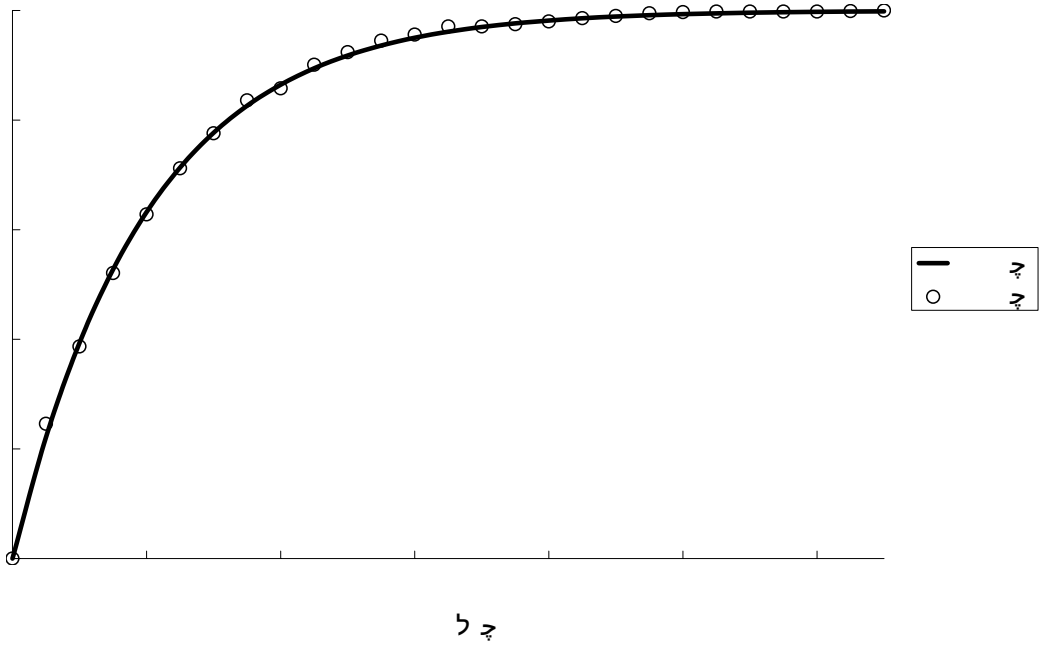


図 2:100,000bit

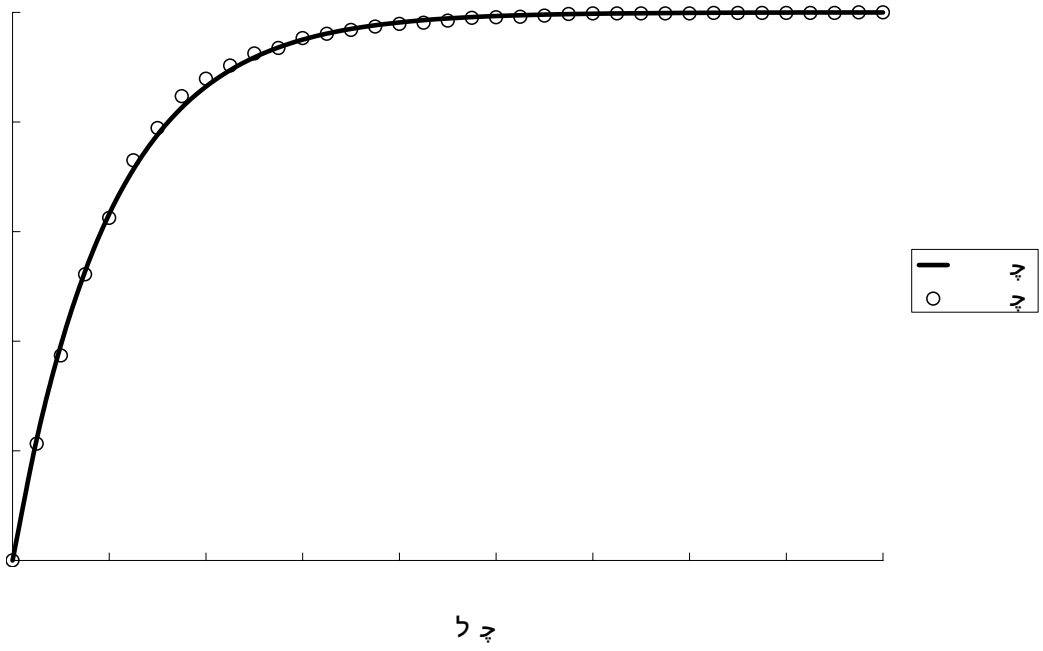


図 3:1,000,000bit

3.5.7 考察

推奨パラメータの範囲で実験を行い、基になる理論分布とほぼ合致していることが確認された。

3.6 DFT 検定

3.6.1 目的

DFT 検定は，0 と 1 からなる乱数列を ± 1 の実数値系列と見なし，離散フーリエ変換（Discrete Fourier Transform）を行い，周波数成分に分解する．その各周波数成分の絶対値が閾値を超えない割合を求めることにより乱数列のランダム性を調べる．

3.6.2 記号の定義

ε ：0 と 1 からなる乱数列

n ：乱数列の長さ

d ：95 %閾値点を越えない周波数成分の個数の実測値と理論値の差を正規化した確率変数

3.6.3 推奨パラメータ

乱数長 n に関して，NIST は 1000bit 以上を推奨している．

3.6.4 検定方法

Step1　0 と 1 からなる乱数長 n の乱数列 $\varepsilon = \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n (\varepsilon_i \in \{0, 1\}, i = 1, 2, \cdots, n)$ を -1 と 1 からなる乱数列 $X = x_1, x_2, \cdots, x_n$（ただし，$x_i = 2\varepsilon_i - 1$）に変換する．

Step2　Step1 で変換した乱数列 X を以下の式：

$$f_j = \sum_{k=1}^{n} x_k \exp\left(i\frac{2\pi(k-1)j}{n}\right) \quad \text{ただし，} i \equiv \sqrt{-1} \tag{3.24}$$

により，離散フーリエ変換（Discrete Fourier Transform）し，周波数成分 $f_j (j = 0, 1, \cdots, n-1)$ を求める．ここで，$f_j = \bar{f}_{n-j} (j = 0, \frac{n}{2}$ の場合は除く）という共役関係が生じるので，$f_0, \cdots, f_{\lfloor \frac{n-1}{2} \rfloor}$ の周波数成分だけを検定に使用する．

Step3　周波数成分 f_j の絶対値 $|f_j|$ の 95 %点である閾値 $T = \sqrt{3n}$ を計算し，閾値 T を超えない周波数成分の個数の期待値 $N_0 = 0.95n/2$ を求める．

Step4　$|f_j|$ の中で閾値 T を超えない周波数成分の個数の実測値 N_1 を求め，次式：

$$d = \frac{N_1 - N_0}{\sqrt{n(0.95)(0.05)/2}} \tag{3.25}$$

で定義される正規化確率変数 d を計算する．

Step5　確率変数 d が標準正規分布に従うと仮定し，確率変数 d の値が標準正規分布の棄却域（危険率 0.01）に入るかどうかを，$P-value$ という以下の式：

$$P-value = erfc\left(\frac{|d|}{\sqrt{2}}\right) \tag{3.26}$$

で計算される値を用いて決定する．$P-value$ の値が 0.01 以上ならば入力乱数はランダムであるとする．

3.6.5　理論背景

DFT 検定の問題点として，閾値の近似による確率変数分布のずれ，および閾値近似を補正した確率変数分布の分散値減少が濱野ら [3]，Kim ら [4] によって指摘されている．また，山本らは分散値減少の要因の一つとして，パーセバルの定理に由来する周波数成分のエネルギー制限であると推定している [5].

3.6.6　確率変数 d と標準正規分布との比較

ここで，乱数長 n が 10^3, 10^4, 10^5, 10^6bit の場合で，確率変数：d が標準正規分布に従うかどうか，シミュレーション実験を実行した結果を以下に示す．なお，全ての乱数長の場合で乱数生成アルゴリズムには NIST のプログラムに付随している G-Using SHA-1 を使用し，標本数は 1000 とした．

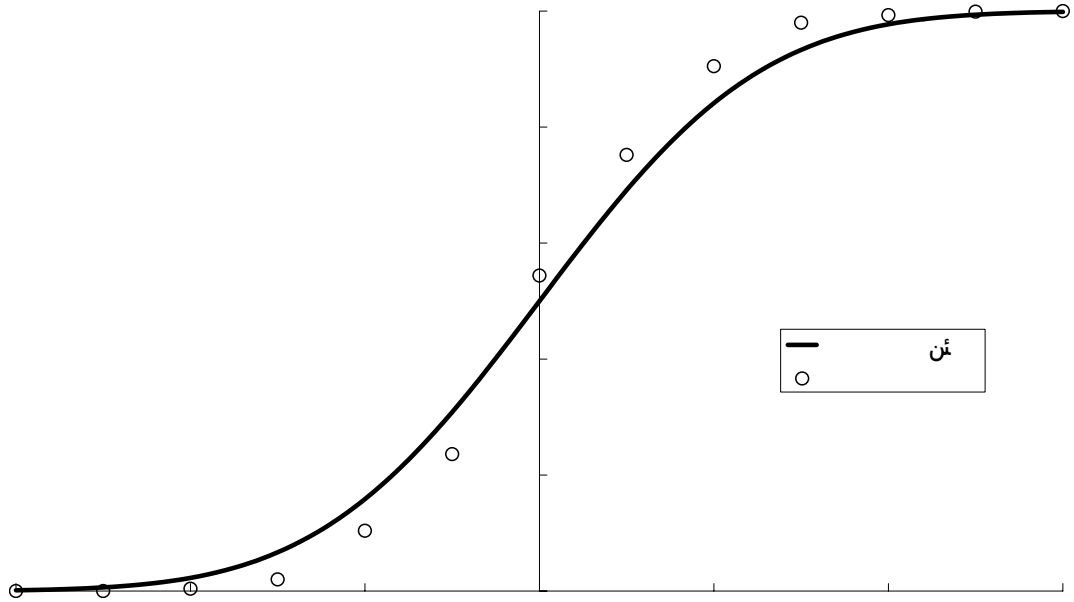


図 3.13: $n = 10^3$bit の場合の一例

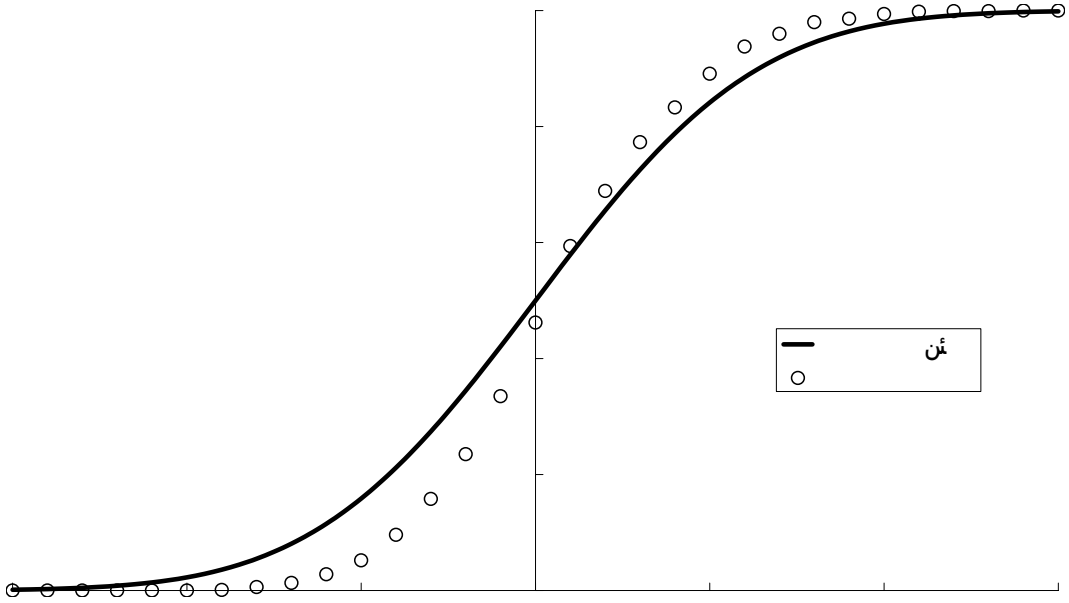


図 3.14: $n = 10^4$bit の場合の一例

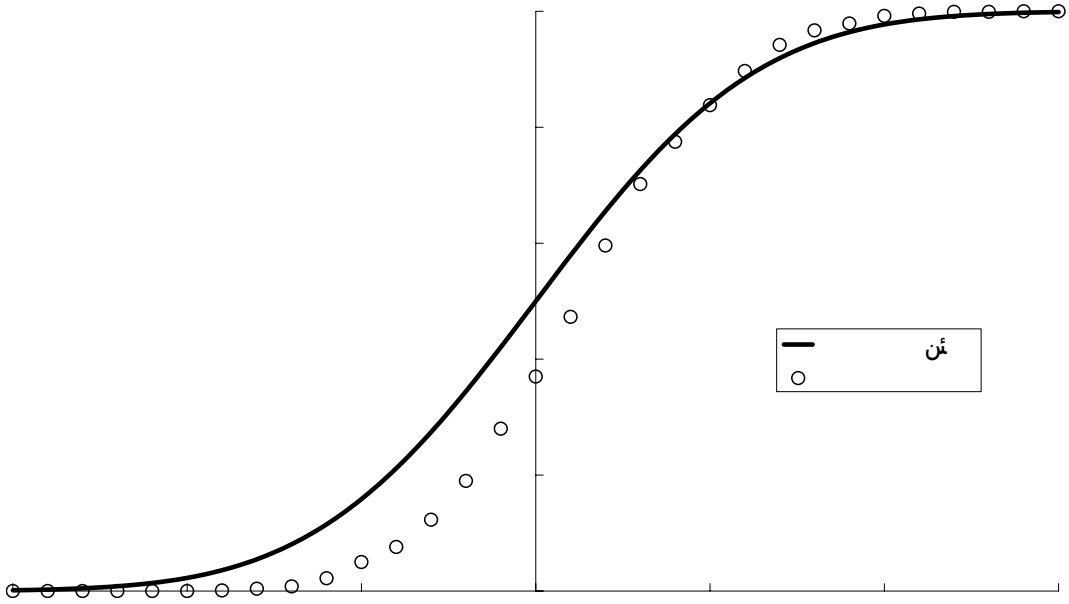


図 3.15: $n = 10^5$bit の場合の一例

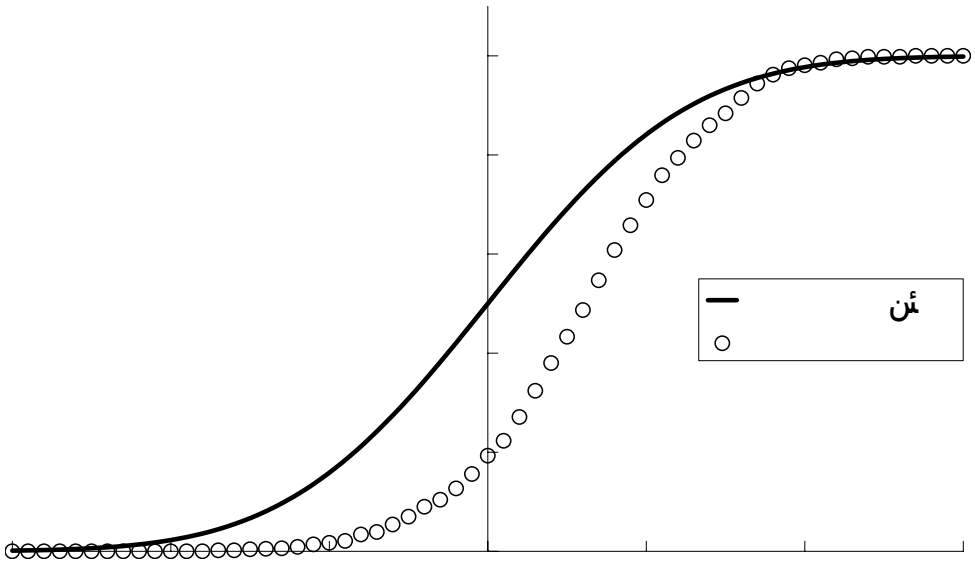


図 3.16: $n = 10^6$bit の場合の一例

3.6.7 考察

実験結果から，NIST の定義した確率変数 d では，理論分布に従っていないことがわかる．また，この現象は，乱数長が長くなるにつれて，より顕著に現れる結果となった．濱野らは，この現象の要因として，2 つの問題点を挙げている [3, 4]．

1 つめの問題点は閾値の近似による理論分布とのずれである．閾値 T を周波数成分 f_j の絶対値 $|f_j|$ の分布関数：$F(x) = 1 - \exp(-\frac{x^2}{n})$ から求めると，$T = \sqrt{-(\ln 0.05)n} = \sqrt{2.9957323n}$ となる．この閾値 T を NIST が $T = \sqrt{3n}$ と近似したために，図 3.13〜3.16 のように理論分布とずれが生じると濱野らは考察している．

2 つめの問題点は閾値補正後の確率変数 d の分散値減少である．1 つめの問題点で示した閾値の近似を補正した場合，確率変数 d は図 3.17 のようになる．ただし，図 3.17 は乱数長 $n = 10^6$ の場合で濱野らの追試を実行したものである．

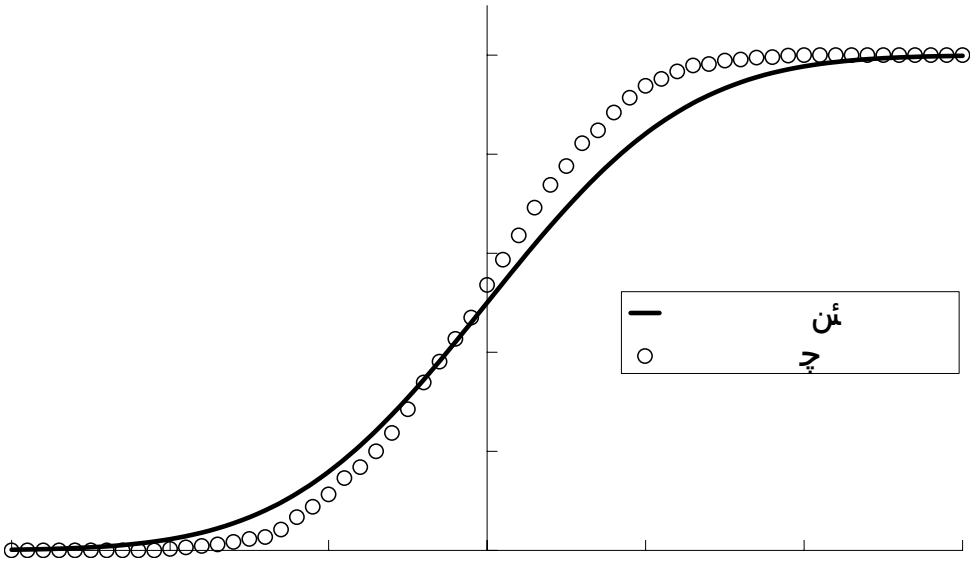


図 3.17: 閾値補正後の確率変数 d ($n = 10^6$bit の場合)

図 3.17 のように，閾値補正後も確率変数 d と理論分布には依然として，ずれがみられる．濱野らは，閾値補正後の確率変数 d の分布が平均 0，分散 $(0.7)^2$ の正規分布に近いことから，閾値を超えない周波数成分の個数の実測値 N_1 の分散値が 50 %になるのではないかと考察している．また，山本らは分散値減少の要因の一つとして，パーセバルの定理に由来する周波数成分のエネルギー制限であると推定している [5]．

3.7 重なりの無いテンプレート適合検定

3.7.1 目的

重なりの無いテンプレート適合検定は、乱数列を N 個のブロックに分割し、各ブロックごとに m ビットのテンプレートが適合する回数を調べ、N ブロックそれぞれの適合回数を χ^2 検定することにより適合回数の偏りを調べるものである。

3.7.2 記号の定義

ε ：0 と 1 からなる乱数列

n ：乱数列の長さ

m ：テンプレートの長さ

B ：非周期的なビット列からなるテンプレート

M ：ブロックの長さ

N ：ブロックの個数。プログラム中では、$N = 2^3 = 8$ が与えられている。

$\chi^2(obs)$ ：χ^2 分布統計量

3.7.3 推奨パラメータ

テンプレートの長さ m として 9 または 10 が推奨されており、乱数列の長さ n は $2^{20} = 1,048,576$ が指定されている。

3.7.4 検定方法

Step1 乱数列 ε を長さ M の N 個のブロックに分割する。

Step2 ブロック上に m ビットの窓を置き、ブロックの先頭から窓の中のビット列とテンプレート B を照合する。適合しなかった場合は、窓を 1 ビットだけずらし、適合した場合は m ビットずらす。$j(1 \leq j \leq N)$ 番目のブロックにおけるテンプレート B の適合回数を W_j とする。

Step3 各ブロックの適合回数 W_j は (3.27) 式で与えられる平均 μ、(3.28) 式で与えられる分散 σ^2 の正規分布に従うので、χ^2 分布統計量 $\chi^2(obs)$ を (3.29) 式により計算する。

$$\mu = \frac{M - m + 1}{2^m} \tag{3.27}$$

$$\sigma^2 = M\left(\frac{1}{2^m} - \frac{2m-1}{2^{2m}}\right) \tag{3.28}$$

$$\chi^2(obs) = \sum_{j=1}^{N} \frac{(W_j - \mu)^2}{\sigma^2} \tag{3.29}$$

Step4 $\chi^2(obs)$ は自由度 N の χ^2 分布に従うので、$\chi^2(obs)$ が棄却域に入るかどうかを (3.30) 式で計算される $p\text{-}value$ の値を用いて決定する。$p\text{-}value$ の値が 0.01 以上ならば入力乱数はランダムであるとする。

$$p\text{-}value = \mathbf{igamc}\left(\frac{N}{2}, \frac{\chi^2(obs)}{2}\right) \tag{3.30}$$

3.7.5 理論背景

実際のプログラムでは非周期的なビット列からなるテンプレートを用いて、窓を常に 1 ビットずつずらすことにより、3.7.4 検定方法 Step2 の処理を行っている。非周期的なビット列からなるテンプレートを用いることにより、適合した場合は m ビットずらすという処理をしなくても重なりなくテンプレートが適合する回数 W_j を求めることができる。ここで、非周期的なビット列からなるテンプレート $B = (\varepsilon_1^0, \varepsilon_2^0, \cdots, \varepsilon_m^0)$ とは、

$$B \neq \left\{j, 1 \leq j \leq m-1, \varepsilon_{j+k}^0 = \varepsilon_k^0, k = 1, 2, \cdots, m-j\right\} \tag{3.31}$$

である。

中心極限定理よりブロックの長さ M が十分大きければ、W_j は (3.27)、(3.28) 式で与えられる平均 μ、分散 σ^2 の正規分布に従う。従って、(3.29) 式で与えられる $\chi^2(obs)$ は自由度 N の χ^2 分布に従う。

3.7.6 統計量の分布

乱数長 n を $2^{20} = 1,048,576$ とし、テンプレートの長さ m が 9 と 10 の場合について、各ブロックにおけるテンプレート B の適合回数 W_j と (3.29) 式で与えられる $\chi^2(obs)$ の分布を調べた。なお、$m = 9$ のとき、テンプレート B として"000000001"を使用し、$m = 10$ のときは"0000000001"を使用した。また、乱数生成器として NIST のプログラムに付随している G Using SHA-1 を使用し、標本系列数を 1000 とした。

W_j の分布と理論分布の比較

W_j が (3.27)、(3.28) 式で示される平均 μ、分散 σ^2 の正規分布に従うかどうか、計算機実験を行った結果を図 3.18 に示す。

$\chi^2(obs)$ の分布と理論分布の比較

$\chi^2(obs)$ が自由度 $N = 8$ の χ^2 分布に従うかどうか、計算機実験を行った結果を図 3.19 に示す。

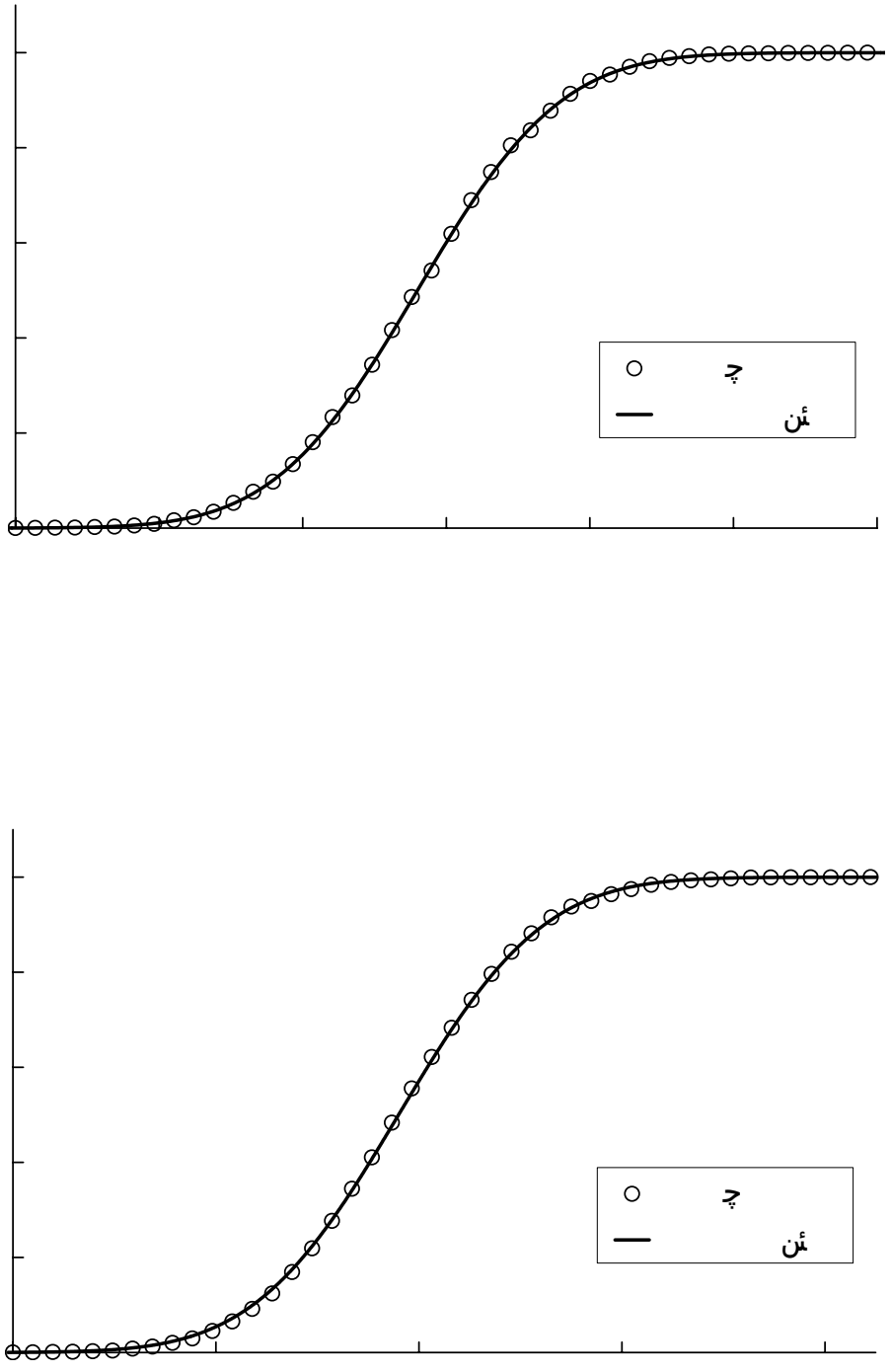


図 3.18: W_j の実測累積確率分布と理論正規分布の分布関数の比較

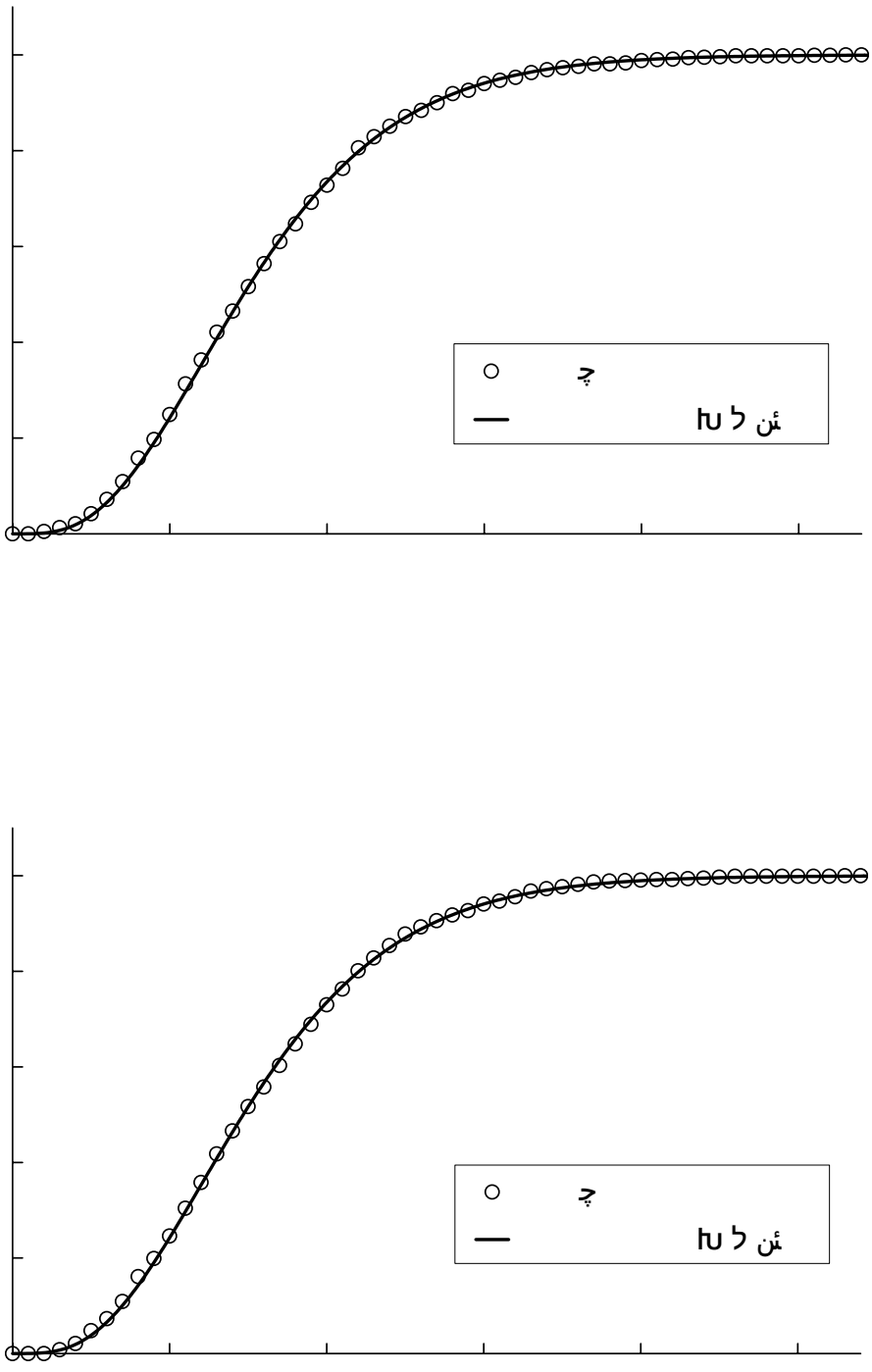


図 3.19: $\chi^2(obs)$ の実測累積確率分布と自由度８の χ^2 分布の分布関数の比較

3.7.7　考察

推奨パラメータの範囲で実験を行い、基になる理論分布とほぼ合致していることが確認された。

3.8 重なりのあるテンプレート適合検定

3.8.1 目的

重なりのあるテンプレート適合検定は、乱数列を N 個のブロックに分割し、各ブロックを m 文字のテンプレートが適合する回数により $K+1=6$ 個のクラスに割り当て、その度数を χ^2 検定することにより適合回数の偏りを調べるものである。

3.8.2 記号の定義

ε ：0 と 1 からなる乱数列

n ：乱数列の長さ

m ：テンプレートの長さ

B ：m ビット全てが 1 のテンプレート

K ：自由度。プログラム中では、$K=5$ が与えられている。

M ：ブロックの長さ。プログラム中では、$M=1032$ が与えられている。

N ：ブロックの個数

$\chi^2(obs)$ ：χ^2 分布統計量

3.8.3 推奨パラメータ

テンプレートの長さ m として 9 または 10 が推奨されており、乱数列の長さ n は 1,000,000 が指定されている。

3.8.4 検定方法

Step1 乱数列 ε を長さ M の N 個のブロックに分割する。

Step2 ブロック上に m ビットの窓を置き、ブロックの先頭から窓の中のビット列とテンプレート B を照合する。適合したしないにかかわらず、窓を 1 ビットずつずらしていき、各ブロックにおける適合回数を数える。$j(1 \leq j \leq N)$ 番目のブロックにおける適合回数を W_j とする。

Step3 適合回数 0 のクラスを x_0、1 のクラスを x_1、2 のクラスを x_2、3 のクラスを x_3、4 のクラスを x_4、5 以上のクラスを x_5 とし、Step2 で求めた W_j から各クラス $x_i(0 \leq i \leq 5)$ の度数 ν_i を求める。

Step4 入力系列が真の乱数列である場合の各ブロックの適合回数が、クラス x_i に該当する確率 π_i を (3.32) 式により計算する。

$$\left.\begin{aligned}
\pi_0 &= e^{-\eta} \\
\pi_1 &= \frac{\eta}{2}e^{-\eta} \\
\pi_2 &= \frac{\eta e^{-\eta}}{8}(\eta+2) \\
\pi_3 &= \frac{\eta e^{-\eta}}{8}\left(\frac{\eta^2}{6}+\eta+1\right) \\
\pi_4 &= \frac{\eta e^{-\eta}}{16}\left(\frac{\eta^3}{24}+\frac{\eta^2}{2}+\frac{3\eta}{2}+1\right) \\
\pi_5 &= 1-(\pi_0+\pi_1+\pi_2+\pi_3+\pi_4)
\end{aligned}\right\} \tag{3.32}$$

ただし、

$$\eta = \frac{\lambda}{2} \tag{3.33}$$

$$\lambda = \frac{M-m+1}{2^m} \tag{3.34}$$

Step5 χ^2 分布統計量 $\chi^2(obs)$ を (3.35) 式により計算する。

$$\chi^2(obs) = \sum_{i=0}^{5}\frac{(\nu_i - N\pi_i)^2}{N\pi_i} \tag{3.35}$$

Step6 $\chi^2(obs)$ は自由度 $K=5$ の χ^2 分布に従うので、$\chi^2(obs)$ が棄却域に入るかどうかを (3.36) 式で計算される $p\text{-}value$ の値を用いて決定する。$p\text{-}value$ の値が 0.01 以上ならば入力乱数はランダムであるとする。

$$p\text{-}value = \mathbf{igamc}\left(\frac{5}{2}, \frac{\chi^2(obs)}{2}\right) \tag{3.36}$$

3.8.5 理論背景

各ブロックにおけるテンプレートの適合回数 W_j は複合ポアソン分布に従う [11]。確率変数 U が複合ポアソン分布に従うとき、確率 $P(U=u)$ は

$$P(U=u) = \frac{e^{-\eta}}{2^u}\sum_{l=1}^{u}\left(\begin{array}{c} u-1 \\ l-1 \end{array}\right)\frac{\eta^l}{l!} \tag{3.37}$$

で与えられるので、$P(U=0)$,$P(U=1)$,$\cdots$,$P(U=4)$ は

$$\left.\begin{aligned}
P(U=0) &= e^{-\eta} \\
P(U=1) &= \frac{\eta}{2}e^{-\eta} \\
P(U=2) &= \frac{\eta e^{-\eta}}{8}(\eta+2) \\
P(U=3) &= \frac{\eta e^{-\eta}}{8}\left(\frac{\eta^2}{6}+\eta+1\right) \\
P(U=4) &= \frac{\eta e^{-\eta}}{16}\left(\frac{\eta^3}{24}+\frac{\eta^2}{2}+\frac{3\eta}{2}+1\right)
\end{aligned}\right\} \tag{3.38}$$

となる。従って、$\pi_0, \pi_1, \cdots, \pi_5$ は (3.32) 式である。本検定は、W_j を $K+1=6$ 個のクラスに分けているので、(3.35) 式の $\chi^2(obs)$ は自由度 $6-1=5$ の χ^2 分布に従う。

3.8.6 $\chi^2(obs)$ の分布と理論分布の比較

乱数長 n を $1,000,000$ とし、テンプレートの長さ m が 9 と 10 の場合について、π_i が (3.32) 式に従うかどうか、また、(3.35) 式で与えられる χ^2 分布統計量 $\chi^2(obs)$ が自由度 $K=5$ の χ^2 分布に従うかどうか、計算機実験を行った結果を図 3.20 と図 3.21 に示す。なお、乱数生成器として NIST のプログラムに付随している G Using SHA-1 を使用し、標本系列数を 1000 とした。

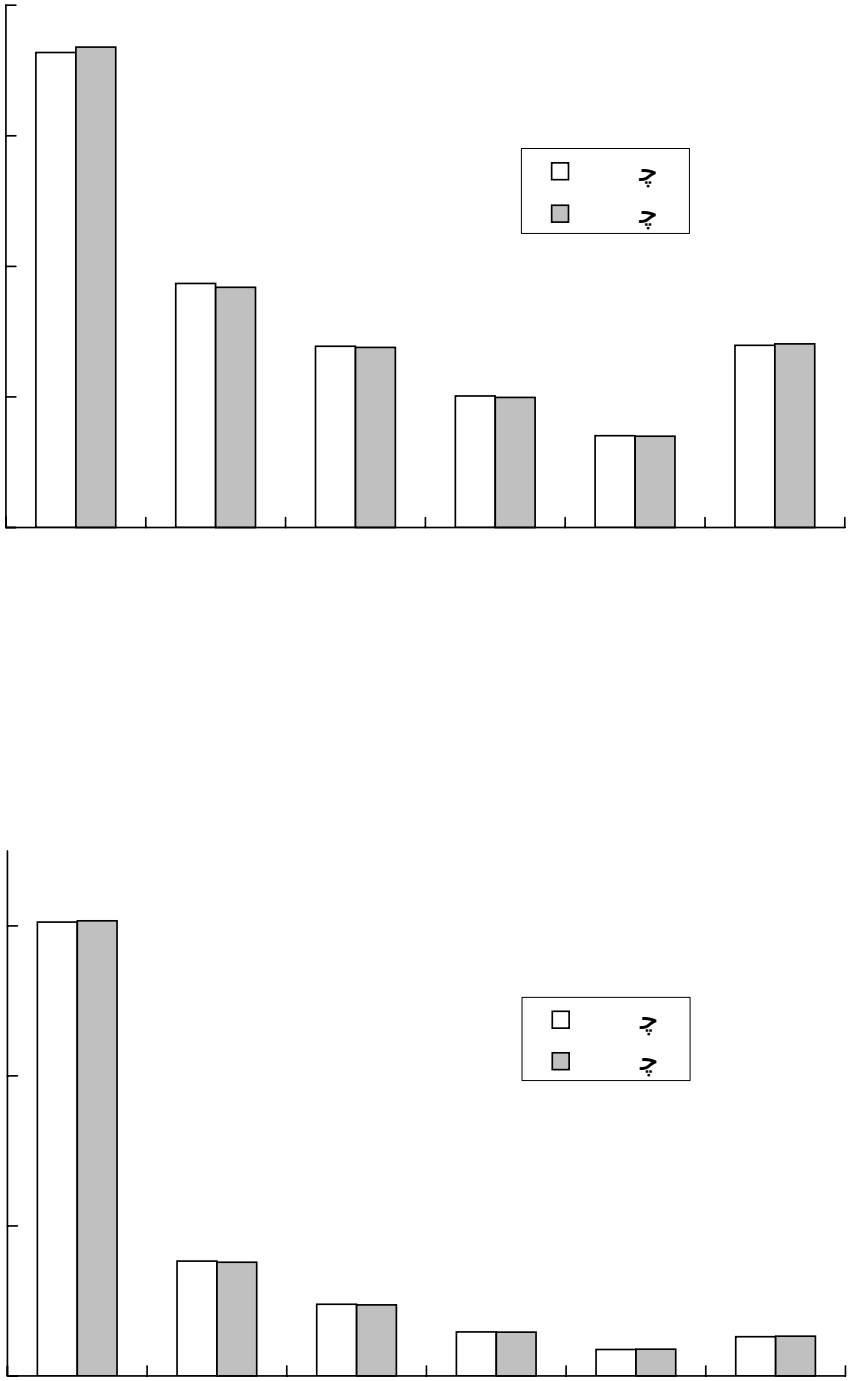


図 3.20: π_i の実測値と理論値の比較

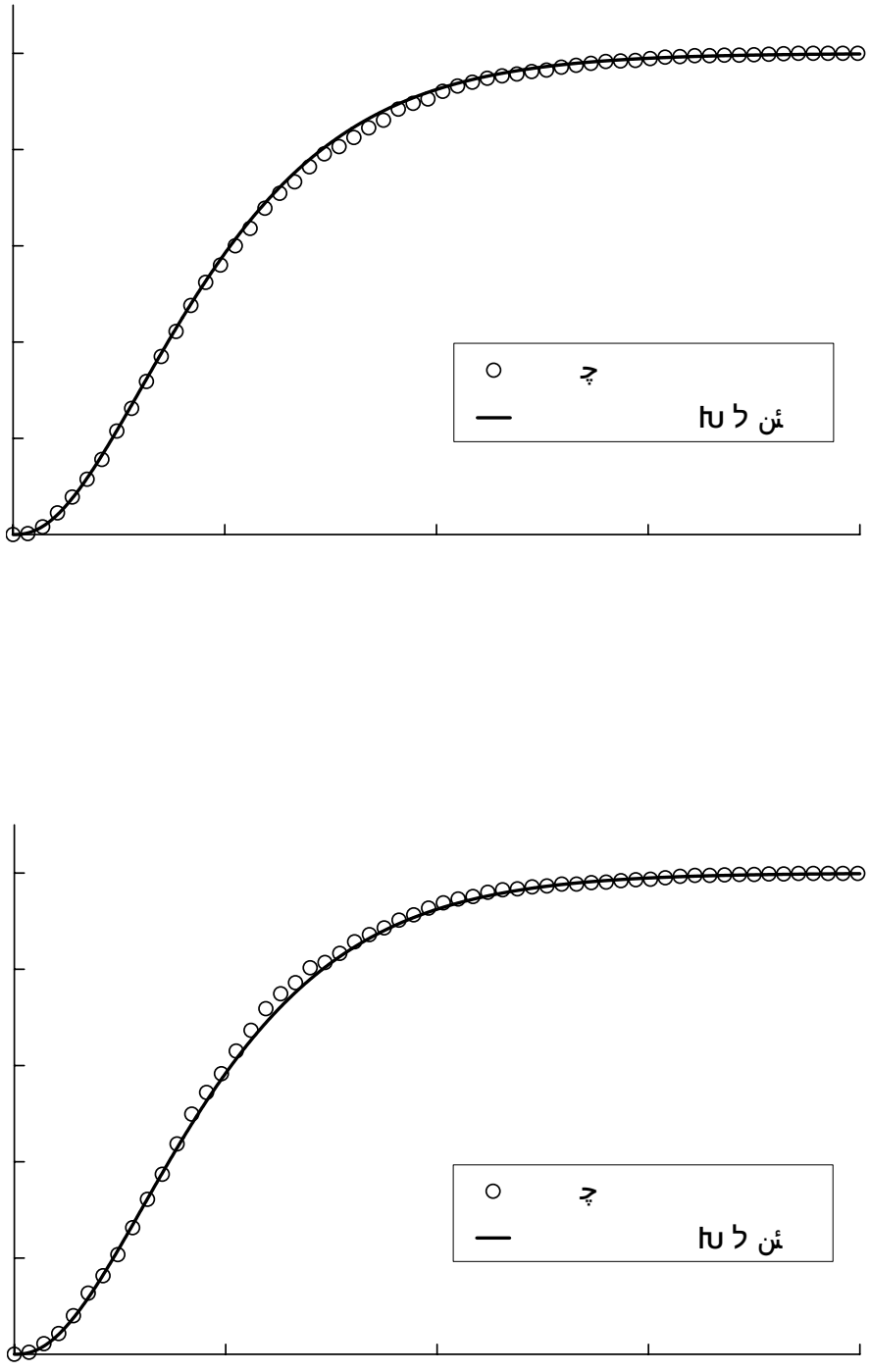


図 3.21: $\chi^2(obs)$ の実測累積確率分布と自由度 5 の χ^2 分布の分布関数の比較

3.8.7 考察

推奨パラメータの範囲で実験を行い、基になる理論分布とほぼ合致していることが確認された。

3.9 Maurer の「ユニバーサル統計量」検定

3.9.1 目的

Maurer の「ユニバーサル統計量」検定は、乱数列における長さ L ビットのパターンの間隔を調べることにより、乱数列の一様性を調べるものである。

3.9.2 記号の定義

ε ：0 と 1 からなる乱数列

n ：乱数列の長さ

L ：ブロックの長さ

Q ：初期セグメントのブロック数

K ：検定用セグメントのブロック数

f_n ：正規分布統計量

3.9.3 推奨パラメータ

ブロックの長さ L は $6 \leq L \leq 16$ の範囲にとる。また、初期セグメントのブロック数 Q は $Q = 10 \cdot 2^L$ で与えられ、乱数長 n は $6 \leq L \leq 15$ のとき、

$$(10 \cdot 2^L + 1000 \cdot 2^L)L \leq n < (10 \cdot 2^{L+1} + 1000 \cdot 2^{L+1})(L+1)$$

$L = 16$ のとき、

$$(10 \cdot 2^L + 1000 \cdot 2^L)L \leq n$$

を満たすようにとる。表 3.1 にこれらの関係をまとめておく。

3.9.4 検定方法

Step1 乱数列 ε を長さ L のブロックに分割する。先頭から Q ブロック分を初期セグメントとし、残り K ブロック分を検定用セグメントとする。ただし、$Q + K = \lfloor n/L \rfloor$ である。

Step2 T_j の初期値を 0 とし、「i 番目の L ビットブロックを 2 進数とみなしたときの値が $j(0 \leq j \leq 2^L - 1)$ のとき $T_j = i$ とする」という処理を初期セグメントの先頭ブロックから初期セグメントの最終ブロックまで順に行う $(1 \leq i \leq Q)$。

表 3.1: 推奨乱数長

L	n	$Q = 10 \cdot 2^L$
6	387,840〜904,959	640
7	904,960〜2,068,479	1280
8	2,068,480〜4,654,079	2560
9	4,654,080〜10,342,399	5120
10	10,342,400〜22,753,279	10240
11	22,753,280〜49,643,519	20480
12	49,643,520〜107,560,959	40960
13	107,560,960〜231,669,759	81920
14	231,669,760〜496,435,199	163840
15	496,435,200〜1,059,061,759	327680
16	1,059,061,760〜	655360

T_j は、j の 2 進数表現を L ビットのビット列とみなしたときに、そのビット列が初期セグメントで最後に現れた位置を表す。

Step3 sum の初期値を 0 として、「i 番目の L ビットブロックを 2 進数とみなしたときの値が j のとき、

$$sum = sum + \log_2(i - T_j) \tag{3.39}$$

とし、新たに $T_j = i$ とする」という処理を検定用セグメントの先頭ブロックから検定用セグメントの最終ブロックまで順に行う $(Q + 1 \leq i \leq Q + K)$。

注） (3.39) 式はプログラム的な書き方をしているが、数学的に記述すれば $sum_Q = 0$ として (3.39)′ 式である。

$$sum_i = sum_{i-1} + \log_2(i - T_j) \qquad (Q + 1 \leq i \leq Q + K) \tag{3.39}'$$

Step4

$$f_n = \frac{sum}{K} \tag{3.40}$$

を計算する。

Step5 f_n は表 3.2 にある平均 $\mu(L)$、(3.41),(3.42) 式により求められる標準偏差 σ の正規分布に従うので、f_n が棄却域に入るかどうかを (3.43) 式で計算される $p\text{-}value$ の値を用いて決定する。$p\text{-}value$ の値が 0.01 以上なら入力乱数はランダムであるとする。

表 3.2: 各 L に対する平均 $\mu(L)$ と $V(L)$

L	$\mu(L)$	$V(L)$
6	5.2177052	2.954
7	6.1962507	3.125
8	7.1836656	3.238
9	8.1764248	3.311
10	9.1723243	3.356
11	10.170032	3.384
12	11.168765	3.401
13	12.168070	3.410
14	13.167693	3.416
15	14.167488	3.419
16	15.167379	3.421

$$\sigma = c\sqrt{\frac{V(L)}{K}} \tag{3.41}$$

$$c = 0.7 - \frac{0.8}{L} + \left(4 + \frac{32}{L}\right)\frac{K^{-3/L}}{15} \tag{3.42}$$

$$p\text{-}value = \mathbf{erfc}\left(\left|\frac{f_n - \mu(L)}{\sqrt{2}\sigma}\right|\right) \tag{3.43}$$

3.9.5 理論背景

表 3.2 にある f_n の平均 $\mu(L)$ は次式により計算される [12]。

$$\mu(L) = 2^{-L}\sum_{i=1}^{\infty}(1 - 2^{-L})^{i-1}\log_2 i \tag{3.44}$$

また、f_n の標準偏差 σ は経験的に (3.41) 式で与えられるが、Coron と Naccache によって c の最新の近似式が次のように示されている [13]。

$$c = 0.7 - \frac{0.8}{L} + \left(1.6 + \frac{12.8}{L}\right)K^{-4/L} \tag{3.45}$$

なお、本検定のプログラム中では、(3.45) 式ではなく (3.42) 式が用いられている。

3.9.6 f_n の分布と理論分布の比較

ブロックの長さ L が 6 と 7 の場合について、(3.40) 式の統計量 f_n が表 3.2 にある平均 $\mu(L)$、(3.41),(3.42) 式で与えられる標準偏差 σ の正規分布に従うかどうか、計算機実験を行った結果を図 3.22 に示す。また、L が 6 の場合については、f_n を (3.45) 式を用いて得られる理論分布とも比較した。その結果を図 3.23 に示す。表 3.3 は (3.42) 式を用いた σ と (3.45) 式を用いた σ の比較である。なお、乱数生成器として NIST のプログラムに付随している G Using SHA-1 を使用し、乱数長 n は $L = 6$ のとき 500,000、$L = 7$ のとき 1,000,000 として、標本系列数は 1000 とした。

表 3.3: 標準偏差 σ の比較（$L = 6$）

	(3.42) 式	(3.45) 式
標準偏差 σ	0.003399802572	0.003398625966

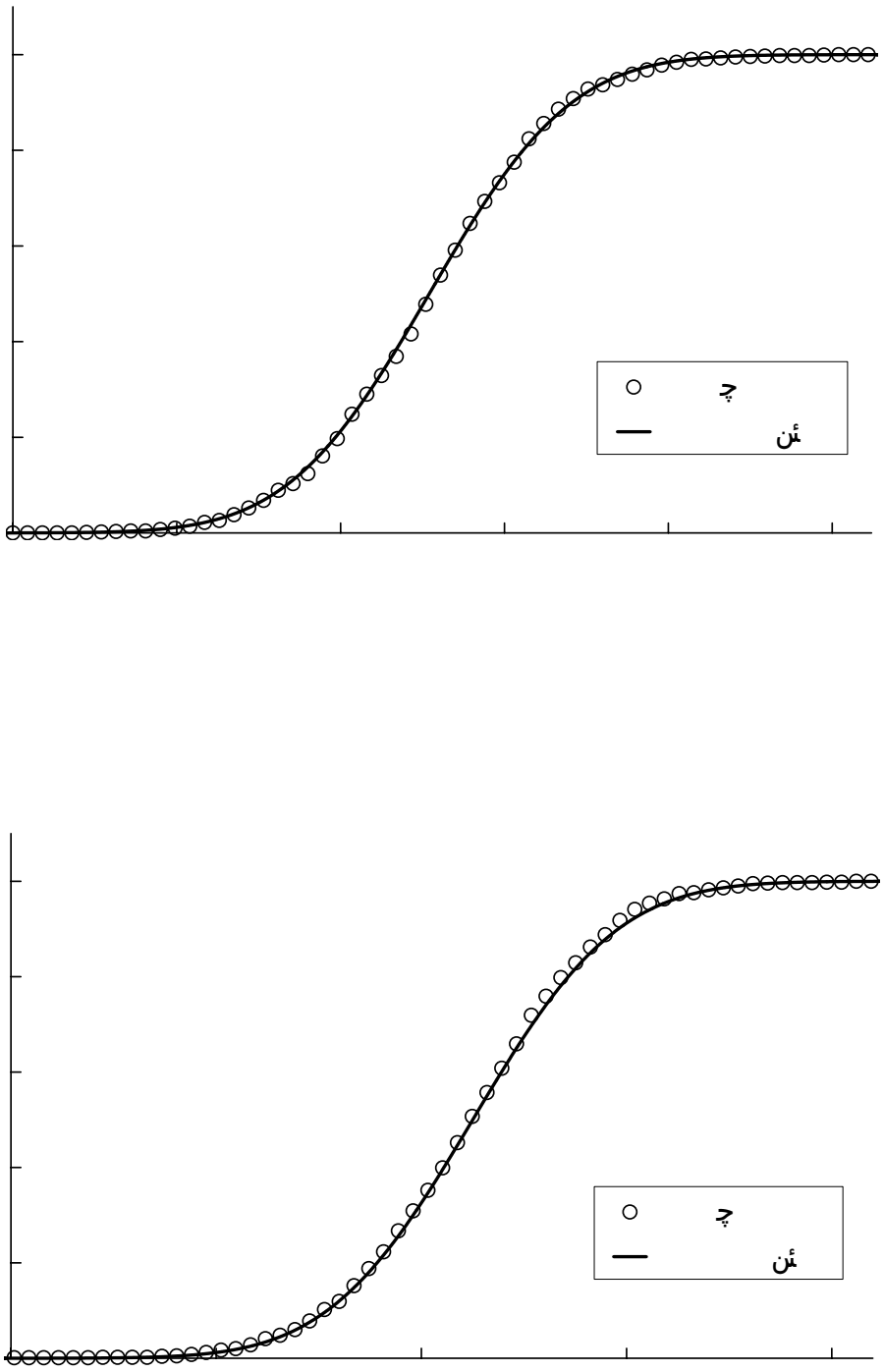


図 3.22: f_n の実測累積確率分布と理論正規分布の分布関数の比較

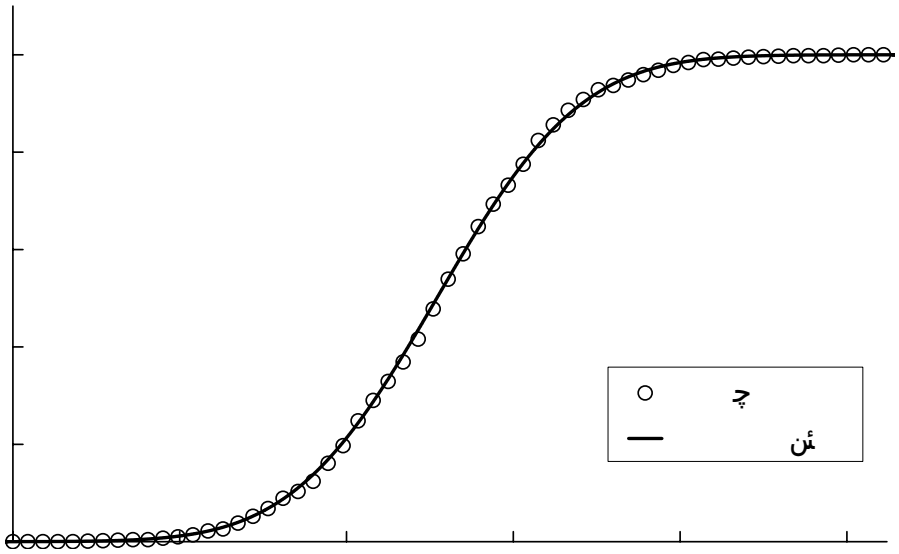


図 3.23: (3.45) 式を用いて得られる理論分布との比較 (L=6)

3.9.7 考察

推奨パラメータの範囲で実験を行い、基になる理論分布とほぼ合致していることが確認された。また、(3.42) 式と (3.45) 式どちらを用いても、理論分布に大差は見られなかった。

3.10 Lempel-Ziv 圧縮検定

3.10.1 目的

Lempel-Ziv 圧縮検定は 0 と 1 からなる乱数列に Lempel-Ziv 圧縮アルゴリズムを適用し，増分分解された部分列数を調べ，乱数列の一様性・圧縮不可能性を調べるものである．

3.10.2 記号の定義

ε ：0 と 1 からなる乱数列

n ：乱数列の長さ

$W(n)$ ：乱数列を部分列に区切った時の部分列の総数

3.10.3 推奨パラメータ

乱数長 n に関して，NIST は 10^6bit 以上を推奨している．

3.10.4 検定方法

Step1　0 と 1 からなる乱数長 n の乱数列 $\varepsilon = \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n (\varepsilon_i \in \{0,1\}, i = 1, 2, \cdots, n)$ を増分分解法により部分列に分解し，このときの部分列の個数を $W(n)$ とする．

Step2　$W(n)$ を正規化した確率変数：$\frac{W(n)-E[W(n)]}{\sigma[W(n)]}$ が標準正規分布に従うと仮定し，確率変数が標準正規分布の棄却域（危険率 0.01）に入るかどうかを，$P-value$ という以下の式：

$$P - value = \frac{1}{2} erfc\left(\frac{E[W(n)] - W(n)}{\sqrt{2\sigma^2}}\right) \tag{3.46}$$

で計算される値を用いて決定する．$P - value$ の値が 0.01 以上ならば入力乱数はランダムであるとする．

ただし，$W(n)$ の平均値 $E[W(n)]$，分散 $\sigma^2[W(n)]$ について，NIST は次式を示している．

$$E[W(n)] = \lim_{n\to\infty} \frac{n}{\log_2 n} \tag{3.47}$$

$$\sigma^2[W(n)] \approx \frac{n[C + \delta(\log_2 n)]}{\log_2^3 n} \qquad \left(C = 0.26600, |\delta(\cdot)| < 10^{-6}\right) \tag{3.48}$$

3.10.5 理論背景

乱数長$n = 10^6$bit の時，$W(n)$ の平均値 $E[W(n)]$，分散 $\sigma^2[W(n)]$ は (3.47)，(3.48) 式より，$E[W(n)] = 50171.66594$，　$\sigma^2[W(n)] = 33.59365$ となることが知られている [6]．しかし，NIST は付属のソースプログラムにおいて，乱数生成器 G-Using SHA-1 および Blum-Blum-Shub の発生乱数を元に，$E[W(n)] = 69588.20190000$，　$\sigma^2[W(n)] = 73.23726011$ と実験的に理論値を定めている．

3.10.6 $W(n)$ の分布と理論分布との比較

ここで，乱数長 n が 10^6bit の場合で，$W(n)$ が理論分布に従うかどうか，シミュレーション実験を実行した結果を以下に示す．なお，乱数生成アルゴリズムには NIST のプログラムに付随している G-Using SHA-1 を使用し，標本数は 1000 とした．また，理論分布は NIST のソースプログラムおよびドキュメント＜(3.47), (3.48) 式＞の両方の場合を示した．

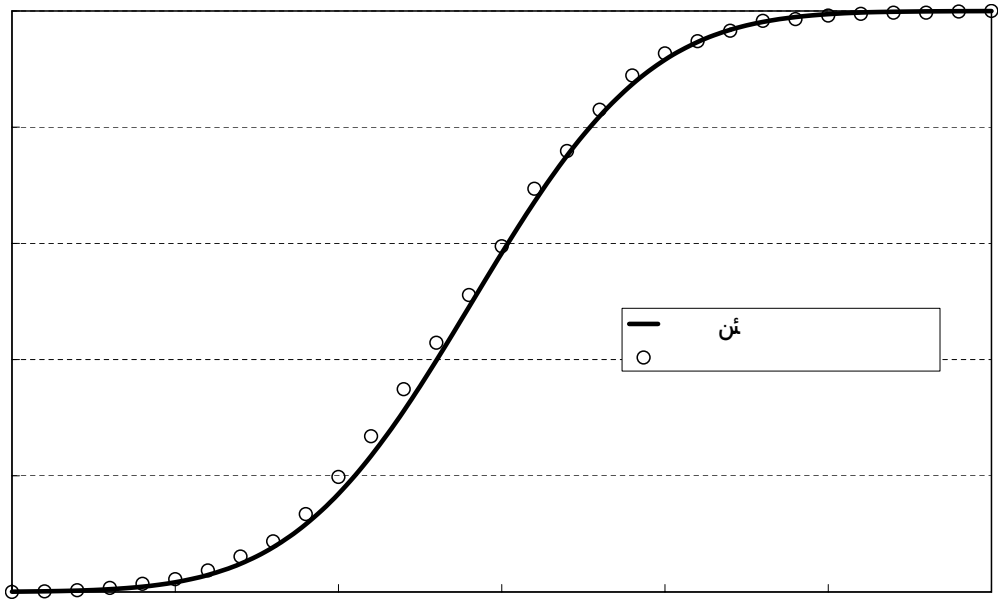


図 3.24: $n = 10^6$bit の時の W(n) の累積分布の一例および NIST のソースプログラムに基づく理論分布

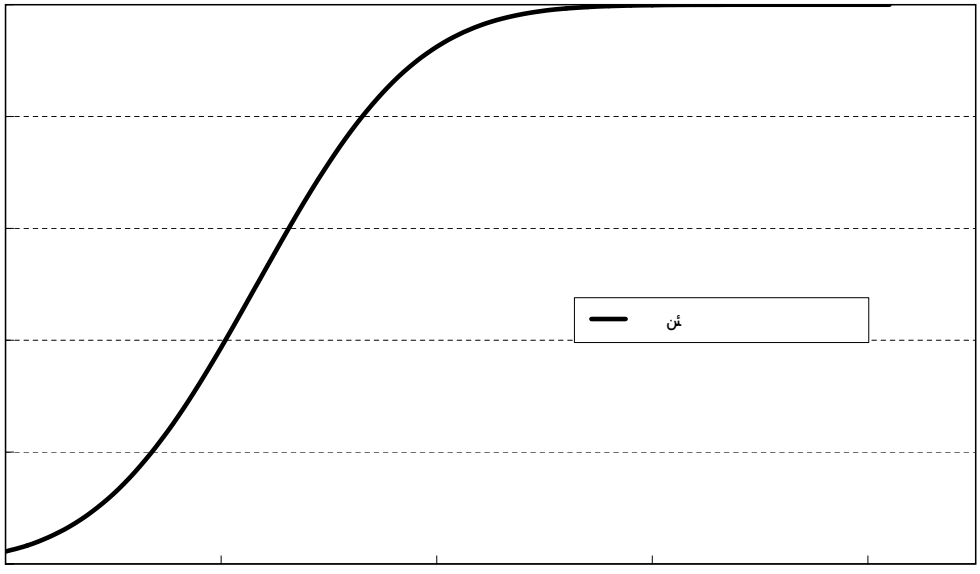


図 3.25: $n = 10^6$bit の時の NIST のドキュメントに基づく理論分布

3.10.7 考察

図 3.24，3.25 より，$W(n)$ の分布は NIST のドキュメントに基づく理論分布と大きくずれているのがわかる．よって，NIST が示す理論式を本検定法の理論的根拠とするには，乱数長 $n = 10^6$bit において，誤差が大きすぎるといえる．一方，NIST のソースプログラムに基づく理論分布と比較すると，ほぼ合致していることが確認できる．しかし，この理論分布は実験的に定められたものであり，理論に基づくものでないことに注意が必要である．

3.11 線形複雑度検定

3.11.1 目的

線形複雑度検定とは乱数列を長さ M ビットのブロックに分割し、ブロックごとの線形複雑度を求めることにより乱数列の周期性を調べるものである。

3.11.2 記号の定義

n :乱数列の長さ
ε :“ 0 ”と“ 1 ”からなる乱数列（ε=ε_1,ε_2,$\cdots$,ε_n）
M :ブロックの長さ
K :自由度（プログラム中で $K = 6$ が与えられている。）
$\chi^2(\mathrm{obs})$:カイ二乗統計量

3.11.3 推奨パラメータ

NIST は乱数長 n を 10^6bit 以上, ブロックの長さ M を 500≤M≤5000 となるように推奨している。

3.11.4 検定方法

Step1 入力した乱数列 n を長さ M のブロックに分割する。$N = \lfloor \frac{n}{M} \rfloor$

Step2 Berlekamp-Massey アルゴリズムを使って、N 個のブロックそれぞれの線形複雑度 L_i を求める。L_i とは i 番目のブロックの中で、全てのビットを生み出す LFSR の最も短い長さである。つまり、ビットの組合せによって L_i ビットの数列で、次のビット（L_i+1）が作られる。

Step3 真の乱数列である場合の線形複雑度の平均の理論値 μ を次式で計算する。

$$\mu = \frac{M}{2} + \frac{9 + (-1)^{M+1}}{36} - \frac{\frac{M}{3} + \frac{2}{9}}{2^M} \tag{3.49}$$

Step4 各ブロック（$1 \leq i \leq N$）について T_i の値を計算する。

$$T_i = (-1)^M (L_i - \mu) + \frac{2}{9} \tag{3.50}$$

Step5 T_i の値によって、表 1 に従って ν_0〜ν_6 に振り分けその個数を求める。

ν_i	T_i の値
ν_0	$T_i \leq -2.5$
ν_1	$-2.5 < T_i \leq -1.5$
ν_2	$-1.5 < T_i \leq -0.5$
ν_3	$-0.5 < T_i \leq 0.5$
ν_4	$0.5 < T_i \leq 1.5$
ν_5	$1.5 < T_i \leq 2.5$
ν_6	$T_i > 2.5$

表１：T_i に対する度数 ν_i

Step6　統計量 $\chi^2(obs)$ を次の計算式で計算する。

$$\chi^2(obs) = \sum_{i=0}^{K} \frac{(\nu_i - N\pi_i)^2}{N\pi_i} \tag{3.51}$$

ここで、π_i の値は π_0=0.01047 ， π_1=0.03125 ， π_2=0.125 ， π_3=0.5 ， π_4=0.25 ， π_5=0.0625 , π_6=0.02078 である。

Step7　確率変数 $\chi^2(obs)$ がカイ２乗分布に従うと仮定し、確率変数 $\chi^2(obs)$ の値がカイ２乗分布の棄却域（危険率 0.01）に入るかどうかを、$P-value$ という以下の式：

$$P - value = igamc\{\frac{K}{2}, \frac{\chi^2(obs)}{2}\} \tag{3.52}$$

で計算される値を用いて決定する。$P-value$ の値が 0.01 以上ならば入力乱数はランダムであるとする。

3.11.5　理論背景

長さ n の 2 元系列 s^n が真にランダムな場合、線形複雑度 $L(s^n) = L_n$ の、平均値 $n = EL(s^n)$、分散を与える式が存在する [18]。しかし、確率変数 $(L_n - \mu_n)/\delta_n$ は、標準正規分布に従うわけではなく、n の偶数または奇数により、2 つの幾何分布の合成で得られる離散的分布になる（それらの 1 つは負の値のみをとる）。厳密に言えば、漸近分布は存在しない。n が偶数の場合と、奇数の場合で、別の極限分布として処理する必要がある。

こうした事実により、以下の統計量の系列を採用する。

$$T_n = (-1)^n[L_n - \xi_n] + \frac{2}{9} \tag{3.53}$$

ここで

$$\xi = \frac{n}{2} + \frac{4 + r_n}{18} \tag{3.54}$$

統計量は、整数値のみをとり、ランダム変数 T の分布に収束する。この極限分布は、右にゆがみを持つ以下の分布である。

$$P(T=0)=\frac{1}{2} \tag{3.55}$$

$$P(T=k)=\frac{1}{2^{2k}} \qquad (k=1,2,\cdots) \tag{3.56}$$

$$P(T=k)=\frac{1}{2^{2|k|+1}} \qquad (k=-1,-2,\cdots) \tag{3.57}$$

(3.56) 式より、

$$P(T\geq k>0)=\frac{1}{3\times 2^{2k-2}} \tag{3.58}$$

$k\leq 0$ の場合、(3.57) 式より、次式となる。

$$P(T\leq k)=\frac{1}{3\times 2^{2|k|-1}} \tag{3.59}$$

観測値 T_{obs} に対応する P-value は以下で評価される。$k=[|T_{obs}|]+1$ とし、P-value は

$$\frac{1}{3\times 2^{2k-1}}+\frac{1}{3\times 2^{2k-2}}=\frac{1}{2^{2k-1}} \tag{3.60}$$

この分布は離散的であること、および、P-value の一様性を得るのは不可能であることを考慮し、他のほかの検定で使用されたものと同じ手法を使用する。

すなわち、$n=MN$ として、長さ n の文字列を、それぞれ長さ M の N 個のブロックに分割する。(3.53) 式の線形複雑度に基づく検定では、各ブロックの T_M を評価し、(M に応じた) $K+1$ 個のクラスに分ける。N 個のブロックの T_M を $K+1$ 個のクラスに分け、各クラスの頻度を $\nu_0,\nu_1,\cdots,\nu_K$ (ただし,$\nu_0+\nu_1+\cdots+\nu_K=N$) とする。

これらのクラスの理論的確率 $\pi_0,\pi_1,\cdots,\pi_k$ は、(3.56) 式および (3.57) 式から決定される。その為、極限分布の (3.56) 式および (3.57) 式が適切な近似を与えるよう、M は十分大きくなければならない。M は 500 を超える必要があり、$500\leq M\leq 5000$ となるよう M を選択することが望ましい。

各クラスの頻度は χ^2 統計量としてまとめる。

ランダム性の仮説のもとで、この統計量は、自由度 K の近似的カイ二乗分布となる。結果の P-value は、

$$\frac{1}{\Gamma(\frac{K}{2})\cdot 2^{\frac{K}{2}}}\int_{\chi^2(obs)}^{\infty}e^{-\frac{u}{2}}\cdot u^{\frac{K}{2}-1}du=igamc\left(\frac{K}{2},\frac{\chi^2(obs)}{2}\right) \tag{3.61}$$

χ^2 近似が成り立つ為の条件は、控えめに見積もって、

$$N\min\pi_i\geq 5 \qquad (i=0,1,\cdots,K) \tag{3.62}$$

十分な大きさの M と N の値に対して、以下のクラス分け $(K = 6)$ が適切である。$(T \leq -2.5)$, $(-2.5 < T \leq -1.5)$, $(-1.5 < T \leq -0.5)$, $(-0.5 < T \leq 0.5)$, $(0.5 < T \leq 1.5)$, $(1.5 < T \leq 2.5)$ および $(T > 2.5)$ である。

これらの各クラスの確率は、$\pi_0 = 0.0147$、$\pi_1 = 0.03124$、$\pi_2 = 0.12500$、$\pi_3 = 0.50000$、$\pi_5 = 0.6250$、$\pi_6 = 0.020833$ である。これらの確率は、正規近似から得られた数値 0.0041、0.0432、0.1944、0.2863、0.0135 とは大きく異なっている。

3.11.6 確率変数 $\chi^2(obs)$ とカイ２乗分布との比較

本章では乱数長 n を 10^6bit,M を 500,1000 の場合で、確率変数 $\chi^2(obs)$ がカイ２乗分布に従うかどうか実験を行った結果を以下に示す。また、全ての測定は乱数生成アルゴリズムとして NIST のプログラムに付随している G-Using SHA-1 を使用し、標本数を 1000 とした。

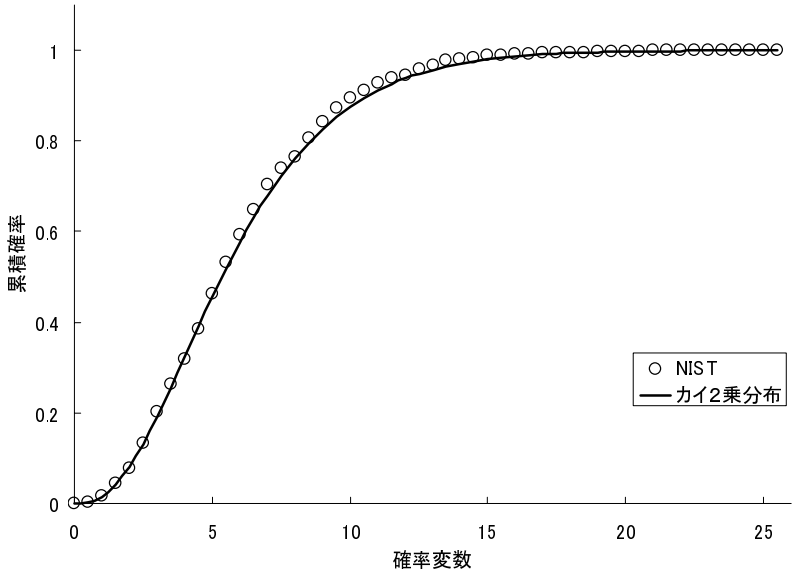


図 3.26: M=500

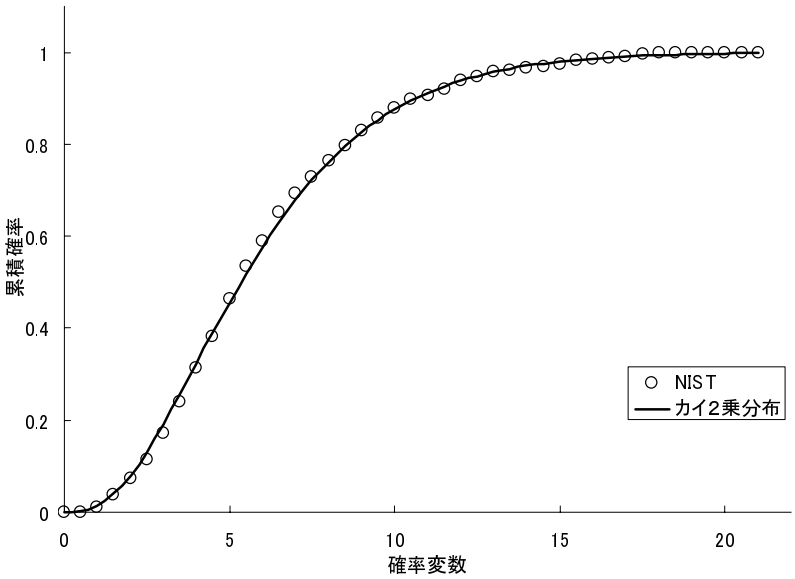


図 3.27: M=1000

3.11.7　考察

推奨パラメータの範囲で実験を行い、基になる理論分布とほぼ合致していることが確認された。

3.12 系列頻度検定

3.12.1 目的

系列頻度検定は取り得る全ての m ビットのパターンの発生頻度に着目し、全ての m ビットパターンが均等に現れているかを検定する。

3.12.2 記号の定義

m:ブロックのビット長
n:乱数の長さ
ε:0 と 1 からなる乱数列 $\varepsilon = (\varepsilon_1, \varepsilon_2, \cdots \varepsilon_n)$
$\bigtriangledown\psi_m^2$ および $\bigtriangledown^2\psi_m^2$:観測された m ビットパターンの頻度が理想的なものと、どれほど合致しているかを表す評価量

3.12.3 推奨パラメータ

NIST は m と n を $m < \lfloor \log_2 n \rfloor - 2$ となるように選ぶとしている。

3.12.4 検定方法

Step1

ε の最上位ビットから (m-1) ビットを最下位ビットの後ろに付け加え ε' を作る。

Step2

取りうる全ての m ビットブロック列 $i_1, i_2, \cdots i_m$ の出現頻度を求め、それを $\nu_{i_1 \cdots i_m}$ と定義する。
(m-1) ビットのブロック列、(m-2) ビットのブロック列についても出現頻度を求め、それぞれ $\nu_{i_1 \cdots i_m - 1}$,$\nu_{i_1 \cdots i_m - 2}$ とする。

Step3

以下の計算をする。

$$\psi_m^2 = \frac{2^m}{n} \sum_{i_1, i_2, \cdots i_m} (\nu_{i_1 \cdots i_m} - \frac{n}{2^m})^2 = \frac{2^m}{n} \sum_{i_1, i_2, \cdots i_m} \nu_{i_1 \cdots i_m}^2 - n \qquad (3.63)$$

$$\psi_{m-1}^2 = \frac{2^{m-1}}{n} \sum_{i_1,i_2,\cdots i_{m-1}} (\nu_{i_1\cdots i_{m-1}} - \frac{n}{2^{m-1}})^2 = \frac{2^{m-1}}{n} \sum_{i_1,i_2,\cdots i_{m-1}} \nu_{i_1\cdots i_{m-1}}^2 - n \tag{3.64}$$

$$\psi_{m-2}^2 = \frac{2^{m-2}}{n} \sum_{i_1,i_2,\cdots i_{m-2}} (\nu_{i_1\cdots i_{m-2}} - \frac{n}{2^{m-2}})^2 = \frac{2^{m-2}}{n} \sum_{i_1,i_2,\cdots i_{m-2}} \nu_{i_1\cdots i_{m-2}}^2 - n \tag{3.65}$$

Step4

以下の計算を行う。

$$\bigtriangledown\psi_m^2 = \psi_m^2 - \psi_{m-1}^2 \tag{3.66}$$

$$\bigtriangledown^2\psi_m^2 = \psi_m^2 - 2\psi_{m-1}^2 + \psi_{m-2}^2 \tag{3.67}$$

Step5

統計量 $\bigtriangledown\psi_m^2$ および $\bigtriangledown^2\psi_m^2$ が χ^2 分布に従うと仮定し、統計量 $\bigtriangledown\psi_m^2$,$\bigtriangledown^2\psi_m^2$ の値が χ^2 分布の棄却域 (危険率 0.01) に入るかどうかを、P-value という以下の式

$$P - value1 = \mathbf{igamc}(2^{m-2}, \bigtriangledown\psi_m^2/2) \tag{3.68}$$

$$P - value2 = \mathbf{igamc}(2^{m-3}, \bigtriangledown^2\psi_m^2/2) \tag{3.69}$$

で計算される値を用いて決定する。P-value の値が 0.01 以上ならば入力乱数はランダムであるとする。

3.12.5 理論背景

Serial Test は与えられた長さのパターンの出現頻度の均一性に着目する。与えられた乱数から作った $\varepsilon' = (\varepsilon_1, \varepsilon_2, \cdots \varepsilon_n, \varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{m-1})$ において $i_1, i_2, \cdots, i_m$ という長さmの 0 と 1 からなるパターンを全通り、つまり 2^m 通り考え、その $(i_1, i_2, \cdots, i_m)$ というパターンの出現頻度として $\nu_{i_1,i_2,\cdots,i_m}$ というものを定義する。

ここで、式 (3.63) で表される ψ_m^2 というものを考えるとこれは χ^2 型の統計量である。しかし出現頻度 $\nu_{i_1,i_2,\cdots,i_m}$ はそれぞれが独立でないため χ^2 分布であると仮定すると誤りとなる。そこで χ^2 分布に従うような統計量として式 (3.66),(3.67) のようなものを考えると，$\bigtriangledown\psi_m^2$ は自由度 2^{m-1} の χ^2 分布に、$\bigtriangledown^2\psi_m^2$ が自由度 2^{m-2} の χ^2 分布に従う [16] [17] [18]。
$\bigtriangledown\psi_m^2$ が χ^2 分布に従うことは Good によって示されている [19]。

3.12.6 統計量 $\bigtriangledown\psi_m^2$,$\bigtriangledown^2\psi_m^2$ と χ^2 分布との比較

全ての測定は乱数生成アルゴリズムとして NIST のプログラムに付随している G-Using SHA-1 を用い、乱数長を 1,000,000、標本数を 1000 として行った。NIST

は $\bigtriangledown\psi_m^2$ が 2^{m-1} の、$\bigtriangledown^2\psi_m^2$ が 2^{m-2} の自由度の χ^2 分布に従うとしている。実験値と理論値の比較を、$m = 2, 3$ 及び 16 について以下の図に示す。

m=2 の場合

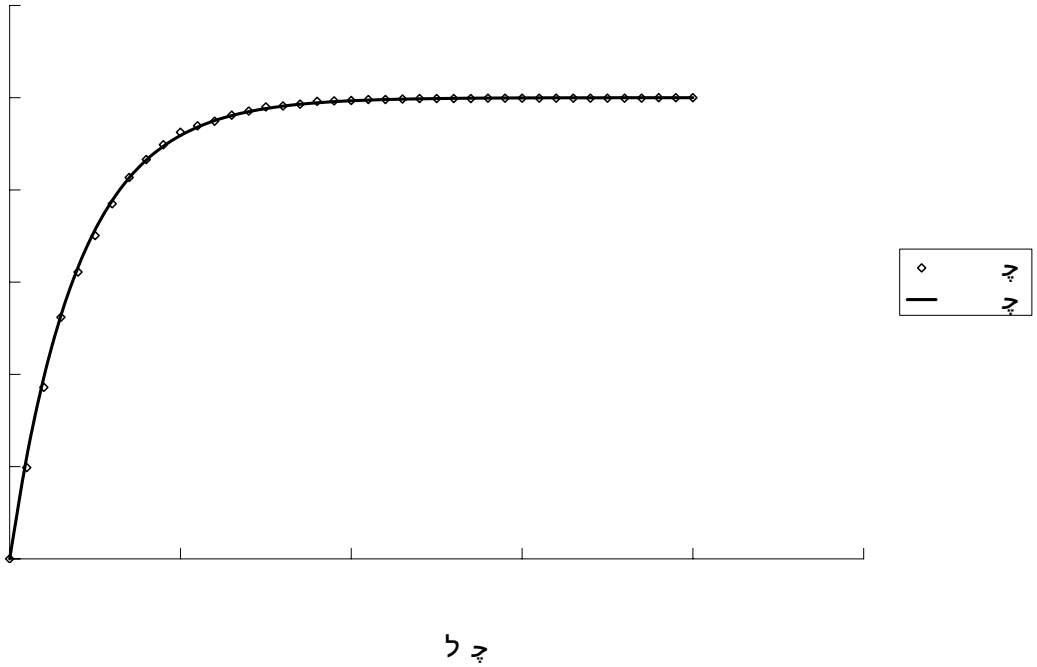


図 1:$\bigtriangledown\psi_m^2$

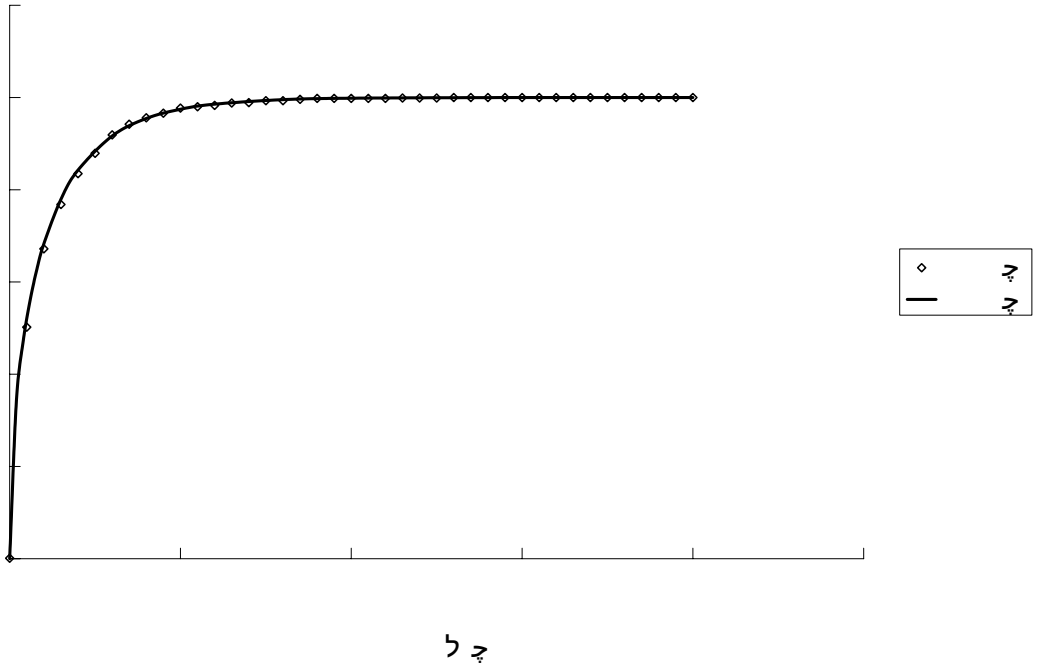


図 2:$\bigtriangledown^2\psi_m^2$

m=3 の場合

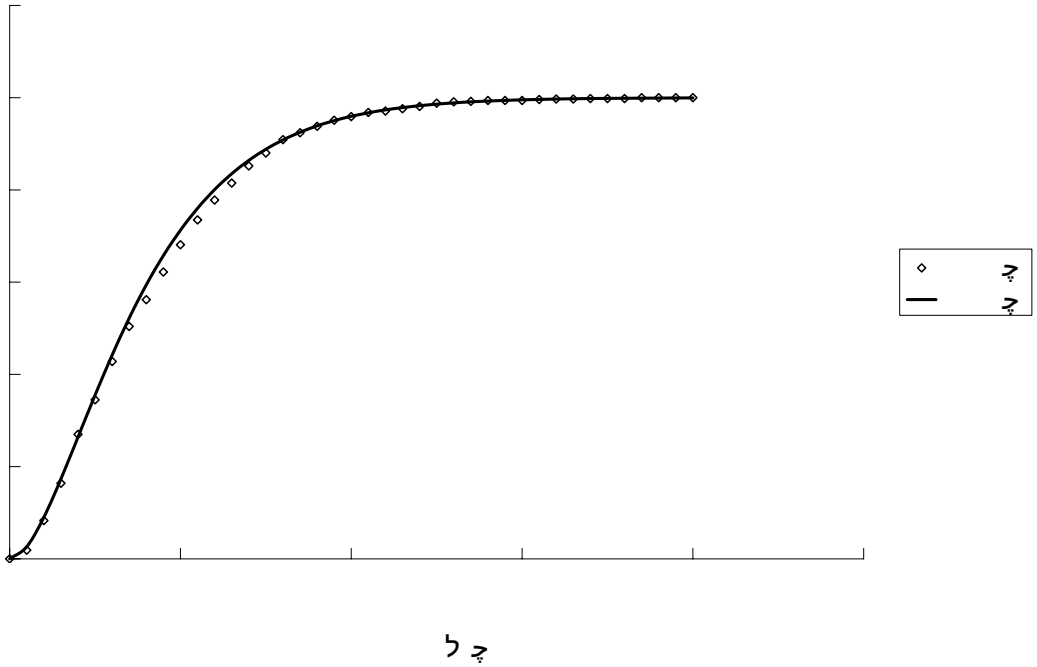


図 3:$\bigtriangledown\psi_m^2$

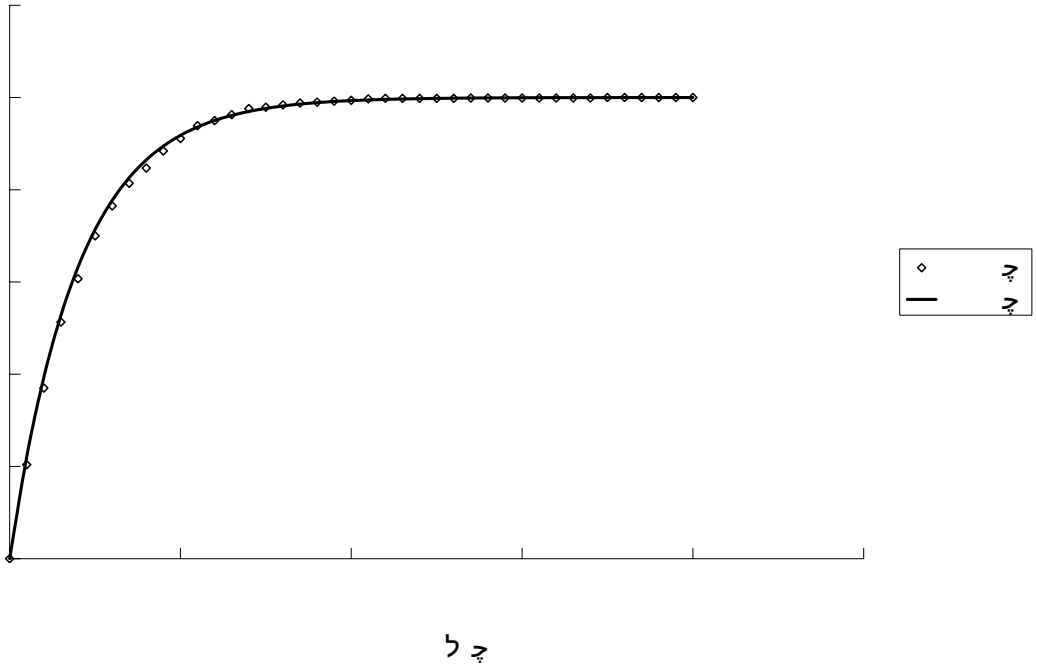


図 4:$\bigtriangledown^2\psi_m^2$

m=16 の場合
自由度 k が、k>30 の時、$\sqrt{2X} - \sqrt{2k-1}$ が正規分布に近似できるため，以下に図を作成 [22]。ここで X はカイ二乗値である。

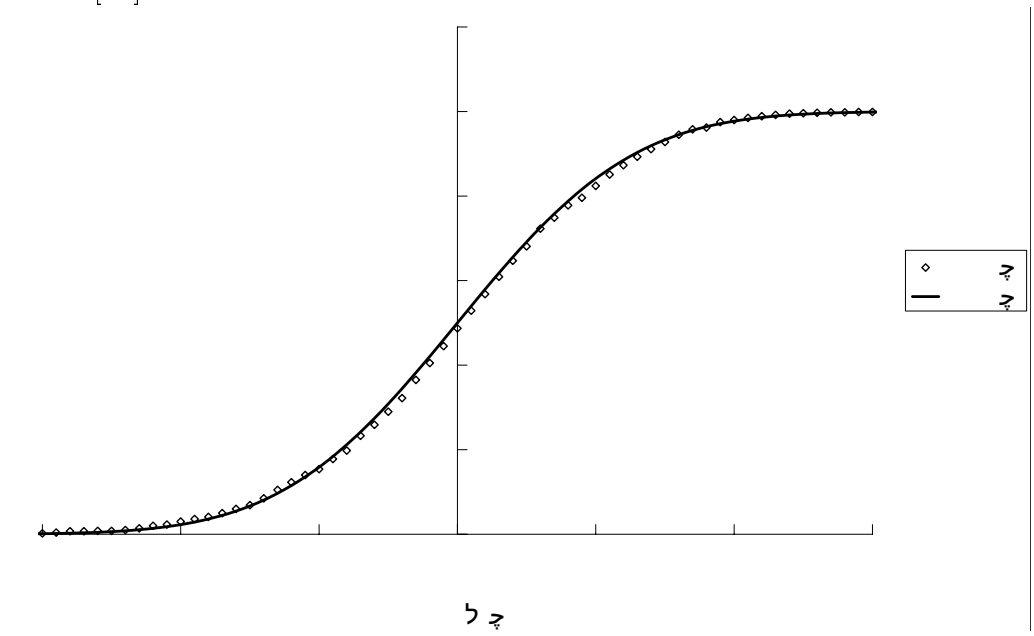


図 5:$\bigtriangledown\psi_m^2$

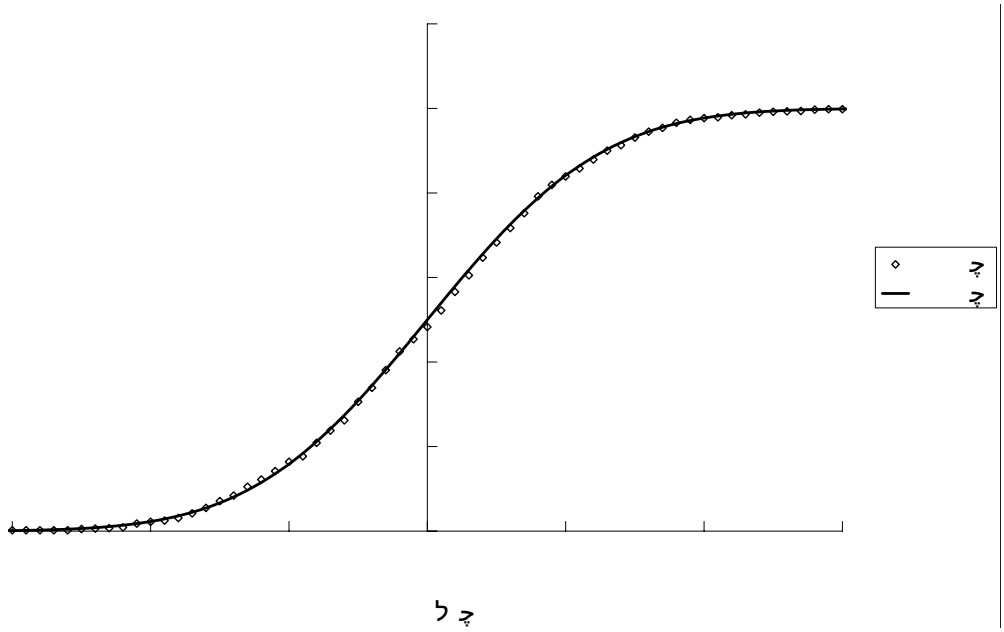


図 6:$\bigtriangledown^2\psi_m^2$

3.12.7　考察

推奨パラメータの範囲で実験を行い、基になる理論分布とほぼ合致していることが確認された。

3.13 近似エントロピー検定

3.13.1 目的

近似エントロピー検定はとり得る全ての m ビットのパターンの発生頻度に着目し、全ての m ビットパターンが均等に現れているかを検定する。

3.13.2 記号の定義

m:各ブロックのビット長
n:乱数列の長さ
ε:0 と 1 からなる乱数列 $\varepsilon = (\varepsilon_1, \varepsilon_2, \cdots \varepsilon_n)$
$\chi^2(obs)$:検定で測定される近似エントロピー評価量 $ApEn(\mathrm{m})$ が理想値とどれほど合致しているかを表す χ^2 統計量

3.13.3 推奨パラメータ

NIST は m,n を $m < \lfloor \log_2 n \rfloor - 2$ となるように選ぶとしている。

3.13.4 検定方法

Step1

ε の最上位ビットから (m-1) ビットを最下位ビットの後ろに付け加え n 個の重なりのある m ビットのブロックを作る。

Step2

取りうる全ての m ビットブロック列の出現頻度を求めそれを $\sharp i$ とおく。
ここで i は m ビットブロックを 2 進法と見た場合の値である。

Step3

全ての i について $C_i^m = \dfrac{\sharp i}{n}$ を計算する。

Step4

以下の計算をする。

$$\phi^{(m)} = \sum_{i=0}^{2^m-1} C_i^m \log C_i^m \tag{3.70}$$

Step5

m=m+1 として上記 Step1 から Step4 を繰り返す。

Step6

以下の計算をする。

$$\chi^2 = 2n[\log 2 - ApEn(m)] \tag{3.71}$$

ここで

$$ApEn(m) = \phi^{(m)} - \phi^{(m+1)} \tag{3.72}$$

Step7

統計量 χ^2 が χ^2 分布に従うと仮定し、統計量 χ^2 の値が χ^2 分布の棄却域 (危険率 0.01) に入るかどうかを、P-value という以下の式

$$P - value = \mathbf{igamc}(2^{m-1}, \frac{\chi^2}{2}) \tag{3.73}$$

で計算される値を用いて決定する。P-value の値が 0.01 以上ならば入力乱数はランダムであるとする。

3.13.5 理論背景

近似エントロピー評価量 (1996) は、繰り返し文字列について Pincus と Singer により考案された [20]。$Yi(m) = (\varepsilon_i, \cdots, \varepsilon_i + m - 1)$ として、

$$C_i^m = \frac{1}{n+1-m} \sharp\{j : 1 \le j < n - m, Y_j(m) = Y_i(m)\} = \pi_\ell \tag{3.74}$$

および

$$\Phi^{(m)} = \frac{1}{n+1-m} \sum_{i=1}^{n+1-m} \log C_i^m \tag{3.75}$$

を考える。C_i^m は、文字列におけるパターン $Y_i(m)$ の相対度数であり、$-\Phi^{(m)}$ は、長さ m の $2m$ 個のパターンの集合の持つ標本分布のエントロピーであり、次式に書き直せる。

$$\Phi^{(m)} = \sum_{\ell=1}^{2^m} \pi_\ell \log \pi_\ell \tag{3.76}$$

ここで π_ℓ はストリングにおけるパターン $\ell = (i_1, \ldots, i_m)$ の相対度数である。

次数 $m(m \ge 1)$ の近似エントロピー $ApEn$ は、次のように定義される

$$ApEn(m) = \Phi^{(m)} - \Phi^{(m+1)} \tag{3.77}$$

ただし、$ApEn(0) = -\Phi^{(1)}$ である。「$ApEn(m)$ は、1 だけずれた位置にある隣接した、長さ m のブロックの似ている度合いを対数度数で評価したものである。したがって、$ApEn(m)$ の小さな値は、系列内の強い規則性、または依存性を意味する。逆に大きければ、不規則性、ランダム性が大きいことを意味する」[20]

Pincus and Kalman(1997) は、系列の近似エントロピー $ApEn(m)$ が最大の値をとる場合、m-irregular(m-random) であると定義した。彼らは e,π,$\sqrt{2}$ および $\sqrt{3}$ の 2 進、および 10 進展開について数量 $ApEn(m)$ ($m = 0, 1, 2$) を評価し、$\sqrt{3}$ の展開が π の展開よりも大きな不規則性を示すという結論を導いた。

固定ブロック長 m に対して、長いランダム (不規則) な文字列では、$ApEn(m)$ $\sim \log 2$ と予測される。$n[\log 2 - ApEn(m)]$ の極限分布は、自由度 $2m$ のカイ 2 乗分布となる。この事実は、Rukhin(2000) の示す通り、統計検定の基礎となる。

このように、$\chi^2(obs) = n[log2 - ApEn(m)]$ として、P-value は

$$\mathbf{igamc}(2^{m-1}, \frac{\chi^2(obs)}{2}) \tag{3.78}$$

である。

実際には、より正確な近似エントロピーとして、元の入力系列を循環させた系列 $(\varepsilon_1, \ldots, \varepsilon_n, \quad \varepsilon_1, \ldots, \varepsilon_{m-1})$ を考えて近似エントロピーを考えねばならない。すなわち、$\nu_{i_1 \ldots i_m}$ は、元の文字列の循環版におけるテンプレート $(i_1, \ldots, i_m)$ の相対度数として、

$$\tilde{\Phi}^{(m)} = \sum_{i_1 \ldots i_m} \nu_{i_i \ldots i_m} \log \nu_{i_i \ldots i_m} \tag{3.79}$$

を計算し、近似エントロピーを

$$A\tilde{p}En(m) = \tilde{\Phi}^{(m)} - \tilde{\Phi}^{(m+1)} \tag{3.80}$$

と定義する。

Jensen の不等式によると、s 元系列であらゆる m に対して $\log s \geq A\tilde{p}En(m)$ であるが、$\log s < ApEn(m)$ となる場合もある (ここでは、$s = 2$)。したがって、変更されたエントロピーの最大値は、単に $\log s$ であり、これは、$n = S^m$ のときに得られ、このとき、すべての長さ m のパターン分布は一様である。

n が大きい場合、$ApEn(m)$ とその修正版は大きく違わない。固定された m の場合、n が大きければ、$\Phi^{(m)}$ および $\tilde{\Phi}^{(m)}$ は近い値となる。したがって Pincus の近似エントロピーとその修正版もまた、ほぼ等しく、それらの漸近的分布も一致する。

3.13.6 統計量 χ^2 と χ^2 分布との比較

全ての測定は乱数生成アルゴリズムとして NIST のプログラムに付随している G-Using SHA-1 を用い、乱数長を 1,000,000、標本数を 1000 として行った。
NIST は得られる統計量が自由度 2^m の χ^2 分布に従うとしている。

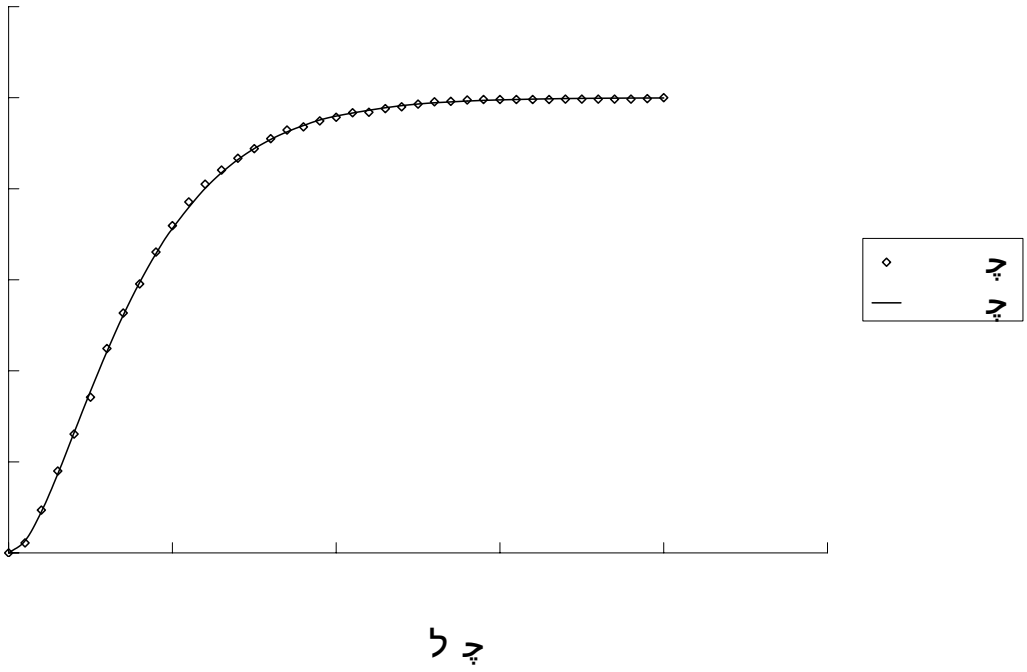


図 1:m=2 の場合

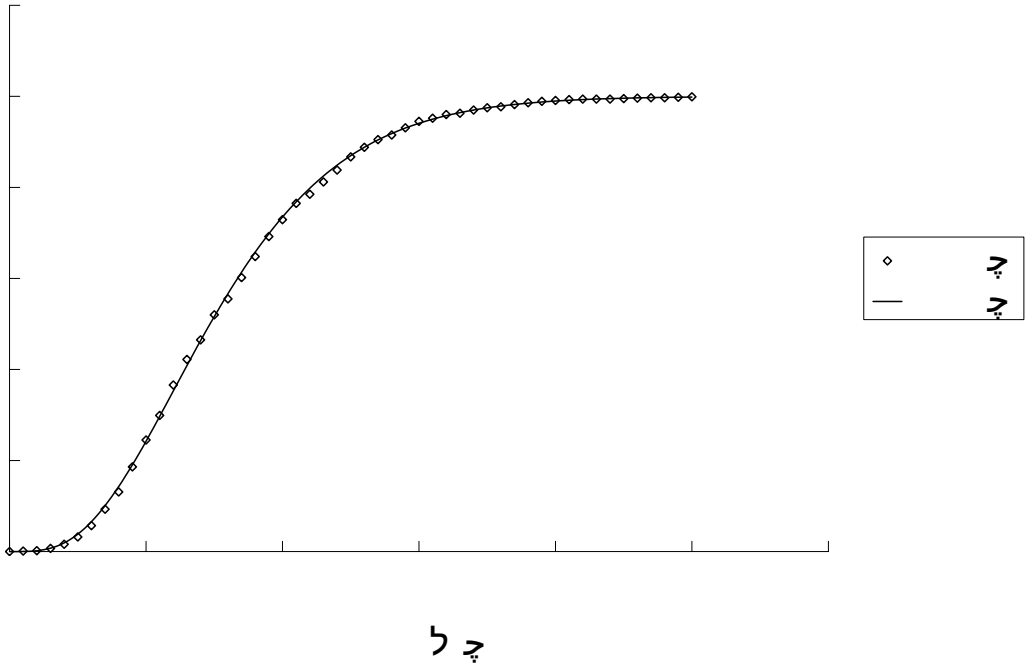


図 2:m=3 の場合

自由度 k が k>30 の時、$\sqrt{2X} - \sqrt{2k-1}$ が正規分布に近似できるため，以下に図を作成 [22]。ここで X はカイ 2 乗値である。

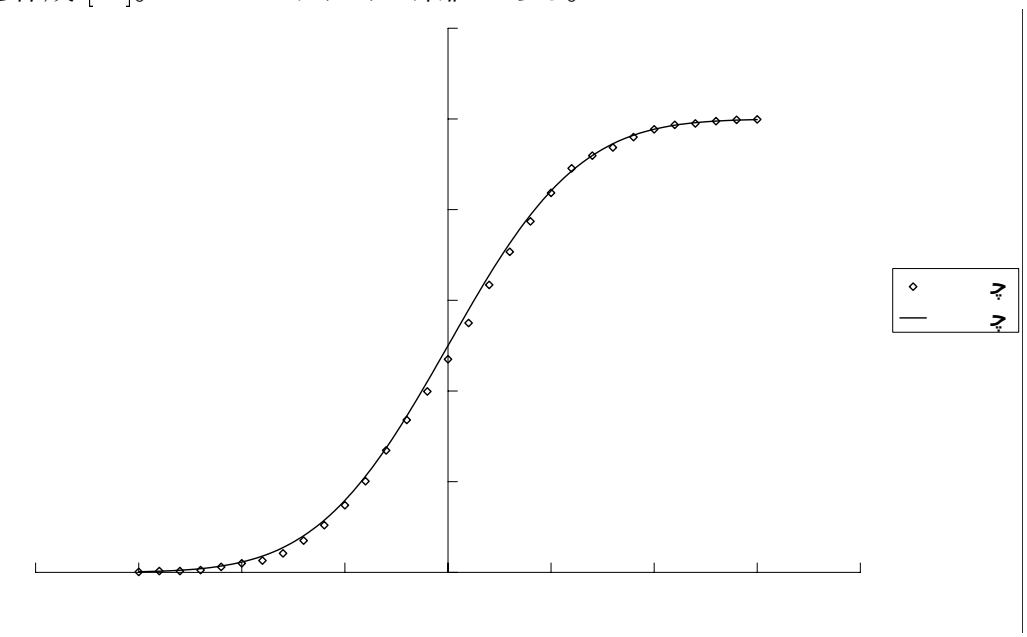


図 3:m=10 の場合

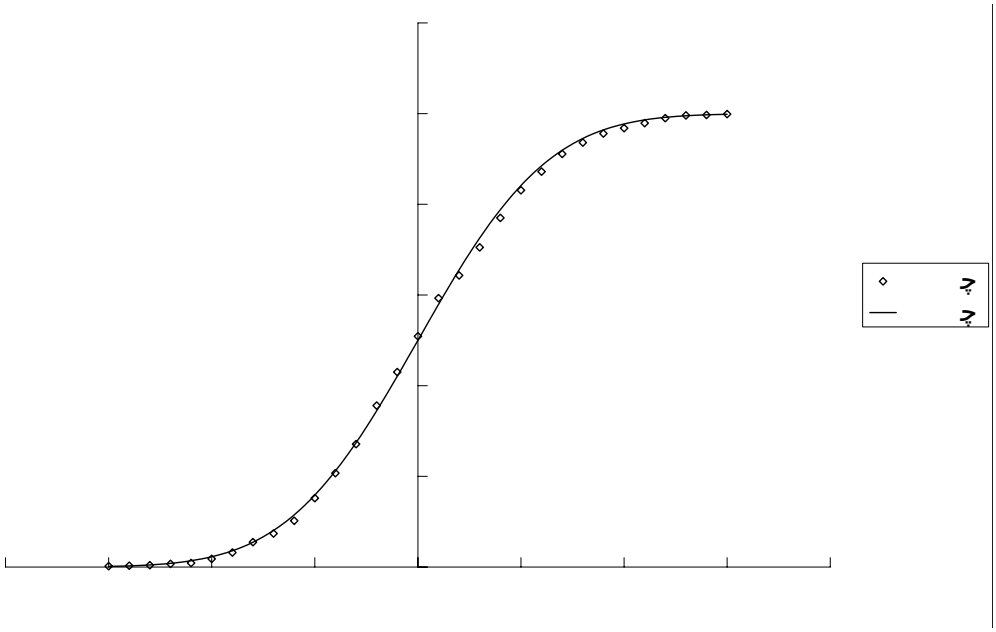


図 4:m=11 の場合

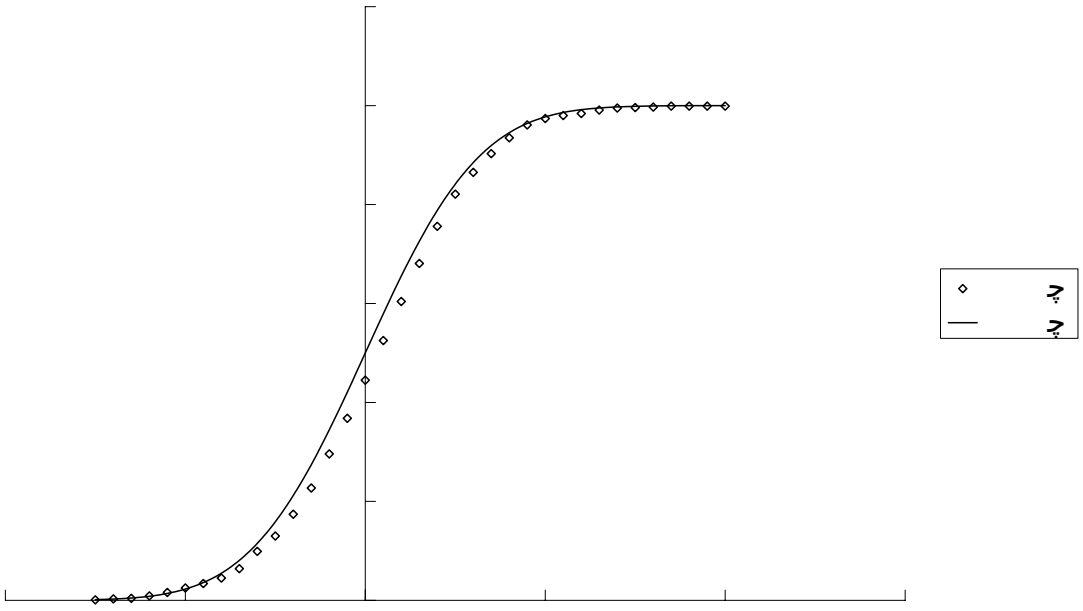


図 5:m=12 の場合

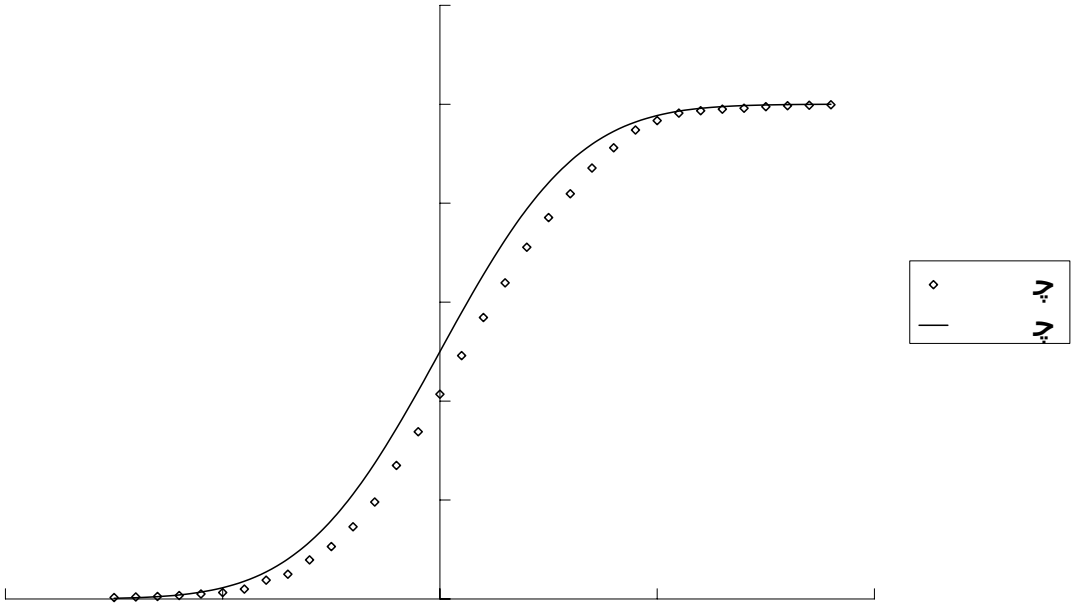


図 6:m=13 の場合

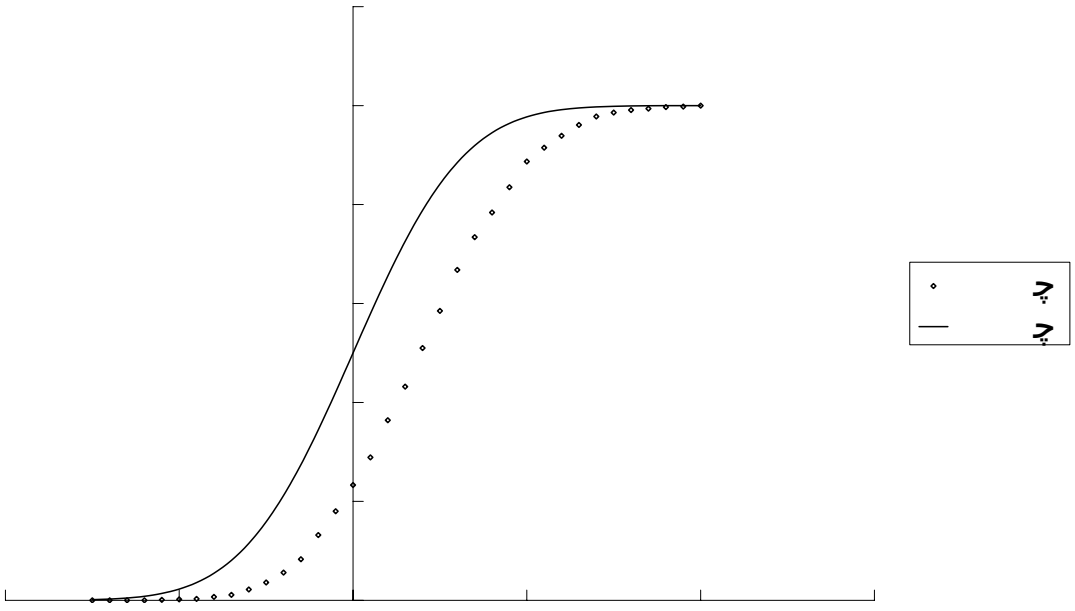


図 6:m=14 の場合

3.13.7 考察

$n = 100$ 万 のときは $m > 12$ の場合、実験値と理論値に乖離が見られる。これは m とともにブロックの数が 2^m と増加していくため、長さ n の乱数列から 1 つのブロックに入るブロック列に出現頻度が平均値で $\frac{n}{2^m}$ と m に対し指数関数的に小さくなっていくことからと思われる。ちなみにこの実験で n=100 万,m=14 とした場合、１つのブロック列は平均的に６個と少なく実験データの誤差につながったものと考えられる。

NIST は推奨値として $m < \lfloor \log_2 n \rfloor - 2$ としているが、プログラム中では $m > \lfloor \log_2 n \rfloor - 5$ ではデータの信頼性が低いとしている。しかし、この実験データからはそれでもまだ信頼性が低く、n=100 万ビットでは $m < 12$ 程が適当であると見られ、それを式として表すと $m < \lfloor \log_2 n \rfloor - 7$ となる。

3.14 累積和検定

3.14.1 目的

累積和検定とは0と1からなる入力数列を-1、1に変換し、先頭または一番後ろから1ビットずつその値を加算していき、加算操作中における絶対値の最大値の偏りを調べるものである。

3.14.2 記号の定義

n ：乱数列の長さ
ε ：0と1からなる乱数列（ε=ε_1,ε_2,...,ε_n）
z ：(-1,+1）で表される数列における部分和の絶対値の最大値。

3.14.3 推奨パラメータ

乱数列は$n \geqq 100$bitとなるようにとる。

3.14.4 検定方法

Step1　乱数列εの0,1を$X_i = 2\varepsilon_i - 1$を使って-1と+1の値X_iに変える。

Step2　Xの値を順々に加え、部分和S_iを求める。mode=0のときX_1から、mode=1のときはX_nから順々に値を加えていく。

Step3　確率変数z=$max_{1 \leqq k \leqq n}|S_k|$を求める。$max_{1 \leqq k \leqq n}|S_k|$は部分和$S_k$の絶対値の最大値である。

Step4　確率変数zが(3.84)式に従うと仮定し、確率変数zの値が理論分布の棄却域(危険率0.01)に入るかどうかを、$P-value$という以下の式：

$$P-value = 1 - \sum_{k=(\frac{-n}{z}+1)/4}^{(\frac{n}{z}-1)/4} [\Phi(\frac{(4k+1)z}{\sqrt{n}}) - \Phi(\frac{(4k-1)z}{\sqrt{n}})] + \sum_{k=(\frac{-n}{z}-3)/4}^{(\frac{n}{z}-1)/4} [\Phi(\frac{(4k+3)z}{\sqrt{n}}) - \Phi(\frac{(4k+1)z}{\sqrt{n}})] \tag{3.81}$$

で計算される値を用いて決定する。$P-value$の値が0.01以上ならば入力乱数はランダムであるとする。

ここで、

$$\Phi(z) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{z} \exp\{-\frac{u^2}{2}\} du \tag{3.82}$$

である。

3.14.5 理論背景

この検定は、± 1 によって表される系列の部分和の最大絶対値を使用する。この統計量が大きい場合、系列の前段階に 1 が多すぎるか、または 0 が多すぎることを意味している。小さな値は、0 と 1 が均等に混ざっていることを示している。また、$S'_k = X_n + \ldots + X_{n-k+1}$ とした逆方向累積和に対しても検定を考える事ができ、この定義では、検定結果の解釈は、前述の「前段階」が「後段階」に置き換えたものとなる。

この検定は部分和の絶対値の最大値の極限分布にもとづいている。$max_{1 \leq k \leq n}|S_k|$ の分布は次式に従う。

$$\begin{aligned} \lim_{n\to\infty} P\left(\frac{max_{1\leqq k\leqq n}|S_k|}{\sqrt{n}} \leqq z\right) &= \frac{1}{\sqrt{2\pi}} \int_{-z}^{z} \sum_{k=-\infty}^{\infty} (-1)^k \exp\left\{-\frac{(u-2kz)^2}{2}\right\} du \\ &= \frac{4}{\pi} \sum_{j=0}^{\infty} \frac{(-1)^j}{2j+1} \exp\left\{-\frac{(2j+1)^2\pi^2}{8z^2}\right\} = H(z) \quad , z > 0 \end{aligned} \tag{3.83}$$

検定統計量を $max_{1 \leq k \leq n}|S_k|(obs)/\sqrt{n}$ とすると、ランダム性仮説は z の値が大きい場合、棄却され、対応する P-value は、式 (3.84)〜(3.87) で定義される $G(z)$ を使用して、$1 - H(max_{1 \leq k \leq n}|S_k|(obs)/\sqrt{n}) = 1 - G(max_{1 \leq k \leq n}|S_k|(obs)/\sqrt{n})$ である。

式 (3.83) の最終行の級数表現 $H(z)$ は、すぐに収束し、z の小さな値についてのみ、この $H(z)$ を数値計算に使用する必要があるが、有る程度大きい値に対しては、次の関数 $G(z)$ 又はその近似式で十分である。

$$G(z) = \frac{1}{\sqrt{2\pi}} \int_{-z}^{z} \sum_{k=-\infty}^{\infty} (-1)^k \exp\left\{-\frac{(u-2kz)^2}{2}\right\} du$$

$$= \sum_{k=-\infty}^{\infty} (-1)^k [\Phi((2k+1)z) - \Phi((2k-1)z)] \tag{3.84}$$

$$= \Phi(z) - \Phi(-z) + 2\sum_{k=1}^{\infty} (-1)^k [\Phi((2k+1)z) - \Phi((2k-1)z)]$$

$$= \Phi(z) - \Phi(-z) + 2\sum_{k=1}^{\infty} [2\Phi((4k-1)z) - \Phi((4k+1)z) - \Phi((4k-3)z)] \tag{3.85}$$

$$\approx \Phi(z) - \Phi(-z) - 2\left[2\Phi(3z) - \Phi(5z) - \Phi(z)\right] \tag{3.86}$$

$$\approx 1 - \frac{4}{\sqrt{2\pi}z}\exp\{-\frac{z^2}{2}\} \qquad z \to \infty \tag{3.87}$$

ここでΦ (z) は、標準正規分布である。

(3.84) 式を k の偶数と奇数で分ければ、次式である。

$$H(z) = \sum_{k=-\infty}^{\infty}\left[\Phi((4k+1)z) - \Phi((4k-1)z)\right] - \sum_{k=-\infty}^{\infty}\left[\Phi((4k+3)z) - \Phi((4k+1)z)\right] \tag{3.88}$$

ここで、直接的にRevesz(1990)p.17 の定理 2.6 を使用して、以下が得られる [24]。

$$P\left(max_{1\leqq k\leqq n}|S_k| \geqq z\right) = 1 - \sum_{k=-\infty}^{\infty} P((4k-1)z < S_n < (4k+1)z)) + \sum_{k=-\infty}^{\infty} P((4k+1)z < S_n < (4k+3)z)) \tag{3.89}$$

(3.81) 式の P-value は、$1 - H(z)$ に (3.89)、(3.88) 式を代入したものである。

3.14.6 確率変数 z と理論分布の比較

乱数長 n が 100、1,000、10,000、100,000、1,000,000bit で、mode=0、mode=1 それぞれの場合のおいて、確率変数 z が (3.84) 式に従うかどうか、シミュレーション実験を実行した結果を以下に示す。$k = 1$ で近似している (3.85) 式では正確な値がでないため、(3.84) 式を $k = 3$ の場合までで近似し、理論分布を求めた。

なお、乱数生成アルゴリズムにはNIST に付随している G-Using SHA-1 を使用し、標本数は 1000 とした。

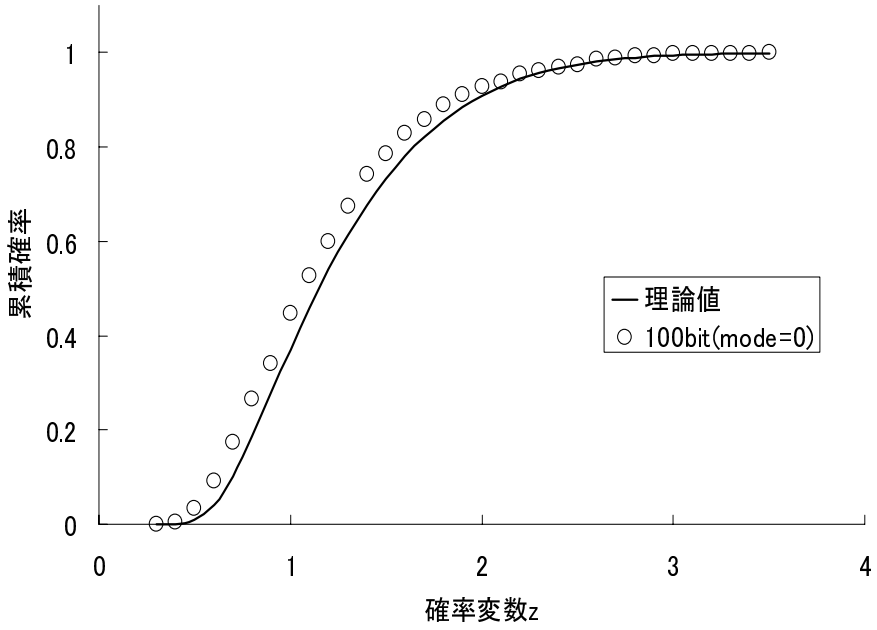


図 3.28: 100bit(mode=0)

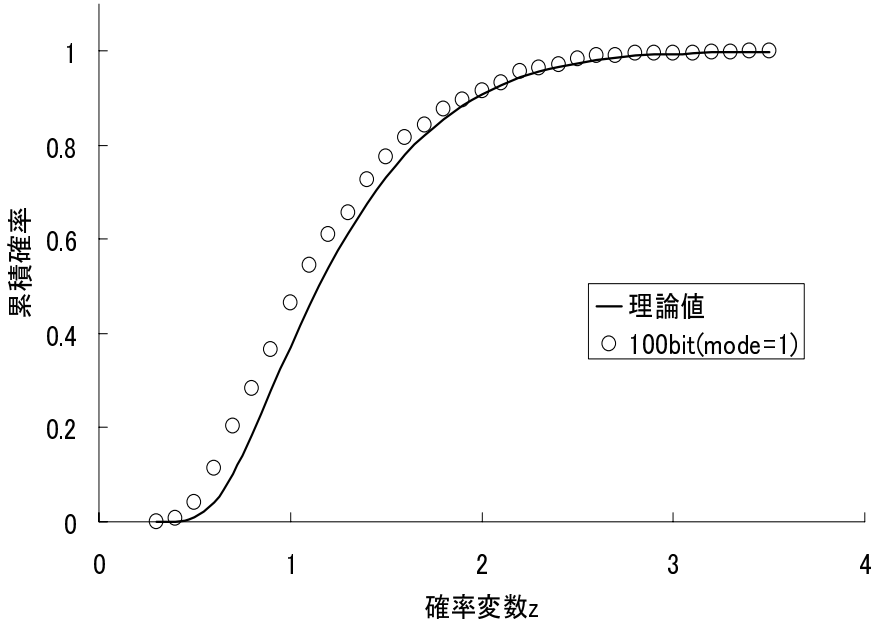


図 3.29: 100bit(mode=1)

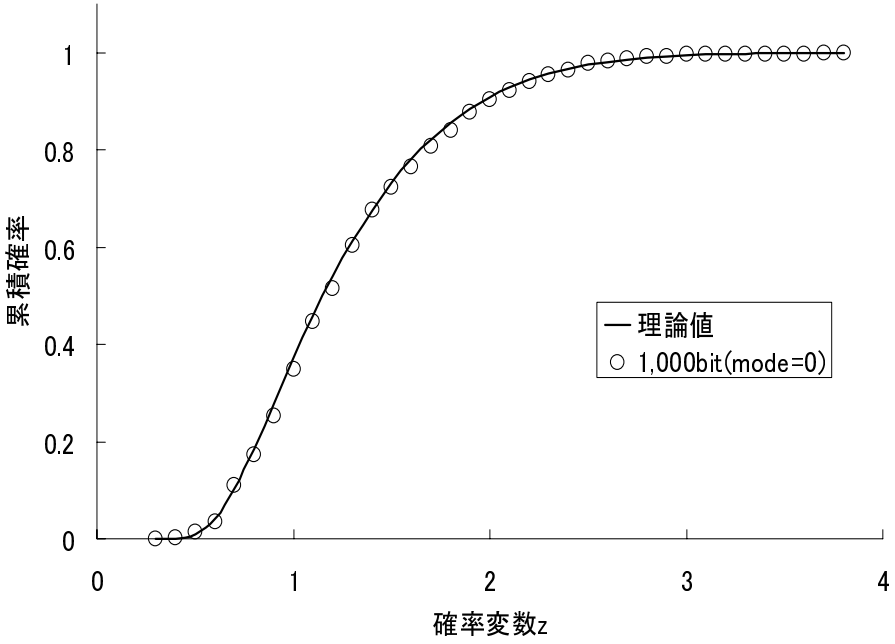


図 3.30: 1000bit(mode=0)

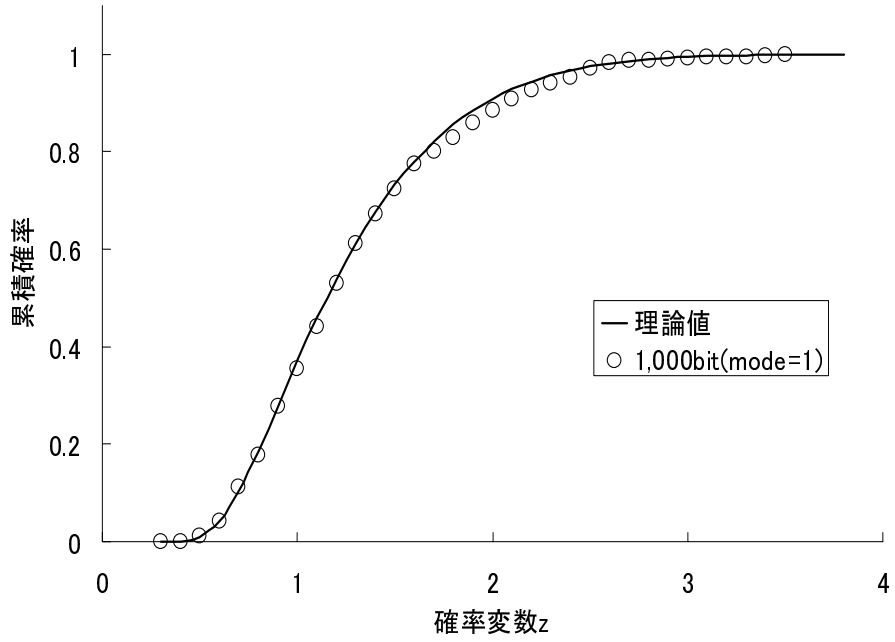


図 3.31: 1000bit(mode=1)

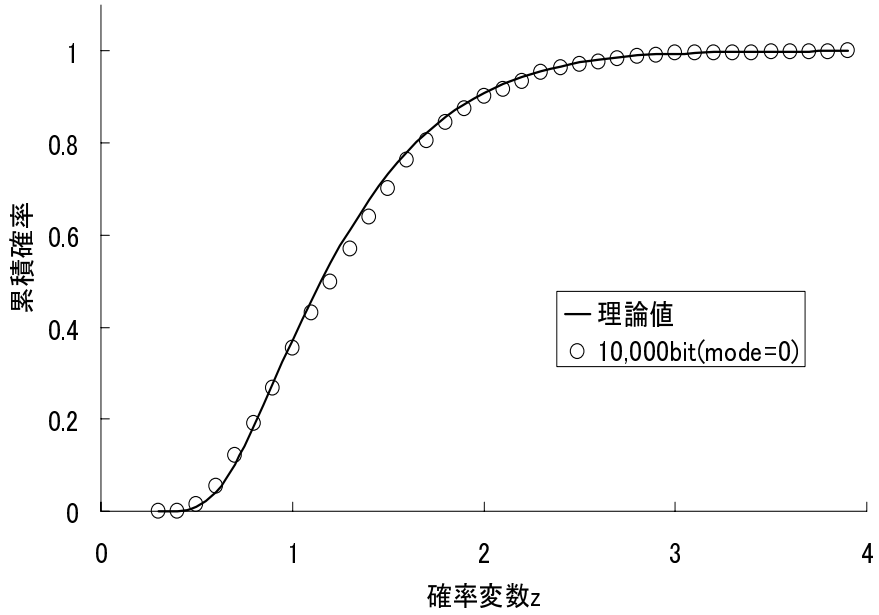


図 3.32: 10000bit(mode=0)

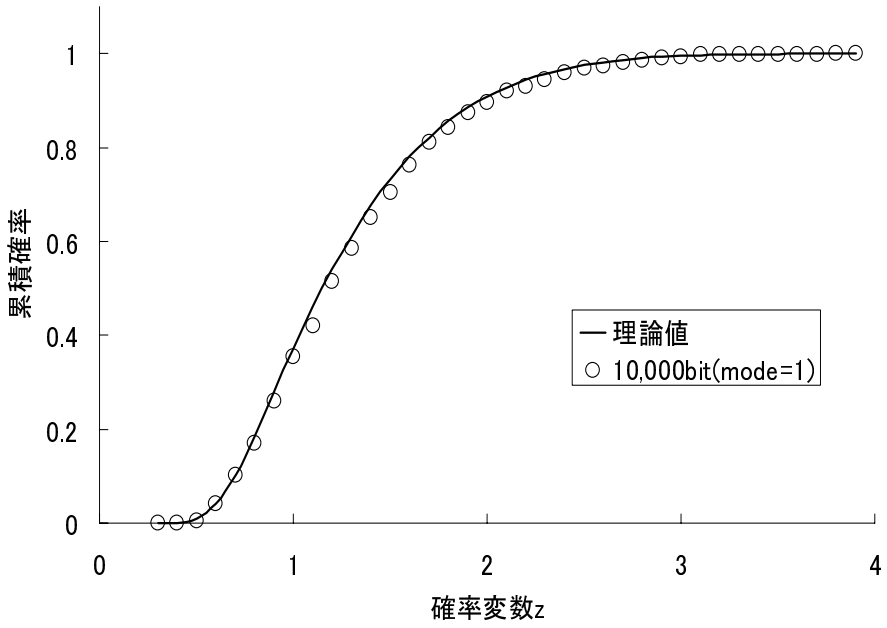


図 3.33: 10000bit(mode=1)

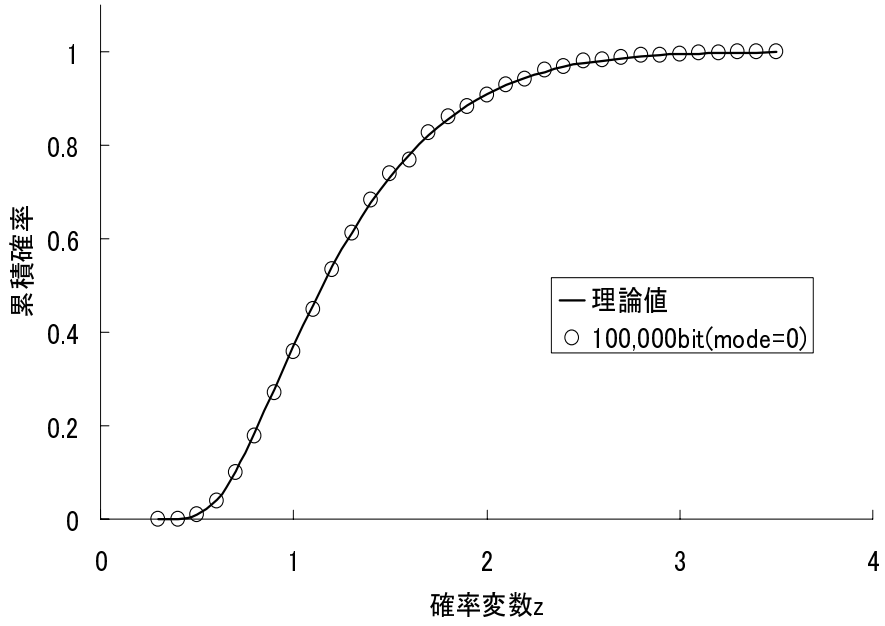


図 3.34: 100000bit(mode=0)

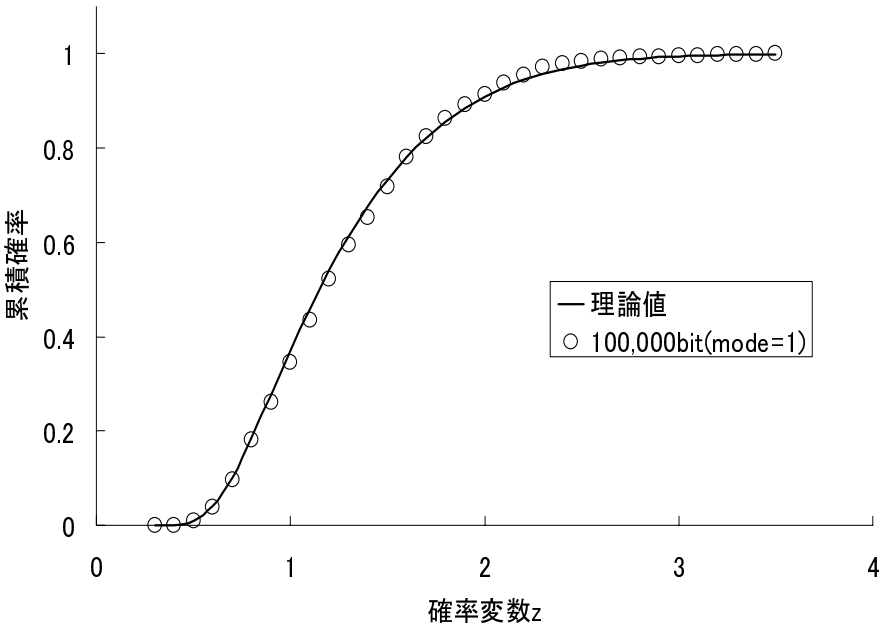


図 3.35: 100000bit(mode=1)

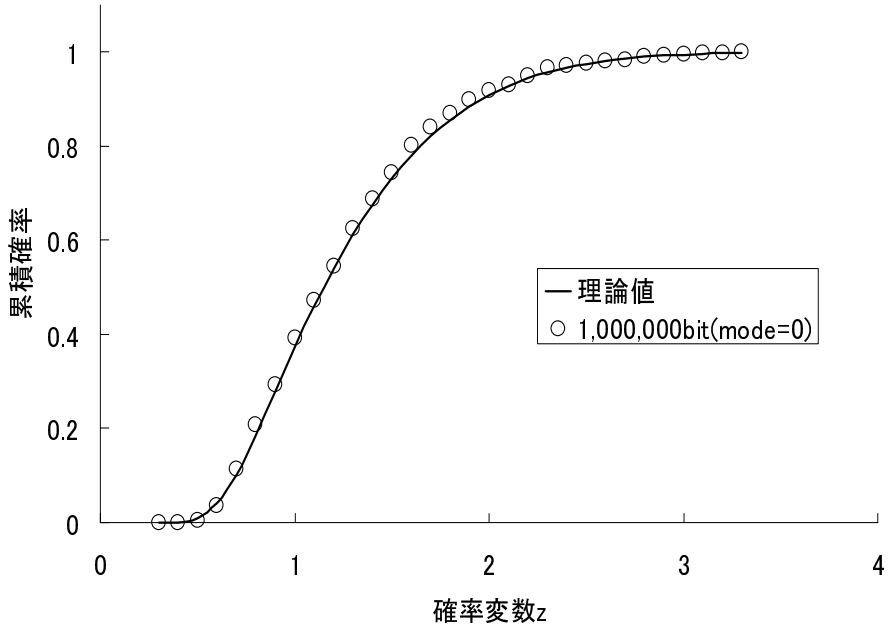


図 3.36: 1000000bit(mode=0)

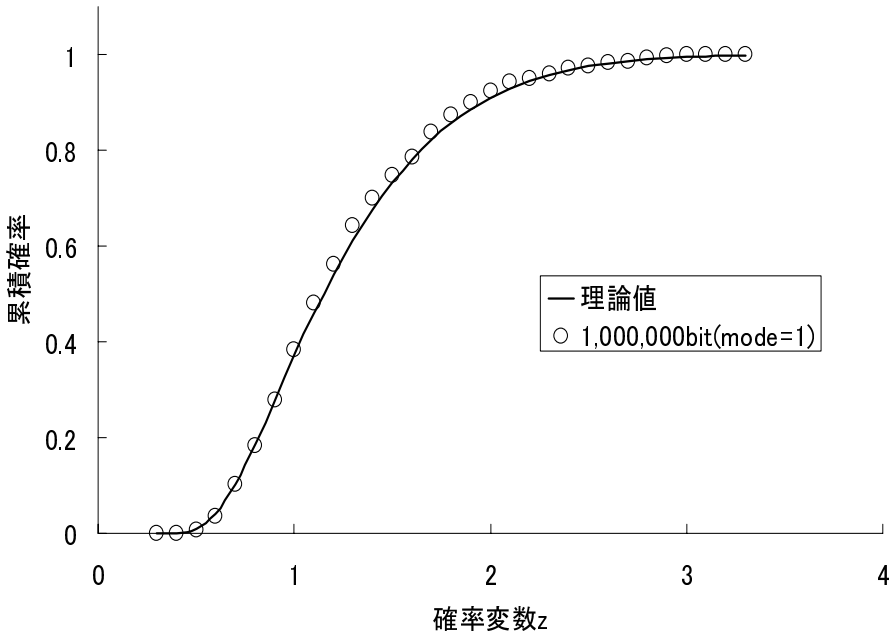


図 3.37: 1000000bit(mode=1)

3.14.7　考察

推奨パラメータの範囲で実験を行い、系列の長さが小さいところでは若干のずれが見られるが、基になる理論分布とほぼ合致していることが確認できた。

3.15 ランダム回遊検定

3.15.1 目的

ランダム回遊検定とは、入力数列の 0 と 1 を-1 と 1 に変換して先頭から加算していき、合計の値が 0 の場所から次に 0 になるまでを 1 つのサイクルと考え、サイクルごとに 8 種類 (-4〜-1、1〜4) の状態値 x の出現数の偏りを調べるものである。

3.15.2 記号の定義

n ：乱数列の長さ
ε ：0 と 1 の値からなる乱数列（ε=ε_1,ε_2,...,ε_n）
$\chi^2(obs)$ ：χ^2 統計量

3.15.3 推奨パラメータ

乱数列は $n \geqq 10^6$bit となるようにとる。

3.15.4 検定方法

Step1　乱数列（ε）の 0,1 を $X_i = 2\varepsilon_i - 1$ を使って-1 と+1 の値 X_i に変える。

Step2　X の値を X_1 から順々に加え、部分和 S_i を求める。$S = \{S_i\}$ と表す。

Step3　数列 S の一番最初と最後に 0 を結びつけ、新しい数列 S' を作る。$S' = 0, s_1, s_2, \ldots, s_n, 0$

Step4　J を求める。J は、S' の先頭をのぞく 0 の個数である。また J は、隣り合う 0 をそれぞれ先頭、末尾とするサイクルの個数でもある。もし、J<500 なら検定を中止する。

Step5　各サイクルにおいて、8 個の状態値 $x(-4 \leqq x \leqq -1, 1 \leqq x \leqq 4)$ について、x の現れる回数を求める。

Step6　8 個の状態値 x それぞれについて、$\nu_k(x)$ を求める。$\nu_k(x)$ は、状態値 x の出現度数が k となるサイクルの数をあらわす。ただし $(0 \leqq k \leqq 5)$ で、$\nu_5(x)$ は状態値 x の出現度数が 5 以上のサイクル数とする。

Step7　8 個の状態値 x それぞれに対し、統計量 $\chi^2(obs)$ を求める。

$$\chi^2(obs) = \sum_{k=0}^{5} \frac{(\nu_k(x) - J\pi_k(x))^2}{J\pi_k(x)} \tag{3.90}$$

$\pi_k(x)$ は、状態値 x の出現度数が k となる確率である。なお、$\pi_k(x)$ の値は表 1 の通りである。

表 1

$\|x\|$	$\pi_0(x)$	$\pi_1(x)$	$\pi_2(x)$	$\pi_3(x)$	$\pi_4(x)$	$\pi_5(x)$
1	0.5000	0.2500	0.1250	0.0625	0.0312	0.0312
2	0.7500	0.0625	0.0469	0.0352	0.0264	0.0791
3	0.8333	0.0278	0.0231	0.0193	0.0161	0.0804
4	0.8750	0.0156	0.0137	0.0120	0.0105	0.0733

Step8　統計量 $\chi^2(obs)$ が χ^2 分布に従うと仮定し、統計量 $\chi^2(obs)$ の値が χ^2 分布の棄却域 (危険率 0.01) に入るかどうかを、$P-value$ という以下の式：

$$P - value = \mathbf{igamc}\left(\frac{5}{2}, \frac{\chi^2(obs)}{2}\right) \tag{3.91}$$

で計算される値を用いて決定する。$P-value$ の値が 0.01 以上ならば入力乱数はランダムであるとする。

3.15.5　理論背景

サイクル数 J の分布として以下のような式が知られている。

$$\lim_{n\to\infty} P\left(\frac{J}{\sqrt{n}} < z\right) = \sqrt{\frac{2}{\pi}} \int_0^z e^{-\frac{u^2}{2}} du, \quad z > 0 \tag{3.92}$$

J の値が小さいとき、すなわち $P-value$ の値が小さいとき、ランダムであるという仮定を棄却する。

ここでは、サイクル数 J が J<500 である場合ランダムであるという仮定を満たさないと考え、J<500 であれば、検定を中止する。

状態値 x の出現度数が k の確率 $\pi_k(x)$ の値は、以下の式で計算される。

$$\pi_0(x) = 1 - \frac{1}{2|x|}$$
$$\pi_k(x) = \frac{1}{4x^2}\left(1 - \frac{1}{2|x|}\right)^{k-1} \quad k = 1, 2, 3, 4 \tag{3.93}$$
$$\pi_5(x) = \frac{1}{2|x|}\left(1 - \frac{1}{2|x|}\right)^4$$

この $\pi_k(x)$ を用いて、統計量 $\chi^2(obs)$ の値は (3.90) 式で与えられる。

統計量 $\chi^2(obs)$ は自由度 5 の χ^2 分布に近似的に従うことより、$P - value$ の値は以下の式で求められる。

$$1 - \mathbf{P}\left(\frac{5}{2}, \frac{\chi^2(obs)}{2}\right) \tag{3.94}$$

上式より、(3.91) 式が導かれる。

3.15.6 統計量 $\chi^2(obs)$ と χ^2 分布との比較

乱数長 n が 10^6bit の場合で、統計量 $\chi^2(obs)$ が χ^2 分布に従うかどうか、シミュレーション実験を実行した結果を次ページ以降に示す。なお、乱数生成アルゴリズムには NIST に付随している G-Using SHA-1 を使用し、標本数は 1000 とした。

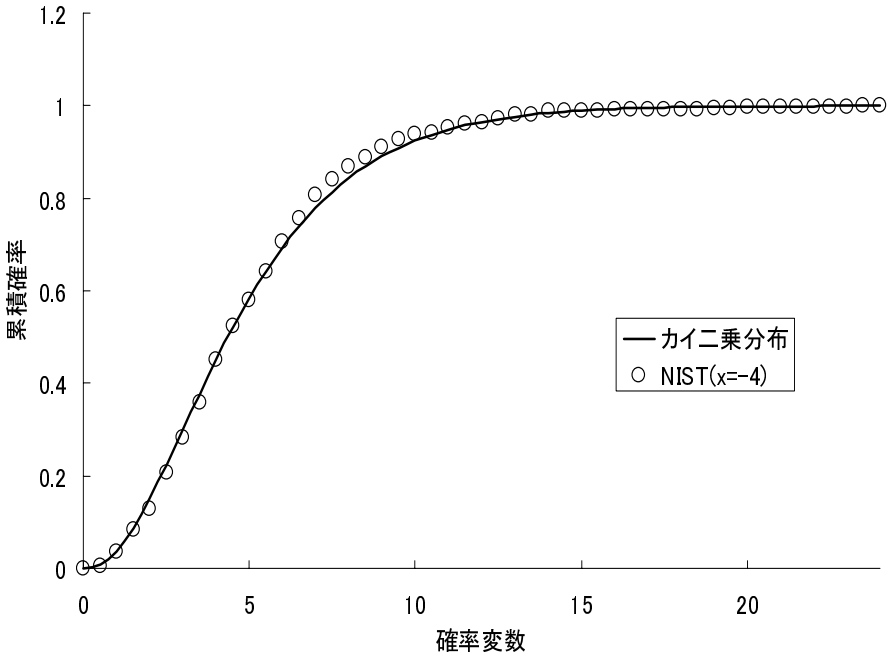


図 3.38: x=-4

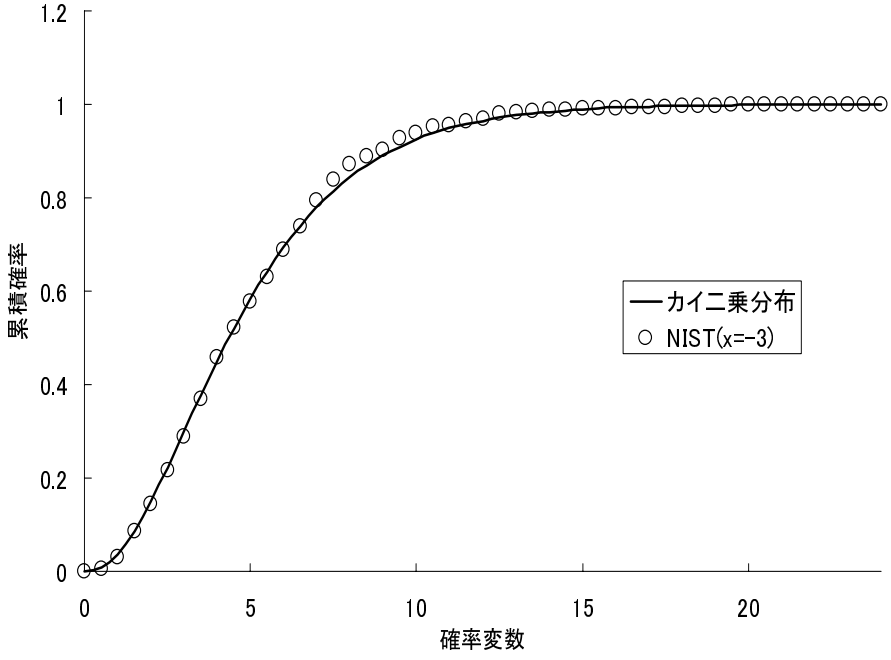


図 3.39: x=-3

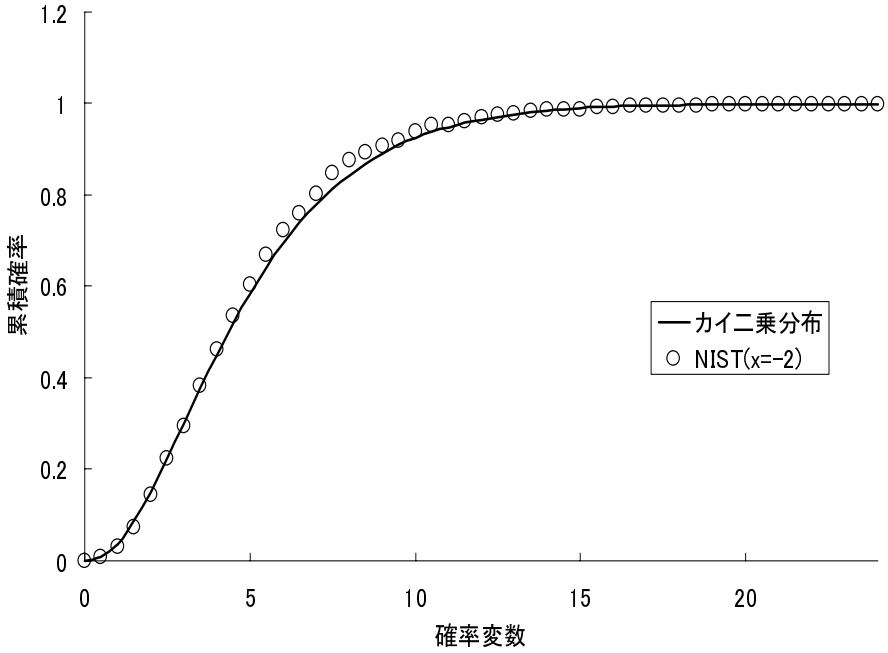


図 3.40: x=-2

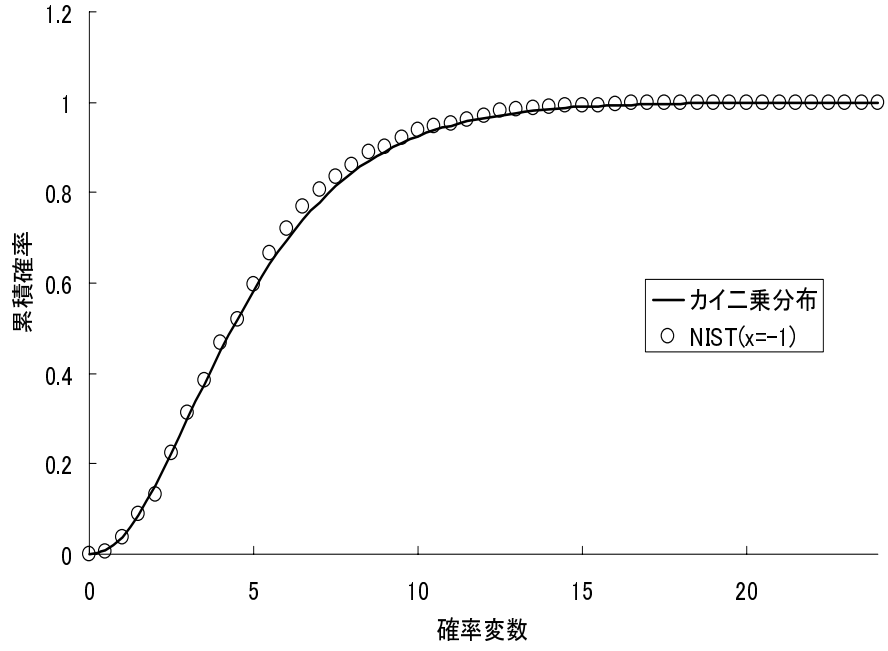


図 3.41: x=-1

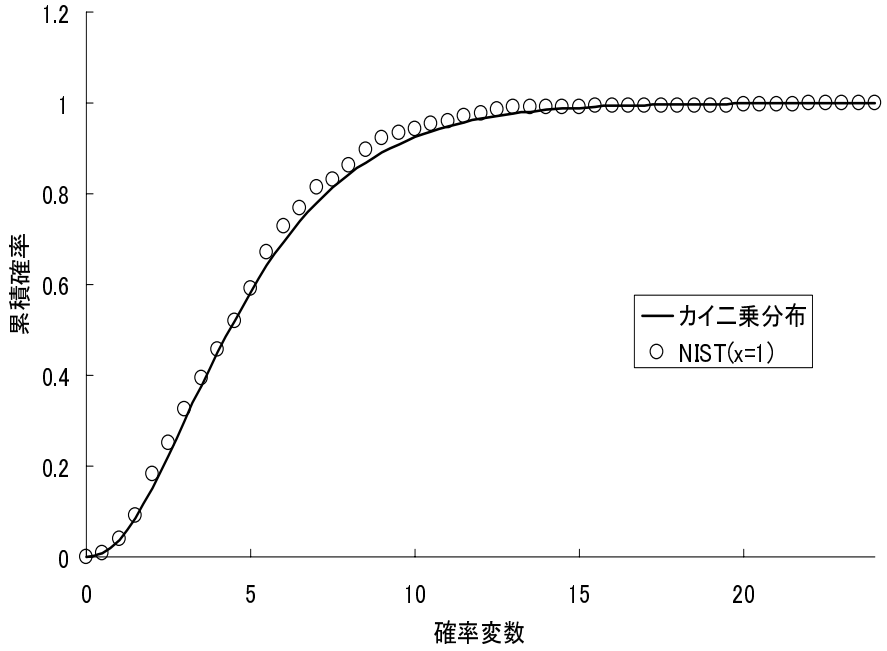


図 3.42: x=1

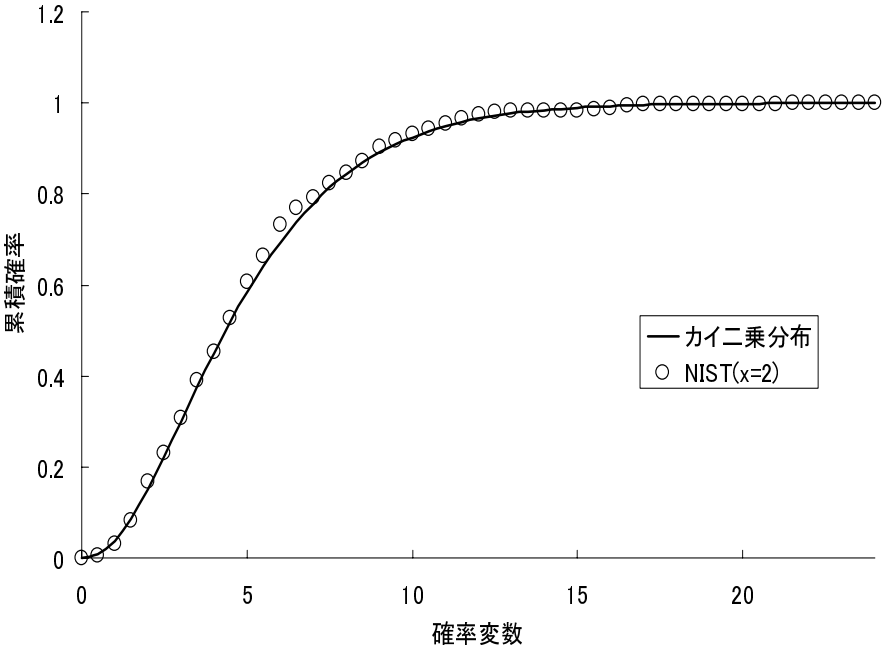


図 3.43: x=2

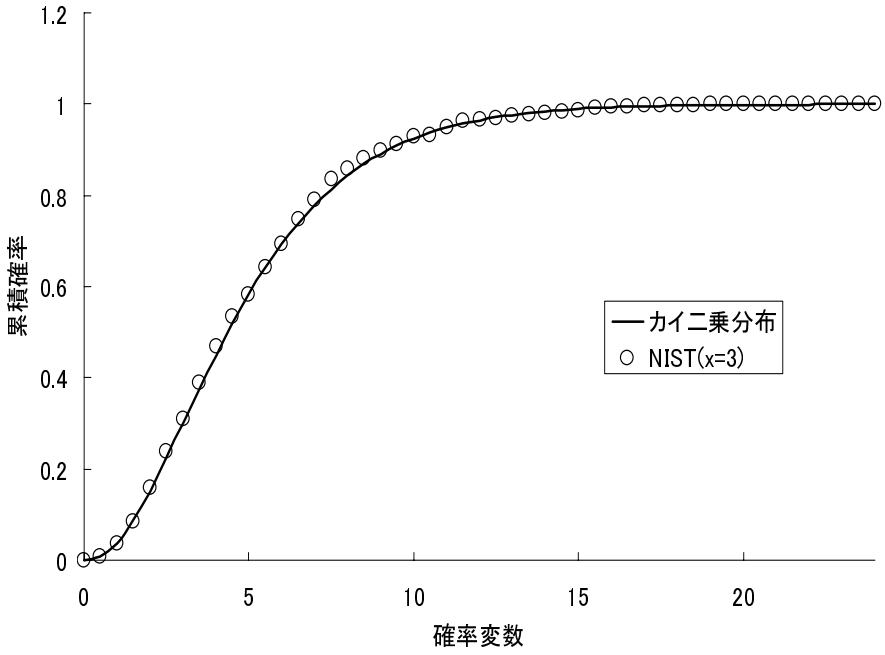


図 3.44: x=3

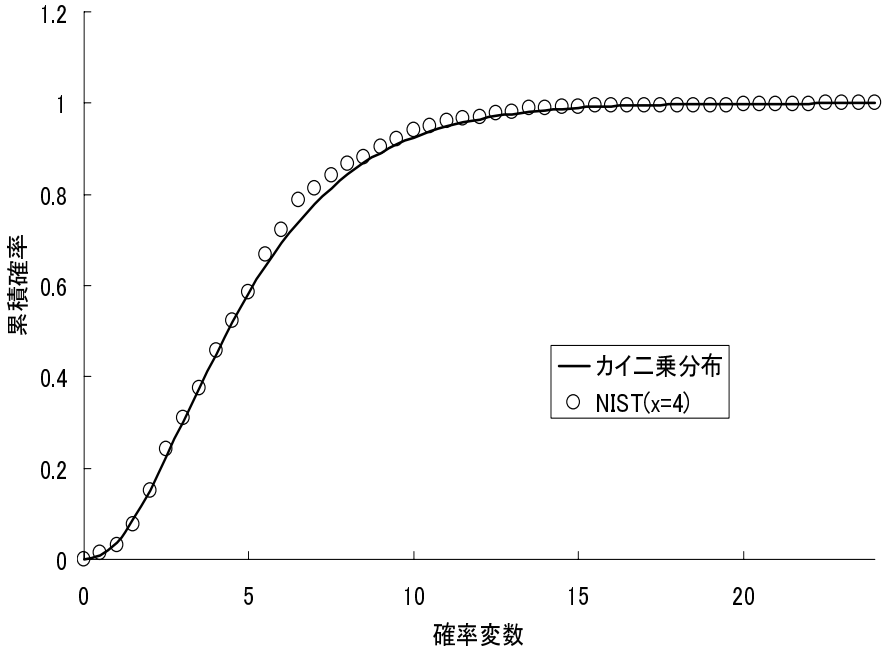


図 3.45: x=4

3.15.7　考察

推奨パラメータの範囲で実験を行い、基になる理論分布とほぼ合致していることが確認できた。

3.16 変形ランダム回遊検定

3.16.1 目的

変形ランダム回遊検定とは、入力数列の 0 と 1 を-1 と 1 に変換し、先頭から加算していく。入力数列の先頭から最後までをまとめて扱い、18 種類 (-9〜-1,1〜9) の状態値 x の出現数の偏りを調べるものである。

3.16.2 記号の定義

n ：乱数列の長さ
ε ：0 と 1 からなる乱数列（ε=ε_1,ε_2,...,ε_n）
$\xi(x)$ ：正規分布統計量

3.16.3 推奨パラメータ

乱数列は $n \geq 10^6$bit となるようにとる。

3.16.4 検定方法

Step1　乱数列（ε）の 0,1 を $X_i = 2\varepsilon_i - 1$ を使って-1 と+1 の値 X_i に変える。

Step2　X の値を X_1 から順々に加え、部分和 S_i を求める。$S = \{S_i\}$ と表す。

Step3　数列 S の一番最初と最後に 0 を結びつけ、新しい数列 S' を作る。$S' = 0, s_1, s_2, \ldots, s_n, 0$　また、S' のサイクル数 J を求める。

Step4　確率変数 $\xi(x)$ を求める。$\xi(x)$ は $-9 \leq x \leq -1, 1 \leq x \leq 9$ を満たす 18 個の状態値 x について、x が S' の中に現れる回数である。

Step5　確率変数 $\xi(x)$ が標準正規分布に従うと仮定し、確率変数 $\xi(x)$ の値が標準正規分布の棄却域 (危険率 0.01) に入るかどうかを、$P - value$ という以下の式：

$$P - value = erfc\left(\frac{|\xi(x) - J|}{\sqrt{2J(4|x| - 2)}}\right) \tag{3.95}$$

で計算される値を用いて決定する。$P - value$ の値が 0.01 以上ならば入力乱数はランダムであるとする。

3.16.5 理論背景

この検定では、系列がランダムであるという仮定のもと検定を行うが、サイクル数 J が J<500 である場合この仮定を満たさないと考え、J<500 であれば検定を中止する。

統計量 $\xi(x)$ は中心極限定理を用いて、平均 J、分散 $J(4|x|-2)$ の正規分布となり、以下の (3.96) 式で表される。

$$\lim_{J\to\infty} P\left(\frac{\xi_J(x)-J}{\sqrt{J(4|x|-2)}} < z\right) = \Phi(z) \tag{3.96}$$

上式から $P-value$ の値を求める (3.95) 式が導かれる。

3.16.6 確率変数 $\xi(x)$ と標準正規分布の比較

乱数長 n が 10^6bit の場合で、確率変数 $\xi(x)$ が標準正規分布に従うかどうか、シミュレーション実験を実行した結果を以下に示す。なお、乱数生成アルゴリズムには NIST に付随している G-Using SHA-1 を使用し、標本数は 1000 とした。

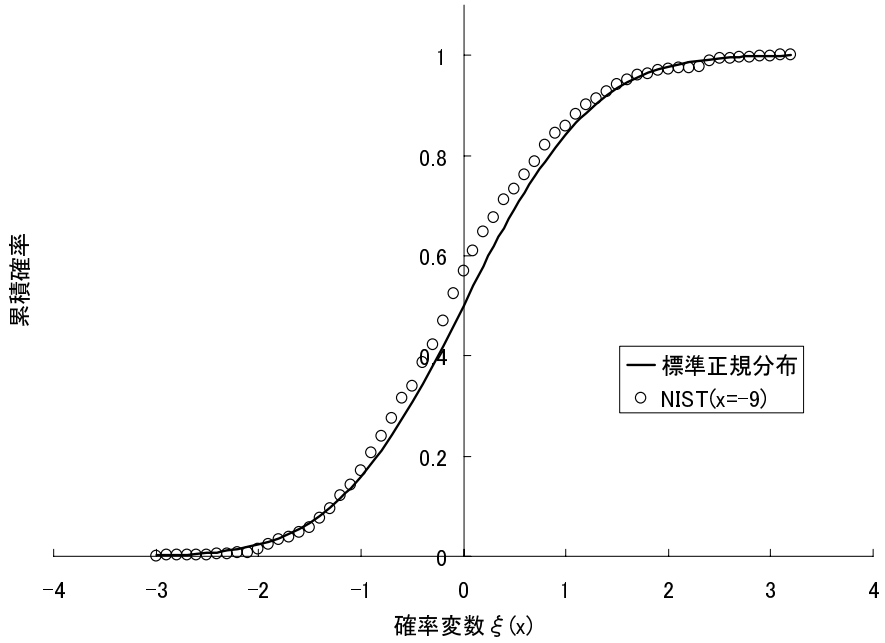


図 3.46: x=-9

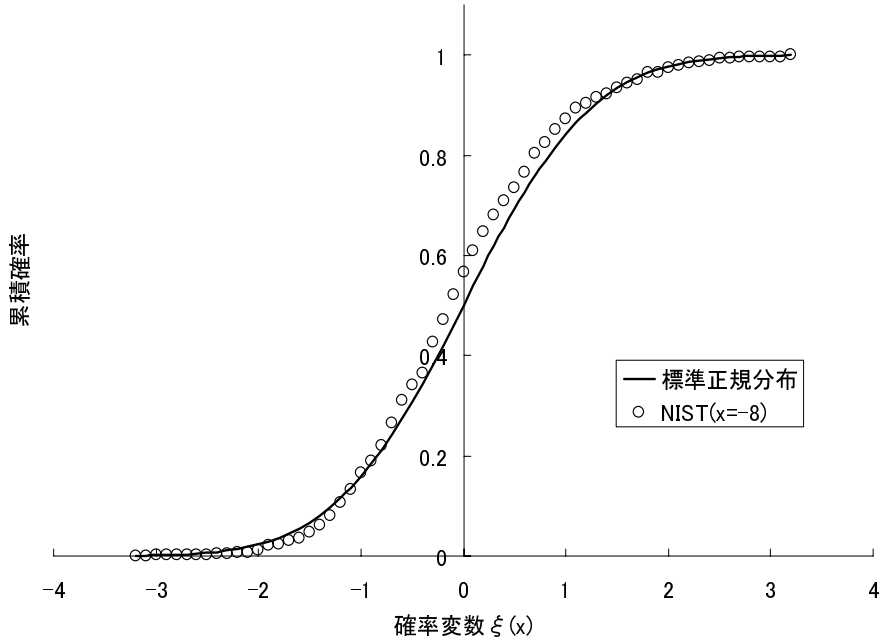


図 3.47: x=-8

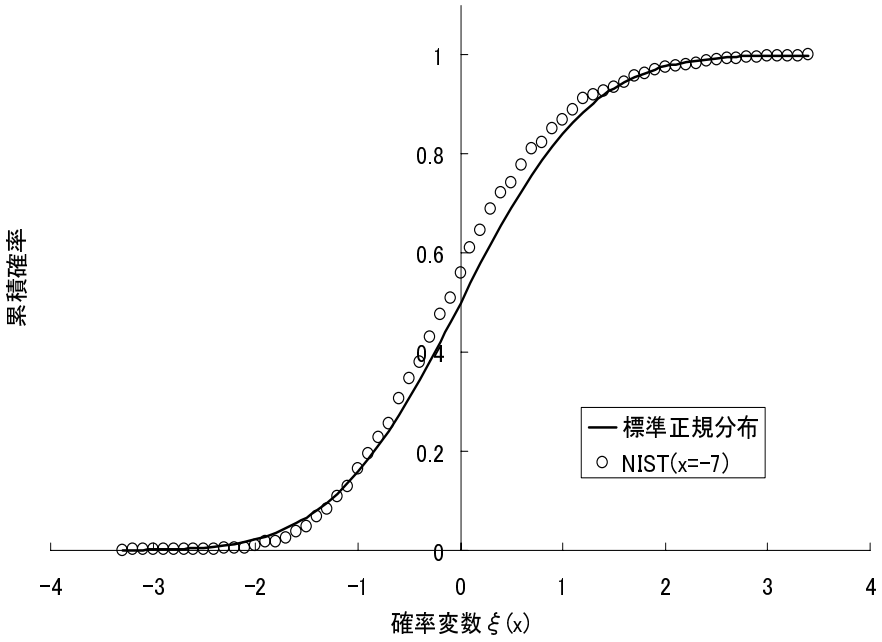


図 3.48: x=-7

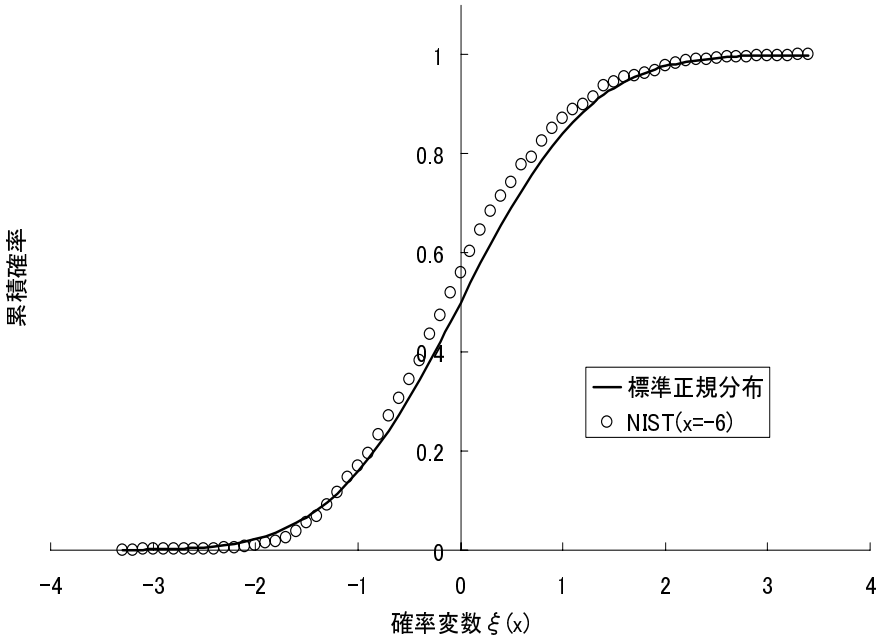


図 3.49: x=-6

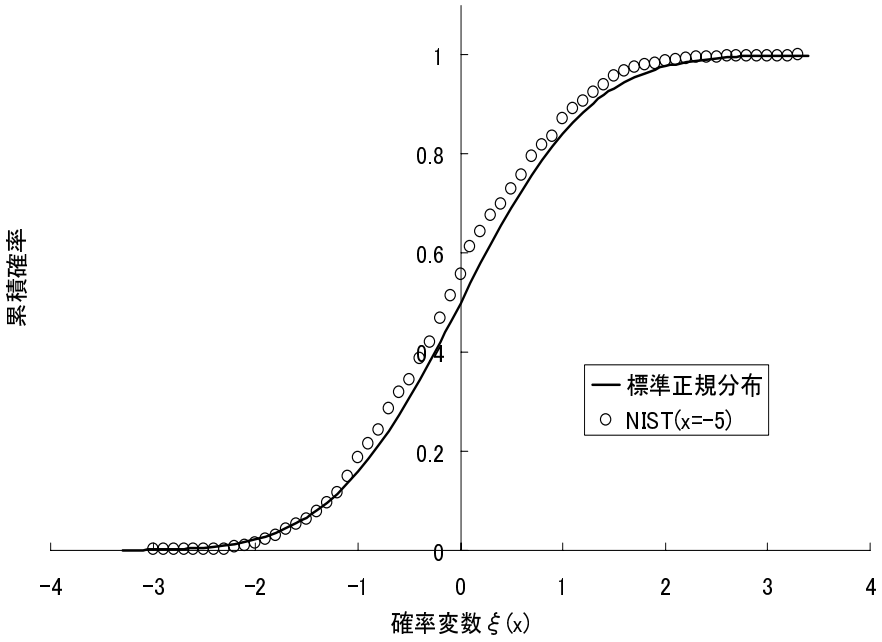


図 3.50: x=-5

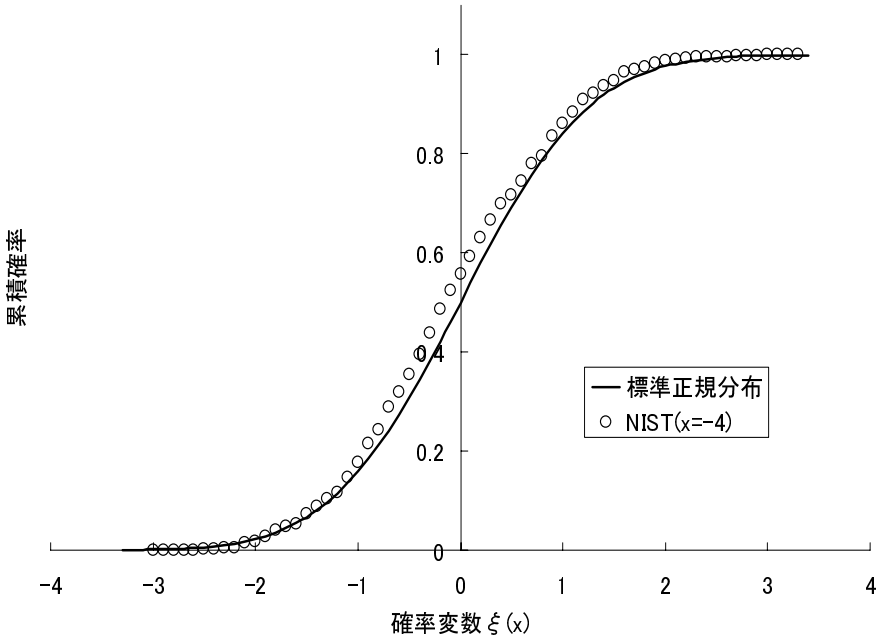


図 3.51: x=-4

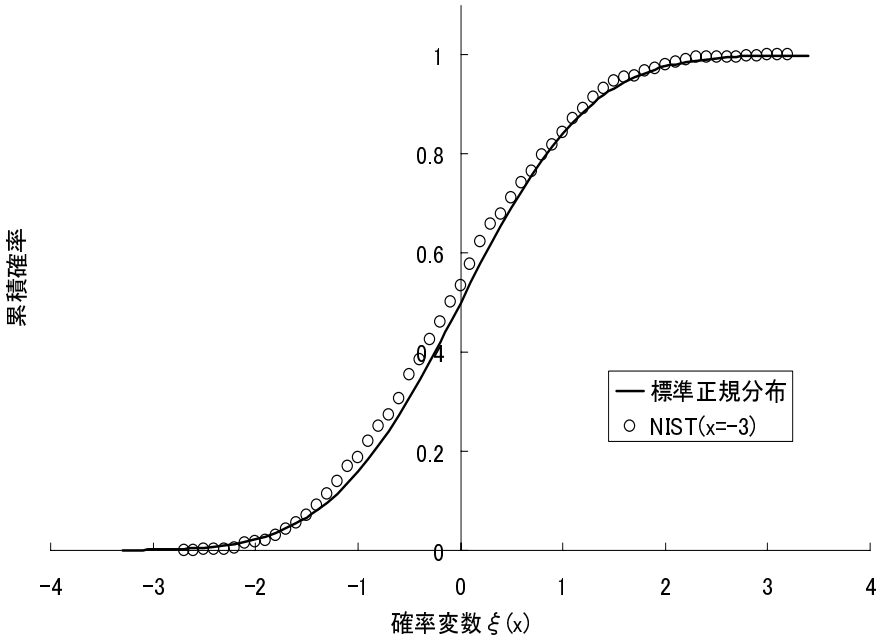


図 3.52: x=-3

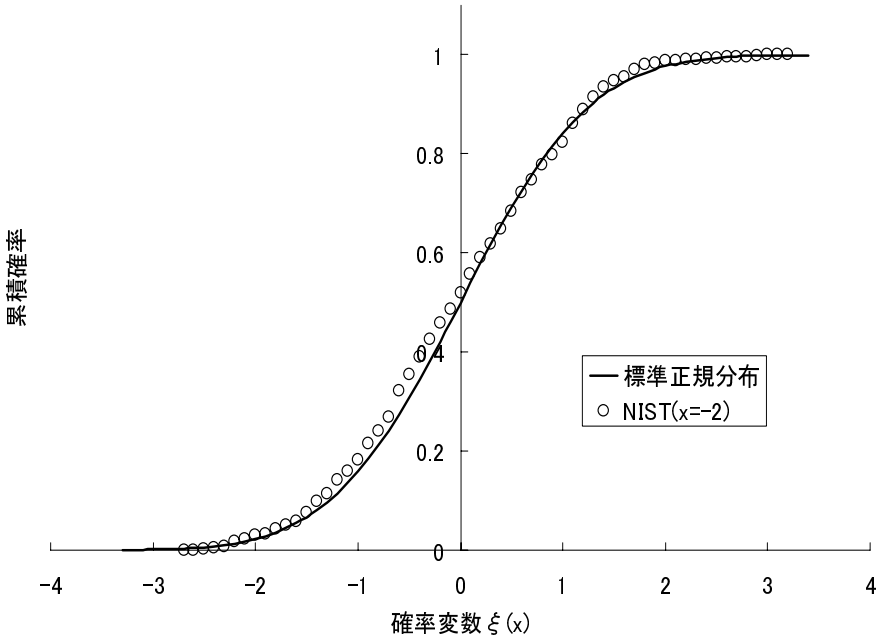


図 3.53: x=-2

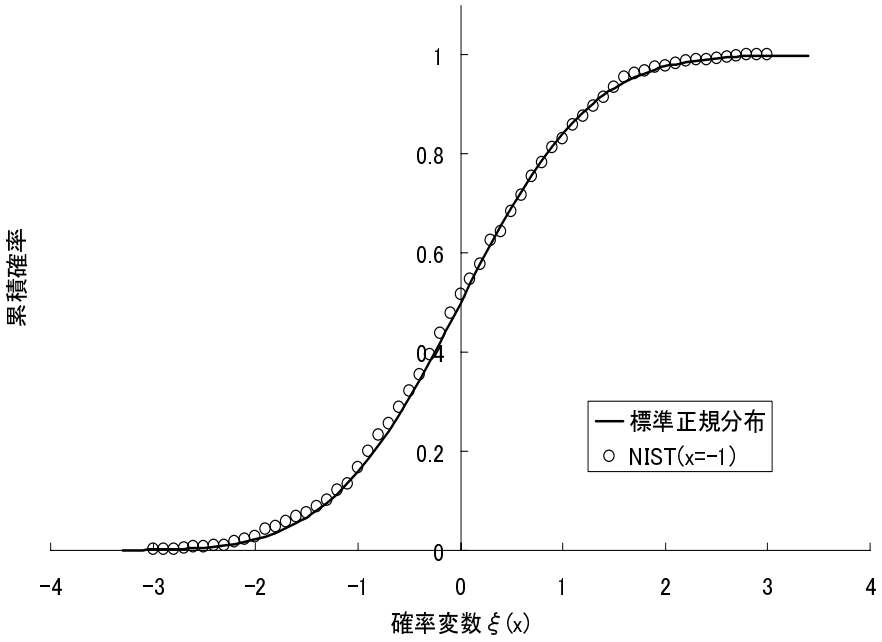


図 3.54: x=-1

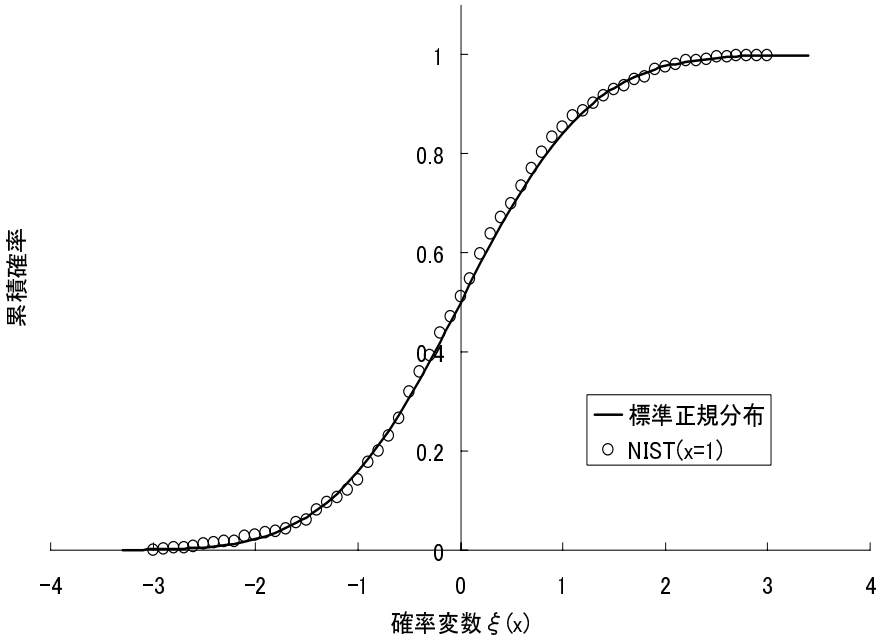


図 3.55: x=1

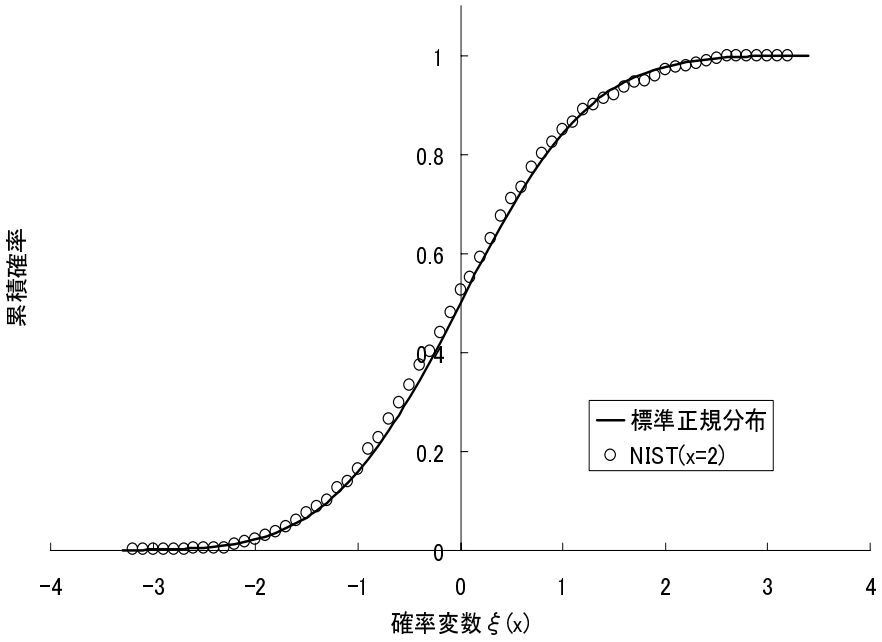


図 3.56: x=2

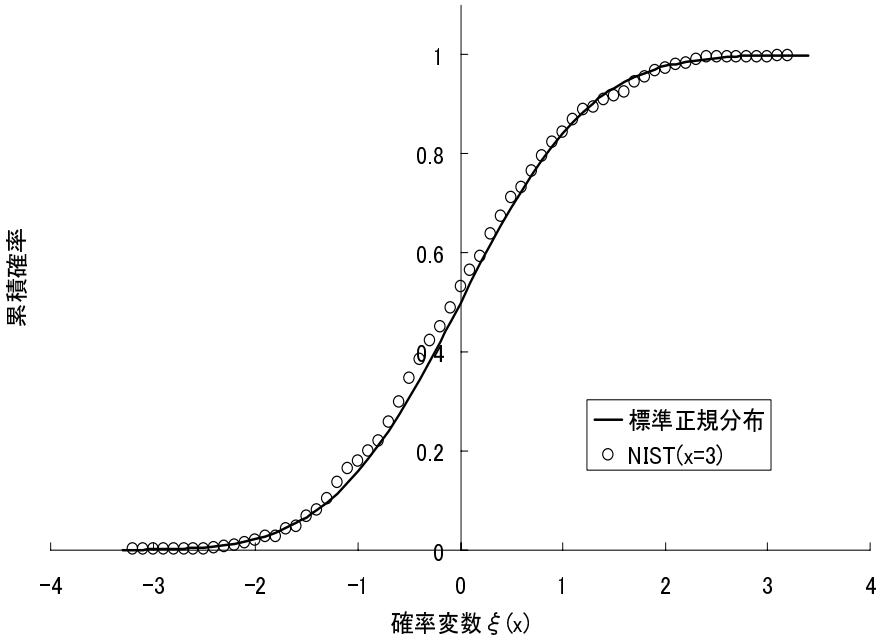


図 3.57: x=3

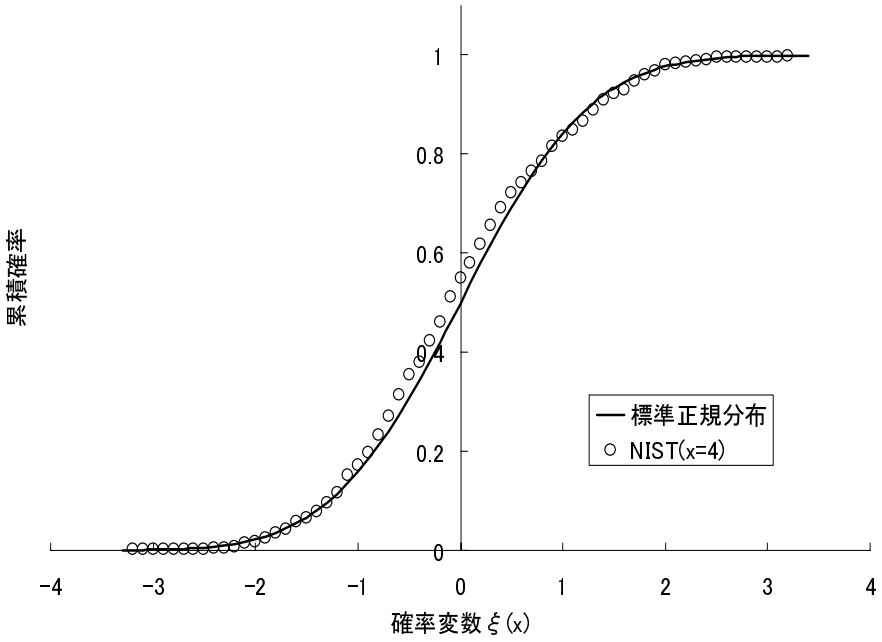


図 3.58: x=4

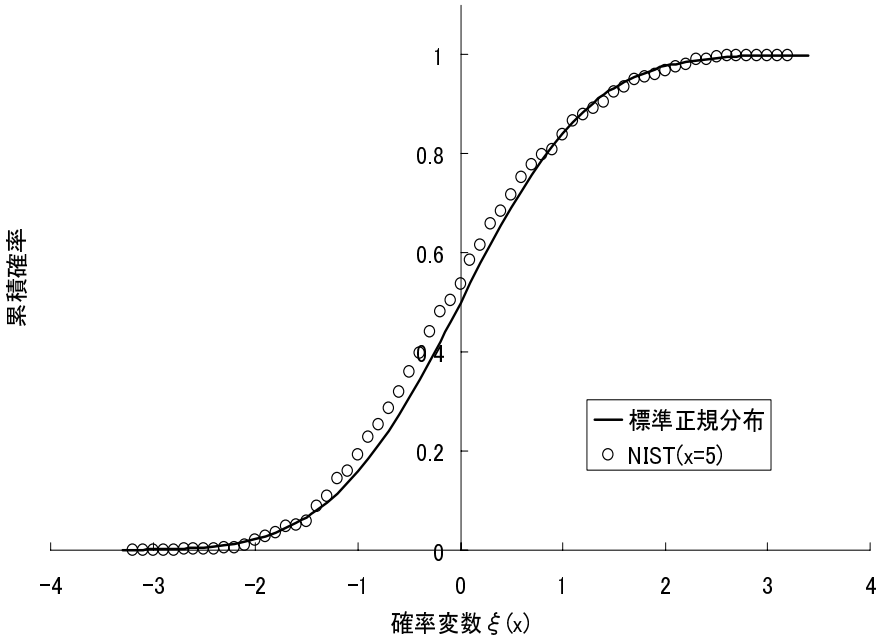


図 3.59: x=5

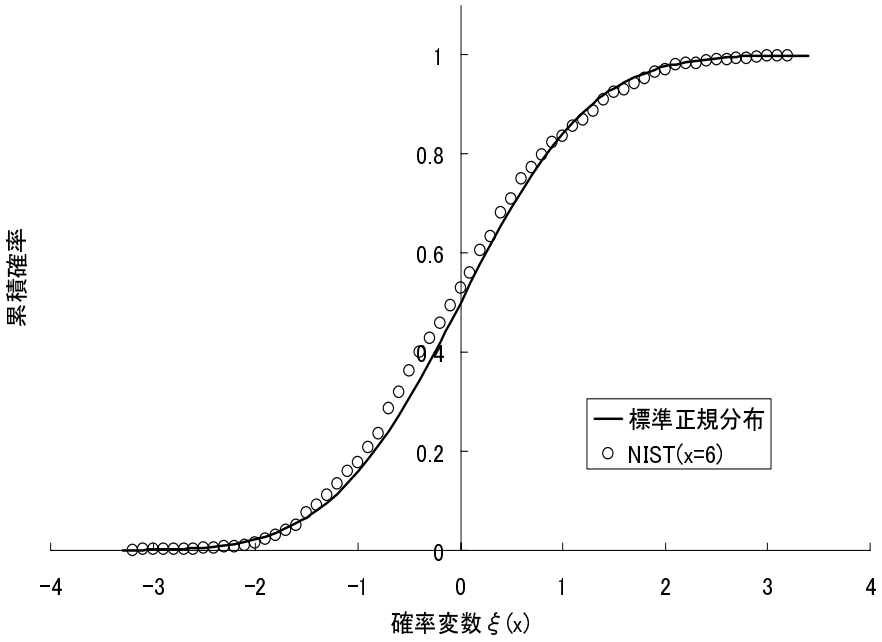


図 3.60: x=6

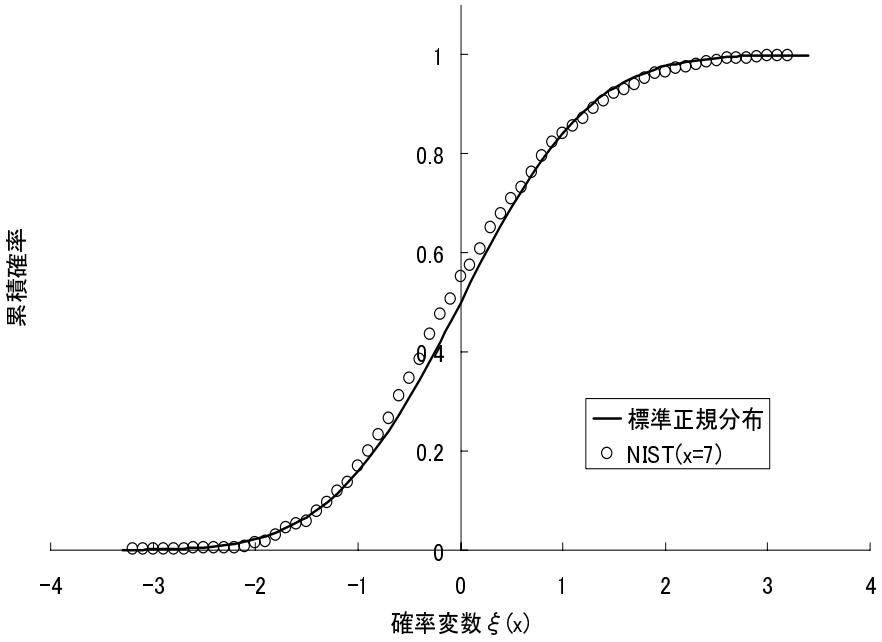


図 3.61: x=7

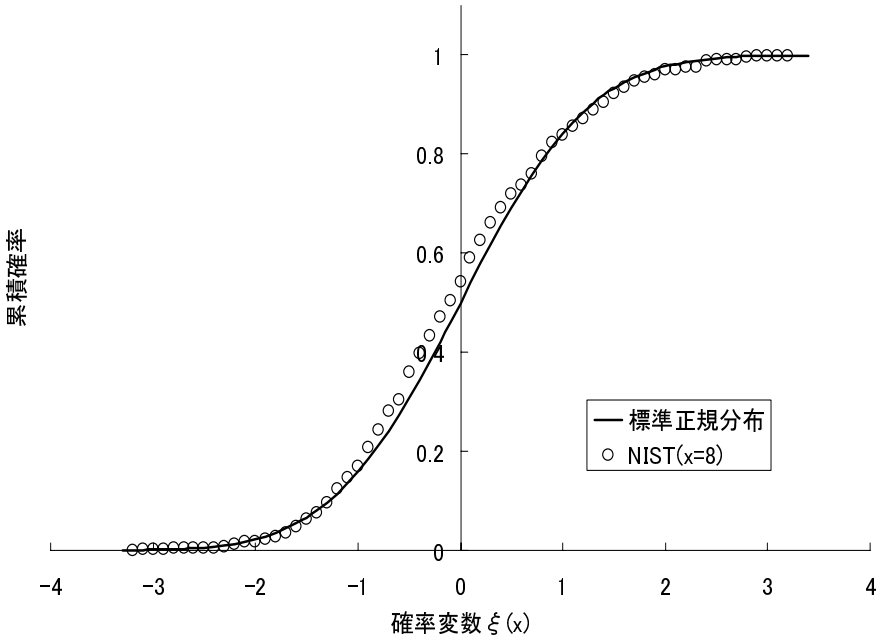


図 3.62: x=8

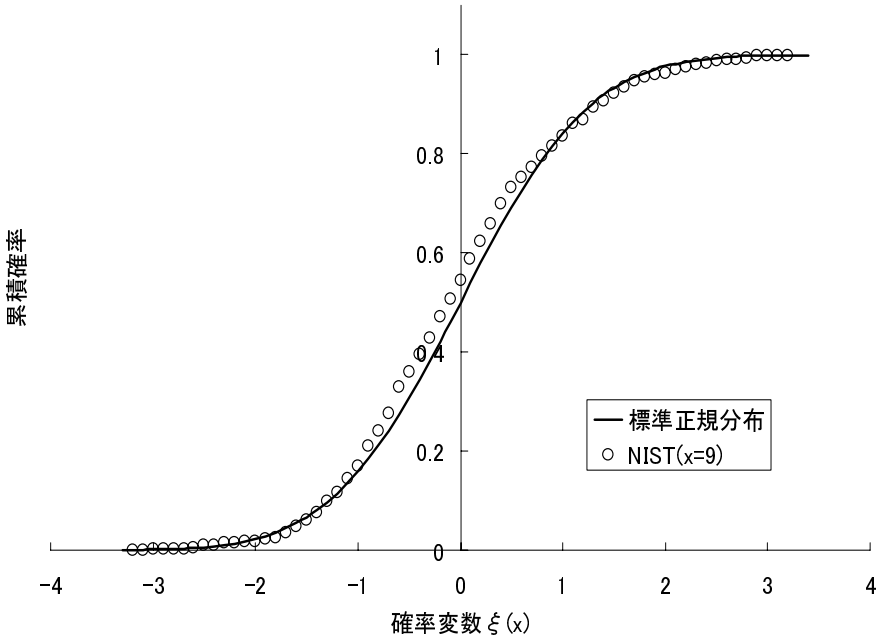


図 3.63: x=9

3.16.7　考察

推奨パラメータの範囲で実験を行い、基になる理論分布とほぼ合致しているが状態値 x の絶対値の値が大きいほど、理論分布から少し離れている傾向がある。

表１に状態値 z における確率変数 $\xi(x)$ の合計値を示す。これは、今回の実験では J<500 の数は標本数 1000 本中 362 本であったので、検定を行えた残りの標本数 638 本の合計値である。

状態値 x の絶対値の値が大きいほど、理論分布から少し離れている傾向があるのは、以下の表にもあらわれているように確率変数 $\xi(x)$ は状態値 x の出現度数を表しているので、状態値 x の絶対値の値が大きいほど出現度数は減り、実験データの信頼度が低くなるのが原因だと考えられる。

表１

状態値 x	-9	-8	-7	-6	-5	-4	-3	-2	-1
$\xi(x)$ の合計	724320	724656	727084	727097	726615	728543	731701	733840	736210
状態値 x	1	2	3	4	5	6	7	8	9
$\xi(x)$ の合計	736646	735149	733854	732732	730265	731111	731215	729142	728680

第4章　おわりに

本報告書ではSP 800-22の16種類の検定法に対し，その背景の理論分布と，実際の試験値の分布を実験的に比較し，検定法の理論的根拠の妥当性を調査した．ここでは，理想乱数源としてGenerator-Using SHA-1を仮定し，理論的に想定される統計量の分布と，実験結果の分布を比較し，その検定法の妥当性を調査した．パラメータの設定範囲は，SP 800-22で推奨されている値である．実験値が理論分布に合致しているかの判断は，分布曲線を比較し定性的におこなった．理由は以下である．

- Generator-Using SHA-1の理想性に関する疑問
- 実験分布と理論分布の一致性を合否検定すると、合格閾値の設定により細部の不一致が見過ごされる危険が有ること

実験結果として，DFT検定，Lempel-Ziv圧縮検定では，理論分布と試験値の分布に大きな違いが有ること．近似エントロピー検定において，推奨パラメータの一部においては，理論分布からの乖離が見られることがわかった．

現在までに，DFT検定，Lempel-Ziv圧縮検定に関し，疑問点の指摘が学会で行われている．これらの検定法と同程度の理論－実験分布曲線の乖離が見られた場合，合致していないと判断するならば，各種検定法の評価は以下である．

1. 頻度検定	○
2. ブロック単位の頻度検定	○
3. 連検定	○
4. ブロック単位の最長連検定	○
5. 2 値行列ランク検定	○
6. DFT 検定	× ※1
7. 重なりの無いテンプレート適合検定	○
8. 重なりのあるテンプレート適合検定	○
9. Maurer の「ユニバーサル統計量」検定	○
10. Lempel-Ziv 圧縮検定	× ※2
11. 線形複雑度検定	○
12. 系列頻度検定	○
13. 近似エントロピー検定	△ ※3
14. 累積和検定	○
15. ランダム回遊検定	○
16. 変形ランダム回遊検定	○

※1　長い系列長に対し理論分布の補正が必要
※2　有限長系列の分布に関する新たな理論解析
※3　推奨パラメータの設定条件を狭めた方が妥当

参考文献

[1] NIST, Special Publication 800-22, “ A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications ”, (http://csrc.nist.gov/rng/SP800-22b.pdf,
http://csrc.nist.gov/rng/errata2.pdf)

[2] NIST, Special Publication 800-22, “ NIST Statistical Test Suite ”,
(http://csrc.nist.gov/rng/sts-1.5.tar,
http://csrc.nist.gov/rng/rng2.html)

[3] 濱野健二, 佐藤史生, 石川正興, “ 離散フーリエ変換を用いた乱数検定（Randomness Test using Discrete Fourier Transform）”, 防衛庁技術研究本部技報第 6841 号, 平成 15 年 9 月

[4] 金成主, 梅野健, 長谷川晃朗, “ NIST のランダム性評価テストについて ”, 信学技報 Vol.103 No.499 ISEC2003-87（2003-12）

[5] 山本尚史, 金子敏信, “ NIST SP800-22 の DFT 検定に関する一考察 ”, 信学技報 Vol.104 No.200 ISEC2004-50（2004-07）, pp.61-64, 2004

[6] 金子敏信, “擬似乱数生成系の検定方法に関する調査報告書－ Lempel-Ziv 圧縮検定について－ ”, (http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/documents/
rep_ID0206.pdf,
http://cryptrec.nict.go.jp/PDF/wat-rep2003/rep_ID0206.pdf)

[7] 廣瀬勝一, “ 擬似乱数生成系の検定方法に関する調査 調査報告書 ”, (http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/documents
/rep_ID0207.pdf,
http://cryptrec.nict.go.jp/PDF/wat-rep2003/rep_ID0207.pdf)

[8] 情報処理振興事業協会 セキュリティセンター, “ 電子政府情報セキュリティ技術開発事業 擬似乱数検証ツールの調査開発 調査報告書 ”, (http://www.ipa.go.jp/security/fy14/crypto/pseudo_rundum/

rundum_inve.pdf)

[9] I.N.Kovalenko(1972), "Distribution of the linear rank of a random matrix", Theory of Probability and its Applications.17,pp.342-346.

[10] G.Marsaglia and L.H.Tsay(1985), "Matrices and the structure of random number sequences", Linear Algebra and its Applications.Vol.67,pp.147-156.

[11] O.Chrysaphinou and S.Papastavridis,"A Limit Theorem on the Number of Overlapping Appearances of a Pattern in a Sequence of Independent Trials." ,Probability Theory and Related Fields,Vol.79(1988),pp.129-143

[12] Ueli M.Maurer,"A Universal Statistical Test for Random Bit Generators",Journal of Cryptology.Vol.5,No.2,1992,pp.89-105

[13] J-S Coron and D.Naccache,"An Accurate Evaluation of Maurer's Universal Test",Proceedings of SAC'98(Lecture Notes in Computer Science),Berlin:Springer-Verlag,1998

[14] H. Gustafson, E. Dawson, L. Nielsen, and W. Caelli (1994), "A computer package for measuring the strength of encryption algorithms," Computers and Security. 13, pp. 687-697.

[15] R.A. Rueppel, Analysis and Design of Stream Ciphers. New York: Springer, 1986.

[16] M.Kimberley(1987), "Comparison of two Statistical tests for keystream sequences", Electronics Letters.23,pp.365-366.

[17] D.E.Knuth, "The Art of Computer Programming. Vol.2,3rd ed.Reading", Addison-Wesley,Inc.,pp.61-80

[18] A.J.Menezes,P.C.van Oorschot,and S.A.Vanstone(1997), "Handbook of Applied Cryptography.Boca Raton, FL", CRC Press,p.181

[19] I.J.Good(1953), "The serial test for sampling numbers and other tests for randomness", Proc.Cambridge Philos.Soc.. 47,pp.276-284

[20] S.Pincus and B.H.Singer,"Randomness and degrees of irregularity",Proc.Natl.Acad.Sci.USA.Vol93,March 1996,pp.2083-2088.

[21] A.Rukhin(2000),"Approximate entropy for testing randomness",Journal of Applied Probably.Vol.37,2000

[22] 森村英典,“ 確率・統計 ”, 朝倉書店

[23] Frank Spitzer,"Principles of Random Walk", Princceton, Van Nostrand, 1964(especially p.269)

[24] Pal Revesz, "Random Walk in Random And Non-Random Environments" Singapore, World Scientific, 1990

[25] NIST, " Randomness Testing of the Advanced Encryption Standard Candidate Algorithms ", (http://csrc.nist.gov/rng/AES-REPORT2.doc)

[26] NIST, " Randomness Testing of the Advanced Encryption Standard Finalist Candidates ", (http://csrc.nist.gov/rng/aes-report-final.doc)

[27] G.Marsaglia, " DIEHARD "
(http://stat.fsu.edu/～geo/diehard.html)

[28] D.E.Knuth, " The Art of Computer Programming Vol , Seminumerical Algorithms Third Edition ", Addison Wesley

[29] 伏見正則, " 乱数 ", 東京大学出版

[30] NIST, FIPS PUB 186-2, " Digital Signature Standard (DSS) ",
(http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf) , 2000