

(千葉大学学位申請論文)

1次元非線形写像を利用した擬似乱数生成系の解析法
および統計的乱数性の合理的な判定法に関する研究

2010年1月

千葉大学大学院理学研究科

基盤理学専攻 数学・情報数理学コース

奥富秀俊

あらまし

暗号理論／技術の役割は今日の高度情報化社会では極めて重要である。なかでも乱数は暗号理論／技術のあらゆる場面と密接な関係をもっている。最近では無線タグや低消費電力といった視点から、非線形写像のシンプルな構造を利用して擬似乱数を生成するといった研究がある。しかし現時点では解析面が不足している等の理由により広く認知された技術までには至っていない。本論文はこのような乱数の生成と評価に関する研究内容を述べたものであり、特に非線形写像を反復するたびに一部の値（ビット）を抽出して得られた擬似ランダムビット列に対する初期値推測法とパラメータ推測法について述べている。本生成系において初期値とパラメータはシード（鍵）依存値であることから、本推測法はその安全性解析と位置付けられる。本論文では更に、暗号技術分野で今日標準的に使われ、米国連邦政府が公開している NIST 亂数検定法（統計的乱数検定）に関する研究内容について述べている。特にこの NIST 亂数検定法に含まれる検定法の誤りに関し、著者らの報告も含め数多くの報告があること、また、NIST による最終的なランダム性の判定法が極めて曖昧であること等の課題がある点に着目し、NIST 亂数検定法を用いて合理的かつ明確にランダム性の判定を与えるための方法を提案している。そして経験的に良質だとされる（あるいは良質でないという報告のない）擬似乱数生成法を用いた判定例を用いて、提案した方法の妥当性を示している。

謝 辞

本研究を進めるにあたり、終始御理解ある指導と御助言をいただきました主任研究指導員（副査）の千葉大学中村勝洋教授に謹んで感謝申し上げます。中村教授には、進学以前から共同研究を介して多大なご支援をいただきました。改めて感謝いたします。また、本論文の審査を通じて適切な御助言を賜りました主査の千葉大学渚 勝教授、副査の西田康二教授、桜井貴文准教授、汪金芳准教授に心より感謝申し上げます。

本研究の遂行が困難だった初期から現在まで、深い御理解と暖かい御支援をいただきました新田基博氏（東芝情報システム（以降 TJ と表す））、白土浩氏（元 TJ 事業部長）、守谷岳雄氏（TJ 事業部長）に心より感謝申し上げます。また、本研究遂行の実質的なチャンスを与えていただいた情報処理推進機構（以降 IPA と表す）未踏ソフトウェア創造事業、並びに、当事業のプロジェクトマネージャを担当していただいた長谷川正治氏（元日本ルーセント・テクノロジー代表取締役副社長）に深謝いたします。特に、長谷川氏の御理解と新田氏の御尽力無しには、本研究の遂行は到底有り得ませんでした。改めて感謝の意を表したいと思います。

本研究を業務として遂行する機会を与えていただいた六反田喬氏（元 TJ 取締役社長）、常岡正義氏（元 TJ 取締役）、並びに、御助言を賜りました才所敏明氏（元東芝ソリューションセンター長）、川村信一氏（東芝研究開発センター／産業技術総合研究所）、大熊建司氏（東芝研究開発センター／IPA）、香田徹氏（九州大学教授）に謹んで感謝申し上げます。特に六反田氏には中村教授との運命的な出会いを作っていました。また、常岡氏には中村教授との共同研究の遂行と事業化の両立に向けて多大なる御支援と御指導をいただきました。改めて感謝申し上げます。

事業面でお世話になった TJ（旧）開発営業部の和田秀逸氏（元事業部長）、石井直史氏、細目紀子氏、中澤章氏、前田直樹氏、並びに、技術開発面の担当をしていただきました TJ 大石武彦氏、関根正騎氏、（故）大岸伸之氏に心から感謝申し上げます。製品化に関して、多くの皆様にお世話になりました。また、活発な議論をすることができました。皆様との取り組みは一生忘れることができないと思います。皆様には厚くお礼を申し上げたいと思います。

本研究のよき理解者であり、よきパートナーである TJ の岩野隆氏、金田学氏、並びに、本研究関連について多くのディスカッションとアドバイスを賜りました糸井千岳氏（日本大学理工学部教授）、著者の修士課程在学中の担当指導員であり、修了後も都度相談させていただいた相澤正満氏（日本大学理工学部教授）、川上一郎氏（元日本大学理工学部教授）に深謝致します。

博士課程進学に関して寛大なる御理解と御支援を頂きました TJ 田窪譲二氏（常務取締役）、大関勝巳氏（室長）、大西裕氏（部長）、浅川一満氏（部長）、上河俊介氏（グループ長）に感謝申し上げます。特に浅川氏には、業務に就きながら課程博士として進学するという難しい側面に関して、都度柔軟な解決策を思案していただきました。深々とお礼を申し上げたいと思います。

最後に、幼少の折より理数系の道へ進む動機を与えていただき、そして、信念を持ち継続することの重要さを教えていただいた両親に感謝致します。特に父には特許取得の知恵を拝借し、一連の研究の全ての段階において適切なアドバイスいただきました。改めて感謝致します。

2010 年 2 月 奥富秀俊

目次

あらまし	i
謝 辞	iii
第 1 章 序 論	1
1.1 研究の背景	1
1.2 研究課題の所在	1
1.3 本論文の構成	4
第 2 章 非線形写像を利用した擬似ランダムビット列の生成について	7
2.1 1 次元非線形写像の反復により得られる系列	7
2.2 パラメータ $a = 2$ のテント写像	12
2.3 パラメータ $a \leq 1$ および $a > 2$ のテント写像	13
2.4 パラメータ $1 < a < 2$ のテント写像	14
2.4.1 数値実験による周期長の探索について	15
2.4.2 数値実験による経験分布の偏り（軌道 $\{x_i\}$ の偏り）について	21
2.5 テント写像を利用した擬似ランダムビット列の生成に関する初步的な案とその乱数検定結果	24
第 3 章 1 次元非線形写像から得られる擬似ランダムビット列に対する初期値推測法およびパラメータ推測法	27
3.1 初期値推測法とは	27
3.1.1 初期値推測法とは	27
3.1.2 初期値推測法の先行研究	28
3.2 テント写像の最上位ビット抽出系列に対する初期値推測法(必要条件からの解)[23],[26]	30
3.2.1 観測ビット列を用いた最終値 $x_n = f^n(x_0)$ の多項式関数形の決定	31
3.2.2 最終値 $x_n = f_a^n(x_0)$ の存在範囲の必要条件から得た初期値解	33
3.2.3 本節のまとめ	34
3.3 $a = 2$ のテント写像の最上位ビット抽出系列に対する初期値推測法（厳密な解）[26]	34
3.3.1 区間から区間への写像の連鎖の様子～状態遷移図	34
3.3.2 状態遷移図を用いた最終値 $x_n = f_a^n(x_0)$ の厳密な存在範囲の取得	35
3.3.3 必要十分性を考慮した初期値解	36
3.3.4 本節のまとめ	37

3.4	$1 < a < 2$ のテント写像の最上位ビット抽出系列に対する初期値推測法（厳密な解） [26]	37
3.4.1	区間から区間への写像の連鎖の様子	37
3.4.2	Type-0 の分離および初期値解	39
3.4.3	区間 A 内、区間 B 内での遷移	40
3.4.4	区間 A_1 から 区間 B' への遷移	41
3.4.5	区間 B_1, B'_1 から 区間 RA, RA' への遷移	42
3.4.6	状態遷移図を用いた最終値 $x_n = f_a^n(x_0)$ の厳密な存在範囲の取得	44
3.4.7	Type-1 の初期値解	45
3.4.8	Type-2 の初期値解	46
3.4.9	Type-3 の初期値解	46
3.4.10	本節のまとめ	47
3.5	テント写像の任意のビット桁（上位 t 桁目のビット / 下位側のビット）を抽出した系列に対する初期値推測法 [24],[25]	49
3.5.1	$a = 2$ のテント写像の任意のビット桁抽出系列に対する初期値推測法 [24]	49
3.5.2	$1 < a < 2$ のテント写像の任意のビット桁抽出系列に対する初期値推測法 [25]	53
3.5.3	下位側を抽出した系列に対する初期値推測法に関する考察	57
3.5.4	本節のまとめ	58
3.6	生成法が有限精度で実装された場合の初期値推測法 [27]	59
3.6.1	有限精度のテント写像モデル	59
3.6.2	有限精度のテント写像モデルの n 回反復写像と観測ビット列の関係	60
3.6.3	有限精度のテント写像モデルから生成されたランダムビット列の初期値推測	63
3.6.4	無限精度で実装された生成法の場合の初期値解からの乖離 $D/(qa^n)$ の大きさについて	64
3.6.5	観測ビット列の長さが十分に長い場合（写像の反復回数 n が大きい場合）について	65
3.6.6	本節のまとめ	66
3.7	パラメータ推測法とは	67
3.8	テント写像の最上位ビット抽出系列に対するパラメータ推測法 [23]	67
3.9	Wu らのパラメータの推測法 [22]	68
3.10	本章で示した推測法（3.3 節～3.9 節）の性能および考察	70
3.10.1	最上位ビットを抽出した系列に対する初期値推測法（3.3 節,3.4 節）により推測可能な範囲	70
3.10.2	任意桁目のビット（上位 k 桁目のビット / 下位側のビット）を抽出した系列に対する初期値推測法（3.5 節）により推測可能な範囲	71
3.10.3	有限精度で実装された生成法から得られる系列に対する初期値推測法（3.6 節）により推測可能な範囲	72
3.10.4	有限精度の場合（最上位ビット抽出）でも初期値候補を数点に絞り込むことができるこの理由に関する考察	75
3.10.5	Wu らのパラメータの推測法（3.9 節）の性能 / 推測可能な範囲 [28]	77

第 4 章	解析法の視点から考えた解析が困難となるケースについて	81
4.1	各推測法の視点において推測が困難となる場合	81
4.1.1	最上位ビット抽出系列に対する初期値推測法 , パラメータ推測法の観点	81
4.1.2	任意桁目のビット (上位 k ビット桁目 / 下位側ビット) 抽出系列に対する初期値推測法 , パラメータ推測法の観点	82
4.1.3	Wu らのパラメータ推測法の観点	85
4.1.4	その他 , 有限精度の場合のテント写像の特性から考えた留意点	85
4.2	各推測法の視点において推測が困難となる擬似乱数生成アルゴリズムの一例	86
第 5 章	NIST 亂数検定 [46][47] を用いた合理的なランダム性の判定法についての研究	91
5.1	NIST 亂数検定に含まれる検定法誤り ~ 本研究に至る経緯について	91
5.2	NIST 亂数検定の概要	92
5.2.1	NIST 亂数検定の手順	92
5.2.2	Proportion 評価の曖昧さ	94
5.2.3	全ての検定項目が Proportion 評価で合格する確率の概算	95
5.2.4	概算に基づく評価とその不十分性	96
5.3	NIST 亂数検定を用いたランダム性の合理的な判定法についての提案 [70]	97
5.3.1	前提条件	97
5.3.2	提案する判定法の概要	97
5.3.3	本判定法で得られる p-value について	98
5.3.4	個々の検定項目毎のランダム性の判定	98
5.3.5	全体評価 ~ 亂数生成法の最終評価	99
5.4	本判定法を用いたランダム性の評価実験	100
5.4.1	第 1 段階の検定に誤りがある検定項目の実験結果の説明	100
5.4.2	第 1 段階の検定に誤りがない検定項目の実験結果の説明	105
5.4.3	全体的な評価 ~ 亂数生成法の最終判定	106
5.5	本判定法に関する考察	107
5.5.1	個々の検定法の誤りや誤差の影響	107
5.5.2	グレーゾーンについて	107
5.5.3	本判定法のもう 1 つの側面	108
5.6	本章のまとめ	108
第 6 章	結論	109
付録 A	力オス数理に関する諸定義 , 定理類	111
A.1	位相共役 (位相同形)	111
A.1.1	パラメータ $b = 4$ のロジスティック写像 L_4 とパラメータ $a = 2$ のテント写像 f_2 の位相共役の関係 h	111
A.1.2	パラメータ $b = 4$ のロジスティック写像 L_4 とパラメータ $c = 2$ の平方写像 Q_2 の位相共役の関係 h	112
A.2	リヤプノフ指数	112

A.2.1	傾き $1 < a \leq 2$ のテント型写像における初期誤差の広がり	113
付録 B	グレイコードおよびグレイコードに基づく推測法に関する付録	115
B.1	Baptista, および Alvarez らによる 1 次元非線形写像を利用した暗号化手法 [32][33]	115
B.2	グレイコード (Gray Code) [31]	115
B.2.1	グレイコードについて	115
B.3	平方写像の最上位ビット抽出系列とグレイコードの関係	116
B.4	Alvarez らの, 平方写像からの最上位ビット抽出系列に対するグレイコードに基づく 初期値推測法 [21]	120
B.5	テント写像の最上位ビット抽出系列とグレイコードの関係	123
付録 C	NIST 乱数検定 / 統計検定に関する付録	127
C.1	提案する判定法において, p-value が限りなく 1 または 0 に近い場合として考えられ るパターン	127
C.2	提案する判定法によるランダム性判定実験結果 (全データ)	127
参考文献		133

第 1 章

序 論

1.1 研究の背景

インターネットが一般に普及してから 10 年以上が経過する。以後現在に至るまでの間に通信速度の改善と、携帯インフラを巻き込むことによって利便性が劇的に向上した。今やネットショッピング、ホテルや航空機の予約、オンラインバンキングなど日常生活に欠かせないものとなった。このなかには個人情報や金銭に関するデータをやりとりする場面が少なくない。この高度情報化社会を陰で支えているのが情報セキュリティ技術であり、中でもネットワーク上で個人を特定／認証する技術、機密情報を保護する技術、情報の破壊や改ざんを検知する技術は暗号技術と呼ばれる情報セキュリティ技術の中核部を成す。暗号技術の中でも「乱数」は重要な要素技術の 1 つであり、例えば安全な鍵の発行のために乱数が利用され、安全な通信を開始する際に乱数が利用される。共通鍵ブロック暗号ではそれ自体がランダム変換であり、あるシステムは理想的な乱数が与えられることが前提となる等、乱数は暗号技術の様々な場面との密接な関係がある。また、最近では、無線タグや低消費電力といった視点での軽量なモジュールが望まれており、非線形写像の反復というシンプルな構造にて得られるカオス的な系列を擬似乱数生成法として応用しようという取り組みがある。これらは初期条件に敏感に反応する性質を有しており、初期値にわずかな差を与えるだけで全く異なる系列を生成できることから、擬似ランダムビット列の生成源としての利用が期待される。しかし現時点では解析法が不十分である等から安全性の評価が遅れ気味であり、この関係で実用化に至っていないことが課題となっている。

1.2 研究課題の所在

非線形写像と擬似ランダムビット列の関係については、古くから、パラメータ $a = 2$ のテント写像（式（1.1））、およびこれと位相共役（付録 A.1）の関係にあるパラメータ $b = 4$ のロジスティック写像（式（1.2））、パラメータ $c = 2$ の平方写像（式（1.3））等を反復する度に得られる値 x_i の最上位ビット（2進小数点数の小数点以下の最上位桁のビット）を抽出して構成されたビット列 $\{b_i\}$ は、0,1 の出現確率が等しい理想的なランダムビット列であること（ベルヌーイ試行の結果として得られる系列と

等価であること)が知られている[1]~[7].

$$f_a(x) = \begin{cases} ax & (0 \leq x < 1/2) \\ a(1-x) & (1/2 \leq x \leq 1) \end{cases} \quad (1.1)$$

$$L_b(x) = bx(1-x) \quad (1.2)$$

$$Q_c(x) = x^2 - c \quad (1.3)$$

ただし、これには留意すべき点があり、ビット列生成法、すなわち、式(1.1)~式(1.3)の写像が無限の演算精度で実装されている場合に限られる。有限精度で実装した場合は、パラメータ $a = 2$ のテント写像の場合であれば、演算精度に相応したごく短い回数の写像後に必ず固定点 $x = 0$ に落ち込む。従って、ベルヌーイ試行の結果として得られる系列と等価でありうるのは、初期の短い回数の写像までに得られる系列に限られる。パラメータ $b = 4$ のロジスティック写像の場合は、数値実験によって得られた経験的な性質として、

- 最終的に初期値に依存した周期軌道に至る
- 周期軌道は複数個現れ。周期長の短いものから長いものまである
- 演算精度を変化させると初期値と周期軌道の対応関係が変化する

が挙げられる[42]~[45]。つまり、異なる初期値であっても同一の周期軌道に陥る可能性が高いため、有限精度で実装する場合には系の制御が難しいと考えられる[10]。また、 $a = 2$ のテント写像、 $b = 4$ のロジスティック写像、 $c = 2$ の平方写像を反復する度に最上位ビットを抽出して得られた系列を擬似ランダムビット列とした場合は、その解析面から、記号力学に基づく初期値推測法[18]、グレイコードに基づく初期値推測法[21]によって、当該系列を生成し得る初期値範囲をほぼ厳密^{*1}に得ることができる。従って、写像の度に単純に最上位ビットを抽出した系列を擬似ランダムビット列とするだけでは安全ではないといえる。

一方で、パラメータ $a < 2$ のテント写像、およびパラメータ $b < 4$ のロジスティック写像から得られる系列の頻度分布には偏りがあることが知られている[8],[9]。この関係で、任意のパラメータにおけるテント写像やロジスティック写像を擬似乱数生成源として積極的に利用することは検討されてこなかったと考えられる。最近の研究によると、中位桁以下の下位側のビットを抽出した場合であれば、有限精度で実装した場合であっても、0,1の出現頻度が等頻度に近づく傾向にあることが経験的に判ってきた[36]~[40]。特に $a < 2$ のテント写像は固定点 $x = 0$ へ落ち込むパスが無いため、 $a = 2$ に比べて系列長の長いランダム系列を得ることができる。さらに、所定回数の写像後に内部状態を変化させる等の手法を併用することによって、比較的小さな演算精度の場合でも、統計的視点で良質なランダムビット列が生成できることが経験的に判ってきた[11], [13]~[17]。しかしながら、これらの生成系が安全であるかの視点では述べられていない。

上記の生成系を実用化へ導くためには(実用性を見定めるためには)、統計的視点による評価(乱数検定)以外に、上記生成系に対する基本的な解析法を得ることと、解析法を得た上で安全性に関する理論的視点による評価を与えることが必要である。尚、上記の生成系は、初期値およびパラメータがシード(鍵)と関係する値と考えられることから、擬似ランダムビット列生成法と、当生成法によ

^{*1} 「ほぼ厳密に」の意味は、当推測法により得られる初期値範囲の境界を含む場合もあれば含まない場合もあることを意味する。

り生成された擬似ランダムビット列が既知情報として与えられたときに、当該系列を生成し得る初期値およびパラメータを推測することが重要だと考えられる。しかし、任意のパラメータにおけるテント写像やロジスティック写像の一般的な性質が十分に理解され整理されていないこと、また、テント写像やロジスティック写像の有する初期条件に鋭敏な性質により、有限精度で実装された場合に得られる系列と無限精度で実装された場合に得られる系列とでは全く異なる系列となってしまう等の理由により、解析法に関する研究が遅れ気味である。この関係で、生成法が有限精度で実装され、かつ、任意の初期値と任意のパラメータ ($1 < a < 2$, $3.5 < b < 4$) が選ばれ、かつ、任意桁目のビットが抽出された場合の一般的なケースについての初期値またはパラメータを推測する手法は存在しない。ただ、限定的な条件下において初期値、またはパラメータを推測する手法が示されていた [19] ~ [22], [29] ~ [34]。しかし、推測範囲が厳密でない場合が多く、また、基本的に無限精度と有限精度を区別していないこともあり、推測に必要な計算量（探索量）等が明確に示されていない。本論文では、非線形写像のごく単純な例であるテント写像を例に挙げ、任意のパラメータのテント写像を写像する毎に最上位ビット、或は任意桁目のビットを抽出するといったごく単純な擬似ランダムビット列生成法を考える。そして、当生成法が無限精度で実装された場合に得られる擬似ランダムビット列が与えられたときに、当該系列を生成し得る初期値の推測手法、および、パラメータの推測法について述べる。また、当生成法が有限精度で実装された場合に得られる擬似ランダムビット列に対する初期値解の性質について述べる。さらに、初期値 / パラメータを 1 点に絞り込むまでに必要な計算量（探索量）について述べ、最後に推測が困難となるケースを整理して、本論文で扱った推測法による解析を困難とするような擬似ランダムビット列生成法の一例を示す。

前述までの内容は、テント写像を利用した生成法のみを対象とする理論的な評価法であった。一般的な擬似ランダムビット列生成法についても適用できる統計的な評価法として乱数検定法がある。今日では、NIST^{*2} が定める SP.800-22[46][47] が広く使われている。本論文では、NIST SP.800-22 を NIST 亂数検定と呼ぶことにする。NIST 亂数検定は、現在計 15 の検定法、計 188 の検定項目で構成される。各検定項目を実施することを第 1 段階の検定とすると、第 1 段階の検定結果を束ねた統計量を用いて第 2 段階の検定を実施し、第 2 段階の検定結果をもとに最終的な評価を与える仕組みとなっている（第 2 段階の検定とは文献 [46][47] の Uniformity と Proportion に相当する）。

NIST 亂数検定は、発表当初から現在に至るまでに、著者らを含む多くの研究者によって、個々の検定法（第 1 段階の検定）に関する誤りの指摘や修正に関する多くの報告がなされている [48] ~ [66]。しかし、現時点では、NIST が正式に対応した修正は少ないため、このことを知らない利用者は正確な検定を行っていないことになる。さらに著者らは、最終的な評価（第 2 段階の検定）を与える際の Proportion 評価が、極めて曖昧に終わっていると考えている。本論文では、まず、個々の検定法の修正状況について整理し、次いで、NIST が示す Proportion 評価は曖昧に終わっていることの理由を述べる。次いで、合理的かつ明確にランダム性を判定するための一案について述べる。最後に、本判定法案を利用した判定実験例を示し、本判定法案の妥当性を示す。

^{*2} National Institute of Standards and Technology (NIST) で「米国標準技術局」と訳される

1.3 本論文の構成

本論文は乱数の生成と評価に関する内容を述べたものである。生成法に関しては特に非線形写像を利用した擬似乱数生成法に焦点を当てている。理論的な評価に関しては、非線形写像を利用したごく単純な生成法のモデルを定義し、当生成法から得られる擬似ランダムビット列が既知情報として与えられたときに、当該系列を生成し得る初期値推測法とパラメータ推測法について述べる。最後に推測が困難となるケースについて整理し、推測が困難となるような擬似ランダムビット列生成法の一例を挙げる。本生成系では初期値とパラメータはシード（鍵）と関係する値である。従って、ここで述べる推測法は安全性解析と関係する内容であるためその検討意義は大きい。統計的な評価に関しては、暗号技術分野で今日標準的に使われている NIST 亂数検定法について触れる。NIST 亂数検定に含まれる検定法には誤りが含まれるとの報告が多くあるため、その修正状況について整理する。さらに NIST による最終的な判定法が極めて曖昧であることを述べ、NIST 亂数検定法を用いて合理的かつ明確にランダム性の判定を与えるための一案について述べる。

各章の構成は以下である。

第2章では、はじめにテント写像やロジスティック写像から得られる系列がランダムな挙動を呈することや初期条件に敏感な性質等を示し、これらの系列をランダムビット列の生成源（抽出源）として利用する案について触れる。一方で、写像のパラメータに任意の値を選んだ場合（テント写像の場合は $1 < a < 2$ に相当する）は、周期長の見積もりが困難であること、また、最上位ビットに偏りが生じる等の性質を有することから、数值実験の結果として経験的に得られたデータに基づき、テント写像から擬似ランダムビット列を生成するまでの留意点について記す。本章の最後では当該留意点を考慮して生成された系列が統計的に良質なランダム性を有すること（乱数検定の結果）を示す。

第3章では、テント写像から得られた擬似ランダムビット列に対する初期値推測法とパラメータ推測法について述べる。

第3章の前半では、はじめに比較的簡単に得ることができる必要条件のみを考慮した場合の初期値推測法を述べる。次に、十分条件を考慮することによって得られる厳密な初期値解を示す。一般的に十分条件を得ることは容易なことではないが、本論文では部分分割した区間から区間への写像の関係を調べ上げ、最終的に区間から区間の推移（写像の連鎖）を「状態遷移」として整理することができたために容易に達成することができる事を示す。次いで任意のビット桁を抽出した場合の推測法を示す。任意ビット桁抽出の場合は推測範囲が多数箇所に膨れ上がり、与えられた擬似ランダムビット列の生成に実際に使われた初期値が含まれる範囲を一意的に絞り込むことはできないことを示す。次いで、生成法が有限精度の計算機に実装された場合に得られる系列を対象とした初期値推測法を示す。有限精度を考慮する理由は、テント写像は初期条件鋭敏性を有するため、演算精度を考慮した場合とそうでない場合では（無限精度と有限精度とでは）全く異なる系列となるためである。

第3章の後半では、パラメータ推測法について述べる。パラメータの推測に関しても、前章で示した初期値推測法と同じ推測式および「状態遷移」を利用する。初期値の推測の場合は、当推測式をパラメータが既知のもとで初期値について解くことによって得た点に対し、パラメータの推測の場合は、当推測式を初期値が既知ものとでパラメータについて解くことによって得られることを示す。また、

参考のため，Wu らによって示されるグレイコードを利用したパラメータ推測法を述べる。Wu らの推測法は，初期値が未知のもとでパラメータを推測する手法であるため，解析法としては，より現実的なケースを想定したものといえる。

第 3 章の最後に，本章で述べた初期値推測法によって推測可能なこと（推測可能な範囲），ならびに，推測のために必要となる探索量について触れる。

第 4 章では，第 3 章で述べた推測法の視点において，改めて推測が困難となる場合について整理する。そして，ここで述べた推測法により解析が困難となるような擬似ランダムビット列生成法の一例を挙げ，当生成法の評価（推測に必要な計算量と乱数検定結果）を与える。

第 5 章では，NIST 亂数検定を利用した統計的なランダム性の判定を合理的に与える手法について述べる。情報セキュリティ分野においては NIST 亂数検定がほぼ標準的に使われているが，NIST 亂数検定に含まれる個々の検定法（本論文では第 1 段階の検定と呼ぶ）には誤りが含まれるという報告が多くある。はじめに現時点での修正に関する情報を整理する。次いで，NIST が示す最終判定（本論文では第 2 段階の検定と呼ぶ）は極めて曖昧であることを述べ，個々の検定法（第 1 段階の検定）にはまだ誤りが含まれる可能性があることを考慮した上で合理的に最終判定を与える方法の提案について述べる。そして，本案によるランダム性の判定例をいくつか記す。最後に本研究を通して得た内容からのまとめを述べる。

第 6 章では，今後の展望を述べて本論文のまとめとする。

第 2 章

非線形写像を利用した擬似ランダムビット列の生成について

本研究の目的は、テント写像やロジスティック写像等の非線形写像の反復によって得られる系列のランダム性を利用した擬似ランダムビット列の生成法を考えたときに、当該生成法の安全性の評価を与えることを目的とした基本的な解析法を整理することである。尚、本論文では特に断りがない限り、非線形写像の中で最もシンプルであるテント写像を中心に考えるものとする。本章では、テント写像の反復によって得られる系列の特徴および、テント写像の反復によって得られる系列を利用した擬似ランダムビット列の生成案について触れる。この生成案は、次章以降で触れる解析法の解析対象となるものである。

2.1 1 次元非線形写像の反復により得られる系列

テント写像 f_a (tent map), ロジスティック写像 L_b (logistic map), 平方写像 Q_c (quadratic map) は以下の式 (2.1) ~ 式 (2.3) で定義される。

$$\text{テント写像 } f_a : I_a \rightarrow I_a \ (I_a = [0, 1]), \quad f_a(x) = \begin{cases} ax & (0 \leq x < 1/2) \\ a(1-x) & (1/2 \leq x \leq 1) \end{cases} \quad (2.1)$$

$$\text{ロジスティック写像 } L_b : I_b \rightarrow I_b \ (I_b = [0, 1]), \quad L_b(x) = bx(1-x) \quad (2.2)$$

$$\text{平方写像 } Q_c : I_c \rightarrow I_c \ (I_c = \left[\frac{-1 - \sqrt{1 + 4c}}{2}, \frac{1 + \sqrt{1 + 4c}}{2} \right]), \quad Q_c(x) = x^2 - c \quad (2.3)$$

これらの写像 $f : I \rightarrow I$ により、ある初期値 $x_0 \in I$ が順次 $x_0 \mapsto x_1 \mapsto x_2 \mapsto \cdots \mapsto x_n$ と写像されていくことを考える。すなわち $x_{i+1} = f(x_i)$ ($i = 0, 1, 2, \dots, n-1$) として、自身の値を写像 f により繰り返し写像していくこと（写像の反復）を考える。このとき、上記の各写像のパラメータ a, b, c および初期値 x_0 が適切に与えられていれば^{*1}、系列 $\{x_0, x_1, x_2, \dots, x_n\}$ はランダムな挙動を呈する場合があることが知られている（図 2.4 ~ 図 2.6）。

^{*1} ここでは、さしあたり $1 < a \leq 2$ (テント写像), $3.5 < b \leq 4$ の短周期領域以外 (ロジスティック写像), $1 < c \leq 2$ (平方写像) としておく。この範囲以外では、写像の定義域上の全ての点は固定点に落ち込むか無限遠法へ発散する。

本論文で扱う「非線形写像を利用した擬似ランダムビットの生成」とは、上記の写像を反復する毎に得られる系列 $\{x_i\}_{i=0}^n$ がランダムな挙動を呈する(図2.4~図2.6)ことを利用して、系列 $\{x_i\}_{i=0}^n$ から、ある規則に従い2値系列(バイナリシーケンス) $\{b_i\}_{i=0}^n$ を得ることをいう。

2値系列の作り方には様々な方法が考えられるが、本論文では、主として、第 i 回目の写像を行う度に($i = 0, 1, 2, \dots$)、 x_i の最上位ビット / 上位 t ビット桁目を 1 ビット($w = 1$)、或は複数の w ビットを抽出して構成された $\{b_i\}_{i=0}^{nw}$ について考えるものとする。(現実的な生成法を考えた場合は、より複雑な手法が考えられる)。

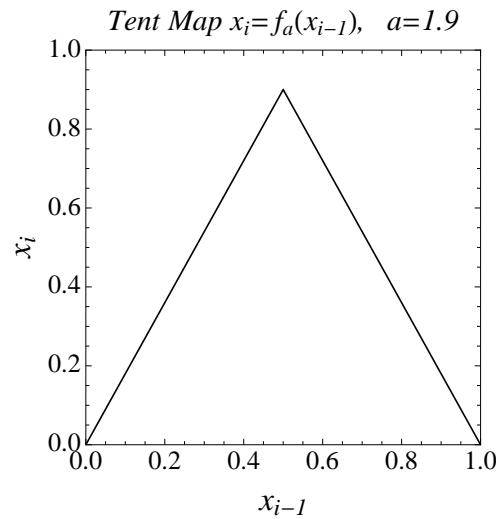


図 2.1 テント写像 $x_i = f_a(x_{i-1})$

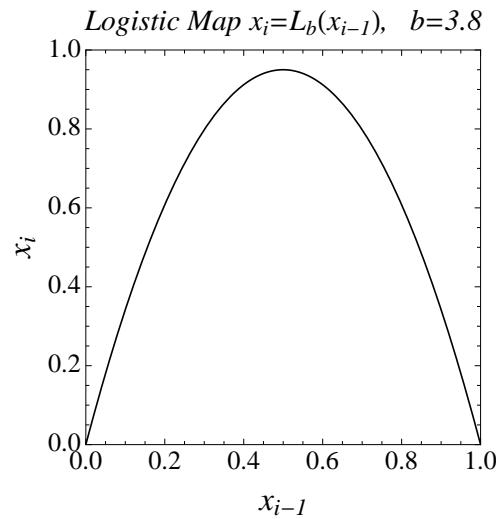
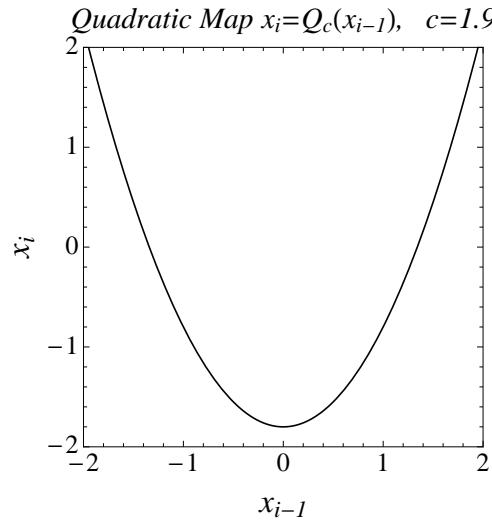
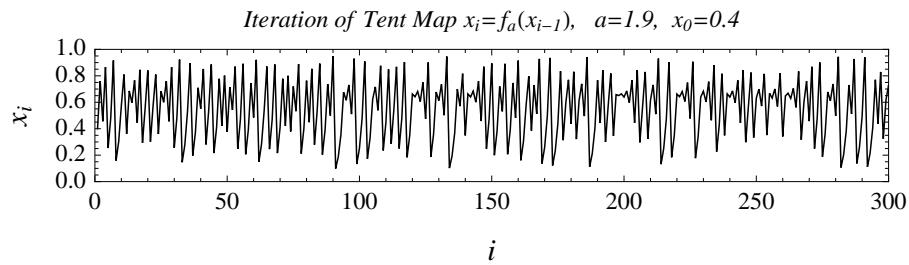
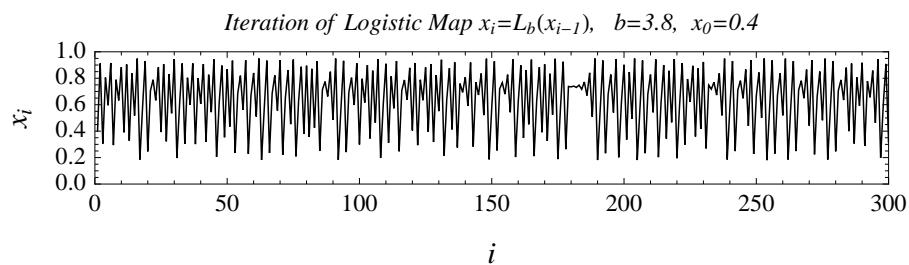
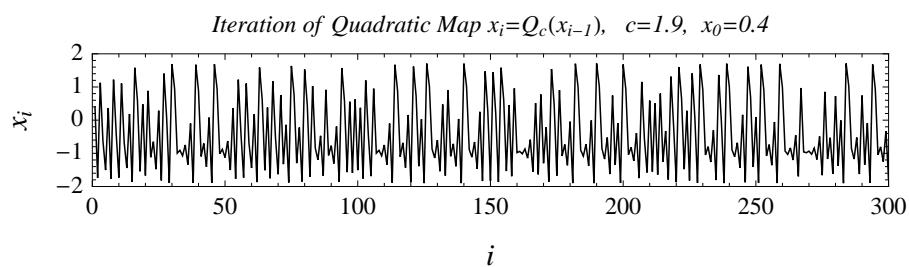


図 2.2 ロジスティック写像 $x_i = L_b(x_{i-1})$

図 2.3 平方写像 $x_i = Q_c(x_{i-1})$ 図 2.4 テント写像 f_a の反復によって得られる系列 ($a = 1.9, x_0 = 0.4$)図 2.5 ロジスティック写像 L_b の反復によって得られる系列 ($b = 3.9, x_0 = 0.4$)図 2.6 平方写像 Q_c の反復によって得られる系列 ($c = 1.9, x_0 = 0.4$)

ただし、系列 $\{x_i\}$ の出力の全桁をそのままランダムビット列として利用することは、極めて特殊な条件の下で生成された場合^{*2} 以外では期待できない。この理由は、図 2.4～図 2.6 からも明らかのように、軌道 $\{x_i\}$ はある値の付近に集まりやすい傾向があるためである。しかしながら軌道 $\{x_i\}$ は、あるランダムな要素をもちらながら遷移（変化）している様子が伺える。つまり、ここで述べる「非線形写像を利用した擬似ランダムビットの生成」とは、上記のテント写像、ロジスティック写像、平方写像の反復にて得られる系列 $\{x_i\}$ を、擬似ランダムビット列（2 値化系列 $\{b_i\}_{i=0}^n$ ）の「生成源」として利用しようというものである点を改めて強調しておく。

系列 $\{x_i\}$ のランダム性以外において、テント写像、ロジスティック写像、平方写像を擬似ランダムビット列 $\{b_i\}_{i=0}^n$ の生成源として利用することに関して期待されることとは、主として以下の 3 点が挙げられる。

1 点目は、処理の単純さである。擬似ランダムビット列の生成、或は、最終的な擬似ランダムビット列へと加工する前段部に相当するランダムソースを得る部分としては、処理が単純（軽量性、高速性）であることが望ましい。

2 点目は、テント写像、ロジスティック写像、平方写像は、初期条件鋭敏性（SDIC:Sensitive Dependence on Initial Condition）を有するため、初期値 x_0 のみならず、パラメータ a, b, c に僅かな差を与えるだけで、全く異なる系列 $\{x_i\}$ を生成できる点である。すなわち、異なる系列を生成するための制御が比較的容易であると考えられる（図 2.7、図 2.8）。

3 点目は、遅れ時間 t における自己相関係数が 0 付近の値を示し（図 2.9、図 2.9）、また、パワースペクトルに周期を示す線成分を含まない（図 2.11、図 2.12）などの非周期が挙げられる。（ただしパラメータ a が小さくなると、周波数の大きいほうのパワーが若干強くなる傾向がある。）

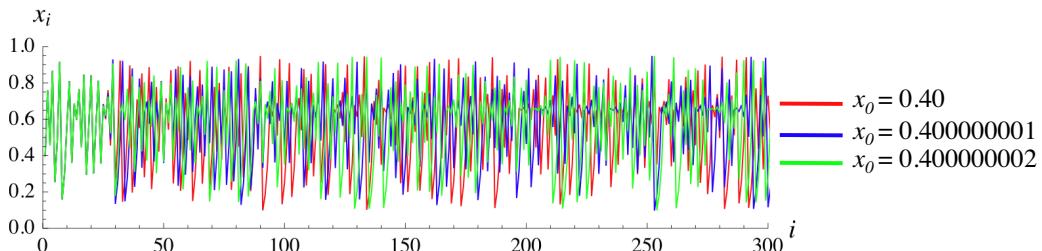


図 2.7 テント写像 f_a の初期条件敏感性 ($a = 1.9$ のとき)

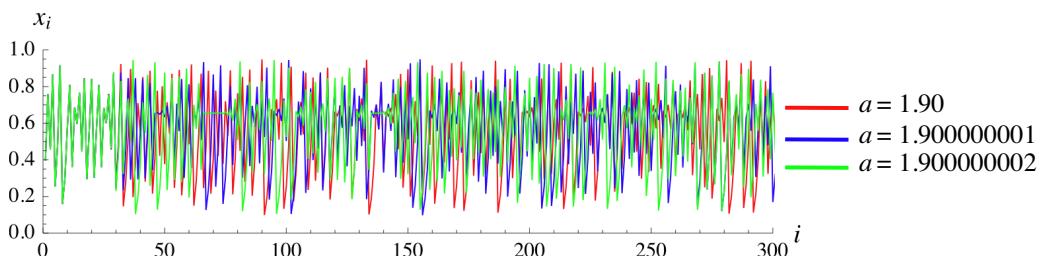
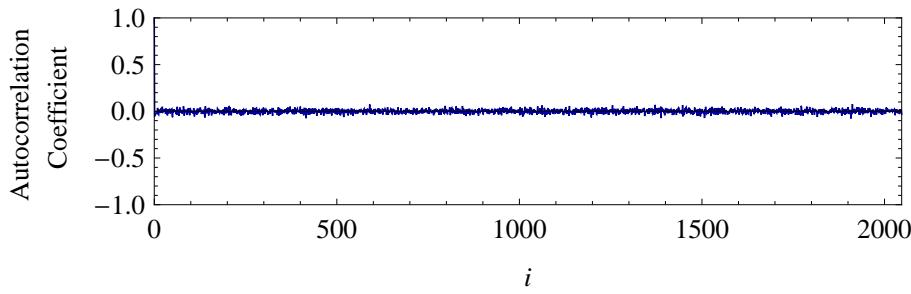
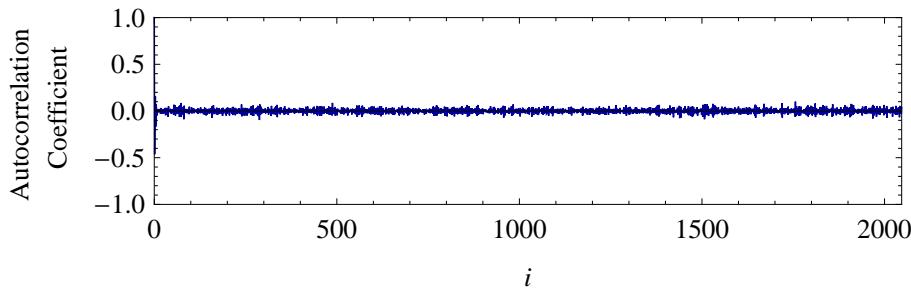
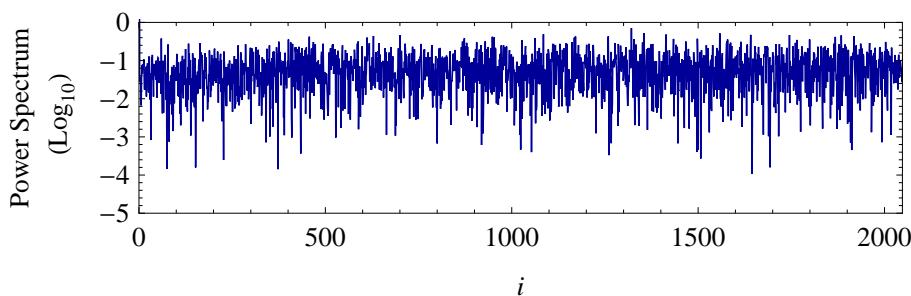
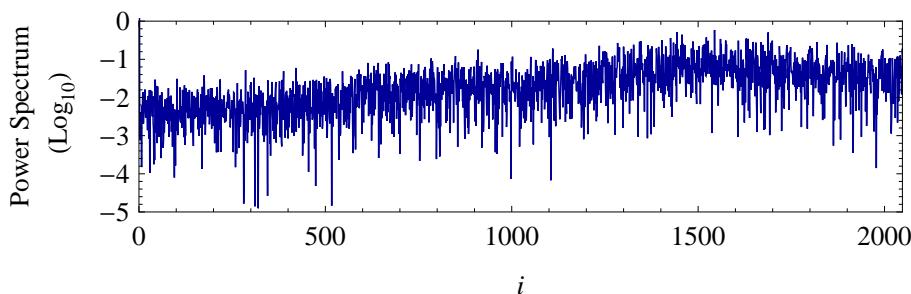


図 2.8 テント写像 f_a の初期条件敏感性 ($x_0 = 0.4$ のとき)

^{*2} 例えばパラメータ $a = 2$ のテント写像を無限の精度で実装した場合

図 2.9 テント写像 f_a の遅れ時間 i における自己相関係数 ($a = 1.99$ のとき)図 2.10 テント写像 f_a の遅れ時間 i における自己相関係数 ($a = 1.8$ のとき)図 2.11 テント写像 f_a のパワースペクトル ($a = 1.99$ のとき)図 2.12 テント写像 f_a のパワースペクトル ($a = 1.8$ のとき)

上記の生成系においては、初期値 x_0 および各写像のパラメータ a, b, c が、擬似ランダムビット生成のためのシード（鍵）、或はシード（鍵）依存値であると考えられる。

以降では、1次元の非線形写像の中でも最も単純であるテント写像を例として、パラメータ a の違いによる $\{x_i\}$ 系列の性格の違いについて触れる。

2.2 パラメータ $a = 2$ のテント写像

パラメータ $a = 2$ のテント写像 f_2 （式(2.1)）、および、これと位相共役（位相同形）（付録A.1）の関係にあるパラメータ $b = 4$ のロジスティック写像 L_4 （式(2.2)）と、 $c = 2$ の平方写像 Q_2 （式(2.3)）は、写像を反復する毎に得られる $\{x_i\}$ 系列から、式(2.4)に従い最上位ビットを抽出した場合に、0,1の出現確率が等しい理想的なランダムビット列 $\{b_i\}$ が得られることが知られている。言い換えると、 $\{b_i\}$ は「公平なコイン投げ」（ベルヌーイ試行）の結果として得られる系列と等価であることが知られている。

$$b_i = \begin{cases} 0 & (0 \leq x_i < 1/2) \\ 1 & (1/2 \leq x_i \leq 1) \end{cases} \quad (2.4)$$

しかし、上記には注意があり、テント写像の場合は、 f_a に与える初期値 $x_0 \in I_a$ ($I_a = [0, 1]$) に2進表記の有限桁で表せるような値を選んだ場合は、有限の回数の反復後に固定点 $x = 0$ に落ち込み、それ以降永久に $x = 0$ から脱出できない。例えば x_0 が以下のように2進表記したときの小数点以下の桁が t 桁（演算精度が t ビット）で与えられた場合を考えると、

$$x_0 = (0.b_1b_2b_3 \cdots b_{t-1}b_t)_2, \quad b_j = \{0, 1\} \quad (0 \leq j \leq t)$$

$a = 2$ のテント写像 $f_2(x)$ とは、 x または $1 - x$ を2倍する処理であるため、 x または $1 - x$ の左1ビットシフト処理と等しい。つまり、 $x_0 < 0.5$ の場合 ($b_1 = 0$ のとき) は $x_1 = (\underbrace{0.b_2b_3b_4 \cdots b_t 0}_t)_2$ となる。一方で、 $x_0 \geq 0.5$ の場合 ($b_1 = 1$ のとき) は、まず $1 - x$ の処理は、 x の小数点以下の全ビットを反転させた後に ($\underbrace{0.000 \cdots 01}_t$)₂ を加算する処理に等しく、

$$\begin{aligned} 1 - x &= (0.1b_2b_3 \cdots b_{t-1}b_t)_2 \oplus (\underbrace{0.111 \cdots 11}_t)_2 + (\underbrace{0.000 \cdots 01}_t)_2 \\ &\stackrel{\text{def}}{=} (0.b'_1b'_2b'_3 \cdots b'_{t-1}b'_t)_2 \end{aligned}$$

その後に左1ビットシフトをするので $x_1 = (\underbrace{0.b'_2b'_3b'_4 \cdots b'_t 0}_t)_2$ である。このようにして最下位桁から順に0が入るので t 回目の写像後には $x_t = (\underbrace{0.000 \cdots 00}_t)_2$ となる。

つまり、 $a = 2$ のテント写像 $f_2(x)$ を反復する度に最上位ビットを抽出した系列 $\{b_i\}$ が「公平なコイン投げ」（ベルヌーイ試行）の結果として得られる系列と等価になるのは、このアルゴリズムが無限の演算精度で実装され、かつ、無限桁の初期値 x_0 （無理数、或は循環小数となる有理数）を与えたときに限られる。このアルゴリズムを今日の有限精度のデジタルコンピュータ（小数点以下の精度が t ビット）に実装した場合に、我々が実際に得ることができるのは、初期の $t - 1$ 回目の反復までに得られる高々 t ビット ($\{b_i\}_{i=0}^{t-1}$) である。すなわち、特殊な数値演算法を用いず今日の標準的な倍精度浮

動小数点演算で実装した場合は、仮数部の精度は $t = 52$ ビットであることから、 $t - 1 = 51$ 回目の反復までに得られる計 $t = 52$ ビットである。ランダムビット列長がこの程度の長さでしかないのであれば、今日の一般的な擬似乱数生成法が生成する擬似ランダムビット列の長さに対して遙かに短い。

2.3 パラメータ $a \leq 1$ および $a > 2$ のテント写像

我々の最大の関心ごとは、テント写像 $f_a : I_a \rightarrow I_a$ ($I_a = [0, 1]$) によって、 I_a 上の点を $x_i \xrightarrow{f_a} x_{i+1}$ ($x_{i+1} = f_a(x_i)$) として写像を繰り返していくとき、最終的に x_i がどのような状態になるかということである。

$a \leq 1$ および $a > 2$ の場合は、 I_a 上の全ての点は、写像繰り返していくうちに（ステップ i を増加させていくうちに）、 $\{x_i\}$ は単調増加または単調減少を繰り返して、 $i \rightarrow \infty$ の極限において 0 または ∞ に漸近収束（発散）するか、あるいは、少ない回数の写像後に固定点 $x = 0$ にダイレクト（直接 $x = 0$ を選んで）落ち込む。従ってこの系をランダムビット列の生成源として利用しようという発想には至らない。

$a = 0$ の場合は、区間 $[0, 1]$ 上の全ての点（初期値）は 1 回目の写像後に固定点 $x = 0$ に陥る。

$$\begin{aligned} x_0 < 0.5 \text{ のとき} &: x_1 = ax_0 = 0 \quad (\because a = 0) \\ x_0 \geq 0.5 \text{ のとき} &: x_1 = a(1 - x_0) = 0 \quad (\because a = 0) \end{aligned}$$

$a = 1$ の場合は、区間 $[0, 1/2)$ 上の点（初期値）は、その点自体が固定点である。区間 $[1/2, 1]$ 上の点（初期値）は、1 回目の写像で $1 - x_0$ に移された以降は区間 $[0, 1/2)$ の場合と同じになる。

$$\begin{aligned} x_0 < 0.5 \text{ のとき} &: x_1 = ax_0 = x_0 \quad (\because a = 1) \\ x_0 \geq 0.5 \text{ のとき} &: x_1 = a(1 - x_0) = 1 - x_0 \quad (< 0.5) \\ &x_2 = ax_1 = a(1 - x_0) = 1 - x_0 \quad (\because a = 1) \end{aligned}$$

$0 < a < 1$ の場合は、区間 $[0, 1]$ 上の全ての点（初期値）を出発した軌道 $\{x_i\}$ は、写像のたびに a の割合で値を小さくしながら固定点 0 に漸近収束する。計算機に実装した場合は、そのプログラムは有限回の反復後にアンダーフローでストップする。

$$\begin{aligned} x_0 < 0.5 \text{ のとき} &: x_0 \mapsto ax_0 \mapsto a^2x_0 \mapsto \dots \\ &\text{すなわち } \lim_{i \rightarrow \infty} a^i x_0 = 0 \quad (\because a < 1) \\ x_0 \geq 0.5 \text{ のとき} &: x_0 \mapsto a(1 - x_0) \mapsto a^2(1 - x_0) \mapsto \dots \\ &\text{すなわち } \lim_{i \rightarrow \infty} a^i (1 - x_0) = 0 \quad (\because a < 1) \end{aligned}$$

$a > 2$ の場合は、 $x_i (= f_a^i(x_0))$ が区間 $(\frac{1}{a}, \frac{a-1}{a})$ に入ったとき、それ以降の軌道 $\{x_i\}$ は一定の割合で絶対値量 $|x_i|$ を大きくしながら $-\infty$ に発散する。計算機に実装した場合は、そのプログラムは有限回の反復後にオーバーフローでストップする。

$$\begin{aligned} x_i \in \left(\frac{1}{a}, \frac{a-1}{a}\right) &\mapsto x_{i+1} \in \left(1, \frac{a}{2}\right] \\ &\mapsto x_{i+2} \in \left[-a\left(\frac{a}{2} - 1\right), 0\right) \\ &\mapsto x_{i+3} \in \left[-a^2\left(\frac{a}{2} - 1\right), 0\right) \\ &\dots \mapsto x_{i+j} \in \left[-a^{j-1}\left(\frac{a}{2} - 1\right), 0\right) \xrightarrow{j \rightarrow \infty} [-\infty, 0) \end{aligned}$$

2.4 パラメータ $1 < a < 2$ のテント写像

パラメータ $1 < a < 2$ の場合（すなわち写像の傾きが $1 < a < 2$ ）には興味深いことが生じる。初期値 $x = 0$ は固定点であり、 $x = 1$ は1回目の写像後に固定点 $x = 0$ に至るので、ここでは初期値 $x_0 \in (0, 1)$ を考える。 $1 < a < 2$, $x_0 \in (0, 1)$ の場合は、固定点 $x = 0$ へ写像される点は存在しないことが図 2.13 よりも明らかである。

$$\exists x \in (0, 1) (f_a(x) = 0) \quad (1 < a < 2 \text{ のとき}) \quad (2.5)$$

このことに関係して、 $a = 2$ のときは（ただし有限精度の場合）、区間 $(0, 1)$ 上の全ての点は、僅か t 回 (t は演算精度) の反復後に固定点 $x = 0$ に至り、以後永久に $x = 0$ に留まるが、 $1 < a < 2$, $x_0 \in (0, 1)$ のときは固定点 $x = 0$ に落ち込むことがなくなり、最終的に区間 $[a(1 - \frac{a}{2}), \frac{a}{2}]$ 内をある長さの周期で巡回するようになる（図 2.13 および図 2.14, 図 2.15 を参照）。

ただ、 $1 < a < 2$ の場合は、 $a = 2$ の場合と同じく軌道 $\{x_i\}$ があらゆる長さの周期を有するか否か^{*3} についての詳しいことは判っていない。いずれにしても、軌道 $\{x_i\}$ を有限精度のデジタル計算機で求めた場合（演算誤差を含む点に留意）は、無限の周期を有することはあり得ない^{*4}。

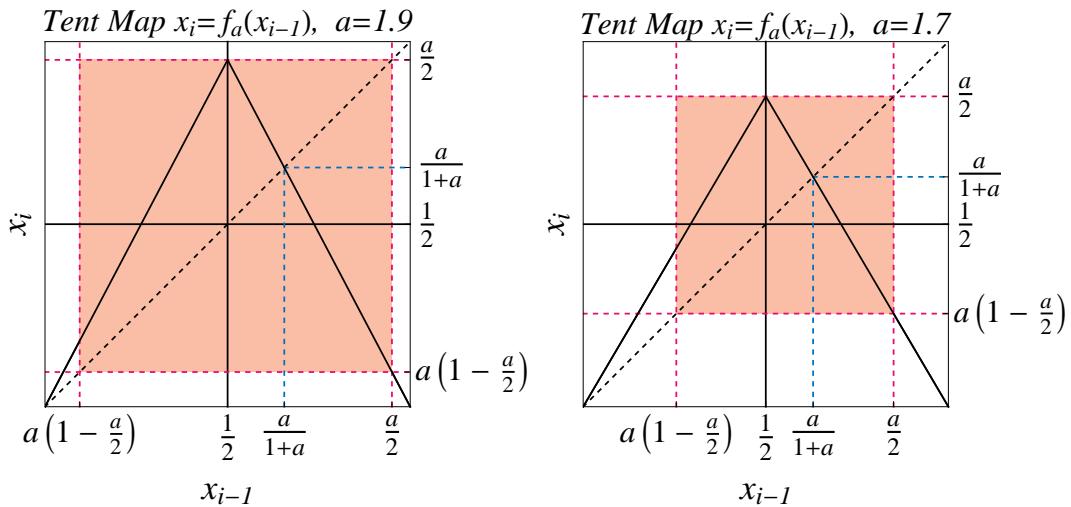
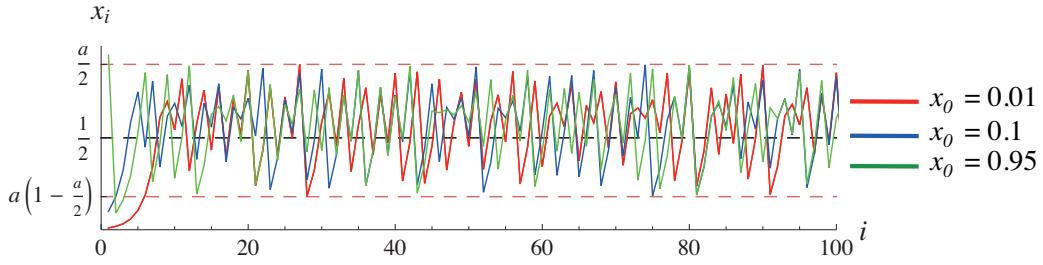
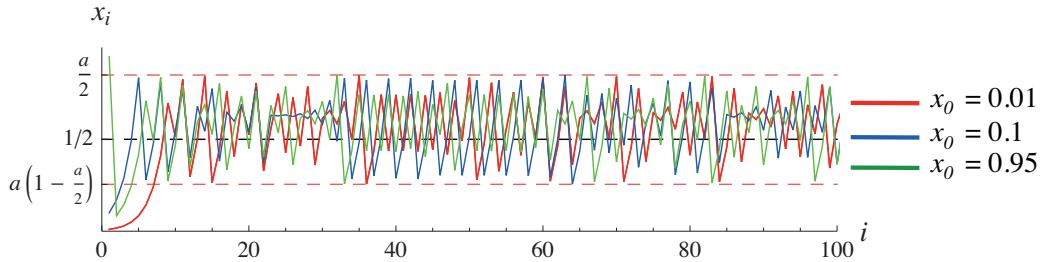


図 2.13 $1 < a < 2$ のテント写像

^{*3} $a = 2$ の場合は、 $f_2^l(x_i) = x_i$ となる l が全ての自然数について成立するような l と、これに対応する $x_i \in [0, 1]$ が存在することが知られている ($\exists x_i \in [0, 1] \forall l \in \mathbb{N} (f_2^l(x_i) = x_i)$)

^{*4} 本研究の最終的な目標は、「有限精度のデジタル計算機」によって擬似ランダムビット列を生成すること、および、「有限精度のデジタル計算機」によって生成された擬似ランダムビット列についての解析法を得ることである。

図 2.14 テント写像の反復によって得られる系列 ($a = 1.9$)図 2.15 テント写像の反復によって得られる系列 ($a = 1.7$)

2.4.1 数値実験による周期長の探索について

$1 < a < 2$, $x_0 \in (0, 1)$ の場合は, $a = 2$ のときと異なり, 短期間に固定点 x_0 に落ち込むことはなく, 区間 $[a(1 - \frac{a}{2}), \frac{a}{2}]$ 内をある周期で巡回する. 本節では, この様子を計算機で調べた実験結果を示す. 実験にあたっては, 倍精度 浮動小数点演算 (演算精度 $t = 52$), および 単精度 浮動小数点演算 (精度 $t = 23$) を用いた.

倍精度浮動小数点演算の精度は $t = 52$ であるため, 区間 $(0, 1)$ 上で $2^{52} - 1$ 個の点を含む. これら全ての初期値候補を調べることは計算量的に容易ではないので, いくつかの代表点 (パラメータ a , および初期値 x_0 の組) について調査した. 結果を表 2.1, 表 2.2 に示した. 表内の数値は傾き a において初期値 x_0 を出発した軌道が最終的に行き着く周期軌道の周期長を意味する. 尚, 同一のパラメータ a において, 異なる初期値 $x_0 \neq x'_0$ であっても同じ長さの周期長を示す箇所は, それぞれ x_0, x'_0 を出発した軌道は, 最終的に同じ周期軌道に陥ることを意味している. 単精度浮動小数点演算 ($t = 23$) を用いた場合の結果は表 2.3, 表 2.4 に示した.

表2.1 テント写像の周期長調査1(倍精度 浮動小数点演算($t = 52$))表の数値は傾き a において初期値 x_0 を出発した軌道が最終的に行き着く周期軌道の周期長を意味する

x_0	$a =$									
	1.40	1.41	1.42	1.43	1.44	1.45	1.46	1.47	1.48	1.49
0.400	1112522	18441274	112649458	99611417	13467165	77188324	36241496	65868506	8992973	13444005
0.405	9661234	18441274	112649458	45764195	15683095	77188324	4879819	65868506	8992973	8243126
0.410	9661234	37596400	38505370	45764195	43754716	77188324	4879819	65868506	20789133	13444005
0.415	20934746	18441274	38505370	99611417	43754716	77188324	4879819	65868506	20789133	13444005
0.420	79283880	37596400	1958697	29036046	13467165	77188324	4879819	65868506	8992973	13444005
0.425	9661234	18441274	38505370	99611417	15683095	77188324	36241496	65868506	8992973	8243126
0.430	79283880	37596400	38505370	45764195	43754716	77188324	4879819	65868506	8992973	8243126
0.435	1112522	11272090	38505370	45764195	15683095	77188324	4879819	65868506	8992973	13444005
0.440	1112522	18441274	112649458	99611417	13467165	77188324	4879819	65868506	8992973	13444005
0.445	9661234	1455472	38505370	45764195	43754716	77188324	4879819	65868506	20789133	13444005
0.450	79283880	18441274	38505370	45764195	15683095	77188324	4879819	65868506	8992973	13444005
0.455	79283880	37596400	890111	45764195	13467165	77188324	4879819	65868506	8992973	8243126
0.460	79283880	37596400	38505370	45764195	15683095	77188324	4879819	65868506	8992973	13444005
0.465	79283880	18441274	112649458	99611417	15683095	77188324	4879819	65868506	8992973	8243126
0.470	20934746	18441274	38505370	99611417	43754716	77188324	4879819	65868506	20789133	8243126
0.475	20934746	18441274	112649458	99611417	43754716	77188324	4879819	65868506	8992973	13444005
0.480	79283880	11272090	38505370	99611417	15683095	77188324	4879819	65868506	8992973	13444005
0.485	79283880	18441274	112649458	45764195	43754716	77188324	4879819	65868506	8992973	8243126
0.490	79283880	18441274	112649458	99611417	43754716	77188324	4879819	65868506	8992973	8243126
0.495	20934746	37596400	112649458	99611417	43754716	77188324	4879819	65868506	8992973	13444005
0.500	79283880	18441274	112649458	99611417	43754716	77188324	4879819	65868506	8992973	8243126
x_0	$a =$									
	1.50	1.51	1.52	1.53	1.54	1.55	1.56	1.57	1.58	1.59
0.400	13367591	124026855	43153488	15429997	39029828	162424986	140437594	12001820	109295237	14429837
0.405	13367591	124026855	43153488	15429997	16157046	162424986	41673935	12001820	109295237	14429837
0.410	13367591	135370917	43153488	15429997	16157046	63157237	5287170	12001820	109295237	14429837
0.415	13367591	124026855	43153488	15429997	16157046	63157237	41673935	12001820	109295237	14429837
0.420	13367591	124026855	43153488	15429997	39029828	63157237	41673935	12001820	109295237	14429837
0.425	36892648	135370917	43153488	15429997	20631842	63157237	595065	37487874	109295237	14429837
0.430	36892648	124026855	43153488	15429997	3950914	63157237	140437594	37487874	109295237	14429837
0.435	13367591	124026855	43153488	15429997	23923192	162424986	140437594	12001820	109295237	14429837
0.440	13367591	124026855	43153488	20503926	16157046	162424986	140437594	12001820	109295237	14429837
0.445	13367591	124026855	43153488	15429997	23923192	162424986	41673935	12001820	109295237	12792961
0.450	36892648	124026855	43153488	15429997	48139101	63157237	41673935	25629034	109295237	14429837
0.455	36892648	124026855	43153488	15429997	48139101	63157237	140437594	37487874	21512668	14429837
0.460	36892648	124026855	43153488	15429997	16157046	162424986	41673935	12001820	109295237	12792961
0.465	13367591	135370917	43153488	15429997	23923192	162424986	140437594	12001820	109295237	12792961
0.470	36892648	124026855	43153488	15429997	16157046	63157237	140437594	12001820	109295237	14429837
0.475	36892648	124026855	43153488	15429997	23923192	162424986	140437594	12001820	109295237	12792961
0.480	13367591	124026855	43153488	15429997	48139101	63157237	140437594	12001820	109295237	14429837
0.485	36892648	124026855	43153488	15429997	16157046	63157237	41673935	25629034	109295237	14429837
0.490	13367591	124026855	43153488	15429997	39029828	63157237	140437594	25629034	109295237	14429837
0.495	36892648	124026855	43153488	15429997	16157046	63157237	140437594	37487874	109295237	14429837
0.500	13367591	124026855	43153488	15429997	39029828	162424986	5287170	12001820	109295237	14429837
x_0	$a =$									
	1.60	1.61	1.62	1.63	1.64	1.65	1.66	1.67	1.68	1.69
0.400	23572433	33279868	177962810	123164290	49003303	1479818	102080195	773960	32182606	134223871
0.405	27017522	11750855	177962810	123164290	49003303	82960958	102080195	87662209	32182606	134223871
0.410	11246254	103927594	177962810	123164290	49003303	82960958	102080195	87662209	32182606	134223871
0.415	27017522	103927594	177962810	123164290	49003303	82960958	102080195	87662209	32182606	134223871
0.420	27017522	103927594	177962810	123164290	49003303	82960958	102080195	87662209	32182606	134223871
0.425	13889975	103927594	177962810	123164290	49003303	82960958	102080195	87662209	32182606	134223871
0.430	18920077	103927594	177962810	123164290	49003303	82960958	102080195	87662209	32182606	134223871
0.435	13889975	103927594	177962810	123164290	49003303	82960958	102080195	87662209	32182606	134223871
0.440	18920077	28724173	177962810	123164290	49003303	82960958	102080195	87662209	32182606	134223871
0.445	13889975	103927594	177962810	123164290	49003303	82960958	102080195	87662209	32182606	134223871
0.450	11246254	103927594	177962810	123164290	49003303	82960958	102080195	87662209	32182606	134223871
0.455	23572433	103927594	177962810	123164290	49003303	82960958	102080195	87662209	32182606	134223871
0.460	27017522	11954428	177962810	123164290	49003303	82960958	102080195	87662209	32182606	134223871
0.465	18920077	28724173	177962810	123164290	49003303	82960958	102080195	87662209	32182606	134223871
0.470	27017522	103927594	177962810	123164290	49003303	955786	102080195	87662209	32182606	134223871
0.475	18920077	103927594	177962810	123164290	49003303	82960958	102080195	87662209	32182606	134223871
0.480	18920077	33279868	177962810	123164290	49003303	82960958	102080195	87662209	32182606	134223871
0.485	13889975	103927594	177962810	123164290	49003303	1479818	102080195	87662209	32182606	134223871
0.490	23572433	103927594	177962810	123164290	49003303	82960958	58550832	87662209	32182606	134223871
0.495	18920077	103927594	177962810	123164290	49003303	82960958	102080195	87662209	26389469	134223871
0.500	13889975	103927594	11954428	5678318	49003303	82960958	102080195	87662209	32182606	134223871

表 2.2 テント写像の周期長調査 2 (倍精度 浮動小数点演算 ($t = 52$))表の数値は傾き a において初期値 x_0 を出発した軌道が最終的に行き着く周期軌道の周期長を意味する

x_0	$a =$	1.70	1.71	1.72	1.73	1.74	1.75	1.76	1.77	1.78	1.79
0.400	1113766	21920404	8048475	83358339	153627056	5760602	72136759	103019138	76018894	25339959	
0.405	55670321	150430226	8048475	83358339	153627056	5760602	72136759	103019138	76018894	25983434	
0.410	55670321	150430226	163998482	83358339	153627056	5760602	72136759	103019138	76018894	23065142	
0.415	55670321	21920404	8048475	83358339	153627056	5760602	27040573	103019138	76018894	25339959	
0.420	1113766	21920404	43718226	83358339	153627056	5760602	6873771	103019138	36327555	14702902	
0.425	1113766	150430226	8048475	83358339	153627056	5760602	27040573	103019138	76018894	14702902	
0.430	55670321	21920404	163998482	83358339	153627056	5760602	72136759	103019138	76018894	14702902	
0.435	1113766	150430226	163998482	47257686	153627056	5760602	72136759	103019138	36327555	37769584	
0.440	39282612	21920404	43718226	47257686	153627056	5760602	6873771	103019138	76018894	23065142	
0.445	55670321	150430226	163998482	83358339	153627056	5760602	27040573	103019138	36327555	25983434	
0.450	39282612	150430226	163998482	83358339	153627056	5760602	6873771	103019138	76018894	25983434	
0.455	55670321	21920404	163998482	83358339	153627056	5760602	1678299	103019138	76018894	23065142	
0.460	55670321	150430226	163998482	47257686	153627056	5760602	72136759	103019138	76018894	14702902	
0.465	1113766	150430226	163998482	83358339	153627056	5760602	72136759	103019138	76018894	14702902	
0.470	55670321	21920404	163998482	83358339	153627056	5760602	72136759	103019138	76018894	25983434	
0.475	1113766	21920404	163998482	47257686	153627056	5760602	2689541	72136759	103019138	76018894	23065142
0.480	55670321	21920404	163998482	83358339	153627056	5760602	72136759	103019138	76018894	25339959	
0.485	55670321	21920404	163998482	10643262	153627056	5760602	27040573	103019138	36327555	23065142	
0.490	55670321	21920404	163998482	83358339	153627056	5760602	72136759	103019138	76018894	14702902	
0.495	1113766	150430226	163998482	83358339	153627056	5760602	72136759	103019138	76018894	25983434	
0.500	55670321	150430226	163998482	83358339	153627056	5760602	27040573	103019138	76018894	23065142	
x_0	$a =$	1.80	1.81	1.82	1.83	1.84	1.85	1.86	1.87	1.88	1.89
0.400	123095338	189496347	142612121	66975064	19439263	85824337	13214675	42607794	12028131	31379406	
0.405	123095338	189496347	50219205	66975064	19439263	85824337	13214675	42607794	62101856	165781073	
0.410	123095338	189496347	142612121	66975064	19439263	85824337	68811990	42607794	62101856	165781073	
0.415	123095338	16156647	142612121	66975064	19439263	85824337	13214675	42607794	62101856	101081609	
0.420	123095338	16156647	50219205	66975064	78910462	85824337	13214675	42607794	62101856	165781073	
0.425	123095338	189496347	35669687	56122557	19439263	85824337	13214675	42607794	12028131	165781073	
0.430	123095338	16156647	50219205	66975064	78910462	85824337	2153028	42607794	12028131	165781073	
0.435	17070898	16156647	51401836	66975064	78910462	85824337	68811990	42607794	12028131	101081609	
0.440	123095338	189496347	51401836	66975064	78910462	85824337	13214675	42607794	12028131	101081609	
0.445	123095338	189496347	51401836	66975064	19439263	85824337	13214675	42607794	12028131	165781073	
0.450	123095338	142612121	66975064	19439263	85824337	13214675	42607794	12028131	101081609		
0.455	123095338	189496347	142612121	66975064	19439263	85824337	34996890	42607794	11336197	101081609	
0.460	123095338	189496347	142612121	66975064	19439263	85824337	13214675	42607794	62101856	165781073	
0.465	123095338	189496347	142612121	66975064	24127515	85824337	13214675	42607794	12028131	165781073	
0.470	123095338	189496347	142612121	66975064	78910462	85824337	13214675	42607794	12028131	101081609	
0.475	123095338	189496347	35669687	66975064	19439263	85824337	68811990	42607794	12028131	101081609	
0.480	17070898	16156647	142612121	66975064	78910462	85824337	13214675	42607794	62101856	165781073	
0.485	123095338	189496347	142612121	66975064	19439263	85824337	68811990	42607794	12028131	101081609	
0.490	123095338	16156647	50219205	66975064	19439263	85824337	68811990	42607794	12028131	101081609	
0.495	123095338	189496347	142612121	66975064	19439263	85824337	68811990	42607794	12028131	101081609	
0.500	123095338	189496347	50219205	66975064	19439263	85824337	34996890	42607794	12028131	101081609	
x_0	$a =$	1.90	1.91	1.92	1.93	1.94	1.95	1.96	1.97	1.98	1.99
0.400	174970811	112575214	53704577	103799807	98351026	81262919	11505983	81954754	58058645	295899934	
0.405	174970811	6882635	73414788	103799807	141336907	81262919	33202604	81954754	21858737	295899934	
0.410	174970811	6882635	73414788	103799807	98351026	94828796	3244818	4882190	58058645	295899934	
0.415	174970811	112575214	73414788	135606525	98351026	76954081	33202604	82114859	58058645	295899934	
0.420	20093181	6882635	73414788	135606525	98351026	81262919	33202604	82114859	58058645	295899934	
0.425	20093181	112575214	73414788	135606525	141336907	76954081	33202604	81954754	71483569	295899934	
0.430	174970811	112575214	73414788	5067330	98351026	94828796	33202604	81954754	58058645	295899934	
0.435	174970811	112575214	73414788	103799807	141336907	94828796	33202604	82114859	58058645	295899934	
0.440	59297320	54033707	53704577	135606525	98351026	76954081	33202604	81954754	71483569	26070936	
0.445	20093181	112575214	53704577	135606525	141336907	81262919	33202604	82114859	58058645	295899934	
0.450	174970811	109111576	73414788	135606525	98351026	94828796	33202604	81954754	71483569	295899934	
0.455	20093181	54033707	73414788	135606525	141336907	76954081	33202604	82114859	71483569	295899934	
0.460	174970811	112575214	73414788	135606525	141336907	81262919	33202604	82114859	58058645	295899934	
0.465	20093181	6882635	73414788	135606525	98351026	94828796	33202604	81954754	58058645	295899934	
0.470	20093181	112575214	53704577	135606525	98351026	81262919	11505983	81954754	999510	295899934	
0.475	59297320	6882635	73414788	135606525	98351026	76954081	33202604	82114859	71483569	295899934	
0.480	59297320	109111576	73414788	135606525	141336907	94828796	33202604	81954754	58058645	295899934	
0.485	59297320	112575214	73414788	135606525	98351026	94828796	33202604	82114859	58058645	295899934	
0.490	174970811	112575214	53704577	103799807	98351026	94828796	33202604	82114859	58058645	295899934	
0.495	174970811	112575214	73414788	103799807	141336907	81262919	14166203	81954754	58058645	295899934	
0.500	174970811	112575214	53704577	135606525	98351026	81262919	11505983	81954754	58058645	295899934	

表2.3 テント写像の周期長調査3(单精度浮動小数点演算($t = 23$))表の数値は傾き a において初期値 x_0 を出発した軌道が最終的に行き着く周期軌道の周期長を意味する

x_0	$a =$									
	1.40	1.41	1.42	1.43	1.44	1.45	1.46	1.47	1.48	1.49
0.400	4586	2672	1220	3468	2272	840	945	3120	100	1766
0.405	4586	5930	3771	3468	2272	840	945	3120	100	1766
0.410	4586	5930	1220	3468	2272	840	945	3120	3212	1766
0.415	4586	2672	3771	3468	2272	840	945	3120	3212	1766
0.420	4586	5930	385	3468	2272	840	945	3120	3212	263
0.425	4586	2672	1220	3468	1271	840	945	3120	3212	1766
0.430	2594	5930	1220	3468	1271	840	945	423	3212	1766
0.435	4586	5930	3771	3468	2272	840	945	3120	3212	1766
0.440	4586	5930	1220	3468	1271	840	945	3120	100	1766
0.445	4586	2672	1220	3468	1271	840	945	3120	3212	4959
0.450	4586	5930	1220	3468	2272	840	945	3120	3212	1766
0.455	4586	2672	3771	3468	2272	840	945	3120	100	1766
0.460	4586	2672	3771	3468	1271	840	945	3120	100	1766
0.465	4586	2672	3771	3468	1271	840	320	3120	100	1766
0.470	4586	5930	3771	3468	2272	840	320	3120	100	1766
0.475	4586	2672	385	3468	1271	840	945	3120	100	1766
0.480	4586	5930	1220	3468	1271	840	945	3120	100	1766
0.485	4586	5930	1220	3468	2272	840	320	3120	3212	1766
0.490	4586	5930	3771	3468	2272	840	945	3120	100	4959
0.495	2594	2672	3771	3468	2272	840	302	3120	3212	1766
0.500	4586	5930	1220	3468	2272	840	945	3120	100	1766
x_0	$a =$									
	1.50	1.51	1.52	1.53	1.44	1.45	1.46	1.47	1.48	1.49
0.400	2	124	1733	1650	1541	929	654	2605	1441	530
0.405	300	626	1733	3497	1541	4989	2082	2605	767	2215
0.410	300	626	1361	3497	1541	4989	654	2605	767	2215
0.415	300	824	1361	3497	1541	4989	654	2605	767	530
0.420	300	626	1361	1650	1541	4989	654	2605	767	58
0.425	300	626	3106	3497	1541	4989	654	2605	767	58
0.430	300	626	1733	3497	1541	4989	654	2605	767	58
0.435	300	824	1733	282	1541	4989	654	2605	767	58
0.440	300	626	1733	3497	1541	4989	654	2605	767	58
0.445	300	626	1733	3497	1541	4989	654	2605	1441	530
0.450	300	626	1361	3497	1541	4989	654	2605	767	530
0.455	300	626	1733	1650	1541	4989	654	2605	767	58
0.460	300	626	1733	1650	1541	4989	654	2605	767	58
0.465	300	626	1733	3497	1541	4989	654	2605	1441	58
0.470	300	626	1733	3497	1541	929	654	2605	767	58
0.475	300	824	1361	3497	1541	4989	268	2605	767	530
0.480	300	39	1733	3497	1541	929	654	2605	767	2215
0.485	300	626	3106	3497	1541	4989	2082	2605	1441	58
0.490	300	626	1733	3497	1632	929	654	2605	1441	58
0.495	300	124	1733	3497	1541	929	654	2605	1441	58
0.500	300	824	1733	3497	1541	4989	2082	2605	767	58
x_0	$a =$									
	1.60	1.61	1.62	1.63	1.64	1.65	1.66	1.67	1.68	1.69
0.400	766	4918	3205	2107	3232	300	6082	3051	842	4154
0.405	1418	294	3205	2107	1450	1999	6082	1165	3967	4154
0.410	766	4918	3205	2107	3232	1999	6082	3051	3967	4154
0.415	766	4918	3205	2107	572	1999	6082	1165	842	4154
0.420	1418	4918	3205	2107	5232	1999	11	1165	3967	4154
0.425	766	4918	2579	2107	3232	1999	6082	1165	3967	4154
0.430	766	4918	3205	2107	3232	300	6082	3051	3967	4154
0.435	766	4918	3205	705	3232	1999	6082	3051	3967	4154
0.440	766	700	3205	2107	3232	300	11	1165	842	4154
0.445	766	700	883	2107	3232	1999	11	1165	204	4154
0.450	766	4918	3205	2107	3232	1999	6082	3051	3967	4154
0.455	1418	4918	883	2107	3232	1999	11	3051	3967	4154
0.460	766	4918	3205	2107	3232	300	6082	1165	3967	4154
0.465	1418	4918	3205	2107	3232	1999	6082	3051	842	4154
0.470	766	4918	2579	2107	3232	300	6082	3051	842	4154
0.475	1418	4918	3205	2107	3232	300	6082	1165	842	4154
0.480	766	4918	3205	2107	3232	300	6082	186	3967	4154
0.485	766	4918	3205	2107	3232	300	6082	1165	3967	4154
0.490	160	4918	3205	2107	3232	1999	6082	1165	3967	4154
0.495	766	4918	883	2107	3232	1999	6082	1165	3967	4154
0.500	766	4918	3205	597	3232	1999	6082	1165	842	4154

表 2.4 テント写像の周期長調査 4 (单精度 浮動小数点演算 ($t = 23$))表の数値は傾き a において初期値 x_0 を出発した軌道が最終的に行き着く周期軌道の周期長を意味する

x_0	$a = 1.70$									
	1.70	1.71	1.72	1.73	1.74	1.75	1.76	1.77	1.78	1.79
0.400	1280	7219	290	1827	5812	2399	2723	7322	1809	11703
0.405	1445	7219	290	1827	5812	2399	2723	7322	1809	11703
0.410	1280	2272	1689	1827	5812	2399	2723	1109	1809	11703
0.415	1280	7219	669	1827	5812	2399	803	7322	1809	11703
0.420	1445	7219	290	1827	5812	2399	2723	7322	1809	11703
0.425	1280	2272	669	1827	5812	2399	2723	7322	1809	11703
0.430	1445	7219	669	1827	5812	2399	2723	7322	594	11703
0.435	1445	2272	290	1827	5812	2399	803	7322	1809	11703
0.440	1445	7219	669	1827	5812	2399	2723	7322	1809	11703
0.445	1445	2272	669	1827	5812	2399	2723	7322	1809	742
0.450	1280	7219	1689	1827	5812	2399	2723	7322	1809	11703
0.455	1280	7219	669	1827	5812	2399	28	1109	1809	11703
0.460	1280	7219	2364	1827	5812	2399	803	1109	1809	742
0.465	1445	7219	290	1827	5812	2399	28	7322	1809	11703
0.470	1445	7219	669	1827	5812	2399	2723	7322	1809	11703
0.475	1445	7219	290	1827	5812	2399	803	7322	1809	11703
0.480	1445	7219	669	1827	5812	2399	803	7322	1809	11703
0.485	1445	2272	1689	1827	5812	2399	2723	7322	1809	742
0.490	1445	7219	2364	1827	5812	2399	28	7322	6017	11703
0.495	1445	7219	669	1827	5812	2399	803	7322	1809	11703
0.500	1445	2272	290	1827	5812	2399	803	7322	1809	11703
x_0	$a = 1.80$									
	1.80	1.81	1.82	1.83	1.84	1.85	1.86	1.87	1.88	1.89
0.400	293	2429	3130	4668	53	711	4908	9127	2400	4847
0.405	2037	2429	4958	492	8633	711	4908	9127	2311	4847
0.410	5323	2429	4958	492	53	711	2201	9127	2311	4847
0.415	121	2429	4958	542	53	711	4908	9127	2400	4847
0.420	5323	2429	3130	4668	53	711	4908	9127	2400	4847
0.425	2037	2429	4958	492	8633	711	4908	9127	2400	4847
0.430	5323	68	3130	492	53	711	4908	9127	2400	4847
0.435	5323	2429	3287	4668	53	711	4908	9127	2400	4847
0.440	5323	2429	3130	4668	53	711	4908	9127	2400	4847
0.445	5323	2429	3130	492	53	711	4908	9127	2400	4847
0.450	5323	2429	3130	542	8633	711	4908	9127	2400	383
0.455	5323	2429	3130	492	8633	711	2201	9127	2400	4847
0.460	5323	2429	3130	492	53	711	4908	9127	2400	4847
0.465	121	2429	4958	492	8633	711	4908	9127	2400	4847
0.470	5323	2429	4958	4668	53	711	4908	9127	2400	4847
0.475	293	2429	4958	492	53	711	4908	9127	2400	4847
0.480	293	2429	4958	542	53	711	4908	9127	2400	4847
0.485	2037	2429	3130	492	8633	711	4908	9127	2400	4847
0.490	121	2429	3130	492	53	711	4908	9127	646	4847
0.495	121	2429	3130	492	8633	711	4908	9127	2400	4847
0.500	121	2429	3130	4668	8633	711	4908	9127	2400	4847
x_0	$a = 1.90$									
	1.90	1.91	1.92	1.93	1.94	1.95	1.96	1.97	1.98	1.99
0.400	741	560	787	344	1586	4299	4572	3735	4311	1481
0.405	8544	560	787	344	1586	4299	4572	3735	124	3828
0.410	8544	560	688	344	647	4299	3630	751	4311	1481
0.415	8544	560	787	688	8949	4299	4572	751	4311	3828
0.420	8544	2389	787	344	1586	4299	4572	751	4311	3828
0.425	8544	560	787	344	8949	4299	4572	3735	4311	765
0.430	8544	560	787	344	8949	4299	4572	3735	4311	3828
0.435	8544	560	787	344	8949	4299	4572	3735	4311	3828
0.440	8544	560	787	344	8949	4299	4572	751	4311	3828
0.445	8544	560	688	344	1586	4299	4572	3735	227	3828
0.450	8544	560	787	344	8949	4299	4572	3735	4311	3828
0.455	8544	2389	787	344	1586	4299	4572	3735	4311	3828
0.460	8544	560	787	344	8949	4299	4572	3735	124	1481
0.465	8544	560	787	344	8949	4299	3630	3735	4311	1481
0.470	8544	2389	787	344	1586	4299	3630	3735	4311	1481
0.475	8544	560	787	344	1586	4299	3630	3735	4311	1481
0.480	8544	560	787	344	8949	4299	4572	3735	124	3828
0.485	8544	560	787	344	8949	4299	4572	3735	124	3828
0.490	8544	560	787	344	8949	4299	3630	751	4311	3828
0.495	8544	560	787	344	1586	4299	4572	3735	4311	3828
0.500	8544	560	787	344	8949	4299	494	3735	4311	3828

周期長の調査より、有限精度で実装されたテント写像の軌道 $\{x_i\}$ について、以下に記す関係があることが判る。

パラメータ a ($1 < a < 2$) のテント写像を $f_a : I'_a \rightarrow I'_a$ ($I'_a = (0, 1)$) とする。有限精度を考えているので、区間 I'_a に含まれる点の数は有限個で $|I'_a| = 2^t - 1$ である（或は有限集合の濃度 $\#(I'_a) = 2^t - 1$ ）。倍精度浮動小数点演算 ($t = 52$) の場合では、 m は約 $1 \sim 10$ が観測される（数値実験により探索した限りでは）。 m は a, t に依存して不規則に変化する（ m と a, t の詳細な関係については現時点では判らない）。各周期軌道を構成する点の集まりを P_1, P_2, \dots, P_m と表すことにする。 $P_i \cap P_j = \emptyset$ ($i \neq j$) である。当然ながら $P_i \subset I'_a$ ($1 \leq i \leq m$) である。また、 $\bigcup_{i=1}^m P_i (= P_1 \cup P_2 \cup \dots \cup P_m) \subseteq I_a^F \subset I'_a$ である（ただし $I_a^F = [a(1 - \frac{a}{2}), \frac{a}{2}]$ ）。前述の数値実験の結果より、倍精度浮動小数点演算 ($t = 52$) の場合では、周期軌道の周期長すなわち $|P_i|$ はおおよそ $10^6 \sim 10^8$ で、周期軌道を構成する点の数はおおよそ $\bigcup_{i=1}^m |P_i| = |\bigcup_{i=1}^m P_i| \approx 10^9 (\approx 2^{30})$ である。1回以上の写像後に P_i 上の点に至る点の集まりを Q_i とする（図2.16における枝葉の部分（周期軌道以外の点））。 $Q_i = \{x | x \in I'_a, f_a^l(x) \in P_i, l \geq 1\}$ ($1 \leq i \leq m$)。 $Q_i \cap Q_j = \emptyset$ ($i \neq j$) である。尚、 $Q_i \cap P_i = \emptyset$ である。 $(\bigcup_{i=1}^m P_i) \cap (\bigcup_{i=1}^m Q_i) = \emptyset$, $(\bigcup_{i=1}^m P_i) \cup (\bigcup_{i=1}^m Q_i) = I'_a$ の関係にある。

上述の内容、および、有限精度で実装されたテント写像やロジスティック写像の性質に関する最近の研究報告 [15] ~ [18], [36] ~ [45] をまとめると、有限精度（デジタル計算機）で実装された場合におけるテント写像（概ねパラメータは $1.5 < a < 2$ ）は、経験的に以下に記す性質を有すると整理できる（数値実験の結果）。

性質 2.4.1 初期値を出発した軌道は最終的に周期軌道に至る（図2.16）。

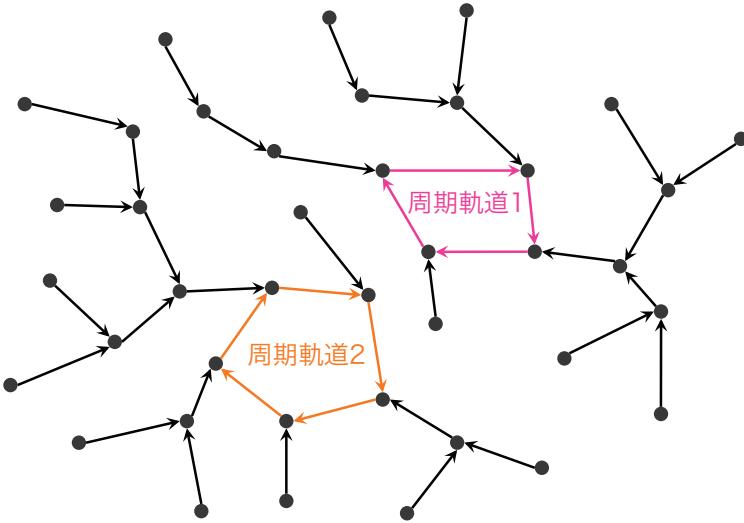
性質 2.4.2 同一のパラメータ、同一の演算精度、演算法の下では、周期軌道は複数個観測される（図2.16）。どの周期軌道に至るかは初期値に依存する。初期値と周期軌道の対応関係は知られていない。

性質 2.4.3 周期軌道の周期長は様々な長さのものが観測されるが、周期軌道を構成する点が占める数の割合は、与えられた演算精度で考えうる状態の総数に対して極めて小さいという傾向が見られる（表2.1、表2.2より）。

性質 2.4.4 パラメータおよび演算精度、演算法が変化すると、周期軌道の数およびその周期長は変化する（表2.1表2.2と、表2.3表2.4の関係より）。両者の対応関係は知られていない。

上記の性質2.4.1に関して補足すると、区間 $I'_a = (0, 1)$ 上の全ての点を初期値 x_0 とする軌道 $\{x_i\}$ （系列 $\{x_i\}$ ）は、所定回数の写像後に区間 $[a(1 - \frac{a}{2}), \frac{a}{2}] \stackrel{\text{def}}{=} I_a^F$ （図2.13参照）内に含まれる周期軌道に落ち込む。

上記の性質2.4.3に関して補足すると、倍精度浮動小数点演算（仮数部の2進桁数が $t = 52$ ）で実装した場合は、周期軌道の周期長（ $f_a^l(x_i) = x_i$ となる l ）は概ね $10^6 \sim 10^8$ 程度である（表2.1、表2.2）。一方で、倍精度浮動小数点演算の場合に $I'_a = (0, 1)$ に含まれる点の数の総数は $2^{52} - 1 \approx 10^{15}$ なので、これに対して周期軌道を構成する点の数が占める割合はかなり小さいといえる。

図 2.16 $1 < a < 2$ のテント写像における軌道 $\{x_i\}$ のイメージ図

区間 $I'_a = (0, 1)$ 上の全ての点を初期値とする軌道は最終的に周期軌道に陥る

2.4.2 数値実験による経験分布の偏り（軌道 $\{x_i\}$ の偏り）について

文献 [6], [7] によると、パラメータ $a = 2$ のテント写像は（ルベーグ測度に対して絶対連続な）不变測度を有しており、理想的な環境で、無限桁の初期値を与えた場合に得られる軌道 $\{x_i\}_{i=0}^{\infty}$ は、区間 I_a 内のある点 $x \in I_a$ の近傍を何回も訪れ（そして、そのような x_0 が区間内の至る所に存在する）、また、その頻度は区間 I_a 内で等頻度であることが知られている。

一方で、パラメータ $1 < a < 2$ の場合は、 $a = 2$ の場合と異なり、不变測度を有するか否かについて詳しいことは判っていない。少なくとも、有限精度のデジタル計算機によって数値実験した限りでは（経験上の頻度分布）、軌道 $\{x_i\}_{i=0}^n$ が区間 I_a 内のある点 $x \in I_a$ の近傍を訪れる頻度には、位置 x に関係した明らかな偏りがある。尚、演算精度を変更しても、同一のパラメータ a であれば、ほぼ同じ形の分布は得られるが、微妙に異なるものとなる。

テント写像を有限精度の演算（倍精度浮動小数点演算）で実装した場合に観測される経験上の頻度分布を図 2.17 に示す。

これより、テント写像を有限精度の計算機で実装した場合は、 $1 < a < 2$ の場合には $a = 2$ に比べて長い周期の信号を得ることができるが、系列 $\{x_i\}$ （軌道 $\{x_i\}$ ）から写像ステップ i 毎に x_i の最上位ビットを抽出して構成された系列 $\{b_i\}$ は等頻度性を有していないことが容易に推測される。

しかしながら、写像の度に x_i の中位桁 8 ビットを抽出して得られた系列

$$w_i = x_i \times 2^{26} \bmod 256, \quad w_i = \{0, 1, 2, \dots, 255\} \quad (2.6)$$

を考えた場合は、 $x_i \times 2^{26} \bmod 256$ に関する頻度分布は等頻度性を有することが数値実験により確認できる（図 2.18）。

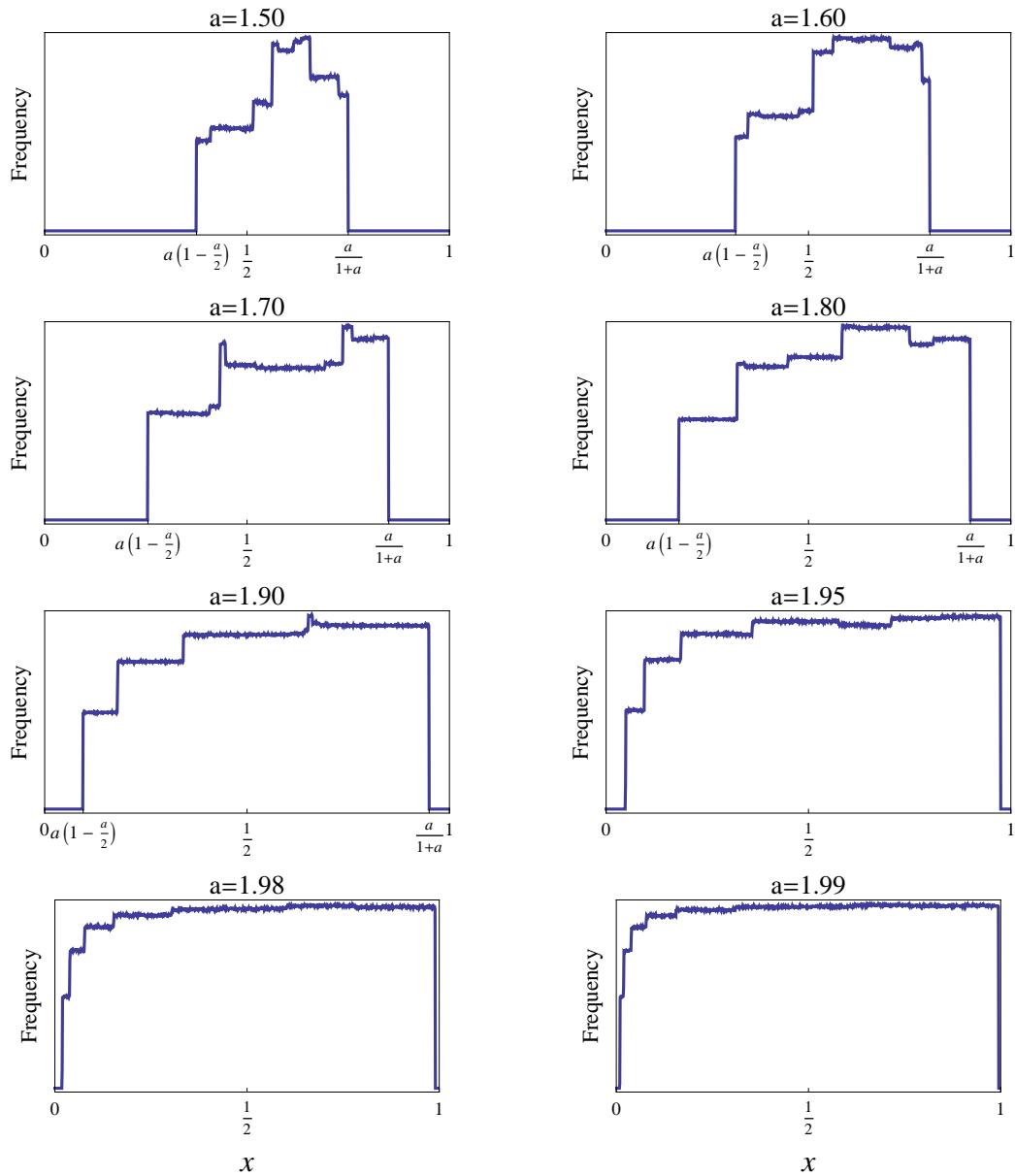
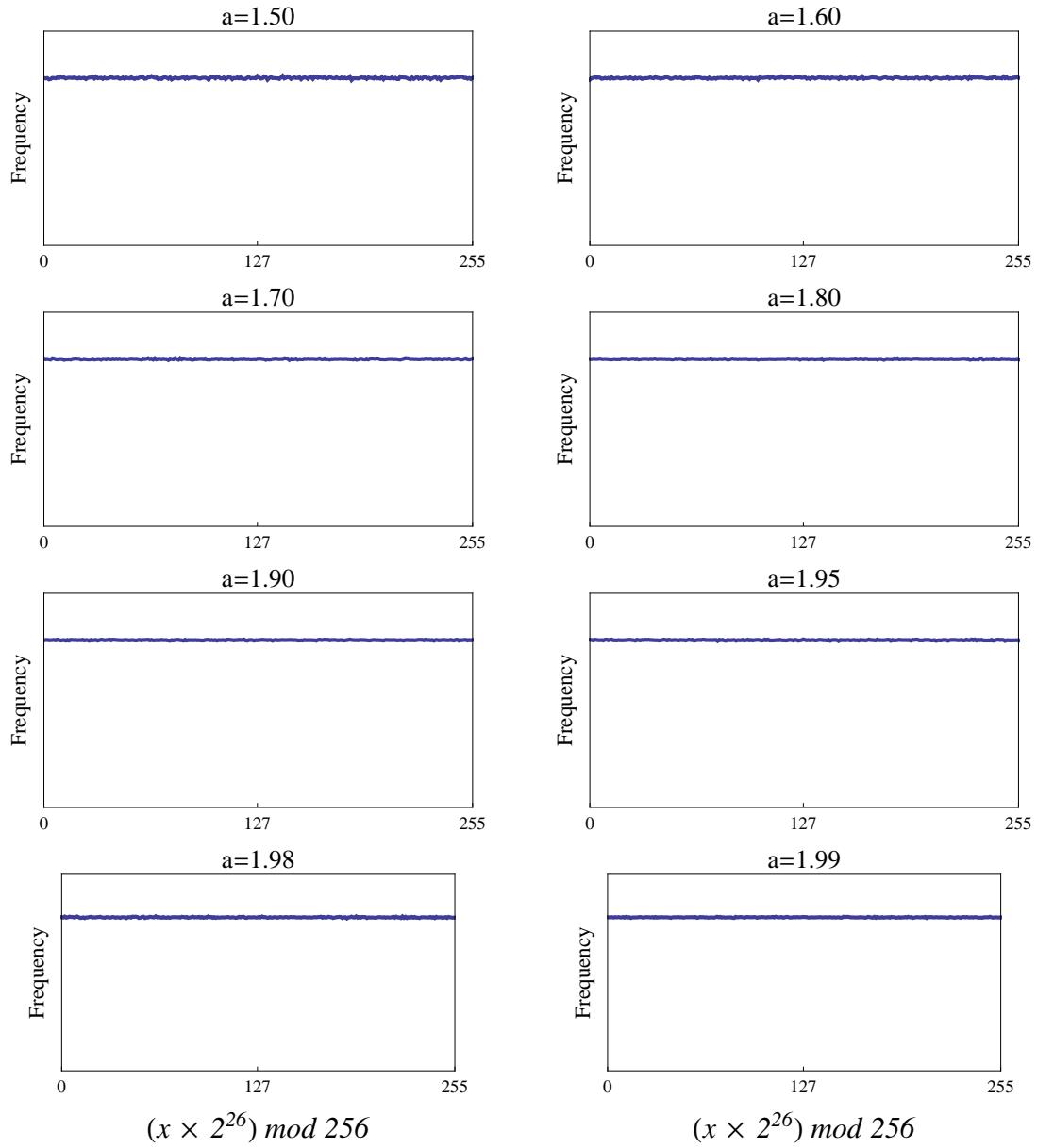


図 2.17 テント写像 ($1 < a < 2$) における経験上の頻度分布 (軌道 $\{x_i\}$ の偏り)

図 2.18 テント写像 ($1 < a < 2$) の中位桁 8 ビットを抽出した系列の経験上の頻度分布

2.5 テント写像を利用した擬似ランダムビット列の生成に関する初步的な案とその乱数検定結果

前節までの内容をまとめると， $a = 2$ の場合は理想的なランダムビット列を得ることができることが知られているが，それは無限精度の演算と無限桁の初期値を与えることが前提となっている。有限精度の演算（演算精度 t ）と有限桁の初期値を与えた場合は，高々 t ビットの系列しか得られない。 $1 < a < 2$ の場合は， $a = 2$ と比較して，長い周期の信号を得ることができるが，系列 $\{x_i\}$ （軌道 $\{x_i\}$ ）には偏りがあり，系列 $\{x_i\}$ の最上位ビットを抽出して構成された系列 $\{b_i\}$ の 0,1 の出現頻度は等頻度でない。一方で，図 2.18 より明らかであるが，系列 $\{x_i\}$ の下位側の桁を抽出した場合の等頻度性は良くなる傾向がある。図 2.18 では，演算精度 $t = 52$ に対して，上位 26 桁目から 8 ビット抽出した例を示したが，その 8-bit 等頻度性は良好である。

上記までで不明な点は周期長である。系列 $\{x_i\}$ の周期は，パラメータ a ，初期値 x_0 ，演算精度 t に依存して不規則に変化（関連性が現時点では判らない）するので制御は難しい。前節で示した数値実験の結果によると，倍精度浮動小数点演算では 10^6 程度あることが確認できる。文献 [18] においても，ロジスティック写像の場合でも倍精度浮動小数点演算で 10^6 程度であることが示されている。このことから，以下の実験 2.5.1 に示すごく単純な生成系を考え，さしあたり NIST 亂数検定（統計検定）を実施してみると，このごく単純な生成系から生成される擬似ランダムビット列は良質なランダム性を有することが判る。

実験 2.5.1 倍精度浮動小数点演算（演算精度 $t = 52$ ） で実装することを前提とする。初期値 $x_0 = 0.400001$ に固定し，パラメータ a を $1.5 < a < 2$ の範囲から 1 つ選ぶ。テント写像を反復 $x_{i+1} = f_a(x_i)$ するたびに x_i の小数点以下 26 ビット桁目を 1 ビット抽出して b_i を得る ($b_i = \lfloor x_i \times 2^{26} \rfloor \bmod 2$)。 $n = 1,000,000$ までに 1,000,000 ビットの系列を生成する。次に a を変えて同様のことを 1,000 回繰り返し，NIST 亂数検定の推奨量（1,000,000 ビット × 1,000 系列）を生成する。

NIST が示す評価は曖昧であるため，本論文の 5 章に記す評価法を用いて評価を行う（詳細は 5 章に記す）。5 章で示す評価法は，NIST 亂数検定を複数回実施して得られる統計量が，理論分布と適合しているか否かを検定項目毎に見るものである。ここでは，上記の NIST 亂数検定の推奨量のさらに 500 倍の被検定データを，異なる a を用いて生成し（重複して同じ a を選ばない），NIST 亂数検定を 500 回繰り返したときの統計量に対する評価結果を示す。結果は表 2.5 である。

検定項目は #1 ~ #161 まであり（詳細は表 5.1），それぞれの検定項目毎に p-value が示される。p-value は経験分布（実験値）と理論分布の適合度を表している。p-value が 0.01 以上ならば，当該検定項目に合格したとする。0.0001 未満は不合格とする。0.0001 ~ 0.01 の場合はグレーゾーンとして，いったん評価保留とする。本実験においては，検定項目 #49 と #91 がグレーゾーンとなり，他の検定項目の p-value は全て 0.01 以上であった。グレーゾーン（評価保留）となった検定項目は，5 章で示す評価法では他の手法を交えて総合的に判定するが仕組みとしている。ここでは，他の手法として母平均の推定と母分散の推定を行った。その結果，グレーゾーンにある 2 つの検定法は，母平均の推定，母分散の推定においては双方ともパスしたことから，当該 2 検定項目は「グレーゾーンで合格」と判断した。全ての検定項目がグレーゾーン以上で合格していることから，本生成系のランダム性は良いと判定する（最終判定）（表 2.6, 表 2.7）。

表 2.5 亂数検定結果

表は、実験 2.5.1 で示すテント写像を利用した初步的な生成法（パラメータ固定、上位 26 ビット目抽出）に対する、5 章で示す判定法によるランダム性の判定結果である（500set 分）。表内の数値は各検定項目（#1～#161）毎の二項分布（理論分布）への適合度を表す p-value である。#49 と #91 がグレーゾーン扱い（p-value が 0.0001 以上 0.01 未満）となった。その他の検定項目には合格した（p-value が 0.01 以上）。

#1	0.845304	#42	0.41611	#83	0.277476	#124	0.369926
#2	0.128618	#43	0.117094	#84	0.145982	#125	0.595336
#3	0.193565	#44	0.871996	#85	0.781807	#126	0.806884
#4	0.334484	#45	0.107115	#86	0.151111	#127	0.150089
#5	0.455372	#46	0.0411486	#87	0.873299	#128	0.485172
#6	0.535322	#47	0.718843	#88	0.83041	#129	0.319423
#7	0.164331	#48	0.706996	#89	0.908457	#130	0.406751
#8	0.920366	<u>#49</u>	<u>0.00715394</u>	#90	0.851927	#131	0.269355
#9	0.730263	#50	0.392689	<u>#91</u>	<u>0.00494132</u>	#132	0.53951
#10	0.388351	#51	0.24581	#92	0.668499	#133	0.775237
#11	0.849174	#52	0.466504	#93	0.349634	#134	0.659672
#12	0.942063	#53	0.109649	#94	0.480121	#135	0.589286
#13	0.826562	#54	0.377879	#95	0.070051	#136	0.907786
#14	0.550297	#55	0.970633	#96	0.524017	#137	0.351599
#15	0.417761	#56	0.387732	#97	0.150822	#138	0.660393
#16	0.967685	#57	0.0364168	#98	0.120435	#139	0.107016
#17	0.175259	#58	0.0915964	#99	0.813882	#140	0.845986
#18	0.798155	#59	0.667384	#100	0.426739	#141	0.476585
#19	0.352381	#60	0.448946	#101	0.722116	#142	0.714878
#20	0.986542	#61	0.726128	#102	0.394729	#143	0.760132
#21	0.65132	#62	0.518676	#103	0.399704	#144	0.0391465
#22	0.203786	#63	0.178545	#104	0.073736	#145	0.151441
#23	0.524109	#64	0.434808	#105	0.366145	#146	0.770845
#24	0.598836	#65	0.355142	#106	0.401554	#147	0.80292
#25	0.170211	#66	0.215595	#107	0.903793	#148	0.219769
#26	0.218315	#67	0.297334	#108	0.586525	#149	0.201913
#27	0.185264	#68	0.44761	#109	0.846196	#150	0.822163
#28	0.0971545	#69	0.277477	#110	0.713531	#151	0.965698
#29	0.723627	#70	0.600717	#111	0.0223778	#152	0.486428
#30	0.600032	#71	0.997152	#112	0.399031	#153	0.644316
#31	0.0960274	#72	0.97572	#113	0.0708602	#154	0.803157
#32	0.525017	#73	0.10512	#114	0.868101	#155	0.217527
#33	0.842781	#74	0.344561	#115	0.9938	#156	0.191824
#34	0.736399	#75	0.453119	#116	0.477947	#157	0.163466
#35	0.758262	#76	0.675169	#117	0.296981	#158	0.123605
#36	0.0579388	#77	0.233552	#118	0.0453045	#159	0.425447
#37	0.227821	#78	0.705276	#119	0.536992	#160	0.574181
#38	0.100859	#79	0.676684	#120	0.44245	#161	0.0134581
#39	0.476483	#80	0.497894	#121	0.600717		
#40	0.75458	#81	0.0139713	#122	0.446405		
#41	0.463652	#82	0.902754	#123	0.776259		

表 2.6 p-value がグレーゾーンにある検定項目の「PASS」数に関するヒストグラム

PASS 数 検定項目	PASS 数における観測度数																
	981 以下	982	983	984	985	986	987	988	989	990	991	992	993	994	995	996	997 以上
#49	3	10	10	10	9	23	33	50	63	57	79	56	32	24	25	9	7
#91	2	12	6	10	20	23	44	53	53	64	60	50	50	24	23	5	1

表 2.7 p-value がグレーゾーンにある検定項目の、二項分布への適合度、母平均推定、母分散推定

検定項目	二項分布への適合度検定			母分散既知での母平均の推定			母分散の推定			3 つの検定結果を考慮した上で判定		
	p-value	<結果>	$\hat{\mu}_{min}$	$\hat{\mu}_{max}$	<結果>	\hat{U}_{min}	\hat{U}_{max}	<結果>				
#49	0.00715394	<GRAY>	989.588	990.312	< >	8.820	12.226	< >				グレーゾーンで合格
#91	0.00494132	<GRAY>	989.356	990.080	< >	8.511	11.797	< >				グレーゾーンで合格

上記の実験 2.5.1 より，倍精度浮動小数点演算で実装したテント写像の中位桁を抽出して得られた系列は統計的にランダム性は良いことが確認された．ただ，本生成系を擬似ランダムビット生成法として提案するには，周期長の把握（演算精度に依存）や，計算機の演算特性差によって全く異なる軌道になってしまふ互換性問題の解決や，任意のパラメータにおいてもランダム性が得られる等に関する理論的な説明，等々が不可欠だと考える．特に情報セキュリティ分野での利用を考えるには，どの程度まで安全な運用が可能かに関する説明が不可欠である．安全性に関しては，本生成系に対する基本的な解析法／攻撃法に関する情報が必要で，本生成系に関しては多くのことが知られていない．将来的に本生成系の安全性の評価を可能とすることを目標として，次章では，本生成系に関する解析法に関する内容を述べる．

第3章

1次元非線形写像から得られる擬似ランダムビット列に対する初期値推測法およびパラメータ推測法

3.1 初期値推測法とは

3.1.1 初期値推測法とは

本稿で扱う初期値推測法は以下のことをいう（広義の定義）。

定義 3.1.1（初期値推測法の定義（広義の定義）） x_0 を初期値として，テント写像，ロジスティック写像，平方写像等の1次元非線形写像の n 回反復過程 $x_{i+1} = f(x_i)$ ($0 \leq i < n$) で得られる $n+1$ 個の値 $\{x_0, x_1, \dots, x_n\}$ を考える。この系列 $\{x_i\}$ をもとに，ある規則に従い生成された m ビットの2値化系列 $\{b_0, b_1, \dots, b_{m-1}\}$ が与えられたとする。このとき，2値化系列 $\{b_i\}$ の生成規則，およびパラメータ（テント写像の場合は a ，ロジスティック写像の場合は b ，平方写像の場合は c ）を既知として，当該擬似ランダムビット列を生成し得る初期値 x_0 の範囲を推測することをいう^{*1}。

上述および2章で触れた生成系に関しては，初期値および各パラメータがシード／鍵から導かれる「シード／鍵依存値」と考えられる。すなわち，本章で述べる初期値推測法，および次章で述べるパラメータ推測法とは，与えられた系列からシード／鍵情報を得る（鍵をリカバリする）手法とほぼ同義である。従って本推測法は，本生成系の実用性（安全性面）の評価を与える際には不可欠なツールであり，また，これによって安全性に関する多くの情報が得られると考えられる。

パラメータ $1 < a < 2$ のテント写像を反復する度に下位側の桁を抽出した場合と，さらにあるタイミングで内部状態（ a や x_i ）に変動を加える等の複雑化手法を併用した場合に得られる擬似ランダムビット列は，統計的に良質なランダム性を有することが経験的に判っている [11] ~ [17]。すなわち，最終的な目標は，下位側の桁を抽出した場合や，複雑化手法を併用した場合における推測法を得ることである。（しかしこれらは一般的に難しい。）一方，複雑化手法を併用するしないに關わらず，初期

^{*1} 広義の定義では，系列 $\{x_i\}$ から 2 値化系列 $\{b_i\}$ の生成規則は任意とする。ただし，生成規則は既知とする。尚，本論文においては，主として，2 値化系列の生成規則として第 i 回目の写像ごとに x_i の最上位ビットまたは上位から所定桁目のビットを抽出して，計 $n+1$ ビットのランダムビット列 $\{b_i\}$ を生成することを考える。これを狭義の定義とする。

値の推測に関しては、与えられた情報（擬似ランダムビット列）から、如何にして正確に x_i の軌道を再現（追跡）できるかが重要な鍵を握っている。そして、 x_i 軌道の追跡には、テント写像の場合であれば写像の度に式(2.1)のどちらの関数 ($f_a(x) = ax$ または $f_a(x) = a(1-x)$) が選ばれて合成されていくかが重要で、この情報は x_i の最上位ビットが握っている（すなわち b_i 系列）。従って、下位側桁の抽出の場合であっても、複雑化手法を併用する場合でも、最上位ビット抽出系列に対する初期値推測法に帰着するものと予想される。従って、本章の次節以降においては、まずは、比較的推測が容易な最上位ビット抽出系列に対する厳密な初期値範囲を推測する手法を整理することからはじめる。

解析にあたり注意すべき点は、擬似ランダムビット列の生成は、今日では有限精度のデジタル計算機（いわゆる PC）で生成するのが一般的だと考えられるが、有限精度で実装されたテント写像から得られる $\{x_i\}$ 系列は演算誤差の影響を受けていることである。つまり、実際に我々が現実的に得ることができる系列とは、式(2.1)が本来生成する系列（無限精度の場合に得られる系列）とは異なることを意識しなければならない。特にテント写像等は初期条件鋭敏性（SDIC 性）を有するので、有限精度の場合と、無限精度の場合（或は演算精度を考慮しない場合）では互いに全く異なる軌道となるため、その推測法も異なり、また、推測が困難になることが予測される。はじめに無限精度の場合（或は演算精度を考慮しない場合）について推測法を整理し、有限精度の演算で実装されたテント写像から得られる系列に対する解析法は本章の最後で触れる。

3.1.2 初期値推測法の先行研究

本論文で示す初期値推測法とほぼ目的を同じくする解析法としては、例えば文献 [18] ~ [30] がある。本論文で示す初期値推測法を含め、推測法に関する研究は（文献 [18] ~ [26]）は主として 4 つの種類に分類できる。[分類 1] は、Baptista によって示された 1 次元非線形写像を利用した暗号化手法 [32] (1998 年)、および、Alvarez らによって示された 1 次元非線形写像を利用した暗号化手法 [33] (1999 年) に対する解析法 / 攻撃法が、部分的に本論文で扱う初期値推測 / パラメータ推測の目的を果たすものであり、グレイコードに基づく推測法である [21] ~ [30]。[分類 2] は、大熊らによる記号力学系を利用した推測法である [18]。[分類 3] は、本間一糸井による写像の前後関係を探索していく手法である [19]。[分類 4] は、文献 [26] で示される推測法で、ランダムビット列 $\{b_i\}$ から n 回写像後の関数形 $f^n(x_0)$ を決定して、さらに最終値 x_n の存在範囲の条件を用いて $x_n = f^n(x_0)$ を x_0 について解く手法である。以下に、[分類 1 ~ 3] について簡単に記す（[分類 4] は次節以降で詳しく述べる）。

[分類 1] : グレイコード [31] に基づく推測法 [32] ~ [30]

Baptista、および Alvarez らは、1 次元非線形写像の反復回数を暗号文とする暗号化手法を示した [32][33]（この暗号化手法のアイデアを簡潔にまとめたものを付録 B.1 節に記した）。尚、Baptista、および Alvarez らの暗号系には解析法 / 攻撃法が存在し、本論文で示す初期値推測法と関係があるのものとしては、Alvarez ら [29]、Cusick [30]、Wu [22] らによって示された、最上位ビット抽出系列とグレイコード [31] B.2 節の関係を利用した解析法がある。

経緯について少し触れると、Alvarez らは平方写像（1D Quadratic Map）(式(2.3))^{*2} を反復す

^{*2} 1D Quadratic Map $x_{i+1} = f_c(x_i) = x_i^2 - c$ は、本来ならば 1 次元 2 次写像 / 1 次元 2 次の写像と呼ぶべきだが、本論文では単に平方写像と呼ぶことにする。1D(1 Dimensional) は、ユークリッド空間の次元を意味している。写像関数は x のみを更新するので 1 次元である。また写像関数は $x^2 - x$ なので 2 次（2 次方程式）である。

る度に最上位ビットを抽出した系列とグレイコードの関係を示した [29]。その後 Cusick は、上記の Alvarez ら [29] の内容について定理と証明を整理した [30]。Cusick により整理された定理 [30] は、平方写像に限らず、テント写像、ロジスティック写像等の写像関数の形が定義域を中心に山型（図）になっている写像においても基本的に成立する。Wu らは、Cusick により示された定理 [30] をロジスティック写像の場合において判りやすく整理したものを示した [22]。この 3 つの文献 [29][30][22] に示される定理のうち、重要な 3 つの定理を、テント写像の場合について表したものを作成 B.5 節に記した（定義 B.5.1、定理 B.5.2、定理 B.5.3、定理 B.5.4）。

上記のグレイコードを利用した初期値推測 [29] は、観測ビット列 $\{b_i\}_{i=0}^n \equiv \mathbf{b}$ のグレイコードのオーダー（付録 B.2.2 節）を O_G とすると、観測ビット列 \mathbf{b} を生成し得る初期値は、 $O_{G+1} \stackrel{\text{def}}{=} (O_G 2^{n+1} + 1)/2^{n+1}$ となる系列 \mathbf{b}_+ を生成し得る初期値 x_{0+} と、 $O_{G-1} \stackrel{\text{def}}{=} (O_G 2^{n+1} - 1)/2^{n+1}$ となる系列 \mathbf{b}_- を生成し得る初期値 x_{0-} の間にあるという関係を利用する。ただ、この手法は厳密な初期値範囲^{*3}を得られない場合がある（例えば、パラメータ $a < 2$ のテント写像は、考えうる全てのビットパターンを生成し得ないため、 O_{G+1} となる系列 \mathbf{b}_+ や、 O_{G-1} となる系列 \mathbf{b}_- が存在しない場合がある）。また、境界を含むか否かについては基本的に追跡できない（境界を含むか含まないかは対象外である）。

[分類 2]：記号力学系に基づく推測法 [18]

大熊らは、記号力学系に基づく初期値推測法を示した [18]。この推測法は、 $a = 2$ のテント写像は極めて特殊な性質を有することを利用している。

$a = 2$ のテント写像の n 回反復過程より計 $n + 1$ ビットの最上位ビット抽出系列 $\{b_i\}_{i=0}^n$ が与えられたとする。 $a = 2$ の場合は、 2^{n+1} 個ある全てのビットパターン ($b_i = \{0, 1\}$) を等頻度に生成することができて、それぞれ各ビットパターンを生成する初期値の幅は等しく $1/2^{n+1}$ である。記号力学系より、左から (0 から) l 番目の区間とビット列の関係は

$$l = 2^{n+1} \sum_{j=0}^n \left(2^{-(j+1)} \bigoplus_{i=0}^j b_i \right) \quad (3.1)$$

であることが知られている [3]。これより、系列 $\{b_i\}_{i=0}^n$ を生成し得る初期値の区間は

$$\sum_{j=0}^n \left(2^{-(j+1)} \bigoplus_{i=0}^j b_i \right) < x_0 < \sum_{j=0}^n \left(2^{-(j+1)} \bigoplus_{i=0}^j b_i \right) + 2^{-(n+1)} \quad (3.2)$$

と求めることができる。

本推測法は、パラメータ $a = 2$ のテント写像、およびこれと位相共役の関係にある写像のみに限定されており、パラメータ $1 < a < 2$ では適切な初期値範囲を得られない（未対応である）。また、[分類 1] と同様に境界を含むか否かについては追跡できない。

[分類 3]：写像の前後関係を細かく探索していく手法 [19]

先に示した 2 つの分類のものは、パラメータ ($1 < a < 2$) において、適切な初期値範囲が得られない場合があるか、または非対応であるが、本間・糸井らは、任意のパラメータ $1 < a \leq 2$ のテント写

^{*3} 観測ビット列 $\{b_i\}_{i=0}^n \equiv \mathbf{b}$ を生成し得る正確な初期値範囲のこと

像から得られた最上位ビット抽出系列に対してほぼ厳密な初期値範囲を得る初期値推測アルゴリズムを示した [19] . 示されるものはアルゴリズムであって、解の数理構造までは整理されていため、数理的な全体像は掴みづらいものとなっている（例えば式 (3.2) のような一般解は示されない）. 尚、ほぼ厳密という意味は、本アルゴリズムを例えれば Mathematica (数式処理系) で追跡した場合には、厳密な解の範囲を得ることもできるが、数値計算アルゴリズムとして数値処理する場合には、演算誤差のために境界付近の値は定かでないということである .

[分類 4] : 最終値 x_n の存在範囲条件を用いて多項式 $x_n = f^n(x_0)$ の解を求める手法 [26]

著者らは、文献 [26] にて、任意のパラメータ $1 < a \leq 2$ のテント写像からの最上位ビット抽出系列に対する、厳密な初期値解を得る手法を示した .

当推測法は、擬似ランダムビット列 $\{b_i\}$ から、最終値 $x_n = f^n(x_0)$ に関する多項式関数形を決定できること、および最終値 x_n の存在範囲の条件を用いて、当多項式を x_0 について解くといったごく初步的な解析手法によって説明できる点が特徴である . 尚、本手法によって厳密な初期値範囲を得るには、最終値 x_n の厳密な存在範囲を知る必要がある . 一般に $1 < a < 2$ の場合はこれが困難な場合があるが、区間の遷移の仕組みを状態遷移図としてまとめたことによって、最終値 x_n の厳密な存在範囲を簡単に求めることができるようになった . 詳細は次節以降で述べる .

3.2 テント写像の最上位ビット抽出系列に対する初期値推測法（必要条件からの解）[23],[26]

本節では、はじめに本節で示す推測法の推測対象となる擬似ランダムビット列 / 擬似ランダムビット列生成法、およびその初期値推測法について定義する . 次いで、写像の n 回の反復によって得られる観測ビット列（擬似ランダムビット列）から n 回写像関数形（多項式関数形） $f_a^n(x_0)$ を決定できることを示す . 最後に最終値 x_n の存在範囲の必要条件から得た $x_n = f_a^n(x_0)$ を x_0 について解いて整理した解を示す .

定義 3.2.1 (擬似ランダムビット列の生成 (最上位ビット抽出)) $x_0 \in I_a$, ($I_a = [0, 1]$) を初期値として、パラメータ a ($1 < a \leq 2$) のテント写像 (式 (3.3)) の n 回反復過程 $x_{i+1} = f_a(x_i)$ ($0 \leq i < n$) で得られる計 $n + 1$ 個の値 $\{x_0, x_1, \dots, x_n\}$ ($= \{x_i\}_{i=0}^n$) を考える . ここで扱う擬似ランダムビット列^{*4}とは、第 i 回目 ($i \geq 0$) の写像ごとに、式 (3.4) に従い x_i の最上位ビットを抽出して構成された計 $n + 1$ ビットの系列 $\{b_0, b_1, \dots, b_n\}$ ($= \{b_i\}_{i=0}^n$) のことをいう . 尚、当該擬似ランダムビット列の

^{*4} 本論文では、 $S_a(x_0, n) \equiv \{b_0, b_1, \dots, b_n\}$ のことを、擬似ランダムビット列と称する以外に、最上位ビット抽出系列、観測ビット列と称する場合もある .

生成関数を $S_a(x_0, n)$ と表す .

$$f_a : I_a \mapsto I_a, (I_a \in [0, 1])$$

$$f_a(x) = \begin{cases} ax & (x < 1/2) \\ a(1-x) & (x \geq 1/2) \end{cases} \quad (3.3)$$

$$b_i = \begin{cases} 0 & (x_i < 1/2) \\ 1 & (x_i \geq 1/2) \end{cases} \quad (3.4)$$

$$S_a(x_0, n) \equiv \{b_0, b_1, \dots, b_n\} \quad (= \{b_i\}_{i=0}^n) \quad (3.5)$$

定義 3.2.2 (定義 3.2.1 の生成法から生成された擬似ランダムビット列に対する初期値推測法) 本節で述べる初期値推測法とは , 定義 3.2.1 で示される生成法 $S_a(x_0, n)$ により生成された計 $n+1$ ビットの擬似ランダムビット列 $\{b_i\}_{i=0}^n$ が与えられたときに , パラメータ a ($1 < a \leq 2$) を既知として , 当該系列 $\{b_i\}_{i=0}^n$ を生成し得る初期値 x_0 の範囲を推測する手法のことを言う .

3.2.1 観測ビット列を用いた最終値 $x_n = f^n(x_0)$ の多項式関数形の決定

本推測法の着眼点は , 定義 3.2.1 で示される生成法 $S_a(x_0, n)$ において , x_i から擬似ランダムビット b_i を抽出する際に , 最上位ビット抽出式 (3.4) によって 0 または 1 が選ばれる領域と , テント写像式 (3.3) の $f_a(x) = ax$ (ここでは左側関数とよぶ) と , $f_a(x) = a(1-x)$ (ここでは右側関数とよぶ) の定義域が同じことである . すなわち以下の関係が判る .

$$\begin{cases} b_i = 0 & \Rightarrow x_i < 1/2 \Rightarrow \text{次は左側関数によって写像される } x_{i+1} = ax_i \\ b_i = 1 & \Rightarrow x_i \geq 1/2 \Rightarrow \text{次は右側関数によって写像される } x_{i+1} = a(1-x_i) \end{cases} \quad (3.6)$$

この関係を見していくと , 擬似ランダムビット列 $\{b_i\}_{i=0}^n$ と , テント写像の n 回反復の合成写像 $f_a^n(x_0)$ の関係について以下の定理を得る .

定理 3.2.3 x_0 を初期値とし , 傾き a を既知とする . 定義 3.2.1 で示される生成法 $S_a(x_0, n)$ により生成された計 $n+1$ ビットの擬似ランダムビット列 (観測ビット列) $\{b_i\}_{i=0}^n$ が与えられたとき , 式 (3.3) の n 回反復による合成写像 $f_a^n(x_0)$ は , 観測ビット列 $\{b_i\}_{i=0}^n$ を用いて以下のように決定される .

$$x_n = f_a^n(x_0) = \sum_{i=1}^n p_i a^i + q a^n x_0 \quad (3.7)$$

$$p_i = \frac{b_{n-i}}{\hat{b}_{n-i}} \prod_{k=n-i}^{n-1} \hat{b}_k \quad (3.8)$$

$$q = \prod_{k=0}^{n-1} \hat{b}_k \quad (3.9)$$

$$\hat{b}_i = 1 - 2b_i \quad (3.10)$$

証明 式 (3.7) ~ (3.10) をまとめて記すと以下である .

$$x_n = f_a^n(x_0) = \sum_{i=1}^n \left(a^i \frac{b_{n-i}}{\hat{b}_{n-i}} \prod_{k=n-i}^{n-1} \hat{b}_k \right) + a^n x_0 \prod_{k=0}^{n-1} \hat{b}_k \quad (3.11)$$

一方で、テント写像式(3.3)は、ビット抽出ルール式(3.4)と、式(3.10)を用いて以下の式で表わすことができる。

$$\begin{aligned}x_{i+1} &= f_a(x_i) \\&= (1 - b_i)(ax_i) + b_i(a(1 - x_i)) \\&= b_i a + (1 - 2b_i)ax_i \\&= b_i a + \hat{b}_i ax_i\end{aligned}\tag{3.12}$$

以降において、式(3.11)が任意の自然数 n について成立していることを帰納的に示す。

はじめに $n = 1$ のときに式(3.11)が成り立つことを示す。式(3.12)より、

$$\begin{aligned}x_1 &= f_a(x_0) \\&= b_0 a + \hat{b}_0 ax_0 \\&= a \frac{b_0}{\hat{b}_0} \hat{b}_0 + ax_0 \hat{b}_0\end{aligned}\tag{3.13}$$

であることから、これは式(3.11)において $n = 1$ とした場合に他ならない。すなわち $n = 1$ のときに式(3.11)は成立する。

次に式(3.11)が任意の自然数 $n = m$ ($m \geq 1$)について成立すると仮定したときに、 $n = m + 1$ についても成立することを示す。 $n = m + 1$ のときは、式(3.12)より、

$$\begin{aligned}x_{m+1} &= f_a(x_m) \\&= b_m a + \hat{b}_m ax_m \\&= ab_m + ab_m \hat{b}_m x_m\end{aligned}$$

ここで、 $n = m$ ($m \geq 1$)のときに式(3.11)が成立するという仮定から、

$$\begin{aligned}x_{m+1} &= ab_m + ab_m \left\{ \sum_{i=1}^m \left(a^i \frac{b_{m-i}}{\hat{b}_{m-i}} \prod_{k=m-i}^{m-1} \hat{b}_k \right) + a^m x_0 \prod_{k=0}^{m-1} \hat{b}_k \right\} \\&= ab_m + ab_m \sum_{i=1}^m \left(a^i \frac{b_{m-i}}{\hat{b}_{m-i}} \prod_{k=m-i}^{m-1} \hat{b}_k \right) + ab_m a^m x_0 \prod_{k=0}^{m-1} \hat{b}_k \\&= ab_m + \sum_{i=1}^m \left(a^{i+1} \frac{b_{m-i}}{\hat{b}_{m-i}} \prod_{k=m-i}^m \hat{b}_k \right) + a^{m+1} x_0 \prod_{k=0}^m \hat{b}_k\end{aligned}\tag{3.14}$$

の関係を得る。

ここで $j = i + 1$ とすると、式(3.14)は、以下の式(3.15)として表すことができる。

$$x_{m+1} = ab_m + \sum_{j=2}^{m+1} \left(a^j \frac{b_{m-j+1}}{\hat{b}_{m-j+1}} \prod_{k=m-j+1}^m \hat{b}_k \right) + a^{m+1} x_0 \prod_{k=0}^m \hat{b}_k\tag{3.15}$$

また、ここで、式(3.15)の第2項目の \sum の中身を U_j とおくと、

$$U_j = a^j \frac{b_{m-j+1}}{\hat{b}_{m-j+1}} \prod_{k=m-j+1}^m \hat{b}_k\tag{3.16}$$

である。このとき、式(3.15)の第1項目は U_1 と表すことができる。

$$U_1 = a \frac{b_m}{\hat{b}_m} b_m^{\wedge} = ab_m \quad (3.17)$$

これより、式(3.15)は以下の式(3.18)と表すことができる。

$$x_{m+1} = \sum_{j=1}^{m+1} \left(a^j \frac{b_{m+1-j}}{\hat{b}_{m+1-j}} \prod_{k=m+1-j}^m \hat{b}_k \right) + a^{m+1} x_0 \prod_{k=0}^m \hat{b}_k \quad (3.18)$$

式(3.18)は、 $n = m + 1$ としたときの式(3.11)に等しい。よって、式(3.11)は任意の自然数 n について成立する。

□

式(3.7)～(3.10)より、最終値 x_n は、観測ビット列 $\{b_i\}_{i=0}^n$ を用いて、初期値 x_0 を唯一の未知変数とする1次式として表せる。これより、区間 $[0, 1]$ 上で任意に選ばれた1つの x_0 に対応する1つの x_n が存在することが判る（逆に1つの x_n に対応する1つの x_0 が存在する）。従って、 x_n の厳密な存在範囲を知ることができれば、初期値 x_0 の厳密な存在範囲を、方程式 $x_n = f_a^n(x_0)$ の解として得ることができる。しかし、一般的には x_n の厳密な存在範囲を知ることは容易でない場合が多い（ x_n の厳密な存在範囲の求め方は3.3節で述べる）。 x_n の存在範囲の必要条件（最上位ビット抽出ルール式(3.4)）を用いた場合の解を次節に示す。

3.2.2 最終値 $x_n = f_a^n(x_0)$ の存在範囲の必要条件から得た初期値解

推測法 3.2.4（最終値 x_n の存在範囲の必要条件から得られた解） 最上位ビット抽出ルール式(3.4)より、最終ビット b_n の情報から最終値 x_n の存在範囲について以下に示す必要条件を得る。

$$\begin{cases} b_n = 0 \Rightarrow 0 \leq x_n < 1/2 \\ b_n = 1 \Rightarrow 1/2 \leq x_n \leq 1 \end{cases} \quad (3.19)$$

この不等式を前節で示した式(3.7)～(3.10)を用いて、初期値 x_0 について整理すると以下の式(3.20)～(3.23)を得る。

(i) $b_n = 0, q > 0$ のとき

$$\frac{-\sum_{i=1}^n p_i a^i}{q a^n} \leq x_0 < \frac{1/2 - \sum_{i=1}^n p_i a^i}{q a^n} \quad (3.20)$$

(ii) $b_n = 0, q < 0$ のとき

$$\frac{1/2 - \sum_{i=1}^n p_i a^i}{q a^n} < x_0 \leq \frac{-\sum_{i=1}^n p_i a^i}{q a^n} \quad (3.21)$$

(iii) $b_n = 1, q > 0$ のとき

$$\frac{1/2 - \sum_{i=1}^n p_i a^i}{q a^n} \leq x_0 \leq \frac{1 - \sum_{i=1}^n p_i a^i}{q a^n} \quad (3.22)$$

(iv) $b_n = 1, q < 0$ のとき

$$\frac{1 - \sum_{i=1}^n p_i a^i}{q a^n} \leq x_0 \leq \frac{1/2 - \sum_{i=1}^n p_i a^i}{q a^n} \quad (3.23)$$

上記に示した解(式(3.20)~(3.23))は、 x_n の存在範囲の必要条件(ビット抽出ルール式(3.4))により得た解であり、実際に与えられた擬似ランダムビット列 $\{b_i\}$ を生成し得る初期値範囲よりも若干広い範囲を示す場合がある。このことは、実際の最終値 $x_n = f_a^n(x_0)$ が存在する範囲は、区間 $[0, 1/2]$ または $[1/2, 1]$ よりも狭い場合があることと関係している。 $a = 2$ の場合の不確かさは、式(3.20)~(3.23)で示される境界のを含むか否か程度であるが(境界値は正しい)、 $1 < a < 2$ の場合は解として不適切な区間をも含んでいる。

つまり、本推測法で厳密な初期値 x_0 の範囲を得るには、厳密な最終値 x_n の範囲を知ることが重要になる。次節以降では、テント写像の特性を考慮することによって、最終値 x_n の範囲を厳密に求める手法について触れる。はじめに、比較的容易である傾き $a = 2$ の場合を考え、次いで $1 < a < 2$ について整理する。

3.2.3 本節のまとめ

本節では、観測ビット列から最終値 $x_n = f_a^n(x_0)$ の多項式関数形を決定できることを示した。また、ビット抽出ルールから最終ビット b_n が抽出された最終値 x_n の存在範囲(必要条件)を知ることができる点を利用して、多項式関数 $x_n = f_a^n(x_0)$ を初期値 x_0 について解いて初期値範囲(初期値解)を得るという手法を示した。ただし、一般に最終値 x_n の存在範囲は、ビット抽出ルール式(3.4)で示される範囲よりも狭いため、本節で示した初期値解は厳密ではない(真の初期値範囲よりも若干広い範囲を示す(狭いことはない))。次節以降では、最終値 x_n の範囲を厳密に求める手法について触れ、これより厳密な初期値解を得る手法を示す。

3.3 $a = 2$ のテント写像の最上位ビット抽出系列に対する初期値推測法(厳密な解)[26]

本節では傾き $a = 2$ の場合の厳密な初期値解を示す。 $a = 2$ の場合は、結論からすると、前節で示した必要条件から得られた解(式(3.20)~(3.23))との差は、境界を含むか否か(開区間 or 閉区間)が異なるだけであるが、写像の性質として重要な点が含まれている。以降では、具体的にテント写像の定義域を分割した「区間」が $a = 2$ のテント写像 f_a によって、どのように写像されるか(推移するか)について示す。

3.3.1 区間から区間への写像の連鎖の様子～状態遷移図

傾き $a = 2$ のテント写像 $f_a(x)$ の定義域 $I_a = [0, 1]$ を、ビット抽出区間(式(3.4))に従って、 $A = [0, 1/2]$, $B = [1/2, 1]$ と分割し、

$$\begin{cases} b_i = 0 \Rightarrow x_i \in [0, 1/2] \equiv A \\ b_i = 1 \Rightarrow x_i \in [1/2, 1] \equiv B \end{cases}$$

それぞれの区間が写像される範囲を調べることから始める。各区間の定義域とその写像先の関係は以下の式(3.24)~(3.25)である。 B は f_a によって $A \cup B$ へ写像されるが、 A は f_a によって B の境界

値 $x = 1$ を含まない範囲 $A \cup B'$ に写像される。

$$A = [0, 1/2) \rightarrow [0, 1) = A \cup B' \quad (3.24)$$

(ただし, $B' = [1/2, 1)$)

$$B = [1/2, 1] \rightarrow [0, 1] = A \cup B \quad (3.25)$$

補足すると, 仮に $x_i \in A$ とすると (この場合は $b_i = 0$ である), 式 (3.24) より, $x_{i+1} = f_a(x_i) \in A$ または $x_{i+1} = f_a(x_i) \in B'$ が生じているということになる。そして, 仮に $b_{i+1} = 0$ であれば, $x_{i+1} = f_a(x_i) \in A$ が生じていて, $b_{i+1} = 1$ であれば, $x_{i+1} = f_a(x_i) \in B'$ が生じていることが判る。

$$\begin{cases} x_i \in A & \mapsto x_{i+1} \in A, (\text{if } b_{i+1} = 0) \\ x_i \in A & \mapsto x_{i+1} \in B', (\text{if } b_{i+1} = 1) \end{cases}$$

後者が生じている場合では, $x_{i+1} \in B' = [1/2, 1) \subset B$ なので, $b_{i+1} = 1$ であっても, $x_{i+1} \in B'$ ($= [1/2, 1)$) であり, ビット抽出ルールで示される範囲よりも狭い (境界 $x = 1$ を含まない) ということが判る。前節で示した前節で示した必要条件から得られた解 (式 (3.20) ~ (3.23)) との差が生じるポイントはここである。

次に, 式 (3.24) に関して B' が次のステップ以降にどのように写像されるかを考えると以下となっている。

$$B' = [1/2, 1) \rightarrow (0, 1] = A' \cup B \quad (3.26)$$

(ただし, $A' = (0, 1/2)$)

$$A' = (0, 1/2) \rightarrow (0, 1) = A' \cup B' \quad (3.27)$$

3.3.2 状態遷移図を用いた最終値 $x_n = f_a^n(x_0)$ の厳密な存在範囲の取得

上記より, 傾き $a = 2$ の場合は, 式 (3.24) ~ (3.27) に示される 4 つの区間の写像の連鎖で構成されていることが判る。この区間から区間への推移 (写像の連鎖) の様子を状態遷移図としてまとめたのが図 3.1 である。

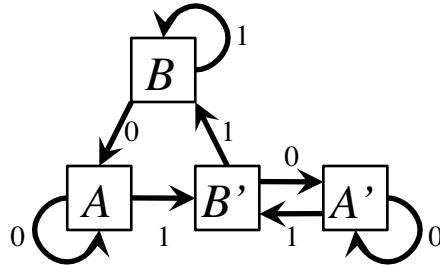


図 3.1 パラメータ $a = 2$ のときに x_i が含まれる区間の状態遷移図

状態遷移図 3.1 の見方を説明する。はじめに初期値 x_0 の存在する区間を決定する。ここでは, 定義 3.2.1 よりテント写像の定義域は $I_a = [0, 1]$ としているので, 初期値が含まれる区間は $[0, 1/2) = A$, または $[1/2, 1] = B$ である。これは観測ビット b_0 より, $b_0 = 0 \Rightarrow x_0 \in A$, $b_0 = 1 \Rightarrow x_0 \in B$ と一意的に決定される (A' , B' ではない点に注意)。そして, 次のビット $b_1 = 0$ な

らば0の矢印の方向に進めて， $b_1 = 1$ ならば1の矢印の方向に進めるときの状態（ x_1 が含まれる区間）に行き当たる。あくまでも，区間 A からの遷移（写像先）は，式(3.24)より， $A \cup B'$ であるのだが，観測ビット列 $\{b_i\}$ が与えられていれば，事後処理的（事後情報から）にどちらの区間に遷移した（写像された）かが判るのでこの操作が成り立つ。尚，いうまでもないが，この状態遷移図上で状態を1つ進めていく操作とは， f_a によって1回写像することに対応している。この操作を観測ビット列 $\{b_i\}$ に沿って（ $\{b_i\}$ に従って）繰り返していくと，第*i*回目の写像後の値 $x_i = f_a^i(x_0)$ が含まれる区間を厳密に求めることができる。すなわち最終値 x_n が含まれる区間が厳密に求めることができる。

3.3.3 必要十分性を考慮した初期値解

推測法 3.3.1 ($a = 2$ において最終値 x_n の厳密な存在範囲から得られた解) 状態遷移図を用いて求めた，最終値 x_n が含まれる区間が X_n （ $x_n \in X_n$ ， $X_n = \{A, A', B, B'\}$ ）であったとする。 $x_n = f_a^n(x_0) \in X_n$ を，区間 X_n の範囲を用いて x_0 について解いたものが求めようとする初期値の範囲である。

すなわち， $X_n = A$ （ $x_n \in A$ ）の場合は， $0 \leq x_n (= f_a^n(x_0)) < 1/2$ を x_0 について解いたものがこの場合の解で，以下の式(3.28)である（前節で示した式(3.20)，式(3.21)がそのまま厳密な解を与えていた）。 $X_n = A'$ （ $x_n \in A'$ ）の場合は， $0 < x_n (= f_a^n(x_0)) < 1/2$ を x_0 について解いたものがこの場合の解で，以下の式(3.29)である。 $X_n = B$ （ $x_n \in B$ ）のときは， $1/2 \leq x_n (= f_a^n(x_0)) \leq 1$ を x_0 について解いたものがこの場合の解で，以下の式(3.30)である（前節で示した式(3.22)，式(3.23)がそのまま厳密な解を与えていた）。 $X_n = B'$ （ $x_n \in B'$ ）の場合は， $1/2 \leq x_n (= f_a^n(x_0)) < 1$ を x_0 について解いたものがこの場合の解で，以下の式(3.31)である。

(i)' $b_n = 0$ ， $X_n = A$ （ $x_n \in A$ ）のとき $(\Rightarrow 0 \leq x_n (= f_a^n(x_0)) < 1/2)$

$$\Rightarrow \begin{cases} \frac{-\sum_{i=1}^n p_i a^i}{q a^n} \leq x_0 < \frac{1/2 - \sum_{i=1}^n p_i a^i}{q a^n} & (q > 0 \text{ のとき}) \\ \frac{1/2 - \sum_{i=1}^n p_i a^i}{q a^n} < x_0 \leq \frac{-\sum_{i=1}^n p_i a^i}{q a^n} & (q < 0 \text{ のとき}) \end{cases} \quad (3.28)$$

(ii)' $b_n = 0$ ， $X_n = A'$ （ $x_n \in A'$ ）のとき $(\Rightarrow 0 < x_n (= f_a^n(x_0)) < 1/2)$

$$\Rightarrow \begin{cases} \frac{-\sum_{i=1}^n p_i a^i}{q a^n} < x_0 < \frac{1/2 - \sum_{i=1}^n p_i a^i}{q a^n} & (q > 0 \text{ のとき}) \\ \frac{1/2 - \sum_{i=1}^n p_i a^i}{q a^n} < x_0 < \frac{-\sum_{i=1}^n p_i a^i}{q a^n} & (q < 0 \text{ のとき}) \end{cases} \quad (3.29)$$

(iii)' $b_n = 1$ ， $X_n = B$ （ $x_n \in B$ ）のとき $(\Rightarrow 1/2 \leq x_n (= f_a^n(x_0)) \leq 1)$

$$\Rightarrow \begin{cases} \frac{1/2 - \sum_{i=1}^n p_i a^i}{q a^n} \leq x_0 \leq \frac{1 - \sum_{i=1}^n p_i a^i}{q a^n} & (q > 0 \text{ のとき}) \\ \frac{1 - \sum_{i=1}^n p_i a^i}{q a^n} \leq x_0 \leq \frac{1/2 - \sum_{i=1}^n p_i a^i}{q a^n} & (q < 0 \text{ のとき}) \end{cases} \quad (3.30)$$

(iv)' $b_n = 1$, $X_n = B'$ ($x_n \in B'$) のとき ($\Rightarrow 1/2 \leq x_n (= f_a^n(x_0)) < 1$)

$$\Rightarrow \begin{cases} \frac{1/2 - \sum_{i=1}^n p_i a^i}{q a^n} \leq x_0 < \frac{1 - \sum_{i=1}^n p_i a^i}{q a^n} & (q > 0 \text{ のとき}) \\ \frac{1 - \sum_{i=1}^n p_i a^i}{q a^n} < x_0 \leq \frac{1/2 - \sum_{i=1}^n p_i a^i}{q a^n} & (q < 0 \text{ のとき}) \end{cases} \quad (3.31)$$

3.3.4 本節のまとめ

本推測法により厳密な初期値解を得るには、最終値 x_n の厳密な存在範囲を知ることが重要である（一般に最終値 x_n の厳密な範囲を知ることは困難である）。本節では、パラメータ $a = 2$ に限定した場合について、 x_i が含まれる区間から区間への推移（写像の連鎖）を調べたところ、この様子を状態遷移図として整理することができたため、この状態遷移図を利用して、最終値 x_n の存在範囲を容易に得ることができことを示した。これよりパラメータ $a = 2$ の場合の厳密な初期値解を得ることができることを示した。

3.4 $1 < a < 2$ のテント写像の最上位ビット抽出系列に対する初期値推測法（厳密な解）[26]

パラメータ $1 < a < 2$ の場合の初期値推測は、 $a = 2$ の場合に比べて複雑になる。ここでも前節までに記した初期値推測法と同様のことを $1 < a < 2$ について考える。すなわち、3.2 節で示した必要条件から得られた解に対して十分性を与えることを検討する。これには、最終値 $x_n = f_a^n(x_0)$ の厳密な存在範囲を知る必要がある。前節と同様に区間から区間への写像の連鎖を調べることからはじめる。その詳細は追って次節以降に記すが、結論として初期値解は Type-0 ~ Type-3 の 4 つのパターンに整理される。Type-0 は、3.2 節で示した解（必要条件のみから得られた解）がそのまま利用できる場合である。Type-1 と Type-2 は、以降で定義する区間全体から（次の）区間全体へ写像されるという関係が毎写像ごとに保たれている場合である（後に述べるが、これは、系列中に 1 に続く 0 の連の長さが理論上の最大値となるような 0 の連を含まない場合である）。Type-1 と Type-2 の関係は、パラメータ $a = 2$ の場合（3.3 節）での区間 A, B と区間 A', B' の関係と同様の関係にある。Type-3 は、以降で定義する区間全体から（次の）区間全体へ写像されるという関係がある時点で保たれなくなる場合である（後に述べるが、これは、系列中に 1 に続く 0 の連の長さが理論上の最大値となるような 0 の連を含む場合である）。この場合は関係が保たれる範囲に分割して処理することを示す。

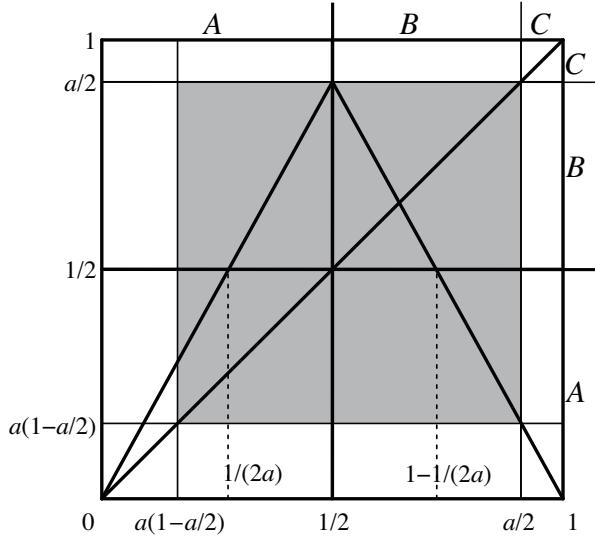
3.4.1 区間から区間への写像の連鎖の様子

以降では、パラメータ $1 < a < 2$ のテント写像 $f_a(x)$ の定義域 $I_a = [0, 1]$ を、図 3.2 に示される 3 つの区間 $A \sim C$ に分割して考える。

$$A = [0, 1/2] \quad (3.32)$$

$$B = [1/2, a/2] \quad (3.33)$$

$$C = (a/2, 1] \quad (3.34)$$

図 3.2 テント写像 ($1 < a < 2$)

ここで説明の都合上で、区間 A をさらに RA , LA に分割することにする。

$$RA = [a(1 - a/2), 1/2] \quad (3.35)$$

$$LA = [0, a(1 - a/2)] \quad (3.36)$$

パラメータ $1 < a < 2$ の場合は区間 C に初期値 x_0 が存在することは有り得るが、 $i \geq 1$ において x_i が C に存在することはないあるいは、 f_a によって、 C に写像されるような区間は存在しない。

$$\nexists x \in I_a, f_a(x) \in C \quad (3.37)$$

また、区間 B からは A の一部である RA へ写像されることはあるが、 A の残りの部分 LA へ写像されることはない。

$$\nexists x \in B, f_a(x) \in LA \quad (3.38)$$

前節と同様に区間から区間の写像（推移）様子を、まずは簡単に示せる範囲で記すと以下の式となっている。

$$LA = [0, a(1 - a/2)] \rightarrow [0, a^2(1 - a/2)] = LA \cup \underline{RA \text{ の一部}} \quad (3.39)$$

$$RA = [a(1 - a/2), 1/2] \rightarrow [a^2(1 - a/2), a/2] = \underline{RA \text{ の一部}} \cup B' \quad (3.40)$$

$$B = [1/2, a/2] \rightarrow [a(1 - a/2), a/2] = RA \cup B \quad (3.41)$$

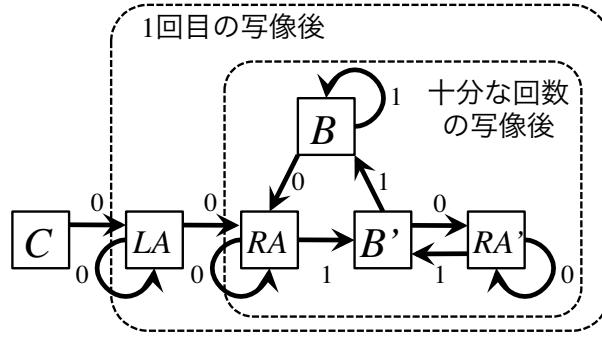
$$B' = [1/2, a/2] \rightarrow (a(1 - a/2), a/2] = RA' \cup B \quad (3.42)$$

$$RA' = (a(1 - a/2), 1/2) \rightarrow (a^2(1 - a/2), a/2] = \underline{RA' \text{ の一部}} \cup B' \quad (3.43)$$

$$C = (a/2, 1] \rightarrow [0, a(1 - a/2)] = LA \quad (3.44)$$

ただし、 $B' = [1/2, a/2]$

ただし、 $RA' = (a(1 - a/2), a/2)$

図 3.3 テント写像 ($1 < a < 2$) の連鎖 (おおざっぱな分類)

この系を複雑にしているのは、上記式 (3.39) ~ 式 (3.44) において「 RA の一部」「 RA' の一部」へと写像される場合である。この部分に至った場合は、ここから次に写像される区間を式 (3.39) ~ 式 (3.44) のみでは記述できない。つまり区間から区間の連鎖がいったん途切れてしまう。

パラメータ $1 < a < 2$ の場合は、上記のように厄介である。区間と区間の連鎖の詳細を調べていく前に、説明の都合上、はじめに次節で示す特殊なケースを分離して考えることにする。そして、次々節以降で改めて区間と区間の連鎖の詳細を考えていくことにする。

3.4.2 Type-0 の分離および初期値解

本推測法により厳密に（正確な）初期値の範囲を得るには、最終値 x_n の厳密な存在範囲を得ることである。パラメータ $1 < a < 2$ の場合は、図 3.2、図 3.3 からも明らかではあるが、特殊なケースを除き、十分多くの回数の写像後の最終値 $x_n = f_a^n(x_0)$ は $[a(1 - a/2), a/2] = RA \cap B$ である。また、区間 C に初期値 x_0 があることは有り得るが $n \geq 1$ において $x_n \notin C$ である。ここでいう特殊なケースとは、最終値 x_n が区間 $[0, a(1 - a/2)) = LA$ に存在する可能性がある場合を指している。このケースを Type-0 とよぶことにする。

以下では、計 $n + 1$ の擬似ランダムビット列 $\{b_i\}_{i=0}^n$ が得られているとして、Type-0 のケースを $\{b_i\}_{i=0}^n$ から判断することを考える。 $x_n \in LA$ は、ビット列 $b_n = 0$ が抽出される領域にあるので、最終ビット $b_n = 1$ の系列は対象外となる。また、 x_i がひとたび区間 B または B' に入った場合は、以降は区間 RA に移っても LA に移ることはない。すなわち、 b_i が $(0 \text{ or } 1) \rightarrow 1 \rightarrow 0$ のパターンを示すケースは Type-0 の要求 ($x_n \in LA$) を満たさない。この時点で、Type-0 の要求を満たすケースは、 $\{b_i\}_{i=0}^n = \{0, 0, \dots, (\text{all } 0), \dots, 0\}$ ということになる。尚、観測ビット列の先頭ビットが $b_0 = 1$ の場合は、 $x_0 \in C$ の場合であれば、 C から LA に移ったあと、ずっと LA に留まる場合が考えられる。すなわち、先頭ビットが 1 で、以降のビットが全て 0 のケース $\{1, 0, 0, \dots, (\text{all } 0), \dots, 0\}$ も Type-0 の条件を満たす。

つまり、先頭ビット以外のビットが全て 0 となる上記 2 つの系列が Type-0 である。尚、Type-0 の場合の解は、 $x_n \in [a(1 - a/2), 1/2)$ となる場合もあるので、 $0 \leq x_n = f_a^n(x_0) < 1/2$ として、多項式 $x_n = f_a^n(x_0)$ を x_0 について解いたものが解であり、3.2 節で示した式 (3.20) または式 (3.21) がそのまま Type-0 における厳密な解（十分性）を与えている。

逆にいうと、 $\{b_i\}_{i=0}^n$ が、ここで示した 2つのビットパターン以外の場合は、式 (3.20) または式 (3.21) が解ではないことを意味している。

3.4.3 区間 A 内、区間 B 内での遷移

本節以降では本題に戻り、前節で述べた Type-0 を除いた場合について区間と区間の連鎖について示す。

$x_i \in A$ の場合は、 $x_i \mapsto x_{i+1}$ において、観測ビットのパターンで $0 \rightarrow 1, 0 \rightarrow 0$ を生じ得る。観測ビットが $0 \rightarrow 1$ となる場合の区間から区間の遷移(写像)は。 $[1/(2a), 1/2] \stackrel{\text{def}}{=} A_1 \rightarrow [1/2, a/2] = B'$ で生じている。 $A_1 \rightarrow B'$ の詳細は次節で述べるとして、ここでは観測ビットが $0 \rightarrow 0$ となる区間を考える。まず、 A 内から A_1 へ移る区間 A_2 を考えると、 $A_2 \stackrel{\text{def}}{=} [1/(2a^2), 1/(2a)] \rightarrow A_1 = [1/(2a), 1/2]$ である。同様にして $A_{j+1} \rightarrow A_j$ ($j \geq 1$) を考えると、

$$A_j = \left[\frac{1}{2a^j}, \frac{1}{2a^{j-1}} \right) \quad (3.45)$$

となっている。尚、 $A_{j+1} \rightarrow A_j$ ($j \geq 1$)、および $A_1 \rightarrow B'$ は全単射 (bijection) であることに留意されたい。区間 A_m に関して、十分大きな m ($m \rightarrow \infty$) に対しては以下が成立する。

$$A_1 \cup A_2 \cup A_3 \cup \dots = \lim_{m \rightarrow \infty} \bigcup_{i=1}^m A_i = A \quad (3.46)$$

$x_i \in B$ の場合は、 $x_i \mapsto x_{i+1}$ において、観測ビットのパターンで $1 \rightarrow 0, 1 \rightarrow 1$ を生じ得る。観測ビットが $1 \rightarrow 0$ となる場合の区間から区間の遷移(写像)は。 $(1 - 1/(2a), a/2] \stackrel{\text{def}}{=} B_1 \rightarrow [a(1 - a/2), 1/2] = RA$ で生じている。 $B \rightarrow RA$ の詳細は次々節で述べるとして、ここでは観測ビットが $1 \rightarrow 1$ となる $B_{j+1} \rightarrow B_j$ ($j \geq 1$) を考えると、

$$B_j = (g(j), g(j-2)] \quad (j = 1, 3, 5, \dots \text{奇数}) \quad (3.47)$$

$$B_j = [g(j-2), g(j)) \quad (j = 2, 4, 6, \dots \text{偶数}) \quad (3.48)$$

$$g(t) = \sum_{0 \leq s \leq t} \frac{(-1)^s}{a^s} - \frac{(-1)^t}{2a^t} \quad (t \geq -1) \quad (3.49)$$

となることが帰納法を用いて容易に導かれる。このとき、十分大きな m ($m \rightarrow \infty$) に対して以下が成立する。

$$B_1 \cup B_2 \cup B_3 \cup \dots = \lim_{m \rightarrow \infty} \bigcup_{i=1}^m B_i = B \quad (3.50)$$

ここまでをまとめると以下である。

$$(観測ビット) 0 \rightarrow 0 \Rightarrow A_j \rightarrow A_{j-1} \quad (j \geq 2) \quad (3.51)$$

$$1 \rightarrow 1 \Rightarrow B_j \rightarrow B_{j-1} \quad (j \geq 2) \quad (3.52)$$

$$0 \rightarrow 1 \Rightarrow A_1 \rightarrow B' \quad (3.53)$$

$$1 \rightarrow 0 \Rightarrow B_1 \rightarrow RA \quad (3.54)$$

ここまで理解できることは、観測ビットが同一の値を連続する場合は($0 \rightarrow 0$ または $1 \rightarrow 1$)、それは $A_{j+1} \rightarrow A_j$ ($j \geq 1$) または $B_{j+1} \rightarrow B_j$ ($j \geq 1$) で生じていて(式(3.51), 式(3.52)), $A_{j+1} \rightarrow A_j$ および $B_{j+1} \rightarrow B_j$ は全単射ということである。および、観測ビットが異なるビットに移る場合は($0 \rightarrow 1$ または $1 \rightarrow 0$), $A_1 \rightarrow B'$ または $B \rightarrow RA$ で生じていて(式(3.53), 式(3.54)), $A_1 \rightarrow B'$ または $B \rightarrow RA$ は全単射ということである。

しかし、 B' に移った以降、式(3.52) および式(3.54) とどのように接続の関係があるか (B' と $B_{j+1} \rightarrow B_j$ ($j \geq 1$) の関係はどうであるか) 或は、 RA に移った以降、式(3.51) および式(3.53) とどのように接続の関係があるか (RA と $A_{j+1} \rightarrow A_j$ ($j \geq 1$) の関係はどうであるか) までは判らない。この詳細を次の 3.4.4 節, 3.4.5 節で述べる。

3.4.4 区間 A_1 から 区間 B' への遷移

本節では、 $A_1 \rightarrow B'$ と写像された以降について触れる。 B' は B に対して境界値 $a/2$ を含まない。境界値 $a/2$ は $B_1 = (1 - 1/(2a), a/2]$ に属するので、ここで新たに B_1 対して境界値 $a/2$ を含まない $(1 - 1/(2a), a/2) \stackrel{\text{def}}{=} B'_1$ を考える。この場合は、式(3.50) に対応する関係は以下の式(3.55) である。

$$B'_1 \cup B_2 \cup B_3 \cup \dots = \lim_{m \rightarrow \infty} \bigcup_{i=1}^m B_i = B' \quad (3.55)$$

$0 \rightarrow 1$ に移った以降に、長さ 2 以上の 1 の連を観測したならば、それは、 $A_1 \rightarrow B'$ の際に、 B_2 以後 (B_m ($m \geq 2$)) に移ったことになる(ダッシュがつかない)。例えば、 $0 \rightarrow 1 \rightarrow 1 \rightarrow 1 \rightarrow 0$ であれば、 $0 \rightarrow 1$ のとき B_3 に移っている。 $0 \rightarrow 1 \rightarrow 1 \rightarrow 1 \rightarrow 1$ であれば、 $0 \rightarrow 1$ のとき B_m ($m \geq 4$) に移っている。この場合(長さ 2 以上の 1 の連を観測)は、以降の写像は式(3.52) より最終的に B_1 を経由して RA に移るため、 B'_1 の影響を受けない(関係ない)。

一方で、 $0 \rightarrow 1 \rightarrow 0$ の場合(1 の連の長さが 1)は、それは、 $A_1 \rightarrow B'$ の際に B'_1 に移っていることが決定する。この場合は、次の写像先は、 RA に対して境界値 $a(1 - a/2)$ を含まない区間 $(a(1 - a/2), 1/2) \stackrel{\text{def}}{=} RA'$ に移る。

例 3.4.1 観測ビットのパターンが $\dots \rightarrow 0 \rightarrow 1 \rightarrow 1 \rightarrow 1 \rightarrow 0$ (ビット列終端)の場合は、 x_i が含まれる区間は $\dots A_1 \rightarrow B_3 \rightarrow B_2 \rightarrow B_1 \rightarrow RA$ と遷移したことが判明する。 $\dots \rightarrow 0 \rightarrow 1 \rightarrow 0$ (ビット列終端)の場合は、 $\dots A_1 \rightarrow B'_1 \rightarrow RA'$ と遷移したことが判明する。つまり、0 と 0 に挟まれた 1 の連の長さ m が $m \geq 2$ であれば、最終値 $x_n \in RA$ で、 $m = 1$ であれば、最終値 $x_n \in RA'$ である。

例 3.4.2 $\dots \rightarrow 0 \rightarrow 1 \rightarrow 1 \rightarrow 1$ (ビット列終端)の場合は、 $\dots A_1 \rightarrow B_3 \rightarrow B_2 \rightarrow B_1$ の場合もあれば、 $\dots A_1 \rightarrow B_{50} \rightarrow B_{49} \rightarrow B_{48}$ の場合もあり得る。従ってこの場合は $x_n \in B$ である。 $\dots \rightarrow 0 \rightarrow 1$ の場合は $x_n \in B'$ となる。

本節で明らかになったことは、観測ビット列が $0 \rightarrow 1$ となった以降、次に $1 \rightarrow 0$ となるまでの間に、区間 A_1 から B 内のどの区間に接続(写像)されたかを、 $0 \rightarrow 1$ に続く 1 の連の長さから特定できることを述べた。ここで新たに区間 RA' が生じた。次節では、 RA および RA' と写像された以降について触れる。

3.4.5 区間 B_1, B'_1 から 区間 RA, RA' への遷移

本節では、 $B_1 \rightarrow RA$ または、 $B'_1 \rightarrow RA'$ と写像された以降について触れる。 RA, RA' は一般的には A_j ($j \geq 1$) の単純な和集合として表現できない。また、1と1に挟まれた0の連の長さ^{*5} には理論上の最大値が存在し、これを m とすると、長さ m の理論上最大の0の連^{*6} を生じ得る区間は式(3.45)で表される区間 $A_m = [1/(2a^m), 1/(2a^{m-1}))$ よりも狭く以下である^{*7}。

$$\left[a\left(1 - \frac{a}{2}\right), \frac{1}{2a^{m-1}} \right) \stackrel{\text{def}}{=} A_m^* \quad (3.56)$$

$$\left(a\left(1 - \frac{a}{2}\right), \frac{1}{2a^{m-1}} \right) \stackrel{\text{def}}{=} A'^*_m \quad (3.57)$$

尚、 m の値（最大の0の連の長さ^{*6}）は以下の通りである。

$$\begin{aligned} \inf A_m &\leq \inf RA (= \inf A_m^*) < \sup A_m \\ \Leftrightarrow \frac{1}{2a^m} &\leq a\left(1 - \frac{a}{2}\right) < \frac{1}{2a^{m-1}} \\ \Leftrightarrow m &< \log_a\left(\frac{1}{2-a}\right) \leq m+1 \\ \therefore m &= \lceil \log_a\left(\frac{1}{2-a}\right) \rceil - 1 \end{aligned} \quad (3.58)$$

これより RA, RA' は以下のよう表される。

$$RA = A_1 \cup \cdots \cup A_{m-1} \cup A_m^* = \left(\bigcup_{i=1}^{m-1} A_i \right) \cup A_m^* \quad (3.59)$$

$$RA' = A_1 \cup \cdots \cup A_{m-1} \cup A'^*_m = \left(\bigcup_{i=1}^{m-1} A_i \right) \cup A'^*_m \quad (3.60)$$

$1 \rightarrow 0$ に移った以降に観測された0の連の長さ k が m 未満 (m は理論上で最大となる0の連の長さ式(3.58)) であれば、それは、 $B_1 \rightarrow RA$ または $B'_1 \rightarrow RA'$ の際に、 A_m 以外の A_k ($1 \leq k < m$) に移ったことになる。例えば、 $m = 5$ としたとき、 $1 \rightarrow 0 \rightarrow 0 \rightarrow 0 \rightarrow 1$ であれば、 $1 \rightarrow 0$ のときに A_3 に移っている。 $1 \rightarrow 0 \rightarrow 0 \rightarrow 0 \rightarrow 0$ であれば、 $1 \rightarrow 0$ のときに A_4 または、 A_5^* or A'^*_5 に移っている。

$B_1 \rightarrow RA, B'_1 \rightarrow RA'$ の際に、仮に $A_1 \sim A_{m-1}$ に移った場合は、式(3.51)より、いずれは A_1 を経由して B' に移るので、 A_m^*, A'^*_m とは関係なく推移を考えることができる（影響を受けない）。一方で、 $B_1 \rightarrow RA, B'_1 \rightarrow RA'$ の際に A_m^*, A'^*_m に移った場合は、以降の写像において以下のように遷

^{*5} RA に含まれる x_i が、写像後の x_{i+1} も RA に留まることのできる回数に等しい。

^{*6} 本稿では、以降、「理論上最大の0の連」または「0の連の最大値」という表現がされた場合は、1と1に挟まれた0の連、およびその最大値のことを意味する。

^{*7} 長さ m の0の連を生じ得る範囲は $A_m = [1/(2a^m), 1/(2a^{m-1}))$ であるが、Type-0以外は、 $a(1 - a/2)$ より小さい値を取ることがないので、 $A_{m \inf}^* = RA_{m \inf} = a(1 - a/2)$ とした。

移する (A_1 の全範囲に写像されることはない).

$$A_j^* \rightarrow A_{j-1}^* \quad (2 \leq j \leq m) \quad (3.61)$$

$$A_j'^* \rightarrow A_{j-1}'^* \quad (2 \leq j \leq m) \quad (3.62)$$

$$A_j^* = \left[a^{m-j+1} \left(1 - \frac{a}{2}\right), \frac{1}{2a^{j-1}} \right) \quad (3.63)$$

$$A_j'^* = \left(a^{m-j+1} \left(1 - \frac{a}{2}\right), \frac{1}{2a^{j-1}} \right) \quad (3.64)$$

パラメータ $1 < a < 2$ の場合が複雑になる点は上記である。そして、理論上最大となる 0 の連を観測した場合は、基本的に、その時点以降の x_i が含まれる区間を詳細に追跡する必要が生じる。これはとても面倒なことである。本推測法では、Type-0 を除いて理論上最大となる 0 の連を観測した場合（直前に記した内容）は、0 の連の終了位置で系列を分割して処理するとして合理的に対処した（この詳細は 3.4.9 節）。

尚、観測ビット列 $\{b_i\}$ が 0 の連の長さ k ($\leq m$) を観測して終了した場合は、最終値 x_n は $x_n \in A_1 \cup \dots \cup A_{m-k} \cup A_{m-k+1}^*$ である（例 3.4.5）。これを簡単に記すために以下を定義して、 $x_n \in RA_{m-k+1}$ と表すこととする。 $z = m - k + 1$ とすると以下のように表せる。

$$RA_z = A_1 \cup \dots \cup A_{z-1} \cup A_z^* = \left(\bigcup_{j=1}^{z-1} A_j \right) \cup A_z^* \quad (3.65)$$

$$RA'_z = A_1 \cup \dots \cup A_{z-1} \cup A_z'^* = \left(\bigcup_{j=1}^{z-1} A_j \right) \cup A_z'^* \quad (3.66)$$

$(RA \equiv RA_m, RA' \equiv RA'_m \text{ である})$

例 3.4.3 観測ビットが $\dots \rightarrow 1 \rightarrow 1 \rightarrow 0 \rightarrow 0 \rightarrow 0 \rightarrow 1 \rightarrow \dots$ の場合（0 の連の長さ $k = 3$ ）で、 $k < m$ ならば（ m は理論上で最大となる 0 の連の長さ）、 x_i が含まれる区間は $\dots B_2 \rightarrow B_1 \rightarrow A_3 \rightarrow A_2 \rightarrow A_1 \rightarrow B' \rightarrow \dots$ と遷移したと判る。尚、 $k = m (= 3)$ であれば、 $\dots B_2 \rightarrow B_1 \rightarrow A_3^* \rightarrow A_2^* \rightarrow A_1^* \rightarrow B'$ の一部 $\rightarrow \dots$ である。

例 3.4.4 観測ビットが $\dots \rightarrow 1 \rightarrow 1 \rightarrow 0 \rightarrow 0 \rightarrow 0$ （ビット列終端）の場合（0 の連の長さ $k = 3$ ）で、 $m = 6$ ならば（ m は理論上で最大となる 0 の連の長さ）、 x_i が含まれる区間の遷移として以下が考えられる。ただし系列中に理論上最大となる 0 の連を含まないとする。

$$\dots B_2 \rightarrow B_1 \rightarrow A_3 \rightarrow A_2 \rightarrow A_1$$

$$\dots B_2 \rightarrow B_1 \rightarrow A_4 \rightarrow A_3 \rightarrow A_2$$

$$\dots B_2 \rightarrow B_1 \rightarrow A_5 \rightarrow A_4 \rightarrow A_3$$

$$\dots B_2 \rightarrow B_1 \rightarrow A_6^* \rightarrow A_5^* \rightarrow A_4^*$$

従って、 $x_n \in A_1 \cup A_2 \cup A_3 \cup A_4^* = RA_4$ である。尚、式 (3.65) より、最後の 0 の連の長さが $k = 3$ なので、 $RA_{m-k+1} = RA_4$ と考えても良い。

例 3.4.5 観測ビットが $\dots \rightarrow 0 \rightarrow 1 \rightarrow 0 \rightarrow 0 \rightarrow 0$ （ビット列終端）の場合（0 の連の長さ $k = 3$ ）で、 $m = 6$ ならば（ m は理論上で最大となる 0 の連の長さ）、 x_i が含まれる区間の遷移として以下が

考えられる。ただし系列中に理論上最大となる0の連を含まないとする。

$$\begin{aligned} & \cdots A_1 \rightarrow B'_1 \rightarrow A_3 \rightarrow A_2 \rightarrow A_1 \\ & \cdots A_1 \rightarrow B'_1 \rightarrow A_4 \rightarrow A_3 \rightarrow A_2 \\ & \cdots A_1 \rightarrow B'_1 \rightarrow A_5 \rightarrow A_4 \rightarrow A_3 \\ & \cdots A_1 \rightarrow B'_1 \rightarrow A'_6 \rightarrow A'_5 \rightarrow A'_4 \end{aligned}$$

従って $x_n \in A_1 \cup A_2 \cup A_3 \cup A'_4 = RA'_4$ である。尚、式(3.66)より、最後の0の連の長さが $k = 3$ なので、 $RA'_{m-k+1} = RA'_4$ と考えても良い。(”ダッシュ”が付くか否かは直前の1の連の長さ k が $k = 1$ or $k \geq 2$ によって分かれる)。

本節で明らかになったことは、観測ビット列が $1 \rightarrow 0$ となった以降、次に $0 \rightarrow 1$ となるまでの間に、区間 B_1 または B'_1 から A 内のどの区間に接続(写像)されたかを、 $1 \rightarrow 0$ に続く0の連の長さから特定できることを述べた。尚、観測ビット列中に理論上で最大となる0の連を含まない場合は、 x_i が含まれる区間の連鎖を、ここまでに定義した区間から区間への写像の連鎖として表すことができる。しかし、観測ビット列中に理論上で最大のとなる0の連を含む場合は(理論上最大となる0の連の長さを m とする)、新たに、 A_m^* , A'_m という区間が生じ、これ以降は、ここまでに定義した区間から区間への写像の連鎖のみでは表すことができなくなる。このケースが生じる度に、都度、新たな区間を定義していく必要が生じるが、以降に示す推測法においては、観測ビット列中に理論上で最大のとなる0の連を含む場合は、系列を前後に分割して処理する方針とする。

3.4.6 状態遷移図を用いた最終値 $x_n = f_a^n(x_0)$ の厳密な存在範囲の取得

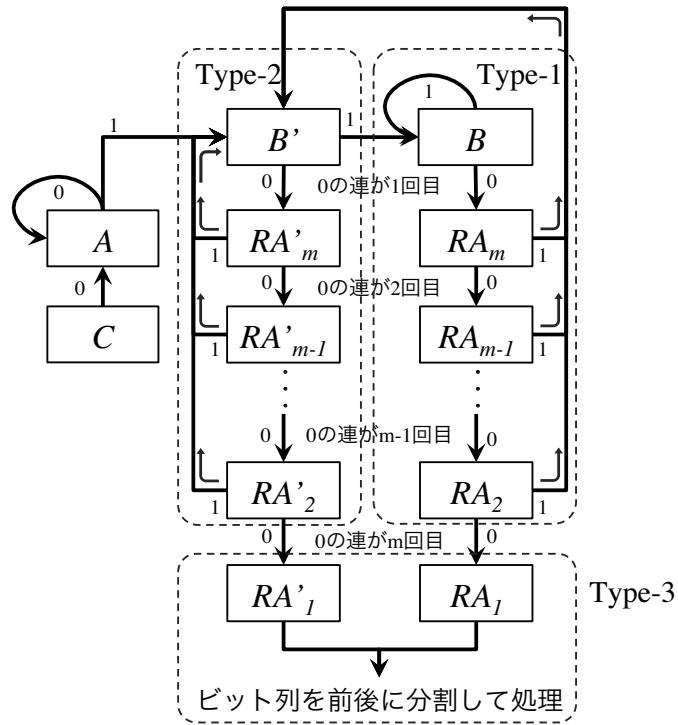
本推測法によって厳密な初期値解を得るには、最終値 $x_n = f_a^n(x_0)$ の厳密な存在範囲を得ることである。本節では、まず、3.4.3節、3.4.4節、3.4.5節で示した内容をまとめた状態遷移図(図3.4)を示し、この状態遷移図を利用して $x_n = f_a^n(x_0)$ の厳密な範囲を求めて、その後、以下に示すType-1 ~ Type-3の3つの分類に分けて初期値解を求める事を示す。尚、Type-0の場合は既に3.4.2節で述べたので、ここでは省く。

状態遷移図3.4の動作は以下の通りである。まず、初期値 x_0 の属する場所は図中の A, B, C で、 $b_0 = 0$ ならば $A, b_0 = 1$ ならば B または C とする^{*8}。以降、次のビットが0または1によって、それぞれ図で示された方向に進める。これを観測ビット列の長さ分だけ繰り返す。

観測ビット列中に理論上最大の0の連(その長さを m とする)を含まないならば、 x_n は状態遷移図中のType-1またはType-2のいずれかにある。例えば、 $x_n \in RA'_3$ であれば、 $RA'_3 \inf < x_n < RA'_3 \sup$ として方程式 $f_a^n(x_0) = x_n$ を x_0 について解いた範囲が x_0 の厳密な解である。Type-1の場合の解は3.4.7節、Type-2の場合の解は3.4.8節に記す。

観測ビット列中に理論上最大の0の連(その長さ m)を含む場合は状態遷移図中のType-3に行き当たる。この場合は、理論上最大の0の連が観測された位置で系列を前後に区切り(理論上最大の0の連が観測された最後のビットを重複して区切る)、それぞれの系列毎に処理する。詳細は3.4.9節に記す。

^{*8} $b_0 = 1$ のときに B または C であるが、 $b_0 \rightarrow b_1$ が $1 \rightarrow 1$ の場合は必ず $x_0 \in B$ であるため、この場合は $x_0 \in B$ とする。これ以外では、 $1 \rightarrow 0$ または $0 \rightarrow 1$ となった時点での状態は同じ場所をさすようになるので問題はない。尚、 $1 \rightarrow$ 全て 0 の場合は Type-0 として分離しているので問題はない。

図 3.4 テント写像 ($1 < a < 2$) における x_i が含まれる区間の状態遷移図

3.4.7 Type-1 の初期値解

Type-1 は、Type-0 (3.4.2 節で示した) を除き、観測ビット列中に $1 \rightarrow 0$ に続く最大の 0 の連を含まない場合で^{*7}、 x_n が状態遷移図 3.4 の $RA_1 \sim RA_{m-1}$ または B に存在する場合である。最後に観測された 0 の連の長さを $j (< m)$ とすると、 $b_n = 0 \Rightarrow x_n \in RA_{m-j+1} = [a^j(1 - \frac{a}{2}), \frac{1}{2}]$ 、 $b_n = 1 \Rightarrow x_n \in B = [\frac{1}{2}, \frac{a}{2}]$ である。これより、上記区間を境界として方程式 $f_a^n(x_0) = x_n$ を x_0 について解くと以下の解を得る (式 (3.67) ~ (3.70))。

(i)" $b_n = 0, q > 0$ のとき

$$\frac{a^j(1 - a/2) - \sum_{i=1}^n p_i a^i}{q a^n} \leq x_0 < \frac{1/2 - \sum_{i=1}^n p_i a^i}{q a^n} \quad (3.67)$$

(ii)" $b_n = 0, q < 0$ のとき

$$\frac{1/2 - \sum_{i=1}^n p_i a^i}{q a^n} < x_0 \leq \frac{a^j(1 - a/2) - \sum_{i=1}^n p_i a^i}{q a^n} \quad (3.68)$$

(iii)" $b_n = 1, q > 0$ のとき

$$\frac{1/2 - \sum_{i=1}^n p_i a^i}{q a^n} \leq x_0 \leq \frac{a/2 - \sum_{i=1}^n p_i a^i}{q a^n} \quad (3.69)$$

(iv)'' $b_n = 1, q < 0$ のとき

$$\frac{a/2 - \sum_{i=1}^n p_i a^i}{q a^n} \leq x_0 \leq \frac{1/2 - \sum_{i=1}^n p_i a^i}{q a^n} \quad (3.70)$$

3.4.8 Type-2 の初期値解

Type-2 は、前節と同じく Type-0(3.4.2 節で示した)を除き、観測ビット列中に $1 \rightarrow 0$ に続く最大の 0 の連を含まない場合で^{*7}、 x_n が状態遷移図 3.4 の $RA'_1 \sim RA'_{m-1}$ または B' に存在する場合である。最後に観測された 0 の連の長さを $j(< m)$ とすると、 $b_n = 0 \Rightarrow x_n \in RA'_{m-j+1} = (a^j(1 - \frac{a}{2}), \frac{1}{2})$ 、 $b_n = 1 \Rightarrow x_n \in B' = [\frac{1}{2}, \frac{a}{2})$ である。これより、上記区間を境界として方程式 $f_a^n(x_0) = x_n$ を x_0 について解くと以下の解を得る(式 (3.71) ~ (3.74))。

(i)''' $b_n = 0, q > 0$ のとき

$$\frac{a^j(1 - a/2) - \sum_{i=1}^n p_i a^i}{q a^n} < x_0 < \frac{1/2 - \sum_{i=1}^n p_i a^i}{q a^n} \quad (3.71)$$

(ii)''' $b_n = 0, q < 0$ のとき

$$\frac{1/2 - \sum_{i=1}^n p_i a^i}{q a^n} < x_0 < \frac{a^j(1 - a/2) - \sum_{i=1}^n p_i a^i}{q a^n} \quad (3.72)$$

(iii)''' $b_n = 1, q > 0$ のとき

$$\frac{1/2 - \sum_{i=1}^n p_i a^i}{q a^n} \leq x_0 < \frac{a/2 - \sum_{i=1}^n p_i a^i}{q a^n} \quad (3.73)$$

(iv)''' $b_n = 1, q < 0$ のとき

$$\frac{a/2 - \sum_{i=1}^n p_i a^i}{q a^n} < x_0 \leq \frac{1/2 - \sum_{i=1}^n p_i a^i}{q a^n} \quad (3.74)$$

3.4.9 Type-3 の初期値解

Type-3 は、Type-0 を除いて観測ビット列中に理論上の最大の 0 の連を含む場合である。この場合は、基本的に最大の 0 の連を観測した以降の x_i の範囲を写像する度に追跡する必要がある。これは面倒であるが、最大の 0 の連を観測した位置で系列を前後に分割し(最大の 0 の連が観測された最後のビットを重複して分割)，分割した系列毎に本推測法を適用することによって達成される。

例えば、観測ビット列 $\{b_i\}_{i=0}^n$ において、長さ m の最大の 0 の連が検出された位置が t ビット目 ($m < t < n$) だったとする(ここでは t ビット目以降に長さ m の最大の 0 の連を含まないとする)。この場合は、 t ビット目を重複して、系列を前後に分割し、 $\mathbf{b}_1 = \{b_i\}_{i=0}^t$ 、 $\mathbf{b}_2 = \{b_i\}_{i=t}^n$ とする。はじめに、後の系列 \mathbf{b}_2 に対して Type-1 または Type-2 を適用し、 x_t の存在範囲 $x_t \in X_{t2}$ を求める。また、前の系列 \mathbf{b}_1 に対して状態遷移図を適用することによって求まった x_t の存在範囲を $x_t \in X_{t1}$ とする。実際に x_t が存在する範囲は、 $X_{t1} \cap X_{t2} \stackrel{\text{def}}{=} Y_t$ であることから、前の系列 \mathbf{b}_1 に対して、 $x_0 \in Y_t$ ($Y_{t \inf} < x_t (= f_a^n(x_0)) < Y_{t \sup}$) として、この不等式を x_0 について整理したものが解である。尚、系列中に 0 の最大の連が複数箇所存在する場合も同様の処理を繰り返すことによって達成される。

例 3.4.6 初期値 $x_0 = 0.208984375 (= 214/1024)$, パラメータ $a = 1.96484375 (= 503/256)$, 写像の反復回数 $n = 10$ とする。定義 3.2.1 で示される生成法によって生成された計 $n + 1 = 11$ ビットの擬似ランダムビット列 $S_a(x_0, n) = \{b_i\}_{i=0}^n = \{0, 0, 1, 0, 1, 0, 1, 0, 0, 0\}$ が与えられたとき, パラメータ a を既知として, 本節 3.4 節で示した推測法（厳密な初期値範囲を得る）により当該系列を生成し得る初期値範囲を推測する。

はじめに, 本系列中に理論上最大の 0 の連(長さ m とする)を含むか否かを調べる。式 (3.58) より, $m = \lceil \log_a(\frac{1}{2-a}) \rceil - 1 = 4$ なので, 当該系列は 0 の最大の連を含まない。状態遷移図より $x_n \in RA'_2$ が判明し, この場合は Type-2 であることが判明する。定理 3.2.3 より導かれる式 (3.7) ~ 式 (3.10) より, $\{r_i\}_{i=1}^n = \{1, 1, -1, -1, 1, 1, -1, -1, -1\}$, $\{p_i\}_{i=1}^n = \{0, 0, 1, 0, -1, 0, 1, 0, 0\}$, $q = -1$ が計算される。最後の 0 の連の長さは 3 なので $j = 3$ として式 (3.72) (Type-2) を解くと, $0.20816542831117904 < x_0 < 0.2090054930463704$ を得る。

例 3.4.7 初期値 $x_0 = 0.12890625 (= 132/1024)$, パラメータ $a = 1.96484375 (= 503/256)$, 写像の反復回数 $n = 9$ とする。定義 3.2.1 で示される生成法によって生成された計 $n + 1 = 10$ ビットの擬似ランダムビット列 $S_a(x_0, n) = \{b_i\}_{i=0}^n = \{0, 0, 0, 1, 0, 0, 0, 0, 1, 1\}$ が与えられたとき, パラメータ a を既知として, 本節 3.4 節で示した推測法（厳密な初期値範囲を得る）により, 当該系列を生成し得る初期値範囲を推測する。

はじめに, 本系列中に理論上最大の 0 の連(長さ m とする)を含むか否かを調べる。式 (3.58) より, $m = \lceil \log_a(\frac{1}{2-a}) \rceil - 1 = 4$ なので, 当該系列は 0 の最大の連を含む。従って, 0 の連の最大値が観測された位置 $i = 7 (= t$ とする) を重複して系列を 2 つに分割し, $b_1 = \{0, 0, 0, 1, 0, 0, 0, 0, 0\}$, $b_2 = \{0, 1, 1\}$ とする。はじめに b_2 を x_t (t は最大の 0 の連が観測された位置) について解くと, 状態遷移図より $x_n \in RA_3$ であることが判明する。定理 3.2.3 より $q = -1$ が計算され, 最後の 0 の連の長さ $j = 2$ として式 (3.68) (Type-1) を解くと, $x_t \in (0.2544731610337972, 0.37943314269452866] \stackrel{\text{def}}{=} X_{t2}$ を得る。次に b_1 の最終値の存在範囲を状態遷移図で追うと, $x_t \in RA'_1 = (a^4(1 - a/2), 1/2) = (0.2619899472524594, 0.5) \stackrel{\text{def}}{=} X_{t1}$ が判明する。 x_t の存在範囲の条件は $X_{t1} \cap X_{t2}$ であるため,

$$\begin{aligned} X_{t2} &= (0.2544731610337972, 0.37943314269452866] \\ X_{t1} &= (0.2619899472524594, 0.5) \\ X_{t1} \cap X_{t2} &= (0.2619899472524594, 0.37943314269452866] \end{aligned}$$

である。次に, b_1 に対して, $x_t = f_a^t(x_0) \in X_{t1} \cap X_{t2}$ としてこの不等式を x_0 について解くと, $0.12847437989922403 \leq x_0 < 0.12951317937306578$ を得る。

3.4.10 本節のまとめ

本推測法により厳密な初期値解を得るには, 最終値 x_n の厳密な存在範囲を知ることが重要である(一般に最終値 x_n の厳密な範囲を知ることは困難である)。本節では, パラメータ $1 < a < 2$ の場合について, $a = 2$ と同様に x_i が含まれる区間から区間への推移(写像の連鎖)を調べ, 特に, 観測ビット列中に 1 に続く 0 の連の理論上の最大値が含まれない場合においては, x_i が含まれる区間から区間への推移を状態遷移図として整理できることを示した。これより, 厳密な初期値範囲

が数理的に整理された形で得ることができることを示した。一方で、観測ビット中に1に続く0の連の理論上の最大値が含まれる場合であっても、系列を前後に分割し、分割した系列単位で絞り込んでいくことによって、厳密な初期値範囲を得ることができることを示した。

3.5 テント写像の任意のビット桁(上位 t 桁目のビット / 下位側のビット)を抽出した系列に対する初期値推測法 [24],[25]

3.5.1 $a = 2$ のテント写像の任意のビット桁抽出系列に対する初期値推測法 [24]

定義 3.5.1 (擬似ランダムビット列の生成(上位 t ビット桁目の抽出)) $x_0 \in I_a$, ($I_a = [0, 1]$) を初期値として, パラメータ a ($1 < a \leq 2$) のテント写像(式(3.75))の n 回反復過程 $x_{i+1} = f_a(x_i)$ ($0 \leq i < n$) で得られる計 $n+1$ 個の値 $\{x_0, x_1, \dots, x_n\}$ ($= \{x_i\}_{i=0}^n$) を考える。ここで扱う擬似ランダムビット列^{*9}とは, 第 i 回目 ($i \geq 0$) の写像ごとに, 式(3.76)に従い x_i の上位 t ビット桁目を抽出して得られた計 $n+1$ ビットの擬似ランダムビット列 $\{c_0, c_1, \dots, c_n\}$ ($= \{c_i\}_{i=0}^n$) のことをいう。尚, 当該擬似ランダムビット列の生成関数を $S_{a,t}(x_0, n)$ と表す。

$$f_a : I_a \mapsto I_a, (I_a \in [0, 1])$$

$$f_a(x) = \begin{cases} ax & (x < 1/2) \\ a(1-x) & (x \geq 1/2) \end{cases} \quad (3.75)$$

$$c_i = \lfloor 2^t x_i \rfloor \mod 2 \quad (3.76)$$

$$S_{a,t}(x_0, n) \equiv \{c_0, c_1, \dots, c_n\} (= \{c_i\}_{i=0}^n)$$

定義 3.5.2 (定義 3.5.1 の生成法から生成された擬似ランダムビット列に対する初期値推測法) 本節で述べる初期値推測法とは, 定義 3.5.1 で示される生成法 $S_{a,t}(x_0, n)$ により生成された計 $n+1$ ビットの擬似ランダムビット列 $\{c_i\}_{i=0}^n$ が与えられたときに, パラメータ a ($1 < a \leq 2$) を既知として, 当該系列 $\{c_i\}_{i=0}^n$ を生成し得る初期値 x_0 の範囲を推測することを言う。

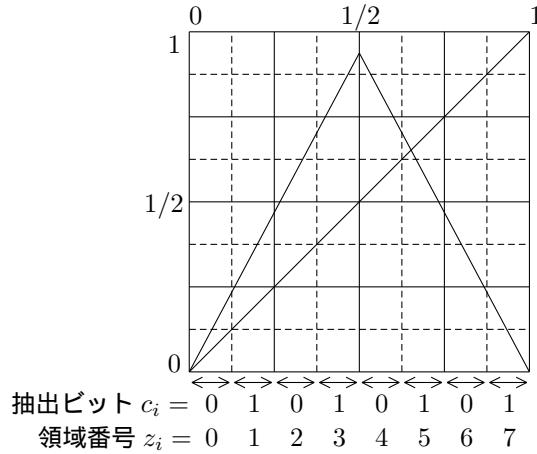


図 3.5 ($t = 3$) 上位 3 ビット桁目抽出の場合

任意桁目のビットを抽出する(上位 t ビット桁目を抽出)の場合では, 式(3.76)よりビット抽出領

*9 テント写像からの第 t ビット桁抽出系列, あるいは下位側ビット桁抽出系列と称する場合もある。

域は複数個所(計 2^t 箇所)存在する。尚、ここでは便宜のため、0,1のビット抽出領域を、以下の定義にてラベリングすることにする(図3.5)。

定義3.5.3 定義3.5.1で示される生成法 $S_{a,t}$ によって、テント写像の n 回の反復で得られる $n+1$ 個の状態 $\{x_0, x_1, \dots, x_n\}$ からそれぞれ上位 t ビット桁目を抽出して得られた系列 $\{c_0, c_1, \dots, c_n\}$ を考えたとき、 c_i の抽出元である x_i の含まれる領域の番号を z_i と呼ぶこととする。このとき、 $z_i = \omega$ であるとは以下を意味する。

$$z_i = \omega \Leftrightarrow x_i \in (\omega/2^t, (\omega+1)/2^t) \quad (3.77)$$

$$(\omega \in \mathbb{Z}; 0 \leq \omega < 2^t)$$

これより、式(3.77)の ω が偶数のときに $c_i = 0$ 、奇数のときに $c_i = 1$ と決定されることが判る。

$$c_i = \begin{cases} 0 & \Rightarrow z_i = 2\lambda \text{ すなわち } x_i \in \left(\frac{2\lambda}{2^t}, \frac{2\lambda+1}{2^t}\right) \\ 1 & \Rightarrow z_i = 2\lambda + 1 \text{ すなわち } x_i \in \left(\frac{2\lambda+1}{2^t}, \frac{2\lambda+2}{2^t}\right) \end{cases} \quad (3.78)$$

$$(\lambda \in \mathbb{Z}; 0 \leq \lambda < 2^{t-1})$$

このことは一方で、初期値 x_0 から抽出された c_0 が0または1として与えられたならば、以下の式(3.79)を満たす全ての整数値 λ ($\lambda \in \mathbb{Z}; 0 \leq \lambda < 2^{t-1}$)が c_0 の抽出元である x_0 が存在する領域 z_0 の候補であることを意味する。

$$z_0 \text{の候補} = 2\lambda + c_0 \quad (3.79)$$

次に知りたいのは、それぞれの z_0 の候補(初期値 x_0 が含まれる領域)を出発した z_i 軌道が、テント写像式(3.75)によってどのように決定されるか(z_i の遷移)である。そして、写像のパラメータ $a=2$ に限っては、 z_i の遷移ルールと観測ビット c_i の関係について以下の定理が導かれる。

定理3.5.4 パラメータ $a=2$ のテント写像の n 回写像過程で得られた $n+1$ ビットからなる上位 t ビット桁目抽出系列が $\{c_0, c_1, \dots, c_n\}$ と与えられたとき、 c_i の抽出元である x_i が含まれる領域番号 z_i の写像 $z_{i+1} = g(z_i)$ は以下である

$$z_{i+1} = g(z_i) = \begin{cases} 2z_i + c_{i+1} & (0 \leq z_i < 2^{t-1}) \\ 2(2^t - 1 - z_i) + c_{i+1} & (2^{t-1} \leq z_i < 2^t) \end{cases} \quad (3.80)$$

証明 $z_i < 2^{t-1}$ の場合では、テント写像 $x_{i+1} = f_2(x_i) = 2x_i$ が選ばれる。このとき、 x_i が含まれる領域番号を $z_i = \omega$ ($\omega < 2^{t-1}$)とすると、 z_i の区間は、 $(\frac{\omega}{2^t}, \frac{\omega+1}{2^t}) \rightarrow (\frac{2\omega}{2^t}, \frac{2(\omega+1)}{2^t})$ へ写像される。写像後の区間は、 $(\frac{2\omega}{2^t}, \frac{2\omega+1}{2^t})$ と $(\frac{2\omega+1}{2^t}, \frac{2\omega+2}{2^t})$ に分割でき、それぞれは式(3.77)より、 $z_{i+1} = 2\omega$ 、 $z_{i+1} = 2\omega + 1$ を意味する。ここで c_{i+1} は既知情報なので、 $c_{i+1} = 0$ ならば前者が選ばれ、 $c_{i+1} = 1$ ならば後者が選ばれているはずである。よって、 $z_{i+1} = 2z_i + c_{i+1}$ である。

$z_i \geq 2^{t-1}$ の場合は、テント写像 $x_{i+1} = f_2(x_i) = 2(1-x_i)$ が選ばれる。このとき、 x_i が含まれる領域番号 $z_i (= \omega$ ($\omega \geq 2^{t-1}$))の区間は、 $(\frac{\omega}{2^t}, \frac{\omega+1}{2^t}) \rightarrow (\frac{2(2^t-\omega-1)}{2^t}, \frac{2(2^t-\omega)}{2^t})$ へ写像される。写像後の区間は $(\frac{2(2^t-\omega)}{2^t}, \frac{2(2^t-\omega)+1}{2^t})$ と $(\frac{2(2^t-\omega)+1}{2^t}, \frac{2(2^t-\omega)+2}{2^t})$ に分割でき、それぞれは式(3.77)より、 $z_{i+1} = 2(2^t - \omega - 1)$ 、

$z_{i+1} = 2(2^t - \omega - 1) + 1$ 意味する。ここで c_{i+1} は既知情報なので、 $c_{i+1} = 0$ ならば前者が選ばれ、 $c_{i+1} = 1$ ならば後者が選ばれているはずである。よって、 $z_{i+1} = 2(2^t - 1 - z_i) + c_{i+1}$ である。

□

これより, z_0 候補を式 (3.79) より与えれば, 観測ビット c_i と式 (3.80) から z_i 軌道が一意に決定される。上記にて z_i 軌道 ($= z_i$ 系列) が求まったならば, 式 (3.81) によって z_i 系列は z_i の含まれる最上位ビット系列 (b_i 系列) に変換でき, 最終状態 x_n は x_0 を唯一つの未知数とする 1 次式として表すことができ, 全章で述べた最上位ビット抽出系列の初期値推測法に帰着できる。

$$b_i = h(z_i) = \lfloor \frac{z_i}{2^{t-1}} \rfloor = \begin{cases} 0 & (z_i < 2^{t-1}) \\ 1 & (z_i \geq 2^{t-1}) \end{cases} \quad (3.81)$$

$$x_n = f_2^n(x_0) = \sum_{i=1}^n p_i 2^i + q 2^n x_0 \quad (3.82)$$

$$p_i = \frac{h(z_{n-i})}{\hat{h}(z_{n-i})} \prod_{k=n-i}^{n-1} \hat{h}(z_k) \quad (3.83)$$

$$q = \prod_{k=0}^{n-1} \hat{h}(z_k) \quad (3.84)$$

$$\hat{h}(z_i) = 1 - 2h(z_i) \quad (3.85)$$

最終状態 x_n が含まれる領域は z_n であることから, z_n の境界値が不等式に与える境界値となり, これを x_0 について解くと以下である。

(i). $q > 0$ のとき

$$\frac{z_n/2^t - \sum_{i=1}^n p_i 2^i}{q 2^n} < x_0 < \frac{(z_n + 1)/2^t - \sum_{i=1}^n p_i 2^i}{q 2^n} \quad (3.86)$$

(ii). $q < 0$ のとき

$$\frac{(z_n + 1)/2^t - \sum_{i=1}^n p_i 2^i}{q 2^n} < x_0 < \frac{z_n/2^t - \sum_{i=1}^n p_i 2^i}{q 2^n} \quad (3.87)$$

$|q| = 1$ なので, 1 つの z_0 候補からは, 解の範囲を $1/2^{n+t}$ の幅に絞り込むことができる様子が判る。

z_i 軌道の独立性

以下にパラメータ $a = 2$ のときに示される定理定理 3.5.4 に関する重要な系を記す。写像 F を反復して得られる軌道が互いに独立しているとは, 「ステップ i にて異なる値同士は, F による写像後のステップ $i+1$ においても異なる」ということを意味するものとする。すなわち以下とする。

$$u_i \neq v_i \implies u_{i+1} = F(u_i) \neq v_{i+1} = F(v_i) \quad (3.88)$$

系 3.5.5 z_i が定理 3.5.4 で示される遷移ルールに従う場合, 式 (3.78)), 式 (3.79) から得られる 2^{t-1} 個の z_0 候補を出発する 2^{t-1} 個の z_i 軌道(遷移パターン)は互いに独立である。

証明 定義 3.5.3 より, 上位 t ビット桁目の抽出では, $z_i = \omega$ の取りうる状態の集合 A は,

$$A = \{\omega \in \mathbb{Z}; 0 \leq \omega \leq 2^t - 1\} \quad (3.89)$$

である。また、 $c_0 = 0, c_0 = 1$ となる z_0 候補の集合 E, O は、それぞれ、 A のうちの偶数の集合と奇数の集合なので、

$$E = \{(\omega =)2\lambda \in \mathbb{Z} ; 0 \leq \lambda \leq 2^{t-1} - 1\} \quad (3.90)$$

$$O = \{(\omega =)2\lambda + 1 \in \mathbb{Z} ; 0 \leq \lambda \leq 2^{t-1} - 1\} \quad (3.91)$$

である ($E \cup O = A$)。ここで $i \geq 0$ に対して、 c_i から c_{i+1} へと遷移するパターンは計4通り考えられるので、各ケース毎に E, O がどのように写像されるかを示すと以下 (a)~(d) である。

(a). $\{c_i, c_{i+1}\} = \{0, 0\}$ のとき

$c_i = 0$ なので、対象とする集合は E である。尚、式 (3.80) は区間によって写像関数が異なるので、 E を部分集合

$$E0 = \{2\lambda \in \mathbb{Z} ; 0 \leq \lambda \leq 2^{t-2} - 1\} \quad (3.92)$$

$$E1 = \{2\lambda \in \mathbb{Z} ; 2^{t-2} \leq \lambda \leq 2^{t-1} - 1\} \quad (3.93)$$

に分割すると ($E0 \cup E1 = E$)、 $E0$ と $E1$ は式 (3.80) によって、それぞれ、

$$E0^* = \{4\lambda \in \mathbb{Z} ; 0 \leq \lambda \leq 2^{t-2} - 1\} \quad (3.94)$$

$$E1^* = \{4\lambda + 2 \in \mathbb{Z} ; 0 \leq \lambda \leq 2^{t-2} - 1\} \quad (3.95)$$

へ写像される。ここで、 $E0^* \cup E1^*$ は A のうちの偶数全体の集合を表しており、 $E0^* \cup E1^* = E$ である。また、式 (3.94)、式 (3.95) より、 $c_i = 0$ となる z_i の集合 E は、 $c_{i+1} = 0$ のとき、式 (3.80) によって E へ1対1に写像されることが判る ($E \rightarrow E$)。

(b). $\{c_i, c_{i+1}\} = \{0, 1\}$ のとき

$c_i = 0$ なので、対象とする集合は E である。同じく E を、部分集合 $E0, E1$ ($E0 \cup E1 = E$) に分割すると、 $E0$ と $E1$ は式 (3.80) によって、それぞれ、

$$E0^* = \{4\lambda + 1 \in \mathbb{Z} ; 0 \leq \lambda \leq 2^{t-2} - 1\} \quad (3.96)$$

$$E1^* = \{4\lambda + 3 \in \mathbb{Z} ; 0 \leq \lambda \leq 2^{t-2} - 1\} \quad (3.97)$$

へ写像される。ここで、 $E0^* \cup E1^*$ は A のうちの奇数全体の集合を表しており、 $E0^* \cup E1^* = O$ である。従って、 $c_i = 0$ となる z_i の集合 E は、 $c_{i+1} = 1$ のとき、式 (3.80) によって O へ1対1に写像される ($E \rightarrow O$)。

(c). $\{c_i, c_{i+1}\} = \{1, 0\}$ のとき

$c_i = 1$ なので、対象とする集合は O である。上記と同様のことを考えると（途中略）、 $c_i = 1$ となる z_i の集合 O は、 $c_{i+1} = 0$ のとき、式 (3.80) によって E へ1対1に写像される ($O \rightarrow E$)。

(d). $\{c_i, c_{i+1}\} = \{1, 1\}$ のとき

$c_i = 1$ なので、対象とする集合は O である。上記と同様のことを考えると（途中略）、 $c_i = 1$ となる z_i の集合 O は、 $c_{i+1} = 1$ のとき、式 (3.80) によって O へ1対1に写像される ($O \rightarrow O$)。

上記より、式 (3.80) において E を定義域とする写像、 O を定義域とする写像は、それぞれ1対1写像であることが示された。すなわち、 E の異なる元 $e1 \neq e2$ ($e1, e2 \in E$) に対しては、 $g(e1) \neq g(e2)$

で, O の異なる元 $o1 \neq o2$ ($o1, o2 \in O$) に対しては, $g(o1) \neq g(o2)$ である. z_0 の候補の集合は $c_0 = 0$ ならば E , $c_0 = 1$ ならば O と $i = 0$ の時点であらかじめ分割されているので, それぞれに対して 2^{t-1} 個存在する z_0 候補を出発する 2^{t-1} 個の z_i 軌道は互いに独立である.

□

3.5.2 $1 < a < 2$ のテント写像の任意のビット桁抽出系列に対する初期値推測法 [25]

前節ではパラメータ $a = 2$ のテント写像から上位 t ビット桁目を抽出した系列が対象であったに対して, 本節では任意のパラメータ a ($1 < a \leq 2$) のテント写像から同じく上位 t ビット桁目を抽出した系列を対象とする. すなわち, ビット抽出ルールは同じく式 (3.76) であり, 式 (3.77) の $z_i = \omega$ が偶数のときに $c_i = 0$, 奇数のときに $c_i = 1$ と決定される. そして, 式 (3.79) を満たす全ての整数値 λ ($\lambda \in \mathbb{Z}; 0 \leq \lambda < 2^{t-1}$) が c_0 の抽出元である x_0 が存在する領域 z_0 の候補となる.

異なる点は z_i の遷移ルールである. パラメータ $a = 2$ の場合は式 (3.80) のように示されたが, パラメータ a ($1 < a \leq 2$) の場合は以下に示すように複雑な場合分けが生じる.

(1). Type-1. $|\lfloor az_i \rfloor - \lfloor a(z_i + 1) \rfloor| = 1$ のときの z_i 遷移ルール

$|\lfloor az_i \rfloor - \lfloor a(z_i + 1) \rfloor| = 1$ の場合 (図 3.6) を Type-1 とよぶ事にする. Type-1 では, $c_{i+1}=0$ または 1 となるようなビット抽出領域 z_{i+1} は, それぞれ 1 つずつ存在し, $\lfloor az_i \rfloor \mod 2$ が 0 または 1 によってさらに (a),(b) の 2 つに分類される. この場合の z_i 遷移ルールは以下である.

(a). $\lfloor az_i \rfloor \mod 2 = 0$ ($0 \leq z_i < 2^{t-1}$) または

$\lfloor a(2^t - 1 - z_i) \rfloor \mod 2 = 0$ ($2^{t-1} \leq z_i < 2^t$) のとき

(a-0). $c_{i+1} = 0$ のとき

$$z_{i+1} = \begin{cases} \lfloor az_i \rfloor + 0 & (0 \leq z_i < 2^{t-1}) \\ \lfloor a(2^t - 1 - z_i) \rfloor + 0 & (2^{t-1} \leq z_i < 2^t) \end{cases} \quad (3.98)$$

(a-1). $c_{i+1} = 1$ のとき

$$z_{i+1} = \begin{cases} \lfloor az_i \rfloor + 1 & (0 \leq z_i < 2^{t-1}) \\ \lfloor a(2^t - 1 - z_i) \rfloor + 1 & (2^{t-1} \leq z_i < 2^t) \end{cases} \quad (3.99)$$

(b). $\lfloor az_i \rfloor \mod 2 = 1$ ($0 \leq z_i < 2^{t-1}$) または

$\lfloor a(2^t - 1 - z_i) \rfloor \mod 2 = 1$ ($2^{t-1} \leq z_i < 2^t$) のとき

(b-0). $c_{i+1} = 0$ のとき

$$z_{i+1} = \begin{cases} \lfloor az_i \rfloor + 1 & (0 \leq z_i < 2^{t-1}) \\ \lfloor a(2^t - 1 - z_i) \rfloor + 1 & (2^{t-1} \leq z_i < 2^t) \end{cases} \quad (3.100)$$

(b-1). $c_{i+1} = 1$ のとき

$$z_{i+1} = \begin{cases} \lfloor az_i \rfloor + 0 & (0 \leq z_i < 2^{t-1}) \\ \lfloor a(2^t - 1 - z_i) \rfloor + 0 & (2^{t-1} \leq z_i < 2^t) \end{cases} \quad (3.101)$$

(2). Type-2. $|\lfloor az_i \rfloor - \lfloor a(z_i + 1) \rfloor| = 2$ のときの z_i 遷移ルール

$|\lfloor az_i \rfloor - \lfloor a(z_i + 1) \rfloor| = 2$ の場合 (図3.7) を Type-2 とよぶ事にする。Type-2 では, $c_{i+1}=0$ または 1 となるようなビット抽出領域 z_{i+1} は, 1つまたは2つ存在する。さらに $\lfloor az_i \rfloor \bmod 2$ が 0 または 1 によって (c),(d) の2つに分類される。この場合の z_i 遷移ルールは以下である。

(c). $\lfloor az_i \rfloor \bmod 2 = 0$ ($0 \leq z_i < 2^{t-1}$) または

$\lfloor a(2^t - 1 - z_i) \rfloor \bmod 2 = 0$ ($2^{t-1} \leq z_i < 2^t$) のとき

(c-0). $c_{i+1} = 0$ のとき (分岐が発生)

$$z_{i+1} = \begin{cases} \lfloor az_i \rfloor + 0 & (0 \leq z_i < 2^{t-1}) \\ \lfloor a(2^t - 1 - z_i) \rfloor + 0 & (2^{t-1} \leq z_i < 2^t) \end{cases} \quad (3.102)$$

$$z_{i+1} = \begin{cases} \lfloor az_i \rfloor + 2 & (0 \leq z_i < 2^{t-1}) \\ \lfloor a(2^t - 1 - z_i) \rfloor + 2 & (2^{t-1} \leq z_i < 2^t) \end{cases} \quad (3.103)$$

(c-1). $c_{i+1} = 1$ のとき

$$z_{i+1} = \begin{cases} \lfloor az_i \rfloor + 1 & (0 \leq z_i < 2^{t-1}) \\ \lfloor a(2^t - 1 - z_i) \rfloor + 1 & (2^{t-1} \leq z_i < 2^t) \end{cases} \quad (3.104)$$

(d). $\lfloor az_i \rfloor \bmod 2 = 1$ ($0 \leq z_i < 2^{t-1}$) または

$\lfloor a(2^t - 1 - z_i) \rfloor \bmod 2 = 1$ ($2^{t-1} \leq z_i < 2^t$) のとき

(d-0). $c_{i+1} = 0$ のとき

$$z_{i+1} = \begin{cases} \lfloor az_i \rfloor + 1 & (0 \leq z_i < 2^{t-1}) \\ \lfloor a(2^t - 1 - z_i) \rfloor + 1 & (2^{t-1} \leq z_i < 2^t) \end{cases} \quad (3.105)$$

(d-1). $c_{i+1} = 1$ のとき (分岐が発生)

$$z_{i+1} = \begin{cases} \lfloor az_i \rfloor + 0 & (0 \leq z_i < 2^{t-1}) \\ \lfloor a(2^t - 1 - z_i) \rfloor + 0 & (2^{t-1} \leq z_i < 2^t) \end{cases} \quad (3.106)$$

$$z_{i+1} = \begin{cases} \lfloor az_i \rfloor + 2 & (0 \leq z_i < 2^{t-1}) \\ \lfloor a(2^t - 1 - z_i) \rfloor + 2 & (2^{t-1} \leq z_i < 2^t) \end{cases} \quad (3.107)$$

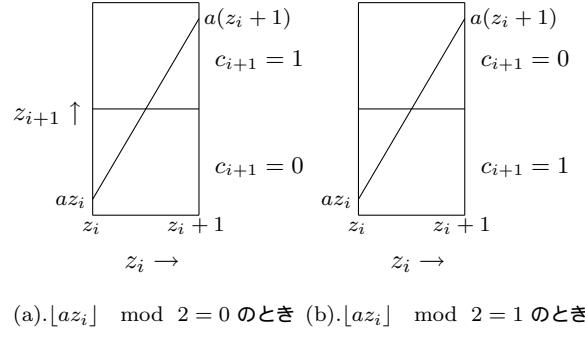


図 3.6 Type-1. $|\lfloor az_i \rfloor - \lfloor a(z_i + 1) \rfloor| = 1$ のとき

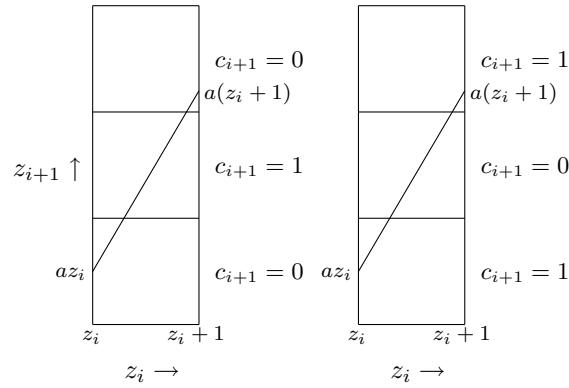


図 3.7 Type-2. $|\lfloor az_i \rfloor - \lfloor a(z_i + 1) \rfloor| = 2$ のとき

(3). z_i 軌道の確定と初期値推測

パラメータ $1 < a < 2$ の場合では、 x_i が含まれる領域 z_i の遷移ルールは上記 (a-0) ~ (d-1) の計 8 パターンに分類される。特に (c-0) と (d-1) の 2 つは、1 対 2 の写像で定義されるため、推測する z_i 軌道に分岐が生じる。そのどちらも候補として扱わなければならない。すなわち、最終的に z_i 軌道の数は、初期の z_0 の候補数 (2^{t-1}) よりも増える事になる。

この点に注意して、上記 (a-0) ~ (d-1) に基づいて z_i 軌道 (= z_i 系列) を決定すれば、後は $a = 2$ の場合と同様である。すなわち、それぞれの z_i 軌道 (= z_i 系列) 每に、式 (3.81) に従って最上位

ビット系列 (b_i 系列) に変換して、最終状態 x_n を x_0 を变数に含む 1 次式を決定する。

$$x_n = f_a^n(x_0) = \sum_{i=1}^n p_i a^i + q a^n x_0 \quad (3.108)$$

$$p_i = \frac{h(z_{n-i})}{\hat{h}(z_{n-i})} \prod_{k=n-i}^{n-1} \hat{h}(z_k) \quad (3.109)$$

$$q = \prod_{k=0}^{n-1} \hat{h}(z_k) \quad (3.110)$$

$$\hat{h}(z_i) = 1 - 2h(z_i) \quad (3.111)$$

最終状態 x_n が含まれる領域は z_n であることから、 x_n の境界値は z_n を用いて $z_n/2^t < x_n < (z_n + 1)/2^t$ と表せるのでこれを x_0 について解くと以下を得る。

(i). $q > 0$ のとき

$$\frac{z_n/2^t - \sum_{i=1}^n p_i a^i}{q a^n} < x_0 < \frac{(z_n + 1)/2^t - \sum_{i=1}^n p_i a^i}{q a^n} \quad (3.112)$$

(ii). $q < 0$ のとき

$$\frac{(z_n + 1)/2^t - \sum_{i=1}^n p_i a^i}{q a^n} < x_0 < \frac{z_n/2^t - \sum_{i=1}^n p_i a^i}{q a^n} \quad (3.113)$$

パラメータ $a = 2$ の場合では、 z_0 候補は 2^{t-1} 個存在し、それぞれの z_0 毎に固有の z_i 軌道 (z_i 系列) が決定されて、それぞれの z_i 系列毎に求まつた解の範囲 (2^{t-1} 個) 内に当該系列をし得る初期値が含まれていた [24]。 $a < 2$ の場合では、(c-0) と (d-1) の分岐に関してどちらか一方が正しい軌道である可能性が高い等の理由から、上記にて求めた解の範囲の全てに当該系列を生成し得る初期値を含む訳ではない（偽の解が含まれる）。偽の解の判別は、実際に求まつた解から系列を生成してみない限り判らない。また、一方で、上記にて求めた複数の解のうち、当該系列を生成した初期値を生成し得る初期値を含む場合でも、境界値付近（不等式）は正しくない（境界値付近は当該系列を生成し得ない）といった不確定な要素を含む。後者についての補正の考え方は文献 [23] で述べたが、ここでは省略する。

例 3.5.6 初期値 $x_0 = 0.35$ 、パラメータ $a = 64535/32768 = 1.96945$ とする。定義 3.5.2 で示される生成法 $S_{a,t}(x_0, n)$ により、 $n = 5$ 回の写像反復で得られる合計 $n+1 = 6$ 個の状態 $\{x_0, x_1, \dots, x_5\}$ から、式 (3.76) に従い上位第 $t = 3$ ビット桁目を抽出して得られた合計 $n+1 = 6$ ビットの系列 $\{c_0, c_1, \dots, c_5\} = \{0, 1, 0, 0, 1, 1\}$ が与えられているものとする。このとき本推測法によって、当該系列と同じ系列を生成し得る初期値 x_0 の推測を行う。結果は表 3.1 に示した。

表 3.1 の結果について説明する。まず、 $t = 3$ なので、 z_0 の候補数は $2^{t-1} = 4$ 個あり、その候補は $c_0 = 0$ および式 (3.79) より、 $0, 2, 4, 6$ と決定される。その後 (a-0) ~ (d-1) に従い $z_1 \sim z_5$ を決定する。その際に (c-0), (d-1) に分岐があるため、 z_i 軌道の数は増えていく。 z_i 軌道 (z_i 系列) が決定したら、式 (3.81) にて最上位ビット系列 (b_i 系列) に変換し、式 (3.109)、式 (3.110) にて多項式係数を決定する。この段階で x_n を x_0 の 1 变数で表せる。最終状態 x_n の範囲は z_n の存在範囲に等しいという境界値条件を利用して、式 (3.112) または式 (3.113) にて x_0 (推測値) の範囲を特定する。

3.5 テント写像の任意のビット桁(上位 t 桁目のビット / 下位側のビット)を抽出した系列に対する初期値推測法 [24],[25]57

表 3.1 初期値推測例

((3.112),(3.113) で求めた解の区間を , 区間幅の 1/1000 で探索)					
$z_0 \sim z_5$	$p_1 \sim p_5$	q	$x_0 \min$	$x_0 \max$	stat.
0 1 2 4 5 3	1 -1 0 0 0	1	0.077095	0.081313	
0 1 2 4 5 5	1 -1 0 0 0	1	0.085532	0.089751	×
0 1 2 4 7 1	1 -1 0 0 0	1	0.068657	0.072876	
2 3 6 2 3 5	0 0 1 0 0	-1	0.232503	0.236722	×
2 3 6 2 3 7	0 0 1 0 0	-1	0.224066	0.228284	×
2 3 6 2 5 3	1 0 -1 0 0	1	0.204003	0.208222	×
2 3 6 2 5 5	1 0 -1 0 0	1	0.212440	0.216659	×
2 5 4 6 1 1	0 1 -1 1 0	-1	0.372410	0.376628	×
2 5 4 6 1 3	0 1 -1 1 0	-1	0.363972	0.368191	
2 5 4 6 3 5	0 1 -1 1 0	-1	0.355535	0.359753	
2 5 4 6 3 7	0 1 -1 1 0	-1	0.347097	0.351316	
4 5 4 6 1 1	0 1 -1 1 -1	1	0.623372	0.627590	×
4 5 4 6 1 3	0 1 -1 1 -1	1	0.631809	0.636028	×
4 5 4 6 3 5	0 1 -1 1 -1	1	0.640247	0.644465	×
4 5 4 6 3 7	0 1 -1 1 -1	1	0.648684	0.652903	×
4 7 0 0 1 1	0 0 0 1 -1	1	0.496463	0.500682	
4 7 0 0 1 3	0 0 0 1 -1	1	0.504901	0.509119	
6 1 2 4 5 3	1 -1 0 0 1	-1	0.918687	0.922905	×
6 1 2 4 5 5	1 -1 0 0 1	-1	0.910249	0.914468	×
6 1 2 4 7 1	1 -1 0 0 1	-1	0.927124	0.931343	×
6 3 6 2 3 5	0 0 1 0 -1	1	0.763278	0.767497	×
6 3 6 2 3 7	0 0 1 0 -1	1	0.771716	0.775934	
6 3 6 2 5 3	1 0 -1 0 1	-1	0.791778	0.795997	×
6 3 6 2 5 5	1 0 -1 0 1	-1	0.783341	0.787560	

× ... 範囲内に観測ビット列を生成し得る初期値を含まない

... 範囲内に観測ビット列と同じ系列を生成し得る初期値を含む

... 範囲内に観測ビット列を生成した初期値を含む

3.5.3 下位側を抽出した系列に対する初期値推測法に関する考察

上位 t ビット桁目抽出の場合のポイントは , パラメータ $a = 2$ の場合では , 解の範囲は 2^{t-1} 個 ($= z_0$ 候補数 (式 (3.79))) だけ存在して , 全ての解の範囲内に与えられた系列と同じ系列を生成し得る初期値が含まれていたが , パラメータ $1 < a < 2$ の場合は , (c-0),(d-1) の分岐によって z_i 系列の数が増えていくため , (式 (3.112)) または (式 (3.113)) にて評価しなければならない量が増える点 , および , 2.3.4 節の実験例のように , 求めた解の全てに , 与えられた系列と同じ系列を生成し得る初期値を含む訳ではない点である . つまり , (c-0),(d-1) の分岐が生じるケース (Type-2) を多く含むことは , 本推測のための計算量が増える事を意味する . 例えば , パラメータ a が 2 付近であれば , 分岐の生じる Type-2 が , 分岐のない Type-1 よりも圧倒的に多いため , 推測のための計算量が多くなる事が予想される . (ただし , Type-2 であっても , (c-1),(d-0) の場合は分岐が生じない .)

尚 , 本推測法は , パラメータ $1 < a \leq 2$ のテント写像から得られた系列を対象としたものであるが , ここでの推測法と同様の「考え方」が , 仮に , パラメータ $a > 2$ の写像にも適用できると仮定するならば , パラメータ a が , より大きな値であれば (c-0),(d-1) のような分岐が増えるため , 推測のための計算量はさらに増えることになる .

3.5.4 本節のまとめ

パラメータ a ($1 < a \leq 2$) のテント写像 (式 (3.75)) の n 回反復過程 $x_{i+1} = f_a(x_i)$ ($0 \leq i < n$) で得られる計 $n+1$ 個の値 $\{x_0, x_1, \dots, x_n\}$ ($= \{x_i\}_{i=0}^n$) から, 写像のたびに x_i の上位 t ビット桁目を抽出して構成された計 $n+1$ ビットの擬似ランダムビット列 $\{c_0, c_1, \dots, c_n\}$ ($= \{c_i\}_{i=0}^n$) が与えられたときに, パラメータ a ($1 < a \leq 2$) を既知として, 当該系列 $\{c_i\}_{i=0}^n$ を生成し得る初期値 x_0 の範囲を推測する手法を示した.

パラメータ $a = 2$ の場合では, 解の範囲は 2^{t-1} 個だけ存在し, 全ての解の範囲内に与えられた系列と同じ系列を生成し得る初期値が含まれることを示した. 一方で, $1 < a < 2$ の場合は, (c-0),(d-1) の分岐によって z_i 系列の数が増えていくため, 式 (3.112) または式 (3.113) を評価するために必要な計算量が増えることを示した. また, 求めた解の全てに与えられた系列と同じ系列を生成し得る初期値を含む訳ではなく(偽の解を多くむ), 含む場合でも(式 (3.112)) または(式 (3.113)) の境界付近が正しくない(当該系列を生成し得ない)といった不確定な要素が多く含まれることが判った.

本推測法では z_i の遷移は写像の前後の2つの状態しか考えていないため, 多くの過去の状態を考慮することによって不確定さを減らすことができる可能性があると考えられる. 効率化の検討が今後の課題である.

3.6 生成法が有限精度で実装された場合の初期値推測法 [27]

テント写像やロジスティック写像等の非線形写像は、初期条件に鋭敏な性質 (SDIC:Sensitive Dependence on Initial Condition) を有することが知られている。これは初期の僅かな差が写像を反復する度に指数関数的に広がって行き、僅かな回数の写像後には値域全体に広がってしまう性質をいう。テント写像やロジスティック写像を有限精度の計算機に実装した場合は、写像の度に最下位桁が丸められるため（最近接丸め、切り捨て等様々ある）、コンピュータに実装して得られる可観測系列は、本来の軌道（無限精度の場合に得られる系列）と全く異なる軌道になる。この性質／影響は、コンピュータアーキテクチャの違いによる微小な演算特性差にまで及ぶので、同じソースコードであっても処理系によって異なる結果をもたらしてしまう（非互換性）。ある意味非常に興味深く、乱数生成源として活用するには魅力的に思える。

前節までに示した推測法は、暗黙のうちに理想的な環境（無限精度）を前提としているので、有限精度の計算機に実装された生成法が生成する系列に対しては有効的な初期値解を与えないことが容易に推測される。さらに初期条件鋭敏性の影響で推測は困難になるであろうことが予測された。

本節では、コンピュータに実装された生成法（現実的に誤差が含まれる有限精度の演算による生成法）が生成する擬似ランダムビット列が与えられたときに、当該系列を生成し得る初期値の範囲がどのような場所に存在するかを明らかにする。そして、前節までに述べた無限精度の場合の初期値推測法による解と対比して示す。

3.6.1 有限精度のテント写像モデル

本節では、式(2.1)で示されるパラメータ $1 < a < 2^{*10}$ のテント写像をコンピュータに実装した場合に、写像の度に演算誤差が加わることを考慮したテント写像のモデルを考える。尚、本論文において有限精度のモデルを考えるにあたっては、IEEE 754に準じた倍精度浮動小数点表記および演算を想定している^{*11}。IEEE 754にはいくつかの丸めモードが定義されているが、本論文においては、最近接丸め（指定精度内で最も近い値への近似）が用いられるものとする。

有限精度で実装された（演算誤差を生じる）テント写像（その関数 $g_a(x)$ ）を以下に示す式(3.114)と定義する。

$$\begin{aligned} x_{i+1} &= g_a(x_i) \\ &\stackrel{\text{def}}{=} f_a(x_i) + \delta_{i+1} \\ &= \begin{cases} ax_i + \delta_{i+1} & (0 \leq x < 1/2) \\ a(1 - x_i) + \delta_{i+1} & (1/2 \leq x \leq 1) \end{cases} \end{aligned} \quad (3.114)$$

x_i は、初期値 x_0 から写像関数 $g_a(x)$ による第 i 回目の写像後の値である。 δ_i は、そのときに加わる演算誤差である（第 i 回目の写像の計算で加わる演算誤差）。尚、特に断りがない限り x_i は 2 進表

^{*10} パラメータが $a = 2$ の場合は特殊で、結果として誤差を含まずに計算できる（左 1 ビットシフト）。従って、本論文で述べる推測法は $1 < a < 2$ の場合を想定している。

^{*11} IEEE 754 は浮動小数点の表記および演算の標準規格である。かつては様々な種類があったが、今日の代表的な CPU(FPU)、およびソフトウェアにおいて最も広く採用されている。正式名称は IEEE Standard for Floating-Point Arithmetic (ANSI/IEEE Std 754-2008)

記された値であることに留意されたい。

演算誤差 δ_i の実態について触れる。 x_i が既に2進表記されていることを考慮すれば、 $1 - x_i$ において演算誤差は生じないことが判る。演算誤差を考慮しない通常のテント写像式(2.1)を、有限精度の計算機に実装した際に生じる演算誤差とは、 $a \times x_i$ または $a \times (1 - x_i)$ の積算における丸め誤差である^{*12}。

次いで δ_i の大きさについて触れる。倍精度浮動小数点演算(IEEE 754)を考えた場合は仮数部の精度は52ビットである。尚、演算においては、指数部は扱う数値の最大のものに固定される。掛け合わせる数の一方はパラメータ a ($1 < a < 2$) で、もう一方は $0 \leq x_i \leq 1$ または $0 \leq 1 - x_i \leq 1$ であることから、掛け合わせる数で最大のものは常に a である ($0 \leq x_i \leq 1 < a < 2$)。 $1 < a < 2$ であることから、 a は2進表記で常に $(1.c_1c_2 \dots c_{52})_2 \times 2^0$, $c_j \in \{0, 1\}$, $1 \leq j \leq 52$ と表現される。つまり、本演算で扱う最も大きい数のオーダー(指数部の数)は0である。従って、本演算で表現することができる最小値は 2^{-52} である(倍精度浮動小数点演算(IEEE 754)では仮数部の精度は52ビットなので)。本論文では、この値を ε と呼ぶことにする ($\varepsilon = 1/2^{52}$)。尚、本論文での端数処理は最近接丸めを考えているので、

$$|\delta_i| \leq \varepsilon/2 \Leftrightarrow |\delta_i| \leq 1/2^{53} \quad (3.115)$$

であることに注意されたい。

3.6.2 有限精度のテント写像モデルの n 回反復写像と観測ビット列の関係

以降では、コンピュータに初期値を与える際にも誤差が生じることを考える。真の初期値を \hat{x}_0 と表し、コンピュータのメモリ上に格納される初期値を $x_0 = \hat{x}_0 + \delta_0$ とする。 x_0 を初期値として、式(3.114)で定義されるパラメータ a の有限精度のテント写像モデルの n 回反復過程 $x_{i+1} = g_a(x_i)$ ($0 \leq i < n$) で得られる $n+1$ 個の値 $\{x_0, x_1, \dots, x_n\}$ を考える。式(3.4)に従い、各ステップ i 毎に x_i の最上位ビットを抽出して構成された計 $n+1$ ビットの擬似ランダムビット列 $\{b_0, b_1, \dots, b_n\}$ が与えられたとする。このとき、式(3.114)で定義される有限精度のテント写像モデルの n 回反復写像 $x_n = g_a^n(x_0) = g_a^n(\hat{x}_0 + \delta_0)$ の多項式の係数と、観測ビット列 $\{b_0, b_1, \dots, b_n\}$ との関係について以下の定理を得ることができる。

定理 3.6.1 \hat{x}_0 を真の初期値とし、 \hat{x}_0 を2進変換する際に生じる丸め誤差を δ_0 とする。コンピュータのメモリ上に格納される初期値を $x_0 = \hat{x}_0 + \delta_0$ とする。また、パラメータ a ($1 < a < 2$) は既知とする。式(3.114)、式(3.4)に従って構成された計 $n+1$ ビットの擬似ランダムビット列 $\{b_0, b_1, \dots, b_n\}$ が与えられたとき、式(3.114)の n 回反復による合成写像 $g_a^n(x_0) = g_a^n(\hat{x}_0 + \delta_0)$ は、観測ビット列

^{*12} IEEE 754 の倍精度浮動小数点表記において仮数部は52ビットである。仮数部が52ビットどうしの積算は104ビットに膨れ上がるが、これを52ビットに丸める端数処理時に誤差が介入する。尚、本論文においての端数処理は「切り捨て」ではなく「最近接丸め」を考える。

$\{b_0, b_1, \dots, b_n\}$ を用いて以下のように決定される^{*13} .

$$\begin{aligned} x_n &= g_a^n(\hat{x}_0 + \delta_0) \\ &= \left(\sum_{i=1}^n p_i a^i \right) + q a^n \hat{x}_0 + \left(\sum_{i=1}^n s_i a^i \right) + \delta_n \end{aligned} \quad (3.116)$$

$$p_i = \frac{b_{n-i}}{\hat{b}_{n-i}} r_i \quad (3.117)$$

$$q = r_n \quad (3.118)$$

$$r_i = \prod_{k=n-i}^{n-1} \hat{b}_k \quad (3.119)$$

$$s_i = \delta_{n-i} r_i \quad (3.120)$$

$$\hat{b}_i = 1 - 2b_i \quad (3.121)$$

証明 式 (3.116) ~ (3.121) をまとめて記すと以下の式 (3.122) を得る .

$$\begin{aligned} x_n &= g_a^n(\hat{x}_0 + \delta_0) \\ &= \left(\sum_{i=1}^n \left(a^i \frac{b_{n-i}}{\hat{b}_{n-i}} \prod_{k=n-i}^{n-1} \hat{b}_k \right) \right) + a^n \hat{x}_0 \prod_{k=0}^{n-1} \hat{b}_k \\ &\quad + \left(\sum_{i=1}^n \left(a^i \delta_{n-i} \prod_{k=n-i}^{n-1} \hat{b}_k \right) \right) + \delta_n \end{aligned} \quad (3.122)$$

一方で , 有限精度のテント写像モデル式 (3.114) は , 最上位ビット抽出ルール式 (3.4) と併せて以下の式 (3.123) と表現できる .

$$\begin{aligned} x_{i+1} &= g_a(x_i) \\ &= (1 - b_i)(ax_i) + b_i a(1 - x_i) + \delta_{i+1} \\ &= b_i a + (1 - 2b_i)ax_i + \delta_{i+1} \\ &= b_i a + \hat{b}_i ax_i + \delta_{i+1} \end{aligned} \quad (3.123)$$

以降において , 式 (3.122) が任意の自然数 n について成立することを帰納的に示す .

はじめに $n = 1$ のときに式 (3.122) が成り立つことを示す . 式 (3.123) より ,

$$\begin{aligned} x_1 &= g_a(x_0) = g_a(\hat{x}_0 + \delta_0) \\ &= b_0 a + \hat{b}_0 a(\hat{x}_0 + \delta_0) + \delta_1 \\ &= a \frac{b_0}{\hat{b}_0} \hat{b}_0 + a \hat{x}_0 \hat{b}_0 + a \delta_0 \hat{b}_0 + \delta_1 \end{aligned} \quad (3.124)$$

であることから , これは式 (3.122) において $n = 1$ とした場合に他ならない . すなわち , $n = 1$ のときに式 (3.122) は成立している .

^{*13} a は 2 進変換後の値が格納されているものとする (誤差を考えない). 擬似ランダムビット生成プログラム内では 2 進変換後の値が使われること , および , ここではパラメータ a は既知として扱うので , この前提に問題はない .

次に式(3.122)が任意の自然数 $n = m$ ($m \geq 1$)について成立すると仮定したとき, $n = m + 1$ についても成立することを示す。 $n = m + 1$ のときは、式(3.123)より、

$$\begin{aligned} x_{m+1} &= g_a(x_m) \\ &= b_m a + \hat{b}_m a x_m + \delta_{m+1} \\ &= ab_m + ab_m \hat{x}_m + \delta_{m+1} \end{aligned} \quad (3.125)$$

である。ここで $n = m$ のときに式(3.122)が成立するという仮定から、

$$\begin{aligned} x_{m+1} &= ab_m + ab_m \left\{ \left(\sum_{i=1}^m \left(a^i \frac{b_{m-i}}{\hat{b}_{m-i}} \prod_{k=m-i}^{m-1} \hat{b}_k \right) \right. \right. \\ &\quad + a^m \hat{x}_0 \prod_{k=0}^{m-1} \hat{b}_k \\ &\quad + \left. \left(\sum_{i=1}^{m-1} \left(a^i \delta_{m-i} \prod_{k=s-i}^{m-1} \hat{b}_k \right) \right) \right. \\ &\quad \left. + \delta_m \right\} + \delta_{m+1} \\ &= ab_m + \left(\sum_{i=1}^m \left(a^{i+1} \frac{b_{m-i}}{\hat{b}_{m-i}} \prod_{k=m-i}^m \hat{b}_k \right) \right) \\ &\quad + a^{m+1} \hat{x}_0 \prod_{k=0}^m \hat{b}_k \\ &\quad + \left(\sum_{i=1}^m \left(a^{i+1} \delta_{m-i} \prod_{k=m-i}^m \hat{b}_k \right) \right) \\ &\quad + ab_m \delta_m + \delta_{m+1} \end{aligned} \quad (3.126)$$

の関係を得る。

$j = i + 1$ とおくと、式(3.126)は

$$\begin{aligned} x_{m+1} &= ab_m + \left(\sum_{j=2}^{m+1} \left(a^j \frac{b_{m+1-j}}{\hat{b}_{m+1-j}} \prod_{k=m+1-j}^m \hat{b}_k \right) \right) \\ &\quad + a^{m+1} \hat{x}_0 \prod_{k=0}^m \hat{b}_k \\ &\quad + \left(\sum_{j=2}^{m+1} \left(a^j \delta_{m+1-j} \prod_{k=m+1-j}^m \hat{b}_k \right) \right) \\ &\quad + ab_m \delta_m + \delta_{m+1} \end{aligned} \quad (3.127)$$

ここで、式(3.127)の第2項目の \sum の中身を U_j 、第4項目の \sum の中身を V_j とする、

$$U_j = a^j \frac{b_{m+1-j}}{\hat{b}_{m+1-j}} \prod_{k=m+1-j}^m \hat{b}_k \quad (3.128)$$

$$V_j = a^j \delta_{m+1-j} \prod_{k=m+1-j}^m \hat{b}_k \quad (3.129)$$

となる。このとき、式(3.127)の第1項目は U_1 、第5項目は V_1 と表すことができる。

$$U_1 = a^1 \frac{b_m}{\hat{b}_m} \hat{b}_m \equiv ab_m \quad (3.130)$$

$$V_1 = a^1 \delta_m \hat{b}_m \equiv a \hat{b}_m \delta_m \quad (3.131)$$

これより、式(3.127)は以下の式(3.132)と表すことができる。

$$\begin{aligned} x_{m+1} &= \left(\sum_{j=1}^{m+1} U_j \right) + a^{m+1} \hat{x}_0 \prod_{k=0}^m \hat{b}_k \\ &\quad + \left(\sum_{j=1}^{m+1} V_j \right) + \delta_{m+1} \\ &= \left(\sum_{j=1}^{m+1} \left(a^j \frac{b_{m+1-j}}{\hat{b}_{m+1-j}} \prod_{k=m+1-j}^m \hat{b}_k \right) \right) \\ &\quad + a^{m+1} \hat{x}_0 \prod_{k=0}^m \hat{b}_k \\ &\quad + \left(\sum_{j=1}^{m+1} \left(a^j \delta_{m+1-j} \prod_{k=m+1-j}^m \hat{b}_k \right) \right) \\ &\quad + \delta_{m+1} \end{aligned} \quad (3.132)$$

式(3.132)は $n = m + 1$ としたときの式(3.122)に等しい。よって、式(3.122)は任意の自然数 n について成立する。

□

3.6.3 有限精度のテント写像モデルから生成されたランダムビット列の初期値推測

以下の式(3.133)により D を定義すると、式(3.116)は以下の式(3.134)と表せる。

$$D \stackrel{\text{def}}{=} \left(\sum_{i=1}^n s_i a^i \right) + \delta_n \quad (3.133)$$

$$\begin{aligned} x_n &= g_a^n(\hat{x}_0 + \delta_0) \\ &= \sum_{i=1}^n p_i a^i + q a^n \hat{x}_0 + D \end{aligned} \quad (3.134)$$

3.2節で示した無限精度の場合の初期値推測と同じく、最上位ビット抽出ルール(式(3.4))より得た x_n の存在範囲の必要条件(不等式(3.19))を用いて、式(3.116)~(3.121)を初期値 x_0 について整理すると以下の解を得る(式(3.135)~(3.138))。

(i)' $b_n = 0, q > 0$ のとき

$$\frac{-\sum_{i=1}^n p_i a^i - D}{q a^n} \leq \hat{x}_0 < \frac{1/2 - \sum_{i=1}^n p_i a^i - D}{q a^n} \quad (3.135)$$

(ii)' $b_n = 0, q < 0$ のとき

$$\frac{1/2 - \sum_{i=1}^n p_i a^i - D}{q a^n} < \hat{x}_0 \leq \frac{-\sum_{i=1}^n p_i a^i - D}{q a^n} \quad (3.136)$$

(iii)' $b_n = 1, q > 0$ のとき

$$\frac{1/2 - \sum_{i=1}^n p_i a^i - D}{q a^n} \leq \hat{x}_0 \leq \frac{1 - \sum_{i=1}^n p_i a^i - D}{q a^n} \quad (3.137)$$

(iv)' $b_n = 1, q < 0$ のとき

$$\frac{1 - \sum_{i=1}^n p_i a^i - D}{q a^n} \leq \hat{x}_0 \leq \frac{1/2 - \sum_{i=1}^n p_i a^i - D}{q a^n} \quad (3.138)$$

これより、有限精度で実装された生成法が生成するランダムビット列の初期値解（式(3.135)～(3.138)）は、当該系列が無限精度で実装された生成法が生成するランダムビット列だと考えたときに、無限精度の場合の推測法から得られる初期値解（式(3.20)～(3.23)）（ただし最終値 x_n の存在範囲の必要条件から得られる初期値解）から $D/(qa^n)$ だけ離れた場所に存在することが判る^{*14}。

3.6.4 無限精度で実装された生成法の場合の初期値解からの乖離 $D/(qa^n)$ の大きさについて

本節では、有限精度で実装された生成法が生成するランダムビット列の初期値解（式(3.135)～(3.138)）と、当該系列が無限精度で実装された生成法が生成するランダムビット列だと考えたときに、無限精度の場合の推測法から得られる初期値解（式(3.20)～(3.23)）（ただし最終値 x_n の存在範囲の必要条件から得られる初期値解）との乖離 $D/(qa^n)$ の大きさを概算により求める。

これには $D/(qa^n)$ について考える最小値と最大値を見積もればよい。見積もりにあたり、有限精度のテント写像モデル式(3.114)において、第 i 回目の写像で生じる演算誤差 δ_i は常に最大となるように選ぶこととする。つまり、 $\delta_i = \varepsilon/2$ または $-\varepsilon/2$ として考える。式(3.133)は、式(3.118)～(3.120)より、

$$D = \left(\sum_{i=1}^n s_i a^i \right) + \delta_n = \left(\sum_{i=1}^n r_i \delta_{n-i} a^i \right) + \delta_n \quad (3.139)$$

である。ここで、 r_i ($1 \leq i \leq n$) と q は、それぞれ、式(3.119),(3.118)より、 -1 または $+1$ （正負の符号）であることから、 $D/(qa^n)$ は以下のときに最小値となり、

$$\begin{cases} \delta_n = +\frac{\varepsilon}{2}, r_i \delta_{n-i} = +\frac{\varepsilon}{2} (1 \leq i \leq n), q = -1 \\ \text{または} \\ \delta_n = -\frac{\varepsilon}{2}, r_i \delta_{n-i} = -\frac{\varepsilon}{2} (1 \leq i \leq n), q = +1 \end{cases} \quad (3.140)$$

また、以下のときに最大値となる。

$$\begin{cases} \delta_n = +\frac{\varepsilon}{2}, r_i \delta_{n-i} = +\frac{\varepsilon}{2} (1 \leq i \leq n), q = +1 \\ \text{または} \\ \delta_n = -\frac{\varepsilon}{2}, r_i \delta_{n-i} = -\frac{\varepsilon}{2} (1 \leq i \leq n), q = -1 \end{cases} \quad (3.141)$$

^{*14} パラメータが $a \neq 2$ の場合は、 n 回写像後の $x_n = f_a^n(x_0)$ の存在範囲は、式(3.4)で与えられる範囲よりも狭いので、式(3.135)～(3.138)で与えられる範囲内の全ての点が観測ビット列を生成し得る初期値であるとは限らない（観測ビット列以外の系列を生成する初期値をも含む）。これと同じくして、式(3.135)～(3.138)の不等号“ \leq ”についても、境界を含むか否か（等号を含むか否か）はケースバイケースである[26]。

ここで、パラメータ a は $1 < a < 2$ であることに注意すれば、

$$\begin{aligned} \left(\frac{D}{qa_n} \right)_{min} &= -\frac{\frac{\varepsilon}{2}(1 + \sum_{i=1}^n a^i)}{a^n} \\ &= -\frac{\varepsilon}{2a^n} \sum_{i=0}^n a^i = -\frac{\varepsilon}{2a^n} \frac{1 - a^{n+1}}{1 - a} \\ &> -\frac{a}{2(a-1)}\varepsilon \end{aligned} \quad (3.142)$$

$$\begin{aligned} \left(\frac{D}{qa_n} \right)_{max} &= \frac{\frac{\varepsilon}{2}(1 + \sum_{i=1}^n a^i)}{a^n} \\ &= \frac{\varepsilon}{2a^n} \sum_{i=0}^n a^i = \frac{\varepsilon}{2a^n} \frac{1 - a^{n+1}}{1 - a} \\ &< \frac{a}{2(a-1)}\varepsilon \end{aligned} \quad (3.143)$$

の関係を得る。従って以下の式 (3.144) と整理される。

$$\left| \frac{D}{qa^n} \right| < \beta\varepsilon, \quad \left(\beta = \frac{a}{2(a-1)} \right) \quad (3.144)$$

ここまでではパラメータ $1 < a < 2$ の場合を考えてきたが、本推測法の推測対象となる生成系の現実問題を考慮すると、パラメータ a は 2 付近が選ばれることが望ましいと考えられる。理由は、小さな a を選んだ場合は、最終的に x_i が落ち着く周期軌道の値域 $[a(1 - a/2), a/2]$ が狭くなるためである。ここでは概ね $1.5 < a < 2$ が適当であるとして、下記の a 値について具体的に式 (3.144) を評価すると、

パラメータ $a = 1.99$ のとき	$ D/(qa^n) < 1.00505\varepsilon$
パラメータ $a = 1.8$ のとき	$ D/(qa^n) < 1.125\varepsilon$
パラメータ $a = 1.5$ のとき	$ D/(qa^n) < 1.5\varepsilon$

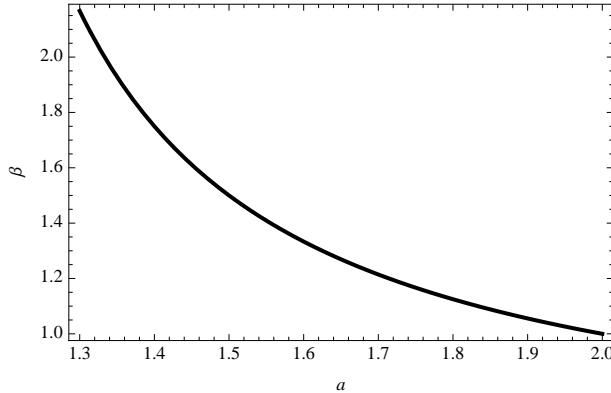
を得る（図 3.8 参照）。

従って、有限精度で実装された生成法が生成するランダムビット列の初期値解（式 (3.135) ~ (3.138)）は、当該系列が無限精度で実装された生成法が生成するランダムビット列だと考えたときに、無限精度の場合の推測法から得られる初期値解（式 (3.20) ~ (3.23)）（最終値 x_n の存在範囲の必要条件から得られる初期値解）からごく僅かに離れた場所に存在し、最も離れている場合でも、有限精度演算で表現できる最小の値 ε の高々 1.5 倍程度の距離（ $1.5 < a < 2$ として概算）であることが判る。

3.6.5 観測ビット列の長さが十分に長い場合（写像の反復回数 n が大きい場合）について

写像の反復回数 n （観測ビット列の長さ $n+1$ ）が、以下で示される式 (3.145) を満たす程度に大きい場合は、式 (3.135) ~ (3.138) で示される初期値解の値の幅 ($1/(2a^n)$) は、有限精度演算で表現できる最小の値 ε よりも小さくなる。

$$\frac{1}{2a^n} < \varepsilon \Leftrightarrow n > \log_a \frac{1}{2\varepsilon} \quad (3.145)$$

図 3.8 パラメータ a と $\beta = a/(2(1-a))$ の関係

この場合の初期値解（式 (3.135) ~ (3.138)）は以下のように整理される。

$$\hat{x}_0 = \frac{1/2 - \sum_{i=1}^n p_i a^i}{q a^n} + \beta \varepsilon, \quad \left(-\frac{a}{2(a-1)} < \beta < \frac{a}{2(a-1)} \right) \quad (3.146)$$

パラメータを概ね $1.5 < a < 2$ としたときの β は、概ね、

$$\beta = \{-2, -1, 0, 1, 2\} \quad (3.147)$$

と計算される。すなわちこのことは、観測ビット列長が式 (3.145) で示される以上の長さがあれば、当該系列を生成する初期値を僅か 5 点に絞り込むことができるということを意味している。

3.6.6 本節のまとめ

有限精度で実装されたテント型写像を反復する度に最上位ビットを抽出して得られた擬似ランダムビット列が与えられたときに、当該系列を生成し得る初期値範囲の推測法を示した。

3 章において、理想的な環境（演算誤差を考慮しない無限精度）で実装されたテント型写像を反復する度に最上位ビットを抽出して得られた擬似ランダムビット列に対する初期値推測法を示したが、テント型写像は初期条件に鋭敏な性質を持つので、演算誤差を考慮した場合と、考慮しない場合とでは、互いに全く異なる系列となることから、無限精度で実装された生成法から生成される系列に対する初期値解は、有限精度で実装された生成法から生成される系列に対する適切な初期値解になり得ないことが容易に予想された。

本推測法は、演算誤差（最近接丸めによる誤差）を考慮して定義されたテント型写像 $g_a(x)$ の n 回反復の合成写像関数形 $x_n = g_a^n(x_0)$ が観測ビット列を用いて一意に決定できることを利用して、最終値 x_n の存在範囲の条件を用いて初期値範囲を限定するものである。そして、有限精度で実装された生成法により生成される擬似ランダムビット列に対する初期値解は、当該系列が無限精度で実装された生成法により生成される擬似ランダムビット列だと仮定したときに、無限精度の場合の推測法から得られる初期値解からごく僅かに離れた場所に存在することを示した。生成系は、傾き $1.5 < a < 2$ が現実的に利用されるものと仮定すると、無限精度の場合の解と有限精度の場合の解が最も離れている場合でも、有限精度演算で表現できる最小の値 ε の高々 1.5 倍程度の距離であることを示した。

3.7 パラメータ推測法とは

本論文における解析対象である、定義 3.2.1 で示される生成系 $S_a(x_0, n)$ においては、初期値 x_0 とパラメータ a がシード（鍵）と直接的な関係をもつ値である。前節までは、パラメータを既知としたときに、生成系 $S_a(x_0, n)$ において観測ビット列を生成し得る初期値範囲の推測法について述べたが、逆に、初期値を既知としたときには、生成系 $S_a(x_0, n)$ において観測ビット列を生成し得るパラメータ範囲の推測が可能である。

定義 3.7.1 (本論文で扱うパラメータ推測法の定義(広義)) x_0 を初期値として、テント写像、ロジスティック写像、平方写像等の 1 次元非線形写像の n 回反復過程 $x_{i+1} = f(x_i)$ ($0 \leq i < n$) で得られる $n + 1$ 個の値 $\{x_0, x_1, \dots, x_n\}$ を考える。この系列 $\{x_i\}$ をもとに、ある規則に従い生成された m ビットの 2 値化系列 $\{b_0, b_1, \dots, b_{m-1}\}$ が与えられたとする。このとき、2 値化系列 $\{b_i\}$ の生成規則、および初期値 x_0 を既知として（未知でもよい）、当該擬似ランダムビット列を生成し得るパラメータ（テント写像の場合は a 、ロジスティック写像の場合は b 、平方写像の場合は c ）の範囲を推測する手法のことをいう^{*15}。

パラメータの推測の場合も、初期値推測の場合と基本的な部分は同じである。例えば、観測ビット列から n 回写像後の最終値 $x_n = f_a^n(x_0)$ の多項式関数形を決定し、状態遷移図で最終値 x_n の厳密な範囲を求める作業は全く同じである。そして、最上位ビット抽出系列の場合、任意桁目のビット（上位 t ビット桁目 / 下位側ビット）を抽出した場合、生成法が有限精度で実装された場合等において、それぞれ考えなければならないことも同じである。従って、ここでは、最上位ビット抽出系列の場合についてのみ触れておく。

3.8 テント写像の最上位ビット抽出系列に対するパラメータ推測法

[23]

定義 3.8.1 (定義 3.2.1 の生成法から生成された擬似ランダムビット列に対するパラメータ推測法) 本節で述べる初期値推測法とは、定義 3.2.1 で示される生成法 $S_a(x_0, n)$ により生成された計 $n + 1$ ビットの擬似ランダムビット列 $\{b_i\}_{i=0}^n$ が与えられたときに、初期値 x_0 を既知として、当該系列 $\{b_i\}_{i=0}^n$ を生成し得るパラメータ a の範囲を推測する手法のことを言う。

以前に述べた定義 3.2.1 で示される生成法 $S_a(x_0, n)$ から得られた計 $n + 1$ ビットの擬似ランダムビット列 $\{b_i\}_{i=0}^n$ が与えられたとき、定理 3.2.3、および式 (3.7) ~ 式 (3.10) によって、観測ビット列から $x_n = f_a^n(x_0)$ の関数形が決定できる。ここでは、初期値 x_0 を既知として、パラメータ a を未知としているので、最終値 $x_n = f_a^n(x_0)$ は、未知変数 a の最大次数が n となる多項式関数となる。尚、パラメータ推測においても、初期値推測と同様で、最終値 x_n の厳密な存在範囲を知る必要があるが、これは、3.4 節で示される内容および状態遷移図 3.4 を用いて同様に求める。そして、最終値 x_n の存

^{*15} 広義の定義では、系列 $\{x_i\}$ から 2 値化系列 $\{b_i\}$ の生成規則は任意とする。ただし、生成規則は既知とする。尚、本論文においては、主として、2 値化系列の生成規則として第 i 回目の写像ごとに x_i の最上位ビットまたは上位から所定桁目のビットを抽出して、計 $n + 1$ ビットのランダムビット列 $\{b_i\}$ を生成することを考える。これを狭義の定義とする。

在範囲の条件を用いて, $x_{n\inf} < x_n (= f_a^n(x_0)) < x_{n\sup}$ を a について解くことによって求められる.

例 3.8.2 パラメータ $a = 503/256 (= 1.96484375)$, 初期値 $x_0 = 0.4$, 写像の反復回数 $n = 7$ とする. 定義 3.2.1 で示される生成系によって生成された計 $n + 1 = 8$ ビットの擬似ランダムビット列 $S_a(x_0, n) = \{b_i\}_{i=0}^n = \{0, 1, 0, 1, 0, 1, 1, 1\}$ が与えられたする. 定理 3.2.3 より, $f_a^n(x_0) = a - a^2 + a^4 - a^6 + 0.4a^7$ を得る. 状態遷移図より $x_n \in B = [1/2, a/2]$ が判明する. $1/2 \leq f_a^n(x_0) \leq a/2$ として a を求めると, $1.949058314354192 \leq a \leq 1.9866871050246235$ を得る(図 3.8 参照).

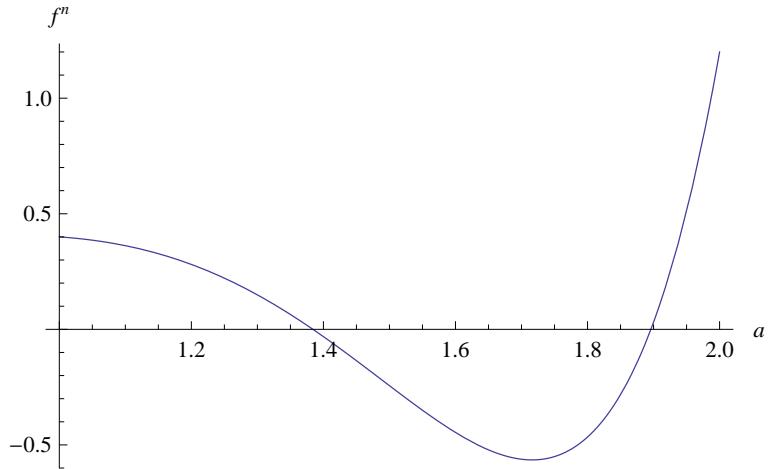


図 3.9 $f_a^n(x_0)$

3.9 Wu らのパラメータの推測法 [22]

本論文の前節までに扱った内容は, パラメータが既知の下での初期値推測法と, 初期値が既知の下でのパラメータ推測法であった. また, 最上位ビット抽出系列(小数点以下(2進小数点)の最上位ビット)に対しては, 初期値またはパラメータを一意的かつ厳密に求めることができるものであった. 一方で, Wu らはロジスティック写像(式(2.2))の最上位ビット抽出系列とグレイコード[31]の関係を利用したパラメータの推測法を示した[22]. 尚, 当推測法は, 初期値が未知の下でのパラメータの推測法であるため, 当推測法により一意的にパラメータを推測できるのであれば非常に効果的な推測法といえる. 本節では Wu らのパラメータ推測法を紹介する.

グレイコードについては付録 B.2 節に示した. グレイコードからバイナリコードへの変換 τ は式(B.2), および, バイナリコードからグレイコードへの変換 τ^{-1} は式(B.1)に示した. Wu らのパラメータ推測法は, Alvarez ら[29], Cisick[30]によって示される定理(付録 B.3 節)を利用する. これをテント写像の場合について示したものを作成 B.5 節の定理 B.5.2, 定理 B.5.3, 定理 B.5.4 に示した. 推測法の定義は, 初期値 x_0 を未知とする以外は定義 3.8.1 と同じである.

推測法 3.9.1 (Wu らのパラメータ推測法) Wu らのパラメータ推測法は, 最上位ビット抽出系列とグレイコードの関係(定理 B.5.2 ~ 定理 B.5.4)以外に, テント写像から得られた $\{x_i\}$ 系列が, 工

ルゴード的な性質^{*16} を有することが前提となる。具体的には以下の手順によって求める。

1. 定理 B.5.2～定理 B.5.4に基づいて、あらかじめ、パラメータ a と a におけるグレイコードのオーダーの最大値 $G(S_a(a/2, n))$ の関係（図 B.6）を得ておく。
2. 定義 3.2.1 に従い生成された計 $n+1$ ビットの擬似ランダムビット列 $S_a(x_0, n) = \mathbf{b}$ が与えられたとする。 $1 \leq i < n$ について、 \mathbf{b} の左 i ビットシフト系列に対するグレイコードのオーダー $G_i = G(L^i(\mathbf{b}))$ ($G_1 \sim G_{n-1}$) を算出する。
3. G_i ($1 \leq i < n$) の中から最大値を選び G_{max} とする。図 B.6 より G_{max} に対応する a を選びこれを推測値とする。

上記の推測法 3.9.1 について補足する。定理 B.5.2, 定理 B.5.3 より、パラメータ a のときのグレイコードのオーダーの最大値は、初期値を $a/2$ としたときに S_a によって生成される系列から得られることが判る。テント写像の反復によって得られる系列がエルゴード的な性質^{*16} を有するならば、任意の初期値 $x_0 \in (0, 1)$ を出発した軌道 $\{f_a^t(x_0)\}$ は、いずれ $x = a/2$ (或は $x = a/2$ の近傍) を通過するはずである。ここで $t (1 \leq t < n)$ において $x = a/2$ (或は $x = a/2$ に最も近い値) を通過したとする。 $x_t = f_a^t(x_0)$ を新たな初期値として得られる系列 $S_a(x_t, n-t)$ とは、観測ビット列 $\mathbf{b} (= S_a(x_0, n))$ を t 回左シフトした系列 $L^t(\mathbf{b})$ に他ならない。つまり、 $G_i = G(L^i(\mathbf{b}))$, ($1 \leq i < n$) (すなわち $G_1 \sim G_{n-1}$) を算出したならば、その最大値 G_{max} は、定理 B.5.3 より、上記の x_t において得られた値のはずである。その後、定理 B.5.4 の関係を示す図 B.6 より、 G_{max} に対応する a を求めこれを推測値とする。

従って、Wu らのパラメータ推測法は、初期値 x_0 を出発した軌道 $\{f_a^t(x_0)\}$ が写像の値域の最大値である $x = a/2$ (或は $x = a/2$ に限りなく近い値) を通過しない限り、正確なパラメータ値を得ることができない。これには、十分に長い長さの観測ビット列が与えられている必要があるので、本論文で示した推測法（パラメータが既知の下での初期値推測法、初期値が既知の下でのパラメータ推測法）と比較して、真のパラメータを得るまでの必要な情報量と計算量が大きいと推測される。文献 [22] には、当推測法の性能についての詳細が触れられていないため、3.10.5 節にて、Wu らの推測法の効果／性能を見積もることにする。

^{*16} ある初期値を出発した軌道が、写像の値域上の任意の点の近傍を非周期的に何回も通過すること。並びにそのような初期値が写像の定義域上の至る箇所に存在すること

3.10 本章で示した推測法(3.3節~3.9節)の性能および考察

3.10.1 最上位ビットを抽出した系列に対する初期値推測法(3.3節,3.4節)により推測可能な範囲

3.3節, 3.4節では, 定義3.2.1で示される擬似ランダムビット列生成法 S_a が無限精度で実装されているとして(演算精度を考慮しない), 当該生成法から得られる系列, すなわち, パラメータ $a = 2$, および, $1 < a < 2$ のテント写像 f_a を写像する度に $(x_{i+1} = f_a(x_i), i \geq 0)$, x_i の最上位ビット(2進小数点以下の上位1ビット桁目)を抽出した系列 $s_a(x_0, n) = \{b_i\}_{i=0}^n = \mathbf{b}$ が与えられたときに, パラメータ a が既知の下で当該系列 \mathbf{b} を生成し得る初期値範囲を求める手法を示した.

結論からすると, 最上位ビットを抽出した場合であれば, 如何なるパラメータ($1 < a \leq 2$)であっても, 初期値範囲を厳密かつ一意的に得ることができる. その効率/性能は, 計 $n + 1$ ビットのビット列 $\{b_i\}_{i=0}^n$ が与えられたときに, 式(3.67)~式(3.70), 或は, 式(3.71)~式(3.74)より, 写像の定義域 $I_a = [0, 1]$ に対して, I_a 内の約 $1/(2a^n)$ の幅の区間に絞り込むことができると概算される. つまり, 全探索の場合は, 区間 $I_a = [0, 1]$ 上の全ての点を調べ上げる必要があるが, 本推測法を用いることによって, 探索量を約 $1/(2a^n)$ 以下に抑えることができる. 従って, 本推測法は暗号学的な視点において効率的な推測法/攻撃法ということができる^{*17}.

推測範囲について補足する. 観測ビット列 $\{b_i\}_{i=0}^n = \mathbf{b}$ が与えられたときに, 当推測法により得られる初期値範囲を $Y_{\mathbf{b}}$ とする. ここで, 0から n ビット目までが \mathbf{b} と等しく, $n + 1$ ビット目が 0となる系列 \mathbf{b}' と, 0から n ビット目までが \mathbf{b} と等しく, $n + 1$ ビット目が 1となる系列を \mathbf{b}'' を考える.

$$\begin{aligned}\mathbf{b} &= \{b_0, \dots, b_n\} \\ \mathbf{b}' &= \{b'_0, \dots, b'_n, 0\}, \quad b'_i = b_i \ (0 \leq i \leq n) \\ \mathbf{b}'' &= \{b''_0, \dots, b''_n, 1\}, \quad b''_i = b_i \ (0 \leq i \leq n)\end{aligned}$$

このとき, 当推測法による \mathbf{b}' に対する初期値範囲 $Y_{\mathbf{b}'}$, ならびに, 当推測法による \mathbf{b}'' に対する初期値範囲 $Y_{\mathbf{b}''}$ は, $Y_{\mathbf{b}} = Y_{\mathbf{b}'} \cup Y_{\mathbf{b}''}$ という関係にある. 尚, $1 < a < 2$ の場合は, $Y_{\mathbf{b}'} = \emptyset$ または $Y_{\mathbf{b}'} = \phi$ の場合がある. $Y_{\mathbf{b}'} \subseteq Y_{\mathbf{b}}$, $Y_{\mathbf{b}''} \subseteq Y_{\mathbf{b}}$ である.

さらに補足すると, $\{b_i\}_{i=0}^n$ が既知のもとでの, 次のビット b_{n+1} が 0 または 1 である条件付き確率(事後確率) $Pr\{b_{n+1} = 0 | b_n\}, Pr\{b_{n+1} = 1 | b_n\}, b_n \in \{0, 1\}$ は, 系列 $\{b_i\}_{i=0}^n$ 中に, 理論上最大となる 0 の連を含まない場合(3.4.5節を参照)には, 式(3.67)~式(3.70), 或は, 式(3.71)~式(3.74)より,

$$Pr\{b_{n+1} = 0 | b_n\} = \frac{a-1}{a}, \quad b_n \in \{0, 1\} \quad (3.148)$$

$$Pr\{b_{n+1} = 1 | b_n\} = \frac{1}{a}, \quad b_n \in \{0, 1\} \quad (3.149)$$

と計算される. 一方で, 理論上最大となる 0 の連を含む場合は, この値の限りではない(ケースバイケース).

^{*17} 暗号学的視点では, 一般的に, 暗号鍵を特定するにあたり, 全探索に対して 1 ビットでも計算量を少なくできるのであれば攻撃に成功したとする.

3.10.2 任意桁目のビット（上位 k 桁目のビット / 下位側のビット）を抽出した系列に対する初期値推測法（3.5 節）により推測可能な範囲

3.5 節では、 x_i の上位 k 桁目のビット（2進小数点数の小数点以下の上位 k 桁目のビット / 下位側のビット）を抽出した場合で、かつ、生成法 $S_{a,k}(x_0, n)$ は無限精度（演算精度を考慮しない）で実装された場合を仮定した場合における初期値推測法を示した。

（3.5 節では上位 t 桁目と表現したが、説明の都合上、以降では上位 k 桁目と表現する。）

最上位ビット抽出 ($k = 1$) の場合は観測ビット列から一意的に初期値範囲を得ることができる点に対して、任意桁目のビット（上位 k 桁目のビット / 下位側のビット）を抽出した場合は、最上位ビット抽出の場合での式 (3.20)～式 (3.23) に相応する推測式（不等式）が複数個生じる。また、全ての推測式から得られる初期値（初期値の候補）が、実際に観測ビット列を生成し得る初期値を含むとは限らないため、3.5 節で示した全ての $\{z_i\}$ 軌道（全ての推測式）について初期値範囲を得る必要があり、推測のための計算量が増えるばかりか、真の初期値が含まれる範囲を一意的に得ることはできない（例 3.5.6 を参照）。

つまり、任意のビット桁（上位 k 桁目のビット / 下位側のビット）を抽出した場合に、3.5 節で示した推測法から推測可能なことは、観測ビット列を生成し得る初期値が存在する可能性がある場所 / 候補を得ることまでであり、真の初期値が含まれる範囲を厳密かつ一意的に得ることはできない。従って、観測ビット列を生成し得る初期値が存在する可能性がある場所 / 候補を絞り込んだ後は、各候補が示す初期値候補の範囲の全てを探索する必要がある。

ここでは、推測式の候補の数の期待値を試算する。理由は、推測式の候補の数が本生成系に対する推測に必要な計算量的と関係するためである。

x_i から上位 k ビット桁目が抽出される場合を考えると、まずははじめに、3.5 節で示した z_0 の候補が 2^{k-1} 個現れる。その後は、それぞれの z_0 候補を出発する $\{z_i\}$ 軌道に分岐が生じる場合がある。

分岐が生じない場合、すなわち 3.5.2 節で示す (a),(b) のケース（Type-1）が生じる確率 P_1 、および、分岐が生じる可能性がある場合、すなわち 3.5.2 節で示す (c),(d) のケース（Type-2）が生じる確率 P_2 は、テント写像の特性より、

$$\begin{cases} P_1 &= 2 - a \\ P_2 &= a - 1 \end{cases} \quad (3.150)$$

と算出される。

分岐が生じる可能性がある場合で、実際に分岐が生じるか否かは観測ビット列に依存する。ここでは、観測ビットは 0 と 1 がランダムかつほぼ等頻度に現れることを前提とすると、分岐が生じる確率と、分岐が生じない確率はそれぞれ $1/2$ なので、分岐が生じる可能性がある場合において分岐が生じない確率（条件付き確率）は $P_{2,1}$ と、分岐が生じる可能性がある場合において分岐が生じる確率（条件付き確率） $P_{2,2}$ は、

$$\begin{cases} P_{2,1} = (a - 1)/2 \\ P_{2,2} = (a - 1)/2 \end{cases} \quad (3.151)$$

である。従って、1 つの z_0 候補あたり、観測ビット 1 ビットあたりに生じる $\{z_i\}$ 軌道の数の期待

値は、

$$P_1 \times 1 + P_{2,1} \times 1 + P_{2,2} \times 2 = (2-a) + \frac{a-1}{2} \times 3 = \frac{a+1}{2} \quad (3.152)$$

である^{*18}。またこの値は、観測ビットが1ビット増えたときの軌道の数の増量（倍率）を意味するので、観測ビット列長が n の場合は、

$$\left(\frac{a+1}{2}\right)^n \quad (3.153)$$

と計算される。上位 k 桁目のビットを抽出する場合は z_0 候補は 2^{k-1} 個あることから、上位 k 桁目のビット抽出、観測ビット列長 n における $\{z_i\}$ 軌道の数の期待値、すなわち、推測式の数の期待値 $E\{M\}$ は、

$$E\{M\} = 2^{k-1} \left(\frac{a+1}{2}\right)^n \quad (3.154)$$

と計算される。

式(3.154)は、前後のビット関係のみを考えた場合であるため、 j ($j > 1$)回写像の関係や、0の連の最大値よりも長い10の連を含むパターンを省く等を考慮することによって、実際に評価すべき推測式の数は式(3.154)よりも少なくすることができる。ただしの場合でも、推測アルゴリズム中における反復回数は、式(3.154)で示される量となる。

3.10.3 有限精度で実装された生成法から得られる系列に対する初期値推測法(3.6節)により推測可能な範囲

3.6節では、生成法が有限精度で実装された場合に得られる擬似ランダムビット列に対する初期値推測法を示した。有限精度を考慮する理由は、テント写像は初期条件に鋭敏な性質を持つため、生成法が無限精度(演算精度を考慮しない場合)で実装された場合に得られる系列と、有限精度で実装された場合に得られる系列とでは、ある時点以降に全く異なる系列となるためであり、すなわち、無限精度(演算精度を考慮しない場合)で実装された生成法から得られる系列に対する初期値推測法(3.3節、3.4節、3.5節)のままで、有限精度で実装された生成法から得られる系列に対しての有効な初期値解を与えることなく、推測が不可能となる。また、推測の困難性が予測された。

しかし、3.6節で示した内容より、最上位ビット抽出の場合であれば、有限精度で実装された生成法から得られる系列に対する初期値解は、当該系列が無限精度(演算精度を考慮しない場合)で実装された生成法から生成されたと仮定したときに、無限精度の場合の推測法が示す初期値範囲から僅かに離れたところに存在することが判明した。つまり、推測は困難でないことが判った。

特に観測ビット列 n が式(3.145)で示される程度に十分に長い場合は($n > \log_a \frac{1}{2\varepsilon}$)、式(3.135)～式(3.138)で示される解の範囲は、与えられた演算精度 t で表現できる値 $\varepsilon = 1/2^t$ 以下となるので、初期値の候補は多くとも5点ほどに絞れることができた(式(3.146)、式(3.147))。このために最低限必要な系列長 n (式(3.145))を改めて $n_0(a, t)$ として整理すると、

$$n_0(a, t) = \left\lceil \log_a \left(\frac{1}{2\varepsilon}\right) \right\rceil = \log_a \lceil 2^{t-1} \rceil \quad (3.155)$$

^{*18} もともと1つであった軌道が、観測ビットが1ビット増えたときに、期待値にして $(a+1)/2$ に増えるということ

である。式(3.155)は、倍精度浮動小数点演算($t = 52, \varepsilon = 1/2^{52}$)の場合に図3.10、单精度浮動小数点演算($t = 23, \varepsilon = 1/2^{23}$)の場合に図3.11、に示す関係にある。

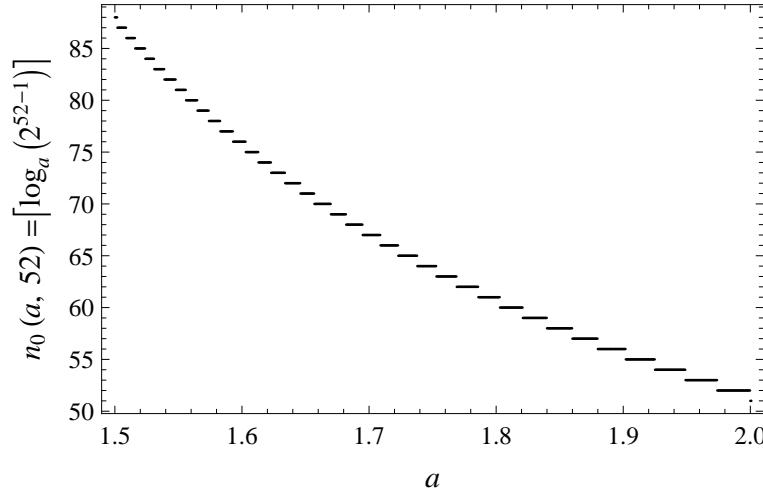


図3.10 倍精度浮動小数点演算($t = 52$)において、初期値を数点に絞り込むために最低限必要な系列長 $n_0(a, 52)$

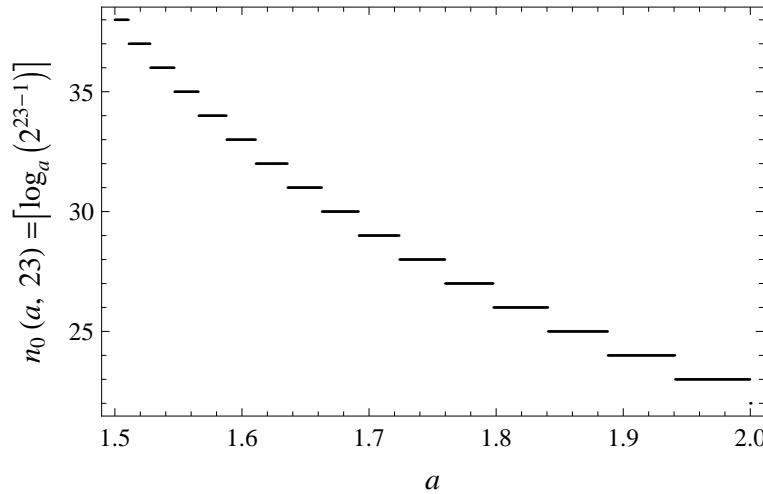


図3.11 单精度浮動小数点演算($t = 23$)において、初期値を数点に絞り込むために最低限必要な系列長 $n_0(a, 23)$

すなわち、最上位ビット抽出の場合では、有限精度で実装された生成法から得られた擬似ランダムビット列の長さが $n_0(a, t)$ (式(3.155)) 以上であれば、式(3.146), 式(3.147)より得た5点の推測値の候補のうち1点が真の初期値であり、その真の初期値は、次のビット b_{n+1} 以降に生じるビット列を含めた系列 $\{b_i\}_{i=0}^m$, ($m > n$)に対する初期値をも兼ねている。つまり、無限精度の場合は次のビットの推測は確率的であったが、有限精度の場合は確定的となる（擬似ランダムビット列の長さが $n_0(a, t)$ 以上の場合）^{*19}。言い換えると、観測ビット列長が $n_0(a, t)$ 以上の長さを有していたとして

^{*19} 有限精度の場合の解の集合は所詮は有限集合であるため、式(3.135)～式(3.138)で示される解の範囲が ε 以下となる

も、当該系列を生成し得る初期値を、これ以上（5点に絞り込んだ以上）に絞り込むことはできないことを意味している。また、 $n_0(a, t)$ よりも長い系列が与えられていたとしても、その系列の初期の $n_0(a, t)$ ビットの部分系列のみで初期値推測は達成できることを意味している。このことは、有限精度の場合の初期値解を得るために計算量の上限を考える上で重要な意味をもつ。

上述（初期値解は多くとも5点に絞れること）は、最上位ビット抽出系列の場合について述べたものであるが、下位側のビットが抽出された場合（上位 k 衍目のビット抽出）は、前節（3.10.2節）で述べたように推測式の数が増えることは免れ得ない。ただし、上述のように、観測ビット列の上限を $n_0(a, t)$ に抑えることができる。そして、上位 k 衍目のビット抽出における、有限精度の場合の探索量 M の期待値 $E\{M\}$ は、式(3.154)、式(3.155)、および1つの推測式あたり5点に絞り込めることに注意すると、

$$E\{M\} = 5 \cdot 2^{k-1} \left(\frac{a+1}{2}\right)^{n_0(a, t)} \quad (3.156)$$

として与えられる。尚、 $k \leq t$ の関係にあることから、 $k = t$ のときに式(3.156)は最大（最下位ビット抽出のときに探索量 M が最大）となる。

式(3.156)について、倍精度浮動小数点演算 ($t = 52$)、最下位ビット（上位 $k = 52$ ビット目）抽出の場合の関係を図3.12に示す。倍精度浮動小数点演算 ($t = 52$)、中位衍ビット（上位 $k = 26$ ビット目）抽出の場合の関係を図3.13に示す。単精度浮動小数点演算 ($t = 23$)、最下位ビット（上位 $k = 23$ ビット目）抽出の場合の関係を図3.14に示す。

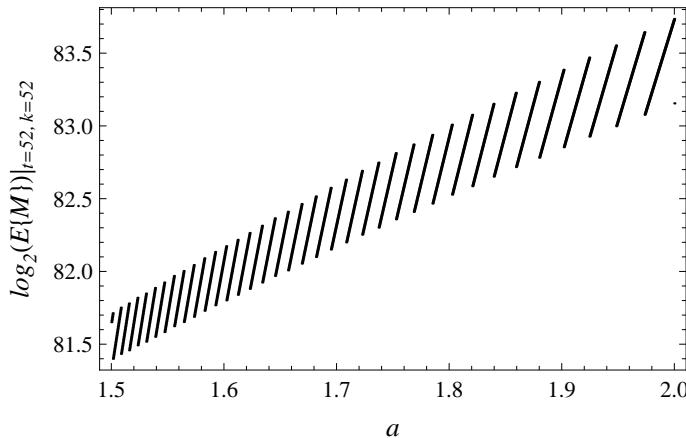


図3.12 倍精度浮動小数点演算 ($t = 52$)、最下位ビット（上位 $k = 52$ ビット目）抽出の場合に、初期値の特定に必要な探索量の期待値 $E\{M\}$ （対数表記）

これより、倍精度浮動小数点演算 ($t = 52$) で実装した場合で、最下位ビット抽出 ($k = 52$) の場合は、3.6節で示した推測法により初期値を1点に絞り込むために必要な探索量は、図3.12（式(3.156)）より、約80ビット以上ということになる。この見積もり値は、理論上最大の0の連を含むパターン等を省いていないため、実際にはこの値よりも少ない量に抑えられる。本節では、これ以上の考察は避けるが、倍精度浮動小数点演算 ($t = 52$) の場合は、初期値 x_0 の候補数は $2^{52} - 1$ なので、

場合は ($n > \log_a \frac{1}{2\varepsilon}$ 式(3.145))、真の解は1点に絞り込まれていることを意味している

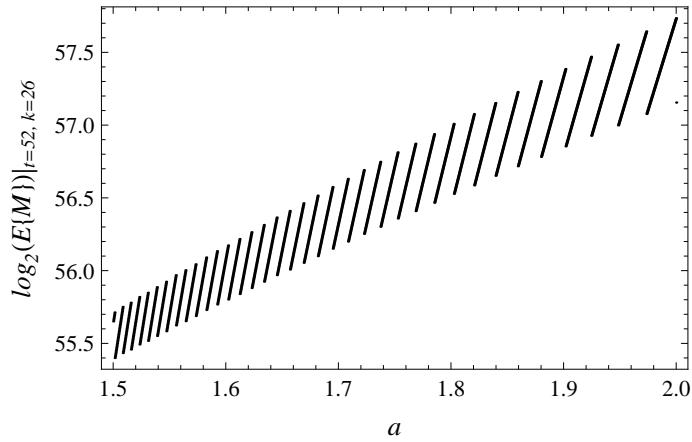


図 3.13 倍精度 浮動小数点演算 ($t = 52$) , 中位桁ビット (上位 $k = 26$ ビット目) 抽出の場合に , 初期値の特定に必要な探索量の期待値 $E\{M\}$ (対数表記)

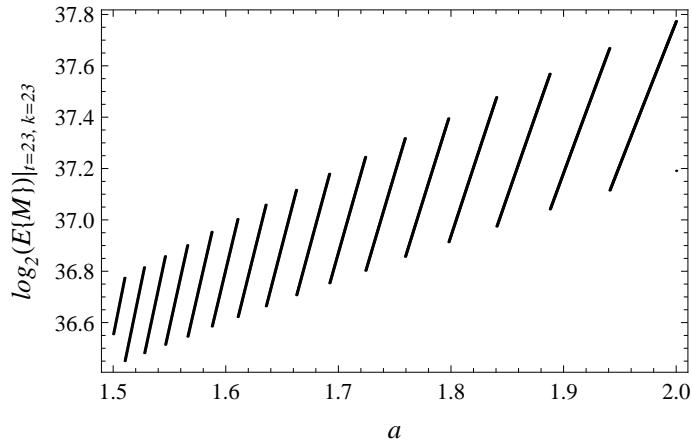


図 3.14 単精度 浮動小数点演算 ($t = 23$) , 最下位ビット (上位 $k = 23$ ビット目) 抽出の場合に , 初期値の特定に必要な探索量の期待値 $E\{M\}$ (対数表記)

初期値の全探索量（ブルトフォースアタック）が 52 ビットであることを考慮すると，本推測法による初期値の探索は効果的ではないといえる。

3.10.4 有限精度の場合（最上位ビット抽出）でも初期値候補を数点に絞り込むことができるこの理由に関する考察

テント写像が初期条件に鋭敏な性質を有する関係で，有限精度で実装された場合に得られる系列は，ある時点以降に全く異なる系列となることから，この場合の初期値推測は推測性が予測された。しかし，3.6 節により，最上位ビット抽出の場合であれば，無限精度の場合の推測法が示す初期値範囲から僅かに離れたところに存在することが判明し，推測は困難でないことが判明した。この理由について考察する。

有限精度の場合の初期値解は，式 (3.135) ~ 式 (3.138) に示される範囲である。ここで，ある系列

$\{b_i\}_{i=0}^n \stackrel{\text{def}}{=} \mathbf{b}$ と, \mathbf{b} の先頭ビット(0ビット目)から $j-1$ ビット目($1 \leq j \leq n$)までが等しく, j ビット目が異なる系列 $\{b'_i\}_{i=0}^n \stackrel{\text{def}}{=} \mathbf{b}'$ ($b_i = b'_i$ ($0 \leq i < j$), $b_j \neq b'_j$) を考える。そして, 系列 \mathbf{b} についての初期値の推測値 $x_{0,\mathbf{b}}$ と, 系列 \mathbf{b}' についての初期値の推測値 $x_{0,\mathbf{b}'}$ の差 $\Delta (= |x_{0,\mathbf{b}} - x_{0,\mathbf{b}'}|)$ を考えたとき, Δ と j は以下の関係にあることが判る。

$$\begin{aligned} j = 1 \text{ のとき } \Delta &= \frac{1}{2a} \\ j = 2 \text{ のとき } \Delta &= \frac{1}{2a^2} \\ j = m \text{ のとき } \Delta &= \frac{1}{2a^m} \end{aligned}$$

すなわち, 系列 \mathbf{b} と系列 \mathbf{b}' の差が, 推測値の差として与える影響が一番大きいのが, 兩系列が第1ビット目($j=1$)で初めて差が生じる場合であり, $j=2, 3, \dots$ の順で小さくなることが判る。そして, 第 j ビット目ではじめて差が生じるような場合は, 推測値の差は $1/(2a^j)$ であることが判る。すなわち, 兩系列が十分大きい m ビット目ではじめて差が出るような関係にある場合は, それぞれの系列ごとに得た初期値の推測値どうしの差は僅かである。

従って, 無限精度で実装された(演算精度を考慮しない)生成法から得られた系列 \mathbf{b} と, 有限精度で実装された生成法から得られた系列 \mathbf{b}' が, 互いに初期の系列は等しく, ある時点以降で差が生じる(先頭ビットから数ビット目までは等しい)のであれば, 推測値の差に大きな影響を与える先頭ビットから数ビット目までの部分系列は等しいので, この関係で, 推測値の差は大きなものとならないと推測される。

そこで, 兩系列が, 初期のどの程度の間まで等しいか(先頭ビットから何ビット目までが等しいか)について試算する。無限精度で実装された(演算精度を考慮しない)場合のテント写像の n 回写像後の値 $f_a^n(x_0)$ と, 有限精度モデルによる n 回写像後の値 $g_a^n(x_0)$ との差は, 式(3.7), 式(3.134)より,

$$g_a^n(x_0) - f_a^n(x_0) = D \quad (3.157)$$

である。 D は, 式(3.144)より.

$$|D| < \beta \varepsilon a^n = \frac{a^{n+1}}{2(a-1)} \varepsilon, \quad (\because \beta = \frac{a}{2(a-1)}) \quad (3.158)$$

の関係にある。また, $f_a^n(x_0)$ の最上位ビットと, $g_a^n(x_0)$ の最上位ビットに, 確実に差が生じるのは,

$$|D| = |g_a^n(x_0) - f_a^n(x_0)| > 1/2 \quad (3.159)$$

となるときであり, 式(3.158), 式(3.159)より,

$$\frac{a^{n+1}}{2(a-1)} \varepsilon > 1/2 \quad (3.160)$$

の関係を得る。このような n は, 倍精度浮動小数点演算($t=52, \varepsilon=1/2^{52}$)のときは, 具体的なパラメータ a に対して以下である。

$$\begin{aligned} a = 1.99 \text{ のとき } n &= 51.3 \\ a = 1.8 \text{ のとき } n &= 59.9 \\ a = 1.5 \text{ のとき } n &= 86.2 \end{aligned} \quad (3.161)$$

従って、無限精度の場合の最上位ビット抽出系列と、有限精度の場合の最上位ビットを抽出系列は、遅くとも上の式に示される $[n]$ ビット目までに差が生じる。言い換えると、両系列は、最大でも $[n]$ ビット目までが等しいといえる。このことからも、有限精度の場合の解は、無限精度の場合の解の近くに存在することが判る。

3.10.5 Wu らのパラメータの推測法（3.9 節）の性能 / 推測可能な範囲 [28]

Wu らによって示されたパラメータ推測法は、特に生成系の演算精度を考慮したものではないため、現実的に有限精度で実装された（コンピュータに実装された）生成法から得られる系列に対して、どのような効果があるかについての定量的な面が示されていない。本節の以降では、はじめに有限精度で実装されたテント写像やロジスティック写像の性質（最近の研究報告よりまとめたもの）を示し、次いで、この性質を考慮した上で、IEEE 754 に準じた倍精度浮動小数点演算で実装された定義 3.2.1 の生成法から得られる系列に対する当推測法の効果についての考察を述べる。

パラメータ推定の探索量とそれに必要な観測ビット列長について

本節では、Wu らのパラメータ推測法によって、真のパラメータを 1 点に絞り込むために要する探索量 M と観測ビットの長さ n との関係について示す。Wu らの推測法では、グレイコードのオーダーの最大値が得られる $x = a/2$ が周期軌道上にある場合には、当推測法によって真のパラメータを得ることができるが、2.4.1 節で示した有限精度で実装されたテント写像の性質（性質 2.4.1～性質 2.4.4 および図 2.16）を考慮すると、周期軌道は複数個あるため $x = a/2$ を含まない場合があること、さらに $x = a/2$ が周期軌道上にある可能性は極めて低いことが判る。すなわち、Wu らの推測法によって真のパラメータを一意的に得ることはほぼ期待できない。

そこで、当推測法（推測法 3.9.1）により得られる推測値とは、ある $i (1 \leq i < n)$ において、 $x_i = f_a^i(x_0)$ が $x = a/2$ の近傍 $x = a/2 - \delta_x$ を通過した際に得られたものとして考える。この誤差 δ_x がパラメータの推測誤差 δ_a として現れる。

はじめに、パラメータを 1 点に絞り込むまでに必要な探索量 M を固定したときに許されるパラメータの推測誤差 δ_a との関係を示し、次いで、パラメータの推測誤差 δ_a とグレイコードのオーダーの観測誤差 δ_G の関係を求める。次に、 δ_G と δ_x の関係を求め、最後に、初期値 x_0 を出発した軌道が、平均して何回目の写像後に区間 $[a/2 - \delta_x, a/2] \stackrel{\text{def}}{=} X$ を通過するか ($f_a^n(x_0) \in X$ となる最初の n) を数値実験によって求める。

パラメータの推測誤差 δ_a とパラメータを 1 点に絞り込むまでに必要な探索量 M の関係

δ_a を定めたときは、真のパラメータを推定するために残された探索量 M は、与えられた演算精度で表現し得る最小の値 ε を用いて

$$M = \delta_a / \varepsilon \quad (3.162)$$

と計算される。これと逆に探索量 M を固定した場合には以下の関係にある。

$$\delta_a = M\varepsilon \quad (3.163)$$

本稿では、生成法は IEEE 754 に準じた倍精度浮動小数点演算（仮数部の精度は 52 ビット）で実装されていることを前提とする。従って $\varepsilon = 2^{-52}$ として計算する。尚、以降では具体的に $M = 2^{30}$ の

場合（探索量を30ビット以内に納めること）を考えることにする。この場合の δ_a は式(3.163)より以下に示す値となる。

$$\delta_a = M\varepsilon = 2^{30} \times 2^{-52} = 2^{-22} \quad (3.164)$$

δ_x とグレイコードのオーダの誤差 δ_G の関係

パラメータの推測誤差 δ_a とグレイコードのオーダの観測誤差 δ_G は、図B.6の関係から見積もることができる。ただし、 δ_a と δ_G の関係は a の値によって変化するので、以降では、 $a = 1.9$ の場合を考えることにする。 $a = 1.9$ のときのグラフの傾き(Δ_G/Δ_a)は、その前後の点を用いて約0.353と計算される。これより、 $M = 2^{30}$ (探索量30ビット)の場合の δ_G は以下の値となる。

$$\delta_G = 0.353\delta_a = 0.353 \times 2^{-22} = 2^{-23.5} \quad (a = 1.9) \quad (3.165)$$

δ_x とグレイコードのオーダの誤差 δ_G の関係

式(B.3)の関係を考慮すると、グレイコードのオーダーで $\delta_G = 2^{-23}$ の誤差を得るということは、ある2つの系列を考えたときに、2つの系列の0~22ビット目までの計23ビットが一致していて、23ビット目以降が異なるような系列から得られることが判る。この関係は、 $x = a/2$ を出発した軌道から得られる最上ビット抽出系列と、 $x = a/2 - \delta_x$ を出発した軌道から得られる最上ビット抽出系列との関係に相当する。0~22ビット目までの系列 $\{b_0, b_1, \dots, b_{22}\}$ は、定義3.2.1の生成法から $S_a(a/2, 22)$ として求めることができる。そして、 δ_x は、当系列 $S_a(a/2, 22)$ を生成し得る x の区間を求めることによって得られる。この計算には、文献[26]で示される初期値推測法を利用することができます(途中計算省略、文献[26]を参照)。

$$\begin{aligned} [a/2 - \delta_x, a/2] &= [0.94999991101, 0.95] \stackrel{\text{def}}{=} X \\ \delta_x &= 0.0000000889 \end{aligned} \quad (3.166)$$

と算出される^{*20}。

軌道が区間 $[a/2 - \delta_x, a/2] = X$ を通過するまでに必要な写像回数(観測ビット列長) n の関係

前節までに判ったことは、 $M, \delta_a, \delta_G, \delta_x$ の対応関係と、パラメータの探索量を $M = 2^{30}$ (30ビット)に抑えるためには、軌道 $\{f_a^n(x_0)\}$ が、いずれ式(3.166)で示される狭い区間 X に入る必要があるということである($f_a^n(x_0) \in X$ となる n が存在すること)。本稿では、区間(0, 1)を等間隔に1,000分割した点を初期値 x_0 の候補として選び、それぞれの初期値の候補を出発した軌道が $x_n = f_a^n(x_0) \in X$ となる最小の n を数値計算より求め、その平均値 \bar{n} と、最大値 n_{max} を調べた。結果は、 $a = 1.9$ のときに、 $\bar{n} = 8.13 \times 10^6$ 、最大値 $n_{max} = 47,559,343$ となった。

同様のことを、 $M = 2^{40}, 2^{30}$ のとき、および、 $a = 1.9, 1.8, 1.7, 1.6$ のときに実施した数値計算結果を表3.2に示す。実験は $M = 2^{30}$ 未満となる場合についても試みたが、特に $M = 2^{28}$ 以下の場合は、この条件下で算出される区間 $[a/2 - \delta_x, a/2] = X$ を通過する軌道が存在しないか^{*21}、或は

^{*20} 文献[26]は、生成法が無限精度で実装された生成法に対する解を示したものであるが、有限精度で実装された場合の解について示した文献[27]を考慮すると、両者の差は僅かであることから(ε の数倍程度しか離れていない)、ここでは初期値解の誤差は無視する。

^{*21} 探索量 M を小さくするとこれに応じて δ_x も小さくなる(区間 X の幅は狭くなる)。

$n = 2^{36}$ （本実験での写像回数の最大値）までの写像回数以内に到達し得ないかの理由で，多くの初期値候補から解を得ることができなかった。

表 3.2 パラメータ推定に必要な探索量 M とその達成に必要な観測ビット列長の平均値 \bar{n} ，最大値 n_{max} （数値実験結果）

探索量 M	パラメータ a					観測ビット列長	
		δ_a	Δ_G/Δ_a (図 B.6 より算出)	δ_G	δ_x	\bar{n} (平均値)	n_{max} (最大値)
2^{40}	1.9	2^{-12}	0.353	$2^{-13.50}$	2.065×10^{-5}	3.490×10^4	272,753
	1.8	2^{-12}	0.06067	$2^{-16.04}$	1.074×10^{-5}	6.006×10^4	557,885
	1.7	2^{-12}	0.02265	$2^{-17.46}$	3.056×10^{-5}	1.557×10^4	136,679
	1.6	2^{-12}	0.00278	$2^{-20.49}$	1.911×10^{-5}	2.566×10^4	155,950
2^{30}	1.9	2^{-22}	0.353	$2^{-23.50}$	8.90×10^{-8}	8.125×10^6	47,559,343
	1.8	2^{-22}	0.06067	$2^{-26.04}$	8.07×10^{-8}	8.395×10^6	60,404,368
	1.7	2^{-22}	0.02265	$2^{-27.46}$	2.66×10^{-8}	1.498×10^7	66,583,387
	1.6	2^{-22}	0.00278	$2^{-30.49}$	1.20×10^{-7}	3.524×10^6	14,573,596

考 察

実験結果（表 3.2）の意味することは，生成法が倍精度浮動小数点演算で実装されていることを考えた場合において，Wu らのパラメータ推測法（初期値が未知のもとでパラメータを推測する手法）により真のパラメータを絞り込むことを考えた場合には，探索量を 2^{40} （40 ビット）以内に収めるためには約 $10^4 \sim 10^5$ の長さの擬似ランダムビット列が必要で，探索量を 2^{30} （30 ビット）以内に収めるためには約 $10^6 \sim 10^7$ の長さの擬似ランダムビット列が必要だということである。一方で，3 章で述べた，初期値を既知とした場合のパラメータの推測法 [23]，並びにパラメータ既知とした場合の初期値推測法 [26] と，有限精度で実装された生成法に対する初期値推測法から得られる解の範囲の性質 [27] を考慮によると，初期値を既知とした場合では演算精度と同程度の長さの観測ビット列が与えられたならば（本稿の場合では 100 ビットあれば十分），解は数点に絞り込むことが可能であることが判る（1 点に絞り込めないのは演算誤差の影響）。従って，初期値を未知としてパラメータを推測することの困難性を伺い知ることができる。

尚，今回の実験の限りでは，探索量を $M = 2^{30}$ （30 ビット）未満に収めることを考えた場合には， M の条件下で算出される区間 $[a/2 - \delta_x, a/2] = X$ に収まるような軌道が存在しないか，或は $n = 2^{36}$ （本実験での写像回数の最大値）までの写像回数以内に到達し得ないかの理由で，多くの初期値から解を得ることができなかった。この原因は，2.4.1 節で示した性質 2.4.2, 性質 2.4.3（および図 2.16）を考慮すると，おそらく前者によるものだと推測される。Wu らのパラメータ推測法は，テント写像やロジスティック写像から得られる系列がエルゴード的な性質^{*16} を有することを前提とするが，有限精度で実装されたテント写像やロジスティック写像から得られた系列においては，これを前提とすることは難しいであろうことを伺い知ることができる。

第 4 章

解析法の視点から考えた解析が困難となるケースについて

2 章では、1 次元写像の最も単純な例であるテント写像 f_a を反復する度に得られる $\{x_i\}$ 系列のランダム性について触れた。そして、数値計算により周期軌道に陥ること、並びに $\{x_i\}$ 軌道の分布の偏り等を示した。有限精度で実装されたテント写像の経験的な性質について述べた。一方で、写像の度に x_i の下位側の桁を抽出して構成した $\{b_i\}$ 系列を考えた場合は、0,1 の頻度が経験的に等頻度に近づく傾向があり、乱数検定の結果からも統計的に良質なランダムビット列が生成できていることを述べた。

3 章では、テント写像を利用したごく単純な擬似ランダム生成系を定義し（テント写像を反復する度に得られる値の一部（最上位ビット、上位 t ビット目）を抽出する）、当生成系から生成された擬似ランダムビット列が既知情報として与えられたときに、パラメータが既知の下で当該系列を生成し得る初期値を推測する手法、ならびに、初期値が既知の下で当該系列を生成し得るパラメータを推測する手法について触れた。また後半では、Wu らの、初期値が未知の下でパラメータを推測する手法について説明した。本生成系においては、初期値およびパラメータは擬似ランダムビット生成のためのシード（鍵）と深く関係する値だと考えられるため、3 章で述べた推測法は生成系の安全性解析と直結する内容のため重要である。また、より発展的な生成法の検討、ならびにその安全性の評価を与えるに際して、重要な情報をもたらすものと考える。

本章では、3 章で述べた推測法の視点において、改めて推測が困難となる場合について整理する。そして、本論文で述べた推測法により解析が困難となるような擬似ランダムビット列生成法の一例を挙げ、当生成法の評価（推測に必要な計算量と乱数検定結果）を与える。

4.1 各推測法の視点において推測が困難となる場合

4.1.1 最上位ビット抽出系列に対する初期値推測法、パラメータ推測法の観点

任意の初期値 $x_0 \in (0, 1)$ 、および任意のパラメータ ($a \in (1, 2]$) のテント写像からの最上位ビット抽出系列に関しては、3.3 節、3.4 節で述べた初期値推測法（パラメータ既知）によって、並びに、3.8

節で述べたパラメータ推測法（初期値既知）によって、厳密かつ、一意的にその初期値／パラメータを求めることができる。

最上位ビット抽出系列の場合に、初期値／パラメータの範囲が一意的に求まる理由は以下の2点である。

1. 0,1のビットが抽出される領域と、テント写像の $f(x) = ax$ （左側関数）または $f(x) = a(1-x)$ （右側関数）が定義される領域が等しいため。（これによって観測ビットから合成すべき関数が一意的に決定する。）
2. 初期値 x_0 を含め写像の度に x_i からその2進小数点数の最上位ビットを抽出しているため。

1点目に関しては、関数の定義域と、ビット抽出領域を異なるものとすることで、推測式に分岐を与えることができる。この場合は、上位 k 衔目のビットを抽出した場合と同様に評価すべき推測式の数を増やすことができる。

2点目に関しては、例えば、 $m - 1$ 回の写像の間はビット抽出を行なわず、 m 回の間隔をおいてビット抽出する場合であれば、すなわち、 $n = m \times s$ 回の写像で得られる $\{x_i\}_{i=0}^{m-s}$ から $\{b_i\}_{i=1}^s$ が生成されている場合では、欠如している計 $n - s = (m - 1)s$ ビット分の最上位ビットの情報を埋めない限り $x_n = f^n(x_0)$ の多項式関数形を決定できない。この場合、 $M^{(m-1)s}$ とおりのビットパターンを考えられることから、探索量 M は

$$\begin{aligned} M &= 2^{n-m} = 2^{(m-1)s} \\ \Leftrightarrow \log_2 M &= (m-1)s \quad \text{ビット} \end{aligned} \tag{4.1}$$

である。従って観測ビット列長が s であれば m が大きいほど推測のための計算量を増やすことができる。ただし、このことに応じてビット列生成速度は犠牲になることは避けられない。

上述のことは、任意桁目のビット（上位 t ビット桁目／下位側ビット）を抽出した場合に適用しても相応の効果がある。

4.1.2 任意桁目のビット（上位 k ビット桁目／下位側ビット）抽出系列に対する初期値推測法、パラメータ推測法の観点

任意桁目のビット（上位 k ビット桁目／下位側ビット）抽出系列の場合は、推測のための計算量が増えることは既に述べた。また、3.10.3節では、生成系が倍精度浮動小数点演算で実装した場合において、3.5.2節で示す推測法により、1つの推測式あたり初期値を5点に絞り込むことができるとしたときに、初期値を1点に絞り込むために必要となる探索量について触れた（式(3.156)）。尚、式(3.156)では、 $\{z_i\}$ 軌道の候補から最上位ビット系列 $\{b_i\}$ に変換する際に、 $\{b_i\}$ の中に0の連の最大値より長い0の連が含まれるパターンを省いていない。これを省くことによって、実際に評価すべき推測式の数（探索量）を抑えることができる。ここでは、0の連の最大値より長い0の連が含まれるパターンを省いた場合の探索量の期待値を試算する。

観測ビット列はランダムかつ0,1の出現頻度は等頻度性を有するとする。パラメータ a のときの0の連の長さの最大値を $l(a)$ とする。 $l(a)$ は、式(3.58)より、

$$l(a) = \lceil \log_a \left(\frac{1}{2-a} \right) \rceil - 1 \tag{4.2}$$

として表される。すなわち、0 の連の長さは $l(a)$ となることはありえるが、 $l(a) + 1$ となることはない。

$\{z_i\}$ 軌道から $\{b_i\}$ 軌道に変換して、 $\{b_i\}$ 軌道の i ビット目を考える。観測ビット列の仮定より、 $\{z_i\}$ はランダムに与えられているとする。 i ビット目から $i - l(a)$ ビット目までの計 $l(a) + 1$ ビットが偶然にも 0 であった場合は、その軌道から導かれる推測式は評価しなくてよいとして省くことができる。この場合は、1 つの z_0 候補あたりで、観測ビットの 1 ビットあたりに生じる $\{z_i\}$ 軌道の数の期待値は、3.10.2 節より、

$$\frac{1}{2^{l(a)+1}} \times 0 + \frac{2^{l(a)+1} - 1}{2^{l(a)+1}} \times (P_1 \times 1 + P_{2,1} \times 1 + P_{2,2} \times 2) = \frac{2^{l(a)+1} - 1}{2^{l(a)+1}} \times \frac{a+1}{2} \quad (4.3)$$

と概算される。これより、観測ビット列長が n の場合は、

$$\left(\frac{2^{l(a)+1} - 1}{2^{l(a)+1}} \times \frac{a+1}{2} \right)^n \quad (4.4)$$

と修正される（式 (3.153) 参照）。上位 k 衍目のビットを抽出する場合は z_0 候補は 2^{k-1} 個あることから、 k, n における $\{z_i\}$ 軌道の数の期待値、すなわち、推測式の数の期待値 $E\{M'\}$ は、

$$E\{M'\} = 2^{k-1} \left(\frac{2^{l(a)+1} - 1}{2^{l(a)+1}} \times \frac{a+1}{2} \right)^n \quad (4.5)$$

である。

次に生成法が有限精度（演算精度 t ）で実装された場合を考える。有限精度の場合に得られる系列に対する初期値推測は、 $n_0(a, t)$ ビット（式 (3.155)）以上の観測ビット列が与えられていれば、1 つの推測式あたり、初期値の候補を 5 点に絞り込むことができる。すなわち、上位 k 衍目のビット抽出の場合は、式 (4.5) の z_i 軌道毎に 5 点の候補が存在することになり、この場合の探索量 M' の期待値は、

$$E\{M'\} = 5 \cdot 2^{k-1} \left(\frac{2^{l(a)+1} - 1}{2^{l(a)+1}} \times \frac{a+1}{2} \right)^{n_0(a, t)} \quad (4.6)$$

である。

式 (4.6) について、倍精度 浮動小数点演算 ($t = 52$)、最下位ビット（上位 $k = 52$ ビット目）抽出の場合の関係を図 4.1 に示す。倍精度 浮動小数点演算 ($t = 52$)、中位衍ビット（上位 $k = 26$ ビット目）抽出の場合の関係を図 4.2 に示す。単精度 浮動小数点演算 ($t = 23$)、最下位ビット（上位 $k = 23$ ビット目）抽出の場合の関係を図 4.3 に示す。

留意点を述べる。式 (4.6) および、図 4.1 は、 $\{z_i\}$ 軌道の候補数から最上位ビット系列 $\{b_i\}$ に変換する際に、 $\{b_i\}$ の中に、0 の連の最大値より長い 0 の連が含まれるパターンを省いてから推測法により初期値を得るとしたときに、初期値を 1 点に絞り込むまでに必要な探索量の期待値を意味している。 $\{z_i\}$ 軌道の候補の数自体（0 の最大連を省く前）は、式 (3.156) および、図 3.12 で示される量であることには変わりがないので、計算機プログラム上のループの上限や、計算機上に確保しなければならないメモリ量は、上式でなく式 (3.156) を考えるべきである。

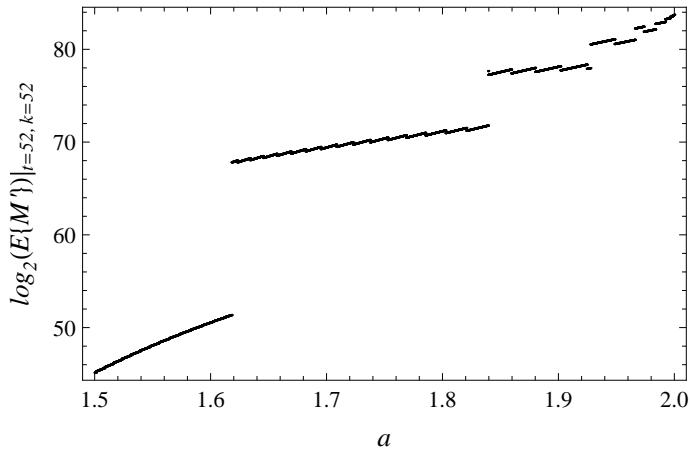


図 4.1 倍精度 浮動小数点演算 ($t = 52$) , 最下位ビット (上位 $k = 52$ ビット目) 抽出の場合に , 初期値の特定に必要な探索量の期待値 $E\{M'\}$ (対数表記)

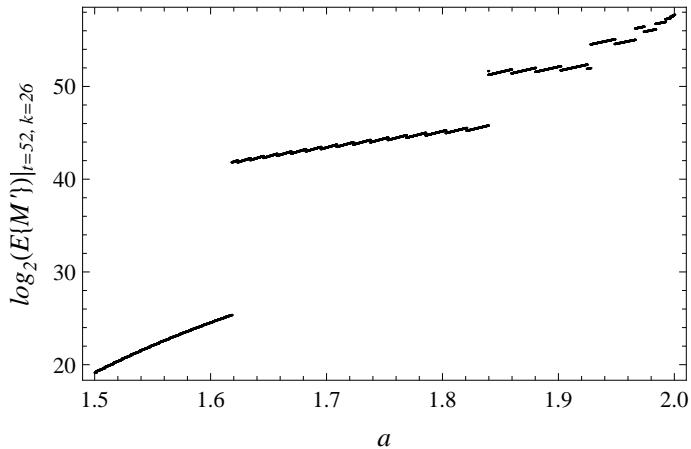


図 4.2 倍精度 浮動小数点演算 ($t = 52$) , 中位桁ビット (上位 $k = 26$ ビット目) 抽出の場合に , 初期値の特定に必要な探索量の期待値 $E\{M'\}$ (対数表記)

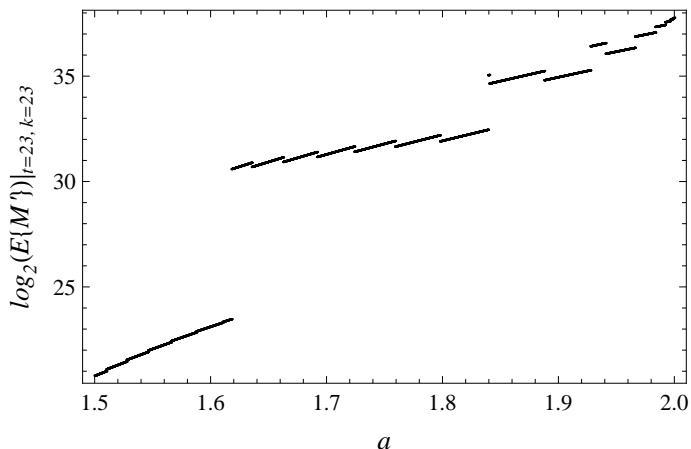


図 4.3 単精度 浮動小数点演算 ($t = 23$) , 最下位ビット (上位 $k = 23$ ビット目) 抽出の場合に , 初期値の特定に必要な探索量の期待値 $E\{M'\}$ (対数表記)

4.1.3 Wu らのパラメータ推測法の観点

Wu らのパラメータ推測法（初期値が未知の下でのパラメータの推測）の性能については 3.10.5 節で示した。これより、Wu らの推測法は、本論文で示したパラメータが既知の下での初期値推測法、および、初期値が既知の下でのパラメータ推測法に比べて遙かに効率が悪いことが判る。すなわち、初期値を未知としたときのパラメータの推測の困難性を伺い知ることができる。

しかし、初期値とパラメータはシード（鍵）依存値であることを考えると、初期値またはパラメータのどちらか一方が既知情報として与えられていると考える方が稀であり、より現実的な解析法を検討するにあたっては、初期値とパラメータは未知情報であると考えるほうが現実的である。すなわち、Wu らの手法の考え方は重要である。

Wu らの推測法は、テント写像 f_a のパラメータ a が固定されていることが前提となっている。従って a を頻繁に変化させることによって推測を困難にさせることができる。

例えば、写像毎に（或は一定の回数の写像後に）パラメータを変化させることができると挙げられる。パラメータ a の区間 J ($a \in J$) を決めておき、区間 J 内の値の全てを等頻度に巡回させるようなアルゴリズムを用意すれば、 J の大きさ相応の効果がある。 $|J| = v$ （或は $\#J = v$ ）とすれば、全探索量は単純に v 倍となる ($\log_2 v$ ビット分多くすることができる)。

また、 u 個のパラメータ $\{a_0, a_1, \dots, a_{u-1}\}$, $a_j \in J_j$ ($0 \leq j < u$) $|J_j| = v_j$ （或は $\#J_j = v_j$ ）を用意して、 i 回目の写像で $a_{i \bmod u}$ を使うこととし、それぞれ区間 J_j 内の値の全てを等頻度に巡回させるようなアルゴリズムを用意すれば、パラメータの組み合わせの総数は $\prod_{j=0}^{u-1} v_j$ となる。簡単のため $v_j \approx v$ ($0 \leq j < u$) とすると、全探索量は単純に v^u 倍に及ぶ ($u \log_2 v$ ビット分多くすることができる)。

4.1.4 その他、有限精度の場合のテント写像の特性から考えた留意点

有限精度演算の場合のテント写像の性質（性質 2.4.1～性質 2.4.4）を考慮すると、パラメータ a が固定されている場合は、異なる初期値を出発した軌道であっても、十分な回数の写像後には、いずれ同一の短い周期軌道に至る場合があるため^{*1}、このような系から抽出された擬似ランダムビット列は、自ずとある時点以降に同一のパターンとなる。従って、シードの一部を初期値として割り与えることは避けるべきである。この観点からも、4.1.3 節で述べたパラメータを変化させた場合に、パラメータの変化量をシードから求めることが得策だと考えられる。最も単純な手法としては、 $a \in J, |J| = v$, $J = \{\eta_0, \eta_1, \dots, \eta_{v-1}\}$ 、とし、はじめに J の t 番目の要素が選ばれていたとする、シードから得た情報を $s < v$ に対して、 J の中から次に選ばれる値の要素番号 t を $t = t + s \bmod v$ と更新して選ぶことが挙げられる。

^{*1} 周期軌道の数は数個しかないので、この可能性は極めて高いといえる。

4.2 各推測法の視点において推測が困難となる擬似乱数生成アルゴリズムの一例

本節では、4.1節で整理した内容をもとに、本論文で扱った推測法の視点において推測を困難とさせるような擬似乱数生成アルゴリズムの一例を挙げる。尚、ここで示すアルゴリズムは、テント写像を利用した擬似ランダムビット生成のコア部であり、例えばシードから内部パラメータへ変換する部分や（シードの設計）、生成された擬似ランダムビット列を整形して出力する部分等は含まない（完成されたものではない）。この点を留意されたい。

擬似ランダムビット生成法 4.2.1 ここでは、整数演算化表記したテント写像 $F_A : I \rightarrow I$ を用いる（式(4.7)）。演算処理は「小数点以下切り捨て」である。 $I = (0, 2M)$, $M = 2^{28}$ とする。すなわち x_i の精度は 29 ビットである ($x_i \in I$, $x_i \in \mathbb{N}$)。

$$x_{i+1} = F_A(x_i) = \begin{cases} \lfloor x_i A/M \rfloor & (x < M) \\ \lfloor (2M - x_i)A/M \rfloor & (x \geq M) \end{cases} \quad (4.7)$$

4.1.1 節、4.1.2 節を考慮して、 $m = 8$ 回の写像毎に、 x_i の最下位ビット（上位 29 ビット目）を 1 ビットを抽出する。また、4.1.3 節を考慮して、パラメータは m 回の写像毎に変化させることにする。パラメータは $u = 16$ 個確保し ($A_0 \sim A_{15}$)、それぞれのパラメータの値域を、

$$A_j \in J_j = [p, p + \delta_j) \quad (0 \leq j < u) \quad (4.8)$$

$$\begin{aligned} p &= 483183820, \\ \delta_0 &= 53533523, \quad \delta_1 = 53533541, \quad \delta_2 = 53533553, \quad \delta_3 = 53533567, \\ \delta_4 &= 53533607, \quad \delta_5 = 53533609, \quad \delta_6 = 53533619, \quad \delta_7 = 53533631, \\ \delta_8 &= 53533643, \quad \delta_9 = 53533651, \quad \delta_{10} = 53533679, \quad \delta_{11} = 53533691, \\ \delta_{12} &= 53533699, \quad \delta_{13} = 53533723, \quad \delta_{14} = 53533751, \quad \delta_{15} = 53533759 \end{aligned}$$

とする。 $|J_j| = \delta_j$ ($\#J_j = \delta_j$) である。尚、ここでは、 δ_j ($0 \leq j < u$) は素数である。初期の $A_0 \sim A_{15}$ はシードから算出されるものとして、ここでは、上式の範囲からランダムに選ばれることにする。パラメータは、 m 回の写像毎に $A_0 \rightarrow A_1 \rightarrow \dots \rightarrow A_{15}$ が選ばれる。そして、 A_{15} が選ばれた後は再び A_0 が選ばれるものとする。ただし、

$$A_j = ((A_j - p) + s_j \mod \delta_j) + p \quad (0 \leq j < u) \quad (4.9)$$

として A_j を更新したものを利用する。 A_j の変化量を意味する s_j ($0 \leq j < u$) は、ここでは 24 ビット幅の整数値 ($s_j \in [0, 2^{24})$) とする。 s_j はシードから算出されるものとして、ここでは、当生成法による擬似ランダムビット列の生成開始以前にランダムに与えるものとする。また、初期値 x_0 もビット列の生成開始以前にランダムに与えるものとする。

擬似ランダムビット生成法 4.2.1 の評価

はじめに初期値推測について評価する。演算精度は $t = 29$, 上位 $k = 29$ ビット桁目抽出である。演算精度が $t = 29$ のときの図 3.10 に相当する関係を図 4.4 に示した。これより, $t = 29$ の場合は, 仮に最上位ビット抽出の場合で, かつ, 写像毎にビットが抽出されていたならば, 約 32 回目の写像までに得られた情報により初期値候補を 5 点に絞り込むことができる。また, $t = 29, k = 29$ のときの図 4.1 に相当する関係を図 4.5 に示した。生成法で使われているパラメータの最小値は $p/M \approx 1.80$ なので, 仮に写像毎にビットが抽出されていたならば, 初期値を絞り込むまでに必要な探索量は 40 ビットである。一方で, 本生成法は, $m = 8$ 回の写像毎にビットを抽出しているので, 4.1.1 節の関係より, 32 回目の写像までに $32 - 8 = 24$ ビット分が未知である。この未知分を加えると $40 + 24 = 64$ ビットとなる。すなわち, 本生成法 ($t = 29, k = 29$) の強度は約 64 ビットである。一方で, 区間 I 上の全探索量は 29 ビットであることから, 初期値推測法を適用した場合の探索量は, 全探索よりも大きいことになる。

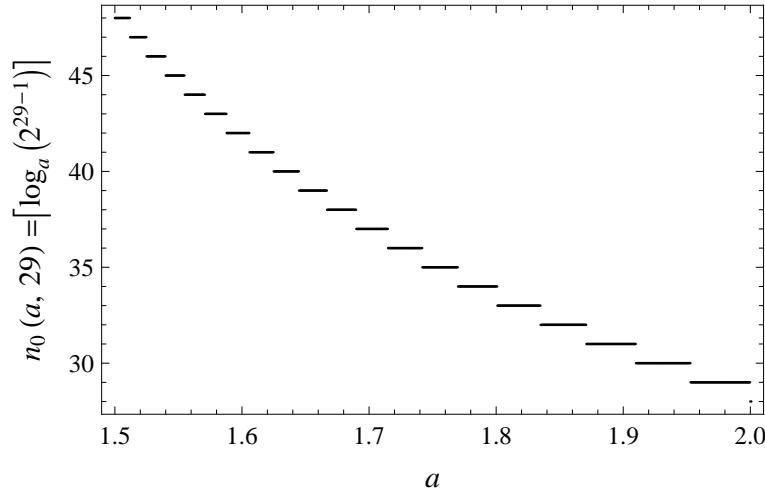


図 4.4 初期値を数点に絞り込むために最低限必要な系列長 $n_0(a, 29)$ (演算精度 $t = 29$ のとき)

次いでパラメータ推測 (Wu ら) について評価する。本生成法はパラメータが変化するので, 大量のビット列が与えられないと特定できない, 本生成法は, 4.1.3 節で示した後者の例に相当し, $\delta_j (0 \leq j < u) \approx 2^{25.67}$ とすると, 同一のパラメータが使われる周期は約 $u \times m \times 2^{25} = 16 \times 8 \times 2^{25} = 2^{32}$ である。従って, 写像毎に変化するパラメータの全てを特定しようとした場合は, $2^{32} \times w$ の長さのビット列が必要である。 w は表 3.2 の \bar{n} に相当する量である。 $t = 29$ の場合における w はここでは見積もっていないが, 仮に $w = 1$ としても相当な量である。

また, 擬似ランダムビット生成法 4.2.1 についての, 5 章で示す判定法によるランダム性の判定結果 (500set 分) を表 4.1, 表 4.2, 表 4.3 に示した。この結果, グレーゾーンにある検定項目は計 4 項目 (#156, #8, #54, #100) あった。尚, グレーゾーン以下となるものは無かった。そして, グレーゾーンにある 4 検定項目については, 5 章で示す判定法に従い, 母平均の推定, 母分散の推定を実施した。その結果, 適合度検定, 母平均の推定, 母分散の推定の 3 つの視点の検定の全てにおいて不合格となるケースはないことから, 当該 4 検定項目は「グレーゾーンで合格」と判断する。従って擬似

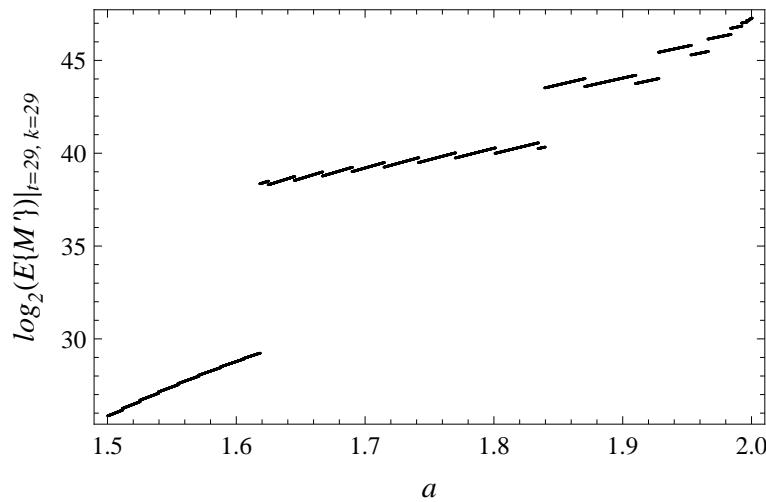


図 4.5 $t = 29, k = 29$ のときの図 4.1 に相応する探索量

ランダムビット生成法 4.2.1 は、全ての検定項目がグレーゾーン以上で合格しているので、良質な擬似ランダムビット生成法だと判断する。

表 4.1 亂数検定結果

表は、擬似ランダムビット生成法 4.2.1 に対する、5 章で示す判定法によるランダム性の判定結果である(500set 分)。表内の数値は各検定項目 (#1 ~ #161) 每の二項分布(理論分布)への適合度を表す p-value である。#8, #54, #100, #156 がグレーゾーン扱い(p-value が 0.0001 以上 0.01 未満)となった。その他の検定項目には合格した PASS(p-value が 0.01 以上)。

# 1	0.401089	# 42	0.699063	# 83	0.422101	# 124	0.958750
# 2	0.109505	# 43	0.200221	# 84	0.268726	# 125	0.329290
# 3	0.524764	# 44	0.816286	# 85	0.411247	# 126	0.888531
# 4	0.630594	# 45	0.170614	# 86	0.767349	# 127	0.286815
# 5	0.754607	# 46	0.700103	# 87	0.590908	# 128	0.621721
# 6	0.256530	# 47	0.174872	# 88	0.961085	# 129	0.322931
# 7	0.110686	# 48	0.278203	# 89	0.061413	# 130	0.935564
# 8	0.001272	# 49	0.865575	# 90	0.087798	# 131	0.027012
# 9	0.610183	# 50	0.805775	# 91	0.324296	# 132	0.015286
# 10	0.073673	# 51	0.974308	# 92	0.507424	# 133	0.428008
# 11	0.504845	# 52	0.275935	# 93	0.810287	# 134	0.799038
# 12	0.532123	# 53	0.253633	# 94	0.971170	# 135	0.293328
# 13	0.244250	# 54	0.007670	# 95	0.389698	# 136	0.612749
# 14	0.681227	# 55	0.280241	# 96	0.973051	# 137	0.375198
# 15	0.532047	# 56	0.048145	# 97	0.536358	# 138	0.560672
# 16	0.721260	# 57	0.150327	# 98	0.305951	# 139	0.760872
# 17	0.922522	# 58	0.721073	# 99	0.217418	# 140	0.706530
# 18	0.870070	# 59	0.196167	# 100	0.009931	# 141	0.377464
# 19	0.411849	# 60	0.830257	# 101	0.808124	# 142	0.900097
# 20	0.406356	# 61	0.769156	# 102	0.788102	# 143	0.846290
# 21	0.252700	# 62	0.125802	# 103	0.397140	# 144	0.063819
# 22	0.117395	# 63	0.964802	# 104	0.350012	# 145	0.358218
# 23	0.355094	# 64	0.642246	# 105	0.722474	# 146	0.814524
# 24	0.746663	# 65	0.182072	# 106	0.074045	# 147	0.081845
# 25	0.103004	# 66	0.475925	# 107	0.926889	# 148	0.805372
# 26	0.428303	# 67	0.713591	# 108	0.448068	# 149	0.263276
# 27	0.044413	# 68	0.628246	# 109	0.549511	# 150	0.617270
# 28	0.072751	# 69	0.473773	# 110	0.343319	# 151	0.341548
# 29	0.369080	# 70	0.821236	# 111	0.316900	# 152	0.375052
# 30	0.835363	# 71	0.784762	# 112	0.118805	# 153	0.888196
# 31	0.370098	# 72	0.685399	# 113	0.179289	# 154	0.386571
# 32	0.820130	# 73	0.272243	# 114	0.190477	# 155	0.545910
# 33	0.062027	# 74	0.449986	# 115	0.058654	# 156	0.001147
# 34	0.598251	# 75	0.043890	# 116	0.032941	# 157	0.035042
# 35	0.569981	# 76	0.226760	# 117	0.999359	# 158	0.996166
# 36	0.543823	# 77	0.247968	# 118	0.831324	# 159	0.302840
# 37	0.721736	# 78	0.152075	# 119	0.994677	# 160	0.145082
# 38	0.760527	# 79	0.949933	# 120	0.378237	# 161	0.942647
# 39	0.302877	# 80	0.223555	# 121	0.247921		
# 40	0.131541	# 81	0.097335	# 122	0.360176		
# 41	0.777357	# 82	0.508460	# 123	0.381438		

表 4.2 p-value がグレーゾーンにある検定項目の「PASS」数に関するヒストグラム

PASS 数 検定項目	PASS 数における観測度数																
	981 以下	982	983	984	985	986	987	988	989	990	991	992	993	994	995	996	997 以上
#156	9	3	5	9	16	26	54	50	71	56	68	59	30	27	6	9	2
#8	13	3	7	6	15	21	42	36	60	70	66	51	45	31	17	14	3
#54	7	1	10	9	19	26	31	65	66	57	55	45	45	19	21	14	10
#100	10	3	5	13	14	19	29	52	54	84	75	46	36	26	19	10	5

表 4.3 p-value がグレーゾーンにある検定項目の、二項分布への適合度、母平均推定、母分散推定

検定項目	二項分布への適合度検定		母分散既知での母平均の推定			母分散の推定			3 つの検定結果を 考慮した上ででの判定
	p-value	<結果>	$\hat{\mu}_{min}$	$\hat{\mu}_{max}$	<結果>	\hat{U}_{min}	\hat{U}_{max}	<結果>	
#156	0.00715394	<GRAY>	989.180	989.904	<x>	7.766	10.765	< >	グレーゾーンで合格
#8	0.00494132	<GRAY>	989.586	990.310	< >	9.146	12.679	< >	グレーゾーンで合格
#54	0.00715394	<GRAY>	989.502	990.226	< >	9.236	12.802	< >	グレーゾーンで合格
#100	0.00494132	<GRAY>	989.540	990.264	< >	8.502	11.785	< >	グレーゾーンで合格

第 5 章

NIST 亂数検定 [46][47] を用いた合理的なランダム性の判定法についての研究

5.1 NIST 亂数検定に含まれる検定法誤り～本研究に至る経緯について

暗号および暗号アプリケーション用の統計的な乱数検定法として，NIST^{*1} が定める SP.800-22[46][47] が広く使われている（本論文では，以降，NIST SP.800-22 を NIST 亂数検定と呼ぶことにする）。NIST 亂数検定はドキュメントおよびツールとして配布されている^{*2}。特にツールに関しては，2001 年に公開されて以降，度重なる修正／バージョンアップがされており，本論文の執筆時点（2009 年 6 月）での最新版は Ver2.0b（2008 年 8 月リリース）である。公開以降から現在までの間に，著者らを含め，多くの研究者によって，NIST 亂数検定に含まれる検定法の誤りに関する報告がされている（例えば，文献 [48]～[69] がある）。この中には NIST によって正式に修正されたものもあれば，未対応のものもある。

ここで Ver2.0b と，それ以前の Ver1.0 ベース（Ver1.8 まで）との差について簡単に触れておく。Lempel-Ziv 圧縮検定（Lempel-Ziv Compression Test）は，文献 [48][49][50] 等で誤りの指摘があり，その後 Ver1.7 で正式に削除された。尚，現在も削除されたままである。DFT 検定（Discrete Fourier Transform Test）は，文献 [51] および，文献 [48][49][52]～[57] にて誤りの指摘と修正に関する報告がある。そして，Ver1.7 において，文献 [48][49] で示される内容で修正された。しかし，著者らは文献 [57] において，この修正は不十分かもしれないことを述べた。その後，NIST は 2009 年 2 月 9 日付で DFT 検定に誤りがあることを認めた^{*3}。重なりのあるテンプレート適合検定（Overlapping Template Matching Test）は，文献 [59][60] にて，理論値の計算に近似が使われていることによる誤差の指摘がある。尚，文献 [47] の 3.8 節に記載される内容より，NIST は本指摘を認知したと思われるが，Ver2.0b（ツールの最新版）はこれに未対応である。また，ランダム回遊検定（Random Excursion Test）においては，最終の巡回列の扱いに関する修正がなされている。

^{*1} National Institute of Standards and Technology (NIST) で「米国標準技術局」と訳される

^{*2} http://csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html で配布されている。

^{*3} NIST は，以下のサイトで DFT 検定は修正されるまで使用しないよう促している。
http://csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html

上記は NIST が正式に対応した修正であるが、これ以外の検定法の誤りについての報告もある。例えば、文献 [62][63][64] では、ユニバーサル統計量検定 (Maurer's Universal Statistical Test) の理論モデルの修正が報告されている。文献 [65][66] では、ブロック単位の最長連続検定 (Test for the Longest Run of Ones in a Block) において、計算中に近似が使われることによる誤差と、 χ^2 検定自体に含まれる誤差の報告がある。

上記の研究報告は、主として、NIST 亂数検定に含まれる個々の検定法（以降に述べる第1段階の検定に相当する）の誤りや誤差に関する内容であり、NIST が示す最終的な合否判定（以降に述べる第2段階の検定に相当する）の曖昧さを指摘する報告は殆どない。個々の検定法（第1段階の検定）の誤りの修正は、上述のとおり、多くの研究者の尽力によって検討されており、今後は精度が向上していくものと期待される。しかし、最終的な合否判定（第2段階の検定）が曖昧に終わってしまうと、結局のところ明確な評価を与えたことにはならない。

本論文は最終的な合否判定（以降に述べる第2段階の検定）と関係するもので、NIST 亂数検定を利用して統計的なランダム性の評価を与える際に、検定者は、どのような結果が得られれば明確に合否を判定（評価）できるのか、或は、検定者の評価結果を見た第三者は、検定者からどのような結果が提示されるならば、検定者が与えた判定結果（評価結果）を納得できるのか、という視点からのものである。そして、NIST 亂数検定を用いることを前提として、ランダム性の判定を明確に達成するための判定法の一案を述べる。

尚、本論文で示す判定法は、文献 [48] ~ [66] で示される個々の検定法（第1段階の検定）に含まれる誤り以外にも、理論で示されること（無限の概念や近似が駆使されている）と現実的に得られる計算結果との間に無視できない誤差が介入していることも考慮し、現実的かつ合理的な判定を与えることを目的としたものである。

以降、5.2 節、5.2.1 節にて NIST 亂数検定の概要を述べ、5.2.2 節にて Proportion 評価の曖昧さを述べる。次いで、5.2.3 節にて、188 個ある検定項目の全てが Proportion で合格する確率を概算し、5.2.4 節にて、この概算に基づく評価（判定）と、その不十分さを述べる。その後、5.3 節にて、本論文で示す判定法について触れる。5.4 節では、本判定法を用いた AES,SHA1,DES ベースの乱数生成法の判定実験結果を述べる。5.5 節で考察を述べ、5.6 節でまとめを述べる。

5.2 NIST 亂数検定の概要

5.2.1 NIST 亂数検定の手順

NIST 亂数検定 (Ver2.0b) は、表 5.1 に示す 15 の検定法、計 188 の検定項目で構成される^{*4}。そして、1,000,000 ピットを 1 系列として、1 系列単位で各検定法（各検定項目）を実施し、これを 1,000 系列分繰り返した結果を総合的に判断する仕組みになっている。尚、本論文では、上記の作業を「NIST 亂数検定を 1set 実施する」と呼ぶことにする。具体的には以下のとおりである。

^{*4} 1 つの検定法あたり、複数の検定項目を有する検定法がある。

表 5.1 NIST 亂数検定に含まれる検定法

検定法の名称	検定項目の番号	検定項目の数 (p-value) の数
Frequency Test / 等頻度検定	#1	1
Frequency test within a Block / ブロック単位の等頻度検定	#2	1
Runs Test / 連検定	#3	1
Test for the Longest Run of Ones in a Block / ブロック単位の最長連検定	#4	1
Binary Matrix Rank Test / 2 値行列ランク検定	#5	1
Discrete Fourier Transform Test / DFT 検定(離散フーリエ変換検定)	#6	1
Non-overlapping Template Matching Test / 重なりのないテンプレート適合検定	#7~#154	148
Overlapping Template Matching Test / 重なりのあるテンプレート適合検定	#155	1
Maurer's Universal Statistical Test / ユニバーサル統計量検定	#156	1
Lempel-Ziv Compression Test / Lempel-Ziv 圧縮検定	(削除)	1
Liner Complexity Test / 線形複雑度検定	#157	1
Serial Test / 系列検定	#158, #159	2
Approximate Entropy Test / 近似エントロピー検定	#160	1
Cumulative Sums Test / 累積和検定	#161, #162	2
Random Excursions Test / ランダム回遊検定	#163~#170	8
Random Excursions Variant Test / ランダム回遊変量検定	#171~#188	18

第1段階の検定

第1段階の検定は、被検定データの1系列を1,000,000ビットとして、表5.1に示した計188の検定項目を実施する⁵。このとき、各検定項目ごとにp-valueと呼ばれる統計量が算出される。NISTは、第1段階の検定での棄却率を $\alpha = 0.01$ (1%)に設定しているので、p-valueが0.01以上ならば、当該系列は当該検定項目において「PASS」したとする⁶。

第2段階の検定(最終評価)

第2段階の検定は、第1段階の検定を $n=1,000$ 系列分繰り返した結果として得られる以下2つの統計量の妥当性を検定項目毎に判断する。

1つはUniformity(一様性)の評価で、p-valueの出現頻度の等頻度性を検定項目毎に判断する。もう1つはProportion(合格比率)の評価で、第1段階の検定で「PASS」する系列の数は、正規分布 $N(\mu, \sigma^2) = N(990, 9.9)$ ⁷に従うと考えて、「PASS」した数が $\mu \pm 3\sigma$ 以内に収まればよいとする⁸。

表 5.2 NIST 亂数検定を 10set 実施したときの Proportion 結果

Proportion 評価で不合格となった検定項目の番号（表 5.1 参照）を記す

検定実施番号	G-AES ^{*1}	G-SHA1 ^{*2}	G-DES ^{*3}
1	#4	全て合格	#45, #75
2	#183	#75	全て合格
3	#123	#16	全て合格
4	# 114, #152	#98	#4
5	全て合格	全て合格	全て合格
6	全て合格	#62, #177	全て合格
7	全て合格	全て合格	#25, #92
8	#161	全て合格	#131
9	全て合格	#40	全て合格
10	#138	全て合格	#182

^{*1}: ANSI X9.31 で定められる AES ベースの擬似乱数生成法 [72][73]^{*2}: FIPS-186 で定められる SHA1 ベースの擬似乱数生成法（入力オプションがないタイプ）[74][75][76]^{*3}: FIPS-186 で定められる DES ベースの擬似乱数生成法を NIST が改造したもの（NIST 亂数検定 Ver1.5 に付属）[74][77][78]

5.2.2 Proportion 評価の曖昧さ

NIST によって示される Proportion の合否条件は、個々の検定項目が満たすべき条件であって、計 188 個ある検定項目が全て合格する必要があるか否か（或はどうであればよいいか）については示していない。このことに触れる理由は、実際に、NIST 亂数検定を実施してみると、計 188 個ある検定項目が Proportion 評価で全て合格するケースは意外と少ないと経験的に気づくためである。例えば以下である。

検定者は、NIST 亂数検定を 1set 実施してみる。このとき、ある検定項目が不合格となったことに気づく。検定者の心理を考えると、シードを換えて再度検定を試みるであろう。すると今度は、先に不合格となった検定項目には合格したが、新たに別の検定項目が不合格となった… 表 5.2 は、このようにして、NIST 亂数検定を 10set 実施したときの結果である。表 5.2 からも明らかであるが、いずれか 1 つ以上の検定項目が Proportion 評価で不合格となるケースが散在する。NIST は、このような状況下でどのような評価を与えればよいかについては示すことはないので^{*9}、最終的な評価は検定者に委ねられることになる。例えば、以下 2 つのパターンが考えられる。1 つは、テストなのだから全ての検定項目が合格しなければならないという解釈である。もう 1 つは、不合格となった検定項目の割合が、検定における第 1 種の誤りの確率程度ならば、「よいだろう」とする解釈である（この解

^{*5} NIST の推奨どおり、Non Overlapping Template Matching Test のパラメータを $m=9$ とした場合は計 188 の検定項目が存在する。

^{*6} p-value は、0 から 1 の間の実数値で、実験で得た経験分布とその理論上の分布との適合度を表す。1 ならば適合、0 は非適合を意味する。

^{*7} 試行回数 $n = 1000$ 、棄却率 $\alpha = 0.01$ （成功率 $p = 1 - \alpha = 0.99$ ）のとき、期待値 $\mu = np = 1000 \times (1 - \alpha) = 990$ 、分散 $\sigma^2 = np(1 - p) = 1000 \times (1 - \alpha) \times \alpha = 9.9$

^{*8} 第 1 段階の検定で「PASS」した数が 981~999 であれば、正規分布 $N(990, 9.9)$ の $\mu \pm 3\sigma$ 以内に収まる。

^{*9} NIST が示すのは NIST 亂数検定を 1set 実施したときの評価であって、複数 set 実施したときの評価を示すものではない。

積は 5.2.3 節で示す).

このように、最終評価は、異なる結論が導かれ兼ねない曖昧なものとなっている。

5.2.3 全ての検定項目が Proportion 評価で合格する確率の概算

表 5.3 真にランダムな系列に対して、188 個の検定項目のうち k 個が Proportion で「合格」する確率 γ_k

合格数 k	不合格数 $188-k$	γ_k		AES 選考時の基準 (文献 [71] 参照)	
		NIST 亂数検定の基準			
		二項分布 で計算	正規分布 で計算		
188	0	0.538	0.776	0.992	
187	1	0.334	0.197	0.0078	
186	2	0.103	0.025	3.08×10^{-5}	
185	3	0.021	0.002	8.03×10^{-8}	

ここでは、仮に良質なランダム性を有するデータを検定したときに、果たして 188 個ある検定項目の全てが Proportion 評価で合格するか否かについて検証する。そこで、以下に示す 3 点の前提のもとで、計 188 個存在する検定項目のうち k 個 ($0 \leq k \leq 188$, $k \in \mathbb{N}$) の検定項目が Proportion 評価で「合格」する確率 γ_k を「概算」として求める^{*10}。結果は表 5.3 となる。

前提 1 ここでの概算では、(ある 1 つの検定項目につき,) 第 1 段階の検定を「PASS」した数が $\mu - 3\sigma$ 以上ならば、Proportion 評価で「合格」したと考える^{*11}。具体的に記すと、「PASS」数が 981 以上の場合がこれに相当する。

前提 2 前提 1 に示した条件の下での、Proportion 評価で「合格」する確率 θ は二項分布から求める^{*12}。具体的には、 $\theta = 0.996712\dots$ である^{*13}。

前提 3 ここでの概算では、計 188 個存在する全ての検定項目は互いに独立であると仮定する。

表 5.3 からは(二項分布で考えた場合は)、仮に被検定データが真のランダム性を有していた場合であっても、計 188 個存在する検定項目の全てが合格する確率は約 54% しかなく、いずれか 1 つの検定項目のみが不合格となる確率は約 33%，いずれか 2 つの検定項目のみが不合格となる確率は約 10% に達することが判る^{*14}。従って、計 188 個存在する全ての検定項目が合格したときに限り被検

*10 前提 1~3 の下では、 γ_k の分布は二項分布 $B(188, \theta)$ に従う。 θ は、ある 1 つの検定項目が Proportion で合格する確率である。

*11 NIST がドキュメントにて示す合格条件は、第 1 段階の検定を「PASS」した数が $\mu \pm 3\sigma$ ^{*7} 以内に収まることである[46][47]。一方、ツールがファイルに出力する実行結果 (finalAnalysisReport の最下段を参照) には、 $\mu - 3\sigma$ の閾値は記録されているが、 $\mu + 3\sigma$ の閾値は記録されていない。つまり、+ 側に 3σ 超えた場合 (合格数が多い場合) は許容すると思われる。

*12 第 1 段階の検定で「PASS」する数の分布は、厳密には、試行回数 $n=1000$ 、成功 rate $p=1-\alpha=0.99$ の二項分布 $B(n, p)=B(1000, 0.99)$ に従う。 n が十分大きいときには、二項分布は正規分布に近似できるので、NIST は、Proportion の合格条件を正規分布で考えて $\mu \pm 3\sigma$ 以内と設定している。しかし、 $n=1000$ では、まだ近似は良いとはいえない(特に分布の両端)。ここでは、前提 1 に示した条件での Proportion 評価で「合格」する確率 θ は二項分布から計算する。

*13 $\theta = P_{B(1000, 0.99)}\{981 \leq X \leq 1000\} = \sum_{x=981}^{1000} \binom{1000}{x} 0.99^x (1-0.99)^{1000-x} = 0.996712$

*14 NIST は、第 1 段階の検定で「PASS」する数の分布は正規分布に従うと考えて Proportion の合格条件を $\mu \pm 3\sigma$

定データのランダム性は良いと判定することは正しい判定法とは言えない。このことは、NIST 亂数検定を 1set 実施した限りでは正確な判定ができないことを示している。

尚、表 5.3 には、参考として AES 選考時の合否基準 [71] を採用した場合の概算値も掲載した^{*15}。例えば低速な物理乱数生成器では、複数 set 分の十分な被検定データを取得するのが困難な場合がある。AES 選考時の合否基準 [71] を用いた場合は、全ての検定項目が合格する確率は約 99% と計算されるので、1set しか実施できない状況で大雑把に評価したい場合には参考になる。ただ、本節で述べた概算に基づく評価は厳密とは言えない。このことの詳細を次節以降で述べる。

5.2.4 概算に基づく評価とその不十分性

前節の内容を配慮すると、検定者が、検定を複数実施して様子を伺ってみることは、むしろ自然の流れだと思われる。そして、表 5.2 の結果を得る。表 5.2 には、不合格となった検定項目が散在している。合否の判定はどうすればよいだろうか。手っ取り早い方法としては、表 5.2 の実験結果が、表 5.3 に示した分布に従うか否かで判断することが考えられる。しかし、表 5.3 は、前節で示した前提の下での概算なので、この分布への適合度検定を試みることは不適切である。以下に、その具体的な不十分性を 3 点示す。

1 点目は、各検定項目は完全に独立しているか否かは判らない点である。この場合は、表 5.3 で示される γ_k は正確な数値ではない（あくまでも概算値）。従って、この分布への適合度検定は意味をなさない。

2 点目は、この概算は、異なる検定項目を、棄却率が $\alpha = 0.01$ の同じもの同士として同一に扱うが、冒頭でも触れたとおり、個々の検定法にはまだ誤りが含まれる可能性がある。特に、後述の 5.5.1 節で述べる点からも、全ての検定項目の棄却率が等しく正確に 1% で設計されているか否かは疑わしい^{*16}。つまり、この現状では、異なる検定項目を、棄却率が $\alpha = 0.01$ の同じもの同士として同一に扱うことはできない。

3 点目は、被検定データが、仮に、ある特定の検定項目に限って、不合格を多く（または少なく）排出する傾向があったとしても、表 5.3 の分布への適合度検定を試みる限りでは、不合格となった検定項目の総量しか扱ないので（不合格となった検定項目が何であるかまでは追跡しないので）、この傾向を見抜けない。

以内と設定している。Proportion 評価で「合格」する確率 θ の計算を、正規分布で計算した場合は $\theta = P_N\{X \geq \mu - 3\sigma\} = 0.99865$ である。この場合は、188 個ある検定項目が全て合格する確率は約 78% となり、二項分布で求めた場合と大きく異なる結果を得る（表 5.3、*12 を参照）。

^{*15} AES 選考時の Proportion の合格条件は、第 1 段階の検定で「PASS」する系列の割合に関する p-value が 0.0001 以上となることである。検定する系列の数が 1,000 のときは「PASS」する系列の数が 976 以上のときにこの条件を満たす。詳細は文献 [71] の第 2 章と Appendix C を参照。

^{*16} 文献 [68] によると、DFT 検定の棄却率は、1% より小さく（合格させやすく）設定されていて、Lempel-Ziv 圧縮検定、重なりのあるテンプレート適合検定、ユニバーサル統計量検定の棄却率は、1% より大きく（合格させにくく）設定されていることが読み取れる。

5.3 NIST 亂数検定を用いたランダム性の合理的な判定法についての提案 [70]

前章までを踏まえ，本章では，NIST 亂数検定を用いることを前提とした上で，ランダム性を合理的に判定する手法の一案を述べる．

5.3.1 前提条件

はじめに，本論文で示す判定法の方向性 / 前提条件を 2 点記す．

1 点目は，5.2.4 節の内容を踏まえて，異なる検定項目を同一のものとして扱うことは避け，個々の検定項目毎に明確な判定をする方針とする．この場合は，全ての検定項目が判定基準をクリアしたならば，乱数生成法のランダム性は良いと総合的に判断できる．すなわち，全体評価（最終評価）が明確となる．

2 点目は，NIST 亂数検定は，この分野では標準的に広く使われている．NIST 亂数検定の枠組み（仕様）は崩さないで，NIST 亂数検定を複数回実施したときに得られる新たな統計量を用いて，合理的な判定を下す方針とする．

5.3.2 提案する判定法の概要

ここで改めて Proportion 評価で生じていることを記す．仮に被検定データがランダムな性質を持っていた場合は，第 1 段階の検定で「PASS」する数は二項分布 $B(1000, 0.99)$ に従う．そして，NIST 亂数検定を 1 set 実施することは，この分布上の点を無作為に 1 つ選ぶことに等しい．このとき， $1 - \theta = 0.003288$ の確率で「不合格」の領域の点が選ばれる．ということが生じている．すなわち，NIST 亂数検定を独立に複数 set 実施したならば，「PASS」した数の分布（ヒストグラム）は，二項分布 $B(1000, 0.99)$ に従うはずである．そこで，両者の適合の様子を観察する（検証する）という案が浮かぶ．以下に，判定法のアウトラインを示す．

提案するランダム性の判定法（アウトライン）::

step-1: 第 1 段階の検定を，NIST の推奨量どおり ($n = 1000$ 系列) 実施して，検定項目毎に「PASS」となった系列の数を記憶する．

step-2: *step-1* を M_{set} 実施して (NIST 亂数検定を M_{set} 実施して)，各 set で「PASS」した数に関するヒストグラム（経験分布）を，検定項目毎に作成する^{*17}．

step-3: *step-2* で得たヒストグラム（経験分布）と，その理論上の分布との適合度（p-value）を，検定項目毎に算出する^{*18 *19}．

^{*17} 著者らは $M = 1000$ を推奨する．

^{*18} 理論上の分布とは， $B(1000, 0.99)$ の確率分布に M を乗じたものである．

^{*19} 本論文では．ここでの適合度を示す数値は χ^2 検定と同じ手法で χ^2 値を算出して，これを p-value に変換したものとする．

step-4: *step-3* で得た p-value から、個々の検定項目毎にランダム性を判定する。p-value が極端に小さな値でなければ、当該検定項目において合格したと考える（判定の詳細は 5.3.4 節で記す）。

step-5: 最終評価（全体評価）を与える。*step-4* において、全ての検定項目が合格していれば、当該乱数生成法は良い乱数生成法だと判断する。

5.3.3 本判定法で得られる p-value について

本判定法の *step-3* で得られる p-value とは、実験により得た経験分布（*step-2* のヒストグラム）と、その理論上の分布^{*18}との適合度を正確に示す数値であることを暗に期待しているが、第1段階の検定法に誤差を含む場合は、棄却率 1% の検定として正しく設計されていないことになるので、正確に 1% で棄却する検定にならない。ここで得られる p-value は期待したものと異なる数値であり得ることを認識しておく必要がある。

このことに触れる理由は、通常、検定結果について議論する際には、検定法は正しく設計されていることが前提となるが、文献 [48] ~ [66] で示される内容と、特に、以降の 5.5.1 節で示す内容を勘案すると、現実的に NIST 亂数検定を扱う上では、第1段階の検定において、検定法に誤りや誤差が含まれている可能性があることを念頭に入れておかねばならないからである。

ここで得られる p-value が限りなく 1 に近い場合と、0 に近い場合の極値については、それぞれがどのようなケースから生じるかについては本論文の付録 C.1 節にて示した。検定法に明らかな誤りがある場合は、複数の乱数生成法を検定したときに、ほぼ全ての乱数生成法の結果（p-value）が極めて 0 に近い値となるであろうことから、この旨を経験的に知ることができる（この例は、以降の 5.4.1 節で実験例を示す）。問題は、検定法に「ごく僅かな誤差」が含まれる場合である。仮に真のランダム性を有する被検定データを、誤差を含んだ検定法で検定したときに得られる p-value は、誤差を含まない正確な検定法で検定したときに得られる p-value よりも小さめの値となるはずである（理論分布のほうがズレているので適合はよくない）。つまり、現実的に得られる p-value（検定法に誤差が介入するときの値）は、真の値（検定法に誤差が無いときに得られる値）よりも小さめ（誤差の程度に相応した揺らぎがある）と考えられる。

以降では、まず 5.3.4 節にて、個々の検定項目毎に *step-3* で得られる p-value から、それぞれの検定項目の視点でのランダム性の判定について記す。次いで、5.3.5 節にて、個々の検定項目毎の判定を総合した全体評価について触れる。

5.3.4 個々の検定項目毎のランダム性の判定

p-value が 0.01 以上の場合

統計検定の慣例では、棄却率は 5% あるいは 1% が利用されること、また、NIST は 1% を採用していること等から、本判定法においても、*step-3* で得られた p-value が 0.01 以上の場合には、当該検定項目において「合格」と判断する。

p-value が概ね 0.0001 以上 0.01 未満の場合

5.3.3 節で触れた検定法に含まれる「ごく僅かな誤差」を考慮すると、*step-3* で得られた p-value が微妙に 0.01 を下回った場合の扱いには注意が必要である。

仮に、付録 C.1 の (B-2) のケース（検定法が間違いで、被検定データがランダム性を有する）が生じているならば、誤差を含む検定法で検定したときに得られる p-value は、誤差を含まない正確な検定法で検定したときに得られる p-value よりも小さい値となるはずである。このことによって、0.01 未満となった可能性がある。一方で、付録 C.1 の (B-1) のケース（検定法が正しく、被検定データがランダム性を有していない）が生じていて、被検定データのランダム性がよくない可能性もある。現時点では、検定の全ての過程をとおして含まれる誤差の見積もりはされていないので（この見積もりは困難な場合がある）、上記のどちらが生じているかは判断できない。本論文では、この、正確な判断ができない領域を「グレーゾーン」と呼ぶことにする。尚、本論文では、p-value が概ね 0.0001 以上 0.01 未満の場合を「グレーゾーン」とする。

「グレーゾーン」の下限値を概ね 0.0001 とした理由について述べる。ランダムと非ランダムを明確に線引きすることは根本的に難しい問題であるが、NIST は、第 1 段階の検定の棄却率を 0.01 としていることに対して、第 2 段階の検定のうち Uniformity の評価は 0.0001 としている。また、AES 選考時においては、第 2 段階の検定のうち Proportion の評価においても 0.0001 とした経緯がある [71]。これらを勘案して、著者らは、微妙な判定におけるひとつの区切りを 0.0001 とした。

p-value が「グレーゾーン」にある場合の判定は、その他の手段によって、実験により得た経験分布（step-2 のヒストグラム）と、その理論上の分布^{*18} の「乖離／非適合」を検討することにする。例えば、実験データの平均値、不偏標本分散、グラフ化／可視化が参考になると考えられる。そして、本判定法においては、経験分布と理論上の分布との間に明確な「乖離／非適合」が見いだせない場合は、「グレーゾーンで合格」という扱いとする。ただし、ここは検定者の主觀が介入する場所であるため、ここで用いたその他の手段による結果等、この状況を詳細に説明する情報を提供することを義務とする。

これによって、p-value が「グレーゾーン」にある場合の合否理由を第三者に対して説明できる。また、仮に、検定者が与えた評価結果に納得いかない第三者がいたとしても、第三者側で個別に判断するための情報が提供されることになる。

p-value が概ね 0.0001 未満の場合

step-3 で得られた p-value が極めて小さな値となった場合（本論文では概ね 0.0001 未満となった場合）は、当該検定項目において「不合格」と判定する。

5.3.5 全体評価～乱数生成法の最終評価

step-4 において、「不合格」と判定された検定項目が 1 つも存在しない場合は、すなわち、全ての検定項目が「合格」または「グレーゾーンで合格」と判定された場合は、当該乱数生成法は「良い」乱数生成法だとする。本判定法の最大の特徴はここにあり、最終評価（全体評価）の「明確さ」にある。

5.4 本判定法を用いたランダム性の評価実験

本判定法を $M = 1000$ (NIST 亂数検定を $M = 1000\text{set}$)、および NIST 亂数検定のパラメータを表 5.4 に示す値^{*20} を用いて実施したときの実験結果を表 5.5 に示す。表 5.5 には紙面の都合で一部のデータしか掲載していないが、付録 C.2 に全データを掲載した。また、誤りが報告されている検定法については、修正版を用いたときの実験結果を表 5.6 に示す。使用した乱数生成法は、先の表 5.2 と同じ G-AES, G-SHA1, G-DES, G-SHA1(v1.5), G-DES(v1.8) である。表内の数値は、本判定法の *step-3* で得られる p-value であり、実験により得た経験分布 (*step-2* のヒストグラム) と、その理論上の分布^{*18} との適合度^{*21} を表している。尚、ランダム回遊検定 (#163–#170)、ランダム回遊変量検定 (#171–#188) の 2 つの検定法は、他の検定と異なる特殊な仕様となっていて、全ての系列の検定結果を得ることができないので本論文では対象外とする。

以降では、実験の詳細について述べる。まず、5.4.1 節にて、第 1 段階の検定に誤りがある検定法（検定項目）についての実験結果を説明する。次いで、5.4.2 節にて、第 1 段階の検定に誤りがない検定法（検定項目）についての実験結果を説明する。その後、5.4.3 節にて、全体的な評価～乱数生成法の最終判定を述べる。

表 5.4 NIST 亂数検定のパラメータ（本論文での実験に用いたパラメータ）

検定項目番号	検定法略式名称	検定パラメータ
#2	BlkFrq	$m = 100$
#4	LngRun	$M = 10000$
#7–#154	N-ovlp	$m = 9$
#155	Ovlp	$m = 9$
#156	Univ	$L = 7 Q = 1280$
#158–#159	Serial	$m = 5$
#167	LinCmp	$M = 500$
#160	ApEntrop	$m = 5$

5.4.1 第 1 段階の検定に誤りがある検定項目の実験結果の説明

DFT 検定 (#6), Lempel-Ziv 圧縮検定

DFT 検定 (#6) と、Lempel-Ziv 圧縮検定（削除）は、本実験においても、p-value は全ての乱数生成法で極めて小さい値となった（表 5.5）。この 2 つの検定法に誤りがあることは既知であるため [48] ~ [56]、表 5.5 で示される結果は、本判定法においても当検定法の誤りを検知したことによるものと考えられる。尚、DFT 検定に関しては、NIST が Ver1.7 で修正した手法 [48][49] を用いたときの実験結果を表 5.6 に示した。しかし、依然と小さい値のままである。このことについて著者らは、DFT 検定の修正は不十分である可能性があることを述べた [57]。その後、NIST は 2009 年 2 月 9 日付けで DFT 検定に誤りがあることを発表した^{*3}。現時点では、NIST からは DFT 検定の再修正版は発

^{*20} 表 5.4 に示すパラメータは、NIST 亂数検定 Ver1.5 の時点でのデフォルト値である。尚、最新の Ver2.0b ではこのデフォルト値に変更があったが、その理由は定かでない。

^{*21} 適合度は、 χ^2 検定と同じ手法で χ^2 値を算出して、これを p-value に変換したものである。実験は、 $M = 1000$ として実施しているので、 χ^2 検定の制約^{*22} を考慮して、合格数が 981 以下と、997 以上は、それぞれ 1 つのクラスにまとめ。計 17 クラス（自由度 16）として計算した。

表 5.5 G-AES,G-SHA1,G-DES,G-SHA1(v1.5),G-DES(v1.8) から生成した系列に対する , 本判定法の step-3 におけるランダム性判定実験結果を表す p-values

検定項目 番号	検定法 略式名称	G-AES* ¹	G-SHA1* ²	G-DES* ³	G-SHA1(V1.5)* ⁴	G-DES(V1.8)* ⁵
#1	Frq	0.51	0.59	0.42	0.44	0.74
#2	BlkFrq	0.51	0.047	0.0022	1.14E-5	0.012
#3	Runs	0.036	0.37	0.65	0.68	0.47
#4	LngRun	0.030	6.3E-08	8.9E-11	6.63E-08	1.24E-04
#5	Rank	0.98	0.13	0.43	0.30	0.38
#6	DFT	Underflow	Underflow	Underflow	Underflow	Underflow
#7	N-ovlp(1)	0.57	0.002	0.85	0.51	0.21
#16	N-ovlp(10)	0.65	0.50	0.92	0.023	0.18
#106	N-ovlp(100)	0.75	0.16	0.26	0.074	0.087
(#7-#154 のうち 3 項目だけ表示)						
#155	Ovlp	1.5E-71	5.6E-73	4.1E-72	4.0E-60	8.8E-57
#156	Univ	1.4E-77	4.1E-66	6.0E-81	1.4E-72	8.2E-80
削除	Lmpl	2.4E-74	5.9E-62	4.8E-67	2.6E-66	2.7E-66
(Ver1.7 以降で正式に削除)						
#157	LinCmp	0.23	0.003	0.58	0.23	0.43
#158	Serial(1)	0.62	0.66	0.61	0.023	0.071
#159	Serial(2)	0.65	0.91	0.11	0.38	0.53
#160	ApEntrop	0.64	0.77	0.88	0.65	0.68
#161	Cums(1)	0.53	0.37	0.92	0.78	0.57
#162	Cums(2)	0.50	0.43	0.49	0.32	0.015
#163-170	Rnd-Ex	他と同一の指標での数値が得られないので対象外とする				
#171-188	Rnd-Ex	他と同一の指標での数値が得られないので対象外とする				

*1 : ANSI X9.31 で定められる AES ベースの擬似乱数生成法 [72],[73]

*2 : FIPS-186 で定められる SHA1 ベースの擬似乱数生成法 (入力オプションがないタイプ) [74],[75],[76]

*3 : FIPS-186 で定められる DES ベースの擬似乱数生成法の NIST 改造版 (NIST 亂数検定 Ver1.5 に付属) [74],[77],[78]

*4 : NIST 亂数検定 Ver1.5 に付属

*5 : NIST 亂数検定 Ver1.8 に付属

表されていない . Lempel-Ziv 圧縮検定は削除されたままである .

重なりのあるテンプレート適合検定 (#155)

重なりのあるテンプレート適合検定 (#155) の誤りについては , 文献 [59][60] にて報告されている . 本実験でも , 当検定 (#155) の p-value は , 全ての乱数生成法で極めて小さい値となった (表 5.5) . 従って , 本判定法においても当検定 (#155) の誤りを検知できたと考えられる . 尚 , 同文献 [59][60] で示される修正 (実験値と比較するための理論値が近似により算出されることによる誤差の修正) を反映させた修正版を用いたときの実験結果を表 5.6 に示した . 修正版を用いた場合は , いずれも 0.01 以上の良好な値となった . 従って , 本修正が正しいと仮定するならば (誤りが正しく修正されていると仮定するならば) , 被検定データは , 当検定 (#155) の視点においてランダムであると判断できる . 尚 , 本修正は , ツール Ver2.0b には反映されていない .

ユニバーサル統計量検定 (#156)

本実験では , ユニバーサル統計量検定 (#156) の p-value も , 全ての乱数生成法で極めて小さな値となった (表 5.5) . このことより , 著者らは , 当検定 (#156) にも誤りがある可能性があることを述

表 5.6 修正された検定法を用いたときの、G-AES,G-SHA1,G-DES,G-SHA1(v1.5),G-DES(v1.8)から生成した系列に対する、本判定法の step-3 におけるランダム性判定実験結果を表す p-values

検定項目 の番号	検定法の 略式名称	G-AES ^{*1}	G-SHA1 ^{*2}	G-DES ^{*3}	G-SHA1(V1.5) ^{*4}	G-DES(V1.8) ^{*5}
#4	LngRun	0.096	0.73	0.19	0.58	0.54 (文献 [65][66] で示される修正版を利用)
#6	DFT	8.0E-118	7.2E-116	9.7E-138	9.6E-99	2.8E-94 (文献 [48][49] で示される修正版を利用)
#155	Ovlp	0.78	0.88	0.12	0.86	0.94 (文献 [59][60] で示される修正版を利用)
#156	Univ	0.50	0.77	0.99	0.66	0.96 (文献 [63][64] で示される修正版を利用)

*1 : ANSI X9.31 で定められる AES ベースの擬似乱数生成法 [72][73]

*2 : FIPS-186 で定められる SHA1 ベースの擬似乱数生成法 (入力オプションがないタイプ) [74][75][76]

*3 : FIPS-186 で定められる DES ベースの擬似乱数生成法の NIST 改造版 (NIST 亂数検定 Ver1.5 に付属) [74][77][78]

*4 : NIST 亂数検定 Ver1.5 に付属

*5 : NIST 亂数検定 Ver1.8 に付属

べた [64]。ただし現時点では NIST による正式な対応はない。この点については、文献 [63] にて理論モデルの修正が議論されている。同文献で示される修正（理論モデルの修正）を反映させた修正版を用いたときの実験結果を表 5.6 に示した。修正版を用いた場合は、いずれも 0.01 以上の良好な値となった。従って、本修正が正しいと仮定するならば（誤りが正しく修正されていると仮定するならば）、被検定データは、当検定 (#156) の視点においてランダムであると判断できる。

ブロック単位の最長連検定 (#4)

本実験結果（表 5.5），および，他の乱数生成法を用いた実験（本論文では省略）より，著者らは，ブロック単位の最長連検定 (#4) の p-value は，やや小さめの値になる傾向があることを認識していた [68][69]。この点については，文献 [65] にて，当検定 (#4) に含まれる誤差について報告がされている。具体的に記すと，この報告から，当検定 (#4) では経験分布と理論上の分布との χ^2 検定が行われるが，理論上の確率値の算出に近似が使われていて，近似を使わないときと比較して，（確率値で）最大 0.0015 の誤差を含むクラスがあることが判る。さらに，同文献では，当検定 (#4) で用いられる χ^2 検定は，その制約^{*22} の限界付近で実施していることに対する懸念も述べられている。著者らは，この χ^2 検定の制約の限界付近で χ^2 検定を実施したときの誤差を見積もった。具体的に記すと， χ^2 分布は多項分布の近似であることから，多項分布を実際に計算機で解いて作った累積分布と， χ^2 分布の累積分布の比較を試みた。その結果，棄却率 0.01 を想定した検定は，実際には，棄却率 0.010433 で実施されていることが判った（その差は僅か 0.000433）[66]。文献 [65][66] で示される双方の修正を反映させた修正版を用いたときの実験結果を表 5.6 に示した。修正版を用いた場合は，いずれも 0.01 以上の良好な値となった。尚，当検定 (#4) の場合は，検定法の全過程を通して含まれる誤差を詳しく調べたケースといえる。修正版は，適切に修正されたと考えられるので，被検定データは，ブロック単位の最長連検定 (#4) の視点においてランダムであると判断できる。尚，この検定

^{*22} E_j を期待度数， O_j を観測度数とする。 χ^2 検定は， $\chi^2_{obs} = \sum_{j=1}^u (O_j - E_j)^2 / E_j$ が χ^2 分布のよい近似となっていることを利用する。一般的に $E_j \geq 5$, $u \geq 5$ として検定すれば誤差は小さいことが知られている（文献 [79] の第 9 章 3 節参照）。

法も、現時点では NIST による正式な対応はない。

表 5.7 p-value がグレーゾーンにある検定項目の、「PASS」数に関するヒストグラム（経験分布）

PASS 数 検定項目	PASS 数における観測度数																
	981 以下	982	983	984	985	986	987	988	989	990	991	992	993	994	995	996	997 以上
G-AES																	
#19	12	17	15	29	38	42	59	98	133	121	107	93	91	72	39	21	13
#139	3	17	13	14	44	47	59	105	97	120	133	114	107	60	40	17	10
G-SHA1																	
#81	3	14	17	16	48	48	73	109	142	118	102	123	74	45	38	25	5
#136	5	9	13	26	34	61	105	81	145	99	131	100	73	59	35	16	8
#7	4	13	15	19	51	45	73	110	136	122	104	118	77	47	36	25	5
#157	9	16	17	25	36	53	97	80	131	118	120	110	90	47	28	14	9
#100	6	9	19	21	31	51	77	71	144	121	121	120	73	49	53	19	15
#98	15	6	18	20	27	64	71	102	119	116	150	87	91	56	39	12	7
G-DES																	
#128	13	7	16	20	51	59	69	93	100	152	110	95	84	74	35	21	1
#2	3	4	7	10	29	39	68	106	101	116	156	111	100	69	53	21	7
#114	11	8	18	26	43	43	87	91	137	126	125	75	97	54	30	18	11
#49	16	8	17	24	35	50	66	92	100	101	144	129	88	76	27	18	9
G-SHA1(v1.5)																	
#2	8	8	5	22	30	37	69	77	116	109	134	109	97	66	62	36	15
#13	7	5	19	31	33	42	75	79	131	117	100	103	106	66	48	30	8
#30	10	3	22	32	36	51	79	92	119	144	119	91	74	62	47	10	9
#40	6	14	14	27	33	58	56	112	112	104	144	104	104	73	64	41	29
G-DES(v1.8)																	
#69	13	5	18	24	52	54	94	125	97	113	118	90	75	70	29	14	9
#109	3	6	25	24	31	77	90	101	95	112	112	119	80	69	27	18	11
#154	8	11	23	23	49	48	83	104	114	104	108	91	80	63	49	28	14
#80	9	10	22	25	49	46	84	107	112	105	106	89	82	64	49	27	14
#142	8	13	15	23	45	69	73	83	114	128	141	94	83	42	37	16	16
#106	14	7	17	35	39	46	55	87	111	128	132	103	76	73	45	24	8

表 5.8 p-value がグレーゾーンにある検定項目の、二項分布への適合度、母平均推定、母分散推定

検定項目	二項分布への 適合を示す p-value	母分散既知での母平均の推定			母分散の推定			3つの検定の 全てが不合格 となるもの
		$\hat{\mu}_{min}$	$\hat{\mu}_{max}$	<結果>	\hat{U}_{min}	\hat{U}_{max}	<結果>	
G-AES								
#19	0.001220	989.623	990.135		10.127	12.754	×	
#139	0.006850	989.808	990.320		8.929	11.246		
G-SHA1								
#81	0.000133	989.504	990.016		8.738	11.005		
#136	0.000848	989.457	989.969	×	8.665	10.913		
#7	0.001955	989.499	990.011		8.775	11.051		
#157	0.003049	989.377	989.889	×	9.116	11.480		
#100	0.004816	989.743	990.255		9.166	11.544		
#98	0.008083	989.525	990.037		8.928	11.245		
G-DES								
#128	0.001255	989.511	990.023		9.279	11.686		
#2	0.002170	990.152	990.664	×	7.648	9.632	×	<<< 該当 >>>
#114	0.007562	989.449	989.961	×	9.196	11.581		
#49	0.008728	989.692	990.204		9.546	12.022		
G-SHA1(v1.5)								
#2	1.12E-05	990.204	990.716	×	9.350	11.776		
#13	0.003545	989.839	990.351		9.606	12.097		
#30	0.006676	989.489	990.001		9.123	11.489		
#40	0.006735	989.686	990.198		9.486	11.947		
G-DES(v1.8)								
#69	4.22E-05	989.307	989.819	×	9.373	11.805		
#109	0.000286	989.506	990.018		9.168	11.547		
#154	0.000505	989.570	990.082		10.435	13.143	×	
#80	0.000615	989.563	990.075		10.447	13.157	×	
#142	0.008185	989.464	989.976	×	9.408	11.849		
#10	0.008650	989.687	990.199		9.942	12.521	×	

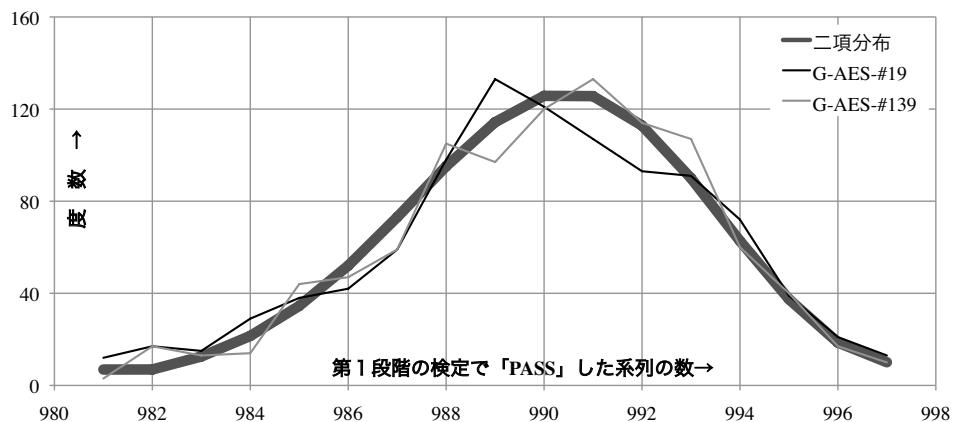


図 5.1 p-value がグレーゾーンにある検定項目の経験分布と理論分布の適合の様子 (G-AES)

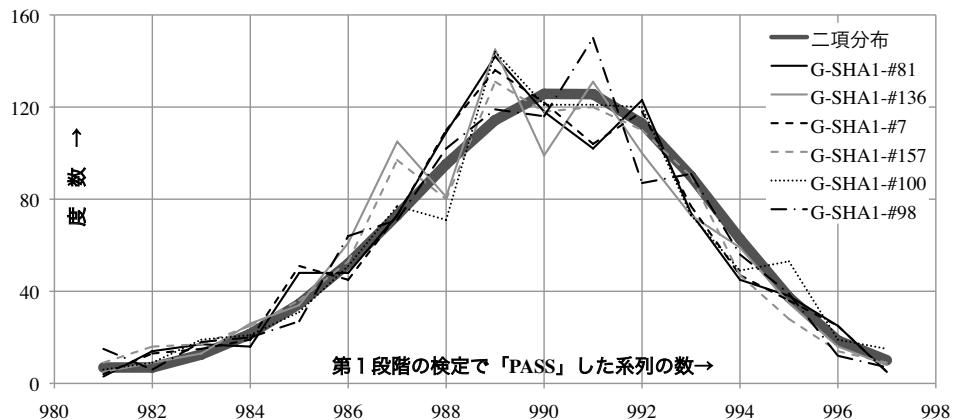


図 5.2 p-value がグレーゾーンにある検定項目の経験分布と理論分布の適合の様子 (G-SHA1)

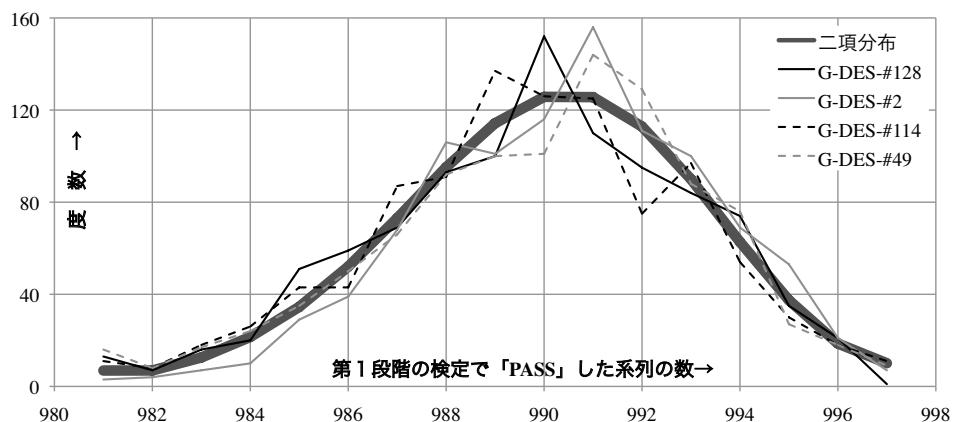


図 5.3 p-value がグレーゾーンにある検定項目の経験分布と理論分布の適合の様子 (G-DES)

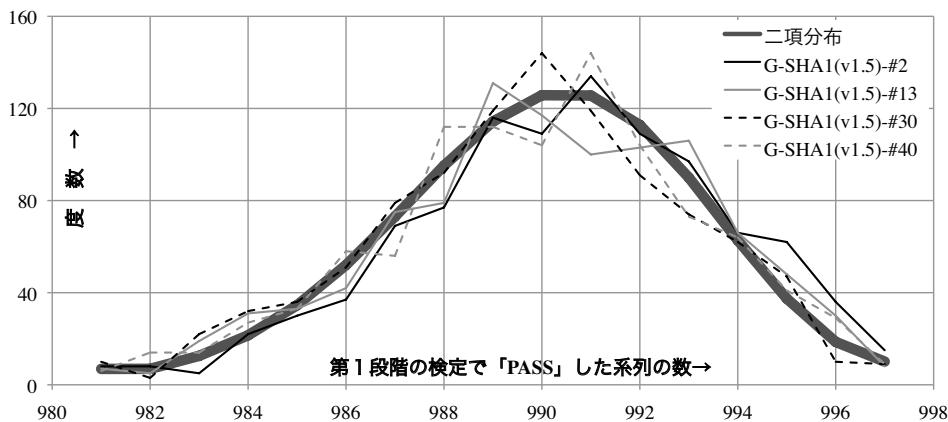


図 5.4 p-value がグレーゾーンにある検定項目の経験分布と理論分布の適合の様子 (G-SHA1(v1.5))

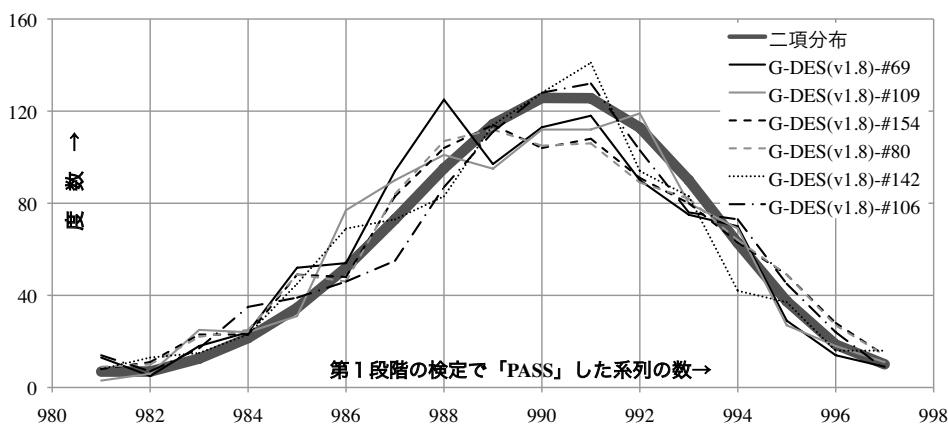


図 5.5 p-value がグレーゾーンにある検定項目の経験分布と理論分布の適合の様子 (G-DES(v1.8))

5.4.2 第1段階の検定に誤りがない検定項目の実験結果の説明

誤りの報告がない検定法（検定項目）については（表 5.5, 表 5.8），G-SHA1(v1.5) のブロック単位の等頻度検定（#2）と，G-DES(v1.8) の重なりのないテンプレート適合検定（#69）が 0.0001 を若干量下回ったが（いずれも 10^{-5} のオーダー），その他においては，p-value が極端に小さい値となるケースは見られなかった。重なりのないテンプレート適合検定（#7～#154）については，紙面の都合で表中に全ての p-value を示していないが，上記の G-DES(v1.8) の #69 以外で p-value が 0.0001 を下回るケースは見られなかった。

尚，p-value が 0.0001 を若干量下回った上記の 2 検定項目（G-SHA1(v1.5) のブロック単位の等頻度検定（#2），G-DES(v1.8) の重なりのないテンプレート適合検定（#69））は，「若干量」であることを理由に，本論文においては「グレーゾーン」として扱い様子を見るこにする。

3 つの乱数生成法をとおして，p-value が「グレーゾーン」にあるケースは，表 5.7, 表 5.8 に示す

計 22箇所存在した(全 880 中 22 箇所). これらについては, 5.3.4 節に従い, 二項分布への適合以外のその他の手段を併用して総合的に判断する方針とする. その他の手段として, 本論文においては母分散既知での母平均の区間推定, および, 母分散の区間推定(それぞれ有意水準 $\alpha = 0.01$, 表 5.8 参照)^{*23}, そして実験データの分布形のチェックを行った(図 5.1~図 5.5)^{*24}. 尚, 母分散既知での母平均の区間推定, および, 母分散の区間推定については, 理論上の平均値と分散の値が, 推定区間外となった場合に有為として棄却することにする.

この結果, 二項分布への適合度, 母分散既知での母平均の区間推定, 母分散の区間推定の 3つの検定(それぞれ有意水準 $\alpha = 0.01$)の全てにおいて棄却されたケースが G-DES のブロック単位の等頻度検定 (#2) であった. 3つの視点で棄却されているので, G-DES は, ブロック単位の等頻度検定 (#2) の視点において理想的なランダム性を有していない可能性が高い.

その他グレーゾーンにある検定項目においては, 母平均の区間推定, 母分散の区間推定のどちらかが棄却されても, 図 5.1~図 5.5 を考慮した結果より, 本論文においては特に顕著な差は見られないと判断する(明らかな乖離 / 積極的な有意性のみピックアップする).

ここで, p-value が 0.0001~0.01 程度では, もとより実験値と理論値に大差はないと考えられるので, 「グレーゾーンで不合格」となるケースはあるのか?との疑念が生じるかもしれない. 著者らの今まで実験の限りでは, 一検定項目の視点でランダム性が劣ることが知られている生成法を当該検定項目で検定した場合は, その結果の p-value が 0.0001~0.01 程度ならば, 分布の形および標本平均に明らかな偏りが現れることを確認している.

5.4.3 全体的な評価 ~ 亂数生成法の最終判定

前節までをふまえて, 本実験で扱った乱数生成法(G-AES, G-SHA1, G-DES)の最終判定(全体的な評価)を与える. 本論文においては, 誤りが報告されている検定法のうち, 重なりのあるテンプレート適合検定 (#155), ユニバーサル統計量検定 (#156), ブロック単位の最長連続検定 (#4) に関しては修正版を用いることにする. すなわち, 上記 3つの検定法の実験結果は表 5.6 である. また, これ以外の検定法の実験結果は表 5.5 である. ただし, DFT 検定 (#6) は, 注の*3 で示す理由により対象外とする. また, ランダム回遊検定 (#163~#170), ランダム回遊変量検定 (#171~#188) は, 4 章の冒頭で述べた理由により対象外とする.

表 5.8 より, グレーゾーン(グレーゾーンを下回るものも含む)にある計 22 の検定項目のうち, G-DES のブロック単位の等頻度検定 (#2) は, 二項分布への適合度, 母平均の推定, 母分散の推定の 3つの検定において有意水準 $\alpha = 0.01$ のもとで棄却されたことを理由に, 「不合格」(「グレーゾーンで不合格」と判定する). その他の検定項目については, 母分散の推定または, 母平均の推定のどちらか一方が棄却されるか, または, 双方とも棄却されないという結果となった. これらの検定項目は, 図 5.1~図 5.5 を考慮して, 経験分布と二項分布との間に大きな乖離は無いと判断できるので, 積極的な有意性の根拠を得られないことから, 本論文では「グレーゾーンで合格」と判定する.

これより, G-AES, G-SHA1, G-SHA1(v1.5), G-DES(v1.8) は, 全ての検定項目がグレーゾーン

^{*23} 各期待値は $E(\bar{X})=\mu = 990$, $E(U^2)=\sigma^2=9.9$ である.

^{*24} 文献 [26] では, 標本平均値, 標本分散値を参考とするのみであったが, 本論文ではそれぞれ区間推定を実施した. 尚, その他の手段として, どのような手法を採用すべきかについては検討の余地を残す.

以上で合格しているので、最終的に良質な擬似乱数生成法であると判定する。G-DES はブロック単位の等頻度検定 (#2) の視点で不合格と判定されるので、最終的にランダム性がやや劣る擬似乱数生成法であると判定する。

5.5 本判定法に関する考察

5.5.1 個々の検定法の誤りや誤差の影響

本判定法の要は、実験により得た経験分布 (*step-2* のヒストグラム) と、その理論上の分布^{*18} との適合度の計算と評価である。当然ながら、理論値が正確でないと正しい判定ができない。仮に被検定データが理想的なランダム性を有していた場合で、かつ、検定法に誤りが含まれる場合は、*step-3* で算出される p-value は一般的に小さい値となる。文献 [48] ~ [66] に示される内容を考察すると、誤りが指摘されている検定法は、以下の 3 つのタイプに分類できる。

- (1). 検定法の理論的な誤り
- (2). 近似計算が使われることによる誤差
- (3). χ^2 検定等の基本的な統計手段に含まれる誤差

(1) は DFT 検定、Lempel-Ziv 圧縮検定、ユニバーサル統計量検定で生じていた。(2) は重なりのあるテンプレート適合検定で生じていた。(2) と (3) の双方が生じていたものがブロック単位の最長連検定であった。一般的に (2) と (3) は軽視されがちだと思われる。しかし、ブロック単位の最長連検定 (#4) は、 χ^2 検定の制約^{*22} の限界付近で実施しているので、棄却率 0.01 を想定した検定は、実際には棄却率 0.010433 で実施されていた。この僅かな誤差が、表 5.5 の p-value を小さめの値としていた (5.4.1 節を参照。表 5.6(修正版での検定結果) も参照)。もし、この僅かな誤差に気付かなかつた場合は、表 5.5 の結果から、G-SHA1, G-DES, G-SHA1(v1.5), G-DES(v1.8) は、非ランダムであると判定されてもおかしくない。

このように、本判定法は、検定法に含まれる微小な誤差に敏感に反応する。従って、本判定法を利用する上では、検定法の全過程を通して含まれる誤差 ((1) ~ (3)) は極力小さく抑えられていなければならない。しかし現状では、この誤差の見積もりはされていない。この見積もりは難しい場合がある。例えば、 χ^2 分布は多項分布の近似として用いられる訳だが、自由度と総度数が大きくなると、多項分布の累積分布を求めるることは計算量的に困難になる。この課題の達成は現実的に難しいかもしれない。この点は今後の課題である。

5.5.2 グレーゾーンについて

5.3.4 節では、本判定法の *step-3* で得られる p-value が、概ね 0.0001 以上 0.01 未満の場合を「グレーゾーン」として扱うことを述べた。「グレーゾーン」では、他の手段を併用して、経験分布と、その理論上の分布の乖離を調べ、両者の乖離が明らかでない場合は、「グレーゾーンで合格」として扱うことを見た。一方、前節 (5.5.1 節) では、本判定法は、検定法に含まれるごく僅かな誤差をも検知する特徴があり、また、現状では、5.5.1 節で示した (1) ~ (3) の全段階を通して含まれる誤差の見積もりはされていないことを述べた (難しい場合がある)。この現状を考慮すると、p-value が 0.01 未

満となった場合でも、それは、被検定データがランダム性を有するにもかかわらず検定法に僅かな誤差が含まれるためなのか（付録 C.1 の (B-2) のタイプ）、或は、検定法は正確で被検定データが僅かに非ランダムであるのか（付録 C.1 の (B-1) のタイプ）の区別がつかない。つまり、p-value が 0.01 未満となった場合でも、一方的に被検定データが非ランダムであると決定できない。従って、現実的に、かつ、合理的に、被検定データのランダム性を検定しようとするならば、本判定法において「グレーゾーン」を設置することは、むしろ適切だと考える。

5.5.3 本判定法のもう 1 つの側面

本判定法は、個々の検定法が正確なときに、被検定データのランダム性を正確に判定できるが、一方で、これとは逆に、良質なランダム性を有する被検定データが与えられたときには、個々の検定法が正しく設計されているか否かを判定できる。そこで、あらゆる種類の乱数生成法を本判定法で判定したときに、p-value が小さい値を取る傾向にある検定法が発見されたならば、その検定法には誤りが含まれている可能性が高いと経験的に判断できる。先の実験に関しては、誤りの報告がされている検定法のうち、DFT 検定 (#6)、Lempel-Ziv 圧縮検定（削除）、重なりのあるテンプレート適合検定 (#155)、ユニバーサル統計量検定 (#156) の p-value は、どの乱数生成法においても極めて小さい値となった（表 5.5 参照）。これらは、本判定法により検定法の誤りを経験的に検知した例である。すなわち、第 1 段階の検定に使われる新たな検定法が提案されたならば、その検定法が正しく設計されているか否かを、本判定法でチェックするという使い方もある。

5.6 本章のまとめ

本論文では、NIST 亂数検定の Proportion 評価が極めて曖昧に終わる点に関して、最終的な合否が明確に与えられる判定法の一案を述べた。それは、NIST 亂数検定を複数 set 実施して、set 每の合格数に関するヒストグラム（実験から得た経験分布）とその理論上の分布との適合度を見るものである。本判定法では、全ての検定項目において両者の適合が良いときに乱数生成法のランダム性は良いと判断できるため、最終評価（全体評価）が明確となる。一方で、NIST 亂数検定に採用されている検定法の誤りに関する報告が後を絶たない。また、これと関係して、検定法の全過程を通して含まれる誤差量が正確に見積もられていない（これは困難な場合がある）。従って、両者の適合度が合格ラインを微妙に下回った場合でも、それは、検定法に含まれる誤差の影響である可能性を捨て切れない。そこで本判定法においては、明らかに合否が判定できる領域の中間にグレーゾーンを設けた。そして、p-value がグレーゾーンにある検定項目に関しては、他の手段によって両者の乖離を調べ、このときに特に明らかな乖離が見つけられない場合は、本判定法ではグレーゾーンで合格させるという考え方を示した。尚、本判定法による判定の精度を上げるためにも、個々の検定法に含まれる誤差を極力少なく抑えなければならないことを示した。特に理論値の計算において近似が使われている場合や、 χ^2 検定の制約に対して十分なマージンがあるか否か等について、いまいちど見直す必要があることを述べた。今後の課題としては、本判定法によって得られる結果の信頼性をさらに向上させる目的で、検定の全過程を通して含まれる誤差を把握し、誤差とグレーゾーンとの関係を詳細に把握することが挙げられる。および、本判定法を、今回対象外としたランダム回遊検定（Random Excursion Test）と、ランダム回遊変量検定（Random Excursion Variant Test）にも対応させることが挙げられる。

第 6 章

結 論

本論文の前半では、1次元非線形写像から得られる系列がランダムな挙動を呈することや初期条件に敏感な性質を示し、これらの系列をランダムビット列の生成源（抽出源）として利用する案について触れた。次いで、テント写像を反復する度に最上位ビット、或は任意桁目のビットを抽出して擬似ランダムビット列を構成するといった、ごく初步的な擬似ランダムビット生成系があったと仮定して、当該系列を生成し得る初期値、ならびにパラメータの推測法を検討し、どの程度までにシード依存値が推測できるかということについて述べた。本生成系において初期値とパラメータはシード（鍵）依存値であることから、本推測法はその安全性解析と位置付けられるため重要である。そして、推測が困難となるケースについて整理し、本論文で扱った推測法によって解析が困難となる擬似ランダムビット列生成法の一例を示した。尚、ここで示した内容は、今後、より発展的な擬似ランダムビット列生成法を設計するに際して重要な情報を与えるものと考えられる。

本論文の後半では、暗号技術分野で今日標準的に使われている NIST 亂数検定法（統計的乱数検定）に含まれる検定法の誤りに関し、著者らの報告も含め数多くの報告があることを述べ、また、NIST による最終的なランダム性の判定法が極めて曖昧であること等の課題がある点を述べた。これに対して本論文では、NIST 亂数検定法を用いて合理的かつ明確にランダム性の判定を与えるための方法を提案した。そして経験的に良質だとされる（あるいは良質でないという報告のない）擬似乱数生成法を用いた判定実験例を用い提案した判定法の妥当性を示した。

今後の課題としては、まず非線形写像を用いた擬似乱数生成法に対する解析面としては、本論文で扱った以外の視点をも取り込んで解析法を進化させていくこと、ならびに、より多くの視点をも考慮した上で解析が困難となるケースを整理し、非線形写像を利用した擬似乱数生成法の設計指標としてまとめていくことが挙げられる。

NIST の乱数検定に関しては、まず当検定法に含まれる個々の検定法（第1段階の検定）の誤りが修正されること、あるいは誤差が最小に抑えられるように修正されることを強く主張したい。また、ランダム性の最終判定（第2段階の検定）においては、本論文で示した判定法、或は相応のものに代替する等によって、評価者および評価結果を見た第三者が明確に理解できるような最終判定の枠組みの重要性を主張することが挙げられる。また、著者らの有する数多くの擬似乱数生成法の判定結果の例や考え方を Web で公表するなどして、検定者に多くの情報を提供する等が挙げられる。

付録 A

力オス数理に関する諸定義，定理類

A.1 位相共役（位相同形）

定義 A.1.1 ((位相共役(位相同形)) 2つの写像 f と g を考える。 $f : I \rightarrow I$, $g : J \rightarrow J$ とする。写像 f と g が位相共役の関係にある(位相同形である)とは, $f = h \circ g \circ h^{-1}$ を満たす1対1写像 h が存在することを言う。すなわち, $x_i \in I$ と, $z_i \in J$ に対して, $x_i = h(z_i)$, $z_i = h^{-1}(x_i)$ となる $h(\cdot)$ が存在し, また, このとき, $x_{i+1} = f(x_i) = h(g(h^{-1}(x_i)))$, $z_{i+1} = g(z_i) = h^{-1}(f(h(z_i)))$ である。

(文献 [1],[6],[7] を参照した)

$$\begin{array}{ccc} x_i \in I & \xrightarrow{f} & x_{i+1} \in I \\ h^{-1} \downarrow & & \uparrow h \\ z_i \in J & \xrightarrow{g} & z_{i+1} \in J \end{array}$$

A.1.1 パラメータ $b = 4$ のロジスティック写像 L_4 とパラメータ $a = 2$ のテント写像 f_2 の位相共役の関係 h

パラメータ $b = 4$ のロジスティック写像 $L_4 : I \rightarrow I$ ($I = [0, 1]$) と, パラメータ $a = 2$ のテント写像 $f_2 : J \rightarrow J$ ($J = [0, 1]$) には以下に示す位相共役の関係が存在する。

$$\begin{aligned} x_{i+1} &= L_4(x_i) \\ z_{i+1} &= f_2(z_i) \end{aligned}$$

としたとき,

$$h^{-1}(x) = \frac{2}{\pi} \sin^{-1} \sqrt{x} \quad (\text{A.1})$$

$$h(z) = \sin^2 \frac{\pi}{2} z \quad (\text{A.2})$$

A.1.2 パラメータ $b = 4$ のロジスティック写像 L_4 とパラメータ $c = 2$ の平方写像 Q_2 の位相共役の関係 h

パラメータ $b = 4$ のロジスティック写像 $L_4 : I \rightarrow I$ ($I = [0, 1]$) と、パラメータ $c = 2$ の平方写像 $Q_2 : J \rightarrow J$ ($J = [-2, 2]$) には以下に示す位相共役の関係が存在する。

$$\begin{aligned} x_{i+1} &= L_4(x_i) \\ z_{i+1} &= Q_2(z_i) \end{aligned}$$

としたとき、

$$h^{-1}(x) = -4x + 2 \quad (\text{A.3})$$

$$h(z) = -z/4 + 1/2 \quad (\text{A.4})$$

A.2 リヤブノフ指数

テント型写像等の非線形写像を扱うとき、写像の度に、初期の僅かな誤差が指數関数的に広がっていく性質（初期値鋭敏性）を示すものとして、よく Lyapunov 指数が用いられる。以下に、Lyapunov 指数について説明する（文献 [6] の 2.5 節、文献 [5] 参照）。

ある x_0 と、 x_0 から微少量 δx 離れた $x_0 + \delta x$ の 2 つの初期値を考える。 $x_{i+1} = \tau(x_i)$ で規定される 1 次元写像によって、両者の差は、 n 回写像後に以下に広がる。

$$\frac{|\tau^n(x_0 + \delta x) - \tau^n(x_0)|}{|\delta x|} \quad (\text{A.5})$$

もし両者が指數関数的に離れるとするとき、

$$\frac{|\tau^n(x_0 + \delta x) - \tau^n(x_0)|}{|\delta x|} = e^{n \cdot \lambda(x_0, \tau)} \quad (\text{A.6})$$

を満たす $\lambda(x_0, \tau) > 0$ が存在するはずである。十分大きな n と十分小さな δx については以下がいえる。

$$\begin{aligned} \lambda(x_0, \tau) &= \lim_{n \rightarrow \infty} \frac{1}{n} \lim_{\delta x \rightarrow 0} \log_e \left| \frac{\tau^n(x_0 + \delta x) - \tau^n(x_0)}{\delta x} \right| \\ &= \lim_{n \rightarrow \infty} \frac{1}{n} \log_e \left| \frac{d\tau^n(x)}{dx} \right|_{x=x_0} \end{aligned} \quad (\text{A.7})$$

ここで、微分の連鎖則（以下式 (A.8)）を利用すると、

$$\frac{d\tau^n(x)}{dx} \Big|_{x=x_0} = \tau'(x_{n-1}) \cdot \tau'(x_{n-2}) \dots \tau'(x_0) \quad (\text{A.8})$$

$$\lambda(x_0, \tau) = \lim_{n \rightarrow \infty} \frac{1}{n} \log_e \sum_{i=0}^{n-1} |\tau'(x_i)| \quad (\text{A.9})$$

と整理される。 $\lambda(x_0, \tau)$ を Lyapunov 指数という。

A.2.1 傾き $1 < a \leq 2$ のテント型写像における初期誤差の広がり

以下に、テント型写像（式 (2.1)）について λ_{tent} を見積もる。 $f_a(x)$ は 1 次関数であることから、 $f_a(x)$ の 1 階導関数は、 x に関係せず $|f'(x)| = a$ （定数）となる。式 (A.9) について、有限の n に対しては以下を得る。

$$\begin{aligned}\lambda_{\text{tent}} &= \frac{1}{n} \log_e \sum_{i=0}^{n-1} |f'(x_i)| \\ &= \frac{1}{n} \log_e \sum_{i=0}^{n-1} a = \frac{1}{n} \log_e na = \frac{1}{n} \cdot n \log_e a \\ &= \log_e a > 0 \quad (\because 1 < a \leq 2)\end{aligned}\tag{A.10}$$

つまり、テント写像はパラメータが $1 < a \leq 2$ のときに初期値鋭敏性をもつ。

付録 B

グレイコードおよびグレイコードに基づく推測法に関する付録

Baptista[32] , および Alvarez ら [33] は , 1 次元非線形写像の反復回数を暗号文とする暗号化手法を示した . 一方で , 当該暗号系に対する解析法として , Alvarez ら [20][21] , Wu ら [22] は , 以下に示す最上位ビット抽出系列とグレイコードの関係 [29][30][22] を利用した解析法を示した . ここでは上記の重要な部分を記す .

B.1 Baptista , および Alvarez らによる 1 次元非線形写像を利用した暗号化手法 [32][33]

Baptista[32] , および Alvarez ら [33] は , 1 次元非線形写像の反復回数を暗号文とする暗号化手法を示した . 以下において , この暗号化手法の本質的な部分について簡潔にまとめたものを述べる .

[暗号化の手順]

1. 写像 $f : I \rightarrow I$ とする . 初期値を $x_0 \in I$ とする . 初期値 x_0 と利用する写像のパラメータは , あらかじめ暗号化側と復号側で共有されているものとする . 1 バイト (8 ビット) の平文 $c \in X$, $X = \{\xi \mid 0 \leq \xi < 256, \xi \in \mathbb{Z}\}$ に対応する区間 $I_c \subset I$ を決める . ただし $I_u \cup I_v = \phi$ ($u \neq v$, $u, v \in X$) とする . $I_0 \cap I_1 \cap \cdots \cap I_{255} \subseteq I$ である .
2. 暗号化は $x_n = f^n(x_0) \in I_c$ となるような n を探してこれを暗号文 $e (= n)$ とする ($e \in \mathbb{N}$) .
3. 復号は $x_e = f^e(x_0)$ として $x_e \in I_d$ であれば d を復号文とする .
4. この暗号系では , 初期値 x_0 と使われる写像のパラメータが暗号鍵 (Key) となる .

B.2 グレイコード (Gray Code) [31]

B.2.1 グレイコードについて

グレイコードとはグレイによって示された符号語のことをいい , バイナリコードと以下に示す対応関係にある .

定義 B.2.1 (グレイコードとバイナリコードの対応関係) n ビットのバイナリコードを $s =$

表 B.1 バイナリコードとグレイコードの関係(4ビット)

バイナリコード $s_0s_1s_2s_3 (= \mathbf{s})$	グレイコード $g_0g_1g_2g_3 (= \mathbf{g})$	グレイコードのオーダ $g_o(\mathbf{s}), \mathbf{s} = \tau^{-1}(\mathbf{g})$ ($G(\mathbf{g})$)
0000	0000	0/16
0001	0001	1/16
0010	0011	2/16
0011	0010	3/16
0100	0110	4/16
0101	0111	5/16
0110	0101	6/16
0111	0100	7/16
1000	1100	8/16
1001	1101	9/16
1010	1111	10/16
1011	1110	11/16
1100	1010	12/16
1101	1011	13/16
1110	1001	14/16
1111	1000	15/16

$\{s_0, s_1, \dots, s_{n-1}\}$ とする ($s_i = \{0, 1\}$). グレイコードとは, バイナリコードに対して以下に示す変換 τ によって得られた n ビットの $\mathbf{g} = \{g_0, g_1, \dots, g_{n-1}\}$ のことをいう ($g_i = \{0, 1\}$).

$$\mathbf{g} = \tau(\mathbf{s}) = \begin{cases} i = 0 \text{ のとき : } g_0 = s_0 \\ i \geq 1 \text{ のとき : } g_i = s_i \oplus s_{i-1} \end{cases} \quad (\text{B.1})$$

式 (B.1) より, 逆変換 τ^{-1} (グレイコードからバイナリコードへの変換) は以下の式 (B.2) として表せる.

$$\mathbf{s} = \tau^{-1}(\mathbf{g}) = \begin{cases} i = 0 \text{ のとき : } s_0 = g_0 \\ i \geq 1 \text{ のとき : } s_i = g_i \oplus s_{i-1} \end{cases} \quad (\text{B.2})$$

定義 B.2.2 (グレイコードのオーダ) グレイコードのオーダとは, グレイコードからバイナリコードに変換後の $\tau^{-1}(\mathbf{g}) \stackrel{\text{def}}{=} \mathbf{s}$ を 2進小数点数と見なしたときに, これを 10進小数点数に変換 (その変換を g_o とする) した値のことをいう. つまり, 以下の式 (B.3) のことをいう.

$$order = g_o(\tau^{-1}(\mathbf{g})) = g_o(\mathbf{s}) = \sum_{i=0}^{n-1} s_i / 2^{i+1} \quad (\text{B.3})$$

尚, 本稿では $g_o \circ \tau^{-1} = G$ と表すこととする.

$$order = g_o(\tau^{-1}(\mathbf{g})) = G(\mathbf{g}) \quad (\text{B.4})$$

B.3 平方写像の最上位ビット抽出系列とグレイコードの関係

Alvarez ら [29], および Cusick[30] によって示された, 平方写像 (quadratic map) からの最上位ビット抽出系列とグレイコードの関係を示す. 尚, 以下に示す定理の証明は文献 [29][30][22] を参照

されたい。

定義 B.3.1 (平方写像からの擬似ランダムビット列の生成 (最上位ビット抽出)) $x_0 \in I_c$, ($I_c = [-(1+\sqrt{1+4c})/2, (1+\sqrt{1+4c})/2]$) を初期値として, パラメータ c ($1 < c \leq 2$) の平方写像(式(B.5)) の n 回反復過程 $x_{i+1} = Q_c(x_i)$ ($0 \leq i < n$) で得られる計 $n+1$ 個の値 $\{x_0, x_1, \dots, x_n\}$ ($= \{x_i\}_{i=0}^n$) を考える。ここで扱う擬似ランダムビット列とは, 第 i 回目 ($i \geq 0$) の写像ごとに, 式(B.6) に従い x_i の最上位ビットを抽出して構成された計 $n+1$ ビットの系列 $\{b_0, b_1, \dots, b_n\}$ ($= \{b_i\}_{i=0}^n$) のことをいう。尚, ここでは当該擬似ランダムビット列の生成関数を $SQ_c(x_0, n)$ と表す。

$$\begin{aligned} Q_c : I_c &\mapsto I_c, (I_c = [-(1 + \sqrt{1 + 4c})/2, (1 + \sqrt{1 + 4c})/2]) \\ Q_c(x) &= x^2 - c \end{aligned} \quad (\text{B.5})$$

$$b_i = \begin{cases} 0 & (x_i \geq 0) \\ 1 & (x_i < 0) \end{cases} \quad (\text{B.6})$$

$$SQ_c(x_0, n) \equiv \{b_0, b_1, \dots, b_n\} \quad (= \{b_i\}_{i=0}^n) \quad (\text{B.7})$$

定義 B.3.2 (左シフト) 系列 $\{b_0, b_1, b_2, \dots, b_n\}$ が与えられたとき, 当該系列の i 回の左シフト $L^i(\cdot)$ とは以下のことを意味する。

$$\begin{aligned} L(\{b_0, b_1, b_2, \dots, b_n\}) &= \{b_1, b_2, \dots, b_n\} \\ L^2(\{b_0, b_1, b_2, \dots, b_n\}) &= \{b_2, b_3, \dots, b_n\} \\ L^i(\{b_0, b_1, b_2, \dots, b_n\}) &= \{b_i, b_{i+1}, \dots, b_n\} \end{aligned}$$

定義 B.3.3 (平方写像のシンボリック系列) 初期値を $x_0 = 0$ ($x = 0$ は平方写像 $Q_c(x)$ 式(B.5) が極小値を示す場所である) として, 定義 B.3.1 の生成法に従い生成された系列 $SQ_c(0, n)$ の左 1 ビットシフト系列, すなわち $L(SQ_c(0, n))$ のことを平方写像のシンボリック系列と呼ぶ。尚, $Q_c(0) = -c$ であるため, $L(SQ_c(0, n))$ は, $Q_c(0) = -c$ を新たな初期値として生成された $SQ_c(-c, n-1)$ に他ならない。

$$L(SQ_c(0, n)) = SQ_c(-c, n-1) \quad (\text{B.8})$$

本論文では $SQ_c(-c, n-1)$ (或は $SQ_c(-c, m)$, ($m \rightarrow \infty$)) もシンボリック系列とする。

定理 B.3.4 (初期値とグレイコードのオーダの関係) 2つの初期値 ξ_1, ξ_2 ($\xi_1, \xi_2 \in [-(1 + \sqrt{1 + 4c})/2, (1 + \sqrt{1 + 4c})/2]$) から, 定義 B.3.1 の生成法に従い生成された系列 $SQ_c(\xi_1, n)$, $SQ_c(\xi_2, n)$ を考える。 $SQ_c(\xi_1, n)$, $SQ_c(\xi_2, n)$ をグレイコードとみなしたとき, 以下に示す関係が常に成立する (図 B.1 参照)。

$$\xi_1 < \xi_2 \Rightarrow G(SQ_c(\xi_1, n)) \geq G(SQ_c(\xi_2, n)) \quad (\text{B.9})$$

定理 B.3.5 (グレイコードのオーダの最大値) 定義 B.3.1 の生成法に従い生成された系列 $SQ_c(x_0, n)$ の i 回左シフト系列 $L^i(SQ_c(x_0, n))$ を考えたとき ($1 \leq i < n$), 以下に示す関係が常に成立する。

$$G(L^i(SQ_c(x_0, n))) \leq G(SQ_c(-c, n-i)) \quad (\text{B.10})$$

すなわち, 定義 B.3.3 より, シンボリック系列が常にグレイコードのオーダの最大を与える (図 B.2 参照)。

定理 B.3.6 (パラメータとグレイコードのオーダの最大値) 2つのパラメータ η_1, η_2 , ($\eta_1, \eta_2 \in (1, 2]$) を考える。このとき以下に示す関係が常に成立する。

$$\eta_1 < \eta_2 \Rightarrow G(SQ_{\eta_1}(-\eta_1, n)) \geq G(SQ_{\eta_2}(-\eta_2, n)) \quad (\text{B.11})$$

すなわち、異なるパラメータのシンボリック系列に対するグレイコードのオーダ同士を比較したとき、パラメータが大きいほどグレイコードのオーダは大きい(図 B.3 参照)。

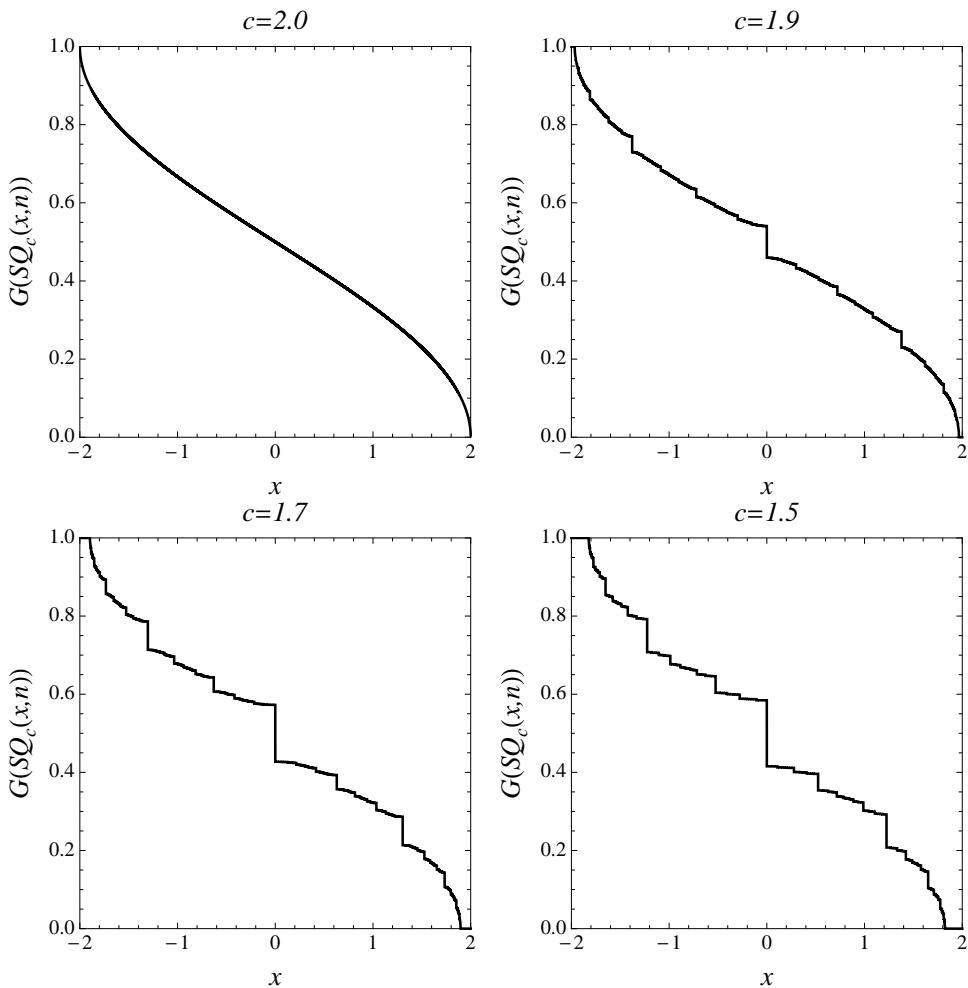


図 B.1 定理 B.3.4 の内容を示す図

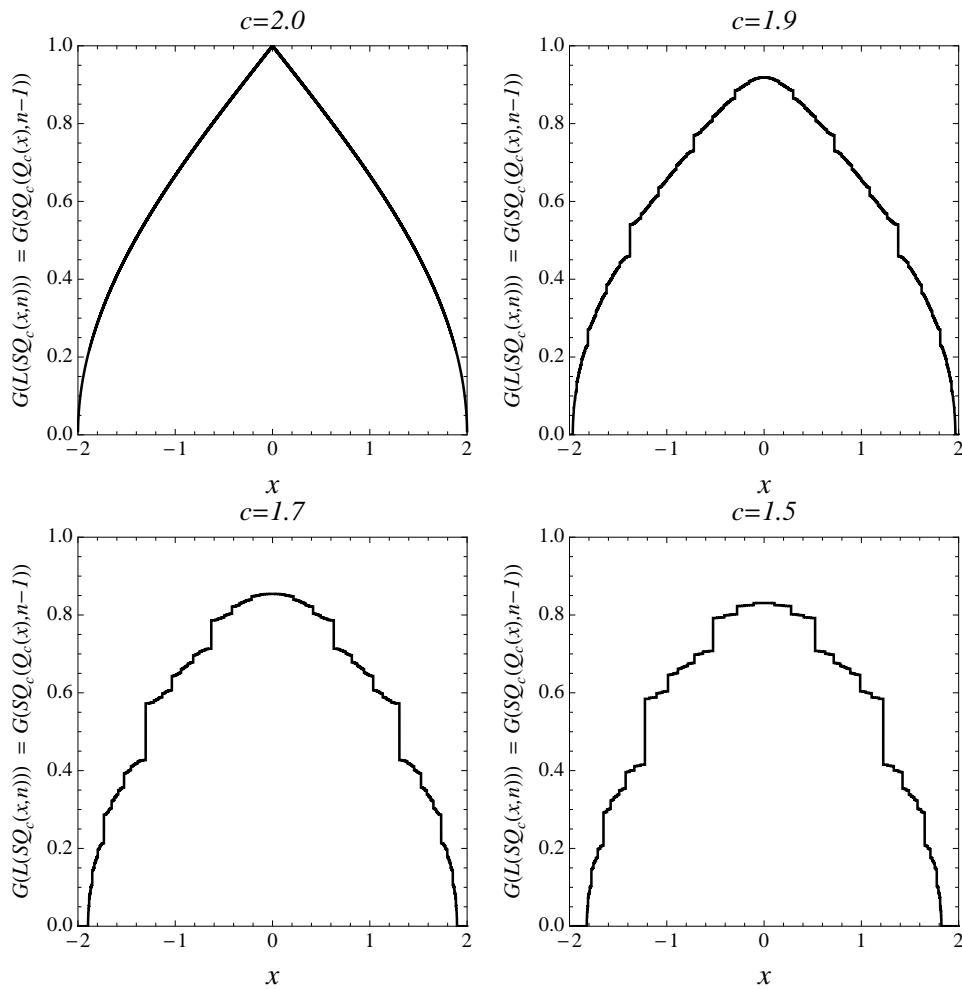


図 B.2 定理 B.3.5 の内容を示す図

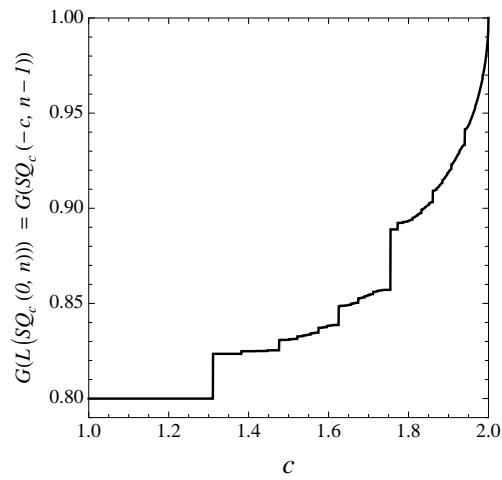


図 B.3 定理 B.3.6 の内容を示す図

B.4 Alvarez らの，平方写像からの最上位ビット抽出系列に対するグレイコードに基づく初期値推測法 [21]

B.3 節では，平方写像からの最上位ビット抽出系列とグレーコードの関係を示した。本節では，Alvarez らによる，平方写像からの最上位ビット抽出系列に対するグレイコードを用いた初期値推測法 [21] を記す。

推測法 B.4.1 (Alvarez らの初期値推測法 [21]) 初期値 x_0 ，パラメータ c ，写像の反復回数を n とする。定義 B.3.1 にて示される生成法から生成された擬似ランダムビット列を $\mathbf{b} \equiv \{b_i\}_{i=0}^n (= SQ_c(x_0, n))$ とする。パラメータ c ，および擬似ランダムビット列 \mathbf{b} が既知として与えられたとき，当該系列 \mathbf{b} を生成し得る初期値 x_0 の範囲を推測することをいう。

式 (B.5) より， $i = 1$ のときは $x_1 = x_0^2 - c$ なので $x_0 = \pm\sqrt{c + x_1}$ である。また，ビット抽出ルール式 (B.6) より， $b_0 = 0 \Rightarrow x_0 \geq 0$ ， $b_0 = 1 \Rightarrow x_0 < 0$ であることから，

$$\begin{cases} b_0 = 0 \Rightarrow x_0 = +\sqrt{c + x_1} \\ b_0 = 1 \Rightarrow x_0 = -\sqrt{c + x_1} \end{cases} \quad (\text{B.12})$$

である。 $i = 2$ のときは，

$$\begin{cases} \{b_0, b_1\} = \{0, 0\} \Rightarrow x_0 = +\sqrt{c + \sqrt{c + x_2}} \\ \{b_0, b_1\} = \{0, 1\} \Rightarrow x_0 = +\sqrt{c - \sqrt{c + x_2}} \\ \{b_0, b_1\} = \{1, 0\} \Rightarrow x_0 = -\sqrt{c + \sqrt{c + x_2}} \\ \{b_0, b_1\} = \{1, 1\} \Rightarrow x_0 = -\sqrt{c - \sqrt{c + x_2}} \end{cases} \quad (\text{B.13})$$

である。ここで， $w_i = 1 - 2b_i$ すると，

$$w_i = 1 - 2b_i = \begin{cases} +1 & (b_i = 0) \\ -1 & (b_i = 1) \end{cases} \quad (\text{B.14})$$

$i = n$ のときは，

$$x_0 = w_0 \sqrt{c + w_1 \sqrt{c + w_2 \sqrt{c + \cdots + w_n \sqrt{c + x_n}}}} \quad (\text{B.15})$$

を得る。

また，与えられた擬似ランダムビット列 $\mathbf{b} \equiv \{b_i\}_{i=0}^n (= SQ_c(x_0, n))$ のグレイコードのオーダーは，式 (B.4) より $G(\mathbf{b}) \stackrel{\text{def}}{=} O_G$ である。次に初期値 x_0 の範囲を求める。Alvarez ら [21] によると，ここで定理 B.3.4 の結果を利用して，グレイコードのオーダーが O_G となる系列，すなわち \mathbf{b} を生成する初期値は， $O_{G+1} \stackrel{\text{def}}{=} (O_G 2^{n+1} + 1)/2^{n+1}$ となる系列 \mathbf{b}_{+1} を生成する初期値 x_{0+} と， $O_{G-1} \stackrel{\text{def}}{=} (O_G 2^{n+1} - 1)/2^{n+1}$ となる系列 \mathbf{b}_{-1} を生成する初期値 x_{0-} の間にあるという関係を利用する。

具体的には， \mathbf{b} と \mathbf{b}_{+1} のビット列が互いに等しいビットを保っている間 ($m_+ \leq n$) までのビット列 \mathbf{s}_{+1} について式 (B.14) によるビット列 \mathbf{w}_{+1} を作成し，式 (B.15) を $x_{m+} = 0$ として得られる初期値 x_{0+} と， \mathbf{b} と \mathbf{b}_{-1} のビット列が互いに等しいビットを保っている間 ($m_- \leq n$) までのビット列 \mathbf{s}_{-1} について式 (B.14) によるビット列 \mathbf{w}_{-1} を作成し，式 (B.15) を $x_{m-} = 0$ として得られる初期値 x_{0-} との間にあるとして求める^{*1}。

以下に具体的な推測例を示す。

例 B.4.2 (Alvarez らの初期値推測法 [21] による推測例) $c = 1.8, x_0 = 0.232323, n = 10$ とする。このとき，定義 B.3.1 にて示される生成法にて，計 $n + 1 = 11$ ビットの擬似ランダムビット列 $SQ_c(x_0, n) \equiv \mathbf{b} = \{0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1\}$ を得る。系列 \mathbf{b} のグレーコードのオーダは式 (B.4) より $O_G = G(\mathbf{b}) = 877/2048$ である。従って， $O_{G+1} = (877+1)/2048, O_{G-1} = (877-1)/2048$ である。一方で，式 (B.3) の関係から， $O_{G+1} = 878/2048$ となる系列は $\mathbf{b}_{+1} = \{0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1\}$ で， $O_{G-1} = 876/2048$ となる系列は $\mathbf{b}_{-1} = \{0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0\}$ が判る。それぞれの系列 $\mathbf{b}_{+1}, \mathbf{b}_{-1}$ が， \mathbf{b} と互いに等しいビットを保っているまでのビット列 $\mathbf{s}_{+1}, \mathbf{s}_{-1}$ を求める。 \mathbf{b}_{+1} と \mathbf{b} は第 8 ビット目 ($m_+ = 8$) までが等しく^{*2}， \mathbf{b}_{-1} と \mathbf{b} は第 9 ビット目 ($m_- = 9$) までが等しい^{*2} ので以下の式となる。

$$\begin{aligned}\mathbf{b} &= \{0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1\} \\ \mathbf{b}_{+1} &= \{0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1\} \\ \mathbf{s}_{+1} &= \{0, 1, 0, 1, 1, 0, 1, 1, 0\}\end{aligned}\tag{B.16}$$

$$\begin{aligned}\mathbf{b} &= \{0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1\} \\ \mathbf{b}_{-1} &= \{0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0\} \\ \mathbf{s}_{-1} &= \{0, 1, 0, 1, 1, 0, 1, 1, 0, 1\}\end{aligned}\tag{B.17}$$

次に式 (B.14) より，それぞれのビット列 $\mathbf{s}_{+1}, \mathbf{s}_{-1}$ に対応するビット列 $\mathbf{w}_{+1}, \mathbf{w}_{-1}$ を求める。

$$\begin{aligned}\mathbf{s}_{+1} &= \{0, 1, 0, 1, 1, 0, 1, 1, 0\} \\ \mathbf{w}_{+1} &= \{1, -1, 1, -1, -1, 1, -1, -1, 1\}\end{aligned}\tag{B.18}$$

$$\begin{aligned}\mathbf{s}_{-1} &= \{0, 1, 0, 1, 1, 0, 1, 1, 0, 1\} \\ \mathbf{w}_{-1} &= \{1, -1, 1, -1, -1, 1, -1, -1, 1, -1\}\end{aligned}\tag{B.19}$$

^{*1} $x_{m+} = 0, x_{m-} = 0$ として式 (B.15) を解く理由は，平方写像では $x = 0$ が 0, 1 ビット抽出領域式 (B.6) の境界値であることと関係している。

^{*2} 定義より先頭ビットは第 $i = 0$ ビット目として扱うことに注意。

$\mathbf{w}_{+1}, \mathbf{w}_{-1}$ を利用して、それぞれ式 (B.15) を $x_{m+} = 0, x_{m-} = 0$ として解くと、

$$\begin{aligned} x_{0+} &= +\sqrt{c - \sqrt{c + \sqrt{c - \sqrt{c + \sqrt{c - \sqrt{c + \sqrt{c - \sqrt{c + \sqrt{c - \sqrt{c + \sqrt{c}}}}}}}}}}} \\ &= 0.22542076157765326 \end{aligned} \quad (\text{B.20})$$

$$\begin{aligned} x_{0-} &= +\sqrt{c - \sqrt{c + \sqrt{c - \sqrt{c + \sqrt{c - \sqrt{c + \sqrt{c - \sqrt{c + \sqrt{c + \sqrt{c - \sqrt{c}}}}}}}}}}} \\ &= 0.24344132797929077 \end{aligned} \quad (\text{B.21})$$

を得る。上記の x_{0+}, x_{0-} を境界とする範囲 $(0.22542076157765326, 0.24344132797929077)$ が、ここで求める初期値解である。

B.5 テント写像の最上位ビット抽出系列とグレイコードの関係

Alvarez ら [29]、および Cusick[30] によって示された、平方写像 (quadratic map) からの最上位ビット抽出系列とグレイコードの関係は、テント写像やロジスティック写像においても成立する^{*3}。Wu ら [22] はこの関係を利用してロジスティック写像におけるパラメータ推測法を示した。以下では、テント写像からの最上位ビット抽出系列とグレイコードの関係について触れる。定理の証明は文献 [29][30][22] を参照されたい。

定義 B.5.1 (テント写像のシンボリック系列) 初期値を $x_0 = 1/2$ (テント写像 $f_a(x)$ 式 (B.5) が極大値を示す場所) として、定義 3.2.1 の生成法に従い生成された系列 $S_a(1/2, n)$ の左 1 ビットシフト系列 (定義 B.3.2)，すなわち $L(S_a(1/2, n))$ のことをテント写像のシンボリック系列と呼ぶ。尚、 $S_a(1/2) = a/2$ であるため、 $L(S_a(1/2, n))$ は、 $f_a(1/2) = a/2$ を新たな初期値として生成された $S_a(a/2, n - 1)$ に他ならない。

$$L(S_a(1/2, n)) = S_a(a/2, n - 1) \quad (\text{B.22})$$

本論文では $S_a(a/2, n - 1)$ (或は $S_a(a/2, m)$, ($m \rightarrow \infty$)) もシンボリック系列とする。

定理 B.5.2 (初期値とグレイコードのオーダの関係) 2つの初期値 ξ_1, ξ_2 ($\xi_1, \xi_2 \in [0, 1]$) から、定義 3.2.1 の生成法に従い生成された系列 $S_a(\xi_1, n)$, $S_a(\xi_2, n)$ を考える。 $S_a(\xi_1, n)$, $S_a(\xi_2, n)$ をグレイコードとみなしたとき、以下に示す関係が常に成立する (図 B.4 参照)。

$$\xi_1 < \xi_2 \Rightarrow G(S_a(\xi_1, n)) \leq G(S_a(\xi_2, n)) \quad (\text{B.23})$$

定理 B.5.3 (グレイコードのオーダの最大値) 定義 3.2.1 の生成法に従い生成された系列 $S_a(x_0, n)$ の i 回左シフト系列 $L^i(S_a(x_0, n))$ を考えたとき ($1 \leq i < n$)、以下に示す関係が常に成立する。

$$G(L^i(S_a(x_0, n))) \leq G(S_a(a/2, n - i)) \quad (\text{B.24})$$

すなわち、定義 B.5.1 より、シンボリック系列が常にグレイコードのオーダの最大を与える (図 B.5 参照)。

定理 B.5.4 (パラメータとグレイコードのオーダの最大値) 2つのパラメータ η_1, η_2 , ($\eta_1, \eta_2 \in (1, 2]$) を考える。このとき以下に示す関係が常に成立する。

$$\eta_1 < \eta_2 \Rightarrow G(S_{\eta_1}(\eta_1/2, n)) \leq G(S_{\eta_2}(\eta_2/2, n)) \quad (\text{B.25})$$

すなわち、異なるパラメータのシンボリック系列に対するグレイコードのオーダ同士を比較したとき、パラメータが大きいほどグレイコードのオーダは大きい (図 B.6 参照)。

^{*3} 写像関数形が写像の定義域を中心に対象で、写像の中心に極大値 / 極小値を持つような凸型の写像

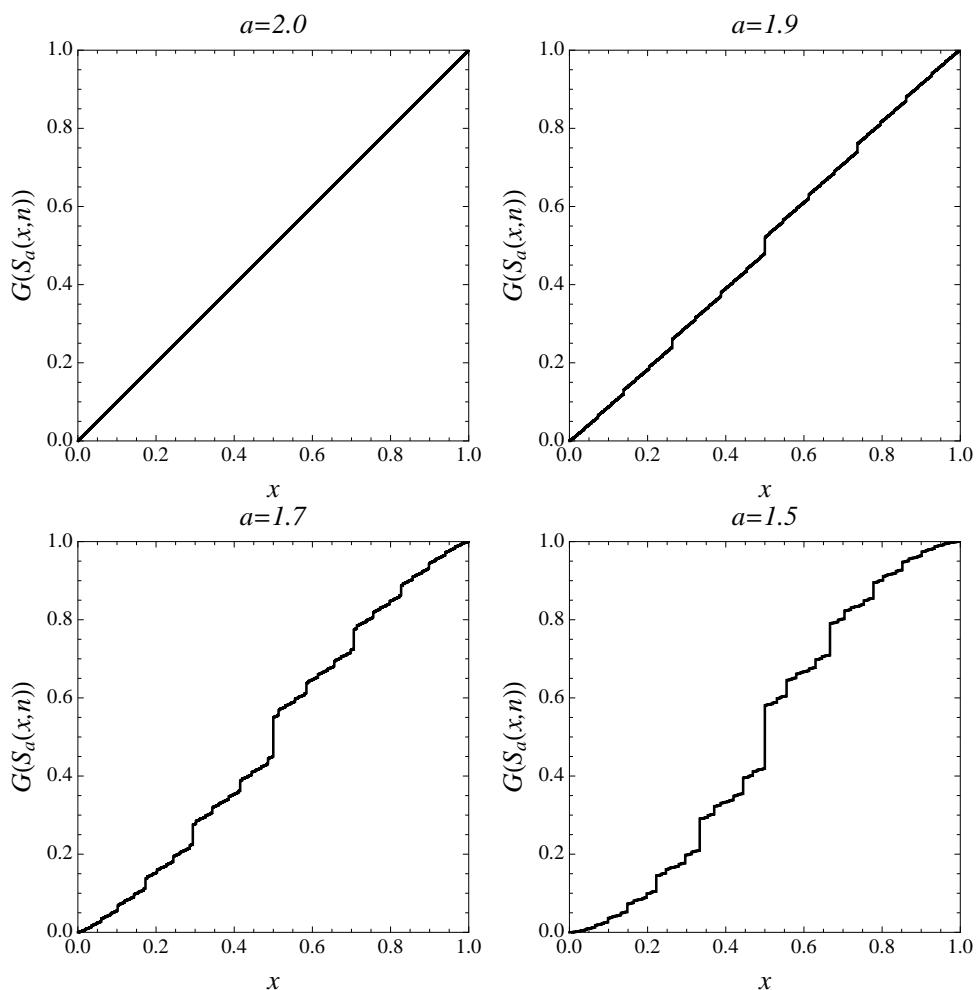


図 B.4 定理 B.5.2 の内容を示す図

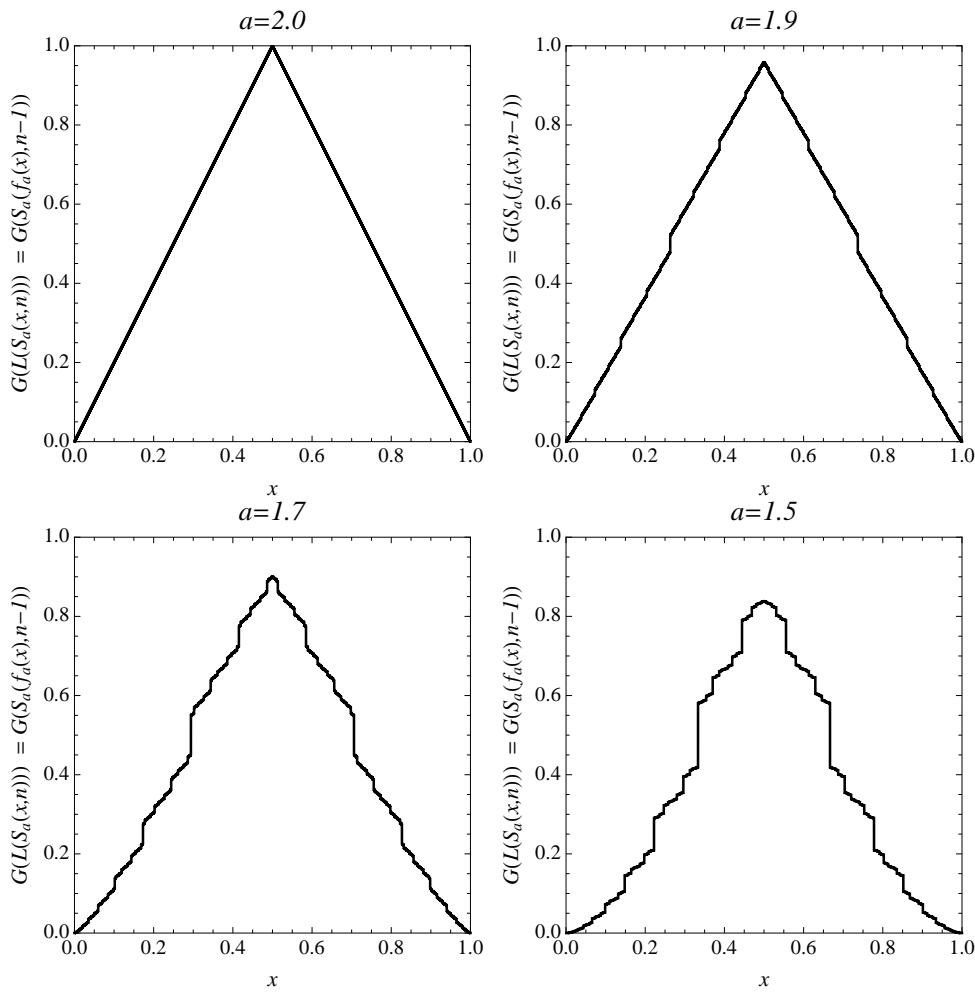


図 B.5 定理 B.5.3 の内容を示す図

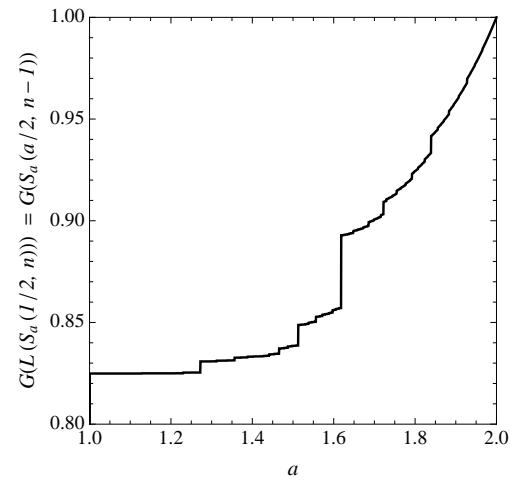


図 B.6 定理 B.5.4 の内容を示す図

付録 C

NIST 乱数検定 / 統計検定に関する付録

C.1 提案する判定法において，p-value が限りなく 1 または 0 に近い場合として考えられるパターン

p-value が限りなく 1 に近い場合

- (A-1). 検定法が棄却率 1% の検定として正確に設計されている場合で，かつ，被検定データが検定法の視点でのランダム性を有する場合 .
- (A-2). 検定法が棄却率 1% の検定として正確に設計されていないにも関わらず，結果として，被検定データのうち 1% が検定法によって棄却される場合 .
(この場合は被検定データはランダム性を有していない)

p-value が限りなく 0 に近い場合

- (B-1). 検定法が棄却率 1% の検定として正確に設計されている場合で，かつ，被検定データが検定法の視点でのランダム性を有していない場合 .
- (B-2). 被検定データがランダム性を有しているにも関わらず，検定法が棄却率 1% の検定として正確に設計されていない場合 .
- (B-3). 検定法が棄却率 1% の検定として正確に設計されていない場合で，かつ，被検定データがランダム性を有していない場合で，かつ，(A-2) でない場合 .

C.2 提案する判定法によるランダム性判定実験結果（全データ）

表 C.1 G-AES⁽¹⁾,G-SHA1⁽²⁾,G-DES⁽³⁾,G-SHA1(v1.5)⁽⁴⁾,G-DES(v1.8)⁽⁵⁾ から生成した系列に対する、本判定法の step-3 におけるランダム性判定実験結果を表す p-value 全データ（その 1）

検定項目 番号	検定法 略式名称	G-AES ⁽¹⁾	G-SHA1 ⁽²⁾	G-DES ⁽³⁾	G-SHA1 (V1.5) ⁽⁴⁾	G-DES (V1.8) ⁽⁵⁾
#1	Frq	0.511642	0.587573	0.416057	0.044452	0.736605
#2	BlkFrq	0.505586	0.046849	0.002170	1.13E-05	0.012443
#3	Run	0.036357	0.372141	0.646333	0.684385	0.471442
#4	LngRun	0.017280	0.731343	0.190524	0.579188	0.538502
#5	Rank	0.982126	0.132229	0.433084	0.300382	0.379525
#6	DFT	8.00E-118	7.25E-116	9.71E-138	9.62E-99	2.84E-94
#7	N-ovlp	0.574160	0.001955	0.854451	0.512532	0.206539
#8	N-ovlp	0.495635	0.193384	0.211141	0.144984	0.811562
#9	N-ovlp	0.895502	0.335857	0.170103	0.885942	0.357894
#10	N-ovlp	0.286166	0.965022	0.203053	0.993881	0.344565
#11	N-ovlp	0.642199	0.577144	0.852020	0.121568	0.548005
#12	N-ovlp	0.506667	0.115523	0.657728	0.092233	0.610185
#13	N-ovlp	0.416096	0.299640	0.801172	0.687533	0.834210
#14	N-ovlp	0.849016	0.738843	0.204527	0.003545	0.578575
#15	N-ovlp	0.761109	0.395631	0.837293	0.637538	0.495224
#16	N-ovlp	0.654873	0.496167	0.921083	0.023331	0.181298
#17	N-ovlp	0.783151	0.155071	0.822994	0.449619	0.202167
#18	N-ovlp	0.749527	0.154006	0.481512	0.569412	0.133413
#19	N-ovlp	0.001220	0.031070	0.143747	0.900551	0.228789
#20	N-ovlp	0.535671	0.959583	0.260050	0.257296	0.030461
#21	N-ovlp	0.244918	0.606975	0.202354	0.581686	0.025729
#22	N-ovlp	0.091323	0.381036	0.362234	0.015028	0.184329
#23	N-ovlp	0.044421	0.629151	0.251909	0.228472	0.017944
#24	N-ovlp	0.909214	0.320296	0.285420	0.923877	0.567321
#25	N-ovlp	0.461060	0.627906	0.622523	0.769024	0.636734
#26	N-ovlp	0.079567	0.694263	0.033757	0.890758	0.524787
#27	N-ovlp	0.383319	0.961733	0.324576	0.359305	0.549204
#28	N-ovlp	0.517136	0.098154	0.258546	0.381516	0.522965
#29	N-ovlp	0.751913	0.729503	0.781000	0.659807	0.334250
#30	N-ovlp	0.625921	0.676679	0.491262	0.787557	0.162841
#31	N-ovlp	0.996693	0.447873	0.796911	0.006676	0.150970
#32	N-ovlp	0.858729	0.345361	0.808049	0.305590	0.470601
#33	N-ovlp	0.496092	0.917777	0.603948	0.755002	0.347489
#34	N-ovlp	0.113641	0.999794	0.101689	0.618292	0.317972
#35	N-ovlp	0.213407	0.204650	0.638255	0.099082	0.913754
#36	N-ovlp	0.999827	0.571319	0.971291	0.801818	0.568039
#37	N-ovlp	0.188428	0.046394	0.932086	0.445837	0.279901
#38	N-ovlp	0.182340	0.724371	0.011692	0.856605	0.263795
#39	N-ovlp	0.845987	0.289797	0.552799	0.782734	0.931942
#40	N-ovlp	0.099676	0.089614	0.987865	0.566956	0.715764
#41	N-ovlp	0.387093	0.034168	0.572215	0.006735	0.388700
#42	N-ovlp	0.473166	0.630842	0.854085	0.613667	0.653338
#43	N-ovlp	0.285030	0.159924	0.879838	0.352856	0.658338
#44	N-ovlp	0.820992	0.052170	0.703295	0.044092	0.147854

(1) : ANSI X9.31 で定められる AES ベースの擬似乱数生成法 [72],[73]

(2) : FIPS-186 で定められる SHA1 ベースの擬似乱数生成法（入力オプションがないタイプ）[74],[75],[76]

(3) : FIPS-186 で定められる DES ベースの擬似乱数生成法の NIST 改造版（NIST 亂数検定 Ver1.5 に付属）[74],[77],[78]

(4) : NIST 亂数検定 Ver1.5 に付属

(5) : NIST 亂数検定 Ver1.8 に付属

表 C.2 G-AES⁽¹⁾,G-SHA1⁽²⁾,G-DES⁽³⁾,G-SHA1(v1.5)⁽⁴⁾,G-DES(v1.8)⁽⁵⁾から生成した系列に対する、本判定法のstep-3におけるランダム性判定実験結果を表すp-value全データ(その2)

検定項目 番号	検定法 略式名称	G-AES ⁽¹⁾	G-SHA1 ⁽²⁾	G-DES ⁽³⁾	G-SHA1 (V1.5) ⁽⁴⁾	G-DES (V1.8) ⁽⁵⁾
#45	N-ovlp	0.031548	0.511830	0.047726	0.289273	0.648687
#46	N-ovlp	0.923149	0.276104	0.366141	0.677791	0.935509
#47	N-ovlp	0.598221	0.538751	0.921530	0.011827	0.198230
#48	N-ovlp	0.359090	0.577075	0.287418	0.906306	0.118914
#49	N-ovlp	0.235799	0.234223	0.008728	0.817493	0.467382
#50	N-ovlp	0.237038	0.699274	0.327685	0.756794	0.740492
#51	N-ovlp	0.677648	0.896263	0.084679	0.154547	0.318521
#52	N-ovlp	0.174485	0.400336	0.504376	0.299069	0.674649
#53	N-ovlp	0.955188	0.562323	0.317526	0.765354	0.458458
#54	N-ovlp	0.043580	0.181517	0.097087	0.304159	0.820453
#55	N-ovlp	0.042125	0.784732	0.932669	0.037224	0.159880
#56	N-ovlp	0.658485	0.942808	0.472849	0.896935	0.057235
#57	N-ovlp	0.829038	0.587975	0.304238	0.380684	0.202496
#58	N-ovlp	0.074183	0.537194	0.273317	0.258496	0.713691
#59	N-ovlp	0.383680	0.016632	0.041892	0.061985	0.759331
#60	N-ovlp	0.329417	0.504959	0.267978	0.067479	0.378387
#61	N-ovlp	0.506068	0.769667	0.695495	0.225860	0.543709
#62	N-ovlp	0.608920	0.599817	0.123986	0.522124	0.737774
#63	N-ovlp	0.421722	0.654865	0.079427	0.044029	0.656966
#64	N-ovlp	0.873300	0.735598	0.511333	0.154212	0.063525
#65	N-ovlp	0.377192	0.579523	0.483393	0.515157	0.464456
#66	N-ovlp	0.239087	0.874196	0.292810	0.046765	0.193615
#67	N-ovlp	0.061760	0.655572	0.208873	0.492365	0.354271
#68	N-ovlp	0.321760	0.091431	0.897051	0.392332	0.994683
#69	N-ovlp	0.503441	0.922386	0.555791	0.932705	4.22E-05
#70	N-ovlp	0.017463	0.086044	0.122644	0.722159	0.468280
#71	N-ovlp	0.726102	0.942922	0.010446	0.399893	0.864751
#72	N-ovlp	0.935434	0.173751	0.672427	0.070501	0.121444
#73	N-ovlp	0.818226	0.160314	0.039642	0.944842	0.031289
#74	N-ovlp	0.629810	0.069342	0.445334	0.075603	0.841642
#75	N-ovlp	0.552610	0.902614	0.961376	0.277763	0.021294
#76	N-ovlp	0.085087	0.131470	0.139811	0.672358	0.508697
#77	N-ovlp	0.569399	0.887735	0.390126	0.412185	0.581586
#78	N-ovlp	0.116640	0.575062	0.092872	0.541485	0.768867
#79	N-ovlp	0.983632	0.089726	0.134952	0.615728	0.667257
#80	N-ovlp	0.630183	0.062979	0.071860	0.999400	0.000615
#81	N-ovlp	0.867937	0.000133	0.830426	0.651149	0.251500
#82	N-ovlp	0.341235	0.175732	0.591569	0.154306	0.535279
#83	N-ovlp	0.070483	0.208782	0.943666	0.574676	0.060618
#84	N-ovlp	0.891994	0.472434	0.170906	0.983951	0.505625
#85	N-ovlp	0.056939	0.042324	0.868306	0.184732	0.104634
#86	N-ovlp	0.263541	0.179044	0.471528	0.161369	0.782991
#87	N-ovlp	0.860214	0.335140	0.590688	0.287252	0.753290
#88	N-ovlp	0.380506	0.311938	0.395982	0.775131	0.875100

(1) : ANSI X9.31で定められるAESベースの擬似乱数生成法 [72],[73]

(2) : FIPS-186で定められるSHA1ベースの擬似乱数生成法(入力オプションがないタイプ) [74],[75],[76]

(3) : FIPS-186で定められるDESベースの擬似乱数生成法のNIST改造版(NIST乱数検定Ver1.5に付属) [74],[77],[78]

(4) : NIST乱数検定Ver1.5に付属

(5) : NIST乱数検定Ver1.8に付属

表 C.3 G-AES⁽¹⁾,G-SHA1⁽²⁾,G-DES⁽³⁾,G-SHA1(v1.5)⁽⁴⁾,G-DES(v1.8)⁽⁵⁾ から生成した系列に対する、本判定法の step-3 におけるランダム性判定実験結果を表す p-value 全データ（その 3）

検定項目 番号	検定法 略式名称	G-AES ⁽¹⁾	G-SHA1 ⁽²⁾	G-DES ⁽³⁾	G-SHA1 (V1.5) ⁽⁴⁾	G-DES (V1.8) ⁽⁵⁾
#89	N-ovlp	0.994803	0.696921	0.304527	0.599329	0.305763
#90	N-ovlp	0.141866	0.608610	0.281628	0.010300	0.136497
#91	N-ovlp	0.047739	0.403486	0.980793	0.747563	0.320307
#92	N-ovlp	0.051073	0.222524	0.623733	0.742660	0.428967
#93	N-ovlp	0.546982	0.371555	0.976314	0.206803	0.025570
#94	N-ovlp	0.874273	0.262550	0.282698	0.758063	0.720525
#95	N-ovlp	0.5277383	0.811021	0.614428	0.306149	0.667742
#96	N-ovlp	0.573979	0.135823	0.958703	0.236966	0.172274
#97	N-ovlp	0.308103	0.270532	0.000637	0.031706	0.693636
#98	N-ovlp	0.672152	0.008083	0.727561	0.650633	0.993063
#99	N-ovlp	0.774613	0.771627	0.338817	0.768641	0.019566
#100	N-ovlp	0.405274	0.004816	0.899282	0.467773	0.362448
#101	N-ovlp	0.442885	0.049330	0.444108	0.530646	0.652800
#102	N-ovlp	0.777049	0.470996	0.018303	0.384817	0.657089
#103	N-ovlp	0.772258	0.498483	0.534292	0.064077	0.414363
#104	N-ovlp	0.604767	0.110883	0.965643	0.745403	0.583261
#105	N-ovlp	0.493560	0.116945	0.157036	0.936470	0.477747
#106	N-ovlp	0.754174	0.160623	0.260596	0.073894	0.008650
#107	N-ovlp	0.556800	0.243326	0.170049	0.429141	0.625513
#108	N-ovlp	0.996289	0.349143	0.994870	0.358046	0.402971
#109	N-ovlp	0.984148	0.502194	0.914477	0.113767	0.000286
#110	N-ovlp	0.371879	0.367344	0.463312	0.358455	0.076872
#111	N-ovlp	0.192552	0.296030	0.160319	0.200990	0.887469
#112	N-ovlp	0.438741	0.191522	0.667742	0.143822	0.156527
#113	N-ovlp	0.957719	0.169943	0.981745	0.213097	0.593590
#114	N-ovlp	0.416673	0.411204	0.007562	0.307192	0.393862
#115	N-ovlp	0.550024	0.249490	0.045651	0.923651	0.577394
#116	N-ovlp	0.185711	0.861277	0.242544	0.014085	0.311039
#117	N-ovlp	0.476086	0.747916	0.307096	0.448203	0.960947
#118	N-ovlp	0.788342	0.857026	0.732942	0.065489	0.027222
#119	N-ovlp	0.656868	0.013449	0.604602	0.103847	0.487242
#120	N-ovlp	0.862849	0.216656	0.241714	0.115079	0.052866
#121	N-ovlp	0.207353	0.155569	0.070362	0.051565	0.246985
#122	N-ovlp	0.130000	0.900606	0.150288	0.633776	0.584287
#123	N-ovlp	0.561553	0.795941	0.129442	0.208202	0.423813
#124	N-ovlp	0.205739	0.098695	0.956016	0.601629	0.201403
#125	N-ovlp	0.777404	0.687849	0.688684	0.351630	0.648794
#126	N-ovlp	0.206805	0.545516	0.015981	0.965160	0.427397
#127	N-ovlp	0.986315	0.457089	0.694937	0.735228	0.745962
#128	N-ovlp	0.756872	0.676312	0.001255	0.592213	0.286370
#129	N-ovlp	0.249945	0.754911	0.111314	0.363152	0.828502
#130	N-ovlp	0.185634	0.449685	0.084485	0.245287	0.027056
#131	N-ovlp	0.391977	0.493764	0.257474	0.320170	0.166724
#132	N-ovlp	0.528464	0.112426	0.281041	0.929007	0.995848

(1) : ANSI X9.31 で定められる AES ベースの擬似乱数生成法 [72],[73]

(2) : FIPS-186 で定められる SHA1 ベースの擬似乱数生成法（入力オプションがないタイプ）[74],[75],[76]

(3) : FIPS-186 で定められる DES ベースの擬似乱数生成法の NIST 改造版（NIST 亂数検定 Ver1.5 に付属）[74],[77],[78]

(4) : NIST 亂数検定 Ver1.5 に付属

(5) : NIST 亂数検定 Ver1.8 に付属

表 C.4 G-AES⁽¹⁾,G-SHA1⁽²⁾,G-DES⁽³⁾,G-SHA1(v1.5)⁽⁴⁾,G-DES(v1.8)⁽⁵⁾ から生成した系列に対する、本判定法の step-3 におけるランダム性判定実験結果を表す p-value 全データ(その4)

検定項目 番号	検定法 略式名称	G-AES ⁽¹⁾	G-SHA1 ⁽²⁾	G-DES ⁽³⁾	G-SHA1 (V1.5) ⁽⁴⁾	G-DES (V1.8) ⁽⁵⁾
#133	N-ovlp	0.206539	0.097937	0.328963	0.373569	0.829888
#134	N-ovlp	0.972585	0.976775	0.176605	0.961148	0.190825
#135	N-ovlp	0.080260	0.014480	0.271786	0.692236	0.936351
#136	N-ovlp	0.308681	0.000848	0.012456	0.529295	0.205356
#137	N-ovlp	0.386701	0.022613	0.496664	0.790274	0.589264
#138	N-ovlp	0.121043	0.120429	0.101339	0.449879	0.247139
#139	N-ovlp	0.006850	0.190734	0.288350	0.941800	0.964634
#140	N-ovlp	0.750600	0.587046	0.429340	0.488706	0.568589
#141	N-ovlp	0.998123	0.449268	0.072296	0.044163	0.080940
#142	N-ovlp	0.082727	0.718326	0.092837	0.934422	0.008185
#143	N-ovlp	0.215391	0.277552	0.685743	0.848980	0.370473
#144	N-ovlp	0.714707	0.041214	0.314694	0.975444	0.529247
#145	N-ovlp	0.492888	0.916813	0.516654	0.866012	0.113632
#146	N-ovlp	0.354990	0.186850	0.106055	0.970385	0.993762
#147	N-ovlp	0.314608	0.692433	0.930058	0.125210	0.985290
#148	N-ovlp	0.057547	0.832797	0.165915	0.168051	0.717519
#149	N-ovlp	0.907583	0.010833	0.793597	0.638586	0.261173
#150	N-ovlp	0.513535	0.305650	0.021261	0.721196	0.054505
#151	N-ovlp	0.270102	0.850312	0.132156	0.489953	0.458453
#152	N-ovlp	0.373730	0.889537	0.010788	0.060369	0.325858
#153	N-ovlp	0.262763	0.958558	0.126046	0.653450	0.092915
#154	N-ovlp	0.731830	0.119855	0.039553	0.999821	0.000505
#155	Ovlp	0.782706	0.876291	0.123940	0.862607	0.935737
#156	Univ	0.496553	0.772962	0.987193	0.660505	0.955358
N/A	Lmpl	2.35E-74	5.90E-62	4.84E-67	2.62E-66	2.65E-66
#157	LinCmp	0.230077	0.003049	0.583721	0.227817	0.424813
#158	Serial(1)	0.619872	0.656691	0.605798	0.022688	0.070536
#159	Serial(2)	0.650058	0.909619	0.114766	0.378497	0.532580
#160	ApEntrop	0.636962	0.768829	0.879385	0.651299	0.675878
#161	Cums(1)	0.529722	0.368710	0.918737	0.784333	0.568850
#162	Cums(2)	0.504079	0.434747	0.491467	0.321863	0.014652

(1) : ANSI X9.31 で定められる AES ベースの擬似乱数生成法 [72],[73]

(2) : FIPS-186 で定められる SHA1 ベースの擬似乱数生成法(入力オプションがないタイプ) [74],[75],[76]

(3) : FIPS-186 で定められる DES ベースの擬似乱数生成法の NIST 改造版(NIST 亂数検定 Ver1.5 に付属) [74],[77],[78]

(4) : NIST 亂数検定 Ver1.5 に付属

(5) : NIST 亂数検定 Ver1.8 に付属

参考文献

- [1] 香田徹, “カオスによる信号処理,” 電子情報通信学会 基礎・境界ソサイエティ Fundamentals Review Vol.2 No.4, pp.16–36, April 2009.
- [2] Edwin Atlee Jackson, “Perspectives of Nonlinear Dynamics 1,” Cambridge University Press, 1991.
- [3] Robert L. Devaney, “An Introduction to Chaotic Dynamical Systems Second Edition,” Perseus Books Publishing, 1989.
- [4] Robert L. Devaney, “A First Course in Chaotic Dynamical Systems : Theory and Experiment,” Perseus Books Publishing, 1992.
- [5] K. T. Alligood, T. D. Sauer, J. A. Yorke, “Chaos. An Introduction to Dynamical Systems,” Springer-Verlag, New York, 1997.
- [6] 香田徹, “離散力学系のカオス,” コロナ社, 1998.
- [7] 香田徹, “非線形理論, 電子情報通信レクチャーシリーズ D-3,” コロナ社, 2009.
- [8] 下條隆嗣, “カオス力学入門,” 近代科学社, 1992.
- [9] 長島弘幸, 馬場良和, “カオス入門 — 現象の解析と数理”, 培風館, 1992.
- [10] 香田徹, 柿元厚志, “擬似乱数とカオス,” 情報処理学会論文誌, Vol.27, No.3, pp289-296, 1986.
- [11] 渡辺栄治, “線形写像の有限精度における一方向性から構成した擬似乱数生成法,” 情報処理学会研究報告 2003-CSEC-22(17), pp.21-29, July 2003.
- [12] 宮崎武, 上原聰, 今村恭己, “ロジスティック写像を用いた擬似乱数生成の問題点と、安全な利用方法について,” 2004 年暗号と情報セキュリティシンポジウム (SCIS2004), 4A2-3, January 2004.
- [13] 奥富秀俊, 中村勝洋, “整数演算をベースにしたパラメータ可変の非線形写像を用いた擬似乱数生成法とその評価,” SITA2003, 8.1, November 2003.
- [14] Hidetoshi OKUTOMI, Katsuhiro NAKAMURA, “Pseudo Random Number Generation Method based on Nonlinear Integer Mapping with Parameters Variable and its Randomness Evaluation,” 2004 International Symposium on Information Theory and its Applications (ISITA2004), paper #358, October 2004.
- [15] 岩野隆, 金田学, 奥富秀俊, “一次元写像を用いた擬似乱数生成におけるパラメータ変動の効果について,” 2007 年暗号と情報セキュリティシンポジウム (SCIS2007), 3E2-5, January 2007.
- [16] 岩野隆, 金田学, 奥富秀俊, “一次元写像を用いた擬似乱数生成におけるパラメータ可変の効果について,” 信学技報 Vol.106, No.596, ISEC2006-123, pp.47-51, March 2007.
- [17] 岩野隆, 金田学, 奥富秀俊, “テント型写像を用いた擬似乱数生成における内部状態変動の効果について,” 2008 年暗号と情報セキュリティシンポジウム (SCIS2008), 2A2-4, January 2007.
- [18] 大熊健司, 櫻井幸一, “一次元写像に基づくカオス擬似乱数列の暗号論的安全性について,” 1999

- 年暗号と情報セキュリティシンポジウム (SCIS'99), A-7-1, 1999.
- [19] 本間真, 糸井千岳, 興治文子, 渡瀬龍右, 坂元啓紀, “一次元写像を利用した擬似乱数生成法における初期値解析法について,” 信学技報 ISEC2006-75, pp.23-27, September 2006.
 - [20] E.Alvarez, H.Montoya, M.Romera, G.pastor, “Cryptanalysis of a chaotic encryption system,” Physics Letters A276(2000) 191-196.
 - [21] E.Alvarez, H.Montoya, M.Romera, G.pastor, “Cryptanalysis of an ergodic chaotic cypher,” Physics Letters A311(2003) 172-179.
 - [22] Xiaogang Wu, Hanping Hu, Baoliang Zhag, “Parameter estimation only from the symbolic sequences generated by chaos system,” Chaos, Solitons and Fractals 22(2004) 359-366.
 - [23] 奥富秀俊, 岩野隆, 中村勝洋, “一次元写像に基づく擬似ランダム系列の初期状態の解析について,” 2007 年暗号と情報セキュリティシンポジウム (SCIS2007), 3E2-4, January 2007.
 - [24] 奥富秀俊, 岩野隆, 中村勝洋, “1次の非線形写像から得られた擬似ランダムビット列の初期値推測法について,” 2007 年情報理論とその応用シンポジウム (SITA2007), 2.3, November 2007.
 - [25] 奥富秀俊, 岩野隆, 中村勝洋, “テント型写像から得られるランダムビット列の初期値推測法について,” 2008 年暗号と情報セキュリティシンポジウム (SCIS2008), 2A2-1, January 2008.
 - [26] 奥富秀俊, 中村勝洋, “テント型写像から得られる擬似ランダムビット列の初期値推測法について,” 電子情報通信学会論文誌 VOL.J92-A, No.7, pp.487-497, July 2009.
 - [27] 奥富秀俊, 中村勝洋, “有限精度のテント型写像から得られた擬似ランダムビット列の初期値推測法について,” 2009 年暗号と情報セキュリティシンポジウム (SCIS2009), 1F2-3, January 2009.
 - [28] 奥富秀俊, 中村勝洋, “テント写像から得られた擬似ランダムビット列のパラメータ推測法に関する考察,” 2010 年暗号と情報セキュリティシンポジウム (SCIS2010), 2D1-2, January 2010.
 - [29] E.Alvarez, H.Montoya, M.Romera, G.pastor, “Gray codes and 1D quadratic maps,” Electronics Letters 34(1998) 1304-1306.
 - [30] Cusick TW, “Gray codes and the symbolic dynamics of quadratic maps,” Electronics Letters 35(1999) 468-469.
 - [31] Gray F., “Pulse code communication,” U.S.Patent 2632058, March 17, 1953.
 - [32] M.S.Baptista, “Cryptography with chaos,” Physics Letters A240 (1998) 50-54.
 - [33] E.Alvarez, A.Fernandez, P.Garcia, J.Jimenez, A.Marcano, “New approach to chaotic encryption,” Physics Letters A263 (1999) 373-375.
 - [34] Wai-kit Wong, Lap-piu Lee, Kwok-wo Wong, “A modified chaotic cryptographic method,” Computer Physics Communications 138 (2001) 234-236.
 - [35] 興治文子, 坂元啓紀, 渡瀬龍右, 糸井千岳, “一般の傾きを持つテント写像から得られるビット列の性質,” 2007 年暗号と情報セキュリティシンポジウム (SCIS2007), 2E2-3, January 2007
 - [36] 金田学, 岩野隆, 奥富秀俊, “整数演算化したテント型写像におけるビット出現頻度に関する考察,” 2009 年暗号と情報セキュリティシンポジウム (SCIS2009), 2F1-1, January 2009
 - [37] 荒木俊輔, 富崎武, 上原聰, “有限精度のロジスティック写像における演算精度と解像度に関する一考察,” 2010 年暗号と情報セキュリティシンポジウム (SCIS2010) 3D3-3, January 2010
 - [38] 荒木俊輔, 富崎武, 上原聰, “整数上のロジスティック写像におけるビット毎の出現頻度に関する一考察,” 2009 年暗号と情報セキュリティシンポジウム (SCIS2009) 2F1-3, January 2009
 - [39] Shunsuke Araki, Takeru Miyazaki, Satoshi Uehara, “A Study on Occurrence Rates per Bit

- for the Logistic Map over Integers,” 2008 International Symposium on Information Theory and its Applications (ISITA2008), paper #264, December 2008.
- [40] 荒木俊輔, 宮崎武, 上原聰, “擬似乱数に用いる整数上のロジスティック写像に関する一考察,” 2008 年暗号と情報セキュリティシンポジウム (SCIS2008), 2A2-5, January 2008
- [41] 宮崎武, 荒木俊輔, 上原聰, “端数処理の異なる整数上のロジスティック写像による系列の性質について,” 2010 年暗号と情報セキュリティシンポジウム (SCIS2010), 3D3-1, January 2010
- [42] 宮崎武, 荒木俊輔, 上原聰, “整数上のロジスティック写像から得られる系列の短い周期をもつループについて,” 2009 年暗号と情報セキュリティシンポジウム (SCIS2009), 2F1-2, January 2009
- [43] Takeru Miyazaki, Shunsuke Araki, Satoshi Uehara, “Period and Link Length of the Logistic Map over Integers,” 2008 International Symposium on Information Theory and its Applications (ISITA2008), paper #264, December 2008.
- [44] 宮崎武, 荒木俊輔, 上原聰, “整数上のロジスティック写像のループとその周期に関する一考察,” 2008 年暗号と情報セキュリティシンポジウム (SCIS2008), 2A2-4, January 2008
- [45] 宮崎武, 荒木俊輔, 上原聰, “ロジスティック写像の整域における性質,” 2007 年暗号と情報セキュリティシンポジウム (SCIS2007), 3E2-2, January 2007
- [46] A. Rukhin. and et al, “A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications,” NIST, Special Publication 800-22, May 15, 2001.
- [47] A. Rukhin. and et al, “A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications,” NIST, Special Publication 800-22 Revision1, August 2008.
- [48] 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, pp.21-27, December 2003 .
- [49] S. Kim, K. Umeno, and A. Hasegawa, “Corrections of the NIST Statistical Test Suite for Randomness,” Cryptology ePrint Archive, Report 2004/018, 2004.
- [50] 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, 2004 年 1 月
- [51] 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,” 防衛庁技術研究本部技報 第 6841 号, 平成 15 年 9 月 .
- [52] 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, pp.61-64, July 2004.
- [53] W. Killman, J. Schuth, W. Thumser, and I. Uludag, “A Note Concerning the DFT Test in NIST Special Publication 800-22,” T-Systems, Systems Integration, July 2004.
- [54] 廣瀬勝一, “擬似乱数生成系の検定法に関する調査報告書,” http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/documents/rep_ID0207.pdf, 2004 年 1 月
- [55] 廣瀬勝一, “擬似乱数生成系の検定法に関する調査報告書～NIST SP800-22 の離散フーリエ変換検定について～,” http://www2.nict.go.jp/y/y213/cryptrec_publicity

- /rep_ID0212.pdf, 2005 年 1 月
- [56] K.Hamano, “The distribution of the spectrum for the discrete Fourier transform test included in SP800-22,” IEICE Trans. Fundamentals, vol. E88-A, no. 1, pp.67-73, 2005.
 - [57] 金田学, 奥富秀俊, 中村勝洋, “NIST 亂数検定における離散フーリエ変換検定に関する考察,” 信学技報 Vol.106, No.596, ISEC2006-124, pp.53-58, March 2007.
 - [58] 竹田裕一, 藤井光昭, 鎌倉稔成, 渡邊則生, 杉山高一, “NIST の乱数検定法のテンプレート適合検定における問題点,” 信学技法 Vol.105, No.484, ISEC 2005-110, pp.1-4, December 2005.
 - [59] Kenji HAMANO, Toshinobu KANEKO, “Correction of Overlapping Template Matching Test Included in NIST Randomness Test Suite,” ISITA2006, November 2006.
 - [60] K. Hamano and T. Kaneko, “The Correction of the Overlapping Template Matching Test Included in NIST Randomness Test Suite,” IEICE Transactions of Electronics, Communications and Computer Sciences 2007, E90-A(9), pp 1788-1792.
 - [61] Ueli M. Maurer, “A Universal Statistical Test for Random Bit Generators,” Journal of Cryptology. Vol. 5, No. 2, 1992, pp. 89-105.
 - [62] 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.
 - [63] Jean-Sebastien Coron, “On the Security of RandomSources,” Public-Key Cryptography, vol. 1560 of Lecture Notes in Computer Science, pp. 29-42, Springer-Verlag, 1999.
 - [64] 金田学, 奥富秀俊, 中村勝洋, “NIST 亂数検定における Maurer’s “Universal Statistical” Test に関する考察”, 2007 年暗号と情報セキュリティシンポジウム (SCIS2007), 1E2-3 ,January 2007.
 - [65] 濱野健二, “NIST 亂数検定に含まれる最長連検定の修正,” 信学技報 Vol.107, No.44, ISEC2007-3, pp.17-21, May 2007.
 - [66] 奥富秀俊, 金田学, 中村勝洋, “NIST 亂数検定に関する考察 ~特に最長連検定の評価をめぐって~,” 2008 年暗号と情報セキュリティシンポジウム (SCIS2008), 4A1-6 , January 2008.
 - [67] 栗原貴志, 奥富秀俊, 中村勝洋, “NIST 亂数検定での Random Excursions Test における検定統計量の理論値の妥当性に関する考察,” 2010 年暗号と情報セキュリティシンポジウム (SCIS2010), 3D3-4 , January 2010.
 - [68] 奥富秀俊, 金田学, 山口健二, 中村勝洋, “NIST 亂数検定を用いた乱数性の評価に関する考察,” 2006 年暗号と情報セキュリティシンポジウム (SCIS2006), 1E2-3, January 2006.
 - [69] 奥富秀俊, 金田学, 山口健二, 中村勝洋, “NIST 亂数検定を用いた乱数性能の評価について,” 信学技報 Vol.105, No.666, ISEC2005-165, pp.79-84, March 2006.
 - [70] 奥富秀俊, 中村勝洋, “NIST 亂数検定を用いた合理的なランダム性の判定法に関する考察,” 電子情報通信学会論文誌 VOL.J93-A, No.1, pp.11-22, January 2010.
 - [71] Juan Soto and Lawrence Bassham, “Randomness Testing of the Advanced Encryption Standard Finalist Candidates,” Computer Security Division National Institute of Standards and Technology, March 28, 2000.
 - [72] “Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA),” ANSI X9.31-1988, September 1998.
 - [73] “NIST-Recommended Random Number Generator Based on ANSI X9.31,” Appendix A.2.4

Using the 3-Key Triple DES and AES Algorithms, National Institute of Standards and Technology, January 2005.

- [74] “Digital Signature Standard (DSS),” Appendix 3.2 ALGORITHM FOR COMPUTING m VALUES OF x, FIPS Publication 186-2 (+Change Notice), National Institute of Standards and Technology, January 2000.
- [75] “Digital Signature Standard (DSS),” Appendix 3.3 CONSTRUCTING THE FUNCTION G FROM THE SHA-1, FIPS Publication 186-2 (+Change Notice), National Institute of Standards and Technology, January 2000.
- [76] A.Menezes, et al., “Handbook of Applied Cryptography,” Chapter 5.3.2 FIPS 186 generator, 5.15 Algorithm, CRC Press, Inc., 1997.
- [77] “Digital Signature Standard (DSS),” Appendix 3.4 CONSTRUCTING THE FUNCTION G FROM THE DES, FIPS Publication 186-2 (+Change Notice), National Institute of Standards and Technology, January 2000.
- [78] A.Menezes, et al., “Handbook of Applied Cryptography,” Chapter 5.3.2 FIPS 186 generator, 5.16 Algorithm, CRC Press, Inc., 1997.
- [79] P.G.Hoel, “入門数理統計学,” 第 9 章 3 節 χ^2 検定の制約, 培風館, 1978.