1 次元置換的セルオートマトンの位相圧力

Topological pressure on one-dimensional permutative cellular automata

行木 孝夫 (Takao Namiki)[1]
[1] 北海道大学大学院理学研究院数学部門 (Department of Mathematics, Hokkaido University)
e-mail : nami@math.sci.hokudai.ac.jp

1 概要

力学系のカオス性を測る指標の一つは位相エントロピーである．セルオートマトンを力学系とみなした場合の位相エントロピーに関し，1 次元両側置換的な時間発展規則をもつセルオートマトンであれば位相エントロピーは相空間としてのフルシフトの位相エントロピーに対して時間発展規則の幅に応じた定数倍となっている．本講演では位相エントロピーを拡張した概念である位相圧力に関して ECA90 に対する結果を紹介する．

2 背景

セルオートマトンは様々な分野で研究対象となる系であり，力学系としての立場をとれば離散的な相空間をもつ離散力学系である．N 要素を持つ有限集合 $S = \{0, \ldots, N-1\}$ を記号とよび，記号の両側無限列全体 $X = S^{\mathbb{Z}}$ を記号空間とよぶ．これを相空間とする力学系を考える．$f : S^{r+s+1} \to S$ $(r > 0,\ s > 0)$ を規則とし，$T : X \to X$ を $x \in X$ について $(T(x))_i = f(x_{i-r}, \ldots, x_{i+s})$ と定義する．$x \in X$ の各成分について時間発展が一様に規則 f によって定まる力学系であり，この力学系 (X, T) を N 状態 $r + s + 1$ 近傍セルオートマトンとよぶ．

セルオートマトンの典型的な例は $N = 2$，$r = s = 1$ であり，この場合を Elmentary Cellular Automata (ECA) とよぶ．ECA は Wolfram が 1980 年代後半に網羅的に研究した [1]．ECA は 256 通りの規則をが存在し, 通し番号をつけられる．よく知られている規則は ECA90 $f(x_{i-1}, x_i, x_{i+1}) = x_{i-1} + x_{i+1} \bmod 1$ および ECA150 $f(x_{i-1}, x_i, x_{i+1}) = x_{i-1} + x_i + x_{i+1} \bmod 1$ である．これら 2 規則は一様拡大的であり，カオス的である．

記号空間上のシフト $\sigma : X \to X$ は $x \in X$ について $(\sigma x)_i = x_{i+1}$ で与えられる．片側シフトは $X = S^{\mathbb{N}}$ の場合である．一般に，シフトはカオス的な力学系との位相共役を与える基本的な力学系である．シフト (X, σ) に対して $Fix(X, \sigma^n) = \{x \in X | \sigma^n x = x\}$ は周期 n をもつ周期点の集合である．シフトの位相エントロピー $h(X, \sigma)$ を

$$h(X, \sigma) = \lim_{n \to \infty} \frac{1}{n} \log |Fix(X, \sigma^n)| = \log N$$

で定義する．ここで，$|Fix(X, \sigma^n)|$ は n 周期点の数であり，N^n に等しい．特に，位相エントロピーは位相共役のもとで不変であるから力学系の分類に重要な役割を持つ．また，位相エントロピーが正であれば力学系はカオス性を持ち，位相エントロピーが高いほどカオス性が強い．

また，位相エントロピーを一般化した位相圧力をポテンシャル関数 U のもとで次のように定義する．U は X 上の連続関数とする．$S_n U(x) = \sum_{k=0}^{n-1} U(\sigma^k x)$ として分配関数 $Z_n(U)$ を次で定義する．

$$Z_n(U) = \sum_{x \in Fix(X, \sigma^n)} \exp(-S_n U(x))$$

位相圧力 $P(U)$ を次の極限が存在するとき

$$P(U) = \lim_{n\to\infty} \frac{1}{n} \log Z_n(U)$$

で与える．

3　主結果

ECA90 (X, T_{90})，ECA150 (X, T_{150}) は $N = 4$ の片側シフトと位相共役である [3]．この位相共役は，X を x_0，x_1 による筒集合による分割 $\{[00], [01], [10], [11]\}$ をとることで与えられる．従って，ECA90，ECA150 の位相エントロピーも求められ，$h(X, T_{90}) = h(X, T_{150}) = \log 4 = 2\log 2$ である．

$w = (w_i)_{i=0}^{r+s-1} \in S^{r+s}$ に対し，$f_w^{right} : S \to S$ を $a \in S$ に対して $f(w_0, \ldots, w_{r+s-1}, a)$ で定める．また，$f_w^{left} : S \to S$ を $a \in S$ に対して $f(a, w_0, \ldots, w_{r+s-1})$ で定める．f_w^{right} と f_w^{left} が共に全射なとき，規則 f を両側置換的という [2].

よく知られている通り，両側置換的な規則によって定まるセルオートマトンは N^{r+s} 個の記号によるシフトと位相共役であり，位相エントロピーは $\log N^{r+s} = (r+s)\log N$ である．この結果は両側置換的なセルオートマトンの位相エントロピーがシフトの位相エントロピー $\log N$ の $r+s$ 倍であり，規則の幅だけカオス性が強いことを示している．

ECA90，ECA150 に対し，位相エントロピーを位相圧力に拡張する．次の命題が成立する．

命題 1　ポテンシャル関数 U は $x \in X$ の x_0 および x_1 のみに依存するものとする．また，$U(00) = U(11), U(10) = U(01)$ を仮定する．$a = \exp(-U(00)), b = \exp(-U(01))$ とする．このとき, シフトの位相圧力は $P(U, X, \sigma) = \log(a+b)$, ECA90, ECA150 の位相圧力は $P(U, T_{90}) = P(U, X, T_{150}) = \log 2(a+b) = \log 2 + P(U, X, \sigma)$ である．

4　おわりに

両側置換的セルオートマトン ECA90，ECA150 の位相圧力について単純なポテンシャル関数のもとでシフトの位相圧力との関係を与えた．この関係の力学系としての意味については今後の問題である．セルオートマトンはシフト可換な連続写像として特徴づけられ，シフトの性質がどれだけセルオートマトンに移行するかという一般的な問題設定ができる [4]．この観点からは，ポテンシャル関数の一般化，また，相空間を Markov シフトあるいは sofic シフトとした場合の問題も残っている．

参考文献

[1] S. Wolfram, Theory and Application for Cellular Automata, World Scientific, 1986

[2] G. A. Hedlund, Endomorphisms and Automorphisms of the shift dynamical system, Mathematics Systems Theory, 3 (1969), 320–375

[3] K. Matsumoto, C^*-Algebras Associated with Cellular Automata, Mathematica Scandinavica, 75 (1994) 195–216

[4] 行木孝夫, セルオートマトンとエルゴード理論, 応用数理,13 (2003), 125–136

謝辞　本研究は科学研究費補助金 23K2578503 の支援を受けた．

RAID のための完全グラフの辺順序

Edge orderings in the complete graphs for RAID

足立 智子 (Tomoko Adachi)[1], 新谷 誠 (Makoto Araya)[2]
[1] 静岡理工科大学 (Shizuoka Institute of Science and Technology), [2] 静岡大学 (Shizuoka University)
e-mail : adachi.tomoko@sist.ac.jp

1 はじめに

RAID (Redundant Array of Independ Disks) は，分散システムにおいてディスクの処理速度と安全性を高める技術である ([1]). 情報を格納したインフォメーションディスクをグラフの辺に，パリィティチェック用のチェックディスクをグラフの頂点に対応させ，インフォメーションディスクにアクセスしていく際のチェックディスクの個数が少なくなるようにインフォメーションディスクのアクセス順序を考える.

Cohen et. al. (2001) [2] や Cohen and Colbourn (2004)[3] は，n 頂点の完全グラフについて ladder ordering の存在性を示し，RAID のパフォーマンスについて考察を与えた.

本研究では，頂点数 n が小さい場合に，完全グラフにおける ladder ordering の辺順序を具体的に列挙し，頂点と辺の結合関係とその順序から ladder ordering の同値性や周期性などの特徴を調べる.

2 用語の説明

n 個の頂点, m 本の辺を持つグラフ $G = (V, E)$ を考える. m 以下のある正整数 d を固定し,「window」と呼ぶ. グラフ G の辺順序を $\{0, 1, \cdots, m-1\}$ 上の置換 π で与える. window d と辺順序 π を持つグラフ G に対して，$m+1-d$ 個の部分グラフ $G_i^{\pi,d}$ $(i = 0, 1, ..., m-d)$ を定める. ここで，$G_i^{\pi,d}$ は，G の部分グラフであり，連続する d 本の辺 $\{e_{\pi(i)}, e_{\pi(i+1)}, \cdots, e_{\pi(i+d-1)}\}$ を持つものである. これを，辺順序 π のもとで，連続する d 本の辺の集合が窓から見えている状態，すなわち RAID において連続する d 個のインフォメーションディスクにアクセスしている状態であるとみなす. このときの RAID のアクセスコストを，$G_i^{\pi,d}$ において連続する d 本の辺が接続する頂点の個数の最大値 f であると考え，d-アクセスコストと呼ぶ. 与えられた d に対して，アクセスコスト f ができ得る限り小さくなるような辺順序 π を見つけることが，RAID のパフォーマンスとして良い.

3 本研究の結果

本稿では，頂点 v_1, v_2, v_3, v_4 のことを，v を省略してそれぞれ $1, 2, 3, 4$ と書く場合がある. また，頂点 v_i, v_j に接続する辺 (v_i, v_j) のことを ij と書く場合がある.

完全グラフ K_4 を考える. window $d = 3$ に対して，アクセスコストが最小になるように辺順序を列挙していった. その結果，連続する d 本の辺が接続する頂点は 3 個または 4 個になった. すべてを 3 個で抑えることはできない.

結果 1 完全グラフ K_4 において,「window」$d = 3$ に対する ladder ordering は，辺順序を考慮せずに，グラフの同型に着目すると，下記の 2 種類になる.

$(12, 13, 23, 24, 34, 14, ...)$ (図 1 および図 3)

$(12, 13, 23, 34, 24, 14, ...)$ (図 2)

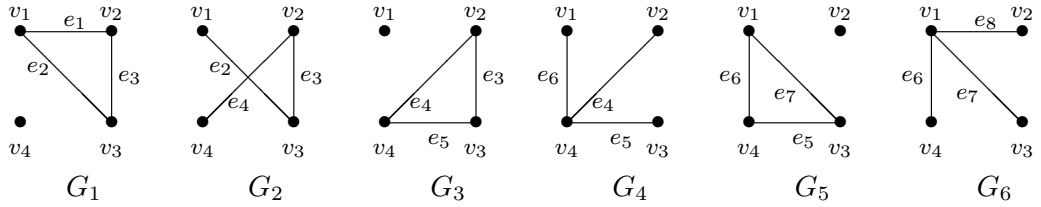


図 1.　K_4 のある Ladder odering

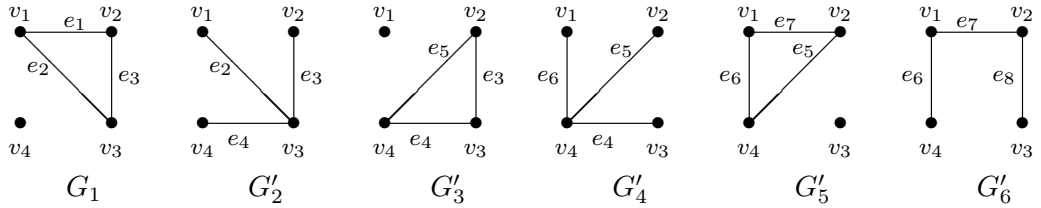


図 2.　K_4 の別の Ladder odering

G_3 と G'_3 はグラフとしては同じであるが，辺順序としては異なる．G_1, G_3, G_5 はグラフとしては同型であり，一見すると周期 2 と思える．しかし，辺順序を含めてグラフの同値性を考えると，G_7, G_{13} は辺順序グラフを含めたグラフとしては同値であるといえるが，G_7, G_9 は辺順序グラフを含めたグラフとしては同値であるとはいえない．したがって，図 3 の周期 6 が Ladder ordering の最短の周期となる．ここで, 図 3 の G_{12} の次のグラフ $G13$ は，$e_{13} = (v_1, v_3)$, $e_{14} = (v_1, v_2)$, $e_{15} = (v_2, v_3)$ になり，辺順序を含めて G_7 と同型なグラフになる．

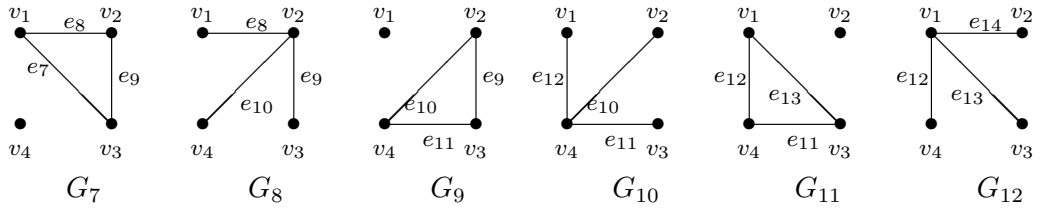


図 3.　K_4 のある Ladder odering の周期

謝辞　本研究は JSPS 科研費 JP25K07111 の助成を受けたものである．

参考文献

[1] P. Chen, E. Lee, G. Gibson, R. Katz and D. Ptterson: RAID: High-performance, reliable secondary storage, *ACM Computing Surveys*, Vol. 26 (1994), pp. 145–185.

[2] M. Cohen, C. Colbourn and D. Froncek: Ladder orderings of pairs and RAID performance, *Computing and Combinatorics: Proc. 7th annual international conference, COCOON 2001*, Lect. Notes Comp. Sci. 2108, Springer-Verlag, pp. 420–431 (2001).

[3] M. Cohen and C. Colbourn: Cluttered orderings for the complete graph, *Discrete applied mathematics*, vol. 138 (2004), pp. 35–46.

楕円曲線上の Me 演算によって生成される 2 値系列の統計的乱数性

Statistical Randomness of Binary Sequences Generated by Me Operation on Elliptic Curves

山内 蓮太 (Renta Yamauchi)[1]，林 夏生 (Natsuo Hayashi)[1]，宮﨑 武 (Takeru Miyazaki)[2]，荒木 俊輔 (Shunsuke Araki)[3]，上原 聡 (Satoshi Uehara)[1]
[1] 北九州市立大学 (The University of Kitakyushu)， [2] 九州情報大学 (Kyushu Institute of Information Sciences)， [3] 九州工業大学 (Kyushu Institute of Technology)
e-mail : yamauchi.renta@is.env.kitakyu-u.ac.jp

1 序論

白勢は有限体 $\mathbb{F}_p$ 上の楕円曲線 $E/\mathbb{F}_p$ で与えられる点 P, Q に対して新たな演算である Me 演算 $P \oplus Q$ を定義した [1]．この Me 演算は，可換律・べき等律・加法に対する分配律といった性質を持ち，白勢はこの Me 演算を用いた応用の一例として，擬似乱数生成器を提案している [1]．しかし，この生成器から得られる 2 値系列の統計的性質についての詳細な評価は行なっていない．生成器から得られる系列の予測困難性を保証するには十分な統計的検証が欠かせない．

本稿では，白勢が提案した生成器から得られる 2 値系列に対して統計的乱数性を評価する．さらに，ビット長を 256 ビット・224 ビット・192 ビットとする素数 p に対して出力値における各ビット位置の ‘0’ および ‘1’ の出現頻度を調査し，各演算精度において偏りのあるビットを除いた出力値を連結して得られた 2 値系列に対しても同様に統計的乱数性を評価した．

2 Me 演算

本稿で使用する楕円曲線を次のように定義する．$p \equiv 3 \pmod 4$ かつ $p \geq 7$ を満たす素数 p に対し，楕円曲線 $E(\mathbb{F}_p)$ を Weierstrass 標準形 $y^2 = x^3 + ax + b$ とする．また，点の個数 $\#E(\mathbb{F}_p) = 2d (d$ は奇数)，位数 2 の点 T がただ 1 つ存在し，その y 座標は 0 である．特別な元 $\mathcal{Z}$ を導入し，集合 $\varepsilon(\mathbb{F}_p) = E(\mathbb{F}_p) \cup \{\mathcal{Z}\}$ を定義する．加算は $P + \mathcal{Z} = \mathcal{Z} + P = \mathcal{Z}$，$\mathcal{Z} + \mathcal{Z} = \mathcal{Z}$ と拡張される．演算 $\mathrm{sign} : \varepsilon(\mathbb{F}_p)\backslash\{\mathcal{O}\} \to \{0, \pm 1\}$ をルジャンドル記号により $\mathrm{sign}((x_0, y_0)) = (\frac{y_0}{p})$ とする．

整数 $k \geq 2$ に対して，Me 演算 $P \oplus Q$ を以下で定義する．

(i) 任意の $P \in \varepsilon(\mathbb{F}_p)$ に対して，次式とする．

$$P \oplus \mathcal{Z} = \mathcal{Z} \oplus P = P$$

(ii) 共に $\mathcal{Z}$ でない P, Q に対して，次式とする．

$$P \oplus Q = \begin{cases} P & \text{if } P = Q \\ \mathcal{Z} & \text{if } \mathrm{sign}(P - Q) = 0 \\ kP - (k-1)Q & \text{if } \mathrm{sign}(P - Q) = 1 \\ kQ - (k-1)P & \text{if } \mathrm{sign}(P - Q) = -1 \end{cases}$$

これにより，Me 演算での逆元 $\ominus P = P + T$，減算 $P \ominus Q = P \oplus (\ominus Q)$ も導入される．また，$\mathcal{Z}$ が単位元となり，全ての P に逆元が存在する．通常の加算 $+$ は群を成し，$\oplus$ と $+$ は分配律を満たす．

3 Me 演算に基づく擬似乱数生成器

Me 演算 $\oplus$ を用いて，楕円曲線上の離散対数問題の困難性に基づく擬似乱数生成器が提案された [1]．ただし，この方式では有理点の個数を $\#E(\mathbb{F}_p) = 2l$（l は奇素数）とし，$G \in E(\mathbb{F}_p)$ を生成元，$T \in E(\mathbb{F}_p)$ を位数 2 の元とする．

初期値 $a_0 \in \mathbb{N}$ ($\mathbb{N}$ は自然数を表す) を選び，$\{a_i\}_{i\geq 0}$ に関する漸化式を次式で定義する．

$$a_i = x(a_{i-1}G \oplus T)$$

ただし，$x(\cdot)$ は楕円曲線上の点の x 座標を意味する．また，a_i の最下位ビット (LSB) を連結し，最終的な擬似乱数系列とする．

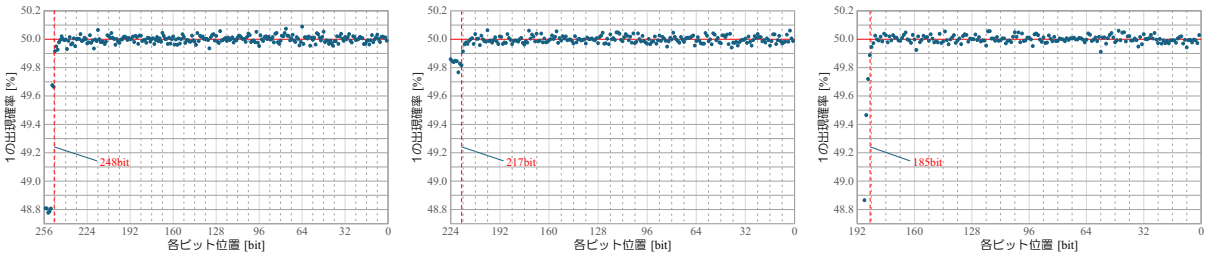
4　統計的乱数性の評価

本実験では次の評価を行った．①：128 ビットセキュリティである 256 ビットの楕円曲線に対して，白勢による擬似乱数生成器の出力値系列を NIST SP800-22 による統計的乱数性を評価した．②：128 ビット・112 ビット・96 ビットの各セキュリティレベルを意識し，それぞれに対応するビット長 256 ビット・224 ビット・192 ビットの素数 p の演算精度の楕円曲線において，各出力点 a_i のビット位置に対する出現頻度の偏りを確認した．③：② の結果をもとに，それらの演算精度において上位ビットを排除した，偏りのないビット位置のみの出力ビットを連結した 2 値系列についても，NIST SP800-22 に基づく評価を行った．

① の結果，生成された 2 値系列は NIST 検定の全 188 項目を通過し，最下位ビットの系列が高い乱数性を有することが確認された．

② の結果を図 1 に示す．256 ビット演算精度では上位 8 ビット，224 ビットおよび 192 ビット演算精度では上位 7 ビットにおいて，‘1’ の出現確率に有意な偏りが確認された．いずれの結果においても，特に上位 7 ビットにおいて共通して，‘0’ と ‘1’ の出現頻度に偏りが見られた．一方，それ以外のビット位置では 1 の出現確率が概ね 49.9% ～ 50.1% の範囲に収まり，統計的な偏りはほとんど見られなかった．このことから，偏りのある上位ビットを除いた出力値は乱数系列に使用できる．

③ の結果では，各精度において偏りのないビット位置のみを連結して得た系列も，NIST 検定の全項目を通過した．このことから，最下位ビットに限らず，適切なビット位置を選択することで高品質な擬似乱数系列を得られる可能性が示された．



(a) 256 ビット演算精度　(b) 224 ビット演算精度　(c) 192 ビット演算精度

図 1: 各ビット演算精度のビット位置ごとの ‘1’ の出現確率

5　結論

本稿では，白勢が提案した Me 演算を用いた 2 値系列は最下位ビットに限らず，偏りのある上位ビットを除いた出力値は高い乱数性を保持していることがわかった．このことから，複数ビットの出力によって乱数系列の生成効率が上がることを示した．

参考文献

[1] 白勢政明，楕円曲線の Me 演算の負演算とその応用，コンピュータセキュリティシンポジウム 2019 予稿集，(2019)，1528-1534.