セルオートマトンのプライマリーな局所規則

粉川 竜治 Ryuji Kokawa[1]　　藤尾 光彦 Mitsuhiko Fujio[2]

[1] 近畿大学大学院産業理工学研究科
Graduate School of Humanity-oriented science and engnieering, Kindai University
[2] 近畿大学産業理工学部
Faculty of Humanity-oriented science and engnieering, Kindai University

1　まえがき

セルオートマトン理論では各セルに状態値が配置されたものを様相と呼び，セルオートマトンは様相を様相へ移す変換として定義される．一般の様相変換との違いは，各セルの次状態がそのセルの近傍での現在の状態のみによって決定されることにある．この決定規則を局所遷移規則と呼ぶ．セルオートマトンは格子点などの均質な空間で定義されることが多く，この場合，規則の適用は移動不変性を仮定される．すなわち異なったセルにおいても，参照される近傍は丁度セルのズレだけ平行移動したものとなっており，平行移動した形での規則が適用される．1 次元 2 値の様相はビット列と見なすことができ，この場合セルオートマトンはビット列の変換と見なされる．計算万能性を持つセルオートマトンの存在が知られており，セルオートマトンを利用した複雑なビット列操作が可能と考えられる．実際そのような中で，1987 年には P. Guan[1] によってセルオートマトンを用いた公開鍵暗号が提案されている．P. Guan のセルオートマトン公開鍵暗号は RSA 暗号で用いられる素数や，楕円曲線暗号で用いられる楕円曲線上の点演算の代わりに，セルオートマトンの（局所規則の）合成が利用する．合成された局所規則が公開鍵とされ，合成に用いた局所規則を秘密鍵とする．

本研究では，セルオートマトン公開鍵暗号の実現を進めるために局所規則と，それを合成してできる合成規則の関係を考え，合成規則ではない局所規則すなわちプライマリーな局所規則について考える．これは因数分解における素数にあたる．なお，局所規則の合成・分解を考えるためには（サイズ・形状ともに）異なった近傍（依存性）を持つセルオートマトンを同時に考える必要があることに注意する．一般的なセルオートマトンの局所規則の合成については既に定義がされている．セルオートマトン公開鍵暗号の実用化における問題点として，

1. 可逆なセルオートマトンを見つけること、あるいは個々のセルオートマトンについて、それが可逆となるような様相集合（リミットサイクル）を決定すること

2. 公開鍵として利用する合成された局所規則からそれを構成する局所規則を求めること，いわゆる因数分解の可否，および可能であるならばその計算量を見積もること

があげられる．ここでは 2 を中心に考える．現在のところ局所合成の因数分解に関するアルゴリズムは知られておらず，単純に合成して調べるしかない．そこで近傍サイズの小さなものから順に素な局所規則を決定することを試みた．

局所規則の合成について考える為に，2 近傍の局所規則同士で合成して 3 近傍の局所規則を，2 近傍の局所規則と 3 近傍の局所規則を合成して 4 近傍の局所規則を，3 近傍の局所規則同士で合成して 5 近傍の局所規則の生成を行った．一般に $r-$ 近傍（依存）の局所規則と $s-$ 近傍（依存）の局所規則を合成すると $r+s-1$ 近傍（依存）の局所規則が得られる．

局所規則の合成を行った結果，異なる複数の組み合わせから同じ合成規則が生成されることが発見できたことから，因数分解は一意でないことがわかった．ただし素因数分解の一意性の可否は未検証である．

2　セルオートマトンの概要

セルオートマトンとは，

- $k(\geq 2)$ 個の状態を持つセル
- 正方形セルが格子状に並んだ様相空間
- セルの状態を変化（発展）させる局所規則

からなる離散的並列計算モデルである．

セルオートマトンのセルは $k(\geq 2)$ 個の異なる状態を持ち，その中には静止状態と呼ばれる特別な状態が含まれる．本研究では最も単純である $k=2$ で考え，それぞれの状態を 0 と 1 の記号もしくは白と黒の色で表す．

セルオートマトンのセル格子は $n(\geq 1)$ で定義され，セルオートマトンの研究の大半は 1 次元または 2 次元のセルオートマトンを対象としている．本研究では 1 次元セルオートマトンについて考える．また一般的に，セルの数は無限である．

セルオートマトンは離散的な時間間隔でセルの状態を変化（発展）させる．この時、セルの次の時間ステップにおける状態は局所規則によって決定される．局所規則は規則集合であり，一つのセルおよび近傍内のセルから次の時間ステップにおける一つのセルの状態への関数である．一般的な 1 次元セルオートマトンのセルの近傍は，あるセル c の左側にある r 個のセルおよび右側にある r 個のセルの集合をセル c の近傍セルと定義され，セル c 自身も含めた近傍は $2r+1$ 個のセルとなる．セル c とその近傍セルの状態に対し，次の時間ステップにおけるセル c の状態の対応させたものが局所規則である．局所規則は図 1 のように表であらわすことができる．またこの図における出力列 00011110 を 2 進数と見なし，それを 10 進数に変換した 30 は規則番号と呼ばれ，図 1 のセルオートマトンは ECA における規則 30 番もしくはルール 30 と呼ばれる．

セルオートマトンは，様相空間をそれ自身へ移す変換として遷移関数を定義することができる．

セルの両側に近傍をとるセルオートマトンの中で，最も単純なセルオートマトンは半径 $r=1$ で，セルが持つ状態数 $k=2$ である．このセルオートマトンは，近傍セと次の時間ステップにおける状態の組み合わせ，すなわち局所規則が $2^{2^3}=256$ 通り存在する．一般にこ

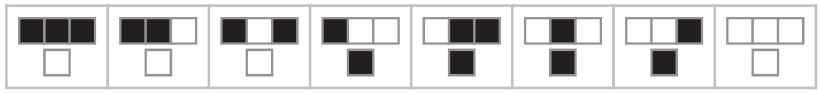

図 1: ECA の局所規則の例．ECA におけるルール 30

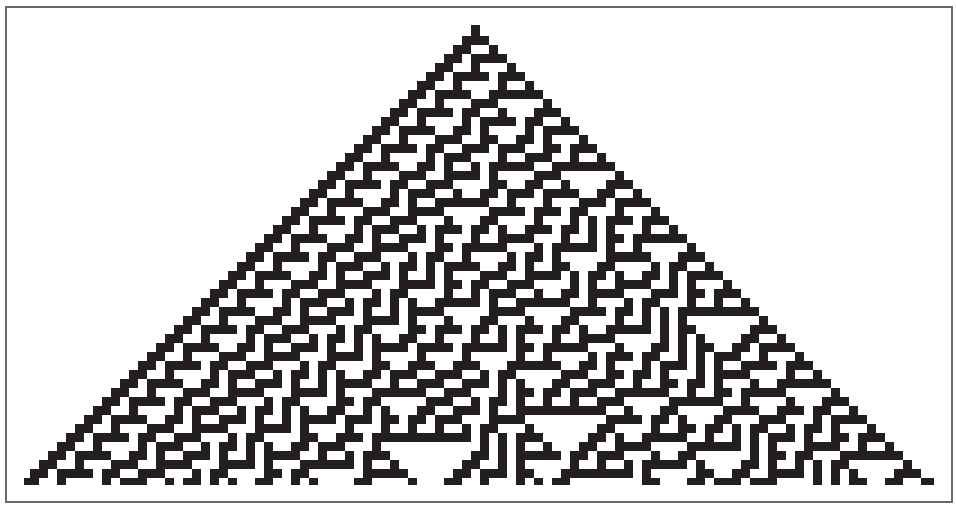

図 2: 単一の黒セルの初期配置から図 1 の規則で５０回セルの状態を変化させた．上から下に向かって時間が進んでいる

のセルオートマトンは初等セルオートマトン（elementary cellular automaton, ECA）と呼ばれる．

また，本研究ではセルの片側だけに近傍をとるセルオートマトンについても考える．片側だけに近傍をとるセルオートマトンの中で最も単純なセルオートマトンは，セルが持つ状態数が $k=2$ で，セル c と左右どちらか 1 つだけに近傍にとるセルオートマトンで，その近傍数は 2 となる．このセルオートマトンには局所規則を $2^{2^2}=16$ 通り存在する．

3　局所規則の合成

3.1　群 G 上のセルオートマトン

以下において，2 元 $0,1$ からなるブール代数を $\mathbf{2}$ で表す．

本研究ではセルオートマトンを局所性と等質性の観点から一般的に考えるため，群における離散力学系として定式化する．すなわち，群 G の冪集合 $\mathscr{C}=2^G$ を様相空間と考え，G の部分規則集合 $V\subseteq G$ の部分集合族 $\mathfrak{L}\subseteq 2^V$ を V に台を持つ局所規則と考える．ここにおいて，局所規則 $\mathfrak{L}$ の働きは次のようなものである．様相 c の遷移後のサイト $g\in G$ における状態 $c'(g)$ は，その周辺の状態パターンを群作用で単位元 e の周辺 V に移したものが $\mathfrak{L}$ に帰属するか否かによって決定する．明示的には

$$c\mapsto c'=\{g\in G\mid g^{-1}c\cap V\in\mathfrak{L}\}$$

となる．このような遷移関数は

変換 $T\colon\mathscr{C}\to\mathscr{C}$ で，群 G の作用と可換なもの:

$$T(ac)=a(T(c)),(a\in G,c\in\mathscr{C})$$

として特徴づけられる．ただし，様相 $c\in\mathscr{C}$ への $a\in G$ の作用は $ac=\{ag\mid g\in c\}$ である．

通常の無限長無いし周期 N の 1 次元セルオートマトンはアーベル群 $G=\mathbb{Z}$ ないし $\mathbb{Z}_N$ において，原点対称な区間 $V=[-r,r]$ を考えた場合に当たる．

3.2　代数構造

ブール代数 B に値をとる集合 X 上の関数空間 B^X には点毎の演算によるブール代数の構造を考える．すなわち，$f,g\in B^X$ に対し

$$\begin{aligned}(f\vee g)(x) &:= f(x)\vee g(x)\quad(x\in X)\\ (f\wedge g)(x) &:= f(x)\wedge g(x)\quad(x\in X)\\ (\neg f)(x) &:= \neg(f(x))\qquad(x\in X)\end{aligned}$$

と定める．このとき

$$f\leq g\Leftrightarrow f(x)\leq g(x)\quad(\forall x\in X)$$

が成り立つ．$B=2$ の場合は集合束としての構造と一致し，$\vee,\wedge,\neg$ および $\leq$ はそれぞれ，和集合，共通部分，補集合をとる演算および包含関係となる．

G 上の遷移関数の全体 $\mathcal{T}_G$ はブール代数 $[2^G \to 2^G] = (2^G)^{(2G)}$ の部分代数をなす．また V に台を持つ局所規則の全体 $\mathcal{L}_V = [2^V \to 2]$ には $2^{(2^V)}$ としてのブール代数の構造を考える．これらはすべて完備である．

また，$V \subseteq W \subseteq G$ に対しては $2^V \subseteq 2^W$ であるから，$\mathcal{L}_V$ は $\mathcal{L}_W$ の部分束となる．ただし，補をとる演算はいずれの代数におけるものであるかに依存するので，台を明示する必要があるときには $\neg_V$ のように表すものとする．

これより G の部分集合の増大列 $\mathfrak{F} = \{V_i\}_{i\in\mathbb{Z}}$ $(i \le j \Rightarrow V_i \subseteq V_j)$ が与えられれば G 上の局所規則全体 $\mathcal{L}_G$ にフィルター付けが定まる:

$$i \le j \Rightarrow \mathcal{L}_{V_i} \subseteq \mathcal{L}_{V_j} \tag{1}$$

次小節 (定理 1) で見るように $\mathcal{L}_V$ は関数全体のなすブール代数 $\mathcal{T}_G$ の部分ブール代数 $\mathcal{T}_V$ と同型である．これによって $\mathcal{T}_G$ にも同様のフィルタ付け構造が入る．

3.3 局所規則と遷移規則の対応

V に台を持つ局所規則 $\mathfrak{L} \in \mathcal{L}_V$ に対し，G 上の遷移関数 $T_{\mathfrak{L}} \in \mathcal{T}_G$ を

$$T_{\mathfrak{L}}(c) = \{g \in G \mid g^{-1}c \cap V \in \mathfrak{L}\} \quad (c \in \mathscr{C})$$

で定める．$T_{\mathfrak{L}}$ が G の作用と可換であることは容易に確かめられる．

遷移関数から局所規則への逆の対応を考えるため，局所規則の台に相当する概念として，遷移関数の局所性領域の概念を導入する．$T\colon \mathscr{C} \to \mathscr{C}$ を遷移関数，$V \subseteq G, g \in G$ とする．任意の様相 $c, c' \in \mathscr{C}$ について

$$c \cap V = c' \cap V \Rightarrow g \in T(c) \iff g \in T(c')$$

が成り立つとき T はサイト g において V 上局所的であるといい，V を T の g における局所性領域と呼ぶ．サイト g において V 上局所的な遷移関数の全体を $\mathcal{T}_{g,V}$ は $\mathcal{T}_G$ の完備な部分ブール代数である．

単位元 e において，V 上局所的な遷移関数の全体 $\mathcal{T}_{e,V}$ を簡単のため $\mathcal{T}_V$ で表すものとすれば $\mathcal{T}_V = \mathcal{T}_{g,gV}$ が成り立つ．

単位元 e において V 上局所的な遷移関数 $T \in \mathcal{T}_V$ から V に台を持つ局所規則 $\mathfrak{L}_T \in \mathcal{T}_V$ を

$$\mathfrak{L}_T = \{c \in 2^V \mid e \in T(c)\}$$

によって定める．T が G の作用と可換であることから，任意の g に対して

$$\mathfrak{L}_T = \{g^{-1}c \in \mathscr{C} \mid c \in 2^{gV}, g \in T(c)\}$$

が成り立つ．

定理 1 写像 $\mathcal{T}_V \ni T \mapsto \mathfrak{L}_T \in \mathcal{L}_V$ および $\mathcal{L}_V \ni \mathfrak{L} \mapsto T_{\mathfrak{L}} \in \mathcal{T}_V$ は共にブール代数の同型写像であって，互いに他の逆写像である．

Proof. 2つの写像がブール代数の順同型であることは直接確かめられるので，後半部分のみ示す．$T \in \mathcal{T}_V$ に対し

$$\begin{aligned} T_{\mathfrak{L}_T} &= \{g \in G \mid g^{-1}c \cap V \in \mathfrak{L}_T\} \\ &= \{g \in G \mid e \in T(g^{-1}c \cap V)\} \end{aligned}$$

T は e において V 上局所的だから

$$= \{g \in G \mid e \in T(g^{-1}c)\}$$

さらに T は G の作用と可換であるから

$$= \{g \in G \mid g \in T(c)\} = T(c).$$

一方 $\mathfrak{L} \in \mathcal{L}_V$ に対し

$$\begin{aligned} \mathfrak{L}_{T_{\mathfrak{L}}} &= \{c \in 2^V \mid e \in T_{\mathfrak{L}}(c)\} \\ &= \{c \in 2^V \mid c \cap V \in \mathfrak{L}\} = \mathfrak{L}. \end{aligned}$$

よって $T \mapsto \mathfrak{L}_T, \mathfrak{L} \mapsto T_{\mathfrak{L}}$ は互いに他の逆写像である． □

$V \subseteq W$ のとき $\mathcal{L}_V$ は $\mathcal{L}_W$ の部分束になるが，これと同時に $\mathcal{T}_V$ は $\mathcal{T}_W$ の部分束になる．より詳細には次が成り立つ．

命題 1 $V \subseteq W \subseteq G$ とする．

1. $\mathcal{L}_V$ は $\mathcal{L}_W$ のイデアルである．すなわち，部分束でありかつ $\mathfrak{M} \subseteq \mathfrak{L}(\mathfrak{L} \in \mathcal{L}_V, \mathfrak{M} \in \mathcal{L}_W)$ ならば $\mathfrak{M} \in \mathcal{L}_V$．
2. $\mathcal{T}_V$ は $\mathcal{T}_W$ の部分ブール束である．すなわち，部分束でありかつ $T \in \mathcal{T}_V$ に対し $\neg_V T = \neg_W T$．

このことは，それぞれの空間で埋め込み $\mathcal{L}_V \subseteq \mathcal{L}_W$，$\mathcal{T}_V \subseteq \mathcal{T}_W$ が同型対応 $\mathcal{L}_V \cong \mathcal{T}_V, \mathcal{L}_W \cong \mathcal{T}_W$ と整合しないことを意味する．実際 $\mathfrak{L} \in \mathcal{L}_V$ を $\mathcal{L}_W$ の元とみて対応する遷移関数を $T^W_{\mathfrak{L}}$ と表せば，$T^W_{\mathfrak{L}} \leq T_{\mathfrak{L}}$ となる．一方，$T \in \mathcal{T}_V$ を $\mathcal{T}_W$ の元とみて対応する局所規則を $\mathfrak{L}^W_T$ と表せば，$\mathfrak{L}_T \subseteq \mathfrak{L}^W_T$ となる．

したがってまた G の部分集合の増大列 $\mathfrak{F} = \{V_i\}_{i \in \mathbb{Z}}$ によって得られる $\mathcal{L}_G$ のフィルター付け (1) と同様にして $\mathcal{T}_G$ のフィルタ付け

$$i \leq j \Rightarrow \mathcal{T}_{V_i} \subseteq \mathcal{T}_{V_j} \tag{2}$$

が得られるが (1) はイデアルによるフィルター付けであるのに対し，(2) は部分ブール代数によるフィルター付けである．前者からさらに次数付けに移行出来るが，後者は出来ない．

3.4 局所規則の合成

$V, W \subseteq G$ の積を

$$V \otimes W = \{vw \in G \mid v \in V, w \in W\}$$

で定める．これはアーベル群における Minkovskii 和 $\oplus$ の非可換版である．次に $\mathfrak{L} \in \mathcal{L}_V, \mathfrak{M} \in \mathcal{L}_W$ の局所合成を

$$\mathfrak{L} \diamond \mathfrak{M} = \{c \in 2^{V \otimes W} \mid \sigma_c^{-1}(\mathfrak{M}) \in \mathfrak{L}\}$$

と定義する．ここで $\sigma_c{:}V \to 2^W$ は，$c \in 2^{V\otimes W}$ に対し，

$$\sigma_c(v) = v^{-1}c \cap W$$

で定義される写像で，${\sigma_c}^{-1}(\mathfrak{M})$ はこの写像による $\mathfrak{M} \subseteq 2^W$ の逆像となる V の部分集合を表す．$\mathfrak{L} \diamond \mathfrak{M}$ はこれが $\mathfrak{L}$ のいずれかの元と一致するような様相 c の全体として定義されている．定義より $\mathfrak{L} \diamond \mathfrak{M} \in \mathcal{L}_{V\otimes W}$ である．

これを局所合成と呼ぶのは次の定理による．

定理 2 $\mathfrak{L} \in \mathcal{L}_V, \mathfrak{M} \in \mathcal{L}_W$ に対し $T_{\mathfrak{L}} \in \mathcal{T}_V$ と $T_{\mathfrak{M}} \in \mathcal{T}_W$ の合成写像 $T_{\mathfrak{L}} \circ T_{\mathfrak{M}}$ は e において $V \otimes W$ 上局所的な遷移関数であって，

$$T_{\mathfrak{L}} \circ T_{\mathfrak{M}} = T_{\mathfrak{L}\diamond\mathfrak{M}}$$

を満たす．

Proof. 最初に $T_{\mathfrak{L}} \circ T_{\mathfrak{M}} \in \mathcal{T}_{V\otimes W}$ を示す．G の作用と可換であることは明らかであるから e において $V \otimes W$ 上局所的であることを示せばよい．任意の様相 c に対して $T_{\mathfrak{m}}(c)$ と σ_c の定義から

$$T_{\mathfrak{M}}(c) \cap V = \{v \in V \mid \sigma_c(v) \in \mathfrak{M}\} \tag{3}$$

であることに注意する．そこで，2 つの様相 c, c' が $c \cap (V \otimes W) = c' \cap (V \otimes W)$ を満たすとする．この場合，任意の $v \in V$ に対し $vW \subseteq V \otimes W$ だから，特に $c \cap vW = c' \cap cW$，すなわち $\sigma_c(v) = \sigma_c(v)$ が成立する．よって先の注意により

$$T_{\mathfrak{M}}(c) \cap V = T_{\mathfrak{M}}(c') \cap V$$

を得る．一方

$$e \in T_{\mathfrak{L}}(T_{\mathfrak{m}}(c)) \iff T_{\mathfrak{M}}(c) \cap V \in \mathfrak{L} \tag{4}$$

(c' についても同様) だから

$$e \in T_{\mathfrak{L}}(T_{\mathfrak{M}}(c)) \iff T_{\mathfrak{L}}(T_{\mathfrak{M}}(c'))$$

となる．よって $T_{\mathfrak{L}} \circ T_{\mathfrak{M}}$ は e において $V \otimes W$ 上局所的である．

次に $\mathfrak{H} = \mathfrak{L}_{T_{\mathfrak{L}}\circ T_{\mathfrak{M}}}$ とおく．定理 1 により $\mathfrak{H}$ は $V \otimes W$ に台を持つ局所規則であって，$T_{\mathfrak{H}} = T_{\mathfrak{L}} \circ T_{\mathfrak{M}}$ を満たす唯一のものである．したがってこの $\mathfrak{H}$ が $\mathfrak{L} \diamond \mathfrak{M}$ に一致することを示せばよい．定義により

$$\begin{aligned}
\mathfrak{H} &= \{c \in 2^{V\otimes W} \mid e \in (T_{\mathfrak{L}}(T_{\mathfrak{M}}(c)))\} \\
&\text{(4) より} \\
&= \{c \in 2^{V\otimes W} \mid T_{\mathfrak{M}}(c) \cap V \in \mathfrak{L}\} \\
&\text{(3) より} \\
&= \{c \in 2^{V\otimes W} \mid \{v \in V \mid \sigma_c(v) \in \mathfrak{M}\} \in \mathfrak{L}\} \\
&= \{c \in 2^{V\otimes W} \mid {\sigma_c}^{-1}(\mathfrak{M}) \in \mathfrak{L}\} \\
&= \mathfrak{L} \diamond \mathfrak{M}.
\end{aligned}$$

□

3.5　フィルター付けと次数付け

G の部分集合の増大列 $\mathfrak{F} = \{V_i\}_{i\in\mathbb{Z}}$ が

$$V_i \otimes V_j \subseteq V_{i+j} \tag{5}$$

を満たすものとする．このとき，$\mathfrak{L}_G$ のフィルター付け (1)，$\mathcal{T}$ のフィルター付けはそれぞれ

$$\mathcal{L}_{V_i} \diamond \mathcal{L}_{V_j} \subseteq \mathcal{L}_{V_{i+j}} \tag{6}$$

$$\mathcal{T}_{V_i} \circ \mathcal{T}_{V_j} \subseteq \mathcal{T}_{V_{i+j}} \tag{7}$$

を満たす．

3.3 節の最期に注意したように，局所規則のブール代数 $\mathcal{L}_G$ の方はイデアルによるフィルター付けであることから，次の次数付きブール代数を得る:

$$\mathscr{L} = \otimes_i \mathscr{L}_i$$

ただし $\mathscr{L}_i$ は商ブール代数

$$\mathscr{L}_i = \mathcal{L}_{V_i}/\mathcal{L}_{V_{i-1}}$$

であって，本質的に V_i に台を持つ局所規則の全体とみなせる．$\mathscr{L}$ は局所合成から定まる積

$$\mathscr{L}_i \diamond \mathscr{L}_j \subseteq \mathscr{L}_{i+j}$$

を持つ．$\mathscr{L}$ を群 G 上の局所規則のなす次数ブール代数と呼ぶ．$\mathscr{L}$ の構造が列 $\mathfrak{F}$ のとり方にどれだけ依存するかは不明である．

4　計算結果

本研究では 2 近傍の局所規則同士での合成から 3 近傍の局所規則を，2 近傍の局所規則と 3 近傍の局所規則から 4 近傍の局所規則を，3 近傍の局所規則同士での合成から 5 近傍の局所規則を求めた．

4.1　具体的な合成手順

まず通常の 1 次元セルオートマトンを考える．この場合 $G = \mathbb{Z}$（無限長の場合）または $\mathbb{Z}_N$（N-周期の場合）である．左右に近傍をとる局所規則を考えるならば

$$V_i = \begin{cases} \emptyset & (i < 0) \\ \{-i, \cdots, 0, \cdots, i\} & (i \geq 0) \end{cases}$$

ととれば（N-周期系で i が $N/2$ を超える場合は $V_i = G$ とする），列 $\mathfrak{F} = \{V_i\}$ は (5) を満たす増大列である．この場合，等号

$$V_i \otimes V_j = V_{i+j}$$

が成り立つ．
次に，左右片側だけに近傍を取る局所規則の場合を考える．

$$V_i = \begin{cases} \emptyset & (i < 0) \\ \{0, \cdots, i-1, i\} & (i \geq 0) \end{cases}$$

ただし，N-周期系で $N \geq i$ の場合は $V_i = G$ とする．このときも列 $\mathfrak{F} = \{V_i\}$ は増大列で (5) を統合で満たす．
2^{V_i} を 2^{i+1} と同一視し，V_i に台を持つ局所規則 $\mathfrak{L} \subseteq \mathcal{L}_{V_i}$ を $i+1$ 変数関数 $\mathfrak{L}(x_0, \cdots, x_i)$ として表す．ただし

$$\mathfrak{L}(x_0. \cdots, x_i) = \begin{cases} 1 & ((x_0, \cdots, x_i) \in \mathfrak{L}) \\ 0 & ((x_0, \cdots, x_i) \notin \mathfrak{L}) \end{cases}$$

このとき $\mathfrak{L}$ が定める遷移関数は

$$T_{\mathfrak{L}}{:}(c_n) \mapsto (c'_n), c'_n = \mathfrak{L}(c_n, \cdots, c_{n+1})$$

となる．ただし，N-周期のときは添え字は N を法として考える．
今，局所規則 $\mathfrak{L} \in \mathcal{L}_{V_i}, \mathfrak{M} \in \mathcal{L}_{V_j}$ の合成 $\mathfrak{L} \diamond \mathfrak{M} \in \mathcal{L}_{V_{i+j}}$ は

$$(\mathfrak{L} \diamond \mathfrak{M})(x_0, \cdots, x_{i+j}) = \mathfrak{L}(\mathfrak{M}(x_0, \cdots, x_j), \cdots, \mathfrak{M}(x_i, \cdots, x_{i+j}))$$

と簡単に記述できる．

4.2　2 近傍同士の合成

3 近傍の局所規則を $\mathfrak{L} \in \mathcal{L}_{V_2}$，2 近傍の局所規則を $\mathfrak{M}, \mathfrak{N} \in \mathcal{L}_{V_1}$ としたとき，

$$\mathfrak{L}(x_0, x_1, x_2) = (\mathfrak{M} \diamond \mathfrak{N})(x_0, x_1, x_2) = \mathfrak{M}(\mathfrak{N}(x_0, x_1), \mathfrak{N}(x_1, x_2))$$

となる．2 近傍の局所規則同士で合成した結果，62 個の 3 近傍の局所規則が生成された．生成された局所規則は，合成の組み合わせが複数存在している．以下に 2 近傍の局所規則の合成表を示す．

$\mathfrak{N}\backslash\mathfrak{M}$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	255	0	255	0	255	0	255	0	255	0	255	0	255	0	255
1	0	236	16	252	2	238	18	254	1	237	17	253	3	239	19	255
2	0	209	34	243	12	221	46	255	0	209	34	243	12	221	46	255
3	0	192	48	240	12	204	60	252	3	195	51	243	15	207	63	255
4	0	139	68	207	48	187	116	255	0	139	68	207	48	187	116	255
5	0	136	68	204	34	170	102	238	17	153	85	221	51	187	119	255
6	0	129	66	195	24	153	90	219	36	165	102	231	60	189	126	255
7	0	128	64	192	8	136	72	200	55	183	119	247	63	191	127	255
8	0	55	8	63	64	119	72	127	128	183	136	191	192	247	200	255
9	0	36	24	60	66	102	90	126	129	165	153	189	195	231	219	255
10	0	17	34	51	68	85	102	119	136	153	170	187	204	221	238	255
11	0	0	48	48	68	68	116	116	139	139	187	187	207	207	255	255
12	0	3	12	15	48	51	60	63	192	195	204	207	240	243	252	255
13	0	0	12	12	34	34	46	46	209	209	221	221	243	243	255	255
14	0	1	2	3	16	17	18	19	236	237	238	239	252	253	254	255
15	0	0	0	0	0	0	0	0	255	255	255	255	255	255	255	255

4.3 2 近傍と 3 近傍の合成

局所規則の合成は非可換であるため 2 近傍の局所規則と 3 近傍の局所規則の合成は，2 近傍の局所規則を $\mathfrak{A} \in \mathcal{L}_{V_1}$，3 近傍の局所規則を $\mathfrak{B} \in \mathcal{L}_{V_2}$，4 近傍の局所規則を $\mathfrak{C} \in \mathcal{L}_{V_3}$ としたとき，

$$
\begin{aligned}
\mathfrak{C}(x_0, x_1, x_2, x_3) &= (\mathfrak{A} \diamond \mathfrak{B})(x_0, x_1, x_2, x_3) \\
&= \mathfrak{A}(\mathfrak{B}(x_0, x_1, x_2), \mathfrak{B}(x_1, x_2, x_3)) \\
\mathfrak{C}(x_0, x_1, x_2, x_3) &= (\mathfrak{B} \diamond \mathfrak{A})(x_0, x_1, x_2, x_3) \\
&= \mathfrak{B}(\mathfrak{A}(x_0, x_1), \mathfrak{A}(x_1, x_2), \mathfrak{A}(x_2, x_3))
\end{aligned}
$$

の 2 通り存在する．上を計算した結果，2 近傍同士の時と同じように一つの局所規則を生成する合成の組み合わせが複数存在した．また異なる素な局所規則の組み合わせから同じ合成規則が生成されることも確認できた．

4.4 5 近傍の局所規則を生成する合成

5 近傍の局所規則は 3 近傍の局所規則同士の組み合わせと，2 近傍の局所規則と 4 近傍の局所規則の組み合わせから生成される．今回は 3 近傍同士の合成した結果，上の結果と同様に同じ局所規則が異なる組み合わせから生成されることが確認できた．

4.5　規則全体における合成規則の割合

次数 i の局所規則全体における合成規則は次数 1 から次数 $i-1$ までの局所規則の組み合わせの総和よりも小さくなる．また合成規則はすべて複数の組み合わせを持つことから，次数 1 から次数 $i-1$ までの組み合わせの総和の半分以下と考えられ，次数 i の局所規則全体における局所規則の割合は

$$\sum_{k=1}^{i-1}(\mathcal{L}_{V_k} * \mathcal{L}_{V_{i-k}})/2\mathcal{L}_{V_i} = \sum_{k=1}^{i-1}(2^{2^{k+1}} * 2^{2^{i-(k+1)}})/(2 * 2^{2^{i+1}})$$

と表すことができる．

5　まとめ

本研究では 2 近傍の局所規則同士の合成から 3 近傍の局所規則を，2 近傍の局所規則と 3 近傍の局所規則の合成から 4 近傍の局所規則を，3 近傍の局所規則の合成から 5 近傍の局所規則を求めた結果，同じ合成規則が異なる組み合わせから生成されることを，また同じ合成規則を生成する組み合わせには異なる素な局所規則が含まれることから，5 近傍までの局所規則における素な局所規則の確認と局所規則の因数分解は一意には求められないこと，素因数分解も一意には求められない可能性があることが分かった．

一つの合成された局所規則が複数の合成パターンを持つことは，セルオートマトン公開鍵暗号においては，一つの公開鍵に対して複数の秘密鍵が対応することになる．公開鍵である合成規則から秘密鍵である合成パターンを求めるには，局所規則の分解が出来ない為に，公開鍵よりも近傍が小さい局所規則の合成パターンをすべて試す必要がある．局所規則は近傍数に応じて総数が指数関数的に増えていくため，公開鍵の近傍数をある程度大きくすればその合成パターンを求めるのにはかなりの時間とメモリが必要になる．また一つの公開鍵に対して複数の秘密鍵が対応することは，秘密鍵を複数の受信者に割り当てることで暗号文を共有することが出来る．

参考文献

[1] P.Guan. *Cellular automaton public key cryptosystem.* Complex Systems. 1:51-56. 1987

[2] J.L.Schiff. 梅尾博司.『セルオートマトン』．共立出版．2011

[3] 小倉久和.『情報の基礎離散数学　ー演習を中心としたー』．近代科学社．1999

[4] 藤尾光彦.『$\mathrm{XOR}^2 = 90$　ー局所遷移規則のなす次数ブール代数の構造についてー』．2007 年度冬の LA シンポジウム．2007