IS

情報システム学科
Department of Information Systems

研究室 数理情報研究室　教員名 斉藤　隆　カテゴリー IT・IoT・AI・ロボティクス

有限体上の多項式を状態とするセルオートマトン

1　セルオートマトン

定義 1.1 (1 次元セルオートマトン)
$\mathrm{CA} = (Q, Z, N, f)$
Q：状態集合　有限体 $\mathrm{GF}(q) = \mathrm{GF}(p^n)$,
　p：素数，n：自然数，$|Q| = q = p^n$
Z：整数全体の集合　セル空間，セルの位置 $i \in Z$
N：近傍
f：局所関数

$$f : Q \times Q \times Q \to Q$$
$$f(x, y, z) = u_0 + u_1 x + u_2 y + \cdots + u_i x^h y^j z^k + \cdots + u_{q^3-2} x^{q-1} y^{q-1} z^{q-2} + u_{q^3-1} x^{q-1} y^{q-1} z^{q-1},$$
$$u_i \in Q \ (0 \le i \le q^3 - 1)$$

x，y，z はそれぞれ近傍セル，
-1（左），0（自分自身），$+1$（右）の状態

以下，$N = \{-1, 0, +1\}$ とし，$\mathrm{CA} = (Q, f)$ と書く。

定義 1.2 (大域写像 F)
様相の集合 $C = Q^Z$
様相 $c \in C$ の位置 $i \in Z$ のセルの状態 $c(i)$
$F : C \to C$
$F(c)(i) = f(c(i-1), c(i), c(i+1))$
$F^{t+1}(c) = F(F^t(c))$，$F^0(c) = c$

例 1.1 (GF(4))
$\mathrm{GF}(4) = \mathrm{GF}(2^2) = \{0, 1, \omega, 1+\omega\}$
$\omega^2 + \omega + 1 = 0$

$+$	0	1	ω	$1+\omega$
0	0	1	ω	$1+\omega$
1	1	0	$1+\omega$	ω
ω	ω	$1+\omega$	0	1
$1+\omega$	$1+\omega$	ω	1	0

$\cdot$	0	1	ω	$1+\omega$
0	0	0	0	0
1	0	1	ω	$1+\omega$
ω	0	ω	$1+\omega$	1
$1+\omega$	0	$1+\omega$	1	ω

2　情報 X と CA[X]

定義 2.1 (多項式状態 $Q[X]$)
情報変数 X：セルの未知の状態，情報
多項式 $g : Q \to Q$
$$g(X) = a_0 + a_1 X + \cdots + a_i X^i + \cdots + a_{q-1} X^{q-1},$$
$$a_i \in Q \ (0 \le i \le q-1)$$
$Q[X] = \{g \mid g : Q \to Q\}$, $|Q[X]| = q^q$, $Q[X] \supset Q$

例 2.1 $g(X) = a_0 + a_1 X + a_2 X^2$,
$a_i \in \mathrm{GF}(3) = \{0, 1, 2\}$

a_0	a_1	a_2	$g(X)$	$g(0)$	$g(1)$	$g(2)$
0	0	0	0	0	0	0
0	0	1	X^2	0	1	1
	$\vdots$		$\vdots$		$\vdots$	
2	2	0	$2+2X$	2	1	0
2	2	1	$2+2X+X^2$	2	2	1
2	2	2	$2+2X+2X^2$	2	0	2

定義 2.2 (多項式状態 CA[x])
$\mathrm{CA} = (Q, f) \Rightarrow \mathrm{CA}[X] = (Q[X], f_X)$
$f_X : Q[X] \times Q[X] \times Q[X] \to Q[X]$
　f と同じ近傍の多項式，$x, y, z \in Q[X]$
様相集合 $C_X = Q[X]^Z$
大域写像 $F_X : C_X \to C_X$

3　CA[X] と CA

定義 3.1 (置換 ψ)
$g(X) \in Q[X], a \in Q \Rightarrow \psi_a(g) = g(a)$
$\psi_a : Q[X]^Z \to Q^Z$
$\psi_a(c)(i) = \psi_a(c(i)), i \in Z.$

定理 3.1
- CA[X] が単射 ⇔ CA が単射
- CA[X] が全射 ⇔ CA が全射
- CA[X] が可逆 ⇔ CA が可逆

4　完全性と退化

定義 4.1 (完全様相)
$G \subseteq Q[X]$ が完全
⇔ G の多項式（と定数）から
　$+$，$-$，$\cdot$ を使って X が計算できる
様相 c_X が完全
⇔ $G_{c_X} = \{c_X(i) \mid i \in Z\} \subseteq Q[X]$ が完全

例 4.1 $\{\omega X + (1+\omega)X^2, X + (1+\omega)X^2\}$
$$\Rightarrow \omega \cdot (\omega X + (1+\omega)X^2) \cdot (X + (1+\omega)X^2)$$
$$= \omega \cdot (1+\omega)X = X$$

定理 4.1 (非完全性の単調性)
c が完全でない ⇒ $F(c)$ が完全でない

定義 4.2 (退化)
$|\{\psi_a(c) \mid a \in Q\}| = |Q| - m$
⇒ $c_X \in Q[X]^Z$ が m-退化
m を退化度とよび $m(c_X)$ と書く。
　$m(c_X) \neq 0$ のとき，様相 c_X は退化。

定理 4.2 (退化の単調性)
$m(c_X) \le m(F(c_X))$

定理 4.3 様相が完全 ⇔ 様相が退化していない

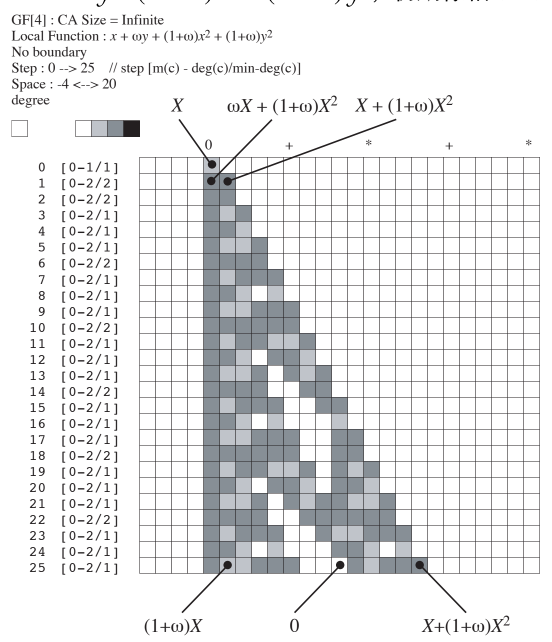
5　完全性と可逆性

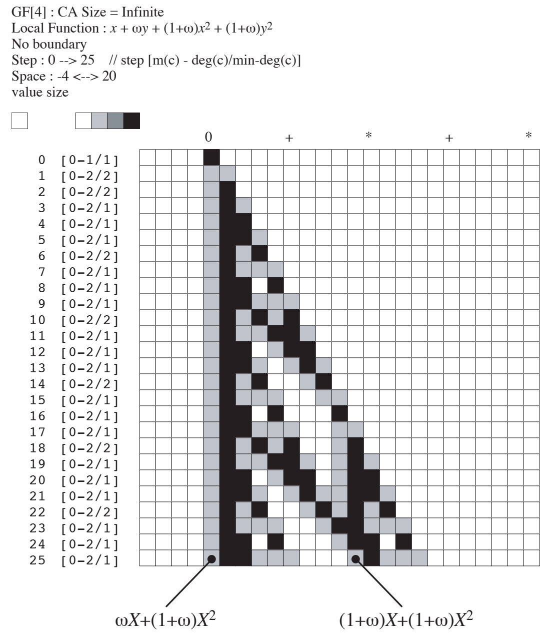
定義 5.1
大域写像 F が可逆
⇔ 逆写像 F^{-1} があるセルオートマトンの大域写像

定義 5.2 完全な様相の集合 $C_X^{cp} \subseteq C_X$
$F_X(C_X^{cp}) \subseteq C_X^{cp}$ ⇒ 大域写像 F_X は完全性保存

定理 5.1 CA[X] が完全性保存 ⇔ CA が可逆

例 5.1 (Korec's reversible 4-state CA)
$Q = \mathrm{GF}(4)$
$f = x + \omega y + (1+\omega)x^2 + (1+\omega)y^2$，初期様相 $\bar{0}X\bar{0}$





$f = x + \omega y + (1+\omega)x^2 + (1+\omega)y^2$　(Korec)
⇔ $f = y + (1+\omega)z + (1+\omega)y^2 + (1+\omega)z^2$ (reverse)

degree　$c_X \in C_X$ に対して
$$\deg(c_X) = \max\{\deg(c_X(i)) \mid i \in Z\}$$
value size
　$g \in Q[X]$ に対して
$$V(g) = |\{g(0), g(1), \cdots, g(\alpha_i), \cdots, g(\alpha_{q-1})\}|$$