一次元可逆性セルオートマトンの暗号・符号への応用

研究概要

セルオートマトンは複雑系の中でも中心的な研究対象であり、物理学（粒子の衝突力学）、生物学（細胞の自己増殖）、化学（結晶の生成）、交通工学等への応用があるが本研究は一次元可逆性セルオートマトンを用いて暗号・符号への応用を研究する。

総合情報学部 総合情報学科

佐藤 忠一 教授 Tadakazu Sato

研究キーワード：並列写像 局所関数 セルオートマトン 暗号

URL： http://researchmap.jp/read0129616

研究シーズの内容

一次元セルオートマトンは同一の有限オートマトンを直線状に並べ各オートマトンは自分の周辺のオートマトンの状態を見て、同一の局所関数で一斉に変換するネットワーク型の並列処理システムである。1つの局所関数 $f(x_1,\cdots,x_n)$ が与えられると自分のオートマトンを含めたn個のオートマトンの状態を見て、次の時刻での自分の新しい状態が $f(x_1,\cdots,x_n)$ で計算される。このプロセスを各オートマトンが一斉に行いそれぞれの状態を変える。この局所関数はオートマトンの状態の集合を Q とすると Q のnタップルから Q への写像であり、一斉の変換は並列写像と呼ばれ、状態の空間分布から新しい状態の空間分布を与える写像となる。

可逆性セルオートマトンとはこの並列写像 F が逆変換を有するときで、ある局所関数の並列写像が F の逆写像になっている時である。二次元以上のセルオートマトンでは可逆性を判定するアルゴリズムが存在しないが一次元セルオートマトンでは可逆性を判定するアルゴリズムが存在する。

本研究では局所関数 $f(x_1,\cdots,x_n)$ からド・ブルーチングラフを作り、その状態遷移行列を A で表すとAは記号列上の行列であり、記号の連接を乗法とする非可換環上の行列である。このAの代数構造を調べることによりセルオートマトンが可逆性を持つか否かが決定できる。

可逆性の判定条件：一次元セルオートマトンが可逆性を有するための必要かつ十分条件は次の等価な各命題が成立することである。

(1) 状態遷移行列 A は唯一の非零の固有値 $(a_0+a_1+\cdots+a_{m-1})$ を持つ。ここで Q=$\{a_0,a_1,\cdots,a_{m-1}\}$
(2) A の隣接行列は行列の乗法表が閉じてそれらの行列はすべて唯一の非零の固有値 1 を持つ。

活用例・産業界へのアピールポイント

新しい暗号化の実用化

特記事項(関連する発表論文・特許名称・出願番号等)