

タイトル	一次元可逆性セルオートマトンの暗号・符号への応用			
分野	キーワード	① 並列写像	② 局所関数	
情報・通信				
研究者氏名: 佐藤 忠一		[お問い合わせ先]		
(所属: 総合情報学部総合情報学科)		TEL: 049-239-1444		
		メールアドレス: sato_t@toyo.jp		

【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。すなわち、与えられた入力系列を可逆性セルオートマトンで変換(暗号化、符号化)する。そして、変換された系列を逆セルオートマトンで逆変換(解読、復号化)する。そのために、セルオートマトンが可逆性を有する条件を調べる。

【研究内容】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 $f(x_1, \dots, x_n)$ 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 $f(x_1, \dots, x_n)$ 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 $f(x_1, \dots, x_n)$ からド・ブルーチンググラフを作り、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、記号の接続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 $(a_0 + a_1 + \dots + a_{m-1})$ を持つ。ここで $Q = \{a_0, a_1, \dots, a_{m-1}\}$
- (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。

【実用化・活用が見込まれる分野・対象業種等】
新しい暗号化の実用化

【関連特許】(特許名称・出願番号等)