

カオス分岐におけるカオス性の考察

元井 和征 清水 能理

八戸工業大学

1 はじめに

カオス力学系を用いた秘匿通信システムを構築する場合、カオス発振回路の時系列はカオス性を有している必要がある^[1, 3, 5]。一方、確率・統計論に基づいた時系列解析の 1 つにサロゲートデータ法を用いたカオス性の検定が提案されている^[2]。そこで、カオス発振回路における有効なパラメータ値を、サロゲートデータ法を応用して決定することを目的とする。

2 問題の記述

秘匿通信系のカオス時系列は、変調部と復調部とも同様のカオス性が必要となる^[3, 5, 7]。カオスモデルは、分岐パラメータの値により軌道の位相的性質を変える現象が起こる。カオス挙動を示すとき多くの不安定周期点を持っているが、パラメータのとり値によっては周期性を示す窓を生じる^[1, 4]。よって、カオス利用のシステムにおけるパラメータ設定が問題となる。

3 カオス発生回路

カオスの生じる電気回路として、負性抵抗を有する Chua 回路に注目した。3 階の系のカオス発生回路で、インダクタ、抵抗、2 個のキャパシタ、非線形抵抗から成る^[1, 2, 6](図 1)。

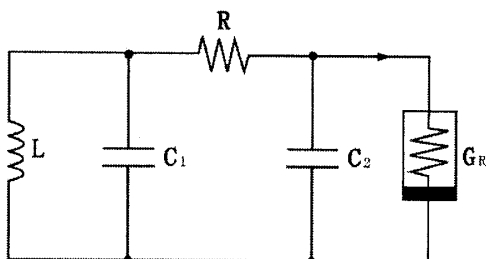


図 1 Chua 回路

Chua 回路の分岐図(図 2)を見ると、系がカオス的振る舞いをする領域は推定できるが、窓の存在を確認し難いことがわかる。

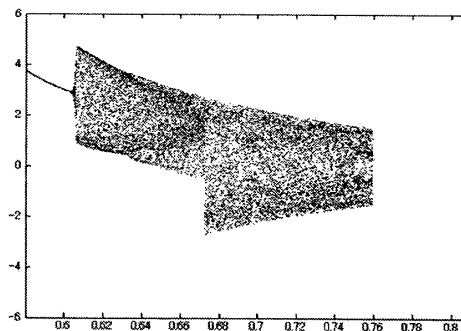


図 2 Chua 回路の分岐図

4 サロゲート法^[2]

カオス応答を示す重要な要因は非線形性にある。サロゲートデータ法は、観測された時系列に対する線形確率過程の存在を帰無仮説として提示し、非線形統計量の推定を通じて検定する。そして、帰無仮説を棄却することで非線形の存在を示す。基本アルゴリズムは、(1)「観測された時系列信号は、時間的に全く無相関である」という帰無仮説に従うランダム・シャッフル(RS)、(2) 帰無仮説「観測された時系列信号は、時間的に線形相関を持つ確率的データである」に従うフーリエ・変換(FT)、(3) 帰無仮説「観測された時系列信号は、非線形確率過程から作り出されたが、観測する際に性的な単調非線形変換を施されたことにより得られたデータである」に従うアンプリチュード・アジャステッド・フーリエ・変換(AAFT)である。

5 提案手法

提案する分岐パラメータ設定手法について、以下にまとめる。

- (1) Chua 回路における分岐パラメータ G の値を変化させていき、各値のときの Chua 回路から出力される時系列信号を計算する。
- (2) 横軸に G の値、縦軸に出力信号の状態を取る。各 G の値において、(1)で得られた信号の値を重ねてプロットし、カオス分岐図を作成する。
- (3) (2)で作成した分岐図の形態をもとに、時系列がカオス的振る舞いをする領域の分岐パラメータ値の範囲を推定する。

Consideration of Chaotic Characteristic in Chaos Bifurcation

Kazumasa MOTOI · Hachinohe Institute of Technology

Yoshimasa SHIMIZU · Hachinohe Institute of Technology

(4) 推定した領域において特定した分岐パラメータ値を用いたときの時系列データに対して、サロゲート法を適用し、シミュレート結果からカオス窓か否かの検定を行う。

6 シミュレーション

FT サロゲート法を用いた数値実験の結果を以下に示す。オリジナルデータとサロゲートデータの統計量を比較すると、表 1 のように平均、分散ともにサロゲートデータ作成過程において統計量が保存されていた。一方、FT アルゴリズムの性質上、頻度分布は保存されない。図 3 と図 5 の信号を比較すると、オリジナルデータ時系列信号の構造は全く壊されている。このことから、分岐パラメータが 0.70 値をとる場合、時系列信号は線形なダイナミクスで表現することが難しいことがわかる。

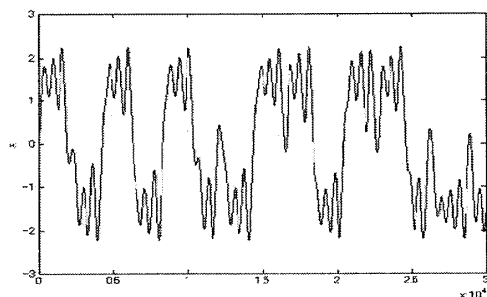


図 3 Chua 回路における時系列信号 ($G=0.70$)

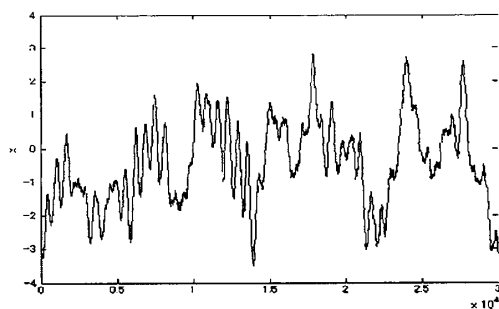


図 4 FT サロゲート変換信号 ($G=0.70$)

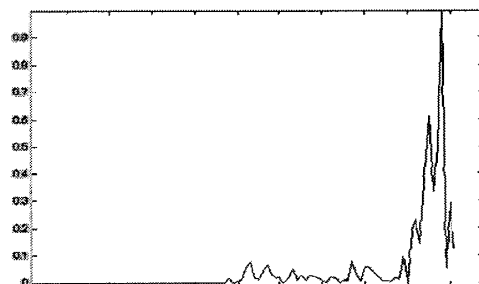


図 5 変換信号のパワースペクトル ($G=0.70$)

表 1 FT サロゲートデータ作成過程において保存される統計量

平均	分散	頻度分布	自己相関
○	○	×	○

※保存される○ 保存されない×

7 カオス分岐を用いた秘匿通信システムへの応用

カオス分岐を行った変調部の状態は、カオス性を保持していなければならないので、分岐パラメータの範囲を検証する必要がある^[6,7]。よって、サロゲート法によるカオス性の検定と分岐図を用いたカオス分岐パラメータの範囲設定を行う。カオス同期化部の状態を暗号鍵として用いてカオス分岐を発生させたカオス波形に基づいた暗号化関数を設計し、暗号化・復号を行う。従来の手法のように暗号化関数を複雑にする必要がなく、その逆関数を求める困難さが小さい。

8 まとめ

カオス分岐図を用いて設定した分岐パラメータ値における Chua 回路からの時系列信号に対し、サロゲートデータ法を適用し、カオス性の検定を行った。特定パラメータ値における Chua 回路からの出力がカオス的であることを示すことができ、サロゲートデータ法を用いたカオス検定は有効であった。

よって、カオス同期化部の状態を暗号鍵として用い、変調部、復調部にカオス分岐を発生させる Chua 回路を用いた秘匿通信システムにおける分岐パラメータの探索は、サロゲートデータ法を用いることが有効である。

参考文献

- [1] 鈴木 昱雄:カオス入門, コロナ社, 2000
- [2] 合原一幸, 池口徹, 山田泰司, 小室元政:カオス時系列解析の基礎と応用, 産業図書, 2000
- [3] 潮 俊光:「カオス同期化制御とその秘匿通信への応用」, 情報処理学会 pp. 525-530, 1995
- [4] 合原一幸:カオスセミナー, 海文堂出版, 1994
- [5] 潮 俊光:「カオスの通信への応用」, 電子情報通信学会, pp. 47-54, 1997
- [6] 藤井恭平, 清水能理:カオス発生回路を用いた秘匿通信システムの製作, 平成 20 年度 第 1 回情報処理学会東北支部研究会, 講演資料, セッション 1, 講演番号 4, 2008.12
- [7] 目黒友紀, 清水能理:カオス制御を応用したカオス同期化システム, 平成 20 年度 第 2 回情報処理学会東北支部研究会, 講演資料, セッション 2, 講演番号 9, 2008.12
- [8] 元井和征, 清水能理:カオス分岐と窓に関する考察, 平成 20 年度 第 4 回情報処理学会東北支部研究会, 講演資料, 2009.2