L-008

カオス通信系における標本化・量子化の影響

Influence of Sampling and Quantization in Chaos Communication System

清水 能理
Yoshimasa Shimizu

1. まえがき

情報の漏洩を防ぐため、通信系の構築では秘匿性を向上させる必要がある。カオスデータの特徴解析を行い、通信系構築における秘匿性向上に活用する。カオスデータの中には様々な秘匿性が隠されている。また、あらゆる組合せの多値を内包しており、鍵とコード表のバランスも非常に良い。自然界に存在するカオスデータをモデリングすることで、ディジタル通信系に応用するためには、離散化といった操作を行う必要があり、カオス性への影響が懸念される。カオスデータを、秘匿通信系に用いられる同期システムに応用しコンピュータで処理するためには、標本化・量子化データを用いる必要があり、分岐パラメータを適切に設定する必要がある。カオス性の検定にはサロゲート法などがあるが、ポアンカレ切断面（セクション）最適化や量子化の評価が必要である[1-3]。

2. 問題の記述

アナログのカオスデータをディジタル系に応用するためには、標本化および量子化といった操作を行う必要がある。システムのデータを離散化してコンピュータで処理する場合、その影響を評価することも重要である。したがって、ポアンカレ切断面リカレンスプロットの手法を応用し、カオス試供回路の代表である Chua 回路を対象として、セクション（切断面）の最適化を考察する。連続時間データを離散化する方法として、ポアンカレセクション法や量子化する同相変換法がある。得られたデータのカオス性を定量的に評価するサロゲート法があるが、セクションの最適化や量子化データの評価には煩雑である。一方、セクション出力データからポアンカレ写像が容易に得られる[4-6]。

3. 提案手法

同一のカオスデータでも選択するセクションによってはカオス性が示唆されない場合がある。これは量子化に伴う量子化誤差の原因となると考えられる。よって、最適なセクション選択とその評価が必要となる。そこで、連続時間データを離散化するとき、ポアンカレ写像を用いる[2]。連続時間データに対し標本化・量子化を行い、カオス性の検証を行う。セクション最適化や量子化の評価には、サロゲート法を適用する。各セクションにおける離散化データをポアンカレ写像で表わし、量子化データのサロゲート法カオス評価結果と比較する。

八戸工業大学, Hachinohe Institute of Technology

4. 標本化

ポアンカレ切断面は、同方向に通過するストレンジアトラクタ軌道の交点を、プロットしたグラフを表す。ポアンカレ切断面の指定は、ポアンカレ切断面リカレンスプロットにおいて、注目している点のインデックスを指定することで行う。ポアンカレ切断面である位相空間の超平面を座標系として、プロットされた全ての点について、各座標軸における最小値を新たな座標とする下限点と、ポアンカレ切断面を通過する軌道の交点とのユークリッドノルムをプロットしたグラフとして表示される。

5. 量子化

標本化で得られた離散時間信号のアナログデータを、整数などの離散値で、近似的に変換操作する。ある範囲のアナログ値は、全て一つのディジタル値に変換されてしまうため、測定データとしては連続しない離散値となる。信号の強度を表現するのに、どのくらいの情報量を用いるかを量子化ビット数とすると、変換した際に生じる量子化誤差は、真のアナログ値と離散化値との誤差である。量子化誤差を小さくするためには、変換のビット数を多くする必要がある。したがって、ディジタル変換には式(1)の同相変換量子化を用い、カオスの内部状態をディジタルデータへと変換する。

$$y_{t,n} = \frac{2}{\pi}\arcsin\sqrt{x_t}\cdot 2^n$$
$$Y_{t,n} = \left[\frac{2}{\pi}\arcsin\sqrt{x_t}\cdot 2^n\right] \quad \cdots(1)$$

カオスの内部状態は無理数であるが、同相変換量子化したデータを観測すると、有理数で表される時系列としてカオスが観測できる。

6. サロゲート法

観測された時系列信号に対する線形確率過程の存在を帰無仮説として提示し、ある非線形統計量の推定を通じて検定する。帰無仮説を棄却することで時系列信号における非線形の存在を示す。帰無仮説に従うサロゲートデータを多数作りだし、統計的性質がオリジナルと異なることを示す。

7. カオス性の評価

サロゲートデータの特徴量が正規分布すると仮定できる場合、以下の式（2）で定義する検定統計量 S を用いて評価する。Q_H が正規分布するとき、$S>1.96$ であれば有意水準 $\alpha=0.05$ で与えられた帰無仮説を棄却し、カオス性を判定

する。

$$S = \frac{|Q_0 - \mu Q_H|}{\sigma Q_H} \quad \cdots(2)$$

Q_0：オリジナルデータの非線形統計量
μQ_H：サロゲートデータの非線形統計量
σQ_H：サロゲートデータの非線形統計量標本標準偏差

6．シミュレーション

カオス発振回路である Chua 回路のアトラクタに対して、ポアンカレ切断面リカレンスプロットを用いた。連続アナログデータを離散化した後、得られた標本化データからポアンカレ写像を生成した。最適セクションの決定方法を模索するため、複数のセクションのサンプリングを行い、それぞれの評価・比較を行った。図１に、Chua 回路のストレンジアトラクタを示す。このとき、３次元データに対して、ポアンカレ切断面を用いた標本化データは、図２のようになった。さらに、ポアンカレ写像は、図３のように計算できた。

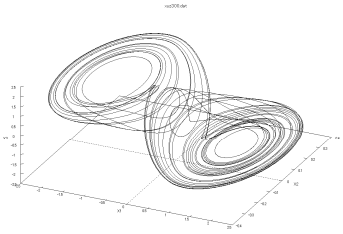

図１　ストレンジアトラクタ（Chua 回路）

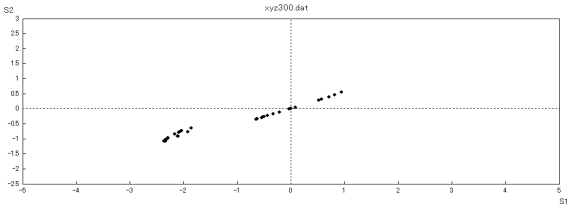

図２　Chua 回路のポアンカレ切断面

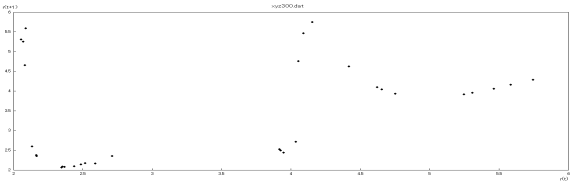

図３　Chua 回路のポアンカレ写像

Chua 回路からの出力に対して、ポアンカレ切断面を用いた標本化と、さらに同相変換量子化を行い得られた３次元データのうち、x 変数の時系列に対して、リアプノフ指数を用いたカオス性の検証を行った。分解能８で同相変換量子化した、ディジタルカオスデータのリアプノフスペクトラムは、図４のようになった。

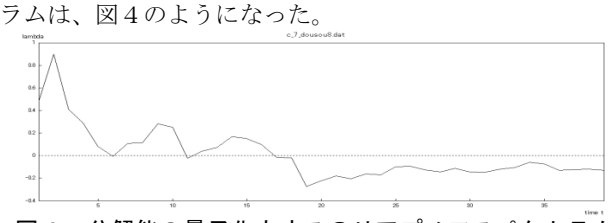

図４　分解能８量子化カオスのリアプノフスペクトラム

表１は、各サロゲートデータアルゴリズム法に対する検定統計量の結果と比較である。

表１　サロゲート法における検定統計量 S

	RS	FS	FT	AAFT	IAAFT
S of Chua	0.621	3.6884	0.2123	0.335	5.8020

8．ディジタル通信

ディジタル通信システムの秘匿性向上のため、カオスデータを応用するには、同相変換量子化を用いてアナログからディジタルへ、データの量子化を行う。このとき、カオスデータがカオス性を保持していなければ、正常な暗号化処理と復号処理ができない。暗号化および復号の手法は、以下の手順とする。

①送信系と受信系とで同期化制御を行い、得られた状態を共通鍵とする。

②共通鍵を初期値と分岐パラメータ値に用いて発生させた状態を量子化して得られるカオス乱数と、情報信号との EXOR（排他的論理和）を計算して、暗号を生成する。

③復号演算は、暗号化と同じ EXOR を用いることできる。カオスを量子化する際、カオス性が失われていないか判定するため、リアプノフ指数スペクトラム計算部とサロゲートデータ計算部を、暗号化演算部に設け、カオス性の評価を逐次的に行う。

9．まとめ

カオスデータのストレンジアトラクタに対して、ポアンカレセクションを用いて、セクション最適化の方法を検討した。定性的な方法としてポアンカレ切断面、定量的な方法としてリアプノフ指数を用いた。次に、同相変換量子化を行い、アナログデータをディジタルデータへと変換した。このときリアプノフ指数を適用し、カオス性の判定手法を検証した。さらに、セクション出力データに対し、サロゲートアルゴリズム法を応用して検定を行った。このとき、ポアンカレ写像と比較を行い、量子化データのカオス評価を検討した。量子化の影響は、カオスデータのディジタル化に伴う量子化誤差が、カオス判定に用いる統計量 [1]に影響をもたらしたと考えられる。

今後は、①別の位置の切断面で標本化したデータと比較すること、②最適なポアンカレ切断面の設定手法について、サロゲート法も用いてカオス性の有無を判定すること、を目標に進める。さらに、定量的な方法として、サロゲートデータのリアプノフ指数を用いる手法も考えられる。

参考文献

[1] 鈴木昱雄：カオス入門，コロナ社（2000）.
[2] 合原一幸：カオスセミナー，海文堂出版（1994）.
[3] 潮 俊光：カオス通信への応用，電子情報通信学会論文誌 A，Vol.J82-A，pp.1801-1807（1999）.
[4] 庄野克房：カオスエンジニアリング，シュプリンガー・フェラアーク東京（2002）.
[5] 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）.
[6] 鳥谷部 大地，清水能理，石鉢大輔：ポアンカレ切断面に基づく時系列解析を用いたカオス通信系構築，計測自動制御学会第 258 回研究集会講演資料（2010）.