

アナログ CMOS カオス回路による乱数生成

○濱里 主巳 常田 明夫 井上 高宏
(熊本大学工学部)

1 はじめに

カオスは、決定論的システムから生じるランダムな現象であり、その代表的な応用例は乱数生成器である。カオス軌道を生成するために、計算機がしばしば用いられるが、デジタル演算により生成されたカオス軌道は周期軌道となるため、真の乱数とはいえない。一方、アナログ回路より生成されるカオス軌道は非周期軌道となり、周期性の問題は解決できるが、生成されたカオス軌道の統計的性質(乱数としての性能評価)にはほとんど注意が払われていない。本稿では、良好な統計的性質をもつ非周期カオス系列の生成を目的として、アナログ回路で実現可能な 1 次元写像を提案し、計算機シミュレーション、及び実験によりその特性を検討する。

2 区分線形 N 型写像

カオスは 1 次元差分方程式 $x_{n+1} = \tau(x_n)$ ($n = 0, 1, 2, \dots$) で生成することが可能である。ここで、 $\tau(\cdot)$ は非線形写像である。これをアナログ回路で実現する場合、雑音等による揺らぎを考慮しなければならず、あるクラスのカオス写像では、定常的にカオスを生成することができない。しかしながら、写像の定義域が値域よりも広い写像を用いると、カオス系列の値が値域からある程度飛び出しても、定義域を外れることなく定常的にカオス系列を生成することが可能である。

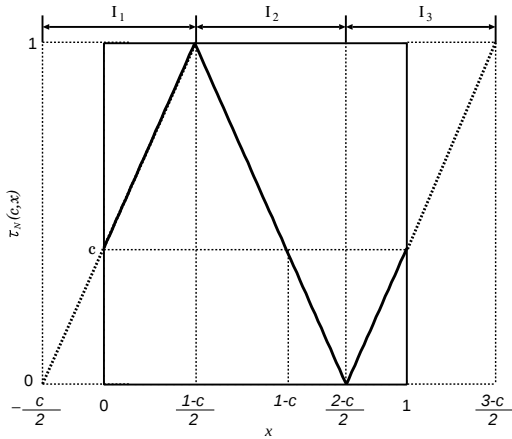


図 1: 区分線形 N 型写像

本稿では、そのような写像として、次式で定義される区分線形 N 型写像 τ_N を用いる。(図 1 参照)

$$\tau_N(c, x) = \begin{cases} 2x + c & (x \in I_1) \\ -2x - c + 2 & (x \in I_2) \\ 2x + c - 2 & (x \in I_3) \end{cases} \quad (1)$$

ここで I_1, I_2 , および I_3 は、それぞれ次のような部分区間である。

$$I_1 = [-\frac{c}{2}, \frac{1-c}{2}), \quad I_2 = [\frac{1-c}{2}, \frac{2-c}{2}), \quad I_3 = [\frac{2-c}{2}, \frac{3-c}{2}]$$

また、 c は写像 τ_N のパラメータで、 $0 < c < 1$ を満たす。この写像は一様不変密度をもち、また、適切な 2 値関数を用いると、理想乱数である平衡 *i.i.d.* 2 値系列が生成できることが証明されている [1]。

3 回路設計

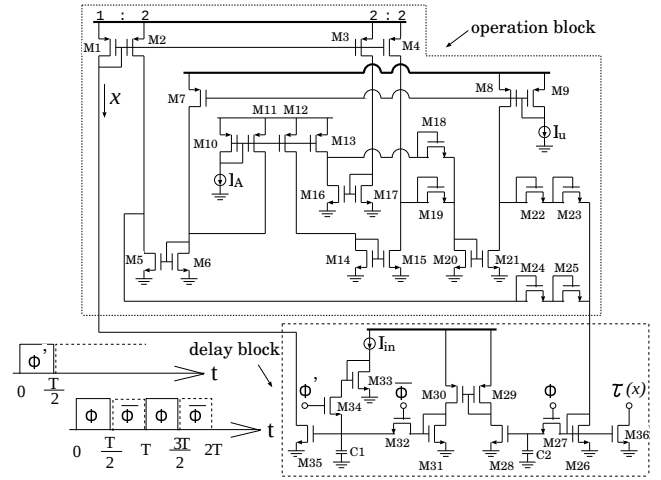


図 2: 区分線形 N 型写像に基づいた離散時間型アナログ CMOS カオス回路

区分線形 N 型写像 $\tau_N(\cdot)$ を回路で構成するために、式 (1) を次式のように書き直す。

$$\tau_N(c, x) = I_u \ominus (2x \ominus I_A + I_A \ominus 2x) + 2x \ominus (I_u + I_A) \quad (2)$$

ここで、 $\ominus$ は次式で定義される限界差演算子である。

$$x \ominus y = \begin{cases} x - y & (x > y) \\ 0 & (x \leq y) \end{cases} \quad (3)$$

図 2 に示すように、区分線形 N 型写像に基づいた離散時間型アナログ CMOS カオス回路を設計した。この回路は、演算部と遅延部で構成されている。演算部は式 (2) に基づいており、 $\ominus$ は *n*MOS ダイオード接続を用いて構成している。また、図 2 に示された比はカレントコピーの比を示している。遅延部には離散時間システムに適したスイッチトカレント (SI) 技術を用いて構成している。ただし、 I_{in} は初期値に相当する。このようにして、演算部の出力 $\tau(x)$ は、1 周期 (T) ごとに遅延部で遅延され、入力 x にフィードバックされる。この行程を繰り返して区分線形 N 型写像に基づいた 1 次元差分方程式を実現している。

4 シミュレーション

表 1: 提案回路の各 MOSFET のパラメータ値

素子番号 $M_i (i = 1 \sim 36)$	$L(\mu\text{m})$	$W(\mu\text{m})$
$M_i (i = 1, 5 \sim 26, 28 \sim 31, 33, 35, 36)$	13.32	28.12
$M_i (i = 2 \sim 4)$	13.32	56.24
$M_i (i = 27, 32, 34)$	2.22	4.81

図 2 の提案回路について、回路シミュレータ HSPICE を用いて回路シミュレーションを行った。提案回路は、オンセミコンダクタ社の $1.2\mu\text{m}$ CMOS プロセスをターゲットとして設計を行っており、電源電圧は 5.0V とした。ただし、 $I_u = 10.0\mu\text{A}$, $I_A = 5.0\mu\text{A}$, $I_{in} = 1.5\mu\text{A}$, $C1=C2=1\text{pF}$ として、 $T = 1\text{ms}$ 刻みで写像を 10 万回繰り返した。また、提案回路における MOS トランジスタのチャネル長 L , チャネル幅 W の値を表 1 に示す。

まず、図 2 の提案回路で実現される区分線形 N 型写像が、理論上の写像をどれほど精度よく実現できるかどうかを調べるために、HSPICE による回路シミュレーションで生成された長さ 5,000 のカオス実数値系列のリターンマップを図 3 に示す。図 3 より、ほぼ理論通りの区分線形 N 型写像を実現していることがわかる。

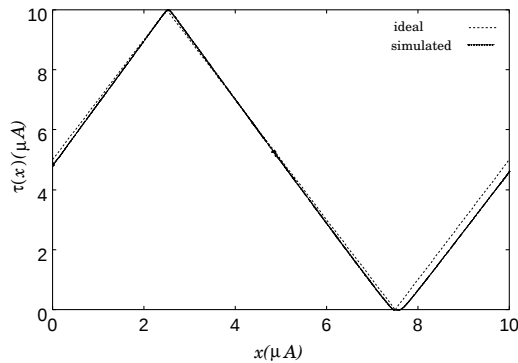


図 3: 提案回路のリターンマップ

次に、写像の区間 $[0\mu\text{A}, 10\mu\text{A}]$ を 20 等分に区切り、HSPICE による回路シミュレーションで生成された長さ 10 万のカオス実数値系列の値の出現頻度分布を調べた。その結果を図 4 に示す。図 4 より、多少揺らぎは生じているが、理論通り、ほぼ一様性を満たしていることがわかる。

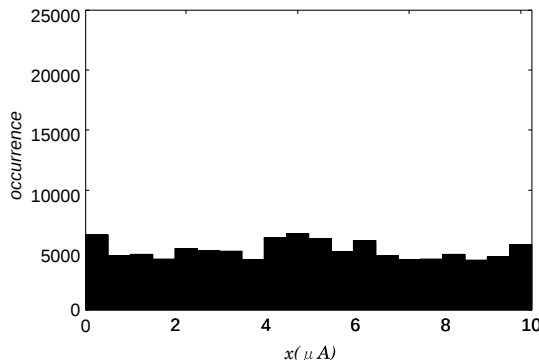


図 4: 提案回路によるカオス実数値系列の頻度分布

5 実験結果

提案回路を VDEC によりオンセミコンダクタ社の $1.2\mu\text{m}$ CMOS プロセスでチップ化した。提案回路において N 型写像を実現する演算部の動作を確認するために、演算部の入出力特性を測定した。その結果、図 5 に示すように理論値と比較すると、多少のずれがみられる。

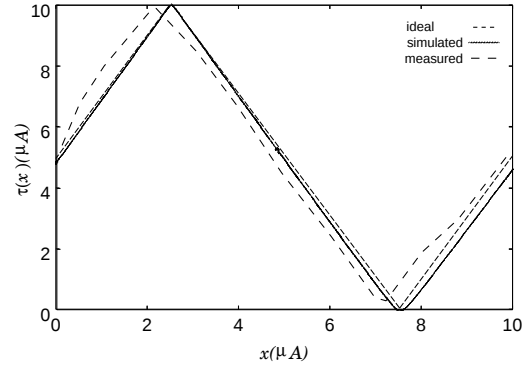


図 5: 一次元写像の測定結果

6 まとめ

アナログ回路での実現が容易な区分線形 N 型写像を用い、その写像をアナログ CMOS 回路で実現した。シミュレーションを行った結果、提案回路が一般的な非周期乱数を生成できる見通しを得た。

また、提案回路を VDEC によりチップ化し、演算部の動作確認のための実験を行った。実験結果は N 型写像を実現する提案回路の演算部の動作が理想の写像と多少の違いがあることを示しており、写像を実現する回路の精度向上、及び高速化が求められる。

参考文献

- [1] A. Tsuneda, K. Eguchi, and T. Inoue, "Design of Chaotic Binary Sequences with Good Statistical Properties Based on Piecewise Linear Into Maps," *Proc. of the 7th International Conference on Microelectronics for Neural, Fuzzy, and Bio-Inspired Systems*, pp.261-266, 1999.
- [2] K. Hamazato, A. Tsuneda, M. Hano, T. Inoue, K. Eguchi "An Analog CMOS Circuit Generating Chaotic Sequences Based on Piecewise Linear N-Shaped Maps," *Proc. of ITC-CSCC 2001*, pp.604-607, 2001.

お問い合わせ先

熊本大学工学部電気システム工学科 常田明夫

Tel:096-342-3853

E-mail:tsuneda@eecs.kumamoto-u.ac.jp