

学籍番号 氏名	V21068 倉地 真輝	指導教員	藤枝 直輝
題目	PC-FPGA 間の通信を使用した FPGA の動作可視化システムの構築		

1 はじめに

FPGA (Field Programmable Gate Array) とは、設計者がフィールド (現場) で論理回路の構成をプログラムできるゲート (論理回路) を集積したデバイスのことである。システムを実際に動作させるときは、その動作を利用者によりわかりやすい形で可視化することが求められる。八代 [1] は、FPGA 内部の真性乱数生成器 (TRNG) [2] の動作を対象とした FPGA 単体での可視化システムを提案した。このシステムでは、生成した乱数を使ってランダムな座標に繰り返し点を打つ様子と、点描の結果からモンテカルロ法を用いて求めた円周率の推定値を、1 つの映像として出力する。

本研究では、PC-FPGA 間通信を利用して、FPGA の回路動作を PC 上で可視化するシステムを構築することを目的とする。これにより PC-FPGA 間でのインタラクティブな可視化を可能にすることを目指す。

2 研究背景

TRNG [2] とは、物理的現象を元に規則性のないビット列を出力する回路である。本研究では、遷移効果リングオシレータ (TERO) を使った TRNG [2] を扱う。SR ラッチを禁止状態から一気に保持状態へと切り替えると、回路はしばらくの間発振する。その発振の回数が偶数か奇数かを数えて、乱数を取り出すのが TERO の動作原理である。TERO を改良した TC-TERO [3] では、この回路の調整をパラメータで行える。

八代のシステム [1] は、(1) 乱数の生成・評価システムと (2) グラフィックパターン生成システムをベースに設計されている。(1) は TC-TERO [3] を用いて乱数を生成し、ファイルに保存するシステムである。(2) はグラフィックパターン生成回路から出力された信号を、HDMI 信号に変換し、出力するシステムである。

3 提案システムとその評価

今回提案するシステムも、先行研究と同様にプロセッサ側で制御プログラムを動作させ、FPGA 上の回路を起動させる。システムは、(1) 乱数の生成システム、(2) 乱数の評価システム、(3) グラフィックパターン生成システムで設計されている。このうち (1) のみを FPGA 側で行い、(2) と (3) は PC 側で行う。(1) は、乱数を生成・保存する点は先行研究と同じである。ただし、乱数はグラフィックパターン生成システムには直接送られず、ファイル転送で PC に送られる。(2) は、PC 上で読み込んだ乱数ファイルを使って点描を繰り返したときに、モンテカルロ法によって推計された円周率を算出するシステムである。本研究では、先行研究と異なり、推計された円周率に対して二項検定を行った際の p 値も計算する。(3) は、PC 上で読み込んだ乱数ファイルを用いた点描の様子を表示するシステムである。

システムの動作を確認するため、異なるパラメータで乱数を生成し、出力結果を比較した。乱数に偏りがある場合、不自然な縞模様が描画されたり、算出された円周率が π からほど遠い値になったり、p 値が 0 や 1 を示したりすることが確認された。

データサイズと描画時間との関係性を評価するため、異なるデータサイズで描画時間を測定する実験を行った。データサイズは 16 KB, 32 KB, 48 KB, 64 KB の 4 通りとした。その結果、データサイズと描画時間との間にはおおむね比例関係が成り立ち、64 KB での描画時間の平均は 262 ms であった。64 KB の乱数生成に要した時間は 1794 ms であったので、リアルタイム可視化を目指す際にもこのシステムを流用できそうである。

4 おわりに

本研究では、FPGA の動作可視化システムの構築及び改良を PC, FPGA の両方を用いて行った。今後の課題としては、乱数データの転送方法をプログラムによる自動化を視野に入れて考えることが挙げられる。

参考文献

- [1] 八代航輔, FPGA を用いた TRNG の可視化システムの構築, 卒業論文, 愛知工業大学, 2024
- [2] O. Petura, U. Mureddu, N. Bochard, V. Fischer, L. Bossuet, A Survey of AIS-20/31 Compliant TRNG Cores Suitable for FPGA Devices, in FPL 2016, pp 1–10, 2016
- [3] N. Fujieda, On the feasibility of TERO-based true random number generator on Xilinx FPGAs, in FPL 2020, pp. 103–108, 2020