令和２（２０２０）年度　卒業研究報告書概要

課程，学籍番号，氏名	課程：電気・電子情報工学課程，学籍番号：B193285，氏名：AIMAN HAFIZ
工学分野名：情報通信システム	指導教員名：市川周一

題　　目：和　オンライン乱数検定回路の高位合成に関する予備調査

（英　Preliminary research on high-level synthesis of online random number test circuit)

Abstract

This study presents the implementations of 3 tests from the Diehard Test, which are Count of 1's (stream) Test, Count of 1's (specific) Test and Run Test for Xilinx FPGA.

The evaluation environment includes 3 types of FPGA boards (Spartan-7 board, Kintex-7 board and Virtex-7 board), VHDL as Hardware Description Language, and Vivado (2020.1) System Edition as behavioral simulation, logic synthesis and implementation. VHDL source code is created using High Level Synthesis in Vivado HLS (2020.1). The C-language code for each test is simulated and high level synthesized in Vivado HLS to create the VHDL source code .

The evaluation results indicate that Kintex-7 board and Virtex-7 board can be used for implementation. Spartan-7 cannot be used for implementation because of resource shortage. Kintex-7 board can be used but the resource of utilization is near to 100%. Virtex-7 board is the most suitable because the resource utilization remains around 60%. If the IO and DSP cell is not included, the resource utilization remains around 20%.

概要

真性乱数生成器(TRNG)は物理現象等に基づいて乱数を生成するため、出力が予測不可能である。乱数品質は動作環境に影響されるので、乱数品質を保証するために乱数検定が必要である。

Suresh ら(2013) は NIST テストの内 6 種の検定(Frequency (Monobit) Test, Test for Frequency Within A Block, Runs Test, Test for The Longest Runs of Ones in A Block, Non Overlapping Template Matching Test, Binary Matrix Rank Test)をハードウェアとして実装した。Yang ら(2015)はソフトウェアとハードウェアを用いて、全ての NIST テストでオンライン乱数検定回路を実装した。Leonard ら(2020)は NIST テストの 2 種の検定と他のテストでバイアス修正のための再構成可能 TRNG を開発した。奥田(2019)は、NIST テストの 4 種の検定(Frequency (Monobit) Test, Test for Frequency Within A Block, Runs Test, Test for The Longest Runs of Ones in A Block)を小型のハードウェアで実装した。

本研究の目的は Diehard テストを Vivado HLS で高位合成し、Xilinx 社の FPGA ボードに実装し、乱数品質を検定することである。本研究では、奥田(2019)が扱った NIST テストに対応する Diehard テストの内、３種の検定、Count of 1's (stream)、Count of 1's (specific)、Runs Test、を選択した。各テストの C 言語プログラムを Vivado HLS(2020.1)でシミュレーションし、高位合成して、VHDL 記述を生成した。VHDL 記述は Xilinx Vivado で処理して、合成と実装を行った。実装には、Spartan-7、Kintex-7、Virtex-7 の３つの FPGA ボードを使用した。

実装の結果、Kintex-7 と Virtex-7 のボードに実装可能であることが分かった。Spartan-7 ではリソース不足により、実装不可能である。Kintex-7 のボードには実装可能であるが、リソース使用率がほぼ 100%に達しており、実用的とは言えない。Virtex-7 のボードではリソースの使用率は約 60%にとどまった。IO と DSP のセル以外では、Virtex-7 のボードのリソースの使用率は約 20%である。

発表する際の課程を記入　　電気・電子情報工学　課程　　発表番号　44

（学籍が他課程所属の学生も発表する課程を記入すること）