Galois Field Arithmetic Unit

Sabbir Ahmed, Jeffrey Osazuwa, Howard To, Brian Weber

February 21, 2018

Abstract

The Galois Field Arithmetic Unit (GFAU) generated all the elements in the Galois field of a binary-coded decimal primitive polynomial. The arithmetic logic unit (ALU) computed the degree of the inputted polynomial and the order of its finite field and allowed addition, subtraction, multiplication, division and logarithm between the elements. GFAU utilized a Spartan 6 FPGA for the computations, a pair of 512Kb asynchronous integrated circuit SRAM memory chips for storage, and an Arduino microcontroller for user interface. Galois fields, consisting of a finite number of elements, are represented by $GF(q)$, where q must be a power of a prime. The binary field is the most frequently used Galois field. The GFAU handled primitive polynomials in $GF(2^n)$, where $2 \leq n \leq 15$. Galois fields have various applications in error detection and correction (EDAC). Specifically, cyclic redundancy checks (CRC) is an EDAC that employ $GF(2)$. EDAC has many expensive calculations that are difficult for low powered and inexpensive microcontrollers to handle. The GFAU project made Galois field computations more accessible to such low powered devices.