Galois Field Arithmetic Unit

Sabbir Ahmed, Jeffrey Osazuwa, Howard To, Brian Weber

February 5, 2018

Abstract

The Galois Field Arithmetic Unit (GFAU) project was an arithmetic logic unit (ALU) that generated all the terms in the Galois field of an input primitive polynomial and allowed addition, subtraction, multiplication, division and logarithm operations between them. Galois Fields, consisting of a finite number of elements, are represented by $GF(q)$, where q must be a power of a prime. There exists exactly one finite field for each prime power. The binary field is the most frequently used Galois Field. The GFAU will handle 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 power and inexpensive microcontrollers to handle. The GFAU project made Galois Field computations more accessible to such low powered devices.