MEMO NUMBER: GFAU SRS
DATE: November 22, 2017
TO: EFC LaBerge
FROM: Sabbir Ahmed, Jeffrey Osazuwa, Howard To, Brian Weber
SUBJECT: System Requirement Specifications

1 Introduction

A Galois Field is a field with a finite number of elements. The nomenclature $GF(q)$ is used to indicate a Galois Field with q elements. In $GF(q)$, the parameter q must be a power of a prime. For each prime power there exists exactly one finite field. The binary field $GF(2)$ is the most frequently used Galois field (1).

The Galois Field Arithmetic Unit will handle irreducible polynomials in $GF(2^n)$, where $2 \leq n \leq 16$. The arithmetic logic unit (ALU) will generate all the terms in the field of the polynomial, and allow the user to view and apply the following Galois operations: addition, subtraction, multiplication, division and logarithm.

1.1 Document Overview

This document serves as the System Requirements Specification for the Galois Field Arithmetic Unit. The description and requirements of the project are embodied in this document.

The Specification is divided into separate segments pertaining to individual components and requirements on different levels. Figures and tables are attached where necessary to assist in demonstrating concepts.

1.2 Mission Scenario

Galois Fields have various applications in error detection and correction (EDAC). Specifically, cyclic redundancy checks (CRC) is an EDAC that employ $GF(2)$ (2). EDAC has many expensive calculations that are difficult for low power and inexpensive microcontrollers to handle. The GFAU will make Galois Field computations more accessible to such low powered devices.

2 System Overview

The GFAU prototype will be composed of discrete modules residing in a single programmable board. Individual modules will be programmed to solely complete an assigned task. Although modules are assigned individual tasks, they should not have exclusive components for its functionality.

2.1 System Boundary Diagram

Figure 1 provides the System Boundary Diagram of the GFAU.

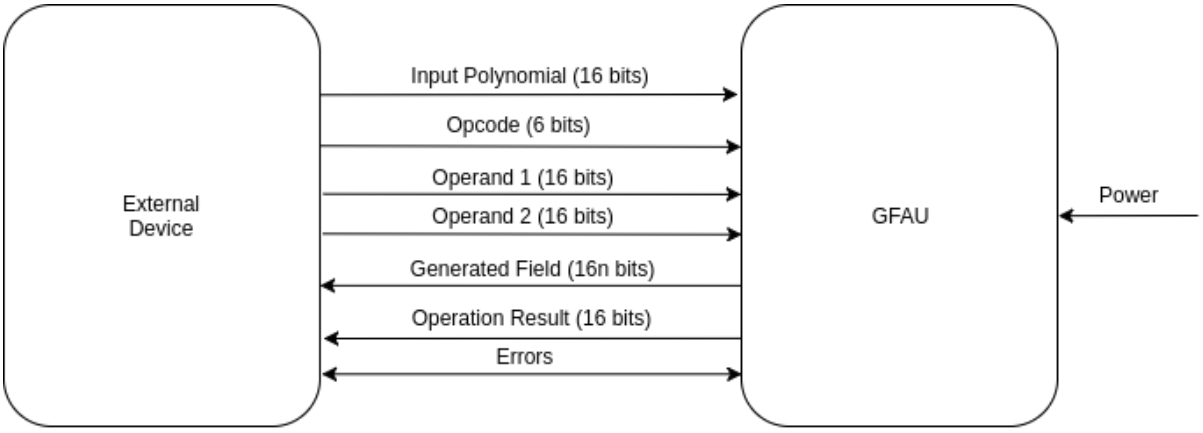

Figure 1: System Boundary Diagram of the Galois Field Arithmetic Unit , where n is the Number of Terms

The user I/O interface are handled by the external device which are transferred via busses. The user inputs consist of the mode bit, the input generating polynomial and the binary operation(s) along with their corresponding operands. The external device transfers the data to the unit to perform the desired operations. The GFAU will return the outputs and any errors detected back to the external device.

2.2 Functional Flow Diagram

Figure 2 provides the functional flow of the GFAU.

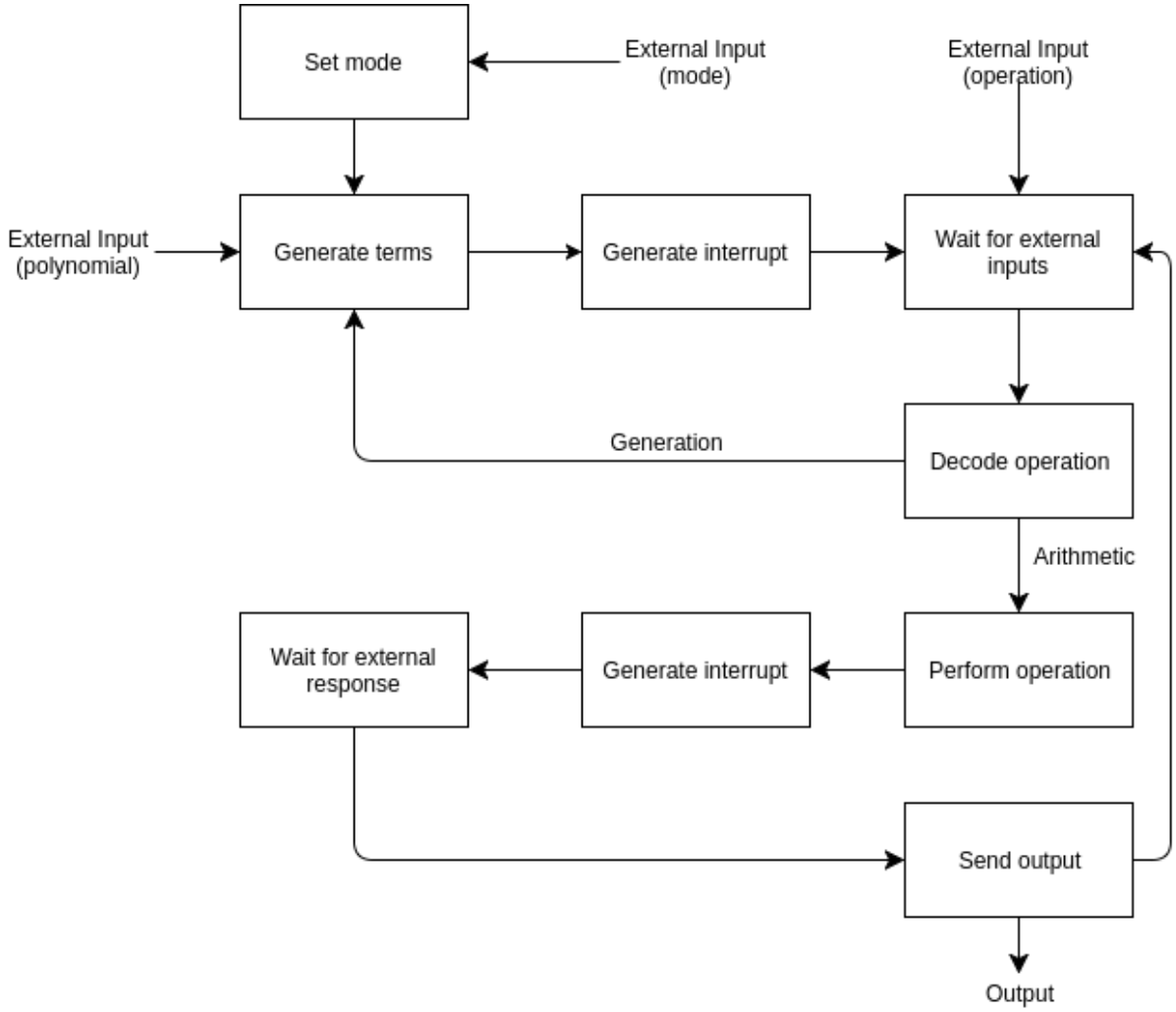

Figure 2: Functional Flow Diagram of the Galois Field Arithmetic Unit

The diagram provides a high-level overview of the sequence of processes that take place in the unit. In total, the unit waits for an input from the user in three separate instances. The order of the inputs are essential for the unit to proceed as desired. The **mode** input sets the width of the data bus in the GFAU. The **polynomial** input consist of the generating polynomial to generate its terms in the Galois field. The **operation** input consists of the two operands along with the desired binary operation.

2.3 Data Flow Diagram

Figure 3 provides the data flow diagram of the GFAU.

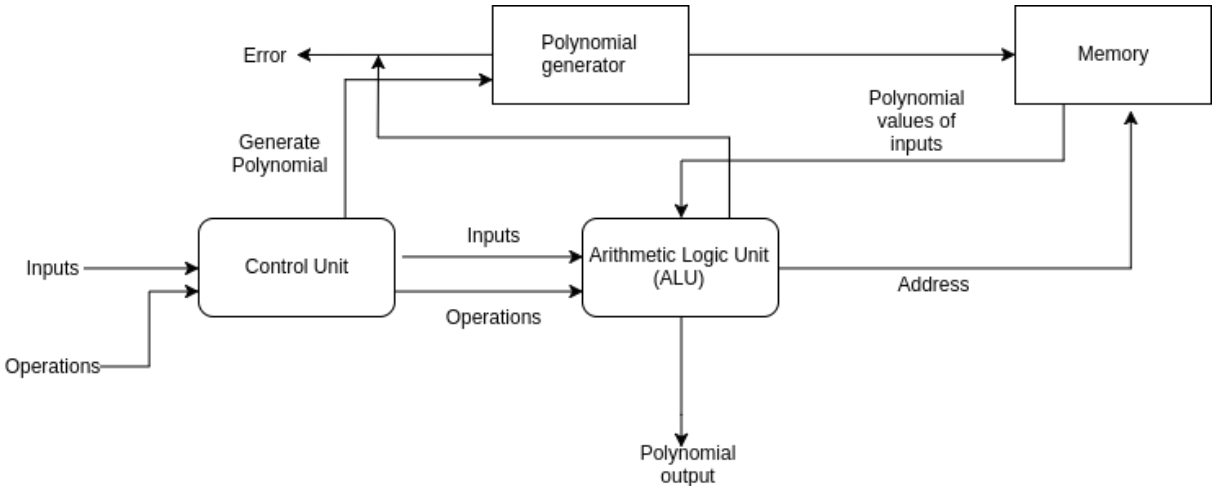

Figure 3: Data Flow Diagram of the Galois Field Arithmetic Unit

The diagram provides a lower-level view of the system emphasizing the individual components and their role in converting the input data to the desired output. The **Error** lines are used by multiple components to send interrupt signals to the user when required.

3 Requirements

3.1 Functional Requirements

The GFAU shall perform the functions outlined below.

3.1.1. The GFAU shall generate terms from input irreducible polynomials of degrees 2 to 8.

3.1.2. The GFAU shall handle operations on terms from $GF(2)$ to $GF(8)$.

3.1.3. The GFAU should generate terms from input irreducible polynomials of degrees 2 to 16.

3.1.4. The GFAU should handle operations on terms from $GF(2)$ to $GF(16)$.

3.1.5. The GFAU shall perform addition, subtraction, multiplication, division, and logarithm operations in the Galois Field.

3.1.6. The GFAU shall handle inputs given in their element or polynomial from depending on the opcode provided from the external device.

3.1.7. The GFAU shall be able to generate outputs in their element or polynomial depending on the opcode from the external device.

3.2 Cost and Package Constraints

This section outlines all design constraints imposed by the customer, from which the remainder of the requirements are derived.

3.2.1. The total cost of the prototype shall not exceed $400.

3.2.2. The total area of prototype printed circuit board (PCB) shall not exceed 24 inches square.

3.2.3. The cost at mass production shall not exceed $1 per chip.

3.2.4. The package of the final product shall not exceed 64 pins and should use fewer than 64 pins.

3.3 Hardware Requirements

The GFAU shall prioritize hardware portability, as it provides flexibility in the ranges of its specifications. The hardware specifications shall include reasonably bounded ranges.

3.3.1. The GFAU shall be functional at a variety of clock speeds at a minimum range of (4 MHz - 100 MHz).

3.3.2. The GFAU shall not exceed a thermal design power (TDP) of (1) W in a final implementation.

3.3.3. The GFAU shall operate normally at a temperature range of -40°C to ~85°C.

3.3.4. The input voltage for the unit shall be (5) V.

3.4 Software and Testing Requirements

Software testing through extensive simulations in hardware description language (HDL) shall be incorporated into the requirements of the GFAU. Simulations allow for convenient debugging and minimizes the risks of unintended behavior in the prototype. Before purchasing hardware, the HDL code shall pass the following required tests.

3.4.1. All HDL code shall be synthesizable.

3.4.2. The simulations shall prove the HDL code functions, as intended, with (99%) certainty.

3.4.3. During verification, values (such as gate delays) shall be parametrized to readily match the specifications of candidate hardware.

3.5 Signal Testing and Requirements

To ensure that all communication occurs accurately between the external device and the GFAU, all output signals shall not exceed rise and fall times of (1 ns). All signals shall incorporate an oscilloscope to measure their timings. A digital logic analyzer shall be used to verify the output signals.

3.6 Communication Requirements

The GFAU shall be able to communicate with a wide variety of external devices with commonly used communication methods outlined below.

3.6.1. The GFAU shall provide the external device the option to select between a 8, 16, (or 32) bit data-bus.

3.6.2. The GFAU shall set a ready pin after the completion of the given operation.

3.6.3. The GFAU shall allow the external device to use polling or interrupts to monitor the ready pin to pull the data from the bus.

3.6.4. The GFAU shall push relatively small blocks of data over a bus to the external device using a common or easy-to-implement protocol on one clock.

3.6 (A) Error Codes

Error signals shall be sent to the external device in the following cases.

3.6.5. The GFAU shall produce an error if its input polynomial is reducible.

3.6.6. The GFAU shall produce an error if an operand exceeds the bounds Galois Field generated by the input polynomial.

3.6.7. The GFAU shall produce an error if an operand is attempted to be divided by 0 (zero).

3.6.8. The GFAU shall produce an error if it does not receive all the inputs from the external device.

References

(1) Wolfram Math World, "Finite Field." *Wolfram Math World*, 2017. (Online document). Availble: http://mathworld.wolfram.com/FiniteField.html. (Accessed: Nov. 21, 2017).

(2) N. Matloff , "Cyclic Redundancy Checking." *University of California at Davis*, 2001. (Online). Availble: http://heather.c s.ucdavis.edu/ matloff/Networks/CRC/Old/ErrChkCorr.html. (Accessed: Nov. 21, 2017).