MEMO NUMBER: GFAU SOW
DATE: December 1, 2017
TO: EFC LaBerge
FROM: Sabbir Ahmed, Jeffrey Osazuwa, Howard To, Brian Weber
SUBJECT: Galois Field Arithmetic Unit Statement of Work

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 Purpose and Scope

This Statement of Work outlines and elaborates the tasks necessary to implement the project. The document also details their corresponding milestones and deadlines and how the contribution will be divided within the team.

2 Roles and Division of Labor

This project requires equal team work on all tasks because of the steep learning curve on implementing coprocessors with programmable boards. None of the team members have comprehensive prior knowledge or training on field programmable gate array units, and are therefore required to learn the concepts

concurrently.

Although there is no clear division of labor within the team, each members have been implicitly designated unofficial roles. Table 1 provides an estimated division of labor among the members of Galois Field Arithmetic Unit.

Table 1: Estimated Division of Labor of Galois Field Arithmetic Unit

Member	Responsibilities
Sabbir	• Validate the system inputs and outputs through the operations in the unit • Provide background information on the mathematical concepts and theoretical design • Finalize written reports and deliverables
Jeffrey	• Design modules using the hardware description language • Support the designing processes by providing test benches and by synthesizing the individual modules
Howard	• Act as the point of contact between the team and the project manager and other consultants • Schedule team meetings and milestones
Brian	• Maintain and validate the digital design of the system at various levels • Oversee the designing of the system using the hardware description language • Finalize written reports and deliverables

Along with the assigned responsibilities, each members of the GFAU shall contribute to programming the individual modules in the system. Each members shall also contribute to authoring the documents supporting the project design and requirements.

3 Tasks

3.1 Research

The initial set of tasks relate to research efforts to fully understand the requirements and develop an implementation of the GFAU.

3.1.1 Background

The team shall conduct research on the mathematics and theoretical concepts related to Galois fields. The GFAU generates terms in specified Galois fields and stores them for further operations. Therefore, a strong understanding on such topics is essential for successful and accurate computations.

3.1.2 Devices

The team shall conduct research on the implementation and synthesis of digital design on programmable boards and their corresponding best practices.

3.1.2.1 Field Programmable Gate Array (FPGA)

The team shall conduct research to address the following inquiries regarding FPGA development boards and design.

3.1.2.1.1. The team shall conduct trade studies on designs commonly used for arithmetic operations which are performed in the GFAU.

3.1.2.1.2. The team shall identify styles and best practices for hardware synthesizable VHDL code.

3.1.2.1.3. The team shall identify hardware specifications deemed important before purchase.

3.1.2.1.4. The team shall identify hardware specifications to meet the requirements detailed in the System Requirements Specifications.

3.1.2.2 External Devices

The team shall conduct research to address the following inquiries regarding external devices interfacing the FPGA development board.

3.1.2.2.1. The team shall identify the external devices suitable for interfacing the GFAU.

3.1.2.2.2. The team shall conduct a study of protocols commonly used to communicate with coprocessors to determine how to communicate with the widest range of the most commonly used microprocessors.

3.1.2.2.3. The team shall identify hardware specifications of the external devices to meet the requirements detailed in the System Requirements Specifications.

3.2 Design

3.2.1 System Boundary

The team shall design a system boundary diagram detailing the functions, inputs and outputs of the system. The team shall also develop and maintain additional diagrams elaborating various hierarchical and functional views of the project, including the functional flow and data flow diagrams.

3.2.2 Schematics

The team shall develop schematics and other documentation necessary for the development phase. For the final product, the team shall develop a high-level schematic consisting of all the modules in the system. The schematic shall be divided into segments to be elaborated on a lower level by individual members.

3.2.3 System Design Document

The team shall compile a System Design Document detailing the architectural, logical and physical design of every level of the system.

3.3 Software Implementation

3.3.1 Design in VHSIC Hardware Description Language (VHDL)

The team shall implement independent and discrete VHDL modules for each of the operations in the GFAU. The source code shall be written and comprehensively documented using the best practices and standards imposed by the *IEEE Standard VHDL Language Reference Manual* (2009).

3.3.2 Simulation and Synthesis in VHDL

The team shall test each module after completion to minimize syntax and implementation warnings and errors. Individual test benches shall be written to accompany their corresponding module for every module in the system. The team shall complete the modules using using syntax that is synthesizable for use in the chosen FPGA. Each module shall be independently synthesized to ensure they match the intended schematics and designs. The team should complete all simulations and software testing by the end of December.

3.3.3 External Devices

The system may require external devices, such as memory. The team shall abstract and simulate their behavior in VHDL before the physical integration to validate their functionality. The VHDL code written to describe the behavior of external devices does not necessarily have to be synthesizable.

3.3.3.1 External Device Library

The team may provide a library for the external device to interface the GFAU system. The library may include methods, protocols and constants to establish communication with and send and receive signals to the GFAU prototype.

3.4 Purchases

Before purchase, the team shall conduct research on external memory chips suitable for storing the lookup tables created during the polynomial term generation. Research on the external memory interface includes simulation and testing of its truth tables using VHDL. The team shall concurrently conduct research to find a development board which satisfies the requirements outlined in the System Requirements Document.

3.5 Hardware

3.5.1 Integration

The team shall integrate the system with an FPGA board bounded by the constraints detailed in the Systems Requirement Specifications. The board shall successfully communicate with a microcontroller for user interface and its external

memories. The team shall complete the hardware integration phases by mid-spring after all final purchases.

3.5.2 Hardware Testing

The team shall continuously test the FPGA board and its external components before, during and after the integration with the VHDL system modules. The testing of the hardware in the system shall serve as the final milestone for the project during the end of the spring semester.

3.5.2.1. The team shall conduct logical tests of the prototype using a Digital Logic Analyzer to verify the logical correctness and timing constraints of the GFAU.

3.5.2.2. The team shall conduct testing of both input and output signals using an oscilloscope to verify all signals going in and out of the GFAU meet the requirements outlined in Section 3.5 of the System Requirements Specification.

4 Deliverables

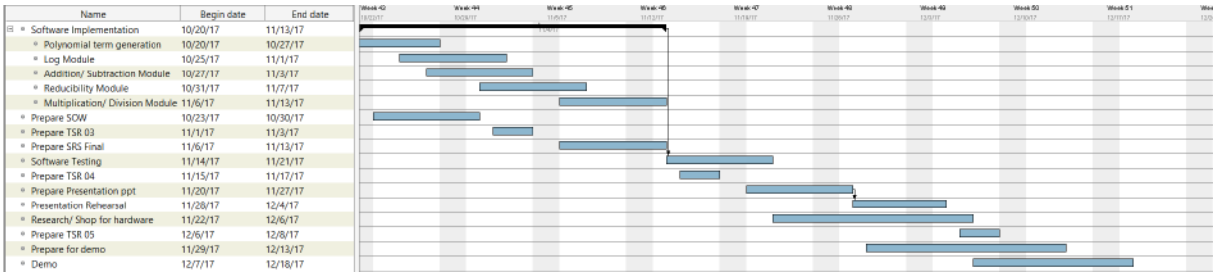
Table 2 details the expected deliverables throughout the project and shall be completed concurrently with the project development.

Table 2: Deliverables

Deliverable	Description	Deadline
System Specification Requirements	The team shall develop a detailed specification of the unit. The specification document shall include both hardware and software requirements and constraints. The System Specification Requirements also detailed all the inputs and outputs of the GFAU.	November 22nd, 2017
Weekly Team Status Reports	The team shall deliver bimonthly status reports to Dr. LaBerge discussing the completed tasks and issues encountered during the period. They shall also include planned tasks for the next period.	Bimonthly
Preliminary Design Review	The team shall present a Preliminary Design Review of the project to Dr. LaBerge in the first week of December.	December 6th, 2017
Completed Design Review	The team shall present a final review of the GFAU to Dr. LaBerge and others in May, 2018.	May, 2018
Demo	The team shall present a fully functional demo of the GFAU to Dr. LaBerge and others in May, 2018.	May, 2018

5 Timeline

Figure 1 below shows a timeline of the capstone project in a Gantt Chart.



Name	Begin date	End date
Software Implementation	10/20/17	11/13/17
Polynomial term generation	10/20/17	10/27/17
Log Module	10/25/17	11/1/17
Addition/ Subtraction Module	10/27/17	11/3/17
Reducibility Module	10/31/17	11/7/17
Multiplication/ Division Module	11/6/17	11/13/17
Prepare SOW	10/23/17	10/30/17
Prepare TSR 03	11/1/17	11/3/17
Prepare SRS Final	11/6/17	11/13/17
Software Testing	11/14/17	11/21/17
Prepare TSR 04	11/15/17	11/17/17
Prepare Presentation ppt	11/20/17	11/27/17
Presentation Rehearsal	11/28/17	12/4/17
Research/ Shop for hardware	11/22/17	12/6/17
Prepare TSR 05	12/6/17	12/8/17
Prepare for demo	11/29/17	12/13/17
Demo	12/7/17	12/18/17

Figure 1: Capstone Schedule

References

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

(2) Design Automation Standards Committee of IEEE Computer Society, *IEEE Standard VHDL Language Reference Manual*, IEEE Computer Society, 2009.