Galois Field Arithmetic Unit (GFAU)

Sabbir Ahmed, Jeffrey Osazuwa, Howard To, Brian Weber, Dr. E.F. Charles LaBerge
Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County

What are Galois Fields?

A field with a finite number of elements, Galois fields are a key part of number theory, abstract algebra, arithmetic algebraic geometry, and cryptography. In error detection and correction, Galois fields are utilized in cyclic redundancy check (CRC) which are used in digital networks and storage devices to detect accidental changes to raw data.

Table 1: Elements of $x^3 + x^2 + x^0$

Element	Symbol	Decimal	Polynomial	Symbol	Decimal
0	NULL	NULL	0 + 0 + 0	000	0
x^0	000	0	0 + 0 + x^0	001	1
x^1	001	1	0 + x^1 + 0	010	2
x^2	010	2	x^2 + 0 + 0	100	4
x^3	011	3	x^2 + 0 + x^0	101	5
x^4	100	4	x^2 + x^1 + x^0	111	7
x^5	101	5	0 + x^1 + x^0	011	3
x^6	110	6	x^2 + x^1 + 0	110	6

Figure 1: Operations of elements of $x^3 + x^2 + x^0$

$$x^5 + x^2 = x^4 \qquad x^5 \times x^2 = x^0 \qquad x^5 - x^2 = x^4$$
$$x^5 \div x^2 = x^3 \qquad x^2 \div x^5 = x^4 \qquad \log(x^5) = 5$$

Objective

To design a scalable arithmetic logic unit (ALU) capable of generating elements in the Galois field of an irreducible polynomial and perform addition, subtraction, multiplication, division and logarithm for low powered devices.

Design Approach

- Scalable, parameterized and efficient design prioritized over specific platform hardware requirements
- Designed entirely in VHSIC Hardware Description Language (VHDL) modules and packages
- Capability of design limited only by external memory capacity
- Interface **<BRIAN>**

Prototype Design Specification

- Budget under $400.
- Cost of large scale production less than $1 per chip
- Area of less than 24 in^2

Design Overview

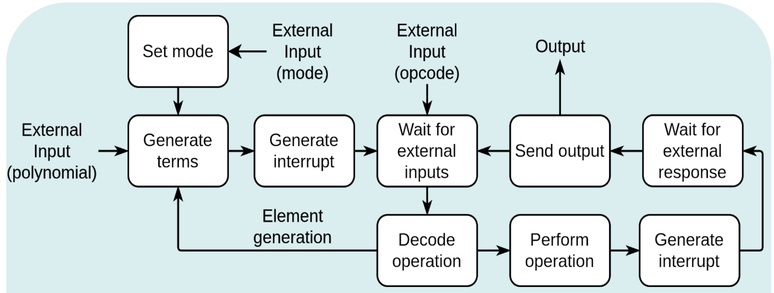


Figure 3: Functional Flow Diagram

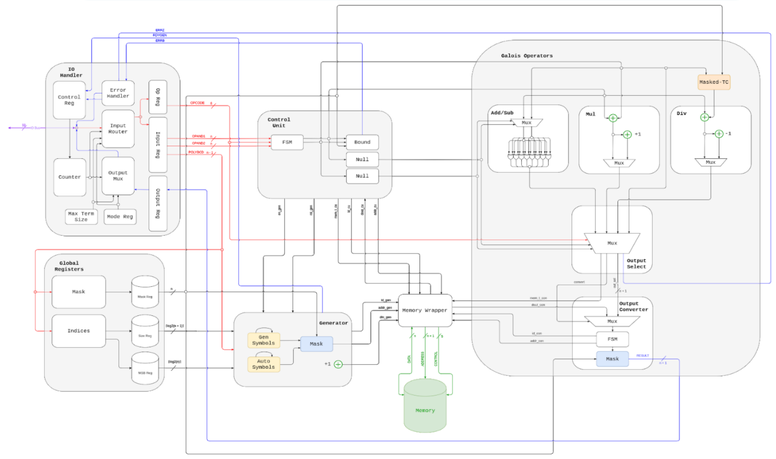
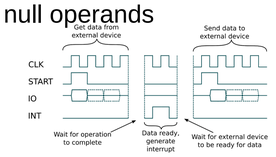


Figure 4: High Level Block Schematic

Modules

- **Global Registers**
  - Generated by priority encoders
  - Size index, most significant bit index, and mask
- **Generator**
  - Generates elements in their element and polynomial forms
  - Alerts the user when process is complete
- **Operators**
  - Performs addition, subtraction, multiplication, division and logarithm of Galois operands
  - Checks null errors
- **Control unit**
  - Determines operations requested through 6-bit opcode
  - Converts operands into their counterpart forms if necessary
  - Checks operand memberships and null operands
- **IO Handler**
  - Afsdfs
  - Asffds
  - f
- **Memory wrapper**
  - Handle memory read and write requests from the generator, operators and control unit



Results

Conclusion