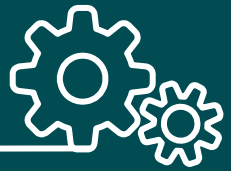
GALOIS FIELD ARITHMETIC UNIT



Sabbir Ahmed, Jeffrey Osazuwa, Howard To, Brian Weber

CMPE 450: Preliminary Design Review

OVERVIEW

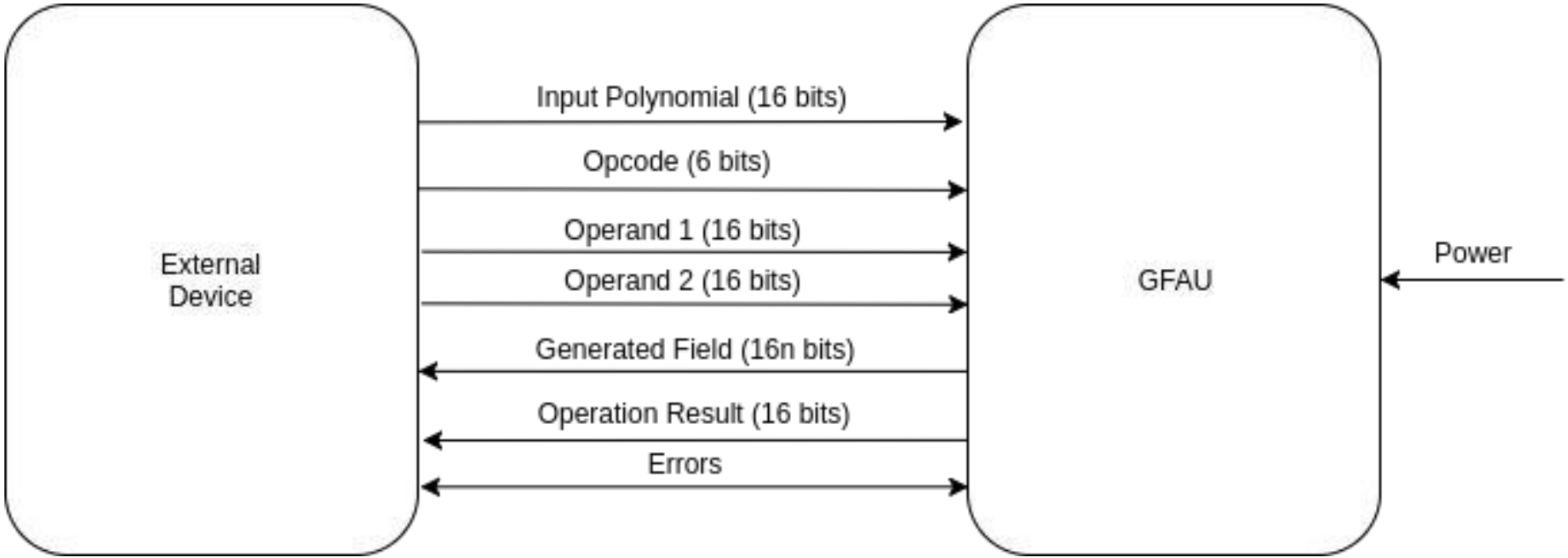
Review

SRR	PDR	CDR
Introduction to concepts	Hardware Configuration items	Complete design
Functional Flow	Software Configuration items	
Data Flow	Interface Requirements	
Trade Studies		
Testing Methods		

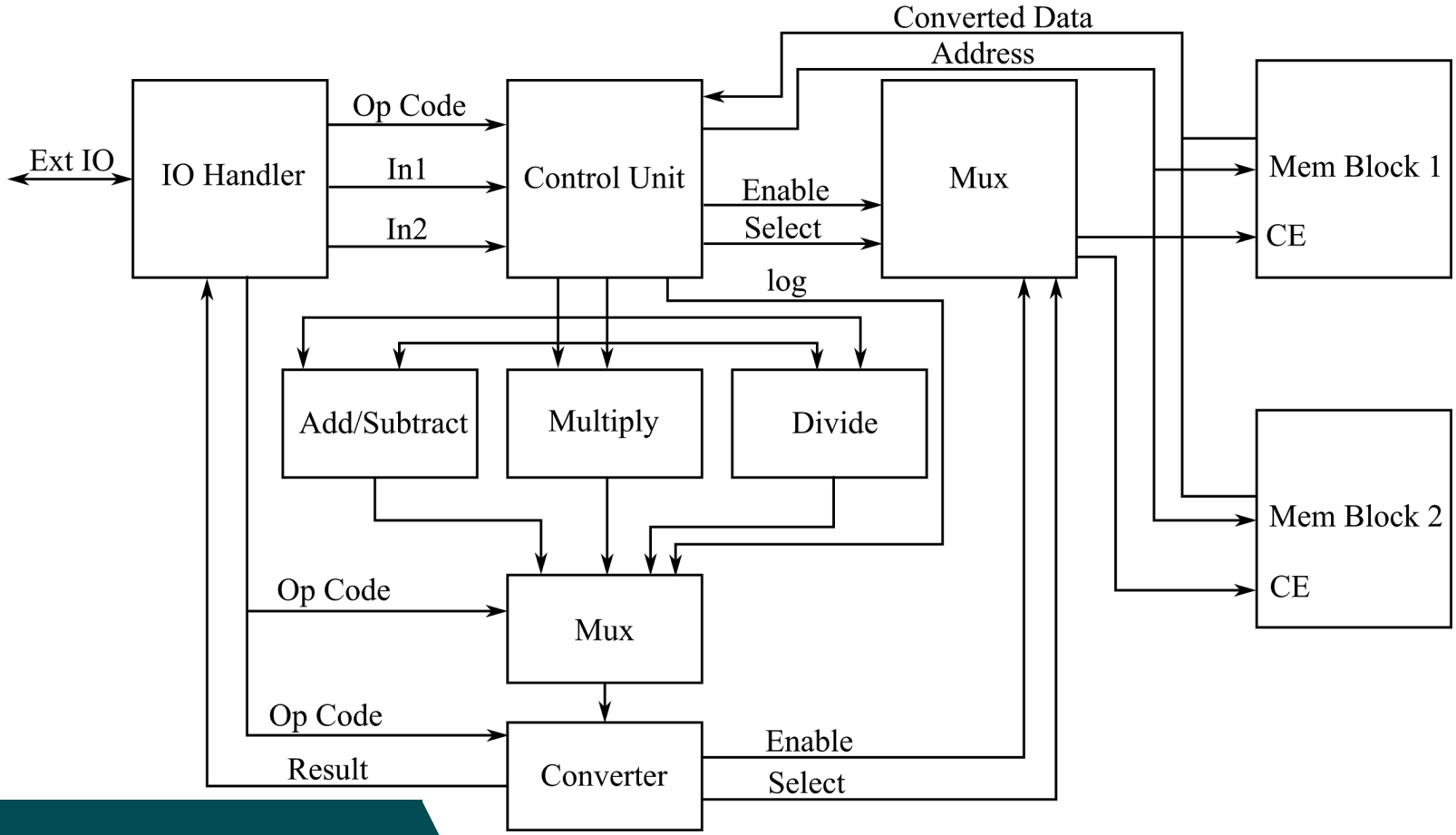
Modifications since SRR

- **ASIC Design**
  - Time inefficiency with exclusive use of port maps
  - Behavioral VHDL design not permitted
- **16th Degree Polynomial**
  - 16-bit data signals cover 0 - 15 degrees
  - Inconvenient alternatives
    - 16-bits with special handling for zeroth degree?
    - 17-bit data signals?
    - 32-bit data signals (left padded with 15 zeros)?
- **System Boundary Diagram**
  - Updated input and output sizes

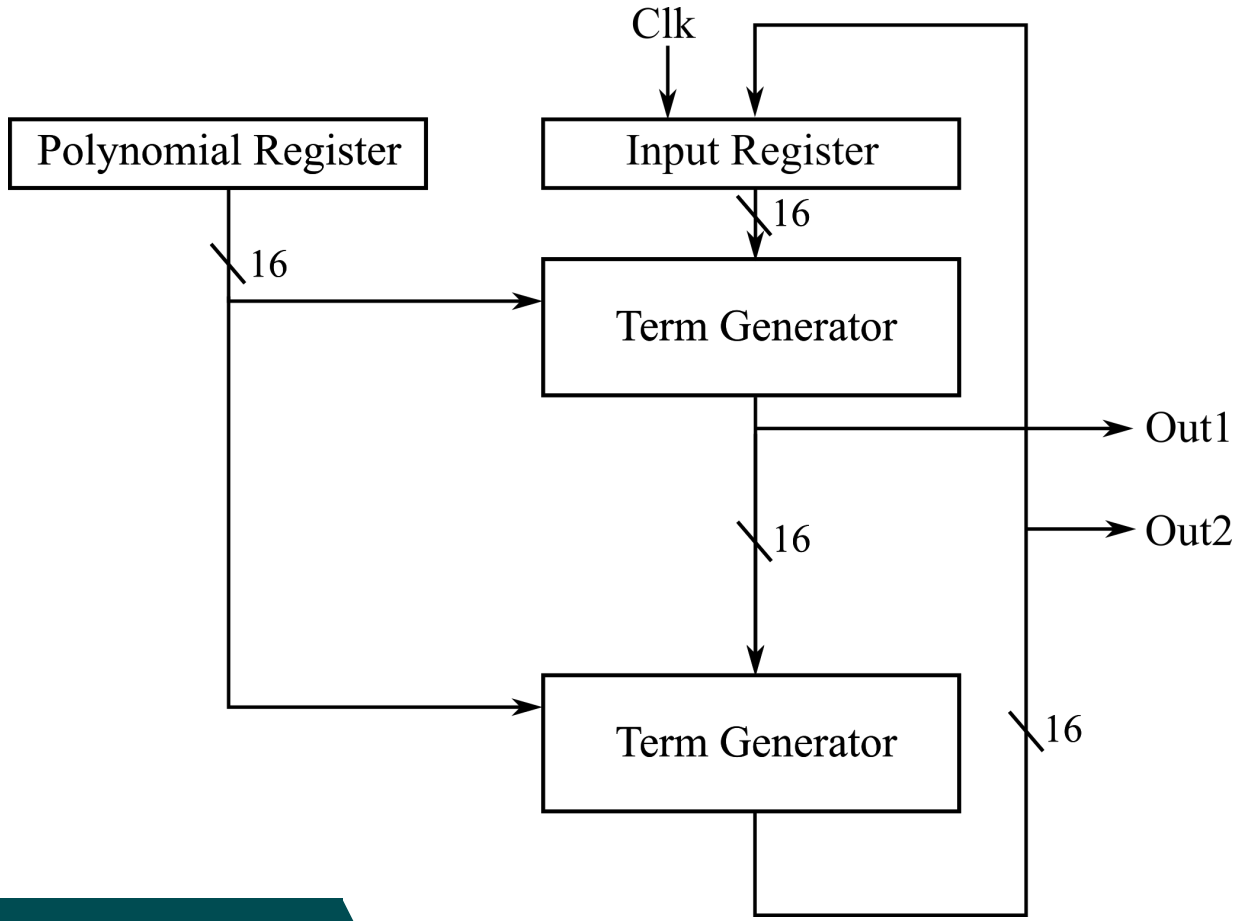
System Boundary Diagram



HARDWARE CONFIGURATION ITEMS

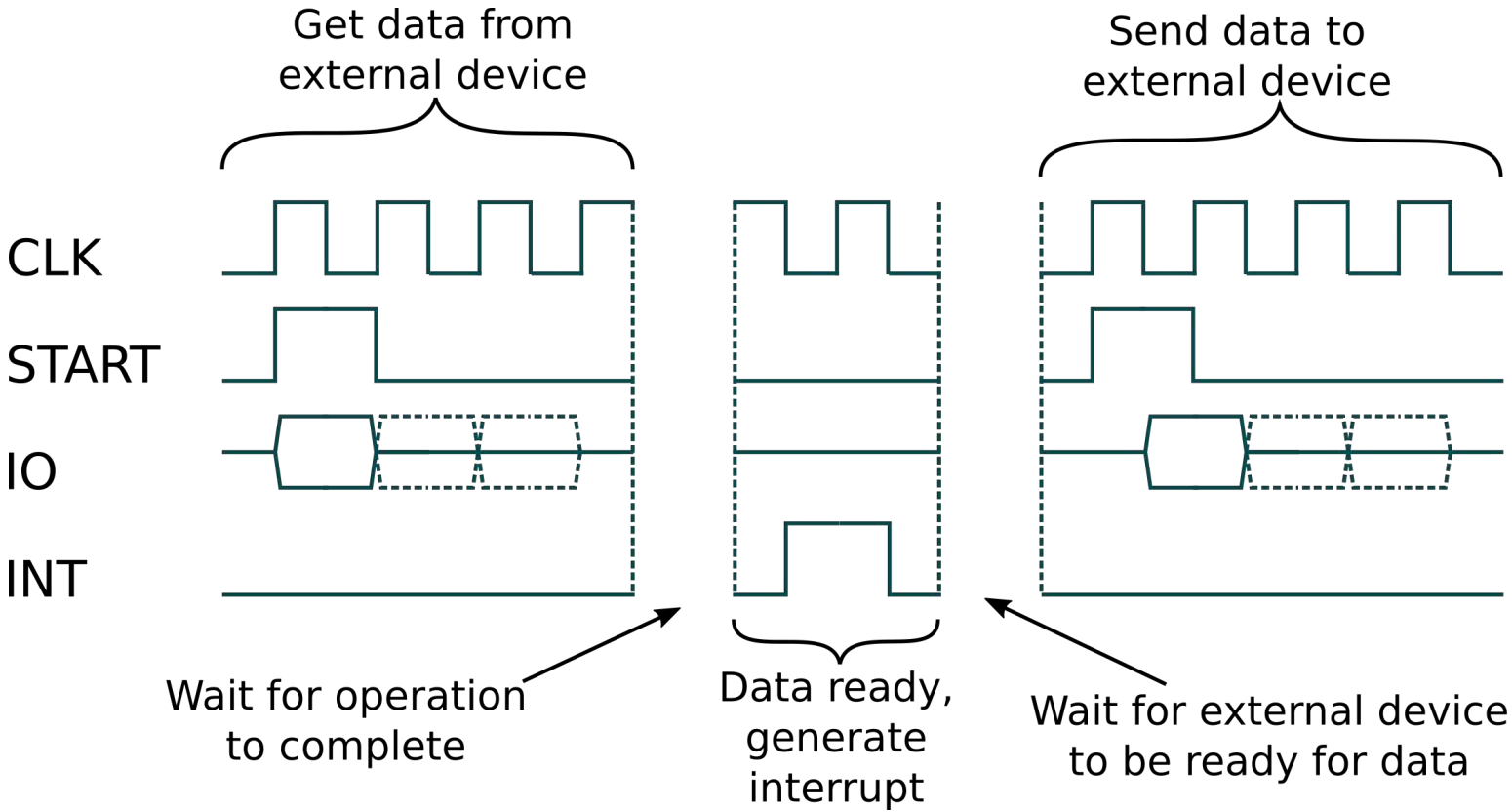


High Level System View



Polynomial Generation

Timing Diagram

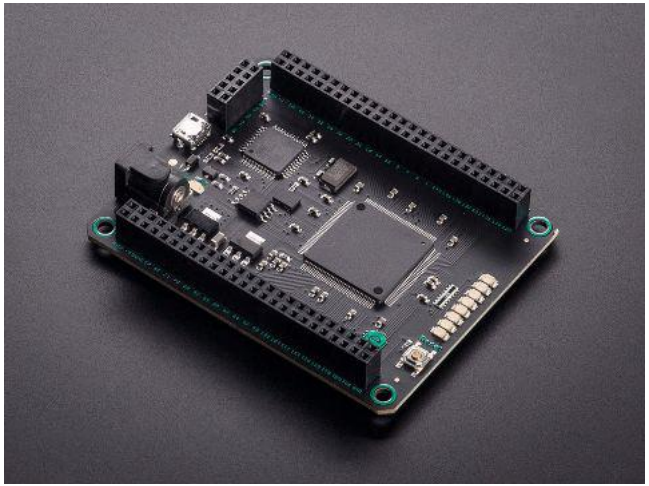


Interface Requirements

- External device must have at least an 8 bit bus to communicate with the GFAU
- Bus defaults to 8 bits on startup
- External device may set the mode to increase the bus size to up 16 or 32 bits

Preliminary Design Overview

Mojo FPGA Development Board



Source: adafruit

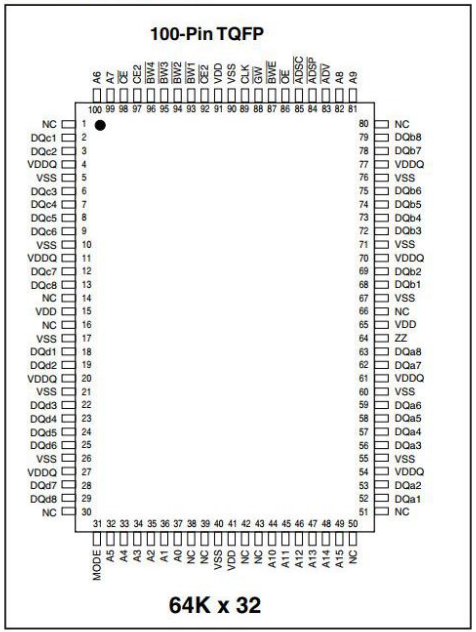
Development Board Specifications

- **Spartan 6 XC6SLX9 FPGA**
- **84 digital IO pins**
- **8 analog inputs**
- **On board voltage regulation that can handle 4.8V - 12V**
- **A ATmega32U4 microcontroller**
  - Used for configuring the FPGA, USB communications, and reading the analog pins
- **On board flash memory**
  - Stores the FPGA configuration file

Preliminary Design Synthesis

64K x 32 Synchronous Pipelined Static RAM

PIN CONFIGURATION



Source: Integrated Silicon Solution Inc.

External Memory Specifications

- 4 ns write and access times
- 133 MHz max clock speed
- 64KB of memory in 32 bit words
- Burst read and write functionality

SOFTWARE CONFIGURATION ITEMS

$$x^3 + x^2 + x^0$$

Element	Symbol	Polynomial	Symbol
0	1111 1111 1111 1111	0 + 0 + 0	0000 0000 0000 0000
x^0	0000 0000 0000 0000	0 + 0 + x^0	0000 0000 0000 0001
x^1	0000 0000 0000 0001	0 + x^1 + 0	0000 0000 0000 0010
x^2	0000 0000 0000 0010	x^2 + 0 + 0	0000 0000 0000 0100
x^3	0000 0000 0000 0011	x^2 + 0 + x^0	0000 0000 0000 0101
x^4	0000 0000 0000 0100	x^2 + x^1 + x^0	0000 0000 0000 0111
x^5	0000 0000 0000 0101	0 + x^1 + x^0	0000 0000 0000 0011
x^6	0000 0000 0000 0110	x^2 + x^1 + 0	0000 0000 0000 0110

Statistic	Expression
Total number of terms	2^n
Maximum degree of terms	2^n - 2
Number of bits of terms	n
Offset bit	n + 1

Galois Fields: Terms

$$x^3 + x^2 + x^0$$

Operation	Operand types
Addition	Polynomial
Subtraction	Polynomial
Multiplication	Element
Division	Element
Logarithm	Element

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

Galois Fields: Operations

Storage Allocation

- Terms are stored in their element and polynomial forms
- Separate, parallel memory
- Convenient memory lookup

VHDL Modules: Terms and Operations

- **Term generation and validation modules**
  - Irreducible Polynomial Validator
  - Polynomial Term Generator
- **Galois operation modules**
  - Galois Adder / Subtractor
  - Galois Multiplier
  - Galois Divider
  - Galois Logarithm Calculator

VHDL Modules: Arithmetic Logic Units

- 16-bit Carry-Lookahead Adders (CLAs)
- 16-bit Masked Two's Complement

$$-3 \xrightarrow{\text{2's complement}} 1111\ 1111\ 1111\ 1101$$

$$-3 \xrightarrow{\text{masked 2's complement}} 0000\ 0000\ 0000\ 0101$$

- Polynomial Degree Calculator

$$x^3 + x^2 + x^0 \xrightarrow{\text{polynomial degree}} 0000\ 0000\ 0000\ 0011$$

- Overflow Bit Calculator

$$x^3 + x^2 + x^0 \xrightarrow{\text{offset bit}} 0000\ 0000\ 0000\ 0100$$

VHDL Modules: Arithmetic Logic Units

- **Arithmetic Exceptions**
  - Zero Handler
  - Out-of-bounds Handler

VHDL Modules: Control Units

Operation Codes (Opcodes)

$$\underbrace{OP_1 OP_2 OP_3}_{\text{Instruction}} \underbrace{IO_1 IO_2 IO_3}_{\text{I/O Type}}$$

OP	Instruction	I/O	Description
000	Generate Terms	xxx	N/A
001	Addition/Subtraction	0/1,0/1,0/1	0 = element, 1 = polynomial
010	Multiplication	0/1,0/1,0/1	0 = element, 1 = polynomial
011	Division	0/1,0/1,0/1	0 = element, 1 = polynomial
100	Logarithm	0/1,x,0/1	0 = element, 1 = polynomial
101	Reset	xxx	N/A
110	Set Mode	0/1,0/1,x	00 = 16, 01 = 32, 10 = 64
111	No Operation	xxx	N/A

VHDL Modules

- **Multiplexers**
  - Memory Lookup
  - Output Selector
- **Discrete logic gates**

Schedule

- Slightly behind schedule as planned
- Finish VHDL coding and testing over winter break
- Hardware Research
- Purchase hardware in January

QUESTIONS?