Lecture A3:

Finite Fields of the Form GF(2^n)

4^{th} Year Course- CCSIT, UoA

Lecture goals

- To review finite fields of the form *GF* (2^n)

- To show how arithmetic operations can be carried out by directly operating on the bit patterns for the elements of *GF* (2^n)

Consider Again the Polynomials Over *GF* (2)

- Here are some examples:

$$x + 1$$
$$x^2 + x + 1$$
$$x^2 + 1$$
$$x^3 + 1$$

$$x$$
$$1$$
$$x^5$$
$$x^{10000}$$

- We could also shown polynomials with negative coefficients, but recall that in *GF* (2), –1 is the same as +1.
- Obviously, the number of such polynomials is infinite.
- The polynomials can be subject to the algebraic operations of addition and multiplication in which the coefficients are added and multiplied according to the rules that apply to *GF* (2).
- As stated in the previous lecture, the set of such polynomials forms a ring, called the polynomial ring.

Modular Polynomial Arithmetic (1)

- Let's now add one more twist to the algebraic operations we carry out on all the polynomials over *GF* (2):
- We will first choose a particular irreducible polynomial, as for example $x^3 + x + 1$

(By the way there exist only two irreducible polynomials of degree 3 over *GF* (2). The other is $x^3 + x^2 + 1$.)

- We will now consider all polynomials defined over *GF* (2) modulo the irreducible polynomial $x^3 + x + 1$.
- In particular, when an algebraic operation (*we are obviously talking about polynomial multiplication*) results in a polynomial whose degree equals or exceeds that of the irreducible polynomial, we will take for our result the remainder modulo the irreducible polynomial.

Modular Polynomial Arithmetic (2)

- For example,

$$(x^2 + x + 1) \times (x^2 + 1) \ mod \ (x^3 + x + 1)$$

$$\begin{aligned}
&= (x^4 + x^3 + x^2) + (x^2 + x + 1) \ mod \ (x^3 + x + 1) \\
&= (x^4 + x^3 + x + 1) \ mod \ (x^3 + x + 1) \\
&= -x^2 - x \\
&= x^2 + x
\end{aligned}$$

- Recall that $1 + 1 = 0$ in *GF* (2). This is what we used in getting to the second expression on the right hand side.
- For the division by the modulus in the above example, we used the result

$$\frac{(x^4 + x^3 + x + 1)}{(x^3 + x + 1)} = x + 1 + \frac{-x^2 - x}{x^3 + x + 1}$$

- Obviously, for the division on the left hand side, our first quotient term is x. Multiplying the divisor by x yields $x^4 + x^2 + x$ that when subtracted from the dividend gives us $x^3 - x^2 + 1$. This dictates that the next term of the quotient be 1, and so on.

How Large is the Set of Polynomials When Multiplications are Carried Out Modulo $x^3 + x + 1$

- With multiplications modulo $x^3 + x + 1$, we have only the following eight polynomials in the set of polynomials over *GF* (2):

$$\begin{array}{l} 0 \\ 1 \\ x \\ x + 1 \end{array} \qquad \begin{array}{l} x^2 \\ x^2 + 1 \\ x^2 + x \\ x^2 + x + 1 \end{array}$$

- We will refer to this set as *GF* (2^3) where the power of 2 is the degree of the modulus polynomial.
- Our conceptualization of *GF* (2^3) is analogous to our conceptualization of the set Z_8. The eight elements of Z_8 are to be thought of as integers modulo 8. So, basically, Z_8 maps all integers to the eight in the set Z_8. Similarly, *GF* (2^3) maps all of the polynomials over *GF* (2) to the eight polynomials shown above.
- But note the crucial difference between *GF* (2^3) and Z_8: *GF* (2^3) is a field, whereas Z_8 is NOT.

How Do We Know That *GF* (2^3) is a Finite Field? (1)

- We do know that *GF* (2^3) is an abelian group because of the operation of polynomial addition satisfies all of the requirements on a group operator and because polynomial addition is commutative.
- *GF* (2^3) is also a commutative ring because polynomial multiplication distributes over polynomial addition (and because polynomial multiplication meets all the other stipulations on the ring operator: closedness, associativity, commutativity).
- *GF* (2^3) is an integral domain because of the fact that the set contains the multiplicative identity element 1 and because if for $a \in GF(2^3)$ and $b \in GF(2^3)$ we have

$$a \times b = 0 \; mod \; (x^3 + x + 1)$$

then either $a = 0$ or $b = 0$.

How Do We Know That $GF(2^3)$ is a Finite Field? (2)

- $GF(2^3)$ is a finite field because it is a finite set and because it contains a unique multiplicative inverse for every non-zero element.
- $GF(2^3)$ contains a unique multiplicative inverse for every non- zero element for the same reason that Z_7 contains a unique multiplicative inverse for every non-zero integer in the set. (For a counterexample, recall that Z_8 does not possess multiplicative inverses for 2, 4, and 6.)
- In other words, for every non-zero element $a \in GF(2^3)$ there is always a unique element $b \in GF(2^3)$ such that $a \times b = 1$.
- This follows from the fact if you multiply a non-zero element a with each of the eight elements of $GF(2^3)$, the result will the eight distinct elements of $GF(2^3)$.

How Do We Know That *GF* (2^3) is a Finite Field? (3)

- Obviously, the results of such multiplications must equal 1 for exactly one of the non- zero element of *GF* (2^3). So if $a \times b = 1$, then b must be the multiplicative inverse for a.
- The same thing happens in Z_7. If you multiply a non-zero element a of this set with each of the seven elements of Z_7, you will get seven distinct answers. The answer must therefore equal 1 for at least one such multiplication. When the answer is 1, you have your multiplicative inverse for a.
- For a counterexample, this is not what happens in Z_8. When you multiply 2 with every element of Z_8, you do not get eight distinct answers. (Multiplying 2 with every element of Z_8 yields {0, 2, 4, 6, 0, 2, 4, 6} that has only four distinct elements).
- The upshot is that *GF* (2^3) is a finite field.

GF (2^n) is a Finite Field for Every *n*

- None of the arguments on the previous three pages is limited by the value 3 for the power of 2. That means that *GF* (2^n) is a finite field for every n.
- To find all the polynomials in *GF* (2^n), we obviously need an irreducible polynomial of degree n.
- AES arithmetic is based on *GF* (2^8). It uses the following irreducible polynomial

$$x^8 + x^4 + x^3 + x + 1$$

- The finite field *GF* (2^8) used by AES obviously contains 256 distinct polynomials over *GF* (2).
- In general, *GF* (p^n) is a finite field for any prime p. The elements of *GF* (p^n) are polynomials over *GF* (p) (which is the same as the set of residues Z_p).

Representing the Individual Polynomials in $GF(2^n)$ by Binary Code Words (1)

- Recall the eight polynomials in $GF(2^3)$ when the modulus polynomial is $x^3 + x + 1$ (See the next page).
- We now claim that there is nothing sacred about the variable x in such polynomials.
- We can think of x^i as being merely a place-holder for a bit.
- That is, we can think of the polynomials as bit strings corresponding to the coefficients that can only be 0 or 1, each power of x representing a specific position in a bit string.
- So the 2^3 polynomials of $GF(2^3)$ can therefore be represented by the bit strings shown in the next page.

Representing the Individual Polynomials in $GF(2^n)$ by Binary Code Words (2)

$$\begin{array}{rcl} 0 & \Rightarrow & 000 \\ 1 & \Rightarrow & 001 \\ x & \Rightarrow & 010 \\ x + 1 & \Rightarrow & 011 \\ x^2 & \Rightarrow & 100 \\ x^2 + 1 & \Rightarrow & 101 \\ x^2 + x & \Rightarrow & 110 \\ x^2 + x + 1 & \Rightarrow & 111 \end{array}$$

- If we wish, we can give a decimal representation to each of the above bit patterns. The decimal values between 0 and 7, both limits inclusive, would have to obey the addition and multiplication rules corresponding to the underlying finite field.
- Exactly the same approach can be used to come up with 2^n bit patterns, each pattern consisting of n bits, for a set of integers that would constitute a finite field, provided we have available to us an irreducible polynomial of degree n.