

## Lecture 7: Finite Fields (PART 4)

### PART 4: Finite Fields of the Form $GF(2^n)$

### Theoretical Underpinnings of Modern Cryptography

### Lecture Notes on “Computer and Network Security”

by Avi Kak (kak@purdue.edu)

January 28, 2017

4:08pm

©2017 Avinash Kak, Purdue University



#### 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  $GF(2^n)$
- **Perl and Python implementations for arithmetic in a Galois Field using my BitVector modules**

# CONTENTS

	<i>Section Title</i>	<i>Page</i>
7.1	Consider Again the Polynomials over $GF(2)$	3
7.2	Modular Polynomial Arithmetic	5
7.3	How Large is the Set of Polynomials When Multiplications are Carried Out Modulo $x^2 + x + 1$	8
7.4	How Do We Know that $GF(2^3)$ is a Finite Field?	10
7.5	$GF(2^n)$ a Finite Field for Every $n$	14
7.6	Representing the Individual Polynomials in $GF(2^n)$ by Binary Code Words	15
7.7	Some Observations on Bit-Pattern Additions in $GF(2^n)$	18
7.8	Some Observations on Arithmetic Multiplication in $GF(2^n)$	20
7.9	Direct Bitwise Operations for Multiplication in $GF(2^8)$	22
7.10	Summary of How a Multiplication is Carried Out in $GF(2^8)$	25
7.11	Finding Multiplicative Inverses in $GF(2^n)$ <b>with Implementations in Perl and Python</b>	27
7.12	Using a Generator to Represent the Elements of $GF(2^n)$	35
7.13	Homework Problems	39

## 7.1: CONSIDER AGAIN THE POLYNOMIALS OVER $GF(2)$

- Recall from Lecture 6 that  $GF(2)$  is a finite field consisting of the set  $\{0, 1\}$ , with modulo 2 addition as the group operator and modulo 2 multiplication as the ring operator. In Section 6.7 of Lecture 6, we also talked about polynomials over  $GF(2)$ . Along the lines of the examples shown there, here are some more:

$$x + 1$$

$$x^2 + x + 1$$

$$x^2 + 1$$

$$x^3 + 1$$

$$x$$

$$1$$

$$x^5$$

$$x^{10000}$$

...

...

The examples shown only use 0 and 1 for the coefficients in the polynomials. Obviously, we could also have shown polynomials with negative coefficients. However, as you'd recall from Lecture 6,  $-1$  is the same as  $+1$  in  $GF(2)$ . [\[Does  \$23 \* x^5 + 1\$  belong to the set of polynomials](#)

defined over  $GF(2)$ ? How about  $-3 * x^7 + 1$ ? The answer to both questions is yes. Can you justify the answer?]

- 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**.

## 7.2: MODULAR POLYNOMIAL ARITHMETIC

Let's now add one more twist to the algebraic operations we carry out on all the polynomials over  $GF(2)$ :

- In Section 6.11 of Lecture 6, I defined an **irreducible polynomial** as a polynomial that cannot be factorized into lower-degree polynomials. From the set of **all** polynomials that can be defined over  $GF(2)$ , let's now consider the following *irreducible polynomial*:

$$x^3 + x + 1$$

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

- For the set of **all** polynomials over  $GF(2)$ , let's now consider polynomial arithmetic **modulo** the irreducible polynomial  $x^3 + x + 1$ .
- To explain what I mean by polynomial arithmetic modulo the irreducible polynomial, when an algebraic operation — *we are*

[Click here to download full PDF material](#)