MATH 314 Spring 2019 - Class Notes

02/18/2019

Scribe: Trung Nguyen

Summary: Today we covered fields, polynomials, operations within fields and irreducible polynomials.

Notes:

Goal:

- Find F_{2^n}
- Finite Fields with 2^n elements
- Note: This field is not $Z_{2^n} \pmod{2^n}$

Replace Z by $F_2[x]$

- R[x] polynomials with coefficients in R
- $F_2[x]$ polynomials with coefficients in F_2
- F_2={0,1}

Example:

$g(x) = x^4 + x + 1 \in F[x]$
$f(x = x^5 + x \in F_2[x])$

$f(x) + g(x) = (x^5 + x) + (x^4 + x + 1) = x^5 + x^4 + 1$ (+ and - are the same)

$f(x) \times g(x) = (x^5 + x) \times (x^4 + x + 1) = (x^9 + x^6 + x^5) + (x^5 + x^2 + x)$
$=x^9 + x^6 + x^2 + x$

Division with remainder:
remainder has degree, smaller than the quotient

$$\begin{array}{r|l} & x \\ \hline x^4+x+1 & x^5 \qquad + x \\ & -x^5 - x^2 - x \\ \hline & -x^2 \end{array}$$

$x^5 + x \equiv x^2 \pmod{x^4 + x + 1}$ (+ and - are the same)

In order to get a field we need a modulus that doesn't have a divisor
-We call this polynomial irreducicble

<u>Example:</u> $x^2 + x + 1$
Find Polynomials that are smaller t: x, $x + 1$, 1, 0 (no need to check for 1 and 0)
check

$$
\begin{array}{r|l}
 & \quad x+1 \\
\hline
x) & x^2 + x + 1 \\
 & \underline{-\,x^2} \\
 & \qquad x \\
 & \quad \underline{-\,x} \\
 & \qquad\quad 1
\end{array}
$$

$$
\begin{array}{r|l}
 & \qquad\quad x \\
\hline
x+1) & x^2 + x + 1 \\
 & \underline{-\,x^2 - x} \\
 & \qquad\qquad 1
\end{array}
$$

So the polynomial (mod $x^2 + x + 1$) forms a field, this is F_4.

+	0	1	x	x+1
0	0	1	x	x+1
1	1	0	x+1	x
x	x	x+1	0	1
x+1	x+1	x	1	0

*	0	1	x	x+1
0	0	0	0	0
1	0	1	x	x+1
x	0	x	$x + 1$	1
x+1	0	x+1	1	x

To make F_{2^n}, we pick F(x) to an irreducible polynomial in F[x] of degree n
Then do arimethic mod F(x) to get $F_2[x]$

<u>Fact:</u> There exist irreducible polynomials of every degree