MAT 3343, APPLIED ALGEBRA, FALL 2003

Handout 5: The representation of GF(16)

Peter Selinger

Let α be a root of the primitive polynomial $x^4 + x + 1 \in \mathbb{Z}_2[x]$. The non-zero elements of $\mathrm{GF}(16) = \mathbb{Z}_2(\alpha) = \mathbb{Z}_2[x]/(x^4 + x + 1)$ can be represented by the powers of α as follows:

Element	a^0	a^1	a^2	a^3
$0 = 0$	0	0	0	0
$\alpha^0 = 1$	1	0	0	0
$\alpha^1 = \alpha$	0	1	0	0
$\alpha^2 = \alpha^2$	0	0	1	0
$\alpha^3 = \alpha^3$	0	0	0	1
$\alpha^4 = 1 + \alpha$	1	1	0	0
$\alpha^5 = \alpha + \alpha^2$	0	1	1	0
$\alpha^6 = \alpha^2 + \alpha^3$	0	0	1	1
$\alpha^7 = 1 + \alpha + \alpha^3$	1	1	0	1
$\alpha^8 = 1 + \alpha^2$	1	0	1	0
$\alpha^9 = \alpha + \alpha^3$	0	1	0	1
$\alpha^{10} = 1 + \alpha + \alpha^2$	1	1	1	0
$\alpha^{11} = \alpha + \alpha^2 + \alpha^3$	0	1	1	1
$\alpha^{12} = 1 + \alpha + \alpha^2 + \alpha^3$	1	1	1	1
$\alpha^{13} = 1 + \alpha^2 + \alpha^3$	1	0	1	1
$\alpha^{14} = 1 + \alpha^3$	1	0	0	1
$\alpha^{15} = 1$	1	0	0	0

Arithmetic in $\mathrm{GF}(16)$ can be easily performed using this representation. Addition is performed by representing elements as polynomials in α of degree less than 4. Multiplication is performed using the representation of nonzero elements as powers of α. For example,

$$\begin{aligned}
\frac{1+\alpha+\alpha^3}{1+\alpha^2+\alpha^3} + \alpha + \alpha^2 &= \frac{\alpha^7}{\alpha^{13}} + \alpha + \alpha^2 \\
&= a^{-6} + \alpha + \alpha^2 \quad \text{(since } \alpha^{15} = 1\text{)} \\
&= a^9 + \alpha + \alpha^2 \\
&= \alpha + \alpha^3 + \alpha + \alpha^2 \\
&= \alpha^2 + \alpha^3.
\end{aligned}$$

[*Source: Gilbert, Modern Algebra with Applications*]