

Solutions of a quartic GF(2) polynomial

Peter M. Maurer
Department of Computer Science
P.O. Box 97356
Baylor University
Waco, TX 76798-7356

$$x^4 + x^3 + x^2 + x + 1$$

$$a^4 + a^3 + a^2 + a + 1 = 0$$

$$a^4 = a^3 + a^2 + a + 1$$

$$a^5 = 1$$

$$a^6 = a$$

$$a^7 = a^2$$

$$a^8 = a^3$$

$$a^9 = a^3 + a^2 + a + 1$$

$$a^{10} = 1$$

$$a^{11} = a$$

$$a^{12} = a^2$$

$$a^{13} = a^3$$

$$a^{14} = a^3 + a^2 + a + 1$$

$$a^{15} = 1$$

$$a^{16} = a$$

$$(a^2)^4 + (a^2)^3 + (a^2)^2 + (a^2) + 1 =$$

$$a^8 + a^6 + a^4 + a^2 + 1 =$$

$$(a^3 + a^2 + a + 1)(a^3 + a^2 + a + 1) + a^2(a^3 + a^2 + a + 1) + (a^3 + a^2 + a + 1) + a^2 + 1 =$$

$$a^6 + a^5 + a + 1 =$$

$$a^5 + 1 =$$

$$a^4 + a^3 + a^2 + a + 1 = 0$$

$$a^{12} + a^9 + a^6 + a^3 + 1 = a^2 + a^2 + a^3 + a^3 + a + a + 1 + 1 = 0$$

$$(x + a)(x + a^2)(x + a^3)(x + z) = x^4 + x^3 + x^2 + x + 1$$

$$\begin{aligned}
(x+a)(x+a^2)(x+a^3)(x+z) &= \\
(x^2+ax+a^2x+a^3)(x+a^3)(x+z) &= \\
(x^3+ax^2+a^2x^2+a^3x^2+a^3x+a^4x+a^5x+a^6)(x+z) &= \\
x^4+(a^3+a^2+a+z)x^3+(a^3z+a^2z+az+a^2+a)x^2 & \\
+(z+a^4z+a^3z+a)x+za &= x^4+x^3+x^2+x+1
\end{aligned}$$

$$za = 1$$

$$z = a^4$$

$$z = a^3 + a^2 + a + 1$$

OK

Let a be an arbitrary solution to $x^4 + x^3 + x^2 + x + 1$. Then the other solutions to $x^4 + x^3 + x^2 + x + 1$ are a^2 , a^3 and $a^3 + a^2 + a + 1$. Note that the four solutions are mathematically indistinguishable.

Note that the relations given above are true for *all* solutions to $x^4 + x^3 + x^2 + x + 1$, so if s is a solution to $x^4 + x^3 + x^2 + x + 1$, then so is s^2 . $x^5 - 1 = (x - 1)(x^4 - x^3 - x^2 - x - 1)$ is the eigenpolynomial of the following matrix:

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \end{pmatrix}$$

This means that if e is an eigenvalue of A , then so is e^2 . Thus A can be similar to A^2 (and in fact *is* similar to A^2).