Hochschule Aschaffenburg
IW
Dr. Ing. Wilfried Dankmeier

Eppstein im Taunus, 20.04.2010

**Codierungsverfahren SS 2010**
**Hilfsblatt zur Berechnung der Elemente eines Galoisfeldes GF($2^4$)**
Zum BCH-Code (zyklischer Code zur Korrektur von t unabhängigen Ein-Bit-Fehlern)

**Beispiel:** Galoisfeld GF($2^4$) mit dem definierenden irreduziblen Poynom f(x) = $x^4 + x + 1$ , die Koeffizienten sind die natürlichen Zahlen MOD 2 aus dem endlichen Körper $Z_2$, nehmen also nur die beiden Werte 0 oder 1 an.

**Irreduzible Polynome** über $Z_2$ lassen sich nicht in Produkte aus Polynomen geringeren Grades über $Z_2$ zerlegen. Sie entsprechen in Polynomringen über $Z_2$ damit den gewöhnlichen Primzahlen.

**Definition der Nullstelle β** des Polynoms f(x) = $x^4 + x + 1$: Aus f(**β**) = $\beta^4 + \beta + 1 = 0$ ergibt sich $\beta^4 = (-\beta - 1) \text{ MOD } 2 = \beta + 1$ (im $Z_2$ gilt „+“ 0 „-“)

**Elemente** des daraus aufgebauten Galoisfeldes sind 0 und alle Potenzen von **β**. Das Galoisfeld hat die Eigenschaften eines **Körpers**, d. h., Addition, Subtraktion, Multiplikation und Division der Elemente (außer Division mit 0) ergibt immer wieder ein Element dieses Galoisfeldes.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| $0$ | = | $0$ | | | | | | |
| $\beta^0$ | = | $1$ | | | | | | |
| $\beta$ | = | $\beta^1$ | | | | | | |
| $\beta^2$ | = | $\beta^2$ | | | | | | |
| $\beta^3$ | = | $\beta^3$ | | | | | | |
| $\beta^4$ | = | $\beta + 1$ | | | | | | |
| $\beta^5$ | = | $\beta^4 \cdot \beta$ | = | | = | | = | |
| $\beta^6$ | = | $\beta^5 \cdot \beta$ | = | | = | | = | |
| $\beta^7$ | = | $\beta^6 \cdot \beta$ | = | | = | | = | |
| $\beta^8$ | = | $\beta^7 \cdot \beta$ | = | | = | | = | |
| $\beta^9$ | = | $\beta^8 \cdot \beta$ | = | | = | | = | |
| $\beta^{10}$ | = | $\beta^9 \cdot \beta$ | = | | = | | = | |
| $\beta^{11}$ | = | $\beta^{10} \cdot \beta$ | = | | = | | = | |
| $\beta^{12}$ | = | $\beta^{11} \cdot \beta$ | = | | = | | = | |
| $\beta^{13}$ | = | $\beta^{12} \cdot \beta$ | = | | = | | = | |
| $\beta^{14}$ | = | $\beta^{13} \cdot \beta$ | = | | = | | = | |
| $\beta^{15}$ | = | $\beta^{14} \cdot \beta$ | = | | = | | = | |
| $\beta^{16}$ | = | $\beta^{15} \cdot \beta$ | = | | = | | = | |
| $\beta^{17}$ | = | $\beta^{16} \cdot \beta$ | = | | = | | = | |

Copyright 2006