Datensicherheit, Übung 4

Henry Haustein

Aufgabe 1

Wenn ich mich nicht verguckt habe, dann hat Kode 1 ein $d_{min} = 2$ und Kode 2 ein $d_{min} = 1$. Damit kann nur Kode 1 Fehler erkennen. Korrektur ist keine möglich.

Aufgabe 2

(a) Es gilt $k = 3$, damit $n = 2^3 - 1 = 7$, $l = n - k = 4$ und $d_{min} = 3$

(b) Maximal 2 Bitfehler oder maximal 3 Bündelfehler

(c) Multiplikationsverfahren: $(x^3 + x + 1) \cdot (x^2 + x + 1) = x^5 + x^4 + 1 \mod 2 \Rightarrow 110001$
Divisionsverfahren: $(x^2 + x + 1) \cdot x^3 = x^5 + x^4 + x^3$, Ermittlung Rest:

$$\frac{x^5 + x^4 + x^3}{x^3 + x + 1} = x^2 + x + \frac{-2x^2 - x}{x^3 + x + 1}$$

Im $GF(2)$ ist der Rest dann $-x = x$. Damit würde kodiert werden $x^5 + x^4 + x^3 + x \Rightarrow 111010$.

(d) Es gilt:

$$\frac{x^6 + x^4 + x^2 + x + 1}{x^3 + x + 1} = x^3 - 1 + \frac{x^2 + 2x + 1}{x^3 + x + 1}$$

also wurde die Bitfolge nicht richtig übertragen.

$$\frac{x^6 + x^3 + x^2 + x}{x^3 + x + 1} = x^3 - x + \frac{2x^2 + 2x}{x^3 + x + 1}$$

allerdings ist in $GF(2)$ der Rest äquivalent zu 0, damit wurde die Bitfolge richtig übertragen.

(e) b_1 ist nicht richtig übertragen worden, damit ist keine Dekodierung möglich.
Falls b_2 mit dem Multiplikationsverfahren kodiert wurde, so ist die dekodierte Folge 1010. Divisionsverfahren: Die ersten 4 Stellen sind die dekodierte Folge, also 1001.

(f) Beim Empfänger kommt an: $1101001 \oplus 0011101 = 1110100$. Dekodierung (Multiplikationsverfahren):

$$\frac{x^6 + x^5 + x^4 + x^2}{x^3 + x + 1} = x^3 + x^2 - 2 + \frac{2x + 2}{x^3 + x + 1}$$

wobei der Rest äquivalent zu 0 ist. Es wird kein Fehler erkannt, obwohl es einen Fehler gab.

Aufgabe 3

(a) $k_1 = 4$ und $k = 5$, damit $n = 2^4 - 1 = 15$, $l = 10$ und $d_{min} = 4$

(b) Maximal 3 Bitfehler oder maximal 5 Bündelfehler oder ungeradzahlige Fehlermuster

(c) b_2 hat 7 Einsen und b_4 hat 9 Einsen. Bei b_1 sind 5 Bits hintereinander falsch, diese können erkannt werden. Bei b_3 gibt es 6 Einzelfehler, damit ist keine Erkennung möglich.

Aufgabe 4

Nein, Kodierung schützt nicht vor Angreifern. Angreifer können die Leitung abhören und die Nachricht dekodieren (↗ Vertraulichkeit), sie können sogar die Nachricht abfangen, verändern, neu kodieren und über die Leitung schicken! (↗ Integrität)