

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 $d_{min} = 3$. Damit sind beide Kodes in der Lage 1 bzw. 2 Fehler zu erkennen, aber nur Kode 2 kann einen Fehler korrigieren.

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: $(x^3 + x + 1) \cdot (x^2 + x + 1) = x^5 + x^4 + 1 \pmod{2} \Rightarrow 110001$
Divisionsverfahren: ?
- (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 (?)
Falls b_2 mit dem Multiplikationsverfahren kodiert wurde, so ist die dekodierte Folge 1010. Divisionsverfahren?
- (f) ?

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 4 Bündelfehler oder ungeradzahlige Fehlermuster
- (c) b_2 hat 7 Einsen und b_4 hat 9 Einsen

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)