

## 1. Endlicher Körper $\mathbb{F}_8$

Es soll die Determinante von  $A$  berechnet werden:

$$\det \begin{pmatrix} 1 & 2 & 3 \\ 0 & 3 & 4 \\ 5 & 4 & 2 \end{pmatrix} = 1 * 3 * 2 + 2 * 4 * 5 + 3 * 0 * 4 - (3 * 3 * 5 + 2 * 0 * 2 + 1 * 4 * 4)$$

Nun sind wir aber in dem Körper  $\mathbb{F}_8$ , und da muss man so geschickt rechnen. Modulo geht ja leider auch nicht, da es sich nicht um eine Primzahl handelt. Man muss jetzt also die Elemente des Körpers als Polynome über  $\mathbb{F}_2$  betrachten und mit denen rechnen. Die Polynome sehen wie folgt aus:

$0 : 0$	$4 : x^2$
$1 : 1$	$5 : x^2 + 1$
$2 : x$	$6 : x^2 + x$
$3 : x + 1$	$7 : x^2 + x + 1$

Jetzt zu den Rechnungen ...

$$\begin{aligned} 1 * 3 * 2 &= 1 * (x + 1) * x = (x^2 + x) \mod (x^3 + x^2 + 1) = x^2 + x = 6 \\ 2 * 4 * 5 &= x * x^2 * (x^2 + 1) = (x^5 + x^3) \mod (x^3 + x^2 + 1) = x^2 + x = 6 \\ 3 * 0 * 4 &= (x + 1) * 0 * x^2 = 0 \\ 3 * 3 * 5 &= (x + 1) * (x + 1) * (x^2 + 1) \\ &= (x^2 + 1) * (x^2 + 1) = (x^4 + 1) \mod (x^3 + x^2 + 1) = x^2 + x = 6 \\ 2 * 0 * 2 &= x * 0 * x = 0 \\ 1 * 4 * 4 &= 1 * x^2 * x^2 = x^4 \mod (x^3 + x^2 + 1) = x^2 + x + 1 = 7 \end{aligned}$$

Nebenrechnungen ...

$$\begin{array}{r} (x^5 + x^3) : (x^3 + 1) = x^2 + x \\ -(x^5 + x^4 + x^2) \\ \hline x^4 + x^3 + x^2 \\ -(x^4 + x^3 + x) \\ \hline x^2 + x \end{array}$$

$$\begin{array}{r} (x^4 + 1) : (x^3 + x^2 + 1) = x + 1 \\ -(x^4 + x^3 + x) \\ \hline x^3 + x + 1 \\ -(x^3 + x^2 + 1) \\ \hline x^2 + x \end{array}$$

$$\begin{array}{r} (x^4) : (x^3 + x^2 + 1) = x + 1 \\ -(x^4 + x^3 + x) \\ \hline x^3 + x \\ -(x^3 + x^2 + 1) \\ \hline x^2 + x + 1 \end{array}$$

Nach den Multiplikationen folgen nun noch die Additionen:

$$\begin{aligned} 6 + 6 + 0 - (6 + 0 + 7) &= (x^2 + x) + (x^2 + x) - ((x^2 + x) + (x^2 + x + 1)) \\ &= 2x^2 + 2x - (2x^2 + 2x + 1) = 0 - 1 = 1 \end{aligned}$$

Die Determinante in  $\mathbb{F}_8$  ist also 1.

## 2. Erweiterter Linearcode

a)

b)

## 3. Hamming-Code

Als erstes wird mit der Prüfmatrix getestet, ob auch die Nachricht fehlerfrei übertragen wurde:

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

Das bedeutet also, dass ein Bit bei der Übertragung gekippt ist, und zwar das siebte, da 111 die Binärdarstellung von 7 entspricht. Die Nachricht kann also zu 1001100 korrigiert werden. Die letzten drei Bits sind Paritätsbits, daher war die ursprünglich gesendete Nachricht 1001.

## 4. Konstruktion eines Codes

Es soll ein  $(4,2,3)$ -Code über einem möglichst kleinen Alphabet konstruiert werden. Daraus folgt, dass  $G : Q^2 \rightarrow Q^4$  und  $H : Q^4 \rightarrow Q^{4-2}$ . Es ist bekannt, dass  $rg(H) = 4 - 2 = 2$  sein muss. Weil wir  $(0,0)$  ja nicht in der Prüfmatrix drin haben dürfen, fällt  $\mathbb{F}_2$  schonmal als Alphabet raus. Gucken wir uns das ganze also für  $\mathbb{F}_3$  an. Jetzt dann die Prüfmatrix. Bei der Prüfmatrix in Standardform ist hinten immer die Einheitsmatrix, also fehlen nur die ersten beiden Spalten. Diese können beliebig gewählt werden aus dem Raum, nur dürfen keine 2 Vektoren linear abhängig werden:

$$H = \begin{pmatrix} 1 & 2 & 1 & 0 \\ 2 & 2 & 0 & 1 \end{pmatrix}$$

Bei der Generatormatrix steht oben wieder die Einheitsmatrix und darunter der negierte Anfang. Die Generatormatrix ergibt sich dann also als

$$G = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 2 & 1 \\ 1 & 1 \end{pmatrix}$$