2.4 Lineare Codes

Ist K ein Körper, so ist bekanntlich der Vektorraum $V = K^n$ aller Funktionen von $\{1, \ldots, n\}$ nach K mit punktweiser Addition und punktweiser Skalierung ein Vektorraum über K. Ist K ein endlicher Körper, so können wir K als ein Alphabet auffassen und Codes über K betrachten; es ist dann zwingend $|K|$ eine Primzahlpotenz, und umgekehrt gibt es zu jeder Primzahlpotenz q einen bis auf Isomorphie eindeutig bestimmten Körper mit q Elementen, denn wir mit $\mathbb{F}_q$ bezeichnen. (Ist q eine Primzahl, so ist $\mathbb{F}_q \cong \mathbb{Z}_q$, der Restklassenring modulo q.) Ein *(linearer) q-adischer $[n, k]$-Code* ist ein k-dimensionaler Untervektorraum C von $\mathbb{F}_q^n$. Da jeder k-dimensionale Untervektorraum über $\mathbb{F}_q$ isomorph zu $\mathbb{F}_q^k$ ist, enthält ein q-adischer $[n, k]$-Code genau q^k Elemente. Aus dem gleichen Grund haben Geraden, Ebenen, Hyperebenen etc. von K^n stets die gleiche Zahl Elemente (nämlich q, q^2, q^{n-1} etc.), ein hier oft verwendeter Sachverhalt.

Untervektorräume von K^n lassen sich auf verschiedene Weisen durch Matrizen beschreiben. Im Gegensatz zu der in der Linearen Algebra verbreiteten und historisch bedingten Lesart der Elemente von K^n als „Spaltenvektoren" werden in der Codierungstheorie die Elemente aus K^n als „Zeilenvektoren" gedacht, da sie zumeist Worte sind. So ist zum Beispiel für eine Matrix $G \in K^{m \times n}$ und ein $x \in K^m$ das Produkt $x \cdot G$ durch $(x \cdot G)(i) := \sum_{j=1}^{k} x(j) \cdot G(j, i)$ für $i \in \{1, \ldots, n\}$ erklärt, also aus K^n. Tatsächlich ist $x \cdot G$ die durch x dargestellte Linearkombination der Zeilen von G. Variiert man x, so erhält man folglich den *Zeilenraum*

$$C := \{x \cdot G : x \in K^m\}$$

der Matrix G. Er ist ein Untervektorraum von K^n der Dimension $\mathrm{rg}(G)$, wobei $\mathrm{rg}(G)$ der *Zeilenrang* von G ist, also die größte Anzahl linear unabhängiger Zeilenvektoren von G. In der Linearen Algebra zeigt man, daß dies zugleich die größte Anzahl linear unabhängiger Spaltenvektoren von G ist, also gleich dem *Spaltenrang* von G. Infolgedessen nennt man $\mathrm{rg}(G)$ auch schlicht den *Rang* von G. Ist K ein endlicher Körper, so ist folglich C ein $[n, \mathrm{rg}(G)]$-Code, und wir nennen G eine *Generatormatrix* oder einen *Generator* von C, falls die Zeilen von G linear unabhängig sind. Jeder lineare Code hat einen Generator.

Ist jetzt $H \in K^{n \times m}$, so definiert auch

$$C := \{x \in K^n : x \cdot H = 0\}$$

einen Untervektorraum von K^n. Er hat die Dimension $n - \mathrm{rg}(H)$, ist also im Fall eines endlichen Körpers K ein linearer $[n, n - \mathrm{rg}(H)]$-Code, und wir nennen H eine *Prüfsummenmatrix* oder auch *Kontrollmatrix* für C. Den Spalten von H entsprechen dabei Gleichungen der Form $x \cdot h = 0$, die genau dann alle erfüllt sind, wenn x aus C stammt. Jeder lineare Code hat auch eine Prüfsummenmatrix.

Zwischen Generator- bzw. Prüfsummenmatrizen und dem Minimalabstand der durch sie bestimmten Codes bestehen folgende fundamentale Zusammenhänge.

Satz 8 *Sei C ein q-adischer $[n,k]$-Code. Dann gilt*

(i) $d(C) = \min\{d(x,0) : x \in C \setminus \{0\}\}$.

(ii) Ist G eine $k \times n$-Generatormatrix von C, so gilt $d(C) = \min\{d(xG,0) : x \in K^k \setminus \{0\}\}$.

(iii) Ist H Prüfsummenmatrix von C so gilt $d(C) \geq d$ genau dann, wenn jede *Auswahl von weniger als d Zeilen von H linear unabhängig ist.*

Beweis. Sind $x \neq y$ aus C so auch $x-y \in C\setminus\{0\}$ und es gilt $d(x,y) = d(x-y,0)$. Also gilt $\{d(x,y) : x \neq y \text{ aus } C\} \subseteq \{d(x,0) : x \in C \setminus \{0\}\}$ und trivialerweise $\supseteq$; beide Mengen von Abstandswerten sind folglich gleich, haben insbesondere das gleiche Minimum, nämlich $d(C)$. Dies zeigt (i).

Nach Definition sind die Zeilen von G in (ii) linear unabhängig, das heißt der Nullvektor läßt sich aus ihnen nur trivial kombinieren. Folglich ist $C \setminus \{0\} = \{xG : x \in K^m \setminus \{0\}\}$, woraus (ii) folgt.

Seien $H(i,\cdot)$ die Zeilen von $H \in \mathbb{F}_q^{n\times m}$ und $d(C) < d$. Wegen (i) gibt es ein $x \in C \setminus \{0\}$ mit $J := \{\{1,\ldots,n\} : x_j \neq 0\}$, $|J| < d$. Es ist

$$0 = (xH)(i) = \sum_{j=1}^{n} x(j)H(j,i) = \sum_{j\in J} x(j)H(j,\cdot)(i)$$

für alle $i \in \{1,\ldots,m\}$, also $\sum_{j\in J} x(j)H(j,\cdot) = 0$. Folglich besitzt der Nullvektor aus $\mathbb{F}_q^m$ eine nichttriviale Darstellung durch weniger als d Zeilen von H.

Sind umgekehrt für $J \subseteq \{1,\ldots,n\}$, $|J| < d$, die Zeilen $H(j,\cdot)$ mit $j \in J$ linear abhängig, so gibt es $x \in \mathbb{F}_q^n$ mit $x \neq 0$ und $x_j = 0$ für alle $j \in \{1,\ldots,n\} \setminus J$ sowie $xH = 0$, also $x \in C \setminus \{0\}$ mit $d(x,0) < d$. Folglich ist $d(C) < d$. Dies zeigt (iii). □

Wir betrachten den Vektorraum $\mathbb{F}_q^k$, $k \geq 2$, mit q^k vielen Elementen. Da jede Gerade genau q viele Elemente hat und verschiedene Geraden nur den Nullvektor gemeinsam haben, jede Gerade also durch einen von wahlweise $q-1$ Vektoren aus $\mathbb{F}_q^k \setminus \{0\}$ bestimmt ist, „zerfällt" $\mathbb{F}_q^k$ in $n := (q^k-1)/(q-1)$ viele Geraden. Aus jeder dieser Geraden wähle man einen von 0 verschiedenen Repräsentanten, diese mögen die Zeilen der $n \times k$-Matrix H bilden. Die Repräsentanten der durch die k Einheitsvektoren bestimmten Geraden sind linear unabhängig, daher hat H den (vollen) Rang k. Der durch die Prüfsummenmatrix H gegebene Code C ist daher ein $[n,n-k]$-Code. Jeder auf diese Weise konstruierbare Code heißt ein *q-adischer $[n,n-k]$-Hamming-Code* oder schlicht ein *Hamming-Code*.

Satz 9 *Jeder Hamming-Code ist perfekt* 1*-fehlerkorrigierend.*

Beweis. Sei H eine $n \times k$-Prüfsummenmatrix wie in der Definition und C der durch sie bestimmte Hamming-Code. Je zwei Zeilen von H sind dann linear unabhängig, also gilt $d(C) \geq 3$ wegen (iii) aus Satz 8. Die drei Repräsentanten der vom ersten und zweiten Einheitsvektor ($k \geq 2$!) sowie deren Summe aufgepannten Geraden sind jeoch linear abhängig, so daß $d(C) \leq 3$ gilt, folglich $d(C) = 3$. Daher ist C 1-fehlerkorrigierend. Es ist $|B_1(0)| = 1 + n(q-1) = q^k$ und daher die Hamming-Schranke gleich $q^n/q^k = q^{n-k}$, also gleich $|C|$. Somit ist C perfekt 1-fehlerkorrigierend. □

Codes $C, D \subseteq A^n$ heißen *äquivalent*, wenn es eine Permutation π von $\{1, \ldots, n\}$ mit

$$D = \{x_{\pi(1)} \ldots x_{\pi(n)} : x_1 \ldots x_n \in C\}$$

gibt (das heißt: die Wörter aus D entstehen durch Vertauschen der Positionen der Buchstaben gemäß π aus den Wörtern in C). Hierdurch wird eine Äquivalenzrelation auf der Menge aller n-Codes über A definiert. Äquivalente Codes besitzen den gleichen Minimalabstand, und äquivalente lineare Codes sind als Vektorräume isomorph.

Satz 10 *Jeder q-adische $[n, k]$-Code ist äquivalent zu einem Code C mit Erzeuger $G = (E_k\, P)$, wobei E_k die k-te Einheitsmatrix ist und P eine $k \times (n-k)$-Matrix. Die Matrix $\binom{-P}{E_{n-k}}$ ist dann Prüfsummenmatrix von C.*

Beweis. Zunächst bringt man eine beliebige $k \times n$-Generatormatrix für den gegebenen Code mittels des Gaußschen Algorithmus' auf Zeilenstufenform. Der Zeilenraum bleibt dadurch bekanntlich unverändert, die neue Matrix erzeugt daher denselben Code. Durch Tauschen der Stufenanfangsspalten an die ersten k Positionen entsteht eine Generatormatrix G der angegebenen Gestalt für einen zum gegebenen Code äquivalenten Code C; dieser ist ebenfalls ein $[n, k]$-Code.

Der durch die Prüfsummenmatrix $H := \binom{-P}{E_{n-k}}$ vermöge $D := \{w \in K^n : wH = 0\}$ gegebene Code ist ein $[n, n - \operatorname{rg} H]$-Code, also wegen $\operatorname{rg} H = n - k$ ebenfalls ein $[n, k]$-Code. Nun folgt aus $w \in C$ zunächst $w = xG$ für ein $x \in K^k$ und daraus

$$w \cdot H = xGH = x(E_k\, P)\begin{pmatrix} -P \\ E_{n-k} \end{pmatrix} = x(-E_kP + PE_{n-k}) = x(-P + P) = 0,$$

also $w \in D$. Somit ist C ein Untervektorraum von D der gleichen Dimension wie D, also gleich D. □

Sei K ein Körper und $x \in K^n$. Sei $\widehat{x} \in K^{n+1}$ definiert durch $\widehat{x}(i) := x(i)$ für $i \in \{1, \ldots, n\}$ und

$$\widehat{x}(n+1) := -\sum_{i=1}^{n} x(i).$$

Wir sagen, das Wort $\widehat{x}$ entstehe aus x durch *Erweiterung um eine (kanonische) Prüfsummenstelle*. Die hierdurch gegebene Abbildung $\widehat{\ }: K^n \to K^{n+1}$ ist linear (ein Vektorraumhomomorphismus), das heißt $\widehat{x+y} = \widehat{x} + \widehat{y}$ und $\widehat{\lambda x} = \lambda \widehat{x}$ für alle $x, y \in K^n$ und $\lambda \in K$.

Satz 11 *Sei C ein q-adischer $[n,k]$-Code. Dann gilt:*

(i) $\widehat{C} := \{\widehat{c} : c \in C\}$ *ist ein q-adischer $[n+1,k]$-Code.*

(ii) Ist G Generatormatrix mit den Spalten $x_1, \ldots, x_n$ und $x := -\sum_{i=1}^{n} x_i \in K^k$, so ist $\widehat{G} := (G\, x)$ Generatormatrix für $\widehat{C}$.

(iii) Ist H eine $n \times (n-k)$-Prüfsummenmatrix für C, so ist die durch Hinzufügen einer 0-Zeile und danach Hinzufügen einer Spalte mit lauter Einsen aus H entstehende $(n+1) \times (n-k+1)$-Matrix $\widehat{H}$ eine Prüfsummenmatrix für $\widehat{C}$.

(iv) Ist $q = 2$ und $d(C)$ ungerade, so ist $d(\widehat{C}) = d(C) + 1$.

Beweis. Die Matrix $\widehat{G}$ aus (ii) hat unverändert (Spalten-) Rang k, erzeugt also einen $[n+1,k]$-Code D. Ist $\lambda_1, \ldots, \lambda_k$ eine Darstellung von $c \in C$ durch die Zeilen $g_1 \ldots g_k$ von G, so ist dies auch eine Darstellung von $\widehat{c}$ durch die linear unabhängigen Zeilen $\widehat{g_1}, \ldots, \widehat{g_k}$ von $\widehat{G}$. Somit ist $\hat{C} \subseteq D$, also ist $\hat{C}$ ein k-dimensionaler Untervektorraum des k-dimensionalen Vektorraums D und folglich gleich D. Dies zeigt (i) und (ii).

Für (iii) beobachtet man, daß für jedes $w \in C$ $\widehat{w}h = 0$ ist für jede Spalte h von $\widehat{H}$, auch für die letzte. Daher ist $\widehat{C}$ ein k-dimensionaler Untervektorraum des Vektorraums $D := \{w \in K^{n+1} : w\widehat{H} = 0\}$. Wegen $\mathrm{rg}(\widehat{H}) = \mathrm{rg}(H) + 1$ ist $n+1-\mathrm{rg}(\widehat{H}) = n+1-(n-k+1) = k$, also D ein $[n+1,k]$-Code, und wieder folgt $\widehat{C} = D$ und daraus (iii).

Wegen $d(\widehat{x}, 0) \in \{d(x,0), d(x,0)+1\}$ folgt $d(\widehat{x},0) \geq d(x,0)$ Sei nun $q = 2$. Dann hat jedes Wort in $\widehat{C}$ geraden Hammingabstand zur 0 (ist nämlich $d(x,0)$ ungerade, so ist $\widehat{x}(n+1) = 1$, und ist $d(x,0)$ gerade, so ist $\widehat{x}(n+1) = 0$). Insbesondere ist $d(\widehat{C})$ gerade, also $d(\widehat{C}) = d(C) + 1$. Dies zeigt (iv). □