2.1 Codes: einige Grundbegriffe

Wir stellen die wichtigsten Grundbegriffe für Codes über dem „Alphabet“ $\mathbb{F}_q$, also über einem endlichen Körper mit q Elementen zusammen. Dabei kommt dem Fall $q = 2$, allgemeiner $q = 2^t$ eine besondere Bedeutung zu; wichtig ist auch noch der Fall $q = 3$.

Definition 2.1.1 Das *Hamming-Gewicht* oder die *Hamming-Norm* von $\mathbf{c} \in \mathbb{F}_q^n$ ist definiert als

$$\operatorname{wt} \mathbf{c} := |\{i \mid c_i \neq 0\}| \,.$$

Der *Hamming-Abstand* von $\mathbf{c}$ zu $\mathbf{c}'$ ist definiert als

$$d(\mathbf{c}, \mathbf{c}') = d_H(\mathbf{c}, \mathbf{c}') := \operatorname{wt}(\mathbf{c} - \mathbf{c}')$$

Die Funktion $d_H : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{R}_{\geq 0}$ ist eine Metrik (im üblichen Sinne der Analysis oder Topologie).

Definition 2.1.2 Ein *Code* (genauer: *Block-Code*) der Blocklänge n ist eine Teilmenge $C \subseteq \mathbb{F}_q^n$. Ein *linearer Code* ist ein Untervektorraum von $\mathbb{F}_q^n$. Man spricht von einem binären Code, wenn das Alphabet gleich $\mathbb{F}_2 = \{0, 1\}$ ist.

Im Zusammenhang mit Gittern sind nur lineare Codes von Interesse (siehe Satz 2.3.3 unten). Allerdings spielen gelegentlich nicht-lineare Codes eine analoge Rolle für nicht-gitterförmige (aber immerhin noch periodische) Kugelpackungen. In technischen Anwendungen zur Fehlerkorrektur bei Datenübertragung benutzte Codes sind in der Regel ebenfalls linear. Dieses ist u.a. dadurch begründet, dass dann Algorithmen zur Codierung und Decodierung effizienter gestaltet werden können.

Die folgende Definition sprechen wir nur noch für $q = 2$ aus. Für andere Alphabete, bzw. für noch allgemeinere „Codes”, spielen nämlich allgemeinere Metriken als die hier benutzte Hamming-Metrik eine Rolle.

Definition und Bemerkung 2.1.3 Der *Minimalabstand* eines Codes $C \subset \mathbb{F}_2^n$ ist definiert als

$$\min C := \min\{d_H(\mathbf{c}, \mathbf{c}') \mid \mathbf{c}, \mathbf{c}' \in C, \mathbf{c} \neq \mathbf{c}'\} \,.$$

Falls C linear ist, so gilt

$$\min C = \min\{\operatorname{wt} \mathbf{c} \mid \mathbf{c} \in C \smallsetminus \{\mathbf{0}\} \,.$$

Ein $[n, k, d]$-Code ist ein linearer Code $C \subseteq \mathbb{F}_2^n$ der Dimension k mit Minimalabstand $\min C = d$.

Oft kennt man nur eine untere Schranke d für den Minimalabstand. Wir sprechen dann von einem $[n, k, \geq d]$-Code.

Wir wenden uns nun der Frage zu, wann wir zwei Codes als „im wesentlichen gleich“ (isomorph) ansehen. Bei Codes spricht man üblicherweise von Äquivalenz. Zwei Codes sollten auf jeden Fall äquivalent sein, wenn sie sich lediglich um eine Permutation der Komponenten der Codewörter unterscheiden. Allerdings gibt es gute Gründe, für größere Alphabete als $\{0, 1\}$ eine etwas gröbere Äquivalenzrelation zu benutzen, die auch gewisse Permutationen der Symbole, nicht nur der Koordinaten, erlaubt. Wir führen das im folgenden etwas aus.

Definition 2.1.4 a) Zwei Codes C und C' heißen *permutations-äquivalent*, wenn sie durch geeignete Vertauschung der Koordinaten ineinander überführt werden:

$$C' = \{x_{\sigma(1)} x_{\sigma(2)} \dots x_{\sigma(n)} \mid \mathbf{x} \in C\}$$

für eine geeignete Permutation $\sigma \in S_n$.

b) Zwei Codes derselben Länge n über demselben $\mathbb{F}_q$ heißen (linear) *distanz-äquivalent*, wenn es eine Permutation $\sigma \in S_n$ und Skalare $t_1, \dots, t_n \in \mathbb{F}_q \smallsetminus \{0\}$ gibt derart, dass

$$C' = \{(t_1 x_{\sigma(1)}, \dots, t_n x_{\sigma(n)} \mid \mathbf{x} \in C\}\,.$$

Der Grund für die Bezeichnung distanz-äquivalent liegt in folgendem.

Bemerkung 2.1.5 Die linearen Abbildungen $\varphi : \mathbb{F}_q^n \to \mathbb{F}_q^n$, die die Hamming-Distanz erhalten, d.h.

$$d_H(\mathbf{x}, \mathbf{y}) = d_H(\varphi\mathbf{x}, \varphi\mathbf{y}) \qquad \text{für alle } \mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n\,,$$

sind genau die Abbildungen der Form

$$\mathbf{x} \mapsto (t_1 x_{\sigma(1)}, \dots, t_n x_{\sigma(n)})\,, \quad t_i \in \mathbb{F}_q \smallsetminus \{0\},\ \sigma \in S_n\,.$$

Wenn wir im folgenden einfach von *Äquivalenz* von Codes sprechen, so ist immer Distanz-Äquivalenz gemeint.

Als nächstes besprechen wir die Beschreibung von linearen Codes durch Matrizen. Es gibt hierfür zwei Möglichkeiten.

Definition 2.1.6 Wenn C ein $[n, k]$-Code ist, so heißt jede $(k \times n)$-Matrix G, deren Zeilen eine Basis von C bilden, eine *Erzeugermatrix* (generator matrix) von C. Eine $(n - k) \times n$-Matrix H, deren Lösungsmenge C ist, d.h.

$$C = \{\mathbf{x} \in \mathbb{F}_q^n \mid H\mathbf{x}^t = 0\}\,,$$

heißt *Kontrollmatrix* (parity check matrix) von C.

Die Zeilen einer Kontrollmatrix sind notwendig linear unabhängig. Wenn umgekehrt H eine $(n-k) \times n$-Matrix vom Rang $n-k$ mit $Hx^t = 0$ für alle $x \in C$ ist, so ist aus Dimensiongründen C bereits der ganze Lösungsraum, also H eine Kontrollmatrix.

Für Erzeuger- und Kontrollmatrizen gibt es einen Art Normalform, die wir als nächstes besprechen.

Proposition 2.1.7 *a) Jeder lineare Code ist permutations-äquivalent zu einem Code mit Erzeugermatrix der Form*

$$G = (E_k, P) \qquad E_k \text{ die } k \times k\text{-Einheitsmatrix}.$$

b) Wenn (E_k, P) eine Erzeugermatrix eines Codes C ist, so ist

$$(-P^t, E_{n-k})$$

eine Kontrollmatrix für C, und umgekehrt.

Beweis: a) Wenn G irgendeine Erzeugermatrix ist, so ist eine geeignete $k \times k$-Untermatrix regulär, nach geeigneter Permutation sind dies die ersten k Spalten. Durch geeignete Zeilen-Operationen, die den erzeugten Code nicht ändern, wird hieraus die $k \times k$-Einheitsmatrix.

b) Die angegebene Matrix H ist eine $(n-k) \times k$-Matrix, und

$$G \cdot H^t = (E_k, P)\begin{pmatrix} P \\ E_{n-k} \end{pmatrix} = -P + P = 0\,.$$

□

Wir kommen schließlich zum Begriff des geraden binären Codes. Hier haben alle Codewörter gerades Hamminggewicht bzw. sie genügen der „Paritätsgleichung" $\sum_{i=1}^{n} x_i = 0 \in \mathbb{F}_2$.

Definition und Bemerkung 2.1.8 Wir betrachten binäre Codes.

a) Ein Code heißt *gerade*, falls alle seine Codewörter gerades Gewicht haben.

b) Der *erweiterte Code* eines gegebenen Codes C ist der Code

$$\widehat{C} := \{(x_1, x_2, \ldots, x_n, \sum_{i=1}^{n} x_i) \mid (x_1, x_2, \ldots, x_n) \in C\}.$$

c) Jeder erweiterte Code $\widehat{C}$ ist gerade.

d) Wenn C ein $[n, k, d]$-Code ist, so ist $\widehat{C}$ ein $[n+1, k, d']$-Code mit $d' = d$ für gerades d und $d' = d + 1$ für ungerades d.

In der folgenden Definition ist $\mathbf{x} \cdot \mathbf{y} := \sum_{i=1}^{n} x_i y_i$ das Standard-Skalarprodukt auf $\mathbb{F}_q^{\,n}$.

Definition und Bemerkung 2.1.9 Es sei C ein Code über dem Alphabet $\mathbb{F}_q$.

a) $C^\perp := \{\mathbf{y} \in \mathbb{F}_2^{\,n} \mid \mathbf{x} \cdot \mathbf{y} = 0 \text{ für alle } \mathbf{x} \in C\}$ heißt der *duale Code* zu C. Dieses ist ein linearer Code.

b) Wenn C linear von der Dimension k ist, dann hat $C^\perp$ die Dimension $n - k$.

c) Der Code C heißt *selbstorthogonal*, wenn $C \subseteq C^\perp$ ist.

d) Der Code C heißt *selbstdual*, wenn $C = C^\perp$ ist.

Falls q ungerade ist, muss in gewissen Sitatuationen die Definition des dualen Codes etwas modifiziert werden. Auf $\mathbb{F}_q^{\,n}$ gibt es dann nämlich noch eine zweite, nicht-äquivalente reguläre symmetrische Bilinerform (deren Determinante ein Nicht-Quadrat in $\mathbb{F}_q$ ist). Für Anwendungen auf Gitter wird die Bilinearform von der Diskriminantenform des Gitters herkommen (siehe 1.5.7); hier spielt das Standardskalarprodukt keine Sonderrolle.

Die folgende Bemerkung ergibt sich unmittelbar aus den Definitionen; sie beruht darauf, dass wir das Standardskalarprodukt benutzt haben.

Bemerkung 2.1.10 Es sei C ein linearer Code.

a) Eine Matrix ist genau dann Erzeugermatrix von C, wenn sie Kontrollmatrix von $C^\perp$ ist.

b) Eine Matrix ist genau dann Kontrollmatrix von C, wenn sie Erzeugermatrix von $C^\perp$ ist.

Die folgende Definition führt zu zahlreichen interessanten Resultaten und Verallgemeinerungen, die wir hier nicht behandeln können. Trotzdem wird sie später in dieser Vorlesung wieder auftauchen, weil es analoge Konzepte für Gitter gibt und auch Zusammenhänge zwischen beidem.

Definition 2.1.11 Für einen lineare Code C heißt die Zahlenfolge $(a_j(C))_{j=0,\ldots,n}$ mit

$$a_j(C) := \#\{\mathbf{c} \in C \mid \mathrm{wt}(\mathbf{c}) = j\}$$

die *Gewichtsverteilung* von C. Das Polynom

$$A_C(X, Y) := \sum_{j=0}^{n} a_j(C) X^{n-j} Y^j$$

heißt (homogener) *Gewichtszähler* von C.

2.2 Einige wichtige Codes

Hamming-Codes.
Die Grundidee der Hamming-Codes ist, dass sie den Minimalabstand 3 haben, also einen Fehler korrigieren können, und unter allen solchen Codes eine möglichst hohe Dimension k (relativ zur Blocklänge n) haben, d.h. eine möglichst große *Informationsrate* k/n. Die folgende Konstruktion erreicht dieses Ziel in optimaler Weise, d.h. mit beweisbar größtmöglicher Anzahl von Codewörtern (sog. „perfekte Codes"). Der Preis, den man dafür zahlt, ist, dass Hamming-Codes nur in relativ wenigen Dimensionen existieren (abhängig vom Alphabet $\mathbb{F}_q$).

Wir klären zunächst, wann ein linearer Code den Minimalabstand 3 hat.

Lemma 2.2.1 Ein linearer Code C sei durch die Kontrollmatrix H gegeben. Dann ist $\min C \geq 3$ genau dann, wenn zwei beliebige Spalten von H linear unabhängig sind.

Beweis: Es seine $\mathbf{h}_1, \ldots, \mathbf{h}_n$ die Spalten einer Kontrollmatrix. Ein Wort $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ liegt in C genau dann, wenn $\sum_{i=1}^n x_i \mathbf{h}_i = \mathbf{0}$ ist. Ein Codewort vom Gewicht m entspricht also einer nicht-trivialen Relation zwischen m Spalten von H. Hieraus folgt die Behauptung. □

Sei C ein Code der Blocklänge n mit Minimalabstand 3 und r der Rang einer Erzeugermatrix H. Dann ist die Dimension $k = n - r$, die Informationsrate $k/n = (n-r)/n$ ist bei gegebenem r also umso größer, je größer n ist, das heißt, je mehr Spalten H hat. Keine zwei Spalten von H sind proportional zueinander, und die größtmögliche Anzahl solcher Spalten ist die Anzahl aller eindimensionalen Unterräume von $\mathbb{F}_q^n$. Diese Anzahl ist offenbar gleich $\frac{q^r-1}{q-1}$, speziell gleich $2^n - 1$ für binäre Codes.

Definition und Bemerkung 2.2.2 Ein linearer Code über $\mathbb{F}_q$ heißt *Hamming-Code*, wenn er die Parameter

$$\left[n_r := \frac{q^r - 1}{q - 1},\ n_r - r,\ 3 \right]$$

für ein $r \in \mathbb{N}$ besitzt. Dann sind keine zwei Spalten einer Kontrollmatrix des Codes proportional zueinander, und alle möglichen Spalten der Länge r kommen in einer Kontrollmatrix vor.

Nach der vorangegangenen Diskussion ist die Eigenschaft, dass die Spalten einer Kontrollmatrix eines Hamming-Codes paarweise nicht proportional zueinander sind, unabhängig von der Wahl der Kontrollmatrix. Dieses sieht man auch leicht direkt, ohne den Zusammenhang mit dem Minimalabstand. Zwei Kontrollmatrizen gehen nämlich durch Zeilenumformungen auseinander hervor, also auch die aus zwei festen Spalten gebildeten Untermatrizen. Dabei ändert sich deren Rang $(= 2)$ nicht.

Die Tatsache, dass die Spalten der Kontrollmatrix genau ein Vertretersystem für die eindimensionalen Unterräume von $\mathbb{F}_q^n$ durchlaufen, hat noch eine weitere Konsequenz. Wenn wir nämlich zwei solche $r \times n_r$-Matrizen betrachten, so können diese offenbar durch geeignete Vertauschung der Spalten und anschließendes Multiplizieren jeder Spalte mit einem gewissen Skalar $\neq 0$ ineinander überführt werden. Entsprechendes gilt dann für die Lösungsräume der Matrizen (mit jeweils dem inversen Skalar), das heißt für die beiden zugehörigen Codes. Wir haben also folgendes eingesehen.

Bemerkung 2.2.3 Für festes r und q sind je zwei Hamming-Codes C und C' zueinander äquivalent. Dementsprechend werden wir oft von *dem* $[n_r, n_r - r, 3]$-Hamming-Code sprechen; Bezeichnung $\mathcal{H}_n$. Der erweiterte Code heißt entsprechend $[n_r + 1, n_r - r, 4]$-Hamming-Code.

Schon einfache Beispiele zeigen, dass für $q > 2$ zwei Hamming-Codes im allgemeinen nicht permutations-äquivalent sind.

Wir wollen nun die oben gemachte Aussage präzisieren, dass die Hamming-Codes in gewissem Sinn bestmöglich sind.

Definition 2.2.4 Ein (nicht notwendig linearer) Code heißt *perfekt*, falls die Hamming-Kugeln von einem festen Radius e um die Codewörter eine disjunkte Zerlegung des $\mathbb{F}_q^n$ bilden.

Offenbar gibt es bei gegebenem Code nur eine Möglichkeit für e (es reicht schon, die Anzahl der Codewörter zu kennen). Für gegebenes e und n existiert im Allgemeinen kein perfekter Code. Wenn er existiert, ist die Anzahl der Codewörter eindeutig bestimmt, wie sich unmittelbar aus der Definition ergibt. Ein perfekter Code hat die größtmögliche Anzahl von Codewörtern unter allen Codes, für die die Kugeln vom Radius e für je zwei verschiedene Codewörter disjunkt sind. Das sind genau die Codes mit Minimalabstand $\geq 2e + 1$. (Solche Codes können bei dem üblichen Modell der Maximum-Likelihood-Decodierung e Fehler korrigieren.)

Eine Hamming-Kugel vom Radius 1 im $\mathbb{F}_q^n$ hat offenbar $1 + n(q-1)$ Elemente (einschließlich Mittelpunkt). Ein Code C mit Minimalabstand 1 ist also perfekt genau dann, wenn $|C|(1 + n(q-1)) = q^n$ ist. Für einen Hamming-Code zu den Parametern q und r ist $n(q-1) = q^r - 1$ und $|C| = q^{n-r}$. Somit haben wir bewiesen:

Satz 2.2.5 *Jeder Hamming-Code ist perfekt.*

Im binären Fall sind die kleinsten Parameter von Hamming-Codes $[3, 1, 3]$, $[7, 4, 3]$, $[15, 11, 3]$, $[31, 26, 3]$. Besonders wichtig, sowohl innerhalb der Codierungstheorie, als auch für Anwendungen auf Gitter, ist der (erweiterte) $[8, 4, 4]$-Hamming-Code. Wir zeigen jetzt, dass dieser Code durch seine Parameter sogar eindeutig bestimmt ist (gemeint ist natürlich „eindeutig bis auf Äquivalenz“).

Proposition 2.2.6 *Es gibt bis auf Äquivalenz genau einen binären* $[8,4,4]$*-Code. Eine Erzeugermatrix hierfür ist*

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

Beweis: Nach 2.1.7 kann eine Erzeugermatrix nötigenfalls nach Übergang zu einem äquivalenten Code in der Gestalt $(E_4\, A)$, E_4 die 4×4-Einheitsmatrix, gewählt werden. Da der Minimalabstand 4 sein soll, so muß jede Zeile von A mindestens 3 Einsen haben. Ebenso muß jede Summe von zwei Zeilen von A mindestens zwei Einsen haben, d.h. die Nullen in verschiedenen Zeilen von A müssen an verschiedenen Stellen stehen. So kommt man nach geeigneter Permutation der Spalten zwangsläufig auf die obige Matrix. □

Reed-Muller-Codes

Hier ist der Körper gleich $\mathbb{F}_2$. Es seien natürliche Zahlen $r \geq 0$, $m \geq 1$ fixiert. Mit F_m bezeichnen wir den Vektorraum aller Funktionen $\mathbb{F}_2^m \to \mathbb{F}_2$, und mit $F_{m,r} \subset F_m$ der Unterraum aller Funktionen, die durch Polynome vom Grad $\leq r$ dargestellt werden. Wir wollen $F_{m,r}$ als Code interpretieren und müssen dazu F_m mit $\mathbb{F}_2^{2m}$ identifizieren, also Koordinaten einführen. Dazu werden die Vektoren von $\mathbb{F}_2^m$ in folgender Form fest durchnummeriert:

$$\begin{aligned} v_0 &= 000\ldots \\ v_1 &= 100\ldots \\ v_2 &= 010\ldots \\ v_3 &= 110\ldots \end{aligned}$$

also lexikographisch „von hinten“. Mit anderen Worten Wenn $j = \sum \varepsilon_i 2^i$ ist , so ist

$$v_j = \varepsilon_0\varepsilon_1\ldots\varepsilon_{m-1}$$

(umgedrehte Binäredarstellung von j). Einer Funktion $f \in F_m$ wird nun der Vektor ihrer Funktionswerte zugeordnet:

$$f \mapsto \underline{f} = (f(v_0), f(v_1), \ldots, f(v_{n-1}))\,.$$

Beispiel: Die Koordinatenfunktion $z_i(x_1, x_2, \ldots, x_m) = x_i$.

$$m = 3 \qquad \begin{aligned} \underline{z_1} &= 01010101 \\ \underline{z_2} &= 00110011 \\ \underline{z_3} &= 00001111 \end{aligned}$$

Definition 2.2.7 $\mathcal{R}(r,m) = \{\underline{f} \mid f \in F_{m,r}\}$ heißt *Reed-Muller-Code* der Ordnung r und Länge 2^m.

Proposition 2.2.8 *$\mathcal{R}(r,m)$ hat die Dimension*

$$1+\binom{m}{1}+\binom{m}{2}+\ldots+\binom{m}{r}$$

und den Minimalabstand 2^{m-r}.

Beweis: (0) Wir bemerken vorweg, dass die Abbildung $f \in F_m$ als charakteristische Funktionen von Teilmengen $M \subset \mathbb{F}_2^m$ gedeutet werden können:

$$\begin{array}{lcll} f & \mapsto & M_f & = \{v \mid f(v)=1\} \\ f_M & \leftarrow & M & \\ f_M(v) & & = & \begin{cases} 0 & \text{für} \quad v \notin M \\ 1 & \text{für} \quad v \in M \end{cases} . \end{array}$$

Der Hamming-Norm entspricht dabei die Kardinalität:

$$\|\underline{f}_M\| = |M| \ , \quad M \subseteq \mathbb{F}_2^m \, .$$

(1) Alle Abbildungen $f \in F_m$ sind Polynomfunktionen. Beweis durch Induktion nach m: Sei $f = f_M$ gegeben, schreibe

$$\begin{aligned} & M = M_0 \dot\cup (e_m + M_1) \, , \\ & M_0, M_1 \subseteq F_2^{m-1} \times \{0\} \subset \mathbb{F}_2^m \, , \\ & e_m = 00\ldots01 \, . \end{aligned}$$

Es ist $f_M = f_{M_0} + f_{(e_m+M_1)}$

$$(*) \qquad = p_0(z_0,\ldots,z_{m-1})(1+z_m) + p_1(z_0,\ldots,z_{m-1})z_m \, ,$$

wobei p_0, p_1 Polynome sind, die nach Induktionsvoraussetzung $f|_{\mathbb{F}_2^{m-1}}$ bzw. die Funktion $v \mapsto f(v+e_m)$, $v \in \mathbb{F}_2^{m-1}$ darstellen. Also wird f_M selbst durch ein Polynom dargestellt.

(2) Zur Berechnung des Minimalabstandes verwenden wir wieder Induktion nach m und die Formel $(*)$ für $f = f_M \in F_r$. Wenn wir p_0, p_1 als Funktionen auf $\mathbb{F}_2^{m-1}$ auffassen, so ist

$$\underline{f} = (\underline{p_0}, \underline{p_0}) * (\underbrace{11\ldots1}_{2^{m-1}}\underbrace{00\ldots0}_{2^{m-1}}) + (\underline{p_1}, \underline{p_1}) * (00\ldots011\ldots1) \, ,$$

wobei $(\underline{a}, \underline{b})$ dem Vektor aus zwei Blöcken $\underline{a}, \underline{b}$ bezeichnet und $*$ die komponentenweise Multiplikation. Also ist $\|\underline{f}\| = \|\underline{p_0}\| + \|\underline{p_1}\|$. Es ist $\operatorname{grad} p_0 \leq r$ und $\operatorname{grad}(p_0+p_1) \leq r-1$, also auch $\operatorname{grad} p_1 \leq r$. Mittels der Induktionsannahme folgt $\|\underline{f}\| \geq 2 \cdot 2^{(m-1)-r} = 2^{m-r}$, wie gewünscht.

Eine Funktion der Gestalt $z_{j_1} \dots z_{j_r}$ hat als charakteristische Funktion des linearen Teilraumes $z_{j_1} = \ldots = z_{j_r} = 1$ die Norm 2^{m-r}, nach (0). Also ist 2^{m-r} der genaue Minimalabstand.

(3) Wegen $z_i^2 = z_i$ werden Polynomfunktionen und damit alle Funktionen linear erzeugt von den Funktionen

$$z_{j_1} \dots z_{j_s},\ 1 \leq j_1 < j_2 < \ldots < j_s \leq m,\ s = 1, 2, \dots$$

Hiervon gibt es $1 + m + \binom{m}{2} + \ldots + \binom{m}{m-1} + 1 = 2^m$ Stück. Dieses ist die Dimension des Vektorraumes aller Funktionen $\mathbb{F}_2^m \to \mathbb{F}_2$. Also müssen die genannten Funktionen linear unabhängig sein, und die Formel für die Dimension von $\mathcal{R}(r, m)$ ist klar. □

Beispiel 2.2.9 (1) Der Reed-Muller Code $\mathcal{R}(3, 1)$ ist der eindeutig bestimmte (siehe 2.2.6) $[8, 4, 4]$-Code.

(2) Der Reed-Muller Code $\mathcal{R}(4, 1)$ ist ein $[16, 5, 8]$-Code. Er wird später für die Konstruktion des 16-dimensionalen Barnes-Wall-Gitters benutzt.

Ohne Beweis notieren wir noch, wie der duale Code eines Reed-Muller Codes aussieht:

Satz 2.2.10 *Der duale Code eines Reed-Muller Codes ist wieder ein Reed-Muller Code. Genauer ist $\mathcal{R}(r, m)^\perp$ äquivalent zu $\mathcal{R}(m - 1 - r, m)$.*

Man beachte, dass die Dimensionen von $\mathcal{R}(r, m)$ und $\mathcal{R}(m - 1 - r, m)$ sich jedenfalls zur Blocklänge 2^m aufaddieren, wie es für zueiander duale Codes sein muss. Man kann den dualen Code leicht bestimmen, wenn man $\mathcal{R}(r, m)$ mittels der sogenannten $(u, u + v)$-Konstruktion oder Plotkin-Konstruktion induktiv aus $\mathcal{R}(r, m - 1)$ $\mathcal{R}(r - 1, m - 1)$ konstruiert.

Literaturhinweise zu 2.1 und 2.2. Gut zu dieser Vorlesung passen die folgenden stark algebraisch orientierten Lerhbücher:

Werner Lütkebohmert: *Codierungstheorie*, Vieweg-Verlag 2003

Wolfgang Willems: *Codierungstheorie*, Verlag de Gruyter 1999

Außerdem ist folgender etwas knapper geschriebene Klassiker zu nennen (lange Zeit das Buch zur algebraischen Codierungstheorie):

J.H. van Lint: *Introduction to Coding Theory*, Springer-Verlag, Graduate Texts in Mathematics, 3. Auflage 1999.