5 Lineare Codes

5.1 Grundbegriffe

Von nun an ist q stets eine Primzahlpotenz. Wir betrachten den (bis auf Isomorphie eindeutigen) Körper $GF(q)$ mit q Elementen. Das Alphabet ist stets $GF(q)$.

Definition. Ein *linearer Code* C ist ein Unterraum des Vektorraumes $GF(q)^n$. C ist ein $[n, k, d; q]$-Code, falls

$$\begin{aligned} C &\subseteq GF(q)^n,\ n = \text{Länge} \\ \dim C &= k,\ \text{also } |C| = q^k\,, \\ d(C) &\geq d\,. \end{aligned}$$

Sei $c = (c_1, \ldots, c_n) \in GF(q)^n$, dann ist wie bisher $w(c) = \#\{i : c_i \neq 0\}$ das *Gewicht* von c. Sind u, v Codewörter des linearen Codes C, so gilt $\Delta(u, v) = w(u - v)$, wobei $u - v \in C$ ist. Somit haben wir für lineare Codes C

$$d(C) = \min_{0 \neq v \in C} w(v)\,.$$

Lineare Codes sind die Codes, die in der Praxis verwendet werden. Sie können mit Hilfe einer Generatormatrix bzw. Kontrollmatrix bequem dargestellt werden.

Definition. G heißt *Generatormatrix* des $[n, k, d; q]$-Codes C, falls die Zeilen $c_1, \ldots, c_k$ von G eine Basis von C sind, also

$$G = \begin{bmatrix} \ldots & c_1 & \ldots \\ \ldots & c_2 & \ldots \\ & \vdots & \\ \ldots & c_k & \ldots \end{bmatrix},$$

G ist $k \times n$-Matrix. Es gilt somit

$$c \in C \Longleftrightarrow c = \lambda_1 c_1 + \ldots + \lambda_k c_k,\ \lambda_i \in GF(q)\,.$$

Bemerkung. Ist B invertible $k \times k$-Matrix, so ist BG ebenfalls Generatormatrix, da $b_i G \in C$ ist für alle Zeilen $b_1, \ldots, b_k$ von B, und $rk(BG) = r(G) = k$

ist.

Definition. Ist C $[n,k,d;q]$-Code, so heißt der orthogonale Unterraum $C^\perp$ der zu C *duale Code*. Es ist also

$$v \in C^\perp \Longleftrightarrow v \cdot u = 0 \text{ für alle } u \in C\,.$$

wobei $v \cdot u = \sum_{i=1}^{n} v_i u_i$ das übliche innere Produkt ist. Wir haben $\dim C^\perp = n-k$.

Wegen der Linearität ist

$$v \in C^\perp \Longleftrightarrow v \cdot c_i = 0 \text{ für } \{c_1,\ldots,c_k\} \text{ Basis von } C\,,$$

das heißt

$$v \in C^\perp \Longleftrightarrow Gv^T = 0\,.$$

Definition. H heißt *Kontrollmatrix* von C, falls H Generatormatrix von $C^\perp$ ist. H ist also eine $(n-k)\times n$-Matrix mit

$$c \in C \Longleftrightarrow Hc^T = 0\,.$$

Beispiel. Der Wiederholungscode ist linearer Code in $GF(q)^n$ mit Dimension $= 1$ und Generatormatrix $G = (1\,1\ldots1)$. Sei $q = 2$, dann ist

$$H = \begin{bmatrix} 1\,1\,0 & \ldots & 0 \\ 1\,0\,1\,0 & \ldots & 0 \\ \vdots & \ldots & \\ 1\,0\,0 & \ldots & 1 \end{bmatrix}$$

Kontrollmatrix, $rk(H) = n-1$, des Wiederholungscodes.

Satz 22. *Sei $G = [I_k|A]$ Generatormatrix des $[n,k,d;q]$-Codes, wobei I_k die Einheitsmatrix der Ordnung k ist und A eine $k\times(n-k)$-Matrix. Dann ist $H = [-A^T|I_{n-k}]$ eine Kontrollmatrix von C.*

Beweis. Wir müssen $GH^T = 0$ zeigen. Wir haben

$$GH^T = [I_k|A]\begin{bmatrix} -A \\ \hline I_{n-k} \end{bmatrix} = -A + A = 0\,.$$

Satz 23. *Sei C ein $[n, k, d; q]$-Code und H eine Kontrollmatrix von C. Dann gilt*

$$d(C) \geq d \Longleftrightarrow \text{ je } d-1 \text{ Spalten von } H \text{ sind linear unabhängig.}$$

Beweis. Es seien $u_1, u_2, \ldots, u_n$ die Spalten von H. Für ein Codewort $c = (c_1, \ldots, c_n) \in C$ gilt $Hc^T = 0$, das heißt

$$c_1 u_1 + \ldots + c_n u_n = 0\,.$$

Angenommen, $w(c) = m \leq d-1$ mit $c_{i_1} \neq 0, \ldots, c_{i_m} \neq 0$. Dann ist

$$c_{i_1} u_{i_1} + \ldots + c_{i_m} u_{i_m} = 0\,,$$

und die $m \leq d-1$ Spalten $u_{i_1}, \ldots, u_{i_m}$ sind linear abhängig. Nehmen wir umgekehrt an, dass $u_{j_1}, \ldots, u_{j_m}$ linear abhängig sind mit $m \leq d-1$. Dann gibt es $c_{j_1}, \ldots, c_{j_m}$, nicht alle $= 0$, mit

$$c_{j_1} u_{j_1} + \ldots + c_{j_m} u_{j_m} = 0\,,$$

und wir erhalten ein Codewort $c = (0 \ldots c_{j_1}, \ldots, c_{j_m}, \ldots 0) \in C$ mit Gewicht $m \leq d-1$. Die Kontraposition ergibt die Aussage des Satzes. □

Beispiel. Der Satz gibt eine konkrete Methode an, um Codes mit vorgegebener Distanz zu konstruieren. Der erste interessante Fall ist $d = 3$. Um $[n, k, 3; q]$-Codes zu erhalten, benötigen wir eine Kontrollmatrix mit $r = n-k$ Zeilen und n Spalten, so dass je zwei Spalten linear unabhängig sind. Jede Spalte ist ein Vektor $\neq 0$ aus $GF(q)^r$. Ist $u \neq 0$ ein solcher Vektor, so sind genau die Vielfachen λu linear abhängig. Die Maximalzahl der Spalten in $GF(q)^r$, von denen je zwei linear unabhängig sind, ist demnach

$$n = \frac{q^r - 1}{q - 1}\,.$$

Definition. Ein Hamming Code $H_{r;q}$ über $GF(q)$ ist $[n, k, 3; q]$-Code mit einer Kontrollmatrix wie eben konstruiert:

$$n = \frac{q^r - 1}{q - 1},\ k = \frac{q^r - 1}{q - 1} - r, \quad (r \geq 2).$$

Satz 24. *Jeder Hamming Code $H_{r;q}$ über $GF(q)$ ist 1-perfekt.*

Beweis. Die Hamming Schranke für $d(C) = 3$ ist

$$|C| \leq \frac{q^n}{1 + n(q-1)}\,.$$

Für $H_{r;q}$ haben wir wegen $n = \frac{q^r-1}{q-1}$

$$\left|H_{r;q}\right| = q^k = \frac{q^n}{q^r} = \frac{q^n}{1 + n(q-1)}\,,$$

als ist $H_{r;q}$ 1-perfekt. □

Beispiel. Sei $q = 2$. Für $r = 2$ erhalten wir $n = 3$, $k = 1$, also den Wiederholungscode $C = \{000, 111\}$ mit Kontrollmatrix $H = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$. Für $r = 3$ ist die Kontrollmatrix

$$H = \left[\begin{array}{ccc|cccc} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array}\right]$$

und nach obigem Satz

$$G = \left[\begin{array}{ccc|cccc} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right]$$

eine Generatormatrix. Der so erhaltene Hamming Cod $H_{3;2}$ ist natürlich genau der im vorigen Kapitel konstruierte Fano Code.

Bemerkungen. Die folgenden Operationen erhalten die Linearität von Codes:

1. Permutation der Spalten (die Parameter n, k, d bleiben erhalten),
2. Multiplikation einer Spalte mit einem Element $\neq 0$ (die Parameter bleiben erhalten),
3. Verkürzung.

5.2 Schranken für lineare Codes

Gegeben n, d und eine Primzahlpotenz q, so setzen wir

$$A_q(n,d) = \max(|C| : C \subseteq GF(q)^n \text{ linear mit } d(C) \geq d).$$

Es gilt also stets $A_q(n,d) \leq M_q(n,d)$.

Beispiel. Wir wissen $M_2(12,6) = 24$ (da eine Hadamard Matrix der Ordnung 12 existiert), aber natürlich ist $A_2(12,6) < 24$, da $A_2(n,d)$ eine 2-Potenz sein muß. Allgemein ist $A_q(n,d) = q^k$, wobei k die Dimension eines optimalen Codes ist.

Satz 25 (Singleton Schranke)**.** *Wenn ein $[n,k,d;q]$-Code C existiert, so gilt $k \leq n-d+1$. Ist Gleichheit erfüllt, so heißt C linearer* MDS-Code.

Beweis. Wir wissen $M_q(n,d) \leq q^{n-d+1}$ und somit $|C| = q^k \leq q^{n-d+1}$, also $k \leq n-d+1$. Ein zweiter Beweis folgt aus Satz 23. Die Kontrollmatrix H ist eine $(n-k) \times n$-Matrix, in der je $d-1$ Spalten linear unabhängig sind, das heißt $rk(H) \geq d-1$. Da $rk(H)$ höchstens die Anzahl der Zeilen sein kann, folgt $d-1 \leq n-k$. □

Wir können diese Schranke folgendermaßen verschärfen. In $A_q(n,d)$ geben wir n und d vor und suchen das *maximale* k, so dass ein $[n,k,d;q]$-Code existiert. Alternativ geben wir k und d vor und suchen das *minimale* n, so dass ein $[n,k,d;q]$-Code existiert. Es sei $N_q(k,d)$ diese minimale Länge n.

Lemma 2. *Es gilt $N_q(1,d) = d$ und*

$$N_q(k,d) \geq d + N(k-1, \lceil \frac{d}{q} \rceil) \quad (k \geq 2).$$

Beweis. Der Wiederholungscode der Länge d gibt $N_q(1,d) = d$. Es sei C ein $[N_q(k,d), k, d; q]$-Code mit der Generatormatrix G. Aus der Minimalität von $N_q(k,d)$ folgt, dass es ein Codewort vom Gewicht d gibt, da wir ansonsten den Code verkürzen könnten. Nach den Bemerkungen am Ende des vorigen

Abschnittes können wir G von der Form

$$G = \left(\begin{array}{c|c} 0 \ \ldots \ 0 & \overbrace{1 \ \ldots \ 1}^{d} \\ \hline G_1 & G_2 \end{array}\right)$$

annehmen. Es seien $c_1, c_2, \ldots, c_k$ die Zeilen von G. Wir setzen $c_i = (u_i|v_i)$, wobei u_i das Wort in G_1 und v_i in G_2 ist. □

Behauptung. $rk(G_1) = k - 1$.

Angenommen, dies ist falsch, dann sind die Zeilen $u_2, \ldots, u_k$ von G_1 linear abhängig, das heißt $\lambda_2 u_2 + \cdots + \lambda_k u_k = 0$, nicht alle $\lambda_i = 0$. Daraus folgt $c = \lambda_2 c_2 + \cdots + \lambda_k c_k = (0 \ldots 0, y_1 \ldots y_d) \in C$, $c \neq 0$ (da die c_i linear unabhängig sind). Wegen $d(C) = d$ sind alle $y_i \neq 0$ und nicht alle gleich einem festen y, da ansonsten $c = yc_1$ wäre. Es sei $y_1 \neq y_2$, dann ist $c' = c - y_1 c_1 \in C$, $c' \neq 0$ und $w(c') < d$, im Widerspruch zu $d(C) = d$.

Die Matrix G_1 erzeugt also einen $[N_q(k,d) - d, k-1, d_1; q]$-Code C_1 mit $d(C_1) = d_1$. Es sei $u = \lambda_2 u_2 + \cdots + \lambda_k u_k \in C$ von minimalem Gewicht d_1, und $c = (u|v) = \lambda_2 c_2 + \cdots + \lambda_k c_k$. Jedes Wort $yc_1 = (0 \ldots 0 \ y \ldots y) \in C$ hat Abstand $\geq d$ von c, das heißt $\Delta((y \ldots y), v) \geq d - d_1$. Mit anderen Worten jedes $y \in GF(q)$ kommt in v höchstens d_1 Mal vor. Da v Länge d hat, folgt $d \leq qd_1$ oder $d_1 \geq \frac{d}{q}$, das heißt $d_1 \geq \lceil \frac{d}{q} \rceil$. Aus der Definition von $N_q(k,d)$ erhalten wir somit

$$N_q(k-1, \lceil \frac{d}{q} \rceil) \leq N_q(k-1, d_1) \leq N_q(k,d) - d\,. \qquad \square$$

Iteration zusammen mit $\lceil \frac{1}{q} \lceil \frac{d}{q^{i-1}} \rceil \rceil \geq \lceil \frac{d}{q^i} \rceil$ liefert die folgende Schranke.

Satz 26 (Griesmer Schranke)**.** *Wir haben*

$$N_q(k,d) \geq d + \lceil \frac{d}{q} \rceil + \lceil \frac{d}{q^2} \rceil + \cdots + \lceil \frac{d}{q^{k-1}} \rceil\,.$$

Beispiel. Sei $n = 16$, $d = 8$, $q = 2$. Die Singleton Schranke ergibt $k \leq 16 - 8 + 1 = 9$, während Griesmer besagt

$$16 = 8 + \lceil \frac{8}{2} \rceil + \lceil \frac{8}{2^2} \rceil + \lceil \frac{8}{2^3} \rceil + \lceil \frac{8}{2^4} \rceil.$$

also ist ein $[16, 5, 8; 2]$-Code möglich, aber $k = 6$ nicht mehr. Wir wissen $M_2(16, 8) = 32 = 2^5$ mit der Hadamard Konstruktion, aber die Hadamard Codes sind nicht linear. Die folgende Konstruktion ergibt einen $[16, 5, 8; 2]$-Code, also $A_2(16, 8) = 32$.

Es seien $C_1, C_2 \subseteq \{0, 1\}^n$, $|C_1| = M_1$, $|C_2| = M_2$ beliebige Codes mit $d(C_1) = d_1$, $d(C_2) = d_2$. Wir definieren den Code $C = C_1 * C_2$ durch $\{(u, u + v) : u \in C_1, v \in C_2\}$. C ist ein Code der Länge n, und es gilt

a. $|C| = |C_1||C_2|$,

b. $d(C) = \min(2d_1, d_2)$.

Ferner ist C linear, falls C_1 und C_2 linear sind.

Die Reed-Muller Codes $C(r, m)$ werden rekursiv definiert. Es ist $C(0, m) = \{00 \ldots 0, 11 \ldots 1\}^{2^m}$, $C(m, m) = \{0, 1\}^{2^m}$ und für $0 \leq r \leq m$ ist

$$C(r + 1, m + 1) = C(r + 1, m) * C(r, m).$$

Man prüft leicht nach, dass $C(r, m)$ linearer Code ist mit Länge $n = 2^m$, Dimension $k = \sum_{i=0}^{r} \binom{m}{i}$ und Distanz 2^{m-r}.

Für $m = 4$, $r = 1$ ist $C(4, 1)$ ein $[16, 5, 8; 2]$-Code.

Beispiel. $n = 12$, $d = 5$, $q = 2$. Die Griesmer Schranke ergibt $12 = 5 + \lceil \frac{5}{2} \rceil + \lceil \frac{5}{2^2} \rceil + \lceil \frac{5}{2^3} \rceil + \lceil \frac{5}{2^4} \rceil$, also $k \leq 5$. Die Plotkin Schranke für beliebige Codes war $M_2(12, 5) \leq 48$. Nach Griesmer ist theoretisch ein $[12, k = 5, d = 5; 2]$-Code C mit $|C| = 32$ möglich, aber es kann gezeigt werden, dass $A_2(12, 5) = 16$ ist, während $M_2(12, 5) = 32$ ist.

Auch die untere Schranke läßt sich auf lineare Codes übertragen. Die Gilbert-Varshamov Schranke besagte

$$M_q(n, d) \geq \frac{q^n}{\sum_{i=0}^{d-1} \binom{n}{i} (q - 1)^i}.$$

Wenn also

$$\frac{q^n}{\sum_{i=0}^{d-1}\binom{n}{i}(q-1)^i} \geq q^k$$

oder äquivalent

$$\sum_{i=0}^{d-1}\binom{n}{i}(q-1)^i \leq q^{n-k}$$

gilt, so existiert ein (n,d,q)-Code C mit $|C| = q^k$. Eine geringfügige Abschwächung reicht schon für die Existenz eines *linearen* Codes aus.

Satz 27 (Gilbert-Varshamov Schranke für lineare Codes)**.** *Wenn*

$$\sum_{i=0}^{d-2}\binom{n-1}{i}(q-1)^i < q^{n-k}$$

gilt, so existiert ein $[n,k,d;q]$*-Code* $C \quad (d \geq 2)$*.*

Beweis. Wir müssen eine $(n-k)\times n$-Matrix konstruieren, so dass je $d-1$ Spalten linear unabhängig sind. Wir beginnen mit einem beliebigen Vektor $u_1 \neq 0$ aus $GF(q)^{n-k}$ als erster Spalte. Angenommen wir haben bereits $m < n$ Spalten $u_1,\ldots,u_m$ konstruiert, so dass je $d-1$ linear unabhängig sind. Nicht in Frage als nächste Spalte kommen (klassifiziert nach der Länge der Linearkombination)

$$1 + m(q-1) + \binom{m}{2}(q-1)^2 + \ldots + \binom{m}{d-2}(q-1)^{d-2}\,.$$

Wegen $m < n$ ist $m \leq n-1$, also ist diese Summe kleiner als q^{n-k} nach Voraussetzung und es existiert ein Vektor $v = u_{m+1} \in GF(q)^{n-k}$, den wir hinzufügen können. □

Beispiel. $n = 13$, $d = 5$, $q = 2$. Wir haben

$$\sum_{i=0}^{3}\binom{12}{i} = 1 + 12 + 66 + 220 = 299 < 2^9 = 2^{13-4}\,.$$

Somit existiert ein $[13,4,5;2]$-Code, $A_2(13,5) \geq 16$.

5.3 Codierung und Decodierung von linearen Codes

Sei $C \subseteq GF(q)^n$ linearer Code der Dimension k und

$$G = \begin{pmatrix} \dots & c_1 & \dots \\ \dots & c_2 & \dots \\ & \vdots & \\ \dots & c_k & \dots \end{pmatrix}$$

eine $k \times n$-Generatormatrix, also $C = \{\lambda_1 c_1 + \ldots + \lambda_k c_k : \lambda_i \in GF(q)\}$.

Wir fassen die Nachrichten als Wörter der Länge k aus $GF(q)^k$, $u = (\lambda_1, \ldots, \lambda_k)$, auf.

Die Codierung ist $u \xrightarrow{\varphi} uG$

$$u \longrightarrow \lambda_1 c_1 + \ldots + \lambda_k c_k \in C\,.$$

In der Praxis wird der Nachrichtenstrom in Blöcke der Länge k zerlegt

$$x = \underbrace{x_1 \ldots x_k}_{x^{(1)}} \big| \underbrace{x_{k+1} \ldots x_{2k}}_{x^{(2)}} \big| \underbrace{x_{2k+1} \ldots x_{3k}}_{x^{(3)}} \big| \ldots$$

und in entsprechende Codewörter der Länge n

$$x \xrightarrow{\varphi} x^{(1)}G \big| x^{(2)}G \big| x^{(3)}G \big| \ldots$$

codiert. Die Rate ist $\frac{k \log q}{n}$.

Der wichtigste Fall ist, wenn G von der Form $G = [I_k|A]$ ist. Wir haben dann

$$u \xrightarrow{\varphi} uG = (\underbrace{u}_{k}, \underbrace{uA}_{r=n-k}).$$

Die ersten k Symbole sind die Informationssymbole, die restlichen $r = n - k$ die Kontrollsymbole, r heißt die *Redundanz*. Man spricht dann von einer *systematischen Codierung*.

Beispiel. Der Paritätscode über $GF(2)$ hat die Generatormatrix

$$G = \left(\begin{array}{ccccc|c} 1 & & & & & 1 \\ & & & 0 & & 1 \\ & 1 & & & & \vdots \\ & & \ddots & & & \\ 0 & & & & 1 & 1 \end{array}\right)$$

mit der Codierung

$$u = (\lambda_1, \ldots, \lambda_k) \xrightarrow{\varphi} (\lambda_1, \ldots, \lambda_k, \sum_{i=1}^{k} \lambda_i)\,.$$

Nun zur Decodierung. Wir verwenden die Hamming Decodierung: Wird $y \in GF(q)^n$ empfangen, so decodiere y zu einem Codewort c mit minimalem Abstand von y, das heißt Gewicht $w(y-c) = \min$. Die möglichen *Fehlerwörter* $e = y - c$, $c \in C$, ergeben die Nebenklasse $y - C$ der Untergruppe C_+ in $GF(q)^n_+$. Hat C Dimension k, so gibt es q^{n-k} Nebenklassen.

Praxis I. Stelle eine Liste der Nebenklassen von C zusammen mit einer Liste der Wörter von minimalem Gewicht aus den jeweiligen Nebenklassen. Falls mehrere existieren, wähle eines. Diese Wörter heißen die *Nebenklassenführer*.

Nebenklassen	Nebenklassenführer	
C	0	
$y - C$	e	$w(e) = \min$ in $y - C$
$z - C$	f	$w(f) = \min$ in $z - C$
$v - C$	g	$w(g) = \min$ in $v - C$
$\vdots$	$\vdots$	

Algorithmus: Es wird y empfangen.

1. Man sieht nach, in welcher Nebenklasse y liegt.

2. Decodiere $y \xrightarrow{\psi} y - e$, e Nebenklassenführer in der Nebenklasse $y - C$.

Zur praktischen Durchführung des Algorithmus verwendet man eine Kontrollmatrix.

Hilfssatz. *Sei H Kontrollmatrix von C. Dann liegen y_1, y_2 genau dann in derselben Nebenklasse von C, wenn $Hy_1^T = Hy_2^T$ gilt.*

Beweis. Die Wörter y_1, y_2 liegen genau dann in derselben Nebenklasse, wenn

$$y_1 - y_2 = c \in C \Leftrightarrow H(y_1^T - y_2^T) = 0 \Leftrightarrow Hy_1^T = Hy_2^T. \qquad \square$$

Es genügt also, Hy^T zu berechnen. Wird y empfangen, so heißt Hy^T das *Syndrom* von y. Es gibt q^{n-k} Syndrome.

Praxis II. Stelle eine Liste der Syndrome auf, zusammen mit den jeweiligen Nebenklassenführern.

$$\begin{array}{ll} \text{Syndrome} & \text{Nebenklassenführer} \\ n-k \left\{ \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \right. & \underbrace{0\,0\,\ldots\,0}_{n} \\ n-k \left\{ \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \right. & e \text{ mit } He^T = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix},\ w(e) = \min \\ \vdots & \vdots \end{array}$$

Algorithmus: Es werde y empfangen.

1. Berechne das Syndrom Hy^T, mit Nebenklassenführer e,
2. Decodiere $y \xrightarrow{\psi} y - e$.

Beispiel. $q = 2$. $H = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$, $n = 4$, $k = 2$.

Syndrome	Nebenklassenführer
$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$	0 0 0 0
$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$	1 0 0 0
$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$	0 1 0 0
$\begin{pmatrix} 1 \\ 1 \end{pmatrix}$	0 0 0 1

Angenommen, es wird $y = 1111$ empfangen. Dann ist $Hy^T = \binom{1}{0}$, also wird y zu $y - 1000 = 0111 \in C$ decodiert. Wir hätten auch 0010 als Nebenklassenführer mit Syndrom $\binom{1}{0}$ wählen können. Man sieht also, dass C einen Fehler erkennen kann, aber im allgemeinen nicht korrigieren.

Allgemein erkennen wir, dass t-fehlerkorrigierend bedeutet, dass die Wörter vom Gewicht $\leq t$ verschiedene Syndrome haben müssen, also Nebenklassenführer *verschiedener* Nebenklassen sind. Da es q^{n-k} Syndrome gibt, folgt daraus sofort die Hamming Schranke $\sum_{i=0}^{t} \binom{n}{i}(q-1)^i \leq q^{n-k}$.

Beispiel. Betrachten wir den 1-perfekten Hamming Code $H_{3;2}$ mit $n = 7$, $k = 3$, $q = 2$ und Kontrollmatrix

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

Zu jedem Syndrom $s \in GF(2)^3$ gehört genau ein Nebenklassenführer vom Gewicht ≤ 1. Zu $s_0 = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ gehört 0000000 und zu $s_j = j$-te Spalte von H offenbar $0\,0\,\ldots\,1\,0\ldots0$ mit 1 an j-ter Stelle. Wir haben somit den Algorithmus:

1. Berechne $Hy^T = s_j$.
2. Ist $j = 0$, so ist $y \in H_{3;2}$,

   ist $j > 0$, so decodiere y zu $y + (00.\overset{j}{\overset{\downarrow}{1}}.0)$.

Wird zum Beispiel $y = 1110011$ empfangen, so ist $Hy^T = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$ (6.Spalte) und $y \xrightarrow{\psi}$ 1110001.

5.4 Gewichtsverteilung und der Satz von MacWilliams

Ist $C \subseteq A^n$ ein beliebiger Code über dem Alphabet A, so interessieren wir uns für die Gewichtsverteilung der Codewörter:

$$A_i = \#\{c \in C : w(c) = i\}, \quad i = 0, 1, \ldots, n\,.$$

Ist insbesondere $C \subseteq GF(q)^n$ linear, so ist $d(C) = \min(i > 0 : A_i \neq 0)$.

Definition. Das Polynom $W_C(x, y) = \sum_{i=0}^{n} A_i x^{n-i} y^i$ ist das (homogene) *Gewichtspolynom* von C.

Beispiel. Der Hamming Code $H_{3;2}$ hat

$$W_{H_{3;2}}(x, y) = x^7 + 7x^4y^3 + 7x^3y^4 + y^7\,,$$

und der Code $\overline{H}_{3;2}$ (mit Paritätscheck)

$$W_{\overline{H}_{3;2}}(x, y) = x^8 + 14x^4y^4 + y^8\,.$$

Ein wichtiger Satz stellt eine Verbindung zwischen den Gewichtspolynomen von C und $C^\perp$ her. Dazu benötigen wir einige Vorbereitungen.

Sei G eine endliche abelsche Gruppe, additiv geschrieben, und S^1 die multiplikative Gruppe der komplexen Zahlen vom Betrag 1, also $S^1 = \{e^{ix} : 0 \leq x \leq 2\pi\}$ mit $e^{ix} \cdot e^{iy} = e^{i(x+y)}$.

Definition. Ein *Charakter* χ von G ist ein Homomorphismus $\chi : (G, +) \longrightarrow (S^1, \cdot)$, also $\chi(0) = 1$, $\chi(g + h) = \chi(g)\chi(h)$.

Der Charakter χ_0, der alles auf 1 abbildet, heißt der *triviale* Charakter. Die Charaktere bilden mit Multiplikation $(\chi\chi')(g) = \chi(g)\chi'(g)$ eine Gruppe, mit χ_0 als neutralem Element.

Es sei $|G| = n$, dann gilt $ng = 0$ für alle $g \in G$, und somit $\chi(ng) = \chi(g)^n = 1$ für alle g. Die Bilder unter χ sind also n-te *Einheitswurzeln*, das heißt Nullstellen der Gleichung $x^n = 1$. Die Gruppe G der Charaktere ist somit endlich.

Lemma 3. *Sei χ Charakter von G. Dann gilt*

$$\sum_{g\in G}\chi(g) = \begin{cases} |G| & \chi = \chi_0 \\ 0 & \chi \neq \chi_0\,. \end{cases}$$

Beweis. Für $\chi = \chi_0$ ist $\chi_0(g) = 1$ für alle $g \in G$, und somit $\sum_{g\in G}\chi(g) = |G|$. Sei nun $\chi \neq \chi_0$, z.B. $\chi(h) \neq 1$. Dann ist

$$\chi(h)\sum_{g\in G}\chi(g) = \sum_{g\in G}\chi(h)\chi(g) = \sum_{g\in G}\chi(h+g) = \sum_{g\in G}\chi(g),$$

da $h+g$ mit g wieder ganz G durchläuft. Wegen $\chi(h) \neq 1$, folgt $\sum_{g\in G}\chi(g) = 0$. $\square$

Frage. Existiert immer ein nichttrivialer Charakter, sofern $|G| \geq 2$ ist. Die Antwort ist ja, die Gruppe der Charaktere ist stets isomorph zu G.

Für den uns interessierenden Fall $G = GF(q)_+$ können wir das direkt sehen. Es sei $q = p^m$, dann ist $GF(q)$ ein Vektorraum der Dimension m über dem Primkörper $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$. Sei $\{1, \alpha_2, \alpha_3, \ldots, \alpha_m\}$ eine Basis. Für $\alpha = \lambda_1 \cdot 1 + \lambda_2\alpha_2 + \cdots + \lambda_m\alpha_m$, $\lambda_i \in \mathbb{Z}_p$, definieren wir

$$\chi(\alpha) = \zeta^{\lambda_1}, \quad \zeta = e^{\frac{2\pi i}{p}} \text{ primitive } p\text{-te Einheitswurzel.}$$

Wegen $\chi(\alpha+\beta) = \zeta^{\lambda_1+\mu_1} = \zeta^{\lambda_1}\zeta^{\mu_1} = \chi(\alpha)\chi(\beta)$ und $\chi(1) = \zeta \neq 1$ ist χ ein nichttrivialer Charakter.

Beispiel. $GF(4) = \{0, 1, \alpha, 1+\alpha\}$. Der oben konstruierte Charakter ist

$$\chi: \begin{array}{rcl} 0 & \longrightarrow & 1 \\ 1 & \longrightarrow & -1 \\ \alpha & \longrightarrow & 1 \\ 1+\alpha & \longrightarrow & -1 \end{array}$$

Als zweite Vorbereitung benötigen wir eine Summenumkehrformel. Sei χ ein nichttrivialer Charakter von $K_+ = GF(q)_+$ und $f : K^n \longrightarrow I$ eine beliebige Abbildung von K^n in einen Integritätsbereich.

Definition. Die *Hadamard Transformierte* von f ist $\widehat{f} : K^n \longrightarrow I$ mit

$$\widehat{f}(u) = \sum_{v\in K^n}\chi(u\cdot v)f(v) \quad (u \in K^n)\,,$$

wobei $u \cdot v = \sum_{i=1}^{n} u_i v_i$ das Skalarprodukt in K^n ist, und χ ein fester nichttrivialer Charakter von $GF(q)_+$.

Lemma 4. *Sei $C \subseteq K^n$ ein linearer Code, $f : K^n \longrightarrow I$, dann gilt*

$$\sum_{v \in C^\perp} f(v) = \frac{1}{|C|} \sum_{u \in C} \widehat{f}(u)\,.$$

Beweis. Wir haben

$$\begin{aligned} \sum_{u \in C} \widehat{f}(u) &= \sum_{u \in C} \sum_{v \in K^n} \chi(u \cdot v) f(v) \\ &= \sum_{v \in K^n} f(v) \sum_{u \in C} \chi(u \cdot v). \end{aligned}$$

Falls $v \in C^\perp$ ist, so ist $u \cdot v = 0$ für alle $u \in C$, somit $\chi(u \cdot v) = 1$, also ist die innere Summe gleich $|C|$.

Sei $v \notin C^\perp$, dann ist $C \not\subseteq \langle v \rangle^\perp$ und somit $C \cap \langle v \rangle^\perp \subseteq C$ ein $(k-1)$-dimensionaler Unterraum von C, $k = \dim C$. Die Gruppe C_+ zerfällt in $\frac{|C|}{|C \cap \langle v \rangle^\perp|} = q$ Nebenklassen. Zwei Codewörter u_1, u_2 sind in derselben Nebenklasse genau dann, wenn

$$u_1 - u_2 \in C \cap \langle v \rangle^\perp \Longleftrightarrow (u_1 - u_2) \cdot v = 0 \Longleftrightarrow u_1 \cdot v = u_2 \cdot v\,.$$

Jede Nebenklasse wird also durch ein Element $\lambda \in K$, $u \cdot v = \lambda$ repräsentiert. Es folgt

$$\#\{u \in C : u \cdot v = \lambda\} = q^{k-1} \text{ für alle } \lambda \in K\,,$$

und somit für die innere Summe

$$q^{k-1} \sum_{\lambda \in K} \chi(\lambda) = 0$$

nach Lemma 3. $\square$

Satz von MacWilliams. *Es sei $C \subseteq GF(q)^n$ linearer Code. Dann gilt*

$$W_{C^\perp}(x, y) = \frac{1}{|C|} W_C(x + (q-1)y, x - y).$$

Beweis. Die Behauptung ist äquivalent zu

$$\sum_{v\in C^\perp} x^{n-w(v)}y^{w(v)} = \frac{1}{|C|}\sum_{u\in C}(x+(q-1)y)^{n-w(u)}(x-y)^{w(u)}\,.$$

Wir betrachten die Funktion $f : GF(q)^n \longrightarrow GF(q)[x,y]$, $f(u) = x^{n-w(u)}y^{w(u)}$. Nach Lemma 4 bleibt zu zeigen, dass

$$\widehat{f}(u) = (x+(q-1)y)^{n-w(u)}(x-y)^{w(u)}$$

gilt. Wir setzen wieder $K = GF(q)$, $u = u_1\dots u_n$, $v = v_1\dots v_n$ und haben

$$\begin{aligned}\widehat{f}(u) &= \sum_{v\in K^n}\chi(u\cdot v)x^{n-w(v)}y^{w(v)}\\ &= \sum_{v\in K^n}\chi(u_1v_1+\cdots+u_nv_n)x^{n-w(v)}y^{w(v)}\\ &= \sum_{v\in K^n}\prod_{i=1}^{n}\chi(u_iv_i)x^{1-\overline{v}_i}y^{\overline{v}_i}\end{aligned}$$

wobei $\widehat{v}_i = 1$ für $v_i \neq 0$, $\widehat{v}_i = 0$ für $v_i = 0$ ist. Der letzte Ausdruck ist

$$\begin{aligned}&= \sum_{v_1\in K}\cdots\sum_{v_n\in K}\prod_{i=1}^{n}\chi(u_iv_i)x^{1-\widehat{v}_i}y^{\widehat{v}_i}\\ &= \prod_{i=1}^{n}\sum_{a\in K}\chi(u_ia)x^{1-\widehat{a}}y^{\widehat{a}}\,.\end{aligned}\qquad(1)$$

Für $u_i = 0$ ist die innere Summe

$$\sum_{a\in K}\chi(0)x^{1-\widehat{a}}y^{\widehat{a}} = x+(q-1)y\,.$$

Für $u_i \neq 0$ durchläuft u_ia den Körper K, und es gilt $\widehat{u_ia} = \widehat{a}$. Die innere Summe ist daher

$$\sum_{a\in K}\chi(a)x^{1-\widehat{a}}y^{\widehat{a}} = x+\sum_{a\neq 0}\chi(a)y = x-y\,,$$

da nach Lemma 3

$$\sum_{a\in K, a\neq 0} \chi(a) = -\chi(0) = -1$$

ist. Für das Produkt (1) erhalten wir somit

$$\widehat{f}(u) = (x + (q-1)y)^{n-w(u)}(x-y)^{w(u)}$$

wie behauptet. □

Folgerung. *Für einen selbstdualen Code $C = C^{\perp}$ gilt*

$$W_C(x,y) = \frac{1}{q^{n/2}} W_C(x + (q-1)y, x-y).$$

Beispiel. Der erweiterte Hamming Code $\overline{H}_{3;2}$ ist selbstdual, also gilt

$$W_{\overline{H}_{3;2}}(x,y) = \frac{1}{16} W_{\overline{H}_{3;2}}(x+y, x-y)\,.$$

5.5 Golay Codes

Neben Shannon und Hamming war Golay ein Pionier der Codierungstheorie. Nach ihm sind zwei berühmte perfekte Codes benannt.

Ein Code $C \subseteq A^n$, $|A| = q$, heißt bekanntlich t-perfekt, falls

$$|C| = \frac{q^n}{\sum_{i=0}^{t} \binom{n}{i} (q-1)^i}$$

gilt. Wir betrachten lineare perfekte Codes, also $|C| = q^k$, $k = \dim C$.

Für $t = 1$ haben wir unendlich viele 1-perfekte Codes, die Hamming Codes, konstruiert.

$t = 2$: Für $q = 2$ haben wir die Existenz bereits ausgeschlossen. Für $q = 3$

muß gelten

$$\begin{aligned} & 1+2n+4\binom{n}{2} = 3^{n-k} \\ \iff\ & 1+2n+2n^2-2n = 3^{n-k} \\ \iff\ & 2n^2+1 = 3^{n-k}\,, \end{aligned}$$

und wegen $t \geq 2$ ist $n \geq 5$. Aus der Zahlentheorie weiß man, dass die Gleichung $2n^2+1 = 3^s$ nur die Lösung $n = 11$, $s = 5$ hat ($2 \cdot 121 + 1 = 243 = 3^5$). Es könnte also ein 2-perfekter $[n = 11, k = 6, d = 5; q = 3]$-Code existieren.

$t = 3$: Für $q = 2$ erhalten wir die Gleichung

$$1 + n + \binom{n}{2} + \binom{n}{3} = 2^{n-k}, \quad n \geq 7,$$

und man sieht leicht, dass die einzigen Lösungen $n = 7$, $k = 1$ und $n = 23$, $k = 12$ sind. Im ersten Fall haben wir den Wiederholungscode.

Wir wollen nun zeigen, dass tatsächlich ein 2-perfekter $[11, 6, 5; 3]$-Code G_{11} und ein 3-perfekter $[23, 12, 7; 2]$-Code G_{23} existiert, und dies sind die Golay Codes.

Satz 28 (Tietäväinen, van Lint)**.** *Außer den Wiederholungscodes (n ungerade, $q = 2$), den Hamming und Golay Codes gibt es keine weiteren linearen perfekten Codes.*

Konstruktion der Codes G_{11} und G_{12}.

Es sei $GF(3) = \{0, 1, -1\}$. Die folgende 6×11-Generatormatrix G erzeugt G_{11} und die Matrix $\overline{G} = G+$ Paritätsspalte den Code G_{12}:

$$G = \left(\begin{array}{cccccc|ccccc|c} 1 & & & & & & 0 & 1 & -1 & -1 & 1 & 1 \\ & 1 & & & & 0 & 1 & 0 & 1 & -1 & -1 & -1 \\ & & 1 & & & & -1 & 1 & 0 & 1 & -1 & -1 \\ & & & 1 & & & -1 & -1 & 1 & 0 & 1 & -1 \\ & & & & 1 & & 1 & -1 & -1 & 1 & 0 & -1 \\ & 0 & & & & 1 & 1 & 1 & 1 & 1 & 1 & 0 \end{array}\right)$$

$\uparrow$ für $\overline{G}$

Die Zeilen von G seien $c_1, \ldots, c_6$ bzw. $\overline{c}_1, \ldots, \overline{c}_6$ für $\overline{G}$.

Offenbar ist $\dim G_{11} = \dim G_{12} = 6$. Wenn wir zeigen können, dass $d(G_{12}) = 6$ ist, so folgt $d(G_{11}) = 5$, und G_{11} ist 2-perfekt.

Behauptung. G_{12} ist selbstdual, $G_{12}^{\perp} = G_{12}$.

Man prüft direkt nach, dass $\overline{c}_i \cdot \overline{c}_j = 0$ für alle i und j gilt. Daraus folgt $G_{12} \subseteq G_{12}^{\perp}$ und somit $G_{12} = G_{12}^{\perp}$ wegen $\dim G_{12} = 6 = \frac{n}{2}$ $(n = 12)$.

Für $c = (\lambda_1 \ldots \lambda_{12}) \in G_{12}$ ist $c \cdot c = \sum_{i=1}^{12} \lambda_i^2 = w(c)$ und somit $w(c) \equiv 0 \pmod 3$ wegen $c \cdot c = 0$ in $GF(3)$. Es bleibt also zu zeigen, dass $w(c) = 3$ nicht möglich ist.

Wenn $c \in G_{12}$ Linearkombination von ≥ 4 Zeilen $\overline{c}_i$ ist, so folgt (wegen der Einheitsmatrix I_6) $w(c) \geq 4$. Wenn $c = \overline{c}_i$ ist, so gilt $w(c) = 6$. Wenn $c \in G_{12}$ Linearkombination von zwei oder drei Zeilen ist, so sieht man ebenfalls sofort $w(c) > 3$. Es folgt $d(G_{12}) = 6$ und somit $d(G_{11}) = 5$.

Wir wollen nun die Gewichtsverteilung von G_{11} bestimmen. Wir haben $|G_{11}| = 3^6 = 729$. Die Koeffizienten sind $A_0 = 1$, $A_1 = A_2 = A_3 = A_4 = 0$. Was ist A_5? Da G_{11} 2-perfekt ist, liegt jedes Wort vom Gewicht 3 in genau einer Kugel um ein Codewort vom Gewicht 5, und wir erhalten

$$\binom{11}{3} 2^3 = A_5 \cdot 10\,,$$

also $A_5 = 132$.

Zur Bestimmung von A_6 gehen wir analog vor. Jedes Wort vom Gewicht 4 liegt in genau einer Kugel um ein Codewort vom Gewicht 5 oder 6. Daraus folgt

$$\binom{11}{4} 2^4 = A_5 \cdot 25 + A_6 \cdot 15\,,$$

also $A_6 = 132$. Die Folge der Gewichtskoeffizienten ist für G_{11} schließlich

$$A_0 = 1, A_5 = A_6 = 132, A_8 = 330, A_9 = 110, A_{11} = 24$$

und für G_{12}

$$A_0 = 1, A_6 = 264, A_9 = 440, A_{12} = 24\,.$$

Wir können aus G_{11} und G_{12} Steiner Systeme konstruieren. Wir betrachten die 132 Codewörter in G_{11} vom Gewicht 5, und $X = \{1, 2, \ldots, 11\}$ die Koordinatenstellen. Der Träger von $c \in G_{11}$ ist $B(c) = \{i \in X : c_i \neq 0\}$. Mit c hat auch $-c$ Gewicht 5 mit $B(c) = B(-c)$. Für jedes andere Codewort c' vom Gewicht 5 gilt $B(c') \neq B(c)$ wegen $\Delta(c, c') \geq 5$. Wir haben also $\frac{132}{2} = 66$ verschiedene Träger, die wir nun als Blöcke (der Größe 5) in $X = \{1, \ldots, 11\}$ auffassen. Es sei nun $D \subseteq X$ mit $|D| = 4$. Angenommen D ist in zwei Blöcken $B = B(c)$ und $B' = B(c')$ enthalten. Dies bedeutet für G_{11} die Existenz von c, c' vom Gewicht 5 mit

$$\begin{aligned} c &= 0 \ldots 0 a_1 \cdot a_2 \cdot a_3 \cdot a_4 \ldots b .. 0 \cdots, \quad a_i \neq 0, \;\; b \neq 0 \\ c' &= 0 \ldots 0 a_1' \cdot a_2' \cdot a_3' \cdot a_4' \ldots 0 .. b' \cdots, \quad a_i' \neq 0, \;\; b' \neq 0 \end{aligned}$$

Wegen $\Delta(c, c') \geq 5$ muß für mindestens drei Indizes j, z.B. $j = 1, 2, 3$, $a_j' = -a_j$ gelten. Daraus würde aber $\Delta(-c, c') \leq 3$ folgen, Widerspruch. Eine 4-Menge ist also in höchstens einem Block enthalten, und wegen

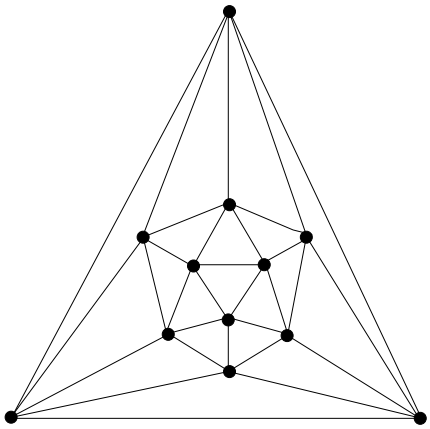
$$\binom{11}{4} = \frac{11 \cdot 10 \cdot 9 \cdot 8}{24} = 330 = 66 \cdot 5$$

in *genau* einem 5-Block. Wir erhalten also ein 4-(11,5) Steiner System. Ebenso erhält man ein 5-(12,6) Steiner System aus den Wörtern vom Gewicht 6 in G_{12}.

Konstruktion der Codes G_{23} und G_{24}

Wiederum konstruieren wir zunächst einen $[n = 24, k = 12, d = 8; 2]$-Code G_{24} und erhalten dann durch Verkürzung einen $[23, 12, 7; 2]$-Code G_{23}. Es gibt viele Möglichkeiten, G_{24} zu konstruieren, die vielleicht eleganteste Methode

verwendet den Ikosaedergraphen:



Wir nummerieren die Ecken des Graphen mit 1 bis 12. Es sei $A = (a_{ij})$ die Adjazenzmatrix des Graphen, also

$$a_{ij} = \begin{cases} 1 & \text{falls } \{i,j\} \text{ Kante} \\ 0 & \text{sonst,} \end{cases}$$

und fassen A als Matrix über $GF(2)$ auf. A ist somit eine symmetrische Matrix mit 5 Einsen in jeder Zeile und Spalte, und Nullen in der Hauptdiagonale. Es seien a_i und a_j die i-te bzw. j-te Zeile von A, dann gilt

$$a_i \cdot a_j = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$$

da $a_i \cdot a_i = 5 \equiv 1 \pmod 2$ und $a_i \cdot a_j = 2$ oder $0 \equiv 0 \pmod 2$ für $i \neq j$ ist. Es ist also $A^2 = I$ gleich der Einheitsmatrix der Ordnung 12.

Es sei nun $J = \begin{pmatrix} 1 \dots 1 \\ \dots \\ 1 \dots 1 \end{pmatrix}$ die 12×12-Matrix aus lauter Einsen über $GF(2)$.
Dann gilt $J^2 = \begin{pmatrix} 12 \dots 12 \\ 12 \dots 12 \end{pmatrix} = O$ gleich der Nullmatrix der Ordnung 12.

Wir betrachten nun folgende Generatormatrix G:

$$G = [I|J + A]\,.$$

G ist also eine 12×24-Matrix mit jeweils einer Eins in der vorderen Hälfte und 7 Einsen in der hinteren Hälfte.

Behauptung. Der von G erzeugte Code C ist selbstdual.

Es gilt

$$\begin{aligned} GG^T &= [I|J+A][\frac{I}{J+A}] = I + (J+A)^2 \\ &= I + J^2 + A^2 = I + I = O\,. \end{aligned}$$

Es gilt also $C \subseteq C^\perp$ und somit $C = C^\perp$ wegen $\dim C = 12$.

Behauptung. Ist $(u|v) \in C$, so ist auch $(v|u) \in C$. Wir haben

$$\begin{aligned} (J+A)G &= (J+A)[I|J+A] = [J+A|(J+A)^2] \\ &= [J+A|I]\,, \end{aligned}$$

das heißt, $[J+A|I]$ ist ebenfalls Generatormatrix von C. Schreiben wir die Zeilen von G als $c_i = (e_i|f_i)$, so bilden also auch $c_i' = (= (f_i|e_i)$ eine Basis. Aus $(u|v) = \sum \lambda_i c_i \in C$ folgt $u = \sum \lambda_i e_i$, $v = \sum \lambda_i f_i$, also $(v|u) = \sum \lambda_i c_i' \in C$.

Behauptung. Der Code C ist ein $[24, 12, 8; 2]$-Code, genannt *Golay Code* G_{24}.

Wir wissen, dass C selbstdual ist und alle Basiswörter Gewicht 8 haben. Mit Induktion nach der Länge der Linearkombination sieht man leicht, dass alle Codewörter c ein Gewicht $w(c) \equiv 0 \pmod 4$ haben. Wir müssen also nur noch Gewicht 4 ausschließen. Sei $(u|v) \in C$ mit Gewicht 4. Da auch $(v|u) \in C$ ist, können wir uns auf folgende Fälle beschränken:

	$w(u)$	w(v)
1.	0	4
2.	1	3
3.	2	2

Der erste Fall ergibt das Nullwort. Im zweiten Fall erhalten wir ein Zeile von G mit $w(u|v) = 8$. Im dritten Fall ist $(u|v) = c_i + c_j$ Summe von zwei Zeilen $c_i = (e_i|f_i)$, $c_j = (e_j|f_j)$ mit

$$w(c_i + c_j) = w(e_i + e_j) + w(f_i + f_j)\,.$$

Nun ist $e_i = (0 \ldots 1 \ldots 0)$ Einheitsvektor mit 1 an i-ter Stelle, also $w(e_i+e_j) = 2$. Ferner ist $f_i = 1 + a_i$, wobei 1 der Vektor der Länge 12 aus lauter Einsen ist, und a_i die i-te Zeile von A. Wir haben somit

$$\begin{aligned} w(f_i + f_j) &= w(1 + a_i + 1 + a_j) = w(a_i + a_j) \\ &= w(a_i) + w(a_j) - 2 \cdot \#\{\text{Nachbarn von } i \text{ und } j\} \\ &\geq 5 + 5 - 4 = 6\,, \end{aligned}$$

und daher $w(c_i + c_j) \geq 8$.

Der verkürzte Code ist dann der 3-perfekte $[23, 12, 7; 2]$-Code G_{23}.

Auch hier erhalten wir Steiner Systeme. Nach einem früheren Satz bilden die Codewörter in G_{23} vom Gewicht 7 ein 4-(23,7) Steiner System. Die Anzahl A_7 der Codewörter vom Gewicht 7 berechnet sich aus

$$\binom{23}{4} = A_7 \binom{7}{3} = 35A_7\,,$$

mit dem Ergebnis $A_7 = 253$. Analog berechnet man $A_8 = 506$. Im Golay Code G_{24} gilt also $A_8 = 759$. Damit ist wegen $11 \ldots 1 \in G_{24}$, also $A_i = A_{24-i}$, die gesamte Gewichtsverteilung gegeben:

	A_0	A_8	A_{12}	A_{16}	A_{24}
G_{24}	1	759	2576	759	1

Für G_{23} haben wir wegen $11 \ldots 1 \in G_{23}$ analog $A_i = A_{23-i}$ und erhalten die Verteilung

	A_0	A_7	A_8	A_{11}	A_{12}	A_{15}	A_{16}	A_{23}
G_{23}	1	253	506	1286	1286	506	253	1

Für G_{24} beweist man analog, dass die Codewörter in G_{24} vom Gewicht 8 ein 5-(24,8) Steiner System bilden.

Der Golay Code G_{24} kann auch zur Konstruktion eines besonders interessanten nichtlinearen binären Codes herangezogen werden. Mit Permutation der

Spalten schreiben wir die Generatormatrix von G_{24} in der Form

$$G = \begin{array}{c} \\ 7 \\ \\ \\ \\ 5 \end{array} \overbrace{\left\{ \begin{array}{c} \\ \\ \\ \\ \\ \end{array} \right.}^{} \overbrace{\left(\begin{array}{cccc|c} 1 & & & 1 & \\ & 1 & 0 & 1 & \\ & & \ddots & \vdots & G_1 \\ 0 & & & 1 \;\; 1 & \\ \hline & & & & \\ & & O & & G_2 \\ & & & & \end{array} \right)}^{} \begin{array}{c} 8 \\ \\ \\ \\ \\ \\ \\ \end{array} \quad \overbrace{\begin{array}{c} 16 \\ \\ \\ \\ \\ \\ \\ \end{array}}^{}$$

Es gibt $2^5 = 32$ Codewörter in G_{24}, die mit $\underbrace{0\,0\ldots0}_{8}$ beginnen (die Linearkombinationen der Zeilen $c_8, \ldots, c_{12}$ von G. Sei $b_i = 0 \ldots 1 \ldots 0\,1 \in GF(2)^8$, $i = 1, \ldots, 7$, dann gibt es $2^5 = 32$ Codewörter in G_{24}, die mit b_i beginnen (die Linearkombination von $c_8, \ldots, c_{12}$ plus c_i). Mit D bezeichnen wir die Mengen dieser $8 \cdot 2^5 = 2^8$ Codewörter. Der *Nordstrom-Robinson Code* $\mathcal{N} \subseteq \{0,1\}^{16}$ ist D verkürzt auf die Spalten 9 bis 24. Wegen $d(G_{24}) = 8$ sind die verkürzten Wörter alle verschieden, also $|\mathcal{N}| = 2^8 = 256$, und wir haben $d(\mathcal{N}) = 6$, da sich die Wörter aus D in den ersten acht Koordinaten an höchstens zwei Stellen unterscheiden. $\mathcal{N}$ ist also ein (nichtlinearer) binärer $(16, 6)$-Code mit $|\mathcal{N}| = 2^8$.

Wir haben somit $M_2(16, 6) \geq 2^8$ und erhalten durch dreimalige Punktierung $M_2(13, 6) \geq 2^5$, also $M_2(12, 5) = M_2(13, 6) \geq 32$. Bisher kennen wir die obere Schranke $M_2(12, 5) \leq 48$, durch lineare Programmierung kann dies zu $M_2(12, 5) \leq 32$ verbessert werden. Es gilt also $M_2(12, 5) = 32$, während andererseits gezeigt werden kann, dass $A_2(12, 5) = 16$ ist. Resultat: Es existiert ein nichtlinearer $(12, 5)$-Code C mit $|C| = 32$, aber kein linearer.