Die sporadische Gruppe M_{24} als Automorphismengruppe des Golaycodes

von David Dursthoff

Die meisten Abschnitte dieses Textes beruhen auf dem Buch „Twelve Sporadic Groups“ von Robert L. Griess, Jr., siehe [Gr]. Die endlichen einfachen Gruppen werdem im 1. Kapitel kurz vorgestellt. Im 2. Kapitel werden einige benötigte Sätze über Gruppen zusammengefasst. Das 3. Kapitel behandelt den Hexacode, einen [8,3,4]-Code, und gibt eine kurze Zusammenfassung über Codes. Die Konstruktion des binären Golaycodes ist das Hauptthema des 4. Kapitels. Die Eindeutigkeit und die Einfachheit der Automorphismengruppe, M_{24}, wird im 5. Kapitel bewiesen. Im letzten Kapitel wird dann kurz M_{23}, eine ebenfalls einfache Untergruppe von M_{24} behandelt.

Inhaltsverzeichnis

1 Endliche einfache Gruppen und ihre Klassifikation

Eine endliche einfache Gruppe ist eine nicht-triviale endliche Gruppe, die nur triviale Normalteiler besitzt ($\{1\}$ und die Gruppe selbst). Aus den einfachen Gruppen kann man alle endliche Gruppen zusammensetzen.

Satz 1.1 ***(Klassifikationssatz endlicher einfacher Gruppen)***
G sei eine endliche einfache Gruppe.
Dann ist G von einem der folgenden Typen:

- *G ist zyklisch von Primzahlordnung (falls G abelsch).*
- *G ist eine alternierende Gruppe A_n mit Grad $n \geq 5$.*
- *G ist eine Gruppe vom Lie-Typ (siehe Tabelle 1)*
- *G ist eine von 26 sporadischen Gruppen (siehe Tabelle 2)*

Der Beweis des Satzes war im Februar 1981 vollendet. An ihm wurde mehrere Jahrzehnte von Dutzenden von Mathematikern gearbeitet. Dazu wurden auch auf Computerergebnisse zurückgegriffen.Der Beweis hat eine Länge von ca. 15.000 Seiten, verteilt auf 300 bis 500 einzelne Artikel (nicht alle veröffentlicht).

Tabelle 1: Die 16 Serien endlicher einfacher Gruppen vom Lie-Typ

Serie	Parameter	Name
PSL(n,q)	$n \geq 2,\ (n,q) \neg (2,2),(2,3)$	proj. spez. lin. Gruppen
PSU(n,q)	$n \geq 3,\ (n,q) \neq (3,2)$	proj. unitäre Gruppen
PSp(2m,q)	$m \geq 2,\ (m,q) \neq (2,2)$	proj. symplektische Gruppen
Ω_{2m+1}	≥ 3, q ungerade	orthogonale Gruppen
$P\Omega^+_{2m}$	$m \geq 4$	proj. orthog. Gruppen
$P\Omega^-_{2m}$	$m \geq 4$	"
$G_2(q)$	$q \geq 3$	
$F_4(q)$		
$E_6(q)$		
$E_7(q)$		
$E_8(q)$		
${}^2E_6(q)$		
${}^3D_4(q)$		Steinberg-Trialitäts-Gruppen
${}^2B_2(q)$	$q = 2^{2m+1}$	Suzuki-Gruppen
${}^2G_2(q)$	$q = 3^{2m+1}$	Ree-Gruppen
${}^2F_4(q)$	$q = 2^{2m+1}$	Ree-Gruppen
${}^2F_4(2)'$		Tits-Gruppe

Tabelle 2: Die 26 sporadischen Gruppen

Bezeichnung (Entdeckungs − / Konstruktionsjahr)	*Ordnung*	*...in Primzahlzerlegung*
M_{11} (1861)	7920	$2^4 \cdot 3^2 \cdot 5 \cdot 11$
M_{12} (1861)	95040	$2^6 \cdot 3^3 \cdot 5 \cdot 11$
J_1 (1965)	175560	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$
M_{22} (1861)	443520	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$
J_2„(1968)	604800	$2^7 \cdot 3^3 \cdot 5^2 \cdot 7$
M_{23} (1861)	10200960	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$
HS (1967)	44352000	$2^9 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11$
J_3 (1968/69)	50232960	$2^7 \cdot 3^5 \cdot 5 \cdot 17 \cdot 19$
M_{24} (1861)	244823040	$2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$
McL (1969)	898128000	$2^7 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11$
He (1969)	4030387200	$2^{10} \cdot 3^3 \cdot 5^2 \cdot 7^3 \cdot 17$
Ru (1972/73)	145926144000	$2^{14} \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 13 \cdot 29$
Suz (1969)	448345497600	$2^{13} \cdot 3^7 \cdot 5^2 \cdot 7 \cdot 11 \cdot 23$
ON (1973)	460815505920	$2^9 \cdot 3^4 \cdot 5 \cdot 7^3 \cdot 11 \cdot 19 \cdot 31$
Co_3 (1969)	495766656000	$2^{10} \cdot 3^7 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$
Co_2 (1969)	42305421312000	$2^{18} \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$
Fi_{22} (1971)	64561751654400	$2^{17} \cdot 3^9 \cdot 5^2 \cdot 7 \cdot 11 \cdot 23$
F_5, HN (1973/76)	273030912000000	$2^{15} \cdot 3^{10} \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 19 \cdot 31$
Ly (1972/73)	51765179004000000	$2^8 \cdot 3^7 \cdot 5^6 \cdot 7 \cdot 11 \cdot 31 \cdot 37 \cdot 67$
F_3, Th (196973/76)	90745943887872000	$2^{14} \cdot 3^6 \cdot 5^6 \cdot 7 \cdot 11 \cdot 19$
Fi_{23} (1971)	4089470473293004800	$2^{18} \cdot 3^{13} \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23$
Co_1 (1969)	4157776806543360000	$2^{21} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$
J_4 (1976/80)	86775571046077562880	$2^{21} \cdot 3^3 \cdot 5v7 \cdot 11^3 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 43$
Fi_{24} (1971)	1255205709190661721292800	$2^{21} \cdot 3^{16} \cdot 5^2 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 29$
$F_2,\ B$ (1973/77)	4154781481226426191177580 544000000	$2^{41} \cdot 3^{13} \cdot 5^6 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot$ $23 \cdot 31 \cdot 47$
$\mathrm{F}_1,\ M$ (1973/81)	808017424794512875886459904 96171075700575436800000000	$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot$ $23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$

Die 26 sporadischen Gruppen sind die einfachen Gruppen, die sich nicht in die anderen Familien einordnen lassen. Sie wurden von 1861 bis 1981 entdeckt und konstruiert. Die größte Gruppe, das Monster M, wurde 1981 von Robert L. Griess, Jr. konstruiert. Sie hat eine Ordnung von zirka $8 \cdot 10^{53}$. Dass M einfach ist bewiesen im Jahre 1973 Bernard Fischer und Robert L. Griess, Jr. unabhängig voneinander. 20 der sporadischen Gruppen lassen sich aus dem Monster konstruieren. Sie bilden die Happy Famely. Die 6 Ausnahmen ($J_1,\ J_3,\ J_4,\ ON,\ Ru$, und Ly) werden auch als Parias bezeichnet.

Die ersten fünf sporadischen Gruppen, die Mathieu-Gruppen $M_{11},\ M_{12},\ M_{22},\ M_{23},\ M_{24}$ entdeckte Émile Léonard Mathieu (1835-1890). Erst hundert Jahre später, im Jahre 1965, entdeckte Zvonimir Janko die nächste sporadische Gruppe, J_1.

In diesem Vortrag wird M_{24} als Automorphismengruppe des erweiterten binären Golaycodes konstruiert und bewiesen, dass sie eindeutig und einfach ist. Als einfache Folgerung erhält man die Konstruktion und die Einfachheit von M_{23}. Die Mathieu-Gruppen M_{24} und M_{12} sind 5-fach transitiv auf 24 bzw. 12 Punkten (d.h. sie bilden 5 verschiedene Punkte auf jede Wahl von 5

verschiedenen Punten ab). Die Mathieu-Gruppen M_{23} und M_{11} sind noch 4-fach transitiv auf 23 bzw. 11 Punkten. M_{22} ist noch 3-fach transitiv auf 22 Punkten. M_{24}, M_{23}, M_{12} und M_{11} sind mit den Symmetrischen Gruppen S_n und den Alternierenden Gruppen A_m zusammen die einzigen 4-fach transitiven Permutationsgruppen ($n \geq 5$ und $m \geq 6$).

Eine gute Zusammenfassung der Geschichte der Entdeckung der sporadischen Gruppen geben auch [Hi] und [Go].

.

2 Sätze aus der Gruppentheorie

Lemma 2.1 *Sei G eine Gruppe und N ein Normalteiler. G operiere primitiv Menge M.*
Wenn N nicht trivial auf M operiert, so operiert es N transitiv.

Beweis: Sei $M = \{Nm_1, ..., Nm_n\}$ die Partition der Bahnen unter N. Dann ist $\{N_{m_1}, ..., N_{m_n}\}$ G-invariant, denn: Sei $g \in \mathcal{G}$

$$gNm_i = Ngm_i = Nm_j \text{ für } gm_i \in Nm_j$$

Damit ist $\{Nm_1, ..., Nm_n\} = \{\{m\}|\ m \in M\}$ oder $|\{Nm_1, ..., Nm_n\}| = 1$. Da N nicht trivial operiert, existiert ein $m \in M$ mit $|Nm| > 1$. Also gilt der Fall $|\{Nm_1, ..., Nm_n\}| = 1$ und damit N transitiv. □

Satz 2.2 ***(Burnsides Satz vom normalen p-Komplement)***
Sei G eine Gruppe, p eine Primzahl und P eine p-Sylowuntergruppe von G mit $P \leq Z(N_G(P))$.
Dann hat G ein normales p-Komplement, d.h. es existiert ein $N \lhd G$ mit $N \cap P = \{1\}$ und $G = NP$.

Beweis: Siehe [Go2] oder [1].

Lemma 2.3 *Sei G eine p-Gruppe, d.h. $|G| = p^a$.*
Dann gilt $|Aut(G)| = p^b n$ mit $b \leq a$, $p \nmid n$ und n teilt $|GL(a,p)| = \prod_{i=0}^{a-1}(p^d - p^i)$.

Beweis: Siehe z.B. [Hu], S. 273ff.

Lemma 2.4 *Sei $n > 1$ und $m = n$ oder $m = n + 1$. x sei ein n-Zykel in S_m.*
Dann sind Zentralisator und Normalisator gegeben durch

$$C_{S_m}(x) = < x > \text{ und } N_{S_m}(x) \cong < x > \rtimes (\mathbb{Z}/n\mathbb{Z})^*$$

Beweis: siehe Übung 3, A6 zur Computeralgebra, SS 2010.

Lemma 2.5 ***(Frattini-Argument)***
Sei G eine Gruppe, K Normalteiler und $P \leq K$. G lasse die K-Konjugationsklasse von P invariant.
Dann gilt $G = N_G(P)K$.

Beweis: Sei $g \in G$. Dann gilt $g^{-1}Pg = k^{-1}Pk$ für ein $k \in K$. Dann ist aber $gk^{-1} \in N_G(p)$, also $g = (gk^{-1})k \in N_G(P)K$. □

3 Der Hexacode

In diesem Kapitel betrachten wir einen Code über $\mathbb{F}_4^6$. $(\ ,\ )$ sei die semilineare symmetrische Bilinearform mit $(x,y) := \sum_{i=1}^{6} \sigma(x_i) \cdot y_i$ für $x, y \in \mathbb{F}_4^6$. σ bezeichne den einzigen nicht-trivialen Körperautomorphismus auf $\mathbb{F}_4$, den Frobeniusautomorphismus ($\sigma(c) = c^2 =: \overline{c}$).

Es ist $\mathbb{F}_4 := \{0, 1, \omega, \overline{\omega}\}$ mit $\omega^2 = \overline{\omega} = \omega + 1$, $\overline{\omega}^2 = \omega$ und $\overline{\omega}\omega = 1$.

Zunächst eine kurze Wiederholung der wichtigsten Eigenschaften von Codes.

Definition 3.1 *Sei K ein Körper.*

- *Ein Untervektorraum $C \leq K^n$ mit Dimension k heißt (linearer) Code der Länge n und Dimension k. Elemente von C heißen Codewörter.*
- *Der Hamming-Abstand zweier Codewörter $c, c' \in C$ ist definiert als $d(c,c') := |\{i|\ c_i \neq c'_i\}|$. Der Hamming-Abstand ist eine Metrik.*
- *Das Gewicht eines Codeworts $c \in C$ ist $wt(c) = |\{i \mid c_i \neq 0\}| = d(c,0)$.*
- *Das Minimalgewicht $wt(C)$ eines Codes C ist definiert als das minimale Gewicht aller Codewörter ungleich 0. Der minimale Abstand zwischen Codewörtern ist gleich dem Minimalgewicht. ´*
- *Ist $C \leq K^n$ mit $Dim(C) =: k$ und $wt(C) =: d$, so heißt C ein [n,k,d]-Code.*

Definition 3.2 *Sei K ein Körper und $C \leq K^n$ ein Code.*

- *Eine Monomialtransformation ist eine Abb. $f \in GL(n,K)$, die die Standard-Basisvektoren $e_1 = (1,0,...,0), ..., e_n = (0,...,0,1)$ folgender Maßen abbildet:*

$$f(e_i) = c_i e_{\tau(i)}, \quad c_i \in K^*,\ \tau \in S_n.$$

  Das heißt, sie erhält die Menge der Erzeugnisse der Basisvektoren $\{< e_1 >, ..., < e_n >\}$. Dann ist f ein Produkt aus einer Diagonalmatrix $Diag(c_1, ..., c_n) \in Diag(n,K) := \{f \in GL(n,K)|\ f\ Diagonalmatrix\}$ und einer Permutationsmatrix, die man aus τ erhält. Schreibe $Perm(n,K)$ als die Gruppe aller Permutationsmatrizen.
- *$Mon(n,K)$ bezeichne die Gruppe aller Monomialtrasformationen.*

$$Mon(n,K) = Diag(n,K) \rtimes Perm(n,K) \cong K^* \wr S_n \ (\wr \text{ bezeichnet dar Kranzprodukt})$$

- *Die Gruppe der Körperautomorphismen $Aut(K)$ operiert auf K^n koordinatenweise. Sei Γ die von den Körperautomorphismen induzierte Gruppe von Transformationen in $\Gamma L(n,K)$ (Gruppe der bijektiven semilinearen Abbildungen). Dann definiere $Mon^*(n,K)$ als die Gruppe aller semilinearen Monomialtransformationen, die $e_1, ..., e_n$ folgendermaßen abbilden:*

$$f(e_i) = c_i e_{\tau(i)}, \quad c_i \in K^*,\ \tau \in S_n \ \text{ und } f(av) = \sigma(a) f(v)\ \forall a \in K,\ v \in K^n$$

  für einen Körperautomorphismus σ.
- *$Mon^*(n,K) = Mon(n,K) \rtimes \Gamma = [Diag(n,K) \rtimes Perm(n,F)] \rtimes \Gamma$. Eine semilineare Transformation $f \in Mon^*(n,K)$ lässt sich also durch $f = (D, \tau, \sigma)$ darstellen, $D \in Diag(n,K)$, $\tau \in S_n$ und $\sigma \in Aut(K)$.*

- *Die (semilineare) Automorphismengruppe des Codes C ist*

$$Aut^*(C) := \{g \in Mon^*(n,K) | g(C) = C\}.$$

  $Aut(n,K) := Aut^*(n,K) \cap Mon(n,K)$ ist die Gruppe aller linearen Codeautomorphismen.

- *Zwei Codes $C, D \leq K^n$ heißen äquivalent, falls ein $g \in Mon^*(n,K)$ existiert, sodass $g(C) = D$ gilt. Existiert so ein g aus $Mon(n,K)$, so heißen C und D linear äquivalent.*

Bemerkung 3.3 *Ist $K = \mathbb{F}_2$, so gilt $Mon^*(n,K) = Mon(n,K) \cong S_n$.*

Nun zum Thema dieses Kapitels, der Untersuchung des Hexacodes.

Definition 3.4 *Ein **Hexacode** bezeichnet einen [6,3,4]-Code über $\mathbb{F}_4$. Codewörter eines Hexacode heißen Hexacodewörter. $\mathcal{H}$ sei der Standard-Hexacode, der von den folgenden Vektoren erzeugt wird:*

$$v_1 := (\omega\overline{\omega}|\omega\overline{\omega}|\omega\overline{\omega})$$
$$v_2 := (\overline{\omega}\omega|\overline{\omega}\omega|\omega\overline{\omega})$$
$$v_3 := (\omega\overline{\omega}|\overline{\omega}\omega|\overline{\omega}\omega)$$
$$v_4 := (\overline{\omega}\omega|\omega\overline{\omega}|\overline{\omega}\omega)$$

Die Schreibweise wird später klar. Die Koordinaten 1&2, 3&4 und 5&6 bilden jeweils Koordinaten-Blöcke. Im Folgenden wird bewiesen, dass $\mathcal{H}$ tatsächlich ein Hexacode ist. $\mathcal{H}$ ist sogar bis auf Äquivalenz der einzige Hexacode. Für einen Beweis siehe [Gr].

Bemerkung 3.5

- *$Dim(\mathcal{H}) = 3$. Jeweils drei der oberen vier Vektoren bilden eine Basis.*
- *$\mathcal{H}$ ist selbst-orthogonal bezüglich unserer Bilinearform $(x,y) = \sum \overline{x_i} y_i$. Also ist ein Vektor genau dann ein Codewort, wenn es orthogonal auf allen Codewörtern des Erzeugendensystem steht.*

Lemma 3.6 *Sei $x \in \mathbb{F}_4^6$, $s := x_1 + x_2$*
Dann ist $x \in \mathcal{H}$ genau dann, wenn

a) $s = x_1 + x_2 = x_3 + x_4 = x_5 + x_6$ *und*

b) $x_i + x_j + x_k = s \cdot \omega^{(-1)^{(i+j+k+1)}} \quad \forall i \in \{1,2\}, j \in \{3,4\}, k \in \{5,6\}$

*Bemerkung: s heißt **Steigung**, die zweite Bedingung nennen wir **Hexacode-Kriterium**.*

Beweis: „ $\Rightarrow$ “ : Für die Vektoren v_i des Erzeugendensystem (s. Def.(3.4)) gelten die beiden Bedingungen. Damit gelten sie auch für alle Linearkombinationen, also für alle Codewörter.
“ $\Leftarrow$ “ : $x \in \mathbb{F}_4^6$ erfülle die beiden Kriterien $\Rightarrow$ $(x, v_1) = \sum_{i=1}^6 x_i \cdot \overline{v_{1i}} =$

$$x_1\overline{\omega} + x_2\omega + x_3\overline{\omega} + x_4\omega + x_5\overline{\omega} + x_6\omega \overset{\overline{\omega}=\omega+1}{=} \omega \underbrace{(x_1 + x_2)}_{=s} + x_1 + \omega \underbrace{(x_3 + x_4)}_{=s} + x_3 + \omega \underbrace{(x_5 + x_6)}_{=s} + x_5 =$$

$$3\omega s + x_1 + x_3 + x_5 \overset{Hexacode-Krit.}{=} \omega s + \omega^{1+3+5+1} = \omega s + \omega s = 0 \Rightarrow x \in < v_1 >^{\perp}$$
$$(x, v_2) = x_1\omega + x_2\overline{\omega} + x_3\omega + x_4\overline{\omega} + x_5\overline{\omega} + x_6\omega = 3\omega s + x_2 + x_4 + x_5 = \omega s + \omega^{2+4+5+1} = \omega s + \omega s = 0 \Rightarrow x \in < v_1, v_2 >^{\perp}$$
$$(x, v_3) = x_1\overline{\omega} + x_2\omega + x_3\omega + x_4\overline{\omega} + x_5\omega + x_6\overline{\omega} = 3\omega s + x_1 + x_4 + x_6 = \omega s + \omega^{1+4+6+1} = \omega s + \omega s = 0 \Rightarrow x \in < v_1, v_2, v_3 >^{\perp} = \mathcal{H}^{\perp} = \mathcal{H}$$ □

Satz 3.7

(i) Das Minimalgewicht von $\mathcal{H}$ ist 4. Hexacodewörter haben ein Gewicht von 0, 4 oder 6.

(ii) $\mathcal{H}$ ist ein Hexacode.

Beweis: Zu (i): Das Gewicht jedes Hexacodeworts ist durch 2 teilbar, da die Gewichte der Elemente $v_1, ..., v_4$ des Erzeugendensystems durch 2 teilbar sind. Sei nun $x \in \mathcal{H}$ mit $wt(x) \leq 2$. Damit hat es die Steigung 0, da mindestens einer der Koordinatenblöcke, (x_1, x_2), (x_3, x_4) oder (x_5, x_6), gleich $(0, 0)$ ist. Damit gilt $x_i \neq 0$ und $x_j \neq 0$ für einen Block $i\&j$, $i < j$, und $x_k = 0\ \forall k \in \{1, ..., 6\}\backslash\{i, j\}$ Seien $k, l \notin \{i, j\}$ in unterschiedlichen Blöcken. Dann ist nach dem Hexacodekriterium $0 = \omega^{(-1)^{i+k+l+1}} s = x_i + x_l + x_k = x_i$, also $x_i = 0$ und ebenso $x_j = 0$. Damit ist aber $x = 0$, also gibt es keine Hexacodewörter mir Gewicht 2. v_1 ist ein Hexacodewort mit Gewicht 6 und $v_1 + v_2 = (11|11|00)$ eines mit 4.

Zu (ii): Nach Bem.(3.5) ist $Dim(\mathcal{H}) = 3$ und nach (i) $wt(\mathcal{H}) = 4$. □

Satz 3.8 ***(Fehlerkorrektur-Eigenschaften des Hexacodes)***

(i) 3 gegebene Koordinaten sind Teil eines eindeutigen Hexacodeworts, d.h. zu $a_{i_1}, a_{i_2}, a_{i_3} \in \mathbb{F}_4$ mit $i_1, i_2, i_3 \in \{1, ..., 6\}$ pw. vers. existiert genau ein Hexacodewort $h \in \mathcal{H}$ mit $h_{i_j} = a_{i_j}\ \forall j = 1, 2, 3$.

(ii) Für 5 gegebene Koordinaten gibt es genau ein Hexacodewort, dass mindestens 4 dieser Koordinaten enthält, d.h. zu $a_{i_1}, a_{i_2}, a_{i_3}, a_{i_4}, a_{i_5} \in \mathbb{F}_4$ mit $i_1, i_2, i_3, i_4, i_5 \in \{1, ..., 6\}$ pw. vers. existiert genau ein Hexacodewort $h \in \mathcal{H}$ und ein $k \in \{1, ..., 5\}$ mit $h_{i_j} = a_{i_j}\ \forall j \in \{1, ..., 5\}\backslash\{k\}$.

Beweis: Zu (i): Seien $a_{i_1}, a_{i_2}, a_{i_3} \in \mathbb{F}_4$ mit $i_1, i_2, i_3 \in \{1, ..., 6\}$ und $i_1 < i_2 < i_3$. $\Psi : \mathcal{H} \to \mathbb{F}_4^3,\ h \mapsto (h_{i_1}, h_{i_2}, h_{i_3})$ sei die Projektion auf die drei Koordinaten i_1, i_2 und i_3.

Ψ injektiv: Sei $h \in \mathcal{H}$ mit $\Psi(h) = 0$. Dann ist $wt(h) \leq wt(\Psi(h)) + 3 = 3 \overset{d(\mathcal{H})=4}{\Rightarrow} h = 0$.
$\overset{Dimensionsgründe}{\Longrightarrow} \Psi(\mathcal{H}) = \mathbb{F}_4^3$. Also ist Ψ ein Isomorphismus. $\Psi^{-1}(a_{i_1}, a_{i_2}, a_{i_3}) \in \mathcal{H}$ ist dann das gesuchte Hexacodewort.

Zu (ii): Seien $a_{i_1}, a_{i_2}, a_{i_3}, a_{i_4}, a_{i_5} \in \mathbb{F}_4$ mit $i_1, i_2, i_3, i_4, i_5 \in \{1, ..., 6\}$ und $i_1 < i_2 < i_3 < i_4 < i_5$. Sei $k \in \{1, ..., 6\}\backslash\{i_1, ..., i_5\}$ die fehlende Koordinate und $\varphi : \mathbb{F}_4^6 \to \mathbb{F}_4^5$ sei die Projektion auf die 5 anderen Koordinaten.

$\varphi|_{\mathcal{H}}$ ist injektiv: Sei $h \in \mathcal{H}$ mit $\Psi(h) = 0$. Dann ist $wt(h) \leq wt(\varphi(h)) + 1 = 1 \overset{d(\mathcal{H})=4}{\Rightarrow} h = 0$. Also ist $\varphi(\mathcal{H})$ ein [5,3,3]-Code. Für $h \in \mathcal{H}$ def. $S(h) := \{x \in \mathbb{F}_4^5 |\ wt(\varphi(h) - x) \leq 1\}$. Die S(h) sind dann disjunkt und

$$|\bigcup_{h \in \mathcal{H}} S(h)| = \sum_{h \in \mathcal{H}} |S(h)| = |\mathcal{H}| \cdot |S(h)| = 4^3 \cdot (1 + 5 \cdot 3) = 4^5 = |\mathbb{F}_4^5|.$$

Also ist $\varphi(\mathcal{H})$ ein perfekter, 1-fehlerkorrigierender Code. Zu $a := (a_{i_1}, ..., a_{i_5})$ existiert dann genau ein $h \in \mathcal{H}$ mit $a \in S(h)$, also $wt(\varphi(h) - a) \leq 1$. h ist dann das Hexacodewort mit den gewünschten Eigenschaften. □

Nun untersuchen wir die Automorphismengruppe des Hexacodes. Die Gruppe $Z \cong C_3$ operiert auf $\mathcal{H}$ durch Multiplikation mit Potenzen von ω.

$S \cong S_4$ operiert auf $\mathcal{H}$ wie folgt:
Es ist $S = V \rtimes T$ mit $V \cong C_2 \times C_2$ und $T \cong S_3$. Dann operiert V, indem sie in 2 von

den 3 Blöcken die Koordinaten innerhalb der Blöcke vertauscht. T operiert durch Permutation der Blöcke, wobei die Reihenfolge der Elemente jeweils gleich bleiben. Da die Gruppen jeweils Basiselemente auf Basiselemente von $\mathcal{H}$ abbilden, ist die Operation wohldefiniert und es gilt $Z, S \leq Aut(\mathcal{H})$.

Satz 3.9 ***(Charakterisierung von*** $Aut^*(\mathcal{H})$***)***
Sei $Aut^*(\mathcal{H}) = \{g \in Mon^*(6, \mathbb{F}_4) |\ g(\mathcal{H}) = \mathcal{H}\}$ *die Automorphismengruppe des Hexacodes.* $Aut^*(\mathcal{H})$ *operiert auf* $X := \{< e_1 >, ..., < e_6 >\}$. $\pi' : Aut^*(\mathcal{H}) \to Sym(X) = S_6$ *sei die Permutationsdarstellung.*

Dann gilt

(i) $\pi'(S) \cong S_4$ *und* $\pi'(Aut^*(\mathcal{H})) = S_6$

(ii) $Kern(\pi') = Z \cong C_3$

(iii) $|Aut^*(\mathcal{H})| = 3 \cdot 6! = 2^4 \cdot 3^3 \cdot 5 = 2160$

(iv) $\pi'(Aut(\mathcal{H})) = A_6$ *und damit* $|Aut(H)| = 2^3 \cdot 3^3 \cdot 5 = 1080$

Beweis: Sei $X = \{1, ...6\}$ mit der üblichen Nummerierung. Dann ist

$$\pi'(S) =< (1,3)(2,4), (1,2)(3,4), (1,5)(2,6) > \cong S_4.$$

S ist transitiv auf X, aber imprimitiv ($\{\{< e_1 >, < e_2 >\}, \{< e_3 >, < e_4 >\}, \{< e_5 >, < e_6 >\}\}$ ist invariante Partition).

$\alpha := (A, \sigma)$ mit σ der nicht-triviale Körperautomorphismus und $A = \begin{pmatrix} 1 & & & & & \\ & 0 & 1 & & & \\ & 1 & 0 & & & \\ & & & 1 & & \\ & & & & \omega & \\ & & & & & \overline{\omega} \end{pmatrix}$

Es ist $\alpha \in Aut^*(\mathcal{H})$ ($\alpha \in^* (6, \mathbb{F}_4)$ und $\alpha(v_i) \in \mathcal{H}$). Es gilt $\alpha^2 = Id$: Sei $h \in \mathcal{H}$

$$\Rightarrow\ \alpha^2(h) = \alpha(Diag(\sigma(h_1), \sigma(h_3), \sigma(h_2), \sigma(h_4), \omega\sigma(h_5), \overline{\omega}\sigma(h_6))) =$$

$$Diag(h_1, h_2, h_3, h_4, \omega\overline{\omega}h_5, \overline{\omega}\omega h_6) = h$$

α operiert auf X als Transposition $(2,3)$. Also $\pi'(< \alpha >) =< (2,3) >$ und damit

$$\pi(Aut^*(\mathcal{H})) =< (1,3)(2,4), (1,2)(3,4), (1,5)(2,6), (2,3) >= S_6.$$

Zu (ii): Sei $\mu \in Kern(\pi')$. $\Rightarrow g \in Diag(6, \mathbb{F}_4) \rtimes \Gamma,\ g(00|11|11) = (00|ab|cd)$

$$\overset{Steigung\ =0}{\Rightarrow}\ a = b \wedge c = d\ \overset{Hexacode.-Krit.}{\Rightarrow}\ 0 = 0 + a + c\ \Rightarrow\ a = b = c = d.$$

Analog gilt $g(e_1) = ae_1,\ g(e_2) = ae_2$, also $g = \omega^j I_6$ oder $g = (\omega^j I_6, \sigma)$, σ bezeichne den nicht-trivialen Körperautomorphismus $c \mapsto c^2$. Damit ist $Z =< \omega^j I_6 > \leq Kern(\pi')$. Wäre $g = (\omega^j I_6, \sigma)$, so wäre auch $(I_6, \sigma) \in Kern(\pi')$. Es gilt aber $(01|01|\omega\overline{\omega}) \in \mathcal{H}$ (orthogonal auf allen Codewörtern des Erzeugendensystems) und $\sigma(01|01|\omega\overline{\omega}) = (01|01|\overline{\omega}\omega) \notin \mathcal{H}$. Also $Z = Kern(\pi_1)$.

Zu (iii): Nach (i) und (ii) ist $|Aut^*(\mathcal{H})| = |Kern(\pi')|6! = 3 \cdot 6! = 2^4 3^3 \cdot 5$.

Zu (iv) $[Aut^*(\mathcal{H}) : Aut(\mathcal{H})] = |Aut(\mathbb{F}_4)| = 2$. Wegen $Z = Kern(\pi') \leq Aut(\mathcal{H})$ ist damit $|\pi(Aut(\mathcal{H}))| = 6!/2$, also $\pi'(Aut(\mathcal{H})) = A_6$ und $|Aut(H)| = 2^3 \cdot 3^3 \cdot 5 = 1080$. □

4 Der binäre Golaycode

Definition 4.1 ***(Golaycode)***
Der binäre Golaycode bezeichnet einen [24,12,8]-Code über $\mathbb{F}_2$.
Dies ist üblicherweise der erweiterte Golaycode, der aus dem [23,12,7]-Golaycode durch hinzufügen eines Kontrolbits hervorgeht (sodass alle Codewörter ein gerades Gewicht haben). In diesem Vortrag verwende ich nur den erweiterten Golaycode. Bez.: $\mathcal{C}, \mathcal{C}_{24}, \mathcal{G}$.

Ω bezeichne eine 24-elementige Menge. Dann ist $Pot(\Omega) = \{0,1\}^{\Omega}$, die Menge aller charakteristischen Funktionen, ein 24-dimensionaler $\mathbb{F}_2$-Vektorraum mit

$$A + B \;=\; (A \backslash B) \;\cup (B \backslash A) \;=\; (A \cup B) \backslash (A \cap B) \quad \forall A, B \in Pot(\Omega)$$

$$1A = A \; und \; 0A = \emptyset \; \forall A \in Pot(\Omega)$$

$Pot(\Omega)$ ist also isomorph zu $\mathbb{F}_2^{24}$.

Auf $Pot(\Omega)$ kann man die Gewichtsfunktion definieren: $wt : Pot(\Omega) \to \mathbb{N}_0, \; A \mapsto |A|$

Die Standard-Basis von $Pot(\Omega)$ seien alle einelementigen Mengen $\{x\}$. Dann ist die Gruppe der Monomialtransformationen $Mon(Pot(\Omega)) = Sym(\Omega) \cong S_{24}$, wobei $Sym(\Omega)$ auf $Pot(\Omega)$ durch Anwenden auf jedes Mengenelement operiert. Nach Bem.(3.3) ist

$$Mon^*(Pot(\Omega)) = Mon(Pot(\Omega)) = Sym(\Omega).$$

Mit $AB := A \cap B$ wird $Pot(\Omega)$ zu einer $\mathbb{F}_2$-Algebra.
$Pot(\Omega)_g := \{A \in Pot(\Omega) \mid |A| \; ist \; gerade\}$ ist eine Teilalgebra von $Pot(\Omega)$.

$(A, B) := |A \cap B| \; (mod \; 2)$ ist eine symmetrische Bilinearform auf $Pot(\Omega)$.

Ω kann man in eine geordnete Partition Ξ aus sechs 4-elementigen Mengen $K_1, ..., K_6$ zerlegen. Die K_i heißen Spalten. Dann sei $l : \Omega \to \mathbb{F}_4$ eine Abbildung, die eingeschränkt auf jede der K_i bijektiv ist. l heißt eine skalare Labelabbildung.

Ω kann man dann folgendermaßen darstellen:

	K_1 K_2	K_3 K_4	K_5 K_6
0			
1			
ω			
$\overline{\omega}$			

Die Zeilen der oberen Darstellung sind die $R_c = l^{-1}(c)$ für $c \in \mathbb{F}_4$.

Somit kann man ein $x \in \Omega$ mit (c,i) identifizieren, wobei $c = l(x)$ und i so gewählt, dass $x \in K_i$ gilt. Ω steht also in Bijektion zu der Menge $\Omega_{(\Xi,l)} := \mathbb{F}_4 \times \{1, ..., 6\}$. Ψ sei die Bijektion.

Zur skalaren Labelabbildung kann man einen $\mathbb{F}_2$-Vektorraum-Homomorphismus

$$\mathcal{L} : Pot(\Omega) \to \mathbb{F}_4^6, \; A \mapsto \; (\mathcal{L}_1(A), ..., \mathcal{L}_6(A)) \; mit \; \mathcal{L}_i(A) := \sum_{x \in A \cap K_i} l(x),$$

die sogenannte (6-Tubel-)Labelabbildung definieren. Die $\mathcal{L}_i$ sind die i-ten Komponenten der Labelabbildung.

Jeder Menge kann man dann ein Label zuordnen. So hat zum Beispiel die Menge

	K_1	K_2	K_3	K_4	K_5	K_6
0	1					
1		1	1	1		
ω			1		1	
$\overline{\omega}$			1			1

das Label $(01|01|\omega\overline{\omega})$.

Definition 4.2 *Eine Menge $A \in Pot(\Omega)$ heißt **ausgewogen**, falls $|A \cap K_i|$ gerade für alle K_i bzw. ungerade für alle K_i ist. Dann nennen wir A gerade oder von gerader Parität bzw. ungerade oder von ungerader Parität.*

*A heißt **wohlausgewogen**, falls zusätzlich $|A \cap R_0|$ gerade bzw. ungerade ist.*

Lemma 4.3

(i) Für $S,T \in Pot(\Omega)$ ist $i_{S,T} : Pot(\Omega) \to \mathbb{F}_2,\ A \mapsto (A,S)+(A,T) = (A,S+T)$ eine Linearform.

(ii) Die Linearformen $i_{(K_1,K_2)},...,i_{(K_1,K_6)}$ und $i_{(K_1,R_0)}$ sind linear unabhängig.

(iii) $\mathcal{B} := \bigcap_{j=2}^{6} Kern(i_{(K_1,K_j)})$ hat Dimension 19 und es gilt: $A \in \mathcal{B} \Leftrightarrow A$ ist ausgewogen.

(iv) $\mathcal{W} := \mathcal{B} \cap Kern(i_{(K_1,R_0)})$ hat Dimension 18 und es gilt: $A \in \mathcal{W} \Leftrightarrow A$ ist wohlausgewogen.

Beweis: Zu (i): klar.
Zu (ii): Sei $(a_1,...,a_6) \in \mathbb{F}_2^6$ mit $f := a_1 i_{(K_1,R_0)} + \sum_{j=2}^{6} a_j i_{(K_1,K_j)} = 0$. Dann muss f aber auch alle 1-el. Mengen in Ω auf 0 abbilden, also auch Elemente, die nur in K_1+K_j liegen. Damit gilt $a_2 = ... = a_6 = 0$. Es gilt $i_{K_1,R_0} \neq 0$, also ist auch $a_1 = 0$.
Zu (iii): $Dim(Kern(i_{(K_1,K_j)})) = 23$. Da $i_{(K_1,K_2)},...,i_{(K_1,K_6)}$ l.u., ist $Dim(\mathcal{B}) = 24-5 = 19$. $A \in \mathcal{B} \Leftrightarrow i_{(K_1,K_i)}(A) \equiv 0\ (mod\ 2)\ \forall i = 2,...,6 \Leftrightarrow |A \cap K_1| = |A \cap K_i|\ \forall i = 2,...,6 \Leftrightarrow A$ ausgewogen.
Zu (iv): $Dim(\mathcal{W}) = Dim(\mathcal{B}) - 1 = 18$. $A \in \mathcal{W} \Leftrightarrow A \in \mathcal{B} \ \wedge\ i_{(K_1,R_0)}(A) \equiv 0\ (mod\ 2) \Leftrightarrow A$ wohlausgewogen. □

Lemma 4.4 *$\mathcal{L}$ bildet $\mathcal{W}$ auf $\mathbb{F}_4^6$ ab, ist also eingeschränkt auf $\mathcal{W}$ immer noch surjektiv.*

Beweis: Sei $x \in \mathbb{F}_4^6$. S sei die 6-el. Menge, für die $|A \cap K_i| = 1 \forall i$ und $\mathcal{L}(S) = x$ gilt. Dann ist S ausgewogen.

Falls $x = (0,...,0)$, so ist S nicht wohlausgewogen, aber $S + K_1$ ist es. Also ist $S + K_1 \in \mathcal{W}$ und $\mathcal{L}(S + K_1) = x$.

Falls $x \neq (0,...,0)$ und S nicht wohlausgewogen, so existiert ein $i \in \{1,...,6\}$ mit $\mathcal{L}_i(S) = x_i \neq 0$. Dann ist $S + K_i$ wohlausgewogen und $\mathcal{L}(S + K_i) = x$. □

Definition 4.5 $\mathcal{G} := \mathcal{W} \cap \mathcal{L}^{-1}(\mathcal{H})$

Codewörter aus $\mathcal{G}$ sind also genau die Teilmengen von Ω, die wohlausgewogen sind und ein Hexacodewort als Label besitzen.

Satz 4.6 *$\mathcal{G}$ ist ein Golaycode.*

Beweis: $\nu : \mathbb{F}_4^6 \to \mathbb{F}_4^6/\mathcal{H}$ sei der natürliche Epimorphismus. Dann ist $\mathcal{G} = Kern(\nu \circ \mathcal{L}|_{\mathcal{W}})$. $\Rightarrow$ $Dim(\mathcal{G}) = Dim(\mathcal{W}) - Dim_{\mathbb{F}_2}(\mathbb{F}_4^6/\mathcal{H}) = 18 - 6 = 12$. Also ist $\mathcal{G}$ ein binärer [24,12,d]-Code.

Bleibt zu zeigen, dass das Minimalgewicht d=8 ist: $d \leq 8$, da $K_1+K_2 \in \mathcal{G}$. Sei nun $B \in \mathcal{G}\backslash\{\emptyset\}$ mit $wt(B) = |B| = d$.

Falls B ungerade: Dann hat B in jeder Spalte mindestens ein Element, also $wt(B) \geq 6$. Da B wohlausgewogen, liegen im Schnitt mit der Reihe R_0 auch ungerade viele Elemente. Wäre $wt(B) = 6$, so hätte das Label $\mathcal{L}(B)$ ungerade viele Koordinaten gleich 0, ein Widerspruch zu $\mathcal{L}(B) \in \mathcal{H}$. Also hat B in einer Spalte 3 Elemente $\Rightarrow |B| \geq 5 + 3 = 8$.

Falls B gerade: $\Rightarrow\ \mathcal{L}_i(B) \neq 0 \Leftrightarrow |B \cap K_i| = 2$. Also ist $wt(B) = d \geq 2wt(\mathcal{L}(B))$.

Ann. $d < 8$: Dann ist $wt(\mathcal{L}(B)) < 4$. $\Rightarrow \mathcal{L}(B) = 0$. $\overset{B\neq\emptyset}{\Rightarrow}$ $|B \cap K_i| = 4$ für ein i. Da B wohlausgewogen liegt eine weitere Spalte in B : $|B \cap K_j| = 4$ für ein $j \neq i$, also $|B| = d \geq 4 + 4 = 8$, ein Widerspruch zur Annahme.

Also ist $d = 8$. □

Definition 4.7

- *Eine geordnete Partition P von Ω aus 6 Mengen mit je 4 Elementen heißt ein **geordnetes Sextett**, falls $X_1 + X_2 \in \mathcal{G}\ \forall X_1, X_2 \in P$.*
- *P_u bezeichne das zugehörige **ungeordnete Sextett** (die ungeordnete Partition).*
- *Eine **skalare Labelabbildung** ist eine Abbildung $\varphi : \Omega \to \mathbb{F}_4$ mit $\varphi|_X$ bijektiv $\forall X \in P$ für ein geordnetes Sextett P.*
- *$\Phi : Pot(\Omega) \to \mathbb{F}_4^6,\ A \mapsto\ (\Phi_1(A), ..., \Phi_6(A))$ mit $\Phi_i(A) := \sum_{x\in A\cap K_i} \varphi(x)$ ist die **(6-Tupel-) Labelabbildung** der skalaren Labelabbildung φ. Die Φ_i sind die i-ten Komponenten der Labelabbildung.*
- *Ξ, l, $\mathcal{L}$ (s.o.) sind die Standard-Vertreter von geordnetem Sextett, skalarer Labelabbildung und 6-Tupel-Label-Abbildung.*

Bemerkung 4.8 *Sei (P, φ) ein Paar aus geordneter Partition $P = \{X_1, ..., X_6\}$ und skalarem Label φ.*

- *Analog zu oben kann man einen Golaycode mit P und φ konstruieren. Bezeichnung: $\mathcal{G}(P, \varphi)$. $\mathcal{G}$ bezeichne den Standard-Golaycode $\mathcal{G}(\Xi, l) = \mathcal{G}$.*
- *Die Wahl von P und φ ist nicht eindeutig. So ist zum Beispiel $\mathcal{G}(\{K_3, K_4, K_1, K_2, K_5, K_6\}, l) = \mathcal{G}$. Auch Sextette mit verschiedenen ungeordneten Sextetten können den gleichen Golaycode erzeugen (mit verschiedenen Labelabbildungen).*
- *$\Psi : \Omega \to \Omega_{(P,\varphi)} := \mathbb{F}_4 \times \{1, ..., 6\},\ x \mapsto (l(x), i)$ mit $x \in X_i$ ist eine Bijektion. Sie ermöglicht eine einfache Beschreibung der Elemente von Ω, falls ein Sextett und eine Labelabbildung fest gewählt sind.*

Im folgenden Kapitel werden wir sehen, dass alle Golaycodes linear äquivalent sind. Zunächst untersuchen wir aber noch einige Eigenschaften des Golaycodes $\mathcal{G}$.

Bemerkung 4.9 *Für ein $h \in \mathcal{H}$ definiere $A_h := \{x \in \Omega \mid \Psi(x) = (c, i) \in \Omega_{(\Xi,l)}$ mit $c = h_i\}$ die 6-el. Menge, die vom Label auf h abgebildet wird.*

Dann ist $B_h :=\ K_1 + A_h$ ein Element vom Golaycode $\mathcal{G}$.

Die B_h für $h \in \mathcal{H}$ und die „Doppelspalten“ $K_i + K_j$ erzeugen $\mathcal{G}$.

Satz 4.10

(i) $\Omega \in \mathcal{G}$. *Also ist mit jedem Codewort* B *auch sein Komplement* $\Omega + B$ *ein Codewort.*

(ii) $\mathcal{G}$ *ist ein 4-dividierbarer Code*

(iii) $\mathcal{G}$ *ist selbst-orthogonal.*

(iv) $\mathcal{G}$ *hat das Gewichtspolynom* $A(x) = 1 + 759x^8 + 2576x^{12} + 759x^{16} + x^{24}$.

Beweis: Zu (ii): Die Gewichte alles Codewörter des Erzeugendensystems (s. Bem(4.9)) sind durch 4 teilbar, damit ist das Gewicht jedes Codeworts durch 4 teilbar. Siehe dazu den Beweis in [Wi].

Zu (iii): Nach (i) und(ii) gibt es nur Codewörter des Gewichts 0,8,12,16 und 24 (zu jedem Gewicht gibt es tatsächlich mindestens ein Codewort). Seien nun $B, C \in \mathcal{G}$. Dann gilt modulo 4:

$$0 \equiv wt(B + C) = wt(B) + wt(C) - 2|B \cap C| \equiv -2|B \cap C| \ (mod\ 4).$$

Also enthält der Schnitt gerade viele Elemente. Damit gilt $(B, C) = [|B \cap C|] \ (mod\ 2) \cong 0$, also sind B und C orthogonal zueinander.

Zu (iv): Man verwende den Dualitätssatz von Jessie MacWilliams über das Gewichtspolymom, vergleiche dazu [Wi].

Nun ist es noch hilfreich den Cocode $Pot(\Omega)/\mathcal{G}$ zu betrachten:

Satz 4.11 *Sei* $A \in Pot(\Omega)$ *mit* $|A| \leq 4$.
Dann gilt:

(i) $|A| < 4 \implies \forall C \in A + \mathcal{G},\ C \neq A$ *gilt* $|C| > 4$

(ii) $|A| = 4 \implies$ *Es existieren genau 6 Mengen* $A_1, ..., A_6$ *mit* $|A_i| = 4$ *und* $A + \mathcal{G} = A_i + \mathcal{G}$.

(iii) $Pot(\Omega)/\mathcal{G} = \{A + \mathcal{G} |\ |A| \leq 4\}$

Beweis: Zu (i): Sei $A \in Pot(\Omega)$ mit $|A| < 4$. Sei $C \in Pot(\Omega)$ mit $C \neq A$ und $C + \mathcal{G} = A + \mathcal{G}$. Dann ist $\emptyset \neq A + C \in \mathcal{G}$. Damit gilt $8 \leq wt(A + C) = \underbrace{wt(A)}_{<4} + wt(C) - \underbrace{2wt(A \cap C)}_{\geq 0} \ \Rightarrow\ wt(C) > 4$.

Zu (ii): Nach (i) gibt es $\binom{24}{0} + \binom{24}{1} + \binom{24}{2} + \binom{24}{3} = 2325$ Elemente des Cocodes, die keine Menge mit 4 Elementen enthält. Bleiben $|Pot(\Omega)/\mathcal{G}| - 2325 = 1771 = \frac{1}{6}\binom{24}{4}$ Elemente. Also gibt es ein $A \in Pot(\Omega)$ mit $|A| = 4$ und $M := \{C \in A + \mathcal{G} |\ |C| = 4\}$ hat mindestens 6 Elemente. Hat M gneu 6 Elemente, so folgt die Behauptung. Sein also $A_1, A_2 \in M, A_1 \neq A_2$. Dann ist $8 \leq wt(\underbrace{A_1 + A_2}_{\in \mathcal{G},\ da\ A_1 + \mathcal{G} = A_2 + \mathcal{G}}) \leq 4 + 4 \ \Rightarrow\ A_1 \cap A_2 = \emptyset$. Damit ist $M = \{A_1, ..., A_6\}$ für passende A_i.

Zu (iii): Folgt aus (i) und (ii). □

Folgerung 4.12 *Die* $A + \mathcal{G}$ *für 4-el. Mengen A sind genau die ungeordneten Sextette. Es gibt* $\frac{1}{6}\binom{24}{4} = 1771 = 7 \cdot 11 \cdot 23$ *(ungeordnete) Sextette. Jede 4-elementige Menge ist Teil genau eines Sextetts.*

Lemma 4.13 *Seien $P = \{X_1, ..., X_6\}$ und $P' = \{Y_1, ..., Y_6\}$ ungeordnete Sextette, $P \neq P'$. Dann gilt:*

(i) $\exists i, j$ *mit* $|X_i \cap Y_j| \geq 2$.

(ii) Gilt (evtl. nach Umnummerierung) $|X_1 \cap Y_1| = 3$ *und damit o.B.d.A.* $|X_1 \cap Y_2| = 1$ *und* $|X_2 \cap Y_1| = 1$, *so folgt* $|X_2 \cap Y_3| = 3$ *und* $|X_i \cap Y_j| = 1$ $\forall i, j \in \{3, ..., 6\}$.

Beweis: o.B.d.A. $|X_1 \cap Y_1| \geq |X_i \cap Y_i|$ $\forall i, j \in \{1, ..., 6\}$.

Zu (i): Annahme $|X_1 \cap Y_1| = 1$: Dann gelte, evtl. nach Umnummerierung, $|X_1 \cap Y_2| = |X_1 \cap Y_2| = 1$. Damit ist

$$wt(X_1 + X_2 + Y_1 + Y_2) = 8 + 8 - 2\underbrace{|(X_1 + X_2) \cap (Y_1 + Y_2)|}_{\geq 3} \leq 16 - 2 \cdot 3 = 10$$

Also ist $wt(X_1+X_2+Y_1+Y_2) = 8$, da $X_1+X_2+Y_1+Y_2 \in \mathcal{G}$. Dann muss $|(X_1+X_2)\cap(Y_1+Y_2)| = 4$, also $|X_2 \cap Y_2| = 1$, gelten. Es gelte weiterhin $|X_1 \cap Y_3| = |X_1 \cap Y_4| = |X_3 \cap Y_1| = |X_4 \cap Y_1| = 1$. Damit ergibt sich mit dem gleichen Argument wie oben, folgende Größen der Schnitte $X_i \cap Y_j$:

	Y_1	Y_2	Y_3	Y_4	Y_5	Y_6
X_1	1	1	1	1	0	0
X_2	1	1	1	1	0	0
X_3	1	1	1	1	0	0
X_4	1	1	1	1	0	0
X_5	0	0	0	0		
X_6	0	0	0	0		

Dann gilt aber $|X_5 \cap Y_5| > 1$ oder $|X_5 \cap Y_6| > 1$. Ein Widerspruch zu $|X_1 \cap Y_1|$ maximal.

Zu (ii): Es gilt $|X_1 \cap Y_1| = 3$. Dann gilt o.B.d.A. $|X_1 \cap Y_2| = |X_2 \cap Y_1| = 1$. Dann ist $wt(X_1+X_2+Y_1+Y_2) = 8+8-2|(X_1+X_2)\cap(Y_1+Y_2)| \geq 16-2\cdot 5 = 6 \Rightarrow wt(X_1+X_2+Y_1+Y_2) = 0 \Rightarrow X_1 + X_2 = Y_1 + Y_2 \Rightarrow |X_2 \cap Y_2| = 3$.

Es ist $X_1 + \mathcal{G} + Y_1 + \mathcal{G} = (X_1 + Y_1) + \mathcal{G}$ mit $|X_1 + Y_1| = 4 + 4 - 2\cot 3 = 2$. Für $i, j \notin \{1, 2\}$ gilt dann $|X_i + Y_j| > 4$ nach Satz(4,11), denn $X_i + Y_j \in X_1 + Y_2 + \mathcal{G}$). Also ist

$$|X_i \cap Y_j| = \frac{|X_i| + |Y_j| - |X_i + Y_j|}{2} < \frac{4 + 4 - 4}{2} = 2.$$

Die Verteilung der Schnitte ist dann

	Y_1	Y_2	Y_3	Y_4	Y_5	Y_6
X_1	3	1	0	0	0	0
X_2	1	3	0	0	0	0
X_3	0	0	1	1	1	1
X_4	0	0	1	1	1	1
X_5	0	0	1	1	1	1
X_6	0	0	1	1	1	1

Definition 4.14 ***(Steiner-System)***
Ein Steinersystem S mit Paarametern (a,b,n), $a, b, n \in \mathbb{N}$, ist eine Familie S von b-elementigen Mengen, die Teilmengen einer Menge Ω mit n Elementen sind. Außerdem gelte:

$$A \subseteq \Omega \text{ mit } |A| = a \Rightarrow \exists!\ B \in S :\ A \subseteq B.$$

Satz 4.15 *Sei $A \in Pot(\Omega)$ eine Menge mit 5 Elementen.*

Dann gibt es genau ein 8-el. Codewort von $\mathcal{G}$, das A enthält. Die Menge aller Codewörter mit Gewicht 8 ist also ein (5,8,24)-Steinersystem (auch Witt-Design genannt).

Beweis: Sei $\mathcal{G}_8 := \{B \in \mathcal{G} | \ |B| = 8\}$ und $A \subseteq \Omega$ mit $|A| = 5$. Sei $C \in \mathcal{G}$ mit $n := |A + C| \leq 4$ (ex. nach Satz(4.11)). n ist ungerade, da sonst $wt(C) = |A + C| - |A| + 2|A \cap C| = -5 + |A + C| + 2wt|A \cap C|$ ungerade wäre.

Annahme n=1: Es ist $1 = wt(A + C) = wt(A) + wt(C) - 2wt(A \cap C) \quad \Leftrightarrow \quad wt(C) = -4 + 2wt(A \cap C) \leq -4 + 2 \cdot 5 = 6$. Ein Widerspruch.

Also ist n=3 und damit $wt(A \cap C) = (5 - 3 + wt(N))/2 \geq (2 + 8)/2 = 5$. Wegen $wt(A) = 5$ ist damit $A \subseteq C$. $C \in \mathcal{G}_8$, denn $wt(C) = 3 - 5 + 2 \cdot 5 = 8$. Es gibt höchstens ein solches C aufgrund des Minimalabstands von $\mathcal{G}$.

5 Eigenschaften der Automorphismengruppe des Golaycodes

Die Automorphismengruppe unseres Golaycodes ist $Aut^*(\mathcal{G}) = Aut(\mathcal{G}) = \{f \in S_{24} |\ f(\mathcal{G}) = \mathcal{G}\}$. Im Folgenden werden wir sehen, dass $Aut(\mathcal{G})$ gleich M_{24}, der fünften Mathieu-Gruppe, ist. Also haben wir diese dann mit $M_{24} := Aut(\mathcal{G})$ konstruiert.

Definition 5.1 $\mathfrak{N} := Stab_{Aut(\mathcal{G})}(\Xi_u)$ *operiert auf* Ξ_u *durch Anwenden.* $\pi_0 : \mathfrak{N} \to Sym\Xi_u$ *sei die zugehörige Permutationsdarstellung und* L *der Kern.*

Satz 5.2

(i) $\mathbb{F}_4^6$ *operiert auf* Ω *bezüglich dem Sextett* Ξ *und dem Label* l *durch*

$$\mathbb{F}_4^6 \times \Omega \to \Omega,\ (v, x) = (v, \Psi^{-1}(c, i)) \mapsto v^{\pi_1}(x) := \Psi^{-1}(c + v_i, i)$$

Schreibe $\pi_1 : \mathbb{F}_4^6 \to Sym(\Omega),\ \pi_1(v) := v^{\pi_1}$ *für die Permutationsdarstellung.* π_1 *ist injektiv.*

(ii) Damit operiert $\mathbb{F}_4^6$ *auf* $Pot(\Omega)$ *durch Anwenden der oberen Operation auf jedes Mengenelement. Die Operation ist linear.* $\pi(\mathbb{F}_4^6) \leq Mon(Pot(\Omega)) = Sym(\Omega)$

(iii) $\mathcal{H}^{\pi_1} := \pi_1(\mathcal{H}) \leq Aut(\mathcal{G})$.

(iv) $Mon^*(6, \mathbb{F}_4)$ *operiert auf* Ω *bezüglich dem Sextett* Ξ *und dem Label* l *durch*

$$Mon^*(6, \mathbb{F}_4) \times \Omega \to \Omega,\ (g, x) = ((\sigma, D, \tau), \Psi^{-1}(c, i)) \mapsto g^{\pi_1}(x) := \Psi^{-1}(\sigma(c)D_i, \tau(i))$$

Schreibe ebenfalls $\pi_1 : Mon^*(6, \mathbb{F}_4) \to Sym(\Omega),\ \pi_1(g) := g^{\pi_1}$ *für die Permutationsdarstellung.* π_1 *ist injektiv.*

(v) Damit operiert $Mon^*(6, \mathbb{F}_4)$ *auf* $Pot(\Omega)$ *analog zu oben. Die Operation ist auch linear.*

(vi) $Aut^*(\mathcal{H})^{\pi_1} := \pi_1(Aut^*(\mathcal{H})) \leq Aut(\mathcal{G})$.

Beweis: (i),(ii),(iv),(v) klar. Für $v \in \mathcal{H}$ definiere $A_v := \{x \in \Omega \mid \Psi(x) = (c, i) \in \Omega_{(\Xi,l)}\ mit\ c = v_i\}$ und $B_v := K_1 + A_v \in \mathcal{G}$ wie in Bem.(4.9).

Zu (i): Sei $h \in \mathcal{H}$. Zeige $h^{\pi_1}(\mathcal{G})) = \mathcal{G}$. Es ist

$$h^{\pi_1}(B_v) = h^{\pi_1}(K_1) + h^{\pi_1}(A_v) = K_1 + \{\Psi^{-1}(v_1 + h_1, i), ..., \Psi^{-1}(v_6 + h_6, 6)\} = K_1 + A_{v+h} = B_{v+h}\ \forall v \in \mathcal{H}.$$

Außerdem gilt $h(K_i + K_j) = K_i + K_j$. Also bildet h dieses Erzeugendensystem (s. Bem (4.9)) von $\mathcal{G}$ auf sich ab. Also ist $\mathcal{H} \leq Aut(\mathcal{G})$.

Zu (v): Sei $g = (D, \tau, \sigma) \in Aut^*(\mathcal{H}),\ D \in Diag(n, K),\ \tau \in S_n,\ \sigma \in Aut(\mathbb{F}_4)$. Dann ist

$$g^{\pi_1}(B_v) = g^{\pi_1}(K_1) + g^{\pi_1}(A_v) = K_{\tau(1)} + \{g^{\pi_1}(\Psi^{-1}(v_i, i)) |\ i = 1, ..., 6\} =$$

$$K_{\tau(1)} + \{\Psi^{-1}(\sigma(v_i)D_i, \tau(i)) |\ i = 1, ..., 6\} = K_{\tau(1)} + A_{g^{\pi_1}(v)} = K_1 + A_{g^{\pi_1}(v)} + K_1 + K_{\tau(1)} =$$

$$B_{g^{\pi_1}(v)} + K_1 + K_{\tau(1)} \forall v \in \mathcal{H}.$$

Außerdem gilt $g(K_i + K_j) = K_{\tau(i)} + K_{\tau(j)}$, also auch $Aut^*(\mathcal{H}) \leq Aut(\mathcal{G})$. □

Folgerung 5.3

(i) $(\mathcal{H} \rtimes Aut(\mathcal{H}))^{\pi_1} \leq \mathfrak{N}$

(ii) $\mathcal{H}^{\pi_1} \leq L$.

(iii) $\pi_0 : \mathfrak{N} \to Sym\Xi_u$ *ist surjektiv.*

Beweis: Zu (i): $\mathcal{H}^{\pi_1},\ Aut^*(\mathcal{H})^{\pi_1} \leq \mathfrak{N}$ nach dem Satz oben. Es gilt $\mathcal{H}^{\pi_1} \cap Aut^*(\mathcal{H})^{\pi_1} = \{Id\}$, denn $Aut^*(\mathcal{H})$ erhält die Zeile R_0, aber in $\mathcal{H}$ ist $(0, ..., 0)$ das einzige Element mit dieser Eigenschaft. Damit ist $(\mathcal{H} \rtimes Aut^*(\mathcal{H}))^{\pi_1} = \mathcal{H}^{\pi_1} \rtimes Aut^*(\mathcal{H})^{\pi_1} \leq \mathfrak{N}$.

Zu (ii): $\mathcal{H}^{\pi_1}$ erhält die Spalten: $h^{\pi_1}(K_i) = K_i\ \forall h \in \mathcal{H}$.

Zu (iii): Nach dem Satz über die Eigenschaften von $Aut^*(\mathcal{H})$ (s. Satz(3.9)) operiert $Aut^*(\mathcal{H})$ durch Anwenden auf der Menge $\{< e_1 >, ..., < e_6 >\}$. $Aut^*(\mathcal{H})$ operiert wie S_6 auf der Menge. Damit operiert es auch wie S_6 auf den Spalten K_i, denn $\mathcal{L}(Pot(K_i)) =< e_i >$. □

Satz 5.4 ***(Stabilisator eines ungeordneten Sextetts)***

(i) Der Stabilisator des ungeordneten Sextetts $\mathfrak{N}$ *ist isomorph zu* $\mathcal{H} \rtimes Aut^*(\mathcal{H})$.

(ii) $Stab_{\mathfrak{N}}(K_i)$ *operiert wie* S_4 *auf* K_i.

Beweis: Zu (i): Es gilt $|\mathcal{H} \rtimes Aut^*(\mathcal{H})| = 4^3 \cdot 3 \cdot 6!$ teilt $|\mathfrak{N}|$. Also reicht es zu zeigen: $4^3 \cdot 3 \cdot 6! = |\mathfrak{N}| = |Bild(\pi_0)| \cdot |L| = 6!|L| \ \Leftrightarrow\ |L| = 4^3 \cdot 3$.

Dies ist erfüllt, falls $L =< \mathcal{H}^{\pi_1}, \mu^{\pi_1} >$ mit $\mu \in Aut^*(\mathcal{H})$ und $| < \mu > | = 3$ gilt. Definiere $\mu \in Aut^*(\mathcal{H})$ als die Abbildung „Multiplikation mit ω“, d.h.: $\mu^{\pi_1} =$

K_1	K_2	K_3	K_4	K_5	K_6
○	○	○	○	○	○
↓	↓	↓	↓	↓	↓

Oder genauer: $\mu^{\pi_1}(\Psi^{-1}(c, i)) = \Psi^{-1}(\omega \cdot c, i)\ \ \forall (c, i)\Omega_{(\Xi,l)}$. μ ist in $Aut^*(\mathcal{H})$, da $\mu = Diag(\omega, ..., \omega) \in Aut^*(\mathcal{H})$.

$L \geq < \mathcal{H}^{\pi_1}, \mu^{\pi_1} >$ ist klar.

$L \leq < \mathcal{H}^{\pi_1}, \mu^{\pi_1} >$: Sei $g \in L$. $a_i := g(\Psi^{-1}(0, i)) \overset{Fehlerkor.\ von\ \mathcal{H},\ s.\ Satz(3.8)}{\Longrightarrow} \exists!\ h \in \mathcal{H}$ mit $h = (l(a_1)l(a_2)|l(a_3) * | * *)$. Indem man g durch $g \cdot h^{\pi_1}$ ersetzt, kann man o.B.d.A. annehmen, dass $l(a_1) = l(a_2) = l(a_3) = 0$ gilt.

Wähle A als die Menge

	K_1	K_2	K_3	K_4	K_5	K_6
0		1	1			
1	1					
ω	1					
$\overline{\omega}$	1					

Dann ist $B = K_1 + R_0 \in \mathcal{G}$ das eindeutige 8-el. Codewort mit $A \subset B$.

$$g(A) = g(K_1) + \{g(\Psi^{-1}(0,1)), g(\Psi^{-1}(0,2)), g(\Psi^{-1}(0,3))\} = K_1 + \{\Psi^{-1}(0,1), \Psi^{-1}(0,2), \Psi^{-1}(0,3)\} =$$

$$A \overset{A=g(A)\subset(B)}{\Rightarrow} g(B) = B\ \Rightarrow g(\Psi^{-1}(0,i)) = \Psi^{-1}(0,i)\ \forall i = 1, ..., 6$$

$L_0 := \{f \in L |\ f(\Psi^{-1}(0,i)) = \Psi^{-1}(0,i)\ \forall i = 1, ..., 6\}$ operiert auf jedem K_i und insb. auf jedem $K_i^* = K_i \backslash \{0\}$.

Es gilt also nun $g \in L_0$. Zeige $g \in < \mu^{\pi_1} >$: Zunächst sei $f \in L_0$ so gewählt, dass f auf einem K_i trivial operiert. Seien $j,k,l,p,q \in \{1,...,6\}$ so gewählt, dass $\{\{i,n\},\{j,k\},\{p,q\}\} = \{\{1,2\},\{3,4\},\{5,6\}\}$ gilt, also sie die Koordinatenblöcke von $\mathcal{H}$ bilden. Für $c \in \mathbb{F}_4^*$ definiere $B' \in \mathcal{G}$ als das Codewort, das $A' := K_i \backslash \{\Psi^{-1}(c,i)\} + \Psi^{-1}(0,j),(0,k)\})$ enthält.
Für $i = 1,\ c = \omega$ und $(j,k) = (3,4)$ ist zum Beispiel B' die Menge

	K_1	K_2	K_3	K_4	K_5	K_6
0	1		1	1		
1	1					
ω		1			1	1
$\overline{\omega}$	1					

Beh.: $B' = A' + Psi^{-1}(\{(c,n),(c,p),(c,q)\})$
Denn:

$$|B' \cap K_m| = \begin{cases} 1, & falls\ m \neq i \\ 3, & falls\ m = i \end{cases} \text{ und } |B' \cap R_0| = 3 \Rightarrow \text{ B' wohlausgewogen}$$

$$\mathcal{L}_m(B') = \begin{cases} 0, & falls\ m = j \ \vee \ m = k \\ c, & sonst \end{cases} \Rightarrow \mathcal{L}(B') \text{ ist } (cc|cc|00),(cc|00|cc) \text{ oder } (00|cc|cc).$$ Also ist es ein Hexacodewort. Womit B' die angegebene Form haben muss.

Wegen $g(A') = A'$ ist dann $g(B') = B' \overset{c,j,k \text{ beliebig gewählt}}{\Longrightarrow}$ f operiert auf jedem K_i trivial.

Die Operation von L_0 auf jeder der K_i^* liefert einen Homomorphismus von L_0 nach $Sym(K_i^*) \cong S_3$ Somit induziert g ein Permutation aus S_3. μ^{π_1} induziert einen 3-Zykel auf jedem K_1^*. Operiert g auf einem K_i^* als 3-Zykel, so operiert $g\mu^{\pi_1}$ oder $g(\mu^2)^{\pi_1}$ trivial auf diesem K_i^* und damit trivial auf Ω.

Es bleibt noch auszuschließen, dass g als Transposition auf jeder K_i^* operiert. Man nehme an, dies gelte. O.B.d.A. fixiert g $\Psi^{-1}(1,1)$ (sonst g durch $g\mu^{\pi_1}$ oder $g(\mu^2)^{\pi_1}$ ersetzen). Dann fixiert g aber die folgenden zwei Codewörter punktweise:

	K_1	K_2	K_3	K_4	K_5	K_6
0	1	1	1	1		
1	1	1	1	1		
ω						
$\overline{\omega}$						

	K_1	K_2	K_3	K_4	K_5	K_6
0	1	1			1	1
1	1	1			1	1
ω						
$\overline{\omega}$						

Also fixiert g die ganze Zeile R_1. Damit vertauscht g R_ω und $R_{\overline{\omega}}$ und operiert somit wie der nicht-triviale Körperautomorphismus von $\mathbb{F}_4$. Dieser liegt aber nicht in $Aut^*(\mathcal{H})$ (s. Satz(3.9)) und auch nicht in $Aut(\mathcal{G})$, denn das Codewort

	K_1	K_2	K_3	K_4	K_5	K_6
0	1		1			1
1		1		1		1
ω					1	1
$\overline{\omega}$						

würde von g auf

	K_1	K_2	K_3	K_4	K_5	K_6
0	1		1			1
1		1		1		1
ω						
$\overline{\omega}$					1	1

abgebildet. Dieses ist aber kein Codewort, da die Menge das Label $(01|01|\overline{\omega\omega}) \notin \mathcal{H}$ besitzt. Dies ist ein Widerspruch zur Annahme $g \in Aut(\mathcal{G})$.

Also ist $g \in < \mu^{\pi_1} >$. Damit ist $L =< \mathcal{H}^{\pi_1}, \mu^{\pi_1} >$ und $\mathfrak{N} = (\mathcal{H} \rtimes Aut^*(\mathcal{H}))^{\pi_1}$.

Zu (i): Es ist $L \leq Stab_{\mathfrak{N}}(K_i)$. Oben haben wir gesehen, dass L wie A_4 auf K_i operiert.

$\alpha := (A, \sigma)$ mit σ der nicht-triviale Körperautomorphismus und $A = \begin{pmatrix} 1 & & & & & \\ & 1 & & & & \\ & & 1 & & & \\ & & & 1 & & \\ & & & & \omega & \\ & & & & & \overline{\omega} \end{pmatrix}$

Es ist $\alpha \in Aut^*(\mathcal{H})$ und $\alpha^2 = Id$ (es ist das selbe α wie in Satz(3.9)). α^{π_1} operiert auf K_1 als Transposition. Ist $i \neq 1$, so wähle α entsprechend anders durch Vertauschen der Koordinatenblöcke $(\{1,2\},\{3,4\},\{5,6\})$ in A. Insgesamt gibt es ein Element aus $Stab_{\mathfrak{N}}(K_i)$, das als Transposition auf K_i operiert. Also induziert $Stab_{\mathfrak{N}}(K_i)$ $Sym(K_i) \cong S_4$ auf K_i. □

Folgerung 5.5 $|\mathfrak{N}| = |\mathcal{H}| \cdot |Aut^*(\mathcal{H})| = 4^3 \cdot 2^4 \cdot 3^3 \cdot 5 = 2^{10} \cdot 3^3 \cdot 5$

Beweis: (3.9) (Ordnung von $Aut^*(\mathcal{H})$) und (5.4) (Struktur von $\mathfrak{N}$)

Lemma 5.6 *Sei (P, φ) ein Paar aus geordneter Partition mit sechs 4-el. Mengen und skalarem Label.*
Dann gibt es genau ein $\sigma \in Sym(\Omega)$ mit $\sigma(P, \varphi) = (\Xi, l)$. Außerdem ist dann $\sigma(\mathcal{G}(P, \varphi)) = \mathcal{G}(\Xi, l) = \mathcal{G}$.

Beweis: (P, φ) und (Ξ, l) ordnen jedem Element aus Ω jeweils eine eindeutige Koordinate aus $\mathbb{F}_4 \times \{1, ..., 6\}$ zu. Also gibt es genau ein $\sigma \in Sym(\Omega)$, das die Koordinaten überträgt. Trivialerweise bildet σ wohlausgewogen Mengen auf wohlausgewogen Mengen ab. Sei nun $B \in \mathcal{G}(P, \phi)$, Φ die 6-Tupel-Labelabbildung von (P, φ) und $P = \{X_1, ..., X_3\}$. Dann ist

$$\mathcal{L}(\sigma(B)) = (\sum_{x \in \sigma(B) \cap K_i} l(x))_{i=1,...,6} = (\sum_{x \in \sigma(B) \cap \sigma(X_i)} l(x))_{i=1,...,6} =$$

$$(\sum_{y \in B \cap K_i} l(\sigma^{-1}(y)))_{i=1,...,6} = (\sum_{y \in B \cap X_i} \phi(y))_{i=1,...,6} = \Phi(B) \in \mathcal{H}.$$

□

Satz 5.7 ***(Erzeugen einer Labelabbildung)***
Sein $\mathcal{C}$ ein Golaycode und $P = \{X_1, ..., X_6\}$ ein geordnetes Sextett (bzgl. $\mathcal{C}$).
Dann gibt es genau 192 skalare Labelabbildungen φ, sodass $\mathcal{G}(P, \varphi) = \mathcal{C}$ ist.

Beweis: $M := X_1 \times A_2 \times \mathbb{F}_4$ mit $A_2 := \{(x, y) \in_2 \times X_2 |\ x \neq y\}$ („Anti-Diagonale“), $N := \{\varphi$ skalare Labelabbildung $|\ \mathcal{C} = \mathcal{G}(P, \varphi)\}$. M hat die Kardinalität $4 \cdot 12 \cdot 4 = 192$. Das Ziel ist es, eine Bijektion zwischen M und N zu finden.

Vorbemerkung 1: Für $x \in X_1, y \in X_2$ und $p \in X_3$ bezeichne $O(x, y, p)$ die eindeutige 8-el. Menge, das die 5-el. Menge $X_1 - \{x\} + \{y, p\}$ enthält. Da $O(x, y, p)_1 + X_i$ für alle $1 < i \leq 6$ gerade ist, ist $O(x, y, p) \cap X_i$ eine 1-el. Menge.

Vorbemerkung 2: Seien nun $x \in X_1, y, z \in X_2$ mit $y \neq z$ und $p, q \in X_3$. Dann ist $O(x, y, p) \cap O(x, z, q) \cap (X_3 + X_4 + X_5 + X_6)$ eine 1-el. Menge.
Bew.: $O(x, y, p) \neq O(x, z, q) \Rightarrow 8 \leq |O(x, y, p) + O(x, z, q)| = |O(x, y, p)| + |O(x, z, q)| - 2|O(x, y, p) \cap O(x, z, q)| = 16 - 2|O(x, y, p) \cap O(x, z, q)| \Rightarrow 4 \geq |O(x, y, p) \cap O(x, z, q)| = |X_1 - \{x\}| + |O(x, y, p) \cap O(x, z, q) \cap (X_3 + X_4 + X_5 + X_6)| = 3 + |O(x, y, p) \cap O(x, z, q) \cap (X_3 + X_4 + X_5 + X_6)| \Rightarrow |O(x, y, p) \cap O(x, z, q) \cap (X_3 + X_4 + X_5 + X_6)| = 1$ da sich zwei Codewörter in einer Menge mit gerade vielen Elementen schneiden.

Sei $w \in X_3$ fest. $F : N \to M, \varphi \mapsto (a, (b, c), \delta)$ mit $\varphi(a) = \varphi(b) = 0, \varphi(c) = 0$ und $\varphi(w) = 0$. F soll die gesuchte Bijektion sein.

Dazu ist zunächst zu zeigen, dass F injektiv ist: Sei $\varphi \in N$ mit $F(\varphi) = (a, (b, c), \delta)$ wie oben. Zunächst zeigen wir, dass dies φ auf $(X_3 + X_4 + X_5 + X_6)$ festlegt. Es ist $O' := O(a, c, w)$ durch $\mathcal{G}(P, \varphi)$ und $(a, (b, c), w)$ eindeutig festgelegt. Ebenso $h := \Phi(O') = (01|\delta * | * *) \in \mathcal{H}$ durch O', also durch $F(\varphi)$ festgelegt nach den Fehlerkorrektur-Eigenschaften von $\mathcal{H}$ (s. Satz (3.8)). Es ist nach Steigung und Hexacode-Kriterium (s. Lemma(3.6)) $\{\delta, h_4, h_5, h_6\} = \mathbb{F}_4$. $O_q := O(a, b, q)$ für ein $q \in X_3$, unabhängig von φ eindeutig bestimmt. Dann ist wieder nach Bem. (3,x) $\Phi(O_2) = (00|\lambda\lambda|\lambda\lambda)$. Also haben alle Elemente aus $O_w \cap (X_3 + X_4 + X_5 + X_6)$ das Label δ, und zwar unabhängig von φ. Ebenso ist das Label der Elemente aus $O_q \cap (X_3 + X_4 + X_5 + X_6)$ durch $\varphi(x)$ mit $\{x\} = O_q \cap O'$ festgelegt. Das Label von x wiederum ist durch h festgelegt. Damit ist φ auf $X_3 + X_4 + X_5 + X_6$ durch $F(\varphi)$ festgelegt. Mit anderen Worten: Die Bijektion $X_3 + X_4 + X_5 + X_6 \leftrightarrow \mathbb{F}_4 \times \{3, 4, 5, 6\}$, die Punkte aus Ω Koordinaten zuordnet, ist durch $F(\varphi)$ festgelegt.

Jetzt wird φ auf $X_1 + X_2$ festgelegt: Für $c \in \mathbb{F}_4$ definiere $B_c \in \mathcal{C}$ als die 8-el. Menge, die $\{\Psi^{-1}(c, 4), \Psi^{-1}(0, 5)\} + X_6 \backslash \{\Psi^{-1}(0, 6)\}$ enthält. Das Label ist $\Phi(B_c) = (cc|cc|00)$. Da B_c ungerade, ist $|B_c \cap X_1| = |B_c \cap X_2| = 1$, womit die Element im Schnitt von B_c und $X_1 + X_2$ das Label c haben müssen. Damit ist φ auch auf $X_1 + X_2$ festgelegt. $F(\varphi)$ bestimmt also das Label, F ist somit injektiv.

Bleibt die Surjektivität zu zeigen: Sei $(a, (b, c), \delta) \in M$. Gesucht ist ein Label $\varphi : \Omega \to \mathbb{F}_4$ mit $F(\varphi) = (a, (b, c), \delta)$ und $\mathcal{G}(P, \varphi) = \mathcal{C}$. $\Phi : \Omega \to \mathbb{F}_4^6$ sei die zugehörige 6-Tupel-Labelabbildung (bzgl. P). $w \in X_3$ ist fest gewählt und es ist $\varphi(w) := \delta$, $\varphi(a) := \varphi(b) := 0$ und $\varphi(c) := 1$ definiert.

$P' = \{T_1, ..., T_6\}$ sei das Sextett, das $T_1 := X_1 \backslash \{a\} \cup \{b\}$ und $T_2 := (X_1 + X_2) \backslash T_1 = X_2 \backslash \{b\} \cup \{a\}$ enthält. Nach Lemma (4.13) gilt dann $|T_i \cap X_j| = 1\ \forall i, j \in \{3, 4, 5, 6\}$.

Zunächst definieren wir φ auf $X_3 + X_4 + X_5 + X_6$: $O'' := O(a, c, w)$, $\Phi(O'') = (01|\delta\delta'|\delta''\delta''')$ mit $\{\delta, \delta', \delta'', \delta'''\} = \mathbb{F}_4 (s. Lemma(3.6))$. Für die 3 neuen Elemente in O'' definieren wir φ als δ, δ' bzw. δ''', je nach Zugehörigkeit zu X_4, X_5 oder X_6. Es ist $|T_j \cap O''| = 1\ \forall j = 3, ..., 6$ (man verwende $T_1 + T_j = O(a, c, \alpha)$ mit $X_3 \cap T_3 = \{\alpha\}$, dann folgt mit der Vorb. 2 die Beh.). Auf T_j,

$j = 3, ..., 6$ definieren wir das Label φ als λ genau dann, wenn der im Schnitt mit O'' liegende Punkt bereits das Label λ besitzt. In dem Fall definiere $F_\lambda := T_j$.

Nun zum Labeln von X_1+X_2: Für $s \in \mathbb{F}_4$ nehme ein Hexacodewort der Form $h := (0s|cd|ef)$. s ist die Steigung des Hexacodeworts und falls $s \neq 0$ gilt, so gilt wieder nach Lemma(3.6) $\{c, d, e, f\} = \mathbb{F}_4$. $U(cdef) := X_3 \cap F_c + X_4 \cap F_d + X_5 \cap F_e + X_6 \cap F_f$ ist eine 4-el. Menge. Sei U das (ungeordnete) Sextett, das $U_3 := U(cdef)$ enthält. Für $s = 0$ ist U=P'. Für $s \neq 0$ sind die weiteren Elemente von U $U_4 := U(dcfe), U_5 := U(efcd), U_6 := U(fedc)$ (analog definiert) und zwei weitere 4-el. Mengen $U_1 := U(cdef)_1$ und $U_2 := U(cdef)_2$, wobei U_1 sich mit X_1 in 3 Elementen schneidet und mit X_2 in einem und U_2 entsprechend umgekehrt. Für $t \neq s$ definiere analog $h' := (0t|c'd'|e'f')$ und $U' = \{U'_1, ..., U'_6\}$. Dann ist $U \neq U'$.

Es ist $a \notin U_1$ und $a \notin U'_1$, denn sonst wäre $a \in U_1 = T_1$ für $s = 0$ und für $s \neq 0$

$$|(T_1+F_0)\cap(U_1+U_3)| = |(T_1\cap U_1)|+|F_0\cap U_3| = |X_1\backslash\{a\}\cap U_1|+|\{b\}\cap U_1|+1 = 2+|\{b\}\cap U_1|+1 = 4,$$

da $T_1 + F_0, U_1 + U_3 \in \mathcal{C}$. $\Rightarrow$ $b \in U_1 \Rightarrow \Phi(U_1 + U_3) = (*0|cdef) \in \mathcal{H}$. Der Abstand zu h ist kleiner als 4, womit $(*0|cdef) = h$, also $* = 0$ und $s = 0$ folgen würde, ein Widerspruch. Also ist $a \notin U_1$. Für U'_1 gilt dies natürlich entsprechend.

Damit gilt $U_1 \cap X_1 = U'_1 \cap X_1$, also $|U_1 \cap U'_1| = 3$ (da $U \neq U' \Rightarrow U_1 \neq U'_1$) und somit mit Lemma(4.13) $|U_i \cap U'_j| = 1$ für alle $i, j \in \{3, ..., 6\}$.

Nun kann man dem eindeutigen Element, das in U_1 und X_2 liegt das Label s geben. Dies ist nach den Überlegungen oben wohldefiniert. b wird damit tatsächlich das Label 0 gegeben, da b in $U(0000)_1 = T_1$ liegt. c bekommt das Label 1, da man dafür das Hexacodewort $(01|\delta\delta'|\delta''\delta''')$ verwenden kann. Zur Definition des Labels auf X_1 verwende man analog Hexacodewörter des Typs $(s0|cd|ef)$. a bekommt das Label 0.

Nun haben wir eine skalare Labelabbildung φ mit $F(\varphi) = (a, (b, c), \delta)$ definiert. Bleibt zu zeigen, dass damit tatsächlich der Golaycode konstruiert wird, d.h. $\mathcal{G}(P, \varphi) = \mathcal{C}$.

Unter Φ bekommt jede Doppelspalte $K_i + K_j$ das Label $(00|00|00)$ und die vier Mengen $T_1+F_{\lambda\}}$, $\lambda \in \mathbb{F}_4$, jeweils das Label $(00|\lambda\lambda|\lambda\lambda)$. Diese Codewörter erzeugen einen 8-dimensionalen Untervektorraum H von $\mathcal{C}$ und $\mathcal{G}(P, \varphi)$. Weiterhin liegen die 6 Codewörter, die durch Hexawörter der Form $(0s|**|**)$ bzw. $(s0|**|**)$, $s \neq 0$, konstruiert werden, in $\mathcal{C}$ und $\mathcal{G}(P, \varphi)$, aber nicht in H. Sie erzeugen damit $\mathcal{C}/H$. Damit folgt $\mathcal{C} \leq \mathcal{G}(P, \varphi)$ und aus Dimensionsgründen die Gleichheit. □

Satz 5.8 *Der Golaycode $\mathcal{G}$ ist bis auf lineare Äquivalenz eindeutig.*

Beweis: Sei $\mathcal{C}$ ein Golaycode und P ein geordnetes Sextett. Dann gibt es nach dem vorherigen Satz(5.7) eine skalare Labelabbildung , sodass $\mathcal{C} = \mathcal{G}(P, \varphi)$ ist. Dann existiert nach Lemma(5.6) ein $\sigma \in Sym(\Omega) \cong Mon(24, \mathbb{F}_2)$ mit $\sigma(\mathcal{C}) = \mathcal{G}(\Xi, l) = \mathcal{G}$. Also sind die Codes $\mathcal{C}$ und $\mathcal{G}$ linear äquivalent. □

Lemma 5.9

(i) Es gibt eine Bijektion zwischen $Aut(\mathcal{G})$ und $\{(P, \varphi)|$ P ist geordnetes Sextett, φ skalare Labelabbildung, $\mathcal{G}(P, \varphi) = \mathcal{G}\}$.

(ii) $Aut(\mathcal{G})$ operiert transitiv sowohl auf den geordneten wie auch auf den ungeordneten Sextetten.

Beweis: Zu (i): $M := \{(P,\varphi)|$ P ist geordnetes Sextett, φ skalare Labelabbildung, $\mathcal{G}(P,\varphi) = \mathcal{G}\}$ Dann ist

$$\kappa : Aut(\mathcal{G}) \to M,\ g \mapsto\ g(\Xi, l)\ \ (\Xi \text{ Std.-Sextett, l Std.-Label})$$

eine Bijektion mit Umkehrabbildung

$$\kappa^{-1}((P,\varphi)) = g\ mit\ g(P,\varphi) = (\Xi, l)$$

Nach Lemma(5.6) existiert so ein $g \in Sym(\Omega)$. Wegen $\mathcal{G}(P,\varphi) = \mathcal{G} = \mathcal{G}(\Xi, l)$ ist $g \in Aut(\mathcal{G})$. g ist eindeutig, also ist κ bijektiv.

Zu (ii): Zu einem geordneten Sextett P gibt eine skalare Labelabbildung φ mit $\mathcal{G}(P,\varphi) = \mathcal{G}$. Mit dem gleichen Argument wie oben gibt es dann ein $g \in Aut(\mathcal{G})$ mit $g(P,\varphi) = (\Xi, l)$, also $g(P) = \Xi$. □

Satz 5.10 $|Aut(\mathcal{G})| = 244.823.040 = 2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$

Beweis: Ξ_u ist das zu Ξ gehörende ungeordnete Sextett. Es gilt $|Stab_{Aut(\mathcal{G})}(\Xi_u)| = 2^6 \cdot 3 \cdot 6! = 2^{10}3^35$ nach Folgerung(5.5). Außerdem gibt es nach Folgerung(4.12) $1771 = 7{\cdot}11{\cdot}23$ ungeordnete Sextette. Insgesamt gilt damit

$$|Aut(\mathcal{G})| = |Aut(\mathcal{G})\Xi_u| \cdot |Stab_{Aut(\mathcal{G})}(\Xi_u)| = 2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$$

□

Satz 5.11 *$Aut(\mathcal{G})$ ist 5-fach transitiv auf Ω, aber nicht 6-fach transitiv.*

Beweis: Sei $(x_1, ..., x_5) \in \Omega^5$ ein Tupel mit pw. unters. x_i. Dann bildet $Aut(\mathcal{G})$ dieses Tupel folgendermaßen auf das Tupel $(y_1, ..., y_5) =$

	K_1	K_2	K_3	K_4	K_5	K_6
0	1	5				
1	2					
ω	3					
$\overline{\omega}$	4					

ab: Sei P das Sextett, das $X_1 := \{x_1, ..., x_4\}$ enthält. Es sei $x_5 \in X_2$. Wegen der Transitivität auf Sextetten ist o.B.d.A. $P = \Xi$. Der Stabilisator des ungeordneten Sextetts $\mathfrak{N}$ ist transitiv auf den Spalten, also o.B.d.A. $X_1 = K_1$ und $X_2 = K_2$. Nach Satz(5.4)(ii) operiert der Stabilisator von K_1 wie S_4 auf K_1. Also gibt es ein $g \in Aut(\mathcal{G})$ mit $g(x_i) = y_i\ \forall i = 1, ..., 4$ und $g(x_5) \in K_2$. Durch die Operation eines Elements aus $< (01|01|\omega\overline{\omega}) > \leq \mathcal{H}$ kann man x_5 auf y_5 abbilden.

Wäre $Aut(\mathcal{G})$ 6-fach transitiv, so wäre $Stab_{Aut(\mathcal{G})}(\{y_1, ..., y_5\})$ transitiv auf $\Omega\backslash\{y_1, ..., y_5\}$, einer 19-el. Menge. 19 teilt aber nicht $|Aut(\mathcal{G})|$. □

Satz 5.12 ***(Einfachheit von** M_{24}**)*** *Die fünfte Mathieugruppe ist definiert als $M_{24} := Aut(\mathcal{G})$. Dann ist M_{24} eine einfache Gruppe.*

Beweis: Sei S eine 23-Sylowuntergruppe. Dann ist $N_{S_{24}}(S) = S \rtimes C_{22}$ nach Lemma (2.4). Also ist $N_{M_{24}}(S) = S \rtimes U$ mit $U \leq C_{22}$.

Ann. $U = C_{22}$: Dann folgt mit Sylows Sätzen

$$|Syl_{23}(M_{24})| = \frac{|M_{24}|}{|N_{M_{24}}(S)|} = 2^9 \cdot 3^3 \cdot 5 \cdot 7 = 24^3 \cdot 35 \equiv 12 \not\equiv 1 \ (mod\ 23)$$

Ein Widerspruch. Also jetzt die Annahme $U = C_2$:

$$\Rightarrow |Syl_{23}(M_{24})| \equiv 12 \cdot 11 \equiv -6 \not\equiv 1 \ (mod\ 23)$$

Wiederum ein Widerspruch zu den Sylow-Sätzen. Fehlt noch $U = \{1\}$:

$$\Rightarrow |Syl_{23}(M_{24})| \equiv 12 \cdot 22 \equiv -12 \not\equiv 1 \ (mod\ 23)$$

Wieder ein Widerspruch. Also ist

$$N_{M_{24}}(S) \cong S \rtimes C_{11}$$

Es ist tatsächlich $|Syl_{23}(M_{24})| \equiv 12 \cdot 2 \equiv 1 \ (mod\ 23)$.

Nun sei $K \lhd M_{24}$, $K \neq \{1\}$, minimal.

1. Fall $S \subseteq K$: Nach dem Frattini-Argument ist dann $N_{M_{24}}(S)K = M_{24}$. Falls $N_K(S) = S$, so ist $S \leq Z(N_K(S))$. Dann hat K nach Burnsides Satz (2.2) ein normales 23-Komplement, d.h es existiert ein $N \lhd K$ mit $N \cap P = \{1\}$ und $K = NS$. Dann gilt auch $N \triangle M_{24}$, denn N ist die einzige Untergruppe von K der Ordnung $\frac{|K|}{|S|}$ (wegen $S = N_K(S)$ gibt es nach den Sylow-Sätzen $|N|$ konjugierte Untergruppen zu S, also $22|N| = |K| - |N|$ Elemente der Ordnung 23). Aufgrund der Minimalität von K folgt $N = \{1\}$ und $K = S$. Dies ist aber ein Widerspruch, da S nicht normal ist, denn $|Syl_{23}(M_{24})| > 1$.

Also ist $N_{M_{23}}(S) = N_K(S) \subseteq K \ \Rightarrow \ K = M_{24}$, also ist M_{24} einfach.

2. Fall $S \cap K = \{1\}$: Mit Lemma(2.1) und der Tatsache, dass M_{24} primitiv auf Ω ist (da 2-fach transitiv), folgt 24| $|K|$ und dann 3| $|K|$. Sei nun P eine 3-Sylowuntergruppe von K. Damit ist nach dem Frattini-Argument $M_{24} = N_{M_{24}}(P)K$.

$$\Rightarrow \ S \subseteq N_{M_{24}}(P) \ \Rightarrow \ \exists\, \varphi : S \to Aut(P) \text{ Homomorphismus}$$

φ ist der triviale Homomorphismus, da sonst 23 $|Aut(P)|$ teilen müsste ($|Aut(P)| = 3^b m$, m teilt $\prod_{i=1}^{3}(3^i - 1) = 2 \cdot 8 \cdot 26 = 2^5 \cdot 13$ nach Satz(2.3)).

Also zentralisiert S jedes Element aus P. Sei $x \in P$ mit $| < x > | = 3$. Dann gilt

$$gxg^{-1} = x \ \forall g \in S \ \Leftrightarrow \ x^{-1}gx = g \ \forall g \in S$$

Damit wäre $< x > \leq N_{M_{24}}(K)$. Dies ist aber ein Widerspruch, da $|N_{M_{24}}(K)|$ nicht von 3 geteilt wird. Damit folgt $S \cap K \neq \{1\}$, also die Einfachheit von M_{24}. □

Bemerkung 5.13

- *$M_{24} \leq S_{24}$ ist bis auf Konjugation wohldefiniert und eindeutig.*
- *M_{24} ist eine sporadische Gruppe.*

Beweis: Im Kapitel haben wir gesehen, dass der Golaycode existiert und eindeutig bis auf lineare Äquivalenz ist. Damit gilt dies auch für $M_{24} = Aut(\mathcal{G})$.

Nach dem Klassifikationssatz über endliche einfache Gruppen gibt es keine einfache Gruppe der Ordnung von M_{24}, die eine zyklische Gruppe von Primzahlordnug, eine alternierende Gruppe oder eine endliche Gruppe vom Lie-Typ ist. Also ist M_{24} eine Sporadische Gruppe, und zwar die 9.-kleinste.

6 Untergruppen von M_{24}

Definition 6.1 *Sei $a \in \Omega$ fest.*
Dann definiere $\Omega^* := \Omega \backslash \{a\}$ und $p : \Omega \to \Omega^*$ die Projektion auf Ω^*.

Bemerkung 6.2 *$p(\mathcal{G})$ ist der binäre [23,12,7]-Golaycode. Es einer der perfekten Codes. Die Automorphismengruppe ist gerade $M_{23} := Stab_{M_{24}}(\omega)$. M_{23} ist die 4. Mathieugruppe, eine sporadische Gruppe (Beweis s.u.). Aus den Eigenschaften von M_{24} folgt*

- *M_{23} ist 4-fach transitiv auf Ω^**
- $|M_{23}| = \frac{2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23}{24} = 2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$

Satz 6.3 *M_{23} ist einfach.*

Beweis: Der Beweis geht fast analog wie der zur Einfachheit von M_{24}.

Sei also S eine 23-Sylowuntergruppe. Dann ist $N_{S_{23}}(S) = S \rtimes C_{22}$ nach Lemma (2.4). Also ist $N_{M_{23}}(S) = S \rtimes U$ mit $U \leq C_{22}$. Wegen $24 \equiv 1 \ (mod\ 23)$ hat $N_{M_{23}}(S)$ die gleiche Ordnung wie $N_{M_{24}}(S)$ (s. Bew. zu Satz(5.12)). Also gilt

$$N_{M_{23}}(S) \cong S \rtimes C_{11}$$

Sei $K \lhd M_{23}$, $K \neq \{1\}$, minimal. K operiert transitiv auf Ω^*, da M_{24} primitiv operiert (s. Lemma (2.1)). 23 teilt also $|K|$. $\Rightarrow$ $S \subseteq K$.

Es gilt also der 1. Fall des Beweises zu (5.12). Analog folgt auch hier $K = M_{23}$. Damit ist M_{23} einfach. □

Literatur

[Go] Daniel Gorenstein, Finite Simple Groups. Harper and Row, 1982

[Go2] Daniel Gorenstein, Finite Groups. Harper and Row, 1980, 2. Auflage.

[Gr] Robert L. Griess, Jr., Twelve Sporadic Groups. Springer-Verlag, 1998

[Hi] Gerhard Hiss, Die sporadischen Gruppen.

[Hu] B.Huppert, Endliche Gruppen I. Springer-Verlag, 1967.

[Wi] Wolfgang Willems, Codierungstheorie und Kryptographie. Birkhäuser-Verlag, 2008

[1] *http : //groupprops.subwiki.org/wiki/Burnside's_normal_p − complement_theorem*