Mathieugruppen und Permutationscodes

von
David Dursthoff

Bachelorarbeit in Mathematik

vorgelegt der
Fakultät für Mathematik, Informatik und Naturwissenschaften
der Rheinisch-Westfälischen Technischen Hochschule Aachen

im August 2011

angefertigt am Lehrstuhl D für Mathematik
Prof. Dr. Gabriele Nebe

Inhaltsverzeichnis

1 Einleitung **3**

2 Grundlagen **7**
2.1 Gruppen . . . 7
2.2 Lineare Codes . . . 8

3 M_{24} als Automorphismengruppe des Golaycodes **11**
3.1 Der Hexacode . . . 11
3.2 Der binäre Golaycode . . . 14
3.2.1 Konstruktion über den Miracle-Octade-Generator . . . 15
3.2.2 Eigenschaften . . . 17
3.3 Die Automorphismengruppe . . . 20
3.3.1 Der Sextett-Stabilisator . . . 20
3.3.2 Eindeutigkeit des Golaycodes . . . 24
3.3.3 Eigenschaften der Automorphismengruppe . . . 26
3.4 Untergruppen von M_{24} . . . 28
3.4.1 M_{23} und M_{22} . . . 28
3.4.2 Der Octad-Stabilisator . . . 29
3.4.3 M_{12} und M_{11} . . . 32

4 M_{24} als Permutationscode **35**
4.1 Permutationscodes . . . 35
4.1.1 Permutationen als Codewörter . . . 35
4.1.2 Ein Decodieralgorithmus . . . 37
4.2 Der Code M_{24} . . . 38
4.3 Codieren und Decodieren mit M_{24} . . . 41
4.3.1 7 und weniger Fehler . . . 42
4.3.2 8 Fehler . . . 43
4.3.3 9 und mehr Fehler . . . 45

Literatur **48**

A UBB7 **51**

B UBB8 **53**

C Decodieralgorithmus **55**

Kapitel 1

Einleitung

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 gilt einer der folgenden Fälle:

- *G ist zyklisch von Primzahlordnung (genau dann, wenn G abelsch).*
- *G ist eine alternierende Gruppe ($G \cong A_n$) 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. Der Beweis hat eine Länge von ca. 15.000 Seiten, verteilt auf 300 bis 500 einzelne Artikel, von denen nicht alle veröffentlicht wurden.

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, wurde 1981 von Robert Griess konstruiert. Sie hat eine Ordnung von zirka $8 \cdot 10^{53}$. Dass das Monster einfach ist, bewiesen im Jahre 1973 Bernard Fischer und Robert Griess unabhängig voneinander. 20 der sporadischen Gruppen, die Happy Family, lassen sich aus dem Monster konstruieren. Die 6 Ausnahmen (J_1, J_3, J_4, ON, Ru, und Ly) werden 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). Mathieu suchte nach mehrfach transitiven Gruppen. M_{11} und M_{12} konstruierte er, indem er mit einer C_8 begann und diese transitiv erweiterte, bis er eine fünfach-transitive Gruppe auf 12 Punkten (M_{12}) erhielt. M_{11} ist dann der Stabilisator eines Punktes.

Die größte Mathieugruppe, M_{24}, kann auf vielfältige Weise konstruiert werden. Mathieu ging analog wie bei M_{12} vor, man könnte aber auch einfach die Erzeuger angeben:

$$(1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23),$$
$$(3,17,10,7,9)(4,13,14,19,5)(8,18,11,12,23)(15,20,22,21,16),$$
$$\text{und} \quad (1,24)(2,23)(3,12)(4,16)(5,18)(6,10)(7,20)(8,14)(9,21)(11,17)(13,22)(15,19).$$

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}	$m \geq 3, q$ *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 (1973/76)	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	$2^{41} \cdot 3^{13} \cdot 5^6 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot$ $23 \cdot 31 \cdot 47$
$F_1,\ M$ (1973/81)	808017424794512875886459904 96171075700575436800000000	$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot$ $23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$

Im 3. Kapitel dieser Arbeit wird M_{24} als Automorphismengruppe des erweiterten binären Golaycodes konstruiert und bewiesen, dass sie eindeutig und einfach ist. Alle kleineren Mathieugruppen treten als Untergruppen auf. Das 3. Kapitel beruht auf dem Buch „Twelve Sporadic Groups“ von Robert L. Griess Jr., siehe [Gr]. Robert Griess verwendet zur Konstruktion den sogenannten Miracle-Octade-Generator, wie ihn Robert Curtis in [Cu] einführte.

Die Mathieu-Gruppen M_{24} und M_{12} sind 5-fach transitiv auf 24 bzw. 12 Punkten. 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. Dies sind mit Ausnahme der symmetrischen und alternierenden Gruppen die einzigen 4-fach bzw. 5-fach transitiven Gruppen.

Satz 1.2 *Sei $G \leq S_n$, $n \in \mathbb{N}$, eine 4-fach transitive Permutationsgruppe.*
Dann ist G isomorph zu

(i) S_n,

(ii) A_n,

(iii) M_{11} *und n=11,*

(iv) M_{12} *und n=12,*

(v) M_{23} *und n=23 oder*

(vi) M_{24} *und n=24*

(Siehe [Cam99], S. 110)

Eine gute Zusammenfassung der Geschichte der Entdeckung der sporadischen Gruppen geben Gerhard Hiss (s. [Hi]) und Daniel Gorenstein (s. [Go]).

Im 4. Kapitel werden Permutationscodes behandelt. Dabei werden Analogien zwischen Teilmengen und Permutationen von $\{1, ..., n\}$, also zwischen linearen Codes über $\mathbb{F}_2$ und Permutationscodes, behandelt.

Permutationen kann man als Codes nutzen, indem man sie als Listen schreibt, wobei der i-te Eintrag dem Bild von i entspricht. Dabei können besonders gut Permutationsgruppen als Permutaionscodes genutzt werden, da die Eigenschaften der Permutationsgruppen viele Eigenschaften der Codes bestimmen. Eine Zusammenfassung gibt Peter Cameron in [Cam10].

Robert Bailey hat in seiner Dissertation ([Ba06a]) und [Ba09] eine Möglichkeit zum Decodieren angegeben. Diese hat er auf M_{11} angewendet und zusammen mit John Bray in [Ba-Br] M_{11} auf ihren Nutzen als Code untersucht.

Ähnlich vorgehend habe ich M_{24} als Permutationscode untersucht. M_{24} ist ein Code der Länge 24 auf einem Alphabet von 24 Elementen mit Minimalabstand 16. Damit kann man 7-Fehler korrigieren. Wie ich zeigen werde, ist M_{24} in der Praxis quasi 8-fehlerkorrigierend, denn falls 8-Fehler auftreten, so ist die Wahrscheinlichkeit, dass richtig decodiert wird, zirka $1 - 2,5 \cdot 10^{-9}$.

Beenden möchte ich dieses Kapitel mit einer Geschichte über die Hall-Janko-Wales-Gruppe J_2, eine sporadische Gruppe. Deren Konstruktion haben Hall und Wales in einem Text mit Titel „The simple group of order 604800“[1] veröffentlicht. Kurz darauf erhielt Hall einen sehr kurzen Artikel mit dem Titel „The simple group of order 604801“ - 604801 ist eine Primzahl!
(S. [Gr], S. 123)

[1] Marshall Hall Jr., David Wales, The Simple Group of Order 604,800. Journal of Algebra 9, 417-450 (1968).

Kapitel 2

Grundlagen

In diesem Kapitel werden wir einige Sätze für Gruppen, speziell Permutationsgruppen, die in den nächsten Kapiteln benötigt werden, wiederholen.

2.1 Gruppen

Definition 2.1 *Sei $n \in \mathbb{N}$. Eine Gruppe $G \leq S_n$ heißt **Permutationsgruppe** vom Grad n. G operiert treu auf $\underline{n} := \{1, ..., n\}$.*

Definition 2.2 *Sei $G \leq S_n$, $n \in \mathbb{N}$, eine Permutationsgruppe.*

- *G ist k-fach transitiv, falls zu jedem beliebigen k-Tupel von pw. vers. Punkten ein Gruppenelement existiert, dass dieses auf $(1, 2, ..., k)$ abbildet.*
- *G ist scharf k-fach transitiv, falls G k-fach transitiv und für alle k-Tupel $(a_1, ..., a_k) \in \underline{n}^k$ der punktweise Stabilisator*

$$Stab_G((a_1, ..., a_k)) = \bigcap_{i=1}^{k} Stab_G(a_i) = 1 \text{ ist.}$$

Lemma 2.3 *Sei G eine Gruppe, N ein Normalteiler und M eine endliche Menge. G operiere primitiv und N nicht-trivial auf M (falls G eine Permutationsgruppe und $N \neq 1$ ist, so ist die letzte Voraussetzung immer erfüllt).*
Dann operiert 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 $g \in G$

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

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. □

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

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

Beweis: O.B.d.A. $x = (1, 2, ..., k)$. Es gilt $C_{S_n}(x) =< x >$, da $< x >$ abelsch und transitiv ist. (Der Beweis verwendet, dass der Zentralisator regulär auf $\underline{k}$ operieren muss, siehe z.B. [Hu], S. 158.)

Sei $g \in N_{S_n}(< x >)$ dann gilt

$$^g x = (g(1), g(2), ..., g(k)) \in < x >,$$

also $g(k+1) = k+1$ falls $n = k+1$. Insgesamt operiert $N_{S_n}(< x >)$ also auf k Punkten, $N_{S_n}(< x >) \leq S_k$. $< x >$ operiert regulär auf $\underline{k}$ und damit

$$N_{S_n}(< x >) =< x > \rtimes Stab(1).$$

Es gilt

$$Stab(1) \cong Aut(< x >) \cong (\mathbb{Z}/k\mathbb{Z})^*$$

□

Satz 2.5 ***(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 z.B. [**?**], S.419.

Satz 2.6 ***(P. Halls Folgerung aus dem Burnside'schem Basissatz)***
Sei G eine p-Gruppe, d.h. $|G| = p^a$, p Primzahl und $a \in \mathbb{N}$.

Dann gilt $|Aut(G)| = p^b n$, $b \in \mathbb{N}$, mit $p \nmid n$ und n teilt $|GL(a,p)| = \sum_{i=0}^{a-1}(p^d - p^i)$.

Beweis: Siehe z.B. [Hu], S. 275

Satz 2.7 ***(Frattini-Argument)***
Sei G eine Gruppe, $K \lhd G$, $P \leq K$. G lasse die K-Konjugationsklasse von P invariant (d.h. $^G P =^K P$).

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 $g = (gk^{-1})k \in N_G(P)K$. □

2.2 Lineare Codes

Definition 2.8 ***(Codes)***
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 2.9 ***(Selbst-Orthogonalität und -Dualität)***
Sei K ein Körper und $(\ ,\ )$ eine Bilinearform oder allgemeiner eine Sesquilinearform auf K^n (also $(av, w) = \sigma(a)(v, w)$ und $(v, aw) = a(v, w)$ für $a \in K,\ v, w \in K^n$ und $\sigma \in Aut(K)$).
$C \leq K^n$ sei ein Code und

$$C^\perp := \{\ x \in K^n |\ (x, c) = 0\ \forall c \in C\}$$

bezeichne den orthogonalen Code.

- *C heißt **selbst-orthogonal**, falls $C \subseteq C^\perp$ gilt.*
- *C heißt **selbst-dual**, falls $C = C^\perp$ gilt.*

Definition 2.10 ***(Automorphismengruppe eines Codes)***
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:*

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

  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. $Perm(n, K)$ sei die Gruppe aller Permutationsmatrizen.
- *$Mon(n, K)$ bezeichne die Gruppe aller Monomialtrasformationen.*

  $$Mon(n, K) = Diag(n, K) \rtimes Perm(n, K) \cong K^* \wr S_n$$

- *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:*

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

  und für einen Körperautomorphismus σ.
- *$Mon^*(n, K) = Mon(n, K) \rtimes \Gamma = [Diag(n, K) \rtimes Perm(n, K)] \rtimes \Gamma$. 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 solch ein g aus $Mon(n, K)$, so heißen C und D linear äquivalent.*

Bemerkung 2.11 *Ist $K = \mathbb{F}_2$, so gilt $Mon^*(n, K) = Mon(n, K) \cong S_n$.*

Kapitel 3

M_{24} als Automorphismengruppe des Golaycodes

In diesem Kapitel werden wir erst den Golaycode und dann die 5. Mathieugruppe M_{24} als Automorphismengruppe konstruieren. Das Kapitel beruht auf Robert Griess' Buch „Twelve Sporadic Groups“, siehe [Gr].

3.1 Der Hexacode

In diesem Abschnitt betrachten wir den Hexacode, einen Code über $\mathbb{F}_4^6$. Die Konstruktion ist auch in [Con-Sl] zu finden.

$(\ ,\ )$ sei die Sesquilinearform auf $\mathbb{F}_4^6$ 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 bezeichnet $\mathbb{F}_4 = \{0, 1, \omega, \overline{\omega}\}$ mit $\omega^2 = \overline{\omega} = \omega + 1,\ \overline{\omega}^2 = \omega$ und $\overline{\omega}\omega = 1$.

Definition 3.1 *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:*

$$\begin{aligned} v_1 &:= (\omega\overline{\omega}|\omega\overline{\omega}|\omega\overline{\omega}) \\ v_2 &:= (\overline{\omega}\omega|\overline{\omega}\omega|\omega\overline{\omega}) \\ v_3 &:= (\omega\overline{\omega}|\overline{\omega}\omega|\overline{\omega}\omega) \\ v_4 &:= (\overline{\omega}\omega|\omega\overline{\omega}|\overline{\omega}\omega) \end{aligned}$$

Die Schreibweise wird später klar. Die Koordinaten 1&2, 3&4 und 5&6 bilden jeweils Koordinatenblöcke. Im Folgenden wird bewiesen, dass $\mathcal{H}$ tatsächlich ein Hexacode ist. $\mathcal{H}$ ist sogar bis auf Äquivalenz der einzige Hexacode (siehe [Gr] für einen Beweis). Im Folgenden werden wir noch 3 weitere Charakterisierungen von $\mathcal{H}$ sehen.

Bemerkung 3.2 *(i) $Dim(\mathcal{H}) = 3$. Jeweils drei der oberen vier Vektoren bilden eine Basis.*

(ii) $\mathcal{H}$ ist selbst-dual bezüglich $(\ ,\ )$. Also ist ein Vektor genau dann ein Codewort, wenn es orthogonal auf allen Codewörtern des Erzeugendensystems steht (2. Charakterisierung).

Lemma 3.3 ***(3. Charakterisierung)***
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) $x_i + x_j + x_k \ = \ \omega^{(-1)^{(i+j+k+1)}} \cdot s \ \ \forall i \in \{1,2\}, j \in \{3,4\}, k \in \{5,6\}$

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

Beweis: „ $\Rightarrow$ “ : Für die Vektoren v_i des Erzeugendensystems (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 $\Rightarrow \ (x, v_1) = \sum_{i=1}^{6} x_i \cdot \overline{v_{1i}} =$
$x_1\overline{\omega} + x_2\omega + x_3\overline{\omega} + x_4\omega + x_5\overline{\omega} + x_6\omega \ = \ \omega \underbrace{(x_1 + x_2)}_{=s} + x_1 + \omega \underbrace{(x_3 + x_4)}_{=s} + x_3 + \omega \underbrace{(x_5 + x_6)}_{=s} + x_5 =$
$3\omega s + x_1 + x_3 + x_5 \overset{Hexacode-Krit.}{=} \omega s + \omega^{1+3+5+1} = \omega s + \omega s = 0 \ \Rightarrow \ x \in < v_1 >^{\perp}$
$(x, v_2) = x_1\omega + x_2\overline{\omega} + x_3\omega + x_4\overline{\omega} + x_5\overline{\omega} + x_6\omega = 3\omega s + x_2 + x_4 + x_5 = \omega s + \omega^{2+4+5+1} = \omega s + \omega s =$
$0 \ \Rightarrow \ x \in < v_1, v_2 >^{\perp}$
$(x, v_3) = x_1\overline{\omega} + x_2\omega + x_3\omega + x_4\overline{\omega} + x_5\omega + x_6\overline{\omega} = 3\omega s + x_1 + x_4 + x_6 = \omega s + \omega^{1+4+6+1} = \omega s + \omega s =$
$0 \ \Rightarrow \ x \in < v_1, v_2, v_3 >^{\perp} = \mathcal{H}^{\perp} = \mathcal{H}$ □

Bemerkung 3.4 *Die 4. Charakterisierung ist*

$$\mathcal{H} = \{ \ (ab|c\phi(a)|\phi(b)\phi(c)) \mid \phi(x) := ax^2 + bx + c\}.$$

Satz 3.5 *(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. $v_1 + v_2 = (11|11|00)$ hat Gewicht 4, somit ist $wt(\mathcal{H}) = 4$.

Zu (ii): Nach Bem.(3.2)(i) ist $Dim(\mathcal{H}) = 3$ und nach (i) $wt(\mathcal{H}) = 4$. □

Satz 3.6 ***(Fehlerkorrektur-Eigenschaften des Hexacodes)***

3-er Problem *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 $h_{i_j} = a_{i_j} \ \forall j = 1, 2, 3$.*

5-er Problem *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: 1. 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 ist injektiv, denn sei $h \in \mathcal{H}$ mit $\Psi(h) = 0$. Dann ist $wt(h) \leq wt(\Psi(h)) + 3 = 3 \overset{d(\mathcal{H})=4}{\Rightarrow} h = 0$.

Aus Dimensionsgründen ist Ψ ein Isomorphismus und $\Psi^{-1}(a_{i_1}, a_{i_2}, a_{i_3}) \in \mathcal{H}$ das gesuchte Hexacodewort.

2. 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. □

Dies ist ein sehr nützlicher Satz, da man schnell sehen kann, wann Hexacodewörter existieren können. Wie diese aussehen müssen, kann man mit an den Bahnen der folgenden Untergruppe der Automorphismengruppe ablesen .

Definition 3.7 *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 Elemente in 2 von den 3 Blöcken (1&2, 3&4 und 5&6) die Koordinaten innerhalb der Blöcke vertauschen. T operiert durch Permutation der Blöcke, wobei die Reihenfolgen der Elemente jeweils gleich bleiben.

Bemerkung 3.8 *Da die Gruppen jeweils Basiselemente auf Basiselemente von $\mathcal{H}$ abbilden, ist die Operation wohldefiniert und es gilt $Z, S \leq Aut(\mathcal{H})$. Elemente von Z und S kommutieren, denn Elemente aus S sind Permutationsmatrizen und aus Z Skalarmatrizen. Es gilt also $Z \times S \leq Aut(\mathcal{H})$.*

Satz 3.9 *Die Bahnen von $Z \times S$ sind wie folgt gegeben:*

Vertreter	*Bahnlänge*
(00|00|00)	1
(00|11|11)	9
(11|$\omega\omega$|$\overline{\omega}\overline{\omega}$)	6
($\omega\overline{\omega}$|$\omega\overline{\omega}$|$\omega\overline{\omega}$)	12
(01|01|$\omega\overline{\omega}$)	36

Beweis: Mit Hilfe des Lemmas (2.3) sehen wir, dass alle Vertreter Hexacodewörter sind.

Nun haben Hexacodewörter aus der Bahn von (00|11|11) einen Koordinatenblock = 00. Dieser kann an beliebiger Position liegen durch Anwenden eines Elementes aus $T \leq S$. Elemente aus V (Vertauschungen innerhalb der Blöcke) verändern das Hexacodewort nicht. $|Z(00|11|11)| = 3$ (Multiplikation mit 1, ω oder $\overline{\omega}$)

$$\Rightarrow\ |Z \times S(00|11|11)| = 9.$$

Vertauschungen innerhalb der Koordinatenblöcke verändern auch $(11|\omega\omega|\overline{\omega}\overline{\omega})$ nicht.

$$|S(11|\omega\omega|\overline{\omega}\overline{\omega})| = 6 \text{ und } Z(11|\omega\omega|\overline{\omega}\overline{\omega}) \subseteq S(11|\omega\omega|\overline{\omega}\overline{\omega})\ \Rightarrow\ |Z \times S(11|\omega\omega|\overline{\omega}\overline{\omega})| = 6.$$

$|T(\omega\overline{\omega}|\omega\overline{\omega}|\omega\overline{\omega})| = 1$, $|V(\omega\overline{\omega}|\omega\overline{\omega}|\omega\overline{\omega})| = 4$ und natürlich $|Z(\omega\overline{\omega}|\omega\overline{\omega}|\omega\overline{\omega})| = 3$

$$\Rightarrow\ |Z \times S(\omega\overline{\omega}|\omega\overline{\omega}|\omega\overline{\omega})| = 12.$$

$|T(01|01|\omega\overline{\omega})| = 3$, $|V(01|01|\omega\overline{\omega})| = 4$ und $|Z(01|01|\omega\overline{\omega})| = 3$

$$\Rightarrow\ |Z \times S(01|01|\omega\overline{\omega})| = 36$$

Das sind alle Bahnen denn $1 + 9 + 6 + 36 + 12 = 64 = |\mathcal{H}|$. □

Satz 3.10 ***(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.*

(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* $|Aut(H)| = 2^3 \cdot 3^3 \cdot 5 = 1080$

(v) $Aut*(\mathcal{H})$ *ist die einzige nicht spaltende Erweiterung* $3 \cdot S_6$. *Einen Beweis gibt Robert Griess in [Gr], S. 32 (Griess zeigt, dass es eine nicht abelsche Untergruppe von Ordnung 27 gibt).*

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 $\alpha \in Aut^*(\mathcal{H})$ ($\alpha \in Mon^*(6, \mathbb{F}_4)$ 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 $(01|01|\omega\overline{\omega}) \in \mathcal{H}$ 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 $|Aut^*(\mathcal{H})| = |Kern(\pi')|6! = 3 \cdot 6! = 2^4 \cdot 3^3 \cdot 5$.

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 $|Aut(H)| = 2^3 \cdot 3^3 \cdot 5 = 1080$. □

3.2 Der binäre Golaycode

Definition 3.11 ***(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 Kontrollbits hervorgeht, sodass alle Codewörter ein gerades Gewicht haben. Hier verwenden wir nur den erweiterten Golaycode. Bez.: $\mathcal{G}, \mathcal{C}, \mathcal{C}_{24}$.

3.2.1 Konstruktion über den Miracle-Octade-Generator

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.(2.11) ist

$$Mon^*(Pot(\Omega)) = Mon(Pot(\Omega)) = Sym(\Omega) = S_{24}.$$

$$(A, B) := \; |A \cap B| \mod 2$$

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 skalare Labelabbildung.

Ω kann man dann folgendermaßen darstellen:

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

Dies ist der sogenante Miracle-Octad-Generator (MOG), wobei Octads 8-elementige Mengen bezeichnen. Diese kann man mit dem MOG besonders gut erkennen und untersuchen.

Die Zeilen der oberen Darstellung heißen $R_c = l^{-1}(c)$ 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 sind, 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-Tupel-)Labelabbildung, definieren. Die $\mathcal{L}_i$ heißen 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 $(01|01|\omega\overline{\omega})$.

Man beachte, dass wenn 2 Punkte eines Spalte besetzt sind, das Label dieser Spalte nie 0 ist. Ist ein Punkt fest gewählt, so kann man durch hinzufügen eines Punktes ein Label $1, \omega$ oder $\overline{\omega}$ erreichen. Sind 3 Punkte einer Spalte besetzt, so ist das Label das des freien Punktes.

Definition 3.12 *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 (wenn A gerade) bzw. ungerade (wenn A ungerade) ist.*

Lemma 3.13 *(i) Für $S, T \in Pot(\Omega)$ ist $i_{S,T} : Pot(\Omega) \to \mathbb{F}_2,\ A \mapsto (|A \cap S| + |A \cap T|) \mod 2 = (|A \cap (S+T)|) \mod 2$ 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 3.14 *$\mathcal{L}$ 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 ungerade.

Falls $x = (0, ..., 0)$, so ist S nicht wohlausgewogen ($|S \cap R_0| = 6$), 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 ist, 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 3.15 $\mathcal{G} := \mathcal{W} \cap \mathcal{L}^{-1}(\mathcal{H})$

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

*Codewörter mit Gewicht 8 heißen **Octad** und mit Gewicht 12 **Dodecad**.*

Satz 3.16 *$\mathcal{G}$ 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 ein oder drei Elemente, also $wt(B) \geq 6$. Da B wohlausgewogen ist, 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 ist, 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 $d = 8$. □

Bemerkung 3.17 *Die Octads sind im MOG folgendermaßen gegeben:*

(i) Ungerade Octads schneiden genau eine Spalte in 3 Punkten und alle anderen in einem Punkt.

(ii) Gerade Octads sind entweder „Doppelspalten", also der Form $K_i + K_j$, oder schneiden 4 Spalten in jeweils 2 Punkten. Gerade Octads haben als Label immer ein Hexacodewort vom Gewicht 0 oder 4.

Definition 3.18
- *Eine geordnete Partition P von Ω aus 6 Mengen mit je 4 Elementen heißt ein **geordnetes Sextett**, falls $A + C \in \mathcal{G}\ \forall A, C \in P$.*
- *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 3.19 *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.*

3.2.2 Eigenschaften

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

Satz 3.20 *(i) $\Omega \in \mathcal{G}$. Also ist mit jedem Codewort B auch sein Komplement $\Omega + B$ ein Codewort und $\mathcal{G}$ ist 2-dividierbar..*

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

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

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

Beweis: Zu (i): $\Omega \in \mathcal{G}$ klar und jedes Codewort hat gerades Gewicht, da Codewörter ausgewogene Mengen sind.

Zu (ii): $d(\mathcal{G}) = 8$, also gibt es keine Codewörter vom Gewicht 2, 4 oder 6. Wegen (i) gibt es dann auch keine vom Gewicht 22, 20 und 18. Ein Codewort vom Gewicht 10 widerspricht der Definition der Codewörter, damit gibt es auch keine vom Gewicht 14.

Also gibt es nur Codewörter vom Gewicht 0,8,12,16 und 20 (zu jedem Gewicht gibt es tatsächlich mindestens ein Codewort).

Zu (iii): Seien $B, C \in \mathcal{G}$. Dann gilt modulo 4

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

Also enthält der Schnitt gerade viele Elemente. Damit gilt $(B,C) \equiv |B \cap C| \ \equiv 0(mod\ 2)$, also sind B und C orthogonal zueinander. $\mathcal{G}$ ist also selbst-orthogonal. Die Selbst-Dualität folgt aus $Dim(\mathcal{G}) = 12 = 24/2$.

Zu (iv): Man verwende den Dualitätssatz von Jessie MacWilliams. Daraus resultiert ein lineares Gleichungssytem mit nur einer ganzzahligen Lösung, siehe dazu [Wi], S. 46. □

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

Satz 3.21 *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 enthalten. 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 genau 6 Elemente, so folgt die Behauptung. Sein also $A_1, A_2 \in M, A_1 \neq A_2$. Dann ist $8 \leq wt(\underbrace{A_1 + A_2}_{\in \mathcal{G}}) \leq 4 + 4 \ \Rightarrow\ A_1 \cap A_2 = \emptyset$. Damit ist $M = \{A_1, ..., A_6\}$ für passende A_i.

Zu (iii): Folgt aus (i) und (ii) aus Ordnungsgründen. □

Folgerung 3.22 *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 eines eindeutigen Sextetts.*

Lemma 3.23 *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* $|X_2 \cap Y_1| = 3$ *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, $|X_1 \cap Y_2| = |X_2 \cap Y_1| = 1$. 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 $wt(X_1 + X_2 + Y_1 + Y_2) = 8 + 8 - 2|(X_1 + X_2) \cap (Y_1 + Y_2)| \leq 16 - 2 \cdot 5 = 6 \;\Rightarrow\; wt(X_1 + X_2 + Y_1 + Y_2) = 0 \;\Rightarrow\; X_1 + X_2 = Y_1 + Y_2 \;\Rightarrow\; |X_2 \cap Y_2| = 3$.

Es ist $X_1 + \mathcal{G} + Y_1 + \mathcal{G} = (X_1 + Y_1) + \mathcal{G}$ mit $|X_1 + Y_1| = 4 + 4 - 2 \cdot 3 = 2$. Für $i, j \notin \{1, 2\}$ gilt dann $|X_i + Y_j| > 4$ nach Satz(3.21), 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 3.24 ***(Steiner-System)***
Ein ***Steinersystem*** *S mit Parametern (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 3.25 *Sei $A \in Pot(\Omega)$ eine Menge mit 5 Elementen.*

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

Beweis: Sei $\mathcal{G}_8 := \{\mathcal{O} \in \mathcal{G} \mid |\mathcal{O}| = 8\}$ und $A \subseteq \Omega$ mit $|A| = 5$. Dann existiert $C \in \mathcal{G}$ mit $n := |A + C| \leq 4$ (ex. nach Satz (3.21)). n ist ungerade, da sonst $wt(C) = |A + C| - |A| + 2|A \cap C| = -5 + |A + C| + 2|A \cap C|$ ungerade wäre.

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

Also ist n=3 und damit $|A \cap C| = (5 - 3 + wt(C))/2 \geq (2 + 8)/2 = 5$. Wegen $|A| = 5$ 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 $\mathcal{G}$. □

In Kapitel 4 werden wir noch sehen, dass man zusätzlich zu diesem 5-er Problem auch ein 7-er Problem lösen kann. Zu 7 Punkten existiert immer ein Octad, das mindestens 6 der 7 Punkte enthält.

Folgerung 3.26 *(i) Jedes Dodecad ist Summe von 2 Octads, die sich in 2 Punkten schneiden. Kein Dodecad enthält ein Octad.*

(ii) Jedes gerade Octad ist Summe von 2 ungeraden Octads

(iii) 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 Octad.

(iv) Die B_h und die „Doppelspalten" $K_i + K_j$ erzeugen $\mathcal{G}$.

Beweis: Zu (i): Sei $\mathcal{D} \in \mathcal{G}$ ein Dodecad und $\mathcal{O}$ ein Octad, das 5 Punkte von $\mathcal{D}$ enthält, nach dem vorherigen Satz existiert $\mathcal{O}$. Dann gilt $|\mathcal{O} \cap \mathcal{D}| \in \{6, 8\}$. Wäre $|\mathcal{O} \cap \mathcal{D}| = 8$, so hätte $\mathcal{O} + \mathcal{D} \in \mathcal{G}$ Gewicht 4. Also kann $\mathcal{D}$ $\mathcal{O}$ micht enthalten und es gilt $|\mathcal{O} \cap \mathcal{D}| = 6$. Damit ist $\mathcal{O} + \mathcal{D}$ ein Octad, das $\mathcal{O}$ in 2 Punkten schneiden muss, denn

$$(\mathcal{O} + \mathcal{D}) + \mathcal{O} = \mathcal{D}$$

Zu (ii): Sei $\mathcal{O}$ ein gerades Octad. Dann ist $\mathcal{O}$ eine Doppelspalte (bzgl. des Standardsextetts Ξ) oder in 4 Spalte liegen je 2 Punkte (Bem (3.17)).

Ist $\mathcal{O}$ eine Doppelspalte, so seien $x_1, x_2, x_3 \in \mathcal{O}$ aus der 1. Spalte und $x_4 \in \mathcal{O}$ aus der anderen. Sei $x_5 \in (\Omega + \mathcal{O})$ und $\mathcal{O}'$ das Octad, dass $x_1, ..., x_5$ enthält. Insbesondere ist $\mathcal{O}'$ ungerade. Dann ist auch $\mathcal{O} + \mathcal{O}'$ ein ungerades Octad.

Ist $\mathcal{O}$ keine Doppelspalte, so wähle $x_1, ..., x_4 \in \mathcal{O}$ so, dass aus jeder Spalte, die $\mathcal{O}$ schneidet, je ein Punkt ausgewählt wird. Desweiteren sei $x_5 \in (\Omega + \mathcal{O})$ aus einer Spalte, die $\mathcal{O}$ nicht schneidet. Sei $\mathcal{O}'$ das Octad, dass $x_1, ..., x_5$ enthält. Damit sind $\mathcal{O}'$ und $\mathcal{O} + \mathcal{O}'$ ungerade Octads.

(iii) klar

Zu (iv:) Ein ungerades Octad hat immer die Form B_h für ein $h \in \mathcal{H}$ oder es ist die Summen aus einem B_h und einer Doppelspalte (Man beachte dazu, wie die ungeraden Octads nach Bem. (3.17) im MOG vorkommen). Die ungeraden Octads erzeugen nach (i) und (ii) $\mathcal{G}$. □

3.3 Die Automorphismengruppe

Die Automorphismengruppe unseres Golaycodes ist $Aut^*(\mathcal{G}) = Aut(\mathcal{G}) = \{f \in S_{24} |\ f(\mathcal{G}) = \mathcal{G}\}$. Indem wir $M_{24} := Aut(\mathcal{G})$ definieren, haben wir damit auch die größte Mathieugruppe konstruiert. Wir wollen die Ordnung und weitere Eigenschaften ermitteln, indem wir die Operation auf Sextetts betrachten. Zunächst untersuchen wir den Sextett-Stabilisator.

3.3.1 Der Sextett-Stabilisator

Definition 3.27 *$\mathfrak{N} := Stab_{Aut(\mathcal{G})}(\Xi_u)$ operiert auf dem ungeordneten Sextett Ξ_u durch Anwenden. $\pi_0 : \mathfrak{N} \to Sym(\Xi_u)$ sei die zugehörige Permutationsdarstellung und L der Kern.*

Satz 3.28 *(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. Man beachte, dass die Permutationsmatrizen die Zeilen* $R_0,...,R_{\overline{\omega}}$ *erhalten.*

(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 Folg. (3.26).

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.Folg. (3.26)) 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 3.29

(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: $h^{\pi_1}(K_i)=K_i\ \forall h\in\mathcal{H},\ i\in\{1,...,6\}$.

Zu (iii): Nach dem Satz über die Eigenschaften von $Aut^*(\mathcal{H})$ (s. Satz (3.10)) 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 $\mathcal{L}(Pot(K_i))=<e_i>$. □

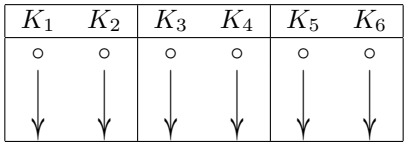
Satz 3.30 ***(Stabilisator eines ungeordneten Sextetts)***

(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 $|\mathcal{H}\rtimes Aut^*(\mathcal{H})|=4^3\cdot3\cdot6!$ teilt $|\mathfrak{N}|$. Also reicht es zu zeigen: $4^3\cdot3\cdot6!=|\mathfrak{N}|=|Bild(\pi_0)|\cdot|L|=6!|L|\ \Leftrightarrow\ |L|=4^3\cdot3$.

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.: $\mu^{\pi_1}=$



Oder genauer: $\mu^{\pi_1}(\Psi^{-1}(c,i)) = \Psi^{-1}(\omega \cdot c, i) \ \forall (c,i) \in \Omega_{(\Xi,l)}$. 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 $g \in L$. $a_i := g(\Psi^{-1}(0,i))$. Wegen dem 3-er Problem von $\mathcal{H}$ (s. Satz (3.6)) existiert genau ein $h \in \mathcal{H}$ 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 Octad mit $A \subset B$.

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

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

$L_0 := \{f \in L |\ f(\Psi^{-1}(0,i)) = \Psi^{-1}(0,i) \ \forall i = 1, ..., 6\}$ 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:

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

$$\mathcal{L}_m(B') = \begin{cases} 0, & falls\ m = j \ \vee \ m = k \\ c, & sonst \end{cases} \Rightarrow \mathcal{L}(B') \text{ ist } (cc|cc|00), (cc|00|cc) \text{ oder } (00|cc|cc). \text{ Also ist}$$

$\mathcal{L}(B') \in \mathcal{H}$, womit B' die angegebene Form haben muss.

Wegen $g(A') = A'$ ist dann $g(B') = B'$, und weil c, j, k beliebig gewählt sind, operiert f auf jedem K_i trivial.

Also operiert ein $g \in L_0$ auf allen K_i bzw. K_i^* gleich. 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 eine Permutation aus S_3. 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 jedem 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 (3.10)) 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 (ii): 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 3.31 $|\mathfrak{N}| = |\mathcal{H}| \cdot |Aut^*(\mathcal{H})| = 4^3 \cdot 2^4 \cdot 3^3 \cdot 5 = 2^{10} \cdot 3^3 \cdot 5$

3.3.2 Eindeutigkeit des Golaycodes

Lemma 3.32 *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 $\sigma(P,\varphi) = (\Xi, l)$. Insbesondere gilt $\sigma(\mathcal{G}(P,\varphi)) = \mathcal{G}(\Xi,l) = \mathcal{G}$.

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 wohlausgewogene Mengen auf wohlausgewogene Mengen ab. Sei nun $B \in \mathcal{G}(P,\phi)$, Φ die 6-Tupel-Labelabbildung von (P,φ) und $P = \{X_1,...,X_6\}$. Dann ist für $i = 1,...,6$

$$\mathcal{L}(\sigma(B))_i = (\sum_{x\in\sigma(B)\cap K_i} l(x))_i = (\sum_{x\in\sigma(B)\cap\sigma(X_i)} l(x)\ )_i = (\sum_{y\in B\cap K_i} l(\sigma^{-1}(y)))_i =$$

$$(\sum_{y\in B\cap X_i} \phi(y))_i = \Phi(B)_i \ \Rightarrow\ \Phi(B) \in \mathcal{H}$$

□

Satz 3.33 ***(Erzeugen einer Labelabbildung)***
Seien $\mathcal{C}$ 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 $A_2 := \{(x,y) \in X_2 \times X_2 |\ x \neq y\}$ („$Anti-Diagonale$“), $N := \{\varphi$ 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 $O(x,y,p)$ das eindeutige Octad, das die 5-el. Menge $X_1 - \{x\} + \{y,p\}$ enthält. Da $O(x,y,p) \cap (X_1 + X_i)$ für alle $1 < i \leq 6$ gerade ist, ist $O(x,y,p) \cap X_i$ eine 1-el. Menge. Dies sieht man auch daran, dass $O(x,y,p)$ ein ungerades Octad ist und nach Bem. (3.X) diese Form hat.

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 (3.5)). Es ist nach Steigung und Hexacode-Kriterium (s. Lemma(3.3)) $\{\delta, h_4, h_5, h_6\} = \mathbb{F}_4$. $O_q := O(a,b,q)$ für ein $q \in X_3$, unabhängig von φ eindeutig bestimmt. Dann ist wieder nach (3.3) $\Phi(O_2) = (00|\lambda\lambda|\lambda\lambda)$. 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 das Octad, das $\{\Psi^{-1}(c,4), \Psi^{-1}(0,5)\} + X_6 \backslash \{\Psi^{-1}(0,6)\}$ enthält. Das Label ist $\Phi(B_c) = (cc|cc|00)$. Da B_c ungerade ist, ist $|B_c \cap X_1| =$

$|B_c \cap X_2| = 1$, womit die Elemente 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 (3.23) 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(3.3)). 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 $J_\lambda := T_j$.

Nun zum Label 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 (3.3) $\{c,d,e,f\} = \mathbb{F}_4$.

$$U(cdef) := X_3 \cap J_c + X_4 \cap J_d + X_5 \cap J_e + X_6 \cap J_f$$

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, der 6-Tupel-Labelabbildúng von „*varphi*, 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 3.34 *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 eine skalare Labelabbildung φ, sodass $\mathcal{C} = \mathcal{G}(P,\varphi)$ ist. Dann existiert nach Lemma (3.32) ein $\sigma \in Sym(\Omega)$ mit $\sigma(\mathcal{C}) = \mathcal{G}(\Xi, l) = \mathcal{G}$. Also sind die Codes $\mathcal{C}$ und $\mathcal{G}$ linear äquivalent. □

3.3.3 Eigenschaften der Automorphismengruppe

Lemma 3.35

(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(3.32) 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 es 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 3.36 $|Aut(\mathcal{G})| = 244.823.040 = 2^{10}\cdot 3^3\cdot 5\cdot 7\cdot 11\cdot 23$

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 (3.31). Außerdem gibt es nach Folgerung (3.22) $1771 = 7\cdot 11\cdot 23$ 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 3.37 *$Aut(\mathcal{G})$ ist 5-fach transitiv auf Ω, aber nicht 6-fach transitiv. Damit ist $Aut(\mathcal{G})$ auch transitiv auf der Menge der Octads.*

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 (3.30)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 $\cap_{i=0}^{5} Stab_{Aut(\mathcal{G})}(y_i)$ transitiv auf $\Omega\backslash\{y_1,...,y_5\}$, einer 19-el. Menge. 19 teilt aber nicht $|Aut(\mathcal{G})|$.

$Aut(\mathcal{G})$ ist transitiv auf Octads, da jedes Octad durch 5 Punkte festlegt wird. □

Satz 3.38 ***(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 (2.5) ein normales 23-Komplement, d.h es existiert ein $N \lhd K$ mit $N \cap S = \{1\}$ und $K = NS$. Dann gilt auch $N \lhd M_{24}$, 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 $N_{M_{24}}(S) = N_K(S) \subseteq K \ \Rightarrow \ K = M_{24}$, also ist M_{24} einfach.

2. Fall $S \cap K = \{1\}$: Mit Lemma (2.3) 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 P. Halls Satz (2.6)).

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 der 1. Fall und somit die Einfachheit von M_{24}. □

Bemerkung 3.39

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

Beweis: In diesem Kapitel haben wir gesehen, dass der Golaycode existiert und bis auf lineare Äquivalenz eindeutig ist. Damit sind alle Automorphismengruppe in S_{24} konjugiert.

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.

3.4 Untergruppen von M_{24}

3.4.1 M_{23} und M_{22}

Definition 3.40 *Sei $a \in \Omega$ fest.*
Dann definiere $\Omega^* := \Omega \backslash \{a\}$ und $p : \Omega \to \Omega^*$ die Projektion auf Ω^*.

Bemerkung 3.41 *$p(\mathcal{G})$ ist der binäre [23,12,7]-Golaycode. Er ist einer der perfekten Codes und die Automorphismengruppe ist gerade $M_{23} := Stab_{M_{24}}(\omega)$, die 4. Mathieugruppe, eine weitere sporadische Gruppe (Beweis s.u.). Aus den Eigenschaften von M_{24} folgt*

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

Definiere M_{22} und M_{21} als punktweise Stabilisator von 2 bzw. 3 Punkten.

Satz 3.42 *M_{23} ist einfach und eine sporadische Gruppe.*

Beweis: Der Beweis kann fast analog wie der zur Einfachheit von M_{24} geführt werden.

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 (3.38)). 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.X)). 23 teilt also $|K|$. $\Rightarrow$ $S \subseteq K$.

Es gilt also der 1. Fall des Beweises zu (3.28). Analog folgt auch hier $K = M_{23}$. Damit ist M_{23} einfach und aus Ordnungsgründen eine sporadische Gruppe. □

Um die Einfachheit von M_{22} zu beweisen, nutzen wir, dass

$$M_{21} \cong PSL(3, 5)$$

gilt. Einen Beweis gibt Robert Griess in [Gr].

Satz 3.43 *M_{22} ist einfach und damit eine sporadische Gruppe.*

Beweis: Sei $K \neq 1$ ein minimaler Normalteiler und M_{21} der Stabilisator eines Punktes. M_{22} ist 3-fach transitiv, also insbesondere primitiv. Somit ist M_{21} maximale Untergruppe. M_{21} ist einfach und kein Normalteiler, damit gilt

$$K \cap M_{21} = \{1\} \text{ oder } K = M_{22}.$$

Angenommen $K \cap M_{21} = \{1\}$

$$\Rightarrow KM_{21} = M_{22}.$$

Es folgt $|K| = 22$, aber dann hat K nur eine 11-Sylow-Untergruppe P. P ist charakteristisch in K, also Normalteiler von M_{22}. Dies ist ein Widerspruch zur Minimalität von K. □

3.4.2 Der Octad-Stabilisator

Sehr nützlich ist der folgende Satz.

Satz 3.44 ***(Stabilisator eines Octads)***
Der Stabilisator eines Octads ist isomorph zur affinen Gruppe

$$Aff(4,2) \cong C_2^4 \rtimes A_8$$

Der punktweise Stabilisator ist der Normalteiler C_2^4, dieser operiert regulär auf $\mathcal{O} + \Omega$.

Beweis: Da M_{24} transitiv auf Octads ist, betrachten wir $\mathcal{O} := K_1 + K_2 =$

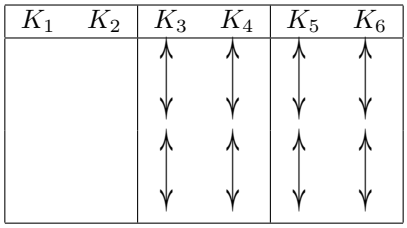
	K_1	K_2	K_3	K_4	K_5	K_6
0	1	1				
1	1	1				
ω	1	1				
$\overline{\omega}$	1	1				

$H := Stab_{M_{24}}(\mathcal{O})$ hat die Ordnung $\frac{|M_{24}|}{759} = 16 \cdot \frac{8!}{2}$.

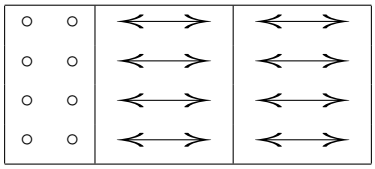
Schreibe h_1, h_ω und $h_{\overline{\omega}}$ für die Automorphismen von $\mathcal{G}$, die von den Hexacodewörter $(00|11|11)$, $(00|\omega\omega|\omega\omega)$ bzw. $(00|\overline{\omega\omega}|\overline{\omega\omega})$ induziert werden. Man sieht leicht $< h_1, h_\omega, h_{\overline{\omega}} > \cong V_4$. Ebenso stabilisieren die Automorphismen h_σ $\mathcal{O}$ punktweise, wobei die h_σ von den Automorphismen des Hexacodes, den Permutationsmatrizen zu $\sigma \in < (3,4)(5,6), (3,5)(4,6) >$ induziert werden. Die Automorphismen kommutieren (man überzeuge sich anhand der Zeichnungen unten). Insgesamt ist dann

$$R := < h_1, h_\omega, h_{(3,4)(5,6)}, h_{(3,5)(4,6)} > \cong C_2^4.$$

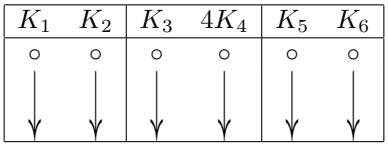
$h_1 = (00|11|11)^\pi =$



$h_{(3,4)(5,6)} =$



R operiert regulär auf $\mathcal{O} + \Omega$ und liegt im Kern der Permutationsdarstellung $\eta : H \to Sym(\mathcal{O})$. Wir zeigen $|\eta(H)| = \frac{8!}{2}$ und damit $\eta(H) = A_8$. Da S 5-fach transitiv auf $\mathcal{O}$ ist, wird $|\eta(H)|$ von $8 \cdot 7 \cdot 6 \cdot 5 \cdot 4$ geteilt. 3^2 teilt $|\eta(H)|$, denn der bekannte Automorphismus $\mu^{\pi_1} =$



operiert unterschiedlich auf $\mathcal{O} = K_1 + K_2$ und $K_1 + R_0 =$

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

Somit gilt dann $\eta(H) = A_8$ und $Kern(\eta) = R$ aus Ordnungsgründen.

Es bleiben noch die Isomorphien zu zeigen. Zunächst ist R ein regulärer Normalteiler. Also ist der Stabilisator S eines Punktes aus $\mathcal{O} + \Omega$ ein Komplement, denn S und R haben trivialen Schnitt (R op. regulär) und $|RS| = |H|$. $S \cong H/R \cong A_8$. S stabilisiere einen Punkt der 0-Zeile R_0. Dann ist $\mu \in S$, aber μ kommutiert nicht mit h_1. Also gibt es einen nicht-trivialen Homomorphismus

$$S \to Aut(R) \cong GL(4,2).$$

S ist einfach, also ist der Homomorphismus injektiv. Wegen $|A_8| = |GL(4,2)|$ folgt

$$H = R \rtimes S \cong C_2^4 \rtimes A_8 \cong C_2^4 \rtimes GL(4,2).$$

Man sieht hier auch einen Isomorphismus für $A_8 \cong GL(4,2)$. □

Auf der Struktur des Octad-Stabilisators bauen viele Sätze des letzten Kapitels auf. Einige wichtige Folgerungen erarbeiten wir sofort.

Satz 3.45 *(i) M_{24} ist transitiv auf der Menge der Paaren von Octads mit einer gleicher Kardinalität der Schnitte.*

(ii) Der Octad-Stabilisator ist 3-fach transitiv auf dem Komplement.

(iii) M_{24} ist transitiv auf der Menge der Dodecads

Beweis:

Sein $\mathcal{O} := K_1 + K_2$, $S := Stab(\mathcal{O})$ und $M_n := \{\mathcal{O}' \mid |\mathcal{O}'| = 8 \text{ und } |\mathcal{O}' \cap \mathcal{O}| = n\}$ für $n = 0, 2, 4$.

(ii) folgt direkt aus $Stab(\mathcal{O}) \cong Aff(4,2)$ und der Identifizierung des punktweisen Stabilisators $R \cong \mathbb{F}_2^4$ mit dem affinen Raum.

Wir zeigen zunächst (i) für n=4 und n=2 (daraus folgt direkt (iii) nach Folgerung (3.26)), dann für n=0.

Sei $\mathcal{O}' \in M_4$. $Stab(\mathcal{O})$ operiert 6-fach transitiv auf $\mathcal{O}$, also können wir o.B.d.A. annehmen, dass $\mathcal{O} \cap \mathcal{O}' = K_1$ gilt. $\mathcal{O}'$ ist eine gerade Menge und muss Label 0 haben, also $\mathcal{O}' = K_1 + K_i$ für ein $i \in \{3,4,5,6\}$. M_{24} operiert wie S_6 auf den Spalten, also existiert ein $g \in M_{24}$ mit

$$g(K_1) = K_1,\ g(K_2) = K_2 \text{ und } g(K_i) = K_3 \ \Rightarrow\ g \in Stab(\mathcal{O}) \text{ und } g(\mathcal{O}') = K_1 + K_3.$$

Nun sei $\mathcal{O}'' \in M_2$. $Stab(\mathcal{O})$ operiert 6-fach transitiv auf $\mathcal{O}$, also können wir o.B.d.A. annehmen, dass $\mathcal{O} \cap \mathcal{O}'' =$

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

gilt. $\mathcal{O}''$ ist somit ungerade und es gilt o.B.d.A

$$|\mathcal{O}'' \cap K_3| = 5 \text{ und } |\mathcal{O}'' \cap K_i| = 1\ \forall i \leq 4.$$

$$\Rightarrow \mathcal{L}(\mathcal{O}'') = (00|aa|aa) \text{ für ein } a \in \mathbb{F}_4$$

Dann gilt $(00|aa|aa)^{\pi_1} \in Stab(\mathcal{O}'')$ und $(00|aa|aa)^{\pi_1}(\mathcal{O}'') =$

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

Sei $\mathcal{O}''' \in M_0$. Nach (ii) o.B.d.A. $|\mathcal{O}''' \cap K_3| \leq 3$, somit gilt $\mathcal{O}''' = K_3 + K_i$ für ein $i \in \{4,5,6\}$. Dann existiert ein $g \in Stab(\{K_1, ..., K_6\}) \cap Stab(\mathcal{O})$ mit $g(\mathcal{O}''') =$

	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		

□

Folgerung 3.46 *(i) In der oberen Notation gilt*

$$\begin{aligned} |M_0| &= 30 \\ |M_2| &= 448 \\ |M_4| &= 280 \end{aligned}$$

(ii) Der Sextett-Stabilisator ist eine maximale Untergruppe von M_{24}.

Beweis: Zu (i): M_0 müssen wir leider fast komplett durchzählen. Sei $\mathcal{O}' \in M_0$. Dann ist $\mathcal{O}'$ gerade und hat ein Label der Form $(00|aa|aa)$ für ein $a \in \mathbb{F}_4$. $\mathcal{O}'$ ist genau dann eine Doppelspalte, wenn $a = 0$. Hierzu gibt es $\binom{4}{2} = 6$ Mengen. Gilt

$$|\mathcal{O}' \cap K_i| = 2 \ \forall i \in \{3,4,5,6\},$$

so ist $a \in \mathbb{F}_4^*$. Hierzu gibt es 3 Möglichkeiten, die sich alle gleich verhalten. Also nehmen wir $a = 1$ an. Desweiteren können wir $\mathcal{O}' \supseteq$

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

voraussetzen, da wir sonst das Komplement in $K_3 + K_4 + K_5 + K_6$ betrachten könnten.

Nun gibt es noch 4 Möglichkeiten für $\mathcal{O}'$, denn in einer Spalte müssen immer die 2 Punkte mit Label 0 und 1 oder mit ω und $\overline{\omega}$ besetzt sein, und in gerade vielen Spalten muss der Punkt mit Label 0 besetzt sein. Die 4 Mengen sind dann

	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		
ω					1	1
$\overline{\omega}$					1	1

	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

	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	

Also gilt insgesamt

$$|M_0| = 6 + 3 \cdot 2 \cdot 4 = 30.$$

$$|M_4| = \tbinom{8}{4}\frac{16}{4} = 280,$$

denn die 4 Schnittpunkte mit $\mathcal{O}$ sowie ein weiterer Punkt der 4 verbleibenden legen ein Octad aus M_4 fest.

Damit folgt

$$|M_2| = 759 - 1 - |M_0| - |M_4| = 448.$$

Zu (ii): Wir zeigen, dass M_{24} primitiv auf den Octads operiert, dann folgt, dass $Stab(\mathcal{O})$ eine maximale Untergruppe ist. Sei $\mathcal{B}$ ein Block mit $\mathcal{O} \in \mathcal{B}$. Ist $\mathcal{O}' \in \mathcal{B}$ mit $\mathcal{O} \in M_n$ für $n \in \{0, 2, 4\}$, so gilt $M_n \subset \mathcal{B}$ (Satz (3.45)). Also gilt

$$|\mathcal{B}| = 1 + \epsilon_0 30 + \epsilon_2 448 + \epsilon_4 280,\ \epsilon_n \in \{0, 1\}.$$

Da $|\mathcal{B}|$ 759 teilen muss, folgt $|\mathcal{B}| \in \{1, 759\}$. □

3.4.3 M_{12} und M_{11}

Nun können wir die beiden kleinsten Mathieugruppen konstruieren.

Definition 3.47 *Sei $\mathcal{D}$ ein Dodecad. Definiere $M_{12} := Stab(\mathcal{D})$ und M_{11} als Stabilisator eines Punktes. M_{24} hat die Ordnung $12 \cdot 11 \cdot 10 \cdot 9 \cdot 8$.*

Bemerkung 3.48 *(i) Sei $M_{12} = Stab(\mathcal{D})$ mit $\mathcal{D} =$*

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

unser Standard-Dodecad. Man kann den Ternäre Golaycode und damit M_{12} auch über den Mini-MOG konstruieren. Der Mini-MOG ist ähnlich wie unser MOG, aber nur mit 4 Spalten und 3 Zeilen und einer Labelabbildung nach $\mathbb{F}_3 = \{0, +, -\}$. Den Mini-MOG können wir auch im MOG wiederfinden, indem man in unserem Dodecad die linken 3 Punkte runterklappt:

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

Die Automorphismengruppe des ternären Golaycodes ist allerdings die nicht spaltende Erweiterung $2 \cdot M_{12}$, die keine Untergruppe von M_{24} ist.

(ii) Eine Obergruppe von M_{12} ist

$$Stab_{M_{24}}(\{\mathcal{D}, \Omega + \mathcal{D}\}) = M_{12} \rtimes C_2.$$

Dies ist eine transitive maximale Untergruppe von M_{12}.

(iii) M_{12} ist transitiv auf

$$\{(\mathcal{O}, \mathcal{O}')|\ \mathcal{O}, \mathcal{O}'\ Octads,\ \mathcal{O} + \mathcal{O}' = \mathcal{D}\}$$

Satz 3.49 *M_{12} operiert treu und scharf 5-fach transitiv auf dem Dodecad, das M_{24} definiert.*

Beweis: Sei M_{12} der Stabilisator unseres Standard-Dodecads $\mathcal{D}$ (s.o.). Es gilt

$$|M_{12}| = \frac{|M_{24}|}{2576} = 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8.$$

Also zeigen wir die 5-fache Transitivität, daraus folgen die anderen Behauptungen. Seien $x_1, ..., x_5 \in \mathcal{D}$. Es existiert ein Octad $\mathcal{O}$ mit $x_1, ..., x_5 \in \mathcal{O}$ und $|\mathcal{O} \cap \mathcal{D}| = 6$ (Folg (3.26)). Nach der letzten Bemerkung können wir $\mathcal{O} = K_5 + K_6$ annehmen. Wir suchen nun ein $g \in Stab(\mathcal{O}) \cap Stab(\mathcal{D})$ mit $g((x_1, ..., x_5)) =$

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

Dazu zeigen wir, dass $G := Stab(\mathcal{O}) \cap Stab(\mathcal{D}) \cong S_6$ gilt. Nach Satz (3,X) ist $Stab(\mathcal{O}) = RS$, wobei R der punktweise Stabilisator von $\mathcal{O}$ und S der Stabilisator eines Punktes aus $\Omega + \mathcal{O}$. Es gilt

$$Stab_{RS}(\mathcal{O} \backslash \mathcal{D}) = RK$$

mit $K \leq S$ der Stabilisator von 2 Punkten des Octads, also $K \cong S_6$. Es gilt

$$G \leq RK \text{ und } G \cap R = \{1\} \ \Rightarrow\ G \leq K.$$

Es gibt $\frac{2576 \cdot \binom{12}{5}}{6} = 340032$ Paare aus Dodecad und Octad, wie $(\mathcal{D}, \mathcal{O})$.

$$\Rightarrow\ |G| = \frac{|M_{24}|}{340032} = 6!\ \Rightarrow\ G = K \cong S_4$$

□

Satz 3.50 *M_{12} und M_{11} sind sporadische einfache Gruppen.*

Beweis: Der Beweis funktioniert analog zum Beweis der Einfachheit von M_{24} bzw. M_{23}. Sei $G \in \{M_{12}, M_{11}\}$ und $n \in \{12, 11\}$.

Also sei S eine 11-Sylowuntergruppe. Dann ist $N_{S_n}(S) = S \rtimes C_{10}$ nach Lemma (2.4). Also ist $N_G(S) = S \rtimes U$ mit $U \leq C_{10}$.

Mit Sylows Sätzen folgt

$$N_G(S) \cong S \rtimes C_5$$

Nun kann man vollkommen analog zum Beweis der Einfachheit von M_{24} bzw. M_{23} vorgehen, um zu beweisen, dass M_{12} und M_{11} einfach sind ($N_G(S)$ verhält sich wie $C_{23} \rtimes C_{11}$, der Normalisator einer 23-Sylowuntergruppe der größeren Gruppen). □

Kapitel 4

M_{24} als Permutationscode

Zwischen Teilmengen und Permutationen von $\underline{n}$ gibt es einige Analogien. So kann man Erstere als Wörter in linearen Codes über $\mathbb{F}_2$ nutzen. In diesem Kapitel sehen wir, wie man Letztere als Codewörter in Permutationscodes nutzen kann.

4.1 Permutationscodes

4.1.1 Permutationen als Codewörter

Definition 4.1

- *Sei $n \in \mathbb{N}$ Dann ist*

$$H_n := \underline{n}^n = \{a = [a_1, ..., a_2] \mid a_i \in \{1, ..., n\}\ \}$$

*der **Hamming-Raum**. Die Elemente (=Abbildungen) werden hier in Listenschreibweise ($a = [a_1, ..., a_n]$) geschrieben und heißen auch Wörter. Mit der Komposition der Abbildungen wird H_n zu einem Monoid mit 1-Element $Id = [1, 2, ..., n]$.*

- *Auf H_n kann man den **Hamming-Abstand** definieren:*

$$d(a, b) := |\{i \in \underline{n} \mid a_i \neq b_i\}|,\ a, b \in H_n$$

- *Nun bietet sich noch ein **Gewicht** an:*

$$wt(a) := d(a, Id),\ a \in H_n$$

- ***Minimalabstand einer Menge von Abbildungen** $A \subseteq H_N$:*

$$d(A) := min\{\ d(a, b) \mid a, b \in H_n\}$$

- ***Minimalgewicht einer Menge von Abbildung** $A \subseteq H_n$:*

$$wt(A) := min\{wt(a) \mid a \in H_n\}$$

- *Ein **Permutationscode** ist eine Menge von Permutationen. Die Permutationen sind die Codewörter. Permutationsgruppen nennen wir auch **Gruppencodes**.*

Bemerkung 4.2 *Der Hamming-Abstand hat für Elemente der symmetrischen Gruppe $S_n \subseteq H_n$ einige schöne Eigenschaften. Für $a, b \in H_n$ und $\tau, \sigma \in S_n$ sieht man sofort*

- $d(a, b) = d(\sigma a, \sigma b) = d(a\sigma, b\sigma)$

- $d({}^{\tau}\sigma, Id) = d(\sigma, Id)$
- $d(\sigma,\tau) = wt(\tau^{-1}\sigma) = n - |Fix(\tau^{-1}\sigma)|$, *wobei* $Fix(\sigma) := \{i \in \underline{n} \mid \tau^{-1}\sigma(i) = i\}$ *die Menge der Fixpunkte einer Permutation* $\sigma \in S_n$ *bezeichtet.*

Um den Minimalabstand einer Gruppe zu bestimmen, recht es also aus, die Fixpunkte jeder Konjugiertenklasse zu ermitteln (GAP-Befehl „NaturalCharacter“).

Beispiel 4.3 *(i)* $d(A_n) = 3\ \forall n \geq 3$

(ii) Die additive Gruppe des Golaycodes kann als Permutationscode auf $\mathbb{F}_2 \times \underline{24}$ *genutzt werden. Hier fassen wir* $\mathcal{G} \leq \mathbb{F}_2^{24}$ *auf und ein* $c \in \mathcal{G}$ *induziert die Permutaton mit*

$$((a,i)) \mapsto (a + c_i, i),\ a \in \mathbb{F},\ i \in \underline{24}$$

Das Codewort ist dann aus disjunkten 2-Zykeln zusammengesetzt.

Bemerkung 4.4 *(i) Ist* $G \leq S_n$ *scharf k-fach transitiv, so bilden 2 verschiedene Permutationen höchstens k-1 Punkte gleich ab, also* $d(G) \geq n-k+1$. *Andererseits gibt es eine Permutation* $\neq Id$, *die die ersten k-1 Punkte fest lässt, also* $d(G) = n-k+1$.

(ii) Sei $S \leq G$ *der Stabilisator eines Punktes. Dann gilt* $d(S) = d(G)$.

Satz 4.5 ***(Analogie zur Singolton-Schranke)***
Sei $n \in \mathbb{N}$ *und* $G \leq S_n$ *ein Gruppencode mit* $d(G) = d$.
Dann gilt

$$|G| \leq n(n-1)\cdots d.$$

Gleichheit gilt genau dann, wenn G scharf $n-d+1-$*fach transitiv ist.*

Beweis: Wir definieren die Stabilisatorkette

$$G_0 \geq G_1 \geq ... \geq G_{n-d-1},\ G_0 := G \text{ und } G_i := Stab_{G_{i-1}}(i),\ i \geq 1.$$

Dann gilt $G_{n-d+1} = \{1\}$, denn sei

$$g \in G_{n-d+1} \ \Rightarrow\ d(g, Id) \leq n - (n-d+1) = d-1 \ \Rightarrow\ g = Id$$

$$\Rightarrow\ |G| = |G_0 \cdot 1||G_1| \overset{(...)}{=} (\prod_{i=0}^{n-d} \underbrace{|G_i \cdot (i+1)|}_{\leq n-i}) \underbrace{|G_{n-d+1}|}_{=1} \leq n(n-1)\cdots d.$$

Gleichheit gilt genau dann, wenn die Stabilisatoren volle Ordnung haben, also genau dann, wenn G scharf (n-d)-fach transitiv ist. □

Mengen von Permutationen können also als Codes genutzt werden. Übertragen werden dabei Permutationen in Listenschreibweise. Ein gewisser Minimalabstand zwischen den Permutationen ermöglicht ein Erkennen und Korrigieren von Fehlern. Eine Einschränkung auf Permutationsgruppen ist häufig sinnvoll.

Angenommen, die Permutationsgruppe $G \leq S_n$ wäre k-fach transitiv. Dann kann man beliebige Nachrichten aus $\underline{n}^k$ übertragen, indem man einem $v \in \underline{n}$ ein $g \in G$ mit $g(1,...,k) = v$ zuordnet und dieses überträgt.

Um Permutationsgruppen als Codes zu nutzen, ist es noch notwendig, eine Möglichkeit der Fehlererkennung und -Korrektur, also der Decodierung einer empfangenen Liste zurück zur gesendeten Liste (=Permutation) anzugeben.

4.1.2 Ein Decodieralgorithmus

Zum Decodieren hat Bailey in [Ba06a] und [Ba09] einen Algorithmus angegeben, der Bases verwendet. Bases werden auch in der Speicherung einer Gruppe verwendet. Dazu die folgende Definition.

Definition 4.6 *Sei G eine Permutationsgruppe auf $\underline{n}$ und $a_1, ...a_k \in \underline{n}$ pw. verschieden. $G_0 \leq G_1 \leq ... \leq G_k$ sei die Stabilisatorkette, d.h. $G_0 := G$ und G_i der punktweise Stabilisator von $a_1, ..., a_i,\ i > 0$. $(a_1, ..., a_k)$ heißen Base, falls $G_k = \{1\}$. Eine Base heißt irreduzibel, falls kein a_i Fixpunkt von G_{i-1} ist, also wenn man keinen Punkt der Base weglassen kann.*

Permutationen einer Gruppe sind eindeutig durch ihr Abbildungsverhalten auf einer Base festgelegt. Die Idee des Decodieralgorithmus ist es, zu einem empfangenen Wort eine Base zu finden, auf deren Punkten kein Fehler im Wort passiert ist. Dann gibt es nur eine Permutation, die mit dem empfangenen Wort auf der Base übereinstimmt. Diese muss dann die gesendete sein. Damit dieses Verfahren immer funktioniert, muss gewährleistet werden, dass für jede auftretende Fehlermenge (bis zu einer gewissen Schranke) so eine Base gefunden werden kann. Dazu die folgende Definition.

Definition 4.7 *Sei G eine Permutationsgruppe auf $\underline{n}$, U eine Menge von Bases und $r \in \mathbb{N}$.*

U heißt r-Uncovering-by-Bases (r-UBB), falls für alle r-elementigen Teilmengen $A \subseteq \underline{n}$ eine Base $B \in U$ existiert, sodass $A \cap B = \emptyset$ gilt.

Meist wählen wir $r = \frac{\lfloor d \rfloor - 1}{2}$, wobei d den Minimalabstand der Gruppe bezeichnet. Ist einfach von einer UBB die Rede, so ist eine solche r-UBB gemeint.

Algorithmus 4.8 *Seien eine Permutationsgruppe G auf $\underline{n}$ und eine r-UBB $U = \{B_1, ..., B_m\}$ gegeben.*
Eingabe: Ein Wort $w \in H_n$ mit Minimalabstand $\leq r$ zu G.
Ausgabe: Eine Permutation $g \in G$ mit $d(g, w) \leq r$.
Für i=1,...,m betrachte B_i: Hat w Wiederholungen auf B_i so fahre mit B_{i+1} fort (schließlich müssen Fehler auf Punkten aus B_i passiert sein). Ansonsten gibt es höchstens ein $g \in G$, dass B_i wie w abbildet. Gilt $d(g, w) \leq r$, so gib g aus. Ansonsten fahre mit B_{i+1} fort.

Es ist leicht zu sehen, dass dieser Algorithmus immer die richtige Permutation ausgibt, falls nicht zu viele Fehler aufgetreten sind. Mit leichten Modifizierungen gibt der Algorithmus alle Permutationen aus, die minimalen Abstand zum empfangenen Wort haben. Voraussetzung ist, dass die UBB passend gewählt ist. Bailey gibt in [Ba06a] eine Implementierung des Algorithmus in GAP an. Diese werden wir - leicht modifiziert - nutzen.

Beispiel 4.9 *(i) Betrachten wir A_4. Es ist $d(A_4) = 3$ und $\{\{1, 2\}, \{3, 4\}\}$ ist eine UBB. Angenommen wir empfangen das Wort $[2, 3, 4, 3]$. Mit der ersten Base erhalten wir die Permutation (1,2,3)=[2,3,1,4], aber es gilt $d([2, 3, 1, 4], [2, 3, 4, 3]) = 2$. Mit der 2. Base finden wir dann (1,2)(3,4) und $d([2, 1, 3, 4], [2, 3, 4, 3]) = 1$.*

(ii) Sei G eine scharf k-fach transitive Permutationsgruppe auf $\underline{n}$ mit $d(G) = n - k + 1$. Dann bilden k verschiedene Punkte immer eine irreduzible Base. Eine UBB ist immer ein Covering. Ein (n,k,r)-Covering ist eine Menge von Teilmengen von $\underline{n}$, Blöcke genannt, sodass jede r-elementige Teilmenge von $\underline{n}$ in mindesten einem Block liegt. Hat man also ein Covering gefunden, so bilden die Komplemente der Blöcke, sozusagen ein Uncovering, eine UBB. Viele Coverings findet man beispielsweise in der Datenbank „La Jolla Covering Repository“ von Daniel M. Gordnon, siehe [LaJ].

Die Effizienz des Algorithmus hängt stark von der Größe der r-UBB ab. Bailey hat in [Ba09] gezeigt, dass der Zeitaufwand des Algorithmus

$$mO(kn)$$

beträgt. m bezeichnet die Länge der verwendeten UBB und k die Länge der Bases. Der Speicheraufwand ist dann

$$mO(kn^2).$$

Wie der folgende Satz zeigt, existiert für jede Permutationsgruppe in allen relevanten Fällen eine r-UBB.

Satz 4.10 *Sei $G \leq S_n$, $n \in \mathbb{N}$, eine Permutationsgruppe und $r < d(G)$.*
Dann existiert eine r-UBB.

Beweis: Angenommen, es existiert keine UBB, d.h. es existiert eine r-elementige Menge A, die mit jeder Base nicht-leeren Schnitt hat. Dann enthält $\underline{n}\backslash A$ keine Base, der punktweise Stabilisator S ist also nicht trivial und es existiert ein $g \in S$ mit $g \neq Id$. Dann gilt aber

$$d(g, Id) = n - |Fix(g)| \leq n - |\underline{n}\backslash A| = r < d(G).$$

Es folgt $g = Id$ und damit ein Widerspruch. □

4.2 Der Code M_{24}

Ähnlich wie den Code M_{12} (s. [Ba06a] und [Ba-Br]) kann man auch den Code M_{24} untersuchen. Dabei hat man aber größere Probleme, denn M_{24} ist im Gegensatz zu M_{12} nicht scharf transitiv. Damit ist der Minimalabstand schwerer zu bestimmen und zur Konstruktion einer UBB kann man sich nur bedingt der Covering-Datenbank bedienen.

Für Rechnungen in GAP werden wir die Standardkopie von M_{24} verwendet. Diese wird von den drei Permutationen

$$(1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23),$$
$$(3,17,10,7,9)(4,13,14,19,5)(8,18,11,12,23)(15,20,22,21,16),$$
und $(1,24)(2,23)(3,12)(4,16)(5,18)(6,10)(7,20)(8,14)(9,21)(11,17)(13,22)(15,19)$ erzeugt.

Eine Möglichkeit, auf $\{1,...,24\}$ ein Sextett und ein Label zu definieren, sodass die Automorphismengruppe des resultierenden Golaycodes gerade dieser M_{24} entspricht, ist

	K_1	K_2	K_3	K_4	K_5	K_6
0	1	2	3	11	21	20
1	4	5	8	13	12	24
ω	6	22	9	23	15	16
$\overline{\omega}$	7	17	19	18	14	10

Zunächst bestimmen wir den Minimalabstand. Dies könnte man mit GAP tun, allerdings kann man auch die Konstruktion der vorherigen Kapitel nutzen. Zunächst behandeln wir ein 7-er Problem für den Golaycode. Dies kann man ähnlich zu den 3-er und 5-er Problemen des Hexacodes formulieren. Das 5-er Problem des Golaycodes (5 Punkte liegen in einem eindeutigen Octad) haben wir bereits häufig genutzt.

Lemma 4.11 ***(7-er Problem)***
Zu 7 beliebigen Punkten aus Ω existiert ein Octad, das mindestens 6 dieser Punkte enthält.

Beweis: Falls solch ein Octad existiert, so ist es eindeutig bestimmt, denn 2 Octads haben einen Schnitt mit höchstens 4 Elementen. Es gibt also $759 \cdot 8$ verschiedene 7-elementigen Mengen, die in einem Octad liegen und $759 \cdot \binom{8}{6} \cdot (24-8)$ Mengen, die einen 6-el. Schnitt mit einem Octad haben.
Wegen

$$759 \cdot 8 + 759 \cdot \binom{8}{6} \cdot (24-8) = 6072 + 340032 = 346104 = \binom{24}{7}$$

sind dies alle 7-el. Mengen. □

Lemma 4.12 ***(Permutationen mit minimalem Abstand)***

(i) Sei $g \in M_{24}$ mit $d(g, Id) = 16$. (g hat minimales Gewicht nach dem folgenden Satz)

Dann bilden die Fixpunkte ein Octad. g stabilisiert das Octad punktweise und ist somit ein Produkt aus 8 disjunkten Transpositionen.

(ii) Alle Permutationen mit Gewicht 16 liegen in einer Konjugiertenklasse.

Beweis: Zu (i): g stabilisiert insbesondere 7 Punkte, also nach dem vorherigen Lemma 6 Punkte eines Octads $\mathcal{O}$. Dann liegt g in $Stab(\mathcal{O})$ (die 6 Punkte legen sowohl das $\mathcal{O}$ als auch $g(\mathcal{O})$ fest, also $g(\mathcal{O}) = \mathcal{O}$).

Der Stabilisator operiert nach Satz (3.44) wie A_8 auf $\mathcal{O}$. Also operiert g wie die Identität, liegt also im punktweisen Stabilisator, die 8 Fixpunkte sind also die Punkte des Codeworts. Die Struktur des punktweisen Stabilisators liefert die Zykelstruktur von g.

Zu (ii): Sei $g \in M_{24}$ mit Gewicht 16, g stabilisiere das Octad $\mathcal{O}$ punktweise. Wir wollen zeigen, dass g zu

K_1	K_2	K_3	K_4	K_5	K_6
		↑	↑	↑	↑
		↓	↓	↓	↓
		↑	↑	↑	↑
		↓	↓	↓	↓

$= (00|11|11)^{\pi_1} \in \mathcal{H}^{\pi_1}$ (vgl. Satz (3.44)) konjugiert ist. Zunächst ist M_{24} transitiv auf Octads, also existiert ein $h \in M_{24}$ mit $h(\mathcal{O}) = K_1 + K_2$. Dann liegt ${}^h g$ im punktweisen Stabilisator R von $K_1 + K_2$. $Stab(K_1 + K_2)$ operiert 3-fach transitiv auf $\Omega + K_1 + K_2$ (Satz (3.45)), also insbesondere transitiv auf $R\backslash\{1\}$ per Konjugation (R operiert regulär auf $\Omega + K_1 + K_2$). Also existiert ein $k \in Stab(K_1 + K_2)$ mit

$$^{kh}g = (00|11|11)^{\pi_1}.$$

□

Lemma 4.13 *Auf der Menge der 6-elementigen Teilmengen von Ω hat M_{24} 2 Bahnen. Trennende Invariante ist die Eigenschaft, ob eine Menge in einem Octad liegt oder nicht. Der punktweise Stabilisator ist isomorph zu*

$$C_2^4 \text{ bzw. } C_3.$$

Insbesondere hat eine Base mehr als 6 Elemente.

Beweis: Sei A eine 6-elementige Menge, die Teil eines Octads $\mathcal{O}$ ist. M_{24} ist transitiv auf Octads und der Stabilisator operiet wie A_8 auf dem Octad. Es existiert also ein $g \in M_{24}$ mit $g(A) =$

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

Dies ist ein Vertreter der ersten Bahn. Der punktweise Stabilisator ist gleichzeitig der punktweise Stabilisator des Octads, also isomorph zu C_2^4.

Nun sei B eine 6-elementige Menge, die nicht Teilmenge eines Octads ist. O.B.d.A. ist $B \cap (K_1 + K_2) =$

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

Der 6. Punkt liegt dann in $\Omega + K_1 + K_2$. Der punktweise Stabilisator operiert regulär, also existiert ein Automorphismus h mit $h(B) =$

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

Dies ist ein Vertreter der 2. Bahn. Schreibe G für den punktweisen Stabilisator. Klar ist

$$G \leq Stab_{M_{24}}(K_1 + K_2).$$

Seien R der punktweise Stabilisator von K_1+K_2 und $S := Stab_{Stab(K_1+K_2)}(\Psi^{-1}(0,3))$ (Stabilisator der Punktes links oben in $\Omega + K_1 + K_2$). Nach Satz (3.44) gilt dann $Stab_{M_{24}}(K_1 + K_2) = RS$. $G \leq S \cong A_8$ und damit $G \cong C_3$, denn G ist der Stabilisator von 5 Punkten in $K_1 + K_2$. □

Satz 4.14 *Der Minimalabstand von M_{24} ist 16. Alle irreduziblen Bases sind durch 7 Punkte, die zusammen nicht Teilmenge eines Octads sind, gegeben.*

Beweis: Sei $g \in M_{24}$, $g \neq Id$, mit minimalen Abstand zu Id. Dann gilt $d(g, Id) \leq 16$, also fixiert g über 7 Punkte. Nach dem 7-er Problem gibt es also 6 Fixpunkte, die in einem Octad $\mathcal{O}$ liegen. Mit Satz (3.44) liegt g damit im punktweisen Stabilisator. Dieser operiert regulär auf $\Omega + \mathcal{O}$. Also ist kein Punkt aus $\Omega + \mathcal{O}$ ein Fixpunkt von g, also $d(g, Id) = 16$.

Eine irreduzible Base hat 7 oder mehr Element (Lemma (4.13)) und liegt nicht in einem Octad (Satz(3.44)). 6 Punkte der Base liegen nach dem 7-er Problem also in einem Octad $\mathcal{O}$. Elemente, die diese Punkte fest lassen, liegen im punktweisen Stabilisator von $\mathcal{O}$. Dieser operiert aber regulär auf $\Omega + \mathcal{O}$. Ein beliebiger weiterer Punkt aus $\Omega + \mathcal{O}$ vervollständigt also die Base. Eine irreduzible Base ist also eine 7-elementige Menge, die nicht Teilmenge eines Octads ist. □

Folgerung 4.15 *(i) Auf der Menge der 7-elementigen Teilmengen von Ω hat M_{24} 2 Bahnen, die Bahn der Bases und die der Teilmengen von Octads.*

(ii) Betrachtet man die irreduziblen Bases als Tupel, so hat M_{24} 7 Bahnen. Trennende Invariante ist die Position des Punktes, der nicht Teil des zur Base gehörenden Octads ist.

Beweis: Zu (i): Sei A eine 7-elementige Menge, die Teil des Octads $\mathcal{O}$ ist. M_{24} ist transitiv auf Octads und ein Octad-Stabilisator operiert wie A_8 auf dem Octad, also transitiv auf 7 -elementigen Mengen. Es existiert also ein $g \in M_{24}$ mit $g(A) =$

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

Der punktweise Stabilisator ist isomorph zu C_2^4, also ist $g(A)$ keine Base und $g(A)$ ein Vertreter der Bahn der Nicht-Bases.

Nun sei B eine 7-elementige Menge, die nicht Teilmenge eines Octads ist. Dann ist B nach dem vorherigen Satz eine Base. Mit dem 7-er Problem sehen wir, dass 6 Punkte aus B in einem Octad liegen. Mit den Argumenten oben können wir o.B.d.A. annehmen, dass

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

diese 6 Punkte sind. Der punktweise Stabilisator von $K_1 + K_2$ operiert regulär auf $\Omega + K_1 + K_2$ (Satz (3.44)), also existiert ein $g \in M_{24}$, sodass $g(B)$ unsere Standart-Base $[1, 2, 3, 4, 5, 6, 7]$ ist:

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

Damit liegen alle Bases als Mengen betrachtet in einer Bahn.

Zu (ii): Seien $(a_1, ..., a_7),\ (b_1, ..., b_7) \in \underline{24}^7$ zwei irreduzible Bases. Dann liegen jeweils 6 Punkte in einem Octad, a_i und b_j seien die Punkte, die nicht im jeweiligen Octad liegen.

1. Fall $i = j$: M_{24} ist transitiv auf Octads und 6-fach transitiv auf jedem Octad, also existiert ein $g \in M_{24}$ mit

$$g(a_l) = b_l \ \forall l \neq i.$$

Der punktweise Stabilisator von $\{b_l |\ l \neq i\}$ operiert regulär auf dem Komplement des Octads, also existiert ein h mit

$$h(b_l) = b_l \ \forall l \neq i \text{ und } h(a_i) = b_i \ \Rightarrow \ hg((a_1, ..., a_7)) = (b_1, ..., b_7)$$

2.Fall $i \neq j$: O.B.d.A sind die Octads, mit denen sich die Bases in 6 Punkten schneiden, dieselben. $\mathcal{O}$ sei dieses Octad. Angenommen, es existiert ein $g \in M_{24}$ mit $g((a_1, ..., a_7)) = (b_1, ..., b_7)$. Dann gilt $g \in Stab(\mathcal{O})$, denn g bildet 5 Punkte von $\mathcal{O}$ (a_l für $l \neq i, j$) auf 5 Punkte von $\mathcal{O}$ ab (b_l für $l \neq i, j$). Dies ist aber ein Widerspruch, denn dann kann g $a_j \in \mathcal{O}$ nicht auf $b_j \notin \mathcal{O}$ abbilden. □

Bemerkung 4.16 *Alle irreduziblen Bases haben die gleiche Kardinalität. Damit nennt man M_{24} eine IBIS-Gruppe („Invariant Bases of Invariant Size"). Peter Cameron und Dmitrii Fon-der-Flaas haben in [Cam-Fo] gezeigt, dass für Permutationsgruppen folgende Aussagen äquivalent sind:*

(i) Alle irreduziblen Bases haben die gleiche Kardinalität

(ii) Irreduzible Basen (als Tupel) werden von Umordnung erhalten

(iii) Die Irreduziblen Bases bilden eine Basis eines Matroids.

Zur Weiteren Erklährung siehe [Cam02]

4.3 Codieren und Decodieren mit M_{24}

Angenommen, wir senden eine Permutation $g \in M_{24}$ und erhalten ein Wort $w \in H_{24}$. Dann ist $d(w, g)$ die Anzahl an Fehlern, die aufgetreten sind. Die Frage ist, können wir aus w auf g schließen, d.h. g aus w decodieren, wobei wir ein Wort immer zu einer Permutation mit minimalem Abstand decodieren. Für niedrige $d(w, g)$ ist dies immer möglich ($d(w, g) \leq 7$), für höhere nicht unbedingt.

Indem wir g durch $Id = [1, ..., 24]$ und w durch $g^{-1}w$ ersetzen, können wir das Problem mit folgenden Definitionen genauer formulieren.

Definition 4.17 *Sei $w \in H_{24}$. Wir nehmen den Fall an, dass Id gesendet wurde und wir w erhalten haben.*

- *$d(w, M_{24}) := min\{d(w, g) |\ g \in M_{24}\}$. Wir decodieren w immer zu einem $g \in M_{24}$ mit $d(w, g) = d(w, M_{24})$.*
- *Ist $d(w, Id) = d(w, M_{24})$ und ist Id die einzige Permutation mit diesem Abstand (d.h. w wird immer richtig decodiert), so ist w ein **grünes** Wort.*
- *Ist $d(w, Id) = d(w, M_{24})$ und gibt es weitere Pemutationen mit diesem Abstand (d.h. w wird nicht immer richtig decodiert, kann aber richtig decodiert werden), so ist w ein **gelbes** Wort.*
- *Gilt $d(w, Id) > d(w, M_{24})$ (d.h. w wird nie richtig decodiert), so ist w ein **rotes** Wort.*
- *$P(M_{24}, i)$ bezeichne die Wahrscheinlichkeit, das ein Wort w mit $d(w, Id) = i$ grün ist. (Dies ist natürlcih auch die Wahrscheinlichkeit für $d(w, g) = i$, falls g statt Id gesendet wurde.) $Q(M_{24}, i)$ und $R(M_{24}, i)$ bezeichnen entsprechend die Wahrscheinlichkeiten, dass ein Wort gelb bzw. rot ist.*

In diesem Abschnitt werden wir die Wahrscheinlichkeiten für $i \leq 8$ und $i \geq 21$ berechnen. Für $i \leq 7$ und $i \leq 8$ werden wir zwei konkrete Implementierung des Decodieralgorithmus konstruieren.

4.3.1 7 und weniger Fehler

Treten 7 oder weniger Fehler auf, so kann man immer korrekt decodieren, alle Wörter sind grün. Die Schwierigkeit des effektiven Decodierens ist die Wahl einer passenden UBB. Eine erste Möglichkeit wäre, sich ausreichend Bases zu suchen, sodass diese eine UBB bilden. Dies führt aber schnell zu sehr großen UBBs. (Z.B. pro Octad Auswahl von 6 Punkten + 8-mal. einen weiteren Punkt − denn 7 Punte sind immer disjunkt zu einem Octad $\Longrightarrow$ die UBB enthält $759 \cdot 8 = 6072$ Bases).

Eine weitere Möglichkeit ist es mit einem Covering zu beginnen. Dann bilden die Komplemente der Blöcke ein Uncovering. Falls es sich bei diesen nur um Bases handelt, so hat man eine UBB gefunden. Ansonsten kann man die Mengen, die keine Bases bilden, leicht durch Bases ersetzen. Hierbei verwenden wir, dass M_{24} eine IBIS-Gruppe ist.

Dass dieses Vorgehen für M_{24} sinnvoll ist, zeigt das folgende Lemma.

Lemma 4.18 *Die Wahrscheinlichkeit, dass 7 Punkte eine Base bilden, ist zirka 0,98.*

Beweis: Nach Folgerung (4.15) gibt es $759 \cdot 8 = 6072$ 7-elementige Mengen, die keine Bases sind, und $759 \cdot \binom{8}{6} \cdot 16 = 340032$, die es sind.

Es ist $\frac{340032}{\binom{24}{7}} = 56/57 \approx 0,98$. □

Für M_{24} kann man sich aus Gordons Datenbank [LaJ] ein (24,17,7)-Covering der Größe 58 heraussuchen. Die Menge der Komplemente heißt UBB7 (für 7-Fehler korrigierend), siehe Anhang A. Mit GAP finden wir, dass alle Komplemente Bases sind (bzgl. der Standard-Kopie von M_{24}). Also gilt

Satz 4.19 *UBB7 ist eine 7-UBB der Größe 58.*

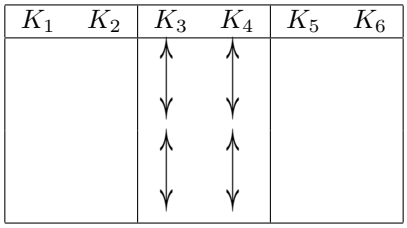
Nun kann man damit den Decodieralgorithmus in GAP implementieren. Die GAP-File und einige Beispiele sind in Anhang C angeben.

4.3.2 8 Fehler

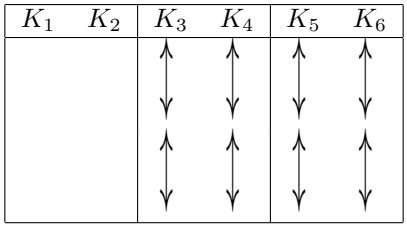
Um den Code praktisch zu nutzen, ist es interessant, sich anzusehen, wie sich der Decodieralgorithmus bei mehr als 7 Fehlern verhält. Dabei hat man zwei Probleme. Zunächst ist mit der oben gewählten UBB nicht gewährleistet, dass jede Fehlermenge disjunkt zu einer Base der UBB ist. Zum Zweiten ist nicht gewährleistet, dass eine Permutation mit minimalem Abstand zum empfangenen Wort tatsächlich auch gesendet wurde.

Das erste Problem kann man für bis zu 8 auftretenden Fehlern lösen, indem man sich ein (24,17,8)-Covering aus der Datenbank sucht und die Komplemente untersucht. Dabei findet man zwei Mengen, die keine Bases sind. Durch Ersetzen dieser erhält man die UBB UBB8 mit 128 Bases. Siehe Anhang B für UBB8 und Anhang C für Beispiele des Decodierens.

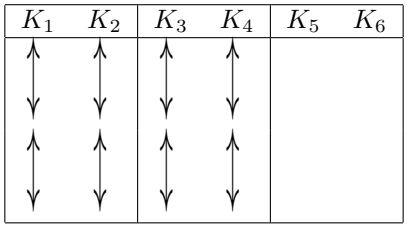
Auch das zweite Problem hat bei 8 Fehlern noch wenig Auswirkungen. Sind höchstens 8 Fehler aufgetreten, so hat die richtige Permutation minimalen Abstand, aber nicht unbedingt als einzige (dies gilt bei mehr Fehlern nicht mehr). Man erkennt also, ob man richtig decodieren kann oder nicht. Ein Beispiel eines Wortes mit 3 nächsten Permutationen ist



Es hat Abstand 8 zu Id, $(00|11|11)^{\pi} =$



und $(11|11|00)^{\pi} =$



Bailey und Bray haben in [Ba-Br] gezeigt, dass M_{12} quasi ein 4-Fehler korrigierder Code ist. Die Wahrscheinlichkeit, dass ein Wort von 4 Fehlern richtig decodiert wird ist zirka 0,96. Man beachte, dass $d(M_{12}) = 8$, denn M_{12} ist scharf 5-fach transitiv.

Für M_{24} kann man ähnlich vorgehen, um zu zeigen dass bei M_{24} die Wahrscheinlichkeit, ein Wort mit 8 Fehlern richtig zu decodieren, sogar $1 - 10^9$ ist. Dies wird das Hauptresultat dieses Unterabschnitts sein.

Angenommen wir haben ein Wort w empfangen und die Permutation $g \in M_{24}$ hat Abstand 8 zu w. Dann hat $g^{-1}w$ Abstand 8 zu Id. Um die Wahrscheinlichkeit, dass w grün ist, zu ermitteln, muss man die Wörter zählen, die Abstand 8 zu Id und zu genau 0,1,2,... weiteren Permutationen haben. Dafür zählen wir die Wörter, die Abstand 8 zu Id und 0,1,2,... weiteren Permutationen

haben, also alle grünen und gelben Wörter. Die gesuchte Wahrscheinlichkeit ist dann

$$\frac{\#grüne\ Wörter}{\#grüne\ Wörter + \#gelbe\ Wörter}.$$

Bemerkung 4.20 $|\{\ w \in H_{24} \mid d(w, Id) = 8\}| = \binom{24}{8} \cdot 23^8 = 57.595.458.655.602.351$ *Dies ist die Anzahl aller grünen und gelben Wörter.*

Lemma 4.21 *Sei $g \in M_{24}$ mit $d(g, Id) = 16$.*
Dann gibt es $\binom{16}{8}$ Wörter $w \in H_{24}$ mit $d(w, Id) = d(w, g) = 8$.

Beweis: g lässt 8 Punkte fix. Diese Punkte bilden ein Octad nach Lem. (4.12). Sei w nun ein gesuchtes Wort. Dann stimmt w mit Id und g in je 16 Punkten überein. w und Id stimmen also auf mindestens 8 Punkten überein (d.h. w lässt diese fix), die keine Fixpunkte von g sind. Dann muss aber w auf den 8 Fixpunkten von g mit g und Id übereinstimmen und muss die verbleibenden 8 Punkte gleich wie g abbilden. w ist also durch seine 8 Fixpunkte, die g nicht fix lässt, festgelegt. □

Folgerung 4.22 $|\{\ (w, g) \in H_{24} \times M_{24} \mid d(w, Id) = d(w, g) = 8\}| = 759 \cdot 15 \cdot \binom{16}{8} = 146.524.950$

Beweis: g liegt im punktweisen Stabilisator eines Octads. Also gibt es $759 \cdot 15$ Permutationen mit Abstand 16 zu Id. Zu 8 der nicht-fixen Punkte von g gehört dann nach dem oberen Lemma genau ein Wort, dass die Bedingungen erfüllt. □

Satz 4.23 *Sei $w \in H_{24}$.*
Dann gibt es höchstens 3 Permutationen in M_{24} mit Abstand 8 zu w.

Beweis: O.B.d.A. stimmt w mit Id in 8 Punkten überein. Sei $g \in M24$ mit $d(w, g) = 8$. Dann lässt g nach Lemma (4.17) das Octad $\mathcal{O}_1$ fest. w bildet $\mathcal{O}_1$ wie g und Id ab. Weiterhin existiert eine 8-el. Menge $A \subseteq \Omega$, deren Punkte w und g gleich abbilden. Dann sind Id und w auch auf den fehlenden Punkten $B := \Omega + A + \mathcal{O}_1$ gleich.

Angenommen es existiert eine weitere Permutation $h \in M_{24}$ mit $d(w, h) = 8$. Dann sind die Fixpunkte von h das Octad $\mathcal{O}_2$. Es gilt $\mathcal{O}_2 \neq \mathcal{O}_1$, da w sonst keinen Punkt aus $\Omega + \mathcal{O}_1$ wie h abbildet. Weiterhin gilt $d(g, h) = 16$, also liegt $h^{-1}g$ im punktweisen Stabilisator des Octads $\mathcal{O}_3 \neq \mathcal{O}_1$. g und h bilden nur $\mathcal{O}_3$ gleich ab, also bildet w $\mathcal{O}_3$ auch so ab. $\Omega + \mathcal{O}_3$ sind damit alle Fixpunkte von w und $w \in S_{24}$. Es gilt damit $\mathcal{O}_3 = A$ und $\mathcal{O}_2 = B$. g ist also auf A und B und damit auf ganz Ω durch w eindeutig festgelegt, falls es existiert. Damit sind keine weiteren Permutationen mit Abstand 8 zu w möglich. □

Folgerung 4.24 *Sein $w \in H_{24}$ und $g, h, k \in M_{24}$ pw. vers. mit $d(w, g) = d(w, h) = d(w, k) = 8$.*
Dann gilt $w \in S_{24}$, und die Punkte, auf denen w mit g und h, g und k bzw. h und k übereinstimmt bilden jeweils Octads. Zusammen partitionieren sie Ω.

Beweis: O.B.d.A. g=Id. Es tritt dann genau der Fall im oberer Beweis ein. Die Fixpunkte von h und k und die Nicht-Fixpunkte von w bilden dann eine Partition in 3 Octads. w ist durch Id, h und k festgelegt und damit $w \in S_{24}$. Im Beispiel am Anfang dieses Kapitels tritt dieser Fall auf.

Lemma 4.25 $|\{(g, h, w) \mid g, h \in M_{24},\ w \in H_{24},\ d(w, Id) = d(w, g) = d(w, h) = 8\}| = 759 \cdot 30 \cdot 7 = 159.390$

Beweis: Es gibt 759 Möglichkeiten für das Octad der Fixpunkte von g. Sei $\mathcal{O}_g \in \mathcal{G}$ dieses Octad. Sei $\mathcal{O}_h \in \mathcal{G}$ das Fixpunkt-Octad von h. Dann sind $\mathcal{O}_g$ und $\mathcal{O}_h$ disjunkt und es gibt 30 Möglichkeiten für $\mathcal{O}_h$ (Folg. (3.46)). $\mathcal{O}$ komplementiere $\mathcal{O}_g + \mathcal{O}_h$. w fixiert nur die Punkte aus $\mathcal{O}$ nicht. Dort ist es durch g und h festgelegt und g und h bilden $\mathcal{O}$ gleich ab. Damit sind w und h durch g festgelegt. Wir bestimmen die Möglichkeiten, g zu wählen. Es gibt 7 Möglichkeiten für so ein g, denn:

M_{24} ist transitiv auf der Menge der Octads, also existiert ein $\sigma \in M_{24}$ mit $\sigma(\mathcal{O}_g) = K_1 + K_2$. $Stab(K_1 + K_2)$ ist transitiv auf den Octads, die leeren Schnitt mit $K_1 + K_2$ haben (Satz (3.45)), also existiert ein $\tau \in Stab(K_1 + K_2)$ mit $\tau(\mathcal{O}_h) = K_3 + K_4$. Man ersetze nun g, h und w durch ihre Konjugierten mit $\tau\sigma$. Dann erfüllen sie immer noch die oberen Bedingungen und g ist Element eines Normalteilers des punktweisen Stabilisators mit Index 2 ($\cong C_2^3$). Die Erzeuger sind die Automorphismen, die von den Hexawörter (00|11|11) und (00|$\omega\omega$|$\omega\omega$) und von der Permutation (3,4)(5,6) der Spalten induziert werden. Zieht man die Identität ab, so bleiben 7 Möglichkeiten. □

Damit haben wir alle Mengen gezählt, um unser Hauptresultat zu beweisen.

Satz 4.26 *Die Wahrscheinlichkeit, dass ein Wort mit 8 Fehlern immer richtig decodiert wird, beträgt zirka* $1 - 2,5 \cdot 10^{-9}$.

Beweis: Zunächst noch einmal zusammengefasst die oben bestimmten Kardinalitäten:

$$\begin{aligned}
a_1 &:= |\{\ w \in H_{24} \mid d(w, Id) = 8\}| = \tbinom{24}{8} \cdot 23^8 = 57.595.458.655.602.351 \\
a_2 &:= |\{\ (w, g) \in H_{24} \times M_{24} \mid d(w, Id) = d(w, g) = 8\}| \ = \ 759 \cdot 15 \cdot \tbinom{16}{8} \ = \ 146.524.950 \\
a_3 &:= |\{(g, h, w) \mid g, h \in M_{24},\ w \in H_{24},\ d(w, Id) = d(w, g) = d(w, h) = 8\}| = 759 \cdot 30 \cdot 7 = 159.390
\end{aligned}$$

Mit n_i bezeichne man die Anzahl an Wörtern mit Abstand 8 zu Id, die insgesamt zu genau i Permutationen Abstand 8 haben ($i = 1, 2, 3$). n_1 ist die Anzahl aller grünen und $n_2 + n_3$ die Anzahl aller gelben Wörter.

Man erhält das folgende Gleichungssystem:

$$\begin{aligned}
n_1 + n_2 + n_3 &= a_1 \\
n_2 + 2n_3 &= a_2 \\
2n_3 &= a_3
\end{aligned}$$

Die Lösung ist

$$\begin{aligned}
n_1 &= 57595458509157096 \\
n_2 &= 146365560 \\
n_3 &= 79695
\end{aligned}$$

Die Wahrscheinlichkeit, dass Wort mit Abstand 8 zu Id grün ist, ist dann

$$\frac{n_1}{n_1 + n_2 + n_3} \approx 1 - 2,5 \cdot 10^{-9}$$

□

4.3.3 9 und mehr Fehler

Für mehr als 8 Fehler kann es vorkommen, dass das Codewort mit dem geringsten Abstand nicht das übertragene ist, d.h. es treten rote Wörter auf. Die Decodierung kann also falsch sein. Erschwerend kommt hinzu, dass es keine bekannten (24,17,r)-Covernings für $r > 8$ gibt (zumindest nach [LaJ]). Somit kann man eine r-UBB nicht auf diesem Weg konstruieren, obwohl r-UBB's für $r \leq 15$ existieren (Satz (4.10)).

Um $P(M_{24}, r), Q(M_{24}, r)$ und $R(M_{24}, r)$ für $r \leq 15$ mit dem Computer zu berechnen, könnte man wie Bailey und Bray (für M_{12}, s. [Ba-Br]) vorgehen. Man betrachte nacheinander alle Vertreter der Bahnen von r-elementigen Mengen (bzg. der Operation von M_{24}) als Fehlermengen. Dabei bestimmt man die Anzahl aller grünen, gelben und roten Wörter, deren Fehlermenge gerade die Vertretermenge ist (dies sind aufsummiert 23^r Wörter). Zum Decodieren verwendet man den

Decodieralgorithmus. Ohne eine kleine $r - UBB$ ist dieser aber wenig effektiv und zeitaufwendig. Deswegen habe ich darauf verzichtet. Die Wahrscheinlichkeit, dass 9 oder mehr Fehler auftreten, ist auch sehr gering.

Sind 20 oder mehr Fehler aufgetreten, so kann man die Wahrscheinlichkeiten wieder „von Hand“ bestimmen. Dies hat aber wohl eher wenig praktischen Nutzen.

Lemma 4.27 *Es gibt keine grünen Wörter für $r \geq 18$.*

Beweis: Sei $w \in H_{24}$ mit $r := d(w, Id) \geq 18$. Die Menge $A := \{x \in \underline{n} |\ w(x) = x\}$, auf der w und Id übereinstimmen, hat $24 - r \leq 6$ Elemente. Damit ist der punktweise Stabilisator nicht trivial, es gibt also ein $g \in M_{24}$, $g \neq Id$, mit $g(x) = x$ für alle $x \in A$. Damit gilt $d(w, g) \leq r$ und w gelb oder rot. □

Lemma 4.28 *Sei $w \in H_{24}$ mit $d(w, Id) \geq 20$. $A := \{x \in \Omega |\ w(x) = x\}$ bezeichne das Komplement der Fehlermenge.*

Dann ist w genau dann gelb, wenn A das Bild von w ist (d.h. falls man w als Liste schreibt, kommen genau die Punkte aus A vor).

Beweis: „ $\Rightarrow$ “ : Angenommen, es existiert ein $y \in \underline{n}$ mit $w(y) \notin A$. $|A| \leq 4$ und M_{24} ist 5-fach, transitiv, also existiert eine Permutation $g \neq Id$ mit

$$g(y) = w(y) \text{ und } \forall x \in A\ g(x) = x.$$

$$\Rightarrow\ d(w, g) \leq 24 - (|A| + 1).$$

Also ist w ein rotes Wort, ein Widerspruch.

„ $\Leftarrow$ “ : In w (als Liste geschrieben) kommen nur $|A| = 24 - d(w, Id)$ Zahlen vor, also

$$d(w, Id) = d(w, S_{24}) \leq d(w, M_{24}).$$

Damit ist w nicht rot und aus dem letzten Lemma folgt, dass w dann ein gelbes Wort sein muss. □

Satz 4.29 *Für $r \geq 20$ gibt es genau $(24 - r)^r$ gelbe Wörter, d.h. für die Wahrscheinlichkeiten gilt*

$$P(M_{24}, r) = 0,\ \ Q(M_{24}, r) = \frac{(24 - r)^r}{23^r},\ \ R(M_{24}, r) = 1 - \frac{(24 - r)^r}{23^r}$$

Beweis: Sei w ein Wort mit $d(w, Id) = r$ und A das Komplement der Fehlermenge wie in den letzten Lemmata. Dann gilt $|A| \leq 4$, also gibt es ein $g \in M_{24}$ mit $g(A) = \{1, 2, ..., 24 - r\}$. Man ersetze w durch gwg^{-1}.

Es gibt 23^r Wörter, die nur auf $A = \{1, 2, ..., 24 - r\}$ mit Id übereinstimmen, wobei nach dem letzten Lemma genau $|A|^r = (24 - r)^r$ davon gelbe Wörter sind. Es gibt keine grünen Wörter, die Wahrscheinlichkeiten ergeben sich entsprechend □

Zum Abschluss sind hier alle berechneten Wahrscheinlichkeiten angegeben.

r	$P(M_{24}, r)$ (grüne Wörter)	$Q(M_{24}, r)$ (gelbe Wörter)	$R(M_{24}, r)$ (rote Wörter)
0-7	1	0	0
8	$1 - 2,5 \cdot 10^{-9}$	$2,5 \cdot 10^{-9}$	0
9-17	?	?	?
18-19	0	?	?
20	0	$6{,}4 \cdot 10^{-16}$	$1 - 6,4 \cdot 10^{-16}$
21	0	$2,7 \cdot 10^{-19}$	$1 - 2,7 \cdot 10^{-19}$
22	0	$4,6 \cdot 10^{-24}$	$1 - 4,6 \cdot 10^{-24}$
23	0	$4,8 \cdot 10^{-32}$	$1 - 4,8 \cdot 10^{-32}$
24	0	0	1

Literaturverzeichnis

[Ba06a] Robert F. Bailey, Permutation groups, error-correcting codes and uncoverings, Doktorarbeit, University of London (2006).

[Ba06b] Robert F. Bailey, Uncovering-by-bases for base-transitive permutation groups. Des. Codes Cryptogr. 41, 153-176 (2006).

[Ba09] Robert F. Bailey, Error-correcting codes from permutation groups. Discrete Math. 309, 42534265 (2009).

[Ba-Br] Robert F. Bailey, John N. Bray, Decoding the Mathieu Group M_{12}. Adv. Math Commun. 1, 477-487 (2007).

[Cam99] Peter J. Cameron, Permutation groups. Cambridge University Press (1999).

[Cam-Fo] Peter J. Cameron, Dmitrii G.Fon-Der-Flaas, Bases for permutation groups and matrods. European Journal of Combinatorics 24, 881-890 (2003).

[Cam02] Peter J. Cameron, Polynomial aspects of codes, matroids and permutation groups. http://www.maths.qmw.ac.uk/ pjc/csgnotes/cmpgpoly.pdf (2002).

[Cam10] Peter J. Cameron, Permutation codes. European Journal of Combinatorics 31, 482-490 (2010).

[Con-Sl] John H. Conway, Neil L.A. Sloane, Spere Packings, Lattices and Groups, Grundlehren der mathematischen Wissenschaft 290. Springer-Verlag (1988).

[Cu] Robert Curtis, A new combinatorial approach to M_{24}. Mathematics Proceedings of the Cambridge Philosophical Society 79, 25-42 (1976).

[GAP] The GAP Group, GAP: Groups, Algorithms and Programming. Version 4.4.12 (17.12.2008). http://gap-system.org

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

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

[Hi] Gerhard Hiss, Die sporadischen Gruppen. Jahresbericht der DMV 105, 169-193 (2003).

[Hu] Bertram Huppert, Endliche Gruppen I. Springer-Verlag (1967).

[LaJ] D.M.Gordon, La Jolla Covering Repository (Datenbank für Coverings). http://www.ccrwest.org/cover.html (24.6.2011).

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

Anhang A

UBB7

[16, 17, 18, 19, 20, 22, 23]
[15, 17, 19, 21, 22, 23, 24]
[15, 16, 18, 21, 22, 23, 24]
[15, 16, 17, 19, 20, 21, 24]
[14, 18, 20, 21, 22, 23, 24]
[14, 16, 18, 19, 20, 23, 24]
[14, 16, 17, 20, 22, 23, 24]
[14, 16, 17, 18, 19, 22, 24]
[14, 15, 18, 19, 20, 22, 23]
[14, 15, 17, 18, 20, 21, 24]
[14, 15, 16, 19, 20, 21, 22]
[14, 15, 16, 17, 18, 21, 23]
[13, 17, 18, 19, 20, 22, 24]
[13, 16, 19, 20, 21, 22, 23]
[13, 16, 17, 18, 20, 21, 23]
[13, 16, 17, 18, 19, 21, 22]
[13, 15, 18, 19, 21, 23, 24]
[13, 15, 17, 20, 21, 22, 23]
[13, 15, 16, 18, 20, 22, 24]
[13, 15, 16, 17, 19, 23, 24]
[13, 14, 17, 19, 20, 21, 23]
[13, 14, 17, 18, 19, 21, 22]
[13, 14, 16, 18, 19, 21, 24]
[13, 14, 16, 17, 21, 22, 24]
[13, 14, 15, 19, 20, 22, 24]
[13, 14, 15, 17, 18, 23, 24]
[13, 14, 15, 16, 20, 21, 23]
[13, 14, 15, 16, 19, 22, 23]
[13, 14, 15, 16, 17, 18, 20]

[4, 5, 6, 7, 8, 10, 11]
[3, 5, 7, 9, 10, 11, 12]
[3, 4, 6, 9, 10, 11, 12]
[3, 4, 5, 7, 8, 9, 12]
[2, 6, 8, 9, 10, 11, 12]
[2, 4, 6, 7, 8, 11, 12]
[2, 4, 5, 8, 10, 11, 12]
[2, 4, 5, 6, 7, 10, 12]
[2, 3, 6, 7, 8, 10, 11]
[2, 3, 5, 6, 8, 9, 12]
[2, 3, 4, 7, 8, 9, 10]
[2, 3, 4, 5, 6, 9, 11]
[1, 5, 6, 7, 8, 10, 12]
[1, 4, 7, 8, 9, 10, 11]
[1, 4, 5, 6, 8, 9, 11]
[1, 4, 5, 6, 7, 9, 10]
[1, 3, 6, 7, 9, 11, 12]
[1, 3, 5, 8, 9, 10, 11]
[1, 3, 4, 6, 8, 10, 12]
[1, 3, 4, 5, 7, 11, 12]
[1, 2, 5, 7, 8, 9, 11]
[1, 2, 5, 6, 7, 9, 10]
[1, 2, 4, 6, 7, 9, 12]
[1, 2, 4, 5, 9, 10, 12]
[1, 2, 3, 7, 8, 10, 12]
[1, 2, 3, 5, 6, 11, 12]
[1, 2, 3, 4, 8, 9, 11]
[1, 2, 3, 4, 7, 10, 11]
[1, 2, 3, 4, 5, 6, 8]

Anhang B

UBB8

$[1, 2, 3, 4, 5, 7, 9]$
$[1, 2, 3, 4, 5, 7, 10]$
$[1, 2, 3, 4, 7, 10, 11]$
$[1, 2, 3, 4, 8, 9, 11]$
$[1, 2, 3, 5, 6, 8, 9]$
$[1, 2, 3, 5, 6, 8, 10]$
$[1, 2, 3, 5, 6, 10, 11]$
$[1, 2, 3, 5, 7, 9, 11]$
$[1, 2, 3, 6, 7, 8, 11]$
$[1, 2, 3, 7, 8, 9, 10]$
$[1, 2, 4, 5, 6, 8, 11]$
$[1, 2, 4, 5, 8, 9, 10]$
$[1, 2, 4, 5, 9, 10, 11]$
$[1, 2, 4, 6, 7, 8, 9]$
$[1, 2, 4, 6, 7, 9, 10]$
$[1, 2, 4, 6, 7, 9, 11]$
$[1, 2, 5, 7, 8, 10, 11]$
$[1, 2, 6, 8, 9, 10, 11]$
$[1, 3, 4, 5, 6, 7, 8]$
$[1, 3, 4, 5, 6, 9, 11]$
$[1, 3, 4, 5, 7, 8, 11]$
$[1, 3, 4, 6, 8, 9, 10]$
$[1, 3, 4, 6, 8, 10, 11]$
$[1, 3, 5, 6, 7, 9, 10]$
$[1, 3, 5, 8, 9, 10, 11]$
$[1, 3, 6, 7, 9, 10, 11]$
$[1, 4, 5, 6, 7, 8, 10]$
$[1, 4, 5, 6, 7, 10, 11]$
$[1, 4, 7, 8, 9, 10, 11]$
$[1, 5, 6, 7, 8, 9, 11]$
$[1, 14, 16, 17, 18, 22, 23]$
$[1, 15, 16, 17, 19, 21, 23]$
$[2, 3, 4, 5, 6, 7, 11]$
$[2, 3, 4, 5, 6, 9, 10]$
$[2, 3, 4, 5, 8, 10, 11]$
$[2, 3, 4, 6, 7, 8, 10]$
$[2, 3, 4, 6, 9, 10, 11]$
$[2, 3, 5, 6, 8, 9, 11]$
$[2, 3, 7, 8, 9, 10, 11]$
$[2, 4, 5, 6, 7, 8, 9]$
$[2, 4, 5, 7, 8, 9, 11]$
$[2, 4, 6, 7, 8, 10, 11]$
$[2, 5, 6, 7, 8, 9, 10]$
$[2, 5, 6, 7, 9, 10, 11]$
$[2, 14, 16, 17, 18, 22, 23]$
$[2, 15, 16, 17, 19, 21, 23]$
$[3, 4, 5, 7, 8, 9, 10]$
$[3, 4, 5, 7, 9, 10, 11]$
$[3, 4, 6, 7, 8, 9, 11]$
$[3, 5, 6, 7, 8, 10, 11]$
$[3, 14, 16, 17, 18, 22, 23]$
$[3, 15, 16, 17, 19, 21, 23]$
$[4, 5, 6, 8, 9, 10, 11]$
$[4, 14, 16, 17, 18, 22, 23]$
$[4, 15, 16, 17, 19, 21, 23]$
$[5, 14, 16, 17, 18, 22, 23]$
$[5, 15, 16, 17, 19, 21, 23]$
$[6, 14, 16, 17, 18, 22, 23]$
$[7, 14, 16, 17, 18, 22, 23]$
$[7, 15, 16, 17, 19, 21, 23]$
$[8, 14, 16, 17, 18, 22, 23]$
$[8, 15, 16, 17, 19, 21, 23]$
$[9, 14, 16, 17, 18, 22, 23]$
$[12, 13, 14, 15, 16, 21, 23]$
$[12, 13, 14, 15, 17, 18, 20]$
$[12, 13, 14, 15, 17, 22, 24]$
$[12, 13, 14, 16, 18, 19, 20]$
$[12, 13, 14, 16, 19, 22, 24]$
$[12, 13, 14, 17, 19, 21, 23]$
$[12, 13, 14, 18, 20, 21, 23]$
$[12, 13, 14, 18, 20, 22, 24]$
$[12, 13, 14, 21, 22, 23, 24]$

[12, 13, 15, 16, 17, 18, 24]
[12, 13, 15, 16, 17, 20, 22]
[12, 13, 15, 17, 18, 22, 23]
[12, 13, 15, 17, 20, 21, 24]
[12, 13, 16, 18, 19, 21, 22]
[12, 13, 16, 18, 19, 23, 24]
[12, 13, 16, 19, 20, 21, 24]
[12, 13, 16, 19, 20, 22, 23]
[12, 14, 15, 16, 17, 19, 23]
[12, 14, 15, 18, 19, 21, 24]
[12, 14, 15, 18, 19, 22, 23]
[12, 14, 15, 19, 20, 21, 22]
[12, 14, 15, 19, 20, 23, 24]
[12, 14, 16, 17, 18, 21, 24]
[12, 14, 16, 17, 20, 21, 22]
[12, 14, 16, 17, 20, 23, 24]
[12, 15, 16, 18, 20, 21, 23]
[12, 15, 16, 18, 20, 22, 24]
[12, 15, 16, 21, 22, 23, 24]
[12, 17, 18, 19, 20, 21, 23]
[12, 17, 18, 19, 20, 22, 24]
[12, 17, 19, 21, 22, 23, 24]
[12, 18, 20, 21, 22, 23, 24]
[13, 14, 15, 16, 17, 19, 21]
[13, 14, 15, 16, 18, 20, 23]
[13, 14, 15, 16, 18, 21, 22]
[13, 14, 15, 16, 20, 21, 24]
[13, 14, 15, 16, 22, 23, 24]
[13, 14, 17, 18, 19, 20, 21]
[13, 14, 17, 18, 19, 23, 24]
[13, 14, 17, 19, 20, 22, 23]
[13, 14, 17, 19, 21, 22, 24]
[13, 15, 17, 18, 19, 21, 22]
[13, 15, 17, 19, 20, 23, 24]
[13, 15, 18, 19, 20, 22, 24]
[13, 15, 18, 19, 21, 23, 24]
[13, 15, 19, 20, 21, 22, 23]
[13, 16, 17, 18, 20, 22, 24]
[13, 16, 17, 18, 21, 22, 23]
[13, 16, 17, 20, 21, 23, 24]
[13, 18, 20, 21, 22, 23, 24]
[14, 15, 16, 17, 18, 19, 22]
[14, 15, 16, 17, 19, 20, 24]
[14, 15, 17, 18, 20, 22, 24]
[14, 15, 17, 18, 21, 23, 24]
[14, 15, 17, 20, 21, 22, 23]
[14, 16, 18, 19, 20, 21, 23]
[14, 16, 18, 19, 22, 23, 24]
[14, 16, 19, 20, 21, 22, 24]
[15, 16, 17, 18, 19, 20, 21]
[15, 16, 17, 18, 19, 20, 23]
[15, 16, 17, 19, 21, 22, 24]
[15, 16, 17, 19, 21, 23, 9]
[15, 16, 17, 19, 22, 23, 24]
[15, 18, 20, 21, 22, 23, 24]
[17, 18, 20, 21, 22, 23, 24]

Anhang C

Decodieralgorithmus

Hier ist der Decodieralgorithmus als GAP-Code angegeben. Siehe auch [Ba06a], S. 130. Zur Bestimmung des Gruppenelementes, das eine Base wie eine gegebene Wort abbildet (Base-and-strong-generators-Algorithmus), wird die Standard-Funktion von GAP („RepresentativeAction“) verwendet. In der Eingabe bezeichnet G die Gruppe, U die UBB, n den Permutationsgrad von G, r die Anzahlt an maximal zu korrigierenden Fehlern und w das zu decodierende Wort.

```
UBBDecode:=function(G,U,n,r,w)
   local z,x,y,i,h,L;
   L:=[];
   for x in U do
      y:=[];
      for i in [1..Size(x)] do
         y[i]:=w[x[i]];
      od;
       if Size(Set(y))=Size(x) then
           h:=RepresentativeAction(G,x,y,OnTuples);
           if h<>fail then
              z:=OnTuples([1..n],h);
              if DistanceVecFFE(z,w)<=r then
                 if not z in L then
                    Add(L,z);
                 fi;
              fi;
            fi;
       fi;
   od;

   return L;
end;
```

Hier seien noch einige Beispiele der Verwendung in GAP angegeben:

```
gap> #Standard-Kopie von M24:
gap> M24;
Group([(1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23),
  (3,17,10,7,9)(4,13,14,19,5)(8,18,11,12,23)(15,20,22,21,16),
  (1,24)(2,23)(3,12)(4,16)(5,18)(6,10)(7,20)(8,14)(9,21)(11,17)(13,22)(15,19) ])


gap> #Wort mit 7 Fehlern:
gap> w:=[ 2, 3, 4, 5, 6, 7, 8, 8, 9, 10, 11, 12, 13, 14, 15,
 16, 17, 18, 19, 20, 21, 22, 23, 24 ];
[ 2, 3, 4, 5, 6, 7, 8, 8, 9, 10, 11, 12, 13, 14, 15,
 16, 17, 18, 19, 20, 21, 22, 23, 24 ]

gap> #wird decodiert mit UBB7, s. S. 42, zu
gap> UBBDecode(M24, UBB7 , 24 , 7 , w);
[ [ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15,
 16, 17, 18, 19, 20, 21, 22, 23, 24 ] ]


gap> #Wort mit 8 Fehlern:
gap> w1:=ShallowCopy(w);;
gap> w1[8]:=1;;
gap> w1;
[ 2, 3, 4, 5, 6, 7, 8, 1, 9, 10, 11, 12, 13, 14, 15,
 16, 17, 18, 19, 20, 21, 22, 23, 24 ]

gap> #kann von obererm Alg nicht decodiert werden:
gap> UBBDecode(M24, UBB7 , 24 , 7 , w1);
[  ]

gap> UBBDecode(M24, UBB7 , 24 , 8 , w1);
[ [ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15,
 16, 17, 18, 19, 20, 21, 22, 23, 24 ] ]
gap> #klappt zufaellig

gap> #mit UBB8, s. S. 43, kannn immer decodiert werden:
gap> UBBDecode(M24, UBB8 , 24 , 8 , w1);
[ [ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15,
 16, 17, 18, 19, 20, 21, 22, 23, 24 ] ]

gap> #w1 ist also ein gruenes Wort


gap> #Ein gelbes Wort ist die Permutation aus dem Beispiel auf S. 42:
gap> a:=(3,8)(9,19)(11,13)(23,18);
(3,8)(9,19)(11,13)(18,23)

gap> #in Listenschreibweise:
gap> wa:=OnTuples([1..24],a);
```

```
[ 1, 2, 8, 4, 5, 6, 7, 3, 19, 10, 13, 12, 11, 14, 15,
 16, 17, 23, 9, 20, 21, 22, 18, 24 ]

gap> UBBDecode(M24, UBB8 , 24 , 8 , wa);
[ [ 1, 2, 8, 4, 5, 6, 7, 3, 19, 16, 13, 21, 11, 15,
   14, 10, 17, 23, 9, 24, 12, 22, 18, 20 ],
  [ 4, 5, 8, 1, 2, 7, 6, 3, 19, 10, 13, 12, 11, 14, 15,
   16, 22, 23, 9, 20, 21, 17, 18, 24 ],
  [ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15,
   16, 17, 18, 19, 20, 21, 22, 23, 24 ] ]

gap> #also drei naechste Permutationen
```