Handout

Die sporadische Gruppe M_{24} als Automorphismengruppe des Golaycodes

10.12.2010

von David Dursthoff

Der Vortrag beruht größtenteils auf dem Buch „Twelve Sporadic Groups“ von Robert L. Griess, Jr. .

1 Sätze aus der Gruppentheorie

Lemma 1.1 *Sei G eine Gruppe und N ein Normalteiler. G operiere primitiv Menge M.*
Wenn N nicht trivial auf M operiert, so operiert es N transitiv.

Satz 1.2 ***(Burnsides Satz vom normalen p-Komplement)***
Sei G eine Gruppe, p eine Primzahl und P eine p-Sylowuntergruppe von G mit $P \leq Z(N_G(P))$.
Dann hat G ein normales p-Komplement, d.h. es existiert ein $N \lhd G$ mit $N \cap P = \{1\}$ und $G = NP$.

Lemma 1.3 *Sei G eine p-Gruppe, d.h. $|G| = p^a$.*
Dann gilt $|Aut(G)| = p^b n$ mit $b \leq a$, $p \nmid n$ und n teilt $|GL(a,p)| = \prod_{i=0}^{a-1}(p^d - p^i)$.

Lemma 1.4 *Sei $n > 1$ und $m = n$ oder $m = n+1$. x sei ein n-Zykel in S_m.*
Dann sind Zentralisator und Normalisator gegeben durch

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

Lemma 1.5 ***(Frattini-Argument)***
Sei G eine Gruppe, K ein Normalteiler und $P \leq K$. G lasse die K-Konjugationsklasse von P invariant.
Dann gilt $G = N_G(P)K$.

2 Der Hexacode

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

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

Definition 2.1 *Sei K ein Körper und $C \leq K^n$ ein Code.*

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

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

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

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

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

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

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

  für einen Körperautomorphismus σ.

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

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

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

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

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

Definition 2.2 *Ein **Hexacode** bezeichnet einen [6,3,4]-Code über $\mathbb{F}_4$. Codewörter eines Hexacode heißen Hexacodewörter. $\mathcal{H}$ sei der Standard-Hexacode, der von den folgenden Vektoren erzeugt wird:*

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

Bemerkung 2.3

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

Lemma 2.4 *Sei $x \in \mathbb{F}_4^6$, $s := x_1 + x_2$*
Dann ist $x \in \mathcal{H}$ genau dann, wenn

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

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

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

Satz 2.5

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

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

Satz 2.6 ***(Fehlerkorrektur-Eigenschaften des Hexacodes)***

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

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

Satz 2.7 ***(Charakterisierung von*** $Aut^*(\mathcal{H})$***)***
Sei $Aut^*(\mathcal{H}) = \{g \in Mon^*(6, \mathbb{F}_4) |\ g(\mathcal{H}) = \mathcal{H}\}$ *die Automorphismengruppe des Hexacodes.* $Aut^*(\mathcal{H})$ *operiert auf* $X := \{< e_1 >, ..., < e_6 >\}$. $\pi' : Aut^*(\mathcal{H}) \to Sym(X) = S_6$ *sei die Permutationsdarstellung.*

Dann gilt

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

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

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

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

3 Der binäre Golaycode

Definition 3.1 ***(Golaycode)***
Der binäre Golaycode bezeichnet einen [24,12,8]-Code über $\mathbb{F}_2$.
Dies ist üblicherweise der erweiterte Golaycode, der aus dem [23,12,7]-Golaycode durch hinzufügen eines Kontrolbits hervorgeht (sodass alle Codewörter ein gerades Gewicht haben). In diesem Vortrag verwende ich nur den erweiterten Golaycode. Bez.: $\mathcal{C}, \mathcal{C}_{24}, \mathcal{G}$.

Ω bezeichne eine 24-elementige Menge.

- $Pot(\Omega) = \{0, 1\}^\Omega$ (Menge aller charakteristischen Funktionen) ist ein 24-dimensionaler $\mathbb{F}_2$-Vektorraum mit

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

$$1A = A \text{ und } 0A = \emptyset\ \forall A \in Pot(\Omega)$$

- Die Gruppe der Monomialtransformatinen ist $Mon^*(Pot(\Omega)) = Mon(Pot(\Omega)) = Sym(\Omega) \cong S_{24}$.
- $(A, B) := \ |A \cap B|\ (mod\ 2)$ 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.
- $l : \Omega \to \mathbb{F}_4$ heißt skalare Labelabbildung, falls l eingeschränkt auf jede der K_i bijektiv ist.

- Zur skalaren Labelabbildung kann man einen $\mathbb{F}_2$-Vektorraum-Homomorphismus
$$\mathcal{L} : Pot(\Omega) \to \mathbb{F}_4^6,\ A \mapsto\ (\mathcal{L}_1(A), ..., \mathcal{L}_6(A)) \text{ mit } \mathcal{L}_i(A) := \sum_{x \in A \cap K_i} l(x),$$
die sogenannte (6-Tubel-)Labelabbildung definieren. Die $\mathcal{L}_i$ sind die i-ten Komponenten der Labelabbildung.

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

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

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

Definition 3.2 *Eine Menge $A \in Pot(\Omega)$ heißt **ausgewogen**, falls $|A \cap K_i|$ gerade für alle K_i bzw. ungerade für alle K_i ist. Dann nennen wir A gerade oder von gerader Parität bzw. ungerade oder von ungerader Parität.*

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

Lemma 3.3

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

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

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

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

Lemma 3.4 *$\mathcal{L}$ bildet $\mathcal{W}$ auf $\mathbb{F}_4^6$ ab, ist also eingeschränkt auf $\mathcal{W}$ immer noch surjektiv.*

Definition 3.5 $\mathcal{G} := \mathcal{W} \cap \mathcal{L}^{-1}(\mathcal{H})$

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

Satz 3.6 *$\mathcal{G}$ ist ein Golaycode.*

Definition 3.7

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

Bemerkung 3.8 *Sei (P, φ) ein Paar aus geordneter Partition $P = \{X_1, ..., X_6\}$ und skalarem Label φ.*

- *Analog zu oben kann man einen Golaycode mit P und φ konstruieren. Bezeichnung: $\mathcal{G}(P, \varphi)$. $\mathcal{G}$ bezeichne den Standard-Golaycode $\mathcal{G}(\Xi, l) = \mathcal{G}$.*
- *$\Psi : \Omega \to \Omega_{(P,\varphi)} := \mathbb{F}_4 \times \{1, ..., 6\},\ x \mapsto (l(x), i)$ 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.*

Satz 3.9

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

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

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

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

Satz 3.10 *Jede 4-elementige Menge ist Teil genau eines ungeordneten Sextetts. Es gibt $\frac{1}{6}\binom{24}{4} = 1771 = 7 \cdot 11 \cdot 23$ ungeordnete Sextette.*

Definition 3.11 ***(Steiner-System)***
Ein Steinersystem S mit Paarametern (a,b,n), $a, b, n \in \mathbb{N}$, ist eine Familie S von b-elementigen Mengen, die Teilmengen einer Menge Ω mit n Elementen sind. Außerdem gelte:

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

Satz 3.12 *Sei $A \in Pot(\Omega)$ eine Menge mit 5 Elementen.*
Dann gibt es genau ein 8-el. Codewort von $\mathcal{G}$, das A enthält. Die Menge aller Codewörter mit Gewicht 8 ist also ein (5,8,24)-Steinersystem (auch Witt-Design genannt).

4 Eigenschaften der Automorphismengruppe des Golaycodes

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

Definition 4.1 $\mathfrak{N} := Stab_{Aut(\mathcal{G})}(\Xi_u)$ *operiert auf Ξ_u durch Anwenden. $\pi_0 : \mathfrak{N} \to Sym\Xi_u$ sei die zugehörige Permutationsdarstellung und L der Kern.*

Satz 4.2

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

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

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

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

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

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

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

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

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

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

Folgerung 4.3

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

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

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

Satz 4.4 ***(Stabilisator eines ungeordneten Sextetts)***

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

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

Folgerung 4.5 $|\mathfrak{N}| = |\mathcal{H}| \cdot |Aut^*(\mathcal{H})| = 4^3 \cdot 2^4 \cdot 3^3 \cdot 5 = 2^{10} \cdot 3^3 \cdot 5$

Lemma 4.6 *Sei* (P, φ) *ein Paar aus geordneter Partition mit sechs 4-el. Mengen und skalarem Label.*

Dann gibt es genau ein $\sigma \in Sym(\Omega)$ *mit* $\sigma(P, \varphi) = (\Xi, l)$. *Außerdem ist dann* $\sigma(\mathcal{G}(P, \varphi)) = \mathcal{G}(\Xi, l) = \mathcal{G}$.

Satz 4.7 ***(Erzeugen einer Labelabbildung)***
Sein $\mathcal{C}$ *ein Golaycode und* $P = \{X_1, ..., X_6\}$ *ein geordnetes Sextett (bzgl.* $\mathcal{C}$*).*

Dann gibt es genau 192 skalare Labelabbildungen φ*, sodass* $\mathcal{G}(P, \varphi) = \mathcal{C}$ *ist.*

Satz 4.8 *Der Golaycode* $\mathcal{G}$ *ist bis auf lineare Äquivalenz eindeutig.*

Satz 4.9

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

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

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

Satz 4.10 ***(Einfachheit von*** M_{24}***)*** *Die fünfte Mathieugruppe ist definiert als* $M_{24} := Aut(\mathcal{G})$.

Dann ist M_{24} *eine einfache Gruppe.*

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