RWTH AACHEN UNIVERSITY

Selbstduale Codes und Invariantentheorie

Gabriele Nebe, RWTH Aachen

Heidelberg, 5.6.2008.

Code $C \subseteq A^N$, **Alphabet** A, **Länge** N.
Für $c = (c_1, \ldots, c_N), c' = (c'_1, \ldots, c'_N)$ ist der **Hammingabstand**

$$d(c, c') = |\{1 \leq i \leq N \mid c_i \neq c'_i\}|$$

Ist $d(c, c') \geq 3$ für alle $c \neq c' \in C$, so kann C einen Fehler korrigieren, allgemeiner kann C mindestens e Fehler korrigieren, falls $d(c, c') \geq 2e + 1$ für alle $c \neq c' \in C$.

Das **Codepolynom** p_C des Codes $C \subseteq A^N$ ist

$$p_C := \sum_{c \in C} \prod_{i=1}^{N} x_{c_i} \in \mathbb{C}[x_a \mid a \in A]_N$$

ein komplexes homogenes Polynom vom Grad N in $|A|$ Variablen.

Ziel ist es, Eigenschaften des Codes C in Invarianzeigenschaften seines Codepolynoms zu übersetzen. Dabei beschränken wir uns auf **endliche lineare Codes**, das Alphabet A ist ein endlicher Linksmodul für einen Ring R und $C \leq A^N$ ist ein R-Teilmodul.
Dann ist nämlich der **Minimalabstand**

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

gleich dem **Minimalgewicht**

$$w(C) := \min\{w(c) := d(c, 0) \mid c \neq 0 \in C\},$$

da $d(c, c') = w(c - c')$.
Das Minimalgewicht lässt sich am **Hamminggewichtszähler**

$$\mathrm{hwe}_C(x, y) = p_C(x, y, \ldots, y) = \sum_{c \in C} x^{N-w(c)} y^{w(c)} \in \mathbb{C}[x, y]_N$$

ablesen.

Beispiel: Der Tetracode.

$$t_4 := \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 1 \end{bmatrix} \leq \mathbb{F}_3^4$$

$$p_{t_4}(x_0, x_1, x_2) = x_0^4 + x_0 x_1^3 + x_0 x_2^3 + 3x_0 x_1^2 x_2 + 3x_0 x_1 x_2^2.$$

$$\mathsf{hwe}_{t_4}(x, y) = p_{t_4}(x, y, y) = x^4 + 8xy^3.$$

Sei $\beta : A \times A \to \mathbb{Q}/\mathbb{Z}$ **regulär** ($a \mapsto (x \mapsto \beta(a,x))$ ist ein Isomorphismus $A \to \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})$). Der **duale Code** ist

$$C^{\perp} := \{v \in A^N \mid \sum_{i=1}^{N} \beta(c_i, v_i) = 0 \text{ für alle } c \in C\}.$$

C heißt **selbstdual**, falls $C = C^{\perp}$.

MacWilliams Identität (1962).
Sei $|A| = q$. Dann ist

$$\mathrm{hwe}_{C^{\perp}}(x,y) = \frac{1}{|C|}\,\mathrm{hwe}_C(x + (q-1)y, x - y).$$

Ist C also selbstdual, so ist hwe_C invariant unter der

MacWilliams Transformation

$$h_q : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \frac{1}{\sqrt{q}} \begin{pmatrix} 1 & q-1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

Satz von Gleason und Pierce (1967):
Sei $C = C^{\perp} \leq \mathbb{F}_q^N$ so dass $w(c) \in m\mathbb{Z}$ für alle $c \in C$ und ein $m > 1$.
Dann ist C einer der folgenden Typen von Codes:

I) $q = 2$ und $m = 2$ (alle selbstdualen binären Codes).
II) $q = 2$ und $m = 4$ (doppeltgerade binäre Codes).
III) $q = 3$ und $m = 3$ (alle selbstdualen ternären Codes).
IV) $q = 4$ und $m = 2$ (alle Hermitesch selbstdualen Codes).

o) $q = 4$ und $m = 2$ (gewisse Euklidisch selbstduale Codes).

d) q beliebig $m = 2$ und $C = \perp^{N/2} [1, a]$.

Die selbstdualen Codes in I) bis IV) dieses Satzes heißen Typ I, II, III und IV Codes.
Für Codes vom Typ I, II und IV ist der Hamminggewichtszähler also ein Polynom in x^2 und y^2, (bei Typ II sogar in x^4 und y^4), für Typ III Codes ein Polynom in x und y^3.

Der Satz von Gleason (ICM, Nizza, 1970)
Der Hamminggewichtszähler eines selbstdualen Codes vom Typ I,II,III oder IV läßt sich eindeutig als Polynom in f und g darstellen, wobei

Typ	f	g
I	x^2+y^2	$x^2y^2(x^2-y^2)^2$
II	$x^8+14x^4y^4+y^8$	$x^4y^4(x^4-y^4)^4$
III	x^4+8xy^3	$y^3(x^3-y^3)^3$
IV	x^2+3y^2	$y^2(x^2-y^2)^2$

Beweis des Satzes von Gleason.
Sei $C \leq \mathbb{F}_q^N$ ein Code vom Typ T = I,II,III oder IV. Dann ist $C = C^\perp$ also hwe_C invariant unter der MacWilliams Transformation h_q.
Nach Gleason-Pierce, ist hwe_C auch invariant unter

$$d_m := \mathrm{diag}(1, \zeta_m) : x \mapsto x, y \mapsto \zeta_m y$$

(wo $\zeta_m = \exp(2\pi i/m)$ primitive m-te Einheitswurzel). Also liegt

$$\mathrm{hwe}_C \in \mathrm{Inv}(\langle h_q, d_m \rangle =: G_T)$$

im Invariantenring der endlichen komplexen Matrixgruppe G_T. In allen vier Fällen ist G_T eine komplexe Spiegelungsgruppe der Ordnung $2 \cdot 8, 8 \cdot 24, 4 \cdot 12, 2 \cdot 6$ und der Invariantenring von G_T ist der Polynomring $\mathbb{C}[f, g]$.

Folgerung: Die Länge eines Codes vom Typ II ist durch 8 teilbar und die eines Typ III Codes ist durch 4 teilbar.
Beweis: $\zeta_8 I_2 \in G_{\mathrm{II}}$, $\zeta_4 I_2 \in G_{\mathrm{III}}$.

Aus dem Satz von Gleason erhält man eine obere Schranke an das Minimalgewicht eines selbstdualen Codes der Länge N. Codes die diese Schranke erreichen heißen **extremal**.

Satz. $d(C) \leq m + m\lfloor \frac{N}{\deg(g)} \rfloor$.

Typ I) $d(C) \leq 2 + 2\lfloor \frac{N}{8} \rfloor$. Typ II) $d(C) \leq 4 + 4\lfloor \frac{N}{24} \rfloor$.
Typ III) $d(C) \leq 3 + 3\lfloor \frac{N}{12} \rfloor$. Typ IV) $d(C) \leq 2 + 2\lfloor \frac{N}{6} \rfloor$.

Bemerkung.
Für Typ I Codes gibt es eine bessere obere Schranke

$$d(C) \leq 4 + 4\lfloor \frac{N}{24} \rfloor + a$$

wo $a = 2$ für $N \pmod{24} = 22$ und 0 sonst.

Beweis. (für Typ I Codes)
Sei $C = C^{\perp} \leq \mathbb{F}_2^{2d}$. Dann ist hwe_C eine Linearkombination von

$$\begin{array}{lccccccc}
f^d = & x^{2d} & +dx^{2d-2}y^2 & & +* & +\ldots & & +\ldots \quad +\ldots \\
f^{d-4}g = & 0 & +x^{2d-2}y^2 & & +* & +\ldots & & +\ldots \quad +\ldots \\
f^{d-8}g^2 = & 0 & & +0 & +x^{2d-4}y^4 & +\ldots & & +\ldots \quad +\ldots \\
\vdots & \vdots & & \vdots & \vdots & & & \\
f^{d-4b}g^b = & 0 & & +0 & +0 & +\ldots & +x^{2d-2b}y^{2b} & +\ldots
\end{array}$$

wobei $b := \lfloor \frac{d}{4} \rfloor = \dim(\mathbb{C}[f,g]_{2d}) - 1$.
Dieser Raum enthält ein eindeutiges Polynom von der Form

$$p_{ext} = x^{2d} + a_{b+1}x^{2d-2-2b}y^{2b+2} + a_{b+2}x^{2d-4-2b}y^{2b+4} + \ldots$$

Man kann zeigen, dass a_{b+1} immer positiv ist, und daher

$$d(C) \leq 2 + 2b = 2 + 2\lfloor \frac{N}{8} \rfloor$$

.

Zurück zur allgemeinen Situation:
A ein endlicher R-Linksmodul, $q := |A|$,
$\beta : A \times A \to \mathbb{Q}/\mathbb{Z}$ regulär, $C \leq A^N$ Code,

dualer Code $C^\perp := \{v \in A^N \mid \sum_{i=1}^{N} \beta(c_i, v_i) = 0 \text{ für alle } c \in C\}$.

Codepolynom $p_C := \sum_{c \in C} \prod_{i=1}^{N} x_{c_i} \in \mathbb{C}[x_a \mid a \in A]_N$

MacWilliams Identität:
Ist $C = C^\perp$, so ist p_C invariant unter der Variablensubstitution

$$h_\beta : x_a \mapsto \frac{1}{\sqrt{q}} \sum_{b \in A} \exp(2\pi i \beta(b, a)) x_b.$$

Ist $C \leq A^N$ ein linearer Code, so ist $C = uC$ für alle $u \in R^*$ (Einheiten von R) und daher p_C invariant unter der Permutation

$$m_u : x_a \mapsto x_{ua}.$$

Ist $C \subseteq C^\perp$ ein **selbstorthogonaler** Code, so ist für alle $c = (c_1, \ldots, c_N) \in C$ und alle $r \in R$

$$\sum_{i=1}^{N} \beta(c_i, rc_i) = 0$$

also $\prod_{i=1}^{N} x_{c_i}$ (und somit auch p_C) invariant unter der diagonalen Variablentransformation

$$d_r : x_a \mapsto \exp(2\pi i \beta(a, ra)) x_a.$$

Die Gruppe

$\mathcal{C}(\beta) = \langle m_u, d_r, h_{\beta,e} \mid r \in R, u \in R^*, e \in R \text{ sym. Idempot. } \rangle \leq \mathsf{GL}_q(\mathbb{C})$

heißt die **zugehörige Clifford-Weil Gruppe**.

Satz.
Ist $C = C^{\perp}$ ein selbstdualer Code, so ist $p_C \in \mathrm{Inv}(\mathcal{C}(\beta))$ im Invariantenring der zugehörigen Clifford-Weil Gruppe.

Hauptsatz. (N., Rains, Sloane (1999-2006))
Ist R direktes Produkt von Matrixringen über Kettenringen, so ist

$$\mathrm{Inv}(\mathcal{C}(\beta)) = \langle p_C \mid C = C^{\perp} \rangle.$$

Ein solcher Satz gilt i.a. nicht für Hamminggewichtszähler.

Die Clifford-Weil Gruppe der Typ III Codes.

$$R = \mathbb{F}_3 = A,\ \beta(x,y) = \frac{1}{3}xy$$

$$\mathcal{C}(\mathrm{III}) = \langle m_2 = \begin{pmatrix} 100 \\ 001 \\ 010 \end{pmatrix}, d_1 = \mathrm{diag}(1,\zeta_3,\zeta_3), h_\beta = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \zeta_3 & \zeta_3^2 \\ 1 & \zeta_3^2 & \zeta_3 \end{pmatrix} \rangle$$

Die Clifford-Weil Gruppe der Typ IV Codes.

$$R = \mathbb{F}_4 = A,\ \beta(x,y) = \frac{1}{2}\,\mathrm{trace}(x\overline{y})$$

wo $\overline{x} = x^2$, $\mathbb{F}_4 = \mathbb{F}_2[\omega]$, $\omega^2 + \omega + 1 = 0$.

$$\mathcal{C}(\mathrm{IV}) = \langle m_\omega = \begin{pmatrix} 1000 \\ 0001 \\ 0100 \\ 0010 \end{pmatrix}, d_\omega = \mathrm{diag}(1,\text{-}1,\text{-}1,\text{-}1), h_\beta = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & \text{-}1 & \text{-}1 \\ 1 & \text{-}1 & 1 & \text{-}1 \\ 1 & \text{-}1 & \text{-}1 & 1 \end{pmatrix} \rangle$$

Symmetrisierungen.

Die Adjungtion bzgl. der regulären Form β liefert eine Involution $r \mapsto r^J$ auf R, wobei $\beta(x, ry) = \beta(r^J x, y)$ für alle $x, y \in A$.

Die **zentrale unitäre Gruppe** ist

$$\mathsf{ZU}(R, J) := \{g \in Z(R) \mid gg^J = g^J g = 1\}.$$

Satz. $m(\mathsf{ZU}) := \{m_u \mid u \in \mathsf{ZU}(R, J)\}$ liegt im Zentrum von $\mathcal{C}(\beta)$.

Seien $B_0, \ldots, B_n$ die $\mathsf{ZU}(R, J)$-Bahnen auf A.
Die **symmetrisierte Clifford-Weil Gruppe** ist

$$\mathcal{C}^s(\beta) = \{g^s \mid g \in \mathcal{C}(\beta)\} \leq \mathsf{GL}_{n+1}(\mathbb{C})$$

Ist

$$g(\frac{1}{|B_i|} \sum_{v \in B_i} x_v) = \sum_{j=0}^{n} a_{ij} (\frac{1}{|B_j|} \sum_{w \in B_j} x_w)$$

so ist

$$g^s(b_i) = \sum_{j=0}^{n} a_{ij} b_j.$$

Bemerkung. Der Invariantenring der symmetrisierten Gruppe besteht genau aus den symmetrisierten Invarianten der Gruppe. Ist letzter von Codepolynomen erzeugt, so ist erster durch die **symmetrisierten Codepolynome** p_C^s erzeugt.

symmetrisiertes Codepolynom

$$p_C^s = \sum_{c \in C} \prod_{j=0}^{n} x_j^{a_j(c)} \in \mathbb{C}[x_0, \ldots, x_n]$$

wobei für $c = (c_1, \ldots, c_N) \in C$ und $0 \leq j \leq n$

$$a_j(c) = |\{1 \leq i \leq N \mid c_i \in B_j\}|.$$

Neue Interpretation von Gleason's Satz.

Für die Codes von Typ I,II,III,IV ist die zentrale unitäre Gruppe transitiv auf $A - \{0\}$, es gibt also genau 2 Bahnen:

$$x \leftrightarrow \{0\},\ y \leftrightarrow A - \{0\}$$

und die symmetrisierten Codepolynome sind genau die Hamminggewichtszähler.

$$\mathcal{C}(\mathrm{III}) = \langle m_2 = \begin{pmatrix} 100 \\ 001 \\ 010 \end{pmatrix}, d_1 = \mathrm{diag}(1, \zeta_3, \zeta_3), h_\beta = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \zeta_3 & \zeta_3^2 \\ 1 & \zeta_3^2 & \zeta_3 \end{pmatrix} \rangle$$

liefert die symmetrisierte Gruppe

$$G(\mathrm{III}) = \langle m_2^s = I_2, d_1^s = \mathrm{diag}(1, \zeta_3), h_\beta^s = h_3 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 2 \\ 1 & -1 \end{pmatrix} \rangle$$

Ebenso für die Typ IV Codes:

$$\mathcal{C}(\text{IV}) = \langle m_\omega = \begin{pmatrix} 1000 \\ 0001 \\ 0100 \\ 0010 \end{pmatrix}, d_\omega = \text{diag}(1, \text{-}1, \text{-}1, \text{-}1), h_\beta = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1\text{-}1\text{-}1 \\ 1\text{-}1 & 1\text{-}1 \\ 1\text{-}1\text{-}1 & 1 \end{pmatrix} \rangle$$

liefert als Symmetrisierung

$$G(\text{IV}) = \langle m_\omega^s = I_2, d_\omega^s = \text{diag}(1, -1), h_\beta^s = h_4 = \frac{1}{2} \begin{pmatrix} 1 & 3 \\ 1 & -1 \end{pmatrix} \rangle$$

Hermitesch selbstduale Codes über $\mathbb{F}_9$:

$R = A = \mathbb{F}_9, \beta(x,y) = \frac{1}{3}\mathrm{trace}(x\overline{y})$, $\overline{y} = y^3$.

Sei $\langle\alpha\rangle = \mathbb{F}_9^*$ und $\zeta := \zeta_3 = \exp(\frac{2\pi i}{3}) \in \mathbb{C}$. Wir schreiben die Matrizen bezüglich der $\mathbb{C}$-Basis

$$(0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7)$$

von $\mathbb{C}[A] \cong \mathbb{C}^9$.

$d_1 := \mathrm{diag}(1, \zeta^2, \zeta, \zeta^2, \zeta, \zeta^2, \zeta, \zeta^2, \zeta)$,

$$m_\alpha := \begin{pmatrix} 100000000 \\ 000000001 \\ 010000000 \\ 001000000 \\ 000100000 \\ 000010000 \\ 000001000 \\ 000000100 \\ 000000010 \end{pmatrix}, \quad h := \frac{1}{3}\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \zeta^2 & \zeta & 1 & \zeta & \zeta & \zeta^2 & 1 & \zeta^2 \\ 1 & \zeta & \zeta & \zeta^2 & 1 & \zeta^2 & \zeta^2 & \zeta & 1 \\ 1 & 1 & \zeta^2 & \zeta^2 & \zeta & 1 & \zeta & \zeta & \zeta^2 \\ 1 & \zeta & 1 & \zeta & \zeta & \zeta^2 & 1 & \zeta^2 & \zeta^2 \\ 1 & \zeta & \zeta^2 & 1 & \zeta^2 & \zeta^2 & \zeta & 1 & \zeta \\ 1 & \zeta^2 & \zeta^2 & \zeta & 1 & \zeta & \zeta & \zeta^2 & 1 \\ 1 & 1 & \zeta & \zeta & \zeta^2 & 1 & \zeta^2 & \zeta^2 & \zeta \\ 1 & \zeta^2 & 1 & \zeta^2 & \zeta^2 & \zeta & 1 & \zeta & \zeta \end{pmatrix}$$

Die zugehörige Clifford-Weil Gruppe hat Ordnung 192 und Molienreihe

$$\frac{\theta(t)}{(1-t^2)^2(1-t^4)^2(1-t^6)^3(1-t^8)(1-t^{12})}$$

wobei

$$\begin{aligned}\theta(t) := \; & 1 + 3t^4 + 24t^6 + 74t^8 + 156t^{10} + 321t^{12} + 525t^{14} + 705t^{16} \\ & + 905t^{18} + 989t^{20} + 931t^{22} + 837t^{24} + 640t^{26} + 406t^{28} \\ & + 243t^{30} + 111t^{32} + 31t^{34} + 9t^{36} + t^{38}\,.\end{aligned}$$

Der Invariantenring hat also in etwa

$$\theta(1) + 9 = 6912 + 9 = 6921$$

Erzeuger.

Wie kommen wir jetzt an die Hamminggewichtszähler ?

Die zentrale unitäre Gruppe

$$\mathsf{ZU}(R,J) = \{x \in \mathbb{F}_9^* \mid x\overline{x} = x^4 = 1\} = (\mathbb{F}_9^*)^2$$

hat 3 Bahnen auf $A = \mathbb{F}_9$:

$$\{0\} = X_0,\ \{1,\alpha^2,\alpha^4,\alpha^6\} =: X_1,\ \{\alpha,\alpha^3,\alpha^5,\alpha^7\} =: X_2$$

$$\mathcal{C}^s = \langle d_1^s := \mathsf{diag}(1,\zeta^2,\zeta),\ m_\alpha^s := \begin{pmatrix}100\\001\\010\end{pmatrix},\ h^s := \frac{1}{3}\begin{pmatrix}1 & 4 & 4\\ 1 & 1\text{-}2\\ 1\text{-}2 & 1\end{pmatrix}\rangle$$

hat Ordnung $\frac{192}{4} = 48$. Der Invariantenring der symmetrisierten Clifford-Weil Gruppe ist ein Polynomring in den symmetrisierten Codepolynomen

$$q_2 = x_0^2 + 8x_1x_2, \quad q_4 = x_0^4 + 16(x_0x_1^3 + x_0x_2^3 + 3x_1^2x_2^2)$$

$$q_6 = x_0^6 + 8(x_0^3x_1^3 + x_0^3x_2^3 + 2x_1^6 + 2x_2^6)$$
$$+72(x_0^2x_1^2x_2^2 + 2x_0x_1^4x_2 + 2x_0x_1x_2^4) + 320x_1^3x_2^3$$

der 3 Codes mit Erzeugermatrizen

$$\begin{bmatrix} 1 & \alpha \end{bmatrix},\ \begin{bmatrix} 1 & 1 & 1 & 0\\ 0 & 1 & 2 & 1 \end{bmatrix},\ \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1\\ 1 & 1 & 1 & 0 & 0 & 0\\ 0 & \alpha & 2\alpha & 0 & 1 & 2 \end{bmatrix}.$$

Die zugehörigen Hamminggewichtszähler sind

$$\begin{aligned} r_2 = q_2(x,y,y) &:= x^2 + 8y^2\,, \\ r_4 = q_4(x,y,y) &:= x^4 + 32xy^3 + 48y^4\,, \\ r_6 = q_6(x,y,y) &:= x^6 + 16x^3y^3 + 72x^2y^4 + 288xy^5 + 352y^6 \end{aligned}$$

und erzeugen den Ring $\mathrm{Ham}(9^H)$ erzeugt durch die Hamminggewichtszähler der Hermitesch selbstdualen Codes über $\mathbb{F}_9$.
$\mathrm{Ham}(9^H) = \mathbb{C}[r_2, r_4] \oplus r_6\mathbb{C}[r_2, r_4]$ mit der Relation

$$r_6^2 = \frac{3}{4}r_2^4 r_4 - \frac{3}{2}r_2^2 r_4^2 - \frac{1}{4}r_4^3 - r_2^3 r_6 + 3r_2 r_4 r_6\,.$$

Folgerung: $C = C^\perp \leq \mathbb{F}_9^N \Rightarrow d(C) \leq 1 + N/2$.

Der Ring $\mathrm{Ham}(9^H)$ ist kein Invariantenring einer endlichen Gruppe.
$G := \langle -I_2, h_9 \rangle$ hat Ordnung 4,

$$\mathrm{Ham}(9^H) \subset \mathrm{Inv}(G) = \mathbb{C}[x^2 + 8y^2, xy - y^2]$$

Höhere Codepolynome.

Seien $c^{(i)} := (c_1^{(i)}, \ldots, c_N^{(i)}) \in A^N$, $i = 1, \ldots, m$ nicht notwendig verschiedene Codeworte. Für jede Spalte $a := (a_1, \ldots, a_m)^{tr} \in A^m$ setzen wir

$$z_a(c^{(1)}, \ldots, c^{(m)}) := |\{j \in \{1, \ldots, N\} \mid c_j^{(i)} = a_i \text{ für alle } i \in \{1, \ldots, m\}\}| \,.$$

Das **Geschlecht-m Codepolynom** von C ist

$$p_m(C) := \sum_{(c^{(1)}, \ldots, c^{(m)}) \in C^m} \prod_{a \in A^m} x_a^{z_a(c^{(1)}, \ldots, c^{(m)})} \in \mathbb{C}[x_a : a \in A^m] \,.$$

$$\begin{array}{cccccc} c_1^{(1)} & c_2^{(1)} & \ldots & c_j^{(1)} & \ldots & c_N^{(1)} \\ c_1^{(2)} & c_2^{(2)} & \ldots & c_j^{(2)} & \ldots & c_N^{(2)} \\ \vdots & \vdots & \ldots & \vdots & \ldots & \vdots \\ c_1^{(m)} & c_2^{(m)} & \ldots & c_j^{(m)} & \ldots & c_N^{(m)} \\ & & & \uparrow & & \\ & & & a \in A^m & & \end{array}$$

Beispiele.

$C = i_2 = \{(0,0),(1,1)\} \leq \mathbb{F}_2^2$ hat $p_2(C) = x_{00}^2 + x_{11}^2 + x_{01}^2 + x_{10}^2$.

$$C = e_8 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix} \leq \mathbb{F}_2^8.$$

Codepolynom $p_{e_8}(x,y) = \mathsf{hwe}_{e_8}(x,y) = x^8 + 14x^4y^4 + y^8$.

$$\begin{aligned} p_2(e_8) \; &= x_{00}^8 + x_{01}^8 + x_{10}^8 + x_{11}^8 + 168x_{00}^2x_{01}^2x_{10}^2x_{11}^2 + \\ &\quad 14(x_{00}^4x_{01}^4 + x_{00}^4x_{10}^4 + x_{00}^4x_{11}^4 + x_{01}^4x_{10}^4 + x_{01}^4x_{11}^4 + x_{10}^4x_{11}^4) \end{aligned}$$

Für jeden Code $C \leq A^N$ und $m \in \mathbb{N}$ sei

$$C(m) := R^{m\times 1} \otimes C = \{(c^{(1)}, \ldots, c^{(m)})^{tr} \mid c^{(1)}, \ldots, c^{(m)} \in C\} \leq (A^m)^N.$$

Dann ist das Geschlecht m Codepolynom von C genau das gewöhnliche Codepolynom von $C(m)$,

$$p_m(C) = p_{C(m)}.$$

Ist C ein R-linearer selbstdualer Code, so ist $C(m) \leq (A^m)^N$ ein selbstdualer Code für den Matrixring $R^{m\times m}$. Also ist

$$p_m(C) \text{ invariant unter } \mathcal{C}_m(\beta)$$

der **zugehörigen Geschlecht-m Clifford-Weil Gruppe.**

Beispiel: $\mathcal{C}_2(\mathrm{I})$**.**

$$R = \mathbb{F}_2^{2\times 2}, R^* = \mathsf{GL}_2(\mathbb{F}_2) = \langle a := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ b := \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \rangle$$

$A = \mathbb{F}_2^2 = \{\begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}\}$, symmetrisches Idempotent $e = \mathsf{diag}(1, 0)$

$$\mathcal{C}_2(\mathrm{I}) \ = \langle m_a = \begin{pmatrix} 1000 \\ 0010 \\ 0100 \\ 0001 \end{pmatrix},\ m_b = \begin{pmatrix} 1000 \\ 0001 \\ 0100 \\ 0010 \end{pmatrix},$$

$$h_e = \frac{1}{\sqrt{2}} \begin{pmatrix} 1\ 1\ 0\ 0 \\ 1\text{-}1\ 0\ 0 \\ 0\ 0\ 1\ 1 \\ 0\ 0\ 1\text{-}1 \end{pmatrix},\ d_e = \mathsf{diag}(1, -1, 1, -1)\rangle$$

$\mathcal{C}_2(\mathrm{I})$ hat Ordnung 2304 und Molienreihe

$$\frac{1+t^{18}}{(1-t^2)(1-t^8)(1-t^{12})(1-t^{24})}$$

wobei Erzeuger als die Geschlecht 2 Codepolynome von

$$i_2, e_8, d_{12}^+, g_{24}, \text{ und } (d_{10}e_7f_1)^+$$

gewählt werden können.

$$\mathrm{Inv}(\mathcal{C}_2(\mathrm{I})) = \mathbb{C}[i_2, e_8, d_{12}^+, g_{24}] \oplus (d_{10}e_7f_1)^+\mathbb{C}[i_2, e_8, d_{12}^+, g_{24}]$$

Höhere Clifford-Weil Gruppen für Typ I, II, III, IV.

$$\mathcal{C}_m(\mathrm{I}) = 2_+^{1+2m}.O_{2m}^+(\mathbb{F}_2)$$

$$\mathcal{C}_m(\mathrm{II}) = Z_8 Y 2^{1+2m}.\mathsf{Sp}_{2m}(\mathbb{F}_2)$$

$$\mathcal{C}_m(\mathrm{III}) = Z_4.\mathsf{Sp}_{2m}(\mathbb{F}_3)$$

$$\mathcal{C}_m(\mathrm{IV}) = Z_2.U_{2m}(\mathbb{F}_4)$$

Zusammenfassung.

- Gleason (1970) Hamminggewichtszähler für Typ I,II,III,IV Codes erzeugen Invariantenring einer Gruppe.
- Seitdem wurden Sätze à la Gleason für viele Typen von Codes einzeln bewiesen.
- E. Rains, N. Sloane, N. (1999-2006):

Self-dual codes and invariant theory. (Springer 2006)

- Abstrakte Definition eines Typs eines Codes und der zugehörigen Clifford-Weil Gruppe $\mathcal{C}$.
- Geschlecht m Codepolynome sind invariant unter $\mathcal{C}_m$.
- Für eine große Klasse von Ringen erzeugen sie Inv($\mathcal{C}_m$).
- Durch Symmetrisierung zu den Hamminggewichtszählern.

Hecke Operatoren für Codes.

Motivation.
Bestimme lineare Relationen zwichen den $p_m(C)$ mit
$C \in M_N(T) = \{C \leq A^N \mid C \text{ Typ } T \text{ Code }\}$.

$M_{16}(\text{II}) = [e_8 \perp e_8] \cup [d_{16}^+]$ und diese beiden Codes haben die gleichen Geschlecht 1 und 2 Codepolynome. $p_3(e_8 \perp e_8)$ und $p_3(d_{16}^+)$ sind linear unabhängig.

$h(M_{24}(\text{II})) = 9$, die Geschlecht 6 Codepolynome sind linear unabhängig und es gibt eine Relation für die vom Geschlecht 5.

$h(M_{32}(\text{II})) = 85$ die Geschlecht 10 Codepolynome sind linear unabhängig und es gibt eine Relation für die vom Geschlecht 9.

Drei verschiedene Ansätze:

1) Bestimme alle Codes bis auf Permutationsäquivalenz sowie deren Codepolynome.
Ist $\dim(C) = n = N/2$, so gibt es $\prod_{i=0}^{d-1}(2^n - 2^i)/(2^d - 2^i)$ Teilräume der Dimension d in C.
$N = 32, d = 10$ liefert mehr als 10^{18} Teilräume.

2) Benutze den Satz von Molien:
$\mathrm{Inv}_N(\mathcal{C}_m(\mathrm{II})) = \langle p_m(C) \mid C \in M_N(\mathrm{II}) \rangle$
und die erzeugende Funktion für $a_N := \dim(\mathrm{Inv}_N(\mathcal{C}_m(\mathrm{II})))$ ist

$$\sum_{N=0}^{\infty} a_N t^N = \frac{1}{|\mathcal{C}_m(\mathrm{II})|} \sum_{g \in \mathcal{C}_m(\mathrm{II})} (\det(1 - tg))^{-1}$$

Problem: $\mathcal{C}_{10}(\mathrm{II}) \leq \mathrm{GL}_{1024}(\mathbb{C})$ hat Ordnung $> 10^{69}$.

3) Benutze Hecke Operatoren.

Sei T ein Typ selbstdualer Codes über einem **Körper** $\mathbb{F}_q$.

$$M_N(T) = \{C \leq \mathbb{F}_q^N \mid C \text{ von Typ } T\} = [C_1] \dot\cup \ldots \dot\cup [C_h]$$

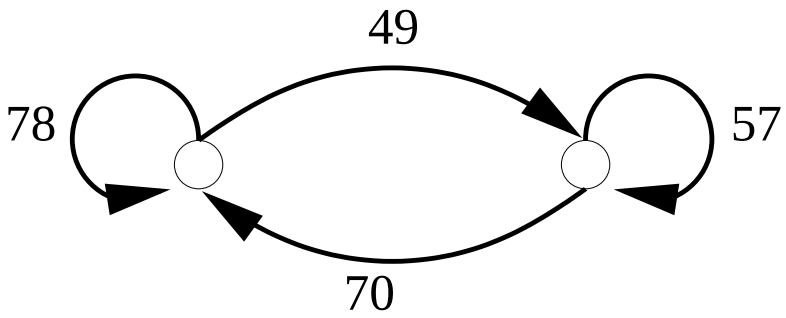
wobei $[C]$ die **Permutationsäquivalenzklasse** von C bezeichnet.
Dann ist $n := \frac{N}{2} = \dim(C)$ für alle $C \in M_N(T)$.
$C, D \in M_N(T)$ heißen **benachbart**, falls $\dim(C) - \dim(C \cap D) = 1$.
In Zeichen: $C \sim D$.

$$\mathcal{V} = \mathbb{C}[C_1] \oplus \ldots \oplus \mathbb{C}[C_h] \cong \mathbb{C}^h$$

$$K_N(T) \in \mathrm{End}(\mathcal{V}),\ K_N(T) : [C] \mapsto \sum_{D \in M_N(T), D \sim C} [D].$$

Kneser-Hecke Operator.
(Adjazenzmatrix des Nachbarschaftsgraphen)

Beispiel. $M_{16}(\mathrm{II}) = [e_8 \perp e_8] \cup [d_{16}^+]$



$$K_{16}(\mathrm{II}) = \begin{pmatrix} 78 & 49 \\ 70 & 57 \end{pmatrix}$$

$\mathcal{V}$ trägt ein positiv definites Hermitesches Skalarprodukt

$$\langle [C_i], [C_j] \rangle := |\operatorname{Aut}(C_i)| \delta_{ij}.$$

Theorem. (N. 2006)
Der Kneser-Hecke Operator K ist selbstadjungiert.

$$\langle v, Kw \rangle = \langle Kv, w \rangle \text{ für alle } v, w \in \mathcal{V}.$$

Beispiel. $\frac{7}{10} = \frac{|\operatorname{Aut}(e_8 \perp e_8)|}{|\operatorname{Aut}(d_{16}^+)|}$ also

$$\operatorname{diag}(7, 10) K_{16}(\mathrm{II})^{\mathsf{Tr}} = K_{16}(\mathrm{II}) \operatorname{diag}(7, 10).$$

$$p_m : \mathcal{V} \to \mathbb{C}[X], \sum_{i=1}^{h} a_i[C_i] \mapsto \sum_{i=1}^{h} a_i p_m(C_i)$$

ist eine lineare Abbildung mit Kern

$$\mathcal{V}_m := \ker(p_m).$$

$$\mathcal{V} =: \mathcal{V}_{-1} \geq \mathcal{V}_0 \geq \mathcal{V}_1 \geq \ldots \geq \mathcal{V}_n = \{0\}.$$

ist eine Filtrierung von $\mathcal{V}$ mit zugehöriger orthogonaler Zerlegung

$$\mathcal{V} = \bigoplus_{m=0}^{n} \mathcal{Y}_m \text{ wo } \mathcal{Y}_m = \mathcal{V}_{m-1} \cap \mathcal{V}_m^{\perp}.$$

Beispiel.

$$\mathcal{V}_0 = \{\sum_{i=1}^{h} a_i[C_i] \mid \sum a_i = 0\}$$

und

$$\mathcal{V}_0^{\perp} = \mathcal{Y}_0 = \langle \sum_{i=1}^{h} \frac{1}{|\operatorname{Aut}(C_i)|}[C_i] \rangle.$$

Theorem. (N. 2006)
$\mathcal{Y}_m = \mathcal{Y}_m(N)$ ist der Eigenraum von $K_N(T)$ zum Eigenwert $\nu_N^{(m)}(T)$ mit $\nu_N^{(m)}(T) > \nu_N^{(m+1)}(T)$ für alle m.

Type	$\nu_N^{(m)}(T)$
q_{I}^E	$(q^{n-m} - q - q^m + 1)/(q-1)$
q_{II}^E	$(q^{n-m-1} - q^m)/(q-1)$
q^E	$(q^{n-m} - q^m)/(q-1)$
q_1^E	$(q^{n-m-1} - q^m)/(q-1)$
q^H	$(q^{n-m+1/2} - q^m - q^{1/2} + 1)/(q-1)$
q_1^H	$(q^{n-m-1/2} - q^m - q^{1/2} + 1)/(q-1)$

Folgerung. Der Nachbarschaftsgraph ist zusammenhängend.
Beweis: Der maximale Eigenwert der Adjazenzmatrix ist einfach (mit Eigenraum $\mathcal{Y}_0$).

Beispiel: $M_{16}(\mathrm{II}) = [e_8 \perp e_8] \cup [d_{16}^+]$
$(2^{8-m-1} - 2^m : m = 0, 1, 2, 3) = (127, 62, 28, 8)$

$$K_{16}(\mathrm{II}) = \begin{pmatrix} 78 & 49 \\ 70 & 57 \end{pmatrix}$$

hat Eigenwerte 127 und 8 mit Eigenvektoren $(7, 10)$ und $(1, -1)$.
Also ist

$$\mathcal{Y}_0 = \langle 7[e_8 \perp e_8] + 10[d_{16}^+] \rangle$$

$$\mathcal{Y}_1 = \mathcal{Y}_2 = 0$$

$$\mathcal{Y}_3 = \langle [e_8 \perp e_8] - [d_{16}^+] \rangle.$$

$M_{24}(\mathrm{II}) = [e_8^3] \cup [e_8 d_{16}] \cup [e_7^2 d_{10}] \cup [d_8^3] \cup [d_{24}] \cup [d_{12}^2] \cup [d_6^4] \cup [d_4^6] \cup [g_{24}]$

$K_{24}(\mathrm{II}) =$

$$\begin{pmatrix}
213 & 147 & 344 & 343 & 0 & 0 & 0 & 0 & 0 \\
70 & 192 & 896 & 490 & 7 & 392 & 0 & 0 & 0 \\
10 & 14 & 504 & 490 & 0 & 49 & 980 & 0 & 0 \\
1 & 3 & 192 & 447 & 0 & 36 & 1152 & 216 & 0 \\
0 & 990 & 0 & 0 & 133 & 924 & 0 & 0 & 0 \\
0 & 60 & 480 & 900 & 1 & 206 & 400 & 0 & 0 \\
0 & 0 & 72 & 216 & 0 & 3 & 1108 & 648 & 0 \\
0 & 0 & 0 & 45 & 0 & 0 & 720 & 1218 & 64 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1771 & 276
\end{pmatrix}$$

m	0	1	2	3	4	5	6
ν_m	2047	1022	508	248	112	32	-32
$\dim(\mathcal{Y}_m)$	1	1	1	2	2	1	1

$\langle 99[e_8^3] - 297[e_8 d_{16}] - 3465[d_8^3] + 7[d_{24}] + 924[d_{12}^2]$
$+4928[d_6^4] - 2772[d_4^6] + 576[g_{24}] \rangle = \ker(p_5) = \mathcal{V}_5$

Die Dimension von $\mathcal{Y}_m(N)$ für die doppelt-geraden selbstdualen binären Codes.

N, m	0	1	2	3	4	5	6	7	8	9	≥ 10
8	1										
16	1	0	0	1							
24	1	1	1	2	2	1	1				
32	1	1	2	5	10	15	21	18	8	3	1

Die Molien Reihe von $\mathcal{C}_m$(II) ergibt sich somit als

$$1 + t^8 + a(m)t^{16} + b(m)t^{24} + c(m)t^{32} + \ldots$$

wo

m	1	2	3	4	5	6	7	8	9	≥ 10
a	1	1	2	2	2	2	2	2	2	2
b	2	3	5	7	8	9	9	9	9	9
c	2	4	9	19	34	55	73	81	84	85

dim($\mathcal{Y}_m(N)$) für die binären selbstdualen Codes

N, m	0	1	2	3	4	5	6	7	8	9	10	11
2	1											
4	1											
6	1											
8	1	1										
10	1	1										
12	1	1	1									
14	1	1	1	1								
16	1	2	1	2	1							
18	1	2	2	2	2							
20	1	2	3	4	4	2						
22	1	2	3	6	7	4	2					
24	1	3	5	9	15	13	7	2				
26	1	3	6	12	23	29	20	8	1			
28	1	3	7	18	40	67	75	39	10	1		
30	1	3	8	23	65	142	228	189	61	10	1	
32	1	4	10	33	111	341	825	1176	651	127	15	1

Die Molien-Reihe von $\mathcal{C}_m(\mathrm{I})$ ist

$$1 + t^2 + t^4 + t^6 + 2t^8 + 2t^{10} + \sum_{N=12}^{\infty} a_N(m) t^N$$

wo

$$a_N(m) := \dim\langle\ \mathrm{cwe}_m(C) : C = C^{\perp} \leq \mathbb{F}_2^N \rangle$$

sich aus der folgenden Tabelle ergibt:

m, N	12	14	16	18	20	22	24	26	28	30	32
2	3	3	4	5	6	6	9	10	11	12	15
3	3	4	6	7	10	12	18	22	29	35	48
4	3	4	7	9	14	19	33	45	69	100	159
5	3	4	7	9	16	23	46	74	136	242	500
6	3	4	7	9	16	25	53	94	211	470	1325
7	3	4	7	9	16	25	55	102	250	659	2501
8	3	4	7	9	16	25	55	103	260	720	3152
9	3	4	7	9	16	25	55	103	261	730	3279
10	3	4	7	9	16	25	55	103	261	731	3294
≥ 11	3	4	7	9	16	25	55	103	261	731	3295