Kneser-Hecke-Operatoren in der Codierungstheorie

von

Elisabeth Nossek

An der Fakultät für Mathematik, Informatik und Naturwissenschaften
der Rheinisch-Westfälischen Technischen Hochschule Aachen
zur Erlangung des akademischen Grades einer
Diplom-Mathematikerin
vorgelegte

DIPLOMARBEIT

in Mathematik

Angefertigt am Lehrstuhl D für Mathematik
bei Professor G. Nebe

Inhaltsverzeichnis

Kapitel 1

Einleitung

Diese Diplomarbeit beschäftigt sich mit Kneser-Hecke-Operatoren in der Codierungstheorie, wie sie in [Neb06] eingeführt bzw. in Definition 2.3.1 definiert werden. Ursprünglich wurden solche Hecke-Operatoren in der Theorie der Modulformen betrachtet (s. z.B. [KK07] Kapitel 4). Eine mögliche Konstruktion dieser Hecke-Operatoren mit Hilfe von Gittern ist in [NV01] gegeben.

Die meisten gittertheoretischen Konstruktionen haben ihr Analogon in der Codierungstheorie. Theta-Reihen von Gittern sind Modulformen zu einer geeigneten Modulgruppe. Entsprechend sind Gewichtszähler (2.2.6) selbstdualer Codes invariant unter der sogenannten Clifford-Weil-Gruppe und erzeugen sogar den Invariantenring (siehe dazu [GRS06]), womit eine Beziehung zur Invariantentheorie besteht.

Das Konzept der Hecke-Operatoren und insbesondere ihre gittertheoretische Konstruktion wurde in [Neb06] auf die Codierungstheorie übertragen. Diese Kneser-Hecke-Operatoren sind Endomorphismen des $\mathbb{C}$-Vektorraums der formalen Linearkombinationen von Äquivalenzklassen gewisser selbstdualer Codes deren Konstruktion stark auf dem Kneserschen Nachbarschaftsverfahren beruht.

Bezeichnet $\mathcal{F} = [C_1] \dot{\cup} \ldots \dot{\cup} [C_h]$ die Menge aller selbstdualer Codes in $\mathbb{F}_q^N$ eines gewissen Typs wie in Definition 2.1.3, wobei $[C_j]$ die Permutationsäquivalenzklasse des Codes $C_j \in \mathcal{F}$ bezeichnet, so ist der zugehörige Kneser-Hecke-Operator $T \in \mathbb{C}^{h \times h}$ der Endomorphismus, der $[C_j]$ auf die Summe der Äquivalenzklassen aller Kneser-Nachbarn $\sum_{D \sim C_j} [D]$ abbildet (Definition 2.3.1). Hierbei heissen zwei Codes $C, D \in \mathcal{F}$ benachbart, falls $\dim(C/C \cap D) = 1$ ist. In [Neb06] werden die Eigenwerte sowie eine Eigenraumzerlegung von T für alle klassischen Typen selbstdualer Codes über Körpern berechnet.

Ziel dieser Diplomarbeit ist es, die höheren Hecke-Operatoren

$$T_k : [C_j] \mapsto \sum_{D \sim_k C_j} [D]$$

explizit als Polynome in T zu schreiben. Hierbei bedeutet $D \sim_k C$, dass $\dim(C/C \cap D) = k$ ist.

Es stellt sich heraus, dass alle diese Operatoren Polynome in T_1 sind, Formeln für die Koeffizienten sind 3.4.1 angegeben und Beispiele findet man in Kapitel 4.

Dazu betrachte ich die Adjazenzmatrizen $A_k \in \{0,1\}^{\mathcal{F}\times\mathcal{F}}$, der k-Nachbarschaftsrelation auf $\mathcal{F}$. Diese kann ich mit einfachen graphentheoretischen Methoden als Polynom in A_1 ausdrücken. Da man T_k aus A_k durch Symmetrisieren erhält (siehe 3.1.1 bzw. 3.1.2) sind dies auch die gesuchten Polynome für die Hecke-Operatoren T_k.

Für viele Familien $\mathcal{F}$ von Codes, insbesondere für Codes von klassischem Typ, gibt es eine endliche Gruppe G die transitiv auf $\mathcal{F}$ operiert, meist ist dies die orthogonale, unitäre oder symplektische Gruppe. Wie Prof. Hiss während meines Seminarvortrags bemerkte ergibt sich durch diese Betrachtungsweise eine schöne Interpretation der Ergebnisse im Kontext der Darstellungstheorie endlicher Gruppen mit BN-Paar:

Die Adjazenzmatrizen der Nachbarschaftsgraphen kann man als Elemente des $\mathbb{C}G$-Endomorphismenrings von $\mathbb{C}^{\mathcal{F}}$ auffassen, also dem $\mathbb{C}G$-Endomorphismenring des Permutationsmoduls $\mathbb{1}^G_{\mathrm{Stab}_G(C)}$ für einen Code C aus $\mathcal{F}$. Aus der Darstellungstheorie ist bekannt, dass $\mathrm{End}_{\mathbb{C}G}(\mathbb{1}^G_{\mathrm{Stab}_G(C)})$ isomorph zum $\mathbb{C}$-Algebrenerzeugnis der Doppelnebenklassen von G modulo $\mathrm{Stab}_G(C)$ ist.

Als Resultat erhält man dass $\mathrm{End}_{\mathbb{C}G}(\mathbb{C}^{\mathcal{F}})$ von den durch die Adjazenzmatrizen A_k induzierten Endomorphismen als $\mathbb{C}$-Vektorraum erzeugt wird. Genauer stimmen die Endomorphismen A_k mit den Operationen der kanonischen, aus der Theorie der BN-Paare (die in [Tay92] erläutert wird) gegebenen, Vertreter t_k der Doppelnebenklassen $\mathrm{Stab}_G(C)\backslash G/\mathrm{Stab}_G(C)$ überein. Abschließend kann man folgern, dass die $\mathbb{C}$-Algebra $\mathrm{End}_{\mathbb{C}G}(\mathbb{C}^{\mathcal{F}})$ bereits von A_1 erzeugt wird und somit kommutativ ist.

Kapitel 2

Grundlagen

2.1 Lineare Codes

Zuerst möchte ich einige grundlegende Definitionen und Sätze zu linearen Codes aus [Neb07] übernehmen.

2.1.1 Definition

1. *Ein linearer Code C über $\mathbb{F}_q$ der Länge N ist ein linearer Teilraum $C \leq \mathbb{F}_q^N$.*

2. *Auf $\mathbb{F}_q^n$ definieren wir eine symmetrische nicht ausgeartete Bilinearform oder hermitsche Form $b : \mathbb{F}_q^N \times \mathbb{F}_q^N \to \mathbb{F}_q$ $b(x,y) := \sum_{i=1}^N x_i\overline{y_i}$ wobei $^- : \mathbb{F}_q \to \mathbb{F}_q$ entweder die Identität (für die Bilinearform) oder ein nichttrivialer Automorphismus der Ordnung 2 (für die hermitsche Form) ist.*

3. *$C^\perp := \{x \in \mathbb{F}_q : b(x,y) = 0 \; \forall y \in C\}$ ist der duale Code zu C*

4. *C heißt selbstdual falls $C = C^\perp$ und selbstorthogonal falls $C \subset C^\perp$*

5. *$\mathrm{wt}(c) := |\{1 \leq i \leq N : c_i \neq 0\}|$ heißt Hamminggewicht von $c \in C$*

Der folgende Satz aus der linearen Algebra gilt allgemein für Teilräume von Vektorräume mit nichtausgearteter Bilinearform, also im besonderen auch für $C \leq \mathbb{F}_q^N$.

2.1.2 Satz

Sei (V, b) ein n-dimensionaler Vektorraum mit nichtausgearteter Bilinearform, U_1 und U_2 Untervektorräume von V, dann gilt:

1. $(U_1 \cap U_2)^\perp = U_1^\perp + U_2^\perp$

2. $(U_1 + U_2)^\perp = U_1^\perp \cap U_2^\perp$.

Beweis:
Wähle folgendermaßen eine Basis von V:
$B = (b_1, \ldots, b_m, b_{m+1}, \ldots, b_{n_1}, b_{n_1+1}, \ldots, b_{n_2+n_1-m}, \ldots, b_n)$ mit $m = \dim(U_1 \cap U_2)$, $n_1 = \dim(U_1)$ und $n_2 = \dim(U_2)$ so dass:

$$\begin{aligned} U_1 &= \langle b_1, \ldots, b_{n_1} \rangle \\ U_2 &= \langle b_1, \ldots, b_m, b_{n_1+1}, \ldots, b_{n_2+n_1-m} \rangle \\ U_1 \cap U_2 &= \langle b_1, \ldots, b_m \rangle \end{aligned}$$

Wähle nun die zu B duale Basis $B^* = (b_i^*)_{1 \le i \le n}$ mit $b(b_i, b_j^*) = \delta_{i,j}$. Dann ergibt sich:

$$\begin{aligned} U_1^\perp &= \langle b_{n_1+1}^*, \ldots, b_n^* \rangle \\ U_2^\perp &= \langle b_{m+1}^*, \ldots, b_{n_1}^*, b_{n_2+n_1-m+1}^*, \ldots, b_n^* \rangle \\ (U_1 \cap U_2)^\perp &= \langle b_{m+1}^*, \ldots, b_n^* \rangle \end{aligned}$$

woraus direkt die erste Behauptung folgt, und:

$$U_1^\perp \cap U_2^\perp = \langle b_{n_2+n_1-m+1}^*, \ldots, b_n^* \rangle = (U_1 + U_2)^\perp$$

also die zweite Behauptung.

q.e.d.

2.1.3 Definition
Eine Familie $\mathcal{F}$ selbstdualer Codes ist eine Menge selbstdualer Codes aus dem gleichen $\mathbb{F}_q$-Vektorraum, die vom gleichem Typ sind. Wobei der Typ eines Codes ein Menge von Eigenschaften ist wie z.B. die Charakteristik des Grundkörpers, ob eine hermitesche oder eine bilineare Form vorliegt und eventuell eine Zusatzeigenschaft wie doppeltgerade (also $4|\mathrm{wt}(c) \forall c \in C$) oder enthält das Wort $(1, \ldots, 1)$, (siehe auch 3.3).

Ich werde nun noch eine Operation der S_N auf $\mathbb{F}_q^N$ und einen dadurch induzierte Äquivalenzrelation auf den Codes einer Familie definieren.

2.1.4 Definition

1. *S_N operiert auf $\mathbb{F}_q^N$ durch vertauschen der Komponenten also*

$$\pi(f_1, \ldots, f_N) = (f_{\pi^{-1}(1)}, \ldots, f_{\pi^{-1}(N)}).$$

2. *Zwei Codes C, C' $\in \mathcal{F}$ heißen (permutations-)äquivalent wenn es eine Permutation $\pi \in S_N$ gibt, so dass $C' = \pi(C)$.*

3. *$[C]$ bezeichnet die Äquivalenzklasse des Codes C*

4. *Die Gruppe* $\mathrm{Aut}(C) := \{\pi \in S_N : \pi(C) = C\}$ *heißt Automorphismengruppe von C.*

2.1.5 Bemerkung
Unter dem Stabilisator eines Teilraums $W \leq C$ unter der Operation von $\mathrm{Aut}(C)$ *versteht man*

$$\mathrm{Stab}_{\mathrm{Aut}(C)}(W) := \{\pi \in \mathrm{Aut}(C) : \pi(w) \in W \forall w \in W\}$$

.

2.2 Der Vektorraum $\mathcal{V}$ und Gewichtszähler

Auf dem im folgenden definierten Vektorraum $\mathcal{V}$ wird der Kneser-Hecke-Operator operieren. Der vollständige Gewichtszähler steht in direktem Zusammenhang mit den Eigenräumen des Kneser-Hecke-Operators.

2.2.1 Definition
Sei $\mathcal{V} := \langle [C] : C \in \mathcal{F} \rangle_{\mathbb{C}}$ der $\mathbb{C}$-Vektorraum der formalen Linearkombinationen von Äquivalenzklassen von Codes einer festen Familie $\mathcal{F}$. Somit ist $\mathcal{B} := \{[C] : C \in \mathcal{F}\}$ eine Basis von $\mathcal{V}$.

$$([C], [D]) := |\mathrm{Aut}(C)|\delta_{[C],[D]}$$

definiert ein hermitesches, positiv definites Skalarprodukt auf $\mathcal{V}$, da für $[C] \neq [D]$

$$([C], [D]) = |\mathrm{Aut}(C)|\delta_{[C],[D]} = 0 = \overline{|\mathrm{Aut}(D)|\delta_{[D],[C]}} = \overline{([D], [C])}$$

und für jedes $v \neq 0 \in \mathcal{V}$

$$v = \sum_{[C] \in \mathcal{B}} v_{[C]}[C]$$

mit $v_{[C]} \neq 0$ für mindestens ein $[C] \in \mathcal{B}$ so folgt:

$$(v, [C]) = v_{[C]}|\mathrm{Aut}(C)| \neq 0$$

für ein solches $[C]$, da $|\mathrm{Aut}(C)| \neq 0$.

Um den vollständigen Gewichtszähler von Geschlecht m definieren zu können, brauchen wir einige Begriffe zu Polynomen in q^m Variablen.

2.2.2 Definition

1. $\mathcal{P}_m := \mathbb{C}[x_a : a \in \mathbb{F}_q^m]$ *sei der Ring der Polynome in* q^m *Variablen über* $\mathbb{C}$.
2. $\mathcal{M}_m := \{\prod_{a\in\mathbb{F}_q^m} x_a^{e_a} : \sum_{a\in\mathbb{F}_q^m} e_a = N\}$ *seien die Monome von Grad* N *in* $\mathcal{P}_m$.
3. $\mathrm{rk}(X) := \dim\langle a : e_a > 0\rangle$ *für* $X = \prod_{a\in\mathbb{F}_q^m} x_a^{e_a} \in \mathcal{M}_m$ *ist der Rang von* X.
4. $\mathcal{M}_m^* := \{X \in \mathcal{M}_m : \mathrm{rk}(X) = m\}$ *sein die Monome von Rang* m

Zu einer $m \times N$-Matrix über $\mathbb{F}_q$ kann man auf folgende Art ein Monom in $\mathcal{M}_m$ definieren:

2.2.3 Definition
Sei $\underline{c} := (c^{(1)}, c^{(2)}, \ldots, c^{(m)})^{tr} \in (\mathbb{F}_q^N)^m = \mathbb{F}_q^{m\times N}$, *dann ist*

$$\mathrm{mon}(\underline{c}) := \prod_{v\in\mathbb{F}_q^m} x_v^{a_v(\underline{c})} \in \mathcal{M}_m$$

das zu $\underline{c}$ *gehörende Monom, wobei*

$$a_v(\underline{c}) := |\{i \in \{1, \ldots, \mathbb{N}\} : c_i^{(j)} = v_j \forall 1 \le j \le m\}|$$

mit $v = (v_1, \ldots, v_m)^{tr} \in \mathbb{F}_q^{m\times 1}$. $a_v(\underline{c})$ *ist die Anzahl von Spalten der* $m \times N$ *Matrix* $\underline{c}$ *die gleich* v *sind.*

2.2.4 Definition
Sei $X \in \mathcal{M}_m$ *und* C *ein linearer Code in* $\mathbb{F}_q^N$ *dann ist:*

$$a_X(C) := |\{\underline{c} := (c^{(1)}, \ldots, c^{(m)})^{tr} \in C^m : \mathrm{mon}(\underline{c}) = X\}|$$

2.2.5 Bemerkung
$a_X(C)$ *hängt nur von der Äquivalenzklasse von* C *ab,* $a_X([C])$ *ist also wohldefiniert, wodurch man kann man die Definition 2.2.4 auf ganz* $\mathcal{V}$ *erweitern kann:*

$$a_X : \mathcal{V} \to \mathbb{C}, \sum_{[C]\in\mathcal{B}} v_C[C] \mapsto \sum_{[C]\in\mathcal{B}} v_C a_X(C)$$

2.2.6 Definition
Der vollständige Gewichtszähler von Geschlecht m *ist definiert durch*

$$\mathrm{cwe}_m := \sum_{X\in\mathcal{M}_m} a_X(C)X \in \mathcal{P}_m$$

mit $\mathrm{cwe}_0 := 1$.
Diese Definition kann man folgendermaßen auf ganz $\mathcal{V}$ *ausdehnen:*

$$\mathrm{cwe}_m : \mathcal{V} \to \mathcal{P}_m, v \mapsto \sum_{X \in \mathcal{M}_m} a_X(v) X$$

Um die Beziehung zwischen dem vollständigen Gewichtszähler vom Geschlecht m und m-1 analysieren zu können definieren wir:

2.2.7 Definition
Ein Analogon zum Siegelschen Φ*-Operator ist gegeben durch:*

$$\Phi : \mathcal{P}_m \to \mathcal{P}_{m-1}, x_a \mapsto \begin{cases} x_{\epsilon^{-1}(a)} & \text{für } a \in \epsilon(\mathbb{F}_q^{m-1}) \\ 0 & \text{sonst} \end{cases}$$
$$\epsilon : \mathbb{F}_q^{m-1} \to \mathbb{F}_q^m, (a_1, \ldots, a_{m-1}) \mapsto (a_1, \ldots, a_{m-1}, 0)$$

2.2.8 Bemerkung
Durch Φ *gehen homogene Polynome vom Grad N in* $\mathcal{P}_m$ *entweder auf die Null in* $\mathcal{P}_m$ *oder wieder auf ein homogenes Polynom vom Grad N über.*

Nun kann man den Kern des vollständigen Gewichtszählers von Geschlecht m genauer betrachten.

2.2.9 Definition
Für $m \in \mathbb{N}_0$ *sei:*

$$\begin{aligned} \mathcal{V}_m &:= \mathrm{kern}(\mathrm{cwe}_m) \leq \mathcal{V} \\ \mathcal{V}_m &= \{v \in \mathcal{V} : a_X(v) = 0 \forall X \in \mathcal{M}_m\} \end{aligned}$$

Aus $\Phi(\mathrm{cwe}_m(v)) = \mathrm{cwe}_{m-1}(v)\ \forall v \in \mathcal{V}$ folgt $\mathcal{V}_m \leq \mathcal{V}_{m-1}$ und da die vollständigen Gewichtszähler vom Geschlecht n auf der Basis $\mathcal{B}$ von $\mathcal{V}$ linear unabhängig sind erhält man die folgende Filtration auf V:

2.2.10 Bemerkung
Man erhält nun für $\mathcal{V}$

$$\begin{aligned} \mathcal{V} := \quad & \mathcal{V}_{-1} \geq \mathcal{V}_0 \geq \cdots \geq \mathcal{V}_n \quad &= \{0\} \\ \mathcal{V} = \quad & \mathcal{V}_n^{\perp} \geq \mathcal{V}_{n-1}^{\perp} \geq \cdots \geq \mathcal{V}_{-1}^{\perp} \quad &= \{0\} \end{aligned}$$

wobei $n = N/2 = \dim(C)$ *ist.*

Für $\mathcal{V}_m^{\perp}$ kann man auf ein Erzeugendensystem angeben:

2.2.11 Bemerkung
Sei $X \in \mathcal{M}_m$ und

$$b_X := \sum_{[C]\in\mathcal{B}} \frac{a_X(C)}{|\mathrm{Aut}(C)|}[C] \in \mathcal{V}$$

dann gilt $\mathcal{V}_m^\perp = \langle b_X : X \in \mathcal{M}_m\rangle$ und $(b_X, v) = a_X(v)$ für alle $v \in \mathcal{V}$.

Beweis:
Mit $v := \sum_{[C]\in\mathcal{B}} v_C[C] \in \mathcal{V}$ gilt

$$\begin{aligned}
(b_X, v) &= \left(\sum_{[C]\in\mathcal{B}} \frac{a_X(C)}{|\mathrm{Aut}(C)|}[C], \sum_{[D]\in\mathcal{B}} v_D[D]\right) \\
&= \sum_{[C]\in\mathcal{B}} \frac{a_X(C)}{|\mathrm{Aut}(C)|}\left([C], \sum_{[D]\in\mathcal{B}} v_D[D]\right) \\
&= \sum_{[C]\in\mathcal{B}} \frac{a_X(C)}{|\mathrm{Aut}(C)|}\left(\sum_{[D]\in\mathcal{B}} v_D([C],[D])\right) \\
&= \sum_{[C]\in\mathcal{B}} \frac{a_X(C)}{|\mathrm{Aut}(C)|}|\mathrm{Aut}(C)|v_C \\
&= \sum_{[C]\in\mathcal{B}} v_C a_X(C) = a_X(v)
\end{aligned}$$

Sei nun $\mathcal{U}_m := \langle b_X : X \in \mathcal{M}_m\rangle$ so folgt:

$$\begin{aligned}
&\mathcal{U}_m^\perp = \{v \in \mathcal{V} : (b_X, v) = a_X(v) = 0 \ \forall X \in \mathcal{M}_m\} = \mathcal{V}_m \\
&\Rightarrow \mathcal{U}_m = \mathcal{V}_m^\perp
\end{aligned}$$

q.e.d.

2.2.12 Bemerkung
Für den Vektorraum $\mathcal{V}$ gibt es folgende orthogonale Zerlegung:

$$\mathcal{V} = \perp_{m=0}^{n} \mathcal{Y}_m$$

mit:

$$\mathcal{Y}_m := \mathcal{V}_m^\perp \cap \mathcal{V}_{m-1} = \{v \in \mathcal{V}_m^\perp : (v, x) = 0 \forall x \in \mathcal{V}_{m-1}^\perp\}.$$

Beweis:
Klar ist, dass $\mathcal{Y}_m \subseteq \mathcal{Y}_{m-1}^{\perp}$ und $\mathcal{Y}_m \subseteq \mathcal{Y}_{m+1}^{\perp}$ da:

$$\begin{aligned} \mathcal{Y}_{m-1}^{\perp} = \quad & (\mathcal{V}_{m-1}^{\perp} \cap \mathcal{V}_{m-2})^{\perp} = \quad \mathcal{V}_{m-1} + \mathcal{V}_{m-2}^{\perp} \supseteq \mathcal{V}_{m-1} \cap \mathcal{V}_m^{\perp} = \mathcal{Y}_m \\ \mathcal{Y}_{m+1}^{\perp} = \quad & (\mathcal{V}_{m+1}^{\perp} \cap \mathcal{V}_m)^{\perp} = \quad \mathcal{V}_{m+1} + \mathcal{V}_m^{\perp} \supseteq \mathcal{V}_m^{\perp} \cap \mathcal{V}_{m-1} = \mathcal{Y}_m \end{aligned}$$

Zeige nun noch, dass $\mathcal{V}_i^{\perp} = \mathcal{Y}_i + \mathcal{V}_{i-1}^{\perp}$ und wähle dazu eine Orthogonalbasis $\mathcal{B}_{i-1}$ von $\mathcal{V}_{i-1}^{\perp}$.
Sei nun $v \in \mathcal{V}_i^{\perp}$, falls $v \in \mathcal{V}_{i-1}$ gilt $v \in \mathcal{Y}_i$. Für $v \notin \mathcal{V}_{i-1}$ gibt es eine Teilmenge $\emptyset \neq B \subseteq \mathcal{B}_{i-1}$ mit $(v, b) \neq 0$ für alle $b \in B$, definiere also

$$v' := v - \sum_{b \in B} \frac{(v,b)}{(b,b)} b$$

Dies ist möglich da $(\cdot, \cdot)$ ein positiv definites Skalarprodukt ist. Dann gilt $(v', b) = 0$ für alle $b \in B$ und $(v', b') = 0$ für alle $b' \in \mathcal{B}_{i-1}$ mit $(v, b') = 0$, also $v' \in \mathcal{Y}_i$ und $v = v' + \sum_{b \in B} \frac{(v,b)}{(b,b)} b \in \mathcal{Y}_i + \mathcal{V}_{i-1}^{\perp}$.

q.e.d.

Diese Zerlegung ist, wie in 2.3.5 bewiesen wird, die Eigenraumzerlegung von $\mathcal{V}$ bezüglich des ersten Kneser-Hecke-Operators, der im nächsten Abschnitt definiert wird.

2.3 Der Kneser-Hecke-Operator

Nun kommen wir zur Definition des Kneser-Hecke-Operators und zu einigen wichtigen Resultaten aus [Neb06].

2.3.1 Definition
Sei $\mathcal{F}$ eine Familie selbstdualer Codes der Länge N und der Dimension $n = N/2$, dann heißen $C, D \in \mathcal{F}$ k-Nachbarn oder auch k-Kneser-Nachbarn $C \sim_k D$ falls $\dim(C \cap D) = \dim(C) - k$ für $0 \leq k \leq n$.
Die Abbildung

$$T_k : \mathcal{V} \to \mathcal{V}, T_k([C]) := \sum_{D \sim_k C} [D]$$

heißt k-ter Kneser-Hecke-Operator auf $\mathcal{F}$.

2.3.2 Satz
Für $0 \leq k \leq n$ ist T_k ein selbstadjungierter linearer Operator auf dem Vektorraum $\mathcal{V}$.

Beweis:
Da T_k linear ist, reicht es die Selbstadjungiertheit für die Elemente der Basis $\mathcal{B}$ nachzuprüfen, seinen also $[C], [D] \in \mathcal{B}$. Aus der Symmetrie der Nachbarschaftsrelation und der Invarianz der Nachbarschaftsrelation unter der Operation der S_N auf $\mathcal{V}$ erhält man:

$$\begin{aligned}
&\frac{N!}{|\mathrm{Aut}(D)|}|\{C' \in \mathcal{F} : C' \sim_k D \wedge C' \cong C\}| \\
&= \sum_{\tilde{D} \cong D} |\{C' \in \mathcal{F} : C' \sim_k \tilde{D} \wedge C' \cong C\}| \\
&= \sum_{\tilde{C} \cong C} |\{D' \in \mathcal{F} : D' \sim_k \tilde{C} \wedge D' \cong D\}| \\
&= \frac{N!}{|\mathrm{Aut}(C)|}|\{D' \in \mathcal{F} : D' \sim_k C \wedge D' \cong D\}|
\end{aligned}$$

wobei $\cong$ hier Permutationsäquivalent bedeutet.
Daraus folgt nun direkt

$$\begin{aligned}
(T_k([C]), [D]) &= \sum_{D' \sim_k C} ([C], [D']) \\
&= |\mathrm{Aut}(D)||\{D' \in \mathcal{F} : D' \sim_k C \wedge D' \cong D\}| \\
&= |\mathrm{Aut}(C)||\{C' \in \mathcal{F} : C' \sim_k C \wedge C' \cong C\}| \\
&= \sum_{C' \sim_k D} ([C'], [D]) = ([C], T_k([D]))
\end{aligned}$$

q.e.d.

2.3.3 Lemma
Sei $\underline{c} := (c^{(1)}, \ldots, c^{(m)})^{tr} \in C^m$ *und* $X := \mathrm{mon}(\underline{c})$, $\underline{b} := (b^{(1)}, \ldots, b^{(m)})^{tr} \in C^m$ *mit* $\langle b^{(1)}, \ldots, b^{(m)} \rangle = \langle c^{(1)}, \ldots, c^{(m)} \rangle$ *so gilt:*

$$a_X(v) = a_{\mathrm{mon}(\underline{b})}(v) \quad \forall v \in \mathcal{V}.$$

Beweis:
Da $\langle b^{(1)}, \ldots, b^{(m)} \rangle = \langle c^{(1)}, \ldots, c^{(m)} \rangle$ gilt gibt es eine Matrix $A \in \mathrm{GL}_m(\mathbb{F}_q)$ so dass $A\underline{c} = \underline{b}$. Sei $D \in \mathcal{F}$ ein Code und $\pi(\underline{c}) \in D^m$ für ein $\pi \in S_N$ enthalten ist, so gilt auch $A\pi(\underline{c}) \in D^m$ da $\langle \pi(\underline{c}) \rangle = \langle A\pi(\underline{c}) \rangle$ mit $A \in \mathrm{GL}_m(\mathbb{F}_q)$. Da A die Spalten von $\underline{c}$ injektiv abbildet und π nur die Reihenfolge der Spalten verändert gilt

$$\mathrm{mon}(A\pi(\underline{c})) = \mathrm{mon}(A\underline{c}) = \mathrm{mon}(\underline{b}).$$

Also gibt es zu jedem $(d^{(1)}, \ldots, d^{(m)})^{tr} \in D^m$ mit $\mathrm{mon}(d^{(1)}, \ldots, d^{(m)}) = X$ ein

$$(e^{(1)}, \ldots, e^{(m)})^{tr} = A(d^{(1)}, \ldots, d^{(m)})^{tr} \in D^m$$

mit

$$\mathrm{mon}(e^{(1)}, \ldots, e^{(m)}) = \mathrm{mon}(\underline{b}).$$

Da A invertierbar ist gibt es auch zu jedem $(e^{(1)}, \ldots, e^{(m)})^{tr} \in D^m$ mit $\mathrm{mon}(e^{(1)}, \ldots, e^{(m)}) = \mathrm{mon}(\underline{b})$ ein

$$(d^{(1)}, \ldots, d^{(m)})^{tr} = A^{-1}(e^{(1)}, \ldots, e^{(m)})^{tr} \in D^m$$

mit

$$\mathrm{mon}(d^{(1)}, \ldots, d^{(m)}) = X.$$

Man kann deswegen folgern, dass

$$a_X(D) = a_{\mathrm{mon}(\underline{b})}(D) \quad \forall D \in \mathcal{F}$$

gilt, woraus direkt die Behauptung folgt. q.e.d.

Den folgenden, zentralen Satz aus [Neb06] kann man nur für Familien von Codes beweisen die spezielle Bedingungen erfüllen, die aber von allen Familien von Codes eines klassischen Typs (siehe 3.3) erfüllt werden.

2.3.4 Vorbemerkung
Für den folgenden Satz benötigen wir noch folgendes:

1. *Wähle eine geeignete Teilmenge $\mathcal{M}_m^0 \subseteq \mathcal{M}_m^*$ so dass $\mathcal{V}_m = \{v \in \mathcal{V} : a_X(v) = 0 \forall X \in \mathcal{M}_m^0\}$*
2. *Wähle $\mathcal{F}$ so dass für alle $C \in \mathcal{F}$ und für alle $\underline{c} := (c^{(1)}, \ldots, c^{(m)}) \in C^m$ mit $\mathrm{mon}(\underline{c}) \in \mathcal{M}_m^0$ gilt:*

   $$\alpha_m := \sum_{E \in \mathcal{E}_C(\underline{c})} \alpha_E$$

   mit

   $$\mathcal{E}_C(\underline{c}) := \{E \leq C : \dim(E) = n-1, \underline{c} \in E^m\}$$

   und $\alpha_E = \alpha_E(C) := |\{D \in \mathcal{F} : D \cap C = E\}|$
3. *Die Anzahl der (m-1)-dimensionalen Teilräume des $\mathbb{F}_q^m$ ist*

   $$\beta_m := \frac{q^m - 1}{q - 1}.$$

Die Bedingungen aus 2.3.4 sind für alle klassischen Typen von Codes erfüllt, siehe dazu 3.3 oder [Neb06].

2.3.5 Satz
Falls 2.3.4 erfüllt ist, sind $\mathcal{Y}_m \leq \mathcal{V}$ genau die Eigenräume von T_1 in $\mathcal{V}$ zu den Eigenwerten $\nu_m := \alpha_m - \beta_m$.

Beweis:
Es genügt zu zeigen, dass $T_1(v) = \nu_m v$ für alle $v \in \mathcal{V}_{m-1}/\mathcal{V}_m$, also

$$T_1(v) - \nu_m v \in \mathcal{V}_m = \text{kern}(\text{cwe}_m)$$

für

$$v := \sum_{[C]\in\mathcal{B}} v_C[C] \in \mathcal{V}_{m-1} = \text{kern}(\text{cwe}_{m-1})$$

Was gleichbedeutend ist mit

$$a_X(T_1(v) - \nu_m v) = 0 \; \forall X \in \mathcal{M}_m^0$$

Nach Definition gilt:

$$T_1(v) = \sum_{[C]\in\mathcal{B}} v_C \sum_{\substack{E\leq C \\ \dim(E)=n-1}} \sum_{\substack{D\in\mathcal{F} \\ E=D\cap C}} [D]$$

Berechne also für $X \in \mathcal{M}_m^0$ und festes $C \in \mathcal{F}$:

$$\sum_{\substack{E\leq C \\ \dim(E)=n-1}} \sum_{\substack{D\in\mathcal{F} \\ E=D\cap C}} a_X([D]). \tag{2.1}$$

Sei dabei $\underline{c} := (c^{(1)}, \ldots, c^{(m)}) \in D^m$ für ein $D \sim_1 C$, so dass $\text{mon}(\underline{c}) = X \in \mathcal{M}_m^0$, daraus folgt insbesondere dass $\underline{c} = (c^{(1)}, \ldots, c^{(m)})$ eine linear unabhängige Folge ist. Dann sei $W := \langle c^{(1)}, \ldots, c^{(m)} \rangle$. Zerlege nun die Summe

(2.1) in zwei Anteile:

$$\begin{aligned}
&\sum_{\substack{E\leq C\\ \dim(E)=n-1}} \sum_{\substack{D\in\mathcal{F}\\ E=D\cap C}} a_X([D])\\
=&\sum_{\substack{E\leq C\\ \dim(E)=n-1}} \sum_{\substack{D\in\mathcal{F}\\ D\cap C=E}} |\{\underline{c}\in D^m : \mathrm{mon}(\underline{c})=X\}|\\
=&\sum_{D\sim_1 C} |\{\underline{c}\in D^m : \mathrm{mon}(\underline{c})=X\}|\\
=&\sum_{D\sim_1 C} |\{\underline{c}\in D^m : \underline{c}\in C^m \wedge \mathrm{mon}(\underline{c})=X\}|\\
+&\sum_{D\sim_1 C} |\{\underline{c}\in D^m : \langle\underline{c}\rangle\not\leq C \wedge \mathrm{mon}(\underline{c})=X\}|\\
=&\underbrace{\sum_{\substack{\underline{c}\in\mathbb{F}_q^{m\times N},\langle\underline{c}\rangle\leq C\\ \mathrm{mon}(\underline{c})=X}} |\{D\sim_1 C : \underline{c}\in D^m\}|}_{=(a)} + \underbrace{\sum_{\substack{\underline{c}\in\mathbb{F}_q^{m\times N},\mathrm{mon}(\underline{c})=X\\ \dim(\langle\underline{c}\rangle\cap C)=m-1}} |\{D\sim_1 C : \underline{c}\in D^m\}|}_{=(b)}
\end{aligned}$$

Dann kann man die beiden Teilsummen (a) und (b) getrennt auswerten, mit 2.3.4 folgt:

$$(a)=\sum_{\substack{\underline{c}\in\mathbb{F}_q^{m\times N},\langle\underline{c}\rangle\leq C\\ \mathrm{mon}(\underline{c})=X}} \alpha_m = a_X(C)\alpha_m \;\forall X\in\mathcal{M}_m^0$$

Bei der zweiten Teilsumme ist zu beachten dass $D:=(C+\langle\underline{c}\rangle)^\perp+\langle\underline{c}\rangle$ der eindeutig festgelegte 1-Nachbar von C ist der $\langle\underline{c}\rangle$ enthält, denn gäbe es einen weiteren 1-Nachbarn E mit

$$\begin{aligned}
&\langle\underline{c}\rangle\leq E\\
\Rightarrow&(C+\langle\underline{c}\rangle)\geq E\geq(C+\langle\underline{c}\rangle)^\perp\\
\Rightarrow&(C+\langle\underline{c}\rangle)^\perp+\langle\underline{c}\rangle\leq E
\end{aligned}$$

und mit 2.1.2 folgt:

$$((C+\langle\underline{c}\rangle)^\perp+\langle\underline{c}\rangle)^\perp=(C+\langle\underline{c}\rangle)\cap\langle\underline{c}\rangle^\perp$$

und deswegen

$$\dim((C+\langle\underline{c}\rangle)^\perp+\langle\underline{c}\rangle)=n=\dim(E)$$

also aus Dimensionsgründen ist $E = (C + \langle \underline{c} \rangle)^{\perp} + \langle \underline{c} \rangle$ und der 1-Nachbar von C der $\langle \underline{c} \rangle$ enthält ist eindeutig bestimmt.

Damit folgt:

$$\begin{aligned}
(b) &= |\{\underline{c} \in \mathbb{F}_q^{m\times N} : \mathrm{mon}(\underline{c}) = X \wedge \dim(\langle \underline{c} \rangle \cap C) = m-1\}| \\
&= \sum_{U \leq C, \dim(U)=m-1} |\{\underline{c} \in \mathbb{F}_q^{m\times N} : \mathrm{mon}(\underline{c}) = X \wedge \langle \underline{c} \rangle \cap C = U\}| \\
&= \sum_{U \leq C, \dim(U)=m-1} (|\{\underline{c} \in \mathbb{F}_q^{m\times N} : \mathrm{mon}(\underline{c}) = X \wedge U \leq \langle \underline{c} \rangle\}| \\
&\qquad\qquad - |\{\underline{c} \in C^m : \mathrm{mon}(\underline{c}) = X \wedge U \leq \langle \underline{c} \rangle\}|) \\
&= \sum_{U \leq C, \dim(U)=m-1} \left(|\{\underline{c} \in \mathbb{F}_q^{m\times N} : \mathrm{mon}(\underline{c}) = X \wedge U \leq \langle \underline{c} \rangle\}|\right) - \beta_m a_X([C]) \\
&= \left(\prod_{i=1}^{m} \beta_m\right)^{-1} \sum_{Y \in \mathcal{M}_{m-1}^0} (a_Y(C) |\{\underline{c} \in \mathbb{F}_q^{m\times N} : \mathrm{mon}(\underline{c}) = X \wedge \\
&\qquad\qquad \exists \underline{b} \in C^m, \mathrm{mon}(\underline{b}) = Y \wedge \langle \underline{b} \rangle \leq \langle \underline{c} \rangle\}|) - \beta_m a_X([C])
\end{aligned}$$

Da

$$f(X,Y) := |\{\underline{c} \in \mathbb{F}_q^{m\times N} : \mathrm{mon}(\underline{c}) = X \wedge \exists \underline{b} \in C^m, \mathrm{mon}(\underline{b}) = Y \wedge \langle \underline{b} \rangle \leq \langle \underline{c} \rangle\}|$$

unabhängig von der betrachteten Äquivalenzklasse $[C]$ ist kann man Fall (a) und Fall (b) folgendermaßen zusammenfügen:

$$\begin{aligned}
a_X(T(v)) &= \sum_{[C]\in\mathcal{B}} v_C \sum_{D \sim_1 C} a_X([D]) \\
&= \sum_{[C]\in\mathcal{B}} v_C \left(\alpha_m a_X([C]) + \sum_{Y \in \mathcal{M}_{m-1}^0} a_Y([C]) f(X,Y) - a_X([C])\beta_m\right) \\
&= (\alpha_m - \beta_m) \sum_{[C]\in\mathcal{B}} v_C a_X([C]) + \sum_{[C]\in\mathcal{B}} \left(v_C \sum_{Y \in \mathcal{M}_{m-1}^0} a_Y([C]) f(X,Y)\right) \\
&= (\alpha_m - \beta_m) \sum_{[C]\in\mathcal{B}} v_C a_X([C]) + \sum_{Y \in \mathcal{M}_{m-1}^0} \left(f(X,Y) \sum_{[C]\in\mathcal{B}} v_C a_Y([C])\right) \\
&= (\alpha_m - \beta_m) \sum_{[C]\in\mathcal{B}} v_C a_X([C]) = (\alpha_m - \beta_m) v \; \forall X \in \mathcal{M}_m^0
\end{aligned}$$

da

$$\sum_{[C]\in\mathcal{B}} v_C a_Y([C]) = 0$$

weil $v \in \ker(\mathrm{cwe}_{m-1})$ und Y und alle $X \in \mathcal{M}_m^0$. Somit folgt die Behauptung.
q.e.d

Mittels der polynomialen Darstellung von T_k in T_1, die wir im folgenden herleiten werden kann, man dieses Ergebnis von T_1 direkt auf T_k übertragen und erhält deswegen simultane Diagonalisierbarkeit für Kneser-Hecke-Operatoren.

2.4 Der Nachbarschaftsgraph

Nun benötigen wir noch einige grundlegende Definitionen und Sätze aus der Graphentheorie, um eine andere Betrachtungsweise der Nachbarschaftsrelationen, die Nachbarschaftsgraphen, einführen zu können.

2.4.1 Definition
Ein Graph $(E, \sim)$ besteht aus einer endlichen Menge $E := \{e_1, \ldots, e_n\}$, der sogenannten Eckenmenge, und einer symmetrischen Relation $\sim$ auf der Eckenmenge, in Relation stehende Ecken nennt man adjazent oder benachbart. Man definiert zu $(E, \sim)$ noch die Kantenmenge K in der alle adjazenten Eckenpaare enthalten sind $K := \{\{e_i, e_j\} : e_i, e_j \in E\}$. Die symmetrische Matrix

$$A := \begin{bmatrix} a_{11} & \ldots & a_{1|E|} \\ \vdots & & \vdots \\ a_{1|E|} & \ldots & a_{|E||E|} \end{bmatrix}$$

mit

$$a_{ij} := 1_{(e_i,e_j)} := \begin{cases} 1, & e_i \sim e_j \\ 0, & \textit{sonst} \end{cases}$$

heißt Adjazenzmatrix des Graphen.

2.4.2 Definition
Eine Folge von Ecken $(e_0, \ldots, e_n)$ in einem Graphen $(E, \sim)$ heisst Weg der Länge n von e_0 nach e_n, falls für alle $0 \leq i \leq n-1$ gilt $e_i \sim e_{i+1}$. Der Abstand von e_i und e_j $d_{(E,\sim)}(e_i, e_j)$ ist die Länge des kürzesten Weges von e_i nach e_j.

2.4.3 Satz
Sei A die Adjazenzmatrix eines Graphen, dann gilt $(A^n)_{i,j}$ ist gleich der Anzahl der Wege der Länge n von der Ecke e_i zur Ecke e_j.

Beweis: per Induktion:

$$\begin{aligned} n = 2 : A^2 &= (\sum_{i=1}^{|E|} a_{ki} a_{ij})_{1 \leq j,k \leq |E|} \\ &= (\sum_{i=1}^{|E|} 1_{(e_j,e_i)} 1_{(e_i,e_k)})_{1 \leq j,k \leq |E|} \\ &= (|\{\text{Wege der Länge 2 von } e_j \text{ nach } e_k\}|)_{1 \leq j,k \leq |E|} \end{aligned}$$

Sei $n \in \mathbb{N}$:

$$\begin{aligned} n &\rightarrow n+1 : \\ A^{n+1} &= A^n A = (\sum_{i=1}^{|E|} A_{ki}^{(n)} A_{ij})_{1 \leq j,k \leq |E|} \\ &= (\sum_{i=1}^{|E|} |\{\text{Wege der Länge n von } e_k \text{ nach } e_i\}| 1_{(e_i,e_k)})_{1 \leq j,k \leq |E|} \\ &= (|\{\text{Wege der Länge n+1 von } e_j \text{ nach } e_k\}|)_{1 \leq j,k \leq |E|} \end{aligned}$$

q.e.d.

2.4.4 Definition
Der k-Nachbarschaftsgraph einer Familie von Codes $\mathcal{F}$ ist der Graph mit der Eckenmenge $E := \{C : C \in \mathcal{F}\}$ und der k-Nachbarschaftsrelation $\sim_k$. Es sind also genau die Codes adjazent, die k-Nachbarn sind.

Kapitel 3

T_k als Polynom in T_1

Um T_k als Polynom in T_1 darzustellen werden, wir zuerst den Zusammenhang zwischen T_k und der Adjazenzmatrix des k-Nachbarschaftsgraphen A_k herstellen und dann mittels 2.4.3 A_1^k als Linearkombination der A_i mit $1 \leq i \leq k$ und E_N schreiben.

3.1 T_k und der k-Nachbarschaftsgraph

3.1.1 Satz
Sei A_k die Adjazenzmatrix des k-Nachbarschaftsgraphen $(\mathcal{F}, \sim_k)$ und T_k der k-te Kneser-Hecke-Operator auf $\mathcal{V} := \langle [C] : C \in \mathcal{F} \rangle$. Dann gibt es Matrizen $U \in \{0,1\}^{|\mathcal{F}| \times \dim(\mathcal{V})}$ und $V \in \{0,1\}^{\dim(\mathcal{V}) \times |\mathcal{F}|}$, so dass $V A_k U = T_k$.

Beweis:
O.B.d.A. seien die Ecken des Nachbarschaftsgraphen so angeordnet, dass die permutationsäquivalenten Codes immer direkt aufeinander folgen, ferner sei $m_0 := 0$, $m_i := \sum_{j=1}^{i} |[C_j]|$ für $1 \leq i \leq \dim(\mathcal{V})$, wobei $|[C_i]|$ die Anzahl der Codes in der i-ten Äquivalenzklasse bzgl. der in der Adjazenzmatrix gewählten Anordnung bezeichne. Dann erfüllen

$$V = (v_{ij})_{1 \leq i \leq \dim(\mathcal{V}), 1 \leq j \leq |\mathcal{F}|} \text{ mit } v_{ij} := \begin{cases} 1 & \text{für } m_{i-1} + 1 \leq j \leq m_i \\ 0 & \text{sonst} \end{cases}$$

$$U = (u_{ij})_{1 \leq i \leq |\mathcal{F}|, 1 \leq j \leq \dim(\mathcal{V})} \text{ mit } u_{ij} := \begin{cases} 1 & \text{für } i = m_j \\ 0 & \text{sonst} \end{cases}$$

gerade die Behauptungen, da durch die Linksmultiplikation mit V gerade für jede Äquvivalenzklasse über die k-Nachbarn von C_i summiert wird, was

genau die Anzahl der k-Nachbarn von C_i entspricht die in einer Äquvivalenzklasse liegen und dann wird durch die Rechtsmultipliktion mit U für jede Äquivalenzklasse genau ein Eintrag ausgewählt wird, was der Wahl eines Repräsentanten entspricht. q.e.d.

3.1.2 Satz
Mit U und V aus 3.1.1 folgt für A_k und T_k:

$$VA_k^sU = T_k^s \; \forall s \in \mathbb{N}$$

.

Beweis:
Sei $A_k := (a_{ij})_{1\leq i,j\leq|\mathcal{F}|}$, dann ist

$$A_k^2 = (\sum_{l=1}^{|\mathcal{F}|} a_{il}a_{lj})_{1\leq i,j\leq|\mathcal{F}|}$$

und es sei $UA_kV = T_k := (t_{ij})_{1\leq i,j\leq\dim(\mathcal{V})}$ und $t_{ij} := \sum_{r=m_{i-1}+1}^{m_i} a_{rm_j}$, wobei $m_i := \sum_{j=1}^{i} |[C_j]|$ wie im Beweis von Satz 3.1.1. Dann gilt wie in 3.1.1:

$$T_k([C_j]) = \sum_{i=1}^{d} t_{ij}[C_i] \tag{3.1}$$

Wir zeigen die Aussage per Induktion zunächst s=2:

$$\begin{aligned} T_k^2 &= T_k(T_k([C_j])) = \sum_{i=1}^{d} t_{ij}T_k([C_i]) = \sum_{i=1}^{d} t_{ij} \sum_{r=1}^{d} t_{ri}[C_r] \\ &= \sum_{r=1}^{d} \left(\sum_{i=1}^{d} t_{ij}t_{ri} \right) [C_r]. \end{aligned}$$

bleibt also zu zeigen dass $(VA_k^2U)_{ij} = \sum_{r=1}^{d} t_{rj}t_{ir}$:

$$\begin{aligned} (VA_k^2U)_{ij} &= \sum_{r=m_{i-1}+1}^{m_i} \left(\sum_{l=1}^{|\mathcal{F}|} a_{rl}a_{lm_j} \right) = \sum_{l=1}^{|\mathcal{F}|} \left(a_{lm_j} \sum_{r=m_{i-1}+1}^{m_i} a_{rl} \right) \\ &= \sum_{l=1}^{|\mathcal{F}|} a_{lm_j}t_{iv(l)} \end{aligned}$$

mit $v(l) := j$ für alle $m_{j-1} < l \leq m_j$

$$= \sum_{l=1}^{|\dim(\mathcal{V})|} \left(x_{il} \sum_{r=m_{l-1}+1}^{m_l} a_{rm_j} \right) = \sum_{l=1}^{|\dim(\mathcal{V})|} x_{il} x_{lj}$$

Sei nun $VA_k^s U = T_k^s$ erfüllt so gilt $VA_k^{s+1}U = T_k^{s+1}$:

$$A_k^{s+1} = A_k A_k^s = (\sum_{w=1}^{|\mathcal{F}|} a_{iw} b_{wj})_{1 \leq i,j \leq |\mathcal{F}|} \text{ mit } A_k^s := (b_{ij})_{1 \leq i,j \leq |\mathcal{F}|}$$

Sei:

$$\begin{aligned} y_{ij} &:= \sum_{r=m_{i-1}+1}^{m_i} b_{rm_j} \overset{\text{I.V.}}{=} (T_k^s)_{ij} \\ T_k^{s+1} &= T_k(T_k^s([C_j])) = \sum_{r=1}^{\dim(\mathcal{V})} y_{rj} T_k([C_r]) \\ &= \sum_{r=1}^{\dim(\mathcal{V})} y_{rj} \sum_{l=1}^{\dim(\mathcal{V})} t_{lr}[C_l] = \sum_{l=1}^{\dim(\mathcal{V})} \left(\sum_{r=1}^{\dim(\mathcal{V})} y_{rj} t_{lr} \right) [C_l] \end{aligned}$$

andererseits gilt:

$$\begin{aligned} (VA_k^{s+1}U)_{ij} &= \sum_{l=m_{i-1}+1}^{m_i} \left(\sum_{w=1}^{|\mathcal{F}|} a_{lw} b_{wm_j} \right) \\ &= \sum_{w=1}^{|\mathcal{F}|} \left(b_{wm_j} \sum_{l=m_{i-1}+1}^{m_i} a_{lw} \right) = \sum_{w=1}^{|\mathcal{F}|} \left(b_{wm_j} t_{iv(w)} \right) \\ &= \sum_{w=1}^{\dim(\mathcal{V})} \left(t_{iw} \sum_{l=m_{w-1}+1}^{m_w} b_{lm_j} \right) = \sum_{w=1}^{\dim(\mathcal{V})} t_{iw} y_{wj} \end{aligned}$$

und damit folgt die Behauptung. q.e.d.

Aus dieser Beziehung zwischen der Adjazenzmatrix des k-Nachbarschaftsgraphen und des k-ten Kneser-Hecke-Operators folgt, dass man einen polynomialen Zusammenhang zwischen den Adjazenzmatrizen A_k auf die Kneser-Hecke-Operatoren T_k übertragen kann.

3.1.3 Satz
Seien A_k die Adjazenzmatrix des k-Nachbarschaftsgraphen einer Familie von Codes $\mathcal{F}$, A_1 die Adjazenzmatrix des zugehörigen 1-Nachbarschaftsgraphen und T_1 bzw. T_k die entsprechenden Kneser-Hecke-Operatoren, dann gilt:

$$A_k = \sum_{i=1}^{k} p_i A_1^i \Rightarrow T_k = \sum_{i=1}^{k} p_i T_1^i \tag{3.2}$$

Beweis:
Der Zusammenhang folgt direkt mit 3.1.2 durch rechtsseitiges Multiplizieren mit U und linksseitiges Multiplizieren mit V. q.e.d.

3.1.4 Satz
Seien $C, D \in \mathcal{F}$ und $C \sim_k D$, dann ist $d_{(\mathcal{F},\sim_1)}(C, D) = k$

Beweis:
z.z.: $\dim(C) - \dim(C \cap D) = d_{(\mathcal{F},\sim_1)}(C, D)$
„$\geq$“:
Konstruiere iterativ einen Weg der Länge k von C nach D:

$$C_1 := X + (C + X)^\perp$$

mit $C \cap D \leq X \leq D$ und $\dim(X) = n - k + 1$.
Beh.: C_1 ist in $\mathcal{F}$ und $C_1 \sim_1 C$ und $C_1 \sim_{k-1} D$.
Es gilt $C_1 = C_1^\perp$:
da $X \leq D = D^\perp$ folgt $D \leq X^\perp$ und somit $X \leq X^\perp$ mit 2.1.2 folgt weiter:

$$\begin{aligned} C_1^\perp &= ((C + X)^\perp + X)^\perp = (C + X) \cap X^\perp \\ &= (C \cap X^\perp) + (X \cap X^\perp) = (C + X)^\perp + X = C_1 \end{aligned}$$

Somit ist C_1 selbstdual und da $X \leq D$ ist C_1 auch vom gleichen Typ wie D, also $C_1 \in \mathcal{F}$.
Es gilt $C_1 \sim_1 C$: da $C \cap D \leq X \leq X^\perp$ liegt nach 2.1.2 $C \cap D \leq C \cap X^\perp = (C + X)^\perp$, durch weiteres anwenden von 2.1.2 ergibt sich:

$$\begin{aligned} \dim(C_1 \cap C) &= \dim\left((X + (C + X)^\perp) \cap C\right) \\ &= \dim((X \cap C) + ((C + X)^\perp \cap C^\perp)) \\ &= \dim((C \cap D) + (C + X)^\perp) \\ &= \dim((C + X)^\perp) = n - 1 \end{aligned}$$

Es bleibt zu zeigen, dass $C_1 \sim_{k-1} D$:

$$\begin{aligned}\dim(C_1 \cap D) &= \dim((X + (C + X)^\perp) \cap D) \\ &= \dim(X + ((C + X)^\perp \cap D)) \\ &= \dim(X + (C + X + D)^\perp) = \dim(X) = k + 1\end{aligned}$$

Damit folgt $\dim(C) - \dim(C \cap D) \geq d_{(\mathcal{F},\sim_1)}(C, D)$.

„$\leq$“:
Annahme: Sei $d := d_{(\mathcal{F},\sim_1)}(C, D) < \dim(C) - \dim(C \cap D)$. Daraus folgt $\exists C_i \in \mathcal{F}$ für $1 \leq i \leq d-1$ mit $C \sim_1 C_1 \sim_1 \cdots \sim_1 C_{d-1} \sim_1 C_d =: D$. Zeige nun per Induktion über i dass

$$\dim(C \cap \bigcap_{j=1}^{i} C_j) \geq n - i$$

. I.A.: $\dim(C \cap C_1) = n - 1$ folgt da $C \sim_1 C_1$
I.V.: $\dim(C \cap \bigcap_{j=1}^{i} C_j) \geq n - i$
I.S.: $i \to i + 1$:

$$\dim(C_i \cap C_{i+1}) = n - 1 \Rightarrow \exists! b_i \in C_i \text{ mit } \langle b_i \rangle \not\leq C_{i+1}$$

Fall 1: $\langle b_i \rangle \leq C \cap \bigcap_{j=1}^{i} C_i$

$$\Rightarrow \dim(C \cap \bigcap_{j=1}^{i} C_i \cap C_{i+1}) = \dim(C \cap \bigcap_{j=1}^{i} C_i) - 1 \overset{\text{I.V.}}{\geq} n - (i + 1)$$

Fall 2: $\langle b_i \rangle \not\leq C \cap \bigcap_{j=1}^{i} C_i$

$$\Rightarrow \dim(C \cap \bigcap_{j=1}^{i} C_i \cap C_{i+1}) = \dim(C \cap \bigcap_{j=1}^{i} C_i) \overset{\text{I.V.}}{\geq} n - i \geq n - (i + 1)$$

Daraus folgt: $\dim(C \cap D) = \dim(C \cap C_d) \geq n - d$, was im Widerspruch zur Annahme steht.

q.e.d.

3.2 Wege durch den Nachbarschaftsgraphen

Nun werden wir die Wege durch den 1-Nachbarschaftsgraphen in Abhängigkeit der Nachbarschaftsrelation zwischen den Endpunkten zählen.

3.2.1 Satz
Sei $\mathcal{F}$ eine Familie von Codes der Länge $N = 2n$ über $\mathbb{F}_q$ und $G := (\mathcal{F}, \sim_1)$ der Nachbarschaftsgraph zu $\mathcal{F}$. Seien nun $C, D \in \mathcal{F}$ mit $C \sim_m D$, dann gilt für $k, m \in \mathbb{N}_0$

$$a_{k,m} := |\{\text{Wege der Länge } k \text{ von } C \text{ nach } D\}| = \sum_{j=m-1}^{m+1} a_{k-1,j} B_j^{(m)}$$

mit $a_{k,m} = 0$ für $k < m$, $a_{0,0} := 1$ und $B_j^{(m)} := |\{E \in \mathcal{F} : E \sim_j C \wedge E \sim_1 D\}|$. Für negative Werte von k oder m ergänzt man $a_{k,m} := 0$.

Beweis:
Man kann die Wege der Länge k von C nach D, $C \sim_1 C_1 \sim_1 \cdots \sim_1 C_{k-1} \sim_1 D$ als Wege der Länge k-1 bis zu C_{k-1} betrachten. Die möglichen C_{k-1} kann man dann in 3 Klassen unterteilen nämlich die mit Abstand m-1 zu C, mit Abstand m zu C und mit Abstand m+1 zu C. Andere Fälle sind nicht möglich, da $d(C, C_{k-1}) > m + 1$ im Widerspruch zu $C \sim_m D \sim_1 C_{k-1}$ steht und $d(C, C_{k-1}) < m - 1$ zu einen Weg einer Länge kleiner m von C nach D führen würde und somit zu einem Widerspruch zu $C \sim_m D$.

q.e.d.

3.2.2 Definition

1. *Für $m \geq 1$ bezeichne β_m die Anzahl der (m-1)-dimensionalen Teilräume in einem m-dimensionalen Vektorraum über $\mathbb{F}_q$, wobei $\beta_0 := 0$. Also $\beta_m = \frac{q^m - 1}{q - 1}$.*

2. *Sei $\mathcal{F}$ eine Familie von n-dimensionalen Codes und F ein (n-m)-dimensionaler Teilraum von $\mathbb{F}_q^N$ für den es $C \sim_m D \in \mathcal{F}$ gibt, so dass $F = C \cap D$. Dann ist*

$$\gamma_{n-m}(\mathcal{F}) := |\{M \leq F : \dim(M) = n - m - 1, \exists\, E \sim_{m-1} C \in \mathcal{F} \text{ so dass } C \cap E = M\}|$$

3. *Zu einer Familie von Codes $\mathcal{F}$ definiert man,*

$$\alpha(\mathcal{F}) := |\{C_i \in \mathcal{F} : C_i \cap C = F \text{ für festes } F \text{ mit } F = C \cap D, C \sim_1 D\}|$$

3.2.3 Satz
Seien C und D wie oben und $B_{m-1}^{(m)}$ die Anzahl der $E \in \mathcal{F}$ mit $E \sim_{m-1} C$ und $E \sim_1 D$. Dann ist

$$B_{m-1}^{(m)} = \beta_m$$

.

Beweis:
Nach Vorraussetzung liegt E auf einem kürzesten Weg von C nach D. Also gibt es nach Konstruktion 3.1.4 mindestens soviele E wie es $(n-m+1)$-dimensionale Teilräume von D gibt, die $C \cap D$ enthalten, also gerade die eindimensionalen Teilräume in $D/(C \cap D)$, und das sind genau β_m.
Angenommen, es gäbe ein $E \in \mathcal{F}$ mit $X = E \cap C$ und $E \neq (D+X)^\perp + X$: da

$$\begin{aligned} & X \not\leq D \quad \wedge \quad X \leq E \\ \Rightarrow & \dim(D \cap X) = n - (m-1) - 1 = n - m \end{aligned}$$

und mit

$$\begin{aligned} & X \leq C \wedge \dim(D \cap C) = n - m \\ & \Rightarrow X \cap D = C \cap D. \end{aligned}$$

Genau wie in 3.1.4 ergibt sich:

$$\begin{aligned} & (D+X)^\perp + X \sim_1 D \\ & \text{mit } D \cap (D+X)^\perp + X = (D+X)^\perp. \end{aligned}$$

Da $E = E^\perp \leq X^\perp$

$$(D+X)^\perp \cap E = D \cap X^\perp \cap E = D \cap E$$

aus Dimensionsgründen folgt nun:

$$\begin{aligned} & (D+X)^\perp = D \cap E \\ & \Rightarrow (D+X)^\perp \leq E \wedge X \leq E \\ & \Rightarrow (D+X)^\perp + X \leq E \end{aligned}$$

Da aber:

$$\begin{aligned} & \dim((D+X)^\perp + X) = n = \dim(E) \\ & \Rightarrow E = (D+X)^\perp + X, \end{aligned}$$

was im Widerspruch zur Annahme steht.

q.e.d.

3.2.4 Satz
Seien C, D und $B_j^{(m)}$ wie oben und $m \geq 2$, dann ist $B_m^{(m)} = \beta_m(\alpha(\mathcal{F}) - 1)$.

Beweis:
Betrachten wir nun alle Möglichkeiten für $E \in \mathcal{F}$ mit $\dim(E \cap C) = n - m$ und $\dim(D \cap E) = n - 1$.
Für $\dim(C \cap E + D \cap E)$ gibt es dann zwei Möglichkeiten:

Fall 1: $C \cap D \cap E = C \cap D$
In diesem Fall ist $\dim(C \cap E + D \cap E) = n - 1$, also gilt:

$$C \cap E + D \cap E = D \cap E.$$

Dann gibt es für $F = E \cap D$ genau soviele Möglichkeiten wie es (m-1)-Dimensionale Teilräume in $D/(C \cap D)$ gibt, also β_m und für festes F gibt es dann noch $\alpha(\mathcal{F}) - 1$ Möglichkeiten einen Nachbarn E von D auszusuchen, der nicht auf einem kürzesten Weg von C nach D liegt auszusuchen.
Was für den ersten Fall zu $\beta_m \alpha(\mathcal{F})$ Nachbarn mit den geforderten Eigenschaften führt.

Fall 2: $C \cap D \cap E < C \cap D$
Dann ist $\dim(C \cap D \cap E) = n - m - 1$ und es folgt

$$\begin{aligned}\dim((C \cap E) + (D \cap E)) &= \dim(C \cap E) + \dim(D \cap E) - \dim(C \cap D \cap E) \\ &= n - m + n - 1 - (n - m - 1) = n.\end{aligned}$$

Also benötigen wir einen (n-1)-dimensionalen Teilraum $X \leq D$ der $C \cap D$ nicht enthält, um zu diesem dann einen 1-Nachbarn E von D zu konstruieren, der folgende Eigenschaften hat: $X \leq E \leq X^\perp$ und $\dim(E \cap C) = n - m$.
Da aber

$$X^\perp \cap C = C \cap D \subset D$$

und damit

$$E \cap C \subseteq C \cap D,$$

woraus aus Dimensionsgründen

$$E \cap C = C \cap D$$

folgt. Dies führt aber zu $\dim(C \cap D \cap E) = n - m$ was im Widerspruch zur Annahme steht.

Insgesammt ergibt sich:

$$B_m^{(m)} = \beta_m(\alpha(\mathcal{F}) - 1)$$

q.e.d.

3.2.5 Satz
Seien C, D und $B_j^{(m)}$ *wie oben, dann gilt*

$$B_{m+1}^{(m)} = \gamma_{n-m}(\mathcal{F})(\beta_{m+1} - \beta_m)\alpha(\mathcal{F}).$$

Beweis:
Sei $E \in \mathcal{F}$ mit $C \sim_{m+1} E \sim_1 D$ dann gilt

$$\dim(C \cap E) = n - m - 1 = \dim(C \cap D \cap E),$$

D liegt also auf einem kürzesten Weg von C nach E. Es folgt

$$\dim((C \cap E) + (D \cap E)) = n - m - 1 + n - 1 - (n - m - 1) = n - 1$$

und deswegen

$$(C \cap E) + (D \cap E) = D \cap E.$$

Für $C \cap D \cap E = C \cap E \leq C \cap D$ gibt es $\gamma_{n-m}(\mathcal{F})$ Wahlmöglichkeiten. $D \cap E$ entspricht den m-dimensionalen Teilräumen von $D/(C \cap D \cap E)$ die $D \cap C/(C \cap D \cap E)$ nicht enthalten, von solchen extistieren

$$\beta_{m+1} - \beta_m = q^m.$$

Dannnach bleiben nur noch $\alpha(\mathcal{F})$ Möglichkeiten für E, als Nachbarn von D über dem festgewählten Teilraum.
Insgesamt folgt also:

$$B_{m+1}^{(m)} = \gamma_{n-m}(\mathcal{F})q^m\alpha(\mathcal{F})$$

q.e.d.

Wenn man die Ergebnisse zusammenfügt erhält man für:

$$\begin{aligned} a_{k,m} &= a_{k-1,m-1}B_{m-1}^{(m)} + a_{k-1,m}B_m^{(m)} + a_{k-1,m+1}B_{m+1}^{(m)} \\ &= \beta_m a_{k-1,m-1} + \beta_m(\alpha(\mathcal{F}) - 1)a_{k-1,m} \\ &+ \gamma_{n-m}(\mathcal{F})(\beta_{m+1} - \beta_m)\alpha(\mathcal{F})a_{k-1,m+1}. \end{aligned}$$

3.3 $\alpha(\mathcal{F})$ und $\gamma_{n-m}(\mathcal{F})$ für verschiedene Typen von Codes

Da $\alpha(\mathcal{F})$ und $\gamma_{n-m}(\mathcal{F})$ vom Typ der Codes abhängen, werden wir sie nun für die klassischen Typen berechnen.

3.3.1 Euklidische selbstduale Codes über Körpern mit gerader Charakteristik

3.3.1 Satz
Sei $\mathbb{F}_q$, mit $q = 2^f, f \in \mathbb{N}$ ein Körper mit gerader Charakteristik und $\mathcal{F}$ eine Familie von selbstdualen Codes $C = C^\perp$ der Länge N über $\mathbb{F}_q$, mit $b(v,w) = \sum_{i=1}^{N} v_i w_i$ als euklidischer Bilinearform. Dann ist:

- $\alpha(\mathcal{F}) = q$
- $\gamma_{n-m}(\mathcal{F}) = \beta_{n-m-1}$.

Beweis:
Seien $C \sim_1 D \in \mathcal{F}$ mit $C \cap D = F$. Alle Codes E aus $\mathcal{F}$, für die $C \cap E = F$ gilt, entsprechen den 1-dimensionalen selbstdualen Teilräumen von $F^\perp/F$. Da $\mathbf{1} := (1, \ldots, 1) \in \mathbb{F}_q^N$ in jedem Code aus $\mathcal{F}$ enthalten ist, ist $\mathbf{1}$ auch in F enthalten und somit gilt für alle Elemente $c = (c_1, \ldots, c_N) \in F^\perp$:

$$0 = b(c,1) = \sum_{i=1}^{N} c_i = \sum_{i=1}^{N} c_i^2 = b(c,c),$$

da $\mathbb{F}_q$ Charakteristik 2 hat. Also sind alle $q+1$ eindimensionalen Teilräume von $F^\perp/F$ selbstdual und C hat q Nachbarn über F für alle $F \leq C$ mit $\dim(F) = n-1$ und $\mathbf{1} \in F$.
Um den zweiten Teil der Behauptung zu zeigen, betrachtet man $C \sim_m D$ mit $C \cap D = E$ und einen beliebigen n-1-dimensionalen Teilraum X von D der $\mathbf{1}$ enthält aber nicht E.
Da

$$X^\perp \cap C = C \cap D \subset D$$

(aus Dimensionsgründen) gibt es noch $\alpha(\mathcal{F})$ Nachbarn $D' \sim_1 D$ mit

$$D' \cap C = X \cap E.$$

Jeder beliebige (n-m-1)-dimensionale Teilraum von E der $\mathbf{1}$ enthält, liefert also einen (m+1)-Nachbarn D' von C. Diese (n-m-1)-dimensionalen Teilräume $\langle \mathbf{1} \rangle \leq F \leq E$ entsprechen geraden den (n-m-2)-dimensionalen Teilräumen von $E/\langle \mathbf{1} \rangle$, und somit gibt es β_{n-m-1} solche Teilräume. q.e.d.

3.3.2 Doppeltgerade Codes über $\mathbb{F}_2$

3.3.2 Satz
Sei $\mathcal{F}$ die Familie der doppeltgeraden selbstdualen Codes der Länge N über $\mathbb{F}_2$, d.h. für $C \in \mathcal{F}$ und $c \in C$ gilt, dass $wt(c)$ durch 4 teilbar ist. Die Bilinearform b sei definiert wie oben. Dann gilt:

- $\alpha(\mathcal{F}) = 1$
- $\gamma_{n-m}(\mathcal{F}) = \beta_{n-m-1}$.

Beweis:
Analog zu 3.3.1 folgt, dass für alle $F = C \cap D$ mit $C, D \in \mathcal{F}$ und $\dim(F) = n-1$ $F^\perp/F$ $q+1 = 3$ selbstorthogonale eindimensionale Teilräume hat. Wählen wir nun 3 Erzeuger b_1, b_2, b_3, so dass $C = \langle b_1 \rangle + F$, dann ist $b_3 = b_1 + b_2$, da $F^\perp/F$ 2-dimensional ist und $q = 2$. Da $F^\perp/F$ mit der durch b induzierten, nicht ausgearteten quadratischen Form ein quadratischer Raum über $\mathbb{F}_2$ ist der mit C/F einen maximalen totalisotropen Teilraum enthält, folgt, dass $F^\perp/F$ hyperbolisch ist und die Grammatrix zu b über $F^\perp/F$ bezüglich (b_1, b_2) folglich gleich $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ sein muss (siehe auch [Kne02]). Also gilt:

$$\begin{aligned} \mathrm{wt}(b_3) &= \mathrm{wt}(b_1 + b_2) \\ &= \mathrm{wt}(b_1) + \mathrm{wt}(b_2) - 2b(b_1, b_2) \\ &= \mathrm{wt}(b_1) + \mathrm{wt}(b_2) - 2 \\ &\equiv_4 2. \end{aligned}$$

somit ist das Gewicht von b_3 nicht durch 4 teilbar folglich ist $F + \langle b_3 \rangle \notin \mathcal{F}$, und C und D sind die einzigen Codes in $\mathcal{F}$, die über F liegen. Daraus folgt auch, dass alle $F \leq C$ mit $\dim(F) = n-1$ und $\mathbf{1} \in F$ als Schnitt von C mit einem anderen Code aus $\mathcal{F}$ vorkommen.
Der zweite Teil der Behauptung folgt analog zu 3.3.1.

q.e.d.

3.3.3 Euklidische selbstduale Codes über Körpern mit ungerader Charakteristik

3.3.3 Satz
Sei $\mathbb{F}_q$ mit $q = p^f, f \in \mathbb{N}$ und p ungerade Primzahl, $\mathcal{F}$ eine Familie von selbstdualen Codes der Länge N über $\mathbb{F}_q$ mit der obigen Bilinearform, so gilt:

- $\alpha(\mathcal{F}) = 1$
- $\gamma_{n-m}(\mathcal{F}) = \beta_{n-m}$.

Beweis:
Sei $F \leq C$ ein eindimensionaler Teilraum von C.

Alle von C verschiedenen Codes $D \in \mathcal{F}$, die F enthalten, sind selbstduale Räume mit $F \leq D \leq F^\perp$, und entsprechen damit eindimensionalen Teilräumen von $F^\perp/F$ $\langle d \rangle + F$ die selbstorthogonal sind. Auch C kann man analog schreiben als $C = F + \langle c \rangle$ mit $c \in F^\perp$ selbstorthogonal. $F^\perp/C$ ist eindimensional, also kann man $C + \langle e \rangle = F^\perp$ schreiben für ein $e \in F^\perp$, das nicht in C liegt. Mit $\langle e \rangle + F$ liefert auch $\langle e + ac \rangle + F$ für alle $a \in \mathbb{F}_q^*$ eindimensionale Teilräume von $F^\perp/F$. $\langle e + ac \rangle + F$ mit $a \in \mathbb{F}_q$ und $\langle c \rangle + F$ liefert alle $q + 1 = \frac{q^2-1}{q-1}$ eindimensionalen Teilräume von $F^\perp/F$. Betrachte nun:

$$b(e + ac + F, e + ac + F) = b(e, e) + 2ab(e, c) = 0$$
$$\Leftrightarrow a = \frac{b(e, e)}{2b(e, c)} \text{ da } b(e, c) \neq 0, \text{ weil } e \notin C^\perp = C$$

Es gibt also ein eindeutiges $a \in \mathbb{F}_q$ so dass $(e + ac) + F$ selbstorthogonal und damit aus Dimensionsgründen selbstdual ist und damit genau einen selbstdualen Code $D \neq C$. Somit folgt der erste Teil der Behauptung.
Um den zweiten Teil der Behauptung zu zeigen, betrachte $C, D \in \mathcal{F}$ m-Nachbarn mit $E := C \cap D$. Wähle nun einen beliebigen (n-1)-dimensionalen Teilraum X von D der E nicht enthält, somit liefert X durch $E \cap X$ mit $\dim(E \cap X) = \dim(E) - 1 = n - m - 1$ einen beliebigen (n-m-1)-dimensionalen Teilraum von E. Da $\dim(X^\perp \cap C) = n - m$ gilt und somit

$$X^\perp \cap C = C \cap D \subset D,$$

ist D der einzige Code über X in $\mathcal{F}$, dessen Schnitt mit C größer ist als $E \cap X$. D.h. es gibt einen 1-Nachbarn D' von D mit $D' \cap C = E \cap X$. q.e.d.

3.3.4 Euklidische selbstduale Codes in ungerader Charakteristik die 1 enthalten

3.3.4 Satz
Sei $\mathbb{F}_q$ mit $q = p^f, f \in N$ und p ungerade Primzahl, $\mathbf{1} := (1, \ldots, 1) \in \mathbb{F}_q^N$, $\mathcal{F}$ eine Familie von selbstdualen Codes der Länge N über $\mathbb{F}_q$ mit $\mathbf{1} \in C \, \forall \, C \in \mathcal{F}$ und der obigen Bilinearform, so ist:

- $\alpha(\mathcal{F}) = 1$
- $\gamma_{n-m}(\mathcal{F}) = \beta_{n-m-1}$.

Beweis:
Der Beweis ist analog zum Beweis von 3.3.3 bzw. 3.3.1.

3.3.5 Bemerkung
Die Länge N der Codes muss durch die Charakteristik p von $\mathbb{F}_q$ teilbar sein, damit $b(\mathbf{1}, \mathbf{1}) = 0$ und $\mathbf{1}$ in einem selbstdualen Code enthalten sein kann.

3.3.5 Hermitesche selbstduale Codes

Sei $\mathbb{F}_q$ mit $q = r^2$ und r eine Primpotenz. Sei b die hermitesche Form bezüglich des nicht trivialen Galoisautomorphismus $^- : a \mapsto a^r$ von $\mathbb{F}_q$ über $\mathbb{F}_r$ und damit

$$C^\perp = \{v \in \mathbb{F}_q^N : \sum_{i=1}^{N} c_i \bar{v_i} \, \forall \, c \in C\}.$$

3.3.6 Satz
Sei $\mathcal{F}$ die Familie der selbstdualen Codes der Länge N über $\mathbb{F}_q$ mit der hermiteschen Form b, so gilt:

- $\alpha(\mathcal{F}) = r = \sqrt{q}$
- $\gamma_{n-m}(\mathcal{F}) = \beta_{n-m}$.

Beweis:
Sei $E \leq C$ ein (n-1)-dimensionaler selbstorthogonaler Teilraum von $\mathbb{F}_q^N$. Dann ist $E^\perp/E$ ein nichtausgearteter hermitescher Raum über $\mathbb{F}_q$ und deswegen isometrisch zu $\mathbb{F}_q^2$ mit der hermiteschen Form $((x_1, x_2), (y_1, y_2)) = x_1\bar{y_1} + x_2\bar{y_2}$. Die selbstdualen Codes, die E enthalten, entsprechen also gerade den eindimensionalen selbstorthogonalen Teilräumen von $E^\perp/E$ und wegen der angegebenen Isometrie gerade den eindimensionalen selbstorthogonalen Teilräumen von $\mathbb{F}_q^2$:

$$\langle x \rangle \leq \langle x \rangle^\perp \Leftrightarrow ((x_1, x_2), (x_1, x_2)) = x_1^{r+1} + x_2^{r+1} = 0$$

$(1, -1)$ ist ein solches Element von $\mathbb{F}_q^2$. Da $(r + 1) \mid |\mathbb{F}_q^*| = q - 1$, existiert genau eine zyklische Untergruppe von $\mathbb{F}_q^*$ mit der Ordnung r+1 und somit gibt es genau r von 1 verschiedene Elemente $x \in \mathbb{F}_q$ mit $x^{r+1} = 1$ und $((x, -1)(x, -1)) = 0$. Die dadurch gegebenen Elemente erzeugen r+1 selbstorthogonale Teilräume von denen einer C entspricht und die anderen r Teilräume zu r weiteren selbstdualen Codes führen.
Die zweite Behauptung folgt analog zu 3.3.3.

q.e.d.

3.3.6 Hermitesche selbstduale Codes die 1 enthalten

3.3.7 Satz
Sei $\mathcal{F}$ die Familie der selbstdualen Codes der Länge N mit $\mathbf{1} \in C \, \forall \, C \in \mathcal{F}$ über $\mathbb{F}_q$ mit der hermiteschen Form b, so gilt:

- $\alpha(\mathcal{F}) = r = \sqrt{q}$

- $\gamma_{n-m}(\mathcal{F}) = \beta_{n-m-1}$.

Beweis:
Die Behauptungen folgen analog zu 3.3.6 und 3.3.1.

3.3.8 Bemerkung
Auch hier muss die Länge N der Codes durch die Charakteristik p von $\mathbb{F}_q$ teilbar sein, damit $b(\mathbf{1}, \mathbf{1}) = 0$ und somit $\mathbf{1}$ in einem selbstdualen Code enthalten sein kann.

3.4 Der polynomiale Zusammenhang zwischen den Adjazenzmatrizen

Wie wir in 2.4.3 gezeigt haben, enthält die r-te Potenz der Adjazenzmatrix die Anzahlen der Wege der Länge r von der i-ten zur j-ten Ecke, wenn wir dies auf den Nachbarschaftsgraphen anwenden, dann können wir die Wege nach der Nachbarschaftsbeziehung der Endpunkte aufteilen, also in Wege der Länge r von C_i nach C_j mit $C_i \sim_k C_j$. Da die Anzahl der Wege der Länge r a_{nk} (siehe Satz 3.2.1) für die in Abschnitt 3.3 behandelten Familien von Codes von klassischem Typ unabhängig von der konkreten Wahl von C_i bzw. C_j ist kann man folgende Gleichung für die r-te Potenz der Adjazenzmatrix des 1-Nachbarschaftsgraphen A_1^r:

$$A_1^r = \sum_{k=0}^{r} a_{rk} A_k \qquad 0 \leq r \leq n, \tag{3.3}$$

wobei $A_{(0)}$ die Einheitsmatrix ist und $\sim_0$ so definiert ist, dass jeder Code aus $\mathcal{F}$ genau sein eigener „nullter Nachbar“ ist.

3.4.1 Satz
Sei $(b_{ij})_{0\leq i,j\leq n} := ((a_{ij})_{0\leq i,j\leq n})^{-1}$, dann gilt:

$$A_i = \sum_{k=0}^{i} b_{ik} A_1^k \tag{3.4}$$

für $0 \leq i \leq n$.

Beweis:
Schreibt man die n Gleichungen 3.3 in Matrixschreibweise, dann erhält man einen untere $(n+1) \times (n+1)$-Dreiecksmatrix $(a_{ij})_{0\leq i,j\leq n}$ für die wegen Satz

3.1.4 $a_{ii} \neq 0$ für alle $0 \leq i \leq n$ gilt und somit ist $(a_{ij})_{0\leq i,j\leq n}$ invertierbar. Also kann man 3.3 folgendermaßen umformen:

$$\begin{pmatrix} a_{00} & \dots & 0 \\ \vdots & \ddots & \vdots \\ a_{n0} & \dots & a_{nn} \end{pmatrix} \begin{pmatrix} A_0 \\ A_1 \\ \vdots \\ A_n \end{pmatrix} = \begin{pmatrix} A_1^0 \\ A_1^1 \\ \vdots \\ A_1^n \end{pmatrix}$$

$$\Leftrightarrow \begin{pmatrix} A_0 \\ A_1 \\ \vdots \\ A_n \end{pmatrix} = \begin{pmatrix} a_{00} & \dots & 0 \\ \vdots & \ddots & \vdots \\ a_{n0} & \dots & a_{nn} \end{pmatrix}^{-1} \begin{pmatrix} A_1^0 \\ A_1^1 \\ \vdots \\ A_1^n \end{pmatrix} = \begin{pmatrix} b_{00} & \dots & 0 \\ \vdots & \ddots & \vdots \\ b_{n0} & \dots & b_{nn} \end{pmatrix} \begin{pmatrix} A_1^0 \\ A_1^1 \\ \vdots \\ A_1^n \end{pmatrix}$$

Da das Inverse einer Unteren Dreicksmatrix wieder einen untere Dreiecksmatrix ergeben sich direkt die n Gleichungen aus 3.4. q.e.d.

3.5 T_k als Polynom in T_1

Nun kann man wie in 3.2 angekündigt von den Adjazenzmatrizen auf die Kneser-Hecke-Operatoren übergehen und erhält:

3.5.1 Hauptsatz
Sei T_k der k-te Kneser-Hecke-Operator zu einer Familie von Codes von einem in 3.3 aufgeführten Typ, dann gilt mit den in 3.4.1 definierten b_{ki}:

$$T_k = \sum_{i=0}^{k} b_{ki} T_1^i$$

Beweis:
folgt direkt aus 3.4.1 und 3.1.3. q.e.d.

3.5.2 Korollar
Mit den Vorraussetzungen aus Satz 3.5.1 und ν_m für $0 \leq m \leq \dim(\mathcal{V})$ wie in 2.3.5 gilt:

$$\lambda_m := \sum_{k=0}^{i} b_{ik} \nu_m^k \quad \forall\, 1 \leq m \leq \dim(\mathcal{V}),$$

sind die Eigenwerte von T_i und die T_i sind für alle $i \in \mathbb{N}$ simultan diagonalisierbar.

Kapitel 4

Beispiele

4.1 Euklidische selbstduale Codes über Körpern mit gerader Charakteristik

Sei $\mathcal{F}$ die Familie der selbstdualen Codes von Länge 8 über $\mathbb{F}_2$, dann zerfällt $\mathcal{F}$ in 2 Äquivalenzklassen von Codes e_8 und dem zweifachen Wiederholungscode von Dimension 4 i_2^4. Der erste Hecke-Operator in dieser Basis laute

$$T_1 = \begin{pmatrix} 7 & 7 \\ 2 & 12 \end{pmatrix}$$

Für T_2, T_3 und T_4 ergeben sich dann folgende Polynome in T_1:

	T_2	T_3	T_4
I	$\frac{-14}{3}$	2	$\frac{14}{9}$
T_1	$\frac{-1}{3}$	$\frac{-47}{21}$	$\frac{61}{45}$
T_1^2	$\frac{1}{3}$	$\frac{-4}{21}$	$\frac{-5}{21}$
T_1^3	0	$\frac{1}{21}$	$\frac{-11}{315}$
T_1^4	0	0	$\frac{1}{315}$

Sei $\mathcal{F}$ die Familie der selbstdualen Codes von Länge 12 über $\mathbb{F}_2$, dann zerfällt $\mathcal{F}$ in 3 Äquivalenzklassen von Codes $(e_8 \perp i_2^2)$, d_{12}^+ und i_2^6. Der erste Hecke-Operator in dieser Basis laute

$$T_1 = \begin{pmatrix} 41 & 14 & 7 \\ 30 & 31 & 1 \\ 30 & 2 & 30 \end{pmatrix}$$

Für T_2 bis T_6 ergeben sich dann folgende Polynome in T_1:

	T_2	T_3	T_4	T_5	T_6
I	$\frac{-62}{3}$	$\frac{62}{7}$	$\frac{3286}{45}$	$\frac{-1030}{21}$	$\frac{-257114}{19845}$
T_1	$\frac{-1}{3}$	$\frac{-239}{21}$	$\frac{2251}{315}$	$\frac{161317}{9765}$	$\frac{-82933}{6615}$
T_1^2	$\frac{1}{3}$	$\frac{-4}{21}$	$\frac{-67}{35}$	$\frac{14176}{9765}$	$\frac{106679}{205065}$
T_1^3	0	$\frac{1}{21}$	$\frac{-11}{315}$	$\frac{-386}{3255}$	$\frac{60986}{615195}$
T_1^4	0	0	$\frac{1}{315}$	$\frac{-26}{9765}$	$\frac{-64}{29295}$
T_1^5	0	0	0	$\frac{1}{9765}$	$\frac{-19}{205065}$
T_1^6	0	0	0	0	$\frac{1}{615195}$

Sei $\mathcal{F}$ die Familie der selbstdualen Codes von Länge 12 über $\mathbb{F}_2$, dann zerfällt $\mathcal{F}$ in 4 Äquivalenzklassen von Codes mit folgenden Repräsentanten $(e_8 \perp i_2^3)$, $(d_{12}^+ \perp i_2)$, $(e_7 \perp e_7)^+$ und i_2^7. Der erste Hecke-Operator in dieser Basis laute

$$T_1 = \begin{pmatrix} 61 & 42 & 16 & 7 \\ 30 & 55 & 40 & 1 \\ 14 & 49 & 63 & 0 \\ 70 & 14 & 0 & 42 \end{pmatrix}$$

Für T_2 bis T_7 ergeben sich dann folgende Polynome in T_1:

	T_2	T_3	T_4	T_5	T_6	T_7
I	-42	18	$\frac{1638}{5}$	$\frac{-6930}{31}$	$\frac{-1946}{5}$	$\frac{6018138}{19685}$
T_1	$\frac{-1}{3}$	$\frac{-165}{7}$	$\frac{223}{15}$	$\frac{13723}{155}$	$\frac{-227093}{3255}$	$\frac{-257319}{19685}$
T_1^2	$\frac{1}{3}$	$\frac{-4}{21}$	$\frac{-1307}{315}$	$\frac{10336}{3255}$	$\frac{140479}{22785}$	$\frac{-717636}{137795}$
T_1^3	0	$\frac{1}{21}$	$\frac{-11}{315}$	$\frac{-2822}{9765}$	$\frac{151226}{615195}$	$\frac{69679}{964565}$
T_1^4	0	0	$\frac{1}{315}$	$\frac{-26}{9765}$	$\frac{-1664}{205065}$	$\frac{570554}{78129765}$
T_1^5	0	0	0	$\frac{1}{9765}$	$\frac{-19}{205065}$	$\frac{-1811}{26043255}$
T_1^6	0	0	0	0	$\frac{1}{615195}$	$\frac{-8}{5208651}$
T_1^7	0	0	0	0	0	$\frac{1}{78129765}$

Sei $\mathcal{F}$ die Familie der selbstdualen Codes von Länge 16 über $\mathbb{F}_2$, dann zerfällt $\mathcal{F}$ in 7 Äquivalenzklassen $(e_8 \perp i_2^4)$, $(d_{12}^+ \perp i_2^2)$, $(e_7 \perp e_7)^+ \perp i_2$, $(d_8 \perp d_8)^+$, i_2^8, $(e_8 \perp e_8)$ und d_{16}^+.

Der erste Hecke-Operator in dieser Basis laute

$$T_1 = \begin{pmatrix} 83 & 84 & 64 & 14 & 7 & 2 & 0 \\ 30 & 81 & 80 & 60 & 1 & 0 & 2 \\ 14 & 49 & 91 & 98 & 0 & 2 & 0 \\ 2 & 24 & 64 & 162 & 0 & 1 & 1 \\ 140 & 56 & 0 & 0 & 56 & 0 & 2 \\ 14 & 0 & 64 & 49 & 0 & 78 & 49 \\ 0 & 56 & 0 & 70 & 1 & 70 & 57 \end{pmatrix}$$

Für T_2 bis T_8 ergeben sich dann folgende Polynome in T_1:

	T_2	T_3	T_4	T_5	T_6	T_7	T_8
T_1^0	$\frac{-254}{3}$	$\frac{254}{7}$	$\frac{12446}{9}$	$\frac{-618490}{651}$	$\frac{-17659858}{3969}$	$\frac{1016542}{279}$	$\frac{2628169750}{6274989}$
T_1^1	$\frac{-1}{3}$	$\frac{-1007}{21}$	$\frac{9547}{315}$	$\frac{783521}{1953}$	$\frac{-65672491}{205065}$	$\frac{-37712527271}{78129765}$	$\frac{2606889557}{6274989}$
T_1^2	$\frac{1}{3}$	$\frac{-4}{21}$	$\frac{-181}{21}$	$\frac{64672}{9765}$	$\frac{6921911}{205065}$	$\frac{-762510388}{26043255}$	$\frac{-84763825091}{19923090075}$
T_1^3	0	$\frac{1}{21}$	$\frac{-11}{315}$	$\frac{-410}{651}$	$\frac{331706}{615195}$	$\frac{4950577}{5208651}$	$\frac{-3422118617}{3984618015}$
T_1^4	0	0	$\frac{1}{315}$	$\frac{-26}{9765}$	$\frac{-4096}{205065}$	$\frac{1420346}{78129765}$	$\frac{93628441}{19923090075}$
T_1^5	0	0	0	$\frac{1}{9765}$	$\frac{-19}{205065}$	$\frac{-6931}{26043255}$	$\frac{4987649}{19923090075}$
T_1^6	0	0	0	0	$\frac{1}{615195}$	$\frac{-8}{5208651}$	$\frac{-21809}{19923090075}$
T_1^7	0	0	0	0	0	$\frac{1}{78129765}$	$\frac{-247}{19923090075}$
T_1^8	0	0	0	0	0	0	$\frac{1}{19923090075}$

Die Koeffizienten wurden mit Hilfe des folgenden Magma-Programms [BCP97] berechnet:

```
//a berechnet rekursiv die Koeffizienten von (T_1)^k bei T_m in
//der, wobei n die Dimension der Codes bezeichnet.
function a(k,m,n)
        if [k,m] eq [0,0] then
                return 1;
        elif m le -1 then
                return 0;
```

```
        elif k le m-1 then
                return 0;
        else
                return ((2^m-1)*(a(k-1,m-1,n)+a(k-1,m,n))+
                        (2^(n-1-m)-1)*2^(m+1)*a(k-1,m+1,n));
        end if;
end function;

//A gibt die Koeffizienten der Polynome von T_1 bis T_{n-1} in
//Potenzen von T_1 spaltenweise wieder
function A(n)
        B:=[];
        for m in [0 .. n] do
                for k in [0 .. n] do
                        B:=Append(B,a(m,k,n));
                end for;
        end for;
        C:=Matrix(RationalField(), n+1, n+1, B);
        C:=Transpose(C);
        return(C ^-1);
end function;
```

A(n) liefert dann eine Matrix in deren Einträgen die Koeffizienten der Polynome der Familie von Typ 1 Codes in $\mathbb{F}_2^{2n}$.

4.2 Doppeltgerade Codes über $\mathbb{F}_2$

Sei $\mathcal{F}$ die Familie der selbstdualen doppeltgeraden Codes von Länge 16, dann zerfällt $\mathcal{F}$ in 2 Äquivalenzklassen von Codes mit folgenden Repräsentanten $(e_8 \perp e_8)$ und d_{16}^+. Der erste Hecke-Operator in dieser Basis laute

$$T_1 = \begin{pmatrix} 78 & 49 \\ 70 & 57 \end{pmatrix}$$

Für T_2 bis T_8 ergeben sich dann folgende Polynome in T_1:

	T_2	T_3	T_4	T_5	T_6	T_7	T_8
T_1^0	$\frac{-127}{3}$	0	$\frac{15748}{45}$	0	$\frac{-251968}{405}$	0	$\frac{16125952}{103275}$
T_1^1	0	$\frac{-505}{21}$	0	$\frac{1019236}{9765}$	0	$\frac{-187059392}{2232279}$	0
T_1^2	$\frac{1}{3}$	0	$\frac{-1373}{315}$	0	$\frac{1928764}{205065}$	0	$\frac{-53578060096}{19923090075}$
T_1^3	0	$\frac{1}{21}$	0	$\frac{-3173}{9765}$	0	$\frac{8325532}{26043255}$	0
T_1^4	0	0	$\frac{1}{315}$	0	$\frac{-443}{41013}$	0	$\frac{26329052}{6641030025}$
T_1^5	0	0	0	$\frac{1}{9765}$	0	$\frac{-4231}{26043255}$	0
T_1^6	0	0	0	0	$\frac{1}{615195}$	0	$\frac{-20821}{19923090075}$
T_1^7	0	0	0	0	0	$\frac{1}{78129765}$	0
T_1^8	0	0	0	0	0	0	$\frac{1}{19923090075}$

Sei $\mathcal{F}$ die Familie der selbstdualen doppeltgeraden Codes von Länge 24 über $\mathbb{F}_2$, dann zerfällt $\mathcal{F}$ in 9 Äquivalenzklassen von Codes mit folgenden Repräsentanten $(e_8 \perp e_8 \perp e_8)$, $(d_{16} \perp e_8)$, $(e_7^2 \perp d_{10})^+$, $(d_8^3)^+$, d_{24}^+, $(d_{12}^2)^+$, $(d_6^4)^+$, $(d_4^6)^+$ und g_{24}.

Der erste Hecke-Operator in dieser Basis laute

$$T_1 = \begin{pmatrix} 213 & 147 & 1344 & 343 & 0 & 0 & 0 & 0 & 0 \\ 70 & 192 & 896 & 490 & 7 & 392 & 0 & 0 & 0 \\ 10 & 14 & 504 & 490 & 0 & 49 & 980 & 0 & 0 \\ 1 & 3 & 192 & 447 & 0 & 36 & 1152 & 216 & 0 \\ 0 & 990 & 0 & 0 & 133 & 924 & 0 & 0 & 0 \\ 0 & 60 & 480 & 900 & 1 & 206 & 400 & 0 & 0 \\ 0 & 0 & 72 & 216 & 0 & 3 & 1108 & 648 & 0 \\ 0 & 0 & 0 & 45 & 0 & 0 & 720 & 1218 & 64 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1771 & 276 \end{pmatrix}$$

Für T_2 bis T_{12} ergeben sich dann folgende Polynome in T_1:

	T_2	T_3	T_4	T_5	T_6	T_7
T_1^0	$\frac{-2047}{3}$	0	$\frac{4184068}{45}$	0	$\frac{-1214575168}{405}$	0
T_1^1	0	$\frac{-8185}{21}$	0	$\frac{279749476}{9765}$	0	$\frac{-152552494400}{318897}$
T_1^2	$\frac{1}{3}$	0	$\frac{-22493}{315}$	0	$\frac{565542844}{205065}$	0
T_1^3	0	$\frac{1}{21}$	0	$\frac{-53093}{9765}$	0	$\frac{2813288092}{26043255}$
T_1^4	0	0	$\frac{1}{315}$	0	$\frac{-7739}{41013}$	0
T_1^5	0	0	0	$\frac{1}{9765}$	0	$\frac{-81031}{26043255}$
T_1^6	0	0	0	0	$\frac{1}{615195}$	0
T_1^7	0	0	0	0	0	$\frac{1}{78129765}$
T_1^8	0	0	0	0	0	0
T_1^9	0	0	0	0	0	0
T_1^{10}	0	0	0	0	0	0
T_1^{11}	0	0	0	0	0	0
T_1^{12}	0	0	0	0	0	0

	T_8	T_9	T_{10}	T_{11}	T_{12}
T_1^0	$\frac{2409717133312}{103275}$	0	$\frac{-1392971968675 84}{3408075}$	0	$\frac{2037718994177 2288}{1993723875}$
T_1^1	0	$\frac{5470508037786 4192}{29681338275}$	0	$\frac{-5625850535740 24134656}{401000816362905}$	0
T_1^2	$\frac{-4648714590789 76}{19923090075}$	0	$\frac{9070453389912 9532832}{212548063387275}$	0	$\frac{-6541078702139 75805997875 2}{5938922340538 71377625}$
T_1^3	0	$\frac{-4597029008608 576}{10180699028325}$	0	$\frac{7667892614144 631197696}{213192084019338 44325}$	0
T_1^4	$\frac{1256318985 2}{6641030025}$	0	$\frac{-3910982012587 2448}{104148551059764 75}$	0	$\frac{1752631117398 8151296}{1706787065609 3664225}$
T_1^5	0	$\frac{5223596745 2}{3393566342775}$	0	$\frac{-2853493349191 21216}{213192084019338 44325}$	0
T_1^6	$\frac{-70723}{2846155725}$	0	$\frac{6100412007 88}{104148551059764 75}$	0	$\frac{-3128147554088 94016}{1746043168118 38185021 75}$
T_1^7	0	$\frac{-984661}{10180699028325}$	0	$\frac{2157266600596}{213192084019338 44325}$	0
T_1^8	$\frac{1}{19923090075}$	0	$\frac{-1900373}{104148551059764 75}$	0	$\frac{4093794437 56}{5820143893727 939500725}$
T_1^9	0	$\frac{1}{10180699028325}$	0	$\frac{-3471701}{213192084019338 44325}$	0
T_1^{10}	0	0	$\frac{1}{104148551059764 75}$	0	$\frac{-1855943}{2910071946863969 7503625}$
T_1^{11}	0	0	0	$\frac{1}{213192084019338 44325}$	0
T_1^{12}	0	0	0	0	$\frac{1}{8730215840591909 2510875}$

Sei $\mathcal{F}$ die Familie der selbstdualen doppeltgeraden Codes von Länge 32 über $\mathbb{F}_2$, dann zerfällt $\mathcal{F}$ in 85 Äquivalenzklassen von Codes die in [CPS92] klassifiziert werden. Der erste Kneser-Hecke-Operator in der in [CPS92] angegebenen Basis laute:

241	3640	16016	0	12870	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	332	924	3520	0	990	6930	12672	0	924	6468	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	30	362	400	90	0	2700	2880	4800	420	420	12600	0	0	0	3024	5040	0	0	0	0	0	0	0	0	0	0	0
0	14	49	388	0	18	882	1008	3528	0	0	0	2520	8232	0	0	0	252	3528	12348	0	0	0	0	0	0	0	0
1	0	112	0	370	140	140	3584	0	0	3136	7840	0	0	0	0	12544	0	0	0	0	0	0	0	0	0	0	0
0	14	0	64	49	391	49	1792	0	784	0	2744	3584	0	0	0	0	1792	12544	0	0	0	0	70	980	0	0	0
0	2	24	64	1	1	475	256	1536	0	112	1400	0	3584	2016	0	0	0	1792	1792	10752	0	0	0	140	0	0	0
0	1	7	20	7	10	70	592	140	14	98	980	280	1960	0	294	294	70	1820	3430	5880	0	0	0	0	0	0	0
0	0	3	18	0	0	108	36	640	0	0	252	42	1526	1512	0	126	0	0	756	5292	4536	0	0	0	70	0	0
0	1	14	0	0	60	0	192	0	405	427	420	640	0	0	1008	0	480	5760	3360	0	0	0	0	900	400	0	0
0	1	2	0	12	0	60	192	0	61	411	780	320	320	0	144	864	0	960	5760	2880	0	0	0	0	0	0	0
0	0	2	0	1	1	25	64	64	2	26	584	64	448	72	48	192	0	192	768	3840	864	0	0	30	0	0	0
0	0	0	15	0	6	0	84	49	14	49	294	439	343	0	0	0	54	1596	1176	3528	0	0	0	0	0	0	0
0	0	0	3	0	0	18	36	109	0	3	126	21	761	216	0	0	0	72	522	2808	2592	0	0	0	30	0	0
0	0	0	0	0	0	15	0	160	0	0	30	0	320	768	0	0	0	0	0	1440	4080	384	0	0	0	30	0
0	0	3	0	0	0	0	120	0	30	30	300	0	0	0	424	60	0	1200	2400	1200	0	0	0	0	0	0	0
0	0	1	0	2	0	0	24	40	0	36	240	0	0	0	12	512	20	520	740	1920	0	0	0	0	0	0	0
0	0	0	7	0	14	0	98	0	49	0	0	252	0	0	0	343	719	1862	343	0	0	0	10	490	980	0	0
0	0	0	1	0	1	7	26	0	6	7	42	76	56	0	42	91	19	658	651	924	0	0	0	10	0	0	0
0	0	0	1	0	0	2	14	12	1	12	48	16	116	0	24	37	1	186	757	1044	216	0	0	10	0	0	0
0	0	0	0	0	0	2	4	14	0	1	40	8	104	36	2	16	0	44	174	1270	612	0	0	0	10	0	0
0	0	0	0	0	0	0	0	12	0	0	9	0	96	102	0	0	0	0	36	612	1356	64	0	0	0	10	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	231	0	0	0	0	0	0	1540	516	0	0	0	0	10
0	0	0	0	0	294	0	0	0	0	0	0	0	0	0	0	0	5376	0	0	0	0	0	412	1372	0	0	0
0	0	0	0	0	3	21	0	0	36	0	252	0	0	0	0	0	192	384	1344	0	0	0	1	646	1152	216	0
0	0	0	0	0	0	0	0	28	3	0	0	0	168	0	0	0	72	0	0	1512	0	0	0	216	1307	648	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	126	0	0	0	0	0	0	1680	0	0	45	720	1417	64
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1932	0	0	0	1771	475
0	0	0	0	3	0	0	0	0	0	0	144	0	0	0	0	384	0	0	0	0	0	0	1	4	0	0	0
0	0	0	0	0	2	4	0	0	0	48	48	0	0	0	0	0	0	512	256	0	0	0	0	4	0	0	0
0	0	0	0	0	0	3	0	0	3	3	78	0	0	0	16	0	0	192	192	192	0	0	0	3	0	0	0
0	0	0	0	0	1	0	28	0	0	0	49	24	0	0	0	0	34	588	98	0	0	0	1	14	0	0	0
0	0	0	0	0	0	1	4	0	0	0	25	0	24	0	12	12	2	60	178	192	0	0	0	2	0	0	0
0	0	0	0	0	0	1	0	0	0	4	16	0	0	24	0	32	0	0	128	256	0	0	0	4	0	0	0
0	0	0	0	0	0	0	2	7	1	0	14	14	0	0	0	7	6	148	112	168	0	0	0	12	8	0	0
0	0	0	0	0	0	0	0	4	1	2	0	24	0	0	0	24	0	48	168	72	0	0	0	0	1	0	0
0	0	0	0	0	0	0	2	1	0	1	8	1	13	0	0	13	1	34	75	168	0	0	0	0	1	0	0
0	0	0	0	0	0	0	0	2	0	0	3	2	14	0	2	0	0	20	58	162	36	0	0	1	1	0	0
0	0	0	0	0	0	0	0	1	0	0	3	0	6	6	0	3	0	6	30	138	84	0	0	0	2	0	0
0	0	0	0	0	0	0	0	0	0	0	12	0	0	6	0	0	0	0	0	192	48	0	0	1	0	1	0
0	0	0	0	0	0	0	0	0	0	0	0	0	8	4	0	0	0	0	12	108	132	0	0	0	1	1	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	0	0	0	0	0	72	176	16	0	0	0	2	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	240	36	0	0	0	1	1
0	0	0	0	0	0	0	0	0	0	0	0	294	0	0	0	0	84	0	0	0	0	0	4	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	45	49	0	0	0	36	252	0	0	0	0	0	0	14	0	0
0	0	0	0	0	0	0	0	0	0	0	0	3	21	0	0	0	3	42	21	126	0	0	0	4	18	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	7	0	0	0	12	0	84	42	0	0	3	16	6	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	84	0	0	0	9	16	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	21	0	0	0	21	4
0	0	0	0	0	0	0	0	0	0	0	0	5	5	0	0	0	0	60	60	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	12	0	0	0	72	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	2	4	0	0	0	0	8	52	24	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	6	0	0	0	0	0	0	0	0	72	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	1	3	0	6	3	45	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	6	6	42	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	4	8	24	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	4	0	0	0	16	12	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	6	12	12	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	12	12	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	12	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	9	3	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	8	4	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	6	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	1	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4900	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	3430	0	4480	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	140	1680	0	4480	2520	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	700	4900	0	1400	0	9800	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	1260	210	1260	7560	7560	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	6300	0	0	0	9600	2800	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	900	900	0	0	5400	0	800	9600	0	0	0	0	0	0	0	0	0	0	0	0	0	2400	0	0	0	0	0	0
30	30	780	80	2000	720	640	0	2560	2880	5760	2160	0	0	0	0	0	0	0	0	0	0	0	0	2560	3840	0	0	1440
0	0	0	180	0	0	2940	1470	1470	8820	0	0	0	0	0	120	600	1680	0	0	0	1960	0	5880	0	0	0	0	0
0	0	0	0	540	0	0	0	1170	3780	3240	0	6480	0	0	0	40	720	0	0	0	120	0	720	0	0	4320	0	0
0	0	0	0	0	450	0	0	0	0	4800	450	4800	4800	0	0	0	0	800	0	0	0	0	0	0	0	0	2400	0
0	0	1000	0	6000	0	0	0	0	12000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	8000	0	0	0
100	0	0	0	1200	1800	400	400	5200	0	7200	0	0	0	0	0	0	0	0	0	0	0	400	0	0	4800	0	0	7200
0	0	0	1190	3430	0	5880	0	6860	0	0	0	0	0	0	160	2240	7840	0	0	0	0	0	0	0	0	0	0	0
0	70	420	210	1050	0	1480	140	2380	4200	2520	0	0	0	0	0	160	1120	720	0	0	1120	0	1120	0	1680	6720	5040	0
0	10	120	10	890	360	320	140	1500	3480	3600	0	2160	0	0	0	0	160	0	0	0	320	0	2080	0	240	1920	2880	0
0	0	20	0	160	120	80	10	560	1620	2760	360	3240	1440	0	0	0	160	240	0	0	0	20	160	320	600	2240	1440	240
0	0	0	0	0	0	0	0	0	360	1680	90	3960	3520	640	0	0	0	120	320	0	0	0	0	0	0	0	0	180
0	0	0	0	0	0	0	0	0	0	0	0	0	7700	2310	0	0	0	0	0	440	0	0	0	0	0	0	0	0
2401	0	0	18816	0	0	0	0	0	0	0	0	0	0	0	4096	0	0	0	0	0	0	0	0	0	0	0	0	0
7	21	252	192	1344	1512	4608	0	0	8064	0	1512	0	0	0	0	0	4096	6912	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	576	21	504	1512	6048	0	4536	0	0	0	64	3456	6912	5184	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	315	5040	6720	448	0	0	0	2880	10240	3072	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	12397	0	0	0	0	0	16192	0	0	0	0	0	0	0	0
436	435	0	384	384	432	0	0	9216	0	0	1728	0	0	0	0	0	0	0	0	0	0	2048	0	2048	0	0	0	13824
145	436	624	128	256	144	0	1536	6144	1536	0	1728	0	0	0	0	0	0	0	0	0	0	0	4096	0	0	0	9216	4608
0	39	518	0	480	504	384	192	1536	4032	1152	432	864	0	0	0	0	0	0	0	0	0	0	0	0	2304	4096	2304	0
49	49	0	734	1666	0	1456	0	2744	1176	0	0	0	0	0	64	192	3584	1008	0	0	0	0	3136	3136	0	9408	0	3528
1	2	60	34	1046	72	224	0	904	1992	2304	0	864	0	0	0	0	128	0	0	0	192	0	512	832	768	4032	144	0
2	2	112	0	128	618	256	0	512	1280	3072	288	768	384	0	0	0	0	128	0	0	0	128	0	0	512	0	3200	1088
0	0	84	52	392	252	958	70	616	1596	1260	0	0	0	0	8	112	1168	1440	432	0	112	84	1064	224	1848	3360	3024	0
0	72	144	0	0	0	240	451	1560	1080	0	648	648	0	0	0	32	0	0	0	0	1184	444	1152	0	2016	1152	6912	432
6	12	48	14	226	72	88	65	1330	852	648	216	1080	0	0	0	16	160	0	0	0	160	48	688	224	1176	2352	2304	1080
0	1	42	2	166	60	76	15	284	1204	1296	72	1008	288	0	0	0	96	96	0	0	32	0	384	160	392	1760	1392	24
0	0	6	0	96	72	30	0	108	648	1560	36	1128	672	0	0	0	48	112	48	0	0	0	48	96	96	768	504	276
2	6	24	0	0	72	0	48	384	384	384	819	1776	192	128	0	0	0	192	0	0	0	0	0	0	768	0	768	672
0	0	3	0	24	12	0	3	120	336	752	111	1856	832	128	0	0	0	64	128	0	0	0	0	0	0	192	264	0
0	0	0	0	0	9	0	0	0	144	672	18	1248	1784	224	0	0	0	0	128	64	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	90	1440	1680	811	0	0	0	0	0	192	0	0	0	0	0	0	0	0
0	0	0	1176	0	0	4116	0	0	0	0	0	0	0	0	437	588	6860	0	0	0	0	2401	7203	9604	0	0	0	0
0	0	0	108	0	0	1764	147	1764	0	0	0	0	0	0	18	703	1764	3024	0	0	1029	0	882	0	5292	5292	0	0
0	0	0	48	84	0	438	0	420	756	756	0	0	0	0	5	42	1340	1296	1080	0	42	7	483	532	252	3024	1512	756
0	0	0	6	0	21	240	0	0	336	784	126	672	0	0	0	32	576	1768	1440	192	0	0	0	0	168	672	924	168
0	0	0	0	0	0	54	0	0	0	252	0	1008	672	0	0	0	360	1080	2246	512	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	1470	588	0	0	0	630	2240	1382	0	0	0	0	0	0	0	0
0	0	0	0	180	0	60	185	600	360	0	0	0	0	0	0	35	60	0	0	0	641	0	1500	0	2340	2700	2160	0
16	0	0	0	0	216	144	222	576	0	0	0	0	0	0	8	0	32	0	0	0	0	458	1752	384	1008	0	2592	1944
0	4	0	8	64	0	76	24	344	576	144	0	0	0	0	1	4	92	0	0	0	200	73	823	388	480	2016	2016	288
1	0	0	12	156	0	24	0	168	360	432	0	0	0	0	2	0	152	0	0	0	0	24	582	968	144	2016	0	432
0	0	18	0	48	18	66	21	294	294	144	108	0	0	0	0	12	24	36	0	0	156	21	240	48	1352	1384	1512	198
0	0	8	3	63	0	30	3	147	330	288	0	108	0	0	0	3	72	36	0	0	45	0	252	168	346	1792	828	252
0	1	4	0	2	25	24	16	128	232	168	24	132	0	0	0	0	32	44	0	0	32	12	224	0	336	736	1444	338
2	2	0	4	0	34	0	4	240	16	368	84	0	0	0	0	0	64	32	0	0	0	36	128	128	176	896	1352	1216
0	0	0	0	24	12	12	0	63	174	224	0	204	0	0	0	2	36	40	12	0	6	3	120	60	186	708	504	66
0	0	3	0	12	3	12	0	12	150	296	0	72	132	0	0	0	24	44	24	0	0	0	24	96	24	576	252	42
0	0	0	0	0	30	0	0	0	0	320	0	0	240	36	0	0	0	80	0	24	0	0	0	0	0	0	0	60
0	0	3	0	6	6	6	3	42	90	120	40	138	0	0	0	0	8	30	8	0	24	9	72	16	204	360	660	99
0	0	0	0	8	0	2	1	20	56	116	16	168	32	0	0	0	8	24	18	0	8	0	48	32	88	304	288	72
0	0	0	0	0	3	0	0	12	36	84	4	156	90	0	0	0	8	12	32	0	0	1	24	24	12	192	156	66
0	0	0	0	0	0	0	0	0	27	63	0	126	126	16	0	0	0	18	26	8	0	0	0	0	27	108	54	0
0	0	0	0	0	0	0	0	0	0	48	9	96	148	36	0	0	0	6	32	14	0	0	0	0	0	0	72	18
0	0	0	0	0	0	0	0	0	0	0	0	117	156	52	0	0	0	0	26	26	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0	0	0	168	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4032
0	9	0	0	0	72	0	0	0	0	0	72	0	0	0	0	0	0	0	0	0	0	192	0	0	0	0	2304	576
0	0	28	0	0	42	0	0	0	0	0	84	0	0	0	0	0	0	0	0	0	0	0	0	0	896	0	1344	0
0	0	1	0	0	6	0	6	0	48	48	6	12	0	0	0	0	0	0	0	0	0	6	96	0	32	0	408	108
0	0	0	0	6	3	0	0	24	24	24	15	30	0	0	0	0	0	0	0	0	0	0	0	0	120	192	252	114
0	0	0	0	0	0	0	0	18	0	36	0	36	0	0	0	0	0	0	0	0	0	3	18	12	0	72	216	108
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	3	0	0	0	0	0	24	0	24	0	0	0	0	0	0	0	0	8	0	64	0	0	0	96
0	0	0	0	0	0	0	0	0	4	16	2	24	8	0	0	0	0	0	0	0	0	0	8	8	16	64	48	12
0	0	0	0	0	0	0	0	0	0	3	0	12	12	0	0	0	0	0	0	0	0	0	0	0	3	24	36	9
0	0	0	0	0	0	0	0	0	0	0	3	0	0	6	0	0	0	0	0	0	0	0	0	0	0	0	0	72
0	0	0	0	0	0	0	0	0	0	0	0	3	3	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	9	0	0	0	0	0	0	0	0	0	0	0	0	0	18	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	30	30	0	30	0	0	0	0	0	0	0	0	6	0	15	0	30	120	180	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1440	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	4320	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	6400	640	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7200	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	5760	0	0	4320	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
240	1920	1920	0	2160	5760	2880	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
180	1920	1920	0	720	2880	5760	5120	1280	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	4620	0	0	0	0	15400	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13824	0	0	0	0	0	0	0	0	0	1296	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4608	0	0	0	0	0	0	0	0	0	0	1296	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	4608	0	6912	0	0	0	0	0	0	0	864	864	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3528	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	4608	2304	0	1728	6912	0	0	0	0	0	0	0	0	2592	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1088	4096	1024	1024	3072	0	6144	0	0	0	0	144	288	1152	2304	0	0	576	0	0	0	0	0	0	0	0	0	0	0
0	4032	4032	0	3024	3024	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
432	0	0	0	5184	5184	0	0	0	0	0	0	0	3888	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1080	3024	576	0	3024	4320	3456	0	0	0	0	0	0	0	2592	2592	0	0	0	0	0	0	0	0	0	0	0	0	0
24	2784	2400	0	2160	4032	3456	2304	0	0	0	0	0	432	864	0	0	0	1728	0	0	0	0	0	0	0	0	3456	0
276	1792	2368	256	1440	4176	4032	2688	1536	0	0	0	0	216	432	864	0	0	3456	1152	0	0	0	0	0	0	0	1728	0
672	0	0	0	5120	6144	2048	0	3072	0	12	36	144	288	2880	0	0	1152	4608	0	384	0	0	0	0	0	0	0	0
0	1088	384	0	1104	4032	4992	3584	2048	1024	0	0	0	36	360	576	0	0	3456	3072	0	768	0	0	0	0	0	1152	0
0	0	1056	192	0	1152	4320	5376	4736	2048	0	0	0	0	0	0	0	108	1728	4608	0	1152	1728	0	0	0	0	0	0
0	0	0	216	0	0	0	5120	8640	5120	0	0	0	0	0	0	0	0	0	0	540	8640	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	10584	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
756	4536	3024	0	1512	4536	6048	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
168	2240	2464	448	2520	6048	4032	5376	1344	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	504	1008	0	504	3402	8064	5824	5376	1792	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	441	0	0	0	7840	10290	7840	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	1080	0	0	6480	6480	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	7776	0
1944	1728	0	0	7776	0	3456	0	0	0	0	648	0	1944	0	5184	0	2592	0	0	0	0	0	0	0	0	0	0	0
288	2880	576	0	2592	5184	3456	0	0	0	0	0	0	1296	0	1296	0	0	5184	0	0	0	0	0	0	0	0	2592	0
432	2160	3456	0	864	5184	5184	0	0	0	0	0	0	0	0	1296	0	1296	7776	0	0	0	0	0	0	0	0	0	0
198	2232	288	0	3672	4752	864	1728	0	0	0	0	216	216	3240	0	0	0	5184	1728	0	0	0	0	0	0	0	2592	0
252	2124	1728	0	1620	4104	3456	1728	0	0	0	0	0	0	1296	648	0	0	5184	3456	0	0	0	0	0	0	0	2592	0
338	1344	672	0	2640	3456	2496	768	768	0	0	36	72	612	1512	1728	0	0	3456	4608	0	0	1152	0	0	0	0	3456	0
1216	704	448	64	1584	3456	4224	0	768	0	36	36	0	648	2736	3456	0	576	3456	4608	1152	0	0	0	0	0	0	0	0
66	1916	1312	64	1188	2988	3456	1920	768	0	0	0	0	216	864	972	0	0	4752	5184	0	2304	0	0	0	0	0	2376	0
42	1312	2112	256	288	2376	3672	3072	1152	0	0	0	0	108	216	432	0	108	5184	5760	0	2304	1728	0	0	0	0	864	0
60	640	2560	924	0	0	2880	3840	4200	0	0	0	0	0	0	0	0	540	0	5760	540	5760	4320	0	0	0	0	0	0
99	792	192	0	2132	3000	1888	960	384	256	0	6	36	558	1764	1032	0	96	6048	4032	0	2304	1536	768	0	0	0	3024	0
72	664	528	0	1000	2990	2304	1600	768	256	0	0	0	144	864	696	0	192	5760	5376	0	3072	1536	1536	0	0	0	2160	0
66	576	612	48	472	1728	3164	1936	1344	384	0	0	0	72	216	768	0	102	4248	6768	288	3456	1824	2688	0	0	0	1152	0
0	360	576	72	270	1350	2178	2972	1896	672	0	0	0	0	0	108	0	0	3240	6156	0	5184	2160	4320	0	0	0	648	0
18	192	288	105	144	864	2016	2528	2778	1248	0	0	0	0	0	0	0	54	1728	4608	324	5472	3024	6912	0	0	0	0	0
0	0	0	0	234	702	1404	2184	3042	2360	0	0	0	0	0	0	0	0	0	2808	0	5616	2808	11232	0	0	0	0	0
4032	0	0	0	0	0	0	0	0	0	472	938	0	0	2688	14336	0	2688	0	0	7168	0	0	0	0	256	0	0	0
576	0	0	0	1536	0	0	0	0	0	134	472	72	5184	1536	8192	0	384	4608	0	3072	0	4096	0	0	0	256	0	0
0	0	0	0	2688	0	0	0	0	0	0	21	528	448	6720	0	256	0	5376	0	0	7168	0	0	0	0	0	7168	0
108	384	192	0	1488	1152	768	0	0	0	0	54	16	984	840	2400	512	480	4608	6656	384	768	3072	3072	0	0	0	4160	0
114	384	96	0	1176	1728	576	0	0	0	1	4	60	210	2512	1280	0	96	6816	6144	0	3840	384	3072	0	0	0	3072	512
108	324	144	0	516	1044	1536	192	0	0	4	16	0	450	960	2066	0	192	5112	7488	640	2304	2560	3840	0	0	0	1836	1024
0	0	0	0	0	0	0	0	0	0	0	0	1	56	0	0	1504	84	1344	1792	168	4032	2688	10752	6272	0	42	0	4032
96	0	192	96	256	1536	1088	0	384	0	4	4	0	480	384	1024	768	924	6528	4608	704	3840	4480	4096	0	0	128	0	1024
12	176	192	0	336	960	944	640	256	0	0	1	4	96	568	568	256	136	5456	6528	64	4992	2304	4864	1024	0	0	1680	512
9	108	120	12	126	504	846	684	384	96	0	0	0	78	288	468	192	54	3672	6780	216	5152	2592	6624	1536	0	0	984	1152
72	0	0	36	0	0	1152	0	864	0	4	12	0	144	0	1280	576	264	1152	6912	1954	1440	3776	9216	0	16	48	0	3840
0	48	48	12	72	288	432	576	456	192	0	0	3	9	180	144	432	45	2808	5152	45	5952	2520	8640	2688	0	0	576	1440
0	0	72	18	96	288	456	480	504	192	0	1	0	72	36	320	576	105	2592	5184	236	5040	3400	8448	2304	0	16	576	1728
0	0	0	0	14	84	196	280	336	224	0	0	0	21	84	140	672	28	1596	3864	168	5040	2464	10608	4032	0	4	336	2576
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1085	0	930	2480	0	4340	1860	11160	6944	0	0	248	3720
0	0	0	0	0	0	0	0	0	0	155	0	0	0	0	0	0	0	0	0	17360	0	0	0	0	496	868	0	13888
0	0	0	0	0	0	0	0	0	0	0	35	0	0	0	0	5040	1680	0	0	1680	0	8960	7680	0	28	496	0	7168
0	330	120	0	630	1350	960	480	0	0	0	0	20	325	960	765	0	0	6300	6560	0	3840	1920	3840	1024	0	0	2902	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	60	160	1080	30	720	2880	300	3600	2160	11040	5760	1	16	0	4960

Für T_2 bis T_16 ergeben sich dann folgende Polynome in T_1:

	T_2	T_3	T_4	T_5	T_6	T_7	T_8	T_9
T_1^0	$\frac{-32767}{3}$	0	$\frac{1073577988}{45}$	0	$\frac{-5023118037568}{405}$	0	$\frac{164276052300623872}{103275}$	0
T_1^1	0	$\frac{-131065}{21}$	0	$\frac{10274340988}{1395}$	0	$\frac{-20534090957504}{10287}$	0	$\frac{875409787929665695744}{6702237675}$
T_1^2	$\frac{1}{3}$	0	$\frac{-360413}{315}$	0	$\frac{145950676924}{205065}$	0	$\frac{-282076364035273408}{2846155725}$	0
T_1^3	0	$\frac{1}{21}$	0	$\frac{-851813}{9765}$	0	$\frac{731534634652}{26043255}$	0	$\frac{-159375289461838528}{80162984475}$
T_1^4	0	0	$\frac{1}{315}$	0	$\frac{-124475}{41013}$	0	$\frac{3316511938652}{6641030025}$	0
T_1^5	0	0	0	$\frac{1}{9765}$	0	$\frac{-1309831}{26043255}$	0	$\frac{14218497317852}{3393566342775}$
T_1^6	0	0	0	0	$\frac{1}{615195}$	0	$\frac{-8082901}{19923090075}$	0
T_1^7	0	0	0	0	0	$\frac{1}{78129765}$	0	$\frac{-16406101}{10180699028325}$
T_1^8	0	0	0	0	0	0	$\frac{1}{19923090075}$	0
T_1^9	0	0	0	0	0	0	0	$\frac{1}{10180699028325}$
T_1^{10}	0	0	0	0	0	0	0	0
T_1^{11}	0	0	0	0	0	0	0	0
T_1^{12}	0	0	0	0	0	0	0	0
T_1^{13}	0	0	0	0	0	0	0	0
T_1^{14}	0	0	0	0	0	0	0	0
T_1^{15}	0	0	0	0	0	0	0	0
T_1^{16}	0	0	0	0	0	0	0	0

	T_{10}	T_{11}	T_{12}	T_{13}
T_1^0	$\frac{-172288484270899462144}{3408075}$	0	$\frac{7813036635279189328448}{1993723875}$	0
T_1^1	0	$\frac{-269431201058824386542305 28}{129355102055255}$	0	$\frac{2214389432434310677608716734300 16}{2817433499698980337 5}$
T_1^2	$\frac{6966109759944006965534 72}{212548063387275}$	0	$\frac{-292042952392955605726485544 96}{1126930235396340375}$	0
T_1^3	0	$\frac{1373841541449413488848896}{417205643873460 75}$	0	$\frac{-616170470593704119564616929902592}{4864571289135260454126375}$
T_1^4	$\frac{-146093376676193862 4}{82006733117925}$	0	$\frac{850554970886536679286550528}{582014389372793950072 5}$	0
T_1^5	0	$\frac{-218230100609192917 12}{292043950711422525}$	0	$\frac{142110137486112772216004730 88}{476727986335255524504384 75}$
T_1^6	$\frac{176941834659988}{104148551059764 75}$	0	$\frac{-261815089770288388307 2}{174604316811838185021 75}$	0
T_1^7	0	$\frac{7183085179746 76}{213192084019338443 25}$	0	$\frac{-667437527458709036992}{461349664195408572101017 5}$
T_1^8	$\frac{-33019733}{104148551059764 75}$	0	$\frac{190928647445548}{582014389372793950072 5}$	0
T_1^9	0	$\frac{-660176 21}{213192084019338443 25}$	0	$\frac{744589387019308}{476727986335255524504384 75}$
T_1^{10}	$\frac{1}{104148551059764 75}$	0	$\frac{-43665863}{291007194686396975036 25}$	0
T_1^{11}	0	$\frac{1}{213192084019338443 25}$	0	$\frac{-3721681}{103636518768533809674866 25}$
T_1^{12}	0	0	$\frac{1}{873021584059190925108 75}$	0
T_1^{13}	0	0	0	$\frac{1}{715091979502883286756577125}$
T_1^{14}	0	0	0	0
T_1^{15}	0	0	0	0
T_1^{16}	0	0	0	0

	T_{14}	T_{15}	T_{16}
T_1^0	$\frac{-1763900680367912726592222528}{257190379875}$	0	$\frac{28899748747147882112487018987 52}{16854971545108125}$
T_1^1	0	$\frac{-1549947137358959870464596067695561015296}{26200087780939835498413177 5}$	0
T_1^2	$\frac{5049908457152195944530148276048809 1648}{1101791770920317585529295875}$	0	$\frac{-17988306239545017547724251718387150310342656}{1557584925685244994016717597198125}$
T_1^3	0	$\frac{7552218779495643348721322633787684935434 24}{78342231778308920525333410321391 25}$	0
T_1^4	$\frac{-1336320169024759510626294281692774 4}{5071580909175643673996971012 5}$	0	$\frac{49394224333307596159809324932541145950453 76}{7334511656559250152325321493446250812 5}$
T_1^5	0	$\frac{-2963776994951016722735777665471794380 8}{1279589785712379035247112368582723 75}$	0
T_1^6	$\frac{6575119374622675087871536046 08}{2343070380039147377386600607775}$	0	$\frac{-1853854614051886207880389334290786156544}{2515737498199822802247585272252064028687 5}$
T_1^7	0	$\frac{898812465829978321706154708582 4}{7677538714274274211482674211496342 5}$	0
T_1^8	$\frac{-3104213782030343986668 8}{4686140760078294754773201215 55}$	0	$\frac{923136858964495433490973929021 44}{5031474996399645604495170544504128057375}$
T_1^9	0	$\frac{-1054589654382988946823232}{7677538714274274211482674211496342 5}$	0
T_1^{10}	$\frac{1914791446952 92}{5349475753514035108188585862 5}$	0	$\frac{-2525942719314485631792064}{2287034089272566183861441156592785480625}$
T_1^{11}	0	$\frac{880771783511044}{2326526883113416427722022488332225}$	0
T_1^{12}	$\frac{-49164834 1}{1171535190019573688693300303887 5}$	0	$\frac{4092709823288608308}{2515737498199822802247585272252064028687 5}$
T_1^{13}	0	$\frac{-894276949}{3838769357137105741337105748171 25}$	0
T_1^{14}	1	0	$\frac{-1431131477}{2515737498199822802247585272252064028687 5}$
T_1^{15}	$\frac{1171535190019573688693300303887 5}{0}$	1	0
T_1^{16}	0	$\frac{3838769357137105741337105748171 25}{0}$	1
			$\frac{2515737498199822802247585272252064028687 5}{}$

Die Koeffizienten wurden mit Hilfe des folgenden Magma-Programms [BCP97] berechnet:

```
//a berechnet rekursiv die Koeffizienten von (T_1)^k bei T_m in
//der, wobei n die Dimension der Codes bezeichnet.

function a(k,m,n)
        if [k,m] eq [0,0] then
                return 1;
        elif m le -1 then
                return 0;
        elif k le m-1 then
                return 0;
        else
                return ((2^m-1)*a(k-1,m-1,n)+
                        (2^(n-1-m)-1)*2^m*a(k-1,m+1,n));
        end if;
end function;

//A gibt die Koeffizienten der Polynome von T_1 bis T_{n-1} in
//Potenzen von T_1 spaltenweise wieder
function A(n)
        B:=[];
        for m in [0 .. n] do
                for k in [0 .. n] do
                        B:=Append(B,a(m,k,n));
                end for;
        end for;
        C:=Matrix(RationalField(), n+1, n+1, B);
        C:=Transpose(C);
        return(C^(-1));
end function;
```

A(n) liefert dann eine Matrix in deren Einträgen die Koeffizienten der Polynome der Familie von Typ 2 Codes in $\mathbb{F}_2^{2n}$.

Kapitel 5

Der Ring der Endomorphismen auf $\mathcal{V}$

5.1 klassische Typen

Wie in den Fällen in Kapitel 3.3 wird immer ein Vektorraum $V := \mathbb{F}_q^N$ mit einer nicht ausgearteten ϵ-Sesquilinearform $b : V \times V \to \mathbb{F}_q$ betrachtet. Nach dem Satz von Witt (siehe z.B. [Tay92, Theorem 7.4]) operiert die Isometriegruppe $G(V, b)$ transitiv auf der Menge

$$\mathcal{F} := \{C = C^\perp \leq \mathbb{F}_q^N\}$$

aller selbstdualen Codes in (V, b).
Genauer gilt für die einzelnen Fälle:
a) Euklidisch selbstduale Codes in $\mathbb{F}_q^N$ mit q gerade und

$$b(x, y) = \sum_{i=1}^{N} x_i y_i$$

Hier gilt $\mathbf{1} \in C = C^\perp$ also entspricht jeder selbstduale Code C einem maximal isotropen Teilraum

$$C/\langle \mathbf{1} \rangle \leq \mathbf{1}^\perp/\langle \mathbf{1} \rangle =: V.$$

Hier ist

$$\mathbf{1}^\perp = \{x \in \mathbb{F}_q^n \mid \sum_{i=1}^{N} x_i = 0\}$$

und $\mathbf{1} \in \mathbf{1}^\perp$ da die Länge N gerade ist. Die alternierende Bilinearform $\overline{b}$: $V \times V \to \mathbb{F}_2$ ist vertreterweise definiert durch

$$\overline{b}(x + \langle \mathbf{1} \rangle, y + \langle \mathbf{1} \rangle) := \sum_{i=1}^{N} x_i y_i.$$

Diese Bilinearform ist unabhängig von der Wahl der Vertreter $x, y \in \mathbf{1}^\perp$. Es ist für $x \in \mathbf{1}^\perp$

$$\overline{b}(x + \langle \mathbf{1} \rangle, x + \langle \mathbf{1} \rangle) = \sum_{i=1}^{N} x_i^2 = (\sum_{i=1}^{N} x_i)^2 = (b(x, \mathbf{1})^2 = 0$$

also ist die Form $\overline{b}$ alternierend. Die Symmetriegruppe $G(V, \overline{b})$ ist also die symplektische Gruppe $\mathrm{Sp}_{N-2}(\mathbb{F}_q)$.

b) Doppelt-gerade binäre Codes: $q = 2$,

$$b(x, y) = \sum_{i=1}^{N} x_i y_i,$$

C isotrop genau dann wenn $\mathrm{wt}(c) \in 4\mathbb{Z}$ für alle $c \in C$. Hier ist N immer durch 8 teilbar.
Wie in a) betrachten wir $V = \mathbf{1}^\perp / \langle \mathbf{1} \rangle$. Die Bedingung doppelt gerade zu sein, lässt sich mit Hilfe einer quadratischen Form auf V ausdrücken:

$$\begin{aligned} q &: V \to \mathbb{F}_2 \\ q(x + \langle \mathbf{1} \rangle) &:= \frac{\mathrm{wt}(x)}{2} + 2\mathbb{Z}. \end{aligned}$$

Diese Form ist wohldefiniert, da $\mathrm{wt}(x) \in 2\mathbb{Z}$ ist für alle $x \in \mathbf{1}^\perp$ und die Länge N durch 4 teilbar ist. Die zu q gehörende Bilinearform ist

$$\overline{b}(x, y) = q(x + y) - q(x) - q(y).$$

da

$$\begin{aligned} q(x + y) - q(x) - q(y) &= \frac{1}{2} \left(\mathrm{wt}(x + y) - \mathrm{wt}(x) - \mathrm{wt}(y) \right) \\ &= \frac{1}{2} \left(\mathrm{wt}(x) + \mathrm{wt}(y) - 2 \sum_{i=1}^{N} x_i y_i \mathrm{wt}(x) - \mathrm{wt}(y) \right) \\ &= -b(x, y) = b(x, y) \end{aligned}$$

Die Symmetriegruppe in diesem Fall ist $G(V, q) = O^+_{N-2}(\mathbb{F}_2)$, die orthogonale Gruppe über $\mathbb{F}_2$ zu einem quadratischen Raum der Dimension $N - 2$ mit Witt-Defekt 0.

c) Euklidisch selbstduale Codes in F_q^N mit q ungerade und

$$b(x, y) = \sum_{i=1}^{N} x_i y_i,$$

Hier ist $V = \mathbb{F}_q^N$ und $b(x,y) = \sum_{i=1}^N x_i y_i$. $G(V,b) = O_N^+(\mathbb{F}_q)$ ist die orthogonale Gruppe über $\mathbb{F}_q$ zu einem quadratischen Raum der Dimension N mit Witt-Defekt 0.

c') Euklidisch selbstduale Codes in in $\mathbb{F}_q^N$ mit q ungerade, die den Einsvektor $\mathbf{1}$ enthalten und mit $b(x,y) = \sum_{i=1}^N x_i y_i$.
Dazu betrachtet man

$$V = \mathbf{1}^\perp / \langle \mathbf{1} \rangle$$

mit der wie in a) wohldefinierten symmetrischen Bilinearform

$$\overline{b}(x + \langle \mathbf{1} \rangle, y + \langle \mathbf{1} \rangle) := \sum_{i=1}^N x_i y_i.$$

Die Symmetriegruppe ist $G(V,\overline{b}) = O_{N-2}^+(\mathbb{F}_q)$ ist die orthogonale Gruppe über $\mathbb{F}_q$ zu einem quadratischen Raum der Dimension $N-2$ mit Witt-Defekt 0.

d) Hermitesche selbstduale Codes in $\mathbb{F}_q^N$ mit $q = r^2$ einem Quadrat einer Primzahlpotenz, und

$$b(x,y) := \sum_{i=1}^N x_i y_i^r.$$

Hier ist $V = \mathbb{F}_q^N$ und $G(V,b) = U_N(\mathbb{F}_q)$ ist die unitäre Gruppe.

d')Hermitesche selbstduale Codes in $\mathbb{F}_q^N$ mit $q = r^2$ einem Quadrat einer Primzahlpotenz, die den Einsvektor $\mathbf{1}$ enthalten und mit

$$b(x,y) := \sum_{i=1}^N x_i y_i^r.$$

C isotrop, falls $\mathbf{1} \in C$. Hier ist N durch $p = \mathrm{char}(\mathbb{F}_q)$ teilbar.
Wie vorher entsprechen diese Codes den maximal isotropen Teilräumen von $V = \mathbf{1}^\perp / \langle \mathbf{1} \rangle$ mit wohldefinierter hermitescher Form

$$\overline{b}(x + \langle \mathbf{1} \rangle, y + \langle \mathbf{1} \rangle) := \sum_{i=1}^N x_i y_i^r$$

und $G(V,\overline{b}) = U_{N-2}(\mathbb{F}_q)$ ist die unitäre Gruppe.

Zusammenfassend erhalten wir in allen Fällen eine Gruppe $G(V,b)$, die transitiv auf der Menge der selbstdualen isotropen Codes operiert, also ist

5.1.1 Satz
$\mathcal{F} := \{C = C^\perp \leq \mathbb{F}_q^N \mid C \text{ isotrop } \} = C_0 \cdot G(V,b)$ *für ein* $C_0 \in \mathcal{F}$.

5.2 Endomorphismen und Adjazenzmatrizen

5.2.1 Definition
Sei $\mathcal{W} := \{\sum_{C\in\mathcal{F}} a_C e_C \mid a_C \in \mathbb{C}\}$ *der Vektorraum der formalen* $\mathbb{C}$*-Linearkombinationen der Codes einer Familie* $\mathcal{F}$.

Die symmetrische Gruppe S_N operiert auf $\mathcal{F}$ und also auch auf $\mathcal{W}$.

5.2.2 Bemerkung
Der Vektorraum $\mathcal{V}$ *(siehe 2.2.1) über der gleichen Familie* $\mathcal{F}$ *ist isomorph zu* $\mathcal{W}/S_N$.

Die Gruppe $G = G(V,b)$ aus Satz 5.1.1 operiert transitiv auf der Familie $\mathcal{F}$ und $\mathcal{W}$ sei der zugehörige Permutationsmodul, also die induzierte Darstellung $\mathbb{1}_S^G$ der trivialen Darstellung des Stabilisators S eines Elements aus $\mathcal{F}$. (siehe z.B. [Isa76, Lemma 5.14])

5.2.3 Satz
$\mathcal{W}$ *ist ein* $\mathbb{C}G$*-Modul, wobei* $G = G(V,b)$ *die Gruppe aus Satz5.1.1 sei, und es gilt*

$$W \cong \mathbb{1}_S^G$$

mit $S := Stab_G(C_0)$ *und* $C_0 \in \mathcal{F}$.

5.2.4 Definition
Der Endomorphismus A_k *von* $\mathcal{W}$ *sei definiert als*

$$\begin{aligned} A_k : \mathcal{W} &\to \mathcal{W} \\ e_C &\mapsto \sum_{D\sim_k C} e_D. \end{aligned}$$

5.2.5 Bemerkung
A_k *in der Basis* $(C : C \in \mathcal{F})$ *geschrieben ergibt die Adjazenzmatrix des* k*-Nachbarschaftsgraphen auf* $\mathcal{F}$.

5.2.6 Satz
$A_k \in End_{\mathbb{C}G}(\mathcal{W})$

Beweis:
Für alle $g \in G$ gilt:

$$A_k(ge_C) = \sum_{D \sim_k gC} e_D = \sum_{D \sim_k C} ge_D = gA_k(e_C).$$

q.e.d.

Ein klassischer Satz der Darstellungstheorie sagt aus, dass die Endomorphismenalgebra $\mathrm{End}_{\mathbb{C}G}(\mathbb{1}_S^G)$ eines induzierten Moduls isomorph ist zur Algebra der formalen Linearkombinationen der Doppelnebenklassen $\langle SgS | g \in G \rangle_{\mathbb{C}}$. Dabei ist die Multiplikation der Doppelnebenklassen definiert durch

$$(SgS)(ShS) = \sum SaS, \text{ falls } gShS = \dot{\bigcup} aS$$

(siehe [Fre83, Hilfssatz 1.8]).
Der Isomorphismus $\langle SgS | g \in G \rangle_{\mathbb{C}} \to \mathrm{End}_{\mathbb{C}G}(\mathbb{1}_S^G)$ bildet SgS auf den Endomorphismus φ_g ab, mit

$$\varphi_g(e_{aC_0}) = a(\varphi_g(e_{C_0})) = \sum_b e_{abC_0}$$

wobei $SgS = \dot{\bigcup} bS$, also bC_0 die Elemente der S-Bahn von gC_0 durchläuft.

5.2.7 Satz

$$\mathrm{End}_{\mathbb{C}G}(\mathcal{W}) = \mathrm{End}_{\mathbb{C}G}(\mathbb{1}_S^G) \cong \langle SgS | g \in G \rangle_{\mathbb{C}}$$

5.3 BN-Paare

Wie in [Tay92] Kapitel 5 definieren wir:

5.3.1 Definition
Ein BN-Paar einer Gruppe G, ist ein Paar von Untergruppen B und N für die folgende Axiome erfüllt sind:

1. $G = \langle B, N \rangle$.
2. $H := B \cap N$ *ist ein Normalteiler von* N.
3. $W := N/H$ *hat ein Erzeugendensystem* $\{w_i : i \in I\}$ *mit* $w_i^2 = 1$ *für alle* i *aus der Indexmenge* I.

4. Für $w_i = n_i H$ und $n \in N$ gilt

(a) $n_i B n_i \neq B$ und,

(b) $n_i B n \subseteq (B n_i n B) \cup (BnB)$.

W heißt dann Weylgruppe von G.

5.3.2 Definition
Sei nun G eine Gruppe mit BN-Paar und I die Indexmenge von oben, dann ist $W_J := \langle w_j : j \in J \rangle$ mit $J \subseteq I$ ein Untergruppe der Weylgruppe W. N_J sei dann die Untergruppe von N für die $N_J/H = W_J$ ist.

$$P_J := BN_JB \leq G$$

und die die zu P_J konjugierten Untergruppen von G heißen parabolische Untergruppen.

5.3.3 Satz
Sei G eine Gruppe mit BN-Paar und P_J eine parabolische Untergruppe und W_J die dazugehörige Untergruppe der Weylgruppe W, dann gilt:

$$P_J \backslash G / P_J \cong W_J \backslash W / W_J$$

als $\mathbb{C}$-Vektorräume.

Beweis:
siehe [Car85] 2.8.1. q.e.d.

In allen betrachteten Fällen hat der Vektorraum V eine Basis

$$(e_1, \ldots, e_m, f_1, \ldots, f_m)$$

mit $b(e_i, f_j) = \delta_{ij}$ so dass $\langle e_1, \ldots e_m \rangle$ und $\langle f_1, \ldots, f_m \rangle$ maximal total isotrope Teilräume sind (insbesondere ist auch $q(e_i) = 0$ im Fall **b**) und $m = n$ bzw. $m = n - 1$ in den entsprechenden Fällen.

5.3.4 Satz
Sei $\mathcal{F}$ eine Familie von euklidischen selbstdualen Codes über $\mathbb{F}_q^N$ und sei $U := \langle e_1, \ldots, e_m \rangle \leq V$ unter dem entsprechenden Homomorphismus von oben. Dann gibt es eine Basis $\mathcal{B} = (e_1, \ldots, e_m, f_1, \ldots, f_m)$ von V für die folgendes gilt:

$$\begin{aligned} b(e_i, f_i) &= 1 \quad \forall 1 \leq i \leq m \\ b(e_i, f_j) &= 0 \quad \forall 1 \leq i, j \leq m \wedge i \neq j \\ b(f_i, f_j) &= 0 \quad \forall 1 \leq i, j \leq m \end{aligned}$$

Beweis:
Wählt man eine beliebige Basis, die mit einer Basis von U beginnt, so gilt für die Grammatrix Γ der hermiteschen Form b:

$$\Gamma = \begin{pmatrix} 0 & A \\ A^{tr} & B \end{pmatrix}$$

mit $A \in \mathrm{GL}_m(V)$ da b nicht ausgeartet ist und $B = B^{tr}$ mit der Zerlegung $B = C + C^{tr}$ und $C \in \mathbb{F}_q^{m \times m}$. Nun führt man zuerst folgenden Basiswechsel durch:

$$\begin{pmatrix} A^{-1} & 0 \\ 0 & I_m \end{pmatrix} G \begin{pmatrix} A^{-tr} & 0 \\ 0 & I_m \end{pmatrix} = \begin{pmatrix} 0 & I_m \\ I_m & B \end{pmatrix}$$

Dann kann man mit einem weiteren Basiswechsel folgendermassen eine Basis mit den gewünschten Eigenschaften erreichen:

$$\begin{pmatrix} I_m & 0 \\ -C & I_m \end{pmatrix} \begin{pmatrix} 0 & I_m \\ I_m & B \end{pmatrix} \begin{pmatrix} I_m & 0 \\ -C^{tr} & I_m \end{pmatrix} = \begin{pmatrix} 0 & I_m \\ I_m & 0 \end{pmatrix}$$

q.e.d.

5.3.5 Satz
Sei $\mathcal{F}$ eine Familie von hermitescher selbstdualen Codes über $\mathbb{F}_q^N$ und sei $U := \langle e_1, \ldots, e_m \rangle \leq V$ unter dem entsprechenden Homomorphismus von oben. Dann gibt es eine Basis $\mathcal{B} = (e_1, \ldots, e_n, f_1, \ldots, f_n)$ von V so dass folgendes gilt:

$$\begin{aligned} b(e_i, f_i) &= 1 \quad \forall 1 \leq i \leq m \\ b(e_i, f_j) &= 0 \quad \forall 1 \leq i, j \leq m \wedge i \neq j \\ b(f_i, f_j) &= 0 \quad \forall 1 \leq i, j \leq m \end{aligned}$$

Beweis:
Wählt man eine beliebige Basis, die mit einer Basis von U beginnt, so gilt für die Grammatrix Γ der hermiteschen Form b:

$$\Gamma = \begin{pmatrix} 0 & A \\ \bar{A}^{tr} & B \end{pmatrix}$$

mit $A \in \mathrm{GL}_m(\mathbb{F}_q)$ da b nicht ausgeartet ist und $B = \bar{B}^{tr}$ mit der Zerlegung $B = C + \bar{C}^{tr}$ und $C \in \mathbb{F}_q^{m \times m}$. Nun führt man zuerst folgenden Basiswechsel durch:

$$\begin{pmatrix} A^{-1} & 0 \\ 0 & I_m \end{pmatrix} G \begin{pmatrix} \bar{A}^{-tr} & 0 \\ 0 & I_m \end{pmatrix} = \begin{pmatrix} 0 & I_m \\ I_m & B \end{pmatrix}$$

Dann kann man mit einem weiteren Basiswechsel folgendermassen eine Basis mit den gewünschten Eigenschaften erreichen:

$$\begin{pmatrix} I_m & 0 \\ -C & I_m \end{pmatrix} \begin{pmatrix} 0 & I_m \\ I_m & B \end{pmatrix} \begin{pmatrix} I_m & 0 \\ -\bar{C}^{tr} & I_m \end{pmatrix} = \begin{pmatrix} 0 & I_m \\ I_m & 0 \end{pmatrix}$$

q.e.d. Nach [Tay92, Seite 85] ist in allen Fällen ausser für $G = O_N(F_q)$ die Weylgruppe isomorph zu $C_2^m \rtimes S_m$. Die Weylgruppe kann als Untergruppe von $G(V, b)$ realisiert werden, wobei jede Permutation $\sigma \in S_m$ durch die Abbildung

$$\iota(\sigma) : \begin{cases} e_i \mapsto e_{\sigma(i)} \\ f_j \mapsto f_{\sigma(j)} \end{cases} \quad \text{für alle } i, j$$

und die Standarderzeuger π_i der C_2^m durch die Abbildungen

$$\iota(\pi_i) : \begin{cases} e_i \mapsto f_i & \\ e_j \mapsto e_j, & \text{für alle } j \neq i \\ f_j \mapsto f_j, & \text{für alle } j \neq i \end{cases}$$

dargestellt sind.

5.3.6 Lemma
Die Abbildung $\iota : W \to N \leq G$ ist ein Gruppenmonomorphismus mit $\iota(n(N \cap B)) = n$ für alle Elemente $n \in \text{Bild}(\iota)$.

Ist G die orthogonale Gruppe, so ergibt sich eine kleine Schwierigkeit: Die Gruppe G selbst besitzt kein BN-Paar (s. [Tay92, Seite 85]), sondern nur eine Untergruppe vom Index 2.

5.3.7 Satz
([Tay92, Theorem 11.61]) Sei (V, q) ein quadratischer Raum über dem endlichen Körper $\mathbb{F}$ mit Witt-Defekt 0 und sei $U \leq V$ ein total isotroper Teilraum. Definiere $D : O(V, q) \to \mathbb{Z}/2\mathbb{Z}$ durch $D(g) := \dim(U/U \cap g(U)) + 2\mathbb{Z}$. Dann ist D ein wohldefinierter Epimorphismus, die sogenannte Dickson-Invariante. *Der Kern von D wird mit $SO(V, q)$ bezeichnet und hat 2 Bahnen auf $\mathcal{F}$.*

Der Stabilisator S eines jeden maximal isotropen Teilraums C_0 ist in $SO(V, q)$ enthalten. Die beiden Bahnen von $SO(V, q)$ auf $\mathcal{F}$ sind gegeben durch

$$\mathcal{F}_0 := \{C \in \mathcal{F} \mid \dim(C_0/C \cap C_0) \text{ gerade } \}$$

und

$$\mathcal{F}_1 := \{C \in \mathcal{F} \mid \dim(C_0/C \cap C_0) \text{ ungerade } \}.$$

Da jede Permutation $\sigma \in S_N$ mit Signum -1 jeden Code in $\mathcal{F}_0$ auf einen in $\mathcal{F}_1$ abbildet ([GN, Lemma 7.1]) enthält schon $\mathcal{F}_0$ ein Vertretersystem aller Äquivalenzklassen und wir ersetzen dann $\mathcal{W}$ durch den Teilraum $\mathcal{W}_0$ erzeugt von $\{e_C \mid C \in \mathcal{F}_0\}$. Es ist $A_k(W_0) \subset W_0$ genau dann wenn k gerade ist.

5.3.8 Lemma
([Tay92, Seite 170]) Die Weylgruppe von $SO(V,q)$ ist

$$W_0 := \langle \pi_1\pi_i \mid 2 \leq i \leq m \rangle \rtimes S_m.$$

5.3.9 Satz
Sei $G = G(V,b)$ die Symmetriegruppe von (V,b) wie oben und $G = SO(V,q)$ der Kern der Dickson-Invariante im quadratischen Fall und $C_0 \in \mathcal{F}_0$. Sei $S := \mathrm{Stab}_G(C_0)$. Dann ist S eine parabolische Untergruppe von G mit zugehöriger Weylgruppe $W_S = S_m$.

Beweis:
Œ sei $C_0 = \langle e_1, \ldots, e_m \rangle$. Dann ist das Bild von S_m in G enthalten im Stabilisator S von C_0. Weiter ist

$$S = \{ \begin{pmatrix} A & B \\ 0 & A^* \end{pmatrix} \in G \}$$

wobei $A^* = A^{-tr}$ im symplektischen und orthogonalen Fall und $A^* = \overline{A}^{-tr}$ im unitären Fall. Dabei ist die Projektion

$$S \to \mathrm{GL}_m(\mathbb{F}), \begin{pmatrix} A & B \\ 0 & A^* \end{pmatrix} \mapsto A$$

ein Gruppenepimorphismus, dessen Kern das unipotente Radikal

$$\{ \begin{pmatrix} I & B \\ 0 & I \end{pmatrix} \in S \}$$

ist. Also ist die Levy-Gruppe von S isomorph zur $\mathrm{GL}_m(\mathbb{F})$ mit S_m als Weylgruppe. q.e.d.

5.3.10 Satz
In den Fällen in denen die Weylgruppe $W = C_2^m \rtimes S_m$ ist gilt:

$$W = \dot{\bigcup}_{k=0}^{m} W_S t_k W_S \text{ mit } t_k := \prod_{i=1}^{k} \pi_i.$$

Beweis:
Sei $(\prod_{i\in I}\pi_i, \sigma)$ mit $I \subseteq \{1,\ldots,n\}$ und $\sigma \in S_n$ ein beliebiges Element von W. Wähle nun $(1,\alpha) \in W_J$ mit $\alpha(i_j) = j$ für $I = \{i_1,\ldots,i_m\}$ mit $m \leq n$. Dann ist auch $(1, \sigma^{-1}\alpha^{-1})$ in W_J.

$$\begin{aligned}
&(1,\alpha)(\prod_{i\in I}\pi_i,\sigma)(1,\sigma^{-1}\alpha^{-1})\\
&= (1,\alpha)(\prod_{i\in I}\pi_i,\alpha^{-1})\\
&= (\prod_{i\in I}\pi_{\alpha(i)},1) = (\prod_{i=1}^{|I|}\pi_i,1)\\
&= (t_{|I|},1)\\
&\Rightarrow (\prod_{i\in I}\pi_i,\sigma) \in W_J t_{|I|} W_J
\end{aligned}$$

q.e.d.

5.3.11 Satz
Für $G = SO_N(\mathbb{F}_q)$ und $W = W_0$ gilt:

$$W = \dot{\bigcup}_{0\leq k\leq \frac{m}{2}} W_S t_{2k} W_S \text{ mit } t_k := \prod_{i=1}^{k}\pi_i.$$

Beweis:
Der Beweis verläuft analog zu dem Beweis von Satz 5.3.10. q.e.d.

Mit [Car85, Proposition 2.8.1] erhält man also auch

5.3.12 Korollar
Für die in Satz 5.3.10 betrachteten Gruppen G gilt:

$$G = \dot{\bigcup}_{k=0}^{m} S\iota(t_k)S$$

und für die $G = SO_N(\mathbb{F}_q)$ gilt:

$$G = \dot{\bigcup}_{0\leq k\leq \frac{m}{2}} S\iota(t_{2k})S.$$

Wir wenden nun den $\mathbb{C}$-Algebrenhomomorphismus:

$$\varphi : S\backslash G/S \to \mathrm{End}_{\mathbb{C}G}(\mathbb{1}_S^G)$$

auf die explizit gegebenen Doppelnebenklassenvertreter $\iota(t_k)$ $k = 0,\ldots,m$ an und finden:

5.3.13 Satz
$\varphi(S\iota(t_k)S) = A_k$.

Beweis:
Da G transitiv ist, genügt es, die Gleichheit der Bilder von e_{C_0} zu zeigen. Es ist $\iota(t_k)C_0 = \langle f_1, \ldots, f_k, e_{k+1}, \ldots, e_m\rangle =: C_k$. Ist $s \in S$ und $D := s(C_k)$ so ist $\dim(C_0/(D \cap C_0)) = k$. Umgekehrt gibt es nach dem Satz von Witt für jedes $D \in \mathcal{F}$ mit $\dim(C_0/(D \cap C_0)) = k$ ein $s \in S$ mit $s(C_k) = D$. Genauer: Wähle eine Basis $B = (c_1, \ldots, c_k, d_1, \ldots, d_k, b_{k+1}, \ldots b_m, a_{k+1} \ldots a_m)$ von $\mathbb{F}_q^N$ (bzw. $\mathbf{1}^\perp/\langle\mathbf{1}\rangle$) mit $\langle b_{k+1}, \ldots b_m\rangle = C_0 \cap D$ (bzw. $= C_0 \cap D/\langle\mathbf{1}\rangle$) $\langle c_1, \ldots, c_k, b_{k+1}, \ldots b_m\rangle = C_0$ (bzw. $C_0/\langle\mathbf{1}\rangle$) und $\langle d_1, \ldots, d_k, b_{k+1}, \ldots b_m\rangle = D$ (bzw. $D/\langle\mathbf{1}\rangle$). Dann kann man ein $g \in G$ definieren durch:

$$g : \begin{cases} e_i \mapsto c_i, & 1 \le i \le k \\ f_i \mapsto d_i, & 1 \le i \le k \\ e_i \mapsto b_i, & k+1 \le i \le m \\ f_i \mapsto a_i, & k+1 \le i \le m \end{cases}$$

Nach Definition ist $g(C_k) = D$ und $g(C_0) = C_0$ und somit $g \in S$. Also ist die S-Bahn von C_k genau

$$\{D \in \mathcal{F} \mid \dim(C_0/(D \cap C_0)) = k\} =: X$$

und

$$\varphi(St_kS) : e_{C_0} \mapsto \sum_{D \in X} e_D = A_k(e_{C_0}).$$

q.e.d.

Literaturverzeichnis

[BCP97] Bosma, W. ; Cannon, J. ; Playoust, C.: The Magma algebra system. I. The user language. In: *J. of Symbolic Comupation* 24 (1997), Nr. 3-4, S. 235–265

[Car85] Carter, R. W.: *Finite Groups of Lie Type.* Wiley, 1985

[CPS92] Conway, J. H. ; Pless, V. ; Sloane, N. J. A.: The Binary Self-Dual Codes of Length up to 32: A Revised Enumeration. In: *J. Combinatorial Theory, Series A* 60 (1992)

[Fre83] Freitag, E.: *Siegelsche Modulformen.* Springer-Verlag, 1983

[GN] Günther, A. ; Nebe, G.: *Automorphisms of doubly-even self-dual binary codes.* – erscheint in LMS Bulletin

[GRS06] G.Nebe ; Rains, E. M. ; Sloane, N. J. A.: *Self-dual codes and invariant theory.* Springer-Verlag, 2006

[Isa76] Isaacs, M.: *Character Theory of Finite Groups.* Academic Press, 1976

[KK07] Koecher, M. ; Krieg, A.: *Elliptische Funktionen und Modulformen.* 2. Auflage. Springer-Verlag, 2007

[Kne02] Kneser, M.: *Quadratische Formen.* Springer-Verlag, 2002

[Neb06] Nebe, G.: Kneser-Hecke-operators in coding theory. In: *Abh. Math. Sem. Univ. Hamburg* 76 (2006), S. 79–90

[Neb07] Nebe, G.: *Gitter und Codes.* SS 2007. – Vorlesungsskript, RWTH-Aachen

[NV01] Nebe, G. ; Venkov, B.: On Siegel modular forms of weight 12. In: *Journal für die reine und angewandte Mathematik* 531 (2001), S. 40–60

[Tay92] Taylor, D.: *The Geometry of the Classical Groups*. Heldermann, 1992

Erklärung

Hiermit versichere ich, dass ich die Aufgabenstellung selbständig bearbeitet und keine ausser den angegebenen Hilfsmitteln verwendet habe.

Aachen, 24. März 2009