Zyklenzeiger linearer Gruppen und Abzählung linearer Codes

Harald Fripertinger

Vortrag im Rahmen des 33. Séminaire Lotharingien de Combinatoire in der TU Bergakademie Freiberg vom 11. bis 17. September 1994

Abstract

Verfahren zur Berechnung der Zyklenzeiger der natürlichen Aktionen von linearen und projektiven Gruppen werden vorgeführt und bei der Bestimmung der Anzahl von Isometrieklassen linearer Codes angewendet.

Die Berechnung der *Zyklenzeiger linearer Gruppen* über dem endlichen Körper F_2 (bestehend aus zwei Elementen) und die Bestimmung der Anzahl von Klassen binärer *linearer* (n, k)*-Codes* erfolgte bereits Ende der 50-ger Jahre; siehe [10]; nun ist es interessant, Verallgemeinerungen davon auf beliebige endliche Körper F_q (mit $q = p_0^r$, p_0 eine Primzahl (die Charakteristik von F_q), q die Mächtigkeit des Körpers) zu untersuchen. Notation und Sprechweisen sind an [6] angepaßt.

1 Zyklenzeiger linearer Gruppen

Die Gruppe $\mathrm{GL}(k, F_q) := \{A \in M_k(F_q) \mid A^{-1} \text{ existiert}\}$ (die Gruppe aller regulären $k \times k$-Matrizen, bzw. aller Matrizen A mit $\det(A) \in F_q^* := F_q \setminus \{0\}$) operiert auf dem Vektorraum F_q^k

$$\mathrm{GL}(k, F_q) \times F_q^k \to F_q^k, \qquad (A, v) \mapsto Av$$

auf natürliche Weise. Nach Definition berechnet sich der *Zyklenzeiger* dieser Gruppenaktion als

$$Z(\mathrm{GL}(k, F_q), F_q^k) = \frac{1}{|\mathrm{GL}(k, F_q)|} \sum_{A \in \mathrm{GL}(k,F_q)} \prod_{i=1}^{q^k} x_i^{a_i(A)} \in \mathbb{Q}[x_1, x_2, \ldots],$$

wobei $(a_1(A), a_2(A), \ldots)$ der *Zykeltyp* der von A induzierten Permutation ist, d.h. diese Permutation zerfällt in $a_i(A)$ disjunkte Zykel der Länge i. Zur rationellen Bestimmung dieses Zyklenzeigers gehe man wie folgt vor:

1. Bestimmung der Konjugiertenklassen in $\mathrm{GL}(k, F_q)$.
2. Bestimmung der Mächtigkeit der Konjugiertenklassen.
3. Bestimmung des Zykeltyps eines Repräsentanten jeder Konjugiertenklasse. (Es ist bekannt, daß konjugierte Elemente vom gleichen Zykeltyp sind.)

1.1 Bestimmung der Konjugiertenklassen in $\mathrm{GL}(k, F_q)$

Die dafür benötigte Theorie ist die Theorie der *Normalformen* von Matrizen bzw. Vektorraumendomorphismen A, welche auf der Zerlegung eines Vektorraums in bezüglich A *zyklische Unterräume* aufbaut. Man spricht dann von *klassischen kanonischen Normalformen* oder *rational kanonischen Normalformen*. Diese sollen kurz erläutert werden: Sei $p(x) = \sum_{i=0}^{d} a_i x^i$ mit $a_d = 1$ ein normiertes Polynom in $F_q[x]$, dann ist die *Begleitmatrix* $B(p)$ von $p(x)$ definiert als folgende $d \times d$-Matrix:

$$B(p) := \begin{pmatrix} 0 & 0 & \dots & 0 & 0 & -a_0 \\ 1 & 0 & \dots & 0 & 0 & -a_1 \\ 0 & 1 & \dots & 0 & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 & -a_{d-2} \\ 0 & 0 & \dots & 0 & 1 & -a_{d-1} \end{pmatrix}.$$

Weiters ist die *Hyperbegleitmatrix* von $p^j(x)$ folgende Blockmatrix

$$H(p^j) := \left.\begin{pmatrix} B(p) & 0 & 0 & \dots & 0 & 0 \\ E_{1d} & B(p) & 0 & \dots & 0 & 0 \\ 0 & E_{1d} & B(p) & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & B(p) & 0 \\ 0 & 0 & 0 & \dots & E_{1d} & B(p) \end{pmatrix}\right\} j\text{-mal}.$$

Dabei ist

$$E_{1d} = (e_{ij})_{1 \le i,j \le d} \text{ mit } e_{ij} = \begin{cases} 1 & \text{falls } (i,j) = (1,d), \\ 0 & \text{sonst.} \end{cases}$$

Falls $\lambda = (\lambda_1, \lambda_2, \dots)$ einen Zykeltyp einer Zahl $c \in \mathbb{N}$ bezeichne, d.h. $c = \sum_i i\lambda_i$, so sei $D(p, \lambda)$ jene Blockdiagonalmatrix bestehend aus λ_1 Begleitmatrizen $B(p)$, λ_2 Hyperbegleitmatrizen $H(p^2)$ usw.

$$D(p, \lambda) = \mathrm{diag}(\underbrace{B(p), \dots, B(p)}_{\lambda_1}, \underbrace{H(p^2), \dots, H(p^2)}_{\lambda_2}, \dots).$$

Als Teiler des charakteristischen Polynoms von einem Vektorraumisomorphismus $A \in \mathrm{GL}(k, F_q)$ können alle über $F_q[x]$ irreduziblen normierten Polynome $p(x) \in$

$F_q[x]$ vom Grad kleiner gleich k auftreten mit Ausnahme des Polynoms $p(x) = x$. Man bestimme alle diese Polynome, bezeichne sie mit $p_1, p_2, \ldots$ und bestimme deren Grade $d_1, d_2, \ldots$. Um alle Konjugiertenklassen von $\mathrm{GL}(k, F_q)$ zu bestimmen, berechne man alle Lösungen $c = (c_1, c_2, \ldots)$ von

$$\sum_i c_i d_i = k,$$

und zu jeder Lösung bestimme man alle möglichen Zykeltypen

$$\lambda^{(i)} = (\lambda_1^{(i)}, \lambda_2^{(i)}, \ldots)$$

von c_i. Dann bilde man alle möglichen Blockdiagonalmatrizen der Form

$$\mathrm{diag}\left(D(p_1, \lambda^{(1)}), D(p_2, \lambda^{(2)}), \ldots\right).$$

In jeder Konjugiertenklasse liegt dann genau so eine Blockdiagonalmatrix. Im weiteren werden wir feststellen, daß man für die Berechnung des Zyklenzeigers von $\mathrm{GL}(k, F_q)$ nicht die genaue Gestalt der einzelnen Konjugiertenklassen kennen muß. Insbesondere muß man nicht die einzelnen über F_q irreduziblen Polynome bestimmen.

1.2 Bestimmung der Mächtigkeit der Konjugiertenklassen

Untersuchungen dieser Art gehen bereits auf DICKSON [2] zurück. Es ist dabei üblich aus der Mächtigkeit des *Zentralisators* von $A \in \mathrm{GL}(k, F_q)$ die Mächtigkeit der Konjugiertenklasse zu bestimmen. Bei KUNG [7] findet man folgendes Ergebnis: Sei $p(x) \in F_q[x]$ ein irreduzibles normiertes Polynom vom Grad d, und sei λ ein Zykeltyp von $c \in \mathbb{N}$, so kann die Anzahl der regulären Matrizen, die mit der Matrix $D(p, \lambda)$ kommutieren, als

$$b(d, \lambda) := \prod_{i=1}^{c} \prod_{j=1}^{\lambda_i} (q^{d\mu_i} - q^{d(\mu_i - j)})$$

berechnet werden, wobei

$$\mu_i := \sum_{k=1}^{i} k\lambda_k + \sum_{k=i+1}^{c} i\lambda_k.$$

Diese Zahl hängt nur von λ und vom Grad d des Polynoms, nicht jedoch von der speziellen Gestalt von $p(x)$ ab. Die Anzahl der mit

$$\mathrm{diag}(D(p_1, \lambda^{(1)}), D(p_2, \lambda^{(2)}), \ldots)$$

kommutierenden Matrizen ist dann

$$\prod_i b(d_i, \lambda^{(i)}).$$

1.3 Bestimmung des Zykeltyps eines Repräsentanten jeder Konjugiertenklasse

In jeder Konjugiertenklasse gibt es genau eine Matrix, die Blockdiagonalmatrix von Hyperbegleitmatrizen von über F_q irreduziblen Polynomen ist. Die Operation von $\mathrm{diag}(D(p_1,\lambda^{(1)}), D(p_2,\lambda^{(2)}),\ldots)$ auf F_q^k entspricht dem *direkten Produkt* der Operationen der einzelnen Diagonalblöcke auf gewissen Unterräumen von F_q^k, d.h. das direkte Produkt $\times_i \times_j \times_{k=1}^{\lambda_j^{(i)}} H(p_i^j)$ operiert auf $\times_i \times_j \times_{k=1}^{\lambda_j^{(i)}} F_q^{jd_i}$. Kennt man die Zykelstruktur von $H(p_i^j)$ auf $F_q^{jd_i}$, so kann man mit Hilfe einer bekannten Operation für Zykeltypen den Zykeltyp des direkten Produktes bestimmen. Diese Operation ist die in beiden Komponenten multiplikative und lineare Fortsetzung von

$$x_{i_1}^{j_1} \times x_{i_2}^{j_2} := x_{\mathrm{kgV}(i_1,i_2)}^{j_1 j_2\, \mathrm{ggT}(i_1,i_2)}$$

auf $\mathbb{Q}[x_1,x_2,\ldots]$. Für die Berechnung des Zykeltyps von $H(p^j)$ auf F_q^{jd} zeigt es sich, daß man den *Exponenten*, die *Periode* bzw. die *Ordnung* von $p(x)$ bestimmen muß. Dieser Exponent ist für Polynome mit $p(0) \neq 0$ durch

$$\exp(p) := \min\{n \in \mathbb{N} \mid p(x) \mid x^n - 1\}$$

definiert. Der Zykeltyp von $H(p^j)$ auf F_q^{jd}, wobei $p(x)$ ein irreduzibles, normiertes Polynom in $F_q[x]$ ist, ist dann gleich

$$x_1 \prod_{i=1}^{j} x_{e_i}^{(q^{id}-q^{(i-1)d})/e_i}$$

mit $e_i := \exp(p^i) = \exp(p)p^{t_i}$, wobei $t_i = \min\{n \in \mathbb{N}_0 \mid p_0^n \geq i\}$ und p_0 die Charakteristik von F_q ist.

Weiters kann man berechen, welche Zahlen als Exponenten von über F_q irreduziblen, normierten Polynomen vom Grad d auftreten können, und zu gegebenem Exponenten die Anzahl dieser Polynome bestimmen. Im Fall $d = e = 1$ gibt es 2 normierte Polynome vom Grad d mit Exponent e, nämlich $p(x) = x$ und $p(x) = x - 1$. Sonst gilt: Ist e ein Teiler von $q^d - 1$ und e teilt nicht $q^r - 1$ für $1 \leq r < d$, so gibt es $\varphi(e)/d$ irreduzible, normierte Polynome vom Grad d mit Exponent e in $F_q[x]$, wobei φ die Eulersche φ-Funktion ist. Dies zeigt nun, daß man nicht die einzelnen irreduziblen Polynome vom Grad kleiner gleich k bestimmen muß, um den Zyklenzeiger von $\mathrm{GL}(k, F_q)$ zu bestimmen.

Nun komme ich zum 2. Abschnitt meines Vortrags:

2 Abzählung linearer (n,k)-Codes

Ein *linearer* (n,k)-*Code* über dem Körper F_q ist ein k-dimensionaler Unterraum des Vektorraums F_q^n. Wie üblich schreibe ich die Codewörter $x \in F_q^n$ als

Zeilenvektoren $x = (x_1, \ldots, x_n)$. Oft wird ein (n,k)-Code C durch seine *Generatormatrix* gegeben. Diese ist eine $k \times n$-Matrix Γ, deren Zeilen eine Basis von C bilden, und es gilt dann

$$C = \left\{ x \cdot \Gamma \mid x \in F_q^k \right\}.$$

Zwei lineare (n,k)-Codes C_1, C_2 heißen äquivalent, falls es eine lineare *Isometrie* (bezüglich der *Hamming Distanz*) gibt, die C_1 auf C_2 abbildet. Dies kann mit Hilfe von Gruppenaktionen wie folgt formuliert werden: Es existiert $(\psi, \pi) \in F_q^* \wr S_{\underline{n}}$ mit $(\psi, \pi)(C_1) = C_2$. In dieser Situation ist es sinnvoll F_q^n mit der Menge $F_q^{\underline{n}}$, der Menge aller Abbildungen von $\underline{n} := \{1, 2, \ldots, n\}$ nach F_q, zu identifizieren. Das *Kranzprodukt* $F_q^* \wr S_{\underline{n}}$ operiert auf folgende Weise auf $F_q^{\underline{n}}$:

$$F_q^* \wr S_{\underline{n}} \times F_q^{\underline{n}} \to F_q^{\underline{n}}, \qquad ((\psi, \pi), f) \mapsto \psi(\cdot) f(\pi^{-1} \cdot).$$

Dieser Äquivalenzbegriff von Codes überträgt sich zu einem Äquivalenzbegriff für Generatormatrizen. Dazu seien Generatormatrizen $\Gamma \in M_{k,n}(F_q)$ als Funktionen

$$\Gamma : \underline{n} \to F_q^k \setminus \{0\}$$

aufgefaßt, wobei $\Gamma(i)$ die i-te Spalte von Γ ist. (Ich untersuche nur Matrizen ohne 0-Spalten.) Obige Gruppenaktion schreibt sich nun zu folgender Gruppenaktion auf der Menge aller $k \times n$-Matrizen (unabhängig von deren Rang) um:

$$(\mathrm{GL}(k, F_q) \times F_q^* \wr S_{\underline{n}}) \times (F_q^k \setminus \{0\})^{\underline{n}} \to (F_q^k \setminus \{0\})^{\underline{n}}$$

$$((A, (\psi, \pi)), \Gamma) \mapsto A\psi(\cdot)\Gamma(\pi^{-1} \cdot).$$

Dem Konzept von SLEPIAN folgend, sei S_{nkq} die Anzahl der Äquivalenzklassen von linearen (n,k)-Codes über F_q, die keine 0-Spalten enthalten, das heißt für jedes $i \in \underline{n}$ gibt es ein Codewort x, sodaß $x_i \neq 0$. Die Anzahl der Äquivalenzklassen *injektiver Codes* sei mit $\bar{S}_{nkq}$ bezeichnet. Ein Code heißt injektiv, falls es für alle $i, j \in \underline{n}$ mit $i \neq j$ und für alle $\alpha \in F_q^*$ ein Codewort x gibt, sodaß $x_i \neq \alpha x_j$. Weiters sei T_{nkq} die Anzahl der Bahnen von $k \times n$-Matrizen ohne 0-Spalten über F_q und $\bar{T}_{nkq}$ die Anzahl der Bahnen von $k \times n$-Matrizen Γ mit der Eigenschaft, daß für alle $i, j \in \underline{n}$ mit $i \neq j$ und für alle $\alpha \in F_q^*$ der Vektor $\Gamma(i)$ verschieden ist von $\alpha\Gamma(j)$. Von den Matrizen, die zur Berechnung von T_{nkq} bzw. $\bar{T}_{nkq}$ herangezogen werden, wird aber nicht verlangt, daß ihr Rang gleich k ist. Es gilt

$$S_{nkq} = T_{nkq} - T_{n,k-1,q}$$

$$\bar{S}_{nkq} = \bar{T}_{nkq} - \bar{T}_{n,k-1,q}$$

mit den Anfangsbedingungen $S_{n1q} = 1$ für $n \in \mathbb{N}$, $\bar{S}_{11q} = 1$ und $\bar{S}_{n1q} = 0$ für $n > 1$.

Im Fall $q = 2$ wird aus dem Kranzprodukt $F_q^* \wr S_{\underline{n}}$ die Gruppe $S_{\underline{n}}$, es bleibt somit genau eine Gruppe übrig, die auf $F_q^k \setminus \{0\}$ operiert und genau eine Gruppe, die auf $\underline{n}$ operiert. Da auf dem Definitionsbereich die symmetrische Gruppe operiert, erhält man durch geeignete Substitution in dem Zyklenzeiger von $\mathrm{GL}(k, F_2)$ auf $F_2^k \setminus \{0\}$ die Anzahl der $S_{\underline{n}} \times \mathrm{GL}(k, F_2)$-Bahnen solcher Funktionen Γ (siehe [1]). Man erhält

$$\sum_{n=0}^{\infty} T_{nk2} x^n = Z\left(\mathrm{GL}(k, F_2), F_2^k \setminus \{0\} \,|x_i = \sum_{j=0}^{\infty} x^{ij}\right) =$$

$$= Z\left(\mathrm{GL}(k, F_2), F_2^k \setminus \{0\} \,|x_i = \frac{1}{1 - x^i}\right)$$

und

$$\sum_{n=0}^{\infty} \bar{T}_{nk2} x^n = Z\left(\mathrm{GL}(k, F_2), F_2^k \setminus \{0\} \,|x_i = 1 + x^i\right).$$

Im Fall $q \neq 2$ operiert das Kranzprodukt $F_q^* \wr S_{\underline{n}}$ sowohl von rechts, als auch von links auf der Menge aller Abbildungen $(F_q^k \setminus \{0\})^{\underline{n}}$. Auf LEHMANN [8, 9] geht die folgende Bijektion Φ zurück:

$$\Phi \colon F_q^* \wr S_{\underline{n}} \backslash\backslash (F_q^k \setminus \{0\})^{\underline{n}} \to S_{\underline{n}} \backslash\backslash \left(F_q^* \backslash\backslash (F_q^k \setminus \{0\})\right)^{\underline{n}}$$

$$\Phi(F_q^* \wr S_{\underline{n}}(\Gamma)) = S_{\underline{n}}(\bar{\Gamma}),$$

wobei

$$\bar{\Gamma} \colon \underline{n} \to F_q^* \backslash\backslash (F_q^k \setminus \{0\}), \qquad i \mapsto F_q^*(\Gamma(i))$$

und wobei $S_{\underline{n}}$ auf $F_q^* \backslash\backslash (F_q^k \setminus \{0\})^{\underline{n}}$ nach der Definition $(\pi, \bar{\Gamma}) \mapsto \bar{\Gamma} \circ \pi^{-1}$ operiert. Diese Bijektion erlaubt das Problem wie folgt umzuformulieren:

$$\left(S_{\underline{n}} \times \mathrm{GL}(k, F_q)\right) \times \left(F_q^* \backslash\backslash (F_q^k \setminus \{0\})\right)^{\underline{n}} \to \left(F_q^* \backslash\backslash (F_q^k \setminus \{0\})\right)^{\underline{n}}$$

$$\left((\pi, A), \bar{\Gamma}\right) \mapsto A \bar{\Gamma} \pi^{-1},$$

wobei die Gruppe $\mathrm{GL}(k, F_q)$ auf $F_q^* \backslash\backslash (F_q^k \setminus \{0\})$ nach folgender Definition operiert:

$$(A, F_q^*(v)) \mapsto F_q^*(Av).$$

Die Menge der F_q^*-Orbiten $F_q^* \backslash\backslash (F_q^k \setminus \{0\})$ ist der $(k-1)$-dimensionale *projektive Raum* $\mathrm{PG}(k-1, F_q)$ und die Permutationsdarstellung von $\mathrm{GL}(k, F_q)$ ist die *projektive lineare Gruppe* $\mathrm{PGL}(k, F_q)$. Kennt man also den Zyklenzeiger von $\mathrm{PGL}(k, F_q)$, so kann man wie im Fall $q = 2$ vorgehen und die Anzahl der Klassen linearer (n, k)-Codes bestimmen. Für die Bestimmung der T_{nkq} bzw. $\bar{T}_{nkq}$ erhält man folgende Formeln:

$$\sum_{n=0}^{\infty} T_{nkq} x^n = Z\left(\mathrm{PGL}(k, F_q), \mathrm{PG}(k-1, F_q) | x_i = \sum_{j=0}^{\infty} x^{ij}\right) =$$

$$= Z\left(\mathrm{PGL}(k,F_q),\mathrm{PG}(k-1,F_q)|x_i=\frac{1}{1-x^i}\right),$$

$$\sum_{n=0}^{\infty}\bar{T}_{nkq}x^n = Z\left(\mathrm{PGL}(k,F_q),\mathrm{PG}(k-1,F_q)|x_i=1+x^i\right).$$

Zur Berechnung dieses Zyklenzeigers geht man analog wie bei der Berechnung des Zyklenzeigers von $\mathrm{GL}(k,F_q)$ vor. Nur die Berechnung des Zykeltyps muß abgeändert werden. Man berechnet den sogenannten *Subzykeltyp* von $A \in \mathrm{GL}(k,F_q)$. Ein Vektor $v \in F_q^k \setminus \{0\}$ liegt in einem Subzykel der Länge j, falls j die kleinste natürliche Zahl ist, für die ein $\alpha \in F_q^*$ existiert, sodaß $A^n v = \alpha v$. Für die Berechnung von Subzykellängen benötigt man den *Subexponenten* bzw. die *integrale Ordnung* eines Polynoms $p(x) \in F_q[x]$ mit $p(0) \neq 0$. Dieser ist definiert durch

$$\mathrm{subexp}(p) := \min\left\{t \in \mathbb{N} \mid \exists \alpha_0 \in F_q \text{ sodaß } p(x) \mid x^t - \alpha_0\right\}.$$

Das Element α_0 heißt auch *integrales Element* von $p(x)$ (und ist für Polynome mit $p(0)\neq 0$ eindeutig bestimmt). Sei $p(x)$ ein irreduzibles, normiertes Polynom vom Grad d mit Subexponent e und integralem Element $\alpha_0 \in F_q^*$, dann hat die Matrix $H(p^j)$ den Subzykeltyp

$$\prod_{i=1}^{j} x_{e_i,\alpha_0^{e_i/e}}^{(q^{id}-q^{(i-1)d})/e_i},$$

wobei $e_i = \mathrm{subexp}(p^i) = ep^{t_i}$ mit $t_i = \min\{n \in \mathbb{N}_0 \mid p_0^n \geq i\}$. Wie vorne bezeichnet p_0 die Charakteristik von F_q. Die Unbestimmten sind mit 2 Indizes versehen: der erste beinhaltet die Subzykellänge, der zweite ist das zugehörige integrale Element. Überdies ist der Exponent von $x_{i,\alpha}$ stets durch $q-1$ teilbar.

In einem zweiten Schritt muß man eine Verallgemeinerung des direkten Produktes von Zyklenzeigern zu einem direkten Produkt von Subzyklenzeigern angeben. Dies erfolgt durch

$$x_{i_1,\beta^{r_1}}^{j_1} \otimes x_{i_2,\beta^{r_2}}^{j_2} := x_{i_1,\beta^{r_1}}^{j_1} x_{i_2,\beta^{r_2}}^{j_2} x_{i_3,\beta^{r_3}}^{j_3}.$$

Dabei ist $F_q^* = \langle\beta\rangle$ und

$$i_3 = \mathrm{kgV}(i_1,i_2)\frac{q-1}{\mathrm{ggT}\,(q-1,\mathrm{kgV}(i_1,i_2)r_1/i_1 - \mathrm{kgV}(i_1,i_2)r_2/i_2)}$$

$$r_3 \equiv \frac{r_1 i_3}{i_1} \equiv \frac{r_2 i_3}{i_2} \bmod q-1$$

und

$$j_3 = \frac{i_1 j_1 i_2 j_2}{i_3}.$$

Setzt man $\otimes$ linear und multiplikativ in beiden Komponenten fort, so berechnet man den Subzykeltyp von $\mathrm{diag}(A_1,A_2)$ als $\otimes$-Verknüpfung der Subzykeltypen von A_1 und A_2. Auf diese Weise bestimmt man den *Subzyklenzeiger* von $\mathrm{GL}(k, F_q)$ auf $F_q^k \setminus \{0\}$ als Summe der Subzykeltypen aller Elemente von $\mathrm{GL}(k, F_q)$ geteilt durch die Gruppenordnung. Streicht man dann die Indizes α in $x_{i,\alpha}$ und teilt man die Exponenten von x_i durch $q-1$ (d.h. man faßt jeweils $q-1$ Vektoren $\{v, \beta v, \ldots, \beta^{q-2} v\} = \langle\beta\rangle(v) = F_q^*(v)$ zu einem Element von $\mathrm{PG}(k-1, F_q)$ zusammen), so erhält man den Zyklenzeiger von $\mathrm{PGL}(k, F_q)$. Zur Bestimmung der Subexponenten und integralen Elemente von über F_q irreduziblen, normierten Polynomen sei noch folgendes erwähnt: Sei $e > 1$ ein Teiler von $q^d - 1$ und e teile nicht $q^r - 1$ für $1 \leq r < d$. Sei weiters $h := \mathrm{ggT}(q-1, e)$, dann gilt: Für jedes $\alpha \in F_q^*$ mit multiplikativer Ordnung h gibt es genau

$$\frac{\varphi(e)}{d\varphi(h)}$$

verschiedene irreduzible, normierte Polynome $p(x) \in F_q[x]$ vom Grad d mit Exponent e und Subexponent e/h und integralem Element α.

Damit ist es möglich wie vorne beschrieben den Zyklenzeiger von $\mathrm{PGL}(k, F_q)$ zu bestimmen und somit auch die Anzahl der Klassen linearer (n, k)-Codes über beliebigen endlichen Körpern F_q zu ermitteln. Die hier vorgeführten Verfahren wurden bereits in SYMMETRICA (einem Computer Algebra System zur Darstellungstheorie und Kombinatorik der symmetrischen Gruppen und anderer Gruppen) programmiert und zur Abzählung linearer Codes verwendet. Als kleine Illustration der Leistungsfähigkeit der in [4] vorgestellten Algorithmen seien die Zahlen der Isometrie Klassen linearer (n, k)-Codes über F_q für $q = 3$ und 4 angegeben.

Eine genauere Darstellung der hier vorgetragenen Themen sind in [3] und [5] geplant.

References

[1] N.G. De Bruijn. Pólya's Theory of Counting. In E.F. Beckenbach, Editor, *Applied Combinatorial Mathematics*, Kapitel 5, Seiten 144 – 184. Wiley, New York, 1964.

[2] L.E. Dickson. *Linear Groups*. Dover Publications, Inc., New York, 1958.

[3] H. Fripertinger. Cycle indices of linear, affine and projective groups. Nicht veröffentlicht.

[4] H. Fripertinger. Enumeration of isometry classes of linear (n, k)-codes over $GF(q)$ in SYMMETRICA. *Bayreuther Mathematische Schriften*, 49:215 – 223, 1995. ISSN 0172-1062.

[5] H. Fripertinger und A. Kerber. Isometry classes of indecomposable codes. G.Cohen,M.Giusti,T.Mora (eds.),*Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, LNCS 948, 1995, pp.194-202.

[6] A. Kerber. *Algebraic Combinatorics via Finite Group Actions.* B. I. Wissenschaftsverlag, Mannheim, Wien, Zürich, 1991. ISBN 3-411-14521-8.

[7] J.P.S. Kung. The Cycle Structure of a Linear Transformation over a Finite Field. *Linear Algebra and its Applications*, 36:141 – 155, 1981.

[8] H. Lehmann. Das Abzähltheorem der Exponentialgruppe in gewichteter Form. *Mitteilungen aus dem Mathem. Seminar Giessen*, 112:19 – 33, 1974.

[9] H. Lehmann. *Ein vereinheitlichender Ansatz für die REDFIELD – PÓLYA – de BRUIJNSCHE Abzähltheorie.* Dissertation, Universität Giessen, 1976.

[10] D. Slepian. Some Further Theory of Group Codes. *The Bell System Technical Journal*, 39:1219 – 1252, 1960.

Table 1: Number of isometry classes of linear (n,k)-codes over F_3, where columns of zeros are not allowed.

$n\backslash k$	1	2	3	4	5	6	7
1	1	0	0	0	0	0	0
2	1	1	0	0	0	0	0
3	1	2	1	0	0	0	0
4	1	4	3	1	0	0	0
5	1	5	8	4	1	0	0
6	1	8	19	15	5	1	0
7	1	10	39	50	24	6	1
8	1	14	78	168	118	37	7
9	1	17	151	538	628	255	53
10	1	22	280	1789	3759	2266	518
11	1	26	506	5981	26131	28101	7967
12	1	33	904	20502	208045	500237	230165
13	1	38	1571	70440	1.788149	11.165000	11.457192
14	1	46	2687	241252	15.675051	269.959051	734.810177
15	1	53	4520	812381	135.088306	6509.617382	50106.349550
16	1	63	7474	2.674456	1123.937633	151407.115499	3.365565.864529
17	1	71	12156	8.562016	8961.374245	3.358439.044687	216.942933.517425
18	1	83	19491	26.612531	68333.073432	70.853158.173793	13315.081085.011815
19	1	93	30763	80.233923	498519.876882	1422.491253.596747	777125.587904.335661

Table 2: Number of isometry classes of injective linear (n, k)-codes over F_3, where columns of zeros are not allowed.

$n\backslash k$	1	2	3	4	5	6	7
1	1	0	0	0	0	0	0
2	0	1	0	0	0	0	0
3	0	1	1	0	0	0	0
4	0	1	2	1	0	0	0
5	0	0	3	3	1	0	0
6	0	0	4	8	4	1	0
7	0	0	4	19	15	5	1
8	0	0	3	44	61	26	6
9	0	0	3	91	277	162	40
10	0	0	2	199	1439	1381	375
11	0	0	1	401	8858	17200	5923
12	0	0	1	806	62311	311580	182059
13	0	0	1	1504	459828	6.876068	9.427034
14	0	0	0	2659	3.346151	159.373844	608.045192
15	0	0	0	4304	23.246482	3609.085016	40932.394177
16	0	0	0	6472	152.150717	77820.525594	2.689924.561256
17	0	0	0	8846	934.417218	1.585853.806095	168.808656.255926
18	0	0	0	11127	5384.092498	30.517085.050170	10054.654260.189282
19	0	0	0	12723	29148.064514	555.334469.037874	568100.206087.336919

Table 3: Number of isometry classes of linear (n, k)-codes over F_4, where columns of zeros are not allowed.

$n\backslash k$	1	2	3	4	5	6	7
1	1	0	0	0	0	0	0
2	1	1	0	0	0	0	0
3	1	2	1	0	0	0	0
4	1	4	3	1	0	0	0
5	1	6	9	4	1	0	0
6	1	9	24	17	5	1	0
7	1	12	55	70	28	6	1
8	1	17	131	323	189	44	7
9	1	22	318	1784	1976	490	65
10	1	30	772	12094	36477	13752	1240
11	1	37	1881	89437	923978	948361	102417
12	1	48	4568	668922	25.124571	91.149571	25.983495
13	1	59	10857	4.843901	665.246650	9163.203790	9229.228790
14	1	74	25276	33.456545	16677.221922	887802.519854	3.433862.618525
15	1	90	57340	219.445013	393513.820272	81.226850.913333	1235.275542.789440
16	1	110	126546	1367.508687	8.746404.847560	6995.509895.858546	420983.966000.848855
17	1	131	271821	8112.982336	183.604673.384799	568026.309364.649897	135.464277.950330.542478
18	1	158	568714	45940.917668	3651.189061.424972	43.605786.853186.808968	41211.648695.055403.242662
19	1	186	1.159878	248958.221585	68984.762728.576459	3173.908501.513177.711047	11.882925.353489.748367.899821

Table 4: Number of isometry classes of injective linear (n, k)-codes over F_4, where columns of zeros are not allowed.

$n\backslash k$	1	2	3	4	5	6	7
1	1	0	0	0	0	0	0
2	0	1	0	0	0	0	0
3	0	1	1	0	0	0	0
4	0	1	2	1	0	0	0
5	0	1	4	3	1	0	0
6	0	0	8	10	4	1	0
7	0	0	10	35	19	5	1
8	0	0	13	136	122	33	6
9	0	0	17	657	1320	376	52
10	0	0	19	3849	25619	11632	1057
11	0	0	19	23456	645751	845949	95960
12	0	0	17	138200	16.822798	81.806606	25.058580
13	0	0	13	761039	418.686704	8140.667601	8935.079862
14	0	0	10	3.880522	9757.619492	775867.907732	3.317031.738218
15	0	0	8	18.294487	212356.023661	69.608988.504682	1188.156545.352085
16	0	0	5	79.884393	4.324364.325987	5866.545477.361639	402824.242293.156876
17	0	0	3	323.922715	82.656563.598884	465371.337968.846503	128.876144.128834.834992
18	0	0	2	1223.091788	1487.726907.561588	34.847717.443512.158622	38965.296608.277082.280167
19	0	0	1	4311.839430	25290.829421.058624	2470.448907.990450.018140	11.161512.263255.300041.612255

Adresse: Harald Fripertinger
Institut für Mathematik
Karl-Franzens-Universität Graz
Heinrichstr. 36/4
A–8010 Graz
Austria
e-mail: `harald.fripertinger@balu.kfunigraz.ac.at`