

# Vorlesung Symmetrische Gruppen

## §1. Kartenmischen - mathematisches Modell

### 1.1 Definition

Out-shuffle Out ist das eindeutige Element der  $\Sigma_N$  (symmetrische Gruppe) mit

$$Out(k) \equiv 2k \pmod{(N-1)} \text{ für } N \text{ gerade, } 0 \leq k < N-1$$

$$Out(k) \equiv 2k \pmod{N} \text{ für } N \text{ ungerade, } 0 \leq k \leq N-1, 0(N-1) = N \dots$$

In Shuffle In ist das eindeutige Element der  $\Sigma_N$  (symmetrische Gruppe) mit

$$In(k) \equiv 2k+1 \pmod{(N+1)} \text{ für } N \text{ gerade}$$

$$In(k) \equiv 2k+1 \pmod{N} \text{ für } N \text{ ungerade}$$

G Gruppe,  $g \in G$ :  $\text{ord}(g) = \underline{\text{Ordnung}}$  von  $g = \min \{\ell \in \mathbb{N} : g^\ell = 1\}$  oder  $\infty$ , falls kein  $\ell$  existiert.

Die Ordnung eines Gruppenelements teilt die Gruppenordnung.

$(\mathbb{Z}/m\mathbb{Z})^* = \{\bar{k} : 0 < k \leq m \text{ mit } \text{ggT}(k, m) = 1\}$  bildet eine Gruppe (bezüglich Multiplikation), die prime Restklassengruppe modulo m. Die Ordnung (Elementanzahl) von  $(\mathbb{Z}/m\mathbb{Z})^*$  ist die Anzahl der zu  $m$  teilerfremden natürlichen Zahlen zwischen 0 und  $m$ . Diese Zahl wird mit  $\varphi(m)$  bezeichnet (Eulers Phi-Funktion).

$$p \text{ Primzahl} \Rightarrow \varphi(p) = p - 1$$

$$p \text{ Primzahl, } d \geq 1 \Rightarrow \varphi(p^d) = p^d \left(1 - \frac{1}{p}\right) = p^d - p^{d-1}$$

$$m = p^{d_1} \dots p^{d_k} \Rightarrow \varphi(m) = m \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right) = (p_1^{d_1} - p_1^{d_1-1}) \dots (p_k - p_{d_{k-1}})$$

### 1.2 Theorem

Sei  $N = 2n$ . Dann gilt  $\text{ord}(Out) = \text{ord}(\bar{2})$  in  $(\mathbb{Z}/N-1)^*$ .

### 1.3 Proposition

$$\text{ord}_{\Sigma_{2n-1}}(Out) = \text{ord}_{\Sigma_{2n}}(Out)$$

$$\text{ord}_{\Sigma_{2n-1}}(In) = \text{ord}_{\Sigma_{2n}}(Out)$$

$$\text{ord}_{\Sigma_{2n-2}}(In) = \text{ord}_{\Sigma_{2n}}(Out)$$

### 1.4 Proposition

$$\text{Schreibe } Shu(k) = 2k + \delta, \delta = \begin{cases} 0, & Shu = Out \\ 1, & Shu = In \end{cases}$$

Sei  $N = 2n - 1$ , und seinen  $S_1, \dots, S_k$  In- oder beliebig gewählte Out-Shuffles.

$$\Rightarrow S_k \circ \dots \circ S_1(j) \equiv 2^k j + \sum_{i=1}^k 2^{k-i} \delta(S_i) \pmod{N}.$$

**1.5 Definition**

Das einfache Abheben bei  $N$  Karten ist die Permutation  $C$  mit  $C(k) \equiv k-1 \pmod N$  ( $C$ : simple cut).

**1.6 Theorem** (Golomb 1961):

$$N = 2n \Rightarrow \langle Out, C \rangle = \Sigma_n$$

Also:  $Out$  und  $C$  erzeugen jede beliebige Anordnung der Karten, das ist also fair!

**Definition**

Seien  $N, H$  Gruppen,  $\theta : H \rightarrow \text{Aut}(N)$  ein Gruppenhomomorphismus, wobei  $\text{Aut}(N) = \{\alpha : N \rightarrow N \text{ Gruppenisomorphismus}\}$   
 Setze  $S = N \times H$  als Menge mit Multiplikation.

$$(n_1, h_1) \cdot (n_2, h_2) = \left( \underbrace{n_1 \cdot \theta(h_1)(n_2)}_{\text{in } N}, \underbrace{h_1 h_2}_{\text{in } H} \right)$$

dann ist  $S$  eine Gruppe, das semidirekte Produkt von  $N$  und  $H$ .  
 Bezeichnung:  $S = N \rtimes H$ .

**1.7 Theorem** (Golomb, 1961)

Sei  $N = 2n-1$ . Dann gilt:

$$\langle Out, C \rangle = \langle C \rangle \rtimes \langle Out \rangle,$$

$$\text{insbesondere: } |\langle Out, C \rangle| = |\langle C \rangle| \cdot |\langle Out \rangle| = N \cdot \text{ord}_{\Sigma_N}(Out).$$

**§2. Permutationen, Young-Diagramme, Tableaux und Flugzeug-Passagiere****2.1 Definition**

Sei  $\pi \in \Sigma_n$ , und sei  $\pi(1) \pi(2) \cdots \pi(n)$  das aus den Bildwerten gebildete Wort.

Eine aufsteigende Bilderfolge von  $\pi$  ist eine Indexfolge  $i_1 < i_2 < \cdots < i_k$  mit  $\pi(i_1) < \pi(i_2) < \cdots < \pi(i_k)$ .  $k$  heißt die Länge der aufsteigenden Teilfolge ( $1 \leq k \leq n$ ).

$is(\pi)$ : = Länge der längsten aufsteigenden Teilfolge

$ds(\pi)$ : = Länge der längsten absteigenden Teilfolge

**2.2 Theorem** (Erdős + Szekeres, 1935)

Seien  $p, q \in \mathbb{N}$ ,  $\pi \in \Sigma_{p \cdot q + 1}$ . Dann gilt  $is(\pi) > p$  oder  $ds(\pi) > q$ .

**2.3 Definition**

Sei  $n \in \mathbb{N}$ , eine Komposition von  $n$  ist eine endliche Folge  $\lambda = (\lambda_1, \lambda_2, \cdots, \lambda_l)$  mit

$$\sum_{i=1}^l \lambda_i = n.$$

Eine Partition ist eine Komposition mit schwach absteigenden Einträgen  $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_l > 0$  (immer alle  $\lambda_i \in \mathbb{N}$ ). Schreibweise:  $\lambda \vdash n$  heißt  $\lambda$  ist eine Partition von  $n$ .  $\Lambda = \{\text{Kompositionen von } n\}$  (bei festem  $n$ , ist  $\Lambda^+ = \{\text{Partitionen}\}$ ).

Veranschaulichung durch Young-Diagramme

$$(4,1) \leftrightarrow \begin{array}{|c|c|c|c|} \hline \square & \square & \square & \square \\ \hline \square & & & \\ \hline \end{array}$$

$$(2,2,1) \leftrightarrow \begin{array}{|c|c|} \hline \square & \square \\ \hline \square & \square \\ \hline \square & \\ \hline \end{array}$$

allgemein  $\lambda : (\lambda_1, \dots, \lambda_l) \leftrightarrow$  Diagramm mit  $l$  Zeilen, mit  $\lambda_i$  Boxen in Zeile  $i$

## 2.4 Definition

Sei  $\lambda \vdash n, Y(\lambda)$  das Young-Diagramm von  $\lambda$ . Ein Tableau  $t$  der Form  $\lambda$  ist eine injektive Abbildung  $\{1, \dots, n\} \rightarrow$  Boxen von  $Y(\lambda)$ .  $t$  heißt Standard-Tableau, wenn in den Zeilen und Spalten aufsteigende Folgen stehen.

## 2.5 Theorem

Sei  $n \in \mathbb{N}$ , dann gilt  $\sum_{\lambda \in \Lambda^+(n)} |\{t : \text{Standard-Tableau der Form } \lambda\}|^2 = n!$  Also gibt es eine Bijektion zwischen den Elementen der  $\Sigma_n$  und Paaren von Standard-Tableaux, beide von der Form  $\lambda, \lambda \in \Lambda^+(n)$ .

## 2.6 Theorem (Schützenberger, 1961)

Sei  $\pi \in \Sigma_n, \pi \xrightarrow{\text{RSK}} (\lambda, P, Q)$ . Dann gilt:

- (a)  $is(\pi) = \lambda_1$
- (b)  $ds(\pi) = \lambda'_1$

## 2.7 Proposition

Für  $\pi = x_1 \cdots x_n$  sei  $\pi^r := x_n \cdots x_1$ . Dann gilt  $\lambda(\pi^r) = \lambda(\pi)^t =$  Transposition von  $\lambda(\pi)$  und  $P(\pi^r) = P(\pi)^t$

## 2.8 Theorem (Schützenberger, 1963)

Für  $\pi \in \Sigma_n$  gilt

$$P(\pi^{-1}) = Q(\pi) \text{ und } Q(\pi^{-1}) = P(\pi)$$

## 2.9 Proposition (Viennot, 1976)

$$\pi \xrightarrow{\text{RSK}} (P, Q) \text{ mit Schattendiagramm } \{L_1, x_i, y_i\} \Rightarrow \forall j : P_{1,j} = y_{L_j} \text{ und } Q_{1,j} = x_{L_j}$$

**2.10 Theorem** (Viennot, 1976)

Für  $\pi \xleftrightarrow{\text{RSK}} (P, Q)$  gilt :  $\pi^{(i)} \xleftrightarrow{\text{RSK}} (P^{(i)}, Q^{(i)})$  und  $P_{i,j} = y_{L_j}^{(i)}, Q_{i,j} = x_{L_j}^{(i)} \forall i, j$

**2.11 Korollar** (Schensted, 1961)

Für den Erwartungswert (der Wartezeit)  $E(n) = \frac{1}{n!} \sum_{w \in \Sigma_n} is(w)$  gilt  
 $E(n) = \left( \sum_{\lambda \vdash n} \lambda_1 (f^\lambda)^2 \right) \cdot \frac{1}{n!}$

**§ 3. Kombinatorische Verteilungen****3.1 Definition**

Für  $\pi \in \Sigma_n$  sei  $c_i(\pi) := \#$  Zyklen der Länge  $i$ .  $(c_1, \dots, c_n)$  heißt der Zyklentyp von  $\pi$ , oder Zyklusstruktur.

**3.2 Proposition**

Zu gegebenem Zyklentyp  $(c_1, \dots, c_n)$  gibt es

$$\frac{n!}{(1^{c_1} c_1! 2^{c_2} c_2! \dots, n^{c_n} c_n)}$$

viele  $\pi \in \Sigma_n$  von diesem Typ.

**3.3 Definition**

Sei  $c(n, \cdot) := \#\{\pi \in \Sigma_n : \pi \text{ hat genau } k \text{ Zyklen}\}$ ,  $s(n, k) := (-1)^{n-k} c(n, k)$ . Die Zahlen  $s(n, k)$  heißen Stirling-Zahlen erster Art, die  $c(n, k)$  heißen vorzeichenlose Stirling-Zahlen erster Art.

**3.4 Proposition**

Es gilt die Rekursionsformel

$$c(n, k) = (n-1) c(n-1, k) + c(n-1, k-1) \forall n, k \geq 1$$

**3.5 Proposition:**

Für eine Unbestimmte  $x$  und  $n \geq 0$  gilt:

$$\sum_{k=0}^n c(n, k) x^k = x(x+1)(x+2) \dots (x+n-1)$$

**3.6 Definition**

Sei  $\pi \in \Sigma_n, \pi = (a_1 a_2 \dots a_n)$ . Die Descent-Menge (Abstiegsmenge) von  $\pi$

$$D(\pi) = \{i | a_i > a_{i+1}\}, d(\pi) := |D(\pi)|$$

$$A(n, k) := \#\{\pi \in \Sigma_n : d(\pi) = k-1\}$$

Für  $S \subseteq \{1, \dots, n-1\}$  ( $n \notin D(\pi)$  ist  $\alpha(S) = \#\{\pi : D(\pi) \subseteq S\}$  und  $\beta(S) = \#\{\pi : D(\pi) = S\}$ )

### 3.7 Proposition

Sei  $S = \{s_1 < s_2 < \dots < s_k\} \subseteq \{1, \dots, n-1\}$ .

Dann gilt

$$\alpha(S) = \binom{n}{s_1, s_2 - s_1, s_3 - s_2, \dots, n - s_k}$$

(= Multinomialkoeffizient)

### 3.8 Definition

$$A_n(x) := \sum_{\pi \in \Sigma_n} x^{1+d(\pi)}$$

heißt ein Eulersches Polynom also

$$A_n(x) = \sum_{k=1}^n A(n, k)x^k,$$

deshalb heißt  $A(n, k)$  eine Eulersche Zahl

### 3.9 Proposition

$$\begin{aligned} A(n, k+1) &= \#\{\pi \in \Sigma_n : \#\{i : \pi(i) \geq i\} = K+1\} \\ &= \#\{\pi \in \Sigma_n : \#\{i : \pi(i) > i\} = K\} \end{aligned}$$

### 3.10 Proposition

(a) Seien  $i \neq j$  in  $\{1, \dots, n\}$ ,  $\pi$  eine zufällige Permutation in  $\Sigma_n$ . Schreibe  $\pi$  in Zyklen. Die Wahrscheinlichkeit, daß  $i$  und  $j$  im selben Zyklus von  $\pi$  liegen ist  $\frac{1}{2}$ .

(b) Seien  $i, k \in \{1, \dots, n\}$ ,  $\pi$  zufällig in  $\Sigma_n$ , wieder  $\pi$  in Zyklen geschrieben. Die Wahrscheinlichkeit, daß  $i$  in einem  $k$ -Zyklus (d.h. in einem Zyklus der Länge  $k$ ) von  $\pi$  liegt, ist  $\frac{1}{n}$  (also unabhängig von  $k$ ).

### 3.11 Definition

Sei  $\lambda \vdash n$ ,  $Y(\lambda)$  das Young-Diagramm (= Ferrer Diagramm) von  $\lambda$ ,  $b$  eine Box. Der Haken  $H_b$  von  $b$  besteht aus  $b$  und allen Boxen rechts von  $b$  in derselben Zeile und allen Boxen unterhalb von  $b$  in derselben Spalte.  $h_b := \#\{\text{Boxen in } H_b\}$

### 3.12 Theorem (Hakenformel; Frame, Robinson und Thrall 1953)

$$f^\lambda = \#\{\text{standard Young tableaux der Form } \lambda\} = n! \frac{n!}{\prod_{b \text{ Box in } Y(\lambda)} h_b}$$

## § 4. Aufsteigende Teilfolgen, statistische Verteilungen und Analysis

Spiel: Patience-Sortieren

Naive Strategie (greedy, gefräßig):

Stapel von links nach rechts (neue immer rechts anschließen), neue Karte möglichst weit links platzieren.

### 4.1 Proposition

Seien  $n$  Karten gegeben, gemischt durch  $\pi \in \Sigma_n$  (also oberste Karte  $\pi(1)$  usw). Dann produziert die gefräßige Strategie  $is(\pi)$  Stapel und das ist optimal.

### 4.2 Theorem (Baik - Deift - Johansson, 1999):

Für  $t \in \mathbb{R}$ ,  $\pi \in \Sigma_n$  gleichmäßig verteilt, gilt

$$\lim_{n \rightarrow \infty} P\left(\frac{is_n(\pi) - 2\sqrt{n}}{n^{\frac{1}{6}}} \leq t\right) = F(t) \quad (\text{Tracy-Widom-Verteilung})$$

## § 5. Partitionenfunktion $p(n)$ in der Zahlentheorie

### 5.1 Theorem

(Hardy + Ramanujan 1918, Rademacher 1937 (neue Beweise 1943, 1973):

$$\forall n \in \mathbb{N} : p(n) = \frac{1}{\pi\sqrt{2}} \sum_{k=1}^{\infty} A_k(n) \sqrt{k} \left[ \frac{\partial}{\partial x} \frac{\sinh\left(\left(\frac{\pi}{k}\right)\left(\frac{2}{3}\left(x - \frac{1}{24}\right)\right)^{\frac{1}{2}}\right)}{\left(x - \frac{1}{24}\right)^{\frac{1}{2}}}\right]_{x=n}$$

wobei  $[x]$  = größte ganze Zahl  $\leq x$

sinus hyperbolicus  $\sinh(x) = \frac{1}{2}(e^x - e^{-x})$

$$A_k(n) = \sum_{h \bmod k, (h,k)=1} \omega_{h,k} e^{-2\pi i n h/k}$$

$$(\omega_{h,k})^{24} = 1, \quad \omega_{h,k} = \begin{cases} \left(\frac{-k}{h}\right) \exp\left(-\pi i \left(\frac{1}{4}(2 - hk - h) + \frac{1}{12}(k - k^{-1})(2h - h' + h^2 h')\right)\right), & h \text{ ungerade} \\ \left(\frac{-h}{k}\right) \exp\left(-\pi i \left(\frac{1}{4}(k - 1) + \frac{1}{12}(k - k^{-1})(2h - h' + h^2 h')\right)\right), & k \text{ ungerade} \end{cases}$$

wobei  $h'$  so gewählt ist, daß  $hh' \equiv -1 \pmod{k}$  und  $\left(\frac{a}{b}\right)$  das Legendre-Symbol ist bzw. seine Verallgemeinerung zum Legendre-Jacobi-Symbol:

Erst das Legendre-Symbol, wenn  $b$  eine Primzahl  $p$  ist:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & a \text{ quadratischer Rest mod } p, \text{ also } x^2 \equiv a \pmod{p} \text{ lösbar} \\ -1, & \text{Nichtrest} \\ 0, & (a, p) \neq 1 \end{cases}$$

und für beliebige  $b$ :  $\left(\frac{a}{b}\right) = \prod_{i=1}^e \left(\frac{a}{p_i}\right)^{\alpha_i}$  für  $b = \prod_{i=1}^e p_i^{\alpha_i}$

## § 6. Knoten und Zöpfe

### 6.1 Definition

Die Artinsche Zopfgruppe  $B_n$  hat  $n-1$  Erzeuger  $T_1, \dots, T_{n-1}$  und genügt den Relationen (also  $B_n =$  freie Gruppe modulo Relationen):

$$T_i T_j = T_j T_i \text{ falls } |i - j| > 1$$

$$T_i T_j T_i = T_j T_i T_j \text{ falls } |i - j| = 1$$

$B_n$  bildet surjektiv auf  $\Sigma_n$  ab:  $T_i \mapsto$  Transposition  $(i, i+1) = s_i$

### 6.2 Satz

Das Jones-Polynom  $V$  ist eine Knotenvariante.

### 6.3 Definition

Die Hecke-Algebra  $H_q(n)$  von  $\Sigma_n$  ist die  $k$ -Algebra mit Erzeugern  $g_i$ ,  $i = 1, \dots, n-1$ , und Relationen

$$g_i^2 = (q-1)g_i + q \cdot 1 \quad (q = 1 : \text{Symmetrische Gruppe, Transpositionen})$$

$$g_i g_{i+1} g_i = g_{i+1} g_i g_{i+1} \quad (\text{Zopfrelation})$$

$$g_i g_j = g_j g_i \text{ für } |i - j| > 1$$