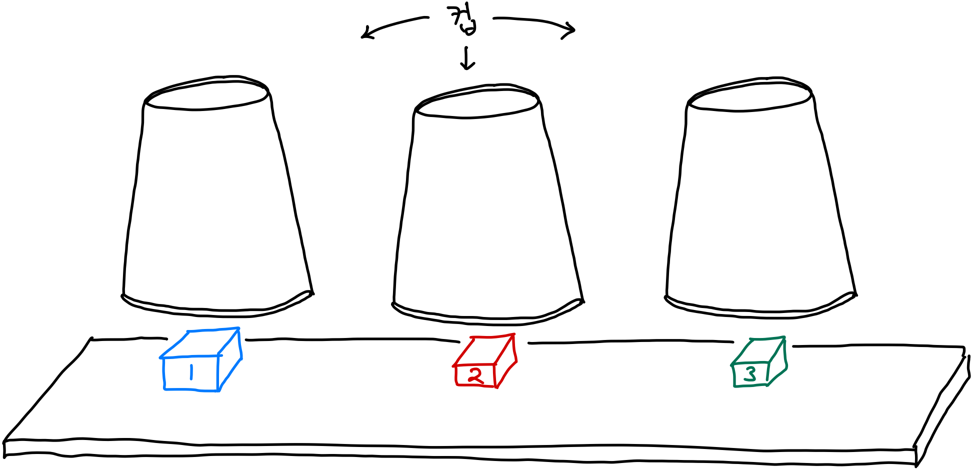
Random walks on S_n

안 희 성

성균관대 수학과

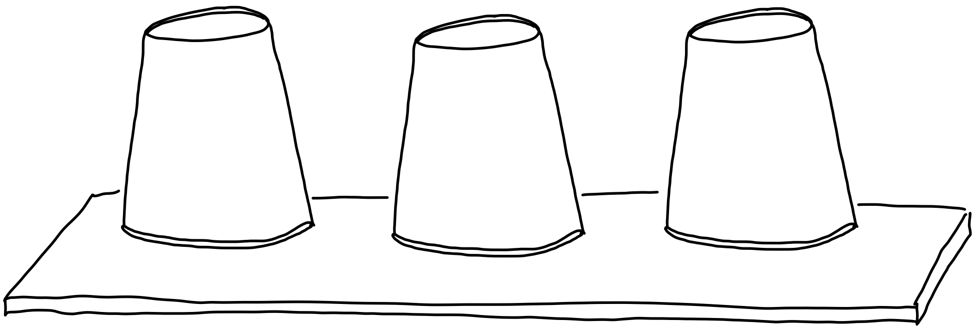
2026. 03. 16 MIMIC

문제

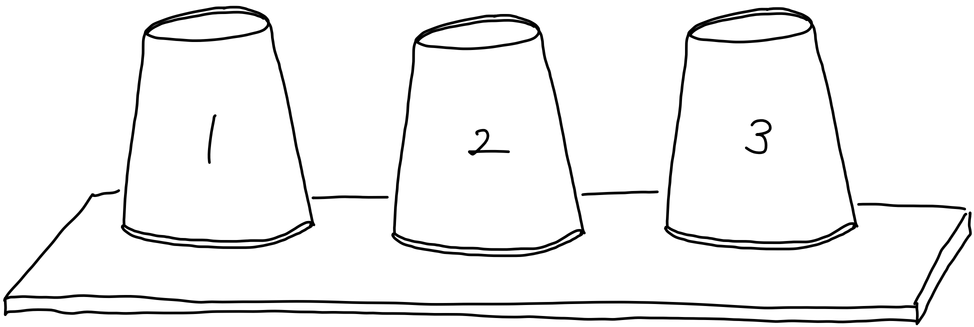


순서를 기억하세요.

문제

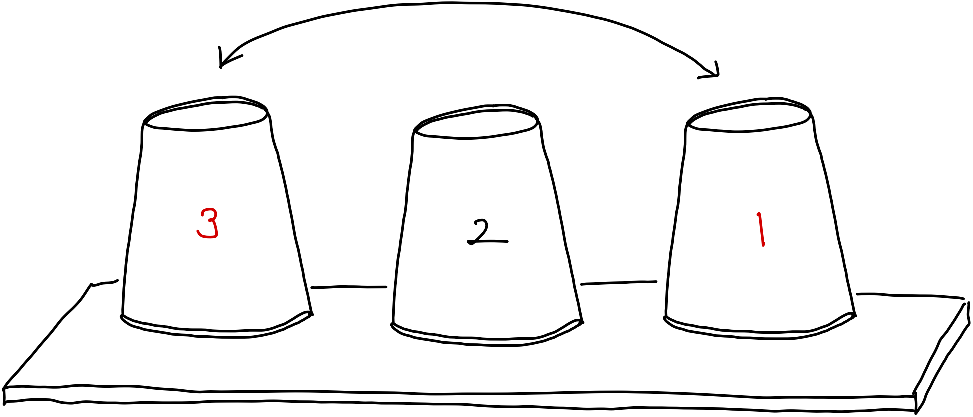


문제



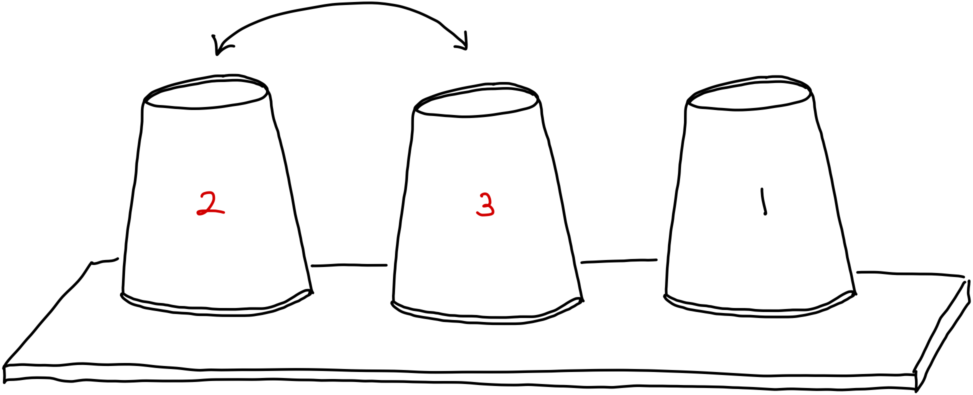
예를 들면

문제

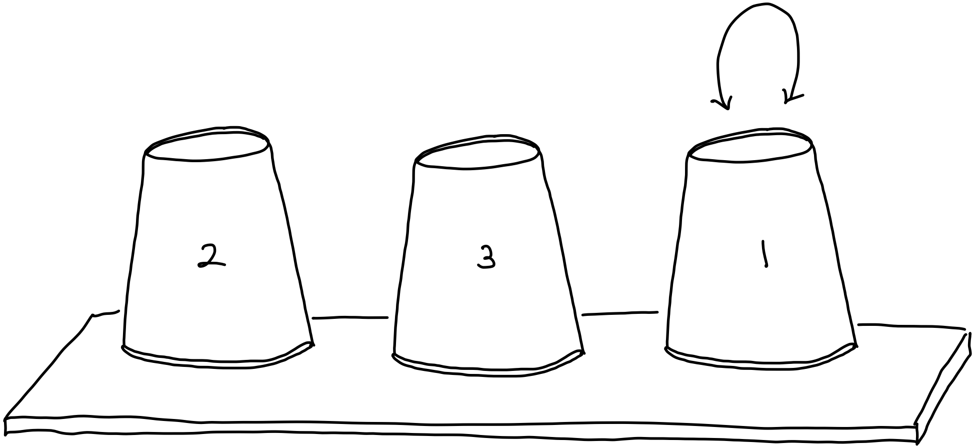


컵 두 개를 선택해서 위치를 바꿉니다.

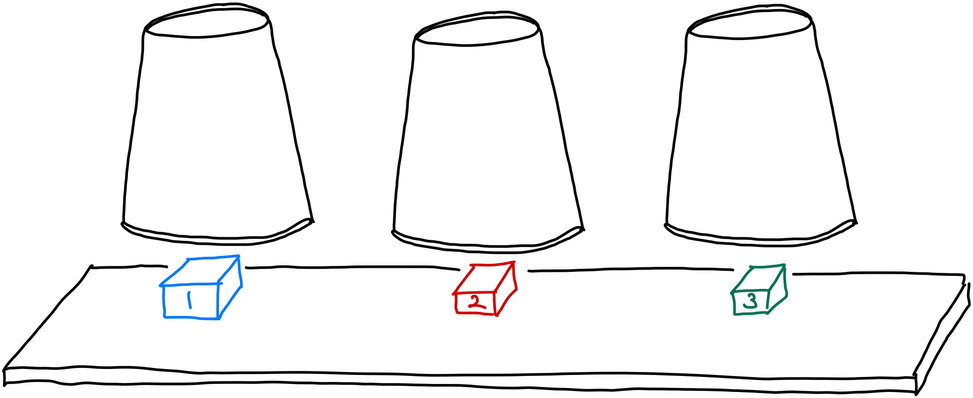
문제



문제

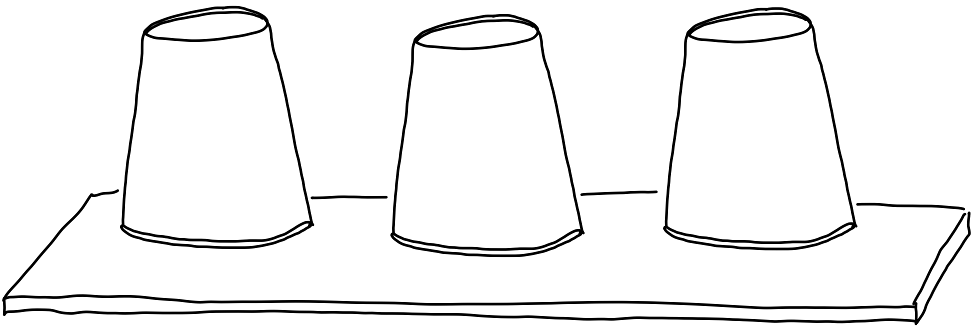


문제

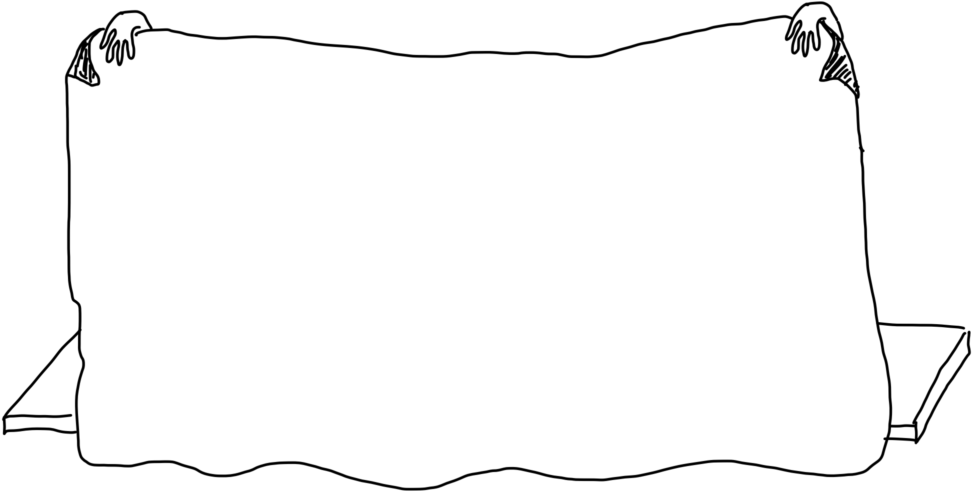


순서를 기억하세요.

문제

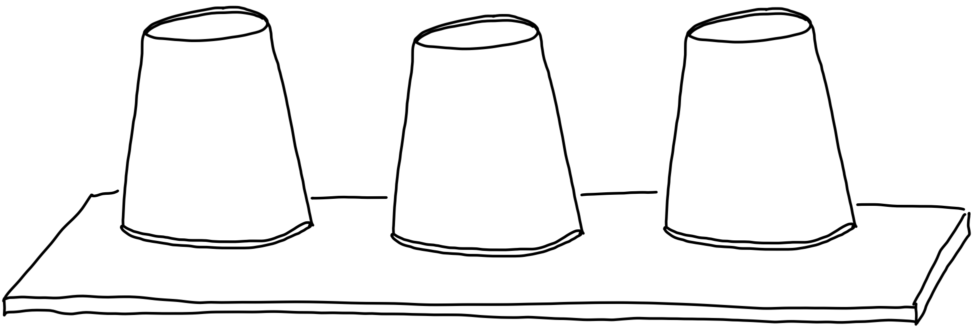


문제



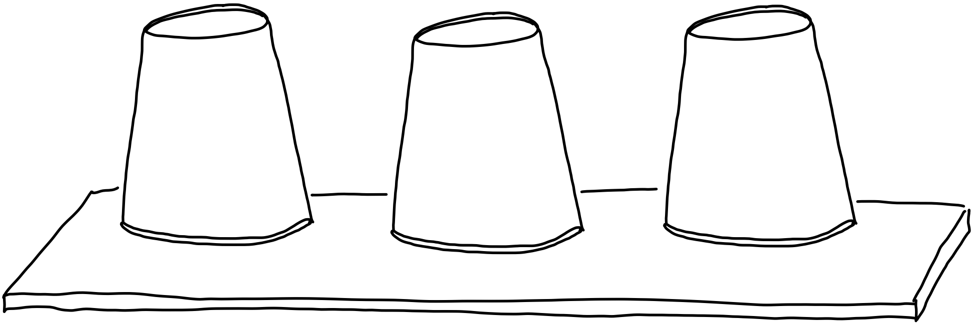
그런데 가리고.

문제



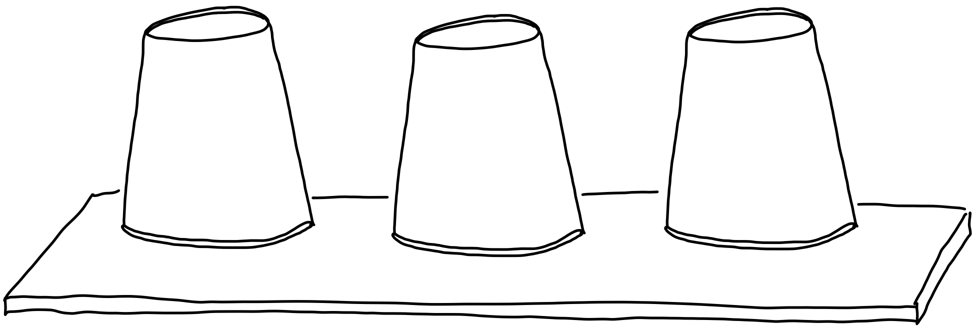
1번 돌렸다면 순서는?

문제



1번 돌렸다면 순서는? 2 3 1 은 불가능.

문제



멫번을 돌려야 확률이 다 같아질까?

목차

1. 모델링

2. Fourier transform on S_n

3. 확률이 얼마나 빠르게 다 같아질까?

모델링

$$1 \to 1$$
$$2 \to 2$$
$$3 \to 3$$

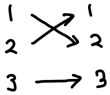
처음 상태 1 2 3 $\longrightarrow$ $e \in S_3$

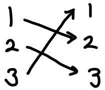
모델링

처음 상태 1 2 3 $\longrightarrow$ $e \in S_3$

$$S_3 = \{ f : \{1,2,3\} \to \{1,2,3\} \mid f \text{ is a bijection} \}$$

$$= \{ e,\ (1\,2),\ (2\,3),\ (1\,3),\ (1\,2\,3),\ (1\,3\,2) \}$$





모델링

처음 상태 1 2 3 $\longrightarrow$ $e \in S_3$

$\downarrow$ 돌리기

2 1 3 $\longrightarrow$ $(1\,2)e$

모델링

처음 상태 1 2 3 $\longrightarrow$ $e \in S_3$

$\downarrow$ 돌리기

2 1 3 $\longrightarrow$ $(1\,2)e$

$\underbrace{(1\,2) \text{ or } (2\,3) \text{ or } (3\,1)}_{\text{transposition}}$ or e 이어야 함

모델링

random variable

$$\begin{array}{ccc} X_0 & \longrightarrow & e \in S_3 \\ \downarrow & & \\ X_1 & \longrightarrow & (1\,2)e \end{array}$$

모델링

random variable

$$X_0 = e$$

$$\downarrow$$

$$X_1 = \xi_1 e \qquad \xi_1 : \text{randomly chosen } \begin{matrix}\text{transposition} \\ \text{or} \\ \text{identity}\end{matrix}$$

모델링

random variable

$$X_0 = e$$

$$\downarrow$$

$$X_1 = \xi_1 e$$

$$\downarrow$$

$$X_2 = \xi_2 \xi_1 e$$

$$\downarrow$$

$$X_3 = \xi_3 \xi_2 \xi_1 e$$

$$\downarrow$$

$$\vdots$$

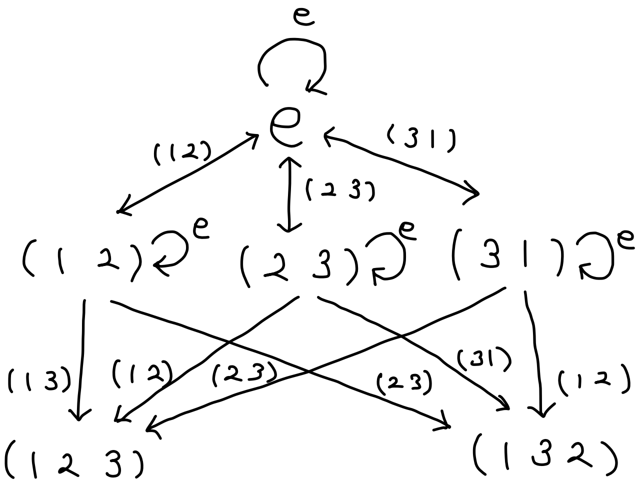
시각화

e

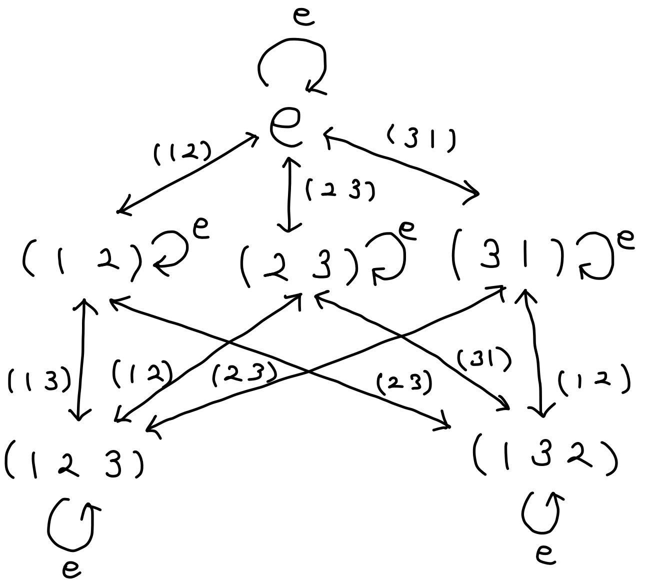
시각화

$$\begin{tikzcd}
 & e \arrow[loop above, "e"] \arrow[dl, "(12)"'] \arrow[d, "(23)"] \arrow[dr, "(31)"] & \\
(1\ 2) & (2\ 3) & (3\ 1)
\end{tikzcd}$$

시각화

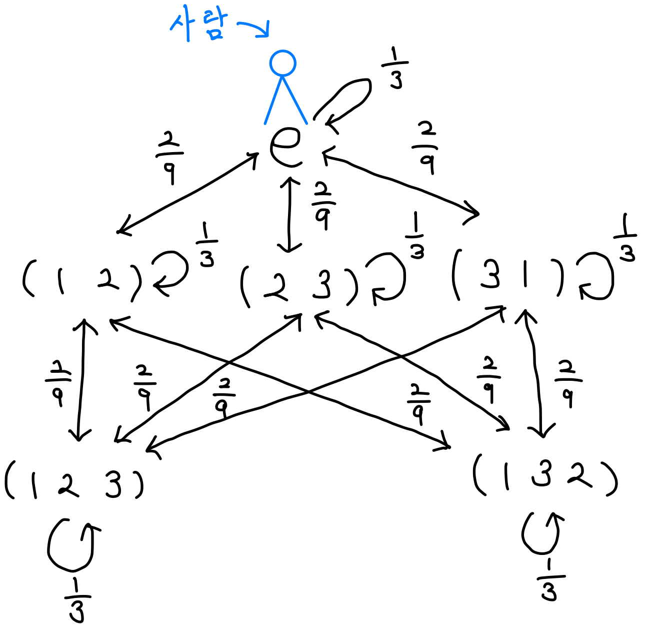


시각화 edge 몇개 지운 Cayley graph



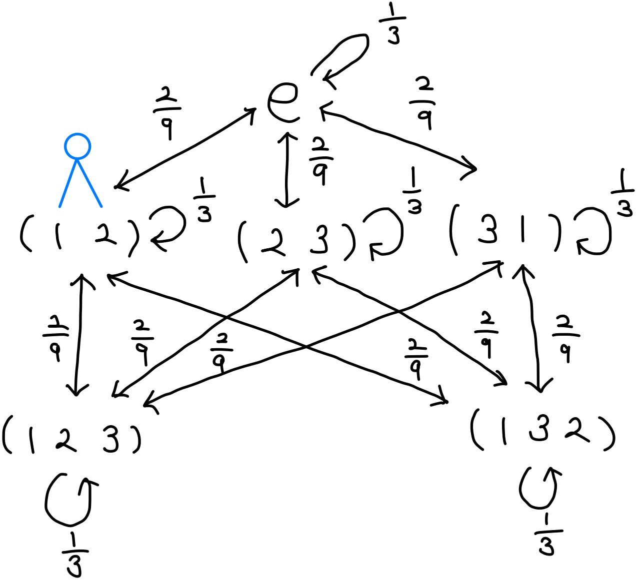
시각화

Random walk



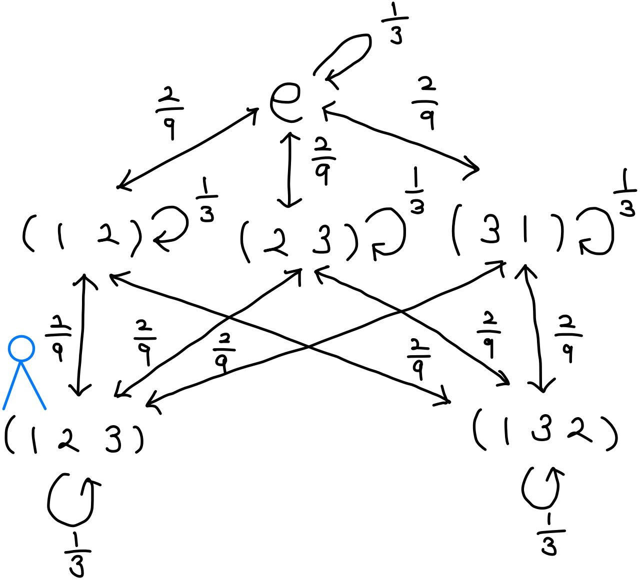
시각화

Random walk



시각화

Random walk



시각화

Random walk

$Q(e) = \frac{3}{9}$;

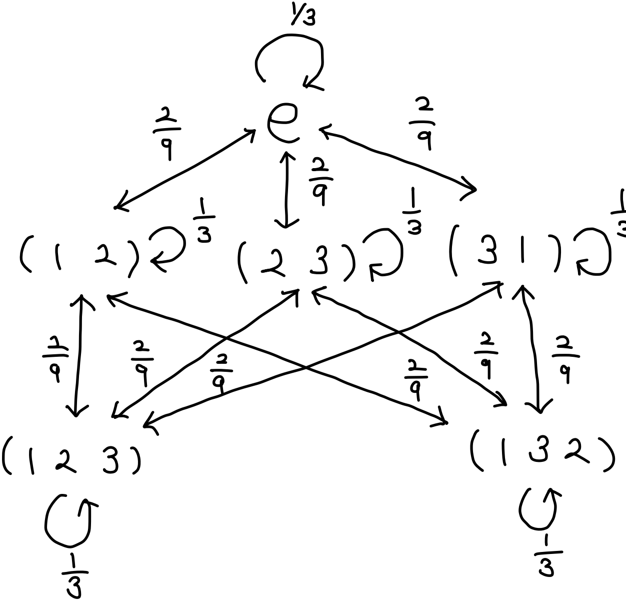
$Q(\tau) = \frac{2}{9}$;

w/ τ : trans.

$Q(\sigma) = 0$

otherwise

$\sum_{g \in G} Q(g) = 1$



e 에서 출발해서 n 번 이동했을 때 g 에 있을 확률은?

두가지 관점

① Random walk 는 Markov chain

$\Rightarrow$ transition matrix

② Convolution

Transition matrix

$$
P = \begin{array}{c|cccccc}
 & e & (12) & (23) & (13) & (123) & (132) \\
\hline
e & \frac{3}{9} & \frac{2}{9} & \frac{2}{9} & \frac{2}{9} & 0 & 0 \\
(12) & \frac{2}{9} & \frac{1}{3} & 0 & 0 & \frac{2}{9} & \frac{2}{9} \\
(23) & & & & & & \\
(13) & & & & & & \\
(123) & & & & \frac{2}{9} & & \\
(132) & & & & & &
\end{array}
$$

(1 2 3) 에서
(1 3) 으로 갈 확률

Transition matrix

행렬 곱

$$P^2 = \begin{array}{c|cccccc} & e & (12) & (23) & (13) & (123) & (132) \\ \hline e & & & & \frac{4}{27} & & \\ (12) & & & & & & \\ (23) & & & & & & \\ (13) & & & & & & \\ (123) & & & & & & \\ (132) & & & & & & \end{array}$$

e 에서 출발해서 2 번 이동했을 때 (1 3) 에 있을 확률

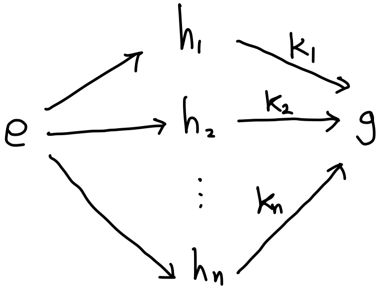
Transition matrix

$$P^{n} = \begin{array}{c|cccccc} & e & (1\,2) & (2\,3) & (1\,3) & (1\,2\,3) & (1\,3\,2) \\ \hline e & & & & & & \\ (1\,2) & & & & & & \\ (2\,3) & & & & & & \\ (1\,3) & & & & & & \\ (1\,2\,3) & & & & & & \\ (1\,3\,2) & & & & & & \end{array}$$

e 에서 출발해서 n 번 이동했을 때 g 에 있을 확률

Convolution

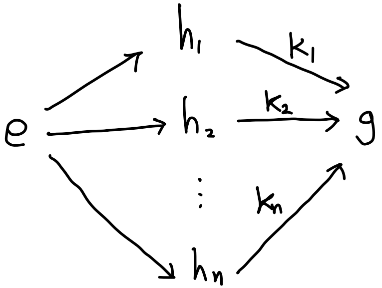
e에서 출발해서 2번 이동했을 때 g에 있을 확률은?



Convolution

e에서 출발해서 2번 이동했을 때 g에 있을 확률은?

$= P(X_2 = g)$



Convolution

$P(X_2 = g)$

$$\begin{tikzcd}
 & h_1 \arrow[dr, "k_1"] & \\
e \arrow[ur] \arrow[r] \arrow[ddr] & h_2 \arrow[r, "k_2"] & g \\
 & \vdots & \\
 & h_n \arrow[uur, "k_n"'] &
\end{tikzcd}$$

$$k_i h_i = g$$

Convolution

$P(X_2 = g)$

$$\begin{tikzcd}
 & h_1 \arrow[dr, "k_1"] & \\
e \arrow[ur] \arrow[r] \arrow[ddr] & h_2 \arrow[r, "k_2"] & g \\
 & \vdots & \\
 & h_n \arrow[uur, "k_n"'] &
\end{tikzcd}$$

$$k_i h_i = g$$

$$k_i = g h_i^{-1}$$

Convolution

$$P(X_2 = g) = \sum_{h \in G} Q(h)\,Q(gh^{-1})$$

h를 뽑고 gh^{-1}를 뽑을 확률

$$k_i h_i = g$$

$$k_i = g h_i^{-1}$$

Convolution

$$p(X_2 = g) = Q * Q(g) := \sum_{h \in G} Q(h)\,Q(gh^{-1})$$

$*$: convolution

Convolution

$$p(X_2 = g) = Q * Q(g) := \sum_{h \in G} Q(h) Q(gh^{-1})$$

$$p(X_3 = g) = Q * (Q * Q)(g) = \sum_{h \in G} Q(h) (Q * Q)(gh^{-1})$$

Convolution

$$p(X_2 = g) = Q * Q(g) := \sum_{h \in G} Q(h) Q(gh^{-1})$$

$$p(X_3 = g) = Q * (Q * Q)(g) = \sum_{h \in G} Q(h) (Q * Q)(gh^{-1})$$

$$\vdots$$

$$p(X_k = g) = Q^{k*}(g) = Q * Q^{(k-1)*}(g)$$

: k 번 이동했을 때 g에 있을 확률

순서가 2 1 3 일 확률은 어떻게 변할까?

k번 이동했을 때 순서가 2 1 3 일 확률

= k번 이동했을 때 (1 2) 에 있을 확률

순서가 2 1 3 일 확률은 어떻게 변할까?

k번 이동했을 때 순서가 2 1 3 일 확률

= k번 이동했을 때 (1 2) 에 있을 확률

$$= P(X_k = (1\ 2)) = Q^{k*}((1\ 2))$$

순서가 2 1 3 일 확률은 어떻게 변할까?

k번 이동했을 때 순서가 2 1 3 일 확률

= k번 이동했을 때 (1 2) 에 있을 확률

$$= P(X_k = (1\ 2)) = Q^{k*}((1\ 2))$$

$$Q^{1*}((1\ 2)) = \frac{2}{9} \approx 0.222$$

$$Q^{2*}((1\ 2)) = \frac{4}{27} \approx 0.148$$

$$Q^{3*}((1\ 2)) = \frac{14}{81} \approx 0.173$$

$$Q^{4*}((1\ 2)) = \frac{40}{243} \approx 0.165$$

$$Q^{5*}((1\ 2)) = \frac{122}{729} \approx 0.167$$

순서가 2 1 3 일 확률은 어떻게 변할까?

k번 이동했을 때 순서가 2 1 3 일 확률

= k번 이동했을 때 (1 2) 에 있을 확률

$$= P(X_k = (1\ 2)) = Q^{k*}((1\ 2))$$

$$Q^{1*}((1\ 2)) = \frac{2}{9} \approx 0.222$$

$$Q^{2*}((1\ 2)) = \frac{4}{27} \approx 0.148$$

$$Q^{3*}((1\ 2)) = \frac{14}{81} \approx 0.173$$

$$Q^{4*}((1\ 2)) = \frac{40}{243} \approx 0.165$$

$$Q^{5*}((1\ 2)) = \frac{122}{729} \approx 0.167$$

$$U((1\ 2)) = \frac{1}{6} \approx 0.166$$

$$Q^{k*}(g) \longrightarrow U(g) = \frac{1}{|G|} \quad \text{as } k \longrightarrow \infty$$

$$Q^{k*}(g) \longrightarrow U(g) = \frac{1}{|G|} \quad \text{as } k \to \infty$$

얼마나 가까운가?

Definition

Q_1, Q_2 : probability distribution on G.

Variation distance:

$$\|Q_1 - Q_2\| = \frac{1}{2}\sum_{g\in G} |Q_1(g) - Q_2(g)|$$

컵을 얼마나 돌려야 랜덤이 가까워질까?

→ Q^{k^*}와 U의 Variation distance는

얼마나 빨리 감소할까?

컵을 얼마나 돌려야 랜덤이 가까워질까?

→ Q^{k*} 와 U 의 Variation distance 는 얼마나 빨리 감소할까?

→ 주어진 $\varepsilon > 0$ 에 대해 $\| Q^{k*} - U \| < \varepsilon$ 이려면 k 는 얼마나 커야 할까?

$$P^k_{e,g} = Q^{k*}(g) \rightsquigarrow \text{계산 어려움}$$

(transition matrix)

2. Fourier transform on S_n

Fourier transform

$$Q * Q$$

$$\downarrow$$

$$\boxed{\text{Fourier transform}}$$

$$\downarrow$$

$$\hat{Q} \times \hat{Q}$$

Fourier transform

$f : \mathbb{R} \to \mathbb{C}$

$$\hat{f}(\xi) = \int_{-\infty}^{\infty} f(x) e^{-2\pi i \xi x} \, dx$$

Fourier transform

$f : \mathbb{R} \to \mathbb{C}$

$$\hat{f}(\xi) = \int_{-\infty}^{\infty} f(x) e^{-2\pi i \xi x} \, dx$$

: $\langle f(x), e^{2\pi i \xi x} \rangle$ 와 비슷

$\left(\langle f, g \rangle = \int_{-\infty}^{\infty} f \bar{g} \right)$

Fourier transform

$f : \mathbb{R} \to \mathbb{C}$

$$\hat{f}(\xi) = \int_{-\infty}^{\infty} f(x) e^{-2\pi i \xi x} \, dx$$

: $\langle f(x), e^{2\pi i \xi x} \rangle$ 와 비슷

$\left(\langle f, g \rangle = \int_{-\infty}^{\infty} f \bar{g} \right)$

$\{ e^{2\pi i \xi x} \}$: 함수 공간의

basis와 비슷

틀린 내용임

Fourier transform

G : finite group

$f : \mathbb{R} \to \mathbb{C}$ $\longrightarrow$ $Q : G \to \mathbb{C}$

$\hat{f}(\xi) = \int_{-\infty}^{\infty} f(x) e^{-2\pi i \xi x} \, dx$ $\longrightarrow$ $\hat{Q}(\rho) = \sum_{g \in G} Q(g) \rho(g)$

: $\langle f(x), e^{2\pi i \xi x} \rangle$ 와 비슷

$\left(\langle f, g \rangle = \int_{-\infty}^{\infty} f \bar{g} \right)$

$\{ e^{2\pi i \xi x} \}$: 함수 공간의

basis와 비슷

Fourier transform

G : finite group

$f : \mathbb{R} \to \mathbb{C}$ $\longrightarrow$ $Q : G \to \mathbb{C}$

$\hat{f}(\xi) = \int_{-\infty}^{\infty} f(x) e^{-2\pi i \xi x}\, dx$ $\longrightarrow$ $\hat{Q}(\rho) = \sum_{g \in G} Q(g)\rho(g)$

: $\langle f(x), e^{2\pi i \xi x} \rangle$ 와 비슷 : $\langle Q, \rho_{ij} \rangle$

$\left(\langle f, g \rangle = \int_{-\infty}^{\infty} f \bar{g} \right)$ $\left(\langle f, g \rangle = \sum f \bar{g} \right)$

$\{ e^{2\pi i \xi x} \}$: 함수 공간의 basis와 비슷 $\longrightarrow$ $\{ \rho_{ij} \}$: $L^2(G)$ 의 basis

Fourier transform

좋은 성질들을 공유하지 않을까?

- Fourier inversion

$$f = \check{\hat{f}} \longrightarrow Q = \check{\hat{Q}}$$

- Plancherel theorem

$$\|f\|_1^2 = \|\hat{f}\|_2^2 \longrightarrow \|Q\|_1^2 = \|\hat{Q}\|_2^2$$

Fourier transform

$$\hat{Q}(\rho) = \sum_{g \in G} Q(g)\,\rho(g)$$

dim V × dim V
invertible
matrices

ρ : representation $\quad G \longrightarrow GL(V)$

Fourier transform

$$\hat{Q}(\rho) = \sum_{g \in G} Q(g)\,\rho(g)$$

ρ : representation $\quad G \longrightarrow GL(V)$

Example ($G = S_3$)

$\pi : S_3 \longrightarrow GL(3;\mathbb{C})$

$e \longmapsto \begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix}$ $\qquad (1\ 3) \longmapsto \begin{pmatrix} & & 1 \\ & 1 & \\ 1 & & \end{pmatrix}$

$(1\ 2) \longmapsto \begin{pmatrix} & 1 & \\ 1 & & \\ & & 1 \end{pmatrix}$ $\qquad (1\ 2\ 3) \longmapsto \begin{pmatrix} & & 1 \\ 1 & & \\ & 1 & \end{pmatrix}$

$(2\ 3) \longmapsto \begin{pmatrix} 1 & & \\ & & 1 \\ & 1 & \end{pmatrix}$ $\qquad (1\ 3\ 2) \longmapsto \begin{pmatrix} & 1 & \\ & & 1 \\ 1 & & \end{pmatrix}$

Fourier transform

$$\hat{Q}(\rho) = \sum_{g \in G} Q(g)\, \rho(g)$$

ρ : representation $\quad G \longrightarrow GL(V)$

Example ($G = S_3$)

$$\pi((1\,2))\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \\ 3 \end{pmatrix}$$

$\pi : S_3 \longrightarrow GL(3;\mathbb{C})$

$$e \longmapsto \begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix} \qquad (1\,3) \longmapsto \begin{pmatrix} & & 1 \\ & 1 & \\ 1 & & \end{pmatrix}$$

$$(1\,2) \longmapsto \begin{pmatrix} & 1 & \\ 1 & & \\ & & 1 \end{pmatrix} \qquad (1\,2\,3) \longmapsto \begin{pmatrix} & & 1 \\ 1 & & \\ & 1 & \end{pmatrix}$$

$$(2\,3) \longmapsto \begin{pmatrix} 1 & & \\ & & 1 \\ & 1 & \end{pmatrix} \qquad (1\,3\,2) \longmapsto \begin{pmatrix} & 1 & \\ & & 1 \\ 1 & & \end{pmatrix}$$

Representation

$\rho(g) w \in W, \ \forall w \in W$

$W \leq V$. If W is $\rho(g)$-invariant, $\forall g \in G$,

then $\exists \ \rho(g)|_W$, $\forall g \in G$.

Representation

$W \subseteq V$. If W is $\rho(g)$- invariant $\forall g \in G$,

then $\exists\, \rho(g)\big|_W \;\; \forall g \in G$.

Definition

$\rho|_W : G \longrightarrow GL(W)$ is a subrepresentation

$g \longmapsto \rho(g)|_W$

Representation

$W \leq V$. If W is $\rho(g)$- invariant $\forall g \in G$,

then $\exists\, \rho(g)\big|_W \ \forall g \in G$.

Definition

$$\rho|_W : G \longrightarrow GL(W) \quad \text{is a subrepresentation}$$
$$g \longmapsto \rho(g)|_W$$

Example

$W = \text{span}\left\{ \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \right\}$ is $\pi(S_3)$- invariant

$\pi\big|_W : G \to GL(W)$ by $\pi\big|_W(g) = I$ is a subrep'n

Representation

Definition

ρ is irreducible if

$\exists$ only two subrep'n : $G \to \{I\}$ and ρ

Representation

Definition

ρ is irreducible if

$\exists$ only two subrep'n : $G \to \{I\}$ and ρ

Example ($G = S_3$)

$\pi|_W : G \to GL(\text{span}\{\begin{pmatrix}1\\1\\1\end{pmatrix}\})$ is irreducible

since $\dim(\text{span}\{\begin{pmatrix}1\\1\\1\end{pmatrix}\}) = 1$.

Representation

Recall

$\operatorname{span}\left\{\begin{pmatrix}1\\1\\1\end{pmatrix}\right\}$ is $\pi(S_3)$-invariant

Note

By change of basis to $\left\{\begin{pmatrix}1\\1\\1\end{pmatrix}, \cdot, \cdot\right\}$,

irreducible

$$\pi(g) = P \begin{pmatrix} \boxed{1} & 0 & 0 \\ 0 & \boxed{?} & \\ 0 & & \end{pmatrix} P^{-1}$$

irreducible

Representation

Theorem (Maschke)

G : finite group

$\rho : G \to GL(V)$

$$\rho(g) = \begin{pmatrix} \boxed{\pi_1(g)} & & & \\ & \boxed{\pi_2(g)} & & \\ & & \ddots & \\ & & & \boxed{\pi_n(g)} \end{pmatrix}$$

w/ $\pi_i : G \to W_i$, $W_i \leq V$, irreducible

Representation

There are 3 irreducible representations on S_3 (up to isomorphism)

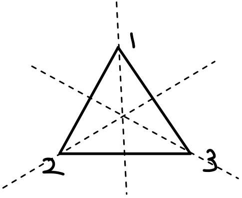
1. $\pi_1 : S_3 \longrightarrow GL(\mathbb{C})$

$$\sigma \longmapsto 1$$

2. $\pi_2 : S_3 \longrightarrow GL(\mathbb{C})$

$$\sigma \longmapsto \operatorname{sgn}(\sigma)$$

3. $\pi_3 : S_3 \longrightarrow GL(2;\mathbb{C})$



Representation

There are 3 irreducible representations on S_3 (up to isomorphism)

1. $\pi_1 : S_3 \longrightarrow GL(\mathbb{C})$ $\qquad d\pi_1 = \dim \mathbb{C} = 1$
   $\sigma \longmapsto 1$

2. $\pi_2 : S_3 \longrightarrow GL(\mathbb{C})$ $\qquad d\pi_2 = 1$
   $\sigma \longmapsto \mathrm{sgn}(\sigma)$

3. $\pi_3 : S_3 \longrightarrow GL(2;\mathbb{C})$ $\qquad d\pi_3 = 2$

Representation

$$\hat{Q}(\rho) = \sum_{g \in G} Q(g)\rho(g)$$

1. $\hat{Q}(\pi_1) = Q(e)(1) + Q(\tau)(1+1+1) = 1\, I_{(1)}$

2. $\hat{Q}(\pi_2) = -\frac{1}{3} I_{(1)}$

3. $\hat{Q}(\pi_3) = \begin{pmatrix} \frac{1}{3} & 0 \\ 0 & \frac{1}{3} \end{pmatrix} = \frac{1}{3} I_{(2)}$

Representation

$$\hat{Q}(\rho) = \lambda I \quad \Rightarrow \quad \widehat{Q^{*k}} = (\hat{Q})^k = (\lambda I)^k = \lambda^k I$$

Representation

$$\hat{Q}(\rho) = \lambda I \quad \Rightarrow \quad \widehat{Q^{*k}} = (\hat{Q})^k = (\lambda I)^k = \lambda^k I$$

Lemma (Schur)

ρ : irreducible representation

If $\rho(h) A \rho^{-1}(h) = A \ \forall h \in G$, then $A = \lambda I$

Representation

$$\hat{Q}(\rho) = \lambda I \quad \Rightarrow \quad \widehat{Q^{*k}} = (\hat{Q})^k = (\lambda I)^k = \lambda^k I$$

Lemma (Schur)

ρ : irreducible representation

If $\rho(h) A \rho^{-1}(h) = A \ \forall h \in G$, then $A = \lambda I$

Example

$$\pi(g)\hat{Q}(\pi)\pi^{-1}(g) = \hat{Q}(\pi), \quad \forall g \in S_3$$

Thus, $\hat{Q}(\pi) = \lambda I$

Representation

Definition

$f : G \to \mathbb{C}$ is a class function if

$f(hgh^{-1}) = f(g)$, $\forall h \in G$

$$\rho(h)\,\hat{Q}(\rho)\,\rho(h)^{-1} = \rho(h)\Big(\sum_{g\in G} Q(g)\rho(g)\Big)\,\rho(h)^{-1}$$

$$= \sum_{g\in G} Q(g)\,\rho(hgh^{-1})$$

$$= \sum_{g\in Q} Q(g)\,\rho(g) = \hat{Q}(\rho)$$

Representation

Definition

$f : G \to \mathbb{C}$ is a class function if

$$f(hgh^{-1}) = f(g), \quad \forall h \in G$$

Example

Conjugacy classes of S_3 are

$\{e\}$	$\{(1\ 2), (2\ 3), (3\ 1)\}$	$\{(1\ 2\ 3)\ (1\ 3\ 2)\}$
$\rho = \frac{3}{9}$	$\rho = \frac{2}{9}$	$\rho = 0$

왜 representation 일까?

$$P^k = U D^k U^{-1}$$

(transition matrix)

$$P = a_1 \rho_1 + a_2 \rho_2 + \cdots + a_2 \rho_n$$

$$= U \begin{pmatrix} \lambda_1 I_1 & & \\ & \ddots & \\ & & \lambda_n I_n \end{pmatrix} U^{-1}$$

왜 representation 일까?

Note

Let $G = \{g_1, \dots, g_n\}$

$$e_{g_i} = (0, \cdots, 0, 1, 0, \cdots, 0).$$

The homomorphism $\rho : G \to GL(|G| ; \mathbb{C})$

$$g \longmapsto \begin{pmatrix} e_{gg_1} \\ e_{gg_2} \\ \vdots \\ e_{gg_n} \end{pmatrix}$$

is a regular representation.

왜 representation 일까?

Example

$$e_e = (1, 0, 0, 0, 0, 0)$$

$$e_{(12)} = (0, 1, 0, 0, 0, 0)$$

$$\vdots$$

$$e_{(132)} = (0, 0, 0, 0, 0, 1)$$

$$(12)e = (12)$$

$$(12)(12) = e$$

$$(12)(23) = (123)$$

$$(12)(31) = (132)$$

$$(12)(123) = (23)$$

$$(12)(132) = (31)$$

왜 representation 일까?

— Example

$e_e = (1, 0, 0, 0, 0, 0)$

$e_{(12)} = (0, 1, 0, 0, 0, 0)$

$\vdots$

$e_{(132)} = (0, 0, 0, 0, 0, 1)$

$(12)e = (12)$

$(12)(12) = e$

$(12)(23) = (123)$

$(12)(31) = (132)$

$(12)(123) = (23)$

$(12)(132) = (31)$

$\rho_{reg} : G \to GL(6; \mathbb{C})$

$$g \longmapsto \begin{pmatrix} e_{gg_1} \\ e_{gg_2} \\ \vdots \\ e_{gg_n} \end{pmatrix}$$

$$\rho_{reg}((12)) = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ & & & & & \\ & & & & & \\ & & & & & \end{pmatrix}$$

왜 representation 일까?

— Example

$$e_e = (1, 0, 0, 0, 0, 0)$$
$$e_{(12)} = (0, 1, 0, 0, 0, 0)$$
$$\vdots$$
$$e_{(132)} = (0, 0, 0, 0, 0, 1)$$

$$\rho_{reg} : G \to GL(6; \mathbb{C})$$
$$g \longmapsto \begin{pmatrix} e_{gg_1} \\ e_{gg_2} \\ \vdots \\ e_{gg_n} \end{pmatrix}$$

$$\begin{aligned}
(12)\,e &= (1\ 2) \\
(12)(1\ 2) &= e \\
(12)(2\ 3) &= (1\ 2\ 3) \\
(12)(3\ 1) &= (1\ 3\ 2) \\
(12)(1\ 2\ 3) &= (2\ 3) \\
(12)(1\ 3\ 2) &= (3\ 1)
\end{aligned}$$

$$\rho_{reg}((12)) = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

왜 representation 일까?

Note

image

P is a linear combination of $\rho(S_3)$

(transition matrix)

$$P = \sum_{g \in G} Q(g)\,\rho_{reg}(g)$$

왜 representation 일까?

Note

P is a linear combination of $\rho(S_3)$ ← image

(transition matrix)

$$P = \sum_{g\in G} Q(g)\,\rho_{reg}(g)$$

P_{ij} : i 에서 j 로 갈 확률 $= Q(g)$, $\exists g \in G$

$$\sum_{g\in G} Q(g)\,\rho_{reg}(g)_{ij} = \underset{gi=j}{Q(g)} + \underbrace{0+0+0+0+0}_{gi\neq j} = Q(g)$$

왜 representation 일까?

$$P = \sum_{g \in G} Q(g)\, \rho_{reg}(g)$$

$$= \sum_{g \in G} Q(g)\; U \begin{pmatrix} \boxed{\pi_1(g)} & & & \\ & \boxed{\pi_2(g)} & & \\ & & \ddots & \\ & & & \boxed{\pi_n(g)} \end{pmatrix} U^{-1} \qquad (1)$$

$$= U \begin{pmatrix} \boxed{\sum_{g \in G} Q(g)\, \pi_1(g)} & & \\ & \ddots & \\ & & \boxed{\sum_{g \in G} Q(g)\, \pi_n(g)} \end{pmatrix} U^{-1} \qquad (2)$$

왜 representation 일까?

$$P = U \begin{pmatrix} \boxed{\sum_{g \in G} Q(g)\pi_1(g)} & & \\ & \ddots & \\ & & \boxed{\sum_{g \in G} Q(g)\pi_n(g)} \end{pmatrix} U^{-1} \quad (2)$$

$$= U \begin{pmatrix} \hat{Q}(\pi_1) & & \\ & \ddots & \\ & & \hat{Q}(\pi_n) \end{pmatrix} U^{-1} \quad (3)$$

$$= U \begin{pmatrix} \lambda_1 I_1 & & \\ & \ddots & \\ & & \lambda_n I_n \end{pmatrix} U^{-1} \quad (4)$$

왜 representation 일까?

$$P = U \begin{pmatrix} \hat{Q}(\pi_1) & & \\ & \ddots & \\ & & \hat{Q}(\pi_n) \end{pmatrix} U^{-1} \qquad (3)$$

Fact. U is unitary

$\Rightarrow \quad \|Q\|_1 = \|\hat{Q}\|_2 \qquad$ (plancherel)

왜 representation 일까?

$$P = U \begin{pmatrix} \hat{Q}(\pi_1) & & \\ & \ddots & \\ & & \hat{Q}(\pi_n) \end{pmatrix} U^{-1} \qquad (3)$$

Fact. U is unitary

$\Rightarrow \quad \|Q\|_1 = \|\hat{Q}\|_2 \qquad$ (plancherel)

w/ $\langle P, Q \rangle_1 = \sum_{g \in G} P(g) Q(g)$

$\langle \hat{P}, \hat{Q} \rangle_2 = \frac{1}{|G|} \sum_{\rho \in \hat{G}} d_\rho \operatorname{Tr}\left(\hat{P}(\rho), \overline{\hat{Q}(\rho)}^{tr} \right)$

$\hat{G}$: irr. rep'n

3. 확률이 얼마나 빠르게 다 같아질까?

Upper bound lemma

$$\boxed{\| Q^{*k} - U \|^2 \le \frac{1}{4} \sum_{\rho \neq 1} d_\rho \| \hat{Q}(\rho) \|^{2k}}$$

pf) $\| Q^{*k} - U \|^2$

(1) $$= \left(\frac{1}{2} \sum_{g \in G} | Q^{*k}(g) - U(g) | \right)^2$$ (definition)

(2) $$\le \frac{1}{4} |G| \sum_{g \in G} | Q^{*k}(g) - U(g) |^2$$ (Cauchy-Schwarz)

(3) $$= \frac{1}{4} |G| \, \| Q^{*k}(g) - U(g) \|_2$$ (plancherel)

(3) $$= \frac{1}{4} |G| \, \| Q^{*k}(g) - U(g) \|_2$$ (plancherel)

(4) $$= \frac{1}{4} \sum_{\rho \neq 1} d_\rho \, \mathrm{Tr}\left(\widehat{Q^{*k}} \right) \left(\overline{\widehat{Q^{*k}}} \right)^t$$ $\left(\hat{U}(\rho) = \begin{cases} I & \rho = 1 \\ 0 & \rho \neq 1 \end{cases} \right)$

$$= \frac{1}{4} \sum_{\rho \neq 1} d_\rho \, \| \hat{Q}(\rho) \|^k$$

Hilbert-schmidt norm

$\| A \| = \mathrm{Tr}(AA^*)$

(3) $$= \frac{1}{4} |G| \, \| Q^{*k}(g) - U(g) \|_2$$ (plancherel)

(4) $$= \frac{1}{4} \sum_{\rho \neq 1} d_\rho \, \mathrm{Tr}\left(\widehat{Q^{*k}} \right) \left(\overline{\widehat{Q^{*k}}} \right)^t$$ $$\left(\hat{U}(\rho) = \begin{cases} I & \rho = 1 \\ 0 & \rho \neq 1 \end{cases} \right)$$

$$= \frac{1}{4} \sum_{\rho \neq 1} d_\rho \, \| \hat{Q}(\rho) \|^k$$

Hilbert-schmidt norm

$\| A \| = \mathrm{Tr}(AA^*)$

irr. rep'n, d_ρ, $\| \hat{Q}(\rho) \|$ 에 의해

$\| Q^{*k} - U \|^2 < \varepsilon$ 을 만족하는 k (컵을 돌리는 횟수)

값이 결정됨

irr. rep'n, d_ρ, $\|\hat{Q}(\rho)\|$

irreducible

$$\hat{Q}(\rho) = \lambda I \quad \Rightarrow \quad \|\hat{Q}(\rho)\| = d_\rho \lambda^2$$

irr. rep'n, d_ρ, $\|\hat{Q}(\rho)\|$

irreducible

$$\hat{Q}(\rho) = \lambda I \quad \Rightarrow \quad \|\hat{Q}(\rho)\| = d_\rho \lambda^2$$

$$\mathrm{Tr}(\hat{Q}(\rho)) = \mathrm{Tr}(\lambda I) = d_\rho \lambda$$

irr. rep'n, d_ρ, $\mathrm{Tr}(\rho(\tau))$

---

irreducible

$$\hat{Q}(\rho) = \lambda I \quad \Rightarrow \quad \| \hat{Q}(\rho) \| = d_\rho \lambda^2$$

$$\begin{array}{ccc} \mathrm{Tr}(\hat{Q}(\rho)) & = & \mathrm{Tr}(\lambda I) \\ \parallel & & \parallel \\ \sum_{g \in G} Q(g)\, \mathrm{Tr}(\rho(g)) & & d_\rho \lambda \\ \parallel & & \\ \frac{1}{3} d_\rho + 3 \times \frac{2}{9} \mathrm{Tr}(\rho(\tau)) & & \end{array}$$

transposition ($Q(\tau) = \frac{2}{9}$)

irr. rep'n, d_ρ, $\mathrm{Tr}(\rho(\tau))$

$$\left\{ \begin{array}{c} \text{partition} \\ \text{of } n \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{irreducible} \\ \text{representations} \\ \text{of } S_n \end{array} \right\}$$

Example

$3 = 3$

$= 2 + 1$ $\Rightarrow$

$= 1 + 1 + 1$

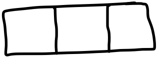
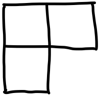
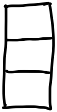
S_3 의 irr. rep'n 3가지

(3) — π_1 (trivial)

$(2, 1)$ — π_3 $(d_{(2,1)} = 2)$

$(1, 1, 1)$ — π_2 (sgn)

irr. rep'n, d_ρ, $\mathrm{Tr}(\rho(\tau))$

irr. rep'n	Young diagram
(3) — π_1	
$(2,1)$ — π_3	
$(1,1,1)$ — π_2	

$\{1,2,3\}$을 오른쪽/아래로 증가하도록 넣는 경우의 수

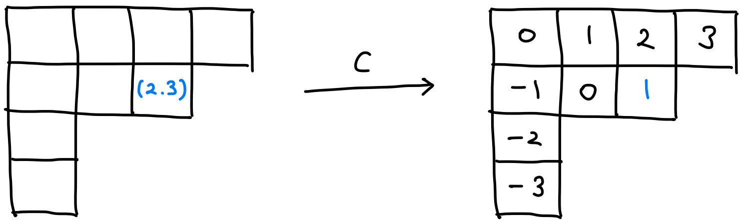
irr. rep'n, d_ρ, $\mathrm{Tr}(\rho(\tau))$

irr. rep'n	Young diagram	
(3) — π_1	$\begin{array}{\|c\|c\|c\|}\hline 1 & 2 & 3 \\ \hline\end{array}$	$d_{\pi_1} = 1$
$(2,1)$ — π_3	$\begin{array}{\|c\|c\|}\hline 1 & 2 \\ \hline 3 \\ \cline{1-1}\end{array}$ $\quad$ $\begin{array}{\|c\|c\|}\hline 1 & 3 \\ \hline 2 \\ \cline{1-1}\end{array}$	$d_{\pi_3} = 2$
$(1,1,1)$ — π_2	$\begin{array}{\|c\|}\hline 1 \\ \hline 2 \\ \hline 3 \\ \hline\end{array}$	$d_{\pi_2} = 1$

irr. rep'n, d_ρ, $\mathrm{Tr}(\rho(T))$

Content $c(i,j) = j - i$

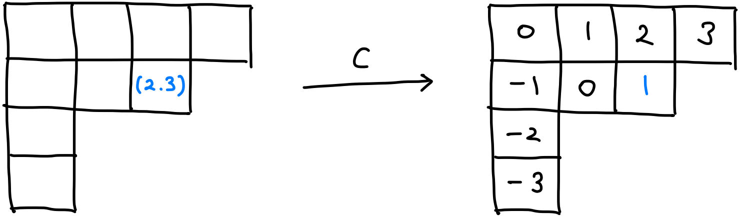
$c(2,3) = 3 - 2 = 1$



irr. rep'n, d_ρ, $\mathrm{Tr}(\rho(\tau))$

Content $c(i,j) = j - i$

$c(2,3) = 3 - 2 = 1$



$$\mathrm{Tr}(\rho(\tau)) = \frac{d_\rho}{\binom{n}{2}} \sum c(i,j)$$

irr. rep'n, d_ρ, $\mathrm{Tr}(\rho(T))$

irr. rep'n	Young diagram	$\mathrm{Tr}(\rho(T))$
(3) — π_1	$\begin{array}{\|c\|c\|c\|}\hline 0 & 1 & 2 \\ \hline \end{array}$	$\frac{1}{3}\cdot 3 = 1$
$(2,1)$ — π_3	$\begin{array}{\|c\|c\|}\hline 0 & 1 \\ \hline -1 \\ \cline{1-1} \end{array}$	0
$(1,1,1)$ — π_2	$\begin{array}{\|c\|}\hline 0 \\ \hline -1 \\ \hline -2 \\ \hline \end{array}$	$\frac{1}{3}\cdot(-3) = -1$

Conclusion

Theorem (Diaconis, Shahshahani (1981))

Let $k = \frac{1}{2} n \log n + cn$. For $c > 0$,

$$\| Q^{*k} - U \| \leq a e^{-2c}$$

constant

Conclusion

Theorem (Diaconis, Shahshahani (1981))

Let $k = \frac{1}{2} n \log n + cn$. For $c > 0$,

$$\| Q^{*k} - U \| \leq \underbrace{a}_{\text{constant}} e^{-2c}$$

Example

트럼프 카드 52 장을 2 장씩 뽑아 섞을 때는

$\frac{1}{2} \cdot 52 \cdot \log 52 \approx 103$번 섞으면 고루 섞인다.