離散数理工学　第 5 回
離散代数：対称群と置換群

岡本 吉央
okamotoy@uec.ac.jp

電気通信大学

2018 年 11 月 15 日

最終更新：2018 年 11 月 14 日　14:27

スケジュール 前半 (予定)

1. 数え上げの基礎：二項係数と二項定理 (10/4)
- ⋆ 休講 (10/11)
2. 数え上げの基礎：漸化式の立て方 (10/18)
3. 数え上げの基礎：漸化式の解き方 (基礎) (10/25)
- ⋆ 休講 (11/1)
4. 数え上げの基礎：漸化式の解き方 (発展) (11/8)
5. 離散代数：対称群と置換群 (11/15)
- ⋆ 休講 (11/22)
6. 離散代数：有限群 (11/29)
7. 離散代数：有限群の応用 (12/6)

注意：予定の変更もありうる

スケジュール 後半 (予定)

8. 離散確率論：確率的離散システムの解析 (12/13)
★ 中間試験 (12/20)
9. 離散確率論：乱択データ構造とアルゴリズム (基礎) (1/10)
10. 離散確率論：乱択データ構造とアルゴリズム (発展) (1/17)
11. 離散確率論：マルコフ連鎖 (基礎) (1/24)
12. 離散確率論：マルコフ連鎖 (発展) (1/31)
13. 離散確率論：エントロピー (2/7)
★ 期末試験 (2/14?)

注意：予定の変更もありうる

今日の目標

置換群に関する基礎的な用語が使えるようになる

- 置換，二行記法，巡回記法，互換
- 偶置換，奇置換
- 置換群，対称群，交代群
- 生成系

http://www.cs.utexas.edu/~panni/

https://resources.mpi-inf.mpg.de/conferences/adfocs-01/program.html

この問題の出自 (データ構造に関する論文)

- Anna Gál, Peter Bro Miltersen: The cell probe complexity of succinct data structures. Theor. Comput. Sci. 379(3): 405–417 (2007)

100 囚人の問題：設定

設定

- 100 人の死刑囚
- 死刑囚には番号が振られている $(1, 2, \ldots, 100)$
- 死刑囚は一人ずつ部屋に連れられて行き，そこで以下を行う
  - その部屋には $1, 2, \ldots, 100$ と番号の書かれた箱がある
  - 箱には $1, 2, \ldots, 100$ の中の番号が 1 つだけ書かれた紙が入っている
  - 紙に書かれている番号はすべて異なる
  - 死刑囚はその中の 50 個の箱を開けられる
  - 開けた箱の中に自分と同じ番号の紙が入っていれば「成功」
  - そうでなければ「失敗」
- 全員の死刑囚が成功すれば，全員釈放．そうでなければ，全員死刑

死刑囚は前もって相談できる

問題

死刑囚はどれほどの確率で「全員釈放」されるか？

簡単な戦略

各死刑囚は，一様ランダムに 50 個の箱を明ける

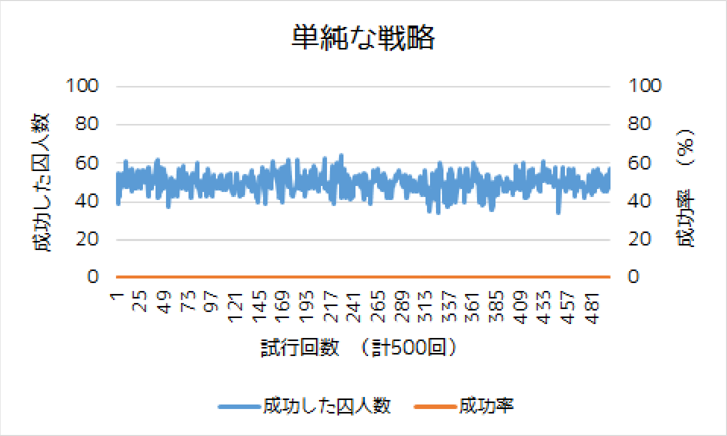
この戦略で「全員釈放」となる確率は？

- 1 人の死刑囚が成功する確率は $\dfrac{50}{100} = \dfrac{1}{2}$
- $\therefore$ 100 人全員が成功する確率は

$$\left(\frac{1}{2}\right)^{100} \approx 7.89 \times 10^{-31}$$

これは「ほぼ 0」

500 回の試行


単純な戦略
成功した囚人数
100
80
60
40
20
0
成功率（%）
1
25
49
73
97
121
145
169
193
217
241
265
289
313
337
361
385
409
433
457
481
試行回数　（計500回）
成功した囚人数
成功率

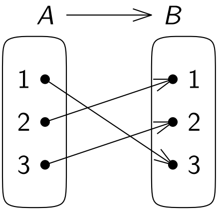
目次

置換

有限集合 X

置換とは？

X 上の置換とは，X から X への全単射のこと



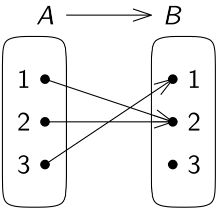
$\{1, 2, 3\}$ 上の置換

復習：全単射

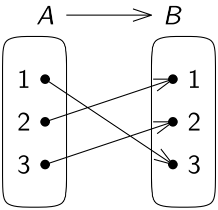
集合 A, B と写像 $f\colon A \to B$

全単射とは？

f が全単射であるとは，全射であり，かつ，単射であること



全単射ではない



全単射である

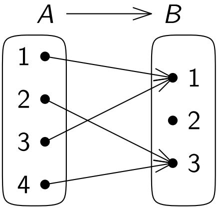
復習：全射

集合 A, B と写像 $f\colon A \to B$

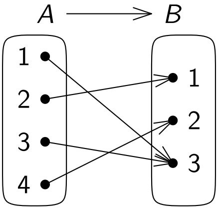
全射とは？

f が全射であるとは，次を満たすこと

$$\text{任意の } b \in B \text{ に対して，ある } a \in A \text{ が存在して } b = f(a)$$



全射ではない



全射である

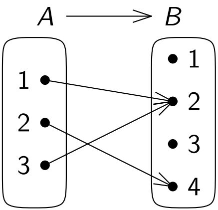
復習：単射

集合 A, B と写像 $f\colon A \to B$

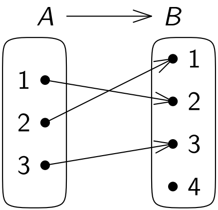
単射とは？

f が単射であるとは，次を満たすこと

$$\text{任意の } a, a' \in A \text{ に対して，} \quad f(a) = f(a') \text{ ならば } a = a'$$



単射ではない



単射である

復習：写像の合成

集合 A, B, C と写像 $f\colon A \to B$, $g\colon B \to C$

写像の合成とは？

写像 f と g の合成を $g \circ f\colon A \to C$ と表記し，任意の $x \in A$ に対して

$$(g \circ f)(x) = g(f(x))$$

とすることで定義する

注意：f の終域と g の始域が同じでないといけない
(同じでないときは合成を定義できない)

復習：写像の合成：例

- $A = \{1, 2, 3\}$, $B = \{4, 5, 6, 7\}$, $C = \{8, 9\}$
- 写像 $f \colon A \to B$ を次で定義
  - $f(1) = 5$, $f(2) = 4$, $f(3) = 7$
- 写像 $g \colon B \to C$ を次で定義
  - $g(4) = 8$, $g(5) = 9$, $g(6) = 9$, $g(7) = 8$

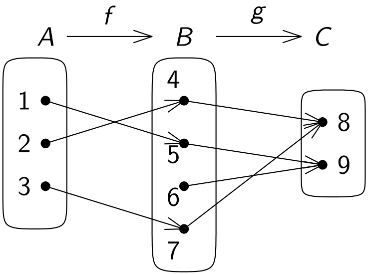
このとき，$g \circ f \colon A \to C$ を考えると，

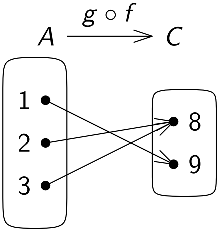
$$(g \circ f)(3) = g(f(3)) = g(7) = 8$$

復習：写像の合成：例 (続)

- $A = \{1,2,3\}$, $B = \{4,5,6,7\}$, $C = \{8,9\}$
- 写像 $f\colon A \to B$ を次で定義
  - $f(1) = 5$, $f(2) = 4$, $f(3) = 7$
- 写像 $g\colon B \to C$ を次で定義
  - $g(4) = 8$, $g(5) = 9$, $g(6) = 9$, $g(7) = 8$

このとき，$g \circ f\colon A \to C$ を考えると，





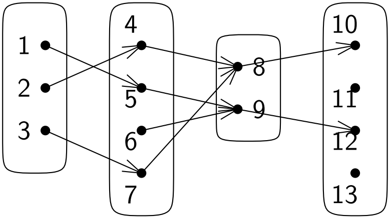
写像の合成の性質 (1)

集合 A, B, C, D と写像 $f\colon A \to B$, $g\colon B \to C$, $h\colon C \to D$

演習問題 (結合法則)

写像として，$h \circ (g \circ f) = (h \circ g) \circ f$

$$A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$$



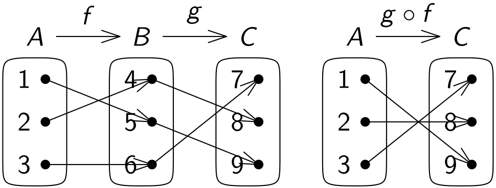
この性質より，$h \circ (g \circ f)$ や $(h \circ g) \circ f$ を $h \circ g \circ f$ と書くことが正当化される

写像の合成の性質 (2)

集合 A, B, C と写像 $f\colon A \to B$, $g\colon B \to C$

演習問題 (全単射の合成も全単射)

f と g が全単射 $\Rightarrow$ $g \circ f$ も全単射



復習：恒等写像

集合 A と写像 $f\colon A \to A$

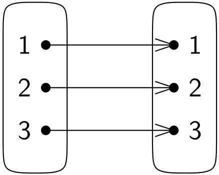
恒等写像とは？

f が恒等写像であるとは，任意の $a \in A$ に対して $a = f(a)$ であること

- $A \to A$ の恒等写像を id_A と書くこともある
- 例：$A = \{1, 2, 3\}$ のとき $f\colon A \to A$ で

$$f(1) = 1, \quad f(2) = 2, \quad f(3) = 3$$

$$A \xrightarrow{\mathrm{id}_A} A$$



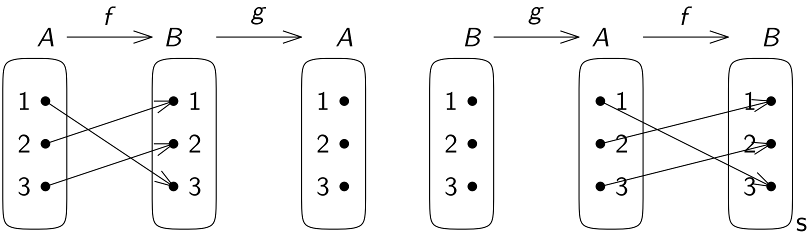
注：恒等写像は置換である

復習：逆写像

集合 A, B と写像 $f\colon A \to B$

逆写像とは？

f の**逆写像**とは，写像 $g\colon B \to A$ で，$g \circ f = \mathrm{id}_A$ かつ $f \circ g = \mathrm{id}_B$ を満たすもの　($\mathrm{id}_A\colon A \to A$，$\mathrm{id}_B$ は恒等写像)



記法

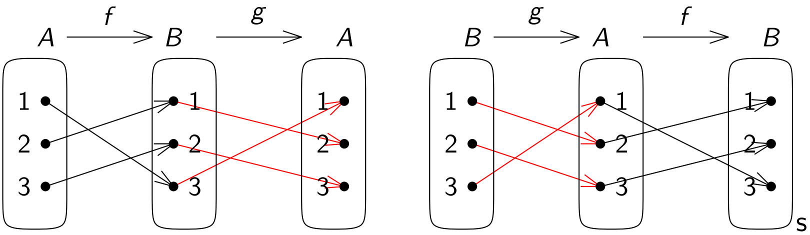
f の逆写像が存在するとき，それを f^{-1} で表す

復習：逆写像

集合 A, B と写像 $f\colon A \to B$

逆写像とは？

f の逆写像とは，写像 $g\colon B \to A$ で，$g \circ f = \mathrm{id}_A$ かつ $f \circ g = \mathrm{id}_B$ を満たすもの　($\mathrm{id}_A\colon A \to A$，$\mathrm{id}_B$ は恒等写像)



この f の逆写像は存在する

記法

f の逆写像が存在するとき，それを f^{-1} で表す

復習：逆写像の性質

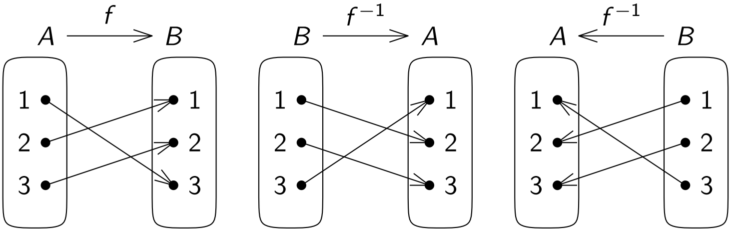
集合 A, B，写像 $f\colon A \to B$

逆写像が存在するための必要十分条件

写像 f の逆写像が存在する $\Leftrightarrow$ f が全単射

逆写像の性質

全単射 f の逆写像 f^{-1} も全単射

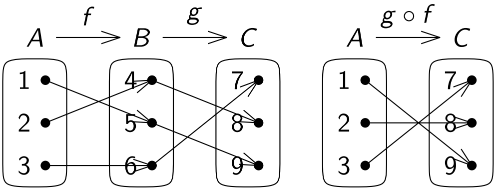


写像の合成の性質 (3)

集合 A, B, C と全単射 $f\colon A \to B$, $g\colon B \to C$

演習問題 (合成の逆写像は逆写像の合成)

写像として，$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$



置換の性質 (ここまでのまとめ)

有限集合 X

ここまでのまとめ

1. 恒等写像 id_X は X 上の置換
2. π が X 上の置換 $\Rightarrow$ π^{-1} も X 上の置換
3. π, ρ が X 上の置換 $\Rightarrow$ $\pi \circ \rho$ も X 上の置換

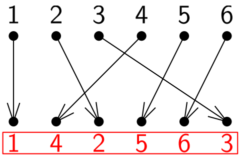
置換の文脈では以下の用語・記法も使う

- id_X は X 上の恒等置換で，e と書くことがある
- 置換 π に対して，π^{-1} を π の逆置換
- 置換の合成を置換の積とも言う
- $\pi \circ \rho$ を $\pi\rho$ とも書く
- $\pi \circ \pi$ を π^2 とも書く (π^3, π^4 なども使う)
- $\pi^{-1} \circ \pi^{-1}$ を π^{-2} とも書く (π^{-3}, π^{-4} なども使う)
  - 注：$(\pi^2)^{-1} = (\pi^{-1})^2$

置換を見て何を思うか？

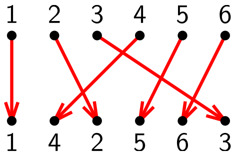
置換を見て何を思うか？ (1)

順列としての置換　(静的な見方)



置換を見て何を思うか？ (2)

全単射としての置換 (動的な見方)



2 つの見方を柔軟に使い分けることができるとよい

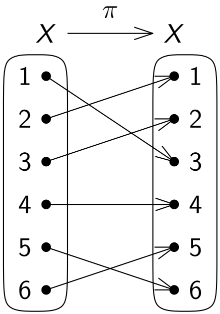
置換の二行記法

有限集合 $X = \{1, 2, \ldots, n\}$

置換の二行記法

X 上の置換 π を次のように書くことがある

$$\pi = \begin{pmatrix} 1 & 2 & \cdots & n \\ \pi(1) & \pi(2) & \cdots & \pi(n) \end{pmatrix}$$



$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 4 & 6 & 5 \end{pmatrix}$$

注意

- 二行記法で用いる括弧は必ず丸括弧
- $X = \{1, 2, \ldots, n\}$ でなくても，
  同じ記法を用いることができる

二行記法に慣れる

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 4 & 6 & 5 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 1 & 6 & 2 & 5 \end{pmatrix}$$ のとき,

$$\begin{aligned}
\pi \circ \sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 4 & 6 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 1 & 6 & 2 & 5 \end{pmatrix} \\
&= \begin{pmatrix} 4 & 3 & 1 & 6 & 2 & 5 \\ 4 & 2 & 3 & 5 & 1 & 6 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 1 & 6 & 2 & 5 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 3 & 5 & 1 & 6 \end{pmatrix}, \\
\pi^{-1} &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 4 & 6 & 5 \end{pmatrix}^{-1} \\
&= \begin{pmatrix} 3 & 1 & 2 & 4 & 6 & 5 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 6 & 5 \end{pmatrix}.
\end{aligned}$$

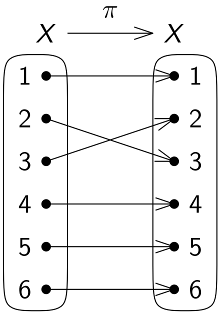
特殊な置換：隣接互換 (基本互換)

有限集合 $X = \{1, 2, \dots, n\}$

隣接互換とは？

X 上の置換 π が**隣接互換**であるとは，ある i を用いて次のように書けること

$$\pi = \begin{pmatrix} 1 & 2 & \cdots & i & i+1 & \cdots & n \\ 1 & 2 & \cdots & i+1 & i & \cdots & n \end{pmatrix}$$



$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 2 & 4 & 5 & 6 \end{pmatrix}$$

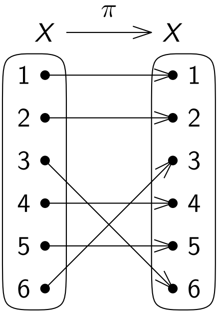
特殊な置換：互換

有限集合 $X = \{1, 2, \ldots, n\}$

互換とは？

X 上の置換 π が**互換**であるとは，ある i, j を用いて次のように書けること

$$\pi = \begin{pmatrix} 1 & 2 & \cdots & i & \cdots & j & \cdots & n \\ 1 & 2 & \cdots & j & \cdots & i & \cdots & n \end{pmatrix}$$



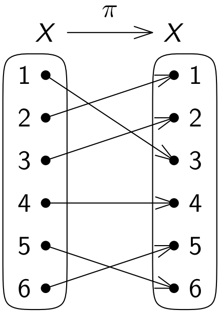
$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 6 & 4 & 5 & 3 \end{pmatrix}$$

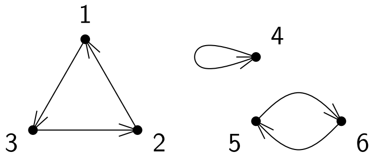
注意

- 隣接互換は互換である

目次

置換の巡回記法：直感





二行記法：$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 4 & 6 & 5 \end{pmatrix}$

巡回記法：$\pi = (1\ 3\ 2)(5\ 6)$

置換の巡回置換

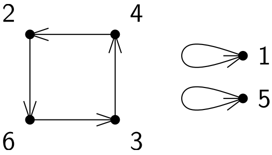
有限集合 $X = \{1, 2, \ldots, n\}$

巡回置換とは？

X 上の置換 π が巡回置換であるとは,
ある $x \in X$ と自然数 $k \geq 2$ が存在して，次が成り立つこと

- $x, \pi(x), \pi^2(x), \ldots, \pi^{k-1}(x)$ がすべて異なり,
- $x = \pi^k(x)$ であり,
- 任意の $y \in X - \{x, \pi(x), \ldots, \pi^{k-1}(x)\}$ に対して，$y = \pi(y)$

巡回置換を $\pi = (x\ \pi(x)\ \pi^2(x)\ \cdots\ \pi^{k-1}(x))$ とも表す　　(巡回記法)

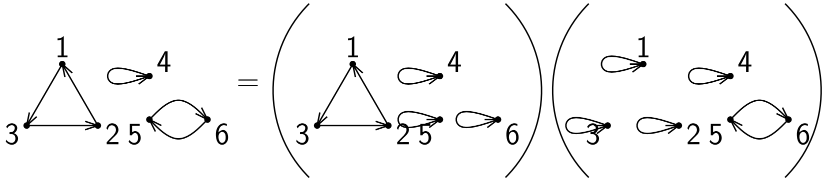


$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 4 & 2 & 5 & 3 \end{pmatrix} = (2\ 6\ 3\ 4)$$

置換の巡回記法

巡回記法とは？

置換を互いに素な巡回置換の積 (合成) として表したもの



$$\pi = (1\ 3\ 2)(5\ 6)$$

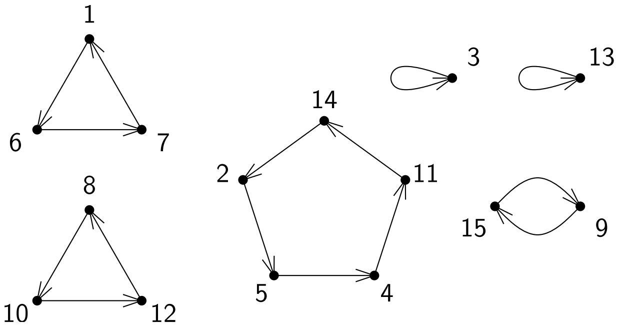
巡回記法に慣れる (1)

- 二行記法

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 6 & 5 & 3 & 11 & 4 & 7 & 1 & 10 & 15 & 12 & 14 & 8 & 13 & 2 & 9 \end{pmatrix}$$

- 巡回記法

$$(1\ 6\ 7)(2\ 5\ 4\ 11\ 14)(8\ 10\ 12)(9\ 15)$$



巡回記法に慣れる (2)

$X = \{1, 2, 3, 4\}$ 上の置換をすべて考えてみる

$$\begin{pmatrix}1 & 2 & 3 & 4\\1 & 2 & 3 & 4\end{pmatrix} = () \quad (\text{or, } e)$$

$$\begin{pmatrix}1 & 2 & 3 & 4\\1 & 2 & 4 & 3\end{pmatrix} = (3\ 4)$$

$$\begin{pmatrix}1 & 2 & 3 & 4\\1 & 3 & 2 & 4\end{pmatrix} = (2\ 3)$$

$$\begin{pmatrix}1 & 2 & 3 & 4\\1 & 3 & 4 & 2\end{pmatrix} = (2\ 3\ 4)$$

$$\begin{pmatrix}1 & 2 & 3 & 4\\1 & 4 & 2 & 3\end{pmatrix} = (2\ 4\ 3)$$

$$\begin{pmatrix}1 & 2 & 3 & 4\\1 & 4 & 3 & 2\end{pmatrix} = (2\ 4)$$

$$\begin{pmatrix}1 & 2 & 3 & 4\\2 & 1 & 3 & 4\end{pmatrix} = (1\ 2)$$

$$\begin{pmatrix}1 & 2 & 3 & 4\\2 & 1 & 4 & 3\end{pmatrix} = (1\ 2)(3\ 4)$$

$$\begin{pmatrix}1 & 2 & 3 & 4\\2 & 3 & 1 & 4\end{pmatrix} = (1\ 2\ 3)$$

$$\begin{pmatrix}1 & 2 & 3 & 4\\2 & 3 & 4 & 1\end{pmatrix} = (1\ 2\ 3\ 4)$$

$$\begin{pmatrix}1 & 2 & 3 & 4\\2 & 4 & 1 & 3\end{pmatrix} = (1\ 2\ 4\ 3)$$

$$\begin{pmatrix}1 & 2 & 3 & 4\\2 & 4 & 3 & 1\end{pmatrix} = (1\ 2\ 4)$$

巡回記法に慣れる (3)

$X = \{1, 2, 3, 4\}$ 上の置換をすべて考えてみる

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} = (1\ 3\ 2)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} = (1\ 3\ 4\ 2)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} = (1\ 3)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} = (2\ 3\ 4)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (1\ 3)(2\ 4)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} = (1\ 3\ 2\ 4)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} = (1\ 4\ 3\ 2)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} = (1\ 4\ 2)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} = (1\ 4\ 3)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix} = (1\ 4)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} = (1\ 4\ 2\ 3)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (1\ 4)(2\ 3)$$

目次

100 囚人の問題：設定

設定

- 100 人の死刑囚
- 死刑囚には番号が振られている $(1, 2, \ldots, 100)$
- 死刑囚は一人ずつ部屋に連れられて行き，そこで以下を行う
  - その部屋には $1, 2, \ldots, 100$ と番号の書かれた箱がある
  - 箱には $1, 2, \ldots, 100$ の中の番号が 1 つだけ書かれた紙が入っている
  - 紙に書かれている番号はすべて異なる
  - 死刑囚はその中の 50 個の箱を開けられる
  - 開けた箱の中に自分と同じ番号の紙が入っていれば「成功」
  - そうでなければ「失敗」
- 全員の死刑囚が成功すれば，全員釈放．そうでなければ，全員死刑

死刑囚は前もって相談できる

問題

死刑囚はどれほどの確率で「全員釈放」されるか？

100 囚人の問題：簡単な戦略

簡単な戦略

各死刑囚は，一様ランダムに 50 個の箱を明ける

この戦略で「全員釈放」となる確率は？

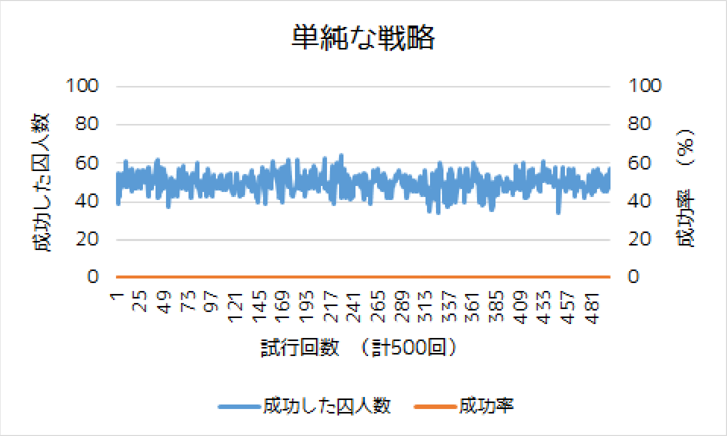
- 1 人の死刑囚が成功する確率は $\dfrac{50}{100} = \dfrac{1}{2}$
- $\therefore$ 100 人全員が成功する確率は

$$\left(\frac{1}{2}\right)^{100} \approx 7.89 \times 10^{-31}$$

これは「ほぼ 0」

シミュレーション：単純な戦略

500 回の試行



100 囚人の問題：賢い戦略 (Sven Skyum による)

賢い戦略

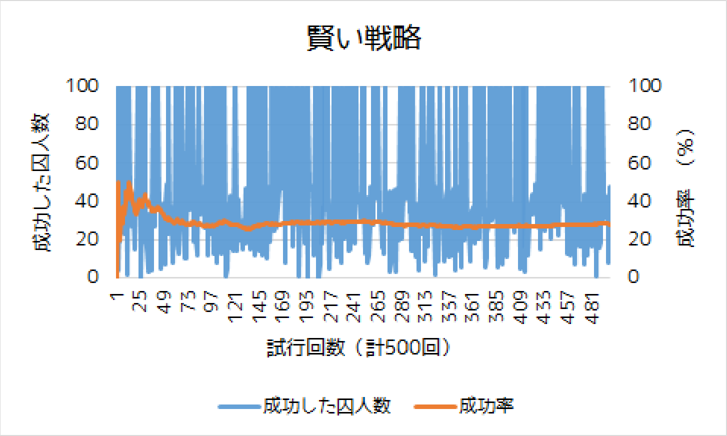
囚人 i は次の戦略を取る

(1) まず，箱 i を開ける
(2) いま開けた箱の紙に書いてあるのが i ならば，成功で終了
(3) そうでなければ，その紙に書いてある番号の箱を開けて (2) に戻る

これだけ

シミュレーション：賢い戦略

500 回の試行



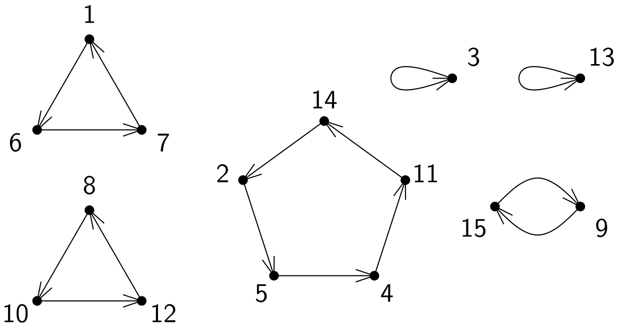
成功率 28.2%

解析：賢い戦略 (1)

鍵となる考え

「箱 i の中にある紙の番号が $\pi(i)$」という置換 π を考える

置換の巡回表現



すべての囚人が成功するのはいつか？

置換における互いに素な巡回置換の長さがどれも 50 以下であるとき

解析：賢い戦略 (2)

ある囚人が失敗するのはいつか？

置換における互いに素な巡回置換に長さが 50 を超えるものがあるとき

長さが 50 を超える巡回置換は 1 つしかない (要素数が 100 だから)

- その巡回置換の長さを ℓ とする ($\ell > 50$)
- 要素数 100 の置換の中で，長さ ℓ の巡回置換を持つものの総数は

$$\binom{100}{\ell}(\ell-1)!(100-\ell)!$$

- 整理すると

$$\binom{100}{\ell}(\ell-1)!(100-\ell)! = \frac{100!}{\ell!(100-\ell)!}(\ell-1)!(100-\ell)! = \frac{100!}{\ell}$$

解析：賢い戦略 (2)

ある囚人が失敗するのはいつか？

置換における互いに素な巡回置換に長さが 50 を超えるものがあるとき

- したがって，失敗確率は

$$\frac{1}{100!}\sum_{\ell=51}^{100}\frac{100!}{\ell}=\sum_{\ell=51}^{100}\frac{1}{\ell}\approx 0.68$$

- したがって，成功確率は

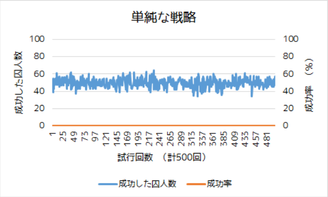
$$1-\sum_{\ell=51}^{100}\frac{1}{\ell}\approx 1-0.68=0.32$$

つまり，およそ 32 パーセントで成功する

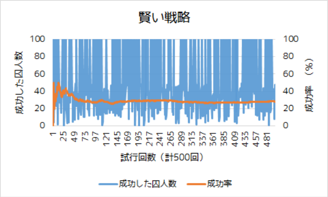
シミュレーション (再掲)

500 回の試行

単純な戦略



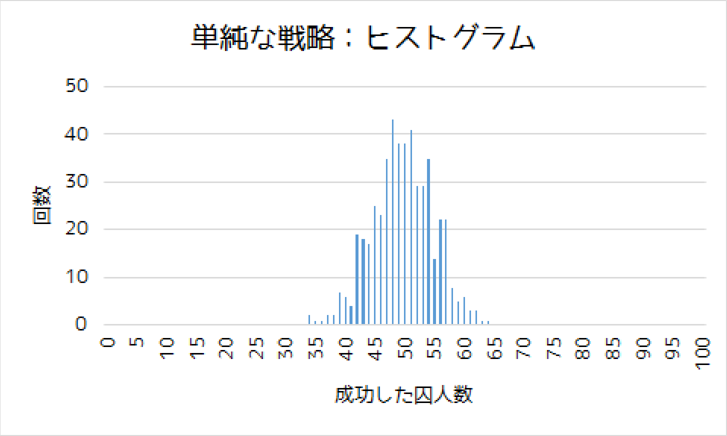
賢い戦略



何が起きているのか？

シミュレーション：単純な戦略 (ヒストグラム)

500 回の試行



成功した囚人数が 50 の周りに分布 (50 = 成功した囚人数の期待値)

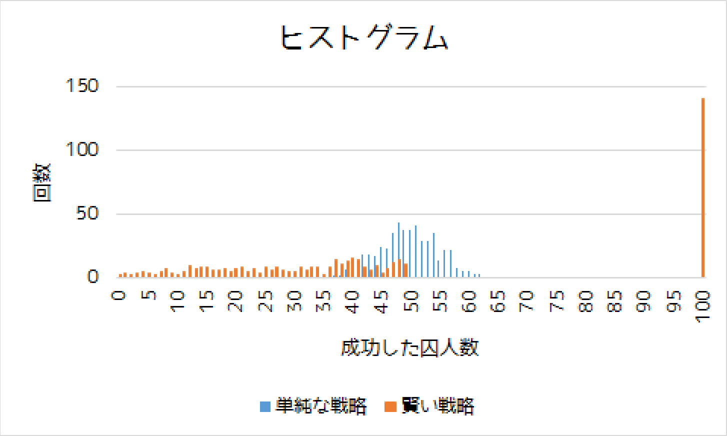
シミュレーション：賢い戦略 (ヒストグラム)

500 回の試行

成功した囚人数が 50 の周りに分布していない

シミュレーション：ヒストグラムを重ねて描いたもの

500 回の試行

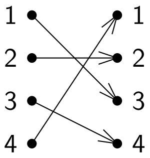


賢い戦略は囚人ごとの「独立性」を壊している

目次

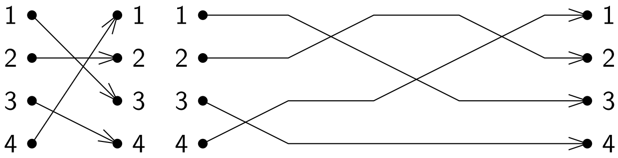
置換を互換の積として表してみる

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} =$$



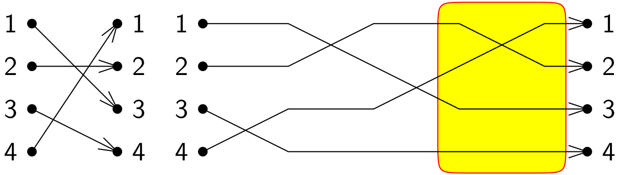
置換を互換の積として表してみる

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} = (1\ 2)(2\ 3)(1\ 2)(3\ 4)$$



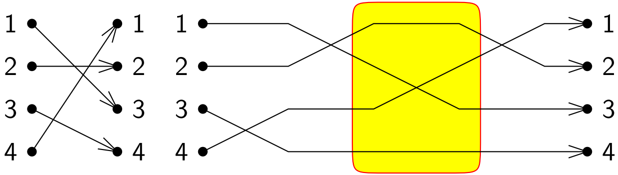
置換を互換の積として表してみる

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} = (1\ 2)(2\ 3)(1\ 2)(3\ 4)$$



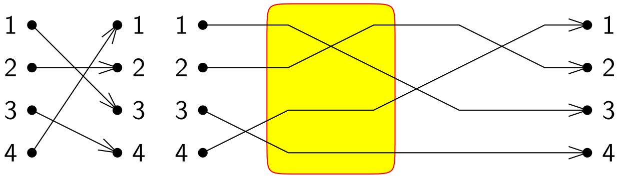
置換を互換の積として表してみる

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} = (1\ 2){\color{red}(2\ 3)}(1\ 2)(3\ 4)$$



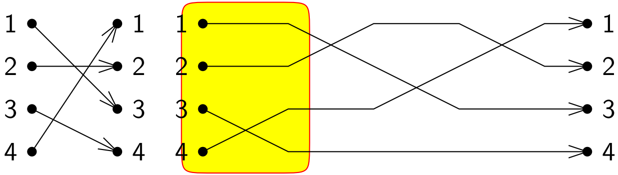
置換を互換の積として表してみる

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} = (1\ 2)(2\ 3)\textcolor{red}{(1\ 2)}(3\ 4)$$



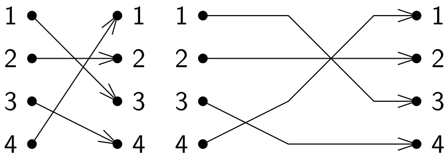
置換を互換の積として表してみる

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} = (1\ 2)(2\ 3)(1\ 2)(3\ 4)$$



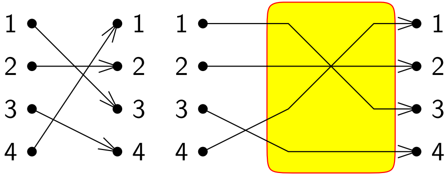
置換を互換の積として表してみる：Part 2

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} = (1\ 3)(3\ 4)$$



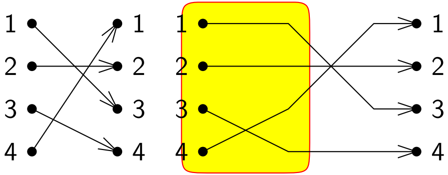
置換を互換の積として表してみる：Part 2

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} = (1\ 3)(3\ 4)$$



置換を互換の積として表してみる：Part 2

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} = (1\ 3)(3\ 4)$$



置換を互換の積として表してみる：互換の数の偶奇性

ここまでのまとめ

- 任意の置換は，いくつかの互換の積 (合成) として表せる
- その表し方は，一通りではない

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} = (1\ 2)(2\ 3)(1\ 2)(3\ 4) = (1\ 3)(3\ 4)$$

しかし，次が (一般的に) 言える

性質：互換の数の偶奇性

任意の有限集合 X 上の任意の置換 π に対して，
π を互換の積として表したとき，現れる互換の数の偶奇は必ず等しい

偶置換と奇置換

性質：互換の数の偶奇性 (再掲)

任意の有限集合 X 上の任意の置換 π に対して，
π を互換の積として表したとき，現れる互換の数の偶奇は必ず等しい

この性質をもとにして，次の用語を定義する

偶置換，奇置換とは？

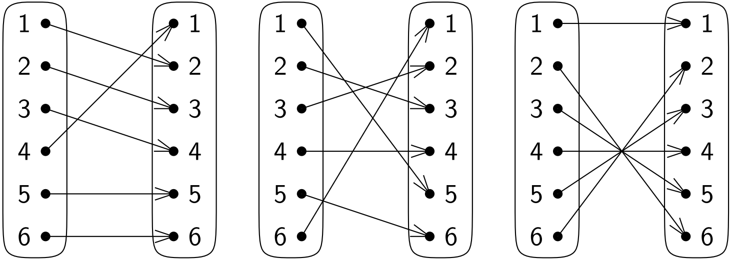
偶置換とは，偶数個の互換の積として表せる置換のこと
奇置換とは，奇数個の互換の積として表せる置換のこと

例：

- 恒等置換 e は偶置換
- 巡回置換 $(1\ 2\ 3\ 4)$ は奇置換　　$((1\ 2\ 3\ 4) = (1\ 2)(2\ 3)(3\ 4))$

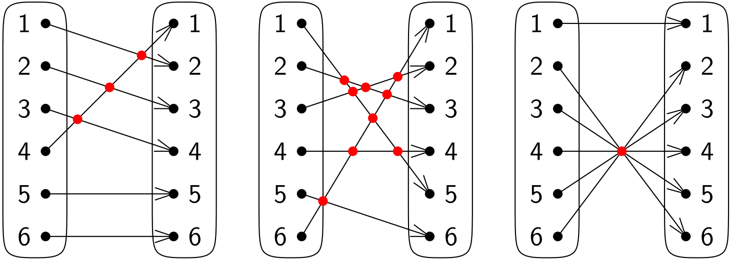
偶置換か奇置換か，簡単に判別するには？

「交点の数」の偶奇を調べればよい



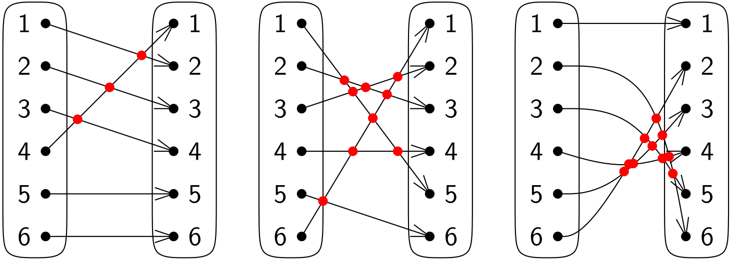
偶置換か奇置換か，簡単に判別するには？

「交点の数」の偶奇を調べればよい



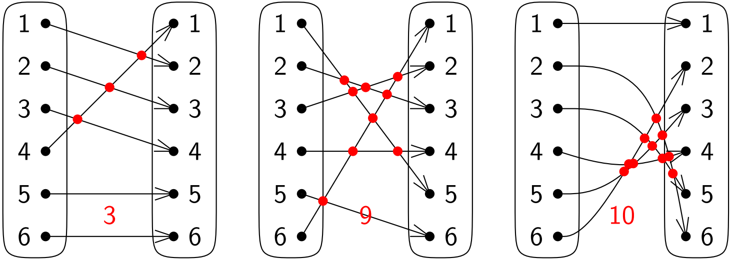
偶置換か奇置換か，簡単に判別するには？

「交点の数」の偶奇を調べればよい



偶置換か奇置換か，簡単に判別するには？

「交点の数」の偶奇を調べればよい



目次

置換群とは？

有限集合 X

置換群とは？

X 上の置換群とは，X 上の置換の集合 S で以下を満たすもの

1. $e \in S$ (恒等置換を持つ)
2. $\pi, \sigma \in S$ ならば $\pi\sigma \in S$ (積で閉じている)
3. $\pi \in S$ ならば $\pi^{-1} \in S$ (逆置換も持つ)

代表的な置換群 (1)：対称群

有限集合 X

対称群とは？

X 上の**対称群**とは，X 上の置換をすべて集めた集合

- $S(X)$, $\mathcal{S}(X)$, $\mathfrak{S}(X)$ と書くことが多い
- $|X| = n$ のときは，n 次の対称群 (n 次対称群) と呼ばれ，S_n, $\mathcal{S}_n$, $\mathfrak{S}_n$ と書くことが多い

例：$X = \{1, 2, 3\}$ のとき

$$S_3 = \{e, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$$

注：$|S_n| = n!$

代表的な置換群 (2)：交代群

有限集合 X

交代群とは？

X 上の交代群とは，X 上の偶置換をすべて集めた集合

- $A(X)$, $\mathcal{A}(X)$, $\mathfrak{A}(X)$ と書くことが多い
- $|X| = n$ のときは，n 次の交代群 (n 次交代群) と呼ばれ，A_n, $\mathcal{A}_n$, $\mathfrak{A}_n$ と書くことが多い

例：$X = \{1, 2, 3\}$ のとき

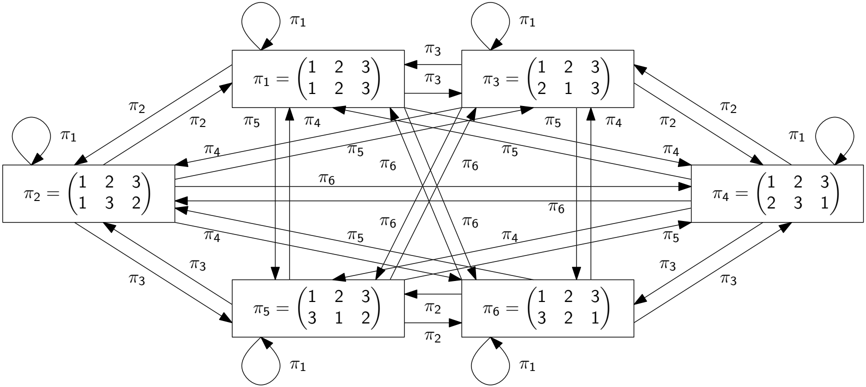
$$A_3 = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$$

注：$|A_n| = n!/2$

目次

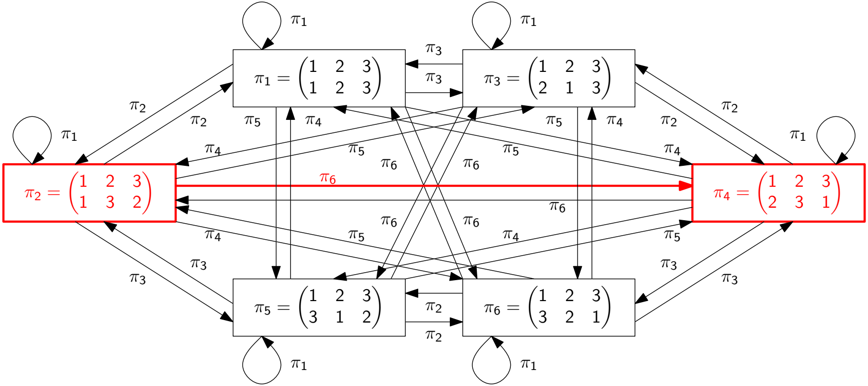
対称群の生成 (1)

ケーリー・グラフ (定義は後ほど)



対称群の生成 (1)

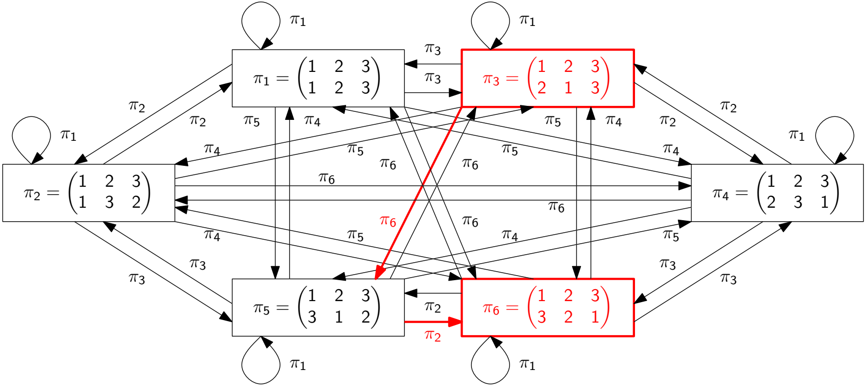
ケーリー・グラフ (定義は後ほど)



$\pi_2\pi_6 = \pi_4$

対称群の生成 (1)

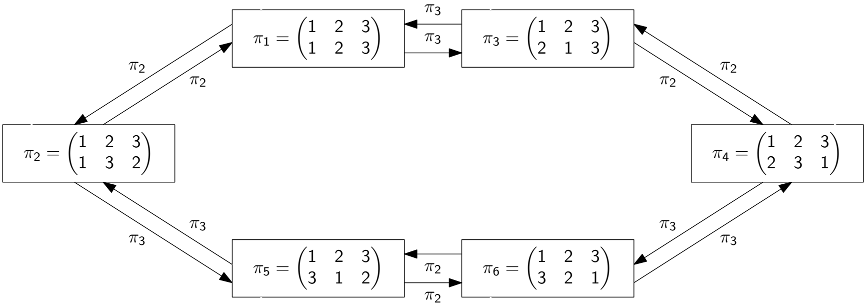
ケーリー・グラフ (定義は後ほど)



$\pi_3\pi_6\pi_2 = \pi_6$

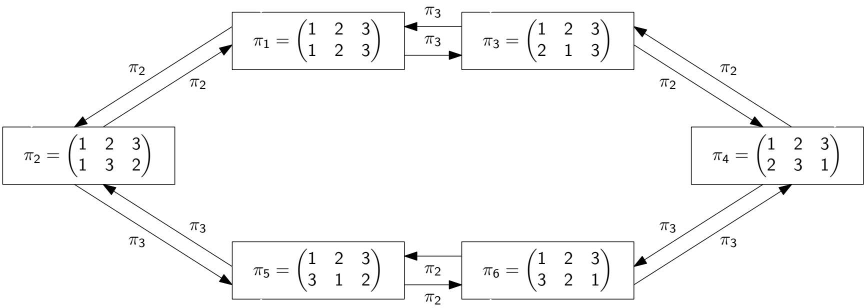
対称群の生成 (2)

ケーリー・グラフ (定義は後ほど)



対称群の生成 (2)

ケーリー・グラフ (定義は後ほど)



π_2, π_3 は対称群 S_3 を生成する

置換群を生成する (1)

例題 1

$X = \{1, 2, 3\}$ 上の置換群で，$\pi = (1\ 2\ 3)$ が生成するものを G とすると，G は何？

$$\boxed{e}$$

置換群を生成する (1)

例題 1

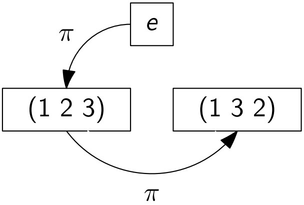
$X = \{1, 2, 3\}$ 上の置換群で，$\pi = (1\ 2\ 3)$ が生成するものを G とすると，G は何？

$$\boxed{e} \xrightarrow{\pi} \boxed{(1\ 2\ 3)}$$

置換群を生成する (1)

例題 1

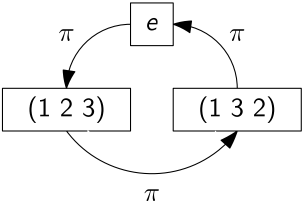
$X = \{1, 2, 3\}$ 上の置換群で，$\pi = (1\ 2\ 3)$ が生成するものを G とすると，G は何？



置換群を生成する (1)

例題 1

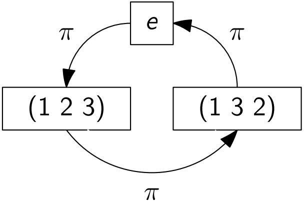
$X = \{1, 2, 3\}$ 上の置換群で，$\pi = (1\ 2\ 3)$ が生成するものを G とすると，G は何？



置換群を生成する (1)

例題 1

$X = \{1, 2, 3\}$ 上の置換群で，$\pi = (1\ 2\ 3)$ が生成するものを G とすると，G は何？



よって，$G = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$

置換群を生成する (2)

例題 2

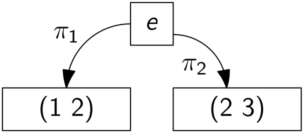
$X = \{1,2,3\}$ 上の置換群で，
$\pi_1 = (1\ 2)$ と $\pi_2 = (2\ 3)$ が生成するものを G とすると，G は何？

$$\boxed{e}$$

置換群を生成する (2)

例題 2

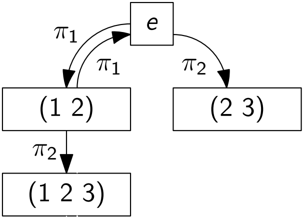
$X = \{1, 2, 3\}$ 上の置換群で，
$\pi_1 = (1\ 2)$ と $\pi_2 = (2\ 3)$ が生成するものを G とすると，G は何？



置換群を生成する (2)

例題 2

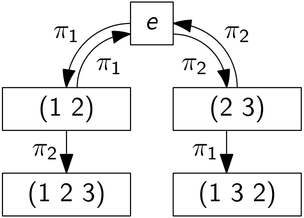
$X = \{1, 2, 3\}$ 上の置換群で，
$\pi_1 = (1\ 2)$ と $\pi_2 = (2\ 3)$ が生成するものを G とすると，G は何？



置換群を生成する (2)

例題 2

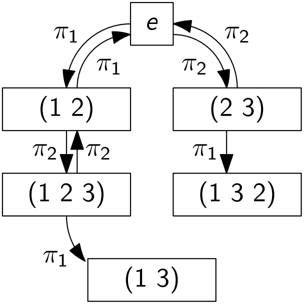
$X = \{1, 2, 3\}$ 上の置換群で，
$\pi_1 = (1\ 2)$ と $\pi_2 = (2\ 3)$ が生成するものを G とすると，G は何？



置換群を生成する (2)

例題 2

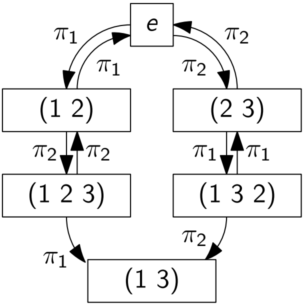
$X = \{1, 2, 3\}$ 上の置換群で，
$\pi_1 = (1\ 2)$ と $\pi_2 = (2\ 3)$ が生成するものを G とすると，G は何？



置換群を生成する (2)

例題 2

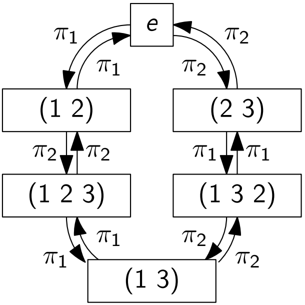
$X = \{1, 2, 3\}$ 上の置換群で，
$\pi_1 = (1\ 2)$ と $\pi_2 = (2\ 3)$ が生成するものを G とすると，G は何？



置換群を生成する (2)

例題 2

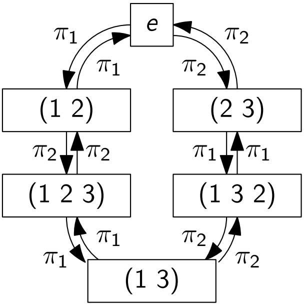
$X = \{1, 2, 3\}$ 上の置換群で，
$\pi_1 = (1\ 2)$ と $\pi_2 = (2\ 3)$ が生成するものを G とすると，G は何？



置換群を生成する (2)

例題 2

$X = \{1, 2, 3\}$ 上の置換群で，
$\pi_1 = (1\ 2)$ と $\pi_2 = (2\ 3)$ が生成するものを G とすると，G は何？



よって，$G = \{e, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\} = S_3$

置換群の生成系

有限集合 $X = \{1, 2, \ldots, n\}$

置換の集合が生成する置換群とは？

X 上の置換の集合 S に対して，S が生成する X 上の置換群とは，
X 上の置換群で，S を含むような最小のもの
$\langle S \rangle$ と書く

先ほどの例：$X = \{1, 2, 3\}$ のとき

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

注：$\langle \{(1\ 2), (2\ 3)\} \rangle$ と書かず，$\langle (1\ 2), (2\ 3) \rangle$ と書くことも多い

用語

置換群 G に対して，$G = \langle S \rangle$ であるとき，
S を G の生成系と呼ぶ (ことがある)

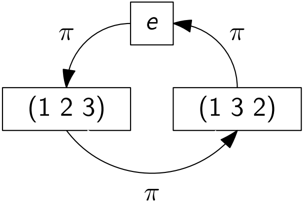
ケーリー・グラフ

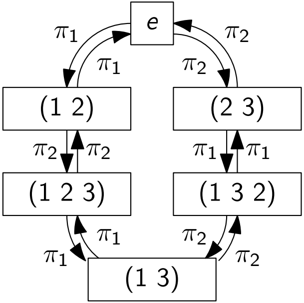
置換群 G とその生成系 S

ケーリー・グラフとは？

(G, S) のケーリー・グラフとは，次で定義される有向グラフ

- 頂点集合は G
- 孤 $(\pi, \pi') \in G \times G$ がある $\Leftrightarrow$ ある $\sigma \in S$ が存在して，$\pi' = \pi\sigma$





目次

今日の目標

今日の目標

置換群に関する基礎的な用語が使えるようになる

- 置換，二行記法，巡回記法，互換
- 偶置換，奇置換
- 置換群，対称群，交代群
- 生成系

残った時間の使い方

- 演習問題をやる
  - 相談推奨 (ひとりでやらない)
- 質問をする
  - 教員と TA は巡回
- 退室時，小さな紙に感想など書いて提出する ← 重要
  - 内容は何でも OK
  - 匿名で OK

目次