離散最適化基礎論　第 3 回
最小包囲円問題 (2)：乱択アルゴリズム

岡本 吉央
okamotoy@uec.ac.jp

電気通信大学

2017 年 10 月 27 日

最終更新：2017 年 10 月 27 日　11:34

概要

主題

離散最適化のトピックの１つとして幾何的被覆問題を取り上げ，
その数理的側面と計算的側面の双方を意識して講義する

なぜ講義で取り扱う？

- 「離散最適化」と「計算幾何学」の接点として重要な役割を果たしているから
- 様々なアルゴリズム設計技法・解析技法を紹介できるから
- 応用が多いから

スケジュール 前半 (予定)

1. 幾何的被覆問題とは？ (10/6)
- ⋆ 国内出張のため休み (10/13)
2. 最小包囲円問題 (1)：基本的な性質 (10/20)
3. 最小包囲円問題 (2)：乱択アルゴリズム (10/27)
- ⋆ 文化の日のため休み (11/3)
4. クラスタリング (1)：k-センター (11/10)
5. 幾何ハイパーグラフ (1)：VC 次元 (11/17)
- ⋆ 調布祭 のため 休み (11/24)
6. 幾何ハイパーグラフ (2)：ε ネット (12/1)

注意：予定の変更もありうる

スケジュール 後半 (予定)

7. 幾何的被覆問題 (1)：線形計画法の利用 (12/8)
8. 幾何的被覆問題 (2)：シフト法 (12/15)
9. 幾何的被覆問題 (3)：局所探索法 (12/22)
10. 幾何的被覆問題 (4)：局所探索法の解析 (1/5)

★ センター試験準備 のため 休み (1/12)

11. 幾何ハイパーグラフ (3)：ε ネット定理の証明 (1/19)
12. 幾何アレンジメント (1)：合併複雑度と ε ネット (1/26)
13. 幾何アレンジメント (2)：合併複雑度の例 (2/2)
14. 最近のトピック (2/9)
15. 期末試験 (2/16？)

注意：予定の変更もありうる

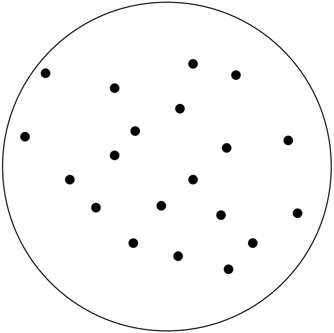
今日の内容

最小包囲円問題に対する乱択アルゴリズム

- 最小包囲円アルゴリズムの復習
- 最小包囲円アルゴリズムの乱択化
- 乱択アルゴリズムの解析

最小包囲円問題

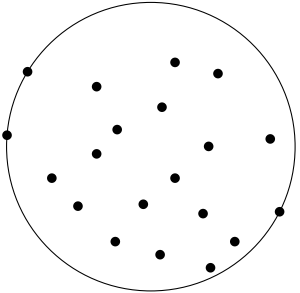
平面上にいくつか点が与えられたとき
それらをすべて含む円の中で面積が最小のものを求めよ



注意：円に対しては，面積の最小化 $\Leftrightarrow$ 半径の最小化

最小包囲円問題

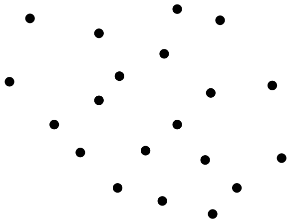
平面上にいくつか点が与えられたとき
それらをすべて含む円の中で面積が最小のものを求めよ



注意：円に対しては，面積の最小化 $\Leftrightarrow$ 半径の最小化

記法

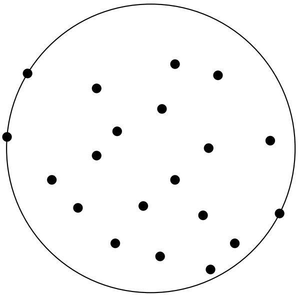
- $P \subseteq \mathbb{R}^2$：与えられる平面上の点の集合
- $\mathrm{sed}(P)$：P の**最小包囲円** (smallest enclosing disk)
  - P を含む円で面積最小のもの



「最小包含円」と呼ぶこともある

記法

- $P \subseteq \mathbb{R}^2$：与えられる平面上の点の集合
- $\mathrm{sed}(P)$：P の最小包囲円 (smallest enclosing disk)
  - P を含む円で面積最小のもの

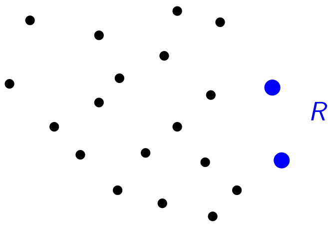


「最小包含円」と呼ぶこともある

記法

- $P \subseteq \mathbb{R}^2$：与えられる平面上の点の集合
- $R \subseteq P$：部分集合
- $\mathrm{sed}(P, R)$：R を境界上に持つ P の包囲円の中で，面積最小のもの

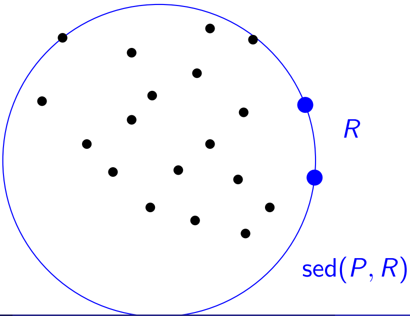
R 以外の点が境界にあってもよい



記法

- $P \subseteq \mathbb{R}^2$：与えられる平面上の点の集合
- $R \subseteq P$：部分集合
- $\mathrm{sed}(P, R)$：R を境界上に持つ P の包囲円の中で，面積最小のもの

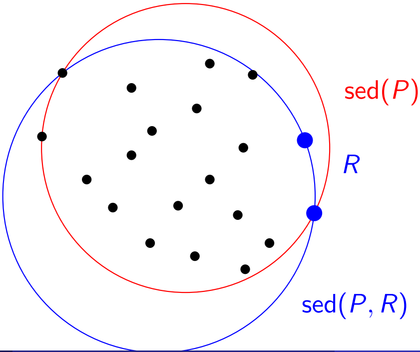
R 以外の点が境界にあってもよい



記法

- $P \subseteq \mathbb{R}^2$：与えられる平面上の点の集合
- $R \subseteq P$：部分集合
- $\mathrm{sed}(P, R)$：R を境界上に持つ P の包囲円の中で，面積最小のもの

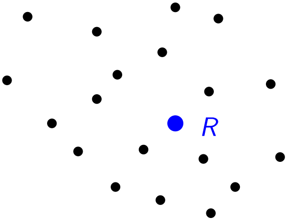
R 以外の点が境界にあってもよい



記法

- $P \subseteq \mathbb{R}^2$：与えられる平面上の点の集合
- $R \subseteq P$：部分集合
- $\mathrm{sed}(P, R)$：R を境界上に持つ P の包囲円の中で，面積最小のもの

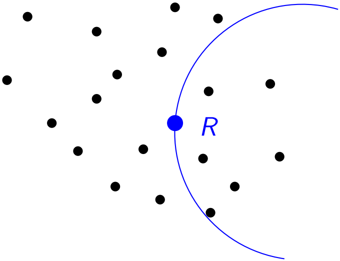
注意：$\mathrm{sed}(P, R)$ は存在しないかもしれない



記法

- $P \subseteq \mathbb{R}^2$：与えられる平面上の点の集合
- $R \subseteq P$：部分集合
- $\mathrm{sed}(P, R)$：R を境界上に持つ P の包囲円の中で，面積最小のもの

<u>注意</u>：$\mathrm{sed}(P, R)$ は存在しないかもしれない



入力：有限点集合 $P \subseteq \mathbb{R}^2$ ($|P| \geq 1$)，$R \subseteq P$

(1) $|P| \leq 2$ ならば，$\mathrm{sed}(P, R)$ を直接計算して，終了

(2) $|R| \geq 3$ ならば，$\mathrm{sed}(P, R)$ を直接計算して，終了

(3) $|P| \geq 3$ かつ $|R| \leq 2$ ならば，$p \in P - R$ を任意に選ぶ

(3-1) $\mathrm{sed}(P - \{p\}, R)$ を再帰的に計算 (存在しないならば終了)

(3-2) $\mathrm{sed}(P - \{p\}, R)$ が存在し，$p \in \mathrm{sed}(P - \{p\}, R)$ ならば，
$\mathrm{sed}(P, R) = \mathrm{sed}(P - \{p\}, R)$ として，終了

(3-3) $\mathrm{sed}(P - \{p\}, R)$ が存在し，$p \notin \mathrm{sed}(P - \{p\}, R)$ ならば，
$\mathrm{sed}(P, R \cup \{p\})$ を再帰的に計算して，
$\mathrm{sed}(P, R) = \mathrm{sed}(P, R \cup \{p\})$ として，終了

観察

- 前ページの命題より，このアルゴリズムの出力は正しい
- 再帰呼出において，$|P|$ が減るか，または，$|R|$ が増えるので，アルゴリズムは必ず終了する

入力：有限点集合 $P \subseteq \mathbb{R}^2$ ($|P| \geq 1$)，$R \subseteq P$

(1) $|P| \leq 2$ ならば，$\mathrm{sed}(P, R)$ を直接計算して，終了

(2) $|R| \geq 3$ ならば，$\mathrm{sed}(P, R)$ を直接計算して，終了

(3) $|P| \geq 3$ かつ $|R| \leq 2$ ならば，$p \in P - R$ を任意に選ぶ

(3-1) $\mathrm{sed}(P - \{p\}, R)$ を再帰的に計算 (存在しないならば終了)

(3-2) $\mathrm{sed}(P - \{p\}, R)$ が存在し，$p \in \mathrm{sed}(P - \{p\}, R)$ ならば，
$\mathrm{sed}(P, R) = \mathrm{sed}(P - \{p\}, R)$ として，終了

(3-3) $\mathrm{sed}(P - \{p\}, R)$ が存在し，$p \notin \mathrm{sed}(P - \{p\}, R)$ ならば，
$\mathrm{sed}(P, R \cup \{p\})$ を再帰的に計算して，
$\mathrm{sed}(P, R) = \mathrm{sed}(P, R \cup \{p\})$ として，終了

P の最小包囲円を求めるためには？

$R = \emptyset$ として，このアルゴリズムを動かせばよい

ステップ (1), (2) の「直接計算」は (前回の) 演習問題

結論：このアルゴリズムの計算量

平面上に与えられた n 個の点の最小包囲円は $O(n^4)$ 時間で計算できる

この結論は「当たり前」(もっと簡単なアルゴリズムで実現できる)

実際に動かしてみた

次のように実装してみた

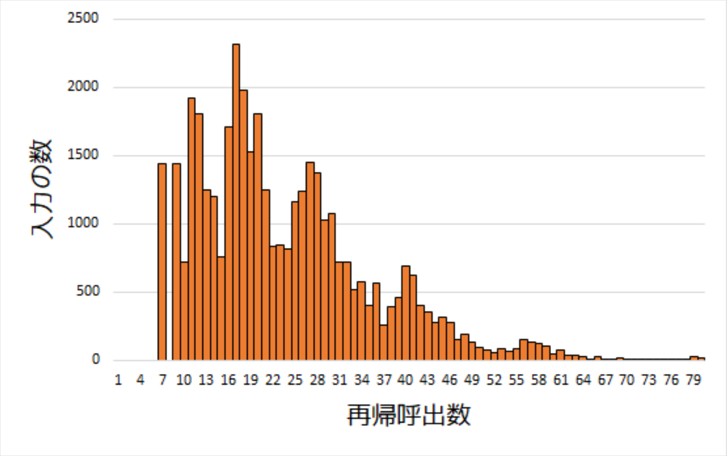
- ステップ 3 の「$p \in P - R$ を任意に選ぶ」という部分は，「添え字が最大のものを選ぶ」とした

次のような入力を考えてみた

$$\begin{array}{ccccccc} \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\ 1 & 2 & 3 & 4 & & n{-}1 & n \end{array}$$

- 添え字の付け方を全通り試してみた (つまり，$n!$ 通り)
- $n = 8$ とした (注：$8! = 40,320$)

アルゴリズムにおける再帰呼出回数の頻度分布



最小値 7，最大値 80，平均値 23.69，中央値 21

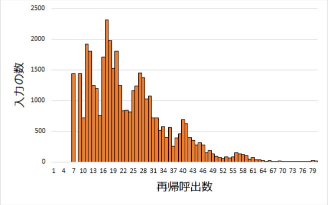
実際に動かしてみた：実験結果 — 考察

考察

- 「最悪の場合」は，そんなに起こらない
- 「平均の場合」は,「最悪の場合」よりもはるかによい

⇝ 乱数を使えば,「最悪の場合」を避けやすくなるのではないか？

アルゴリズムにおける再帰呼出回数の頻度分布



目次

1. 最小包囲円を求めるアルゴリズム：乱択化
2. 確率の復習
3. 乱択アルゴリズムの解析
4. 今日のまとめ

入力：有限点集合 $P \subseteq \mathbb{R}^2$ ($|P| \geq 1$)，$R \subseteq P$

(1) $|P| \leq 2$ ならば，$\mathrm{sed}(P, R)$ を直接計算して，終了

(2) $|R| \geq 3$ ならば，$\mathrm{sed}(P, R)$ を直接計算して，終了

(3) $|P| \geq 3$ かつ $|R| \leq 2$ ならば，$p \in P - R$ を一様分布に従って選ぶ

(3-1) $\mathrm{sed}(P - \{p\}, R)$ を再帰的に計算 (存在しないならば終了)

(3-2) $\mathrm{sed}(P - \{p\}, R)$ が存在し，$p \in \mathrm{sed}(P - \{p\}, R)$ ならば，
$\mathrm{sed}(P, R) = \mathrm{sed}(P - \{p\}, R)$ として，終了

(3-3) $\mathrm{sed}(P - \{p\}, R)$ が存在し，$p \notin \mathrm{sed}(P - \{p\}, R)$ ならば，
$\mathrm{sed}(P, R \cup \{p\})$ を再帰的に計算して，
$\mathrm{sed}(P, R) = \mathrm{sed}(P, R \cup \{p\})$ として，終了

「$p \in P - R$ を一様分布に従って選ぶ」とは？

各点 $p \in P - R$ を確率 $\dfrac{1}{|P - R|}$ で選ぶ

言い換えると，任意の $p \in P - R$ に対して

$$\Pr(\text{ステップ (3) で } p \text{ が選ばれる}) = \frac{1}{|P - R|}$$

今から行うこと：乱択アルゴリズムの解析

- 記法：$t(P, R) =$ 入力を P, R としたときの計算量 (確率変数)
- 考えたい量：**最悪期待計算量**

$$\tilde{t}(n, k) = \max\{\mathrm{E}[t(P, R)] \mid |P| = n, |R| = k\}$$

つまり，計算量の期待値 (平均) が最も大きくなる入力を考える

前回考えた量：

$$\begin{aligned} t(n, k) &= (|P| = n, |R| = k \text{ のときの最悪計算量}) \\ &= \max\{t(P, R) \mid |P| = n, |R| = k\} \end{aligned}$$

(ただし，$t(P, R)$ は確率的に決まるものではなかった)

1. 最小包囲円を求めるアルゴリズム：乱択化
2. 確率の復習
3. 乱択アルゴリズムの解析
4. 今日のまとめ

確率空間とは？

確率空間とは，集合 Ω と，関数 $\mathrm{Pr}\colon \Omega \to \mathbb{R}$ の対 (Ω, Pr) で次を満たすもののこと

1. 任意の $\omega \in \Omega$ に対して，$0 \leq \mathrm{Pr}(\omega) \leq 1$
2. $\displaystyle\sum_{\omega \in \Omega} \mathrm{Pr}(\omega) = 1$

この講義では，2 にある和が定義できる場合のみ考える (例えば，$\Omega = \mathbb{R}$ の場合は考えない)

例：公平なサイコロ

公平なサイコロを振ったときの出目を表す確率空間は

- $\Omega = \{1, 2, 3, 4, 5, 6\}$
- $\mathrm{Pr}(1) = \mathrm{Pr}(2) = \mathrm{Pr}(3) = \mathrm{Pr}(4) = \mathrm{Pr}(5) = \mathrm{Pr}(6) = \dfrac{1}{6}$

事象とは？

- 確率空間 (Ω, Pr) における**事象**とは，Ω の部分集合のこと
- 事象 $A \subseteq \Omega$ に対して，A の確率を次で定義

$$\mathrm{Pr}(A) = \sum_{\omega \in A} \mathrm{Pr}(\omega)$$

例：サイコロ

$A = \{1, 3, 5\} \subseteq \{1, 2, 3, 4, 5, 6\} = \Omega$ に対して

$$\mathrm{Pr}(A) = \mathrm{Pr}(1) + \mathrm{Pr}(3) + \mathrm{Pr}(5) = \frac{1}{6} + \frac{1}{6} + \frac{1}{6} = \frac{1}{2}$$

(A は「出目が奇数である」という事象)

事象とは？

- 確率空間 $(\Omega, \Pr)$ における**事象**とは，Ω の部分集合のこと
- 事象 $A \subseteq \Omega$ に対して，A の確率を次で定義

$$\Pr(A) = \sum_{\omega \in A} \Pr(\omega)$$

用語

- Ω：全事象
- $\emptyset$：空事象
- 各 $\omega \in \Omega$：根元事象
- 各 $A \subseteq \Omega$ に対する $\Omega - A$：A の余事象

注意

$\Pr(\Omega) = 1$，$\Pr(\emptyset) = 0$

確率変数とは？

確率空間 $(\Omega, \Pr)$ 上の (実数値) **確率変数**とは,
各根元事象に実数を割り当てる関数 $X\colon \Omega \to \mathbb{R}$

例：サイコロ

「出目の 2 乗」を表す確率変数 X $(\Omega = \{1, 2, 3, 4, 5, 6\})$

$$
\begin{aligned}
&X(1) = 1, && X(2) = 4, && X(3) = 9,\\
&X(4) = 16, && X(5) = 25, && X(6) = 36
\end{aligned}
$$

- 事象「$X = a$」は「$\{\omega \in \Omega \mid X(\omega) = a\}$」を表す
- つまり，$\Pr(X = a) = \displaystyle\sum_{\omega : X(\omega) = a} \Pr(\omega)$
- 同様に，$\Pr(X \leq a) = \displaystyle\sum_{\omega : X(\omega) \leq a} \Pr(\omega)$

例：公平なサイコロ

「出目の 2 乗」を表す確率変数 X に対して

- $\Pr(X = 9) = \Pr(3) = \dfrac{1}{6}$
- $\Pr(10 \leq X \leq 30) = \Pr(4) + \Pr(5) = \dfrac{1}{6} + \dfrac{1}{6} = \dfrac{1}{3}$

事象と述語：表記法

- Ω 上の述語「P」を「$\{\omega \in \Omega \mid P(\omega)\}$」という事象と同一視する
- つまり，$\Pr(P) = \displaystyle\sum_{\omega : P(\omega)} \Pr(\omega)$

例：公平なサイコロ

- $\Pr(\text{出目が偶数}) = \Pr(2) + \Pr(4) + \Pr(6) = \dfrac{1}{2}$
- $\Pr(\text{出目が 3 以上}) = \Pr(3) + \Pr(4) + \Pr(5) + \Pr(6) = \dfrac{2}{3}$

- これで，$\Pr(P \text{ かつ } Q), \Pr(P \text{ または } Q), \Pr(P \text{ ではない})$ のような表記も可能

(離散) 確率空間 $(\Omega, \Pr)$

排反事象とは？

2 つの事象 A と B が排反であるとは

$$A \cap B = \emptyset$$

であること

注：A と B が排反であるとき，$\Pr(A \cap B) = 0$

独立事象とは？

2 つの事象 A と B が独立であるとは

$$\Pr(A \cap B) = \Pr(A) \cdot \Pr(B)$$

であること

(離散) 確率空間 $(\Omega, \Pr)$

確率変数の独立性とは？

確率変数 $X, Y \colon \Omega \to \mathbb{R}$ が独立であるとは，任意の $a, b \in \mathbb{R}$ に対して

$$\Pr(X = a \text{ かつ } Y = b) = \Pr(X = a) \cdot \Pr(Y = b)$$

となること

(離散) 確率空間 $(\Omega, \Pr)$

確率変数の独立性とは?: 相互独立性

確率変数 $X_1, X_2, \ldots, X_n \colon \Omega \to \mathbb{R}$ が互いに独立であるとは,
任意の $J \subseteq \{1, 2, \ldots, n\}$ と任意の $a_i \in \mathbb{R}$ $(i \in J)$ に対して

$$\Pr\left(\bigwedge_{i \in J} (X_i = a_i)\right) = \prod_{i \in J} \Pr(X_i = a_i)$$

となること

例

サイコロを n 回振り，i 回目の出目を X_i とするとき，
$X_1, X_2, \ldots, X_n$ は互いに独立

証明：任意の $J \subseteq \{1, \ldots, n\}$ と任意の $a_i \in \mathbb{R}$ $(i \in J)$ に対して

$$\begin{aligned}
\Pr\left(\bigwedge_{i \in J} (X_i = a_i)\right) &= \begin{cases} \left(\dfrac{1}{6}\right)^{|J|} & (\text{すべての } i \text{ に対して } a_i \in \{1, \ldots, 6\}) \\ 0 & (\text{そうでない}) \end{cases} \\
&= \prod_{i \in J} \Pr(X_i = a_i)
\end{aligned}$$

(離散) 確率空間 $(\Omega, \Pr)$

確率の加法性

事象 A, B が排反であるとき，$\Pr(A \cup B) = \Pr(A) + \Pr(B)$

確率の加法性：系

事象 A, A_1, A_2 が $\Omega = A_1 \cup A_2$ と $A_1 \cap A_2 = \emptyset$ を満たすとき

$$\Pr(A) = \Pr(A \cap A_1) + \Pr(A \cap A_2)$$

注：$\Pr((A \cap A_1) \cap (A \cap A_2)) = \Pr(\emptyset) = 0$

余事象の確率

任意の $A \subseteq \Omega$ に対して，

$$\Pr(\Omega - A) = 1 - \Pr(A)$$

(離散) 確率空間 $(\Omega, \Pr)$，事象 A, B，$\Pr(B) \neq 0$

条件つき確率とは？

事象 B のもとでの A の条件つき確率とは

$$\Pr(A \mid B) = \frac{\Pr(A \cap B)}{\Pr(B)}$$

例：公平なサイコロを 1 つ振る

偶数が出たという条件のもとで 2 が出る確率は

$$\frac{\Pr(\text{偶数が出て，かつ，2 が出る})}{\Pr(\text{偶数が出る})} = \frac{\Pr(\text{2 が出る})}{\Pr(\text{偶数が出る})} = \frac{1/6}{1/2} = \frac{1}{3}$$

偶数が出たという条件のもとで 3 が出る確率は

$$\frac{\Pr(\text{偶数が出て，かつ，3 が出る})}{\Pr(\text{偶数が出る})} = \frac{\Pr(\emptyset)}{\Pr(\text{偶数が出る})} = 0$$

(離散) 確率空間 $(\Omega, \Pr)$

確率の加法性：系

事象 A, A_1, A_2 が $\Omega = A_1 \cup A_2$ と $A_1 \cap A_2 = \emptyset$ を満たすとき

$$\Pr(A) = \Pr(A \cap A_1) + \Pr(A \cap A_2)$$

- ここで，$\Pr(A_1), \Pr(A_2) \neq 0$ のとき

$$\Pr(A \mid A_1) = \frac{\Pr(A \cap A_1)}{\Pr(A_1)}, \quad \Pr(A \mid A_2) = \frac{\Pr(A \cap A_2)}{\Pr(A_2)}$$

- したがって，上の仮定の下で

$$\Pr(A) = \Pr(A \mid A_1)\Pr(A_1) + \Pr(A \mid A_2)\Pr(A_2)$$

期待値

期待値とは？

確率空間 $(\Omega, \Pr)$ 上の自然数値確率変数 X の**期待値**とは

$$\mathrm{E}[X] = \sum_{i=0}^{\infty} i \cdot \Pr(X = i)$$

注：期待値が存在しない (発散する) 場合もある

例：公平なサイコロ

$X =$ サイコロの出目 とすると

$$\mathrm{E}[X] = 1 \cdot \frac{1}{6} + 2 \cdot \frac{1}{6} + 3 \cdot \frac{1}{6} + 4 \cdot \frac{1}{6} + 5 \cdot \frac{1}{6} + 6 \cdot \frac{1}{6} = \frac{7}{2}$$

期待値：例

$X =$ サイコロの出目 とすると

$$\begin{aligned} \mathrm{E}[X] &= 1 \cdot \frac{1}{6} + 2 \cdot \frac{1}{6} + 3 \cdot \frac{1}{6} + 4 \cdot \frac{1}{6} + 5 \cdot \frac{1}{6} + 6 \cdot \frac{1}{6} = \frac{7}{2}, \\ \mathrm{E}[X^2] &= \sum_{i=0}^{\infty} i \cdot \Pr(X^2 = i) \\ &= 1^2 \cdot \frac{1}{6} + 2^2 \cdot \frac{1}{6} + 3^2 \cdot \frac{1}{6} + 4^2 \cdot \frac{1}{6} + 5^2 \cdot \frac{1}{6} + 6^2 \cdot \frac{1}{6} = \frac{91}{6} \end{aligned}$$

X のとりうる値は $1, 2, 3, 4, 5, 6$ なので，
X^2 のとりうる値は $1^2, 2^2, 3^2, 4^2, 5^2, 6^2$ で，それぞれ確率 $1/6$ で生起する

期待値：例

$X =$ サイコロの出目 とすると

$$\begin{aligned} \mathrm{E}[X] &= 1 \cdot \frac{1}{6} + 2 \cdot \frac{1}{6} + 3 \cdot \frac{1}{6} + 4 \cdot \frac{1}{6} + 5 \cdot \frac{1}{6} + 6 \cdot \frac{1}{6} = \frac{7}{2}, \\ \mathrm{E}[X^2] &= \sum_{i=0}^{\infty} i \cdot \Pr(X^2 = i) \\ &= 1^2 \cdot \frac{1}{6} + 2^2 \cdot \frac{1}{6} + 3^2 \cdot \frac{1}{6} + 4^2 \cdot \frac{1}{6} + 5^2 \cdot \frac{1}{6} + 6^2 \cdot \frac{1}{6} = \frac{91}{6} \end{aligned}$$

X のとりうる値は $1, 2, 3, 4, 5, 6$ なので，
X^2 のとりうる値は $1^2, 2^2, 3^2, 4^2, 5^2, 6^2$ で，それぞれ確率 $1/6$ で生起する

確率変数の関数の期待値

自然数値関数 $f \colon \mathbb{N} \to \mathbb{N}$ に対して

$$\mathrm{E}[f(X)] = \sum_{i=0}^{\infty} f(i) \cdot \Pr(X = i)$$

条件つき期待値とは？

事象 A のもとでの X の条件つき期待値とは

$$\mathrm{E}[X \mid A] = \sum_{i=0}^{\infty} i \cdot \Pr(X = i \mid A)$$

例：公平なサイコロ

X = サイコロの出目，A = 偶数が出るという事象 とすると

$$\mathrm{E}[X \mid A] = 1 \cdot 0 + 2 \cdot \frac{1}{3} + 3 \cdot 0 + 4 \cdot \frac{1}{3} + 5 \cdot 0 + 6 \cdot \frac{1}{3} = 4$$

性質

全事象 Ω が A と B に分割されるとき ($\Omega = A \cup B, A \cap B = \emptyset$)
$\Pr(A) \neq 0$，$\Pr(B) \neq 0$ ならば

$$\mathrm{E}[X] = \mathrm{E}[X \mid A] \Pr(A) + \mathrm{E}[X \mid B] \Pr(B)$$

証明：

$$\begin{aligned}
\mathrm{E}[X] &= \sum_i i \cdot \Pr(X = i) \\
&= \sum_i i \cdot (\Pr(X = i \mid A) \Pr(A) + \Pr(X = i \mid B) \Pr(B)) \\
&= \left(\sum_i i \cdot \Pr(X = i \mid A) \right) \Pr(A) + \left(\sum_i i \cdot \Pr(X = i \mid B) \right) \Pr(B) \\
&= \mathrm{E}[X \mid A] \Pr(A) + \mathrm{E}[X \mid B] \Pr(B) \qquad \square
\end{aligned}$$

期待値の線形性

2 つの自然数値確率変数 X, Y と定数 c に対して

$$\mathrm{E}[X+Y] = \mathrm{E}[X] + \mathrm{E}[Y], \quad \mathrm{E}[cX] = c\mathrm{E}[X]$$

例：サイコロを 2 回振ったとき，
1 回目の出目を X，2 回目の出目を Y とすると

$$\begin{aligned}
\mathrm{E}[X+Y] &= \mathrm{E}[X] + \mathrm{E}[Y] = \frac{7}{2} + \frac{7}{2} = 7 \\
\mathrm{E}[2X] &= 2\mathrm{E}[X] = 2 \cdot \frac{7}{2} = 7 \\
\mathrm{E}[X] + \mathrm{E}[7-X] &= \mathrm{E}[X + (7-X)] = \mathrm{E}[7] = 7
\end{aligned}$$

独立確率変数の積の期待値

2 つの自然数値確率変数 X, Y が独立であるとき，

$$\mathrm{E}[XY] = \mathrm{E}[X] \cdot \mathrm{E}[Y]$$

例：サイコロを 2 回振ったとき，
1 回目の出目を X，2 回目の出目を Y とすると
X と Y は独立なので，

$$\mathrm{E}[XY] = \mathrm{E}[X] \cdot \mathrm{E}[Y] = \frac{7}{2} \cdot \frac{7}{2} = \frac{49}{4}$$

互いに独立な確率変数の積の期待値

n 個の自然数値確率変数 $X_1, X_2, \ldots, X_n$ が互いに独立であるとき，

$$\mathrm{E}\left[\prod_{i=1}^{n} X_i\right] = \prod_{i=1}^{n} \mathrm{E}[X_i]$$

例：サイコロを n 回振ったとき，i 回目の出目を X_i とする

- $X_1, \ldots, X_n$ は互いに独立　(前述)
- したがって，

$$\mathrm{E}\left[\prod_{i=1}^{n} X_i\right] = \prod_{i=1}^{n} \mathrm{E}[X_i] = \left(\frac{7}{2}\right)^n$$

目次

1. 最小包囲円を求めるアルゴリズム：乱択化
2. 確率の復習
3. 乱択アルゴリズムの解析
4. 今日のまとめ

入力：有限点集合 $P \subseteq \mathbb{R}^2$ ($|P| \geq 1$)，$R \subseteq P$

(1) $|P| \leq 2$ ならば，$\mathrm{sed}(P, R)$ を直接計算して，終了

(2) $|R| \geq 3$ ならば，$\mathrm{sed}(P, R)$ を直接計算して，終了

(3) $|P| \geq 3$ かつ $|R| \leq 2$ ならば，$p \in P - R$ を一様分布に従って選ぶ

(3-1) $\mathrm{sed}(P - \{p\}, R)$ を再帰的に計算 (存在しないならば終了)

(3-2) $\mathrm{sed}(P - \{p\}, R)$ が存在し，$p \in \mathrm{sed}(P - \{p\}, R)$ ならば，
$\mathrm{sed}(P, R) = \mathrm{sed}(P - \{p\}, R)$ として，終了

(3-3) $\mathrm{sed}(P - \{p\}, R)$ が存在し，$p \notin \mathrm{sed}(P - \{p\}, R)$ ならば，
$\mathrm{sed}(P, R \cup \{p\})$ を再帰的に計算して，
$\mathrm{sed}(P, R) = \mathrm{sed}(P, R \cup \{p\})$ として，終了

今から行うこと：乱択アルゴリズムの解析

- 記法：$t(P, R) =$ 入力を P, R としたときの計算量 (確率変数)
- 考えたい量：最悪期待計算量

$$\tilde{t}(n, k) = \max\{\mathrm{E}[t(P, R)] \mid |P| = n, |R| = k\}$$

乱択アルゴリズムの解析 (1)

- $|P| = n \geq 3$, $|R| = k \leq 2$ とする
- $\tilde{t}(n,k) = \mathrm{E}[t(P,R)]$ となるような P と R を考える
  (つまり，P と R は期待計算量を最大とする入力)
- このとき，次が成り立つ

$$
\begin{aligned}
&\mathrm{E}[t(P,R)] \\
&= \sum_{p \in P-R} \Pr(p \text{ が選ばれる}) \cdot \mathrm{E}[t(P,R) \mid p \text{ が選ばれる}] \\
&= \sum_{p \in P-R} \frac{1}{n-k} \mathrm{E}[t(P,R) \mid p \text{ が選ばれる}] \\
&= \frac{1}{n-k} \sum_{p \in P-R} \mathrm{E}[t(P,R) \mid p \text{ が選ばれる}]
\end{aligned}
$$

乱択アルゴリズムの解析 (2)

E[$t(P,R)$ | p が選ばれる]

$$
\begin{aligned}
&= O(1) + \mathrm{E}[t(P - \{p\}, R)] + \Pr(p \notin \mathrm{sed}(P - \{p\}, R)) \cdot \mathrm{E}[t(P, R \cup \{p\})] \\
&\leq O(1) + \tilde{t}(n-1, k) \qquad + \Pr(p \notin \mathrm{sed}(P - \{p\}, R)) \cdot \tilde{t}(n, k+1)
\end{aligned}
$$

目標

あとは，$\Pr(p \notin \mathrm{sed}(P - \{p\}, R))$ (の上界) が分かればよい

点集合 P ($|P| \geq 2$)，部分集合 $R \subseteq P$，$|R| \leq 2$

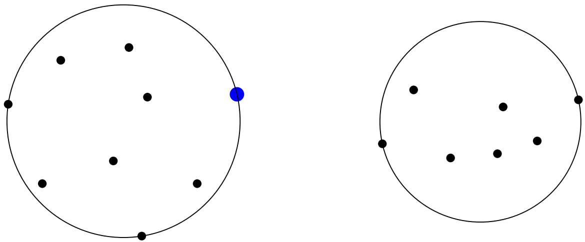
補題

$\mathrm{sed}(P,R)$ が存在するとき，ある $S \subseteq P$ が存在し，次を満たす

- $|S| \leq 3$, $R \subseteq S$
- $\mathrm{sed}(P,R) = \mathrm{sed}(S,R)$

<u>証明</u>：$\mathrm{sed}(P,R)$ の境界上にある点の集合を Q とする

- $|Q| \leq 3$ のとき，$S = Q$



点集合 P ($|P| \geq 2$)，部分集合 $R \subseteq P$，$|R| \leq 2$

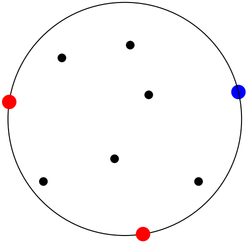
補題

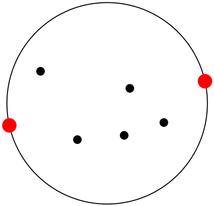
sed(P, R) が存在するとき，ある $S \subseteq P$ が存在し，次を満たす

- $|S| \leq 3$, $R \subseteq S$
- $\mathrm{sed}(P, R) = \mathrm{sed}(S, R)$

証明：sed(P, R) の境界上にある点の集合を Q とする

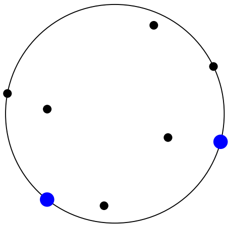
- $|Q| \leq 3$ のとき，$S = Q$





証明 (続)：sed(P, R) の境界上にある点の集合を Q とする

- $|Q| \geq 4$ のとき，$R \subseteq S$ として，$3 - |R|$ 個の点を $Q - R$ から選んで，S を作る
- どのように選ぶのか？ $\rightsquigarrow$ $P - R$ の点を微小に動かして考える

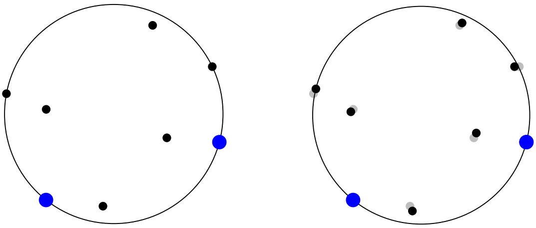


- 動かした後で sed(P, R) を考えると，その境界上には 3 点しかないので，それを S とすればよい

□

証明 (続)：sed(P, R) の境界上にある点の集合を Q とする

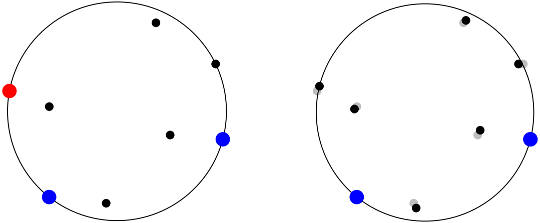
- $|Q| \geq 4$ のとき，$R \subseteq S$ として，$3 - |R|$ 個の点を $Q - R$ から選んで，S を作る
- どのように選ぶのか？ $\rightsquigarrow$ $P - R$ の点を微小に動かして考える



- 動かした後で sed(P, R) を考えると，その境界上には 3 点しかないので，それを S とすればよい □

証明 (続)：sed(P, R) の境界上にある点の集合を Q とする

- $|Q| \geq 4$ のとき，$R \subseteq S$ として，$3 - |R|$ 個の点を $Q - R$ から選んで，S を作る
- どのように選ぶのか？ $\rightsquigarrow$ $P - R$ の点を微小に動かして考える



- 動かした後で sed(P, R) を考えると，その境界上には 3 点しかないので，それを S とすればよい

□

乱択アルゴリズムの解析 (3)

目標

あとは，$\Pr(p \notin \mathrm{sed}(P - \{p\}, R))$ (の上界) が分かればよい

補題

$\mathrm{sed}(P, R)$ が存在するとき，ある $S \subseteq P$ が存在し，次を満たす

- $|S| \leq 3$, $R \subseteq S$
- $\mathrm{sed}(P, R) = \mathrm{sed}(S, R)$

$\therefore$ $\mathrm{sed}(P, R) = \mathrm{sed}(S, R)$ となる S (ただし，$|S| \leq 3, R \subseteq S$) を考えると

- $p \notin \mathrm{sed}(P - \{p\}, R)$ ならば，$p \in S - R$ となる
- すなわち，

$$\Pr(p \notin \mathrm{sed}(P - \{p\}, R)) \leq \Pr(p \in S - R) = \frac{|S - R|}{|P - R|} \leq \frac{3}{n - k}$$

$$
\begin{aligned}
&\mathrm{E}[t(P,R) \mid p \text{ が選ばれる}]\\
&= O(1) + \mathrm{E}[t(P-\{p\},R)] + \Pr(p \notin \mathrm{sed}(P-\{p\},R)) \cdot \mathrm{E}[t(P, R\cup\{p\})]\\
&\le O(1) + \tilde{t}(n-1,k) \qquad + \Pr(p \notin \mathrm{sed}(P-\{p\},R)) \cdot \tilde{t}(n,k+1)\\
&\le O(1) + \tilde{t}(n-1,k) \qquad + \frac{3}{n-k} \cdot \tilde{t}(n,k+1)
\end{aligned}
$$

$$
\begin{aligned}
&\therefore \tilde{t}(n,k)\\
&\le \frac{1}{n-k} \sum_{p\in P-R} \mathrm{E}[t(P,R) \mid p \text{ が選ばれる}]\\
&\le O(1) + \tilde{t}(n-1,k) + \frac{3}{n-k} \cdot \tilde{t}(n,k+1)
\end{aligned}
$$

これで，漸化式が得られた

乱択アルゴリズムの解析 (5)：ここまでのまとめ

最悪期待計算量を $\tilde{t}(n,k)$ とすると

$$\tilde{t}(n,k) \le \begin{cases} O(1) & (n \le 2 \text{ のとき}) \\ O(n) & (k \ge 3 \text{ のとき}) \\ O(1) + \tilde{t}(n-1,k) + \dfrac{3}{n-k} \cdot \tilde{t}(n,k+1) & (\text{その他のとき}) \end{cases}$$

あとは，これを解けばよい

$n \geq 3$ かつ $k = 2$ のとき，

$$\begin{aligned}
\tilde{t}(n,2) &\leq O(1) + \tilde{t}(n-1,2) + \frac{3}{n-2} \cdot \tilde{t}(n,3) \\
&\leq O(1) + \tilde{t}(n-1,2) + \frac{3}{n-2} \cdot O(n) \\
&\leq O(1) + \tilde{t}(n-1,2) + O(1) \\
&\leq \tilde{t}(n-1,2) + O(1)
\end{aligned}$$

したがって，$t(n,2) \leq O(n)$

乱択アルゴリズムの解析 (7)：漸化式

$n \geq 3$ かつ $k = 1$ のとき，

$$
\begin{aligned}
\tilde{t}(n,1) &\leq O(1) + \tilde{t}(n-1,1) + \frac{3}{n-1} \cdot \tilde{t}(n,2) \\
&\leq O(1) + \tilde{t}(n-1,1) + \frac{3}{n-1} \cdot O(n) \\
&\leq O(1) + \tilde{t}(n-1,1) + O(1) \\
&\leq \tilde{t}(n-1,1) + O(1)
\end{aligned}
$$

したがって，$t(n,1) \leq O(n)$

$n \geq 3$ かつ $k = 0$ のとき，

$$\begin{aligned}\tilde{t}(n,1) &\leq O(1) + \tilde{t}(n-1,0) + \frac{3}{n}\cdot\tilde{t}(n,1)\\ &\leq O(1) + \tilde{t}(n-1,0) + \frac{3}{n}\cdot O(n)\\ &\leq O(1) + \tilde{t}(n-1,0) + O(1)\\ &\leq \tilde{t}(n-1,0) + O(1)\end{aligned}$$

したがって，$t(n,0) \leq O(n)$

結論

平面上に与えられた n 個の点の最小包囲円を計算する問題には
最悪期待計算量が $O(n)$ であるアルゴリズムが存在する

目次

1. 最小包囲円を求めるアルゴリズム：乱択化
2. 確率の復習
3. 乱択アルゴリズムの解析
4. 今日のまとめ

最小包囲円問題に対する乱択アルゴリズム

- 最小包囲円アルゴリズムの復習
- 最小包囲円アルゴリズムの乱択化
- 乱択アルゴリズムの解析

この内容は次の論文に基づく

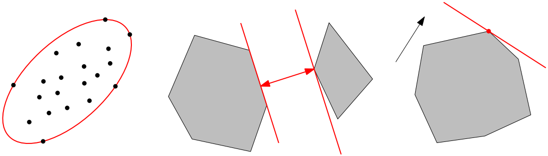
- E. Welzl. Smallest enclosing disks (balls and ellipsoids). In: H. Maurer (ed), *New Results and New Trends in Computer Science*, Lecture Notes in Computer Science **555** (1991) pp. 359–370.

https://www.inf.ethz.ch/personal/emo/EmoPortrait.JPG

「最小包囲円問題」は「LP 型問題 (LP-type problem)」の特別な場合

LP 型問題としてモデル化できる問題

- 最小包囲楕円問題
- 交わらない 2 つの凸多角形間の距離の計算
- 線形計画問題
- ……



原論文は次のもの (Wikipedia にも解説あり)

- Jiří Matoušek, Micha Sharir, Emo Welzl. A subexponential bound for linear programming, Algorithmica **16** (1996) 498–516.

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

1. 最小包囲円を求めるアルゴリズム：乱択化
2. 確率の復習
3. 乱択アルゴリズムの解析
4. 今日のまとめ