1 Algorithm

1.1 $\mathcal{O}$ notation

与えられた関数 $g(n)$ に対して、$\mathcal{O}(g(n))$ によって関数の集合

$$\mathcal{O}(g(n)) = \{f(n) : \text{ある正の定数 } c, n_0 \text{が存在して、すべての } n \geq n_0 \text{に対して } 0 \leq f(n) \leq cg(n) \text{ を満たす } \}$$

を表現する。

入力が一定数以下はオーバーヘッドがあったりで、ノイズなので入力が一定数以上を表現するために n_0 を設けている。

2 整数

2.1 ユークリッド互除法

2 つの整数 a,b が与えられたとき、a,b の最大公約数が知りたい.a,b を以下のように表現したとき、a と b の公約数の集合は a と r の公約数の集合と等しくなる。

$$b = qa + r \ (0 <= r < a)$$

証明 $d|a \wedge d|b \equiv d|a \wedge d|r$ を証明する。

戦略として、 $(d|a \wedge d|b \rightarrow d|a \wedge d|r) \wedge (d|a \wedge d|r \rightarrow d|a \wedge d|b)$ を証明する。

$d|a \wedge d|b \rightarrow d|a \wedge d|r$ の証明

仮定より、$\exists q_a, q_b(a = q_a d, b = q_b d)$

$$\begin{aligned} b &= aq + r \\ q_b d &= (q_a d)q + r \qquad (\text{仮定から a と b を置換}) \\ r &= q_b d - q q_a d \\ r &= d(q_b - q q_a) \end{aligned}$$

ここで、 q_b, q_a, q は整数であり、整数の掛け算、引き算は整数に閉じるので $(q_b - q q_a)$ は整数したがって、$\exists n(r = dn)$ がいえるので、$d|r$ がいえる。よって、$d|a \wedge d|b \rightarrow d|a \wedge d|r$

3 統計

3.1 条件つき確率

2 つの事象 A,B に対し、A が起こった状況のもとで B が起こる条件つき確率といい、以下のように表す

$$P(B|A) = \frac{P(A \cap B)}{P(A)}$$

考え方としては、$P(B|A)$ を given として与えられている事象 A の個数と事象 A かつ B の個数と捉えて以下のように導く

$$
\begin{aligned}
P(B|A) &= \frac{n(A \cap B)}{n(A)} \\
&= \frac{\frac{n(A \cap B)}{n(U)}}{\frac{n(A)}{n(U)}} \qquad (\text{分子, 分母を n(U) で割る}) \\
&= \frac{P(A \cap B)}{P(A)}
\end{aligned}
$$

条件付き確率を以下の形にしたものを乗法定理という。

$$P(A \cap B) = P(B|A) \cdot P(A)$$

3.2 ベイズの定理

$$
\begin{aligned}
P(X \cap Y) &= \frac{n(X \cap Y)}{n(U)} \\
&= \frac{n(X \cap Y)}{1} \cdot \frac{1}{n(U)} \\
&= \frac{n(X \cap Y)}{n(X)} \cdot \frac{n(X)}{n(U)} \\
&= P(Y|X) \cdot P(X) \\
&\text{同様に} \\
P(X \cap Y) &= \frac{n(X \cap Y)}{n(U)} \\
&= \frac{n(X \cap Y)}{1} \cdot \frac{1}{n(U)} \\
&= \frac{n(X \cap Y)}{n(Y)} \cdot \frac{n(Y)}{n(U)} \\
&= P(X|Y) \cdot P(Y) \\
&\text{従って} \\
P(Y|X)P(X) &= P(X|Y)P(Y) \\
\underbrace{P(X|Y)}_{\text{事後確率}} &= \underbrace{P(X)}_{\text{事前確率}} \cdot \underbrace{\frac{P(Y|X)}{P(Y)}}_{\text{修正項}}
\end{aligned}
$$