

* متغیر احتمال کل و قاعده بیر

• مثال

* نکاتی درباره احتمال شرطی

* وقایع مستقل

• مثال رمزنگاری یک‌بار مصرف one-time pad

* وقایع دوبه دو مستقل و وقایع مشترک مستقل

* متغیر احتمال کل و قاعده بیر (Total prob. thm. & Bayes' thm.) :

• قاعده احتمال کل: معرفی کنید $A_1, \dots, A_n$ یک اقرار از منضای نمونه باشند و

$A_i \in \mathcal{F}$, $B \in \mathcal{F}$ یک واقعه دلخواه باشد. آنگاه می‌توانیم بنویسیم:

$$P(B) = P[B \cap \Omega] = P[B \cap \underbrace{(A_1 \cup \dots \cup A_n)}_{=\Omega}]$$

$$= P[(B \cap A_1) \cup \dots \cup (B \cap A_n)]$$

$$= P[(B \cap A_1)] + \dots + P[(B \cap A_n)]$$

$$= P[B|A_1] \cdot P[A_1] + \dots + P[B|A_n] \cdot P[A_n]$$

(قاعده احتمال)

• قاعده بیز: ممکن است محاسب مستقیم $P[A|B]$ سخت باشد ولی به راحتی

(عملیات) محاسب $P[B|A]$ و $P[B|A^c]$ راحت تر باشد.

تغییر بیز بیان می کند:

$$P[A|B] = \frac{P[A \cap B]}{P[B]}$$

استفاده از قاعده
امثال

$$= \frac{P[B|A] \cdot P[A]}{P[B|A] \cdot P[A] + P[B|A^c] \cdot P[A^c]}$$

75-8815 • قاعده بیس در حالت کلی تر یا فرض آیند $A_1, \dots, A_n$ یک احتمال زیرای منفی متناهی باشند :

$$P[A_1 | B] = \frac{P[B | A_1] \cdot P[A_1]}{\sum_{i=1}^n P[B | A_i] \cdot P[A_i]}$$

• نکته: در هر دو قضیه اگر $A_1, A_2, \dots$ نامتناهی مجموعه هم باشند روابط بالا برقرار است.

مثال: فرض کنید دو جعبه داریم.

جعبه اول: a توپ سفید و b توپ سیاه

جعبه دوم: c توپ سفید و d توپ سیاه

یک توپ به صورت کاملاً اتفاقی از جعبه اول بری داریم و داخل جعبه دوم می‌اندازیم.
بعد از جعبه دوم یک توپ بری داریم.

امثال اینکه توپ دوم سفید باشد چقدر است؟

• حل: دوامقه سقریف و کین بر صب رنگد توب لول:

$$B = \{ \text{توب اول سیاه} \}, \quad W = \{ \text{توب اول سفید} \}$$

$$A = \{ \text{توب دوم سفید} \} \quad \text{واقعه مورد نظر؛}$$

$$P[A] = P[A|B] \cdot P[B] + P[A|W] \cdot P[W]$$

$$= \frac{c}{c+d+1} \cdot \frac{b}{a+b} + \frac{c+1}{c+d+1} \cdot \frac{a}{a+b}$$

$$= \frac{bc + ac + a}{(c+d+1)(a+b)}$$

* نکته‌ی درباره اقبال شرطی

در ادامه به بررسی حالات ممکن در اقبال شرطی $P[B|A]$ نسبت به $P[B]$ می پردازیم:

$$P[B|A]$$

$$P[B|A] = \frac{P[A \cap B]}{P[A]} = P[B] \quad \text{اگر } \leftarrow \text{ دو واقعه } A, B \text{ از هم}$$

مستقل هستند و یکنویس:

$$A \perp B$$

$$\Leftrightarrow P[A|B] = P[A] \quad \checkmark$$

$$P[B|A] > P[B] \quad \text{اگر } \leftarrow \text{ دو واقعه همبستگی را تقویت و کنند}$$

$$P[A|B] > P[A] \quad \Leftrightarrow$$

$$P[B|A] < P[B] \quad \text{اگر } \leftarrow \text{ دو واقعه همبستگی را تضعیف می کنند}$$

$$P[A|B] < P[A] \quad \Leftrightarrow$$

* عرض کنید که $P[B|A] = 1$ یعنی اگر A واقع شود حتما B واقع شده است.

به زبان ساده تر، اگر A رخ دهد، B حتما رخ می دهد.

به زبان ساده‌تر: $A \Rightarrow B$

فرض کنیم $P(B) \neq 1$. در نتیجه داریم:

$$P(B|A) > P(B)$$

(یعنی واقعه A ، واقعه B را تقویت می‌کند)

$$\Rightarrow P(A|B) > P(A)$$

این همان حقیقتی است که علیه ادلی زدیم. یعنی اگر $A \Rightarrow B$ لزوماً معنی‌شده گفت $B \Rightarrow A$ ولی می‌شد نتیجه گرفت داشت B احتمال وقوع A را افزایش می‌دهد.

مثال: داریم: $P(\text{ایه‌ی } A) > P(\text{ایه‌ی } A) = 1$

$$\Rightarrow P(\text{ایه‌ی } A | \text{ایه‌ی } A) > P(\text{ایه‌ی } A)$$

* نتیجه: اگر A و B یکدیگر را تقویت کنند $\Leftrightarrow$

① A, B^c همدیگه را تقویت می کنند.

② A, B^c همدیگه را تقویت می کنند.

* سوال: اگر دو واقعه همدیگه را تقویت می کنند آیا حتماً بین آنها رابطه علت و معلولی وجود دارد (یعنی مثلاً یکی علت دیگری باشد)؟

پاسخ: نه لزوماً

مثال: بیماری ریوی دگیاری ۲۰۰۰ (یکی علت دیگری است)

مثال: میزان تبخیر آب و ارتقاء دما کتب (هیچ کدام علت دیگری نیستند).

* مثال: فرض کنید B واقعه A را تقویت می کند و C هم واقعه A را تقویت می کند.

آیا $B \cap C$ هم A را تقویت می کند؟ پاسخ: نه لزوماً

• مثال نفی: (آزمایشی مقارنی با مقارن بین امضا) $\{1, 2, \dots, 10\} = \{1, 2, \dots, 10\}$

$$A = \{1, 2, 5, 6\}, \quad B = \{1, 2, 3\}, \quad C = \{3, 5, 6\}$$

$$P[A] = \frac{4}{10}, \quad P[A|B] = \frac{2}{3}, \quad P[A|C] = \frac{2}{3}$$

$$P[A|B \cap C] = P[\{1, 2, 5, 6\} | \{3\}] = 0 \quad \checkmark$$

* نتایج مستقل:

• در اینجا دو رویداد A و B مستقل هستند اگر که:

$$P[A \cap B] = P[A] \cdot P[B]$$

• در اینجا $P[A \cap B] = P[A] \cdot P[B]$

$$P[B] \neq 0 \quad \Leftrightarrow \quad P[A|B] = P[A]$$

$$P[A] \neq 0 \quad \Leftrightarrow \quad P[B|A] = P[B]$$

• اگر که A و B مستقل باشند و گوییم وابسته هستند.

independent

• نتیجه: اگر $A \perp B$ نشان دهیم: $A \perp B$ و $A \perp B$
(کتاب پاپولس ۰.۳۵)

• سوال: اگر $A \perp B$ و $A \perp C$ آیا می توان نتیجه گرفت که: $A \perp (B \cap C)$
پاسخ:

برای بررسی این سوال مثال زیر را در نظر بگیرید.

* مثال: فرض کنید دو کله X و Y داریم (برای راحتی با ۰ و ۱ نمایشی دهیم) که به طور مستقل به تاب سته اند.

$X: \begin{cases} 0 & : \text{ با احتمال } P \\ 1 & : \text{ با احتمال } 1-P \end{cases}$

$Y: \begin{cases} 0 & : \frac{1}{2} \text{ احتمال} \\ 1 & : \frac{1}{2} \text{ احتمال} \end{cases}$

مضامین متوجه به تاب سته اند. دو کله:

مغای متواتر تا ب لغتزمان دو کله:

$$\Omega = \left\{ \overset{x}{\downarrow} \overset{y}{\downarrow} (0,0), (0,1), (1,0), (1,1) \right\}$$

تقریب
آزمایش
مقایسه

← تا ب دو کله مستقل

$$P[\{(0,0)\}] = \frac{P}{2}, \quad P[\{(0,1)\}] = \frac{P}{2}$$

$$P[\{(1,0)\}] = \frac{1-P}{2}, \quad P[\{(1,1)\}] = \frac{1-P}{2}$$

• و نتایج زیر را در محاسبه می:

$$P[A_0] = P \quad \leftarrow \quad A_0 = \{(0,0), (0,1)\} \quad \leftarrow \quad \text{واقعه } X=0$$

$$P[A_1] = 1-P \quad \leftarrow \quad A_1 = \{(1,0), (1,1)\} \quad \leftarrow \quad \text{واقعه } X=1$$

$$P[B_0] = \frac{1}{2} \quad \leftarrow \quad B_0 = \{(0,0), (1,0)\} \quad \leftarrow \quad \text{واقعه } Y=0$$

$$P(B_1) = \frac{1}{2} \leftarrow B_1 = \{(0,1), (1,1)\} \leftarrow Y=1 \text{ واقع}$$

$$P(C_0) = \frac{1}{2} \leftarrow C_0 = \{(0,0), (1,1)\} \leftarrow Z = X \oplus Y = 0 \text{ واقع}$$

$$P(C_1) = \frac{1}{2} \leftarrow C_1 = \{(0,1), (1,0)\} \leftarrow Z = X \oplus Y = 1 \text{ واقع}$$

• دست‌گیر داریم:

$$P(A_0 \cap B_0) = \frac{P}{2} = P(A_0) \cdot P(B_0) \Rightarrow A_0 \perp B_0$$

به طور مشابه: $A_0 \perp C_0$

$$A_0 \perp B_1, \quad A_1 \perp B_0, \quad A_1 \perp B_1 \quad \text{و همچنین:}$$

$$A_0 \perp C_1, \quad A_1 \perp C_0, \quad A_1 \perp C_1 \quad \text{و همچنین:}$$

• حالی خواهم بررسی کنیم

$$\text{If } A_0 \perp B_0 \text{ و } A_0 \perp C_0 \stackrel{?}{\Rightarrow} A_0 \perp (B_0 \cap C_0)$$

$$P[A_0 \cap (B_0 \cap C_0)] = \underbrace{P[\{(0,0)\}]}_{= \frac{P}{2}} \neq \underbrace{P[A_0]}_{= P} \cdot \underbrace{P[B_0 \cap C_0]}_{= \frac{P}{2}}$$

در نتیجه پاسخ سوال بالا منفی است.

• کاربرد مثال بالا در رمزنگاری :

فرض کنید اکرم می خواهد یک بیت (مثلا x) پیامی بیکد بفرستد.

یک نفر کاتال را استراق سمع می کند. این دو نفر چه می توانند بکنند؟

با توجه به صرف های بالا به روشن زیر عمل کنیم.

قبل از ارسال فرضی کنید اکرم و یاکد یک مسکه مشترک برناب کرده باشند و از یک طریق

مطلوبی با هر دو اکتز آن گذاکنند یا کنند (y).



(one-time pad encryption)

از طرف های با لایه یکم که: $A_0 \ll C_0$ و $A_1 \ll C_1$ و $A_0 \ll C_1$ و $A_1 \ll C_0$

یعنی آدم به جینی با مشاهده بیت Z هیچ اطلاعاتی در مورد بیت اکرم نیست
نمی آورد.

از طرف ریزر $A_0 \ll (B_0 \wedge C_0)$ و $A_0 \ll (B_0 \wedge C_1)$ و ...

یاکب یک حرف های در مورد X می تواند با دانستن همدان Y و Z بیزند.

در واقع یاکب با محاسبه $Y \oplus Z$ می تواند اطلاعات کامل در مورد X را

$$= Y \oplus (X \oplus Y) = X$$

• آخرین: نشان دهید که لا متقارن باشد داریم $A \neq C$.

و در این صورت ۲ در بدجی و نشانده املائی در مورد X بدست بیاورد.

$$\Omega_1 = \left\{ \underbrace{(\downarrow, \downarrow)}_{\gamma_4}, \underbrace{(\downarrow, \downarrow)}_{\gamma_4}, \underbrace{(\downarrow, \downarrow)}_{\gamma_4}, \underbrace{(\downarrow, \downarrow)}_{\gamma_4} \right\}$$

کوچک بزرگ

$$\Omega_2 = \left\{ \underbrace{(\downarrow, \downarrow)}_{\gamma_4}, \underbrace{(\downarrow, \downarrow)}_{\gamma_4}, \underbrace{(\downarrow, \downarrow)}_{\gamma_2} \right\}$$

$$P \left[\begin{array}{c} \text{کسی که در خانه} \\ \text{بهر} \end{array} \mid \begin{array}{c} \text{کسی که در راباز کرده} \\ \text{بهر} \end{array} \right] \rightarrow \begin{array}{l} \Omega_1 \rightarrow \left\{ \underbrace{(\downarrow, \downarrow)}_{\gamma_4}, \underbrace{(\downarrow, \downarrow)}_{\gamma_4}, \underbrace{(\downarrow, \downarrow)}_{\gamma_4} \right\} \\ \Omega_2 \rightarrow \left\{ \underbrace{(\downarrow, \downarrow)}_{\gamma_4}, \underbrace{(\downarrow, \downarrow)}_{\gamma_2} \right\} \end{array}$$

$$P[\text{خوشنبردگ: پسر}] = P[\text{پسر} = \text{خوشنبردگ}] = \frac{1}{2}$$

$$\rightarrow \mathcal{I}_1 = \left\{ \frac{P[(\text{پ}, \text{پ})]}{P[\text{کسی که در راه زنده که است: پسر}]} = \frac{1/4}{3/4} = \frac{1}{3} \right.$$

$$\rightarrow \mathcal{I}_2 = \left\{ \frac{P[(\text{پ}, \text{پ})]}{P[\underbrace{(\text{پ}, \text{پ})}_{1/4}, \underbrace{(\text{پ}, \text{د})}_{1/2}]} = \frac{1/4}{3/4} = \frac{1}{3} \right.$$