Lecture 01: Mathematical Basics

Bayes Rule

- For events A and B, Bayes' Rule states

$$\Pr[A, B] = \Pr[A] \cdot \Pr[B|A]$$

  - English: Probability of events A and B is equal to the probability of event A multiplied by the probability of event B conditioned on event A

- More generally,

$$\Pr[A, B|Z] = \Pr[A|Z] \cdot \Pr[B|A, Z]$$

  - Think: English Version of this identity
  - Think: Proof of this statement using Bayes' Rule

Chain Rule

- Chain Rule states

$$\Pr[A_1, \ldots, A_n] = \prod_{i=1}^{n} \Pr[A_i | A_1, \ldots, A_{i-1}]$$

  - Think: Prove this using the generalized Chain Rule and induction
- In general

$$\Pr[A_1, \ldots, A_n | Z] = \prod_{i=1}^{n} \Pr[A_i | A_1, \ldots, A_{i-1}, Z]$$

Union Bound

- By Inclusion-Exclusion Principle we have

$$\Pr[A \vee B] = \Pr[A] + \Pr[B] - \Pr[A \wedge B]$$

- Union-bound can be deduced from above

$$\Pr[A \vee B] \leqslant \Pr[A] + \Pr[B]$$

- In general

$$\Pr[\bigvee_{i=1}^{t} A_i] \leqslant \sum_{i=1}^{t} \Pr[A_i]$$

  - Think: Prove using induction
  - Think: Tightness of the inequality

AM-GM-HM Inequality

- AM-GM inequality states: For $a, b \geqslant 0$

$$\frac{a+b}{2} \geqslant \sqrt{ab}$$

- Equality hold if and only if $a = b$
  - Think: Proof?
- GM-HM inequality states: For $a, b \geqslant 0$

$$\sqrt{ab} \geqslant \left(\frac{\frac{1}{a} + \frac{1}{b}}{2} \right)^{-1}$$

  - Think: Using AM-GM prove GM-HM

AM-GM Generalization

- AM-GM directly gives the following inequality

$$\frac{\sum_{i=1}^{n} a_i}{n} \geqslant \left(\prod_{i=1}^{n} a_i\right)^{1/n}$$

  - Think: Use AM-GM and induction to prove this
  - Think: Tightness characterization

- More generally, for $\alpha_i \in \mathbb{Q}$ such that $\alpha_i \geqslant 0$, for all $i \in [n]$, and $\sum_{i=1}^{n} \alpha_i = 1$ we have: For $a_i \geqslant 0$, for all $i \in [n]$, we have

$$\sum_{i=1}^{n} \alpha_i a_i \geqslant \prod_{i=1}^{n} a_i^{\alpha_i}$$

  - Think: Proof (Hint: Multiply with GCD of denominator)
  - Think: Tightness

AM-GM Generalization

- For $\alpha_i \in \mathbb{R}$ such that $\alpha_i \geqslant 0$, for all $i \in [n]$, and $\sum_{i=1}^{n} \alpha_i = 1$ we have: For $a_i \geqslant 0$, for all $i \in [n]$, we have

$$\sum_{i=1}^{n} \alpha_i a_i \geqslant \prod_{i=1}^{n} a_i^{\alpha_i}$$

  - Think: Proof

Cauchy-Schwarz Inequality

- Cauchy-Schwarz states: For positive a_is and b_is we have

$$\sum_{i=1}^{n} a_i b_i \leqslant \left(\sum_{i=1}^{n} a_i^2\right)^{1/2} \cdot \left(\sum_{i=1}^{n} b_i^2\right)^{1/2}$$

- Equality holds if and only if a_i/b_i is identical for all $i \in [n]$.
- Intuition: Dot product of two vectors is at most the product of their lengths, and equality holds if and only if the vectors are parallel or anti-parallel
- Think: Proof
- Read: Hölder's Inequality

Jensen's Inequality

- Let f be "convex upwards"
- Then, for $\alpha \in [0, 1]$, Jensen's Inequality states

$$f(\alpha a + (1-\alpha)b) \leqslant \alpha f(a) + (1-\alpha)f(b)$$

- Intuition: Chord is above the function-curve
- In general for $\alpha_i \geqslant 0$ such that $\sum_{i=1}^{n} \alpha_i = 1$, we have:

$$f\left(\sum_{i=1}^{n} \alpha_i a_i\right) \leqslant \sum_{i=1}^{n} \alpha_i f(a_i)$$

- Convex upward functions: $f(x) = x^{1+\varepsilon}$ (for positive x), $f(x) = x \ln x$ (for positive x), $f(x) = \exp(x)$, $f(x) = \exp(-x)$
- Think: Deduce previous inequalities using Jensen's Inequality on appropriate functions

Useful Inequalities

- There exists a constant $c \in (0,1)$ such that the following holds ($c = 1/2$ suffices): For $x \in [0,c]$ we have

$$\exp(-x - x^2) \leqslant (1-x) \leqslant \exp(-x) \leqslant 1 - x + x^2$$

- Think: Prove $(1-x) \leqslant \exp(-x)$ using the "tangent is below the curve" intuition

Birthday Paradox

- Let $U = \{1, \ldots, n\}$ be the universe
- We draw k independent samples uniformly at random from the universe
- In particular, for the birthday problem we have $n = 365$
- Suppose we draw k samples $s_1, \ldots, s_k$
- Let Coll_k be the event that there exists i, j such that $i < j \leqslant k$ and the $s_i = s_j$

Birthday Paradox

- We have the following:

$$\Pr[\neg \mathsf{Coll}_k] = 1 \cdot \left(1 - \frac{1}{n}\right)\left(1 - \frac{2}{n}\right) \cdots \left(1 - \frac{k-1}{n}\right)$$
$$= \prod_{i=1}^{k-1} \left(1 - \frac{i}{n}\right)$$

Lower Bound

$$
\begin{aligned}
\Pr[\neg \mathsf{Coll}_k] &\geqslant \prod_{i=1}^{k-1} \exp\left(-\frac{i}{n} - \frac{i^2}{n^2}\right) \\
&= \exp\left(-\frac{\sum_{i=1}^{k} i}{n} - \frac{\sum_{i=1}^{k} i^2}{n^2}\right) \\
&= \exp\left(-\frac{(k-1)k}{n} - \frac{(k-1)(k-1/2)k}{n^2}\right) \\
&= \exp\left(-\frac{k^2}{n} + O(1/\sqrt{n})\right), \qquad \text{for } k = O(\sqrt{n}) \\
&\geqslant 1 - \frac{k^2}{n} + O(1/\sqrt{n})
\end{aligned}
$$

- Think: Choose $k = \alpha\sqrt{n}$ and compute the lower bound
- Think: If we want to avoid collisions with probability 0.99, what will be a good choice of k?

Upper Bound

$$
\begin{aligned}
\Pr[\neg \mathsf{Coll}_k] &\leqslant \prod_{i=1}^{k-1} \exp\left(-\frac{i}{n}\right) \\
&= \exp\left(-\frac{\sum_{i=1}^{k} i}{n}\right) \\
&= \exp\left(-\frac{(k-1)k}{n}\right) \\
&= \exp\left(-\frac{k^2}{n} + O(1/\sqrt{n})\right), \qquad \text{for } k = O(\sqrt{n}) \\
&\leqslant 1 - \frac{k^2}{n} + \frac{k^4}{n^2} + O(1/\sqrt{n})
\end{aligned}
$$

- Think: Choose $k = \alpha\sqrt{n}$ and compute the upper bound
- Think: What will be a good choice of k such that collisions happen with probability 0.99?

Thinking Exercise

- A new way to compute $\Pr[\neg \mathsf{Coll}_k]$
- Let NoColl_t be the event that the sample s_t is distinct from all samples $(s_1, \dots, s_{t-1})$
- Note that $\neg \mathsf{Coll}_k = \mathsf{NoColl}_1 \wedge \mathsf{NoColl}_2 \wedge \cdots \wedge \mathsf{NoColl}_k$
- Think: Compute $\Pr[\mathsf{NoColl}_t \mid \mathsf{NoColl}_1, \dots, \mathsf{NoColl}_{t-1}]$
- Think: Apply Chain Rule to evaluate $\Pr[\neg \mathsf{Coll}_k]$