Discrete Mathematics and Probability Theory

Daniel Deng

1 Basic Facts

$$(P \implies Q) \equiv (\neg P \vee Q)$$
$$\mathbb{Q} \equiv \{\tfrac{a}{b} \mid a, b \in \mathbb{Z}\}$$
$$(|S| = k) \implies (|\mathcal{P}(S)| = 2^k)$$
$$(S \subseteq \mathbb{N}) \wedge (S \neq \emptyset) \implies \exists \min(S)$$

2 Stable Matching

Definition 2.1 (Stable Matching)**.** Stable Matching is job optimal and candidate pessimal.

3 Graphs

4 Modular Arithmetic

Definition 4.1 (Greatest Common Divisor)**.** $(\exists a, b)\,(\gcd(x, y) = ax + by)$

Definition 4.2 (Galois Field)**.** $(\forall \text{ prime n})\,(\text{GF(n)} := \text{mod n space})$

Definition 4.3 (Chinese Remainder Theorem)**.**

5 Discrete Probability

Definition 5.1 (Discrete Probability Space)**.** For any discrete probability space Ω

- $(\forall \omega \in \Omega)\,(0 \leq \mathbb{P}(\omega) \leq 1)$;
- $\sum_{\omega \in \Omega} \mathbb{P}(\omega) = 1$.

Definition 5.2 (Event)**.** For all events $A \in \Omega$,

$$\mathbb{P}(A) = \sum_{\omega \in A} \mathbb{P}(\omega) = \frac{|A|}{|\Omega|}$$

5.1 Conditional Probability

Definition 5.3 (Conditional Probability)**.**

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

Definition 5.4 (Total Probability Rule)**.** Let $A_1, \ldots, A_n$ be partitions of Ω. Then

$$\mathbb{P}(B) = \sum_{i=1}^{n} \mathbb{P}(B \cap A_i) = \sum_{i=1}^{n} \mathbb{P}(B|A_i)\mathbb{P}(A_i)$$

Remark. If events A and B are positively correlated, $\mathbb{P}(A|B) > \mathbb{P}(A)$. If they are negatively correlated, $\mathbb{P}(A|B) < \mathbb{P}(A)$.

Definition 5.5 (Maximum Likelihood Estimation)**.**

$$\theta_{MLE} = \operatorname*{argmax}_{\theta} \mathbb{P}(X|\theta)$$

Definition 5.6 (Maximum A Posteriori Estimation)**.**

$$\theta_{MAP} = \operatorname*{argmax}_{\theta} \mathbb{P}(\theta|X) = \operatorname*{argmax}_{\theta} \frac{\mathbb{P}(X|\theta)\mathbb{P}(\theta)}{\mathbb{P}(X)} = \operatorname*{argmax}_{\theta} \mathbb{P}(X|\theta)\mathbb{P}(\theta)$$

Remark. If the probability space Ω is uniform, then $\theta_{MLE} = \theta_{MAP}$.

Definition 5.7 (Mutual Independence)**.**

$$\mathbb{P}\left(\bigcap_{i=1}^{n} A_i\right) = \prod_{i=1}^{n} \mathbb{P}(A_i)$$

Remark. Events A and B are independent *iff* $\mathbb{P}(A|B) = \mathbb{P}(A)$.

5.2 Product Rule

Definition 5.8 (Product Rule)**.**

$$\mathbb{P}\left(\bigcap_{i=1}^{n} A_i\right) = \prod_{i=1}^{n} \mathbb{P}\left(A_i | \bigcap_{j<i} A_j\right)$$

5.3 Inclusion-Exclusion Principle

Definition 5.9 (Inclusion-Exclusion Principle)**.**