양자계산복잡도이론 학습일지

김태원

최초 작성 : 2023년 8월 27일
최근 편집 : 2023년 8월 27일

차 례

차 례 **2**

제 1 장 계산 **3**

1.1 대각화 3

제 2 장 튜링 **6**

제 1 장

계산

1.1 대각화

함수 f가 정의역$_{\text{domain}}$ Δ상의 원소를 공역$_{\text{codomain}}$ Γ상의 원소로 사상$_{\text{maps to}}$한다는 말을 아래처럼 표기한다.

$$f : \Delta \to \Gamma.$$

f의 치역$_{\text{range}}$은 아래와 같다.

$$\{f(x) \in \Gamma | x \in \Delta\}.$$

f의 치역이 공역 Γ와 같다면 f는 전사$_{\text{surjective}}$다. 그리고 Δ상의 상이한 원소를 Γ상의 상이한 원소로 사상하는 f는 단사$_{\text{injective}}$다. f가 전사이고 단사라면 전단사$_{\text{bijcetive}}$다.

성질$_{\text{property}}$ P의 특성함수$_{\textit{characteristic function}}$ $c_P : \mathbb{N} \to \{0, 1\}$로 $n = P \Rightarrow c_p(n) = 0$을 만족한다. 이때 성질 P는 수를 두 집합으로 분할$_{\text{partition}}$한다.

집합 Σ가 열거가능$_{\textit{enumerable}}$ 혹은 가산이라는 필요충분조건$_{\text{iff}}$은 Σ가 공집합이거나 전사 함수 $f : \mathbb{N} \to \Sigma$가 존재한다는 것이다.

정리 1.1. 자연수 순서쌍 $\langle i, j\rangle$의 집합은 가산이다.

Proof. 순서쌍을 그림 1.1과 같이 지그재그 꼴의 대각선으로 배열한다. 그리고

$$\begin{array}{lllll}
0 \mapsto \langle 0,0\rangle & 1 \mapsto \langle 0,1\rangle & 3 \mapsto \langle 0,2\rangle & 6 \mapsto \langle 0,3\rangle & \\
 & 2 \mapsto \langle 1,0\rangle & 4 \mapsto \langle 1,1\rangle & 7 \mapsto \langle 1,2\rangle & \dots \\
 & & 5 \mapsto \langle 2,0\rangle & 8 \mapsto \langle 2,1\rangle & \\
 & & & 9 \mapsto \langle 3,0\rangle &
\end{array}$$

와 같이 전단사 $f : \mathbb{N} \to \mathbb{N}^2$를 정의할 수 있다. □

$$
\begin{array}{ccccccccc}
\langle 0,0\rangle & \rightarrow & \langle 0,1\rangle & & \langle 0,2\rangle & & \langle 0,3\rangle & \cdots & \\
& \swarrow & & \swarrow & & \swarrow & & \swarrow & \\
\langle 1,0\rangle & & \langle 1,1\rangle & & \langle 1,2\rangle & & \langle 1,3\rangle & \cdots & \\
& \swarrow & & \swarrow & & \swarrow & & & \\
\langle 2,0\rangle & & \langle 2,1\rangle & & \langle 2,2\rangle & & \langle 2,3\rangle & \cdots & \\
& \swarrow & & \swarrow & & & & & \\
\langle 3,0\rangle & & \langle 3,1\rangle & & \langle 3,2\rangle & & \langle 3,3\rangle & \cdots & \\
\vdots & \swarrow & \vdots & & \vdots & & \vdots & &
\end{array}
$$

그림 1.1: 대각 논법

정리 1.2 (칸토어 정리(1874))**.** 가산이 아닌 무한집합이 존재한다.

Proof. $\mathbb{N}$의 멱집합 $\mathcal{P}$가 아래처럼 존재한다.

$$X \in \mathcal{P} \iff X \subseteq \mathbb{N}.$$

역으로 함수 $f : \mathbb{N} \to \mathcal{P}$가 존재하여 $\mathcal{P}$가 가산이라고 하자. 우선 $\mathbb{N}$의 부분집합 D를 아래처럼 둔다.

$$D = \{n \in \mathbb{N} : n \notin f(n)\}.$$

$D \in \mathcal{P}$이고 f가 $\mathcal{P}$상의 원소에 대해 가산이기에 어떤 $d \in \mathbb{N}$가 존재하여 $f(d) = D$를 만족할 것이다. 그리하여 모든 $n \in f(d)$에 대해 아래와 같다.

$$n \in f(d) \iff n \notin f(n).$$

이는 모순이다. 따라서 f와 같은 열거 함수는 존재할 수 없다. 따라서 멱집합 $\mathcal{P}$는 가산일 수 없다. 즉 비가산$_{\text{indenumerable}}$이다. $\square$

여기서 D를 대각$_{\text{diagonal}}$집합이라고 한다. 대각집합을 직접 사용하지 않고도 대각화의 발상으로 다시 증명할 수도 있다.

Proof. 무한 이진문자열$_{\text{binary strings}}$의 집합 $\mathbb{B}$가 존재한다. 역으로 열거 함수 $f : \mathbb{N} \to \mathbb{B}$가 존재한다고 가정하자.

$$
\begin{gathered}
0 \to b_0 : \underline{0}110001010011\ldots \\
1 \to b_1 : 1\underline{1}00101001101\ldots \\
2 \to b_2 : 11\underline{0}0101100001\ldots \\
\vdots
\end{gathered}
$$

대각선을 따라 $n \in \mathbb{N}$을 n번째 문자열 $b_n \in \mathbb{B}$의 $n+1$번째 자릿수$_{\text{digit}}$로 사상하는 것이다. 그리고 이제 그 n번째 자릿수에 대해 0과 1을 뒤바꾼다. 이렇게 대각자릿수를 뒤

집은 문자열 d는 b_0과 1번째 자릿수에 대해 다르고, b_1은 2번째 자릿수에 대해 다르고, b_2는 3번째 자릿수에 대해 다르다. 따라서 모든 $n \in \mathbb{N}$을 $b_n \in \mathbb{B}$에 대해 사상한 집합은 $d \in \mathbb{B}$를 포함하지 않는다. 그리하여 $f : \mathbb{N} \to \mathbb{B}$는 열거함수가 아니다. 이는 모순이다. 따라서 모든 함수 $f : \mathbb{N} \to \mathbb{B}$는 열거함수일 수 없고, 따라서 $\mathbb{B}$는 비가산이다. $\square$

제 2 장

튜링