양자계산복잡도이론 학습일지

김태원

최초 작성 : 2023년 8월 27일
최근 편집 : 2023년 8월 28일

차 례

제 1 장

계산

1.1 대각화

함수 f가 정의역domain Δ상의 원소를 공역codomain Γ상의 원소로 사상maps to한다는 말을 아래처럼 표기한다.

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

f의 치역range은 아래와 같다.

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

f의 치역이 공역 Γ와 같다면 f는 전사surjective다. 그리고 Δ상의 상이한 원소를 Γ상의 상이한 원소로 사상하는 f는 단사injective다. f가 전사이고 단사라면 전단사bijcetive다.

성질property P의 **특성함수***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 분할partition한다.

집합 Σ가 **열거가능***enumerable* 혹은 가산이라는 필요충분조건iff은 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

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

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

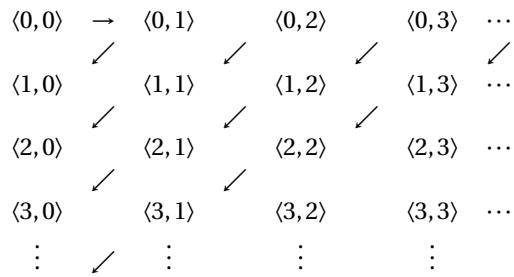

그림 1.1: 대각 논법

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

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

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

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

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

$D \in \mathscr{P}$이고 f가 $\mathscr{P}$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 $\mathscr{P}$는 가산일 수 없다. 즉 비가산indenumerable이다. □

여기서 D를 대각diagonal집합이라고 한다. 대각집합을 직접 사용하지 않더라도 대각화라는 발상만으로 다시 증명할 수도 있다.

Proof. 무한 이진문자열binary strings의 집합 $\mathbb{B}$가 존재한다. 역으로 열거 함수 $f : \mathbb{N} \to \mathbb{B}$가 존재한다고 가정하자.

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

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

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 열거함수 $f : \mathbb{N} \to \mathbb{B}$는 존재하지 않는다. 다시 말해 $\mathbb{B}$는 비가산이다. □

1.2 계산가능성

알고리즘을 부분함수에 대한 계산computation으로 정의할 수 있다. 부분함수partial function란 정의역상의 인자argument에 대해 출력이 존재하지 않을 수도 있는 사상 f다.

또한 계산가능성computability을 계산기computer의 크기나 속도와 완전히 무관하게 정의할 수 있다. 이처럼 급진적인 추상화는 알고리즘 계산의 가능성과 한계에 대해 내놓을 수 있는 모든 주장을 강화한다. 계산 모델로는 튜링장치Turing Machine가 있을 수 있다.

논제 1.1 (튜링 1936)**.** 비형식적으로 말해 효과적으로 계산가능한 수치 함수는 실상 전부 적절한 튜링장치로 계산가능한 함수들이다.

튜링 논제에서 유의해야 하는 표현은 수치함수*numerical function*다. 모든 비수치nonnumerical 객체 X를 어떤 수로 사상 혹은 부호화할 수 있다. 이런 X를 표준형식언어standard formal languages상의 표현식*expressions*이라고 부른다.

정의 1.1. 수치적인 성질 혹은 관계가 효과적으로 결정가능*effectively decidable*하다는 말의 필요충분조건*iff*은 그 특성함수가 효과적으로 계산가능하다는 것이다.

정의 1.2. 집합 Σ가 효과적으로 결정가능하다는 말의 필요충분조건*iff*은 Σ의 성질에 대한 특성함수 c_Σ가 효과적으로 계산가능하다는 것이다.

정리 1.3. 모든 자연수 집합은 효과적으로 결정가능하다.

정리 1.4. Σ가 효과적으로 결정가능한 집합이라면 그 여집합*complement* $\overline{\Sigma}$도 효과적으로 결정가능한 집합이다.

Proof. $\Sigma \subseteq \mathbb{N}$이 유한하다면 특성함수 c_Σ는 항상 1이나 0의 값을 지닌다. 이런 함수는 무차별대입brute-force 알고리즘으로 1이나 0을 계산가능하다. 따라서 모든 자연수 집합은 효과적으로 결정가능하다.

또한 특성함수 c_Σ가 효과적으로 계산가능하다면 $\overline{\Sigma}$의 특성함수 $\overline{c}$는 다음처럼 정의될 수 있다.

$$\overline{c}(n) = 1 - c_\Sigma(n)$$

그리고 c_Σ의 계산가능성으로 $\overline{c}$ 또한 계산가능하다. □

정의 1.3. 집합 Σ는 효과적으로 열거가능*effectively enumerable*하다는 말의 필요충분조건은 Σ가 공집합이거나 효과적인 계산가능 함수가 존재하여 Σ를 열겨한다는 것이다.

정리 1.5. Σ가 효과적으로 결정가능한 집합이라면 효과적으로 열거가능하다.

Proof. $s \in \Sigma$가 있다고 하자. 그리고 입력 n에 대해 $n \in \Sigma$를 효과적으로 확인할 수 있는 알고리즘에 대해 $n \in \Sigma$라면 n을 출력하고 $n \notin \Sigma$라면 s를 출력한다고 하자. 이 알고리즘은 전사함수 $f : \mathbb{N} \to \Sigma$를 계산한다. 따라서 Σ는 효과적으로 열거가능하다. □

정리 1.6. Σ와 그 여집합 $\overline{\Sigma}$가 모두 효과적으로 열거가능한 집합이라면 Σ는 효과적으로 결정가능하다.

Proof. Σ가 계산가능함수 f에 의해 열거가능한 집합이며 $\overline{\Sigma}$가 계산가능함수 g에 의해 열거가능한 집합이라고 하자. 차례로 계산한다.

$$f(0), g(0), f(1), g(1), f(2), g(2), \ldots$$

임의로 주어진 s에 대해 $s \in \Sigma \iff s \notin \overline{\Sigma}$ 혹은 $s \in \overline{\Sigma} \iff s \notin \Sigma$이므로 s는 무조건 출력된다. 다시 말해 어떤 m이 존재하여 $f(m) = s$를 만족하거나 어떤 n이 존재하여 $g(n) = s$를 만족한다. 따라서 f 혹은 g는 효과적으로 계산가능하기에 Σ 혹은 $\overline{\Sigma}$가 결정가능한 집합이다. 그리고 $\overline{\overline{\Sigma}} = \Sigma$이므로 Σ는 효과적으로 결정가능하다. □

이쯤 알고리즘을 더 명확하게 정의한다.

정의 1.4. 알고리즘의 정의역은 입력 $n \in \mathbb{N}$에 대해 알고리즘 실행이 언젠가는 종결하고 어떤 수를 출력으로 내놓는 자연수의 집합이다.

정리 1.7. W가 효과적으로 열거가능한 집합인 필요충분조건은 W가 어떤 알고리즘의 정의역이라는 것이다.

Proof. ($\Rightarrow$) W가 열거가능한 집합이라고 하자. 그렇다면 정의상 (i) W가 공집합이거나 (ii) 계산가능함수 f가 존재하여 W를 열거한다.

(i)의 경우 아무 출력도 내놓지 않는 알고리즘 아무거나 고르면 된다. (ii)의 경우 어떤 알고리즘 Π가 존재하여 함수 f를 계산한다. Π로 더 복잡한 알고리즘 Π^+를 구성할 수 있다. 주어진 입력 n에 대해 Π로 루프loop하며 $f(0), f(1), f(2), \ldots$를 계산하다가 어떤 i에 대해 $f(i) = n$인 경우 멈추고 i를 출력한다. 따라서 Π^+의 정의역은 W다.

($\Leftarrow$) W가 어떤 알고리즘 Π의 정의역이라고 하자. W가 공집합이라면 W는 열거가능하다. W가 공집합이 아니라고 하자. 정리 1.1에 의해 각각의 가능한 쌍 $\langle i, j \rangle$에 대해 $n \in \mathbb{N}$과 일대일대응이 존재한다. 그리고 이에 계산가능함수 $\mathrm{fst}(n)$과 $\mathrm{snd}(n)$이 존재하여

각각 n번째 쌍의 첫 번째 성분 i와 두 번째 성분 j를 반환한다. 이들 함수로 Π'를 다음처럼 정의한다.

주어진 입력 n에 대해 $i = \mathrm{fst}(n)$과 $j = \mathrm{snd}(n)$를 계산한다. 그리고 Π를 입력 i에 대해 j번 실행한다. Π가 입력 i에 대해 어떤 출력 j로 정지$_{\mathrm{halt}}$하면 Π'는 i를 출력한다. 그 외의 경우 Π'는 o를 출력한다.

n이 증가할 때마다 Π'는 모든 i, j에 대해 Π를 확인한다. 그리고 Π가 결국 어떤 출력을 내놓는 i를 출력한다. 그리하여 Π'는 Π의 정의역 W를 치역으로 지니는 함수를 계산한다. 따라서 W는 열거가능하다. □

정리 1.8. 모든 효과적으로 열거가능한 자연수 집합들의 집합 $\mathscr{W}$는 열거가능하다.

당연하다. 이는 아래 같은 따름정리를 유도한다.

정리 1.9. 어떤 집합은 효과적으로 열거가능하지 않기에 효과적으로 결정가능하지 않다.

Proof. 정리 1.2에 의해 $\mathbb{N}$의 멱집합 $\mathscr{P}$는 열거가능하지 않다. 따라서 $\mathscr{W} \neq \mathscr{P}$다. 그러나 $\mathscr{W} \subset \mathscr{P}$다. 그래서 $\mathscr{W}$에 없는 것들이 $\mathscr{P}$에는 존재한다. 즉 효과적으로 열거가능하지 않은 집합들이 존재하는 것이다. 정리 1.5의 대우에 의해 이들 집합은 결정불가능하다. □

정리 1.10 (열거가능집합의 근본 정리)**.** 효과적으로 열거가능한 집합 K가 존재하여 여집합 $\overline{K}$는 효과적으로 열거불가능하다.

Proof. K를 아래처럼 정의한다.

$$K := \{e | e \in W_e\}.$$

정의상 모든 e에 대해 아래가 성립한다.

$$e \in \overline{K} \iff e \notin W_e.$$

그래서 $\overline{K}$는 모든 W_e에 대해 다르다. 그래서 $\overline{K}$는 효과적으로 열거가능한 집합이 아니다. W_e가 전부이기 때문이다.

$\overline{K}$가 효과적으로 열거불가능하기에 $\overline{K}$는 $\mathbb{N}$ 전체일 수 없다. 그리하여 K는 공이 아닌 집합이다. o를 K상의 어떤 원소로 두고 알고리즘 Π''를 아래처럼 정의한다.

> 주어진 입력 n에 대해 $i = \mathrm{fst}(n), j = \mathrm{snd}(n)$을 계산한다. 그리고 알고리즘 Π_i를 찾아 입력 i에 대해 j번 실행한다. Π_i가 입력 i에 대해 j로 출력하며 정지한다면 Π''는 i를 출력한다. 이외의 경우 Π''는 기본값 o를 출력한다.

n이 증가하며 Π''는 모든 쌍 $\langle i, j \rangle$에 대해 실행한다. 그래서 Π''의 출력은 i가 Π_i의 정의역인 모든 i의 집합이다. 즉 $i \in W_i$이며 다시 말해 K다. 따라서 K는 효과적으로 열거가능하다. □

정리 1.11. 어떤 효과적으로 열거가능한 집합은 결정가능하지 않다.

Proof. 열거불가능한 여집합을 지니는 임의의 열거가능 집합 K를 취한다. K가 결정가능하다고 가정하자. 정리 1.4에 의해 K가 결정가능하면 그 여집합 $\overline{K}$ 또한 결정가능할 것이다. 하지만 그렇다면 정리 1.5에 의해 $\overline{K}$는 열거가능 집합일 것이다. 이는 모순이다. 따라서 어떤 열거가능 집합은 결정불가능하다. □

제 2 장

튜링