

양자계산복잡도이론 학습일지

김태원

최초 작성 : 2023년 8월 27일

최근 편집 : 2023년 8월 29일

차 례

차 례	2
제 1 장 계산	3
1.1 대각화	3
1.2 계산가능성	5
1.3 결정가능성	5
1.4 열거가능성	6
1.5 공리화된 이론	10
1.6 표현과 포착	11

제 1 장

계산

1.1 대각화

함수 f 가 정의역 Δ 상의 원소를 공역 Γ 상의 원소로 사상 *maps to* 한다는 말을 $f : \Delta \rightarrow \Gamma$ 와 같이 표기하고 f 의 치역 *range*은 $\{f(x) \in \Gamma \mid x \in \Delta\}$ 다. f 의 치역이 공역 Γ 와 같다면 f 는 전사 *surjective*다. 그리고 Δ 상의 상이한 원소를 Γ 상의 상이한 원소로 사상하는 f 는 단사 *injective*다. f 가 전사이고 단사라면 전단사 *bijjective*다. 이제 시작하자.

정의 1.1. 성질 *property* P 의 특성함수 *characteristic function* $c_P : \mathbb{N} \rightarrow \{0, 1\}$ 는 n 이 성질 P 를 만족하면 $c_P(n) = 1$ 인 함수다. 이때 성질 P 는 \mathbb{N}^2 을 두 집합으로 분할 *partition*한다.

정의 1.2. 집합 Σ 가 열거가능 *enumerable* 혹은 가산이라는 필요충분조건 *iff*은 Σ 가 공집합이거나 전사 함수 $f : \mathbb{N} \rightarrow \Sigma$ 가 존재한다는 것이다.

위 두 정의와 아래 정리는 기초집합론에서 자주 다루는 내용이다.

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

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

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

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

¹통상적으로 참을 1로 표현하지만 괴델과 불완전성을 다루는 1장에 한해 참을 0으로 나타낸다.

²물론 \mathbb{N} 은 모든 자연수의 집합을 나타낸다.

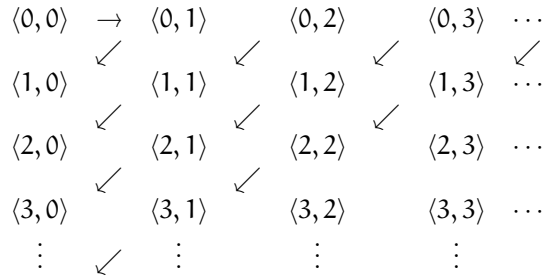


그림 1.1: 대각 논법

아래는 이른바 칸토어 정리다.

정리 1.2. 가산이 아닌 무한집합이 존재한다.

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

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

함수 $f : \mathbb{N} \rightarrow \mathcal{P}$ 가 존재하여 \mathcal{P} 가 가산이라고 가정한다. 이어서 \mathbb{N} 의 부분집합 D 를 아래처럼 둔다.

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

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

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

모순이다. 따라서 f 와 같은 열거 함수는 존재할 수 없고 멍집합 \mathcal{P} 는 가산일 수 없다. 즉 비가산^{indenumerable}이다. □

여기서 D 를 대각^{diagonal}집합이라고 한다. 대각집합을 직접 사용하지 않더라도 대각화라는 발상만으로 다시 증명할 수도 있다.

Proof. 무한 이진문자열^{binary strings}의 집합 \mathbb{B} 가 존재한다. 열거 함수 $f : \mathbb{N} \rightarrow \mathbb{B}$ 가 존재한다고 가정한다.

$$\begin{aligned}
 0 &\rightarrow b_0 : 0110001010011\dots \\
 1 &\rightarrow b_1 : 1100101001101\dots \\
 2 &\rightarrow b_2 : 1100101100001\dots \\
 &\vdots
 \end{aligned}$$

대각선을 따라 $n \in \mathbb{N}$ 을 n 번째 문자열 $b_n \in \mathbb{B}$ 의 $n + 1$ 번째 자릿수_{digit}로 사상한다. 그리고 이제 각 n 번째 자릿수에 대해 0과 1을 뒤바꾼다. 이렇게 대각자릿수를 뒤집은 각 문자열 d_i 는 b_0 과 1번째 자릿수에 대해 다르고, b_1 과 2번째 자릿수에 대해 다르고, b_2 와 3번째 자릿수에 대해 다르다. 따라서 모든 $n \in \mathbb{N}$ 을 $b_n \in \mathbb{B}$ 에 대해 사상한 집합은 $d_i \in \mathbb{B}$ 를 포함하지 않는다. 그리하여 $f: \mathbb{N} \rightarrow \mathbb{B}$ 는 (전사가 아니라는) 열거함수가 아니다. 모순이다. 따라서 열거함수 $f: \mathbb{N} \rightarrow \mathbb{B}$ 는 존재하지 않는다. 즉 \mathbb{B} 는 비가산이다. \square

1.2 계산가능성

대각화라는 발상은 온갖 알고리즘에서 유용하게 쓰인다. 우선 알고리즘을 부분함수³에 대한 계산_{computation}이라고 대단히 추상적으로 정의할 수 있다. 또한 계산가능성_{computability}을 컴퓨터의 크기나 속도와 완전히 무관하게 대단히 추상적으로 정의할 수 있다. 이처럼 급진적인 추상화는 알고리즘 및 계산의 가능성과 한계에 대해 내놓을 수 있는 모든 주장을 극단적으로 강화한다. 이런 맥락에서 컴퓨터 혹은 계산모델_{computation model}로는 튜링장치_{Turing Machine}를 전제한다.

논제 1.1 (튜링 1936). 효과적으로 계산가능하다고 비형식적으로 말할 수 있는 수치함수는 실상 전부 적절한 튜링장치로 계산가능한 함수다.

유의해야 하는 표현은 수치함수_{numerical function}다. 어차피 모든 비수치_{nonnumerical} 객체 X 를 어떤 자연수(의 열)로 사상 혹은 부호화할 수 있기 때문이다. 또한 튜링장치에 의한 계산가능성과 동치인 개념이 그냥 깔끔하게 함수의 계산가능성이 아니라 ‘효과적인’ 계산가능성이므로 거추장스러운 ‘효과적인’이라는 표현이 줄줄 따라다닐 예정이다. 여기서 ‘효과’란 성능 따위가 아니라 말 그대로 어떤 효과를 지닌다는 뜻이다.

1.3 결정가능성

효과적인 계산가능성 개념에 기초하여 효과적인 결정가능성 개념을 정의한다.

정의 1.3. 성질이 효과적으로 결정가능하다_{effectively decidable}는 필요충분조건은 성질의 특성함수가 효과적으로 계산가능하다는 것이다.

정의 1.4. 집합 Σ 가 효과적으로 결정가능하다는 필요충분조건은 Σ 의 성질에 대한 특성함수 c_Σ 가 효과적으로 계산가능하다는 것이다.

효과적인 결정가능성은 특성함수의 효과적인 계산가능성으로 정의되고 이 사실은 \mathbb{N} 의 모든 유한 부분집합에 대해 번역될 수 있다.

³부분함수_{partial function}란 정의역상의 인자_{argument}에 대해 출력이 존재하지 않을 수도 있는 사상 f 다.

정리 1.3. 모든 유한한 자연수 집합은 효과적으로 결정가능하다.

Proof. Σ 가 유한한 자연수 집합이라고 하자. 정의 1.1에 의해 특성함수 c_Σ 는 $\Sigma \subset \mathbb{N}$ 에 대해 항상 1이나 0의 값을 지닌다. Σ 가 유한집합이기 때문에 특성함수 c_Σ 는 무차별 대입 brute-force 알고리즘으로 1이나 0으로 효과적으로 계산가능⁴하다. 따라서 정의 1.4에 의해 모든 유한한 자연수 집합은 효과적으로 결정가능하다. \square

한 집합의 효과적인 결정가능성은 그 여집합 complement의 결정가능성도 보장한다.

정리 1.4. Σ 가 효과적으로 결정가능한 집합이라면 여집합 $\bar{\Sigma}$ 도 효과적으로 결정가능한 집합이다.

Proof. 효과적으로 결정가능한 집합 Σ 가 있다고 하자. 정의 1.4에 의해 Σ 의 특성함수 c_Σ 는 효과적으로 계산가능하다. c_Σ 가 효과적으로 계산가능하기에 다음처럼 정의된 $\bar{\Sigma}$ 의 특성함수 \bar{c} 는 효과적으로 계산가능하다.

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

다시 정의 1.4에 의해 $\bar{\Sigma}$ 또한 효과적으로 결정가능한 집합이다. \square

1.4 열거가능성

이제 함수의 효과적인 계산가능성을 이용해 집합의 효과적인 열거가능성을 정의한다. ‘계산가능 함수’가 실상 ‘알고리즘’이라는 사실을 적극적으로 쥐어짠다.

정의 1.5. 집합 Σ 가 효과적으로 열거가능하다 *effectively enumerable*는 필요충분조건은 Σ 가 공집합이거나 효과적인 계산가능 함수가 존재하여 Σ 를 열거한다는 것이다.

즉 정의 1.2를 돌이키면 Σ 의 효과적인 열거가능성은 알고리즘으로서의 전사 함수 $f: \mathbb{N} \rightarrow \Sigma$ 의 존재성으로 정의된다.

정리 1.5. Σ 가 효과적으로 결정가능한 집합이라면 효과적으로 열거가능하다.

Proof. 효과적으로 결정가능한 집합 Σ 가 있다고 하자. $s \in \Sigma$ 를 고정하고 정의 1.4에 의해 임의의 입력 n 에 대해 n 이 Σ 에 속하는지 나타내는 특성함수 c_Σ 를 효과적으로 계산할 수 있는 알고리즘 Π 를 구성한다. Π 는 아래처럼 정의된다.

$$\Pi(n) = \begin{cases} n & n \in \Sigma \text{인 경우} \\ s & n \notin \Sigma \text{인 경우} \end{cases}$$

⁴‘계산가능성’과 ‘알고리즘의 존재성’이 대단히 비슷한 쓰임새를 지닌다는 사실을 확인할 수 있다.

Π 의 정의역은 \mathbb{N} 이고 치역은 Σ 다. 따라서 정의 1.2와 1.5에 의해 Σ 는 효과적으로 열거 가능하다. \square

알고리즘의 정의역이라는 개념이 증명에서 중요하게 쓰인다는 사실을 확인할 수 있다. 알고리즘을 한 번 더 사용해 보자.

정리 1.6. Σ 와 그 여집합 $\bar{\Sigma}$ 모두 효과적으로 열거가능한 집합이면 Σ 는 효과적으로 결정 가능하다.

Proof. 열거가능 집합 Σ 이 존재하며 여집합 $\bar{\Sigma}$ 또한 열거가능하다고 하자. 정의 1.5에 의해 Σ 와 $\bar{\Sigma}$ 에 대해 각각 계산가능함수 f 와 g 가 존재한다. f 와 g 가 출력할 수 있는 모든 s 에 대해 아래와 같은 상황이 성립한다.

$$s \in \Sigma \iff s \notin \bar{\Sigma}$$

다시 말해 어떤 m 이 존재하여 $f(m) = s$ 를 만족하거나 어떤 n 이 존재하여 $g(n) = s$ 를 만족한다. 따라서 정리 1.4에 의해 c_Σ 혹은 $c_{\bar{\Sigma}}$ 를 계산하는 알고리즘 Π 를 Σ 나 $\bar{\Sigma}$ 에 대해 구성할 수 있다. 아래는 Σ 에 대해 구성한 Π_Σ 다.

$$\Pi_\Sigma(s) = \begin{cases} 0 & s \in \Sigma \text{인 경우} \\ 1 & s \notin \Sigma \text{인 경우} \end{cases}$$

그리고 임의의 공이 아닌 집합 A 에 대해 $\bar{\bar{A}} = A$ 다. 따라서 Σ 는 정의 1.4에 의해 효과적으로 결정가능한 집합이다. \square

이쯤 알고리즘의 정의역을 정의해 알고리즘을 더 분명하게 다룬다.

정의 1.6. 알고리즘의 정의역은 입력 $n \in \mathbb{N}$ 에 대해 알고리즘이 언젠가는 종결하며 어떤 수를 출력으로 내놓도록 하는 자연수의 집합이다.

알고리즘의 정의역은 실상 효과적으로 열거가능한 집합과 같은 말이다. 이 사실을 증명할 때는 알고리즘으로 알고리즘을 구성해 루프를 구성하는 기법이 유용하다. 또한 알고리즘의 정의상 종결을 유도해야 하기에 꽤 복잡해 보일 수 있다.

정리 1.7. W 가 효과적으로 효과적으로 열거가능한 집합인 필요충분조건은 W 가 어떤 알고리즘의 정의역이라는 것이다.

Proof. 필요충분조건을 양방향으로 증명한다.

(\Rightarrow) W 가 열거가능한 집합이라고 하자. 정의 1.5에 의해 아래가 성립한다.

1. W 가 공집합이거나

2. 계산가능 함수 f 가 존재하여 W 를 열거한다. 즉 $i \in \mathbb{N}$ 에 대해 아래와 같다.

$$n \in W \iff f(i) = n$$

첫 번째 경우 아무 출력도 내놓지 않는 알고리즘 아무거나 고르면 된다. 두 번째 경우 함수 f 를 계산하는 알고리즘 Π 를 구성한다. 그리고 Π 로 다시 알고리즘 Π^+ 를 구성한다. 알고리즘 Π^+ 는 입력 $n \in W$ 에 대해 Π 로 루프_{loop}하며 $f(0), f(1), f(2), \dots$ 를 계산하다가 어떤 i 에 대해 $f(i) = n$ 인 경우 멈추고 i 를 출력한다. 여기서 Π^+ 가 입력으로 취하는 값 n 은 W 상의 임의의 원소다. 따라서 W 는 Π^+ 의 정의역이다.

(\Leftarrow) W 가 알고리즘 Π 의 정의역이라고 하자. 정의 1.5에 의해 W 가 공집합이라면 W 는 열거가능하다. W 가 공집합이 아니라고 가정하고 $o \in W$ 를 고정하자. 정리 1.1에 의해 $n \in \mathbb{N}$ 과 $\langle i, j \rangle$ 에 대해 일대일대응이 존재한다. 이 사실을 바탕으로 계산가능 함수 $\text{fst}(n)$ 과 $\text{snd}(n)$ 을 구성한다. 각각 n 번째 쌍의 첫 번째 성분 i 와 두 번째 성분 j 를 반환하는 함수다. 이들 함수로 새로운 알고리즘 Π' 를 다음처럼 구성한다.

Π' 는 우선 주어진 입력 $n \in \mathbb{N}$ 에 대해 $i = \text{fst}(n)$ 와 $j = \text{snd}(n)$ 를 계산한다. 그리고 $i \notin W$ 라면 o 를 출력한다. $i \in W$ 라면 i 를 입력으로 Π 를 j 번 루프한다. Π 가 어떤 입력 i 에 대해 어떤 출력 j 로 정지하면 Π' 는 $i \in W$ 를 출력한다.

즉 Π' 는 \mathbb{N} 를 Π 의 정의역 W 로 사상한다. 따라서 정의 1.5에 의해 W 는 효과적으로 열거가능한 집합이다. \square

아래는 당연한 사실이며 따로 증명하지 않겠다.

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

그런데도 이 사실은 아래 따름정리를 유도하기에 중요하다.

정리 1.9. 어떤 집합은 효과적으로 열거불가능하고 그래서 효과적으로 결정불가능하다.

Proof. 정리 1.2에 의해 \mathbb{N} 의 멍집합 \mathcal{P} 는 열거가능하지 않다. 즉 효과적으로 열거불가능한 집합이 존재한다. 그리고 정리 1.5의 대우에 의해 \mathcal{P} 는 효과적으로 결정불가능하다.

더 강력하게 증명할 수도 있다. 정리 1.8에 의해 모든 효과적으로 열거가능한 자연수 집합들의 집합 \mathcal{W} 는 열거가능하다. 그렇기에 당연히 $\mathcal{W} \neq \mathcal{P}$ 이지만 더 중요한 함의는 바로 $\mathcal{W} \subset \mathcal{P}$ 다. 즉 \mathcal{W} 의 원소가 아니어서 효과적으로 열거불가능한 집합들이 존재하며 그렇기에 효과적으로 결정불가능한 집합들이 존재한다. \square

아래 정리에는 대각화 구성 과 루프 등 지금까지 학습한 기법이 총동원된다.

정리 1.10 (열거가능집합의 근본 정리). 효과적으로 열거가능한 집합 K 가 존재하여 여집합 \bar{K} 는 효과적으로 열거불가능하다.

Proof. 효과적으로 열거가능한 집합 K 가 존재하면 그 여집합 \bar{K} 가 효과적으로 열거불가능하다는 사실 (i)를 증명하고 이 사실에 기초해 효과적으로 열거가능한 집합 K 의 존재성 (ii)를 증명한다.

(i) 효과적으로 열거가능한 집합 K 는 정리 1.8에서 구성한 모든 효과적으로 열거가능한 집합들의 집합 \mathcal{W} 상 임의의 e 번째 원소 W_e 라는 집합이다. 이 사실을 아래처럼 나타낼 수 있다.

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

여집합의 정의상 모든 e 에 대해 아래가 성립한다.

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

이 사실은 e 뿐만 아니라 모든 W_e 에 대해 성립한다. 즉 \bar{K} 는 정리 1.9에서 언급한 \mathcal{P}/\mathcal{W} 상의 원소다. 다시 말해 \bar{K} 는 효과적으로 열거불가능하다.

(ii) \bar{K} 가 효과적으로 열거불가능하므로 \bar{K} 는 \mathbb{N} 전체일 수 없다. 그리하여 K 는 공이 아닌 집합이다. o 를 K 상의 어떤 원소로 고정하고 알고리즘 Π'' 를 아래처럼 정의한다.

주어진 입력 $n \in \mathbb{N}$ 에 대해 $i = \text{fst}(n), j = \text{snd}(n)$ 을 계산한다. 그리고 $i \notin K$ 라면 o 를 출력한다. $i \in K$ 라면 알고리즘 Π_i 를 찾아 입력 i 에 대해 j 번 루프한다. Π_i 가 입력 i 에 대해 j 를 출력하며 정지하면 Π'' 는 i 를 출력한다.

즉 Π'' 는 \mathbb{N} 을 각 Π_i 의 치역인 K 로 사상한다. 따라서 정의 1.5에 의해 K 는 효과적으로 열거가능하다. \square

이 증명을 통해 정리 1.9를 강화할 수 있다.

정리 1.11. 어떤 효과적으로 열거가능한 집합은 결정가능하지 않다.

Proof. 정리 1.10과 같이 효과적으로 열거불가능한 여집합을 지니는 임의의 효과적으로 열거가능한 집합 K 를 구성한다. 이에 K 가 효과적으로 결정가능하다고 가정하자. 그리고 K 가 효과적으로 결정가능하면 정리 1.4에 의해 그 여집합 \bar{K} 또한 효과적으로 결정가능하다. 하지만 그렇다면 정리 1.5에 의해 \bar{K} 가 효과적으로 열거가능한 집합일 것이다. 모순이다. 따라서 어떤 열거가능 집합은 결정불가능하다. \square

이제 계산가능성, 결정가능성, 열거가능성이라는 강력한 도구로 이론과 언어의 문제를 다룬다.

1.5 공리화된 이론

효과적으로 공리화된 이론 *effectively axiomatized theory*은 구문론 *syntax* \mathcal{L} 과 의미론 *semantics* \mathcal{I} 에 대해 결정가능성의 정의 1.4로 정의된다. 여기서 ‘wff’라고 나타내는 잘 형성된 공식 *well-formed formulae*은 간신히 의미를 부여할 수 있거나 남아도는 자유변수 탓에 깔끔하지 않은 대상이다. 중요한 것은 문장이다. 문장은 닫힌 wffs로서 자유변수가 남아돌지 않는다.

정의 1.7. T는 아래를 만족하는 경우만 효과적으로 공리화된 이론이다.

1. T를 표현하는 형식화된 언어 $L = \langle \mathcal{L}, \mathcal{I} \rangle$ 가 존재하여 \mathcal{L} 의 \mathcal{L} -wff가 무엇인지 효과적으로 결정가능하다.
2. 어떤 \mathcal{L} -wff가 T의 공리인지 효과적으로 결정가능하다.
3. T의 증명체계가 존재하여 \mathcal{L} -wff 배열이 증명설계규칙을 따르는지 효과적으로 결정가능하다.
4. \mathcal{L} -wff 배열이 T의 공리로 증명을 구성할 수 있는지 효과적으로 결정가능하다.

이제 중요한 단어들을 빠르게 정의한다.

정의 1.8. 이론 T의 공리에서 논리적 증명체계로 문장 φ 가 유도될 때 φ 를 T의 정리 *theorem*라고 부르고 $T \vdash \varphi$ 라고 표기한다.

정의 1.9. 이론 T가 타당하다 *sound*는 필요충분조건은 T의 모든 정리가 참이라는 것이다.

정의 1.10. 이론 T가 효과적으로 결정가능하다는 필요충분조건은 T의 정리로 존재하는 성질이 효과적으로 결정가능한 성질이라는 것이다. 다시 말해 T의 언어로 주어진 임의의 문장 φ 에 대해 $T \vdash \varphi$ 인지 결정하는 알고리즘이 존재한다는 것이다.

정의 1.11. 이론 T가 문장 φ 를 결정한다는 필요충분조건은 $T \vdash \varphi$ 이거나 $T \vdash \neg\varphi$ 라는 것이다. 이론 T가 φ 를 올바르게 결정한다는 말은 φ 가 참이라면 $T \vdash \varphi$ 이고 φ 가 거짓이라면 $T \vdash \neg\varphi$ 라는 뜻이다.

정의 1.12. 이론 T가 부정완전 *negation-complete*하다는 필요충분조건은 T가 제 언어의 모든 문장 φ 를 결정한다는 것이다. 다시 말해 모든 문장 φ 에 대해 $T \vdash \varphi$ 이거나 $T \vdash \neg\varphi$ 라는 것이다.

정의 1.13. T가 모순적 *inconsistent*이라는 필요충분조건은 어떤 문장 φ 가 존재하여 $T \vdash \varphi$ 와 $T \vdash \neg\varphi$ 를 모두 지닌다는 것이다.

이제 효과적인 열거가능성의 개념 1.5로 아래처럼 정리한다. 여기서 알파벳이란 언어에 대해 주어지는 임의의 유한집합이다.

정리 1.12. T가 효과적으로 공리화된 이론일 때 이 집합들은 효과적으로 열거가능하다.

1. T 의 wff들의 집합
2. T 의 문장들의 집합
3. T 상에서 구성가능한 증명들의 집합
4. T 의 정리들의 집합

Proof. T 가 효과적으로 공리화된 이론이라고 하자. 정의 1.7에 의해 T 는 유한 알파벳으로 구성된 형식 언어를 지닌다. 그리고 유한 알파벳상의 모든 문자열은 대각화 알고리즘을 통해 효과적으로 열거될 수 있다. 길이 1의 문자열, 길이 2의 문자열, \dots 길이 n 의 문자열들에 대해 각각 알파벳 순서로 효과적으로 열거하는 알고리즘 Π_1 이다. 또한 다시 정의 1.7에 의해 wff를 효과적으로 결정할 수 있는 알고리즘 Π_2 가 존재한다. 따라서 Π_1 이 가능한 모든 문자열을 대각화하는 가운데 Π_2 로 wff를 효과적으로 결정하여 이들만 효과적으로 열거하는 통합적인 알고리즘 Π_3 을 구성한다. 여기서 ‘wff’를 ‘문장’으로 대체하면 1,2의 증명이 끝난다.

T 상에서 구성가능한 증명은 wff의 배열과 같고 증명들의 집합은 wff의 배열들의 집합과 같다. 각 배열 길이 i 와 배열상의 wff의 길이 j 와 알파벳 순서로 효과적으로 열거하는 대각화 알고리즘 Π_4 를 구성한다. 그리고 wff의 배열은 무차별대입 알고리즘과 wff 결정 알고리즘 Π_2 로 구성할 수 있다. 그리하여 T 상에서 구성가능한 증명들이 효과적으로 열거가능하므로 각 wff 배열에 대해 증명설계규칙을 따르는지 효과적으로 결정가능한 알고리즘 Π_5 를 구성한다. 따라서 정의 1.7에 의해 3,4의 증명이 끝난다. \square

이론의 무모순성consistency과 부정완전성은 결정가능성을 보장한다.

정리 1.13. 임의의 무모순적이고 효과적으로 공리화된 부정완전 이론 T 는 효과적으로 결정가능하다.

Proof. T 가 임의의 무모순적이고 효과적으로 공리화된 부정완전 이론이라고 하자. 정리 1.12에 의해 T 의 정리를 효과적으로 열거하는 알고리즘 Π_1 이 존재한다. Π_1 에 따라 정리들을 효과적으로 열거하는 가운데 부정완전의 정의 1.12에 의해 ϕ 가 나타나면 $\neg\phi$ 는 정리가 아니라고 결정하고 $\neg\phi$ 가 나타나면 ϕ 는 정리가 아니라고 결정하는 알고리즘 Π_2 를 구성한다. 또한 무모순의 정의 1.13의 정의에 의해 위와 같은 Π_2 는 정리와 정리가 아닌 문장을 전부 분할하는 알고리즘이다. 다시 말해 T 의 언어로 주어진 임의의 문장 ϕ 에 대해 $T \vdash \phi$ 를 결정하는 알고리즘이 존재한다. 따라서 결정가능성의 정의 1.10에 의해 T 는 효과적으로 결정가능하다. \square

1.6 표현과 포착

앞서 언급한 구문론과 의미론의 쌍 $\langle \mathcal{L}, \mathcal{A} \rangle$ 의 의미를 명시할 필요가 있다. 이 쌍은 어떤 언어 L_A 을 구성한다. \mathcal{L}_A 는 표준 1차논리 구문론을 지닌다. \mathcal{L}_A 의 논리 어휘는 아래와

같은 것들이다.

$$\wedge, \vee, \rightarrow, \leftrightarrow, a, b, \dots, e, u, \dots, z, \forall, \exists, =$$

\mathcal{L}_A 의 비논리 어휘는 아래와 같다.

1. 상수 0
2. 다음 수_{successor} 함수 S^5
3. 함수표현식 $+$, \times

\mathcal{L}_A 의 항_{term}은 ‘0’과 ‘S’, ‘+’, ‘ \times ’로 만들 수 있는 변수다. 그 외 어떤 것도 항일 수 없다.

여기서 ‘=’는 \mathcal{L}_A 의 유일한 술어_{predicate}다. 따라서 원자_{atomic} wff는 모두 임의의 항 ‘a’, ‘b’에 대해 ‘a = b’ 꼴로 서술된다. 일반적으로 wff는 원자 wff에 양화사와 연결사를 1차논리의 표준에 따라 사용한 것이다.

의미론 \mathcal{I}_A 를 해석_{interpretation}이라고 볼 수 있다. \mathcal{I}_A 는 항에 대해 값을 배정하거나 모든 \mathcal{L}_A 문장에 대해 고유한 해석을 효과적으로 배정한다. 그리하여 \mathcal{I}_A 가 효과적으로 형식화된 언어일 수 있다.

아래 정의에서 $\varphi(\bar{n})$ 은 $\varphi(x)$ 상의 ‘x’에 대해 수치 n 을 부여한 것이다.

정의 1.14. 성질 P 가 하나의 자유변수를 지닌 언어 L 상의 wff $\varphi(x)$ 로 표현된다_{expressed}는 필요충분조건은 모든 n 에 대해 아래와 같다는 것이다.

- n 이 성질 P 를 지니면 $\varphi(\bar{n})$ 은 참이다.
- n 이 성질 P 를 지니지 않는다면 $\neg\varphi(\bar{n})$ 은 참이다.

수치함수 f 는 형식 언어에 대해 아래처럼 정의된다.

정의 1.15. 수치함수 f 가 언어 L 상의 wff $\varphi(x, y)$ 로 표현된다는 필요충분조건은 임의의 m, n 에 대해 아래와 같다는 것이다.

- $f(m) = n$ 이면 $\varphi(\bar{m}, \bar{n})$ 이 참이다.
- $f(m) \neq n$ 이면 $\neg\varphi(\bar{m}, \bar{n})$ 이 참이다.

이를 간단하게 정리할 수 있다.

정리 1.14. L 이 성질 P 를 표현할 수 있는 필요충분조건은 L 이 P 의 특성함수 c_P 를 표현할 수 있다는 것이다.

Proof. 아래 두 가지를 확인해야 한다.

1. $\varphi(x)$ 가 P 를 표현하면 $(\varphi(x) \wedge y = 0) \vee (\neg\varphi(x) \wedge y = 1)$ 이 c_P 를 표현한다.
2. $\psi(x, y)$ 가 c_P 를 표현하면 $\psi(x, 0)$ 이 P 를 표현한다.

⁵형식언어는 sans-serif체로 나타낸다

우선 $\varphi(x)$ 가 P 를 표현한다고 하자. 정의 1.14에 의해

$c_P(m) = 0$ 이라면 $\varphi(\bar{m})$ 이 참이고 $(\varphi(\bar{m}) \wedge 0 = 0) \vee (\neg\varphi(\bar{m}) \wedge 0 = 1)$ 이 참이다.

$c_P(m) \neq 0$ 이라면 $\neg\varphi(\bar{m})$ 이 참이고 $(\varphi(\bar{m}) \wedge 0 = 0) \vee (\neg\varphi(\bar{m}) \wedge 0 = 1)$ 은 거짓이다. 그리하여 아래 같은 부정이 참이다.

$$\begin{aligned} & \neg((\varphi(\bar{m}) \wedge 0 = 0) \vee (\neg\varphi(\bar{m}) \wedge 0 = 1)) \\ & \equiv \neg(\varphi(\bar{m}) \wedge 0 = 0) \wedge \neg(\neg\varphi(\bar{m}) \wedge 0 = 1) \end{aligned}$$

따라서 정의 1.15에 의해 L 은 c_P 를 표현할 수 있다.

$\psi(x, y)$ 가 c_P 를 표현한다고 하자. 정의 1.15에 의해

$$\begin{aligned} c_P(m) = n & \Rightarrow \psi(\bar{m}, \bar{n}) \\ c_P(m) \neq n & \Rightarrow \neg\psi(\bar{m}, \bar{n}) \end{aligned}$$

m, n 은 임의로 주어지기에 $n = 0$ 으로 둔다. 이에 아래가 성립한다.

$$\begin{aligned} c_P(m) = 0 & \Rightarrow \psi(\bar{m}, 0) \\ c_P(m) \neq 0 & \Rightarrow \neg\psi(\bar{m}, 0) \end{aligned}$$

따라서 정의 1.14에 의해 L 이 성질 P 를 표현한다. □

표현보다 중요한 것이 증명 혹은 어떤 성질의 포착_{capture}이다.

정의 1.16. 이론 T 가 성질 P 를 *wff* $\varphi(x)$ 로 포착하는 필요충분조건은 임의의 n 에 대해 아래가 성립하는 것이다.

- n 이 성질 P 를 지닌다면 $T \vdash \varphi(\bar{n})$ 이다.
- n 이 성질 P 를 지니지 않는다면 $T \vdash \neg\varphi(\bar{n})$ 이다.

포착과 표현의 차이를 명시하는 편이 낫겠다. 성질 P 가 주어진 이론상 표현가능하다는 말은 그 이론의 언어의 풍부함에 의존하고 P 가 이론에 의해 포착가능하다는 말은 그 이론의 공리와 증명체계의 풍부함에 의존한다. 즉 $\varphi(x)$ 가 타당한 이론 T 상에서 성질 P 를 포착한다면 $\varphi(x)$ 는 P 를 표현한다.