양자계산복잡도이론 학습일지

김태원

최초 작성 : 2023년 8월 27일

최근 편집 : 2023년 8월 29일

차 례

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**$_{\textit{characteristic function}}$ $c_P : \mathbb{N} \to \{0, 1\}$는 $n = P \Rightarrow c_p(n) = 0$을 만족한다. 이때 성질 P는 $\mathbb{N}$을 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

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

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

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

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 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.

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

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

은 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 수치함수는 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. 튜링 논제는 일종의 공리이기에 효과적으로 계산가능하다라는 말을 튜링장치로 계산가능하다라는 말로 바꿔 생각해야 한다. 이와 같은 계산가능성 개념에 기초하여 결정가능성 개념을 정의한다.

정의 1.1. 성질이 <u>효과적으로 결정가능*effectively decidable*</u>하다는 필요충분조건은 그 특성함수가 효과적으로 계산가능하다는 것이다.

정의 1.2. 집합 Σ가 <u>효과적으로 결정가능</u>하다는 말의 필요충분조건은 Σ의 성질에 대한 특성함수 c_Σ가 효과적으로 계산가능하다는 것이다.

여기서 효과란 성능 따위가 아니라 말 그대로 어떤 효과를 지닌다는 뜻이다. 결정가능성은 특성함수의 계산가능성으로 정의되고 이는 $\mathbb{N}$의 모든 유한 부분집합에 대해 번역될 수 있다. 또한 한 집합의 결정가능성은 그 여집합의 결정가능성 또한 보장한다. 정리하면 아래와 같다.

정리 1.3. 모든 유한한 자연수 집합은 효과적으로 결정가능하다.

Proof. $\Sigma \subseteq \mathbb{N}$이 유한하다면 특성함수 c_Σ는 항상 1이나 0의 값을 지닌다. 이런 함수는 무차별대입brute-force 알고리즘으로 1이나 0을 계산할 수 있다. 따라서 정의 1.2에 의해 모든 유한한 자연수 집합은 효과적으로 결정가능하다. □

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

Proof. 효과적으로 결정가능한 집합 Σ가 있다고 하자. 정의 1.2에 의해 Σ의 특성함수 c_Σ는 효과적으로 계산가능하다. c_Σ가 효과적으로 계산가능하기에 $\overline{\Sigma}$의 특성함수 $\overline{c}$는 다음처럼 정의될 수 있다.

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

그리고 c_Σ의 계산가능성으로 $\overline{c}$ 또한 계산가능하다. 다시 정의 1.2에 의해 $\overline{\Sigma}$ 또한 효과적으로 결정가능한 집합이다. □

이제 함수의 계산가능성을 이용해 집합의 열거가능성을 정의한다. 여기서 '계산가능 함수'란 실상 알고리즘과 같다.

정의 1.3. 집합 Σ가 <u>효과적으로 열거가능$_{effectively\ \ enumerable}$</u>하다는 필요충분조건은 Σ가 공집합이거나 효과적인 계산가능 함수가 존재하여 Σ를 열거한다는 것이다.

집합의 결정가능성은 열거가능성을 보장한다.

정리 1.5. Σ가 효과적으로 결정가능한 집합이라면 효과적으로 열거가능하다.

Proof. 효과적으로 결정가능한 집합 Σ가 있다고 하자. $s \in \Sigma$를 고정하고 임의의 입력 n에 대해 n이 Σ에 속하는지 효과적으로 확인하는 알고리즘 Π를 구성한다. Π는 아래처럼 정의된다.

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

여기서 Π는 전사함수 $f : \mathbb{N} \to \Sigma$를 계산한다. 따라서 Σ는 효과적으로 열거가능하다. □

아래 정리는 집합과 그 여집합의 열거가능성에서 각 계산가능함수의 존재를 추출해 집합 혹은 여집합의 여집합의 계산가능성을 유도한다.

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

Proof. 열거가능 집합 Σ이 존재하며 그 여집합 $\overline{\Sigma}$ 또한 열거가능하다고 하자. 정의 1.3에 의해 Σ와 $\overline{\Sigma}$에 대해 각각 계산가능함수 f와 g가 존재한다. f와 g가 출력할 수 있는 있는 모든 s에 대해 아래와 같은 상황이 성립한다.

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

다시 말해 어떤 m이 존재하여 $f(m) = s$를 만족하거나 어떤 n이 존재하여 $g(n) = s$를 만족한다. 따라서 특성-알고리즘 Π를 Σ나 $\overline{\Sigma}$에 대해 구성할 수 있다. 아래는 Σ에 대해 구성한 Π_Σ다.

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

그리고 임의의 공이 아닌 집합 A에 대해 $\overline{\overline{A}} = A$다. 따라서 Σ는 정의 1.2에 의해 효과적으로 결정가능한 집합이다. □

이쯤 알고리즘의 정의역을 정의해 알고리즘을 더 분명하게 다룬다.

정의 1.4. 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. *W가 효과적으로 효과적으로 열거가능한 집합인 필요충분조건은 W가 어떤 알고리즘의 정의역이라는 것이다.*

Proof. 필요충분조건을 양방향으로 증명한다.

($\Rightarrow$) W가 열거가능한 집합이라고 하자. 정의 1.3에 의해 아래가 성립한다.

1. W가 공집합이거나
2. 계산가능 함수 f가 존재하여 W를 열거한다. 즉

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

첫 번째 경우 아무 출력도 내놓지 않는 알고리즘 아무거나 고르면 된다. 두 번째 경우 함수 f를 계산하는 알고리즘 Π를 구성한다. 그리고 Π로 다시 알고리즘 Π^+를 구성한다. 알고리즘 Π^+는 입력 $n \in W$에 대해 Π로 루프$_{\text{loop}}$하며 $f(0), f(1), f(2), \ldots$를 계산하다가 어떤 i에 대해 $f(i) = n$인 경우 멈추고 i를 출력한다. 여기서 Π^+가 입력으로 취하는 값 n은 W상의 임의의 원소다. 따라서 W는 Π^+의 정의역이다.

($\Leftarrow$) W가 알고리즘 Π의 정의역이라고 하자. 정의 1.3에 의해 W가 공집합이라면 W는 열거가능하다. W가 공집합이 아니라고 가정하고 $o \in W$를 고정하자. 정리 1.1에 의해 $n \in \mathbb{N}$와 $\langle i, j \rangle$에 대해 일대일대응이 존재한다. 이 사실을 바탕으로 계산가능 함수 $\mathrm{fst}(n)$과 $\mathrm{snd}(n)$을 구성한다. 각각 n번째 쌍의 첫 번째 성분 i와 두 번째 성분 j를 반환하는 함수다. 이들 함수로 새로운 알고리즘 Π'를 다음처럼 구성한다.

> Π'는 우선 주어진 입력 $n \in \mathbb{N}$에 대해 $i = \mathrm{fst}(n)$와 $j = \mathrm{snd}(n)$를 계산한다. 그리고 $i \notin W$라면 o를 출력한다. $i \in W$라면 i를 입력으로 Π를 j번 루프한다. Π가 어떤 입력 i에 대해 어떤 출력 j로 정지하면 Π'는 $i \in W$를 출력한다.

즉 Π'는 $\mathbb{N}$를 Π의 정의역 W로 사상한다. 따라서 정의 1.3에 의해 W는 효과적으로 열거가능한 집합이다. □

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 멱집합 $\mathcal{P}$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 아니라서 효과적으로 열거불가능한 집합들이 존재하며 그렇기에 효과적으로 결정불가능한 집합들이 존재한다. □

아래 정리에는 대각화 구성을 비롯하여 지금까지 학습한 기법이 총동원된다.

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

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

(i) 효과적으로 열거가능한 집합 K는 정리 1.8에서 구성한 모든 효과적으로 열거가능한 집합들의 집합 $\mathcal{W}$상 임의의 e번째 원소 We라는 집합이다. 이 사실을 아래처럼 나타낼 수 있다.

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

여집합의 정의상 모든 e에 대해 아래가 성립한다.

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

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

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

> 주어진 입력 $n \in \mathbb{N}$에 대해 $i = \mathrm{fst}(n), j = \mathrm{snd}(n)$을 계산한다. 그리고 $i \notin K$라면 o를 출력한다. $i \in K$라면 알고리즘 Π_i를 찾아 입력 i에 대해 j번 루프한다. Π_i가 입력 i에 대해 j를 출력하며 정지하면 Π''는 i를 출력한다.

즉 Π''는 $\mathbb{N}$을 각 Π_i의 치역인 K로 사상한다. 따라서 정의 1.3에 의해 K는 효과적으로 열거가능하다. □

이 증명을 통해 정리 1.9를 강화할 수 있다.

정리 1.11. 어떤 효과적으로 열거가능한 집합은 결정가능하지 않다.

Proof. 정리 1.9와 같이 효과적으로 열거불가능한 여집합을 지니는 임의의 효과적으로 열거가능한 집합 K를 구성한다. 이에 K가 효과적으로 결정가능하다고 가정하자. 그리고 K가 효과적으로 결정가능하면 정리 1.4에 의해 그 여집합 $\overline{K}$ 또한 효과적으로 결정가능할 것이다. 하지만 그렇다면 정리 1.5에 의해 $\overline{K}$가 효과적으로 열거가능한 집합일 것이다. 이는 모순이다. 따라서 어떤 열거가능 집합은 결정불가능하다. □

1.3 공리화된 이론

효과적으로 공리화된 이론$_{\textit{effectively axiomatized theory}}$은 구문론$_{\text{syntax}}$ $\mathcal{L}$과 의미론$_{\text{semantics}}$ $\mathcal{I}$에 대해 결정가능성의 개념으로 정의된다.

정의 1.5. T는 아래를 만족하는 경우만 <u>효과적으로 공리화된 이론</u>이다.

1. T를 표현하는 형식화된 언어 $\langle \mathcal{L}, \mathcal{I} \rangle$가 존재하여 $\mathcal{L}$의 잘 형성된 형식 문장$_{\textit{well-formed formulae sentence}}$ 혹은 $\mathcal{L}$-*wffs*가 무엇인지 효과적으로 결정가능하다.

2. 어떤 $\mathcal{L}$-*wffs*가 T의 공리인지 효과적으로 결정가능하다.

3. T의 증명체계가 존재하여 $\mathcal{L}$-*wffs* 배열이 증명설계규칙을 따르는지 효과적으로 결정가능하다.

4. $\mathcal{L}$-*wffs* 배열이 T의 공리로 증명을 구성할 수 있는지 효과적으로 결정가능하다.

이제 중요한 표현들을 정의한다.

정의 1.6. 이론 T의 공리에서 <u>문장$_{\textit{sentence}}$</u> φ로의 유도가 논리적 증명체계를 사용해 주어질 때 φ를 T의 <u>정리$_{\textit{theorem}}$</u>라고 부르고 $T \vdash \varphi$라고 표기한다.

정의 1.7. 이론 T가 타당하다$_{sound}$는 필요충분조건은 T의 모든 정리가 참이라는 것이다. 타당성은 보통 참인 공리와 참을 보존하는 증명체계의 문제다.

정의 1.8. 이론 T가 효과적으로 결정가능하다는 필요충분조건은 T의 정리로 존재하는 성질이 효과적으로 결정가능한 성질이라는 것이다. 다시 말해 T의 언어로 주어진 임의의 문장 φ에 대해 $T \vdash \varphi$인지 결정하는 알고리즘이 존재한다는 것이다.

정의 1.9. 이론 T가 문장 φ를 결정한다는 필요충분조건은 $T \vdash \varphi$이거나 $T \vdash \neg\varphi$라는 것이다. 이론 T가 φ를 올바르게 결정한다는 말은 오직 φ가 참이라면 $T \vdash \varphi$이고 φ가 거짓이라면 $T \vdash \neg\varphi$라는 뜻이다.

정의 1.10. 이론 T가 부정완전$_{negation\text{-}complete}$하다는 필요충분조건은 T가 제 언어의 모든 문장 φ를 결정한다는 것이다. 다시 말해 모든 문장 φ에 대해 $T \vdash \varphi$이거나 $T \vdash \neg\varphi$라는 것이다.

정의 1.11. T가 모순적$_{inconsistent}$이라는 필요충분조건은 어떤 문장 φ가 존재하여 $T \vdash \varphi$와 $T \vdash \neg\varphi$를 모두 지닌다는 것이다.

이어 효과적인 열거가능성의 개념으로 아래처럼 정리한다.

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

1. T의 *wffs* 집합
2. T의 문장들의 집합
3. T상에서 구성가능한 증명들의 집합
4. T의 정리들의 집합

Proof. T가 효과적으로 공리화된 이론이라고 하자. 정의 1.5에 의해 T는 유한 알파벳로 구성된 형식 언어를 지닌다. 그리고 유한 알파벳상의 모든 문자열은 대각화 알고리즘을 통해 효과적으로 열거될 수 있다. 길이 1의 문자열, 길이 2의 문자열, $\cdots$ 길이 n의 문자열들에 대해 각각 알파벳 순서로 효과적으로 열거하는 알고리즘 Π_1이다. 또한 다시 정의 1.5에 의해 wffs를 효과적으로 결정할 수 있는 알고리즘 Π_2가 존재한다. 따라서 Π_1이 가능한 모든 문자열을 대각화하는 가운데 Π_2로 wffs를 효과적으로 결정하여 이들만 효과적으로 열거하는 통합적인 알고리즘 Π_3을 구성한다. 여기서 'wffs'를 '문장'으로 대체하면 1, 2의 증명이 끝난다.

T상에서 구성가능한 증명은 wffs의 배열과 같고 증명들의 집합은 wffs의 배열들의 집합과 같다. 각 배열 길이 i와 배열상의 wffs의 길이 j와 알파벳 순서로 효과적으로 열거하는 대각화 알고리즘 Π_4를 구성한다. 그리고 wffs의 배열은 무차별대입 알고리즘과 wffs 결정 알고리즘 Π_2로 구성할 수 있다. 그리하여 T상에서 구성가능한 증명들이 효과적으로 열거가능하므로 각 wffs 배열에 대해 증명설계규칙을 따르는지 효과적으로 결정가능한 알고리즘 Π_5를 구성한다. 따라서 정의 1.6에 의해 3, 4의 증명이 끝난다. □

이론의 무모순성consistency과 부정완전성은 결정가능성을 보장한다.

정리 1.13. 임의의 무모순적이고 효과적으로 공리화된 부정완전 이론 T는 효과적으로 결정가능하다.

Proof. T가 임의의 무모순적이고 효과적으로 공리화된 부정완전 이론이라고 하자. 정리 1.12에 의해 T의 정리를 효과적으로 열거하는 알고리즘 Pi_1이 존재한다. Π_1에 따라 정리들을 효과적으로 열거하는 가운데 부정완전의 정의 1.10에 의해 ϕ가 나타나면 $\neg\phi$는 정리가 아니라고 결정하고 $\neg\phi$가 나타면 ϕ는 정리가 아니라고 결정하는 알고리즘 Π_2를 구성한다. 또한 무모순의 정의 1.11의 정의에 의해 위와 같은 Π_2는 정리와 정리가 아닌 문장을 전부 분할하는 알고리즘이다. 다시 말해 T의 언어로 주어진 임의의 문장 ϕ에 대해 $T \vdash \phi$를 결정하는 알고리즘이 존재한다. 따라서 결정가능성의 정의 1.8에 의해 T는 효과적으로 결정가능하다. □

1.4 표현과 포착

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

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

$\mathcal{L}_A$의 비논리 어휘는 아래와 같다.

1. 상수 0
2. 다음 수successor 함수 S
3. 함수표현식 $+, \times$

$\mathcal{L}_A$의 항term은 '0'과 'S', '+', '×'로 만들 수 있는 변수다. 그 외 어떤 것도 항일 수 없다.

여기서 '='는 $\mathcal{L}_A$의 유일한 술어predicate다. 따라서 원자atomic wffs는 모두 임의의 항 'α', 'β'에 대해 '$\alpha = \beta$' 꼴로 서술된다. 일반적으로 wffs는 원자 wffs에 양화사와 연결사를 1차논리의 표준에 따라 사용한 것이다.

의미론 $\mathcal{I}_A$를 해석interpretation이라고 볼 수 있다. $\mathcal{I}_A$는 항에 대해 값을 배정하거나 모든 $\mathcal{L}_A$ 문장에 대해 고유한 해석을 효과적으로 배정한다. 그리하여 L_A가 효과적으로 형식화된 언어일 수 있다.

아래 정의에서 $\varphi(\overline{n})$은 $\varphi(x)$상의 'x'에 대해 수치 n을 부여한 것이다.

정의 1.12. 성질 P가 하나의 자유변수를 지닌 언어 L상의 *wff* $\varphi(x)$로 표현된다*expressed*는 필요충분조건은 모든 n에 대해 아래와 같다는 것이다.

- n이 성질 P를 지니면 $\varphi(\overline{n})$은 참이다.
- n이 성질 P를 지니지 않는다면 $\neg\varphi(\overline{n})$은 참이다.

수치함수 f는 형식 언어에 대해 아래처럼 정의된다.

정의 1.13. 수치함수 f가 언어 L상의 *wff* $\varphi(x, y)$로 표현된다는 필요충분조건은 임의의 m, n에 대해 아래와 같다는 것이다.

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

이를 간단하게 정리할 수 있다.

정리 1.14. L이 성질 P를 표현할 수 있는 필요충분조건은 L이 P의 특성함수 c_P를 표현할 수 있다는 것이다.

Proof. 아래 두 가지를 확인해야 한다.

1. $\varphi(x)$가 P를 표현하면 $(\varphi(x) \wedge y = 0) \vee (\neg\varphi(x) \wedge y = 1)$이 c_p를 표현한다.
2. $\psi(x, y)$가 c_P를 표현하면 $\psi(x, 0)$이 P를 표현한다.

우선 $\varphi(x)$가 P를 표현한다고 하자. 정의 1.12에 의해

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

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

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

따라서 정의 1.13에 의해 L은 c_P를 표현할 수 있다.

$\psi(x, y)$가 c_P를 표현한다고 하자. 정의 1.13에 의해

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

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

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

따라서 정의 1.12에 의해 L이 성질 P를 표현한다. □

다만 표현보다 중요한 것은 증명 혹은 어떤 성질의 포착$_{capture}$이다.

정의 1.14. 이론 T가 성질 P를 *wff* $\varphi(x)$로 포착하는 필요충분조건은 임의의 n에 대해 아래가 성립하는 것이다.

- n이 성질 P를 지닌다면 $T \vdash \varphi(\overline{n})$이다.
- n이 성질 P를 지니지 않는다면 $T \vdash \neg\varphi(\overline{n})$이다.

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