

자동 증명 프로그램 개발 개념 구상

한남대학교 수학과

20172581 김남훈

1. 소개

기계를 이용해 어떤 명제를 자동으로 증명한다는 구상은 매우 오래 전부터 존재했으며, 컴퓨터가 실제로 등장하기 전에 이미 연구되어 왔다. 구체적으로는 1879년 수학자 **고틀롭 프레게**가 술어 논리학을 창시했을 때부터 기계에게 명제를 증명하게 하려는 연구가 있어 왔다고 할 수 있다. 최초의 자동 증명 프로그램은 1956년 개발된 **Logic Theorist**이며, 이후 다양한 자동 증명 프로그램이 개발되었다.

2. 자동증명 프로그램의 구조

현재 다양한 종류의 자동 증명 프로그램들이 개발되어 있으며, 다양한 구조와 기술, 그리고 이론에 기반하여 증명을 수행한다. 이 섹션에서는 앞으로 개발할 자동 증명 프로그램의 구조를 간단히 설명할 것이다.

2.0. 기본 개념

$G = (V, E)$ 를 그래프라고 하자.

- $x_1, \dots, x_n \in V$ 에 대해, 모든 $i \in \{1, \dots, n-1\}$ 에 대해 $(x_i, x_{i+1}) \in E$ 이라면 (x_1, \dots, x_n) 을 G 위의 **경로**라고 한다. 이 때, x_1 을 경로의 **시작점**, x_n 을 경로의 **끝점**이라 한다.
- 모든 $x, y \in V$ 에 대해 x 를 시작점으로, y 를 끝점으로 갖는 경로가 존재한다면 G 를 **연결 그래프**라고 한다.
- G 위의 경로 X 의 시작점과 끝점이 같다면 X 를 G 위의 **회로**라 한다. G 가 회로를 갖지 않는다면 G 를 **포레스트**라고 한다. G 가 포레스트이면서 연결 그래프이면 G 를 **트리**라고 한다.
- 트리의 한 정점 r 을 **루트(root)**로 정의한다면 이 트리를 **루트를 갖는 트리**라고 한다. 모든 정점은 루트가 될 수 있다.
- r 을 시작점으로, 한 정점 y 를 끝점으로 갖는 경로는 트리의 성질에 의해 유일한데, y 의 바로 이전에 오는 정점을 x 라 하면 x 를 y 의 **부모**라 한다. 반대로 y 는 x 의 **자녀**라 한다.
- 자녀를 갖지 않는 정점을 **리프**라 한다. 루트를 제외한 모든 정점은 유일한 부모를 가지며 루트는 부모를 갖지 않는다.

2.1. 명제를 트리로 변환하는 방법

$x + y = zw$ 라는 명제는, $x + y$ 와 zw 가 같으면 참을, 다르면 거짓을 반환하는 함수로 볼 수 있다. 마찬가지로 $+$ 라는 기호는 양 쪽의 변수를 받아 두 변수의 합을 반환하는 함수로 볼 수 있다.

$$\text{plus}(a, b) = a + b$$

$$\text{mul}(a, b) = ab$$

$$\text{equal}(a, b) = \begin{cases} \text{true} & \text{if } a = b \\ \text{false} & \text{if } a \neq b \end{cases}$$

로 놓으면, 위의 등식, 다시 말해 함수는 다음과 같은 형태로 다시 작성할 수 있다.

$$\text{equal}(\text{plus}(x, y), \text{mul}(z, w))$$

이 때, 가장 바깥쪽에 있는 함수를 트리의 루트로 놓고 각 정점이 나타내는 함수의 입력들을 정점의 자녀로 놓으면 위 함수는 다시 다음과 같이 나타낼 수 있다.

