Goodstein's theorem

전한울
hanuljeon95@gmail.com

2021년 4월 25일

요 약

이 글에서는 참이지만 페아노 산술 위에서 증명 불가능한 명제의 대표적인 예시인 굿스타인 정리를 알아볼 것이다. 굿스타인 정리를 알기 위한 개념들을 소개한 후 굿스타인 정리를 증명할 것이며, 왜 굿스타인 정리가 증명 불가능한지 또한 설명할 것이다. 마지막으로, 굿스타인 정리의 독립성과 연관이 있는 겐첸의 산술의 무모순성 증명에 대해서 간략하게 소개할 것이다.

1 Preliminaries

굿스타인 정리는 굿스타인이 1944년에 [2] 처음 제시한 명제이다. 굿스타인은 이 명제를 제시했을 때부터 주어진 명제가 페아노 산술과 독립일 것이라 추정했지만, 이의 증명은 38년 뒤에서야 Kirby와 Paris에 의해 처음 이루어졌다. [4] 이 글에서는 굿스타인 정리의 증명과 이의 독립성 증명을 알아볼 것이다. 굿스타인 정리를 알아보기 전에 필요한 사전지식에 대해 알아보도록 하자.

Acknowledgment

이 글은 2016년 10월 29일에 있었던 '멍청한 세미나'라는 학부생 발표를 위해 작성되었던 원고를 수정한 것이다. 당시 발표에 참여했던 분들, 그리고 세미나 운영과 원고 출판에 큰 역할을 한 권현우 씨에게 감사의 말씀을 드린다.

1.1 Ordinal number

집합론을 배우면서 서수를 이미 배웠지만 잘 기억이 안 나거나 서수를 배운 적이 없는 독자를 위하여 서수에 대해 설명할 필요가 있어 보인다. 여기선 서수의 엄밀한 정의가 필요하지 않다. 다만 서수가 무엇이며 어떻게 다루는 지만 알면 충분하다. 이 문단에서 나오는 정리들의 증명은 다루지 않는다. 증명이 궁금한 독자는 [5]를 확인하길 바란다.

기수가 집합의 크기를 대표하는 수라면 서수는 정렬집합의 순서형을 대표하는 수이다. 여기서 정렬집합은 임의의 부분집합이 항상 최소원을 가지는 수를 말하며, 좀 더 직관적인 언어로 서술해보자면 사람을 한 명 세워두고 그 뒤로 계속 사람을 이어 붙였을 때 나올 수 있는 줄의 모양을 가리킨다. 우선 유한한 수의 사람을 줄세운다면

$$0 < 1 < 2 < \cdots < n-1$$

과 같이 생겼을 것이고 이 순서형을 n이라고 부를 것이다. 그리고 아무도 없는 줄을 0이라고 쓸 것이다.

하지만 수학에서 나오는 대상이 모두 유한하지만은 않다. 이제 무한히 긴 줄을 상상해보자. 유한한 줄 뒤에 사람을 끝없이 붙인다면 나오는 줄은 일단 이렇게 생겼을 것이다:

$$0 < 1 < 2 < 3 < \cdots < n < n+1 < \cdots$$

이는 우리들이 잘 아는 자연수의 순서집합 $(\mathbb{N}, <)$과 똑같다. 그리고 우리는 위 순서형을 ω라 부를 것이다. 하지만 여기서 끝이 아니다. 저 끝이 없어 보이는 줄 뒤에도 사람이 더 설 수 있다. 이제 저 줄 뒤에다 사람을 한 명 더 붙여보자:

$$0 < 1 < 2 < 3 < \cdots < n < n+1 < \cdots < \omega$$

이 줄은 ω와는 판이하게 다르게 생겼다. 왜냐면 ω에는 마지막에 선 사람이 없다. (좀 더 엄밀하게 말하자면, 최대원이 없다.) 하지만 새로 생긴 줄은 그렇지 않다. 우리는 이렇게 생긴 줄을 $\omega+1$이라 부를 것이다. 마찬가지로 뒤에 사람을 계속 붙여서 $\omega+2$, $\omega+3$ 그리고 $\omega+n$ 같은 것을 만들 수 있을 것이다. 물론 ω라는 줄 뒤에도 무한히 많은 사람을 붙일 수 있다. 이 줄은 이렇게 생겼을 것이다:

$$0 < 1 < 2 < \cdots < \omega < \omega+1 < \omega+2 < \cdots$$

이를 $\omega+\omega$, 혹은 $\omega \cdot 2$라고 부를 것이다. 그리고 $\omega \cdot 2$에다 ω같이 생긴 줄을 계속 붙이다 보면 $\omega \cdot 3$, $\omega \cdot 4$같은 것을 얻을 수 있을 것이고 마침내 $\omega \cdot \omega$, 혹은 ω^2을 얻을 수 있을 것이다. ω^2을 그림으로 나타내보면 다음과 같다:

지금까지 본 서수들을 순서대로 나열해보자:

$$0, 1, 2, 3, \cdots, \omega, \omega+1, \omega+2, \cdots, \omega \cdot 2, \cdots, \omega \cdot 3, \cdots\cdots, \omega^2$$

여기서 ω, $\omega\cdot 2$ 같은 서수들은 꼭 $\cdots$ 뒤에 나옴을 알 수 있다. 반면 $\omega+1$이나 3, $\omega\cdot 2+3$의 경우 그 앞에 그보다 작은 서수가 있다. 어떤 서수 바로 앞에 자신보다 더 작은 서수가 있으면 이를 따름서수*(successor ordinal)*라 부르고, 그렇지 않은 서수를 극한서수*(limit ordinal)*라 부른다. 특히, 따름서수는 모두 $\alpha+1$꼴이다.

이제 다시 딱딱한 이야기로 돌아가보자. 앞 문단에서 서수가 모든 정렬집합의 순서형을 대표한다고 했다. 이 사실을 좀 더 엄밀하게 쓰면 다음과 같다:

Theorem 1.1. 임의의 정렬집합 $(X,\prec)$에 대해 어떤 서수 α가 있어

$$(X,\prec)\cong\{\xi:\xi<\alpha\}$$

이다. 즉, 임의의 정렬집합은 적당한 서수들의 집합과 순서동형이다.

특히나 위 정리에서 나오는, 특정 서수보다 작은 모든 서수들의 집합을 initial section이라 부른다. 위 정리를 다시 말하면, 임의의 정렬 순서가 어떤 initial section과 동형이란 것이다.

그런데 우리는 서수가 뭔지 잘 정의한 적이 없다. 서수가 정렬집합을 대표한단 사실을 이용해서, 동형인 정렬집합들을 동치류로 분류한 다음 하나씩 뽑아오는 방법을 생각할 수도 있다. 하지만 우리는 그 방법 대신 좀 생소해 보이는 정의를 도입할 것이다. 위의 예시에도 드러나있듯, 순서형 n은 n보다 작은 모든 자연수를 모은 것과 같다. 이러한 사실은 위에서 예시로 든 무한서수에 대해서도 통용되었다: 가령, ω는 ω보다 작은 모든 서수를 모아놓은 것이고, $\omega+1$은 $\omega+1$보다 작은 모든 서수를 모아놓은 것이다. 따라서 만약 $\alpha<\beta$라면 α는 β라는 순서형 안에 들어간다. 즉, $\alpha\in\beta$이다. 즉, $\in$을 마치 서수들에 대한 순서처럼 쓸 수 있단 것이다. 게다가, $\in$이 서수들에 대한 순서이므로 $\alpha\in\beta$이고 $\beta\in\gamma$라면 $\alpha\in\gamma$일 것이다. 즉, $\beta\in\gamma$이면 $\beta\subseteq\gamma$라는 것이다. 우리는 이 성질들을 서수의 정의로 삼을 것이다:

Definition 1.2. 집합 α가 서수(*ordinal number*)라는 것은

(1) $\beta\in\alpha$이면 $\beta\subseteq\alpha$이고

(2) $(\alpha,\in)$이 정렬순서집합이란 것이다.

참고로 Theorem 1.1은 위 정의대로 정의된 서수에 대해서 성립한다. 다만 이 글에서 위의 정의를 쓸 일은 많지 않다. 위 정의가 이해가 안 된다면 신경쓰지 않아도 무리는 없을 것이다.

서수의 제일 중요한 특징은 서수에 대한 귀납법이나 재귀적 정의가 가능하다는 것이다. 그리고 서수에 대한 귀납법을 초한귀납법(*transfinite induction*), 서수에 대한 재귀를 초한재귀(*transfinite recursion*)라 부른다.

Theorem 1.3 (Transfinite induction). 모든 서수들의 모임 Ord과 그 부분 모임 $C \subseteq \mathrm{Ord}$에 대해

(1) $0 \in C$이고

(2) $\alpha \in C$일 때 $\alpha + 1 \in C$이며

(3) 극한서수 λ에 대해 $\alpha < \lambda$인 모든 α에 대해 $\alpha \in C$일 때 $\lambda \in C$이면

$C = \mathrm{Ord}$이다.

Theorem 1.4 (Transfinite recursion). 모든 집합들의 모임 V에 대해 정의되는 함수 $F : V \to V$에 대해 유일한 $G : \mathrm{Ord} \to V$가 있어 $G(\alpha) = F(F \restriction \alpha)$이다.

여기서 $F \restriction \alpha = \{(\beta, F(\beta)) : \beta < \alpha\}$이다. 즉, $F(F \restriction \alpha)$는 $\beta < \alpha$와 그 함수값 $F(\beta)$를 매개변수로 정의되는 함수와 같다.

1.2 Ordinal arithmetic

앞에서 서수에 대해 덧셈이나 곱셈을 별 언급도 없이 사용했다. 이 문단에선 서수의 덧셈, 곱셈, 지수 연산을 정의할 것이다. 또한 엡실론 수라고 부르는 특정한 종류의 서수도 정의할 것이다.

서수의 덧셈은 두 서수를 '이어붙인' 서수의 순서형으로 주어진다. 좀 더 엄밀하게 말하자면, 서수의 덧셈 $\alpha + \beta$는 집합 $\alpha \sqcup \beta = \alpha \times \{0\} \cup \beta \times \{1\}$ 위의 순서

$$(\xi, i) \prec (\eta, j) \iff i < j \text{ or } (i = j \text{ and } \xi < \eta)$$

로 주어지는 순서집합 $(\alpha \sqcup \beta, \prec)$과 순서동형인 유일한 서수로 정의된다. 덧붙이자면, $\prec$는 $\alpha \sqcup \beta$ 위의 정렬순서이다.

덧셈을 초한 재귀를 써서 다음과 같이 정의할 수도 있다:

- $\alpha + 0 = \alpha$
- $\alpha + (\beta + 1) = (\alpha + \beta) + 1$
- 극한서수 λ에 대해 $\alpha + \lambda = \sup_{\gamma < \lambda}(\alpha + \gamma)$

여기서 $S(\alpha) = \alpha + 1 := \alpha \cup \{\alpha\}$은 어떤 서수 바로 다음에 나타나는 서수이다.

이제 덧셈을 정의했으니 곱셈을 정의할 차례이다. 곱셈은 두 서수의 곱집합을 사전식으로 나열한 것의 순서형으로 주어진다. 물론 그게 정렬집합임을 확인해야겠지만, 운 좋게도 정렬집합이다.

또한 곱셈도 재귀적인 정의가 가능하다:

- $\alpha \cdot 0 = 0$
- $\alpha \cdot (\beta + 1) = \alpha \cdot \beta + \alpha$
- 극한서수 λ에 대해 $\alpha \cdot \lambda = \sup_{\gamma<\lambda}(\alpha \cdot \gamma)$

곱셈도 있으니 지수 연산도 정의될 것이다. 지수 연산은 그냥 재귀적으로 다음과 같이 정의하자:

- $\alpha^0 = 1$
- $\alpha^{\beta+1} = \alpha^\beta \cdot \alpha$
- 극한서수 λ에 대해 $\alpha^\lambda = \sup_{\gamma<\lambda} \alpha^\gamma$

지수 연산에 대응되는 순서집합은 좀 많이 복잡하다. 이는 [5]을 참고하길 바란다.

이제 연산들이 만족하는 성질을 알아보자. 우리들이 아는 자연수의 연산의 성질을 어느 정도까진 만족한다.

Proposition 1.5. 서수 α, β, γ에 대해 다음이 성립한다.

(1) $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$

(2) $\alpha + \beta = \alpha + \gamma$이면 $\beta = \gamma$이다.[1)]

(3) $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$

(4) $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$

(5) $\alpha \geq 1$이고 $\alpha \cdot \beta = \alpha \cdot \gamma$이면 $\beta = \gamma$이다. [1)]

(6) $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$

(7) $\alpha \geq 2$이고 $\alpha^\beta = \alpha^\gamma$이면 $\beta = \gamma$이다.

(8) $\alpha^{\beta+\gamma} = \alpha^\beta \alpha^\gamma$

(9) $\alpha^{\beta\gamma} = (\alpha^\beta)^\gamma$

(10) $\gamma \leq \alpha$일 때 어떤 $\rho < \beta$와 δ가 있어 $\alpha = \gamma\delta + \rho$이다.

골때리게도 덧셈과 곱셈의 교환법칙은 일반적으로 성립하지 않는다. 가령 $1 + \omega = \omega \neq \omega + 1$이고 $2 \cdot \omega = \omega \neq \omega \cdot 2$이다. 또한, 여기서 적혀 있지 않는 우분배법칙 또한 성립하지 않는다.

서수 ω^2은 덧셈에 대해 닫혀 있다. 즉, $\alpha, \beta < \omega^2$이면 $\alpha + \beta < \omega^2$이다. 그리고 ω^ω는 덧셈과 곱셈에 대해 닫혀 있다. 그러면 덧셈, 곱셈과 지수 연산에 대해

1) 여기서 $=$를 $<$로 바꿔도 성립한다.

모두 닫혀 있는 서수도 있을까? 그러한 서수를 엡실론 수라고 부르며, 다음과 같이 정의한다:

Definition 1.6. 엡실론 수는 $\omega^\varepsilon = \varepsilon$을 만족하는 ε을 가리킨다. 특히 엡실론 수 중 제일 작은 것을 ε_0이라 나타낸다.

제일 작은 엡실론 수 ε_0은 다음과 같이 구성할 수 있다: $\alpha_0 = 1$, $\alpha_{n+1} = \omega^{\alpha_n}$으로 두면 $\alpha = \sup_{n<\omega} \alpha_n$로 두자. 그러면 $\alpha = \omega^\alpha$임을 확인할 수 있다. 따라서 α는 엡실론 수이다. 그리고 만약 $\xi < \alpha$이면 어떤 n이 있어 $\alpha_n \leq \xi < \alpha_{n+1}$이고 따라서 $\alpha_{n+1} \leq \omega^\xi$이다. 즉, $\xi < \omega^\xi$이다. 따라서 α는 제일 작은 엡실론 수이다.

이 글에서 중요한 역할을 하는 서수의 성질 중 하나는 서수를 마치 ω진법 전개를 하듯 나타낼 수 있다는 것이다. 그리고 그 표현은 다른 진법 전개와 마찬가지로 유일하다:

Theorem 1.7. 임의의 서수 α에 대해 어떤 서수들의 유한열 $\gamma_0 > \gamma_1 > \cdots > \gamma_k$와 자연수열 $n_0, \cdots, n_k$가 있어

$$\alpha = \omega^{\gamma_0} \cdot n_0 + \cdots + \omega^{\gamma_k} \cdot n_k$$

이다. 또한 이런 전개는 유일하며, 이를 α의 칸토어 표준형*(Cantor normal form)*이라고 한다.

특히, $\alpha < \varepsilon_0$이면 α의 칸토어 표준형에 나타나는 모든 지수의 크기가 α보다 작아야 한다.[2] 주어진 $\alpha < \varepsilon_0$의 칸토어 표준형에서 나타나는 (원래 수보다 작은) 지수까지 모두 칸토어 전개하면 그 서수를 자연수와 곱셈, 지수 연산, 자연수와 ω만을 써서 나타낼 수 있는데 이를 완전 칸토어 표준형(*complete Cantor normal form*)이라 부른다.

1.3 Computable and Primitive recursive functions

우리들이 주로 보는 자연수에 대한 함수들은 대개 기계적으로 계산이 가능하다. 달리 표현하자면, 주어진 함수를 컴퓨터를 써서 계산하는 프로그램을 짤 수 있다. 만약 어떤 함수 $f : \mathbb{N} \to \mathbb{N}$을 계산하는 프로그램을 짤 수 있다면 우리는 f를 계산가능하다고 할 것이다. 이의 엄밀한 정의는 후술하기로 한다.

하지만 우리들이 일상적으로 보는 함수들은 그냥 계산가능할 뿐 아니라 원시 재귀 함수(*Primitive recursive function*)이기까지 하다. 프로그래머들의 언어를 약간 빌리자면, 원시 재귀 함수는 기본적인 사칙연산과 조건문, 유한한 단계 안에 끝나는 루프문으로 짤 수 있는 함수이다.

2) 그러지 않은 수는 엡실론 수이다. 엡실론 수의 경우 칸토어 표현의 지수와 원래 수 크기가 같을 수 있다. 가령, ε_0의 칸토어 표준형은 ω^{ε_0}이다.

Definition 1.8 (Primitive Recursive Function, Computable function)**.** 원시 재귀함수들의 집합은 다음에 대해 닫혀 있는 집합 중 제일 작은 집합이다.

(1) $n \geq 0$에 대해 상수함수 $c : \mathbb{N}^n \to \mathbb{N}$와 후자 함수 S는 원시 재귀이다.

(2) Projection $P_k : \mathbb{N}^n \to \mathbb{N}$, $P_k(x_0, \cdots, x_{n-1}) = x_k$는 원시 재귀이다.

(3) 두 원시 재귀 함수의 합성도 원시 재귀이다: $f : \mathbb{N}^k \to \mathbb{N}$, $g_1, \cdots, g_k : \mathbb{N}^m \to \mathbb{N}$이 원시 재귀 함수일 때 $h(x) = f(g_1(x), \cdots, g_k(x))$도 원시 재귀이다.

(4) (원시 재귀) k자리 함수 $f : \mathbb{N}^k \to \mathbb{N}$과 $k+2$자리 함수 g에 대해 다음과 같이 정의되는 함수 h도 원시 재귀이다:

- $h(0, x_1, \cdots, x_k) = f(x_1, \cdots, x_k)$
- $h(S(y), x_1, \cdots, x_k) = g(y, h(y, x_1, \cdots, x_k), x_1, \cdots, x_k)$

그리고 아래 연산에 대해서도 닫혀 있는 최소의 집합족을 계산가능한 함수들의 족이라 부를 것이다:

(5) (μ-재귀) 함수 h에 대해 $\mu(h)(a_1, \cdots, a_k) = b$라는 것은 b가 $h(b, a_1, \cdots, a_k) = 0$을 만족하는 최소의 자연수인 것이다.

μ-재귀 정의에서 알 수 있듯, $\mu(h)(a_1, \cdots, a_k)$가 항상 잘 정의된단 보장이 없다. 이 경우엔 $\mu(h)(a_1, \cdots, a_k)$의 값을 정의하지 않는다. 즉, $(a_1, \cdots a_k) \notin \operatorname{dom} \mu(h)$이다. 튜링 머신을 써서 계산가능성을 정의하지 않은 것에 실망한 독자는 [10]같은 적당한 computability theory 교재를 참고하길 바란다.

함수 외에도 $\mathbb{N}$의 부분집합에 대해서도 계산가능성을 논할 수 있다. $A \subseteq \mathbb{N}$이 계산가능하단 것은 그 소속함수 χ_A가 계산가능하단 것이다. 달리 말하면, 어떤 자연수가 주어졌을 때 그 자연수가 A에 속하는지 그렇지 않은지 판정하는 알고리즘이 존재한단 것이다.

이 글에서 계산가능성의 구체적인 정의를 써서 무언가를 증명하는 일은 없을 것이다. 대신 어떤 함수가 주어졌을 때 그 함수를 계산하는 알고리즘을 스케치하는 정도로만 언급할 것이다.

1.4 Peano and Primitive Recursive Arithmetic

페아노 산술은 주세페 페아노(Giuseppe Peano)가 산술의 엄밀한 기초가 없음을 깨닫고 도입한 체계이다. 여기서 산술이라 함은 자연수에 관한 이론을 가리킨다. 정의를 하기 이전에 실해석학 시간 때 실수 체계를 어떻게 공리적으로 정의했는지 떠올려보자. 0과 1, 덧셈, 곱셈, 순서 관계 $\leq$로 시작해서 이들에 대한 공리와

완비성 공리를 준다. 이 때 각 공리는 우리들이 받아들일 수 있는 교환법칙, 결합법칙 같은 것들로 이루어져 있다.

페아노 산술 역시 실수의 공리적 정의와 크게 다르지 않게 정의된다. 페아노 공리계는 0과 '후자 함수' S, 덧셈과 곱셈, 순서 기호로 이루어져 있다. 여기서 후자 함수 (Successor function)은 어떤 수 '다음 수'를 가리키는 함수이다. 즉 $S(n) = n + 1$이다.

Definition 1.9 (Peano Arithmetic, PA)**.** 페아노 산술은 다음과 같은 공리로 이루어져 있다:

S1. $\forall x : S(x) \neq 0$

S2. $\forall x : x = 0 \vee (\exists y : S(y) = x)$

S3. $\forall x \forall y : S(x) = S(y) \to x = y$

A1. $\forall x : x + 0 = 0$

A2. $\forall x \forall y : x + S(y) = S(x + y)$

M1. $\forall x : x \cdot 0 = 0$

M2. $\forall x \forall y : x \cdot S(y) = x \cdot y + x$

O1. $\forall x \forall y x \leq y \leftrightarrow \exists z : y = x + z$

Ind. 성질 P에 대해 $P(0)$이고 $\forall n : P(n) \to P(S(n))$이면 모든 자연수 n에 대해 $P(n)$이 성립한다.

여기서 Ind.에서 등장하는 '성질'이란 단어가 모호하단 느낌을 받을 것이다. 여기서 성질은 특정한 자연수를 모아놓은 집합 중 묘사할 수 있는 것이다. 우리들은 $P(n)$을 n을 자유변수로 갖는 논리식으로 생각할 것이다.

페아노 산술에서 제일 핵심적인 공리는 귀납법 공리이다. 귀납법 공리는 가령 지수 연산이나 팩토리얼같이 재귀적으로 정의되는 함수를 정의할 수 있게끔 해 주고, 산술의 많은 정리를 이끌어낸다. 하지만 많은 경우 귀납법 전체가 필요하지 않다. 귀납법을 약화시킨 정도로 충분할 때도 있다. 하지만 귀납법 공리가 우리들이 아는 함수들을 정의하는 데 필요하단 것에 유의하자. 따라서 귀납법을 약화시킨 체계는 우리들이 원하는 함수를 모두 포함하고 있어야 한다. 여기서는 우리들이 원하는 함수를 원시 재귀 함수로 두자.

Definition 1.10 (Primitive Recursive Arithmetic, PRA)**.** PRA는 PA에서 각 원시 재귀 함수 h에 대응하는 함수 기호를 추가한 뒤 그 함수들의 정리를 공리로 둔 다음 PA에서 Ind.을 다음과 같이 약화시킨 공리

$\phi(x)$가 *bounded quantifier*[3]만을 quantifier로 가지는 논리식일 때 $\phi(0)$이고 $\forall n : \phi(n) \to \phi(n+1)$이면 $\forall n \phi(n)$이다.

로 대체한 체계이다.

2 Goodstein's theorem

이제 굿스타인 정리가 뭔지 알아보자. 알아보기 이전에 한 가지 정의할 것이 있다:

Definition 2.1 (b진법 전개)**.** 자연수 m에 대해, m의 초b진법 전개는 m의 b진법 전개에서 나타나는 b 위의 지수를 모두 b진법 전개한 것이다.

가령, 25252의 초3진법 전개는

$$1 \cdot 3^{3^2} + 2 \cdot 3^{2 \cdot 3+1} + 1 \cdot 3^{2 \cdot 3} + 1 \cdot 3^{1 \cdot 3+2} + 2 \cdot 3^{1 \cdot 3+1} + 2 \cdot 3^3 + 2 \cdot 3^1 + 1$$

이다. 그리고 $3^{3^{3^{11}}}$의 초3진법 전개는 $3^{3^{3^{3^2+2}}}$이다.

굿스타인 정리의 주인공은 다음과 같이 정의되는 굿스타인 수열이다:

Definition 2.2. 굿스타인 수열 $G(k) = \langle a_n \rangle_{n \geq 2}$은 다음과 같이 정의되는 수열이다:

1. $a_2 = k$이다.
2. a_{n+1}은 a_n의 초n진법 전개에서 모든 n을 $n+1$로 바꾸고 거기서 1을 뺀 것이다.

가령, $a_2 = 4 = 2^2$일 때 $a_3 = 3^3 - 1 = 2 \cdot 3^2 + 2 \cdot 3 + 2$이다. 그리고 $a_4 = 2 \cdot 4^2 + 2 \cdot 4^1 + 1$이다. $G(4)$는 마치 계속 증가할 것만 같다. 심지어 초기값이 조금만 더 커져도 수열은 괴랄한 값을 보인다. 가령, $a_2 = 19$인 경우 $a_5 \approx 1.8 \times 10^{2184}$이고 $a_6 \approx 2.6 \times 10^{36305}$이다. 따라서 $G(k)$는 마치 무한대로 발산할 것처럼 보인다. 하지만

Theorem 2.3 (Goodstein). 임의의 굿스타인 수열 $G(k)$는 궁극적으로 0이 된다.

굿스타인 정리의 증명은 뜬금없게도 서수를 사용한다. 한 번 확인해보자:

Proof. 증명의 편의를 위해 함수를 몇 개 정의할 것이다. 자연수 $n > 0$과 $2 \leq b \leq c$에 대해 $S_c^b(m)$을 m의 초b진법 전개에서 나오는 b를 모두 c로 바꾼 것이라 하자. 그리고 $S_\omega^b(m)$을 m의 초b진법 전개에서

3) $\forall x < t$꼴이나 $\exists x < t$꼴로 이뤄진 한량사

1. 밑을 계수 앞으로 빼고 (즉, $a_k \cdot n^{e_k}$을 $n^{e_k} \cdot a_k$로 바꾸고)

2. b를 모두 ω로 바꾼 것

이라 하자. 가령

$$S^3_\omega(3^{2\cdot 3^3} + 2 \cdot 3^3 + 2) = \omega^{\omega^\omega \cdot 2} + \omega^\omega \cdot 2 + 2$$

이다. 위 정의를 좀 더 엄밀하게 쓰면 다음과 같은 귀납적인 정의가 나타날 것이다. $2 \le b < c \le \omega$에 대해

1. $S^b_c(a) = a$ for $0 \le a < b$

2. $S^b_c(b^{e_0} \cdot a_0 + \cdots + b^{e_k} \cdot a_k) = c^{S^b_c(e_0)} \cdot a_0 + \cdots + c^{S^b_c(e_k)} \cdot a_0$ for $e_0 > \cdots > e_k$ and $0 \le a_i < b$ for $i = 0, 1, \cdots k$.

그리고 완전 칸토어 표준형에서 나타나는 정수가 모두 b 이하인 α에 대해 $T^\omega_b(\alpha)$를 그 표현에서 나타나는 모든 ω를 b로 바꾼 것이라 하자. 가령

$$T^\omega_4(\omega^\omega + \omega^2 \cdot 2) = 4^4 + 4^2 \cdot 2 = 72$$

이다. 좀 더 엄밀하게 써 보자면 다음과 같다: 우선 α의 칸토어 표현형에서 나타나는 '제일 큰 정수' $C(\alpha)$를 다음과 같이 귀납적으로 정의하자:

1. $C(n) = n$ for $n < \omega$

2. $C(\omega^{\alpha_0} \cdot n_0 + \cdots + \omega^{\alpha_k} \cdot n_k) = \max\{C(\alpha_0), \cdots, C(\alpha_k), n_0, \cdots, n_k\}$

그리고 $C(\alpha) < b$인 α에 대해 $T^\omega_b(\alpha)$를 S^a_b와 비슷하게 정의한다. 그 detail은 생략하겠다. 그러면 다음 사실을 증명할 수 있다:

Lemma 2.4. $2 \le b \le c \le \omega$, $C(\alpha), C(\beta) < b$라 하자. 이 때

1. $T^\omega_b(S^b_\omega(m)) = m$

2. $S^b_\omega(T^\omega_b(\alpha)) = \alpha$

3. $m < n$이면 $S^b_c(m) < S^b_c(n)$이다.

4. $\alpha < \beta$이면 $T^\omega_b(\alpha) < T^\omega_b(\beta)$이다.

위에서 뒤 두 사실의 증명은 약간 tricky하다. 이의 증명은 두 b진법 전개와 칸토어 표준형의 크기 비교가 사전식 배열의 크기 비교같이 행동한단 데서 따라 나온다.

이제 굿스타인 수열을 저 함수를 써서 정의해보자. 굿스타인 수열 $G(k) = \langle a_n \rangle_{n\geq 2}$을 $a_2 = k$,

$$a_{n+1} = \max(S^n_{n+1}(a_n) - 1, 0)$$

으로 정의하자. 그리고 그에 대응하는 서수열 $\langle \alpha_n \rangle_{n\geq 2}$를 $\alpha_k = S^n_\omega(a_k)$로 정의하자. 만약 $a_n > 0$이라면

$$\alpha_n = S^n_\omega(a_n) = S^{n+1}_\omega(S^n_{n+1}(a_n)) = S^{n+1}_\omega(a_{n+1} + 1) > \alpha_{n+1}$$

이다. 따라서 a_n은 계속 0보다 클 수 없다. 즉, $a_n = 0$인 n이 존재한다. □

3 Independence of Goodstein's theorem

굿스타인 정리는 서문에서 밝혔듯 PA에서 증명 불가능하다. 그러면 왜 증명 불가능한가? 이 문단에선 그 이유를 알아보고자 한다. 하지만 그 이전에 굿스타인 정리를 페아노 산술의 명제로써 서술할 수 있을까를 물어야 할 것이다. 다행히도 답은 '예'이다. 수열의 재귀적인 정의나 초b진법 전개라는 개념 자체가 산술에서 정의 가능하다. 재귀적인 정의는 귀납법 덕에 가능하고, 숫자들의 나열을 요구하는 초b진법 전개의 경우 자연수로 자연수들의 유한 길이 순서쌍을 'code할 수 있기' 때문에 가능하다.

그러면 굿스타인 정리의 증명을 페아노 산술에다 집어넣을 수 있을까? 서수가 등장하므로 거기서부터 문제가 발생할 것 같지만 마냥 그렇지는 않다. 왜냐면 '크지 않은' 서수는 산술 안에다 집어넣을 수 있기 때문이다. 다음 소문단에서 어떻게 서수를 산술에다 집어넣는지 설명할 것이다. 증명을 집어넣는 과정에서 문제는 서수를 집어넣은 후에 그게 진짜 서수임을 확인하는 과정에서 생긴다.

3.1 How to code ordinals by naturals

이 문단에선 서수를 자연수로 code하는 방법을 설명할 것이다. 제일 엉성한 방법은 이럴 것이다: 만약 α가 가산 서수라면 어떤 전단사 $f : \alpha \to \mathbb{N}$이 있을 것이다. α의 ordering을 집어넣기 위해서, $\mathbb{N}$의 부분집합을 다음과 같이 정의한다:

$$P = \{2^a 3^b : f^{-1}(a) < f^{-1}(b)\}$$

그러면 $P \subseteq \mathbb{N}$은 α의 원소가 어떻게 나열되었는지 정보를 담고 있으므로, P를 안다면 α를 복구할 수 있다.

이 방법은 한 가지 결점을 지니고 있다. 저기서 f가 어떤 함수인 지 알 수 없다는 것이다. 따라서 P의 정체도 불분명하다. 좀 더 엄밀하게 말하자면, 짝수의 집합과는 달리 P를 산술 안에서 정의할 수 있단 보장이 없다. 특히, $n \in P$인지

판정하는 컴퓨터 프로그램이 존재한단 보장을 할 수 없다. 하지만 우리들이 집합의 내부가 어떻게 생겼는지 구체적으로 알 수 있는 부류의 집합은 computable 한 것뿐이다.[4] 따라서 우리들은 서수를 *computable*하게 code해야 한다.

다행히도, 우리들은 ε_0 미만의 서수에 대해서만 신경쓰면 된다. 게다가, ε_0보다 작은 모든 서수는 완전 칸토어 표현을 가진다. 우리는 완전 칸토어 표현을 이용해서 서수를 집어넣을 것이다. 개략적인 아이디어는 완전 칸토어 표현을 마치 꼭짓점에 자연수를 달고 있는 유한 트리처럼 생각하는 것이다.

본격적인 정의를 하기 전에 함수 하나를 정의하고 가자.

$$\langle a_0, \cdots, a_\ell \rangle := 2^\ell 3^{a_0} \cdots p_{\ell+1}^{a_\ell}$$

은 자연수 순서쌍을 하나의 자연수로 code하는 함수이다. 이 함수는 computable 하고 모든 유한 길이 자연수 순서쌍들의 집합 $\mathbb{N}^{<\omega}$에서 $\mathbb{N}$으로 가는 단사함수이다.

Definition 3.1. 서수 $\alpha < \varepsilon_0$과 그 칸토어 표현 $\alpha = \omega^{\alpha_0} + \omega^{\alpha_1} + \cdots + \omega^{\alpha_n}$, $\alpha_0 \geq \alpha_1 \geq \cdots \geq \alpha_n$에 대해 재귀적으로

$$\nu(\alpha) = \langle \nu(\alpha_0), \cdots, \nu(\alpha_n) \rangle$$

으로 정의한다. 그리고 $\nu(0) = \langle\rangle$로 준다.

가령 자연수 k는 $\langle \underbrace{\langle\rangle, \cdots, \langle\rangle}_{k \text{ times}} \rangle$와 "같이 주어진다. 그리고 이렇게 정의된 표현은 다음과 같은 좋은 성질들을 가진다.

Theorem 3.2. ν는 다음과 같은 성질을 만족한다*:*

1. 임의의 서수 $\alpha < \varepsilon_0$은 유일한 표현을 가진다*.*
2. 서수 표현들의 집합 $\{\nu(\alpha) : \alpha < \varepsilon_0\}$은 *computable*하다*.*
3. 서수 간의 순서를 *code*한 집합 $R = \{\langle \nu(\alpha), \nu(\beta) \rangle : \alpha \leq \beta < \varepsilon_0\}$ 또한 *computable*하다*.*

Proof. 1을 보이기 위해서 ν가 잘 정의되고 단사임을 확인해야 한다. 이는 ε_0 미만의 서수가 유일한 완전 칸토어 표현을 가진단 것과 귀납법을 써서 확인할 수 있다.

2와 3은 동시에 귀납적으로 증명할 것이다. $A_0 = \{\langle\rangle\}$, $R_0 = A_0 \times A_0$으로 두고 다음과 같이 정의하자:

4) computable하지 않은 집합의 예시로 ZF에서 증명 불가능한 명제들의 집합이 있다. 이 경우 심지어 어떤 명제들이 주어진 집합에 속하느냐 마느냐가 large cardinal의 존재성에 달려 있다! 즉, 산술만으로는 주어진 집합의 원소를 완벽히 파악할 수 없다.

- $x \in A_{n+1}$ iff $x = \langle y_0, \cdots, y_r \rangle$ for some $y_0, \cdots, y_r \in A_n$ such that $(y_i, y_{i+1}) \in R_n$ for all $i = 0, 1, \cdots, r-1$.
- $(x, y) \in R_{n+1}$ iff $x, y \in A_{n+1}$ and if $x = \langle a_0, \cdots, a_r \rangle$, $y = \langle b_0, \cdots, b_s \rangle$ then either $r < s$ or ($r = s$ and the least i s.t. $a_i \neq b_i$ satisfies $(a_i, b_i) \in R_n$).[5)]

그리고 $A = \bigcup_n A_n$, $R = \bigcup_n R_n$으로 두자. 이 때 다음을 보일 것이다:

- $\nu(\alpha) \in A$.
- $\alpha \leq \beta$ iff $(\nu(\alpha), \nu(\beta)) \in R$
- A, R은 computable하다.

첫 두 가지는 서수에 대한 귀납법을 써서 보일 수 있다. 첫 번째 것만 보이기로 하자. 우선 $\nu(0) \in A_0$이다. 이제 모든 $\beta < \alpha$에 대해 $\nu(\beta) \in A$라 가정하자. 만약 $\alpha = \omega^{\beta_0} + \cdots + \omega^{\beta_r}$, $\alpha > \beta_0 \geq \cdots \geq \beta_r$이라면 가정에 의해 각 i에 대해 $\nu(\beta_i) \in A$이다. 이제 $\forall i : \nu(\beta_i) \in A_n$인 n을 찾자. 그러면 역시 귀납법 가정에 의해 $(\nu(\beta_i), \nu(\beta_{i+1})) \in R_n$이고, 따라서 A_{n+1}의 정의에 의해 $\nu(\alpha) \in A_{n+1}$이다.

n에 대한 귀납법을 쓰면 각 A_n과 R_n이 computable함을 알 수 있다: 가령, 만약 A_n, R_n이 computable하다면 A_{n+1}도 computable함을 다음과 같은 알고리즘으로 확인할 수 있다:

Data: A natural number x
Result: It determines whether $x \in A_{n+1}$
if *x is not of the form $2^l p_1^{e_1} \cdots p_l^{e_l}$* **then**
  print $x \notin A_{n+1}$;
end
Let $x = \langle e_1, \cdots, e_l \rangle$.
for $i = 1$ *to* l **do**
  if $e_i \notin A_n$ **then**
    print $x \notin A_{n+1}$;
  else if $(e_{i-1}, e_i) \in R_n$ **then**
    print $x \notin A_{n+1}$;
  end
end
print $x \in A_{n+1}$;

하지만 각 A_n이 재귀적이라고 해서 A가 재귀적이란 보장은 없다. $x \notin A$이려면 모든 n에 대해 $x \notin A_n$임을 체크해야 하고 이를 유한 시간 내에 끝낼 수 있단 보장이 없기 때문이다. 하지만 이 경우에는 유한 시간 안에 판정하는 방법이 있다: x가 pairing인지 확인하고 맞다면 그 pairing의 원소들이 pairing인지

5) 저기서 저러한 최소의 i가 없다면 $(x, y) \in R_{n+1}$이다.

확인하는 과정을 반복한다. 만약 여기서 하나라도 pairing이 아니라면 x는 A의 원소가 아니다. pairing을 '계속 뜯어보는 작업'은 언젠간 끝나고 총 n번의 확인 끝에 끝났을 때 $x \in A_n$인지 아닌지를 확인하면 충분하다.

R이 computable하단 것을 보이는 건 간단하다: 두 $a, b \in A$에 대해 $a \neq b$라면 $(a, b) \in R$과 $(b, a) \in R$ 중 단 하나만 성립하기 때문이다. 따라서 저 둘을 동시에 체크하면 된다. □

따라서 우리는 위의 서수 표현을 서수와 동일시할 수 있을 것이다. 하지만 위에서 정의한 서수 표현 체계는 ε_0 미만의 서수만을 표현할 수 있다. 적당히 다른 체계를 도입해서 ε_0 이상의 서수에 대응하는 표현을 줄 수 있을까? 그 답은 '예'이다. 하지만 여기엔 한계가 있다. 어떤 computable한 서수 표현 체계를 가져와도 다음 정의를 만족하는 서수만을 표현할 수 있기 때문이다:

Definition 3.3. 어떤 서수 α가 *computable*하단 것은 어떤 computable subset $D \subseteq \mathbb{N}$과 computable relation $R \subseteq \mathbb{N} \times \mathbb{N}$이 있어 $(D, R) \cong (\alpha, <)$인 것이다.

그리고 다행히도, 모든 computable ordinal을 표현할 수 있는 서수 표현 체계가 존재한다. Kleene가 처음 구성한 그 체계에 대한 세부사항과 서수 표현에 대한 좀 더 자세한 내용은 [10, p. 205-210]을 참고하길 바란다.

이제 우리들은 'primitive recursive한 서수열', 'computable한 서수열'이 뭔지 말할 수 있다. 어떤 서수열 $\langle \alpha_n \rangle_{n=0}^{\infty}$이 *primitive recursive*하단 것은 그 서수 표현들의 열 $\langle \nu(\alpha_n) \rangle_{n=0}^{\infty}$이 primitive recursive한 것이다.

3.2 Indepencence – A Proof

굿스타인 정리의 독립성이 보여진 것은 굿스타인이 자신의 정리를 발표하고 나서 약 20년 뒤였다. Kirby와 Paris가 자연수의 비표준 모형을 써서 굿스타인 정리가 PA에서 증명될 수 없음을 보였다.[4] 이 글에서는 Rathjen의 증명[7]을 소개할 것이다. 해당 증명은 다음 사실에서 시작한다:

Theorem 3.4 (Gentzen). [6] PRWO(ε_0)을 *'*ε_0보다 작은 서수들로 이뤄진 *primitive recursive sequence*는 무한히 감소할 수 없다.*'*이라는 진술이라 하자. 그러면

1. PRA + PRWO(ε_0)은 Con(PA)를 증명한다.
2. PA는 PRWO(ε_0)를 증명할 수 없다.

위 사실을 겐첸의 무모순성 증명이라 부른다. 왜냐면 적당한 초한 서수의 정렬가능성을 '믿는다면' 산술이 무모순함 또한 '믿을 수 있기' 때문이다. 이 글에

6) 오류 정정: 멍청한 세미나 원고에 실렸던 글에서는 PRA 위에서 PRWO(ε_0)과 Con(PA)가 동치라고 기술했으나, 이는 틀린 서술이다. PRWO(ε_0)는 PA의 1-consistency같은 Con(PA)보다 더 강한 명제를 증명할 수 있다.

서는 위 명제의 증명을 하지 않을 것이다. 이 정리에 대한 추가적인 사실은 뒷 절에서 다룰 것이다.

굿스타인은 본인의 논문 [2]를 겐첸의 결과와 그 의의를 소개하면서 시작하고 있고, 그 이후 n진법 전개와 칸토어 표준형을 비교하는 설명을 하고 있다. 또한 굿스타인은 ε_0 미만의 감소하는 서수열이 다음 정리에서 진술하는 형태로 나타남을 주장했다:

Proposition 3.5. $\varepsilon_0 > \alpha_0 > \alpha_1 > \cdots$가 감소하는 서수열이라 하자. 그러면 서수열 $\langle \alpha_r \mid r < \omega \rangle$은 각 $r < \omega$에 대해

1. $m_{r+1} \geq m_r$,
2. $n_{r+1} < S^{m_r}_{m_{r+1}}(n_r)$

이 있어 $\alpha_r = S^{m_r}_{\omega}(n_r)$이다.

따라서 굿스타인은 겐첸의 무모순성 정리로부터 착안해서, $\mathsf{PRWO}(\varepsilon_0)$을 자연수에 대한 명제로 바꿈으로써 PA와 독립인 명제를 얻어낼 수 있을 것이라 짐작했을 것이라 생각할수 있다. 실제로, [7]은 폴 버네이즈(Paul Bernays)의 편지로부터 굿스타인의 원고 [2]는 굿스타인 정리의 독립성에 대한 주장도 포함하고 있었을 것이라고 주장하고 있다. 하지만, 굿스타인은 버네이즈의 지적을 받은 후 독립성에 대한 주장을 원고에서 빼 버렸다고 한다.

우리들이 볼, Rathjen이 [7]에서 한 굿스타인 정리의 독립성 증명도 상술한 같은 아이디어를 따라갈 것이다: 만약 PA가 모순을 함의한다면, 겐첸의 정리에 의해 무한히 감소하는 ε_0보다 작은 서수로 이뤄진 primitive recursive sequence가 존재한다. 그리고 이로부터 굿스타인 정리의 반례를 만들어낼 것이다.[7] 대우를 취하면, 굿스타인 정리가 페아노 산술의 무모순성을 증명하게 됨을 알 수 있다.

본격적인 증명에 들어가기 전에 증명의 개요를 스케치해보자. 우리들은 주어진 서수 감소열로부터 느리게 감소하는 서수열을 만들 것이다. 그 '느리게 감소하는' 서수열 $\langle \beta_n \rangle$은, β_n을 바로 $(n+2)$-초진법 전개로 바꿔도 별 문제 없게 생긴 수열이다. 그리고 $\langle b_n \rangle = G(T^{\omega}_2(\beta_0))$으로 줄 것이다. 그 다음 $b_n \leq T^{\omega}_{n+2}(\beta_n)$임을 보일 것이다. 따라서 b_n은 절대 0이 될 수 없다.

이 작업을 하기 위해선 좀 많은 보조정리가 필요하다. 주어진 서수 $\alpha < \varepsilon_0$의 칸토어 표현 $\alpha = \omega^{\beta_0} \cdot n_0 + \cdots + \omega^{\beta_k} \cdot n_k$에 대해 α의 길이 $|\alpha|$를

$$|\alpha| = \max\{|\beta_1|, \cdots, |\beta_k|, n_0, \cdots, n_k\} + 1$$

7) 따라서 아래 증명이 이해가 안 된다면 거꾸로 읽어보길 권한다.

로 정의하자. $|\alpha|$는 α의 완전 칸토어 표현이 (기호열로써) 대충 얼마나 긴지 나타내는 척도 역할을 한다.

Lemma 3.6. 함수 $\ell : \mathbb{N} \to \mathbb{N}$에 대해 $\ell^0(l) = l$, $\ell^{n+1} = \ell(\ell^n(l))$로 정의하자. 이 때 *Grzegorczyk hierarchy* $\langle f_l \rangle_{l\in\mathbb{N}}$은 $f_0(n) = n+1$, $f_{l+1}(n) = f_l^n(n)$으로 주어지는 함수족이다.

임의의 r변수 원시 재귀 함수 h에 대해 어떤 n이 있어 임의의 순서쌍 $\vec{x}$에 대해 $h(\vec{x}) \le f_n(\max(2, \vec{x}))$ 이다.

Proof. 우선 증명에 앞서 위의 함수들이 만족하는 성질들을 열거해보자:

1. $f_i(0) = \delta_{i0}$, $f_i(1) = 2$.
2. 각 f_l은 증가함수이다.
3. $n \ge 1$이면 $f_l(n) \le f_{l+1}(n)$. 따라서 $l \le m$이면 $f_l(n) \le f_m(n)$이다.
4. $n \ge 2$이면 $f_l(f_m(n)) \le f_{\max(l,m)+1}(n)$이다.

이의 증명은 귀납법을 쓰면 쉽게 가능하다. 이제 원래 증명하려는 명제로 돌아가자. 원시 재귀 함수의 정의가 재귀적이므로, 그 정의를 따라 귀납적으로 증명할 것이다. 상수함수와 후자 함수, projection을 적당한 f_n으로 bound하는 것은 어렵지 않다. 만약 $h(x) = g_0(g_1(x), \cdots, g_k(x))$, $g_i(x) \le f_n(\max(2, x))$라면

$$\begin{aligned} h(x) &\le f_n(\max(2, g_1(x), \cdots, g_k(x))) \\ &\le f_n(\max(2, f_n(\max(2, x)))) \le f_{n+1}(\max(2, x)) \end{aligned}$$

이다. 따라서 f_n으로 bound되는 함수들의 합성 또한 적당한 f_l로 bound된다.

이제 f_n으로 bound되는 함수들의 원시 재귀로 주어지는 함수 또한 적당한 f_l로 bound됨을 보이자. 보다 정확히는, 적당한 $n \ge 2$에 대해 $g(\vec{x}) \le f_n(\max(2, \vec{x}))$, $\varphi(\vec{x}, y, \vec{z}) \le f_n(\max(2, \vec{x}, y, \vec{z}))$일 때

- $h(0, x) = g(x)$
- $h(S(y), x) = \varphi(x, y, h(y, x))$

로 주어지는 함수를 bound시킬 것이다. 우선 $h(0, x) \le f_n(\max(2, x))$이다. 만약 $h(y, x) \le f_n^{y+1}(\max(2, x, y))$이라 가정하면

$$\begin{aligned} h(y+1, x) &\le f_n(\max(2, x, y, h(y, x))) \le f_n(\max(2, x, y, f_n^{y+1}(\max(2, x, y))) \\ &\le f_n^{y+2}(\max(2, x, y)) \end{aligned}$$

이다. $w = \max(2, x, y)$라 두었을 때 따라서

$$\begin{aligned} h(y,x) &\leq f_n^{y+2}(w) \leq f_n^{w+2}(w) \leq f_n^2(f_{n+1}(w)) \leq f_n^n(f_{n+1}(w)) \\ &\leq f_{n+1}^2(w) \leq f_{n+2}(w) \end{aligned}$$

이다. □

Lemma 3.7. f를 원시 재귀 함수라 하자. 이 때 어떤 원시 재귀 함수 $g : \mathbb{N}^2 \to \omega^\omega$가 있어

(1) $m < f(n)$이면 $g(n,m) > g(n,m+1)$이고

(2) 어떤 K가 있어 임의의 m, n에 대해 $|g(n,m)| \leq K \cdot (n+m+1)$이다.

Proof. Lemma 3.6에 의해, $f = f_l$에 대해서만 확인해도 된다. l에 대한 귀납법을 써서 적당한 k와 위 성질을 만족하는 $g : \mathbb{N}^2 \to \omega^k$를 찾을 것이다: 우선 $l = 0$인 경우 $g(n,m) = \max(n+2-m, 0)$으로 둔다. 이제 $g : \mathbb{N}^2 \to \omega^k$가 위의 성질들을 f에 대해 만족한다고 가정하자. f^i를 f를 i번 합성한 것이라 하고 $f'(n) = f^n(n)$을 f의 대각화라고 하자. 이 때 $m < f'(n)$에 대해

$$g'(n,m) := \omega^k \cdot (n-i) + g(f^i(n), j)$$

로 정의하자. 여기서 i, j는 $m = f(n) + f^2(n) + \cdots + f^i(n) + j$, $i < n$, $j < f^{i+1}(n)$인 유일한 자연수이다. $m \geq f'(n)$일 때 $g'(n,m) = 0$으로 둔다.

이제 g'가 원하는 조건을 만족함을 확인하자. $m < f'(n)$이라 가정하자. 우선 조건 (1)부터 확인해야 한다. 여기서 $j + i < f^{i+1}(n)$인 경우와 $j + 1 = f^{i+1}(n)$인 경우로 나뉜다. 첫 번째 경우는 g에 대한 귀납적 가정에 의해

$$\begin{aligned} g'(n,m) &= \omega^k \cdot (n-i) + g(f^i(n), j) \\ &\geq \omega^k \cdot (n-i) + g(f^i(n), j+1) = g'(n, m+1) \end{aligned}$$

이다. 반면 $j + 1 = f^{i+1}(n)$인 경우 어떤 자연수도 ω보다 작단 사실에 의해

$$\begin{aligned} g'(n,m) &= \omega^k \cdot (n-i) + g(f^i(n), j) \\ &\geq \omega^k \cdot (n-i-1) + g(f^i(n), 0) = g'(n, m+1) \end{aligned}$$

이다. 이제 조건 (2)를 확인하자. 이를 증명하기 이전에, $|\alpha + \beta| \leq |\alpha| + |\beta|$임을 확인하자. $\alpha = a_0\omega^{\delta_0} + \cdots + a_N\omega^{\delta_N}$, $\beta = b_0\omega^{\delta_0} + \cdots + b_N\omega^{\delta_N}$이라 하자. $a = \max_i a_i$, $b = \max_i b_i$, 라 하면

$$|\alpha + \beta| \leq \max(a+b, |\delta_0|, \cdots, |\delta_N|) + 1 \leq |\alpha| + |\beta|$$

이다. 이제 K를 $|g(m,n)| \leq K(m+n+1)$을 만족하는 상수라 하자. 그리고 $m < f'(n)$인 경우만 고려하고 i, j를 증명 첫 부분에서 언급한 것과 같게 두자. 그러면

$$\begin{aligned} |g'(n,m)| &= |\omega^k(n-i) + g(f^i(n), j)| && \leq \max(k+1, n-i) + |g(f^i(n), j)| \\ &\leq (k+1)(n-i) + K(f^i(n) + j + 1) && \leq (k+1)Kn + (k+1)K(m+1) \\ &= (k+1)K(n+m+1) \end{aligned}$$

이다. □

Corollary 3.8. 임의의 감소하는 *primitive recursive sequence of ordinals* $\varepsilon_0 > \beta_0 > \beta_1 > \cdots$으로부터 느리게 감소하는 *primitive sequence* $\langle \alpha_n \rangle$을 만들 수 있다. 여기서 느리게 감소한단 것은 어떤 K가 있어 $|\alpha_i| \leq K \cdot (i+1)$이란 것이다.

Proof. $f(n) = |\beta_{n+1}|$로 두고 위 보조정리를 적용해서 함수 g를 얻자. 이 때 $g(n,m) > g(n,m+1)$ for every $m < |\beta_{n+1}|$이고 $|g(n,m)| \leq K \cdot (n+m+1)$이다. 이제

$$\alpha_j = \omega^\omega \cdot \beta_n + g(n,m)$$

로 주자. 여기서 $j = |\beta_0| + \cdots + |\beta_n| + m$ for $m < |\beta_{n+1}|$이다. 이 때 $|\omega^\omega \beta_n| \leq 2 + |\beta_n|$이므로

$$\begin{aligned} |\alpha_j| &\leq |\omega^\omega \beta_n| + |g(n,m)| \leq 2 + |\beta_n| + K(n+m+1) \\ &\leq 2K(n + |\beta_n| + m + 1) \leq 2K(|\beta_0| + \cdots + |\beta_n| + m + 1) \\ &= 2K(j+1) \end{aligned}$$

이다. 그리고 $j < |\beta_0|$인 경우는 $\alpha_j = \omega^\omega \cdot \beta_0 + |\beta_0| + 1 - j$로 준다. 이 경우 사실 $|\alpha_j|$는 상수에 의해 bound된다. 따라서 이 경우도 적당한 K가 있어 $|\alpha_j| \leq K \cdot (j+1)$이다. □

Theorem 3.9. 느리게 감소하는 *primitive recursive descending sequence of ordinals* $\varepsilon_0 > \alpha_0 > \alpha_1 > \cdots$에 대해, 즉, 어떤 K가 있어 $|\alpha_i| \leq K \cdot (i+1)$을 만족하는 서수열에 대해 어떤 감소하는 *primitive recursive* 서수열 $\varepsilon_0 > \beta_0 > \beta_1 > \cdots$이 있어 $C(\beta_r) \leq r+1$을 만족한다.

Proof. $\omega_{(0)} = \omega$, $\omega_{(n+1)} = \omega^{\omega_{(n)}}$이라 두자. $\alpha_0 < \varepsilon_0$에 대해 $\omega \cdot \alpha_0 < \omega_{(s)}$, $K < s$인 s를 찾고 $j < K$에 대해

$$\beta_j = \omega_{(s)} + \cdots + \omega_{(s-K+j+1)}$$

로 주자. 그리고

$$\beta_{K\cdot(n+1)+i} = \omega \cdot \alpha_n + K - i$$

로 주자. 그러면 $\beta_r > \beta_{r+1}$임을 쉽게 확인할 수 있다. 그리고 $j < K$일 때 $C(\beta_j) = 1$이며 $C(\alpha_n) \leq |\alpha_n| \leq K \cdot (n+1)$이므로

$$C(\beta_{K\cdot(n+1)+i}) = C(\omega \cdot \alpha_n + K - i) \leq 1 + K(n+1)$$

이다. 따라서 모든 r에 대해 $C(\beta_r) \leq r + 1$이다. □

Lemma 3.10. $\varepsilon_0 > \beta_0 > \beta_1 > \cdots$ 이 $C(\beta_n) \leq n + 1$을 만족하는 *primitive recursive*한 서수열이라 하자. 그러면 굿스타인 수열 $G(T_2^\omega(\beta_0))$은 절대 *0*으로 끝나지 않는다.

Proof. $\langle b_n \rangle = G(T_2^\omega(\beta_0))$에 대해 $b_n \geq T_{n+2}^\omega(\beta_n)$임을 보일 것이다. $C(\beta_n) \leq n + 1$이므로 우변은 절대 0일 수 없고, 따라서 $b_n > 0$이다.

$n = 0$일 경우 위 부등식은 자명하다. 이제 $b_n \geq T_{n+2}^\omega(\beta_n)$이 성립한다 가정하자. 이 때 $C(\beta_n) \leq n + 1$이므로 가정에 의해 $S_{n+3}^{n+2}(b_n) \geq S_{n+3}^{n+2}(T_{n+2}^\omega(\beta_n))$이다. 양변에 1을 빼면 좌변은 b_{n+1}이 되고, 우변은 $T_{n+3}^\omega(\beta_n) - 1$이 된다. 그런데 $C(\beta_{n+1}) \leq n + 2$이므로 $T_{n+3}^\omega(\beta_n) > T_{n+3}^\omega(\beta_{n+1})$이다. 따라서 $T_{n+3}^\omega(\beta_n) - 1 \geq T_{n+3}^\omega(\beta_{n+1})$이고 원하는 부등식을 얻는다. □

따라서 무한히 감소하는 ε_0보다 작은 서수로 이루어진 원시재귀열로부터 굿스타인 정리의 반례를 얻었다. 즉, 굿스타인 정리가 성립하면 ε_0보다 작은 서수로 이뤄진 감소하는 원시재귀열은 언젠간 0이 된다. 그리고 후자는 PA의 무모순성과 동치이다. 따라서 괴델의 불완전성 정리에 의해 굿스타인 정리는 PA에서 증명될 수 없다.

4 Gentzen's consistency result

위에서 소개한 굿스타인 정리의 독립성 증명은 굿스타인 정리를 겐첸의 무모순성 정리에 환원하는 식으로 이루어졌다. 하지만 막상, 겐첸의 정리에 대해서는 어떠한 증명도 소개하지 않았다. 따라서 이 글을 마무리하기 전에 겐첸의 무모순성 정리의 증명의 역사와 개요를 알아보려고 한다. (만약 겐첸의 증명에 관심이 없고 굿스타인 정리의 독립성 증명에만 관심이 있다면, [12]를 처음부터 끝까지 읽는 것도 괜찮은 선택지이다.)

4.1 Historical background

겐첸의 산술의 무모순성의 배경에는 힐베르트의 형식주의가 있다. 브라우어의 직관주의에 대항에서, 힐베르트는 우리들이 하는 수학을 유한론적인 수학으로 환

원하고, 그 무모순성을 유한론적으로 증명해내는 프로그램을 계획한다. 하지만, 힐베르트의 프로그램이라 불리는 그 원안은 1931년에 발표된 괴델의 불완전성 정리에 의해 불가능함이 판명났다. 특히, 폰 노이만이 괴델의 결과로부터 관찰했듯, 괴델의 정리는 페아노 산술 PA가 자기 자신의 무모순성을 보일 수 없다는 귀결로 이어진다.[8] 괴델의 정리에 대해 힐베르트의 입장 중 기록으로 남은 것은 1934년에 출판된 '수학 기초'(Grundlagen der Mathematik) 초판 서문에 나오는 다음 문장 하나뿐이라고 한다:

> "Jenes Ergebnis zeigt in der Tat auch nur, daßman für die weitergehenden Widerspruchsfreiheitsbeweise den finiten Standpunkt in einer schäferen Weise ausnutzen muß, [...]"
>
> (괴델의 정리는) 오로지 더 나아간 무모순성 증명을 위해서 유한론적인 방법이 더 철저히 적용되어야 함을 보여줄 뿐이고 [...]

하지만 버네이즈의 진술에 따르면, 힐베르트는 괴델의 정리를 처음 접하고 분노와 절망으로 가득 찼으나, 이후 해당 문제를 좀 더 건설적으로 바라보려고 했다고 한다. 한편 버네이즈는 힐베르트가 그의 프로그램에 대해 꽤 큰 전환을 만들어낼 수 있었다는 데에 감명받았다고 회고했다.

비록 힐베르트의 첫 시도는 실패했지만, 힐베르트 프로그램 자체는 다소 변형된 형태로 계속되었다. 힐베르트의 시도는 게르하르트 겐첸(Gerhard Gentzen)에게 영향을 주었다. 그는 1932년에 이중 부정 해석 (double-negation interpretation)이라 불리는, 고전 논리적인 페아노 산술을 구성주의적인 하이팅 산술 (Heyting arithmetic, HA)로 환원하는 방법을 발견했다.[9] 따라서 하이팅 산술이 '무모순함'을 보이기만 하면 페아노 산술 또한 무모순함을 보일 수 있게 되었다. 물론, 여기서 무모순성 증명은 힐베르트가 처음 생각한, '자기 자신의 무모순성을 증명'하는 것이 될 수 없고, 무모순성이 그럴 듯한 다른 체계에 산술을 환원하는 작업이 된다. 결국 1935년, 겐첸은 PRA 위에서 ε_0의 정렬성을 가정해서 하이팅 산술의 무모순성을 보이는 데 성공한다.

겐첸의 증명의 개요를 살펴보기에 앞서, 겐첸의 이후 인생사를 간략하게 짚어보려고 한다. 겐첸의 연구는 2차 대전이 시작되면서 사실상 중단되었다. 겐첸은 1937년에 나치당에 가입했고, 1943년까지는 괴팅겐 대학에 머물렀으나, 1939년부터 1941년까지는 군 복무를 수행하였다. 그는 1942년에 하빌리타치온 논문을 제출한 이후 학생들을 가르칠 권한을 얻게 되어, 프라하 독일 대학교(Deutsche Universität Prag, 현 카렐 대학교)에 부임하게 된다. 하지만 전쟁 막바지에 프라

8) 역설적이게도, 괴델은 원래 불완전성 정리가 아니라, 산술로부터 해석학의 무모순성을 증명하는 것이 목표였다고 한다. 여기서 '해석학'은, 현대적인 관점에서는 2차 산술로 해석하는 것이 옳을 것이다.

9) 괴델 역시 이를 독립적으로 발견했기 때문에 괴델-겐첸 이중 부정 해석이라 부르기도 한다.

하 봉기가 일어났고, 이후 소련군의 진군으로 프라하 독일 대학 내 모든 교직원은 전쟁포로가 된다. 겐첸은 소련군에 의해 억류되었고, 3개월 후 아사하게 된다.

4.2 Ordinal analysis for PA

겐것은 1935년에 처음으로 무모순성 증명을 내놓았다. 하지만, 해당 증명은 Fan theorem을 사용하고 있었고, 이에 대한 비판을 받았다. 해당 비판이 유효한 것은 아니였지만, 겐첸의 증명이 여전히 비구성적이였기 때문에 겐첸은 해당 증명을 철회했다. 현재 잘 알려진 증명은 겐첸이 1938년에 두 번째로 내놓은 증명이다. 겐첸의 증명은 유한주의적이지만, motivation이 잘 드러나지 않는다고 알려져 있으며 겐첸이 사용한 방법이 그대로 현재에도 사용되는 것은 아니라 한다. 우리들은 겐첸의 원래 증명의 개요를 살펴보는 대신, 다소 개작된 방법의 개요를 볼 것이다.

우선, 겐첸의 무모순성 정리의 진술을 다시 보자. 이번엔 우리들에게 필요한 것 외로 겐첸이 실제로 더 이뤄낸 결과도 같이 볼 것이다:

Theorem 4.1 (Gentzen). $\mathsf{PRWO}(\varepsilon_0)$을 '$\varepsilon_0$보다 작은 서수들로 이뤄진 *primitive recursive sequence*는 무한히 감소할 수 없다.'이라는 진술이라 하자. 그러면

1. $\mathsf{PRA} + \mathsf{PRWO}(\varepsilon_0)$은 $\mathsf{Con}(\mathsf{PA})$를 증명한다. 따라서 PA는 $\mathsf{PRWO}(\varepsilon_0)$를 증명할 수 없다.
2. PA는 *ordertype*이 ε_0 미만인 *primitive recursive order*에 대한 초한귀납법을 증명한다.
3. 만약 $\prec$가 *primitive recursive relation*이고 PA가 $\prec$에 대한 초한귀납법을 증명한다면, $\prec$의 순서형은 ε_0보다 작다.[10]

뒤의 두 결과는 PA의 증명론적 서수*(proof-theoretic ordinal)*이 ε_0임을 나타낸다.[11]

겐첸의 증명은 특수한 형태의 형식 증명을 분석하는 과정을 요한다. 편의성을 위해, 우리는 Sequent calculus라는 새로운 형태의 논리 체계를 도입할 것이다. 또한, 우리들은 다음과 같은 더 약한 명제를 증명할 것이며 겐첸의 증명 대신 다른 증명법을 따라갈 것이다:

---

10) 해당 진술에 기술적인 함정이 있다: $\prec$에 대한 그냥 산술의 논리식에 대한 초한귀납법이 아니라, 산술의 언어에 자유로운 단항 관계기호 X를 추가해서 얻은 언어 $\mathcal{L}_{\mathsf{PA}}(X)$ 위에서의 초한귀납법이다.

11) 어떤 computable한 이론 T의 증명론적 서수는

$$|T| = \sup\{\text{ordertype}(\prec) \mid \prec \text{ is primitive recursive and } T \vdash \mathrm{TI}(\prec, X)\}$$

로 정의된다. 여기서 $\mathrm{TI}(\prec, X)$는 X라는 자유 관계기호를 허용한 $\prec$ 위에서의 초한귀납법을 말한다.

Theorem 4.2. $\mathsf{TI}(\varepsilon_0)$을 ε_0 위에서의 초한귀납법이라 하자. 그러면 $\mathsf{PRA}+\mathsf{TI}(\varepsilon_0)$은 $\mathsf{Con}(\mathsf{PA})$를 증명한다.

Sequent calculus를 정의하는 방법은 다양하게 있지만, 우리들은 [1]의 방식을 따를 것이다.[12)]

우리들이 정의할 논리 체계는 $\neg$을 따로 갖고 있지 않으며, 모든 atomic formula R이 대응하는 negated form $\neg R$을 갖는다고 가정한다. 우리들은 주어진 atomic formula와 그 부정을 싸잡아서 *literal*이라 부를 것이다. 그리고 주어진 논리식(formula)의 부정은 드 모르간 법칙에 의해 주어지는 것으로 생각하자. 논리식들의 유한집합을 *sequent*라 부를 것이며, Γ 혹은 Δ 등으로 나타낼 것이다. 우리들이 소개할 논리 체계에서 sequent는 마치 $\bigvee\Gamma$와 같이 해석될 것이고, 따라서 empty sequent는 모순명제를 가리킨다.

Definition 4.3 (One-sided sequent calculi G)**.** G는 다음과 같은 공리를 가지고 있다:

$$\Gamma, \neg L, L$$

for any sequent Γ and a literal L.

그리고 G는 다음과 같은 추론 규칙으로 이뤄져 있다:

$$\frac{\Gamma, A_0 \vee A_1, A_i}{\Gamma, A_0 \vee A_1}(\vee)_i\,(i=0,1) \qquad \frac{\Gamma, A_0 \wedge A_1, A_0 \quad \Gamma, A_0 \wedge A_1, A_1}{\Gamma, A_0 \wedge A_1}(\wedge)$$

$$\frac{\Gamma, \exists x A(x), A(t)}{\Gamma, \exists x A(x)}(\exists) \qquad \frac{\Gamma, \forall x A(x), A(a)}{\Gamma, \forall x A(x)}(\forall)$$

여기서 $(\forall)$의 경우, 자유변수 a가 lower sequent $\Gamma, \forall x A(x)$에서 나타나면 안 된다. 또한, G의 경우 다음과 같은 cut rule을 가진다:

$$\frac{\Gamma, \neg C \quad C, \Delta}{\Gamma, \Delta}(\mathrm{cut})$$

위의 공리와 추론 규칙으로 이뤄진 체계를 G라 하며, G에서 cut rule을 뺀 체계를 G_1이라 부를 것이다. 만약 주어진 sequent Γ가 증명을 갖는다면 $\mathsf{GTI}(\varepsilon_0) \vdash \Gamma$라고 나타낸다.

위에서 정의한 논리 체계는 고전 명제 논리와 완전히 동일함이 알려져 있다.

다른 추론 규칙들과 달리, cut rule은 upper sequent에 있던 논리식이 lower sequent의 부분논리식으로 나타날 필요가 없이 그냥 사라질 수 있다. 만약 어떤

12) 독자에 따라 [12]에 나타나는 방법을 따를 수도 있다. 이 경우도 디테일을 제외하면 대체로 비슷한 흐름을 따른다.

sequent의 증명이 cut을 갖지 않는다면, 해당 증명에서 나타나는 모든 명제는 결론의 부분논리식이 될 것이다:

Definition 4.4. A를 논리식이라 했을 때 A의 부분논리식들의 집합 $\mathrm{Sufml}(A)$를 다음과 같이 정의하자:

1. $\mathrm{Sufml}(L) = \{L\}$ (L이 literal인 경우)
2. $\mathrm{Sufml}(A_0 * A_1) = \{A_0 * A_1\} \cup \bigcup_{i=0,1} \mathrm{Sufml}(A_i)$ ($* \in \{\vee, \wedge\}$).
3. $\mathrm{Sufml}(\mathbf{Q}xA(x)) = \{\mathbf{Q}xA(x)\} \cup \bigcup \{\mathrm{Sufml}(A(t)) \mid t \text{ is a term}\}$ ($\mathbf{Q} \in \{\forall, \exists\}$.)

Proposition 4.5 (Subformula property). Γ가 *cut*을 사용하지 않는 증명 *(cut-free proof)*를 갖는다고 하자. 그러면 해당 증명에 나타나는 모든 논리식은 Γ의 원소의 부분논리식이다.

따라서 모든 증명이 cut-free proof로 바뀔 수 있다면 증명을 분석하는 데 있어 매우 유용할 것이다. 실제로, 위에서 소개한 G는 이를 만족한다.

Theorem 4.6 (Cut-elimination theorem for G). $\vdash \Gamma$라 하자. 그러면 Γ의 *cut-free proof*가 있다.

이로부터 특히 일차 술어 논리가 무모순함을 알 수 있다: 만약 명제 논리가 모순을 증명한다면 empty sequent의 증명이 존재해야 하고, 특히 empty sequent의 cut-free proof가 존재한다. 그런데 cut-free proof에서 나타나는 모든 명제는 empty sequent 상의 명제의 subformula여야 하는데, 모든 증명은 공리로부터 출발하고 empty sequent는 공리가 아니다. 따라서 empty sequent의 cut-free proof는 존재할 수 없다.

겐첸의 PA의 '무모순성 증명'도 위와 비슷한 절차를 밟는다. 하지만, 페아노 산술의 공리를 단순히 G의 공리로 추가하는 방법은 작동하지 않는다고 알려져 있다. 그 대신, 우리들은 G를 변형해서 일종의 무한 연역 체계를 만들 것이다. 그리고 그 연역 체계가 증명해내는 명제가 PA로부터 증명할 수 있는 명제와 같음을 확인하고, 해당 체계가 cut elimination을 만족함을 확인할 것이다.

Definition 4.7 (ω-logic G_ω)**.** ω-logic은 predicate symbol로 $\{=, \neq\}$와 unary relation symbol들 및 그 부정을 가지며, 따름수 연산 S와 0을 포함한 함수 기호들을 갖는다. 각 함수 기호 f는 어떤 함수 $f^{\mathbb{N}} : \mathbb{N}^k \to \mathbb{N}$으로 해석될 수 있다. 그리고 논리식은 자유변수가 없는 닫힌 식 *(closed formula)*만을 고려할 것이다. 각 term t에 대해, 그 값 $t^{\mathbb{N}}$을 t에서 나타나는 함수 기호 f를 모두 그 해석 $f^{\mathbb{N}}$으로 바꿨을 때 얻어지는 값으로 생각하자. 무한 G_ω는 다음과 같은 공리로 이뤄져 있다: G_1의 공리와 더불어, 다음 공리를 추가적으로 갖는다:

- $\Gamma, t_0 = t_1$ ($t_0^{\mathbb{N}} = t_1^{\mathbb{N}}$일 때,)

- $\Gamma, t_0 \neq t_1$ ($t_0^{\mathbb{N}} \neq t_1^{\mathbb{N}}$일 때,)

또한, G_ω는 G_1에서 ($\forall$) 대신 다음과 같은 추론 규칙을 만족한다:

$$\frac{\Gamma, \forall x A(x), A(0) \quad \Gamma, \forall x A(x), A(S0) \quad \Gamma, \forall x A(x), A(SS0) \quad \cdots}{\Gamma, \forall x A(x)} (\forall\omega)$$

ω-logic은 자연수 구조 $\mathbb{N}$ 위에서 다루어지는 논리 구조이다. 해당 논리가 꼭 산술을 형상화할 필요는 없지만, 이 글에서는 그런 경우만 고려할 것이다. G_ω 또한 G_1과 마찬가지로 cut elimination을 만족한다:

Theorem 4.8. 만약 $\mathsf{G}_\omega + (cut) \vdash A$라면 $\mathsf{G}_\omega \vdash A$이다.

Cut elimination에 대해 이야기하기 전에, 위의 G_ω를 어떻게 PRA같은 약한 산술에서 구현할 수 있는 지 짚고 넘어가자. 여기서 omega-rule이 무한 규칙이란 데에 주목하자. 해당 규칙을 도입해서 얻어내는 proof tree는 자연수로 code할 수 없을 것이다. (그러한 proof tree가 자연수보다 많을 것이기 때문이다.) 여기서 우리들이 하는 형식 증명이 유한하고 계산가능하단 데서 착안해서, omega-rule의 upper sequent들의 집합이 primitive recursive하다는 조건을 걸자. 그렇게 하면 무한한 증명들의 집합을 그 자연수 code로 대체할 수 있고, 특히 PRA 같은 체계에서도 무한 증명을 다룰 수 있게 될 것이다.

비록 이 글에서는 위의 정리들의 증명을 소개하지 않겠지만, [1]에서 다루는 cut elimination의 증명은 cut-free proof를 직접 구성하지 않고 귀류법을 이용해서 비구성적인 증명을 한다.[13] Cut elimination을 구성적으로 증명하기 위해서, 우리들은 '증명의 복잡도'와 'cut으로 사라지는 논리식의 복잡도'를 G_ω에 반영해서 변형할 것이다.

Definition 4.9 (Degree of a formula)**.** 어떤 논리식 A의 degree $\mathrm{dg}(A)$를 다음과 같이 귀납적으로 정의하자:

1. $\mathrm{dg}(L) = 0$ for a literal L,
2. $\mathrm{dg}(A_0 * A_1) = \max\{\mathrm{dg}(A_0), \mathrm{dg}(A_1)\} + 1$, $* \in \{\wedge, \vee\}$, and
3. $\mathrm{dg}(\mathbf{Q}xA(x)) = \mathrm{dg}(A(a)) + 1$, $\mathbf{Q} \in \{\forall, \exists\}$.

Definition 4.10. G를 $\mathsf{G}_\omega + T + (\mathrm{cut})$이라 하자. 여기서 T는 어떤 닫힌 논리식들의 집합이고, 각 $A \in T$에 대해 A에 대응하는 추론 규칙이 major formula를 갖지 않는 경우만을 고려하자.[14]

13) 좀 더 구체적으로는, Weak Kőnig's lemma를 이용한다.

14) 세부사항에 대해서는 [1], 3장 1절을 참고할 것. Major formula는 연역 규칙에서 없어지는 formula를 subformula로써 흡수하는 공식을 말하며, 흡수당하는 공식을 minor formula라고 부른다. 가령, ($\wedge$)의 경우 $A_0 \wedge A_1$이 major formula, 각 A_i가 minor formula이다. (Cut)은 major, minor formula 둘 다 갖지 않는다.

이 때 $\mathsf{G}\left|\frac{\alpha}{c}\right.\Gamma$은 'Cut formula의 depth가 c 이하이고 proof tree의 높이가 α 이하인 Γ의 증명이 있다'는 의미이며, 다음과 같이 귀납적으로 정의된다:

1. 만약 Γ가 G의 공리이면 $\mathsf{G}\left|\frac{\alpha}{c}\right.\Gamma$가 항상 성립한다.
2. 만약 $\dfrac{\{\Gamma_i \mid i \in I\}}{\Gamma}$가 G의 추론 규칙 중 (cut)이 아닌 것이고, 모든 $i \in I$에 대해 $\mathsf{G}\left|\frac{\beta}{c}\right.\Gamma_i$이고 $\beta < \alpha$이면 $\mathsf{G}\left|\frac{\alpha}{c}\right.\Gamma$이다.
3. 만약 $\mathsf{G}\left|\frac{\beta}{c}\right.\Gamma, \neg C$, $\mathsf{G}\left|\frac{\beta}{c}\right.C, \Gamma$이며 $\mathrm{dg}(C) < c$이면 $\mathsf{G}\left|\frac{\alpha}{c}\right.\Gamma, \Delta$이다.

그러면 다음 사실을 보일 수 있다:

Theorem 4.11 (Cut-elimination theorem). $2_c(\alpha)$를 귀납적으로 $2_0(\alpha) = \alpha$, $2_{c+1}(\alpha) = 2^{2_c(\alpha)}$라 하자. 이 때 $\mathsf{G}\left|\frac{\alpha}{c}\right.\Gamma$이면 $\mathsf{G}\left|\frac{2_c(\alpha)}{0}\right.\Gamma$이다.

해당 정리의 증명은 [1]의 3장 1절을 참고하기 바란다. 또한, 해당 정리를 증명하는 과정에서 α에 대한 귀납법을 사용하기 때문에 $\mathsf{TI}(\varepsilon_0)$가 사용된다. 이제 페아노 산술을 ω-logic 에 embed할 것이다.[15)]

Definition 4.12. 우리들은 ω-logic G 중 함수 기호가 다음과 같이 주어진 것을 고려할 것이다: 각 primitive recursive function f에 대해 그에 대응하는 함수 기호 F_f를 갖는다. F_f의 해석은 f로 주어진다.[16)] Primitive recursive relation은 그 characteristic function으로 대신 생각한다.

또한, 페아노 산술 PA는 $\mathsf{G}_1 + (cut)$에 다음 공리를 추가한 것이다. 여기서 a는 eigenvariable이고 t는 term이다.

$$\frac{\Gamma, A(0) \quad \neg A(a), \Gamma, A(Sa) \quad \neg A(t), \Gamma}{\Gamma}\,(\mathrm{VJ})$$

위에서 제시한 공리들과 추론 규칙들의 집합은 primitive recursive하고, 함의 관계 $\left|\frac{\alpha}{c}\right.$ 역시 primitive recursive하게 정의됨을 알 수 있다. 또한 서수 표현의 산술과 관련된 기초적인 성질들은 PRA에서 증명될 수 있다. 따라서 [1] 3장 1절의 증명들은 PRA로 옮겨올 수 있다. 또한, 다음 사실로부터 PA의 정리를 G의 정리로 옮겨올 수 있음을 알 수 있다:

Theorem 4.13 ([1], Lemma 4.4). $\Gamma(\vec{a})$를 PA 위에서의 *sequent*이고, $\Gamma(\vec{a})$가 자유변수를 $\vec{a}$만 갖는다 하자. *Numeral*[17)]들의 열 $\vec{n}$에 대해, $\Gamma(\vec{n})$을 Γ에서 $\vec{a}$를 $\vec{n}$

15) [1]에서는 bounded quantification과 unbounded quantification을 나눠서 취급하고 있다. 이는 PA의 subtheory를 다루기 위해서 구분지은 것으로, 우리들은 PA의 subtheory가 목적이 아니므로 이런 구분을 짓지 않을 것이다.

16) [1]에서는 elementary function이라 불리는, 사칙연산 및 임의 합과 곱, $x \mapsto 2^x$에 의해 생성되는 함수족을 대신 고려한다.

17) $S^n 0$ 꼴의 term을 가리킨다.

으로 바꾼 것이라 하자. 만약 $\mathsf{PA} \vdash \Gamma(\vec{a})$라면, 어떤 $k, n, m < \omega$가 있어 임의의 $\vec{n}$에 대해 $\left|\frac{\omega \cdot k + m}{n}\right. \Gamma(\vec{n})$이 성립한다.

따라서 G의 cut elimination에 의해, 다음을 알 수 있다:

Theorem 4.14 ($\mathsf{PRA} + \mathsf{TI}(\varepsilon_0)$)**.** PA는 무모순하다.

Proof. PA가 모순을 함의한다 가정하자. 그러면 G는 empty sequent를 증명한다. Cut elimination에 의해, empty sequent의 cut-free proof가 존재한다. 하지만 모든 증명은 공리로부터 시작하고, 공리는 empty sequent가 아니여서 모순이다. □

사실 우리들은 좀 더 강력한 결과를 얻을 수 있다: $\mathsf{PRA} + \mathsf{PRWO}(\varepsilon_0)$는 PA의 1-consistency 또한 증명해낸다. 여기서 PA의 1-consistency란 다음 진술을 가리킨다:

$$\forall \ulcorner A \urcorner \in \Sigma_1 [\mathsf{PA} \vdash \ulcorner A \urcorner \implies \mathrm{Tr}_1(\ulcorner A \urcorner)].$$

여기서 Tr_1은 partial truth predicate로, PRA 위에서 정의 가능함이 알려져 있다. 또한 Tr_1는 Σ_1-논리식 A에 대해 $\mathrm{Tr}_1(\ulcorner A \urcorner) \leftrightarrow A$를 만족한다.

Theorem 4.15 ($\mathsf{PRA} + \mathsf{TI}(\varepsilon_0)$)**.** PA는 *1-consistent*하다.

Proof. A가 $\exists x B(x, t)$꼴의 논리식이라 하자. 여기서 B는 x만을 자유변수로 가지며 B는 bounded formula이다. 우리들은 PA가 PRA를 포함하고 있다고 가정하고 있으므로, 일반성을 잃지 않고 B가 quantifier-free라 가정해도 무방하다.[18] 만약 $\mathsf{PA} \vdash \exists B(x, t)$라면 어떤 $\alpha < \varepsilon_0$이 있어 $\left|\frac{\alpha}{0}\right. \exists x B(x, t)$가 성립한다. 연역체계 G에서 $\exists$를 도입하는 방법은 ($\exists$)를 적용하는 방법밖에 없으므로 어떤 $\beta < \alpha$와 term s가 있어 $\left|\frac{\beta}{0}\right. B(s, t)$이다. 그리고 이는 G의 정의에 의해 $B(s, t)$와 동치이다. 따라서 $\exists x B(x, t)$가 성립한다. □

참고로, PA의 귀납법을 Σ_1-논리식으로 제한해서 얻어지는 $\mathsf{I}\Sigma_1$ 위에서 PRWO와 PA의 1-consistency는 동치이다. 이의 증명은 [1]의 4장을 참고하기 바란다. 이 글에서 Theorem 4.1의 증명을 다루지 않을 것이다. 이에 대한 증명은 적당한 다른 문헌, 가령 [1] 혹은 [6] 등을 참고하기 바란다.

References

[1] Toshiyasu Arai. *Ordinal Analysis with an Introduction to Proof Theory.* Springer, 2020.

18) PRA는 임의의 quantifier-free formula A에 대해 어떤 term t가 있어 $A \leftrightarrow (t = 0)$임을 증명한다.

[2] R. L. Goodstein. "On the Restricted Ordinal Theorem". In: *The Journal of Symbolic Logic* 9.2 (June 1944), pp. 33–41.

[3] Reinhard Kahle. "Gentzen's consistency proof in context". In: *Gentzen's Centenary – The Quest for Consistency*. Ed. by Reinhard Kahle and Michael Rathjen. Springer, 2015, pp. 3–24.

[4] Laurie Kirby and Jeff Paris. "Accessible Independence Results for Peano Arithmetic". In: *Bull. London Math. Soc.* 14 (Aug. 1982), pp. 285–293.

[5] Kenneth Kunen. *Set theory: an introduction to independence proofs*. North-Holland, 1980.

[6] Wolfram Pohlers. *Proof theory: The first step into impredicativity*. Springer Science & Business Media, 2008.

[7] Michael Rathjen. "Goodstein's theorem Revisited". In: *Gentzen's Centenary – The Quest for Consistency*. Ed. by Reinhard Kahle and Michael Rathjen. Springer, 2015, pp. 229–242.

[8] Michael Rathjen and Wilfried Sieg. "Proof Theory". In: *The Stanford Encyclopedia of Philosophy*. Ed. by Edward N. Zalta. Fall 2020. Metaphysics Research Lab, Stanford University, 2020.

[9] E. F. Robertson and J. J. O'Connor. *Gerhard Gentzen*. Sept. 2001. URL: https://mathshistory.st-andrews.ac.uk/Biographies/Gentzen/.

[10] Hartley Rogers. *Theory of Recursive Functions and Effective Computability*. MIT Press, 1987.

[11] William W Tait. "Gentzen's original consistency proof and the Bar Theorem". In: *Gentzen's Centenary – The Quest for Consistency*. Ed. by Reinhard Kahle and Michael Rathjen. Springer, 2015, pp. 213–228.

[12] Henry Towsner. *Goodstein's theorem, ε_0, and unprovability*. 2020. URL: https://www.sas.upenn.edu/~htowsner/GoodsteinsTheorem.pdf.