循環証明の話

秋津 早苗　(@akitsu-sanae)

ML Day #2 2018-9-16

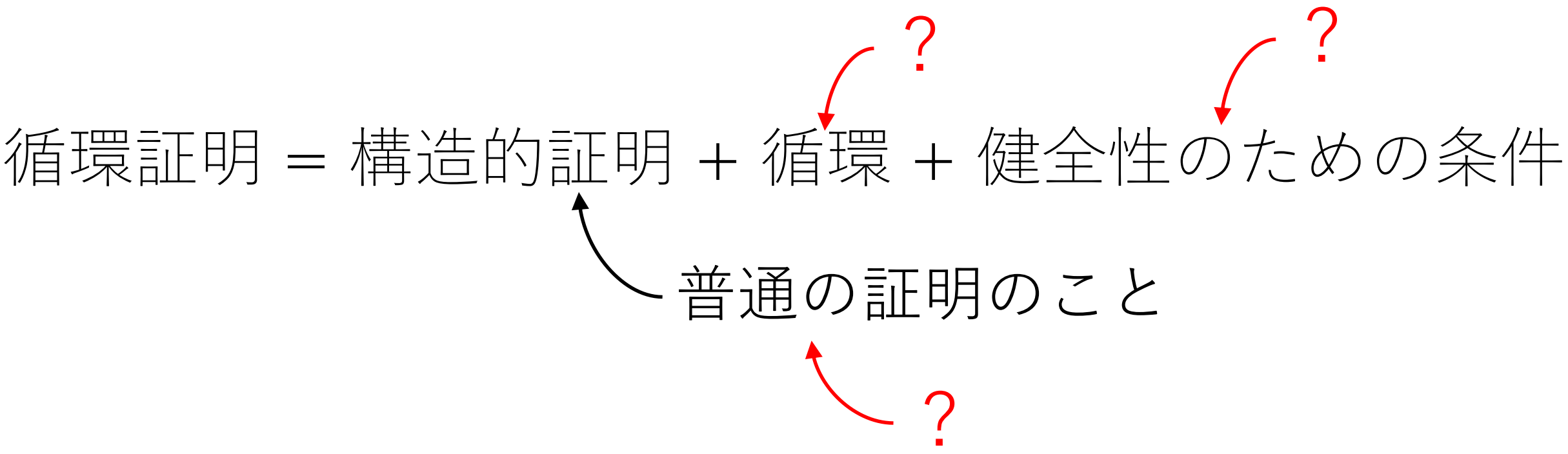
ごめんなさい！
MLじゃなくて証明の話をします！

循環証明の話をします！

循環証明 = 構造的証明 + 循環 + 健全性のための条件

普通の証明のこと

循環証明の話をします！



普通の証明，とは？

判断式 $\Gamma \vdash \Delta$ ：“$\wedge\Gamma$ を前提として $\vee\Delta$が成り立つ”という式

Γ, Δ ： 論理式の列

推論規則 $\dfrac{\Gamma' \vdash \Delta'}{\Gamma \vdash \Delta}$：$\Gamma' \vdash \Delta'$が成り立てば$\Gamma \vdash \Delta$が成り立つという規則

公理 ： 無前提に正しいと認める論理式 e.g.)$\phi \vdash \phi, \vdash 0 = 0$

健全性 ： $\Gamma \vdash \Delta$の証明が存在するなら$\Gamma \vdash \Delta$は妥当である

証明したい判断式を推論規則で変形して公理の形まで持っていく

「自然数は偶数か奇数である」ことの証明

$$N(x) \vdash E(x) \vee O(x)$$

自然数 $N(x) \equiv_{\mu} x = 0 \vee N(x-1)$
偶数　$E(x) \equiv_{\mu} x = 0 \vee O(x-1)$
奇数　$O(x) \equiv_{\mu} E(x-1)$

「自然数は偶数か奇数である」ことの証明

$$\frac{\vdash E(0) \vee O(0) \qquad N(x-1), E(x-1) \vee O(x-1) \vdash E(x) \vee O(x)}{N(x) \vdash E(x) \vee O(x)}$$

自然数 $N(x) \equiv_{\mu} x = 0 \vee N(x-1)$

偶数　$E(x) \equiv_{\mu} x = 0 \vee O(x-1)$

奇数　$O(x) \equiv_{\mu} E(x-1)$

「自然数は偶数か奇数である」ことの証明

$$\dfrac{\dfrac{\vdash E(0)}{\vdash E(0) \vee O(0)} \qquad N(x-1), E(x-1) \vee O(x-1) \vdash E(x) \vee O(x)}{N(x) \vdash E(x) \vee O(x)}$$

自然数 $N(x) \equiv_{\mu} x = 0 \vee N(x-1)$

偶数　$E(x) \equiv_{\mu} x = 0 \vee O(x-1)$

奇数　$O(x) \equiv_{\mu} E(x-1)$

「自然数は偶数か奇数である」ことの証明

$$\dfrac{\dfrac{\dfrac{}{\vdash 0 = 0 \vee N(0-1)}}{\vdash E(0)}}{\vdash E(0) \vee O(0)} \qquad \dfrac{}{N(x-1), E(x-1) \vee O(x-1) \vdash E(x) \vee O(x)}$$

$$N(x) \vdash E(x) \vee O(x)$$

自然数 $N(x) \equiv_{\mu} x = 0 \vee N(x-1)$

偶数　$E(x) \equiv_{\mu} x = 0 \vee O(x-1)$

奇数　$O(x) \equiv_{\mu} E(x-1)$

「自然数は偶数か奇数である」ことの証明

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash 0 = 0}\ \text{OK}}{\vdash 0 = 0 \vee N(0-1)}}{\vdash E(0)} \qquad N(x-1), E(x-1) \vee O(x-1) \vdash E(x) \vee O(x)}{N(x) \vdash E(x) \vee O(x)}$$

自然数 $N(x) \equiv_\mu x = 0 \vee N(x-1)$

偶数　$E(x) \equiv_\mu x = 0 \vee O(x-1)$

奇数　$O(x) \equiv_\mu E(x-1)$

「自然数は偶数か奇数である」ことの証明

$$\frac{N(x-1), E(x-1) \vee O(x-1) \vdash E(x) \vee O(x)}{N(x) \vdash E(x) \vee O(x)}$$

自然数 $N(x) \equiv_{\mu} x = 0 \vee N(x-1)$

偶数　$E(x) \equiv_{\mu} x = 0 \vee O(x-1)$

奇数　$O(x) \equiv_{\mu} E(x-1)$

「自然数は偶数か奇数である」ことの証明

$$\dfrac{\dfrac{N(x-1), E(x-1) \vdash E(x) \vee O(x) \qquad N(x-1), O(x-1) \vdash E(x) \vee O(x)}{N(x-1), E(x-1) \vee O(x-1) \vdash E(x) \vee O(x)}}{N(x) \vdash E(x) \vee O(x)}$$

自然数 $N(x) \equiv_{\mu} x = 0 \vee N(x-1)$

偶数　$E(x) \equiv_{\mu} x = 0 \vee O(x-1)$

奇数　$O(x) \equiv_{\mu} E(x-1)$

「自然数は偶数か奇数である」ことの証明

$$\dfrac{\dfrac{N(x-1), E(x-1) \vdash E(x) \vee E(x-1)}{N(x-1), E(x-1) \vdash E(x) \vee O(x)} \qquad N(x-1), O(x-1) \vdash E(x) \vee O(x)}{\dfrac{N(x-1), E(x-1) \vee O(x-1) \vdash E(x) \vee O(x)}{N(x) \vdash E(x) \vee O(x)}}$$

自然数 $N(x) \equiv_{\mu} x = 0 \vee N(x-1)$

偶数　$E(x) \equiv_{\mu} x = 0 \vee O(x-1)$

奇数　$O(x) \equiv_{\mu} E(x-1)$

「自然数は偶数か奇数である」ことの証明

OK

$$\dfrac{\dfrac{\dfrac{E(x-1)\vdash E(x-1)}{N(x-1),E(x-1)\vdash E(x)\vee E(x-1)}}{N(x-1),E(x-1)\vdash E(x)\vee O(x)}\qquad N(x-1),O(x-1)\vdash E(x)\vee O(x)}{\dfrac{N(x-1),E(x-1)\vee O(x-1)\vdash E(x)\vee O(x)}{N(x)\vdash E(x)\vee O(x)}}$$

自然数 $N(x)\equiv_{\mu} x=0\vee N(x-1)$

偶数 $E(x)\equiv_{\mu} x=0\vee O(x-1)$

奇数 $O(x)\equiv_{\mu} E(x-1)$

「自然数は偶数か奇数である」ことの証明

$$\dfrac{\dfrac{N(x-1), O(x-1) \vdash E(x) \vee O(x)}{N(x-1), E(x-1) \vee O(x-1) \vdash E(x) \vee O(x)}}{N(x) \vdash E(x) \vee O(x)}$$

自然数 $N(x) \equiv_{\mu} x = 0 \vee N(x-1)$

偶数　$E(x) \equiv_{\mu} x = 0 \vee O(x-1)$

奇数　$O(x) \equiv_{\mu} E(x-1)$

「自然数は偶数か奇数である」ことの証明

$$\dfrac{\dfrac{\dfrac{N(x-1), O(x-1) \vdash x = 0 \vee O(x-1) \vee O(x)}{N(x-1), O(x-1) \vdash E(x) \vee O(x)}}{N(x-1), E(x-1) \vee O(x-1) \vdash E(x) \vee O(x)}}{N(x) \vdash E(x) \vee O(x)}$$

自然数 $N(x) \equiv_{\mu} x = 0 \vee N(x-1)$

偶数　$E(x) \equiv_{\mu} x = 0 \vee O(x-1)$

奇数　$O(x) \equiv_{\mu} E(x-1)$

「自然数は偶数か奇数である」ことの証明

OK

$$\dfrac{\dfrac{\dfrac{\dfrac{O(x-1) \vdash O(x-1)}{N(x-1), O(x-1) \vdash x = 0 \vee O(x-1) \vee O(x)}}{N(x-1), O(x-1) \vdash E(x) \vee O(x)}}{N(x-1), E(x-1) \vee O(x-1) \vdash E(x) \vee O(x)}}{N(x) \vdash E(x) \vee O(x)}$$

自然数 $N(x) \equiv_{\mu} x = 0 \vee N(x-1)$

偶数　$E(x) \equiv_{\mu} x = 0 \vee O(x-1)$

奇数　$O(x) \equiv_{\mu} E(x-1)$

「自然数は偶数か奇数である」ことの証明

証明完了！

$$\dfrac{\dfrac{\dfrac{\dfrac{O(x-1) \vdash O(x-1)}{N(x-1), O(x-1) \vdash x = 0 \vee O(x-1) \vee O(x)}}{N(x-1), O(x-1) \vdash E(x) \vee O(x)}}{N(x-1), E(x-1) \vee O(x-1) \vdash E(x) \vee O(x)}}{N(x) \vdash E(x) \vee O(x)}$$

自然数 $N(x) \equiv_{\mu} x = 0 \vee N(x-1)$

偶数　$E(x) \equiv_{\mu} x = 0 \vee O(x-1)$

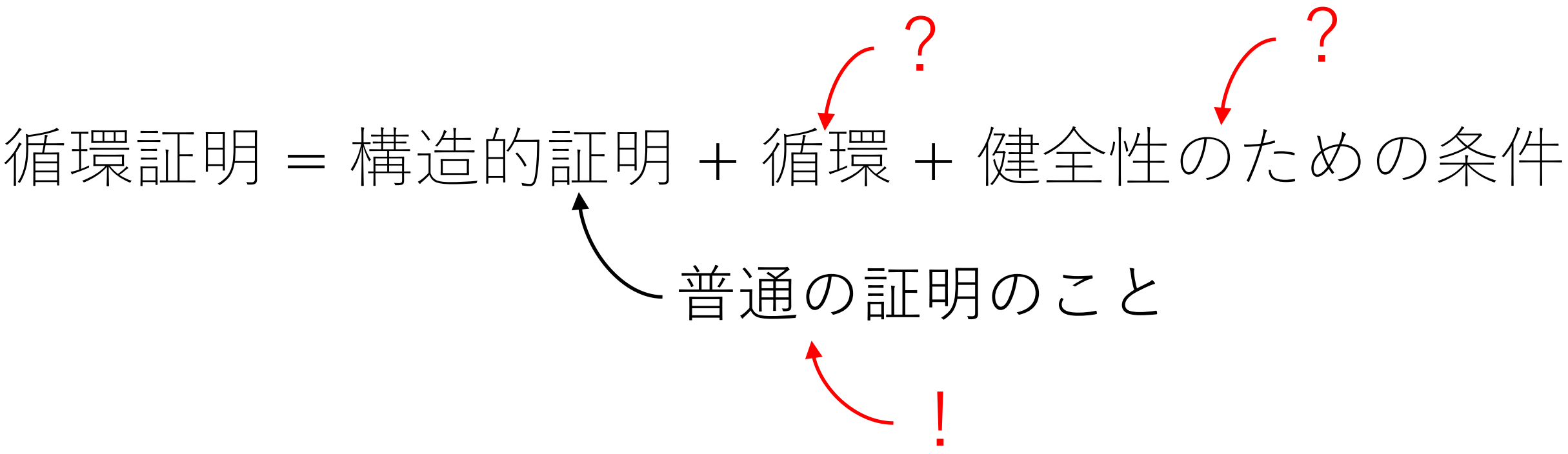
奇数　$O(x) \equiv_{\mu} E(x-1)$

なぜこれでいいのか？

- 推論規則 $\dfrac{\Gamma' \vdash \Delta'}{\Gamma \vdash \Delta}$ はlocally soundであることが求められる
  - $\Gamma' \vdash \Delta'$が妥当であれば$\Gamma \vdash \Delta$も妥当である
- 公理は妥当である

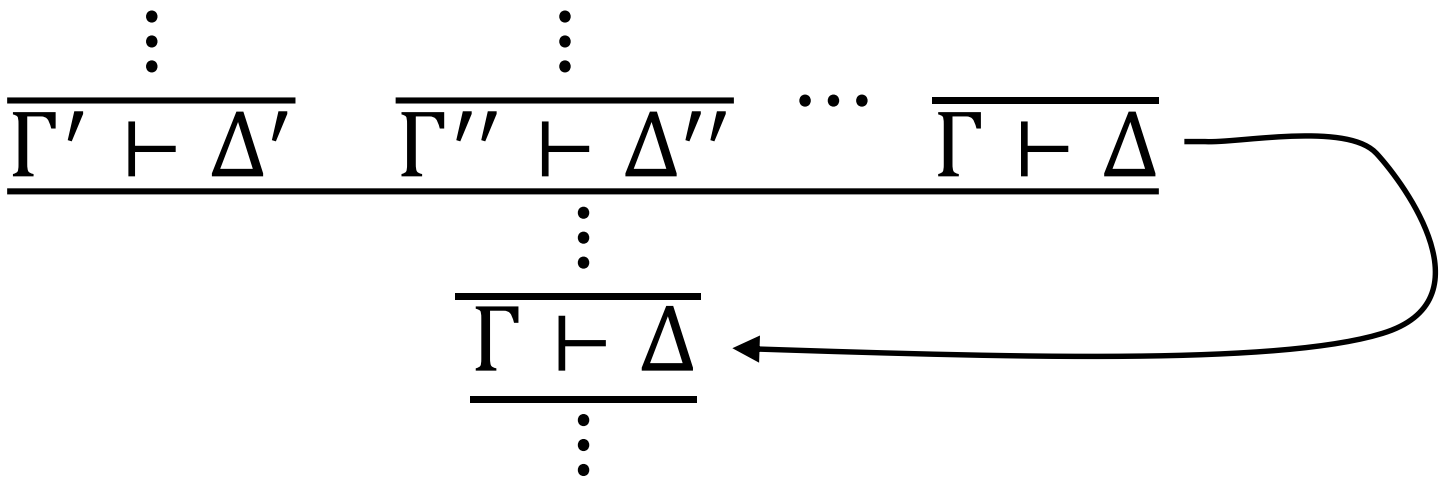
- 証明図を作ることは，含意を重ねることで
  「公理が妥当であれば帰結も妥当である」
  ことを示すのと同じ

循環証明とは



循環

- 導出の途中に出てきた判断式を再利用できる！



「自然数は偶数か奇数である」ことの証明

$$\dfrac{\dfrac{\dfrac{\dfrac{\vdots}{\vdash E(0) \vee O(0)}}{x = 0 \vdash E(x) \vee O(x)} \qquad \dfrac{\dfrac{\dfrac{\dfrac{N(x) \vdash O(x) \vee E(x)}{N(x-1) \vdash O(x-1) \vee E(x-1)}}{N(x-1) \vdash x = 0 \vee O(x-1) \vee E(x-1)}}{N(x-1) \vdash E(x) \vee E(x-1)}}{N(x-1) \vdash E(x) \vee O(x)}}{x = 0 \vee N(x-1) \vdash E(x) \vee O(x)}$$

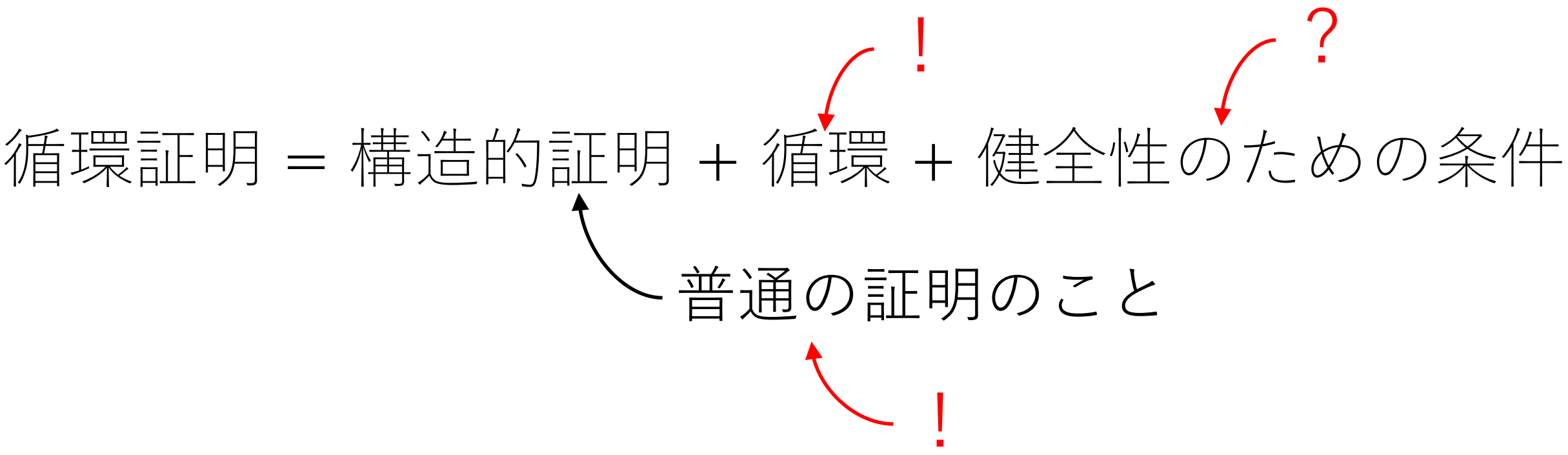
$$N(x) \vdash E(x) \vee O(x)$$

自然数 $N(x) \equiv_\mu x = 0 \vee N(x-1)$

偶数　$E(x) \equiv_\mu x = 0 \vee O(x-1)$

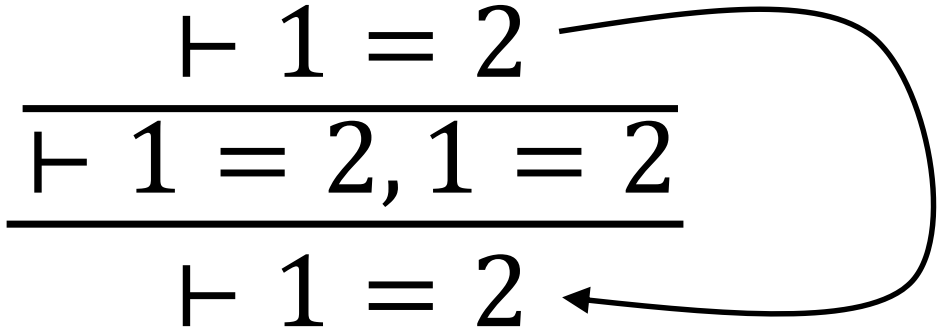
奇数　$O(x) \equiv_\mu E(x-1)$

循環証明とは



健全性のための条件

循環を無制限に許していいの？



明らかに間違っている判断式が証明できちゃう！！

なにがマズいのか？

- 構造的証明（普通の証明）はなんで健全だったのか？

  → local soundnessによって妥当であるための十分条件が伝播し，最後にそれらが公理によって閉じられていたから

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\vdots}{\vdash 1=2}}{\vdash 1=2,1=2}}{\vdash 1=2}}{\vdash 1=2,1=2}}{\vdash 1=2}$$

無制限に循環を許すと，その循環を無限回使うことで公理によって閉じられないパスが存在しうる！

健全性のための条件

＝「循環が無限回使われない」ための条件

1. 循環を無限回使うと，何かしらの無限降下列を構成できることを示す
2. でもその何かしらは整礎であることを示す

→ 背理法から循環は無限回使われないことがわかる

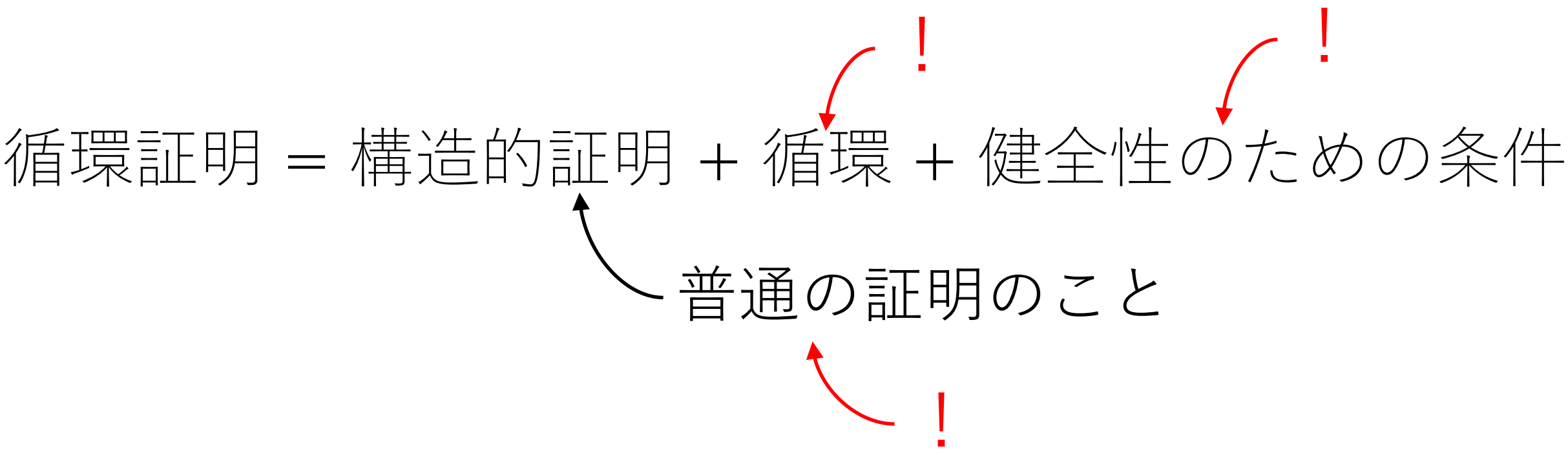
どう形式化するかは様々だけど循環証明体系の直観は大体これ

帰納法と無限降下法の関係

帰納法	無限降下法
$\dfrac{\Gamma, \forall x' < x.\,[x'/x]\phi \vdash \phi, \Delta}{\Gamma \vdash \forall x.\,\phi, \Delta}$	$\dfrac{\Gamma, \phi \vdash \exists x' < x.\,[x'/x]\phi, \Delta}{\Gamma, \exists x.\,\phi \vdash \Delta}$

片方のϕを否定するともう片方が得られる
→　実質言ってることは同じ
→　循環は帰納法と同等の役割

循環証明とは



循環証明の何がうれしいの？

構造的証明で帰納法を使うのは色々考える必要があって難しい

- 帰納法の仮定はどうするか？
- 帰納法をどのタイミングで使うか？

循環証明なら先に論理式を適当に分解していって後で循環を結べそうな所を探せばいい！

→ 証明探索が楽

Cyclist

- 循環証明器をつくるためのフレームワーク
- DemoページではCyclistを使ったSeparation Logicの自動定理証明器を試すことができる
- http://www.cyclist-prover.org/
- https://github.com/ngorogiannis/cyclist

僕の研究の宣伝

既存体系の問題点

既存の循環証明体系では，証明系から「見えていない」部分 (背景理論) で定義された帰納的構造に対して帰納法を回せない

解決！！

背景理論のソルバを使えば無限に使われないことが示せる循環も許すことで，そのような帰納法も回せる循環証明体系を提案しました！

「一階不動点論理の循環証明体系とプログラム検証への応用」
in 2018年日本ソフトウェア科学会

まとめ

循環証明 = 構造的証明 + 循環 + 健全性のための条件

- 構造的証明：判断式を推論規則によって公理の妥当性に帰着
- 循環：証明の途中に出てきた判断式を再利用できる
- 健全性のための条件：無限に循環しないための条件

循環証明のフレームワークCyclist
僕の研究の話：循環証明体系の証明能力を上げたよ！

参考

Brothertonによる循環証明の紹介スライド：
http://www0.cs.ucl.ac.uk/staff/J.Brotherston/slides/PARIS_FLoC_07_18_part1.pdf
http://www0.cs.ucl.ac.uk/staff/J.Brotherston/slides/PARIS_FLoC_07_18_part2.pdf