Структурна индукция

Трифон Трифонов

λ-смятане и теория на доказателствата, 2018/19 г.

26 февруари 2019 г.

Какво разбираме под индукция?

Интуитивно понятие:

- Показваме решението на най-простото твърдение (база, дъно)
- Допускаме, че твърдението е вярно (индукционно допускане)
- С негова помощ доказваме твърдението за нов случай (стъпка)

Задача

Да се докаже, че $2 + 4 + \ldots + 2n = n(n+1)$.

Доказателство.

- за $n = 0$: трябва да проверим, че $0 = 0.1$ ✓
- нека допуснем, че сме доказали свойството за дадено n
- ще го докажем за $n + 1$:
- $(2+4+\ldots+2n)+2(n+1) = n(n+1)+2(n+1) = (n+1)(n+2)$ ✓

Следователно: доказахме свойството за произволно n. □

Проблеми с интуитивното понятие

Задача (George Pólya)

Да се докаже, че всички коне са един и същи цвят.

Доказателство. Къде е грешката?

- за $n = 1$: един кон тривиално е един и същи цвят.
- нека допуснем, че сме доказали свойството за дадено n
- да разгледаме група от $n + 1$ коне
- да махнем **последния** кон, получаваме група от n коне
  - те са един и същи цвят по индукционно допускане
- да махнем **първия** кон, получаваме друга група от n коне
  - те са един и същи цвят по индукционно допускане
- оттук следва, че всички $n + 1$ коне са един и същи цвят

Следователно: доказахме свойството за произволно n. □

Индуктивна дефиниция на множества

Трябва да започнем от по-базово понятие: множество.
Какво означава да дефинираме множество по индукция?

Пример: Дефинираме индуктивно множеството N такова, че:

- $o \in N$,
- ако $X \in N$, то $s(X) \in N$.

Примерни елементи на N: o, $s(o)$, $s(s(s(s(s(o)))))$, $\ldots$
Вярно ли е, че $s(a) \in N$? Защо?
При индуктивна дефиниция обикновено подразбираме най-малкото множество, което изпълнява индуктивните клаузи.

Доказателство по индукция чрез индуктивна дефиниция

Да докажем свойството $A(n)$ по индукция се свежда до индуктивна дефиниция на множество.

Да разгледаме множеството T от елементи n, за които $A(n)$ е истина.

Да докажем нещо по индукция означава да проверим, че:

- $A(o)$; т.е. $o \in T$
- Ако $A(n)$, то $A(s(n))$; т.е. ако $n \in T$, то $s(n) \in T$

Но тогава $T = N$, т.е. A е вярно за всяко $n \in N$.

Всъщност доказахме A с индукция по структурата на множеството N.

Проблеми на полуформалната дефиниция

Да дефинираме по индукция следното множество:

- $B \subseteq N$
- $o \in B$
- ако $X \notin B$, то $s(X) \in B$

$B = ?$

- $B = \{o, s(s(o)), s(s(s(s(o)))), \ldots\}$
- $B = \{o, s(o), s(s(s(o))), s(s(s(s(s(o))))), \ldots\}$

И двете множества са минимални!

Монотонни оператори

Имаме нужда от формален подход към индукцията. За основа ще използваме теория на множествата.
Нека фиксираме непразно множество U (универсум).
С $\mathcal{P}(U) := \{X \subseteq U\}$ означаваме множеството от всички подмножества на U.

Дефиниция

Оператор над U наричаме тотална функция $\Gamma : \mathcal{P}(U) \to \mathcal{P}(U)$.

Дефиниция

Операторът Γ наричаме *монотонен*, ако за произволни $X \subseteq Y$ е вярно, че $\Gamma(X) \subseteq \Gamma(Y)$.

Примери за монотонни оператори

- $\Gamma_1(X) := \emptyset, \quad \Gamma_2(X) := U$
- $\Gamma_3(X) := Y$ за произволно фиксирано $Y \subseteq U$
- $\Gamma_4(X) := X$
- $\Gamma_5(X) := X \cup \{o\}$
- $\Gamma_6(X) := \{f(x) \mid x \in X\}$ за произволна функция $f : U \to U$
- Ако Γ' и Γ'' са монотонни, то $\Delta_1(X) := \Gamma'(X) \cup \Gamma''(X)$ и $\Delta_2(X) := \Gamma'(X) \cap \Gamma''(X)$ са монотонни
- $\Gamma_7(X) := \{o\} \cup \{s(x) \mid x \in X\}$.

Интуиция: монотонните оператори само добавят, но не премахват елементи от аргумента си.

Неподвижни точки

Дефиниция

Множеството X наричаме *неподвижна точка* на оператора Γ, ако $\Gamma(X) = X$.

Кои са неподвижните точки на операторите Γ_i?

Пример: N е неподвижна точка на Γ_7.

Може ли един оператор да има повече от една неподвижна точка?

За да използваме неподвижна точка за дефиниция на множество трябва да казваме коя от тях имаме предвид.

Теорема на Knaster-Tarski

Теорема

Ако Γ *е монотонен оператор, то той има единствена най-малка неподвижна точка* X_Γ.

Доказателство.

Дефинираме

$$X_\Gamma := \bigcap \{X \subseteq U \mid \Gamma(X) \subseteq X\}.$$

□