Дискретни структури, лекция 2: доказателства по индукция

Минко Марков
minkom@fmi.uni-sofia.bg

Факултет по Математика и Информатика
Софийски Университет "Свети Климент Охридски"

23 октомври 2024 г.

Обикновена индукция

Типичната ситуация е такава. Даден е предикат $P(n)$ и трябва да докажем $\forall n \in \mathbb{N} : P(n)$. Схемата на доказателствата по индукция върху естествените числа е следната.

- Доказваме $P(0)$, като просто проверяваме истинността на предиката за $n = 0$.
- Допускаме $P(n)$ за **произволно** $n \in \mathbb{N}$ и въз основа на това допускане доказваме $P(n+1)$.

Числата на Fibonacci са $F_0 = 0$, $F_1 = 1$, $F_n = F_{n-1} + F_{n-2}$ за $n \geqslant 2$. Докажете, че за всяко $n \geqslant 1$:

$$F_{n-1}F_{n+1} - F_n^2 = (-1)^n \tag{1}$$

Доказателство.

Базата е $n = 1$ (а не $n = 0$). Ако $n = 1$, то (1) става $F_0F_2 - F_1^2 = (-1)^1$, тоест $0 \cdot 1 - 1 = -1$, което очевидно е вярно. ✓

Индуктивното предположение е, че за някое (а не за всяко!) $n \geqslant 1$ е изпълнено $F_{n-1}F_{n+1} - F_n^2 = (-1)^n$.

Пример за доказателство по индукция (2)

В индуктивната стъпка ще докажем, че $F_n F_{n+2} - F_{n+1}^2 = (-1)^{n+1}$. Започваме от допускането

$$F_{n-1} F_{n+1} - F_n^2 = (-1)^n$$

Умножаваме по -1:

$$F_n^2 - F_{n-1} F_{n+1} = (-1)^{n+1}$$

Заместваме F_{n-1} с $F_{n+1} - F_n$ (имаме право, понеже $n + 1 \geqslant 2$):

$$\begin{aligned} F_n^2 - (F_{n+1} - F_n) F_{n+1} &= (-1)^{n+1} \leftrightarrow \\ F_n^2 + F_n F_{n+1} - F_{n+1}^2 &= (-1)^{n+1} \leftrightarrow \\ F_n (F_n + F_{n+1}) - F_{n+1}^2 &= (-1)^{n+1} \end{aligned}$$

Но $F_n + F_{n+1} = F_{n+2}$, така че $F_n F_{n+2} - F_{n+1}^2 = (-1)^{n+1}$. **QED**

Силна индукция

Даден е предикат $P(n)$ и трябва да докажем $\forall n \in \mathbb{N} : P(n)$. Схемата на доказателствата със силна индукция върху естествените числа е следната.

- Доказваме $P(0)$, като просто проверяваме истинността на предиката за $n = 0$.
- Допускаме, че за **произволно** $n \in \mathbb{N}$ са изпълнени:
  - $P(0)$,
  - $P(1)$,
  - $\ldots$,
  - $P(n)$

  Въз основа на тези допускания, или само част от тях, доказваме $P(n+1)$.

Пример за доказателство със силна индукция (1)

Теорема 1

Всяко естествено число, по-голямо или равно на 2, е произведение на едно или повече прости числа.

Доказателство: Ще докажем теоремата със силна индукция. Базата е $n = 2$ (а **не** $n = 0$). Твърдението за стойност на аргумента 2 е тривиално вярно: 2 е произведение на едно просто число, а именно 2. С това доказахме базовия случай.

Индуктивното предположение е, че за произволно $n \geqslant 2$ е вярно, че за всяко $k \in \{2, 3, \ldots, n\}$ е вярно, че k е произведение от едно или повече прости числа.

Пример за доказателство със силна индукция (2)

В индуктивната стъпка разлеждаме твърдението за стойност на аргумента $n+1$. Следните подслучаи са изчерпателни:

- $n+1$ е просто. Тогава $n+1$ се явява произведение на едно просто число.
- $n+1$ е съставно. Тогава по дефиниция $n+1 = p \cdot q$, където $p, q \in \{2, 3, \ldots, n\}$. Съгласно индуктивното предположение, и p, и q са произведения от едно или повече прости числа. Тогава $n+1$ е произведение от едно или повече прости числа. **QED**

Силната индукция е еквивалентна на обикновената

Силната индукция е еквивалентна на обикновената, а се казва "силна" по дидактични причини. Дефинираме предиката $Q(n)$ така:

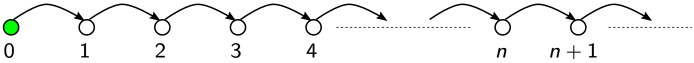
$P(k)$ *е в сила за* $k \in \{0, 1, \ldots, n\}$

Тоест, $Q(n)$ е $P(0) \wedge P(1) \wedge \cdots \wedge P(n-1) \wedge P(n)$.

Да докажем $P(n)$ със силна индукция е същото като да докажем $Q(n)$ с обикновена индукция.

Достижимост от базата при обикновената индукция

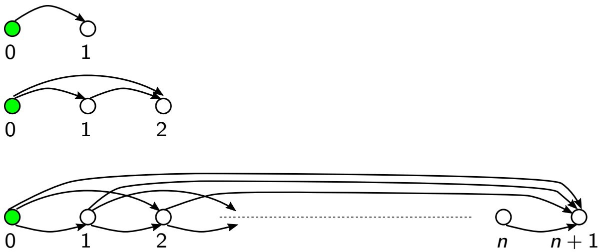
При обикновената индукция, $P(0)$ доказва $P(1)$, $P(1)$ доказва $P(2)$, и т.н. Безкрайният граф "$P(i)$ доказва $P(j)$" изглежда така:



Всяка стойност на аргумента е достижима от базата.

Достижимост от базата при силната индукция

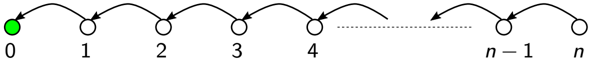
При силната индукция, $\boxed{P(0)}$ доказва $P(1)$, $\boxed{P(0) \text{ и } P(1)}$ доказват $P(2)$, $\boxed{P(0),\ P(1) \text{ и } P(2)}$ доказват $P(3)$, и т.н.



Всяка стойност на аргумента е достижима от базата.

Достижимост на базата при обикновената индукция

При обикновената индукция, $P(n)$ се доказва чрез $P(n-1)$, $P(n-1)$ се доказва чрез $P(n-2)$, и т.н., $P(1)$ се доказва чрез базата $P(0)$. Крайният граф "$P(i)$ се доказва чрез $P(j)$", започвайки от някакво $P(n)$, изглежда така:

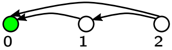


Базата е достижима от всяка стойност на аргумента. Базата не може да бъде "прескочена".

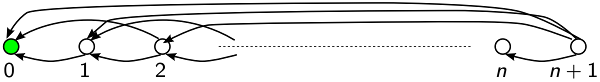
Достижимост на базата при силната индукция

При силната индукция, крайният граф "$P(i)$ се доказва чрез $P(j)$", започвайки от някаква стойност на аргумента, изглежда така:

- за аргумент 1: 

- за аргумент 2: 

- в общия случай за аргумент n:



Базата е достижима от всяка стойност на аргумента. Базата не може да бъде "прескочена".

Да се докаже, че

$$\forall n \geqslant 1 : F_{2n-1} = F_n^2 + F_{n-1}^2 \tag{2}$$

База: $n = 1$. Наистина, лявата страна става $F_{2 \cdot 1 - 1} = F_{2-1} = F_1 = 1$, а дясната страна става $F_1^2 + F_{1-1}^2 = F_1^2 + F_0^2 = 1 + 0 = 1$. ✓

Ползваме силна индукция. За някое $n \geqslant 1$ допускаме

$$F_1 = F_1^2 + F_0^2$$
$$F_3 = F_2^2 + F_1^2$$
$$\dots$$
$$F_{2n-3} = F_{n-1}^2 + F_{n-2}^2 \tag{3}$$
$$F_{2n-1} = F_n^2 + F_{n-1}^2 \tag{4}$$

Ще докажем

$$F_{2n+1} = F_{n+1}^2 + F_n^2 \tag{5}$$

Друг пример с д-во на св-во на числа на Fibonacci (2)

ВНИМАНИЕ: доказателството е формално некоректно!

$$
\begin{aligned}
F_{2n+1} &= F_{2n} + F_{2n-1} && \text{// по дефиниция} \\
&= F_{2n-1} + F_{2n-2} + F_{2n-1} && \text{// понеже } F_{2n} = F_{2n-1} + F_{2n-2} \\
&= 2F_{2n-1} + F_{2n-2} \\
&= 3F_{2n-1} - F_{2n-3} && \text{// понеже } F_{2n-1} = F_{2n-2} + F_{2n-3} \\
&= 3(F_n^2 + F_{n-1}^2) - (F_{n-1}^2 + F_{n-2}^2) && \text{// ползваме (4) и (3)} \\
&= 3F_n^2 + 2F_{n-1}^2 - F_{n-2}^2 \\
&= 3F_n^2 + 2F_{n-1}^2 - (F_n - F_{n-1})^2 && \text{// понеже } F_{n-2} = F_n - F_{n-1} \\
&= 2F_n^2 + 2F_nF_{n-1} + F_{n-1}^2 && \text{// понеже } F_{n-1} = F_{n+1} - F_n \\
&= 2F_n^2 + 2F_n(F_{n+1} - F_n) + (F_{n+1} - F_n)^2 \\
&= F_{n+1}^2 - F_n^2
\end{aligned}
$$

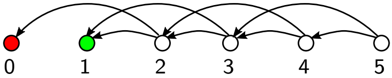
Но това е точно дясната страна на (5). **QED**

Първо, F_{2n-3} и F_{n-2} са недефинирани при $n = 1$, а в индуктивното предположение казахме, че $n \geqslant 1$, така че е възможно $n = 1$.

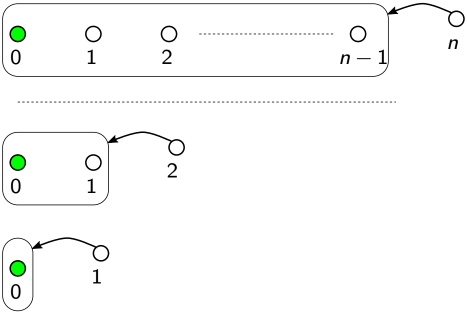
Второ, ако $P(n)$ е предикатът $F_{2n-1} = F_n^2 + F_{n-1}^2$, ето как "върви назад" доказателството на, да кажем, $P(5)$:

- P_5 се доказва чрез $P(4)$ и $P(3)$,
- P_4 се доказва чрез $P(3)$ и $P(2)$,
- P_3 се доказва чрез $P(2)$ и $P(1)$,
- P_2 се доказва чрез $P(1)$ и $P(0)$.

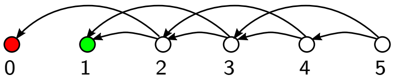
Имаме проблем: $P(0)$ не е дефинирано, понеже в него би имало $F_{0-1} = F_{-1}$. В някакъв смисъл, "прескачаме" базата $P(1)$:



По какво се отличава проблемното доказателство със силна индукция на слайдове (13) и (14) от общата схема, описана на слайд (5)? По това, че в общата схема доказателството за някое $P(n)$ става чрез "блок" $\boxed{P(0),\, P(1),\, \dots,\, P(n-1)}$, който обаче става все по-къс при движението назад, докато се "свие" само до $\boxed{P(0)}$, така че единствената база $P(0)$ е достатъчна:



При невалидното доказателство на слайдове (13) и (14), този "блок" винаги е с дължина 2, поради което базата бива "прескочена".



Ето коректно доказателство на (2). Базовите случаи са $n = 1$ и $n = 2$. Наистина, (2) става

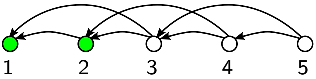
$$F_{2\cdot 1-1} = F_1^2 + F_0^2 \;\leftrightarrow\; F_1 = 1 + 0 \checkmark \quad // \text{ при } n = 1$$
$$F_{2\cdot 2-1} = F_2^2 + F_1^2 \;\leftrightarrow\; F_3 = 1 + 1 \checkmark \quad // \text{ при } n = 2$$

Индуктивното предположение е, за някое $n \geqslant 2$:

$$F_{2n-3} = F_{n-1}^2 + F_{n-2}^2$$
$$F_{2n-1} = F_n^2 + F_{n-1}^2$$

Сега F_{2n-3} и F_{n-2} са винаги дефинирани, тъй като $n \geqslant 2$.

Индуктивната стъпка е същата като на слайд (14). Да прескочим базата вече е невъзможно, понеже тя е “блок” от две съседни стойности.



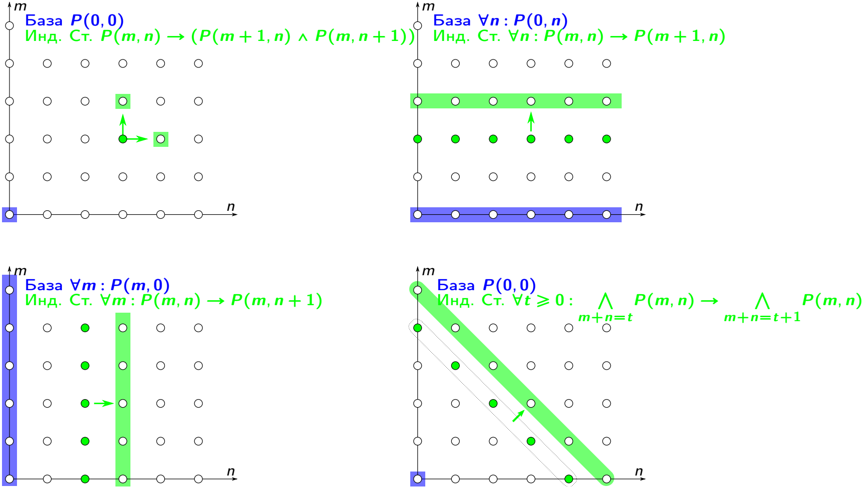
Доказваме предикат $P(x)$, като домейнът е някакво индуктивно дефинирано множество $M = (M_0, \mathcal{F})$. Схемата е тази.

- За всеки елемент x от M_0 проверяваме истинността на $P(x)$.
- Допускаме $P(x)$ за **произволно** $x \in M$ и въз основа на това допускане доказваме, че за всеки y, който се получава при прилагането на операциите от $\mathcal{F}$ върху текущото M, $P(y)$ е вярно.

Тази индукция се казва *структурна индукция*, на английски е *structural induction*, и се прилага широко в области като теорията на графите.

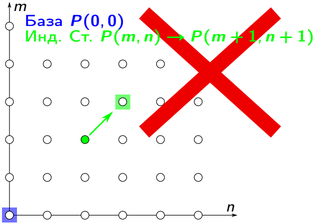
Всъщност, всяка индукция е структурна. Обикновената е върху естествените числа, а те са индуктивно дефинирано множество. Говорим за структурна индукция като нещо отделно по дидактични причини.

Доказваме предикат $P(m, n)$, където $m \in \mathbb{N}$ и $n \in \mathbb{N}$.



Отново става дума за достижимост от базата и на базата.

Това обаче е невалидно доказателство!



Нито всяка наредена двойка е достижима от базата, нито от всяка наредена двойка можем да достигнем базата. Тук има доказателство на $\forall n \in \mathbb{N} : P(n, n)$, но това не е същото като $\forall m, n \in \mathbb{N} : P(m, n)$.

Пример за д-во по индукция с две променливи (1)

Да се докаже по индукция

$$\forall m, n \in \mathbb{N}^+ : \sum_{k=1}^{m} k(k+1)\cdots(k+n-1) = \frac{m(m+1)\cdots(m+n)}{n+1} \qquad (6)$$

Нека $P(m,n)$ е предикатът със смисъл (6). За доказателството ще ползваме

$\forall n \geqslant 1 : P(1,n)$ като база

$\forall n \geqslant 1 : P(m,n) \rightarrow P(m+1,n)$ като индукт. предп. и стъпка

Базовият случай е $m = 1$, за всяко n. Няма да ползваме индукция по n, въпреки че е възможно. Ще докажем $\forall n \geqslant 1 : P(1, n)$ директно. Разглеждаме **произволно** $n' \geqslant 1$ и $P(1, n')$. По този начин се освободихме от квантора. Предикатът $P(1, n')$ е

$$\sum_{k=1}^{1} k(k+1)\cdots(1+n'-1) = \frac{1(1+1)\cdots n'(1+n')}{n'+1}$$

което е същото като

$$1 \cdot 2 \cdots n' = 1 \cdot 2 \cdots n'$$

което очевидно е вярно. Доказахме базата. ✓

Допускаме $P(m, n)$ за някои $m, n \in \mathbb{N}^+$. По-подробно, допускаме

$$\sum_{k=1}^{m} k(k+1)\cdots(k+n-1) = \frac{m(m+1)\cdots(m+n)}{n+1} \quad // \text{ за някои } m, n \in \mathbb{N}^+ \tag{7}$$

Разглеждаме

$$\left(\sum_{k=1}^{m} k(k+1)\cdots(k+n-1)\right) + (m+1)(m+2)\cdots(m+n) \tag{8}$$

От една страна, (8) е същото като

$$\sum_{k=1}^{m+1} k(k+1)\cdots(k+n-1) \tag{9}$$

заради свойствата на сумирането.

От друга страна, ако приложим индуктивното предположение (7) към (8), получаваме

$$
\begin{aligned}
&\frac{m(m+1)\cdots(m+n)}{n+1} + (m+1)(m+2)\cdots(m+n) = \\
&\frac{m(m+1)\cdots(m+n)}{n+1} + \frac{(m+1)(m+2)\cdots(m+n)(n+1)}{n+1} = \\
&\frac{m(m+1)\cdots(m+n) + (m+1)(m+2)\cdots(m+n)(n+1)}{n+1} = \\
&\frac{(m+1)(m+2)\cdots(m+n)(m+n+1)}{n+1}
\end{aligned}
\tag{10}
$$

От (9) и (10) заключаваме, че

$$
\sum_{k=1}^{m+1} k(k+1)\cdots(k+n-1) = \frac{(m+1)(m+2)\cdots(m+n)(m+n+1)}{n+1}
$$

Но това е точно $P(m+1, n)$. Използвайки индуктивното предположение (7), доказахме $P(m+1, n)$.
Съгласно принципа на математическата индукция, в сила е (6).

КРАЙ